

Diavol, Software S0659 | MITRE ATT&CK®

Archived: 2026-04-05 17:59:12 UTC

Enterprise [T1071 .001 Application Layer Protocol: Web Protocols](#)

[Diavol](#) has used HTTP GET and POST requests for C2.^[1]

Enterprise [T1485 Data Destruction](#)

[Diavol](#) can delete specified files from a targeted system.^[1]

Enterprise [T1486 Data Encrypted for Impact](#)

[Diavol](#) has encrypted files using an RSA key though the `CryptEncrypt` API and has appended filenames with ".lock64".^[1]

Enterprise [T1491 .001 Defacement: Internal Defacement](#)

After encryption, [Diavol](#) will capture the desktop background window, set the background color to black, and change the desktop wallpaper to a newly created bitmap image with the text "All your files are encrypted! For more information see "README-FOR-DECRYPT.txt".^[1]

Enterprise [T1083 File and Directory Discovery](#)

[Diavol](#) has a command to traverse the files and directories in a given path.^[1]

Enterprise [T1562 .001 Impair Defenses: Disable or Modify Tools](#)

[Diavol](#) can attempt to stop security software.^[1]

Enterprise [T1105 Ingress Tool Transfer](#)

[Diavol](#) can receive configuration updates and additional payloads including wscopy.exe from C2.^[1]

Enterprise [T1490 Inhibit System Recovery](#)

[Diavol](#) can delete shadow copies using the `IVssBackupComponents` COM object to call the `DeleteSnapshots` method.^[1]

Enterprise [T1106 Native API](#)

[Diavol](#) has used several API calls like `GetLogicalDriveStrings` , `SleepEx` , `SystemParametersInfoAPI` , `CryptEncrypt` , and others to execute parts of its attack.^[1]

Enterprise [T1135 Network Share Discovery](#)

[Diavol](#) has a `ENMDSKS` command to enumerates available network shares.^[1]

Enterprise [T1027 Obfuscated Files or Information](#)

[Diavol](#) has Base64 encoded the RSA public key used for encrypting files.^[1]

[.003 Steganography](#)

[Diavol](#) has obfuscated its main code routines within bitmap images as part of its anti-analysis techniques.^[1]

Enterprise [T1057 Process Discovery](#)

[Diavol](#) has used `CreateToolhelp32Snapshot` , `Process32First` , and `Process32Next` API calls to enumerate the running processes in the system.^[1]

Enterprise [T1021 .002 Remote Services: SMB/Windows Admin Shares](#)

[Diavol](#) can spread throughout a network via SMB prior to encryption.^[1]

Enterprise [T1018 Remote System Discovery](#)

[Diavol](#) can use the ARP table to find remote hosts to scan.^[1]

Enterprise [T1489 Service Stop](#)

[Diavol](#) will terminate services using the Service Control Manager (SCM) API.^[1]

Enterprise [T1082 System Information Discovery](#)

[Diavol](#) can collect the computer name and OS version from the system.^[1]

Enterprise [T1016 System Network Configuration Discovery](#)

[Diavol](#) can enumerate victims' local and external IPs when registering with C2.^[1]

Enterprise [T1033 System Owner/User Discovery](#)

[Diavol](#) can collect the username from a compromised host.^[1]

Source: <https://attack.mitre.org/software/S0659>