Joint Cybersecurity Advisory

TLP:CLEAR

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 report is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules.

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 (Cyber Centre)
- 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

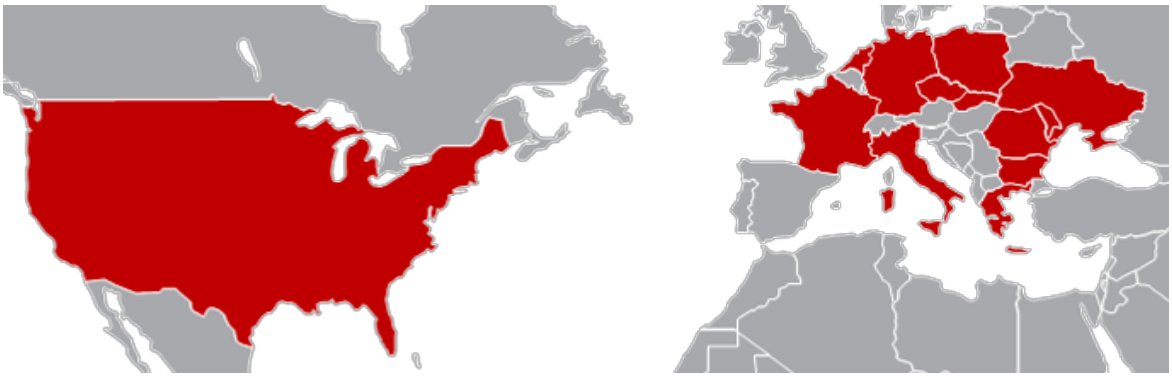


Figure 1: Countries with Targeted Entities

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 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].