ATTACK TRADECRAFT

DLL Side-Loading in Real Attacks: Executive Summary

To effectively neutralize machine-speed, in-memory threats, defense systems must decouple from the fragile operating systems they protect.

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

EXECUTIVE SUMMARY

The Q1 2026 MUDDYWATER Operation Olalampo campaign across North Africa and the MENA region serves as a stark, undeniable leading indicator of the future of cyber warfare. By mastering DLL side-loading, in-memory process hollowing, and the weaponization of digitally signed EDR binaries, adversaries have effectively bypassed the foundational principles of traditional endpoint security. The extraction of privileged session tokens via tools like ChromElevator, combined with AI-assisted malware development, creates a highly lethal environment where legacy, cloud-reliant detection platforms are simply outpaced and outmaneuvered.

01 The Erosion of the Secure Perimeter

In the contemporary cybersecurity ecosystem, the concept of a hardened network perimeter has been entirely dismantled. Advanced Persistent Threats (APTs) no longer seek to batter down firewalls; instead, they compromise endpoints through social engineering, weaponize legitimate administrative tools, and operate silently within the volatile memory of trusted processes. For the financial sector, where the integrity of transactions and the confidentiality of client data are paramount, this shift in adversarial tradecraft represents an existential threat. Traditional security paradigms—heavily reliant on static file analysis, application whitelisting, and reactive, cloud-based telemetry—are experiencing catastrophic, systemic failures against these memory-centric attack vectors.[1]

02 The North African and MENA Campaign

In early 2026, MUDDYWATER launched Operation Olalampo, a highly coordinated offensive targeting over 100 government, telecommunications, and financial entities across North Africa and the Middle East.[2] This campaign utilized compromised email accounts, routed through anonymizing VPNs, to distribute sophisticated spear-phishing lures that appeared as legitimate diplomatic or financial correspondence.[2] This campaign demonstrated a devastating mastery of Dynamic Link Library (DLL) side-loading, memory manipulation, and advanced credential theft specifically designed to subvert Endpoint Detection and Response (EDR) solutions.[3]

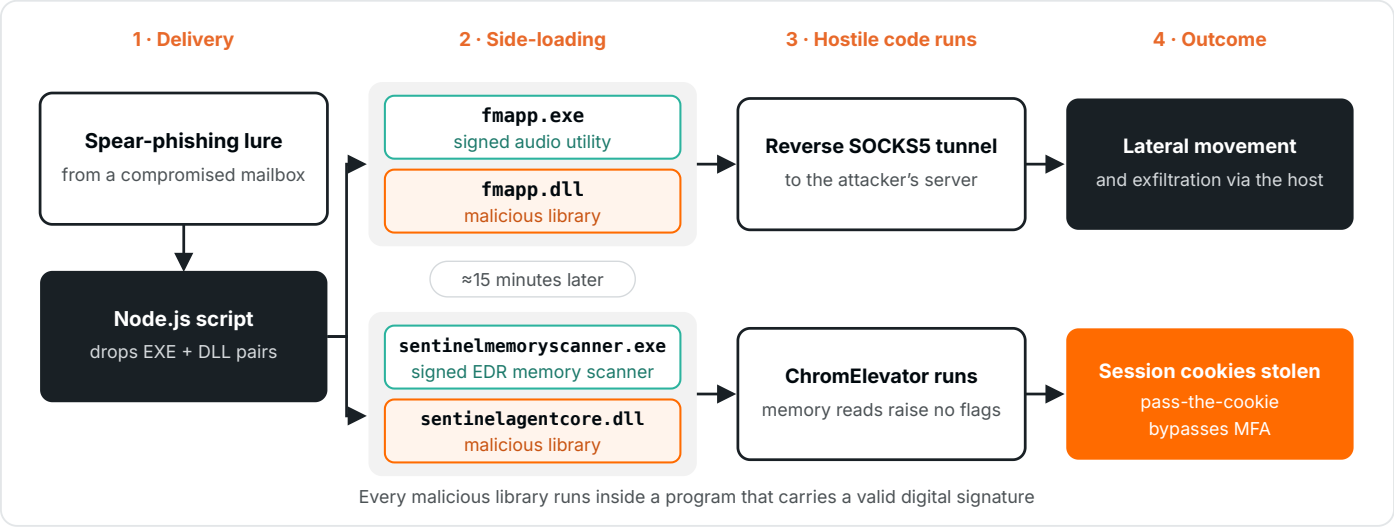

Figure 1. The side-loading chain in the Operation Olalampo intrusions: two signed programs, two malicious libraries[4]

The primary objective of these intrusions was not immediate financial extortion via ransomware, but rather deep network espionage, the prepositioning of persistent access, and the systemic harvesting of highly privileged credentials.[5] To achieve this, the threat actors deployed a newly developed

arsenal of malware families designed specifically to evade detection by operating entirely within system memory.

