INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-14 18:51 UTC

FrostyNeighbor: Belarusian APT Conducts Pre-Screening Espionage Campaign Against Polish and Ukrainian Government Organizations

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0315
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Government organizations in Poland and Ukraine, specific systems not publicly detailed
Published	2026-05-14T12:59:25
Discovery Source	Rss

Executive Summary

A newly identified Belarusian nation-state group, FrostyNeighbor, is conducting targeted espionage operations against government organizations in Poland and Ukraine. The group pre-screens targets before delivering spear-phishing payloads, indicating a deliberate effort to evade detection and improve campaign success rates. Organizations supporting or adjacent to NATO and Eastern European government functions face elevated risk of credential theft, data exfiltration, and persistent access compromise.

Technical Analysis

FrostyNeighbor is a newly tracked Belarusian APT conducting espionage operations against Polish and Ukrainian government entities. The group employs victim fingerprinting prior to payload delivery, consistent with MITRE ATT&CK reconnaissance techniques T1593 (Search Open Websites/Domains), T1589 (Gather Victim Identity Information), T1591 (Gather Victim Org Information), and T1592 (Gather Victim Host Information). Initial access is assessed via spear-phishing (T1566.001) and phishing for information (T1598). Infrastructure acquisition techniques T1583 are used to support operations. Post-access activity likely involves keylogging or input capture (T1056) and command-and-control over application layer protocols (T1071). FrostyNeighbor is assessed as a distinct group separate from UNC1151/Ghostwriter, though behavioral overlap with other known regional actors cannot be excluded. No publicly disclosed malware families, specific IOCs, or attributed tooling have been associated with this campaign in available open-source reporting. Source quality score is 0.64 and public technical reporting is limited; assessment should be verified against primary intelligence feeds before high-confidence operational decisions.

Action Checklist

1. Step 1: Containment. Identify personnel with government, defense, or policy roles who receive external email and assess their exposure to unsolicited inbound contact from Eastern European or unknown senders; restrict or monitor inbound attachments originating from external (non-organization) domains at the mail gateway, prioritizing newly registered or low-reputation domains.
2. Step 2: Detection. Review email gateway and proxy logs for outbound HTTP/HTTPS requests triggered by document opens (tracking pixel or URL beacon behavior), indicating pre-screening lure delivery; look for requests to low-reputation or newly registered domains initiated from document viewers (Word, Acrobat) or browser processes shortly after mail receipt.
3. Step 3: Eradication. Enforce attachment sandboxing and URL detonation on all inbound email; disable automatic external content loading in Microsoft Office (disable 'Update automatic links at open' and block external resource fetching via Group Policy Object); review and harden macro and OLE settings per CIS Benchmark for Microsoft Office.
4. Step 4: Recovery. Validate that no unauthorized persistence mechanisms (scheduled tasks, registry run keys, new user accounts) exist on endpoints belonging to personnel who received suspect communications; confirm endpoint telemetry is feeding SIEM with sufficient fidelity to detect T1056 (keylogging) and T1071 (C2 beaconing) behaviors.
5. Step 5: Post-Incident. Review spear-phishing awareness training coverage for personnel in government-adjacent, policy, or international liaison roles; assess whether current detection rules cover pre-screening tradecraft (document-triggered outbound web requests) and add or tune rules if coverage gaps exist; map current controls against MITRE ATT&CK techniques T1566.001, T1598, T1593, and T1592 to identify gaps.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to national CERT (CERT Polska / UA-CERT as applicable) and senior leadership if any endpoint belonging to government-adjacent or NATO-liaison personnel shows confirmed beacon callback to a FrostyNeighbor-attributed domain, evidence of post-exploitation persistence (new scheduled tasks, run key modifications, unauthorized accounts), or if credential access indicators (T1056 keylogging artifacts, LSASS access events) are identified — these conditions indicate the campaign has progressed beyond pre-screening to active compromise of a high-value espionage target.
Recovery Notes	Before returning targeted endpoints to full operational status, confirm via KAPE or Velociraptor triage collection that no persistence mechanisms survive and that Shimcache/Amcache show no execution of unknown binaries during the pre-screening window. Maintain elevated monitoring for at least 30 days post-containment, specifically watching for low-and-slow C2 beaconing (T1071) and staged data collection (T1074) behaviors consistent with FrostyNeighbor transitioning from pre-screening to active espionage operations against validated targets. Brief affected personnel individually on the specific lure characteristics observed in this campaign — government policy documents or diplomatic correspondence themes — so they can recognize and report follow-on spear-phishing attempts that FrostyNeighbor may launch once pre-screening confirms target validity.

