Threat Intelligence

Module 3

Threat Intelligence Module – Map

MAP REF

- 3.1 Introduction
- 3.2 Threat Intelligence Reports
- 3.3 Threat Intelligence Research
- 3.4 Threat Sharing and Exchanges
- 3.5 Indicators of Compromise

Introduction

In the previous module, we discussed the 2 mindsets of a Threat Hunter:

1. A hunter that relies mostly on threat intelligence

2. A hunter that relies mostly on digital forensics

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

"Threat Intelligence is data on threats."

Let’s go into more detail on this definition.

As you may recall, for that data to become intelligence it has to be processed, analyzed, and become actionable data.

The data will be pertinent to your infrastructure and assets.
The data will include context, not just indicators.

A more thorough definition of Threat Intelligence, from Gartner, is as follows:

> ***"Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard."***

The intelligence will contain more than IP addresses, file hashes, etc. It will contain TTPs, advice on how to stop their attack, etc.

Remember that this type of hunter is relying on information looking for **known** threats.

This module will describe the manual efforts a threat hunter will take to obtain threat data.

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

3.1 Introduction

A **SIEM** is a Security Information and Event Management solution. A SIEM is a centralized collection point where all logs (firewall, network, application, event, etc.) are collected in which the Security Analyst can analyze instead of logging into various consoles to view log data. The logs can also contain external data. We'll look at SIEMs later.

3.1 Introduction

With that being said, 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

3.2 Threat Intelligence Reports

MAP REF

There are several trusted third-parties that collect and gather cyber intel data and Threat Intelligence reports.

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

FireEye

The first trusted source is **FireEye**.

They create and publish an annual threat report and regularly publish threat intelligence reports.

3.2 Threat Intelligence Reports

MAP REF

FireEye

When navigating to their website, under Resources > Threat Intelligence Reports, you'll have immediate access to threat intelligence reports regarding threat actors, such as APT28, and threat groups, such as FIN6.

FireEye

The naming convention for Financial Threats are known as **FIN** groups. In the previous, slide a FIN6 was listed.

According to Mitre, FIN6 is a cyber crime group that steals credit card data and sells it in underground markets. They target PoS (Point of Sale) systems in the retail and hospitality sector.

FireEye

As you may recall, each vendor might have a different naming convention for a particular threat group.

The FIN6 group is also known as G0037 under Mitre's naming convention.

FireEye

As mentioned before, FireEye also publishes an annual threat report on trends from the year's breaches and cyber attacks called M-Trends.

According to their website, the M-Trends report provides an intelligence-led look at various topics such as emerging global threats and latest defensive strategies.

3.2 Threat Intelligence Reports

MAP REF

FireEye

The latest edition of M-Trends is published, M-Trends 2017.

Let’s highlight certain sections of the report but it is highly recommended to read the entire report.

FireEye

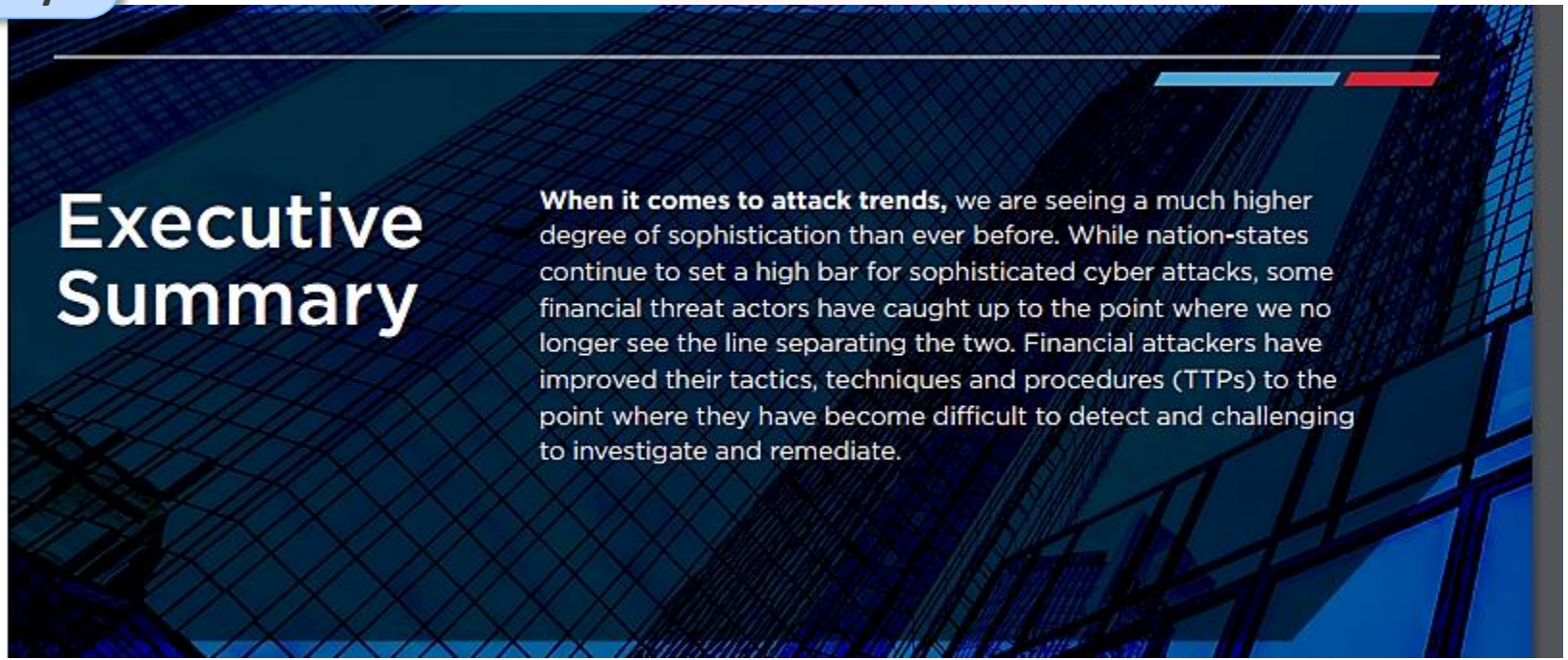
Let’s start with the Executive Summary.

