INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-08 14:00 UTC

TCLBanker Banking Trojan Weaponizes Victims' Own Accounts to Spread via WhatsApp and Outlook

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0290
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Logitech AI Prompt Builder (trojanized MSI installer), Microsoft Outlook, WhatsApp Web (Chromium-based), Chromium-based browsers, 59 unnamed banking/fintech/cryptocurrency platforms
Published	2026-05-07T18:06:52
Discovery Source	Rss

Executive Summary

Elastic Security Labs has identified TCLBanker, a banking trojan targeting 59 financial platforms across banking, fintech, and cryptocurrency sectors. The malware spreads itself by hijacking victims' active WhatsApp Web and Microsoft Outlook sessions to send malicious links to contacts, dramatically amplifying its reach beyond the initial infection vector. Organizations with employees accessing financial platforms or using browser-based messaging face credential theft, account takeover, and potential lateral movement into corporate financial systems.

Technical Analysis

TCLBanker is a banking trojan attributed to operators linked to the Maverick/Sorvepotel LATAM family, distributed via a trojanized Logitech AI Prompt Builder MSI installer. The installer uses DLL side-loading (T1574.002, CWE-506) to load malicious code without triggering standard endpoint detection. Post-installation, the malware establishes WebSocket-based C2 (T1071.002) for remote operator control and executes autonomous propagation by hijacking active WhatsApp Web browser sessions and Microsoft Outlook accounts (T1534, T1078) to distribute malicious links to victim contacts. Additional capabilities include keylogging (T1056.001), form grabbing (T1056.004), screen capture (T1113), credential harvesting from browsers (T1555.003), session cookie theft (T1539), process discovery (T1057), and Windows Command Shell execution (T1059.003). Geo-fencing logic (T1614.001, T1497.001) currently restricts active payload execution to

Brazil-locale systems, consistent with LATAM trojan tradecraft ahead of geographic expansion. No CVE has been assigned. Provisionally associated CWEs: CWE-506 (Embedded Malicious Code), CWE-494 (Download of Code Without Integrity Check), CWE-357 (Insufficient UI Warning of Dangerous Operations). No vendor patch exists; the trojanized installer is not from Logitech's official distribution channels. Primary research source: Elastic Security Labs.

Action Checklist

1. Containment: Block execution of unsigned or unverified MSI installers using application control policies (Windows Defender Application Control or equivalent). Alert on or block any Logitech AI Prompt Builder installation activity that did not originate from Logitech's official download portal. Isolate any endpoint where the trojanized installer is detected.
2. Detection: Hunt for DLL side-loading patterns associated with the MSI installer: unexpected DLLs loaded from the installer's working directory. Monitor for anomalous WebSocket connections from browser processes (chrome.exe, msedge.exe) to non-standard endpoints. Review Outlook send logs and WhatsApp Web session activity for mass-contact outreach from individual accounts. Elastic Security Labs published behavioral indicators in their research, prioritize those signatures in your EDR and SIEM.
3. Eradication: Remove any instance of the trojanized Logitech AI Prompt Builder MSI. Terminate and rotate all active browser sessions for affected users, specifically WhatsApp Web and Outlook Web Access tokens. Force re-authentication and invalidate session cookies for compromised accounts (T1539 mitigation). Revoke and reissue credentials for any financial platform accounts accessible from affected endpoints.
4. Recovery: Verify no persistence mechanisms remain: check scheduled tasks, registry run keys, and startup entries consistent with T1547. Confirm no unauthorized forwarding rules exist in affected Outlook accounts. Monitor outbound communications from recovered endpoints for 30 days. Notify contacts of affected users that malicious links may have been sent from legitimate accounts.
5. Post-Incident: This campaign exposed gaps in installer verification, browser session isolation, and outbound communication monitoring. Enforce code-signing requirements for all MSI installers. Implement conditional access policies requiring re-authentication before accessing financial platforms from corporate endpoints. Given the documented LATAM trojan pattern of geographic expansion, extend monitoring beyond Brazil-locale triggers, geo-fencing is an operator control, not a reliable defense boundary.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if any of the 59 targeted banking, fintech, or cryptocurrency platform credentials are confirmed stolen, if Outlook or WhatsApp Web mass-send activity is detected indicating active propagation to external contacts (triggering potential breach notification obligations under GLBA, PCI DSS, or applicable state privacy law), or if the responding team lacks EDR visibility into browser process behavior and cannot confirm session token theft did not occur.

