INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 19:02 UTC

OXLOADER Delivers CastleStealer Through Poisoned Google Ads in Financially Motivated Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0539
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	End users exposed to Google Ads platform; no specific enterprise software products affected, attack targets users via malvertising delivery chain
Published	2026-06-22T09:20:12
Discovery Source	Rss

Executive Summary

Elastic Security Labs has identified an active malvertising campaign deploying a new malware loader, OXLOADER, through poisoned Google Ads to deliver the CastleStealer infostealer. The campaign is sector-agnostic, targeting any user who encounters the malicious advertisements, with a likely Russian-speaking, financially motivated threat actor behind it. The primary business risk is credential theft and financial data exfiltration affecting employees who browse the web using corporate or personal devices, bypassing perimeter defenses entirely.

Technical Analysis

OXLOADER is a previously undocumented staged loader delivered via malicious Google Ads (malvertising). It functions as a trojanized software installer, downloading and executing CastleStealer, an infostealer focused on credential harvesting and financial data exfiltration. The loader exhibits CWE-494 (Download of Code Without Integrity Check) and CWE-506 (Embedded Malicious Code) characteristics. The delivery chain abuses the Google Ads platform to bypass network perimeter controls, as traffic originates from a legitimate advertising network. MITRE ATT&CK techniques involved include T1566/T1566.002 (Phishing/Spearphishing Link), T1204.001/T1204.002 (User Execution), T1105 (Ingress Tool Transfer), T1055 (Process Injection), T1552 (Unsecured Credentials), T1555 (Credentials from Password Stores), T1539 (Steal Web Session Cookie), and T1041 (Exfiltration over C2 Channel). Attribution is assessed by Elastic Security Labs as a likely Russian-speaking, financially motivated actor; no formal group designation has been assigned. No CVE

identifiers are associated with this campaign. There is no vendor patch, this is a delivery-chain and user-behavior problem, not a software vulnerability.

