United States Courts
Southern District of Texas
FILED
April 13, 2021
Nathan Ochsner, Clerk of Court

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE SEARCH OF: Certain Microsoft Exchange Servers Infected with Web Shells	CASE NO. 4:21mj755

MOTION TO PARTIALLY UNSEAL SEARCH WARRANT AND RELATED DOCUMENTS AND [PROPOSED] ORDER

The United States of America, by and through its Acting United States Attorney, Jennifer B. Lowery, and S. Mark McIntyre, Assistant United States Attorney for the Southern District of Texas, and respectfully moves this Honorable Court for an Order partially unsealing the search warrant and application for the search warrant, and fully unsealing the motion to seal and sealing order in the above-captioned matter. Due to the conclusion of the FBI operation described in the application, the law enforcement justification for sealing this material, except for the redacted parts of the search warrant and application for the search warrant, appended hereto, no longer exists. Additionally, such unsealing will further enable the government's reasonable efforts to provide notice of the search to some victims.

The law enforcement justification for continuing to seal the redacted parts of the search warrant and application for search warrant is as stated in the motion to seal. Disclosure of the redacted information would likely result in the subjects of the investigation destroying or tampering with evidence, or otherwise taking steps to thwart the investigation, based on the knowledge of that information and the sources of it.

Respectfully submitted,

JENNIFER B. LOWERY
Acting United States Attorney
Southern District of Texas

By: *<u>/s/ S. Mark McIntyre</u>*
S. Mark McIntyre
Assistant United States Attorney
(713) 567-9000

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE SEARCH OF:
Certain Microsoft Exchange Servers
Infected with Web Shells

CASE NO. 4:21mj755

ORDER

Pursuant to the United States' motion and for good cause shown, the motion to seal and sealing order in the above-captioned matter shall be unsealed. The redacted search warrant and redacted application for search warrant appended to the Government's motion shall be unsealed. Any copy of the search warrant and application for search warrant that is unredacted shall remain sealed.

SIGNED at Houston, Texas on this 13th day of April, 2021.

Peter Bray
Honorable Peter Bray
United States Magistrate Judge

TRUE COPY I CERTIFY
ATTEST: *April 13, 2021*
NATHAN OCHSNER, Clerk of Court
By: Kathy Murphy
Deputy Clerk

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

Sealed
Public and unofficial staff access
to this instrument are
prohibited by court order.

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

CERTAIN MICROSOFT EXCHANGE SERVERS
INFECTED WITH WEB SHELLS

Case No. 4:21 mJ755

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment "A"

located in the ________________ District of Multiple, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;

☑ contraband, fruits of crime, or other items illegally possessed;

☑ property designed for use, intended for use, or used in committing a crime;

□ a person to be arrested or a person who is unlawfully restrained.

TRUE COPY I CERTIFY ATTEST:
NATHAN OCHSNER, Clerk of Court
By ____________
Deputy Clerk

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 371	Conspiracy
18 U.S.C. 1030(a)(2)	Theft from a Protected Computer
18 U.S.C. 1030(a)(5)(A)	Damage to a Protected Computer

The application is based on these facts:

(See Attached Affidavit)

☑ Continued on the attached sheet.

☑ Delayed notice of 30 days *(give exact ending date if more than 30 days:* ___________ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached she[redacted]

Applicant's signature

[redacted] FBI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

Telephone *(specify reliable electronic means)*.

Date: 4/9/21

Judge's signature

City and state: Houston, Texas

Peter Bray, United States Magistrate Judge

Printed name and title

United States Courts
Southern District of Texas
FILED

APR 09 2021

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Sealed
Public and unofficial staff access to this instrument are prohibited by court order.

