IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No. 15-CIV-1315
	)	
v.	)	
	)	
ANDREY GHINKUL	)	
a/k/a ANDREI GHINCUL	)	
a/k/a Smilex, et al.	)	
	)	
Defendants.	)	

DECLARATION OF SPECIAL AGENT BRIAN STEVENS IN SUPPORT OF APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Brian Stevens, declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation in Pittsburgh, Pennsylvania. I make this declaration in support of the United States of America's Application For An Emergency Temporary Restraining Order And Order To Show Cause Re Preliminary Injunction. I make this declaration of my own personal knowledge or on information and belief where noted and, if called as a witness, I could and would testify completely to the truth of the matters set forth herein.

2. I currently investigate criminal computer intrusions in the Pittsburgh Field Office Cyber Squad. I have been trained in investigative tools and techniques required to pursue criminals employing sophisticated online tools such as peer-to-peer botnets and Virtual Private Networks (VPN).

3. As used herein, the following terms have the following meanings:

a. "Malware" is malicious software, usually loaded onto a computer without the knowledge of the computer's owner or user. For example, computer viruses are malware.

b. A "botnet" is a network of computers that cyber criminals have infected with malware that gives a cyber criminal access to each computer and allows a cyber criminal to control each computer remotely.

c. A "botmaster" is a cyber criminal controlling a botnet.

d. An Internet Protocol (IP) address is the unique address of a computer or other device connected to a network, and is used to route Internet communications to and from the computer or other device.

e. "Peer-to-peer" refers to a means of networking computers such that they communicate directly with each other, rather than through a centralized management point.

f. A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

I. Overview of Bugat/Dridex Malware and Botnet

4. Bugat/Dridex is a type of malware that has infected hundreds of thousands of computers and caused financial losses likely in excess of $25 million worldwide. Defendants are central figures in a sophisticated criminal syndicate that is responsible for distributing Bugat/Dridex and maintaining its associated botnet of infected computers. As explained in detail below, the recent neutralization of the Bugat/Dridex central control infrastructure by law enforcement in the United Kingdom has provided the opportunity for the FBI to seize control of the Bugat/Dridex botnet and prevent Defendants from reacquiring control of the botnet and causing further damage.

5. Bugat/Dridex operates primarily as a banking Trojan, or malicious computer program, which misrepresents itself in order to persuade a victim to install it, capable of stealing

user credentials that victims enter on banking websites. Bugat/Dridex accomplishes the theft of this confidential financial information through the use of keystroke logging and web injects. Keystroke logging is the action of recording (or logging) the keys struck on a keyboard. This action is usually done surreptitiously by a computer program (i.e., keylogger) to capture the keys typed on a computer without the typist's knowledge. Malware that uses keystroke logging often will provide the captured keystrokes to those who caused the malware to be installed or to a place designated by them. Through keystroke logging, computer intruders are able to obtain online banking credentials as soon as the user of the infected computer logs into their account. After obtaining this information, these intruders can access the victim's online bank account and execute unauthorized electronic funds transfers ("EFT"), such as Automated Clearing House ("ACH") payments or wire transfers, to accounts that they control.

6. Web injects introduce (or inject) malicious computer code into a victim's web browser while the victim browses the Internet and "hijacks" the victim's Internet session. Different injects are used for different purposes. Some web injects are used to display false online banking pages into the victim's web browser to trick the victim into entering online banking information, which is then captured by the individual employing the web inject.

7. Once a machine is infected with Bugat/Dridex, it becomes a "bot," or compromised computer, which joins the vast network of infected computers that are controlled and operated by Defendants.

8. Bugat/Dridex is a multifunctional malware package that has been in use since late 2009. The primary goal of Bugat/Dridex malware is to infect computers, steal credentials, and then obtain money from victims' bank accounts. Bugat/Dridex malware is generally distributed

through a process known as “phishing,” where spam emails are distributed to victims. The emails appear legitimate and are carefully crafted to entice the victim to click on a hyperlink or to open an attached file. In the event a user clicks on a hyperlink, the user is then redirected to an exploit kit, which is a web based software program that scans the victim’s computer and operating systems for vulnerabilities and, upon discovering one, forces the download of a malicious file upon the victim. In the event the victim opens an attached file, he or she is directly infected either by the Bugat/Dridex malware, or by a loader program, which then downloads the Bugat/Dridex payload. Bugat/Dridex, like most modern malware families, is specifically crafted to defeat antivirus and other protective measures employed by victims. As the individuals behind Bugat/Dridex improved the malware and added functionality, the name of the malware changed, at one point being called Cridex, and later Dridex. However, each version was based on the same original Bugat source code and Dridex operates in the same fundamental way as its predecessors. Because we are seeking authority to remediate Dridex, which is a recent iteration of Bugat, all references to the relevant malware and associated botnet in this affidavit will be to “Bugat/Dridex.”

