UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TENNESSEE
AT KNOXVILLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

ROMAN KHLYNOVSKIY
a.k.a. ROMAN HLYNOVSKIY
a.k.a. РОМАН ХЛЫНОВСКИЙ

Defendant.

NO. 3:25CR84

JUDGES Varlan/McCook

INDICTMENT

The Grand Jury charges the following:

COUNT ONE
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers and Identity Theft)

I. INTRODUCTION

1. "Malware" is malicious software designed to disrupt computer operations, gather sensitive information, facilitate remote access to private computer systems, and perform other unauthorized actions on computer systems. Common examples of malware include remote access trojans, ransomware, and "info stealers" such as keyloggers.

2. "Ransomware" is a type of malware designed to encrypt some or all of the data on a computer. Malicious cyber actors that deploy ransomware typically extort the user of an encrypted computer by demanding that the user pay a ransom in order to decrypt and recover the

data on the computer. Malicious cyber actors can use multiple types of ransomware, often referred to as ransomware variants, to encrypt victim files. These variants behave in unique ways, such as leaving different ransom notes or renaming files with different file extensions.

3. "Encryption," in the context of ransomware, involves the use of a computer code to convert victim computer data from its original form into a form that is unusable. This conversion into unusable and unreadable code cannot be reversed without the use of a secret and complex password, commonly referred to as a "decryption key." There is often no possible way for a ransomware victim to successfully decrypt and recover their files without this decryption key.

4. "INC" is a ransomware variant and is also known as Lynx. INC ransomware operates using a business model known as "Ransomware as a service" ("RaaS"). Under this model, a central administrative group referred to as administrators will both develop and maintain the underlying ransomware code. They then sell or license this code to other hackers, called "affiliates," who identify victims and deploy the code to initiate ransomware attacks. Sometimes these affiliates can form organized groups, referred to as "affiliate groups." At times, administrators also conduct their own ransomware attacks as well. Members of INC serve other distinct roles, including as negotiators.

5. A "vulnerability" in the context of information technology, such as computers and networking equipment, is a flaw in software or hardware that can be exploited by a malicious cyber actor to perform an unintended action. In severe cases, these vulnerabilities allow malicious cyber actors to gain remote access to or run unwanted computer code on the vulnerable machine.

6. "Remote desktop capabilities," also referred to as "Remote Desktop Protocol" or "RDP," generally allow legitimate users to remotely access and interact with a computer as if they were logged in at the physical machine. However, these capabilities can be exploited and abused by malicious cyber actors who might use stolen credentials to log into and run commands on a victim computer. Various services offer RDP, including Citrix. Citrix is a service that offers cloud computing and is often used to allow an entity's employees to remotely work and collaborate with other employees. Threat actors often use compromised Citrix accounts to remotely access an organization's internal network in a manner that appears legitimate. Once inside, they can browse file shares, access sensitive systems, and exfiltrate data without immediately triggering security alerts, leveraging the trusted access associated with the stolen credentials.

7. "Cobalt Strike" is penetration testing software owned by a U.S.-based company. A penetration test is a simulated cyberattack performed on a computer network, authorized by the owner of that computer network, to reveal cybersecurity issues or flaws on a company's network so that those issues can be fixed. Penetration testing software, such as Cobalt Strike, includes a suite of hacking tools used to facilitate a penetration test. While Cobalt Strike was designed to be used legitimately, it has also been abused by malicious cyber actors who use unauthorized versions of Cobalt Strike to facilitate attacks on unwitting victims. Cobalt Strike is split into client and server components, and the server component is known as a team server.

8. A "command and control" ("C2") server is a computer used for the specific purpose of facilitating the "command" and "control" of other computers or devices. A C2 server can be used to perform a variety of malicious tasks, such as sending commands to malware

installed on victim computers and recording the responses from those commands so that they can be viewed by malicious cyber actors.

9. "Bitcoin" is a type of virtual currency, not issued by any government, bank, or company, which is generated and controlled through a decentralized, peer-to-peer network. Acquiring Bitcoin can be done by purchasing Bitcoin from a cryptocurrency exchange with traditional fiat currency or through cryptocurrency mining. Cryptocurrency exchanges frequently allow users to exchange one type of cryptocurrency, such as Bitcoin, for others, such as Monero, or for fiat currency.

