JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: JCSA-20241010-001

October 10, 2024

Update on SVR Cyber Operations and Vulnerability Exploitation

SUMMARY

The Federal Bureau of Investigation (FBI), the National Security Agency (NSA), Cyber National Mission Force (CNMF), and the United Kingdom's National Cyber Security Centre (NCSC-UK) are releasing this joint Cybersecurity Advisory (CSA) to highlight the tactics, techniques, and procedures (TTPs) employed by the Russian Federation's Foreign Intelligence Service (SVR) in recent cyber operations and provide network defenders with information to help counter SVR cyber threats.

Since at least 2021, Russian SVR cyber actors – also tracked as APT29, Midnight Blizzard (formerly Nobelium), Cozy Bear, and the Dukes – have consistently targeted US, European, and global entities in the defense, technology, and finance sectors to collect foreign intelligence and enable future cyber operations, including in support of Russia's ongoing invasion of Ukraine since February 2022. Their operations continue to pose a global threat to government and private sector organizations.

The authoring agencies are releasing this CSA to warn network defenders that SVR cyber actors are highly capable of and interested in exploiting software vulnerabilities for initial access [T1190] and escalation of privileges [T1068]. Organizations should prioritize rapid patch deployment and keep software up to date. The SVR continues using TTPs such as spearphishing [T1566], password spraying [T1078], abuse of supply chain [T1195] and trusted relationships [T1199], custom and

The authoring agencies recommend the following mitigations to protect their networks. See the **Mitigations** section for the complete list.

- Reduce attack surface by disabling Internet-accessible services that you do not need, or restrict access to trusted networks, and removing unused applications and utilities from workstations and development environments.
- Require and enforce multi-factor authentication whenever possible.
- Regularly audit cloud-based accounts and applications with administrative access to email for unusual activity.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA cybersecurity reporting inquiries, contact CybersecurityReports@nsa.gov.

bespoke malware, cloud exploitation, and living-off-the-land techniques to gain initial access, escalate privileges, move laterally, maintain persistence in victim networks and cloud environments, and exfiltrate information. SVR actors often use The Onion Router (TOR) network, leased and compromised infrastructure, and proxies to obfuscate activity.

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 15.1. See the ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to ATT&CK tactics and techniques. For assistance with mapping malicious cyber activity to the ATT&CK framework, see Best Practices for MITRE ATT&CK Mapping and Decider Tool.

Victims

SVR cyber operations generally have two types of intended victims: targets of intent and targets of opportunity.

Targets of intent include government and diplomatic entities, technology companies, think tanks, international organizations, and cleared defense contractors. These groups are targeted for the purpose of collecting foreign intelligence and technical data as well as establishing accesses to enable subsequent downstream/supply chain compromises. These targets include governments and organizations in North America and Western Europe as well as public and private sector organizations in Asia, Africa, Russia's near abroad, and South America. Since 2021, SVR cyber operations have continued against Ukraine, likely in support of Russian war efforts.

Targets of opportunity represent entities with Internet-accessible infrastructure vulnerable to exploitation through publicly disclosed vulnerabilities, weak authentication controls, or system misconfigurations. SVR cyber operators consistently scan Internet-facing systems for unpatched vulnerabilities. This mass scanning and opportunistic exploitation of vulnerable systems, as opposed to more targeted operations, increase the threat surface to include virtually any organization with vulnerable systems. The SVR takes advantage of opportunistic victims to host malicious infrastructure, conduct follow-on operations from compromised accounts, or to attempt to pivot to other networks.

- In 2023, SVR cyber actors conducted opportunistic exploitation of a JetBrains TeamCity CVE to target an energy trade association, software development firms, hosting companies, tools manufacturers, and information technology companies.
- Also in 2023, SVR cyber actors used Microsoft Teams accounts impersonating technical support entities to send spearphishing messages [T1566] via Microsoft Teams Chat to socially engineer the victims to grant the actors account access. The campaign was enabled by compromises of poorly secured Microsoft customer tenants operated by numerous small businesses [T1584.005]. After obtaining access to those small businesses' accounts, the SVR created platforms in those victim environments to enable operations targeting their intended victim organizations, which included government agencies, technology and manufacturing firms, and non-governmental organizations.

Infrastructure

SVR cyber intrusions include a heavy focus on remaining anonymous and undetected. The actors use TOR extensively throughout intrusions – from initial targeting to data collection – and across network infrastructure. The actors lease operational infrastructure using a variety of fake identities and low reputation email accounts [T1583]. The SVR obtains infrastructure from resellers of major hosting providers.

