v2

Threat Hunting Professional

Threat Intelligence

Section 01 | Module 03

Table of Contents

3.1

Introduction

3.1 Introduction

In the previous module, Module 2 – Threat Hunting Terminology, we discussed the 2 mindsets of a Threat Hunter:

1. A hunter that relies mostly on threat intelligence
2. A hunter that relies primarily on digital forensics

Now, we'll go deeper into the first type of hunter, the one that relies on threat intelligence.

"Threat Intelligence is data on threats."

3.1 Introduction

As you may recall, for data to become intelligence, it has to be processed, analyzed, and become actionable. The data will be pertinent to your infrastructure and assets. The data will include context, not just indicators.

The intelligence may contain more than IP addresses, file hashes, etc. It may contain TTPs, advice on how to stop their attack, etc. Remember that this type of hunter is relying on the information of **known** threats.

3.1 Introduction

The rest of this module will primarily focus on the manual efforts a threat hunter will take to take to obtain threat data.

Of course, the preferred method would be through automation (*data automatically fed into a security appliance, such as a SIEM, which works harmoniously with a combination of other security appliances to give you intelligence*), but that is beyond the scope of this course.

3.1 Introduction

Although discussed in a later module, a **SIEM** is a Security Information and Event Management solution. It is a centralized collection point where all logs (firewall, network, application, event, etc.) are collected, so that the Security Analyst can analyze them in one place, instead of logging into various consoles to view log data. The logs can also contain external data.

To really benefit from cyber threat intelligence, you should already be gathering internal data using a SIEM before you start looking for threat intel externally.

Threat Intelligence Reports and Research

3.2 Threat Intelligence Reports

Several trusted third-parties collect and gather cyber intel data and release Threat Intelligence reports. These reports typically cover malicious activity that was observed and explain specific threat actors associated with that activity.

As a threat hunter, you should be accustomed to reading these reports when they are released.

3.2 Threat Intelligence Reports

Some of those third-parties include but not limited to:

- FireEye
- Verizon
- TrustWave
- CrowdStrike
- Palo Alto Networks
- Cylance
- F-Secure

Note - we are not promoting one vendor over another or any company's services/equipment.

3.2.1 Threat Intelligence Reports - FireEye

For the sake of completeness, if we take FireEye as an example, they create and publish threat intelligence reports regularly, as well as an annual threat report.

The regular reports are available on their website, under Resources > Threat Intelligence Reports. Those reports focus on threat intelligence regarding threat actors, such as APT28, and threat groups, such as FIN6.

https://www.fireeye.com/current-threats/threat-intelligence-reports.html
https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html
https://www.fireeye.com/solutions/financial-services/rpt-fin6.html

3.2.1 Threat Intelligence Reports - FireEye

The naming convention for Financial Threats is known as **FIN** groups. In the previous slide, FIN6 was listed. According to MITRE, FIN6 is a cybercrime group that steals credit card data and sells it in underground markets. They target PoS (Point of Sale) systems in the retail and hospitality sectors.

As you may recall, each vendor might have a different naming convention for a particular threat group. For example, the FIN6 group is also known as G0037 under MITRE's naming convention.

https://attack.MITRE.org/groups/G0037/

3.2.1 Threat Intelligence Reports - FireEye

The annual threat report from FireEye, called M-Trends, focuses on trends from the year's breaches and cyber-attacks. According to their website, the M-Trends report provides an intelligence-led look at various topics, such as emerging global threats and the latest defensive strategies.

The latest edition of M-Trends is published here. Although we will highlight certain sections of the report, it is highly recommended to read the entire report.

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

3.2.1 Threat Intelligence Reports - FireEye

The Executive Summary of M-Trends 2019 outlines:

On the surface, not much has changed over the past 10 years. 2018 was much like 2017, and 2017 like the preceding years. We continue to see large impactful incidents, though fewer high-profile public disclosures. Extortion cases are on the rise, assisted by cryptocurrency and other forms of non-attributable payment. Cryptocurrencies are also directly targeted via wallets, payment systems and miners.

The significant trends or shifts we saw in 2018 were:

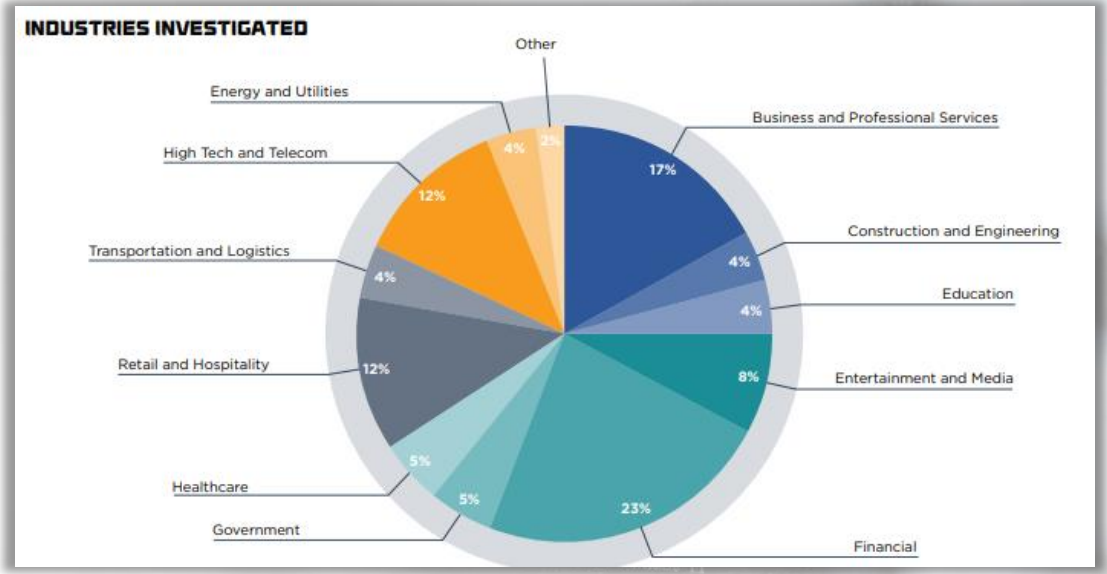
- A significant increase in public attribution performed by governments. Recent years have seen a significant increase in private sector attribution of attack activity, but the past year saw a significant number of attacks publicly attributed by way of indictments from the U.S., U.K., Netherlands and Germany. Some of these were assisted by data from private sector companies such as FireEye. Governments have not changed their operational rules of engagement, but they are combating threats publicly through indictments.
- As more and more customers move to software as a service and cloud, attackers are following the data. Attacks against cloud providers, telecoms, and other organizations with access to large amounts of data have increased.

