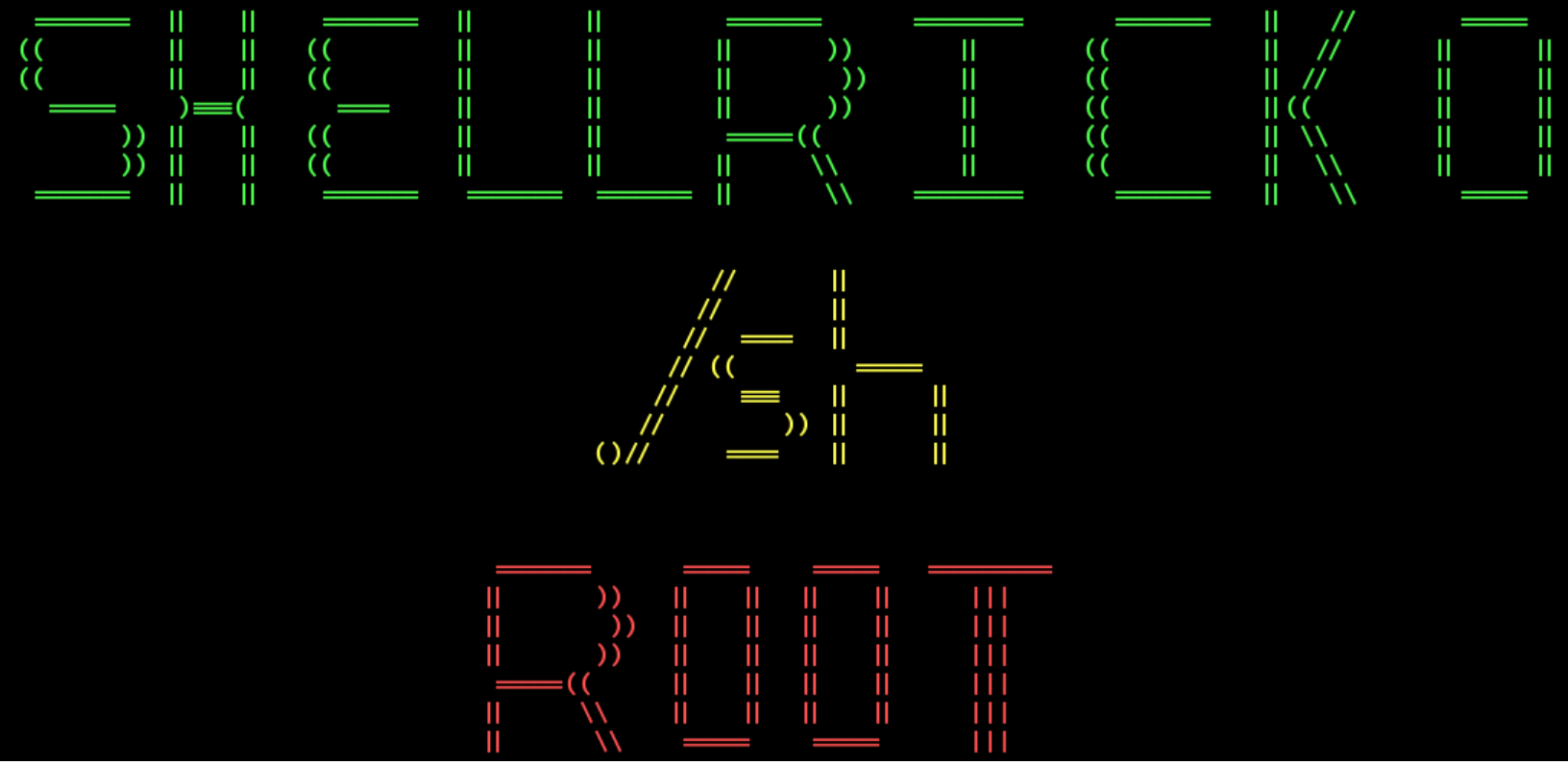


Incident Report

Client: Lockman Group

TeamWork:

- **Sh3llr1ck0**

Content.

