INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-23 19:01 UTC

Russia Deploys AI-Augmented Malware in Cyberwarfare Operations Against Ukraine

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0357
Type	Threat Campaign
Severity	HIGH
Affected Products	Ukrainian government, energy, and military networks; unspecified endpoints targeted by Russian state-sponsored threat actors
Published	2026-05-21
Discovery Source	Gemini

Executive Summary

Russian state-sponsored threat actors are reportedly embedding AI capabilities directly into malware tooling used against Ukrainian government, energy, and military networks, enabling dynamic payload adaptation rather than static attack scripts. If confirmed at scale, this capability could reduce the effectiveness of signature-based defenses across sectors beyond Ukraine, including critical infrastructure operators and defense-adjacent organizations in NATO-aligned nations. Attribution to Russian state actors is high confidence; the specific technical claim of AI-embedded malware remains low-to-medium confidence pending corroborating analysis or sample disclosure.

Technical Analysis

Ukrainian officials report that Russian threat actors have integrated generative AI or large language model components into malware execution chains, enabling on-the-fly command generation and behavioral adaptation. This aligns with MITRE ATT&CK techniques T1587.001 (Develop Capabilities: Malware), T1059 (Command and Scripting Interpreter), T1027 (Obfuscated Files or Information), T1071 (Application Layer Protocol), and T1566 (Phishing) as probable delivery and execution vectors. No specific malware family, CVE, CWE, or technical indicators of compromise have been publicly disclosed. No CISA KEV entry exists for this campaign. All five cited sources are Tier 3 (vendor threat blogs, news outlets, and government advisories); primary-tier corroboration from CISA, MITRE ATT&CK, or NVD was not located at time of analysis. The claimed capability - AI generating malicious commands dynamically within a running execution chain - would represent a meaningful detection evasion evolution against signature-based and static-analysis defenses, but this remains unverified by technical sample analysis. Confidence in broad Russia attribution: HIGH. Confidence in AI-embedding technical specifics: LOW-TO-MEDIUM.

Action Checklist

1. Step 1: Containment. Review and tighten egress filtering on Ukrainian-nexus or Eastern European IP ranges for government, energy, and defense-sector organizations. Enforce application-layer protocol controls per NIST AC-4 (Information Flow Enforcement) to limit unauthorized data flows from affected network segments. This is a precautionary measure given no confirmed IOCs are available.
2. Step 2: Detection. Shift detection posture toward behavioral and heuristic analysis. Because no signatures or IOCs are publicly available for this campaign, prioritize anomaly-based detections: hunt for unusual scripting interpreter invocations (T1059), abnormal outbound protocol usage (T1071), and obfuscated payload execution (T1027) in endpoint and network telemetry per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). Enable and review system file analysis capabilities for modification of system executables and configuration files on endpoints in scope.
3. Step 3: Eradication. No specific patch, malware family, or remediation path is available for this campaign. Apply credential hardening and credential rotation for privileged accounts on systems in targeted sectors. Audit scripting interpreter access per NIST AC-6 (Least Privilege) and restrict execution of unsigned or unapproved scripts. Remove or disable unnecessary scripting engines on endpoints not requiring them.
4. Step 4: Recovery. Validate endpoint integrity using system file analysis and system initialization configuration analysis to confirm no unauthorized startup configuration changes. Confirm audit logging is intact per NIST AU-9 (Protection of Audit Information) - adaptive malware may attempt to suppress or modify logs to evade retrospective analysis. Verify MFA enforcement on all remote access and administrative interfaces per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access).
5. Step 5: Post-Incident. This campaign exposes reliance on signature-based detection as a primary control. Conduct a control gap review against NIST SI-4 (System Monitoring) to assess coverage of behavioral detection capabilities. Evaluate whether existing SIEM rules and EDR policies would surface dynamically generated commands that have no known signature. Document findings and update detection engineering backlog. Monitor CISA, MITRE ATT&CK, and CERT-UA for technical indicators as this campaign develops.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and notify CISA (for US-based critical infrastructure operators) or national CERT if behavioral detections fire on endpoints in government, energy, or defense-adjacent networks, if log gaps or tampering artifacts are discovered indicating active compromise, or if any lateral movement indicators (Event ID 4648 — Logon with Explicit Credentials, Event ID 4769 — Kerberos Service Ticket Requested for sensitive targets) are observed on systems processing operational technology (OT) or classified data.

