Pacific Northwest
NATIONAL LABORATORY

PNNL-32630

Cyber Criminal Organization Dossier for VOLTTRON™

Provided by Shamrock Cyber

February 2022

Josh Bigler
Angie Chastain
Paul Francik
Catie Himes
Danielle Nodine
Emma Lancaster
Patrick O’Connell
Aaron Phillips
Shawn Ricketts
Garret Seppala
Torri Simmons
Bianca Steele
Chance Younkin

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

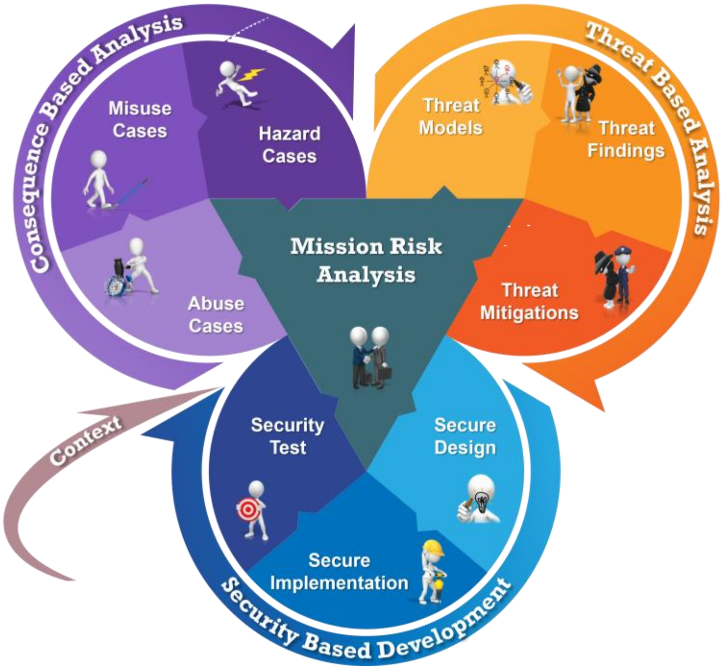
Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <https://www.ntis.gov/about>
Online ordering: http://www.ntis.gov

PNNL-32630

Cyber Criminal Organization Dossier for VOLTTRON™

February 2022

Josh Bigler
Angie Chastain
Paul Francik
Catie Himes
Danielle Nodine
Emma Lancaster
Patrick O’Connell
Aaron Phillips
Shawn Ricketts
Garret Seppala
Torri Simmons
Bianca Steele
Chance Younkin



Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Contents

Figures

Tables

Acronyms and Abbreviations

CCO	cyber-criminal organization
CIA	Confidentiality, Integrity, and Availability
FAE	functional abuse element
IDDIL-ATC	Identify Assets, Define the Attack Surface, Decompose the System, Identify Attack Vectors, List the Threat Actors, Analysis & Assessment, Triage, Controls
OSA	Open-Source Analysis
PNNL	Pacific Northwest National Laboratory
SAST	Static Application Security Testing
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
TAE	Technical Abuse Element
TBA	Threat Based Analysis
TMT	Threat Modeling Tool

1.0 Introduction

The VOLTTRON team is engaged with Pacific Northwest National Laboratory's (PNNL's) ***Shamrock Cyber*** Team to provide cybersecurity analyses of the VOLTTRON software. Shamrock offers several software services, as shown in Figure 1. These services are ultimately used together to inform business decision makers and minimize mission risk. This ***Cyber Criminal Dossier*** is part of Shamrock's Consequence-Based Analysis services. The dossier summarizes abuse case analysis of VOLTTRON within the adversarial context of a ***cyber-criminal organization***.

> ***Consequence-Based Analysis*** – analyzes the abuse, misuse, and hazards that determine the risks of developing and deploying a system.
>
> ***Threat-Based Software Analysis*** – determines and prioritizes threats against the software system and recommends mitigations. The result is a Threat Profile that contains a threat model, threat findings, and mitigations.
>
> ***Secure Software Development*** – applies security best practices to the software development life cycle. This includes secure design, secure code review, vulnerability scanning, and security testing.

Figure 1. Shamrock Cyber services.

This context was selected by the VOLTTRON development team because of the general prevalence of ransomware attacks executed by cyber-criminal organizations across the VOLTTRON business sectors. The destructive and disruptive consequences of ransomware attacks are significant across these sectors and should thus be addressed. This dossier provides abuse case scenarios for two plausible attack types. No specific cyber-criminal organization is identified in this dossier, so the pseudonym ***CCO*** for Cyber Criminal Organization will be used as the hypothetical adversary.

The analysis determined CCO to be primarily motivated by financial gain through cyber-enabled extortion. The means for executing this extortion may be any of the following:

- Denial of access or controls to VOLTTRON or the systems it interacts with or controls
- Encryption, destruction, or corruption of critical data
- Threats to publicly release or sell stolen sensitive data.