10. "Bitcoin addresses" are locations where Bitcoin can be sent and received. A Bitcoin address is analogous to a bank account number and is represented by a 26-to-35 character-long case-sensitive string of letters and numbers. To transfer Bitcoin out of one Bitcoin address and into another, an individual needs that address's unique corresponding private key. A private key is analogous to a bank account password. Little to no personally identifiable information about a Bitcoin account holder is transmitted during a Bitcoin transfer.

11. An "Internet Protocol address," also referred to as an "IP address," is a unique numeric address used by digital devices on the Internet. An IP address, for present purposes, looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 149.101.1.32). 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. The records of which provider controls which IP addresses are maintained in publicly searchable databases. Some computers have static – that is, long-term – IP addresses, while other computers have dynamic – that is, frequently changed – IP addresses.

12. "Electronic medical records," also referred to as "EMRs," are digital versions of patients' paper charts, containing medical history, diagnoses, medications, treatment plans, photographs, and other healthcare information maintained by a provider. EMRs are used to document, store, and access sensitive patient care data securely.

13. The SCHOOL VICTIM is a school system located in the Eastern District of Tennessee.

14. The SOFTWARE VICTIM is a software company headquartered in the United States that offers information technology and other digital services to, among other entities, hospitals and healthcare facilities.

15. The KENTUCKY HOSPITAL VICTIM is a hospital group with a cancer center located in Kentucky.

16. The CALIFORNIA HOSPITAL VICTIM is a hospital located in California that uses services offered by the SOFTWARE VICTIM.

17. The ARKANSAS HOSPITAL VICTIM is a hospital located in Arkansas that uses services offered by the SOFTWARE VICTIM.

18. The NEW JERSEY HOSPITAL VICTIM is a hospital group located in New Jersey that uses services offered by the SOFTWARE VICTIM.

19. The MISSOURI HOSPITAL VICTIM is a hospital group headquartered in Missouri and uses services offered by the SOFTWARE VICTIM.

20. The Defendant, ROMAN KHLYNOVSKIY is also known as Roman Hlynovskiy, and using the Cyrillic alphabet is also known as РОМАН ХЛЫНОВСКИЙ. KHLYNOVSKIY is a national of Kazakhstan.

21. At all times material to this indictment, the 8-Digits Team was an affiliate group that used the INC ransomware variant, among others.

22. At all times material to this indictment, KHLYNOVSKIY was a member of the 8-Digits Team.

II. CHARGE

23. From on or about October 13, 2021, through on or about July 31, 2025, in the Eastern District of Tennessee and elsewhere, ROMAN KHLYNOVSKIY did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit an offense against the United States, that is:

a. to intentionally access a computer without authorization and thereby obtain information from a protected computer for the purposes of private financial gain and thereby obtained information that has a value in excess of $5,000, in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B);

b. 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, and cause loss to persons during a 1-year period from the defendant's course of conduct affecting protected computers aggregating at least $5,000 in value, cause the modification and impairment of the medical examination, diagnosis, treatment, or care of individuals, cause threat to public health or safety, and cause damage affecting 10 or more protected computers during a 1-year period in violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(c)(4)(B);

c. to knowingly and with intent to extort from any person any money and 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 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, in violation of 18 U.S.C. §§ 1030(a)(7)(B), 1030(a)(7)(C) and 1030(c)(3)(A); and

d. to knowingly transfer, possess, and use, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, and in connection with, an unlawful activity that constitutes a violation of federal law, to wit, violations of 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(A), and 1030(a)(7)(C), and such transfer, possession, and use of a means of identification occurred in and affecting interstate and foreign commerce and as a result, KHLYNOVSKIY and others known and unknown to the grand jury obtained a thing of value aggregating at least $1,000 during a one year period, in violation of 18 U.S.C. §§ 1028(a)(7) and 1028(b)(1)(D).

III. PURPOSE AND GOAL OF THE CONSPIRACY

24. It was the purpose of the conspiracy for ROMAN KHLYNOVSKIY and other conspirators to unlawfully enrich themselves by: (a) gaining unauthorized access to vulnerable victims' computers; (b) stealing victim data; (c) taking steps to expand unauthorized access and maintain access to victims' networks; (d) deploying ransomware on victim computers; (e) extorting victims by demanding a ransom in exchange for the ability to decrypt the data, or

threatening the public release of stolen victim data; (f) collecting ransom payments in the form of cryptocurrency, and (g) transferring the ransom payments to various virtual currency addresses, cryptocurrency exchangers, and different forms of cryptocurrency in order to conceal and disguise the nature, location, source, ownership, and control of ransom payments.

