AUSA Tom Peabody
AUSA Jennifer Chang
AUSA Ann Marie Ursini
Assistant Deputy Chief Adrienne L. Rose

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

| | |
|---|---|
| UNITED STATES OF AMERICA<br><br>v.<br><br>PETER STOKES<br>also known as "Bouquet," "Spencer," and "Jordan" | CASE NUMBER: 25 CR 812<br><br>**UNDER SEAL** |

**SUPERSEDING CRIMINAL COMPLAINT**

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

**Count One**

From in or around 2023 to in or around April 2026, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 371 | conspiring and agreeing with others known and unknown to defraud the United States and commit offenses against the United States, that is to: (a) intentionally access a computer without authorization and thereby obtain information from a protected computer, that is a computer used in a manner that affects interstate and foreign commerce, and the offense having been committed for private financial gain, in furtherance of any tortious act in violation of the Constitution and laws of the United States and of any State, and the value of the information obtained having exceeded $5,000, contrary to 18 U.S.C. § 1030(a)(2)(C) and (c)(2)(B); (b) knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, and cause loss to persons during a one-year period from the conspirators' course of conduct affecting protected computers aggregating at least $5,000 in value, and cause damage affecting 10 or more protected computers during a one-year period, contrary to 18 U.S.C. § 1030(a)(5)(A) and (c)(4)(A); and (c) knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and |

| | |
|---|---|
| | foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to 18 U.S.C. § 1030(a)(7)(B), (a)(7)(C), and (c)(3)(A). |

**Count Two**

From on or about May 12, 2025 to on or about May 15, 2025, at Mount Prospect, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §§ 1030(a)(2)(C), 1030(c)(2)(B) and 2 | intentionally accessing a computer without authorization and thereby obtaining information from a protected computer, for purposes of private financial gain, in furtherance of any criminal or tortious act in violation of the Constitution and laws of the United States and of any State, and the value of the information obtained having exceeded $5,000. |

**Count Three**

From on or about May 12, 2025 to on or about May 15, 2025, at Mount Prospect, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §§ 1030(a)(5)(A), 1030(c)(4)(A), and 2 | knowingly causing the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally causing damage without authorization to a protected computer, and causing loss to persons during a one-year period from the conspirators' course of conduct affecting protected computers aggregating at least $5,000 in value, and causing damage affecting 10 or more protected computers during a one-year period. |

**Count Four**

From on or about May 12, 2025 to on or about May 15, 2025, at Mount Prospect, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. §§ 1030(a)(7), 1030(c)(3)(A) and 2 | knowingly and with intent to extort from any person any money or other thing of value, transmitting in |

| | |
|---|---|
| | interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization and by exceeding authorized access, and a demand and request for money and other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion. |

**Count Five**

From in or around 2023 to in or around April 2026, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 1349 | knowingly and intentionally conspiring with others to devise and intend to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to 18 U.S.C. § 1343. |

**Count Six**

From on or about May 12, 2025 to on or about May 15, 2025, at Mount Prospect, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant violated:

| *Code Section* | *Offense Description* |
|---|---|
| 18 U.S.C. § 1343 and § 2 | knowingly and intentionally devised and intended to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds. |

Venue shall exist pursuant to 18 U.S.C. § 3238 and Fed. R. Crim. P. 18.

This superseding criminal complaint is based upon these facts:

X Continued on the attached sheet.

*Ali Sadiq* **w/p TPP**

ALI SADIQ
Special Agent, Federal Bureau of Investigation (FBI)

Pursuant to Fed. R. Crim. P. 4.1, this Superseding Complaint is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the Complaint and Affidavit by telephone.

Date: April 16, 2026

*Judge's signature*

City and state: Chicago, Illinois

Daniel P. McLaughlin, U.S. Magistrate Judge
*Printed name and title*

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF ILLINOIS

**AFFIDAVIT**

I, ALI SADIQ, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and I have been so employed for 10 years. My current responsibilities include the investigation of cybercrimes and violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, including hacking, computer intrusion, and related conspiracy offenses.

2. This affidavit is submitted in support of a superseding criminal complaint alleging that Peter STOKES has committed offenses in violation of 18 U.S.C. § 371 (conspiracy), §§ 1030(a)(2)(C), (c)(2)(B), (a)(5)(A), (c)(4)(A), (a)(7), and (c)(3)(A) (computer intrusion), § 1349 (wire-fraud conspiracy), § 1343 (wire fraud), and § 2 (aiding and abetting) (the "**Subject Offenses**"), as set forth in the complaint. The initial complaint, signed by the Court on December 22, 2025, is attached hereto as Exhibit A. As explained below, STOKES has been apprehended by Finland on the Court's first arrest warrant and extradition proceedings are now pending.

3. Because this affidavit is being submitted for the limited purpose of establishing probable cause in support of a criminal complaint charging STOKES with the **Subject Offenses** and search warrant applications for evidence, instrumentalities and fruits of the **Subject Offenses**, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts

that I believe establish probable cause to believe that the defendant committed the offenses alleged in the complaint.

4. This affidavit is based on my personal knowledge, my review of data and communications associated with this investigation, information provided to me by other law-enforcement agents and/or foreign governments, information provided by individuals with knowledge of pertinent facts, cyber experts, including those employed by the FBI, my training and experience, and the training and experience of other law-enforcement agents with whom I have consulted.

## CYBER DEFINITIONS

5. Based on my training officials with technical expertise, I know the terms described below have the following meanings or characteristics:

a. "Digital device," as used herein, includes the following three terms and their respective definitions:

i. A "computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. See 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

ii. "Digital storage media," as used herein, means any information storage device in which information is preserved in binary form and includes electrical, optical, and magnetic digital storage devices. Examples of digital storage media include, but are not limited to, compact disks, digital versatile disks ("DVDs"), USB flash drives, flash memory cards, and internal and external hard drives.

iii. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

iv. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security

software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

v. "Computer software" means digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

b. A "server" is a computer or operating system that provided resources, data, services, or programs to other computers (commonly referred to as "clients") over a network. There were many types of servers, including web servers that provide content to web browsers, email servers that act as a post office to send and receive email messages, print servers, virtual private servers, and proxy servers.

c. An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. There are two types of IP addresses, an IPv4 address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). An IPv6 is written as a group of eight hexadecimal numbers separated by a colon (e.g. 2001:0db8:ac10:fe01:6ab8:1c48:a95a:b1c2). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that

is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

e. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

f. "Cache" means the text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

g. "Cryptocurrency," "digital currency," or "virtual currency" is currency that exists only in digital form; it has the characteristics of traditional money, but it did not have a physical equivalent. Bitcoin ("BTC") is an example of cryptocurrency. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public and private keys can be printed or written on a piece of paper or other tangible object. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.

