FinFisher

By Contributors to Wikimedia projects

Published: 2011-11-28 · Archived: 2026-04-05 12:52:47 UTC

From Wikipedia, the free encyclopedia

Suspected FinFisher government users that were active at some point in 2015.

FinFisher, also known as **FinSpy**,[1] is surveillance software marketed by Lench IT Solutions plc, which markets the spyware through law enforcement channels.[1]

FinFisher can be covertly installed on targets' computers by exploiting security lapses in the update procedures of non-suspect software.[2][3][4] The company has been criticized by human rights organizations for selling these capabilities to repressive or non-democratic states known for monitoring and imprisoning political dissidents.[5] Egyptian dissidents who ransacked the offices of Egypt's secret police following the overthrow of Egyptian President Hosni Mubarak reported that they had discovered a contract with Gamma International for €287,000 for a license to run the FinFisher software.[6] In 2014, an American citizen sued the Ethiopian government for surreptitiously installing FinSpy onto his computer in America and using it to wiretap his private Skype calls and monitor his entire family's every use of the computer for a period of months.[7][8]

Lench IT Solutions plc has a UK-based branch, Gamma International Ltd in Andover, England, and a Germany-based branch, Gamma International GmbH in Munich.[9][10] Gamma International is a subsidiary of the Gamma Group, specializing in surveillance and monitoring, including equipment, software, and training services.[9] It was reportedly owned by William Louthean Nelson through a shell corporation in the British Virgin Islands.[11] The shell corporation was signed by a nominee director in order to withhold the identity of the ultimate beneficiary, which was Nelson, a common system for companies that are established offshore.[12]

On August 6, 2014, FinFisher source code, pricing, support history, and other related data were leaked after the Gamma International internal network was hacked by Phineas Fisher.[13]

The FinFisher GmbH opened insolvency proceedings at the Munich Local Court on 02.12.2021,[14] however this is only a restructuring and the company is to continue as Vilicius Holding GmbH.[15]

Elements of the FinFisher suite

[edit]

In addition to spyware, the FinFisher suite offered by Gamma to the intelligence community includes monitoring of ongoing developments and updating of solutions and techniques which complement those developed by intelligence agencies.[16] The software suite, which the company calls "Remote Monitoring and Deployment Solutions", has the ability to take control of target computers and to capture even encrypted data and communications. Using "enhanced remote deployment methods" it can install software on target computers.[17] An "IT Intrusion Training Program" is offered which includes training in methods and techniques and in the use of the company-supplied software.[18]

The suite is marketed in Arabic, English, German, French, Portuguese, and Russian and offered worldwide at trade shows offering an intelligence support system, ISS, training, and products to law enforcement and intelligence agencies.[19]

Method of infection

[edit]

FinFisher malware is installed in various ways, including fake software updates, emails with fake attachments, and security flaws in popular software. Sometimes the surveillance suite is installed after the target accepts installation of a fake update to commonly used software.[2] Code which will install the malware has also been detected in emails.[20] The software, which is designed to evade detection by antivirus software, has versions which work on mobile phones of all major brands.[1]

A security flaw in Apple's iTunes allowed unauthorized third parties to use iTunes online update procedures to install unauthorized programs.[3][4] Gamma International offered presentations to government security officials at security software trade shows where they described how to covertly install the FinFisher spy software on suspects' computers using iTunes' update procedures.

The security flaw in iTunes that FinFisher is reported to have exploited was first described in 2008 by security software commentator Brian Krebs.[3][4][21] Apple did not patch the security flaw for more than three years, until November 2011. Apple officials have not offered an explanation as to why the flaw took so long to patch. Promotional videos used by the firm at trade shows which illustrate how to infect a computer with the surveillance suite were released by WikiLeaks in December 2011.[10]

In 2014, the Ethiopian government was found to have installed FinSpy on the computer of an American citizen via a fake email attachment that appeared to be a Microsoft Word document.[7]

