Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

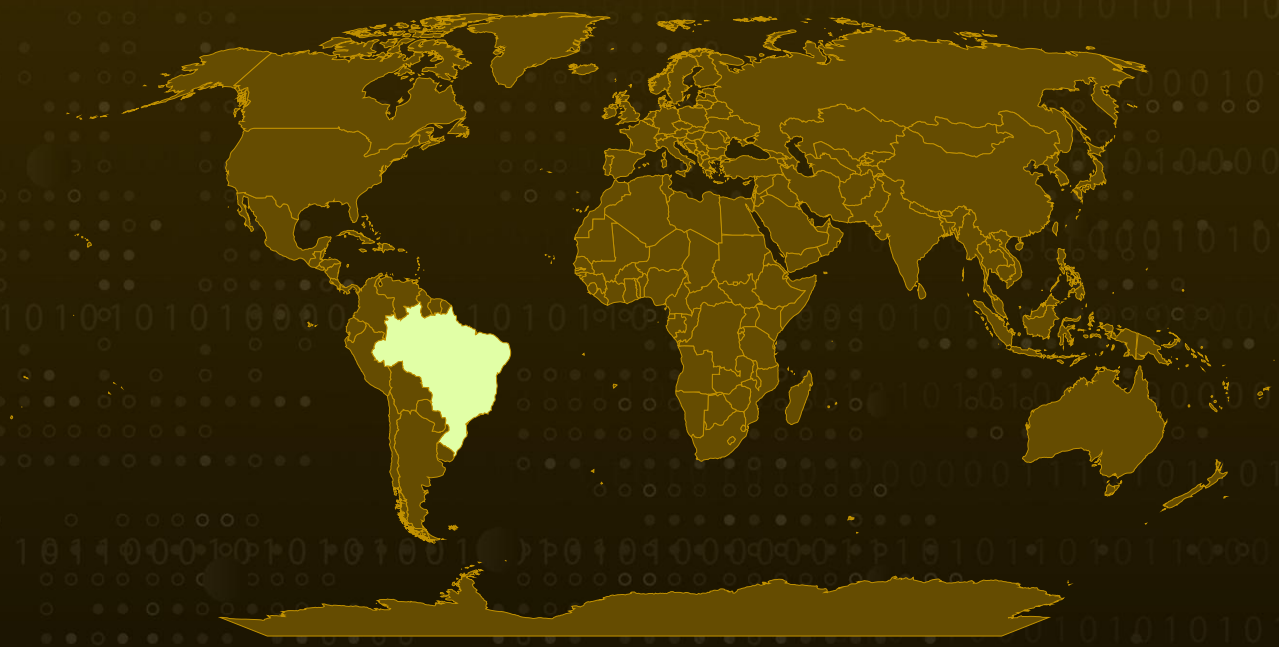
TCLBanker: Trojanized Logitech Installer Fuels Banking Malware Campaign

Date of Publication	Admiralty Code	TA Number
May 11, 2026	A1	TA2026125

Summary

First Seen: 2026
Targeted Region: Brazil
Targeted Platform: Windows
Targeted Products: Chromium-based browsers (Chrome, Edge, Brave, Opera, Vivaldi), Firefox, Microsoft Outlook, WhatsApp Web
Targeted Industries: Banking, Fintech, Cryptocurrency
Malware: TCLBANKER
Campaign: REF3076
Attack: TCLBANKER is a Brazilian banking trojan delivered via trojanized Logitech Logi AI Prompt Builder MSI installers bundled inside ZIP files. It uses DLL side-loading to execute a malicious loader that deploys two .NET Reactor-protected modules: a banking trojan targeting 59 Brazilian financial domains using WPF-based fraud overlays and WebSocket C2, and a worm module that self-propagates via WhatsApp session hijacking and Outlook COM-automated phishing emails.

Attack Regions



Attack Details

#1 A newly discovered banking trojan called TCLBanker is targeting 59 banking, fintech, and cryptocurrency platforms using a trojanized MSI installer disguised as Logitech's AI Prompt Builder. Beyond stealing financial data, the malware also includes self-propagating worm capabilities for both WhatsApp and Outlook, allowing it to automatically spread to additional victims.

#2 TCLBanker is delivered through malicious ZIP archives containing a tampered MSI package that abuses the legitimate, digitally signed Logitech Logi AI Prompt Builder application. The malware relies on DLL side-loading by planting a malicious file named screen_retriever_plugin.dll, disguised as a legitimate Flutter plugin. Once the Logitech application is executed, it unknowingly loads the malicious DLL, triggering the infection chain. Campaigns linked to the malware primarily use phishing lures impersonating Brazilian business services, including fake invoice notifications (NFe) and quotation requests distributed via WhatsApp messages and Outlook emails sent from compromised accounts.

#3 Before activating its payloads, the loader performs extensive environment validation checks to avoid analysis and sandbox detection. It creates multiple system fingerprints using anti-debugging techniques such as PEB flag checks, heap analysis, hardware breakpoint detection, and timing measurements. The malware also validates system characteristics, including hypervisor presence, disk space, CPU and RAM resources, sandbox-related usernames, and Brazilian Portuguese locale settings. These fingerprints are combined into an environment-specific hash that acts as the AES-256 CBC decryption key for the embedded payloads. If the environment does not meet the expected criteria, decryption fails silently, effectively preventing execution in research or analysis environments. To further evade detection, the malware unhooks ntdll.dll, generates direct syscall trampolines, patches ETW telemetry, and continuously monitors for security and reverse-engineering tools such as IDA, Ghidra, x64dbg, dnSpy, Frida, ProcessHacker, and CheatEngine.

