Examples and Goals of Threat Hunting

Table of Contents

Example of Hunting for Cyber Threats

This hunting example comes from the Mandiant M-Trends Report 2015 (https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf).

Compromised Virtual Private Network (VPN) connections give attackers two huge advantages

1. They can persist in an environment without having to deploy backdoors
2. They can blend in by imitating authorized users

Most commonly observed VPN compromise methods across all Mandiant engagements in 2015:

- Single factor – re-used credentials stolen from compromised end-user systems or the Active Directory domain
- Certificate-based multi factor – used available tools (such as Mimikatz) to extract certificates from compromised end-user systems or found certificates that had been distributed in an insecure manner
- Via direct compromise – such as Heartbleed (less common than the others!)

**007 So here's some sort of a concrete example of what we mean when we're talking about hunting for cyber threats. This particular example comes from a Mandiant report from 2015. So in that report, Mandiant has identified throughout all of the different incidents that they've responded to that there are some trends in the patterns of attackers. And in the methods of compromise that they were able to successfully perpetrate on the victims. And so one of the things that they said in the report is that compromise virtual private network connections give the attackers two huge advantages.

The first advantage is that it allows the attacker to persist in the environment without having to deploy additional backdoors. They can just connect directly through the VPN, they have an encrypted channel. They do not have to have another backdoor. They already have a connection. So there's nothing to look for as an administrator outside of the VPN traffic, which can be difficult to differentiate between attacker, non-attacker. Which sort of brings you to the next point. That allows them to blend in if they are able to imitate an authorized user. So those two points are very powerful sort of in the attacker's favor for the use of a virtual private network connection as the avenue of the attack.

So the most commonly observed VPN compromise methods across all of the engagements that Mandiant had in 2015 were the following three problems. Number one, the single factor, if you had a VPN connection which allowed single-factor authentication, then you, an attacker, could reuse credentials that they stole from a compromised end-user system or that they took from something like an Active Directory domain or other directory service.

Number two, if you happen to have a certificate-based multifactor VPN authentication, typically considered a little bit stronger than a single factor, then the attackers would use some other available tools to extract the certificates for that multi-factor from

a compromised end-user system or they would find the certificates within the environment that had been distributed in an insecure manner. So just because you're using multi-factor, it doesn't necessarily mean that you're keeping all of the attackers out. They were able, in this case, to find certificates that had been distributed in an insecure manner. And reuse them.

And finally, there are some of the engagements that Mandiant encountered were via direct compromise. So there was a vulnerability in the actual VPN protocol or in this case they were talking about sort of the Heartbleed bug or other bugs that were similar that allowed you to manipulate the session directly by sending commands directly to the VPN server and receiving a response that would disclose information about how to connect. This was somewhat less common than the other two.

Example Hunting Goal #1

Goal: Prevent VPN compromises by looking for insecure certificates and insecure distribution of certificates.

Methods: Look for

- attached emails in unencrypted form
- available on open network file-shares
- posted in SharePoint systems

Recommended hunting team skills include

- network & infrastructure: Where are all the places we should be hunting?
- security SMEs: What are tell-tale signs of insecure certificates?
- programming: How can we automate the hunt?
- data science: How prevalent is this problem for us?
- visualization: How do we explain the problem and report the results?
- IT/process: What are all the ways you distribute certificates?

**008 Okay. So given all of that information, when we talk about a hunting team, we're talking about how do you use that information and other information like it to come up with strategies for both prevention as well as sort of identification of incidents that you may not already know about but that you highly suspect you might have going on right now.

So from that previous slide and all of the information on it, we've come up with a few example goals and we have a couple, this is the first one, and we'll go through each goal and talk about how we came up with the

goal, what it means, and a few of the things that you might need in order to implement this goal.

But so goal number one in this case was, okay. From what I just read and what I understand about a common method that attackers are using, I'm getting concerned about my own VPN environment. And what I would like to do is prevent VPN compromises by looking for insecure certificates and insecure distribution of certificates. Now, I've already made some assumptions about my environment, which is like I'm not using single-factor, I'm actually using multi-factor. And in this case I'm using certificates for multi-factor instead of something like tokens. So you've already seen that these goals are really very specific to the organization that you work for. You need to tailor them, if you're sitting in a hunting team, you need to tailor the advice that Mandiant has given, or sort of some of the observations that they've made, with your own environment and interpret it into something that's actionable for your own space.