h. "VPN" means a virtual private network. A VPN extends a private network across public networks like the Internet. It enables a host computer to send and receive data across shared or public networks as if they were an integral part of a private network with all the functionality, security, and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The VPN connection across the Internet is technically a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from a private network-hence the name "virtual private network." The communication between two VPN endpoints is encrypted and usually cannot be intercepted by law enforcement.

i. Remote Desktop Protocol, or "RDP", is a protocol that enables users to remotely connect and control a computer from a different computer.

j. "Encryption" is the process of encoding messages or information in such a way that eavesdroppers or hackers cannot read it but authorized parties can. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any unintended party that can see the ciphertext should not be able to determine anything about the original message. An authorized party, however, is able to decode the ciphertext using a decryption algorithm that usually requires a secret decryption key, to which third parties do not have access.

k. "Malware," short for malicious (or malevolent) software, is software used or programmed by attackers to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It can appear in the form of code, scripts, active content, and other software. Malware is a general term used to refer to a variety of forms of hostile or intrusive software. Often it takes the form of "ransomware," meaning software employed onto a system, designed to block the owner's use of the system until a ransom amount, typically in the form of cryptocurrency, is paid to the wrongdoer.

l. "Social engineering" describes deceptive techniques designed to convince another person to reveal specific information or perform a specific action when the perpetrator would not otherwise have access to that information or action. Phishing was a type of social engineering technique.

**PROBABLE CAUSE**

6. In summary, the FBI is investigating the **Subject Offenses** as committed by a criminal cyber group known as "Scattered Spider," also known as "Octo Tempest." PETER STOKES, who has gone by the monikers "Bouquet" and "Jordan", and at relevant times resided in Estonia and the United Arab Emirates, is a member of Scattered Spider responsible for multiple computer intrusions in violation of the **Subject Offenses**.

7. As set forth below, criminal referrals from Microsoft, provider records, records from previous victim-company intrusions, and records from Subject Server 1 show that STOKES has engaged in the **Subject Offenses**. In addition, and more

specifically, STOKES and likely other coconspirators breached Company F, a luxury-jewelry retailer, exfiltrated data from Company F, and made a ransom demand of approximately $8 million in cryptocurrency, between on or about May 12 and on or about May 15, 2025. More specifically, according to records from providers, STOKES opened an account with a provider of a secure-tunneling, data-transfer tool used to access and exfiltrate data from Company F's computer network. STOKES created this account from a Virtual Private Network (VPN) proxy service IP address ending in .168. A Microsoft device identifier (a Global Device ID, or GDID, described below) associated with STOKES is linked to the .168 address.

## I. BACKGROUND ON PETER STOKES, A/K/A "BOUQUET" AND "JORDAN," AND SCATTERED SPIDER

8. The FBI is investigating a group of criminal cyber actors and their associates who are part of a group which gains access to victim companies' employee accounts through fraudulent pretenses, accesses victim companies' computers and networks without authorization, encrypts victim companies' data and/or exfiltrates that data to remote servers, extorts cryptocurrency from the victim companies in order for them to regain control over their computers and data and/or to prevent the dissemination of their data, and launders the illegally obtained funds. The group has been referred to as "Scattered Spider," "Octo Tempest," "UNC3944," and/or "0ktapus." It has targeted victims throughout the United States, including in the Chicagoland area, as well as Companies A through U (certain of which are discussed further below). Scattered Spider has been involved with over 100 network intrusions, resulting in more than approximately $100 million in ransom payments as well as

millions of dollars in damages to the victims.

9. PETER STOKES is a Scattered Spider member who has engaged in numerous intrusions, or assisted in them, including of Company H, Company F, and many others. According to State Department and other records, STOKES is a 19-year-old male who is a dual citizen of the United States and Estonia. During certain incidents described in this affidavit, STOKES lived in Tallinn, Estonia, and the United Arab Emirates, among potentially other locations. STOKES has used the online monikers "Bouquet" and "Jordan," among other names, based on, among other things, communications involving Scattered Spider members.

10. In addition, criminal referrals made by Microsoft implicate STOKES.[1] For example, in an October 2024 referral, Microsoft stated:

> Microsoft analysts have identified information about persona 'spencer'[2], a likely operator for Octo Tempest, and their associated accounts. Persona 'spencer' handles malware associated with Octo Tempest and has handled files associated with persona [Conspirator A's moniker]…. Persona 'spencer' is likely true name Peter Stokes, and probably lives in Tallinn, Estonia. Microsoft analysts have observed online services telemetry associated with persona

[1] Cybersecurity researchers at Microsoft, through the course of their job, have access to data, such as computer machine IDs, IP addresses, and malware samples associated with sophisticated cybergroups. The researchers' function is to identify groups of hackers who appear to operate as a team/cohesive unit (i.e., an Advanced Persistent Threat or APT group). The researchers do this by identifying malicious activity (malware attacks, spear-phishing, etc.) conducted against innocent victims, and then identify the computers used to conduct the attacks. The researchers then identify colleagues of the hacker by finding other computers also accessed from the same IP addresses used by the initially identified hacker. This process enables the source's organization to identify unique groups of hackers and then track those groups to determine new IP addresses the hackers are observed connecting to the Internet from, such as leased server IPs. This also allows the researchers to determine whether these IP addresses are being used to target victims. Microsoft's referrals and reports related to computer intrusions—such as the report about Subject Server 1—have been reliable. In fact, multiple, similar referrals from Microsoft in this and related investigations have been corroborated by later legal process issued by the government.

[2] "spencer" is Microsoft's internal pseudonym for the individual it associates as STOKES.