FinFisher has also been found to engage in politically motivated targeting. In Ethiopia, for instance, photos of a political opposition group are used to "bait" and infect users.[5][*dead link*]

Technical analysis of the malware, methods of infection and its persistence techniques has been published in Code And Security blog in four parts.[22]

Use by repressive regimes

[edit]

- FinFisher's wide use by governments facing political resistance was reported in March 2011 after Egyptian protesters raided State Security Investigations Service and found letters from Gamma International UK Ltd., confirming that SSI had been using a trial version for five months.[23]
- A similar report in August 2012 concerned e-mails received by Bahraini activists and passed on (via a Bloomberg News reporter) to University of Toronto computer researchers Bill Marczak and Morgan Marquis-Boire in May 2012. Analysis of the e-mails revealed code (FinSpy) designed to install spyware on the recipient's computer.[1][20] A spokesman for Gamma claims no software was sold to Bahrain and that the software detected by the researchers was not a legitimate copy but perhaps a stolen, reverse-engineered or modified demonstration copy.[24] In August 2014 Bahrain Watch claimed that the leak of FinFisher data contained evidence suggesting that the Bahraini government was using the software to spy on opposition figures, highlighting communications between Gamma International support staff and a customer in Bahrain, and identifying a number of human rights lawyers, politicians, activists and journalists who had apparently been targeted.[25]
- According to a document dated 7 December 2012 from the Federal Ministry of the Interior to members of the Finance Committee of the German Parliament, the German "Bundesnachrichtendienst", the Federal Surveillance Agency, have licensed FinFisher/FinSpy, even though its legality in Germany is uncertain.[26]
- In 2014, an America citizen sued the Ethiopian government for installing and using FinSpy to record a vast array of activities conducted by users of the machine, all whilst in America. Traces of the spyware inadvertently left on his computer show that information – including recordings of dozens of Skype phone calls – was surreptitiously sent to a secret control server located in Ethiopia and controlled by the Ethiopian government. FinSpy was downloaded on the plaintiff's computer when he opened an email with a Microsoft Word document attached. The attachment contained hidden malware that infected his computer.[7] In March 2017, the United States Court of Appeals for the District of Columbia Circuit found that the Ethiopian government's conduct was protected from liability by the Foreign Sovereign Immunities Act.[27][28]
- In 2015, FinFisher was reported to have been in use since 2012 for the 'Fungua Macho' surveillance programme of Uganda's President Museveni, spying upon the Ugandan opposition party, the Forum for Democratic Change.[29]
- In 2015 it is reported that FinFisher executives sold, illegally, the system to Turkey to enable their security services to spy on government opposition parties. Four former executives were charged in 2023 in Munich with failure to apply for an export licence for the $5.4 million contract.[30]

Reporters Without Borders

[edit]

On 12 March 2013 Reporters Without Borders named Gamma International as one of five "Corporate Enemies of the Internet" and “digital era mercenaries” for selling products that have been or are being used by governments to

violate human rights and freedom of information. FinFisher technology was used in Bahrain and Reporters Without Borders, together with Privacy International, the European Center for Constitutional and Human Rights (ECCHR), the Bahrain Centre for Human Rights, and Bahrain Watch filed an Organisation for Economic Co-operation and Development (OECD) complaint, asking the National Contact Point in the United Kingdom to further investigate Gamma's possible involvement in Bahrain. Since then research has shown that FinFisher technology was used in Australia, Austria, Bahrain, Bangladesh, Britain, Brunei, Bulgaria, Canada, the Czech Republic, Estonia, Ethiopia, Germany, Hungary, India, Indonesia, Japan, Latvia, Lithuania, North Macedonia, Malaysia, Mexico, Mongolia, Netherlands, Nigeria, Pakistan, Panama, Qatar, Romania, Serbia, Singapore, South Africa, Turkey, Turkmenistan, the United Arab Emirates, the United States, Venezuela and Vietnam.[9][10][31][32][33]

Firefox masquerading

[edit]

