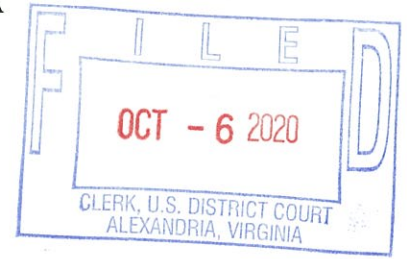


**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**



MICROSOFT CORPORATION, A)
WASHINGTON CORPORATION, AND FS-)
ISAC, INC., A DELAWARE)
CORPORATION,)
PLAINTIFFS,)
V.)
JOHN DOES 1-2, CONTROLLING)
COMPUTER BOTNETS AND THEREBY)
INJURING PLAINTIFFS, AND THEIR)
CUSTOMERS AND MEMBERS,)
DEFENDANTS.)

CIVIL ACTION NO: 1-20 CW 1171

FILED UNDER SEAL

**DECLARATION OF JASON B. LYONS IN SUPPORT OF APPLICATION FOR AN
EMERGENCY *EX PARTE* TEMPORARY RESTRAINING
ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION**

I, Jason B. Lyons, declare as follows:

1. I am a Senior Manager of Investigations in Microsoft Corporation's Digital Crimes Unit ("DCU") Malware & Cloud Crimes Team. I make this declaration in support of Microsoft'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 indicated. If called as a witness, I could and would testify competently to the truth of the matters set forth herein.

2. In my role at Microsoft, I assess technological security threats to Microsoft and the impact of such threats on Microsoft's business and customers. Among my responsibilities are protecting Microsoft's online service assets from network-based attacks. I also participate in the investigation of botnets and participate in court-authorized countermeasures to neutralize and disrupt them. I have personally investigated and assisted in the court-authorized takedown of

several botnets while at Microsoft, including the botnets known as Ramnit, ZeroAccess, Dorkbot, and Necurs. Before joining Microsoft, I worked for Xerox as the Manager of Xerox's Cyber Intelligence Response Team. I also worked for Affiliated Computer Services ("ACS") prior to Xerox's acquisition of ACS. While at ACS, I provided in-court testimony in connection with a temporary restraining order application concerning misappropriation of ACS's intellectual property. Prior to entering the private sector, from 1998 to 2005, I served as a Counterintelligence Special Agent in the United States Army. My duties as a Counterintelligence Special Agent included investigating and combating cyber-attacks against the United States. I obtained certifications in counterintelligence, digital forensics, computer crime investigations, and digital media collection from the United States Department of Defense. A true and correct copy of the current version of my curricula vitae is attached to this declaration as **Exhibit 1**.

3. I have investigated the structure and function of a botnet architecture called "Trickbot" as well as the activities carried out through this botnet, and an assessment of the impact on Microsoft's business and on users of the Internet. The Trickbot botnet has caused, and continues to cause, extreme damage to Microsoft and other parties which, if allowed to continue, will be compounded as the case proceeds.

I. DEFENDANTS

4. The identities and specific locations of the Defendants who have set up and currently operate the Trickbot botnet are currently uncertain. However, we have detected instances of the Trickbot botnet and Trickbot "command and control" infrastructure in many different countries, including the United States, and it is probable that the criminals operating that botnet are also located in different countries.

5. Defendants control the Trickbot botnet through command and control infrastructure comprised of IP addresses maintained on an interconnected network. They use common tools, a common codebase, and common tactics to establish and run the botnet. They appear to share botnet command and control resources. In sum, my investigation has uncovered what is, in effect, a Trickbot botnet criminal enterprise, comprised of Defendants who develop, commercialize and

support the Trickbot botnet using infrastructure designed for the purpose of carrying out the botnet criminal activity.

II. BOTNETS IN GENERAL

6. A botnet is a network made up of end user computers connected to the Internet that have been infected with a certain type of malicious software (“malware” or a “Trojan”) that places them under the control of the individuals or organizations who utilize the infected end user computers to conduct illegal activity. These infected computers are sometimes referred to as “bots.” A botnet network may be comprised of as few as hundreds or as many as tens of thousands or millions of infected end-user computers, thus creating a network of bots.

7. Once an individual or organization has created a botnet, they can use its scale, combined computing power, and ability to monitor and manipulate the online activities of the infected computer devices to engage in malicious, illegal activity. These illegal activities range from distributing ransomware, attacking other computers on the Internet; installing other forms of malicious software; sending spam email; stealing credentials for online accounts, including financial accounts; stealing personal identifying information; stealing confidential data; selling or renting access to the infected computer devices to other cybercriminals; and other illegal activities.

III. THE INVESTIGATION OF THE TRICKBOT BOTNET

8. The botnet at issue in this case—the “Trickbot” botnet—is a prolific and globally dispersed financial malware distribution botnet. I and other Microsoft investigators have been able to identify operational details about the Trickbot botnet, including its command and control infrastructure, the methods of communications among infected computers, how the botnet transmits threats to innocent computers, and the Trickbot botnet’s mechanisms to evade detection and attempts to disrupt its operation. The Trickbot botnet has infected over a million computing devices around the world. Trickbot is a complex and constantly evolving botnet, delivering banking Trojans and ransomware, providing backdoor access to infected machines, and acting as a gateway malware dropper to deploy additional ransomware. For example, once installed, beyond its own financial theft functionality, Trickbot can further deliver the Ryuk ransomware to the

victim's machine. Trickbot can also install other tools for malicious purposes, such as CobaltStrike, which is used to assist with lateral movement and ransomware deployment, and Mimikatz, which is used to extract credentials from the target system.

9. Trickbot is an active, sophisticated, and modular botnet, which enables its operators to easily add or remove capabilities. For example, Trickbot loads many modules that carry out various tertiary tasks that normally involve credential theft, system and network profiling, email and data harvesting, and further propagation of the malware.

10. Once the Trickbot malware infects a new victim computing device, it contacts a command and control computer over the Internet from which it begins to receive instructions and additional malware modules. This effectively places the infected computer under the command of the operators of the botnet.

11. I have obtained copies of the Trickbot code that the Defendants deliver and install on infected end-user computers that are part of the botnet, and have carried out an examination of that code. I have researched the command and control infrastructure of the Trickbot botnet. I have researched the infrastructure used to propagate the Trickbot botnet. I have also reviewed literature published by other well-regarded computer security investigators concerning the Trickbot botnet, and their findings have confirmed my own conclusions regarding the Trickbot botnet malware. Through these and related investigative steps, I have developed detailed information about the size, scope, and illegal activities of the Trickbot botnet.

12. In the course of Microsoft's investigation into the Trickbot botnet, we analyzed approximately 61,000 samples of Trickbot malware. As part of the investigation I, and other Microsoft investigators, purposely infected several investigator-controlled computers with the malware that the Trickbot botnet deploys. This placed the computers under the control of the cybercriminals operating the botnet to enable me and other Microsoft investigators to monitor the telemetry of the Trickbot infrastructure and to monitor all of the illicit communications going to and coming from the infected computers. We then monitored and analyzed the activities of the infected computers and observed initial beacons to the command and control server. We carefully

analyzed the changes that the Trickbot malware makes to Microsoft's operating system and application software during this infection process, and we reverse-engineered the malware to determine how it operates. I participated in and reviewed these investigative techniques.

13. During our investigation, I and other Microsoft investigators observed the infected computers connect to and receive instructions from the Trickbot botnet's command and control servers, and through this method, we were able to identify IP addresses of the command and control servers used to control the Trickbot botnet under investigation. Based on my examination of the IP addresses utilized as Trickbot command and control servers, I was able to determine particular technical features and behaviors associated with such IP addresses, which I was thereafter able to use to confirm that new IP addresses are, in fact, associated with the Trickbot botnet. This verification process has enabled me to accurately identify Trickbot command and control servers that should be disabled, through this action.

14. Based on our investigation and analysis, Microsoft has determined that Trickbot is a substantial and robust delivery mechanism for distributing ransomware and financial targeted malware, carrying out user credential harvesting, and engaging in exploit campaign attacks. I therefore conclude that the primary purpose of the botnet code, the Trickbot botnet and the Defendants' operation is to be a malware-as-a-service for the purpose of stealing account credentials, personal identification information, monetary funds as well as to further propagate the botnet infrastructure itself. I also conclude from these same facts, upon information and belief, that the Defendants must have known and intended that the botnet code, the Trickbot botnet and Defendants' operation of such botnet was to defraud end-user victims of the Trickbot botnet, by means of fraudulent pretenses and representations transmitted over the Internet, as further described below. As further described below, Microsoft has been directly injured in its business and property by these Defendants' acts and their coordinated pattern of acts.

IV. ORGANIZATION OF THE TRICKBOT BOTNET

15. As stated above, a "botnet" is a network of computing devices, connected to the Internet, that are infected with a particular type of malicious software ("malware"). The malware

gives the individuals propagating the botnet—for example, the Defendants in this matter—remote control via the Internet over the operation of the infected computing devices. Botnets can generally take on one of several structures that allow a single criminal or criminal organization to control the vast array of compromised computing devices (sometimes known as “bots”) in the botnet.

16. Like other botnets, the Trickbot botnet is comprised of a large number of victim computers that have been infected by the Defendants with the Trickbot malware. Further, the Trickbot botnet includes computers that have a “command and control” purpose. These command and control computers are utilized by the Defendants to transfer command and control instructions to the infected victim computers, in order to maintain control over the operation of those victim computers and to carry out the numerous types of harmful activities described more fully later in this declaration. Further detail regarding the infected victim computers and the command and control computers is set forth below.

A. Infected Victim Computers

17. The Trickbot botnet is comprised of over a million infected end user computers, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. Trickbot is suspected of using various means of infecting end-user computers. Our investigation determined Trickbot is disseminated via technical exploits of victim computers, malicious spam email or spearphishing campaigns. These campaigns send unsolicited emails that direct users to download malware from malicious websites or trick the user into opening malware through an attachment, such as a Microsoft Word document. The following **Figure 1** shows a deceptive phishing email leveraging Microsoft’s Word trademark and deceiving the user through use of a fraudulent “tax” related theme.

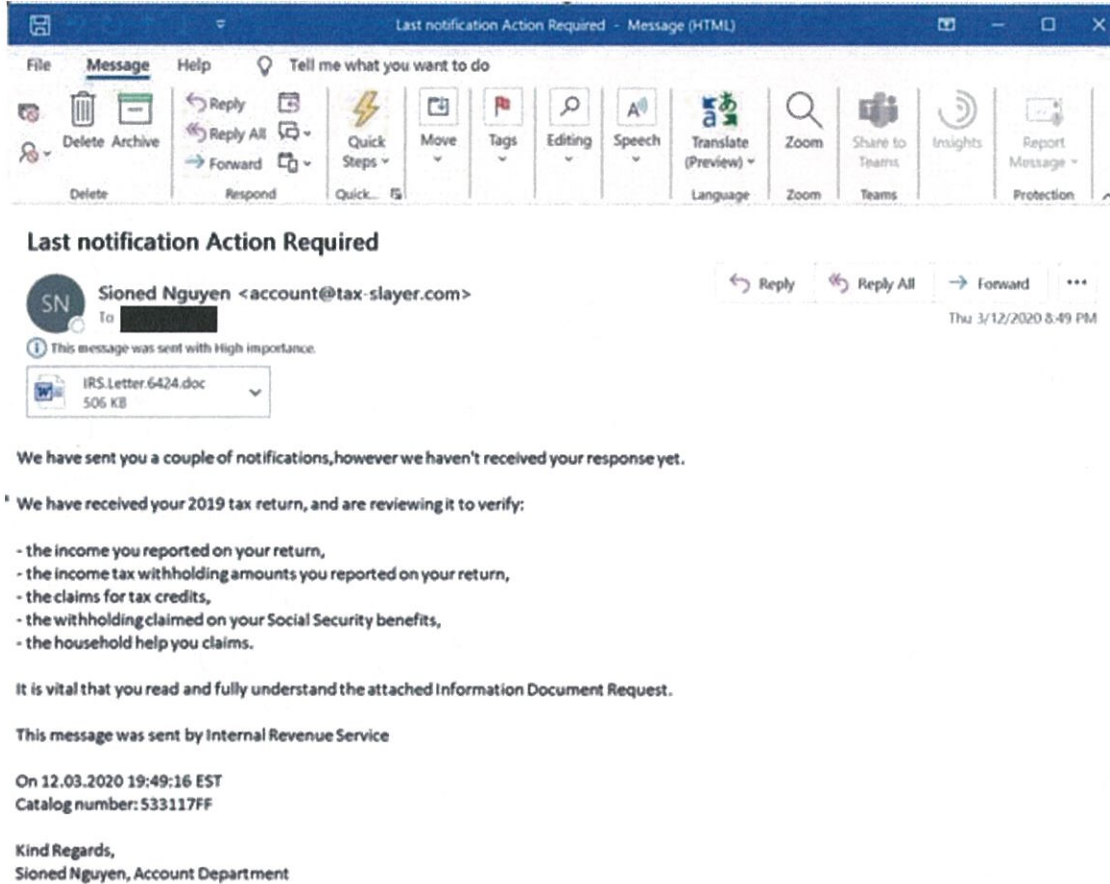


Figure 1

18. The spam email and spearphishing campaigns used to distribute the Trickbot malware have also been using deceptive themes involving public topics of discussion, such as Black Lives Matter and COVID-19, in order to trick users into clicking on documents or links. Figure 2 below is an example of a Black Lives Matter themed email that delivers the Trickbot malware. Figure 3 below is an example of a COVID-19 themed email in the Italian language that delivers the Trickbot malware.