FireEye, along with many others, are pointing out that it has become difficult to differentiate a nation-state threat group and a financial cybercrime group.

3.2 Threat Intelligence Reports

MAP REF

FireEye



FireEye

This is important to note because not every attack or group will be labeled as '**APT**' but they could operate as one.

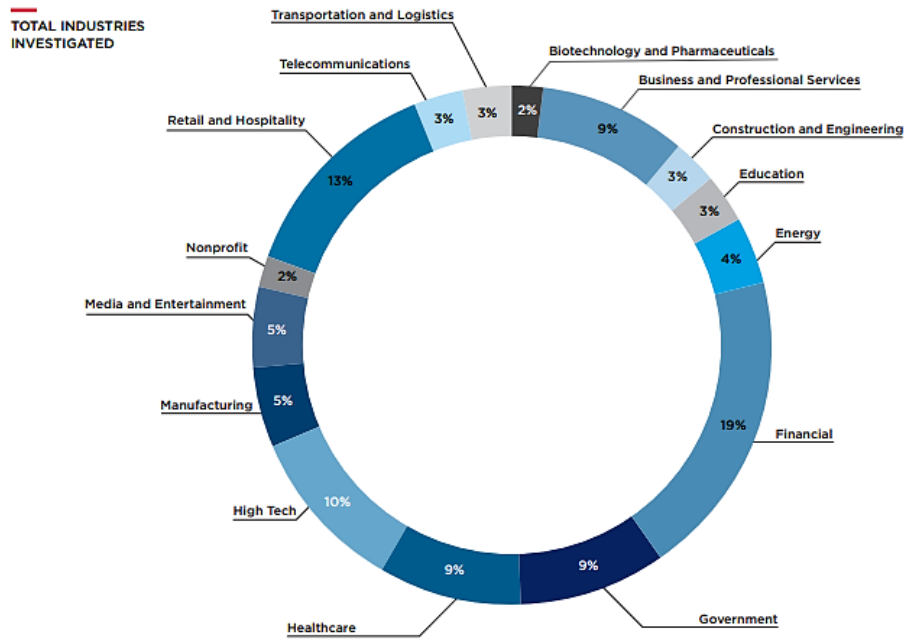
3.2 Threat Intelligence Reports

MAP REF

FireEye

In the screenshot to the right, the image shows us that the two most focused industries are Financial, and Retail and Hospitality.

Note that this is based on FireEye's investigations



FireEye

The Financial industry is marked at 19%, but the previous slide didn't say how much of that is based in Europe, Asia, or Americas?

The screenshot here shows the industries are broken down according to region.

KEY: INDUSTRIES INVESTIGATED

Industry	America	APAC	EMEA	Total
Financial	15%	31%	36%	19%
Retail and Hospitality	15%	7%	10%	13%
High Tech	12%	7%	2%	10%
Healthcare	12%	2%	0%	9%
Business and Professional Services	10%	5%	3%	9%
Government	8%	5%	16%	9%
Manufacturing	5%	7%	5%	5%
Media and Entertainment	5%	7%	2%	5%
Energy	3%	10%	3%	4%
Construction and Engineering	3%	2%	7%	3%
Education	3%	0%	2%	3%
Telecommunications	2%	9%	5%	3%
Transportation and Logistics	2%	5%	7%	3%
Nonprofit	2%	0%	0%	2%
Biotechnology and Pharmaceuticals	2%	3%	2%	2%
Other	1%	0%	0%	0%

FireEye

Note that **APAC** refers to the Asia Pacific region whereas **EMEA** refers to Europe, the Middle East, and Africa.

FireEye publishes threat reports based on specific regions as well.

FireEye

Along with publishing reports specific to a particular region, 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. Get more information of the reports here.

FireEye

The M-Trends 2017 report provides a lot of useful information.

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

3.2 Threat Intelligence Reports

MAP REF

FireEye

Figure 7.
Batch script to hide malware execution.

```
del /f /q /s %windir%\prefetch\*
reg delete "HKCU\Software\Microsoft\Windows\ShellNoRoam\MUICache" /va /f
reg delete "HKLM\Software\Microsoft\Windows\ShellNoRoam\MUICache" /va /f
reg delete "HKCU\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" /va /f
reg delete "HKLM\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache" /va /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU" /va /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist" /va /f
wmic nteventlog where LogFileName='File Replication Service' Call ClearEventlog
wmic nteventlog where LogFileName='Application' Call ClearEventlog
wmic nteventlog where LogFileName='System' Call ClearEventlog
wmic nteventlog where LogFileName='PowerShell' Call ClearEventlog
ren %1 temp000 & copy /y %windir%\regedit.exe temp000 & del temp000
```

FireEye

At this point, it should be noted that we are not promoting one vendor over another and we are not promoting any company's services or equipment.

Verizon

The next vendor we'll look at is Verizon.

Verizon published a report titled 2016 Data Breach Investigations Report.

You can download the report here.

Verizon

As with M-Trends, we will briefly highlight certain parts of this report, but we expect you to read the report on your own.

The prologue is a good starting point and a good reminder to the blue team, including threat hunters.

Verizon

Playing a part on the blue team in information security can, to a very small degree, be compared to the lot of a hapless soldier. The soldier is told to guard a certain hill and to keep it at all costs. However, he is not told who his enemy may be, what they look like, where they are coming from, or when (or how) they are likely to strike. To ride this analogous horse a bit further, the soldier is given a hand-me-down rifle with only a few rounds of ammunition to fulfill his task. It seems a bit unfair really—even the American Revolution got Paul Revere.

With that in mind, we hope that this section and the facts and figures contained in it will go some way toward making you better prepared than our friend mentioned above. After all, "forewarned is forearmed."