9. It is difficult to fully capture the extent of financial loss associated with Bugat/Dridex largely because of the technical hurdles of directly attributing a given financial fraud directly with a specific malware strain. However, based upon my training and experience, interviews with victims, information provided by foreign law enforcement partners, technical monitoring of Bugat/Dridex botnet activities, and examining the records kept by Bugat/Dridex operators, it is my belief that total losses associated with Bugat/Dridex exceed $10 million in the United States and several times that on a worldwide basis.

10. Both the Bugat/Dridex malware and the criminal group controlling it are highly sophisticated. Bugat/Dridex is run as a business by a small number of conspirators primarily based in Russia and Moldova who have years of experience and well-developed trust relationships with one another. The members of the conspiracy have specialized roles within the Bugat/Dridex enterprise, including expanding the botnet by infecting new victims, technical administration of the botnet, and managing the network of money mules[1] who launder stolen funds. Unlike most malware distributors, the Bugat/Dridex enterprise maintains tight control over the Bugat/Dridex malware code and does not appear to sell or distribute it to anyone outside the organization.

11. Bugat/Dridex has also caused and attempted to cause significant financial losses to businesses operating in this District. For example, Penneco Oil, is a petroleum company located in the Western District of Pennsylvania. From August 31, 2012 through September 4, 2012, three unauthorized wire transfers were initiated from the computer of an employee at Penneco Oil, totaling $3,585,120.00. The wire transfers were sent to banks in Eastern Europe and were not recovered. The financial loss due to the wire transfers was assumed by Penneco Oil's bank, First Commonwealth Bank, which is also located in the Western District of Pennsylvania.

12. The FBI had an expert in malware analysis, who regularly performs work for the FBI on a contract basis, analyze the Penneco Oil employee's computer whose credentials were used to perform the transaction. The expert concluded that based upon the malware code and the

[1] Money mules are individuals recruited by criminals for the express purpose of using the mules' accounts to launder stolen funds.

artifacts created by the malware, the computer was infected with Bugat/Dridex malware at a time before the first wire transfer**.** As a result, those persons associated with the Bugat/Dridex malware used the malware to fraudulently obtain online banking credentials of employees at Penneco Oil and used those stolen credentials to falsely represent to First Commonwealth Bank that they were Penneco Oil Employees in order to access Penneco Oil's bank account and to make an electronic funds transfer from Penneco Oil's bank account.

13. In another example, on November 28, 2011, the business manager at the Sharon City School District, located in Sharon, PA, attempted to log into the Sharon City School District's bank account at First National Bank. She found that it was locked. First National Bank told her that someone attempted to access the account, but failed to answer the security questions. The same situation occurred on December 15, 2011. In response, First National Bank issued the business manager a new user ID and password.

14. On December 16, 2011, the business manager accessed the Sharon City School District's account. Later that morning, First National Bank contacted the business manager, seeking verbal confirmation of a $999,000 wire transfer from the Sharon City School District's account. The $999,000 was ultimately destined for Ukraine. The transaction was canceled before the funds were lost.

15. The FBI obtained a forensic analysis of the Sharon City School District's computer used to perform the transaction. An expert concluded, based upon the malware code and the artifacts created by the malware, that the computer was infected with Bugat/Dridex malware at a time before the attempted wire transfer. The analysis also revealed that the infection was the result of a spam email received on November 8, 2011.

16. As a result, those persons associated with the Bugat/Dridex malware used the malware to fraudulently obtain online banking credentials of employees at the Sharon City School District and used those stolen credentials to falsely represent to First National Bank that they were Sharon City School District Employees, in order to access Sharon City School District's bank account and to attempt an electronic funds transfer from Sharon City School District's bank account.