Lockman Group

Incident Report

EMPLOYEE DETAILS

NAME	John Coleman
DEPARTMENT	Operations
PHONE NUMBER	N/A

DESCRIPTION OF INCIDENT

Location: Reserved

Date: 11/04/2023

Time: 9:00 a.m.

Police Notified:

- [ ] Yes
- [x] No

Incident Details

An event was forwarded to IT department and taken to Incident Response Team to Sh3llr1ck0 H4ck.

Files renamed to a different file extension (.t48s39la) making impossible to read every file's content, showing a ransomware's activity affecting files under John Coleman's information and computer storage.

Intruder left a note with instructions to unlock an optional file in order to retrieve a payment from the company and unlock remaining files.

Incident Causes:	Follow Up Recommendations:
Download malicious binary. Usage of unofficial websites to perform downloads.	Restore bakups.

Incident reports are necessary for documenting details of the occurrence while they are most present in the minds of the witnesses and incident reporter. The information that is included in the report can be useful for decision-making on future incidents, identify behavioral patterns and identifying larger issues. To maintain a safe and healthy work environment, a thorough investigation should be undertaken following an incident in order to initiate corrective actions.

REPORTED BY:

Name: Sh3llr1ck0

Position: Independant

Department: Sh3llr1ck0 H4ck.

Investigation.

Under the agreement pacted with company “Lockman Group” our team named “Sh3llr1ck0” started to work analyzing the incident occurred at 9:00 a.m. inside a local laptop with ip address 10.10.X.X being used by the user “John Coleman”. Inside this report we illustrate the steps we took to find information and how the attack known as “Ransomware” got injected in such a device, followed by some recommendations.

To perform our task request, we decided to use the tool “Redline”. Redline is a security tool and provides host investigative capabilities to users in order to find sign of malicious activity through memory and file analysis.

Configuration Steps:

Step 1:
Creation of analysis file. Let’s consider as already installed the tool on the device, however, we provide an official link address to download in the links section.

Step 2:
Initialize redline tool from taskbar or through windows symbol.

Step 3:
Select windows on “Target Platform”.

Step 4:
Click “Edit your script”.

Step 5:
Check and uncheck options as shown in the next images.

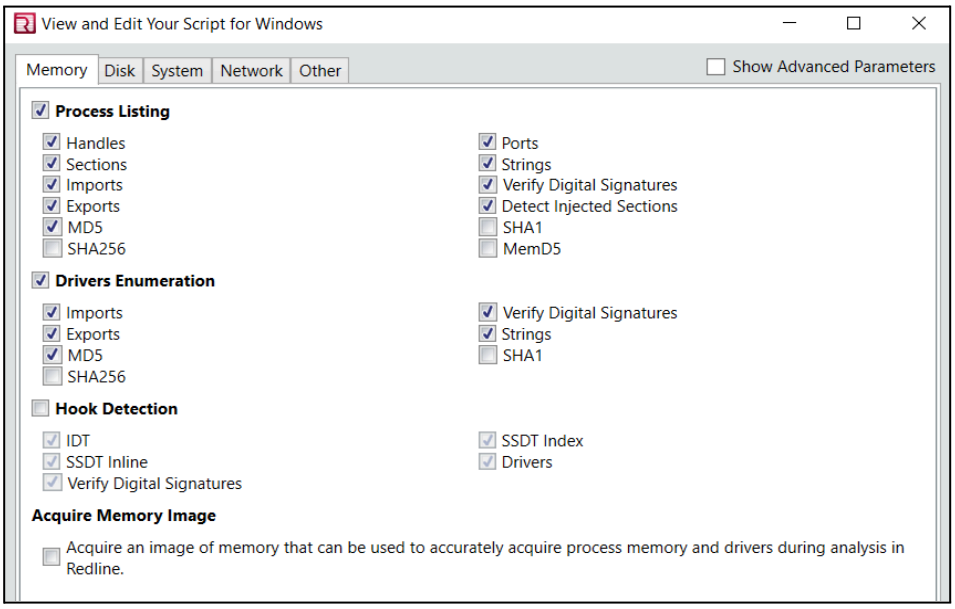


Image 1: Memory section configuration.

