Cadet Blizzard
(Ember Bear, DEV-0586, UAC-0056)

161st Special Purpose Centre of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Military Unit 29155)

Group name	Cadet Blizzard
Alternative names	Ember Bear, DEV-0586, UAC-0056, UNC2589
Country of origin	Russian Federation
Affiliation	Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)
Associated unit	Military Unit 29155, 161st Special Purpose Centre
Threat type	Advanced Persistent Threat (APT)
Primary motivation	Cyber espionage, sabotage, information and psychological operations
Period of activity	2020 – present
Primary targets	Ukraine, NATO countries, the public sector, critical infrastructure

Support the organization’s activities: https://donate.shum-ng.org/

Analytical Summary

Cadet Blizzard (also known as Ember Bear, DEV-0586, and UAC-0056) is a Russian cyber threat group linked to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). According to assessments by Microsoft, CERT-UA, Mandiant, and other research organisations, the group's activities are coordinated by structures associated with Military Unit 29155 and the so-called "Averyanov Brigade".

The group's primary specialisation is the conduct of cyber espionage, destructive cyber operations, and information and psychological operations targeting Ukraine, NATO member states, and European Union countries.

Cadet Blizzard attracted widespread international attention following its deployment of the WhisperGate malware in January 2022, immediately prior to Russia's full-scale invasion of Ukraine. Since then, the group has repeatedly participated in intelligence collection campaigns, the compromise of government information resources, and attacks against critical infrastructure.

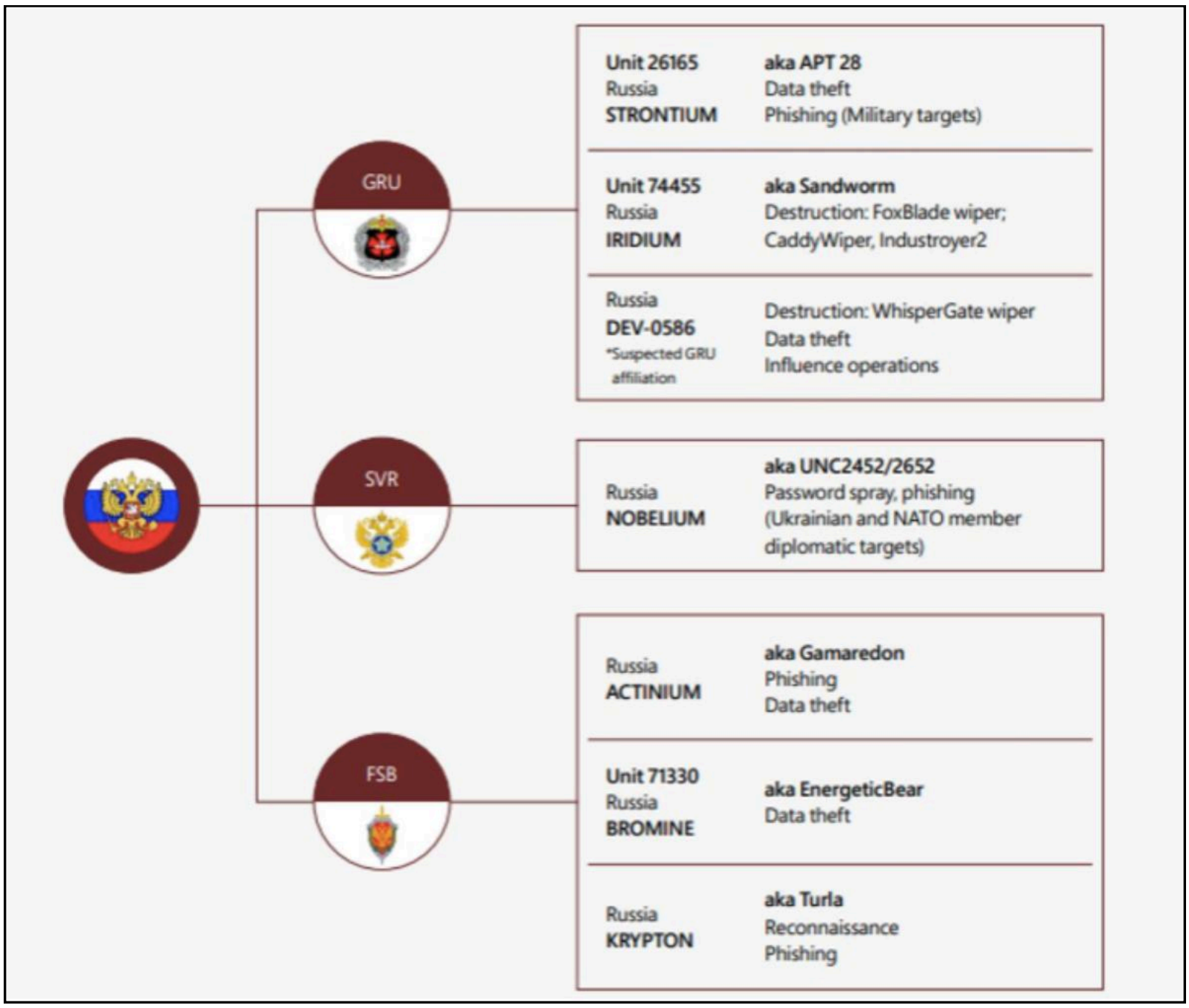
Unlike many other APT groups, Cadet Blizzard combines traditional social engineering techniques, phishing campaigns, and the use of legitimate administrative tools, significantly complicating the detection of its presence within victim networks.

As of 2026, the group remains one of the most active Russian cyber threats targeting Ukraine and its international partners.

STRUCTURAL SCHEME OF THE THREAT CLUSTER

Structural Scheme of the Cadet Blizzard (Ember Bear, DEV-0586, UAC-0056) Threat Cluster Associated with GRU Military Unit 29155

Support the organization's activities: https://donate.shum-ng.org/



Structure of GRU Military Unit 29155 Cyber Units
Primary Areas of Activity and Known Campaigns

Key Analytical Findings

Following 2022, activity associated with this cluster shifted noticeably towards more aggressive and destructive operations against Ukraine. The primary focus moved away from covert intelligence gathering towards the direct disruption of systems and infrastructure.

The principal types of activity include large-scale destructive attacks against Ukrainian infrastructure, the use of wiper malware, including WhisperGate and similar tools, mass defacement of government websites, intelligence operations targeting NATO structures and allied countries, and attacks against organisations that directly or indirectly support Ukraine.

Destructive Attacks Against Ukraine (2022)

In 2022, activity attributed by researchers to this cluster became significantly more destructive. The primary focus shifted from traditional cyber espionage to the direct disruption of government and critical systems.

This was reflected in the following: the destruction or corruption of data on government servers, disruption of government online services, attacks against communications systems and administrative infrastructure, and the synchronisation of cyber attacks with events occurring in the physical domain.

Overall, these campaigns are regarded as an example of state-sponsored APT operations in which cyber activities are employed as part of a broader strategy of influence.

