sqrrl

Securely explore your data

SIX YEARS OF THREAT INTEL

Have we learned nothing?

MANDIANT®

McAfee

APT1

Exposing One of China's C
Espionage Units

SHADOWS IN THE CLOUD:
Investigating Cyber Espionage 2.0

AURORA

February 10, 2010

THE DUKES

7 years of Russian cyberespionage

TLP: WHITE

This whitepaper explores the tools - such as MiniDuke, CosmicDuke, OnionDuke, CozyDuke, etc- of the Dukes, a well-resourced, highly dedicated and organized cyberespionage group that we believe has been working for the Russian Federation since at least 2008 to collect intelligence in support of foreign and security policy decision-making.

F-SECURE LABS
THREAT INTELLIGENCE
Whitepaper

IT STARTED WITH A SIMPLE QUESTION…

Are we getting better at communicating useful threat intel over time?

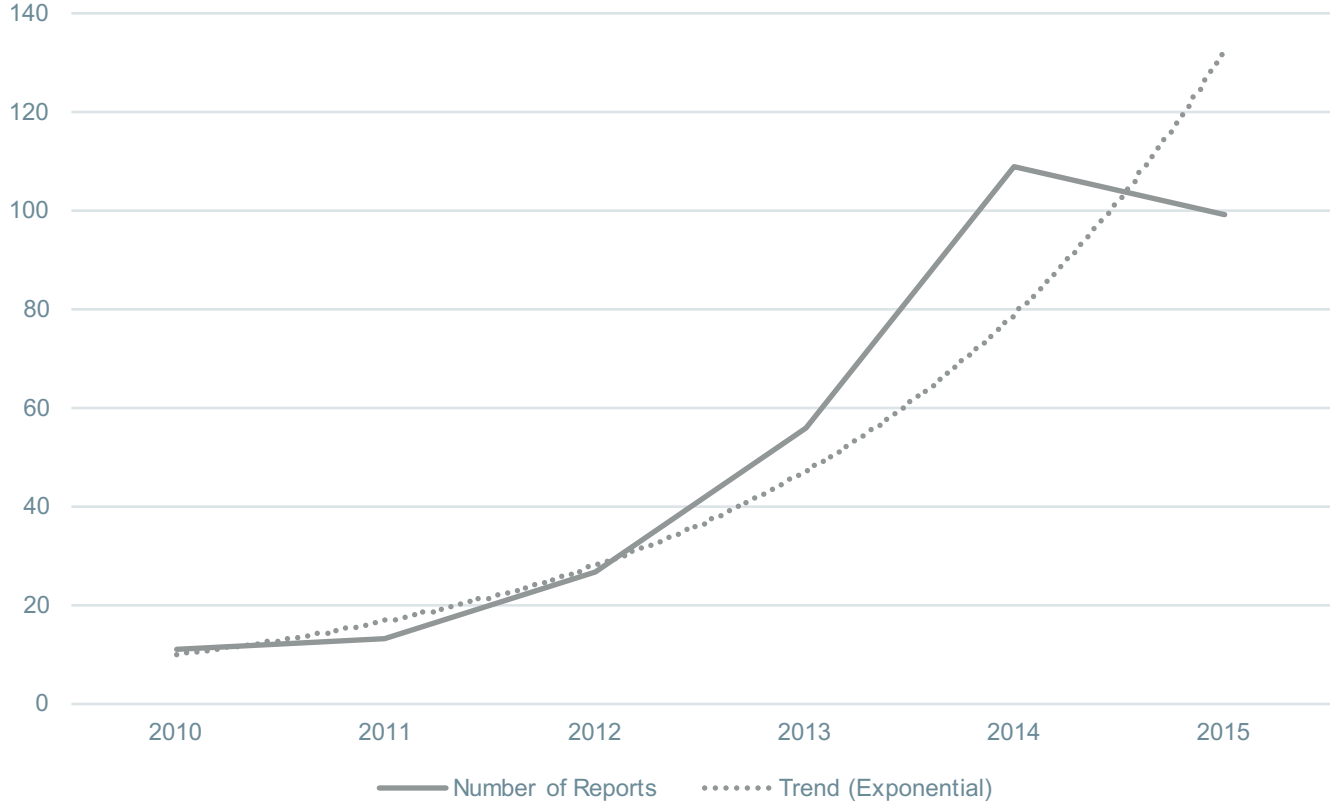
SO I TRIED TO ANSWER THE QUESTION

Focused on “advanced” threats, since that’s where most of the reporting is anyway. Feeds & intel sharing sites are out of scope (for now?)

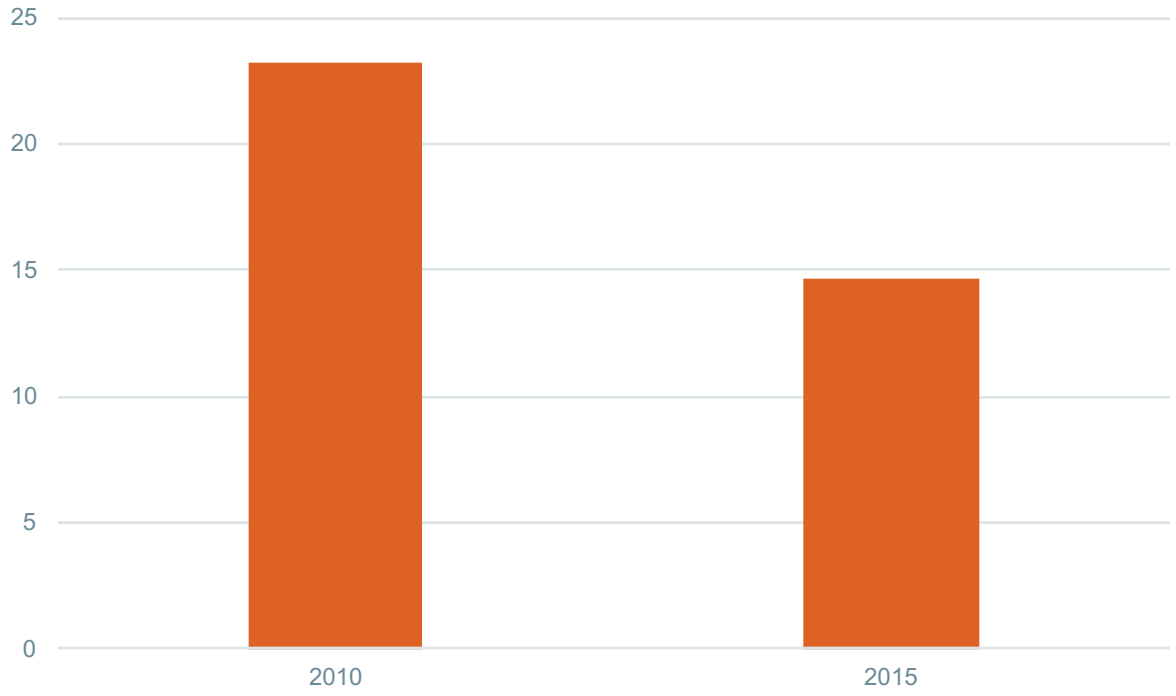
Kiran Bandla’s APTNotes site is a great collection of these reports (https://github.com/kbandla/APTnotes)

