Threat Intel and Containment

Introduction

This room is going to introduce you to what containment involves, as well as some containment strategies. Additionally, this room is going to introduce what threat intelligence is and how it can be used to understand our adversary.

You will use some of the Indicators Of Attack (IOA) & Indicators Of Compromise (IOC) from the module in the practical element of this room to analyse some threat intelligence.

Containment is a crucial phase in incidence response because the core aim is to minimise the damage caused by an incident and prevent further damage. For example, we can prevent our adversary from accessing other devices by containing infected devices. - containment is a fantastic way to preserve and record evidence that can be used in forensic analysis.

Effective containment is essential in restoring normal operations. Once a threat has been successfully contained, normal day-to-day operations can continue.

Threat intelligence, briefly, is the knowledge gained from collecting and analyzing intelligence about a threat actor. Intelligence such as IP addresses can be used to identify a specific threat actor or, for example, analyse their tactics, techniques, and procedures (TTPs). More on this later.

Learning Objectives:

By the end of the room, you should be able to:

- Recognise potential threat intelligence.
- Analyse threat intelligence to understand how an adversary operates.
- Understand what containment involves and some of the approaches that can be taken with their pros and cons.

Room Prerequisites

This room expects you to have:

- At least an understanding that the ATT&CK framework exists.
- Familiarity with IP addresses. I.e., knowing what an IP address (private and public) looks like.

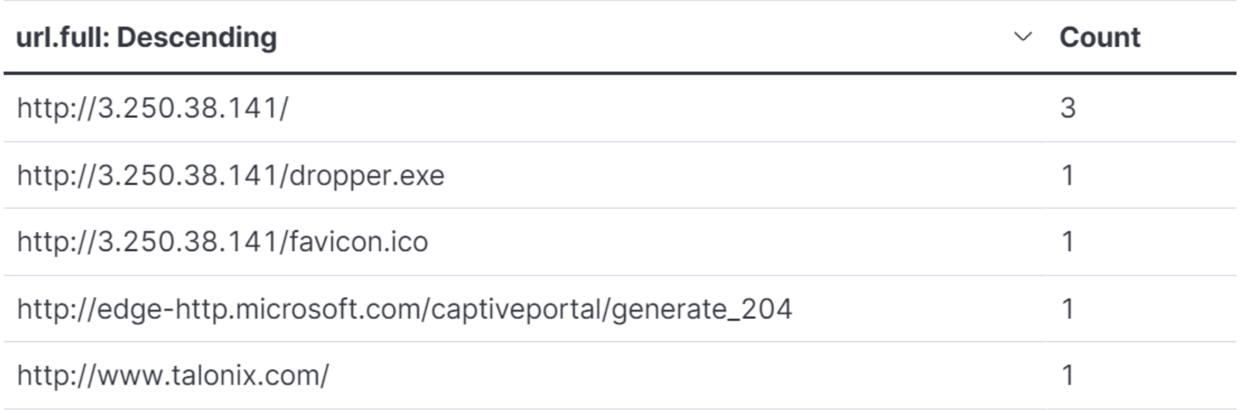
- At least an awareness of adversary techniques, i.e. persistence, lateral movement, etc.
- Be capable of identifying what a hash looks like - I highly recommend checking out the Preparation room that is a part of this module.

Pre-Containment

This stage of the process focuses on the steps necessary to prevent an incident from having further impact.

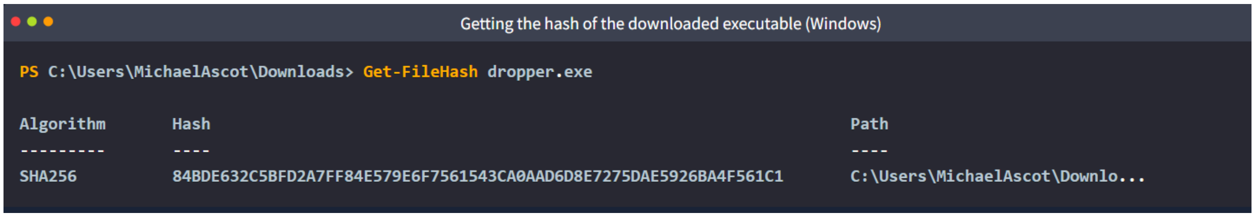
You will be looking to gather as much information as possible about the incident and the adversary. For example, collecting evidence from infrastructure such as Intrusion Detection Systems (IDS) and Security and Information Management Systems (SIEMS). This evidence will form Indicators of Compromise (IOCs).