WhisperGate Attack Chain: From Infrastructure Compromise to Data Destruction

Operations involving wiper malware, particularly WhisperGate, should be regarded as a deliberate destructive campaign in which the primary objective is not the covert theft of data, but its complete and rapid destruction, followed by the disruption of the targeted infrastructure.

From a technical perspective, WhisperGate demonstrated a multi-stage architecture. The initial component mimicked ransomware behaviour; however, it contained no recovery mechanism. Subsequent stages overwrote and destroyed critical data and boot structures, resulting in the effective and irreversible loss of system functionality. The primary targets were Ukrainian government and critical information systems, allowing this activity to be classified as a sabotage-oriented cyber attack.

At the same time, large-scale website defacement operations targeting government web resources were observed. These involved the compromise of government portals, the replacement of legitimate content with propaganda messages, the temporary disruption of access to public services, and the creation of an atmosphere of information chaos. Collectively, these actions served not only a technical purpose but also a pronounced information and psychological function. In some cases, they may also have been used as a cover for deeper intrusion into targeted infrastructure.

Another significant line of activity comprised intelligence operations against NATO structures and Ukraine’s allied states. These included the collection of information on military and political support for Ukraine, analysis of logistics and defence supply chains, and attempts to compromise government, diplomatic, and analytical organisations. The primary objective was to build a strategic intelligence picture for subsequent use in military and political planning.

In addition, sustained activity was observed against organisations involved in supporting Ukraine, including IT companies, cloud service providers, humanitarian organisations, and defence contractors. Typical attack vectors included phishing campaigns, credential compromise, intrusion into internal networks, and the use of compromised systems as pivot points for expanding access across partner ecosystems.

Overall, this body of activity is characterised as a multi-vector, state-sponsored destructive and intelligence campaign in which cyber capabilities are employed simultaneously to disrupt infrastructure, conduct information operations, and collect strategic intelligence.

Ransom note displayed following the compromise of a system by WhisperGate

```
.text:00403B93          mov     [esp+14h+hTemplateFile], 0 ; hTemplateFile
.text:00403B9B          mov     dword ptr [esp+14h], 0 ; dwFlagsAndAttributes
.text:00403BA3          mov     [esp+14h+dwCreationDisposition], 3 ; dwCreationDisposition
.text:00403BAB          mov     [esp+14h+lpSecurityAttributes], 0 ; lpSecurityAttributes
.text:00403BB3          mov     [esp+14h+dwShareMode], 3 ; dwShareMode
.text:00403BBB          mov     [esp+14h+dwDesiredAccess], 10000000h ; dwDesiredAccess
.text:00403BC3          mov     [esp+14h+lpFileName], offset FileName ; "\\\\.\\PhysicalDrive0"
.text:00403BCA          call    CreateFileW
.text:00403BCF          mov     esi, eax
.text:00403BD1          lea     eax, [ebp-2018h]
.text:00403BD7          sub     esp, 1Ch
.text:00403BDA          mov     [esp+14h+lpFileName], esi ; hFile
.text:00403BDD          mov     [esp+14h+dwCreationDisposition], 0 ; lpOverlapped
.text:00403BE5          mov     [esp+14h+lpSecurityAttributes], 0 ; lpNumberOfBytesWritten
.text:00403BED          mov     [esp+14h+dwShareMode], 200h ; nNumberOfBytesToWrite
.text:00403BF5          mov     [esp+14h+dwDesiredAccess], eax ; lpBuffer
.text:00403BF9          call    WriteFile
.text:00403BFE          sub     esp, 14h
.text:00403C01          mov     [esp+14h+lpFileName], esi ; hObject
.text:00403C04          call    CloseHandle
```

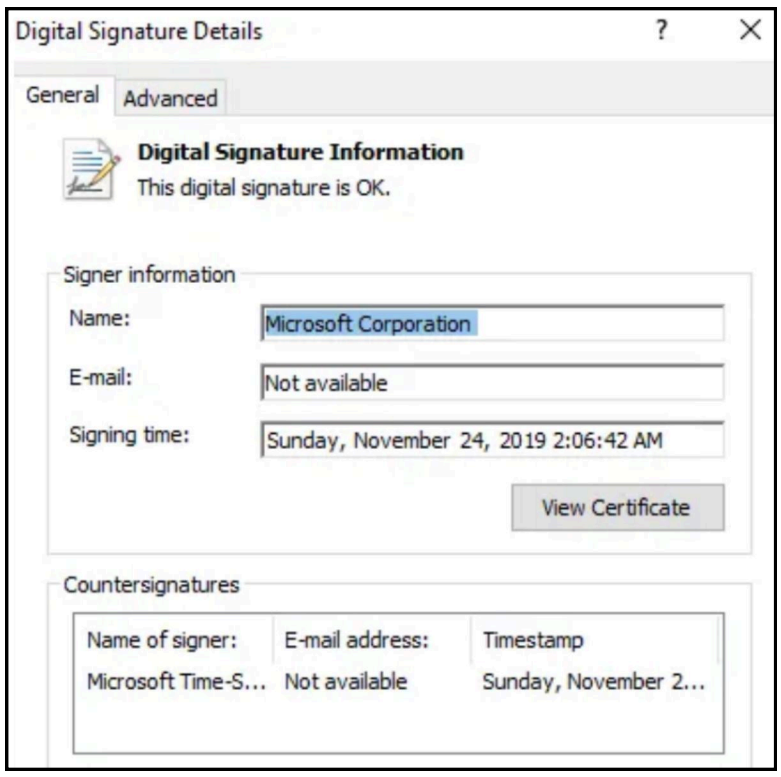
Mechanism of Master Boot Record (MBR) Corruption in WhisperGate

Support the organization’s activities: https://donate.shum-ng.org/

WhisperGate uses the Impacket toolkit to move laterally across the network and execute malicious payloads. The primary file (stage1.exe) is a PE executable that can be covertly placed in various system directories, such as C:\Temp or C:\ProgramData.

Once executed, the malware gains access to the computer's physical disk (PhysicalDrive0), where the Master Boot Record (MBR) is located. It then overwrites the MBR with malicious code containing a ransom note.

As a result, following a system reboot, the operating system is no longer able to boot normally, and the user is presented with a message indicating "disk corruption" together with a ransom demand.

