ISMAIL J. RAMSEY (CABN 189820)
United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. RUSLAN ALEKSANDROVICH PERETYATKO (ПЕРЕТЯТЬКО РУСЛАН АЛЕКСАНДРОВИЧ), and ANDREY STANISLAVOVICH KORINETS (КОРИНЕЦ АНДРЕЙ СТАНИСЛАВОВИЧ), Defendants.	CASE NO. CR23-00447CRB VIOLATIONS: 18 U.S.C. §§ 371, 1030(a)(2)(B) and (C), 1030(a)(5)(A) and 3559(g)(1) – Conspiracy to Commit Computer Fraud and Abuse; 18 U.S.C. §§ 982(a)(2)(B) and 1030(i) – Forfeiture Allegation SAN FRANCISCO VENUE

INDICTMENT

The Grand Jury charges:

Introductory Allegations

At all times relevant to this Indictment:

1. The Russian Federation ("Russia") operated an intelligence and law enforcement agency called the Federal Security Service ("FSB"). The FSB was headquartered in Moscow, Russia, and was comprised of multiple units, including one unit known within the FSB as "Center 18." An operational unit within FSB Center 18 known by cybersecurity investigators as the "Callisto Group" (also known as "Dancing Salome" by Kaspersky Labs, formerly known as "SEABORGIUM," and now known as

"STAR BLIZZARD" by Microsoft Threat Intelligence, and "COLDRIVER" by Google's Threat Analysis Group) and hereinafter referred to as the "Callisto Group," located in Russia.

2. The Callisto Group engaged in a sophisticated, global "spear phishing" campaign to target and gain unauthorized access and to maintain persistent access (i.e., "hack") into the computers and email accounts of targets in numerous countries, including North Atlantic Treaty Organization ("NATO") countries, particularly the United States ("U.S.") and the United Kingdom ("U.K."), as well as other countries such as Ukraine, that was designed to obtain unauthorized access to accounts and information for the benefit of the Russian government. "Spear phishing" is a type of phishing campaign that targets a specific person or group and often will include information known to be of interest to the target. Among the U.K. victims of this campaign were numerous U.K. political figures, think tank researchers and staff, and journalists. In one instance in December 2018, the Callisto Group successfully gained unauthorized access to victim accounts at a think tank in the U.K., and information from those accounts was later leaked to the press in both Russia and the U.K. in advance of U.K. elections in 2019.

3. As part of this campaign, as set forth in detail below, RUSLAN ALEKSANDROVICH PERETYATKO ("PERETYATKO") conspired with ANDREY STANISLAVOVICH KORINETS ("KORINETS") and other Callisto Group actors, known and unknown to the Grand Jury (collectively "the Conspirators"), in a sophisticated spear phishing campaign to target and gain unauthorized access and to maintain persistent access (i.e., "hack") into the computers and email accounts of current and former employees of the United States Intelligence Community ("USIC"), Department of Defense ("DOD"), Department of State ("DOS"), defense contractors, and the Department of Energy's ("DOE") facilities, in the Northern District of California and elsewhere in the United States.

4. The Conspirators' spear phishing campaign in the United States and elsewhere was designed to trick victims into providing their email account credentials and, through use of those credentials, gain unauthorized access to the victim email accounts. The Conspirators used "spoofed" email accounts designed to look like personal and work-related email accounts of current and former employees of the military, DOD, USIC, and DOE facilities, among others. Email spoofing is a technique used in spear phishing attacks to trick users into thinking a message came from a person or

entity they know or trust. The Conspirators also designed the spoofed email accounts to appear to be official email accounts from well-known email service providers. The spoofed email messages contained links to malicious domains and used authentic-looking wording and imagery to trick victims into clicking on the links. Those links led to false websites that were designed to induce the victims to enter their usernames and passwords, allowing the conspirators to harvest the targeted victims' credentials.

5. Once the Conspirators illegally obtained the targeted victims' credentials, they were able to gain unauthorized access to their accounts and take valuable intelligence from their victims' accounts at will, including intelligence related to United States defense, foreign affairs, and security policies, as well as nuclear energy related technology, research, and development. The Conspirators also used information contained in the compromised email accounts to make their spear phishing email accounts appear more authentic and convincing. Additionally, the Conspirators had the ability to reuse the stolen credentials to gain access to other personal and corporate accounts, as well as government portals, where the victim uses the same credentials.

