UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
HAMMOND DIVISION

UNITED STATES OF AMERICA	)	
	)	Case No. 2:24cr88
v.	)	
	)	18 U.S.C. § 371
GUAN TIANFENG (关天烽)	)	18 U.S.C. § 1349

INDICTMENT

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Conspiracy to Commit Computer Fraud)
18 U.S.C. § 371

1. From approximately July 2018 until May 2020, the defendant, GUAN TIANFENG (关天烽), while working for a People's Republic of China (PRC)-based private company that sold its hacking-related services to multiple PRC government agencies, participated in a conspiracy to cause damage to and obtain information by unauthorized access to protected computers. The defendant and his co-conspirators ("Conspirators") acted in furtherance of this conspiracy by acquiring internet domains, servers, and firewalls to test malicious computer code for exploiting a zero-day vulnerability in an identified, widely-used firewall, testing such code, and ultimately using that code to conduct mass, indiscriminate intrusions targeting such firewalls worldwide. The code used to carry out these intrusion campaigns would steal victims' usernames and passwords, and upon victim efforts to reboot the device

as a step towards mitigation, would attack every Windows based computer on the victim's network with ransomware. When, shortly after the intrusion campaign began, the firewall manufacturer deployed a "hotfix" patch (i.e., one that would not require a reboot), the actors unsuccessfully attempted to counter the patch by modifying their malicious code to indiscriminately conduct a ransomware attack upon the patch's deployment.

General Allegations

2. Unless otherwise noted, at all times relevant to this Indictment:

a. A "firewall" was a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. The primary use of a firewall in networking is to secure a network from cyberattacks. For example, a firewall prevents malicious and unwanted content from entering a protected environment. Firewalls are generally connected to the internet.

b. "Structured Query Language" ("SQL") was a programming language for storing and processing information in a relational database, with rows and columns representing different types of data.

c. "Ransomware" was a type of malicious software ("malware") which prevented a user from accessing data stored on a device, usually by encrypting the files. Typically, when a computer is infected with ransomware, the files or computer will generally remain encrypted until a ransom is paid and the perpetrator provides a decryption key.

d. The term "domain name" referred to a string of characters associated with a unique location on the internet. For example, "google.com" is a domain name.

e. The term "internet protocol address" ("IP address") was a numerical label assigned to a computer connected to a network. An IP address facilitates computer-to-computer communication.

f. The term "exploit" referred to malicious computer code that takes advantage of a software vulnerability or flaw.

g. Sichuan Silence Information Technology Co. Ltd. ("Sichuan Silence") was a business based in the PRC that specialized in information security systems and computer network operations against such systems. Sichuan Silence sold its services and the data it obtained through hacking to PRC businesses and government entities, including the Ministry of Public Security (MPS), the National Computer Network Emergency Response Technical Team / Coordination Center of China (CNCERT/CC), and the PRC's Vulnerability Platform. According to its website, as part of its business, Sichuan Silence performs penetration testing and vulnerability mining. It has also developed a product line which can be used to scan and detect overseas network targets in order to obtain valuable intelligence information.

h. FIREWALL PRODUCT 1 was a firewall product sold by Sophos Ltd. ("Sophos"), a computer software and hardware security company based in the United Kingdom. Sophos sold different versions of FIREWALL PRODUCT 1, including hardware devices and virtual appliances. Hardware devices were shipped to customers, while virtual appliances could be obtained online directly from Sophos. Both hardware and virtual versions of FIREWALL PRODUCT 1 were "protected computers," as defined in Title 18, United States Code, Section 1030(e)(2).

i. The Conspirators included GUAN TIANFENG, a resident and citizen of the PRC. GUAN TIANFENG was employed by Sichuan Silence and, among other things, developed exploits.

