POWRUNER, Software S0184 | MITRE ATT&CK®

Archived: 2026-04-05 13:34:19 UTC

Enterprise T1087 .002 Account Discovery: Domain Account

POWRUNER may collect user account information by running `net user /domain` or a series of other commands on a victim.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

POWRUNER can use HTTP for C2 communications.[1][2]

.004 Application Layer Protocol: DNS

POWRUNER can use DNS for C2 communications.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

POWRUNER is written in PowerShell.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

POWRUNER can execute commands from its C2 server.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

POWRUNER can use base64 encoded C2 communications.[1]

Enterprise T1083 File and Directory Discovery

POWRUNER may enumerate user directories on a victim.[1]

Enterprise T1105 Ingress Tool Transfer

POWRUNER can download or upload files from its C2 server.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

POWRUNER may collect local group information by running `net localgroup administrators` or a series of other commands on a victim.[1]

.002 Permission Groups Discovery: Domain Groups

POWRUNER may collect domain group information by running `net group /domain` or a series of other commands on a victim.[1]

Enterprise T1057 Process Discovery

POWRUNER may collect process information by running `tasklist` on a victim.[1]

Enterprise T1012 Query Registry

POWRUNER may query the Registry by running `reg query` on a victim.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

POWRUNER persists through a scheduled task that executes it every minute.[1]

Enterprise T1113 Screen Capture

POWRUNER can capture a screenshot from a victim.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

POWRUNER may collect information on the victim's anti-virus software.[1]

Enterprise T1082 System Information Discovery

POWRUNER may collect information about the system by running `hostname` and `systeminfo` on a victim.[1]

Enterprise T1016 System Network Configuration Discovery

POWRUNER may collect network configuration data by running `ipconfig /all` on a victim.[1]

Enterprise T1049 System Network Connections Discovery

POWRUNER may collect active network connections by running `netstat -an` on a victim.[1]

Enterprise T1033 System Owner/User Discovery

POWRUNER may collect information about the currently logged in user by running `whoami` on a victim.[1]

Enterprise T1047 Windows Management Instrumentation

POWRUNER may use WMI when collecting information about a victim.[1]