So using that goal, you could come up with some methods and each of these methods, again, you have to prioritize which method is going to be most effective or the sort of the best fit for your environment based on what kind of operating systems you run, what kind of business climate you're in, what kind of management acceptance of the activities that you're proposing there

is. But some of the methods that you might come up with to help look for insecure certificates or the insecure distribution of certificates, would be things like looking in attached e-mails for an unencrypted certificate that's been distributed via e-mail. You may also find these certificates available in open network fileshares. Right. Somebody posted their certificate or temporarily put it in a fileshare so that they could pull it over to another device, and then never deleted it.

So these are things that you could search for, right, that would be very valuable to an attacker because they could just copy it and use it as part of their attack without a lot of effort.

Lastly, there's other evidence where a certificate may have been posted in a SharePoint system. And again, if you don't use SharePoint, this probably isn't the right advice for you. But you might be using something else, you might have some kind of wiki. You need to interpret the information in this slide and apply it to your own environment.

So some of the sort of recommended skills for somebody on a hunting team to be able to sort of digest the information that we were talking about and sort of come up with methods and then implement a sort of either code or a process to actually accomplish the method, we would recommend some of the following kinds of skills. You know, somebody

who's familiar with the network and the infrastructure, you know, to answer the question, "Where are all of the places that we should be hunting for something like an insecure certificate or for an insecure distribution?" So somebody who's familiar with all of the different distribution methods that IT or a help desk might commonly deploy. They might be using software or systems to do that, and somebody should be familiar with that infrastructure or the administration of those systems.

This person doesn't necessarily have to be dedicated to the hunting team, but the hunting team should be able to interface with that group and find out the answers to a question like that. Typically you're also going to be looking for somebody who's sort of a security subject matter expert, and they need to answer questions like, "What are some of the telltale signs of an insecure certificate?" So they should be familiar with what a certificate is, the different fields that it has and the values that those fields actually have and figuring out, like, for what kind of certificates are we using? You know, are there methods that are making these more or less secure? Another person, a sort of a programmer or someone who can automate parts of that hunt. So you don't really want to necessarily have people manually digging through e-mails looking for these things. That's going to take a lot of time. If you can have someone who can help you write a script or automate some of that process with code, you can really

look through many, many, many more e-mails and sort of in a much shorter amount of time and without actually having a human devoting time to that type of effort.

We also recommend sort of a data science angle. So, you know, the question of once we've gathered all of this information, like, how do we figure out how much of a problem this is for us? You know, a data scientist can help sort of digest the numbers and figure out the right method for counting the problems and then finally sort of visualizing all of those results. How do you explain that this is the problem? How do you explain the size of it and the magnitude? How do you report those results to somebody who's not familiar with certificates or not familiar with the distribution mechanism, who doesn't understand all of the things that all of these experts understand? How do you communicate the results of them and answer questions that they might have about it? And then lastly, sort of, you know, again, the IT in process, you know, what are all of the ways that you distribute certificates? Not just necessarily the official way, right? So this sort of goes back to the first part. You may have somebody who's knowledgeable about the environment but now you need somebody who's knowledgeable about the practical process as well.

Example Hunting Goal #2

Goal: Find attacks on our network using stolen certificates or attempting to steal certificates.

Methods

- Collect source IPs and geolocation for connections. Alert on large location changes (country/state) which is similar to methods used by enterprise cloud apps.
- Work with departments to reduce false positives for certain staff members
- Alert on presence of tools like Mimikatz (and others) in traffic and on hosts such as via Yara Rules
- Create fake certificates and watch them (aka “Honey Hashes”)
  - consider staging them in risky machines/areas, in DMZ, and/or randomly.
  - set up alerts for attempted use of the fake accounts.
  - Other design considerations: name schema for usernames, high privileges on your domain, proper metadata (last login, etc.)

**009 So we'll move to goal number two. Goal number one, right, was one option. Goal number two is a different option. So using the same information from the report, think about how would we potentially find attacks on our network right now that are using stolen certificates, or consequently, how do we set up our network so that we would be able to determine if in the future somebody is attempting to steal or copy certificates that already are there?

So again, this is a different goal, although very squarely in the threat hunting mindset, right? How do I find out if somebody's actually

already using these things or is going to try to use them in the future? And so we've come up with another list of methods here just to show you a different perspective. So you could take, in this case, you could collect the source IPs and the geolocation for all of the VPN connections that you have and potentially alert on something like a large location change. So if a user one day is logging in from one place and then the next day a different place and then the next day, you know, back to the same place again and then the next day back to the different place again, that could be indicative that there's actually two different people logging in from the same account.

However, if you have somebody like a sales team, right, then you may end up with like a lot of false positives if you have that kind of alert. So you got to work with the departments based on the numbers that you're seeing to reduce those false positives.

Another option here in the methods would be to alert on the presence of tools, such as Mimikatz, and some others that the report mentions or that you can find online, that would help an attacker extract the certificates and copy them from the various hosts, right? There are other rules that you could use, such as Yara, which sort of is a malware signature detection tool that helps you write kind of signatures to detect various kinds of malware. You can look for the traces of files. In this

case, there are some available Yara Rules that you can use to look for the traces of files that allow attackers to extract certificates. So you could set up the infrastructure to detect those kinds of tools and as well as when they're sort of being uploaded or downloaded onto a host.

So another possibility that you could do would be to create some fake certificates. And then watch them, right? So this would be a situation where I know that these certificates are fake. I'm deliberately putting them into places on my environment. And this is sort of similar to a honeypot. There's a term that we found in some of the literature called a Honey Hash. In this case we're sort of using the same idea and saying, "Okay. Let's create a honey certificate," right? So consider where you would put, if you were to do this, where would you put these honey certificates? Where would it make sense to put them? So some of the areas that might make sense would be into the higher risk portions of your network. So for people that might have access to additional information or additional privileges such as administrators, that might be a good idea. But you really sort of need to perform a risk analysis to figure out, "Where's the best place to deploy these honey certificates?" That would just get too complicated to manage, right?

So some of the suggestions here might be put them in high-risk machines. People like the sales team

who have a lot of frequent connections would be a real good target for an attacker, because they could blend in. But if you put some honey certificates on those machines and the attackers try to get them and you get an alert on that, now you have some additional information, right, that helps you to determine that somebody's actually trying to steal a certificate, they're not just traveling place to place.

Another place might be in a DMZ or where you have your internet-facing infrastructure. Some places that are sort of more commonly exposed than others. Or also, I mean, you could really just do it randomly. So you're not distributing everywhere, but you're taking a random sample. There's all kinds of methods, but you need to come up with what makes sense for your own environment. A risk-based approach could be good, combined with a little bit of randomness.

So basically what you do after you've figured out where to put these things is set up some alerts or rules in your environment that show when somebody attempts to use them, right? So if your VPN server gets a connection and somebody's attempting to use a fake certificate to connect to it, you have to decide what to do. Will you allow that connection, but alert on it? Will you disallow it? Obviously still alert on it. But you need to be able to sort of think about, "How much information do I want to give the attacker about

the fact that I'm onto them?" Right? I may want to collect additional information about their activities that I could use either to keep them out more permanently or to use against them in some kind of legal proceeding.

Lastly, you know, a little bit of additional advice. You actually have to design these kinds of things, right? So when you're designing a fake certificate, you need to think about what would be sort of a schema, right, for the username, and does it fit in with my existing schema? So I don't want to give away sort of to the attacker right away that this is obviously a fake. It has to look generally realistic. It might also want to make it sort of attractive to the attacker with things like a high level of privileges on the domain. And be careful because, you know, certificates also have metadata. So you'll need to forge or impart some metadata, things like the last time this certificate was used, and other things like that.

So just a brief, you know, coverage of different kinds of goals that you could do, you know, the reason to show these is these are some of the activities that a hunting team is going to get involved in.

More Advanced Methods

User Behavior Activity Monitoring

- Enterprise tools for comparing user behavior against itself such as
  - Rapid7 InsightUBA (user behavior analytics)
  - Microsoft Advanced Threat Analytics

Resources for Hunting Credential Thefts

- https://dfir-blog.com/2015/11/24/protecting-windows-networks-dealing-with-credential-theft/
- https://isc.sans.edu/forums/diary/Detecting+Mimikatz+Use+On+Your+Network/19311/
- https://adsecurity.org/?tag=yara

**010 So going back to the original example. Here's some more advanced methods, right? So if attackers are blending in with regular users, you could try to do something like user behavior activity monitoring, right? So these enterprise tools for comparing user behavior against itself. Is this normal behavior for this particular users? And we've listed some tools here. We're not endorsing them, but they're available and they are sort of more enterprise level. There's usually more cost associated with these, but you may be able to use this to hunt for users that are not behaving as they normally do. Which may be

indicative that somebody has stolen their VPN credentials.

So there's additional resources here on specifically hunting credential, hunting for credential thefts. There's a few blog posts and other things for detecting tools, as well as the actual link to some of those Yara rules that I mentioned, if you're particularly interested in this particular kind of attack.

About Hunting Goals

About Hunting Goals

Collaboration and consensus

- The decision on a specific hunting goal is often collaborative.
- Usually consensus must be reached between the hunting team and other teams, such as IT, strategy, operations, finance, and others.

Many other goals could be developed from the VPN observation:

- Move from single factor to multi-factor.
- Move from certificate-based multi-factor to token based (or other).
- Make end user machines more resilient to widely available certificate extraction tools, or have hosts to detect their presence/usage.
- Help IT implement a process / tool to ensure that certificates can only be distributed and stored in encrypted form.
- A harder goal is to determine when users on the VPN are acting out of character.

Each option may need to be evaluated and weighed for cost, effectiveness, time to implement, and impact on current operations.

**011 But I think ideally, What we were really trying to show here, and with the examples and with the source material, is that this is about

the goals of hunting teams. So each hunting team has to come up with goals based on different factors. So in this case, right, hunting goals typically need to be collaborative and you're going to want to try to get as much consensus as possible. So usually you need to kind of get to a consensus between the hunting team and then other teams. The hunting team cannot just stand alone and come up with goals on its own and then implement tools and go looking for things. Because in some cases, let's say, they might go looking and putting fake certificates everywhere and somebody in operations goes and finds those certificates and didn't know about that and says, "I have no idea what's going on." And they waste a lot of time and they didn't even know whether to talk to the hunting team about it. And so they didn't even know that that activity was going on.

So that's a fairly common problem, and the hunting team wants to avoid that as much as possible. And so some of the groups that you're typically going to want to interface with would be people like people from IT, people from some kind of strategy group to find out what's going on in the future. People from operations, to make sure that you're not being disruptive to what they have going on. The finance team could be another one. Typically a high-risk area. And many others, right? So the idea here is this is a collaborative process. The goals are something that you're going to want

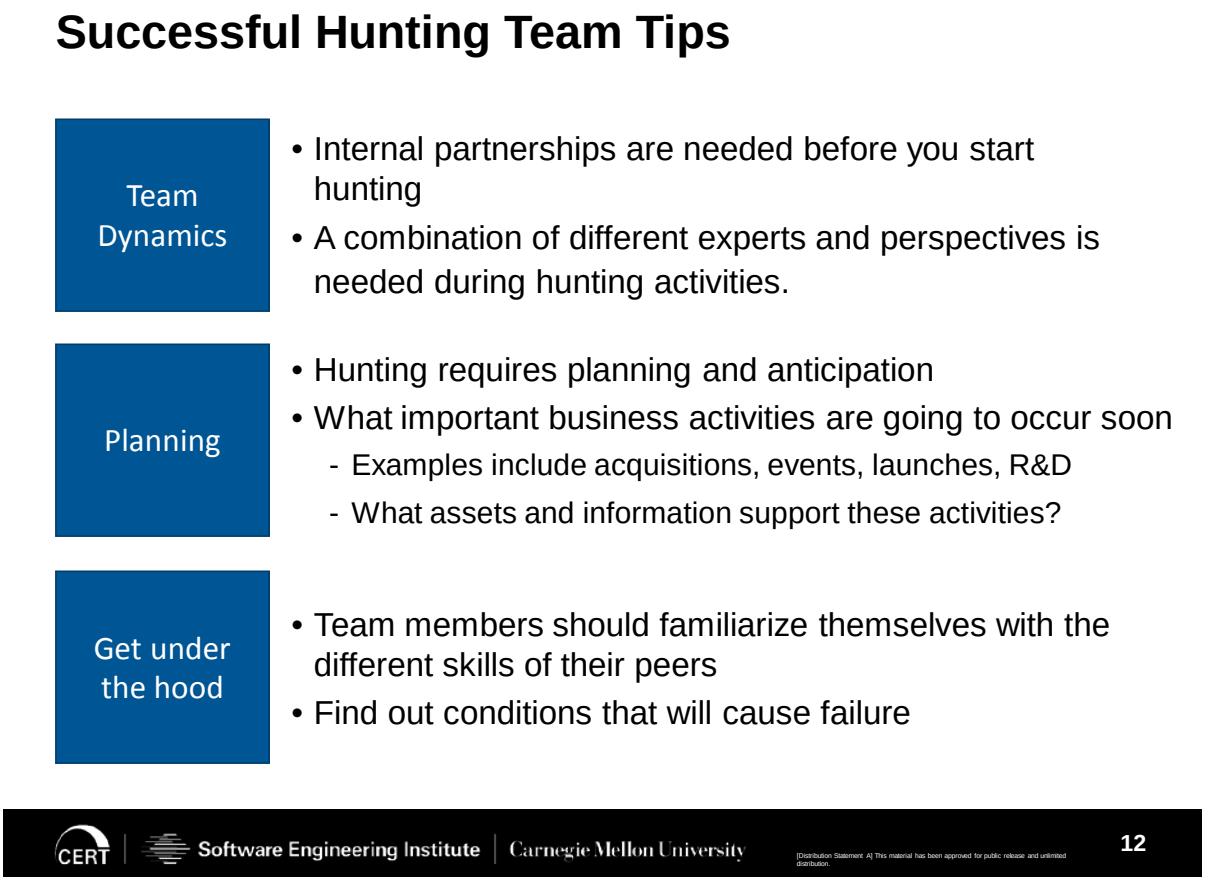
to bring in other groups before you even define, right, to say, "Here's some of the information that we have about--" in this particular example, VPN certificate theft. "Here are some options that we've come up with. Which of these options are palatable? Please talk about the sort of benefits or the risks or issues that you see with each of these options." And then, you know, sort of collectively and through a consensus process, figuring out how to implement those goals.

So there are many, many other goals that could've been developed from that particular observation about VPN credential theft. We put two example goals and then went through the specifics of how to implement that goal and what you would need to implement that goal, but some of the other goals would be, right, if we are on single-factor, we could move to multi-factor. Right? Right away. If we are on something that's certificate-based that's multi-factor, we could move to some other kind of multi-factor solution, such as a token-based, which is much harder to steal. We could try to make our end-user machines more resilient to the widely available certificate extraction tools. We could also help IT implement processes to ensure that certificates can only be distributed or stored through encrypted form. And then it's sort of a harder goal, would be to determine when the users on the VPN are acting out of character, right. And we talked about some tools that might be available, but

they may have a higher cost. So each of these options has a different cost, right. And this is where the consensus process becomes so important, because if you're going to go for a higher-cost option, which might provide a little bit more sort of robustness against an attacker, that's really a decision that's more of a strategy decision for your security environment.

So the hunting team might have originally come up with this goal, but it may turn into something that's bigger and becomes more of an IT strategy, right. To say, "Okay. The hunting team might help us put in a couple of blocks or solutions to search for that hunting," to hunt for that activity, but large, you know, sort of this is now going to become a larger project within IT or within security, to move to something that's, you know, sort of more robust to the current techniques used by attackers today.

So each of the options needs to be evaluated and weighed, right, for things like how effective is this going to be at preventing some of the threat activity that us and other people are seeing? How long is it going to take to implement? What impact is it going to have on our current operations? How much is it going to cost? In fact, how is it even going to be evaluated, right? We've thrown out a few options here for some of the ways you typically evaluate but there's lots of other ways too.



**012 The successful hunting team tips. So team dynamics, right? This is something that's really important. Having an internal partnership set up before you actually start the hunting activity is very important. We talked already in some of the examples about interfacing with teams like IT, having a partnership with IT is going to be very important. We also sort of showed through the example that You really need a combination of different experts and different perspectives that you're going to need during your hunting activity.

On the planning side, and there's quite a lot of planning that goes on,

sort of figuring out what are the important business activities that are going to be occurring. Right. So if we're going to be acquiring a company, okay, then the hunting team has to be ready for when that actual activity starts happening on our network. So what could we do to hunt for infections on that other team's network prior to them joining our network, and then what do we do in terms of sort of what controls or alerts do we want to set up that would show that activity is starting to happen on that network that we are interested in? That's something that the hunting team can start thinking about before that network is even connected, right? So, and finally, always thinking about what sort of assets. And usually we're talking about IT assets or cyber assets and information support the important business activities that are happening. So for things like events or a new site or product launch, what are the cyber assets and the information that's sort of most important that support those activities? What can I do to start hunting before we launch the product, right? So I can start thinking about some of the potential threats to that product once it's more widely available.

And finally, I think we're very much talking about when we say get under the hood, right, we're talking about understanding what other people are doing and figuring out how things work, including when things will fail. So sort of a mindset of getting your

hands dirty, right, and digging in with some of the available commands, or this might be through interviews. But you should really be trying to familiarize your team with the different skills that their peers either in IT or in the business environment have and then figuring out sort of what some of the gaps might be when they develop a product to say, "Oh, well, they may not have been thinking about this." You know, "Their sort of strengths lie over here, so we should, you know, consider some of the other things that maybe they didn't try and maybe we should try those before somebody else does."

Notices

Notices

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0003588