Recovery Notes	After eradication, validate that all browser cookie stores on affected endpoints have been cleared and that re-authentication to WhatsApp Web and Outlook Web Access produces new, clean session tokens with no evidence of concurrent active sessions from unknown IP addresses. Monitor Exchange send logs and browser WebSocket connections daily for 30 days using the Elastic TCLBanker behavioral indicators, as TCLBanker's propagation mechanism means secondary infections among notified contacts may generate new inbound incidents referencing the original victim's identity. Contact all financial platform account security teams for the 59 targeted platforms where credentials were accessible from affected endpoints to request account activity review for the window between estimated initial infection and containment.
Forensic Artifacts	Trojanized Logitech AI Prompt Builder MSI file and its installer working directory: capture SHA-256 hash and all co-located DLLs consistent with T1574.002 side-loading before removal — the specific DLL name and load path is the primary indicator linking the installer to TCLBanker. | Chromium browser Cookie SQLite database (C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Cookies and equivalent Edge path): contains harvested session cookies for the 59 targeted financial platforms, WhatsApp Web authentication tokens, and OWA session identifiers — the direct evidence of what TCLBanker exfiltrated. | Sysmon Event ID 3 (Network Connection) logs from chrome.exe and msedge.exe processes: WebSocket connections to non-standard endpoints are the network-layer signature of TCLBanker's C2 exfiltration of browser session tokens; correlate destination IPs against Elastic's published TCLBanker infrastructure indicators. | Microsoft Exchange message tracking logs or Outlook Sent Items folder export: documents the exact contacts and external domains targeted by TCLBanker's Outlook-based propagation, scopes breach notification obligations, and identifies secondary victims who received malicious links from the compromised account. | Windows Registry Run keys (HKCU and HKLM \Software\Microsoft\Windows\CurrentVersion\Run) and scheduled task XML exports from C:\Windows\System32\Tasks\: TCLBanker persistence artifacts that would survive a browser cookie wipe; absence of entries here after eradication is required before clearing the endpoint for return to service.

Per-Action IR Details

Containment — Block execution of unsigned or unverified MSI installers via application control policies (Windows Defender Application Control or equivalent). Alert on or block any Logitech AI Prompt Builder installation activity that did not originate from Logitech's official download portal. Isolate any endpoint where the trojanized installer is detected.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality) — restrict installer execution to signed, authorized packages, CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Deploy a WDAC policy in audit mode first using PowerShell: `New-CIPolicy -FilePath C:\policy.xml -Level Publisher -ScanPath C:\Windows\System32` then switch to enforce mode after baselining. For endpoints without WDAC, use Sysmon Event ID 11 (FileCreate) filtered on *.msi drops outside of %ProgramFiles% or sanctioned staging paths. Write a Sigma rule matching: `Image: '*\msiexec.exe' CommandLine: '*LogitechAIPromptBuilder*'` and run against Windows Event Log via PowerShell `Get-WinEvent`.

Evidence: Before isolating: capture the full MSI file hash (SHA-256 via `Get-FileHash`), the installer's working directory contents for dropped DLLs consistent with side-loading (look for DLLs co-located with the MSI or in %TEMP%\LogitechAI\), Windows Security Event ID 4688 (Process Creation) showing msiexec.exe ancestry, and Prefetch files at C:\Windows\Prefetch\MSIEXEC.EXE-*.pf confirming execution timestamp. Preserve the trojanized

MSI intact before removal.

