Valak, Software S0476 | MITRE ATT&CK®

Archived: 2026-04-05 12:51:02 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Valak has the ability to enumerate local admin accounts.[1]

.002 Account Discovery: Domain Account

Valak has the ability to enumerate domain admin accounts.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Valak has used HTTP in communications with C2.[1][2]

Enterprise T1119 Automated Collection

Valak can download a module to search for and build a report of harvested credential data.[3]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Valak has used PowerShell to download additional modules.[1]

.007 Command and Scripting Interpreter: JavaScript

Valak can execute JavaScript containing configuration data for establishing persistence.[1]

Enterprise T1555 .004 Credentials from Password Stores: Windows Credential Manager

Valak can use a .NET compiled module named exchgrabber to enumerate credentials from the Credential Manager.[3]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Valak has returned C2 data as encoded ASCII.[2]

Enterprise T1140 Deobfuscate/Decode Files or Information

Valak has the ability to decode and decrypt downloaded files.[1][2]

Enterprise T1114 .002 Email Collection: Remote Email Collection

Valak can collect sensitive mailing information from Exchange servers, including credentials and the domain certificate of an enterprise.[1]

Enterprise T1041 Exfiltration Over C2 Channel

Valak has the ability to exfiltrate data over the C2 channel.[1][2][3]

Enterprise T1008 Fallback Channels

Valak can communicate over multiple C2 hosts.[2]

Enterprise T1564 .004 Hide Artifacts: NTFS File Attributes

Valak has the ability save and execute files as alternate data streams (ADS).[1][2][3]

Enterprise T1105 Ingress Tool Transfer

Valak has downloaded a variety of modules and payloads to the compromised host, including IcedID and NetSupport Manager RAT-based malware.[2][1]

Enterprise T1559 .002 Inter-Process Communication: Dynamic Data Exchange

Valak can execute tasks via OLE.[3]

Enterprise T1112 Modify Registry

Valak has the ability to modify the Registry key `HKCU\Software\ApplicationContainer\Appsw64` to store information regarding the C2 server and downloads.[1][2][3]

Enterprise T1104 Multi-Stage Channels

Valak can download additional modules and malware capable of using separate C2 channels.[2]

Enterprise T1027 Obfuscated Files or Information

Valak has the ability to base64 encode and XOR encrypt strings.[1][2][3]

.002 Software Packing

Valak has used packed DLL payloads.[3]

.011 Fileless Storage

Valak has the ability to store information regarding the C2 server and downloads in the Registry key `HKCU\Software\ApplicationContainer\Appsw64`.[1][2][3]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

Valak has been delivered via spearphishing e-mails with password protected ZIP files.[2]

.002 Phishing: Spearphishing Link

Valak has been delivered via malicious links in e-mail.[3]

Enterprise T1057 Process Discovery

Valak has the ability to enumerate running processes on a compromised host.[1]

Enterprise T1012 Query Registry

Valak can use the Registry for code updates and to collect credentials.[2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Valak has used scheduled tasks to execute additional payloads and to gain persistence on a compromised host.[1][2][3]

Enterprise T1113 Screen Capture

Valak has the ability to take screenshots on a compromised host.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

Valak can determine if a compromised host has security products installed.[1]

Enterprise T1218 .010 System Binary Proxy Execution: Regsvr32

Valak has used `regsvr32.exe` to launch malicious DLLs.[1][2]

Enterprise T1082 System Information Discovery

Valak can determine the Windows version and computer name on a compromised host.[1][3]

Enterprise T1016 System Network Configuration Discovery

Valak has the ability to identify the domain and the MAC and IP addresses of an infected machine.[1]

Enterprise T1033 System Owner/User Discovery

Valak can gather information regarding the user.[1]

Enterprise T1552 .002 Unsecured Credentials: Credentials in Registry

Valak can use the clientgrabber module to steal e-mail credentials from the Registry.[3]

Enterprise T1204 .002 User Execution: Malicious File

Valak has been executed via Microsoft Word documents containing malicious macros.[1][2][3]

Enterprise T1047 Windows Management Instrumentation

Valak can use `wmic process call create` in a scheduled task to launch plugins and for execution.[3]

Source: https://attack.mitre.org/software/S0476/