Be prepared: forewarned is forearmed.

Verizon

This statement is very true. That is why we use threat intelligence to aid us in fighting the ever-growing list of adversaries.

We have to be accustomed to constantly researching and reading, to stay abreast to the latest news in the threat landscape.

Verizon

Within this report it also states that the report was based on the VERIS framework.

We'll discuss more on frameworks that will assist us in sharing information. For now you can read more about VERIS here.

Verizon

You will notice as you read various reports published by different vendors that the research might not align with the others.

Keep in mind these reports are based on the initial vendors research and findings.

TrustWave

Another report worth mentioning is a report from TrustWave.

TrustWave's latest annual report is the 2016 TrustWave Global Security Report. You can get a copy here.

TrustWave

It is not as recent as M-Trend's, but definitely worth reading. You will see data from investigations and/or research dating back to 2015.

Remember that the adversary will stick to an attack pattern, TTPs.

TrustWave

Within the TrustWave's Global Security Report, the conversion of data into actionable intelligence is illustrated.

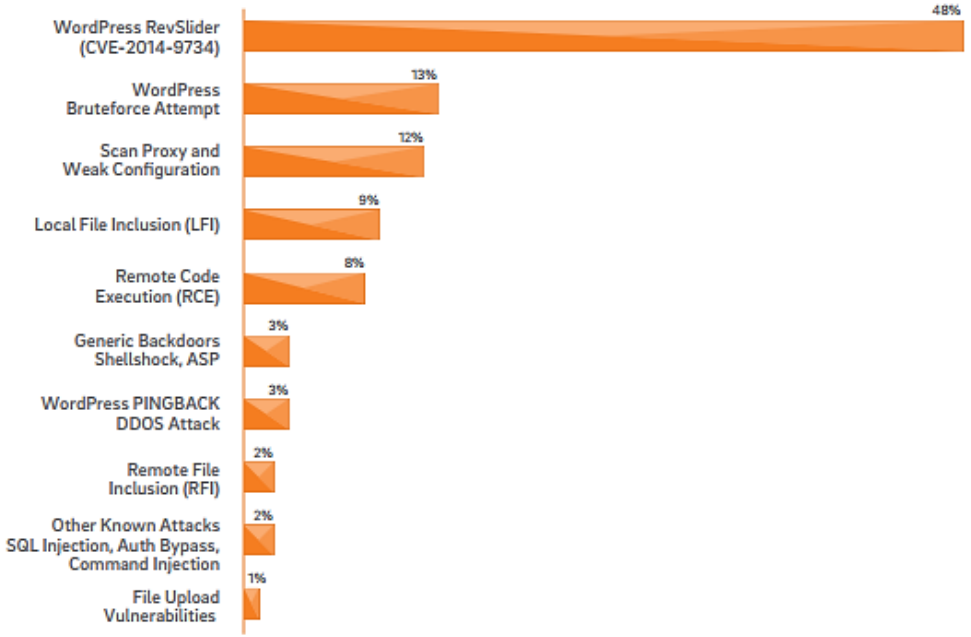
In the Web Attacks section, it discusses the top attack methods based on their research of cybercriminals in 2015.

3.2 Threat Intelligence Reports

MAP REF

TrustWave

TOP OPPORTUNISTIC ATTACK EXPLOIT METHODS OBSERVED BY TRUSTWAVE



3.2 Threat Intelligence Reports

MAP REF

TrustWave

We see that CVE-2014-9734 is listed. It relates to a WordPress plugin known as RevSlider.

WordPress is a popular blogging software that has been widely used for not only blogging but for creating full websites.

TrustWave

This particular plug-in, based on the publisher's website, boasts that it's installed on 2,500,000+ websites.

Many enterprises use this platform for external and internal facing websites.

TrustWave

If your organization doesn't use WordPress then this data would be of no significance to you.

On the other hand if WordPress is used in your organization then this information is definitely of value to you.

TrustWave

From the report, we read more specific information regarding this CVE.

Note that **CVE** means *Common Vulnerabilities and Exposures,* from MITRE.

TrustWave

Let's first look at the official CVE for this vulnerability, CVE-2014-9734.

> *"Directory traversal vulnerability in the Slider Revolution (revslider) plugin before 4.2 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the img parameter in a revslider_show_image action to wp-admin/admin-ajax.php."*

3.2 Threat Intelligence Reports

MAP REF

TrustWave

CVE-ID	
CVE-2014-9734	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Directory traversal vulnerability in the Slider Revolution (revslider) plugin before 4.2 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the img parameter in a revslider_show_image action to wp-admin/admin-ajax.php.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- EXPLOIT-DB:34511
- URL:http://www.exploit-db.com/exploits/34511
- MISC:http://marketblog.envato.com/news/affected-themes/
- MISC:http://marketblog.envato.com/news/plugin-vulnerability/
- MISC:http://packetstormsecurity.com/files/132366/WordPress-Revslider-4.2.2-XSS-Information-Disclosure.html
- MISC:https://blog.sucuri.net/2014/12/revslider-vulnerability-leads-to-massive-wordpress-soaksoak-compromise.html
- MISC:https://plugins.trac.wordpress.org/browser/patch-for-revolution-slider/trunk/revsliderpatch.php
- CONFIRM:https://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html

TrustWave

We also see that there are several links pointing to proof of concept information.

This is nothing new if you have training or experience as a penetration tester.

TrustWave

On page 38 of the TrustWave report, we are given more information about this attack vector.

Of these, the largest share targeted a vulnerability in the popular Slider Revolution ("RevSlider") plugin, which displays a rotating gallery of images on a web page. A vulnerability discovered in 2014 enables an attacker to use the plugin to access files elsewhere on the web server, a technique called local file inclusion (LFI). In an audit log dump of the HTTP request from the ModSecurity web application firewall, an attacker attempts to download the WordPress master configuration file wp-config.php, which contains database credentials and other sensitive information and can often allow an attacker to compromise the website.

