



Russian GRU Targeting Western Logistics Entities and Technology Companies

Executive Summary

This joint cybersecurity advisory (CSA) highlights a Russian state-sponsored cyber campaign targeting Western logistics entities and technology companies. This includes those involved in the coordination, transport, and delivery of foreign assistance to Ukraine. Since 2022, Western logistics entities and IT companies have faced an elevated risk of targeting by the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (85th GTsSS), military unit 26165—tracked in the cybersecurity community under several names (see "Cybersecurity Industry Tracking"). The actors' cyber espionage-oriented campaign, targeting technology companies and logistics entities, uses a mix of previously disclosed tactics, techniques, and procedures (TTPs). The authoring agencies expect similar targeting and TTP use to continue.

Executives and network defenders at logistics entities and technology companies should recognize the elevated threat of unit 26165 targeting, increase monitoring and threat hunting for known TTPs and indicators of compromise (IOCs), and posture network defenses with a presumption of targeting.

This cyber espionage-oriented campaign targeting logistics entities and technology companies uses a mix of previously disclosed TTPs and is likely connected to these actors' wide scale targeting of IP cameras in Ukraine and bordering NATO nations.

The following authors and co-sealers are releasing this CSA:

- United States National Security Agency (NSA)
- United States Federal Bureau of Investigation (FBI)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- Germany Federal Intelligence Service (BND)[1]
- Germany Federal Office for Information Security (BSI)[2]
- Germany Federal Office for the Protection of the Constitution (BfV)[3]
- Czech Republic Military Intelligence (VZ)[4]
- Czech Republic National Cyber and Information Security Agency (NÚKIB)[5]
- Czech Republic Security Information Service (BIS)[6]
- Poland Internal Security Agency (ABW)[7]
- Poland Military Counterintelligence Service (SKW)[8]
- United States Cybersecurity and Infrastructure Security Agency (CISA)
- United States Department of Defense Cyber Crime Center (DC3)
- United States Cyber Command (USCYBERCOM)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Canadian Centre for Cyber Security (CCCS)
- Danish Defence Intelligence Service (DDIS)[9]
- Estonian Foreign Intelligence Service (EFIS)[10]
- Estonian National Cyber Security Centre (NCSC-EE)[11]
- French Cybersecurity Agency (ANSSI)[12]
- Netherlands Defence Intelligence and Security Service (MIVD)[13]

[1] Bundesnachrichtendienst
[2] Bundesamt für Sicherheit in der Informationstechnik
[3] Bundesamt für Verfassungsschutz
[4] Vojenské zpravodajství
[5] Národní úřad pro kybernetickou a informační bezpečnost
[6] Bezpečnostní informační služba
[7] Agencja Bezpieczeństwa Wewnętrznego
[8] Służba Kontrwywiadu Wojskowego
[9] Forsvarets Efterretningstjeneste
[10] Välisluureamet
[11] Küberturvalisuse keskus
[12] Agence nationale de la sécurité des systèmes d'information
[13] Militaire Inlichtingen- en Veiligheidsdienst

Introduction

For over two years, the Russian GRU 85th GTsSS, military unit 26165—commonly known in the cybersecurity community as APT28, Fancy Bear, Forest Blizzard, BlueDelta, and a variety of other identifiers—has conducted this campaign using a mix of known tactics, techniques, and procedures (TTPs), including reconstituted password spraying capabilities, spearphishing, and modification of Microsoft Exchange mailbox permissions.

In late February 2022, multiple Russian state-sponsored cyber actors increased the variety of cyber operations for purposes of espionage, destruction, and influence—with unit 26165 predominately involved in espionage. [1] As Russian military forces failed to meet their military objectives and Western countries provided aid to support Ukraine's territorial defense, unit 26165 expanded its targeting of logistics entities and technology companies involved in the delivery of aid. These actors have also targeted Internet-connected cameras at Ukrainian border crossings to monitor and track aid shipments.

Note: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 17. See Appendix A: MITRE ATT&CK tactics and techniques for a table of the threat actors' activity mapped to MITRE ATT&CK tactics and techniques. This advisory uses the MITRE D3FEND® framework, version 1.0.

Description of Targets

The GRU unit 26165 cyber campaign against Western logistics providers and technology companies has targeted dozens of entities, including government organizations and private/commercial entities across virtually all transportation modes: air, sea, and rail. These actors have targeted entities associated with the following verticals within NATO member states, Ukraine, and at international organizations:

- Defense Industry
- Transportation and Transportation Hubs (ports, airports, etc.)
- Maritime
- Air Traffic Management
- IT Services

In the course of the targeting lifecycle, unit 26165 actors identified and conducted follow-on targeting of additional entities in the transportation sector that had business

ties to the primary target, exploiting trust relationships to attempt to gain additional access [T1199].

The actors also conducted reconnaissance on at least one entity involved in the production of industrial control system (ICS) components for railway management, though a successful compromise was not confirmed [TA0043].

The countries with targeted entities include the following, as illustrated in Figure 1:

- Bulgaria
- Czech Republic
- France
- Germany
- Greece
- Italy
- Moldova
- Netherlands
- Poland
- Romania
- Slovakia
- Ukraine
- United States

Figure 1: Countries with Targeted Entities

Initial Access TTPs

To gain initial access to targeted entities, unit 26165 actors used several techniques to gain initial access to targeted entities, including (but not limited to):

- Credential guessing [T1110.001] / brute force [T1110.003]
- Spearphishing for credentials [T1566]
- Spearphishing delivering malware [T1566]
- Outlook NTLM vulnerability (CVE-2023-23397)
- Roundcube vulnerabilities (CVE-2020-12641, CVE-2020-35730, CVE-2021-44026)
- Exploitation of Internet-facing infrastructure, including corporate VPNs [T1133], via public vulnerabilities and SQL injection [T1190]
- Exploitation of WinRAR vulnerability (CVE-2023-38831)

The actors abused vulnerabilities associated with a range of brands and models of small office/home office (SOHO) devices to facilitate covert cyber operations, as well as proxy malicious activity via devices with geolocation in proximity to the target [T1665]. [2]

Credential Guessing/Brute Force

Unit 26165 actors' credential guessing [T1110.001] operations in this campaign exhibit some similar characteristics to those disclosed in the previous CSA "Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments." [3] Based on victim network investigations, the current iteration of this TTP employs a similar blend of anonymization infrastructure, including the use of Tor and commercial VPNs [T1090.003]. The actors frequently rotated the IP addresses used to further hamper detection. All observed connections were made via encrypted TLS [T1573].

Spearphishing

GRU unit 26165 actors' spearphishing emails included links [T1566.002] leading to fake login pages impersonating a variety of government entities and Western cloud email providers' webpages. These webpages were typically hosted on free third-party services or compromised SOHO devices and often used legitimate documents associated with thematically similar entities as lures. The subjects of spearphishing emails were diverse and ranged from professional topics to adult themes. Phishing emails were frequently sent via compromised accounts or free webmail accounts [T1586.002, T1586.003]. The emails were typically written in the target's native language and sent to a single targeted recipient.

