OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN VIEW

23 AUGUST 2022

(U//FOUO) SUBSTANTIVE REVISION: Russia: Cyber Threat Overview

(U//FOUO) This *Intelligence In View* provides federal, state, local, and private sector stakeholders an overview of Russian Government-affiliated cyber activity targeting the United States and Russian regional adversaries, including disruptive or destructive cyber activity, cyber espionage in support of intelligence collection, and malign foreign influence in service of Russian political agendas. This *In View* also provides examples of malware and tools used by Russian Government-affiliated cyber actors.

(U) CYBER THREAT TO THE HOMELAND

(U) Russia likely will remain a significant threat to US networks, data, and critical infrastructure as it refines and employs its sophisticated cyber espionage, influence, and attack capabilities, particularly in response to international pressure following its unprovoked attack on Ukraine. Russia has previously targeted critical infrastructure in the United States and allied countries to improve—and in some cases demonstrate—its ability to inflict damage during a crisis. Russia's use of destructive malware against Ukrainian infrastructure highlights the potential for such attacks to unintentionally spill over to other countries and threatens the availability of US critical assets and data. Russia will likely use these tools to compromise infrastructure and networks, acquire intellectual property and other proprietary data, undercut public trust in US institutions, and sow discord in the Homeland.

(U) TARGETING AND ATTACKS

(U) The Russian Government almost certainly considers cyber attacks an acceptable option to deter adversaries and control escalation. We have not yet observed Russian Government-affiliated actors conducting a destructive or disruptive cyber attack against the United States. However, Russian Government-affiliated cyber actors have targeted US industrial control system (ICS) and operational technology networks with malware, which, if successful, would provide the Russian Government with the option to conduct disruptive or destructive cyber attacks against US ICS. Russian Government-affiliated cyber actors have targeted a number of US industries and use a range of techniques to gain initial access to target networks. These actors have also demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments—including cloud environments—by using legitimate credentials. This access can enable cyber disruptions that could be used at a foreign policy level to shape other countries' decisions, as well as a deterrence and military tool.

(U) ESPIONAGE

(U//FOUO) Russian Government-affiliated cyber espionage is a persistent threat to federal, state, and local governments, as well as entities in the energy, aviation, transportation, healthcare, and telecommunications industries. Russian Government-affiliated cyber espionage actors support the Kremlin's intelligence requirements, build cyber attack capabilities, and provide Moscow with an asymmetric response to perceived transgressions by the West.

(U) INFLUENCE

(U) Russian Government-affiliated malign influence actors operate a network of state media outlets and covert online journals to amplify topics Russia perceives as divisive in the United States—such as vaccines, refugees and migrants, and mass shootings—likely to weaken US sociopolitical cohesion and undercut confidence in Western liberal democratic institutions. Moscow has used hack-and-leak operations to influence US elections—such as the leaking of 20,000 internal Democratic National Committee[USPER] e-mails during the 2016 presidential election—and to highlight perceived injustices—as with the targeting of the US Anti-Doping Agency[USPER]—resulting in the release of medical records of US athletes in retaliation for the banning of Russian athletes from the 2016 Summer Olympic Games. Moscow will continue to seek new methods of circumventing US social media companies' anti-disinformation activities to further expand its narratives globally.

(U) KEY CYBER OPERATIONS AGAINST THE HOMELAND

(U) In 2020, Russian Foreign Intelligence Service (SVR) cyber actors leveraged its compromise of Solarwinds' Orion platform to distribute the Sunburst malware to devices. Reporting indicates that the SVR used its access to exfiltrate sensitive data.

(U) From 2011 to 2018, Russian state-sponsored cyber actors conducted a multi-stage intrusion campaign to gain remote access to US and international energy sector networks, conduct network reconnaissance, stage ICS-focused malware, and collect ICS-related information. As part of this campaign, actors gained access to US networks that would enable future operations designed to damage power and power delivery systems.

(U) In 2017, Sandworm actors conducted a large-scale cyber attack infecting computers that attempted to update the Ukrainian accounting software M.E.Doc. Though initially targeting Ukraine, the malware spread to other countries, including the United States, causing nearly $1 billion worth of damage to US companies, including critical infrastructure sectors.

(U) In 2016, Russian Government-affiliated cyber actors used spear phishing to access multiple US Democratic National Committee organization networks. These actors later created multiple online personas to release and publicize exfiltrated election-related documents.

GRAPHIC CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Examples of Malware and Tools Used by Russian Government-Affiliated Cyber Actors

