RECEIVED
NOV 28 2016
CLERK, U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

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

UNITED STATES OF AMERICA	)	
	)	
Plaintiff,	)	Civil Action No.
	)	
v.	)	**FILED *EX PARTE***
	)	**AND UNDER SEAL**
"flux"	)	
a/k/a "ffhost,"	)	
	)	
and,	)	
	)	
"flux2"	)	
a/k/a "ffhost2"	)	
	)	
Defendants.	)	

DECLARATION OF SPECIAL AGENT AARON O. FRANCIS IN SUPPORT OF APPLICATION FOR AN EMERGENCY TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION

I, Aaron O. Francis, 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 have been a Special Agent with the FBI for six years. I am currently assigned to the Pittsburgh Division Cyber Intrusion Squad. I have been trained in investigative tools and techniques required to pursue criminals employing sophisticated online tools such as malware, botnets, and Virtual Private Servers (VPS). I have also received training and gained experience

in interviewing and interrogation techniques, the execution of federal search and seizure warrants, and the identification and collection of computer-related evidence.

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. "Ransomware" is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker) so that they cannot be read without a key to decrypt the files.

   c. A "bot" is a computer that has been compromised by malicious software for use in completing malicious and/or illegal tasks via remote direction. Most users that have a computer acting as a bot are not aware that their computers have been compromised. Compromised computer is a term synonymous with bot, and either may be used based on context. A larger number of bots, called a bot network or botnet, are typically controlled by one computer called a command and control server. The owner of the command and control server can direct the botnet to initiate a denial of service attack, send spam, operate as proxies (blindly forwarding Internet data), host phishing sites, or participate in other cybercrime.

   d. A "botmaster" is a cyber-criminal controlling a botnet.

e. A "domain name" is the familiar easy-to-remember name used to identify computers on the internet (e.g. justice.gov). Domain names, like justice.gov, correspond to one or more IP addresses. The Domain Name System (DNS) is a hierarchical naming system for computers connected to the Internet. It associates information with domain names. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer names into IP addresses.

f. The "Internet" is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet may cross state and international borders, even if those computers are located in the same state.

g. An "Internet Service provider" (ISP) is a commercial service that provides Internet connections for its subscribers. In addition to providing access to the Internet via telephone or other telecommunications lines, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with them. Those records could include identifying and billing information, account access

information in the form of log files, e-mail transaction information, and other information.

h. An "Internet Protocol address" (IP address) is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

i. A "money mule" is an individual that receives or sends money transfers for the criminal enterprise. A "witting money mule" is an individual that is conducting the money transfers as a member of the criminal enterprise and is knowledgeable about the criminal activity. An "un-witting money mule" is an individual that may be a victim or witness, who is conducting the money transfers for the criminal enterprise but does not have knowledge of the criminal activity.

j. A "proxy" is a network service for making indirect connections to other network services. A client computer connects to a proxy and instructs it to connect to another computer. The destination computer perceives an incoming connection from the proxy, not the client computer. Like many network services, proxies have legitimate uses, but they are often used by cyber criminals to conceal their identity and location.

k. A "server" is a centralized computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." When a user accesses email, Internet web

pages, or accesses files stored on the network itself, those files are pulled electronically from the server, where they are stored, and are sent to the client's computer via the network or Internet. Notably, server computers can be physically located in any location; for example, it is not uncommon for a network's server to be located hundreds (or even thousands) of miles away from the client computers. In larger networks, it is common for servers to be dedicated to a single task. For example, a server that is configured so that its sole task is to support a World Wide Web site is known simply as a "web server." Similarly, a server that only stores and processes e-mail is known as a "mail server."

l. A "virtual private server" ("VPS") is a virtual server sold as a service by an ISP or Collocation Provider. A VPS runs its own copy of an operating system, such as Windows or Linux. Customers have full control over the entire VPS, and have the ability to install almost any software that runs on the operating system. A VPS is functionally equivalent to having a physical server running at a collocation provider, but allows the collocation provider to cost effectively manage and maximize use of their physical servers by virtualizing multiple systems on one piece of physical hardware.

m. A "sinkhole server" is a server that Law Enforcement directs seized domains to in order to capture data and identify bots for remediation.

n. A "bullet proof hosting service" is a hosting provider that will host virtually any content, including criminal content, from phishing and carding sites to botnet command centers.

Overview of Avalanche Criminal Operation

4. In June 2015, the FBI began collaborating with German and other international law enforcement partners investigating a sophisticated cyber-criminal infrastructure called "Avalanche." Avalanche is a hosting infrastructure that is composed of a worldwide network of servers that is controlled via a highly organized central control system. The Avalanche administrators rent out access to the network to other cyber criminals interested in acquiring bulletproof hosting services over which the criminals conduct malware attacks and operate money mule campaigns to launder the illegal proceeds.

5. Searches and Title III interceptions conducted by the FBI confirmed that the criminal organization that controls the Avalanche infrastructure offers two general types of services to its cyber-criminal customers: (1) the registering of domain names; and (2) the redirecting (or "proxying") of traffic through the secure Avalanche network/infrastructure to the cyber criminals who run both malware and money mule campaigns.