Some campaigns employed multi-stage redirectors [T1104] verifying IP-geolocation [T1627.001] and browser fingerprints [T1627] to protect credential harvesting infrastructure or provide multifactor authentication (MFA) [T1111] and CAPTCHA relaying capabilities [T1056]. Connecting endpoints failing the location checks were redirected to a benign URL [T1627], such as msn.com. Redirector services used include:

- Webhook[.]site
- FrgeIO
- InfinityFree

- Dynu
- Mocky
- Pipedream
- Mockbin[.]org

The actors also used spearphishing to deliver malware (including HEADLACE and MASEPIE) executables [T1204.002] delivered via third-party services and redirectors [T1566.002], scripts in a mix of languages [T1059] (including BAT [T1059.003] and VBScript [T1059.005]) and links to hosted shortcuts [T1204.001].

CVE Usage

Throughout this campaign, GRU unit 26165 weaponized an Outlook NTLM vulnerability (CVE-2023-23397) to collect NTLM hashes and credentials via specially crafted Outlook calendar appointment invitations [T1187]. [4], [5] These actors also used a series of Roundcube CVEs (CVE-2020-12641, CVE-2020-35730, and CVE-2021-44026) to execute arbitrary shell commands [T1059], gain access to victim email accounts, and retrieve sensitive data from email servers [T1114].

Since at least fall 2023, the actors leveraged a WinRAR vulnerability (CVE-2023-38831) allowing for the execution of arbitrary code embedded in an archive as a means of initial access [T1659]. The actors sent emails with malicious attachments [T1566.001] or embedded hyperlinks [T1566.002] that downloaded a malicious archive prepared using this CVE.

Post-Compromise TTPs

After an initial compromise using one of the above techniques, unit 26165 actors conducted contact information reconnaissance to identify additional targets in key positions [T1589.002]. The actors also conducted reconnaissance of the cybersecurity department [T1591], individuals responsible for coordinating transport [T1591.004], and other companies cooperating with the victim entity [T1591.002].

The actors used native commands and open source tools, such as Impacket and PsExec, to move laterally within the environment [TA0008]. Multiple Impacket scripts were used as .exe files, in addition to the python versions, depending on the victim environment. The actors also moved laterally within the network using Remote Desktop Protocol (RDP) [T1021.001] to access additional hosts and attempt to dump Active

Directory NTDS.dit domain databases [T1003.003] using native Active Directory Domain Services commands, such as in Figure 2: Example Active Directory Domain Services command:

```
C:\Windows\system32\ntdsutil.exe "activate instance ntds" ifm "create full C:\temp\[a-z]{3}"
quit quit
```

Figure 2: Example Active Directory Domain Services command

Additionally, GRU unit 26165 actors used the tools Certipy and ADExplorer.exe to exfiltrate information from the Active Directory. The actors installed python [T1059.006] on infected machines to enable the execution of Certipy. Accessed files were archived in .zip files prior to exfiltration [T1560]. The actors attempted to exfiltrate archived data via a previously dropped OpenSSH binary [T1048].

Incident response investigations revealed that the actors would take steps to locate and exfiltrate lists of Office 365 users and set up sustained email collection. The actors used manipulation of mailbox permissions [T1098.002] to establish sustained email collection at compromised logistics entities, as detailed in a Polish Cybercommand blog. [6]

After initial authentication, unit 26165 actors would change accounts' folder permissions and enroll compromised accounts in MFA mechanisms to increase the trust-level of compromised accounts and enable sustained access [T1556.006]. The actors leveraged python scripts to retrieve plaintext passwords via Group Policy Preferences [T1552.006] using Get-GPPPassword.py and a modified ldap-dump.py to enumerate the Windows environment [T1087.002] and conduct a brute force password spray [T1110.003] via Lightweight Directory Access Protocol (LDAP). The actors would additionally delete event logs through the wevtutil utility [T1070.001].

After gaining initial access to the network, the actors pursued further access to accounts with access to sensitive information on shipments, such as train schedules and shipping manifests. These accounts contained information on aid shipments to Ukraine, including:

- sender,
- recipient,
- train/plane/ship numbers,
- point of departure,
- destination,
- container registration numbers,

- travel route, and
- cargo contents.

In at least one instance, the actors attempted to use voice phishing [T1566.004] to gain access to privileged accounts by impersonating IT staff.

Malware

Unit 26165's use of malware in this campaign ranged from gaining initial access to establishing persistence and exfiltrating data. In some cases, the attack chain resulted in multiple pieces of malware being deployed in succession. The actors used dynamic link library (DLL) search order hijacking [T1574.001] to facilitate malware execution. There were a number of known malware variants tied to this campaign against logistics sector victims, including:

- HEADLACE [7]
- MASEPIE [8]

While other malware variants, such as OCEANMAP and STEELHOOK, [8] were not directly observed targeting logistics or IT entities, their deployment against victims in other sectors in Ukraine and other Western countries suggest that they could be deployed against logistics and IT entities should the need arise.

Persistence

In addition to the abovementioned mailbox permissions abuse, unit 26165 actors also used scheduled tasks [T1053.005], run keys [T1547.001], and placed malicious shortcuts [T1547.009] in the startup folder to establish persistence.

Exfiltration

GRU unit 26165 actors used a variety of methods for data exfiltration that varied based on the victim environment, including both malware and living off the land binaries. PowerShell commands [T1059.001] were often used to prepare data for exfiltration; for example, the actors prepared zip archives [T1560.001] for upload to their own infrastructure.

The actors also used server data exchange protocols and Application Programming Interfaces (APIs) such as Exchange Web Services (EWS) and Internet Message Access Protocol (IMAP) [T1114.002] to exfiltrate data from email servers. In multiple

instances, the actors used periodic EWS queries [T1119] to collect new emails sent and received since the last data exfiltration [T1029]. The actors typically used infrastructure in close geographic proximity to the victim. Long gaps between exfiltration, the use of trusted and legitimate protocols, and the use of local infrastructure allowed for long-term collection of sensitive data to go undetected.

Connections to Targeting of IP Cameras

In addition to targeting logistics entities, unit 26165 actors likely used access to private cameras at key locations, such as near border crossings, military installations, and rail stations, to track the movement of materials into Ukraine. The actors also used legitimate municipal services, such as traffic cams.