TrustWave

We are also presented with an example of how that attack would look like in the log files.

```
--fd0b151b-A--
[03/Sep/2014:04:23:23 --0500] VAbeC8Co8AoAABmBX5EAAAAL 85.25.242.250 34609 XXX.XXX.XXX.XXX 80
--fd0b151b-B--
GET //wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php HTTP/1.1
TE: deflate,gzip;q=0.3
Connection: TE, close
Host: REDACTED
User-Agent: lwp-request/5.834 libwww-perl/5.834
```

TrustWave

This data has now become **threat intelligence**.

First, you have information on the attack vector that threatens one of your assets.

Second, you have information about how it is being exploited including how to find it when looking at historical data and when threat hunting.

TrustWave

Remember this is the manual process of obtaining threat intelligence. You can image how long it would take to read annual reports, monthly, or weekly reports from different vendors.

Ultimately, you would like this automatically fed into your SIEM.

CrowdStrike

Even though there are more vendors or organizations that we can discuss, such as ENISA, who also publishes an annual report, we will discuss just one more vendor, CrowdStrike.

CrowdStrike

CrowdStrike released a reported titled CrowdStrike Cyber Intrusion Services Casebook 2016.

You can obtain a copy here.

CrowdStrike

The download page states that this report covers information regarding the DNC (Democratic National Committee) hack, TTPs from specific nation-state and cybercrime groups.

This is a good read.

CrowdStrike

Page 4 of the report outlines 3 key trends based on 12 months of investigations:

1. Attackers are increasing their use of anti-forensic tools.
2. 3rd party trust relationships bring significant risk to the enterprise.
3. Attackers are increasing use of trusted system processes to execute exploits.

CrowdStrike

On page 22 of the CrowdStrike report, the section, *Revealing The Latest Adversary Tradecraft*, discusses the latest adversary trends.

CrowdStrike

Not surprisingly PowerShell is the topic of discussion. Adversaries using PowerShell is a technique known as ‘living off the land’.

PowerShell continues to be an underestimated tool which often times goes unmonitored in the enterprise.

CrowdStrike

The report also mentions the increased use of using WMI to launch PowerShell to download a Meterpreter payload.

We will look into these techniques and how to hunt for them in later modules.

3.2 Threat Intelligence Reports

Now let’s look at vendor’s conducting specific threat reports and how they can be useful to us.

Threat Intelligence Research

Palo Alto

The first vendor we'll discuss in the section is Palo Alto Networks.

Palo Alto Networks Threat Intelligence Team is called Unit 42, and they frequently publish new research.

Palo Alto

These reports are good to monitor. Let's look at a few.

Note, when you navigate to the Unit 42 blog page, their reports are posted as blog postings, not actual downloadable PDF reports.

Palo Alto

Let’s look at the research conducted on a keylogger named NexusLogger.

This will prove how important it is to pull data from multiple sources.

Palo Alto

The blog mentions that this is a cloud-based keylogger that uses the Microsoft .NET Framework.

It collects keystrokes, system information, stored passwords, and screenshots.

It also mentions that it will specifically seek credentials for UPlay, Minecraft, Steam, and Origin gaming websites/platforms.

Palo Alto

Based on their research, this report mentions what industries have been affected by this keylogger: Wholesale, High Tech, and Aerospace and Defense.

The domain that NexusLogger uses is flagged as malicious by blocked by Palo Alto Networks but it might not be blocked by your appliances.

Palo Alto

The NexusLogger is mostly distributed via phishing emails.

In their blog post we are provided with some IOCs to aid us in blocking any potential future phishing attempts.

3.3 Threat Intelligence Research

MAP REF

Palo Alto

The report will give us IOCs regarding the subject lines these phishing emails use to distribute NexusLogger.

Top Email Subjects

1. Needed Products List
2. Re: DCE STATMENT as at 27 FEB 2017 – NS ALYANCE
3. Re: TOP URGENT Editing remittance form (2/26/2017)
4. Re: Revise Shipping Sample FW17 At00129 PI
5. Revise Shipping Sample FW17 At00129 PI
6. TOP URGENT Editing remittance form (2/26/2017)
7. Returned Msg: NEW ORDER
8. RECONFIRM YOUR BANK DETAILS FOR PAYMENT
9. NEW ORDER

Palo Alto

The report also gives us the filenames associated with NexusLogger.

Top Filenames

1. Needed Products4453487doc?gpj.exe
2. DCE STATMENT.doc
3. Scan 09892.doc
4. PO938272.doc
5. PO – BK0214017.exe
6. scan_2371_001.doc
7. Shipping details.exe
8. NEW ORDER_BK150217.exe
9. 20170256477867667557.exe
10. Purchase Order No. LP 68321.doc

Palo Alto

A few more things to note about this keylogger.

The research states that this keylogger is cloud-based and it has a portal where a user, for a price, can build a payload.

Palo Alto

On the NexusLogger portal, it is advertised as a parental monitoring software solution, but based on Unit 42's research the code contains anti-vm and anti-debugging techniques which stems from an open source project called ConfuserEx that was used to obfuscate the .NET compiled code.

Palo Alto

The code executes as traditional malware, by copying itself to the victims machine and deleting itself.

It also contains logic to perform a UAC bypass by making changes to the registry.

Palo Alto

Lastly we are provided with a long list of SHA256 hashes, which are more IOCs, which can be used to catch future attempts of this attack.

SHA256 Hashes

e98b417a8ecf464e113a18cf3f3269fa70f55e40d4228b08840efe61dee064c6
7fa743e2ce8eaa12f9c3e2aedd1f095ae5a50b5af34a202f1f92c0c414cb73c4
0f50c82e9c62eab992b33e4de93baf634d7ce2405cd4fe993b1532d2c775dc21
7153c18bc0a43c4902a6ebb0a7eedf94b3bc4d778295793035998c374cf607a9
bf6d2e3e097317404e57b194cbd8e50a6779603b828aa1b25364e6d81687e6af
6ae054a553120a1b5ffdfbf343ba1e258b188eef448c6474e22d148f7391afaa
7f5eee5c12ac89ab2604655cc7204723100e3ee6a2b6edb327c7c41a289de4f5
38d0d48685148ee070caaf82539083c8b62c8fe048ae6b0c0b3f43a6fe10a25d

Palo Alto

We'll see later on how we can make use of the IOCs we obtain from threat intelligence or the IOCs we create on our own.

