LiteDuke, Software S0513 | MITRE ATT&CK®

Archived: 2026-04-05 14:32:35 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	LiteDuke can use HTTP GET requests in C2 communications.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	LiteDuke can create persistence by adding a shortcut in the `CurrentVersion\Run` Registry key.[1]
Enterprise	T1140		Deobfuscate/Decode Files or Information	LiteDuke has the ability to decrypt and decode multiple layers of obfuscation.[1]
Enterprise	T1070	.004	Indicator Removal: File Deletion	LiteDuke can securely delete files by first writing random data to the file.[1]
Enterprise	T1105		Ingress Tool Transfer	LiteDuke has the ability to download files. [1]
Enterprise	T1027	.002	Obfuscated Files or Information: Software Packing	LiteDuke has been packed with multiple layers of encryption.[1]
		.003	Obfuscated Files or Information: Steganography	LiteDuke has used image files to hide its loader component.[1]
Enterprise	T1012		Query Registry	LiteDuke can query the Registry to check for the presence of `HKCU\Software\KasperskyLab`.[1]

Domain	ID		Name	Use
Enterprise	T1518	.001	Software Discovery: Security Software Discovery	LiteDuke has the ability to check for the presence of Kaspersky security software. [1]
Enterprise	T1082		System Information Discovery	LiteDuke can enumerate the CPUID and BIOS version on a compromised system. [1]
Enterprise	T1016		System Network Configuration Discovery	LiteDuke has the ability to discover the proxy configuration of Firefox and/or Opera.[1]
Enterprise	T1033		System Owner/User Discovery	LiteDuke can enumerate the account name on a targeted system.[1]
Enterprise	T1497	.003	Virtualization/Sandbox Evasion: Time Based Checks	LiteDuke can wait 30 seconds before executing additional code if security software is detected.[1]

Source: https://attack.mitre.org/software/S0513/