

FIN4, Group G0085 | MITRE ATT&CK®

Archived: 2026-04-05 15:10:22 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	FIN4 has used HTTP POST requests to transmit data. [1][3]
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	FIN4 has used VBA macros to display a dialog box and collect victim credentials. [1][3]
Enterprise	T1114	.002	Email Collection: Remote Email Collection	FIN4 has accessed and hijacked online email communications using stolen credentials. [1][3]
Enterprise	T1564	.008	Hide Artifacts: Email Hiding Rules	FIN4 has created rules in victims' Microsoft Outlook accounts to automatically delete emails containing words such as "hacked," "phish," and "malware" in a likely attempt to prevent organizations from communicating about their activities. [1]
Enterprise	T1056	.001	Input Capture: Keylogging	FIN4 has captured credentials via fake Outlook Web App (OWA) login pages and has also used a .NET based keylogger. [1][3]
		.002	Input Capture: GUI Input Capture	FIN4 has presented victims with spoofed Windows Authentication prompts to collect their credentials. [1][3]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	FIN4 has used spearphishing emails containing attachments (which are often stolen, legitimate documents sent from compromised accounts) with embedded malicious macros. [1][3]

Domain	ID	Name	Use
		Phishing: Spearphishing Link	FIN4 has used spearphishing emails (often sent from compromised accounts) containing malicious links. ^[1] ^[3]
Enterprise	T1090	Proxy: Multi-hop Proxy	FIN4 has used Tor to log in to victims' email accounts. ^[1]
Enterprise	T1204	User Execution: Malicious Link	FIN4 has lured victims to click malicious links delivered via spearphishing emails (often sent from compromised accounts). ^[1] ^[3]
		User Execution: Malicious File	FIN4 has lured victims to launch malicious attachments delivered via spearphishing emails (often sent from compromised accounts). ^[1] ^[3]
Enterprise	T1078	Valid Accounts	FIN4 has used legitimate credentials to hijack email communications. ^[1] ^[3]

Source: https://attack.mitre.org/groups/G0085