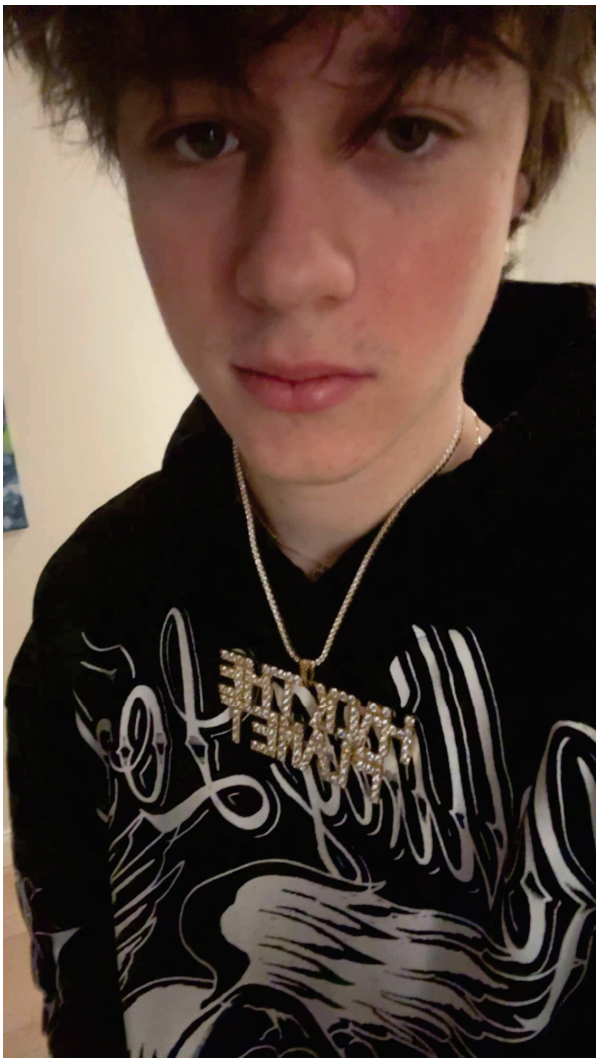
> 'spencer' that indicates likely involvement in dozens of recent Octo Tempest intrusions including those targeting critical infrastructure organizations in the US and UK and has likely been involved with Octo Tempest since 2022.

11. According to Snapchat records for the Subject Snapchat Account,[3] STOKES, in recent years, exhibited substantial wealth for a person his age, boasted about his international travel and wealth, and sent media regarding apprehended Scattered Spider members. For example, images from Facebook and Snapchat suggest Stokes traveled to Paris, Italy, Spain, Germany, New York, Florida, New Mexico, Thailand, and Dubai, and stayed in multiple luxury hotels, between 2024 and 2025, when STOKES was between about 17 and 18 years' old.[4] Much of this travel is confirmed by State Department travel records. See infra ¶ 28. Images from the Subject Snapchat Account also show STOKES possessing numerous watches and substantial cash, as well as apparently diamond-encrusted chains with the words "HACK THE PLANET,"[5] as depicted below.

[3] As reflected in Exhibit A, on December 22, 2025, this Court signed a search warrant for STOKES's Snapchat account with User ID be547f61-dabe-4b6c-867e-e06d07eee7af (the "Subject Snapchat Account"), as well as warrants for, among other facilities, two Apple accounts ("Subject Apple Account 1" and "Subject Apple Account 2" (collectively, "Subject Apple Accounts")) and a Facebook account ("Subject Facebook Account") believed to be used by STOKES, as set forth further in Exhibit A. Searches of the Subject Snapchat Account, Subject Apple Account 2, and the Subject Facebook Account confirmed STOKES's use of them, based on content, communications, and IP addresses, among other relevant information. Based on its search of Subject Apple Account 1, it appears to have been used by multiple individuals including STOKES.

[4] Based on his father's previous occupation as an executive in two major European businesses, STOKES's family appears to be well off.

[5] "Hack the planet!" is a famous line from the 1995 cyberpunk film *Hackers* about juvenile and young-adult computer hackers.



*STOKES in February 2025*[6]

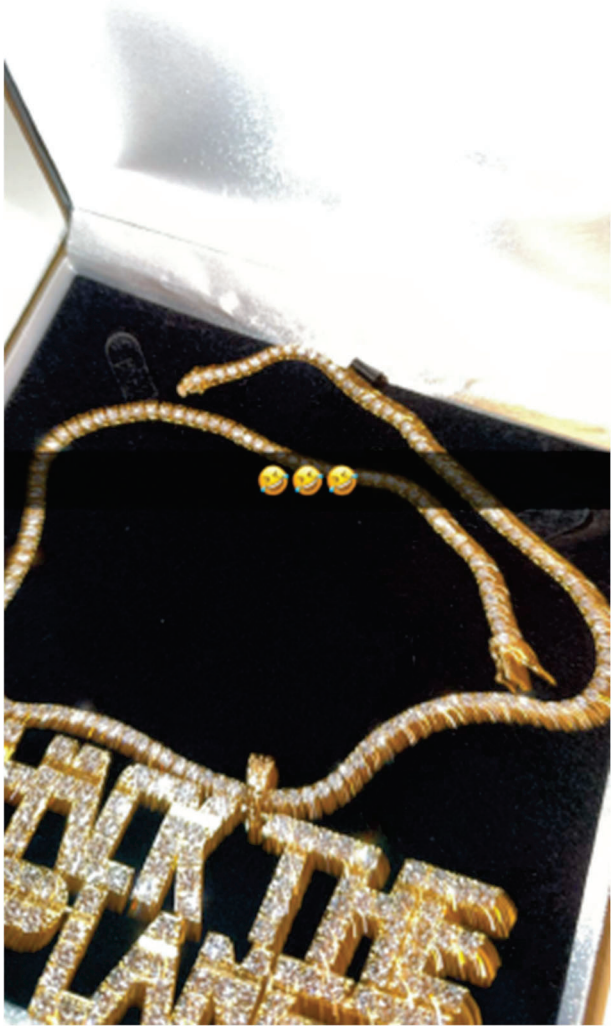


*Image sent by STOKES in December 2024*

12. Snapchat records for STOKES's Subject Snapchat Account show other indications of his involvement in the **Subject Offenses**. For example:

a. On or about March 16, 2025, STOKES sent the following image, depicting monikers associated with mafia characters from the show *Sopranos*. "Peter" is a known moniker for STOKES (and his first name); at least one of the other names

[6] I have identified STOKES in this photograph based on my familiarity with his appearance, through, among other things, review of his social-media accounts and based on a comparison to his U.S. passport photograph.

depicted is a known moniker for a Scattered Spider member, including "auth", Coconspirator A's moniker. Coconspirator A was a U.S.-based Scattered Spider member who, at the time of certain parts of the **Subject Offenses**, was a juvenile, and who has been criminally charged as such by local authorities following an FBI Chicago investigation.


b. On or about January 27, 2025, STOKES sent images of a Police station in Estonia, with the caption "Feel like raymond reddington season 1 episode 1 rn[.]" Raymond Reddington is a character from *The Blacklist*; in season 1, episode 1, Reddington turns himself into the FBI. STOKES later sent an image over the Subject Snapchat Account with the caption "Feds dont know what they just fumbled…"

c. On or about November 26, 2024, Snapchat user domr212, a suspected Scattered Spider member, sent STOKES a video of an individual, dubbed in the video as "Auth"—Coconspirator A—being chased by others, dubbed in the video

as “FBI agents.” The video ends with the caption “Guys he’s veracrypted gg….” Based on my training and experience, VeraCrypt is an open-source encryption software.


d. On or about November 17, 2024, domr212 sent STOKES an image of a computer showing failed login attempts with the caption “Fuck off FBI.”

e. On or about January 12, 2024, a Snapchat user sent STOKES an image of a screenshot containing the mugshot for Noah Michael Urban. Urban, or "Sosa" and "King Bob," was sentenced to a 120-month term of imprisonment in the Middle District of Florida for convictions for wire fraud and aggravated identity theft based on a SIM swapping scheme[7] and has been reported publicly as a member of Scattered Spider.[8] See No. 23-CR-180 (M.D. Fl.).

