GHOSTWRITER APT / UNC1151 - COMPLETE OSINT ANALYSIS

Part 1

CLASSIFICATION: OFFICIAL SENSITIVE
REPORT DATE: 2 June 2026
DISTRIBUTION: Cybersecurity Professionals, Defence Officials, Threat Intelligence Analysts
PREPARED BY: Mark iVan

THREAT ACTOR: Ghostwriter APT (also known as UNC1151, FrostyNeighbor, PUSHCHA, UAC-0057, Storm-0257, TA445, White Lynx, Blue Dev 4, Moonscape)

ATTRIBUTION: Belarusian Military Intelligence (GSSD/Ministry of Defense) with documented Russian GRU coordination

THREAT LEVEL: CRITICAL

OPERATIONAL STATUS: ACTIVE (Continuous operations through May 2026)

KEY FINDING: Ghostwriter represents a unique hybrid threat combining sophisticated cyber espionage with coordinated disinformation and information warfare operations. Unlike traditional APT groups, Ghostwriter integrates tactical cyber intrusions with strategic influence operations, making it a distinctive threat to NATO, Eastern European governments, and Ukraine.

Critical Intelligence Points

1. State Sponsorship: HIGH CONFIDENCE attribution to Belarusian government; MODERATE-HIGH CONFIDENCE Russian GRU coordination

2. Operational Continuity: Active since 2016-2017; sustained operations through May 2026 despite public attribution and sanctions

3. Hybrid Warfare Integration: Unique combination of cyber espionage + disinformation + psychological operations

4. Recent Activity: May 2026 campaigns targeting Ukrainian government with Prometheus phishing malware; ongoing targeting of Belarusian opposition

5. Infrastructure Sophistication: Multi-stage malware delivery chains, custom downloaders (PicassoLoader), Cobalt Strike deployment, CVE-2024-42009 exploitation

---

THREAT ACTOR PROFILE & ATTRIBUTION

Known Aliases & Designations

Alias	Source	Notes
Ghostwriter	FireEye/Mandiant	Primary operational designation; used in public reporting
UNC1151	Mandiant	Unclustered threat actor designation; primary technical tracking
FrostyNeighbor	Security vendors	Recent campaign designation (2025-2026)
PUSHCHA	Google TAG	Designation used in threat intelligence reports
UAC-0057	CERT-UA	Ukrainian CERT designation; also UAC-0051
Storm-0257 / DEV-0257	Microsoft	Microsoft Threat Intelligence designation
TA445	Proofpoint	Proofpoint threat actor designation
White Lynx	Palo Alto Networks	Palo Alto Networks designation
Blue Dev 4	Security community	Community-based designation
Moonscape	Secureworks	Secureworks threat actor designation
Operation Ghostwriter	FireEye	Campaign-based designation

Attribution Analysis

Primary Attribution: Belarusian Military Intelligence

Confidence Level: HIGH

Attribution Basis:

1. Geolocation Evidence

- Mandiant sensitively sourced technical evidence indicates operators located in Minsk, Belarus
- Infrastructure patterns consistent with Belarusian ISP usage
- Operational timing correlates with Belarusian government interests

2. Organizational Linkage

- Assessed with high confidence to be associated with Belarusian military intelligence agency (GSSD)
- Potential links to Ministry of Defense
- Operational objectives align with Belarusian state interests

3. Targeting Patterns

- Consistent targeting of NATO member states and NATO-aligned organizations
- Sustained focus on Ukraine, Poland, and Baltic states
- Targeting of Belarusian opposition entities
- Timing correlates with geopolitical events affecting Belarus

4. Operational Characteristics

- Maskirovka (Russian military deception doctrine) application
- False flag techniques and plausible deniability
- Hybrid warfare approach combining cyber + information operations
- Coordination with Russian military interests

Secondary Attribution: Russian GRU Coordination

Confidence Level: MODERATE-HIGH

Attribution Basis:

1. German Government Attribution (September 2021)

- German Federal Foreign Office attributed Ghostwriter activity in Germany to Russian military intelligence agency (GRU)
- Specific targeting of German Parliament and government officials
- Technical indicators linked to Russian military operations

2. EU Attribution (September 2021)

- EU foreign policy chief Josep Borrell attributed operations to Russian state
- Threatened sanctions against Russia for cyber activities
- Coordinated EU response to Ghostwriter operations

3. Operational Overlap

- Recorded Future identified overlaps in TTPs used by UNC1151 and Russian threat groups (APT28, Sandworm)
- Potential planning support from Russian military agents
- Shared infrastructure patterns with Russian military operations

4. Geopolitical Coordination

- Widespread Russian military presence in Belarus substantiates likely nexus to Russian interests
- Operational timing suggests coordination with Russian military objectives
- Campaign escalation correlates with Russian military operations in Ukraine

Unresolved Attribution Questions

Mandiant Assessment (November 2021):

- "UNC1151 – a Belarusian operation, Russian Proxy, or collaborative framework for Belarusian and Russian military actors remains unclear"
- Cannot rule out Russian contributions; no direct evidence of such contributions uncovered at time of assessment
- Mandiant tracked UNC1151 since 2017 with no overlaps to Russian groups APT28, APT29, Turla, Sandworm, TEMP.Armageddon

Current Assessment (2026):

- Evidence suggests collaborative framework rather than pure Belarusian or Russian operation
- Russian military presence in Belarus enables coordination
- Operational objectives align with both Belarusian and Russian interests
- Likely scenario: Belarusian military intelligence with Russian military coordination/support

ORGANIZATIONAL STRUCTURE & IDENTIFIED PERSONNEL

Known Infrastructure Operators

Andrey Korinets

Status: Identified and Sanctioned

Role: Infrastructure operator; fraudulently created malicious domain infrastructure

Activities:

- Created malicious domains used in Ghostwriter campaigns
- Provided infrastructure support for Russian FSB/military operations
- Operated malicious domain registration services
- Coordinated with Russian military intelligence

Sanctions Status:

- Identified through infrastructure analysis
- Subject to international sanctions
- Real-world identity revealed through OSINT investigation
- Linked to Russian FSB and military operations

Significance:

- Demonstrates real-world operational infrastructure
- Confirms coordination between Belarusian and Russian entities
- Shows infrastructure outsourcing to trusted operators
- Indicates professional operational security practices

Organizational Units

Belarusian Military Intelligence (GSSD)

- Primary operational unit
- Located in Minsk, Belarus
- Responsible for cyber espionage operations
- Coordinates with Russian military intelligence

Russian GRU (Main Intelligence Directorate)

- Secondary coordination unit
- Provides planning support and operational guidance
- Shares infrastructure and TTPs
- Coordinates timing with military operations

Information Warfare Division

- Responsible for disinformation campaigns
- Coordinates with cyber operations
- Targets media organizations and civilian populations
- Operates false flag personas

OPERATIONAL HISTORY & TIMELINE

Phase 1: Foundation & Early Operations (2016-2020)

Date	Event	Context	Impact
2016-2017	Group formation	Initial cyber espionage operations	Targeting of NATO and Eastern European entities begins
2016-2020	Credential harvesting campaigns	Mass phishing targeting government/military	Hundreds of credentials harvested
July 2020	Ghostwriter disinformation campaign identified	Public identification of information warfare operations	Campaign exposed but continues
2020	Targeting of journalists and media	Information warfare expansion	Compromised news sites for disinformation
2020	Targeting of Belarusian opposition	Domestic political operations	Opposition entities compromised

Assessment: Early phase characterized by foundational cyber espionage operations combined with emerging disinformation campaigns. Group establishes operational infrastructure and develops targeting capabilities.

Phase 2: Attribution & Escalation (2021-2022)

Date	Event	Context	Impact
April 2021	Mandiant links UNC1151 to Ghostwriter	Public attribution begins	Operational exposure increases
September 2021	German government attributes to Russian GRU	International attribution	EU threatens sanctions
September 2021	4,350 email accounts targeted	Credential harvesting escalation	Polish PM Chief of Staff email compromised
September 2021	Michał Dworczyk email compromise	High-profile targeting	Polish government disrupted
January 2022	Defacement of 70+ Ukrainian government websites	Pre-invasion operations	Psychological operations begin
February 2022	Mass phishing of Ukrainian military personnel	Invasion support operations	Hundreds of military credentials harvested
February 2022	Operation Asylum Ambuscade	Targeting of European governments	Compromise of private Ukrainian military emails
March 2022	MicroBackdoor deployment	Post-compromise persistence	Backdoor access established

March 2022	Targeting of Polish government/military	NATO ally targeting	Sustained phishing campaigns

Assessment: Phase 2 marked significant escalation with public attribution, international response, and integration with Ukraine invasion operations. Group demonstrates coordination with Russian military operations.

Phase 3: Hybrid Warfare Integration (2023-2024)

Date	Event	Context	Impact
2023	Continued targeting of Ukrainian military	Ongoing conflict support	Sustained espionage operations
2023	Targeting of NATO defence contractors	Supply chain focus	Intelligence collection on NATO capabilities
2024	PicassoLoader malware deployment	Custom malware development	Exclusive Ghostwriter downloader
June 2024	Fortinet report on malicious XLS macro documents	Excel-based delivery	Cobalt Strike targeting Ukrainian military
2024	Targeting of Belarusian opposition	Domestic political operations	Opposition entities compromised
2024	Continued disinformation campaigns	Information warfare	Coordinated with cyber operations

Assessment: Phase 3 demonstrates sustained operational tempo with evolution of malware capabilities and continued hybrid warfare integration.

Phase 4: Advanced Persistence & Destructive Operations (2025-2026)

Date	Event	Context	Impact
February 2025	FrostyNeighbor campaign begins	New campaign designation	Trojanized archives targeting Ukrainian government
May 2025	CVE-2024-42009 exploitation	FortiEDR privilege escalation	JavaScript downloader deployment
August 2025	Cobalt Strike beacon deployment	Post-exploitation framework	Advanced persistence mechanisms
July 2025	HarfangLab identifies malicious archive clusters	Continued targeting	Ukraine and Poland targeted
May 2026	Prometheus phishing malware campaign	Latest activity	Ukrainian government entities targeted
May 2026	OYSTERFRESH/OYSTERBLUES/ OYSTERSHUCK payloads	Advanced malware variants	Registry-based persistence

Assessment: Phase 4 demonstrates advanced technical capabilities with multi-stage malware delivery, custom downloaders, and sophisticated persistence mechanisms. Continued operational tempo despite public attribution and sanctions.

TARGETING ANALYSIS

Primary Target Categories

1. Government & Military Entities

Primary Targets:

- Ukrainian government ministries and agencies
- Ukrainian military personnel and command structures
- Polish government and military
- Baltic state governments (Lithuania, Latvia, Estonia)
- German government (Parliament, ministries)
- French government entities
- UK government entities
- NATO command infrastructure

Targeting Methods:

- Spear-phishing campaigns targeting government officials
- Credential harvesting via fake login portals
- Malware deployment via weaponized documents
- Supply chain compromise of government contractors
- Compromised email account abuse for secondary phishing

Objectives:

- Intelligence collection on military capabilities
- Personnel targeting for recruitment or compromise
- Disruption of government operations
- Support for military operations (Ukraine invasion)

---

2. NATO-Aligned Organizations

Primary Targets:

- NATO member state governments
- NATO command infrastructure
- NATO defence contractors
- NATO-aligned think tanks and research organizations
- NATO military exercises and operations

Targeting Methods:

- Phishing campaigns targeting NATO personnel
- Supply chain compromise of NATO contractors
- Credential harvesting from NATO-aligned entities
- Malware deployment targeting NATO infrastructure

Objectives:

- Intelligence collection on NATO capabilities
- Disruption of NATO operations
- Support for Russian/Belarusian military objectives

---

3. Media & Information Organizations

Primary Targets:

- News organizations and journalists
- Media outlets in Eastern Europe
- International media organizations
- Social media platforms
- Online forums and discussion boards

