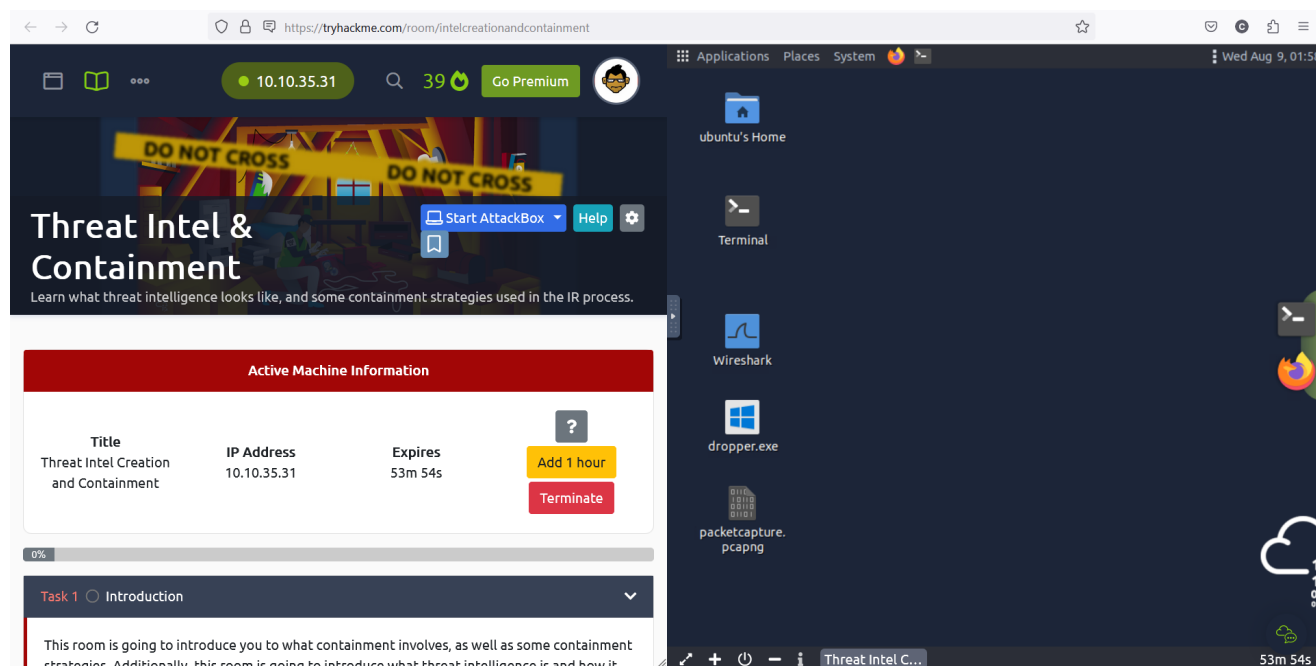


Threat Intel & Containment

09082023Wed

[TryHackMe | Threat Intel & Containment](https://tryhackme.com/room/intelcreationandcontainment)

Learn what threat intelligence looks like, and some containment strategies used in the IR process.



<https://tryhackme.com/room/mitre>

<https://tryhackme.com/room/introtosiem>

<https://www.elastic.co/beats/packetbeat>

<https://tryhackme.com/room/wazuhct>

<https://osint.digitalside.it/>

<https://otx.alienvault.com/>

<https://threatfeeds.io/>

<https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>

<https://www.ncsc.gov.uk/collection/incident-management>

<https://www.sans.org/media/score/504-incident-response-cycle.pdf>

url.full: Descending	Count
http://3.250.38.141/	3
http://3.250.38.141/dropper.exe	1
http://3.250.38.141/favicon.ico	1
http://edge-http.microsoft.com/captiveportal/generate_204	1
http://www.talonix.com/	1

```
Get-FileHash dropper.exe
```

```
sha256sum dropper.exe
```

```
463f1b1e11d4ca4c7a0c9aac540513ff7e681d9e5144bda2af24b86e438d3f4f dropper.exe
```

With this information, we can identify the workstation that has potentially been compromised. We can then further analyse this system to gather further evidence for containment. To illustrate, we can gather the hash of this downloaded file.

Getting the hash of the downloaded executable (Windows)

```
PS C:\Users\MichaelAscot\Downloads> Get-FileHash dropper.exe
```

Algorithm	Hash
Path	
SHA256	848DE632C5BFD2A7FF84E579E6F7561543CA0AAD6D8E7275DAE5926BA4F561C1

C:\Users\MichaelAscot\Downlo...

