Milan, Software S1015 | MITRE ATT&CK®

Archived: 2026-04-05 17:17:21 UTC

Enterprise T1087 .001 Account Discovery: Local Account

Milan has run `C:\Windows\system32\cmd.exe /c cmd /c dir c:\users\ /s 2>&1` to discover local accounts.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Milan can use HTTPS for communication with C2.[1][2][3]

.004 Application Layer Protocol: DNS

Milan has the ability to use DNS for C2 communications.[1][2][3]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

Milan can use `cmd.exe` for discovery actions on a targeted system.[1]

Enterprise T1005 Data from Local System

Milan can upload files from a compromised host.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

Milan has saved files prior to upload from a compromised host to folders beginning with the characters `a9850d2f`.[1]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

Milan can use hardcoded domains as an input for domain generation algorithms.[3]

Enterprise T1070 .004 Indicator Removal: File Deletion

Milan can delete files via `C:\Windows\system32\cmd.exe /c ping 1.1.1.1 -n 1 -w 3000 > Nul & rmdir /s /q`.[1]

Enterprise T1105 Ingress Tool Transfer

Milan has received files from C2 and stored them in log folders beginning with the character sequence `a9850d2f`.[1]

Enterprise T1559 .001 Inter-Process Communication: Component Object Model

Milan can use a COM component to generate scheduled tasks.[1]

Enterprise T1036 Masquerading

Milan has used an executable named `companycatalogue` to appear benign.[1]

.007 Double File Extension

Milan has used an executable named `companycatalog.exe.config` to appear benign.[1]

Enterprise T1106 Native API

Milan can use the API `DnsQuery_A` for DNS resolution.[2]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Milan can encode files containing information about the targeted system.[1][2]

Enterprise T1572 Protocol Tunneling

Milan can use a custom protocol tunneled through DNS or HTTP.[2]

Enterprise T1012 Query Registry

Milan can query `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography MachineGuid` to retrieve the machine GUID.[3]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Milan can establish persistence on a targeted host with scheduled tasks.[1][3]

Enterprise T1082 System Information Discovery

Milan can enumerate the targeted machine's name and GUID.[1][3]

Enterprise T1016 System Network Configuration Discovery

Milan can run `C:\Windows\system32\cmd.exe /c cmd /c ipconfig /all 2>&1` to discover network settings.[1]

Enterprise T1033 System Owner/User Discovery

Milan can identify users registered to a targeted machine.[1]
