Go To Hunt, Then Sleep

by David J. Bianco and Robert M. Lee

Illustrated by Jeff Haas

Chapter One: The Drawing of the Two

The Bad Guys are inside your network today.
From finance to HR they creep.
If you expect to ever rest well,
Go to hunt, then sleep.

Go to Hunt, But First Read

David J. Bianco
Principal Engineer
Target Corporation
@DavidJBianco

Robert M. Lee
CEO
Dragos, Inc.
@RobertMLee

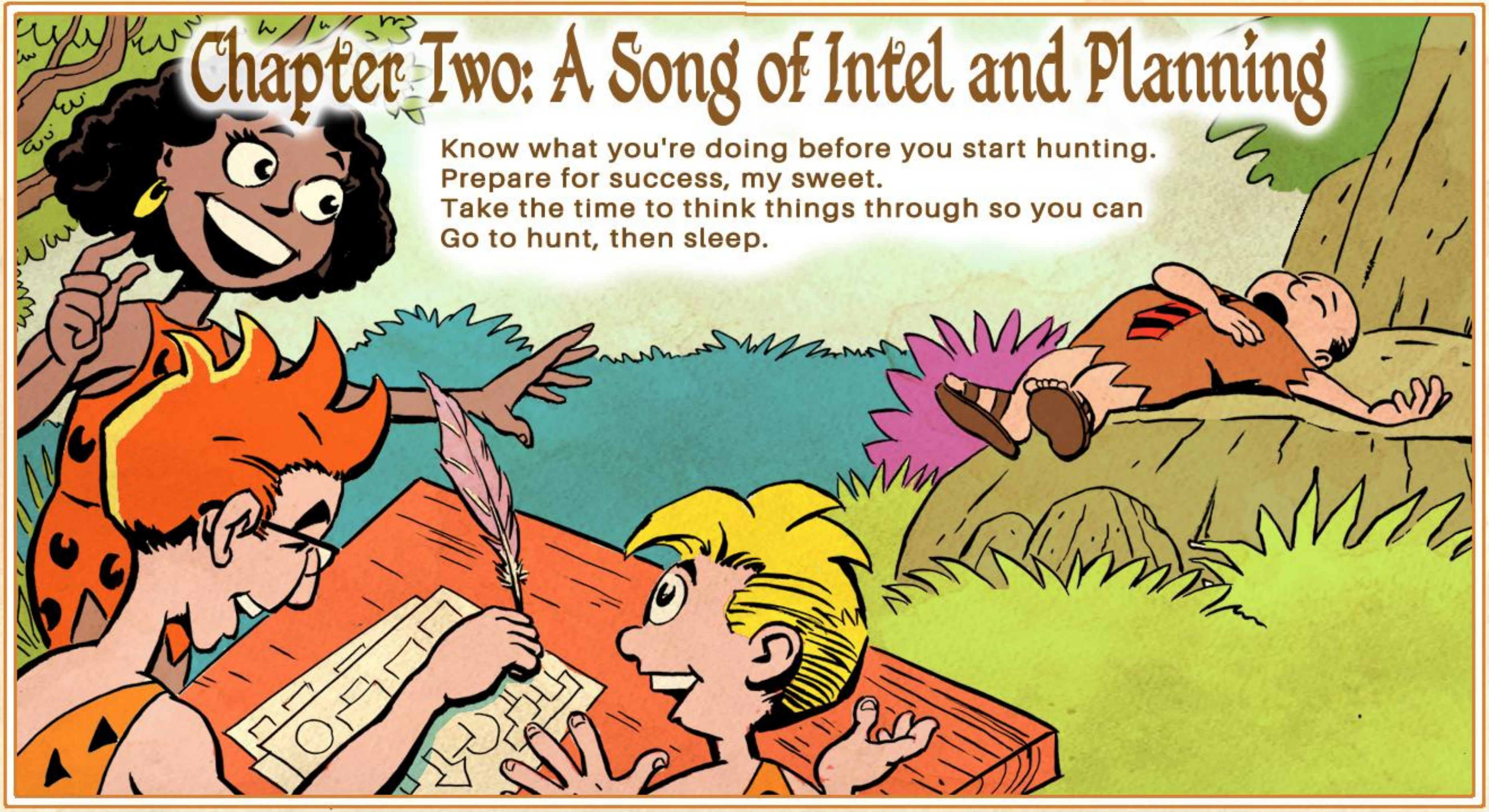
Generating Hypotheses for Successful Threat Hunting
https://goo.gl/Jo9qCA