IV. MANNER AND MEANS OF THE CONSPIRACY

25. The manner and means by which ROMAN KHLYNOVSKIY and other conspirators sought to accomplish the purpose of the conspiracy included, among other things:

a. KHLYNOVSKIY and other conspirators targeted victims in the United States and elsewhere, including schools, hospitals, and healthcare entities, among others.

b. KHLYNOVSKIY and other conspirators used stolen login credentials and exploited other vulnerabilities to obtain unauthorized access to victims' computers.

c. Once they gained access to victims' computers, KHLYNOVSKIY and other conspirators ran commands and other malicious code on victims' computers to expand unauthorized access and maintain access to victims' networks.

d. KHLYNOVSKIY and other conspirators exfiltrated victim data to servers and computers controlled by KHLYNOVSKIY and other conspirators. This victim data included EMRs, among other private data.

e. KHLYNOVSKIY and other conspirators rented servers at a number of hosting providers in the United States and elsewhere to both store stolen victim data and to assist the conspiracy in remaining anonymous.

f. KHLYNOVSKIY and others reviewed EMRs and other private data for sensitive information that could be used to extort the conspiracy's victims.

g. KHLYNOVSKIY and other conspirators deployed ransomware, including the INC ransomware variant, to encrypt victims' computers.

h. KHLYNOVSKIY and other conspirators extorted victims by demanding a ransom in cryptocurrency in exchange for the ability to decrypt data following a ransomware attack.

i. KHLYNOVSKIY and other conspirators extorted victims by threatening to publish stolen victim data unless a ransom was paid in cryptocurrency, and demanded payment in cryptocurrency in exchange for the destruction and deletion of stolen victim data.

j. Despite promising to destroy and delete victim data following the ransom payment, KHLYNOVSKIY and other conspirators would in fact not destroy or delete victim data.

k. KHLYNOVSKIY and other conspirators collected ransom payments in the form of cryptocurrency and transferred those ransom payments to various bitcoin addresses, cryptocurrency exchangers, and different forms of cryptocurrency in order to conceal and disguise the nature, location, source, ownership, and control of ransom payments.

l. KHLYNOVSKIY and other conspirators also knowingly falsely registered a domain name and knowingly used that domain name in the course of their offense.

V. OVERT ACTS

26. In furtherance of the conspiracy and to affect its unlawful objects, KHLYNOVSKIY and other conspirators committed and caused to be committed the following overt acts in the Eastern District of Tennessee and elsewhere:

a. On or about October 13, 2021, KHLYNOVSKIY and other conspirators rented a server to be used as a C2 server to maliciously deploy Cobalt Strike without authorization. That server was assigned the IP address [redacted]

b. On or about August 22, 2023, an INC ransomware affiliate deployed INC ransomware on the SCHOOL VICTIM's computers in the Eastern District of Tennessee, causing those computers to become encrypted and unavailable.

c. On or around December 15, 2023, KHLYNOVSKIY and other conspirators used C2 servers associated with IP addresses [redacted], among other C2 servers rented by KHLYNOVSKIY and other conspirators, to gain unauthorized access to computers operated by the KENTUCKY HOSPITAL VICTIM and thereby obtained EMRs and other records.

d. Beginning on or about December 22, 2023, KHLYNOVSKIY and other conspirators started sending extortion communications to the KENTUCKY HOSPITAL VICTIM through an encrypted email platform.

e. On or about December 22, 2023, KHLYNOVSKIY and other conspirators sent an encrypted email to the KENTUCKY HOSPITAL VICTIM, stating among other things: "Please be advised that [KENTUCKY HOSPITAL VICTIM] was hacked a week ago and 80% of your patient data (including medical records, illness and death records) as well as internal documentation was stolen. This is not a joke,

take these words as seriously as possible because if you don't get in touch with us we are going to leak your patient data, which is HIPAA violation. Also internal documentation, private sensitive data of employees, financial reports will be sent to news outlets, which will result in huge multi-million dollar fines, lawsuits, a drop in capitalization price and loss of reputation, you are well aware and have probably heard about the consequences of data compromise after hacks. It is in your best interest to get in touch with us as soon as possible and keep this incident confidential to avoid problems. After responding to this email and confirming that you are the person responsible for these negotiations, you will receive a file tree, screenshots and further instructions for negotiation."

f. On or about January 9, 2024, KHLYNOVSKIY and other conspirators caused a ransom payment of approximately $9,000,000 in bitcoin to be made by the KENTUCKY HOSPITAL VICTIM.