FinFisher is capable of masquerading as other more legitimate programs, such as Mozilla Firefox. On April 30, 2013, Mozilla announced that they had sent Gamma a cease-and-desist letter for trademark infringement.[34] Gamma had created an espionage program that was entitled firefox.exe and even provided a version number and trademark to appear to be legitimate Firefox software.[35]

In an article of *PC Magazine*, Bill Marczak (member of Bahrain Watch and computer science PhD student at University of California, Berkeley doing research into FinFisher) said of FinSpy Mobile (Gamma's mobile spyware): "As we saw with respect to the desktop version of FinFisher, antivirus alone isn't enough, as it bypassed antivirus scans".[36] The article's author Sara Yin, an analyst at *PC Magazine*, predicted that antivirus providers are likely to have updated their signatures to detect FinSpy Mobile.[36]

According to announcements from ESET, FinFisher and FinSpy are detected by ESET antivirus software as "Win32/Belesak.D" trojan.[37][38]

Other security vendors claim that their products will block any spyware they know about and can detect (regardless of who may have launched it), and Eugene Kaspersky, head of IT security company Kaspersky Lab, stated, "We detect all malware regardless its purpose and origin".[39] Two years after that statement by Eugene Kaspersky in 2012 a description of the technique used by FinFisher to evade Kaspersky protection was published in Part 2 of the relevant blog at Code And Security.

FinFisher has also made headlines in the past because its products were found to be used by authoritarian regimes against opponents in several Middle Eastern countries.[40]

- Computer and Internet Protocol Address Verifier (CIPAV)
- Duqu
- Flame (malware)
- Hacking Team
- Mahdi (malware)
- MiniPanzer and MegaPanzer

- NSA ANT catalog
- R2D2 (trojan)
- Stuxnet
- Tailored Access Operations

1. ^ Jump up to: *a* *b* *c* *d* *Nicole Perlroth (August 30, 2012). "Software Meant to Fight Crime Is Used to Spy on Dissidents". The New York Times. Archived from the original on August 31, 2012. Retrieved August 31, 2012.*
2. ^ Jump up to: *a* *b* *Jennifer Valentino-Devries (2011-11-21). "Surveillance Company Says It Sent Fake iTunes, Flash Updates". The Wall Street Journal. Archived from the original on 2011-11-30. Retrieved 2011-11-28. "Perhaps the most extensive marketing materials came from Gamma's FinFisher brand, which says it works by "sending fake software updates for popular software," from Apple, Adobe and others. The FinFisher documentation included brochures in several languages, as well as videos touting the tools."*
3. ^ Jump up to: *a* *b* *c* *Christopher Williams (2011-11-24). "Apple iTunes flaw 'allowed government spying for 3 years'". The Daily Telegraph. Archived from the original on 2011-11-27. Retrieved 2011-11-28. "A British company called Gamma International marketed hacking software to governments that exploited the vulnerability via a bogus update to iTunes, Apple's media player, which is installed on more than 250 million machines worldwide."*
4. ^ Jump up to: *a* *b* *c* *Marcel Rosenbach (2011-11-22). "Firm Sought to Install Spyware Via Faked iTunes Updates". Der Spiegel. Archived from the original on 2011-11-27. Retrieved 2011-11-28. "Apparently, at least according to a video promoting FinFisher, the software uses Apple's popular iTunes in order to load snooping software onto the computers of the intended suspects."*
5. ^ Jump up to: *a* *b* *Marquis-Boire, Morgan (13 March 2013). "You Only Click Twice: FinFisher's Global Proliferation". University of Toronto Citizen Lab. Archived from the original on 9 August 2014. Retrieved 3 August 2014.*
6. ^ *John Leyden (2011-09-21). "UK firm denies supplying spyware to Mubarak's secret police: RATs nest found in Egyptian spook HQ". The Register. Archived from the original on 2011-11-27. Retrieved 2011-11-28. "Documents uncovered when the country's security service headquarters were ransacked during the Arab Spring uprising suggest that Egypt had purchased a package called FinFisher to spy on dissidents."*
7. ^ Jump up to: *a* *b* *c* *Kopfstein, Janus (March 10, 2014). "Hackers Without Borders". The Washington Post. Archived from the original on August 26, 2014. Retrieved August 24, 2014.*
8. ^ *"American Sues Ethiopian Government for Spyware Infection". Electronic Frontier Foundation. February 18, 2014. Archived from the original on 2014-10-03. Retrieved 2014-08-24.*
9. ^ Jump up to: *a* *b* *c* "Corporate Enemies: Gamma International" Archived 2013-03-16 at the Wayback Machine, *The Enemies of the Internet, Special Edition: Surveillance*, Reporters Without Borders, 12 March 2013.
10. ^ Jump up to: *a* *b* *c* *Vernon Silver (July 25, 2012). "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma". Bloomberg. Archived from the original on August 10, 2012. Retrieved August 31, 2012.*
11. ^ *"Offshore company directors' links to military and intelligence revealed". the Guardian. 2012-11-28. Retrieved 2022-03-28.*
12. ^ *"The 2014 FinFisher Leaks were a precursor to both Vault 7 and Panama Papers". wikileaksdecrypted.com. Archived from the original on 2017-03-28. Retrieved 2017-03-27.*