The Conspiracy and Its Objects

3. From at least in or about July 2018 to at least in or about May 2020, in the Northern District of Indiana and elsewhere within the jurisdiction of the Court,

GUAN TIANFENG,

the defendant, together with others known and unknown to the Grand Jury, did knowingly and intentionally conspire and agree to commit offenses against the United States, that is:

a. to intentionally access computers without authorization, and thereby obtain information from a department or agency of the United States and from at least one protected computer, such conduct having involved an interstate and foreign communication, and the offense was committed for purposes of commercial advantage and private financial gain, with the value of such information exceeding $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and (C), and 1030(c)(2)(B)(i) and (iii); and

b. to knowingly cause the transmission of a program, information, code, and command, and as a result, intentionally cause damage without authorization to protected computers, resulting in loss during a one-year period aggregating at least $5,000 in value, damage affecting one or more computers used by an entity of the United States Government in furtherance of the administration of justice, national defense, or national security, and damage affecting ten or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i).

Manner and Means of the Conspiracy

4. The Conspirators identified a previously unknown (zero-day) SQL injection vulnerability in FIREWALL PRODUCT 1, which allowed an attacker to remotely execute code by using specific strings in SQL database queries.

5. After discovering the zero-day vulnerability, the Conspirators developed an exploit that used the SQL injection vulnerability to remotely execute code using a specific database field on FIREWALL PRODUCT 1.

6. From in or about February 2020 to in or about May 2020, the Conspirators developed and tested the exploit from within the offices of Sichuan Silence on FIREWALL PRODUCT 1 firewalls that they acquired.

7. The Conspirators registered domain names and rented servers to deploy the exploit. In April 2020, the Conspirators deployed the zero-day exploit against approximately 81,000 FIREWALL PRODUCT 1 firewalls throughout the world, including within the Northern District of Indiana, without the knowledge or authorization of Sophos or its customers, the owners and users of FIREWALL PRODUCT 1 firewalls. After Sophos discovered the zero-day vulnerability, it was designated CVE-2020-12271.

8. The exploit was designed to obtain, without authorization, usernames, passwords, and other information stored on FIREWALL PRODUCT 1 firewalls by Sophos customers. This information could provide valid credentials for the attackers to authenticate into the FIREWALL PRODUCT 1 firewalls and pivot into the networks of the victim entities, allowing them to, without authorization, obtain confidential information from additional computers.

9. The Conspirators also used the exploit to deploy encryption software from a prevalent ransomware variant on FIREWALL PRODUCT 1 firewalls. In the initial indiscriminate attack, the Conspirators designed the ransomware to encrypt files if the firewall owner attempted to remediate the

infection by rebooting the firewall.

10. Sophos patched its customers' firewalls approximately two days after the attack occurred. In response, the Conspirators modified their malware to deploy ransomware to victim devices earlier in the exploitation process. Specifically, the actors replaced the parts of the initial attack code designed to obtain information from the firewalls (i.e., to obtain information to enable further undetected access and persistence) with a program designed to deploy the ransomware upon other, pre-reboot mitigation steps (i.e., prioritizing the damaging of a victim computer over expanding access or persistence). However, Sophos's initial patch prevented the Conspirators from using this change to successfully deploy ransomware on patched devices.

Overt Acts

11. In furtherance of the conspiracy, and to accomplish the objects thereof, GUAN TIANFENG and his Conspirators committed the following overt acts, among others, within the Northern District of Indiana and elsewhere:

a. On or about July 26, 2018, a Conspirator registered the domain 9sg.me. The exploit used by the Conspirators was programmed to download a file from this domain that would then cause FIREWALL PRODUCT 1 firewalls to download the "Ragnarök" ransomware. 9sg.me was associated with an IP address resolving to China.

b. On or about March 27, 2020, a Conspirator registered the domain sophosfirewallupdate.com and associated it with an IP address resolving to China. This domain was designed to appear as being associated with Sophos in order to avoid detection. The exploit used by the Conspirators was programmed to download a program from sophosfirewallupdate.com that, without authorization, obtained information from FIREWALL PRODUCT 1 firewalls.

c. On or about February 14, 2020, GUAN TIANFENG registered a FIREWALL PRODUCT 1 firewall ("Test Device 1").

d. On or about February 16, 2020, GUAN TIANFENG registered another FIREWALL PRODUCT 1 firewall ("Test Device 2").

e. On or about February 16, 2020, approximately 20 minutes after GUAN TIANFENG registered Test Device 2, he connected to a Sophos blog post discussing vulnerabilities related to FIREWALL PRODUCT 1.

f. From on or about February 25, 2020, to on or about March 19, 2020, Conspirators developed and tested the exploit on Test Device 1.

