

PHISHING EMAIL ANALYSIS

Malicious Link

Austin Lai

10/5/2022

Table of Contents

Executive Summary.....	2
Introduction	2
Analysis	3
Discovery and Initial Detection	3
Message header analysis of the email.....	3
In-depth analysis.....	3
Original email from sender	3
Malicious link from the email	3
Behavior of malicious link	3
Additional information.....	6
Cookies used in the malicious link to the page.....	6
Har file include all HTTP session request and response	6
Malicious excel file analysis	6
Report "W_256737973.xlsb" against VirusTotal	9
Execute malicious file "W_256737973.xlsb" on AnyRun.....	11
Conclusion.....	15

Executive Summary

This report aims to describe and analyse phishing emails with malicious link that recently occurred and discovered in the environment.

--- OMITTED ---

--- OMITTED ---

--- OMITTED ---

Lastly, we have performed full investigation and analyse of the email, malicious link and malicious file in an isolated and sandboxing environment using multiple tools (such as alert detail from --- OMITTED ---, email header, file command, AnyRun sandbox and VirusTotal).

Phishing email sent from --- OMITTED ---, the sender is not spoofed instead it is a legitimate email account; however, the email account might be compromised. Phishing email crafted with unique email subject title and contains unique malicious link. While investigated all the malicious link, it is redirect to download the same file which is "W_256737973.xlsb".

--- OMITTED ---

--- OMITTED ---

--- OMITTED ---

Phishing remains a popular method of stealing credentials, committing fraud, and distributing malware. The problem of phishing, types of message content of phishing emails, and the basic techniques of phishing email attacks are explained by way of introduction.

Introduction

Phishing emails are a type of targeted email attack where social engineers lure the recipient into performing specific actions such as clicking on a malicious link, opening a malicious attachment, or visiting a web page and entering their personal information. Phishing attacks seek to trick recipients into believing that an email is legitimate, in order to solicit sensitive information (e.g., usernames, passwords, and credit card numbers) or install malware. As a result, phishing is a fundamental component of many cyber-attacks and is often used as a first step in advanced persistent threats.

Phishers use many different techniques to initiate phishing attacks, the main methods used are email, SMS, social media, instant messaging, search engines and malicious websites. Phishers always modify their methods to use any communication method available to reach their victims. The spear phishing is a highly targeted of phishing attack. Rather than sending more phishing emails to anyone, the phisher sends spoofed emails to consumers that appear to originate from somebody they know.

Analysis

Discovery and Initial Detection

--- OMITTED ---

--- OMITTED ---

--- OMITTED ---

Message header analysis of the email

--- OMITTED ---

--- OMITTED ---

--- OMITTED ---

In-depth analysis

Original email from sender

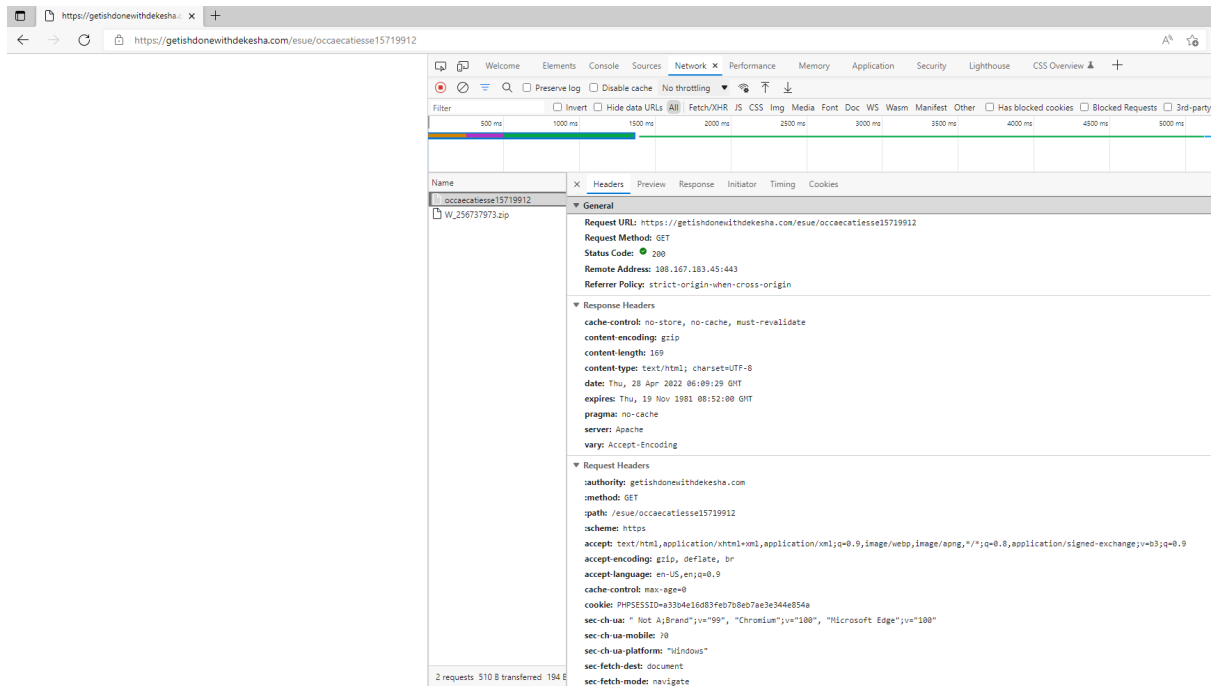
--- OMITTED ---

Malicious link from the email

Behavior of malicious link

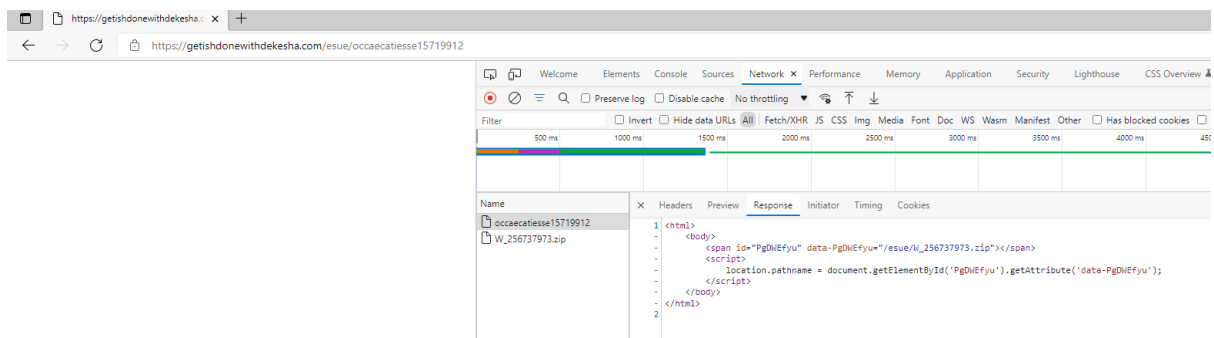
Any user clicked the link will open a blank page as of user view.