g. On or about January 22, 2025, KHLYNOVSKIY and other conspirators gained unauthorized access to the SOFTWARE VICTIM's computers, which were connected to the Internet.

h. On or about January 23, 2025, KHLYNOVSKIY and other conspirators used the credentials of [redacted], an employee of a healthcare facility that uses the SOFTWARE VICTIM's services, to log into [redacted]'s Citrix account without authorization in furtherance of their breach of the SOFTWARE VICTIM's network.

i. Between on or about January 22, 2025, to at least on or about February 25, 2025, KHLYNOVSKIY and other conspirators performed reconnaissance on the

SOFTWARE VICTIM's network, moved laterally through the SOFTWARE VICTIM's network, executed commands, deployed Cobalt Strike, initiated external data transfers, used various attack toolkits, created at least one local administrator account, and uninstalled endpoint security tools.

j. On or about January 24, 2025, KHLYNOVSKIY and other conspirators began exfiltrating data, which included the SOFTWARE VICTIM's data and the data of the SOFTWARE VICTIM's customers, who were primarily hospitals and healthcare providers.

k. On or about January 24, 2025, KHLYNOVSKIY and other conspirators exfiltrated data from the SOFTWARE VICTIM to servers hosted by Amazon Web Services ("AWS") and controlled by the conspiracy.

l. Between on or about January 26, 2025, and on or about February 2, 2025, KHLYNOVSKIY accessed the AWS servers that contained stolen victim data.

m. Beginning on or about February 26, 2025, KHLYNOVSKIY and other conspirators started sending extortion communications to the CALIFORNIA HOSPITAL VICTIM through an encrypted email platform.

n. On or about March 3, 2025, KHLYNOVSKIY and other conspirators demanded 1000 bitcoin, then valued at approximately $90,000,000, in exchange for the deletion of data and to prevent patient records from being published on the Internet.

o. On or about March 3, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the CALIFORNIA HOSPITAL VICTIM, stating among other things: "We advise you to do some research, what a lawsuit after breach with

amount of HIPAA data, more than 50x times less than you have in this case, can be filed after a leak. Imagine the amounts, given the size of the possible breach [redacted]

Check out some of the statements from this link, just for you..."

p. On or about March 3, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the CALIFORNIA HOSPITAL VICTIM, stating among other things: "Why do you think we use bitcoins? The main purpose of cryptocurrency first of all, is to keep everything anonymous. . . ."

q. On or about March 14, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the CALIFORNIA HOSPITAL VICTIM, stating among other things: "In case you are willing so much to know who we are, its a pleasure to introduce ourselves.Our name is 8-Digits Team..."

r. On or about March 20, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the CALIFORNIA HOSPITAL VICTIM, stating among other things: "Lets play a game. We will continuously upgrade our portal, and research your patients medical histories.

Who shall we contact first?

The ones poor little guys who has autism?

[LINK TO FILE OMITTED]

Or is it better to leak history of someone with psychosis who defecates all over the hospital room?

[LINK TO FILE OMITTED]"

s. On or about March 20, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the CALIFORNIA HOSPITAL VICTIM, stating among other things: "Haven't you understand pretty obvious reference in the name of our Team? Its 8-Digits Team, in case you forgot.You should not even bother yourself with offers below 8 digit numbers. We wont accept that, no matter what. . . ."

t. On or about March 20, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the CALIFORNIA HOSPITAL VICTIM, stating among other things: "We are not in a position to even consider price, lower than 8 digits. This kind of offers will get you nowhere.

We analyzed roughly 0.1% of your data. We already found plenty of socially embarrassing histories, which will almost guaranteed get you in court, we wish you good luck then. Here is some examples of what we have found:

autism 219

Chlamydia 390

Gonorrhea 180

Hemorrhoids 570

infertility 208

etc...

Each one of this cases, contains pretty private details up in admission comments. Check it out, its kinda spicy.

[LINK OMITTED] - this guy likes when some other guy's dick is shoved up his ass, what do you think his lawyer will think, when he sees that his sexual life details were leaked on your behalf?

[LINK OMITTED] - how do you think, will this girl try to kill herself when she realizes, every one of her closest environment, know that her ex blackout drunk her, and raped her continuously?

