INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 14:01 UTC

# Russian APT Division of Labor: Gamaredon Brokers Access, Turla Deploys Kazuar Against Ukrainian Targets

**THREAT CAMPAIGN** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0391 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | Ukrainian military and government organizations; no specific commercial products identified |
| **Published** | 2026-06-02T13:00:58+00:00 |
| **Discovery Source** | Rss:T1 Threatintel |

## Executive Summary

ESET researchers confirmed the first documented operational collaboration between two Russian FSB-linked APT groups, Gamaredon and Turla, targeting Ukrainian military and government organizations between February and June 2025. Gamaredon established initial footholds using custom malware, then handed access to Turla, which deployed the Kazuar backdoor for deep espionage operations. This pattern reflects deliberate coordination between Russian state actors. Organizations with Ukrainian government partnerships should treat initial low-sophistication access activity as a potential precursor to high-capability follow-on intrusions.

## Technical Analysis

ESET researchers documented a two-stage intrusion chain spanning February-June 2025, presented by SentinelOne at LabsCon25. Gamaredon (FSB-linked, also tracked as Primitive Bear/Shuckworm) used its proprietary tools PteroGraphin and PteroOdd to establish persistence within Ukrainian military and government networks. These footholds were then transferred to Turla (also FSB-linked, also tracked as Snake/Venomous Bear), which deployed the Kazuar backdoor, a sophisticated .NET-based implant known for encrypted C2 communications and modular espionage capabilities. No CVE identifiers are associated with this campaign; exploitation relied on spearphishing (T1566.001), valid account abuse (T1078), and trusted relationship compromise (T1199) rather than unpatched software vulnerabilities. Key ATT&CK techniques observed: T1566/T1566.001 (spearphishing), T1078 (valid accounts), T1574 (hijack execution flow), T1057 (process discovery), T1560 (archive collected data), T1105 (ingress tool transfer), T1543 (create/modify system process),

T1021 (remote services), T1133 (external remote services), T1083 (file and directory discovery), T1591 (gather victim org information). No patch is applicable; this campaign relied on operational tradecraft rather than software vulnerabilities.