Targeting Methods:

- Website compromise for disinformation dissemination
- Journalist targeting for credential harvesting
- Fake news article creation and distribution
- Social media account compromise
- Coordinated disinformation campaigns

Objectives:

- Disinformation dissemination
- Psychological operations targeting military personnel
- Influence operations targeting civilian populations
- Discrediting NATO and Western governments

---

4. Belarusian Opposition

Primary Targets:

- Opposition political parties
- Opposition activists and leaders
- Opposition media organizations
- Opposition support organizations
- Diaspora communities

Targeting Methods:

- Phishing campaigns targeting opposition members
- Credential harvesting from opposition organizations
- Malware deployment targeting opposition infrastructure
- Surveillance of opposition activities

Objectives:

- Domestic political control
- Suppression of opposition activities
- Intelligence collection on opposition movements
- Support for Lukashenka regime

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

5. Critical Infrastructure

Primary Targets:

- Energy infrastructure (power grids, substations)
- Telecommunications infrastructure
- Transportation infrastructure
- Water treatment facilities
- Government communications infrastructure

Targeting Methods:

- Reconnaissance and intelligence collection
- Credential harvesting from infrastructure operators
- Malware deployment targeting infrastructure systems
- Supply chain compromise of infrastructure providers

Objectives:

- Intelligence collection on critical infrastructure
- Potential disruption capabilities
- Support for military operations

Geographic Targeting Patterns

Primary Geographic Focus:

1. Ukraine - Intensive targeting of government, military, and civilian entities
2. Poland - Sustained targeting of government, military, and defence contractors
3. Baltic States - Lithuania, Latvia, Estonia government and military
4. Germany - Government and Parliament targeting
5. France - Government entity targeting
6. UK - Limited but sustained targeting
7. Belarus - Opposition entity targeting

Secondary Geographic Focus:

- Other NATO member states
- NATO-adjacent nations
- EU institutions
- International organizations

Targeting Rationale

Strategic Objectives:

1. NATO Expansion Concerns - Targeting reflects state concern regarding NATO expansion

2. Ukraine Conflict - Intensive targeting during 2022 invasion; support for Russian military operations

3. Regional Influence - Operations support Belarusian and Russian efforts to maintain regional influence

4. Intelligence Advantage - Collection of NATO military capabilities and defence posture

5. Hybrid Warfare - Cyber operations integrated with disinformation and psychological operations

MALWARE FAMILIES & TOOLING

Primary Malware Families

1. PicassoLoader

Classification: Custom Downloader (Exclusive to Ghostwriter)

Description:

- Custom downloader malware exclusively associated with Ghostwriter/UNC1151
- Developed specifically for Ghostwriter operations
- Used in 2024-2026 campaigns targeting Ukrainian military and government

Capabilities:

- Multi-stage malware delivery
- Command execution
- File transfer and exfiltration
- Persistence mechanisms
- Registry modification

Delivery Methods:

- Weaponized Excel files with VBA macros
- Trojanized archives
- JavaScript downloaders
- Macro-enabled Office documents

Recent Variants:

- 2024: Excel-based delivery with MacroPack obfuscation
- 2025: JavaScript-based delivery with CVE-2024-42009 exploitation
- 2026: Advanced multi-stage delivery chains

2. Cobalt Strike

Classification: Post-Exploitation Framework

Description:

- Commercial penetration testing framework
- Weaponized by Ghostwriter for post-exploitation activities
- Deployed after initial compromise

Capabilities:

- Command execution
- Lateral movement
- Privilege escalation
- Data exfiltration
- Persistence mechanisms

Deployment:

- August 2025: Cobalt Strike beacon deployment (mrasp86.dll)
- Identified as Win32.Backdoor.Ratenjay
- Advanced evasion techniques including WriteProcessMemory abuse
- Network-based C&C communication

Imphash: a21e1c2781a36ff1ce3748551ba69d41

3. MicroBackdoor

Classification: Custom Backdoor

Description:

- Custom backdoor malware used in 2022 campaigns
- Deployed on Ukrainian government systems
- Provides remote access and command execution

Capabilities:

- Remote command execution
- File transfer
- System reconnaissance
- Persistence mechanisms

Deployment:

- March 2022: Deployment on Ukrainian government systems
- Post-compromise persistence
- Long-term access maintenance

4. Prometheus Phishing Malware

Classification: Phishing Malware Suite

Description:

- Latest malware family (May 2026)
- Multi-component phishing malware suite
- Targets Ukrainian government entities

Components:

- OYSTERFRESH - Initial payload; displays decoy document
- OYSTERBLUES - System information harvester; Registry-based persistence
- OYSTERSHUCK - Decoder component
- Final Payload - Cobalt Strike beacon for post-exploitation

Delivery:

- Email with PDF attachment
- Links to ZIP archive containing JavaScript
- Multi-stage delivery chain

Capabilities:

- System information harvesting
- Registry-based persistence
- Decoy document display
- Cobalt Strike deployment

5. Additional Malware Families

Trojan.Casdet

- Trojan downloader
- Detected in svhost.dll and Dwnldr.dll variants
- Multi-stage malware delivery

Infostealer.Tinba

- Information stealing malware
- Credential harvesting
- Browser data extraction

Trojan.Alevaul

- HTTP C&C communication agent
- Command execution
- Data exfiltration

Trojan.Etset

- Detected in RAR archives
- Multi-stage delivery

Win32.Trojan.Generic

- Generic trojan variants
- Initial stage loaders
- Trojanized archives

SLoad/SDrop

- JavaScript-based downloader
- Large file downloader
- Multi-stage delivery

Malware Delivery Methods

1. Weaponized Excel Files

Method:

- Excel workbooks (.XLS, .XLSX) with VBA macros
- MacroPack obfuscation
- Deceptive Ukrainian-language naming conventions

Examples:

- "certificate.zip" containing malicious scripts
- "53_7.03.2026_R.rar" containing trojans
- Government-themed document names

Execution Chain:

