INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 06:47 UTC

Russia-Aligned GREYVIBE Threat Group Uses ChatGPT and Google Gemini to Augment Cyberattacks Against Ukrainian Targets

THREAT CAMPAIGN | **HIGH**

SCC Item ID	SCC-CAM-2026-0404
Type	Threat Campaign
Severity	HIGH
Affected Products	Ukrainian organizations (targets); ChatGPT and Google Gemini (abused as attack enablement tools)
Published	2026-06-03
Discovery Source	Gemini

Executive Summary

A Russia-aligned threat group tracked as GREYVIBE has been observed using commercial AI platforms, ChatGPT and Google Gemini, to accelerate phishing campaigns, assist malware development, and support post-compromise operations against Ukrainian organizations. The AI platforms themselves are not compromised; adversaries are misusing legitimate services to reduce operational cost and improve attack quality. Organizations with Ukrainian partnerships, supply chain ties, or geopolitical exposure should treat this as an indicator of a maturing AI-assisted threat model that will expand beyond current target sets.

Technical Analysis

GREYVIBE, a Russia-aligned threat actor, has incorporated commercial generative AI into multiple offensive phases: phishing lure generation (T1566, T1566.001), malware scripting and development (T1588.001, T1059), reconnaissance and translation support (T1592, T1598), and likely user execution enablement (T1204). The group is reported to have used both ChatGPT and Google Gemini concurrently. No CVE or CWE applies; this is adversarial misuse of legitimate AI services, not a platform vulnerability. Google's GTIG has documented threat actor use of Gemini for scripting, reconnaissance, and translation. Primary MITRE techniques: T1059 (Command and Scripting Interpreter), T1566/T1566.001 (Phishing/Spearphishing Attachment), T1588/T1588.001 (Obtain Capabilities/Malware), T1204 (User Execution), T1592 (Gather Victim Identity Information), T1598 (Phishing for Information). Attribution claim ('GREYVIBE,' 'dual-platform operation') attributed to Check Point but requires primary-source verification. Source quality is secondary-tier (primarily vendor blogs and academic preprints, no primary-source corroboration of GREYVIBE attribution). Confidence in attribution claims is moderate pending primary-source verification from CISA or Check Point.

Action Checklist

1. Step 1: Containment, Assess exposure of Ukrainian-affiliated users, partners, or supply chain contacts. If your organization has operational ties to Ukrainian entities, treat inbound communications from those channels as elevated-risk until further notice. Temporarily increase scrutiny on email attachments and links from Ukrainian domains (NIST IR-4: Incident Handling).
2. Step 2: Detection, Query email gateway logs for phishing indicators consistent with AI-generated lure characteristics: grammatically polished content, low typo rate, personalized salutations in bulk campaigns. Search endpoint logs for execution of scripts via T1059 sub-techniques (PowerShell, cmd, scripting interpreters). Review SIEM for T1566.001 indicators, attachment-based delivery with macro or script payloads. Reference NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs) for logging coverage validation.
3. Step 3: Eradication, No patch exists - this threat is mitigated through detection, response procedures, and user awareness, not software updates. Enforce NIST SI-4 (System Monitoring) to detect anomalous post-compromise behavior. Block or restrict outbound connections to known C2 infrastructure if IOCs are confirmed by your threat intel feed. Review and harden email filtering rules to flag high-fidelity phishing that lacks traditional grammar-based indicators.
4. Step 4: Recovery, Validate that endpoint detection rules account for AI-polished phishing (update rules to reduce dependence on grammar/typo heuristics). Confirm MFA is enforced on all externally exposed applications and remote access (CIS 6.3, CIS 6.4, NIST AC-17). Audit accounts for unauthorized access following any confirmed phishing click. Monitor for lateral movement and credential misuse consistent with post-compromise operations (NIST SI-5 for account compromise monitoring; NIST AC-2 for credential lifecycle management).
5. Step 5: Post-Incident, Document whether existing phishing detection rules were tuned to catch AI-generated lures. Update threat model to include AI-assisted adversarial capability as a baseline assumption, not an edge case. Brief security awareness program to address AI-generated phishing that no longer contains obvious language errors. Map gaps to NIST IR-2 (Incident Response Training) and CIS 7.1 (Vulnerability Management Process). Consider adding AI-misuse indicators to your threat intelligence requirements list.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if any confirmed phishing click is associated with an account holding access to Ukrainian partner PII, contract data, or classified operational information, or if post-compromise lateral movement indicators (Event ID 4648, anomalous Kerberos TGS requests, or impossible-travel logons) are observed on domain controllers or systems processing supply chain communications.