The actors targeted Real Time Streaming Protocol (RTSP) servers hosting IP cameras primarily located in Ukraine as early as March 2022 in a large-scale campaign, which included attempts to enumerate devices [T1592] and gain access to the cameras' feeds [T1125]. Actor-controlled servers sent RTSP DESCRIBE requests destined for RTSP servers, primarily hosting IP cameras [T1090.002]. The DESCRIBE requests were crafted to obtain access to IP cameras located on logically distinct networks from that of the routers that received the request. The requests included Base64-encoded credentials for the RTSP server, which included publicly documented default credentials and likely generic attempts to brute force access to the devices [T1110]. An example of an RTSP request is shown in Figure 1Figure 3.

```
DESCRIBE rtsp://[IP ADDRESS] RTSP/1.0
CSeq: 1
Authorization: Basic <Base64-encoded credentials>
User-Agent: WebClient
Accept: application/sdp

DESCRIBE rtsp://[IP ADDRESS] RTSP/1.0
CSeq: 2
Authorization: Digest username="admin", realm="[a-f0-9]{12}", algorithm="MD5", nonce="[a-f0-
9]{32}", uri="", response="[a-f0-9]{32}"
User-Agent: WebClient
Accept: application/sdp
```

Figure 3: Example RTSP request

Successful RTSP 200 OK responses contained a snapshot of the IP camera's image and IP camera metadata such as video codec, resolution, and other properties depending on the IP camera's configuration.

From a sample available to the authoring agencies of over 10,000 cameras targeted via this effort, the geographic distribution of victims showed a strong focus on cameras in Ukraine and border countries, as shown in Table 1:

Table 1: Geographic distribution of targeted IP cameras

Country	Percentage of Total Attempts
Ukraine	81.0%
Romania	9.9%
Poland	4.0%
Hungary	2.8%
Slovakia	1.7%
Others	0.6%

Mitigation Actions

General Security Mitigations

Architecture and Configuration

- Employ appropriate network segmentation [D3-NI] and restrictions to limit access and utilize additional attributes (such as device information, environment, and access path) when making access decisions [D3-AMED].
    - Consider Zero Trust principles when designing systems. Base product choices on how those products can solve specific risks identified as part of the end-to-end design. [9]
- Ensure that host firewalls and network security appliances (e.g., firewalls) are configured to only allow legitimately needed data flows between devices and servers to prevent lateral movement [D3-ITF]. Alert on attempts to connect laterally between host devices or other unusual data flows.
- Use automated tools to audit access logs for security concerns and identify anomalous access requests [D3-RAPA].
- For organizations using on-premises authentication and email services, block and alert on NTLM/SMB requests to external infrastructure [D3-OTF].

- Utilize endpoint, detection, and response (EDR) and other cybersecurity solutions on all systems, prioritizing high value systems with large amounts of sensitive data such as mail servers and domain controllers [D3-PM] first.
    - Perform threat and attack modeling to understand how sensitive systems may be compromised within an organization's specific architecture and security controls. Use this to develop a monitoring strategy to detect compromise attempts and select appropriate products to enact this strategy.
- Collect and monitor Windows logs for certain events, especially for events that indicate that a log was cleared unexpectedly [D3-SFA].
- Enable optional security features in Windows to harden endpoints and mitigate initial access techniques [D3-AH]:
    - Enable attack surface reduction rules to prevent executable content from email [D3-ABPI].
    - Enable attack surface reduction rules to prevent execution of files from globally writeable directories, such as Downloads or %APPDATA% [D3-EAL].
    - Unless users are involved in the development of scripts, limit the local execution of scripts (such as batch scripts, VBScript, JScript/JavaScript, and PowerShell [10]) to known scripts [D3-EI], and audit execution attempts.
    - Disable Windows Host Scripting functionality and configure PowerShell to run in Constrained mode [D3-ACH].
- Where feasible, implement allowlisting for applications and scripts to limit execution to only those needed for authorized activities, blocking all others by default [D3-EAL].
- Consider using open source SIGMA rules as a baseline for detecting and alerting on suspicious file execution or command parameters [D3-PSA].
- Use services that provide enhanced browsing services and safe link checking [D3-URA]. Significant reductions in successful spearphishing attempts were noted when email providers began offering link checking and automatic file detonation to block malicious content.
- Where possible, block logins from public VPNs, including exit nodes in the same country as target systems, or, if they need to be allowed, alert on them for further

investigation. Most organizations should not need to allow incoming traffic, especially logins to systems, from VPN services [D3-NAM].
- Educate users to only use approved corporate systems for relevant government and military business and avoid the use of personal accounts on cloud email providers to conduct official business. Network administrators should also audit both email and web request logs to detect such activity.

Many organizations may not need to allow outgoing traffic to hosting and API mocking services, which are frequently used by GRU unit 26165. Organizations should consider alerting on or blocking the following services, with exceptions allowlisted for legitimate activity [D3-DNSDL].

- *.000[.]pe
- *.1cooldns[.]com
- *.42web[.]io
- *.4cloud[.]click
- *.accesscan[.]org
- *.bumbleshrimp[.]com
- *.camdvr[.]org
- *.casacam[.]net
- *.ddnsfree[.]com
- *.ddnsgeek[.]com
- *.ddnsguru[.]com
- *.dynuddns[.]com
- *.dynuddns[.]net
- *.free[.]nf
- *.freeddns[.]org
- *.frge[.]io
- *.glize[.]com
- *.great-site[.]net
- *.infinityfreeapp[.]com
- *.kesug[.]com
- *.loseyourip[.]com
- *.lovestoblog[.]com
- *.mockbin[.]io
- *.mockbin[.]org
- *.mocky[.]io
- *.mybiolink[.]io
- *.mysynology[.]net
- *.mywire[.]org
- *.ngrok[.]io
- *.ooguy[.]com
- *.pipedream[.]net
- *.rf[.]gd
- *.urlbae[.]com
- *.webhook[.]site
- *.webhookapp[.]com
- *.webredirect[.]org
- *.wuaze[.]com

Heuristic detections for web requests to new subdomains, including of the above providers, may uncover malicious phishing activity [D3-DNRA]. Logging the requests for each sub-domain requested by users on a network, such as in DNS or firewall logs, may enable system administrators to identify new targeting and victims.

Identity and Access Management

Organizations should take measures to ensure strong access controls and mitigate against common credential theft techniques:

- Use MFA with strong factors, such as passkeys or PKI smartcards, and require regular re-authentication [D3-MFA]. [11], [12] Strong authentication factors are not guessable using dictionary techniques, so they resist brute force attempts.