6. Information related to United States defense, foreign affairs, and security policies, as well as nuclear energy related technology, would be particularly valuable to the Russian government's efforts to engage in malign foreign influence within the United States.

THE DEFENDANTS

7. Defendant, PERETYATKO, is a Russian national, and FSB officer, located in Syktyvkar, Komi Republic, Russia. PERETYATKO, among other things, conspired to spear phish the targeted victims, in support of the Conspirators' goal of obtaining unauthorized access to their targets' email accounts, to obtain information of value to the Russian government.

8. Defendant, KORINETS, is a Russian national, located in the Komi Republic, Russia. KORINETS registered and created infrastructure, including malicious domains for use in the spear phishing emails of the Conspirators, in support of the Conspirators' goal of obtaining unauthorized access to their targets' email accounts and related networks, to obtain information of value to the Russian government.

THE VICTIMS

9. Victims and targets of the conspiracy in the United States included:

a. Former members of the of the USIC;

b. Current and former United States DOS officials, including a retired United States Ambassador who resided in the Northern District of California;

c. Current and former DOD employees, including a retired Air Force General and an employee of a DOD institute, both of whom were located in the Northern District of California;

d. Current defense contractors;

e. Current employees at several of the DOE's 17 facilities across the United States, including in the Northern District of California, which are engaged in technological research and development on, among other things, nuclear energy and security, nuclear deterrence, military applications of nuclear science, global security, advance computing, and national security.

COUNT ONE: (18 U.S.C. § 371 – Conspiracy to Access a Computer Without Authorization and Obtain Information From a Protected Computer and a Government Agency; to Intentionally Cause Damage to a Protected Computer)

10. The allegations contained in paragraphs 1 through 9 are re-alleged here.

11. Beginning at a time unknown to the Grand Jury, but no later than in or about October 2016, and continuing through a date unknown to the Grand Jury, but at least through on or about October 4, 2022, in the Northern District of California and elsewhere, the defendants,

RUSLAN ALEKSANDROVICH PERETYATKO, and
ANDREY STANISLAVOVICH KORINETS,

knowingly and intentionally combined, conspired, confederated, and agreed together, with each other and with others known and unknown to the Grand Jury, to commit the following offenses against the United States:

a. Intentionally access computers without authorization, in the Northern District of California and elsewhere, and obtain thereby information from at least one protected computer, in furtherance of a criminal and tortious act in violation of the laws of California, that is, invasion of privacy, including a violation of California Penal Code Section 502, and where the value of the

information did, and would if completed, exceed $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii) and (iii);

b. Intentionally access computers without authorization, in the Northern District of California and elsewhere, and obtain thereby information from any department or agency of the United States, in furtherance of a criminal and tortious act in violation of the laws of California, that is, invasion of privacy, including a violation of California Penal Code Section 502, and where the value of the information did, and would if completed, exceed $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and 1030(c)(2)(B)(ii) and (iii);

c. Knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization to protected computers, and where the offense did cause and would, if completed, have caused loss during a one-year period aggregating at least $5,000, and damage affecting 10 or more protected computers during any one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B).

Manner And Means Of The Conspiracy

12. The Conspirators used the following manner and means to accomplish their objectives.

13. In furtherance of the conspiracy, the Conspirators attempted to reduce the likelihood of detection by victims and law enforcement by fraudulently registering, creating, and using infrastructure for a wide range of conduct, including the following:

a. Fraudulently registering and creating malicious domains designed to harvest credentials of their victims, using fictitious information to register those domains to thereby conceal their true identities, and using commonly used domain registrar services located both in and outside of the United States to avoid detection;

b. Using U.S.-based URL shortening services to obscure the domains of malicious links and then attaching these shortening links to spear phishing emails to facilitate harvesting credentials from victims who click on the malicious links;

c. Leasing Virtual Private Servers (a "VPS") for the malicious domains outside of the United States, and using fictitious information to register and pay for the VPS service, to thereby conceal their true identities and to hinder investigation by law enforcement;

d. Using "bulletproof hosting"/Virtual Private Network ("VPN") services for Conspirator-controlled infrastructure located in the U.S. A VPN service provides a secure, encrypted connection to a server or network. A bulletproof hosting service is technical infrastructure service provided by an Internet hosting service that is resilient to complaints of illicit activities.; and

e. Using Russian infrastructure located in Russia, for the purpose of transferring large amounts of data from other Conspirator-controlled infrastructure located in the U.S.