We can begin looking at our perimeter defence systems for this information. For example, looking at our setup of ELK with packetbeat, we can see that a workstation has downloaded an executable. Perhaps a user has clicked on a malicious 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

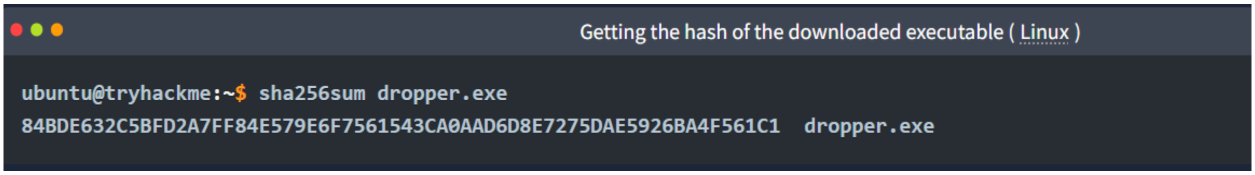
With this information, we can identify the workstation that has potentially been compromised. We can then further analyse this system to gather further evidence for containment. To illustrate, we can gather the hash of this downloaded file.



Getting the hash of the downloaded executable (Windows)

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

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          84BDE632C5BFD2A7FF84E579E6F7561543CA0AAD6D8E7275DAE5926BA4F561C1       C:\Users\MichaelAscot\Downlo...
```



Getting the hash of the downloaded executable (Linux)

```
ubuntu@tryhackme:~$ sha256sum dropper.exe
84BDE632C5BFD2A7FF84E579E6F7561543CA0AAD6D8E7275DAE5926BA4F561C1   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.

****

Answer the questions below:

What does the acronym IDS mean?
Answer: Intrusion Detection System

Containment Strategies

There are a few containment strategies to consider when actioning the containment phase of the incidence response. It is important to consider what strategy is suitable as they all have their pros and cons.

Containment can be considered as the bridge between the identification, scoping and eradication, and recovery phases of the incidence response process.

Isolation

Entire isolation is considered to be a pretty aggressive - but effective - strategy. This strategy involves the incidence response team completely isolating the infected device(s). This can be through network segmentation or physical.

As previously stated, this is pretty aggressive and is noticeable from the adversary. For example, they might realise they can no longer access the infected device(s) and have been discovered. Once an adversary notices this, they may rush to complete their action on objectives. Alternatively, they may change their focus to a compromised system that hasn't been noticed yet.

For the sake of this room, action on objectives is the adversary achieving what they initially set out to do. This could be stealing data, or causing maximum damage to the organisation (i.e. start deleting files or damaging systems), to name a few.

When choosing this strategy, you should consider the following:

- How aggressive do you want the isolation to be?
- Is the adversary likely to rush their action on objectives? Threat intelligence can be used to help determine this.
- Do we understand the adversary enough yet? Perhaps controlled isolation would be more useful here if we do not.

Controlled Isolation

Controlled isolation is a less aggressive strategy in containment. Although, it isn't entirely risk-free.

This strategy involves the incidence response team closely monitoring the adversary's actions. Rather than strictly isolating the infected system(s), the team would keep the system accessible to not tip off the adversary.

An incident response team can gather vital information and intelligence about the adversary by allowing the adversary to continue.

However, the adversary isn't given free-roam. For example, the incident response team can prevent access if the adversary is about to perform something destructive such as wiping or exfilling data. A good "cover story" can be made to convince the adversary why they've suddenly lost access. For example, an announcement could be made that routine maintenance is occurring.

