Hunting Methods on Networks

Table of Contents

Hunting Methods on Networks ........................................................................................................ 2
2014 Survey & Interviews of Methods .......................................................................................... 3
Interviews with Participants Revealed ......................................................................................... 4
Common Observations ................................................................................................................... 5
Study Recommendations ............................................................................................................... 7
Notices .......................................................................................................................................... 10
**039 The SEI has performed a study specifically on hunting methods on networks, and this module is going to cover a little bit about what that study found and some of the conclusions.**
2014 Survey & Interviews of Methods

In 2014, the SEI performed a survey and assessment of non-signature-based approaches, tools, and techniques:

**040 So in 2014, the SEI performed a survey and an assessment of what we call non-signature-based approaches, tools and techniques used by teams in the field that we work with. The goals of the study were to really collect a list of these techniques and approaches, try to observe the adoption or the maturity of the methods that were being used, look for and identify what some of the emerging techniques were in the teams that they were working with, but the real focus was on network-based detection of malicious activity. So the focus is on the network, in this case, not on other parts of the IT environment.
Interviews with Participants Revealed

Hunting Process
1. Mine data.
2. Identify suspicious activity.
3. Investigate.
4. Codify a repeatable analytic.

Analysts perform heuristic queries informed by expert knowledge of the allowed and expected behavior, the controls implemented, and other situational knowledge.

**041 So what they found through the interviews with participants was this sort of general process that the hunters were using. So in this case, they would go out and look for some data that they could mine on the network. So this might have been collected by a network tool or something like network flow data, but there’s other types as well. So after they mine that data, they would identify suspicious activity. So they were trying to identify the difference between regular activity and suspicious activity. If they were able to find it, they would investigate it, and then they would sort of do this initially and then figure out a way to turn it into something that could be repeatable.
So initially the analysts were really performing kind of a heuristic query, which was informed by their knowledge. So they were knowledgeable about the environment, knowledgeable about the typical activity that was happening, and they were sort of applying some rules that were in their head for what they thought might not be that regular activity. And if it worked out, they would then turn that into something that could be automated.

Common Observations

**Common Observations**

Analysts often focus on a few common protocols and apply their understanding of related business processes and their expected behaviors.

Excluding the rest of the data highlights the interesting things that require additional examination.

Process often results in the creation of a repeatable process that looks for suspicious IP addresses, domain names, certificates, and other artifacts.

Automating the repeatable process often results in new signatures that can be deployed to existing infrastructure, which minimizes analysts’ workloads.

**042 Here are some of the common observations from the study and from the methods observed. The analysts**
were really kind of focusing on a few common protocols and applying their understanding of their related business process and the expected behaviors to those protocols. So there was a real focus, starting with the things that they were most familiar with.

Other techniques that they would do which were quite interesting were to do things like excluding a lot of data. Right? So in some cases, we’ve seen teams that might throw out a lot of the common English words, and the things that remain are potentially interesting and that might require additional examination, and there are lists available of the most common English words. It depends on what language and what source you’re talking about. You can even get these words from things like just the most common words from publications or magazines, just the most common English words from books. There’s all kinds of sources available to do that.

Additionally, the process would often result in the creation of a repeatable process. So if they were able to find some suspicious activity, then they could create a repeatable process to look for additional suspicious activity elsewhere. Specifically usually this was for something like an IP address or a domain name or certificate, or just really any other artifact that you could find on a network. If they could find suspicious activity, they would look for signs of that suspicious activity somewhere else.
And then automating that repeatable process would often result in a new signature. Right? So these are sort of non-signature-based approaches, but by using this approach you could result in something that eventually becomes a signature and thus sort of can fit into the existing infrastructure, and then that would sort of minimize the analysts’ workload. So if they could turn something into a signature, then they wouldn’t have to do it anymore and they could go and look at a new or different type of approach.

**Study Recommendations**

**Study Recommendations**

Promote adoption of hunting operations, sandboxing, DNS analytics, and network profiling with both policy and funding, including R&D.

Develop an HR and staffing strategy to support hunting.

Integrate research roles into operational environments for joint learning.

Augment DNS designs to improve DNS analytics and the collection of passive DNS.

Clarify policies regarding deception.

Determine policies to address security and privacy concerns related to large collection and storage.

**043 Some of the recommendations from the study were to-- other teams-- to**
promote the adoption of hunting operations, specifically things like sandboxing, DNS analytics and network profiling, with both policy and with funding, including sort of activities related to research and development. So it was an encouragement to other organizations that these were worthwhile efforts and that they should invest in them. They were also recommending that if you want to do this kind of thing, you're going to need to have the help of HR and a staffing strategy to support hunting. They'll also need to integrate research roles into the operational environment. Sometimes the operators were too focused on closing the work that was on their plate and they really didn't have time to sort of take a breath, look around, figure out ways to automate things so that they didn't have as much time spent per particular report or task, and that that typically would require some amount of sort of research and analysis for some kind of joint team.

Specific to DNS, they were really saying kind of augment your existing DNS to improve your ability to analyze it, including, most specifically, the collection of passive DNS. They found that having some ability to collect passive DNS was quite helpful to the teams that were trying to do non-signature-based analysis of networks. DNS is a really critical part of that, and so passive DNS will give you a record of a lot of the DNS activity that was happening over time on the network without kind of losing that history.
Clarify policies regarding deception. So in this case, what they're talking about is this sort of deception by the hunting team. Some organizations may have not considered that the hunting team would need to deploy deception on the network, and so they may have not even considered sort of what their policies were regarding placing sort of deceptive materials on their network. Examples of deception might be things like fake certificates or honey hashes, where you are actually placing fake credentials on the network and seeing if an attacker tries to use them.

Lastly, they also recommended that you should determine policies to address security and privacy concerns related to the large collection and storage of network data. So sometimes the network data may have other information in it that the employees or other people in the organization would have some privacy concerns with, and so really there would need to be a detailed examination and a risk discussion before the hunting team could really do that in an effective way.