I analyzed all the 2010 reports, plus a random selection of 2015 reports

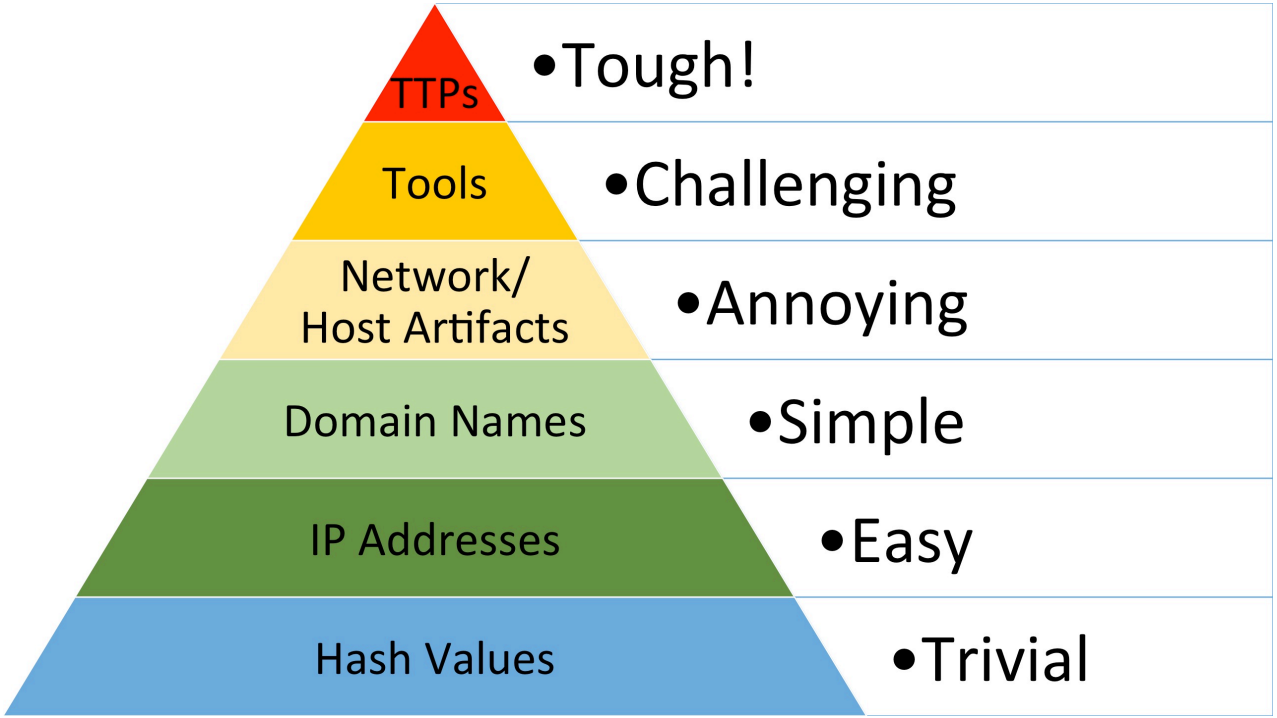
EXPONENTIAL INCREASE IN REPORTS



GOOD THING LENGTH IS GOING DOWN!

