PolyglotDuke, Software S0518 | MITRE ATT&CK®

Archived: 2026-04-05 14:30:19 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	PolyglotDuke has has used HTTP GET requests in C2 communications.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	PolyglotDuke can use a custom algorithm to decrypt strings used by the malware.[1]
Enterprise	T1105		Ingress Tool Transfer	PolyglotDuke can retrieve payloads from the C2 server.[1]
Enterprise	T1112		Modify Registry	PolyglotDuke can write encrypted JSON configuration files to the Registry.[1]
Enterprise	T1106		Native API	PolyglotDuke can use `LoadLibraryW` and `CreateProcess` to load and execute code.[1]
Enterprise	T1027		Obfuscated Files or Information	PolyglotDuke can custom encrypt strings.[1]
		.003	Steganography	PolyglotDuke can use steganography to hide C2 information in images.[1]
		.011	Fileless Storage	PolyglotDuke can store encrypted JSON configuration files in the Registry.[1]
Enterprise	T1218	.011	System Binary Proxy Execution: Rundll32	PolyglotDuke can be executed using rundll32.exe.[1]

Domain	ID		Name	Use
Enterprise	T1102	.001	Web Service: Dead Drop Resolver	PolyglotDuke can use Twitter, Reddit, Imgur and other websites to get a C2 URL.[1]

Source: https://attack.mitre.org/software/S0518