AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Middle District of Florida

United States of America
v.

Michael Scheuer

Defendant(s)

Case No. 6:24-mj- 2118

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of 6/12/24, through 9/23/24 in the county of Orange in the Middle District of Florida, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B)	Knowingly causing the transmission of a program, information, code, or command to a protected computer and intentionally causing damage without authorization in excess of $5,000

This criminal complaint is based on these facts:

See affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Special Agent Timothy Callinan

Printed name and title

Sworn to before me over the telephone or other reliable electronic means and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: 10/23/2024

Judge's signature

City and state: Orlando, Florida

Daniel C. Irick, U.S. Magistrate Judge

Printed name and title

STATE OF FLORIDA **Case No. 6:24-mj-** 2118

COUNTY OF ORANGE

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Timothy Callinan, being duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed with the FBI since March 2018. I am presently assigned to the Orlando Resident Agency of the FBI's Tampa Field Office, where my duties include investigating cybercrime, organized crime, and other major federal violations. I have received training in cyber investigations and criminal enterprise organizations, including in-service training sponsored by the FBI and on-the-job training. I have participated in complex investigations in which federal grand jury subpoenas and court orders were used, as well as participated in the execution of numerous search warrants. I am also in regular contact with law enforcement personnel who specialize in cybercrime and criminal enterprises. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute search warrants issued under the authority of the United States.

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of a criminal complaint against **MICHAEL SCHEUER** ("**SCHEUER**") for a violation of 18 U.S.C. § 1030 (computer fraud). As set forth in more detail below, I believe there is probable cause to believe

that **SCHEUER** knowingly and without authorization caused the transmission of a program, information, code, or command to a protected computer and intentionally caused damage.

3. As also discussed below, there is evidence supporting the exigent arrest of **SCHEUER**. Namely, cellphone data analysis and video footage has shown **SCHEUER** visiting the personal residence of a victim of his denial-of-service attack. His visiting of this victim's residence occurred after hours and following the execution of a search warrant on **SCHEUER**'s residence, seizure of his computers, and notification from Google of the execution of a search warrant on his Google account. Further, analysis of **SCHEUER**'s computers has shown that he maintained a "dox" folder and personal identifiable information for the victims of his denial-of-service attacks. There is probable cause to believe that **SCHEUER** is actively a danger to one or more of the victims of his denial-of-service attacks.

4. Because this affidavit is provided for the limited purpose of establishing probable cause for a criminal complaint, I have not included every fact or facet of the investigation known to me. Rather, this affidavit sets forth those facts necessary to establish the requisite foundation for the criminal complaint against **SCHEUER**. I am familiar with the following facts based upon my personal involvement, as well as information I have obtained from other law-enforcement agencies, regulatory bodies, and open-source materials, including news reports and reports from civilian cybersecurity research firms.

INVESTIGATION

Background and Overview of the Cyber Intrusions

5. On July 9, 2024, a media and entertainment company operating in the Middle District of Florida ("Company A") was made aware of issues with an online program used to create menus (hereinafter referred to as "Menu Creator"). This affidavit omits the actual name of the program, as it is proprietary to Company A.

6. By way of background, Menu Creator is a product of a third-party vendor, Company B, based out of Minnesota but with an office located in the Middle District of Florida, and is used to create menus that are distributed to the portfolio of restaurants operated by Company A. Menu Creator also has several other functionalities, such as pricing, menu management, and inventory management. Company B developed Menu Creator specifically for Company A, and as a result, Company A is the only user of the Menu Creator product.

7. Company A determined that the issues with Menu Creator resulted from unauthorized computer intrusions and deployed an internal incident response team ("IR") to investigate the unauthorized computer intrusions and denial-of-service attacks, described in further detail later in this affidavit. Initial interviews of the individuals who reported the issues to the IR team identified a recently terminated employee, **SCHEUER**, as potentially responsible for the attacks.

8. **SCHEUER**'s job title was "Menu Production Manager," and he was terminated from Company A on or about June 13, 2024, for what was described as

misconduct. According to Company A, **SCHEUER**'s firing was contentious and was not considered to be amicable.

9. Company A provided the FBI with basic identifiers of **SCHEUER** to include his personal email address that was listed in his employment documentation: mjscheue@gmail.com.

