PLEASE DOWNLOAD IF YOU DID NOT RECEIVE THE LINK BEFOREHAND

http://bit.ly/2GxW6Ii

3 STEP YARA

BY MONTY ST JOHN

Monty St John

Who is this guy?

- 25 years of security and analytics – physical, investigations, information, computer forensics, reverse engineering, threat intelligence
- Two decades supporting federal, state, and local LE while in uniform

Forensics and Threat Intelligence

- Better part of past decade acting as a key member of forensic and TI teams deconstructing, analyzing and providing insights into threats and how to thwart them

YARA

PATTERN MATCHING MAGIC

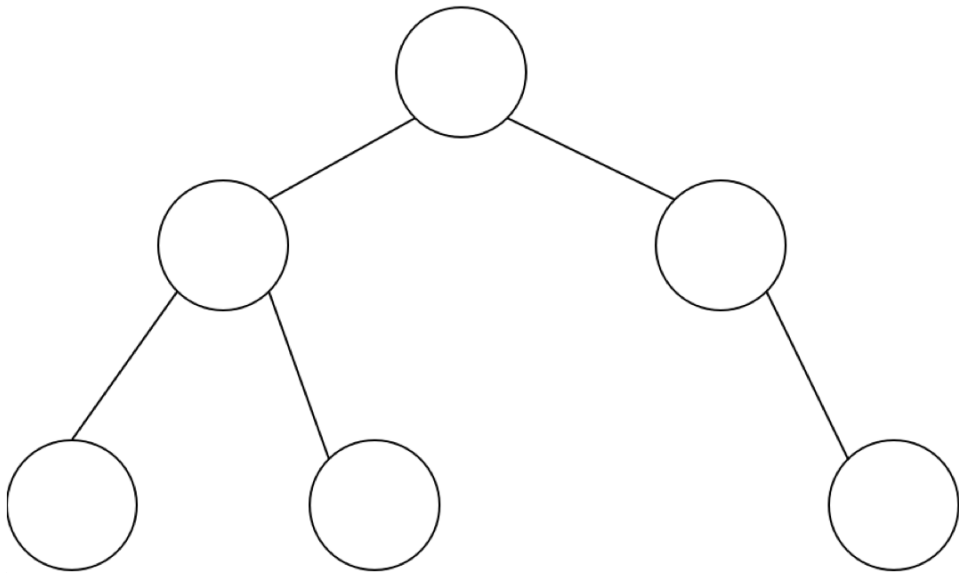
Pattern matching logic. YARA's prime ability is to match patterns.

- Explicit or variable patterns (A = 0, B n = n +C, etc.)

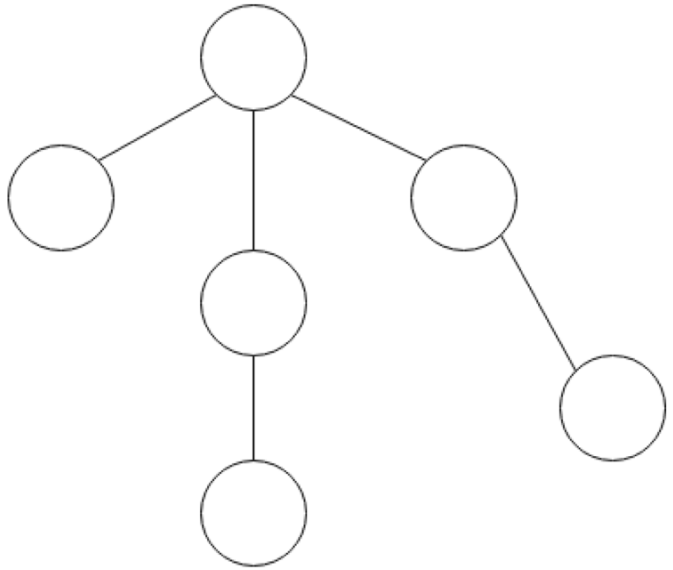
Rule PE_byte_stomping
Rule PE_byte_scavenging
Rule PE_malformed_IAT
Rule PE_malformed_EAT
Rule PE_EP_Beyond_V1
…

