JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB DECLARATION OF VLAD TSYRKLEVICH

I, Vlad Tsyrklevich, declare under penalty of perjury that:

1. I have been retained by Mr. Michaud's defense team to conduct a forensic analysis of the "Network Investigative Technique" (NIT) that was used to search for and seize data in this case. A copy of my *curriculum vitae* is attached to this declaration.

2. On January 11, 2016, I received a password protected disc from the FBI which, according to the information I had been provided by defense counsel, would contain the programming (or "source") code for the investigative technique. Prior to receiving this disc, I had reviewed and agree to abide by the terms of a confidentiality agreement and protective order that had been drafted by the government.

3. After conducting an initial examination of the code that had been provided by the FBI it was apparent that to me that the code was incomplete. A brief

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

explanation of how NITs work and their various components follows, along with an explanation of the missing aspects of the code.

4. **The components of an NIT programming or source code and how they work:** The NIT presented by the FBI works by using an "exploit," a piece of software that takes advantage of a software "vulnerability" in the Tor Browser program. By exploiting this software vulnerability, the NIT is able to circumvent the security protections in the Tor Browser, which under normal circumstances, prevents web sites from determining the true IP address or MAC address of visitors. After exploiting the vulnerability, the NIT delivers a software "payload," a predetermined set of actions, to computers that receive the payload (the "host computer"). The payload used by the FBI in this case collected and then transmitted identifying information about the host computer (including its IP address) along with a unique "identifier" used to associate the target with the identifying information that the NIT collects. As a result, these type of investigative techniques have four primary components:

a. Software that generates a payload and injects a unique identifier into it.

b. The "exploit" that is sent to the target computer to take advantage of a software flaw in the Tor Browser.

c. The "payload" that is run on the target computer to extract identifying information about it (such as its IP address).

d. An additional "server component" that stores and preserves the extracted information and allows investigators to access it.

5. **What the FBI Produced and What is Still Missing:** The government has provided us with one component of the payload (component "c"). However, it is unclear from the limited data provided so far whether the payload that has been provided was the only payload associated with the NIT or whether other payloads were executed. Moreover, the FBI has not furnished component "a" (the server component

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

that generates the payload and injects an identifier); "b" (the exploit component); or "d" (the data preservation component). It is all of these components in combination, not just one or another of them, that constitutes a network investigative technique.

6. **Why the Missing Components are Needed for a Complete and Accurate Analysis:** The accuracy and potential admissibility of the evidence collected by the NIT depends on the accuracy of the data the government claims is associated with the computer that Mr. Michaud allegedly used to access "Website A." In addition, defense counsel has informed me that he is seeking to determine if the NIT used in this case operated in the manner described in various warrant applications and whether its execution may have compromised any data or functions on the target computer. However, the materials provided by the FBI are insufficient to make these determinations or verify that the data extracted from the target computer is accurate for the following reasons:

- The software that generates a payload and injects a unique identifier into it (component "a") is critical to understanding whether the unique identifier used to link a defendant to access of illegal content is actually unique. If the identifier is generated incorrectly, it could cause different users to be incorrectly linked to each other's actions. It is important to note that errors in the use of cryptographic components are pervasive in modern software. The proper generation of unique identifiers hinges on the correct use of a "Pseudo-Random Number Generator," a fundamental cryptographic technology that is frequently misused. Without the missing data, I am unable to make a determination about these issues.

- As noted, the "exploit" used in the NIT (component "b") is intended to execute on the computer that is being identified. Analyzing and understanding the exploit component of the NIT is critical to understanding whether the payload data that has been provided in discovery was the only component executing and reporting information to the government or whether the exploit executed additional functions outside of the scope of the NIT warrant. Without the missing data about the exploit component of the NIT, I am unable to make a determination about these issues.

- In addition, the server component that stores the identifying information returned by the payload (component "d") must faithfully store and reproduce the data it was sent. The correct use of data storage primitives and the programming practices used to avoid data corruption or tampering make analyzing this

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

component of the NIT essential to understanding and verifying the digital "chain of custody" of information derived from the NIT. Without the missing data, I am unable to make a determination about these issues.

