IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Newport News Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 4:16cr16
	)	
EDWARD JOSEPH MATISH, III	)	

DECLARATION OF DR. CHRISTOPHER SOGHOIAN

I, Christopher Soghoian, declare the following under penalty of perjury:

1. I am a researcher focused on privacy, computer security and government surveillance. I completed a B.S. in Computer Science from James Madison University, a M.S. in Security Informatics from The Johns Hopkins University and a Ph.D. in Informatics from Indiana University. My academic research has been published in a number of law journals, and has been cited by several federal and state courts, including by the 9th Circuit Court of Appeals and the State Supreme Courts of New Jersey and Massachusetts.[1]

2. I am currently employed by the American Civil Liberties Union as the Principal Technologist in the ACLU's Speech, Privacy and Technology Project. I am also a visiting fellow at Yale Law School's Information Society Project. I have previously worked in technical roles at the Federal Trade Commission, Google, Apple, and IBM. I have written this declaration as an unpaid volunteer expert for the defense and submit it to the court in my personal capacity, not on behalf of my employer.

3. I have researched the FBI's use of Network Investigative Techniques ("NITs") for more than three years. In 2014, I organized the first-ever academic conference in the United States focused on hacking by law enforcement, held at Yale Law School.[2] I have given several public talks about the use of hacking and malware by the FBI, including at training events for federal judges organized by the Federal Judicial Center.

[1] *See US v. Pineda-Moreno*, 617 F. 3d 1120, Court of Appeals, 9th Circuit 2010 (Kozinski dissental), *State v. Earls*, 70 A. 3d 630 - NJ: Supreme Court 2013 and *Commonwealth v. Augustine*, 467 Mass. 230 - Mass: Supreme Judicial Court 2014.

[2] *See* Law Enforcement and Hacking, Information Society Project, Yale Law School, February 18, 2014, videos online at https://www.law.yale.edu/yls-today/yale-law-school-videos/hacking-technologies-used-law-enforcement and https://www.law.yale.edu/yls-today/yale-law-school-videos/legal-and-policy-implications-hacking-law-enforcement .

4. In 2014, while researching the history of FBI hacking, I discovered that in a 2007 operation, FBI agents impersonated the Associated Press in an effort to deliver surveillance software to a teenager in Timberline, Washington. My subsequent public disclosure of this information resulted in significant news coverage, a formal complaint to the Attorney General from twenty-five news organizations,[3] a Congressional probe into the incident,[4] and a public defense of the practice by the FBI Director.[5]

Network Investigative Techniques

5. As Special Agent Alfin's declaration makes clear, there is some disagreement between Michaud's technical experts and the FBI about what a NIT is and is not. There is also clear disagreement about whether or not a NIT is "malware".

6. The term "Network Investigative Technique" was created by the US government. While researching the history of NITs, I was informed by a senior DOJ official that the term originated in the Computer Crime and Intellectual Property Section within DOJ's Criminal Division.

7. Outside of the law enforcement community, a number of terms of art are used by technical security experts to describe software that is installed without the knowledge and consent of a computer user, and that covertly extracts information from that person's computer. These terms include "malware," "surveillance software," and "Remote Administration Tools" (RATs). These terms are all functionally equivalent.

8. In his declaration, Special Agent Alfin suggests, without citing any supporting evidence, that an essential component of malware is that the software must make permanent changes to the security settings of the target computer.[6] I disagree with this statement.

9. The Ninth Circuit Court of Appeals has described malware as software that "works by, for example, compromising a user's privacy… stealing identities, or spontaneously opening Internet links to unwanted websites…." *See Zango v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009)*. Like the malware in *Zango,* the NIT used by the FBI in the Playpen

[3] *See* The Reporters Committee for Freedom of the Press *et al.*, Letter to Eric H. Holder, Jr. and James B. Comey, Jr., November 6, 2014, http://www.rcfp.org/sites/default/files/2014-11-06-letter-to-doj-fbi-regarding-se.pdf
[4] *See* Senator Patrick Leahy, Letter to Eric Holder Jr., October 30, 2014, http://thehill.com/sites/default/files/10-30-14_leahy_to_holder_re_-_fbi_fake_ap_article.pdf.
[5] See James B. Comey, To Catch a Crook: The F.B.I.'s Use of Deception (Letter To The Editor), New York Times, November 5, 2014, http://www.nytimes.com/2014/11/07/opinion/to-catch-a-crook-the-fbis-use-of-deception.html
[6] *See* Alfin Declaration, paragraph 6, page 2.

investigation compromised the privacy and anonymity of the individuals that visited the site, and forced their web browsers to connect to an unwanted site (the FBI's server in Virginia).

