INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-16 06:38 UTC

Gremlin Stealer Adds Virtualized Packing, WebSocket Hijacking, and Live Crypto Theft to Its Arsenal

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0324
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Chromium-based browsers, Discord, FTP clients, VPN clients, cryptocurrency wallets (Windows endpoints); no specific software versions confirmed in source data
Published	2026-05-15T10:00:52+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Gremlin Stealer, a credential-theft tool sold on Telegram since March 2025, has been updated with capabilities that go beyond passive data collection: it now intercepts cryptocurrency transactions in real time and can hijack live authenticated browser sessions to redirect funds. Any Windows endpoint running Chromium-based browsers, Discord, VPN clients, or cryptocurrency wallets is a potential target. The business risk is direct financial loss from crypto theft and account takeover, compounded by detection evasion techniques that defeat most signature-based security controls.

Technical Analysis

Gremlin Stealer is a C#/.NET infostealer distributed via Telegram by the operator 'CoderSharp'. Updated variants introduce three-layer code obfuscation, .NET resource-embedded XOR-encoded payload delivery, and instruction virtualization through a commercial packer, collectively degrading static and dynamic analysis effectiveness (CWE-506: Embedded Malicious Code; CWE-693: Protection Mechanism Failure; CWE-027: Path Traversal). Credential theft targets Chromium-based browsers (passwords, cookies, autofill), Discord tokens, FTP clients, and VPN configurations (T1555.003, T1539). A clipboard hijacking module (T1115) intercepts cryptocurrency wallet addresses at copy time and silently substitutes attacker-controlled addresses, enabling live fund diversion. A WebSocket-based session hijacking module (T1185) enables takeover of authenticated browser sessions without re-authentication. C2 communication occurs over HTTP/S (T1071.001) with data exfiltration to attacker infrastructure (T1041). Newly identified C2 infrastructure at 194.87.92[.]109 returned zero

VirusTotal detections at time of initial discovery, meaning signature-based endpoint and network controls will not flag this indicator on first encounter. No CVE identifier applies; no vendor patch exists for the malware itself. No specific software version dependencies confirmed, threat is delivery-agnostic. Source: Unit 42 (Palo Alto Networks), T3 vendor intelligence. MITRE coverage: T1497, T1566, T1059.005, T1071.001, T1115, T1027, T1555.003, T1185, T1539, T1027.009, T1140, T1041, T1555, T1583.003, T1622.