10. As part of his job duties, **SCHEUER** was responsible for the creation and publishing of menus for the entire restaurant portfolio of Company A, utilizing Menu Creator and Company A's secure file transfer protocol ("SFTP") servers. Further interviews of Company A employees revealed that **SCHEUER** had intimate knowledge of the system architecture, the menu processing workflow, and potential vulnerabilities within the system. Only employees in **SCHEUER**'s position or a position similar to **SCHEUER** would have the accesses and knowledge to carry out the attacks described below in the manner in which they were carried out.

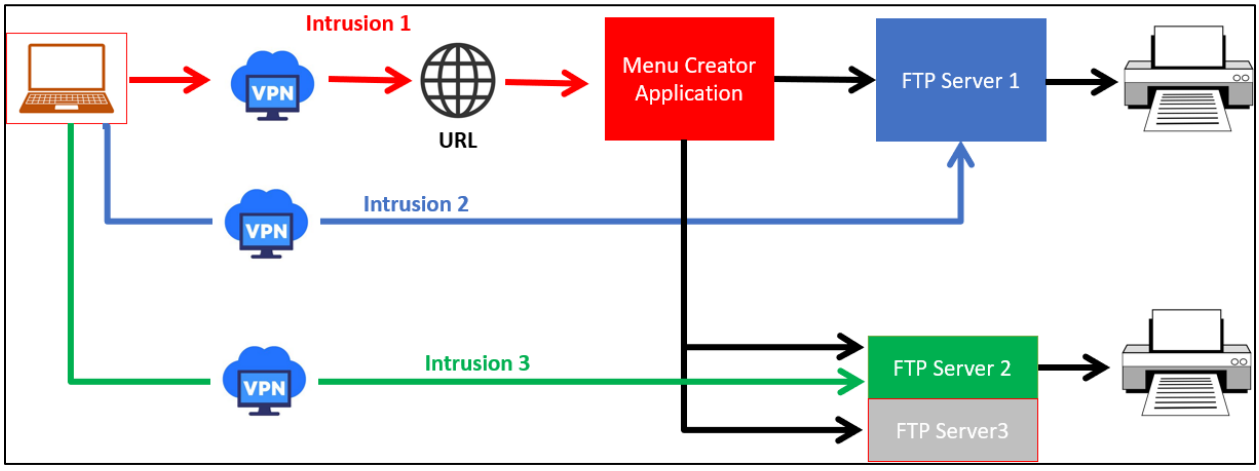
11. Over a period of approximately three months, Company A was the victim of multiple computer intrusions into servers associated with the Menu Creator program. The threat actor manipulated the menus of restaurants owned and operated by Company A. Some of the changes, such as changes to prices and adding profanity to the menus, were more benign.

12. However, the threat actor also made several menu changes that threatened public health and safety. Namely, the threat actor manipulated the allergen information on menus by adding information to some allergen notifications that

indicated certain menu items were safe for individuals with peanut allergies, when in fact they could be deadly to those with peanut allergies.

13. In addition, the threat actor also conducted attacks aimed to disable certain accounts by launching denial-of-service attacks against them. All of these attacks will be described in further detail later in this affidavit.

14. The chart below is meant to act as a summary of the intrusions believed to have been conducted by **SCHEUER**. The laptop image on the far left is not specifically referencing a "laptop" but rather a client device, which could be either a laptop, desktop computer, or tablet. Upon his termination, **SCHEUER** returned his Company A laptop, and it is therefore believed that **SCHEUER** was using his personal computer to conduct the attacks. As discussed, these attacks are sophisticated in nature, and investigators do not believe that **SCHEUER** used mobile devices to carry out the attacks. The red lines represent the path used in Intrusion 1, the blue represent Intrusion 2, and the green are Intrusion 3. The black lines indicate the connection functionality of the Menu Creator system:



Search of Scheuer's Residence

15. On September 23, 2024, pursuant to a federal search warrant (Case No. 6:24-mj-1995) ("Residence Search Warrant"), the FBI searched the residence of **SCHEUER** for evidence related to the intrusions discussed later in this affidavit. **SCHEUER** denied any involvement or wrongdoing in the activities described. Further, **SCHEUER** alleged that Company A was attempting to frame him because they were worried about him and the conditions under which he was terminated. **SCHEUER** stated that he was surprised to see the FBI but that he would not have been surprised if the Sheriff's office came to visit him to ask him to cease and desist with sending emails that could possibly be perceived as threatening.

16. **SCHEUER** admitted he used his personal Google Chrome profile to conduct activities related to Company A while he was employed there. **SCHEUER** was unable to definitively say if he accessed Company A systems after his termination because he believed he may have accessed Company A systems to obtain things like paystubs and other financial information.

