ChChes, Software S0144 | MITRE ATT&CK®

Archived: 2026-04-05 14:50:58 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	ChChes communicates to its C2 server over HTTP and embeds data within the Cookie HTTP header.[1][2]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	ChChes establishes persistence by adding a Registry Run key.[3]
Enterprise	T1555	.003	Credentials from Password Stores: Credentials from Web Browsers	ChChes steals credentials stored inside Internet Explorer.[3]
Enterprise	T1132	.001	Data Encoding: Standard Encoding	ChChes can encode C2 data with a custom technique that utilizes Base64.[1][2]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	ChChes can encrypt C2 traffic with AES or RC4.[1][2]
Enterprise	T1083		File and Directory Discovery	ChChes collects the victim's %TEMP% directory path and version of Internet Explorer.[4]
Enterprise	T1562	.001	Impair Defenses: Disable or Modify Tools	ChChes can alter the victim's proxy configuration.[3]
Enterprise	T1105		Ingress Tool Transfer	ChChes is capable of downloading files, including additional modules.[1][2][4]

Domain	ID		Name	Use
Enterprise	T1036	.005	Masquerading: Match Legitimate Resource Name or Location	ChChes copies itself to an .exe file with a filename that is likely intended to imitate Norton Antivirus but has several letters reversed (e.g. notron.exe).[3]
Enterprise	T1057		Process Discovery	ChChes collects its process identifier (PID) on the victim.[1]
Enterprise	T1553	.002	Subvert Trust Controls: Code Signing	ChChes samples were digitally signed with a certificate originally used by Hacking Team that was later leaked and subsequently revoked.[1][2][3]
Enterprise	T1082		System Information Discovery	ChChes collects the victim hostname, window resolution, and Microsoft Windows version.[1][3]

Source: https://attack.mitre.org/software/S0144