17. As mentioned above, once a victim's computer is infected with Bugat/Dridex, it becomes a "bot" in the vast Bugat/Dridex botnet that is controlled by Defendants. Approximately ten distinct Bugat/Dridex sub-botnets have been observed operating since 2014 and at least one of these sub-botnets has primarily targeted financial institutions located in the United States.[2] The sub-botnets range in number of infected machines, but Internet security researchers[3] identified that one sub-botnet (known as EB120) contained over 100,000 active bots during May, 2015. The infected machines are located all over the world, including a significant amount in the United States.

18. Bugat/Dridex initially utilized a botnet infrastructure whereby the infected victim machines communicated with, and received messages directly from, a multi-layered network of command and control ("C&C") servers. A C&C server is a centralized computer that issues commands to a botnet and receives reports back directly from the compromised computers. The outermost group of servers in the Bugat/Dridex C&C communication architecture (Layer 3) is

[2] Not all of these sub-botnets are currently operating. As of September 15, 2015, a handful of distinct Bugat/Dridex sub-botnets were still operating worldwide.

[3] Through the course of its investigation, the FBI has worked with a number of Internet security researchers, who have proven to be reliable in this and other investigations. All references in this Affidavit to Internet security researchers are to researchers that the FBI has found to be reliable.

made up of hundreds of servers that have been compromised by the perpetrators. The Layer 3 servers, which are also referred to as "admin nodes," forward traffic upstream to a smaller group (Layer 2) of approximately 15 servers that are directly owned by the Bugat/Dridex group. This intermediate layer forwards traffic to the innermost section (Layer 1) of the infrastructure, which is comprised of about two dozen servers and operates as the back-end infrastructure that is controlled directly by the perpetrators.[4] The Bugat/Dridex C&C servers were operated by Defendants and were used to control and push out commands to the botnet.

19. From a criminal's perspective, a traditional command and control architecture is very simple to operate, but is also very vulnerable to disruption and seizure, since any interference between the C&C servers and the victim machines will render the infected bots free from the criminal's control.

20. Beginning in approximately November 2014, the Defendants added peer-to-peer (P2P) functionality to make the botnet infrastructure more resilient to countermeasures by law enforcement. In the P2P botnet, each infected bot (a "peer") maintains a list of other infected peers. The list maintained by the peer consists of routing information that includes IP addresses and port numbers of other peers on the network. To ensure that this list remains active, the peers regularly request new updated bot routing information from "super-peers" on the network. The super-peers get the most updated information directly from the C&C servers that are controlled by the perpetrators. Upon receiving the new routing information from the super-peers, the bots update their lists of peers accordingly. In this way, the super-peers serve as relay points for

[4] There appears to be virtual private network (VPN) communication between the Layer 2 and Layer 1 servers, probably via a common VPN tunnel to the level 2 devices, creating an internal network for the perpetrators that is accessible via VPN.

commands coming from the Bugat/Dridex operators and for encrypted data stolen from victim computers to be sent to the perpetrators. Bugat/Dridex operators can promote any Bugat/Dridex-infected computer to super-peer status.

21. After the upgrade to P2P functionality, peers in the Bugat/Dridex botnet began to contact other peers to get an updated list of malware and potential victims to target. In contrast, before the upgrade, bots were only able to get updates via the centralized C&C servers. The switch to P2P functionality made Bugat/Dridex a more decentralized network and therefore more resilient to take down measures by law enforcement.

22. Despite the concerted effort of Defendants and other criminal actors, law enforcement organizations have been able to gain visibility into the command structure of the Bugat/Dridex botnet. For example, in April, 2015, the National Crime Agency (NCA), a law enforcement agency in the United Kingdom, began an operation to identify components of the Bugat/Dridex peer to peer network in the U.K. During the course of their investigation into Bugat/Dridex, the NCA identified two key C&C servers that were being used to operate the Bugat/Dridex botnet. Because of their central role in issuing commands to bots and updating peer lists, continued functionality of these C&C servers was necessary for Defendants to operate the botnet.