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

3.2.1 Threat Intelligence Reports - FireEye

In the screenshot here, the image shows us that the two most common industries for the generation of the report are Financial, and Business and Professional Services.

Note that this is based on FireEye's investigations.



https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

3.2.1 Threat Intelligence Reports - FireEye

There is an increase of attacks on organizations that had previously experienced a security incident by the same or similarly motivated attack group.

Retargeted incident response clients, by region.

Region	2017	2018
Americas	44%	63%
EMEA	47%	57%
APAC	91%	78%
Global	56%	64%

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

3.2.1 Threat Intelligence Reports - FireEye

The last thing we'll mention regarding the report is that it will outline some of the TTPs uncovered in various investigations.

Figure 26. Example of recovered BITS persistence mechanism.

```
@echo off

bitsadmin /rawreturn /create FirewallPolicyUpdate

bitsadmin /rawreturn /addfile FirewallPolicyUpdate file://c:\windows\system32\
kernel32.dll c:\windows\temp\h.jpg

bitsadmin /rawreturn /setnotifycmdline FirewallPolicyUpdate "rundll32.exe"
"rundll32.exe javascript:""\..\mshtml,RunHTMLApplication "";document.
write();new%%20ActiveXObject(""""WScript.Shell"""").Run(""""c:\\windows\\
syswow64\\WindowsPowerShell\\v1.0\\powershell.exe -ep bypass
-Command $s=(gwmi Win32_OSRecoveryConfiguration).DebugFilePath -split
'\\^|';$b=$ExecutionContext.InvokeCommand.NewScriptBlock([system.Text.
Encoding]::Unicode.GetString([system.Convert]::FromBase64String($s[0])));icm $b
-ArgumentList @($s[1]);Start-Sleep -Milliseconds 1000;"""",0,true)"

bitsadmin /rawreturn /setpriority FirewallPolicyUpdate high

bitsadmin /resume FirewallPolicyUpdate
```


https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

3.2.1 Threat Intelligence Reports - FireEye

FireEye also publishes threat intelligence reports by industry. So if your industry is Education, you will be able to read a report specific to this industry.

You can get more information on these reports here.

https://www.fireeye.com/current-threats/reports-by-industry.html

3.2.2 Threat Intelligence Research

Other than these reports, many companies and researchers frequently publish new research reports on emerging threats, often containing IOCs.

As an example, we'll look into a publication from Palo Alto Network's Unit42 on a recent vulnerability in Citrix ADC and Citrix Gateway.

https://unit42.paloaltonetworks.com/unit42-keyslogger-new-cloud-based-keylogger-enters-market/
https://unit42.paloaltonetworks.com/

3.2.2 Threat Intelligence Research

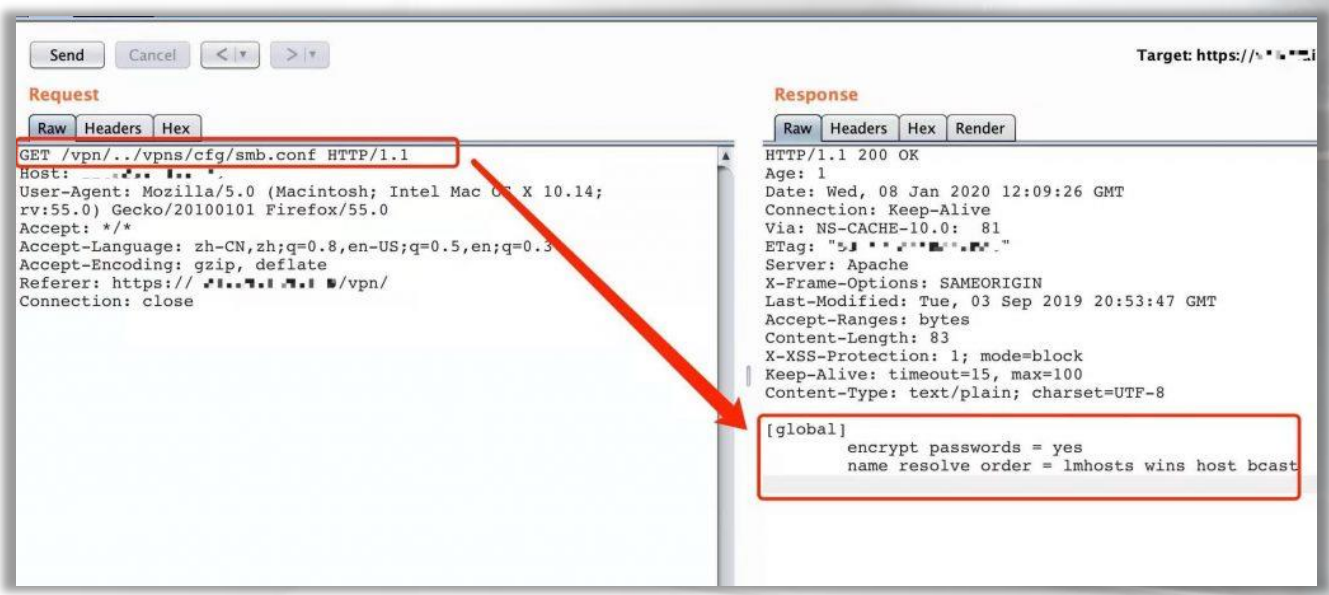
The blog mentions that the vulnerability “allowed remote attackers to easily send directory traversal requests, read sensitive information from system configuration files without the need for user authentication, and remotely execute arbitrary code.”