PHISHING EMAIL ANALYSIS



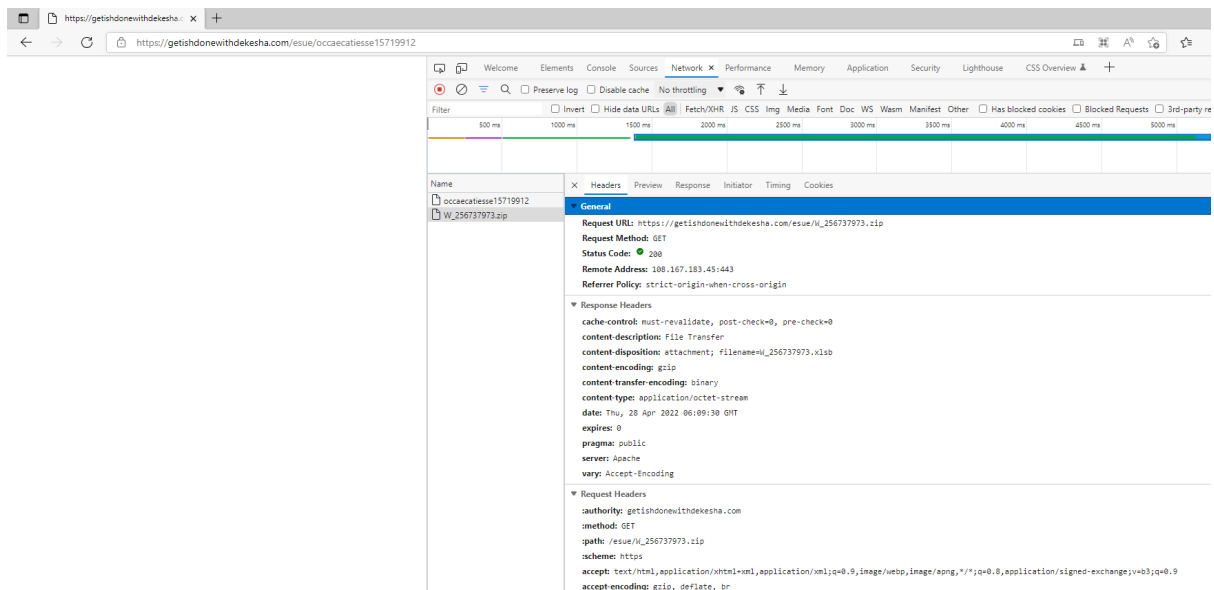
However, the page is scripted with JavaScript to request a zip file named “W_256737973.zip” by using element of “document.getElementById.getAttribute” in JavaScript.

Which pass the “data-PgDWEfyu” variable that is a path to “/esue/W_256737973.zip” as attribute redirect to the zip file.

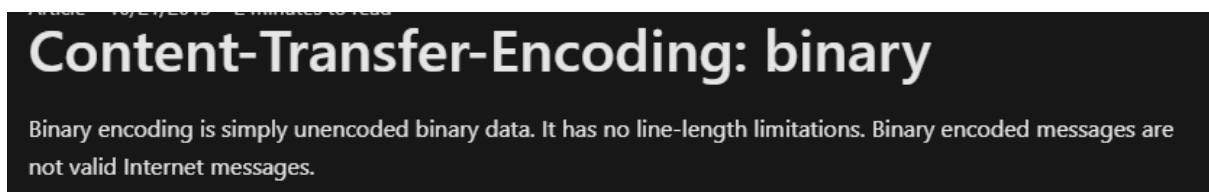


With the redirection to the zip file, the request header changed to download an excel file named “W_256737973.xlsb” with the “content-transfer-encoding: binary”.

PHISHING EMAIL ANALYSIS



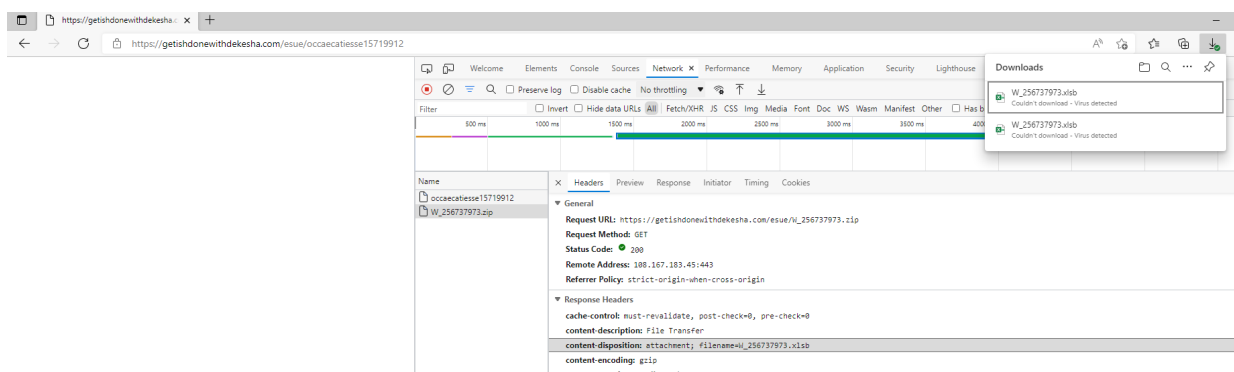
“content-transfer-encoding: binary” is simply unencoded binary data that allow us or malicious actor to download file in binary form, you will refer to the [link here](#) or the image below.