Action Checklist

1. Step 1: Containment. Block known OXLOADER and CastleStealer infrastructure at the DNS and proxy layer immediately. Deploy DNS filtering (e.g., Cisco Umbrella, Infoblox) to block domains identified in Elastic Security Labs reporting. Enforce web proxy policies to flag or block ad-network redirects to executable downloads. Apply CIS Controls v8 4.4 and 4.5 (host and server firewall management) to restrict outbound connections from endpoints to unexpected destinations.
2. Step 2: Detection. Query endpoint detection telemetry and SIEM for: process execution chains spawned from browser processes (T1204.001/T1204.002), unsigned or low-prevalence executables dropped in user temp directories, outbound connections to newly registered or low-reputation domains following ad-click events, and credential store access events outside normal application behavior (T1555, T1552). Review proxy logs for HTTP/S GET requests to ad-redirect chains terminating in executable file downloads. Apply NIST AU-6 (Audit Record Review) and AU-12 (Audit Record Generation) to ensure browser process and file-write events are captured. Use MITRE D3FEND D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to surface anomalous credential store access.
3. Step 3: Eradication. There is no vendor patch for this campaign. Eradication requires: (1) isolating any endpoints where OXLOADER or CastleStealer execution is confirmed; (2) reimaging affected systems rather than attempting manual cleanup given process injection capability (T1055); (3) revoking and rotating all credentials stored in browsers or password managers on affected endpoints per D3FEND D3-CRO (Credential Rotation); (4) invalidating active web session tokens per T1539 exposure. Apply CIS Controls v8 7.1 and 7.2 (Vulnerability Management and Remediation Process) as the governing framework for tracking remediation status across affected assets.
4. Step 4: Recovery. Before returning endpoints to production: verify no persistence mechanisms remain via registry run keys, scheduled tasks, or startup folder entries (D3FEND D3-SICA, System Init Config Analysis); confirm credential rotation is complete for all accounts accessible from affected devices; re-enable endpoint protection with updated signatures for OXLOADER/CastleStealer; monitor reinstated endpoints for 72 hours using enhanced logging. Apply NIST AU-6 review cadence post-recovery to catch reinfection indicators.
5. Step 5: Post-Incident. This campaign exposes gaps in user execution controls and browser-based threat visibility. Immediate control improvements: enforce application allowlisting to prevent unsigned executables from running (CIS Controls v8 2.3, Address Unauthorized Software); deploy or tune DNS-layer filtering for malvertising redirect chains; implement DNS monitoring per NIST AU-2 (Event Logging) to capture ad-network redirects; review and enforce MFA across all corporate accounts to limit credential-theft blast radius (CIS Controls v8 6.3, 6.4, 6.5, MFA requirements); conduct targeted user awareness communication on malvertising risks distinct from standard phishing training.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership and legal/compliance if forensic analysis of the Chrome Login Data artifact or memory image confirms CastleStealer successfully exfiltrated credentials for systems processing PII, PHI, or financial data, as this may trigger breach notification obligations under applicable regulations (GDPR, HIPAA, state data breach statutes); also escalate if more than five endpoints show confirmed OXLOADER execution, indicating campaign-scale exposure rather than isolated incident.
Recovery Notes	Before reinstating any affected endpoint, confirm via Autoruns baseline diff and YARA scan that no OXLOADER persistence mechanisms survive the reimage, and verify through each affected SaaS provider's session management console that all active sessions originating from the compromised endpoint have been terminated. Monitor reinstated endpoints for a minimum of 72 hours post-recovery using enhanced Sysmon logging focused on browser child-process spawning and writes to temp directories, as financially motivated actors behind campaigns of this type have been observed re-targeting recently cleaned endpoints via the same malvertising delivery chain. Treat any recurrence of suspicious browser-spawned execution on a recovered endpoint as a new incident rather than a reinfection, and re-initiate triage from the detection phase.
Forensic Artifacts	Browser SQLite credential stores on affected endpoints: Chrome `%APPDATA%\Local\Google\Chrome\User Data\Default\Login Data`, Firefox `%APPDATA%\Roaming\Mozilla\Firefox\Profiles\*.default\logins.json`, and Edge `%APPDATA%\Local\Microsoft\Edge\User Data\Default\Login Data` — CastleStealer specifically targets these files to harvest stored usernames and passwords, and their last-accessed timestamps confirm whether exfiltration occurred. | Windows Prefetch files at `C:\Windows\Prefetch\` for OXLOADER and CastleStealer executable names — Prefetch entries (parsed with WinPrefetchView or PECmd) provide execution timestamps, run count, and the directory path from which the malicious executable was launched, confirming the user temp directory delivery path. | Web proxy and DNS resolver logs covering the 24-hour window prior to confirmed OXLOADER execution — the full HTTP redirect chain from the poisoned Google Ad click through the intermediate ad-network redirect to the OXLOADER staging domain and executable download URI is the primary delivery-chain evidence and must be preserved before log rotation. | RAM image from any endpoint with confirmed OXLOADER execution — given CastleStealer's delivery via a loader with process injection capability, injected code and decrypted payload artifacts will exist only in memory and will not appear on disk; Volatility3 `windows.pstree` and `windows.malfind` plugins applied to this image will identify hollow or injected processes. | Sysmon Event ID 1 (Process Create) logs from affected endpoints filtered for browser parent processes (chrome.exe, msedge.exe, firefox.exe) spawning unexpected child processes — this execution chain is the definitive host-based indicator of OXLOADER being launched via the malvertising delivery mechanism rather than a legitimate browser extension or update process.

Per-Action IR Details

Step 1: Containment — Block known OXLOADER and CastleStealer infrastructure at the DNS and proxy layer immediately. Deploy DNS filtering (e.g., Cisco Umbrella, Infoblox) to block domains identified in Elastic Security Labs reporting. Enforce web proxy policies to flag or block ad-network redirects to executable downloads. Apply CIS 4.4 and CIS 4.5 (host and server firewall management) to restrict outbound connections from endpoints to unexpected destinations.