14. The Conspirators created and used spoofed email accounts mimicking legitimate persons in the USIC, defense, military, academic, and related communities as a means of inducing confidence about the validity of the emails to their victims. Using such spoofed email accounts of legitimate persons, the Conspirators' sent spear phishing emails that included actual signature lines obtained from their spoofed victims, again to induce confidence about the validity of the emails to their victims. Such spear phishing emails often contained PDF attachments with national security related titles that appeared official and that would appeal to the targeted victim, inducing the victim to open the spear phishing email and PDF, which then directed the targeted victim to a Conspirator-controlled domain that would require the victim to input their account credentials. In some instances, the Conspirators would send a spear phishing email that referred to an attachment that in fact was not attached in order to prompt the targeted victim to respond requesting the "missing" attachment. If the targeted victim replied, then the Conspirators would reply with a malicious attachment.

15. The Conspirators also created spoofed email accounts designed to appear to come from official service providers imploring the victim to enter their access credentials for security reasons. The Conspirators' spear phishing emails from these spoofed accounts, designed to look like official service provider accounts, often warned the targeted victim of a security or account problem and directed the victim to click the link contained in the email, which would direct the targeted victim to a Conspirator-controlled malicious domain designed to harvest the victim's account credentials.

16. The Conspirators would often create these spoofed email accounts and use them on the same day or shortly thereafter, using U.S.-based email services to conceal their location and identity.

17. In certain instances, after gaining unauthorized access to the victim email account, the Conspirators intentionally transmitted codes or commands to ensure that the victim was not notified by

their internal security services of suspicious emails, in order to maintain persistent access to the victim's email account.

18. Through such methods, the Conspirators were able to identify and access sensitive, private information, maintain persistent access to targeted victim accounts, and to obtain and to transfer information of value to the Russian government to infrastructure located in Russia.

OVERT ACTS

19. In furtherance of the conspiracy and to affect its objects, on or about the dates listed below, in the Northern District of California and elsewhere, KORINETS, PERETYATKO, and others, committed the following overt acts, among others:

Falsely Registered Domain Names Used for Credential Harvesting to Gain Unauthorized Access to Email Accounts

a. Between October 2016 and September 2020, KORINETS created and registered numerous malicious domains using false registration information. These domains were registered with commonly used domain name registrars, including domain registrars in the United States. Many of the malicious domains were used by the Conspirators for credential harvesting and were used in conjunction with URL shortening links that were created by the Conspirators using a U.S.-based URL shortening and link management provider.

i. KORINETS fraudulently registered and created malicious domains for use by the Conspirators, including the gsrv[.]site domain, which he created on or about February 2, 2017, and was hosted using a foreign-based VPS service. The Conspirators used the domain gsrv[.]site to conduct credential harvesting through spear phishing e-mails to their intended victims, as discussed below.

ii. Between January 25, 2019, and October 4, 2019, KORINETS fraudulently registered and created a number of domains with U.S.-based one domain name registrar. The domains included notification-node[.]online and en-microsofl[.]live, discussed below, which were used for credential harvesting by the Conspirators.

iii. Between October 14, 2019, and September 11, 2020, KORINETS fraudulently registered and created a number of domains with a U.S.-based domain name registrar

located in the Northern District of California. KORINETS fraudulently registered one particular domain, service-tech[.]website, on January 14, 2020, which was used for credential harvesting by the Conspirators, as discussed below. KORINETS further created two other malicious domains to mimic a U.K. public sector entity.

iv. Between September 2, 2019, and June 18, 2020, KORINETS fraudulently registered and created a number of domains with a foreign domain name registrar, including the domain service-online[.]top, which was used for credential harvesting by the Conspirators.

Spear Phishing Campaign Against Hundreds of Targeted Victims in the US Intelligence Community, the DOD, the DOS, Defense Contractors, and a DOD-Related Institute to Obtain Unauthorized Access to Their Email Accounts

b. PERETYATKO and his Conspirators created and used a number of other spoofed email accounts to mimic legitimate online management accounts, including msn.365.top[@]icloud.com, created on July 1, 2017, and cc.noreply_inc[@]icloud.com, created on or about March 30, 2017. The spear phishing account msn.365.top[@]icloud.com included a bookmark for a malicious domain that the Conspirators created on or about September 15, 2016, to mimic a U.K. public sector entity. The Conspirators used msn.365.top[@]icloud.com through at least January 2021.

