

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

IN THE MATTER OF THE SEIZURE OF THE
DOMAIN NAME:

toknowall.com

Magistrate No. 18-665

~~[UNDER SEAL]~~

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE WARRANT**

I, Michael McKeown, Special Agent of the Federal Bureau of Investigation (“FBI”), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) and have been so employed since January 1999. I am currently assigned to the Pittsburgh Division of the FBI, Cyber Squad. In this capacity, I am charged with investigating possible violations of federal criminal law, specifically those involved with cybercrimes. By virtue of my FBI employment, I perform and have performed a variety of investigative tasks, including functioning as a case agent on computer crime cases. I have received training in the conduct of computer crime investigations. I have also received training and gained experience in interviewing and interrogation techniques, the execution of federal search warrants and seizures, and the identification and collection of computer-related evidence. In addition, I have personally participated in the execution of federal search warrants involving the search and seizure of computer equipment.

2. I am an “investigative or law enforcement officer of the United States” within the meaning of 18 U.S.C. § 2510(7), as a Special Agent of the FBI. As such, I am empowered to conduct investigations of and to make arrests for offenses enumerated in 18 U.S.C. § 2516,

including 18 U.S.C. § 1343 (wire fraud), and for other federal felony offenses, such as 18 U.S.C. § 1030 (fraud and related activity in connection with computers).

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. I make this affidavit, pursuant to Title 21, United States Code, Section 853(f), for issuance of a warrant (the "Seizure Warrant") to seize the following domain name:

toknowall.com

(the "**SUBJECT DOMAIN NAME**") for the purpose of criminal forfeiture.

5. As set forth below, there is probable cause to believe that the **SUBJECT DOMAIN NAME** constitutes personal property that was used or intended to be used to commit or to facilitate the commission of damage to protected computers, in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (B). Accordingly, the **SUBJECT DOMAIN NAME** is subject to criminal forfeiture to the United States pursuant to 18 U.S.C. §§ 1030(i)(1)(A) and (j)(1). Pursuant to 21 U.S.C. § 853(f), the Government may request the issuance of a warrant to seize property subject to forfeiture in the same manner as provided for in a search warrant.

6. The procedure by which the Government will seize the **SUBJECT DOMAIN NAME** and redirect traffic attempting to resolve to that domain from a server controlled by those conducting the criminal activity to a server controlled by the United States, is described herein and set forth in detail in Attachment A to the Warrant and Order.

7. As set forth in greater detail below, the **SUBJECT DOMAIN NAME** is used to control malicious software that has infected electronic devices (i.e., routers) in the United States

and elsewhere, in violation of 18 U.S.C. § 1030(a)(5)(A) and (B) (the “SUBJECT OFFENSES”).

RELEVANT DEFINITIONS

8. Based on my training and experience, I know the following:

Internet Domain Name System

a. A domain name is a simple, easy-to-remember way for people to identify computers on the Internet. For example, “www.justice.gov” and “www.google.com” are domain names. The Domain Name System (“DNS”) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or “labels,” that are delimited by periods, such as “www.example.com.” The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, the “example” second-level domain, and is a web server (denoted by the “www”).

b. DNS servers are computers connected to the Internet that convert domain names that are easy for humans to remember into Internet Protocol (“IP”) addresses, which are unique machine-readable numeric addresses that computers use to identify each other on the Internet. DNS servers are usually owned and operated by Internet Service Providers to be used by their customers. Every computer connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. DNS servers can be said to “resolve” or “translate” domain names into IP addresses.

c. For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domains resolve to which IP addresses. For example, the registry for the “.net,” and “.com” top-level domains is VeriSign, Inc. (“VeriSign”),

12061 Bluemont Way, Reston, Virginia. Registries are responsible for maintaining the registry for each top-level domain. The responsibilities of the registry includes accepting registration requests (whether from registrars or directly from domain name registrants), maintaining a database of the necessary domain name registration data and providing name servers to publish the zone file data (i.e. information about the location of a domain name) throughout the Internet.

d. If an individual or business wants to purchase a domain name, he or she must purchase it through a company called a “domain name registrar.” The registrar, in turn, communicates this purchase to the relevant registry. The registrar also creates the associated DNS records. The registrar owns and manages the name servers, which are used to host the actual DNS records.

e. The individual or business who purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world simply by changing the IP address at the registry.