03 The Evolution of the Malicious Arsenal

Recent telemetry indicates a profound maturation in MUDDYWATER's operational discipline and technical sophistication.[6] The group has transitioned from utilizing off-the-shelf scripts to engineering bespoke, memory-safe malware, indicating a significant investment in long-term, stealthy network persistence. The tooling deployed in Operation Olalampo marks a stark departure from previous MUDDYWATER campaigns. The integration of memory-safe programming languages and the utilization of trusted communication channels for Command and Control (C2) demonstrate a highly evolved evasion strategy.[7]

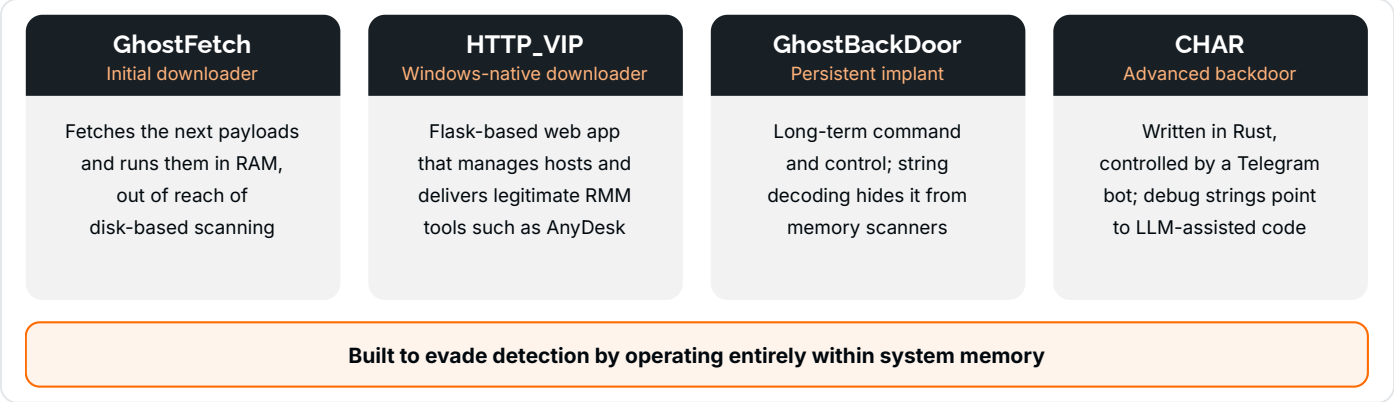

Figure 2. The malware families deployed in Operation Olalampo[8]

The development of the CHAR backdoor is particularly alarming for financial sector defenders. By utilizing the Telegram API for C2 communications, MUDDYWATER operators successfully blend their malicious traffic with normal, encrypted web traffic, bypassing perimeter network detection systems.[9] Furthermore, the evidence of AI-assisted code generation in CHAR's development implies that the threat actor can rapidly iterate and compile polymorphic variations of their tooling, rendering traditional signature-based Anti-Virus (AV) solutions entirely ineffective.[7]

04 Strategic Imperatives

However, analyzing the anatomy of the threat is only half the battle. As adversaries increasingly manipulate the underlying Windows operating system libraries that traditional security tools depend upon, a radical paradigm shift in defensive architecture is mandatory. To effectively neutralize machine-speed, in-memory threats, defense systems must decouple from the fragile operating systems they protect. This series details the necessity of Operating System (OS) independence and real-time DLL live inspection, and how Cyber Crucible's autonomous, kernel-level capabilities provide an unparalleled "unfair advantage" against modern threat actors.[1]