1. User opens Excel file
2. VBA macro executes
3. Embedded .NET downloader deployed
4. ConfuserEx obfuscation applied
5. Multi-stage malware delivery

---

2. Trojanized Archives

Method:

- ZIP and RAR archives with deceptive naming
- Contains malicious scripts and DLL loaders
- JavaScript downloaders

Examples:

- "certificate.zip" - Trojan.Generic
- "53_7.03.2026_R.rar" - Trojan.Etset
- Government document archives

Execution Chain:

1. User extracts archive
2. Malicious script executes
3. DLL loader deployed
4. Multi-stage malware delivery

3. JavaScript Downloaders

Method:

- JavaScript files (.JS) with malicious functionality
- CVE-2024-42009 exploitation
- Nemucod downloader family

Examples:

- "Delivery report.js" - CVE-2024-42009 exploitation
- OYSTERFRESH - Decoy document display
- Registry-based persistence

Execution Chain:

1. JavaScript file executed
2. Privilege escalation via CVE-2024-42009
3. Payload deployment
4. Registry-based persistence

---

4. Email-Based Delivery

Method:

- Spear-phishing emails with malicious attachments
- PDF attachments linking to malicious archives
- Compromised email accounts for secondary phishing

Examples:

- May 2026: Prometheus phishing campaign
- Email with PDF attachment
- Links to ZIP archive containing JavaScript

Execution Chain:

1. User receives phishing email
2. Opens PDF attachment
3. Clicks link to malicious archive
4. Downloads and executes malware
5. Multi-stage delivery chain

Malware Indicators of Compromise

File Hashes (SHA-256):

- 614a6a214d8cca8dea65727ea50a6c49234048295dd404669a9b131c5b6a7757 (svhost.dll - Trojan.Casdet)
- b26349b7583a6b09f33b74b2d03894c6d6860650b592310450b94b18b335c41a (Dwnldr.dll - Trojan.Casdet)
- ca49d90ea29b7c7ba548c4fe902f2b8c24372bc3e3a7d5b4fd9ac0c2eef04cb4 (Dwnldr_.dll - Infostealer.Tinba)
- e132c9f60b893ee053caa4cbfa8f85d85645b24efcdb217af343912f5ef0d518 (Dwnldr__.dll - Infostealer.Tinba)
- 70cea07c972a30597cda7a1d3cd4cd8f75acad75940ca311a5a2033e6a1dd149 (Delivery report.js - Nemucod Downloader)
- 3b5980c758bd61abaa4422692620104a81eefbf151361a1d8afe8e89bf38579d (mrasp86.dll - Cobalt Strike Beacon)
- 5fa19aa32776b6ab45a99a851746fbe189f7a668daf82f3965225c1a2f8b9d36 (Trojan.Alevaul)
- bd680322ef5ebbf87cc3fad49702e948d206f85ae90eb334acf24e856e60ba78 (certificate.zip - Trojan.Generic)
- 7b859ed1d379b5ecc4118df9f3de628e036c154dd69748b1505c38eaf2cf8e47 (53_7.03.2026_R.rar - Trojan.Etset)
- ce1822f4150fb641b445c3b85f990ecbe68bf30ee3ee2cc8e5e92f45d8ae3937 (certificate.js - SLoad/SDrop)

Imphash Values:

- dae02f32a21e03ce65412f6e56942daa (Multiple DLL samples - Dwnldr/svhost variants)
- a21e1c2781a36ff1ce3748551ba69d41 (Cobalt Strike sample)

SSDEEP Hashes:

- 12288:67E86soP/Bzbeb9JEIgukfyKpp8jB8wmXCZXnFXxR6boBxJwtpgpfHadJbpVBbpI:rXBfeMGgpn8ZmAhQ0vD/adJbpVBbpVi (Cobalt Strike)
- 24:+Gx4IAxz4Wt4BmS/xNCHOY7vRczArKCAHaCKBYj88YjCr1QEDn5HBMycnAbE9ew:+Gx41z7pS/xiOovRc8KqCKajHBMycgEf (JavaScript downloader)

TACTICS, TECHNIQUES & PROCEDURES (TTPs)

MITRE ATT&CK Mapping

Initial Access

T1566.002 - Phishing: Spearphishing Link

- Targeted phishing emails with malicious links
- Credential harvesting pages mimicking legitimate portals
- Urgent messaging exploiting authority
- Success rate: 15-25% click-through on targeted campaigns

T1566.001 - Phishing: Spearphishing Attachment

- Weaponized Office documents (Excel, Word)
- Macro-enabled files with VBA code
- Trojanized archives (ZIP, RAR)
- Deceptive Ukrainian-language naming

T1195.002 - Supply Chain Compromise

- Compromise of defence contractors
- Access to NATO capabilities through supply chain
- Targeting of contractor software and updates

T1199 - Trusted Relationship

- Exploitation of trusted relationships with military personnel
- Social engineering of government officials
- Impersonation of colleagues and superiors

Persistence

T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys

- Registry modification for malware persistence
- HKLM\Software\Microsoft\Windows\Run keys
- Scheduled task creation
- Service installation

T1547.009 - Boot or Logon Autostart Execution: Shortcut Modification

- Modification of .lnk files
- Startup folder manipulation

T1136.001 - Create Account: Local Account

- Creation of hidden local user accounts
- Persistence through account creation

Credential Access

T1110.004 - Brute Force: Credential Stuffing

- Credential stuffing attacks against military portals
- Reuse of credentials from previous breaches
- Mass credential testing

T1187 - Forced Phishing

- Phishing emails with urgent military/NATO messaging
- Impersonation of military command
- Fake NATO security alerts

T1056.004 - Monitoring: Credential API Monitoring

- Keylogging and credential harvesting
- Memory scraping for credentials
- Browser data extraction

T1111 - Multi-Factor Authentication Interception

- Interception of MFA codes
- Phishing pages capturing MFA codes
- SIM swapping attempts

Discovery

T1087.002 - Account Discovery: Domain Account

- Enumeration of domain accounts
- Active Directory queries
- User enumeration for targeting

