UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	**SEALED INDICTMENT**
- v. -	:	21 Cr.
NICKOLAS SHARP,	:	21 CRIM 714
Defendant.	:	

COUNT ONE

(Computer Fraud and Abuse – Intentionally Damaging Protected Computers)

The Grand Jury charges:

Relevant Persons and Entities

1. At all times relevant to this Indictment, Company-1 was a technology company headquartered in New York, New York, which manufactured and sold wireless communications products. Company-1's shares are traded on the New York Stock Exchange.

2. At all times relevant to this Indictment, NICKOLAS SHARP, the defendant, was a senior software engineer at Company-1, responsible for software development and cloud infrastructure security, among other things.

Overview of the Criminal Scheme

3. From at least in or about 2020, up to and including in or about 2021, NICKOLAS SHARP, the defendant, repeatedly

misused administrative access provided to him as an information technology employee to download gigabytes of Company-1's confidential data. During the course of this cybersecurity incident (the "Incident"), SHARP caused damage to Company-1's computer systems by altering log retention policies and other files, to conceal his unauthorized activity on the network. While working on a team remediating the effects of the Incident, SHARP sent a ransom note to Company-1, posing as an anonymous attacker who claimed to have obtained unauthorized access to Company-1's computer networks. The ransom note sought 50 Bitcoin, a cryptocurrency, which is the equivalent of approximately $1.9 million based on the prevailing exchange rate at the time, in exchange for the return of the stolen data and the identification of an existing "backdoor," or vulnerability to Company-1's computer systems. After Company-1 refused the demand, SHARP published a portion of the stolen files on a publicly accessible online platform. SHARP subsequently engaged in a media campaign to malign Company-1's response and disclosures related to the Incident, while concealing his own role, causing Company-1 to lose billions of dollars in market capitalization value.

Background

4. At all times relevant to this Indictment, Company-1 used multiple third-party providers to host its data and facilitate its product development. Company-1 maintained an account with Amazon Web Services ("AWS"), which was used to host server infrastructure and manage development of Company-1's new applications and products. The AWS infrastructure included servers that ran a portion of Company-1's operations and hosted certain of Company-1's system, code, and credentials.

5. At all times relevant to this Indictment, Company-1 also subscribed to services from a third-party company named GitHub, Inc. ("GitHub"), which is a provider of internet hosting for software development, developer collaboration, and version control. Through GitHub, Company-1 stored certain development files, as well as the history of changes to those files, in data structures called repositories. Developers employed by Company-1 had individualized accounts on GitHub which provided them with varying levels of access to various repositories hosting Company-1's code and development projects. Company-1 also maintained a high-level access account shared among a group of developers ("GitHub Account-

1"), which provided access to all or nearly all of Company-1's repositories on GitHub. User activity on GitHub is logged.

6. Keybase is an encrypted social networking service that permits users to, among other things, send private messages and files directly to other Keybase users and also to upload files that would be publicly available to any Keybase user.

7. A Virtual Private Network ("VPN") is an internet connection method used to add security and privacy to network connections. When a user connects to a VPN, it creates an encrypted tunnel between the user and a remote server operated by a VPN service. All of the user's internet traffic is encrypted and routed through this tunnel to the ultimate internet or web resource being accessed by the user. Because internet traffic exits the VPN server, the user's computer appears to have the IP address of said server, masking the IP address of the user's computer, and thus his identity and location.

8. Surfshark is a company headquartered in the British Virgin Islands that sells a commercial VPN service (the "Surfshark VPN") to the public, which, as described above, can effectively anonymize their users by replacing their personal

IP addresses with IP addresses operated by Surfshark through its servers.

The Cybersecurity Incident

9. NICKOLAS SHARP, the defendant, was employed by Company-1 from in or about August 2018 up to and including on or about April 1, 2021, including throughout the time period of the Incident in or about December 2020, and the ransom demand in January 2021. SHARP was a senior developer who had access to credentials for Company-1's GitHub and AWS servers.