23. On or around the weekend of September 4, 2015, the National Crime Agency seized the key components of the C&C system for the Bugat/Dridex botnet that were located in the U.K. Because these servers had been disabled, the super-peers and peers have no centralized mechanism to receive new commands or peer lists. We assess that the Bugat/Dridex system has

been temporarily disabled, but the Defendants could re-establish control of the system at any time by registering new C&C servers to issue commands to the botnet.

II. Defendants

A. Andrey Ghinkul

24. A multi-year FBI investigation has revealed that Defendants, who are leaders of a tightly knit group of cybercriminals based primarily in Russia and Moldova, are responsible for Bugat/Dridex. Defendants have deliberately targeted their malicious software at U.S. individuals and companies. Although the full scope of harm caused by Defendants is impossible to calculate, the best evidence available suggests that Bugat/Dridex has resulted in losses to U.S. businesses and individuals of more than $10 million with the true number possibly many times higher. The best evidence also suggests losses in the United Kingdom stemming from Bugat/Dridex likely exceed 20 million British Pounds.

25. Defendants have gone to great lengths to conceal their identities and hide from law enforcement. FBI investigation, review of Defendants' internet chat logs, interviews of victims and industry experts, the establishment of threat specific industry working groups, search warrants, open source research, requests to foreign governments pursuant to Mutual Legal Assistance Treaties and real time attack monitoring, has revealed that, among other tactics, the individuals running Bugat/Dridex use false identities and online monikers, anonymous internet-based payment systems, and an extensive network of money mules to launder the funds stolen during their high tech bank robberies. Despite these tactics, as described below, the FBI has identified a small group of individuals at the very top of the criminal gang responsible for Bugat/Dridex. One of these individuals is Andrey Ghinkul of Chisinau, Moldova.

26. On or about September 18, 2014, Internet security researchers provided the FBI with various screenshots from within Bugat/Dridex administrative portals, which had been updated on or about September 18, 2014. Administrative portals are web applications which allow criminals to manage the day-to-day operations of their botnets. One of the pages within these portals listed the account numbers and account names of various Bugat/Dridex users.

27. Through these screenshots and from other information obtained in this investigation, the FBI learned that Smilex was the online nickname of one of the central figures involved in the Bugat/Dridex conspiracy. Additionally, during the course of its investigation, the FBI became aware that the Bugat/Dridex malware group was utilizing a server that was assigned IP address Redacted PII.113. Internet security researchers provided the FBI with information that this server contained the "admin control panels" used by the Bugat/Dridex group. These control panels provided an interface by which the Bugat/Dridex botnet operators could issue commands to infected computers.

28. Pursuant to a federal search warrant issued on February 10, 2015, the FBI performed searches of various email accounts, including Redacted PII@gmail.com, which, as explained below, is known to be utilized by Defendant "Smilex." These searches revealed evidence of the development and distribution of the Bugat/Dridex malware.

29. Within the email account iavorscaia@gmail.com, the FBI discovered an email sent by Redacted PII@gmail.com to himself at Redacted PII@gmail.com, containing a single zip file. This zip file contained within it an executable file. Further analysis of the executable file by an Internet security researcher revealed that it was a first stage loader for the Bugat/Dridex malware family. This loader, known as Lerspeng, attempts to download Bugat/Dridex malware from a set

of hardcoded websites. Based on information received by Internet security researchers, at one point all of the hardcoded websites hosted Bugat/Dridex downloader executables.

30. Through legal process, the FBI learned that the email account Redacted PII@gmail.com was listed as the recovery email for the email account Redacted PII@gmail.com. Based on this information, it is apparent that the owner of the email account Redacted PII@gmail.com is also the owner of the email account Redacted PII@gmail.com.

31. The FBI obtained a search warrant for the contents of the email account Redacted PII@gmail.com. An analysis of the contents of this account revealed ten emails from the provider responsible for hosting the server at IP address Redacted PII.113, spanning the timeframe June 4, 2014 through March 24, 2015. Seven of these emails were responses to problem tickets that the owner of Redacted PII@gmail.com submitted to the hosting provider regarding this server. Three of these emails were abuse notifications from the provider, asking that the owner of Redacted PII@gmail.com remove malware that had been reported conducting malicious activity from the server. Because a hosting facility will only accept problem tickets from, and will only send abuse reports to, an individual who was listed as an administrative contact, the above information indicates that the owner of the email account Redacted PII@gmail.com was an administrator of the server at IP address Redacted PII.113.