This vulnerability is tracked using CVE-2019-19781 and given a critical risk rating with a score of 9.8.

https://unit42.paloaltonetworks.com/exploits-in-the-wild-for-citrix-adc-and-citrix-gateway-directory-traversal-vulnerability-cve-2019-19781/
https://cve.MITRE.org/cgi-bin/cvename.cgi?name=CVE-2019-19781

3.2.2 Threat Intelligence Research

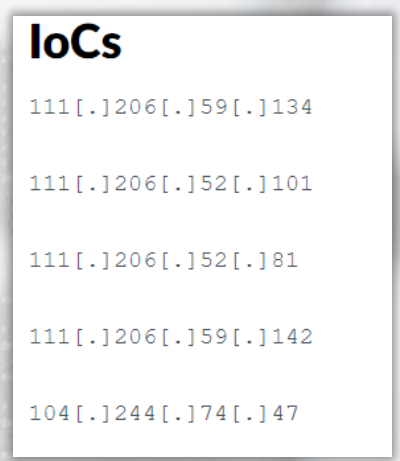
In the publication, a detailed root cause analysis is provided as well as Proof-of-Concept exploitation.



https://unit42.paloaltonetworks.com/exploits-in-the-wild-for-citrix-adc-and-citrix-gateway-directory-traversal-vulnerability-cve-2019-19781/

3.2.2 Threat Intelligence Research

Finally, in the conclusion section, they provide a temporary fix recommended by the vendor as well as IOCs and IP addresses associated with abnormal scanning activity designed to exploit this vulnerability.



https://unit42.paloaltonetworks.com/exploits-in-the-wild-for-citrix-adc-and-citrix-gateway-directory-traversal-vulnerability-cve-2019-19781/

3.2.2 Threat Intelligence Research

When reading a report or research publication, you should try to gain the most out of it by asking questions such as:

- What / how was the objective achieved?
- What can we do to detect this activity?
- Is this similar to previously known activity?

Aim to identify some behavioral trends and map them to TTPs. Focus on those that are difficult to change.

3.2.2 Threat Intelligence Research

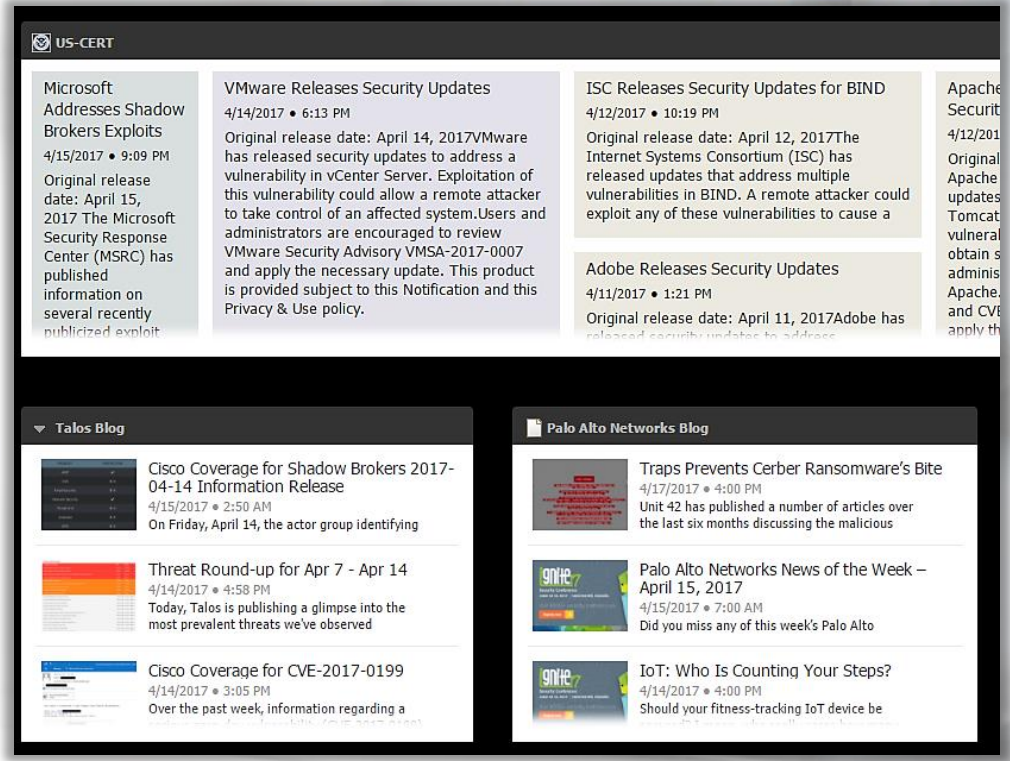
As you can imagine, constantly going through various blogs can be a time consuming and daunting task, especially with more vendors entering into this space.

One suggestion would be to create a dashboard and have feeds auto-populate the dashboard with data from multiple vendors

3.2.2 Threat Intelligence Research

Here is a snippet of the dashboard that we use when gathering threat intelligence from multiple sources.

This will allow us to be constantly in the know as threat intelligence is made available.



Threat Sharing and Exchanges

3.3.1 Threat Sharing and Exchanges – ISACs

Information Sharing and Analysis Centers (ISACs) are member-driven organizations, delivering all-hazards threat and mitigation information to asset owners and operators.

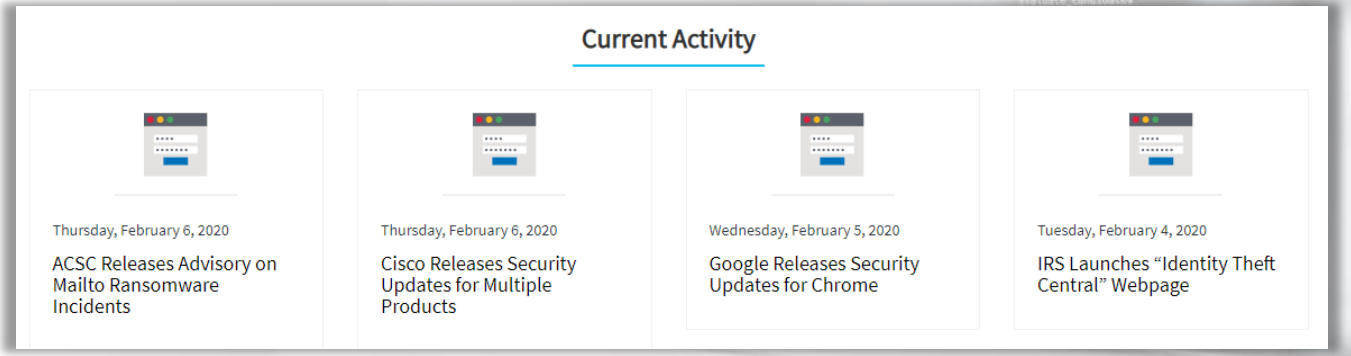
To maintain situational awareness across the various critical infrastructure sectors, ISACs collaborate and share threat and mitigation information with each other, and with other partners through the National Council of ISACs.