Palo Alto

Unit 42 also published an Application Usage and Threat Report. Its an outdated report but still valuable. We suggest that you read it at your own leisure.

You can find report here.

Cylance

The next vendor that we'll look at is Cylance. They publish interesting papers and/or blog posts on threat research.

You can see list of blog postings here.

Cylance

You will find interesting reports called Operation Dust Storm and Operation Cleaver.

These are very good reads on emerging global threats affecting various industries, including industries within the United States.

Cylance

On page 74 of the Cylance #OPCLEAVER report, you will see IOCs ranging from domain names, IP addresses, hashes, etc.

This is always helpful in any threat intelligence report you're reading.

Cylance

Besides these papers, Operation Dust Storm and Operation Cleaver, it's worth highlighting Cylance's blog.

It contains very interesting research loaded with IOCs, and is worth reading.

Cylance

Let’s look at the blog post Threat Spotlight: GhostAdmin Malware.

What is GhostAdmin 2.0?

Cylance

Based on the blog post, GhostAdmin 2.0 is a botnet which was discovered in mid January 2017.

The capabilities of this botnet, also known as Ghost iBot, can range from stealing files to full remote access.

It accomplishes this by using standard Windows libraries.

Cylance

This malware will attempt to capture screenshots and keystrokes and store them in logs under a “Symantec” folder residing in AppData.

The blog shows a snippet of C# code that accomplishes the keylogging task, UserInput.LogUserKeys.

Cylance

The malware, GhostAdmin 2.0, uses Drawing.dll to create the screen captures and uses FTP to upload the keystroke logs and screenshots.

Cylance

GhostAdmin 2.0 uses IRC on port 6667 for it's C2 communications.

C2 is another way of stating command & control.

Remember that this malware is used for a botnet and receives instructions from a botmaster.

Cylance

The Cylance blog post on GhostAdmin 2.0 also shows an extensive list of C2 commands that the botmaster can issue.

```
public static void commandsList(string msg, string sender, StreamWriter writer)
{
    string[] array = new string[]
    {
        "@commands - list all available client commands",
        "@logfile - upload keylog file",
        "@read file <filePath> - read a text file",
        "@download <url> <destination> -  download a remote file from a url",
        "@turn off monitor - put monitor in sleep mode",
        "@turn on monitor - wake monitor from sleep mode",
        "@visit <url> -  browse a specified url",
        "@download <url> <destination> -  download a remote file from a url",
        "@delete* <ext> <source_directory> - delete all files in folder by ext",
        "@delete  file <filepath> - delete a single file",
        "@delete dir <source_directory> - delete a directory",
```

Cylance

There is more that this malware can accomplish but I'll leave the reading up to you.

Lastly, worth mentioning, GhostAdmin 2.0 uses winmm.dll to access the machines microphone to record audio for a specified amount of time.

This is also uploaded via FTP but what I didn't mention earlier is that once the files are uploaded, they are deleted.

Cylance

We are examining certain reports to show you the value of their information and how it will aide us in threat hunting.

This example was an interesting one, as it only uses the Windows Library.

It is its exfil method that should raise a flag.

Cylance

At the end of the research on GhostAdmin 2.0 you will find IOCs of value, in particular the hash for the settings file that is dropped onto the victim that is used for configuration for all the other components of the malware.

As wells the FTP and IRC information.

Cylance

Indicators of Compromise

Configuration/Setting Files:

de60046e23435edf47ddc1cf1dd0fcb64b706e066d289b64855a38551ab3c4fe

Decoded:

FTP Server: secured-apps(dot)com

FTP User: ghostadmin(at)secured-apps.com

IRC Server: irc.blafasel(dot)de

IRC Port: 6667

SHA-256 Hashes:

a50d3218f4a6b7c89d3e8df3463ac3a4704d92acee57cfe8d79200ad0c887aa9

91374f78d11bdb0683f8145ef38645b4c1a5278d89fc07c5d8e94474c079b36f

dbe19b22364e17002fa43626fa04ef5d1b4938db84eae1c71c1f6c296b0ef560

5106d31eeb4e93e6c44d4637fee1a1e5c12c88ddacf668c58828184756bd78eb

Talos

Moving to the next vendor, we'll briefly look at Cisco Talos.

According to their website, Talos is a threat intelligence organization dedicated to providing protection before, during, and after cybersecurity threats.

Talos

Their postings are valuable, especially because they provide official rule sets for Snort and ClamAV among others.

They are not just focused on Cisco appliances.

Talos

Let's look at the posting called "Threat Round-up for Apr 7 – Apr 14".

They list the most relevant threats for the week, their names and what the malware's capabilities are.

Talos

We see a list of IOCs for each of them a little further down in the article.

Java.Trojan.Adwind-6260775-0

INDICATORS OF COMPROMISE

Registry Keys

- **MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\[application name].exe**
  - **Value:** MAXIMUM ALLOWED
- **USER\[uuid]\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN**
  - **Value:** [a-zA-Z]+
  - **Data:** "C:\Users\[user]\AppData\Roaming\Oracle\bin\javaw.exe" -jar "C:\Users\[user]\[a-zA-Z]+\[a-zA-Z]+.[a-zA-Z]+"

Talos

Several of the IOCs has listed mutexes but we haven't discuss that term as of yet.

> A **mutex** (*mutual exclusion*) is an indicator to the malware that the system is already compromised so it won't attempt to re-infect the system.

Note: mutexes can be used for other reasons by malware authors and can also be used by legitimate software.

Talos

We won’t spend more time on Talos, as we immediately see the value of their blog and research.