32. Furthermore, an email sent by Redacted PII@gmail.com on July 5, 2012 contains text that approximately translates to English as "Hello, my jabber handle is Redacted PII@jabber.org, contact me there." The FBI has reviewed numerous jabber chat messages for the user Redacted PII@jabber.org from November 2011 through July 2014. In those chats, Smilex indicates that he is having great difficulty causing infections with spam emails and solicits assistance from

other criminals in developing spam templates. The FBI believes that these emails are part of the work development process as Smilex creates spam templates for the purpose of causing Bugat/Dridex infections.

33. Based on the information in the preceding paragraphs, the FBI believes that the individual using the email accounts Redacted PII@gmail.com, Redacted PII@gmail.com and Redacted PII@gmail.com, and who utilized these accounts to discuss the furtherance of distributing Bugat/Dridex malware, is the same individual who used the Jabber account Redacted PII@jabber.org and the online moniker "Smilex." The evidence above positively links Andrey Ghinkul a/k/a Andrei Ghinkul to the use of the online identity "Smilex."

B. Maksim Yakubets

34. As discussed above, the FBI has reviewed numerous jabber chat logs from November 2011 through July 2014 involving Andrey Ghinkul, who used the nickname Smilex. A number of these chats were with an individual believed to be "Aqua." Based on the content of these Jabber chats, Jabber chats between Ghinkul and other criminal actors, as well as information provided by reliable sources, the FBI believes that "Aqua" is likely to have sufficient control over the Bugat/Dridex botnet to enable him to comply with a TRO from this Court ordering him to halt the scheme. Furthermore, in order to provide the broadest possible notice to Defendants, the FBI believes with a reasonable degree of certainty that "Aqua" is a nickname used by Maksim Viktorovich Yakubets who was last known to reside in Russia at the following address: Redacted PII, Moscow, Russia, Redacted PII.

C. Igor Turashev

35. Earlier in the Bugat/Dridex investigation, a pen register was attained on IP address Redacted PII.140. This IP address connected tens of thousands of times to a server hosted in Turkey that was associated with the distribution of Bugat/Dridex. Google records indicated that this IP address was also used to access the email address Redacted PII@gmail.com. The email address Redacted PII@gmail.com is the registration address for the nickname "nintutu" on a number of online forums dedicated to facilitating criminal activity. There are also several references to "nintutu" contained within Smilex's jabber chats that suggest "nintutu" serves as Aqua's administrator. Based on this and other information learned during the course of the investigation, the FBI believes that "nintutu" is likely to have sufficient control over the Bugat/Dridex botnet to enable him to comply with a TRO from this Court ordering him to halt the scheme. Furthermore, in order to provide the broadest possible notice to Defendants, the FBI believes with a reasonable degree of certainty that "nintutu" is a nickname used by Igor Turashev who was last known to reside in Russia at the following address: Redacted PII, Russia Redacted PII.

D. Maksim Mazilov and Andrey Shkolovoy

36. As discussed above, on or about September 18, 2014, Internet security researchers provided the FBI with various screenshots from within Bugat/Dridex administrative portals, which had been updated on or about September 18, 2014. One of the pages within these portals listed the account numbers and account names of various Bugat/Dridex users, including a user known by the nickname "Caramba." Furthermore, as discussed above, the FBI has reviewed numerous jabber chat logs from November 2011 through July 2014 involving Andrey Ghinkul, who used the name Smilex. A number of these chats were with the user believed to be

"Caramba." Based on the content of these Jabber chats, Jabber chats between Ghinkul and other criminal actors, as well as information provided by reliable sources, the FBI believes that "Caramba" is likely to have sufficient control over the Bugat/Dridex botnet to comply with a TRO from this Court ordering them to halt the scheme. Furthermore, in order to provide the broadest possible notice to Defendants, the FBI believes with a reasonable degree of certainty that "Caramba" is a nickname shared by two individuals who are associates and share the Caramba identity. These individuals are Maksim Mazilov, address Redacted PII, Russia Redacted PII; and Andrey Shkolovoy, address Redacted PII, Russia Redacted PII.