Forensic Artifacts	Web proxy logs (Squid access.log, Zscaler, or Bluecoat) filtered for outbound GET requests from document viewer processes (winword.exe, acrord32.exe) with request timing within 60 seconds of email delivery — the forensic signature of FrostyNeighbor tracking pixel or remote template beacon callbacks used to validate targets before spear-phishing escalation. | Sysmon Event ID 3 (Network Connection) records on targeted endpoints showing winword.exe or acrord32.exe initiating outbound TCP/80 or TCP/443 connections to low-reputation or newly registered domains — the process-to-network correlation that distinguishes document-triggered pre-screening beacons from legitimate Office telemetry. | Full SMTP header dumps for all inbound messages to high-value personnel over 30–60 days prior to detection, preserving the X-Originating-IP, Reply-To, and X-Mailer fields that characterize FrostyNeighbor sender infrastructure and establish the reconnaissance timeline preceding payload delivery. | Windows Prefetch files (C:\Windows\Prefetch\), Shimcache, and Amcache hive exports from targeted endpoints — these execution artifacts reveal whether any binaries were executed during or after document opens in the pre-screening window, indicating whether FrostyNeighbor progressed beyond reconnaissance to initial payload execution on any validated targets. | DNS debug logs or Zeek dns.log entries for all domains queried by targeted personnel endpoints, specifically looking for single-query, no-repeat domains with no prior DNS history — consistent with one-time beacon domains used by FrostyNeighbor to confirm target reachability and avoid reuse that would aid attribution and blocklisting.

Per-Action IR Details

Step 1: Containment — Identify personnel with government, defense, or policy roles who receive external email and assess their exposure to unsolicited inbound contact from Eastern European or unknown senders; restrict or monitor inbound attachments from untrusted external domains at the mail gateway.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected communication channels and reduce attacker pre-screening surface before spear-phishing payloads are delivered to validated targets.

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST AC-2 (Account Management) — scoping privileged/high-value personnel exposure, CIS 9.2 (Use DNS Filtering Services) — block outbound DNS resolution for known pre-screening beacon domains at the gateway level, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — assess personnel attack surface as a risk exposure input

Compensating: Export mail gateway recipient logs and cross-reference against an HR-sourced list of government liaison, policy, and defense-adjacent staff roles. Use PowerShell against Exchange Online or on-prem Exchange: `Get-MessageTrace -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) | Where-Object {$_.FromIP -match '' -or $_.Status -eq 'Delivered'} | Export-Csv mailTrace.csv`. For MTA-level blocking without a commercial gateway, configure Postfix or Sendmail header_checks rules to quarantine `.docx`, `.pdf`, and `.lnk` attachments from domains registered within the last 90 days (use whois batch lookups via a cron-driven shell script against a domain age API such as WhoisXML free tier).

Evidence: Before restricting mail flow, preserve full SMTP header dumps (including `Received:` chain, `X-Originating-IP`, `X-Mailer`, and `Reply-To` anomalies) for all inbound messages to high-value personnel over the prior 30–60 days — FrostyNeighbor pre-screening relies on initial contact emails that precede payload delivery, and these headers establish the reconnaissance timeline. Capture mail gateway quarantine logs and any SPF/DKIM/DMARC failure records that may indicate spoofed sender domains used in the pre-screening phase.

Step 2: Detection — Review email gateway and proxy logs for outbound HTTP/HTTPS requests triggered by document opens (tracking pixel or URL beacon behavior), indicating pre-screening lure delivery; look for requests to low-reputation or newly registered domains initiated from document viewers (Word, Acrobat) or browser processes shortly after mail receipt.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate email delivery timestamps against outbound web proxy telemetry to identify FrostyNeighbor pre-screening beacon callbacks, which serve as the adversary's target validation signal before spear-phishing payload delivery.