13. On or about April 10, 2026, STOKES was arrested in Finland attempting to board a flight to Japan, pursuant to an Interpol notice predicated on this Court's December 22, 2025 arrest warrant for STOKES. He is currently being held in custody pending extradition to the United States. When he was arrested in Finland, STOKES was in possession of, among other electronics, two two-terabyte hard drives.

## II. STOKES'S INVOLVEMENT IN SCATTERED SPIDER ATTACKS (Counts One and Five)

### A. Subject Server 1

14. On or December 22, 2025, the Court signed a search warrant for a storage device containing downloads from a Virtual Private Server ending in .191 ("Subject Server 1"), which Microsoft had identified as a facility used to further the **Subject Offenses**. See Ex. A at 51-55. As set forth below, the government's search

[7] SIM swapping a fraud by which wrongdoers gain access to a victim's cellphone, allowing them to, for example, access financial accounts and monitor multifactor authentication codes sent to the device.

[8] See, *e.g.*, SIM-Swapper, Scattered Spider Hacker Gets 10 Years, *KrebsonSecurity* (Aug. 20, 2025) (available at: https://krebsonsecurity.com/2025/08/sim-swapper-scattered-spider-hacker-gets-10-years/).

of Subject Server 1 showed STOKES's use of it to engage in the **Subject Offenses**. As noted in the initial affidavit in support of the complaint (Ex. A ¶ 69), based on my training and experience, it is very common for sophisticated cybercriminals, like STOKES and Scattered Spider members, to use dedicated servers to conduct the **Subject Offenses**, including, among other means, to engage in discussions with coconspirators over messaging or social-media applications, to store ransomed cryptocurrency, to conduct research into victim companies and employees, to launch ransomware attacks, and to exfiltrate data from victim companies.

15. Evidence from Subject Server 1 demonstrated its use in furtherance of **Subject Offenses**. For example:

a. Subject Server 1 contained exfiltrated records from multiple victim-companies, including Company F and Companies I through U. More specifically, on the C:, E:, F:, G:, and T: drives of Subject Server 1 were confidential, sensitive records for victim-companies. According to representatives of certain of these victim-companies, which were shown file names of files on Subject Server 1 that the FBI believed had been exfiltrated from the respective victim-company during a network intrusion, the victim-company representatives confirmed that the respective records were in fact theirs and exfiltrated during their respective network compromises. For instance, according to a Company Q representative, a U.S.-based insurance company, it experienced an unauthorized intrusion and exfiltration on or about June 7, 2025. Subject Server 1 contained, on its E: drive, in a folder titled "[first word of Company Q]" more than 250,000 files associated with Company Q. According

to a representative Company Q, the company estimated that its losses, including indirect losses, stemming from the incident are between $15 and $20 million. Likewise, according to Company S, it suffered an intrusion using social-engineering in June 2025. On Subject Server 1's E: drive, in a folder titled "[first word of Company S]," were more than 260,000 files associated with Company S. Representatives from Company Q and Company S each confirmed that the files found on Subject Server 1 were the files that were exfiltrated from each company during the respective intrusions.

b. A Telegram search bot, a malicious tool made to be accessible via the Telegram platform from certain Telegram user accounts and designed to allow a user to search apparent victim data on Subject Server 1, was discovered on Subject Server 1's E: drive.

c. Subject Server 1 contained virtual Android mobile devices, which had authentication mobile apps, including Okta and Azure Authenticator. Based on my training and experience, these apps are typically used for multifactor authentication. Several Scattered Spider intrusions have involved social engineering techniques to cause victim-account multifactor authentication codes to be sent to devices under their control. Based on my experience in the investigation, these applications allow the wrongdoers to use the multifactor authenticators they fraudulently obtain from victim companies to gain access to employees' credentials.

d. Subject Server 1 contained chats in a window titled "DragonForce," a known form of ransomware that operates as a ransomware-as-a-

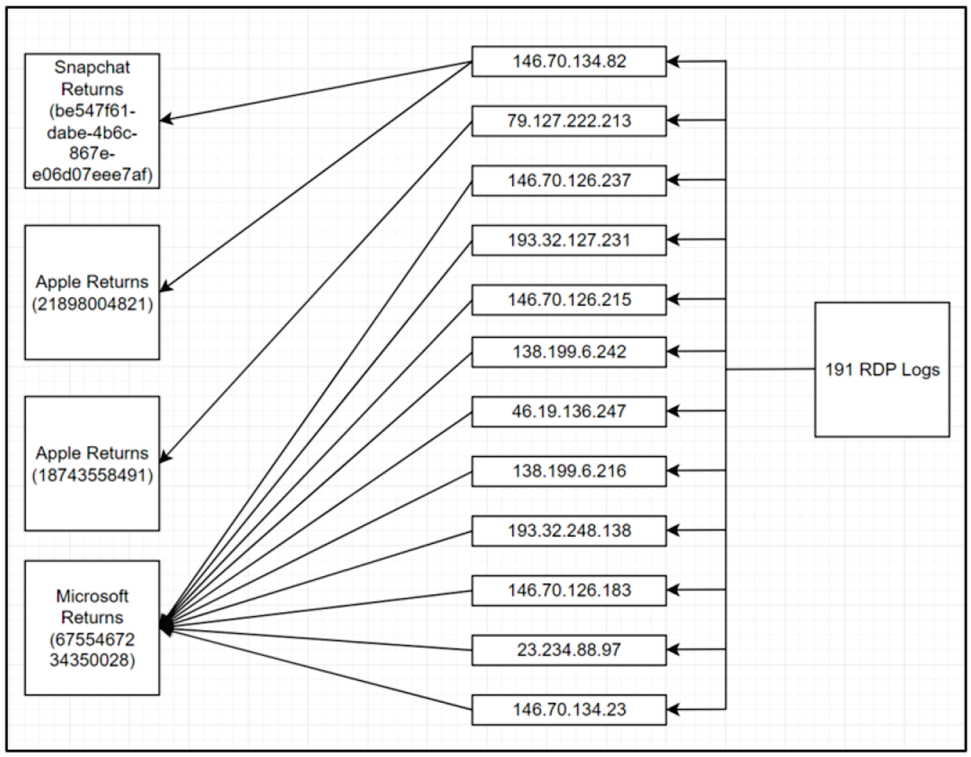
service (Raas) model. In the chats, one user asks "Brother are you going to charge us 500$E [ ] to make a new login after we made you over 1 million? seriously". Based on my role in the investigation, training, and experience, I believe that this message indicates a user of Subject Server 1 complaining about being required to purchase new credentials in order to log into ransomware infrastructure even after a successful ransomware attack.