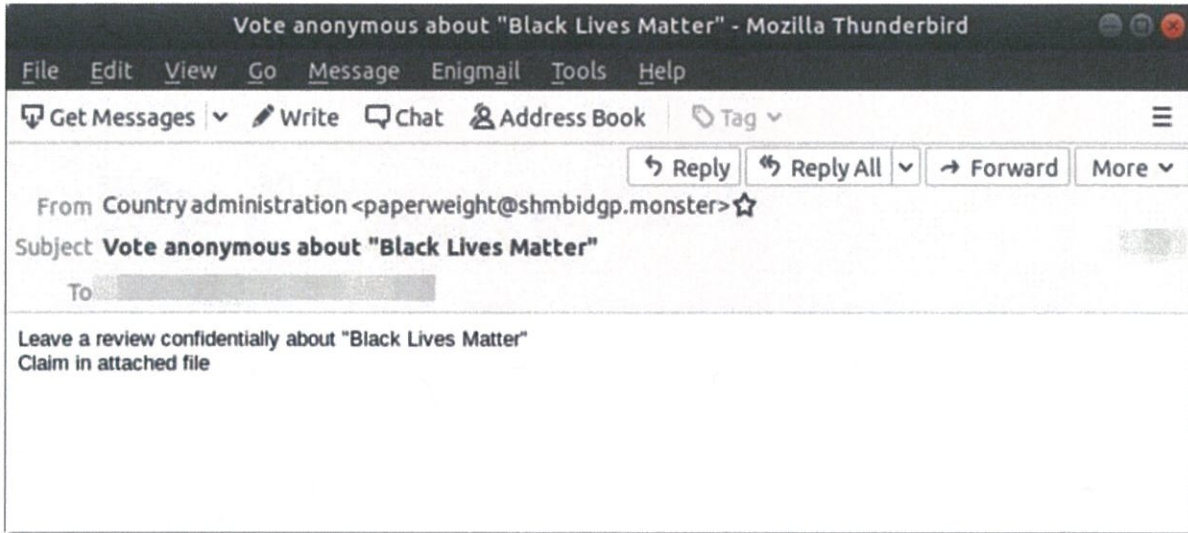


Figure 2

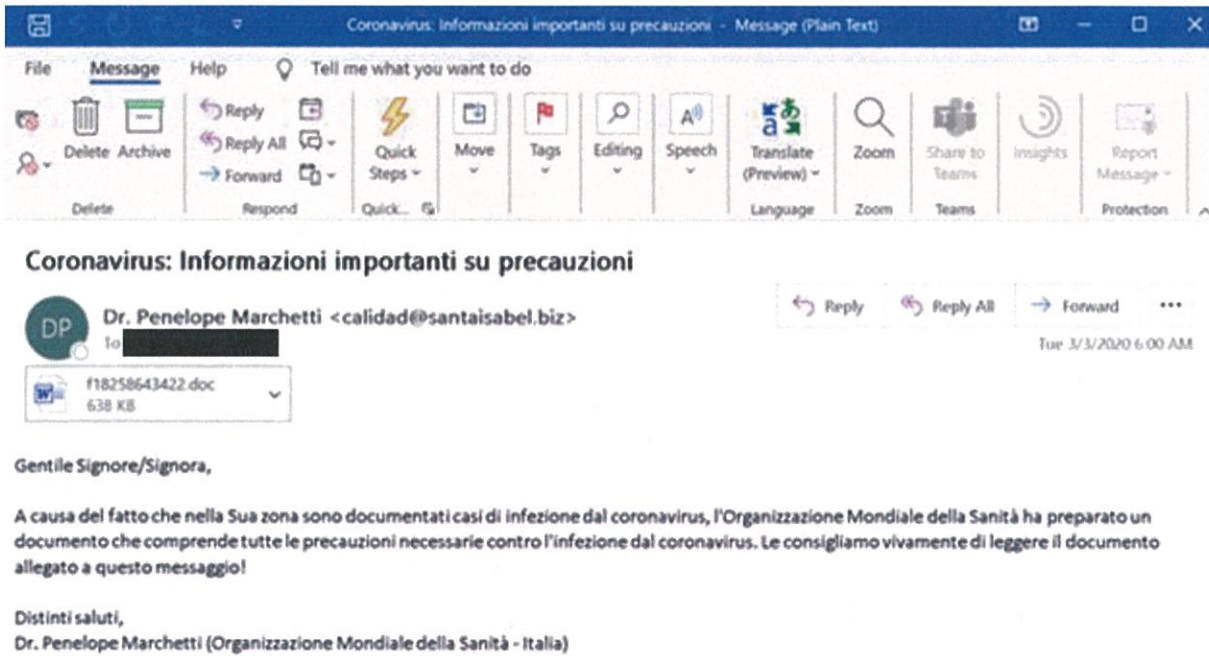


Figure 3

19. In general, the Defendant operators of the Trickbot botnet are constantly engaged in infecting additional end user computers. To counter them, numerous software providers and

software security firms are constantly engaged in trying to remove the Trickbot malware from those computers. Microsoft has conducted an independent investigation to determine the number of computing devices infected by the Trickbot malware. The total number of infected computers in the Trickbot botnet, over time, has been massive. Based on our investigation, we have observed that over a million computers have been infected by the Trickbot malware.

20. The infected victim computers are responsible for performing the daily work of the botnet. Further, owners of the infected victim computers are targets of the Defendants, as Defendants can use these computers to install financial theft malware which enables them to ultimately steal money directly from these individuals' bank accounts, as well as to steal personal information from the owners of the infected computers, encrypt the computers with ransomware and demand a ransom or to engage in other malicious activity directed at these victims.

B. Command and Control Computers

21. The command and control computers are specialized computers and/or software ("servers"). Defendants purchased or leased these servers and use them to send commands to control the Trickbot botnet's infected victim computers. The command and control computers send the most fundamental instructions, modules, updates, and commands, and overall control of the botnets is carried out from these computers. Command and control computers include the servers at various IP addresses (i.e., "Internet Protocol" address) listed in **Exhibit 2** to this declaration (also attached as **Appendix A** to the Complaint), which are described more fully below.

22. Each instance of Trickbot malware infecting a user's computing device is pre-programmed to connect and communicate with several of these command and control servers. When such a connection is made, the servers can download instructions or additional malware to the infected computing device and upload stolen information from it.

23. To create the command and control computers, Defendants set up accounts with web-hosting providers—i.e., companies, usually legitimate, that provide facilities where computers can be connected through high-capacity connections to the Internet and locate their

servers in those facilities. By contacting a command and control server, the Trickbot malware can receive updated commands and modules from and communicate with the Defendants.

1. Overview Of Command And Control Communications Channels

24. After the Trickbot malware infects a victim computing device, it connects over the Internet to one of its pre-programmed command and control servers. In its first communication, it sends the command and control server the victim computer's IP address, the version of Windows running on the computer, a unique computing device identifier and a machine language identifier. At this point, it is ready to begin executing commands sent to it by the Defendant botnet operators.

25. The Defendants are able to send and receive communications between their command and control servers and the infected victim computers in the Trickbot botnet. **Figure 4** below illustrates the communication channels of the Trickbot botnet, between the command and control servers and infected victim computers.

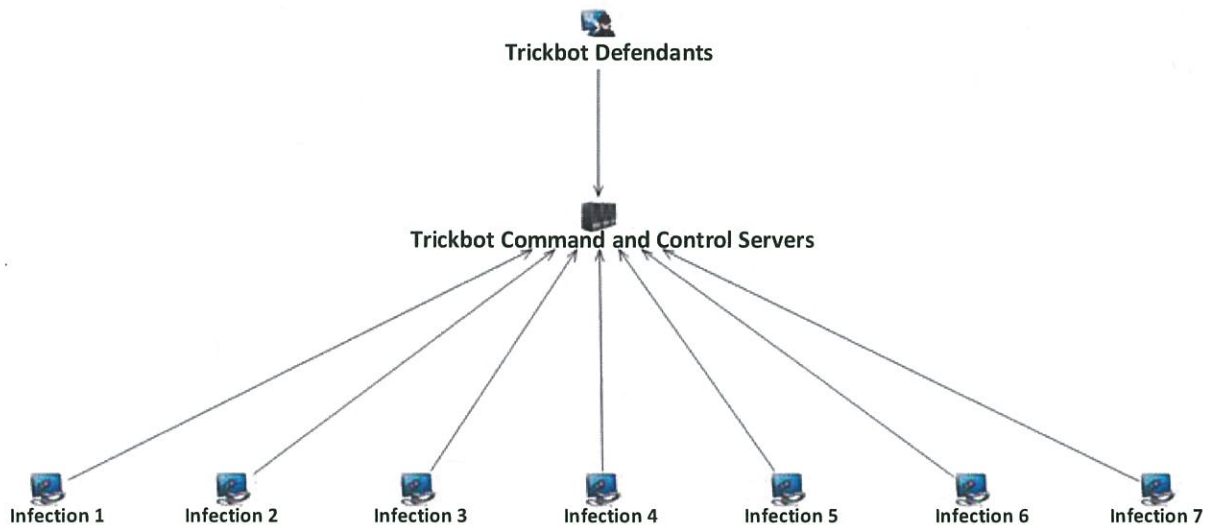


Figure 4

26. The primary command and control communications channel between infected victim computers and Defendants' command and control computers (sometimes abbreviated in this declaration as "C2") is comprised of particular IP addresses associated with servers directly controlled by Defendants. An IP address can be thought of as the physical location on the Internet of a particular computer. An "IP address" is a unique string of numbers separated by a period,

such as “149.154.152.161” that identifies each computer attached to the Internet. Defendants must lease such computers from companies that provide “hosting” services, and which assign to those computers particular IP addresses. The hosting company refers to a type of company that specializes in offering computer hardware, software, connection to the Internet, technical support, and other services to companies and individuals seeking to have some presence on the Internet.

27. Once Trickbot infiltrates a victim’s computer and the malware is installed, the victim computer receives instructions from the botnet command and control servers associated with the primary IP addresses directly controlled by Defendants.

2. The Trickbot Command And Control Communications Tier Is Designed To Evade Technical Counter-Measures

28. The most vulnerable points in the Trickbot botnet architecture are the command and control IP addresses, as they can be identified and, if disconnected from the Internet, the botnet’s communications with infected end-user computers will be severed and propagation of the botnet disabled. As discussed above, I have observed that certain features of the command and control infrastructure enable the botnets to better withstand technical counter-measures. For example, over time, the set of IP addresses with the command and control servers’ changes. Certain IP addresses fall out of use by the infected end-user computers and the Defendants. New IP addresses are added to those that the infected end-user computers used to communicate with. In essence, the set of IP addresses used in the command and control infrastructure is dynamic, making attempts to disable the botnet more challenging.

V. TRICKBOT HAS ATTACKED MANY MICROSOFT CUSTOMERS IN VIRGINIA AND THE EASTERN DISTRICT OF VIRGINIA

29. Through its investigation, Microsoft has determined that Trickbot has affirmatively targeted Microsoft customers in Virginia, including the Eastern District of Virginia.

30. I have recently investigated IP addresses known to be associated with Trickbot. These IP addresses were seen logging into accounts compromised by Trickbot. Technology exists to determine the geographic location of IP addresses. Using such technology, I determined the geographical location of these IP addresses collected during the sample period. I plotted such IP

addresses on maps of Virginia and the Eastern District of Virginia, to represent the location of the relevant activity. Each marker on the maps represents at least one computer to which Defendants have directed the Trickbot malware. As can be seen below, in **Figures 5 and 6**, the Trickbot Defendants have directed their activity toward victims located in Virginia, including in the Eastern District of Virginia and the United States. For example, Defendants have specifically directed the Trickbot malware to computers in Alexandria, Herndon, McLean, Tysons Corner, Falls Church, Arlington and Richmond, Virginia.

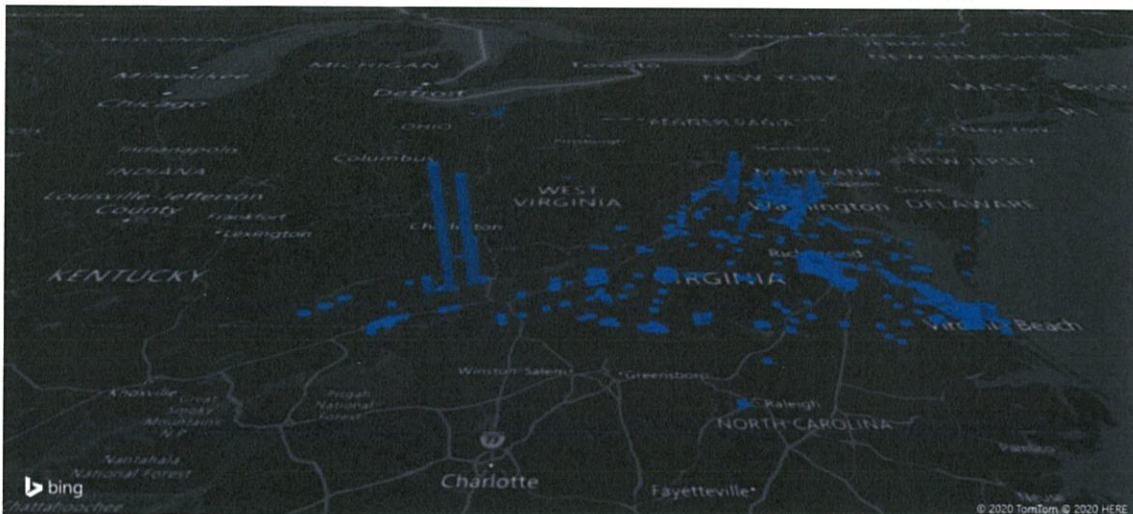


Figure 5

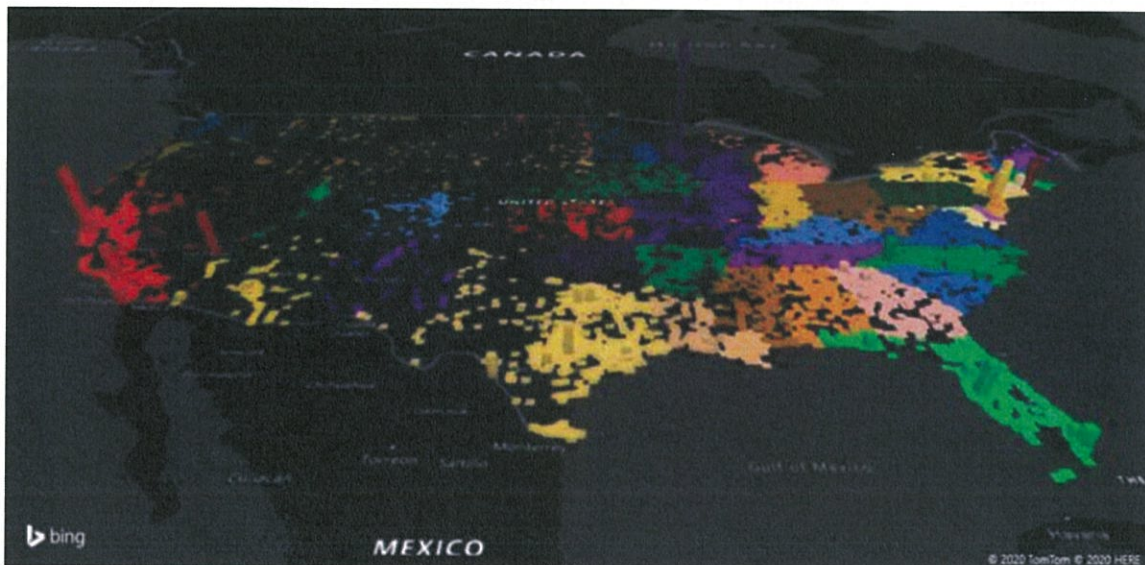


Figure 6

VI. TRICKBOT CAUSES SEVERE HARM

A. Trickbot Causes Severe Harm By Stealing Online Financial Credentials, Stealing Funds And Engaging In Other Malicious Activities Against Victims

31. Trickbot inflicts severe harm on individuals whose computing devices it infects. Once a computing device is infected with Trickbot, Defendants can use the victim's computer to steal the victim's online banking credentials and funds from their online financial accounts, constantly monitor their online activities, send commands and instructions to the infected computing device to control it surreptitiously and deliver malware that, among other things, enables Defendants to take control of the victim's computer and extort money from them. Defendants' primary goal, as made evident by the Trickbot's functionality, is to deliver financial theft malware, deliver ransomware, enable attacks against other computers and to steal online account login IDs, passwords, and other personal identifying information.

