DIGITAL FORENSIC INCIDENT RESPONSE - BRIEF WALKTHROUGH

By Chan YueMeng

CONTENTS

1. Introduction.
2. Verification
3. Infection Vector
4. Scope
5. Remediation
6. Containment
7. Lesson Learnt
8. Not Done Yet…

INTRODUCTION

Hi all. My name is Chan YueMeng and I currently work in a MNC as a Cyber Incident Response Analyst.

After coaching from my peers, seniors and good books regarding DFIR, I start to appreciate the value of performing DFIR when a cyber incident happens.

DFIR stands for Digital Forensics Incident Response.

Current practice of DFIR usually covers the verification, infection vector, scope, remediation and containment in the event of a malware infection incident.

This writeup covers partially on all of them where I will use a case scenario to briefly explain over them.

The information uncover could help to double check on the verification, determine the infection vector, expand the scope, take action on the right remediation as well as contained the incident.

Basically, when a malware infection incident occurs, I will go through below steps to gather my thoughts and findings

- How was it detected in the first place?

- How does the malware got in?

- How the malware remains persistently on the host?

- How does it spread?

- Is it contained?

- What kind of damage the malware have caused?

Please take note that the findings found from the collected artefacts in a malware infection incident are not suitable to be used in court especially where chain of custody is concern. There is usually another Forensic team handling court related cases and usually the DFIR folks and the Forensic folks work together when interesting artefacts are found on a compromise host

VERIFICATION

On a certain day, a DNS callout to a certain malicious domain was observed in the DNS log.

It was blocked on our network perimeter device and no suspicious network traffic was found prior to the DNS callout.

Further verification is preferable to ensure nothing was missed out on all the associated network logs

Follow by that, we need to turn our attention to host artefacts to verify what actually happen on the host that causes the callouts.

This has answer my first question on “How was it detected in the first place?”

Answer:

It was through DNS resolving.

INFECTION VECTOR

Retrieving the usual host artefacts which include the host master file table and the necessary registry files especially the user profile registry, I found strong evidence or indication that the malware was caused by a USB device.

On user profile registry, I manage to locate the persistence mechanism in one of the autostart location on the host.

On the master file table, I manage to correlate the time the malware artefact was created on the host against the time the first DNS callout was observed.

On the software hive (which is another registry), I locate the model of the USB device.

This has actually answer 3 of my questions on the following

- How does the malware got in?

- How the malware remains persistently on the host?

- How does it spread?

Answers:

It manage to get onto the host through USB device.

It has persistence capabilities and it reside in one of the autostart location

High possibility that it is spreadable through USB device

SCOPE

Since we know the USB device is the infection vector, we need to know the scope of the USB device usage as in how many users have actually share the USB device.

You might have asked it should be reflected in the DNS logs base on the source host making the requests.

But there might be a possibility that another user might have copy it out to the host but have not execute it yet.

Checking on the scope is important to ensure remediation and containment are being done as much as possible base on the variant of malware found on the first host (patient zero).

REMEDIATION

For remediation, it depends on the severity of the malware infection found on the host.

For some organisation, they prefer to reimage no matter how “minor” is the infection for example PUA infection (potentially unwanted application)

But again it depend on organisation because reimage always incur operation costs…

Last but not least, you might need to submit the malware found to whatever host protection mechanism you have in place such as your anti-virus vendor as it might not have the signature yet due to the different variant of the malware found.

CONTAINMENT

Sometimes, when we discover new IOC especially new network indicators after we run the malware in a analysis machine (provided we are able to trigger them), we will add them to be blocked by our network perimeter protection mechanism in place.

Sometimes there are additional indicators provided by threat intel company base on the similar malware variant they have analysed before.

For host protection mechanism, our submission to the AV vendor will ensure a signature is created for that malware variant and thus this helps us to further determine additional hosts housing the malware in the event if the infection vector is not by USB itself.

This has answer my question on “Is it contained?”

Answer:

Yes depending on the number of protection or alerting mechanism you have in placed

LESSON LEARNT

When a malware incident happen, base on the infection vector information we will advise the user on what causes the malware infection so that he/she will be aware whats going on and this helps to prevent similar incidents from happening.

The information collected will also help management to generate statistic report to help them on improving the security posture and control of the company.

The lesson learnt could be put to good use for us CIRT as well as we could prepare ourselves and armed with knowledge on how to handle them in the event if similar event happened in the near future.

NOT DONE YET…

The role of a CIRT is not done yet as the proactive approach needs to be kicked in as well.

Of course this is usually handle by a different team but it never hurts to learn more

Cool stuff like yara rule which is used to identify and classify the malware base on the textual or binary patterns helps CIRT to identify different variant of the same malware family as a first or fast triage.

In a proactive approach, you could make use of yara rules to hunt for similar variant in huge malware repository site like virustotal where you could further refine your yara rule and make use of them to scan (hunt) for similar malware not detected by your protection mechanism in place in your company.

Questions?

Email: chan.yuemeng@gmail.com

linkedin: https://sg.linkedin.com/in/chanyuemeng

twitter: https://twitter.com/chanyuemeng