Recovery Notes	Given that AI-adapted malware in this campaign is designed to generate dynamic, non-repeating payloads (T1027), recovery validation must extend beyond static file integrity checks to include continuous behavioral monitoring of restored endpoints for a minimum of 30 days post-recovery using Sysmon and osquery process telemetry. Verify that no scheduled tasks, WMI subscriptions (`Get-WMIObject -Namespace root\subscription -Class __EventFilter`), or service entries were seeded by the malware prior to detection, as Russian APT campaigns against Ukrainian targets have demonstrated long-dwell persistence mechanisms designed to survive credential rotation and reimaging. Maintain heightened egress monitoring and behavioral detection rules established during Steps 1–2 as permanent controls rather than temporary measures, given the ongoing and evolving nature of this state-sponsored campaign.
Forensic Artifacts	Windows PowerShell Script Block Logs (Microsoft-Windows-PowerShell/Operational, Event ID 4104) — AI-generated dynamic payloads will produce unique, non-repeating script block content on each execution, making these logs the highest-fidelity artifact for this campaign's T1059.001 technique usage; collect from all in-scope Windows endpoints before any remediation. | Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connect) logs — capture parent-child process chains showing scripting interpreters (powershell.exe, wscript.exe, mshta.exe) spawned by unexpected parents (svchost, lsass, IIS worker processes) and their subsequent outbound connections, which represent the execution and C2 phases of AI-adapted payload delivery (T1059, T1071). | Windows Security Event Log Event ID 4688 (Process Creation with full command-line auditing enabled) and Event ID 1102 (Audit Log Cleared) — the former captures dynamic payload invocations that bypass signature detection; the latter confirms if the malware's AI-driven evasion component attempted retrospective log suppression (T1070.001), a behavior documented in Russian Sandworm campaigns against Ukrainian infrastructure. | Memory forensic images (acquired via WinPmem or LiME) analyzed with Volatility3 malfind and cmdline plugins — AI-adapted malware in this campaign is expected to operate with minimal or no on-disk footprint using process injection (T1055) or reflective loading, making memory the primary artifact source for payload reconstruction and IOC extraction. | Network packet captures (pcap) at egress choke points filtered for DNS query anomalies (high-frequency queries, long subdomain strings indicating DNS tunneling per T1071.004), HTTP/S traffic with non-standard User-Agent strings or beaconing intervals (jitter patterns), and any non-standard port outbound sessions from endpoints in the government, energy, or defense network segments targeted by this Russian state-sponsored campaign.

Per-Action IR Details

Step 1: Containment — Review and tighten egress filtering on Ukrainian-nexus or Eastern European IP ranges for government, energy, and defense-sector organizations. Enforce application-layer protocol controls per NIST AC-4 (Information Flow Enforcement) to limit unauthorized data flows from affected network segments. This is a precautionary measure given no confirmed IOCs are available.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Windows endpoints, use Windows Firewall with Advanced Security (wf.msc) to create outbound block rules targeting ASN ranges associated with Russian-operated infrastructure (e.g., AS8342 Rostelecom, AS12389 Rostelecom backbone). Run: `netsh advfirewall firewall add rule name='Block RU-Nexus Egress' dir=out action=block remoteip=`. On Linux, apply iptables rules: `iptables -A OUTPUT -d -j DROP`. Use Wireshark or tcpdump on network choke points to capture and review unexpected outbound DNS, HTTP/S, and non-standard port traffic:

`tcpdump -i eth0 -w /tmp/egress_capture.pcap 'not src net 10.0.0.0/8'`. Block or alert on non-standard outbound ports (e.g., 4444, 8080, 1080) using pfSense or iptables if no enterprise firewall is available.

