RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: **EZCL-R07**

The Attribution Game: When Knowing Your Adversary Matters

Katie Nickels

Principal Intelligence Analyst, Red Canary

red canary

#RSAC

Why We're Here

- **What is our goal?**
  - Better understand attribution and how we should handle it
- **How will we achieve it?**
  - Gain this understanding by discussing with each other

Agenda

- **Frame Our Topic**
- **Ask Questions**
  - Ask and answer questions as a large group
- **Dive Deeper**
  - Discuss further in small groups
- **Share Our Takeaways**
  - Provide read-outs from each small group to the large group
- **Wrap Up**

Frame Our Topic

Let’s talk about attribution

What Attribution Can Feel Like

The Classic Mystery Face Game
GUESS WHO ?
Features original art & gameplay
Does your person have blue eyes?
Is your person wearing a hat?
Hasbro Gaming
WARNING:
CHOKING HAZARD Small parts
Not for children under 3 years
Richard
Eric
George
Maria

What is Attribution?

- Associating adversary activity with something else
- Many different definitions → *confusion*

What are Different Types of Attribution?

- We can attribute to…

The "who"

- A person
- A team or unit
- An organization
- A government

The "how"

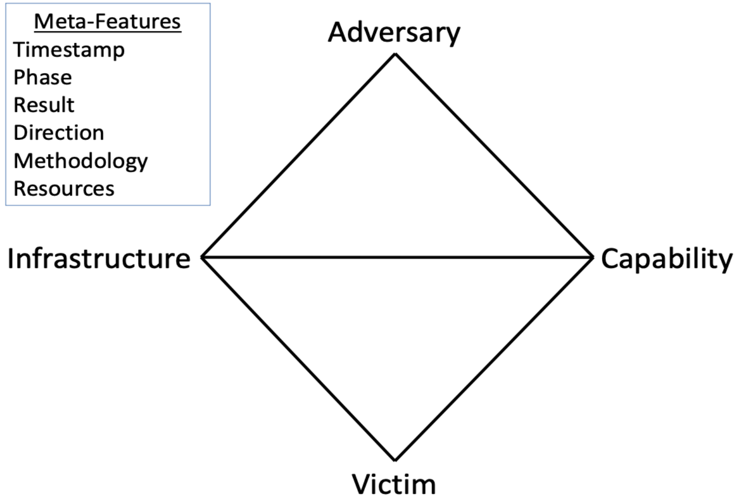
- Tools/malware
- Other code
- Tactics, techniques, and procedures (TTPs)
- Infrastructure

How Do We Perform Attribution?

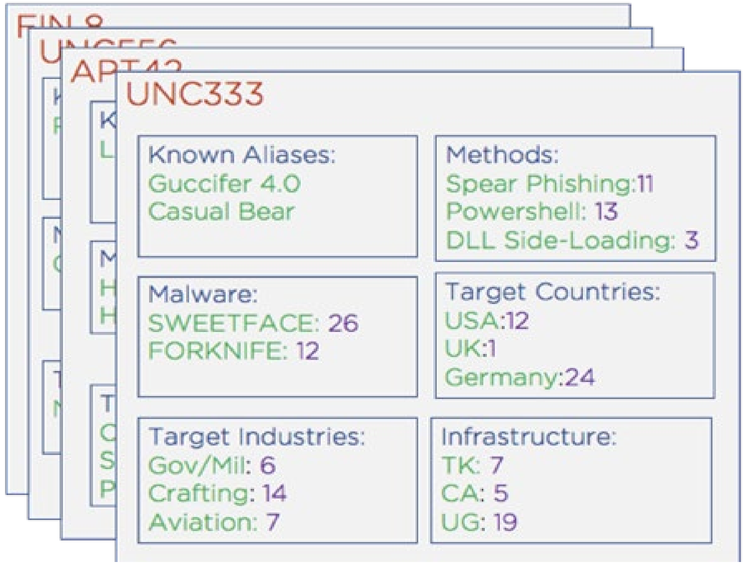
- **Find patterns and connections**
- Look for human fingerprints
  - Personas, email addresses, passwords
- Use operational security failures by adversaries
  - Reusing account names (e.g. UglyGorilla) or infrastructure
- Leverage different sources depending on collection
  - HUMINT (human sources)
  - SIGINT (intercepted communications)
  - OSINT (news stories, WhoIs, Passive DNS, malware research)

Different Methods of Attribution

- Associate what you find with someone else’s research
- Create your own clusters



https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf



UNC333

Known Aliases:
Guccifer 4.0
Casual Bear

Methods:
Spear Phishing:11
Powershell: 13
DLL Side-Loading: 3

Malware:
SWEETFACE: 26
FORKNIFE: 12

Target Countries:
USA:12
UK:1
Germany:24

Target Industries:
Gov/Mil: 6
Crafting: 14
Aviation: 7

Infrastructure:
TK: 7
CA: 5
UG: 19

https://www.fireeye.com/blog/threat-research/2019/03/clustering-and-associating-attacker-activity-at-scale.html

Does Attribution Matter?

- It depends on *what you need:* **your requirements**
- Sometimes it matters a lot
  - Making business decisions
  - Using instruments of power
    - Diplomatic, Informational, Military, Economic
- Sometimes it matters less
  - Defending networks
  - Responding to incidents (what about **red teams**?)

RSAConference2020

Ask Questions

Ask and answer questions as a large group

Dive Deeper

Discuss further in small groups

Possible Discussion Questions

- How does *your* team define attribution?
- What are your key requirements for your cyber threat intelligence team?
- When does attribution matter to your team? When does it **NOT** matter?
- How does your team go about performing attribution?
- What limitations do you have in performing attribution? What additional collection or information could help you?
- How can we better communicate clearly about attribution?

RSAConference2020

Share Our Takeaways

Provide read-outs from each small group to the large group

Wrap up

Talk about how you can apply what you’ve learned

Apply What You've Learned Today

- Decide how your team defines attribution
- Identify your team's requirements around attribution
- Determine how you will track adversaries given those requirements

Thank you!

Katie Nickels

Principal Intelligence Analyst, Red Canary

@LiketheCoins

@RedCanaryCo