STARWHALE, Software S1037 | MITRE ATT&CK®

Archived: 2026-04-05 17:04:16 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	STARWHALE has the ability to contact actor-controlled C2 servers via HTTP.[1][2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	STARWHALE can establish persistence by installing itself in the startup folder, whereas the GO variant has created a `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\OutlookM` registry key.[2][1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	STARWHALE has the ability to execute commands via `cmd.exe`. [1]
		.005	Command and Scripting Interpreter: Visual Basic	STARWHALE can use the VBScript function `GetRef` as part of its persistence mechanism.[1]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	STARWHALE has the ability to create the following Windows service to establish persistence on an infected host: `sc create Windowscarpstss binpath= "cmd.exe /c cscript.exe c:\\windows\\system32\\w7_1.wsf humpback_whale" start= "auto" obj= "LocalSystem"` .[1]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	STARWHALE has the ability to hex-encode collected data from an infected host.[2]
Enterprise	T1005		Data from Local System	STARWHALE can collect data from an infected local host.[2]
Enterprise	T1074	.001	Data Staged: Local Data Staging	STARWHALE has stored collected data in a file called `stari.txt` .[1]

Domain	ID		Name	Use
Enterprise	T1041		Exfiltration Over C2 Channel	STARWHALE can exfiltrate collected data to its C2 servers.[2]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	STARWHALE has been obfuscated with hex-encoded strings.[2]
Enterprise	T1082		System Information Discovery	STARWHALE can gather the computer name of an infected host.[1] [2]
Enterprise	T1016		System Network Configuration Discovery	STARWHALE has the ability to collect the IP address of an infected host.[2]
Enterprise	T1033		System Owner/User Discovery	STARWHALE can gather the username from an infected host.[1][2]
Enterprise	T1204	.002	User Execution: Malicious File	STARWHALE has relied on victims opening a malicious Excel file for execution.[2]

Source: https://attack.mitre.org/software/S1037