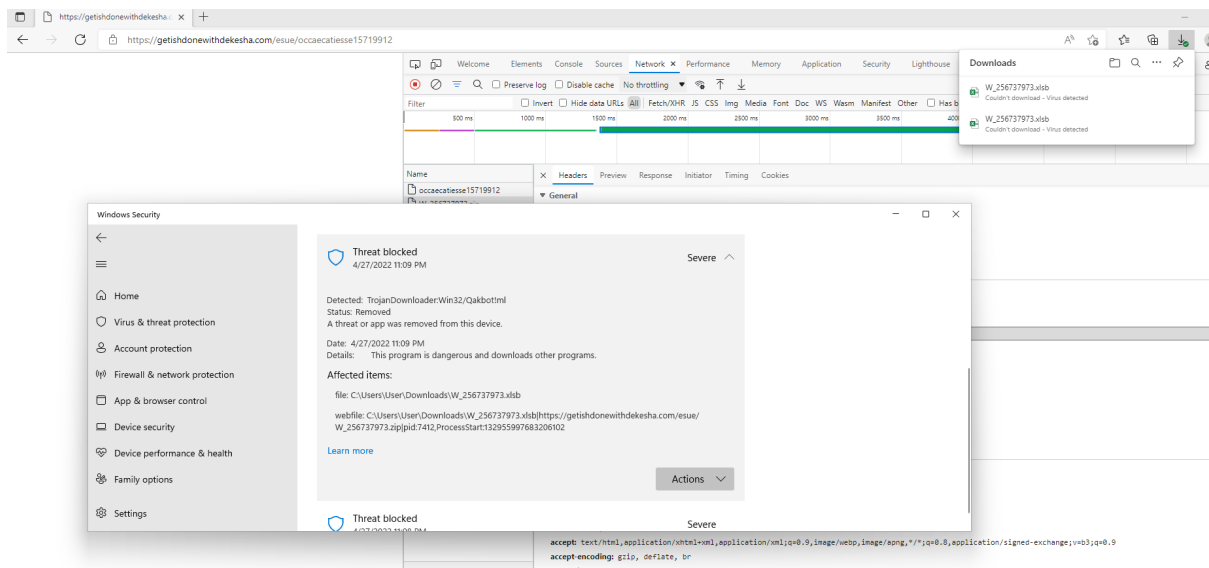
All the above actions and redirections are seamlessly running without user notice.

The result was an excel file named “W_256737973.xlsb” downloaded.

In most cases, modern browser such as Microsoft Edge or Google Chrome leveraging Endpoint Protection such as Windows Defender will be able to detect/flag and block the download.



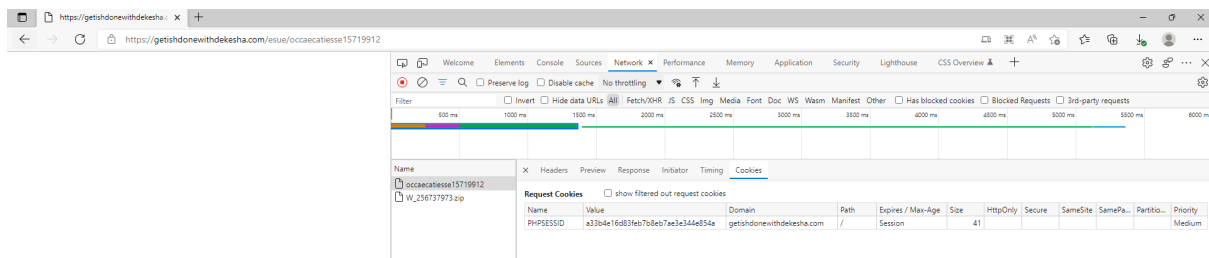
As we view the detail in Windows Defender, it detected as threat and has been removed.



Additional information

Cookies used in the malicious link to the page

Below shown the “cookies” used in the link to the page.



Har file include all HTTP session request and response



getishdnewithdeshesha.com.har

Malicious excel file analysis

We have downloaded the file manually in sandbox or isolated environment to understand and analyse the file.

Using “file” command in Linux show that the file downloaded is a Microsoft Excel file.

```
$ file W_256737973.xlsb
W_256737973.xlsb: Microsoft Excel 2007+
```

String command that output strings content in the file without opening the file.



W_256737973-strings
-command

Checking the extension of the file which is “xlsb”. An **Excel (.xlsb) Binary File Format**, which is a collection of records and structures that specify Excel workbook content. The content can include unstructured or semi-structured tables of numbers, text, or both numbers and text, formulas, external data connections, charts and images.

You may refer to the [link here](#) or image below for details.

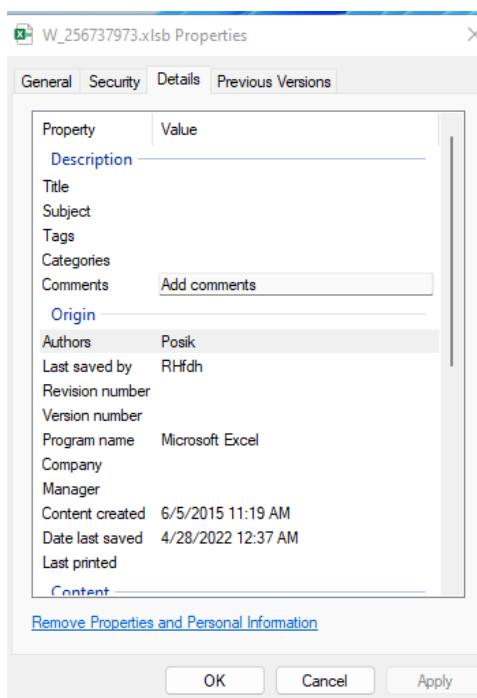
[MS-XLSB]: Excel (.xlsb) Binary File Format

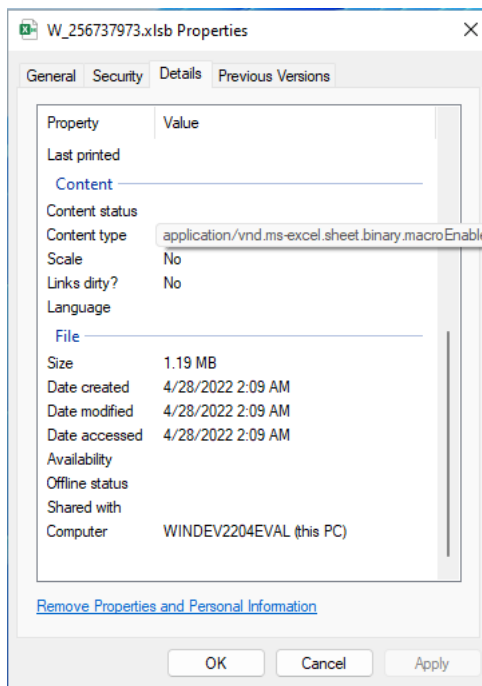
Article • 02/16/2022 • 4 minutes to read