17. During the execution of the search warrant, a total of 4 personal computers were seized and have been, or are in the process of being, imaged for analysis. The computers that were powered on at the time of the search were confirmed to have the "Mullvad" application installed. Mullvad is a virtual private network ("VPN") and was the same VPN that was used in one or more of the intrusions. A VPN conceals information related to its users by encrypting their data and masking

their IP addresses. This hides their browsing activity, identity, and location, allowing for greater privacy and autonomy. While VPNs serve many legitimate purposes, they are often used by threat actors to hide the location from which they are operating.

Intrusion 1 - Menu Creator

18. Upon being made aware of the issues with Menu Creator, Company A initiated an internal investigation into the cyber-attack and discovered there were several changes made to Menu Creator that impacted the integrity of the system. More specifically, employees of Company A noticed that all of the fonts in the application had been replaced by fonts that depicted symbols, also known as wingdings. The fonts were renamed by the threat actor to maintain the name of the original font, but the actual characters appeared as symbols. When launched, Menu Creator reached out to the configuration files to retrieve what it believed to be the correct font, instead, it retrieved the altered font files. As a result of this change, all of the menus within the database were unusable because the font changes propagated throughout the database. Further, this change was so substantial that it caused the Menu Creator system to become inoperable while the font changes were made to all of the menus. Company A was forced to take the Menu Creator application offline while they reverted to backups to regain the ability to operate. As a result of this attack, the Menu Creator system was impacted for a period of 1-2 weeks. Manual processes had to be implemented to account for the issues with Menu Creator.

19. Further research by Company A revealed that on July 3, 2024, the threat actor, later identified as **SCHEUER**, utilized an administrator account for Menu

Creator to create a new user account from IP address 146.70.187.158, which contained a fictitious name, Emily P. Beaman ("EPB"), described further below. The user agent string, which is a common logging field used to identify the type of browser a user is visiting from, indicated the user was accessing Menu Creator from a personal computer and using a Chrome web browser running Windows.

20. Logs from Company A revealed that an IP address used by the EPB account on the same date of the account creation was 146.70.187.158, which resolved to Mullvad. In the case of the credentials used for these intrusions (namely, Intrusions 1, 2, and 3), the credentials were non-individualized, not specific to a particular user, and available for use by multiple employees with administrative access. While **SCHEUER** knew these credentials as a result of his job responsibilities, upon his termination, he no longer had authorization to access the systems. **SCHEUER** was aware of this fact as noted by the creation of the fictitious EPB account to further his activities.

21. On July 4, 2024, one day after the creation of the EPB account, a user from the same IP address, 146.70.187.158, altered the font files which ultimately rendered the menus useless, forcing Company A to move to backups. Shortly thereafter, Company A implemented password resets on all Menu Creator accounts which ended the threat actor's ability to enter Menu Creator. The IP address used in this attack, while not the same exact IP, was from the same IP range **SCHEUER** had previously used to logon to his Company A email account and was also a Mullvad VPN IP address.

Intrusion 2 – SFTP Server 1 and Manipulation of Allergen Information

22. The next step in the menu workflow process was for the approved menus to be transferred to one of three SFTP servers[1] ("SFTP servers"), all owned and maintained by Company B. The SFTP servers each had their own specific purpose, but the overall functionality was to act as a print queue for items ready to be produced by Menu Creator. SFTP Server 1 was the server utilized as a print queue for projects to be printed by Company B. SFTP Server 1 was physically a separate server from SFTP Servers 2 and 3, which were on the same hardware. SFTP Server 2 will be discussed in more detail later in this affidavit as it was also utilized in another attack.

23. In order to access SFTP Server 1, the user would need to enter a valid username and password combination in order to be authenticated on the server. It is important to note that a menu cannot move directly from Menu Creator to Company B's printing process without being transferred to, and ultimately traversing through, SFTP Server 1. More specifically, the menus cannot be printed by Company B without first being added to the SFTP server. Additionally, while files typically come through the SFTP server via the Menu Creator system, it is also possible for files to be uploaded or downloaded directly from the SFTP server.

[1] An SFTP server is a computer software that facilitates the secure exchange of files over a network. It runs the file transfer protocol ("SFTP"), a standard communication protocol that establishes a secure connection between the devices in a client-server architecture and efficiently transmits data over the internet.

24. Company B investigated the logs associated with SFTP Server 1 and identified evidence there was an unauthorized intrusion into SFTP Server 1 after the forced password change on the Menu Creator application following Intrusion 1.

