GAMMA INTERNATIONAL UK LIMITED

INDEX

---

1. Correspondence

a) Letter Bhatt Murphy to Secretary of State for Business Innovation and Skills 12.07.12

b) Letter Treasury Solicitors to Bhatt Murphy solicitors 08.08.12

c) Letter Bhatt Murphy to Treasury Solicitors 09.08.12

d) Letter from Department for Business Innovation and Skills to Bhatt Murphy solicitors 11.09.12

2. Gamma International Literature

a) Finfisher: Government IT intrusion and remote monitoring solutions

b) Gamma International Egypt proposal

c) Gamma International Milipol Qatar 2012 exhibitor description.

3. Expert reports

a) University of Toronto The Citizen Lab Research Brief number 09-July 2012 "From Bahrain with Love: FinFisher's Spy Kit Exposed?"

b) University of Toronto The Citizen Lab Research Brief number 11-August 2012 "The SmartPhone Who Loved Me:

FinFisher Goes Mobile?"

c) Rapid 7 "Analysis of the FinFisher Lawful Interception Malware"

d) Internet Crime Complaints Centre (IC3) intelligence note 08.05.12

e) IC3 intelligence note 12.10.12

4. Press reports

a) The Guardian: British firm offered spy software to Egyptian regime – documents 28.04.11

b) BBC Radio 4 File on Four "UK firm denies 'cyber-spy' deal with Egypt" 20.09.11

c) The Observer: UK 'Exporting surveillance technology to repressive nations' 07.04.12

d) Bloomberg: Cyber Attacks on Activists Traced to Finfisher Spyware Of Gamma 25.07.12

e) Bloomberg "Gamma Says No Spyware Sold to Bahrain: May be Stolen Copy" 27.07.12

f) New York Times "Elusive FinSpy spyware pops up in ten countries". 13.08.12

g) New York Times "Software meant to fight crime is used to spy on dissidents" 30.08.12

Bhatt Murphy Solicitors

Our ref: MPS/FT/002295/0001
Your ref:
Email: m.scott@bhattmurphy.co.uk

27 Hoxton Square
London N1 6NN

Phone 020 7729 1115
Fax 020 7729 1117

www.bhattmurphy.co.uk
DX 36626 Finsbury

Secretary of State for Business Innovation and Skills
Third Floor, 'Orchard 3'
1 Victoria Street
London SW1H OET

12 July 2012

Dear Sir

Export controls for surveillance equipment

We represent Privacy International, a UK-registered charity that works to defend and promote the right to privacy. We write further to correspondence between our client and 10 Downing Street and the Head of Export Control from the Department for Business Innovation and Skills.

Our client is concerned that there appears to have been no substantive progress in the implementation in the UK of export controls for surveillance equipment where clearly urgent action needs to be taken. This letter is intended to be a letter before claim under the pre action protocol to which we would be grateful for a substantive response within the next 21 days.

Privacy International
As you will no doubt be aware, Privacy International is widely regarded as the leading, expert UK charity working on the right to privacy at an international level. As such, it is frequently called upon to give expert testimony to parliamentary and governmental committees around the world. It has advised and reported to international organisations such as the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development and the United Nations.

Privacy International campaigns for a world in which privacy is protected by governments and where technological developments strengthen, rather than undermine, the right to private life.

Summary of the issue
Ten years ago, the value of the global surveillance technology industry was negligible. Today, it is estimated at around $3 billion a year.

Export controls operating in the United Kingdom ("UK") and elsewhere have not kept pace with either developments in this technology, or the related

Partners
Hamish Arnott
Raju Bhatt
Simon Creighton
Fiona Murphy
Tony Murphy
Mark Scott

Solicitors
Nancy Collins
Shamik Dutta
Janet Farrell
Carolynn Gallwey
Alice Hardy
Sophie Naftalin
Nogah Ofer
Michael Oswald
Jed Pennington
Megan Phillips
Jane Ryan

Authorised and regulated by the Solicitors Regulation Authority No. 00287785

Community Legal Service
Criminal Defence Service
Specialist Help Service

growth of the industry. Indeed, there are, as we understand the situation, currently no monitoring or controls imposed on the export of these technologies by the British government.

As a consequence surveillance equipment and technology is now being exported from the UK by British companies to repressive regimes around the world without any controls. Privacy International believes that this equipment is being used by repressive foreign governments for a wide range of abuses. This includes not only serious breaches of the right to privacy but, at the most serious end of the spectrum, Privacy International believes such technology may be being used to gather information on individuals who are then arrested, tortured and, in some cases, executed.

Urgent action needs to be taken by the UK to address and remedy this situation.

Present UK legal position

The UK controls exports in accordance with the Export Control Act 2002 ('2002 Act') and the Export Control Order 2008, which seeks to control military or specified "dual use" items. In addition, there may exist a sanctions regime in place from time to time for specific countries as mandated by EU law.

The 2002 Act provides the power to impose export controls in relation to "goods of any description" (section 1) or "technical assistance of any description" (section 3). The Schedule to the Act provides that export and/or technical assistance controls may be imposed in relation to any goods and/or technical assistance the exportation or use of which is "capable of having a relevant consequence" (Schedule para 2). Such a consequence is defined *inter alia* as follows:

> "***Breaches of international law and human rights***
>
> D The carrying out anywhere in the world of (or of acts which facilitate)—
> (a) .....
>
> (b) .....
>
> (c) internal repression in any country;
>
> (d) breaches of human rights"

As stated by the Parliamentary Under-Secretary of State, Department for Business, Innovation and Skills (Baroness Wilcox) in response to Parliamentary Questions by Lord Alton of Liverpool on 21 November 2011 in respect of concerns about the export to repressive regimes of surveillance equipment by two UK companies, *Creativity Software* and *Detica*, it was

confirmed that such equipment is not currently subject to any export controls. Consequently the UK government claims it has absolutely no information on what equipment may have been sold to repressive governments such as Iran, Syria, Bahrain, Egypt, Tunisia and Libya.

Gamma International

Our client has concerns about a number of UK companies and their exports. These concerns are not limited to one company, one range of products or one country. We set out below specific information about Gamma International but it should be taken as illustrative of a wide scale problem and indicative of the need for the UK to take urgent action.

Gamma International are described on their website as:

> *"Working out of our development headquarters in Andover, United Kingdom, Gamma International's world-class intrusion and IT experts have invented a portfolio of intrusion products called FinFisher.*
>
> *The FinFisher product portfolio is solely offered to Law Enforcement and Intelligence Agencies.*
>
> *The FinFisher suite can be used as individual products and when interconnected give intelligence agencies advanced tools for unsurpassed IT investigation and surveillance techniques within the IT environment."*

The FinFisher range of products are marketed by promotional videos now within the public domain following release by Wikileaks.

Most of the FinFisher products covertly install malicious software (malware) on a user's computer or mobile phone without their knowledge by tricking the user into downloading fake updates from what appear to be legitimate sources such as Blackberry, iTunes or Adobe Flash. Once the updates are accepted by the user, the computer or mobile phone device is infected allowing full access to information held on it. One product, FinFly LAN, is marketed for use for surveillance of individuals staying in hotels. You will no doubt be aware that an Intelligence Note of 8 May 2012 prepared by the Internet Crime Center (IC3) has indicated that:

> *"[r]ecent analysis by the FBI and other government agencies demonstrates that malicious actors are targeting travelers' abroad through pop up windows while establishing an Internet connection in their hotel room."*

One of the products, FinFly ISP, involves a server being inserted in the core internet network of an internet provider to facilitate "infection" of specific target personal computers. A similar product, FinSpy Mobile, works in a similar way to infect mobile phones.

The promotional video with images and text shows :-

- a simulation of an agent deploying "the FinFly ISP server into the Core Network"
- "FinFly ISP [analysing] traffic for easy Target Identification"
- "The Target [using] his private DSL or Dial-Up Account"
- "FinFly ISP [sending] a fake iTunes update to the Target System"
- That "[t]he Target System is now infected with the FinSpy software"
- That "[t]he Headquarters has full access to the Target System"

When an individual's device is "infected", it allows access to emails, social media messaging, and Skype calls. These products also enable the entity doing the targeting to commandeer and remotely operate microphones and cameras on computers and mobile phones, thus effectively turning the targeted device into a bug which the target individual willingly and unknowingly keeps in close proximity.

Privacy International staff have considerable technical knowhow and expertise in the field and have also consulted widely. It is their clear view that the FinFisher range of products and other surveillance equipment of concern designed to access an individual's computer or other device without their consent can be distinguishable from other software which may have other uses and where export controls are not necessary.

The export of these products to repressive regimes

There is cogent evidence that the FinFisher products have been and are still being marketed and sold to repressive regimes. The examples set out below are illustrative of what our client believes to be a much wider problem.

Egypt

Concerns about human rights in Egypt need no introduction.

In April 2011 it was reported in the Guardian that two Egyptian human rights activists found documents from Gamma International amid hundreds of batons and torture equipment when they broke into the headquarters regime's notorious State Security Investigation service (SSI) in March 2011. One of the papers contained an offer dated 29 June 2010 to provide "FinSpy" software, hardware, installation and training to the SSI for 287,000 Euros. The BBC also reported on the issue in September 2011 that files from the Egyptian secret police's "Electronic Penetration Department" described Gamma's products as the "only security system in the world" capable of bugging Skype phone conversations on the internet. Further they noted that the documents detailed a five month trial by the Egyptian secret police which had "proved to be an effective electronic system for penetrating secure systems [which] accesses email boxes of Hotmail, Yahoo and Gmail networks."

Turkmenistan

Turkmenistan operates as a one-party state, dominated by the Democratic Party of Turkmenistan (DPT). Turkmenistan's human rights record has been roundly criticised by NGOs and international human rights bodies including Human Rights Watch and the UN Committee Against Torture (UNCAT).

According to Human Rights Watch http://www.hrw.org/europecentral-asia/turkmenistan:

> *"... five years after the death of dictator Saparmurad Niyazov, President Gurbanguly Berdymukhamedov's authoritarian rule remains entrenched, highlighting Turkmenistan's status as one of the world's most repressive countries. The country remains closed to independent scrutiny, media and religious freedoms are subject to draconian restrictions, human rights defenders face constant threat of government reprisal, and torture is widespread. Turkmenistan has the one of largest natural gas reserves in the world, and the Turkmenistan government continued to expand relations with foreign governments and international organizations, but with no meaningful outcomes for human rights promotion and protection."*

In June 2011 in its Concluding Observations of the Committee Against Torture, Turkmenistan, UNCAT expressed deep concerns over:

> *"... numerous and consistent allegations about the widespread practise of torture and ill-treatment of detainees".* A key area of concern was the Turkmen authorities' repression of activism and civil society, including *"numerous and consistent allegations of serious acts of intimidation, reprisals and threats against human rights defenders, journalists and their relatives, as well as the lack of information provided on any investigations into such allegations...human rights defenders have faced arrest on criminal charges, apparently in retaliation for their work, and trials in which numerous due process violations have been reported."*

The committee urged the Turkmeni government to:

> *"...ensure that human rights defenders and journalists, in Turkmenistan and abroad, are protected from intimidation or violence as a result of their activities."*

Given this context, it is of grave concern that press reports from Germany suggest that Gamma is exporting surveillance equipment and knowhow to Turkmenistan.

We also understand from the same reports that they are also exporting to Oman.

Grounds of challenge

Plainly there is a very real risk, if not an inevitability, that surveillance equipment, such as the FinFisher products, has been, and continues to be, exported to countries where it is highly likely to be used for internal repression and breaches of human rights.

Despite the grave consequences of exporting this equipment, it appears that you have not considered exercising your power to impose export controls under the relevant statutory provisions. Insofar as you have failed to consider exercising your power in light of the evidence outlined above, you have acted unlawfully. If you have considered these issues and concluded that the equipment in question is not capable of "internal repression" or "breaches of human rights" and therefore does not require export controls, that is a clear error of law. The facts set out above show that the equipment in question is clearly capable of contributing to internal repression and breaches of human rights, including breaches of the right to privacy, torture and potentially unlawful killing (all of which are clearly protected in international human rights instruments, see for example the International Covenant on Civil and Political Rights Arts 6, 7 and 17).

Actions now to be taken

We would be grateful for your confirmation within the next 14 days that you will be immediately imposing export controls in relation to surveillance equipment. In the event that you are not prepared to confirm this we would be grateful if you could provide reasons as to why no controls are to be put in place.

We would also be grateful if you could provide to us with appropriate disclosure including but not limited to:

1. All minutes of meetings/correspondence/discussion papers regarding concerns about the exports of surveillance technologies;
2. All minutes of meetings/correspondence/discussion papers regarding any proposals for any export controls on surveillance technologies;
3. Insofar as it is not included in the above, the discussion paper presented by the UK to the Wassenaar arrangement;
4. All minutes of meetings/correspondence with Gamma.

Costs

Due to Privacy International's limited financial resources and in view of the importance of the issues, the legal team including leading counsel have agreed to act under the terms of a "Conditional Fee Agreement" with provision for a success fee.

We sincerely hope for a positive response to this letter but in the event that one is not forthcoming then we reserve the right to issue proceedings without further recourse including if appropriate urgent injunctive relief.

In any such proceedings, because of our client's financial circumstances and given the public interest in bringing this challenge, we will be making an application for Protective Costs Order ("PCO"). We would ask, with a view to saving court time and public money that you undertake not to pursue our client for costs if the claim is unsuccessful. If you were prepared to give such an indication then in the spirit of co–operation our client's legal team will agree to forgo a success fee.

We await hearing from you.

Yours faithfully

Bhatt Murphy

c.c. Mr Tom Smith Head, Expert Control Organisation
Secretary of State for Foreign and Commonwealth Affairs

TSol
LAW AT THE HEART OF GOVERNMENT

Litigation Group

Treasury Solicitor's Department
One Kemble Street, London, WC2B 4TS

Bhatt Murphy Solicitors
DX 36626
Finsbury

DX 123242 Kingsway 6
Switchboard: 0207 210 3000
Direct Line: 0207 210 4711
Direct Fax: 020 7210 3001
francesca.debenham@tsol.gsi.gov.uk

Please Quote: Z1211844/FZD/B5
Your Reference: MPS/FT/002295/0001

AND BY EMAIL: m.scott@bhattmurphy.co.uk

8 August 2012

Dear Sirs

EXPORT CONTROLS FOR SURVEILLANCE EQUIPMENT - PROPOSED JR

1. We refer to your letter before claim under the pre-action protocol for judicial review dated 12 July 2012 (**"the PAP Letter"**). This is the response to that letter of the Secretary of State for Business Innovation and Skills (**"the Secretary of State"**). Please address any future correspondence in this matter to Francesca Debenham quoting the reference above.

2. You have expressed concern about certain *"surveillance equipment"*. The PAP Letter does not identify the relevant surveillance equipment, save to refer by way of example to the FinFisher products produced by a company called Gamma International. It simply alleges that surveillance equipment is being marketed and sold to *"repressive regimes"* where it is likely to be used for internal repression and breach of human rights. You have provided limited evidence in support of your allegations. The PAP Letter refers to two press articles, dating respectively from April and September 2011, suggesting that products produced by Gamma International may have been in the possession of Egyptian security forces. Further you make reference in passing to certain unspecified press reports from Germany, which apparently suggest that such products may have been exported to Turkmenistan and Oman.

3. On this limited basis, you assert that the Secretary of State has *"not considered exercising your power to impose export controls under the relevant statutory*

provisions", and has accordingly acted unlawfully. Alternatively, you assert that if the Secretary of State has in fact considered the exercise of his powers and if he has concluded that the *"the equipment in question" is "not capable of 'internal repression' and 'breaches of human rights'"*, then he has erred in law. In these circumstances, you require confirmation within 14 days that the Secretary of State *"will be immediately imposing export controls in relation to surveillance equipment"*. You do not identify the nature of the proposed export controls or the particular surveillance equipment to which they should apply.

4. The Secretary of State denies that he has acted unlawfully, whether as alleged or at all. The Secretary of State accordingly declines to provide the confirmation you have sought.

Regulation of the export of military and dual-use technologies

5. The United Kingdom is involved in the regulation of the export of military technologies, as well as dual-use technologies at the international level and at the EU level. Some surveillance equipment may be considered as dual-use technology (falling within the dual-use controls currently applicable in the UK) in cases where such technology has certain features e.g. use of cryptography (see further below). However, the regulation of dual-use technology in the UK mostly stems from concerted action at international level resulting in EU legislation directly applicable in the Member States. Whilst powers do exist to impose controls operating solely at the national level, such unilateral controls without the necessary international backing are considered to be ineffective as they can be easily circumvented and are therefore unlikely to have any significant impact in this instance in limiting the trade in surveillance equipment.

6. At the international level, the United Kingdom is a party to the Wassenaar Arrangement. The Wassenaar Arrangement addresses the trade in conventional arms, and "dual-use" goods and technologies, namely those that may be used for both military and civilian purposes. The 41 Participating States maintain a list of relevant goods and technologies in respect of which they have agreed to impose national export controls. The criteria for selection of dual-use items which should be included on the list and therefore subject to export controls include the ability to make a clear and objective specification of the item and the ability to apply controls

effectively. Furthermore, adoption of such controls should not impede legitimate civilian trade.

7. This Wassenaar list has formed the basis of the EU legislation controlling dual-use technology at EU level, namely Council Regulation (EC) No 428/2009 establishing a European regime for the control of exports, transfer, brokering and transit of certain dual-use goods (**"the Dual-Use Regulation"**). Both in the context of the Wassenaar Arrangement and at EU level, the United Kingdom has been at the forefront of attempts to establish and promote such regulation. Another example of relevant EU secondary legislation is Council Regulation (EC) No 1236/2005 establishing a European regime for governing trade with third countries in goods that could be used for the purpose of capital punishment or for the purpose of torture and other inhuman and degrading treatment **("the Torture Regulation").**

8. Most recently, and in the context of negotiations at international and EU level on sanctions against particular countries, the United Kingdom has supported the adoption of EU Regulations directly applicable in the UK and other Member States imposing enhanced restrictions on trade with countries posing a particularly severe risk of internal repression and human rights violations. In two cases, such enhanced restrictions have included controls on certain equipment, software and technology for monitoring or interception of internet or telephone communications. These are specified in Articles 4, 5 and Annex V of Council Regulation (EU) No 36/2012 of 18 January 2012 as amended concerning restrictive measures in view of the situation in Syria (**"the Syria Regulation"**), and Articles 1b, 1c and Annex IV of Council Regulation (EU) No 359/2011 as last amended by Council Regulation (EU) No 264/2012 of 23 March 2012 concerning restrictive measures directed against certain persons, entities and bodies in view of the situation in Iran (**"the Iran Regulation"**). Under these measures the competent authorities of the Member States shall not grant any authorisations for the sale, supply, export or transfer, directly or indirectly, of such equipment, or for the provision of related technical and financial assistance, if they have reasonable grounds to determine that such equipment or services would be used for monitoring or interception, by the Syrian or Iranian regimes or on their behalf, of internet or telephone communications in Syria or Iran

9. Whilst the EU has agreed to the immediate inclusion of controls on certain surveillance equipment as part of the existing sanctions against Iran and Syria in view of the particular seriousness of the situation of those countries, these controls are not

considered to be appropriate or proportionate for the purposes of being generally applied across the board. This is because they potentially include within their scope a range of equipment and technologies which have legitimate commercial uses. Applying such broad controls to all destinations, including those which do not raise the same concerns regarding human rights, would impose disproportionate burdens on legitimate trade. However, as explained further below the United Kingdom government is currently considering with its international and EU-level partners the most appropriate way of extending the existing regulation at the international and EU-level to encompass surveillance equipment more generally.

The Secretary of State's powers under the 2002 Act

10. Pursuant to sections 1 to 4 of the 2002 Act, the Secretary of State has power to make orders in respect of the imposition of export controls, transfer controls, technical assistance controls and trade controls in relation to goods and technology. Section 5 provides for general restrictions on the exercise of those powers, and specifies the circumstances in which they may be exercised. In particular, section 5(2) provides that controls *"may be imposed for the purpose of giving effect to any Community provision or other international obligation of the United Kingdom"*. Further section 5(4) provides that export controls *"may be imposed in relation to any description of goods within one or more of the categories specified in the Schedule for such controls"*. The Schedule provides at paragraph 2(1) that such controls *"may be imposed in relation to any goods the exportation or use of which is capable of having a relevant consequence"*. Paragraph 3(2)(D) specifies as relevant consequences *"The carrying out anywhere in the world of (or acts which facilitate)" "internal repression in any country"* and *"breaches of human rights"*.

11. Accordingly, the Secretary of State has power to make an order imposing export controls in relation to any goods, the exportation or use of which is capable of facilitating internal repression in any country or breaches of human rights. Whether he exercises that power is in the discretion of the Secretary of State, having regard to any of a wide range of factors that he rationally concludes might be relevant to such exercise.

12. The Secretary of State has issued a number of orders under the Export Control Act 2002 (**"the 2002 Act"**), including the Export Order 2008 (**"the 2008 Order"**). The 2008 Order makes provision supplementing the directly applicable requirements in

the Dual-Use Regulation and the Torture Regulation, the former giving effect to the obligations the United Kingdom has undertaken pursuant to the Wassenaar Arrangement to impose controls on the export of certain Dual-Use goods, which as explained above can include in some limited cases surveillance equipment. Where goods are subject to control, applications for licenses to export or trade in those goods are assessed on a case-by-case basis against the Consolidated Criteria relating to export licensing decisions announced to Parliament by the Secretary of State on 26 October 2000, taking into account all relevant factors such as the nature of the goods, the identity of the end-user, the proposed end-use, and risk of diversion to undesirable end-use, and that a licence would not be granted if to do so would breach the Criteria.

13. The Secretary of State, having carried out an assessment of the FinSpy system to which your letter specifically refers, has advised Gamma International that the system does require a licence to export to all destinations outside the EU under Category 5, Part 2 ('Information Security') of Annex I to the Dual-Use Regulation. This is because it is designed to use controlled cryptography and therefore falls within the scope of Annex I to the Dual-Use Regulation. The Secretary of State also understands that other products in the Finfisher portfolio could be controlled for export in the same way. Furthermore, it is likely that the same products would fall within the scope of the enhanced restrictions set out in the Syria Regulation and Iran Regulation if not already controlled under the Dual-Use Regulation as explained above, being "Remote infection equipment" specified in Part A of Annex V and of Annex IV of the Syria and Iran Regulations respectively. Accordingly, in so far as you maintain that all of the surveillance equipment to which you refer is not the subject of export controls in the United Kingdom, the Secretary of State does not consider that to be correct.

The grounds of challenge

14. As to your primary case, the Secretary of State continues at all times to keep under consideration the exercise of his powers to impose export controls under the 2002 Act. You assert in the alternative that the Secretary of State has concluded *"the equipment in question"* is not capable of *"internal repression"* or *"breaches of human rights"*. If and in so far as you are referring to the FinFisher range of products manufactured by Gamma International, the Secretary of State has reached no such conclusion. It remains wholly unclear what other equipment you assert falls within this category; or what export controls that you maintain ought to be imposed.

Furthermore, as set out above, in relation to equipment falling within the scope of the Dual-Use Regulation that was sought to be exported, the risks associated with use would be considered on a case-by-case basis.

15. In any event, and more generally, the regulation of the export of forms of surveillance equipment is an important and complex area of policy requiring careful and ongoing consideration. Moreover, the identification of the relevant types of surveillance equipment that might be subject to any form of further export control requires detailed analysis as this is a technically complex area in which technological developments are fast-moving. There are legitimate countervailing interests that the Secretary of State would have to take into account. In particular, export controls should not operate so as to impose a disproportionate restriction on the legitimate trade in goods and technology. Much of the technology associated with surveillance equipment might also have perfectly legitimate uses in the civilian telecommunications sector. Further, any restriction will only be fully effective at international level and in any event needs to be consistent with the requirements of EU law, and the obligations it imposes with respect to national controls on export of goods. The UK is at the forefront of negotiations at international and EU level aimed at resolving the issues set out above so that technology of concern can be properly identified and regulated at international level.

16. Having considered matters further in the light of these matters and of your letter:

(1) The Secretary of State remains of the view that, subject to the steps referred to below, it would not be appropriate at this time to make any unilateral structural or legislative change to the UK domestic regime. He will continue to keep that option under review.

(2) He proposes to continue to engage with United Kingdom companies supplying surveillance equipment in order to clarify what equipment falls within the scope of existing controls on exports, and in order to ensure that he remains informed as to the state of that market. In this context, and as noted above, the Secretary of State has concluded that the FinSpy product is subject to export control under the provisions of the Dual-Use Regulation.

(3) Further, he is actively considering the possibility of international and/or EU level agreement to further restrictions on the export of surveillance equipment. His current view is that this is by some measure the better option, if further

regulation is required. A unilaterally imposed national restriction on the export from the UK of surveillance equipment without international support would not be effective, as it could be easily circumvented given the likelihood that many of the companies which manufacture such equipment will have offices in other EU and third countries. Finally, it is to be noted that these issues are currently being ventilated amongst the parties to the Wassenaar Arrangement at the initiative of the United Kingdom.

17. In these circumstances, you are invited to reconsider your threat of proceedings.

Costs

18. We note that, in relation to any future proceedings that might be brought, you assert an intention to apply for a Protective Costs Order (**"PCO"**). In order to relieve you of having to make such an application, you have asked the Secretary of State to *"undertake not to pursue our client for costs if the claim is unsuccessful"*. The Secretary of State declines your request:

    (1) He considers that your proposed grounds of challenge proceed on an erroneous basis and are without merit.

    (2) You have failed to provide information that is necessary to allow proper consideration of your request for an undertaking. For example, you have failed to provide any particulars of the financial position of your client, Privacy International.

    (3) Finally, your position appears to be that, if a costs undertaking were to be given, in the event that you should succeed you should nonetheless be permitted to recover all of the costs of any claim you decide to bring at full commercial rates. You note that your legal team, including leading counsel, are operating under the terms of a conditional fee agreement with provision for a success fee, and that you are willing only to forego the relevant success fee if the Secretary of State provides the proposed undertaking. The Secretary of State does not consider that, in this case, that would provide a proper basis for an undertaking to be given.

19. In the circumstances set out above your request for disclosure is also not appropriately made at this stage (leaving aside the difficulties with the substance of

the requests you have made). This request is also being treated as a Freedom of Information Request. A response will be provided in this regard by no later than 13 August 2012.

Yours faithfully

Francesca Debenham
For the Treasury Solicitor

Our ref: MPS/FT/ 001943/0002
Your ref: Q102850F/SMB/B4
Email: m.scott@bhattmurphy.co.uk

Bhatt Murphy Solicitors

27 Hoxton Square
London N1 6NN

Phone 020 7729 1115
Fax 020 7729 1117

www.bhattmurphy.co.uk
DX 36626 Finsbury

Treasury Solicitors

DX 123242 KINGSWAY

By DX & email

9 August 2012

Partners
Hamish Arnott
Raju Bhatt
Simon Creighton
Fiona Murphy
Tony Murphy
Mark Scott

Solicitors
Nancy Collins
Shamik Dutta
Janet Farrell
Carolynn Gallwey
Alice Hardy
Sophie Naftalin
Nogah Ofer
Michael Oswald
Jed Pennington
Megan Phillips
Jane Ryan

Authorised and regulated by the Solicitors Regulation Authority No. 00287785

Dear Madam

Export controls for surveillance equipment

Thank you for your email of 8 August 2012 which we will be considering in more detail with our client.

For present purposes we note that your client *"having carried out an assessment of the FinSpy system....has advised Gamma International that the system does require a licence to export to all destinations outside the EU"*. Some issues immediately arise which we would be grateful if you could provide clarification on:

1. When and in what circumstances was this assessment carried out, the conclusion reached and the advice given that a licence to export was required?
2. Had Gamma International previously sought advice from your client as to whether the FinSpy system required export control, when was this and what was the advice given?
3. What audit has been carried out of the export of the FinSpy system to countries outside the EU prior to the advice referred to in 1 above?
4. What enforcement action is/will be taken against Gamma International for the previous export of the FinSpy system without a licence?
5. Has Gamma International been required to retrospectively apply for licences for the previous export of the FinSpy system? If not why not?
6. Has Gamma International sought any licences to export the FinSpy system and/or provide technical assistance, if so to which countries and which have been granted and which have been refused?
7. Notwithstanding the generality of question 6 above, material in the public domain suggests that the FinSpy system has been used in Egypt, Turkmenistan, Bahrain, Dubai, Ethiopia, Indonesia, Mongolia and Qatar. Has Gamma sought any licences for export of FinSpy or

Community Legal Service
Criminal Defence Service
Specialist Help Service

the provision of technical assistance to any of these countries? If so which ones and were licences granted or refused?

8. Kindly provide a detailed explanation and supporting documentation of exactly what components of FinSpy is controlled?

We await hearing from you.

Yours faithfully

Bhatt Murphy

BIS | Department for Business Innovation & Skills

Europe, International Trade and Development
Export Control Organisation
3rd Floor
1 Victoria Street
London
SW1H OET

Enquiries +44 (0)20 7215 5000
Minicom +44 (0)20 7215 6740
www.bis.gov.uk
Tom Smith@bis.gsi.gov.uk

Bhatt Murphy Solicitors
m.scott@bhattmurphy.co.uk

Direct line +44 (0)207 215 4355
Local fax +44 (0)20 7215 0531
Our ref 12/1303
Your ref MPS/FT/001943/0002

Date 11 September 2012

Dear Sir/Madam,

I refer to your letter dated 9 August 2012 to the Treasury Solicitor's Department with the subject heading 'export controls for surveillance equipment', which we received on 13 August. I am replying in my capacity as the Head of the Export Control Organisation (ECO) within the Department for Business, Innovation and Skills (BIS).

You have asked eight questions. We have treated some of these as a request for disclosure of information under the Freedom of Information Act 2000 (FoIA) in accordance with Department policy, on the basis of the structure of the questions. These questions have been considered against the information BIS held at the time your request was received on 13 August. We have considered the remaining questions without reference to the FoIA as questions of Government policy.

I have answered your questions in the order they were posed for ease of reference. Questions 1, 2, 6, 7 and 8 have been treated as Freedom of Information requests. For the avoidance of doubt, questions 3, 4 and 5 have been considered without reference to the FoIA as questions of Government policy.

Q1 When and in what circumstances was this assessment carried out, the conclusion reached and the advice given that a licence to export was required?

Gamma International submitted a Control List Classification (CLC) enquiry to the ECO (i.e. an enquiry as to whether certain goods or technology fall within any of the controlled lists) in June 2012 and advice was provided by the ECO on 2 August 2012.

Q2 Had Gamma International previously sought advice from your client as to whether the FinSpy system required export control, when was this and what was the advice given?

Gamma International did not previously seek such advice from the ECO.

Q3 What audit has been carried out of the export of the FinSpy system to countries outside the EU prior to the advice referred to in 1 above?

No such audit has been carried out. BIS only has powers under the Export Control Order 2008 to audit exports made under certain licences. Any audit of other exports would fall to Her Majesty's Revenue and Customs (HMRC).

Q4 What enforcement action is/will be taken against Gamma International for the previous export of the FinSpy system without a licence?

Enforcement of export controls is the responsibility of HMRC. BIS does not comment on enforcement issues.

Q5 Has Gamma International been required to retrospectively apply for licences for the previous export of the FinSpy system? If not why not?

BIS does not issue licences retrospectively. Other than in the case of certain Open General Export Licences, where an exporter may register for use of the licence up to 30 days after the first export under that licence, an exporter must have an appropriate licence in place prior to the export of the goods. However, none of these Open General Export Licences would be appropriate for exports of the FinSpy system.

Q6 Has Gamma International sought any licences to export the FinSpy system and/or provide technical assistance, if so to which countries and which have been granted and which have been refused?

Gamma International have not sought any such licences.

Q7 Notwithstanding the generality of question 6 above, material in the public domain suggests that the FinSpy system has been used in Egypt, Turkmenistan, Bahrain, Dubai, Ethiopia, Indonesia, Mongolia and Qatar. Has Gamma sought any licences for export of FinSpy or the provision of technical assistance to any of these countries? If so which ones and were licences granted or refused?

I refer you to the answer at Q6.

In addition, if you or your client hold specific information on breaches of export controls by UK nationals or companies we would strongly encourage you to report this information to the Customs Confidential helpline

(http://search2.hmrc.gov.uk/kb5/hmrc/contactus/view.page?record=k9zpyaj9go) so that the appropriate action can be taken.

Q8 Kindly provide a detailed explanation and supporting documentation of exactly what components of FinSpy is controlled?

As paragraph 13 of the Treasury Solicitors Department's letter to you of 8 August explained, BIS has advised Gamma International that the FinSpy system does require a licence to export to all destinations outside the EU under Category 5, Part 2 ('Information Security') of Annex I to the Dual use Regulation, because it is designed to use controlled cryptography.

In addition, I can confirm that we hold information falling within scope of your request. The information relates to substantive discussions with Gamma International as part of the export licensing process.

The information requested falls within the scope of section 41(1) of the FoIA (information provided in confidence) and is exempt from disclosure because it was provided to the Department in confidence; the release of this information would constitute a breach of confidence which could be actionable in court.

Section 41(1) is an absolute exemption for the purposes of the FoIA. However, in reaching the decision not to release the information requested, the Department has nonetheless also considered whether the information should be released in the public interest, as the public interest test is inherent within the law of confidence.

Having considered all of the known public interest factors for and against disclosure of the information requested, it is the Department's view that there is a strong public interest in protecting this confidence and withholding this information; there are no public interest considerations in relation to this information which outweigh the public interest against disclosure of this information or which would require us to set the duty of confidence aside.

In relation to the questions which have been considered under the terms of the FoIA, if you are unhappy with the result of your request for information, you may request an internal review within two calendar months of the date of this letter. If you wish to request an internal review, please contact me.

If you are not content with the outcome of the internal review, you have the right to apply directly to the Information Commissioner for a decision. The Information Commissioner can be contacted at: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Please remember to quote the reference number above in any future communications.

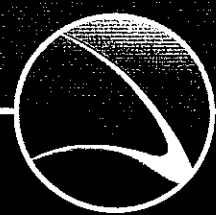
BIS | Department for Business Innovation & Skills

If you would like to follow-up on any of the questions that have not been considered under the FoIA please also contact me directly.

Yours sincerely,

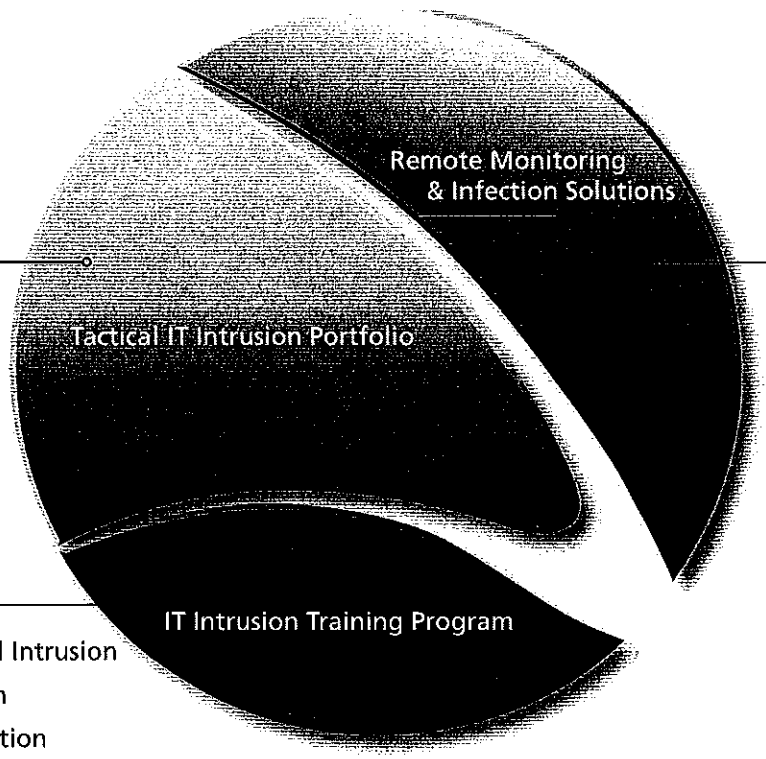
Tom Smith
Head of the Export Control Organisation

FINFISHER™: GOVERNMENTAL IT INTRUSION AND REMOTE MONITORING SOLUTIONS



WWW.GAMMAGROUP.COM

FINFISHER™
IT INTRUSION



- FinIntrusion Kit
- FinUSB Suite
- FinFireWire

FinSpy
- FinSpy
- FinSpy Mobile

FinFly
- FinFly USB
- FinFly LAN
- FinFly Web
- FinFly ISP

- Basic & Advanced Intrusion
- Wireless Intrusion
- Practical Exploitation
- Web Application Penetration
- Custom IT Intrusion Training & Consulting

WWW.GAMMAGROUP.COM

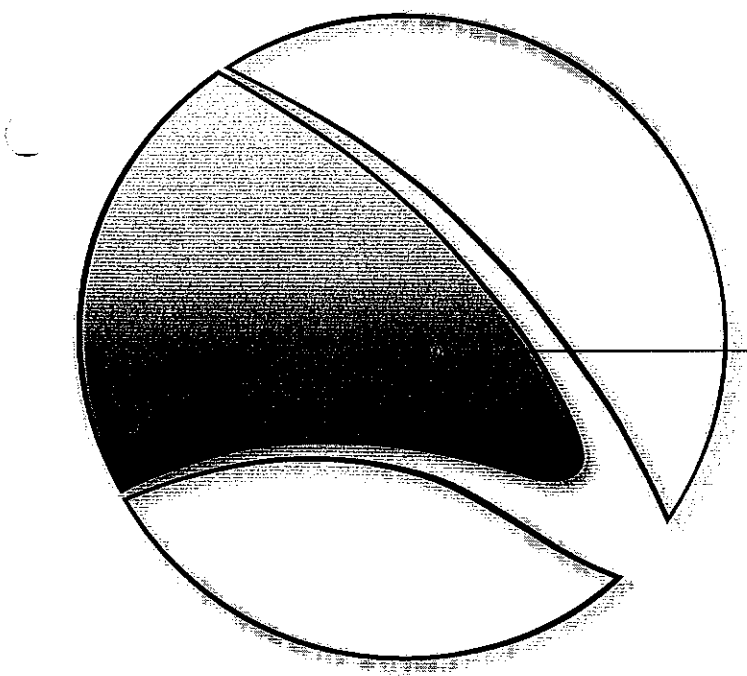
FINFISHER™
IT INTRUSION

Tactical IT Intrusion Portfolio

FININTRUSION KIT

FINUSB SUITE

FINFIREWIRE



Gamma addresses ongoing developments in the IT Intrusion field with solutions to enhance the capabilities of our clients. Easy to use high-end solutions and techniques complement the intelligence community's knowhow enabling it to address relevant Intrusion challenges on a tactical level.

FINFINTRUSION KIT

FinIntrusion Kit was designed and developed by world-class IT Intrusion specialists, who have over 10 years of experience in their area through their work in several Tiger Teams (Red Teams) in the private and government sector assessing the security of different networks and organizations.

The FinIntrusion Kit is an **up-to-date and covert** operational Kit that can be used for most common **IT Intrusion Operations** in defensive and offensive areas. Current customers include **Military CyberWar Departments, Intelligence Agencies, Police Intelligence and other Law Enforcement Agencies**.

QUICK INFORMATION	
Usage:	· Strategic Operations · Tactical Operations
Capabilities:	· Break WEP/WPA Encryption · Network Monitoring (including SSL Sessions) · IT Intrusion Attacks
Content:	· Hardware/Software

Usage Example 1: Technical Surveillance Unit

The FinIntrusion Kit was used to break **the WPA encryption** of a Target's home Wireless network and then monitor his **Webmail (Gmail, Yahoo, ...) and Social Network (Facebook, MySpace, ...) credentials**, which enabled the investigators to **remotely monitor** these accounts from Headquarters without the need to be close to the Target.

Usage Example 2: IT Security

Several customers used the FinIntrusion Kit to successfully **compromise the security** of networks and computer systems for **offensive and defensive** purposes using various Tools and Techniques.

Usage Example 3: Strategic Use-Cases

The FinIntrusion Kit is widely used to remotely gain access to Target Email Accounts and Target Web-Servers (e.g. Blogs, Discussion Boards) and monitor their activities, including Access-Logs and more.

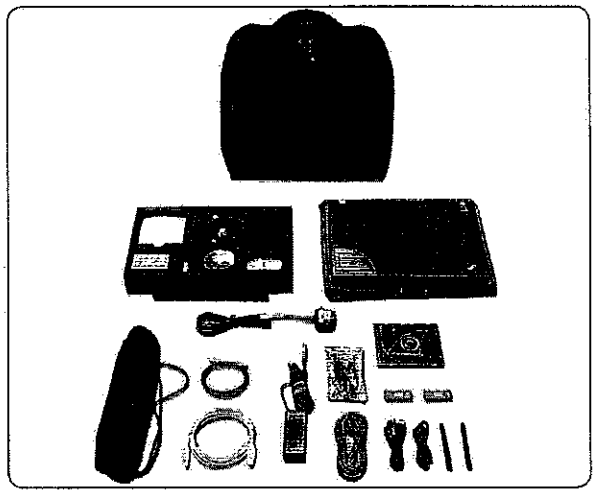
Feature Overview

- Discovers **Wireless LANs (802.11) and Bluetooth® devices**
- Recovers WEP (64 and 128 bit) Passphrases **within 2-5 minutes**
- **Breaks WPA1 and WPA2** Passphrases using Dictionary Attacks
- Actively monitors Local Area Network (Wired and Wireless) and **extracts Usernames and Passwords even for TLS/SSL-encrypted sessions**
- Emulates **Rogue Wireless Access-Point** (802.11)
- Remotely **breaks into Email Accounts** using Network-, System- and Password-based Intrusion Techniques
- **Network Security Assessment** and Validation

For a full feature list please refer to the Product Specifications.

