Hikit, Software S0009 | MITRE ATT&CK®

Archived: 2026-04-02 10:46:49 UTC

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Hikit has used HTTP for C2.[3]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Hikit has the ability to create a remote shell and run given commands.[3]
Enterprise	T1005		Data from Local System	Hikit can upload files from compromised machines.[1]
Enterprise	T1573	.001	Encrypted Channel: Symmetric Cryptography	Hikit performs XOR encryption.[1]
Enterprise	T1574	.001	Hijack Execution Flow: DLL	Hikit has used DLL to load `oci.dll` as a persistence mechanism.[2]
Enterprise	T1105		Ingress Tool Transfer	Hikit has the ability to download files to a compromised host.[1]
Enterprise	T1566		Phishing	Hikit has been spread through spear phishing.[1]
Enterprise	T1090	.001	Proxy: Internal Proxy	Hikit supports peer connections.[1]
Enterprise	T1014		Rootkit	Hikit is a Rootkit that has been used by Axiom. [2] [3]

Domain	ID		Name	Use
Enterprise	T1553	.004	Subvert Trust Controls: Install Root Certificate	Hikit installs a self-generated certificate to the local trust store as a root CA and Trusted Publisher.[4]
		.006	Subvert Trust Controls: Code Signing Policy Modification	Hikit has attempted to disable driver signing verification by tampering with several Registry keys prior to the loading of a rootkit driver component.[3]

Source: https://attack.mitre.org/software/S0009/