Kwampirs, Software S0236 | MITRE ATT&CK®

Archived: 2026-04-05 15:04:50 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Kwampirs collects a list of accounts with the command `net users`.[1]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Kwampirs creates a new service named WmiApSrvEx to establish persistence.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Kwampirs decrypts and extracts a copy of its main DLL payload when executing.[1]

Enterprise T1008 Fallback Channels

Kwampirs uses a large list of C2 servers that it cycles through until a successful connection is established.[1]

Enterprise T1083 File and Directory Discovery

Kwampirs collects a list of files and directories in C:\ with the command `dir /s /a c:\ >> "C:\windows\TEMP[RANDOM].tmp"`.[1]

Enterprise T1105 Ingress Tool Transfer

Kwampirs downloads additional files from C2 servers.[3]

Enterprise T1036 .004 Masquerading: Masquerade Task or Service

Kwampirs establishes persistence by adding a new service with the display name "WMI Performance Adapter Extension" in an attempt to masquerade as a legitimate WMI service.[1]

Enterprise T1135 Network Share Discovery

Kwampirs collects a list of network shares with the command `net share`.[1]

Enterprise T1027 .001 Obfuscated Files or Information: Binary Padding

Before writing to disk, Kwampirs inserts a randomly generated string into the middle of the decrypted payload in an attempt to evade hash-based detections.[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Kwampirs downloads additional files that are base64-encoded and encrypted with another cipher.[3]

Enterprise T1201 Password Policy Discovery

Kwampirs collects password policy information with the command `net accounts`.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

Kwampirs collects a list of users belonging to the local users and administrators groups with the commands `net localgroup administrators` and `net localgroup users`.[1]

.002 Permission Groups Discovery: Domain Groups

Kwampirs collects a list of domain groups with the command `net localgroup /domain`.[1]

Enterprise T1057 Process Discovery

Kwampirs collects a list of running services with the command `tasklist /v`.[1]

Enterprise T1021 .002 Remote Services: SMB/Windows Admin Shares

Kwampirs copies itself over network shares to move laterally on a victim network.[1]

Enterprise T1018 Remote System Discovery

Kwampirs collects a list of available servers with the command `net view`.[1]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Kwampirs uses rundll32.exe in a Registry value added to establish persistence.[1]

Enterprise T1082 System Information Discovery

Kwampirs collects OS version information such as registered owner details, manufacturer details, processor type, available storage, installed patches, hostname, version info, system date, and other system information by using the commands `systeminfo`, `net config workstation`, `hostname`, `ver`, `set`, and `date /t`.[1]

Enterprise T1016 System Network Configuration Discovery

Kwampirs collects network adapter and interface information by using the commands `ipconfig /all`, `arp -a` and `route print`. It also collects the system's MAC address with `getmac` and domain configuration with `net config workstation`.[1]

Enterprise T1049 System Network Connections Discovery

Kwampirs collects a list of active and listening connections by using the command `netstat -nao` as well as a list of available network mappings with `net use`.[1]

Enterprise T1033 System Owner/User Discovery

Kwampirs collects registered owner details by using the commands `systeminfo` and `net config workstation`. [1]

Enterprise T1007 System Service Discovery

Kwampirs collects a list of running services with the command `tasklist /svc`.[1]
