IDENTIFYING UNKNOWN PACKERS WITH 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

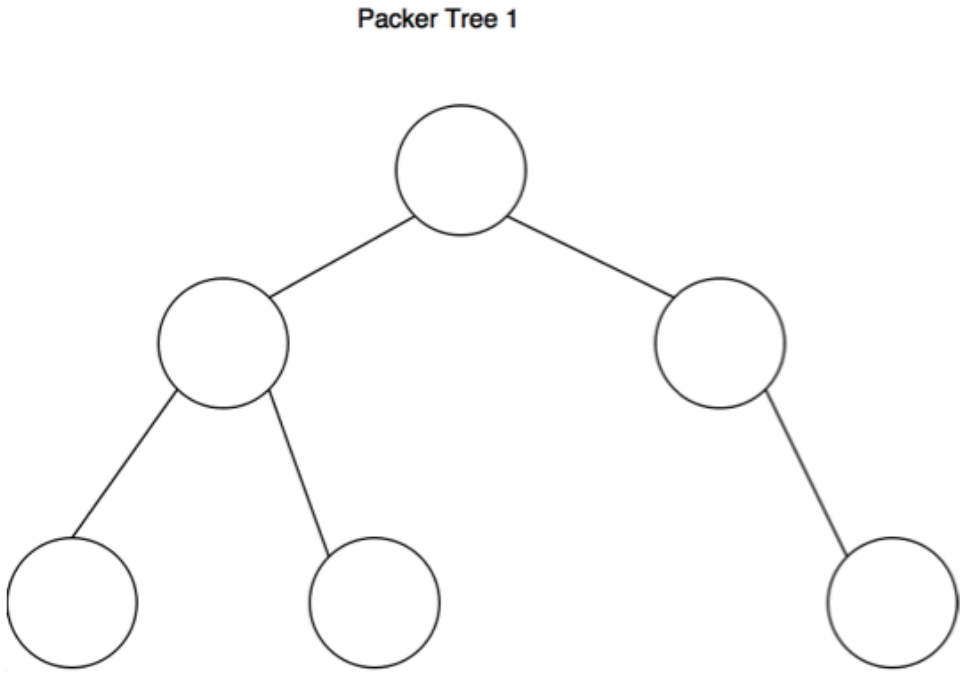
Pattern matching logic. YARA's prime ability is to match patterns.

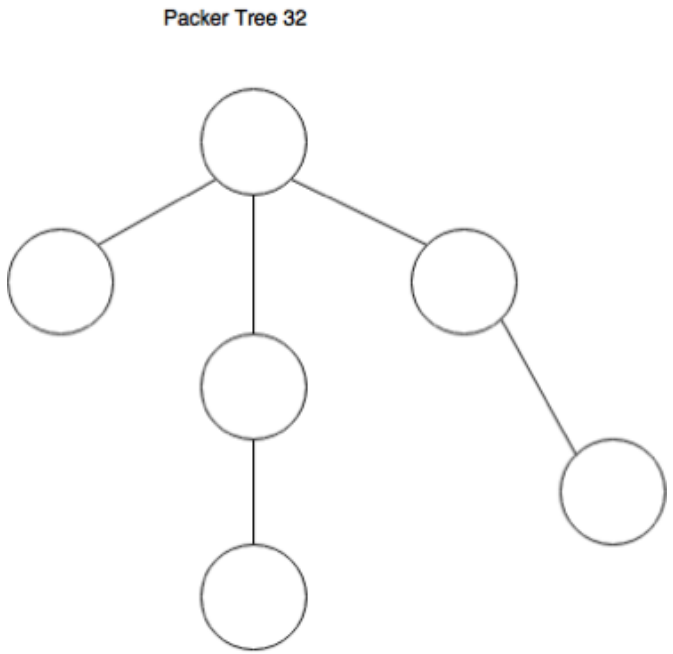
- Explicit or variable patterns (A = 0, B n = n +C, etc.)

