DanBot, Software S1014 | MITRE ATT&CK®

Archived: 2026-04-05 18:23:22 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	DanBot can use HTTP in C2 communication.[1]
		.004	Application Layer Protocol: DNS	DanBot can use use IPv4 A records and IPv6 AAAA DNS records in C2 communications.[1]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	DanBot has the ability to execute arbitrary commands via `cmd.exe`.[1][2]
		.005	Command and Scripting Interpreter: Visual Basic	DanBot can use a VBA macro embedded in an Excel file to drop the payload.[1]
Enterprise	T1005		Data from Local System	DanBot can upload files from compromised hosts.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	DanBot can use a VBA macro to decode its payload prior to installation and execution.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	DanBot can delete its configuration file after installation.[2]
Enterprise	T1105		Ingress Tool Transfer	DanBot can download additional files to a targeted system.[1]

Domain	ID		Name	Use
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	DanBot files have been named `UltraVNC.exe` and `WINVNC.exe` to appear as legitimate VNC tools.[2]
Enterprise	T1027	.013	Obfuscated Files or Information: Encrypted/Encoded File	DanBot can Base64 encode its payload.[1]
Enterprise	T1566	.001	Phishing: Spearphishing Attachment	DanBot has been distributed within a malicious Excel attachment via spearphishing emails.[1]
Enterprise	T1021	.005	Remote Services: VNC	DanBot can use VNC for remote access to targeted systems.[2]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	DanBot can use a scheduled task for installation.[1]
Enterprise	T1204	.002	User Execution: Malicious File	DanBot has relied on victims' opening a malicious file for initial execution.[1][2]

Source: https://attack.mitre.org/software/S1014