F-Secure

The last vendor we'll look at is F-Secure.

They have several papers on threats that we can look at. We'll look at their research paper on The Callisto Group.

F-Secure

Under the Introduction section of this report, we see that this research is based on a threat group that has never been identified.

The focus of the group appears to be intelligence gathering related to European foreign and security policy.

F-Secure

I will let you read the report in its entirety. On page 7 of The Callisto Group report, we are given the IOCs.

F-Secure

APPENDIX A | INDICATORS OF COMPROMISE

SAMPLE HASHES

SHA1 of related RCS Galileo sample. We believe other similar samples exist.

07cdc67d211d175cd9d418dc5482b3f17d93526a

DETECTION NAMES

F-Secure detects **Callisto Group** activity with a variety of generic, behavioral, and other detections including the following:

Gen:Variant.Symmi.54992

PHISHING INFRASTRUCTURE

Domains known or believed to be used in relation to phishing. These may be used as targets of links or as domains for sender email addresses.

accounts-google.eu
accounts-mail.asia
authentification-request.top
auth-login.top
drive-login.com
drive-meet-goodle.ru
emailapp.pw
fco-gov.pw
fco-net.pw

F-Secure

FILE PATHS

Upon infection, known samples of **Callisto Group**'s RCS Galileo have stored copies of themselves in the following locations:

%TEMP%\Microsoft Word.exe
%TEMP%\WinWord.exe
>startup folder<\bleachbit.exe
>startup folder<\BluetoothView.exe

COMMAND & CONTROL INFRASTRUCTURE

Known command & control servers

89.46.102.43

We can continue to list threat research reports from other vendors but we'll leave that search up to you.

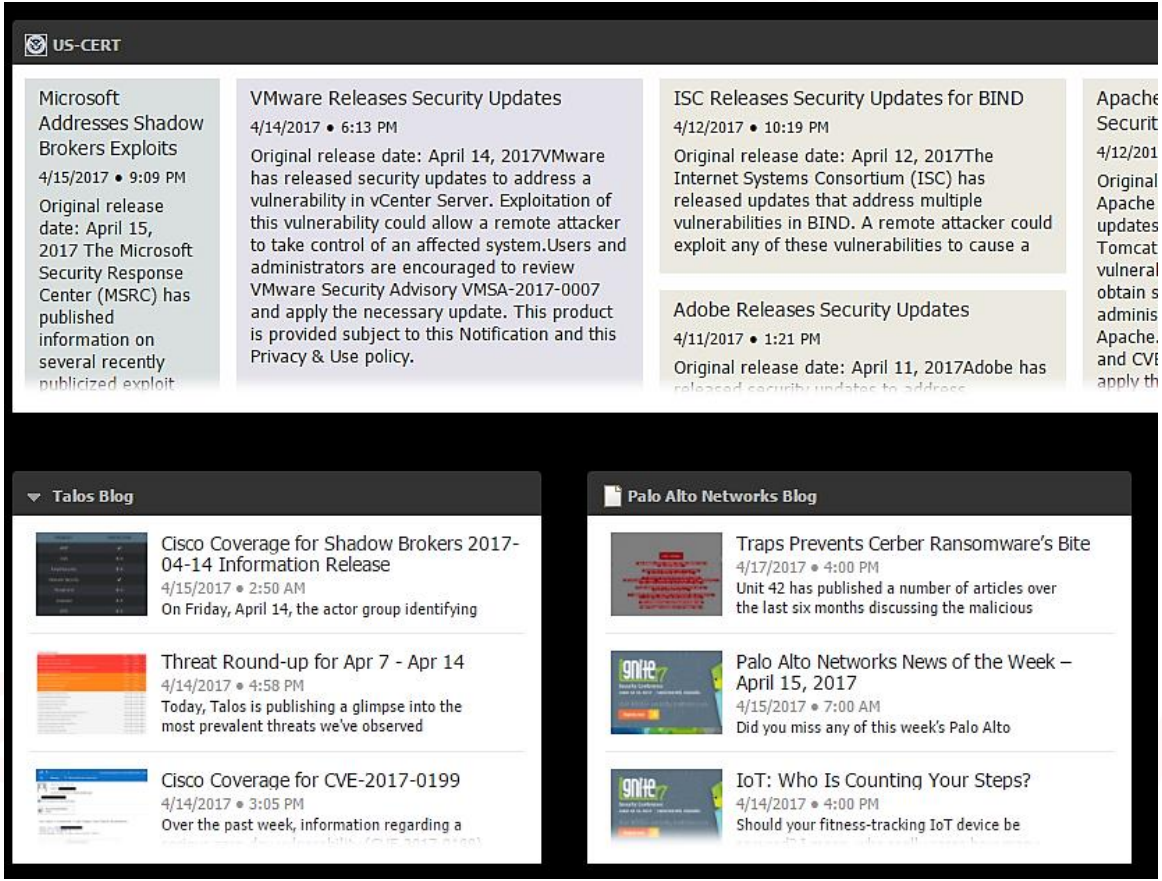
Other vendor's that are worth looking at for threat research are Trend Micro, FireEye and CrowdStrike which we already mentioned in the previous section.

The purpose of this module was to show the manual effort a threat hunter will take to find threat intelligence and to illustrate that utilizing only 1 or 2 vendor's is not enough.

As you can see this can be a time consuming and daunting task, especially with more vendor's entering into this sphere.

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

3.3 Threat Intelligence Research



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

This will allows us to be in the constant know as threat intelligence is made available.

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.

ISACs

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

ISACs

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

US-CERT

United States Computer Emergency Readiness Team (US-CERT) strives for a safer, stronger Internet for all Americans by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners around the world.

You can view website, here.

3.4 Threat Sharing and Exchanges

MAP REF

US-CERT

Apple Releases Security Updates

Published Wednesday, December 6, 2017

Apple has released security updates to address vulnerabilities in multiple products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system.

