Git Your YARA For Nothing and Your Malware for Free

Automating Scanning with thousands of YARA rules

Cooper Quintin - Senior Security Researcher - EFF Threat Lab

Intro

- Cooper Quintin
  - Senior Security Researcher
  - New Parent
  - Laziness is a Virtue
- EFF
  - Non profit
  - Defending civil liberties
  - 30 years
- Threat Lab

Malware that Targets At Risk People

- Activists, human rights defenders, journalists, domestic abuse victims, immigrants, sex workers, minority groups, political dissidents, etc...
- Goals of targeted malware:
  - Gather intelligence on opposition
  - Spy extraterritorially or illegally
  - Blackmail
  - Locate and Capture
  - Harass and Intimidate
  - Stifle freedom of expression

Jeff Bezos Can Afford a Security Team

Cybersecurity and AV companies care about the types of malware that affects their customers (usually enterprise.)

We get to care about the types of malware the infringe on civil liberties and human rights of at risk people.

This guy is not at risk.

Our Goals

- Protect People
- Broaden our communities` understanding of threats and defenses
- Expose bad faith actors
- Make better laws

Typical Process

1. Receive Sample
2. Triage Sample
3. Dynamic Analysis
4. Static Analysis
5. Attribution (is hard)
6. Report

Typical Process

1. Receive Sample
2. Triage Sample
3. Dynamic Analysis
4. Static Analysis
5. Attribution (is hard)
6. Report

Triaging Samples

Goals:

- Determine if sample is known.
- Determine if sample is crimeware/spam or targeted.
- Scan a possibly infected computer for samples to further investigate.

Triaging By Hand

Triaging with YARA

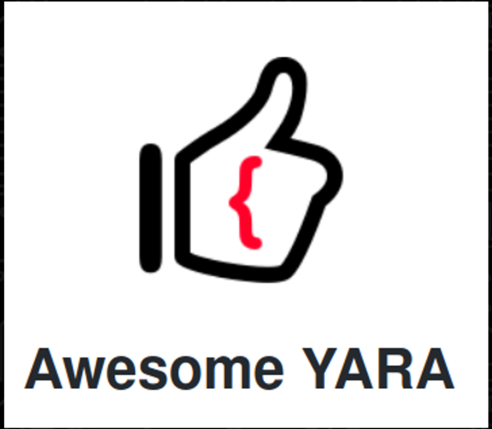
Full Disclosure

1. I am a YARA noob!
2. I am fundamentally lazy.

I love writing Yara rules but I can only write so many useful ones, my time is limited and there is a lot of malware out there.

Luckily people much smarter than me, including people on this stage, have already written a ton of great rules!

Let’s Not Reinvent the Wheel!



https://github.com/InQuest/awesome-yara

Some of My Favorites

- Apple OSX
  - Apple has ~40 YARA signatures for detecting malware on OSX. The file, XProtect.yara, is available locally at /System/Library/CoreServices/XProtect.bundle/Contents/Resources/.
- Citizen Lab Malware Signatures
  - YARA signatures developed by Citizen Lab. Dozens of signatures covering a variety of malware families. The also inclde a syntax file for Vim. Last update was in November of 2016.

Some of My Favorites

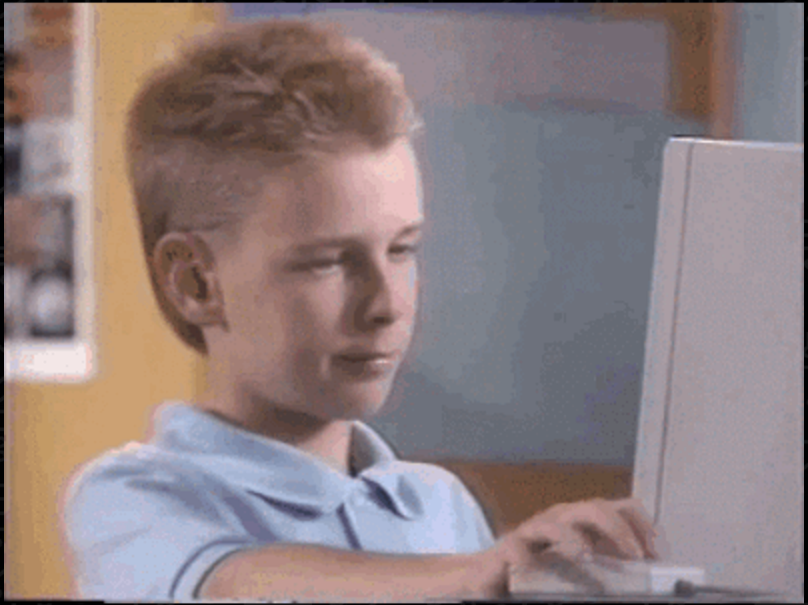
- mikesxrs YARA Rules Collection
  - Large collection of open source rules aggregated from a variety of sources, including blogs and other more ephemeral sources. Over 100 categories, 1500 files, 4000 rules, and 20Mb. If you're going to pull down a single repo to play with, this is the one.
- YaraRules Project Official Repo
  - Large collection of rules constantly updated by the community.

Some of My Favorites

- Florian roth rules
    - Florian Roth's signature base is a frequently updated collection of IOCs and YARA rules that cover a wide range of threats. There are dozens of rules which are actively maintained. Watch the repository to see rules evolve over time to address false positives / negatives.
- X64 Debug Rules
    - Great collection of rules for identifying packers and crypto constants.

“But Cooper, I don’t want to download and dig through almost 50 repositories of yara rules of varying quality, that sounds like a chore.”

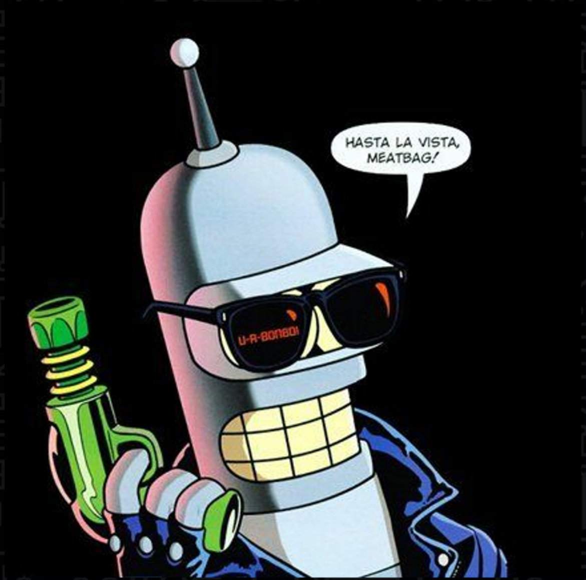
I Got You



Introducing YAYA

Yet Another Yara Automaton

- Download Open Source Rulesets
- Keep them up to date
- Ignore problematic rules
- Add your own rules
- Run scans
- Uses go-yara (thanks Hilko!)
- https://github.com/cooperq/yaya



Demo

Pardon me while I sacrifice this chicken to the demo gods.

Potential Uses

- Put it in your email scanning pipeline.
- Scan a possibly infected server or client device with it.
- Scan cloud storage uploads.
- Quickly triage and classify new samples.

It’s open source so please file bugs and add features if you like it.

Thank you!

Cooper Quintin
Senior Security Researcher
EFF Threat Lab
cooperq@eff.org - twitter: @cooperq

https://github.com/cooperq/yaya