Controls: NIST SI-4 (System Monitoring) — monitor for process-initiated outbound web requests from document viewer processes, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — structured review of proxy and mail gateway logs for beacon patterns, NIST AU-3 (Content of Audit Records) — ensure proxy logs capture parent process name alongside outbound URL, CIS 8.2 (Collect Audit Logs) — confirm email gateway and web proxy logging is enabled and retained with sufficient fidelity, MITRE ATT&CK T1598 (Phishing for Information) — pre-screening lure delivery via tracking beacon, MITRE ATT&CK T1592 (Gather Victim Host Information) — beacon response provides host/user validation to FrostyNeighbor

Compensating: Deploy Sysmon with SwiftOnSecurity config (minimum: Event ID 3 — Network Connection, Event ID 1 — Process Creation) and filter for `winword.exe`, `acrord32.exe`, or `msedge.exe` (Office WebView2) initiating outbound TCP/443 or TCP/80 connections to domains not in an allowlist. Query with: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 3 -and $_.Message -match 'winword|acrord32'} | Select-Object TimeCreated, Message | Export-Csv sysmon_net.csv`. Cross-reference destination domains against VirusTotal and URLScan.io free APIs for domain age and reputation. Use Zeek (formerly Bro) on a network tap or span port to extract HTTP host headers and User-Agent strings — FrostyNeighbor beacons from Office processes will show anomalous UA strings (e.g., `Microsoft Office` UA calling non-Microsoft CDN domains).

Evidence: Capture web proxy logs (Squid access.log or equivalent) filtered for outbound GET requests where the referrer or initiating process is a document viewer, with particular attention to requests occurring within 60 seconds of email delivery timestamps — this timing correlation is the forensic signature of a tracking pixel or remote template injection beacon. Preserve DNS query logs (Windows DNS debug log or Zeek dns.log) for all low-entropy or algorithmically generated domain names queried by endpoints of targeted personnel, as FrostyNeighbor pre-screening infrastructure frequently uses newly registered domains with no prior DNS history.

Step 3: Eradication — Enforce attachment sandboxing and URL detonation on all inbound email; disable automatic external content loading in Microsoft Office (disable 'Update automatic links at open' and block external resource fetching via Group Policy Object); review and harden macro and OLE settings per CIS Benchmark for Microsoft Office.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: eliminate the technical mechanism FrostyNeighbor exploits for pre-screening (automatic external content loading in Office documents) and remove the adversary's ability to validate targets before escalating to spear-phishing payload delivery.

Controls: NIST SI-2 (Flaw Remediation) — address the configuration weakness enabling automatic external content fetch in Office, NIST SI-3 (Malicious Code Protection) — enforce sandbox detonation of inbound attachments before delivery, NIST CM-6 (Configuration Settings) — apply and enforce GPO-based Office hardening, NIST CM-7 (Least Functionality) — disable OLE and macro features not required for business function, CIS 4.6 (Securely Manage Enterprise Assets and Software) — enforce hardened Office config via GPO or Intune, CIS 7.4 (Perform Automated Application Patch Management) — ensure Office is patched to versions supporting Protected View enforcement

Compensating: Apply the following GPO registry keys to all endpoints (deployable via `reg add` in a startup script if GPO infrastructure is unavailable): Set `HKCU\Software\Microsoft\Office\\Word\Options\DontUpdateLinks` = `1` (DWORD) to disable automatic link updates; set `HKCU\Software\Microsoft\Office\\Common\Internet\UseOnlineContent` = `0` to block external content fetching. Enforce macro blocking for non-trusted-signed macros via `HKCU\Software\Microsoft\Office\\Word\Security\VBAWarnings` = `4`. For attachment sandboxing without a commercial product, route inbound mail through a free ClamAV instance with the Sanesecurity third-party signature set enabled, or submit attachments automatically to any.run free tier via their API before release to end-user mailboxes. Validate GPO application with `gpresult /h gpo_report.html` on a sample endpoint.

Evidence: Before applying GPO changes, document the pre-remediation Office registry state on affected endpoints using: `reg export HKCU\Software\Microsoft\Office officeConfig_before.reg` — this establishes the configuration baseline that permitted FrostyNeighbor beaconing and may be required for any regulatory reporting. Also capture any Office Trust Center logs (`%APPDATA%\Microsoft\Office\Recent\` and Protected View event logs under `Applications

and Services Logs\Microsoft\Office Alerts`) that may record prior external content load attempts or macro execution events on targeted endpoints.