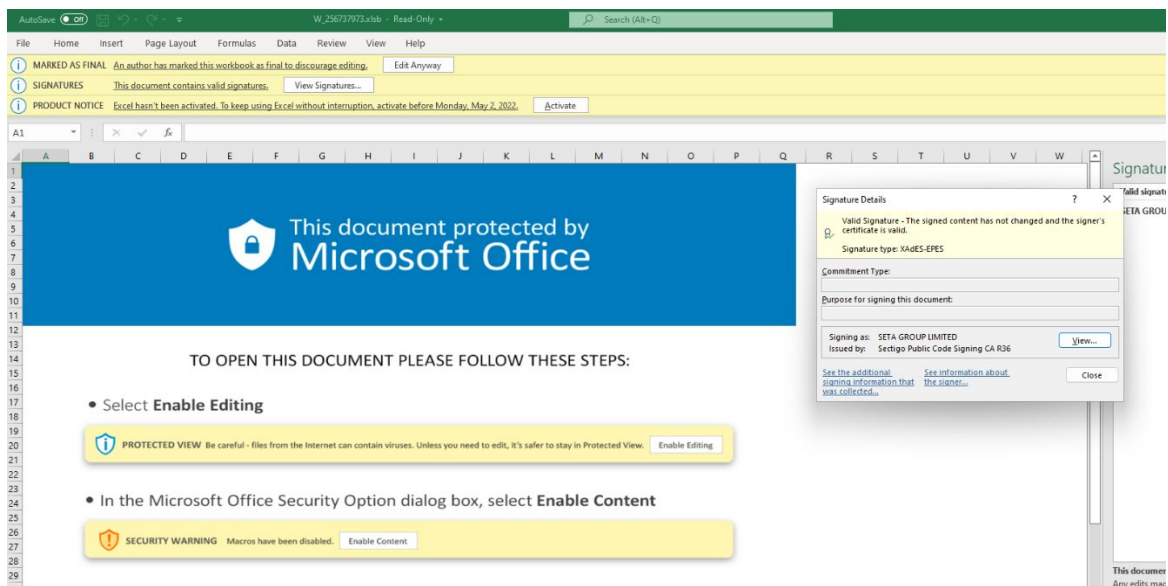
Specifies the Excel (.xlsb) Binary File Format, which is a collection of records and structures that specify Excel workbook content. The content can include unstructured or semi-structured tables of numbers, text, or both numbers and text, formulas, external data connections, charts and images.

Below are the “Properties” of the file.





Open “W_256737973.xlsb” in read-only view as shown below

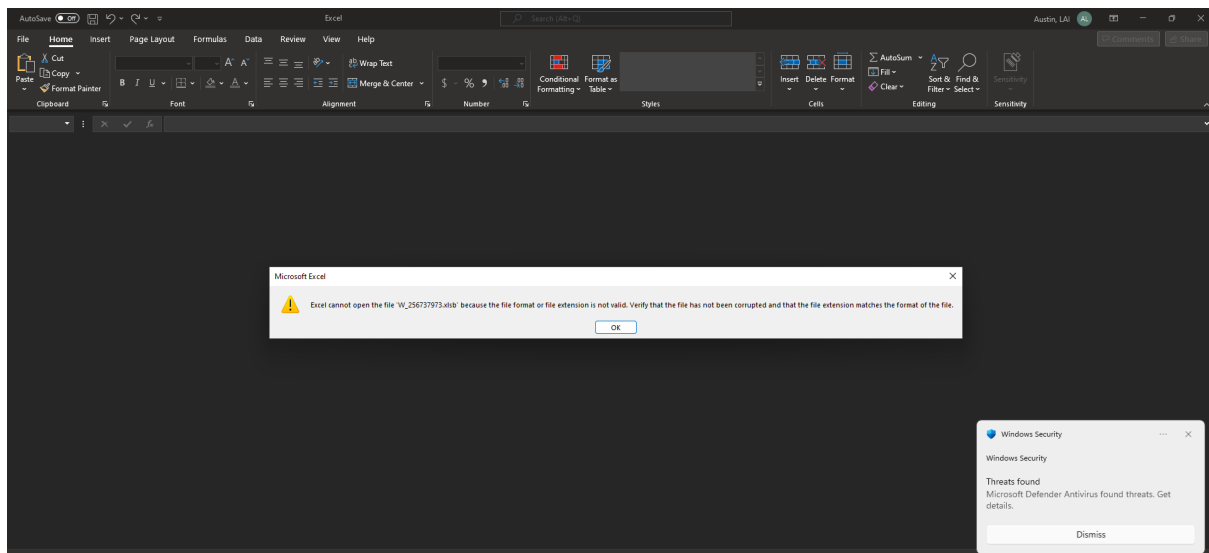


If we enabled write or open the file in normal mode, it will prompt an error message as below