3.3.1 Threat Sharing and Exchanges – ISACs

You can view more information about ISACs, the National Council of ISACs, and a list of member ISACs here.

3.3.2 Threat Sharing and Exchanges – US-CERT

The **United States Computer Emergency Readiness Team (US-CERT)** responds to major incidents, analyzes threats, and provides critical cybersecurity information. You can read more about them on their site. Below is an example of the latest feed.



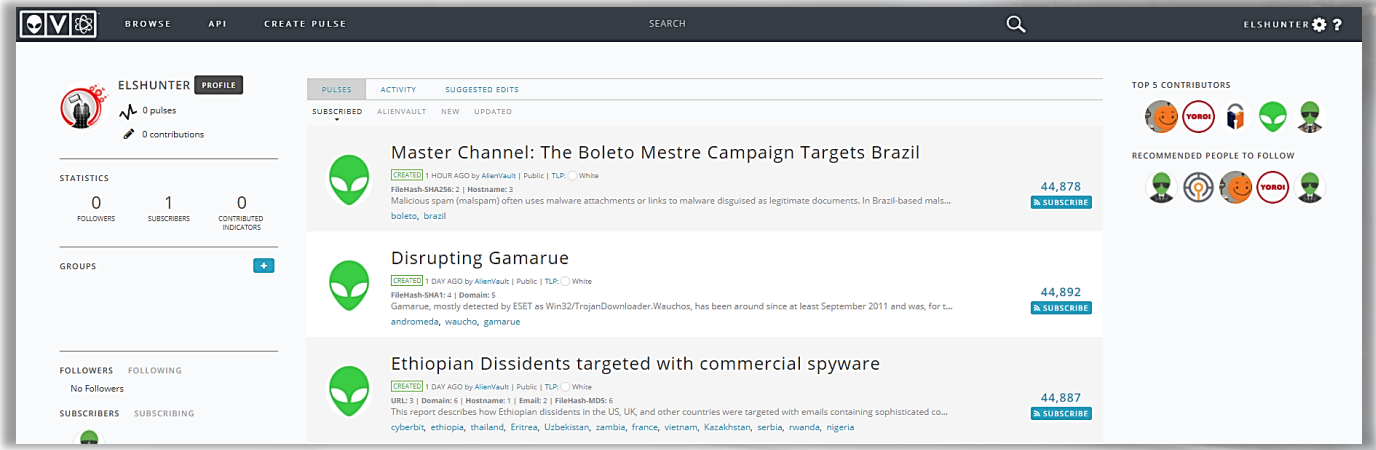
https://www.us-cert.gov/

3.3.2 Threat Sharing and Exchanges – US-CERT

Many countries have similar teams, and you may check with them for information on threat sharing.

3.3.3 Threat Sharing and Exchanges – OTX

AlienVault's Open Threat Exchange is an open threat intelligence community that enables collaborative defense with actionable, community-powered threat data. You can join OTX here to view threat intelligence feed right away.



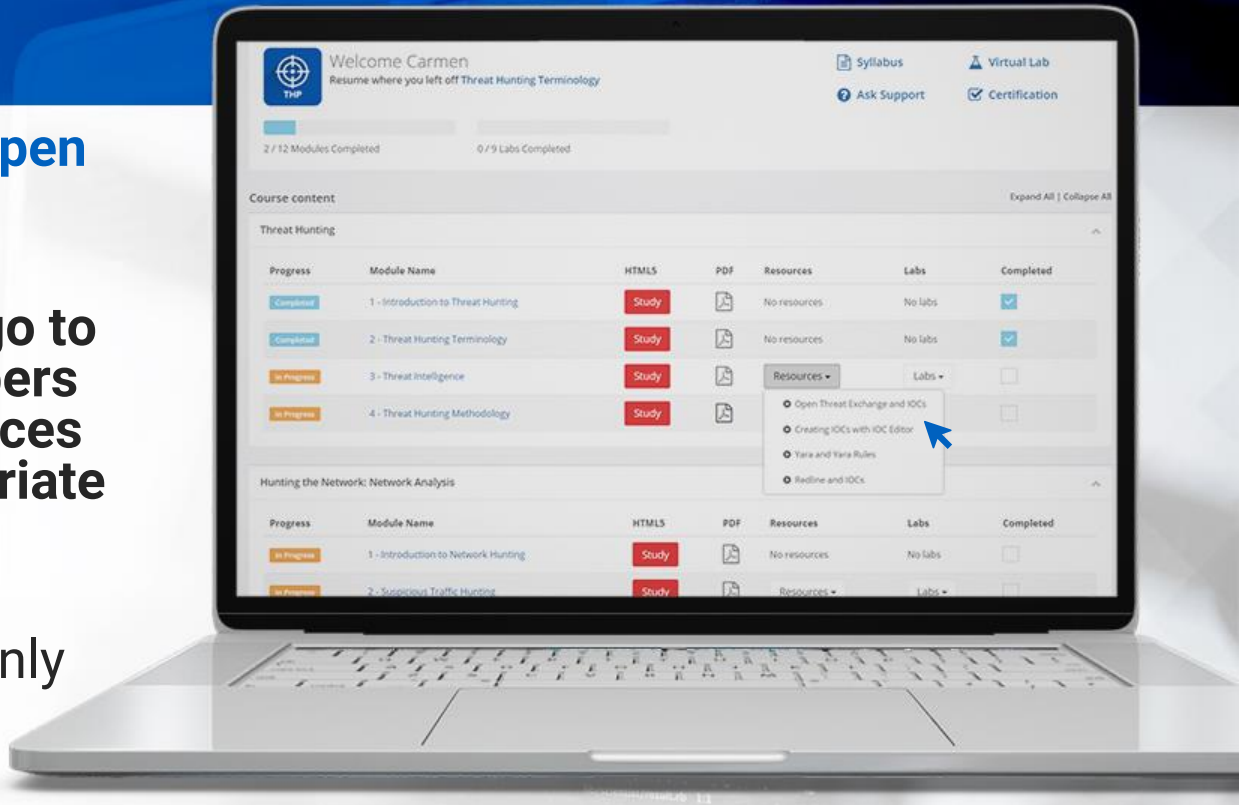
https://www.alienvault.com/open-threat-exchange

3.3.3.1 VIDEO

Check out the video on **Open Threat Exchange & IOCs**!