[LINK OMITTED] - this one, is his anus ruptured from another guy's dick? is the hemorrhoids just a disguise? pretty gross stuff...."

u. On or about March 25, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the CALIFORNIA HOSPITAL VICTIM that provided a link to download additional patient records and stating, among other things: "This is a [redacted] presenting to the ED because she wanted to report her boyfriend [redacted] who was allegedly abusing her physically and emotionally , and wanted to speak to somebody about her situation because she had no one else to talk to about this subject matter. She claims the last time she was raped was [redacted]. The patient requested prophylaxis for possible STD exposure because she recently discovered that her present boyfriend was having sex with prostitutes[.]" The message contained other specific references to multiple patients, including the following: "[LINK OMITTED] She was pregnant [redacted]. One abortion after rape [redacted]. One early miscarriage."

v. On or about March 11, 2025, an INC ransomware negotiator who refers to himself as Andrew and Alexander contacted the SOFTWARE VICTIM informing the SOFTWARE VICTIM that they suffered a computer intrusion and seeking to negotiate.

w. On or about April 2, 2025, KHLYNOVSKIY and other conspirators caused a ransom payment of approximately $5,000,000 in bitcoin to be made by the CALIFORNIA HOSPITAL VICTIM.

x. Beginning on or about April 2, 2025, KHLYNOVSKIY and other conspirators started sending extortion communications to the SOFTWARE VICTIM through an encrypted email platform.

y. On or about April 11, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM, stating among other things: "Since you want to know our name, its a pleasure to introduce ourselves. Our name is 8-Digits Team. Friendly advice - if anybody else tries to contact you on behalf of your possible data breaches, you shouldnt even pay attention to those hilarious claims. We are ready to provide all kinds of proof further, when you are ready to request files."

z. On or about April 12, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM, stating, among other things: "Hi there. You should check this out, in order to catch a better grasp of this incident of ours. We are parsing your patients data with following keywords: HIV AIDS Hepatitis micropenis infertility syphilis erectile Gonorrhea Chlamydia Psoriasis eczema HPV Trichomoniasis autism Down syndrome rape

You can check the link in real time refreshing it, the parsed EMR files are going to appear there time to time:"

The threat actor then provided a hyperlink with access credentials.

The message continued, "…You may be curious, why would we do that? The

reason is simple. We are basically calculating approximate financials to determine the amount of our monetary demand. It might take us up to 1-2 weeks. You need to understand that our position here, allows us to earn money in a lot of ways, we do not really necessary have to cooperate with you, if you decide to cease all communications. However, we are here to cooperate, since we are interested in 1-time payout from you, without all that drudgery, and ruining your business in some way. You shall really advise with your lawyers, they will definitely tell you about the possible losses after data breach this big. Do you want to make the '[SOFTWARE VICTIM]' brand a part of this mess? Hope not. Confirm receival of this message."

aa. On or about April 13, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM, stating among other things: "…We are filtering all the data in our possession, in order to create a list of 500 most influential, powerful, and famous people. This will include top athletes, musicians, artists, top-ranking gov. employees, military servicemen, etc. We are pretty sure that there will be a couple of thousands EMR of people like this amongst the almost 100M we possess... Imagine the amount of moral damages cause to media famous people, after we leak private details on their medical histories. Part of this data is ready to go on a moment notice, to a dozen of lawfirms who are interested in suing you for huge compensations. Its not going to be charitable donations to them, we will arrange fixated % of profits in court, for providing this data."

bb. On or about April 16, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM, stating among other things: "As we already announced yesterday, we have already prepared our list of celebrities across US. There is almost 6k(+3k) of records there:..." The 8-Digits Team then provided a hyperlink and access credentials to download a file that contained a list of individuals to include high-ranking government officials, athletes, celebrities, and other high-profile individuals.

cc. On or about April 17, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM, stating among other things: "We are currently working on a script that will provide us with matches of VIP people across your clients data. The script is not working as fast as we thought it would, but it was still able to find some pretty interesting matches." The 8-Digits Team then provided a list of files that purported to be the medical records of [redacted] and [redacted]

dd. On or about April 18, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM demanding a ransom of $500,000,000 to be paid by the SOFTWARE VICTIM in order to prevent the release stolen data. The message also stated, among other things: "Reviewing everything we have, including VIP people EMR's, rape, substance abuse and STD's histories, millions of EMR files of your clients, we came to a conclusion that you are facing unbearable amount of damages." The 8-Digits Team then provided links to download the EMRs of "VIP people", including [redacted], and

[redacted] The 8-Digits Team also provided a link for [redacted], who the 8-Digits Team claimed has "confirmed HIV."

ee. On or about May 12, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM and claimed responsibility and credit for the December 2023 attack on the KENTUCKY HOSPITAL VICTIM, stating among other things: "P.S.

