Incident Response Room 11_29_24

Incident response is processes and technologies a company uses to detect and react to cyber threats, security breaches, or Cyber Attacks.

Organizations establishes incident procedures and technologies within a formal incident response plan. If they need a direction or a framework to build their plan, then they can use:

- NIST (National institute of Standards and Technology)
- SANS (Sysadmin, Audit, Network and Security)

NIST incident Response Framework has 4 steps:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity
  SANS incident Response Framework has 6 steps:
- Preparation
- identification
- containment
- eradication
- recovery
- lessons learned

These Frameworks(NIST, SANS) are used by organizations worldwide to aide with the development of an effective Incident Response Plan.

"Security is not a product but a **process**"

Scenario:

Investigate and remedy a potential incident impacting a Windows workstation.

- Laptop has been reported becoming extremely slow and acting up.
- User does not know exactly what he was doing when the computer started to slow.
- Web browsing and working on some documents per usual
- Rebooted machine but performance is still running slow

Troubleshooting steps already taken:

- Checked CPU resources and CPU is running Unusually high even after closing all apps.
- IT escalated ticket to the SOC team

Soc team verified that no alert was raised on SIEM or EDR platforms for this workstation.

- One anomaly that has been identified is some outbound connections on the perimeter firewall originating from the workstations IP.
- These connections are not blocked by the Firewall.
- User does not recall attempting these connections.
- This issue has been escalated again but this time to the IR Team (Incident response)

Analysis:

- 32th4ckm3 is using over 50% of the CPU
- This exe is located in a suspicious location, the 'temp ' folder
- PID for 32th4ckm3 is 4404

Using Command prompt:

netstat -aofn | find "4404"

output:

TCP 10.10.250.136:49713 45.33.32.156:42424 SYN_SENT 4404

- Computer IP sending syn packets to a unknown IP, possibly a C2 server
  What you can do to mitigate this IoC (Indicator of Compromise)
- Block the IP with a rule on firewall
- Search IP in the network traffic log to check occurrences of the malware
- Turn the IoC to a monitoring rule on the SIEM to proactively detect any later anomalies

Normally, we would want to do further analysis on this IoC but the room is giving it away and saying this is a crypto Miner

Now what?

- Now that it is confirmed a crypto Miner; proper documentation has to be done on the initial access vector.

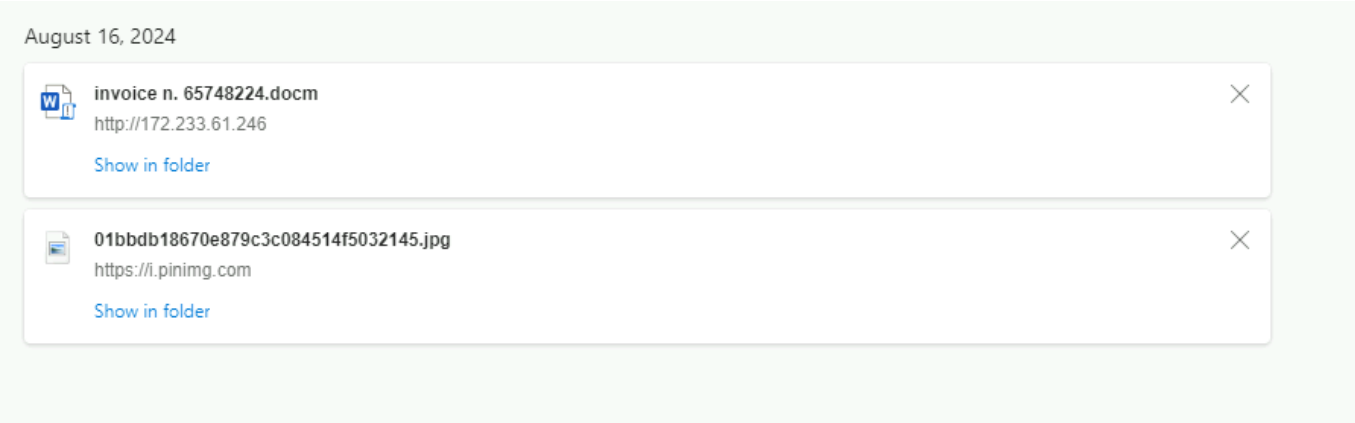
Understanding the initial access vector is crucial because it helps pinpoint the gap in the system; that way you can 'plug up' the gap.

Usually the end-user that is careless is most likely how the compromise came to light.

Further analysis on what was the initial access vector:

- Based off the user's response on what he may have been doing at the time of the computer slowness, we check the browser history:

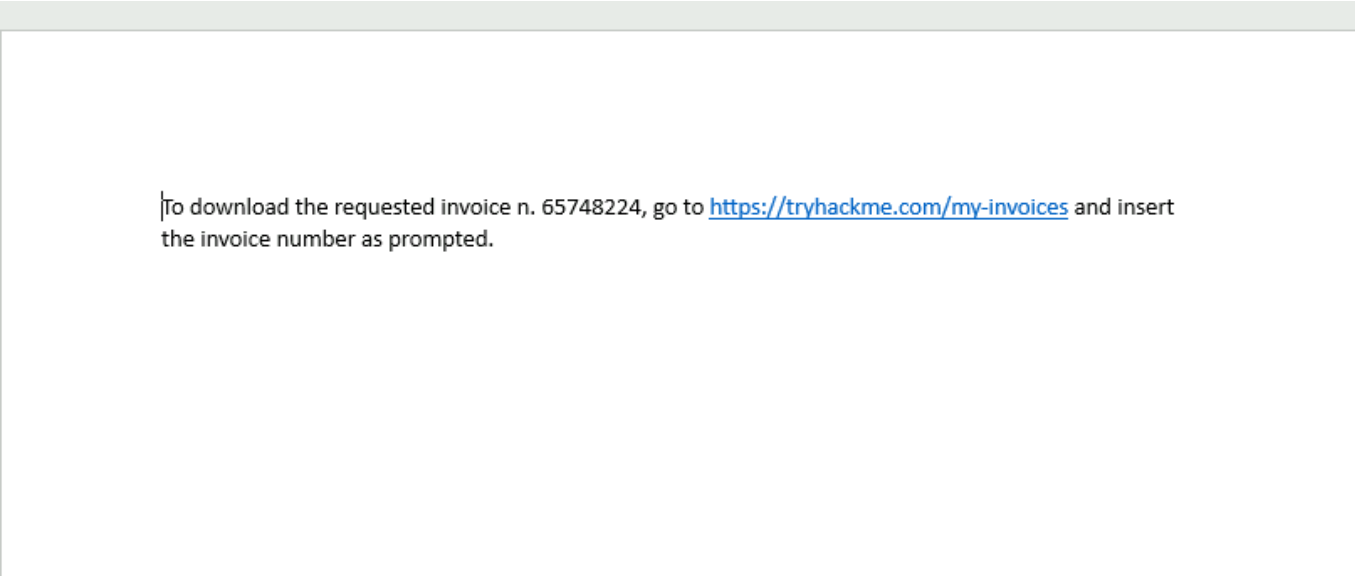
I see two downloads in downloads history:



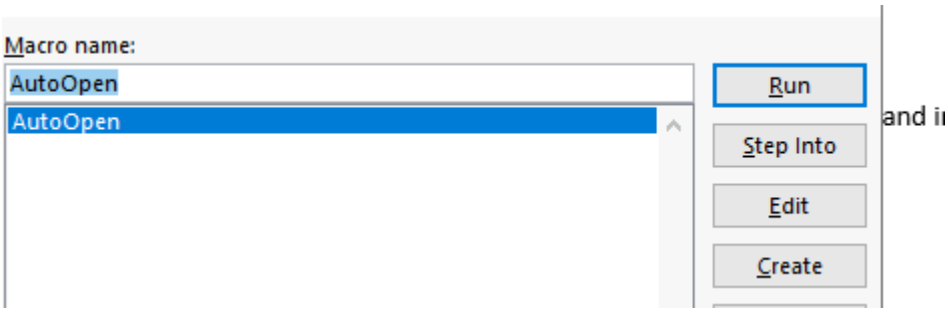
- We can see here that a file named "invoice n. 65748224.docm" coming from a unusual address http://172.233.61.246 when normally, we see more conventional address like https://i.pinimg.com the second file.
- Checking the first file name, the extension docm is a Macro-enabled word document. This means it contains macros. Basically, this document has has hidden instructions.
- In this case, seems like macros was implemented to automatically download when probably clicking a link

Now what?

Let's open the .docm document:



Going to view > Macros will give us a list of macros running:



AutoOpen macro is running.

Containment

Containment has been partially done, as the computer was detached from the network to prevent spread.

- We should stop the process in the task manager
- We should compile a list of the IoCs we have found during our Analysis:

1. The IP and port of the C2 server
2. The url from the Macro
3. The URL embedded in the macro
4. The hash of the malware's executable

Developing a list, will help identify and remediate any other compromised host within the organization. Updating the Monitoring tools with our IoC list. If you add a hash to an EDR blocklist or create a SIEM rule, this will detect connection and prevent later infection from the same threat.

Eradication and Recovery

To fully get rid of the threat, you have to delete any artefacts that were dropped on the machine

We also need to compile a list that contains details of the actions taken.

- Keep track of files names
- folders and other details that we've encountered

So steps we can do to eradicate and recover :

- deleting the malware from the temporary folder where it was running
  I found this in C:\Users\TryCleanUser\AppData\Local\Temp\2

- delete from downloads or where it was downloaded too (C:\Users\TryCleanUser\Downloads)
- Clear the download history where the initial vector was determined.
  Went onto web browser and deleted the history!
- Restoring the registry key to it's normal value
  Closing the cycle

Post-incident Activity

This is a critical phase which focuses on learning from the incident to enhance future response efforts and overall security posture.

- Reviewing the incident
- documenting lessons learned
- integrating the insights into the Incident Response Plan developed during the preparation phase

For this particular scenario, here are some integrations you could apply:

- Implementing an EDR solution able to detect the kind of threat that was just faced (Crypto miners and malicious macro)
- Enforcing a web-browsing control system that would prevent users from navigating to unsafe websites.
- Raising awareness among employees on the potential threat of macro-enabled Office files and navigating suspicious links, like Mandatory Training on the topic
- Discussing the approach of implementing a policy to block the execution of macros as a counter measure, ensuring that this wouldn't disrupt legitimate business operations.