16. Other evidence from Subject Server 1 also demonstrated STOKES's use of it to engage in the **Subject Offenses**. For example:

a. On December 2, 2025, at 12:48 p.m. Pacific Standard Time—which is approximately December 3, 2025, at 12:48 a.m. United Arab Emirates Time, and approximately December 2, 2025, at 10:48 p.m. Estonian Time—a user, believed to be STOKES, wrote "its my birthday g … and I got …. Good news … 1 confirmed bal … targs [targets] … turns out the db [database] … one of the dbs [databases] i got … has transaction data … of wires going to CB … and other exchanges and shit." According to State Department and Estonian records, STOKES's date of birth is December 3, 2006, and based on provider records.

b. RDP logs for Subject Server 1, which ends in .191, contain details about connections from other hosts to Subject Server 1 via the remote-desktop protocol. As explained above, RDP is a method by which a user can remotely connect to a different computer and operate it as if they were physically using that computer; it is frequently used by sophisticated cybercriminals to obfuscate their IP addresses and network infrastructure. A comparison of Subject Server 1's RDP logs with the

search-warrant return records related to Subject Apple Accounts and the Subject Snapchat Account, as well as Microsoft records related to two residential IP addresses used by STOKES,[9] show a time-based correlation between the IP addresses used to access those accounts and the IP addresses used to connect via RDP to Subject Server 1. The comparison looked at all RDP connections to Subject Server 1 and found several instances in which the same IP address was used to RDP to Subject Server 1 and access the accounts within a 24-hour window. That overlap, between August 2025 and May 2025, is depicted below.




[9] More specifically, on or about June 23, 2025, Chief Judge Virginia M. Kendall signed a reverse 18 U.S.C. § 2703(d) order for two Tallin, Estonia IP addresses believed to have been used by STOKES, based on Microsoft records. See 25 M 60220. Such an order required Microsoft, among other providers, to search for all accounts that may have used those Tallin IP addresses and provide associated IP addresses for the accounts that did. Microsoft returns from that order show additional IP addresses that were accessed by the underlying, true IP addresses, indicating STOKES's use of them.

Based on my training and experience, the IP overlap that is depicted above indicates that the individual using RDP into Subject Server 1 is the same individual that was controlling the Apple, Snapchat, and Microsoft accounts—known to be used by STOKES, as set forth in Exhibit A and elsewhere in this affidavit (see supra ¶¶ 11 n.3, 11-12 and infra at ¶ 28)—at particular times between August 2025 and May 2025.

**B. STOKES's Involvement in Company H Intrusion**

17. Evidence further shows that STOKES has been involved in earlier, Scattered Spider-attributed **Subject Offenses**. Specifically, Company H was the victim of a computer intrusion in March 2023. According to Company H, an online-communication platform, on or about March 29, 2023, a threat actor obtained a business partner's credentials and, using social engineering, contacted the company to request a resetting of the employee account's two-factor authentication. Through the attack, the threat actor gained access to Company H's internal resources and support systems, including support tickets submitted by Company H users and users' personally identifiable information. According to Company H, during the attack, Coconspirator A, who had a Company H account used two IP addresses that were also used by a threat actor, indicating that Coconspirator A was one of the threat actors.

18. Company H made a criminal referral to the FBI, which included communications between the suspected threat actors. Based on those communications, Coconspirator A, using a separate Company H username in his first

name, and STOKES, under the username "Bouquet,"[10] discussed and plotted the intrusion. For example, on or about March 30, 2023, shortly after the initial intrusion, between about 0:23 and 3:48 UTC, the two discussed the following[11]:

| | |
|---|---|
| STOKES | im in bed lmk if u need anything |
| Coconspirator A | ok |
| Coconspirator A | yo |
| Coconspirator A | accept vcm |
| Coconspirator A | vm [virtual machine[12]] |
| Coconspirator A | request |
| STOKES | yo |
| STOKES | accepted |
| STOKES | need anything? |
| Coconspirator A | n |
| STOKES | kk |
| Coconspirator A | yo |
| Coconspirator A | can i anydesk [a remote desktop application] |
| Coconspirator A | you |
| Coconspirator A | send code |
| Coconspirator A | i wanna search a [support] ticket |
| STOKES | yo |
| STOKES | send name |
| STOKES | ill search |
| …. | |
| Coconspirator A | lmk when ur out of shower |

[10] According to Company H's referral, the Bouquet account included two images, which, according to Company H, were purportedly of STOKES, which I have compared to STOKES's State Department passport photograph; they do not appear to be the same individual. In addition, however, the "Bouquet" account posted an image in or about January 2023, apparently of homework, with the name "Peter William Stokes" written in the top, right-hand corner. According to a referral provided by Microsoft on October 29, 2024, Microsoft analysts assessed the email address jordanspencer@riseup.net was used by STOKES. Also, as noted above, Coconspirator A confirmed to the FBI that STOKES used the moniker Bouquet.

[11] All bracketed content is based on my understanding of the messages, according to popular acronyms and my training and experience.

[12] A virtual machine (VM) is a software-based emulation of a physical computer that operates in an isolated environment on a host device. It is like a physical computer in that it runs its own operating system and applications independently. It is distinct, however, because it shares the hardware resources of a physical host rather than having its own dedicated physical components.