When the SVR suspects their intrusions have been identified by their victim or law enforcement, they quickly attempt to destroy their infrastructure and any evidence on it. To remain undetected, the SVR frequently uses tools and programs already on victim networks to avoid anti-virus software. During intrusions into cloud environments, the SVR exploits misconfigurations and weak access controls to access information without the need for additional software.

Additionally, SVR infrastructure used to directly interact with victims located in North America almost exclusively consists of endpoints associated with one or more proxy networks [T1665]. These proxy networks, which frequently use networks associated with mobile telephone providers or residential Internet services, are used to attempt to blend in with legitimate users of the victims' network and avoid connections originating from IP addresses associated with datacenters or commercial VPN providers.

To disrupt this activity, organizations should baseline authorized devices and apply additional scrutiny to systems accessing their network resources that do not adhere to the baseline.

Vulnerability Exploitation

In April 2021, the US, UK, and Canadian governments published a joint CSA highlighting the SVR's exploitation of CVEs for initial access. Since then, SVR cyber actors have exploited vulnerabilities at a mass scale to target victims worldwide across a variety of sectors, including:

- **CVE-2022-27924:** CVE-2022-2794 is a command injection vulnerability [CWE-74] that allows an unauthenticated attacker to inject arbitrary memcache commands into a targeted Zimbra instance, causing an overwrite of arbitrary cached entries. SVR cyber actors exploited Zimbra mail servers targeting hundreds of domains worldwide, including through exploitation of the CVE. This allowed the actors to access user credentials and mailboxes without victim interaction. Following the exploitation of those systems, the SVR deployed infrastructure to enable collection from the victims.
- **CVE-2023-42793:** Starting in September 2023, SVR cyber actors have exploited JetBrains TeamCity CVE-2023-42793, which enabled arbitrary code execution via insecure handling of specific paths allowing for authentication bypass.

Based on the SVR cyber actors' TTPs and previous targeting, the authoring agencies assess they have the capability and interest to exploit additional CVEs for initial access, remote code execution, and privilege escalation, including the ones listed below. The below CVEs have all been publicly disclosed; organizations should implement vendor-issued security patches if they have not already.

Table 1: CVEs

CVE	Vendor/Product	Details
CVE-2023-20198	Cisco IOS XE Software web UI feature	Privilege escalation vulnerability [CWE-269] that allows an attacker to create a local user and password combination
CVE-2023-4911	RHSA GNU C Library's dynamic loader ld.so	Buffer overflow vulnerability [CWE-122] that could allow a local attacker to execute code with elevated privileges
CVE-2023-38545	Haxx Libcurl	SOCKS5 heap buffer overflow vulnerability [CWE-122]
CVE-2023-38546	Haxx Libcurl	Missing authorization vulnerability [CWE-862] that allows an attacker to insert cookies in a running program if certain conditions are met
CVE-2023-40289	Supermicro X11SSM-F, X11SAE-F, and X11SSE-F 1.66	Command injection vulnerability [CWE-74] that allows an attacker to elevate privileges
CVE-2023-24023	Bluetooth BR/EDR devices with Secure Simple Pairing and Secure Connections pairing in Bluetooth Core Specification 4.2 through 5.4	Allows certain man-in-the-middle attacks [CWE-300] that force a short key length [CWE-326], and might lead to discovery of the encryption key and live injection, aka BLUFFS.
CVE-2023-40088	Android	Use after free [CWE-416] vulnerability that could lead to remote (proximal, adjacent) code execution
CVE-2023-40076	Google Android 14.0	Permissions bypass vulnerability [CWE-200] that allows an attacker to access credentials and escalate local privileges
CVE-2023-40077	Google Android 11-14	Use after free [CWE-416] vulnerability that can lead to escalation of privileges
CVE-2023-45866	Bluetooth HID Hosts in BlueZ	Improper authentication vulnerability [CWE-287] that could allow an attacker in close proximity to inject keystrokes and carry out arbitrary commands
CVE-2022-40507	Qualcomm	Double free vulnerability [CWE-415]

