INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 18:58 UTC

Gamaredon Exploits WinRAR Path Traversal (CVE-2025-8088) to Deploy Modular Malware Chain Against Ukrainian Targets

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0396
Type	Threat Campaign
CVE ID	CVE-2025-8088, CVE-2026-21509
Severity	CRITICAL
CVSS Base Score	7.5
EPSS Score	0.0910 (93th percentile)
Affected Products	WinRAR (unspecified vulnerable versions); Windows (LNK abuse, scheduled tasks, Alternate Data Streams); Microsoft Office (delivery vector)
Published	2026-06-02T14:21:49
Discovery Source	Rss

Executive Summary

Russia's FSB-linked Gamaredon group is actively exploiting a path traversal vulnerability in WinRAR (CVE-2025-8088, CVSS 7.5) to deliver a four-stage malware chain against Ukrainian government, military, and critical infrastructure organizations. The attack chain deploys tools for initial access, persistence, lateral movement, and data exfiltration, with stolen files staged to AWS S3 buckets and command-and-control routed through Telegram to evade detection. Organizations outside Ukraine with Ukrainian government or defense sector supply chain relationships, or those running unpatched WinRAR, carry meaningful exposure to this campaign.

Technical Analysis

Gamaredon (aka Primitive Bear, Shuckworm, Armageddon), attributed to Russia's FSB, is exploiting CVE-2025-8088, a CWE-22/CWE-73 path traversal vulnerability in WinRAR, to deliver a modular four-stage malware chain. The chain: GammaPhish (phishing dropper, T1566.001), GammaLoad (loader/downloader, T1105), GammaWorm (lateral movement and removable-media propagation, T1091, T1080, T1021), GammaSteel (data collection and exfiltration, T1005, T1083, T1048.002). Delivery is via spearphishing attachments (T1566.001) abusing WinRAR's archive extraction path handling. Persistence uses Windows

scheduled tasks (T1053.005), LNK abuse (T1547.005), and Alternate Data Streams (T1564.004). C2 resolution abuses Telegram channels (T1102, T1102.002) to rotate infrastructure without reconfiguring implants. Exfiltrated data is staged to AWS S3 (T1567.002), blending with legitimate cloud traffic. Additional techniques include obfuscation (T1027, T1027.004), VBScript execution (T1059.005), and DLL/execution hijacking (T1574). CVSS base score of 7.5 is attributed to CVE-2025-8088 per source data; NVD confirmation is recommended before relying on this score operationally. CVE-2026-21509 is referenced in source materials; verification against NVD and CISA KEV is pending and recommended before operational reliance. The campaign is not listed on the CISA KEV catalog as of this report; monitor the catalog for additions.

Action Checklist

1. Containment: Identify all enterprise assets running WinRAR and isolate or restrict archive extraction on internet-facing and high-value systems until patching is confirmed. Block outbound connections to Telegram API endpoints (api.telegram.org) at the perimeter and proxy layers where operationally feasible, per NIST SC-7 (Boundary Protection). Implement egress filtering to flag or block anomalous uploads to AWS S3 endpoints from endpoints that have no legitimate business justification for S3 writes.

2. Detection: Search EDR and SIEM telemetry for WinRAR extracting files to unexpected path locations outside the designated destination folder (indicator of CVE-2025-8088 exploitation). Hunt for scheduled task creation (Event ID 4698/4702), LNK files in startup or temp directories, and files with Alternate Data Stream attachments (CIS 8.2, NIST AU-2). Query for outbound DNS or HTTP to api.telegram.org from non-user endpoints. Flag outbound PUT/POST traffic to amazonaws.com S3 endpoints from workstations or servers with no authorized cloud storage function. Review process trees for WinRAR spawning script interpreters (wscript.exe, cscript.exe) or cmd.exe, consistent with T1059.005 and T1059.

3. Eradication: Apply the vendor-issued WinRAR patch addressing CVE-2025-8088; confirm the patched version against the official RarLab release notes at rarlab.com (NVD entry nvd.nist.gov/vuln/detail/cve-2025-8088 should be consulted for confirmed affected version range once NVD record is fully populated). Remove any unauthorized scheduled tasks, LNK persistence entries, or ADS-bearing files identified during detection. Rotate credentials for any accounts active on systems showing indicators of GammaLoad or GammaSteel execution, per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Audit and disable default or dormant accounts per CIS 5.3 and CIS 4.7.