| | |
|---|---|
| Coconspirator A | ill anydesk it |
| STOKES | when out |
| STOKES | Why |
| Coconspirator A | cause I wanna look thru |
| STOKES | erm ok |
| ... | |
| Coconspirator A | How |
| Coconspirator A | do i search |
| Coconspirator A | Again |
| STOKES | Just |
| STOKES | put whatever |
| STOKES | ui want |
| STOKES | in that |
| STOKES | Search |
| STOKES | Thing |
| … | |
| STOKES | we can term |
| STOKES | any acount |
| STOKES | u got opps? [opposition] |
| ... | LOL |
| Coconspirator A | BRO |
| STOKES | like not term |
| STOKES | disable |
| STOKES | haha |
| Coconspirator A | BRO |
| Coconspirator A | HOW |
| Coconspirator A | SHOW ME |
| … | |
| STOKES | the db [database] is full of google urls |
| STOKES | lmfao |
| STOKES | look |
| Coconspirator A | oh |
| Coconspirator A | wtf |
| Coconspirator A | like |
| Coconspirator A | fake rpeorts |
| … | |
| Coconspirator A | let me try to disable |
| STOKES | wait |
| Coconspirator A | i got a user |
| Coconspirator A | and discrim |
| STOKES | idk |
| STOKES | send |
| STOKES | think uy need |

| | |
|---|---|
| Coconspirator A | ill put |
| STOKES | Email |
| Coconspirator A | in search |
| STOKES | Ok |
| STOKES | How |
| STOKES | did u get |
| STOKES | Advancedsearcghh |
| STOKES | Lmfao |
| Coconspirator A | advanced search |
| STOKES | U CAN SEARCH BY CREDIT CARD NUMBER |
| STOKES | LOL |
| Coconspirator A | Nah |
| Coconspirator A | Via |
| STOKES | Oh |
| STOKES | i thoguht it was VISA |
| STOKES | LMFAO |
| STOKES | Are |
| STOKES | u trying |
| STOKES | to term chris> |
| STOKES | ? |
| Coconspirator A | No |
| Coconspirator A | Haha |
| STOKES | Oh |
| STOKES | Haha |
| Coconspirator A | Should |
| Coconspirator A | i click |
| Coconspirator A | Disable |
| Coconspirator A | LOL |
| … | |
| STOKES | u have 30 mins before i kcik u off btw |
| Coconspirator A | Ok |
| STOKES | i gtg to school |
| Coconspirator A | Ok |
| STOKES | and let this shit dump |
| STOKES | Disable |
| STOKES | LM FAOL |
| Coconspirator A | Nah |
| STOKES | r u making |
| STOKES | disable API [application program interface]? |
| STOKES | LOL |
| … | |
| STOKES | idk if u can like disable any account |
| STOKES | they have to have ticket |

| | |
|---|---|
| STOKES | i think |
| … | |
| STOKES | go offline |
| STOKES | stop disabling |
| STOKES | Btw |
| STOKES | we dont want |
| STOKES | to lose access |
| STOKES | Etc |
| Coconspirator A | Nvm |
| Coconspirator A | dont work |
| STOKES | Arghhh |
| STOKES | we should stop disableing |
| STOKES | ppl |
| Coconspirator A | we should |
| Coconspirator A | not be talking on [abbreviation for Company H] |
| STOKES | tg [Telegram] |

19. Based on my training and experience and my role in this investigation, in this discussion, I believe STOKES and Coconspirator A were discussing Company H's network while they had unauthorized access to it. Specifically, the two discussed, among other things, STOKES gaining access to the network through a virtual machine, how to search for support tickets, disable user accounts, and the fact that they should not be having these discussions on Company H's platform.

## III. COMPANY F COMPUTER INTRUSION (Counts Two, Three, Four, and Six)[13]

20. As set forth below, STOKES was specifically responsible for a May 2025 computer intrusion at Company F. More specifically, between on or about May 12 and on or about May 15, 2025, Company F, a multibillion-dollar, luxury-item retailer, suffered a computer-network intrusion, resulting in the disruption of business

[13] The following information was provided in the government's initial complaint. See Ex A at 31-47. Subsection III.C. has been supplemented with information obtained from the search warrant executed on the Subject Snapchat Account.

operations and the exfiltration of company data. Provider records and IP logs show that STOKES created an account at a provider of a secure-tunneling, data-transfer tool and used that account to effectuate unauthorized access of and, in part, data exfiltration from the Company F network during the intrusion.

### A. Background on Company F Intrusion

21. Regarding the intrusion, according to a Company F representative and a review of Company F network logs:

a. The intrusion incident began on or about May 12, 2025, with several phishing calls[14] to the Company F informational-technology help desk made by one or more threat actors from two Google Voice[15] phone numbers, one ending in 8777 (the "8777 phone number") and one ending in 2742 (the "2742 phone number"). The threat actors pretended to be Company F employee-users and requested a reset of their authentication credentials, including the password and mobile device for multifactor authentication. Using this phishing technique, the threat actors compromised three Company F user accounts within approximately two to three hours.

b. Two of these compromised user accounts belonged to Company F IT administrators. These users had high-privilege user accounts associated with their

[14] These calls were not recorded by Company F, according to a Company F representative.

[15] Google Voice is a web-based VoIP (Voice over Internet Protocol) communication service that provides users with a U.S. phone number for voice calls, voicemail, and text messages. Google Voice is a service that is linked to and accessed from a Google account. When no longer required, a Google Voice number can be unlinked from a certain Google account and made available to be linked to other accounts.

standard user accounts. To access their high-privilege accounts, those users would have to authenticate their standard user accounts and then be assigned a temporary password for their high-privilege account. The threat actors thus obtained access to high-privilege accounts for these two IT administrator accounts by using their compromised standard user accounts.

c. The threat actors then used the high-privilege accounts to gain persistent access to the Company F platforms that control virtual servers and manage cloud computing. In May 2025, these platforms were housed in a Company F data center in New Jersey (the "Company F data center").

d. The threat actors conducted their malicious activity from several Company F virtual servers and virtual desktops in this datacenter. This included a virtual server with a name ending in VB0 (the "Company F server").

e. As part of their malicious activity, the threat actors used a service called ngrok to circumvent Company F network defenses and enable persistent unauthorized access to the Company F data center. According to ngrok, and based on my training and experience, ngrok is a service used by web developers and others to securely connect local servers to the Internet, allowing broader access to information or applications hosted on local servers.[16] These secure connections are sometimes

[16] According to ngrok and my training and experience, ngrok is used to create secure tunnels between an Internet-accessible ngrok endpoint (e.g., https://abc123.ngrok.io) and a service on a server in a local network (e.g., localhost:3000). This is achieved by running an ngrok agent on the local server. It allows external users to access the local service via the ngrok endpoint. Connection events are inbound network connections from users to an ngrok endpoint. Tunnel events are the ngrok agent's registration to receive connections for an endpoint. This includes

called “tunnels.”

f. More specifically, Company F server logs show that on or about May 12, 2025, threat actors downloaded, installed, and executed an ngrok agent—the program that creates a secure tunnel—on the Company F server. According to Company F, the ngrok agent had the authentication token[17] 2x0b1363KPV35LCUuZCkJag0G84_2btDjSM5oY82TQuiLZvaz (the “ngrok authentication token”). The logs further show that the Company F server established multiple tunnel connections with several ngrok servers. As described below, ngrok records for the account with the ngrok authentication token showed that the threat actors used these tunnel connections to transfer about 99.5 megabytes of data to the Company F data center and transfer about 1.27 gigabytes of data from the Company F data center. Based on my training and experience, this pattern of activity likely indicates initial steps by threat actors for establishing persistent unauthorized access to the Company F data center. This typically includes uploading malicious tools and utilities and downloading sensitive data to facilitate reconnaissance, credential theft, privilege escalation, and lateral movement.

g. The threat actors then used the Teleport.sh[18] utility and the

---

information about the ngrok agent, and the two points traffic is being transferred between (e.g., https://abc123.ngrok.io and localhost:3000).