FININTRUSION KIT

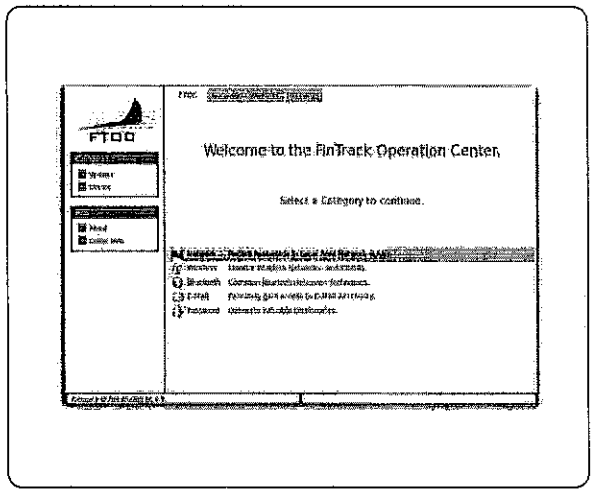
Product Components



FinIntrusion Kit - Covert Tactical Unit

Basic IT Intrusion Components:

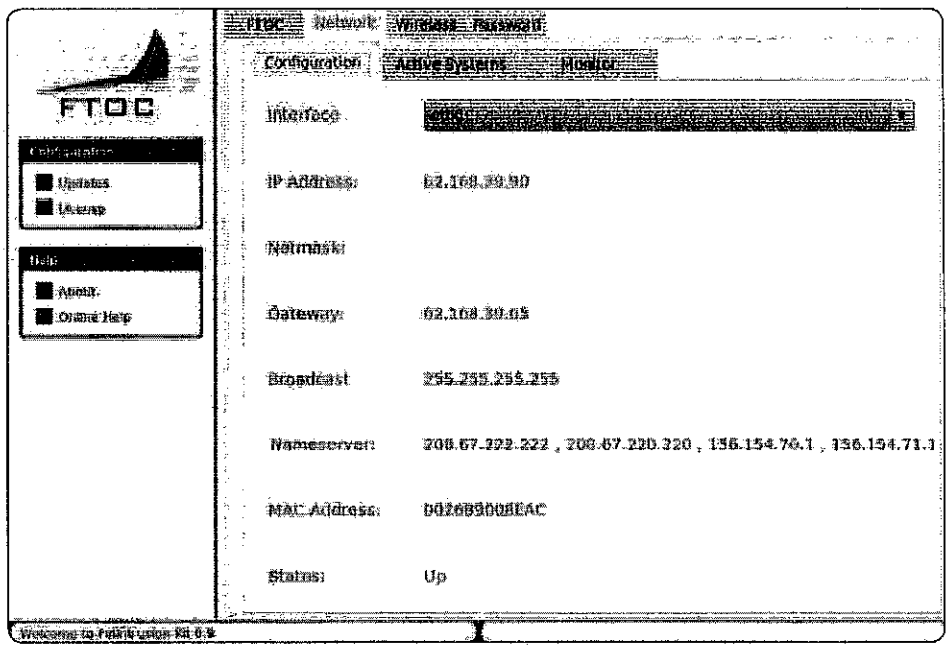
- High-Power WLAN Adapter
- High-Power Bluetooth Adapter
- 802.11 Antennas
- Many Common IT Intrusion Devices



FinTrack Operation Center

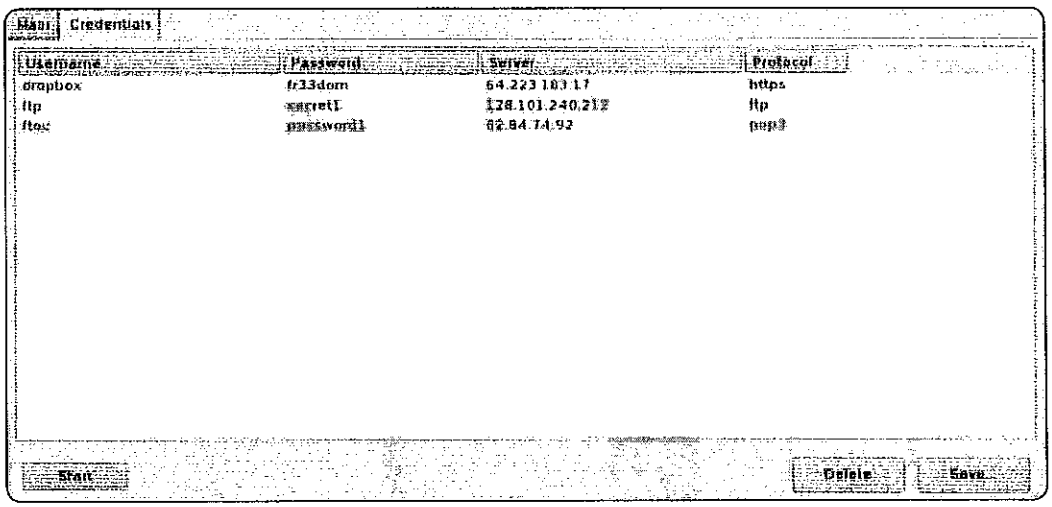
- Graphical User Interface for Automated IT Intrusion Attacks

Automated LAN/WLAN Monitoring



LAN/WLAN Active Password Sniffer

Captures even SSL-encrypted data like Webmail, Video Portals, Online-Banking and more



FINUSB SUITE

The FinUSB Suite is a flexible product that enables Law Enforcement and Intelligence Agencies to quickly and securely extract forensic information from computer systems without the requirement of IT-trained Agents.

It has been used in successful operations around the world where valuable intelligence has been acquired about Targets in covert and overt operations.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Information Gathering · System Access · Quick Forensics
Content:	· Hardware/Software

Usage Example 1: Covert Operation

A source in an Organized Crime Group (OCG) was given a FinUSB Dongle that secretly extracted Account Credentials of Web and Email accounts and Microsoft Office documents from the Target Systems, while the OCG used the USB device to **exchange regular files** like Music, Video and Office Documents.

After returning the USB device to Headquarters the gathered data could be decrypted, analyzed and used to constantly monitor the group remotely.

Usage Example 2: Technical Surveillance Unit

A Technical Surveillance Unit (TSU) was following a Target that frequently visited random Internet Cafés making monitoring with Trojan-Horse-like technology impossible. The FinUSB was used to extract the **data left on the public Terminals** used by the Target after the Target left.

Several documents that the Target opened in his web-mail could be recovered this way. The gathered information included crucial Office files, Browsing History through Cookie analysis, and more.

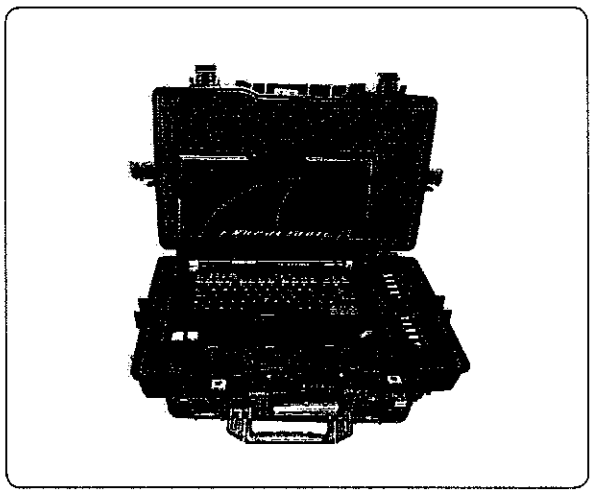
Feature Overview

- Optimized for **Covert Operations**
- Easy usability through **Automated Execution**
- **Secure Encryption** with RSA and AES
- Extraction of **Usernames and Passwords** for all common software like:
  - Email Clients
  - Messengers
  - Browsers
  - Remote Administration Tools
- **Silent Copying of Files** (Search Disks, Recycle-Bin, Last opened/edited/created)
- Extracting **Network Information** (Chat Logs, Browsing History, WEP/WPA(2) Keys, ...)
- Compilation of **System Information** (Running/Installed Software, Hard-Disk Information, ...)

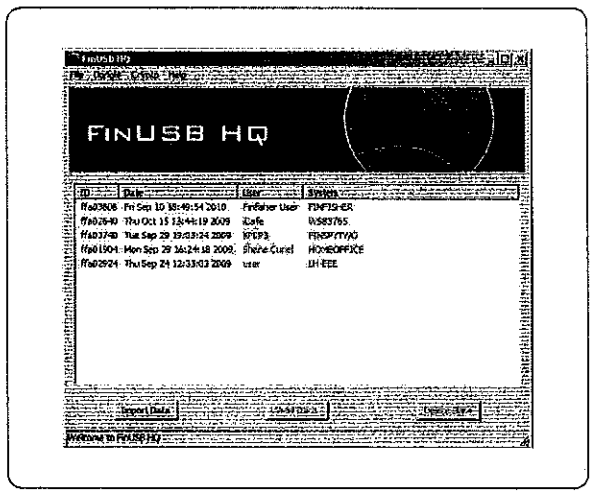
For a full feature list please refer to the Product Specifications.

FINUSB SUITE

Product Components

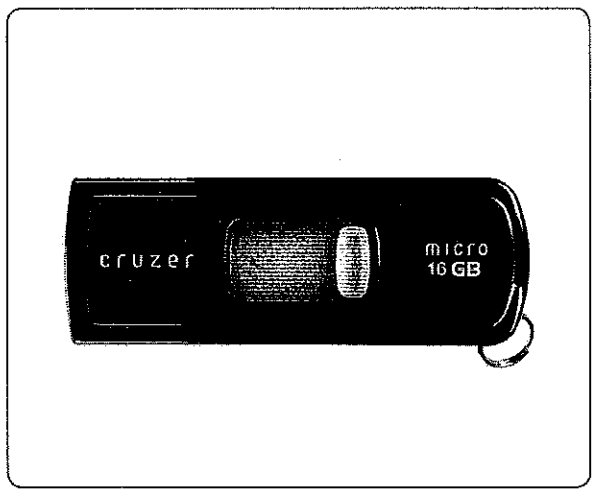


FinUSB Suite - Mobile Unit



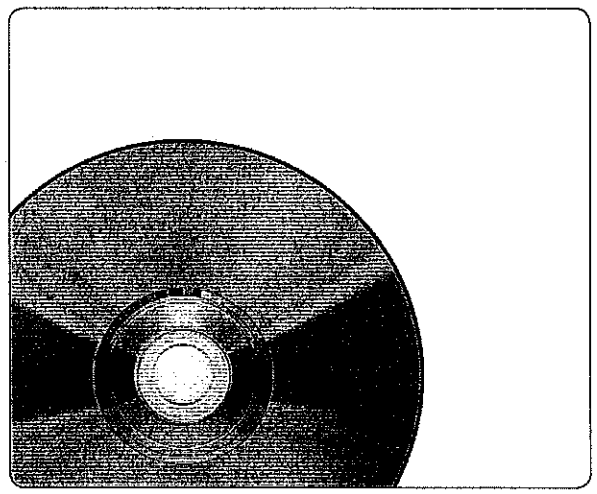
FinUSB HQ

- Graphical User Interface to decrypt and analyze gathered Data
- Configure Dongle Operational Options



10 FinUSB Dongle (U3 - 16GB)

- Covertly extracts data from system
- Encrypts Data on-the-fly



FinUSB - Windows Password Bypass

- Bypass Windows Logon without permanent system modifications

FINUSB SUITE

Easy Usability



1. Pick up a FinUSB Dongle



2. Configure all desired Features / Modules and update your FinUSB Dongle with FinUSB HQ



3. Go to your Target System



4. Plug in your FinUSB Dongle



5. Wait until all data is transferred



6. Go back to your FinUSB HQ

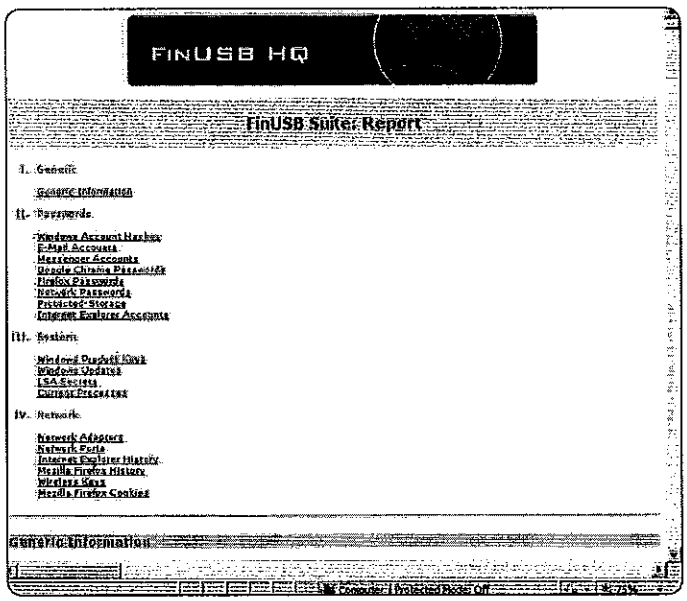


7. Import all Data from FinUSB Dongle



8. Generate Report

Professional Reports



FINFIREWIRE

Technical Surveillance Units and Forensic Experts often face a situation where they need to access a running computer system without shutting it down in order to prevent data loss or save essential time during an operation. In most cases, the Target System is protected with a **password-enabled Screensaver** or the target user is not logged in and the **Login Screen** is active.

FinFireWire enables the Operator to quickly and covertly **bypass the password-protected** screen and access the Target System without leaving a trace or harming essential forensic evidence.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Bypass User Password · Covertly Access System · Recover Passwords from RAM · Enable Live Forensics
Content:	· Hardware/Software

Usage Example 1: Forensic Operation

A **Forensic Unit** entered the apartment of a Target and tried to access the computer system. The computer was **switched on but the screen was locked.**
As they were not allowed, for legal reasons, to use a Remote Monitoring Solution, they would have **lost all data** by switching off the system as the **hard-disk was fully encrypted.** FinFireWire was used to **unlock the running Target System** enabling the Agent to **copy all files** before switching the computer off and taking it back to Headquarters.

Usage Example 2: Password Recovery

Combining the product with **traditional Forensic applications** like Encase®, Forensic units used the **RAM dump functionality** to make a snapshot of the current RAM information and **recovered the Hard-Disk encryption passphrase** for TrueCrypt's full disk encryption.

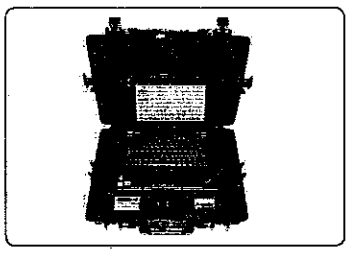
Feature Overview

- **Unlocks User-Logon** for every User-Account
- Unlocks **Password-Protected Screensaver**
- Full Access to **all Network Shares** of User
- **Dumps full RAM** for Forensic analysis
- Enables live forensics **without rebooting** the Target System
- User password is **not changed**
- Supports **Windows, Mac and Linux systems**
- Works with **FireWire/1394, PCMCIA and Express Card**

For a full feature list please refer to the Product Specifications.

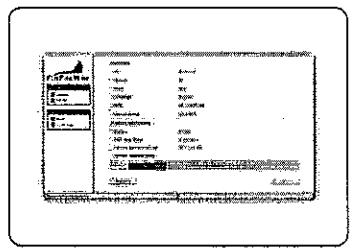
FINFIREWIRE

Product Components



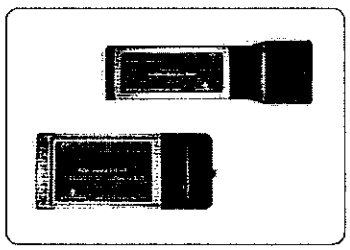
FinFireWire - Tactical Unit

· Complete Tactical System



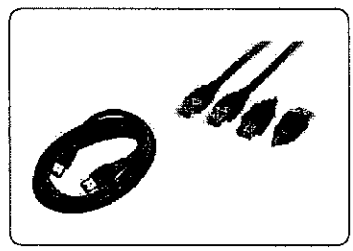
Point-and-Click User Interface

· Easy-to-use User Interface



Connection Adapter Cards

· PCMCIA and ExpressCard Adapter for Target Systems without FireWire port



Universal FinWire CableSet

· 4 pin to 4 pin
· 4 pin to 6 pin
· 6 pin to 6 pin

Usage



1. Go to your Target System



2. Start FinFireWire



3. Plug in FireWire Adapter & Cable



4. Select a Target



5. Wait until System is unlocked

The information contained herein is confidential and subject to change without notice. Gamma Group International shall not be liable for technical or editorial errors or omissions contained herein.

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

Remote Monitoring & Infection Solutions

FINSPY

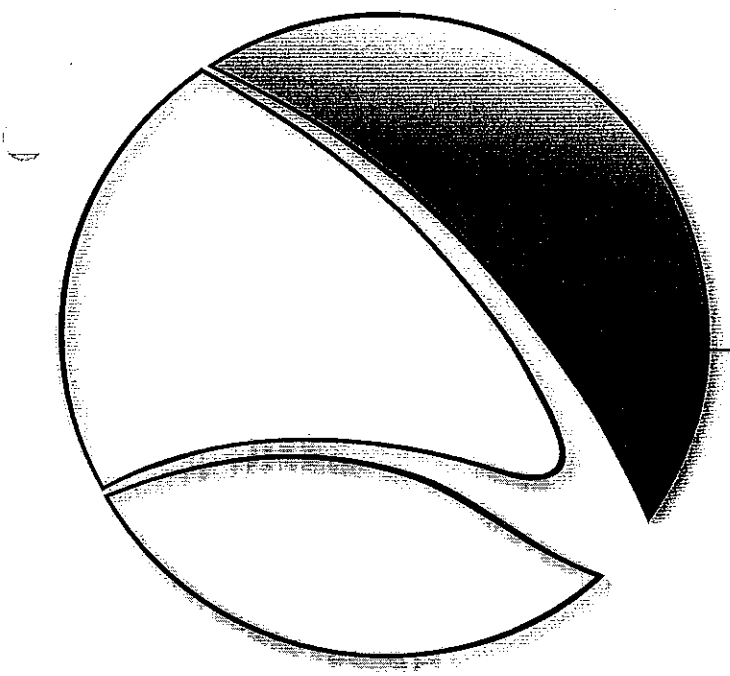
FINSPY MOBILE

FINFLY USB

FINFLY LAN

FINFLY WEB

FINFLY ISP



The Remote Monitoring and Infection Solutions are used to access target systems to give full access to stored information with the ability to take control of target system's functions to the point of capturing encrypted data and communications. When used in combination with enhanced remote infection methods, Government Agencies will have the capability to remotely infect target systems.

FINSPY

FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face the current challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**.

Traditional Lawful Interception solutions face new **challenges** that can only be solved using active systems like FinSpy:
- Data not transmitted over any network
- Encrypted Communications
- Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **for many years**, and valuable intelligence has been gathered about Target Individuals and Organizations.

When FinSpy is installed on a computer system it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

QUICK INFORMATION	
Usage:	· **Strategic Operations** · **Tactical Operations**
Capabilities:	· **Remote Computer Monitoring** · **Monitoring of Encrypted Communications**
Content:	· **Hardware/Software**

Usage Example 1: Intelligence Agency

FinSpy was installed on several computer systems inside **Internet Cafes in critical areas** in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were taken while they were using the system.

Usage Example 2: Organized Crime

FinSpy was **covertly deployed on the Target Systems** of several members of an Organized Crime Group. Using the **country tracing and remote microphone** access, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Computer – Example Features:

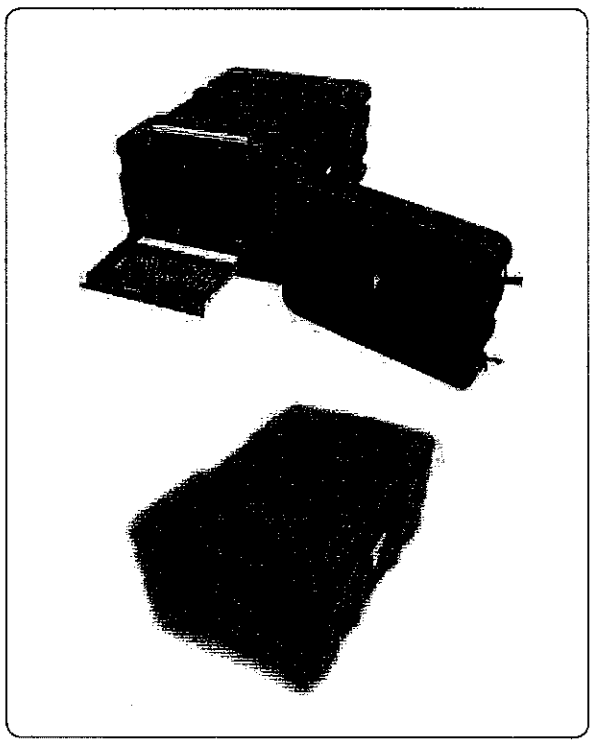
- Bypassing of 40 regularly tested Antivirus Systems
- **Covert Communication** with Headquarters
- Full **Skype Monitoring** (Calls, Chats, File Transfers, Video, Contact List)
- Recording of **common communication** like Email, Chats and Voice-over-IP
- **Live Surveillance** through Webcam and Microphone
- **Country Tracing** of Target
- **Silent extracting of Files** from Hard-Disk
- **Process-based Key-logger** for faster analysis
- **Live Remote Forensics** on Target System
- **Advanced Filters** to record only important information
- Supports most common Operating Systems (**Windows, Mac OSX** and **Linux**)

Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Security Data Encryption and Communication using **RSA 2048 and AES 256**
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality (LEMF)

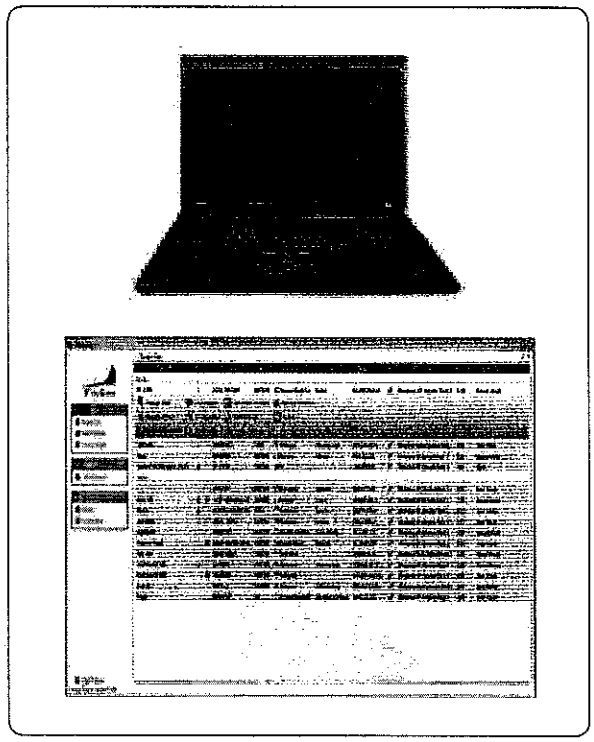
For a full feature list please refer to the Product Specifications.

Product Components



FinSpy Master and Proxy

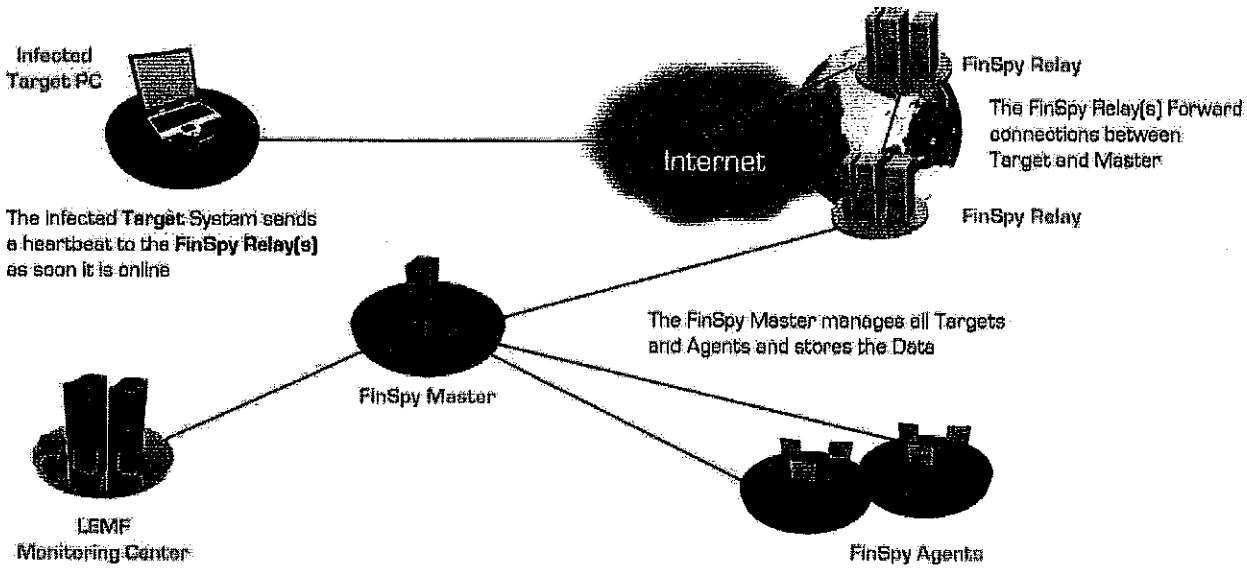
- Full Control of Target Systems
- Evidence Protection for Data and Activity Logs
- Secure Storage
- Security-Clearance based User- and Target Management



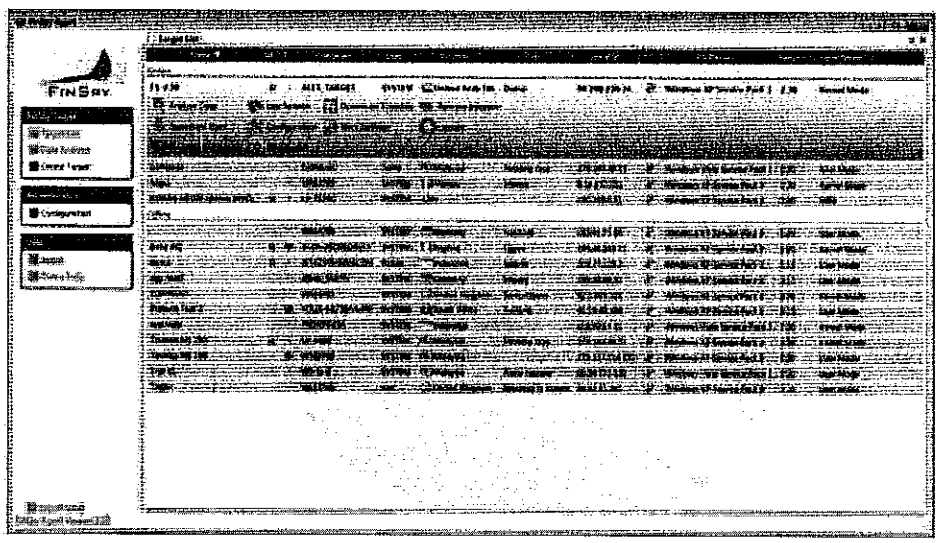
FinSpy Agent

- Graphical User Interface for Live Sessions, Configuration and Data Analysis of Targets

Access Target Computer Systems around the World

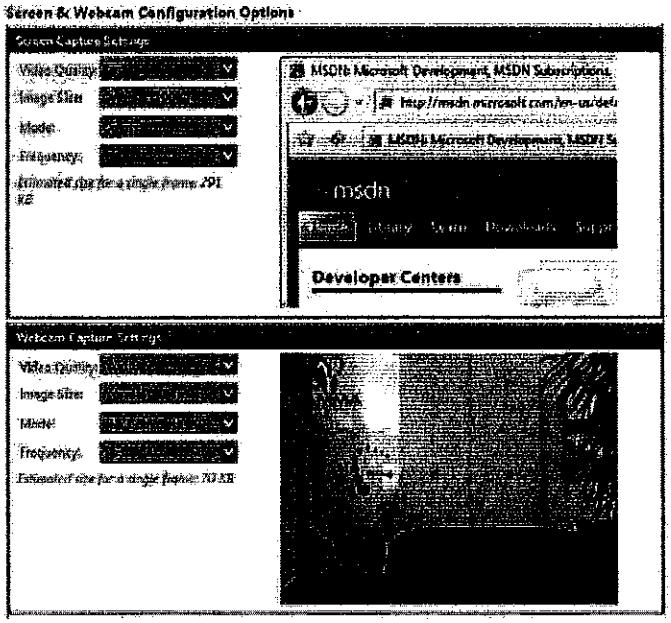


Easy to Use User Interface

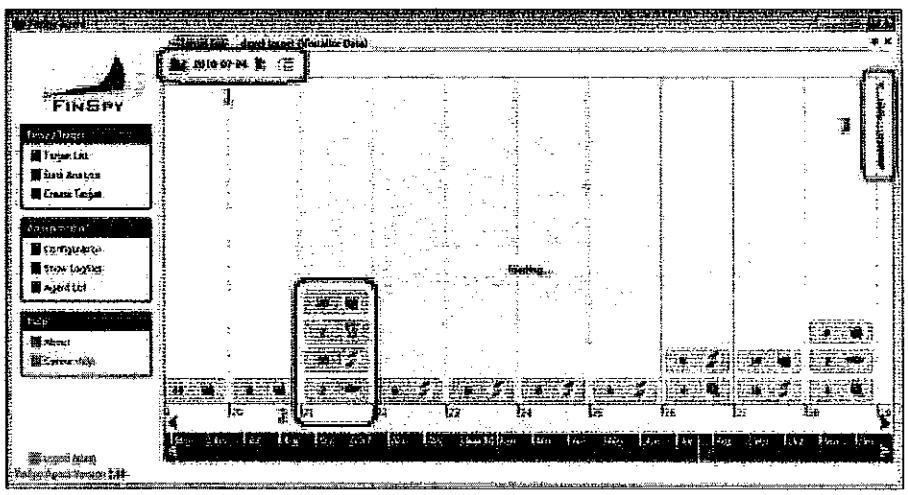


Live and Offline Target Configuration

Screen & Webcam Configuration Options



Full Intelligence on Target System



1. Multiple Data Views
2. Structured Data Analysis
3. Importance Levels for all recorded Files

FINSPY LICENSES

Outline

The FinSpy solution contains 3 types of product licenses:

A. Update License

The Update License controls whether **FinSpy** is able to retrieve new updates from the Gamma Update server. It is combined with the **FinFisher™ After Sales Support** module.After expiry, the **FinSpy** system will still be **fully functional** but no longer able to retrieve the newest versions and bug-fixes from the FinSpy Update server.

B. Agent License

The Agent License controls how many **FinSpy Agents** can login to the **FinSpy Master** in parallel.

Example:

- **5 Agent Licenses** are purchased.
- **FinSpy Agent** licenses can be installed on an unlimited number of systems, however
- Only 5 **FinSpy Agent** systems can login to the **FinSpy Master** and work with the **data at the same time**

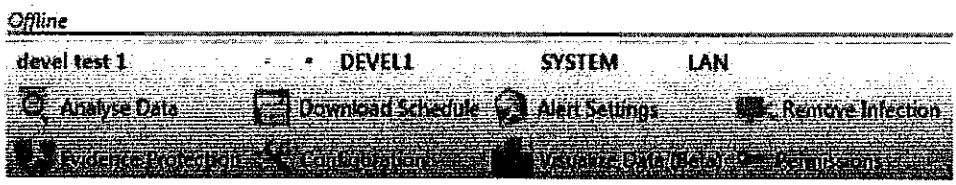
C. Target License

The Target License controls how many **FinSpy Targets** can be **active** in parallel.

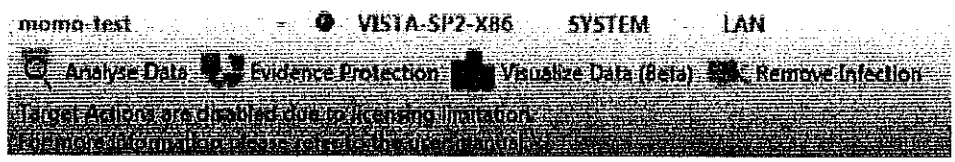
Active refers to **activated FinSpy Target** installations no matter whether the Target System is online or offline.

When **FinSpy Target** is deployed on a Target System and no Target Licenses are available, the **FinSpy Target** gets temporary deactivated and no recording and live access will be possible. As soon as a new License is available (e.g. by upgrading the existing License or de-infecting one of the active **FinSpy Targets**), the Target will be assigned the free license and it will be activated and begin recording and providing live access.

Screenshot active Target with License



Screenshot inactive Target without License



FINSPY MOBILE

FinSpy Mobile is closing the gap of interception capabilities for Governments for most common **smart phone platforms.**

Specifically, organizations **without network or off-air based interception** capabilities can access Mobile Phones and intercept the devices with enhanced capabilities. Furthermore, the solution offers **access to encrypted communications** as well as **data stored on the devices** that is not transmitted.

Traditional tactical or strategic Interception solutions **Face challenges** that can only be **solved using offensive systems** like FinSpy Mobile:

- Data not transmitted over any network and kept on the device
- Encrypted Communications in the Air-Interface, which avoid the usage of tactical active or passive Off-Air Systems
- End-to-end encryption from the device such as Messengers, Emails or PIN messages

FinSpy Mobile has been giving successful results to Government Agencies who gather information **remotely from Target Mobile Phones.**

When FinSpy Mobile is installed on a mobile phone it can be **remotely controlled and monitored** no matter where in the world the Target is located.

QUICK INFORMATION	
Usage:	· Strategic Operations · Tactical Operations
Capabilities:	· Remote Mobile Phone Monitoring
Content:	· Hardware/Software

Usage Example 1: Intelligence Agency

FinSpy Mobile was deployed on **BlackBerry mobile phones** of several Targets to monitor all communications, including **SMS/MMS, Email and BlackBerry Messenger.**

Usage Example 2: Organized Crime

FinSpy Mobile was **covertly deployed on the mobile phones** of several members of an Organized Crime Group (OCG). Using the **GPS tracking** data and **silent calls**, essential information could be gathered from **every meeting that was held** by this group.

Feature Overview

Target Phone – Example Features:

- **Covert Communications** with Headquarters
- Recording of **common communications** like Voice Calls, SMS/MMS and Emails
- **Live Surveillance** through silent Calls
- **File Download** (Contacts, Calendar, Pictures, Files)
- **Country Tracing** of Target (GPS and Cell ID)
- Full Recording of all **BlackBerry Messenger communications**
- Supports most common Operating Systems: **Windows Mobile, iOS (iPhone), BlackBerry and Android**

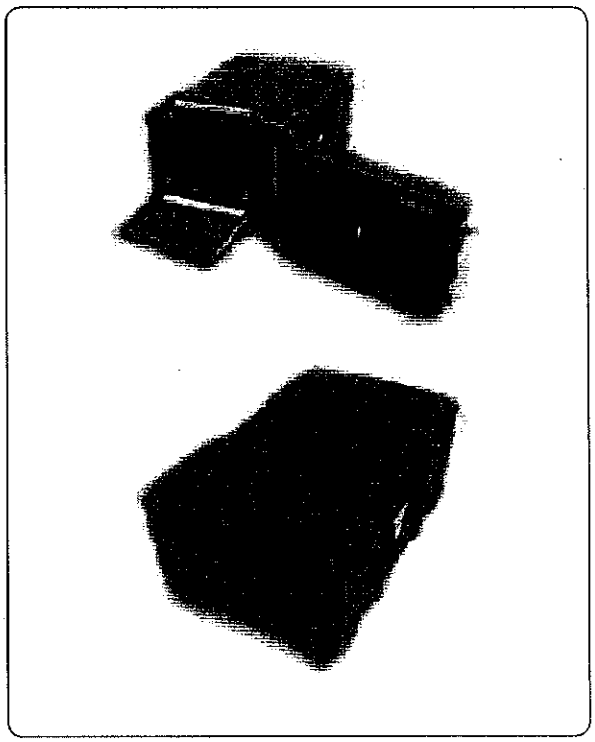
Headquarters – Example Features:

- Evidence Protection (Valid Evidence according to **European Standards**)
- **User-Management** according to Security Clearances
- Security Data Encryption and Communications using **RSA 2048 and AES 256**
- Hidden from Public through **Anonymizing Proxies**
- Can be **fully integrated** with Law Enforcement Monitoring Functionality

For a full feature list please refer to the Product Specifications.

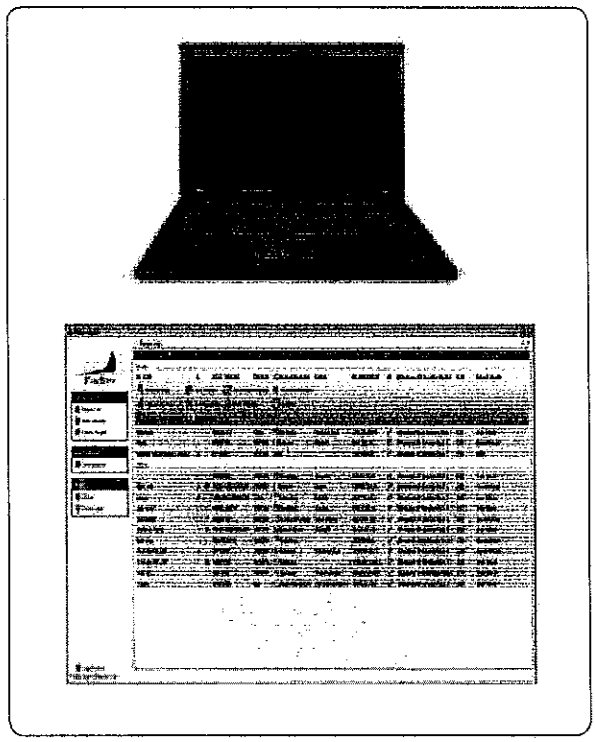
FINSPY MOBILE

Product Components



FinSpy Master and Proxy

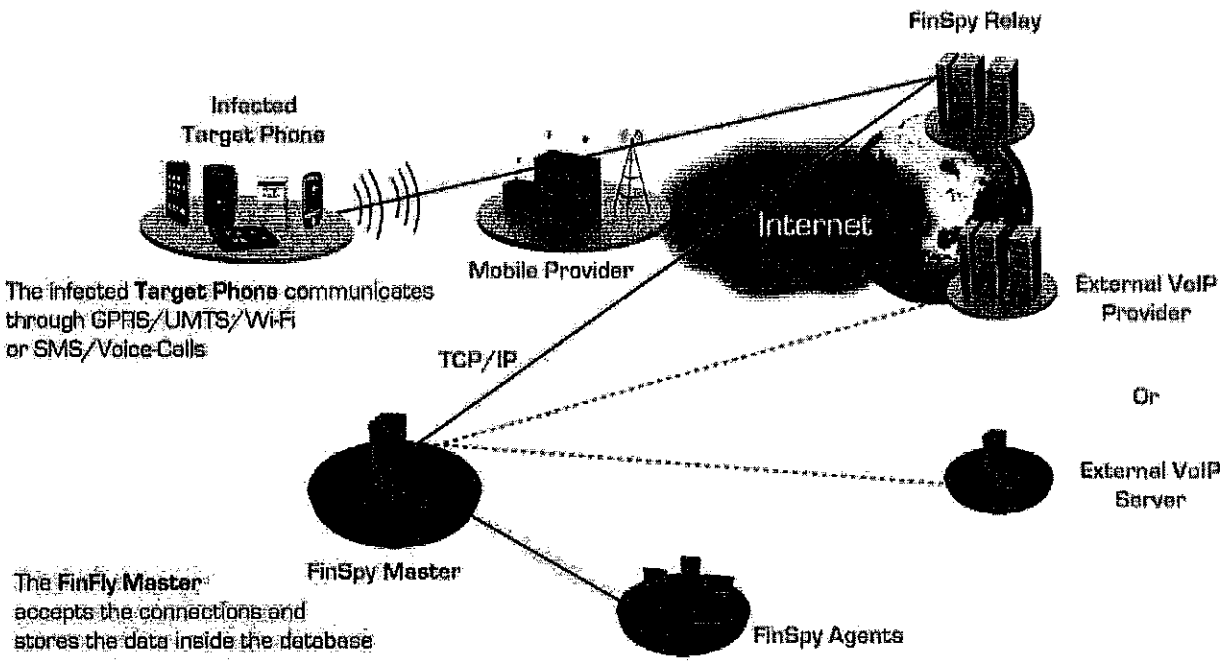
- Full Control of Target Systems
- Evidence Protection for Data and Activity Logs
- Secure Storage
- Security-Clearance based User- and Target Management



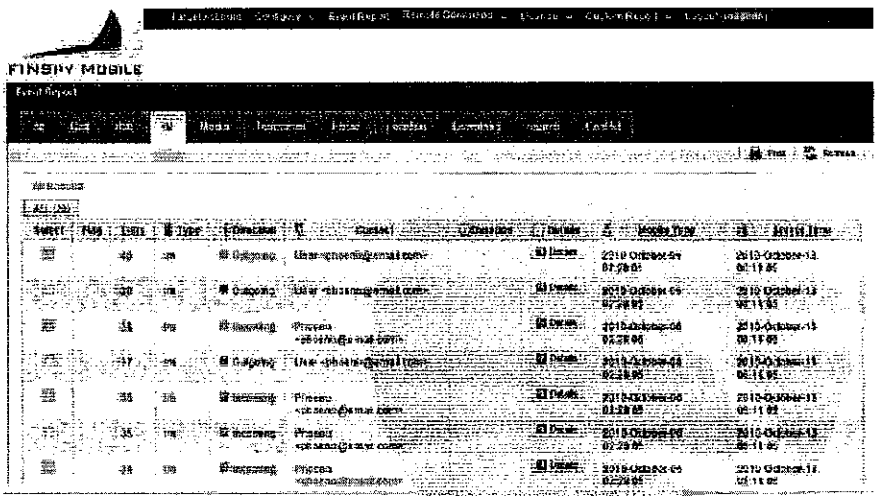
FinSpy Agent

- Graphical User Interface for Live Sessions, Configuration and Data Analysis of Targets

Access Target Mobile Phones around the World



Easy to Use User Interface



FINFLY USB

The FinFly USB provides an easy-to-use and reliable way of installing Remote Monitoring Solutions on computer systems when physical access is available.

Once the FinFly USB is inserted into a computer, it **automatically installs the configured software** with little or no user-interaction and **does not require IT-trained Agents** when being used in operations. The FinFly USB can be used against **multiple systems** before being returned to Headquarters.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target
Content:	· Hardware

Usage Example 1: Technical Surveillance Unit

The FinFly USB was successfully used by **Technical Surveillance Units** in several countries to deploy a Remote Monitoring Solution onto Target Systems that were switched off, by simply **booting the system from the FinFly USB device**.

Usage Example 2: Intelligence Agency

A Source in a domestic terror group was given a FinFly USB that **secretly installed a Remote Monitoring Solution** on several computers of the group when they were using the device to exchange documents between each other. The Target Systems could then be **remotely monitored from Headquarters,** and the FinFly USB was later returned by the Source.

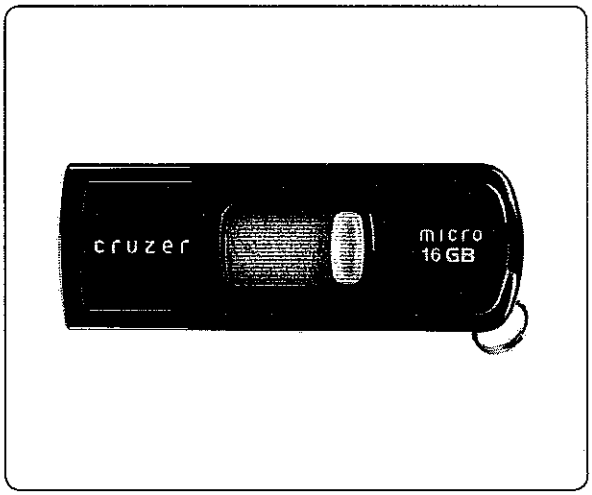
Feature Overview

- **Covertly installs Remote Monitoring Solution** on insertion in Target System
- **Little or no user-interaction** is required
- Functionality can be **concealed by placing regular files** like music, video and office documents on the device
- Infection of **switched off Target System** when **booting from USB**
- Hardware is a **common and non-suspicious USB device**

For a full feature list please refer to the Product Specifications.

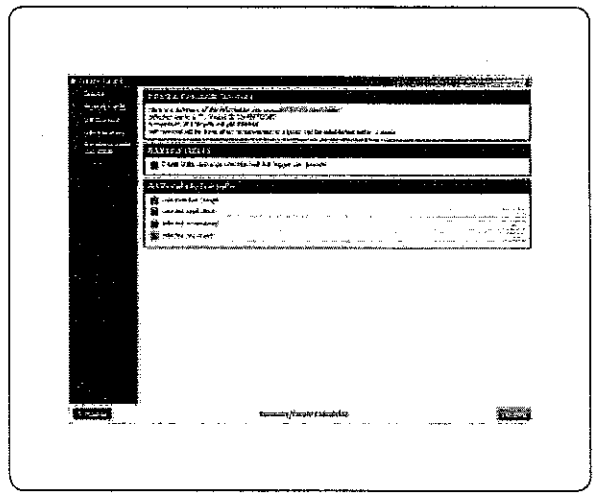
FINFLY USB

Product Components



FinFly USBs

- SanDisk USB Dongle (16GB)
- Deploys a Remote Monitoring Solution on Insertion into Target Systems
- Deploys Remote Monitoring Solution during Boot Process



Full FinSpy Integration

- Automatic generation and activation through FinSpy Agent

The information contained herein is confidential and subject to change without notice. Gamma Group International shall not be liable for technical or editorial errors or omissions contained herein.

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

FINFLY LAN

Some of the major challenges Law Enforcement agencies are facing are **mobile Targets**, where **no physical access** to a computer system can be achieved as well as Targets who **do not open any infected Files** that have been sent via email to their accounts.

In particular, security-aware Targets are **almost impossible to infect** as they keep their systems **up-to-date** and **no exploits** or Basic Intrusion techniques will lead to success.

FinFly LAN was developed to deploy a Remote Monitoring Solution covertly on Target Systems in Local Area Networks (Wired and Wireless/802.11). It is able to **infect Files that are downloaded** by the Target on-the-fly, infect the Target by **sending fake Software Updates** for popular Software or infect the Target by **injecting the Payload into visited Websites**.

QUICK INFORMATION	
Usage:	· Tactical Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System in Local Area Network
Content:	· Software

Usage Example 1: Technical Surveillance Unit

A Technical Surveillance Unit was following a Target for weeks without being able to physically access the target computer. They used FinFly LAN to install the Remote Monitoring Solution on the target computer when he was using a **public Hotspot** at a coffee shop.

Usage Example 2: Anti-Corruption

FinFly LAN was used to remotely install the Remote Monitoring Solution on the computer of a Target while he was using it **inside his hotel room**. The Agents were in another room **connected to the same network** and manipulated the Websites the Target was visiting to trigger the installation.