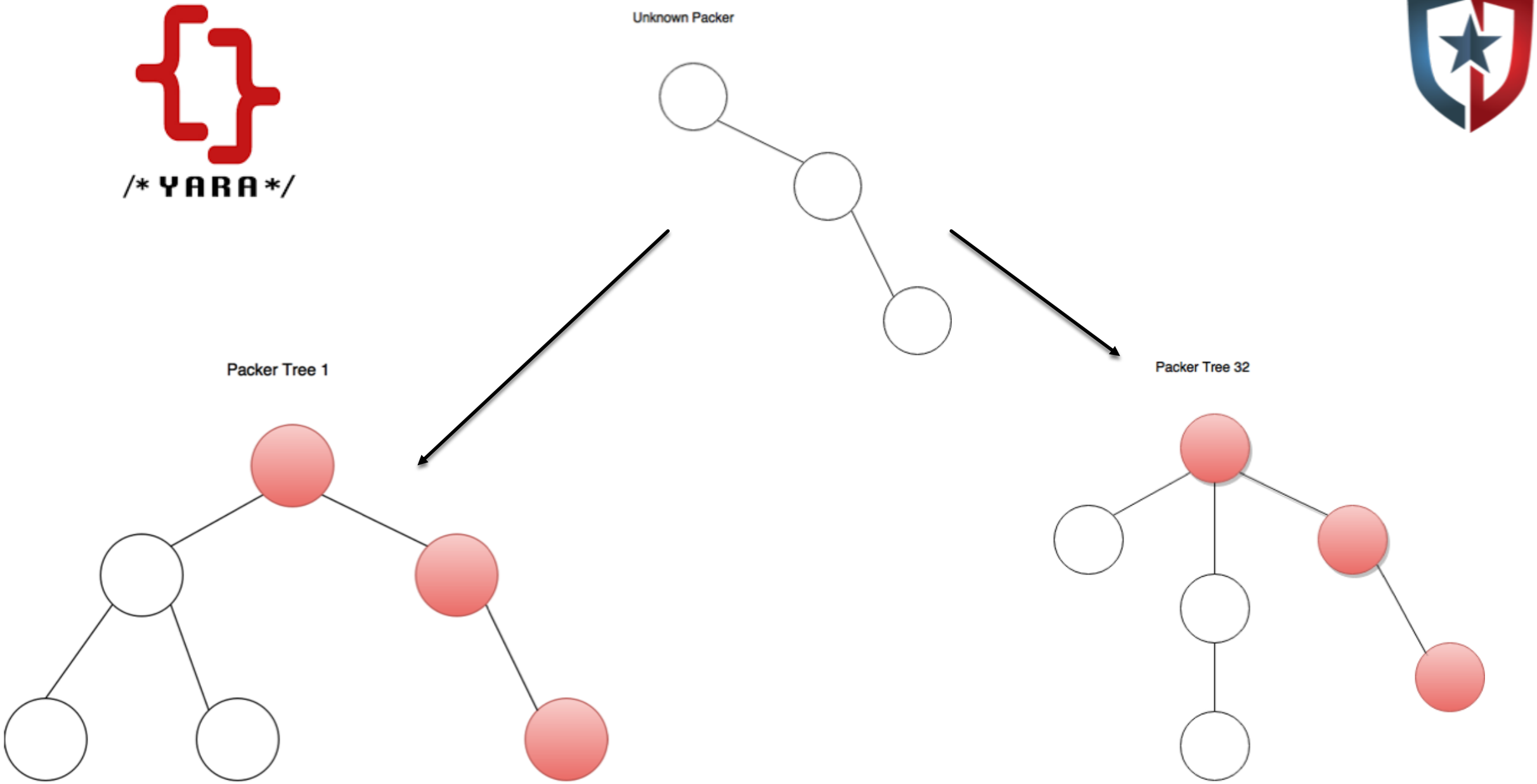
Rule PE_byte_stomping
Rule PE_byte_scavenging
Rule PE_malformed_IAT
Rule PE_malformed_EAT
Rule PE_EP_Beyond_V1
…

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

- Tree pattern matching






/* YARA */
Unknown Packer
Packer Tree 1
Packer Tree 32

Pattern matching logic. 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

Already Using it. It was a no brainer to employ, since we were already employing it.

Flexible. Basic usage of YARA is simple deterministic checks, e.g., string match, yes/no. In reality, higher spectrums of YARA usage allow for heuristic, time-based, order, stacking, spatial-based, and geo-based matching.