6. First, as to the registering of domain names, the Avalanche administrators register domain names with a handful of registrars on behalf of their clients, i.e., other cyber criminals. Malicious domains are necessary to run criminal schemes because domains resolve to IP addresses and servers, which enable victim information to be funneled through a number of servers and back to the individuals running the different families of malware (Malware Actors).

7. For example, once a computer is infected with malware, cyber criminals need a way to get the victim's information. In the case of Avalanche, this is accomplished by generating domains through a number of domain generation algorithms, or DGA's. DGA's are algorithms hardcoded into various families of malware that tell the malware which domains to call back to

with the victim's information. These domains, in turn, are hosted on servers that are controlled by the Malware Actors who now have access to the information obtained from the victim machines. Prior to the FBI's involvement in the case, German authorities broke the domain generation algorithm for much of the malware run over the Avalanche infrastructure. This enabled law enforcement to pre-determine the domains to be generated in the future; to determine which domains belonged to which malware families; and to track the servers where the malicious domains were hosted.[1]

8. Second, as to the proxying of traffic, the administrators of Avalanche proxy (i.e., redirect) traffic coming from the victim's computer to the cyber criminals who run the malware or money mule schemes. To accomplish this, Avalanche operates through a layered, or tiered, network of servers that are controlled through a carefully maintained back-end infrastructure. For example, during the investigation, a victim machine gets infected with malware[2] which is hardcoded with a list of domains to call back to, as discussed above. The malware instructs the victim machine to connect to a domain, which is hosted on a "first-level" Avalanche server with an IP address, e.g., 89.163.134.221. The server with IP address 89.163.134.221 receives information from victim machines (such as login credentials to a bank account) and forwards that information to a

---

[1] The Avalanche perpetrators also register domains on behalf of money mule operations, although unlike malware domains, money mule domains do not appear to be generated by a DGA. This is due to the difference between how malware and money mule campaigns operate. A victim often does not know that their computer has been infected with malware; the victim's computer has been "hijacked" and therefore automatically calls back to a malicious domain hardcoded into the malware. Thus, the malware domains are often a string of random letters and numbers because the infected computer is automatically instructed to check-in with that domain. On the other hand, money mule sites are designed to appear as legitimate business, often targeting people who wish to make money while working at home. Thus, money mule domains are visited knowingly (if unwittingly) by the user, so the domain names are often designed to be easy to remember and the sites hosting the scam designed to appear legitimate.

[2] The administrators of Avalanche do not appear to directly infect victim machines with malware or design the money mule campaigns. Rather, the criminal service offered by Avalanche is the greatly enhanced ability to avoid detection by law enforcement through obfuscating the source and destination traffic from victim machines.

"second-level" Avalanche server with a different IP address, e.g., 162.210.249.90. In the past, that second-level server forwarded the information to a centralized "control unit" that was a server located in Canada that used IP address 68.168.123.202. Finally, the information from the central control unit is forwarded to various "back-end" servers that correspond to the type of malware that the Avalanche customer has used to infect his victims.[3] In sum, the Avalanche clients pay the administrators of Avalanche to direct traffic from victim machines, through a series of proxies that comprise the secure Avalanche network, and then to a back-end server controlled by the perpetrator who can see all the data from the victims he has infected.[4]

9. To further avoid detection, the administrators of Avalanche combine their two basic services—registration of domains and proxying traffic—with a technique known as "fast-fluxing." The basic idea behind fast fluxing is to have numerous IP addresses associated with a single domain name, where the IP addresses are swapped in and out with extremely high frequency, through changing DNS records. The purpose of this fluxing is to thwart detection of malicious domains and IP addresses by law enforcement. Your affiant has queried the DNS servers associated with many Avalanche domains and observed that the Malware Actors have set a very short time-to-live (TTL) value, *i.e.*, 300 seconds, which indicates that the DNS records will expire after 300 seconds, so a new DNS query will then be required. When a new DNS

[3] The first-level usually consists of between 20 and 30 active servers that receive communications directly from infected victim machines. The machines changed frequently, since they are directly in contact with victim machines and therefore most likely to be detected. The second-level contains approximately half a dozen servers and these are maintained for several months at a time. During the course of this investigation, the FBI has placed over half a dozen pen registers on various second-level and back-end servers.

[4] The money mule portion of Avalanche works in the same basic way.

query from the victim machine occurs, the records reveal that the IP address that the malicious domain is hosted on has changed, or "fluxed." [5]

10. Avalanche is remarkable for both the volume and variation of malware and money mule operations funneled through its servers. German authorities estimate that over one million victims have been infected with malware run through the Avalanche infrastructure since this scheme began. Avalanche has also proved to be extremely resilient to counter measures because of the frequency with which the servers in its infrastructure are changed and the measures Malware Actors and Administrators take to conceal their identity. Moreover, the servers used in Avalanche are often paid for through stolen funds or by other means designed to thwart detection by law enforcement.

