GRIFFON, Software S0417 | MITRE ATT&CK®

Archived: 2026-04-05 13:45:03 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	GRIFFON has used a persistence module that stores the implant inside the Registry, which executes at logon.[1]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	GRIFFON has used PowerShell to execute the Meterpreter downloader TinyMet.[1]
		.007	Command and Scripting Interpreter: JavaScript	GRIFFON is written in and executed as JavaScript.[1]
Enterprise	T1069	.002	Permission Groups Discovery: Domain Groups	GRIFFON has used a reconnaissance module that can be used to retrieve Windows domain membership information.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	GRIFFON has used `sctasks` for persistence.[1]
Enterprise	T1113		Screen Capture	GRIFFON has used a screenshot module that can be used to take a screenshot of the remote system.[1]
Enterprise	T1082		System Information Discovery	GRIFFON has used a reconnaissance module that can be used to retrieve information about a victim's computer, including the resolution of the workstation .[1]
Enterprise	T1124		System Time Discovery	GRIFFON has used a reconnaissance module that can be used to retrieve the date and time of

Domain	ID	Name	Use
			the system.[1]

Source: https://attack.mitre.org/software/S0417/