TYPE	NAMES
Backdoor	SUNBURST, CHOPSTICK, EVILTOSS, GOLDMAX, BOSSNAIL, SHRIME, AGENTBTZ, UROBUROS, BADBORSCH, CYCLOPSBLINK
Credential Stealer	TIGHTLOCK, OLDBAIT
Downloader	TRICKSHOW, DUSTSTONE, TINYTASK, SWIFTKICK, KINGCRAB, ONIONDUKE, TADPOLE, MSPROFILE, SOURFAC.CORESHELL, LAKESTONE, LONGCUT, GOFISH
Data Miner	DRUNKBEE, CARWRECK, CRASHDUMMY, WEIRDBIRD
Launcher	ARGUEPATCH, REDFISH, HEXCHAMBER, PLAYDATE
Privilege Escalation Tool	FLATTOP
Dropper	KINGPRAWN, TEARDROP, QUEENBEE, ROYALCOURT, GREEDYHEIR, SMALLBULB, VERNALDROP, OILYPART, SOFTSPOT, MILDMAP, PUREFARE, CHAINLNK, TREEBOOT
Tunneler	GARNETBOX, HTRAN, XTUNNEL
ICS-Capable	INDUSTROYER, TRITON, INDUSTROYER2, HAVEX, BLACKENERGY2
Wiper	NotPetya, HERMETICWIPER, WHISPERGATE, CADDYWIPER, ISSACWIPER, DOUBLEZERO
Web Shell	BLACKCROW
Utility	RUNHIDE, ZOOKEEPER

(U//FOUO) SUBSTANTIVE REVISION: Russia: Cyber Threat Overview (Cont.)

(U//FOUO) Appendix: Russian Government-Affiliated Actors' Common Tactics and Techniques, and Attributed Actor Aliases With Associated Targeted Entities

GRAPHIC CLASSIFICATION: UNCLASSIFIED

(U) Common Tactics and Techniques Employed by Russian Government-Affiliated Cyber Actors[a]

TACTIC	TECHNIQUE
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]
	Phishing for Information [T1598]
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]
Initial Access [TA0001]	Exploit Public-Facing Applications [T1190]
Command and Control	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]
Persistence [TA0003]	Valid Accounts [T1078]
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]
	OS Credential Dumping: NTDS [T1003.003]
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]
	Credentials From Password Stores [T1555]
	Exploitation for Credential Access [T1212]
	Unsecured Credentials: Private Keys [T1552.004]
Command and Control [TA0011]	Proxy: Multi-Hop Proxy [T1090.003]

[a] This table includes tactics and techniques that map to the MITRE ATT&CK for Enterprise framework, version 11. This framework provides a knowledge base of adversary tactics and techniques based on real-world observations. Tactics are the adversary's tactical objectives for performing an action. Each tactic consists of techniques that represent the action an adversary takes to achieve the tactical objective. Each tactic and technique has its own associated ID.

GRAPHIC CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

(U//FOUO) Russian Government-Affiliated Cyber Actors[b]

Name: Aliases *Latest Activity*	TARGETED ENTITIES	ATTRIBUTION
APT28, FANCY BEAR, STRONTIUM, Sednit, Sofacy, Pawn Storm, Group74, SNAKEMACKEREL, and Tsar Team *July 2021*	Government entities, US political parties, anti-chemical weapons organizations, anti-doping organizations, energy sector, educational institutions	Main Intelligence Directorate's (GRU's) Main Special Service Center (GTsSS) Unit 26165
APT29, COZY BEAR, CozyDuke, Dark Halo, The Dukes, NOBELIUM, StellarParticle, and YTTRIUM *July 2022*	US Government entities, research institutes, think tanks, political organizations	SVR
Sandworm, Voodoo Bear, ELECTRUM, IRON VIKING, Quedagh, and Telebots *2020*	Ukrainian energy sector, anti-chemical weapons organizations, government entities, political parties and campaigns, boards of elections, critical infrastructure	GRU's Main Center for Special Technologies (GTsST) Unit 74455
Turla, Venomous Bear, Uroburos, and Waterbug *October 2020*	Government entities, military, education, research, aerospace, telecommunications, pharmaceutical companies	Federal Security Service (FSB)
Energetic Bear, Berserk Bear, Dragonfly, Dragonfly 2.0, Crouching Yeti, and Temp.Isotope *October 2020*	State and local government entities, aviation, energy, ICS, critical infrastructure	FSB Center 16
XENOTIME and TEMP.Veles *October 2017*	ICS	Central Scientific Research Institute of Chemistry and Mechanics
Gamaredon and TEMP.Armageddon *August 2020*	US diplomatic entities	Office of the FSB of Russia in the Republic of Crimea and the city of Sevastopol

[b] This table includes a list of cyber actors that have been publicly assessed to be sponsored by the Russian Government. The authorities that have conducted this attribution include foreign governments and cybersecurity companies. This table does not represent DHS attribution of these cyber actors.

Source, Reference, and Dissemination Information

Prepared By	(U) Cyber Mission Center
Coordination	(U) NGA
For Questions, Contact	(U) DHS-SPS-RFI@hq.dhs.gov
Reporting Suspicious Activity	(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi. (U) To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form. The US-CERT Incident Reporting System provides a secure, web-enabled means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent.
Dissemination	(U) Federal, state, local, and private sector stakeholders.
Warning Notices & Handling Caveats	(U) **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY(U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS. (U) This product contains US person information that has been deemed necessary for the intended recipient to understand, assess, or act on the information provided. It has been highlighted in this document with the label USPER and should be handled in accordance with the recipient's intelligence oversight and/or information handling procedures. Other US person information has been minimized. For all other inquiries, please contact the Homeland Security Single Point of Service, Request for Information Office at DHS-SPS-RFI@hq.dhs.gov, DHS-SPS-RFI@dhs.sgov.gov, DHS-SPS-RFI@dhs.ic.gov.