Since the scope of our incident with you is so large, a lot of people are affected - we will make a huge exception and act of a goodwill, showing you one client of ours. Exclusively for you to verify our credibility, based on how deal was concluded with them. Negotiations were ongoing on mid-December 2023, till the January 2024. They made a one time payment for purging their data - $9.000.000 We recommended them to report a small "possible" data breach in order to avoid huge fines and penalties. https://[KENTUCKY HOSPITAL VICTIM].com/data-breach

After that, everything was ok. Data was purged, incident kept private. We really hope that you are adequate and reasonable enough to keep this intel confidential as well. In case we find out this information got leaked - we are terminating our negotiations with you and proceed to our own actions immediately. No warnings are going to be made. Hope you understand…"

ff. On or about May 21, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM that contained a list of hospitals for which the conspiracy claimed to possess stolen data. That list included the CALIFORNIA HOSPITAL VICTIM with a notation that stated, "already paid".

gg. On or about June 2, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM that threatened to publish stolen data on a leak site created by the 8-Digits Team, stating among other things: "THE AVERAGE RANSOM PAYMENT WE GET FROM ONE HOSPITAL IS $5.000.000(as a goodwill gesture we did offer you to delete [ARKANSAS HOSPITAL VICTIM] data free of charge once you confirm your consent to one of our options, however you have not reacted) WE THOUGHT SO, YOU ARE DELAYING TIME AGAIN. We've been waiting for you to review you everything and make your mind for almost 2 months at the moment. We are sick of this...Thats why we were working whole weekend in order to build something we could show you that could possibly get your mind on a right track again. We invite you to explore our resource dedicated to YOUR cybersecurity incident. It is just the preview version now. However until Friday(6th of June) its going to be ready for publicity eyes - we will remove the password and publish this in the Web, UNLESS YOU RESOLVE THAT MATTER WITH US. IMPORTANT - FOR NOW ON AND FURTHER UNTIL FRIDAY(6th of June) THIS WEBSITE WILL BE PASSWORD PROTECTED. WE HAVE NOT SHARED THIS WEBSITE WITH ANYONE ELSE YET…" KHLYNOVSKIY and other conspirators then sent a hyperlink and credentials to access the leak site, which was on the dark web. The message continued, "…In case we do not get worthy offer which will satisfy us on Friday(6th of June) morning – we're turning our site over to news and media resources where we'll expose the data piece by piece, hospital by hospital, and blame you for the largest healthcare hack in history…"

hh. On or about June 3, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM providing a link to the leak site, stating among other things: "Since your C-level team probably does not have their own copy of Tor Browser, we decided to ease things up for them. Here is clearnet domain we prepared for them to better acknowledge contents of the website. 8digits-team.org [. . .] You're welcome. P.S. By the way, time is not in your favor." The leak site claimed that over 100 healthcare providers were affected, and that the 8-Digits Team possessed over 70 million customer records totaling over 50 terabytes.

ii. On or about June 11, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM, stating among other things: "[a] lot of world-level celebrities affected" and then referenced a list of individuals, including "[redacted]: Unspecified lump in the left breast, unspecified quadrant[.]"

jj. On or about June 23, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM that they would delete the records of several hospitals in exchange for a ransom payment of $3,000,000, stating among other things: "So, we confirm that we understand your chosen hospitals are: [NEW JERSEY HOSPITAL VICTIM] and [MISSOURI HOSPITAL VICTIM].(+ [ARKANSAS HOSPITAL VICTIM] free of charge)

We are already proceeding to necessary preparations in order to complete data removal as quick as possible.

1. We confirm our plans to delete these two hospitals' data. Once we confirm

payment on ourside, we will show you all of the data that's going to be purged with all according proof of data-removal."

kk. On or about June 27, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM that provided the bitcoin address for a ransom payment to be made.

ll. On or about June 27, 2025, KHLYNOVSKIY and other conspirators caused a ransom payment of approximately $3,000,000 in bitcoin to be made by the SOFTWARE VICTIM.

mm. On or about June 27, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM confirming receipt of payment and stating, among other things, "We are ready to provide you the evidence of data-removal process being completed."

nn. On or about July 7, 2025, KHLYNOVSKIY and other conspirators sent an encrypted email to the SOFTWARE VICTIM in the Eastern District of Tennessee, stating among other things, "We confirm that we will indeed delete any files that could be stored in other folders that related, with according evidence being provided to you. This goes for all of the hospitals." The email also included, among other things, a link to a "list of names of more than 70 medical providers including more than 120 hospitals[,]" different pricing models for the deletion of data measured by either the number of records or the number of hospitals, and demands for a "trust payment of $50M."