32. The particular harm caused by Trickbot can be seen in the form of the "modules" that are downloaded and operate as part of the overall Trickbot malware. Once the core Trickbot malware is installed on victim computers, it reaches back out to the command and control servers to retrieve such modules, as reflected in **Figure 7**.

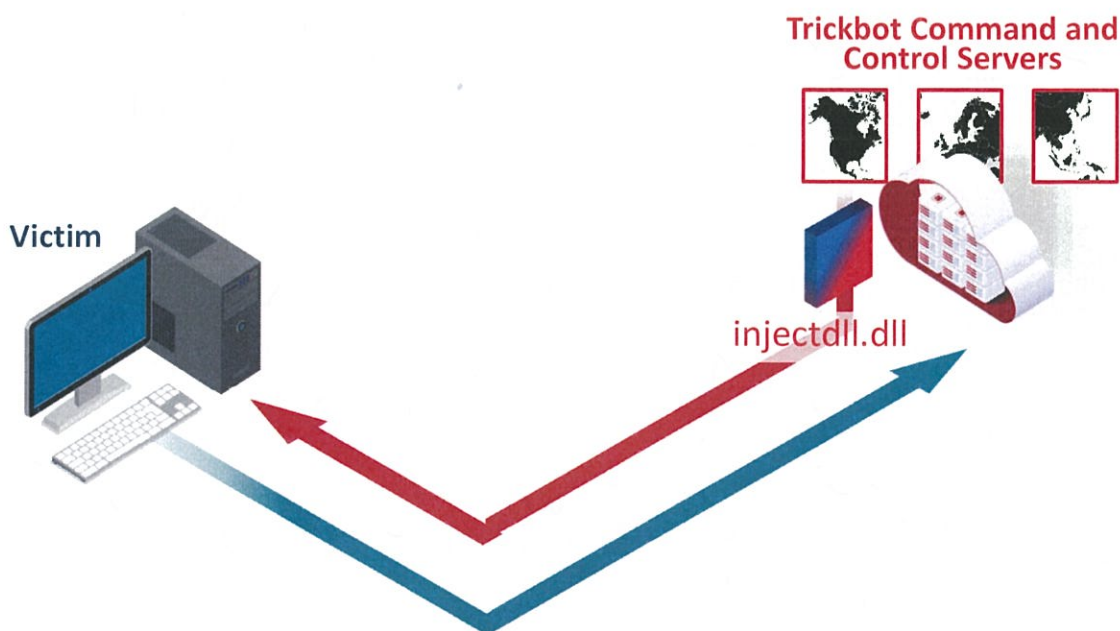


Figure 7

33. Each module has a particular malicious functionality, as set forth in **Figure 8**. Based on my investigation, I believe that Trickbot contains several reconnaissance modules that were updated precisely for the function of going back and evaluating whether a system is worthy of revictimization with ransomware. Once a victim system is identified as a potential target for ransomware, the Trickbot Defendants will deploy an additional payload that carries out additional reconnaissance functionality (using tools such as CobaltStrike and Mimikatz) and finally deploys the Ryuk ransomware on the victim system.

Figure 8	
Module	Purpose
injectDll	Main banker module using “static” and “dynamic” web browser injection and data theft
networkDll	A reconnaissance module that gathers network and system information for the purpose, among many, to determine if the victim machine meets criteria for revictimization with ransomware
Systeminfo	Gather system information
tabDll	Propagate Trickbot via EternalRomance Exploit
wormDll	Propagate Trickbot via SMB - EternalBlue Exploit
shareDll	Propagate Trickbot via Windows Network Shares
vncDll / BCTestDll	Remote control/Virtual Network Computing module to provide backdoor for further module downloads
rdpscanDll	Launch brute-force attacks against selected Windows systems running a Remote Desktop Protocol (RDP) connection exposed to the Internet
Mailsearcher	Searches all files on disk and compares their extensions to a predefined list to harvest email addresses
outlookDll	Gather Outlook credentials
importDll	Gather browser data
PsfIn	Gather point of sale software credentials
squidDll	Gather email addresses stored in SQL servers
aDll	Execute various commands on a Windows domain controller to steal Windows Active Directory Credentials
Pwgrab	Gather credentials, autofill data, history and so on from browsers

34. The primary Trickbot module is called “injectDll.” This module is designed to steal victims’ online banking credentials. Once the Defendants have stolen the credentials, they can log into the victims’ accounts and steal funds. The injectDll module operates using a technique called a “webinject,” sometimes also referred to as a “man-in-the-browser” attack. The injectDll module monitors the victim’s activity and detects when the victim is navigating via their browser to the online portals of a wide variety of financial institutions, including banks, brokerage firms and credit card companies. When the module detects that the user is visiting such a website, it utilizes the webinject method to either send the user to a fake website that mimics the financial institution or to alter or replace content or display additional fields in the website as it appears to the victim in their browser. In this way, the victim believes that they are at the legitimate online financial website, when in fact they are seeing either an entirely fake version of the website to which the Trickbot module has diverted them, or a version of the website that has been manipulated by Defendants. Regardless of which method is used the effect is the same. When the user types their login credentials into the website or types additional information into fraudulent fields injected by the Defendants (such as pin codes, answers to security questions or other personal information), the Defendants are able to intercept that information and use it to log into the user’s online accounts. The Defendants can then initiate funds transfers, resulting in theft of the victim’s money. This process is reflected in **Figure 9**, and is but one example of a webinject targeting a particular financial institution among hundreds globally.

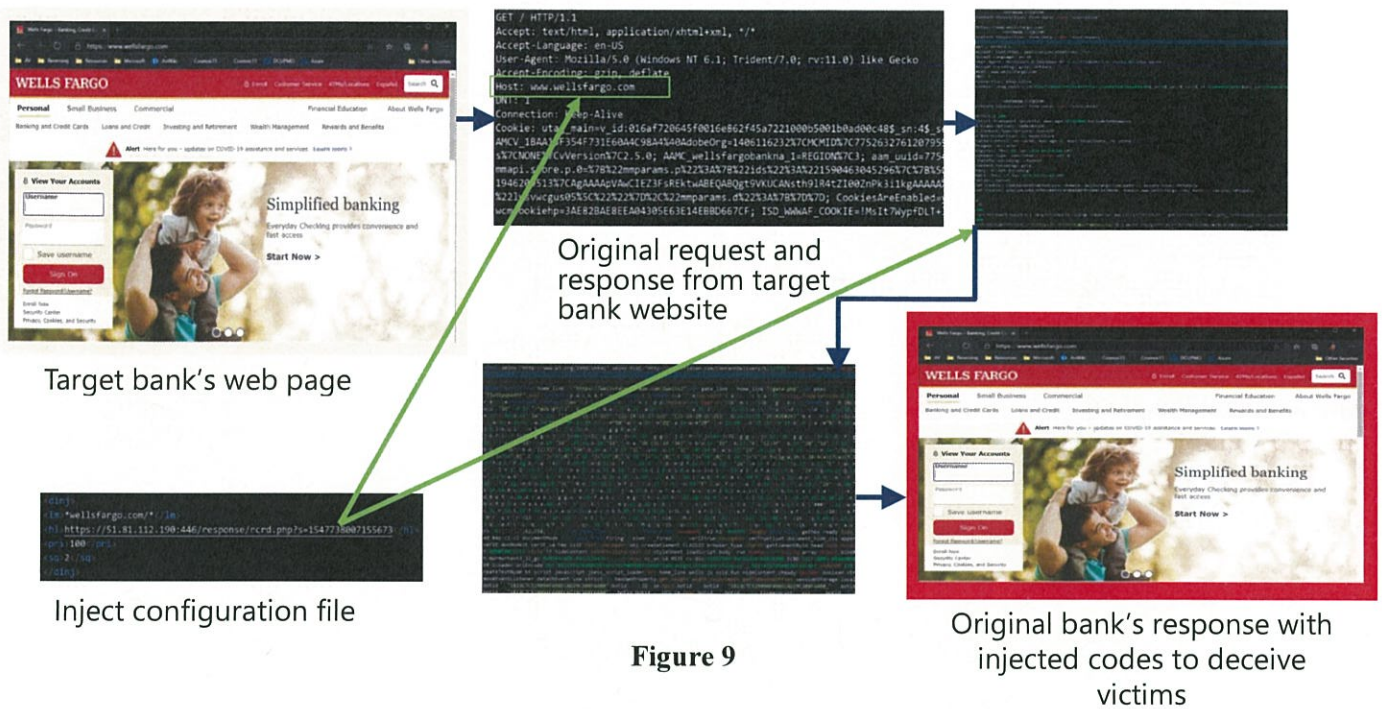


Figure 9

35. The scope and scale of Defendants' targeting of financial institutions is broad and global in nature. Financial institutions including global transaction banks, regional banks, payment processors headquartered in North America, the European Union, and Asia-Pacific have been targeted by the Defendants. Thus, the threat posed by Trickbot is shared by the entire financial industry and Microsoft as both must take substantial steps and make significant investments in defending against these types of activities.

36. As reflected in the chart above, other Trickbot modules are directed at reconnaissance and collection of technical information about the victim machine and network, propagation of the Trickbot malware across the victim's network, remote control of the victim's computer and network, searching for and collecting personal information (online credentials, point of sale software credentials, Windows credentials, email addresses, browser data etc.) and attacking other computers through the victim computers. This malware and its operation have been observed in the wider cybersecurity community as well. For example, attached to this declaration as **Exhibit 3** is a true and correct copy of a research paper by security research firm Deep Instinct

regarding the operation of Trickbot's "Trickbooster" module that has harvested at least 250 million email addresses in order to distribute malicious spam emails from the victim's compromised account to further perpetuate the fraud. This research paper is of the type that I and other cybersecurity researchers rely on in the technical investigation of malware and is consistent with my own direct observations regarding operation of Trickbot during the course of my research.

37. In addition, Trickbot is known to deliver other forms of malicious code, including ransomware. Ransomware is a type of malware that prevents victim user from accessing their systems or personal files and demands ransom payment in order to regain access. The introduction of ransomware into a system can have devastating effects, including most recently an instance of ransomware that crippled the IT network of a German hospital resulting in the death of a woman seeking emergency treatment. Attached to this declaration as **Exhibit 4** is a true and correct copy of an article discussing a ransomware-related death in Germany. Ransomware has also been cited by the Director of the Cybersecurity and Infrastructure Security Agency at DHS as having the potential to sow chaos during the 2020 election. Attached to this declaration as **Exhibits 5 and 6** are a true and correct copy of articles discussing this ransomware threat.

38. There are several variants of ransomware. Crypto-ransomware, for example, is a form of ransomware that encrypts a victim user's files, folders, and hard-drives and demands a ransom in Bitcoin or other cryptocurrency to retrieve the data. Trickbot delivers the Ryuk crypto-ransomware to victim devices. Ryuk is a sophisticated crypto-ransomware because it identifies and encrypts network files and disables Windows System Restore in order to prevent the user from being able to recover from the attack without external backups. Ryuk has been attacking organizations, including municipal governments, state courts, hospitals, nursing homes, enterprises, and large universities. Attached to this declaration as **Exhibit 7** is a true and correct copy of an article discussing Trickbot-delivered Ryuk ransomware attacking Virginia-based Electronic Warfare Associates, a contractor for the Department of Defense. Attached to this declaration as **Exhibit 8** is a true and correct copy of an article discussing Trickbot-delivered Ryuk ransomware attacking the North Carolina city of Durham. Attached to this declaration as **Exhibit**

9 is a true and correct copy of an article discussing Trickbot-delivered Ryuk ransomware crippling Virtual Care Provider Inc., an IT provider to 110 nursing homes and acute-care facilities in 45 states. Attached to this declaration as **Exhibit 10** is a true and correct copy of an article discussing Trickbot-delivered Ryuk ransomware targeting hospitals during the COVID-19 pandemic.

B. Trickbot Causes Severe Harm By Making Unauthorized Changes To The Victim Computers And The Windows Operating System

39. Trickbot inflicts substantial damage on Microsoft whose products and trademarks Defendants systematically abuse as part of the botnet's fraudulent operations. Trickbot severely damages the computing devices it infects, making low-level changes to the operating system including Windows 7, including Windows 8, Windows 8.1, Windows 10 and several versions of Windows Servers. For example, once the Defendants infect a computer with the Trickbot malware, it compromises the underlying code of Microsoft's Windows operating system to alter the behavior of various Windows routines by manipulating various registry key settings and scheduled tasks.

40. During the infection process, the Trickbot malware will copy itself to the user's computer. Depending on the variant, the file can be installed in any one of a number of possible locations. For example, in the context of Microsoft Windows 8, the Trickbot malware changes a number of settings in the user's Windows registry. In particular, the Trickbot malware changes the following registry entry to ensure that its copy runs at each Windows start by inserting the following action: *%windir%\system32\Tasks\services update*. The registry entry corresponds to changes to the file path *C:\Windows\System32\Tasks* where tasks are scheduled to achieve this result. This is a database of configuration settings and options built into Windows operating systems—to ensure that the malware is launched automatically every time the computing device is started. Additional examples of manipulated registry keys and file paths can be found in the Declaration of Rodelio Fiñones. As can be seen in the examples in that declaration and above, the Defendants fraudulently compromise a specific component of the Microsoft Windows 8 operating system that both uses the “Microsoft” and “Windows” trademarks, in order to conceal the activities of the botnet, trade on Microsoft's trademarks and deceive end-user victims of the operating

system.

41. The compromised Windows operating system does not appear any different to the user of the infected computer. The user, thus, thinks the compromised operating system is developed and distributed by Microsoft, despite the fact that it is the operators of the botnet that are compromising the operating system. This harms Microsoft's reputation and goodwill among the public.

C. **Trickbot Causes Severe Harm By Distributing And Installing Other Types Of Dangerous Malware**

42. Trickbot is used in a variety of illegal activities, but it is well-known known as a downloader/dropper for delivering major malware families in what is known as a "malware-as-a-service" criminal business model that delivers ransomware that locks a victim's computer and demands payment to unlock it, banking Trojans that steal funds from victim accounts, and a wide range of other types of malware. The malware distributed by Trickbot that I have identified include Ryuk, which is a type of crypto-ransomware. Trickbot can also distribute malicious code such as CobaltStrike and Mimikatz, which enable ransomware deployment, movement within victim systems and extraction of victim credentials. In other words, one of the Trickbot botnet's major activities is downloading and spreading secondary malware and other malicious code onto Trickbot-infected computers. Trickbot infects a victim's system by being downloaded by other malware, such as the malware called "Emotet," or being delivered through spammed email attachments or malicious advertisements. Also, as indicated above, once installed, Trickbot can propagate itself throughout a network using the EternalRomance and EternalBlue exploits, or by means of Windows Network Shares.