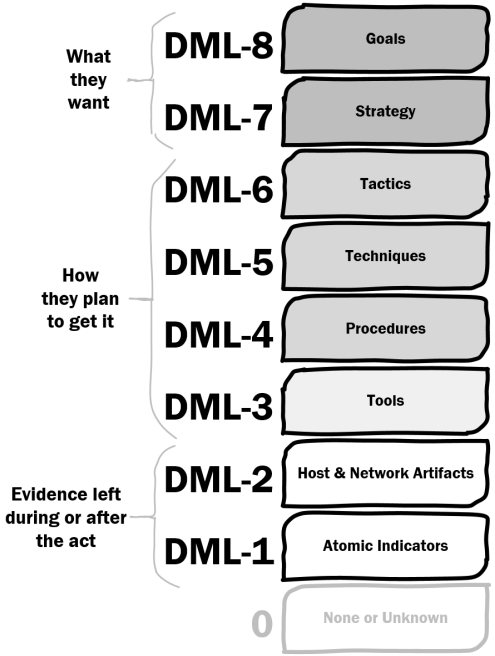


MEASURING INDICATOR USEFULNESS



http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

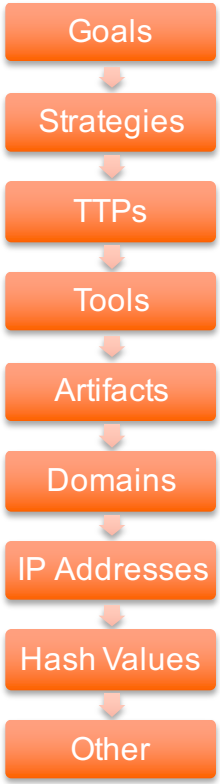
MEASURING INDICATOR USEFULNESS



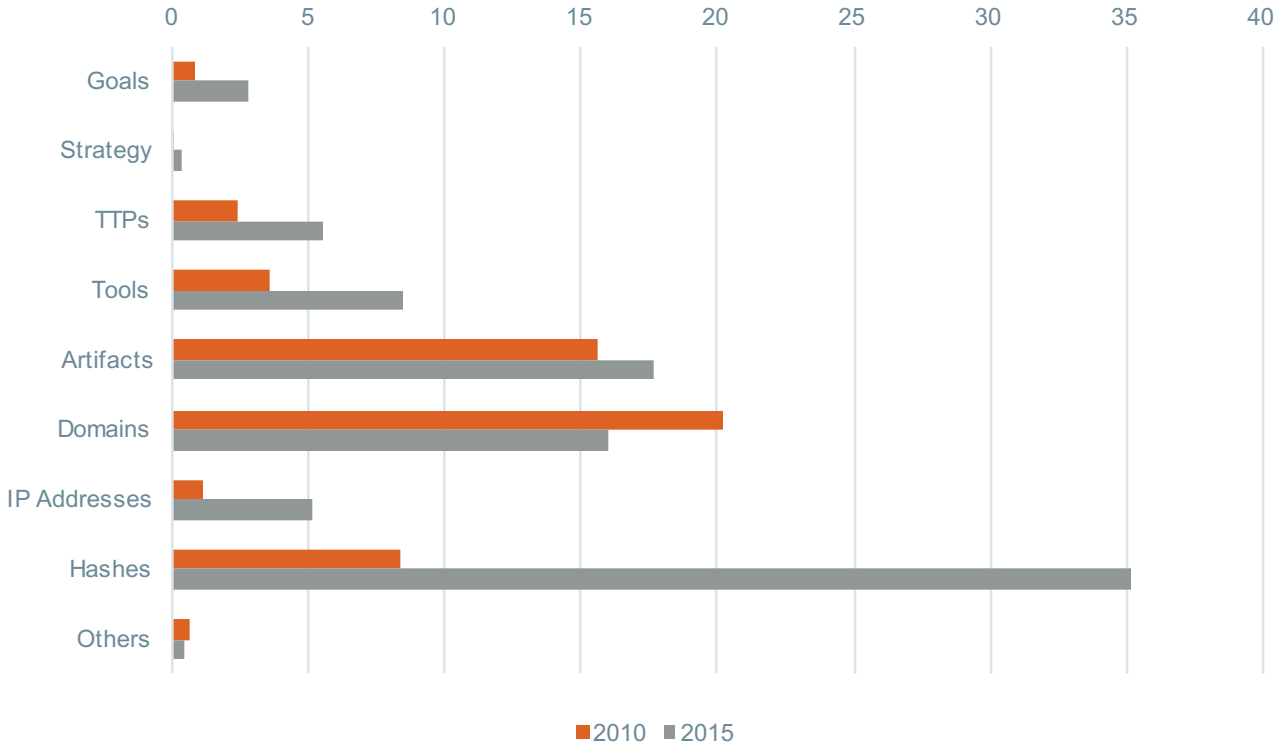
Detection Maturity Levels

http://ryanstillions.blogspot.com

COMBINED INDICATOR HIERARCHY



THE AVERAGE REPORT HAS…



WHAT IS THIS INTEL GOOD FOR?

Detection

- If this event happens, I want to know about it.

Attribution

- Who/what is responsible for this activity?

Profiling

- What are the targeting parameters for this threat?

Prediction

- Given the current state, what can I expect from this threat in the future?

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

@DavidJBianco