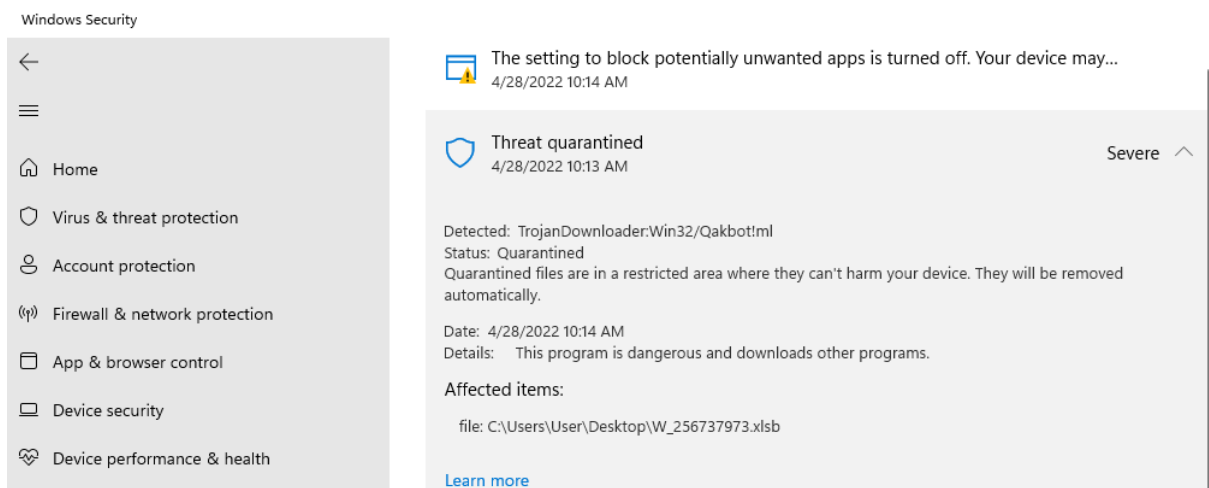
“Excel cannot open the file of "W_256737973.xlsb" because the file format or file extension is not valid. Verify that the file has not been corrupted and that the file extension matches the format of the file.”

Immediately Windows Defender detected a threat associated to the file and blocked it.

PHISHING EMAIL ANALYSIS



Below are the details of the threat associate to "W_256737973.xlsx".



Report "W_256737973.xlsx" against VirusTotal

VirusTotal is free service that analyses files and URLs for viruses, worms, trojans and other kinds of malicious content.

Below is the result from VirusTotal, stated the file is malicious.

PHISHING EMAIL ANALYSIS

9 / 60

9 security vendors and no sandboxes flagged this file as malicious

f6057c8937a5e22457f83188e8199b7703dc6b8ca1910f0c666a5bc6b27b2495
W_256737973.xlsx
xlsx

1.20 MB Size
2022-04-28 08:37:56 UTC a moment ago

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

Security Vendors' Analysis

ClamAV	ⓘ Xls.Downloader.Qbot032217-9941295-0	Cyren	ⓘ XF/Qbot.J.genIEldorado
Fortinet	ⓘ MSExcel/Agent.E4A8ltr.dldr	GData	ⓘ Macro.Trojan-Downloader.Agent.BDH
Ikarus	ⓘ Trojan.XLM.Agent	Kaspersky	ⓘ HEUR:Trojan.MSOffice.Generic
McAfee	ⓘ X97M/Downloader.oy	Sangfor Engine Zero	ⓘ Malware.Generic-XLM.Save.ma35
ZoneAlarm by Check Point	ⓘ HEUR:Trojan.MSOffice.Generic	Acronis (Static ML)	✔ Undetected
Ad-Aware	✔ Undetected	AhnLab-V3	✔ Undetected

You may refer to [this link](#) for all the details reported from VirusTotal.

Some of the details can be used as IOCs (Indicator of Compromised) such as MD5 hash or SHA hash.

MD5:

fa5d01d7c68e39fb316fe70e4346f25b

SHA-1:

c408c585ca060097b4ad7318d4af854682fb4a98

SHA-256:

f6057c8937a5e22457f83188e8199b7703dc6b8ca1910f0c666a5bc6b27b2495

Vhash:

e5b6cdd76764758b2bfc78872481a661

SSDEEP:

*24576:2D1PzyzYQW98VdaKPSmDVvIB1PzyzYQW9e1PzyzYQW9972+AQcNq6s9d:2
DNz+zfTqmFIBNz+zDNz+z86+AQW1s9d*

TLSH:

*T1F64512A2C1E144A3E8F46734134485D182BA28AFF83CEC454BD77DFF2E990F
A6E91594*

File type:

Office Open XML Spreadsheet

Magic Zip archive data, at least v2.0 to extract

TrID:

Excel Binary workbook (62.2%)

TrID:

Excel Microsoft Office Open XML Format document (22.7%)

TrID:

Open Packaging Conventions container (11.7%)

TrID:

ZIP compressed archive (2.6%)

TrID:

PrintFox/Pagefox bitmap (640x800) (0.6%)

File size:

1.20 MB (1255518 bytes)

Execute malicious file “W_256737973.xlsb” on AnyRun.

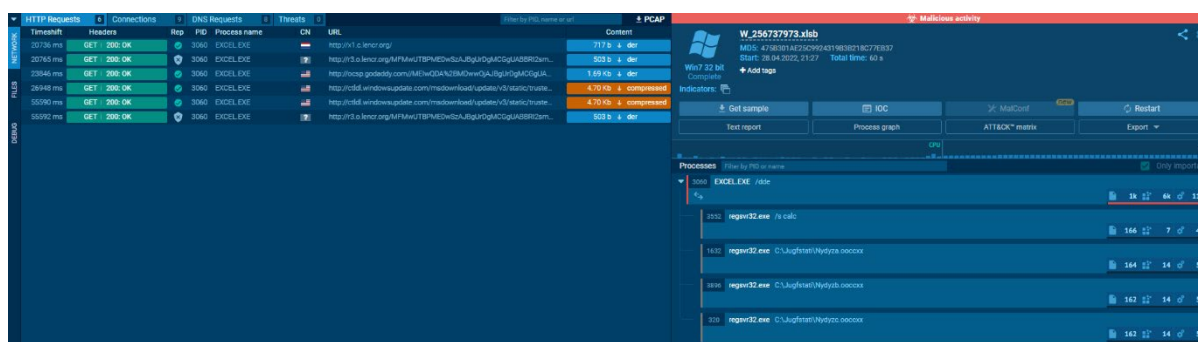
AnyRun is an interactive malware analysis sandbox. The service detects, analyses, and monitors cybersecurity threats. A user-friendly interface allows performing effective and qualitative investigations.

The service shows all processes in real-time. And an analyst can notice all malicious operations before the final version of the report.

