How to Fight Threats in the Modern Age

CounterCraft

Most security professionals will tell you how dynamic today's threat landscape is, and that it is constantly evolving. Everyday, new information circulates. Some of it is highly accurate, and of course some is more speculative. In many cases, cyber attacks are attributed to one criminal group based on some indicators of compromise (IOCs), the type of tools used by the attackers, or their modus operandi (referred to herein as MO). However, the truth is that attribution is often difficult to determine.

We're living in a world that is always on. Nothing sleeps - there's always more to do, and we need to operate efficiently and effectively to stay on top of today's demands. For this reason, **automation is something we have learned to favour. But, some tasks still require the type of attention to detail that you can only do manually. Automating these types of tasks is anything but simple.**

So, even though each attacker is in fact unique, and each attack that takes place can also be unique, we naturally move towards genericizing the evidence. There are, of course, some fundamentals that can be applied in order to help us study our adversaries. In this article I am going to share my thoughts about the 'basics' that play a crucial role in threat fighting.

Indicators of Compromise

Let's begin with the simplest part of threat research (assuming we have some to work with); IOCs. These will fall into three main categories:

- **Infrastructure (network IOCs)**
- **Tools (hashes, mutexes, yara rules, etc.)**
- **Human (specific use of tools, commands, etc.)**

My personal favourites are tools and human based IOCs. It's usually fairly inexpensive to burn an infrastructure and switch to a new one after being discovered, but it's much more labor-intensive to create a new toolset. This is where it gets interesting. It's these tools that can display more unique qualities, and provide details that could even identify an actor. In addition, we all have our own way of doings things, habits and patterns, and enable us to remember information. This subconscious human behaviour is difficult for an attacker to masquerade.

Who can we Trust?

Before we assume these IOCs are genuine, we must remember who we're dealing with. It's common amongst security professionals to blindly trust the information shared by the threat fighting community and threat intelligence vendors without verifying the IOCs are real. Double checking involves testing samples to affirm whether they're part of the malware or tool families that they're believed to be, checking that the domains were active during the corresponding time period, checking that the metadata gathered from the IOCs matches, or checking whether the tool IOC corresponds with the tool's behaviour in the scenario being investigated.

It doesn't sound easy, does it? That's because this level of IOC verification isn't, and in some cases, it's not even possible to double check all the information. We're fortunate that the threat fighting community does a fantastic job.

False Flags

We've acknowledged that not all IOCs should be believed, so perhaps you won't be surprised to hear about false flags. The bad guys know the implications of being exposed, so they won't be quick to risk their identities being revealed easily. Criminals will often use known information in attempts to confuse researchers and link their activity to other actors, for example, to protect themselves.

So if IOCs can be burned easily, and if some are false flags, are all IOCs useless? Not at all. Here, the same problem solving logic we've been using for years can be applied. Attackers are often rushing to get access to meet deadlines, and just like the rest of us, they make mistakes. They might not have enough resources to burn their entire infrastructure or to build a new toolset. Equally, they simply might not care. We've seen advanced actors use the same tools for years, so the obvious course of action should be that we use them too. **Why wouldn't we use something that's straightforward to verify and provides a clear indication that an attack is taking place?**

Threat Modeling

Let's consider threat modeling. This consists of creating an abstraction of the attack, dividing the attack up into logical steps, and analysing the activities carried out by the attacker into high level tactics, techniques and procedures (TTPs) in a bid to define their Modus Operandi.

This process gives us a high-level view of the attack, and often provides a different perspective of the attack. From here, we work to determine how the attackers behave. Admittedly, certain details may be lost, so **threat modeling shouldn't be considered a replacement for IOCs, but instead insights that complement and enhance them.**

MITRE and Threat Mapping

A great deal of valuable research has been done in this field. Personally, I think the MITRE (PRE)ATT&CK knowledge base deserves recognition. This knowledge base enables you to fit low level techniques into more high level TTPs; a specific type of mapping that's particularly hard, because some techniques can fit into more than one step, and equally some can be difficult to fit into any.

This mapping can help to identify an actor's typical behaviour, and get a look at an attacker's activity while they're compromising your network or devices. As a result, we're able to infer whether the attack is still in its early stages, and possibly what the attacker wants to achieve.

Mapping threat models is tricky. Attacker threat models can be quite generic, which can be a good thing, but can also throw out plenty of false positives. However, if the threat model is complex and complete and includes information from multiple attacks, a new attack won't probably expose all the techniques included on it. In most cases it's unlikely you'd be able to identify an actor in the early stages of an attack, but these insights can indicate an attacker's next steps or help determine what type of actor you're facing.

Gathering Information

To close, let's focus on how we gather this information. I'm not talking about sharing information within the threat fighting community, but more specifically about how we obtain this information in the first place.

How do you extract IOCs? Do you have enough visibility of the actor to claim that you uncovered their MO? Or is the MO the one used in the attack you analyzed?

This is the really tricky part. **Incident analysis plays a key role in providing information about the attacker's MO, their tooling, etc.** One option is to attempt to monitor criminals, which comes with its own challenges and is sometimes limited by the researcher's ethics and/or whether you're able to detect any malicious servers and politely ask for their content.

Once you have some evidence to work with, the big, complex, obscure layer between you and the attackers - also known as the internet - makes it difficult to track the bad guys' activity. Privacy is another limitation. If you could simply check people's social media activity and search engine queries, you'd have a really powerful source of information. But no one can do that right?!

Ready for Compromise

The second option is to prepare an entire system ready for compromise. This is something we do using the CounterCraft Cyber Deception Platform. **We develop a playground with realistic security weaknesses to lure attackers and deceive them into thinking they've encountered a network interesting enough to break into.** You control the environment; you monitor it, and you can expand it on the fly if you want to. The CounterCraft Cyber Deception Platform also gives you the option to focus on specific actors, take advantage of their distribution methodology and execute one real document or malware which is part of an ongoing campaign within your system to speed things up.

But it's not just about launching a single vulnerable machine and waiting for something to happen. **It's about having an entire, realistic system enabled that attracts an attacker so that you can gather intelligence while it's being compromised.**

It would take much longer than we have today to explore the entire spectrum of threat fighting, and by tomorrow, it would need to be updated in the context of the continuously evolving threat landscape. One thing we can be sure of is that there is no single solution to win this war. There is no one perfect technology or detection platform to address the multitude of challenges that cyber threats present. The tools and knowledge we have is, however, mature enough to enable us to identify unique data sets and suspicious patterns that successfully strengthen our defenses and protect our systems.

No one said it would be easy, it's not! But it's a Threat Analyst's favorite kind of challenge, and it's actually a lot of fun!