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 SPECIAL AGENT DANIEL ALFIN

Your affiant, Daniel Alfin, being duly sworn and deposed, states the following:

1. I am a Special Agent of the Federal Bureau of Investigation. I am currently assigned to FBI Headquarters, Criminal Investigative Division, Violent Crimes Against Children Section, Major Case Coordination Unit. My duties involve the investigation of individuals using various types of technology to produce, distribute, and trade child pornography. As an Agent assigned to the FBI Violent Crimes Against Children Section, Major Case Coordination Unit, I routinely analyze network data that has been collected pursuant to court order. I hold a University Degree in Information Technology and multiple industry certifications that are recognized by the United States Department of Defense. Additionally, I have completed all stages of FBI Cyber Training including courses on Advanced Network Investigative Techniques, Network Traffic Analysis, Ethical Hacking, and Malware Analysis.

2. Analysis of network data generally consists of identifying the origin, destination, and content of communications that are sent across the Internet. In addition to performing this type of analysis, I am routinely called upon to assist Agents across the FBI with similar analysis. In the past two years, I have analyzed data from more than 30 court-authorized network intercepts and those analyses have been used in affidavits and court filings in several judicial districts.

3. I have been involved in the FBI investigation of the Playpen website since it came online in approximately August 2014. Playpen was a website that existed on an anonymous network and was dedicated to the advertisement and distribution of child pornography. My duties included the review of Playpen's content on multiple occasions, engagement in undercover activities on Playpen, and the coordination of investigative activity aimed at identifying members of Playpen, including the defendant, Edward Matish.

4. In preparing this declaration, I have reviewed evidence and spoken with FBI personnel familiar with the facts and circumstances outlined below. I provide the following summary of the information I have learned as a result.

5. I have also reviewed the declaration of Messrs. Tsyrklevich and Miller, the defense experts, respectively dated January 13, 2016 and May 23, 2016, (hereinafter "Tsyrklevich Dec." and "Miller Dec.") and noted a number of statements that are inaccurate and/or require clarification. I will address several of these in great detail below but will begin by noting one overarching misconception in these declarations. Specifically, Tsyrklevich and Miller attempt to redefine the NIT as something containing multiple components. The NIT, however, consists of a single component: that is, the computer instructions delivered to the defendant's computer after he logged into Playpen that sent specific information obtained from his computer back to the FBI. Those computer instructions, and the information obtained via their execution, have been made available for review in this case. In his expert declarations, Matish describes that component as a "payload."

6. As another threshold matter, I would note that I do not consider the NIT used by the FBI to be "malware," though the experts retained by Mr. Matish describe the NIT in such terms. The word malware is an amalgamation of the words "malicious" and "software". The NIT utilized in this investigation was court-authorized and made no changes to the security settings of the target computers to which it was deployed. As such, I do not believe it is appropriate to describe its operation as "malicious."

7. The NIT computer instructions provided to the defense on May 26, 2016 comprise the only "payload" executed on Matish's computer as part of the FBI investigation resulting in his arrest and indictment in this case. Accordingly, the defense has been given access to the only "payload" as that term is used by the defense in the Tsyrklevich declaration.

8. After the NIT collected the information that it was permitted to collect via the computer instructions sent to Matish's computer, there was nothing that resided on Matish's computer that would allow the government (or some other user) to go back and further access that computer.

9. I have personally executed the NIT on a computer under my control and observed that it did not disable the security firewall, make any changes to the security settings on my computer or otherwise render it more vulnerable to intrusion than it already was. Additionally, it did not "infect" my computer or leave any residual malware on my computer.

10. Matish claims via his expert declarations that the NIT consisted of four components – an "exploit," a "payload," software that generates a payload and injects a unique identifier into it, and a server component that stores the delivered information. Tsyrklevich Dec. p. 2 ¶ 4.

11. As used here, a computer "exploit" consists of lines of code that are able to take advantage of a software vulnerability. In layman's terms, an "exploit" could be thought of as a defect in a lock that would allow someone with the proper tool to unlock it without possessing the key. Here, an "exploit" allowed the FBI to deliver a set of instructions-the NIT-to Matish's computer. Those instructions then gathered specified information, including Matish's IP address, and transmitted that information to government controlled computers. The NIT instructions and results have been provided to the defense for review; the "exploit" has not.

12. Tsyrklevich claims that he requires access to the government's "exploit" to determine if the government "executed additional functions outside the scope of the NIT warrant." Tsyrklevich Dec. p. 3, ¶ 6. He is wrong. Discovery of the "exploit" would do nothing to help him determine if the government exceeded the scope of the warrant because it would explain how the NIT was deployed to Matish's computer, not what it did once deployed.