The ultimate aim is to understand our adversaries here without tipping them off to the fact that they are being monitored. Ultimately, it's a "cat and mouse" game between the incident response team and the adversary.

When choosing this strategy, you should consider the following:

- What is the risk of allowing the adversary to continue?
- Do we know enough about the adversary already?
- If so, perhaps full-on isolation would be best.
- Do we have the appropriate means to stop an adversary before they do something destructive? Can we allocate the resources and human power to closely and constantly monitor the adversary?

Linking Together

The threat intelligence and containment strategies bridge the gap between the incident response process's identification, scoping, eradication, and recovery phases. Furthermore, with good threat intelligence, we have good identification. Threat intelligence is an ever-going process, as you will come to discover in later tasks.

****

Answer the questions below:

What is the name of the containment strategy used when the responders closely monitor the adversary?

Answer: Controlled Isolation

What containment strategy is considered to be the most aggressive?

Answer: Entire Isolation

Creating Threat Intelligence

It is important to understand what threat intelligence looks like. Threat intelligence is anything that can be attributed to a malicious actor. Some common forms of threat intelligence include:

- IP Addresses
- File Hashes
- Domains
- File Names (I.e. toolkits)
- Patterns, activity or techniques of known threat campaigns (TTPs)

Tactics Techniques Procedures (TTPs)

These three ingredients are used to describe the aims, techniques and methods of a threat actor. These are extremely important in understanding how the threat actor operates. For example, what toolkits do they use? What are the threat actor's objectives? Are they trying to steal data or trying to cause damage to the organisation? Is there a criminal or political reason behind their attack?

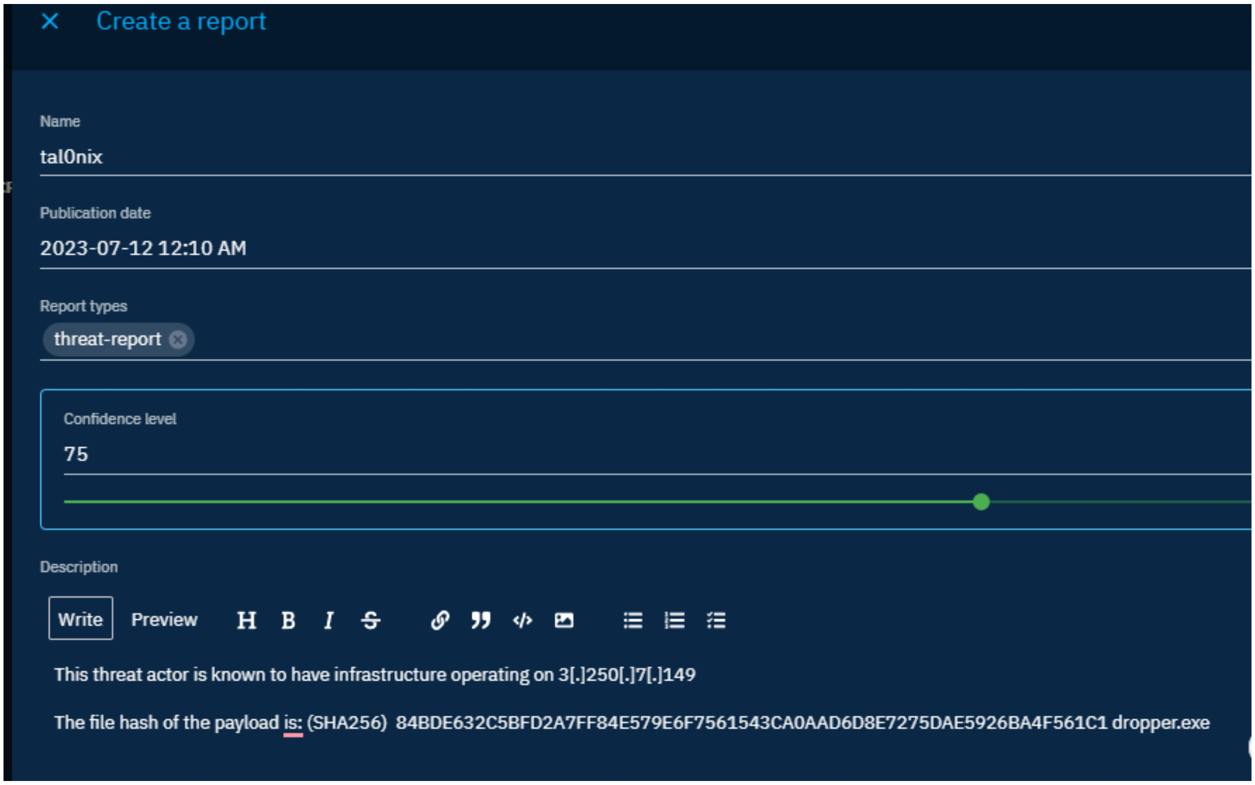
I've broken down the three ingredients below:

- Tactics: This ingredient is the high-level objectives that the threat actor aims to achieve. For example, are they trying to steal data or corporate secrets? Perhaps they're trying to blackmail the organisation or are attacking for bragging rights.
- Techniques: This ingredient is the specific tools or methods the threat actor employs to achieve their tactics. For example, how did the adversary gain entry? Phishing? Are they targeting any specific software or service? What methods are the adversary using to privilege escalate or laterally move across the network?
- Procedures: This ingredient looks at the attack chain used by the adversary. For example, what is the entire process from initial access to action on objectives? To illustrate, a procedure could be phishing -> credential stealing -> accessing a privileged user account -> laterally moving -> stealing sensitive information.

By understanding the TTPs of a threat actor, we can tailor our response to the cyber threat. We can also build a picture of how the threat actor behaves.

Threat Intelligence Platforms

Multiple threat intelligence platforms are available that aid in distributing threat intelligence. For example, OpenCTI is a framework that allows the collaborative sharing of threat intelligence. In this scenario, we can see the generated report for the tal0nix adversary in the OpenCTI framework.



Name: tal0nix

Publication date: 2023-07-12 12:10 AM

Report types: threat-report

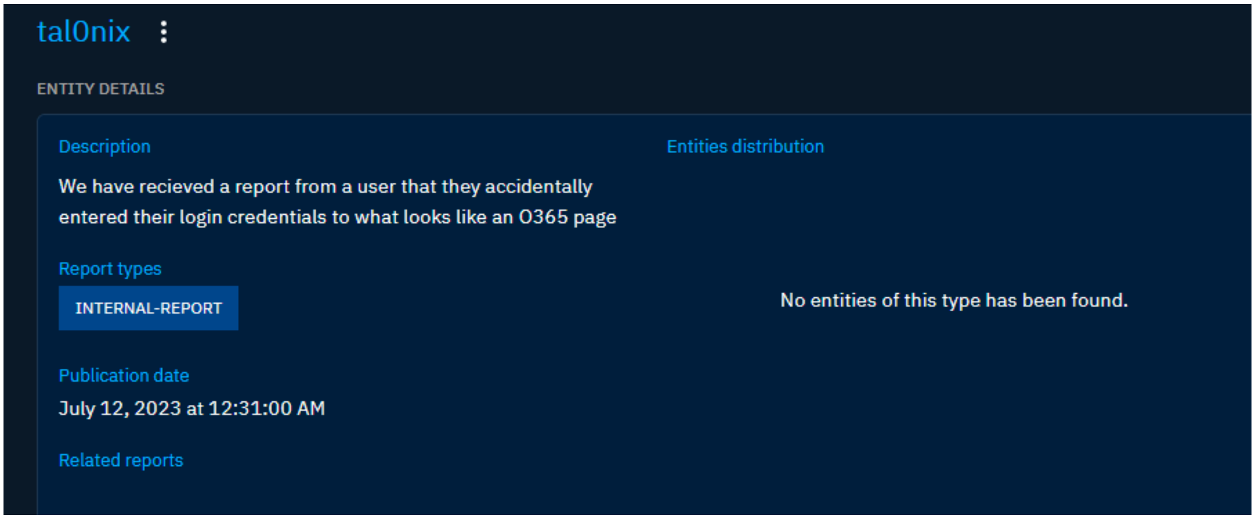
Confidence level: 75

Description

This threat actor is known to have infrastructure operating on 3[.]250[.]7[.]149

The file hash of the payload is: (SHA256) 84BDE632C5BFD2A7FF84E579E6F7561543CA0AAD6D8E7275DAE5926BA4F561C1 dropper.exe