Recovery Notes	Post-containment, maintain elevated monitoring on email gateways and authentication logs for a minimum of 30 days given GREYVIBE's pattern of multi-stage campaigns where initial phishing access is used to establish persistence before operational activity begins. Verify that all accounts interacting with Ukrainian-affiliated communications have MFA enforced and that no OAuth application consents were granted during the suspected exposure window — revoke any unrecognized delegated permissions in Azure AD / Entra ID. Monitor CERT-UA (cert.gov.ua) and CISA advisories weekly for updated GREYVIBE IOCs and adjust email filtering and firewall block rules as new infrastructure is published.
Forensic Artifacts	Email gateway delivery logs (raw SMTP envelope + full headers) for inbound messages from Ukrainian-affiliated sender domains in the 30 days preceding detection — preserves GREYVIBE's AI-generated lure content, spoofed sender patterns, and attachment SHA-256 hashes before log rotation | Windows Security Event ID 4688 (Process Creation with command-line logging enabled) filtered on scripting interpreters (PowerShell.exe, wscript.exe, cscript.exe, mshta.exe) spawned from Office applications — captures the initial execution chain if a GREYVIBE macro or script payload was activated on an endpoint | Sysmon Event ID 3 (Network Connection) records from endpoints that opened suspected GREYVIBE attachments, filtered on outbound connections initiated by Office processes or LOLBins within 60 seconds of file open — identifies C2 callback destinations before persistence is established | Azure AD / Entra ID sign-in logs and OAuth application consent grants for accounts in the elevated-risk Ukrainian partner communication scope, covering 14 days prior to detection — surfaces credential compromise, token theft, or consent phishing completions consistent with GREYVIBE post-compromise objectives | Prefetch files from %SystemRoot%\Prefetch\ on affected endpoints parsed with PECmd (Zimmerman Tools) — reconstructs execution history of certutil.exe, regsvr32.exe, rundll32.exe, and other LOLBins commonly used in Russia-attributed campaigns for payload staging and defense evasion following initial macro execution

Per-Action IR Details

Step 1: Containment — Assess exposure of Ukrainian-affiliated users, partners, or supply chain contacts. If your organization has operational ties to Ukrainian entities, treat inbound communications from those channels as elevated-risk until further notice. Temporarily increase scrutiny on email attachments and links from Ukrainian domains (NIST IR-4: Incident Handling).

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-4 (Information Flow Enforcement), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Export your mail gateway's inbound message trace for the past 30 days filtered on sender domains resolving to Ukrainian TLDs (.ua) or partner-declared Ukrainian MX infrastructure. Without a SIEM, use PowerShell against Exchange/M365 logs: `Get-MessageTrace -SenderAddress *@*.ua -StartDate (Get-Date).AddDays(-30)`. Flag any messages with HTML attachments, .docm/.xlsm payloads, or embedded URLs shortening services (bit.ly, t.co) routed through Ukrainian-affiliated contacts. Maintain a manually curated contact list of known Ukrainian partner email domains and apply enhanced quarantine rules in your email gateway (Postfix milter, Exchange transport rules, or ProofPoint free tier) for that sender scope.