[17] An ngrok authentication token is a unique identifier tied to a single ngrok account. It is used by the ngrok agent to verify the agent's identity to the ngrok cloud service and authorize the creation of secure network tunnels.

[18] Teleport.sh is a utility that can be used to provide secure remote access to servers. By establishing tunnels, it could be used by threat actors to enable persistent unauthorized access to a victim network while circumventing network perimeter defenses.

Amazon S3[19] online storage utility to exfiltrate large amounts of sensitive Company F data, including OneDrive[20] files belonging to Company F employee-users, Microsoft Active Directory[21] data, and Microsoft Operations Management Suite[22] data.

h. Between on or about May 12, 2025, and on or about May 15, 2025, the threat actors were able to maintain persistent access to the Company F network and, primarily using the Teleport.sh utility and the Amazon S3 online storage utility, exfiltrated at least 77 gigabytes of data, despite ongoing attempts by Company F security personnel to block the attack. According to a Company F representative, the threat actors had likely attempted to deploy ransomware on Company F servers but had been thwarted by the security personnel. On May 15, 2025, the threat actors sent a ransom note to several Company F personnel from a Company F email account they had compromised. The ransom note had the subject "IMPORTANT: WE STOLE THE DATA, CONTACT UMMEDIATELY [sic]." In the email, the threat actors claimed they had stolen 100 gigabytes of data "including raw card information and payment details," referring to credit card and related payment information, and threatened to publish the data unless Company F contacted them at a specified email address for

[19] Amazon Simple Storage Service (S3) is an online data storage service offered by Amazon Web Services (AWS). Amazon S3 users can create Internet-accessible endpoints, called buckets, to store and retrieve their data.

[20] In a Microsoft 365 enterprise environment, OneDrive is a user's personal cloud storage space, intended for private work files and drafts.

[21] Microsoft Active Directory is a directory service used to centrally manage users, computers, and other network resources within an organization's network.

[22] Microsoft Operations Management Suite is a collection of cloud-based services designed to manage and monitor both on-premises and cloud environments.

negotiations.

i. On or about May 16, 2025, after Company F security personnel were ultimately successful in evicting the threat actors from the Company F network, Company F contacted the threat actors' email address via third-party negotiators. Between on or about May 16, 2025, and on or about June 2, 2025, the negotiators communicated with the threat actors. During these communications, the threat actors provided samples of the data they had exfiltrated and stated they had cracked passwords belonging to Company F users. Eventually, on or about June 2, 2025, the threat actors sent a message stating "We are wanting to push things forward, after some consideration $8million seems like a good price. Let us know what you think."

j. Company F did not pay the ransom, and no further attempts were made to communicate with the threat actors. According to Company F, however, the losses due to business disruption, investigation, and mitigation were approximately $2 million, and further losses were expected.

### B. The Ngrok Account Was Used in the Company F Computer Intrusion

22. According to Company F event logs, on or about May 12, 2025, a compromised Company F administrator account was used to install an ngrok agent on the Company F server. According to Company F event logs and ngrok records, between on or about May 12, 2025, and on or about May 13, 2025, the ngrok account was used to facilitate unauthorized access to the Company F network and exfiltrate data from the Company F data center.

23. According to ngrok records, on or about May 12, 2025, at 19:21 UTC, an ngrok account with the ngrok authentication token was created and assigned Account ID ac_2x0b16MSTJk4PvjLZMoqt4vOvZM (the "ngrok account"). Also, according to ngrok records, the IP address of the user who created the ngrok account was 68.235.46.168. According to public IP records, the .168 IP address is assigned to a server hosted by Tzulo. According to Tzulo records, that server is in Mount Prospect, Illinois, and that IP address is assigned to a VPN proxy service. According to ngrok records, the ngrok account had five "connection events" and 12 "tunnel events" with the Company F server between on or about May 12 and on or about May 13, 2025—the dates of the intrusion. Accordingly, I believe the ngrok account was used by the threat actors to establish persistent unauthorized access to the Company F network, as described above.

24. According to Google records, on or about May 12, 2025, the Google account with the 8777 phone number—which was used in the phishing calls to Company F—was logged into from the .168 address, the same IP address used to create the ngrok account on the same date. Also, according to Google records, subscriber information for the Google account with the 2742 phone number—the second phone number used in the phishing calls to Company F—included the email address mykccncn109@gmail.com (the "Subject Google Account"). According to ngrok records, subscriber information for the ngrok account included the Subject Google Account. And according to Teleport records, the Subject Google Account is also included in the subscriber information for the Teleport.sh accounts used in the

exfiltration of Company F data. Based on this information, I believe the same threat actors used the 2742 phone number, the 8777 phone number, and the Subject Google Account to effectuate the Company F intrusion.

25. According to Microsoft records, the ngrok account was set up through Global Device Identifier g:6755467234350028 ("the GDID"). According to a Microsoft representative, a Global Device Identifier in the Windows ecosystem is a persistent, device-level identifier designed to uniquely identify an installation of a Windows operating system on a device, either a physical device (e.g., a mobile phone or laptop) or virtual machine, across certain Microsoft services and scenarios. A GDID is a globally unique identifier tied to the installation of Windows on a device. A GDID remains consistent across Windows operating system updates on a device, but a reinstall of Windows, either on the same device or on a different device, will be tied to a new unique GDID.[23]

26. According to Microsoft records, on or about May 12, 2025, at 19:21 UTC—when, according to ngrok records, the ngrok account was created—the device with the GDID accessed, among other ngrok pages, "https://dashboard.ngrok.com/signup," the ngrok page to set up an ngrok account.

27. Microsoft records also indicate: (1) the user of the device assigned the GDID accessed multiple sites from Tzulo servers in May 2025, including the .168 server (the IP address used to create the ngrok account) on May 12, 2025; and (2) the

[23] Thus, one Microsoft user could have multiple GDIDs.

user of the device assigned the GDID, on May 12, 2025 at 22:47 UTC, a little more than three hours after the ngrok account was created, the user visited "[Company F].com" from the .168 proxy server.