Analysts will be able to link up this report with another entry, whereas a user has reported accidentally entering their Office 365 credentials on a phishing page:



tal0nix

ENTITY DETAILS

Description

We have recieved a report from a user that they accidentally entered their login credentials to what looks like an O365 page

Report types

INTERNAL-REPORT

Publication date

July 12, 2023 at 12:31:00 AM

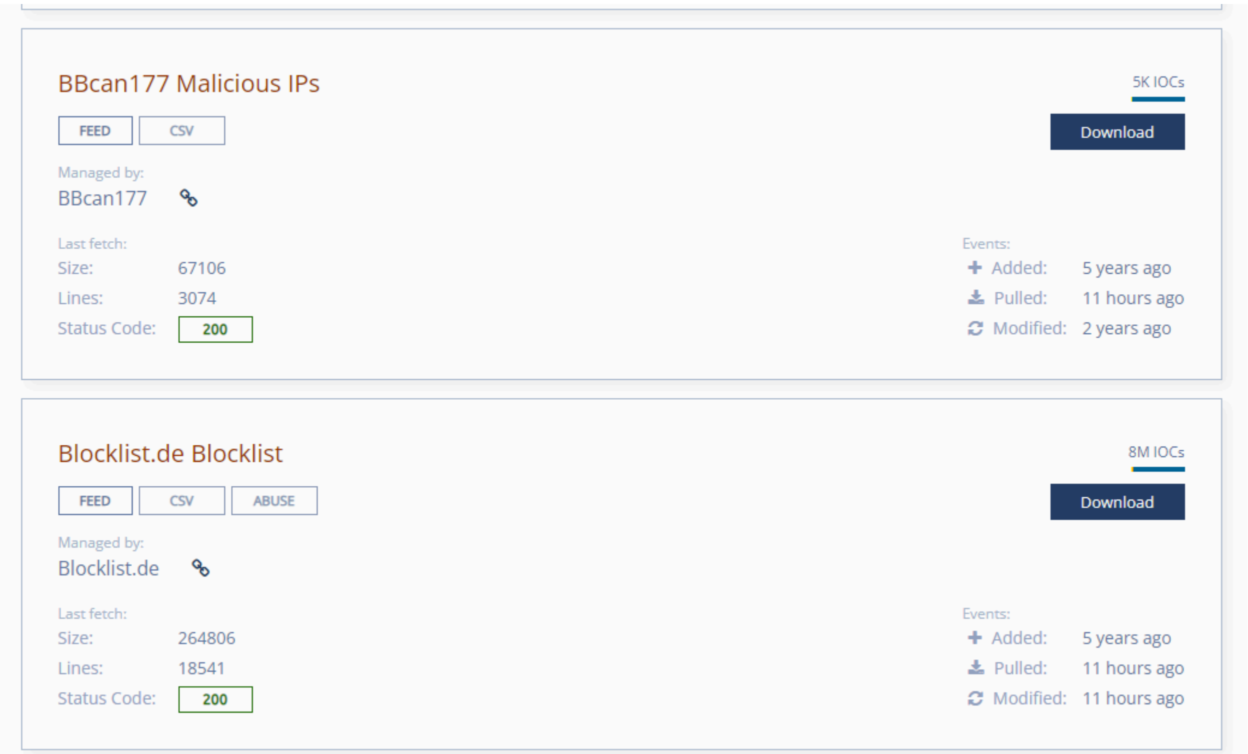
Related reports

Entities distribution

No entities of this type has been found.