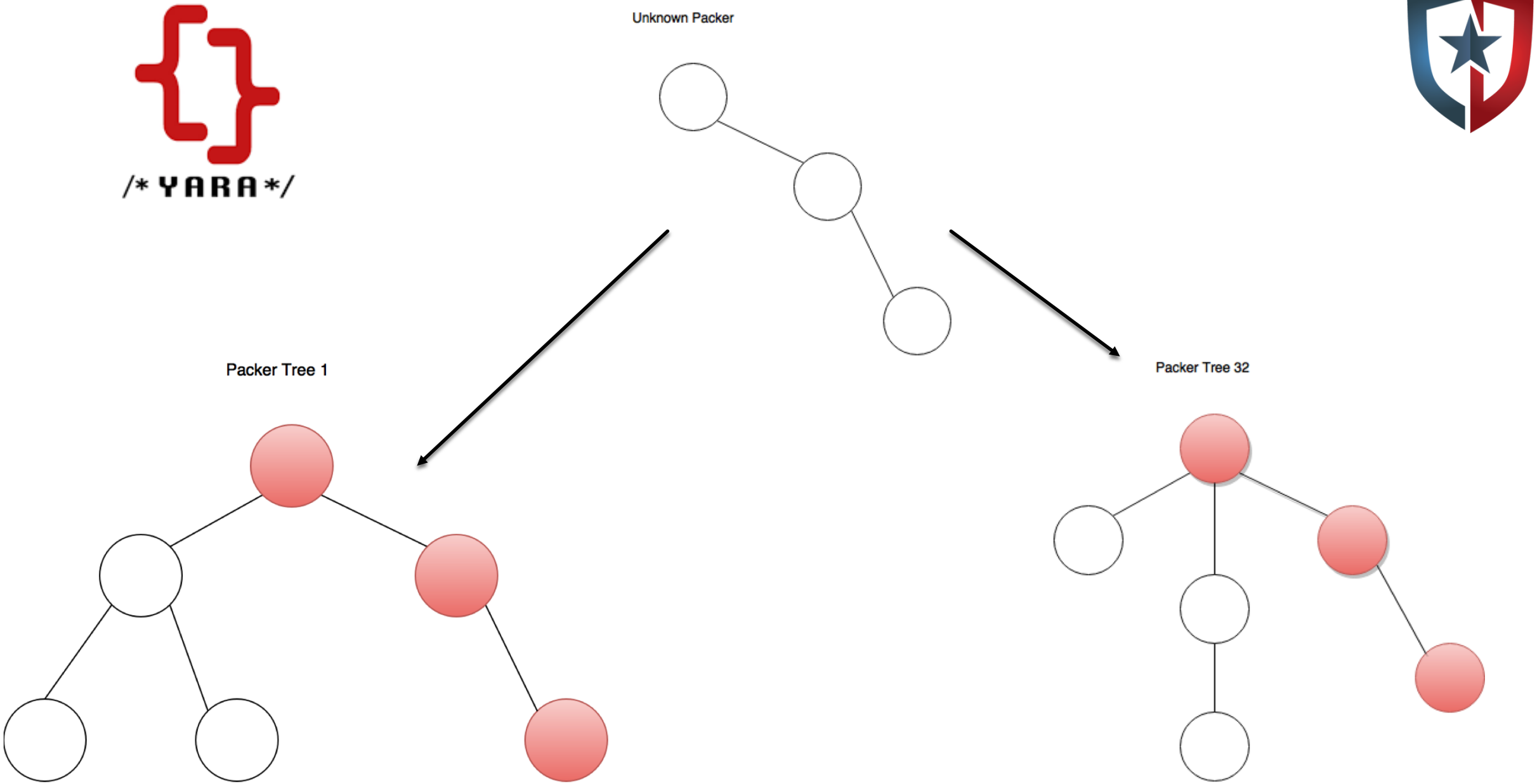
Tree pattern matching

Packer Tree 1



Packer Tree 32




Unknown Packer
Packer Tree 1
Packer Tree 32

Pattern Calculus

Detection	Within X of	Detection	Detection	Constant to	Detection
Detection	Inside of	Detection	Detection	Stacked with	Detection
Detection	Compared to	Detection	Detection	Inverse with	Detection
Detection	Grouped with	Detection	Detection	Outside of	Detection

Who's using YARA

- ActiveCanopy
- Adlice
- BAE Systems
- Bayshore Networks, Inc.
- Blue Coat
- Blueliv
- CrowdStrike FMS
- Fidelis XPS
- FireEye, Inc.
- Fox-IT
- FSF
- Guidance Software
- Heroku
- jsunpack-n

- Kaspersky Lab
- Koodous
- Laika BOSS
- Lastline, Inc.
- Metaflows
- NBS System
- osquery
- PhishMe
- Picus Security
- Radare2

- Raytheon Cyber Products, Inc.
- ReversingLabs
- RSA ECAT
- SpamStopsHere
- Symantec
- Tanium
- The DigiTrust Group
- ThreatConnect

- ThreatStream, Inc.
- Thug
- Trend Micro
- VirusTotal Intelligence
- We Watch Your Website
- Websense
- x64dbg
- YALIH

Organization. How to organize and become efficient.

Best case usage. Where and when to use YARA.