CCO could also use VOLTTRON assets to further their attacks (e.g., as a portion of their attack vector, as a command-and-control link, as stolen processing capabilities, etc.).

The development of this dossier relies on several factors—key among them are the following:

- Adversarial context – the technical capabilities, motives, and level of motivation of the CCO. The assessed "technical capabilities" in this analysis includes the use of the MITRE ATT&CK Matrix to provide a standardized and well-documented reference to adversarial tactics and techniques and to assist the design of system defenses and risk mitigations (a link to the matrix is included in Table 1).
- Functional Abuse Elements (FAEs) – the VOLTTRON functions that CCO can take advantage of and abuse to achieve their goals.
- Technical Abuse Elements (TAEs) – the technical means via vulnerabilities or exploits that enable execution of the FAEs.
- Abuse Cases (Actual) – these scenarios exist when TAEs have been identified that would enable one or more of the FAEs.
- Abuse Case (hypothetical) – these scenarios are listed where it is plausible that a TAE does or could exist that enables one or more of the FAEs but has yet to be fully identified. These hypothetical abuse cases are documented as "watchlist" items to provide enhanced situational awareness for proactive system security.

2.0 Abuse Case Scenarios

The abuse case analysis led to two plausible scenarios in which CCO could execute a successful attack against VOLTTRON. The scenarios are plausible because the FAEs and TAEs align to the adversary context, thus providing clear prioritization of the vulnerabilities (TAEs) that should be addressed to further strengthen VOLTTRON against a CCO attack.

2.1 Scenario 1: Holding the System for Ransom

The CCO, interested in profit, seeks to monitor and control devices, essentially holding that control "hostage" until payment is made.

1. FAE: Deployed agents – CCO could illicitly deploy agents to monitor and control devices in order to determine building efficiency and implement efficiency strategies
   - TAE: Code injection
   - TAE: Improper resource shutdown or release.
2. FAE: Device control – CCO could illicitly control devices based on decisions
   - TAE: Code Injection
   - TAE: Filtering Sensitive Logs
   - TAE: Improper Restriction of XXE Ref.
3. FAE: Improperly provides account access
   - NO TAEs: But place FAE on a "watchlist" because it aligns with CCO motivations.
4. FAE: Illicitly set up database permissions
   - NO TAEs: But place FAE on a "watchlist" because it aligns with CCO motivations.

2.2 Scenario 2: Stealing VOLTTRON Resources

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

1. FAE: Weaponized VOLTTRON
   - TAE: Improper Restriction of XML External Entity Reference (XXE Ref).
2. FAE: Illicitly run scripts
   - TAE: Code Injection
   - TAE: Improper Resource Shutdown or Release.
3. FAE: Abuse system admin authorities and permissions granted by access to the UNIX file system
   - NO TAEs: But place FAE on a "watchlist" because it aligns with CCO motivations.

3.0 Adversary Breakdown

Table 1 shows a breakdown of the parameters for the CCO. The left column shows the parameter name and a definition of the parameter. The right column shows the value of that parameter as determined by the abuse case analysis.

Table 1. Plausible breakdown of hypothetical CCO.

Adversary: *Specific existing adversary if known or identified (e.g., Cult of the Dead Cow, Anonymous, REvil, Fancy Bear, Deep Panda, etc.)*	**No specific adversary identified**
Adversary category: *One of the following:* • *State or state-supported actor* • *Cyber-crime syndicate* • *Hacktivists/disgruntled employee* • *Illicit cyber profiteer* • *Sophisticated hacker* • *Script kiddie*	**Cyber-criminal organization**
Sophistication level: *One of the following:* • *VERY HIGH – State of the art, state level* • *HIGH – Imaginative to unique use of known exploits and scripting of new exploits, capable of running complex campaigns* • *MEDIUM – Use of known exploits and established tactics with some level of adaptability* • *LOW – Rudimentary use of well-known and published exploit*	**MEDIUM TO HIGH** • Can utilize all known tactics and exploits • May have "proprietary" malware/ransomware • Capable of crafting complex campaigns to target specific organizations or persons
Motivation(s) *The primary interests/goals of the adversary, which can be any of the following:* • *Intelligence gathering* • *Cyber warfare* • *Industrial espionage* • *Profit* • *Hacking for hire* • *Political messaging* • *Defamation,* • *Disinformation* • *Vandalism* • *Notoriety* • *Personal curiosity* • *Chaos* • *etc.*	**PROFIT**