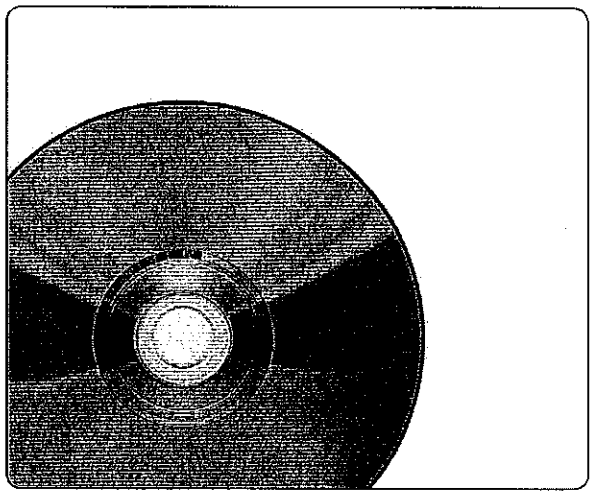
Feature Overview

- **Discovers all Computer Systems** connected to Local Area Network
- Works in **Wired and Wireless (802.11)** Networks
- Can be combined with FinIntrusion Kit for **covert Network Access**
- Hides Remote Monitoring Solution in **Downloads of Targets**
- Injects Remote Monitoring Solution as **Software Updates**
- Remotely installs Remote Monitoring Solution through **Websites visited by the Target**

For a full feature list please refer to the Product Specifications.

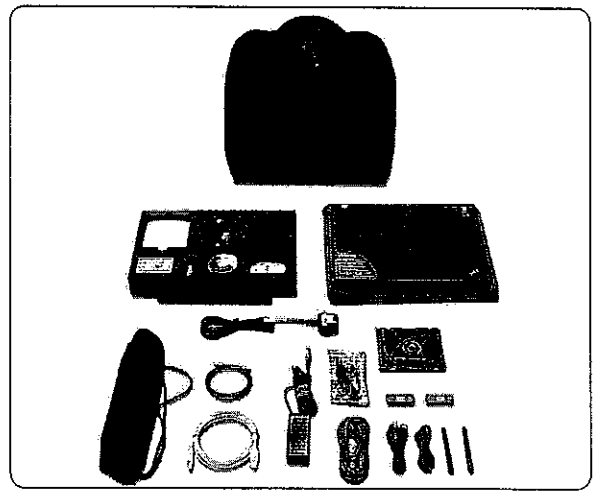
FINFLY LAN

Product Components



FinFly LAN

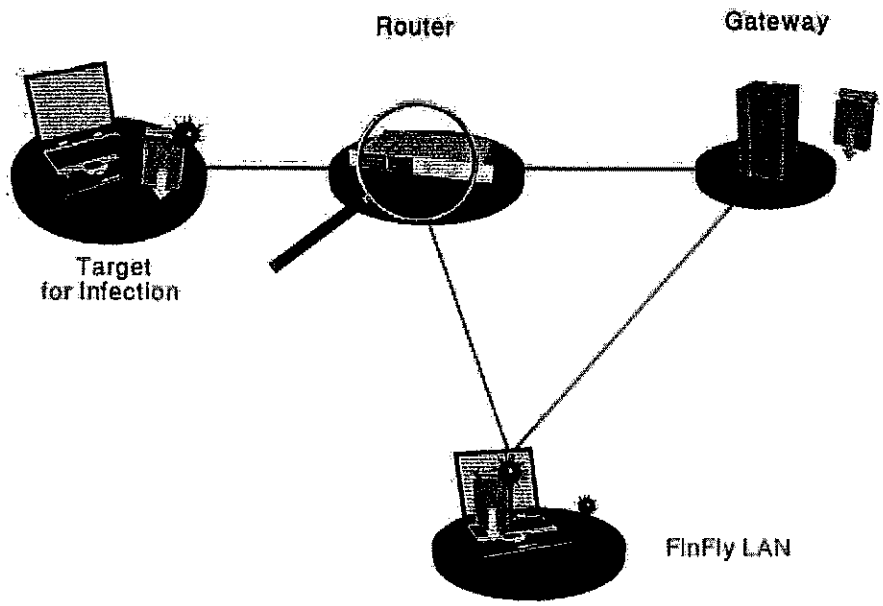
· Linux-based Software with simple User-Interface



FinIntrusion Kit - Integration (Optional)

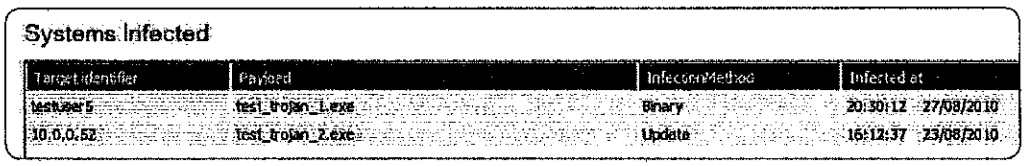
· FinFly LAN will be loaded as a module into the FinIntrusion Kit

Infection through Local Area Networks



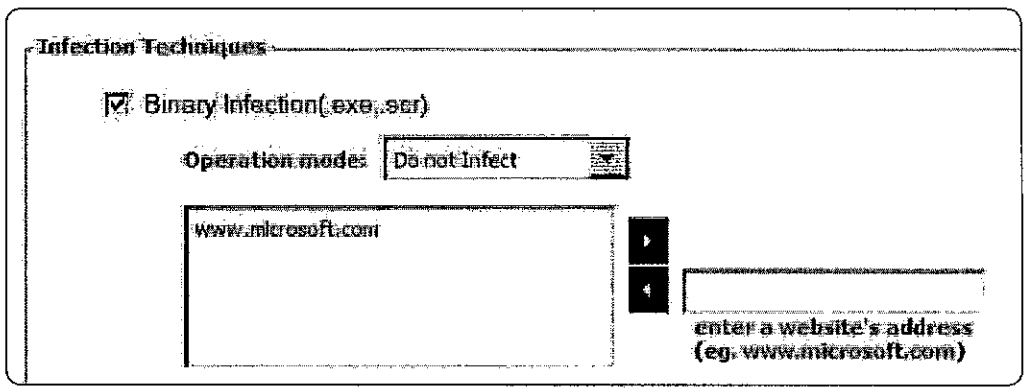
Automated User-Interface

· Simple to use without extensive training



Multiple-Target and Payload Support

· Different Executables can be added for each Target



FINFLY WEB

One of the major challenges in using a Remote Monitoring Solution is to install it onto the Target System, especially when only a little information, like an **Email-address**, is available and **no physical access** can be achieved.

FinFly Web is designed to provide **remote and covert** infection of a Target System by using a wide range of **web-based attacks**.

FinFly Web provides a **point-and-click interface**, enabling the Agent to easily **create a custom infection code** according to selected modules.

Target Systems visiting a prepared website with the implemented infection code will be **covertly infected** with the configured software.

QUICK INFORMATION	
Usage:	· **Strategic Operations**
Capabilities:	· **Deploys Remote Monitoring Solution on Target System through Websites**
Content:	· **Software**

Usage Example 1: Technical Surveillance Unit

After profiling a Target, the unit created a **website of interest** for the Target and sent him the **link through a discussion board**. Upon opening the Link to the unit's website, a Remote Monitoring Solution was installed on the Target System and the Target was **monitored from within Headquarters**.

Usage Example 2: Intelligence Agency

The customer deployed **FinFly ISP within the main Internet Service Provider** of their country. It was **combined with FinFly Web** to remotely **infect Targets that visited government offensive websites** by covertly injecting the FinFly Web code into the targeted websites.

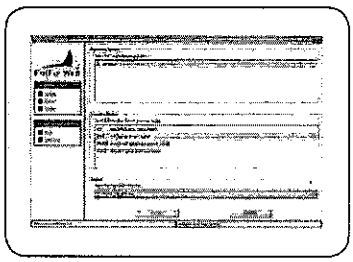
Feature Overview

- **Fully-Customizable** Web Modules
- Can be covertly **installed into every Website**
- Full integration with **FinFly LAN** and **FinFly ISP** to deploy even inside popular Websites like Webmail, Video Portals and more
- Installs Remote Monitoring Solution **even if only email address is known**
- Possibility to target every person visiting **configured Websites**

For a full feature list please refer to the Product Specifications.

FINFLY WEB

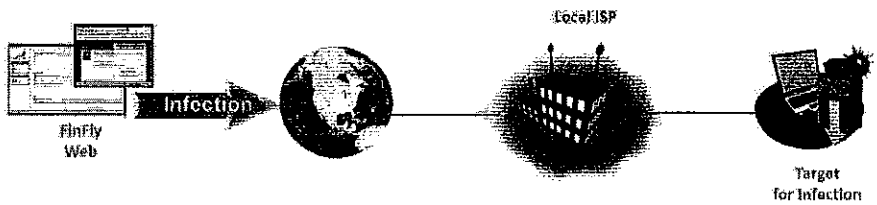
Product Components



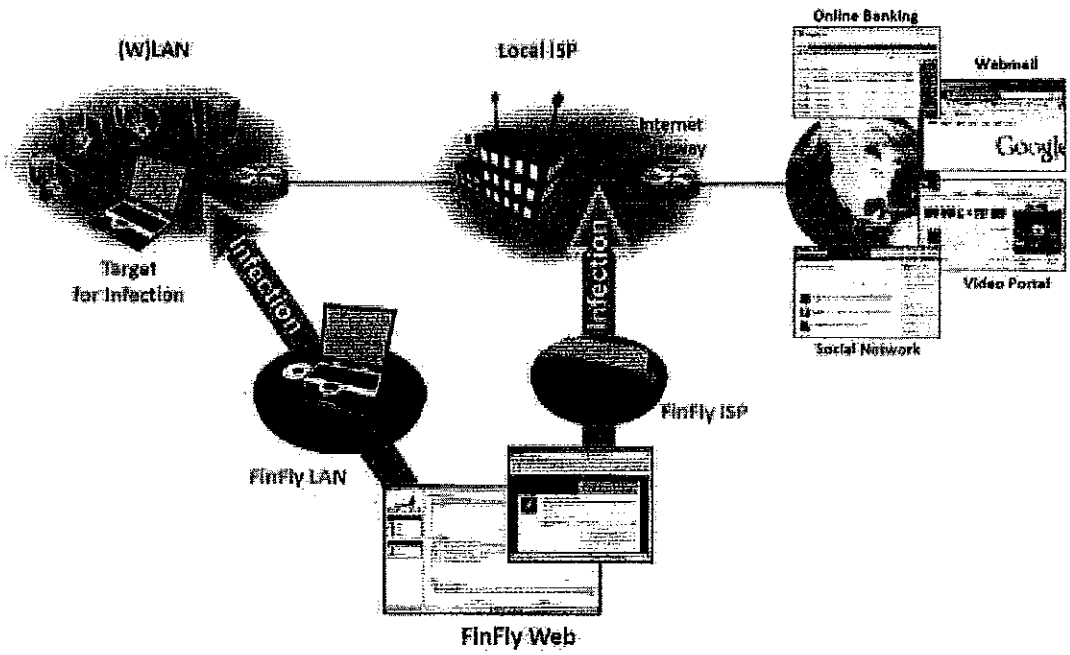
FinFly Web

- Point-and-click software to create custom infection Websites

FinFly Web direct infection

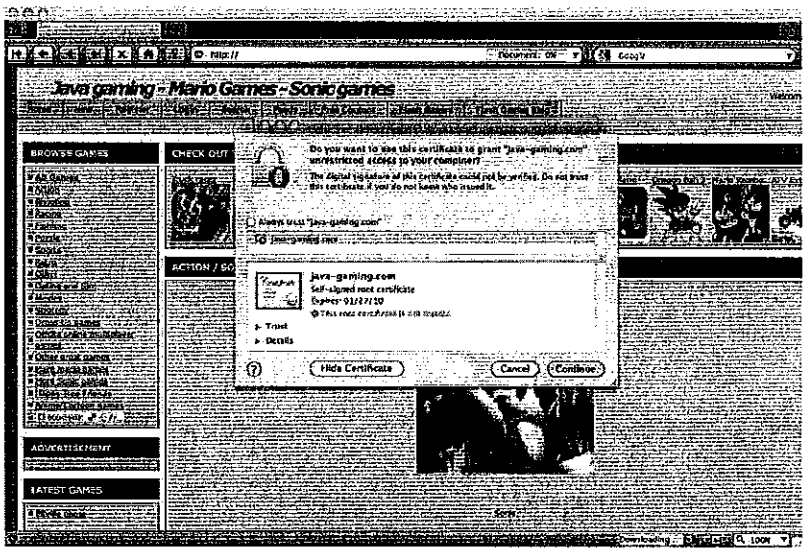


Full integration with FinFly LAN and FinFly ISP



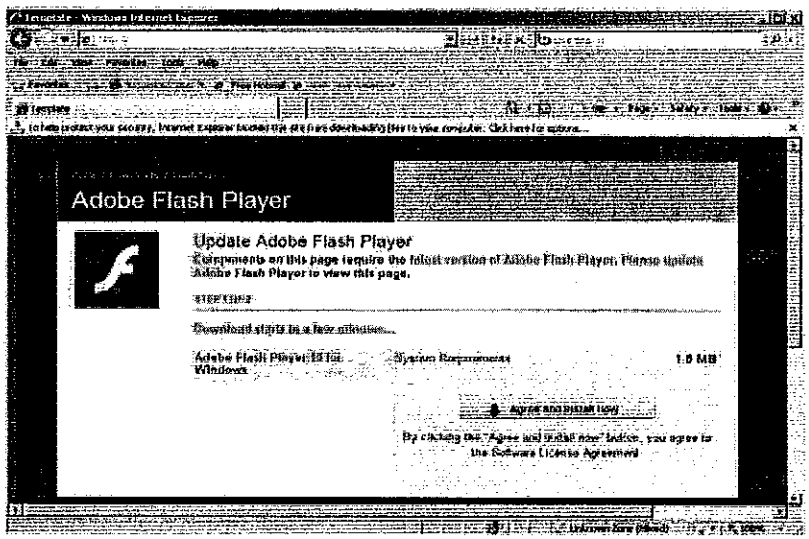
Example: Java Applet (Internet Explorer, Firefox, Opera, Safari)

The website will prompt the Target to accept a Java plug-in that can be signed with any company name (e.g. "Microsoft Corporation")



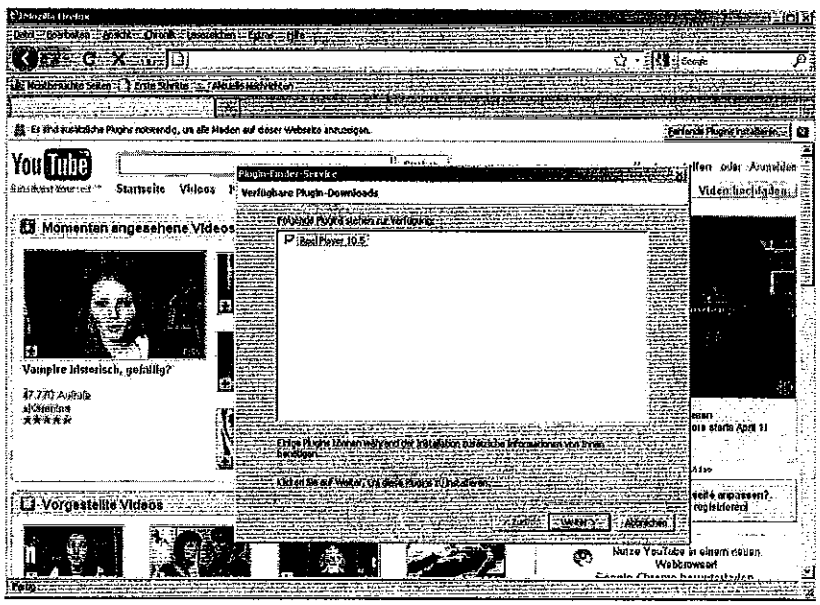
Example: Missing Component (IE, Firefox, Opera, Safari)

The website will pretend that a plug-in/codec etc. is missing on the Target System and prompt it to download and install this software



Example: Missing XPI (Firefox only, all platforms)

This module will prompt the Target to install additional plug-ins in order to be able to view the website.



The information contained herein is confidential and subject to change without notice. Gamma Group International shall not be liable for technical or editorial errors or omissions contained herein.

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

FINFLY ISP

In many real-life operations, physical access to in-country Target Systems cannot be achieved and covert **remote installation** of a Remote Monitoring Solution is required to be able to **monitor the Target from within the Headquarters.**

FinFly ISP is a strategic, **countrywide, as well as a tactical** (mobile) solution that can be **integrated into an ISP's Access and/or Core Network** to remotely install the Remote Monitoring Solution on selected Target Systems.

FinFly ISP appliances are based on **carrier grade server technology,** providing the maximum **reliability and scalability** to meet almost every challenge related to network topologies. A wide-range of Network Interfaces – all **secured with bypass functions** – are available for the required active network connectivity.

Several passive and active methods of Target Identification – from **online monitoring** via passive tapping to **interactive communications** between FinFly ISP and the AAA-Servers – ensure that the Targets are identified and their appropriate traffic is provided for the infection process.

FinFly ISP is able to **infect Files** that are downloaded by the Target **on-the-fly** or infect the Target by **sending fake Software Updates** for popular Software. The new release now integrates Gamma's powerful remote infection application **FinFly Web** to infect Targets on-the-fly by just **visiting any website.**

QUICK INFORMATION	
Usage:	· Strategic Operations
Capabilities:	· Deploys Remote Monitoring Solution on Target System through ISP Network
Content:	· Hardware/Software

Usage Example: Intelligence Agency

FinFly ISP was deployed in the main Internet Service Provider networks of the country and was actively used to remotely deploy a Remote Monitoring Solution on Target Systems. As the Targets have Dynamic-IP DSL Accounts, they are identified with their Radius Logon Name.

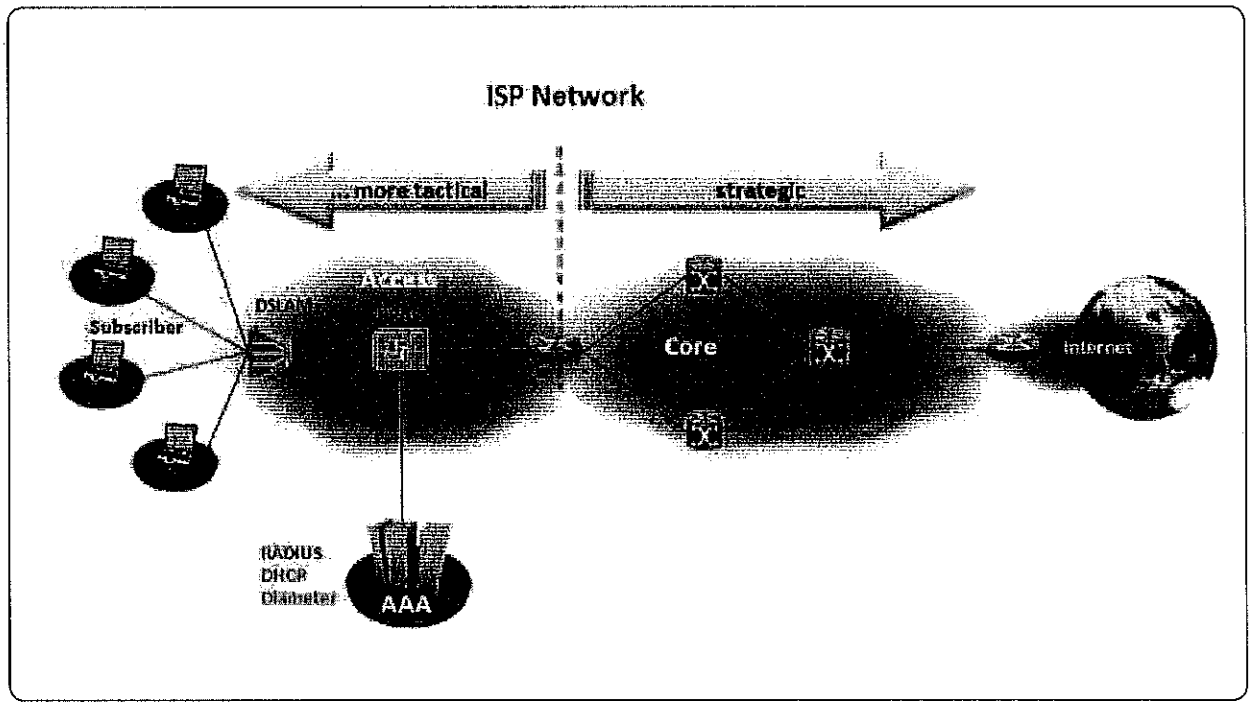
Feature Overview

- Can be installed inside the **Internet Service Provider Network**
- Handles **all common Protocols**
- Selected Targets by **IP address or Radius Logon Name**
- Hides Remote Monitoring Solution in **Downloads by Targets**
- Injects Remote Monitoring Solution as **Software Updates**
- Remotely installs Remote Monitoring Solution through **Websites visited by the Target**

For a full feature list please refer to the Product Specifications.

Different Location Possibilities

- FinFly ISP can be used as a tactical or strategic solution within ISP networks



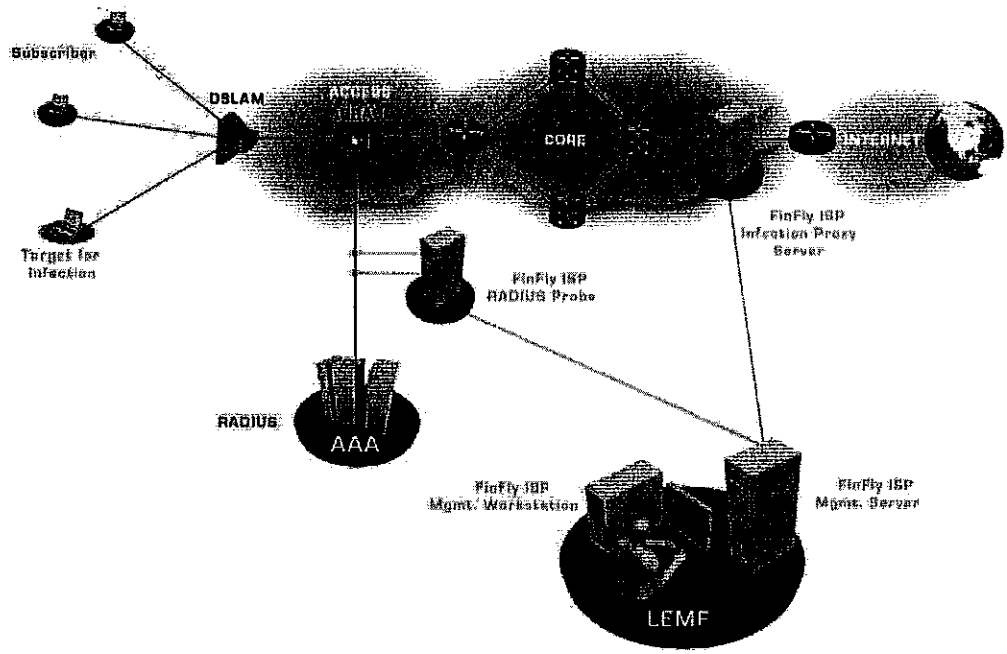
A tactical solution is mobile and the hardware is dedicated to the infection tasks inside the access network close to the targets' access points. It can be deployed on a short-term basis to meet tactical requirements focused on either a specific target or a small number of targets in an area.

A strategic solution would be a permanent ISP/countrywide installation of FinFly ISP to select and infect any target from the remote headquarters without the need for the LEA to be on location.

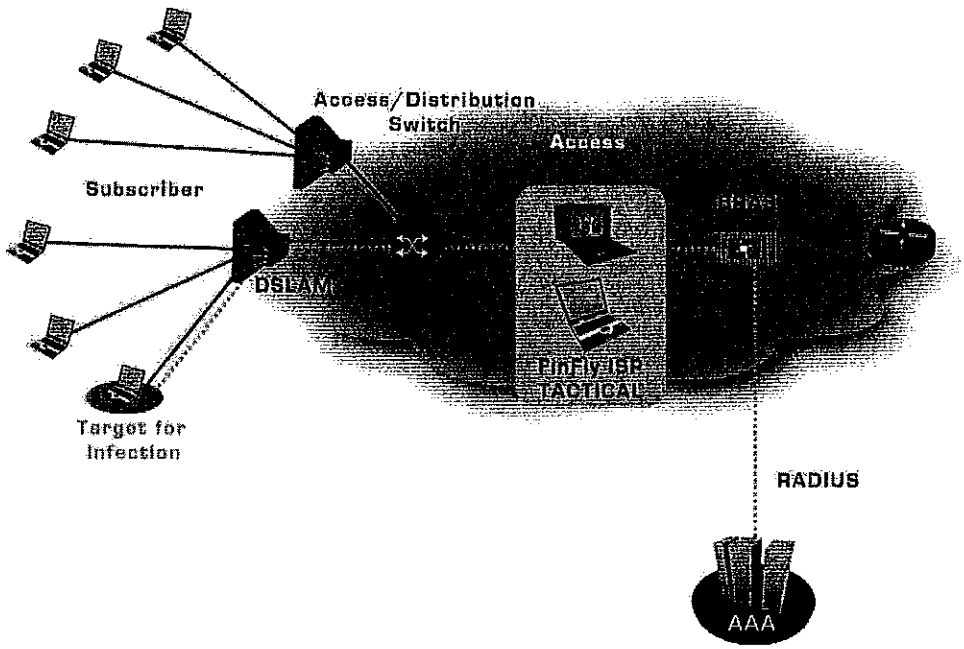
Of course, it is possible to combine tactical and strategic solutions to reach a maximum of flexibility for the infection operations.

Network Setup

Strategic Deployment



Tactical Deployment



FINFLY ISP

Product Components

FinFly ISP Strategic

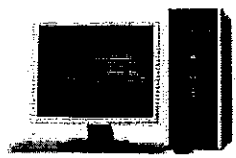
A strategic deployment of FinFly ISP consists at least of the following:

- Management System at the LEMF
- Target Identification Probe Server(s) at the AAA-System of the network
- Infection Proxy Server(s) at, for example, the Internet Gateway(s)

FinFly ISP Servers
Workstation
HP ProLiant DL-Series G7
Business WS



FinFly ISP
HP Z-Series



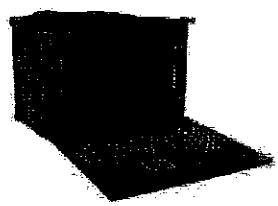
Throughput:	> 20 Gbps
Max. no. of NICs:	2 - 8 NICs
Interfaces:	1GE Copper / Fiber 10GE Copper / Fiber SONET / SDH OC-3 / -192 STM-1 / -64 ATM AAL5
Processors:	1x – 8x Intel XEON
Core:	2 - 8 Cores / Processor
RAM:	12GB -1TB
HDD Capacity:	3 x 146GB - 4.8TB SAS
Features:	HP iLO 3 Redundant Power Redundant Fans Bypass Switch Function (if applicable)
Operating System:	Linux GNU (Debian 5.0) hardened

FinFly ISP Tactical

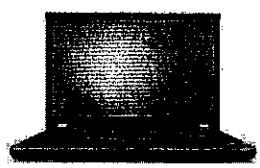
A tactical FinFly ISP System consists of the following:

- Target Identification & Infection Proxy Server Portable
- Management System Notebook

FinFly ISP Tactical
Portable Mgmt.
Atlas A9 17" Portable



FinFly ISP Tactical
Lenovo Thinkpad
T-Series



Throughput:	5 Gbps
Max. no. of NICs:	3 NICs
Interfaces:	1GE Copper / Fiber SONET / SDH OC-3 / -12 STM-1 / -4 ATM AAL5
Processors:	2 x Intel Core i7
Core:	6 Cores / Processor
RAM:	12GB
HDD Capacity:	2 x 1TB SATA
Optical Drive:	DVD+/-RW SATA
Monitor:	1 x 17" TFT
Features:	Bypass Switch Function for NICs
Operating System:	Linux GNU (Debian 5.0) hardened

The technical data /specifications are subject to change without notice.

The information contained herein is confidential and subject to change without notice. Gamma Group International shall not be liable for technical or editorial errors or omissions contained herein.

GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

FinSupport

The FinSupport sustains upgrades and updates of the FinFisher™ product line in combination with an annual support contract.

The FinFisher™ Support Webpage and Support Team provide the following services to our clients:

- Online access to:
  - Latest User Manual
  - Latest Product Specifications
  - Latest Product Training Slides
  - Bug Reporting Frontend
  - Feature Request Frontend
- Regular Software Updates:
  - Bugfixes
  - New Features
  - New Major Versions
- Technical Support via Skype:
  - Bugfixing
  - Partial Operational Support

FinLifelineSupport

The FinLifelineSupport provides professional back-office support for trouble resolution and technical queries. It also provides back-office support remotely, for FinFisher™ SW bug fixes and Hardware replacements under warranty. Furthermore, with FinLifelineSupport the client automatically receives new features and functionalities with the standard release of bug fixes.

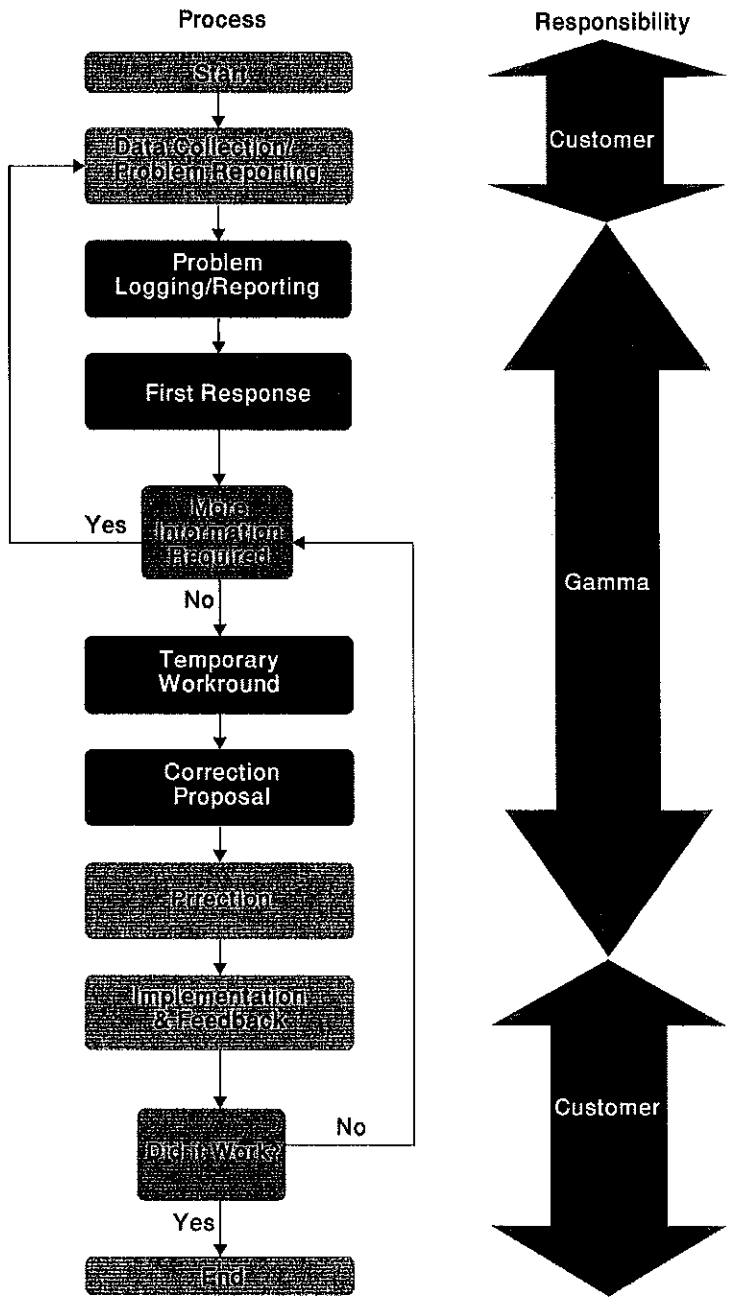
Bug Fixes

FinSupport is a product driven support organization whereby a highly skilled after-sales support manager receives related queries by email or telephone. The after sales support manager is based in Germany and his hours of operation are 09:00 – 17:00 Central European Time (CET).
With the FinLifelineSupport, support is available from 09:00–17:00 CET. If a request for support is logged outside of standard office hours it will be addressed immediately on the next working day.

When the customer reports an incident, we log an Incident Report (IR) and document the priority of the incident. Within a specified period, corrective actions will follow based on the assigned priority. The FinFisher™ team then has the responsibility of coordinating the investigation and resolution of the IR, as well as communicating the status and new information to the IR originator.

For high priority issues, we ensure that the system continues to work smoothly by quickly delivering workaround solutions and tested bug fixes. When the FinFisher™ team delivers a workaround, in parallel it also escalates the Problem Report (PR) to the Research and Development (R&D) department to ensure a quick resolution. These professional support measures ensure that the software meets the highest expectations.

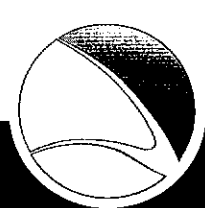
The following flow chart provides an illustration of the typical operational procedure and areas of responsibility (**Note**: in this flow chart, 'customer' represents the originator of the IR):



The following table provides the normal customer incident handling procedure:

Customer	Incident Report (IR) Processing and Tasks
	FinFisher™ has dedicated email, phone/fax hotline contact info for incident reporting.
In cases of a (suspected) hardware/software defect, receive Incident Report (IR) as per the defined communication methods. IR should include: - contract id - customer's name - affected system/ technology - description of defect - priority (see definition below) - available error symptoms	
Customer cooperates by providing further error symptoms, upon request	Within one working day, customer receives the ticket number to confirm receipt and tracks the IR, and also the initial analysis results
	FinLifelineSupport supports collecting error symptoms, upon request
	FinLifelineSupport helps with temporary workaround solution
	FinLifelineSupport provides correction proposal on IR with planned corrective measures & response time, after incident analysis
	FinLifelineSupport provides issue of hard- or software modification, if reported incident requires correction
Customer implements delivered hardware/ software modification. Customer confirms successful correction.	FinLifelineSupport helps with implementing hardware(i)/ software modification

(i) Hardware charged separately if not under warranty.



Definitions of query and fault priority

FinLifelineSupport processes the incoming queries and problem reports according to their urgency. Two factors rate the urgency of an incident, and both are included in each IR:

- 'Priority' based solely on the technical scope of the error
- 'Customer Severity' is a more objective factor and based on the resultant customer impact

The following 'Priority' table provides an overview of the corresponding technical scope:

Priority	Definition	Example
1	critical issue: crucial aspect of system not working	The Proxy is down and no communication to the FinSpy Target can be established.
2	major issue with no workaround	An Antivirus update detects an already installed RMS which requires an immediate update in order to stay operational within the infected system.
3	major issue with workaround	FinSpy Target functionality doesn't operate properly but can be fixed with a workaround solution.
4	minor issue with little impact on system	Wrong icon shown for a downloaded file

Response Times

In 90 percent of all incidents, we will keep our response times as depicted in the table below.

'Working day(s)' = as defined in the German calendar, and thus, excludes holidays observed in Germany.

There are three phases in our response times:

- Initial Response
- Corrective Action Feedback
- Problem Resolution (or Priority De-Escalation)

The time for the 'Initial Response' is from the moment we log an incident to the actual confirmation response sent to the customer acknowledging receipt of the incident.

The 'Initial Response' may also ask for more detailed information or, in less complex cases, may immediately solve the problem.

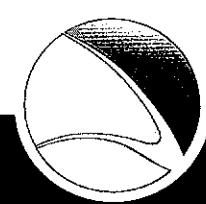
[redacted]

Response Times	Initial Response	Corrective Action Feedback	PROBLEM Resolution/ PRIORITY De-Escalation
Prio 1 - critical issue	Same working day	1 working day(s)	2 working day(s) Please note: Depending on the problem and research required it may take longer to resolve the issue.
Prio 2 - major issue without workaround	Same working day	2 working day(s)	5 working day(s) Please note: Depending on the problem and research required it may take longer to resolve the issue.
Prio 3 - major issue with workaround	Same working day	3 working day(s)	14 working day(s) Please note: Depending on the problem and research required it may take longer to resolve the issue.
Prio 4 - minor issue	Same working day	7 working day(s)	next software update

Software Upgrades

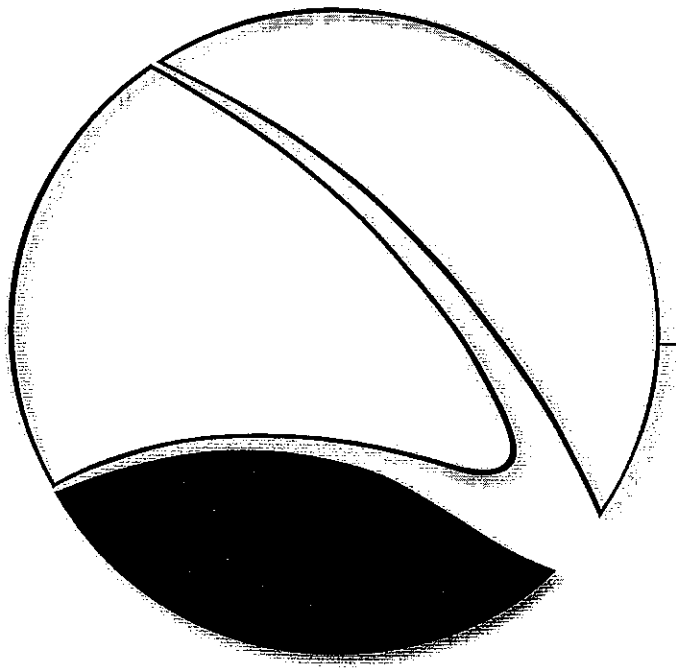
The FinLifelineSupport includes regular Software upgrades and guarantees automatic upgrades to the existing system with Software patches provided via the update system.

These upgrades include new features, new enhancements and new functionality as per the client's roadmap (excluding hardware).



IT Intrusion Training Program

FINTRAINING



The IT Intrusion Training Program includes courses on both, products supplied as well as practical IT Intrusion methods and techniques. This program transfers years of knowledge and experience to end-users, thus maximizing their capabilities in this field.

IT Intrusion Training Program

FINTRAINING

Security awareness is **essential for any government** to maintain IT security and successfully **prevent threats** against IT infrastructure, which may result in a loss of confidentiality, data integrity and availability.

On the other hand, topics like **CyberWar**, Active Interception and Intelligence-Gathering through **IT Intrusion** have become more important on a daily basis and require Governments to **build IT Intrusion teams** to **face these new challenges**.

FinTraining courses are given by **world-class IT Intrusion experts** and are held in **fully practical scenarios** that focus on **real-life operations** as required by the end-user in order to solve their **daily challenges**.

Gamma combines the individual training courses into a **professional training and consulting program** that builds up or enhances the capabilities of an IT Intrusion team. The Training courses are **fully customized** according to the end-user's operational challenges and requirements. In order to ensure full usability of the transferred know-how, **operational in-country support** is provided during the program.

QUICK INFORMATION	
Usage:	· Knowledge Transfer
Capabilities:	· IT Intrusion Know-How · CyberWar Capabilities
Content:	· Training

Sample Course Subjects

- **Profiling** of Target Websites and Persons
- Tracing **anonymous Emails**
- **Remote access** to Webmail Accounts
- **Security Assessment** of Web-Servers & Web-Services
- Practical **Software Exploitation**
- **Wireless IT Intrusion** (WLAN/802.11 and Bluetooth)
- Attacks on **critical Infrastructures**
- Sniffing **Data and User Credentials** of Networks
- **Monitoring Hot-Spots**, Internet Cafés and Hotel Networks
- **Intercepting and Recording Calls** (VoIP and DECT)
- **Cracking Password** Hashes

Consultancy Program

- Full IT Intrusion **Training and Consulting** Program
- Structured build-up and **Training of IT Intrusion Team**
- Full **Assessment of Team** Members
- Practical Training Sessions focus on **Real-Life Operations**
- In-Country **Operational Consulting**

For a full feature list please refer to the Product Specifications.



GAMMAGROUP

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

WWW.GAMMAGROUP.COM



جمهورية مصر العربية

جهاز مباحث أمن الدولة

وزارة الداخلية

ملف خاص بمنتجات

برنامج

FINFISHER

(فينفيشيروا)

الموضوع

عدد الملفات المفتوحة

تاريخ فتح الملف

«انتهاء»

ملاحظة : ممنوع سحب أو إضافة أوراق للملف إلا بمعرفة الموظف المختص.

بسم الله الرحمن الرحيم

مباحث أمن الدولة

الإدارة المركزية لتكنولوجيا المعلومات [سري للغاية]

(مذكرة)

- تقدمت مؤخراً للجهاز شركة أنظمة الاتصالات الحديثة MCS وكيلة عن شركة GAMMA الألمانية العالمية .. المتخصصة في صناعة البرمجيات والأنظمة الإلكترونية الأمنية التي تستهدف اختراق صناديق البريد الإلكتروني .. بعرض لأحد أبرز منتجاتها (برنامج FINFISHER . يتم استخدامه من قبل العديد من الأجهزة الأمنية والإستخبارات العالمية)،وقامت بإمداد الجهاز بنسخة تجريبية " مجانية " منه (عبارة عن جهاز كمبيوتر محمول مثبت عليه البرنامج المشار إليه) لتجربته للوقوف علي إمكانياته الفنية وقدراته في مجال الاختراق الإلكتروني .. حيثُ أسفرت محصلة تجربة نظام الاختراق المشار إليه علي مدار خمسة شهور تقريباً .. عما يلي :-

- كونه نظام إختراق أمني رفيع المستوي يحقق العديد من الإمكانيات الفنية في هذا المجال غير متاحه في مثيلها من أنظمة الاختراق والتي يتمثل أبرزها في (إختراق صناديق البريد الالكتروني علي شبكات " hotmail . yahoo . Gmail " ، إمكانية تحديث ملفات التجسس علي أجهزة العناصر المستهدفة واستخدام أجهزتهم والبصمات الالكترونية الخاصة بهم في التواصل ، التحكم الكامل في أجهزة العناصر المخترقه ، ...) .. فضلاً عن نجاحه في اختراق عناوين الحسابات الشخصية علي شبكة الـ SKYPE

والذي يُعد نظام التواصل الإلكتروني الأكثر أماناً بالنسبة لعناصر النشاط الضار علي شبكة الإنترنت لكونه مشفر ٠

- يُعد اختراق العنصر المستهدف بالنظام المشار إليه بمثابة زرع نظام تجسس كامل بمكان تواجد جهاز الكمبيوتر المخترق .. نظراً لإمكانياته الهائلة والتي تتيح ما يلي :٠

- تسجيل محادثاته الصوتية والمرئية علي شبكة الإنترنت ٠
- تسجيل محادثاته وتحركاته ومحيطيه (صوت وصورة) بالغرفة مكان استخدامه لجهاز الكمبيوتر المخترق (في حالة احتواء جهاز الكمبيوتر المخترق علي كاميرا ومايكروفون كمعظم أجهزة اللاب توب) ٠
- التحكم الكامل بجهاز الكمبيوتر المخترق وإمكانية نسخ جميع محتوياته .. إمكانية اختراق أجهزة الحاسب الآلي المتصلة بشبكة محلية بأكملها .. دون الحاجة إلي استهداف كل جهاز علي حده بعمليات الاختراق الإلكتروني ٠

- تقدمت الشركة المُشار إليها بعرض أسعار يشمل تكلفة نظام الاختراق المُشار إليه كذا تكلفة تدريب عدد ٤ ضباط من العاملين في مجال الاختراق الإلكتروني ، وتقديم الدعم الفني من الشركة لمدة ثلاث أعوام .. إذ بلغ إجمالي السعر ٣٨٨,٦٠٤ ألف يورو ٠

- الرأى

عـــــــــــــرض ــ برجـــــاء النظر ،،،

١ يناير ٢٠١١

بسم الله الرحمن الرحيم

٣٤٨
٣٠٢

الإدارة المركزية لتكنولوجيا المعلومات
مجموعة المتابعة الالكترونية
قسم الاختراق الالكتروني

(سرى للغاية)

السيد اللواء / وكيل الإدارة العامة لأمانة الجهاز للشئون المالية

تحية طيبة ... وبعد ،،

- بالنسبة لكتاب سيادتكم المؤرخ في ٢٠١٠/١٢/٢٢ " مرفق " والخاص بموافاة الإدارة رئاستكم بالمواصفات الفنية لنظام اختراق صناديق البريد الالكتروني المقدم من شركة أنظمة الاتصالات الحديثة وكيلة شركة **GAMMA** الألمانية العالمية المتخصصة في صناعة البرمجيات .. وكذا أسماء الشركات التي يمكن الطرح عليها لمخاطبة القطاع المالي بالوزارة لتخصيص المبلغ المطلوب والبدء في الإجراءات اللازمة ... **نفيد** :-

☒ مرفق المواصفات الفنية للنظام المطلوب مداركته والشركات التي يمكن الطرح عليها .