Staying in the loop and subscribing to community threat intelligence feeds such [DigitalSide Threat Intel](), [AlienVault](), and [threatfeeds.io]() is extremely important. It allows you, as a responder, to use the history of the threat actor to predict future behaviour potentially. If you are able to understand where the adversary might go next, you can begin to implement the necessary containment measures to prevent the threat actor from proceeding.

Of course, using public threat intelligence feeds such as those listed previously in this task, you can arm your SIEM with the necessary alerts before the incident occurs, as seen in the screenshot below.



BBcan177 Malicious IPs

Managed by: BBcan177

Last fetch:

Size: 67106

Lines: 3074

Status Code: 200

Events:

Added: 5 years ago

Pulled: 11 hours ago

Modified: 2 years ago

Blocklist.de Blocklist

Managed by: Blocklist.de

Last fetch:

Size: 264806

Lines: 18541

Status Code: 200

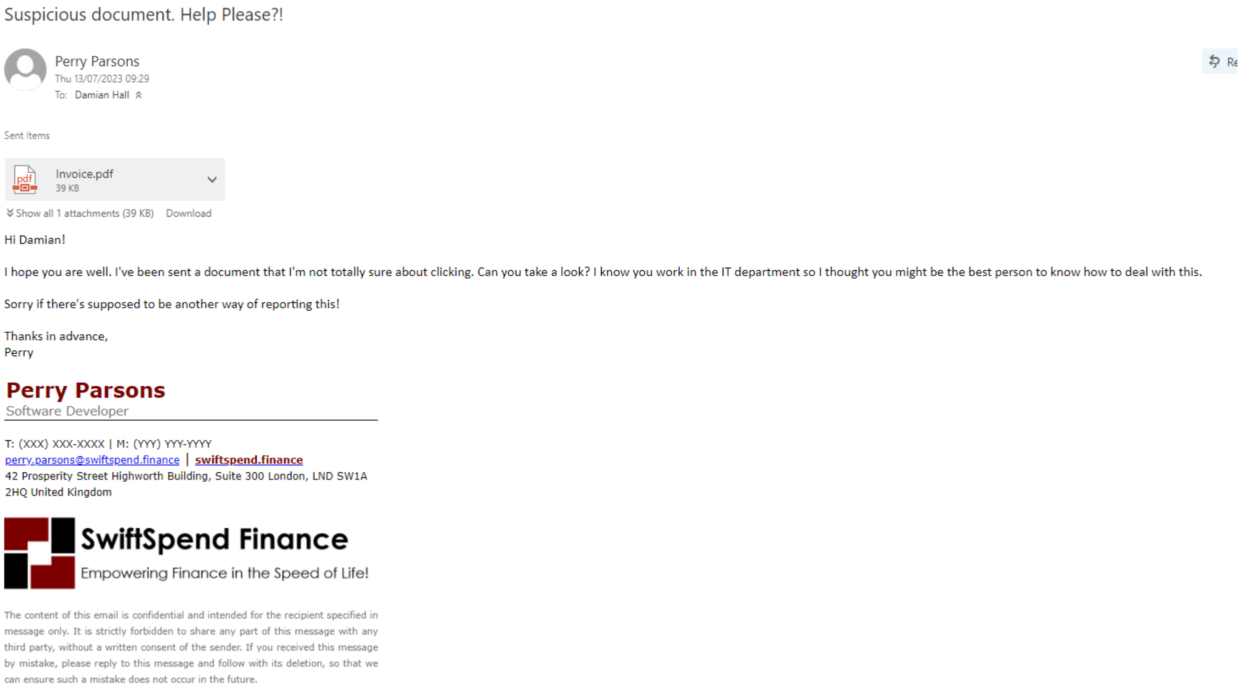
Events:

Added: 5 years ago

Pulled: 11 hours ago

Modified: 11 hours ago

Additionally, there should be appropriate channels for users within an organisation to report suspicious e-mails or documents. For example, Perry at SwiftSpend Finance sent an IT colleague a potentially malicious e-mail (screenshot below). This is not a good process because no clear avenue exists for reporting suspicious attachments. Perry, in this case, just chose Damian because he works with computers. And, of course, by re-attaching the PDF to the e-mail to Damian, Perry has just (unknowingly and with good intentions!) furthered the risk in the organisation.