To ACCESS your video, go to the course in your members area and click the resources drop-down in the appropriate module line.

Note that all videos are only available in Full or Elite Editions of the course. To upgrade, click **LINK**.

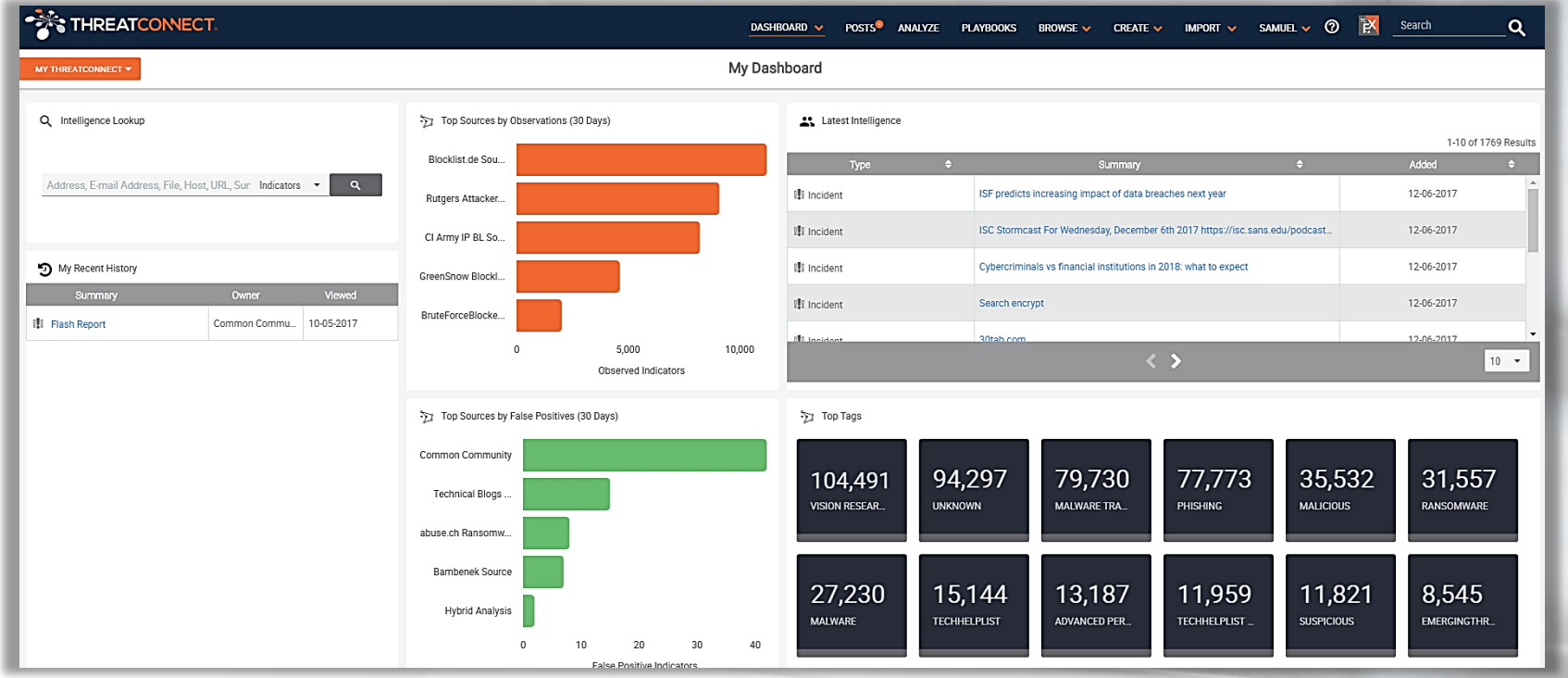


3.3.4 Threat Sharing and Exchanges – Threat Connect

Threat Connect is another platform, similar to OTX, where you can obtain threat intelligence freely. You can create an account and join right away to start sifting through threat intel.

You can join Threat Connect here.

3.3.4 Threat Sharing and Exchanges – Threat Connect



3.3.5 Threat Sharing and Exchanges – MISP

Finally, the **Malware Information Sharing Platform (MISP)** is an open-source software solution for collecting, storing, distributing, and sharing cybersecurity indicators and threats about cybersecurity incident analysis and malware analysis.

http://www.misp-project.org/

3.3.5 Threat Sharing and Exchanges – MISP

MISP provides functionalities to support the exchange of information but also the consumption of said information by Network Intrusion Detection Systems (NIDS) and also log analysis tools, such as SIEMs.

You can visit the MISP Project for detailed information and guidelines here.

http://www.misp-project.org/

Indicators of Compromise

3.4 Indicators of Compromise

Digital Guardian gives a good definition as to what IOCs are.

Indicators of compromise (IOCs) are “pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.”

https://digitalguardian.com/blog/what-are-indicators-compromise

3.4 Indicators of Compromise

Indicators of compromise aid information security and IT professionals in detecting:

- Data breaches
- Malware infections
- Other threat activity

By monitoring for indicators of compromise, organizations can detect attacks and act quickly to prevent breaches from occurring, or limit damages by stopping attacks in earlier stages.

3.4 Indicators of Compromise

When we obtain IOCs from ISACs, threat sharing platforms, etc., we need to get the IOC in the format that our tools will understand. For instance, OTX allows us to download IOCs in the OpenIOC format.

Typically, IOCs are malware signatures, MD5 hashes of malware files, IP addresses, and URLs or domain names of botnet command and control servers.

3.4.1 Indicators of Compromise – OpenIOC

OpenIOC, developed by FireEye, provides a standard format and terms for describing the artifacts encountered during the course of an investigation.