13. The Miller declaration states that "[a] computer system that has been exploited has been fundamentally altered in some way." Miller Dec. p. 2, ¶ 5. Miller cites no authority for that premise. It is incorrect. It is possible for an existing vulnerability in a computer system to be exploited without making any fundamental changes or alterations to that computer system. The Miller declaration also speculates about consequences that may occur "if the security firewall on a computer is disabled by an NIT or other malware." Miller Dec. p. 3, ¶ 7.

14. It is theoretically possible for an exploit to make fundamental changes or alterations to a computer system or to disable its security firewall. However, as noted above, the NIT used here and the exploit used to deliver it did not do so. Other than to point to this theoretical possibility, I am aware of no evidence or indication to which either defense expert points to suggest otherwise.

15. The government has advised the defense that it is willing to make available for its review the two-way network data stream showing the data sent back-and-forth between Matish's computer and the government-controlled computer as a result of the execution of the NIT.

16. Review of this data stream reflecting the information transmitted to the FBI from Matish's computer as a result of the deployment of the NIT confirms that the data sent from Matish's computer is identical to the data the government provided as part of discovery.

17. Review of the network data stream also confirms that that no images were transmitted from Matish's computer to a government-controlled computer or from a government-controlled computer to Matish's computer as a result of the execution of the NIT.

18. Discovery concerning the "server component" is unnecessary because there are alternative means of verifying the accuracy of the NIT information.

19. Tsyrklevich claims that he needs access to the server component in order to confirm that the information obtained from Matish's computer by the NIT and sent to the FBI was accurately stored and reproduced. Tsyrklevich Declaration pp. 3-4. The defense does not need access to government servers to do this, however, because the government has agreed to provide an alternative method of verifying that the information obtained from Matish's computer was accurately recorded. Specifically, the government has offered to provide a copy of the data stream sent by Matish's computer to the government as a result of the execution of the NIT. Tsyrklevich can compare the information sent to the government by the NIT to the information provided in discovery to verify that what the government recorded from Matish's computer is in fact what was sent by Matish's computer. I have reviewed that data stream and, as explained below, confirmed that the information sent by Matish's computer as a result of the NIT matches the information that is stored on the government's servers.

20. When two computers communicate via the Internet, they do so using standard network protocols. Communications over the Internet are sent in "packets," which serve as the means by which computers share information over a network. Just as two people communicating over email exchange individual messages, computers exchange network packets. These packet exchanges follow standard network protocols that permit individual computers to process and exchange information with one another. Just like two people meeting on the street, computers wishing to communicate with one another first exchange greetings through a "handshake,"[1] then exchange information, and part ways with a communication exchange that basically consists of the computers saying "goodbye" to each other.

21. Here, when the NIT was delivered to Matish's computer, it had exactly this sort of interaction with a government-controlled computer. The network packets memorializing this exchange, which have been preserved in a standard file format, make it possible to reconstruct that exchange and see exactly what information was transmitted by Matish's computer to the government.

22. A review of the data file, known as a PCAP file, documenting the exchange contains several network packets exchanged between Matish's computer and the government computer. The initial packets correspond to the initial "handshake" that established the connection between Matish's computer and the government computer. Similarly, the final packets in the

[1] Some protocols that are used to communicate via the Internet do not include a "handshake" as described in this declaration. These other protocols are not relevant to the matter at hand as the communications that occurred as a result of the deployment of the NIT did utilize a network protocol that included a "handshake".

communication correspond to the "goodbye" communication between the two computers. The remaining packet(s) thus contains the substance of the communication, namely, the information collected by the NIT after it was delivered to Matish's computer.

23. Reviewing these packets, I was able to confirm that the information collected from Matish's computer matches the information stored on the government servers that has been provided in discovery. Each of the pieces of information the government-controlled computer recorded being collected from Matish's computer by the NIT appears in the packets. If Tsyrklevich's goal is to verify the accuracy of the information stored by the government, then a review of the network data is all that would be required. The data is not encrypted or redacted thus making such a review possible.

24. Tsyrklevich maintains that he needs access to the computer code that "generates a payload and injects a unique identifier" in order to ensure the identifier used was in fact unique. Tsyrklevich Dec. p. 3 ¶ 6. He is wrong because the unique identifier assigned to Matish's NIT results was in fact unique.

25. Prior to deployment of the NIT, a unique identifier is generated and incorporated into the NIT. When the "activating computer"' sends information to the government as a function of the NIT, that unique identifier is included with the response. When the information is received by the government, a check is performed to ensure that the unique identifier contained within the delivered information matches the unique identifier that was generated by the government. In the matter at hand, all identifiers received by the government, including the one sent by Matish's computer, did match identifiers that were generated by the government and they were in fact unique.

26. The ultimate question posed by Tsyrklevich is not how the unique identifier was generated but if the unique identifier sent to Matish's computer was actually unique. I have reviewed the list of unique identifiers generated during the operation and confirmed that there were in fact no duplicate identifiers generated.