Detection — Hunt for DLL side-loading patterns associated with the MSI installer: unexpected DLLs loaded from the installer's working directory. Monitor for anomalous WebSocket connections from browser processes (chrome.exe, msedge.exe) to non-standard endpoints. Review Outlook send logs and WhatsApp Web session activity for mass-contact outreach from individual accounts. Elastic Security Labs published behavioral indicators in their research — prioritize those signatures in your EDR and SIEM.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), MITRE ATT&CK T1574.002 (DLL Side-Loading), MITRE ATT&CK T1539 (Steal Web Session Cookie), MITRE ATT&CK T1566.002 (Phishing: Spearphishing Link via existing session hijack)

Compensating: Enable Sysmon with a config including Event ID 7 (ImageLoad) to capture DLLs loaded by msiexec.exe or the Logitech AI Prompt Builder process that originate from non-standard paths (flag any DLL loaded from %TEMP%, %APPDATA%, or the installer staging directory). For WebSocket detection without a SIEM, use Wireshark capture filter `tcp.port == 443 && (http.upgrade == "websocket")` on a network tap or the affected host, then filter destination IPs against known Chromium CDN ranges — flag outliers. For Outlook mass-send detection, run: `Get-MessageTrackingLog -EventId SEND -Start (Get-Date).AddHours(-24) | Group-Object Sender | Sort Count -Descending` on Exchange or export .pst sent items and count recipients per message via PowerShell.

Evidence: Sysmon Event ID 7 logs showing the specific side-loaded DLL name and path loaded by the trojanized Logitech process; Sysmon Event ID 3 (Network Connection) from chrome.exe or msedge.exe to non-Google, non-Microsoft IP ranges over port 443 representing exfiltrated session token WebSocket traffic; Microsoft Exchange message tracking logs or Outlook Sent Items folder showing bulk sends to contact list entries within a compressed timeframe (TCLBanker weaponizes existing sessions so sends will appear as the legitimate user); browser process memory or disk-cached WebSocket frames containing harvested WhatsApp Web authentication tokens.

Eradication — Remove any instance of the trojanized Logitech AI Prompt Builder MSI. Terminate and rotate all active browser sessions for affected users, specifically WhatsApp Web and Outlook Web Access tokens. Force re-authentication and invalidate session cookies for compromised accounts (T1539 mitigation). Revoke and reissue credentials for any financial platform accounts accessible from affected endpoints.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-12 (Session Termination) — force termination of compromised browser sessions, NIST IA-5 (Authenticator Management) — revoke and reissue credentials, CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process), MITRE ATT&CK T1539 (Steal Web Session Cookie) — mitigation

Compensating: For session invalidation without enterprise SSO tooling: on the affected host run `Remove-Item -Path 'C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Cookies' -Force` and equivalent for Edge at `C:\Users\\AppData\Local\Microsoft\Edge\User Data\Default\Cookies` — this forces WhatsApp Web and OWA to require full re-authentication on next launch. For the 59 targeted financial platforms, manually trigger 'log out all sessions' or 'revoke all tokens' from each platform's security settings page. Use osquery query `SELECT path, name, value FROM browser_plugins WHERE browser_type='chrome'` to identify any malicious extensions TCLBanker may have installed to persist session access. Verify MSI removal with `Get-Package | Where-Object {$_.Name -like '*Logitech*AI*'}` and confirm no residual DLLs in the installer working directory.

Evidence: Before wiping cookies: export and preserve the browser cookie store (SQLite database at the paths above) as forensic evidence of which platforms' session tokens were present and potentially harvested; capture a process list snapshot (`Get-Process | Select-Object Name, Id, Path`) showing any TCLBanker-associated processes still running; document all financial platform account identifiers visible in browser history (`C:\Users\\AppData\Local\Google\Chrome\User Data\Default\History` SQLite) to scope which of the 59 targeted platforms require credential rotation.

