IDENTITY PROTECTION

Stealing Browser-Protected Credentials: Defeating App-Bound Encryption

The ultimate objective of these sophisticated initial access and evasion techniques is not mere disruption, but the systematic acquisition of highly privileged credentials, cryptographic keys, and active session tokens.

Dennis Underwood, Founder & CEO, Cyber Crucible · November 2026

EXECUTIVE SUMMARY

By stealing active, authenticated session cookies via ChromElevator, MUDDYWATER operators can execute "Pass-the-Cookie" attacks. This technique allows the adversary to hijack live, authenticated web sessions, entirely bypassing MFA prompts and gaining direct, unimpeded access to corporate cloud environments, financial transaction portals, and internal communication platforms.

01 Financial Sector Risk: ChromElevator and App-Bound Encryption

For the financial sector, the ultimate objective of these sophisticated initial access and evasion techniques is not mere disruption, but the systematic acquisition of highly privileged credentials, cryptographic keys, and active session tokens. In the Operation Olalampo campaign, both the fmapp.dll and sentinelagentcore.dll malicious libraries were embedded with a specialized, devastating post-exploitation tool known as ChromElevator.[1]

ChromElevator is an open-source utility specifically engineered to extract saved passwords, active session cookies, and payment card data from Chromium-based web browsers (such as Google Chrome, Microsoft Edge, Brave, and Vivaldi).[1] Historically, credential theft from web browsers involved simple, noisy file reads of the local SQLite databases where this data was stored.

However, in an attempt to thwart this exact type of theft, Google introduced App-Bound Encryption (ABE) in Chrome version 127. ABE cryptographically ties the encryption of browser data to the specific digital identity of the browser application itself, theoretically preventing external malware or unauthorized scripts from decrypting the stored secrets.[2]

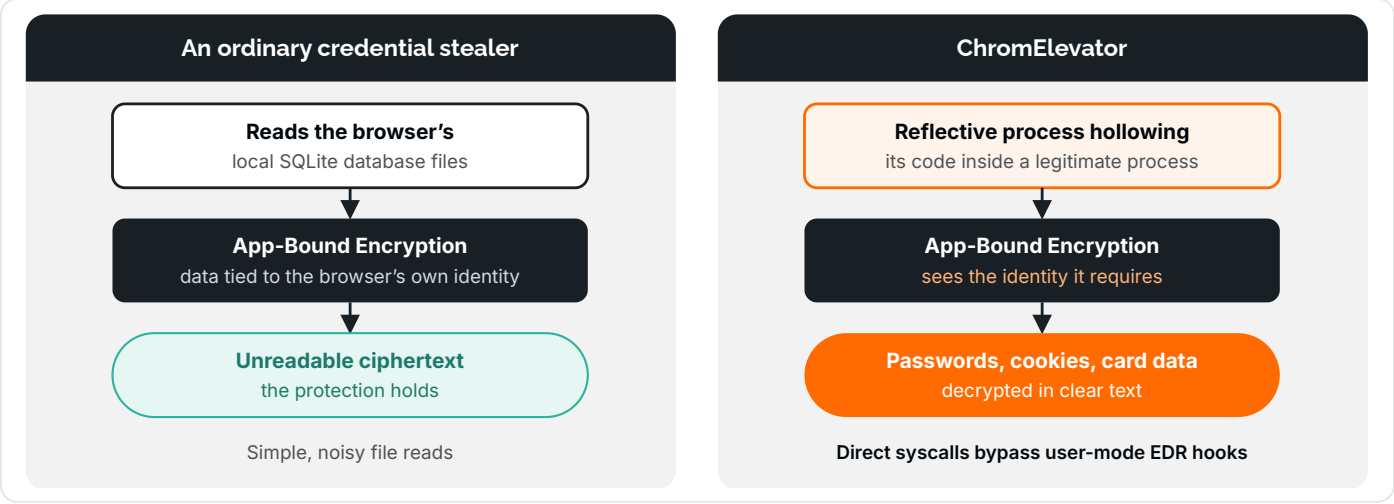

Figure 1. How ChromElevator gets past App-Bound Encryption

MUDDYWATER's implementation of ChromElevator directly and elegantly circumvents this advanced protection.[3] The tool utilizes highly advanced memory manipulation techniques—specifically Reflective Process Hollowing and Direct Syscalls—to bypass App-Bound Encryption. By hollowing out a legitimate process and reflectively injecting malicious code, the malware perfectly mimics the application identity required by the Windows Cryptography API: Next Generation (CNG) to decrypt the browser data.[4] Furthermore, by utilizing Direct Syscalls, ChromElevator bypasses the user-mode API hooks that EDR solutions use to monitor system behavior, interacting directly with the Windows kernel.[3]

Pass-the-Cookie Attacks

The strategic implications of this capability for financial institutions are catastrophic. Modern financial sector security architectures rely almost exclusively on Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and conditional access policies. However, by stealing active, authenticated session cookies via ChromElevator, MUDDYWATER operators can execute "Pass-the-Cookie" attacks.[5]