Reporting. Extracting metadata as boilerplate or enrichment for reporting.

ORGANIZATION

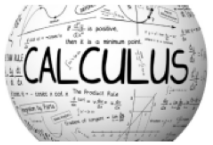
MAKING SENSE OF YOUR YARA BRAIN

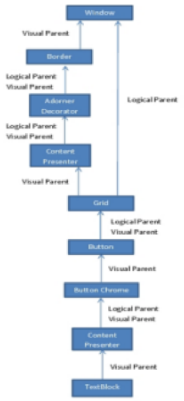
Organization

Stop pouring all your rules into a single glass.

Organization

{ Rule }





Focus on reusability

Organization

- Write once —> use many times
- Structure rules into modules (rulesets)
- Create rule maps to accomplish objectives

Write once — use many times

Structure rules into modules

Create rule maps to achieve objectives

USE CASES

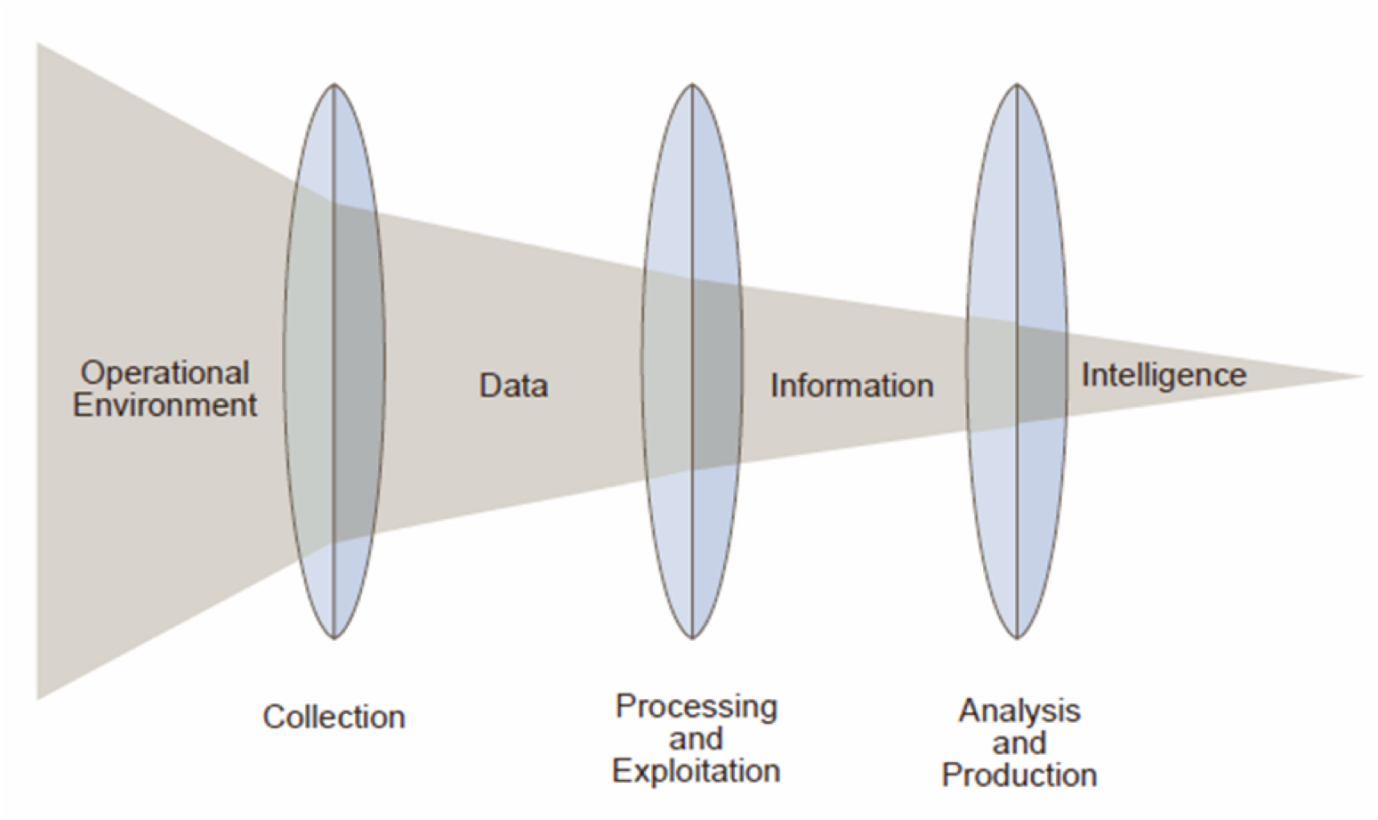
PUTTING YARA TO WORK

Use Case

- Know when to employ YARA; and how to make the rules you need
- Organize rules around your objective e.g., rule mapping