All in violation of 18 U.S.C. §§ 371 and 3559(g).

COUNT TWO
(Conspiracy to Commit Wire Fraud)

27. The allegations set forth in Paragraphs 1 through 22 and Paragraphs 24 through 26 are realleged as if fully set forth herein.

28. From on or about January 23, 2025, through on or about July 31, 2025, in the Eastern District of Tennessee and elsewhere, ROMAN KHLYNOVSKIY and others known and unknown to the Grand Jury, did knowingly, intentionally, and unlawfully combine, conspire, confederate, and agree with each other to commit offenses against the United States, to wit, wire fraud and honest services wire fraud in violation of 18 U.S.C. §§ 1343.

All in violation of 18 U.S.C. §§ 1349 and 3559(g).

COUNT THREE
(Extortion Involving Computers)

29. The allegations set forth in Paragraphs 1 through 22 and Paragraphs 24 through 26 are realleged as if fully set forth herein.

30. From on or about February 26, 2025, through on or about July 31, 2025, in the Eastern District of Tennessee and elsewhere, ROMAN KHLYNOVSKIY and others known and unknown to the Grand Jury, did knowingly and with intent to extort from any person any money or other thing of value, transmit in interstate and foreign commerce a 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 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—that is, the SOFTWARE VICTIM breach and data exfiltration—and knowingly aided and abetted others in doing the same and in attempting to do the same.

All in violation of 18 U.S.C. §§ 1030(a)(7)(B), 1030(a)(7)(C), 1030(c)(3)(A), 2, and 3559(g).

COUNT FOUR
(Conspiracy To Commit Money Laundering)

31. The allegations set forth in Paragraphs 1 through 22 and Paragraphs 24 through 26 are realleged as if fully set forth herein.

32. From on or about January 9, 2024, through on or about July 31, 2025, in the Eastern District of Tennessee and elsewhere, ROMAN KHLYNOVSKIY did knowingly combine, conspire, confederate, and agree with other persons known and unknown to the Grand Jury, to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, fraud and related activity in connection with computers, a violation of 18 U.S.C. §§ 1030(a)(5)(A) and 1030(a)(7)(C), knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of 18 U.S.C. §§ 1956(h) and 3559(g).

COUNT FIVE
(Threats to Commit Intentional Disclosure of Nonconsensual Intimate Images)

33. The allegations set forth in Paragraphs 1 through 22 and Paragraphs 24 through 26 are realleged as if fully set forth herein.

34. From on or after May 19, 2025, through on or about July 31, 2025, in the Eastern District of Tennessee and elsewhere, ROMAN KHLYNOVSKIY and others known and unknown

to the Grand Jury, for the purpose of intimidation, coercion, extortion, and to create mental distress, did intentionally threaten to, in interstate and foreign commerce, use an interactive computer service to knowingly publish intimate visual depictions of identifiable individuals who were not a minor, and the intimate visual depictions were obtained under circumstances in which KHLYNOVSKIY and his conspirators knew and reasonably should have known the identifiable individuals depicted therein had a reasonable expectation of privacy, what was depicted was not voluntarily exposed by the identifiable individuals in a public setting, what was depicted was not a matter of public concern, and the publication of the intimate visual depictions was intended to cause harm.

All in violation of 47 U.S.C. §§ 223(h)(6), 223(h)(2)(A), and 18 U.S.C. §§ 2 and 3559(g)

FORFEITURE ALLEGATION

35. The allegations contained in this Indictment are hereby realleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(1), 982(a)(2)(B), 1030(i), 28 U.S.C. § 2461(c) and 47 U.S.C. § 223(h)(7)(A).

36. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), upon conviction of an offense in violation of 18 U.S.C. § 371, the defendant shall forfeit to the United States, any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of 18 U.S.C. § 371.

37. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), upon conviction of an offense in violation of 18 U.S.C. § 1349, the defendant shall forfeit to the United States any property, real or personal, constituting or derived from proceeds traceable to a violation of 18 U.S.C. § 1349.