43. In order to avoid detection, Trickbot has evolved to include capabilities that would disable Windows services, including any security and antivirus software, including antivirus software provided by Microsoft and other companies such as Sophos, Malwarebytes and others. For example, Trickbot is designed to target Windows Defender by attacking the Registry settings and performing the following steps:

- a. Disable and then delete the WinDefend service.
- b. Terminates the MsMpEng.exe, MSASCuiL.exe, and MSASCui.exe processes.
- c. Adds the DisableAntiSpyware Windows policy and sets it to true to disable Windows Defender and possibly other software.
- d. Disables Windows Security notifications.
- e. Disables Windows Defender real-time protection.

44. When TrickBot detects certain security programs installed, it will configure a debugger for that process using the Image File Execution Options Registry key. This causes the debugger to launch before the program that is executed, and if that debugger does not exist, the expected program will fail to launch.

45. The Trickbot malware can be commanded to download and install additional malware on the infected computing device, causing users whose computing devices are infected with Trickbot to be victimized by other types of malware as well. Each of these secondary malware infections makes further changes to the user's computing device, including by adding files, changing registry settings, opening additional backdoors that allow control by other cybercriminals, and allowing yet further sets of malware to be downloaded onto the computing device. All of these malware variants are designed to attack computing devices running Microsoft Windows operating systems and may themselves be connected to other criminal botnet infrastructure beyond Trickbot receiving additional commands.

46. My investigation has also uncovered evidence that the Trickbot botnet engages in downloading the same type of secondary malware over the same period of time. This evidence confirms that the Trickbot botnet is being used in coordinated malware campaigns for the purpose of infecting computers of innocent victims.

47. Under these circumstances, the Defendants have a vested interest in increasing the number of computers belonging to their Trickbot botnet, as that relates directly to the number of computers they can attempt to infect with secondary malware.

D. Trickbot Causes Severe Harm Both To Microsoft's Reputation, Brands And Goodwill With Its Customers

48. The Trickbot malware infection itself harms Microsoft and Microsoft's customers by damaging the customers' computing devices and the software installed on their computing

devices, including Microsoft's proprietary Windows operating systems. The Trickbot malware is designed to infect and run on computer devices equipped with the Windows operating system. The Windows operating system is licensed by Microsoft to its users.

49. A Trickbot malware infection begins with the download to the user's computing device of the executable files that Trickbot uses to install itself on the computer device. The installation of malicious software in and of itself damages the user's computing device and the Windows operating system on the user's computing device. During the infection of a user's computing device, Trickbot makes changes to the deepest and most sensitive levels of the computing device's operating system, including the kernel, registry, and system files. One purpose of the change is to disable Windows security features.

50. Microsoft's customers whose computing devices are infected with Trickbot are damaged by these changes to Windows, which alter the normal and approved settings and functions of the user's operating system, place hooks into the operating system so Trickbot can hide its presence and activities, destabilize it, and forcibly conscript the computing device into the botnet.

51. Customers are usually unaware of the fact that their computing devices are infected and have become part of the Trickbot botnet. Even if aware of the infection, they often lack technical resources or skills to resolve the problem, allowing their computing devices to be misused indefinitely, as manual steps to remove the malicious software may be difficult for ordinary users.

52. Microsoft devotes significant computing and human resources to combating Trickbot and other malware infections and helping customers determine whether or not their computing devices are infected and, if so, cleaning them. Not only does Microsoft expend resources in helping users combat Trickbot, these efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Microsoft's customers. Microsoft, as a provider of the Windows operating systems, must also incorporate security features in an attempt to stop installation of the Trickbot malware and other malicious software that is distributed

by the Trickbot botnet. Microsoft has expended significant resources to investigate and track the Trickbot Defendants' illegal activities and to counter and remediate the damage caused by the Trickbot botnet to Microsoft, its customers, and the general public.

53. Trickbot irreparably harms Microsoft by damaging its reputation, brands, and customer goodwill. Defendants physically alter and corrupt Microsoft products such as the Microsoft Windows products mentioned above. Trademark registrations for the marks infringed by Defendants are attached to the Complaint as **Appendix B**. In addition, as discussed in the Declaration of Rodelio Fiñones, Trickbot reproduces Microsoft's copyrighted declaring code for Windows 8.1 Software Development Kit, which is required for Trickbot's functionality. Copyright registration for Microsoft's declaring code is attached to the Complaint as **Appendix C**.

54. In effect, once infected, altered, and controlled by Trickbot, the Windows operating system ceases to operate normally and becomes tools for Defendants to conduct their theft. However, they still bear the Microsoft and Windows trademarks. This is obviously meant to and does mislead Microsoft's customers, and it causes extreme damage to Microsoft's brands and trademarks.

55. Microsoft has invested substantial resources in developing high-quality products and services. Due to the high quality and effectiveness of Microsoft's products and services and the expenditures of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, has established strong brands, has developed the Microsoft name and the names of its products and services into strong and famous world-wide symbols that are well-recognized within its channels of trade. Microsoft has registered trademarks representing the quality of its products and services and its brand, including Microsoft, Windows, Word and Outlook.

56. The activities of the Trickbot botnet injure Microsoft and its reputation, brand, and goodwill because users subject to the negative effects of these malicious applications incorrectly believe that Microsoft and Windows are the sources of their computing device problems. As explained above, because of the Trickbot botnet, users of infected computing devices will

experience degraded device performance. There is a great risk that users may attribute this problem to Microsoft and associate these problems with Microsoft's Windows products, thereby diluting and tarnishing the value of the Microsoft and Windows trademarks and brands.

57. To carry out the intrusion into computing devices, Defendants cause the Trickbot malware to make repeated copies of Microsoft's trademarks onto computing devices, in the form of file names, domain names, target names, and/or registry paths containing the trademarks "Microsoft" and "Windows." For example, the OutlookDLL credential stealing module is delivered through a credential stealing module called "Outlook.dll," which infringes Microsoft's Outlook trademark. Further examples of infringement of the "Microsoft," "Windows" and "Outlook" trademarks in registry and file paths are set forth in the Declaration of Rodelio Fifiñones. These uses of Microsoft's trademarks are designed to cause the intrusion into the user's computing device and to confuse the user into believing that the software installed is a legitimate part of the Windows operating system, when it is not.

58. Based on my experience assessing cyber threats and the impact on business, I conclude that customers may, and often do, incorrectly attribute to Microsoft the negative impact of the Trickbot botnet and other malware downloaded to their computing devices as a result of having their computers hijacked and infected with a variety of malware, described earlier in this declaration. Further, based on my experience, I conclude that there is a serious risk that customers may move from Microsoft's products and services because of such activities. Further, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and perceived risks.

VII. DISRUPTING TRICKBOT

59. Given the specific architecture of Trickbot, I believe that if provided advance notice that the command and control IP addresses were to be disabled, the Trickbot operators would take measures to keep Trickbot alive by migrating to new IP addresses. As discussed, Trickbot is designed to evade detection by changing the IP addresses of its command and control servers over time. Therefore, a piecemeal approach to disconnecting the IP addresses will fail. If less than all

of the command and control servers are directed to be taken offline immediately and simultaneously, the Trickbot infected end-user computers will be able to migrate to the remaining servers or to new command and control servers.

60. Based on my experience involving Internet security matters, I believe that the only way to suspend the injury caused by Trickbot is to:

- a. direct the relevant hosting companies to disable the IP addresses;
- b. make the content stored on the command and control servers inaccessible and to disable any and all “backup” systems, arrangements, and services;
- c. direct the hosting companies to suspend all services to the bot-operators, to not warn or aid the operators, and to not enable the circumvention of the order; and
- d. block any effort by the Trickbot operators to purchase or lease additional servers.

61. It is important that the requested actions be closely coordinated, such that the malicious IP addresses, in various locations, are directed by the Court to be turned off immediately upon receipt of any order issued by the Court and in coordination with other efforts, such that these IP addresses are turned off simultaneously. Any delay in disabling the IP addresses would warn the operators of this action and immediately relocate the command and control servers to unidentified servers/locations. In particular, because the Trickbot command and control infrastructure is globally distributed, this relief sought from the Court is being coordinated with legal efforts in many other jurisdictions. Microsoft’s field team across the world are taking analogous steps under the legal authority and legal systems of a number of other countries, to simultaneously disable command and control IP addresses in those jurisdictions. The proposed temporary restraining order is framed in a manner that enables coordinated efforts that will maximize the effectiveness of the effort.

62. In the aggregate, the foregoing steps, which will be carried out upon entry of the requested temporary restraining order, will prevent the Defendants from accessing their command and control infrastructure, will cut off Defendants’ ability to communicate with the infected victim computers, and will effectively disable the operation of the Trickbot botnet. This is the only means by which the Trickbot botnet can be disabled and the serious harm to Microsoft and to millions of computer users can be mitigated and prevented. Once the command and control infrastructure is

disabled, and Microsoft has control of that infrastructure, this will enable Microsoft to assist users impacted by the Trickbot malware in cleaning the malware off of their systems. Further, beyond infecting end user computers, the Trickbot Defendants have also infected a number of “Internet of Things” (IoT) devices, such as routers. The mitigation phase will also involve robust steps to remove the malware from these devices as well.

63. I have recently investigated the command and control IP addresses in the context of the botnet. Based on observing the IP addresses, I conclude that their purpose is to support and propagate the Trickbot botnet, as described above and that they further malicious activity through the botnet. If there is content not associated with Trickbot that is incidentally contained on the servers at these IP addresses, based on my experience as a technologist generally, my work involving Internet security matters specifically and my prior experience carrying out court-authorized cybercrime disruption efforts, I believe that such content can be moved to new IP addresses with only negligible impact on the users.

64. I believe that the only way to suspend the injury caused to Microsoft, its consumers and the public, is to take the steps described in the [Proposed] Ex Parte Temporary Restraining Order and Order to Show Cause Re Preliminary Injunction (“Proposed TRO”). This relief will significantly hinder the Trickbot botnet’s monetization and capability and operational control, and stop the harmful activities of the Defendants.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge. Executed this 5th day of October, 2020, in Alexandria, Virginia.



Jason B. Lyons

EXHIBIT 1

Jason B. Lyons

SUMMARY

Jason Lyons is an experienced investigator specializing in computer investigations. Trained and experienced in hacker methodology/techniques, computer forensics, incident response, electronic discovery, litigation support and network intrusion investigations.

SECURITY CLEARANCE

- Top Secret/SCI-Expired.

CERTIFICATIONS

- Encase Certified Examiner (EnCE) - Guidance Software
- Counterintelligence Special Agent - Department of the Army
- Certified Basic Digital Media Collector - Department of Defense
- Certified Basic Computer Crime Investigator – Department of Defense
- Certified Basic Digital Forensic Examiner – Department of Defense
- State of Texas licensed Private Investigator

TECHNICAL SKILLS

- Network Intrusion Investigations
- Incident Response
- Investigative Network Monitoring
- Investigation Management/Liaison
- Computer Media Evidence Collection
- Computer Forensics
- EnCase Certified Examiner
- PDA and Cell Phone Seizure and Forensics
- Expert Witness Experience
- Technical/Investigative Report Writing

PROFESSIONAL EXPERIENCE'

October 2013 – Present **Microsoft Corporation**
 Digital Crimes Unit
 Microsoft Cyber Crime Center

- Work with public (law enforcement, country certs) and private sectors, and develop international partnerships to support malware disruptions on a global scale
- Conduct proactive malware investigations to identify critical command control infrastructure and to develop disruption strategy to eliminate or severely cripple cyber-criminal infrastructure.
- Document and identify monetization schemes utilized by cyber-criminals ranging from online advertising fraud, ransomware, and targeted financial fraud.
- Work with the Microsoft legal team to develop new legal strategies to disrupt cyber crime through both civil and criminal proceedings.
- Collect electronic evidence to support global malware disruptions and develop criminal referrals for law enforcement.

- Enhance Microsoft's Cyber Threat Intelligence Program (CTIP) which empowers ISP and country CERTS too identify victims of cybercrime.
- Provide expert court testimony with the support of written declarations describing the threat and impact of malware threats on the Microsoft ecosystems.
- Lead and participate in security community working groups that support cybercrime disruption.
- Work with Microsoft Malware Protection Center (MMPC), and other Anti-Virus vendors, to enhance detection of malware and to assist in the development of disruption strategies.

Jun 2012 – Sep 2013

Xerox

**Director of Digital Forensics, eDiscovery, and Incident Response
Dallas, TX**

- Responsible for investigating, reporting, and responding to information security incidents worldwide.
- Manages an incident team who utilizes various forensic techniques to investigate information security incidents to include computer forensics, log analysis, network forensics, Intrusion Detection System (IDS) alerts, and malware analysis.
- Developed threat and risk matrices based on incidents types and report findings to upper management.
- Developed processes and procedures based on incident alerting sources, including escalated IDS alerts, MacAfee EPO, Email Spam filters, and Data Loss Prevention (DLP) alerts.
- Works with multiple vendors to develop proactive Proofs of Concepts (POC) to increase the company's security posture.
- Responsible for managing, coordinating, investigating, and reporting on legal, corporate security, human resources, and ethics investigations involving digital media.

Jan 2012 – Jun 2012

**Manager, Cyber Intelligence Response Team-
Xerox Informations Security Office
Dallas, TX**

- Manager of the Cyber Intelligence Response Team (CIRT) for a fortune 500 company. Responsible for investigating, reporting, and responding to information security incidents worldwide.
- Manages an incident team who utilizes various forensic techniques to investigate information security incidents to include computer forensics, log analysis, network forensics, Intrusion Detection System (IDS) alerts, and malware analysis.
- Developed threat and risk matrices based on incidents types and report findings to upper management.
- Developed processes and procedures based on incident alerting sources, including escalated IDS alerts, MacAfee EPO, Email Spam filters, and Data Loss Prevention (DLP) alerts.
- Works with multiple vendors to develop proactive Proofs of Concepts (POC) to increase the company's security posture.

Aug 2005 – 2012

***Affiliated Computer Services, inc (ACS)
Digital Forensic and eDiscovery Group
Manager of the Digital Forensics Group (DFG)***

- Manager of a fortune 500 company's digital forensic laboratory/group. Responsible for managing, coordinating, investigating, and reporting on legal, corporate security, human resources, and ethics investigations involving digital media.
- Developed policy and procedures for digital evidence acquisition, storage, examination, processing and production.
- Developed and maintained technical investigative support for ACS inside and outside legal counsel on eDiscovery matters. Experienced in developing and executing large eDiscovery collection plans, preserving data in a forensically sound manner, culling of relevant data, presenting data for review, hosting data for review, and producing relevant data for final production.
- Implemented Access Data's Enterprise and eDiscovery solution.