## Action Checklist

1. Step 1: Containment. Audit all external remote access paths (VPN, RDP, external-facing services) for anomalous authentication events, particularly from accounts with elevated privileges. Enforce NIST AC-17 (Remote Access) controls: verify connection requirements are documented and monitored. Isolate any host exhibiting PteroGraphin or PteroOdd behavioral indicators (scheduled task creation, unusual outbound HTTP/HTTPS to dynamic DNS domains). Reference CIS 4.4 and CIS 4.5 to confirm host-based firewall rules block unexpected egress.
2. Step 2: Detection. Hunt for Kazuar backdoor indicators: look for .NET assemblies loaded by non-.NET-native processes, encrypted outbound sessions to unusual intervals suggesting beaconing (T1071), and newly created or modified system services/scheduled tasks (T1543). Review Windows Security Event IDs 4624, 4625, 4648, 4698, 4702, and 7045. Query for PteroGraphin/PteroOdd behavioral signatures: file writes to %TEMP% or %APPDATA% followed by scheduled task registration and outbound connections to Gamaredon-associated dynamic DNS infrastructure. Enable NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) across endpoint and network telemetry. Monitor local account creation and modification (NIST AC-2) and review system file integrity (NIST SI-7) to flag unauthorized persistence mechanisms.
3. Step 3: Eradication. Remove identified persistence mechanisms: delete unauthorized scheduled tasks, services, and registry run keys associated with PteroGraphin, PteroOdd, or Kazuar. Rotate all credentials per NIST IA-5 (Password Management) for any account that authenticated during the suspect window, prioritizing privileged accounts. Revoke and reissue certificates or tokens used by affected services. Audit third-party and trusted partner access paths (T1199) and revoke access that cannot be verified as legitimate per NIST AC-20 (Use of External Systems).
4. Step 4: Recovery. Validate eradication by re-running behavioral hunts across the same timeframe and confirming absence of C2 beaconing. Restore affected systems from verified clean backups only after confirming no Kazuar persistence remains. Re-enable access incrementally, enforcing MFA per CIS 6.3, 6.4, and 6.5 (NIST IA-2). Monitor restored systems with elevated logging fidelity for a minimum of 30 days. Confirm NIST AU-11 (Audit Record Retention) ensures logs from the incident window are preserved for forensic review.
5. Step 5: Post-Incident. This campaign exposes a specific control gap: initial access by a lower-sophistication actor does not always represent the end state. Review detection logic to ensure low-confidence Gamaredon-linked alerts automatically trigger threat hunting workflows rather than being closed as resolved. Implement NIST SI-4 (System Monitoring) enhancements to correlate initial access detections with subsequent lateral movement or new tool deployment. Document lessons learned against NIST IR-4 (Incident Handling) and update playbooks to include a 'secondary actor' hypothesis when state-affiliated initial access is suspected. Evaluate supply chain and trusted partner access under NIST SA-12 and AC-20.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate immediately to national CERT (CERT-UA) and senior leadership if any Kazuar backdoor indicator is confirmed on a host with access to classified military or government data, if evidence of credential harvesting (LSASS access, SAM database reads) is found suggesting lateral movement beyond initially identified hosts, or if the organization lacks the internal DFIR capacity to perform memory forensics on suspected Kazuar-infected systems — this campaign involves FSB-linked actors with nation-state resources and the Turla Kazuar backdoor has documented capabilities beyond what a standard IR team can fully assess without specialized tooling. |
| **Recovery Notes** | Restore only from backups with creation timestamps confirmed to predate February 2025 and validated offline with YARA scanning for Kazuar .NET signatures before reconnecting to the production network. Given Kazuar's modular architecture and Turla's documented long-dwell tradecraft, maintain elevated Sysmon and network logging fidelity on all restored systems for a minimum of 60 days — not 30 — with specific attention to .NET CLR loads by unexpected processes and low-frequency encrypted outbound sessions that could indicate a dormant Kazuar instance reactivating. Re-enable privileged and third-party access only after MFA enforcement is confirmed and all partner access paths documented under NIST AC-20 have been individually reverified as legitimate. |
| **Forensic Artifacts** | Windows Task Scheduler XML definitions under C:\Windows\System32\Tasks\ — PteroGraphin and PteroOdd use scheduled tasks as their primary persistence mechanism; examine creation timestamps, action binary paths, and trigger conditions for tasks created between February–June 2025 that reference executables in %TEMP%, %APPDATA%, or %ProgramData%. \| Sysmon Event ID 7 (Image Loaded) logs filtered for clr.dll and mscorlib.dll loaded by non-.NET-native host processes — Kazuar is a .NET backdoor and its injection into unexpected processes will produce anomalous CLR load events that are the most reliable host-based indicator of active Kazuar execution. \| Windows DNS Client Operational log (Microsoft-Windows-DNS-Client/Operational) and cached DNS entries (ipconfig /displaydns) for queries resolving to dynamic DNS providers (*.ddns.net, *.no-ip.biz, *.hopto.org, *.myftp.org) — Gamaredon's PteroGraphin/PteroOdd infrastructure exclusively uses dynamic DNS for C2, making this log the primary network-layer indicator of Gamaredon staging activity prior to Kazuar handoff. \| Process memory dumps from any svchost.exe, rundll32.exe, or LOLBin process exhibiting jittered encrypted outbound connections — Kazuar stores its encrypted plugin configuration, tasking queue, and operator communications in process memory and does not persist this data to disk, making live memory forensics the only reliable method for full capability assessment and C2 infrastructure extraction. \| HKLM\SYSTEM\CurrentControlSet\Services\ registry hive export and Windows System Event Log Event ID 7045 entries — Turla's Kazuar deployment in this campaign used service-based persistence; the service registration event and associated ImagePath registry value will contain the Kazuar binary path and can be correlated against the Gamaredon initial access timestamp to forensically establish the actor handoff timeline. |

### Per-Action IR Details

**Step 1: Containment — Audit all external remote access paths (VPN, RDP, external-facing services) for anomalous authentication events, particularly from accounts with elevated privileges. Enforce NIST AC-17 (Remote Access) controls: verify connection requirements are documented and monitored. Isolate any host exhibiting PteroGraphin or PteroOdd behavioral indicators (scheduled task creation, unusual outbound HTTP/HTTPS to dynamic DNS domains). Reference CIS 4.4 and CIS 4.5 to confirm host-based firewall rules block unexpected egress.**