Recovery — Verify no persistence mechanisms remain: check scheduled tasks, registry run keys, and startup entries consistent with T1547. Confirm no unauthorized forwarding rules exist in affected Outlook accounts. Monitor outbound communications from recovered endpoints for 30 days. Notify contacts of affected users that malicious links may have been sent from legitimate accounts.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity) — verify restored system integrity, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — sustained monitoring post-recovery, NIST CP-10 (System Recovery and Reconstitution), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), MITRE ATT&CK T1547 (Boot or Logon Autostart Execution) — persistence check, MITRE ATT&CK T1114.003 (Email Collection: Email Forwarding Rule)

Compensating: Enumerate persistence with: `Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft\*'} | Select TaskName, TaskPath` for non-Microsoft scheduled tasks; `reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` for run keys; and `Get-CimInstance Win32_StartupCommand` for startup entries — flag any entry referencing the Logitech AI Prompt Builder path or unsigned binaries in user-writable directories. For Outlook forwarding rules, run: `Get-InboxRule -Mailbox | Select Name, ForwardTo, ForwardAsAttachmentTo, RedirectTo` via Exchange PowerShell. For 30-day monitoring without a SIEM, schedule a daily Sysmon Event ID 3 log review filtering chrome.exe and msedge.exe connections against a blocklist of the C2 IPs published in Elastic's TCLBanker indicators.

Evidence: Autorun entries from the registry paths above captured before and after eradication to confirm removal; Outlook inbox rule export showing the pre-eradication state to document whether TCLBanker installed forwarding rules to a threat-actor-controlled address; Sysmon Event ID 1 (Process Creation) logs from the 30-day monitoring window to detect any TCLBanker re-execution or re-installation attempt; outbound DNS query logs for the 30-day window to detect beacon or C2 re-contact from the recovered endpoint.

Post-Incident — This campaign exposed gaps in installer verification, browser session isolation, and outbound communication monitoring. Enforce code-signing requirements for all MSI installers. Implement conditional access policies requiring re-authentication before accessing financial platforms from corporate endpoints. Given the documented LATAM trojan pattern of geographic expansion, extend monitoring beyond Brazil-locale triggers — geo-fencing is an operator control, not a reliable defense boundary.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling) — update playbook based on lessons learned, NIST IR-8 (Incident Response Plan) — revise plan to address installer verification and session isolation gaps, NIST SI-2 (Flaw Remediation) — formalize code-signing enforcement as a flaw remediation control, NIST SI-7 (Software, Firmware, and Information Integrity) — enforce code-signing via integrity verification, NIST AC-17 (Remote Access) — conditional access policies for financial platform access, CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For code-signing enforcement without enterprise PKI: configure WDAC Publisher rules to block unsigned MSIs: `New-CIPolicyRule -DriverFilePath -Level Publisher` and audit via Sysmon Event ID 11 filtered on .msi extensions dropped outside sanctioned directories. For conditional access without Azure AD Premium or equivalent: implement a browser extension policy via Group Policy (`HKLM\Software\Policies\Google\Chrome\ExtensionInstallAllowlist`) permitting only vetted extensions, and enforce a manual re-authentication requirement for financial platform bookmarks via a pinned internal portal page with session timeout set to 15 minutes. Document the LATAM geographic expansion pattern from the Elastic TCLBanker report in your threat intelligence feed and create a Sigma rule matching the specific WebSocket C2 communication pattern against any IP geolocation outside previously observed TCLBanker infrastructure — not just Brazil.

Evidence: Lessons-learned documentation citing the specific Elastic Security Labs TCLBanker research report as the triggering intelligence source; a gap analysis comparing pre-incident WDAC policy scope against the unsigned

Logitech AI Prompt Builder MSI execution path; Outlook audit logs confirming the volume of malicious outreach sent from compromised accounts (quantify blast radius for breach notification scoping); browser extension inventory from all affected endpoints to confirm no TCLBanker-installed extensions persist post-recovery.