2003 – 2005 ***Department of the Army, 902nd Military Intelligence (MI),
Cyber Counterintelligence Activity (CCA)
Assistant Operations Officer/Counterintelligence Special Agent***

- Assisted in managing of all CCA branch operations to include all cyber investigations, special intelligence collection missions, cyber investigator training, and quality assurance of all investigative products.
- Supervised 35 special agents and computer forensic technicians.
- Prepared detailed investigative briefings which include results of investigations and forensic analysis for executive level officers.
- Conducted national level liaisons with federal intelligence and law enforcement agencies on many national security investigations.
- Conducted network intrusion investigations, computer media forensics examinations, counterintelligence/counterterrorism special operations, and network forensic analysis.

2000 – 2003 ***Department of the Army, 902nd MI, CCA
Counterintelligence Special Agent / Computer Investigator***

- Assistant Supervisory Special Agent (ASSA) of an eight man computer Incident Response Team (IRT) specializing in cyber investigations.
- Accountable for managing, editing and reviewing associated technical and investigative reports pertaining to the IRT's investigations.
- Provided and maintained incident response, computer forensics, evidence handling, and computer media search and seizure training for the members of the IRT.
- While assigned to the IRT, served as lead agent on numerous network intrusion and computer forensic Counterintelligence investigations.

1998-1999 ***Department of the Army, 501st MI Brigade, South Korea
Counterintelligence Special Agent / Liaison Officer***

- Served as liaison officer for a Counterintelligence Resident Office in South Korea.

- Maintained regional-level liaison with foreign government officials to collect strategic information for intelligence reporting.
- Established business partnerships and furthered cooperation between the United States and South Korean investigative/intelligence agencies to accomplish bilateral goals.

EDUCATION

- Graduate from Excelsior College in October 2002, with a Bachelor of Science in Liberal Arts.
- Thirteen hours completed for Masters Degree in Information Technology with University of Maryland University College (UMUC).

TRAINING

- Counterintelligence Agent Course-Department of the Army-1998.
- Counterintelligence Fundamentals Warfare (CIFIW)-Department of the Army-2000.
- Introduction to Computer Search and Seizure-Defense Computer Investigation Training Program (DCITP), Linthicum, MD-2000.
- Introduction to Networks and Computer Hardware (INCH)-DCITP, Linthicum, MD-2000.
- Network Intrusion Analysis Course (NIAC)-DCITP, Linthicum, MD-2001.
- Computer Investigations for Special Agents (CICSA)-Department of the Army-2001.
- Basic Evidence Recovery Techniques (BERT)-DCITP, Linthicum, MD- 2002.
- Basic Forensic Examiner Course (BFE)-DCITP-Linthicum, MD-2002.
- Forensics in a Solaris Environment (FISE)-DCITP-Linthicum, MD-2002.
- SANS-Tracking Hackers/Honey pots-SANS Institute, Dupont Circle, DC-2003.
- Encase Intermediate Analysis and Reporting-Guidance Software, Sterling VA-2004.
- PDA and Cell Phone Seizure and Analysis-Paraben Software, Orlando FL-2005
- Network Monitoring Course (NMC)-DCITP- Linthicum, MD-2005
- Encase Advanced Internet Examinations-Guidance Software, Los Angeles CA-2006
- (FTK) Windows Forensics-AccessData, Dallas TX-2006
- (DNA) Applied Decryption-AccessData, Nashville TN, 2007
- Network Intrusion Course-Guidance Software, Houston, TX, 2010
- SANS-Hacker Techniques, Exploits, and Incident Handling, San Francisco, CA, 2011
- Reverse-Engineering Malware: Malware Analysis Tools and Techniques Washington DC, 2014
- Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response -Virginia Beach VA 2015
- Advanced Memory Forensics & Threat Detection Las Vegas NV 2017

EXHIBIT 2

APPENDIX A

LIST OF IP ADDRESSES AND HOSTING COMPANIES ASSOCIATED
WITH TRICKBOT'S COMMAND AND CONTROL SERVERS

IP Addresses of Command and Control Servers	Hosting Companies/Data Centers Where Defendants Have Placed the Command and Control Servers
104.161.32.103 104.161.32.105 104.161.32.106 104.161.32.109 104.161.32.118	Input Output Flood, LLC d/b/a Ioflood 9030 W. Sahara Ave., Suite 703 Las Vegas, NV 89117 Input Output Flood, LLC d/b/a Ioflood c/o Phoenix NAP, LLC d/b/a phoenixNAP 3402 E University Dr. #6 Phoenix, AZ 85034
104.193.252.221	Hosting Solution Ltd. c/o Hurricane Electric LLC 48233 Warm Springs Blvd Fremont, CA 94539 Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539
107.155.137.19 107.155.137.28 107.155.137.7 162.216.0.163 23.239.84.132 23.239.84.136	Nodes Direct Holdings, LLC 1650 Margaret St Suite 302-351 Jacksonville, FL 32204 Nodes Direct Holdings, LLC 4495 Roosevelt Blvd, Suite 304-241 Jacksonville, FL 32210 Nodes Direct Holdings LLC c/o Cologix, Inc. 421 W. Church St., Suite 429 Jacksonville, FL 32202
107.174.192.162 107.175.184.201	Virtual Machine Solutions LLC 1600 Sawtelle Blvd., Suite 308 Los Angeles, CA 90025

	<p>Virtual Machine Solutions LLC 2801 Robin Rd. Midwest City, OK 73110</p> <p>Virtual Machine Solutions LLC c/o Velocity Servers, Inc. d/b/a ColoCrossing 325 Delaware Ave., Suite 300 Buffalo, NY 14202</p> <p>Velocity Servers, Inc. d/b/a ColoCrossing 8185 Sheridan Dr Buffalo, NY 14221-6002</p>
139.60.163.45	<p>Hostkey USA, Inc. c/o Smyle & Associates 122 East 42nd St., Suite 3900 New York NY 10168</p> <p>Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 501 Franklin Avenue, Suite 200 Garden City, NY 11530</p> <p>Hostkey USA, Inc. c/o Webair Internet Development Company Inc. 1025 Old Country Road Westbury, NY 11590</p> <p>Hostkey USA, Inc. c/o Hurricane Electric LLC 501 Franklin Avenue, Suite 200 Garden City, NY 11530</p> <p>Hurricane Electric LLC 760 Mission Ct. Fremont, CA 94539</p>
156.96.46.27	<p>Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017</p> <p>Fastlink Network, Inc. Fastlink Network – Newtrend Division P.O. Box 17295</p>

	<p>Encino, CA 91416</p> <p>Fastlink Network, Inc. c/o Incorp Services, Inc. 5716 Corsa Ave, Suite 110 Westlake Village, CA 91362</p> <p>Fastlink Network, Inc. 624. S. Grand Ave. Los Angeles, CA 90017</p> <p>Fastlink Network, Inc. and VolumeDrive, Inc. 1143 Northern Blvd. Clarks Summit PA 18411</p> <p>Fastlink Network, Inc. and VolumeDrive, Inc. 9 East Market St Wilkes Barre, PA 18701</p>
<p>195.123.241.13</p> <p>195.123.241.55</p>	<p>Green Floid LLC c/o Business Filings Inc. 1200 South Pine Island Road Plantation, FL 33324</p> <p>Green Floid LLC 119 Grimsby St. – Staten Island New York, NY 10306</p> <p>Green Floid LLC 2707 East Jefferson Street Orlando, FL, 32803</p> <p>Green Floid LLC ITL-Bulgaria Ltd. c/o Equinix, Inc. 1920 E. Maple Ave. El Segundo, CA 90245</p> <p>Equinix, Inc. One Lagoon Dr. Redwood City, CA 94065</p>

	<p>Equinix, Inc. c/o United Agent Group, Inc. 4640 Admiralty Way, 5th Floor Marina del Rey, CA 90292</p>
162.247.155.165	<p>Twinservers Hosting Solutions Inc. 23 Meadowview Circle Nashua, NH 03062</p> <p>Twinservers Hosting Solutions, Inc. c/o DataSite Atlanta BPC, LLC c/o Burges Property & Co. 1130 Powers Ferry Pl. Marietta, GA 30067</p> <p>DataSite Atlanta BPC, LLC Burges Property & Co. 2658 Del Mar Heights Rd. #558 Del Mar, CA, 92014</p> <p>Twinservers Hosting Solutions, Inc. c/o Performive LLC 1130 Powers Ferry Pl. Marietta, GA 30067</p> <p>Performive LLC c/o Holt Ney Zatzoff & Wasserman, LLP 100 Galleria Parkway, Suite 1800 Atlanta, GA, 30339</p>

EXHIBIT 3

Jul 12, 2019 |

250 million Email addresses harvested and counting...

Author: Shaul Vilkomir-Preisman

Supporting research: Tom Nipravski

Update: Further developments on how [TrickBooster operates is accessible here](#).

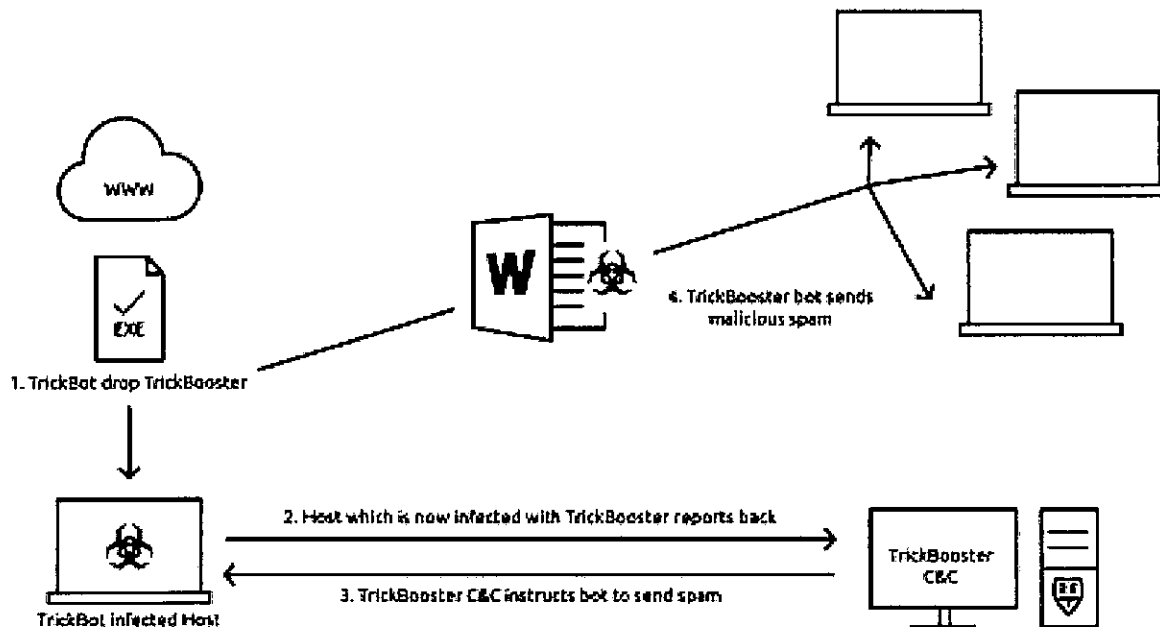
Ever since its discovery in 2016 TrickBot has remained a continuously active and very adaptive actor in the cybercrime threat landscape. What was once a malware family focused on financial data theft is now a robust, elaborate and sophisticated threat, multi-purposed for various types of malicious activity. Recent findings from a currently active and ongoing [TrickBot campaign](#), which features extensive use of signed malware binaries, indicate that it now has a new variant. Alongside its recent addition of a [cookie stealing module](#) it has gained a new partner in crime – a malicious email-based infection and distribution module that shares its code signing certificates (details in IOC section below).

The module is employed to harvest Email credentials and contacts from a victim's address book, inbox, outbox, it can send out malicious spam Emails from the victim's compromised account, and finally delete the sent messages from both outbox and the trash folder, so as to remain hidden from the user. We believe this module is used by Trickbot for several purposes; prorogation and infection, spreading spam for monetization purposes, and harvesting email accounts which can then be traded and used by other campaigns.

During our investigation of this new module and the network infrastructure associated with it, we were able to access infection servers from which the malware is downloaded onto victim machines, as well as command and control servers. We managed to recover a data base containing **250 million e-mail accounts**harvested by TrickBot operators, which most likely were also employed as lists of targets for malicious delivery and infection. The data base includes millions of addresses from government departments and agencies in the US and the UK.

In this blog post we will present our main findings so far based on research conducted in the last 10 days. Our research and analysis into this module, its activity and capabilities continues, and we will update with more details as they become available.

Attack Flow



Infographic showing TrickBooster infection flow.

Stage 1 – Victim machine, infected with TrickBot, receives instruction from TrickBot command and control to download TrickBooster, which is signed with a valid certificate.

Stage 2 – TrickBooster reports back to dedicated command and control server, sending lists of harvested e-mail credentials and addresses.

Stage 3 – TrickBooster command and control server instructs bot to send malicious spam e-mails.

Stage 4 – TrickBooster bot sends malicious infection and spam e-mails.

Deep Instinct's Investigation and Findings

Our investigation started when Deep Instinct detected and prevented a TrickBooster infection attempt using a signed malware binary at a customer environment in the US almost two weeks ago.

Seeing a signed malware binary delivered to a customer environment prompted us to investigate further. We analyzed the malware sample and found swaths of PowerShell code in its memory. Analysis of this PowerShell code immediately led us to the conclusion that we are dealing with a mail-bot.

```
Function Grab {  
  [cmdletbinding()]  
  param(  
    [bool]$collectFromInbox,  
    [bool]$collectFromOutbox,  
    [bool]$collectFromAddressBook,  
    [bool]$collectFromFolders,  
    [System.Object]$cookies  
  )  
  # <...REDACTED...>  
}
```

```
Function Send {  
  [cmdletbinding()]  
  param(  
    [System.Object]$to,  
    [string]$subject,  
    [string]$body,  
    [string]$attachPath,  
    [System.Object]$cookies  
  )  
  # <...REDACTED...>  
}
```

```
Function GetMIMEType {  
  [cmdletbinding()]  
  param(  
    [string]$ext  
  )  
  
  process {  
    $types = @{  
      ".doc" = "application/msword"  
      ".docx" = "application/msword"  
      ".pdf" = "application/pdf"  
      ".ppt" = "application/vnd.ms-powerpoint"  
      ".rar" = "application/x-rar-compressed"  
      ".xls" = "application/vnd.ms-excel"  
      ".xlsx" = "application/vnd.ms-excel"  
      ".zip" = "application/zip"  
      ".7z" = "application/x-7z-compressed"  
    };  
  
    $exType = $types[$ext];  
  }  
  # <...REDACTED...>  
}
```

PowerShell code snippets extracted from TrickBooster's memory, showing functions to harvest e-mails addresses and send malicious spam e-mails.

