Sibot, Software S0589 | MITRE ATT&CK®

Archived: 2026-04-05 16:09:08 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Sibot communicated with its C2 server via HTTP GET requests.[1]
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	Sibot executes commands using VBScript.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Sibot can decrypt data received from a C2 and save to a file.[1]
Enterprise	T1070		Indicator Removal	Sibot will delete an associated registry key if a certain server response is received.[1]
		.004	File Deletion	Sibot will delete itself if a certain server response is received.[1]
Enterprise	T1105		Ingress Tool Transfer	Sibot can download and execute a payload onto a compromised system.[1]
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	Sibot has downloaded a DLL to the `C:\windows\system32\drivers\` fold and renamed it with a `.sys` extension.[1]
Enterprise	T1112		Modify Registry	Sibot has modified the Registry to install a second-stage script in the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\sibo` [1]
Enterprise	T1027	.010	Obfuscated Files or Information: Command Obfuscation	Sibot has obfuscated scripts used in execution.[1]
		.011	Obfuscated Files or Information: Fileless Storage	Sibot has installed a second-stage script in the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\sibo` registry key.[1]

Domain	ID		Name	Use
Enterprise	T1012		Query Registry	Sibot has queried the registry for proxy server information.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Sibot has been executed via a scheduled task.[1]
Enterprise	T1218	.005	System Binary Proxy Execution: Mshta	Sibot has been executed via MSHTA application.[1]
		.011	System Binary Proxy Execution: Rundll32	Sibot has executed downloaded DLLs with `rundll32.exe`.[1]
Enterprise	T1016		System Network Configuration Discovery	Sibot checked if the compromised system is configured to use proxies.[1]
Enterprise	T1049		System Network Connections Discovery	Sibot has retrieved a GUID associated with a present LAN connection on a compromised machine.[1]
Enterprise	T1102		Web Service	Sibot has used a legitimate compromised website to download DLLs to the victim's machine.[1]
Enterprise	T1047		Windows Management Instrumentation	Sibot has used WMI to discover network connections and configurations. Sibot has also used the Win32_Process class to execute a malicious DLL.[

Source: https://attack.mitre.org/software/S0589/