Maximizing value of your Threat Intelligence for Security Incident Response

Assess indicators on a massive scale

PRESENTER: Jonathan Tomek
Director of Threat Research
LookingGlass (www.lgscout.com)

Outline

- Threat Data, both a blessing and a curse
- Determine what is relevant
- Obtain necessary context
- Maintain current data
- Summary and Conclusion
- Questions

Threat Data, both a blessing and a curse

- **Threat Analysts** typically learn and understand context related to the global internet security for future improvement and risk reduction
  - Broad coverage, historical context important
  - Long timeline and focus

- **Incident Responders** respond to an incident or artifact that is occurring or has occurred
  - Accuracy and timeliness of data critical

- Turning data into intelligence that drives more accurate and effective decisions is key to both Threat Analysts and Incident Responders

- Having broad data coverage can help Incident Responders, but can be a significant burden on systems and time to resolution

What Threat Data is relevant to an incident?

- What aspects of an incident are known?
  - Can help drive what threat data is helpful to resolve the incident (**context**)
- What indicators are relevant?
  - How do I determine (**scope, time**)
- Is it possible to act upon all of these indicators?
  - Should we? (**context**)
- Can we reduce the volume?
  - What if we miss a major event! (**relational**)
- Which indicators are better than others?
  - Are the indicators still relevant? (**time**)

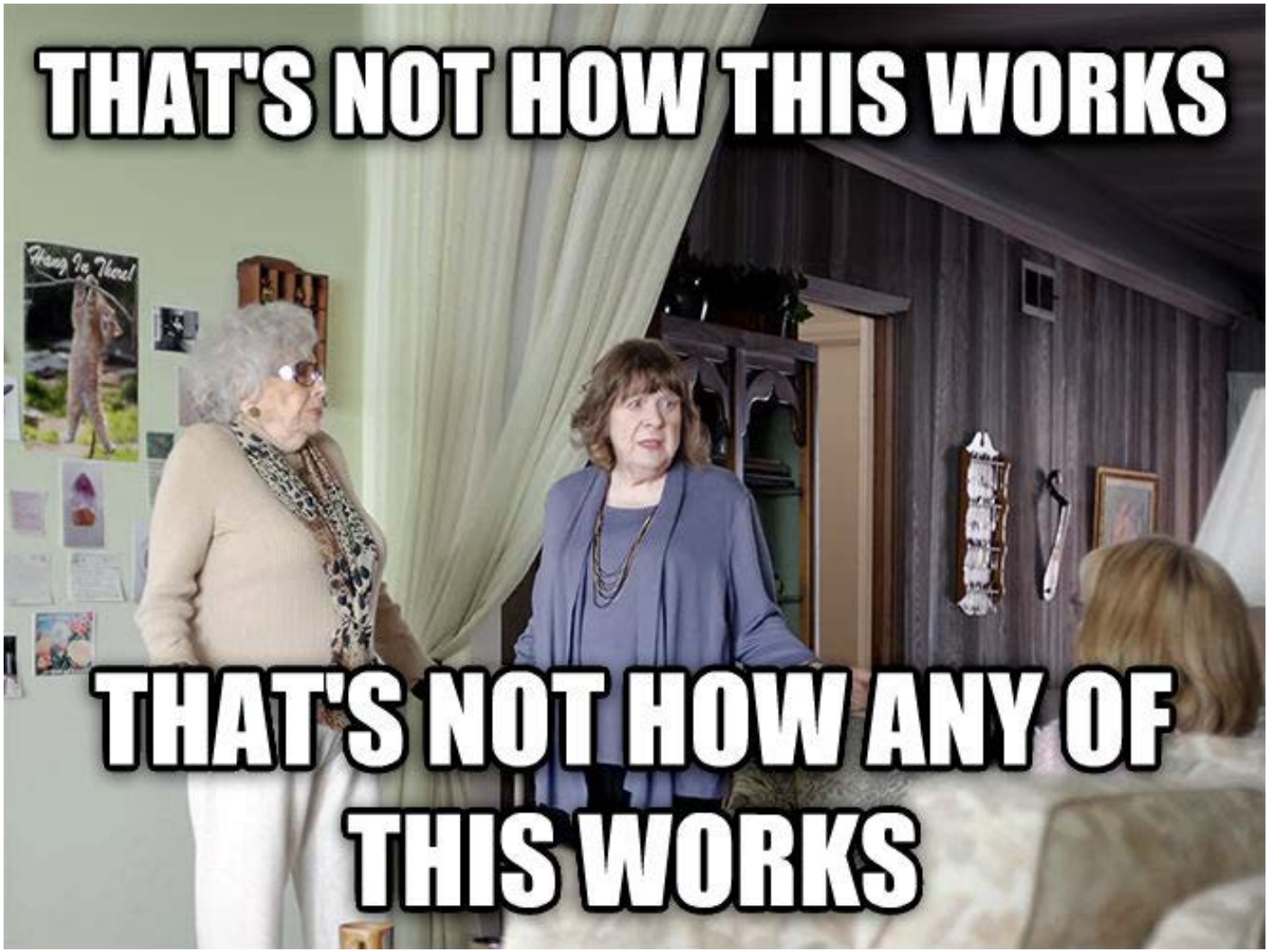
What Threat Data is relevant to an incident?

