Crutch, Software S0538 | MITRE ATT&CK®

Archived: 2026-04-05 18:30:27 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Crutch has conducted C2 communications with a Dropbox account using the HTTP API.[1]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	Crutch has used the WinRAR utility to compress and encrypt stolen files.[1]
Enterprise	T1119		Automated Collection	Crutch can automatically monitor removable drives in a loop and copy interesting files.[1]
Enterprise	T1020		Automated Exfiltration	Crutch has automatically exfiltrated stolen files to Dropbox.[1]
Enterprise	T1005		Data from Local System	Crutch can exfiltrate files from compromised systems.[1]
Enterprise	T1025		Data from Removable Media	Crutch can monitor removable drives and exfiltrate files matching a given extension list.[1]
Enterprise	T1074	.001	Data Staged: Local Data Staging	Crutch has staged stolen files in the `C:\AMD\Temp` directory.[1]
Enterprise	T1041		Exfiltration Over C2 Channel	Crutch can exfiltrate data over the primary C2 channel (Dropbox HTTP API).[1]

Domain	ID		Name	Use
Enterprise	T1567	.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Crutch has exfiltrated stolen data to Dropbox.[1]
Enterprise	T1008		Fallback Channels	Crutch has used a hardcoded GitHub repository as a fallback channel.[1]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Crutch can persist via DLL search order hijacking on Google Chrome, Mozilla Firefox, or Microsoft OneDrive.[1]
Enterprise	T1036	.004	Masquerading: Masquerade Task or Service	Crutch has established persistence with a scheduled task impersonating the Outlook item finder.[1]
Enterprise	T1120		Peripheral Device Discovery	Crutch can monitor for removable drives being plugged into the compromised machine.[1]
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	Crutch has the ability to persist using scheduled tasks.[1]
Enterprise	T1102	.002	Web Service: Bidirectional Communication	Crutch can use Dropbox to receive commands and upload stolen data.[1]