NIST Phase: Containment

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

Controls: CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), NIST AC-4 (Information Flow Enforcement)

Compensating: For teams without Umbrella or Infoblox: configure RPZ (Response Policy Zones) on an internal BIND or Windows DNS server to sinkhole OXLOADER C2 and staging domains from the Elastic Security Labs IOC list. On endpoints, use Windows Firewall with Advanced Security (`netsh advfirewall firewall add rule`) to block outbound connections to identified IP ranges. Deploy a Pi-hole instance on the network segment as an immediate DNS-layer block with zero licensing cost.

Evidence: Before pushing DNS block rules or proxy policy changes that would sever active C2 communications: capture full packet captures (Wireshark/tcpdump) of any endpoint exhibiting suspicious outbound DNS queries or HTTP/S connections to ad-redirect chains. Export current DNS query logs from your resolver showing domains queried by endpoints in the hours preceding this containment action — these short-lived OXLOADER staging domains rotate and the DNS query history is the only record. Capture proxy access logs showing the full redirect chain from the malicious Google Ad click through to the executable download URI before overwriting or rotating those logs.

Step 2: Detection — Query endpoint detection telemetry and SIEM for: process execution chains spawned from browser processes (T1204.001/T1204.002), unsigned or low-prevalence executables dropped in user temp directories, outbound connections to newly registered or low-reputation domains following ad-click events, and credential store access events outside normal application behavior (T1555, T1552). Review proxy logs for HTTP/S GET requests to ad-redirect chains terminating in executable file downloads. Apply NIST AU-6 (Audit Record Review) and AU-12 (Audit Record Generation) to ensure browser process and file-write events are captured. Use D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to surface anomalous credential store access.

NIST Phase: Detection Analysis

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

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

Compensating: Without a SIEM: deploy Sysmon with a configuration tuned to log Event ID 1 (Process Create) and Event ID 11 (File Created) — filter specifically for browser processes (chrome.exe, msedge.exe, firefox.exe) spawning child processes or writing executables to `%APPDATA%\Local\Temp`, `%TEMP%`, or `%USERPROFILE%\Downloads`. Use this PowerShell one-liner to query Sysmon logs: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object { $_.Id -eq 1 -and $_.Message -match 'chrome.exe|msedge.exe|firefox.exe' } | Select-Object TimeCreated, Message`. For credential store access, query Windows Security Event Log for Event ID 4663 (Object Access) against `%APPDATA%\Local\Google\Chrome\User Data\Default\Login Data` and equivalent Firefox/Edge profile paths.

Evidence: This is a detection/analysis step that does not alter live state, so volatile capture is concurrent rather than prerequisite. However, if an endpoint is identified as actively executing OXLOADER or CastleStealer during this query phase, do NOT proceed to further analysis steps without first capturing: running process list (`tasklist /v` or Sysmon Event ID 1 history), active network connections (`netstat -ano` or `Get-NetTCPConnection`), and a listing of files written to `%TEMP%` and `%APPDATA%` in the last 24 hours (`Get-ChildItem -Path $env:TEMP -Force | Sort-Object LastWriteTime -Descending`). These artifacts will be destroyed by any subsequent containment or eradication action.

Step 3: Eradication — There is no vendor patch for this campaign. Eradication requires: (1) isolating any endpoints where OXLOADER or CastleStealer execution is confirmed; (2) reimaging affected systems rather than attempting manual cleanup given process injection capability (T1055); (3) revoking and rotating all credentials stored in browsers or password managers on affected endpoints per D3-CRO (Credential Rotation); (4) invalidating active web session tokens per T1539 exposure. Apply CIS 7.1 and CIS 7.2 (Vulnerability Management and Remediation Process) as the governing framework for tracking remediation status across affected assets.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential rotation without enterprise PAM tooling: generate a prioritized list of credentials at risk by parsing the Chrome `Login Data` SQLite database (if readable pre-reimage) using `sqlite3 'Login Data' 'SELECT origin_url, username_value FROM logins;'` — this identifies exactly which services need forced password resets. For session token invalidation, use each affected service's self-service 'sign out all sessions' function (Google Account, Microsoft Account, corporate SSO) immediately. Document all rotated accounts in a shared incident tracker to confirm 100% coverage before closing the eradication phase.

