SplatCloak, Software S1234 | MITRE ATT&CK®

Archived: 2026-04-05 14:43:38 UTC

Domain	ID		Name	Use
Enterprise	T1083		File and Directory Discovery	SplatCloak has used Windows API to identify files associated with Windows Defender and Kaspersky.[1]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	SplatCloak has identified and disabled API callback features of Windows Defender and Kaspersky.[1]
Enterprise	T1036	.001	Masquerading: Invalid Code Signature	SplatCloak has used a revoked certificate to exploit Windows driver execution policy where certificates issued before a specific date could still load.[1]
Enterprise	T1106		Native API	SplatCloak has utilized Native Windows API calls dynamically through `ZwQuerySystemInformation`.[1]
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	SplatCloak has identified drivers of AV solutions by searching for related filenames, keywords and signed certificates.[1]
Enterprise	T1082		System Information Discovery	SplatCloak has collected the Windows build number using the windows kernel API `RtlGetVersion` to determine if the response is 19000 or higher (Windows 10 version 2004 or later).[1]