c. In 2017, PERETYATKO and his Conspirators used the spoofed email account msn.365.top[@]icloud.com to send spear phishing emails to targeted victims, intended to obtain credentials from those victims, which included links to KORINETS's malicious domain gsrv[.]site. One such spear phishing email sent on September 4, 2017, purported to be a notice of unusual activity from Microsoft Corporation ("Microsoft") and directing the targeted victim, a military official from an Eastern European country, to change the account password, and linking the victim to the malicious domain.

d. In 2017, PERETYATKO and his Conspirators also used the spoofed email account cc.noreply_inc[@]icloud.com to send virtually identical spear phishing emails to targeted victims, and that included links to KORINETS's fraudulent domain gsrv[.]site. One such email was sent to a victim on or about June 12, 2017. The spear phishing email purported to be from Microsoft, advising of unusual activity on the account, and directing the victim to change the account password. The link re-directed to a malicious domain created by KORINETS.

e. On or about December 1, 2017 the Conspirators created a spoofed email account, ms.office.tearn[@]gmail.com, meant to mimic a legitimate Microsoft management account. Using this spoofed account, between approximately December 3, 2017, and August 21, 2020, the Conspirators sent thousands of spear phishing emails. Many of these spear phishing emails included links resolving to KORINETS's fraudulently created domain, service-tech[.]website and en-microsofl[.]live.

f. On or about May 15, 2018, the Conspirators sent spear phishing emails from account ms.office.tearn[@]gmail.com to an email account belonging to a retired Air Force General. Those emails contained a link to the malicious domain service-tech[.]website, which had been fraudulently created by KORINETS.

g. On or about August 16, 2019, the Conspirators sent spear phishing emails from ms.office.tearn[@]gmail.com to the same email account belonging to the retired Air Force General referenced above, each of which contained a link to the malicious domain en-microsofl[.]live, which KORINETS fraudulently created.

h. At least two individuals from the Northern District of California received spear phishing emails from ms.office.tearn[@]gmail.com. Specifically, on February 8, 2018, a former high-ranking DOS employee, who was at the time a military advisor and residing in the Northern District of California, received a spear phishing email from ms.office.tearn[@]gmail.com. The spear phishing email purported to be from Microsoft, advised of a terms of service violation, and instructed the victim to sign in and validate his/her Outlook.com account. The link re-directed to a malicious domain created by the Callisto Group on or about January 4, 2018.

i. Additionally, on August 19, 2019, an employee of a DOD institute, in the Northern District of California, received a spear phishing email from ms.office.tearn[@]gmail.com, purporting to be from Microsoft, advising of unusual activity on the account, and directing the victim to change the account password. The link re-directed to a malicious domain created by KORINETS on or about March 11, 2019, en-microsofl[.]live.

j. On or about August 27, 2019, the Conspirators registered and created a spoofed email account, r*******[@]gmail.com, intended to mimic a true email account used by the same retired Air Force General referenced above, and to be used for spear phishing. On or about December 10 and

11, 2019, using the above spoofed email account, the Conspirators sent an email to an individual who was retired from the U.S. military and a former member of the intelligence community, and was at the time a consultant on intelligence related matters. The email contained a subject line and attachment name "Nation State Sponsored Device Risks.pdf." The PDF contained an embedded link that when opened redirected to KORINETS's malicious domain, notification-node[.]online, created on October 4, 2019.

k. On or about July 10, 2018, the Conspirators created a spoofed email account k**********[@]gmail.com, that was designed to mimic the account of a national security reporter with access to the intelligence community. Using that spoofed email account, the Conspirators sent an email on or about December 5, 2019, to a targeted victim who was a former member of the intelligence community and was, at that time, a current U.S. government official. The email referenced a document and appeared to be an attempt to engage the victim in an email exchange and induce the victim to ask for the document.

l. On or about December 4, 2019, the Conspirators created a spoofed email account, aol.notification.manager[@]gmail.com**,** which was named to mimic a legitimate AOL management account. In all, between December 4, 2019 and at least March 3, 2020, the Conspirators used aol.notification.manager[@]gmail.com to send approximately 170 spear phishing emails to targeted victims. The emails cited "unusual activity" on the account and directed victims to change their passwords by clicking on the link in the email. The malicious links in at least 60 of the spear phishing emails sent from aol.notification.manager[@]gmail.com directed users to two malicious domains service-online[.]top, created on September 2, 2019, and notification-node[.]online, created on October 4, 2019, both by KORINETS. The Conspirators sent one such email on December 6, 2019, targeting a former member of the U.S. intelligence community who at the time taught at a military academy. The email contained a link, that, if clicked, would direct the victim to the malicious domain notification-node[.]online to harvest the victim's credentials. Another such email, sent on March 9, 2020, contained a link to the malicious domain service-online[.]top.

m. Using Conspirator-controlled IP addresses, the Conspirators transferred significant amounts of data between at least April and late October 2020 to an IP address registered in Russia.