25. At or around the time of this intrusion, the actor utilized a valid set of credentials and downloaded a set of approved menus which were legitimately submitted from employees of Company A through Menu Creator and were waiting to be printed. Shortly thereafter, the actor uploaded altered menus to the SFTP server. After the menus were edited by the threat actor, they were re-uploaded to the SFTP server and, therefore, placed in the print queue.

26. On September 16, 2024, Company A identified menus that were printed from SFTP Server 1 with the altered allergen information and pricing changes. More specifically, the threat actor added notations to menu items indicating they were safe for people with specific allergies, which has potentially fatal consequences depending on the severity of the customers' allergies. It is believed these menus were identified and isolated by Company A prior to being shipped out to restaurants and were not distributed further.

Intrusion 3 – SFTP Server 2

27. SFTP Server 2 was used by Company A itself for printing projects (i.e., it was not for printing by Company B). This server was specifically used by Company A to print menus that would be displayed on large boards for viewing outside of the respective restaurant.

28. Company B investigated the logs associated with SFTP Server 2 and identified evidence there was an unauthorized intrusion into SFTP Server 2. To be authenticated on SFTP Server 2, the user would have needed to enter a valid username and password combination, different from that of SFTP Server 1; therefore, this is considered a separate intrusion.

29. It is important to note that a menu cannot move directly from Menu Creator to Company A's own printing process without being transferred to, and ultimately traversing through, SFTP Server 2.

30. Similar to Intrusion 2, the threat actor entered valid credentials and downloaded menus from SFTP Server 2, altered them locally, and uploaded them back to SFTP Server 2.

31. The alterations to these signs were specifically to QR codes, which should direct users to a digital version of the menu. In the altered versions, the threat actor changed the QR codes to direct the users to a miscellaneous website: boycott-israel.org.

32. The altered files were later printed by Company A. But after learning of the intrusion, the printed menus were identified and isolated prior to being shipped out to restaurants and were not distributed further.

33. According to Company A, a conservative estimate of damages caused by **SCHEUER** as a result of the above-mentioned attacks is at least $150,000. The efforts to remediate and ensure all impacted menus have been identified continues to the date of this affidavit.

Denial of Service Attacks – Ceased on September 23, 2024

34. Beginning on or about August 29, 2024, approximately 14 Company A employees were continually locked out of their enterprise accounts by a threat actor, later identified as **SCHEUER**. The threat actor attempted to continually logon to the victim accounts with incorrect passwords. Initially, the threat actor performed manual logon attempts, but shifted to a more sophisticated attack. More specifically, the threat actor developed a script to perform automated logon attempts, and as of the date of this affidavit, the threat actor had attempted over 100,000 logons to the victim accounts.

35. This attack was a form of a denial-of-service ("DoS") attack. Namely, the multiple incorrect logon attempts would cause an account to lockdown and thus render the corporate accounts unusable until the attacks subsided and the passwords could be reset. Because of the amount of traffic the threat actor was sending to the accounts of Company A, investigators do not believe this could be completed from a public internet location. Further, the sustained duration of the attack would indicate the threat actor was committing this attack from a personal computer and within his residence. As a result of the automation of the attacks, it is probable to believe that the threat actor procured a virtual server to commit these attacks.

36. FBI agents executed the Residence Search Warrant at approximately 12:41pm on September 23, 2024, according to body worn camera footage, and first contact with **SCHEUER** was at his front door at approximately 12:48pm. At the conclusion of the operation, representatives from Company A contacted the FBI and

informed them that the DoS attacks ceased at approximately 12:46pm. In other words, in the minutes leading up to his interaction with federal agents, **SCHEUER** ceased the attacks on Company A.

Identifying the Threat Actor

37. With regard to the two separate unauthorized intrusion attacks, IR noted several IP addresses originating from the Mullvad VPN. By using a VPN, the threat actor hoped to mask his location or home IP address.

38. IR compared the IP logs obtained from the unauthorized intrusion attacks to the internal Company A enterprise email logs and was able to identify that, on multiple occasions, **SCHEUER** accessed his Company A email account from Mullvad. Additionally, Company A provided logs that revealed that **SCHEUER** consistently, since at least October 2023, has accessed his company email from a Mullvad IP address or his home internet. Also on multiple occasions, **SCHEUER** accessed the same session from Mullvad, followed by Spectrum IP accounts. This fact pattern illustrates that **SCHEUER** not only uses Mullvad, but also the fact that he has used his home internet to access Company A networks.