**NIST Phase:** Containment

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

**Controls:** NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

**Compensating:** Use Windows Firewall with Advanced Security (netsh advfirewall) to create egress deny rules blocking outbound HTTP/HTTPS to dynamic DNS domains commonly abused by Gamaredon (e.g., *.ddns.net, *.no-ip.org, *.hopto.org). Script discovery with PowerShell: Get-ScheduledTask | Where-Object { $_.TaskPath -notlike '\Microsoft*' } | Select TaskName, TaskPath, Actions. For network-level blocking on a budget, deploy pfSense or OPNsense with a threat feed subscription (e.g., Spamhaus or abuse.ch) to null-route known Gamaredon C2 infrastructure. Capture a full packet trace with Wireshark on suspected hosts before network isolation to preserve C2 beacon timing artifacts.

**Evidence:** Before isolating any host, preserve: (1) Windows Security Event Log entries for Event IDs 4624, 4648 (logon events tied to the suspect privilege escalation window), and 4698/4702 (scheduled task creation/modification — primary PteroGraphin/PteroOdd persistence mechanism); (2) full contents of Task Scheduler XML files under C:\Windows\System32\Tasks\ for any tasks created or modified during the February–June 2025 window; (3) prefetch files from C:\Windows\Prefetch\ for executables associated with PteroGraphin dropper activity; (4) netstat -ano output and active DNS cache (ipconfig /displaydns) capturing live connections to dynamic DNS infrastructure before isolation severs the C2 channel; (5) VPN/RDP authentication logs from the access gateway covering the Gamaredon initial access window for correlation with subsequent Turla Kazuar deployment timing.

**Step 2: Detection — Hunt for Kazuar backdoor indicators: look for .NET assemblies loaded by non-.NET-native processes, encrypted outbound sessions to irregular intervals suggesting beaconing (T1071), and newly created or modified system services/scheduled tasks (T1543). Review Windows Security Event IDs 4624, 4625, 4648, 4698, 4702, and 7045. Query for PteroGraphin/PteroOdd behavioral signatures: file writes to %TEMP% or %APPDATA% followed by scheduled task registration and outbound connections to Gamaredon-associated dynamic DNS infrastructure. Enable NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) across endpoint and network telemetry. Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to flag unauthorized persistence mechanisms.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

**Compensating:** Deploy Sysmon with a hardened config (SwiftOnSecurity or Olaf Hartong's modular config) to capture Event ID 1 (Process Create), Event ID 7 (Image Loaded — catches .NET assembly loads by unexpected parent processes indicative of Kazuar injection), and Event ID 11 (File Create in %TEMP%/%APPDATA%). Write a YARA rule targeting Kazuar's known .NET assembly characteristics and encrypted config blob patterns; scan with: yara -r kazuar_rule.yar C:\Users\ and C:\ProgramData\. Use Sigma rule 'proc_creation_win_schtasks_creation' mapped to MITRE T1053.005 to parse Sysmon logs with chainsaw (a free Sigma-compatible log scanner): chainsaw hunt C:\Windows\System32\winevt\Logs\ --rules sigma_rules\ --mapping mappings\sigma-event-logs-all.yml. For beaconing detection without a SIEM, use Rita (Real Intelligence Threat Analytics) against PCAP or Zeek logs to identify Kazuar's jittered beacon intervals to non-categorized IPs.

**Evidence:** Before tuning detection: (1) Extract Windows System Event Log Event ID 7045 (new service installed) and Security Event ID 4698/4702 entries covering the full February–June 2025 window to establish Gamaredon's initial persistence timeline versus Turla's Kazuar service registration timestamp — the gap between these two timestamps is forensically significant for proving the handoff; (2) Collect Sysmon Event ID 7 logs showing .NET CLR DLL loads (clr.dll, mscorlib.dll) by processes that are not expected .NET hosts (e.g., svchost variants, LOLBins); (3) Pull DNS query logs or Windows DNS Client ETW trace (Microsoft-Windows-DNS-Client/Operational) for queries resolving to dynamic DNS providers during the campaign window, which will map Gamaredon's PteroGraphin/PteroOdd C2 infrastructure; (4) Capture memory from any suspect process using ProcDump (procdump.exe -ma ) before remediation — Kazuar stores its encrypted configuration and tasking in process memory and will not survive a reboot;

(5) Export the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks registry hive to capture scheduled task GUIDs and associated action binaries for PteroGraphin persistence.

