

Proxysvc, Software S0238 | MITRE ATT&CK®

Archived: 2026-04-05 12:37:35 UTC

Domain	ID	Name	Use
Enterprise	T1071	.001 Application Layer Protocol: Web Protocols	Proxysvc uses HTTP over SSL to communicate commands with the control server. ^[1]
Enterprise	T1119	Automated Collection	Proxysvc automatically collects data about the victim and sends it to the control server. ^[1]
Enterprise	T1059	.003 Command and Scripting Interpreter: Windows Command Shell	Proxysvc executes a binary on the system and logs the results into a temp file by using: <code>cmd.exe /c " > %temp%\PM* .tmp 2>&1" .</code> ^[1]
Enterprise	T1485	Data Destruction	Proxysvc can overwrite files indicated by the attacker before deleting them. ^[1]
Enterprise	T1005	Data from Local System	Proxysvc searches the local system and gathers data. ^[1]
Enterprise	T1041	Exfiltration Over C2 Channel	Proxysvc performs data exfiltration over the control server channel using a custom protocol. ^[1]
Enterprise	T1083	File and Directory Discovery	Proxysvc lists files in directories. ^[1]
Enterprise	T1070	.004 Indicator Removal: File Deletion	Proxysvc can delete files indicated by the attacker and remove itself from disk using a batch file. ^[1]

Domain	ID	Name	Use
Enterprise	T1680	Local Storage Discovery	Proxysvc collects volume information for all drives on the system. ^[1]
Enterprise	T1057	Process Discovery	Proxysvc lists processes running on the system. ^[1]
Enterprise	T1012	Query Registry	Proxysvc gathers product names from the Registry key: <code>HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProductName</code> and the processor description from the Registry key <code>HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString</code> . ^[1]
Enterprise	T1082	System Information Discovery	Proxysvc collects the OS version, country name, MAC address, computer name, and physical memory statistics. ^[1]
Enterprise	T1016	System Network Configuration Discovery	Proxysvc collects the network adapter information and domain/username information based on current remote sessions. ^[1]
Enterprise	T1569	.002 System Services: Service Execution	Proxysvc registers itself as a service on the victim's machine to run as a standalone process. ^[1]
Enterprise	T1124	System Time Discovery	As part of the data reconnaissance phase, Proxysvc grabs the system time to send back to the control server. ^[1]

Source: https://attack.mitre.org/software/S0238/