4. Recovery: Validate WinRAR patch deployment across asset inventory (CIS 1.1, CIS 7.3). Confirm no unauthorized scheduled tasks, startup entries, or ADS artifacts remain. Monitor previously affected systems for recurring C2 beaconing to Telegram or S3 exfiltration activity for a minimum of 30 days post-remediation, per NIST SI-4 (System Monitoring). Verify integrity of files on systems where GammaWorm propagation was suspected, including removable media and network shares (D3-SFA, System File Analysis). Re-enable restricted services only after endpoint integrity is confirmed.

5. Post-Incident: Conduct a control gap review against NIST IR-4 (Incident Handling) and IR-8 (Incident Response Plan). Evaluate whether egress filtering policies (NIST AC-4, Information Flow Enforcement) adequately restrict cloud storage uploads to authorized destinations. Assess whether Telegram and other social-platform API endpoints are appropriately categorized in proxy and firewall policy. Review removable media controls given GammaWorm's USB propagation vector (NIST AC-19). Implement or validate MFA on all remote access and administrative accounts (CIS 6.3, CIS 6.4, CIS 6.5, D3-MFA) to raise the cost of lateral movement following initial compromise.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive stakeholders if: any host shows confirmed GammaLoad or GammaSteel execution artifacts; outbound data transfers to S3 buckets are confirmed (indicating active exfiltration of potentially sensitive government, military, or critical infrastructure data); GammaWorm USB propagation artifacts are found on air-gapped or classified-adjacent network segments; or if your organization has contractual, regulatory, or sector-specific obligations (e.g., CISA CIRCIA reporting, FISMA, or defense industrial base requirements) triggered by nation-state attribution to a Russian FSB-linked threat actor.
Recovery Notes	Before re-enabling any systems to full production status, confirm WinRAR is patched to the vendor-verified clean version from rarlab.com on every endpoint in the asset inventory, and validate via the PowerShell registry query that no pre-patch version remains. Maintain continuous monitoring of outbound connections to api.telegram.org and *.amazonaws.com from all previously affected hosts for a minimum of 30 days, as Gamaredon is operationally persistent and has historically re-compromised targets within weeks using secondary implants or re-delivered LNK-based loaders via spearphishing. Any recurrence of Telegram C2 beaconing or S3 PUT activity from a remediated host should be treated as a new incident, not a remediation failure, and the full NIST 800-61r3 lifecycle should be restarted from §3.3.
Forensic Artifacts	WinRAR path traversal exploitation artifacts: Files written outside the user-designated extraction path — specifically, files deposited in '%TEMP%', '%APPDATA%', '%USERPROFILE%', or Windows startup directories by WinRAR.exe, captured via Sysmon Event ID 11 (FileCreate) with ParentImage matching WinRAR.exe and TargetFilename outside expected archive destinations. | GammaLoad/GammaSteel persistence artifacts: Scheduled task XML definitions in 'C:\Windows\System32\Tasks\' or 'C:\Windows\SysWOW64\Tasks\' with creation timestamps correlating to WinRAR extraction events, exported via 'schtasks /query /xml'; and LNK files in '%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\' with target paths pointing to script interpreters or dropped payload files. | Alternate Data Stream staging artifacts: Files in '%TEMP%', '%APPDATA%', or adjacent directories containing non-standard ADS entries (identified via 'Get-Item -Path -Stream * -Recurse | Where-Object Stream -ne ':$DATA'") — GammaSteel has used ADS to hide staged exfiltration data and encrypted credential caches before upload. | C2 and exfiltration network artifacts: DNS query logs and HTTP/HTTPS proxy logs showing resolution of api.telegram.org and specific S3 bucket FQDNs (format: '.s3..amazonaws.com') from affected endpoints, with corresponding PUT/POST request bodies and byte-transfer volumes that indicate staged file exfiltration to Gamaredon-controlled AWS infrastructure. | GammaWorm USB propagation artifacts: LNK files on removable media drives with target paths invoking wscript.exe or cmd.exe against a hidden payload dropped in a folder matching the volume label or a system-like directory name, detectable via recursive directory listing ('Get-ChildItem -Path :\ -Recurse -Force -Include *.lnk') and Sysmon Event ID 11 capturing file creation events on removable media volume paths.