- Implement other mitigations for privileged accounts: including limiting the number of admin accounts, considering using hardware MFA tokens, and regularly reviewing all privileged user accounts [D3-JFAPA].
- Separate privileged accounts by role and alert on misuse of privileged accounts [D3-UAP]. For example, email administrator accounts should be different from domain administrator accounts.
- Reduce reliance on passwords; instead, consider using services like single sign-on [D3-TBA].
    - For organizations using on-premises authentication and email services, plan to disable NTLM entirely and migrate to more robust authentication processes such as PKI certificate authentication.
- Do not store passwords in Group Policy Preferences (GPP). Remove all passwords previously included in GPP and change all passwords on the corresponding accounts [D3-CH]. [13]
- Use account throttling or account lockout [D3-ANET]:
    - Throttling is preferred to lockout. Throttling progressively increases time delay between successive login attempts.
    - Account lockout can leave legitimate users unable to access their accounts and requires access to an account recovery process.
    - Account lockout can provide a malicious actor with an easy way to launch a Denial of Service (DoS).
    - If using lockout, then allowing 5 to 10 attempts before lockout is recommended.
- Use a service to check for compromised passwords before using them [D3-SPP]. For example, “Have I Been Pwned” can be used to check whether a password has been previously compromised without disclosing the potential password.
- Change all default credentials [D3-CRO] and disable protocols that use weak authentication (e.g., clear-text passwords or outdated and vulnerable authentication or encryption protocols) or do not support multi-factor authentication [D3-ACH] [D3-ET]. Always configure access controls carefully to ensure that only well-maintained and well-authenticated accounts have access. [13]

IP Camera Mitigations

The following mitigation techniques for IP cameras can be used to defend against this type of malicious activity:

- Ensure IP cameras are currently supported. Replace devices that are out of support.
- Apply security patches and firmware updates to all IP cameras [D3-SU].
- Disable remote access to the IP camera, if unnecessary [D3-ITF].
- Ensure cameras are protected by a security appliance, if possible, such as by using a firewall to prevent communication with the camera from IP addresses not on an allowlist [D3-NAM].
- If remote access to IP camera feeds is required, ensure authentication is enabled [D3-AA] and use a VPN to connect remotely [D3-ET]. Use MFA for management accounts if supported [D3-MFA].
- Disable Universal Plug and Play (UPnP), Peer-to-Peer (P2P), and Anonymous Visit features on IP cameras and routers [D3-NI].
- Turn off other ports/services not in use (e.g., FTP, web interface, etc.) [D3-ACH].
- If supported, enable authenticated RTSP access only [D3-AA].
- Review all authentication activity for remote access to make sure it is valid and expected [D3-UBA]. Investigate any unexpected or unusual activity.
- Audit IP camera user accounts to ensure they are an accurate reflection of your organization and that they are being used as expected [D3-UAP].
- Configure, tune, and monitor logging—if available—on the IP camera.

Indicators of Compromise (IOCs)

Note: Specific IoCs may no longer be actor controlled, may themselves be compromised infrastructure or email accounts, or may be shared infrastructure such as public VPN or Tor exit nodes. Care should be taken when basing triaging logs or developing detection rules on these indicators. GRU unit 26165 almost certainly uses extensive further infrastructure and TTPs not specifically listed in this report.

Utilities and scripts

Legitimate utilities

Unauthorized or unusual use of the following legitimate utilities can be an indication of a potential compromise:

- ntdsutil – A legitimate Windows executable used by threat actors to export contents of Active Directory

- wevtutil – A legitimate Windows executable used by threat actors to delete event logs
- vssadmin – A legitimate Windows executable possibly used by threat actors to make a copy of the server's C: drive
- ADexplorer – A legitimate window executable to view, edit, and backup Active Directory Certificate Services
- OpenSSH – The Windows version of a legitimate open source SSH client
- schtasks – A legitimate Windows executable used to create persistence using scheduled tasks
- whoami – A legitimate Windows executable used to retrieve the name of the current user
- tasklist – A legitimate Windows executable used to retrieve the list of running processes
- hostname – A legitimate Windows executable used to retrieve the device name
- arp – A legitimate Windows executable used to retrieve the ARP table for mapping the network environment
- systeminfo – A legitimate Windows executable used to retrieve a comprehensive summary of device and operating system information
- net – A legitimate Windows executable used to retrieve detailed user information
- wmic – A legitimate Windows executable used to interact with Windows Management Instrumentation (WMI), such as to retrieve letters assigned to logical partitions on storage drives
- cacls – A legitimate Windows executable used to modify permissions on files
- icacls – A legitimate Windows executable used to modify permissions to files and handle integrity levels and ownership
- ssh – A legitimate Windows executable used to establish network shell connections
- reg – A legitimate Windows executable used to add to or modify the system registry

Note: Additional heuristics are needed for effective hunting for these and other living off the land (LOTL) binaries to avoid being overwhelmed by false positives if these legitimate management tools are used regularly. See the joint guide, Identifying and Mitigating Living Off the Land Techniques, for guidance on developing a multifaceted cybersecurity strategy that enables behavior analytics, anomaly detection, and proactive hunting, which are part of a comprehensive approach to mitigating cyber threats that employ LOTL techniques.

Malicious scripts

- Certipy – An open source python tool for enumerating and abusing Active Directory Certificate Services
- Get-GPPPassword.py – An open source python script for finding insecure passwords stored in Group Policy Preferences
- ldap-dump.py – A script for enumerating user accounts and other information in Active Directory
- Hikvision backdoor string: “YWRtaW46MTEK”

Suspicious command lines

While the following utilities are legitimate, and using them with the command lines shown may also be legitimate, these command lines are often used during malicious activities and could be an indication of a compromise:

- edge.exe “-headless-new -disable-gpu”
- ntdsutil.exe "activate instance ntds" ifm "create full C:\temp\[a-z]{3}" quit quit
- ssh -Nf
- schtasks /create /xml

Outlook CVE Exploitation IOCs

- md-shoeb@alfathdoor[.]com[.]sa
- jayam@wizzsolutions[.]com
- accounts@regencyservice[.]in
- m.salim@tsc-me[.]com
- vikram.anand@4ginfosource[.]com
- mdelafuente@ukwwfze[.]com
- sarah@cosmicgold469[.]co[.]za
- franch1.lanka@bplanka[.]com
- commerical@vanadrink[.]com
- maint@goldenloaduae[.]com
- karina@bhpcapital[.]com
- tv@coastalareabank[.]com
- ashoke.kumar@hbclife[.]in
- 213[.]32[.]252[.]221
- 124[.]168[.]91[.]178
- 194[.]126[.]178[.]8
- 159[.]196[.]128[.]120

Commonly Used Webmail Providers

- portugalmail[.]pt
- mail-online[.]dk
- email[.]cz
- seznam[.]cz

Malicious Archive Filenames Involving CVE-2023-38831

- calc.war.zip
- news_week_6.zip
- Roadmap.zip
- SEDE-PV-2023-10-09-1_EN.zip
- war.zip
- Zeyilname.zip

Brute Forcing IP Addresses

Disclaimer: These IP addresses date June 2024 through August 2024. The authoring agencies recommend organizations investigate or vet these IP addresses prior to taking action, such as blocking.