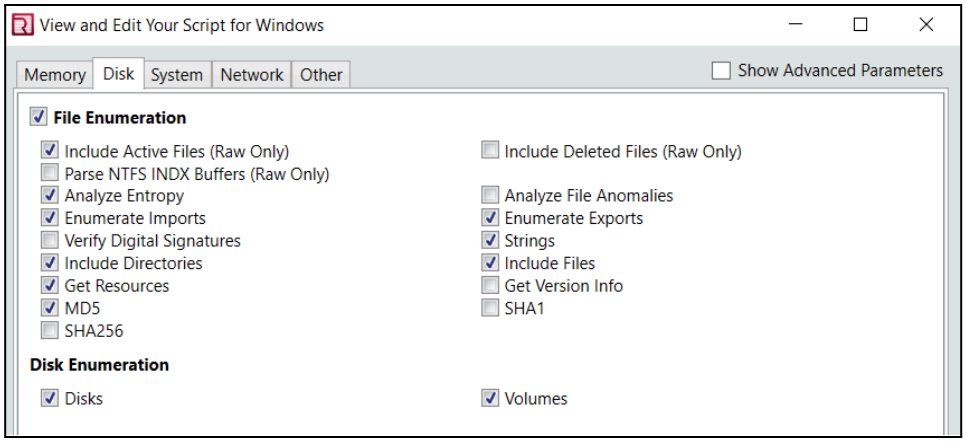


Image 2: Disk section configuration.

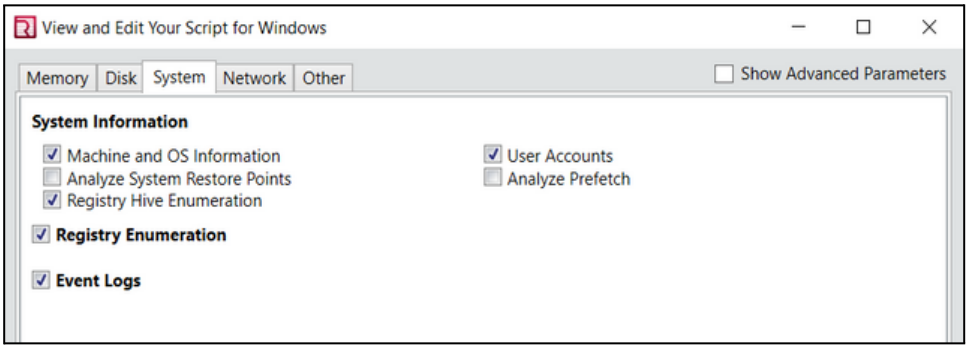


Image 3: System section configuration.

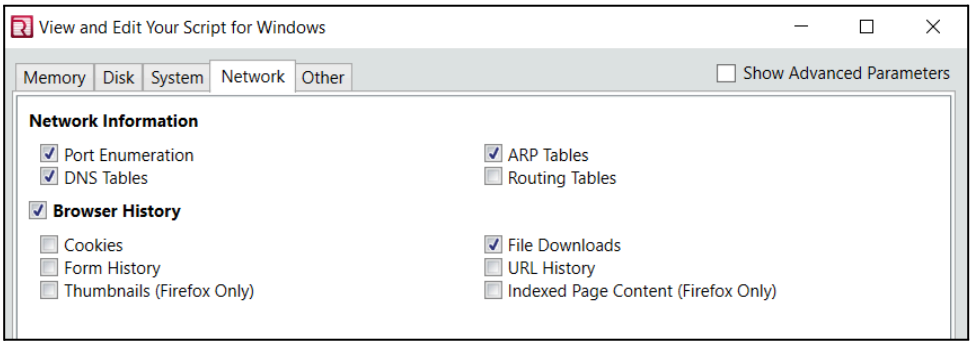


Image 4: Network section configuration.