Per-Action IR Details

Containment — Identify all enterprise assets running WinRAR and isolate or restrict archive extraction on internet-facing and high-value systems until patching is confirmed. Block outbound connections to Telegram API endpoints (api.telegram.org) at the perimeter and proxy layers where operationally feasible, per NIST SC-7 (Boundary Protection). Implement egress filtering to flag or block anomalous uploads to AWS S3 endpoints

from endpoints that have no legitimate business justification for S3 writes.

NIST Phase: Containment

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

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

Compensating: Use Windows Firewall with Advanced Security (wf.msc) or Group Policy to block outbound TCP 443 to 149.154.160.0/20 and 91.108.4.0/22 (Telegram IP ranges) and *.s3.amazonaws.com on systems lacking NGFWs. On Linux, deploy iptables rules: 'iptables -A OUTPUT -d 149.154.160.0/20 -j DROP'. Use pi-hole or local DNS sinkholes to null-route api.telegram.org and s3.amazonaws.com on segments with no legitimate S3 business need. Enumerate WinRAR installations via: 'Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Where-Object DisplayName -like "*WinRAR*" | Select-Object DisplayName,DisplayVersion,PSComputerName'.

Evidence: Before isolating assets, capture: (1) WinRAR extraction history from '%APPDATA%\WinRAR\' including 'WinRAR.log' if logging is enabled; (2) Network flow records (NetFlow/IPFIX or Windows Firewall logs at '%SystemRoot%\System32\LogFiles\Firewall\pfirewall.log') showing prior outbound connections to api.telegram.org or *.amazonaws.com from the candidate host; (3) Firewall/proxy logs showing DNS resolutions and HTTP POST/PUT requests to api.telegram.org or S3 bucket URLs from the affected endpoint; (4) Snapshot of active network connections via 'netstat -anob' and 'Get-NetTCPConnection' before containment to capture any live C2 sessions that would be severed by blocking; (5) Full disk image or at minimum volatile memory capture (via WinPmem or DumpIt) if the host shows active IOC hits, as GammaLoad and GammaSteel are known to operate in-memory.

Detection — Search EDR and SIEM telemetry for WinRAR extracting files to unexpected path locations outside the designated destination folder (indicator of CVE-2025-8088 exploitation). Hunt for scheduled task creation (Event ID 4698/4702), LNK files in startup or temp directories, and files with Alternate Data Stream attachments (CIS 8.2, NIST AU-2). Query for outbound DNS or HTTP to api.telegram.org from non-user endpoints. Flag outbound PUT/POST traffic to amazonaws.com S3 endpoints from workstations or servers with no authorized cloud storage function. Review process trees for WinRAR spawning script interpreters (wscript.exe, cscript.exe) or cmd.exe, consistent with T1059.005 and T1059.

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 SwiftOnSecurity config; Event ID 1 (Process Create) will expose WinRAR.exe spawning cmd.exe, wscript.exe, or cscript.exe. Use Sysmon Event ID 11 (File Create) to catch files written outside expected extraction paths — filter on TargetFilename not matching user-designated archive destination folders. Detect ADS creation via Sysmon Event ID 15 (FileCreateStreamHash). Hunt scheduled tasks without SIEM using: 'Get-ScheduledTask | Where-Object { $_.TaskPath -notlike "\Microsoft*" } | Select-Object TaskName,TaskPath,@{N="Command";E={$_.Actions.Execute}}'. Find LNK files in startup: 'Get-ChildItem "$env:APPDATA\Microsoft\Windows\Start Menu\Programs\Startup*.lnk" -Force'. Enumerate ADS: 'Get-Item C:\Users* -Stream * | Where-Object Stream -ne ":$DATA"'. Use Wireshark capture filter 'host api.telegram.org or host amazonaws.com' on a network tap or span port for hosts lacking EDR.

