HTTPBrowser, Software S0070 | MITRE ATT&CK®

Archived: 2026-04-05 15:14:44 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	HTTPBrowser has used HTTP and HTTPS for command and control.[2][1]
		.004	Application Layer Protocol: DNS	HTTPBrowser has used DNS for command and control.[2][1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	HTTPBrowser has established persistence by setting the `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` key value for `wdm` to the path of the executable. It has also used the Registry entry `HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run vpdn "%ALLUSERPROFILE%\%APPDATA%\vpdn\VPDN_LU.exe"` to establish persistence.[4][1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	HTTPBrowser is capable of spawning a reverse shell on a victim.[2]
Enterprise	T1083		File and Directory Discovery	HTTPBrowser is capable of listing files, folders, and drives on a victim.[2][4]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	HTTPBrowser abuses the Windows DLL load order by using a legitimate Symantec anti-virus binary, VPDN_LU.exe, to load a malicious DLL that mimics a legitimate Symantec DLL, navlu.dll.[4] HTTPBrowser has also used DLL side-loading.[2]

Domain	ID		Name	Use
Enterprise	T1070	.004	Indicator Removal: File Deletion	HTTPBrowser deletes its original installer file once installation is complete.[4]
Enterprise	T1105		Ingress Tool Transfer	HTTPBrowser is capable of writing a file to the compromised system from the C2 server.[2]
Enterprise	T1056	.001	Input Capture: Keylogging	HTTPBrowser is capable of capturing keystrokes on victims.[2]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	HTTPBrowser's installer contains a malicious file named navlu.dll to decrypt and run the RAT. navlu.dll is also the name of a legitimate Symantec DLL.[4]
Enterprise	T1027		Obfuscated Files or Information	HTTPBrowser's code may be obfuscated through structured exception handling and return-oriented programming.[2]

Source: https://attack.mitre.org/software/S0070