ATTACK TRADECRAFT

DLL Side-Loading: How Attackers Hide Inside Trusted Software

To understand the severity of this threat, one must understand how the Windows Operating System dynamically loads supporting code.

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

EXECUTIVE SUMMARY

Adversaries exploit this mechanism by placing a maliciously crafted DLL in the same directory as a legitimate, highly trusted, and digitally signed executable. When the legitimate program is executed, the OS unwittingly loads the malicious library directly into the trusted process's memory space. By hijacking an EDR binary, the attackers effectively turned the organization's watcher into a weapon.

01 The Mechanics of Subversion: DLL Side-Loading Tradecraft

The linchpin of MUDDYWATER's operational success in North Africa is the disciplined, systemic abuse of DLL side-loading.[1] To understand the severity of this threat, one must understand how the Windows Operating System dynamically loads supporting code.

When a Windows executable (an .exe file) is launched, it rarely contains all the code necessary to function. Instead, it relies on shared libraries, known as Dynamic Link Libraries (DLLs), to perform routine tasks such as networking, cryptography, or rendering graphics. If the executable does not specify a hardcoded, absolute file path for these required DLLs, the Windows OS utilizes a predefined "Search Order" to find them. Crucially, the very first location Windows checks is the local directory from which the executable itself was launched.[1]

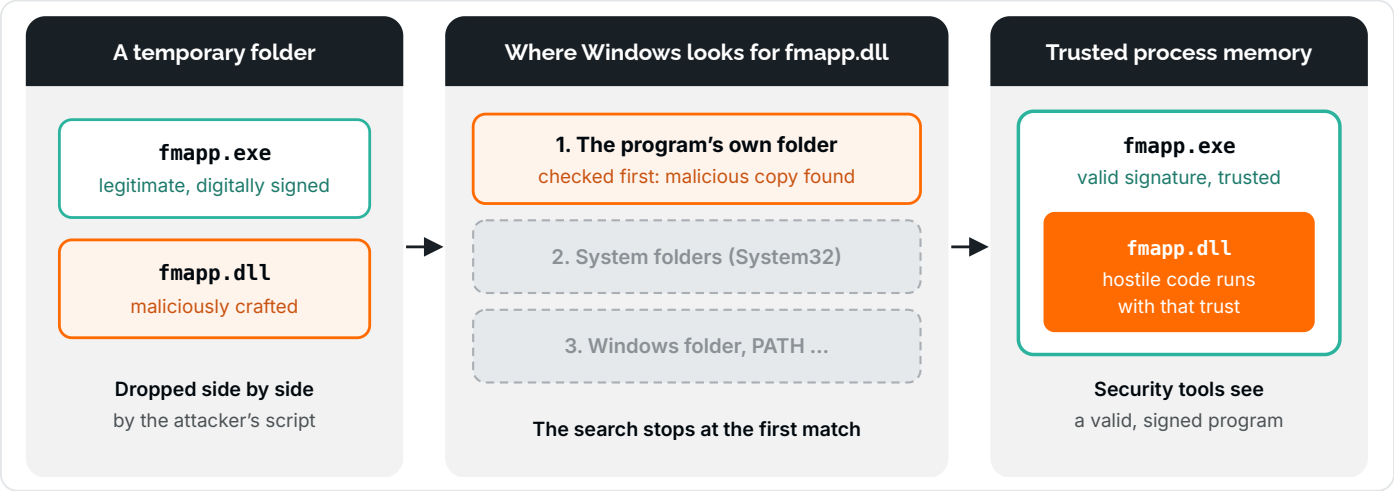

Figure 1. How side-loading uses the Windows DLL search order

Adversaries exploit this mechanism by placing a maliciously crafted DLL in the same directory as a legitimate, highly trusted, and digitally signed executable. When the legitimate program is executed, the OS unwittingly loads the malicious library directly into the trusted process's memory space.

To visualize this, consider the concept of Application Whitelisting as a school security protocol.[2] A "hall pass" allows a student to move freely through the corridors. Traditional security tools look at the executable and see a valid, digitally signed "hall pass" (e.g., a Microsoft or vendor-signed certificate). Because the core executable is legitimate, the security tool ignores the process. However, DLL side-loading allows an attacker to effectively hollow out the student carrying the hall pass and replace their intent with malicious directives. The security guard (the EDR) sees the valid pass, but fails to realize the entity holding it is now a hostile actor.[2]

02 Weaponizing the Supply Chain: Fortemedia and SentinelOne

In the North African Operation Olalampo intrusions, MUDDYWATER operators demonstrated an exceptional understanding of enterprise software ecosystems by specifically targeting two distinct legitimate binaries to facilitate their DLL side-loading chains. These attacks were orchestrated

seamlessly without user interaction, driven entirely by a malicious Node.js script dropping components into temporary directories (node.exe).[3]

The first side-loading vector utilized fmapp.exe, a legitimate, digitally signed audio-driver utility developed by Fortemedia Inc.[4] MUDDYWATER delivered this benign executable alongside a malicious library named fmapp.dll. Upon execution, the trusted Fortemedia application inadvertently loaded the hostile DLL into its memory space. The primary function of this compromised library was to establish a reverse SOCKS5 proxy tunnel, creating a stealthy, persistent connection back to an attacker-controlled C2 server (frequently hardcoded to IPs such as 165.227.82.147 or 157.20.182.49).[4] This encrypted tunnel allowed the adversaries to route lateral movement commands and exfiltrate data directly through the compromised host, bypassing enterprise firewalls.

