Smoke Loader, Software S0226 | MITRE ATT&CK®

Archived: 2026-04-05 14:58:00 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Smoke Loader uses HTTP for C2.[1]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Smoke Loader adds a Registry Run key for persistence and adds a script in the Startup folder to deploy the payload.[1]
Enterprise	T1059	.005	Command and Scripting Interpreter: Visual Basic	Smoke Loader adds a Visual Basic script in the Startup folder to deploy the payload.[1]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	Smoke Loader searches for credentials stored from web browsers.[3]
Enterprise	T1140		Deobfuscate/Decode Files or Information	Smoke Loader deobfuscates its code.[3]
Enterprise	T1114	.001	Email Collection: Local Email Collection	Smoke Loader searches through Outlook files and directories (e.g., inbox, sent, templates, drafts, archives, etc.).[3]
Enterprise	T1083		File and Directory Discovery	Smoke Loader recursively searches through directories for files.[3]
Enterprise	T1105		Ingress Tool Transfer	Smoke Loader downloads a new version of itself once it has installed. It also downloads additional plugins.[1]
Enterprise	T1027	.013	Obfuscated Files or Information:	Smoke Loader uses a simple one-byte XOR method to obfuscate values in the malware.[1]

Domain	ID		Name	Use
			Encrypted/Encoded File	[3]
Enterprise	T1055		Process Injection	Smoke Loader injects into the Internet Explorer process.[3]
		.012	Process Hollowing	Smoke Loader spawns a new copy of c:\windows\syswow64\explorer.exe and then replaces the executable code in memory with malware.[1][2]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Smoke Loader launches a scheduled task.[3]
Enterprise	T1552	.001	Unsecured Credentials: Credentials In Files	Smoke Loader searches for files named logins.json to parse for credentials.[3]
Enterprise	T1497	.001	Virtualization/Sandbox Evasion: System Checks	Smoke Loader scans processes to perform anti-VM checks. [3]

Source: https://attack.mitre.org/software/S0226/