Use Case

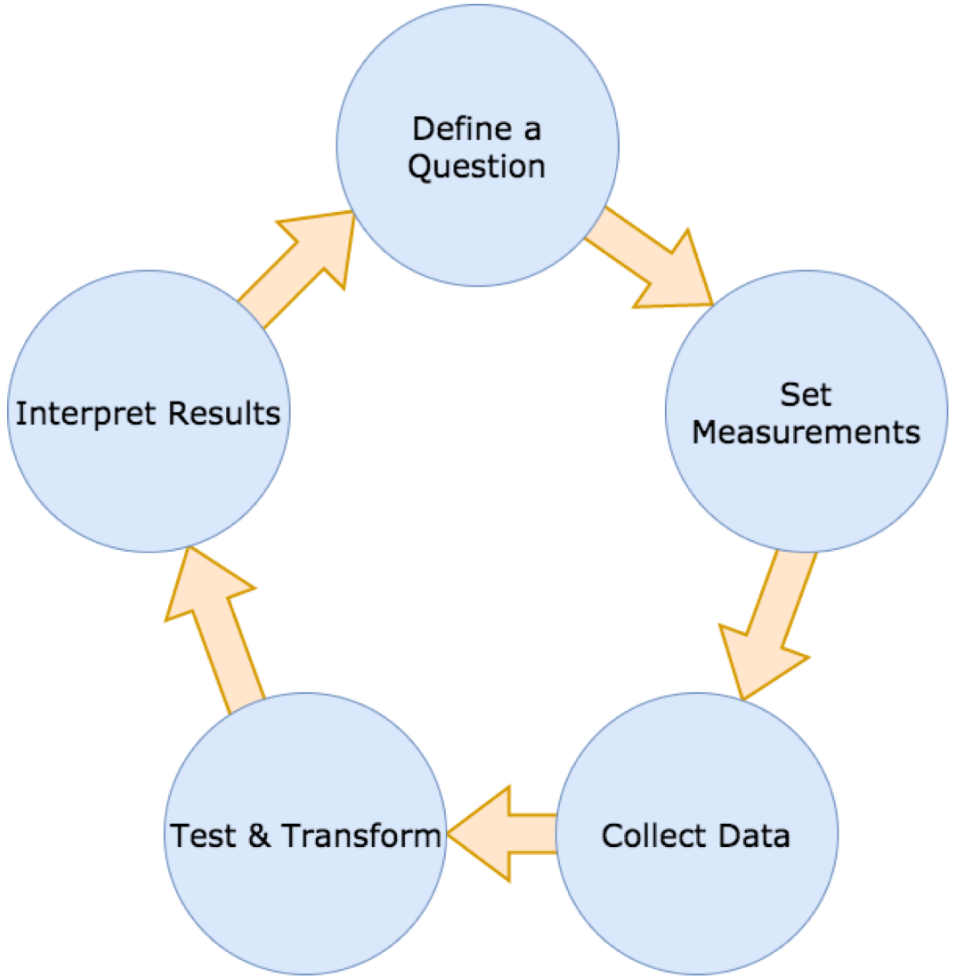
Relationship of Data, Information and Intelligence



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

Use Case

Simplified Analysis Cycle



Use Case

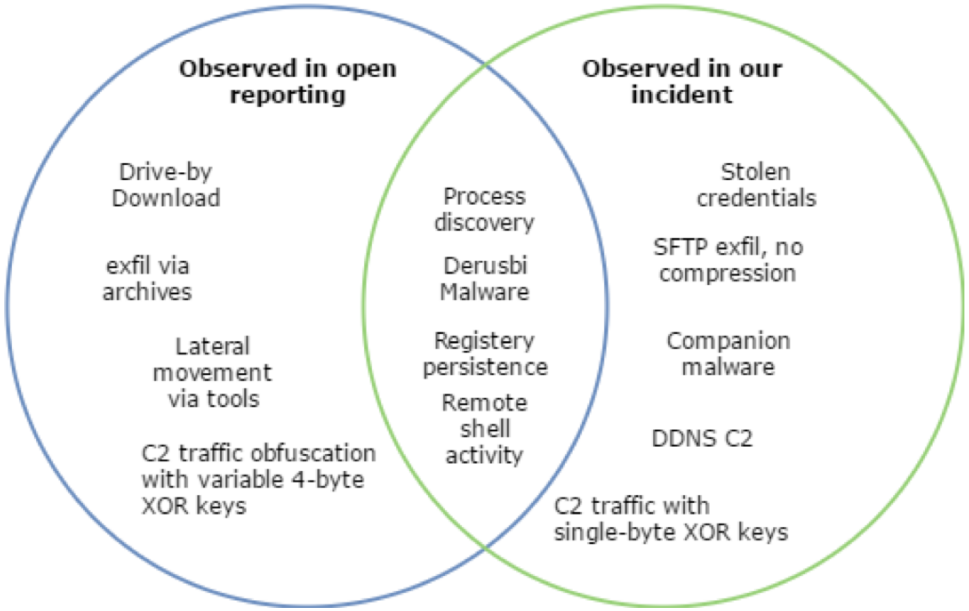
5WHR

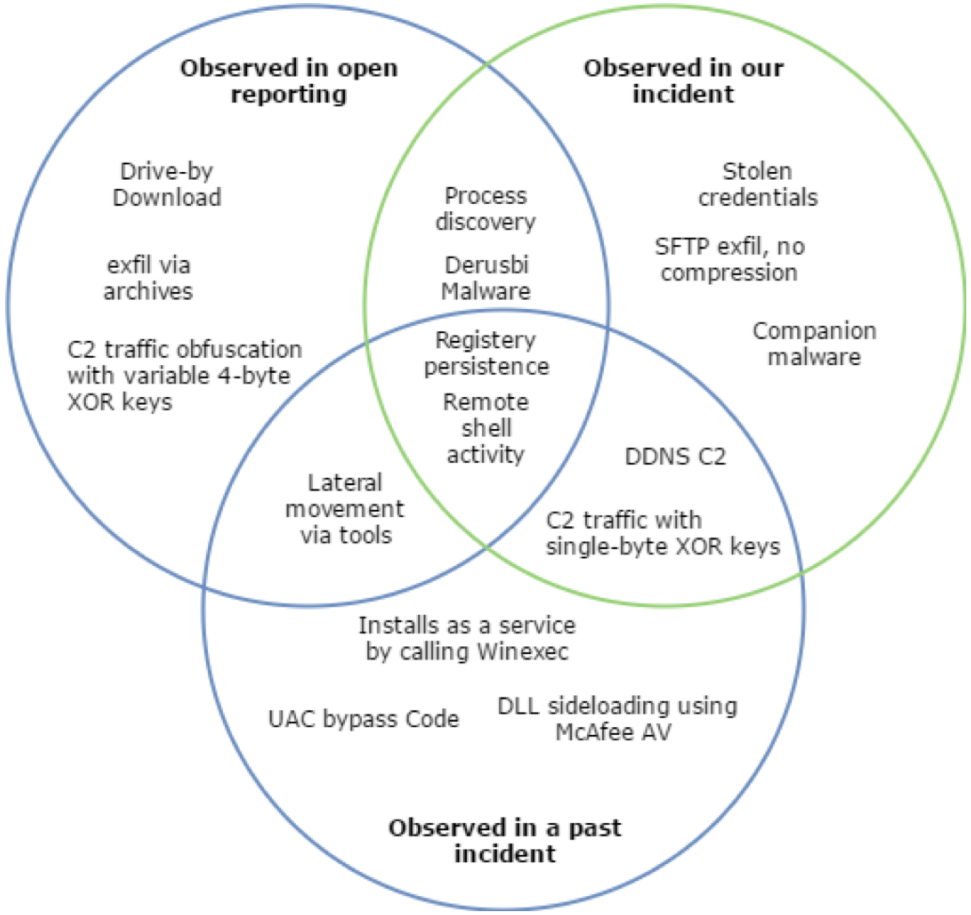
- This method works best for analyzing an event, object or person.
- Requires some some background or close experience in the subject to be effective.