g. On or about March 13, 2020, Conspirators tested the exploit on Test Device 2.

h. On or about March 13, 2020, minutes after testing the exploit on Test Device 2, Conspirators tested the exploit on Test Device 1.

i. On or about March 16, 2020, GUAN TIANFENG registered another FIREWALL PRODUCT 1 firewall ("Test Device 3").

j. Beginning on or about April 22, 2020, and continuing to at least in or about May 2020, Conspirators used the domains sophosfirewallupdate.com and 9sg.me to deploy the exploit previously tested on Test Devices 1 and 2 to access without authorization approximately 81,000 FIREWALL PRODUCT 1 firewalls and the information stored on those devices, including FIREWALL PRODUCT 1 firewalls registered within the Northern District of Indiana.

k. On or about May 7, 2020, Conspirators accessed Sophos's website and viewed information describing Sophos's patch for the FIREWALL PRODUCT 1 vulnerability.

l. On or about May 10, 2020, Conspirators tested an updated version of the exploit on Test Device 1.

(All in violation of Title 18, United States Code, Section 371.)

COUNT TWO
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1349

12. The Grand Jury re-alleges and incorporates by reference the factual allegations contained in paragraphs 1 through 11 as if fully set forth herein.

The Conspiracy and Its Objects

13. From at least July 2018 to at least May 2020, in the Northern District of Indiana and elsewhere within the jurisdiction of the Court,

GUAN TIANFENG,

the defendant, together with others known and unknown to the Grand Jury, did knowingly, intentionally, and willfully combine, conspire, confederate, and agree to violate Title 18, United States Code, Section 1343.

14. It was a part and object of the conspiracy that the defendant, and others known and unknown to the Grand Jury, having devised and intended to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds to execute this scheme and artifice; to wit, communications by means of wires with FIREWALL PRODUCT 1 firewalls and connected networks to create and maintain unauthorized access to those

firewalls and connected networks and to obtain proprietary and valuable information from them.

(All in violation of Title 18, United States Code, Section 1349.)

NOTICE OF FORFEITURE

The Grand Jury finds that there is probable cause that the property described in this NOTICE OF FORFEITURE is subject to forfeiture pursuant to the statutes described herein.

Defendant GUAN TIANFENG is hereby notified, pursuant to Federal Rule of Criminal Procedure 32.2(a), that upon conviction of any of the violations set forth in COUNTS ONE or TWO of this Indictment, he shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2) and 1030(i), any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the violations, and any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to commit such violations.

Defendant GUAN TIANFENG is hereby notified, pursuant to Federal Rule of Criminal Procedure 32.2(a), that upon conviction of any of the violations set forth in COUNT ONE of this Indictment, that he shall forfeit to the United States, pursuant to 18 U.S.C. §§ 981(a)(1)(D)(vi) and 28 U.S.C. § 2461, any property, real or personal, which constitutes or is derived from gross receipts obtained, directly or indirectly, from a violation.

Defendant GUAN TIANFENG is hereby notified, pursuant to Federal Rule of Criminal Procedure 32.2(a), that upon conviction of any of the violations set forth in COUNT TWO of this Indictment, he shall forfeit to the

United States, pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 28 U.S.C. § 2461, any property, real or personal, which constitutes or is derived from proceeds traceable to a violation.

Pursuant to 21 U.S.C. § 853(p), GUAN TIANFENG shall forfeit substitute property, if, by any act or omission of GUAN TIANFENG, the property referenced above cannot be located upon the exercise of due diligence; has been transferred, sold to, or deposited with a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.

(All in accordance with Title 18, United States Code, Sections 982(a)(1)(C), (a)(2)(B), 1030(i); and Fed. R. Crim. P. 32.2.)

A TRUE BILL:

/s/ Foreperson
Foreperson of the Grand Jury

CLIFFORD D. JOHNSON
UNITED STATES ATTORNEY

/s/ Steven J. Lupa
Steven J. Lupa
Assistant United States Attorney

MATTHEW G. OLSEN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION

/s/ Jacques Singer-Emery
Jacques Singer-Emery
Trial Attorney
National Security Cyber Section
National Security Division

George S. Brown
Trial Attorney
National Security Cyber Section
National Security Division