10. On or about July 7, 2020, NICKOLAS SHARP, the defendant, used his personal Paypal, Inc. account to purchase a 27-month subscription to Surfshark VPN. SHARP downloaded Surfshark VPN on multiple devices, including his cell phone and laptop, and used the VPN service prior to the Incident.

11. At all times relevant to this Indictment, NICKOLAS SHARP, the defendant, resided at a residence in Portland, Oregon (the "Sharp Residence"). The internet connection from the Sharp Residence was associated with a specific Internet Protocol address at certain relevant times (the "Sharp IP").

12. On or about December 9, 2020, NICKOLAS SHARP, the defendant, applied for a position at a technology company based in California ("Company-2").

13. On or about December 10, 2020, at approximately 2:55 a.m. UTC,[1] and again at 3:16 a.m., NICKOLAS SHARP, the defendant, used his own Company-1 credentials to access a particular key (the "Key") on Company-1's infrastructure through AWS servers. The connection was made through the Sharp IP. The Key accessed by SHARP permitted the user to, among other things, obtain access to other credentials within Company-1's infrastructure and to run searches through that infrastructure.

14. Approximately two minutes later, on December 10, 2020, at approximately 3:18 a.m., an attacker connected to Company-1's AWS infrastructure using a masked IP provided by the Surfshark VPN. The attacker used the same Key accessed by NICKOLAS SHARP, the defendant, two minutes earlier to connect to AWS and to run a command "getcalleridentity." That command returns the username and account information for the AWS account for which it is run and can validate that the credential is usable.

15. On December 21, 2020, at approximately 9:58 p.m., NICKOLAS SHARP, the defendant, logged into Company-1's GitHub infrastructure via a web browser, using his own Company-1 work

[1] For consistency, unless otherwise noted, all times are in the UTC time zone.

credentials. SHARP logged in through his Sharp IP address, and viewed the names of certain repositories of data.

16. Approximately one minute later, on December 21, 2020, at approximately 9:59 p.m., NICKOLAS SHARP, the defendant, used the Surfshark VPN that masked his true IP address to connect into GitHub through SSH by using Company-1's high-level GitHub Account-1.[2] SHARP used the SSH connection to execute a series of commands to clone Company-1's repositories of data to SHARP's computer.

17. Although throughout the vast majority of the Incident, NICKOLAS SHARP, the defendant, successfully masked his true IP address through the Surfshark VPN, in one fleeting instance during the exfiltration of data, the SHARP IP address was logged making an SSH connection to use GitHub Account-1 to clone a repository. Between December 21, 2020 at approximately 11:47 p.m. and December 22, 2020 at approximately 2:16 a.m., SHARP used the Surfshark VPN to mask his connection while cloning Company-1's GitHub repositories.

---

[2] SSH is a network protocol that gives users, such as system administrators, a way to access a remote machine. An SSH connection by itself does not reveal a list of available GitHub repositories, so a user intending to access or copy any particular repository would have needed to have acquired the names of those repositories through some other prior means, such as through a web browser connection described in the preceding paragraph.

No further clone commands were processed until approximately 39 minutes later, on December 22, 2020, at approximately 2:55 a.m., when GitHub Account-1 received a command to clone another repository from the Sharp IP associated with the Sharp Residence. Approximately nine minutes later, the clone commands continued from GitHub Account-1, once again masked by the Surfshark VPN.

18. On December 22, 2020 at approximately 2:16 a.m., the attacker's exfiltration commands stopped. At around the same time, the internet service at the Sharp Residence went down. At approximately 2:54 a.m., the Internet service at the Sharp Residence was reenabled, and approximately one minute later, the Sharp IP was logged, unmasked by any VPN, using GitHub Account-1 to continue sending clone commands.

19. Over the next several hours, on December 22, 2020 between approximately 3:04 to 5:31 a.m., NICKOLAS SHARP, the defendant, cloned approximately 155 repositories from Company-1 through GitHub Account-1, using the Surfshark VPN to once again mask his IP address.