Mapping of Avalanche Infrastructure

11. Understanding of the Avalanche infrastructure was initially developed by German law enforcement who have been investigating Avalanche as a top priority since 2011. Germany's investigation began after numerous German banks were victims of malware attacks that resulted in millions of dollars in losses. During the course of their investigation, German authorities identified several first and second-level servers located in Germany that were associated with those malware attacks. After receiving court authorization to monitor the activity on those servers, the German authorities were able to identify the worldwide network of servers involved in the attacks. Because the German investigators have had visibility on this network of servers

[5] To further obfuscate their scheme, the administrators of Avalanche deploy an even more sophisticated type of fast fluxing, referred to as "double-flux" or "double fast-flux" which is characterized by multiple nodes within the network registering and de-registering their addresses as part of the DNS Name Server record list. In other words, not only do the IP addresses for domains flux, the name servers that contain those records actually flux as well. This provides an additional layer of redundancy and survivability within the malware network.

for the past several years, they have been able to map its infrastructure and determine when old servers are cycled out and replaced by new servers conducting the same criminal activity. This network/infrastructure of servers is referred to as "Avalanche."

12. In June 2015, the FBI began collaborating with Germany's investigation of the Avalanche infrastructure. As part of that investigation, the FBI obtained court-authorization to place pen register/trap and trace devices[6] on over a half-dozen U.S.-based servers that acted as "second-level" servers in the Avalanche infrastructure.[7] Through these pen register devices, the FBI could see connections from all of the servers that were connecting to the monitored server, as well as where the traffic from the monitored server was sent. These pen register/trap and trace devices further assisted the FBI in "mapping out" or identifying the Avalanche infrastructure of servers.

13. Grand Jury subpoenas were sent to the internet service providers from whom the Malware Actors and Administrators were renting these servers. By reviewing the records and interviewing the victims, the FBI confirmed that two of the servers were paid for with stolen credit cards. The FBI believes that all of the monitored servers were paid for through fraudulent or illegitimately derived means.

14. Regarding the traffic coming *to* the second-level servers, the FBI was able to conduct a frequency analysis to determine which IP addresses connected most often to the monitored servers. In turn, the FBI queried those IP addresses through publicly available sources to

---

[6] A pen register/trap and trace device is a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.

[7] A pen register was also placed on a "back-end" malware server in Buffalo that was the control server for url-zone malware, a banking trojan.

determine which domains were hosted on those first-level servers. Many of the domains hosted on the first-level servers were presaged in the list of domains provided to your Affiant by German authorities as a result of their reverse engineering of the DGA's. Not only were these domains presaged by German authorities, but shortly after the domains were activated, many were determined by security researchers to be malicious. Moreover, as described above, your Affiant has queried the DNS servers associated with many of these domains and observed that the perpetrators used fast-flux and double-flux techniques to constantly change the IP addresses and name servers associated with these domains.

15. Regarding the traffic coming *from* the second-level servers, during the investigation, the FBI saw a remarkably clear pattern where the malware second-level servers all connected with overwhelming frequency to a centralized back-end server. For example, at one time the FBI had pen registers on four second-level malware servers. These servers each sent the vast majority of their traffic (over 90%) to the central control unit, which at that time was located in Canada. The pattern established by both the source and destination traffic to the second-level malware servers indisputably corroborated the workings of the Avalanche infrastructure.

16. The Administrators of Avalanche periodically change central server locations in an effort to avoid detection by law enforcement.

Malware Families Run Over Avalanche

17. Based on mapping of Avalanche by German Law Enforcement and Cyber Security Researchers, and through FBI searches and Title III wiretaps on Avalanche's domain registration server, the following families of malware have been run over the Avalanche Infrastructure during the German and FBI investigation:

a. Andromeda;

b. Corebot;

c. GetTiny;

d. Gozi2;

e. KINS;

f. Matsnu;

g. Nymaim/GozNym;

h. Ranbyus;

i. Rovnix;

j. TeslaCrypt;

k. Tiny Banker aka Tinba;

l. Trusteer App;

m. UrlZone;

n. VM Zeus;

o. Vawtrak; and

p. Xswkit.

18. Based on mapping of Avalanche, the FBI, German Law Enforcement and Cyber Security Researchers have been able to identify multiple families of malware utilizing the Infrastructure. Some of the families utilize Domain Generation Algorithms (DGA) to generate domains that are used to establish a channel of communication from the compromised systems to the command and control servers.

19. Of the families in paragraph 17, seven contain known and reverse engineered Domain Generation Algorithms:

a. Corebot;

b. Matsnu;

c. Nymaim/GozNym;

d. Ranbyus;

e. Rovnix;

f. Tiny Banker aka Tinba; and

g. UrlZone.

These families will be discussed in more detail below.

20. The remaining nine malware families[8] either utilize DGAs to generate domains that have not been reverse engineered, use domains that are hardcoded into the malware itself, or are manually registered by the subjects. Because of this, German Law Enforcement, the FBI, and Cyber Security Researchers have only been able to identify the registered domains associated with these nine malware families.

Domain Generation Algorithms

21. Malware authors are constantly looking for features of persistence, stealthiness and resilience in order to remain functional. One of the most popular mechanisms to bypass law enforcement detection is the use of Domain Generation Algorithms. DGAs are not recent and have existed over the last decade; although in the past they were mainly used as a backup communication mechanism. Nowadays, DGAs are the primary method and the main building

[8] Andromeda; GetTiny; Gozi2; KINS; TeslaCrypt; Trusteer App; VM Zeus; Vawtrak; and Xswkit

block for the establishment of a communication channel between compromised systems and the command and control servers (C&Cs). The adoption of a domain generation algorithm allows criminals to generate a large number of domain names, which are later contacted in the hope of meeting the command and control server (Rendezvous Point). The distributed malware containing the DGA is designed to compute and continuously go over a configurable list of domains in an attempt to retrieve or send information back to the C&C. The domain generation can result not only in a small number of instances but thousands of unique domain names on a daily basis. For instance, the malware family from Conficker.C generates 50.000 domains per day. Thus, making detection more complex and resistant to blacklisting and/or takedown efforts.

