This document is meant to represent the intel that was gathered during the analysis of the possible victim’s disk image.

This lab is meant to simulate a real-life situation where me, as a forensic investigator, tries to determine whether the employee is a victim, or is responsible for the data breach of a fictive company. After gathering the image document, I will start by setting up some information that I find out and fill out the questions from the quiz. At the end, by gathering the pieces of information I found, and trying to reconstruct the timeline of what happened, and give a response whether the employee is a victim or not.

First, we want to know what the initial attack vector was used to compromise the victim system.

After checking the document E01.E01, first of all I decided to check the Users on the machine and see what I can find.

A screenshot of a computer program

Description automatically generated

On the system we can find default user setting done by Windows, and also our employees account JeanK (Jean Krabs), and a suspicious account called “NotTheHacker” (quiz), which was probably created by the attacker.

Then I decided to check the files that can be found in the JeanK’s User folder. I am looking for files, or something suspicious that could be downloaded or appeared on the system.

Downloads folder did not show anything too much interesting except python installer, some other programs, and an image.

A screenshot of a computer

Description automatically generated

The image seems to be harmless, however we can check the Alternate Data Streams to see where it was downloaded from and hosted on: “ReferrerUrl=https://apod.nasa.gov/apod/ap130422.html” (quiz).

In the Documents folder can be found files, that probably got encrypted, and hence corrupted by the attacker. This data should be able to reconstruct afterwards.

A screenshot of a computer

Description automatically generated

Checking the Pictures folder showed a file that contains some important information

A screenshot of a computer

Description automatically generated

This is related to quiz “F0RENSICS:57314e5448554d42”

Further checking showed an interesting and relatively strange executable file, which has .pyc extension, and is located in OneDrive folder. The filename is “FixComputer.pyc” (quiz)

A screenshot of a computer

Description automatically generated

The contents of the file seem to have proven the fact that the data got encrypted in the JeanK Documents.

A screenshot of a computer code

Description automatically generated

The ransomware attacker asked to pay 0.25 BTC to this address “bc1k0enkgdygjrsqtzq2n0yrf2493k99kkfjhx1wlh” (quiz)

A screenshot of a computer

Description automatically generated

This was also written by the script to the desktop of JeanK.

A screenshot of a computer

Description automatically generated

After that, the attacker created a new user on the system, elevated it to Administrator rights, and removed JeanK from the Administrators group.

Also it can be seen that the attacker tried to set up a firewall rule(s) that would allow RDP (Remote Desktop Protocol), and hence more control over the machine.

The attacker seems to have used the cryptography fernet library, which means that we can not read the data back.

A screenshot of a computer program

Description automatically generated

Next, I decided to check upon the NotTheHacker user’s folders, and first took a look at Downloads folder, which contains installer for nmap, which is a tool to check for open ports on the system or network.

A screenshot of a computer

Description automatically generated

Then, I found a hidden folder called .zenmap, which is probably a automatization tool that helps to run scans on the network.

A screenshot of a computer

Description automatically generated

It does not look like there were scans performed on the network considering the recent\_scans.txt file. But we can check the .db file and see the contents of it.

A screen shot of a computer

Description automatically generated

Inside there we can see outputs, which means that there probably were already scans.

Apart from that, does not look like anything much can be found from the first file.

Now it is time to check the possible registry manipulations that happened on the system, and see what else happened.

By mounting the files as File System (read only), I managed to get a hang of the NTUSER.DAT registry hive, which gives more information regarding the actions done, in this case, by the regular user JeanK.

One of the things that we want to check, is what were the files opened by the user.

A screenshot of a computer

Description automatically generated

The path: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Here we can see that after opening the document files, Jean then launched the malicious file. We can see that also Jean accessed a secret file of his company (most probably) called “SecretPlan.md” (quiz).

We can also see what Jean looked up on the internet, for example via Mozilla.

To do that, I went to the path G:\[root]\Users\JeanK\AppData\Roaming\Mozilla\Firefox\Profiles\mggyyq5w.default-release and copied the database places.sqlite to my machine, and opened it with DB Browser for SQLite.

Then I ran the SQL SELECT url FROM moz\_places WHERE url LIKE '%google.com/search%';

And got several results, and one relevant of them was “pinky and the brain”(quiz)

Then, I decided to take a look at the last files that were run by the NotTheHacker.

The path: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

There, I managed to see that the attacker used the zenmap tool, as specified before.