39. In addition to **SCHEUER**'s unfavorable departure from Company A, the timing of the intrusions, and his specific expertise in the software and systems involved in the intrusions, the progression of the DoS attack also links the intrusions to **SCHEUER**. Namely, the DoS attack initially targeted employees involved in **SCHEUER**'s termination; it then progressed to his former, immediate co-workers; and

it then progressed to others. This targeting further narrows the scope of subjects believed to be responsible for the attacks and pinpoints **SCHEUER**.

ANALYSIS OF DATA FROM RESIDENCE SEARCH WARRANT

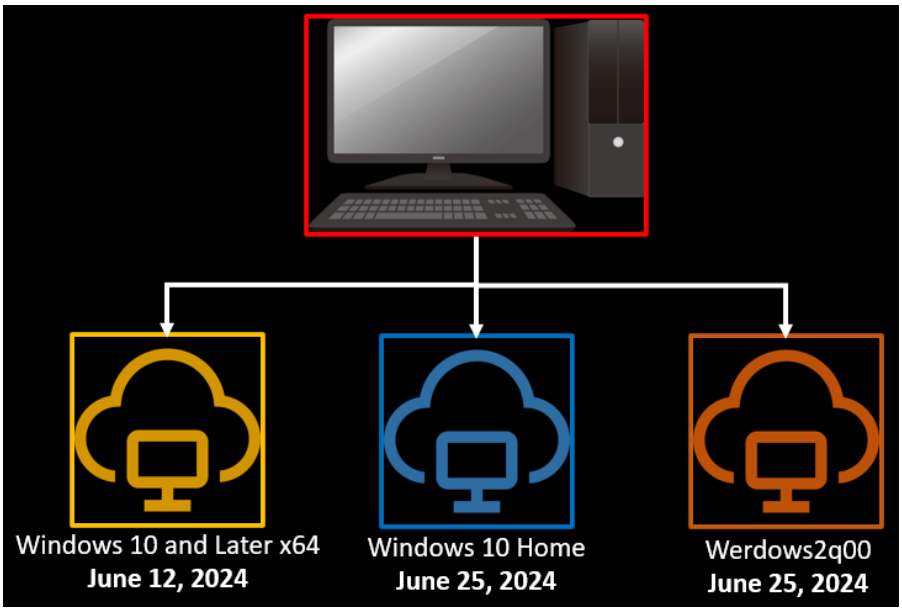
SCHEUER's Computer Setup

40. During the search, **SCHEUER** was interviewed by agents and several items were seized from his residence. **SCHEUER** acknowledged and knowingly executed an advice of rights, form FD-395, thus waiving his right to an attorney, and voluntarily provided information to agents. Of the items seized from the residence, there was a desktop computer located in an office space, which **SCHEUER** led agents to. **SCHEUER** was asked to unlock the computer, which he did. The password provided by **SCHEUER** to the agents was "f9ream," and he specified the password was all lowercase, which later proved to be false when agents attempted to image the computer. After review of a forensic image of the computer, agents discovered the correct password was "f9reAM."

41. Analysis of the forensic image revealed several virtual machines on the desktop computer. A virtual machine ("VM") is an image of operating system, which can be virtually launched within an application on the desktop computer; it is designed to create a layer of separation from the actual desktop and the virtual environment. More specifically, the virtual machine software, combined with the image of an

operating system, allows a user to operate another computer from within their physical computer.

42. In total, there were 3 relevant virtual environments located on the desktop computer that contained evidence of the crimes committed by **SCHEUER**. The following photo depicts the layout of the desktop and the VMs located within it. As the evidence for this investigation is scattered throughout the virtual environments, this will serve as the key for where specific pieces of evidence were recovered:

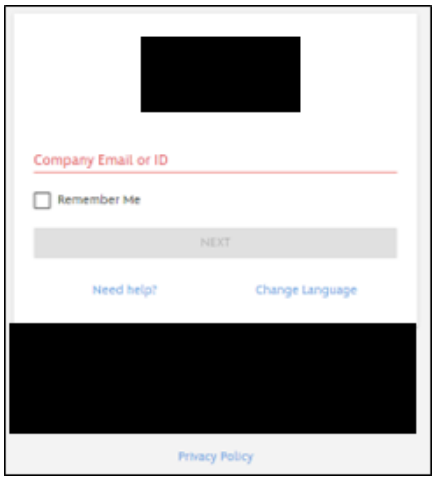


43. The desktop computer with the red box is the desktop computer seized from the residence of **SCHEUER**. The icons below each represent the virtual environments within the desktop computer. The first line of text under each VM represents the name given to the VM by **SCHEUER** and the second line is the date the virtual environment was created. The investigation has revealed that the main VM environment is the orange VM titled Werdows2q00. Even though these are virtual environments, all of the data still physically resides on the desktop computer.