Evidence: Before reclassifying inbound risk posture, preserve: (1) full email headers and raw MIME source for all messages received from Ukrainian-affiliated senders in the prior 30 days — these establish baseline communication cadence and will surface any volume spikes or spoofed-domain patterns consistent with GREYVIBE phishing setup; (2) DNS query logs from your resolver for lookups against .ua domains or Ukrainian-hosted infrastructure in the same window, retrievable from Pi-hole, BIND query logs, or Windows DNS debug logging at %SystemRoot%\System32\dns\dns.log; (3) your current email gateway quarantine queue contents before rule

changes alter what is retained.

Step 2: Detection — Query email gateway logs for phishing indicators consistent with AI-generated lure characteristics: grammatically polished content, low typo rate, personalized salutations in bulk campaigns. Search endpoint logs for execution of scripts via T1059 sub-techniques (PowerShell, cmd, scripting interpreters). Review SIEM for T1566.001 indicators — attachment-based delivery with macro or script payloads. Reference NIST AU-6 (Audit Record Review) and CIS 8.2 (Collect Audit Logs) for logging coverage validation.

NIST Phase: Detection Analysis

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

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

Compensating: Deploy Sysmon with SwiftOnSecurity's config (github.com/SwiftOnSecurity/sysmon-config) and focus on Event ID 1 (Process Create) to catch PowerShell, wscript.exe, cscript.exe, or mshta.exe spawned from Outlook.exe, Word.exe, or Excel.exe — the expected execution chain if a GREYVIBE-attributed macro payload is activated. Without a SIEM, collect Sysmon logs centrally using Winlogbeat shipping to a local Elasticsearch node (free tier) or parse offline with `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1} | Select-Object TimeCreated, Message`. For email-layer detection of AI-polished phishing without grammar heuristics, apply Sublime Security's open detection rules (sublimesecurity.com) or write a Sigma rule targeting bulk-send patterns: identical body hash with unique recipient personalization tokens — a structural fingerprint of AI-generated spear-phishing at scale.

Evidence: Capture before analysis concludes: (1) Windows Security Event Log Event ID 4688 (Process Creation) with command-line auditing enabled — filter on PowerShell.exe, cmd.exe, wscript.exe, cscript.exe where the parent process is an Office application or email client, consistent with GREYVIBE's expected macro or script-based initial execution (MITRE T1059.001, T1059.003); (2) Sysmon Event ID 3 (Network Connection) records showing outbound connections initiated by Office processes or scripting interpreters within 60 seconds of document open — these capture C2 callback attempts before any persistence mechanism runs; (3) Email gateway delivery logs in raw format (not summarized reports) preserving full SMTP envelope data, X-Originating-IP headers, and attachment SHA-256 hashes for all messages received from the elevated-risk sender scope defined in Step 1; (4) Office macro execution records from Windows Application Event Log Event ID 4625 and registry key HKCU\Software\Microsoft\Office\\\Security\VBAWarnings to establish whether macro execution controls were in place at time of delivery.

Step 3: Eradication — There is no patch; this is an abuse-of-service threat vector. Mitigation focuses on controls. Enforce NIST SI-4 (System Monitoring) to detect anomalous post-compromise behavior. Block or restrict outbound connections to known C2 infrastructure if IOCs are confirmed by your threat intel feed. Review and harden email filtering rules to flag high-fidelity phishing that lacks traditional grammar-based indicators.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-4 (System Monitoring), NIST AC-4 (Information Flow Enforcement), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For C2 blocking without a commercial threat intel feed, subscribe to free IOC sources that track Russia-aligned threat infrastructure: abuse.ch URLhaus (urlhaus.abuse.ch), CISA's known bad IPs feed (cisa.gov/stopransomware), and OpenPhish (openphish.com). Convert confirmed IOCs to Windows Firewall block rules via PowerShell: `New-NetFirewallRule -DisplayName 'GREYVIBE-C2-Block' -Direction Outbound -RemoteAddress -Action Block`. For DNS-layer blocking, add confirmed C2 domains to Pi-hole blocklists or Windows DNS RPZ policy. Disable Office macro execution via Group Policy (User Configuration > Administrative Templates > Microsoft Office > Security Settings > VBA Macro Notification Settings = Disabled) or, at minimum, enable Attack Surface Reduction rule GUID 92E97FA1-2EDF-4476-BDD6-9DD0B4DDDC7B (Block Office applications from creating

executable content).