وتفضلوا بقبول فائق الاحترام ،،،

لواء /

" صلاح فؤاد "

مدير الإدارة المركزية لتكنولوجيا المعلومات

٢٠١٠ / ١٢ / ٢٣

بسم الله الرحمن الرحيم

الإدارة العامة لأمانة الجهاز
مجموعة الشئون المالية
قسم الميزانية

١٤٢٦
٢٠١٠/١٢/٢٢

(سري للغاية)

السيد اللواء / مدير الإدارة المركزية لتكنولوجيا المعلومات

تحية طيبة .. وبعد .

- بالنسبة لمذكره العرض على السيد اللواء دكتور / مساعد أول وزير الداخلية - رئيس الجهاز بشأن طلب مداركة نظام إختراق صناديق البريد الألكتروني (برنامج FINFISHER) بإجمالي مبلغ ٣٨٨٦٠٤ يورو (ثلاثة مائة وثمانية وثمانون ألف وستمائة وأربعة يورو) والمقدم من شركة أنظمة الأتصالات الحديثة MCS وكيلة شركة GAMMA الألمانية العالمية والمتخصصة في صناعة البرمجيات والأنظمة الإلكترونية الأمنية ... وتفضل السيد اللواء دكتور / مساعد أول وزير الداخلية - رئيس الجهاز بالموافقة على مداركة النظام.
- برجاء التكرم بموافاتنا بالمواصفات الفنية للنظام المطلوب مداركته وأسماء الشركات التي يمكن الطرح عليها وذلك حتى يمكن مخاطبة القطاع المالي بالوزارة للتخصيص المبلغ المطلوب والبدء في الإجراءات المالية اللازمة .

وتفضلوا بقبول فائق الاحترام ،،

لواء /

وكيل الإدارة العامة لأمانة الجهاز
للشئون الماليه

٢٠١٠/١٢/٢٢

اختان

أولاً : المواصفات الفنية لبرنامج متابعة الأنظمة الإلكترونية

ـ برنامج لمتابعة الأنظمة الإلكترونية على شبكات المعلومات بأنواعها المختلفة (داخلية ، محلية) تمكن مستخدميها من متابعة البروتوكولات التالية:

- بروتوكول نقل النص الفائق HTTP والخاص بإرسال و استقبال البيانات العاملة بأنظمة HTML باستخدام المنفذ رقم ٨٠.
- بروتوكول نقل الملفات FTP والخاص بارسال و استقبال الملفات الالكترونية بجميع أنواعها باستخدام المنفذ رقم ٢٠، ٢١ .
- بروتوكول ارسال البريد البسيط SMTP والخاص بالمعيار الأساسي لإرسال و استقبال المراسلات البريدية على شبكات المعلومات بكافة أنواعها باستخدام المنفذ رقم ٢٥.
- بروتوكول مكتب البريد POP3 والخاص بنقل المراسلات البريدية من خوادم مراسلات البريد باستخدام المنفذ رقم ١١٠ .
- بروتوكول الوصول للرسائل البريدية IMAP و الخاص بنقل المراسلات البريدية باستخدام المنفذ رقم ١٤٣ .
- بروتوكول الوصول للرسائل البريدية WEBMAIL العالمية باستخدام المنفذ رقم ٨٠ .
- تحديد الحسابات والمعرفات (عربي – انجليزي) المستخدمة أثناء الولوج على المواقع المختلفة العاملة بنظام " VB ، IPB ، HTML " سواء لإدارتها أو للدخول عليها .
- إدارة الحواسيب عن بعد وكذا نسخ أو تعديل الملفات المتواجدة على أنظمة الحواسيب العاملة بأنظمة التشغيل المختلفة التي تنتجها شركة مايكروسوفت العالمية.

ثانياً : الشركات التي يمكن الطرح عليها

- الشركة المصرية لإدارة وخدمات الوثائق الهندسية " EDM ".
- شركة أنظمة الاتصالات الحديثة " MCS " .
- شركة تي كومبيوتر.
- شركة تليكوم انتربريز .

بسم الله الرحمن الرحيم

(٢٣٦)
م.م

الإدارة العامة للمعلومات

الإدارة المركزية لتكنولوجيا المعلومات [سري للغاية]

مجموعة المتابعة الإلكترونية

قسم الاختراق الالكتروني

مذكـــــرة

للعرض على السيد اللواء دكتور / مساعد أول الوزير رئيس الجهاز

حول: شركة GAMMA الألمانية العالمية المتخصصة في صناعة البرمجيات والأنظمة الإلكترونية الأمنية .

- **إلحاقاً لما سبق عرضه بشأن تقدم شركة أنظمة الاتصالات الحديثة MCS وكيلة عن شركة GAMMA الألمانية العالمية .. المتخصصة في صناعة البرمجيات والأنظمة الإلكترونية الأمنية التي تستهدف اختراق صناديق البريد الإلكتروني (من أبرز منتجاتها برنامج FINFISHER – يتم استخدامه من قبل العديد من الأجهزة الأمنية والإستخباراتية العالمية)، وإضطلاع الشركة بإبداء استعدادها لإمداد الجهاز بنسخة تجريبية " مجانية " من منتجها المشار إليه(عبارة عن جهاز كمبيوتر محمول مثبت عليه البرنامج المشار اليه) للتجربة للوقوف علي إمكانياته الفنية وقدراته في مجال الاختراق الإلكتروني .. وموافقة رئاسة الجهاز علي إبرام عقد مع الشركة الأجنبية تتبلور أبرز بنوده في (تعهد الجهاز بعدم تسريب نسخة من البرنامج لأي جهة أخري خلال تلك الفترة ، كذا التزام الشركة بعدم التصريح لأي جهه أجنبية أو محلية باستخدام الجهاز للبرنامج المشار إليه) .. فقد أسفرت محصلة تجربة نظام الاختراق المشار إليه علي مدار خمسة شهور تقريباً .. عما يلي : –**
  - **كونه نظام إختراق أمني رفيع المستوي** يحقق العديد من الإمكانيات الفنية في هذا المجال غير متاحه في مثيلها من أنظمة الاختراق والتي يتمثل أبرزها في (إختراق صناديق البريد الالكتروني علي شبكات " Gmail – yahoo – hotmail " ، إمكانية تحديث ملفات التجسس علي أجهزة العناصر المستهدفه وإستخدام أجهزتهم والبصمات الالكترونية الخاصة بهم في التواصل ، التحكم الكامل في أجهزة العناصر المخترقه ، ...) .. فضلاً عن نجاحه في اختراق علي أوبن الحسابات الشخصية علي شبكة الـ SKYPE والذي يعُد لنظام التواصل الإلكتروني الأكثر أماناً بالنسبة لعناصر النشاط الضار علي شبكة الإنترنت لكونه مشفر .
  - **يعد إختراق العنصر المستهدف بالنظام المشار إليه** بمثابة زرع نظام تجسس كامل بمكان تواجد جهاز الكمبيوتر المخترق .. نظراً لإمكانياته الهائلة التي تتيح ما يلي : –
    - تسجيل محادثاته الصوتية والمرئية علي شبكة الإنترنت .
    - تسجيل محادثاته وتحركاته ومحيطه (صوت وصورة) بالغرفة مكان استخدامه لجهاز الكمبيوتر المخترق (في حالة إحتواء جهاز الكمبيوتر المخترق علي كاميرا ومايكروفون كمعظم أجهزة اللاب توب) .
    - التحكم الكامل بجهاز الكمبيوتر المخترق وإمكانية نسخ جميع محتوياته .

- **كما يُتيح نظام الإختراق محل العرض** .. إمكانية إختراق أجهزة الحاسب الآلي المتصلة بشبكة محلية بأكملها .. دون الحاجة إلي إستهداف كل جهاز علي حدا بعمليات الإختراق الإلكتروني .

- **أسفرت تجربة المنتج المشار إليه** ، احتوائه علي بعض السلبيات الفنية ، حيث أمكن مؤخراً بالتنسيق مع الشركة الملتجة .. إجراء بعض التعديلات الجوهرية بالنظام المشار إليه لتجنب تلك السلبيات .

- تقدمت الشركة GAMMA الألمانية مؤخراً بعرض أسعار يشمل تكلفة نظام الإختراق المشار إليه كذا تكلفة تدريب عدد ٤ ضباط من العاملين في مجال الإختراق الإلكتروني ، وتقديم الدعم الفني من الشركة لمدة ثلاث أعوام .. إذ بلغ إجمالي السعر ٣٨٨,٦٠٤ ألف يورو (مرفق عرض الأسعار تفصيلياً) .

- **في ضوء ما سبق** .. يري الموافقة علي الإحالة للإدارة المركزية للشئون المالية لاتخاذ اللازم نحو التنسيق مع قطاع الشئون المالية بالوزارة للبدء في إجراءات التعاقد .

عـــرض : برجاء النظـــر ،،

على سالم صلاح فؤاد

٠٨ ديسمبر ٢٠١٠

اقتراح
للإدارة العامة للمالية (مستشار مالي)
في ضوء التوجيه

* للإدارة المركزية للشئون المالية بالمرفقات
* صورة علم للقسم المالي للعلم
* صورة بالموضوع

٢١ / ١٢ / ٢٠١٠

بسم الله الرحمن الرحيم

الإدارة العامة للمعلومات ..
الإدارة المركزية لتكنولوجيا المعلومات
مجموعة المتابعة الإلكترونية
قسم الاختراق الالكتروني

[سري للغاية]

مذكـــــره

للعرض على السيد اللواء / مساعد أول الوزير رئيس القطاع

عـــن: شركة GAMMA الألمانيـــة العالميـــة المتخصصة فـــي صـــناعة البرمجيـــات والأنظمة الإلكترونية الأمنية.

- **تقدمت مؤخراً للجهاز شركة أنظمة الاتصالات الحديثة MCS** وكيلـــة عـــن شـــركة GAMMA الألمانية العالمية .. المتخصصة في صناعة البرمجيات والأنظمة الإلكترونيـــة الأمنية التي تستهدف اختراق صناديق البريد الإلكتروني (من أبـــرز منتجاتهـــا برنـــامج FINFISHER ـــ يـــتم اســـتخدامه مـــن قبـــل العديـــد مـــن الأجهـــزة الأمنيـــة والإستخباراتية العالمية).
- **أبدت الشركة استعدادها** لإمداد الجهاز بنسخة تجريبية " مجانية " من منتجها المشار إليـــه (عبارة عن جهاز كمبيوتر محمول مثبت عليـــه البرنـــامج المـــشار اليـــه) لتجربتـــه لمـــدة ٣ أســـابيع للوقـــوف علـــي إمكانياتـــه الفنيـــة وقدراتـــه فـــي مجـــال الاختـــراق الإلكتروني .. علي أن يقوم الجهاز والشركة الأجنبية بإبرام عقد تتبلور أبرز بنوده في التعهد بعدم تسريب نسخة من البرنامج لأي جهة أخري خلال تلك الفتـــرة .. كـــذا التـــزام الشركة بعدم التصريح لأي جهه أجنبية أو محلية بإستخدام الجهاز للبرنامج المشار اليه.
- **تقدر تكلفة نظام الإختراق المُشار إليه** بحوالي (٢ مليون جنية مصري تقريباً) .. نظراً لكونه نظام إختراق أمني رفيع المستوي يحقق العديد من الإمكانيات الفنية في هذا المجال غير متاحـــه في مثيلها من أنظمة الاختراق والتي يتمثل أبرزها في (إختراق عناوين الحـــسابات الشخـــصية علـــي شـــبكة الـــ SKYPE ، إختـــراق صـــناديق البريـــد الالكترونـــي علي شبكات " hotmail ـــ yahoo ـــ Gmail " ، إمكانية تحديث ملفات التجسس علـــي أجهزة العناصر المستهدفه وإستخدام أجهـــزتهم والبـــصمات الالكترونيـــة الخاصـــة بهـــم في التواصل ، التحكم الكامل في أجهزة العناصر المخترقه ، ....) .

*** يسعد نظام الـ SKYPE للتواصل الالكتروني .. نظام تواصل عبر الانترنت آمن ومشفر وقد لجأت إليه حالياً معظم الجماعات المتطرفة لتحقيق التواصل فيمـــا بينهم

وهو يتيح لعدد من المشتركين في النظام إجراء محادثات صوتية مشتركة فيما بينهم بطريقة آمنه ومشفرة تحول دون إختراقهم امنياً وتجنباً لعمليات الرصد الأمني (موضوع عرض سابق بشأن عقد اجتماع بمقر وزارة الاتصالات وتكنولوجيا المعلومات برئاسة السيد الدكتور وزير الاتصالات وتكنولوجيا المعلومات وحضور العديد من المسئولين بالأجهزة الأمنية بالبلاد).

- **نظام الاختراق** المشار إليه (FINFISHER) هو نظام الإختراق الأمني الوحيد علي مستوي العالم القادر علي إختراق **برنامج** الـ SKYPE للتواصل الإلكتروني.

- **في ضوء ما سبق** .. يري الموافقة علي توقيع العقد المشار إليه .. والتنسيق مع الشركة لبدء تجربة البرنامج علي اجهزة وشبكة منفصله تماماً عن اجهزة وشبكة الجهاز لمعرفة امكانية ومدي الاستفاده منه في مجال الاختراق الالكتروني.

- " مرفق صورة من العقد المطلوب التوقيع عليه ".

عـــرض : برجاء النظـــر

١٥ اغسطس ٢٠٠٩

٢٠٠٩/٨/١٥

GAMMA
INTERNATIONAL UK LIMITED

FINFISHER PROPOSAL

2. Commercial Offer



GAMMA INTERNATIONAL UK LIMITED

Europe • Asia • Middle East • Africa

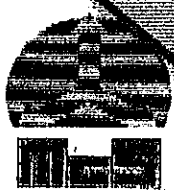


TO: State Security Investigation Department
Cairo
Egypt

OFFER NO. 0610-FF-GUK-061
DATE Tuesday June 29, 2010
CUSTOMER ID EGY-SSD
PAGE 6 / 12

CONTACT PERSON	REFERENCE	SHIPPING METHOD	SHIPPING TERMS	DELIVERY	PAYMENT TERMS	VALIDITY
Johnny Debs	JD	Air Freight	CIP	6-8 weeks	As per Terms & Conditions	1 month

ITEM #	DESCRIPTION	MODEL	QTY	UNIT PRICE (Euros)	LINE TOTAL (Euros)
A	**Remote Intrusion Solution**				
1	**FinSpy**				
1.1	**FinSpy Software**				
1.1.1	FinSpy Proxy License FinSpy Master License FinSpy Generation License	FSPL FSML FSGL	1	188,549.00	188,549.00
1.1.2	FinSpy Agent License (per client)	FSAGL	2	12,887.00	25,774.00
1.1.3	FinSpy Activation License: - Windows - OSX (Q4/2010)	FSPCAL	10	2,646.00	26,460.00
	Including First lifeline Support: FinSpy Update & Upgrade (Year 1)				
1.2	**FinSpy Hardware**				
1.2.1	FinSpy Master Server	FSM	1	6,112.00	6,112.00
1.2.2	FinSpy Agent Workstation	FSAG	2	1,112.00	2,224.00
1.2.3	FinSpy Common & Spare Parts	FSC	1	12,223.00	12,223.00
1.4	**FinSpy - Installation & Training**				
	FinSpy Installation and Product Training Number of Students: 2-4 Location: In-country Duration: 2 days Installation + 3 days Training Documentation: Soft and hard copies Including: airfare, accommodation, subsistence	FSTI	1	19,445.00	19,445.00
				SUBTOTAL	**280,787.00**
				Freight	**6,350.00**
				TOTAL	**287,137.00**



ITEM #	DESCRIPTION	MODEL	QTY	UNIT PRICE (Euros)	LINE TOTAL (Euros)
B	**Remote Infection Tools**				
1	**FinFly Lite**				
	Requires: FinIntrusion Kit as a base unit Consisting of: 1x FinFly Lite License 1x FinFly Lite CD Rom 1x User Manual	FFL	1	34,200.00	34,200.00
	Including FinLifeline Support: FinFly Lite Update & Upgrade (Year 1)				
1.2	**FinFly Lite - Training**				
	FinFly Lite Product Training Number of Students: 2-4 Location: In-country Duration: 2 days (can be integrated in FinIntrusion Kit Product Training) Documentation: Soft and hard copies Including: airfare, accommodation, food	FFLT	1	11,020.00	11,020.00
				SUBTOTAL	**45,220.00**
				Freight	**1,250.00**
				TOTAL	**46,470.00**

OPTIONS:

ITEM #	DESCRIPTION	MODEL	QTY	UNIT PRICE (Euros)	LINE TOTAL (Euros)
	Optional 2nd Year support - FinSpy				
1.1	**FinSpy - Support**				
1.1.1	FinLifeline Support: FinSpy Update & Upgrade Fee (Year 2)	FFLS1	1	6,840.00	6,840.00
	Optional 2nd Year support - FinFly-Lite				
1.3	**FinFly Lite - Support**				
1.3.1	FinLifeline Support: FinFly Lite Update & Upgrade Fee (Year 2)	FSS1	1	48,157.00	48,157.00

MILIPOL QATAR 2012

Exhibitor description

GAMMA GROUP

View the site

GAMMA GROUP

Fellows House, 46 Royce Close
West Portway Industrial Estate
SP10 3TS Andover - Hampshire
UNITED KINGDOM

Tel : +44 126 433 2411
Fax : +44 126 433 2422

http://www.gammagroup.com
info@gammagroup.com

Stands

D 111

Activities

Fields of activities

- Computer access control
- Control Room
- Encryption / Cryptography
- GSM
- High security communication networks
- Intelligence agency
- Mobile communication
- Scanners and walkthrough metal detectors
- Transmitter - Receiver - Transceiver
- Vehicle tracking

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 09 – July 2012

From Bahrain with Love: FinFisher's Spy Kit Exposed?

INTRODUCTION

Click here to read the Bloomberg News article.

The FinFisher Suite is described by its distributors, Gamma International UK Ltd., as "Governmental IT Intrusion and Remote Monitoring Solutions." [1] The toolset first gained notoriety after it was revealed that the Egyptian Government's state security apparatus had been involved in negotiations with Gamma International UK Ltd. over the purchase of the software. Promotional materials have been leaked that describe the tools as providing a wide range of intrusion and monitoring capabilities.[2] Despite this, however, the toolset itself has not been publicly analyzed.

This post contains analysis of several pieces of malware obtained by Vernon Silver of Bloomberg News that were sent to Bahraini pro-democracy activists in April and May of this year. The purpose of this work is identification and classification of the malware to better understand the actors behind the attacks and the risk to victims. In order to accomplish this, we undertook several different approaches during the investigation.

As well as directly examining the samples through static and dynamic analysis, we infected a virtual machine (VM) with the malware. We monitored the filesystem, network, and running operating system of the infected VM.

This analysis suggests the use of "Finspy", part of the commercial intrusion kit, Finfisher, distributed by Gamma International.

DELIVERY

This section describes how the malware was delivered to potential victims using e-mails with malicious attachments.

In early May, we were alerted that Bahraini activists were targeted with apparently malicious e-mails. The emails ostensibly pertained to the ongoing turmoil in Bahrain, and encouraged recipients to open a series of suspicious attachments. The screenshot below is indicative of typical message content:

----- Forwarded Message -----
From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

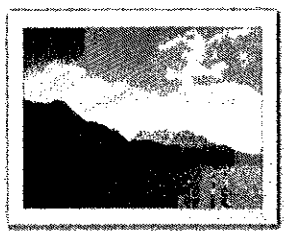
The attachments to the e-mails we have been able to analyze were typically .rar files, which we found to contain malware. Note that the apparent sender has an e-mail address that indicates that it was being sent by "Melissa Chan," who is a real correspondent for Aljazeera English. We suspect that the e-mail address is not her real address.[3] The following samples were examined:

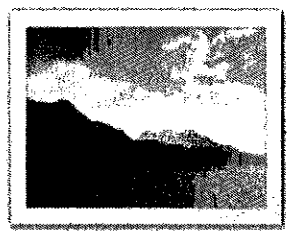
324783fbc33ec117f971cca77ef7ceaf7ce229a74edd6e2b3bd0effd9ed10dcc rar.الفعاليات
c5b39d98c85b21f8ac1bedd91f0b6510ea255411cf19c726545c1d0a23035914
_gpj.ArrestedXSuspects.rar
c5b37bb3620d4e7635c261e5810d628fc50e4ab06b843d78105a12cfbbea40d7
KingXhamadXonXofficialXvisitXtoX.rar
80fb86e265d44fbabac942f7b26c973944d2ace8a8268c094c3527b83169b3cc
MeetingXAgenda.rar
f846301e7f190ee3bb2d3821971cc2456617edc2060b07729415c45633a5a751 Rajab.rar

These contained executables masquerading as picture files or documents:

49000fc53412bfda157417e2335410cf69ac26b66b0818a3be7eff589669d040 dialoge.exe
cc3b65a0f559fa5e6bf4e60eef3bffe8d568a93dbb850f78bdd3560f38218b5c exe.Rajab1.jpg
39b325bd19e0fe6e3e0fca355c2afddfe19cdd14ebda7a5fc96491fc66e0faba exe.image1.jpg
e48bfeab2aca1741e6da62f8b8fc9e39078db57488169 1a464effe797222e632 exe.Rajab.jpg
2ec6814e4bad0cb03db6e241aabdc5e59661fb580bd870bdb50a39f1748b1d14 Suspects.jpg
exe.Arrested
c29052dc6ee8257ec6c74618b6175abd6eb4400412c99ff34763ff6e20bab864 News about the existence of a new dialogue between AlWefaq & Govt..doc

The emails generally suggested that the attachments contained political content of interest to pro-democracy activists and dissidents. In order to disguise the nature of the attachments a malicious usage of the "righttoleftoverride" (RLO) character was employed. The RLO character (U+202e in unicode) controls the positioning of characters in text containing characters flowing from right to left, such as Arabic or Hebrew. The malware appears on a victim's desktop as "exe.Rajab1.jpg" (for example), along with the default Windows icon for a picture file without thumbnail. But, when the UTF-8 based filename is displayed in ANSI, the name is displayed as "gpj.1bajaR.exe". Believing that they are opening a harmless ".jpg", victims are instead tricked into running an executable ".exe" file.[4]


exe.Rajab1.jpg


exe.Rajab.jpg

Upon execution these files install a multi-featured trojan on the victim's computer. This malware provides the attacker with clandestine remote access to the victim's machine as well as comprehensive data harvesting and exfiltration capabilities.

INSTALLATION

This section describes how the malware infects the target machine.

The malware displays a picture as expected. This differs from sample to sample. The sample "Arrested Suspects.jpg" ("gpj.stcepsuS detserrA.exe") displays:



It additionally creates a directory (which appears to vary from sample to sample):

```
C:\Documents and Settings\XPMUser\Local Settings\Temp\TMP51B7AFEF
```

It copies itself there (in this case the malware appears as "Arrested Suspects.jpg") where it is renamed:

```
C:\Documents and Settings\XPMUser\Local Settings\Temp\TMP51B7AFEF\Arrested Suspects.jpg" =>
C:\Documents and Settings\XPMUser\Local Settings\Temp\TMP51B7AFEF\tmpD.tmp
```

Then it drops the following files:

```
C:\DOCUME~1\%USER%\LOCALS~1\Temp\delete.bat
C:\DOCUME~1\%USER%\LOCALS~1\Temp\driverw.sys
```

It creates the folder (the name of which varies from host to host):

C:\Documents and Settings\%USER%\Application Data\Microsoft\Installer\{5DA45CC9-D840-47CC-9F86-FD2E9A718A41}

This process is observable on the filesystem timeline of the infected host:

```
Thu Jun 14 2012 11:50:59     35875 m..b r/rrwxrwxrwx 0       0       22469-128-4 C:/Documents and Settings/XPMUser/Desktop/Arrested Suspects.jpg
                                48 ...b d/drwxrwxrwx 0       0       25931-144-1 C:/Documents and Settings/XPMUser/Local Settings/Temp/TMP5187AFEF
                            909824 ...b r/rrwxrwxrwx 0       0       25932-128-4 C:/Documents and Settings/XPMUser/Local Settings/Temp/tmp0.tmp
Thu Jun 14 2012 11:51:01     35875 .ac. r/rrwxrwxrwx 0       0       22469-128-4 C:/Documents and Settings/XPMUser/Desktop/Arrested Suspects.jpg
                               807 ...b r/rrwxrwxrwx 0       0       25934-128-4 C:/Documents and Settings/XPMUser/Recent/Arrested Suspects.lnk
                            438272 .a.. r/rrwxrwxrwx 0       0       3011-128-3 C:/WINDOWS/system32/shimgvw.dll
Thu Jun 14 2012 11:51:02    389120 .a.. r/rrwxrwxrwx 0       0       2114-128-3 C:/WINDOWS/system32/cmd.exe
                               807 mac. r/rrwxrwxrwx 0       0       25934-128-4 C:/Documents and Settings/XPMUser/Recent/Arrested Suspects.lnk
Thu Jun 14 2012 11:51:03    389120 ..c. r/rrwxrwxrwx 0       0       2114-128-3 C:/WINDOWS/system32/cmd.exe
Thu Jun 14 2012 11:51:08        48 m.c. d/drwxrwxrwx 0       0       25931-144-1 C:/Documents and Settings/XPMUser/Local Settings/Temp/TMP5187AFEF
                            909824 .ac. r/rrwxrwxrwx 0       0       25932-128-4 C:/Documents and Settings/XPMUser/Local Settings/Temp/tmp0.tmp
Thu Jun 14 2012 11:51:09     37024 mac. r/rrwxrwxrwx 0       0       10351-128-4 C:/WINDOWS/Prefetch/CMD.EXE-087B4001.pf
                               56 m.c. d/drwxrwxrwx 0       0       10992-144-6 C:/Documents and Settings/XPMUser/Application Data/Microsoft
                              312 m.cb d/drwxrwxrwx 0       0       25933-144-1 C:/Documents and Settings/XPMUser/Application Data/Microsoft/Installer
                               48 ..c. d/drwxrwxrwx 0       0       25935-144-1 C:/Documents and Settings/XPMUser/Application Data/Microsoft/Installer/{5AA8219B-102B-4404-2F96-57347FF27294}
                            11008 .ac. r/rrwxrwxrwx 0       0       25936-128-3 C:/Documents and Settings/XPMUser/Local Settings/Temp/driverw.sys
```

"driverw.sys" is loaded and then "delete.bat" is run which deletes the original payload and itself. It then infects existing operating system processes, connects to the command and control server, and begins data harvesting and exfiltration.

Examining the memory image of a machine infected with the malware shows that a technique for infecting processes known as **"process hollowing"** is used. For example, the memory segment below from the "winlogon.exe" process is marked as executable and writeable:

```
Process: winlogon.exe Pid: 424 Address: 0x1af0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 19, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01af0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x01af0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x01af0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01af0030  00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00   ................
```

Here the malware starts a new instance of a legitimate process such as "winlogon.exe" and before the process's first thread begins, the malware de-allocates the memory containing the legitimate code and injects malicious code in its place. Dumping and examining this memory segment reveals the following strings in the infected process:

```
00003960  47 4e 55 20 4d 50 3a 20  43 61 6e 6e 6f 74 20 61  |GNU MP: Cannot a|
00003970  6c 6c 6f 63 61 74 65 20  6d 65 6d 6f 72 79 20 28  |llocate memory (|
00003980  73 69 7a 65 3d 25 75 29  0a 00 00 00 47 4e 55 20  |size=%u)....GNU |
00003990  4d 50 3a 20 43 61 6e 6e  6f 74 20 72 65 61 6c 6c  |MP: Cannot reall|
000039a0  6f 63 61 74 65 20 6d 65  6d 6f 72 79 20 28 6f 6c  |ocate memory (ol|
000039b0  64 5f 73 69 7a 65 3d 25  75 20 6e 65 77 5f 73 69  |d_size=%u new_si|
000039c0  7a 65 3d 25 75 29 0a 00  79 3a 5c 6c 73 76 6e 5f  |ze=%u)..y:\lsvn_|
000039d0  62 72 61 6e 63 68 65 73  5c 66 69 6e 73 70 79 76  |branches\finspyv|
000039e0  34 2e 30 31 5c 66 69 6e  73 70 79 76 32 5c 73 72  |4.01\finspyv2\sr|
000039f0  63 5c 6c 69 62 73 5c 6c  69 62 67 6d 70 5c 6d 70  |c\libs\libgmp\mp|
00003a00  6e 2d 74 64 69 76 5f 71  72 2e 63 00 63 20 3d 3d  |n-tdiv_qr.c.c ==|
00003a10  20 30 00 00 00 00 00 00  01 02 03 03 04 04 04 04  | 0...............|
```

Note the string:

y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-tdiv_qr.c

This file seems to correspond to a file in the GNU Multi-Precision arithmetic library:
http://gmplib.org:8000/gmp/file/b5ca16212198/mpn/generic/tdiv_qr.c

The process "svchost.exe" was also found to be infected in a similar manner:

```
Process: svchost.exe Pid: 760 Address: 0xbd0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00bd0000  8b ff 55 8b ec 68 40 47 f1 73 c3 8b ff 55 8b ec   ..U..h@G.s...U..
0x00bd0010  68 c0 68 f3 73 c3 8b ff 55 8b ec 68 ae 8e b4 76   h.h.s...U..h...v
0x00bd0020  c3 8b ff 55 8b ec 68 e2 c0 b5 76 c3 8b ff 55 8b   ...U..h...v...U.
0x00bd0030  ec 68 ff c2 b5 76 c3 8b ff 55 8b ec 68 3d c3 b5   .h...v...U..h=..

0xbd0000 8bff            MOV EDI, EDI
0xbd0002 55              PUSH EBP
0xbd0003 8bec            MOV EBP, ESP
0xbd0005 6840471173      PUSH DWORD 0x73f14740
0xbd000a c3              RET
0xbd000b 8bff            MOV EDI, EDI
0xbd000d 55              PUSH EBP
0xbd000e 8bec            MOV EBP, ESP
0xbd0010 68c068f373      PUSH DWORD 0x73f368c0
0xbd0015 c3              RET
0xbd0016 8bff            MOV EDI, EDI
0xbd0018 55              PUSH EBP
0xbd0019 8bec            MOV EBP, ESP
0xbd001b 68ae8eb476      PUSH DWORD 0x76b48eae
0xbd0020 c3              RET
0xbd0021 8bff            MOV EDI, EDI
0xbd0023 55              PUSH EBP
0xbd0024 8bec            MOV EBP, ESP
0xbd0026 68e2c0b576      PUSH DWORD 0x76b5c0e2
0xbd002b c3              RET
0xbd002c 8bff            MOV EDI, EDI
0xbd002e 55              PUSH EBP
0xbd002f 8bec            MOV EBP, ESP
0xbd0031 68ffc2b576      PUSH DWORD 0x76b5c2ff
0xbd0036 c3              RET
0xbd0037 8bff            MOV EDI, EDI
0xbd0039 55              PUSH EBP
0xbd003a 8bec            MOV EBP, ESP
0xbd003c 68              DB 0x68
0xbd003d 3d              DB 0x3d
0xbd003e c3              RET
0xbd003f b5              DB 0xb5
```

Further examination of the memory dump also reveals the following:

```
018e9ed0  28 94 df 66 12 14 ca 42  aa 76 42 35 15 4d c3 8b  |(..f...B.vB5.M..|
018e9ee0  01 00 00 00 79 3a 5c 6c  73 76 6e 5f 62 72 61 6e  |....y:\lsvn_bran|
018e9ef0  63 68 65 73 5c 66 69 6e  73 70 79 76 34 2e 30 31  |ches\finspyv4.01|
018e9f00  5c 66 69 6e 73 70 79 76  32 5c 73 72 63 5c 74 61  |\finspyv2\src\ta|
018e9f10  72 67 65 74 5c 62 6f 6f  74 6b 69 74 5f 78 33 32  |rget\bootkit_x32|
018e9f20  64 72 69 76 65 72 5c 6f  62 6a 66 72 65 5f 77 32  |driver\objfre_w2|
018e9f30  6b 5f 78 38 36 5c 69 33  38 36 5c 62 6f 6f 74 6b  |k_x86\i386\bootk|
018e9f40  69 74 5f 78 33 32 64 72  69 76 65 72 2e 70 64 62  |it_x32driver.pdb|
018e9f50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
```

This path appears to reference the functionality that the malware uses to modify the boot sequence to enable persistence:

```
y:\lsvn_branches\finspyv4.01\finspyv2\src\target\bootkit_x32driver\objfre_w2k_x86\i386\bootkit_x32driver.pdb
```

A pre-infection vs post-infection comparison of the infected VM shows that the Master Boot Record (MBR) was modified by code injected by the malware.
The strings found in memory "finspyv4.01" and "finspyv2" are particularly interesting. The FinSpy tool is part of the FinFisher intrusion and monitoring toolkit.[5]

OBFUSCATION AND EVASION

This section describes how the malware is designed to resist analysis and evade identification.

The malware employs a myriad of techniques designed to evade detection and frustrate analysis. While investigation into this area is far from complete, we discuss several discovered methods as examples of the lengths taken by the developers to avoid identification.

A virtualised packer is used. This type of obfuscation is used by those that have "strong motives to prevent their malware from being analyzed".[6]

This converts the native x86 instructions of the malware into another custom language chosen from one of 11 code templates. At run-time, this is interpreted by an obfuscated interpreter customized for that particular language. This virtualised packer was not recognised and appears to be bespoke.

Several anti-debugging techniques are used. This section of code crashes the popular debugger, OllyDbg.

```
.text:00401683 finit
.text:00401686 fld ds:tbyte_40168E
.text:0040168C jmp short locret_401698
-------------------------------------
.text:0040168E tbyte_40168E dt 9.223372036854775807e18
-------------------------------------
.text:00401698 locret_401698:
.text:00401698 retn
```

This float value causes OllyDbg to crash when trying to display its value. A more detailed explanation of this can be found here.

To defeat DbgBreakPoint based debuggers, the malware finds the address of DbgBreakPoint, makes the page EXECUTE_READWRITE and writes a NOP on the entry point of DbgBreakPoint.

The malware checks via PEB to detect whether or not it is being debugged, and if it is it returns a random address.

The malware calls ZwSetInformationThread with ThreadInformationClass set to 0×11, which causes the thread to be detached from the debugger.

The malware calls ZwQueryInformationProcess with ThreadInformationClass set to 0x(ProcessDebugPort) and 0x1e (ProcessDebugObjectHandle) to detect the presence of a debugger. If a debugger is detected it jumps to a random address. ZwQueryInformationProcess is also called to check the DEP status on the current process, and it disables it if it's found to be enabled.

The malware deploys a granular solution for Antivirus software, tailored to the AV present on the infected machine. The malware calls ZwQuerySystemInformation to get ProcessInformation and ModuleInformation. The malware then walks the list of processes and modules looking for installed AV software. Our analysis indicates that the malware appears to have different code to Open/Create process and inject for each AV solution. For some Anti-Virus software this even appears to be version dependent. The function "ZwQuerySystemInformation" is also hooked by the malware, a technique frequently used to allow process hiding:

```
********************************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 628 (svchost.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9b2000)
Function: ntdll.dll!ZwQuerySystemInformation at 0x7c90d92e
Hook address: 0xfd34b8
Hooking module: <unknown>

Disassembly(0):
0x7c90d92e e9855b6c84      JMP 0xfd34b8
0x7c90d933 ba0003fe7f      MOV EDX, 0x7ffe0300
0x7c90d938 ff12            CALL DWORD [EDX]
0x7c90d93a c21000          RET 0x10
0x7c90d93d 90              NOP
0x7c90d93e b8ae000000      MOV EAX, 0xae
0x7c90d943 ba              DB 0xba
0x7c90d944 0003            ADD [EBX], AL

Disassembly(1):
0xfd34b8 8bff            MOV EDI, EDI
0xfd34ba 55              PUSH EBP
0xfd34bb 8bec            MOV EBP, ESP
0xfd34bd 56              PUSH ESI
0xfd34be ff7514          PUSH DWORD [EBP+0x14]
0xfd34c1 8b750c          MOV ESI, [EBP+0xc]
0xfd34c4 ff7510          PUSH DWORD [EBP+0x10]
0xfd34c7 56              PUSH ESI
0xfd34c8 ff7508          PUSH DWORD [EBP+0x8]
0xfd34cb ff              DB 0xff
0xfd34cc 15              DB 0x15
0xfd34cd 9c              PUSHF
0xfd34ce 9d              POPF
0xfd34cf fd              STD
```

DATA HARVESTING AND ENCRYPTION

This section describes how the malware collects and encrypts data from the infected machine.

Our analysis showed that the malware collects a wide range of data from an infected victim. The data is stored locally in a hidden directory, and is disguised with encryption prior to exfiltration. On the reference victim host, the directory was:

"C:\Windows\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}."

We conducted forensic examination of the files created in this directory and identified a wide range of data collected. Files in this directory were found to be screenshots, keylogger data, audio from Skype calls, passwords and more. For the sake of brevity we include a limited set of examples here.

The malware attempts to locate the configuration and password store files for a variety browsers and chat clients as seen below:

rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Profiles	NAME NOT FOUND
rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Thunderbird\Profiles	PATH NOT FOUND
rundll32.exe	3996	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Trillian\users\global	PATH NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Profiles	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\.gaim	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\.purple	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Miranda	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\MySpace\IM\users.txt	PATH NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Digsby\digsby.dat	PATH NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\history.dat	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\places.sqlite	SUCCESS
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.txt	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons2.txt	NAME NOT FOUND
rundll32.exe	4024	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons3.txt	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\history.dat	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\places.sqlite	SUCCESS
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\nssckbi.dll	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite	SUCCESS
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4060	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Mozilla\Firefox\Profiles\yz9d0pnf.default\signons.sqlite...	NAME NOT FOUND
rundll32.exe	4068	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS
rundll32.exe	4068	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data\Google\Chrome\User Data\Default\Web ...	PATH NOT FOUND
rundll32.exe	4068	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data\Google\Chrome\User Data\Default\Login...	PATH NOT FOUND
rundll32.exe	4080	QueryOpen	C:\Documents and Settings\XPMUser\Application Data	SUCCESS
rundll32.exe	4080	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Opera\Opera\wand.dat	PATH NOT FOUND
rundll32.exe	4080	QueryOpen	C:\Documents and Settings\XPMUser\Application Data\Opera\Opera7\profile\wand.dat	PATH NOT FOUND
rundll32.exe	4088	QueryOpen	C:\Documents and Settings\XPMUser\Local Settings\Application Data	SUCCESS

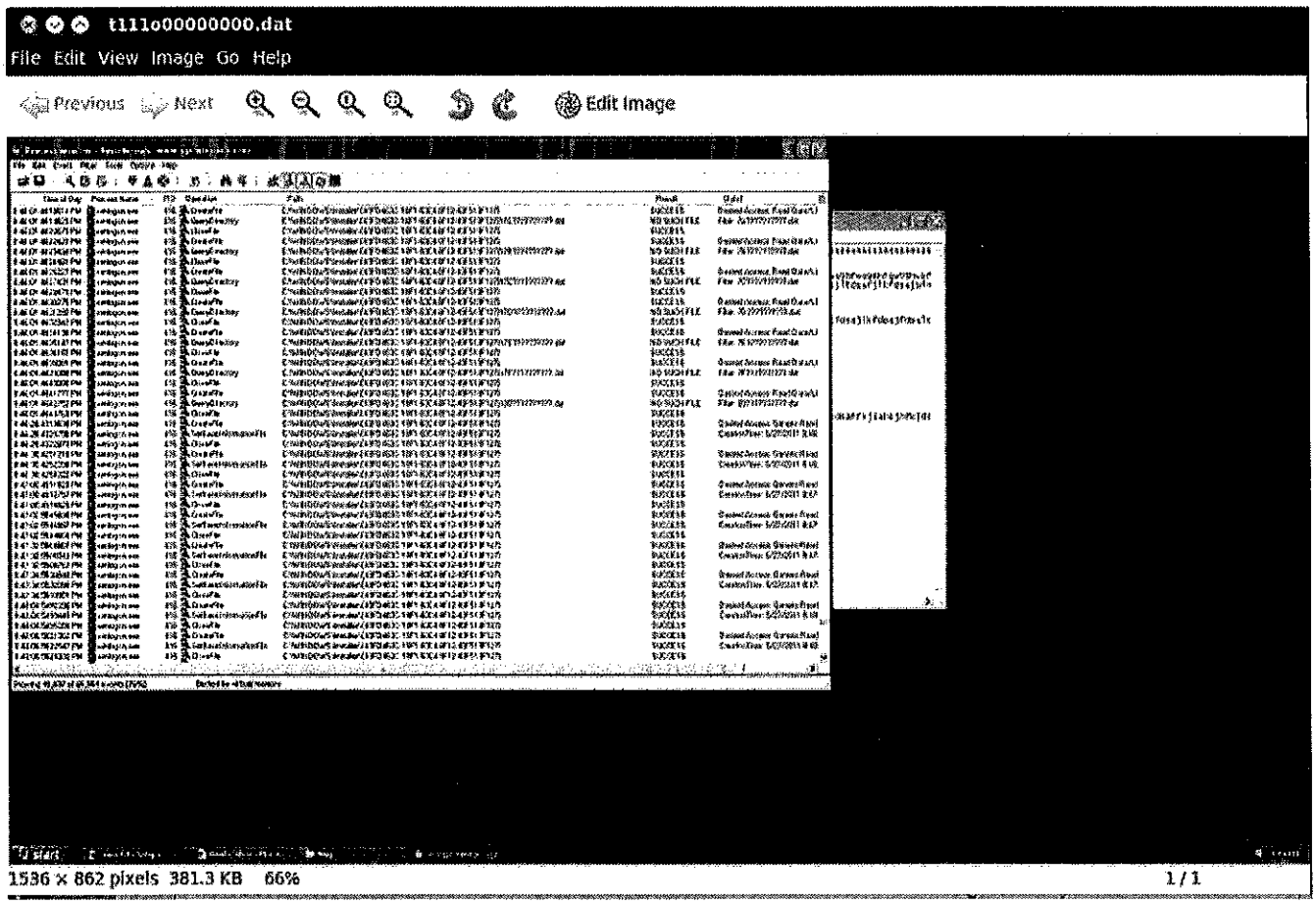
We observed the creation of the file "t111o00000000.dat" in the data harvesting directory, as shown in the filesystem timeline below:

Thu Jun 14 2012 12:31:34 52719 mac. r/rr-xr-xr-x 0 0 26395-128-5 C:/WINDOWS/Installer/{49FD463C-18F1-63C4-8F12-49F518F127}/09e493e2-05f9-4899-b661-c52f3554c644
Thu Jun 14 2012 12:32:18 285691 …b r/rrwxrwxrwx 0 0 26397-128-4 C:/WINDOWS/Installer/{49FD463C-18F1-63C4-8F12-49F518F127}/t111o00000000.dat
Thu Jun 14 2012 12:55:12 285691 mac. r/rrwxrwxrwx 0 0 26397-128-4 C:/WINDOWS/Installer/{49FD463C-18F1-63C4-8F12-49F518F127}/t111o00000000.dat
4096 ..c. -/rr-xr-xr-x 0 0 26447-128-4

The infected process "winlogon.exe" was observed writing this file via Process:

winlogon.exe	420	CreateFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Desired Access: Generic Write,
winlogon.exe	420	SetEndOfFileInformationFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	EndOfFile: 0
winlogon.exe	420	SetAllocationInformationFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	AllocationSize: 0
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 0, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 4,096, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 8,192, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 12,288, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 16,384, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 20,480, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 24,576, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 28,672, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 32,768, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 36,864, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 40,960, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 45,056, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 49,152, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 53,248, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 57,344, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 61,440, Length: 4,096
winlogon.exe	420	WriteFile	C:\WINDOWS\Installer\{49FD463C-18F1-63C4-8F12-49F518F127}\t111o00000000.dat	SUCCESS	Offset: 65,536, Length: 4,096

Examination of this file reveals that it is a screenshot of the desktop:



Many other modules providing specific exfiltration capabilities were observed. Generally, the exfiltration modules write files to disk using the following naming convention: XXY1TTTTTTTT.dat. XX is a two-digit hexadecimal module number, Y is a single-digit hexadecimal submodule number, and TTTTTTTT is a hexadecimal representation of a unix timestamp (less 1.3 billion) associated with the file creation time.

