POWERSTATS, Software S0223 | MITRE ATT&CK®

Archived: 2026-04-05 15:04:25 UTC

Enterprise T1087 .001 Account Discovery: Local Account

POWERSTATS can retrieve usernames from compromised hosts.[3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

POWERSTATS uses PowerShell for obfuscation and execution.[1][4][5][6]

.005 Command and Scripting Interpreter: Visual Basic

POWERSTATS can use VBScript (VBE) code for execution.[4][5]

.007 Command and Scripting Interpreter: JavaScript

POWERSTATS can use JavaScript code for execution.[4]

Enterprise T1132 .001 Data Encoding: Standard Encoding

POWERSTATS encoded C2 traffic with base64.[1]

Enterprise T1005 Data from Local System

POWERSTATS can upload files from compromised hosts.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

POWERSTATS can deobfuscate the main backdoor code.[4]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

POWERSTATS has encrypted C2 traffic with RSA.[3]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

POWERSTATS can disable Microsoft Office Protected View by changing Registry keys.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

POWERSTATS can delete all files on the C:\, D:\, E:\ and, F:\ drives using PowerShell Remove-Item commands.[3]

Enterprise T1105 Ingress Tool Transfer

POWERSTATS can retrieve and execute additional PowerShell payloads from the C2 server.[3]

Enterprise T1559 .001 Inter-Process Communication: Component Object Model

POWERSTATS can use DCOM (targeting the 127.0.0.1 loopback address) to execute additional payloads on compromised hosts.[3]

.002 Inter-Process Communication: Dynamic Data Exchange

POWERSTATS can use DDE to execute additional payloads on compromised hosts.[3]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

POWERSTATS has created a scheduled task named "MicrosoftEdge" to establish persistence.[4]

Enterprise T1027 .010 Obfuscated Files or Information: Command Obfuscation

POWERSTATS uses character replacement, PowerShell environment variables, and XOR encoding to obfuscate code. POWERSTATS's backdoor code is a multi-layer obfuscated, encoded, and compressed blob. [3][4]
POWERSTATS has used PowerShell code with custom string obfuscation [5]

.016 Obfuscated Files or Information: Junk Code Insertion

POWERSTATS has used useless code blocks to counter analysis.[5]

Enterprise T1057 Process Discovery

POWERSTATS has used `get_tasklist` to discover processes on the compromised host.[5]

Enterprise T1090 .002 Proxy: External Proxy

POWERSTATS has connected to C2 servers through proxies.[3]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

POWERSTATS has established persistence through a scheduled task using the command `"C:\Windows\system32\schtasks.exe" /Create /F /SC DAILY /ST 12:00 /TN MicrosoftEdge /TR "c:\Windows\system32\wscript.exe C:\Windows\temp\Windows.vbe"`.[4]

Enterprise T1029 Scheduled Transfer

POWERSTATS can sleep for a given number of seconds.[3]

Enterprise T1113 Screen Capture

POWERSTATS can retrieve screenshots from compromised hosts.[3][5]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

POWERSTATS has detected security tools.[3]

Enterprise T1218 .005 System Binary Proxy Execution: Mshta

POWERSTATS can use Mshta.exe to execute additional payloads on compromised hosts.[3]

Enterprise T1082 System Information Discovery

POWERSTATS can retrieve OS name/architecture and computer/domain name information from compromised hosts.[3][5]

Enterprise T1016 System Network Configuration Discovery

POWERSTATS can retrieve IP, network adapter configuration information, and domain from compromised hosts.[3][5]

Enterprise T1033 System Owner/User Discovery

POWERSTATS has the ability to identify the username on the compromised host.[5]

Enterprise T1047 Windows Management Instrumentation

POWERSTATS can use WMI queries to retrieve data from compromised hosts.[3][4]