Action Checklist

1. Containment, Block the confirmed C2 IP 194.87.92[.]109 at perimeter firewall and DNS sinkholes immediately. Apply blocks across all egress-capable endpoints and network segments where Chromium-based browsers, Discord, or crypto wallets are present. Do not rely solely on VirusTotal reputation; this IP showed zero detections at initial discovery and may remain undetected by signature-based tools.
2. Detection, Query endpoint and network telemetry for outbound connections to 194.87.92[.]109. Hunt for clipboard API access (T1115) by processes other than browser and OS components, review Sysmon Event ID 10 (ProcessAccess) and clipboard monitoring hooks. Look for unusual WebSocket traffic from browser processes to non-CDN external IPs. Search EDR telemetry for .NET assemblies loading XOR-decoded blobs from embedded resources and for processes invoking commercial packer artifacts. Check for anomalous browser cookie access outside normal browser process trees (T1539).
3. Eradication, No vendor patch applies; this is malware, not a software vulnerability. If infection is confirmed: isolate the host, revoke and rotate all browser-stored credentials and session tokens, invalidate active sessions on all services the user accessed from the affected endpoint, and notify affected SaaS providers to force re-authentication. Remove malware artifacts identified by EDR. Assume all clipboard-handled cryptocurrency addresses on the host since first infection are compromised.
4. Recovery, Validate credential revocation across all affected accounts. Re-image endpoints where infection is confirmed rather than attempting in-place cleanup given the obfuscation depth. Monitor previously affected accounts for unauthorized access for a minimum of 30 days post-remediation. Verify no persistence mechanisms (scheduled tasks, registry run keys) remain using T1053 and T1547 hunt queries.
5. Post-Incident, Assess whether browser credential storage policies are enforced (prohibit saving credentials in browsers on endpoints with privileged access). Evaluate clipboard monitoring controls and whether hardware or software crypto wallets with on-device address verification are feasible for employees handling crypto assets. Review detection coverage gap exposed by the zero-detection C2 IP, consider behavioral egress controls over reputation-only controls. Log this gap against NIST CSF DE.CM-1 (network monitoring) and DE.CM-7 (monitoring for unauthorized activity).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately if any confirmed outbound connection to 194.87.92.109 is correlated with browser cookie access or clipboard activity on endpoints with privileged access, cryptocurrency custody, or access to financial systems, OR if unauthorized cryptocurrency transactions are identified — both conditions trigger potential financial loss notification obligations and may require legal counsel engagement depending on jurisdictional breach notification thresholds.
Recovery Notes	Re-image all confirmed-infected endpoints rather than attempting in-place remediation — Gremlin Stealer's virtualized packing and XOR-decoded .NET loader obfuscation make artifact completeness unverifiable without full disk replacement. Force session invalidation and credential rotation on every service accessed from affected endpoints during the infection dwell window, with particular priority on cryptocurrency exchange accounts, financial institution portals, and any SaaS platforms with payment or PII access. Monitor all affected accounts for unauthorized access attempts, password reset requests, and session anomalies for a minimum of 30 days post-remediation, given that harvested session tokens may have been exfiltrated to the threat actor prior to C2 block and could be replayed from actor-controlled infrastructure.
Forensic Artifacts	Sysmon Event ID 10 (ProcessAccess) logs showing non-browser processes (anything outside chrome.exe, msedge.exe, brave.exe) calling OpenClipboard/GetClipboardData APIs — directly evidences Gremlin Stealer's real-time cryptocurrency address substitution via T1115 clipboard hijacking | Chromium SQLite databases at %LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies and Login Data — contents represent the exact credential and session token inventory exfiltrated by Gremlin Stealer's browser data harvesting module; Last Modified timestamps establish the theft window | Sysmon Event ID 3 (Network Connection) and Windows Firewall logs for outbound connections to 194.87.92.109 — establishes C2 beacon timing, dwell period, and which process (browser, injected .NET assembly, or wallet executable) was used as the egress vehicle | Process memory dump of any .NET process with unusual loaded modules — preserves XOR-decoded payload in cleartext in process heap/stack before deallocation, enabling YARA signature development and packer identification for the commercial virtualized packer used by this Gremlin Stealer variant | Windows Prefetch files at C:\Windows\Prefetch\ for unfamiliar executables with last-run timestamps during the suspected infection window — Gremlin Stealer's packed loader will appear as a distinct prefetch entry with a hash-appended name, providing execution proof and enabling timeline reconstruction independent of process creation logs that may have been cleared

Per-Action IR Details

Containment — Block the confirmed C2 IP 194.87.92[.]109 at perimeter firewall and DNS sinkholes immediately. Apply blocks across all egress-capable endpoints and network segments where Chromium-based browsers, Discord, or crypto wallets are present. Do not rely solely on VirusTotal reputation; this IP was clean at discovery.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), 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), CIS 13.4 (Perform Traffic Filtering Between Network Segments)

Compensating: On Windows hosts without enterprise firewall management, deploy the block via PowerShell: `New-NetFirewallRule -DisplayName 'Block Gremlin C2' -Direction Outbound -RemoteAddress 194.87.92.109 -Action Block`. For DNS sinkholing without enterprise DNS, add `194.87.92.109 gremlin-c2.invalid` to the Windows hosts file on each affected endpoint (`C:\Windows\System32\drivers\etc\hosts`). On a perimeter pfSense or OPNsense router,

add the IP to the Firewall > Aliases > Blocked list and apply a floating outbound rule. Validate block using `curl -v --connect-timeout 5 http://194.87.92.109` from an affected segment — expect a connection timeout.

Evidence: Before applying the block, capture a packet capture on the egress interface targeting 194.87.92.109 using Wireshark (`tshark -i -w gremlin_c2.pcap host 194.87.92.109`) to preserve any in-flight C2 beaconing or data exfiltration session already in progress. Extract Sysmon Event ID 3 (Network Connection) logs from affected hosts filtering on DestinationIp=194.87.92.109 to establish first-seen timestamps and which process (browser, wallet executable, or injected process) initiated the connection. Pull Windows Firewall logs (`C:\Windows\System32\LogFiles\Firewall\pfirewall.log`) for prior successful outbound connections to this IP to determine the dwell window before detection.

Detection — Query endpoint and network telemetry for outbound connections to 194.87.92[.]109. Hunt for clipboard API access (T1115) by processes other than browser and OS components — review Sysmon Event ID 10 (ProcessAccess) and clipboard monitoring hooks. Look for unusual WebSocket traffic from browser processes to non-CDN external IPs. Search EDR telemetry for .NET assemblies loading XOR-decoded blobs from embedded resources and for processes invoking commercial packer artifacts. Check for anomalous browser cookie access outside normal browser process trees (T1539).

NIST Phase: Detection Analysis

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

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), CIS 13.6 (Collect Network Traffic Flow Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config and enable Event ID 10 (ProcessAccess) with CallTrace targeting `OpenClipboard` and `GetClipboardData` API calls; filter for source processes outside `chrome.exe`, `msedge.exe`, `explorer.exe`, and `svchost.exe`. Use this PowerShell one-liner to query saved Sysmon logs for clipboard access anomalies: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 10 -and $_.Message -like '*Clipboard*' -and $_.Message -notlike '*chrome*' -and $_.Message -notlike '*explorer*'}`. For WebSocket detection without a SIEM, run Wireshark capture filtered on `tcp.port == 443 and websocket` and inspect TLS SNI values for non-CDN destinations originating from browser processes. To detect XOR-decoded .NET blob loading, deploy the open-source Sigma rule `proc_creation_win_dotnet_xor_loader.yml` against Sysmon logs using `sigma convert -t powershell`. Hunt Chromium cookie theft by monitoring file access to `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies` and `%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Cookies` from processes other than the browser itself using Sysmon Event ID 11 (FileCreate) and Event ID 10 (ProcessAccess).

Evidence: Capture memory from any suspicious .NET process before termination using ProcDump (`procdump.exe -ma gremlin_suspect.dmp`) to preserve XOR-decoded payload in process memory before it is deallocated. Export Sysmon Event ID 10 logs showing `GrantedAccess` to clipboard APIs (`0x001F019F` or `0x001FFFFF`) by non-browser processes. Extract browser process network activity from Chromium's NetLog by enabling it before the hunt (`chrome.exe --log-net-log=netlog.json --net-log-capture-mode=Everything`) to capture WebSocket upgrade handshakes to unknown external IPs. Collect the Chromium `Network Action Predictor` and `History` SQLite databases from `%LOCALAPPDATA%\Google\Chrome\User Data\Default\` to correlate which sites had active authenticated sessions during the infection window — these are the accounts requiring session revocation.

Eradication — No vendor patch applies; this is malware, not a software vulnerability. If infection is confirmed: isolate the host, revoke and rotate all browser-stored credentials and session tokens, invalidate active sessions on all services the user accessed from the affected endpoint, and notify affected SaaS providers to force re-authentication. Remove malware artifacts identified by EDR. Assume all clipboard-handled cryptocurrency addresses on the host since first infection are compromised.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST SI-3 (Malicious Code Protection), CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking

Process)

Compensating: Without an enterprise EDR, enumerate malware persistence manually: run `schtasks /query /fo LIST /v > schtasks_output.txt` and `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run > run_keys.txt` to identify Gremlin Stealer persistence entries. Scan the host with ClamAV using an updated signature database (`clamscan -r --bell -i C:\ --log=clamav_scan.log`) and supplement with a YARA scan targeting XOR-packed .NET assemblies — write a YARA rule matching the known XOR key pattern or packer artifact signature if published in the threat report. For session token revocation on Google accounts, instruct the user to navigate to `myaccount.google.com/security` > `Your devices` > sign out all sessions; for Discord, use `User Settings > Devices > Log Out All Known Devices`. For cryptocurrency address substitution: manually review clipboard history (if enabled via Windows 10+ Clipboard History, `Win+V`) for any crypto address modifications during the suspected infection window.

Evidence: Before isolating the host, image the full disk using FTK Imager or `dd` to preserve the malware binary, packed loader, and any dropped files for post-incident analysis. Export the browser's `Login Data` SQLite file from `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` (copy, do not open in Chrome) to document which credentials were stored and therefore must be treated as fully compromised. Capture the Windows Prefetch files from `C:\Windows\Prefetch\` for any unfamiliar executables with recent last-run timestamps — Gremlin Stealer's virtualized packer will appear as a distinct prefetch entry. Extract `%APPDATA%\Roaming\Microsoft\Windows\Recent\` LNK files to identify files the malware process accessed, including wallet data files and VPN configuration directories.

Recovery — Validate credential revocation across all affected accounts. Re-image endpoints where infection is confirmed rather than attempting in-place cleanup given the obfuscation depth. Monitor previously affected accounts for unauthorized access for a minimum of 30 days post-remediation. Verify no persistence mechanisms (scheduled tasks, registry run keys) remain using T1053 and T1547 hunt queries.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST IA-5 (Authenticator Management), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 4.1 (Establish and Maintain a Secure Configuration Process), CIS 6.1 (Establish an Access Granting Process)

Compensating: Re-image from a known-good baseline and validate OS integrity using DISM (`DISM /Online /Cleanup-Image /ScanHealth`) on the fresh image before returning to production. Post-reimaging, enforce browser credential storage policy via Group Policy (`User Configuration > Administrative Templates > Google > Google Chrome > Password Manager > Enable saving passwords to the password manager = Disabled`) or equivalent registry key `HKLM\SOFTWARE\Policies\Google\Chrome\PasswordManagerEnabled = 0` to prevent recurrence. For 30-day monitoring without a SIEM, configure Windows Event Forwarding to a central collector and set alerts on Event ID 4625 (Failed Logon) and Event ID 4648 (Logon Using Explicit Credentials) for the recovered accounts. Validate scheduled task cleanliness on the reimaged host by running `Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft\*'} | Select TaskName, TaskPath, State | Export-Csv schtasks_postimage.csv` and reviewing for any tasks not present in your baseline.

Evidence: Before re-imaging, preserve a full forensic disk image and export all relevant Windows Event Logs (`System`, `Security`, `Application`, and `Microsoft-Windows-Sysmon/Operational`) to an offline location for post-incident review. Capture and document the current state of all browser profile directories (`%LOCALAPPDATA%\\User Data\`) including `Cookies`, `Login Data`, `Web Data`, and `Local State` files — the `Local State` file contains the DPAPI-encrypted AES key used to protect Chromium cookies, and its compromise confirms the scope of session token theft. Record cryptocurrency wallet transaction logs and blockchain addresses used from the affected host during the infection window to identify any unauthorized transfers initiated via Gremlin Stealer's real-time address substitution capability.

Post-Incident — Assess whether browser credential storage policies are enforced (prohibit saving credentials in browsers on endpoints with privileged access). Evaluate clipboard monitoring controls and whether hardware or software crypto wallets with on-device address verification are feasible for employees handling crypto assets. Review detection coverage gap exposed by the zero-detection C2 IP — consider behavioral egress controls over reputation-only controls. Log this gap against NIST CSF DE.CM-1 (network monitoring)

and DE.CM-7 (monitoring for unauthorized activity).

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 SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Document the detection gap formally: the C2 IP 194.87.92.109 had zero VirusTotal detections at discovery, which invalidates reputation-only egress controls as a primary detection mechanism for Gremlin Stealer campaigns. Implement behavioral egress controls using free tooling: deploy Zeek (formerly Bro) on the network perimeter to alert on low-volume periodic outbound connections to single IPs on ports 80/443 that do not match known CDN ASNs — this catches the C2 beaconing pattern regardless of IP reputation. Draft a policy prohibiting browser-based credential storage on endpoints with access to financial systems or cryptocurrency, enforced via the registry keys documented in Recovery. Convert this incident's Sysmon-based detections into permanent Sigma rules (`clipboard_abuse_non_browser.yml`, `chromium_cookie_access_outside_browser.yml`) and add to your detection library. Submit the C2 IP and any malware hashes to CISA's automated indicator sharing (AIS) program to contribute to community defense.