The second side-loading vector, deployed approximately fifteen minutes after the Fortemedia proxy was established, is far more concerning for enterprise security teams. The attackers executed sentinelmemoryscanner.exe, a legitimate, digitally signed component of the SentinelOne endpoint security suite.[4] This highly privileged EDR binary was used to side-load a malicious library named sentinelagentcore.dll.[1]

The selection of a premier EDR component for side-loading is a calculated, devastating maneuver. Security platforms universally trust their own components, and operating systems are configured to allow these security binaries extensive, unrestricted access to the kernel, physical memory, and the entire file system.[1] By hijacking an EDR binary, the attackers effectively turned the organization's watcher into a weapon. Behavioral heuristics that would normally flag a standard application for performing deep system memory enumeration remain silent, because an EDR memory scanner is inherently designed to read the memory spaces of other processes.[1]

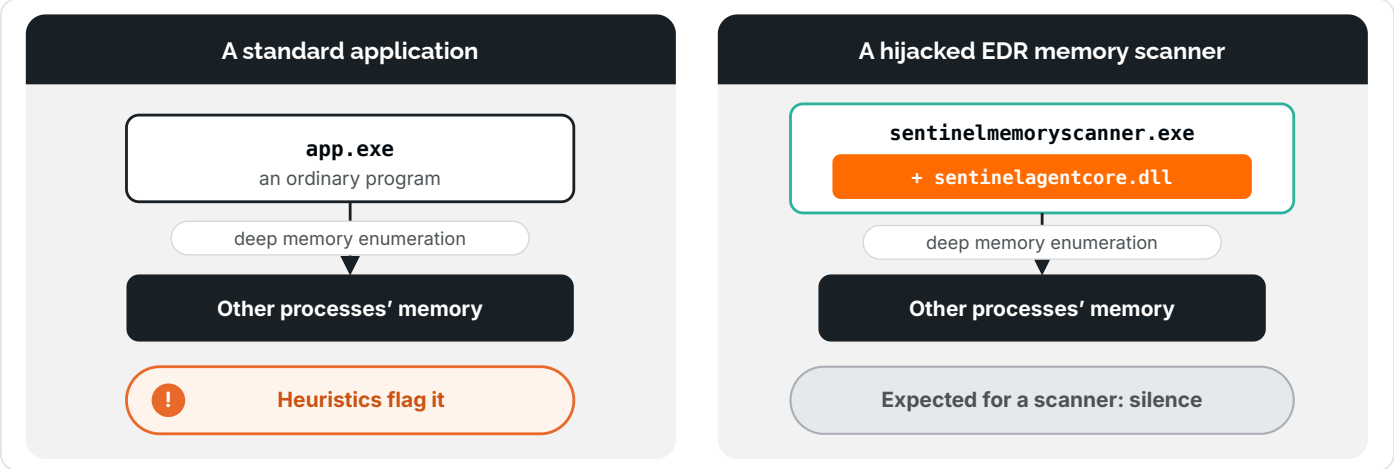

Figure 2. Why a hijacked EDR memory scanner raises no flags

03 The Execution Flow and Living Off the Land (LotL)

Following the successful execution of these malicious DLLs, MUDDYWATER extensively utilized "Living Off the Land" (LotL) techniques. Rather than dropping custom hacking tools onto the disk, they leveraged native Windows administrative utilities to conduct their operations.[5]

PowerShell was heavily leveraged to execute obfuscated scripts, perform deep network reconnaissance, capture system screenshots, and extract Security Account Manager (SAM) registry hives for privilege escalation.[6] Because tools like PowerShell and WMI (Windows Management Instrumentation) are native to the OS and universally whitelisted by traditional security controls, their abuse allows attackers to operate in plain sight, blending malicious espionage with standard IT administrative tasks.[7]

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. Cyber Crucible, internal documentation (Confluence export), 11 March 2026.
3. "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/
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. "Threat actor leverages coin miner techniques to stay under the radar – here's how to spot them," Microsoft Security Blog, accessed June 1, 2026. https://www.microsoft.com/en-us/security/blog/2020/11/30/threat-actor-leverages-coin-miner-techniques-to-stay-under-the-radar-heres-how-to-spot-them/
6. "Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks," CISA, accessed June 1, 2026. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-055a
7. Cyber Crucible, collected white papers, 24 February 2026. Published individually on the Cyber Crucible Intelligence Hub. https://www.cybercrucible.com/intelligence-hub

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 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-how-attackers-hide-in-trusted-software
Book a live technical demo: www.cybercrucible.com/demo