Evidence: Capture before pivoting to eradication: (1) Windows Security Event Log entries for Event ID 4698 (Scheduled Task Created) and 4702 (Scheduled Task Updated) — export via 'wevtutil epl Security C:\evidence\Security.evtx'; (2) Sysmon Event ID 1 process creation logs showing WinRAR.exe parent-child relationships — specifically look for WinRAR.exe > cmd.exe > wscript.exe chains indicating the four-stage dropper execution; (3) LNK file metadata from '%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup\' and '%TEMP%' using LECmd (Eric Zimmermann's tool) to extract target paths, creation timestamps, and machine SID; (4) ADS contents from identified bearer files using 'Get-Item -Stream *' followed by 'Get-Content -Stream ' — ADS is a known GammaSteel staging technique; (5) Proxy/DNS logs showing resolution and connection attempts to api.telegram.org and the specific S3 bucket FQDNs used for exfiltration staging.

Eradication — Apply the vendor-issued WinRAR patch addressing CVE-2025-8088; confirm the patched version against the official RarLab release notes at rarlab.com (NVD entry nvd.nist.gov/vuln/detail/cve-2025-8088 should be consulted for confirmed affected version range once NVD record is fully populated). Remove any unauthorized scheduled tasks, LNK persistence entries, or ADS-bearing files identified during detection. Rotate credentials for any accounts active on systems showing indicators of GammaLoad or GammaSteel execution, per NIST AC-2 (Account Management) and D3-CRO (Credential Rotation). Audit and disable default or dormant accounts per CIS 5.3 and CIS 4.7.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), NIST CM-3 (Configuration Change Control), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.3 (Disable Dormant Accounts), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Patch WinRAR by downloading the latest build directly from rarlab.com (verify file hash against RarLab's published checksums before deploying); push via GPO software installation or a batch script using 'msiexec /qn' or the silent installer flag. Remove unauthorized scheduled tasks: 'schtasks /delete /tn "" /f'. Remove malicious LNK files from startup using 'Remove-Item' with -Force. Strip ADS: 'Get-Item -Stream * | Where-Object Stream -ne ":$DATA" | Remove-Item'. Force AD password resets for affected accounts using: 'Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "" -Force)'. Disable dormant accounts with: 'Get-ADUser -Filter {LastLogonDate -lt (Get-Date).AddDays(-45)} | Disable-ADAccount'.

Evidence: Before removing artifacts: (1) Collect and hash all identified malicious scheduled task XML definitions via 'schtasks /query /xml /tn "" — GammaLoad persistence often uses task names mimicking legitimate Windows services; (2) Acquire bit-for-bit copies of malicious LNK files using 'Copy-Item' to an evidence share before deletion — LNK metadata (MAC timestamps, volume serial, NetBIOS name) is forensically significant for attribution and timeline reconstruction; (3) Extract and preserve full ADS content from all files identified with non-standard streams before stripping — GammaSteel has used ADS to cache stolen credential material; (4) Run Volatility or Redline memory analysis on affected hosts before credential rotation to capture in-memory GammaLoad/GammaSteel artifacts, including injected DLLs and decrypted C2 configuration strings; (5) Pull NTDS.dit snapshot and SYSTEM hive from any domain controller that authenticated accounts present on compromised hosts, as Gamaredon is known to target credential stores post-initial-access.

Recovery — Validate WinRAR patch deployment across asset inventory (CIS 1.1, CIS 7.3). Confirm no unauthorized scheduled tasks, startup entries, or ADS artifacts remain. Monitor previously affected systems for recurring C2 beaconing to Telegram or S3 exfiltration activity for a minimum of 30 days post-remediation, per NIST SI-4 (System Monitoring). Verify integrity of files on systems where GammaWorm propagation was suspected, including removable media and network shares (D3-SFA, System File Analysis). Re-enable restricted services only after endpoint integrity is confirmed.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST SI-4 (System Monitoring), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: Validate patch coverage by running: 'Invoke-Command -ComputerName (Get-ADComputer -Filter *).Name -ScriptBlock { Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Where-Object DisplayName -like "*WinRAR*" | Select-Object DisplayName,DisplayVersion,PSComputerName }' and compare output against the patched version confirmed at rarlab.com. Verify no residual scheduled tasks with: 'schtasks /query /fo LIST /v | Select-String "TaskName|Status|Run As User"'. For removable media integrity checks, use ClamAV with an updated signature set: 'clamscan -r --bell /media/'. Implement a free YARA rule targeting GammaWorm USB propagation artifacts (LNK files with specific target path patterns) and scan network shares with 'yara64.exe \\server\share\ -r'.

