Netwalker, Software S0457 | MITRE ATT&CK®

Archived: 2026-04-05 16:29:57 UTC

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Netwalker has been written in PowerShell and executed directly in memory, avoiding detection.[1][2]

.003 Command and Scripting Interpreter: Windows Command Shell

Operators deploying Netwalker have used batch scripts to retrieve the Netwalker payload.[2]

Enterprise T1486 Data Encrypted for Impact

Netwalker can encrypt files on infected machines to extort victims.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Netwalker's PowerShell script can decode and decrypt multiple layers of obfuscation, leading to the Netwalker DLL being loaded into memory.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Netwalker can detect and terminate active security software-related processes on infected systems.[1][2]

Enterprise T1105 Ingress Tool Transfer

Operators deploying Netwalker have used psexec and certutil to retrieve the Netwalker payload.[2]

Enterprise T1490 Inhibit System Recovery

Netwalker can delete the infected system's Shadow Volumes to prevent recovery.[1][2]

Enterprise T1570 Lateral Tool Transfer

Operators deploying Netwalker have used psexec to copy the Netwalker payload across accessible systems.[2]

Enterprise T1112 Modify Registry

Netwalker can add the following registry entry: `HKEY_CURRENT_USER\SOFTWARE{8 random characters}` .[1]

Enterprise T1106 Native API

Netwalker can use Windows API functions to inject the ransomware DLL.[1]

Enterprise T1027 .009 Obfuscated Files or Information: Embedded Payloads

Netwalker's DLL has been embedded within the PowerShell script in hex format.[1]

.010 Obfuscated Files or Information: Command Obfuscation

Netwalker's PowerShell script has been obfuscated with multiple layers including base64 and hexadecimal encoding and XOR-encryption, as well as obfuscated PowerShell functions and variables.[1][2]

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

The Netwalker DLL has been injected reflectively into the memory of a legitimate running process.[1]

Enterprise T1489 Service Stop

Netwalker can terminate system processes and services, some of which relate to backup software.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Netwalker can detect and terminate active security software-related processes on infected systems.[1]

Enterprise T1082 System Information Discovery

Netwalker can determine the system architecture it is running on to choose which version of the DLL to use.[1]

Enterprise T1569 .002 System Services: Service Execution

Operators deploying Netwalker have used psexec and certutil to retrieve the Netwalker payload.[2]

Enterprise T1047 Windows Management Instrumentation

Netwalker can use WMI to delete Shadow Volumes.[1]
