INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-12 18:51 UTC

OnyxC2 Malware-as-a-Service Targets 210+ Applications with Advanced Data Theft Capabilities

THREAT CAMPAIGN | **HIGH** | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0448
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	210+ applications and browser extensions (Windows environments); specific application list unverified without primary source access
Published	2026-06-11
Discovery Source	Gemini

Executive Summary

OnyxC2 is a newly identified Malware-as-a-Service platform available on criminal underground markets for approximately $250 per month, targeting credentials and session data across 210+ applications and browser extensions in Windows environments. The subscription model puts enterprise-grade infostealing and covert remote access capabilities within reach of low-skill threat actors, significantly broadening the potential attacker pool. Organizations with credential-rich endpoints, browser-based workflows, or inadequate endpoint detection controls face meaningful risk of credential compromise and unauthorized system access.

Technical Analysis

OnyxC2 is a MaaS infostealer and remote access platform targeting Windows environments. Reported capabilities include Hidden Virtual Network Computing (HVNC) for covert interactive remote sessions, DLL sideloading (CWE-427, MITRE T1574.002) for defense evasion by hijacking legitimate application load order, encrypted payload delivery (CWE-326, CWE-506) to bypass endpoint detection, credential harvesting from 210+ applications and browser extensions (T1555, T1539), keylogging (T1056), and C2 communication over standard protocols (T1071). Process injection techniques (T1055) and obfuscation (T1027) are also reported. No CVE identifier is associated with this campaign. The MaaS delivery model (T1219 for remote access tooling) means payloads are operator-customized at purchase. Full technical IOCs and a complete application target list could not be independently verified from primary research sources at time of writing; current sources are based

on secondary and tertiary news reporting from vendor blogs and security news outlets.

Action Checklist

1. Step 1: Containment. Audit endpoints for suspicious DLL sideloading activity in application directories; isolate any host exhibiting unexpected outbound encrypted connections to unknown infrastructure. Restrict lateral movement by enforcing least privilege per NIST AC-6 and limiting remote access sessions per NIST AC-12. Apply CIS 4.4 and CIS 4.5 to ensure host and server firewalls block unsanctioned outbound ports used for HVNC and C2 traffic.
2. Step 2: Detection. Review endpoint detection logs for DLL load order hijacking events (T1574.002), unexpected parent-child process relationships indicative of process injection (T1055), and HVNC-related VNC protocol traffic on non-standard ports. Enable and review audit logs per NIST AU-2 and AU-12 for credential access events across browser processes and application credential stores (T1555, T1539). Query for unsigned or anomalously named DLLs loaded by trusted executables. See detection_guidance field for additional behavioral indicators.
3. Step 3: Eradication. There is no vendor patch for this campaign; eradication depends on removing malicious binaries and restoring clean application states. Rotate all credentials harvested by affected applications and browser sessions per D3-CRO. Remove unauthorized DLLs identified in sideloading investigation. Validate software integrity against known-good hashes per D3-FMBV (file magic byte verification) and D3-SFA (system file analysis). Enforce CIS 2.3 to address unauthorized software present on compromised endpoints.
4. Step 4: Recovery. Verify clean state by re-imaging affected endpoints where feasible, or performing thorough forensic validation of DLL directories and credential stores. Re-enable services only after confirming no residual C2 beaconing. Monitor for re-infection attempts by reviewing outbound encrypted traffic patterns per NIST SI-4 (system monitoring). Confirm MFA is enforced on all accounts whose credentials may have been harvested, per CIS 6.3, CIS 6.4, and CIS 6.5.
5. Step 5: Post-Incident. Assess control gaps this campaign exposed: DLL search order hardening, endpoint detection rule coverage for HVNC and sideloading, and browser credential store protections. Review account inventory per CIS 5.1 and disable dormant accounts per CIS 5.3. Document lessons learned in the incident response playbook. Evaluate whether endpoint detection tooling currently covers T1574.002 and T1055 behavioral signatures. Improve audit log coverage per NIST AU-6 to ensure credential access events are reviewed at defined frequencies.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if forensic evidence confirms credential theft from accounts with access to PII, PHI, or financial data, as OnyxC2's targeting of 210+ applications makes regulated-data exposure highly probable and may trigger breach notification obligations under GDPR, HIPAA, or state privacy statutes; escalate to IR retainer or external DFIR firm if HVNC traffic confirms an active remote operator session, indicating hands-on-keyboard activity beyond automated infostealing.