Other Terms Relevant to Botnet Disruption Operations

f. A “router” is a networking device that forwards data packets between computer networks. Routers direct Internet traffic. A data packet is typically forwarded from one router to another router through the networks that constitute an internetwork until it reaches its destination.

g. Based on open sources, a “network access storage (NAS) device” is dedicated hardware device made up of several hard drives used to store data in a single location. A NAS device offers an easy way for multiple users to access the same data, which is important in situations where users are collaborating on projects.

h. The term “sinkhole” is the redirection of network traffic, which is typically

malicious in nature, from its original destination to a new destination where its malicious function will instead have a harmless or limited effect. The technique is most commonly used by cybersecurity researchers to redirect infected computers in a botnet to specified research machines to capture data about them. The technique is also occasionally used in conjunction with law enforcement operations to take control of infected victim computers in a botnet away from cyber criminals.

i. “Photobucket” is a company that owns and operates an image hosting website of the same name that can be accessed at www.photobucket.com. Photobucket offers cloud storage for images, image file synchronization, image file editing and mobile phone applications to access Photobucket services. Photobucket allows users to store image files in the cloud. Files placed into Photobucket are accessible through their website and mobile phone applications such as Google Android and Apple iOS.

j. “Router malware” typically involves a two-stage infection process. Stage 1 malware is typically executed after the initial compromise of a router. Typically, the initial compromise of routers can be achieved using a variety of techniques such as brute force attacks, exploits, and misconfigurations. The Stage 1 malware will typically contain several methods to locate and install Stage 2 malware. These methods can be in the form of an IP address and/or a domain name, such as the **SUBJECT DOMAIN NAME**, that connects to a computer controlled by the actor(s) on which Stage 2 malware is stored and awaiting deployment. Stage 2 malware typically gives the attacker an array of capabilities that are not available with Stage 1, such as stealing of files and software, deletion of files, elevation or escalation of privileges, keylogging and potential destruction of the victim file system.

**SUMMARY OF EVIDENCE ESTABLISHING PROBABLE CAUSE
TO SEIZE THE SUBJECT DOMAIN NAME**

Background Regarding the “Sofacy Group”

9. The United States is investigating unauthorized computer intrusions being perpetrated by a group known to private cybersecurity investigators as the “Sofacy Group” (also known as apt28, sandworm, x-agent, pawn storm, fancy bear and sednit). According to these cybersecurity researchers, the Sofacy Group is a cyber-espionage group believed to have originated from Russia. Likely operating since 2007, the group is known to typically target government, military, security organizations, and other targets of intelligence value, through a variety of means.

10. In some instances, the Sofacy Group utilizes a variety of malicious software (or “malware”) to carry out its activities. One type of malware attributed to the Sofacy Group is “BlackEnergy.” The BlackEnergy malware started out as crimeware toolkit that allows the malware to perform activities such as credential stealing, data exfiltration, and network traffic monitoring. In addition, BlackEnergy has capabilities that allow it to compromise specific types of routers, specifically ARM and MIPS central processing units typically found in devices such as home routers, mobile phones and tablets.

11. Additionally, BlackEnergy malware has been used in the targeting of critical infrastructure. Based on Department of Homeland Security (DHS) and open source reporting, BlackEnergy 2 was observed being used by the Sofacy Group in a sophisticated malware campaign to target United States Industrial Control Systems (ICSs) between late 2011 through 2014. In addition, BlackEnergy was used in the Ukrainian power grid attack in 2015 that targeted three regional electric power distribution companies impacting approximately 225,000 customers. The attackers used the BlackEnergy malware to gain a foothold into the Information Technology (IT)

networks of the electricity companies. The December 2015 incident was the first known instance where a cyber-attack disrupted electric grid operations.

