Masquerading: Rename Legitimate Utilities, Sub-technique T1036.003 - Enterprise

Archived: 2026-04-05 15:37:39 UTC

ID	Name	Description
G0050	APT32	APT32 has moved and renamed pubprn.vbs to a .txt file to avoid detection.[7]
G0082	APT38	APT38 has renamed system utilities, such as `rundll32.exe` and `mshta.exe`, to avoid detection.[8]
S0046	CozyCar	The CozyCar dropper has masqueraded a copy of the infected system's rundll32.exe executable that was moved to the malware's install directory and renamed according to a predefined configuration file.[6]
G1034	Daggerfly	Daggerfly used a renamed version of rundll32.exe, such as "dbengin.exe" located in the `ProgramData\Microsoft\PlayReady` directory, to proxy malicious DLL execution.[9]
S1111	DarkGate	DarkGate executes a Windows Batch script during installation that creases a randomly-named directory in the `C:\` root directory that copies and renames the legitimate Windows curl command to this new location.[10]
G0093	GALLIUM	GALLIUM used a renamed cmd.exe file to evade detection.[11]
S1020	Kevin	Kevin has renamed an image of `cmd.exe` with a random name followed by a `.tmpl` extension.[12]
G0032	Lazarus Group	Lazarus Group has renamed system utilities such as `wscript.exe` and `mshta.exe`.[13]

ID	Name	Description
G0045	menuPass	menuPass has renamed certutil and moved it to a different location on the system to avoid detection based on use of the tool.[14]
S1183	StrelaStealer	StrelaStealer has used a renamed, legitimate `msinfo32.exe` executable to sideload the StrelaStealer payload during initial installation.[15]

Source: https://attack.mitre.org/techniques/T1036/003