Detection Guidance

Focus detection on three behavioral clusters. First, DLL side-loading at installation: monitor for DLLs loaded from %TEMP% or installer staging directories by msiexec.exe or newly spawned processes. Second, WebSocket-based C2: flag persistent WebSocket connections (wss://) initiated by browser helper processes or injected browser threads to endpoints with no established business context. Third, autonomous propagation: alert on bulk outbound message activity from Outlook (Exchange transport logs, high send-volume anomalies per mailbox) and WhatsApp Web (browser DOM manipulation patterns or automated HTTP POST sequences to web.whatsapp.com outside normal usage hours). Additional behavioral indicators: keylogger artifacts (raw input hooks), screen capture API calls from non-UI processes, and credential access attempts against browser credential stores (T1555.003). Elastic Security Labs' published research contains specific behavioral signatures and should be the primary source for rule construction. MITRE techniques to prioritize in detection rules: T1574.002, T1534, T1539, T1056.001, T1056.004, T1555.003.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Trojanized Logitech AI Prompt Builder MSI installer (distribution URL not publicly confirmed at time of item creation)`	Initial delivery vector — DLL side-loading payload embedded in MSI	HIGH
DOMAIN	`See Elastic Security Labs research publication for confirmed C2 indicators`	WebSocket-based C2 infrastructure — specific domains published in Elastic report	HIGH

Framework Mappings

MITRE-ATTACK

- **T1497.001** — System Checks
- **T1574.002** — DLL Side-Loading
- **T1113** — Screen Capture
- **T1218.007** — Msiexec
- **T1547** — Boot or Logon Autostart Execution
- **T1614.001** — System Language Discovery
- **T1057** — Process Discovery
- **T1071.002** — File Transfer Protocols
- **T1534** — Internal Spearphishing

- **T1078** — Valid Accounts
- **T1555.003** — Credentials from Web Browsers
- **T1539** — Steal Web Session Cookie
- **T1566.002** — Spearphishing Link
- **T1566.001** — Spearphishing Attachment
- **T1056.001** — Keylogging
- **T1056.004** — Credential API Hooking
- **T1059.003** — Windows Command Shell
- **T1021.006** — Windows Remote Management

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **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
- **8.2** — Collect Audit Logs

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
T1497.001	System Checks	Defense-Evasion
T1574.002	DLL Side-Loading	Persistence
T1113	Screen Capture	Collection
T1218.007	Msiexec	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1614.001	System Language Discovery	Discovery
T1057	Process Discovery	Discovery
T1071.002	File Transfer Protocols	Command-And-Control
T1534	Internal Spearphishing	Lateral-Movement
T1078	Valid Accounts	Defense-Evasion
T1555.003	Credentials from Web Browsers	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1566.002	Spearphishing Link	Initial-Access
T1566.001	Spearphishing Attachment	Initial-Access
T1056.001	Keylogging	Collection
T1056.004	Credential API Hooking	Collection
T1059.003	Windows Command Shell	Execution
T1021.006	Windows Remote Management	Lateral-Movement

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/new-tclbanker-malwar...	T3
TCLBANKER: Brazilian Banking Trojan Spreading via ...	https://www.elastic.co/security-labs/tclbanker-brazilian-banking-tr...	T3
A new trojan named TCLBanker, which targets 59 banking ...	https://www.instagram.com/p/DYDb-I3gQmq/	T3

Source	URL	Tier
New TCLBanker malware self-spreads over WhatsApp and ...	https://www.bleepingcomputer.com/news/security/new-tclbanker-malwar...	T3
WhatsApp Web malware spreads banking trojan ...	https://www.foxnews.com/tech/whatsapp-web-malware-spreads-banking-t.. .	T3

Generated 2026-05-08 14:00 UTC by TJS Security Command Center