38. Upon conviction of an offense in violation of 18 U.S.C. § 1030, as set forth in this Indictment, the defendant shall forfeit to the United States of America:

a. 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

b. 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, and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

39. Pursuant to 18 U.S.C. § 982(a)(1), upon conviction of an offense in violation of 18 U.S.C. § 1956, as set forth in this Indictment, the defendant shall forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.

40. Pursuant to 47 U.S.C. § 223(h)(7)(A), upon conviction of an offense in violation of 47 U.S.C. § 223(h)(2), as set forth in the Indictment, the defendant shall forfeit to the United States any material distributed in violation of the offense, the person's interest in property, real or personal, constituting or derived from any gross proceeds of the violation, or any property traceable to such property, obtained or retained directly or indirectly as a result of the violation; and any personal property of the person used, or intended to be used, in any manner or part, to commit or to facilitate the commission of the violation.

41. All funds, including all cryptocurrency funds, associated with the following bitcoin wallets, bitcoin addresses, and cryptocurrency exchange accounts, are subject to forfeiture pursuant to paragraphs 35 through 40 above:

a. [redacted]

b.

c.

d.

e.

f.

g.

h.

i.

j.

k.

l.

m.

n.

o.

42. Pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. §§ 982(b)(1) and 1030(i)(2), 28 U.S.C. § 2461(c), and 47 U.S.C. § 223(h)(7)(B) the defendant shall forfeit substitute property, up to the value of the property subject to forfeiture, if by any act or omission of the defendant, said property, or any portion thereof:

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 that cannot be divided without difficulty.

A TRUE BILL.

SIGNATURE REDACTED

FOREPERSON

MATTHEW R. GALEOTTI
Acting Assistant Attorney General
Criminal Division

By: _____
Frank Lin
Senior Counsel

FRANCIS M. HAMILTON III
United States Attorney
Eastern District of Tennessee

By: _____
Jeremy Dykes
Assistant United States Attorney

CRIMINAL CASE COVER SHEET

By: ☒ INDICTMENT ☐ SUPERSEDING Case Number: 3:25-CR-84
☐ INFORMATION (*Requires AO 455 Waiver of Indictment for Felony Cases*)
☐ RULE 20

USA v. Roman Khlynovskiy a.k.a. ROMAN HLYNOVSKIY a.k.a. РОМАН ХЛЫНОВСКИЙ

☒ Felony ☐ Class A Misdemeanor (*AO 86A Consent form required at Initial Appearance*)
☐ Misdemeanor (Not Class A) ☐ Petty Offense

Immigration Cases
☐ Defendant is being added to existing criminal case ☐ Zone A ☐ Zone B
☐ Charges/Counts Added

Name of Assigned AUSA: Jeremy S. Dykes

Matter Sealed: ✕ YES NO Place of Offense: Knox County
☐ Interpreter Required Language:

Issued: ☐ WARRANT ☐ SUMMONS ☐ WRIT (*Motion to be filed*)

Arresting Agency: ☐ DEA ☐ ATF ☐ USMS ☒ FBI Other:

Current Trial Date (*if any*): before Judge

☐ Criminal Complaint Filed Case Number:
☐ Defendant on Supervised Release Case Number:

Related Case/Attorney:

Case Number: Attorney:

Reason for Related Case Determination:

Defense Counsel (*if any*):

☐ Federal Defender ☐ CJA ☐ Retained

Appointed by Target Letter Case Number:
Appointed in Pending Indictment Case Number:

CHARGES: Total number of Counts for this Defendant: 5

Attorney Signature: _____

CRIMINAL CASE COVER SHEET

Case Number: 3:25-CR-_____

USA v. Roman Khlynovskiy a.k.a. ROMAN HLYNOVSKIY a.k.a. РОМАН ХЛЫНОВСКИЙ

Title & Section	Description of Offense	New Count? Y or N	New Count#	Old Count#
18 U.S.C. §§ 371, 1028, 1030 and 3559(g)	Conspiracy to Commit Fraud and Related Activity in Connection with Computers and Identity Theft	Y	Y	
18 U.S.C. §§ 1349 and 3559(g)	Conspiracy to Commit Wire Fraud	Y	Y	
18 U.S.C. §§ 1030 (a)(7)(B) and (a)(7)(C), 2 and 3559(g)	Extortion Involving Computers	Y	Y	
18 U.S.C. §§ 1956 (h) and 3559(g)	Conspiracy to Commit Money Laundering	Y	Y	
47 U.S.C. § 223, 18 U.S.C. §§ 2 and 3559(g)	Threats to Commit Intentional Disclosure of Nonconsensual Intimate Images	Y	Y	