Evidence: Compile the full incident timeline from first Sysmon Event ID 3 connection to 194.87.92.109 through confirmed eradication, using Windows Security Event Log Event ID 4688 (Process Creation) and Sysmon Event IDs 1 (Process Create), 3 (Network Connection), and 10 (ProcessAccess) to reconstruct the attack chain. Document which browser-stored credentials, session cookies, and clipboard-handled cryptocurrency addresses were exposed during the dwell window — this constitutes the scope of the breach for any required notification assessment. Retain all forensic disk images, memory captures, packet captures, and log exports for a minimum of 12 months per NIST AU-11 (Audit Record Retention) in case of regulatory inquiry or follow-on litigation related to financial losses from crypto theft.

Detection Guidance

Primary behavioral indicators: (1) Outbound connections to 194.87.92[.]109, query firewall, proxy, and DNS logs for this IP. (2) Clipboard API access (ReadClipboardData/SetClipboardData) invoked by non-browser, non-OS processes, Sysmon Event ID 10 or equivalent EDR process access telemetry. (3) WebSocket connections established from browser child processes to external IPs outside known CDN/SaaS ranges, particularly relevant for detecting session hijacking module (T1185). (4) .NET processes loading embedded resources and performing XOR decode operations at runtime, flag in memory-scanning or behavioral EDR rules. (5) Browser credential store (Login Data, Cookies) file access outside normal browser process context, Sysmon Event ID 11 (FileCreate) or file access telemetry on %LOCALAPPDATA%\Google\Chrome\User Data and equivalent Chromium paths. (6) Anomalous child processes spawned from browser instances or Discord. MITRE techniques to prioritize in detection rules: T1115 (Clipboard Data), T1539 (Steal Web Session Cookie), T1185 (Browser Session Hijacking), T1027.009 (Obfuscated Files, Embedded Payloads). Note: The identified C2 IP had zero VirusTotal detections at initial discovery; reputation-based blocking alone is insufficient. Behavioral and network flow analysis are the primary detection layers.

Indicators of Compromise

Type	Value	Context	Confidence
IP	`194.87.92[.]109`	Newly identified Gremlin Stealer C2 server. Zero VirusTotal detections at time of discovery per Unit 42 reporting. Defang brackets included — remove for blocking.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1497** — Virtualization/Sandbox Evasion
- **T1566** — Phishing
- **T1059.005** — Visual Basic
- **T1071.001** — Web Protocols
- **T1115** — Clipboard Data
- **T1027** — Obfuscated Files or Information
- **T1555.003** — Credentials from Web Browsers
- **T1185** — Browser Session Hijacking
- **T1539** — Steal Web Session Cookie
- **T1027.009** — Embedded Payloads
- **T1140** — Deobfuscate/Decode Files or Information
- **T1041** — Exfiltration Over C2 Channel
- **T1555** — Credentials from Password Stores
- **T1583.003** — Virtual Private Server
- **T1622** — Debugger Evasion

NIST-800-53R5

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1566	Phishing	Initial-Access
T1059.005	Visual Basic	Execution
T1071.001	Web Protocols	Command-And-Control
T1115	Clipboard Data	Collection
T1027	Obfuscated Files or Information	Defense-Evasion
T1555.003	Credentials from Web Browsers	Credential-Access
T1185	Browser Session Hijacking	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1027.009	Embedded Payloads	Defense-Evasion
T1140	Deobfuscate/Decode Files or Information	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1555	Credentials from Password Stores	Credential-Access
T1583.003	Virtual Private Server	Resource-Development
T1622	Debugger Evasion	Defense-Evasion

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/gremlin-stealer-evolution/	T3
	https://unit42.paloaltonetworks.com/new-malware-gremlin-stealer-for...	T3

Source	URL	Tier
	https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/	T3
	https://unit42.paloaltonetworks.com/qr-codes-as-attack-vector/	T3
Advanced Threat Prevention - Palo Alto Networks	https://www.paloaltonetworks.com/network-security/advanced-threat-p...	T3

Generated 2026-05-16 06:38 UTC by TJS Security Command Center