June 2024	July 2024	August 2024		
192[.]162[.]174[.]94	207[.]244[.]71[.]84	31[.]135[.]199[.]145	79[.]184[.]25[.]198	91[.]149[.]253[.]204
103[.]97[.]203[.]29	162[.]210[.]194[.]2	31[.]42[.]4[.]138	79[.]185[.]5[.]142	91[.]149[.]254[.]75
209[.]14[.]71[.]127		46[.]112[.]70[.]252	83[.]10[.]46[.]174	91[.]149[.]255[.]122
109[.]95[.]151[.]207		46[.]248[.]185[.]236	83[.]168[.]66[.]145	91[.]149[.]255[.]19
		64[.]176[.]67[.]117	83[.]168[.]78[.]27	91[.]149[.]255[.]195
		64[.]176[.]69[.]196	83[.]168[.]78[.]31	91[.]221[.]88[.]76
		64[.]176[.]70[.]18	83[.]168[.]78[.]55	93[.]105[.]185[.]139
		64[.]176[.]70[.]238	83[.]23[.]130[.]49	95[.]215[.]76[.]209
		64[.]176[.]71[.]201	83[.]29[.]138[.]115	138[.]199[.]59[.]43
		70[.]34[.]242[.]220	89[.]64[.]70[.]69	147[.]135[.]209[.]245
		70[.]34[.]243[.]226	90[.]156[.]4[.]204	178[.]235[.]191[.]182
		70[.]34[.]244[.]100	91[.]149[.]202[.]215	178[.]37[.]97[.]243
		70[.]34[.]245[.]215	91[.]149[.]203[.]73	185[.]234[.]235[.]69
		70[.]34[.]252[.]168	91[.]149[.]219[.]158	192[.]162[.]174[.]67
		70[.]34[.]252[.]186	91[.]149[.]219[.]23	194[.]187[.]180[.]20
		70[.]34[.]252[.]222	91[.]149[.]223[.]130	212[.]127[.]78[.]170
		70[.]34[.]253[.]13	91[.]149[.]253[.]118	213[.]134[.]184[.]167
		70[.]34[.]253[.]247	91[.]149[.]253[.]198	
		70[.]34[.]254[.]245	91[.]149[.]253[.]20	

Detections

Customized NTLM listener

```
rule APT28_NTLM_LISTENER {
	meta:
		description = "Detects NTLM listeners including APT28's custom one"

	strings:
		$command_1 = "start-process powershell.exe -WindowStyle hidden"
		$command_2 = "New-Object System.Net.HttpListener"
		$command_3 = "Prefixes.Add('http://localhost:8080/')"
		$command_4 = "-match 'Authorization'"
		$command_5 = "GetValues('Authorization')"
		$command_6 = "Request.RemoteEndPoint.Address.IPAddressToString"
		$command_7 = "@(0x4e,0x54,0x4c,0x4d,
0x53,0x53,0x50,0x00,0x02,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x28,0x00,0x00,0x01,0x82,0x00
,0x00,0x11,0x22,0x33,0x44,0x55,0x66,0x77,0x88,0x00,0x00,0x00,0x00,0x00,0x00,0x00,0x00)"
		$command_8 = ".AllKeys"

		$variable_1 = "$NTLMAuthentication" nocase
		$variable_2 = "$NTLMType2" nocase
		$variable_3 = "$listener" nocase
		$variable_4 = "$hostip" nocase
		$variable_5 = "$request" nocase
		$variable_6 = "$ntlmt2" nocase
		$variable_7 = "$NTLMType2Response" nocase
		$variable_8 = "$buffer" nocase

	condition:
		5 of ($command_*)
		or
		all of ($variable_*)
}
```

HEADLACE shortcut

```
rule APT28_HEADLACE_SHORTCUT {
	meta:
		description = "Detects the HEADLACE backdoor shortcut dropper. Rule is meant for threat hunting."

	strings:
		$type = "[InternetShortcut]" ascii nocase
		$url  = "file://"
		$edge = "msedge.exe"
		$icon = "IconFile"

	condition:
		all of them
}
```

HEADLACE credential dialogbox phishing

```
rule APT28_HEADLACE_CREDENTIALDIALOG {
	meta:
		description = "Detects scripts used by APT28 to lure user into entering credentials"

	strings:
		$command_1 = "while($true)"
		$command_2 = "Get-Credential $(whoami)"
		$command_3 = "Add-Content"
		$command_4 = ".UserName"
		$command_5 = ".GetNetworkCredential().Password"
		$command_6 = "GetNetworkCredential().Password.Length -ne 0"

	condition:
		5 of them
}
```

HEADLACE core script

```
rule APT28_HEADLACE_CORE {
	meta:
		description = "Detects HEADLACE core batch scripts"

	strings:
		$chcp = "chcp 65001" ascii
		$headless = "start \"\" msedge --headless=new --disable-gpu" ascii

		$command_1 = "taskkill /im msedge.exe /f" ascii
		$command_2 = "whoami>\"%programdata%" ascii
		$command_3 = "timeout" ascii
		$command_4 = "copy \"%programdata%\\" ascii

		$non_generic_del_1 = "del /q /f \"%programdata%" ascii
		$non_generic_del_3 = "del /q /f \"%userprofile%\\Downloads\\" ascii

		$generic_del = "del /q /f" ascii

	condition:
		(
			$chcp
			and
			$headless
		)
		and
		(
			1 of ($non_generic_del_*)
			or
			($generic_del)
			or
			3 of ($command_*)
		)
}
```

MASEPIE

```
rule APT28_MASEPIE {
	meta:
		description = "Detects MASEPIE python script"

	strings:
		$masepie_unique_1 = "os.popen('whoami').read()"
		$masepie_unique_2 = "elif message == 'check'"
		$masepie_unique_3 = "elif message == 'send_file':"
		$masepie_unique_4 = "elif message == 'get_file'"
		$masepie_unique_5 = "enc_mes('ok'"
		$masepie_unique_6 = "Bad command!'.encode('ascii'"
		$masepie_unique_7 = "{user}{SEPARATOR}{k}"
		$masepie_unique_8 = "raise Exception(\"Reconnect"

	condition:
		3 of ($masepie_unique_*)
}
```

STEELHOOK

```
rule APT28_STEELHOOK {
	meta:
		description = "Detects APT28's STEELHOOK powershell script"

	strings:
		$s_1 = "$($env:LOCALAPPDATA\\\\Google\\\\Chrome\\\\User Data\\\\Local State)"
		$s_2 = "$($env:LOCALAPPDATA\\\\Google\\\\Chrome\\\\User Data\\\\Default\\\\Login
Data)"

		$s_3 = "$($env:LOCALAPPDATA\\\\Microsoft\\\\Edge\\\\User Data\\\\Local State)"
		$s_4 = "$($env:LOCALAPPDATA\\\\Microsoft\\\\Edge\\\\User
Data\\\\Default\\\\Login Data)"

		$s_5 = "os_crypt.encrypted_key"
		$s_6 = "System.Security.Cryptography.DataProtectionScope"
		$s_7 = "[system.security.cryptography.protectdata]::Unprotect"
		$s_8 = "Invoke-RestMethod"

	condition:
		all of them
}
```