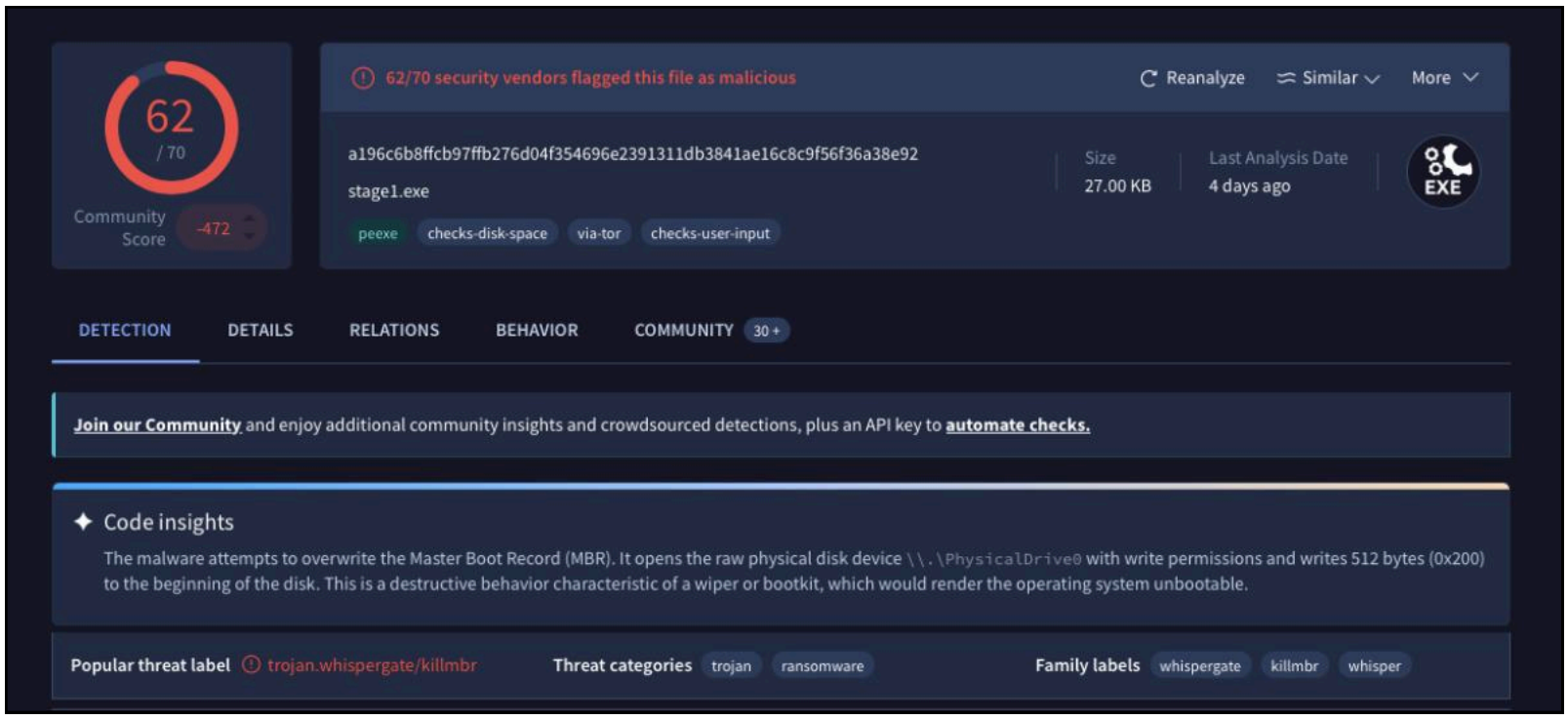


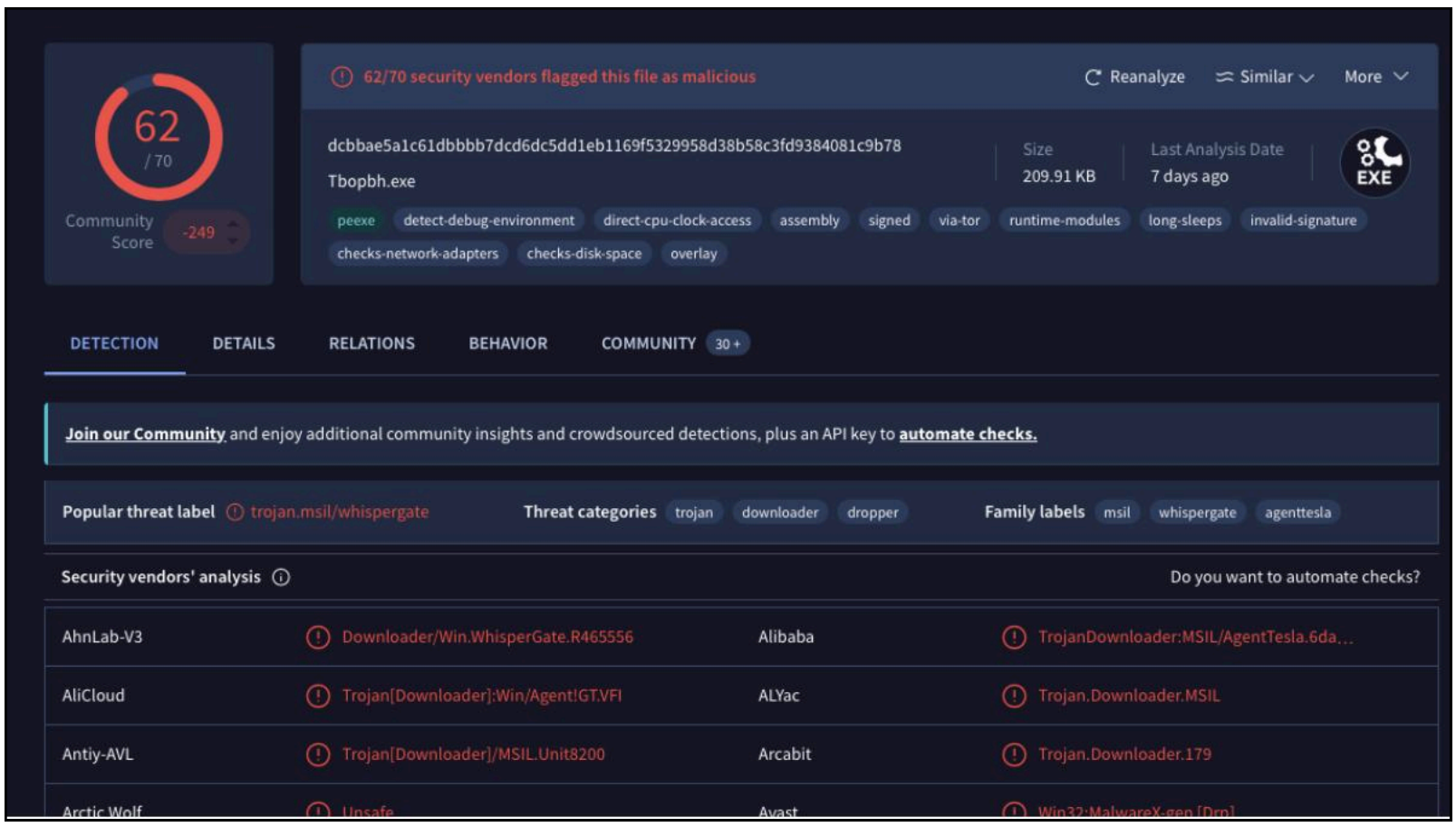
During execution, this application writes 22.53 GB of data to the computer's disk. The original application contains no suspicious code, suggesting that WhisperGate injects malicious code into the process to corrupt files.