Evidence: During recovery validation, preserve: (1) Output of post-patch WinRAR version enumeration across all enterprise endpoints as a dated compliance record; (2) Scheduled task inventory export ('schtasks /query /fo CSV > tasks_post_eradication.csv') for comparison against pre-incident baseline to confirm no persistence survived; (3) Windows Event ID 7045 (New Service Installed) and 4698/4702 logs from the 30-day monitoring window to detect GammaLoad re-establishment attempts via alternative persistence mechanisms; (4) Network flow records for the 30-day post-remediation period flagging any re-emergence of outbound connections to api.telegram.org or amazonaws.com from previously affected hosts — Gamaredon is known to re-compromise targets using secondary implants; (5) Hash logs of all files on removable media and network shares scanned during GammaWorm propagation assessment, retained as chain-of-custody evidence.

Post-Incident — Conduct a control gap review against NIST IR-4 (Incident Handling) and IR-8 (Incident Response Plan). Evaluate whether egress filtering policies (NIST AC-4, Information Flow Enforcement) adequately restrict cloud storage uploads to authorized destinations. Assess whether Telegram and other social-platform API endpoints are appropriately categorized in proxy and firewall policy. Review removable media controls given GammaWorm's USB propagation vector (NIST AC-19). Implement or validate MFA on all remote access and administrative accounts (CIS 6.3, CIS 6.4, CIS 6.5, D3-MFA) to raise the cost of lateral movement following initial compromise.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AC-4 (Information Flow Enforcement), NIST AC-19 (Access Control for Mobile Devices), 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)

Compensating: Conduct the lessons-learned review using the NIST 800-61r3 §4 template questions as a structured agenda — document specifically: (a) how long WinRAR vulnerable versions were in the environment before detection, (b) whether proxy policy had Telegram API categorized before this incident, and (c) whether GammaWorm USB propagation was detected or discovered retrospectively. For MFA on a budget, deploy Windows Hello for Business (no license cost beyond Windows 10/11 Pro) or Duo Security's free tier for up to 10 users on administrative accounts. To harden against future Gamaredon delivery via malicious archives, configure Windows Defender Application Control (WDAC) policy to restrict script interpreter execution (wscript.exe, cscript.exe) from paths outside sanctioned directories — deploy via: 'ConvertFrom-CIPolicy -XmlFilePath -BinaryFilePath '.

Evidence: For the post-incident record, compile: (1) Full incident timeline from first WinRAR exploitation artifact timestamp through confirmed eradication, sourced from Windows Security Event Logs, Sysmon telemetry, and proxy logs — this timeline supports lessons-learned gap analysis and any regulatory notification obligations; (2) Inventory of all accounts that authenticated to affected systems during the incident window, sourced from Windows Security Event ID 4624 (Logon) and 4648 (Explicit Credential Logon) logs, to confirm credential rotation scope was complete; (3) Documentation of all C2 and exfiltration network indicators (specific Telegram bot IDs, S3 bucket names/URLs) observed during the incident, formatted as STIX 2.1 indicators for sharing with sector ISACs or CISA per NIST 800-61r3 §4 information-sharing guidance; (4) Proxy/firewall policy change records showing Telegram API and unauthorized S3 endpoints were blocked post-containment, retained for audit and compliance evidence; (5) Signed chain-of-custody documentation for all forensic artifacts collected during the investigation, required if the incident involves Ukrainian government partner data with potential intelligence or legal significance.

Detection Guidance

Primary detection focus areas: (1) WinRAR process behavior, monitor for WinRAR.exe writing files outside the user-specified extraction directory; flag any WinRAR process spawning script hosts (wscript.exe, cscript.exe, powershell.exe, cmd.exe). (2) Scheduled task abuse, Windows Event IDs 4698 and 4702 indicate scheduled task creation and modification; correlate with non-administrative accounts or unusual task names. (3) LNK persistence, monitor startup folders and HKCU/HKLM Run keys for newly created or modified LNK files,

