Hydraq, Software S0203 | MITRE ATT&CK®

Archived: 2026-04-05 16:28:24 UTC

Enterprise T1134 Access Token Manipulation

Hydraq creates a backdoor through which remote attackers can adjust token privileges.[10]

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

Hydraq creates new services to establish persistence.[3][10][11]

Enterprise T1005 Data from Local System

Hydraq creates a backdoor through which remote attackers can read data from files.[3][10]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Hydraq C2 traffic is encrypted using bitwise NOT and XOR operations.[10]

Enterprise T1048 Exfiltration Over Alternative Protocol

Hydraq connects to a predefined domain on port 443 to exfil gathered information.[10]

Enterprise T1083 File and Directory Discovery

Hydraq creates a backdoor through which remote attackers can check for the existence of files, including its own components, as well as retrieve a list of logical drives.[3][10]

Enterprise T1070 .001 Indicator Removal: Clear Windows Event Logs

Hydraq creates a backdoor through which remote attackers can clear all system event logs.[3][10]

.004 Indicator Removal: File Deletion

Hydraq creates a backdoor through which remote attackers can delete files.[3][10]

Enterprise T1105 Ingress Tool Transfer

Hydraq creates a backdoor through which remote attackers can download files and additional malware components.[3][10]

Enterprise T1112 Modify Registry

Hydraq creates a Registry subkey to register its created service, and can also uninstall itself later by deleting this value. Hydraq's backdoor also enables remote attackers to modify and delete subkeys.[3][10]

Enterprise T1027 Obfuscated Files or Information

Hydraq uses basic obfuscation in the form of spaghetti code.[2][3]

Enterprise T1057 Process Discovery

Hydraq creates a backdoor through which remote attackers can monitor processes.[3][10]

Enterprise T1012 Query Registry

Hydraq creates a backdoor through which remote attackers can retrieve system information, such as CPU speed, from Registry keys.[3][10]

Enterprise T1113 Screen Capture

Hydraq includes a component based on the code of VNC that can stream a live feed of the desktop of an infected host.[10]

Enterprise T1129 Shared Modules

Hydraq creates a backdoor through which remote attackers can load and call DLL functions.[3][10]

Enterprise T1082 System Information Discovery

Hydraq creates a backdoor through which remote attackers can retrieve information such as computer name, OS version, processor speed, memory size, and CPU speed.[10]

Enterprise T1016 System Network Configuration Discovery

Hydraq creates a backdoor through which remote attackers can retrieve IP addresses of compromised machines.[3][10]

Enterprise T1007 System Service Discovery

Hydraq creates a backdoor through which remote attackers can monitor services.[3][10]

Enterprise T1569 .002 System Services: Service Execution

Hydraq uses svchost.exe to execute a malicious DLL included in a new service group.[11]