Persistence. Combining YARA with a bit of code allows you to leverage in outside variables, and pass information from YARA run to YARA run.

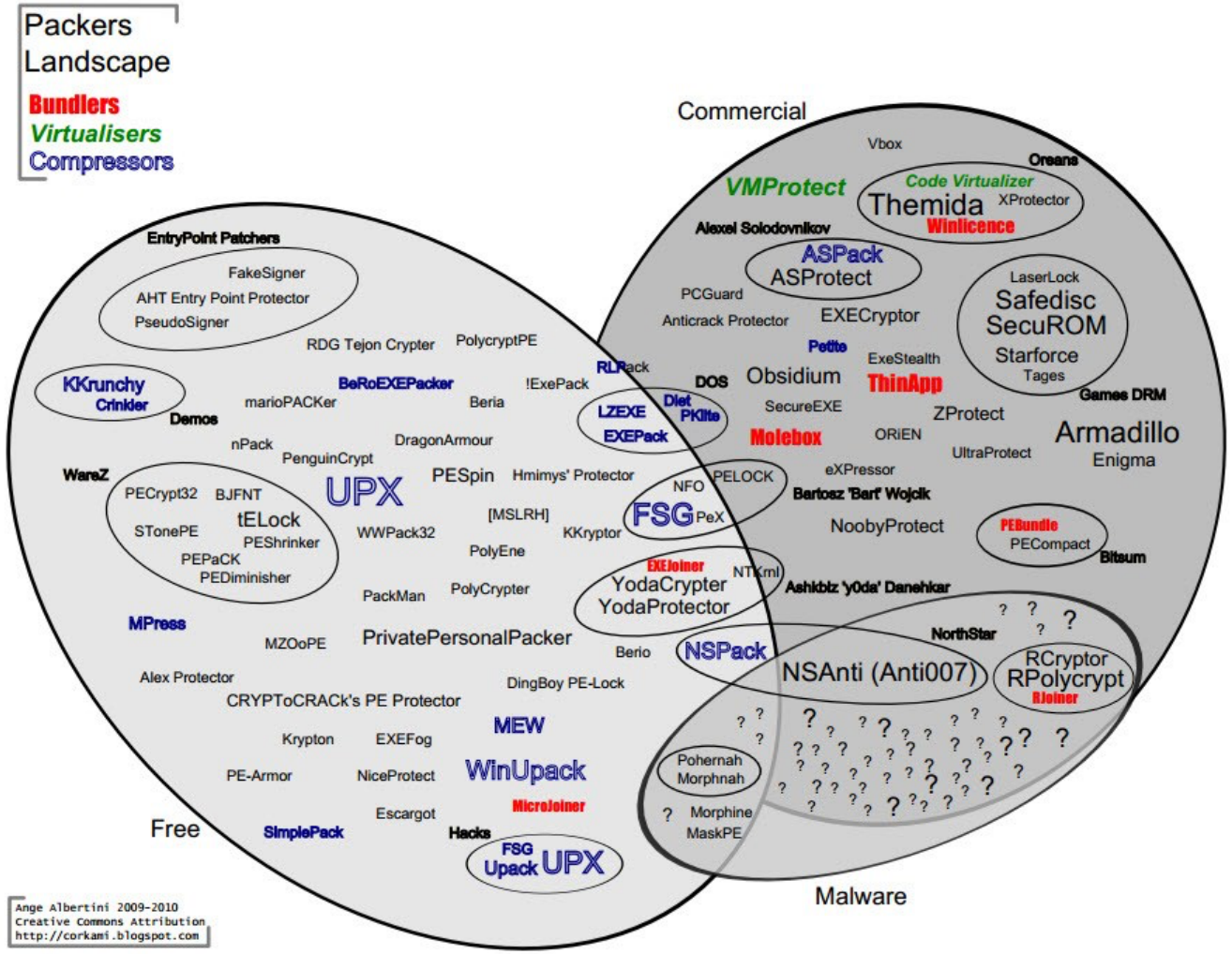
/* YARA */

PACKERS

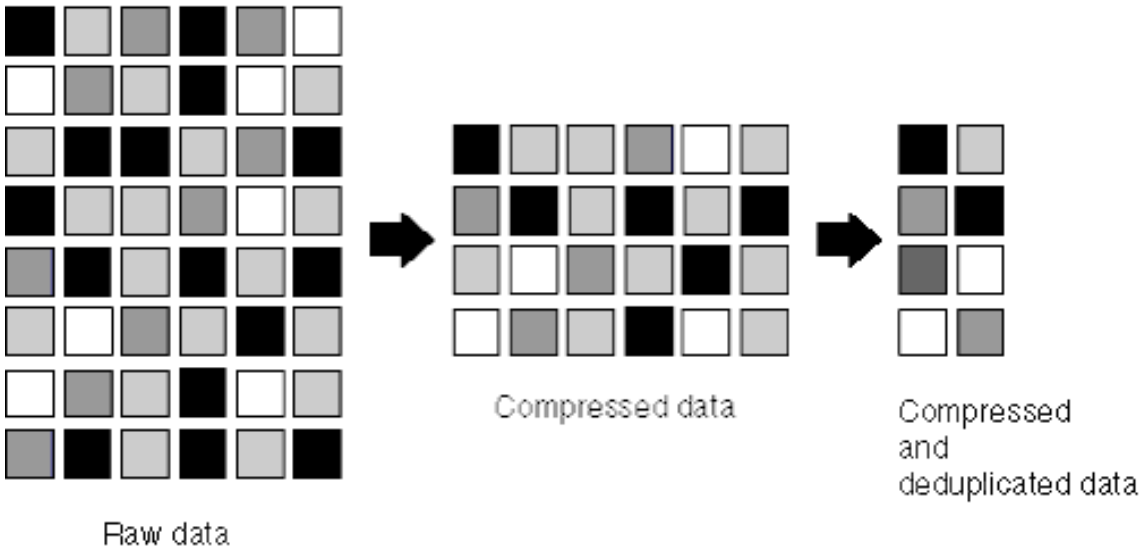
DRIVING INTO THE UNKNOWN

PACKERS

- Packers reduce the physical size of an executable by compressing it.
- A decompression stub is usually then attached, parasitically, to the executable.
- At runtime, the decompression stub expands the original application and transfers control to the *original entry point*.