The ICS Cyber Kill Chain
https://goo.gl/fivxp7

The ThreatHunting Project
http://ThreatHunting.net

MITRE ATT&CK Framework
https://attack.mitre.org

Chapter Two: A Song of Intel and Planning



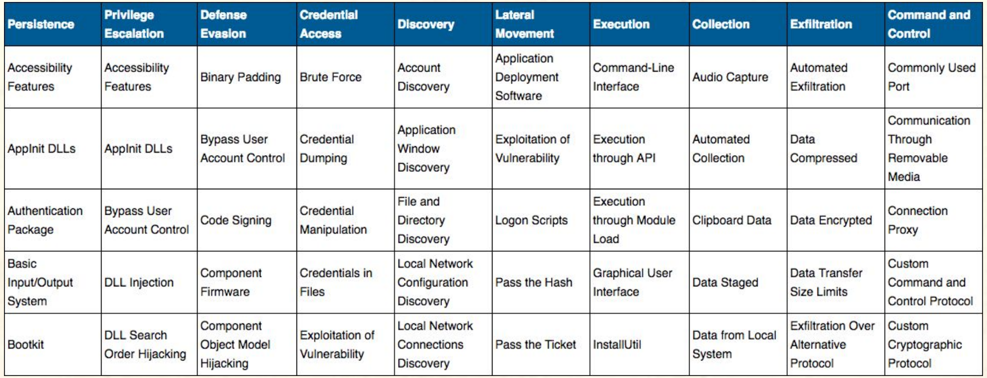
Know what you're doing before you start hunting.
Prepare for success, my sweet.
Take the time to think things through so you can
Go to hunt, then sleep.

Identifying Hunt Targets

Use “friendly intel” to identify core processes and assets.

Use threat intel to identify likely actors and their common tactics and known techniques against those assets.

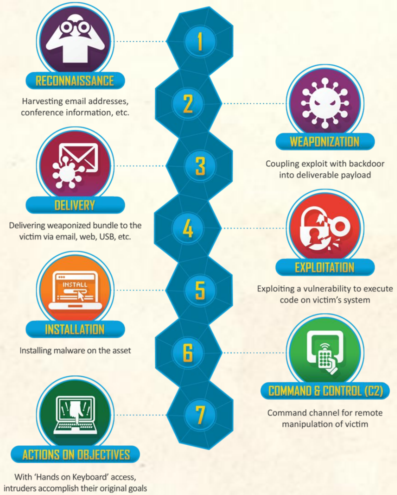
Cross reference with MITRE ATT&CK framework to identify related techniques.



Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Audio Capture	Automated Exfiltration	Commonly Used Port
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Automated Collection	Data Compressed	Communication Through Removable Media
Authentication Package	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Execution through Module Load	Clipboard Data	Data Encrypted	Connection Proxy
Basic Input/Output System	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	Graphical User Interface	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	InstallUtil	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol

Setting Priorities

Plot Tactics/Techniques against the attack lifecycle.



RECONNAISSANCE: Harvesting email addresses, conference information, etc.

WEAPONIZATION: Coupling exploit with backdoor into deliverable payload

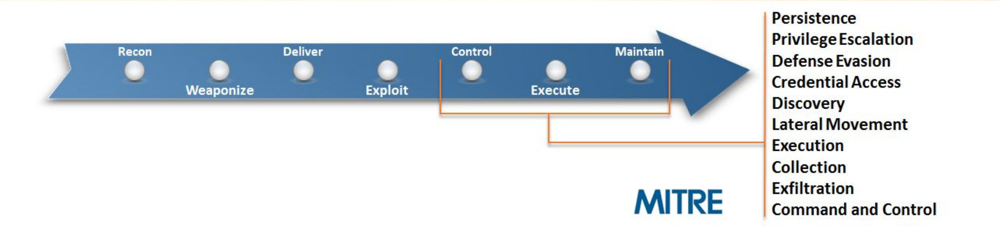
DELIVERY: Delivering weaponized bundle to the victim via email, web, USB, etc.