PSEXEC

```
rule GENERIC_PSEXEC {
	meta:
		description = "Detects SysInternals PSEXEC executable"

	strings:
		$sysinternals_1 = "SYSINTERNALS SOFTWARE LICENCE TERMS"
		$sysinternals_2 = "/accepteula"
		$sysinternals_3 = "Software\\Sysinternals"

		$network_1 = "\\\\%s\\IPC$"
		$network_2 = "\\\\%s\\ADMIN$\\%s"
		$network_3 = "\\Device\\LanmanRedirector\\%s\\ipc$"

		$psexec_1 = "PSEXESVC"
		$psexec_2 = "PSEXEC-{}-"
		$psexec_3 = "Copying %s to %s..."
		$psexec_4 = "gPSINFSVC"


	condition:
		(
			( uint16( 0x0 ) ==0x5a4d )
			and
			( uint16( uint32( 0x3c )) == 0x4550 )
		)
		and
			filesize < 1024KB
		and
		(
			( any of ($sysinternals_*) and any of ($psexec_*) )
			or
			( 2 of ($network_*) and 2 of ($psexec_*))
		)
}
```

Cybersecurity Industry Tracking

The cybersecurity industry provides overlapping cyber threat intelligence, IOCs, and mitigation recommendations related to GRU unit 26165 cyber actors. While not all encompassing, the following are the most notable threat group names related under MITRE ATT&CK G0007 and commonly used within the cybersecurity community:

- APT28 [14]
- Fancy Bear [14]
- Forest Blizzard [14]
- Blue Delta [15]

Note: Cybersecurity companies have different methods of tracking and attributing cyber actors, and this may not be a 1:1 correlation to the U.S. government's understanding for all activity related to these groupings.

Further Reference

To search for the presence of malicious email messages targeting CVE-2023-23397, network defenders may consider using the script published by Microsoft: https://aka.ms/CVE-2023-23397ScriptDoc.

For the Impacket TTP, network defenders may consider using the following publicly available Impacket YARA detection rule: https://github.com/Neo23x0/signature-base/blob/master/yara/gen_impacket_tools.yar

Works Cited

[1] Microsoft. Defending Ukraine: Early Lessons from the Cyber War. 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
[2] FBI et al. Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations. 2024. https://media.defense.gov/2024/Feb/27/2003400753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF
[3] NSA et al. Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments. 2021. https://media.defense.gov/2021/Jul/01/2002753896/-1/-1/0/CSA_GRU_GLOBAL_BRUTE_FORCE_CAMPAIGN_UOO158036-21.PDF
[4] ANSSI. Campagnes d'attaques du mode opératoire APT28 depuis 2021. 2023. https://cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-009/
[5] ANSSI, Targeting and compromise of french entities using the APT28 intrusion set. 2025. https://cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-007/
[6] Polish Cyber Command. Detecting Malicious Activity Against Microsoft Exchange Servers. 2023. https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/detecting-malicious-activity-against-microsoft-exchange-servers/

[7] IBM. Israel-Hamas Conflict Lures to Deliver Headlace Malware. 2023. https://securityintelligence.com/x-force/itg05-ops-leverage-israel-hamas-conflict-lures-to-deliver-headlace-malware/
[8] CERT-UA. APT28: From Initial Attack to Creating Domain Controller Threats in an Hour. 2023. https://cert.gov.ua/article/6276894
[9] NSA. Embracing a Zero Trust Security Model. 2021. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF
[10] NSA et al. Keeping PowerShell: Security Measures to Use and Embrace. 2022. https://media.defense.gov/2022/Jun/22/2003021689/-1/-1/0/CSI_KEEPING_POWERSHELL_SECURITY_MEASURES_TO_USE_AND_EMBRACE_20220622.PDF
[11] National Institute of Standards and Technology (NIST). Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management. 2020. https://pages.nist.gov/800-63-3/sp800-63b.html
[12] NSA. Selecting Secure Multi-factor Authentication Solutions. October 16, 2020. https://media.defense.gov/2024/Jul/31/2003515137/-1/-1/0/MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF
[13] NSA and CSA. NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations. 2023. https://media.defense.gov/2023/Oct/05/2003314578/-1/-1/0/JOINT_CSA_TOP_TEN_MISCONFIGURATIONS_TLP-CLEAR.PDF
[14] Department of Justice. Justice Department Conducts Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate of the General Staff (GRU). 2024. https://www.justice.gov/archives/opa/pr/justice-department-conducts-court-authorized-disruption-botnet-controlled-russian
[15] Recorded Future. GRU's BlueDelta Targets Key Networks in Europe with Multi-Phase Espionage Campaigns. 2024. https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

United States organizations

- **National Security Agency (NSA)**
  Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
  Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
  Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
- **Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI)**
  U.S. organizations are encouraged to reporting suspicious or criminal activity related to information in this advisory to CISA via the agency's Incident Reporting System, its 24/7 Operations Center (report@cisa.gov or 888-282-0870), or 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 user for the activity; the name of the submitting company or organization; and a designated point of contact.
- **Department of Defense Cyber Crime Center (DC3)**
  Defense Industrial Base Inquiries and Cybersecurity Services: DC3.DCISE@us.af.mil
  Media Inquiries / Press Desk: DC3.Information@us.af.mil

United Kingdom organizations

- Report significant cyber security incidents to ncsc.gov.uk/report-an-incident (monitored 24/7)

Germany organizations

- Bundesnachrichtendienst (BND): Media Relations / Press Desk: +49 30 20 45 36 30, pressestelle@bnd.bund.de
- BfV Prevention/Economic Protection Unit: +49 30 18792-3322, wirtschaftsschutz@bfv.bund.de
- BSI Service-Center: +49 800 274 1000, service-center@bsi.bund.de

Czech Republic organizations

- Security Information Service (BIS): cyber.threats@bis.cz
- National Cyber and Information Security Agency (NÚKIB): cert.incident@nukib.gov.cz

Poland organizations

- Poland Military Counterintelligence Service (SKW): cyber.int@skw.gov.pl

Australian organizations

- Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations

- Report incidents by emailing CCCS at contact@cyber.gc.ca.

Estonia organizations

- Estonian Foreign Intelligence Service (EFIS): info@valisluureamet.ee
- Estonian National Cyber Security Centre (NCSC-EE): ria@ria.ee

French organizations

- French organizations are encouraged to report suspicious activity or incident related to information found in this advisory by contacting ANSSI/CERT-FR by email at cert-fr@ssi.gouv.fr or by phone at: 3218 or +33 9 70 83 32 18.