**Step 3: Eradication — Remove identified persistence mechanisms: delete unauthorized scheduled tasks, services, and registry run keys associated with PteroGraphin, PteroOdd, or Kazuar. Rotate all credentials (NIST IA-5, D3-CRO Credential Rotation) for all accounts that authenticated during the suspect window, prioritizing privileged accounts. Revoke and reissue certificates or tokens used by affected services. Audit third-party and trusted partner access paths (T1199) and revoke access that cannot be verified as legitimate per NIST AC-20 (Use of External Systems).**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST IA-5 (Authenticator Management), NIST AC-20 (Use of External Systems), NIST CM-7 (Least Functionality), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

**Compensating:** Use Autoruns (Sysinternals) with VirusTotal integration enabled (Options > Scan Options > Check VirusTotal.com) to enumerate and compare all persistence locations — scheduled tasks, services, registry run keys, WMI subscriptions — against known-good baselines; flag any entry with a VirusTotal detection or an unsigned binary path under %TEMP% or %APPDATA%. For credential rotation without enterprise tooling, use the built-in Active Directory PowerShell module: Get-ADUser -Filter * -Properties PasswordLastSet | Where-Object { $_.PasswordLastSet -lt (Get-Date).AddDays(-1) -and $_.Enabled -eq $true } to scope accounts active during the incident window, then force reset with Set-ADAccountPassword. For third-party access audit (T1199), pull firewall logs filtered to source IPs belonging to partner IP ranges and cross-reference against the Gamaredon-associated dynamic DNS resolution history to identify any trusted-path abuse.

**Evidence:** Before executing eradication: (1) Image all affected endpoint disks using a forensic tool (FTK Imager free edition or dc3dd) prior to deleting any persistence artifacts — Kazuar's full capability set including its plugin architecture may not be fully characterized until forensic analysis is complete; (2) Export the complete registry hive HKLM\SYSTEM\CurrentControlSet\Services\ to preserve Kazuar service registration details including binary path, display name, and ImagePath before deletion; (3) Collect all files written to %APPDATA%, %TEMP%, and C:\ProgramData\ by PteroGraphin/PteroOdd with creation timestamps in the February–June 2025 window using: Get-ChildItem -Path $env:APPDATA,$env:TEMP,'C:\ProgramData' -Recurse -File | Where-Object { $_.CreationTime -gt '2025-02-01' } | Select FullName, CreationTime, LastWriteTime; (4) Dump LSASS memory (with authorization) using ProcDump before credential rotation to assess whether Kazuar performed credential harvesting — this determines the blast radius of the credential rotation scope; (5) Preserve a copy of all scheduled task XML definitions and associated binary hashes before removal to support downstream threat intelligence sharing with CERT-UA and partner organizations.

**Step 4: Recovery — Validate eradication by re-running behavioral hunts across the same timeframe and confirming absence of C2 beaconing. Restore affected systems from verified clean backups only after confirming no Kazuar persistence remains. Re-enable access incrementally, enforcing MFA per CIS 6.3, 6.4, and 6.5 (D3-MFA). Monitor restored systems with elevated logging fidelity for a minimum of 30 days. Confirm NIST AU-11 (Audit Record Retention) ensures logs from the incident window are preserved for forensic review.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AU-11 (Audit Record Retention), NIST CP-10 (System Recovery and Reconstitution), 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), NIST AU-4 (Audit Storage Capacity)

**Compensating:** Before restoring from backup, validate backup integrity and absence of Kazuar implantation in backup images by mounting the backup volume offline and scanning with ClamAV (clamscan -r --detect-pua=yes /mnt/backup) combined with a custom YARA rule targeting Kazuar's known .NET binary signatures. For 30-day elevated monitoring without EDR, configure Sysmon Event ID 3 (Network Connection) logging with a whitelist of approved destinations and

pipe output to a local Elastic Stack (free tier) or simply to a forwarded Windows Event Log on a dedicated log server. Validate absence of beaconing using Rita against newly captured Zeek/PCAP traffic from restored hosts — specifically look for Kazuar's characteristic low-and-slow beacon pattern with jitter to avoid detection. For MFA on a budget, deploy Duo Security free tier (up to 10 users) or configure Windows Hello for Business for administrative accounts.