consistent with T1547 and T1547.005. (4) Alternate Data Streams, use Sysinternals Streams or EDR ADS visibility to identify files with hidden data streams, especially in temp, download, and user profile directories (T1564.004). (5) C2 via Telegram, alert on outbound connections to api.telegram.org originating from non-browser, non-approved processes; this is anomalous for most enterprise environments (T1102, T1102.002). (6) Exfiltration to S3, correlate large or frequent outbound PUT requests to amazonaws.com S3 endpoints from workstations against an authorized cloud storage allowlist (T1567.002, T1048.002). (7) VBScript execution, monitor for vbs file execution from user-writable directories, consistent with T1059.005. Behavioral indicator: a process chain of WinRAR.exe → wscript.exe or cmd.exe → scheduled task registration is high-confidence for this campaign. Reference NIST AU-2 for event logging requirements and NIST AU-6 for review frequency. D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) are applicable countermeasures for post-exploitation detection.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`api.telegram.org`	Abused for C2 infrastructure resolution; Gamaredon implants query Telegram channels to retrieve current C2 endpoints — anomalous when initiated by non-browser processes	HIGH
URL	`amazonaws.com S3 endpoints (pattern: s3.amazonaws.com or s3.[region].amazonaws.com)`	Exfiltration staging destination for GammaSteel-collected data; flag outbound PUT/POST to S3 from endpoints without authorized cloud storage function	HIGH
HASH	`Not available — no confirmed file hashes present in verified source data at time of report`	Hash IOCs for GammaPhish, GammaLoad, GammaWorm, or GammaSteel components were not extractable from T1/T3 sources available; recommend querying threat intel platforms (VirusTotal, MISP) using campaign tag 'Gamaredon' or 'Shuckworm' for current hash sets	LOW

Framework Mappings

MITRE-ATTACK

- **T1053.005** — Scheduled Task
- **T1027** — Obfuscated Files or Information
- **T1102** — Web Service
- **T1071.001** — Web Protocols
- **T1102.002** — Bidirectional Communication
- **T1027.004** — Compile After Delivery
- **T1048.002** — Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

- **T1566.001** — Spearphishing Attachment
- **T1567.002** — Exfiltration to Cloud Storage
- **T1190** — Exploit Public-Facing Application
- **T1564.004** — NTFS File Attributes
- **T1083** — File and Directory Discovery
- **T1005** — Data from Local System
- **T1059** — Command and Scripting Interpreter
- **T1547.005** — Security Support Provider
- **T1021** — Remote Services
- **T1105** — Ingress Tool Transfer
- **T1091** — Replication Through Removable Media
- **T1080** — Taint Shared Content
- **T1547** — Boot or Logon Autostart Execution
- **T1059.005** — Visual Basic
- **T1574** — Hijack Execution Flow

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-7** — Least Functionality
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)
- **CA-7** — Continuous Monitoring
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1053.005	Scheduled Task	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1102	Web Service	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1102.002	Bidirectional Communication	Command-And-Control
T1027.004	Compile After Delivery	Defense-Evasion
T1048.002	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Exfiltration
T1566.001	Spearphishing Attachment	Initial-Access
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1190	Exploit Public-Facing Application	Initial-Access
T1564.004	NTFS File Attributes	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1005	Data from Local System	Collection
T1059	Command and Scripting Interpreter	Execution
T1547.005	Security Support Provider	Persistence

Technique ID	Technique Name	Tactic
T1021	Remote Services	Lateral-Movement
T1105	Ingress Tool Transfer	Command-And-Control
T1091	Replication Through Removable Media	Lateral-Movement
T1080	Taint Shared Content	Lateral-Movement
T1547	Boot or Logon Autostart Execution	Persistence
T1059.005	Visual Basic	Execution
T1574	Hijack Execution Flow	Persistence

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/gamaredon-exploits-winrar-to-deli...	T3
CVE-2025-8088 Detection: WinRAR Zero-Day Is Actively Exploited ...	https://socprime.com/blog/detect-cve-2025-8088-exploitation-for-rom...	T3
CVE-2025-8088 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2025-8088	T1
Known Exploited Vulnerabilities Catalog | CISA	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1
CVE-2025-8088 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2025-8088	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-8088, CVE-2026-21509	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-8088...	T1

Generated 2026-06-02 18:58 UTC by TJS Security Command Center