13. ^ *Andre Meister (August 6, 2014). "Gamma FinFisher hacked: 40 GB of internal documents and source code of government malware published". Netzpolitik.org. Archived from the original on August 6, 2014. Retrieved August 6, 2014.*
14. ^ *"Unternehmensregister". www.unternehmensregister.de. Archived from the original on 2021-12-10. Retrieved 2021-12-10. "Unternehmensregister". Archived from the original on 2021-12-10. Retrieved 2021-12-10.*
15. ^ *"Spyware Finfisher nach Namenswechsel bei neuer Holding Vilicius". heise online (in German). 10 December 2021. Archived from the original on 2021-12-11. Retrieved 2021-12-11.*
16. ^ *"Portfolio". FinFisher IT Intrusion. Gamma Group. Archived from the original on May 8, 2012. Retrieved August 31, 2012. "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." "FinFisher IT Intrusion :: Portfolio". Archived from the original on May 8, 2012. Retrieved August 31, 2012.*
17. ^ *"Portfolio". FinFisher IT Intrusion. Gamma Group. Archived from the original on May 8, 2012. Retrieved August 31, 2012. "The Remote Monitoring and Deployment Solutions are used to access target Systems to give full access to stored information with the ability to take control of target systems' functions to the point of capturing encrypted data and communications. When used in combination with enhanced remote deployment methods, the Government Agencies will have the capability to remotely deploy software on target systems." "FinFisher IT Intrusion :: Portfolio". Archived from the original on May 8, 2012. Retrieved August 31, 2012.*
18. ^ *"Portfolio". FinFisher IT Intrusion. Gamma Group. Archived from the original on May 8, 2012. Retrieved August 31, 2012. "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 endusers, thus maximizing their capabilities in this field." "FinFisher IT Intrusion :: Portfolio". Archived from the original on May 8, 2012. Retrieved August 31, 2012.*
19. ^ *"News". Gamma Group. Archived from the original on October 4, 2012. Retrieved August 31, 2012. "FinFisher IT Intrusion :: News". Archived from the original on October 4, 2012. Retrieved August 31, 2012.*
20. ^ Jump up to: ***a*** ***b*** *Nicole Perlroth (August 13, 2012). "Elusive FinSpy Spyware Pops Up in 10 Countries" (blog by reporter). The New York Times. Archived from the original on August 18, 2012. Retrieved August 31, 2012.*
21. ^ *Brian Krebs (2011-11-23). "Apple Took 3+ Years to Fix FinFisher Trojan Hole". Krebs on Security. Archived from the original on 2011-11-26. Retrieved 2011-11-28. "I first wrote about this vulnerability for The Washington Post in July 2008, after interviewing Argentinian security researcher Francisco Amato about "Evilgrade," a devious new penetration testing tool he had developed."*
22. ^ *Coding and Security (2014-09-19). "FinFisher Malware Analysis and Technical Write-up". Coding and Security. Archived from the original on 2016-03-06. Retrieved 2014-09-19. "Detailed analysis of all components of FinFisher malware"*
23. ^ *"Restrictions on freedom of communication". shorouknews.com (in Arabic). Sunrise Gateway. Archived from the original on 25 March 2014. Retrieved 25 March 2014.*