22. DGAs depend on a combination of fixed and/or dynamically calculated values, i.e., seeds, with multiple properties. These parameters are necessary for the DGA execution and are known to a certain degree. The exception are non-deterministic DGAs, like the DGAs of the Bedep malware family, which use the foreign exchange reference rates published daily by the European Central Bank, as well as Torpig, which used Twitter trends for seeding. In such scenarios, criminals are forced to compete with law enforcement for the registration of domains in each active time window once the unpredictable data used for seeding becomes available. Typical (predictable) parameters include numerical constants such as the character length of domains, e.g., 24, seeds for pseudo random number generators (PRNGs), e.g., 1664525, strings such as the alphabet, e.g., "qwertyuiopasdfghjklzxcvbnm123945678" or the set of possible top level domains (TLDs), e.g., ".com"

23. A seed is the key and most common parameter found among different DGA classes to parameterize the generation of domains. It serves as a shared secret required for the calculation

of generated domains, also referred to by the term Algorithmically-Generated Domains (AGD). Seeds are composed of a set of properties, which are required for the execution of a particular instance of a DGA. Therefore, the actual algorithm of the DGA can remain the same for several versions of a malware family. Changing the seeds is enough to calculate different domains for the different malware versions.

Classes of DGAs

24. Different seeds may have different properties, which may characterize the DGA, for instance:

a. **Time dependent DGA:** This type of DGA incorporates a time based input such as the system time of the compromised host or from a DNS/HTTP response header. In consequence, generated domains will have a validity period.

b. **Deterministic DGA:** Is the type of DGA for which addresses are observable at any point in time, i.e., can be computed for past and future instances, having as requirement availability of all input parameters.

c. **Time dependent non-deterministic DGA:** This type incorporates unpredictable parameters to its execution. This is done in order to disallow arbitrary prediction of future algorithmically-generated domains by using e.g., publicly accessible data for seeding.

d. **Arithmetic-based DGAs** calculate a sequence of values that either have a direct ASCII representation usable for a domain name or designate an offset in one or more hard-coded arrays, constituting the alphabet of the DGA. These are the most common DGAs.

e. **Wordlist-based DGAs** concatenate a sequence of words from one or more wordlists,

resulting in less random looking and therefore more concealed AGDs. These wordlists are either directly embedded in the malware binary or obtained from a publicly accessible source.

f. **Hash-based DGAs** use hexadecimal digest representation of a hash value to produce algorithmically-generated domains, e.g., MD5 or SHA256.

g. **Permutation-based DGAs** derive all possible algorithmically-generated domains through permutation of an initial domain name.

Reverse Engineered DGAs

25. As discussed above, Cyber Security Researchers have been able to reverse engineer DGAs associated with seven of the malware families utilizing the Avalanche Infrastructure. Because of this, Law Enforcement is able to know the entire universe of domains, registered and unregistered, that are possible for each of these malware families.

Corebot

26. Corebot is a Trojan with a focus on stealing banking and credential information. The malware uses social engineering to trick victims into divulging personal information and credentials from several financial platforms. It was first discovered and documented by researchers at Security Intelligence. Among its capabilities, Corebot stands out for its modular design, which allows enhancing the malware with extra features delivered remotely as plug-ins. It includes a DGA, browser-based web injects, which resembles functionality from the Zeus banking Trojan, a preconfigured list of bank urls to be used with its form grabbing module, and a virtual network computing (VNC) module for remote control.

27. Corebot's DGA is deterministic and time dependent. The malware determines the current

date by sending an HTTP request to Google and querying the date and time within the response's header. In addition, it is configurable and designed to generate from 40 to 50 domains for a given date. To generate single domains, it uses the initialized charset, i.e. *"abcdefghijklmnopqrstuvwxy012345678"*, to choose random characters from a composite seed made up of two constants, i.e., 1664525 and 1013904223 and the upper and lower bound for each domain length.

28. Corebot's DGA needs the following parameters:

a. *day:* (current) date.

b. *charset*: corresponds to the length of the array of ASCII characters used when generating the domain.

c. *seed*: the seed is obtained by generating a random number initialized using a hardcoded seed. This binary-embedded value differs among samples seen in the wild.

d. *domain_min_len*: inclusive lower bound on the length of generated domains.

e. *domain_max_len*: exclusive upper bound on the length of generated domains.

In addition, the DGA depends on a predefined value, which determines the amount of domains generated on a daily basis and a list of top level domains (TLDs).

Matsnu

29. Matsnu is a malware dropper, which serves as a vehicle for delivering and executing further malware. Since its first appearance, the malware has evolved not only in terms of its goal but as well as in functionality. Matsnu's main feature is an open door for running system commands on the compromised system. As a result, victims are vulnerable to remote manipulation and illegal execution of further malware. Matsnu uses cryptography, code obfuscation, anti-reversing, anti-

VM and anti-sinkhole techniques as protection schemes to hinder analysis. Matsnu employs HTTP POST requests to submit all information to the C&C. The HTTP POST messages are encrypted with RSA using a public key embedded in the bot binary. The server responds to these POST requests with an AES encrypted payload using a 256-bits AES key that is sent by the bot during its first POST request. Matsnu has been active for several years in the context of the Avalanche infrastructure.