On 15 January 2022, Microsoft reported the discovery of a sophisticated malicious operation targeting multiple organisations in Ukraine. WhisperGate malware consists of two stages: it corrupts the Master Boot Record (MBR), displays a fake ransom note, and encrypts/corrupts files with specified extensions.

Attribution Confidence Level

The attribution of Cadet Blizzard to the GRU is assessed with high confidence, based on a combination of technical indicators, infrastructure overlaps, TTP patterns, and analytical reporting by Microsoft MSTIC, CISA, and other cybersecurity research organisations. While no direct official state attribution has been publicly confirmed, there is a strong and consistent consensus across the cyber threat intelligence community.





Detection of the WhisperGate Sample and Associated Indicators of Compromise (IOCs)

Chronology of activity

- 2020–2021 — early activity, cyber espionage operations and preparatory infrastructure campaigns.
- January 2022 — WhisperGate destructive campaign against Ukrainian government systems.
- 2022 — large-scale attacks on Ukraine's critical infrastructure and defence sector.
- 2023–2024 — expansion of targets to NATO, the EU and organisations supporting Ukraine, including supply-chain operations.
- 2025–2026 — continuation of intelligence-destructive activity with a focus on long-term access operations (persistent access).

Critical infrastructure of Ukraine in 2022

In 2022, Ukraine's critical infrastructure became one of the key targets of destructive cyber operations associated with the activity cluster that researchers attribute to GRU and DEV-0586. This was not about isolated incidents, but a systematic campaign aimed at disrupting the resilience of essential state and civilian services.

The main sectors affected included energy infrastructure, telecommunications operators, transport systems, as well as government IT centres and data centres that ensure the functioning of the state's digital services.

From a tactical perspective, the attacks combined several levels of impact: gaining unauthorised access to internal networks, establishing persistence within the infrastructure, subsequent disruption of systems' operations and, in some cases, destructive actions aimed at damaging or destroying data and services.

The operational effect consisted of creating disruptions in the operation of critical systems, reducing the availability of digital government services and placing an overall burden on infrastructure during a period of crisis.

Defence and security sector organisations of Ukraine

Attacks on the defence and security sector of Ukraine in 2022 had a targeted and multi-stage nature and were aimed at military information systems, structures of the Ministry of Defence of Ukraine, the Security Service of Ukraine and other law enforcement agencies with the purpose of gaining access to internal networks, collecting intelligence data and preparing potential destructive actions, while the typical scenario included phishing, compromise of credentials, establishing persistence within the infrastructure, internal network reconnaissance and, in some cases, the use of malware for further sabotage or data destruction.

Table: attacks on the defence sector

Table: attacks on the defence sector	Attack type	Actions of attackers	Consequences
Military information systems	Phishing, account compromise	Obtaining login credentials, access to email and internal services	Reconnaissance, potential access to internal data
Ministry of Defence of Ukraine	Spear-phishing, malware	Installation of malicious software, establishing persistence in the network	Interception of information, preparation for sabotage
Security Service of Ukraine and related units	Phishing + credential theft	Credential theft, attempts at lateral movement	Compromise of individual accounts, data leakage

Law enforcement agencies (overall)	Intelligence-gathering attacks	Information collection, infrastructure scanning	Preparation for further cyber operations
Defence IT systems	Malware / web-shells	Obtaining remote access to servers	Potential disruption of systems' operations

Conclusion: The attacks had a combined nature — initially phishing and gaining access, followed by establishing persistence in the network, reconnaissance and, in some cases, preparation for destructive actions (wiper activity).

3. International and NATO-related targets 2022–2024

During the period of 2022–2024, expanded intelligence and supply chain activity was recorded against international organisations associated with NATO and the EU, with a focus on government networks of Alliance countries, European Union state institutions, defence contractors, logistics companies providing supplies to Ukraine, as well as IT and cloud providers serving government and defence systems.

The main nature of the operations included targeted phishing of employees, credential theft, compromise of email and corporate accounts, infiltration of infrastructure through suppliers and long-term covert presence in compromised networks.

The purpose of these actions was to obtain intelligence information on military and logistical support for Ukraine, track supply chains, as well as create potential conditions for future cyber operations and compromise of critical infrastructure elements of allies.

4. Organisations associated with support for Ukraine 2023–2024

During 2023–2024, targeted intelligence activity was observed against organisations involved in military, humanitarian and logistical support for Ukraine, with a focus on humanitarian structures, Western IT companies working with the Ukrainian public sector, logistics operators supplying aid and European defence companies.

The main vector of the attacks included targeted phishing of employees, compromise of email and corporate accounts, credential theft, as well as establishing persistent covert access to internal networks with subsequent collection of intelligence information.

The purpose of these operations was to gain access to internal communications, track military and humanitarian assistance to Ukraine, as well as prepare potential future cyber operations within the broader intelligence and sabotage activity.

Sector	TTP	Examples	Consequences
Critical infrastructure	Wiper, sabotage, intrusion	WhisperGate, MBR overwrite	Data destruction, service disruption
Ukraine’s defence sector	Phishing, credential theft	MFA bypass, email compromise	Intelligence collection, network access
NATO / EU	Espionage, supply-chain	Compromise of contractors	Strategic intelligence
Support for Ukraine	Persistence, phishing	Access to IT/logistics	Monitoring of assistance
Government infrastructure	Defacement, malware	Website replacement, web shells	Service destabilisation

MITRE ATT&CK mapping

Фаза	Техніка MITRE	Приклад
Initial Access	T1566 Phishing	Phishing emails
Execution	T1059 Command & Scripting	Payload execution
Persistence	T1505.003 Web Shells	Establishing persistence on servers
Privilege Escalation	T1068 Exploitation	Exploitation of vulnerabilities
Defense Evasion	T1027 Obfuscation	Hidden payloads
Credential Access	T1003 OS Credential Dumping	Password theft
Lateral Movement	T1021 Remote Services	Movement within the network
Impact	T1485 Data Destruction	WhisperGate wiper
Impact	T1491 Defacement	Replacement of web pages

Infrastructure, C2 and tooling

Cadet Blizzard’s activity is characterised by the use of dynamic infrastructure with short-lived domains, compromised servers and legitimate services for covert communication.

The main techniques include the use of phishing infrastructures, compromised accounts, PowerShell scripts, Windows-native tools and custom wiper components. In the case of WhisperGate, the use of a multi-stage architecture was observed, with separate payload components for data destruction and damage to system boot structures.

The use of legitimate administrative tools for covert movement within victim networks (Living-off-the-Land Techniques) is also recorded, which complicates the detection of activity and reduces the effectiveness of traditional security tools.