- Threat Data can include indicators…
  - by the thousands, millions, billions
  - of IP addresses, domains, hashes, emails, protocols, ports
  - by geography
  - by sector/scope
  - Frequency -> “real-time”, daily, ad-hoc
  - Indicators come from many possible sources (usually without much context)
    - Some are reliable/accurate
    - Some are not

All the Things!

- Add all the indicators to our firewalls and SIEMs

We really cannot do that



How to Determine What is Relevant

- Approaching the problem of feeds and other data
  - Some are high quality, low volume
  - Some are high volume, low quality
  - Some are high accuracy, low relevance
  - All of them are needed to detect malicious activity
  - None of them are able to detect every malicious event
- Determine/Assess security posture of assets including patch levels, known vulnerabilities
- Combine all relevant data together
  - Group them by CIDR, AS, Company, Country, etc.
  - Increases context, Decreases volume of indicators

How to Obtain Necessary Context

- Combining all data paints a larger, more detailed picture
  - Look for patterns and connections of related data
  - Having multiple feeds does not hurt, it helps
  - False positives start to find themselves
  - The tree of indicators grows and balances itself out

Happy Little Tree

How to Obtain Necessary Context

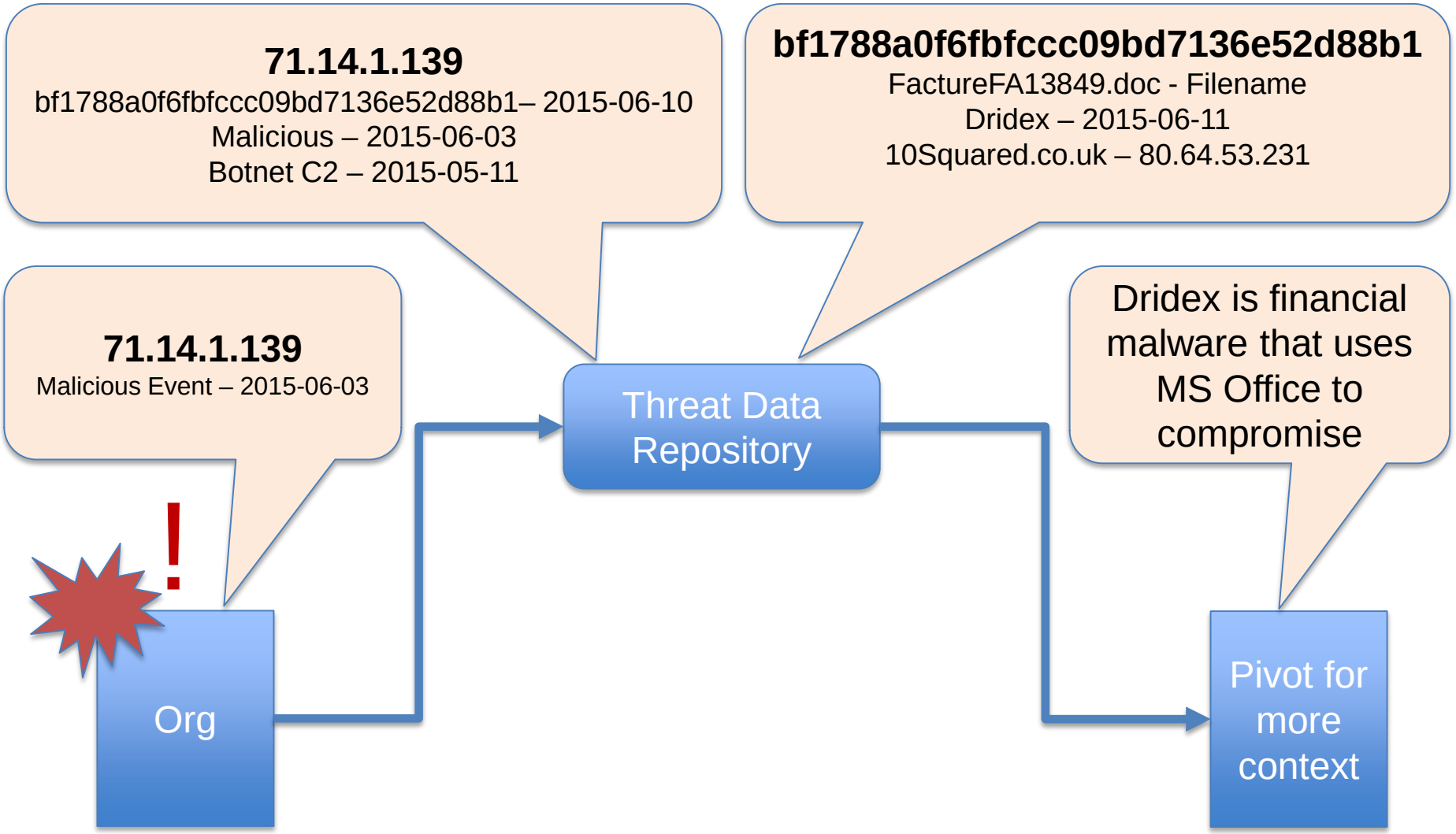
- Indicators overlap, more context
  - Not just labeled as “Malicious”, “Botnet”, “Feed X” anymore
  - Some may still have low context, but that is okay (next point)