IN RE APPLICATION FOR A WARRANT TO SEARCH CERTAIN MICROSOFT EXCHANGE SERVERS INFECTED WITH WEB SHELLS

Case No. 4:21mJ755

(UNDER SEAL)

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41(b)(6)(B) FOR A SEARCH WARRANT

I, [redacted] a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. FBI is investigating computer intrusions into the Microsoft Exchange Servers of several entities located within the Southern District of Texas and elsewhere. These intrusions and the specific zero-day exploits used to accomplish them, described more fully below, result in the installation of unauthorized web shells (i.e., pieces of code or scripts running on a server that enable remote administration) on Microsoft Exchange Servers, which allow the malicious actors to further compromise victim networks. In a report dated March 2, 2021, described more fully below, Microsoft identified a group of actors behind these intrusions as "HAFNIUM," and associated HAFNIUM with state-sponsored actors operating out of China. [redacted]

2. FBI agents, analysts, and computer scientists (collectively "FBI personnel") have identified certain U.S.-based Microsoft Exchange Servers onto which actors installed, prior to the March 2, 2021 report, unauthorized web shells, identified in Attachment A. [redacted]

[redacted] FBI personnel now seek authorization to search the compromised Microsoft Exchange Servers and uninstall the web shells on those servers.

3. Therefore, I make this affidavit in support of an application for a warrant under Federal Rule of Criminal Procedure 41(b)(6)(B) to use remote access techniques to search certain Microsoft Exchange Servers located in the United States, further identified in Attachment A, and to seize or copy electronically stored information that constitutes evidence and/or instrumentalities of unauthorized access and damage to protected computers, further described in Attachment B.

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

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy) ("Subject Offenses") have been committed in the Southern District of Texas and elsewhere. There also is probable cause to search the information described in Attachment A for evidence, contraband, fruits, and/or instrumentalities of the Subject Offenses, further described in Attachment B.

AGENT BACKGROUND

6. I am a Special Agent with the FBI and have been since [redacted] I am currently assigned to a cyber squad [redacted] I have participated in investigations of criminal offenses involving computer fraud and conspiracy, and I am familiar with the means and methods used to commit such offenses. In addition, I have received training in computer security and investigations involving computers and the Internet. For example, I have several

certifications in computer forensics and advanced computer training. I am an "investigative or law enforcement officer" within the meaning of 18 U.S.C. § 2510; that is, an officer of the United States of America who is empowered to investigate and make arrests for offenses alleged in this warrant.

STATUTORY AUTHORITY

7. Federal Rule of Criminal Procedure 41(b)(6)(B) provides that "a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."

8. Title 18, United States Code, Section 1030(a)(5)(A) provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer . . . shall be punished as provided in subsection (c) of this section." Section 1030(e)(2)(B) defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]"

9. Title 18, United States Code, Section 371 provides: "If two or more persons conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, and one or more of such persons do any act

to effect the object of the conspiracy, each shall be fined under this title or imprisoned not more than five years, or both."

PROBABLE CAUSE

A. Mass Compromise of Microsoft Exchange Servers

10. On or about March 2, 2021, Microsoft released a report titled "HAFNIUM targeting Exchange Servers with 0-day exploits." The intrusions described in the Microsoft report involved the use of multiple zero-day exploits to compromise on-premises versions of Microsoft Exchange Servers. Zero-day exploits refer to a flaw or vulnerability in software or hardware that is unknown to the developer of the software or hardware, and is spotted or acted on by a threat actor before the developer has a chance to fix it. Microsoft Exchange Servers are computers that are involved in the process of storing and retrieving emails.

11. According to the Microsoft report, after the HAFNIUM actors compromised Microsoft Exchange Servers, they would install web shells on the servers to facilitate long-term access to victim environments and further exploitation. The actors, for example, use the web shells to communicate with and distribute files to victim computers to infect them with additional malware. These actors have used their unauthorized access to steal the contents of email accounts and address books. The addition of these web shells impairs the integrity of the victim computer and other computers on the victim computer's network.

12. Microsoft assessed that HAFNIUM actors are state-sponsored and operating out of China based on observed victimology, tactics, and procedures. [redacted] According to open-source reporting, these actors began using the zero-day exploits in January 2021. Initially the targets were high-value

intelligence targets in the United States. The scope of targets later expanded. One researcher described them as a “mass exploitation” and “indiscriminate,” seemingly targeting every Microsoft Exchange Server that could be identified. This same researcher suggested that the actors may have found a way to automate the process of exploitation. According to open-source reporting, after the release of Microsoft’s March 2, 2021, report, hackers not affiliated with HAFNIUM began using the zero-day exploits to target entities that had not yet patched the vulnerabilities. According to open-source reporting, there may be at least 60,000 Microsoft customers worldwide whose Microsoft Exchange Servers were compromised through the use of the zero-day exploits described by Microsoft.

13. Since the release of the March 2, 2021, Microsoft report, Microsoft customers have informed the FBI that their Microsoft Exchange Servers were compromised by the zero-day exploits. Among the IP addresses identified by customers as having unauthorized access to their Microsoft Exchange Servers are IP addresses that are assigned to [redacted]

14. [redacted] An example of a web shell file path (anonymized) is https://webmail.[domain][.]net/aspnet_client/system_web/[redacted].aspx. [redacted]

[redacted] Because these web shells were installed before the March 2, 2021 Microsoft report, the FBI assesses [redacted]. As described below, web shells have been installed on servers in the Southern District of Texas and other districts.

15. [redacted]

16. Following the March 2, 2021 Microsoft report, the FBI and CISA conducted a public awareness campaign to inform owners of Microsoft Exchange Servers that such servers were vulnerable to zero-day exploits and the web shells. A public scan of the approximately [redacted] web shells identified by [redacted], conducted on March 31, 2021, revealed that approximately [redacted] web shells were still present on victim servers. Based on my training and experience, most of these victims are unlikely to remove the remaining web shells because the web shells are difficult to find due to their unique file names and paths or because these victims lack the technical ability to remove them on their own.

B. Remote Access, Searches, and Seizures

17. As described above, FBI personnel have identified approximately [redacted] web shells on Microsoft Exchange Servers, presumptively in the U.S., [redacted]. As of on or about March 31, 2021, approximately [redacted] web shells remain on the servers. FBI personnel seek authorization to search the compromised Microsoft Exchange Servers and, through interactions with the web shells, uninstall the approximately [redacted] web shells on those servers, which are identified in Attachment A. By deleting the web shells, FBI personnel will prevent malicious cyber actors from using the web shells to access the servers and install additional malware on them.

18. Microsoft Exchange Servers located in the United States constitute “protected computers” within the meaning of Rule 41(b)(6)(B) and § 1030(e)(2)(B) because they are used in or affecting interstate or foreign commerce or communication, based on their connection to the Internet. The servers have been “damaged” within the meaning of Rule 41(b)(6)(B) and § 1030(e)(8) because the installation of unauthorized web shells has impaired the integrity and availability of data, programs, systems, and information on the servers.

19. The presumptively U.S.-based Microsoft Exchange Servers, corresponding to the approximately [redacted] web shells in Attachment A appear to be located in five or more judicial districts, according to publicly available Whois records and IP address geolocation. These districts include, but are not limited to, the following: Southern District of Texas, District of Massachusetts, Northern District of Illinois, Southern District of Ohio, District of Idaho, Western District of Louisiana, Northern District of Iowa and Northern District of Georgia.

20. This warrant authorizes the United States to seize and copy from Microsoft Exchange Servers located in the United States the web shells identified in Attachment A, and to delete the web shells from those servers. As described above, in addition to identifying the Microsoft Exchange Servers, [redacted] The United States therefore has the technical ability to uninstall the web shells by using those passwords. Using the example described above, FBI personnel will access the web shells, enter passwords, make an evidentiary copy of the web shell, and then issue a command through each of the approximately [redacted] web shells to the servers to delete the web shells themselves. The following is an example of one of the delete commands that will be sent through the web shell (anonymized) located at https://webmail.[domain][.]net/aspnet_client/system_web/ [redacted].aspx: del /f “C:\inetpub\wwwroot\aspnet_client\system_web\[redacted].aspx. The

filename, [redacted].aspx, will vary based on the web shell filename. When conducted through an internal FBI testing process, this command successfully deleted the web shell from an FBI server and did not impact other files or services of the computer. An FBI technical evaluation of the code and a related briefing to an outside expert was also conducted to ensure the code would not adversely affect the victim computers and Microsoft Exchange Server software running on such computers.