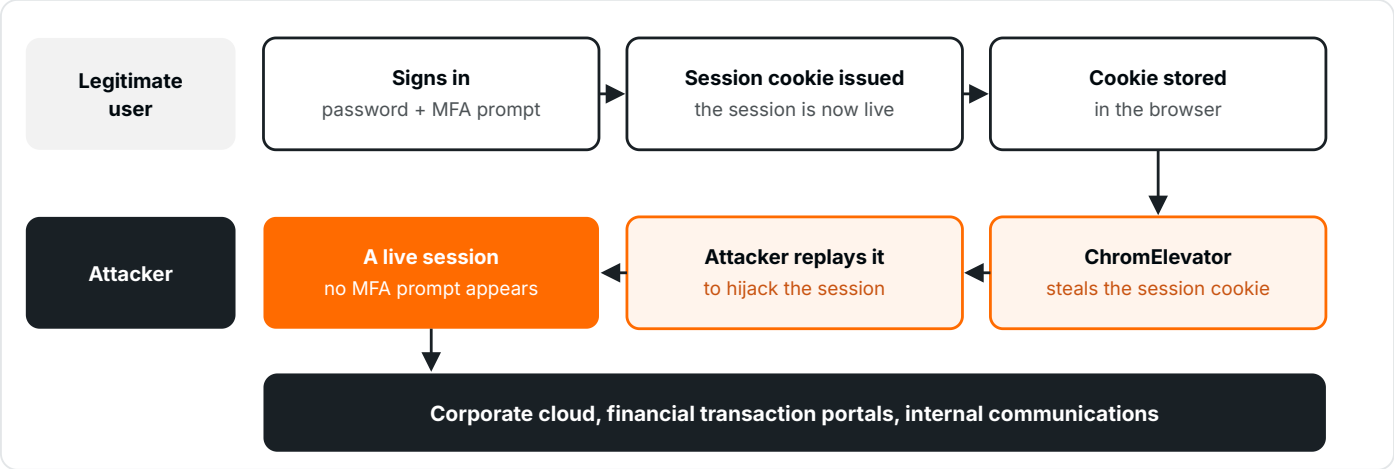

Figure 2. Pass-the-cookie: a stolen session cookie skips the MFA prompt

This technique allows the adversary to hijack live, authenticated web sessions, entirely bypassing MFA prompts and gaining direct, unimpeded access to corporate cloud environments, financial transaction portals, and internal communication platforms. In financial environments where users routinely store credentials in unprotected facilities or browsers, the deployment of tools like ChromElevator leads directly to rapid lateral movement and systemic, unrecoverable compromise.[6] Alongside ChromElevator, MUDDYWATER has deployed a suite of credential harvesters, including CE-Notes (a Chromium data stealer that mimics ChromElevator), LP-Notes (a fake Windows Security dialog used for phishing), and Blub (a cross-browser data stealer targeting Firefox and Opera).[4]

02 Strategic Imperatives for the Financial Sector

For the financial sector, the implications are profound. An architecture that relies on the integrity of the operating system it is trying to protect is structurally doomed to fail. The defense paradigm must definitively shift from reactive resilience and cloud-based telemetry collection to proactive, autonomous, and OS-independent defense.

References

1. "MuddyWater Espionage Campaign Hits 9 Countries in Q1 2026," Safestate, accessed June 1, 2026. https://www.safestate.com/post/muddywater-espionage-campaign-hits-9-countries-in-q1-2026
2. "MuddyWater: Snakes by the riverbank," WeLiveSecurity (ESET), accessed June 1, 2026. https://www.welivesecurity.com/en/eset-research/muddywater-snakes-riverbank/
3. "17 Critical Alerts Covering APT AI Adoption, Pre-Auth Zero-Days, and Supply Chain Worms," SISA Weekly Threat Watch, accessed June 1, 2026. https://www.sisainfosec.com/weekly-threat-watch/17-critical-alerts-covering-apt-ai-adoption-pre-auth-zero-days-and-supply-chain-worms/
4. "Iranian hackers deploy new MuddyViper spyware against Israel," CyberInsider, accessed June 1, 2026. https://cyberinsider.com/iranian-hackers-deploy-new-muddyviper-spyware-against-israel/
5. Cyber Crucible, collected white papers, 24 February 2026. Published individually on the Cyber Crucible Intelligence Hub. https://www.cybercrucible.com/intelligence-hub
6. "2025 CBEST thematic," Bank of England, accessed June 1, 2026. https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/2025-cbest-thematic

Related papers

- **Part 1 of 5:** DLL Side-Loading in Real Attacks: Executive Summary www.cybercrucible.com/intelligence-hub/dll-side-loading-in-real-attacks
- **Part 2 of 5:** DLL Side-Loading: How Attackers Hide Inside Trusted Software www.cybercrucible.com/intelligence-hub/dll-side-loading-how-attackers-hide-in-trusted-software
- **Part 4 of 5:** Why Allow-Listing, Cloud Collectors and EDR Killers Miss It www.cybercrucible.com/intelligence-hub/allow-listing-cloud-collectors-edr-killers-dll-side-loading
- **Part 5 of 5:** OS Independence: Inspecting DLLs Without Trusting the OS www.cybercrucible.com/intelligence-hub/os-independence-inspecting-dlls-without-trusting-the-os
- **Ransomware Defense:** The Technical and Business Failures of Ransomware Key Capture Defense www.cybercrucible.com/intelligence-hub/ransomware-key-capture-defense-failures

Read online (six languages): www.cybercrucible.com/intelligence-hub/stealing-browser-credentials-app-bound-encryption
Book a live technical demo: www.cybercrucible.com/demo