#4 The primary banking trojan component, identified as Tcl.Agent, establishes persistence through a hidden scheduled task named RuntimeOptimizeService that executes at user logon. It continuously monitors the victim's browser activity using UI Automation, checking URLs against a hardcoded list of 59 targeted Brazilian banking, fintech, and cryptocurrency platforms. Once a match is detected, the malware initiates a WebSocket-based command-and-control (C2) session, enabling attackers to remotely execute shell commands, capture screenshots, stream the victim's screen, log keystrokes, hijack clipboard data, control mouse and keyboard activity, browse files, and manage processes. During active sessions, a Task Manager killer runs every 500 milliseconds to block users from inspecting malicious activity.

#5 One of TCLBanker's most advanced features is its WPF-based full-screen overlay framework designed for social engineering and credential theft. The malware displays convincing bank-themed phishing interfaces, including PIN entry prompts, credential collection screens, fake progress bars, vishing wait screens, and counterfeit Windows Update pages. These overlays operate as borderless topmost windows that resist dismissal and include anti-capture mechanisms that prevent them from appearing in screenshots or screen-sharing sessions.

#6 The worm component, tracked as Tcl.WppBot, enables large-scale propagation through both WhatsApp and Outlook. The WhatsApp module hijacks authenticated browser sessions by cloning IndexedDB session data, launching headless Chromium instances with bot-detection bypasses, and automatically sending phishing messages to as many as 3,000 Brazilian contacts in a single campaign. The Outlook module abuses PowerShell COM automation to harvest contacts and distribute phishing emails directly from the victim's mailbox, leveraging trusted sender reputations to evade spam filtering. Researchers also observed that the malware's entire command-and-control and distribution infrastructure is hosted on Cloudflare Workers under a single account identifier.

Recommendations

- **Monitor for DLL Side-Loading via Logitech Applications:** Deploy detection rules targeting the loading of screen_retriever_plugin.dll by LogiAiPromptBuilder.exe or any unsigned DLL loaded by legitimate Flutter-based applications. Alert on DLL loads from non-standard installation paths such as %LocalAppData%\LogiAI.

- **Detect NTDLL Unhooking and ETW Patching:** Implement behavioral detections for processes that reload ntdll.dll from disk (a common unhooking technique) or patch EtwEventWrite with ret instructions. Elastic provides specific detection rules including NTDLL Memory Protection Change via Unsigned DLL and Potential NTDLL Memory Unhooking.

- **Restrict MSI Installer Execution:** Enforce application control policies that block the execution of unsigned or externally sourced MSI installers. Require administrative approval for MSI installations and audit msiexec.exe usage for silent installation flags (/qn) that indicate automated malware deployment.

Harden WhatsApp Web Session Security: Educate users to regularly review and terminate active WhatsApp Web sessions from their mobile devices. Monitor for headless Chromium processes accessing WhatsApp Web IndexedDB data or unexpected browser automation activity on endpoints.

Restrict Outlook COM Automation: Implement policies that limit COM interop access to Microsoft Outlook. Monitor for PowerShell scripts that instantiate Outlook.Application COM objects or enumerate inbox contacts, and alert on unusual bulk email sending patterns from desktop Outlook clients.

Segment and Monitor Financial Application Access: Apply network segmentation and enhanced monitoring for endpoints that access banking and financial platforms. Implement conditional access policies that validate device health and session integrity before allowing access to sensitive financial services.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1218: System Binary Proxy Execution	T1218.007: Msiexec
	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
	T1106: Native API	
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1574: Hijack Execution Flow	T1574.001: DLL
Defense Evasion	T1140: Deobfuscate/Decode Files or Information	
	T1027: Obfuscated Files or Information	

Tactic	Technique	Sub-technique
Defense Evasion	T1622: Debugger Evasion	
	T1497: Virtualization/Sandbox Evasion	T1497.001: System Checks
		T1497.003: Time Based Evasion
	T1685: Disable or Modify Tools	T1685.001: Disable or Modify Windows Event Log
	T1055: Process Injection	
Credential Access	T1056: Input Capture	T1056.001: Keylogging
		T1056.003: Web Portal Capture
	T1185: Browser Session Hijacking	
Discovery	T1057: Process Discovery	
	T1010: Application Window Discovery	
	T1082: System Information Discovery	
	T1614: System Location Discovery	T1614.001: System Language Discovery
Collection	T1113: Screen Capture	
	T1115: Clipboard Data	
	T1114: Email Collection	T1114.001: Local Email Collection
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
Impact	T1529: System Shutdown/Reboot	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	701d51b7be8b034c860bf97847bd59a87dca8481c462532881374696499 5b626, 8a174aa70a4396547045aef6c69eb0259bae1706880f4375af71085eeb53 7059, 668f932433a24bbae89d60b24eee4a24808fc741f62c5a3043bb7c915234 2f40, 63beb7372098c03baab77e0dfc8e5dca5e0a7420f382708a4df79bed2d90 0394
Domains	campanha1-api[.]ef971a42[.]workers[.]dev, mxtestacionamentos[.]com, documents[.]ef971a42[.]workers[.]dev, arquivos-omie[.]com, documentos-online[.]com, afonsoferragista[.]com, doccompartilhe[.]com, recebamais[.]com
IPv4	191[.]96[.]224[.]96

References

https://www.elastic.co/security-labs/tclbanker-brazilian-banking-trojan

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

May 11, 2026 • 9:00 AM

More at www.hivepro.com