TIME AND MANNER OF EXECUTION

21. I request that the Court authorize the government to access the relevant victim computers running Microsoft Exchange Server software located in the United States for a period of fourteen days, beginning on or about April 9, 2021.

22. Because accessing such computers at all times will allow the government to minimize the likelihood of the actors' detection and deployment of countermeasures that could frustrate the authorized search, good cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING AND DELAYED NOTICE

23. Based on my training and experience and my investigation of this matter, I believe that reasonable cause exists to seal this application and warrant, as well as the return to the warrant, and to delay the service of the warrant as normally required until thirty days after execution of the warrant. Pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), delayed notice of the execution of a search warrant is permitted if three requirements are satisfied: (1) the Court finds reasonable cause to believe that providing immediate notification may have an adverse result, as defined in 18 U.S.C. § 2705; (2) the warrant does not allow the seizure of tangible property, wire or electronic communication, or stored wire or electronic information (unless the Court finds reasonable necessity for the seizure); and (3) the warrant provides for the giving of

such notice within a reasonable period after execution, not to exceed 30 days unless the facts of the case justify a longer period. 18 U.S.C. § 3103a(b)(1)-(3). An "adverse result" includes endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, witness intimidation, or "otherwise seriously jeopardizing an investigation." 18 U.S.C. § 2705(a)(2)(A)-(E).

24. The requirements of Rule 41(f)(3) and § 3103a(b) are met in this case, specifically with regard to destruction or tampering of evidence and otherwise seriously jeopardizing the investigation, until the FBI has completed its operation. 18 U.S.C. § 2705(a)(2)(C), (E). Thus, reasonable cause exists to seal this application and warrant, as well as the return to the warrant, and to delay the service of the warrant as normally required until thirty days after execution of the warrant.

25. Based upon the information provided in this Affidavit, my training and experience, and discussions with other Special Agents of the FBI, allowing premature disclosure to the public at large or to individual victim users of web shell-compromised Microsoft Exchange Servers would likely seriously jeopardize the ongoing investigation. Such a disclosure, for example, may give the subjects of this investigation an opportunity to destroy or tamper with evidence or change patterns of behavior. Disclosure also could prompt the subjects to make changes to the web shells before FBI personnel can act pursuant to the requested warrant, which would enable persistent access, further exploitation of the victims, and defeat the efforts of FBI personnel to identify victims and delete web shells.

26. As this warrant seeks delayed notice pursuant to Title 18, United States Code, Section 3103a, it does not seek authorization to seize any tangible property. In addition to delaying notice, pursuant to Title 18, United States Code, Section 3103a(b)(2), reasonable necessity exists

to seize stored electronic information (i.e., web shells) found on the Microsoft Exchange Servers and identified in Attachment A.

27. Accordingly, the United States requests approval from the Court to delay notification until May 9, 2021, 30 days from the first possible date of execution on April 9, 2021, or until the FBI determines that there is no longer need for delayed notice, whichever is sooner. See 18 U.S.C. § 3013a(b)(3) (limiting initial delayed notice to a "reasonable period not to exceed 30 days after the date of its execution," absent a later date certain).

28. While the United States seeks authorization to delay notice, during the period of delayed notice the United States may still seek to notify individual victims or to disclose information obtained as a result of the requested warrant to one or more victims or to private entities or foreign authorities for purposes of mitigating the effects of any computer intrusion or assisting in maintaining the security of computers or networks during the authorized period of delayed notice.

29. When notice is no longer delayed, the United States intends, pursuant to Rule 41(f)(1)(C), to provide notice through a combination of email messages and publication. Federal Rule of Criminal Procedure 41(f)(1)(C) provides the following regarding the means of providing notice of the warrant and receipt:

> For a warrant to use remote access to search electronic storage media and seize or copy electronically stored information, the officer must make reasonable efforts to serve a copy of the warrant and receipt on the person whose property was searched or who possessed the information that was seized or copied. Service may be accomplished by any means, including electronic means, reasonably calculated to reach that person.