Suspicious document. Help Please?!

Perry Parsons
Thu 13/07/2023 09:29
To: Damian Hall

Hi Damian!

I hope you are well. I've been sent a document that I'm not totally sure about clicking. Can you take a look? I know you work in the IT department so I thought you might be the best person to know how to deal with this.

Sorry if there's supposed to be another way of reporting this!

Thanks in advance,
Perry

Perry Parsons
Software Developer

T: (XXX) XXX-XXXX | M: (YYY) YYY-YYYY
perry.parsons@swiftspend.finance | **swiftspend.finance**
42 Prosperity Street Highworth Building, Suite 300 London, LND SW1A
2HQ United Kingdom

SwiftSpend Finance
Empowering Finance in the Speed of Life!

The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

****

Answer the questions below:

What is the term for a set of characters that can be used to give an attribution to a file?
Note: The answer is expecting the singular noun of this term.
Answer: hash

Threat Intelligence Creation Feedback Loop

I want to emphasise how threat intelligence is essential in driving the identification, scoping, and containment phases. For example, threat intelligence can be used to understand the adversary. Is the adversary an Advanced Persistent Threat (APT)? IP addresses or filenames can be used to determine this.

If the adversary is known, perhaps we can understand their potential action on objectives or methodology from published reports, etc.

It's important to remember that the end goal of containment is to make it difficult for the adversary to achieve their goals. It can be considered as "buying time" for the incident response team.

Of course, there's a tricky balance between "collecting all of the intelligence" and giving the adversary enough time to complete their goal. Understanding the adversary quickly will allow us to make an effective containment strategy. Can we understand the adversary enough to predict where they're going next? If so, then we can secure those systems ahead of time.

Whack-a-mole
It is understandable why an organisation may want to eradicate the adversary immediately. However, without adequately scoping and creating threat intelligence with an effective containment strategy, we may miss exactly how truly compromised we are.

Without understanding what systems are compromised, we risk being complacent. For example, backing up and restoring a compromised system and calling it a day (thinking that is it) may lead to us allowing the adversary to harbour on other systems.

Building a better understanding of the adversary leads to a better incident scope. In turn, better scope of the incident means creating a more intelligent and effective containment strategy, ultimately leading to more control over the adversary.

Positive Feedback Loops
The pre-containment and threat intelligence creation stages of the IR process play an essential role in later stages of the IR process (such as recovery and lessons learned). Furthermore, when looking back at the incident, we can determine if our current setup was sufficient for the incident. Did we miss anything? Perhaps we could track the adversary in our network, but there was too much noise in the SIEM that made it difficult to analyse on a real-time basis.

Could any lessons be learnt to prevent the breach in the future? Collecting threat intelligence is an ongoing process for a defensive team.

****

Answer the questions below:

What is the name of the classic arcade game that has been referenced in this task?
Answer: Whack-a-mole

Practical

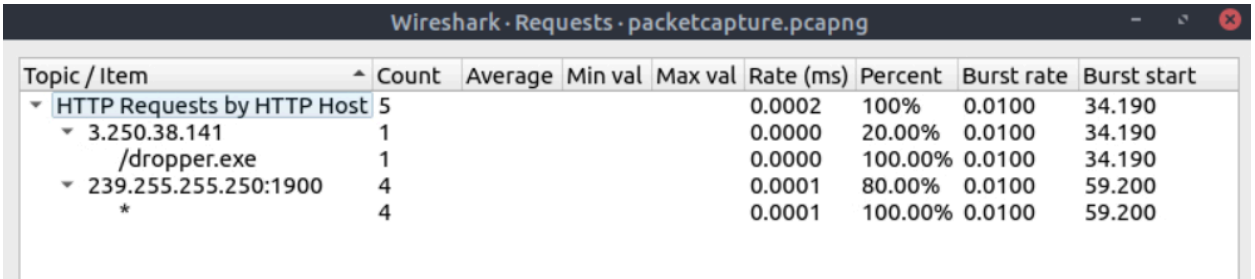
Deploy the machine attached to the task by clicking the green "Start Machine" button within this task. The machine will start in a split-screen view. In case the VM is not visible, use the blue Show Split View button at the top-right of the page.