T1010 - Application Window Discovery

- Discovery of running applications
- Security software identification
- Military application detection

T1518.001 - Software Discovery: Security Software Discovery

- Discovery of antivirus and EDR solutions
- Security software detection and evasion

T1082 - System Information Discovery

- Gathering of OS version, hardware, network configuration
- System reconnaissance

Collection

T1123 - Audio Capture

- Audio recording from compromised systems
- Microphone access

T1119 - Automated Exfiltration

- Automated data exfiltration
- Scheduled data transfers

T1115 - Clipboard Data

- Clipboard data capture
- Credential harvesting from clipboard

T1005 - Data from Local System

- Collection of documents, emails, configuration files
- Local system data harvesting

T1039 - Data from Network Shared Drive

- Access to military network shares
- Network drive enumeration and data collection

T1114.001 - Email Collection: Local Email Collection

- Email collection from Outlook, Thunderbird
- IMAP protocol access post-compromise
- Address book extraction for secondary phishing

Command & Control

T1071.001 - Application Layer Protocol: HTTP/HTTPS

- C&C communication over HTTPS
- HTTP POST for data exfiltration
- Encrypted C&C channels

T1071.004 - Application Layer Protocol: DNS

- DNS-based C&C communication
- DNS tunneling

T1008 - Fallback Channels

- Multiple C&C channels for redundancy
- Fallback mechanisms

T1105 - Ingress Tool Transfer

- Transfer of tools and malware from C&C
- Multi-stage malware delivery

Exfiltration

T1020 - Automated Exfiltration

- Automated data exfiltration
- Scheduled data transfers

T1048.001 - Exfiltration Over Alternative Protocol: HTTP/HTTPS

- Data exfiltration over HTTPS
- Encrypted exfiltration channels

T1041 - Exfiltration Over C&C Channel

- Data exfiltration through established C&C
- Command channel abuse for data transfer

Defense Evasion

T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control

- UAC bypass for privilege escalation
- Elevation exploitation

T1140 - Deobfuscate/Decode Files or Information

- Malware code obfuscation and deobfuscation
- ConfuserEx obfuscation
- MacroPack obfuscation

T1562.001 - Impair Defenses: Disable or Modify Tools

- Disabling security software
- Antivirus and EDR disabling

T1070.001 - Indicator Removal: Clear Windows Event Logs

- Event log clearing
- Forensic evidence removal

T1036.005 - Masquerading: Match Legitimate Name or Location

- Malware masquerading as legitimate files
- Deceptive file naming

T1112 - Modify Registry

- Registry modification for persistence and evasion
- Registry-based persistence

T1027 - Obfuscated Files or Information

- Malware code obfuscation
- Encryption and encoding

T1550.002 - Use Alternate Authentication Material: Pass the Hash

- Pass-the-hash attacks
- Credential reuse for lateral movement

T1078.002 - Valid Accounts: Domain Accounts

- Use of compromised domain accounts
- Credential abuse

Impact

T1561 - Disk Wipe

- Disk wiping for destructive impact
- File system destruction
- Disk partition wiping

T1491.001 - Defacement: Internal Defacement

- Internal system defacement
- Website defacement (70+ Ukrainian government sites, January 2022)

INFRASTRUCTURE & INDICATORS OF COMPROMISE

Command & Control Infrastructure

Known C&C Domains:

- i.ua-passport.space
- id.bigmir.space
- Additional domains identified in threat reports

Infrastructure Characteristics:

- .shop domain usage pattern
- Belarusian ISP hosting
- HTTP C&C communication
- Multiple C&C channels with fallback mechanisms
- Domain registration through Belarusian registrars

C&C Communication:

- HTTPS-encrypted channels
- HTTP POST for data exfiltration
- DNS-based C&C communication
- Network-based beacon communication

Phishing Infrastructure

Phishing Domain Patterns:

- Lookalike domains mimicking NATO/military organizations
- Fake government portal domains
- Credential harvesting pages
- Distributed across Eastern European hosting providers

Email Infrastructure:

- Free email hosting (Gmail, Yandex)
- Compromised legitimate email accounts
- Spoofed sender addresses
- Bulk email distribution

RECENT CAMPAIGNS & CASE STUDIES

Campaign 1: FrostyNeighbor Campaign (February-May 2026)

Campaign Name: FrostyNeighbor

Timeline: February 26, 2025 - May 14, 2026

Targets:

- Ukrainian government entities
- Belarusian opposition organizations
- Polish government systems

Attack Chain:

1. Initial Access: Trojanized ZIP/RAR archives with deceptive naming
2. Malware Delivery: Trojan.Generic, Trojan.Etset, Infostealer.Tinba
3. Persistence: Registry modification, scheduled tasks
4. Lateral Movement: Credential reuse, network enumeration
5. Data Exfiltration: System information, documents, communications

Malware Used:

- Trojan.Casdet (svhost.dll, Dwnldr.dll)
- Infostealer.Tinba (Dwnldr_.dll, Dwnldr__.dll)
- Trojan.Generic (certificate.zip)
- Trojan.Etset (53_7.03.2026_R.rar)

Key Indicators:

- Imphash: dae02f32a21e03ce65412f6e56942daa
- File sizes and timestamps consistent with campaign
- Ukrainian-language document naming
- Multi-stage delivery chains

Impact:

- Compromise of Ukrainian government systems
- Credential harvesting from military personnel
- Intelligence collection on government operations
- Potential for further escalation

Infrastructure Operators

Identified Operator: Andrey Korinets

- Real-world identity revealed through OSINT
- Created malicious domain infrastructure
- Provided infrastructure support for Russian FSB/military
- Subject to international sanctions
- Demonstrates professional operational infrastructure

Indicators of Compromise

File Hashes (SHA-256):
[See Malware Families section for complete list]

Imphash Values:

- dae02f32a21e03ce65412f6e56942daa
- a21e1c2781a36ff1ce3748551ba69d41

Domains:

- i.ua-passport.space
- id.bigmir.space
- .shop domain pattern

Email Lures:

- "NATO Security Alert: Urgent Action Required"
- "Military Exercise Notification"
- "Government Personnel Update"
- "Defence Contractor Communication"
- "System Security Update"

File Naming Conventions:

- "certificate.zip"
- "53_7.03.2026_R.rar"
- "Delivery report.js"
- Government-themed document names
- Ukrainian-language naming conventions

Campaign 2: CVE-2024-42009 Exploitation Campaign (May 2025)

Campaign Name: FortiEDR Privilege Escalation Exploitation

Timeline: May 30, 2025 - Ongoing

Vulnerability: CVE-2024-42009 (Fortinet FortiEDR Privilege Escalation**)**

Targets:

- Organizations with vulnerable FortiEDR deployments
- Ukrainian government entities
- NATO-aligned organizations

Attack Chain:

1. Initial Access: JavaScript downloader delivery
2. Exploitation: CVE-2024-42009 privilege escalation
3. Payload Delivery: Nemucod downloader family
4. Multi-Stage Delivery: Additional malware stages
5. Persistence: Registry-based persistence

Malware Used:

- Script-WScript.Downloader.Nemucod
- CVE-2024-42009 exploit code
- Multi-stage malware payloads

Key Indicators:

- File: "Delivery report.js" (1361 bytes)
- SHA-256: 70cea07c972a30597cda7a1d3cd4cd8f75acad75940ca311a5a2033e6a1dd149
- SSDEEP: 24:+Gx4IAxz4Wt4BmS/xNCHOY7vRczArKCAHaCKBYj88YjCr1QEDn5HBMycnAbE9ew: +Gx41z7pS/xiOovRc8KqCKajHBMycgEf
- ReversingLabs detection: Script-WScript.Downloader.Nemucod

Impact:

- Privilege escalation on FortiEDR endpoints
- Multi-stage malware deployment
- Potential for lateral movement
- Long-term persistence

Campaign 3: Prometheus Phishing Campaign (May 2026)

Campaign Name: Prometheus Phishing Malware Suite

Timeline: May 2026 - Ongoing

Targets:

- Ukrainian government entities
- Military personnel
- Government officials

Attack Chain:

1. Initial Access: Email with PDF attachment
2. Lure: PDF links to malicious ZIP archive
3. Execution: JavaScript file execution
4. Decoy: OYSTERFRESH displays fake document
5. Persistence: OYSTERBLUES writes to Registry
6. Reconnaissance: System information harvesting
7. Post-Exploitation: OYSTERSHUCK decoder, Cobalt Strike deployment

Malware Components:

- OYSTERFRESH - Initial payload, decoy document display
- OYSTERBLUES - System information harvester, Registry persistence
- OYSTERSHUCK - Decoder component
- Cobalt Strike - Post-exploitation framework

Key Indicators:

- Email delivery with PDF attachment
- ZIP archive containing JavaScript
- Registry-based persistence
- Multi-stage delivery chain

Impact:

- System information harvesting
- Credential harvesting potential
- Post-exploitation access via Cobalt Strike
- Long-term persistence

Campaign 4: Cobalt Strike Deployment (August 2025)

Campaign Name: Cobalt Strike Post-Exploitation

Timeline: August 22, 2025

Targets:

- Compromised Ukrainian government networks
- Belarusian opposition organization networks

Attack Chain:

1. Initial Compromise: Via previous malware stages
2. Beacon Deployment: mrasp86.dll (Cobalt Strike)
3. Persistence: Advanced evasion techniques
4. Lateral Movement: Network reconnaissance
5. Data Exfiltration: Command execution and file transfer

Malware Used:

- Cobalt Strike Beacon (Win32.Backdoor.Ratenjay)
- mrasp86.dll (filename)
- Advanced evasion techniques

Key Indicators:

- SHA-256: 3b5980c758bd61abaa4422692620104a81eefbf151361a1d8afe8e89bf38579d
- Imphash: a21e1c2781a36ff1ce3748551ba69d41
- SSDEEP: 12288:67E86soP/Bzbeb9JEIgukfyKpp8jB8wmXCZXnFXxR6boBxJwtpgpfHadJbpVBbpI:rXBfeMGgpn8ZmAhQ0vD/adJbpVBbpVi
- Signature: Cobalt Strike (signed)

Impact:

- Post-exploitation access
- Lateral movement capability
- Long-term persistence
- Advanced command execution

Campaign 5: Brazilian Military Zimbra Zero-Day Campaign (October 2025)

Campaign Name: Zimbra Zero-Day Military Espionage Operation

Status: Attribution Uncertain

Timeline: October 2025

Targets:

- Brazilian Army personnel
- Brazilian military organizations
- Defense-related communications infrastructure

Attack Chain:

1. Initial Access: Delivery of malicious .ICS calendar invitation files
2. Exploitation: Execution of a previously unknown Zimbra zero-day vulnerability
3. Code Execution: Remote execution on targeted Zimbra servers
4. Credential Access: Collection of authentication data and user information
5. Data Exfiltration: Transfer of collected data through Proton-based infrastructure

Malware / Tools Used:

- Malicious ICS (iCalendar) files
- Zimbra Collaboration Suite zero-day exploit
- Custom post-exploitation tooling
- Proton-based infrastructure for exfiltration

Key Indicators:

- Malicious .ICS calendar attachments
- Exploitation of Zimbra Collaboration Suite
- Proton infrastructure used for operational communications
- Targeting focused on military personnel and organizations
- Espionage-oriented collection activity

Impact:

- Unauthorized access to military communications
- Potential exposure of sensitive defense information
- Intelligence collection against military targets
- Demonstration of advanced zero-day exploitation capability
- Increased risk to government and defense-sector email infrastructure

Attribution Assessment:

- Attribution remains unresolved
- Possible state-sponsored espionage operation
- Some reporting suggested potential Belarusian-linked activity
- Alternative hypotheses include Russian intelligence-linked operators or joint operational activity
- Confidence Level: Low

Significance:

- First publicly reported use of the Zimbra zero-day against Brazilian military targets
- Demonstrates advanced exploitation capabilities against government infrastructure
- Highlights continuing uncertainty surrounding Belarusian and Russian cyber-espionage operations
- Relevant to broader assessments of military-focused cyber intelligence collection activity

DISINFORMATION & INFORMATION WARFARE OPERATIONS

Ghostwriter Disinformation Campaign

Campaign Name: Operation Ghostwriter (Information Warfare)

Timeline: July 2020 - Ongoing

Objectives:

- Discredit NATO and Western governments
- Disrupt elections and political processes
- Weaken Western support for Ukraine
- Psychological operations targeting military personnel
- Influence operations targeting civilian populations

Methods:

- Website compromise for disinformation dissemination
- Fake news article creation and distribution
- Social media account compromise
- Coordinated disinformation campaigns
- Impersonation of government officials
- False flag operations

Targets:

- NATO member states
- Eastern European governments
- Media organizations
- Civilian populations
- Military personnel

Key Campaigns:

1. Pre-Invasion Disinformation (2021-2022)

- Discrediting NATO expansion
- Psychological operations targeting military
- Preparation for Ukraine invasion

2. Invasion Support Disinformation (2022)

- Justification for military operations
- Discrediting Ukrainian government
- Psychological operations targeting Ukrainian military

3. Ongoing Disinformation (2023-2026)

- Continued discrediting of NATO
- Support for Russian/Belarusian interests
- Psychological operations targeting military personnel

Hybrid Warfare Integration

Unique Characteristic: Ghostwriter integrates cyber espionage with disinformation operations

Integration Methods:

1. Credential Harvesting for Impersonation

- Stolen credentials used to impersonate government officials
- Compromised email accounts for secondary phishing
- Impersonation for disinformation dissemination

2. Leaked Data for Disinformation

- Exfiltrated documents used in disinformation campaigns
- Selective disclosure for propaganda purposes
- Context manipulation for psychological impact

3. Coordinated Campaigns

- Cyber operations timed with disinformation campaigns
- Psychological operations targeting military personnel
- Influence operations targeting civilian populations

4. Maskirovka (Russian Military Deception)

- False flag operations
- Plausible deniability
- Coordinated deception campaigns

THREAT ASSESSMENT & RISK ANALYSIS

Risk Matrix

Likelihood	Impact	Risk Level	Scenarios
CRITICAL	CRITICAL	CRITICAL	Direct military confrontation; NATO expansion; Ukraine conflict escalation
HIGH	CRITICAL	CRITICAL	Sustained cyber espionage; supply chain compromise; destructive operations
MEDIUM	CRITICAL	HIGH	Disinformation campaigns; psychological operations; infrastructure disruption
HIGH	HIGH	HIGH	Credential harvesting; malware deployment; lateral movement
MEDIUM	HIGH	MEDIUM	Information gathering; reconnaissance; targeting development

Threat Scenarios

Scenario 1: NATO Expansion Trigger

- NATO expansion announcement triggers escalated cyber operations
- Intensive targeting of new NATO member states
- Destructive malware deployment
- Coordinated disinformation campaigns
- Likelihood: MEDIUM-HIGH | Impact: CRITICAL

Scenario 2: Ukraine Conflict Escalation

- Escalation of Ukraine conflict triggers increased cyber operations
- Destructive operations against Ukrainian infrastructure
- Targeting of NATO support infrastructure
- Coordination with Russian military operations
- Likelihood: MEDIUM-HIGH | Impact: CRITICAL

Scenario 3: Supply Chain Compromise

- Compromise of NATO defence contractors
- Access to NATO military capabilities
- Intelligence collection on NATO systems
- Potential for destructive operations
- Likelihood: HIGH | Impact: CRITICAL

Scenario 4: Hybrid Warfare Campaign

- Coordinated cyber, information, and kinetic operations
- Targeting of military personnel and civilian populations
- Psychological operations and disinformation
- Infrastructure disruption
- Likelihood: MEDIUM | Impact: CRITICAL

DEFENSIVE RECOMMENDATIONS

Strategic Level

1. National Cyber Defence Strategy

- Develop comprehensive strategy addressing state-sponsored threats
- Establish clear roles and responsibilities
- Allocate sufficient resources for cyber defence
- Establish coordination with NATO and allied nations

2. Defence Cyber Doctrine

- Develop doctrine addressing state-sponsored cyber threats
- Establish rules of engagement for cyber operations
- Define escalation procedures for cyber incidents
- Establish coordination with NATO

3. Intelligence Sharing

- Establish intelligence sharing with NATO and allied nations
- Share threat intelligence on Ghostwriter
- Coordinate threat intelligence collection
- Establish early warning systems

4. Sanctions & Diplomatic Response

- Support international sanctions against Belarus and Russia
- Coordinate diplomatic response with NATO
- Establish consequences for state-sponsored cyber operations
- Support international norms against cyber attacks

Operational Level

1. Threat Hunting

- Hunt for Ghostwriter infrastructure indicators
- Hunt for malware families and variants
- Hunt for phishing infrastructure
- Hunt for lateral movement and persistence indicators
- Hunt for data exfiltration patterns

2. Detection Engineering

- Implement advanced email filtering and threat detection
- Deploy endpoint detection and response (EDR)
- Implement network detection and response (NDR)
- Monitor for known IOCs and patterns
- Implement user awareness training

3. Identity Hardening

- Implement strong password policies
- Implement multi-factor authentication (MFA)
- Implement privileged access management (PAM)
- Implement credential monitoring and alerting
- Implement credential compartmentalization

4. Zero Trust Architecture

- Implement network segmentation
- Implement least privilege access
- Implement device security and compliance
- Implement access monitoring and alerting
- Implement incident response procedures

Tactical Level

1. SIEM Detections

- Alert on connections to Belarusian ISPs
- Alert on DNS queries to known C&C domains
- Alert on phishing infrastructure access
- Alert on malware persistence indicators
- Alert on credential harvesting indicators