**Evidence:** Before restoring any system: (1) Confirm backup creation timestamps predate February 2025 (Gamaredon's initial access window) — any backup taken after initial compromise may contain PteroGraphin/PteroOdd persistence or Kazuar staging artifacts and must be treated as potentially compromised; (2) Run a final Sysmon Event ID 3 capture over a minimum 24-hour window on each candidate-for-restoration host to confirm no residual Kazuar beacon traffic to dynamic DNS or irregular-interval encrypted sessions is present; (3) Archive all incident-window logs (Windows Security, System, Sysmon, DNS Client, PowerShell/ScriptBlock Operational) to write-protected offline storage per AU-11 before any system rebuild that would overwrite the event log store; (4) Document the precise Kazuar deployment timestamp (derived from Event ID 7045 service install or Task Scheduler XML creation date) relative to last known-clean backup to establish a defensible restoration baseline; (5) Capture a post-eradication Autoruns baseline export from each restored system to serve as a clean-state reference for future anomaly detection.

**Step 5: Post-Incident — This campaign exposes a specific control gap: initial access by a lower-sophistication actor is not always the end state. Review detection logic to ensure low-confidence Gamaredon-linked alerts automatically trigger threat hunting workflows rather than being closed as resolved. Implement NIST SI-4 (System Monitoring) enhancements to correlate initial access detections with subsequent lateral movement or new tool deployment. Document lessons learned against NIST IR-4 (Incident Handling) and update playbooks to include a 'secondary actor' hypothesis when state-affiliated initial access is suspected. Evaluate supply chain and trusted partner access under NIST SA-12 and AC-20.**

**NIST Phase:** Post Incident

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

**Controls:** NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST SA-12 (Supply Chain Protection), NIST AC-20 (Use of External Systems), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** Encode the 'secondary actor handoff' detection hypothesis as a Sigma rule that fires when a host with a prior low-confidence Gamaredon indicator (dynamic DNS C2 connection, PteroGraphin scheduled task creation) subsequently generates Event ID 7045 (new service) or a new .NET assembly load within a 30-day window — this directly models the Gamaredon-to-Turla handoff timeline observed in this campaign. Share finalized IOCs (Kazuar C2 infrastructure, PteroGraphin/PteroOdd file hashes, scheduled task names, registry artifacts) with MISP or OpenCTI (both free, self-hosted) and contribute to CERT-UA's public threat intelligence feeds. Update the incident response playbook with an explicit decision node: 'If initial access actor is assessed as Gamaredon or equivalent access-broker APT, do not close — escalate to full threat hunt for secondary tooling deployment within 72 hours.' Reference MITRE ATT&CK G0047 (Gamaredon Group) and G0010 (Turla) in the playbook for technique cross-referencing.

**Evidence:** For lessons-learned documentation: (1) Reconstruct the full attack timeline from forensic artifacts — specifically the delta between PteroGraphin/PteroOdd first execution (Sysmon Event ID 1 or Prefetch timestamps) and Kazuar first beacon (Sysmon Event ID 3 or DNS query log) to quantify the dwell time of the handoff period and update mean-time-to-detect metrics; (2) Review all Gamaredon-attributed alerts that were closed as resolved during February–June 2025 without escalation to a full hunt — this is the primary control gap this campaign exploits; (3) Inventory all third-party and trusted partner access paths active during the campaign window (firewall allow rules, VPN split-tunnel configs, federated identity trusts) and document which were audited versus assumed legitimate, per NIST SA-12 requirements; (4) Preserve the complete forensic timeline and IOC set in a structured format (STIX 2.1) for submission to CERT-UA and peer Ukrainian government/military sector defenders; (5) Document Kazuar's full plugin capability set as observed in this environment — ESET's reporting indicates Kazuar has modular espionage functions including credential theft, screenshot capture, and keylogging — and assess which data categories were likely exfiltrated to inform breach notification obligations.