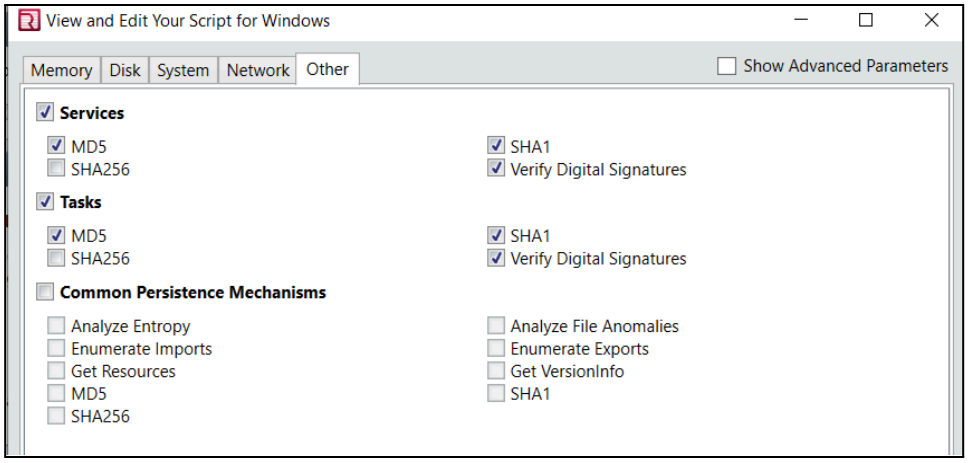
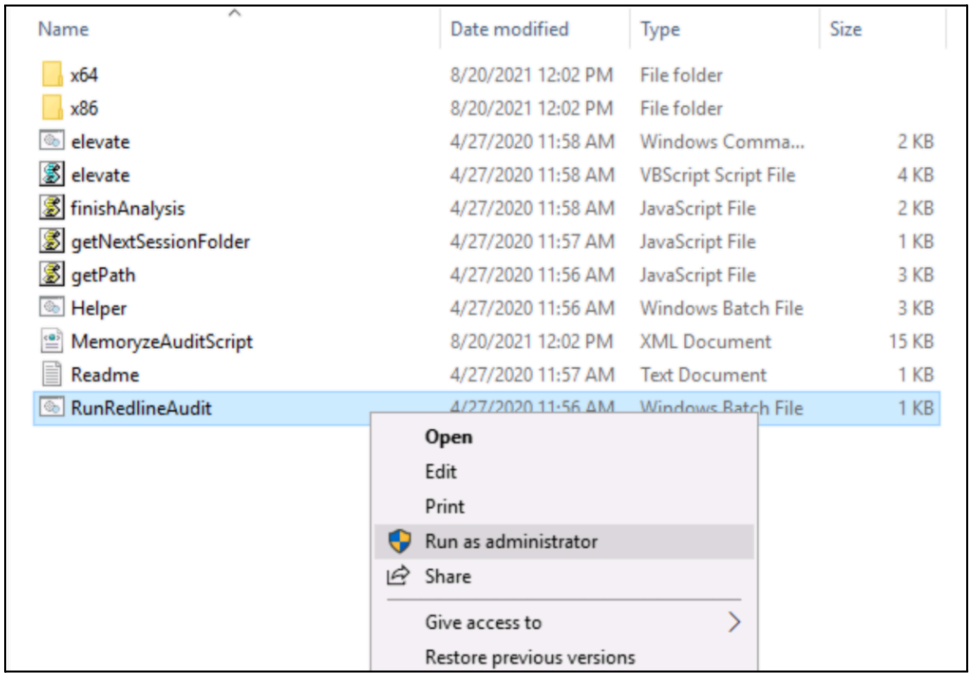


Image 5: Other section configuration.