This course focuses only on the OpenIOC format, while others also exist.

3.4.2 Indicators of Compromise – IOC Editor

IOC Editor is a tool that we'll look at within this course. It is a free tool that provides an interface for managing data and manipulating the logical structures of IOCs.

IOCs are XML documents that help security professionals capture diverse information about threats, including attributes of malicious files, characteristics of registry changes, and artifacts in memory. You can download the tool here.

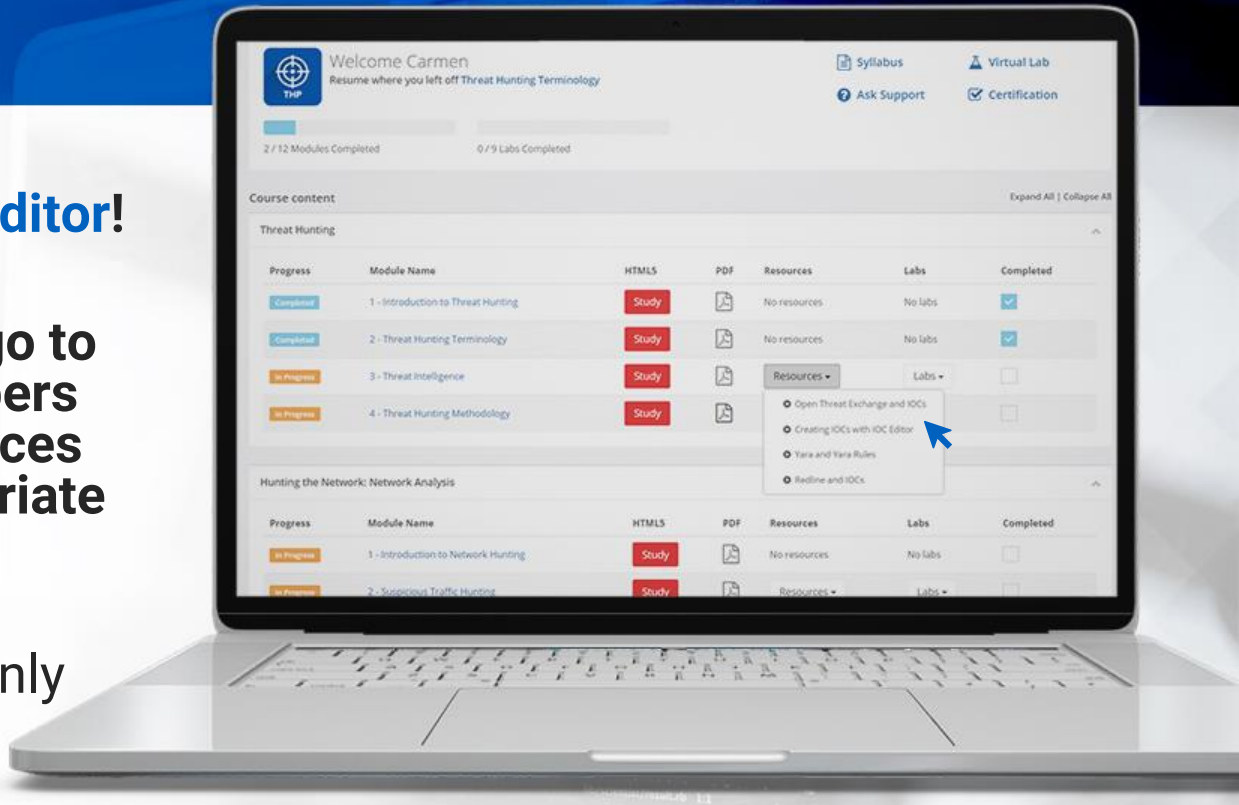
https://www.fireeye.com/services/freeware/ioc-editor.html

3.4.2.1 VIDEO

Check out the video on **Creating IOCs with IOC Editor**!

To ACCESS your video, go to the course in your members area and click the resources drop-down in the appropriate module line.

Note that all videos are only available in Full or Elite Editions of the course. To upgrade, click **LINK**.



3.4.3 Indicators of Compromise – Redline

Another tool from FireEye that we'll look at within this course is Redline.

Although we will look at Redline more extensively when performing memory analysis in a later module, for now, we will use the tool to search for IOCs on a machine.

3.4.3 Indicators of Compromise – Redline

Redline can perform an Indicators of Compromise (IOC) analysis. Supplied with a set of IOCs, the Redline Portable Agent is automatically configured to gather the data required to perform the IOC analysis, and an IOC hit result review.

You can download the tool from here.

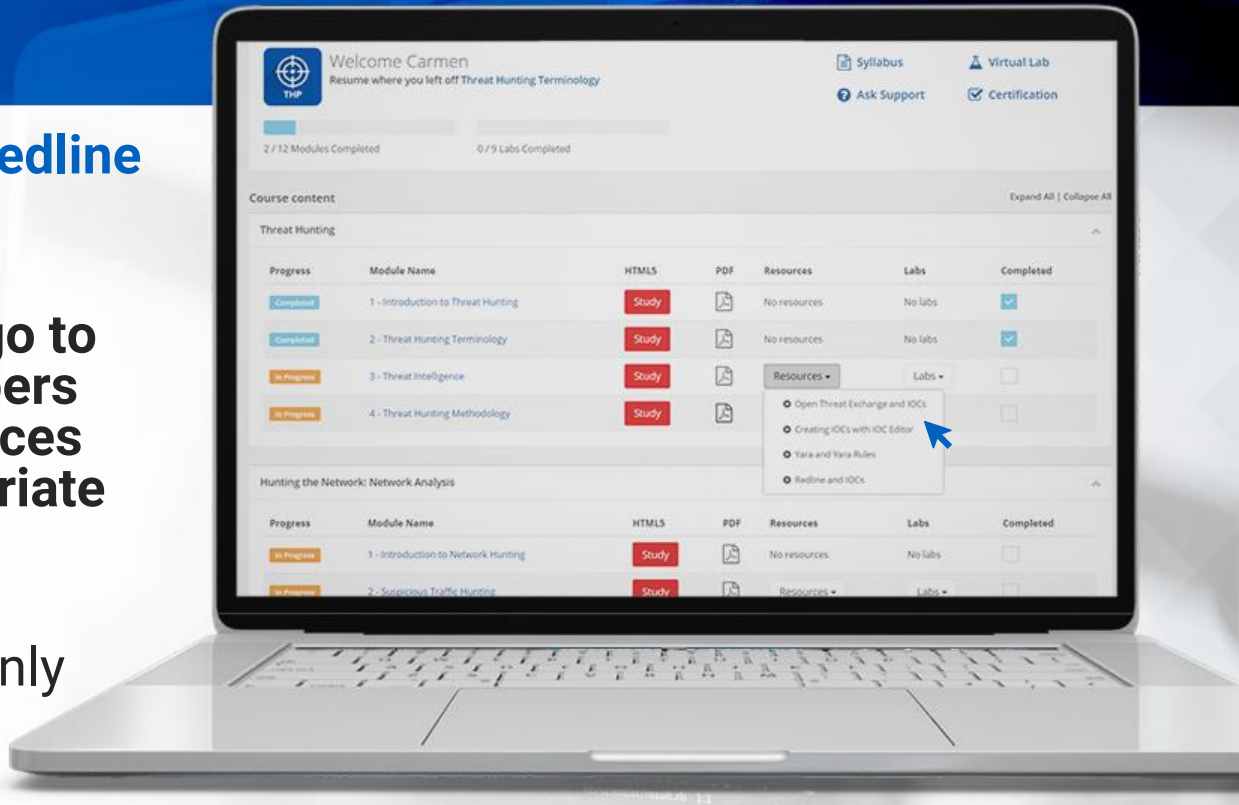
https://www.fireeye.com/services/freeware/redline.html

3.4.3.1 VIDEO

Check out the video on **Redline and IOCs**!

To ACCESS your video, go to the course in your members area and click the resources drop-down in the appropriate module line.

Note that all videos are only available in Full or Elite Editions of the course. To upgrade, click **LINK**.



3.4.4 Indicators of Compromise – YARA

Lastly, in this chapter, let's look at YARA.

YARA is a tool aimed at (but not limited to) helping malware researchers to identify and classify malware samples. With YARA, you can create descriptions of malware families (or whatever you want to describe) based on textual or binary patterns.

3.4.4 Indicators of Compromise – YARA

Even though we won't be performing malware analysis in this course, we will still use YARA to detect the presence of IOCs on a particular machine.

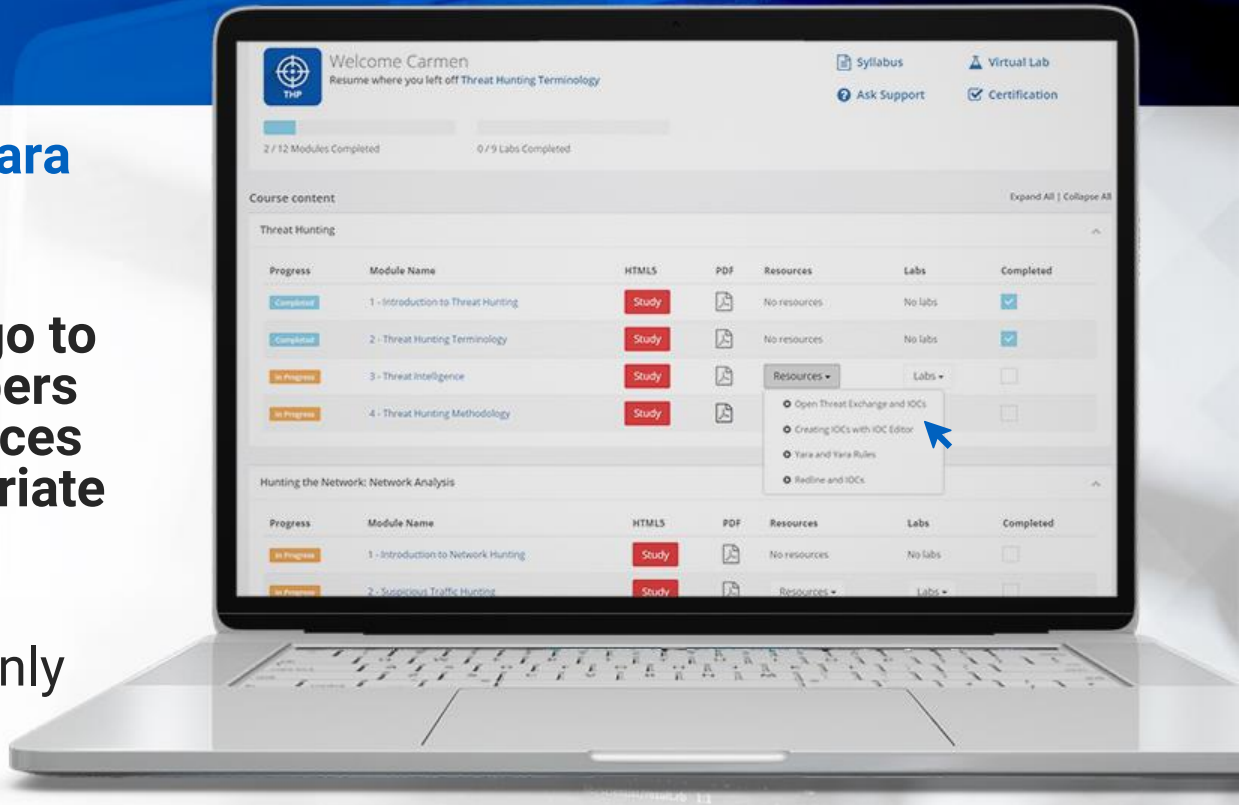
You can read more about Yara and download the tool here.

3.4.4.1 VIDEO

Check out the video on **Yara and Yara Rules**!

To ACCESS your video, go to the course in your members area and click the resources drop-down in the appropriate module line.

Note that all videos are only available in Full or Elite Editions of the course. To upgrade, click **LINK**.

