GOLD SOUTHFIELD, Pinchy Spider, Group G0115

Archived: 2026-04-05 17:56:27 UTC

Domain	ID		Name	Use
Enterprise	T1059	.001	Command and Scripting Interpreter: PowerShell	GOLD SOUTHFIELD has staged and executed PowerShell scripts on compromised hosts.[5]
Enterprise	T1190		Exploit Public-Facing Application	GOLD SOUTHFIELD has exploited Oracle WebLogic vulnerabilities for initial compromise.[1]
Enterprise	T1133		External Remote Services	GOLD SOUTHFIELD has used publicly-accessible RDP and remote management and monitoring (RMM) servers to gain access to victim machines.[1]
Enterprise	T1027	.010	Obfuscated Files or Information: Command Obfuscation	GOLD SOUTHFIELD has executed base64 encoded PowerShell scripts on compromised hosts.[5]
Enterprise	T1566		Phishing	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines.[1]
Enterprise	T1219		Remote Access Tools	GOLD SOUTHFIELD has used the cloud-based remote management and monitoring tool "ConnectWise Control" to deploy REvil.[5]
Enterprise	T1113		Screen Capture	GOLD SOUTHFIELD has used the remote monitoring and management tool ConnectWise to obtain screen captures from victim's machines.[5]

Domain	ID		Name	Use
Enterprise	T1195	.002	Supply Chain Compromise: Compromise Software Supply Chain	GOLD SOUTHFIELD has distributed ransomware by backdooring software installers via a strategic web compromise of the site hosting Italian WinRAR.[1][2][3]
Enterprise	T1199		Trusted Relationship	GOLD SOUTHFIELD has breached Managed Service Providers (MSP's) to deliver malware to MSP customers.[1]

Source: https://attack.mitre.org/groups/G0115