Appendix A: MITRE ATT&CK tactics and techniques

See Table 2 through Table 14 for all the threat actor tactics and techniques referenced in this advisory.

Table 2: Reconnaissance

Tactic/Technique Title	ID	Use
Reconnaissance	TA0043	Conducted reconnaissance on at least one entity involved in the production of ICS components for railway management.
Gather Victim Identity Information: Email Addresses	T1589.002	Conducted contact information reconnaissance to identify additional targets in key positions.
Gather Victim Org Information	T1591	Conducted reconnaissance of the cybersecurity department.
Gather Victim Org Information: Identify Roles	T1591.004	Conducted reconnaissance of individuals responsible for coordinating transport.
Gather Victim Org Information: Business Relationships	T1591.002	Conducted reconnaissance of other companies cooperating with the victim entity.
Gather Victim Host Information	T1592	Attempted to enumerate Real Time Streaming Protocol (RTSP) servers hosting IP cameras.

Table 3: Resource development

Tactic/Technique Title	ID	Use
Compromise Accounts: Email Accounts	T1586.002	Sent phishing emails using compromised accounts.
Compromise Accounts: Cloud Accounts	T1586.003	Sent phishing emails using compromised accounts.

Table 4: Initial Access

Tactic/Technique Title	ID	Use
Trusted Relationship	T1199	Conducted follow-on targeting of additional entities in the transportation sector that had business ties to the primary target, exploiting trust relationships to attempt to gain additional access.
Phishing	T1566	Used spearphishing for credentials and delivering malware to gain initial access to targeted entities.
Phishing: Spearphishing Attachment	T1566.001	Sent emails with malicious attachments.
Phishing: Spearphishing Link	T1566.002	Used spearphishing with included links to fake login pages. Sent emails with embedded hyperlinks that downloaded a malicious archive.
Phishing: Spearphishing Voice	T1566.004	Attempted to use voice phishing to gain access to privileged accounts by impersonating IT staff.
External Remote Services	T1133	Exploited Internet-facing infrastructure, including corporate VPNs, to gain initial access to targeted entities.

Tactic/Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Exploited public vulnerabilities and SQL injection to gain initial access to targeted entities.
Content Injection	T1659	Leveraged a WinRAR vulnerability allowing for the execution of arbitrary code embedded in an archive.

Table 5: Execution

Tactic/Technique Title	ID	Use
User Execution: Malicious Link	T1204.001	Used malicious links to hosted shortcuts in spearphishing.
User Execution: Malicious File	T1204.002	Delivered malware executables via spearphishing.
Scheduled Task/Job: Scheduled Task	T1053.005	Used scheduled tasks to establish persistence.
Command and Scripting Interpreter	T1059	Delivered scripts in spearphishing. Executed arbitrary shell commands.
Command and Scripting Interpreter: PowerShell	T1059.001	PowerShell commands were often used to prepare data for exfiltration.
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Used BAT script in spearphishing.
Command and Scripting Interpreter: Visual Basic	T1059.005	Used VBScript in spearphishing.
Command and Scripting Interpreter: Python	T1059.006	Installed python on infected machines to enable the execution of Certipy.

Table 6: Persistence

Tactic/Technique Title	ID	Use
Account Manipulation: Additional Email Delegate Permissions	T1098.002	Used manipulation of mailbox permissions to establish sustained email collection.
Modify Authentication Process: Multi-Factor Authentication	T1556.006	Enrolled compromised accounts in MFA mechanisms to increase the trust-level of compromised accounts and enable sustained access.
Hijack Execution Flow: DLL Search Order Hijacking	T1574.001	Used DLL search order hijacking to facilitate malware execution.
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	T1547.001	Used run keys to establish persistence.
Boot or Logon Autostart Execution: Shortcut Modification	T1547.009	Placed malicious shortcuts in the startup folder to establish persistence.

Table 7: Defense Evasion

Tactic/Technique Title	ID	Use
Indicator Removal: Clear Windows Event Logs	T1070.001	Deleted event logs through the wevtutil utility.

Table 8: Credential access

Tactic/Technique Title	ID	Use
Brute Force	T1110	Sent requests with Base64-encoded credentials for the RTSP server, which included publicly documented default credentials, and likely were generic attempts to brute force access to the devices.
Brute Force: Password Guessing	T1110.001	Used credential guessing to gain initial access to targeted entities.
Brute Force: Password Spraying	T1110.003	Used brute force to gain initial access to targeted entities. Conducted a brute force password spray via LDAP.
Multi-Factor Authentication Interception	T1111	Used multi-stage redirectors to provide MFA relaying capabilities in some campaigns.
Input Capture	T1056	Used multi-stage redirectors to provide CAPTCHA relaying capabilities in some campaigns.
Forced Authentication	T1187	Used an Outlook NTLM vulnerability to collect NTLM hashes and credentials via specially crafted Outlook calendar appointment invitations.
OS Credential Dumping: NTDS	T1003.003	Attempted to dump Active Directory NTDS.dit domain databases.
Unsecured Credentials: Group Policy Preferences	T1552.006	Retrieved plaintext passwords via Group Policy Preferences using Get-GPPPassword.py.

Table 9: Discovery

Tactic/Technique Title	ID	Use
Account Discovery: Domain Account	T1087.002	Used a modified ldap-dump.py to enumerate the Windows environment.

Table 10: Command and Control

Tactic/Technique Title	ID	Use
Hide Infrastructure	T1665	Abused SOHO devices to facilitate covert cyber operations, as well as proxy malicious activity, via devices with geolocation in proximity to the target.
Proxy: External Proxy	T1090.002	Actor-controlled servers sent RTSP DESCRIBE requests destined for RTSP servers.
Proxy: Multi-hop Proxy	T1090.003	Used Tor and commercial VPNs as part of their anonymization infrastructure
Encrypted Channel	T1573	Connected to victim infrastructure using encrypted TLS.
Multi-Stage Channels	T1104	Used multi-stage redirectors for campaigns.

Table 11: Defense evasion (mobile framework)

Tactic/Technique Title	ID	Use
Execution Guardrails	T1627	Used multi-stage redirectors to verify browser fingerprints in some campaigns.
Execution Guardrails: Geofencing	T1627.001	Used multi-stage redirectors to verify IP-geolocation in some campaigns.

Table 12: Lateral movement

Tactic/Technique Title	ID	Use
Lateral Movement	TA0008	Used native commands and open source tools, such as Impacket and PsExec, to move laterally within the environment.
Remote Services: Remote Desktop Protocol	T1021.001	Moved laterally within the network using RDP.