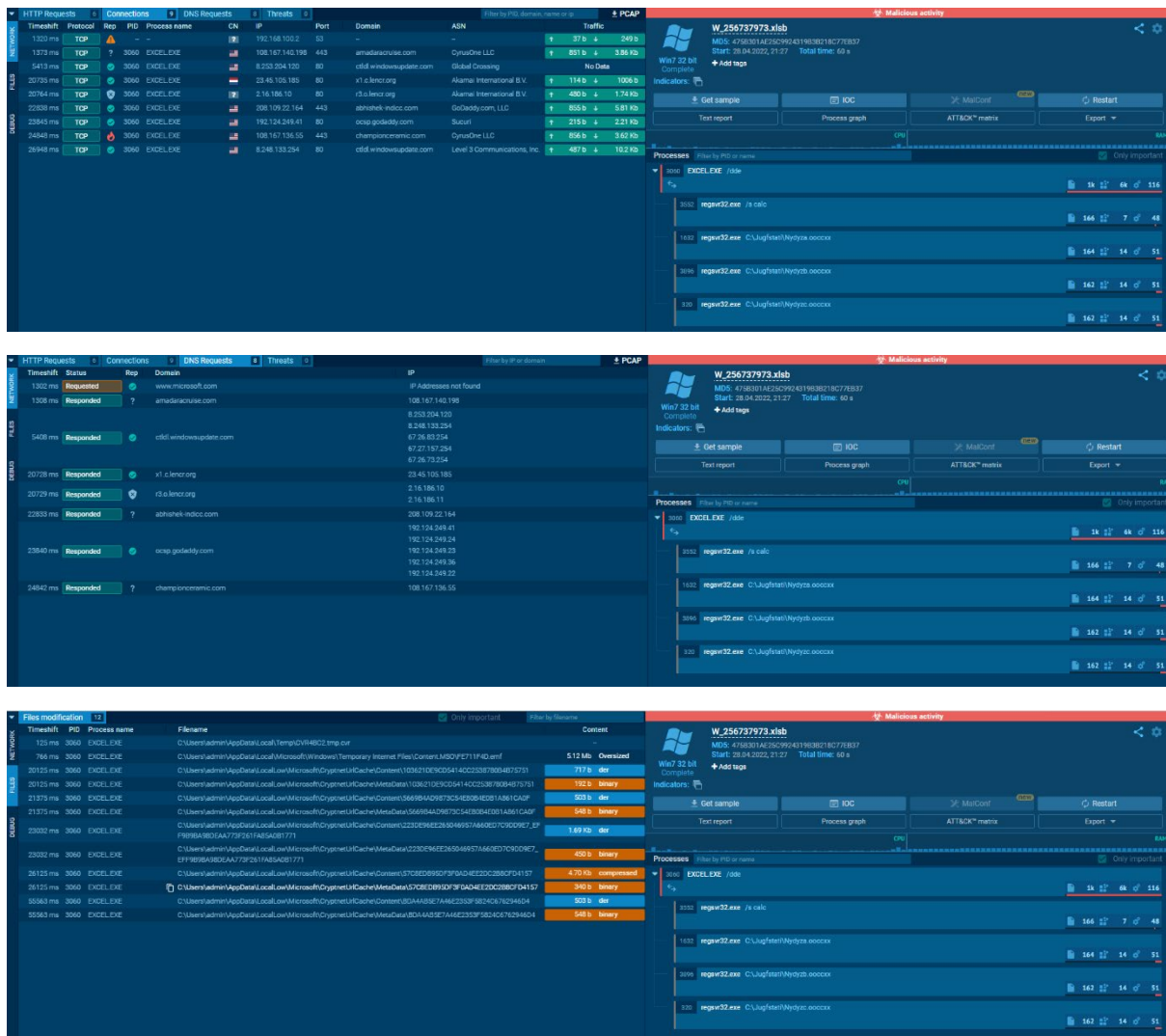
Below is the information retrieve by running malicious file in AnyRun.

Once the file is opened, it start to connect to


“http[:]//r3.o.lencr.org/MFMwUTBPME0wSzAJBgUrDgMCGGUABBR12smg%2ByvTLU%2Fw3mjS9We3NfmzxAQUFC6zF7dYVsuuUAIA5h%2BvnYsUwsYCEgMwPZI8TJaAiNShdtG85TGvIA%3D%3D” and download multiple files. Seamlessly also create and modify multiple registry key as shown in the image below.



PHISHING EMAIL ANALYSIS

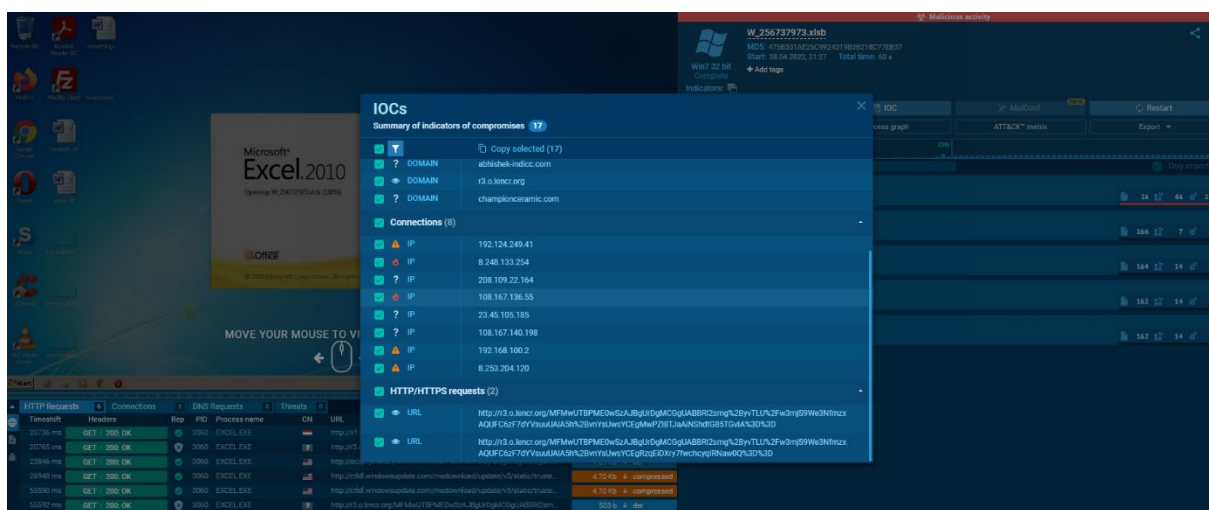
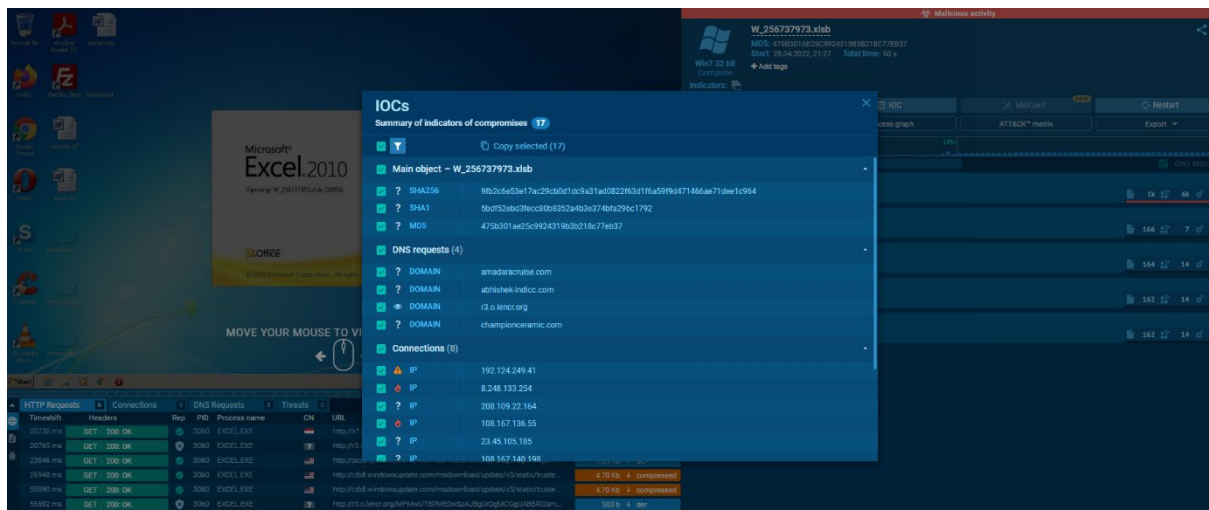


