RSAConference2020

Cooperative Learning

HUMAN ELEMENT

The Attribution Game: When Knowing Your Adversary Matters

RSA Cooperative Learning Session Summary

Session ID EZCL-R07

Katie Nickels, Principal Intelligence Analyst, Red Canary

red canary

All About Attribution

In February at the RSA Conference 2020, it was a pleasure to bring together a group of almost 60 people to discuss a tough topic for analysts: attribution. There are many types and methods of attribution, so we often talk past each other as we debate it. Participants in the discussion listened to me provide a framing discussion to get everyone on the same page about attribution of cyber adversaries. Using that common understanding, we discussed and debated what works, what doesn't, and how we can better tackle the challenge of attribution. I'm pleased to report that it was an excellent discussion full of spirited, respectful debate!

Framing the Issue of Attribution

Defining Attribution

A good place to start in order to have a productive discussion is by defining the word "attribution" in a cybersecurity context. A simple definition I use is that attribution is the act of associating cyber activity with something else. I admit, that's a frustrating and broad definition, but I use it for a reason: many people define and perform attribution differently, which is what leads to this being such a tough topic for us to discuss.

Here are a few common types of attribution that analysts commonly use. I like to bin these into *the who* and *the how*—because as we'll discuss next, sometimes one of these types matters more than another.

The Who

These types of attribution focus more on *who* is behind the activity. Analysts might attribute activity to:

- **A person/persona:** The person behind the keyboard who performed an intrusion or activity developed the malware in question. Analysts may start tracking this via a persona (sometimes based on a handle or account name) and eventually identify the person behind that persona.
- **A team, unit, or organization:** The group of people behind the activity, whether they are a loosely formed hacktivist group, an organized military unit, or a company's red team.
- **A government:** The country behind the activity. (This can get even more complex, because "state-sponsored" isn't straightforward, as Jason Healey discusses in this paper.)

The How

Analysts can also perform attribution based on *how* activity happened, which may completely ignore *the who* behind the keyboard. When attributing based on *how,* analysts often look for some unique attributes of the activity, such as a unique domain, execution sequence, command-line options, code snippet, or some combination of the above.

Analysts might attribute activity based on:

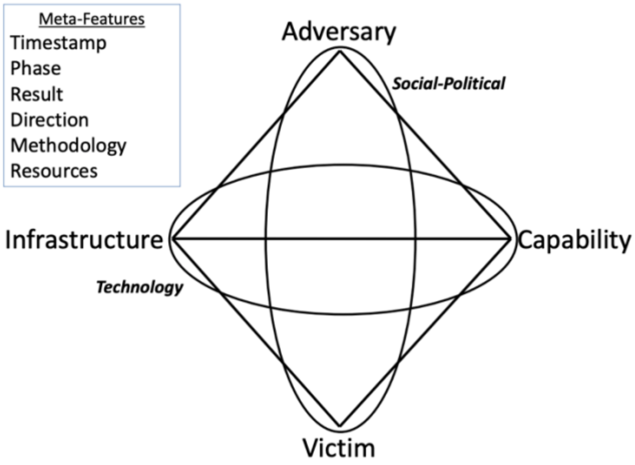
- **Tools/malware:** Adversaries use various tools and malware, both open and closed source, throughout their intrusions. Sometimes these are custom and unique to adversaries, but oftentimes different adversaries use the same tools.
- **Other code**: Adversaries use other code and scriptlets, such as PowerShell, throughout their intrusions.

- **Tactics, techniques, and procedures (TTP):** More broadly, adversaries use TTPs to achieve their goals. MITRE ATT&CK provides a common framework of TTPs that analysts can use to track adversary behaviors.
- **Infrastructure:** Adversaries register and maintain domains, Internet protocol (IP) addresses, and other infrastructure, which can provide unique pivot points for analysts.

Why Not Both?

Of course, analysts can also combine *the who* with *the how* and make attribution assessments based on a mix of the two.

Separating *the who* from *the how* is inspired by (and can be nicely summarized in) the Diamond Model. It divides *the who* into the Social-Political Axis, which also includes the victim in addition to the adversary, and *the how* into the Technology Axis, consisting of capability and infrastructure. As the paper describes, when using the Diamond Model to create activity groups, analysts can choose from the four features, allowing them to focus on *the who, the how*, or both.



To DIY or Not?

To make attribution even more complicated, we have another choice as we do it: we can either create our own clusters to attribute to, or we can attribute to clusters that other teams have created.

Analysts can attribute to:

- **A cluster of activity they observe:** Analysts might also take a look at activity and intrusions they have visibility on and decide to cluster them based on a methodology they choose. There are many different ways to cluster activity—including campaigns, intrusion sets, activity groups, and threat groups—and each team chooses what works for them. Sometimes these clusters are associated with just *the who,* just *the how,* or both *the who and the how.* One method of clustering that allows analysts to choose whether they cluster based on *the who* or *the how* is by creating activity groups based on the Diamond Model. Activity groups may ignore the Adversary feature altogether and focus on clustering based on features like Capability (e.g., malware or techniques) or Infrastructure (e.g., command and control domains or IPs).

- **A cluster of activity someone else has named:** When analysts perform attribution, they might associate what they're seeing with a name that another team has created. For example, FireEye uses the UNC, FIN, and APT designations, and a team might note that activity they're observing overlaps with activity from a group like FIN7.

When Does Attribution Matter?

That brings us to the crux of this debate: does attribution really matter? Well, it depends on both *how* and *why* you're doing it. As we've discussed, there are many types of attribution, and not all of them are suitable for every team's needs (i.e., requirements, but sometimes people are afraid of that word).

Sometimes, *the who* of attribution matters a lot. For a government seeking to use instruments of power (diplomatic, informational, military, economic), *the who* behind the keyboard is important. For example, the U.S. government frequently issues indictments against cyber adversaries (something I've taken an interest in) as well as levies economic sanctions against them. In those cases, attributing *the who* certainly matters.

Other times, *the who* of attribution doesn't matter as much, and focusing on *the how* is sufficient. This isn't always easy to discern, especially when geopolitical tensions are on the rise and we have fear, uncertainty, and doubt about who might target us. Situations like this provide us a good opportunity to reassess which threats we care about, make sure we've accounted for the corresponding TTPs, and reflect upon whether *the who* matters. If adversaries are on your network, does it really matter who is behind the keyboard if your main goal is just to get them out?

For example, as a company focused on defense and detection, we at Red Canary care much more about *the how* of activity so we can track adversary TTPs and better protect our customers. Of course, there are circumstances when *the who* matters to defenders, too… take red teams as an example. If I'm a defender, do I want to be spending my time responding to a red team if there are real adversaries on my network? No way! So, for many defenders, it may be important to track *the who* when it comes to red teams.

Each team is different in what it needs, and, as a result, everyone's needs for attribution differ too. I encourage analysts to carefully consider their own team's needs and then consider the different ways to do attribution to help them decide what makes sense.

Key Discussion Takeaways

Participants in the cooperative learning session dove in with a series of thoughtful discussions and read-outs to the broader group. Key points made by groups included:

- There are many ways to do attribution. Some groups discussed those methods, including looking at timing – whether it's timestamps of operational activity or compile times of malware. While timing isn't always perfectly indicative of where the operators are located, participants noted some cases where they've found the hours some activity has occurred has aligned with working hours in the suspected region where the adversaries were located.
- Some groups care more about the "who," and some care about the "how." Several participants shared the idea that many executives and leaders care about the "who," and it may be on analysts to try to educate them on whether that matters for them or not. Many participants noted that for

their defenders, the “how” is sufficient to help inform them about how to protect against malicious activity.

- Doing attribution can be very complex. Participants discussed complicating factors like the fact that some adversaries have “side gigs,” meaning activity may look similar when it’s two different groups of humans behind the keyboard.
- Many people just think of the “who” when discussing attribution. Several participants noted that their default definition of attribution was just the human side (the “who”), and they hadn’t considered that they could just attribute based on the “how.” Many participants thought that clustering based on tactics, techniques, and procedures (TTPs) was an effective way to go about doing attribution, while ignoring the “who.”
- Multiple groups noted that visibility is key when doing attribution. If teams don’t have the right data or information, it can be difficult to do attribution, especially to humans. Getting visibility on TTPs depends on close partnerships with teams like Security Operations Centers (SOCs).

Keep the Discussion Going

With so many different approaches and needs for it, attribution is complex, and we can best tackle it by sharing our thoughts. I encourage you to keep thinking about attribution in your own teams and consider how it helps your organization. If you’d like to reach out, please feel free to connect with me on LinkedIn or Twitter (@likethecoins).