EXPLOITATION: Exploiting a vulnerability to execute code on victim's system

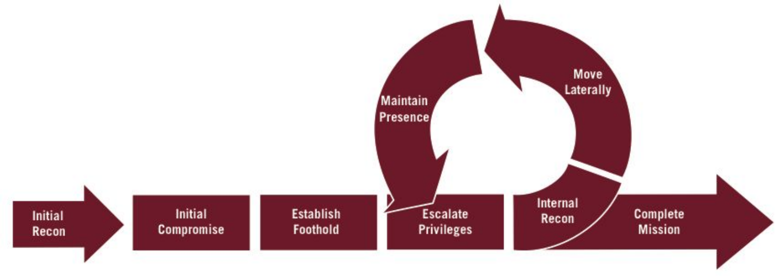
INSTALLATION: Installing malware on the asset

COMMAND & CONTROL (C2): Command channel for remote manipulation of victim

ACTIONS ON OBJECTIVES: With 'Hands on Keyboard' access, intruders accomplish their original goals



- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Execution
- Collection
- Exfiltration
- Command and Control

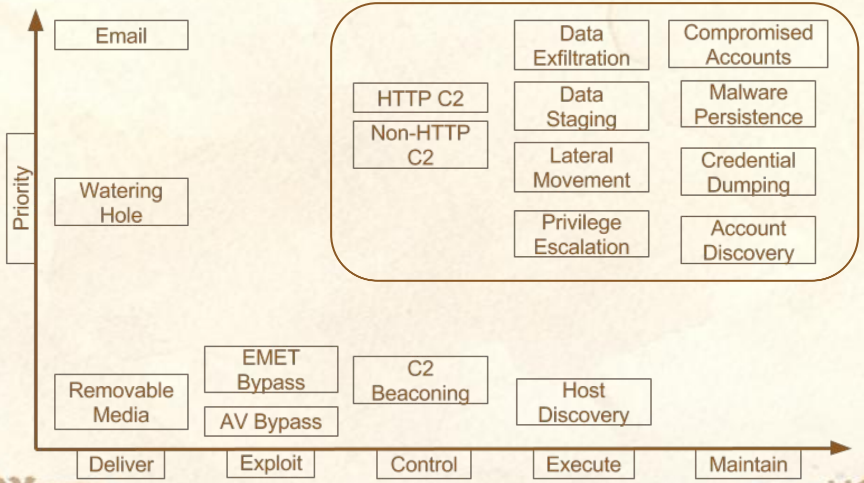


Setting Priorities

Plot Tactics/Techniques against the attack lifecycle.

Rank entries in each phase by potential impact & breadth of activity coverage.

Prioritize on two axes: lifecycle phase and rank in phase.



Creating the Hunt Plan

Research each technique to determine side effects & likely artifacts.

Turn this research into actionable hunt info:

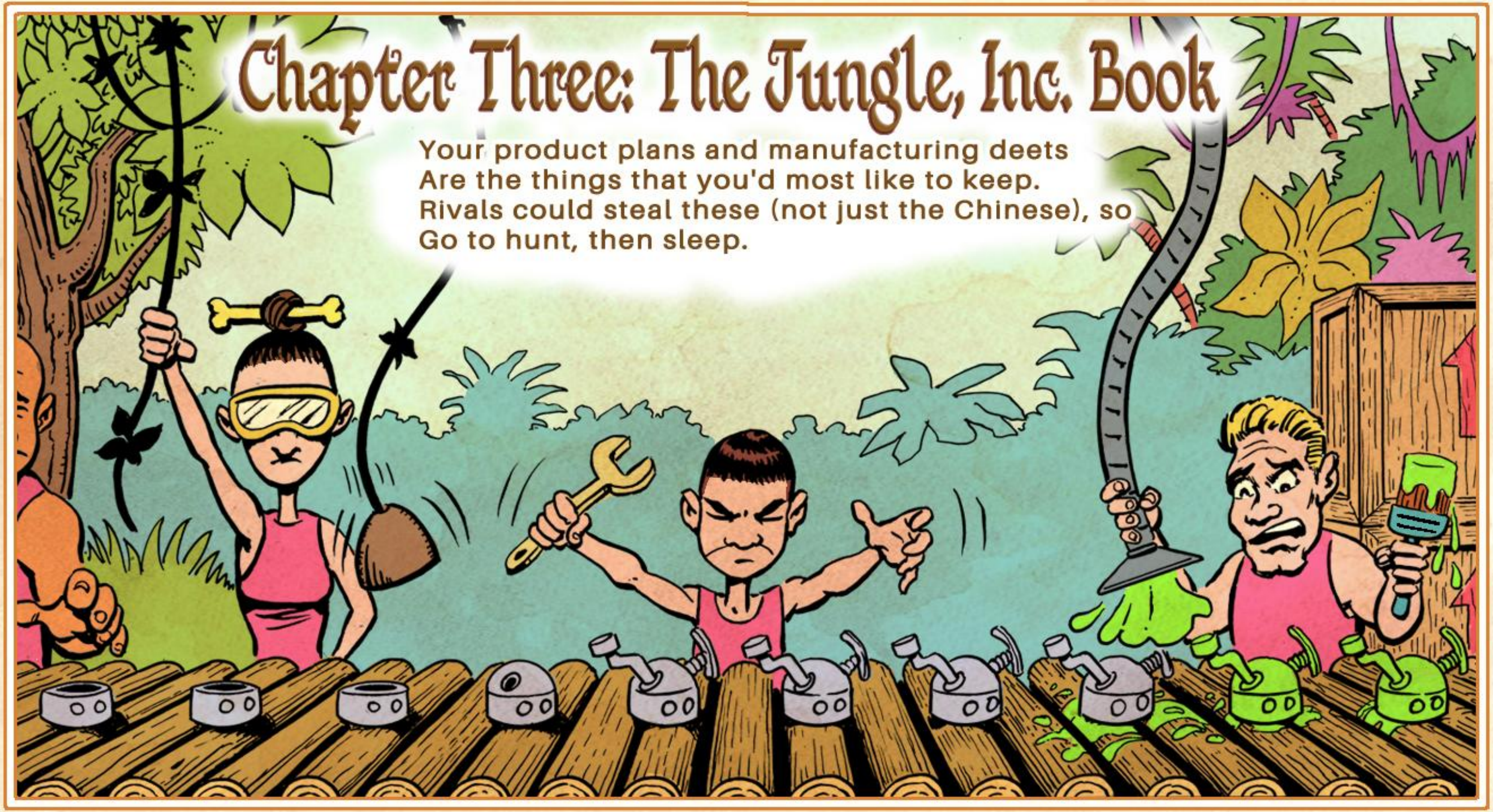
Hunt hypotheses
Data required
Artifacts or effects to look for
Analytic techniques

Schedule these according to your available resources.

Don’t forget to automate successful hunts!

Chapter Three: The Jungle, Inc. Book

Your product plans and manufacturing deets
Are the things that you'd most like to keep.
Rivals could steal these (not just the Chinese), so
Go to hunt, then sleep.



Welcome to the Jungle

Jungle, Inc. is the leading supplier of wildlife-themed fidget spinners to the rainforest industry. Critical assets include:

- Product plans & specifications
- Manufacturing processes
- Market & customer info

Most of their business relies on a single product. Rivals able to produce similar products more cheaply could severely impact their market share, so their biggest concerns are the confidentiality of their product plans and associated manufacturing processes.