Evidence: Before tightening egress rules, capture current baseline outbound traffic using tcpdump or Wireshark for minimum 24 hours to establish normal egress patterns. Collect NetFlow or firewall connection logs (Windows Firewall logs at `%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log`; Linux iptables logs via `/var/log/syslog` or `/var/log/kern.log`) to identify any pre-existing unauthorized outbound sessions. Document all currently established TCP sessions to Eastern European IP space using `netstat -anob` (Windows) or `ss -tnp` (Linux) prior to rule changes. AI-adapted malware in this campaign may use protocol mimicry over HTTP/S (T1071.001) or DNS tunneling (T1071.004) — flag any endpoints initiating unusually high DNS query volumes or large DNS response payloads before egress rules suppress the traffic.

Step 2: Detection — Shift detection posture toward behavioral and heuristic analysis. Because no signatures or IOCs are publicly available for this campaign, prioritize anomaly-based detections: hunt for unusual scripting interpreter invocations (T1059), abnormal outbound protocol usage (T1071), and obfuscated payload execution (T1027) in endpoint and network telemetry per NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs). Enable and review D3-SFA (System File Analysis) for modification of system executables and configuration files on endpoints in scope.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a hardened configuration (SwiftOnSecurity or Olaf Hartong's modular config) to capture Event ID 1 (Process Create), Event ID 3 (Network Connect), Event ID 7 (Image Load), and Event ID 10 (Process Access). Write Sigma rules targeting: (1) PowerShell or cmd.exe spawned by non-interactive parent processes (e.g., svchost, lsass, services.exe) — indicative of T1059 execution by AI-adapted payload; (2) encoded command-line arguments (`-EncodedCommand`, `FromBase64String`, `[char]`) for T1027; (3) outbound connections on uncommon ports from scripting engines. Use osquery with the `process_open_sockets` and `processes` tables to query live endpoints: `SELECT p.name, p.pid, s.remote_address, s.remote_port FROM process_open_sockets s JOIN processes p ON s.pid = p.pid WHERE s.remote_port NOT IN (80,443,53);`. Write YARA rules targeting in-memory obfuscation patterns (base64-encoded shellcode stubs, XOR loops) and scan running processes with YARA via `yara -p 8 rule.yar /proc/*/mem` (Linux) or via YARA's Windows process scanning mode.

Evidence: Collect Windows Security Event Log Event ID 4688 (Process Creation with command-line logging enabled via GPO) filtered on scripting interpreters (powershell.exe, wscript.exe, cscript.exe, mshta.exe, regsvr32.exe) spawned with obfuscated arguments. Collect Sysmon Event ID 1 logs with full command-line arguments from all in-scope endpoints before and after the campaign disclosure date (2026-03-04 baseline). Capture Windows Event ID 4103/4104 (PowerShell Script Block Logging) from `Microsoft-Windows-PowerShell/Operational` log — AI-driven dynamic payload generation would manifest here as novel, non-repeating script block content that defeats signature matching. Review process memory dumps from any flagged endpoints for packed or encrypted payload regions using Volatility3 (`vol.py -f memory.raw windows.malfind`). On Linux targets, collect `/proc//cmdline`, `/proc//maps`, and `/proc//exe` for any interpreter processes with anomalous parent-child relationships.

Step 3: Eradication — No specific patch, malware family, or remediation path is available for this campaign. Apply D3-CH (Credential Hardening) and D3-CRO (Credential Rotation) for privileged accounts on systems in targeted sectors. Audit scripting interpreter access per NIST AC-6 (Least Privilege) and restrict execution of unsigned or unapproved scripts. Remove or disable unnecessary scripting engines on endpoints not requiring them.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Disable unnecessary scripting engines via GPO or registry: set `HKLM\SOFTWARE\Policies\Microsoft\Windows\PowerShell\EnableScripts = 0` on servers with no legitimate PS automation need; remove or rename wscript.exe and cscript.exe on endpoints not requiring them (`takeown /f C:\Windows\System32\wscript.exe && icacls C:\Windows\System32\wscript.exe /deny Everyone:X`). Enable PowerShell Constrained Language Mode via GPO (`__PSLockdownPolicy = 4` in environment variable) to neuter advanced scripting even if an interpreter is present. Rotate all privileged account passwords using a minimum 20-character random passphrase; for service accounts, use Group Managed Service Accounts (gMSA) if on Windows Server 2012+. Audit local administrator accounts on all in-scope endpoints: `Get-LocalGroupMember -Group 'Administrators' | Export-Csv admins.csv` and cross-reference against authorized list. On Linux, audit sudoers: `cat /etc/sudoers && getent group sudo` and remove unauthorized entries.