COMPRESSION

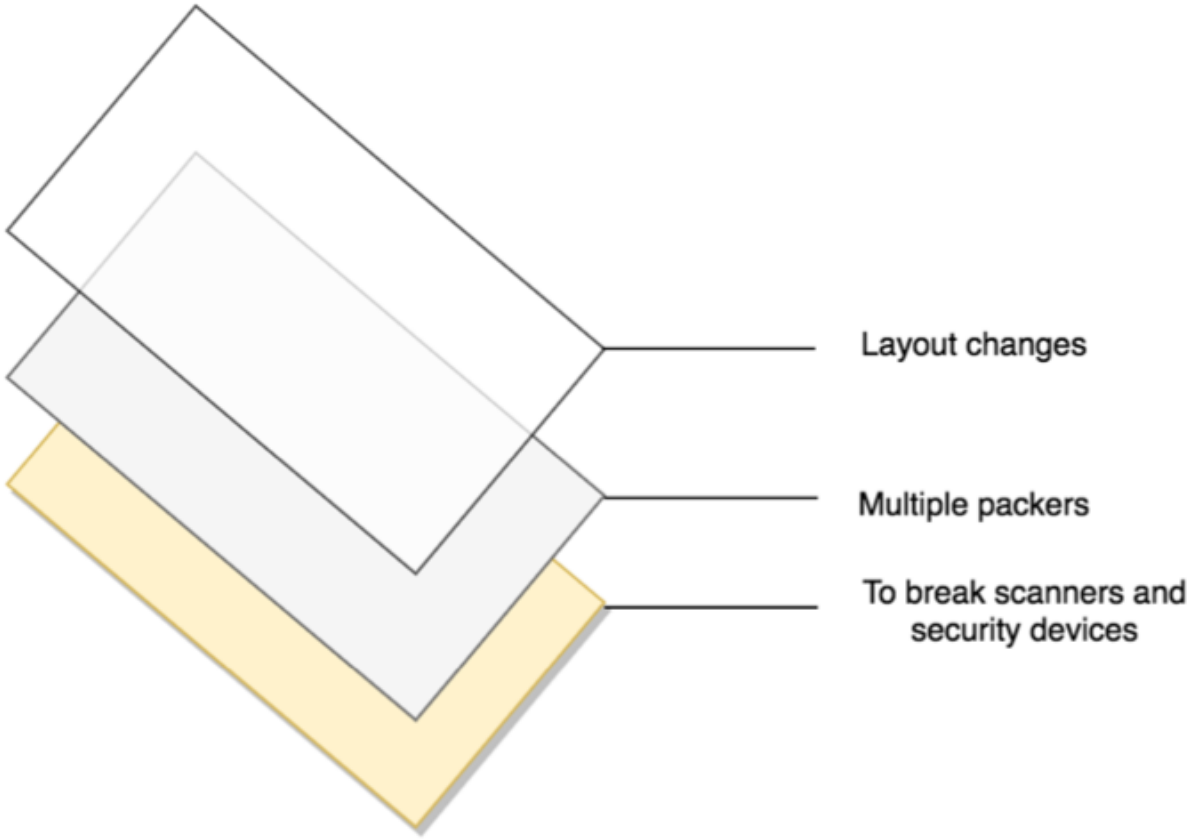


Point 1. Small sized files are respected (likely to pass) more by security devices than large ones.

Point 2. Removing duplicate data helps lower chances of detection, e.g. can deter stacking and counting matching logic by security devices and people.

Point 3. Logistically, small files are easier to handle.

ARMOR

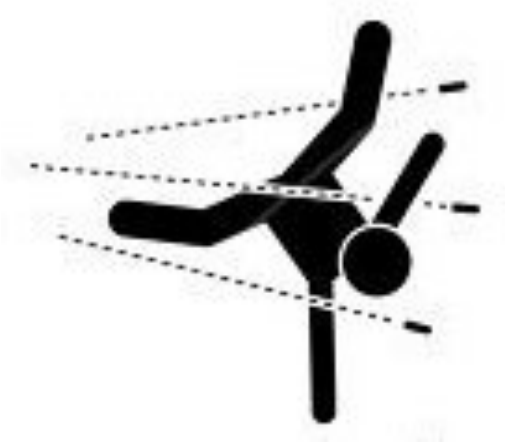


Layout. Adjust and change the layout to raise the difficulty of understanding or reversing the file.