Analytical assessment of the threat

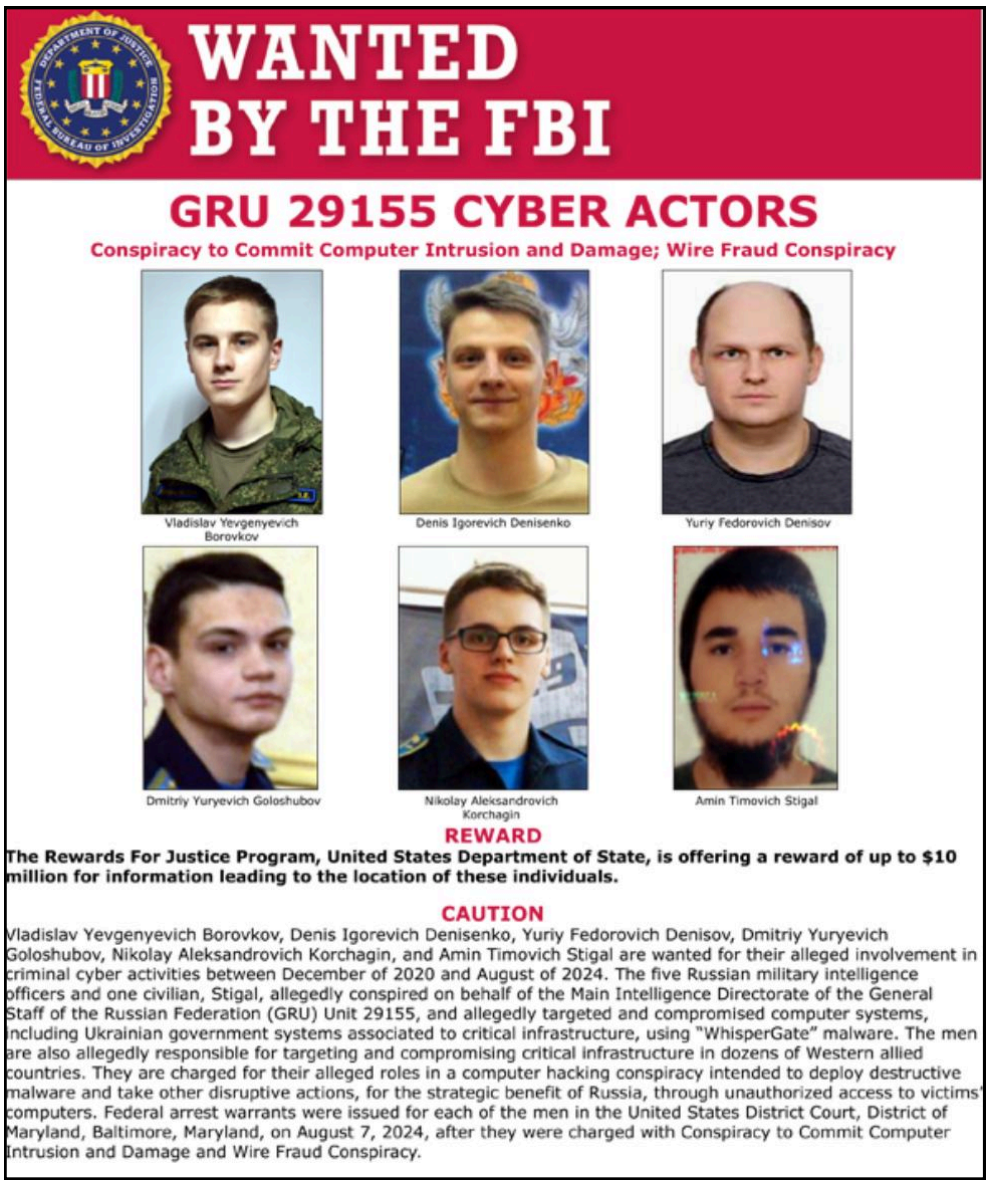
The group demonstrates a comprehensive and hybrid model of APT activity, combining intelligence, information-psychological and destructive cyber operations. The typical scenario involves gaining initial access through phishing or credential compromise, subsequent establishment of persistence in the victim’s infrastructure, internal reconnaissance and expansion of control over the network.

A separate feature of the activity is the use of supply-chain attacks, which allow gaining access not only to direct targets but also to partner organisations and contractors. This approach significantly expands the potential scale of compromise and complicates the detection of the attack source.

An important element of the operations is the use of wiper-type destructive tools aimed at data destruction and disruption of information systems’ operations. Unlike traditional cybercrime campaigns, the primary goal of such attacks is not financial gain, but achieving strategic and operational effects.

Cadet Blizzard’s activity covers the public sector, defence structures, critical infrastructure and international organisations. A particular focus is directed at Ukraine, as well as NATO countries and organisations involved in military, humanitarian and technological support for Ukraine.

Key individuals



WANTED BY THE FBI

GRU 29155 CYBER ACTORS

Conspiracy to Commit Computer Intrusion and Damage; Wire Fraud Conspiracy

Vladislav Yevgenyevich Borovkov

Denis Igorevich Denisenko

Yuriy Fedorovich Denisov

Dmitriy Yuryevich Goloshubov

Nikolay Aleksandrovich Korchagin

Amin Timovich Stigal

REWARD

The Rewards For Justice Program, United States Department of State, is offering a reward of up to $10 million for information leading to the location of these individuals.

CAUTION

Vladislav Yevgenyevich Borovkov, Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Aleksandrovich Korchagin, and Amin Timovich Stigal are wanted for their alleged involvement in criminal cyber activities between December of 2020 and August of 2024. The five Russian military intelligence officers and one civilian, Stigal, allegedly conspired on behalf of the Main Intelligence Directorate of the General Staff of the Russian Federation (GRU) Unit 29155, and allegedly targeted and compromised computer systems, including Ukrainian government systems associated to critical infrastructure, using "WhisperGate" malware. The men are also allegedly responsible for targeting and compromising critical infrastructure in dozens of Western allied countries. They are charged for their alleged roles in a computer hacking conspiracy intended to deploy destructive malware and take other disruptive actions, for the strategic benefit of Russia, through unauthorized access to victims' computers. Federal arrest warrants were issued for each of the men in the United States District Court, District of Maryland, Baltimore, Maryland, on August 7, 2024, after they were charged with Conspiracy to Commit Computer Intrusion and Damage and Wire Fraud Conspiracy.

Support the organization’s activities: https://donate.shum-ng.org/

A reward of up to $10 million is offered for information on individuals who carried out cyberattacks against US critical infrastructure at the direction of a foreign government.

This concerns five Russian military intelligence officers of the GRU (Unit 29155), who are linked to the WhisperGate malware attack against Ukraine prior to the 2022 invasion, as well as to cyber espionage and attacks against infrastructure in Ukraine, the United States and other countries (energy, government and aerospace systems).

Yuriy Fyodorovich Denisov
officer of the GRU RF Unit 29155

Gender: male.
Appearance type: Caucasian.
Hair: short, dark.
Eyes: blue.
Citizenship: Russian Federation.
Date of birth: 17 June 1980.