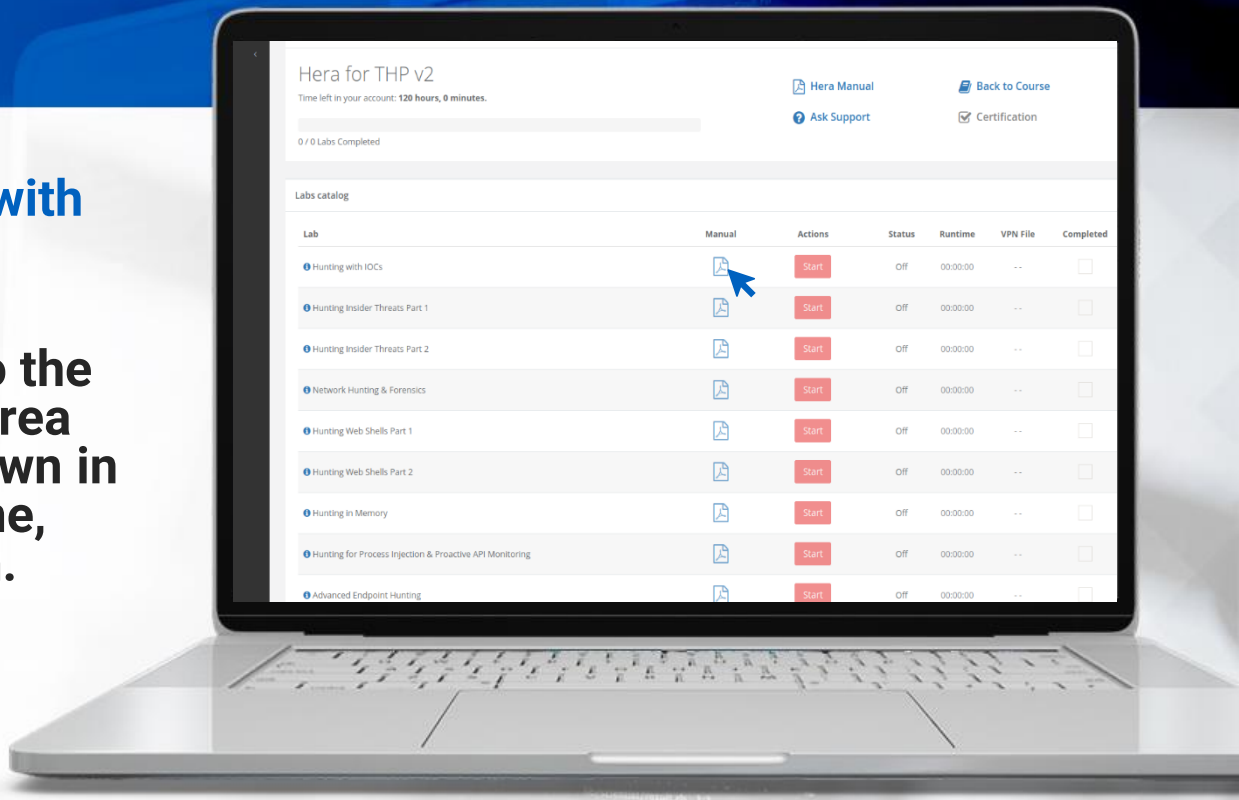


3.4.5 Hera Lab

Put what you've learned to practice with the **Hunting with IOCs** lab!

To ACCESS your lab, go to the course in your members area and click the labs drop-down in the appropriate module line, then click the manual icon.

All labs are only available in Full or Elite Editions of the course. To upgrade, click **LINK**.



***NOTE: some courses contain several labs and manuals, please make sure to click the file icon as it may be a zip that contains multiple lab manuals.**

Conclusion

This concludes this module on Threat Intelligence. We have covered:

- ✓ Manually gathering threat intelligence:
  - Vendors that publish annual threat intelligence reports
  - Vendors that publish occasional threat research reports and/or blogs with IOCs that we can use
  - Threat sharing organizations
- ✓ IOC formats and tools for creating/editing IOCs

References

References

FireEye

https://www.fireeye.com/

Threat Intelligence Reports

https://www.fireeye.com/current-threats/threat-intelligence-reports.html

Complimentary Intel Report: Russia's APT28 Strategically Evolves its Cyber Operations

https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html

From Intrusion to Underground Card Shop

https://www2.fireeye.com/WEB-RPT-FIN6.html

References

FIN6

https://attack.MITRE.org/groups/G0037/

M-Trends 2020

https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

Threat Intelligence Reports by Industry

https://www.fireeye.com/current-threats/reports-by-industry.html

Exploits in the Wild for Citrix ADC and Citrix Gateway Directory Traversal Vulnerability CVE-2019-19781

https://unit42.paloaltonetworks.com/exploits-in-the-wild-for-citrix-adc-and-citrix-gateway-directory-traversal-vulnerability-cve-2019-19781/

References

[Palo Alto Network's Unit42]

https://unit42.paloaltonetworks.com/

[CVE-2019-19781]

https://cve.MITRE.org/cgi-bin/cvename.cgi?name=CVE-2019-19781

[National Council of ISACs]

https://www.nationalisacs.org/

[CISA]

https://www.us-cert.gov/

References

Open Threat Exchange (OTX)

https://www.alienvault.com/open-threat-exchange

ThreatConnect

https://www.threatconnect.com/

MISP

http://www.misp-project.org/

What are Indicators of Compromise?

https://digitalguardian.com/blog/what-are-indicators-compromise

References

IOC Editor

https://www.fireeye.com/services/freeware/ioc-editor.html

Redline

https://www.fireeye.com/services/freeware/redline.html

YARA

https://virustotal.github.io/yara/

Videos

Here's a list of all videos in this module. To **ACCESS** your video, go to the course in your members area and click the resources drop-down in the appropriate module line.

Note that all videos are only available in Full or Elite Editions of the course. To upgrade, click **LINK**.

Open Threat Exchange & IOCs

Creating IOCs with IOC Editor

Redline and IOCs

YARA and YARA Rules

Labs

Hunting with IOCs

Another organization within your ISAC has shared a malicious binary with your security team. They mentioned this malware was detected by one of their threat hunters. The malware was found inside various network shares within the organization, disguising itself as a PDF file. Your manager has tasked you with creating an IOC and YARA rule to scan the network for this malware.

Labs are only available in Full or Elite Editions of the course. To ACCESS your labs, go to the course in your members area and click the labs drop-down in the appropriate module line. To UPGRADE to gain access, click LINK.