### C. STOKES's Involvement in the Company F Intrusion

28. As set forth below, there is probable cause that STOKES is the user of the device that set up the ngrok account used to commit the **Subject Offenses**. More specifically, the GDID assigned to the device that set up the ngrok account has common IP address activity with the Subject Accounts used by STOKES (as identified and described above and in Exhibit A):

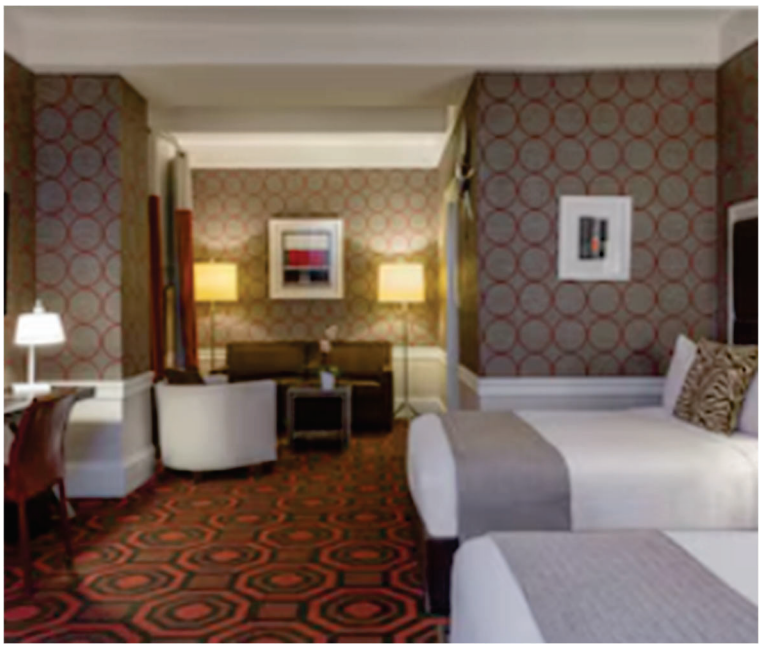
a. On June 4, 2024, at 2:01 PM UTC, the device with the GDID used the IP address 91.129.97.29, geolocated to Tallinn, Estonia, where STOKES lived. On the same date, this IP address was also used to access the Subject Facebook Account at 3:21 PM UTC and the Subject Snapchat Account at 1:57 PM UTC.

b. On November 18, 2024, at 7:31 AM UTC, the device with the GDID used the IP address 207.237.190.238, geolocated to New York, New York. On the same date, this IP address was also used to access Subject Apple Account 1 at 8:34 AM UTC and the Subject Snapchat Account at 3:22 PM UTC. The device with the GDID also used this IP address on November 17, 2024 at 9:21 PM UTC. According to State Department travel records, STOKES travelled to New York, New York from November 15, 2024, and November 18, 2024. Images from the Subject Snapchat Account confirm STOKES was in New York in November 2024, including between approximately November 16 and 18, 2024. These images include ones taken from the

Four Seasons Hotel New York and Waldorf Astoria New York, as well as images taken from a UFC fight that occurred in New York on November 16, 2024.

c. On November 26, 2024, the device with the GDID visited the URL empirehotelnyc.com. This is the website for a hotel named "Empire Hotel", located in New York, New York. According to State Department travel records, STOKES travelled from Frankfurt, Germany to New York, New York, on November 23, 2024, and returned to Frankfurt, Germany on November 29, 2024. On or about November 25, 2024, STOKES sent the image below via his Subject Snapchat Account. According to Empire Hotel New York's public website, the carpet, wallpaper, and furniture match an Empire Hotel suite, as depicted below.

*Image posted on Subject Snapchat Account on or about November 25, 2024*



*Publicly Advertised Empire Hotel Two-Bed Suite*

d. On February 2, 2025, at 2:37 PM UTC, the device with the GDID used the IP address 110.170.208.226, geolocated to Thailand. On the same date, this IP address was also used to access the Subject Snapchat Account at 7:21 PM UTC and the Subject Apple Account 1 at 9:28 AM UTC and Subject Apple Account 2 at 1:30 PM UTC. The device with the GDID also used this IP address on January 31, 2025, at 12:45 PM UTC. Confirming that STOKES was in Thailand around this time, on or about January 31, 2025, he sent an image holding a "WALDORF ASTORIA BANGKOK" water bottle; on or about February 1, 2025, he posted an image of himself captioned "WALDORF ASTORIA BANGKOK."

29. On January 8, 2025, the device with the GDID used the IP address 213.35.168.50[24], geolocated to Tallinn, Estonia, where STOKES lived, to visit the

[24] According to public IP records, this IP address is assigned to "Telia Eesti AS" a major

URL https://login.growtopiagame.com/player/login/dashboard?valKey=40db4045f2d8c572efe8c4a060605726. Based on my training and experience, this indicates the user logged into an online account for the game Growtopia.[25] According to records from Ubisoft, this login accessed a Ubisoft account with the account identifier ACC03E1B-D54F-4EC5-BA63-68276DFF16AD (the "Ubisoft account"). On January 7, 2025, the same IP address (IP Address 213.35.168.50) was used to access Subject Apple Account 2 at 5:17 AM UTC and the Ubisoft account two minutes later, at 5:19 AM UTC. Also, the same IP address was used to access the Subject Snapchat Account, the Subject Facebook Account, and the Subject Apple Accounts on several dates from May 31, 2024, through July 16, 2025.

30. Therefore, based on my training and experience, and overlapping use of the same IP addresses by accounts and devices used by STOKES, I believe that the user of the GDID (who, as discussed above, set up the ngrok account used in the Company F intrusion) is the same person as the user of the Subject Accounts (STOKES). In addition, as explained above, the Subject Google Account was used to set up the ngrok account used in the **Subject Offenses** and the Subject Google Account was also used to set up the 2742 phone number's account and the Teleport.sh accounts used in the attack. Based on my training and experience, this indicates that STOKES also operated the Subject Google Account used in the **Subject Offenses**.

---

national Internet service provider providing broadband, mobile services, and internet infrastructure within Estonia.

[25] Growtopia is a massive multiplayer online game available on the iOS, Android, Windows, and MacOS operating systems. It is owned by the gaming software company Ubisoft.

Finally, as noted above, at least 45 exfiltrated records from Company F (among hundreds of thousands of records from many other victim-companies) were found on Subject Server 1, which, as discussed above (supra ¶ 16), STOKES accessed and used.

**CONCLUSION**

31. For these reasons, I submit that there is probable cause to believe that Peter STOKES has violated the **Subject Offenses**.

FURTHER AFFIANT SAYETH NOT.

*Ali Sadiq* **w/p TPP**

ALI SADIQ
Special Agent, FBI

SWORN TO AND AFFIRMED by telephone April 16, 2026.

Honorable Daniel P. McLaughlin
United States Magistrate Judge