10. The capabilities of NITs used by the FBI in other cases include identical surveillance features as malware used by criminals and foreign governments. These capabilities include being able to remotely activate the webcam and microphone on a victim's computer.[7]

11. The FBI has used the same methods as those used by criminal hackers and foreign governments to deliver malware to targets. This includes the impersonation of journalists[8] and the delivery of malware to large numbers of visitors to a particular website (a technique that experts call a "watering hole attack").[9]

12. The primary difference between the FBI's NITs and the malware used by hackers and authoritarian foreign governments appears to be that the FBI's software is used pursuant to court orders issued by a court in the United States. From a technical perspective, the NIT is still malware.

---

[7] Compare the features of BlackShades, a malware tool used by criminals to the capabilities of the NIT software used by the FBI. *See US v. Yücel*, 97 F. Supp. 3d 413 - Dist. Court, SD New York 2015 ("The malware included a remote access tool ('RAT'), which enabled users 'to remotely control victims' computers, including [by] captur[ing] the victims' keystrokes as they type'—the 'keylogger' function— 'turn[ing] on their webcams, and search[ing] through their personal files.'") *See also* Ellen Nakashima and Craig Timberg, FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance, Washington Post, December 6, 2013 ("The most powerful FBI surveillance software can covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers, say court documents and people familiar with this technology.")

[8] *See* Bill Marczak and John Scott-Railton, Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents, Citizen Lab, Munk School of Global Affairs, The University of Toronto, May 29, 2016, https://citizenlab.org/2016/05/stealth-falcon/ (describing attempts by an entity, believed to be the government of the United Arab Emirates, attemping to deliver malware to dissidents by pretending to be a fictious journalis).

[9] *See* Michael Mimoso, Council on Foreign Relations Website Hit By Watering Hole Attack, IE Zero-Day Exploit, Threatpost, December 29, 2012, https://threatpost.com/council-foreign-relations-website-hit-watering-hole-attack-ie-zero-day-exploit-122912/77352/ . The Department of Justice has taken the position that bulk delivery of NITs in operations like Playpen are not watering hole attacks. As with the question of whether a NIT is malware, the Department of Justice and the technical community do not see eye to eye. *See* David Bitkower, Deputy Assistant Attorney General, Memorandum to Reena Raggi, Chair, Advisory Committee on Criminal Rules, December 22, 2014 http://www.uscourts.gov/file/17944/download at 145 ("The ACLU calls this technique a 'watering hole attack' and suggests that it may violate the Fourth Amendment... The Department disagrees both with that label and with the legal conclusion.")

The Importance Of Encryption

13. When an individual browses the web, data that is transmitted from their computer to the websites they visit must pass through communications networks and networking equipment run by a number of Internet Service Providers. These Internet Service Providers all have the ability to inspect and modify that data as it passes through their network. Internet Service Providers may modify the contents of web pages that are being delivered through their network, in order to to inject advertisements or to facilitate advertising-related tracking of their customers.[10]

14. In addition to the authorized parties that can intercept and tamper with data as it flows over the Internet, authorized parties can do so too, if they have hacked into a server or network that the data passes through. For example, journalists relying on documents from NSA whistleblower Edward Snowden have revealed that Britain's signals intelligence agency hacked into a number of Belgian and German communications networks in order to intercept the communications that flowed through those networks.[11]

15. When individuals use an open, or poorly secured, WiFi network, it is trivially easy for hackers in the vicinity to inspect and modify data that is being transmitted over that WiFi network.[12]

16. In order to protect their customers from a number of privacy and cybersecurity threats, including the interception and tampering of private user data, many major Internet companies use an encrypted connection to protect data that is transmitted to and from their

[10] *See* Gabi Nakibly *et al.*, Website-Targeted False Content Injection by Network Operators, 25th USENIX Security Symposium,, August, 2016, http://www.cs.technion.ac.il/~gnakibly/papers/arXiv1602.07128.pdf. *See also* Nate Anderson, How a banner ad for H&R Block appeared on apple.com—without Apple's OK, Ars Technica, April 8, 2013, http://arstechnica.com/tech-policy/2013/04/how-a-banner-ad-for-hs-ok/. *See also In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, Federal Communications Commission, March 7, 2016, EB-TCD-14-00017601, https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf (describing Verizon's injection of unique tracking IDs into mobile users' web browsing traffic).