Additional Denial of Service Attack Evidence

44. Beginning on or about August 29, 2024, Company A's cyber security team noticed repeated attempts to logon to MyID accounts of several employees at the URL wdpr.service-now.com.

45. Typically, when a company employee navigates to wdpr.service-now.com they are redirected to the MyID logon page, in order to access their company account, as pictured below:



46. As a result of repeatedly attempting to access the MyID accounts utilizing the wrong password, the accounts were locked out and the user would need to reset their password, therefore, denying the users ability to utilize the service. This is a common cyber security practice to prevent adversaries from attempting unauthorized access attacks utilizing a multitude of different techniques revolving around the guessing of a user's password. MyID is the system Company A uses for their employees to access email and other systems needed to carry out their specific job duties.

47. In total, 14 employees accounts were attacked in the DoS attacks. The targets of these attacks were listed below in order of the chronology of the DoS attacks:

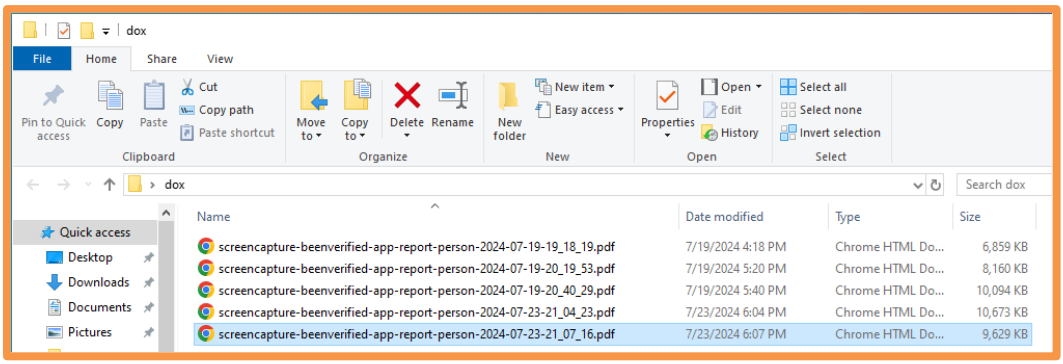
Targeted Users
Victim DP
Victim AG
Victim DH
Victim TS
Victim MB
Victim JV
Victim PW
Victim PT
Victim AM
Victim CS
Victim JK
Victim GH
Victim MS
Victim SP

48. A large majority of the individuals targeted had some type of interaction with **SCHEUER** or were considered to be upper-level management for Company A. More specifically, **SCHEUER** had a specific motive to attack these certain employees.

49. "Dox" folder. Located on the orange VM, **SCHEUER** had a folder on the desktop titled "dox."[2] Within this folder there are 5 files, which contained the personally identifiable information ("PII") of 4 individuals who were targeted by **SCHEUER** in the DoS attacks. This PII was within reports obtained from a third-party website. These reports contained phone numbers, email addresses, physical

[2] According to open-source research, a "dox" is a search for and identifying information on the internet about an individual, typically with the intent to use the information maliciously.

addresses, family members and relatives, jobs and education, social media, and asset information. More specifically, the files contained the PII for Victim DP, Victim AG, Victim DH, and Victim TS. These were also the first 4 individuals that the threat actor, **SCHEUER**, targeted in the DoS attacks. These files were first timestamped on the orange VM between July 19, 2024, and July 23, 2024. There was also a fifth individual for whom **SCHEUER** had a document who appeared to be a relative of Victim DP. A screenshot of the files in the dox folder was as follows:



50. With regard to carrying out the specific attacks, there were multiple evidentiary items located on the virtual machines. While a number of the items located are more technical in nature and speak to "how" **SCHEUER** conducted the DoS attacks, there were also several other pieces of evidence located that show that **SCHEUER** conducted the DoS attacks against the aforementioned individuals. More specifically, investigators located a picture on the orange VM that was captured during the creation of a "snapshot" on the orange VM. A snapshot images the VM at a particular point in time, or creates a "restore point," which a user can then later load to access the VM as it was at the time of the snapshot creation. Creating a snapshot

also captures a screenshot of the VM at the time of the snapshot, which is then displayed as a thumbnail to store the snapshot.