Direct or indirect matching

See XXX YARA rules

Use Case

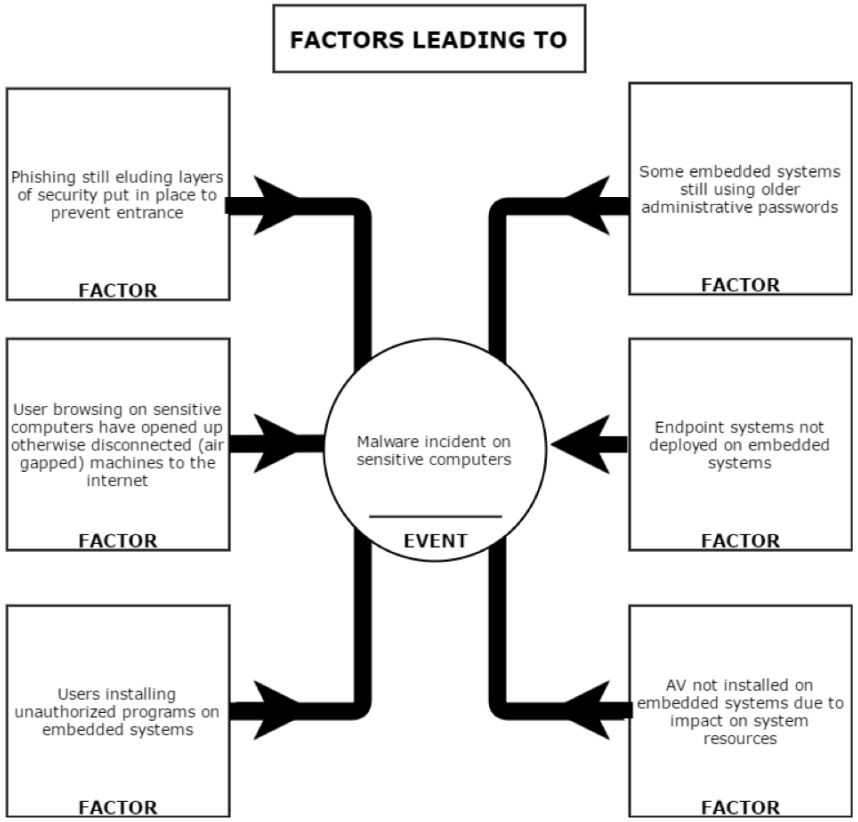

Observed in open reporting
Drive-by Download
exfil via archives
Lateral movement via tools
C2 traffic obfuscation with variable 4-byte XOR keys
Process discovery
Derusbi Malware
Registery persistence
Remote shell activity
Observed in our incident
Stolen credentials
SFTP exfil, no compression
Companion malware
DDNS C2
C2 traffic with single-byte XOR keys

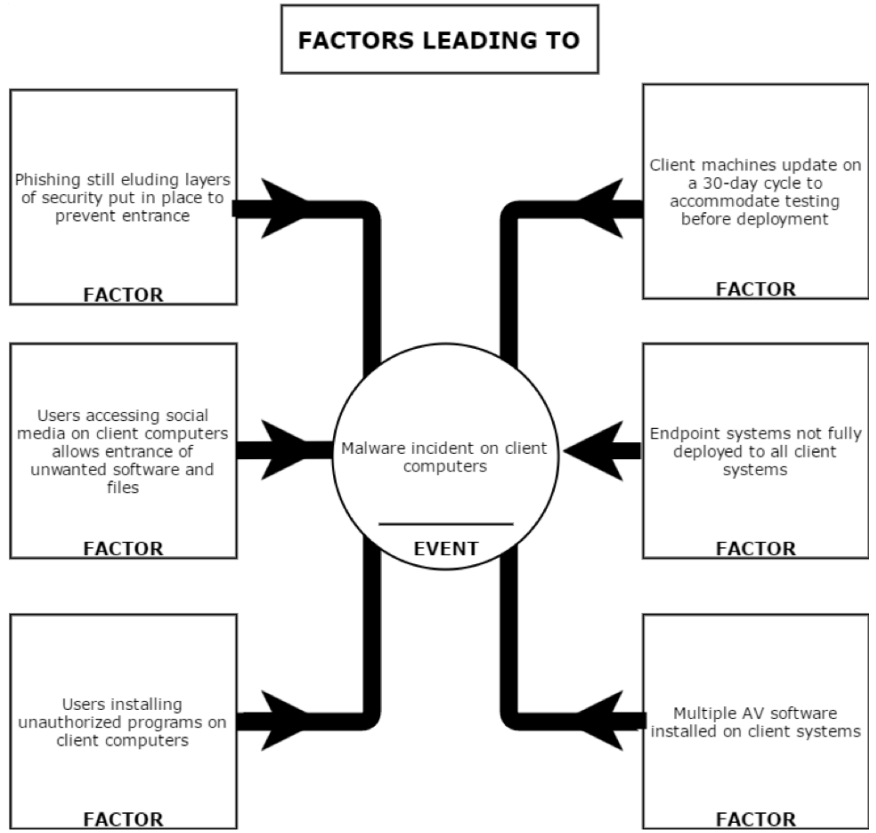

Observed in open reporting
Drive-by Download
exfil via archives
C2 traffic obfuscation with variable 4-byte XOR keys
Observed in our incident
Process discovery
Derusbi Malware
Stolen credentials
SFTP exfil, no compression
Companion malware
Registery persistence
Remote shell activity
DDNS C2
C2 traffic with single-byte XOR keys
Lateral movement via tools
Installs as a service by calling Winexec
UAC bypass Code
DLL sideloading using McAfee AV
Observed in a past incident

Grouping and compare-contrast

See Mach0 yara rules

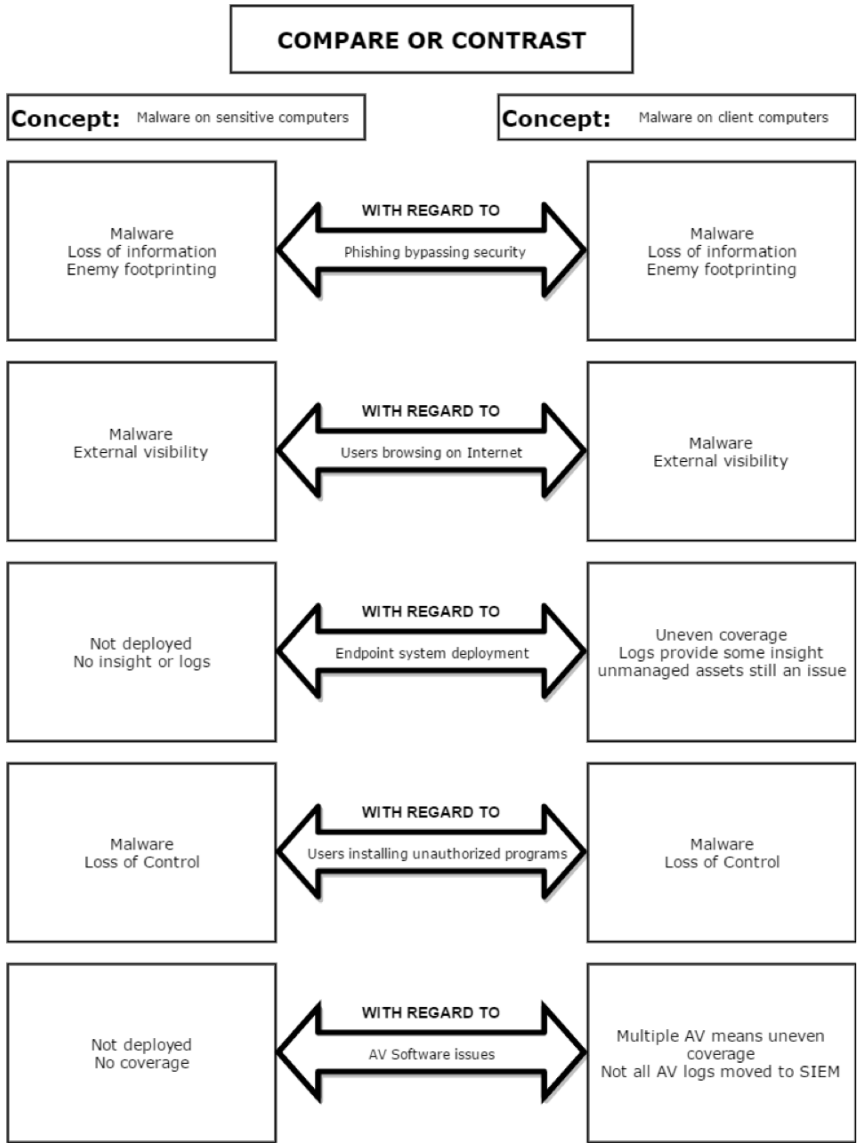
Use Case


FACTORS LEADING TO
Phishing still eluding layers of security put in place to prevent entrance
FACTOR
User browsing on sensitive computers have opened up otherwise disconnected (air gapped) machines to the internet
FACTOR
Users installing unauthorized programs on embedded systems
FACTOR
Malware incident on sensitive computers
EVENT
Some embedded systems still using older administrative passwords
FACTOR
Endpoint systems not deployed on embedded systems
FACTOR
AV not installed on embedded systems due to impact on system resources
FACTOR