A packet capture of the incident has been provided for you and is located on the Desktop. Your task is to analyse the packet capture for threat intelligence to solve the questions below.

****

Answer the questions below:

What is the IP address of the adversary?
Knowing that the adversary got a foothold through the user downloading a file I started by looking at the HTTP requests by host.

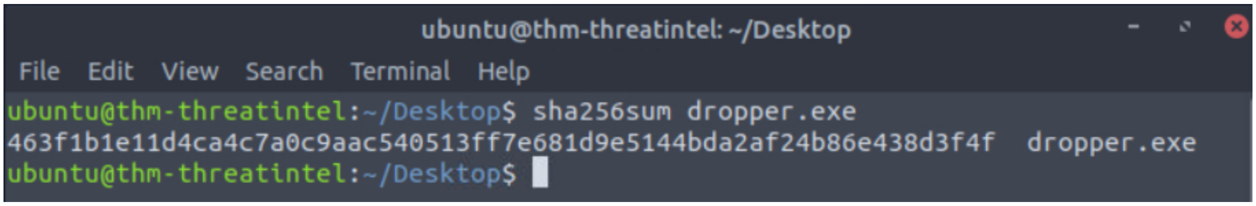


Topic / Item	Count	Average	Min val	Max val	Rate (ms)	Percent	Burst rate	Burst start
HTTP Requests by HTTP Host	5				0.0002	100%	0.0100	34.190
3.250.38.141	1				0.0000	20.00%	0.0100	34.190
/dropper.exe	1				0.0000	100.00%	0.0100	34.190
239.255.255.250:1900	4				0.0001	80.00%	0.0100	59.200
*	4				0.0001	100.00%	0.0100	59.200

We see that dropper.exe was downloaded from 3.250.38.141.
Answer: 3.250.38.141

What is the name of the file that gets downloaded from the adversary's infrastructure?
Answer: dropper.exe

What is the SHA-256 hash value of the value of the executable on the Desktop?


ubuntu@thm-threatintel: ~/Desktop
File Edit View Search Terminal Help

```
ubuntu@thm-threatintel:~/Desktop$ sha256sum dropper.exe
463f1b1e11d4ca4c7a0c9aac540513ff7e681d9e5144bda2af24b86e438d3f4f  dropper.exe
ubuntu@thm-threatintel:~/Desktop$ 
```

Answer: 463f1b1e11d4ca4c7a0c9aac540513ff7e681d9e5144bda2af24b86e438d3f4f

Conclusion

A Re-cap

Again, at the risk of repetition, I want to highlight just how important threat intelligence plays in the identification and scoping, and containment phases of incidence response.

Threat intelligence and containment is an ongoing evolving process. It is not simply done once, rather, it continues as the incident evolves.

Choosing the appropriate containment strategy is paramount. For example, if we are too aggressive, we're going to tip off the adversary and potentially rush them into performing more damaging actions. Or, for example, missing out on the chance to create important threat intelligence or forensic evidence.

Now that you have successfully gathered threat intelligence and implemented an effective containment strategy, you are now ready for the eradication, remediation, and recovery stages of the incident

Incident Response Frameworks and Guidelines

Of course, as is often the case with cyber security, frameworks for this process exist which outline the best practices. For example, the Computer Security Incident Handling Guide published by NIST, or the NCSC (UK GOV)'s Incident Management. Finally, the following cheat sheet published by SANS can be a helpful reminder in the incidence response cycle. It is worth checking out the aforementioned resources for additional reading.