Desired effects/actions: *Description of the actions on target or effects (network, device, or physical) that the adversary intends to employ in support of their motive.*	**COMMAND & CONTROL OF DEPLOYED SYSTEM** (Confidentiality) **MANIPULATION OF SYSTEM FOR PROFIT** (Integrity) **HOLDING OPERATION OF SYSTEM FOR RANSOM** (Availability)
Assessed capabilities: *Description of the types of attacks and complexities of those attacks and campaigns that could be employed by an adversary based on sophistication level, motivations, and desired effects. These are assessed potential capabilities, not observed specific capabilities.*	**KNOWLEDGE AND EXPERIENCE USING OPEN-SOURCE RECON AND EXPLOITATION TOOLS** **COMPUTATIONAL RESOURCES SUCH AS BOTNETS** **ABILITY TO RECRUIT INSIDER AGENTS**
Observed capabilities: *Specific and observed capabilities that are attributed to an adversary (if a specific adversary has been identified).*	**TBD** (Requires identification of specific CCO)
Assessed tactics: *Description of the nature and exploit types and tools that could be employed by an adversary based on sophistication level, motivations, and desired effects. Often presented in terms of industry standards or published lists of vulnerabilities and/or exploits. These are assessed potential tactics, not observed specific tactics.* *Examples:* • *MITRE ATT&CK Matrix – https://attack.mitre.org/* • *CISA Known Exploited Vulnerabilities – https://www.cisa.gov/known-exploited-vulnerabilities-catalog*	**RECONNAISSANCE:** ALL **RESOURCE DEV:** ALL **INITIAL ACCESS:** VALID ACCOUNTS, HARDWARE ADDITIONS, TRUSTED RELATIONSHIP **EXECUTION:** COMMAND AND SCRIPTING INTERPRETER, USER EXECUTION **PERSISTENCE:** ACCOUNT MANIPULATION, CREATE ACCOUNT, CREATE OR MODIFY SYSTEM PROCESS, IMPLANT INTERNAL IMAGE, MODIFY AUTHENTICATION PROCESS, VALID ACCOUNTS **PRIVILEGE ESCALATION:** PROCESS INJECTION, VALID ACCOUNTS **DEFENSE EVASION:** FILE AND DIRECTORY PERMISSIONS MODIFICATION, HIDE ARTIFACTS,

	INDIRECT COMMAND EXECUTION, MASQUERADING, PROCESS INJECTION, VALID ACCOUNTS **CREDENTIAL ACCESS:** ALL **DISCOVERY:** ALL **LATERAL MOVEMENT:** EXPLOITATION OF REMOTE SERVICES, LATERAL TOOL TRANSFER, USE ALTERNATE AUTHENTICATION MATERIAL **COLLECTION:** ADVERSARY-IN-THE-MIDDLE, ARCHIVE COLLECTED DATA, AUTOMATED COLLECTION, DATA FROM INFORMATION REPOSITORIES, DATA FROM LOCAL SYSTEM, INPUT CAPTURE **COMMAND AND CONTROL:** APPLICATION LAYER PROTOCOL, FALLBACK CHANNELS, PROXY, REMOTE ACCESS SOFTWARE, WEB SERVICE **EXFILTRATION:** AUTOMATED EXFILTRATION, EXFILTRATION OVER C2 CHANNEL, EXFILTRATION OVER OTHER NETWORK MEDIUM, EXFILTRATION OVER PHYSICAL MEDIUM, SCHEDULED TRANSFER **IMPACT:** DATA DESTRUCTION, DATA ENCRYPTED FOR IMPACT, DATA MANIPULATION, INHIBIT SYSTEM RECOVERY, RESOURCE HIJACKING, SERVICE STOP

Appendix A Brief on Threat-Based Analysis

The Shamrock Cyber team combines three stages of Threat Based Analysis (TBA), as shown in Figure 2. TBA utilizes portions of Lockheed Martin's IDDIL-ATC methodology (Figure 3) to perform threat analysis. Shamrock optimizes IDDIL-ATC for more cost-effective, time-efficient results that lead to immediately actionable controls. Using the Lockheed Martin nomenclature, Shamrock actually begins with ***Decompose the System***. To accomplish this, Shamrock often requests that ***Usage Narratives*** be written by members of the project team. The narratives provide the Shamrock team with valuable context in simple, non-jargon terms. With this context, the next step is to develop a set of use cases and data flow diagrams that represent the system. Generally, the assets and the attack surface can be identified using these diagrams, thus addressing the ***Identify Assets*** and ***Define the Attack Surface*** steps. From there, Shamrock attempts to ***List Threat Actors***, but this is not yet a rigorous exercise. The use cases, abuse cases, and data flow diagrams represent the ***Shamrock Cyber Threat Model***, which is the foundation for developing the Threat Profile.