ENCRYPTION

The malware uses encryption in an attempt to disguise harvested data in the .dat files intended for exfiltration. Data written to the files is encrypted using AES-256-CBC (with no padding). The 32-byte key consists of 8 readings from memory address 0x7ffe0014: a special address in Windows that contains the low-order-4-bytes of the number of hundred-nanoseconds since 1 January 1601. The IV consists of 4 additional readings.

The AES key structure is highly predictable, as the quantum for updating the system clock **(HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Config\LastClockRate)** is set to 0x2625A hundred-nanoseconds by default, and the clock readings that comprise the key and IV are taken in a tight loop:

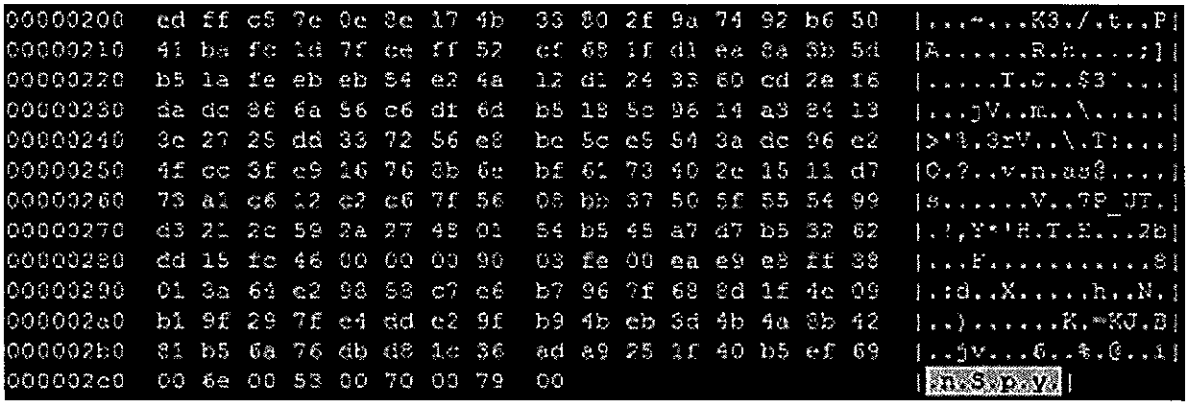
```
...
0x406EA4: 8D45C0 LEA EAX,[EBP-0x40]
0x406EA7: 50 PUSH EAX
0x406EA8: FF150C10AF01 CALL DWORD PTR [0x1AF100C]
0x406EAE: 8B4DE8 MOV ECX,DWORD PTR [EBP-0x18]
0x406EB1: 8B45C0 MOV EAX,DWORD PTR [EBP-0x40]
0x406EB4: 8345E804 ADD DWORD PTR [EBP-0x18],0×4
0x406EB8: 6A01 PUSH 0×1
0x406EBA: 89040F MOV DWORD PTR [EDI+ECX],EAX
0x406EBD: FF152810AF01 CALL DWORD PTR [0x1AF1028]
0x406EC3: 817DE800010000 CMP DWORD PTR [EBP-0x18],0×100
0x406ECA: 72D8 JB 0x406EA4
0x406ECC: 80277F AND BYTE PTR [EDI],0x7F
...
```

The following AES keys were among those found to be used to encrypt records in .dat files. The first contains the same 4 bytes repeated, whereas in the second key, the difference between all consecutive 4-byte blocks (with byte order swapped) is 0x2625A.

```
70 31 bd cc 70 31 bd cc 70 31 bd cc 70 31 bd cc 70 31 bd cc 70 31 bd cc 70 31
bd cc 70 31 bd cc
26 e9 23 60 80 4b 26 60 da ad 28 60 34 10 2b 60 8e 72 2d 60 e8 d4 2f 60 42 37
32 60 9c 99 34 60
```

In all, 64 clock readings are taken. The readings are encrypted using an RSA public key found in memory (whose modulus begins with A25A944E) and written to the .dat file before any other encrypted data. No

padding is used in the encryption, yielding exactly 256 encrypted bytes. After the encrypted timestamp values, the file contains a number of records encrypted with AES, delimited by EAE9E8FF.
In reality, these records are only partially encrypted: if the record's length is not a multiple of 16 bytes (the AES block size), then the remainder of the bytes are written to the file unencrypted. For example, after typing "FinSpy" on the keyboard, the keylogger module produced the following (trailing plaintext highlighted):



The predictability of the AES encryption keys allowed us to decrypt and view these partially-encrypted records in full plaintext. The nature of the records depends on the particular module and submodule. For example, submodule Y == 5 of the Skype exfiltration module (XX == 14), contains a csv representation of the user's contact list:

Record # 0 Length: 243 bytes:
ó
@þÿÌ³Ð
@
¤b¯Opþ192.168.131.67JRecordingEcsv 0þ-0800UTC DST.1þ2012-07-18 18:00:21.:þ1970-01-01 00:16:00Abhwatch1

Record # 1 Length: 96 bytes:
`USERNAME,FULLNAME,COUNTRY,AUTHORIZED,BLOCKED

Record # 2 Length: 90 bytes:
Zecho123,Echo / Sound Test Service,,YES,NO
Record # 3 Length: 95 bytes:
^bhwatch2,Bahrain Watch,United States,YES,NO

Submodule Y == 3 records file transfers. After a Skype file transfer concludes, the following file is created: %USERPROFILE%\Local Settings\Temp\smtXX.tmp. This file appears to contain the sent / received file.

As soon as smtXX.tmp is finished being written to disk, a file (1431XXXXXXXX.dat) is written, roughly the same size as smtXX.tmp. After sending a picture (of birdshot shotgun shell casings used by Bahrain's police) to an infected Skype client, the file 1431028D41FD.dat was observed being written to disk. Decrypting it revealed the following:

Record # 0 Length: 441 bytes:
ı
@þÿÌ³Ð
@
¤b¯Opþ192.168.131.67Abhwatch1Bbhwatch2"CBahrain WatchIreceivedrC:\Documents and Settings\XPMUser\My Documents\gameborev3.jpgJRecording 0þ-0800UTC DST.1þ2012-07-20 12:18:21.:þ2012-07-20 12:18:21

Record # 1 Length: 78247 bytes:
[Note: Record #1 contained the contents of the .jpg file, preceded by hex A731010090051400, and followed by hex 0A0A0A0A.]

Additionally, submodule Y == 1 records Skype chat messages, and submodule Y == 2 records audio from all participants in a Skype call. The call recording functionality appears to be provided by hooking DirectSoundCaptureCreate:

```
************************************************************************
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 424 (winlogon.exe)
Victim module: dsound.dll (0x73f10000 - 0x73f6c000)
Function: dsound.dll!DirectSoundCreate at 0x73f1473b
Hook address: 0x2943b1a
Hooking module: <unknown>

Disassembly(0):
0x73f1473b e9daf3a28e       JMP 0x2943b1a
0x73f14740 51               PUSH ECX
0x73f14741 8b0d0460f673     MOV ECX, [0x73f66004]
0x73f14747 8365fc00         AND DWORD [EBP-0x4], 0x0
0x73f1474b 56               PUSH ESI
0x73f1474c 57               PUSH EDI
0x73f1474d e8b9d6ffff       CALL 0x73f11e0b
0x73f14752 83               DB 0x83

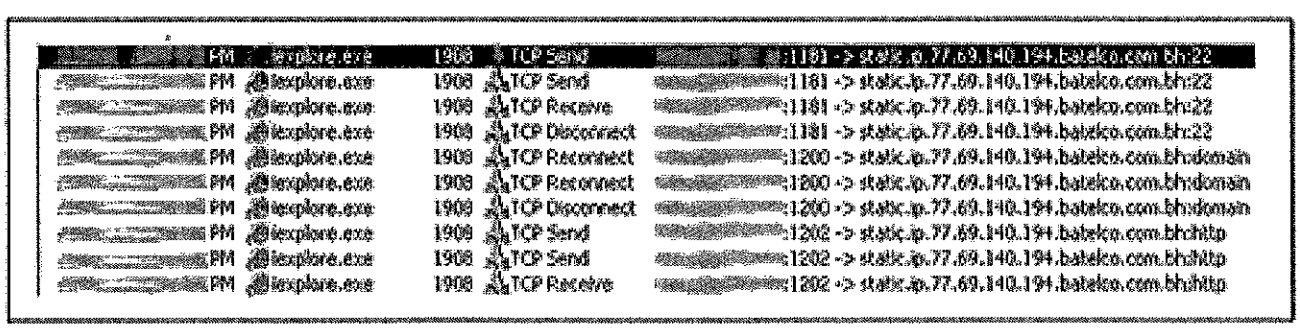
Disassembly(1):
0x2943b1a 8bff              MOV EDI, EDI
0x2943b1c 55                PUSH EBP
0x2943b1d 8bec              MOV EBP, ESP
0x2943b1f 56                PUSH ESI
0x2943b20 ff7510            PUSH DWORD [EBP+0x10]
0x2943b23 8b750c            MOV ESI, [EBP+0xc]
0x2943b26 56                PUSH ESI
0x2943b27 ff7508            PUSH DWORD [EBP+0x8]
0x2943b2a ff15c4ac9402      CALL DWORD [0x294acc4]
0x2943b30 85c0              TEST EAX, EAX

************************************************************************
```

COMMAND AND CONTROL

This section describes the communications behavior of the malware.

When we examined the malware samples we found that they connect to a server at IP address 77.69.140.194



WHOIS data[7] reveals that this address is owned by Batelco, the principal telecommunications company of Bahrain:

inetnum: 77.69.128.0 – 77.69.159.255
netname: ADSL
descr: Batelco ADSL service
country: bh

For a period of close to 10 minutes, traffic was observed between the infected victim and the command and control host in Bahrain.

A summary of the traffic by port and conversation size:

TCP Conversations · Filter: ip.addr == 77.69.140.194

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B	Packets A←B	Bytes A←B	Rel Start	Duration	Bps A→B	Bps A←B
192.168.131.65	1200	77.69.140.194	53	3	186	3	186	0	0	46.533336000	8.9749	165.80	N/A
192.168.131.65	1212	77.69.140.194	53	3	186	3	186	0	0	229.148416000	8.9776	165.75	N/A
192.168.131.65	1217	77.69.140.194	53	3	186	3	186	0	0	447.436820000	8.9725	165.84	N/A
192.168.131.65	1204	77.69.140.194	80	15	1767	8	1273	7	494	101.999621000	2.0481	4972.45	1929.61
192.168.131.65	1205	77.69.140.194	80	15	1767	8	1273	7	494	134.195659000	2.0208	5039.53	1955.64
192.168.131.65	1181	77.69.140.194	22	25	5489	13	4387	12	1102	15.101931000	2.5512	13756.79	3455.66
192.168.131.65	1202	77.69.140.194	80	25	5225	13	4387	12	838	68.840833000	2.7173	12915.95	2467.19
192.168.131.65	1207	77.69.140.194	80	56	7266	27	4312	29	2954	166.481391000	32.9779	1046.04	716.60
192.168.131.65	1213	77.69.140.194	443	1710	1270075	597	59063	1113	1211012	251.429902000	193.7304	2438.98	50008.13
77.69.140.194	4111	192.168.131.65	1219	15660	4766223	8258	498534	7402	4267689	469.714476000	196.8652	20259.71	173425.05

The infected VM talks to the remote host on the following five TCP ports:

22
53
80
443
4111

Based on observation of an infected machine we were able to determine that the majority of data is exfiltrated to the remote host via ports 443 and 4111.

192.168.131.65:1213 -> 77.69.140.194:443 1270075 bytes
192.168.131.65:4111 -> 77.69.149.194:4111 4766223 bytes

CONCLUSIONS ABOUT MALWARE IDENTIFICATION

Our analysis yields indicators about the identity of the malware we have analyzed: (1) debug strings found the in memory of infected processes appear to identify the product and (2) the samples have similarities with malware that communicates with domains belonging to Gamma International.

Debug Strings found in memory

As we previously noted, infected processes were found containing strings that include "finspyv4.01" and "finspyv2":

```
y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-tdiv_qr.c
y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-mul_fft.c
y:\lsvn_branches\finspyv4.01\finspyv2\src\target\bootkit_x32driver\objfre_w2k_x86\i386\bootkit_x32
driver.pdb
```

Publicly available descriptions of the FinSpy tool collected by Privacy International among others and posted on Wikileaks[8] make the a series of claims about functionality:

- Bypassing of 40 regularly tested Antivirus Systems
- Covert Communication with Headquarters
- Full Skype Monitoring (Calls, Chats, File Transfers, Video, Contact List)
- Recording of common communication like Email, Chats and Voice-over-IP
- Live Surveillance through Webcam and Microphone
- Country Tracing of Target
- Silent Extracting of Files from Hard-Disk
- Process-based Key-logger for faster analysis
- Live Remote Forensics on Target System
- Advanced Filters to record only important information
- Supports most common Operating Systems (Windows, Mac OSX and Linux)

Shared behavior with a sample that communicates with Gamma

The virtual machine used by the packer has very special sequences in order to execute the virtualised code, for example:

```
66 C7 07 9D 61 mov word ptr [edi], 619Dh
C6 47 02 68 mov byte ptr [edi+2], 68h
89 57 03 mov [edi+3], edx
C7 47 07 68 00 00 00 mov dword ptr [edi+7], 68h
89 47 08 mov [edi+8], eax
C6 47 0C C3 mov byte ptr [edi+0Ch], 0C3h
```

Based on this we created a signature from the Bahrani malware, which we shared with another security researcher who identified a sample that shared similar virtualised obfuscation. That sample is:

md5: c488a8aaef0df577efdf1b501611ec20
sha1: 5ea6ae50063da8354e8500d02d0621f643827346
sha256: 81531ce5a248aead7cda76dd300f303dafe6f1b7a4c953ca4d7a9a27b5cd6cdf

The sample connects to the following domains:

tiger.gamma-international.de
ff-demo.blogdns.org

The domain **tiger.gamma-international.de** has the following Whois information[9]:

Domain: gamma-international.de
Name: Martin Muench
Organisation: Gamma International GmbH
Address: Baierbrunner Str. 15
PostalCode: 81379
City: Munich
CountryCode: DE
Phone: +49-89-2420918-0
Fax: +49-89-2420918-1
Email: info@gamma-international.de
Changed: 2011-04-04T11:24:20+02:00

Martin Muench is a representative of Gamma International, a company that sells "advanced technical surveillance and monitoring solutions". One of the services they provide is FinFisher: IT Intrusion, including the FinSpy tool. This labelling indicates that the matching sample we were provided may be a demo copy a FinFisher product per the domain **ff-demo.blogdns.org**.

We have linked a set of novel virtualised code obfuscation techniques in our Bahraini samples to another binary that communicates with Gamma International IP addresses. Taken alongside the explicit use of the name "FinSpy" in debug strings found in infected processes, we suspect that the malware is the FinSpy remote intrusion tool. This evidence appears to be consistent with the theory that the dissidents in Bahrain who received these e-mails were targeted with the FinSpy tool, configured to exfiltrate their harvested information to servers in Bahraini IP space. If this is not the case, we invite Gamma International to explain.

RECOMMENDATIONS

The samples from email attachments have been shared with selected individuals within the security community, and we strongly urge antivirus companies and security researchers to continue where we have left off.

Be wary of opening unsolicited attachments received via email, skype or any other communications mechanism. If you believe that you are being targeted it pays to be especially cautious when downloading files over the Internet, even from links that are purportedly sent by friends.

ACKNOWLEDGEMENTS

Malware analysis by Morgan Marquis-Boire and Bill Marczak. Assistance from Seth Hardy and Harry Tuttle gratefully received.

Special thanks to John Scott-Railton.

Thanks to Marcia Hofmann and the Electronic Frontier Foundation (EFF).

We would also like to acknowledge Privacy International for their continued work and graciously provided background information on Gamma International.

FOOTNOTES

[1] http://www.finfisher.com/
[2] http://owni.eu/2011/12/15/finfisher-for-all-your-intrusive-surveillance-needs/#SpyFiles
[3] http://blogs.aljazeera.com/profile/melissa-chan
[4] This technique was used in the recent Madi malware attacks.
[5] http://www.finfisher.com/
[6] Unpacking Virtualised Obfuscators by Rolf Rolles – http://static.usenix.org/event/woot09/tech/full_papers/rolles.pdf
[7] http://whois.domaintools.com/77.69.140.194
[8] E.g. http://wikileaks.org/spyfiles/files/0/289_GAMMA-201110-FinSpy.pdf
[9] http://whois.domaintools.com/gamma-international.de

UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Research Brief
Number 11 – August 2012

The SmartPhone Who Loved Me: FinFisher Goes Mobile?

by Morgan Marquis-Boire, Bill Marczak and Claudio Guarnieri

This post describes our work analyzing several samples which appear to be mobile variants of the FinFisher Toolkit, and ongoing scanning we are performing that has identified more apparent FinFisher command and control servers.

INTRODUCTION

Earlier this year, Bahraini Human Rights activists were targeted by an email campaign that delivered a sophisticated Trojan. In *From Bahrain with Love: FinFisher's Spy Kit Exposed?* we characterized the malware, and suggested that it appeared to be FinSpy, part of the FinFisher commercial surveillance toolkit. Vernon Silver concurrently reported our findings in Bloomberg, providing background on the attack and the analysis, and highlighting links to FinFisher's parent company, Gamma International.

After these initial reports, Rapid7, a Boston-based security company, produced a follow-up analysis that identified apparent FinFisher Command and Control (C&C) servers on five continents. After the release of the Rapid7 report, Gamma International representatives spoke with Bloomberg and The New York Times' Bits Blog, and denied that the servers found in 10 countries were instances of their products.

Following these analyses, we were contacted by both the security and activist communities with potentially interesting samples. From these, we identified several apparent mobile Trojans for the iOS, Android, BlackBerry, Windows Mobile and Symbian platforms. **Based on our analysis, we found these tools to be consistent in functionality with claims made in the documentation for the FinSpy Mobile product**, a component of the FinFisher toolkit. Several samples appear to be either demo versions or "unpackaged" versions ready to be customized, while others appear to be samples in active use.

Promotional literature describes this product as providing:

- Recording of common communications like Voice Calls, SMS/MMS and Emails
- Live Surveillance through silent calls
- File Download (Contacts, Calendar, Pictures, Files)
- Country Tracing of Target (GPS and Cell ID)
- Full Recording of all BlackBerry Messenger communications
- Covert Communications with Headquarters

In addition to analysis of these samples, we are conducting an ongoing scan for FinFisher C&C servers, and have identified potential servers in the following countries: Bahrain, Brunei, the Czech Republic, Ethiopia, Indonesia, Mongolia, Singapore, the Netherlands, Turkmenistan, and the United Arab Emirates (UAE).

MOBILE TROJANS

iOS

It was developed for Arm7, built against iOS SDK 5.1 on OSX 10.7.3 and it appears that it will run on iPhone 4, 4S, iPad 1, 2, 3, and iPod touch 3, 4 on iOS 4.0 and up.

The bundle is called "install_manager.app" and the contents of it are:

```
99621a7301bfd00d98c222a89900aeef ./data
1f73ebf8be52aa14d4d4546fb3242728 ./_CodeSignature/CodeResources
9273880e5baa5ac810f312f8bd29bd3f ./embedded.mobileprovision
2cbe06c89dc5a43ea0e0600ed496803e ./install_manager
23b7d7d024abb0f558420e098800bf27 ./PkgInfo
11e4821d845f369b610c31592f4316d9 ./Info.plist
ce7f5b3d4bfc7b4b0da6a06dccc515f2 ./en.lproj/InfoPlist.strings
3fa32da3b25862ba16af040be3451922 ./ResourceRules.plist
```

Investigation of the Mach-0 binary 'install_manager' reveals the text "FinSpy":

```
0000b780  70 02 00 00 6f 02 00 00  20 00 2f 55 73 65 72 73  |p...o... ./Users|
0000b790  2f 61 64 6d 2f 43 6f 64  65 2f 64 65 76 65 6c 6f  |/adm/Code/develo|
0000b7a0  70 6d 65 6e 74 2f 46 69  6e 53 70 79 56 32 2f 73  |pment/FinSpyV2/s|
0000b7b0  72 63 2f 69 4f 53 2f 43  6f 72 65 54 61 72 67 65  |rc/iOS/CoreTarge|
0000b7c0  74 2f 00 2f 55 73 65 72  73 2f 61 64 6d 2f 43 6f  |t/./Users/adm/Co|
0000b7d0  64 65 2f 64 65 76 65 6c  6f 70 6d 65 6e 74 2f 46  |de/development/F|
0000b7e0  69 6e 53 70 79 56 32 2f  73 72 63 2f 69 4f 53 2f  |inSpyV2/src/iOS/|
0000b7f0  49 6e 73 74 61 6c 6c 65  72 2f 69 6e 73 74 61 6c  |Installer/instal|
0000b800  6c 5f 6d 61 6e 61 67 65  72 2f 69 6e 73 74 61 6c  |l_manager/instal|
0000b810  6c 5f 6d 61 6e 61 67 65  72 2f 6d 61 69 6e 2e 6d  |l_manager/main.m|
```

Further references to "FinSpy" were identified in the binary:

/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/main.m
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/zip/ioapi.c
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/zip/unzip.c
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/zip/crypt.h
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/zip/zip.c
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/zip/
ZipArchive.mm
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/../../../CoreTarget/
CoreTarget/GIFileOps.mm
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/../../../CoreTarget/
CoreTarget/GIFileOps+Zip.m
/Users/adm/Code/development/FinSpyV2/src/iOS/Installer/install_manager/install_manager/../../../CoreTarget/
CoreTarget/GIPath.mm

Additionally, it appears that a developer's certificate belonging to Martin Muench, who is described in The New York Times as Managing Director of Gamma International GmbH and head of the FinFisher product portfolio, is used:

```
0000ee00  0a 0c 0a 41 70 70 6c 65  20 49 6e 63 2e 31 2c 30  |...Apple Inc.1,0|
0000ee10  2a 06 03 55 04 0b 0c 23  41 70 70 6c 65 20 57 6f  |*..U...#Apple Wo|
0000ee20  72 6c 64 77 69 64 65 20  44 65 76 65 6c 6f 70 65  |rldwide Develope|
0000ee30  72 20 52 65 6c 61 74 69  6f 6e 73 31 44 30 42 06  |r Relations1D0B.|
0000ee40  03 55 04 03 0c 3b 41 70  70 6c 65 20 57 6f 72 6c  |.U...;Apple Worl|
0000ee50  64 77 69 64 65 20 44 65  76 65 6c 6f 70 65 72 20  |dwide Developer |
0000ee60  52 65 6c 61 74 69 6f 6e  73 20 43 65 72 74 69 66  |Relations Certif|
0000ee70  69 63 61 74 69 6f 6e 20  41 75 74 68 6f 72 69 74  |ication Authorit|
0000ee80  79 30 1e 17 0d 31 32 30  34 30 33 31 30 33 33 32  |y0...12040310332|
0000ee90  30 5a 17 0d 31 33 30 34  30 33 31 30 33 33 32 30  |0Z..130403103320|
0000eea0  5a 30 81 83 31 1a 30 18  06 0a 09 92 26 89 93 f2  |Z0..1.0.....&...|
0000eeb0  2c 64 01 01 0c 0a 39 43  48 35 39 4d 37 43 33 53  |,d....9CH59M7C3S|
0000eec0  31 2b 30 29 06 03 55 04  03 0c 22 69 50 68 6f 6e  |1+0)..U..."iPhon|
0000eed0  65 20 44 69 73 74 72 69  62 75 74 69 6f 6e 3a 20  |e Distribution: |
0000eee0  4d 61 72 74 69 6e 20 4d  75 65 6e 63 68 31 13 30  |Martin Muench1.0|
```

An ad-hoc distribution profile is present: "testapp":

UUID: "E0A4FAD7-E414-4F39-9DB3-5A845D5124BC".
Will expire on 02.04.2013.
The profile matches the bundle ID (home.install-manager).
The profile was signed by 3 certificates.
The profile may be used by one developer:
Developer Certificate "iPhone Distribution: Martin Muench".
This certificate was used to sign the bundle.

The code signature contains 3 certificates:

Certificate "Apple Root CA":
Will expire on 09.02.2035.
Your keychain contains this root certificate.
Certificate "Apple Worldwide Developer Relations Certification Authority":
Will expire on 14.02.2016.
Certificate "iPhone Distribution: Martin Muench":
Will expire on 03.04.2013.
SHA1 fingerprint: "1F921F276754ED8441D99FB0222A096A0B6E5C65".

The Application has been provisioned to run on the following devices, represented here by their Unique Device Identifiers (UDID):

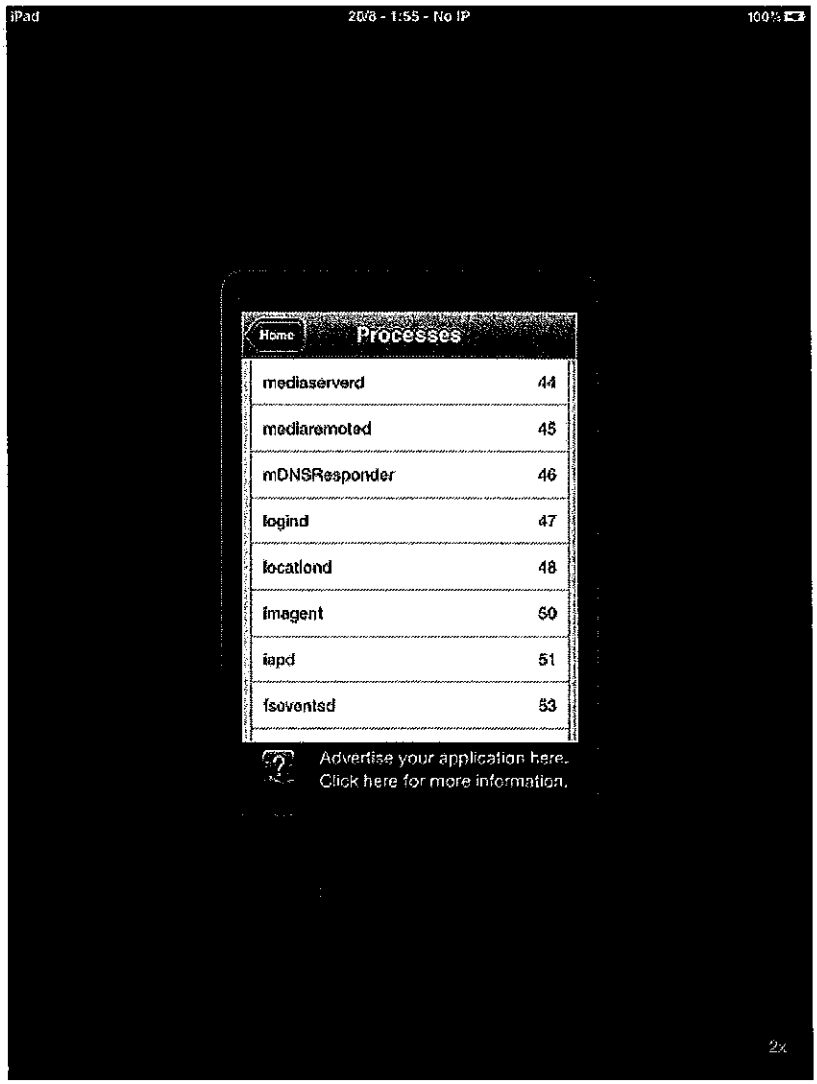
31b4f49bc9007f98b55df555b107cba841219a21,
73b94de27cb5841ff387078c175238d6abac44b2,
0b47179108f7ad5462ed386bc59520da8bfcea86,
320184fb96154522e6a7bd86dcd0c7a9805ce7c0,
11432945ee0b84c7b72e293cbe9acef48f900628,
5a3df0593f1b39b61e3c180f34b9682429f21b4f,
b5bfa7db6a0781827241901d6b67b9d4e5d5dce8

The file is hidden using Spring Board options, and on execution the sample writes out logind.app to /System/Library/CoreServices. 'logind' exists on OSX but not normally on iOS.
It then installs: /System/Library/LaunchDaemons/com.apple.logind.plist

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>Disabled</key>
      <false/>
      <key>Label</key>
      <string>home.logind</string>
      <key>OnDemand</key>
      <false/>
      <key>ProgramArguments</key>
      <array>
            <string>/System/Library/CoreServices/logind.app/logind</string>
            <string></string>
            <string></string>
      </array>
      <key>StandardErrorPath</key>
      <string>/dev/null</string>
</dict>
</plist>
```

This creates persistence on reboot. It launches the logind process, then deletes install_manager.app.

On reboot it runs early in the boot process with ID 47:



This then drops SyncData.app. This application is signed, and the provisioning stipulates:

> "Reliance on this certificate by any party assumes acceptance of the then applicable standard terms and conditions of use, certificate policy and certification practice statements."

Further legal analysis would be necessary to determine whether the program violated the terms of use at the time of its creation.

This application appears to provide functionality for call logging:

```
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget
/MobileLoggingDataTLV.m
_OBJC_METACLASS_$_MobileLoggingDataTLV
_OBJC_CLASS_$_MobileLoggingDataTLV
```

Exfiltration of contacts:

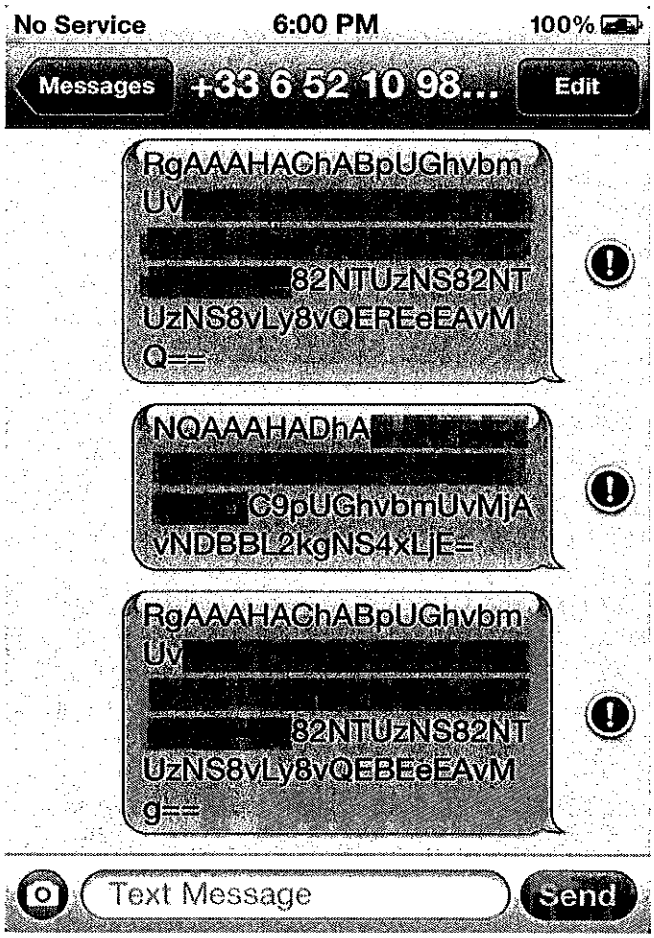
```
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget
/GIAddressBookModule.m
/Users/adm/Library/Developer/Xcode/DerivedData/CoreTarget-gqciilooqcckafgxlngvjezpbymr
/Build/Intermediates/CoreTarget.build/Release-iphoneos/SyncData.build/Objects-normal/armv7
/GIAddressBookModule.o
-[XXXVIII_cI getAddresses:]
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget
/GIAddressBookModuleData.m
```

Target location enumeration:

```
@_OBJC_CLASS_$_CLLocationManager
/Users/adm/Code/development/FinSpyV2/src/iOS/CoreTarget/CoreTarget/GILocationManager.m
/Users/adm/Library/Developer/Xcode/DerivedData/CoreTarget-gqciilooqcckafgxlngvjezpbymr
/Build/Intermediates/CoreTarget.build/Release-iphoneos/SyncData.build/Objects-normal/armv7
/GILocationManager.o
```

As well as arbitrary data exfiltration, SMS interception and more.

SyncData.app exfiltrates base64 encoded data about the device (including the IMEI, IMSI etc) to a remote cellular number.



The 'logind' process attempts to talk to a remote command and control server, the configuration information for which appears to be stored in base64 encoded form in "SyncData.app/84C.dat".

The _CodeSignature/CodeResources file suggests that install manager drops logind.app, SyncData.app and Trampoline.app (Trampoline.app has not been examined).

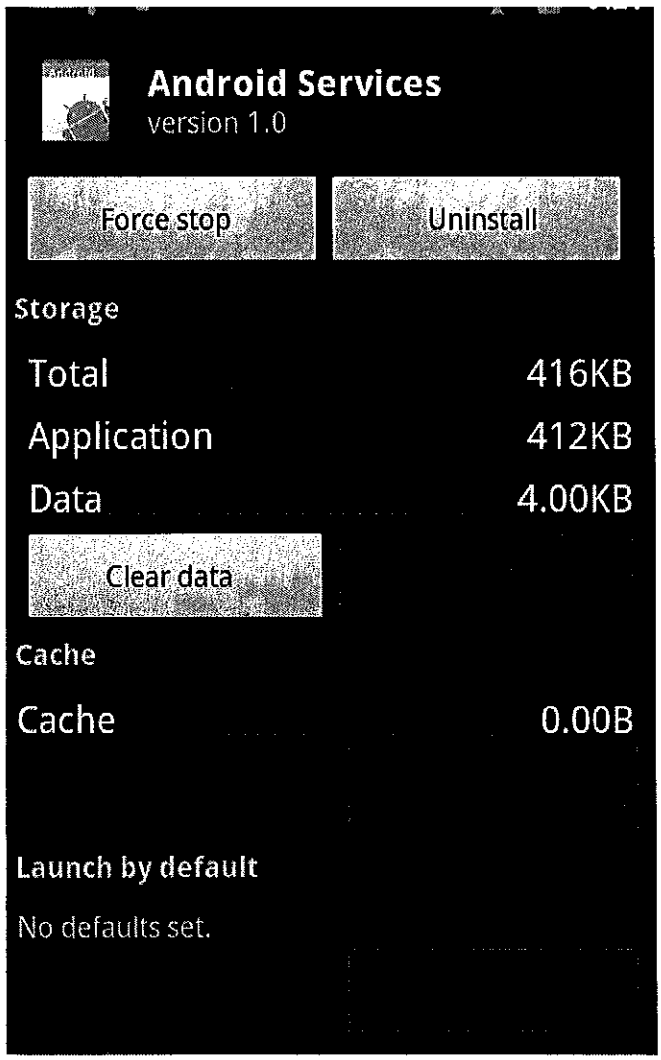
org.logind.ctp.archive/logind.app/logind
org.logind.ctp.archive/SyncData.app/SyncData
org.logind.ctp.archive/trampoline.app/trampoline

Android

The Android samples identified come in the form of APKs.

2e96e343ac10f5d9ace680e456c083e4eceb108f7209aa1e849f11a239e7a682
0d798ca0b2d0ea9bad251125973d8800ad3043e51d4cc6d0d57b971a97d3af2d
72a522d0d3dcd0dc026b02ab9535e87a9f5664bc5587fd33bb4a48094bce0537

The application appears to install itself as "Android Services":



It requests the following permissions:

```
android.permission.ACCESS_COARSE_LOCATION
android.permission.ACCESS_FINE_LOCATION
android.permission.INTERNET
android.permission.READ_PHONE_STATE
android.permission.ACCESS_NETWORK_STATE
android.permission.READ_CONTACTS
android.permission.READ_SMS
android.permission.SEND_SMS
android.permission.RECEIVE_SMS
android.permission.WRITE_SMS
android.permission.RECEIVE_MMS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.PROCESS_OUTGOING_CALLS
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.WAKE_LOCK
android.permission.CHANGE_WIFI_STATE
android.permission.MODIFY_PHONE_STATE
android.permission.BLUETOOTH
android.permission.RECEIVE_WAP_PUSH
```

The first 200 files in the apk are named "assets/Configurations/dummsX.dat", where X is a number from 0-199. The files are 0 bytes in length. The file header entries in the compressed file are normal, but the directory header entries contain configuration information.
The code in the my.api.Extractor.getConfiguration() method opens up the APK file and searches for directory entry headers (PK\x01\x02) then copies 6 bytes from the entry starting at offset 36. These are the "internal file attributes" and "external file attributes" fields. The code grabs these sequences until it hits a 0 value.This creates a base64 encoded string.

The app decodes this string and stores it in a file named 84c.dat (similar to the iOS sample discussed earlier).

Here's the output from one of the samples:

```
KQIAAJBb/gAhAgAAoDOEAAwAAABQE/4AAAAAABAAAABgV/
4AAAAAAAAAAAAMAAAAQBX+AAAAAAAPAAAAcFj+AG1qbV9BTkQMAAAAQGGEACwB
AAANAAAAkGSEAIKHhoGDJgAAAHA3gABkZW1vLWRlLmdhbW1hLWludGVybmF0aW9uYWwu
ZGUbAAAAcDeAAGZmLWRlbW8uYmxvZ2Rucy5vcmcMAAAAQDiAAFAAAAAMAAAAQDiAAF
cEAAAMAAAAQDiAAFgEAAAVAAAAcGOEACs0OTE3MjY2NTM4MDAWAAAAcGqEACs0OTg5
NTQ5OTg5OTA4DwAAAHBmhABtam1fQU5EDAAAAEBlhACmNqEPDAAAAEAh
/gAoBAAADAAAAEANgAB7AAAADAAAAEBohAAAAAAADAAAAEA7gAAAAAACgAAAJBghA
CtEAoAAACQYoQAwAAJAAAAsGeEAAAIAAAAkMZxAIwAAACQeYQAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAEBAQEAAQEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAPQAAAJA0RQA1AAAAoDNFAAwAA
ABAQUUA6AMAAAwAAABAQEUALAEAAAkAAAAwQkUAAAwAAACQZIQAh4aFgQ==
```

The Base64 decoded hexdump is:

```
00000000  29 02 00 00 90 5b fe 00  21 02 00 00 a0 33 84 00  |)....[..!....3..|
00000010  0c 00 00 00 50 13 fe 00  00 00 00 00 10 00 00 00  |....P...........|
00000020  60 57 fe 00 00 00 00 00  00 00 00 00 0c 00 00 00  |`W..............|
00000030  40 15 fe 00 00 00 00 00  0f 00 00 00 70 58 fe 00  |@...........pX..|
00000040  6d 6a 6d 5f 41 4e 44 0c  00 00 00 40 61 84 00 2c  |mjm_AND....@a..,|
00000050  01 00 00 0d 00 00 00 90  64 84 00 82 87 86 81 83  |........d.......|
00000060  26 00 00 00 70 37 80 00  64 65 6d 6f 2d 64 65 2e  |&...p7..demo-de.|
00000070  67 61 6d 6d 61 2d 69 6e  74 65 72 6e 61 74 69 6f  |gamma-internatio|
00000080  6e 61 6c 2e 64 65 1b 00  00 00 70 37 80 00 66 66  |nal.de....p7..ff|
00000090  2d 64 65 6d 6f 2e 62 6c  6f 67 64 6e 73 2e 6f 72  |-demo.blogdns.or|
000000a0  67 0c 00 00 00 40 38 80  00 50 00 00 00 0c 00 00  |g....@8..P......|
000000b0  00 40 38 80 00 57 04 00  00 0c 00 00 00 40 38 80  |.@8..W.......@8.|
000000c0  00 58 04 00 00 15 00 00  00 70 63 84 00 2b 34 39  |.X.......pc..+49|
000000d0  31 37 32 36 36 35 33 38  30 30 16 00 00 00 70 6a  |1726653800....pj|
000000e0  84 00 2b 34 39 38 39 35  34 39 39 38 39 39 30 38  |..+4989549989908|
000000f0  0f 80 00 00 70 66 84 00  6d 6a 6d 5f 41 4e 44 0c  |....pf..mjm_AND.|
00000100  00 00 00 40 65 84 00 a6  36 a1 0f 0c 00 00 00 40  |...@e...6......@|
00000110  21 fe 00 28 04 00 00 0c  00 00 00 40 0d 80 00 7b  |!..(.......@...{|
00000120  00 00 00 0c 00 00 00 40  68 84 00 00 00 00 00 0c  |.......@h.......|
00000130  00 00 00 40 3b 80 00 00  00 00 00 0a 00 00 00 90  |...@;...........|
00000140  60 84 00 ad 10 0a 00 00  00 90 62 84 00 c0 00 09  |`.........b.....|
00000150  00 00 00 b0 67 84 00 00  08 00 00 00 90 c6 71 00  |....g.........q.|
00000160  8c 00 00 00 90 79 84 00  00 00 00 00 00 00 00 00  |.....y..........|
00000170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

Note that the hostnames demo-de.gamma-international.de and ff-demo.blogdns.org are suggestive of a demo or pre-customization version of the FinSpy Mobile tool and are similar to domains identified in our previous report.

We identified samples structurally similar to this sample that spoke to servers in the **United Kingdom** and the **Czech Republic**:

Sample: 0d798ca0b2d0ea9bad251125973d8800ad3043e51d4cc6d0d57b971a97d3af2d
Command and Control: 212.56.102.38
Country: United Kingdom
Company: PlusNet Technologies

Sample: 2e96e343ac10f5d9ace680e456c083e4eceb108f7209aa1e849f11a239e7a682
Command and Control: 80.95.253.44
Country: Czech Republic
Company: T-Systems Czech Republic

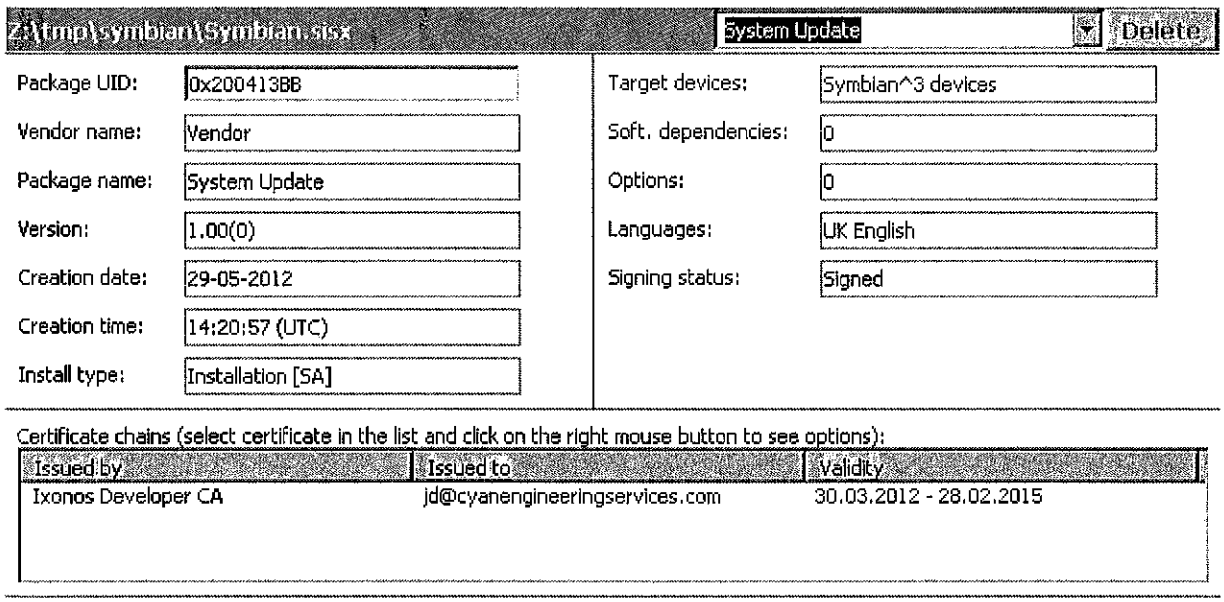
Note that the Czech sample speaks to the same command and control server previously identified by Rapid7.