US-CERT encourages users and administrators to review Apple security pages for the following products and apply the necessary updates:

Read Full Entry »

Google Releases Security Update for Chrome

Published Wednesday, December 6, 2017

Google has released Chrome version 63.0.3239.84 for Windows, Mac, and Linux. This version addresses vulnerabilities that an attacker could exploit to take control of an affected system.

US-CERT encourages users and administrators to review the Chrome Releases page and apply the necessary update.

Read Full Entry »

Announcements

Securing the Internet of Things

The Internet of Things is becoming an important part of everyday life. Being aware of the associated risks is a key part of keeping your information and devices secure.

HIDDEN COBRA - North Korean Malicious Cyber Activity

On November 14, 2017, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) provided technical details on the tools and infrastructure used by cyber actors of the North Korean government. The U.S. Government refers to the malicious cyber activity by the North Korean government as HIDDEN COBRA.

For more information, visit https://www.us-cert.gov/HiddenCobra.

Federal Incident Notification Guidelines

As of April 1, 2017, all federal Executive Branch civilian agencies are required to use the revised Federal Incident Notification Guidelines. Major changes include an updated reporting requirement to include potentially impactful incidents, a new system for assessing impact and severity and the incorporation of guidance for reporting major incidents in accordance with OMB memoranda.

More Announcements »

3.4 Threat Sharing and Exchanges

MAP REF

Many countries have similar teams, you may check others for similar information pertaining to threat sharing.

For example within the course we shared a paper from the Japanese Computer Emergency Response Team (JP-CERT).

DHS/CISCP

The Department of Homeland Security has the **Cyber Information Sharing and Collaboration Program (CISCP).**

You can view the website for this program, here.

You also see they have several other information sharing programs listed such as **Automated Indicator Sharing (AIS)** and a link to **Information Sharing and Analysis Organizations (ISAO)**.

Open Threat Exchange

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 and starting view threat intelligence right away.

Open Threat Exchange

Open Threat Exchange and IOCs

Threat Connect

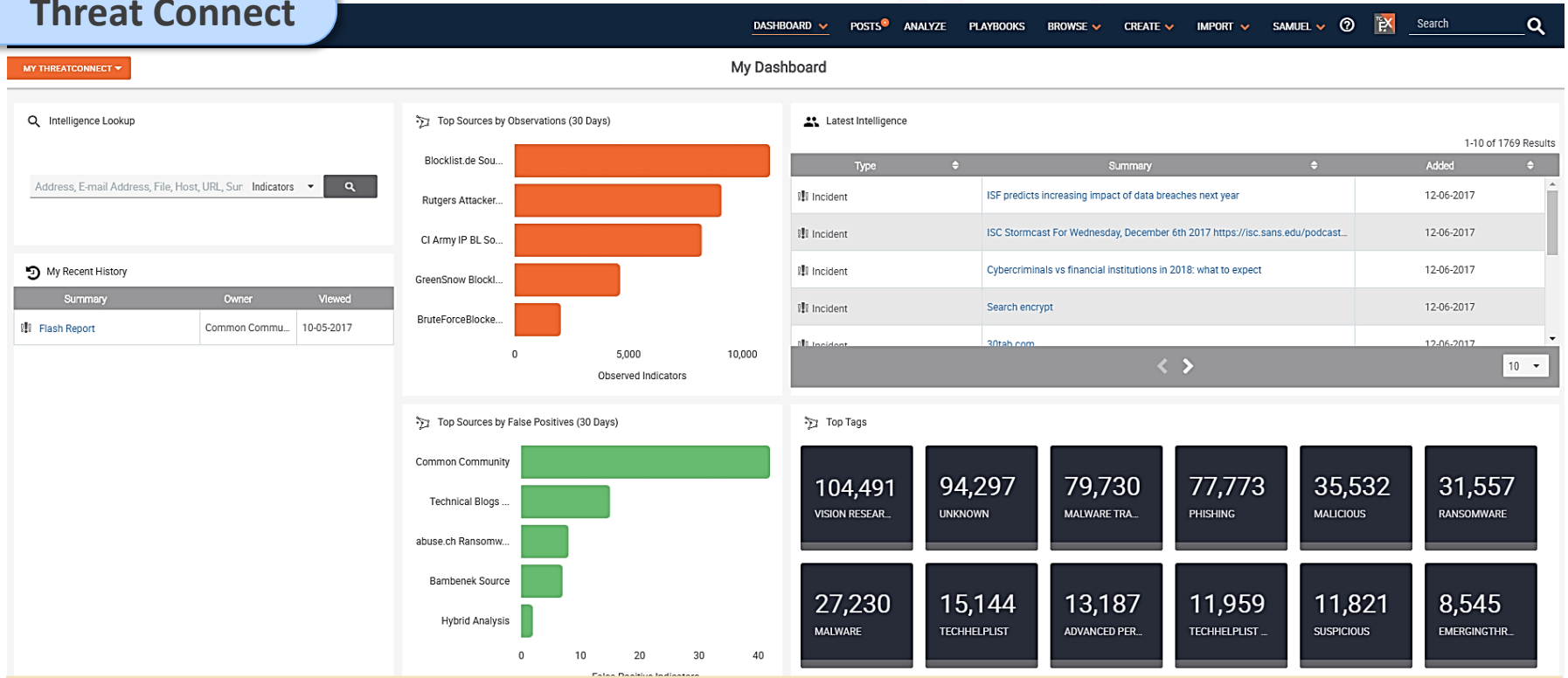
Threat Connect is another platform, similar to OTX, where you can obtain threat intelligence freely. You can also create an account and join right away to start sifting through threat intel.

You can join Threat Connect, here.