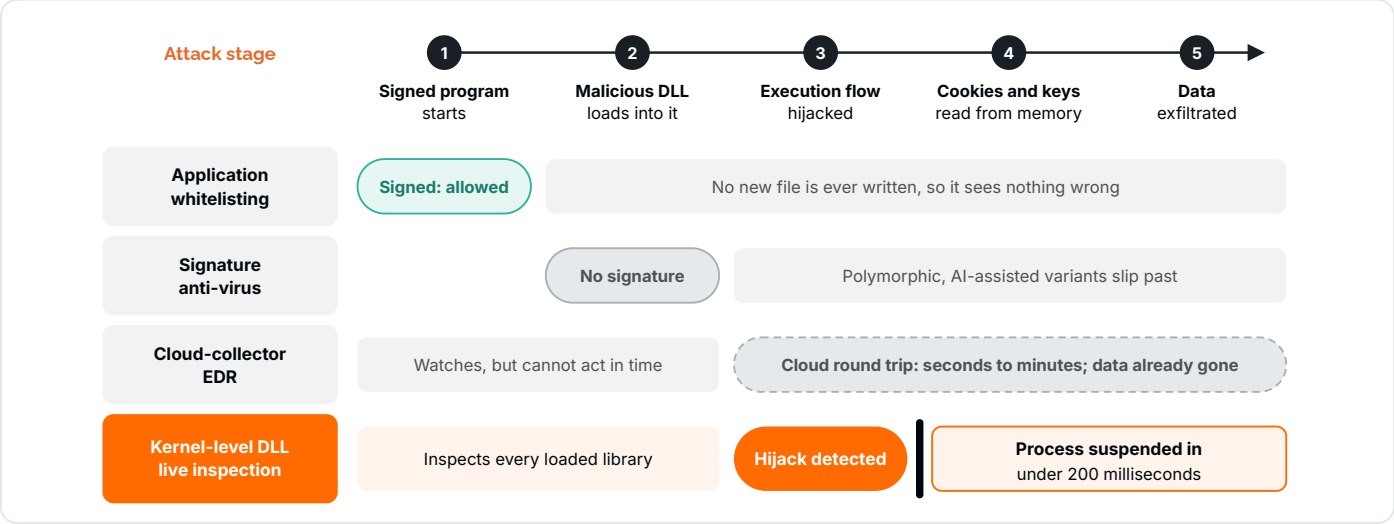

Figure 3. Where legacy controls look, and where kernel-level DLL live inspection acts

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.

By decoupling from vulnerable Windows dependencies and implementing continuous, real-time live inspection of running programs and their supporting DLLs, next-generation platforms like Cyber Crucible strip the adversary of their primary advantage: stealth in memory. Coupled with kernel-level, deterministic Genetic AI capable of neutralizing threats in under

200 milliseconds without relying on human intervention, organizations can construct an unyielding defense. In a threat landscape where cryptographic trust is constantly exploited, survival depends entirely on an architecture that verifies continuously, decides autonomously, and prevents instantly.

References

1. Cyber Crucible, collected white papers, 24 February 2026. Published individually on the Cyber Crucible Intelligence Hub. https://www.cybercrucible.com/intelligence-hub
2. "Cyber News Roundup – October 24 2025," Integrity360, accessed June 1, 2026. https://www.integrity360.com/cyber-news-roundup-october-24-2025
3. "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
4. "Seedworm: Iran-Linked Hackers Breached Korean Electronics Maker in Global Spying Campaign," Security.com (Symantec), accessed June 1, 2026. https://www.security.com/threat-intelligence/iran-seedworm-electronics
5. "Muddying the Tracks: The State-Sponsored Shadow Behind Chaos Ransomware," Rapid7, accessed June 1, 2026. https://www.rapid7.com/blog/post/tr-muddying-tracks-state-sponsored-shadow-behind-chaos-ransomware/
6. "Symantec uncovers Iran-linked Seedworm espionage campaign targeting airport, government, manufacturing sectors," Industrial Cyber, accessed June 1, 2026. https://industrialcyber.co/threats-attacks/symantec-uncovers-iran-linked-seedworm-espionage-campaign-targeting-airport-government-manufacturing-sectors/
7. "The Iranian Cyber Threat Landscape: Inside the Adversary Playbook," ExtraHop, accessed June 1, 2026. https://cloud-assets.extrahop.com/resources/whitepapers/iranian-cyber-threat-landscape-inside-adversary-playbook-white-paper.pdf
8. "Operation Olalampo: Inside MuddyWater's Latest Campaign," Group-IB Blog, accessed June 1, 2026. https://www.group-ib.com/blog/muddywater-operation-olalampo/
9. "Operation Olalampo: MuddyWater's Expanding Campaign Across MENA," Hive Pro, accessed June 1, 2026. https://hivepro.com/threat-advisory/operation-olalampo-muddywater-expanding-campaign-across-mena/

Related papers

- **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 3 of 5:** Stealing Browser-Protected Credentials: Defeating App-Bound Encryption www.cybercrucible.com/intelligence-hub/stealing-browser-credentials-app-bound-encryption
- **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/dll-side-loading-in-real-attacks
Book a live technical demo: www.cybercrucible.com/demo