24. ^ *Vernon Silver (July 27, 2012). "Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy". Bloomberg News. Archived from the original on July 31, 2012. Retrieved August 31, 2012.*
25. ^ *Desmukh, Fahad (7 August 2014). "Bahrain Government Hacked Lawyers and Activists with UK Spyware". Bahrain Watch. Archived from the original on 15 August 2014. Retrieved 22 August 2014.*
26. ^ *Andre Meister (16 January 2013). "Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware". Netzpolitik.org. Archived from the original on 28 July 2013. Retrieved 19 July 2013.*
27. ^ *Note, Recent Case: D.C. Circuit Finds Ethiopia Immune in Hacking Suit, 131 Harv. L. Rev. 1179 (2018).*
28. ^ *Doe v. Federal Democratic Republic of Ethiopia*, 851 F.3d 7 (D.C. Cir. 2017), archived from the original.
29. ^ *Nick Hopkins; Jake Morris (15 October 2015). "UK firm's surveillance kit 'used to crush Uganda opposition'". BBC News Online. Archived from the original on 22 August 2018. Retrieved 21 June 2018.*
30. ^ *"Germany charges four for selling spyware to Turkey". 22 May 2023. Archived from the original on 23 May 2023. Retrieved 23 May 2023.*
31. ^ "FinFisher Mobile Spyware Tracking Political Activists" Archived 2013-05-17 at the Wayback Machine, Mathew J. Schwartz, *Information Week*, 31 August 2012
32. ^ "Researchers Find 25 Countries Using Surveillance Software" Archived 2013-03-14 at the Wayback Machine, Nicole Perlroth, *The New York Times*, 15 March 2013
33. ^ "For Their Eyes Only: The Commercialization of Digital Spying" Archived 2013-05-04 at the Wayback Machine, Morgan Marquis-Boire with Bill Marczak, Claudio Guarnieri, and John Scott-Railton, Citizen Lab and Canada Centre for Global Security Studies, Munk School of Global Affairs, University of Toronto, 1 May 2013
34. ^ "Protecting our brand from a global spyware provider" Archived 2013-05-02 at the Wayback Machine, Mozilla Foundation, April 30, 2013
35. ^ *"June, Daniel, "Mozilla Fights Against Spyware Company and its Exploits"". May 2013. Archived from the original on 2013-07-03. Retrieved 2013-05-08.*
36. ^ Jump up to: ***a*** ***b*** *Sara Yin (August 30, 2012). "Lessons Learnt From FinFisher Mobile Spyware". PC Magazine. Archived from the original on September 3, 2012. Retrieved September 3, 2012.*
37. ^ *Cameron Camp (August 31, 2012). "FinSpy and FinFisher spy on you via your cellphone and PC, for good or evil?". WeLiveSecurity. Archived from the original on October 5, 2017. Retrieved July 25, 2017.*
38. ^ *David Harley (August 31, 2012). "Finfisher and the Ethics of Detection". WeLiveSecurity. Archived from the original on December 22, 2017. Retrieved July 25, 2017.*
39. ^ *Mathew J. Schwartz (August 31, 2012). "FinFisher Mobile Spyware Tracking Political Activists". Information Week. Archived from the original on October 13, 2013. Retrieved September 3, 2012.*
40. ^ *"German prosecutors investigate spyware maker FinFisher | DW | 05.09.2019". Dawn. September 5, 2019. Archived from the original on September 6, 2019. Retrieved September 5, 2019.*

Media related to FinFisher at Wikimedia Commons

- Official website