30. Matsnu's DGA features a deterministic and time-dependent DGA. The implementation allows criminals to set a desired number of domains to be generated per day and a number of days (in the past) in order to reuse previously generated domains. A common configuration seen in multiple samples generates domains for the previous two days.

31. Domain names are based on nouns and verbs from a wordlist, which can be updated at any time by the C&C once Matsnu has successfully reported the infection. This characteristic allows Matsnu to bypass machine learning or phonetic based algorithms for detection of DGA-generated domain names. Such techniques depend on names with no explicit significance, e.g., concatenation of random characters, while Matsnu constructs English-phrased domains and therefore increasing resilience to takedowns.

32. Matsnu's DGA is configured by setting values for the following parameters:

a. *magic_1:* this value is a constant seed embedded within the binary and is used for calculating a random index for selecting words from each of the wordlists.

b. *magic_2:* similar to *magic_1.*

c. *num_domains:* number of domains to generate per day.

d. *days:* interval of days to reuse domains.

Nymaim/GozNym

33. Nymaim is a multipurpose malware family present on the Avalanche infrastructure since at least 2013. Its modus operandi has been shifted a couple of times. First, it was said to be a ransomware and malware dropper in 2013. Then, it was mainly used as a malware dropper and credential stealer, through the use of keylogging, in 2014 and 2015. In 2016, parts of the malware family Gozi were merged into Nymaim in order to enhance Nymaim with wire fraud capabilities. This latest version is also known as Goznym.

34. Nymaim's DGA is deterministic and time-dependent. It takes two parameters as input: the date and a seed. It uses the English alphabet and only lower case letters for domain generation. Its PRNG is xorshift. It generates 30 new domains each day.

35. Nymaim's developers only change small portions of their code over time. The current DGA has been stable for more than one year. However, from time to time they embed new seeds.

36. The algorithm consists of the following steps:

a. derive daily seed from seed and date, this daily seed will be used as input to the random number generator. It repeats the following for the 30 domains.

b. ask xorshift for number, use it as domain length or domain length, generate characters

c. add the "."

d. ask xorshift for a number, use this number to look up the top level domain in a top level domain table

e. output the 30 generated Domains

Ranbyus

37. Ranbyus is a banking Trojan based on the Zeus/Zbot source code leaked in early 2011. Although this family's main functionality is the redirection of cash flows, it does not implement webinjects to manipulate banking websites. Instead, it focuses on the manipulation of remote banking software, e.g., Ranbyus modifies the Java bytecode of iBank2, a popular online banking software in Ukraine. This family has been reported to focus on Ukraine and eastern European countries.

38. Ranbyus DGA takes several input parameters and computes domains in a loop using a date based sliding window. During the first iteration, it uses the current date, for the next iteration (index is -1) it uses instead the current day minus one day. The same behaviour may continue for intervals of 30 days in order to not only generate a new set of domains per day, but also to check domains for the past days. This gives the DGA the benefit of fast changing domains in case domains gets blocked or sinkholed, while at the same time enabling older domains to be used for up to one month if they still work.

39. Ranbyus' DGA can be initialized by providing the following parameters:

a. *domains_per_day:* the malware generates domains with the granularity of 40 domains per date for the last 30 days.

b. *domain_length:* the length among versions of the DGA varies from 14 up to 17.

c. *magic:* hardcoded magic number.

d. *version:* either '32' or '64', distinguishing DGAs of the first ('32') from the second generation ('64')

e. *tlds:* the malware comes packed with a harcoded list of top level domains. TLDs are checked one after another, except of the last one due to an error in the implementation.

40. Ranbyus' DGA has been updated at least once according to changes found in September 2015, which corresponded to an increase in the length of its generated second level domains, e.g. from 14 to 17 characters. This change of length differs from the first version, which used the data variables in the calculation.

Rovnix

41. Rovnix is a banking Trojan with bootkit capabilities. It is based on the Rovnix source code leak and has been used in Avalanche since May 2015.

42. The DGA of the Avalanche version of Rovnix is time-independent and deterministic. It just generates 10,000 domains. The domains are 18 characters long and it uses [a-z] and [1-8] as alphabet. The domains have one of five top level domains: .ru, .com, .net, .biz, and .cn.

43. The DGA works as follows:

a. Initialize PRNG with the hardcoded seed;

b. Generate 10,000 domains as follows:

c. Generate 18 characters, request random number and draw from alphabet;

d. Append the top level domain;

e. request random number and draw it from the set of top level domains; and

f. Return 10,000 generated domains.

TinyBanker aka Tinba

44. Tinba is a banking Trojan with a very small footprint. Its source code has been leaked. As a consequence various groups have implemented their own versions based on the source code leak. An outstanding example is the version including a DGA and message authentication enhancements. Tinba has been part of the Avalanche infrastructure since 2015.

45. Tinba's DGA is a deterministic DGA. The algorithm starts by sending DNS requests and checking for any response. If no successful response is obtained it decreases a hardcoded value and proceeds to generate a new domain. This value is the maximum number of domains to be generated. The generation of domains happens along a looping function using one hardcoded domain name as seed and a harcoded string as the salt. Each of the new generated domains serves as input for generating the next one. A particular characteristic of Tinba's DGA is that it does not use date/time parameters for the domain generation, but rather it uses the domain name as seed for generating the next domain.