III. Need for *Ex Parte* Relief

37. Based on my training and experience, including both my investigation of Bugat/Dridex and other cyber criminal entities and my knowledge of how Bugat/Dridex is operated, if Defendants were to be notified in advance of the planned disruption, they could and would take simple, rapid steps to blunt or defeat the Government's planned disruption of the Bugat/Dridex botnet. Such steps would likely include reestablishing their command and control infrastructure and/or making significant changes to the intermediary communication protocols, which would not take extensive time or effort.[5]

38. Bugat/Dridex is a rapidly evolving malware set, and the Defendants are skilled cyber criminals, easily able to change the malware. Nearly the entire Bugat/Dridex botnet can be

[5] Recent intelligence suggests that Defendants and their criminal colleagues are attempting to establish a successor Bugat/Dridex botnet with a new infrastructure of compromised computers. This development highlights the need to sinkhole the existing infrastructure immediately because Defendants have demonstrated their intention to continue to distribute malware and engage in criminal activity. As explained above, for motivated and able cybercriminals such as Defendants, reclaiming the Bugat/Dridex botnet could be done in a matter of days, if not hours.

updated within 24 hours. The Bugat/Dridex botnet has been updated in this manner previously, including in response to the prior takedown of the GameOver Zeus botnet in 2014.

[REDACTED**]**

IV. Need to Redact Operational Information

40. The sources and methods used to conduct the technical disruption operation of the Bugat/Dridex botnet will remain highly sensitive, even after the operation ends and court papers are unsealed. Exposing those sources and methods would jeopardize future efforts to disrupt similar criminal activity.

41. Specifically, the descriptions of specific vulnerabilities of the Defendants' malware and the technical means by which the Government intends to exploit those vulnerabilities will remain highly sensitive. Making public the vulnerabilities that the Government has identified and the means by which the operation will exploit those vulnerabilities would provide the Defendants, and other malware designers, information they would use to craft malware that is even more resistant to disruption than the malware at issue in this case.

V. Bugat/Dridex Harmed Victims in This District and Throughout the United States

42. Bugat/Dridex has caused enormous injury in this District and throughout the United States. As explained above, it is impossible to fully quantify the losses caused by Bugat/Dridex. Nevertheless, based on its investigation to date, the FBI estimates that Bugat/Dridex has caused more than $10 million in direct loss domestically since Bugat/Dridex was first detected in 2009. The FBI further assesses that, because victims are rarely able (without the technical assistance of the FBI) to directly connect their losses to the theft of their

banking credentials by Bugat/Dridex, these estimates grossly understate the actual losses that Bugat/Dridex has caused.

43. Bugat/Dridex is programmed to defeat the added safeguards that banks place on corporate bank accounts, including one-time authorization codes. Accordingly, Defendants often use Bugat/Dridex to target lucrative corporate bank accounts, especially those belonging to small and mid-sized businesses. The impact of these attacks on these organizations is often devastating.

44. As noted above, from August 31, 2012 through September 4, 2012, three unauthorized wire transfers were initiated from the computer of an employee at Penneco Oil, totaling $3,585,120.00. The wire transfers were sent to banks in Eastern Europe and were not recovered. The financial loss due to the wire transfers was assumed by Penneco Oil's bank, First Commonwealth Bank, which is also located in the Western District of Pennsylvania. Subsequent forensic analysis confirmed that Bugat/Dridex malware was directly responsible for this financial loss.

45. Additionally, as noted above, on December 16, 2011, First National Bank contacted the business manager at the Sharon City School District, seeking verbal confirmation of a $999,000 wire transfer from the Sharon City School District's account. The $999,000 was ultimately destined for the Ukraine. The transaction was canceled because it was not authorized by anyone working for the School District. Subsequent forensic analysis confirmed that Bugat/Dridex malware was directly responsible for this attempted financial loss.

VI. The United States is Prepared to Disrupt the Bugat/Dridex Botnet

46. The FBI has developed a comprehensive technical plan to disrupt the Bugat/Dridex botnet. A review of the technical disruption effort and subsequent remediation campaign is provided below.

[REDACTED**]**

I declare under penalty of perjury under the law of the United States of America that the foregoing is true and correct to the best of my knowledge.

Executed this 8th day of October, 2015, in Pittsburgh, Pennsylvania.

/s/ Brian Stevens
Brian Stevens
Special Agent
Federal Bureau of Investigation