A screenshot of a computer

Description automatically generated

So the last .exe that was run by the attacker was “zenmap.exe”(quiz)

After that, what we can do, is go ahead and get some more information regarding the system, and for example – get the IP addresses appended to the machine. To do that, I mounted the SYSTEM registry hive, which is located in Windows/System32/config. There are also present other important registry hives, and not only the user ones.

The path: SYSTEM\_HIVE\ControlSet001\Services\Tcpip\Parameters\Interfaces

In there, we are looking for additional information regarding the interfaces of the machine and IP addresses. The parameters are called IPaddress or DHCPIPaddress.

A screenshot of a computer

Description automatically generated

We can see 2 in this case, but also the first one is related to the quiz “172.16.43.128”

Important to note, that meanwhile the investigation, I also managed to file the original file that was created to actually encrypt the data

A screen shot of a computer screen

Description automatically generated

Inside here we can get the idea of what happened for sure, and also get the key and try to decrypt the data afterwards. Key “hfUogC40RsWhbqdeD5Ib6QBE4XQTYEUZAYhaBeOy\_bw=”

File was found here “G:\[root]\Users\JeanK\AppData\Local\Temp\vmware-JeanK”

Good news is, I managed to restore at least a file, which is SecretPlan.md contents.

A screen shot of a computer program

Description automatically generated

Here is the script that I ran to do that, and I put the documents into the same folder.

A screenshot of a computer

Description automatically generated

The content inside seems to be a script of the pinky and the brain movie.

Managed to restore ImportantConcept.md file as well

A screen shot of a computer

Description automatically generated

Idea1.md

A screenshot of a computer

Description automatically generated

Idea2.md

A screenshot of a computer

Description automatically generated

Idea3.md

A screenshot of a computer

Description automatically generated

I also managed to get at least a bit of information from the encrypted LetterToBank.docx file, but not sure if it is the full content as the original one:

A screenshot of a computer

Description automatically generated

It says “Letter to bank for budget”

Here is also the script used:

A screen shot of a computer program

Description automatically generated

And here is the Budget.xlsx data that was lost

A screenshot of a computer

Description automatically generated

And here is the script that solved it:

A screenshot of a computer program

Description automatically generated

Apart from that, we can also check for files that were lastly accessed by Jean, and also understand that he probably deleted some files.

In this case, he seems to have deleted a Word file called “LettertoBoss.docx” (quiz)

A screenshot of a computer

Description automatically generated

Path: SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx

I also want to know when did the attacker logged in last time, and for that I can access the SAM registry hive, and get an overview of the users.

The entry looks like this

A screenshot of a computer

Description automatically generated

Why this user? Because in the right bottom corner in hex we can see NotTheHacker.

So, to find the last logon time of the user, it was first needed to get the SID at least, to know for sure who is the user that logged in

This could be found in the Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-351928660-1343639059-3286354232-1001

After that, it could be found via the registry the last logon time

A screenshot of a computer

Description automatically generated

But this time is not accurate as it is specified in UTC format I believe, and it also does not work for the quiz, hence it was easier to check the event viewer.

Logs are situates here: G:\[root]\Windows\System32\winevt\Logs

By opening the security event logs, I found the last logon was at “12:06:55” (quiz)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Meanwhile looking for the last logon, I also managed to find probably the way the attacker exfiltrated the data:

A screenshot of a computer

Description automatically generatedI might believe that the attacker exfiltrated the data via OneDrive, but that is not very likely in my opinion.

One of the last things we want to know, is how the file appeared on the system, and why did the user decide to launch it.

I decided to check out the users emails that are stored in Thunderbird cached data, and similar to that, as the user was using Thunderbird as a mail client.

To do that, I used a Thunderbird Viewer.

By opening this folder G:\[root]\Users\JeanK\AppData\Roaming\Thunderbird\Profiles\kgjq3sdc.default-release

We find out all the possible information.

In this case I am interested in the mails, and if there is anything suspicious.

A screenshot of a computer

Description automatically generated

The only mail is this, and it comes from Koreman Koen, a legend. The subject is “Error with computer” (quiz). It asks the user to launch the attachement. Double click on it will show us the content, where we can see the file that encrypted the data.

A screenshot of a computer

Description automatically generated

Hence, now it is clear how it got onto the PC.

So timeline:

User gets emails

User launches script

Script creates and elevates user to administrator, and enables RDP.

Attacker gets access to PC with his user account, and exfiltrates data

Data exfiltration – not sure, but I suppose it was done via RDP or OneDrive.