Symbian

Samples for Nokia's Symbian platform were identified:

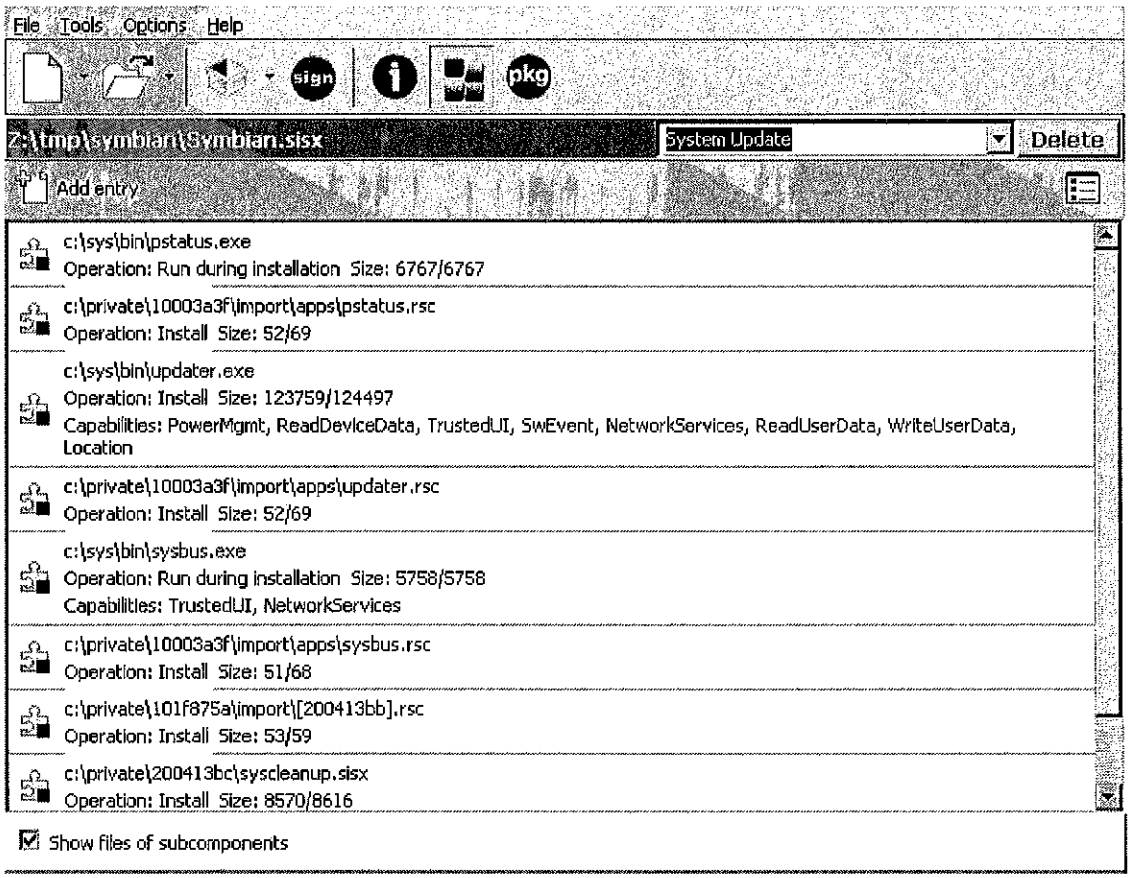
1e7e53b0d5fabcf12cd1bed4bd9ac561a3f4f6f8a8ddc5d1f3d2f3e2e9da0116
Symbian.sisx
eee80733f9664384d6bac4d4e27304748af9ee158d3c2987af5879ef83a59da0
mysym.sisx

The first sample ("Symbian.sisx") identifies itself as "System Update" and appears to have been built on the 29th of May 2012, at 14:20:57 UTC.



The certificate is registered to a jd@cyanengineeringservices.com. WHOIS information indicates that www.cyanengineeringservices.com was anonymously registered (date of first registration: 07-Mar-07) with GoDaddy using Domains By Proxy. Although it includes an attractive front page that states "Mobile Software Development" for "Windows Mobile, iPhone, Android, Symbian and Blackberry," all links (e.g. "Products" "About Us" or "Contacts") lead to an "under construction" blank page.

The sample contains the following components:



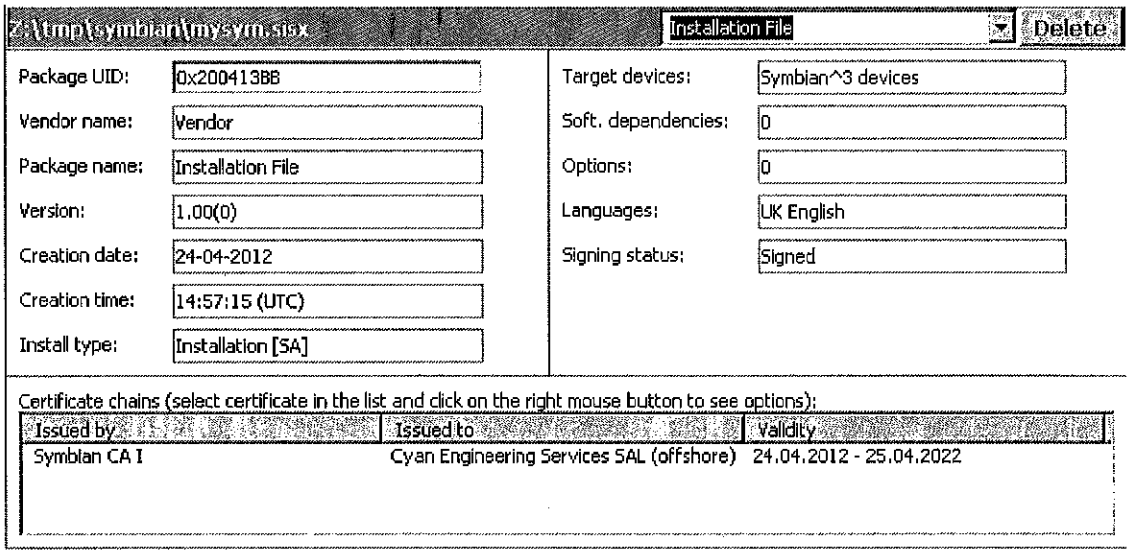
The file "c:\sys\bin\updater.exe" provides the main implant functionality. This requests the following capabilities[1]:

PowerMgmt
ReadDeviceData
TrustedUI
SwEvent
NetworkServices
ReadUserData
WriteUserData
Location

Of special note is the use of TrustedUI. As mentioned in the security section of the Nokia developer notes for Symbian:

> "Trusted UI dialogs are rare. They must be used only when confidentiality and security are critical: for instance for password dialogs. Normal access to the user interface and the screen does not require this."

The second sample ("mysym.sisx") identifies itself as "Installation File" and appears to be signed by the "Symbian CA I" for "Cyan Engineering Services SAL (offshore)," unlike the previous sample, which was registered to jd@cyanengineeringservices.com.



We identified "Cyan Engineering Services SAL (offshore)" as also listed as the registrant on the parked domain www.it-intrusion.com, (Created: 08-Dec-11, also with GoDaddy). However, **it-intrusion.com** does not have a protected registrant. The registrant is listed[2] as a company based in Beirut, Lebanon:

Cyan Engineering Services SAL (offshore)
Broadway Center, 7th Floor
Hamra Street – Chouran 1102-2050
Beirut, Beirut 00000
Lebanon
Domain Domain Name: IT-INTRUSION.COM
Created: 08-Dec-11
Expires: 08-Dec-13
Updated: 08-Dec-11
Administrative Contact: Debs, Johnny

The registrant information for Cyan Engineering Services SAL also connects to Gamma: the name "Johnny Debs" is associated with Gamma International: a Johnny Debs was listed as representing Gamma at the October 2011 Milpol in Paris, and the name occurs elsewhere in discussions of FinFisher.

Examination of this sample reveals the domain demo-01.gamma-international.de potentially indicating a demo or pre-customization copy.

```
00023170  00 82 87 86 81 83 26 00  00 00 70 37 80 00 64 65  |......&...p7..de|
00023180  6d 6f 2d 30 31 2e 67 61  6d 6d 61 2d 69 6e 74 65  |mo-01.gamma-inte|
00023190  72 6e 61 74 69 6f 6e 61  6c 2e 64 65 0c 00 00 00  |rnational.de....|
000231a0  40 38 80 00 57 04 00 00  0c 00 00 00 40 38 80 00  |@8..W.......@8..|
000231b0  58 04 00 00 0c 00 00 00  40 38 80 00 59 04 00 00  |X.......@8..Y...|
000231c0  15 00 00 00 70 63 84 00  2b 34 39 31 37 32 36 36  |....pc..+4917266|
000231d0  36 32 33 36 34 14 00 00  00 70 63 84 00 2b 36 30  |62364....pc..+60|
000231e0  31 32 33 38 33 39 38 39  37 16 00 00 00 70 6a 84  |123839897....pj.|
000231f0  00 2b 34 39 38 39 31 32  31 34 30 35 38 36 35 16  |.+4989121405865.|
00023200  00 00 00 70 6a 84 00 2b  34 39 38 39 31 32 31 34  |...pj..+49891214|
00023210  30 35 38 36 36 0d 00 00  00 70 66 84 00 6d 79 73  |05866....pf..mys|
```

The phone number +60123839897 also shows up in the sample. It has a Malaysian country code.

Blackberry

The identified samples contained the following files:

rlc_channel_mode_updater.cod
rlc_channel_mode_updater-1.cod
rlc_channel_mode_updater.jad

The .cod files are signed by RIM's RBB, RCR, and RRT keys. RBB stands for "RIM BlackBerry Apps API," which allows manipulation of BlackBerry apps, RCR stands for "RIM Crypto API," which allows access to crypto libraries, and RRT stands for "RIM Runtime API," which allows access to other phone functionality such as sending SMS messages.
The signature process is described in RIM's documentation [pdf] about the Blackberry Signing Authority. First, a developer registers a public key with the Blackberry Signing Authority. In order to obtain a signed application, the developer submits a signature request (including his identity and a hash of the binary) signed with his private key to the Signing Authority. The Signing Authority verifies that the signer is authorized to

make requests, and, if so, replies with a copy of the hash signed with the relevant RIM private key. The developer then appends the signature to his binary.

```
00016d80  01 00 00 00 00 00 00 00  01 00 84 00 52 52 54 00  |............RRT.|
00016d90  2e 3f b4 0d 42 70 6d d1  07 dc 6b a5 89 0b 12 37  |.?..Bpm...k....7|
00016da0  46 c1 7a 83 46 5c 86 ba  ca 8e 8d 13 66 70 f3 5a  |F.z.F\......fp.Z|
00016db0  82 37 da aa b2 a0 17 44  a6 1f 1b 07 6b 71 ff 5b  |.7.....D....kq.[|
00016dc0  9e 41 c6 17 30 3d dc ee  5f 3a 0c 6b a6 db 20 8d  |.A..0=.._:.k.. .|
00016dd0  fd d9 f7 1d ba 00 33 db  da 4a 70 75 47 d9 f9 17  |......3..JpuG...|
00016de0  95 eb af 50 7a f2 56 16  4b 10 c4 90 db e3 8f ca  |...Pz.V.K.......|
00016df0  a4 aa 62 dd 39 c2 9e 7e  19 73 ba c8 b4 6c 95 48  |..b.9..~.s...l.H|
00016e00  57 17 d7 f3 1d 63 e7 df  c3 0c 8a 19 d6 80 e4 c5  |W....c..........|
00016e10  01 00 84 00 52 42 42 00  73 fe 79 c8 23 5f 95 12  |....RBB.s.y.#_..|
00016e20  ad 88 0e c4 e5 8c a9 df  ee 60 b1 94 d5 bb 01 86  |.........`......|
00016e30  dd c2 61 c2 6f e0 ed 41  b7 76 99 ef 04 b8 e6 ef  |..a.o..A.v......|
00016e40  7a 91 93 1d f6 dd 2b 42  9e ea a8 c0 61 64 4b 32  |z.....+B....adK2|
00016e50  34 96 fd fc f0 aa 04 04  64 ef d8 77 40 35 2d 00  |4.......d..w@5-.|
00016e60  a8 f5 c2 69 e0 a1 28 45  f3 2c 06 61 ab 2b dc 46  |...i..(E.,.a.+.F|
00016e70  ec 3e 23 8b b4 c8 58 62  f8 64 09 79 b8 a7 a9 6e  |.>#...Xb.d.y...n|
00016e80  7f a1 79 22 48 5d c8 3c  85 2c fb a6 60 52 76 66  |..y"H].<.,..`Rvf|
00016e90  83 c5 a4 d4 27 e1 9b 0d  01 00 84 00 52 43 52 00  |....'.......RCR.|
00016ea0  6c 95 30 18 31 28 6c eb  5f e6 61 b7 2c 2c bb ce  |l.0.1(l._.a.,,..|
00016eb0  44 39 58 40 0d 9a 0c 8b  77 f0 72 0c 5f 5e b1 8c  |D9X@....w.r._^..|
00016ec0  ca 2a ba f9 26 3c 44 6a  f6 7c 93 fb 84 35 e1 1d  |.*..&<Dj.|...5..|
00016ed0  74 6d 9b 34 fd 58 a9 48  ea 88 f8 bb 4b 9d cb 2c  |tm.4.X.H....K..,|
00016ee0  19 36 71 1d 17 ca c6 a5  ab 44 93 e5 6a b7 d3 a6  |.6q......D..j...|
00016ef0  89 f1 0f 45 00 d1 9c 01  b2 d6 77 df d7 b4 c4 f5  |...E......w.....|
00016f00  05 2a 75 91 d7 1f 17 0e  be 37 ab c0 16 e3 2d d8  |.*u......7....-.|
00016f10  62 fe c6 a8 9c 3f 41 7c  8e 10 3c e5 2b 83 c9 23  |b....?A|..<.+..#|
```

The .jad file contains the following hashes for the .cod files:

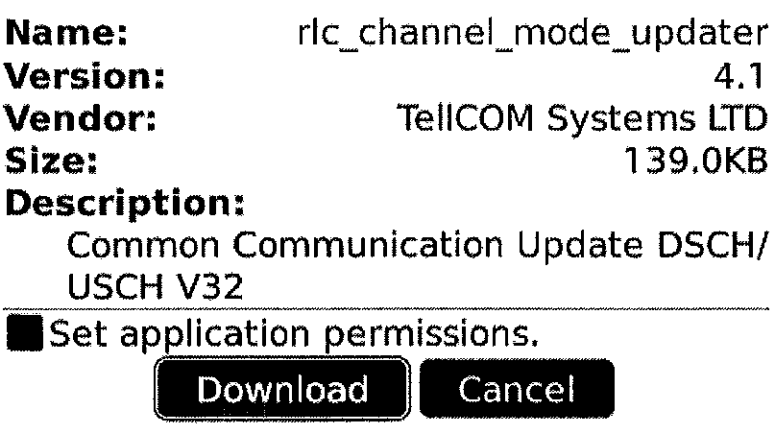
RIM-COD-SHA1-1: 2d 0a a2 b3 54 97 f7 35 fb 40 77 8e e1 ca 7f 8f 3e a0 aa 04
RIM-COD-SHA1: 0f 3b d8 d1 84 da 35 4e 10 94 89 c0 d6 08 70 ad 5e 7a f3 e0

The .jad file also contains a blob of base64 encoded data with the key "RIM-COD-Config." This data contains the URL of the command & control server, TCP ports, phone numbers to exfiltrate data to via SMS, identifiers for the Trojan and target, active modules, and various other configuration parameters.

Decoding this reveals the following servers and phone numbers:

118.97.89.186 – **Indonesia**
+6281310781704 – **Indonesia**
+49456456456 – **Germany**

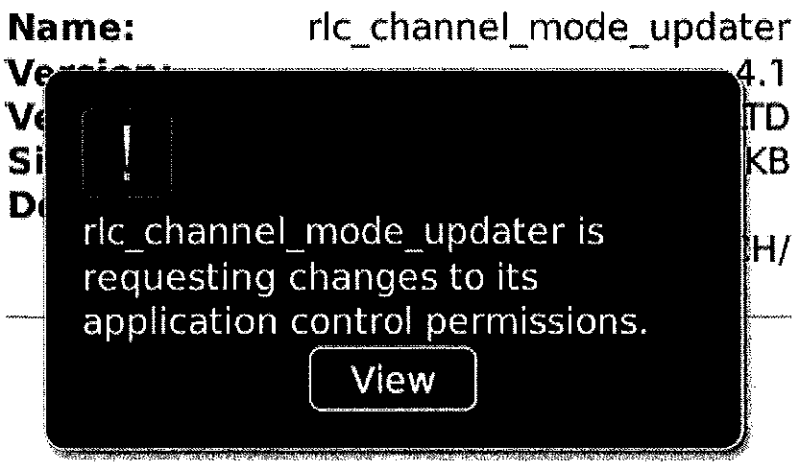
Upon installation, the user is presented with the following screen:



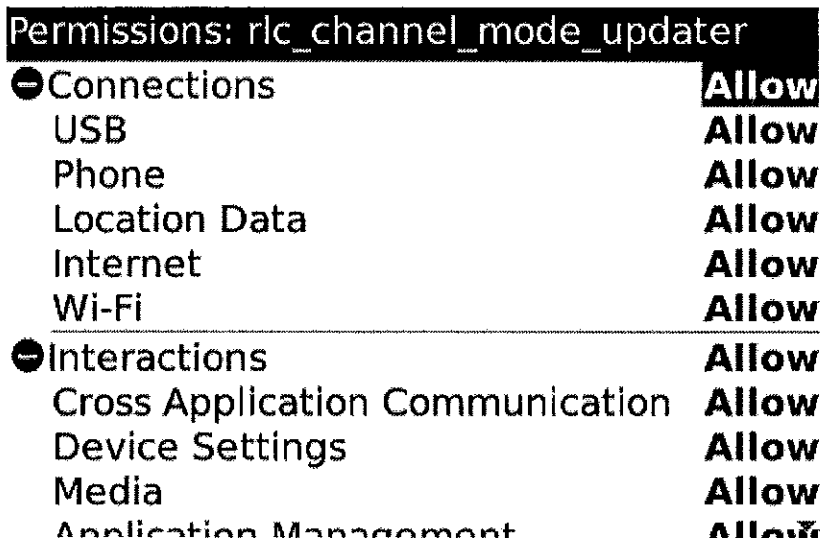
As evidenced by the above screenshot, the app is listed as:

TellCOM Systems LTD Common Communication Update DSCH/USCH V32

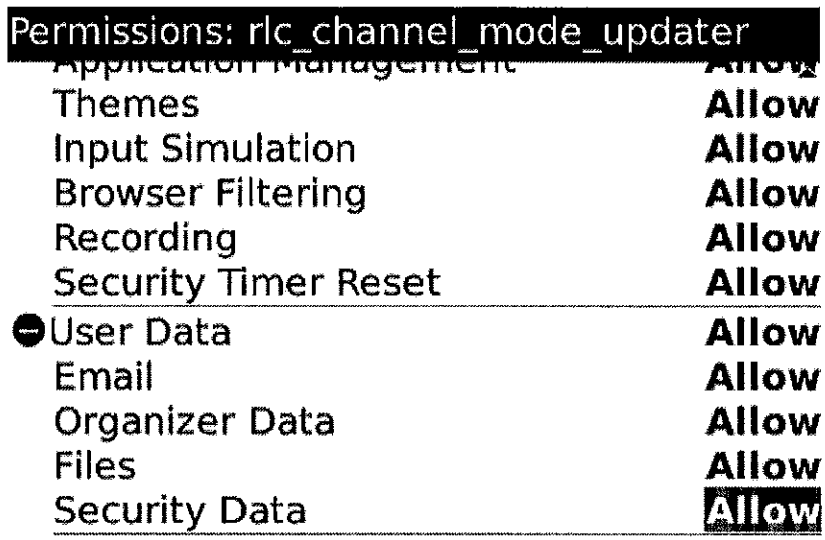
Directly after installing, the application requests enhanced permissions:



The following screen pops up showing the requested permissions:



Scrolling down reveals:



After the user accepts these permissions, the sample attempts to connect to both Internet-based and SMS-based command & control servers. Another sample we analyzed appeared to write a debug log to the device's filesystem. The following information was observed written to the log regarding communication with command & control services.

net.rmi.device.api.fsmbb.phone.PhoneInterface – connecting to http://demo-01.gamma-international.de:1111/ping/XXXXXXXXXXXX;deviceside=true failed: net.rim.device.cldc.io.dns.DNSException: DNS error DNS error

net.rmi.device.api.fsmbb.core.com.protocol.HeartbeatProtocolSMS – Heartbeat type 11 (1346097705922)+ core hb content: XXXXX/123456783648138/666666553648138/12e/666/0/0///

net.rmi.device.api.fsmbb.core.com.SMSCommunication – 1346097743 Success: texting to: //+XXXXXXXXXX msg: XXXXX

net.rmi.device.api.fsmbb.core.com.protocol.HeartbeatProtocolSMS – Heartbeat type 11 (1346097705922)+ extended hb content: XXXXX/123456783648138/XXXXX/999/420/B9700 5.0.

net.rmi.device.api.fsmbb.core.com.SMSCommunication – 1346097743 Success: texting to: //+XXXXXXXXXX msg: XXXXX

We decompiled the Blackberry sample. We provide a high-level overview of the more interesting classes that we successfully decompiled:

net.rmi.device.api.fsmbb.config.ApnDatabase
net.rmi.device.api.fsmbb.config.ApnDatabase$APN

These appeared to contain a database comprising the following GSM APNs. The significance of this database is that it only includes a small set of countries and providers:

Germany: web.vodafone.de, internet.t-mobile
Indonesia: indosatgprs, AXIS, telkomsel, www.xlgprs.net, 3gprs
Brazil: claro.com.br, wapgprs.oi.com.br, tim.br
Mexico: wap.telcel.com

net.rmi.device.api.fsmbb.core.AppMain

This appears to do the main app installation, as well as uninstallation. Installation includes negotiating for enhanced permissions, base64-decoding the "RIM-COD-Config" configuration, and setting up and installing the Configuration. If the configuration contains a "removal date," then automatic removal is scheduled for this time. Installation also involves instantiating "listener" modules, as specified below:

net.rmi.device.api.fsmbb.core.listener.AddressBookObserver

This appears to listen for changes to the address book. It implements the net.rim.blackberry.api.pim.PIMListListener interface.

net.rmi.device.api.fsmbb.core.listener.CallObserver.*

This implements:

net.rim.blackberry.api.phone.PhoneListener
net.rim.blackberry.api.phone.phonelogs.PhoneLogListener
net.rim.device.api.system.KeyListener

This module logs and manipulates phone events, and appears to enable "remote listening" functionality, where the FinSpy Master can silently call an infected phone to listen to conversation in its vicinity (this is referred to as a SpyCall in the code). The module has a facility to hide incoming calls by manipulating the UI, cancelling buzzer and vibration alerts, and toggling the backlight. Upon instantiation, the module calls "*43#" to enable call waiting. If a remote listening call from the master is active, then legitimate incoming calls will trigger call waiting. The module detects these legitimate incoming calls, and places the SpyCall call on call waiting, presenting the legitimate incoming call to the user.

net.rmi.device.api.fsmbb.core.listener.EmailObserver

This appears to record sent and received email messages.

net.rmi.device.api.fsmbb.core.listener.MessengerObserver (Module #68)

This seems to record BBM messages. It appears to do this by periodically checking the path "file:///store/home/user/im/BlackBerry Messenger/"

net.rmi.device.api.fsmbb.core.listener.SMSObserver

This module implements:

net.rim.blackberry.api.sms.SendListener
net.rim.blackberry.api.sms.OutboundMessageListener

Contrary to its name, OutboundMessageListener allows listening for both incoming and outgoing SMS messages. This module also checks for incoming SMS commands from the FinSpy Master. These commands can include an "emergency configuration" update, that can include new addresses and phone numbers for the FinSpy Master.

net.rmi.device.api.fsmbb.core.listener.WAObserver (Module #82)

This appears to monitor WhatsApp, the popular proprietary cross-platform messaging application. It locates the WhatsApp process ID by searching for module names that contain the string "WhatsApp."

At some point, the module calls getForegroundProcessId to see if the WhatsApp process ID is in the foreground. If so, it seems to take a screenshot of the WhatsApp application, via Display.Screenshot. It appears that this screenshot is checked via ".equals" to see if there is any new information on the WhatsApp screen. If there is new information, the screenshot is then JPEG encoded via JPEGEncodedImage.encode.

net.rmi.device.api.fsmbb.core.com.*

Appears to contain the mechanics of communication with the command & control server, including the plaintext TLV-based wire protocol.

Windows Mobile

The Windows Mobile samples we identified are:

2ccbfed8f05e6b50bc739c86ce4789030c6bc9e09c88b7c9d41cbcbde52a2455
507e6397e1f500497541b6958c483f8e8b88190407b307e997a4decd5eb0cd3a
1ff1867c1a55cf6247f1fb7f83277172c443442d174f0610a2dc062c3a873778

All the samples appeared similar, most likely belonging to the same branch release. The relevant parts of the binary are stored in five different resources:

- The first resource contains an OMA Client Provisioning XML file, which is used to store root certificates for running privileged/unprivileged code on the device. In this case it only contained some default example values shipped with Microsoft Windows Mobile SDK.

- The second resource contains the actual dropped payload which contains all the Trojan functionalities.
- The third resource contains a binary configuration file.
- The fourth and fifth resources contain two additional DLL files which are dropped along with the payload.

The main implant is dropped as "services.exe" with the libraries dropped as mapiwinarm.dll and mswservice.dll.

The payload has the following attributes:

File size: 186640 bytes
SHA256:
4b99053bc7965262e8238de125397d95eb7aac5137696c7044c2f07b175b5e7c

This is a multi-threaded and modular engine which is able to run and coordinate a series of events providing interception and monitoring capabilities. When the application starts, a core initialization function is invoked, responsible for preparing execution and launching the main thread.

The main thread consequently runs a set of core components on multiple threads:

- Routines responsible for handling the "heartbeat" notifications.
- Routines which control the execution of the Trojan and its components while monitoring the status of the device.
- A routine which can be used to "wake up" the device.
- A component which handles emergency SMS communications.
- A routine that initializes the use of the Radio Interface Layer.
- A core component that manages a set of surveillance modules.

The Trojan utilises a "Heartbeat Manager", which is a set of functions and routines that, depending on the status of the device or monitored events, communicates notifications back to the command and control server.

These beacons are sent according the following events:

- First beacon.
- A specified time interval elapsing.
- The device has low memory.
- The device has low battery.

- The device changed physical location.
- The Trojan has recorded data available.
- The device has connected to a cellular network.
- The device has a data link available.
- The device connects to a WiFi network.
- An incoming / outgoing call starts.
- The Mobile Country Code (MCC) or Mobile Network Code (MNC) ID changed.
- The Trojan is being uninstalled.
- The SIM changes.

Notifications are sent via SMS, 3G and WiFi, according to availability. Consistent with other platforms, the windows mobile version appears to use base64 encoding for all communications.

In response to such notifications, the implant is able to receive and process commands such as:

```
STOP_TRACKING_CMD
START_TRACKING_CMD
RESEND_FIRST_HEARTBEAT_TCPIP_CMD
RESEND_FIRST_HEARTBEAT_SMS_CMD
REMOVE_LICENSE_INFO_CMD
KEEP_CONNECTION_ALIVE_CMD IGNORED b/c it's an SMS answer
KEEP_CONNECTION_ALIVE_CMD
REMOVE_AT_AGENT_REQUEST_CMD
REMOVE_AT_MASTER_REQUEST_CMD
REMOVE_MAX_INFECTION_REACHED_CMD
```

The command and control server is defined in the configuration file found in the third resource of the dropper. In this sample, the sample connected to the domain: **demo-04.gamma-international.de**
This suggests that such sample is either a demo version or "unpackaged" version ready to be customized.

Together with a DNS or IP command and control server, each sample appears to be provided with two phone numbers which are used for SMS notifications.

The core surveillance and offensive capabilities of the Trojan are implemented through the use of several different modules. These modules are initialized by a routine we called ModulesManager, which loads and launches them in separate threads:

```
LDR     R3, =aTryToLoadModul ; "try to load module: %02X"
MOV     R1, #0
LDR     R2, =aModuleManageme ; "module-management:FxLoadModule"
MOV     R0, R6
STR     R4, [SP,#0x28+var_28]
BL      FinSpy_Log
ADD     R7, R6, R4,LSL#2
LDR     R3, [R7,#0x110]
CMP     R3, #0
MOVNE   R3, #0
STRNE   R3, [R11,#var_24]
BNE     loc_20FE4
CMP     R4, #0x40
BEQ     FinSpy_MM_StartSpyCall
CMP     R4, #0x41
BEQ     FinSpy_MM_StartCallIntercept
CMP     R4, #0x42
BEQ     FinSpy_MM_StartSMS
CMP     R4, #0x43
BEQ     FinSpy_MM_StartLoader
CMP     R4, #0x45
BEQ     FinSpy_MM_StartTracking
CMP     R4, #0x46
BEQ     FinSpy_MM_StartCallLogs
CMP     R4, #0x60
BEQ     loc_20F30
LDR     R3, =aModule02xDoesn ; "module '%02X' doesn't exist"
LDR     R2, =aModuleManageme ; "module-management:FxLoadModule"
MOV     R1, #1
MOV     R0, R6
STR     R4, [SP,#0x28+var_28]
BL      FinSpy_Log
```

There are multiple modules available, including:

- AddressBook: Providing exfiltration of details from contacts stored in the local address book.
- CallInterception: Used to intercept voice calls, record them and store them for later transmission.
- PhoneCallLog: Exfiltrates information on all performed, received and missed calls stored in a local log file.
- SMS: Records all incoming and outgoing SMS messages and stores them for later transmission.
- Tracking: Tracks the GPS locations of the device.

Call Interception

In order to manipulate phone calls, the Trojan makes use of the functions provided by RIL.dll, the Radio Interface Layer.

Some of the functions imported and used can be observed below:

```
LDR     R1, =aRil_getcallwai ; "RIL_GetCallWaitingSettings"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0x6C]
BL      GetProcAddressW
LDR     R1, =aRil_setcallwai ; "RIL_SetCallWaitingStatus"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0x10C]
BL      GetProcAddressW
LDR     R1, =aRil_answer ; "RIL_Answer"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0xAC]
BL      GetProcAddressW
LDR     R1, =aRil_managecall ; "RIL_ManageCalls"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0x118]
BL      GetProcAddressW
LDR     R1, =aRil_getcalllis ; "RIL_GetCallList"
MOV     R3, R0
LDR     R0, [R7,#0x14]  ; hModule
STR     R3, [R7,#0xE0]
BL      GetProcAddressW
```

PhoneCallLog

In order to exfiltrate call logs, the Trojan uses functions provided by the Windows Mobile Phone Library.

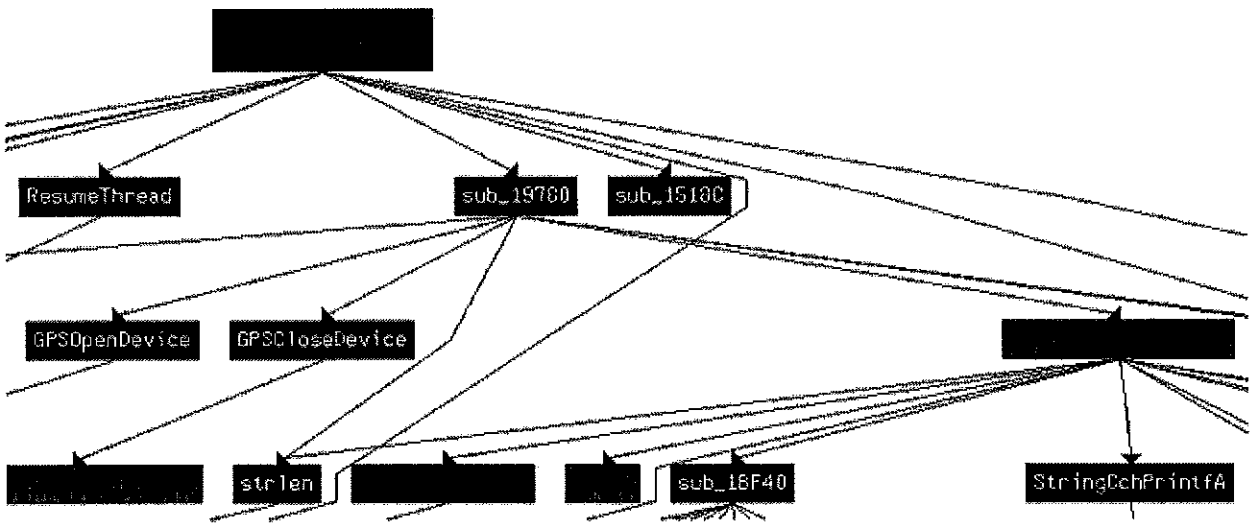
Using PhoneOpenCallLog() and PhoneGetCallLogEntry(), the implant is able to retrieve the following struct for each call being registered by the system:

```
typedef struct {
DWORD cbSize;
FILETIME ftStartTime;
FILETIME ftEndTime;
IOM iom;
BOOL fOutgoing:1;
BOOL fConnected:1;
BOOL fEnded:1;
BOOL fRoam:1;
CALLERIDTYPE cidt;
PTSTR pszNumber;
PTSTR pszName;
PTSTR pszNameType;
PTSTR pszNote;
DWORD dwLogFlags;
CEIOD iodContact;
CEPROPID pidProp;
} CALLLOGENTRY, * PCALLLOGENTRY;
```

This contains timestamps, numbers, names and other data associated with a call.

Tracking

The physical tracking of the device uses the GPS Intermediate Driver functions available on the Windows Mobile/CE platform:



After a successful GPSOpenDevice() call, it invokes GPSGetPosition() which gives access to a GPS_POSITION struct containing the following information:

```
typedef struct _GPS_POSITION {
DWORD dwVersion;
DWORD dwSize;
DWORD dwValidFields;
DWORD dwFlags;
SYSTEMTIME stUTCTime;
double dblLatitude;
double dblLongitude;
float flSpeed;
float flHeading;
double dblMagneticVariation;
float flAltitudeWRTSeaLevel;
float flAltitudeWRTEllipsoid;
GPS_FIX_QUALITY FixQuality;
GPS_FIX_TYPE FixType;
GPS_FIX_SELECTION SelectionType;
float flPositionDilutionOfPrecision;
float flHorizontalDilutionOfPrecision;
float flVerticalDilutionOfPrecision;
DWORD dwSatelliteCount;
DWORD rgdwSatellitesUsedPRNs[GPS_MAX_SATELLITES];
DWORD dwSatellitesInView;
DWORD rgdwSatellitesInViewPRNs[GPS_MAX_SATELLITES];
DWORD rgdwSatellitesInViewElevation[GPS_MAX_SATELLITES];
DWORD rgdwSatellitesInViewAzimuth[GPS_MAX_SATELLITES];
DWORD rgdwSatellitesInViewSignalToNoiseRatio[GPS_MAX_SATELLITES];
} GPS_POSITION, *PGPS_POSITION;
```

This provides the latitude and longitude of the current location of the device.

COMMAND AND CONTROL SERVER SCANNING RESULTS

Following up on our earlier analysis, we scanned IP addresses in several countries looking for FinSpy command & control servers. At a high level, our scans probed IP addresses in each country, and attempted to perform the handshake distinctive to the FinSpy command and control protocol. If a server responded to the handshake, we marked it as a FinSpy node. We expect to release our scanning tools with a more complete description of methodology in a follow-up blog post.

Our scanning yielded two key findings. First, we have identified several more countries where FinSpy Command and Control servers were operating. Scanning has thus far revealed two servers in **Brunei**, one in **Turkmenistan**'s Ministry of Communications, two in **Singapore**, one in the **Netherlands**, a new server in **Indonesia**, and a new server in **Bahrain**.

Second, we have been able to partially replicate the conclusions of an analysis by Rapid7, which reported finding FinSpy command & control servers in ten countries: Indonesia, Australia, Qatar, Ethiopia, Czech Republic, Estonia, USA, Mongolia, Latvia, and the UAE. We were able to confirm the presence of FinSpy on all of the servers reported by Rapid7 that were still available to be scanned. We confirmed FinSpy servers in **Indonesia, Ethiopia, USA, Mongolia**, and the UAE. The remaining servers were down at scanning time. We also noted that the server in the USA appeared to be an IP-layer proxy (e.g., in the style of Network Address Translation)[3].

Rapid7's work exploited a temporary anomaly in FinSpy command & control servers. Researchers at Rapid7 noticed that the command & control server in Bahrain responded to HTTP requests with the string "Hallo Steffi." This behavior did not seem to be active on Bahrain's server prior to the release of our analysis. Rapid7 looked at historical scanning information, and noticed that servers in ten other countries had responded to HTTP requests with "Hallo Steffi" at various times over the previous month. While the meaning of this string and the reason for the temporary anomaly are unknown, a possible explanation is that this was a testing deployment of a server update, and the "Hallo Steffi" message indicated successful receipt of the update. After the publication of Rapid7's analysis, the behavior began to disappear from FinSpy servers.

DETAILS OF OBSERVED SERVERS

Table 1: New Servers

Country	IP	Ports	Owner
Singapore	203.175.168.2	21, 53, 443, 4111	HostSG
Singapore	203.211.137.105	21, 53, 80, 443, 4111	Simple Solution System Pte Ltd
Bahrain	89.148.15.15	22, 53, 80, 443, 4111	Batelco
Turkmenistan	217.174.229.82	22, 53, 80, 443, 4111, 9111	Ministry of Communications
Brunei	119.160.172.187	21	Telekom Brunei
Brunei	119.160.128.219	4111, 9111	Telekom Brunei
Indonesia	112.78.143.34	22, 53, 80, 443, 9111	Biznet ISP
Netherlands	164.138.28.2	80, 1111	Tilaa VPS Hosting

Table 2: Confirmed Rapid7 Servers

Country	IP	Ports	Owner
USA	54.248.2.220	80	Amazon EC2
Indonesia	112.78.143.26	22, 25, 53, 80, 443, 4111	Biznet ISP
Ethiopia	213.55.99.74	22, 53, 80, 443, 4111, 9111	Ethio Telecom
Mongolia	202.179.31.227	53, 80, 443	Mongolia Telecom
UAE	86.97.255.50	21, 22, 53, 443, 4111	Emirates Telecommunications Corporation

It is interesting to note that the USA server on EC2 appeared to be an IP-layer proxy. This judgment was made on the basis of response time comparisons[4].

CONCLUSIONS AND RECOMMENDATONS

The analysis we have provided here is a continuation of our efforts to analyze what appear to be parts of the FinFisher product portfolio. We found evidence of the functionality that was specified in the FinFisher promotional materials. The tools and company names (e.g. Cyan Engineering Services SAL) found in their certificates also suggest interesting avenues for future research.

These tools provide substantial surveillance functionality; however, we'd like to highlight that, without exploitation of the underlying platforms, all of the samples we've described require some form of interaction to install. As with the previously analyzed FinSpy tool this might involve some form of socially engineered e-mail or other delivery, prompting unsuspecting users to execute the program. Or, it might involve covert or coercive physical installation of the tool, or use of a user's credentials to perform a third-party installation.

We recommend that all users run Anti-Virus software, promptly apply (legitimate) updates when they become available, use screen locks, passwords and device encryption (when available). Do not run untrusted applications and do not allow third parties access to mobile devices.

As part of our ongoing research, we have notified vendors, as well as members of the AV community.

ACKNOWLEDGEMENTS

This is a Morgan Marquis-Boire and Bill Marczak production.
Windows mobile sample analysis by Claudio Guarnieri.

Additional Analysis
Thanks to Pepi Zadowsky for OSX expertise and assistance.
Thanks to Jon Larimer and Sebastian Porst for Android expertise.

Additional Thanks
Special thanks to John Scott-Railton.
Additional thanks to Marcia Hofmann and the Electronic Frontier Foundation.
Tip of the hat to John Adams for scanning advice.

ABOUT MORGAN MARQUIS-BOIRE

Morgan Marquis-Boire is a Technical Advisor at the Citizen Lab, Munk School of Global Affairs, University of Toronto. He works as a Security Engineer at Google specializing in Incident Response, Forensics and Malware Analysis.

ABOUT BILL MARCZAK

Bill Marczak is a computer science Ph.D student at UC Berkeley. He is a founding member of Bahrain Watch, a monitoring and advocacy group that seeks to promote effective, accountable, and transparent governance in Bahrain through research and evidence-based activism.

ABOUT CLAUDIO GUARNIERI

Claudio Guarnieri is a Security Researcher at Rapid7. He's daily involved with general Internet badness and his specialties span from malware analysis to botnets tracking and cybercrime intelligence. He's a core member of The Honeynet Project and The Shadowserver Foundation, two no-profit organizations devoted to making Internet a safer place.

FOOTNOTES

[1] A list of Nokia capabilities can be found here.
[2] http://www.whoisentry.com/domain/it-intrusion.com
[3] See Appendix A.
[4] See Appendix A.

APPENDIX A

The server was serving FinSpy on port 80, and SSH on port 22. We measured the SYN/ACK RTT on both ports and compared. The results for port 80:

```
hping -S -p 80 54.248.2.220
HPING 54.248.2.220 (wlan0 54.248.2.220): S set, 40 headers + 0 data bytes
len=44 ip=54.248.2.220 ttl=24 DF id=0 sport=80 flags=SA seq=0 win=5840 rtt=1510.2 ms
len=44 ip=54.248.2.220 ttl=23 DF id=0 sport=80 flags=SA seq=1 win=5840 rtt=740.4 ms
len=44 ip=54.248.2.220 ttl=25 DF id=0 sport=80 flags=SA seq=2 win=5840 rtt=753.4 ms
len=44 ip=54.248.2.220 ttl=24 DF id=0 sport=80 flags=SA seq=3 win=5840 rtt=1001.6 ms
```

The results for port 22:

```
hping -S -p 22 54.248.2.220
HPING 54.248.2.220 (wlan0 54.248.2.220): S set, 40 headers + 0 data bytes
len=44 ip=54.248.2.220 ttl=49 DF id=0 sport=22 flags=SA seq=0 win=5840 rtt=125.7 ms
len=44 ip=54.248.2.220 ttl=49 DF id=0 sport=22 flags=SA seq=1 win=5840 rtt=124.3 ms
len=44 ip=54.248.2.220 ttl=49 DF id=0 sport=22 flags=SA seq=2 win=5840 rtt=123.3 ms
len=44 ip=54.248.2.220 ttl=50 DF id=0 sport=22 flags=SA seq=3 win=5840 rtt=127.2 ms
```

The comparison reveals that port 80 TCP traffic was likely being proxied to a different computer.

Information Security



Analysis of the FinFisher Lawful Interception Malware

Posted by Claudio Guarnieri in Information Security on 08-Aug-2012 06:31:35

It's all over the news once again: **lawful interception malware** discovered in the wild being used by government organizations for intelligence and surveillance activities. We saw it last year when the Chaos Computer Club unveiled a trojan being used by the federal government in Germany, WikiLeaks released a collection of related documents in the Spy Files, we read about an alleged offer from Gamma Group to provide the toolkit FinFisher to the Egyptian government, and we are reading once again now with the same one being delivered to human rights activists in Bahrain along with some spearphishing attacks.

We all are very aware of a rising market of Western companies developing and selling malware for the use of government organizations all around the world, but whenever one of these products is found in other geographical areas, the potential political and ethical implications tend to generate interest.

While I'm trying to provide context for the analysis below, it's not in the scope of this article to digress into the political context of the incident. We are security practitioners interested in technology and when dealing with malware, which in this case can be easily prone to abuses, we want to understand what they do, what's the spread and how we can respond.

The Incident

Several Bahrain activists located both in US and Bahrain started receiving emails with suspicious attachments:



They promptly understood there was something shady with them and forwarded them to journalists from Bloomberg who provided the attachments to some researchers, ending up in a thorough analysis of the files.