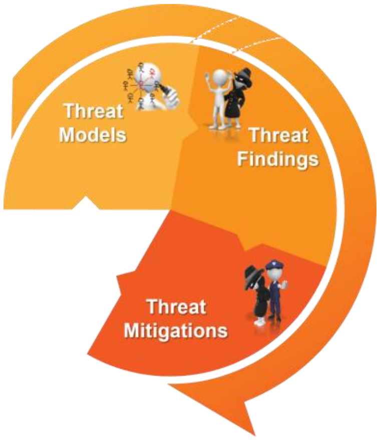
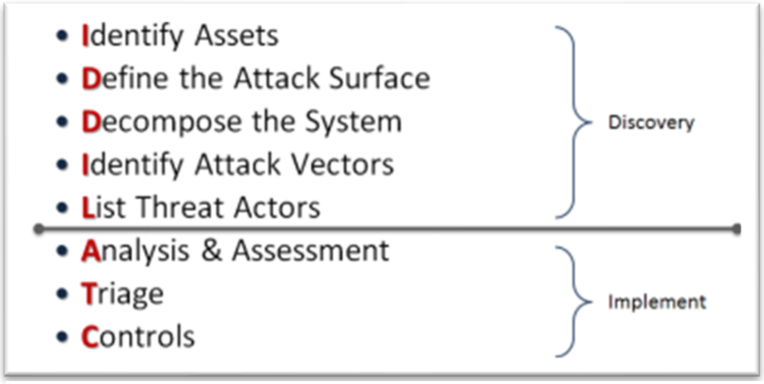


Figure 2. The TBA leaf of Shamrock Cyber.



- Identify Assets
- Define the Attack Surface
- Decompose the System
- Identify Attack Vectors
- List Threat Actors

Discovery

- Analysis & Assessment
- Triage
- Controls

Implement

Figure 3. Lockheed Martin's methodology.

Shamrock asks the project team to set an initial expectation of threat priority based on Confidentiality, Integrity, and Availability (CIA). The CIA Triad (see Figure 4) is a commonly used cybersecurity model.

The Shamrock Cyber team uses the data flow diagrams as input to Microsoft's Threat Modeling Tool (TMT). The TMT is a free download that comes with standard threat templates used by Shamrock. The TMT reads the diagrams and uses the templates to provide initial ***Analysis and Assessment*** as well as ***Triage*** results. The TMT also uses Microsoft's STRIDE model to categorize threats. The initial results from the TMT are then analyzed by Shamrock subject matter experts to complete the ***Shamrock Cyber Threat Findings*** for review by the project team.

Confidentiality
Integrity
Availability

Figure 4. The CIA triad.

With the Threat Findings in hand, Shamrock goes back to the project team to collaboratively analyze and determine mitigations (***Controls***). When this exercise is complete, the Shamrock team organizes the information into the final product, the ***Shamrock Cyber Threat Profile***.

Appendix B Brief on Security Based Development

The Shamrock Cyber Team is establishing Security Based Development (SBD) best practices in the areas depicted in Figure 5. While Shamrock will at some point offer ***Secure Design*** and ***Security Testing***, the current focus is on ***Secure Coding***. For Shamrock, secure coding combines Static Application Security Testing (SAST) and Open-Source Analysis (OSA). The objective is to produce a Vulnerability Profile, which uses a SAST vulnerability scan of the code and an OSA scan to produce initial results. PNNL has adopted Checkmarx as the lab's vulnerability scanner, which does both SAST and OSA scans. Shamrock uses Checkmarx results to perform an analysis that eliminates false positives and condenses information into a simple report for use by the software development team. The full scan is also available in the Vulnerability Profile. The Shamrock process for creating a Vulnerability Profile is a straightforward set of steps:

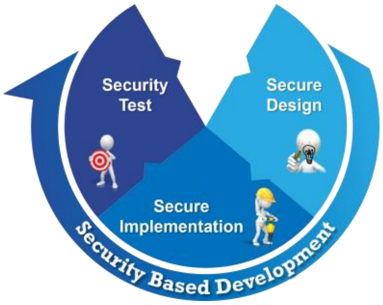


Figure 5. The SBD leaf of Shamrock Cyber

1. Receive source code from development team in the form of a zip file

   The zip file will be unzipped and used as input to the Checkmarx scanner.

2. Run Checkmarx SAST scan

   Every file contained in the zip file will be scanned with results, forming the foundation for Shamrock analysis.

3. Run Checkmarx OSA scan

   Dependency libraries will be checked by Checkmarx, and vulnerable libraries along with out-of-date libraries will be documented, forming the foundation for Shamrock analysis.

4. Analyze SAST scan results

   Results of Shamrock analysis are in the SAST Profile section of a Vulnerability Profile.

5. Analyze OSA scan results

   Results of Shamrock analysis are in the OSA Profile section of a Vulnerability Profile.

6. Deliver a Vulnerability Profile, often accompanied by a Threat Profile

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov