WEBINAR SUMMARY

February 25, 2021

Threat Hunting: IOCs or Anomalies?

Jake Williams, Co-Founder, Rendition Infosec
Josh Pyorre, Senior Security Research Analyst, Cisco Umbrella

KEY TAKEAWAYS

- Threat hunting operates on the assumption that a breach has already occurred.
- Adversary counterintelligence negatively impacts IOC programs.
- Anomaly-based hunting is difficult and requires a normal system baseline.
- IOCs have limits that successful threat hunting moves beyond.

in partnership with

OVERVIEW

Many organizations today hunt for threats using indicators of compromise (IOCs), rather than anomalies. IOCs are easier to search for, and threat hunting for indicators can be outsourced; it can be given to less experienced analysts on the team and even automated.

Anomalies are more challenging to set up, requiring a baseline of the network environment. The same deep network knowledge necessary for anomaly-based threat hunters to succeed in an environment also makes it more difficult for attackers to evade detection with this model.

Both IOC-based and anomaly-based threat hunting can benefit the business, and tools like Cisco Umbrella can help organizations do both well.

CONTEXT

Jake Williams discussed the benefits and challenges of IOC-based and anomaly-based threat hunting. Josh Pyorre shared his own experiences with anomaly-based threat hunting.

KEY TAKEAWAYS

Threat hunting operates on the assumption that a breach has already occurred.

Threat hunting teams begin with the assumption that the organization's traditional cybersecurity defenses have failed and that a breach has already occurred. The instrumentation tools, logging, and live-system data directly impact the hunting strategies used to search for the threat, whether the strategy is IOC based or anomaly based.

Many threat hunting programs focus almost exclusively on searching for indicators because pattern matching IOCs is relatively easy. Anomaly-based hunting is more difficult, but the focus on behaviors, rather than indicators, can provide improved identification of attacks.

Benefits of indicator-based and anomaly-based threat hunting

Indicator-based threat hunting	Anomaly-based threat hunting
– No need to know anything about the environment; an indicator match is a match. – Easier to search for evidence of a specific artifact than examine artifacts and determine if they look normal (anomaly-based hunting). – Trivial to obtain indicators for hunting. – Analysts require less experience to be successful than with anomaly-based hunting. – Much easier to outsource hunting successfully. – Can be fully automated with the right technology stack, including remediation activity.	– While IOCs are fragile and have a finite lifetime, anomalies are less likely to change once a normal baseline is established. – Anomalies are more difficult for an attacker to mitigate than IOCs as they engage in a new environment. – Even when the attacker knows they are targeting an organization with an anomaly-based detection program, the cost to evade detections is much higher than with IOCs. – Anomaly-based programs are substantially more resistant to counterintelligence than IOC-based programs. – Although more upfront cost is required, the returns are usually higher than with IOC-based programs.

> We should be relying on both indicators and anomalies, not just one or the other.
>
> *Jake Williams*

Adversary counterintelligence negatively impacts IOC programs.

Counterintelligence conducted by attackers negatively impacts all threat hunting programs, but it hurts IOC-based threat hunting programs more than anomaly-based programs.

Not all attackers have counterintelligence, but well-funded predators, and especially those funded by nation states, will have these defensive programs. These attackers gather their own intelligence on what type of information and indicators their target is learning about them and then use that information to adjust their attack.

Counterintelligence is harder to conduct on anomaly-based programs:

- **There is no "threat feed" of hunting techniques** as there is with IOC-based programs. This makes collecting counterintelligence on anomaly-based programs harder.
- **IOC offers a higher ROI for adversaries.** Conducting counterintelligence on anomaly-based programs is more costly; attackers need to focus their limited resources on the areas of highest return.
- **Understanding the baseline of normal activities on the target network** requires a lot of extra work for the adversary.

Anomaly-based hunting is difficult and requires a normal system baseline.

The biggest downside to anomaly-based hunting, and the reason many organizations are not using it, is because it is difficult to set up and run.

Key tasks when building a baseline for a new anomaly threat hunting program

- **Enable NetFlow,** at least at the egress point. This monitors the internet protocol (IP) traffic that passes into and out of the router.
- **Understand the organization's event logging posture.** Talk to the system administrators and make sure they are using the right logging that allows for good incident investigations.
- **Get involved with IT and help baseline every new golden image.** This allows the threat hunting team—and the baseline itself—to remain up to date with network changes that, if not identified up front, can lead to false positives and negatives.

A strong knowledge of the environment is necessary to eliminate false positives. This makes outsourcing anomaly-based threat hunting difficult. Additionally, new staff will experience challenges, regardless of threat hunting experience, as they learn about the environment.

Another challenge in baseline for anomaly-based hunting is justifying the cost, especially since threat hunting may not show an immediate ROI. Security and IT teams can work together to justify the cost by showing the organization how the baseline can help other areas of the business, including Security and Operations Center (SOC) monitoring, zero-trust networking preparations, incident response planning, system inventory, audit preparation, and network reliability troubleshooting.

Anomaly-based threat hunting identifies LOLBins, LOBAS, and PUA attacks

Attackers are increasingly using Living off the Land Binaries and Scripts (LOLBins/LOLBAS) and potentially unwanted applications (PUAs) to evade endpoint protection platforms (EPP). This shift is forcing EPPs to move beyond just identifying whether something on the network is bad, to identifying whether *the way it is being used* is bad, with each false positive creating a network outage/denial of service (DoS)

By looking at baseline and behaviors, anomaly-based threat hunting helps properly identify problematic LOLBins, LOLBAS, and PUAs within the environment, where the traditional EEP and IOC-based threat hunting cannot.

IOCs have limits that successful threat hunting moves beyond.

IOC-based threat hunting is a useful technique that has limitations. Solutions like Cisco Umbrella help organizations move beyond indicators and into anomaly-based threat hunting.

> IOCs have limits. You are also going to miss some things because you only know what you know about.
>
> *Josh Pyorre*

For example, Josh Pyorre discussed Emotet, which was originally designed as banking malware to steal sensitive and private information. Mr. Pyorre used Python scripts to pull suspect domains from malware traffic analysis packet captures (PCAPs). He looked more closely at the attributes of these domains with Cisco Umbrella, where he was able to not only see which were associated with known Emotet attacks, but identify first seen and first queried dates, and activity associated with the domains.

While activity for one suspect domain (Figure 1) looked normal under analysis, activity for another (Figure 2) was clearly an anomaly, with one spike on the day it was first registered. This helped identify a false, malware-infested site.

Figure 1: Domain name system (DNS) queries look normal for one site infected by Emotet

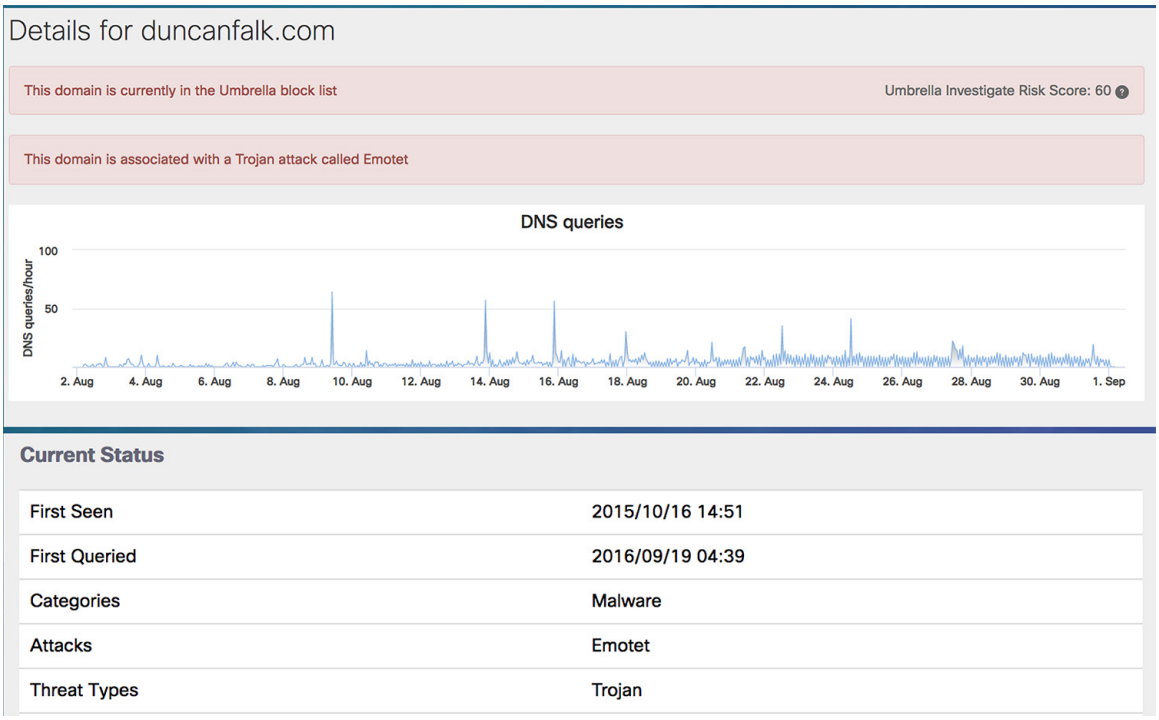
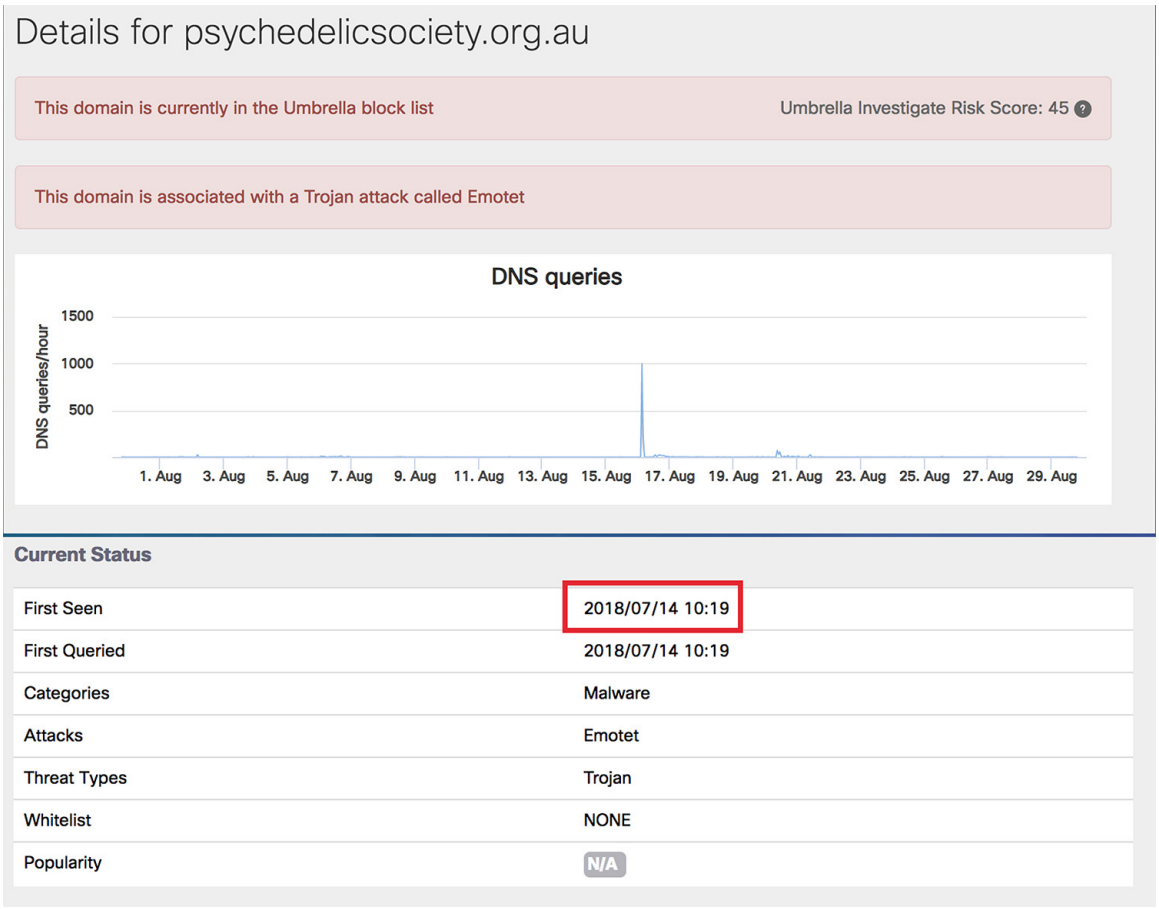


Figure 2: Cisco Umbrella shows an abnormal spike for another Emotet-infected site, on its first seen date



ADDITIONAL INFORMATION

To sign up for a live demo of Cisco Umbrella, visit:
https://umbrella.cisco.com/info/cisco-umbrella-live-demo-webinar

BIOGRAPHIES

Jake Williams

Co-Founder, Rendition Infosec

Jake Williams is the co-founder of Rendition Infosec and a principal consultant performing incident response, computer forensics, penetration testing, malware reverse engineering, and exploit development. Jake is a certified SANS Instructor and course author and trains thousands annually in information security topics.

Prior to founding Rendition Infosec, Jake worked in various roles with the US DoD performing offensive and defensive cyber operations in classified environments. Jake regularly briefs Fortune 500 executives on information security topics and has a knack for translating complex technical topics into verbiage that anyone can understand.

Josh Pyorre

Senior Security Research Analyst, Cisco Umbrella

Josh Pyorre is a senior security research analyst with Cisco Umbrella. Previously, he was a threat analyst at NASA, working as part of the team that built and operated the NASA Security Operations Center at Ames Research Center. He has also worked at Mandiant, helping to build their SOC while conducting incident response for multiple clients. Before working in security, Josh was the technical director for a non-profit providing assistance to the houseless in San Francisco.

His professional interests involve network, computer, and data security with a goal of maintaining and improving the security of as many systems and networks as possible.

Josh has presented at conferences and locations around the world, including DEF CON, B Sides, Source, Derbycon, InfoSecurity World, DeepSec, Qubit, NASA, and various companies and government entities. He was also the host of season one of the security podcast, "Root Access."