Multiple Packers. To break solutions who have a limited capability to handle double or more packers or to use prestidigitation by showing something expected (normal packer) while its custom puckered inside (eluding detection).

Thwarting. Flat out breaks scanners and detectors or inhibits reversing or analysis if detected.

EVASION



Obfuscation

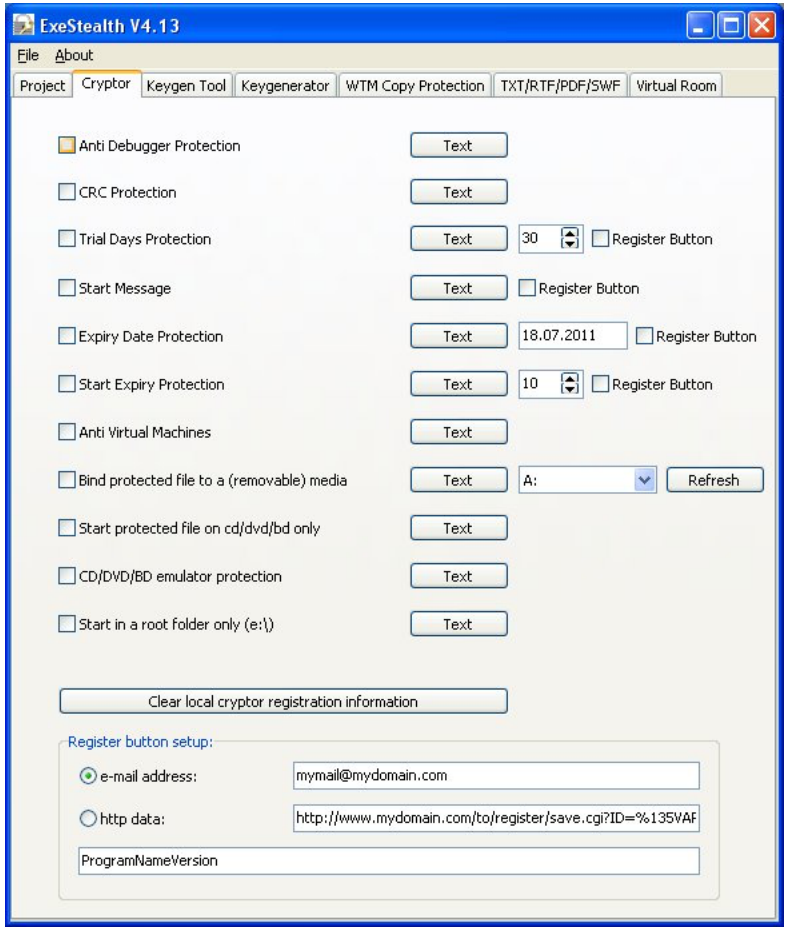
As a way of obfuscating an executable program, i.e., transforming it so the result is still executable and has the same effect when run, but looks different to security and witness devices.