20. NICKOLAS SHARP, the defendant, accessed Company-1's GitHub or AWS data using the Surfshark VPN through at least on or about December 26, 2020. Among other things, SHARP applied one-day lifecycle retention policies to certain logs on AWS

which would have the effect of deleting certain evidence of the intruder's activity within one day.

21. The Incident was discovered by other employees of Company-1 on or about December 28, 2020. At that time, NICKOLAS SHARP, the defendant, joined a team working to assess the scope and damage caused by the Incident and remediate its effects, all while concealing his role in committing the Incident. SHARP made numerous false statements to Company-1's employees and agents to evade detection. For example, upon the team's identification of Surfshark VPN as the tool used by the attacker, SHARP pretended to have never used Surfshark VPN himself.

22. On or about January 7, 2021, at approximately 4:01 a.m., senior employees at Company-1, including an employee located in Manhattan, New York, received a ransom email (the "Ransom Email") from the perpetrator of the Incident. The email was sent through an IP address associated with the Surfshark VPN. The Ransom Email offered, in substance, to return the stolen data and not to publish or use it, in exchange for the payment of 25 Bitcoin. The Ransom Email also offered to identify a purportedly still unblocked "backdoor" used by the attacker for the sum of another 25 Bitcoin. The total amount requested for ransom was equivalent to close to

$1.9 million, based on the prevailing exchange rate between Bitcoin and U.S. dollars at the close of January 7, 2021. The Ransom Email also referenced a chat communication on Keybase, sent by the attacker to a senior security employee at Company-1. That Keybase communication contained a copy of the Ransom Email text as well as uploaded examples of Company-1's stolen data.

23. Company-1 did not pay the ransom prior to the ransom deadline set forth the Ransom Email. On or about January 9, 2021, at approximately 11:57 p.m., three minutes before the ransom deadline was to expire, NICKOLAS SHARP, the defendant, sent an employee of Company-1 a message on Keybase, as the anonymous perpetrator of the Incident. The message read "No BTC. No talk. We done here." The message contained a link to a public Keybase folder on which the perpetrator had uploaded certain of Company-1's stolen proprietary data for public access. Company-1 promptly caused Keybase to remove the folder.

24. On or about January 29, 2021, NICKOLAS SHARP, the defendant, wiped and reset the laptop computer he used to perpetrate the Incident.

25. On or about March 24, 2021, agents from the Federal Bureau of Investigation ("FBI") executed a search warrant on

the Sharp Residence and seized certain electronic devices belonging to NICKOLAS SHARP, the defendant. In the course of the execution of that search, SHARP made numerous false statements to FBI agents, including among other things, in substance, that he was not the perpetrator of the Incident and that he had not used Surfshark VPN prior to the discovery of the Incident. When confronted with records demonstrating that SHARP bought the Surfshark VPN service in July 2020, approximately six months prior to the Incident, SHARP falsely stated, in part and substance, that someone else must have used his Paypal account to make the purchase.

26. Several days after the FBI executed a search warrant on the SHARP Residence and seized certain electronic devices belonging to NICKOLAS SHARP, the defendant, SHARP caused false or misleading news stories to be published about the Incident and Company-1's disclosures and response to the Incident. SHARP identified himself as an anonymous source within Company-1 who had worked on remediating the Incident. In particular, SHARP pretended that Company-1 had been hacked by an unidentified perpetrator who maliciously acquired root administrator access Company-1's AWS accounts. In fact, as SHARP well knew, SHARP had taken Company-1's data using credentials to which he had access in his role as Company-1's

AWS cloud administrator, and SHARP had used that data in a failed attempt to extort Company-1 for millions of dollars.

27. Following the publication of these articles, between Tuesday, March 30, 2021 and Wednesday March 31, 2021, Company-1's stock price fell approximately 20%, losing over four billion dollars in market capitalization.

28. As a result of perpetrating the Incident, NICKOLAS SHARP, the defendant, caused far in excess of $5,000 in losses to Company-1, which included costs incurred by Company-1 to retain forensic outside experts to investigate the Incident and remediate the harm caused by SHARP.