Evidence: Before hardening controls, preserve: (1) current Windows Firewall and proxy logs showing all outbound connections from endpoints that received suspected GREYVIBE lures — these establish pre-hardening C2 communication baselines and may reveal already-active beaconing to Russia-attributed infrastructure; (2) running process list (`Get-Process` with `-IncludeUserName` and module paths) and active network connection table (`netstat -bno` or Sysmon Event ID 3) from any endpoint where a suspicious attachment was opened — capture before firewall rules terminate active sessions; (3) prefetch files from %SystemRoot%\Prefetch\ on affected endpoints (use PECmd from Eric Zimmerman's toolkit) to reconstruct execution history of any LOLBins (PowerShell, mshta, certutil, regsvr32) that GREYVIBE scripts are known to abuse for payload staging.

Step 4: Recovery — Validate that endpoint detection rules account for AI-polished phishing (update rules to reduce dependence on grammar/typo heuristics). Confirm MFA is enforced on all externally exposed applications and remote access (CIS 6.3, CIS 6.4, NIST AC-17). Audit accounts for unauthorized access following any confirmed phishing click. Monitor for lateral movement and credential misuse consistent with post-compromise operations (D3-LAM: Local Account Monitoring; D3-CRO: Credential Rotation).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.3 (Disable Dormant Accounts)

Compensating: Audit MFA enrollment without a commercial IAM platform: query Azure AD/Entra ID with `Get-MgUser -All | Get-MgUserAuthenticationMethod` or use the free Microsoft Entra ID MFA reporting blade to identify accounts with only password authentication on externally exposed apps. For lateral movement detection without EDR, enable Windows Security Event ID 4648 (Explicit Credential Use / Pass-the-Hash indicator), Event ID 4768/4769 (Kerberos TGT/TGS requests — watch for anomalous service ticket requests from workstations), and Event ID 4624 Type 3 (Network Logon) from non-standard source hosts. Deploy DeepBlueCLI (github.com/sans-blue-team/DeepBlueCLI) against collected Windows Event Logs to surface credential abuse patterns at scale without SIEM infrastructure. Reset credentials for any account that clicked a confirmed GREYVIBE lure, prioritizing accounts with access to Ukrainian partnership data or supply chain communications.

Evidence: Preserve before account remediation: (1) Azure AD / Active Directory sign-in logs for all accounts that received or interacted with suspected GREYVIBE phishing, covering the 14 days prior to detection — these capture any OAuth token grants, consent phishing completions, or impossible-travel logon anomalies that indicate credential compromise; (2) Windows Security Event ID 4624 (Successful Logon) and 4625 (Failed Logon) logs from domain controllers, filtered on logon types 3 (Network) and 10 (RemoteInteractive) for accounts in scope — export before any credential rotation invalidates forensic baseline; (3) browser history and credential store artifacts from affected user profiles (%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\History, Chrome equivalent) to determine whether GREYVIBE lures directed victims to credential-harvesting pages mimicking legitimate Ukrainian partner portals.

Step 5: Post-Incident — Document whether existing phishing detection rules were tuned to catch AI-generated lures. Update threat model to include AI-assisted adversarial capability as a baseline assumption, not an edge case. Brief security awareness program to address AI-generated phishing that no longer contains obvious language errors. Map gaps to NIST IR-2 (Incident Response Training) and CIS 7.1 (Vulnerability Management Process). Consider adding AI-misuse indicators to your threat intelligence requirements list.