27. A query of an FBI database containing the information gathered as part of this investigation through the use of the NIT revealed the following: 1) there are no duplicate unique identifiers within the database, meaning that each identifier assigned to an individual Playpen user is in fact unique; 2) the identifier associated with the username "Broden" was in fact unique; and 3) there are no identifiers in the database other than those generated by the deployment of a NIT as part of this investigation; the significance of which is the fact that this proves no outside entity tampered with or fabricated any of the unique identifiers generated as part of the investigation.

28. I have read the Defendant's reply to the Government's Response to the Motion to Compel dated May 23, 2016. In the motion, Matish asserts that there are chain of custody problems caused by the fact that the NIT transmitted data "unencrypted over the traditional internet". This assertion is further supported by the declaration of Matthew Miller who states "the IP address relayed to the FBI was unencrypted and subject to attack by hackers" Miller Dec. p. 3 ¶ 9. He is wrong. 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. Additionally, Miller demonstrates a lack of understanding of how data is transmitted over the internet. Computers that communicate over the internet do so by use of IP Addresses. While the data that is sent and received by the computers may be encrypted, the IP Addresses cannot be encrypted as Miller suggests they should be.

29. Also contained within the defendant's Motion to Compel Discovery is the statement, "defense needs the NIT code to verify the government's allegations that it deployed the NIT based on some specific action taken by Mr. Matish." Motion. p. 2 ¶ 2. This statement is wrong and is not supported by any expert declaration filed on behalf of Mr. Matish. In fact, the Playpen user report for the user "Broden" contains a detailed breakdown of all actions taken by the user "Broden" on the Playpen website including the exact action that triggered the NIT; the accessing of a specific post on the Playpen website that depicted what appeared to be several images of a prepubescent female whose genitals were being licked by a dog.

30. In each instance when I have been tasked with identifying and analyzing malware[2], I did not have advance knowledge of the specific malware for which I was looking or even if malware was actually present, though there was reason to suspect the presence of malware. I have nonetheless been able to locate, identify, and analyze suspected malware notwithstanding the lack of advance knowledge about the particular malware. In this declaration, I will lay out in general terms some of the steps that can be taken to identify and analyze malware and provide additional detail concerning the operation of the NIT used in the FBI investigation at issue in United States v. Matish.

31. Prior to analyzing a device for traces of a malware infection and even without knowledge of the specific type of malware involved, an investigator generally has some information or indication of the presence of malware. For example, an individual's computer could be

[2] The term "malware" generally refers to computer software that impairs the integrity or availability of data, a program, a system, or information. Other common terms that describe various types of malware are "virus", "trojan", and "worm".

experiencing problems with programs failing to operate as intended or a user may notice that data have inexplicably been deleted from the system.

32. If malware does in fact transmit data over the Internet in a similar fashion to how the NIT transmitted data to an FBI controlled computer server, having a copy of the transmitted network data would be a valuable tool that would assist with analyzing a system and searching for malware. If the network data is not encrypted, it will generally contain strings of plain text containing identifiers that can be used as search terms during the course of a forensic analysis. Although the defense has declined to review the network data available in this case, I have reviewed and analyzed that network data. My review confirmed that it is not encrypted and contains various strings that would generally be considered valuable during the course of forensic analysis. For example, a defense expert who suspects that a given device was a target of the NIT could use these search terms to try and assess whether there are any traces of the NIT still left on the target device or if the NIT otherwise remains on the device.

33. Utilization of search terms is just one avenue of analysis available to locate and identify malware on a device. It is also possible to review the list of programs designated to run when a device's operating system loads. Such a review is a crucial step in determining whether a computer may be infected with malware. After identifying and eliminating from consideration known programs that the user intended to execute upon startup, an investigator may focus on any remaining programs whose purpose is unknown. In some instances, malware can be disguised as a legitimate program and can be identified by comparison of the legitimate program's file hash value against the hash value of the suspect program.

34. Where there is reason to suspect a storage device such as a USB drive or even a cellular telephone has been infected with malware, an investigator can undertake a dynamic analysis of any suspect files on that device and verify that those files either do or do not have the ability to execute malicious code. The process of conducting a dynamic malware analysis generally involves creating a copy of a suspect file and executing it in a test environment. The state of the test environment is recorded prior to execution of the file and various programs are active in the test environment that record changes to the system. Additionally, various pieces of software or hardware can be utilized to capture any network data generated by the file upon execution.

35. The devices seized from Mr. Matish are available to the defense for inspection and review, and I believe, based on my training and experience, that the procedures describe above (among others) could be applied to those devices to determine whether there is evidence suggesting that the NIT or a piece of malware was responsible for the collection of child pornography found on Mr. Matish's devices.

DANIEL ALFIN
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATION