Alert (AA22-011A)

Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure

Original release date: January 11, 2022

Note: *this advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 10. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.*

This joint Cybersecurity Advisory (CSA)—authored by the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA)—is part of our continuing cybersecurity mission to warn organizations of cyber threats and help the cybersecurity community reduce the risk presented by these threats. This CSA provides an overview of Russian state-sponsored cyber operations; commonly observed tactics, techniques, and procedures (TTPs); detection actions; incident response guidance; and mitigations. This overview is intended to help the cybersecurity community reduce the risk presented by these threats.

CISA, the FBI, and NSA encourage the cybersecurity community—especially critical infrastructure network defenders—to adopt a heightened state of awareness and to conduct proactive threat hunting, as outlined in the Detection section. Additionally, CISA, the FBI, and NSA strongly urge network defenders to implement the recommendations listed below and detailed in the Mitigations section. These mitigations will help organizations improve their functional resilience by reducing the risk of compromise or severe business degradation.

1. **Be prepared**. Confirm reporting processes and minimize personnel gaps in IT/OT security coverage. Create, maintain, and exercise a cyber incident response plan, resilience plan, and continuity of operations plan so that critical functions and operations can be kept running if technology systems are disrupted or need to be taken offline.

2. **Enhance your organization's cyber posture**. Follow best practices for identity and access management, protective controls and architecture, and vulnerability and configuration management.
3. **Increase organizational vigilance**. Stay current on reporting on this threat. Subscribe to CISA's mailing list and feeds to receive notifications when CISA releases information about a security topic or threat.

CISA, the FBI, and NSA encourage critical infrastructure organization leaders to review CISA Insights: Preparing for and Mitigating Cyber Threats for information on reducing cyber threats to their organization.

Click here for a PDF version of this report.

Technical Details

Historically, Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics—including spearphishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security—to gain initial access to target networks. Vulnerabilities known to be exploited by Russian state-sponsored APT actors for initial access include:

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare (note: this was a zero-day at time.)
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

Russian state-sponsored APT actors have also demonstrated sophisticated tradecraft and cyber capabilities by compromising third-party infrastructure, compromising third-party software, or developing and deploying custom malware. The actors have also demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments—including cloud environments—by using legitimate credentials.

In some cases, Russian state-sponsored cyber operations against critical infrastructure organizations have specifically targeted operational technology (OT)/industrial control systems (ICS) networks with destructive malware. See the following advisories and alerts

for information on historical Russian state-sponsored cyber-intrusion campaigns and customized malware that have targeted ICS:

- ICS Advisory ICS Focused Malware – Havex
- ICS Alert Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
- ICS Alert Cyber-Attack Against Ukrainian Critical Infrastructure
- Technical Alert CrashOverride Malware
- CISA MAR HatMan: Safety System Targeted Malware (Update B)
- CISA ICS Advisory Schneider Electric Triconex Tricon (Update B)

Russian state-sponsored APT actors have used sophisticated cyber capabilities to target a variety of U.S. and international critical infrastructure organizations, including those in the Defense Industrial Base as well as the Healthcare and Public Health, Energy, Telecommunications, and Government Facilities Sectors. High-profile cyber activity publicly attributed to Russian state-sponsored APT actors by U.S. government reporting and legal actions includes:

- **Russian state-sponsored APT actors targeting state, local, tribal, and territorial (SLTT) governments and aviation networks, September 2020, through at least December 2020.** Russian state-sponsored APT actors targeted dozens of SLTT government and aviation networks. The actors successfully compromised networks and exfiltrated data from multiple victims.
- **Russian state-sponsored APT actors' global Energy Sector intrusion campaign, 2011 to 2018.** These Russian state-sponsored APT actors conducted a multi-stage intrusion campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.
- **Russian state-sponsored APT actors' campaign against Ukrainian critical infrastructure, 2015 and 2016.** Russian state-sponsored APT actors conducted a cyberattack against Ukrainian energy distribution companies, leading to multiple companies experiencing unplanned power outages in December 2015. The actors deployed BlackEnergy malware to steal user credentials and used its destructive malware component, KillDisk, to make infected computers inoperable. In 2016, these actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed CrashOverride malware specifically designed to attack power grids.

For more information on recent and historical Russian state-sponsored malicious cyber activity, see the referenced products below or cisa.gov/Russia.

- Joint FBI-DHS-CISA CSA Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- Joint NSA-FBI-CISA CSA Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments
- Joint FBI-CISA CSA Russian State-Sponsored Advanced Persistent Threat Actor Compromises U.S. Government Targets

- Joint CISA-FBI CSA APT Actors Chaining Vulnerabilities against SLTT, Critical Infrastructure, and Elections Organizations
- CISA's webpage Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise
- CISA Alert Russian Government Cyber Activity Targeting Energy Sector and Other Critical Infrastructure Sectors
- CISA ICS Alert: Cyber-Attack Against Ukrainian Critical Infrastructure

Table 1 provides common, publicly known TTPs employed by Russian state-sponsored APT actors, which map to the MITRE ATT&CK for Enterprise framework, version 10. **Note:** these lists are not intended to be all inclusive. Russian state-sponsored actors have modified their TTPs before based on public reporting.[1] Therefore, CISA, the FBI, and NSA anticipate the Russian state-sponsored actors may modify their TTPs as they deem necessary to reduce their risk of detection.

Table 1: Common Tactics and Techniques Employed by Russian State-Sponsored APT Actors

Tactic	Technique	Procedure
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.
	Phishing for Information [T1598]	Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Russian state-sponsored APT actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Russian state-sponsored APT actors have used `cmd.exe` to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.
Persistence [TA0003]	Valid Accounts [T1078]	Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.

Tactic	Technique	Procedure
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Russian state-sponsored APT actors have conducted brute-force password guessing and password spraying campaigns.
	OS Credential Dumping: NTDS [T1003.003]	Russian state-sponsored APT actors have exfiltrated credentials and exported copies of the Active Directory database `ntds.dit`.
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Russian state-sponsored APT actors have performed "Kerberoasting," whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.
	Credentials from Password Stores [T1555]	Russian state-sponsored APT actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.
	Exploitation for Credential Access [T1212]	Russian state-sponsored APT actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.
	Unsecured Credentials: Private Keys [T1552.004]	Russian state-sponsored APT actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Russian state-sponsored APT actors have used virtual private servers (VPSs) to route traffic to targets. The actors often use VPSs with IP addresses in the home country of the victim to hide activity among legitimate user traffic.

For additional enterprise TTPs used by Russian state-sponsored APT actors, see the ATT&CK for Enterprise pages on APT29, APT28, and the Sandworm Team, respectively. For information on ICS TTPs see the ATT&CK for ICS pages on the Sandworm Team, BlackEnergy 3 malware, CrashOveride malware, BlackEnergy's KillDisk component, and NotPetya malware.

Detection

Given Russian state-sponsored APT actors demonstrated capability to maintain persistent, long-term access in compromised enterprise and cloud environments, CISA, the FBI, and NSA encourage all critical infrastructure organizations to:

- **Implement robust log collection and retention.** Without a centralized log collection and monitoring capability, organizations have limited ability to

investigate incidents or detect the threat actor behavior described in this advisory. Depending on the environment, examples include:
    - Native tools such as M365's Sentinel.
    - Third-party tools, such as Sparrow, Hawk, or CrowdStrike's Azure Reporting Tool (CRT), to review Microsoft cloud environments and to detect unusual activity, service principals, and application activity. **Note:** for guidance on using these and other detection tools, refer to CISA Alert Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments.

- **Look for behavioral evidence or network and host-based artifacts** from known Russian state-sponsored TTPs. See table 1 for commonly observed TTPs.
    - To detect password spray activity, review authentication logs for system and application login failures of valid accounts. Look for multiple, failed authentication attempts across multiple accounts.
    - To detect use of compromised credentials in combination with a VPS, follow the below steps:
        - Look for suspicious "impossible logins," such as logins with changing username, user agent strings, and IP address combinations or logins where IP addresses do not align to the expected user's geographic location.
        - Look for one IP used for multiple accounts, excluding expected logins.
        - Look for "impossible travel." Impossible travel occurs when a user logs in from multiple IP addresses that are a significant geographic distance apart (i.e., a person could not realistically travel between the geographic locations of the two IP addresses during the time period between the logins). **Note:** implementing this detection opportunity can result in false positives if legitimate users apply VPN solutions before connecting into networks.
        - Look for processes and program execution command-line arguments that may indicate credential dumping, especially attempts to access or copy the `ntds.dit` file from a domain controller.
        - Look for suspicious privileged account use after resetting passwords or applying user account mitigations.
        - Look for unusual activity in typically dormant accounts.
        - Look for unusual user agent strings, such as strings not typically associated with normal user activity, which may indicate bot activity.

- For organizations with OT/ICS systems:
    - Take note of unexpected equipment behavior; for example, unexpected reboots of digital controllers and other OT hardware and software.
    - Record delays or disruptions in communication with field equipment or other OT devices. Determine if system parts or components are lagging or unresponsive.

Incident Response

Organizations detecting potential APT activity in their IT or OT networks should:

1. Immediately isolate affected systems.
2. Secure backups. Ensure your backup data is offline and secure. If possible, scan your backup data with an antivirus program to ensure it is free of malware.
3. Collect and review relevant logs, data, and artifacts.
4. Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.
5. Report incidents to CISA and/or the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Note: for OT assets, organizations should have a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment. Refer to the Mitigations section for more information.

See the joint advisory from Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for guidance on hunting or investigating a network, and for common mistakes in incident handling. CISA, the FBI, and NSA encourage critical infrastructure owners and operators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail each step for both incident and vulnerability response.

Note: organizations should document incident response procedures in a cyber incident response plan, which organizations should create and exercise (as noted in the Mitigations section).

Mitigations

CISA, the FBI, and NSA encourage all organizations to implement the following recommendations to increase their cyber resilience against this threat.

Be Prepared

Confirm Reporting Processes and Minimize Coverage Gaps

- Develop internal contact lists. Assign main points of contact for a suspected incident as well as roles and responsibilities and ensure personnel know how and when to report an incident.
- Minimize gaps in IT/OT security personnel availability by identifying surge support for responding to an incident. Malicious cyber actors are known to target organizations on weekends and holidays when there are gaps in organizational cybersecurity—critical infrastructure organizations should proactively protect themselves by minimizing gaps in coverage.

- Ensure IT/OT security personnel monitor key internal security capabilities and can identify anomalous behavior. Flag any identified IOCs and TTPs for immediate response. (See table 1 for commonly observed TTPs).

Create, Maintain, and Exercise a Cyber Incident Response, Resilience Plan, and Continuity of Operations Plan

- Create, maintain, and exercise a cyber incident response and continuity of operations plan.
- Ensure personnel are familiar with the key steps they need to take during an incident and are positioned to act in a calm and unified manner. Key questions:
    - Do personnel have the access they need?
    - Do they know the processes?
- For OT assets/networks,
    - Identify a resilience plan that addresses how to operate if you lose access to—or control of—the IT and/or OT environment.
        - Identify OT and IT network interdependencies and develop workarounds or manual controls to ensure ICS networks can be isolated if the connections create risk to the safe and reliable operation of OT processes. Regularly test contingency plans, such as manual controls, so that safety critical functions can be maintained during a cyber incident. Ensure that the OT network can operate at necessary capacity even if the IT network is compromised.
    - Regularly test manual controls so that critical functions can be kept running if ICS or OT networks need to be taken offline.
    - Implement data backup procedures on both the IT and OT networks. Backup procedures should be conducted on a frequent, regular basis. Regularly test backup procedures and ensure that backups are isolated from network connections that could enable the spread of malware.
    - In addition to backing up data, develop recovery documents that include configuration settings for common devices and critical OT equipment. This can enable more efficient recovery following an incident.

Enhance your Organization's Cyber Posture

CISA, the FBI, and NSA recommend organizations apply the best practices below for identity and access management, protective controls and architecture, and vulnerability and configuration management.

Identity and Access Management

- Require multi-factor authentication for all users, without exception.
- Require accounts to have strong passwords and do not allow passwords to be used across multiple accounts or stored on a system to which an adversary may have access.
- Secure credentials. Russian state-sponsored APT actors have demonstrated their ability to maintain persistence using compromised credentials.

    - Use virtualizing solutions on modern hardware and software to ensure credentials are securely stored.
    - Disable the storage of clear text passwords in LSASS memory.
    - Consider disabling or limiting New Technology Local Area Network Manager (NTLM) and WDigest Authentication.
    - Implement Credential Guard for Windows 10 and Server 2016 (Refer to Microsoft: Manage Windows Defender Credential Guard for more information). For Windows Server 2012R2, enable Protected Process Light for Local Security Authority (LSA).
    - Minimize the Active Directory attack surface to reduce malicious ticket-granting activity. Malicious activity such as "Kerberoasting" takes advantage of Kerberos' TGS and can be used to obtain hashed credentials that attackers attempt to crack.
- Set a strong password policy for service accounts.
- Audit Domain Controllers to log successful Kerberos TGS requests and ensure the events are monitored for anomalous activity.
    - Secure accounts.
    - Enforce the principle of least privilege. Administrator accounts should have the minimum permission they need to do their tasks.
    - Ensure there are unique and distinct administrative accounts for each set of administrative tasks.
    - Create non-privileged accounts for privileged users and ensure they use the non- privileged accounts for all non-privileged access (e.g., web browsing, email access).

Protective Controls and Architecture

- Identify, detect, and investigate abnormal activity that may indicate lateral movement by a threat actor or malware. Use network monitoring tools and host-based logs and monitoring tools, such as an endpoint detection and response (EDR) tool. EDR tools are particularly useful for detecting lateral connections as they have insight into common and uncommon network connections for each host.
- Enable strong spam filters.
    - Enable strong spam filters to prevent phishing emails from reaching end users.
    - Filter emails containing executable files to prevent them from reaching end users.
    - Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments.

Note: CISA, the FBI, and NSA also recommend, as a longer-term effort, that critical infrastructure organizations implement network segmentation to separate network segments based on role and functionality. Network segmentation can help prevent lateral movement by controlling traffic flows between—and access to—various subnetworks.

- Appropriately implement network segmentation between IT and OT networks. Network segmentation limits the ability of adversaries to pivot to the OT network even if the IT network is compromised. Define a demilitarized zone that eliminates unregulated communication between the IT and OT networks.
- Organize OT assets into logical zones by taking into account criticality, consequence, and operational necessity. Define acceptable communication conduits between the zones and deploy security controls to filter network traffic and monitor communications between zones. Prohibit ICS protocols from traversing the IT network.

Vulnerability and Configuration Management

- Update software, including operating systems, applications, and firmware on IT network assets, in a timely manner. Prioritize patching known exploited vulnerabilities, especially those CVEs identified in this CSA, and then critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
    - Consider using a centralized patch management system. For OT networks, use a risk-based assessment strategy to determine the OT network assets and zones that should participate in the patch management program.
    - Consider signing up for CISA's cyber hygiene services, including vulnerability scanning, to help reduce exposure to threats. CISA's vulnerability scanning service evaluates external network presence by executing continuous scans of public, static IP addresses for accessible services and vulnerabilities.
- Use industry recommended antivirus programs.
    - Set antivirus/antimalware programs to conduct regular scans of IT network assets using up-to-date signatures.
    - Use a risk-based asset inventory strategy to determine how OT network assets are identified and evaluated for the presence of malware.
- Implement rigorous configuration management programs. Ensure the programs can track and mitigate emerging threats. Review system configurations for misconfigurations and security weaknesses.
- Disable all unnecessary ports and protocols
    - Review network security device logs and determine whether to shut off unnecessary ports and protocols. Monitor common ports and protocols for command and control activity.
    - Turn off or disable any unnecessary services (e.g., PowerShell) or functionality within devices.
- Ensure OT hardware is in read-only mode.

Increase Organizational Vigilance

- Regularly review reporting on this threat. Consider signing up for CISA notifications to receive timely information on current security issues, vulnerabilities, and high-impact activity.

Resources

- For more information on Russian state-sponsored malicious cyber activity, refer to cisa.gov/Russia.
- Refer to CISA Analysis Report Strengthening Security Configurations to Defend Against Attackers Targeting Cloud Services for steps for guidance on strengthening your organizations cloud security practices.
- Leaders of small businesses and small and local government agencies should see CISA's Cyber Essentials for guidance on developing an actionable understanding of implementing organizational cybersecurity practices.
- Critical infrastructure owners and operators with OT/ICS networks, should review the following resources for additional information:
    - NSA and CISA joint CSA NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems
    - CISA factsheet Rising Ransomware Threat to Operational Technology Assets for additional recommendations.

Rewards for Justice Program

If you have information on state-sponsored Russian cyber operations targeting U.S. critical infrastructure, contact the Department of State's Rewards for Justice Program. You may be eligible for a reward of up to $10 million, which DOS is offering for information leading to the identification or location of any person who, while acting under the direction or control of a foreign government, participates in malicious cyber activity against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA). Contact +1-202-702-7843 on WhatsApp, Signal, or Telegram, or send information via the Rewards for Justice secure Tor-based tips line located on the Dark Web. For more details refer to rewardsforjustice.net/malicious_cyber_activity.

Caveats

The information you have accessed or received is being provided "as is" for informational purposes only. CISA, the FBI, and NSA do not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA, the FBI, or NSA.

References

[1] Joint NCSC-CISA UK Advisory: Further TTPs Associated with SVR Cyber Actors

Revisions

January 11, 2022: Initial Version