Table 13: Collection

Tactic/Technique Title	ID	Use
Email Collection	T1114	Retrieved sensitive data from email servers.
Email Collection: Remote Email Collection	T1114.002	Used server data exchange protocols and APIs such as Exchange Web Services (EWS) and IMAP to exfiltrate data from email servers.
Automated Collection	T1119	Used periodic EWS queries to collect new emails.
Video Capture	T1125	Attempted to gain access to the cameras' feeds.
Archive Collected Data	T1560	Accessed files were archived in .zip files prior to exfiltration.
Archive Collected Data: Archive via Utility	T1560.001	Prepared zip archives for upload to the actors' infrastructure.

Table 14: Exfiltration

Tactic/Technique Title	ID	Use
Exfiltration Over Alternative Protocol	T1048	Attempted to exfiltrate archived data via a previously dropped OpenSSH binary.
Scheduled Transfer	T1029	Used periodic EWS queries to collect new emails sent and received since the last data exfiltration.

Appendix B: CVEs exploited

Table 15: Exploited CVE information

CVE	Vendor/Product	Details
CVE-2023-38831	RARLAB WinRAR	Allows execution of arbitrary code when a user attempts to view a benign file within a ZIP archive.
CVE-2023-23397	Microsoft Outlook	External actors could send specially crafted emails that cause a connection from the victim to an untrusted location of the actor's control, leaking the Net-NTLMv2 hash of the victim that the actor could then relay to another service to authenticate as the victim.
CVE-2021-44026	Roundcube Webmail	Roundcube before 1.3.17 and 1.4.x before 1.4.12 is prone to a potential SQL injection via search or search params.
CVE-2020-35730	Roundcube Webmail	An XSS issue was discovered in Roundcube Webmail before 1.2.13, 1.3.x before 1.3.16 and 1.4.x before 1.4.10, where a plaintext email message with JavaScript in a link reference element is mishandled by linkref_addindex in rcube_string_replacer.php.
CVE-2020-12641	Roundcube Webmail	Roundcube Webmail before 1.4.4 allows arbitrary code execution via shell metacharacters in a configuration setting for im_convert_path or im_identify_path in rcube_image.php.

Appendix C: MITRE D3FEND Countermeasures

Table 16: MITRE D3FEND countermeasures

Countermeasure Title	ID	Details
Network Isolation	D3-NI	Employ appropriate network segmentation. Disable Universal Plug and Play (UPnP), Peer-to-Peer (P2P), and Anonymous Visit features on IP cameras and routers.
Access Mediation	D3-AMED	Limit access and utilize additional attributes (such as device information, environment, and access path) when making access decisions. Configure access controls carefully to ensure that only well-maintained and well-authenticated accounts have access.
Inbound Traffic Filtering	D3-ITF	Implement host firewall rules to block connections from other devices on the network, other than from authorized management devices and servers, to prevent lateral movement.
Resource Access Pattern Analysis	D3-RAPA	Use automated tools to audit access logs for security concerns and identify anomalous access requests.
Outbound Traffic Filtering	D3-OTF	Block NTLM/SMB requests to external infrastructure.
Platform Monitoring	D3-PM	Install EDR/logging/cybersecurity solutions onto high value systems with large amounts of sensitive data such as mail servers and domain controllers.
System File Analysis	D3-SFA	Collect and monitor Windows logs for certain events, especially for events that indicate that a log was cleared unexpectedly.
Application Hardening	D3-AH	Enable optional security features in Windows to harden endpoints and mitigate initial access techniques.
Application-based Process Isolation	D3-ABPI	Enable attack surface reduction rules to prevent executable content from email.
Executable Allowlisting	D3-EAL	Enable attack surface reduction rules to prevent execution of files from globally writeable directories, such as Downloads or %APPDATA%.
Execution Isolation	D3-EI	Unless users are involved in the development of scripts, limit the execution of scripts (such as batch, JavaScript, and PowerShell) to known scripts.
Application Configuration Hardening	D3-ACH	Disable Windows Host Scripting functionality and configure PowerShell to run in Constrained mode. Disable protocols that use weak authentication (e.g., clear-text passwords, or outdated and vulnerable authentication or encryption protocols) or do not support multi-factor authentication. Turn off other ports/services not in use (e.g., FTP, web interface, etc.).
Process Spawn Analysis	D3-PSA	Use open source SIGMA rules as a baseline for detecting and alerting on suspicious file execution or command parameters.
URL Reputation Analysis	D3-URA	Use services that provide enhanced browsing services and safe link checking.

Network Access Mediation	D3-NAM	Do not allow incoming traffic, especially logins to systems, from public VPN services. Where possible, logins from public VPNs, including exit nodes in the same country as target systems, should be blocked or, if allowed, alerted on for further investigation. Ensure cameras and other Internet of Things devices are protected by a security appliance, if possible.
DNS Denylisting	D3-DNSDL	Do not allow outgoing traffic to hosting and API mocking services frequently used by malicious actors.
Domain Name Reputation Analysis	D3-DNRA	Heuristic detections for web requests to new subdomains may uncover malicious phishing activity. Logging the requests for each sub-domain requested by users on a network, such as in DNS or firewall logs, may enable system administrators to identify new targeting and victims.
Multi-factor Authentication	D3-MFA	Use MFA with strong factors and require regular re-authentication, especially for management accounts.
Job Function Access Pattern Analysis	D3-JFAPA	Implement other mitigations for privileged accounts: including limiting the number of admin accounts, considering using hardware MFA tokens, and regularly reviewing all privileged user accounts.
User Account Permissions	D3-UAP	Separate privileged accounts by role and alert on misuse of privileged accounts. Audit user accounts on all devices to ensure they are an accurate reflection of your organization and that they are being used as expected.
Token-based Authentication	D3-TBA	Reduce reliance on passwords; instead, consider using services like single sign-on.
Credential Hardening	D3-CH	Do not store passwords in Group Policy Preferences (GPP). Remove all passwords previously included in GPP and change all passwords on the corresponding accounts.
Authentication Event Threshholding	D3-ANET	Use account throttling or account lockout. Throttling progressively increases time delay between successive login attempts. If using account lockout, allow between 5 to 10 attempts before lockout.
Strong Password Policy	D3-SPP	Use a service to check for compromised passwords before using them.
Credential Rotation	D3-CRO	Change all default credentials.
Encrypted Tunnels	D3-ET	Disable protocols that use weak authentication (e.g., clear-text passwords, or outdated and vulnerable authentication or encryption protocols). Use a VPN for remote connections to devices.
Software Update	D3-SU	Apply security patches and firmware updates to all devices. Ensure devices are currently supported. Replace devices that are end-of-life.
Agent Authentication	D3-AA	Ensure authentication is enabled for remote access to devices. If supported on IP cameras, enable authenticated RTSP access only.

User Behavior Analysis	D3-UBA	Review all authentication activity for remote access to make sure it is valid and expected. Investigate any unexpected or unusual activity.