7. The importance of this data to Mr. Michaud's preparation of his defense is hard to overstate because I am aware of a previous instance in which an NIT resulted in indiscriminate targeting. In August 2013, all of the websites hosted by "Freedom Hosting" -- a service, run from servers in France, that hosted websites accessible to users of the Tor network -- began serving an error message with hidden code embedded in the page.[1] That code was specifically designed to exploit a security flaw in a version of the Firefox web browser used to access Tor hidden servers.[2] According to an FBI agent who later testified in an Irish court, the Freedom Hosting service hosted at least 100 child pornography websites.[3] But the service also hosted a number of legitimate sites, including TorMail, a web-based email service that could only be accessed over the Tor network, and the Hidden Wiki, which one news site described as the "de facto encyclopedia of the Dark Net."[4] Even though these sites were serving lawful content, the FBI's "watering hole" attack was performed in an overbroad manner, delivering a NIT to visitors of all of the Freedom Hosting sites, not just to visitors of sites that were engaged in the distribution of illegal content. It is therefore important to Mr. Michaud's defense and trial preparations to determine whether a similarly indiscriminate "watering hole" attack could have affected this case.

DONE this 13th day of January, 2016.

Vlad Tsyklevich

[1] *See* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013), http://www.wired.com/2013/09/freedom-hosting-fbi/.

[2] See Goodin, *Attackers Wield Firefox Exploit to Uncloak Anonymous Tor Users*, Ars Technica (Aug. 5, 2013), http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/.

[3] Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *supra.*

[4] Patrick Howell O'Neill, *An In-Depth Guide to Freedom Hosting, the Engine of the Dark Net*, The Daily Dot (Aug. 4, 2013), http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Vlad Tsyrklevich

(858) 722-6490

http://tsyrklevich.net
vlad@tsyrklevich.net

Skills

Languages: C, Ruby, Assembly (x86/x64, PPC, ARM, MIPS, SPARC), C++/Objective-C, Java, Python, JavaScript

Work Experience

- **Square** — San Francisco, CA and New York, NY
  Security Engineer — *04/2012 – Present*
  - Low-level iOS and Android platform analysis in order to develop custom security assurances and anti-RE measures
  - Develop a complex client-server software protection scheme integrating with an external hardware module
  - Audit services in production datacenters and work with the platform team to fix flaws and introduce new security measures
  - Consult with software engineering teams on secure application development, PKI, and network architecture
- **Irdeto** — San Francisco, CA
  Senior Reverse Engineer — *11/2011 – 04/2012*
  - Analyze and defeat custom protection schemes implemented in user- and kernel-land on Windows
  - Work with partners on hardening their copy-protection mechanisms against reverse engineering
  - Evaluate both in-house and third-party anti-RE solutions for use by our partners and in our software
- **SPARTA, Inc.** — Centreville, VA
  Security Researcher — *05/2006 – 11/2011*
  - Lead new research efforts in reverse engineering, vulnerability discovery and exploit development across Windows, Linux, and embedded platforms
  - Analyze undocumented network protocols and file formats in order to replicate behavior, bypass protection schemes and discover vulnerabilities
  - Reverse engineer armored and packed binaries and bypass anti-reverse engineering protection schemes
  - Develop low-level applications with high-speed, high-stealth and high-reliability considerations

Open Source

- **Metasploit Framework** — *2005 - 2006*
  - Develop payloads for Windows, Linux, Solaris and other operating systems across multiple architectures
  - Port public exploits and write new exploits, shellcode encoders, nop generators and backend plug-ins

Education

University of California, Berkeley
B.A. Applied Math with a focus in Computer Science; GPA: 3.6

Presentations

- Co-speaker at Blackhat USA 2007: Single Sign-On for the Internet: A Security Story
- Speaker at Toorcon San Diego 2006: Polymorphic Shellcode at a Glance

B-005