FIN10, Group G0051 | MITRE ATT&CK®

Archived: 2026-04-05 13:39:09 UTC

Domain	ID		Name	Use
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	FIN10 has established persistence by using the Registry option in PowerShell Empire to add a Run key.[1][2]
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	FIN10 uses PowerShell for execution as well as PowerShell Empire to establish persistence.[1][2]
		.003	Command and Scripting Interpreter: Windows Command Shell	FIN10 has executed malicious .bat files containing PowerShell commands.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	FIN10 has used batch scripts and scheduled tasks to delete critical system files.[1]
Enterprise	T1570		Lateral Tool Transfer	FIN10 has deployed Meterpreter stagers and SplinterRAT instances in the victim network after moving laterally.[1]
Enterprise	T1588	.002	Obtain Capabilities: Tool	FIN10 has relied on publicly-available software to gain footholds and establish persistence in victim environments.[1]
Enterprise	T1021	.001	Remote Services: Remote Desktop Protocol	FIN10 has used RDP to move laterally to systems in the victim environment.[1]

Domain	ID		Name	Use
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	FIN10 has established persistence by using S4U tasks as well as the Scheduled Task option in PowerShell Empire.[1][2]
Enterprise	T1033		System Owner/User Discovery	FIN10 has used Meterpreter to enumerate users on remote systems.[1]
Enterprise	T1078		Valid Accounts	FIN10 has used stolen credentials to connect remotely to victim networks using VPNs protected with only a single factor.[1]
		.003	Local Accounts	FIN10 has moved laterally using the Local Administrator account.[1]

Source: https://attack.mitre.org/groups/G0051/