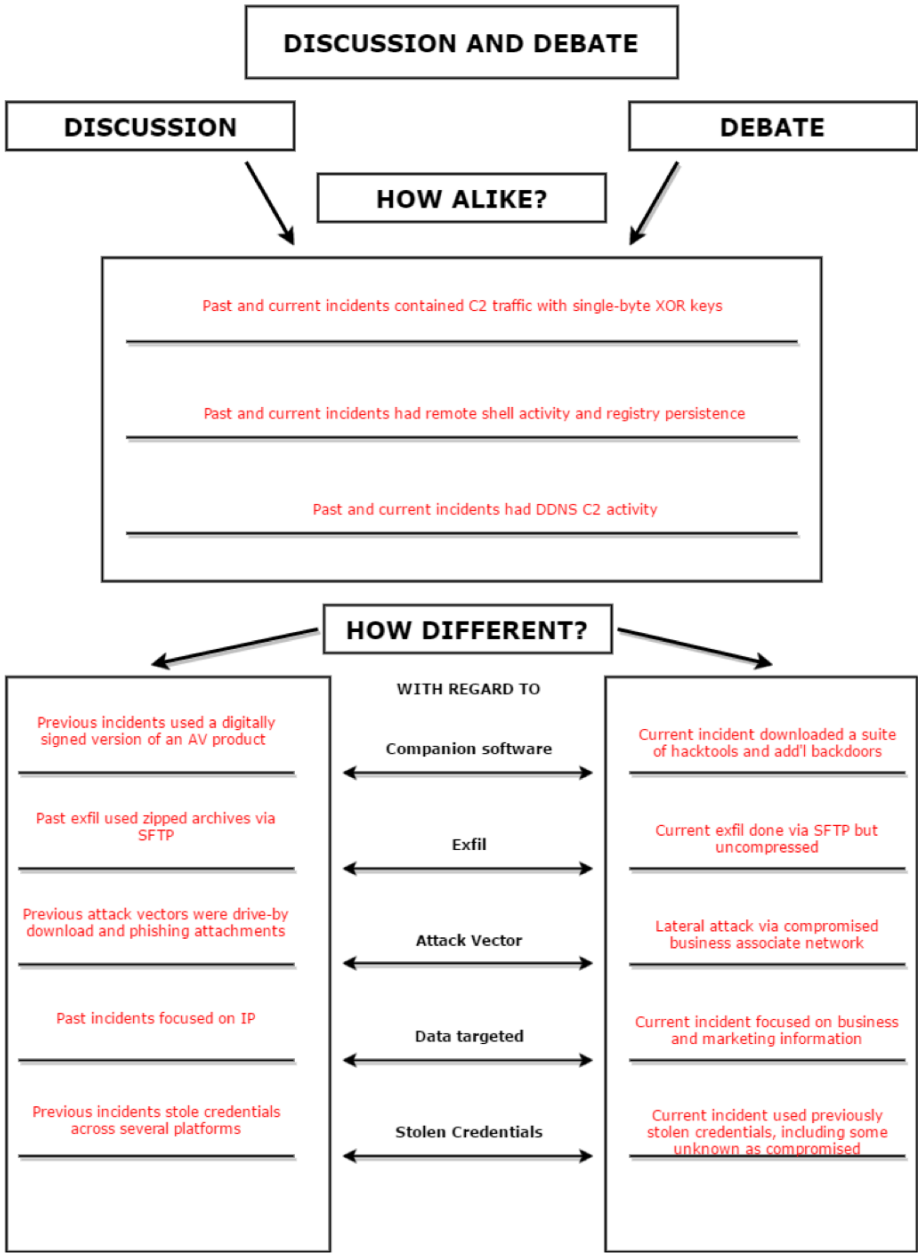

FACTORS LEADING TO
Phishing still eluding layers of security put in place to prevent entrance
FACTOR
Users accessing social media on client computers allows entrance of unwanted software and files
FACTOR
Users installing unauthorized programs on client computers
FACTOR
Malware incident on client computers
EVENT
Client machines update on a 30-day cycle to accommodate testing before deployment
FACTOR
Endpoint systems not fully deployed to all client systems
FACTOR
Multiple AV software installed on client systems
FACTOR

Use Case

Results compare-contrast - Like Factorial but the focus is on the results or implication of the subject



Use Case


DISCUSSION AND DEBATE
DISCUSSION
DEBATE
HOW ALIKE?
Past and current incidents contained C2 traffic with single-byte XOR keys
Past and current incidents had remote shell activity and registry persistence
Past and current incidents had DDNS C2 activity
HOW DIFFERENT?
WITH REGARD TO
Previous incidents used a digitally signed version of an AV product
Companion software
Current incident downloaded a suite of hacktools and add'l backdoors
Past exfil used zipped archives via SFTP
Exfil
Current exfil done via SFTP but uncompressed
Previous attack vectors were drive-by download and phishing attachments
Attack Vector
Lateral attack via compromised business associate network
Past incidents focused on IP
Data targeted
Current incident focused on business and marketing information
Previous incidents stole credentials across several platforms
Stolen Credentials
Current incident used previously stolen credentials, including some unknown as compromised

Heuristic or function-based matching

See PE YARA rules

REPORTING

LEVERAGING YARA FOR REPORTING

Use Case

- Use the meta section of YARA to contain notes
- Use the YARA_Reporter project to write out the metadata, or at least, the rule names

Explore python projects in VM (YARA Reporter)

Files and Slides

https://github.com/CyberDefenses/Conventions

Questions?

Twitter: @montystjohn
LinkedIn: www.linkedin.com/in/monty-st-john-3842692
Github: github.com/corumir
CDI Github: github.com/cyberdefenses