3.4 Threat Sharing and Exchanges

MAP REF

Threat Connect

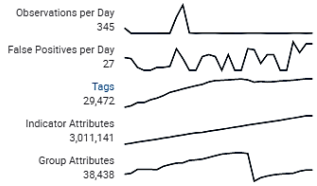


3.4 Threat Sharing and Exchanges

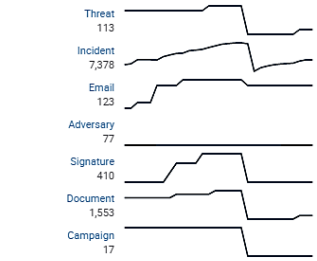
MAP REF

Threat Connect

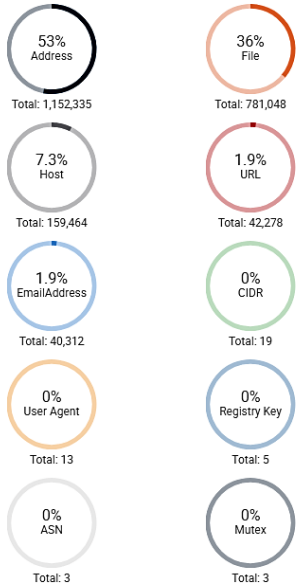
Observations & False Positives (Past Month)



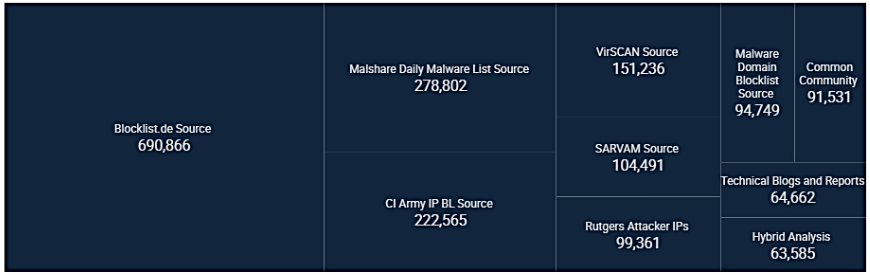
Groups (Past 30 Days)



Indicator Breakdown



Top 10 Largest Intelligence Sources



My Open Tasks

No Results

Summary	Owner	Due Date
No records found		

All Open Tasks

No Results

Summary	Owner	Due Date
No records found		

MISP

The **Malware Information Sharing Platform (MISP)** is free open source software helping information sharing of threat intelligence including indicators.

A threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

You can visit the MISP Project, here.

CRIT

CRITs (Collaborative Research Into Threats) is an open source malware and threat repository that leverages other open source software to create a unified tool for defenders engaged in threat defense.

You can visit CRITs, here.

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.”

3.5 Indicators of Compromise

Indicators of compromise aid information security and IT professionals in detecting data breaches, malware infections, or 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.

When we obtain IOCs from ISACs, threat sharing platforms, etc. we need to obtain the IOC in the format that our tools will accept.

For instance OTX allows us to download IOCs in the OpenIOC format.

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

In the next few slides we'll see the different IOC standards that exist and where you can find more information about these various standards.

STIX

STIX or **Structured Threat Information eXpression** is a structure language and serialization format used to exchange cyber threat intelligence.

At the time of this writing version 2.0 is the current version.

TAXII

Trusted Automated Exchange of Intelligence Information (TAXII) is an application layer protocol for the communication of cyber threat information in a simple and scalable manner.

TAXII is specifically designed to support the exchange of CTI represented in STIX.

STIX and TAXII have been integrated in STIX 2.0.

You can read about both, STIX and TAXII, on the OASIS Cyber

Threat Intelligence Committee's GitHub page, here.

CybOX

At the time of this writing, **CybOX (Cyber Observable eXpression)** has been integrated into STIX 2.0 as well.

You can read more information about this here.

OpenIOC

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

OpenIOC was developed by FireEye and it dates back to 2013, according to the blog post, here.

As of this writing the OpenIOC website (openioc.org) now redirects to FireEye's website, here, where you can download tools, of which contains free tools specific to IOCs.

IOC tools (Indicator of Compromise)

IOC Editor

IOC Editor is a free tool that provides an interface for managing data.

Learn more

IOC Finder

IOC Finder is a free tool for collecting host system data and reporting the presence of IOCs.

Learn more

IOC Writer

IOC Writer provide a python library that allows for basic creation and editing of OpenIOC objects.

Learn more

IOC Editor

IOC Editor is a tool that we'll look at within this course, which is from FireEye.

IOC Editor is a free tool that provides an interface for managing data and manipulating the logical structures of IOCs.

IOC Editor

IOCs are XML documents that help incident responders capture diverse information about threats, including attributes of malicious files, characteristics of registry changes and artifacts in memory.

You can download the tool here.

3.5 IOC & IOC Editor Video

Creating IOCs with IOC Editor

Redline

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

We will look at Redline more extensively when performing memory analysis but for now we'll use the tool to search for IOCs on a machine.

Redline

Redline is able to 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 view more information about the tool and download the tool here.

Redline and IOCs

YARA

Lastly, in this section we'll briefly 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.

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.

Yara and Yara Rules

Hunting with IOCs

This concludes the module on Threat Intelligence.

We have covered:

- ✓ Manually gather threat intelligence from multiple entities
  - 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
- ✓ We also covered IOC formats and tool for creating/editing IOCs

References

References

FireEye Threat Intel Reports

FireEye - FIN6 Report

FireEye - Reports by Industry

Veris Framework

FireEye - APT28 Report

M-Trends 2017

Verizon 2016 Report

TrustWave 2016 Report

References

CVE.MITRE.ORG

ENISA Threat Report

CrowdStrike 2016 Report

Palo Alto – Unit 42

Palo Alto – Application Usage and Threat Report

Cylance Blog

Operation Dust Storm

Operation Cleaver

References


GhostAdmin Malware


Talos - Threat Round-up


Trend Micro TrendLabs


US-CERT


Talos


The Callisto Group


National ISACs


CISCP

References

Open Threat Exchange

Threat Connect

MISP Project

CRITs

Digital Guardian (blog)

STIX & TAXII

CybOX

OpenIOC

References

- FireEye Freeware
- IOC Editor
- Redline
- Yara