SEALED

ASJZ/RIG USAO 2022R00237

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA

v.

AMIN STIGAL,

Defendant.

FILED UNDER SEAL

CRIMINAL NO. LKG 24cr206

(Conspiracy to Commit Computer Intrusion and Damage (18 U.S.C. § 371); Forfeiture (18 U.S.C. §§ 982, and 1030(i), 21 U.S.C. § 853(p))

INDICTMENT

COUNT 1
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

The Grand Jury for the District of Maryland charges that:

At all times relevant:

1. In or around December 2020 to the present, the Russian Federation ("Russia") operated a military intelligence agency called the Main Intelligence Directorate of the General Staff ("GRU"). The GRU had multiple units which engaged in cyber operations that, among other things, involved the destruction of computer systems in foreign countries through computer intrusions.

2. Defendant AMIN STIGAL was a Russian citizen and civilian who knowingly and intentionally conspired with GRU officers including other persons known and unknown to the Grand Jury (collectively the "Conspirators"), to gain unauthorized access (to "hack") into computers associated with the Ukrainian Government or entities associated with the governments of countries that provide support to the Ukrainian Government in resisting Russia's unjustified invasion of Ukraine. First, in the month prior to the full-scale Russian invasion of Ukraine in

February 2022, the Conspirators hacked the computers of dozens of Ukrainian Government entities, including in critical infrastructure, as well as entities responsible for other sectors with no military or defense-related roles, including agriculture, education and science, and emergency services, and destroyed or attempted to destroy those systems in advance of the Russian invasion of Ukraine in February 2022. The Conspirators used software that was designed to appear as if the computers had suffered a ransomware attack, when in fact the data on the computers had been deleted. The Conspirators also stole and leaked through online platforms the personal data of thousands of Ukrainian civilians, including medical records. The purpose of the attack was, in part, to sow concern among Ukrainian citizens regarding the safety of their Government's systems and their personal data in advance of the Russian attack of Ukraine. This campaign became publicly known in cybersecurity circles as the "WhisperGate" campaign.

3. In addition, the Conspirators hacked a Central European country's transportation infrastructure in October 2022. The Central European country was a supporter of Ukraine and had delivered civilian and military aid to Ukraine following the Russian invasion of Ukraine in February 2022.

4. The Conspirators also probed systems in the United States, including multiple sites maintained by a U.S. Government Agency located in Maryland.

5. To conceal their connections to Russia and the Russian Government, the Conspirators used false identities and made false statements about their identities. To further avoid detection, the Conspirators used a network of computers located across the world, including in the United States, and paid for this infrastructure using cryptocurrency.

Defendants

6. The defendant, AMIN STIGAL [Амин Тимович Стигал] is a Russian citizen who supports the activities of the GRU by setting up online infrastructure for GRU officers to use in cyberattacks, including in the deployment of the WhisperGate malware described further below.

Relevant Terms

7. "Bitcoin" or "BTC" was a type of virtual currency, circulated over the Internet as a form of value. Bitcoin were not issued by any Government, bank, or company, but rather were generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin were just one of many varieties of virtual currency.

8. A "darknet website" was a hidden website available through a network of globally distributed relay computers called The Onion Router, or "Tor," network. Unlike standard Internet websites, Tor-based websites anonymize Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking information about the user's computer.

9. "Encryption" was a way of scrambling data so that only authorized parties can read or understand the information. In order to access encrypted data, a user must have access to a password (known as a "decryption key") that enabled the user to decrypt it.

10. "Malware" was malicious computer software intended to, when successfully installed, cause the victim computer to behave in a manner inconsistent with the intention of the owner or user of the victim computer, usually unbeknownst to that person.

11. Voice Over Internet Protocol "VOIP" was a technology that allowed users to make voice calls using a broadband Internet connection instead of a regular phone line.

The Conspiracy

12. Beginning no later than in or around December 2020, and continuing through the date of this Indictment, in an offense that began outside the jurisdiction of any particular State or district of the United States, and continued in the District of Maryland and elsewhere, the defendant, **AMIN STIGAL**, did knowingly and unlawfully conspire with others known and unknown to the Grand Jury to commit an offense against the United States, that is:

a. to 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, with such offense causing: loss to 1 or more persons during a 1-year period aggregating at least $5,000 in value; and damage affecting 10 or more protected computers during a 1-year period; in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B);

Object of the Conspiracy

13. The object of the conspiracy was for STIGAL, together with his co-conspirators, to identify and exploit vulnerabilities in, and obtain unauthorized access to, protected computers belonging to target Governments and infrastructure systems outside of Russia in order to cause damage and render the targeted protected computers inoperable. In addition, it was a further object of the conspiracy for STIGAL, together with his co-conspirators, to exfiltrate data from those protected computers and stage public releases of that data in order to embarrass the target Governments and create concern among their citizens about vulnerabilities to cyberattack.

Manner and Means of the Conspiracy

14. From December 2020 through the present, the Conspirators scanned protected computers worldwide for possible vulnerabilities, including in the District of Maryland, as a preliminary step toward gaining unauthorized access to those protected computers.

15. It was further part of the conspiracy that the Conspirators gained unauthorized access to protected computers by exploiting those vulnerabilities identified through the scanning and stole copies of files and programs that could be accessed from the targeted protected computers.

16. It was further part of the conspiracy that the Conspirators would infect protected computers with malware, which would render those computers unusable. The malware was often disguised to appear like ransomware, but in fact would leave the victim with no method to recover their data.

