VOLTTRON Visual Consequence Profile

PNNL-SA-175437

Pacific Northwest NATIONAL LABORATORY

Adversary

Real | **Hypothetical**

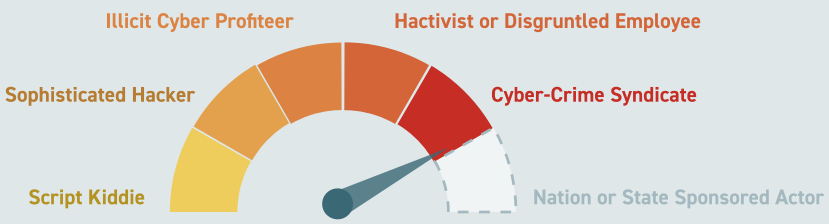
Name

Hypo-Crime

This cyber crime organization may be a group or team of hackers, programmers, or other tech bandits who combine their skills and resources to commit major crimes that might not otherwise be possible.

Desired Goals

- Command & Control of Deployed System
- Manipulation of System for Profit
- Holding Operation of System for Ransom



Can utilize all known tactics and exploits | May have "proprietary" malware/ransomware | Capable of crafting complex campaigns to target specific organizations or persons

Motivations

⚠ = Of Concern

Intelligence Gathering	⚠ **Profit**	Defamation	Notoriety	Other
Cyber Warfare	⚠ **Hacking for Hire**	Disinformation	Personal Curiosity	
Industrial Espionage	Political Messaging	Vandalism	Chaos	

ATTACK SCENARIOS AND PATHWAYS

Concern Level

Ransomware

Affects: Availability

The HCCO seeks to monitor and control devices, essentially holding that control "hostage" until payment is made.

- Deployed Agents
- Device Control
- Improper Account Access
- Illicit Database Permissions

Command & Control

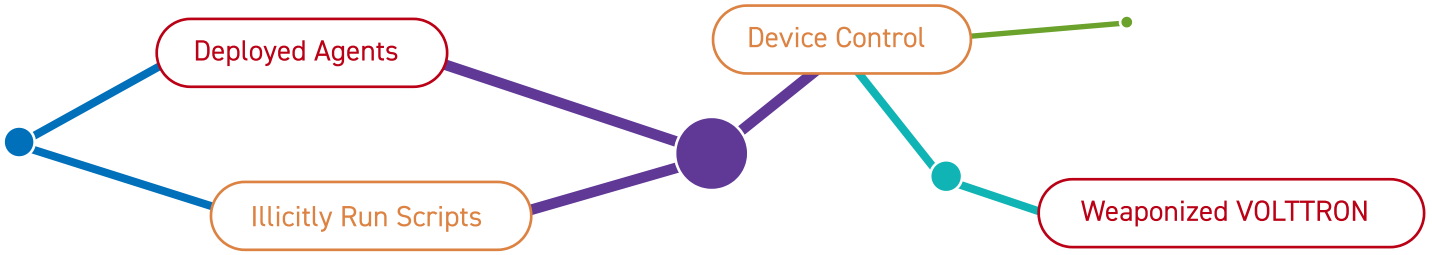
Affects: Confidentiality

The HCCO takes control of the VOLTTRON deployment to redirect the data or computing resources for its own illicit activities.

- Weaponized VOLTTRON
- Illicitly Run Scripts
- Abuse Authorities Granted

Code injection | Improper resource shutdown or release | Improper Restriction of XML External Entity Reference (XXE Ref) | Filtering Sensitive Logs

Shared Techniques



U.S. DEPARTMENT OF ENERGY

PREPARED FOR
VOLTTRON™ (BTO of DOE)

PREPARED BY
Shamrock Cyber | shamrock.cyber@pnnl.gov

JUNE 2022
PNNL-SA-175437