Step 4: Recovery — Validate that no unauthorized persistence mechanisms (scheduled tasks, registry run keys, new user accounts) exist on endpoints belonging to personnel who received suspect communications; confirm endpoint telemetry is feeding SIEM with sufficient fidelity to detect T1056 (keylogging) and T1071 (C2 beaconing) behaviors.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verify that targeted endpoints used by government-adjacent personnel have not been compromised beyond the pre-screening phase before restoring normal operational posture, and confirm detection coverage for FrostyNeighbor post-exploitation TTPs.

Controls: NIST IR-4 (Incident Handling) — execute recovery phase validation as part of the incident handling lifecycle, NIST SI-7 (Software, Firmware, and Information Integrity) — verify endpoint integrity against known-good baseline before return to operation, NIST AU-12 (Audit Record Generation) — confirm logging fidelity sufficient to detect T1056 and T1071 post-compromise behaviors, NIST SI-4 (System Monitoring) — validate SIEM ingestion pipeline for endpoint telemetry continuity, CIS 8.2 (Collect Audit Logs) — ensure endpoint audit logging is active and forwarding for all targeted personnel systems, MITRE ATT&CK T1053.005 (Scheduled Task/Job: Scheduled Task) — check for unauthorized scheduled tasks as FrostyNeighbor persistence mechanism, MITRE ATT&CK T1547.001 (Boot or Logon Autostart Execution: Registry Run Keys) — enumerate run key modifications, MITRE ATT&CK T1056 (Input Capture) — validate detection coverage for keylogging, MITRE ATT&CK T1071 (Application Layer Protocol) — validate C2 beaconing detection coverage

Compensating: Run the following on each targeted endpoint to enumerate persistence: `schtasks /query /fo CSV /v > scheduled_tasks.csv` and `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run` — diff output against a known-good baseline from a non-targeted peer system. For new account enumeration: `net user > local_accounts.txt` and `Get-LocalUser | Where-Object {$_.Enabled -eq $true} | Select Name, LastLogon`. To validate T1056 detection without EDR, deploy Sysmon Event ID 10 (ProcessAccess) filtering for access to `lsass.exe` and monitor for unsigned DLLs loaded into `winlogon.exe` or `csrss.exe` using Sysmon Event ID 7 (ImageLoad). For C2 beaconing detection, use netstat scheduled via Task Scheduler every 5 minutes (`netstat -anob >> c:\ir\netstat_log.txt`) and review for persistent outbound connections on non-standard ports or beaconing intervals.

Evidence: Before clearing endpoints for return to operation, acquire a full artifact triage package using Velociraptor free tier or KAPE (Kroll Artifact Parser and Extractor): collect `$MFT`, Windows Prefetch files (`C:\Windows\Prefetch\`), Shimcache (`HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache`), Amcache (`C:\Windows\AppCompat\Programs\Amcache.hve`), and all scheduled task XML files from `C:\Windows\System32\Tasks\` — these sources will reveal any execution that occurred during the pre-screening window on targeted endpoints even if logs have been partially cleared by the adversary.

Step 5: Post-Incident — Review spear-phishing awareness training coverage for personnel in government-adjacent, policy, or international liaison roles; assess whether current detection rules cover pre-screening tradecraft (document-triggered outbound web requests) and add or tune rules if coverage gaps exist; map current controls against MITRE ATT&CK techniques T1566.001, T1598, T1593, and T1592 to identify gaps.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review focused on FrostyNeighbor's pre-screening reconnaissance tradecraft, update detection engineering to cover document-triggered beacon behavior, and brief high-risk personnel on spear-phishing indicators specific to this campaign's targeting pattern.

Controls: NIST IR-4 (Incident Handling) — post-incident review and playbook update, NIST IR-2 (Incident Response Training) — targeted awareness training update for government-adjacent personnel roles, NIST IR-8 (Incident Response Plan) — update IR plan to incorporate FrostyNeighbor pre-screening phase as a distinct detection scenario, NIST SI-5 (Security Alerts, Advisories, and Directives) — consume and disseminate threat intelligence on FrostyNeighbor TTPs to relevant stakeholders, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — tune

detection rules based on post-incident log review findings, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate pre-screening tradecraft gap findings into the vulnerability management risk register, CIS 17.3 (Train Workforce on Security Awareness) — update phishing simulation content to reflect FrostyNeighbor pre-screening lure characteristics, MITRE ATT&CK T1566.001 (Phishing: Spearphishing Attachment) — validate Sigma/YARA detection rule coverage, MITRE ATT&CK T1598 (Phishing for Information) — confirm detection for pre-screening lure phase, MITRE ATT&CK T1593 (Search Open Websites/Domains) — assess exposure of targeted personnel's public profiles (LinkedIn, government directories) used for target selection, MITRE ATT&CK T1592 (Gather Victim Host Information) — confirm beacon response data that may have been exfiltrated during pre-screening

