SIX YEARS OF THREAT INTEL

Have we learned nothing?
IT STARTED WITH A SIMPLE QUESTION…

Are we getting better at communicating useful threat intel over time?
SO I TRIED TO ANSWER THE QUESTION
Focused on “advanced” threats, since that’s where most of the reporting is anyway. Feeds & intel sharing sites are out of scope (for now?)

Kiran Bandla’s APTNotes site is a great collection of these reports (https://github.com/kbandla/APTnotes)

I analyzed all the 2010 reports, plus a random selection of 2015 reports
EXPONENTIAL INCREASE IN REPORTS

Number of Reports vs. Year

- Solid line: Number of Reports
- Dotted line: Trend (Exponential)
GOOD THING LENGTH IS GOING DOWN!
MEASURING INDICATOR USEFULNESS

- **Tough!**
- **Challenging**
- **Annoying**
- **Simple**
- **Easy**
- **Trivial**
MEASURING INDICATOR USEFULNESS

Detection Maturity Levels

- DML-8: Goals
- DML-7: Strategy
- DML-6: Tactics
- DML-5: Techniques
- DML-4: Procedures
- DML-3: Tools
- DML-2: Host & Network Artifacts
- DML-1: Atomic Indicators

What they want
How they plan to get it
Evidence left during or after the act

© 2016 Sqrrl | All Rights Reserved
COMBINED INDICATOR HIERARCHY

- Goals
- Strategies
- TTPs
- Tools
- Artifacts
- Domains
- IP Addresses
- Hash Values
- Other
THE AVERAGE REPORT HAS…

- Goals
- Strategy
- TTPs
- Tools
- Artifacts
- Domains
- IP Addresses
- Hashes
- Others

© 2016 Sqrrl | All Rights Reserved
There are different types of indicators for different purposes. Most security teams need detection indicators.

Most reports lag events by weeks or months.

If you consume reports, assume low-level indicators are already blown unless otherwise noted.

If you’re looking for detection/response intel, most reports are not for you.
IF YOU PRODUCE REPORTS…

Make consumption easier!

Keep the documents brief. No one can read all these.

• At least, provide a meaty-but-concise exec summary

List indicators in an appendix.

• Group them by type, with bulleted text for high level indicators

• Include relevant context (actor, kill chain phase, etc)

• Provide machine-readable (CSV, JSON, STIX, etc) file to speed consumption and reduce transcription errors
QUESTIONS?

David J. Bianco

dbianco@sqrrl.com

@DavidJBJBianco