FIN5, Group G0053 | MITRE ATT&CK®

Archived: 2026-04-05 14:23:31 UTC

Domain	ID		Name	Use
Enterprise	T1119		Automated Collection	FIN5 scans processes on all victim systems in the environment and uses automated scripts to pull back the results.[2]
Enterprise	T1110		Brute Force	FIN5 has has used the tool GET2 Penetrator to look for remote login and hard-coded credentials.[3][2]
Enterprise	T1059		Command and Scripting Interpreter	FIN5 scans processes on all victim systems in the environment and uses automated scripts to pull back the results.[2]
Enterprise	T1074	.001	Data Staged: Local Data Staging	FIN5 scripts save memory dump data into a specific directory on hosts in the victim environment.[2]
Enterprise	T1133		External Remote Services	FIN5 has used legitimate VPN, Citrix, or VNC credentials to maintain access to a victim environment.[1][3][2]
Enterprise	T1070	.001	Indicator Removal: Clear Windows Event Logs	FIN5 has cleared event logs from victims.[2]
		.004	Indicator Removal: File Deletion	FIN5 uses SDelete to clean up the environment and attempt to prevent detection.[2]
Enterprise	T1588	.002	Obtain Capabilities: Tool	FIN5 has obtained and used a customized version of PsExec, as well as use other tools such as

Domain	ID		Name	Use
				pwdump, SDelete, and Windows Credential Editor. [2]
Enterprise	T1090	.002	Proxy: External Proxy	FIN5 maintains access to victim environments by using FLIPSIDE to create a proxy for a backup RDP tunnel.[2]
Enterprise	T1018		Remote System Discovery	FIN5 has used the open source tool Essential NetTools to map the network and build a list of targets.[2]
Enterprise	T1078		Valid Accounts	FIN5 has used legitimate VPN, RDP, Citrix, or VNC credentials to maintain access to a victim environment.[1][3][2]

Source: https://attack.mitre.org/groups/G0053