Denis, Software S0354 | MITRE ATT&CK®

Archived: 2026-04-02 10:39:46 UTC

Enterprise T1071 .004 Application Layer Protocol: DNS

Denis has used DNS tunneling for C2 communications.[1][2][3]

Enterprise T1560 .002 Archive Collected Data: Archive via Library

Denis compressed collected data using zlib.[2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Denis has a version written in PowerShell.[3]

.003 Command and Scripting Interpreter: Windows Command Shell

Denis can launch a remote shell to execute arbitrary commands on the victim’s machine.[1][3]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Denis encodes the data sent to the server in Base64.[3]

Enterprise T1140 Deobfuscate/Decode Files or Information

Denis will decrypt important strings used for C&C communication.[3]

Enterprise T1083 File and Directory Discovery

Denis has several commands to search directories for files.[1][3]

Enterprise T1574 Hijack Execution Flow

Denis replaces the nonexistent Windows DLL "msfte.dll" with its own malicious version, which is loaded by the SearchIndexer.exe and SearchProtocolHost.exe.[3]

.001 DLL

Denis exploits a security vulnerability to load a fake DLL and execute its code.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Denis has a command to delete files from the victim’s machine.[1][3]

Enterprise T1105 Ingress Tool Transfer

Denis deploys additional backdoors and hacking tools to the system.[3]

Enterprise T1106 Native API

Denis used the `IsDebuggerPresent`, `OutputDebugString`, and `SetLastError` APIs to avoid debugging. Denis used `GetProcAddress` and `LoadLibrary` to dynamically resolve APIs. Denis also used the `Wow64SetThreadContext` API as part of a process hollowing process.[3]

Enterprise T1027 Obfuscated Files or Information

Denis obfuscates its code and encrypts the API names.[3]

.010 Command Obfuscation

Denis has encoded its PowerShell commands in Base64.[3]

Enterprise T1055 .012 Process Injection: Process Hollowing

Denis performed process hollowing through the API calls CreateRemoteThread, ResumeThread, and Wow64SetThreadContext.[3]

Enterprise T1012 Query Registry

Denis queries the Registry for keys and values.[3]

Enterprise T1082 System Information Discovery

Denis collects OS information and the computer name from the victim's machine.[2][3]

Enterprise T1016 System Network Configuration Discovery

Denis uses `ipconfig` to gather the IP address from the system.[3]

Enterprise T1033 System Owner/User Discovery

Denis enumerates and collects the username from the victim's machine.[2][3]

Enterprise T1497 .001 Virtualization/Sandbox Evasion: System Checks

Denis ran multiple system checks, looking for processor and register characteristics, to evade emulation and analysis.[3]