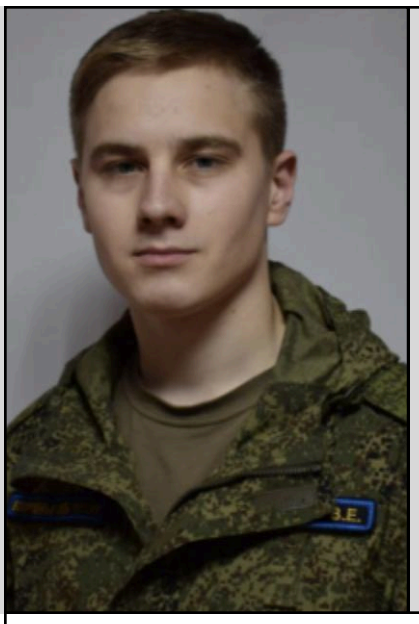
In open-source materials, he appears in civilian clothing and under cover identities, which corresponds to the operational practices of GRU special units.

Yuriy Fyodorovich Denisov is described in open-source investigations as a Russian GRU officer associated with Unit 29155. His activity does not appear to be the work of a lone hacker, but rather participation in a team structure involved in the preparation and technical support of cyberattacks.

He is attributed with involvement in the planning and technical preparation of attacks against Ukraine, including those that used WhisperGate-type malware. Such attacks were aimed not at data theft, but at the destruction or disruption of government and infrastructure systems. In this context, he is described as a participant in activities related to preparing system infections and deploying malicious code through the infrastructure of attacking groups.

He is also associated with the intelligence-gathering component of cyber operations. This includes analysis of target networks, identification of vulnerabilities in government and critical systems, as well as preparation of access for further attacks. It is additionally indicated that similar activities concerned not only Ukraine but also targets in NATO countries, where reconnaissance and infrastructure scanning attempts were carried out.

Within the structure of Unit 29155, he is considered a mid-level technical operator who supported the cyber component of operations. His role is described as preparatory and supporting, meaning that he worked with data, tools and networks prior to the execution of attacks, rather than managing the entire operation.



Vladislav Yevgenyevich Borovkov
officer of the GRU RF Unit 29155

Known as: Vlad Borovkov
Date of birth: 7 October 1997
Gender: male
Citizenship: Russian Federation
Race: white
Appearance type: Caucasian
Hair: brown / dark blond
Eyes: brown
Languages: Russian, English

Vladislav Yevgenyevich Borovkov is described as an officer of Russian military intelligence associated with the cyber direction of GRU Unit 29155. He belongs to the junior officer level and performs technical operator functions in operations related to computer network intrusion and the use of malicious software.

His activity within the structure is considered participation in the practical phase of cyber operations. This includes preparing attack infrastructure, working with target networks, scanning systems, identifying vulnerabilities and providing technical support for malware deployment. Such activities are part of a broader process preceding the direct launch of cyberattacks and ensuring access to target systems.

Within operations associated with Unit 29155, his name is linked to campaigns against Ukraine and NATO countries, where destructive cyber tools were used aimed at disrupting government services and critical infrastructure. These were destabilisation attacks that had not only intelligence-gathering but also destructive characteristics.

Within the structure, he is considered a tactical operator of mid-level or junior rank, who does not conduct strategic planning but is responsible for the technical implementation of specific stages of cyber operations. His role consists of supporting the operation of tools, preparing the attack environment and assisting the processes of gaining access to systems.

SHUM

Denis Igorevich Denisenko
officer of the GRU RF Unit 29155

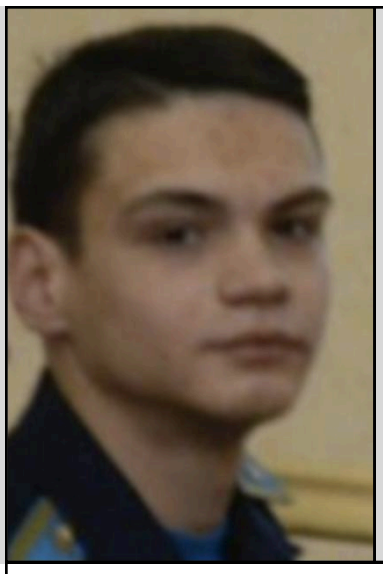
Gender: male
Citizenship: Russian Federation
Race: white
Appearance type: Caucasian
Hair: brown / blond
Eyes: blue
Date of birth: 14 May 1997
Languages: Russian, English

Denis Ihorovich Denisenko is described as an officer associated with the cyber direction within the structure of Russian military intelligence. Within this activity, his role is defined as technical and operational, related to the development and use of tools for attacks on computer networks.

His activity includes participation in the creation and configuration of malicious software, as well as conducting attacks against government and critical infrastructure systems. In such operations, he is considered an operator working with the technical aspects of network intrusion, including preparation of the attack environment, exploitation of vulnerabilities and ensuring access to target systems.

He is also associated with participation in operations against Ukraine and other states, where cyber activity was used as an element of a broader hybrid strategy of influence, including intelligence gathering, destabilisation and disruption of infrastructure operations.

Within the structure, he is considered a mid-level technical officer who ensures the implementation of attacks at the operational level rather than strategic planning of operations.



Dmitriy Yuryevich Goloshubov
officer of the GRU RF Unit 29155

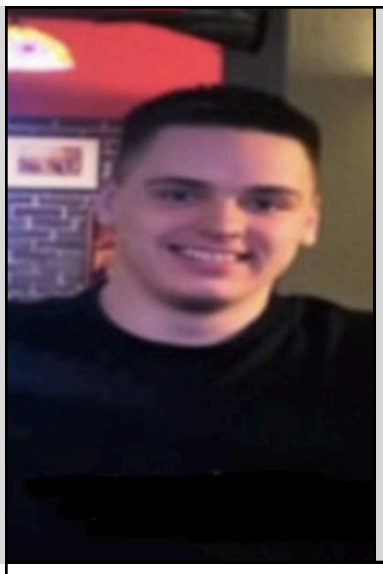
Gender: male
Citizenship: Russian Federation
Race: white
Appearance type: Caucasian
Hair: brown / blond
Eyes: brown
Date of birth: 10 October 1998
Languages: Russian, English

Dmytro Yuriyovich Holoshubov is described as an officer associated with the cyber direction of Russian military intelligence. Within the structure with which he is associated, he performs the role of a technical specialist responsible for the practical implementation of network attacks.

His activity includes participation in the preparation and execution of intrusions into computer systems, including technical configuration of attack tools, ensuring access to target networks and supporting intrusion processes. He is considered an operator working with the infrastructure component of cyber operations rather than a strategic planner.

Within operations associated with the group, his activity is described as participation in campaigns against government and critical systems of Ukraine and other countries, where methods of covert access, network compromise and subsequent use of obtained entry points for deployment of attack tools were applied.

His role is defined as the technical implementation of network intrusions, including support of cyber operations at the infrastructure level and ensuring the functioning of attack mechanisms in target systems.