2. IOC Monitoring

- Monitor for domain registration patterns
- Monitor for IP address reuse patterns
- Monitor for known malware file hashes
- Monitor for phishing lures and patterns
- Monitor for email authentication failures

3. ATT&CK-Based Detections

- Detect phishing and spearphishing (T1566)
- Detect credential access attempts (T1110, T1187, T1056)
- Detect persistence mechanisms (T1547)
- Detect lateral movement (T1550, T1078)
- Detect data exfiltration (T1020, T1048, T1041)

4. Threat Hunting Hypotheses

- Hypothesis 1: Ghostwriter infrastructure present in network traffic
- Hypothesis 2: Compromised credentials used for lateral movement
- Hypothesis 3: Malware persistence mechanisms present on endpoints
- Hypothesis 4: Data exfiltration to known C&C infrastructure
- Hypothesis 5: Phishing infrastructure accessed by military personnel

FUTURE OUTLOOK & ESCALATION RISKS

Likely Evolution

Technical Evolution:

1. Advanced malware with AI-enabled evasion
2. AI-driven phishing campaigns
3. Supply chain targeting expansion
4. Destructive malware development
5. Infrastructure adaptation and evolution

Operational Evolution:

1. Increased coordination with Russian threat actors
2. Hybrid warfare integration expansion
3. Psychological operations escalation
4. Targeting expansion to additional NATO states
5. Escalation during geopolitical tensions

Escalation Risks (12-24 Months)

High-Risk Scenarios:

1. **NATO Expansion** - Further NATO expansion could trigger escalated operations
2. **Ukraine Conflict Escalation** - Escalation of Ukraine conflict could trigger increased operations
3. **Military Confrontation** - Direct military confrontation could trigger destructive operations
4. **Sanctions Escalation** - Increased sanctions could trigger retaliatory operations
5. **Hybrid Warfare Campaign** - Coordinated hybrid warfare combining cyber, information, and kinetic operations

Likelihood Assessment:

- NATO Expansion: MEDIUM-HIGH
- Ukraine Escalation: MEDIUM-HIGH
- Military Confrontation: MEDIUM
- Sanctions Escalation: MEDIUM
- Hybrid Warfare: MEDIUM-HIGH

AI-Enabled Phishing Potential

Emerging Capabilities:

1. Personalized phishing emails generated by AI
2. Voice cloning for impersonation calls
3. Deepfakes for disinformation campaigns
4. Automated social engineering
5. Adaptive phishing based on user responses

Defensive Implications:

- Advanced email security required
- User awareness training on AI-enabled attacks
- Authentication mechanisms resistant to AI attacks
- Incident response procedures for AI-enabled attacks

INTELLIGENCE GAPS & LIMITATIONS

Known Limitations

1. Attribution Uncertainty - Specific operational units and individuals remain uncertain
2. Capability Assessment - Exact technical capabilities and resource allocation partially unknown
3. Infrastructure Visibility - Not all infrastructure may be visible; some C&C channels may remain undetected
4. Personnel Identification - Specific individuals involved in operations largely unknown
5. Coordination Mechanisms - Exact coordination with Russian threat actors partially understood

Collection Gaps

1. Internal Communications - Limited visibility into operational planning
2. Personnel Information - Limited information on specific individuals
3. Resource Allocation - Limited visibility into funding mechanisms
4. Decision-Making - Limited visibility into strategic planning
5. Russian Coordination - Limited visibility into coordination mechanisms

Recommended Monitoring

1. Infrastructure Evolution - Continued monitoring of infrastructure changes
2. Malware Development - Continued monitoring of new malware variants
3. Targeting Patterns - Continued monitoring of targeting expansion
4. Russian Coordination - Continued monitoring of coordination with Russian actors
5. Operational Tempo - Continued monitoring of escalation patterns

CONCLUSION

Ghostwriter/UNC1151 represents a **CRITICAL and persistent threat** to NATO-aligned defence institutions, military personnel, and critical infrastructure. The group's demonstrated capability, sustained operational tempo, and strategic alignment with Belarusian and Russian state interests indicate a long-term threat requiring comprehensive and coordinated defence response.

Key Takeaways:

1. Ghostwriter is state-sponsored with HIGH confidence attribution to Belarus
2. Advanced technical capabilities with sophisticated operational security
3. Strategic focus on NATO member states and NATO-aligned organizations
4. Hybrid warfare integration combining cyber espionage with disinformation
5. Potential for escalation during periods of geopolitical tension
6. Comprehensive defence response required at strategic, operational, and tactical levels

Recommended Actions:

1. Implement comprehensive cyber defence strategy
2. Establish coordination with NATO and allied nations
3. Deploy advanced threat detection and response capabilities
4. Conduct threat hunting for Ghostwriter indicators
5. Implement identity hardening and zero trust architecture
6. Establish incident response procedures
7. Conduct personnel awareness training
8. Establish supply chain security procedures

REFERENCES & SOURCES

- EuRepoC APT Profile: UNC1151
- Ghostwriter in the Shell: Belarus-Russia Nexus Analysis
- Ghostwriter: Hybrid Influence and Espionage Operations
- SentinelOne Labs: Ghostwriter 2025 Campaign Analysis
- Threat Group Cards: Operation Ghostwriter
- Google Cloud: UNC1151 Linked to Belarus Government
- HarfangLab: UAC-0057 Campaign Analysis
- BushidoToken: Ghostwriter APT Infrastructure Tracking
- Council on Foreign Relations: Cyber Operations in Russia-Ukraine War
- Malpedia: Ghostwriter Threat Actor Profile
- The Hacker News: Ghostwriter Prometheus Campaign 2026
- National Security Archive: Attribution and Timeline Analysis
- Rewterz Threat Alert: Ghostwriter Active IOCs
- MalwareBazaar: Trojan.Casdet Sample
- MalwareBazaar: Cobalt Strike Beacon Sample
- MalwareBazaar: CVE-2024-42009 Exploit Sample
- CAPE Sandbox: Cobalt Strike Analysis
- VMRay: Cobalt Strike Beacon Analysis
- Triage: CVE-2024-42009 Exploit Analysis