Following initial analysis, we started looking for more leads on the malware, cross referencing certificate information, sample similarity, and infrastructure used to both deliver and control the malware. We discovered more samples of the malware, both signed and not, additional infrastructure used in the campaign – both to distribute (infection points) and control the malware (C2 Servers). TrickBot samples were also found, signed using the same code signing certificates.

These code signing certificates were apparently issued to various small-to-medium businesses based in the UK. One of which seemingly has very little use for code signing certificates, an air-conditioning, heating and plumbing company, while others do indeed may have a legitimate use for them, according to their registrations.

We continued monitoring the campaign and the infrastructure involved in it, both its infection points and C2 Servers, which were going on and off line, and employing various Geo-IP restrictions and other mechanisms to hamper analysis. It was at one of these servers that we found something that made us realize how successful this campaign is – an Email dump containing approximately 250 million Email addresses.

The Email Database

The recovered Email dump contains massive amounts of commonly used mail provider addresses such as Gmail, Yahoo, etc., but is not limited to these alone. It also contains large amounts of **e-mail addresses from various Government departments and other high-profile targets in both the US and the UK.**

Other organizations found include universities in the UK and Canada, and several provincial agencies and Governments in Canada.

The numbers of listing for common mail providers were as follows:

Gmail.com – 25,863,076 addresses

Yahoo.com – 19,079,339 addresses

Hotmail.com – 11,120,126 addresses

Aol.com – 7,135,831 addresses

Msn.com – 3,512,034 addresses

Yahoo.co.uk – 2,070,848 addresses

Spot checking a few thousands of these compromised Email addresses against previously recorded leaks and breaches, leads us to believe that this is a new mass compromise of e-mails, not previously seen or reported before.

This case, and this significant finding, highlights the success and sophistication of TrickBot, an already very accomplished piece of malware. For a threat actor in the cybercrime sphere, collaborating with a spam malware can bring many possible advantages. Chief among them is the increased ability to distribute your own malware, as spam-bots of all sorts, have been and will likely continue to be, a backbone of malware distribution in general.

As mentioned, TrickBooster is a powerful addition to TrickBot's vast arsenal of tools, modules and collaborations with other malware. This is not only due to the greatly increased spreading and information harvesting ability, but also due to the cover-up of the 'implant' left behind. Following initial deployment of the malware on the victim machine, the implant left behind by the malware, after it finishes initial execution and clean-up goes successfully undetected.

This clean-up is thorough and involves deleting the original infecting executable file, which is a very common practice employed by many malware families. The result is that it is missed by nearly all scanning security vendors, an impressive stealth factor that is much desired among malware operators.

This file, whose main functionality appears to be an e-mail collector targeting *OUTLOOK.exe*, begins its execution by creating an additional thread where this module is looking for an *OUTLOOK.exe* window by using "FindWindow" function with "rctrl_renwnd32" as class name (an identifier of the *OUTLOOK.exe* window).

On the other thread – this module is using COM objects to interact with *OUTLOOK.exe*. It starts doing so by initializing a COM object (CoInitializeEx) and continuing to interact with it by creating an instance of "Microsoft.Office.Interop.Outlook" with "CoCreateInstance". It then tries to start *OUTLOOK.exe* by using "OleRun" function.

When *OUTLOOK.exe* is executed – this module knows to start interacting with it by using Microsoft Outlook Messaging API (MAPI).

MAPI provides the messaging architecture for Microsoft Outlook 2013 and Outlook 2016. It provides a set of interfaces, functions, and other data types to facilitate the development of Outlook messaging applications. Applications use MAPI to manipulate email data, to create email messages and the folders to store them in, and to support notifications of changes to existing MAPI-related data.

This, and more research and analysis of TrickBooster is still ongoing with more details to be published in the near future.

During our investigation of TrickBooster, we have contacted DigiCert/Thawte, who issued the code signing certificates used to sign both TrickBot and TrickBooster samples used in this campaign and requested their revocation. The offending certificates have been revoked by DigiCert/Thawte.

We are also in the process of reporting and providing details to CERTs and other relevant authorities, and we will work with partners in the community to make available the e-mail address dumps in a secure manner.

Indicators of compromise (IOCs)

Shared Certificate Details

Shared Cert 1

Cert SHA1: 5DE6E48A350F60CE11D9D3AC437BE8CCBC3D415C

Issued to: <https://beta.companieshouse.gov.uk/company/08306316>

TrickBot signed sample (SHA256):

3f651b525ceaa941c143b2adc3244b3d4b9af299ad09beea345867258dfbf5e7

TrickBooster signed sample (SHA256):

620020a21c8074d689e80fc1ae29acf8c34d3481ed380f20ad445b88a7bf442e

Shared Cert 2

Cert SHA1: 30A852583F8C2CA4710B431C800E4924C2C727EF

Issued to: <https://beta.companieshouse.gov.uk/company/08549469>

TrickBot signed samples (SHA256):

33eed709eb06f57d371fa97097f821858ad4143900c7aa4c302ce190d51370ff

dcaa278d0dbbd0b068615aef5a87db1cbe664a6f51c5e9cc6a09fe354990fa6

TrickBooster signed sample (SHA256):

65596dd4caa7fa9e8d048dfb5a5e46b04874060eb888d320ee2ced752669f5e

Shared Cert 3

Cert SHA1: 67ED536B62CFE6855F1821DB1FE084616F0592E4

Issued to: <https://beta.companieshouse.gov.uk/company/08480288>

TrickBot signed sample (SHA256):

e7e64753cf91d1d35c3098fcd491f53dda01e83c47f6bede3d5bfe6775fb20c8

TrickBooster signed sample (SHA256):

d96fd330c765b88f3503899755624cbe020ab3e2c53e28d7dee38e7b35f3eab2

TrickBooster Infection servers (servers known to host TrickBooster executables in this campaign)

hxxp://104.216.111.171/

hxxp://85.204.116.92/

TrickBooster Command & Control servers (servers controlling TrickBooster bots involved in this campaign)

185.86.148.63:2050

178.156.202.242:2050

62.109.25.254 (likely Command & Control Server)

TrickBooster file hashes (SHA256, involved in this campaign)

620020a21c8074d689e80fc1ae29acf8c34d3481ed380f20ad445b88a7bf442e

65596dd44caa7fa9e8d048dfb5a5e46b04874060eb888d320ee2ced752669f5e

d96fd330c765b88f3503899755624cbe020ab3e2c53e28d7dee38e7b35f3eab2

f7eeae88c68056ab4087b4a5c7c5797f9075d0384b271f136776ff5249cb497

48d591518b306a91853ac65697dd888a0afa442014b878d777879064091f73e1

fe527937e1e512b72111102d9e18c10120b77cd9832230950ce55a718e75a9f0

FUD TrickBooster “Implant” file hashes (SHA256)

[4ba33bf8a5e8b065f5055dd2c655dc2a271e9587b037e9b3e548b6c51cab3e9e](#)

[702e96fef5b2ad643a0f702b26a3fd237592f778e4fbc707c80e93326fd08d58](#)

[6bf8f079021c8018f6ab37a29091e838918734bf9d1c532852561b6a0d71f12d](#)

Additional File hash IOCs (SHA256)

2787838d3eb2fd14e80eff102b3967c3e5f1ed9f26f0ecc856ee68dfa28b9fd5

688b4a4ef3ac5de4f2c87bb5061f3f0729efe5818d2463437f4e742d9efbcf05

ef61dc27b55fb493c94ffd7022669c95e999fb6e60eb83a78fd462eab5f4b5d6

98a60cb7e0a0337a132def0ad766b8c5dda0d6777bf531d2a5f2493bb3de4348

00ba7cd7bb268fa6f6ef09fa679e5f5d68a27be512da24c556ea04673e852978

b02494ffc1dab60510e6caee3c54695e24408e5bfa6621adcd19301cfc18e329

fc0770975ca3337984c3d4912ef592c805333e8bdf76fd4d3256ebc4e5916be7

f446f39223567f99ae2fb60f372583bc37d54ffe055f20eda8382c14eeea01f5

688b4a4ef3ac5de4f2c87bb5061f3f0729efe5818d2463437f4e742d9efbcf05

4abeab45c0503957e16373fe8f872d6055402614d317b1aa969becf07a6fdb05

9/27/2020

TrickBooster – TrickBot's Email-Based Infection Module - Deep Instinct

748891c0ea84b6f8e2b44ec78acd474338c16e8bc24a975b867ac56ad994d939

ddd9d1a3c2cf31e2d361922c91efc9be6a253ad5854bb2adfdb02bc21a43817b

EXHIBIT 4

First ransomware-related death reported in Germany



September 21, 2020

The Duesseldorf University Clinic in Germany was hit by a ransomware attack last week that forced staffers to direct emergency patients elsewhere. The cyberattack “crippled the entire IT network of the hospital.” As a result, a woman seeking emergency treatment for a life-threatening condition died after she had to be taken to another city for treatment, according to several outlets.

Though the attack occurred earlier during the week and the phone systems was brought back online, other systems remained down. The hospital, however, said that that “there was no concrete ransom demand,” and no clear indications that data is irretrievably lost and that its IT systems are being gradually restarted, according to *AP News*.

According to report from North Rhine-Westphalia state’s justice minister, 30 servers at the hospital were encrypted last week and an extortion note left on one of the servers, news agency dpa reported, says *AP News*. The note called on the addressees to get in touch, but didn’t name any sum and was addressed to the Heinrich Heine University, to which the Duesseldorf hospital is affiliated, and not to the hospital itself.

Duesseldorf police then established contact and told the perpetrators that the hospital, and not the university, had been affected, endangering patients. The perpetrators then withdrew the extortion attempt and provided a digital key to decrypt the data, *AP News* reports.

Mohit Tiwari, Co-Founder and CEO at [Symmetry Systems](#), a San Francisco, Calif.-based provider of cutting-edge Data Store and Object Security (DSOS), notes that hospitals have a particularly challenging setting as they have to prioritize fighting healthcare-related fires all the time and have to work with software (and hardware) that takes years to certify for safety.

"This means the compute infrastructure lags behind due to both business (lower priority expense) and technical (expensive and risky to upgrade) reasons," Tiwari explains. "Perhaps the shift in mindset that hospital executives have to get to is that compute infrastructure in hospitals is key to healthcare, and computing failures are healthcare failures. Further, computing flaws are highly correlated and can spread quickly -- ransomware or breach of large data stores or compromise of medical equipment on a network. These systemic failures look a lot different than safety faults in a machine that would be triggered in specific conditions, and computing failures will soon get a lot harder to get insurance for. With the right investments, there is recent technology that can lift and shift certified workloads into safer virtual machines and put defenses around it, and better identity and authorization methods that prevent small errors from scaling out organization wide."

Terence Jackson, Chief Information Security Officer at [Thycotic](#), a Washington D.C. based provider of privileged access management (PAM) solutions, notes, "The outcome of this event is tragic. I offer condolences to the family of the patient. Yet, this highlights that the consequences of a ransomware attack can be deadly. As details are still emerging, it is thought that the ransomware exploited a vulnerability that a patch had been released to remediate."

According to a recent [Check Point report](#), 80 percent of observed ransomware attacks in the first half of 2020 used vulnerabilities reported and registered in 2017 and earlier – and more than 20 percent of the attacks used vulnerabilities that are at least seven years old. Jackson adds, "Patch management is a critical component to network security."

Rick Holland, Chief Information Security Officer, Vice President Strategy at [Digital Shadows](#), a San Francisco-based provider of digital risk protection solutions, says that, "In the early days of COVID-19, we saw actors stating that they wouldn't target healthcare, so at least some criminal element is publicly against these sorts of attacks. Opportunistic ransomware actors who cast a wide net may not realize that many university systems have significant healthcare components that conduct research and treat patients. Law enforcement agencies are already highly focused on ransomware operators. Still, any attacks that result in the loss of life will only increase the criminals' risk of indictments and arrests. It will be interesting to see how targeting evolves in the future due to this tragic event, but I wouldn't place bets on all criminals avoiding healthcare institutions. There is no honor among thieves."

Mark Kedgley, CTO at [New Net Technologies \(NNT\)](#), a Naples, Florida-based provider of IT security and compliance software, warns this incident won't be the last time that cybersecurity has such a direct impact on human lives. "As the indiscriminate distribution of ransomware hits more IT systems and operational technology underpinning critical infrastructure, like hospitals, energy, and rail and traffic management, we will all be affected more by hacker-instigated disruption," Kedgley says. "As with WannaCry, it seems likely that the vulnerability exploited here was months old, so in theory there was time to mitigate the threat in theory, but it illustrates the importance of running vulnerability scans and acting on findings at least every 30 days if not more frequently. This becomes more difficult in a 24/7 operation like a hospital or power station, where resolving the conflict between the demand for continuous uptime, and maintaining cybersecurity, gets really tough."

EXHIBIT 5

The Cybersecurity 202: Ransomware attack against the 2020 election could disrupt statewide voting databases

By Joseph Marks

September 6, 2019 at 4:40 a.m. PDT

with Tonya Riley

THE KEY

Top government cybersecurity officials are worried that ransomware, which has wreaked havoc by locking up the computer networks of businesses, schools and police stations, could be used to sow chaos during the 2020 election.

Perhaps most damaging of all would be if hackers used ransomware — an attack disabling an organization's computers and encrypting its data — to lock up a state's voter registration database in the days before an election. That would prevent local election officials from verifying that people are voting where they're supposed to, Chris Krebs, the top cybersecurity official at the Homeland Security Department, said yesterday.

Krebs's organization, the Cybersecurity and Infrastructure Security Agency, is launching a major initiative to ensure those databases are protected against ransomware, which was first reported by Reuters last week.

The organization is also contacting more than 8,000 election jurisdictions and urging them to take basic cybersecurity measures to ensure their other election infrastructure is as secure as possible, he said.

"We're not going to let the Russians come back. We're not going to let the Chinese, we're not going to let the Iranians," Krebs said. "We're going to be ready. We're working every day on this problem set."

A ransomware attack could conceivably throw the results of the 2020 presidential election into question and spark deep distrust in the results — without the attackers hacking any voting machines or changing any votes.

Krebs described that as a "worst-case scenario" in a speech at the Billington Cybersecurity Summit. The danger is particularly grave because voter registration databases were targeted by Russian hackers in 2016, according to the report by former special counsel Robert S. Mueller III, and are the piece of election infrastructure most likely to be connected to the Internet.