The emails were sent by the following addresses:

- melissa.aljazeera [at] gmail.com
- freedombhrtoday [at] gmail.com
- mkhalil1975 [at] gmail.com

With the following subjects:

- Existence of a new dialogue - Al-Wefaq & Government authority
- Torture reports on Nabeel Rajab
- King Hamad planning
- Breaking News from Bahrain – 5 Suspects Arrested

Each of these emails contained an archive, following are the ones identified so far:

- *_gpj.Arrested Suspects.rar*
- *King hamad on official visit to .rar*
- *Meeting Agenda.rar*
- *Rajab.rar*

Each of these archives contained several files, including Word documents, images as well as several Windows executables:

- *dialoge.exe* (MD5: ee5b03b5990dc310b77aac1d32da68de)
- *gpj.1egami.exe* (MD5: e82647e42868e0ff0b6357fcf0f6e95f)
- *gpj.stcepsuS detserrA.exe* (MD5: b6d700a58965692e92dce5dbc4323391)
- *gpj.bajaR.exe* (MD5: d1216d3fd238cd87d9a7e433b6892b98)

- *gpj.1bajaR.exe* (MD5: ad6f72b851ebcf7bf7c8b1c551140c5f)

Quickly looking at binary similarities, it was instantly clear that they all belong to the same malware family. We also identified an additional sample from the same batch:

- *wefaq.exe* (MD5: cf7b2e1485771967ece90d32f3076814)

A spokesman from Gamma Group, the company producing the trojan allegedly involved with these attacks, promptly responded to the press stating that FinFisher was never sold to Bahrain and that a copy might have been stolen and re-engineered for some unauthorized use. We're not able to confirm or deny this at the moment.

The Malware

For the sake of this analysis, we are going to use the file "gpj.1bajaR.exe", but all of them showed similar behavior and communicated with the same backend infrastructure.

Following are the complete cryptographic hashes of the binary:

MD5: ad6f72b851ebcf7bf7c8b1c551140c5f
SHA1: 37275cfd9e185b979c15fb8681c4c8434f224ed9
SHA256: cc3b65a0f559fa5e6bf4e60eef3bffe8d568a93dbb850f78bdd3560f38218b5c
SHA512: 909b631a81a54b279eaa46b81973a95af18da4adfff51b3ecbc731f78cfe380e8863872eb0e8648acf65f40560dd4684221f640058df0c4821839ab55b7b6597
Ssdeep: 24576:19E4gjTsw7ir1mLR4pzLgbN9z2iiYXDBaLznBn1F:AxjTsw7irkSOx7z6zB1F

The malware is already available on VirusTotal, which shows some decent Antivirus coverage:
https://www.virustotal.com/file/cc3b65a0f559fa5e6bf4e60eef3bffe8d568a93dbb850f78bdd3560f38218b5c/analysis/

The binary is disguised as a JPG picture, in fact the file name contains the Unicode Right-to-Left Override character in front that whenever displayed in ANSI mode, it will look reversed making the disguise more realistic: in this case "exe.Rajab1.jpg".

The first thing we did was of course give it a quick run in Cuckoo Sandbox, which was able to give some initial insights on the general behavior of the malware.

When executed, the original process proceeds creating the following directory (the name is randomized at every execution):
C:\DOCUME~1\User\LOCALS~1\Temp\\TMP44D8C9F9

If the directory is successfully created, it drops a copy of itself in that same directory, which is also consequently launched.

This new process is actually the one installing the components used to retain access on the compromised machine.
It drops an additional file in the user's Temp directory:
C:\DOCUME~1\User\LOCALS~1\Temp\\driverw.sys

Following are the hashes for this driver:
MD5: 0f8249a2593f38c6bf54b6f366c0cac6
SHA1: ff96eddce7a7663677b80a93fc542db8b06ef6f8
SHA256: 62bde3bac3782d36f9f2e56db097a4672e70463e11971fad5de060b191efb196
SHA512: 363fa00ce6d3eba1a3b2d313bb47df480d1b909074514e52950e1fbf364808c297991e1972f39346f42f2a52162d5329d1a663fa880527b3dfcc618652770909

Ssdeep: 192:cjQ/nPVCoovDy17/Zs15fHaqlIB6pJqwSmX:c0nPz/ZlPaqll+FSG

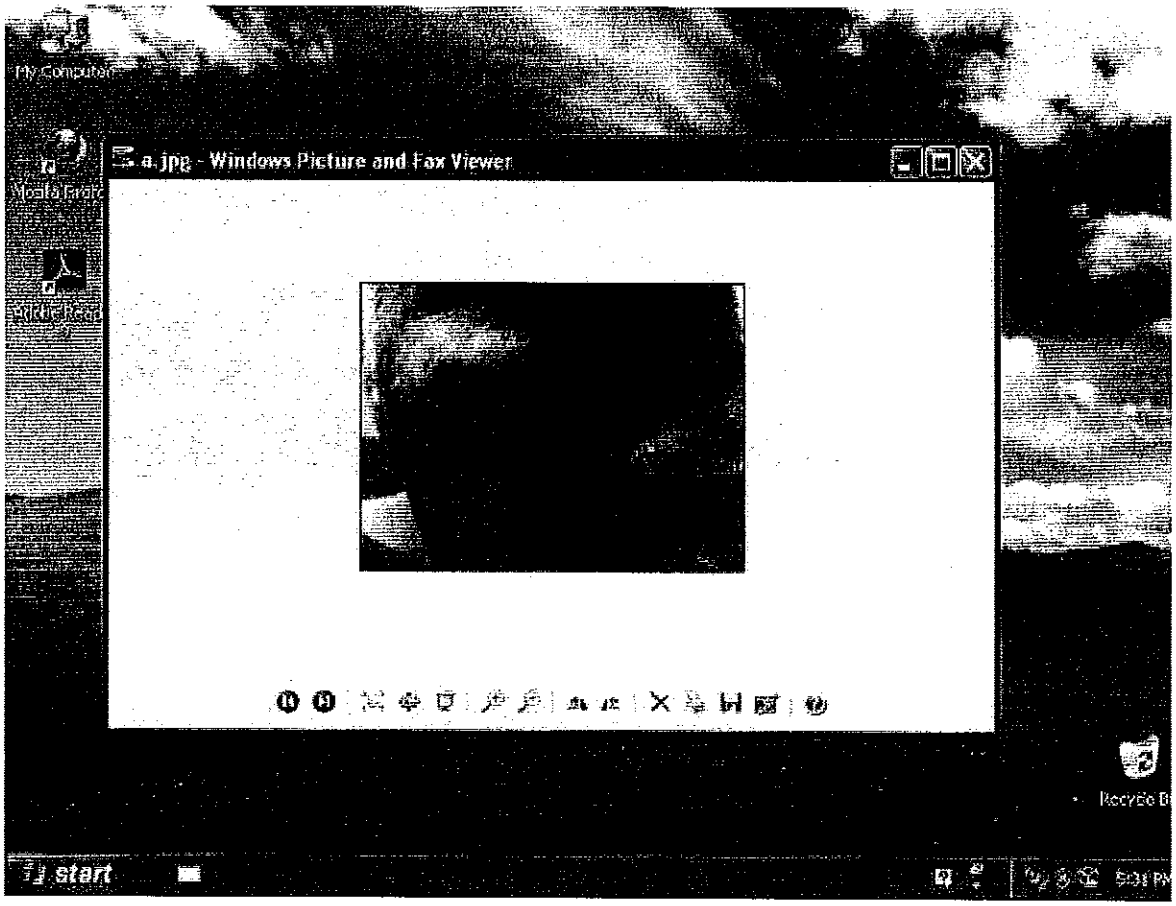
This same file was observed being consistently dropped by all the other payloads associated with these attacks.
Interestingly enough, it was already observed on VirusTotal in early May:
https://www.virustotal.com/file/62bde3bac3782d36f9f2e56db097a4672e70463e11971fad5de060b191efb196/analysis/

The driver is also obfuscated but appears to be able to respond to device control IRPs, a deeper analysis is needed to understand its internal capabilities.

The process concludes its execution by creating the following directory (the name is randomized at every execution):
C:\Documents and Settings\User\Application Data\Microsoft\Installer\{A69832D8-3F71-4241-7493-7551DB00C34C}

This directory is reported to be used for storing all the dumped data, logs and screenshots to be later communicated to the operators' C&C server.

In order to make the execution more realistic to the victim, it also drops an image which is also displayed:



The picture varies from one sample to another.

In this case a sandbox analysis was not enough as no network traffic was observed, therefore a deeper manual inspection was required.
As a matter of fact, the actual malware mechanics comes into play just after a first reboot following the compromise. At this point we can observe severe changes in the system and aggressive takeover of the system processes.

As already reported by CitizenLab in their analysis, winlogon.exe is the first process being injected with malicious code:

```
Process: winlogon.exe Pid: 612 Address: 0x1530000 Vad Tag: VadS Protection: PAG
Flags: CommitCharge: 19, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x01530000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
0x01530010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
0x01530020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x01530030 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 ................
```

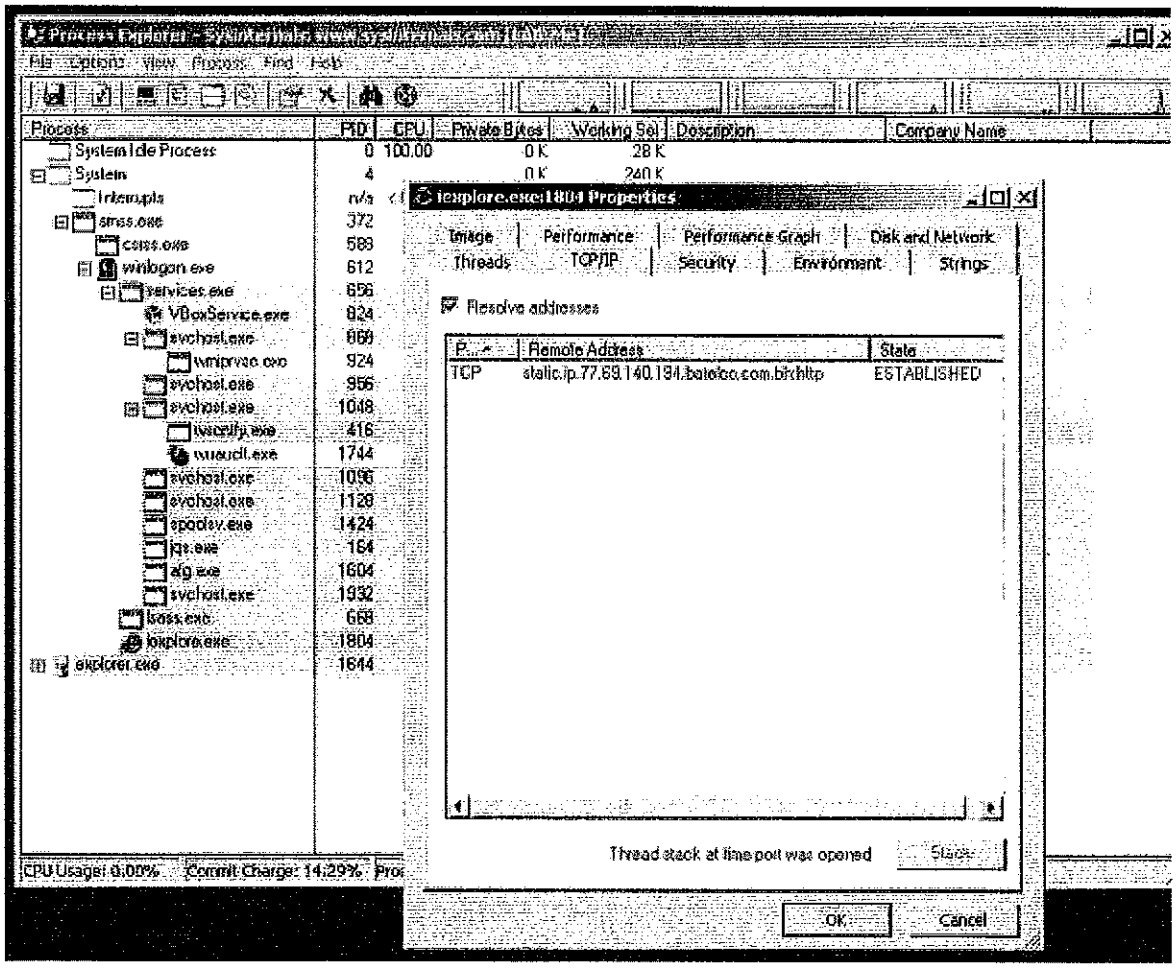
This process is used as a main container for the malware, from which it performs Process Hollowing. This is a common practice in malware development, consisting of spawning legitimate processes and, once loaded, replacing their original code with malicious code.

As a matter of fact, winlogon.exe starts an Internet Explorer instance with the "-nohome" options and performs the takeover:

```
Process: iexplore.exe Pid: 148 Address: 0x150000 Vad Tag: VadS Protection: PAGE
Flags: CommitCharge: 24, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x00150000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
0x00150010 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
0x00150020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x00150030 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ................
```

The network communication is initiated from the context of the Internet Explorer process, which is often used as a convenient way to bypass local firewalls as it is/used to be a trusted application:

```
Offset(V) Local Address Remote Address Pid
---------- ------------------------ ------------------------ ------
0x86335008 10.0.2.15:1036 77.69.140.194:443 148
```



The malware has a very noisy presence in the system, it installs inline user-mode hooks in the following functions in every running process:

ntdll.dll!NtDeviceIoControlFile
ntdll.dll!NtEnumerateKey
ntdll.dll!NtEnumerateValueKey
ntdll.dll!NtQueryDirectoryFile
ntdll.dll!NtQueryKey
ntdll.dll!NtQuerySystemInformation
kernel32.dll!CreateFileW
kernel32.dll!CreateProcessInternalW
kernel32.dll!MoveFileW
kernel32.dll!DeleteFileW
kernel32.dll!MoveFileExW
USER32.dll!PostMessageW
USER32.dll!GetMessageW
USER32.dll!PeekMessageW
USER32.dll!GetMessageA
USER32.dll!SendMessageW
USER32.dll!PeekMessageA
USER32.dll!PostMessageA
GDI32.dll!GetDeviceCaps
GDI32.dll!DeleteDC
GDI32.dll!CreateDCA

GDI32.dll!CreateDCW
GDI32.dll!DPtoLP
GDI32.dll!Escape
GDI32.dll!ResetDCW
GDI32.dll!EndPage
GDI32.dll!EndDoc
GDI32.dll!StartPage
GDI32.dll!ResetDCA
GDI32.dll!SetAbortProc
GDI32.dll!StartDocW
GDI32.dll!StartDocA
ADVAPI32.dll!OpenTraceA
ADVAPI32.dll!OpenTraceW

It also installs an IAT hook of the function ntdll.dll!CsrClientCallServer in winlogon.exe, which is most likely used to catch every new process registered to the CSRSS subsystem.

As also reported by CitizenLab, the samples seem indeed to belong to the FinFisher toolkit.
Following are some strings that can be found into winlogon.exe memory:

y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-tdiv_qr.c
y:\lsvn_branches\finspyv4.01\finspyv2\src\libs\libgmp\mpn-mul_fft.c
y:\lsvn_branches\finspyv4.01\finspyv2\src\target\bootkit_x32driver\objfre_w2k_x8 6\i386
\bootkit_x32driver.pdb
finfisher
finfisher.lnk

We also analyzed the reported "demo" sample:

MD5: c488a8aaef0df577efdf1b501611ec20
SHA1: 5ea6ae50063da8354e8500d02d0621f643827346
SHA256: 81531ce5a248aead7cda76dd300f303dafe6f1b7a4c953ca4d7a9a27b5cd6cdf
SHA512: 0c5a41d45e8939a256c6d24f651619a110b246d5ff5dfa296f68c703ce259ea9420e96ea34c4248
c413e51e4eb5e3f75928318b6fd30251068b5a9f938dd47e0
Ssdeep: 49152:j4XNybwJDejvL6joq2+Sqlk/1jzuUze0uY5nU:EUbwJDc0N21qC9jzuUG
VirusTotal: https://www.virustotal.com/file/81531ce5a248aead7cda76dd300f303dafe6f1b7a4c953ca
4d7a9a27b5cd6cdf/analysis/

Despite some differences (the dropped driver is sensibly bigger compared to the one from Bahrain), the execution flow is exactly the same: similar aggressive presence on the system, same processes chain and same network traffic.

At this stage it's difficult to get a hold of the full functionalities of the malware. We believe that the agent remains silent whenever it doesn't have an active Internet connection and at this very moment we believe it first pulls an updated configuration file instructing it to not do anything at all, therefore all the surveillance plugins seem to be inactive and no file is dropped in "%AppData%\Microsoft\Installer\{A69832D8-3F71-4241-7493-7551DB00C34C}\".

According to CitizenLab's research and WikiLeaks cables, following should be the supported features:

- Bypassing of 40 regularly tested Antivirus Systems
- Covert Communication with Headquarters
- Full Skype Monitoring (Calls, Chats, File Transfers, Video, Contact List)

- Recording of common communication like Email, Chats and Voice-over-IP
- Live Surveillance through Webcam and Microphone
- Country Tracing of Target
- Silent extracting of Files from Hard-Disk
- Process-based Key-logger for faster analysis
- Live Remote Forensics on Target System
- Advanced Filters to record only important information
- Supports most common Operating Systems (Windows, Mac OSX and Linux)

We believe that the Skype interception module is implemented tampering the circular sound buffer from Windows' DirectSound interface, you can find a similar implementation here.

Network Communication

All the samples from the Bahrain attacks try to contact the host located at 77.69.140.194, which belongs to Bahrain Manama Batelco (AS5416).

The malware tries to contact such IP address on multiple ports, either 22, 53, 80 or 443 and establish the communication channel on the first one successfully opened.

The traffic is heavily encrypted and it will require further analysis to dissect, but we were able to isolate some recurring patterns.
The first outgoing packet always starts with the following binary data:
0c 00 00 00 40 01 73 00

This packet, which varies in size and content, is believed to be reporting to the C&C some initial details on the compromised machines and perhaps some local configuration. The answer to this first request is believed to be an updated configuration for the trojan.

And all following packets appear to start with the following binary data:
5c 00 00 00 a0 02 72 00 0c 00 00 00 40 04 fe 00

The following **Snort signatures** should be consistent enough, but due to the small size of the patterns they could cause false positives:

```
alert tcp any any -> any any (msg:"FinFisher Malware Connection
Initialization"; content:"|0c 00 00 00 40 01 73 00|"; offset:0; depth:8;
sid:1000001; rev:1;)

alert tcp any any -> any any (msg:"FinFisher Malware Connection Handshake";
content:"|5c 00 00 00 a0 02 72 00 0c 00 00 00 40 04 fe 00|"; offset:0;
depth:16; sid:1000002; rev:1;)
```

We are looking forward to getting some feedback and suggestions on improved detection and whether any of you get some hits. Email us with your feedback.

Fingerprinting the C&C

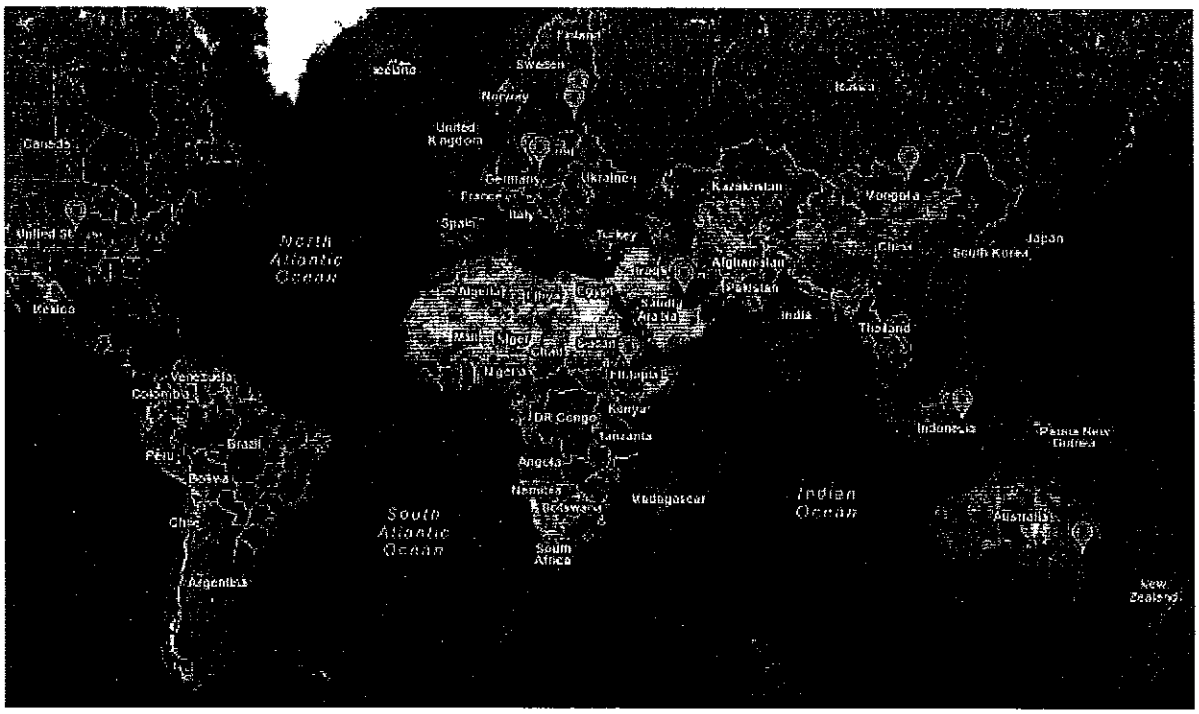
While probing the C&C servers, we noticed an unexpected behavior: all the services binded on the ports the malware tries to exchange binary data with, respond in an unusual way whenever performing any, even malformed, HTTP request.

For example, when connecting through telnet to 77.69.140.194:80 and sending "HEAD /", the service responded the following way:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8
Content-Length:12

Hallo Steffi
```

Odd indeed, but perfect for fingerprinting!
We made a cross-search of this pattern across HD's Internet survey research project Critical.IO, and were able to identify more servers with open services that responded in the exact same way:



Click on the map to get a larger view and browse through updated results.

Follow is the list of the IP addresses discovered:

- 112.78.143.26 ***(Indonesia)***
- 121.215.253.151 ***(Australia)***
- 78.100.57.165 ***(Qatar)***
- 213.55.99.74 ***(Ethiopia)***
- 94.112.255.116 ***(Czech Republic)***
- 213.168.28.91 ***(Estonia)***
- 54.248.2.220 ***(USA)***
- 202.179.31.227 ***(Mongolia)***
- 80.95.253.44 ***(Czech Republic)***
- 81.198.83.44 ***(Latvia)***
- 86.97.255.50 ***(Dubai, UAE)***

At the time of writing, only the Latvian sever is still successfully responding to our fingerprinting. All the others are instantly dropping the connection in the exact same way, most likely filtering off any payload that

doesn't match a given header. This makes us believe that all those C&Cs might have been updated in front of recent leaks and publications on FinFisher, Bahrain included.

Please note: we are not able to determine whether they're actually being used by any government agency, if they are operated by local people or if they are completely unrelated at all: they are simply the results of an active fingerprinting of a unique behavior associated with what is believed to be the FinFisher infrastructure. Our guess is that part of the identified C&Cs are acting as proxies.

Conclusions

It's always interesting to get your hands on governmental malware: it's the subject of much discussion and given the high prices it's likely sold for, it's often very hard to get access to samples, so this has been a great project to work on.

What we found is disturbing though. The malware seems fairly complex and well protected/ obfuscated, but the infection chain is pretty weak and unsophisticated. The ability to fingerprint the C&C was frankly embarrassing, particularly for malware like this. Combined, these factors really don't support the suggestion that thieves refactored the malware for black market use.

That said, once any malware is used in the wild, it's typically only a matter of time before it gets used for nefarious purposes. The infosec community needs to pay attention and take malware exposure seriously. Take action to protect infrastructure and discourage the spread, production and purchase of malware. As we've seen countless times before, and will certainly see again, it's impossible to keep this kind of thing under control in the long term.

I'm sure there will be follow-ups on this case on different sides and people will spend more time on analyzing and debating the ins and outs of the malware. For my part, I'd like to end this post by sincerely thanking the guys from CitizenLab for their original research and Arturo Filastò, Fabio Pietrosanti, Jacob Appelbaum and Quequero for their cooperation in this analysis. Thanks guys!

For updates, you can find me on Twitter at @botherder.

Update #1

The guys at EmergingThreats helped us refine our **Snort rules** a little bit in order to lower the possibility of false positives.
Following are the updated signatures, use them to detect FinSpy in your local networks:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"FinFisher Malware Connection
Initialization"; flow:to_server,established; content:"|0c 00 00 00 40 01 73
00|"; depth:8; sid:1000001; rev:1; classtype:trojan-activity;
reference:url,community.rapid7.com/community/infosec/blog/2012/08/08/finfisher;

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"FinFisher Malware Connection
Handshake"; flow:to_server,established; content:"|5c 00 00 00 a0 02 72 00 0c 00
00 00 40 04 fe 00|"; depth:16; sid:1000002; rev:1; classtype:trojan-activity;
reference:url,community.rapid7.com/community/infosec/blog/2012/08/08/finfisher;
```

Update #2

At the time of writing 8 out of the 12 servers are not responding anymore: all the ports originally used have been filtered or closed off after our analysis and the related news articles have been published.
Even the ones that were actively responding until yesterday, like Latvia and Bahrain, are now inaccessible.
A very odd timing, isn't it?

In the last hours we read of many people questioning the validity of the "Hallo Steffi" pattern, saying that it could be completely unrelated to the FinFisher toolkit, as also Gamma's Muench stated to Bloomberg. Fair enough, we also mentioned in this same blog post that there is no way we can guarantee a direct connection between that string and the malware, we only reported an anomaly on the Bahraini infrastructure and the discovery of the same anomaly in other locations.
We believe that this unusual behavior could have actually been a deception technique adopted by the FinSpy Proxy to disguise the nature of the service, but that when they realized it was actively used for fingerprinting the C&C servers **was promptly disabled to prevent further discoveries**.

Every FinSpy sample is configured with a set of multiple ports that it can try to contact: it will start from the lower port (for example 20), attempt a connection 3 times and then move over to the next one.
When running the Bahraini FinSpy sample, especially now that the server is not responding, it attempts the following connections:

```
13:02:43.747370 IP 10.0.2.15.1035 > 77.69.140.194.22: tcp 0
13:03:05.968816 IP 10.0.2.15.1036 > 77.69.140.194.53: tcp 0
13:03:28.100628 IP 10.0.2.15.1037 > 77.69.140.194.80: tcp 0
13:03:50.332553 IP 10.0.2.15.1038 > 77.69.140.194.443: tcp 0
13:04:21.517231 IP 10.0.2.15.1039 > 77.69.140.194.4111: tcp 0
```

As you can see the last one is port **4111**.
We believe this is the standard FinSpy port and that all the other ones are probably just forwarded to 4111.
The FinSpy "demo" sample contacted port **3111** to **tiger.gamma-international.de** and ff-demo.blogdns.org, close enough.

Another interesting "coincidence" is that all the IP addresses that we observed responding with the "Hallo Steffi" banner also had/have port 4111 open, in fact if you check the only 4 servers currently up you can see:

```
Nmap scan report for bba44246.alshamil.net.ae (86.97.255.50)
Host is up (0.26s latency).
PORT     STATE    SERVICE
22/tcp   open     ssh
53/tcp   open     domain
443/tcp  open     https
4111/tcp open     xgrid

Nmap scan report for 94.112.255.116.static.b2b.upcbusiness.cz (94.112.255.116)
Host is up (0.044s latency).
PORT     STATE  SERVICE
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
443/tcp  open   https
4111/tcp open   xgrid

Nmap scan report for 112.78.143.26
Host is up (0.26s latency).
PORT     STATE  SERVICE
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
443/tcp  open   https
4111/tcp open   xgrid
```

```
Nmap scan report for 213.55.99.74
Host is up (0.16s latency).
PORT     STATE  SERVICE
22/tcp   open   ssh
53/tcp   open   domain
80/tcp   open   http
443/tcp  open   https
4111/tcp open   xgrid
9111/tcp open   DragonIDSConsole
```

The last one also shows port 9111, which we observed along with port 3111 being open fewer times as well.
Is it more convincing now?

Share 12 14 Tweet 257 Like 99

20082 Views Tags: breach, malware, research, cuckoo_sandbox, malware_analysis, finfisher

Average User Rating

(0 ratings)

Comments
4 Comments

Please login to comment



elhoim 09-Aug-2012 04:47

Digging around with some passive DNS, you can find that ic3545.com was resolving to 121.215.253.151 between 2011-04-02 and 2011-04-17 (with 922 requests seen), and to 124.178.225.178 the 2010-11-22 (with 2 requests seen).
No other IP you discovered yield something interesting from passive DNS.

Like (0)



mooo 10-Aug-2012 20:27

As i know, Gmail doesn't allow to send .exe files. So, how does it happen?

Like (0)



Claudio Guarnieri 15-Aug-2012 02:08 (in response to elhoim)

Yes, we are aware of it and we've seen that domain hosting a fake Google page and distributing an executable that we are trying to recover.

Like (0)

Claudio Guarnieri 15-Aug-2012 02:12 (in response to mooo)

They sent RAR archives containing executables and it's not a big deal to bypass those Gmail filters. In addition, the fact that the original email addresses had a @gmail.com



domain doesn't necessarily mean that they used Gmail mailservers, we don't have copies of the original emails so we can't verify the headers.

Like (0)

Intelligence Note

Prepared by the
Internet Crime Complaint Center (IC3)
May 8, 2012

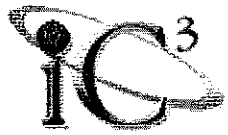
MALWARE INSTALLED ON TRAVELERS' LAPTOPS THROUGH SOFTWARE UPDATES ON HOTEL INTERNET CONNECTIONS

Recent analysis from the FBI and other government agencies demonstrates that malicious actors are targeting travelers abroad through pop-up windows while establishing an Internet connection in their hotel rooms.

Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to setup the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely-used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

The FBI recommends that all government, private industry, and academic personnel who travel abroad take extra caution before updating software products on their hotel Internet connection. Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor may reveal an attempted attack. The FBI also recommends that travelers perform software updates on laptops immediately before traveling, and that they download software updates directly from the software vendor's Web site if updates are necessary while abroad.

Anyone who believes they have been a target of this type of attack should immediately contact their local FBI office, and promptly report it to the IC3's website at http://www.ic3.gov/. The IC3's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The complaint information is also used to identify emerging trends and patterns.



Intelligence Note

Prepared by the
Internet Crime Complaint Center (IC3)
October 12, 2012

SMARTPHONE USERS SHOULD BE AWARE OF MALWARE TARGETING MOBILE DEVICES AND SAFETY MEASURES TO HELP AVOID COMPROMISE

The IC3 has been made aware of various malware attacking Android operating systems for mobile devices. Some of the latest known versions of this type of malware are Loozfon and FinFisher. Loozfon is an information-stealing piece of malware. Criminals use different variants to lure the victims. One version is a work-at-home opportunity that promises a profitable payday just for sending out email. A link within these advertisements leads to a website that is designed to push Loozfon on the user's device. The malicious application steals contact details from the user's address book and the infected device's phone number.

FinFisher is a spyware capable of taking over the components of a mobile device. When installed the mobile device can be remotely controlled and monitored no matter where the Target is located. FinFisher can be easily transmitted to a Smartphone when the user visits a specific web link or opens a text message masquerading as a system update.

Loozfon and FinFisher are just two examples of malware used by criminals to lure users into compromising their devices.

Safety tips to protect your mobile device:

- When purchasing a Smartphone, know the features of the device, including the default settings. Turn off features of the device not needed to minimize the attack surface of the device.
- Depending on the type of phone, the operating system may have encryption available. This can be used to protect the user's personal data in the case of loss or theft.
- With the growth of the application market for mobile devices, users should look at the reviews of the developer/company who published the application.
- Review and understand the permissions you are giving when you download applications.
- Passcode protect your mobile device. This is the first layer of physical security to protect the contents of the device. In conjunction with the passcode, enable the screen lock feature after a few minutes of inactivity.
- Obtain malware protection for your mobile device. Look for applications that specialize in antivirus or file integrity that helps protect your device from rogue applications and malware.
- Be aware of applications that enable Geo-location. The application will track the user's location anywhere. This application can be used for marketing, but can be used by malicious actors raising concerns of assisting a possible stalker and/or burglaries.
- Jailbreak or rooting is used to remove certain restrictions imposed by the device manufacturer or cell phone carrier. This allows the user nearly unregulated control over what programs can be installed and how the device can be used. However, this procedure often involves exploiting significant security vulnerabilities and increases the attack surface of the device. Anytime a user, application or service runs in "unrestricted" or "system" level within an operation system, it allows any compromise to take full control of the device.
- Do not allow your device to connect to unknown wireless networks. These networks could be rogue access points that capture information passed between your device and a legitimate server.
- If you decide to sell your device or trade it in, make sure you wipe the device (reset it to factory default) to avoid leaving personal data on the device.
- Smartphones require updates to run applications and firmware. If users neglect this it increases the risk of having their device hacked or compromised.
- Avoid clicking on or otherwise downloading software or links from unknown sources.

- Use the same precautions on your mobile phone as you would on your computer when using the Internet.

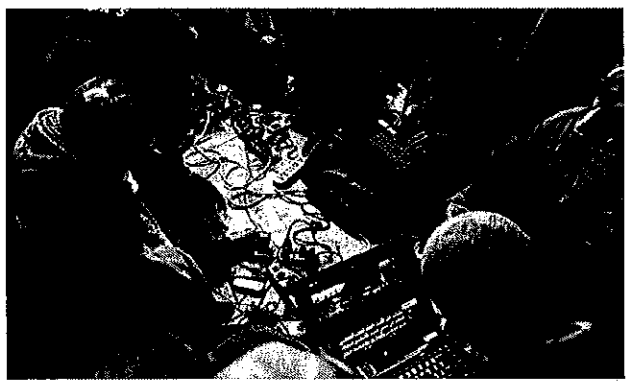
If you have been a victim of an Internet scam or have received an e-mail that you believe was an attempted scam, please file a complaint at www.IC3.gov.

theguardian

British firm offered spying software to Egyptian regime – documents

Gamma International's Finfisher program would have enabled government spies to monitor activists and censor websites

Karen McVeigh
guardian.co.uk, Thursday 28 April 2011 14.05 BST



Egyptian anti-government bloggers work on their laptops from Cairo's Tahrir Square on February 10, 2011
Photograph: Patrick Baz/AFP/Getty Images

A British company offered to sell a program to the Egyptian security services that experts say could infect computers, hack into web-based email and communications tools such as Skype and even take control of other groups' systems remotely, according to documents seen by the Guardian.

Two Egyptian human rights activists found the documents amid hundreds of batons and torture equipment when they broke into the headquarters of the regime's State Security Investigations service (SSI) last month.

One of the papers, in English and headed Finfisher Proposal: Commercial Offer, contained an offer dated 29 June 2010 to provide "FinSpy" software, hardware, installation and training to the SSI for €287,000 (£255,000). The name on the invoice, dated Tuesday 29 June 2010, was Gamma International UK Limited.

Other documents, written in Arabic and marked "ultimately confidential", state that after being offered a "free trial version" of Gamma's Finfisher software to test its ability to hack into email accounts, the SSI concluded it was "a high-level security system" that could get into email accounts of Hotmail, Gmail and Yahoo, as well as allowing "full control" of the computers of "targeted elements". It went on to describe the software's "success in breaking through personal accounts on Skype network, which is considered the most secure method of communication used by members of the elements of the harmful activity because it is encrypted".

The find throws a spotlight on western companies that provide software to security services and agents of oppressive regimes to spy on, censor and block the websites with which activists communicate. Last month a report by OpenNet Initiative said nine countries across the Middle East and North Africa used US and Canadian technology to impede access to online content, including sites with political, social and religious material.

Mostafa Hussein, a Cairo blogger and physician who took the documents, said they formed important evidence against the SSI's activities. "This proposal was sent to a department well known for torture, for abuse of human rights, for spying on political campaigners. This company, Gamma, should be exposed as collaborators in the crimes

of trying to invade our privacy and arrest activists."

Hussein posted the documents online and passed a copy to the Guardian.

A Gamma International website called "Finfisher IT Intrusion" describes its software as allowing "remote monitoring and infection" that can provide "full access to stored information with the ability to take control of the target". It is advertised as capable of "capturing encrypted data and communications" and allowing a "government agency to remotely infect target systems".

The documents found in the SSI HQ, one dated 1 January 2011, said that the proposal from Gamma International had come via a subsidiary company, Modern Communications System. Following a "free" five-month trial, SSI described the software as like "planting a comprehensive spying system in the location where the targeted computer exists". The software could record voice and audio calls, movements through video and audio where the computer was located, and hack into all the computers in the same network.

Rick Ferguson, of internet security company Trend Micro, said: "Our position on commercial spyware is that if the monitoring is being done without the consent of the person being monitored then that would be the theft of information.

"There's certainly an ambiguity of selling that kid of technology to that type of regime. There are a lot of commercial tools to enable you to remotely monitor and manage computers but it's about how those tools are being used and whether those tools are being used covertly."

Amr Gharbeia, an activist who works at the Egyptian Initiative for Personal Rights, said the Finfisher software referred to in the proposal was "a trojan, a software you implant in someone else's device to control it and possibly get data from it. It puts you in the driver's seat so you can see someone else's email and allows also for identity fraud."

When contacted by the Guardian, Gamma International said in a statement: "Gamma International UK Limited manufactures equipment for dealing with security related threats and it supplies only to governments.

"Gamma International UK Limited has not supplied any of its Finfisher suite of products or related training etc to the Egyptian government."

Gamma said it "complies, in all its dealings, with all relevant UK legislation and regulation".

• This article was amended on 30 April 2011 to correct the spelling of Gamma International in the standfirst.

© 2012 Guardian News and Media Limited or its affiliated companies. All rights reserved.

BBC NEWS

TECHNOLOGY

20 September 2011 Last updated at 10:19

UK firm denies 'cyber-spy' deal with Egypt

By Stephen Grey
File on 4, BBC Radio 4

A UK firm offered to supply "cyber-spy" software used by Egypt to target activists, the BBC has learned.

Documents found in the headquarters of the country's security service suggest it was used for a five-month trial period at the end of last year.

Hampshire-based Gamma International UK denies actually supplying the program, which infects computers with a virus that bugs online voice calls and email.

The foreign secretary says he will "critically" examine export controls.

William Hague, who speaks for the government on computer security issues, said: "Any export of goods that could be used for internal repression is something we would want to stop."

He also admitted the law governing software exports was a grey area.

The documents seen by the BBC were found at the looted headquarters of the Egyptian state security building earlier this year.

They describe an offer by Gamma International UK Ltd to supply a software programme called Finfisher.

Finfisher is described as a toolkit "used by many global security and intelligence services" for secretly gaining access to people's computers.

The files from the Egyptian secret police's Electronic Penetration Division described Gamma's product as "the only security system in the world" capable of bugging Skype phone conversations on the internet.

They detail a five-month trial by the Egyptian secret police which found the product had "proved to be an efficient electronic system for penetrating secure systems [which] accesses email boxes of Hotmail, Yahoo and Gmail networks".

Another document discovered by German public television network MDR is thought to reveal the first-known victims of the Finfisher program.

The document describes how, during the period of the software trial, the secret police successfully broke into and recorded encrypted Skype calls.

Sherif Mansour, from the US democracy group Freedom House, was in Egypt last year to help monitor parliamentary elections.

'Outsourcing repression'
Named in the document as a victim of the bugging, he blamed the Finfisher software and urged the British government to take action.

"We democracy and human rights activists already face a lot of troubles and get a lot of threats. I expect that from government but not from software companies.

"We have never looked to them to [be] enabling repression, to outsourcing repression."

According to the Department for Business Innovation and Skills, Finfisher does not require an export licence because it does not use encryption.

Mr Hague told File on 4 that the UK had a strong export licence system.

He said a number of licences had been withdrawn from companies exporting items of concern to Libya, Tunisia and Bahrain - but he conceded software was a difficult product to legislate for.

"This will be a greyer area because there can be many many uses for a given piece of software.

"But nevertheless, we will look at that critically and if any evidence is supplied to the government - or we come across any evidence of British technology used for internal repression in other countries - then we will take the same very tough line on that as we do on other items."

Gamma International UK Ltd is owned by a 49-year-old Briton, Louthean Nelson, who is listed as having addresses in Salisbury, Hamburg and Beirut.

The BBC wanted to ask Mr Nelson about the contradiction between Gamma's claim it did not supply the software, and the information contained in the Egyptian documents. He did not reply.

'Abuse of technology'

But although Gamma has refused to comment publicly, a company representative called Martin Muench is due to speak next week at a **conference in Berlin on cyber warfare**.

Gamma is listed as a "sponsor and exhibitor" with a speaker due to address the conference on "applied hacking techniques used by governmental agencies".

Also speaking at the conference are colonels from the British, US and German armies, and the director of intelligence at US Cybercommand.

Elsewhere in the Middle East, reports emerged this month of **claims that French and South African firms helped monitor phones and the internet for Libya's Col Muammar Gaddafi**.

In Bahrain - where the regime has so far survived the protests - human rights activist Abdul Ghani al-Khanjar says he only learned the extent of surveillance in his country after being arrested.

He had just returned from London where he spoke at a meeting in the House of Lords.

"Within two days, masked civilians and riot police raided my house and arrested me and I have been tortured about my many activities," he told the BBC.

"It was amazing when they showed me some text messages from my phone and told me about my calls."

He added: "This is a bad abuse of technology."

The Bahraini government says it has launched an inquiry into torture allegations. But **Siemens and Nokia have both been implicated in the bad publicity surrounding the case**.

In the past Siemens sold Bahrain a "monitoring centre", which is thought to have allowed the regime to secretly track and bug its citizens' phones. The company is said to have sold the same system to 60 countries worldwide.

But Ben Roome, a spokesman for Nokia Siemens Networks - a joint venture between the two companies, says it has now pulled out of making interception tools, precisely because of concerns that they can be abused.

"If you provide technology you cannot be blind to how potentially it can be used," he said.

File on 4 is on **BBC Radio 4** on Tuesday 20 September at 20:00 BST and Sunday 25 September at 17:00 BST. Listen again via the **Radio 4 website** or download the **podcast**.

More Technology stories



Crowd-funder Kickstarter UK bound
[http://www.bbc.co.uk/news/technology-18780184]
The crowd-sourced funding website Kickstarter is to launch in the UK this autumn, according to its Twitter feed.

Megaupload case delayed to 2013
[http://www.bbc.co.uk/news/technology-18779866]

Syrian abuse ends spy code work
[http://www.bbc.co.uk/news/technology-18783064]

BBC

BBC © 2012 The BBC is not responsible for the content of external sites. Read more.

theguardian | TheObserver

UK 'exporting surveillance technology to repressive nations'

Fears that software similar to that which government wants to use in Britain is being sold to monitor dissidents abroad

Jamie Doward and Rebecca Lewis
guardian.co.uk, Saturday 7 April 2012 21.00 BST



There are fears that UK technology firms could be supporting Assad's Syrian regime. Photograph: -/AFP/Getty Images

Britain is exporting surveillance technology to countries run by repressive regimes, sparking fears it is being used to track political dissidents and activists.

The UK's enthusiastic role in the burgeoning but unregulated surveillance market is becoming an urgent concern for human rights groups, who want the government to ensure that exports are regulated in a similar way to arms.

Much of the technology, which allows regimes to monitor internet traffic, mobile phone calls and text messages, is similar to that which the government has controversially signalled it wants to use in the UK.

The campaign group, Privacy International, which monitors the use of surveillance technology, claims equipment being exported includes devices known as "IMSI catchers" that masquerade as normal mobile phone masts and identify phone users and malware – software that can allow its operator to control a target's computer, while allowing the interception to remain undetected.

Trojan horse software that allows hackers to remotely activate the microphone and camera on another person's phone, and "optical cyber solutions" that can tap submarine cable landing stations, allowing for the mass surveillance of entire populations, are also being exported, according to the group.

Privacy International said it had visited international arms and security fairs and identified at least 30 UK companies that it believes have exported surveillance technology to countries including Syria, Iran, Yemen and Bahrain. A further 50 companies exporting similar technology from the US were also identified. Germany and Israel were also identified as big exporters of surveillance technology, in what is reportedly a £3bn a year industry.

Last month Privacy International asked 160 companies about sales of equipment to repressive regimes. So far fewer than 10 have written back to deny selling to nations with poor human rights records. The campaign group warns: "The emerging information and communications infrastructures of developing countries are being hijacked for surveillance purposes, and the information thereby collected is facilitating

unlawful interrogation practices, torture and extrajudicial executions."

Many of the brochures, presentations and marketing videos used by surveillance companies to promote their technology have now been posted on the WikiLeaks website, while a list of firms identified by Privacy International as a cause for concern has been provided to the Department for Business, Innovation and Skills. The trade minister, Mark Prisk, has been briefed on the situation.

Last month the European council banned the export of surveillance technologies to Iranian authorities in response to serious human rights violations. It has imposed similar bans on exports to Syria.