PCAP file attach below extracted from AnyRun for your references.

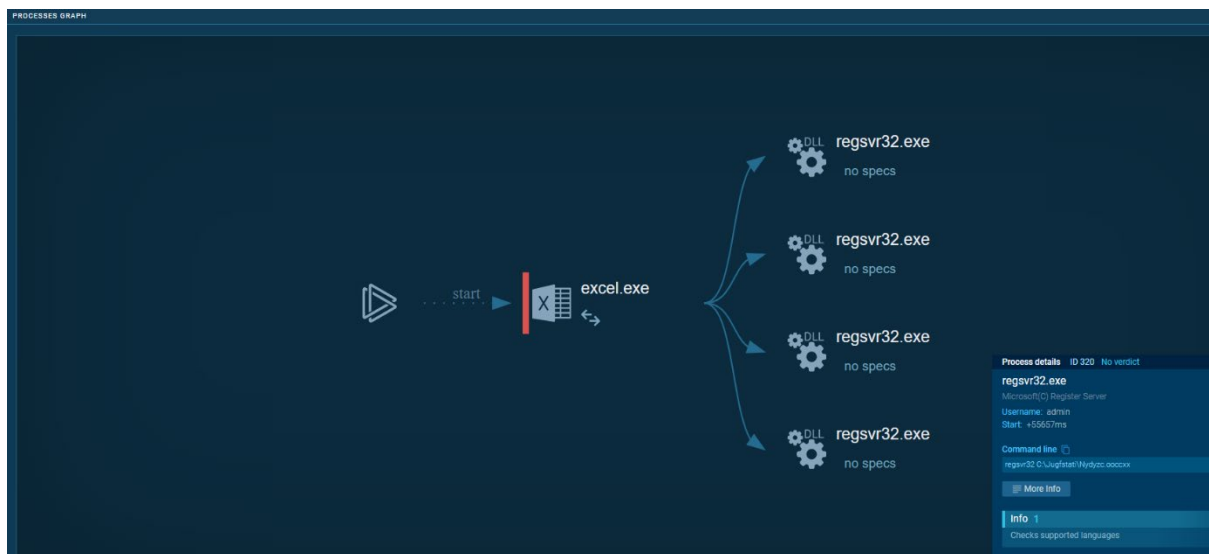

 ab757b27-1bc4-4985
 -a507-ff0b5e29cd6c.p

With the sandbox environment, AnyRun managed to extract IOCs for our reference.

PHISHING EMAIL ANALYSIS

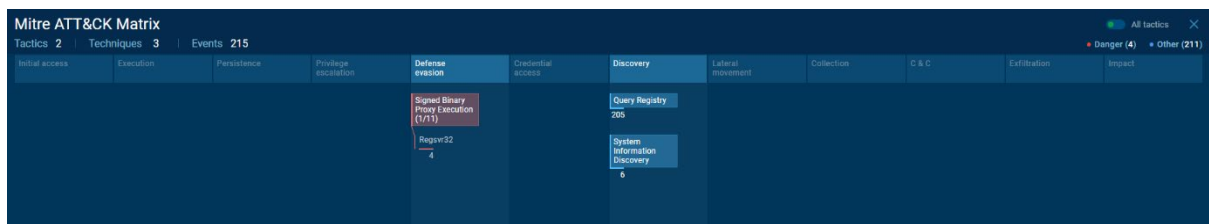


Below shows the process spawned by the malicious file and how it interacts with processes and registry keys.