Chapter Four: Where the Wild Things Are, Hunt

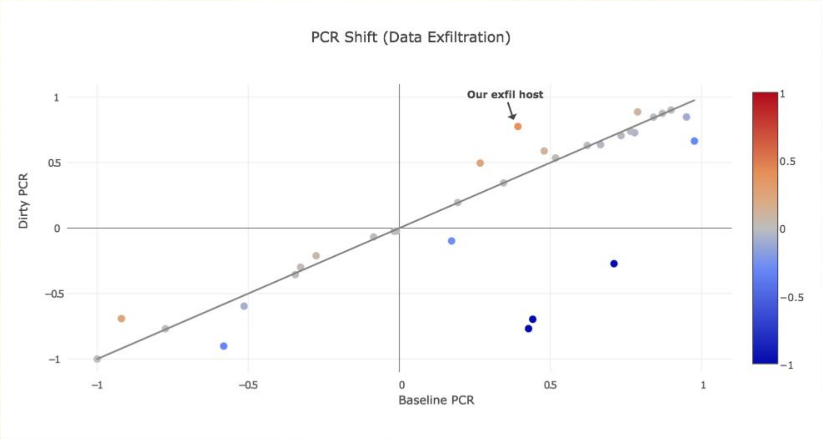
Your plans have real merit, don’t just cover your rear.
Your priorities are spelled out so neat.
These are the things you'll be looking for, dear. Now
Go to hunt, then sleep.

Data Exfiltration via PCR Shift

The Producer-Consumer Ratio (PCR) measures the “shape” of a system’s pattern of network use. Significant shifts in PCR may indicate unusual data movement (staging or exfil).

Hypothesis: Large amount of data being staged/exfiltrated will significantly change PCR from one or few hosts.

Data Required: Network flow records.

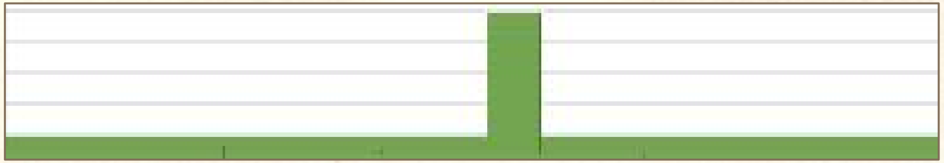


Artifacts & Effects: Large PCR change over time
Analytic Techniques: Visualization

Source: The ThreatHunting Project (https://goo.gl/J7oGE9)

Lateral Movement in Process Logs

An attacker’s first foothold in the environment is unlikely to offer them access to product plans or the ICS environment. Therefore, LM will be necessary.



Hypothesis: Lateral movement will be performed from the command line, requiring the attacker to spawn command shells. Additionally, they will tend to use existing CLI tools to orient themselves when they compromise a new host.

Data Required: Process creation (Win event 4688, Sysmon event 1, EDR logs, etc)

Artifacts & Effects: Command shells started by documents or other weird parents; spikes in use of CLI recon tools

Analytic Techniques: Visualization, stack counting

Source: The ThreatHunting Project (https://goo.gl/ZiqA1R and https://goo.gl/gM8HcM)

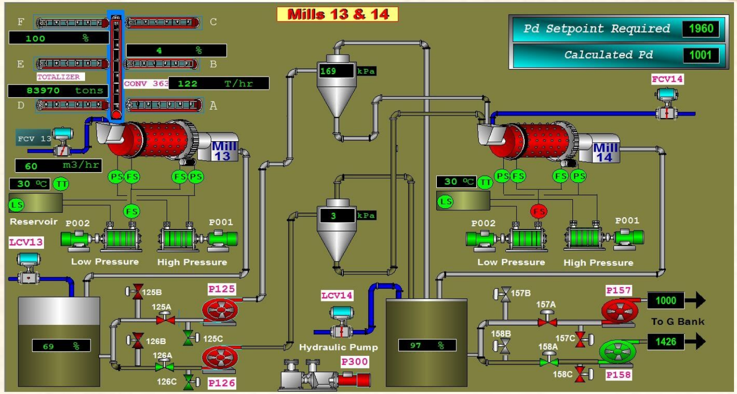
Adversary Positioning on HMIs

Human Machine Interfaces (HMIs) are the Supervisory Control for the Process

HMIs are often on Windows and Linux systems familiar to adversaries, contain important visual information about the physical process, and can be connected for remote usage.

Hypothesis: Adversaries will position on HMIs as familiar territory (Windows and Linux) while learning the industrial process.