“Sofacy Group” Malware Used to Compromise Victim Home Routers

12. The FBI learned of numerous possible victims throughout the United States, to include the Western District of Pennsylvania, that have been infected with a specific type of malware targeting home routers and NAS devices. The FBI and some private sector researchers have named the botnet “VPN Filter.”

13. On August 21, 2017, FBI agents in Pittsburgh interviewed one of the victims located in the Western District of Pennsylvania. This individual was the owner of a home router who confirmed that she had not provided authorization for any third parties to deploy malware onto her router. She voluntarily relinquished her router to the agents. In addition, the victim allowed the FBI to utilize a network tap on her home network that allowed the FBI to observe the network traffic leaving the home router. By focusing on the web traffic, the FBI observed the victim router was trying to connect to the Photobucket website and access the specific Photobucket account identified as “nikkireed11”. Based on these observations, along with information obtained from the FBI’s investigation, the FBI determined that the router was infected with malware.

14. On or about March 9, 2018, the FBI met with a reliable, credible Subject Matter Expert (“SME #1”) working in cyber “threat intelligence.” The SME #1 advised investigating agents that, during the course of his/her duties of gathering intelligence, he/she analyzed several malware samples that he/she had recently download from VirusTotal.¹ Based on the SME #1’s

¹ VirusTotal is a website that aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives. Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software.

analysis, the malware appeared to be targeting different types of routers, specifically ARM and MIPS architectures, similar to the BlackEnergy malware utilized by the Sofacy Group described above in relation to BlackEnergy.

15. Significantly, both malware samples analyzed by SME #1 attempted to contact specific Photobucket accounts as part of a Command and Control (C2) channel,² including the Photobucket account “**nikkireed11**” to which the infected router in the Western District of Pennsylvania was attempting to connect as described above. Also of significance is the fact that two of the malware samples analyzed by SME #1 attempted to communicate with the **SUBJECT DOMAIN NAME** as part of a secondary C2 channel.

16. Specifically, the forensic analysis conducted by SME #1 on the malware samples showed that:

- a. The malware sample with a SHA256 hash³ of 0e0094d9bd396a6594da8e21911a3982cd737b445f591581560d766755097d92 appeared to be Stage 1 malware that tries to communicate with one of four Photobucket accounts (specifically the accounts **nikkireed11**, kmila302, lisabraun87 and katyperry45) and the **SUBJECT DOMAIN NAME**, all of which were being used as C2 channels.

² Command and Control channels allow actors to issue commands and to compromise systems (often Internet-connected computers of home users that then form armies of infected computers under the actors’ control known as botnets). These communications can be as simple as maintaining a timed beacon or "heartbeat" so that the operators running the attack can keep an inventory of the systems they have compromised or use them for more malicious actions, such as remote control or data exfiltration.

³ SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA). Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity.

- b. The malware sample with a SHA256 hash of 50ac4fcd3fbc8abcaa766449841b3a0a684b3e217fc40935f1ac22c34c58a9ec appeared to be Stage 1 malware that tries to communicate with one of twelve Photobucket accounts (eva_green1, monicabelci4, katyperry45, saragray1, millerfred, lisabraun87, jeniferaniston1, amandaseyfried1, **nikkireed11**, suwe8, bob7301 and kmila302) and the **SUBJECT DOMAIN NAME**.

17. In addition to SME #1's analysis, the FBI met with another reliable, credible Subject Matter Expert ("SME #2") working in cyber "threat intelligence" who specializes in the reverse engineering of malware. The SME #2 also conducted forensic analysis on the same two malware samples from VirusTotal as analyzed by SME #1.