About half of states have signed up for DHS to scan their voter registration databases to ensure they're as secure as possible against ransomware, Krebs told reporters on the sidelines of the cybersecurity conference. In some other cases, those states are getting the same cybersecurity scans but from private security companies, he said.

He described the initiative as part of a broader DHS effort to evolve from the 2018 election — when the department focused primarily on helping state and local election agencies achieve basic digital protections against hacking — to envisioning and protecting against what attackers might do next in 2020.

“We are trying to look at, given what we know today ... what’s the worst-case scenario a year from now?” he said. “How could things get worse? That’s what we’re trying to get ahead of.”




Hackers that target businesses and state and local government agencies with ransomware have generally unlocked the victims' files after they paid a ransom, but there’s no guarantee that attackers targeting voter registration databases would do the same — especially if their real goal was to undermine the election rather than to make money.

Ransomware attacks have also grown substantially in recent years as hackers see how lucrative they can be. An August report from the cybersecurity company McAfee Labs found the attacks had increased more than 100 percent over the previous year.


“Ransomware is not a problem that’s going away,” Krebs said. “Every time a company, an agency or jurisdiction or whatever pays [a ransom] out, it just validates the model.”

During a separate cybersecurity conference yesterday, FBI Deputy Assistant Director Tonya Ugoretz urged ransomware victims never to pay ransoms, saying it would encourage more such attacks and could fund other nefarious activities.

Here are details from CBS News’s Olivia Gazis:

 **Olivia Gazis** 
@Olivia_Gazis 

"We do **not** recommend paying the ransom" in ransomware attacks, says FBI's Tonya Ugoretz - even in cases where costs of not paying begin to exceed ransom amount. Victims don't know where money goes, whether files will actually be decrypted & payouts only encourage the activity.

10:42 AM · Sep 5, 2019 



 5  See Olivia Gazis's other Tweets

EXHIBIT 6

Ransomware Attacks Take On New Urgency Ahead of Vote

Attacks against small towns, big cities and the contractors who run their voting systems have federal officials fearing that hackers will try to sow chaos around the election.



By [Nicole Perloff](#) and [David E. Sanger](#)

Sept. 27, 2020

A Texas company that sells software that cities and states use to display results on election night was hit by ransomware last week, the latest of nearly a thousand such attacks over the past year against small towns, big cities and the contractors who run their voting systems.

Many of the attacks are conducted by Russian criminal groups, some with shady ties to President Vladimir V. Putin's intelligence services. But the attack on Tyler Technologies, which continued on Friday night with efforts by outsiders to log into its clients' systems around the country, was particularly rattling less than 40 days before the election.

While Tyler does not actually tally votes, it is used by election officials to aggregate and report them in at least 20 places around the country — making it exactly the kind of soft target that the Department of Homeland Security, the F.B.I. and United States Cyber Command worry could be struck by anyone trying to sow chaos and uncertainty on election night.

Tyler would not describe the attack in detail. It initially appeared to be an ordinary ransomware attack, in which data is made inaccessible unless the victim pays the ransom, usually in harder-to-trace cryptocurrencies. But then some of Tyler's clients — the company would not say which ones — saw outsiders trying to gain access to their systems on Friday night, raising fears that the attackers might be out for something more than just a quick profit.

That has been the fear haunting federal officials for a year now: that in the days leading up to the election, or in its aftermath, ransomware groups will try to freeze voter registration data, election poll books or the computer systems of the secretaries of the state who certify election results.

With only 37 days before the election, federal investigators still do not have a clear picture of whether the ransomware attacks clobbering American networks are purely criminal acts, seeking a quick payday, or Trojan horses for more nefarious Russian interference. But they have not had much success in stopping them. In just the first two weeks of September, another seven American government entities have been hit with ransomware and their data stolen.

"The chance of a local government not being hit while attempting to manage the upcoming and already ridiculously messy election would seem to be very slim," said Brett Callow, a threat analyst at Emsisoft, a security firm.

The proliferation of ransomware attacks that result in data theft is an evolution in Russian tactics, beyond the kind of "hack and leak" events engineered against the Democratic National Committee and Hillary Clinton's campaign chairman, John Podesta, in 2016. By design, whether the attacks are criminal or state sponsored is not clear, and the attacker does not always have to be successful everywhere. Just a few well-placed ransomware attacks, in key battleground states, could create the impression that voters everywhere would not be able to cast their ballots or that the ballots could not be accurately counted — what the cybersecurity world calls a "perception hack."

"We have been hardening these systems since last summer," Christopher Krebs, who runs the Cybersecurity and Infrastructure Security Agency for the Department of Homeland Security, said this month. He noted that the agency was trying to make sure local election officials printed out their electronic poll books, which are used to check in voters, so that they had a backup.

The United States has made "tremendous progress" in the effort, Mr. Krebs added, by "getting on this problem early."

Still, some officials worry that President Trump's repeated assertion about the election that "we're not going to lose this except if they cheat" may be the 2020 equivalent of "[Russia, if you're listening](#)" — seen as a signal to hackers to create just enough incidents to bolster his unfounded claims of widespread fraud.

So far Mr. Trump has focused on mail-in ballots and new balloting systems, but on election night there would be no faster way to create turmoil than altering the reporting of the vote — even if the vote itself was free of fraud.

That would be a classic perception hack: If Mr. Trump was erroneously declared a winner, for example, and then the vote totals appeared to change, it would be easy to claim someone was fiddling with the numbers.

The Russians tried this, and almost got away with it, in Ukraine’s presidential election six years ago. That is one reason the F.B.I. warned last week that the days after the election could result in “disinformation that includes reports of voter suppression, cyberattacks targeting election infrastructure, voter or ballot fraud, and other problems intended to convince the public of the elections’ illegitimacy.”

The F.B.I. warning made no mention of Mr. Trump’s own declarations that if Mr. Biden wins, the election must be illegitimate, or his baseless attacks on the use of mail-in ballots. But on Saturday night at a [rally in Pennsylvania](#), the president openly speculated how an uncertain outcome could throw the election into the courts or Congress, both places where he believes he has an advantage.

Follow the presidential debates live. We'll send you alerts with our analysis in real time.

[Sign up for alerts](#)

[Terms of Service](#) | [Privacy Policy](#)

That is why the surge in ransomware has become such a rising concern. Should an attack be well-timed enough to make it difficult to count votes or certify tallies, it would add to the uncertainty — just what the Russians, and perhaps Mr. Trump himself, are seeking.

Part of the problem is that the full scale of ransomware attacks is not always disclosed.

It was three years after the 2016 election that the Department of Homeland Security, the F.B.I. and even Florida state officials learned that Palm Beach County — which played a critical role in deciding the 2000 election — had its election offices seized by ransomware just weeks before the election.

Sign up to receive an email when we publish a new story about the [2020 election](#).

[Sign Up](#)

Over the past 18 months, cybercriminals — primarily based in Russia and Eastern Europe — have hit the American public sector with more ransomware attacks than in any other period on record, according to Emsisoft, which tracks the incursions. A record 966 ransomware attacks hit the American public sector last year — two-thirds of them targeting state or local governments.

Election 2020 ›

Latest Updates

Updated 1 hour ago

- [Don't expect the debate moderator Chris Wallace to fact-check on Tuesday.](#)
 - [A single congressional district in Nebraska could prove decisive in a close presidential election.](#)
 - [Trump again dismisses a Times investigation that he paid little or no federal income tax for years.](#)
-

Among them: A Texas county that voted for Hillary Clinton in 2016 as well as counties that helped determine the 2016 election in Ohio, Pennsylvania, Florida and Georgia, and other cities and counties that will most likely play a critical role in deciding close Senate races in South Carolina, Kentucky, Colorado and Maine in November.

The F.B.I. concluded that ransomware “will likely threaten the availability of data on interconnected election servers” in November, according to a bureau analysis leaked this summer. The agency cited two recent examples: a ransomware attack in Oregon that locked up county computers and crippled backup data, and another in Louisiana in which cybercriminals hacked the secretary of state’s offices, then waited three months to detonate their ransomware the week of Louisiana’s statewide elections for governor and legislative seats last November.

The Louisiana election proceeded unscathed because officials had the foresight to separate voter rolls from internal networks. Still, some analysts feared the attack was a dry run for Nov. 3.

Sometimes victims pay — as a small town in Florida did. Sometimes they refuse, [as Atlanta did](#) — though it ended up spending more than the ransom demand reconstructing its systems.

The latest victim, Tyler Technologies, has been vague about the details of its attack. Citing a continuing investigation, the company declined to elaborate on the ransom demands, say whether it paid or offer any details about the attackers. And while the company claimed that none of its products “support voting or election systems,” its Socrata dashboard software is used by some election officials to aggregate and share election results.

That display software is precisely the kind of soft target that intelligence agencies warned could be subject to foreign manipulation on Election Day. In the Ukraine case in 2014, Russian hackers got into the software that reported the country's election results to the media, altering it to falsely claim victory for a far-right candidate. Ukrainians caught the hack just in time and reported the correct results on television that night. Tellingly, Russian state media still reported that the far-right candidate had won the presidency.

It was a classic perception hack because even if the actual ballots are untouched, an attack that delayed the vote or cast doubt on the ultimate results could create enough uncertainty in voters' minds that somehow the election was illegitimate.

The Republican-led Senate Intelligence Committee report into the 2016 election even warned against the kind of proclamations Mr. Trump is making about "rigged" elections from the White House press room and at rallies.

"Sitting officials and candidates should use the absolute greatest amount of restraint and caution if they are considering publicly calling the validity of an upcoming election into question," the report said, noting that doing so would only be "exacerbating the already damaging messaging efforts of foreign intelligence services."



Christopher A. Wray, the F.B.I. director, testified before a Senate committee on Thursday. Pool/Tom Williams

Christopher A. Wray, the F.B.I. director, countered the president's claims on Thursday, telling lawmakers that his agency had "not seen, historically, any kind of coordinated national voter fraud effort in a major election, whether it's by mail or otherwise." He was immediately attacked by the White House chief of staff, Mark Meadows. "With all due respect to Director Wray, he has a hard time finding emails in his own F.B.I.," Mr. Meadows said on Fox News.

Still, American officials are walking a thin line. They are trying not to ramp up too many fears about ransomware for fear of amplifying the uncertainty.

But at the same time, security researchers have noted with growing alarm that the ransomware attacks hitting American systems are evolving in disturbing ways. Attackers are not just locking up data, they are stealing it, dumping it online in some cases, and selling access to victims' data on the dark web and privately to nation-state groups. Researchers at Intel471, a threat intelligence firm, recently discovered that Russian cybercriminals had been selling access to victims' data to North Korean hackers, and Russian cybercriminals have a long track record of working hand in hand with the Kremlin.

When the Treasury Department imposed sanctions on members of an elite Russian cybercrime group last December, they outed the group's leader as a member of Russia's Federal Security Service, or F.S.B., a successor to the K.G.B.

Three years ago, the Justice Department [accused two F.S.B. agents](#) of working closely with two cybercriminals to hack 500 million Yahoo accounts. Russian agents allowed cybercriminals to profit from the attack, while mining their access to spy on journalists, dissidents and American officials.

"There is a pax mafiosa between the Russian regime and its cybercartels," said Tom Kellermann, the head of cybersecurity strategy at VMware, who sits on the Secret Service's cyberinvestigations advisory board. "Russia's cybercriminals are treated as a national asset who provide the regime free access to victims of ransomware and financial crime. And in exchange, they get untouchable status."

"It's a protection racket," Mr. Kellermann said. "And it works both ways."

EXHIBIT 7

DOD contractor suffers ransomware infection

Virginia-based EWA has had systems infected with the Ryuk ransomware.



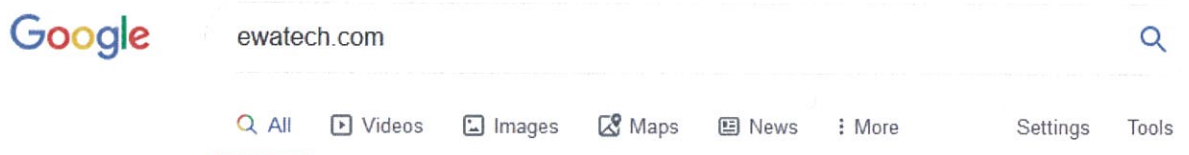
By Catalin Cimpanu for Zero Day | January 29, 2020 -- 23:40 GMT (15:40 PST) | Topic: Security



Electronic Warfare Associates (EWA), a 40-year-old electronics company and a well-known US government contractor, has suffered a ransomware infection, ZDNet has learned.

The infection hit the company last week. Among the systems that had data encrypted during the incident were the company's web servers.

Signs of the incident are still visible online. Encrypted files and ransom notes are still cached in Google search results, even a week after the company took down the impacted web servers.



About 6,630 results (0.27 seconds)

www.ewatech.com ▾

ô,g)?8~ÚÂ\$³F ÇÀCËöç3 ™ ·ícfK Dô=z@»1 WÁ 1...|Hý
M•„o"9KÊsÊJ ...

ô,g)?8~ÚÂ\$³F ÇÀCËöç3 ™ ·ícfK Dô=z@»1 WÁ 1...|Hý M•„o"9KÊsÊJ~€\$ní×'v %oäi {6xW Mä".É
-[ñ@œšò Ì¼?gD—FÒA! ê]œ*TârÇj-ítò bíh' ""J Ý@4 'ÁUò Gç áá ...

www.ewatech.com > corelis_logo.php.RYK ▾

ОЙЪ ЛЬ-İY'ФёН " хЗГs~ъе} W:нь : жинКсЈР ħухКЛаб±я+Э,К' ...

ОЙЪ ЛЬ-İY'ФёН " хЗГs~ъе} W:нь : жинКсЈР ħухКЛаб±я+Э,К' rPЬ P Ым-|rзэ<íжJ; M&rчEcd yБ
Ў6gщ"-ГЙb—гпчЯ KгNED™Ш ЛЬРЬО нь Pw@ечъ ...

www.ewatech.com > RyukReadMe ▾

████████████████████@protonmail.com balance of shadow universe ...

████████████████████@protonmail.com. balance of shadow universe. Ryuk.

Image: ZDNet

Security researchers who reviewed the cached files told ZDNet the encrypted files and ransom note are, without a doubt, a sign of an infection with the Ryuk ransomware.

The security researcher who first discovered these files told ZDNet that several EWA websites appear to have been impacted, such as the sites for:

- EWA Government Systems Inc. -- an EWA subsidiary that provides electronic warfare (EW) products and services to government and commercial markets in cyber defense, radar development, intelligence, security, training, tactical mission planning, information management, and force protection.
- EWA Technologies Inc. -- an EWA subsidiary specialized in JTAG products.
- Simplicikey -- an EWA subsidiary specialized in the manufacturing a consumer-focused Remote Control Electronic Deadbolt.
- Homeland Protection Institute -- a non-profit chaired by the EWA CEO.