30. For those victims whose publicly available Whois records contain contact information, FBI personnel will send an email message from an official FBI email account (@FBI.gov) notifying such a victim of the search. For those victims who use a domain registration

privacy service or whose contact information is not otherwise publicly available, the FBI will send an email message from an official FBI email account to the privacy service or to the provider hosting the victim's domain asking them to provide notice to the client. If none of the above options are available, the FBI will provide notice to the Internet Service Provider (ISP) that hosts the IP address for the victim asking it to provide notice to the client. For each of these email messages, the FBI will attach a copy of the requested warrant and receipt. Finally, the FBI will issue a public notice on its official website (www.fbi.gov) that the FBI conducted the operation to further alert the victims. The Department will issue a similar notice on its official website (www.justice.gov). I believe that this combination of methods is reasonably calculated to reach those persons entitled to service of a copy of the warrant and receipts.

CONCLUSION

31. I submit that this affidavit supports probable cause for a warrant to use remote access to search electronic storage media described in Attachment A and to seize or copy electronically stored information described in Attachment B.

Respectfully submitted,

[redacted]

Special Agent
Federal Bureau of Investigation

Dated: April 9 7, 2021

Subscribed and sworn to me by telephone on 4/9/21, 2021

United States Magistrate Judge

TRUE COPY I CERTIFY ATTEST:
NATHAN OCHSNER, Clerk of Court
By
Deputy Clerk

ATTACHMENT A
PROPERTY TO BE SEARCHED

This warrant applies to Microsoft Exchange Servers located in the United States onto which are installed web shells, identified by the shell paths listed below:

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

Remaining pages of Attachment A are redacted in their entirety

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

This warrant authorizes the use of remote access techniques to search the electronic storage media identified in Attachment A and to seize and copy from the electronic storage media identified in Attachment A the web shells, used by actors to communicate with and distribute files to victim computers to infect them with malware, as evidence and/or instrumentalities of the computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy). This authorization includes the use of remote access techniques to access the web shells and issue commands through the web shells to the software running on the electronic storage media to delete the web shells themselves.

This warrant does not authorize the seizure of any tangible property. Except as provided above, this warrant does not authorize the seizure or copying of any content from the electronic storage media identified in Attachment A or the alteration of the functionality of the electronic storage media identified in Attachment A.

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

Sealed
Public and unofficial staff access to this instrument are prohibited by court order.

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

CERTAIN MICROSOFT EXCHANGE SERVERS INFECTED WITH WEB SHELLS

Case No. 4:21mJ755

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the ____________ District of Multiple
(identify the person or describe the property to be searched and give its location):

See Attachment "A"

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment "B"

YOU ARE COMMANDED to execute this warrant on or before ____________ *(not to exceed 14 days)*

□ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Peter Bray.
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☑ for 30 days *(not to exceed 30)* □ until, the facts justifying, the later specific date of ____________.

Date and time issued: 4/9/21 @ 4:13pm

Judge's signature

City and state: Houston, Texas

Peter Bray, United States Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: ____________________

____
Executing officer's signature

____
Printed name and title

ATTACHMENT A
Property to Be Searched

This warrant applies to Microsoft Exchange Servers located in the United States onto which are installed web shells, identified by the shell paths listed below:

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

https://[redacted]/aspnet_client/system_web/[redacted].aspx

Remaining pages of Attachment A are redacted in their entirety

ATTACHMENT B
PARTICULAR THINGS TO BE SEIZED

This warrant authorizes the use of remote access techniques to search the electronic storage media identified in Attachment A and to seize and copy from the electronic storage media identified in Attachment A the web shells, used by actors to communicate with and distribute files to victim computers to infect them with malware, as evidence and/or instrumentalities of the computer fraud and conspiracy in violation of Title 18, United States Code, Sections 1030(a)(2) (theft from a protected computer), 1030(a)(5)(A) (damage to a protected computer) and 371 (conspiracy). This authorization includes the use of remote access techniques to access the web shells and issue commands through the web shells to the software running on the electronic storage media to delete the web shells themselves.

This warrant does not authorize the seizure of any tangible property. Except as provided above, this warrant does not authorize the seizure or copying of any content from the electronic storage media identified in Attachment A or the alteration of the functionality of the electronic storage media identified in Attachment A.