Evidence: CRITICAL — volatile evidence must be captured BEFORE isolation, reimaging, or credential rotation. Before isolating the endpoint: acquire a full RAM image using WinPmem or Magnet RAM Capture to preserve injected OXLOADER code from any process it has hollowed or injected into (process injection means disk artifacts alone are insufficient). Capture `Get-NetTCPConnection` and `netstat -ano` output to document active C2 channels. Before reimaging: image the full disk or at minimum copy `%TEMP%`, `%APPDATA%\Roaming`, `%APPDATA%\Local\Temp`, browser profile directories (`%APPDATA%\Local\Google\Chrome\User Data\Default\`), and Windows Prefetch (`C:\Windows\Prefetch`) to capture OXLOADER and CastleStealer execution artifacts. Before credential rotation: export the Chrome `Login Data` and `Cookies` SQLite files as evidence of what was accessible to CastleStealer at time of execution.

Step 4: Recovery — Before returning endpoints to production: verify no persistence mechanisms remain via registry run keys, scheduled tasks, or startup folder entries (D3-SICA — System Init Config Analysis); confirm credential rotation is complete for all accounts accessible from affected devices; re-enable endpoint protection with updated signatures for OXLOADER/CastleStealer; monitor reinstated endpoints for 72 hours using enhanced logging. Apply NIST AU-6 review cadence post-recovery to catch reinfection indicators.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Without EDR signature updates: deploy YARA rules published by Elastic Security Labs for OXLOADER and CastleStealer to scan reimaged endpoints before returning them to production — run via `yara -r oxloader.yar C:\` to confirm clean state. For persistence verification without enterprise tooling: use Autoruns (Sysinternals) on the rebuilt endpoint to enumerate all registry run keys (`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`), scheduled tasks, and startup folder entries, comparing against a known-good baseline from a clean reference image. For 72-hour enhanced logging, temporarily increase Sysmon verbosity to include Event ID 13 (Registry Value Set) targeting the run key paths above.

Evidence: Before re-enabling endpoint protection and returning to production, document the clean baseline state: export Autoruns output to a timestamped CSV (`autorunsc.exe -a * -c -h -s > baseline_YYYYMMDD.csv`) so any subsequent persistence mechanism added post-recovery is detectable by diff. This step does not alter volatile live state on a freshly reimaged system, but if performing recovery on a system that was NOT reimaged, apply the same volatile capture requirements from Step 3 before any registry or scheduled task modifications.

Step 5: Post-Incident — This campaign exposes gaps in user execution controls and browser-based threat visibility. Immediate control improvements: enforce application allowlisting to prevent unsigned executables from running (CIS 2.3 — Address Unauthorized Software); deploy or tune DNS-layer filtering for malvertising redirect chains; implement DNS monitoring per NIST AU-2 (Event Logging) to capture ad-network redirects; review and enforce MFA across all corporate accounts to limit credential-theft blast radius (CIS 6.3, CIS 6.4, CIS 6.5 — MFA requirements); conduct targeted user awareness communication on malvertising risks distinct from standard phishing training.

NIST Phase: Post Incident

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

Controls: CIS 2.3 (Address Unauthorized Software), 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-2 (Event Logging)

Compensating: For application allowlisting without enterprise tooling: configure Windows Software Restriction Policies or AppLocker (available in Windows Pro/Enterprise at no cost) to default-deny execution from `%TEMP%`, `%APPDATA%`, and `%USERPROFILE%\Downloads` — the exact paths CastleStealer's OXLOADER dropper uses. For MFA on a constrained budget: enforce FIDO2/passkey or TOTP-based MFA (Google Authenticator, Aegis) on all corporate SaaS accounts using each provider's native MFA enforcement policy, prioritizing email, VPN, and financial systems first given CastleStealer's credential-theft focus. For DNS monitoring without a SIEM, configure syslog export from your DNS resolver and parse it with a cron-driven grep for newly registered domains (domain age < 30 days) using a free threat intel feed such as Newly Registered Domains from WhoisXML API's free tier.