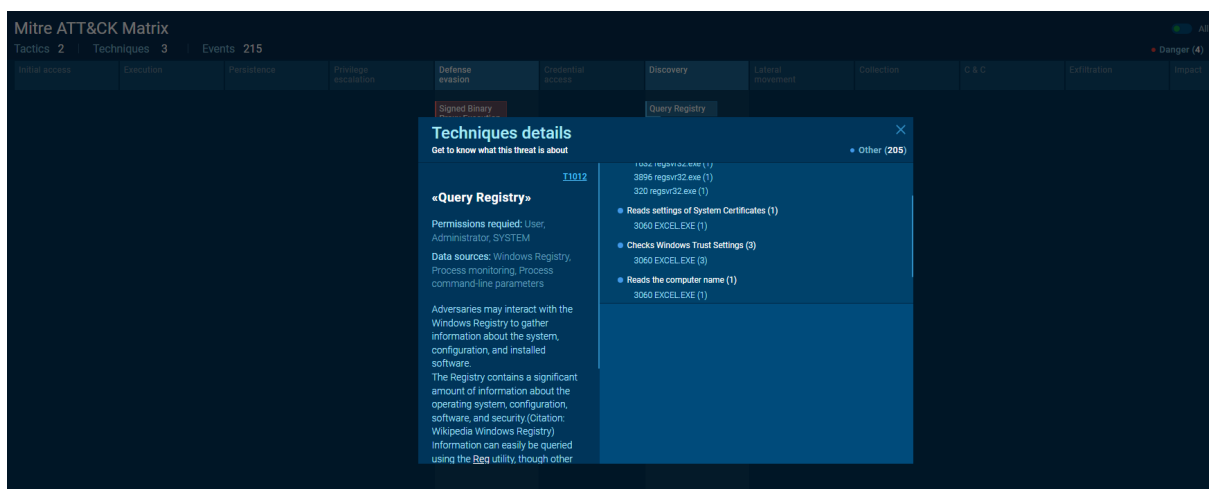
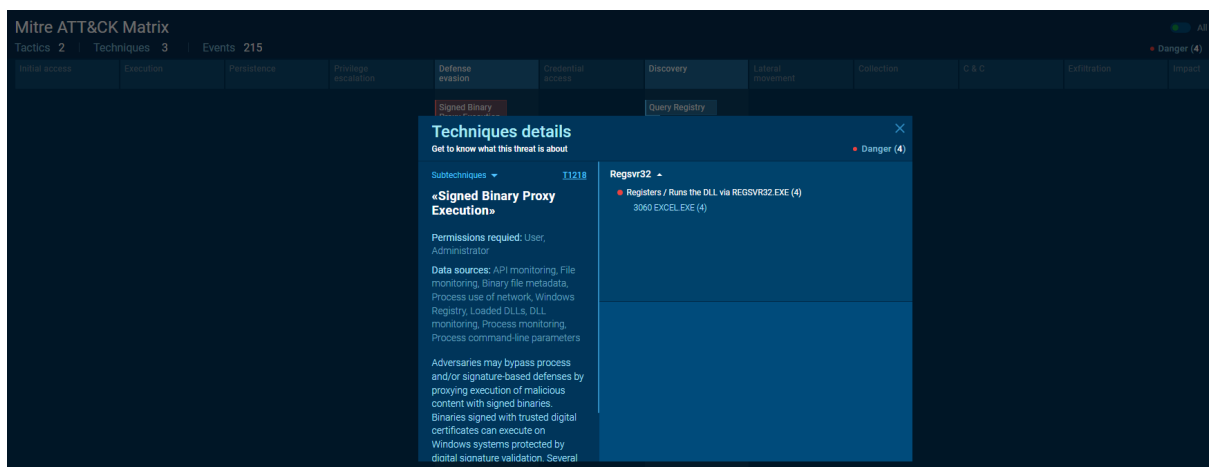


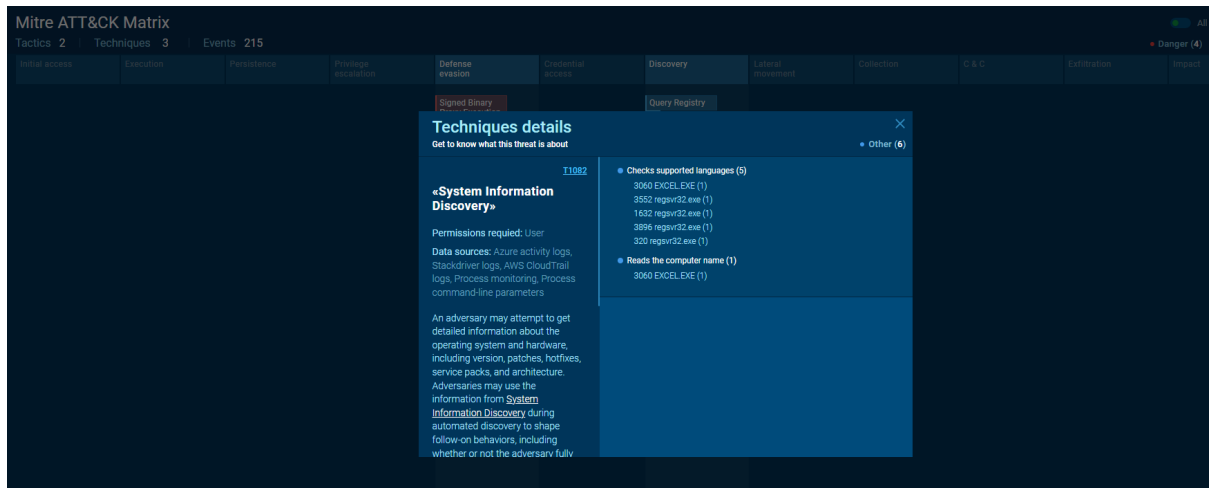
PHISHING EMAIL ANALYSIS

AnyRun also provide the analysis of the malicious file mapping to MITRE ATT&CK Matrix.



Some of the techniques used as below





You may find the malicious file analysis in AnyRun from [this link](#).

You may also refer to the full final report from AnyRun from [this link](#).

Conclusion

A successful early detection of phishing email incident requires the ability to collect relevant data, organizing that data into actionable threat intelligence, and getting that optimized threat intelligence into the hands of incident responders who can then make good decisions that reduces an organization's risk.

Hence, it is recommended to

--- OMITTED ---

--- OMITTED ---

--- OMITTED ---

Last but not least, enlisting users in the fight against phishing-related risks should be a key part of our overall layered security strategy. The good news is that users don't have to be perfect to be effective. We only need enough of them to detect and report a campaign to be able to stop it before any damage is caused.

One way we can do is to **simulate actual attacks**. Depend on the user's response to the simulation, you would then send a "thank you" email to those who accurately identified and reported threats for those who mistook a phishing email for a legitimate one.

Finally, we should consider implementing some sort of rewards plan that will encourage users to report on potential phishing attacks. Such plan should aim to encourage behavioural changes that would motivate employees to identify and report suspected phishing schemes.

At the same time, continually reassure employees that they will not be punished if their actions—such as clicking on a questionable file—may have led to an attack. A punitive approach will only lead to employees hiding their actions, which will be far more damaging to our organization to flight against phishing attacks.