[11] See Ryan Gallagher, Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, The Intercept, December 13, 2014, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/. See also Andy Müller-Maguhn *et al.*, Map Of The Stars: The NSA and GCHQ Campaign Against German Satellite Companies, The Intercept, September 14, 2014, https://theintercept.com/2014/09/14/nsa-stellar/.

[12] *See* Kate Murphy, New Hacking Tools Pose Bigger Threats to Wi-Fi Users, New York Times, February 16, 2011, http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html.

websites. This encryption technology, known as HTTPS, is displayed to the user as a lock icon in a web browser.

17. Encryption typically provides three security benefits: Confidentiality, Integrity and Authentication. What this means is that when a software client (such as a web browser) uses encryption to protect data that is transmitted to a server (such as a web site), encryption protects that data from interception by third parties (confidentiality), it ensures that the client and server will know if a third party has tampered with the data as it is transmitted between them (integrity), and can permit the client and server to be confident that they are talking to each other and not an imposter (authentication).

18. In his declaration, Special Agent Alfin confirms that the NIT used by the FBI in the Playpen operation did not use an encrypted connection to transmit data from the target computers back to the FBI server.[13]

19. Because the FBI's NIT did not use encryption, the data that was transmitted by the NIT to the FBI's server was vulnerable to both interception and tampering by third parties as it was transmitted over the Internet.

20. That the FBI did not use encryption to protect data transmitted between the NIT and the FBI's server is in direct conflict with industry cybersecurity best practices and US government policy.[14]

21. Senior federal officials including the FBI Director have, for nearly half a decade, stressed the importance of using encryption to protect data that is transmitted over the internet.[15]

---

[13] *See* Alfin Declaration, paragraph 28, page 6.
[14] *See* Tony Scott, Policy to Require Secure Connections across Federal Websites and Web Services, infra fn X.
[15] *See* Pamela Jones Harbour, Remarks Before Third FTC Exploring Privacy Roundtable Washington, D.C, March 17, 2010, https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-third-federal-trade-commission-exploring-privacy-roundtable/100317privacyroundtable.pdf ("[Security needs to be a default in the cloud. Today, I challenge all of the companies that are not yet using [HTTPS] by default. That includes all email providers, social networking sites, and any website that transmits consumer data. Step up and protect consumers. Don't do it just some of the time. Make your websites secure by default.") See also Lance Whitney, Senator wants more secure Web sites for Wi-Fi use, CNET News, February 28, 2011, https://www.cnet.com/news/senator-wants-more-secure-web-sites-for-wi-fi-use/. *See also* James B. Comey, Statement Before the House Judiciary Committee Washington, D.C. March 01, 2016, https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy (Encryption is a "key tool to secure commerce and trade, safeguard private information ... and strengthen cyber security").

22. In 2015, the White House announced a new Office of Management and Budget policy requiring all federal agencies to encrypt their websites by the end of 2016.[16] Both the FBI and DOJ websites have since enabled encryption by default.

23. As the FBI did not use encryption to protect the connection between the NIT and the FBI's server, the agency has no way to be sure that the data collected by the NIT was not tampered with by third parties as it was transmitted over the internet to the FBI's server.

24. The integrity protection provided by encryption can be thought of as similar to the role of a tamper-evident seal in an evidence bag used by law enforcement. The digital evidence bag that the FBI used to transmit NIT data was neither signed nor sealed, and the FBI has no way of knowing what happened to the evidence before it reached the FBI's server.

The Network Data Stream

25. The government has offered to permit the defense to examine a copy of the "two-way network data stream", which Special Agent Alfin states "reflect[s] the information transmitted to the FBI from Matish's computer."[17] Special Agent Alfin's description is incorrect. As the network data stream was recorded at an FBI facility, the stream reflects the information received by the FBI, not the information transmitted by the NIT. As the NIT did not use an encrypted connection, the data sent by the NIT may have been modified in transit, and as a result, the data received by the FBI may be different than the data transmitted by the NIT.