Evidence: Before credential rotation, capture a full export of current privileged account membership from Active Directory (`Get-ADGroupMember -Identity 'Domain Admins' -Recursive`) and local admin groups on all in-scope endpoints to establish pre-rotation baseline. Collect Windows Security Event ID 4720 (Account Created), 4722 (Account Enabled), 4728 (Member Added to Global Group), and 4732 (Member Added to Local Group) from Domain Controllers for the 30 days prior to this advisory — AI-augmented intrusions in Russian APT campaigns (consistent with Sandworm/APT44 and UAC-0082 TTPs against Ukrainian targets) frequently pre-stage privileged accounts weeks before operational use. Review scheduled tasks (`schtasks /query /fo LIST /v > scheduled_tasks.txt`) and Windows service registry keys (`HKLM\SYSTEM\CurrentControlSet\Services`) for entries created or modified by non-administrative accounts, which would indicate persistence established by a dynamic payload.

Step 4: Recovery — Validate endpoint integrity using D3-SFA (System File Analysis) and D3-SICA (System Init Config Analysis) to confirm no unauthorized startup configuration changes. Confirm audit logging is intact per NIST AU-9 (Protection of Audit Information) — AI-adapted malware may attempt to suppress or modify logs to evade retrospective analysis. Verify MFA enforcement on all remote access and administrative interfaces per CIS 6.4 (Require MFA for Remote Network Access) and CIS 6.5 (Require MFA for Administrative Access).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), NIST CP-10 (System Recovery and Reconstitution), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Verify Windows Security Event Log and Sysmon log integrity by checking for gaps in event timestamps using: `Get-WinEvent -LogName Security | Select-Object TimeCreated | Sort-Object TimeCreated | Export-Csv log_timeline.csv` — unexplained gaps in a previously active log indicate AI-assisted log suppression or tampering (consistent with T1070.001 — Indicator Removal: Clear Windows Event Logs). Use `sigcheck.exe -e -u -vt C:\Windows\System32\` (Sysinternals) to verify system binary integrity against VirusTotal and known-good hashes without requiring an enterprise FIM solution. Validate startup configuration using `reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run startup_run.reg` and `reg export HKLM\SYSTEM\CurrentControlSet\Services startup_services.reg`, then diff against a known-good baseline. For MFA enforcement without enterprise tooling, enable Windows Hello for Business or deploy Duo Security's free tier for remote access authentication on VPN and RDP gateways.

Evidence: Before clearing or rebuilding any system, acquire forensic memory images using WinPmem (Windows) or LiME kernel module (Linux) and disk images using FTK Imager or `dd` — AI-adapted payloads in this campaign may reside partially in memory with no on-disk footprint (T1055 — Process Injection), meaning disk-only analysis will miss the implant. Collect Windows Event ID 1102 (Audit Log Cleared) and Event ID 104 (System Log Cleared) from Security and System logs, which would confirm deliberate log tampering by the malware's AI-driven evasion component. Capture the Master Boot Record and Volume Boot Record (`dd if=/dev/sda bs=512 count=1 of=mbr.bin`) on Linux energy sector endpoints — Russian Sandworm-linked campaigns against Ukrainian energy infrastructure have historically deployed wiper components (e.g., CaddyWiper, INDUSTROYER2) that modify boot sectors, and recovery must confirm these are intact.