URLZone/Bebloh

46. URLZone, known as well as Bebloh or Shiotob, is a banking trojan first discovered in 2009. Since then, it has been regularly updated in order to remain compatible with later Windows versions. The malware includes functionality to steal user credentials - most notably information related to banking. The malware injects itself into explorer.exe, from there it is capable of gathering information from the victim's environmental variables and registry configuration, deleting files from the IE's Internet Options, e.g., removing the cache's physical content such as HTML pages, pictures, scripts etc.; key logging and serve as backdoor. URLZone requests commands from its C&C server by contacting domains in a polling scheme

one after the other until obtaining a response from its C&C server. URLZone C&C server(s) exist within the context of the Avalanche infrastructure.

47. URLZone includes a deterministic and time-dependent DGA. Predefined URL strings are embedded in each binary serving as the starting point for the DGA. Each seed, i.e, hardcoded domain, and timestamp are passed to the malware DGA function over an infinite loop in an attempt to POST data to the generated domains. The loop stops only when a successful POST is made to a C&C server. The number of generated domains is time-dependent and is taken from the current timestamp after every loop. The elapsed time since the beginning of the malware execution is then compared to different intervals. For instance, if the uptime is between three and six days, then the loop counter is reset to one after 500 iterations. When the loop counter is reset to one, the current domain is also reset to the seed domain. This logic of always resetting back to the seed domain allows the DGA routine to generate domains forever.

48. The bot is configurable with a hardcoded url as seed. The URL is stored in a data structure embedded in the binary where it is also possible to find the timestamps and two more DGA-related values cached during execution. The following url's are hardcoded domain seeds:

a. wtipubctwiekhir.net

b. mygzekuywtuka4a.com

c. dsaoe5pr95.net

d. 4ehxuoqximp94uj.com

e. dogcurbctw.com

f. n9oonpgabxe31.net

g. 2oidwapmv2cwp.com

h. skwskzyp2ktoc.com

i. pb9r9w5bk5bipws.com

j. fjinfobp425xsnt.com

k. ebfszfmcg325fnr.net

l. salayaddu.com

m. latinulcer.com

n. cetintosy.com

o. ox2ybl1nf4muo3.net

p. frijafoute.com

q. oilyalada.com

49. Attachment * through * contain a list of all registered US domains associated with the above 16 malware families utilizing the Avalanche Infrastructure. Attachment * through * contain a list of all unregistered US Domains associated with the seven malware familes with reverse engineered DGAs. The attachments are seperated by TLD.

The Defendants

50. On February 5, 2016, the Honorable Lisa Lenihan signed a search warrant for the Avalanche Jabber and domain registration server. A second search warrant was signed March 25, 2016, by the Honorable Maureen P. Kelly.

51. During the searches of the Avalanche domain registration server, Law Enforcement discovered a list of domains registered by the administrators of Avalanche. Contained in this list of registered domains, were a set of domains registered in or around 2010. Based on prior FBI

investigations and open source information, these domains were registered and used during Zeus v1 campaigns.

52. On March 4, 2016, a Title III intercept authorization was signed for the Avalanche Jabber and Domain Registration server. A second authorization was signed on April 4, 2016, and a third authorization was signed on April 29, 2016.

53. The searches and Title III intercepts of the Avalanche Jabber and domain registration server yielded evidence crucial to the Avalanche investigation. The searches revealed that there were two administrators for the private Jabber run over the server—flux@j[redacted] aka ffhost@[redacted] and flux2@[redacted] aka ffhost2@[redacted].[9] Furthermore a "buddy list" from the Jabber was also located. The buddy list contained more than 100 other Jabber accounts that were authorized to communicate over the server with Flux and Flux2. Your affiant believes that these accounts belong to customers of the Avalanche administrators, who operate the malware and money mule schemes run over the Avalanche infrastructure. As of November 28, 2016, the following private Jabber domains are being used by the Avalanche administrators to communicate with and provide bulletproof hosting services to their customers: axmpp.net; skilljabber.net; and xmppchat.com.

54. Based on my knowledge of the investigation, I know that the administrators of Avalanche advertised their service on various criminal forums. For Example:

a. In November, 2015, an advertisement posted on the criminal forum Verified by "User41" advertised a fast fluxing bullet proof hosting service. The advertisement

[9] The "flux" and 'ffhost" handles for both administrators further demonstrates that the domain registration and Jabber server is the medium over which the administrators of Avalanche offer criminal services (fluxing and fast fluxing registration of malicious domains) to their clients (the users on the buddy list).

instructed potential customers to contact the administrators at flux@[redacted] and flux2@[redacted].

b. On October 12, 2015, a post made to the criminal forum Mazafaka by "Firestarter" advertised a fast fluxing bullet-proof hosting service. The advertisement instructed potential customers to contact the administrators at ffhost@[redacted]. In later posts by the same user this jabber contact was changed to ffhost@[redacted].

c. On March 24, 2016, another post made to Verified by "User41" advertised a fast fluxing bullet proof hosting service. The advertisement again instructed potential customers to contact the administrators at flux@[redacted] and flux2@[redacted].

d. On May 31, 2016, a post made to the criminal forum Mazafaka by "Firestarter" advertised a fast fluxing bullet-proof hosting service. The advertisement instructed potential customers to contact the administrators at ffhost@[redacted] and ffhost2@[redacted]. These jabber monikers were also present on the Title III discussed above.