Nikolay Aleksandrovich Korchagin
officer of the GRU RF Unit 29155

Gender: male
Citizenship: Russian Federation
Race: white
Appearance type: Caucasian
Hair: brown / blond
Eyes: not recorded in stable confirmed data
Date of birth: 16 September 1997
Languages: Russian, English

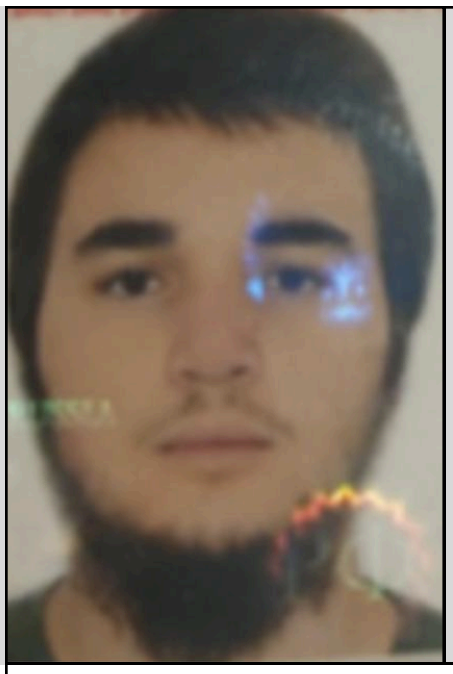
Mykola Oleksandrovych Korchagin is described as an officer associated with the cyber direction of Russian military intelligence. Within the structure with which he is associated, he performs the role of a technical operator in operations involving intrusion into computer systems and maintaining access within compromised networks.

His activity is associated with the stages of cyber operations that begin with obtaining initial access to target systems and continue with maintaining that access. This includes working with compromise infrastructure, supporting stable control over compromised networks and assisting in the deployment of tools for further actions within the system.

Within operations associated with Unit 29155, his role is described as participation in campaigns against government and critical systems of Ukraine and other countries, where cyber activity is used as a tool of destabilisation and long-term covert access to infrastructure.

His function within the structure is defined as tactical: he ensures the technical stability of already compromised systems and supports the operation of attack infrastructure at the stage after initial intrusion.

SHUM



Amin Timovich Stigal
Subject of investigations related to the WhisperGate operation

Place of birth: Grozny, Chechnya, Russia
Gender: male
Citizenship: Russian Federation
Race: white
Appearance type: Caucasian
Hair: brown / dark brown
Eyes: brown
Date of birth: 1 October 2002 (likely primary), 1 August 1996 (used cover identity)
Languages: Russian, English, Arabic

Amin Stigal is described as a civilian individual associated in US allegations with involvement in cyber operations against Ukraine, including the WhisperGate malware-based attack in January 2022. According to the US indictment, he acted in cooperation with individuals linked to Russian military intelligence (GRU) and participated in activities aimed at compromising Ukrainian government and critical systems.

Within this case, Stigal is described as one of the operators involved in cyber operations that included compromising government resources, publishing stolen data, placing destructive messages on Ukrainian government platforms, and attempting to distribute stolen information through the dark web. He is also alleged to have participated in a campaign involving malware designed to destroy data on affected systems, creating the effect of infrastructure destruction.

The Stigal case is considered in the context of a broader model of Russia’s involvement of civilian hackers and young specialists in operations that may serve as an auxiliary or intermediary link between intelligence services and the cybercriminal environment. This model highlights the potential use of such individuals as tools with partial or indirect connections to state structures, allowing the real organisers of attacks to be concealed.

The case materials also indicate that, alongside cyber-related charges against Amin Stigal, there are separate criminal proceedings against his father related to financial cybercrimes; however, they are not considered part of the same operational line.

The overall picture formed by investigators and analysts describes Stigal as a young participant in the cyber environment who may have been involved in complex operations either knowingly or through intermediary structures, where the boundary between criminal activity and state cyber operations becomes blurred.

Amin Timofeyevich Stigal (right) and his father Timur Stigal (left)

WhisperGate Multi-Stage Cyber Operation Model: Intrusion, Propagation and Destructive Impact

Support the organization’s activities: https://donate.shum-ng.org/

The presented scheme reflects the multi-level structure of a wiper-type cyber operation characteristic of WhisperGate. The operation is built on the principle of sequential progression through stages: from initial access to the infrastructure to the complete destruction of data and systems.

At the first stage, network intrusion is carried out through the compromise of user or administrative access points. This is followed by the internal reconnaissance phase, during which attackers study the network structure, identify key servers, databases and infrastructure control elements.

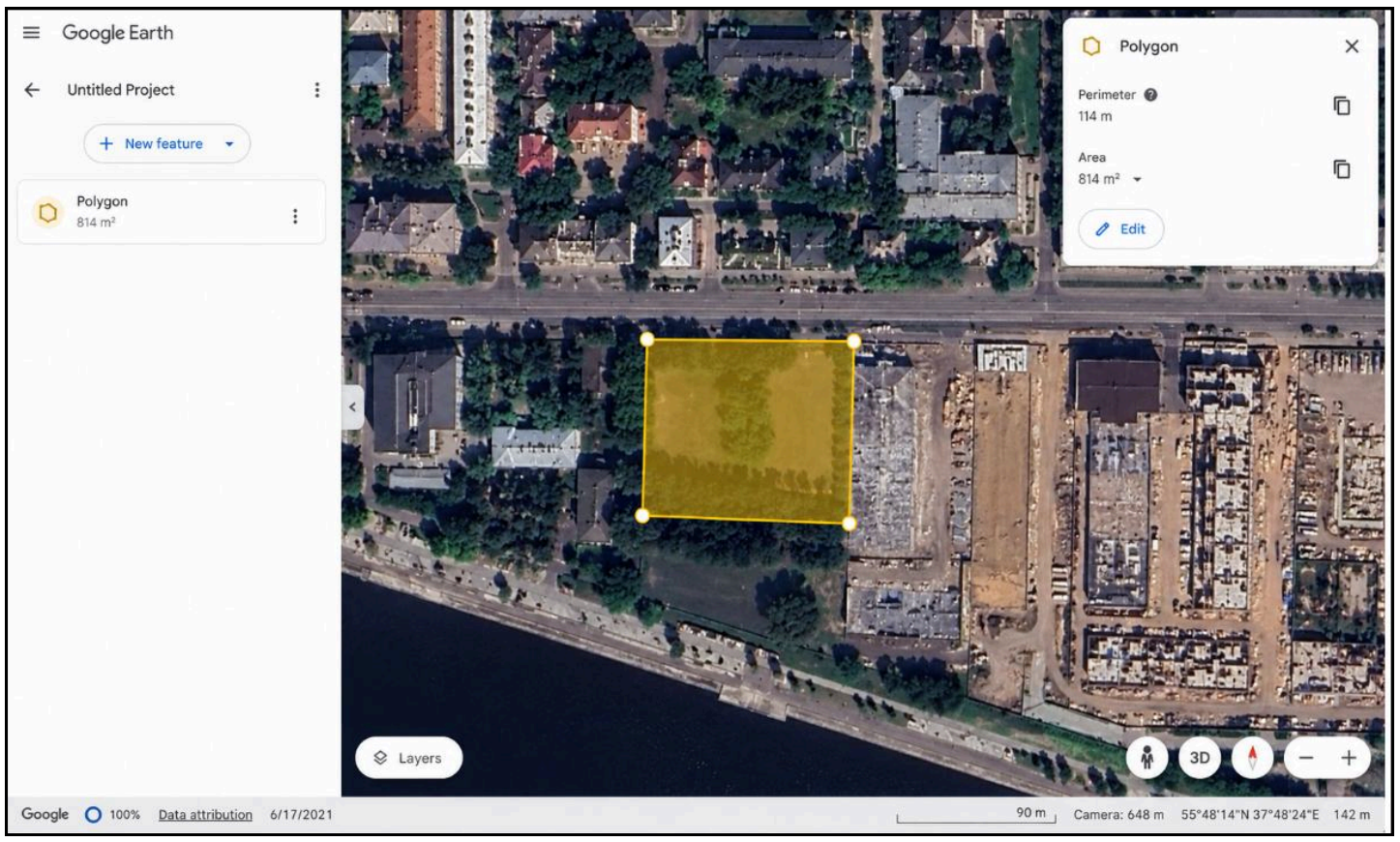
After this, lateral movement within the network takes place in order to expand control and gain access to critical nodes. During the attack preparation stage, malicious components are deployed and the coordinated execution of destructive code is configured.