Getting the hash of the downloaded executable (Linux)

```
ubuntu@tryhackme:~$ sha256sum dropper.exe
848DE632C5BFD2A7FF84E579E6F7561543CA0AAD6D8E7275DAE5926BA4F561C1
dropper.exe
```

With this evidence, we now know that any host with this file is presumed to be infected. We can start creating detection alerts for this file's presence or the attacker's IP address. For example, using a SIEM such as [Wazuh](#) to check for the presence of this file on any device.

Assembling threat intelligence like this is paramount to the pre-containment stage because it allows us to link activity to any previous campaigns or attribute new behaviours to a threat actor.

```
ubuntu@thm-threatintel: ~/Desktop
File Edit View Search Terminal Help
ubuntu@thm-threatintel:~/Desktop$ ls
dropper.exe  mate-terminal.desktop  packetcapture.pcapng  wireshark.desktop
ubuntu@thm-threatintel:~/Desktop$ sha256sum dropper.exe
463f1b1e11d4ca4c7a0c9aac540513ff7e681d9e5144bda2af24b86e438d3f4f dropper.exe
ubuntu@thm-threatintel:~/Desktop$
```

10082023Thu

https://vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=TryHackMe!&proxyIP=10.10.84.207&resize=remote

packetcapture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 44

No.	Time	Source	Destination	Protocol	Length	Info
7608	34.199217	172.16.1.151	3.250.38.141	HTTP	581	GET /dropper.exe HTTP/1.1
7610	34.199547	3.250.38.141	172.16.1.151	HTTP	244	HTTP/1.1 304 Not Modified
7600	34.141855	172.16.1.151	3.250.38.141	TCP	66	58668 → 80 [SYN, ECN, CWR] Seq=0 Win=64240 Len=0 MSS=1460 WS=...
7601	34.142116	3.250.38.141	172.16.1.151	TCP	66	80 → 58668 [SYN, ACK] Seq=0 Ack=1 Win=62727 Len=0 MSS=1460 SA=...
7602	34.142172	172.16.1.151	3.250.38.141	TCP	54	58668 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
7609	34.190461	3.250.38.141	172.16.1.151	TCP	60	80 → 58668 [ACK] Seq=1 Ack=528 Win=62208 Len=0
7611	34.201004	172.16.1.151	3.250.38.141	TCP	54	58668 → 80 [ACK] Seq=528 Ack=191 Win=2102016 Len=0
7943	37.658334	172.16.1.151	3.250.38.141	TCP	54	58668 → 80 [FIN, ACK] Seq=528 Ack=191 Win=2102016 Len=0
7948	37.658649	3.250.38.141	172.16.1.151	TCP	60	80 → 58668 [FIN, ACK] Seq=191 Ack=529 Win=62208 Len=0

Flags: 0x4000, Don't fragment
 Fragment offset: 0
 Time to live: 128
 Protocol: TCP (6)
 Header checksum: 0x0000 [validation disabled]
 [Header checksum status: Unverified]
 Source: 172.16.1.151
 Destination: 3.250.38.141

Transmission Control Protocol, Src Port: 58668, Dst Port: 80, Seq: 1, Ack: 1, Len: 527

Hypertext Transfer Protocol

0010 02 37 08 2e 40 00 00 06 00 00 ac 10 01 97 03 fa - 7 . @
 0020 70 06 e5 2c 00 50 4c 9d 79 fc 0f 3f e5 82 50 18 4 , P L y : 7 - P
 0030 20 14 da 57 00 00 47 45 54 20 2f 64 72 6f 70 70 - W - G E T / dropp
 0040 65 72 2e 65 78 65 20 48 54 54 50 2f 31 2e 31 0d er . exe H T T P / 1 . 1
 0050 0a 48 6f 73 74 3a 20 33 2e 32 35 30 2e 33 38 2e Host : 3 . 250 . 38 .
 0060 31 34 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 141 . Con nection :
 0070 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 keep - a l i v e - Upg
 0080 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 65 rade - Ins e cure - Re
 0090 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 72 2d quests : 1 - User -
 00a0 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 Agent : M ozilla / 5

Destination (ip.dst), 4 byte(s) Packets: 10645 · Displayed: 10 (0.1%) Profile: Default

https://tryhackme.com/room/intelcreationandcontainment

Try Hack Me Dashboard Learn Compete Other 10.10.84.207 41 Go Premium

Threat Intel & Containment

Learn what threat intelligence looks like, and some containment strategies used in the IR process.

101

Start AttackBox Show Split View Help

Active Machine Information

Title	IP Address	Expires	
Threat Intel Creation and Containment	10.10.84.207	27m 56s	? Add 1 hour Terminate

100%

Task 1 Introduction

Task 2 Pre-Containment

Task 3 Containment Strategies