EVASION

“Anti” crowd

The ”anti-” crowd.
Anti-Analysis, Anti-sandbox, anti-VM, etc.

EVASION


ExeStealth V4.13
File
About
Project
Cryptor
Keygen Tool
Keygenerator
WTM Copy Protection
TXT/RTF/PDF/SWF
Virtual Room
Anti Debugger Protection
Text
CRC Protection
Text
Trial Days Protection
Text
30
Register Button
Start Message
Text
Register Button
Expiry Date Protection
Text
18.07.2011
Register Button
Start Expiry Protection
Text
10
Register Button
Anti Virtual Machines
Text
Bind protected file to a (removable) media
Text
A:
Refresh
Start protected file on cd/dvd/bd only
Text
CD/DVD/BD emulator protection
Text
Start in a root folder only (e:\)
Text
Clear local cryptor registration information
Register button setup:
e-mail address:
mymail@mydomain.com
http data:
http://www.mydomain.com/to/register/save.cgi?ID=%135VAF
ProgramNameVersion

EVASION

Transformative

To change its appearance, so the malcode can stay usable for a longer period.

What are we doing here?

- Some packers we know.
- In fact, 1000's of them are documented and identifiable.
- It's the ones we don't know about that are the rub

Where we looked for trouble – and found it!

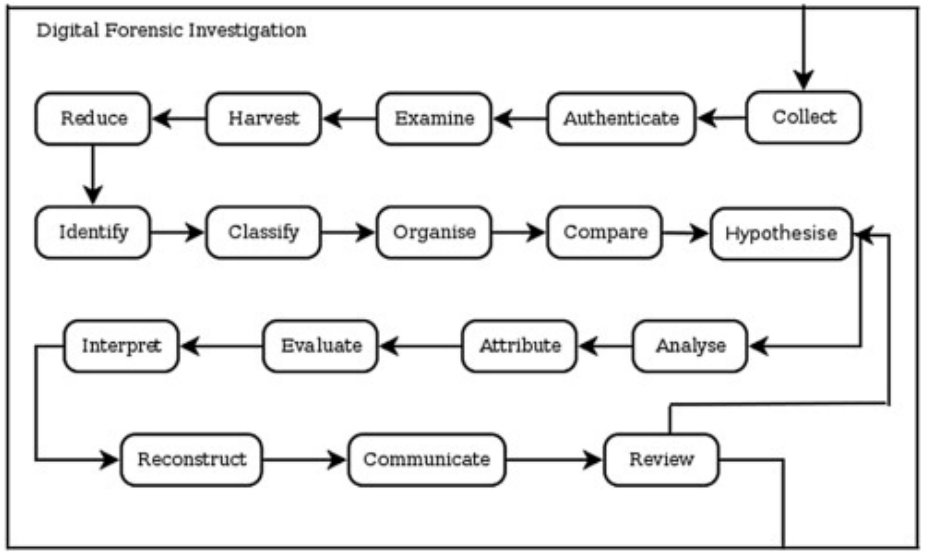
- What did people do before us about finding unknown packers?
- Let's compare it to our own data!

Some results

- The cross-cut of customer benign files showed ~ 5% were packed.
- The same for malicious files we detected over the last year was ~41%
- While this hinted that packing was an indicator for malicious activity, it's not a direct 1:1 by any means

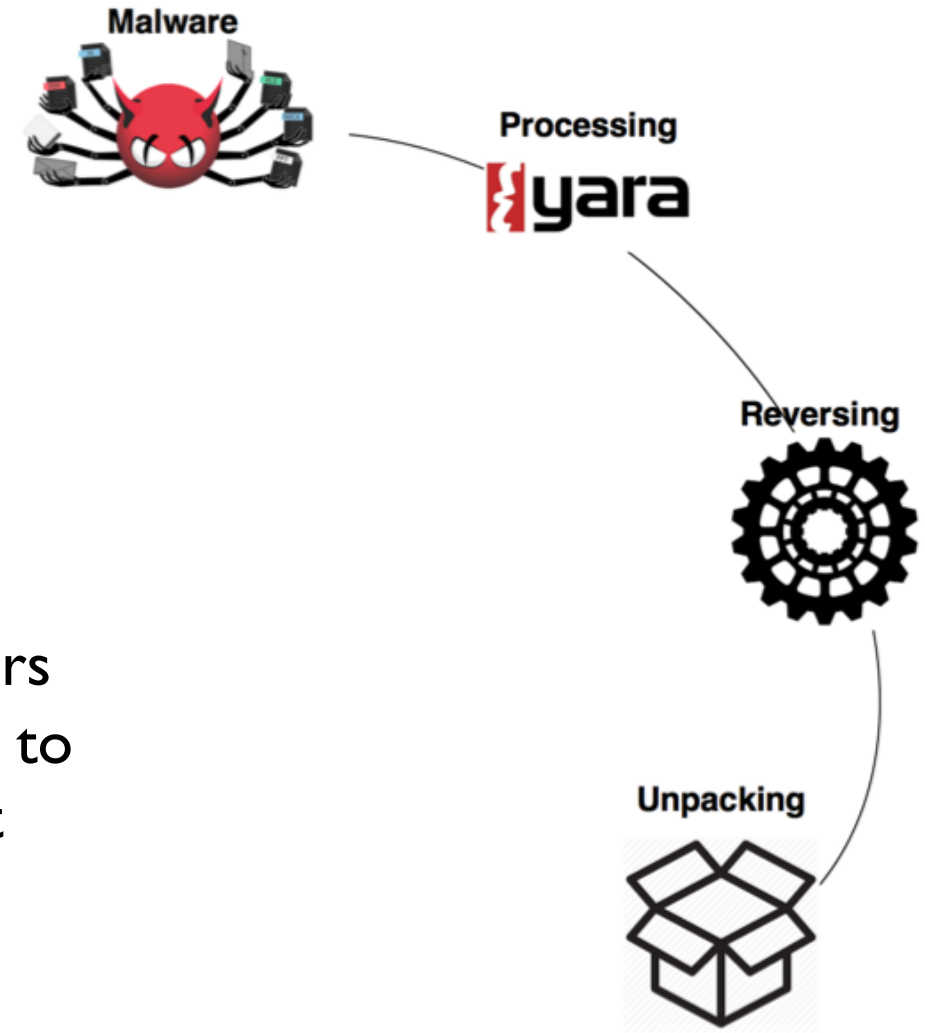
DF/IR Lab ++

- Saw value in using YARA to shape the unpacking effort
- YARA could help identify packer attributes to speed the reversing process
- True goal was an efficiency boost



Some things we checked for

- Entropy and hash
- “anti” tricks
- Structural reorganization
- Byte reuse and stomping
- Code body Evaluation
- Size & location checks (references beyond image size)
- Data within data (binary within hex, etc.)
- …plenty more



The Goal

- identify characteristics of packers
- Pass discovered attributes to reversers
- Push the starting point from zero (0) to halfway by giving intelligence up front

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