CVE-2023-36745	Microsoft Exchange Server	Remote code execution [CWE-502]
CVE-2023-4966	Citrix NetScaler ADC, NetScaler Gateway	Buffer overflow vulnerability [CWE-119]
CVE-2023-6345	Google Chrome	Integer overflow vulnerability [CWE-190] that allows a remote attacker to potentially perform a sandbox escape via a malicious file
CVE-2023-37580	Zimbra	Cross-site scripting (XSS) vulnerability [CWE-79]
CVE-2021-27850	Apache Tapestry	Critical unauthenticated remote code execution vulnerability [CWE-502]
CVE-2021-41773	Apache HTTP server 2.4.99	Directory traversal vulnerability [CWE-35]
CVE-2021-42013	Apache HTTP server 2.4.50	Remote code execution vulnerability [CWE-22]
CVE-2018-13379	Fortinet FortiGate SSL VPN	Path traversal vulnerability [CWE-35]
CVE-2023-42793	JetBrains TeamCity	Authentication bypass vulnerability [CWE-288]
CVE-2023-29357	SharePoint Server	Elevation of privilege vulnerability [CWE-303]
CVE-2023-24955	SharePoint Server	Remote code execution vulnerability [CWE-94]
CVE-2023-35078	Ivanti Endpoint Manager Mobile versions through 11.10	Authentication bypass vulnerability [CWE-288]
CVE-2023-5044	Kubernetes Ingress-nginx	Code injection vulnerability [CWE-94]

ATT&CK TACTICS AND TECHNIQUES

See table 2 for all referenced threat actor tactics and techniques in this advisory.

Table 2: SVR ATT&CK Techniques for Enterprise

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	The actors exploit multiple CVEs for initial access and/or privilege escalation.
Escalation of privileges	T1068	The actors escalate privileges on a compromised host.
Phishing	T1566	The actors commonly conduct spear phishing campaigns.
Valid accounts	T1078	The actors conduct password spraying to access victim environments.
Compromise software supply chain	T1195.002	The actors use trojanized software updates to compromise downstream customers.
Trusted Relationship	T1199	The actors abuse trusted relationships to target other connections.
Compromise Infrastructure	T1584	The actors compromise infrastructure to incorporate in future operations.
Hide Infrastructure	T1665	The actors use residential proxies and TOR to obfuscate infrastructure.
Acquire Infrastructure	T1583	The actors use cryptocurrencies, fake identities, and low reputation email accounts to lease infrastructure.
Compromise Infrastructure: Botnet	T1584.005	The actors compromise numerous third-party systems to form a botnet.

MITIGATIONS

The authoring agencies recommend organizations implement the mitigations below to improve your organization's cybersecurity posture on the basis of the threat actor's activity.

- Prioritize rapid deployment of patches and software updates as soon as they become available. Enable automatic updates where possible.
- Reduce attack surface by disabling Internet-accessible services that you do not need, or restrict access to trusted networks, and removing unused applications and utilities from workstations and development environments.
- Perform continuous threat hunting activities.
- Ensure proper configuration of systems – check for open ports and obsolete or unused protocols, especially on Internet-facing systems.
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce exposure of internal networks.
- Require and enforce multi-factor authentication whenever possible.
- Require additional identity challenges for enrollment of new devices when users are permitted to self-enroll multi-factor authentication mechanisms or register devices on the corporate network.
- Notify users across multiple platforms when devices have been successfully registered to help identify unexpected registrations. Train and encourage users to notice and report unexpected registrations.
- Enable robust logging for authentication services and Internet-facing functions.
- Regularly audit cloud-based accounts and applications with administrative access to email for unusual activity.
- Limit token access lifetimes and monitor for evidence of token reuse.
- Enforce least-privileged access and disable external management capabilities.
- Baseline authorized devices and apply additional scrutiny to systems accessing network resources that do not adhere to the baseline.
- Disable remote downloading of information to non-enrolled devices when possible.

The authoring agencies recommend testing your existing security controls to assess how they perform against the techniques described in this advisory.

REFERENCES

NSA, FBI, CISA Cybersecurity Advisory Russian SVR Targets U.S. and Allied Networks

FBI, DHS Joint Cybersecurity Advisory Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders

UK NCSC, CISA, FBI, NSA Advisory Further TTPs associated with SVR cyber actors

UK NCSC, CISA, CNMF, FBI, NSA, ASD ACSC, CCCS, NZ NCSC Joint Cybersecurity Advisory SVR Cyber Actors Adapt Tactics for Initial Cloud Access (AA24-057A)

FBI, CISA, NSA, UK NCSC, SKW, CERT.PL Joint Cybersecurity Advisory Russian Foreign Intelligence Service (SVR) Exploiting JetBrains TeamCity CVE Globally (AA23-347A)

DISCLAIMER

VERSION HISTORY

October 10, 2024: Initial version.