55. As discussed above, between March, 2016 and May, 2016, the FBI conducted court authorized wiretaps of the Avalanche administrators private jabber server.

56. On April 25, 2016, support@j[redacted] wrote to flux@j[redacted], "I need a VPS." Flux@j[redacted] responded, "for what purpose is this required?" support@j[redacted] stated, "for a botnet."

57. Based on my knowledge of this investigation and my training and experience, support is requesting flux provide hosting services in order to run a botnet over the Avalanche Infrastructure.

Flux, as an administrator of the Infrastructure, is asking why the VPS is needed so he can provide the appropriate service for the customer.

58. On May 5, 2016, ffhost2@[redacted] wrote to maestr0@x[redacted], "we can suggest a fastflux – redirection of traffic to your server (the abuse of service complaints remain with us. You get your usual legal server and we proxy the traffic there). The cost is 150 a week or 450 for 4 weeks. Upon payment we immediately fend off your abuse of service complaints."

59. Based on my knowledge of the investigation and my training and experience, during this chat, ffhost2 is describing the Avalanche hosting service to a potential customer. Ffhost2 further advised the customer that use of this service will cost $150 for a week or $450 for four weeks.

60. On May 11, 2016, flux2@[redacted] wrote to chop@[redacted], "Today is the deadline for hosting payment. If possible pay in Paymer. We would appreciate it ---- [WebMoney Account Number]."

61. Based on my knowledge of the investigation and my training and experience, flux2 is advising Avalanche customer chop that his bill is due. Flux2 further asks chop to use Paymer a form of online currency) and send the funds to WebMoney account [number]. Based on my knowledge of the investigation, this was the WebMoney account that received all Avalanche customer payments.

62. Based on the information in the preceding paragraphs, the FBI believes that the individual using the jabber accounts flux@[redacted] and ffhost@x[redacted] utilized these accounts to administer the Avalanche service. The evidence above positively links flux aka ffhost to the administration of the Avalanche Infrastructure.

63. Based on the information in the preceding paragraphs, the FBI believes that the individual using the jabber accounts flux2@[redacted] and ffhost2@[redacted] are the same person and utilized these accounts to administer the Avalanche service. The evidence above positively links flux2 aka ffhost2 to the administration of the Avalanche Infrastructure.

Need for *Ex Parte* Relief

64. Based on my training and experience, including both my investigation of Avalanche and other cyber-criminal entities and my knowledge of how Avalanche 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 Avalanche Infrastructure. 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.

65. Avalanche is an evolving Infrastructure, and the Defendants are skilled cyber criminals, easily able to change and update their infrastructure and malware running over that infrastructure. Nearly the entire Avalanche Infrastructure can be updated within 24 hours. The Avalanche Infrastructure has been updated in this manner previously.

****[START REQUESTED REDACTION #1 OF 2]****

66. [redacted]

[redacted]

[END REQUESTED REDACTION #1 OF 2]

D. Need to Redact Operational Information

67. The sources and methods used to conduct the technical disruption operation described will remain highly sensitive, even after the operation ends and the indictment and other court papers are unsealed. Exposing those sources and methods would jeopardize future efforts to disrupt similar criminal activity.

68. 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.

Avalanche Subjects Have Harmed Victims in this District and Throughout the United States

69. In January, 2015, German authorities investigated a second-level Avalanche server in Germany using IP address 85.10.206.168 that was suspected of being involved in the distribution of Nymaim, a malware that, among other things, encrypts a victim's files until the victim pays a ransom to the perpetrator. German authorities were able to determine the unique IP address of victim machines that were sending information to the first-level servers, as well as the malicious

domains that were associated with the Nymaim infection. The data suggested that there were many victims worldwide, including in the Western District of Pennsylvania.

70. After the FBI began collaborating with Germany in June 2015, German authorities provided the list of victim IP addresses from the Western District of Pennsylvania that were emanating from computers likely infected with Nymaim in January 2015.

71. The German authorities provided a victim IP address to the FBI. The data from Germany showed that on January 6, 2015 and January 7, 2015, this IP address made direct contact with two first-level Avalanche servers (IP addresses 209.200.45.28 and 191.101.13.217) that were suspected of distributing Nymaim malware to victim machines. These first-level servers forwarded the traffic from the infected machine to the second-level server in Germany (IP address 85.10.206.168) and then onward to a third-level Avalanche server at IP address 217.23.15.11. These servers were mapped and identified as being part of the Avalanche network of servers. German authorities were also able to identify the malicious domain associated with the Nymaim infection as "ivehtxenoe.ru."

72. Based upon this information, the FBI queried the victim IP address through a public records database which showed that this IP address was registered to a state governmental entity in Allegheny County. The FBI called the technical point of contact for the victim to inquire whether there had been any computer intrusions on or around January 7, 2015. This contact confirmed that there had been a computer intrusion on or around January 7, 2015, in which a number of files on its server had been encrypted and that the perpetrators demanded a ransom to decrypt the files. The FBI was subsequently provided copies of paperwork confirming that on January 22, 2015, the

victim paid a ransom of six Bitcoin—roughly $1,400—in exchange for a decryption tool that could be used to decrypt the files.

