MiniDuke, Software S0051 | MITRE ATT&CK®

Archived: 2026-04-02 10:47:35 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	MiniDuke uses HTTP and HTTPS for command and control.[1][2]
Enterprise	T1568	.002	Dynamic Resolution: Domain Generation Algorithms	MiniDuke can use DGA to generate new Twitter URLs for C2.[2]
Enterprise	T1008		Fallback Channels	MiniDuke uses Google Search to identify C2 servers if its primary C2 method via Twitter is not working.[3]
Enterprise	T1083		File and Directory Discovery	MiniDuke can enumerate local drives.[2]
Enterprise	T1105		Ingress Tool Transfer	MiniDuke can download additional encrypted backdoors onto the victim via GIF files.[3][2]
Enterprise	T1027		Obfuscated Files or Information	MiniDuke can use control flow flattening to obscure code.[2]
Enterprise	T1090	.001	Proxy: Internal Proxy	MiniDuke can can use a named pipe to forward communications from one compromised machine with internet access to other compromised machines.[2]
Enterprise	T1082		System Information Discovery	MiniDuke can gather the hostname on a compromised machine.[2]

Domain	ID		Name	Use
Enterprise	T1102	.001	Web Service: Dead Drop Resolver	Some MiniDuke components use Twitter to initially obtain the address of a C2 server or as a backup if no hard-coded C2 server responds.[1][3][2]

Source: https://attack.mitre.org/software/S0051/