It is unclear at the moment how much of the company's internal network was encrypted during the incident.

Despite visible signs of a ransomware incident on its public websites, EWA has not issued any public statement about the incident.

An EWA spokesperson hung up the phone earlier today when ZDNet reached out for comment about the security breach.

The company is a well-known supplier of electronics equipment to the US government. [On its website](#), EWA lists the Department of Defense (DOD), the Department of Homeland Security (DHS), and the Department of Justice (DOJ) as regular customers.

A CONSPICUOUS RYUK STEALER UPDATE

Making matters worse is that Ryuk is not your regular ransomware strain. This type of ransomware is solely used in targeted attacks on high-profile companies.

It is usually installed on infected networks after a victim is infected with the Emotet/TrickBot trojans, two well-known cybercrime-as-a-service platforms.

The Ryuk gang uses the Emotet/TrickBot-infected machine as entry point and launch pad to scan and spread inside a company's internal network, exfiltrate data, and then deploy their ransomware.

The data exfiltration happens via a Ryuk module called the Ryuk Stealer, which security researchers have been spotting deployed in recent Ryuk attacks.

Coincidentally, the Ryuk Stealer was recently update to target files that may hold government and military-related data, [according to a Bleeping Computer report](#), suggesting a concerted effort on the Ryuk gang's side in targeting government and military entities.

EXHIBIT 8

10 MAR 2020 NEWS

Ryuk Ransomware Takes Out Durham, North Carolina



Phil Muncaster UK / EMEA News Reporter, Infosecurity Magazine

Email Phil Follow @philmuncaster

The North Carolina city of Durham has become the latest US municipality struck by ransomware after reports suggested the Ryuk variant forced key services offline.

In an update on Sunday, the local authority claimed that both the City of Durham and Durham County Government are now in the "recovery process" after being hit by the attack on Friday.

Although emergency calls, 911 and "critical public safety systems" were operational throughout, the incident forced the city to shut down its phone system to contain the attack.

"There are phone disruptions to other city facilities and services, such as Durham One Call's phone line at 919-560-1200, Durham Parks and Recreation centers, City Hall, etc," it explained.

However, the municipality's website and app were not affected, and therefore able to deal with residents' bill payments and other services.

According to local reports, the Ryuk ransomware arrived in a phishing email sent to a city employee.

Aleksander Gorkowienko, managing consultant at Spirent Security Labs, argued that organizations need a combination of employee education and technology controls to mitigate the phishing threat.

"Attackers are clever and opportunistic and, by trial and error, they are continuously searching for methods which statistically give them the highest probability of success with the lowest effort. Here we have good evidence that old methods still work well," he added.

"The lesson for the future is that organizations should balance their efforts between investing in the newest technological security solutions and education of their personnel."

Cesar Cerrudo, CTO of IOActive, argued that it's time for local governments in the US to wake up to the ransomware threat.

"City systems are less protected than private sector systems, so it's no surprise that cyber-criminals target them as easier and juicier targets to ensure they keep profiting," he claimed.

"Cities need to start investing more on cybersecurity in general, including education, threat assessment, monitoring, prevention, etc. in order to have well established plans for quick reaction and recovery from cyber-attacks."

EXHIBIT 9

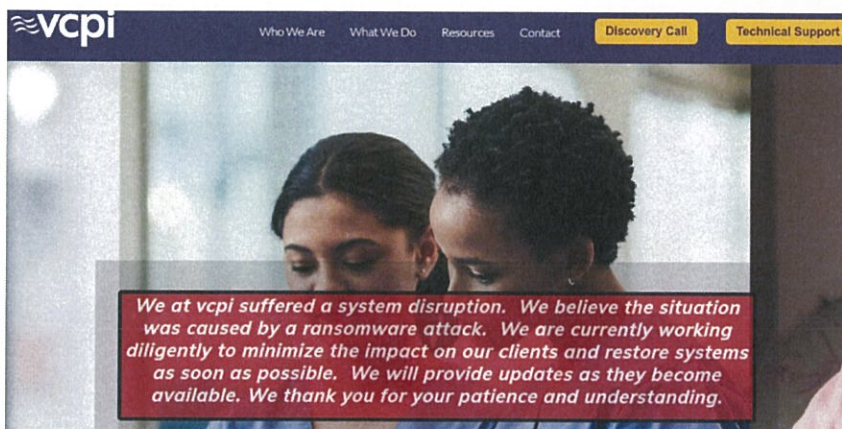


- [About the Author](#)
- [Advertising/Speaking](#)

23
Nov 19

110 Nursing Homes Cut Off from Health Records in Ransomware Attack

A ransomware outbreak has besieged a Wisconsin based IT company that provides cloud data hosting, security and access management to more than 100 nursing homes across the United States. The ongoing attack is preventing these care centers from accessing crucial patient medical records, and the IT company's owner says she fears this incident could soon lead not only to the closure of her business, but also to the untimely demise of some patients.



Milwaukee, Wisc. based [Virtual Care Provider Inc.](#) (VCPI) provides IT consulting, Internet access, data storage and security services to some 110 nursing homes and acute-care facilities in 45 states. All told, VCPI is responsible for maintaining approximately 80,000 computers and servers that assist those facilities.

At around 1:30 a.m. CT on Nov. 17, unknown attackers launched a ransomware strain known as **Ryuk** inside VCPI's networks, encrypting all data the company hosts for its clients and demanding a whopping \$14 million ransom in exchange for a digital key needed to unlock access to the files. Ryuk has made a name for itself targeting businesses that supply services to other companies — particularly cloud-data firms — with the ransom demands set according to the victim's perceived ability to pay.

In an interview with KrebsOnSecurity today, VCPI chief executive and owner **Karen Christianson** said the attack had affected virtually all of their core offerings, including Internet service and email, access to patient records, client billing and phone systems, and even VCPI's own payroll operations that serve nearly 150 company employees.

The care facilities that VCPI serves access their records and other systems outsourced to VCPI by using a [Citrix-based virtual private networking](#) (VPN) platform, and Christianson said restoring customer access to this functionality is the company's top priority right now.

"We have employees asking when we're going to make payroll," Christianson said. "But right now all we're dealing with is getting electronic medical records back up and life-threatening situations handled first."

Christianson said her firm cannot afford to pay the ransom amount being demanded — roughly \$14 million worth of Bitcoin — and said some clients will soon be in danger of having to shut their doors if VCPI can't recover from the attack.

"We've got some facilities where the nurses can't get the drugs updated and the order put in so the drugs can arrive on time," she said. "In another case, we have this one small assisted living place that is just a single unit that connects to billing. And if they don't get their billing into Medicaid by December 5, they close their doors. Seniors that don't have family to go to are then done. We have a lot of [clients] right now who are like, 'Just give me my data,' but we can't."

The ongoing incident at VCPI is just the latest in a string of ransomware attacks against healthcare organizations, which typically operate on razor thin profit margins and have comparatively little funds to invest in maintaining and securing their IT systems.

Earlier this week, a [1,300-bed hospital in France was hit by ransomware](#) that knocked its computer systems offline, causing “very long delays in care” and forcing staff to resort to pen and paper.

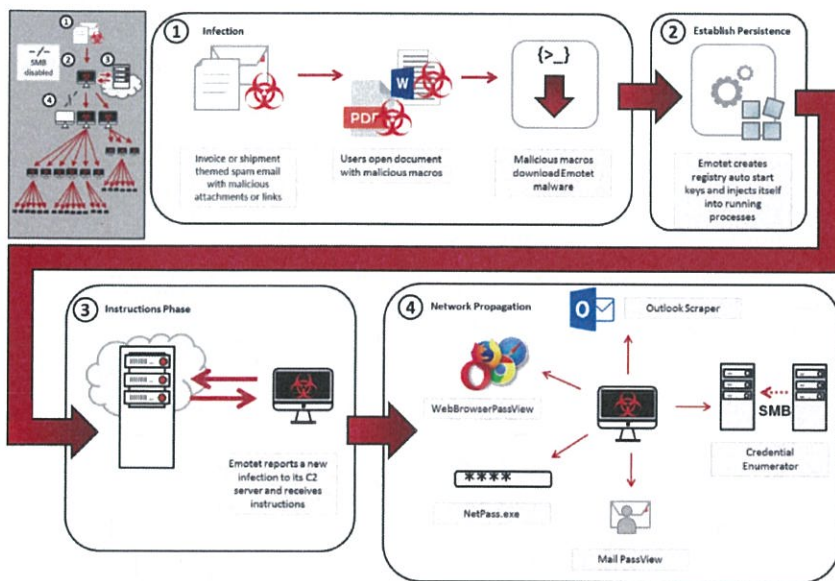
On Nov. 20, Cape Girardeau, Mo.-based **Saint Francis Healthcare System** [began notifying patients about a ransomware attack](#) that left physicians unable to access medical records prior to Jan. 1.

Tragically, there is evidence to suggest that patient outcomes can suffer even after the dust settles from a ransomware infestation at a healthcare provider. [New research](#) indicates hospitals and other care facilities that have been hit by a data breach or ransomware attack can expect to see an increase in the death rate among certain patients in the following months or years because of cybersecurity remediation efforts.

Researchers at Vanderbilt University’s Owen Graduate School of Management took the Department of Health and Human Services (HHS) list of healthcare data breaches and used it to drill down on data about patient mortality rates at more than 3,000 Medicare-certified hospitals, about 10 percent of which had experienced a data breach.

Their findings suggest that after data breaches as many as 36 additional deaths per 10,000 heart attacks occurred annually at the hundreds of hospitals examined. The researchers concluded that for care centers that experienced a breach, it took an additional 2.7 minutes for suspected heart attack patients to receive an electrocardiogram.

Companies hit by the Ryuk ransomware all too often are compromised for months or even years before the intruders get around to mapping out the target’s internal networks and compromising key resources and data backup systems. Typically, the initial infection stems from a booby-trapped email attachment that is used to download additional malware — such as [Trickbot](#) and [Emotet](#).



This graphic from US-CERT depicts how the Emotet malware is typically used to lay the groundwork for a full-fledged ransomware infestation.

In this case, there is evidence to suggest that VCPI was compromised by one (or both) of these malware strains on multiple occasions over the past year. **Alex Holden**, founder of Milwaukee-based cyber intelligence firm [Hold Security](#), showed KrebsOnSecurity information obtained from monitoring dark web communications which suggested the initial intrusion may have begun as far back as September 2018.

Holden said the attack was preventable up until the very end when the ransomware was deployed, and that this attack once again shows that even after the initial Trickbot or Emotet infection, companies can still prevent a ransomware attack. That is, of course, assuming they’re in the habit of regularly looking for signs of an intrusion.

“While it is clear that the initial breach occurred 14 months ago, the escalation of the compromise didn’t start until around November 15th of this year,” Holden said. “When we looked at this in retrospect, during these three days the cybercriminals slowly compromised the entire network, disabling antivirus, running customized scripts, and deploying ransomware. They didn’t even succeed at first, but they kept trying.”

VCPI’s CEO said her organization plans to publicly document everything that has happened so far when (and if) this attack is brought under control, but for now the company is fully focused on rebuilding systems and restoring operations, and on [keeping clients informed](#) at every step of the way.

“We’re going to make it part of our strategy to share everything we’re going through,” Christianson said, adding that when the company initially tried several efforts to sidestep the intruders their phone systems came under concerted assault. “But we’re still under attack, and as soon as we can open, we’re going to document everything.”

EXHIBIT 10

Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic

By

[Lawrence Abrams](#)

- March 26, 2020
- 06:08 PM
- 4



The Ryuk Ransomware operators to continue to target hospitals even as these organizations are overwhelmed during the Coronavirus pandemic.

Last week BleepingComputer [contacted various ransomware groups](#) and asked if they would target hospitals and other healthcare organizations during the pandemic.

With the amount of strain healthcare organizations are under during this pandemic, I was hoping that ransomware operators would avoid these organizations so they can focus on treating people.

Of the seven ransomware operators I contacted, only Maze and DoppelPaymer responded that they would no longer target hospitals.

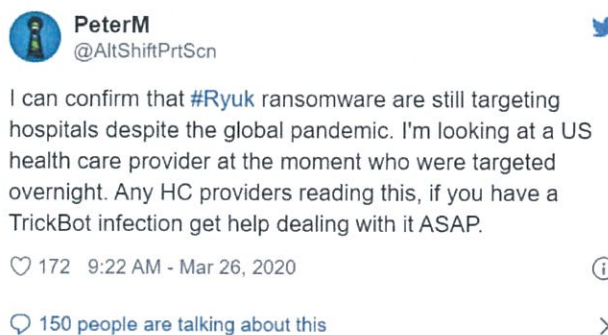
Since then Maze has released the data stolen from a drug testing company that was encrypted before stating they would not target healthcare. They continue to tell BleepingComputer that they will not encrypt hospitals or other healthcare organizations during the pandemic.

Ryuk never responded and continues to target hospitals

One of the ransomware operations we contacted was Ryuk who never responded to our question.

Since then, BleepingComptuer has learned that Ryuk continues to target hospitals even while they are struggling to keep people alive during the Coronavirus pandemic

For example, just this morning PeterM of Sophos tweeted that a US health care provider was attacked and encrypted overnight by Ryuk.



When asked if there were any indicators of compromise (IOCs) that could be shared, he stated it looked like every other Ryuk attack.

"Looks like a typical Ryuk attack at the moment, they deployed the ransomware with PsExec," PeterM stated.

In a conversation with [Vitali Kremez](#), Head of SentinelOne's research division, over the past month, he has seen Ryuk targeting 10 healthcare organizations. Of these ten targets, two are independent hospitals and another is a healthcare network of 9 hospitals in the USA.

9/27/2020

"Not only has their healthcare targeting not stopped but we have also seen a continuous trend of exploiting healthcare organizations in the middle of the global pandemic. While some extortionist groups at least acknowledged or engaged in the discourse of stopping healthcare extortionists, the Ryuk operators remained silent pursuing healthcare targeting even in light of our call to stop," Kremez told BleepingComputer.

BleepingComputer was informed that one of the hospitals is located in a state that is being heavily affected by the Coronavirus at this time.

At any time, but even more so now, encrypting a hospital's data not only affects the ability of a doctor to carry out their job but also whether a patient may live or die.

With everything our medical professionals are dealing with around the world, all people, including ransomware actors, need to give them the space to do their jobs rather than hindering it.

Related Articles:

[Ransomware Gangs to Stop Attacking Health Orgs During Pandemic](#)

[Netwalker Ransomware Infecting Users via Coronavirus Phishing](#)

[Ransomware attack at German hospital leads to death of patient](#)

[University Hospital New Jersey hit by SunCrypt ransomware, data leaked](#)

[Ryuk successor Conti Ransomware releases data leak site](#)