## Detection Guidance

Focus detection on two linked phases. Phase 1 (Gamaredon): Hunt for PteroGraphin and PteroOdd behavioral patterns, scheduled task creation by Office processes or scripting engines (Event ID 4698), outbound connections to Gamaredon-associated dynamic DNS domains (.ddns.net, .hopto.org, .sytes.net clusters historically used by this actor), and file staging in user-writable directories. Phase 2 (Turla/Kazuar): Hunt for encrypted beaconing at irregular jitter intervals from non-browser processes, .NET assembly injection into legitimate processes, and WMI or service creation events (Event IDs 7045, 4697) outside change windows. Cross-correlate: any host that triggered Phase 1 indicators should be prioritized for Phase 2 hunting regardless of whether Phase 1 was resolved. Monitor for unauthorized system file modification (NIST SI-7) and local account creation/modification (NIST AC-2) to detect unauthorized persistence. Network-level: alert on outbound encrypted sessions to newly registered or dynamic DNS domains from hosts in military/government network segments. SIEM rule suggestion: correlate (scheduled task creation by Office/script process) AND (outbound DNS query to dynamic DNS TLD) within a 24-hour window on the same host.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| DOMAIN | `Dynamic DNS infrastructure (.ddns.net, .hopto.org, .sytes.net clusters)` | Historically associated with Gamaredon C2 infrastructure; specific domains from this campaign not publicly confirmed in available sources | MEDIUM |
| HASH | `Not publicly disclosed in available sources` | PteroGraphin and PteroOdd malware samples — hashes not confirmed in T3-tier sources reviewed; check ESET's original research publication for confirmed hashes | LOW |

## Framework Mappings

### MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1566** — Phishing
- **T1574** — Hijack Execution Flow
- **T1078** — Valid Accounts
- **T1057** — Process Discovery
- **T1560** — Archive Collected Data
- **T1566.001** — Spearphishing Attachment
- **T1587.001** — Malware
- **T1105** — Ingress Tool Transfer
- **T1543** — Create or Modify System Process
- **T1021** — Remote Services
- **T1591** — Gather Victim Org Information

- **T1133** — External Remote Services
- **T1199** — Trusted Relationship
- **T1083** — File and Directory Discovery

**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
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **AC-20** — Use of External Systems

**ISO-27001-2022**

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

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1071 | Application Layer Protocol | Command-And-Control |
| T1566 | Phishing | Initial-Access |
| T1574 | Hijack Execution Flow | Persistence |
| T1078 | Valid Accounts | Defense-Evasion |
| T1057 | Process Discovery | Discovery |
| T1560 | Archive Collected Data | Collection |
| T1566.001 | Spearphishing Attachment | Initial-Access |
| T1587.001 | Malware | Resource-Development |
| T1105 | Ingress Tool Transfer | Command-And-Control |
| T1543 | Create or Modify System Process | Persistence |

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1021 | Remote Services | Lateral-Movement |
| T1591 | Gather Victim Org Information | Reconnaissance |
| T1133 | External Remote Services | Persistence |
| T1199 | Trusted Relationship | Initial-Access |
| T1083 | File and Directory Discovery | Discovery |

## Sources

| Source | URL | Tier |
|---|---|---|
| **SentinelLabs - We are hunters, reversers, exploit developers, and tinkerers shedding light on the world of malware, exploits, APTs, and cybercrime across all platforms.** | https://www.sentinelone.com/labs/labscon25-replay-gamaredon-x-turla... | T3 |
| | https://www.sentinelone.com/labs/labscon25-replay-gamaredon-x-turla... | T3 |
| **Russian GRU cyber actors are exploiting vulnerable routers ...** | https://www.facebook.com/FBI/posts/russian-gru-cyber-actors-are-exp... | T3 |
| **CISA Encourages “Shields Up” to Protect Organizations as Cyber ...** | https://www.commerciallitigationupdate.com/cisa-encourages-shields-... | T3 |
| **[PDF] Policy Brief Ukraine's Cyber Defence Evolution - CCDCOE** | https://ccdcoe.org/uploads/2026/03/CCDCOE_Policy_Brief_Ukraines_Cyb... | T3 |



Generated 2026-06-02 14:01 UTC by TJS Security Command Center