

## Lokibot, Software S0447 | MITRE ATT&CK®

Archived: 2026-04-05 16:10:24 UTC

Enterprise [T1548 .002 Abuse Elevation Control Mechanism](#): [Bypass User Account Control](#)

[Lokibot](#) has utilized multiple techniques to bypass UAC.<sup>[4]</sup>

Enterprise [T1071 .001 Application Layer Protocol](#): [Web Protocols](#)

[Lokibot](#) has used HTTP for C2 communications.<sup>[1][4]</sup>

Enterprise [T1059 .001 Command and Scripting Interpreter](#): [PowerShell](#)

[Lokibot](#) has used PowerShell commands embedded inside batch scripts.<sup>[4]</sup>

[.003 Command and Scripting Interpreter](#): [Windows Command Shell](#)

[Lokibot](#) has used `cmd /c` commands embedded within batch scripts.<sup>[4]</sup>

[.005 Command and Scripting Interpreter](#): [Visual Basic](#)

[Lokibot](#) has used VBS scripts and XLS macros for execution.<sup>[4]</sup>

Enterprise [T1555 Credentials from Password Stores](#)

[Lokibot](#) has stolen credentials from multiple applications and data sources including Windows OS credentials, email clients, FTP, and SFTP clients.<sup>[1]</sup>

[.003 Credentials from Web Browsers](#)

[Lokibot](#) has demonstrated the ability to steal credentials from multiple applications and data sources including Safari and the Chromium and Mozilla Firefox-based web browsers.<sup>[1]</sup>

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[Lokibot](#) has decoded and decrypted its stages multiple times using hard-coded keys to deliver the final payload, and has decoded its server response hex string using XOR.<sup>[4]</sup>

Enterprise [T1041 Exfiltration Over C2 Channel](#)

[Lokibot](#) has the ability to initiate contact with command and control (C2) to exfiltrate stolen data.<sup>[5]</sup>

Enterprise [T1083 File and Directory Discovery](#)

[Lokibot](#) can search for specific files on an infected host.<sup>[4]</sup>

Enterprise [T1564 .001 Hide Artifacts: Hidden Files and Directories](#)

[Lokibot](#) has the ability to copy itself to a hidden file and directory.<sup>[1]</sup>

Enterprise [T1070 .004 Indicator Removal: File Deletion](#)

[Lokibot](#) will delete its dropped files after bypassing UAC.<sup>[4]</sup>

Enterprise [T1105 Ingress Tool Transfer](#)

[Lokibot](#) downloaded several staged items onto the victim's machine.<sup>[4]</sup>

Enterprise [T1056 .001 Input Capture: Keylogging](#)

[Lokibot](#) has the ability to capture input on the compromised host via keylogging.<sup>[5]</sup>

Enterprise [T1112 Modify Registry](#)

[Lokibot](#) has modified the Registry as part of its UAC bypass process.<sup>[4]</sup>

Enterprise [T1106 Native API](#)

[Lokibot](#) has used LoadLibrary(), GetProcAddress() and CreateRemoteThread() API functions to execute its shellcode.<sup>[4]</sup>

Enterprise [T1027 Obfuscated Files or Information](#)

[Lokibot](#) has obfuscated strings with base64 encoding.<sup>[1]</sup>

[.002 Software Packing](#)

[Lokibot](#) has used several packing methods for obfuscation.<sup>[1]</sup>

Enterprise [T1566 .001 Phishing: Spearphishing Attachment](#)

[Lokibot](#) is delivered via a malicious XLS attachment contained within a spearphishing email.<sup>[4]</sup>

Enterprise [T1055 .012 Process Injection: Process Hollowing](#)

[Lokibot](#) has used process hollowing to inject itself into legitimate Windows process.<sup>[1][4]</sup>

Enterprise [T1620 Reflective Code Loading](#)

[Lokibot](#) has reflectively loaded the decoded DLL into memory.<sup>[4]</sup>

Enterprise [T1053 Scheduled Task/Job](#)

[Lokibot](#)'s second stage DLL has set a timer using "timeSetEvent" to schedule its next execution.<sup>[4]</sup>

[.005 Scheduled Task](#)

[Lokibot](#) embedded the commands `schtasks /Run /TN \Microsoft\Windows\DiskCleanup\SilentCleanup /I` inside a batch script.<sup>[4]</sup>

Enterprise [T1082 System Information Discovery](#)

[Lokibot](#) has the ability to discover the computer name and Windows product name/version.<sup>[5]</sup>

Enterprise [T1016 System Network Configuration Discovery](#)

[Lokibot](#) has the ability to discover the domain name of the infected host.<sup>[5]</sup>

Enterprise [T1033 System Owner/User Discovery](#)

[Lokibot](#) has the ability to discover the username on the infected host.<sup>[5]</sup>

Enterprise [T1204 .002 User Execution: Malicious File](#)

[Lokibot](#) has tricked recipients into enabling malicious macros by getting victims to click "enable content" in email attachments.<sup>[6][4]</sup>

Enterprise [T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks](#)

[Lokibot](#) has performed a time-based anti-debug check before downloading its third stage.<sup>[4]</sup>

---

Source: <https://attack.mitre.org/software/S0447/>