Spear Phishing Campaign Against Department of Energy Facility Employees Using Government Email Accounts

n. In the spring of 2022, the Conspirators began directing their spear phishing campaign at several of the DOE's facilities. On or about May 30, 2022, the Conspirators created spoofed email account m***.********@outlook[.]com, designed to mimic a current DOS employee. Using this spoofed account, on or about May 30, 2022, the Conspirators sent a spear phishing email to an employee of a DOE facility, a nuclear engineer ("DOE Employee A"), at the employee's government email account. The email requested that DOE Employee A click the link. Days later, DOE Employee A clicked on the link and provided his/her work email account credentials. The Conspirators used the credentials to log into and maintain access to DOE Employee A's account. The Conspirators changed the account's inbox rule to automatically send any Information Technology department emails to DOE Employee A's deleted items folder, to prevent DOE Employee A from being alerted of the Conspirators' logins to the account.

o. In addition, the Conspirators created six additional spoofed email accounts between August 3 and 30, 2022, used to spear phish additional employees of the same DOE facility between those same dates. In particular, one spoofed email account, designed to mimic the personal email account of DOE Employee A, described above, c********[@]hotmail.com, was created on or about August 8, 2022, and sent a spear phishing email on that same date to an employee of the same DOE facility that contained a PDF with a link to a Conspirator-controlled domain.

p. On or about July 27 and 28, 2022, the Conspirators created spoofed email accounts designed to mimic employees from other DOE facilities, including j*******.********.****[@]gmail.com and k*******.********.****[@]gmail.com. Between on or about July 27, 2022, and September 30, 2022, the Conspirators used these email accounts to send spear phishing emails to a number of government employee email accounts at multiple DOE facilities. Some of the emails directed the victims to a document that was not attached, designed to engage in an email

response for the missing document and to later include the document. However, other emails included an attached PDF that, when clicked on, redirected to a Conspirator-controlled domain that required the entry of the victim's credentials to open the document. Specifically, on or about July 27, 2022, the Conspirators, using j*******.********.****[@]gmail.com, sent a spear phishing email to the government email address of an employee of a DOE facility, located in the Northern District of California, which contained a link to a Conspirator-controlled domain.

q. On or about September 28 and October 4, 2022, the Conspirators created two spoofed email accounts designed to mimic another employee of a DOE facility. Between September 29, 2022, and October 4, 2022, the Conspirators used these accounts to send spear phishing emails to government employee email accounts at multiple DOE facilities. In particular, on or about September 28, 2022, two employees at one DOE facility received a spear phishing email from t******.******[@]hotmail.com, that similarly referenced a document that was not attached. On or about September 29, 2022, one employee at that DOE facility responded, asking about the missing attachment. The Conspirators replied on or about September 30, 2022, this time including a PDF that contained a link to a Conspirator-controlled domain, created to harvest the victim's credentials.

All in violation of Title 18, United States Code, Sections 371 and 3559(g)(1).

FORFEITURE ALLEGATION: (18 U.S.C. § 982(a)(2)(B))

20. The allegations of this Indictment are re-alleged here for the purposes of alleging forfeiture pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

21. Upon conviction for the offenses alleged in Count One, the defendants,

RUSLAN ALEKSANDROVICH PERETYATKO, and
ANDREY STANISLAVOVICH KORINETS,

shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), any personal property used or intended to be used to commit or to facilitate the commission of said violations or a conspiracy to violate said provision, and any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, including, but not limited to, a sum of money equal to the total amount of proceeds defendant obtained or derived, directly or indirectly, from

the violations, or the value of the property used to commit or to facilitate the commission of said violations.

All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030, 981(a)(1)(C), 28 U.S.C. § 2461(C), and Federal Rule of Criminal Procedure 32.2.

DATED: 12/5/2023

A TRUE BILL.

/s/

_____
FOREPERSON

ISMAIL J. RAMSEY
United States Attorney

/s/ Martha A. Boersch

_____
MARTHA A. BOERSCH
Chief, Criminal Division