26. The network data stream is not evidence of a chain of custody of the data transmitted by the NIT, nor would examining it reveal if any of the data transmitted by the NIT was tampered with as it was transmitted over the Internet to the FBI's server.

27. The network data stream is akin to a video recording of a forensic scientist at a FBI crime lab opening up an evidence bag and testing the evidence inside. However, if the bag was

[16] *See* Tony Scott, HTTPS-Everywhere for Government, White House Blog, June 8, 2015, https://www.whitehouse.gov/blog/2015/06/08/https-everywhere-government. *See also* Tony Scott, Policy to Require Secure Connections across Federal Websites and Web Services, Memorandum For the Heads of executive departments and agencies, Office of Management and Budget, June 8, 2015, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf.
[17] *See* Alfin Declaration, paragraph 16, page 3.

not sealed, the video footage can only show that the evidence was appropriately handled once it was received by the crime lab, not what may have happened to the evidence between the time when it was placed in the evidence bag and the time that it was received by the crime lab.

28. In his declaration, Special Agent Alfin states that the fact that the FBI's NIT did not use an encrypted connection is actually a good thing, as it enabled the FBI to capture a copy of the network data stream:

> "In fact, the network data stream that has been made available for defense review would be of no evidentiary value had it been transmitted in an encrypted format. Because the data is not encrypted, Matish can analyze the data stream and confirm that the data collected by the government is within the scope of the search warrant that authorized the use of the NIT. Had the data been transmitted in an encrypted format the data stream would be of no evidentiary value as it could not be analyzed."[18]

29. Special Agent Alfin's statement is incorrect. The FBI could have encrypted the connection between the NIT and the FBI's server, while also being able to capture a forensically valid copy of the network data stream.[19]

The Importance of the Exploit Code

30. Engineers routinely make mistakes when designing software and inadvertently introduce software flaws into the code they write. These flaws can, in some cases, be exploited by third parties to gain or exceed authorized access to a computer without the knowledge or consent of the user.

31. It is extremely difficult to write software without exploitable security flaws. Large, respected software companies like Google and Microsoft employ hundreds of engineers focused on computer security yet exploitable security flaws are regularly found in their products.

---

[18] *See* Alfin Declaration, paragraph 28, page 6.

[19] For example, the FBI could have used a termination proxy, so that the connection between the NIT and the FBI's network would be encrypted, after which, the data could flow unencrypted over the FBI's internal network to the NIT server. The network data stream could be captured either on the NIT server itself, or from another device inside the FBI's network.

32. Security researchers regularly discover software security flaws in all kinds of software, including web browsers, word processing programs, operating systems, and even government-grade malware. For example, in 2011, computer security experts discovered exploitable security flaws in surveillance software used by the German police that left systems that were being remotely monitored by the German authorities vulnerable to unauthorized access by third parties.[20]

33. Although it is perhaps possible that the government contractors who created the software exploit and NIT software for the FBI wrote perfect, flaw-free code, it is extremely unlikely. Moreover, the fact that the NIT did not use an encrypted connection to transmit data back to the FBI strongly suggests that the developers who wrote the software did not follow other industry best practices.

34. Special Agent Alfin states in his declaration that while "it is theoretically possible for an exploit to make fundamental changes or alterations to a computer system … the NIT used here and the exploit used to deliver it did not."[21] Even if the FBI did not *intend* to make any permanent modifications to the computers targeted in the Playpen investigation or leave those systems open to compromise by third parties, it is possible that design flaws in the FBI's software may have inadvertently modified the defendant's computer system or otherwise left it in a vulnerable state. To determine what, if any, modifications were made to the defendant's computer system and the state in which it was likely left by the FBI, the defense must be able to examine all of the FBI code that the defendant's computer executed (that is, both the exploit code and the NIT).

DONE this 10th day of June, 2016.

Christopher Soghoian

Christopher Soghoian

[20] *See* Chaos Computer Club analyzes government malware, October 8, 2011, http://ccc.de/en/updates/2011/staatstrojaner.

[21] *See* Alfin Declaration, paragraph 14, page 3.