The final phase is characterised by the activation of the wiper mechanism, which results in data destruction, disruption of operating systems and disabling of server infrastructure. In parallel, an information component is implemented, aimed at psychological pressure and destabilisation, including the publication of messages and dissemination of stolen data.

As a result, the attack leads not only to the technical destruction of systems but also to reduced trust in government digital services, which reinforces the overall destabilising effect.

Location

Military Unit 29155 (161st GRU Centre) and associated cyber cluster groups
Moscow, 11th Parkovaya Street, Building 38A
Coordinates: 55.801–55.803 N, 37.805–37.808 E



Contour of the investigated area defined by coordinates 55.801–55.803 N, 37.805–37.808 E

Support the organization’s activities: https://donate.shum-ng.org/

Contour of the investigated area based on coordinates 55.801–55.803 N, 37.805–37.808 E (Moscow)

The highlighted area represents a rectangular section of urban development defined by coordinates 55.801–55.803 N, 37.805–37.808 E. The contour is used for the analysis of satellite imagery and the structure of the urban environment.

TTP Table:
Ember Bear (DEV-0586 / Cadet Blizzard) — WhisperGate

Phase (Tactic)	Technique (MITRE ATT&CK)	Behaviour Description (specific to the group)
🟢 **Initial Access**	Phishing (T1566)	Use of phishing emails with malicious attachments or links for initial intrusion
🟢 **Initial Access**	Exploit Public-Facing Application (T1190)	Exploitation of vulnerabilities in public-facing services (servers, web applications)
🟡 **Execution**	PowerShell (T1059.001)	Execution of malicious scripts to download and execute payloads
🟡 **Execution**	Windows Command Shell (T1059.003)	Use of cmd.exe to execute commands and scripts
🔵 **Reconnaissance**	System/Network Discovery (T1018, T1046)	Network scanning, identification of servers, domains and critical systems
🔵 **Reconnaissance**	Account Discovery (T1087)	Collection of information about users and administrative accounts
🟠 **Persistence / Movement**	Remote Services (T1021)	Use of RDP/SMB for lateral movement across the network
🟠 **Persistence / Movement**	Valid Accounts (T1078)	Use of stolen or legitimate credentials
🟠 **Lateral Movement**	Pass-the-Hash (T1550.002)	Use of password hashes to access other systems
🟣 **Attack Preparation**	Scheduled Task (T1053)	Creation of tasks to execute malicious code at a specified time
🟣 **Attack Preparation**	Obfuscated/Encoded Files (T1027)	Obfuscation of malicious components before activation
🔴 **Destruction (Impact)**	Disk Wipe (T1561.002)	Destruction of disk structures (MBR/boot)
🔴 **Destruction (Impact)**	Data Destruction (T1485)	Mass destruction of files and data on systems
🔴 **Destruction (Impact)**	System Shutdown/ Reboot (T1529)	Forced reboots and disruption of system functionality
⚫ **Defence Evasion**	Indicator Removal (T1070)	Deletion of files and logs after execution of the attack
🟤 **Psychological Impact**	Defacement (T1491)	Messages/demand screens and demonstrative messages to victims

WhisperGate should be considered a representative example of a modern destructive cyber operation, where technical complexity is combined with a clearly defined destructive objective. It was not a classic cyber espionage campaign or an attempt to obtain financial gain — the primary focus was on maximising disruption of system functionality and creating the effect of sudden digital disorganisation.

It is particularly important that such an attack demonstrates a multi-stage impact model: from initial intrusion and persistence within the infrastructure to the final phase of data destruction and system disruption. This indicates a high level of planning and coordination, characteristic of organised state-level cyber operations.

At the same time, WhisperGate highlights that modern cyber threats extend beyond the purely technical domain. In addition to the physical destruction of data, the psychological and information impact plays an important role, aimed at destabilisation and undermining trust in digital infrastructure.

Thus, this operation is a clear example of how cyberspace is used as a tool of hybrid influence, where technical attacks become part of broader strategic and political objectives.

SOURCES

1. https://attack.mitre.org/groups/G1003/
2. https://www.microsoft.com/security/blog/2024/01/25/cadet-blizzard-emerges-as-a-novel-threat-actor/
3. https://www.cisa.gov/sites/default/files/2024-09/aa24-249a-russian-military-cyber-actors-target-us-and-global-critical-infrastructure.pdf
4. https://www.crowdstrike.com/blog/who-is-ember-bear/
5. https://www.paloaltonetworks.com/blog/security-operations/whispergate-malware-analysis/
6. https://unit42.paloaltonetworks.com/ukraine-cyber-attacks/
7. https://www.mandiant.com/resources/blog/ukraine-cyber-threat-activity
8. https://www.s2w.inc/blog/whispergate-analysis
9. https://arxiv.org/abs/2510.18484
10. https://war-sanctions.gur.gov.ua/ru/sanctions/persons/36234
11. https://thehackernews.com/2024/09/us-offers-10-million-for-info-on.html
12. https://www.opensanctions.org/entities/NK-eeazQVNhtHhNCisAvwakVv/
13. https://rewardsforjustice.net/rewards/gru-officers-unit-29155/
14. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/?ocid=magicti_ta_blog
15. https://www.golosameriki.com/a/russia-father-son-accused-cybercrimes-gru/7701912.html