73. With the assistance of the state governmental entity, the FBI was able to locate the computer believed to be infected by the perpetrators and confirm that the victim IP was an external facing IP address used by the state governmental entity. Subsequent analysis of that machine by an FBI forensics expert confirmed that the victim machine had been infected with Nymaim and that the domain "ivehtxenoe.ru" was found in a page file of the victim machine. This forensic evidence directly corroborated the data provided by German authorities.

74. In September 2016, FBI-Pittsburgh became aware that a company, based in New Castle, PA, was the victim of multiple Account Takeover (ATO) Frauds from February, 2016 through April, 2016. An employee of the New Castle company was interviewed by the FBI. According to the employee, on February 18, 2016, the company received an email containing an attachment that appeared to be an invoice. When the attachment was opened, it was blank.

75. On February 24, 2016, three wire transactions totaling $121,132.08 were attempted from the company's online bank account. The wire transactions were stopped by the company's bank and no money was lost.

76. On April 12, 2016, the New Castle company was contacted by their bank and notified that there were four additional suspicious wire transactions totaling $122,000. The employee notified the bank that the company was not initiating any wire transactions and the suspicious wires were stopped before any money was lost.

77. The employee consented to FBI-Pittsburgh's forensic imaging of the infected machine. After a forensic analysis of the infected machine, GozNym malware was located and identified.

No other malware variant was present on the machine. As discussed above, GozNym is updated version of Nymaim.

78. On April 11, 2016, the FBI-Pittsburgh Office was notified that a company headquartered in Carnegie, Pennsylvania, had been the victim of an ATO fraud that resulted in the issuance of a fraudulent wire transfer in the sum of $387,500 (USD), from a Pittsburgh based Financial Institution to a Bulgarian bank account.

79. An employee of the Carnegie company was interviewed by the FBI. According to employee, on April 07, 2016, company received an email containing a Word attachment. The attachment appeared to be an invoice and, when opened resulted in a malware loader being installed on the machine as confirmed by antivirus logs. On April 11, 2016, at approximately 11:00 am, employee became aware that a fraudulent wire transaction for $387,500 had been initiated from the company's online account. Employee immediately notified the bank and a wire recall was initiated. Ultimately, the wire transfer was recalled and company suffered no loss.

80. After the fraudulent attempt, employee scanned the infected machine with MS Endpoint Virus protection. The antivirus (AV) program quarantined "TojanDownloader:097M." According to the AV logs, this loader was installed on the infected machine on April 7, 2016, the same day the suspicious Word attachment was opened. Based on my experience and open source research, I know that this loader has been used in the recent past to download GozNym malware.

81. Employee consented to FBI-Pittsburgh's forensic imaging of the infected machine. After a forensic analysis of the infected machine, GozNym malware was located and identified. No other malware variant was present on the machine. As discussed above GozNym is an updated version of Nymaim.

82. Additionally, victim machines located in the Western District of Pennsylvania were identified as victims of Corebot. In October 2015, German authorities informed the FBI that a new malware, Corebot, was running over Avalanche. In October 2015, German authorities began to investigate a first level Corebot server in Germany that used IP address 5.230.4.28. Publicly available information shows that the domain "pomppondy.net" resolved to the first level German server that used IP address 5.230.4.28 during the time when the Germans were investigating that server. Furthermore, information from security researchers confirms that the Corebot malware was instructed to call back to the domain "pomppondy.net" as well as a secondary domain "tychebruke.com." German authorities provided a list of many U.S. machines, including a number of machines in the Western District of Pennsylvania, whose IP addresses called back to the German Avalanche server hosting Corebot in October 2015. Based on the foregoing, your affiant has probable cause to believe that these machines were infected with Corebot malware that was run over the Avalanche infrastructure. Furthermore, as referenced above, a search of the Domain Registration Server in February 2016 revealed that these known Corebot domains, "pomppondy.net" and "tychebruke.com," were registered through and are currently listed on the database of domains contained on the Domain Registration Server.

The United States is Prepared to Disrupt Avalanche and the Families of Malware Utilizing the Infrastructure

83. The Germans have developed a plan to disrupt the Avalanche Infrastructure and the families of malware utilizing the Infrastructure. The U.S. Law Enforcement will be assisting German Law Enforcement to execute a plan that is very similar to the disruptions of the Game Over Zeus botnet and the Dridex botnet, both of which were executed in the Western District of

Pennsylvania. A review of the technical disruption effort and subsequent remediation campaign is provided below.

[START REQUESTED REDACTION # 2 of 2]

84. [redacted]

[redacted]

[redacted]

[redacted]

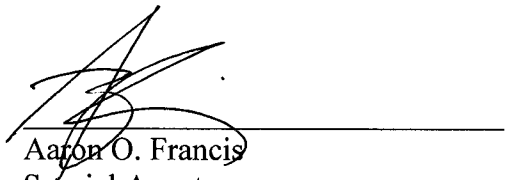
[redacted]

[redacted]

10 [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 28th day of November, 2016, in Pittsburgh, Pennsylvania.



Aaron O. Francis
Special Agent
Federal Bureau of Investigation