Step 5: Post-Incident — This campaign exposes reliance on signature-based detection as a primary control. Conduct a control gap review against NIST SI-4 (System Monitoring) to assess coverage of behavioral detection capabilities. Evaluate whether existing SIEM rules and EDR policies would surface dynamically generated commands that have no known signature. Document findings and update detection engineering backlog. Monitor CISA, MITRE ATT&CK, and CERT-UA for technical indicators as this campaign develops.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a Sigma rule coverage assessment using the Sigma rule repository and sigma-cli to test existing rules against a behavioral hypothesis set derived from ATT&CK techniques T1059 (Command and Scripting Interpreter), T1027 (Obfuscated Files or Information), T1071 (Application Layer Protocol), and T1055 (Process Injection) — the core technique cluster for AI-adapted dynamic malware. Map detection gaps using the ATT&CK Navigator (free, browser-based) to visualize which techniques in the Russian state-sponsored playbook (consistent with Sandworm/APT44, FANCY BEAR/APT28 campaigns documented in CERT-UA advisories) have no behavioral detection coverage. Establish a recurring 48-hour monitoring cadence on CERT-UA (https://cert.ua/en/) and CISA Known Exploited Vulnerabilities catalog for new IOCs as this campaign develops. Document all gap findings in a structured remediation backlog using a simple risk-scored spreadsheet (likelihood × impact) if no GRC platform is available.

Evidence: Collect and preserve all detection rule logs, SIEM query histories, and EDR alert configurations as-of the campaign disclosure date (2026-03-04) to establish the pre-gap-review baseline for the lessons-learned record. Export ATT&CK Navigator layer files showing current detection coverage before the gap review so improvement can be quantitatively measured post-remediation. Retain all network capture files, memory images, and log exports gathered during Steps 1–4 per NIST AU-11 (Audit Record Retention) for a minimum of 12 months — AI-augmented malware campaigns of this scale (Russian state-sponsored, targeting critical infrastructure) are likely to spawn follow-on investigations, regulatory inquiries, or intelligence-sharing obligations under CISA reporting frameworks.

Detection Guidance

No confirmed IOCs, hashes, domains, or IP indicators are publicly available for this campaign at time of analysis. Detection must rely on behavioral and heuristic approaches. Recommended focus areas: (1) Scripting interpreter anomalies - flag unusual parent-child process relationships involving cmd.exe, powershell.exe, wscript.exe, or cscript.exe (T1059); (2) Obfuscation indicators - detect high-entropy strings in command-line arguments, base64-encoded execution, or unusual character substitution patterns in process telemetry (T1027); (3) Abnormal application-layer protocol use - monitor for DNS, HTTP, or HTTPS beaconing from endpoints with irregular timing or payload sizes inconsistent with known application baselines (T1071); (4) Phishing delivery - review email gateway logs for suspicious attachment types and macro-enabled documents targeting Ukrainian-sector personnel (T1566); (5) Capability development signals - monitor external threat intelligence feeds for newly published indicators tied to Russian APT malware development activity (T1587.001). Apply local account monitoring on high-value endpoints. Ensure NIST AU-3 (Content of Audit Records) compliance so records capture process name, user, timestamp, and command arguments sufficient for post-event reconstruction. Note: absence of behavioral alerts does not confirm absence of compromise given the dynamic nature of the claimed capability.

Framework Mappings

MITRE-ATTACK

- **T1587.001** — Malware
- **T1071** — Application Layer Protocol
- **T1566** — Phishing
- **T1059** — Command and Scripting Interpreter
- **T1027** — Obfuscated Files or Information

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1587.001	Malware	Resource-Development
T1071	Application Layer Protocol	Command-And-Control
T1566	Phishing	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1027	Obfuscated Files or Information	Defense-Evasion

Sources

Source	URL	Tier
ESET APT report finds state-backed hackers escalate cyberattacks ...	https://industrialcyber.co/reports/eset-apt-report-finds-state-back...	T3

Source	URL	Tier
[PDF] Cyber Threat Activity Related to the Russian Invasion of Ukraine	https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-a...	T3
2017 Ukraine ransomware attacks - Wikipedia	https://en.wikipedia.org/wiki/2017_Ukraine_ransomware_attacks	T3
Threat Brief: Ongoing Russia and Ukraine Cyber Activity	https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021...	T3
ANALYSIS OF THE CYBERATTACK ON UKRAINIAN ... - csirt mon	https://csirt-mon.wp.mil.pl/aktualnosci/analysis-of-the-cyberattack...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-23 19:01 UTC by TJS Security Command Center