51. On or about September 1, 2024, **SCHEUER** created a snapshot on the orange VM, and a screenshot was also captured of the VM desktop at that moment in time. The screenshot shows **SCHEUER** had four logon screens visible in different Chrome browsers. In the "Company Email or ID" box, the email addresses for Victim AG, Victim DP, Victim DH, and Victim MB are visible. Each of the accounts have a "Your account has been locked out" banner above them. Across the taskbar located at the bottom of the screen for the orange VM there were several windows open including a Chrome browser titled "MenuPro" and a notepad file titled "dox.txt," which was similar to the dox file located on the desktop. The timestamp in the bottom right of the screen, which was captured in Pacific Time, was September 1, 2024, at approximately 6:54pm.

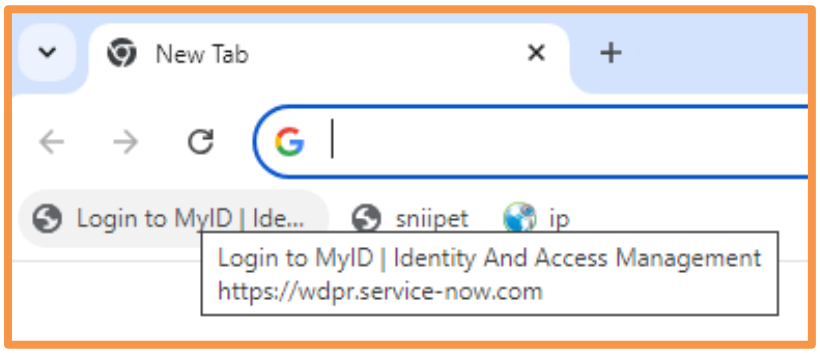
52. Company A provided logs in relation to the DoS attacks that **SCHEUER** was carrying out. On or about September 1, 2024, a single day, there were approximately 7,934 logons attempted against Company A. Below is a summary of all of the attacks for September 1, 2024:

Victim Accounts	Attempts
Victim DP	1,960
Victim MB	2,035
Victim DH	1,981
Victim AG	1,958
Total Attempts	**7,934**

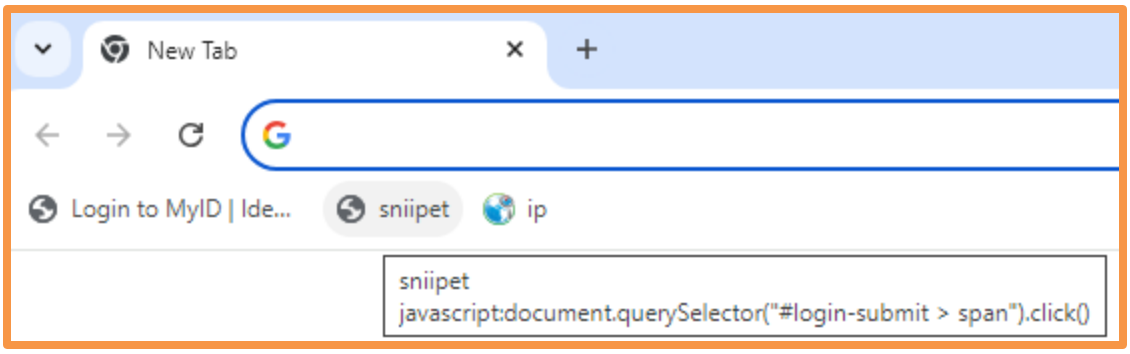
53. As noted in the table, the four accounts in the screenshot from the orange VM coincide with the logs provided by Company A. More importantly, on September 1, 2024, the only accounts attacked were the four depicted in the screenshot on the orange VM.

54. As previously mentioned, there were other technical pieces of evidence located on the orange VM that provided the details on how **SCHEUER** conducted the attacks. While not necessary to lay out in detail in this memo, the following screenshots and items were located on the orange VM and illustrate from a high level how **SCHEUER** automated the attacks.

