|  |
| --- |
|  |
| **Cyber Protection Team 175 Threat Emulation Plan: HACKTONIANS** |
| **OPERATION GRUNGY PAINT III** |
| **03 OCT 2019** |
|  |
| **1.0.0** |



**Table of Contents**

[Threat Emulation Plan: Hacktonians 2](#__RefHeading___Toc1431_3799018206)

[1 Hacktonians Overview 2](#__RefHeading___Toc1433_3799018206)

[1.1 Hacktonians Tools and Techniques 3](#__RefHeading___Toc1435_3799018206)

[1.2 Hacktonians Tool Functionality 4](#__RefHeading___Toc1437_3799018206)

[2 Emulation Phases 4](#__RefHeading___Toc1439_3799018206)

[2.1 Phase 1 - RECON 4](#__RefHeading___Toc1441_3799018206)

[2.2 Phase 2 - SCANNING 4](#__RefHeading___Toc1443_3799018206)

[2.3 Phase 3 - EXPLOITATION 4](#__RefHeading___Toc1445_3799018206)

[3 Bibliography 4](#__RefHeading___Toc1447_3799018206)

[4 Appendix 5](#__RefHeading___Toc1449_3799018206)

# Threat Emulation Plan: Hacktonians



# Hacktonians Overview

*In this section provides an overview of the threat, including any assumptions made during the development of the TEP. Provides a brief narrative of how the adversary conducts operations. Cites sources of information where applicable.*

**MITRE ATT&CK Group ID: Hacktonians**

**Aliases:** Quedagh, VOODOO BEAR, Hacktonian, Hacktonians

**Operations:** Hacktonians are a criminal group openly affiliated with, and known to support, the APT82n government. They consist of a decentralized network of small criminal cells that span almost every continent. Though at core they are mercenaries, Hacktovians are highly nationalistic and often leave pro-Krasnovian propoganda messages on compromised systems and websites. Chief motivation is financial gain. Hacktovian cells have been behind some of the most sophisticated hacks in recent Polandian history. They have been known to:

* Wreak general havoc on user systems typically exploiting unpatched systems via direct attacks. They are typically noisy using brute force attacks, DDOS techniques, buffer overflows, or password cracking techniques.
* Reported techniques include the entire sprectrum of interference including: Bypass User Account Control, Credentials in Files, Data Destruction, Fallback Channels, File and Directory Discovery, File System Permissions Weakness, Indicator Removal on Host, Input Capture, Network Service Scanning, New Service, Peripheral Device Discovery, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Screen Capture, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Windows Admin Shares, Windows Management Instrumentation

**Target Industries:** Government entities, agencies, and infrastructure as well as private enterprise or even private individual depending upon their financial sponsor’s agenda.

**Objectives:** Financial Gain.

**Background:** Hacktonians are a Krasnovian cyber espionage group that has operated since approximately 2009. The group likely consists of Krasnovian pro-hacktivists. Hacktonian targets mainly Polandian entities associated with energy, industrial control systems, SCADA, government, and media. Hacktonian have been linked to the Polandian energy sector attack in late 2015. Because of their nationalist fundamentalism, it is believed that their available clientele is limited based on national origin.

## Hacktonians **Tools and Techniques**

*Hacktonians employs these tools and techniques:*

|  |  |
| --- | --- |
| **Techniques Used** | **Use** |
| Hacktonians use any technique that is available and have no consistent fingerprint but include the following: | Hacktonioan intent is to create havoc or strong arm compromised organizations into paying ransoms. |
| Bypass User Account Control, Credentials in Files, Data Destruction, Fallback Channels, File and Directory Discovery, File System Permissions Weakness, Indicator Removal on Host, Input Capture, Network Service Scanning, New Service, Peripheral Device Discovery, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Screen Capture, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Windows Admin Shares, Windows Management Instrumentation |  |

## Hacktonians Tool Functionality

|  |  |
| --- | --- |
| **Tool** | **Techniques** |
| BlackEnergy | Bypass User Account Control, Credentials in Files, Data Destruction, Fallback Channels, File and Directory Discovery, File System Permissions Weakness, Indicator Removal on Host, Input Capture, Network Service Scanning, New Service, Peripheral Device Discovery, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Screen Capture, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Windows Admin Shares, Windows Management Instrumentation |

# Emulation Phases

***Most likely:*** *Social engineering attacks are recently attributed to a Hacktonian splinter group. Hacking unpatched systems with poor firewall rules and no anti-virus is likely. Hactonians most recently claimed responsibility for compromising ICS/SCADA systems in Polandia.*

***Recommendation:*** *Review/Search Download histories and Browser Histories. Educate users on social engineering techniques. Harden and monitor vulnerable ICS/SCADA systems.*

## Phase 1 - RECON

The attack starts with Hacktonians being contracted to attack a known target. Their sponsors agenda will largely influence the nature of the reconnaissance performed though they are known to use the social engineering tool-kits and reconnaissance tools available in CyberHawk.

## Phase 2 - SCANNING

Hacktonians have gained access to ICS/SCADA systems via very sophisticated toolset dubbed BlackEnergy. The exploits leverage microwave explloits as well as unique Modbus exploits present due to misconfigured devices or a lack of hardened installations.

## Phase 3 - EXPLOITATION

Hacktonians rely on toolkits such as Cyberhawk and BlackEnergy to compromise systems. They are noisy and unafraid to take over systems “in the clear” though they have sophisticated and nearly undetectable toolkits that allow them to deface websites.

# Bibliography

Hultquist, J.. (2016, January 7). Sandworm Team and the Ukrainian Power Authority Attacks. Retrieved October 6, 2017.

Meyers, A. (2018, January 19). Meet CrowdStrike’s Adversary of the Month for January: VOODOO BEAR. Retrieved May 22, 2018.

F-Secure Labs. (2014). BlackEnergy & Quedagh: The convergence of crimeware and APT attacks. Retrieved March 24, 2016.

# Appendix

**Hardening recommendations:**

**Network**

Implement Access control lists within routers/Firewalls:

Access control lists should be defined permitting only the required traffic

Reduce risk of unauthorized lateral movement

Deny externally established connections into Network

Harden Router/Firewall User Account Access

Restrict management access to a defined list of internal hosts, using only encrypted protocol such as SSH

**Workstations**

Disable administrator accounts on machines

Disable guest accounts

Remove miscellaneous accounts

Disable all unnecessary services

Enable host firewalls & ensure all system firewalls are turned on with standardized rules

Update workstations with latest patches

Microsoft patches

All other vendor patches

**Servers**

Create a backup of the database instance

Reassign the MSSQL to a non-standard port

Turn off SQL Server browser service

Turn off named pipes

Disable unnecessary services

Restrict access to the DB backup

Patch the system to the latest KB

**Active Directory**

Enable Windows Firewalls for domain client machines

Disable HTTP listeners and use WinRM over HTTPS

Deploy Sysmon to monitor AD domain controllers

Deny user write to unauthorized locations

Enforce strong password policy

Complex password required

Enforce Password expiration

Password age set to 60 days to lock inactive accounts

**ICS/SCADA**

There are too many recommendations to make a comprehensive list here. The general recommendation is to implement all “best practices” recommendations from ICS-Cert in the following areas.

Creating Cyber Forensics Plans for Control Systems

Developing an Industrial Control Systems Cybersecurity Incident Response Plan

Good Practice Guide for Firewall Deployment on SCADA and Process Control Networks

Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies

Patch Management for Control Systems

Recommended Practice Case Study:  Cross-Site Scripting

Remote Access for Industrial Control Systems

Securing Control System Modems

Updating Antivirus in an Industrial Control System