Evidence: No volatile evidence capture required — this step operates on already-preserved artifacts and closed-system state. However, the lessons-learned review should incorporate: (1) the full DNS query logs showing the malvertising redirect chain from initial ad click to OXLOADER download, as these document the specific ad network abuse path for threat intel sharing; (2) the CastleStealer target credential list extracted from the Chrome `Login Data` artifact captured in Step 3, to confirm completeness of credential rotation; (3) Sysmon Event ID 1 logs showing the browser-spawned OXLOADER process execution chain, to validate and tune detection rules for future malvertising campaigns using similar delivery patterns.

Detection Guidance

Primary detection signals: (1) Browser child process spawning unexpected executables, alert on chrome.exe, msedge.exe, or firefox.exe spawning cmd.exe, powershell.exe, mshta.exe, or wscript.exe (T1059, T1204.001); (2) Unsigned executable writes to %TEMP%, %APPDATA%, or user download directories immediately following ad-redirect web traffic, correlate proxy logs with endpoint file-write events; (3) Process injection activity, monitor for cross-process memory writes from low-reputation parent processes (T1055); (4) Credential store access outside expected application context, alert on LSASS reads, browser credential database access (Login Data, key4.db), or Windows Credential Manager queries by non-browser processes (T1552, T1555, T1539); (5) Outbound C2 communication, flag DNS queries and HTTP/S connections to newly registered domains (<30 days) or domains with low Cisco Umbrella reputation score from endpoints shortly after executable drop (T1041, T1105). NIST AU-2 and AU-6 govern the log sources required. MITRE D3FEND D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) are the primary countermeasures for detection. IOC signatures from the Elastic Security Labs research blog should be loaded into SIEM and EDR as soon as published.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See Elastic Security Labs campaign report for IOC list`	OXLOADER C2 and malvertising redirect infrastructure — IOCs published by Elastic Security Labs; load directly from their research post into SIEM/EDR	HIGH

Framework Mappings

MITRE-ATTACK

- **T1552** — Unsecured Credentials
- **T1566** — Phishing
- **T1041** — Exfiltration Over C2 Channel

- **T1059** — Command and Scripting Interpreter
- **T1204.001** — Malicious Link
- **T1539** — Steal Web Session Cookie
- **T1105** — Ingress Tool Transfer
- **T1566.002** — Spearphishing Link
- **T1204.002** — Malicious File
- **T1583.008** — Malvertising
- **T1555** — Credentials from Password Stores
- **T1055** — Process Injection

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
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552	Unsecured Credentials	Credential-Access
T1566	Phishing	Initial-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1059	Command and Scripting Interpreter	Execution
T1204.001	Malicious Link	Execution
T1539	Steal Web Session Cookie	Credential-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1566.002	Spearphishing Link	Initial-Access
T1204.002	Malicious File	Execution
T1583.008	Malvertising	Resource-Development
T1555	Credentials from Password Stores	Credential-Access
T1055	Process Injection	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/new-oxloader-loader-uses-maliciou...	T3
Google Cloud expands CVE program	https://cloud.google.com/blog/products/identity-security/google-clo...	T3
Google security overview	https://docs.cloud.google.com/docs/security/overview/whitepaper	T3
Google (Ads Platform) Vulnerability Rollup (2026-05-26)	https://techjacksolutions.com/scc-vendor-rollup/google-ads-platform...	T3
Google Ads policies - Advertising Policies Help	https://support.google.com/adspolicy/answer/6008942?hl=en	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-22 19:02 UTC by TJS Security Command Center