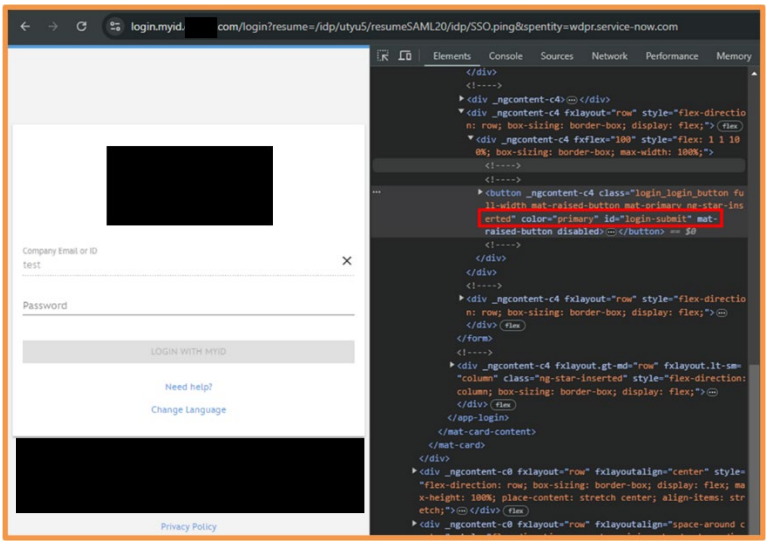
55. The first item identified on the orange VM was a "Favorite" located on the Chrome bookmark bar which directed to the above-mentioned Company A logon portal:



56. Next, there was an icon titled "sniipet," which when hovered over, was a piece of JavaScript code. When clicked, this icon directed the orange VM to locate and click on any object appearing on the screen named "login-submit" and would thus automatically begin clicking on Company A's login when displayed.



57. When navigating to the website referenced in the first bookmark via open source, it is possible to inspect the elements, or code, of the website. With this functionality users are able to identify the name associated with each of the elements that comprise a website. In the instance of Company A's MyID logon page, the logon button was named "login-submit" which was the same name as the JavaScript code above. A screenshot of the open-source research revealing the name of the login button was as follows:



Events during the night of October 22, 2024

58. On October 8, 2024, the FBI obtained a federal search warrant of **SCHEUER**'s Google account (Case No. 6:24-mj-2072). After service of the Google

Search Warrant on Google, Google then provided notification of the search to **SCHEUER** on October 22, 2024. After receiving notification from Google, **SCHEUER** then began emailing the undersigned FBI Special Agent. On one email (dated October 22, 2024), he stated "Please explain this to me." In another email (dated October 23, 2024), he stated "Adding Michelle [**SCHEUER**'s attorney]. Also Tim please add your [Company A] contact, this is taking to [sic] long … Please communicate."

59. Additionally, after receiving notification from Google, **SCHEUER** has been seen outside of at least one of the DoS victim's residences during the night.

60. Namely, on October 22, 2024, at approximately 10:45pm, what appeared to be a grey Kia Telluride arrived and parked in the front of the residence of Victim AG. An individual appearing to be **SCHEUER** exited the vehicle and approached the front door, which was being recorded via a Ring doorbell. **SCHEUER** then bends over and reads the label of a package that was on the doorstep. After reading the label, **SCHEUER** gives the Ring camera a thumbs up, exits the front porch, and returns to the vehicle. Victim AG was able to copy down a license plate number of "Y44ZQD" from the Kia Telluride. According to law enforcement databases, **SCHEUER** owns a grey 2022 Kia Telluride registered to him with the license plate "Y44ZDQ." The address belonging to Victim AG was listed in the documentation recovered from the computer of **SCHEUER**, indicating **SCHEUER** was aware of Victim AG's current address. Relevant images from the Ring doorbell footage show the following:

61. Either immediately following or during the incident, Victim AG contacted Company A to alert them about the presence of **SCHEUER** outside of his home after hours. Victim AG also forwarded the Ring doorbell footage to law enforcement.

62. Investigators have also analyzed cell-site data for **SCHEUER**'s cellphone, which pinpoints **SCHEUER** in Victim AG's neighborhood at the time of

the Ring doorbell footage, specifically entering the neighborhood at around 10:37pm and leaving at around 10:49pm.

63. As a result of the actions of **SCHEUER**, Victim AG left his residence and is currently staying at a hotel.

CONCLUSION

64. Based on the above facts and information, I submit that there is probable cause to believe that on or about June 12, 2024, through September 23, 2024, **SCHEUER** violated 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(B), specifically that he knowingly and without authorization caused the transmission of a program, information, code, or command to intentionally cause damage to a protected computer and caused loss to 1 or more persons during any 1-year period aggregating at least $5,000 in value.

This concludes my affidavit.

Timothy Callinan, Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me
as true and accurate via videoconference consistent
with Fed. R. Crim. P. 4.1 and 41(d)(3)
before me this 23rd day of October, 2024.

HONORABLE DANIEL C. IRICK
U.S. Magistrate Judge