Statutory Allegations

29. From at least in or about 2020, up to at least in or about January 2021, in the Southern District of New York and elsewhere, NICKOLAS SHARP, the defendant, knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct, intentionally caused damage, without authorization, to a protected computer, which caused a loss aggregating to at least $5,000 in value to one and more persons during any one-year period, to wit, SHARP, without authorization, transmitted commands to servers to alter its data retention policies in order to conceal SHARP's access, in

furtherance of a scheme to extort Company-1 for ransom to return its confidential data.

(Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B)(i), 1030(c)(4)(A)(i)(I) and 2.)

COUNT TWO

(Transmission of Interstate Communications with Intent to Extort)

The Grand Jury further charges:

30. The allegations in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

31. From at least in or about 2020, up to at least in or about January 2021, in the Southern District of New York and elsewhere, NICKOLAS SHARP, the defendant, knowingly, and with intent to extort from a person, firm, association and corporation, any money and other thing of value, transmitted in interstate and foreign commerce a communication containing a threat to injure the property and reputation of the addressee and of another, to wit, SHARP transmitted an interstate email and other electronic messages to Company-1 seeking a ransom of 50 Bitcoin in exchange for returning data previously stolen by SHARP from Company-1, and to refrain from publicly identifying a purported remaining vulnerability to obtain unauthorized access to Company-1's computer systems.

(Title 18, United States Code, Sections 875(d) and 2.)

COUNT THREE
(Wire Fraud)

The Grand Jury further charges:

32. The allegations in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

33. From at least in or about 2020 to at least in or about April 2021, in the Southern District of New York and elsewhere, NICKOLAS SHARP, the defendant, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, SHARP, without authorization, downloaded confidential data belonging to Company-1 and altered retention policies to conceal his access, and then while representing that he was remediating the attack, anonymously extorted Company-1 for 50 Bitcoin to return the stolen data and identify a purported remaining vulnerability to obtain unauthorized access to

Company-1's computer systems, which involved interstate communications into and out of the Southern District of New York.

(Title 18, United States Code, Sections 1343 and 2.)

COUNT FOUR

(Making False Statements)

The Grand Jury further charges:

34. The allegations contained in paragraphs 1 through 28 of this Indictment are repeated and realleged as if fully set forth herein.

35. In or about March, 2020, NICKOLAS SHARP, the defendant, in a matter within the jurisdiction of the executive branch of the Government of the United States, knowingly and willfully made a materially false, fictitious, and fraudulent statement and representation and made and used a false writing and document knowing the same to contain a materially false, fictitious, and fraudulent statement and entry, to wit, SHARP made false statements to the FBI regarding, among other things, SHARP's involvement in a cybersecurity incident and extortion attempt at Company-1 in December 2020 and January 2021, as well as SHARP's use of

Surfshark VPN, a particular tool employed by the perpetrator of the incident.

(Title 18, United States Code, Sections 1001 and 2.)

FORFEITURE ALLEGATIONS

36. As a result of committing the offense alleged in Count One of this Indictment, NICKOLAS SHARP, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real or personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of said offenses, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

37. As a result of committing the offenses alleged in Counts Two and Three of this Indictment, NICKOLAS SHARP, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any and all property, real and personal, that constitutes or is derived, directly or indirectly, from proceeds traceable to the commission of said

offenses, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Asset Provision

38. If any of the above-described forfeitable property, as a result of any act or omission of NICKOLAS SHARP, the defendant:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third person;

(c) has been placed beyond the jurisdiction of the Court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 1030 and 981; Title 21, United States Code, Section 853; and

Title 28, United States Code, Section 2461.)

[redacted]

FOREPERSON

Damian Williams / KG

DAMIAN WILLIAMS
United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

NICKOLAS SHARP,

Defendant.

SEALED INDICTMENT

21 Cr. ___

(18 U.S.C. §§ 2, 875, 1001, 1030, and 1343.)

DAMIAN WILLIAMS
United States Attorney.

A TRUE BILL

[redacted]

FOREPERSON

Sealed Indictment, Arrest Warrant
filed 11/18/21 before OTW
VK