But human rights groups said equipment was still being sold to commercial organisations in the two countries and called for the government to take stronger action.

"By the time the embargo is in place the ship has sailed," said Eric King, head of research at Privacy International. "Our research shows the idea that this is not a British problem is wrong. We need governments to act now. In a few years this equipment will need to be updated; these countries don't have the technical expertise to do it, so this is something the UK needs to be aware of and to take action against now."

In December it emerged a British company had offered to sell software to Egyptian security services that experts say could hack into web-based email. The company, Gamma Group International, insists it "complies, in all its dealings, with all relevant UK legislation".

Last year a public outcry forced an Italian company to pull out of supplying Syria with "deep packet investigation" technology that would allow the country's security forces to access internet service providers. But Syriatel Mobile, Syria's largest mobile phone operator, uses blocking technology provided by a Dublin-based company.

Creativity Software (CS), a British firm specialising in "location-based services", sold technology to the mobile network operator MTN Irancell that campaign groups said could be used to track individuals. The company said its technology provided "the same type of activities that are enjoyed by consumers in many other markets – a hugely popular and successful social networking and location-based mobile advertising service".

It is the responsibility of manufacturers to ensure their technology is not used to perpetrate human rights abuses. But there are now calls for them to be subject to stringent export controls requiring a licence to sell abroad.

Privacy International also argues that, in order to prevent dangerous technologies reaching authoritarian regimes through middlemen, there is a need for "end-use" controls that would make it illegal for companies to provide their products when they know or suspect they will be used in human rights abuses.

In a letter to Privacy International, Downing Street said the government was "actively looking at this issue" and was working within the EU to introduce new controls on surveillance.

© 2012 Guardian News and Media Limited or its affiliated companies. All rights reserved.

PRIVACY INTERNATIONAL

Bloomberg.com | Businessweek.com | Bloomberg TV | Premium | Register | Sign In

MARKET SNAPSHOT

	U.S.	EUROPE	ASIA	
DJIA	12,836.40	+160.33	1.26%	
S&P 500	1,354.69	+16.80	1.26%	
NASDAQ	2,884.84	+30.60	1.07%	

IDEAS THAT MATTER

Our Company | Professional | Anywhere

Search News, Quotes and Opinion

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTAINABILITY TV VIDEO RADIO


Jefferies Vies With Goldman for Highest Wall Street Pay


Facebook Earnings 101: Ad Revenue Holds the Key


TV Stations Charge 'Gouge' Rates for Super-PACs

Cyber Attacks On Activists Traced To FinFisher Spyware Of Gamma

By Vernon Silver - Jul 25, 2012 1:06 PM GMT+0100

2 COMMENTS | QUEUE

It's one of the world's best-known and elusive cyber weapons: FinFisher, a spyware sold by U.K.- based Gamma Group, which can secretly take remote control of a computer, copying files, intercepting Skype calls and logging every keystroke.

For the past year, human rights advocates and virus hunters have scrutinized FinFisher, seeking to uncover potential abuses. They got a glimpse of its reach when a FinFisher sales pitch to Egyptian state security was uncovered after that country's February 2011 revolution. In December, anti-secrecy website WikiLeaks published Gamma promotional videos showing how police could plant FinFisher on a target's computer.

Enlarge Image



Husain Abdulla, a U.S. citizen who is director of Americans for Democracy and Human Rights in Bahrain, is considering lawsuits and a complaint to the U.S. State Department about the border-crossing hack. Source: Husain Abdulla via Bloomberg

Enlarge Image



University of Toronto Munk School of Global Affairs' Citizen Lab security researcher Morgan Marquis-Boire. Photographer: Jacob Kepler/Bloomberg

"We know it exists, but we've never seen it -- you can imagine a rare diamond," says Mikko Hypponen, chief research officer at Helsinki-based data security company F-Secure Oyj. (FSC1V) He posted the Egypt documents online last year and said if a copy of the software itself were found, he'd write anti-virus protection against it.

Now he may get his wish.

Researchers believe they've identified copies of FinFisher, based on an examination of malicious software e-mailed to Bahraini activists, they say. Their research, which is being published today by the University of Toronto Munk School of Global Affairs' Citizen Lab, is based on five different e-mails obtained by Bloomberg News from people targeted by the malware.

Global Reach

Pro-democracy activists received the malware in Washington, London and Manama, the capital of Bahrain, the Persian Gulf kingdom that has been gripped by tension since a crackdown on protests last year.

The findings illustrate how the largely unregulated trade in offensive hacking tools is transforming surveillance, making it more intrusive as it reaches across borders and peers into peoples' digital devices. From anywhere on the globe, the software can penetrate the most private spaces, turning on computer web cameras and reading documents as they are being typed.

Get Breaking News emailed to you.

Sign up for Alerts

HEADLINES | MOST POPULAR | RECOMMENDED

Superyachts Anchor In London as 1% Hit Olympics
Q

Facebook, HTC Said to Work on Phone for Mid-'13
Q

Pending Sales of U.S. Homes Unexpectedly Fall
Q

Draghi: ECB Will Do What's Needed on Euro
Q

Possible Derecho Forecast for U.S. Northeast
Q

Gramm: Glass-Steagall Repeal Didn't Cause Crisis
Q

Lazard Profit Falls 50% as AUM Drops
Q

Bo Xilai Wife Charged In Poisoning Death
Q

More News

Advertisement


How to Invest for Income - Free 16 page magazine
Download Now


How Summer Trading Could Increase Returns & Reduce Risk.
Download Free Here


Join the 1000s who have declined the banks -- Earn 8.7% avg gross yield
Learn More Here

Sponsored Links

Maths Teacher Training
Qualify as a maths teacher. Register for more information.
www.education.gov.uk

Free FTSE 350 Tips
Weekly technical Analysts Reports. Free Information Service.
www.sharepages.co.uk

BlackBerry® Bold™ 9790
Upgrade Now To The New BlackBerry® Bold™ 9790 Smartphone. Find More!
www.BlackBerry.com/UK/Bold9790

AdChoices

Enlarge image



Marczak found evidence that traces malicious software e-mailed to Bahraini activists back to FinFisher, a spyware sold by U.K.-based Gamma Group. Photographer: David Paul Morris/Bloomberg

"Selling software that allows for the taking over of computers without rule of law can lead to abuse," says Courtney Radsch, senior program manager for freedom of expression at Washington-based Freedom House, which promotes human rights.

Gamma executive Martin J. Muench declined immediate comment pending research after being e-mailed a Web link to the Citizen Lab report and questions related to its findings. Muench, who leads the FinFisher product portfolio, is the managing director of the group's Munich-based Gamma International GmbH. Gamma Group also markets FinFisher through Andover, England-based Gamma International UK Ltd.

Advertisement



Muench said in a July 23 e-mail that the company can't comment on any individual customers and that Gamma complies with the export regulations of the U.K., U.S. and Germany.

Monitoring Criminals

Muench, 30, said in that e-mail that FinFisher is a tool for monitoring criminals, and that to reduce the risk of abuse of its products the company only sells FinFisher to governments.

The recipients of the Bahrain-related e-mails -- who include a naturalized U.S. citizen who owns gas stations in Alabama, a London-based human rights activist and a British-born economist in Bahrain -- each say they don't know of any law enforcement investigations or charges against them.

Two of the recipients said they were suspicious of the e- mails and didn't click on the attachments, while the third said he tried and failed to download an attachment to his Blackberry.

The analysis of their e-mails showed the malware they received acts as a Trojan, a type of software named after the legendary wooden horse that Greek warriors used to sneak into Troy before sacking the ancient city. It takes screen shots, intercepts voice-over-Internet calls and transmits a record of every keystroke to a computer in Manama.

Stolen Password

Observation of a researcher's purposely-infected laptop in Washington also showed the Trojan stole a password for an e-mail account, which was then accessed without permission.

The malware itself practically came with a product label for a brand of FinFisher called FinSpy, which is marketed for spying on computers: On the infected laptop, the computer code the malicious program installed bore multiple instances of the word "FinSpy," an examination of the computer's memory showed.

The technical evidence of a match came from the work of Morgan Marquis-Boire, a security researcher at Citizen Lab, who analyzed the infected e-mails for this story. He's publishing the detailed report of the findings in a paper today through Citizen Lab, at http://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed.

Digital DNA

Marquis-Boire extracted a signature from the activists' samples -- a sort of digital DNA. He then gave the signature to other researchers to see if they could find a matching sample they might have collected in the course of their work.

The needle-in-a-haystack search came up with a match: a program that bore the hallmarks of a demonstration copy of FinFisher.

The evidence that the new sample they found was FinFisher itself was persuasive, Marquis-Boire said, because the presumed demo connected back to two websites, one with "ff-demo"

In the name and the other with "gamma-international" in the name. The latter website, in turn, was registered to Martin Muench at Gamma International in Munich, online registration data show.

BLOOMBERG TERMINAL
Professional
Anywhere

Bahrain has no policy of targeting political activists through surveillance technology, Lama Bashmi, a spokeswoman for the government's Information Affairs Authority, said in an e-mailed statement.

"Such allegations are taken very seriously and if there is any evidence that there is any misconduct in use of such technology, each case will be investigated immediately according to the laws and regulations of the Kingdom of Bahrain," she said.

Cyber-Arms Bazaar

FinFisher is just one of many increasingly available weapons for sale in the global cyber-arms bazaar.

The hacking techniques go beyond traditional surveillance of phone calls, e-mails and text messages, which governments conduct by tapping into communications networks that pass through their territory. Reports in the past year of repressive regimes using Western gear for domestic surveillance led the U.S. and European Union to impose restrictions on sales to some countries, such as Syria.

Technologies such as FinFisher mark the next step in a digital arms race, and are provided by other companies, such as Milan-based HackingTeam, whose programs, once installed, transmit an infected computer's activities. They are the retail cousins of state-made cyber weapons such as the Stuxnet computer worm, which damaged centrifuges in an Iranian nuclear plant and was jointly developed by the U.S. and Israel, according to the New York Times.

Surveillance Breakthrough

The discovery and tracking of such spyware shows how even the tiniest nations obtain cyber small arms and deploy them at home and across borders.

"We're moving to a new place with surveillance," says John Scott-Railton, a doctoral student at the University of California Los Angeles' Luskin School of Public Affairs who has helped track Trojans in Libya and Syria, where he says pro- regime hackers cobbled together malware attacks from free or inexpensive products available online. He also coordinated research for this study, passing the first malware samples from Bloomberg to Marquis-Boire.

The Bahraini case is a breakthrough because it shows the use of a more sophisticated, invasive hacking tool available for purchase by nations that might not be able to develop their own cyber weapons, Scott-Railton says. "The time for active penetration by states at a widely deployable scale has come," he says.

Hacker Turned Executive

Founded in 1990, Gamma Group relies on hacker-turned- executive Muench to market such capabilities to clients around the world. Just over six feet tall, Muench is a rock star of the global interception-technology conference circuit, listed in agendas only by his initials, MJM.

Wearing a trim black suit and skinny black tie, he attended the ISS World trade show, known in the industry as the Wiretapper's Ball, in Kuala Lumpur, Malaysia, in December. One of his talks was titled "Offensive IT Intelligence Information- Gathering Portfolio -- An Operational Overview."

FinFisher has such mystique that an intelligence worker who helps manage a Southeast Asian country's cybersecurity said Muench's presence at the show was the main reason he took extra precautions to detect hacker threats lurking in the wireless networks at the venue. The operative, who said he has attended a demonstration of the product, insisted that his name not be published because of his intelligence work.

Remotely Controlled

FinFisher promotional materials provide a general view into its capabilities, without naming the countries where it's sold.

"When FinSpy is installed on a computer system it can be remotely controlled and accessed as soon as it is connected to the Internet/network, no matter where in the world the Target System is based," a Gamma brochure published by WikiLeaks says.

In response to questions about FinFisher's deployment, privately held Gamma issued a statement Jan. 27 that quoted Muench saying, "Most people understand that we can't divulge details about our clients, the products they buy or how they use them -- we don't want to tip off the criminals!"

The statement addressed the documents found in Cairo, which priced the system at 388,604 euros ($470,000), including maintenance. Gamma said no sale was made, and the trial version shown during its pitch never targeted unwitting computer users.

"Gamma presented the product FinSpy showing its operational capabilities with a Gamma-supplied special target notebook for demonstration purposes only," the statement said.

In the case of Bahrain, the malware did reach real targets, and led to an analysis of the software.

Suspicious E-mails

In Manama, Ala'a Shehabi, the U.K.-born economist, noticed she and other activists were receiving suspicious e-mails that purported to have news on topics including torture and prisoners. She forwarded them to Bloomberg.

Tests showed that the attached photos and documents would secretly install a program taking over their computers if clicked on and opened.

The analysis by Marquis-Boire exposed how the malicious program went through elaborate processes of hiding itself, running through a checklist of anti-virus programs to see if any were on the computer, and establishing a connection with the server in Manama to which it would send its data.

A dreadlocked New Zealander based in San Francisco, Marquis-Boire has plastered his laptop with a bumper sticker that says, "My other computer is your computer." (He did the research separately from his job as a security engineer at Google Inc., which wasn't involved in this project.)

Virtual Machine

The other half of the analysis involved watching the malware as it went about spying.

Bill Marczak, a computer science doctoral candidate at the University of California Berkeley, also received four samples from Shehabi. He installed the samples on a "virtual machine" on his laptop and monitored the Trojan's behavior. Marczak, who spent his high school years in Bahrain, is a founding member of Bahrain Watch, a group that advocates for more transparent governance in the kingdom.

Marczak established the link to Bahrain by tracing the Trojan's transmissions back to an Internet address in Manama. After receiving the fifth sample from Bloomberg News, Marczak found it led to the same online address.

Other information also pointed to FinFisher. Some details from FinFisher product specification documents obtained by Bloomberg News matched details of what Marczak found as he watched files stream out of his laptop.

MOBILE APPS

Bloomberg

Bloomberg Radio+

Bloomberg TV+

Bloomberg Businessweek+

Jobs by Indeed Rate this Page Made in Windows

Skype Data

According to the product specifications, when FinFisher filches Skype data, it transports the information back to the system's operators in files prefaced with the number 14 and ending with a series of characters representing the time the file was created.

When Marczak made a Skype call on his infected machine in California, he watched the Trojan grab the data -- and send it to Bahrain in files that, indeed, began with 14 and ended with a timestamp.

The apparent use of FinFisher against Bahraini activists underscores the need for broader Western export controls of surveillance technology, says Eric King, the head of research at London-based Privacy International.

The group's lawyers informed U.K. regulators in a July 12 letter that it plans to sue the government for failing to enforce laws already on the books that give it the power to block exports that can be used to violate human rights.

Repression Risk

"Plainly there is a very real risk, if not an inevitability, that surveillance equipment, such as the FinFisher products, has been, and continues to be, exported to countries where it is highly likely to be used for internal repression and breaches of human rights," the letter to the U.K. secretary of state for business innovation and skills said.

The Department for Business is considering Privacy International's letter and will respond, a spokesman said. The U.K. government has proposed that arms-related export controls followed by most Western nations be expanded to add certain surveillance technology, and is pursuing this with other countries, the department said in a statement.

Tensions have simmered in Bahrain since the government cracked down on mass protests last year involving opponents of Sunni Muslim rule over the Shiite majority. At least 35 people died in the violence between Feb. 14 and April 15, 2011, including four police officers and a soldier, according to the Bahrain Independent Commission of Inquiry, which investigated the unrest and found instances of torture. Low-level protests continue in the island nation of 1.2 million people, home to the U.S. Navy's Fifth Fleet.

Infection Attempts

Three Bahraini dissidents who said they received the malware-laden mailings were in Washington, London and Manama when the malware attempted to infect their computers in April and May. The first e-mails they received, sent in April, were titled "Existence of a new dialogue - Al-Wefaq & Government authority" and, in Arabic, "Events this week."

E-mails sent in May had the subject lines "Torture reports on Nabeel Rajab," a reference to a jailed opposition leader; "King Hamad Planning," a reference to the Bahraini king's trip to London for Queen Elizabeth II's diamond jubilee; and "Breaking News from Bahrain -- 5 Suspects Arrested."

Husain Abdulla, a U.S. citizen who is director of Americans for Democracy and Human Rights in Bahrain, said he tried to download the "Existence of a new dialogue" attachment on his Blackberry while walking from a Washington Metro station to meetings at a Congressional office building.

Abdulla, 34, the Mobile, Alabama-based owner of gas stations, now is considering lawsuits and a complaint to the U.S. State Department about the border-crossing hack.

Seeking Protection

"I'm going to take any legal venue I can to protect myself," Abdulla says.

Shehabi, 31, whose e-mails were the first to be analyzed for the study, is a British-born Bahraini activist and an economics lecturer with a PhD from Imperial College London. She received the e-mails in Bahrain.

"This was an attempt at violating my privacy in a country that does not believe in privacy rights," she says. "The U.K. company is responsible for selling infiltration tools to a government they know will use them to repress pro-democracy activists."

London-based Bahraini activist Shehab Hashem, 29, says he received three of the e-mails after he travelled to Sweden and Switzerland to draw attention to human rights violations in Bahrain. Two of those were identical to e-mails Shehabi received. The other, which he provided to Bloomberg News, was the fifth sample in the study.

"I thought it was just spam," he says. "I never thought that someone would be interested in hacking into my computer."

In Finland, Hypponen said before the publication of today's report that he and other malware hunters would enjoy dissecting a FinFisher sample.

"There's lots of chitchat amongst the security people about how it might work, but it's mostly just speculation. Nobody knows for real," he said.

Identifying FinFisher could turn the tables. "It's hard for them to sell a tool to secretly infect computers if anti- virus programs can detect it," he said.

To contact the reporter on this story: Vernon Silver in Rome at vtsilver@bloomberg.net;

To contact the editor responsible for this story: Melissa Pozsgay at mpozsgay@bloomberg.net

Q
What is the queue?
More »Items In Your queue
This is your Bloomberg Queue
The queue will help you find news, save stories for later and take them with you
Learn MoreClose

More News: Sustainability - Health & Population

2 COMMENTS Q QUEUE


184M Gallons of Flood Water Vs. World's Largest Dam


Microsoft Unveils Surface Tablet Computer


EU'S Van Rompuy Says More Pressure Needed on Syria

by Taboola

Maths Teacher Training
Qualify as a maths teacher. Register for more information.
www.education.gov.uk

Phish Your Employees
PhishMe - The Leading User Awareness Education Service
www.PhishMe.com

Cloud Security For Email
Business Solutions for Cloud Based Email Packages for Businesses Only
Mimecast.com/B2BCloudSecurity

AdChoices

Bloomberg moderates all comments. Comments that are abusive or off-topic will not be posted to the site. Excessively long comments may be moderated as well. Bloomberg cannot facilitate requests to remove comments or explain individual moderation decisions.

<:nav id=global-nav>

1 Star | More » New Suggestions

2 comments

Leave a message...

Discussion Community

<:section id=conversation data-role="main">

David_Merkel · a day ago

Don't open suspicious attachments. Use procexp to review processes. Disable processes you can't verify.

Upgrade your e-mail so that it can't be used by others without a cell phone message coming to you to verify authentiolty. Google and Yahoo offer this capability.

- 1 ^0
- Reply
- Share ›

Recommended Stories



Billionaires' Superyachts Dock In Thames for Olympics



U.S. Stocks Rally as ECB's Draghi Pledges to Defend Euro



Draghi Says ECB Will Do What's Needed to Preserve Euro; Economy



Bo Xilai Wife Charged in Poisoning Death of U.K Citizen



European Stocks Rally as Draghi Pledges to Preserve Euro



Zynga Misses Sales, Profit Estimates; Shares Slide

BLOOMBERG.COM News | Opinion | Markets | Personal Finance | Tech | Sustainability | TV | Video | Radio | Archives

ABOUT Our Company | Careers | Advertising | Press Room | Trademarks | Terms of Service | Privacy Policy

SUPPORT AND CONTACT Customer Support Contacts | Feedback | Help | Sitemap

STAY CONNECTED Twitter Facebook LinkedIn google+ StumbleUpon

RELATED BLOOMBERG SITES

Bloomberg Businessweek
Bloomberg Markets Magazine
Bloomberg Institute
Open Bloomberg
□ □□□□□□(□□□)
Bloomberg Link
□□□□(□□□)
Bloomberg Blog
□□□□□□
Bloomberg Books

BLOOMBERG PREMIUM SERVICES

Bloomberg Briefs
Bloomberg New Energy Finance
Bloomberg Government
Bloomberg Sports
Bloomberg Law
Bloomberg BNA

©2012 BLOOMBERG L.P. ALL RIGHTS RESERVED.

Bloomberg.com | Businessweek.com | Bloomberg TV | Premium | Register | Sign In

MARKET SNAPSHOT

U.S.	EUROPE	ASIA	
DJIA	13,437.80	-35.74	-0.27%
S&P 500	1,441.59	+0.11	0.01%
NASDAQ	3,063.93	-1.10	-0.04%



Our Company Professional Anywhere

Search News, Quotes and Opinion

HOME QUICK NEWS OPINION MARKET DATA PERSONAL FINANCE TECH POLITICS SUSTAINABILITY TV VIDEO RADIO


IMF Sees European Banks Facing $4.5 Trillion Sell-Off
Q


Samsung's Joke Is On Apple Fans; That a Good Idea?
Q


Noda Vows 'Decisive Action' on Yen If Needed
Q

Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy

By Vernon Silver - 2012-07-27T13:29:33Z

0 COMMENTS Q QUEUE

Gamma International GmbH's managing director said his company didn't sell its FinFisher spyware to Bahrain, responding to research that showed activists from the Persian Gulf kingdom were targeted by what looked like the software, which can secretly monitor computers.

The Munich-based executive, Martin J. Muench, said he's investigating whether the malicious software sent to activists was a demonstration copy of the product stolen from Gamma and used without permission.

Enlarge image



University of Toronto Munk School of Global Affairs' Citizen Lab security researcher Morgan Marquis-Boire. Photographer: Jacob Kepler/Bloomberg

"As you know we don't normally discuss our clients but given this unique situation it's only fair to say that Gamma has never sold their products to Bahrain," Muench said in an e-mail today.

He was responding for the first time to a July 25 report by Bloomberg News that said researchers believe they've identified copies of FinFisher, based on an examination of the malware e- mailed to Bahraini activists. Their research, published the same day by the University of Toronto Munk School of Global Affairs' Citizen Lab, was based on e-mails obtained by Bloomberg News.

Muench said his company can't yet confirm whether the software analyzed by Citizen Lab is Gamma's product.

FinFisher Portfolio

Gamma International GmbH in Germany is part of U.K.-based Gamma Group. The group also markets FinFisher through Andover, England-based Gamma International UK Ltd. Muench, 30, leads the FinFisher product portfolio.

The Citizen Lab research linked the malware sent to pro- democracy activists to FinSpy, part of the FinFisher spyware tool kit. It can secretly take remote control of a computer, copying files, intercepting Skype calls and logging every keystroke.

Based on details published by Citizen Lab, "it is unlikely that it was an installed system used by one of our clients but rather that a copy of an old FinSpy demo version was made during a presentation and that this copy was modified and then used elsewhere," Muench wrote in his e-mail.

"The modification meant that there was no message sent to our server when the demo product was used against a real target," he said. An unaltered demo would have sent a

HEADLINES | MOST POPULAR RECOMMENDED

U.S. Stocks Little Changed as Investors Weigh Earnings
Q

EADS-BAE Pull Plug on Merger After Governments Balk
Q

Facebook Fought SEC to Mute Mobile Risks Before IPO
Q

Spyware Trail Leads to Beaten Activist, Microsoft Flaw
Q

Bain Capital Buys Apex Tool Group for $1.6 Billion
Q

H&R Block Hires Goldman to Advise on Bank as Capital Rule Looms
Q

More News

Advertisement



Sponsored Links

FTTN Smart Investment
Demand for this Commodity Is Rising Fast - Get In Now, Buy Shares!
www.FirstTitanEnergy.com

First Transfer Fee Free
Great Rates on International Money Transfers. Low Fees. Big Savings.
www.UKForex.co.uk

Gas Oil Prices
Get Today's Gas Oil Prices. Fast Delivery Guaranteed.
SpeedyFuels.co.uk
AdChoices

Job Search Post a Job »

Senior Software Engineer/IT Specialist
Pacificorp - Portland, OR

IT Specialist
Wadley Regional Medical Center - Texarkana, TX

message to Gamma, and the company would have been able to deactivate that copy of the software, he said.

"I can speculate that probably the demonstration version may have been stolen using a flash drive but I have no evidence to support this," Muench said. He added that Gamma will tighten its security during presentations.

The Citizen Lab research showed the malware took screen shots, intercepted voice-over-Internet calls and transmitted a record of every keystroke to a computer in Manama, the capital of Bahrain, which has been gripped by tension since a government crackdown on protests last year.

Muench said the transmissions to Bahrain don't mean the computer ultimately receiving the data is in that country.

"It could simply be a proxy server, which most of our clients setup around the world to anonymize the created network traffic," he said.

He said in the e-mail that Gamma complies with the export regulations of the U.K., U.S. and Germany.

To contact the reporter on this story: Vernon Silver in Rome at vtsilver@bloomberg.net;

To contact the editor responsible for this story: Melissa Pozsgay at mpozsgay@bloomberg.net

More News: Europe · Germany · Middle East · Technology Industry

0 COMMENTS Q QUEUE

Bloomberg moderates all comments. Comments that are abusive or off-topic will not be posted to the site. Excessively long comments may be moderated as well. Bloomberg cannot facilitate requests to remove comments or explain individual moderation decisions.

DISQUS

Sponsored Link

FREE Bloomberg Markets Issue: The World's Richest Hedge Funds

Software Engineer
Marin Software - San Francisco, CA

Software Engineer
Act-On Software, Inc. - Beaverton, OR

IT Specialist
Symmetry Medical - Lansing, MI

Search All Jobs jobs by indeed

job title or company location Go

Advertisement



Advertisements

FOREX.com

Recommended Stories


IMF Sees European Banks Facing $4.5 Trillion Sell-Off
Q


Narula Masters Fed, Beats Funds With 500% Gain: Mortgages
Q



U.S. Stocks Little Changed as Investors Weigh Earnings
Q


'Titanic' Defaults Loom on Restructured India Bank Debt
Q


Bain Capital Buys Apex Tool Group for $1.6 Billion
Q


Nokia Pokes at Apple Maps Errors to Seek Navigation Sales
Q

©2012 BLOOMBERG L.P. ALL RIGHTS RESERVED.

Jobs by Indeed Rate this Page Made in NYC Ad Choices

Q
What is the queue?
More »Items In Your queue
This is your Bloomberg Queue
The queue will help you find news, save stories for later and take them with you
Learn MoreClose
More » New Suggestions
..

- Log In
- Register Now

- The New York Times
- Technology
- Personal Tech
- Business Day

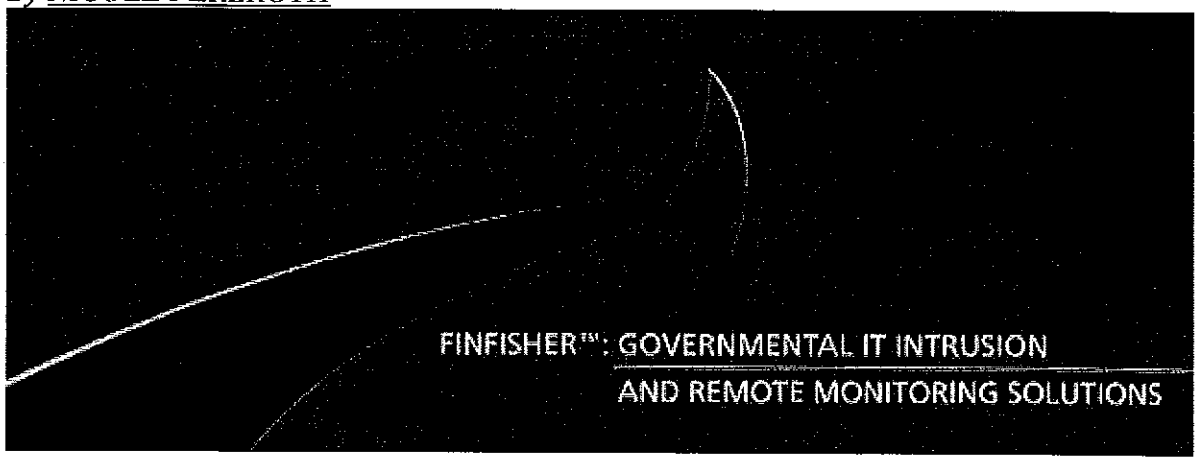
Bits

Go

August 13, 2012, *9:00 am* 18 Comments

Elusive FinSpy Spyware Pops Up in 10 Countries

By NICOLE PERLROTH



Gamma GroupGamma Group markets its FinFisher surveillance product to governments, but researchers say it may be used more broadly.

- Facebook
- Twitter
- Google+
- Save
- E-mail
- Share
- Print

It is one of the more elusive commercial cyberespionage tools available. It is marketed as a way for governments to spy on criminals. And for over a year, virus hunters unsuccessfully tried to track it down. Now it is popping up across the globe, from Qatar to an Amazon server in the United States.

FinFisher is a spyware product manufactured by the Gamma Group, a British company that sells surveillance technology. It says its spyware offers "world-class offensive techniques for information gathering." According to FinFisher's promotional materials, the spyware can be "used

to access target systems, giving full access to stored information with the ability to take control of the target system's functions to the point of capturing encrypted data and communications."

Security researchers who studied the spyware last month said it can grab images of users' computer screens, record their Skype chats, remotely turn on cameras and microphones, and log keystrokes. The Gamma Group markets FinFisher as a way for government law enforcement and intelligence agencies to keep track of criminals, but the researchers' findings suggested that it was being used more broadly.

The spyware first attracted attention in March 2011 after protesters in Egypt raided the country's state security headquarters and found an offer to buy FinFisher for 287,000 euros, or $353,000. Then in May of this year, pro-democracy Bahraini activists, one in London, another in Washington and one in the Bahraini capital, Manama, started receiving suspicious e-mails, which they passed to a Bloomberg reporter.

Bill Marczak, a computer science graduate student, and Morgan Marquis-Boire, a security researcher with the Citizen Lab of the Munk School of Global Affairs at the University of Toronto, analyzed the e-mails and found evidence that they contained FinSpy, part of the FinFisher spyware tool kit. The term "FinSpy" itself appeared in the malware's code.

The findings, published last month, suggested FinFisher technologies were being used for surveillance beyond suspected criminal activity. Martin J. Muench, the managing director of Gamma International, who develops the FinFisher line of products from Munich, did not respond to a request for comment, and a Gamma Group representative did not respond to e-mailed questions. Mr. Muench told Bloomberg that his company did not sell FinFisher spyware to Bahrain, and said the malware might have been a stolen demonstration copy or reverse-engineered by criminals.

But last week, security researchers at Rapid7, a security firm, took the earlier findings a step further. They studied the communication structure of the spyware and found that when they probed the I.P. address of a FinFisher-infected machine with unexpected data, it responded with a unique message: "Hallo Steffi."

Rapid7 scanned the Internet to see if any other I.P. addresses returned the same message and found 11 I.P. addresses in 10 other countries: Indonesia, Australia, Qatar, Ethiopia, the Czech Republic, Estonia, Mongolia, Latvia, the United Arab Emirates and the United States.

The I.P. address tied to FinFisher in the United States is hosted by EC2, Amazon's cloud storage service. Amazon did not respond to a request seeking further information about which customer was using its service to disperse the spyware. As of Monday afternoon, the spyware was still active on Amazon's service.

Security researchers say their findings contradict Mr. Muench's suggestion that the FinSpy samples they found were stolen demonstration copies or had been repurposed by criminals. For one thing, the researchers say the samples are too fully featured to be demonstration versions. For another, they questioned why a company that licenses its product at such a high cost would not have the ability to disable unauthorized copies remotely.

The researchers also said that the imbalance between the sophistication of the spyware and its distribution techniques contradicts Mr. Muench's version of events. The spyware, researchers say, is highly sophisticated, particularly in its obfuscation, which circumvents more than 40 antivirus products on the market. But the unsophisticated way in which it is distributed — in suspicious e-mails rather than through sophisticated or even well-known security exploits, and from easily traceable command-and-control servers — suggests that those who engineered the spyware are much more sophisticated than those who distributed it.

"To steal a malware sample and re-engineer it with this level of encryption requires a set of skills that didn't show up in the infection methods," said Claudio Guarnieri, a researcher from Rapid7 who studied the samples.

Researchers said it was still unclear whether the spyware was being distributed by governments. The I.P. addresses hosting FinSpy in Australia and Bahrain can be traced to Canberra and Manama, their respective capital cities, which would seem to support that claim. But the I.P. addresses in Latvia and Indonesia, for example, are not located in their capital cities.

Mr. Marquis-Boire and Mr. Marczak said they were continuing to study the Bahraini samples and look for more. "I suspect we will find a lot more," Mr. Marquis-Boire said.

-
-
-
- Save
- E-mail
- Share
- Print

Related Articles Also Tagged:

FinFisher, Finspy, Gamma Group, spyware

- **Company Denies Role in Recently Uncovered Spyware**
- **Daily Report: A Surveillance Product Is Aimed at Dissidents**
- **How Two Amateur Sleuths Looked for FinSpy Software**

- Previous Post Daily Report: Google Unveils Plans for Motorola
- Next Post Postmates Mobile Delivery App Quickly Speeds Up

18 Comments

Share your thoughts.

- All
- Reader Picks

Newest
Write a Comment

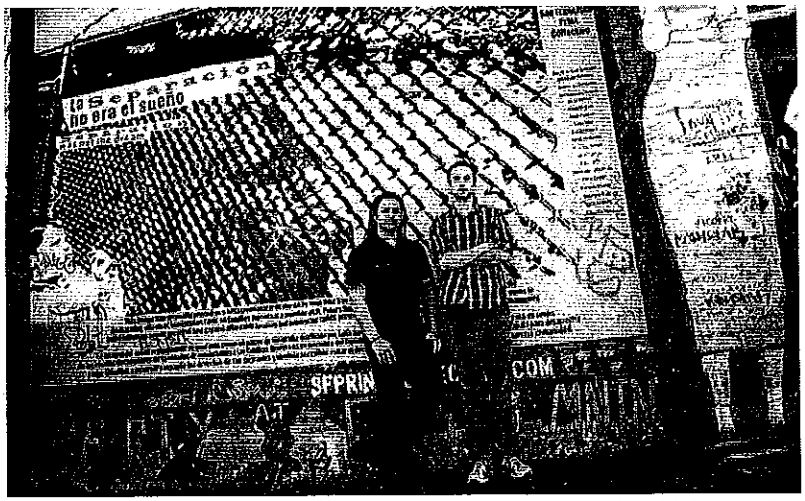
Bits Home Page »

- Previous Post Daily Report: Google Unveils Plans for Motorola
- Next Post Postmates Mobile Delivery App Quickly Speeds Up



Advertise on NYTimes.com

Software Meant to Fight Crime Is Used to Spy on Dissidents



Thor Swift for The New York Times

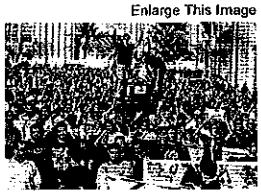
Morgan Marquis-Boire, left, and Bill Marczak have been looking at the use of computer espionage software by governments.

By NICOLE PERLROTH
Published: August 30, 2012

FACEBOOK
TWITTER
GOOGLE+
E-MAIL
SHARE
PRINT
REPRINTS

SAN FRANCISCO — Morgan Marquis-Boire works as a Google engineer and Bill Marczak is earning a Ph.D. in computer science. But this summer, the two men have been moonlighting as detectives, chasing an elusive surveillance tool from Bahrain across five continents.

Enlarge This Image



Hasan Jamali/Associated Press

Chanting antigovernment slogans, mourners escorted the body of a 16-year-old killed by security forces in Bahrain this month.

What they found was the widespread use of sophisticated, off-the-shelf computer espionage software by governments with questionable records on human rights. While the software is supposedly sold for use only in criminal investigations, the two came across evidence that it was being used to target political dissidents.

The software proved to be the stuff of a spy film: it can grab images of computer screens, record Skype chats, turn on cameras and microphones and log keystrokes. The two men said they discovered mobile versions of the spyware customized for all major mobile phones.

But what made the software especially sophisticated was how well it avoided detection. Its creators specifically engineered it to elude antivirus software made by Kaspersky Lab, Symantec, F-Secure and others.

The software has been identified as FinSpy, one of the more elusive spyware tools sold in the growing market of off-the-shelf computer surveillance technologies that give governments a sophisticated plug-in monitoring operation. Research now links it to servers in more than a dozen countries, including Turkmenistan, Brunei and Bahrain, although no government acknowledges using the software for surveillance purposes.

Log in to see what your friends are sharing on nytimes.com
Privacy Policy | What's This?
Log In With Facebook

What's Popular Now

Mr. Romney's Version of Equal Rights

Income Inequality May Take Toll on Growth



Advertise on NYTimes.com

Today's Headlines Daily E-Mail
Sign up for a roundup of the day's top stories, sent every morning.
Sign Up
See Sample | Privacy Policy

Subscribe to Technology RSS Feeds
Technology News
Internet
Start-Ups
Business Computing
Companies
Bits Blog
Personal Tech
Pogue's Posts

MOST E-MAILED
MOST VIEWED

The market for such technologies has grown to $5 billion a year from "nothing 10 years ago," said Jerry Lucas, president of TeleStrategies, the company behind ISS World, an annual surveillance show where law enforcement agents view the latest computer spyware.

FinSpy is made by the Gamma Group, a British company that says it sells monitoring software to governments solely for criminal investigations.

"This is dual-use equipment," said Eva Galperin, of the Electronic Frontier Foundation, an Internet civil liberties group. "If you sell it to a country that obeys the rule of law, they may use it for law enforcement. If you sell it to a country where the rule of law is not so strong, it will be used to monitor journalists and dissidents."

Until Mr. Marquis-Boire and Mr. Marczak stumbled upon FinSpy last May, security researchers had tried, unsuccessfully, for a year to track it down. FinSpy gained notoriety in March 2011 after protesters raided Egypt's state security headquarters and discovered a document that appeared to be a proposal by the Gamma Group to sell FinSpy to the government of President Hosni Mubarak for $353,000. It is unclear whether that transaction was ever completed.

Martin J. Muench, a Gamma Group managing director, said his company did not disclose its customers. In an e-mail, he said the Gamma Group sold FinSpy to governments only to monitor criminals and that it was most frequently used "against pedophiles, terrorists, organized crime, kidnapping and human trafficking."

In May, Mr. Marquis-Boire, 32, of San Francisco, and Mr. Marczak, 24, of Berkeley, Calif., volunteered to analyze some suspicious e-mails sent to three Bahraini activists. They discovered all the e-mails contained spyware that reported back to the same command-and-control server in Bahrain. The apparent use of the spyware to monitor Bahraini activists, none of whom had any criminal history, suggested that it had been used more broadly.

Bahrain has been increasingly criticized for human rights abuses. This month, a 16-year-old Bahraini protester was killed in what activists said was a brutal attack by security forces, but which Bahrain's government framed as self-defense.

The findings of the two men came as no surprise to those in the field. "There has been a clear increase in the availability of penetrating cyberattack tools," said Sameer Bhalotra, President Obama's former senior director for cybersecurity who now serves as the chief operating officer of Impermium, a computer security firm. "These were once the realm of the black market and intelligence agencies. Now they are emerging more and more. The problem is that it only requires small changes to apply a surveillance tool for attack, and in this case it looks like dissidents were targeted."

Since publishing their findings, Mr. Marquis-Boire and Mr. Marczak have started receiving malware samples from other security researchers and from activist groups that suspected they may have been targets. In several cases, the two found that the samples reported back to Web sites run by the Gamma Group. But other samples appeared to be actively snooping for foreign governments.

A second set of researchers from Rapid7, of Boston, scoured the Internet for links to the software and discovered it running in 10 more countries. Indeed, the spyware was running off EC2, an Amazon.com cloud storage service. Amazon did not return requests for clarification, but Mr. Marczak and Mr. Marquis-Boire said the server appeared to be a proxy, a way to conceal traffic.

Mr. Marquis-Boire said a Turkmenistan server running the software belonged to a range of I.P. addresses specifically assigned to the ministry of communications. It is the first clear-cut case of a government running the spyware off its own computer system. Human Rights Watch recently called Turkmenistan one of the "world's most repressive countries" and warned that dissidents faced "constant threat of government reprisal."

Ms. Galperin of the Electronic Frontier Foundation said, "Nobody in their right mind would claim it is O.K. to sell surveillance to Turkmenistan."

The Gamma Group would not confirm it sold software to Turkmenistan. A military attaché at the Turkmenistan Embassy in Washington refused to comment.

Mr. Muench, who for the last month has repeatedly denied that the researchers had pinpointed the company's spyware, sharply reversed course Wednesday.

In a statement released less than an hour after the researchers published their latest findings, Mr. Muench said that a Gamma Group server had been broken into and that several demonstration copies of FinSpy had been stolen.


1. WELL
Get Up. Get Out. Don't Sit.

2. Multivitamin Use Linked to Lowered Cancer Risk

3. EDITORIAL
Mr. Romney's Version of Equal Rights


4. THOMAS L. FRIEDMAN
How to Score the Debate


5. BEERS OF THE TIMES
From the White House, Beer We Can Believe In


6. FRUGAL TRAVELER
7 Manhattan Hotel Rooms for $150, More or Less


7. Small Players Seek an Alternative to the Expense of Pay-Per-Click


8. GAIL COLLINS
Women and the Men Who Yell


9. CRITIC'S NOTEBOOK
A Vision to Avoid Demolition for a '70s Pioneer

10. THE CONVERSATION
Binders, Keepers

Go to Complete List » Show My Recommendations



Female stars step off the scale

ALSO IN ARTS »
A word with Sherie Rene Scott
Anatomy of a Scene: 'Argo'

nytimes.com ARTS

ADVERTISEMENTS

WORLD OF MUSIC
TUNE IN TO THE WORLD OF MUSIC WITH ROLEX

Subscribe to the IHT ORDER NOW
International Herald Tribune

Ads by Google what's this?

Considering Public Cloud?
Don't...until you have metered your current workloads - meter free at www.cloudresourcemeter.com

LAN Network Monitoring
Monitor, Manage & Map Your Network w/ WhatsUp Gold. Try It Free!
Whatsupgold.com/LAN_Network

Download Network Monitor
Manage LAN, WAN, Bandwidth, VoIP used by over 8000 admins. Try now!
OpManager.ManageEngine.com

By Thursday afternoon, several of the FinSpy servers began to disappear, Mr. Marczak said. Servers in Singapore, Indonesia, Mongolia and Brunei went dark, while one in Bahrain briefly shut down before reincarnating elsewhere. Mr. Marquis-Boire said that as he traced spyware from Bahrain to 14 other countries — many of them "places with tight centralized control" — he grew increasingly worried about the people on the other end.

Four months in, he sounds like a man who wants to take a break, but knows he cannot just yet: "I can't wait for the day when I can sleep in and watch movies and go to the pub instead of analyzing malware and pondering the state of the global cybersurveillance industry."

A version of this article appeared in print on August 31, 2012, on page A1 of the New York edition with the headline: Software Meant to Fight Crime Is Used to Spy on Dissidents.

FACEBOOK TWITTER GOOGLE+ E-MAIL SHARE

INSIDE NYTIMES.COM

Ads by Google what's this?

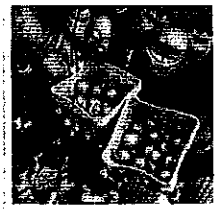
Free Log Monitoring Tool
Search, Alert and Monitor ALL
Your IT data. Free Download!
www.splunk.com/LogMonitoring

TELEVISION »



'Ethel,' a Documentary by Rory Kennedy

HOME & GARDEN »



East New York's West Indian Gardens Flourish

GREAT HOMES »



In a Walkup, the Rules of Subtraction

OPINION »

Fixes: Change's Age of Enlightenment

We're getting smarter about the way we're addressing social problems. And patterns in the most effective solutions are emerging.

FASHION & STYLE »



A Garment District With Some Big Ideas

OPINION »



Gutting: How Not to Choose a President

Home | World | U.S. | N.Y. / Region | Business | Technology | Science | Health | Sports | Opinion | Arts | Style | Travel | Jobs | Real Estate | Autos | Site Map

© 2012 The New York Times Company Privacy Your Ad Choices Terms of Service Terms of Sale Corrections RSS Help Contact Us Work With Us Advertise