17. It was further part of the conspiracy that the Conspirators would exfiltrate data from the targeted protected computers prior to disabling them, and would post that data, including personal information of individuals, for sale on the internet. The data was posted, in part, to sow concern among Ukraine citizens regarding the safety of their Government's systems and their personal data in advance of the Russian invasion of Ukraine.

Overt Acts

STIGAL Creates Conspirators' Accounts

18. From on or about September 17, 2021, through on or about January 28, 2022, STIGAL created or caused to be created five accounts on Company 1's servers for the purpose of use in the Conspirators' attacks. Company 1 was a messaging and VOIP platform located in the United States.

19. From on or about September 17, 2021, through on or about January 18, 2022, STIGAL and other Conspirators caused more than 225 files, including numerous malware scripts to be uploaded to accounts on Company 1's servers, including accounts controlled by STIGAL.

Attack on Ukrainian Government Computer Systems

20. On or about August 19, 2021, the Conspirators scanned more than 2,400 public facing Ukrainian Government websites for potential vulnerabilities, including Diia.gov.ua (DIIA), the website for a Ukrainian Government application that was built in partnership with the United States and allowed the Ukrainian people to connect with Ukrainian Government services and access Ukrainian Government documents.

21. In January 2022, the Conspirators probed a variety of protected computer systems associated with the Ukrainian Government for potential vulnerabilities, including the State Treasury of Ukraine, Ukrainian Maritime Services, and Ukrainian Railways (uz.gov.ua).

22. On or about January 13, 2022, the Conspirators attacked protected computers of at least two dozen Ukrainian Government networks, including the Ministry of International Affairs, the State Treasury, the Judiciary Administration, the State Portal for Digital Services (DIIA), the Ministry of Education and Science, the Ministry of Agriculture, the State Service for Food Safety and Consumer Protection, the Ministry of Energy, the Accounting Chamber for Ukraine, the State Emergency Service, the State Forestry Agency, and the Motor Insurance Bureau, using a malware program known as WhisperGate.

23. The Conspirators infected the targeted protected computers associated with the Ukrainian Government networks with WhisperGate, which uses a two-stage malware program. The first stage wiped the Master Boot Record ("MBR") from the targeted computer. The MBR allows an operating system to be loaded (booted) into a usable interface. Without an MBR, a computer is unable to restart or operate normally.

24. The Conspirators also caused a ransom note to be placed on the targeted protected computer stating:

> Your hard drive has been corrupted. In case you want to recover all hard drives of your organization, You should pay us $10k via bitcoin wallet [address] and send message . . . with your organization name. We will contact you to give further instructions.

In truth, as described further below, although a ransom note was displayed, the data on the targeted computers was destroyed, and therefore not recoverable even if a ransom were paid.

25. The Conspirators also caused the second stage of the malware to be activated. This stage contained a "GET" request to a URL maintained by Company 1. That request resulted in the downloading and execution of a program from an account on Company 1's servers that the Conspirators had created, that corrupted the files on the targeted protected computer, rendering the protected computer inoperable and entirely deleting data from the computer systems.

26. In addition, on or about that same date, January 13, 2022, the Conspirators compromised protected computers hosting the DIIA website and other websites, and caused a message to be displayed in Polish, Russian, and Ukrainian reading: "Ukrainians! All information about you has become public, be afraid and expect the worst. This is for your past, present and future."

Release of Exfiltrated Information

27. Within hours of the attack, on or about January 13, 2022, the Conspirators listed for sale data described as originating from the Ukrainian Government on forums across the darknet, using moniker "Free Civilian," including:

a. Criminal records obtained from Ukrainian Government systems.

b. Patient health data from Ukrainian Government systems; and

c. Motor Insurance Bureau information from Ukrainian Government systems.

28. On that same day, the Conspirators also offered for sale on the internet data for 13.5 million users from Diia.gov.ua for $80,000.

Central European Country Infrastructure Attack

29. In October 2022, the Conspirators probed computer networks associated with a Central European country's transportation sector. The Central European country was a supporter of Ukraine and had delivered civilian and military aid to Ukraine following the Russian invasion of Ukraine in February 2022.

30. As a result of the vulnerabilities discovered in the probing activities, the Conspirators gained access to protected computers associated with a Central European country's transportation section in or around October 2022.

Scanning of U.S. Government Assets in Maryland

31. From on or about August 5, 2021, through on or about February 3, 2022, the Conspirators probed public-facing websites hosted by protected computers and unassigned servers maintained by a Government Agency located in Maryland, 63 times. This probing used the same infrastructure that the Conspirators previously employed to conduct scanning against targets.

18 U.S.C. § 371

FORFEITURE ALLEGATION

The Grand Jury for the District of Maryland further finds that:

1. Pursuant to the Federal Rule of Criminal Procedure 32.2, notice is hereby given to the defendant that the United States will seek forfeiture as part of any sentence in accordance with 18 U.S.C. §§ 982 and 1030(i), and 21 U.S.C. § 853(p) in the event of the defendant's conviction on the offense charged in Count One of this Indictment.

2. Upon conviction of the offense set forth in Count One, the defendant,

AMIN STIGAL

shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B) and 1030(i), any property constituting, or derived from, proceeds obtained directly or indirectly, as a result of such violation, and pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of such violation.

Substitute Assets

3. If any of the property described above, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred, sold to, or deposited with a third party;

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 divided without difficulty

the United States shall be entitled to forfeiture of substitute property pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b).

18 U.S.C. §§ 982, 1030(i)
21 U.S.C. § 853(p)

Erek L. Barron
United States Attorney

SIGNATURE REDACTED

Foreperson
Date: 6/25/24