18. According to SME #2, his/her forensic analysis on the malware samples showed that:

- a. Each of the Stage 1 malware samples contains multiple Photobucket accounts that are being used as the C2 channel. The malware randomly chooses one of the Photobucket accounts.
- b. Once the Photobucket account is selected, the malware attempts to download an image from the Photobucket account that contains an IP address encoded in the EXIF⁴ data of the image where the Stage 2 malware is located.
- c. If the Photobucket C2 channel fails, the malware will direct the infected router to the **SUBJECT DOMAIN NAME** C2 channel in order to obtain the Stage 2 malware.

⁴ EXIF is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression.

d. The encryption algorithm being used in the Stage 1 malware is a modified RC4 stream cipher.⁵

19. Both SME #1 and SME#2 stated the RC4 stream cipher (described above) has only been observed before being used in the BlackEnergy malware, specifically BlackEnergy versions 2 and 3.⁶ As described above, the Sofacy Group has used the BlackEnergy malware in conjunction with malicious cyber activities, including ICS targeting.

20. A comparison of the malware samples identified by SME #1, SME #2 and the FBI, to include the victim home router located in the Western District of Pennsylvania (discussed above), revealed that the malware samples were all fundamentally the same. For example, the two malware samples and the victim home router in the Western District of Pennsylvania all attempted to communicate with the Photobucket account “nikkireed11.” Additionally, the malware samples used a number of the same C2 Photobucket accounts and the **SUBJECT DOMAIN NAME**.

The System That Resolves Communications to SUBJECT DOMAIN NAME

21. According to open-source records, when the actor(s) behind this malicious activity registered the **SUBJECT DOMAIN NAME**, they used the services of “Internet Domain Service BS Corp,” a domain name registrar based in the Bahamas. The domain name registrar reported this registration to VeriSign, the designated registry operator for the “.com” top-level domain. VeriSign updated its records to reflect that the name servers hosting the DNS records for the **SUBJECT DOMAIN NAME** belonged to “swiftydns.com,” in this case “ns1.swiftydns.com” and

⁵ A stream cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.

⁶ The primary modification to the RC4 steam cipher used in the VPNFilter botnet malware is a shortcut that makes for a simpler (and probably less secure) implementation. It is unclear if the actor(s) intentionally introduced this difference in order to break compatibility with other RC4 implementations, or if it was simply a mistake.

“ns2.swiftyns.com”.

22. As part of this registration process, the domain name registrar collects the contact information for this domain and publishes it in publically accessible WHOIS records. According to the initial WHOIS records for the **SUBJECT DOMAIN NAME**, it was registered to “Hew Donnatan” with an email address of “hew241985@gmx.com” and address “88 Wressle Road, Plumley, Plymouth, GB.” Through my training and experience, I know that this information is not confirmed by the registrar and may be fictitious or inaccurate. According to the current WHOIS records for the **SUBJECT DOMAIN NAME**, all of the previous registry information is the same except for the name servers hosting the DNS records which now reflects ones belonging to “topdns.com”, in this case “ns-canada.topdns.com”, “ns-uk.topdns.com” and “ns-usa.topdns.com”.

23. Upon seizure of the **SUBJECT DOMAIN NAME**, the government, like any owner of a domain will have the ability to redirect internet traffic attempting to resolve to that domain to servers of the government’s choosing, in this case one or more servers operated by the government. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the **SUBJECT DOMAIN NAME**, VeriSign, will be directed to restrain the **SUBJECT DOMAIN NAME** pending transfer of all right, title, and interest in the **SUBJECT DOMAIN NAME** to the United States upon completion of forfeiture proceedings. This ensures that changes to the **SUBJECT DOMAIN NAME** cannot be made absent court order or, if forfeited to the United States, without prior consultation of the United States.

24. As a result of the seizure of the **SUBJECT DOMAIN NAME**, the government will redirect any victim router or other device that would attempt to communicate with this domain name to one or more substitute servers which will be configured by the FBI to collect the source

of the communication (e.g., the originating IP address), but not the content of such communications (e.g., stolen data).

