DeerStealer Malware Delivered Via Weaponized .LNK Using LOLBin Tools | Cryptika Cybersecurity

By Blog Writer

Published: 2025-07-22 · Archived: 2026-04-05 17:25:33 UTC

A sophisticated new phishing campaign has emerged, delivering the DeerStealer malware through weaponized .LNK shortcut files that exploit legitimate Windows binaries in a technique known as “Living off the Land” (LOLBin).

The malware masquerades as a legitimate PDF document named “Report.lnk” while covertly executing a complex multi-stage attack chain that leverages mshta.exe, a legitimate Microsoft HTML Application host utility.

The attack represents a significant evolution in malware delivery mechanisms, utilizing Microsoft’s own tools to bypass traditional security measures.

The malicious .LNK file initiates a carefully orchestrated execution sequence that progresses through multiple system binaries before ultimately deploying the DeerStealer payload.

This approach exploits the inherent trust that security systems place in legitimate operating system components, making detection substantially more challenging.

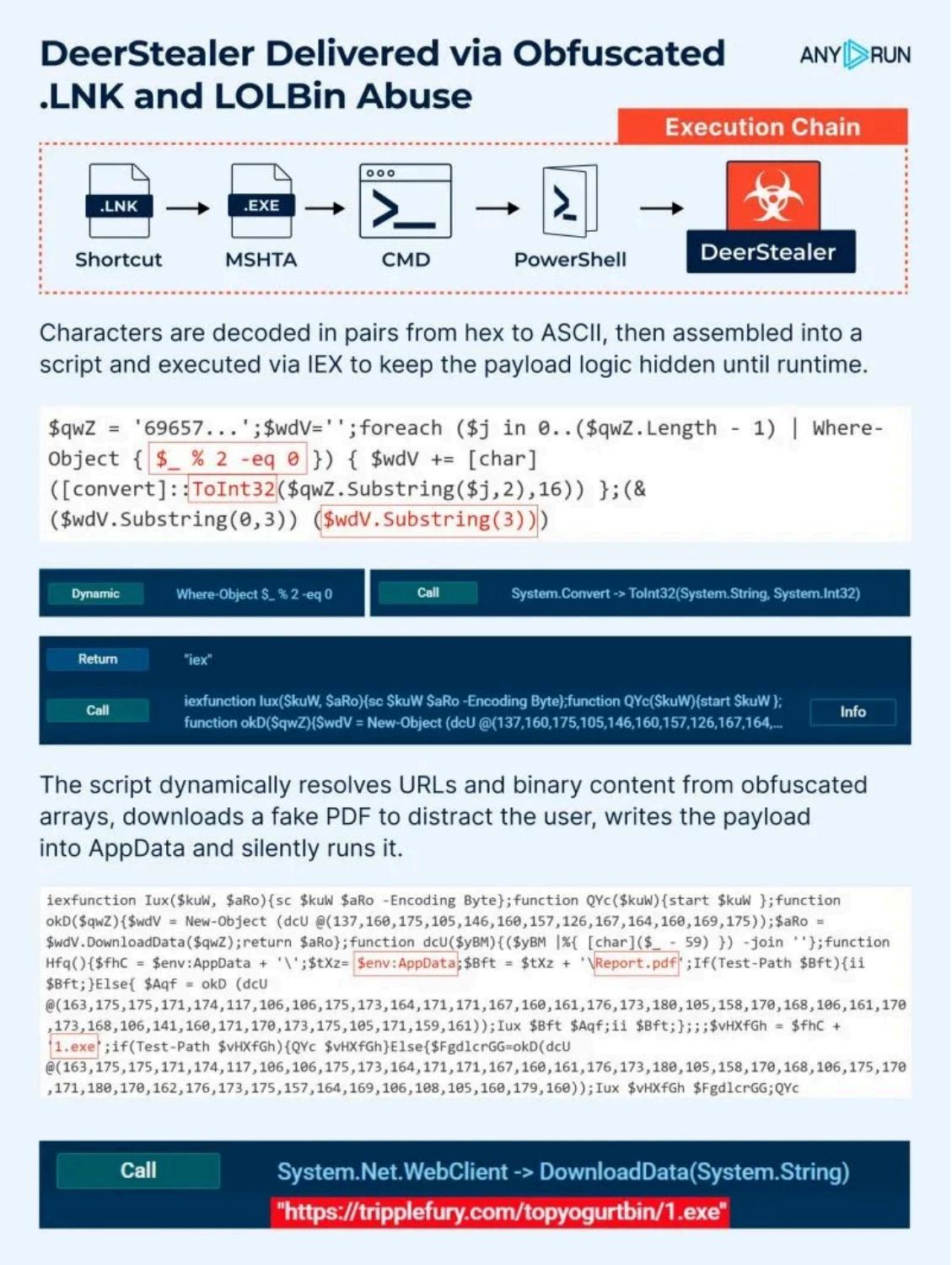
LinkedIn analysts and researchers identified this campaign as particularly concerning due to its sophisticated evasion techniques and the abuse of the MITRE ATT&CK framework technique T1218.005, which specifically covers the malicious use of mshta.exe.

The researchers noted that the attack’s reliance on dynamic path resolution and obfuscated command execution represents a notable advancement in malware sophistication.

Execution Chain and Infection Mechanism

The DeerStealer infection follows a precise five-stage execution chain: .lnk → mshta.exe → cmd.exe → PowerShell → DeerStealer.

The initial .LNK file covertly invokes mshta.exe to execute heavily obfuscated scripts using wildcard paths to evade signature-based detection systems.



DeerStealer Delivered Via Obfuscated .LNK Using LOLBin Abuse (Source – LinkedIn)

The malware dynamically resolves the full path to mshta.exe within the System32 directory, launching it with specific flags followed by obfuscated Base64 strings.

To maintain stealth during execution, both logging and profiling capabilities are disabled, significantly reducing forensic visibility.

The script employs a sophisticated character decoding mechanism where characters are processed in pairs, converted from hexadecimal to ASCII format, then reassembled into executable scripts via PowerShell's IEX

(Invoke-Expression) cmdlet.

This ensures the malicious logic remains hidden until runtime, effectively bypassing static analysis tools.

The final payload delivery involves dynamic URL resolution from obfuscated arrays, simultaneous download of a decoy PDF document to distract victims, and silent installation of the main executable into the AppData directory.

The legitimate PDF opens in Adobe Acrobat as a diversion tactic while the malware establishes persistence.

Key indicators of compromise include the domain tripplefury[.]com and SHA256 hashes fd5a2f9eed065c5767d5323b8dd928ef8724ea2edeba3e4c83e211edf9ff0160 and 8f49254064d534459b7ec60bf4e21f75284fbabfaea511268c478e15f1ed0db9.