- Positive and Negative Weights of Threat Data
  - Indicators are commonly labeled with negative values
  - Positive indicators offset the scale to ensure that not all data looks bad

How to Obtain Necessary Context

- Story time
  - We get an alert of an infected host then do a quick search
  - Find out that IP address is labeled as “Malicious”
  - The IP address is also related to a hash… “Dridex”
  - We can look up more on Dridex, reports, and gain more context for resolution steps
  - Took a low-context low-level indicator and made it relevant

How to Obtain Necessary Context



How to Obtain Necessary Context

- Another benefit to combining a large amount of data
  - Each alert on an indicator is a counter against itself
  - Each indicator also relates to itself going upwards
- Marking a CIDR, AS, Country, Organization as malicious
  - Indicators whether domain or IP address tie to something
  - Domains tie to WHOIS data and companies that host them
  - IP addresses tie to CIDR blocks, AS, Countries
- It is now easier to raise alert levels of other events from this combined context

Story Time part 2

Malicious IP addresses (count)

193.169.245.14 - 2
193.169.245.39 - 3
193.169.245.44 - 10
193.169.245.45 - 9
193.169.245.82 - 1
193.169.245.101 - 1
193.169.245.143 - 9
193.169.245.207 - 5
193.169.245.208 - 1

Subnet 193.169.245.0/24?
Malicious Advertising
Magnitude EK

inetnum: 193.169.244.0 - 193.169.245.255
descr: FOP Zemlyaniy Dmitro Leonidovich
country: NL
organisation: ORG-FZDL2-RIPE
org-name: FOP Zemlyaniy Dmitro Leonidovich
org-type: LIR
address: FOP Zemlyaniy Dmitro Leonidovich
address: Zemlyaniy Dmitro
address: Onore de Balzaka str. 86, app.29
address: 02232
address: Kyiv
address: UKRAINE

Actual full block of IP addresses
193.169.244.0 - 193.169.245.255
We could consider the full range malicious

https://isc.sans.edu/forums/diary/Malicious+Ads+from+Yahoo/17345

How to Maintain Current Data for the (Pre)incident

- The massive volume of indicators overwhelms systems
  - Scaling is very important
- Is it even possible to leverage all the indicators?
  - Possibly, but who has that kind of money
  - Best method is to reduce down to what directly affects you
- Indicators age just like the news
  - A bad domain is not necessarily bad forever
  - Each time a feed alerts on an indicator, timer resets
  - If an indicator is a week, month, year old, is still high alert?

How an Responder Needs to Look at Threat Data

1. Focus on threat data that can provide scope and relevancy to your organization while not under attack

2. Focus on building capability to leverage threat data into threat intelligence for incident response

3. We can combine all these elements together
   - Volume of indicators
   - Context
   - Time
   - Relations

LOOKINGGLASS

Thank you

www.lgscout.com

Jonathan Tomek

Director of Threat Research

Cyber Threat Intelligence Group

jtomek@lgscout.com

@Sakebomb