Data Required: Process creation, VPN logs, and HMI logs



Artifacts & Effects: New process spawning outside of maintenance periods, VPN session lengths/frequency, or HMI logs for undocumented interaction

Analytic Techniques: Configuration and Frequency Analysis

Exfiltration from Data Historian

Data Historians hold the specifics about the physical industrial process.

Espionage would require both the manufacturing schematics (IT) as well as the physical process information ultimately making up the full “recipe” details (ICS), which would require the Historian.

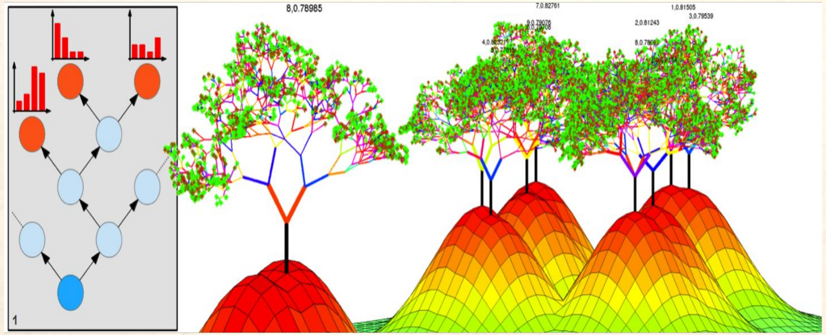
Hypothesis: Exfiltration from Historians would utilize legitimate ICS protocols such as OPC but it would generate consistently larger OPC communications.

Data Required: Network captures of OPC

Artifacts & Effects: Spikes in OPC usage and trends of larger OPC communications over time than previous

Analytic Techniques: Visualization, Configuration Analysis, Time Series Seasonal Decomposition

Machine Learning for HTTP C2



http://www.rhaensch.de/vrf.html

By nature, most HTTP C2 will be slightly different than normal traffic. We may be able to exploit that by applying some simple ML techniques.

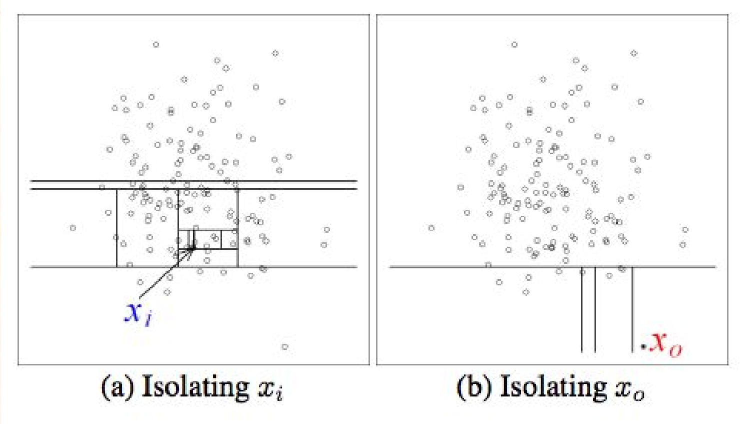
Hypothesis: At least some HTTP C2 transactions are “different enough” that an ML model can learn to find them.

Data Required: Outgoing HTTP logs

Artifacts & Effects: Not Applicable
Analytic Techniques: Random Forests (Supervised), Isolation Forests (Unsupervised)

Source: https://github.com/DavidJBianco/Clearcut

Machine Learning for HTTP C2



(a) Isolating x_i (b) Isolating x_o

http://cs.nju.edu.cn/zhouzh/zhouzh.files/publication/icdm08b.pdf

By nature, most HTTP C2 will be slightly different than normal traffic. We may be able to exploit that by applying some simple ML techniques.

Hypothesis: At least some HTTP C2 transactions are “different enough” that an ML model can learn to find them.

Data Required: Outgoing HTTP logs

Artifacts & Effects: Not Applicable
Analytic Techniques: Random Forests (Supervised), Isolation Forests (Unsupervised)

Source: https://github.com/DavidJBianco/Clearcut

Happily Ever After

Our story is done. You know what to do
When you're back in the office next week.
Make a good plan, aligned with your needs, then
Go to hunt…

Oh, you’re asleep.

The End