Recovery Notes	Re-image affected endpoints rather than attempting in-place remediation wherever operationally feasible, as OnyxC2's MaaS architecture may include persistence mechanisms beyond the identified sideloaded DLL that are difficult to enumerate without full memory forensics. Monitor all accounts confirmed or suspected to have had credentials harvested for at least 90 days post-incident, specifically watching for authentication from new geolocations, new device fingerprints, or unusual access-time patterns that indicate adversary use of stolen session tokens that survived credential rotation. Maintain enhanced outbound traffic monitoring (Wireshark captures or firewall flow logs reviewed daily) on all recovered endpoints for a minimum of 30 days to detect OnyxC2 re-infection attempts, which are operationally trivial for a $250/month MaaS subscriber to retry against the same target.
Forensic Artifacts	Sideloaded OnyxC2 DLL files in user-writable application subdirectories (e.g., %APPDATA%, %LOCALAPPDATA%, or application install directories with misconfigured ACLs) — hash and preserve with full NTFS metadata (created, modified, accessed, MFT entry timestamps) to establish campaign deployment timeline | Browser credential store files accessed by OnyxC2: Chrome and Edge '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data' and '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data' (SQLite databases), Firefox '%APPDATA%\Mozilla\Firefox\Profiles*.default\key4.db' and 'logins.json' — forensic copies document the scope of credential theft and support breach notification assessment | Windows Prefetch files at 'C:\Windows\Prefetch\' for the OnyxC2 loader executable and any spawned child processes — prefetch entries record up to 8 seconds of file system references at process launch, revealing additional components or configuration files loaded by OnyxC2 that may not appear in live process inspection | DPAPI master key usage events in Windows Security Event Log (Event ID 4693 — Credential Manager credentials were backed up/restored, Event ID 4694) correlated with browser process activity timestamps — OnyxC2's browser credential harvesting requires DPAPI decryption using the logged-on user's key, leaving an auditable trail if Security audit policy includes 'Audit Other Account Logon Events' | Network flow records or Wireshark PCAP captures of outbound encrypted sessions from compromised hosts on non-standard ports, preserving the OnyxC2 C2 beacon pattern (connection interval, packet size distribution, destination IP/ASN) and any HVNC session traffic that can be used to fingerprint the specific MaaS infrastructure variant and support attribution or infrastructure takedown reporting to CISA or FBI IC3

Per-Action IR Details

Step 1: Containment — Audit endpoints for suspicious DLL sideloading activity in application directories; isolate any host exhibiting unexpected outbound encrypted connections to unknown infrastructure. Restrict lateral movement by enforcing least privilege per NIST AC-6 and limiting remote access sessions per NIST AC-12. Apply CIS 4.4 and CIS 4.5 to ensure host and server firewalls block unsanctioned outbound ports used for HVNC and C2 traffic.

NIST Phase: Containment

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

Controls: NIST AC-6 (Least Privilege), NIST AC-12 (Session Termination), 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)

Compensating: Run Sysinternals Autoruns and Process Monitor on suspected hosts to identify DLLs loading from non-standard application subdirectories (e.g., user-writable %APPDATA% or %TEMP% paths). Use Wireshark or Windows Firewall logging (netsh advfirewall set allprofiles logging droppedconnections enable) to capture and review outbound encrypted sessions on non-standard ports. Script a PowerShell firewall rule to block outbound traffic on all ports except 80/443/53 from endpoints pending investigation: New-NetFirewallRule -DisplayName 'OnyxC2-Quarantine' -Direction Outbound -Action Block -Protocol TCP -RemotePort 1-79,81-442,444-52,54-65535.

Evidence: BEFORE isolating any host, capture: (1) full RAM image using WinPmem or Magnet RAM Capture to preserve in-memory OnyxC2 payload, injected shellcode, and decrypted C2 configuration; (2) active network connections via 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}' and 'netstat -ano' to record live C2 beacon destinations and HVNC session ports; (3) running process list with parent-child relationships via 'Get-WmiObject Win32_Process | Select ProcessId,ParentProcessId,Name,CommandLine' to capture injected process trees before termination; (4) list of loaded DLLs per process via 'Get-Process | ForEach-Object { $_.Modules }' or Sysinternals Listdlls to identify the sideloaded OnyxC2 DLL before host isolation destroys live state.

Step 2: Detection — Review endpoint detection logs for DLL load order hijacking events (T1574.002), unexpected parent-child process relationships indicative of process injection (T1055), and HVNC-related VNC protocol traffic on non-standard ports. Enable and review audit logs per NIST AU-2 and AU-12 for credential access events across browser processes and application credential stores (T1555, T1539). Query for unsigned or anomalously named DLLs loaded by trusted executables. See detection_guidance field for additional behavioral indicators.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a configuration targeting Event ID 7 (ImageLoaded) filtered for unsigned DLLs loading from %APPDATA%, %TEMP%, or application subdirectories writable by standard users — these are the directories OnyxC2 exploits for sideloading. Write a Sigma rule matching Sysmon Event ID 10 (ProcessAccess) where TargetImage contains browser processes (chrome.exe, msedge.exe, firefox.exe) and SourceImage is an unexpected parent, indicating credential store access. Use osquery query 'SELECT name, path, pid FROM processes WHERE name IN (SELECT name FROM processes) AND on_disk = 0;' to surface injected or memory-resident OnyxC2 components with no backing file on disk.

Evidence: Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on browser child processes (e.g., chrome.exe spawning cmd.exe or powershell.exe) that indicate OnyxC2 credential harvesting activity. Review Sysmon Event ID 3 (Network Connection) for outbound connections from browser processes or injected hosts to non-categorized IPs on non-standard ports consistent with OnyxC2 C2 or HVNC sessions. Check %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data and equivalent paths for Firefox (key4.db, logins.json) and Edge (Login Data) for signs of programmatic read access in filesystem audit logs (Security Event ID 4663). Review DPAPI audit events (Security Event ID 4693) which OnyxC2 would trigger when decrypting browser-stored credentials using the victim user's DPAPI master key.

Step 3: Eradication — There is no vendor patch for this campaign; eradication depends on removing malicious binaries and restoring clean application states. Rotate all credentials harvested by affected applications and browser sessions per D3-CRO. Remove unauthorized DLLs identified in sideloading investigation. Validate software integrity against known-good hashes per D3-FMBV (file magic byte verification) and D3-SFA (system file analysis). Enforce CIS 2.3 to address unauthorized software present on compromised endpoints.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: CIS 2.3 (Address Unauthorized Software), CIS 2.1 (Establish and Maintain a Software Inventory), NIST AC-2 (Account Management)

Compensating: Use PowerShell to enumerate and hash all DLLs in application directories against a known-good baseline: 'Get-ChildItem -Path "C:\Program Files" -Recurse -Filter *.dll | Get-FileHash -Algorithm SHA256 | Export-Csv dll_audit.csv'. Compare output against vendor-provided or CIS benchmark hash lists to identify OnyxC2 sideloaded DLLs that replaced or shadow legitimate libraries. Use ClamAV with an updated signature set and any available YARA rules matching OnyxC2 behavioral patterns (MaaS stealers frequently share packer or string signatures with prior families) to scan %APPDATA%, %TEMP%, and application subdirectories. For credential rotation, prioritize accounts accessed by the 210+ targeted applications — enumerate these via browser saved-password export and application

config files before deleting them, so the rotation list is complete.

Evidence: BEFORE removing any DLL or binary, preserve: (1) full file system copies of the malicious DLLs with metadata intact (creation timestamp, last-modified, last-accessed) using robocopy /COPYALL to a write-once evidence share — OnyxC2 DLL timestamps may reveal campaign deployment timing; (2) registry export of HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs and HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs to document any persistence mechanism planted alongside sideloading; (3) prefetch files from C:\Windows\Prefetch for the malicious executable and sideloaded DLL (e.g., MALICIOUS.EXE-XXXXXXXX.pf) which record execution timestamps and referenced file paths useful for timeline reconstruction; (4) browser credential store files (Chrome Login Data, Firefox key4.db/logins.json, Edge Login Data) in read-only forensic copy BEFORE credential rotation to document the scope of likely credential theft.

Step 4: Recovery — Verify clean state by re-imaging affected endpoints where feasible, or performing thorough forensic validation of DLL directories and credential stores. Re-enable services only after confirming no residual C2 beaconing. Monitor for re-infection attempts by reviewing outbound encrypted traffic patterns per NIST SI-4 (system monitoring). Confirm MFA is enforced on all accounts whose credentials may have been harvested, per CIS 6.3, CIS 6.4, and CIS 6.5.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: 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-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Before returning a recovered endpoint to production, run a Sigma rule sweep against collected Sysmon logs for the prior 30 days to confirm no OnyxC2 sideloading or HVNC beacon pattern recurs post-remediation. Use Wireshark or Windows Firewall logs to monitor outbound encrypted traffic from restored hosts for 14 days, flagging any session to IP ranges that did not exist in the pre-incident baseline. For MFA enforcement on accounts without enterprise IAM tooling, use Microsoft's free Authenticator App enforced via Conditional Access free-tier policies, or for on-premise environments, configure NPS with RADIUS-based MFA using Duo's free tier for up to 10 users.

Evidence: Before re-enabling any service or returning a host to the network, confirm: (1) no established or listening connections on ports previously used for OnyxC2 HVNC sessions by running 'Get-NetTCPConnection | Where-Object {$_.State -in @("Established","Listen")}' and cross-referencing against the C2 IP list documented during initial volatile capture; (2) re-hash all DLLs in application directories and compare against the clean baseline established during eradication to detect any re-planted sideloading component; (3) verify Windows Defender or installed AV definitions are current and a full scan completes clean before the host is returned to production. These checks must be documented with timestamps for post-incident audit evidence.

Step 5: Post-Incident — Assess control gaps this campaign exposed: DLL search order hardening, endpoint detection rule coverage for HVNC and sideloading, and browser credential store protections. Review account inventory per CIS 5.1 and disable dormant accounts per CIS 5.3. Document lessons learned in the incident response playbook. Evaluate whether endpoint detection tooling currently covers T1574.002 and T1055 behavioral signatures. Improve audit log coverage per NIST AU-6 to ensure credential access events are reviewed at defined frequencies.

NIST Phase: Post Incident

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

Controls: CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Harden DLL search order for high-value applications (browsers, Office, credential managers) by setting the SafeDllSearchMode registry key (HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode = 1) and auditing application directories for world-writable permissions using 'icacls C:\Program Files /T /Q' — any directory writable by standard users is an OnyxC2 sideloading candidate. Author a Sysmon + Sigma detection rule for the specific OnyxC2 behavioral pattern: unsigned DLL loaded by a browser or

productivity application from a user-writable path, combined with a subsequent outbound connection from the same process. Submit IOCs (DLL hashes, C2 IPs/domains collected during incident) to MISP or a shared threat intel platform to benefit peer organizations facing the same MaaS subscription campaign.

Evidence: Preserve the complete incident evidence package for post-incident review and potential regulatory disclosure: (1) all volatile captures from Steps 1-4 retained per NIST AU-11 (Audit Record Retention) requirements for your jurisdiction and sector; (2) timeline reconstruction artifact showing first-seen OnyxC2 DLL timestamp, first C2 beacon, and credential access events correlated across Sysmon, Windows Security, and browser logs; (3) full list of accounts and applications confirmed or suspected to have had credentials harvested by OnyxC2, which forms the basis for breach notification assessment if PII or regulated data was accessible through those credentials; (4) documented gap analysis identifying which DLL directories lacked integrity monitoring and which accounts lacked MFA at time of compromise, to drive measurable playbook improvements.

Detection Guidance

Focus detection on four behavioral clusters tied to OnyxC2's reported techniques. First, DLL sideloading (T1574.002): alert on DLLs loaded from user-writable directories by signed, trusted executables; look for DLL names matching known legitimate system DLLs appearing in application working directories rather than system32. Second, process injection (T1055): monitor for unexpected memory write operations across process boundaries and CreateRemoteThread or NtMapViewOfSection API calls originating from browser or common application processes. Third, HVNC activity (T1219): flag VNC protocol traffic, especially on non-standard ports, and look for hidden desktop object creation in Windows session logs. Fourth, credential harvesting (T1555, T1539): monitor for unusual read access to browser profile directories (e.g., Login Data, Cookies files in Chromium-based browser paths), application credential vaults, and Windows Credential Manager. Also alert on C2 beacon patterns (T1071): high-frequency, low-volume encrypted outbound connections to newly registered or low-reputation domains. NIST AU-2 and AU-12 require these event types to be logged; confirm logging is active for process creation, DLL load, network connection, and file access events. D3-LAM (local account monitoring) and D3-SFA (system file analysis) are applicable countermeasures. Note: specific IOC values (hashes, IPs, domains) are not confirmed from primary sources; behavioral detections are the most reliable approach given current source quality.

Framework Mappings

MITRE-ATTACK

- **T1055** — Process Injection
- **T1574.002** — DLL Side-Loading
- **T1539** — Steal Web Session Cookie
- **T1219** — Remote Access Tools
- **T1555** — Credentials from Password Stores
- **T1027** — Obfuscated Files or Information
- **T1056** — Input Capture
- **T1071** — Application Layer Protocol

NIST-800-53R5

- **AC-6** — Least Privilege

- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-13** — Cryptographic Protection

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission Security

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1055	Process Injection	Defense-Evasion
T1574.002	DLL Side-Loading	Persistence
T1539	Steal Web Session Cookie	Credential-Access
T1219	Remote Access Tools	Command-And-Control
T1555	Credentials from Password Stores	Credential-Access
T1027	Obfuscated Files or Information	Defense-Evasion
T1056	Input Capture	Collection
T1071	Application Layer Protocol	Command-And-Control

Sources

Source	URL	Tier
gemini	https://securityaffairs.com/173358/malware/onyxc2-malware-as-a-serv...	T3

Source	URL	Tier
OnyxC2 Malware-as-a-Service Offers Enterprise-Grade Data Theft	https://securityaffairs.com/193523/malware/onyxc2-malware-as-a-serv...	T3
OnyxC2 Stealer Offers Cybercriminals Enterprise-Grade Theft for ...	https://www.securityweek.com/onyxc2-stealer-offers-cybercriminals-e...	T3
OnyxC2 MaaS Stealer Targets 210+ Apps With HVNC and DLL ...	https://www.mallory.ai/stories/019eb739-1a43-7499-8cd0-3bed31ec92d0	T3
A sophisticated new threat just hit the underground market. OnyxC2 ...	https://www.instagram.com/p/DZcxVwcnLRU/	T3

Generated 2026-06-12 18:51 UTC by TJS Security Command Center