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

25. The **SUBJECT DOMAIN NAME** is subject to criminal seizure and forfeiture pursuant to the following statutory provisions.

26. Title 18, United States Code, Section 1030(a)(5)(A) imposes criminal penalties on whoever “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.” Subsection 1030(a)(5)(B) imposes criminal penalties on anyone who “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage.” Title 18, United States Code, Section 1030(e)(2)(B) defines a “protected computer” to include any computer “which is used in or affecting interstate or foreign commerce or communication.” Section 1030(e)(8) defines “damage” broadly, to include “any impairment to the integrity or availability of data, a program, a system, or information.”

27. Pursuant to 18 U.S.C. § 1030(i)(1), a court,

“in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order . . . that such person forfeit to the United States –

(A) such person’s interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation[.]”

28. Pursuant to 18 U.S.C. § 1030(j)(1), for purposes of subsection (i), property subject to forfeiture to the United States includes “[a]ny personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section” and “no property right shall exist” in such property.

29. With respect to procedure, 18 U.S.C. § 1030(i)(2) specifies that “[t]he criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of . . . 21 U.S.C. § 853 . . .” Title 21, United States Code, Section 853(f), in turn, provides that:

The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) of this section [relating to protective orders] may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

30. Finally, pursuant to 21 U.S.C. § 853(l), any district court of the United States “shall have jurisdiction to enter orders as provided in this section without regard to the location of any property which may be subject to forfeiture under this section[.]”

SEIZURE PROCEDURE

31. Upon service of the Warrant and Order, VeriSign, the registry for the “.com” top-level domain (the “SUBJECT REGISTRY”) shall be directed to change the authoritative name server for the **SUBJECT DOMAIN NAME** as detailed in Attachment A to the Warrant and Order, which is fully incorporated herein by reference.

CONCLUSION


32. For the foregoing reasons, I submit that there is probable cause to believe that the **SUBJECT DOMAIN NAME** is used in and/or intended to be used in facilitating and/or committing the **SUBJECT OFFENSES**. Accordingly, the **SUBJECT DOMAIN NAME** is subject to forfeiture to the United States pursuant to 18 U.S.C. § 1030(i)(1)(A) and (j)(1) and 21 U.S.C. § 853, and I respectfully request that the Court issue a seizure warrant for the **SUBJECT**

DOMAIN NAME.

33. Because the warrant will be served on VeriSign who controls the **SUBJECT DOMAIN NAME**, and thereafter, at a time convenient to it, will transfer control of the **SUBJECT DOMAIN NAME** to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.


34. Finally, and in order to protect the ongoing investigation and in consideration that much of the information set forth above is not otherwise publicly available, I respectfully request that this Affidavit be filed and kept under seal until further order of this Court and that notice of the seizure warrant be delayed until 30 days from the issuance of this warrant.

Respectfully submitted,



Michael McKeown
Supervisory Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
this 22nd day of May, 2018.



HONORABLE LISA PUPO LENIHAN
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF PENNSYLVANIA

ATTACHMENT A

(Seizure Warrant and Order to VeriSign, Inc.)

I. SEIZURE PROCEDURE

The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the registry identified in Section II (the "SUBJECT REGISTRY"). Upon seizure of the domain identified in Section III below (the "SUBJECT DOMAIN NAME"), the SUBJECT REGISTRY will take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the **SUBJECT DOMAIN NAME** cannot be made absent a court order, or if forfeited to the United States Government, without prior consultation with the Federal Bureau of Investigation. All name server fields will be changed to reflect the two domain names listed in this Section below and the SUBJECT REGISTRY is directed to change the authoritative name servers for the **SUBJECT DOMAIN NAME** to the following two domain names:

jocelyn.ns.cloudflare.com

plato.ns.cloudflare.com

II. THE SUBJECT REGISTRY

VeriSign, Inc.
12061 Bluemont Way
Reston, Virginia 20190

III. THE SUBJECT DOMAIN NAME

toknowall.com