NIST Phase: Post Incident

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

Controls: NIST IR-2 (Incident Response Training), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST PM-16 (Threat Awareness Program), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a structured lessons-learned using the NIST 800-61r3 §4.1 framework within 5 business days of containment. Without a commercial awareness platform, distribute a one-page internal advisory documenting

GREYVIBE's AI-polished phishing characteristics — specifically: absence of grammar errors, plausible personalization referencing real Ukrainian partner names or project context (likely harvested via OSINT), and lure themes consistent with wartime humanitarian or logistics contexts. Update phishing simulation templates (GoPhish, free tier) to use AI-generated content so staff are tested against realistic current-generation lures rather than legacy grammar-error samples. Add the following Priority Intelligence Requirements (PIRs) to your threat intel collection plan: (1) new GREYVIBE infrastructure IOCs from CERT-UA (cert.gov.ua/articles), (2) ChatGPT and Gemini abuse pattern reporting from OpenAI and Google Transparency reports, (3) Russia-attributed phishing campaigns targeting organizations with Ukrainian supply chain exposure.

Evidence: Compile for post-incident documentation: (1) the full corpus of GREYVIBE-attributed phishing emails received, with headers, body text, and attachment hashes preserved — this becomes the ground-truth training dataset for tuning future detection rules and awareness simulations; (2) a delta analysis comparing pre-incident email filtering rule configurations against post-incident hardened configurations, documenting specifically which grammar-based or typo-detection heuristics were retired and what behavioral or structural rules replaced them; (3) CERT-UA published advisories (cert.gov.ua) referencing GREYVIBE or Russia-aligned AI-assisted phishing campaigns — cross-reference your observed IOCs and lure themes against CERT-UA's public reporting to confirm attribution confidence and identify any TTPs your detection missed.

Detection Guidance

AI-generated phishing lures are harder to catch with grammar-based filters. Shift detection toward behavioral and contextual signals. In email gateway logs: flag high-personalization mass-send patterns, mismatches between sender domain age and email volume, and attachments with embedded scripts. In endpoint logs: monitor for T1059 execution (PowerShell, WScript, cscript) spawned from Office processes, a reliable post-click indicator. In SIEM: correlate T1566.001 delivery events with T1204 user execution and subsequent outbound connections. Apply NIST AU-2 (Event Logging) to ensure email, endpoint, and network telemetry are captured with sufficient fidelity. NIST AU-3 (Content of Audit Records) requires timestamps, source, and outcome fields - validate these are populated. MITRE ATT&CK T1566 detection: look for email headers indicating bulk send infrastructure combined with targeted, personalized body content, a pattern consistent with AI-assisted spearphishing at scale. NIST SI-7 (Information System Monitoring) and AU-3 (Content of Audit Records) apply if post-compromise scripts modify configuration or auth files. No confirmed IOCs are available from the sources reviewed; treat any IOCs from third-party feeds referencing GREYVIBE as medium confidence pending primary-source verification.

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1650** — Acquire Access
- **T1588** — Obtain Capabilities
- **T1566.001** — Spearphishing Attachment
- **T1204** — User Execution
- **T1588.001** — Malware
- **T1566** — Phishing

NIST-800-53R5

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1650	Acquire Access	Resource-Development
T1588	Obtain Capabilities	Resource-Development
T1566.001	Spearphishing Attachment	Initial-Access
T1204	User Execution	Execution
T1588.001	Malware	Resource-Development
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
GTIG AI Threat Tracker: Distillation, Experimentation, and ...	https://cloud.google.com/blog/topics/threat-intelligence/distillati...	T3

Source	URL	Tier
[PDF] Adversarial Misuse of Generative AI - Google	https://services.google.com/fh/files/misc/adversarial-misuse-genera...	T3
Emerging Cybersecurity and Privacy Threats of ChatGPT, Gemini ...	https://www.preprints.org/manuscript/202410.1909	T3
Google: How Threat Actors Use Gemini for Theft & Espionage	https://cybermagazine.com/news/google-how-threat-actors-use-gemini-...	T3
America built ChatGPT and Gemini for the world Now those same ...	https://www.instagram.com/reel/DZFWikvAJFy/	T3

Generated 2026-06-04 06:47 UTC by TJS Security Command Center