Compensating: For detection rule development without a commercial SIEM, publish Sigma rules (free, open format) targeting: process-initiated outbound network connections from `winword.exe` or `acrord32.exe` to domains with registration age under 90 days. Convert Sigma rules to Splunk SPL, Elastic EQL, or Graylog using the free sigmac converter. For ATT&CK gap mapping, use the free MITRE ATT&CK Navigator to load T1566.001, T1598, T1593, and T1592 and score current detection coverage — export the layer as a gap report for leadership. Conduct a targeted 30-minute tabletop exercise with government-liaison personnel using a FrostyNeighbor-specific scenario: an unsolicited email with a policy document attachment arriving from a plausible Eastern European government address, to test recognition and reporting behavior.

Evidence: Compile a post-incident evidence package including: all SMTP header records from the pre-screening contact phase, proxy logs showing beacon callback timing and destination domains, the pre- and post-remediation Office registry export diffs, and any Sysmon Network Connection events correlated to document open timestamps — this package supports both the lessons-learned review and any mandatory reporting to national CERT or government cybersecurity authority (e.g., CERT Polska or UA-CERT) given the targeting of Polish and Ukrainian government organizations.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) are publicly available for FrostyNeighbor at this time. Detection should focus on behavioral indicators consistent with the identified MITRE techniques. Monitor for: (1) outbound HTTP/HTTPS GET requests initiated by Office processes (WINWORD.EXE, EXCEL.EXE) or PDF readers to external domains, a fingerprinting indicator consistent with tracking-pixel lures; (2) spear-phishing emails targeting personnel in government, policy, or intergovernmental roles, particularly those with Polish or Ukrainian government contact; (3) process creation events showing document viewers spawning child processes (cmd.exe, PowerShell, wscript.exe); (4) DNS queries to newly registered or low-reputation domains from workstations shortly after email receipt. Relevant log sources: email gateway logs, proxy/web filter logs (filter on Office process user-agent strings), EDR telemetry (process lineage, network connections from Office processes), DNS query logs. Hunting hypothesis: Identify all outbound web requests where the initiating process is a document viewer and the destination domain was registered within the past 90 days. Note: Detection must account for corporate proxy configurations; outbound requests may be logged at the proxy rather than the endpoint. Cross-reference EDR process lineage with proxy/web filter logs to confirm the initiating Office process.

Framework Mappings

MITRE-ATTACK

- **T1593** — Search Open Websites/Domains
- **T1566.001** — Spearphishing Attachment
- **T1598** — Phishing for Information
- **T1583** — Acquire Infrastructure

- **T1589** — Gather Victim Identity Information
- **T1071** — Application Layer Protocol
- **T1591** — Gather Victim Org Information
- **T1592** — Gather Victim Host Information
- **T1056** — Input Capture

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CA-7** — Continuous Monitoring

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1593	Search Open Websites/Domains	Reconnaissance
T1566.001	Spearphishing Attachment	Initial-Access
T1598	Phishing for Information	Reconnaissance
T1583	Acquire Infrastructure	Resource-Development
T1589	Gather Victim Identity Information	Reconnaissance
T1071	Application Layer Protocol	Command-And-Control
T1591	Gather Victim Org Information	Reconnaissance
T1592	Gather Victim Host Information	Reconnaissance

Technique ID	Technique Name	Tactic
T1056	Input Capture	Collection

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/frostyneighb...	T3
Polish ABW warns cyberattacks shifting from espionage and data ...	https://industrialcyber.co/reports/polish-abw-warns-cyberattacks-sh...	T3
Targeting of Polish government organizations with Follina vulnerability	https://www.cfr.org/cyber-operations/targeting-of-polish-government...	T3
ANALYSIS OF THE CYBERATTACK ON UKRAINIAN ... - csirt mon	https://csirt-mon.wp.mil.pl/aktualnosci/analysis-of-the-cyberattack...	T3
Poland's Critical Infrastructure Under Threat: Lessons Learned	https://www.anomali.com/blog/polands-critical-infrastructure-under-...	T3

Generated 2026-05-14 18:51 UTC by TJS Security Command Center