Step 6:
Select an empty folder to save our configuration.

Running and Importing Script.

Step 1:
Once the loading bar has finished, navigate to the folder previously created and run "RunRedlineAudit" as administrator.



Note: Once the script is running, it might take up to 20 minutes to finish.

Step 2:
You'll notice the cmd window will close automatically and that's the sign it finished its scan. It is enough to double click in the ".mans" file automatically created or importing the file form redline GUI.

Note: Importing the file might take up 10 minutes.

Analysis Incident:
Step 1:
Click on "System Information". Section containing all relevant information regarding the system such as operating system, product name and used logged in.

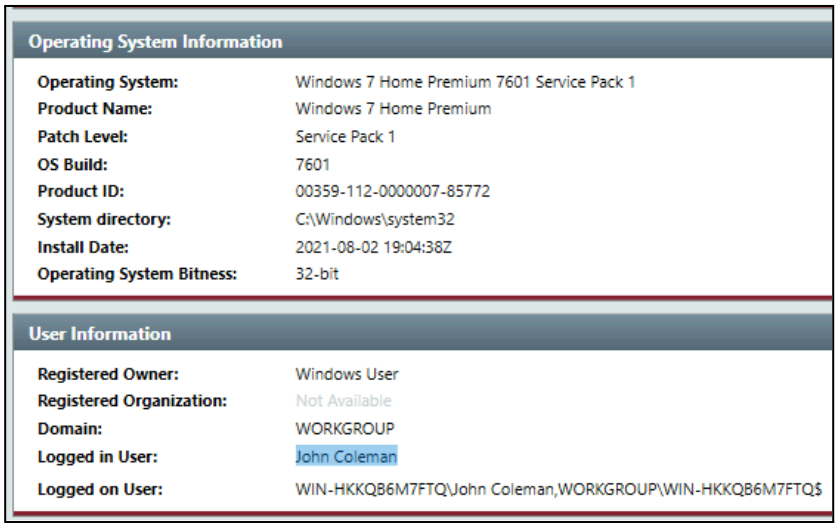


Image 6: System information

Step 2:
Click "File Download History", Section that allows us to see what was downloaded and where.

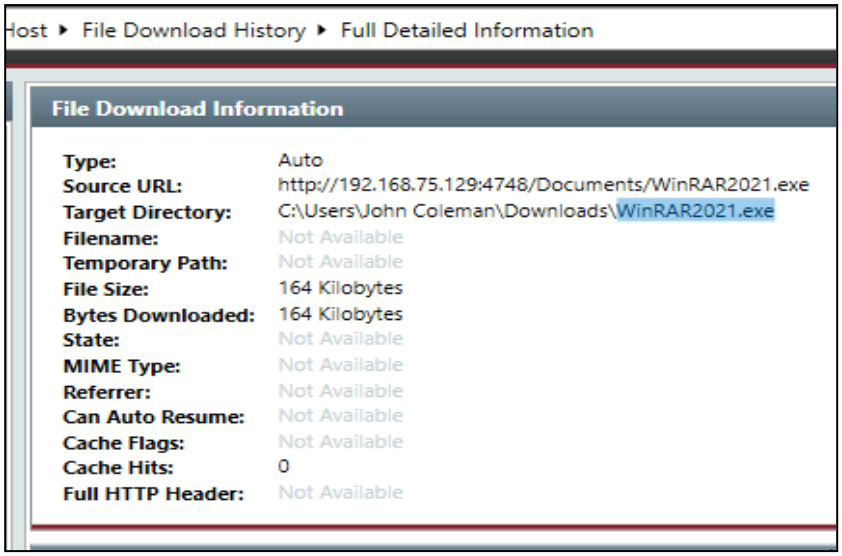


Image 7: Download history.

Step 3:
Click “File System” followed by “Users”, “John Coleman” and “Desktop” in order to see some files renamed and to what format they were renamed.

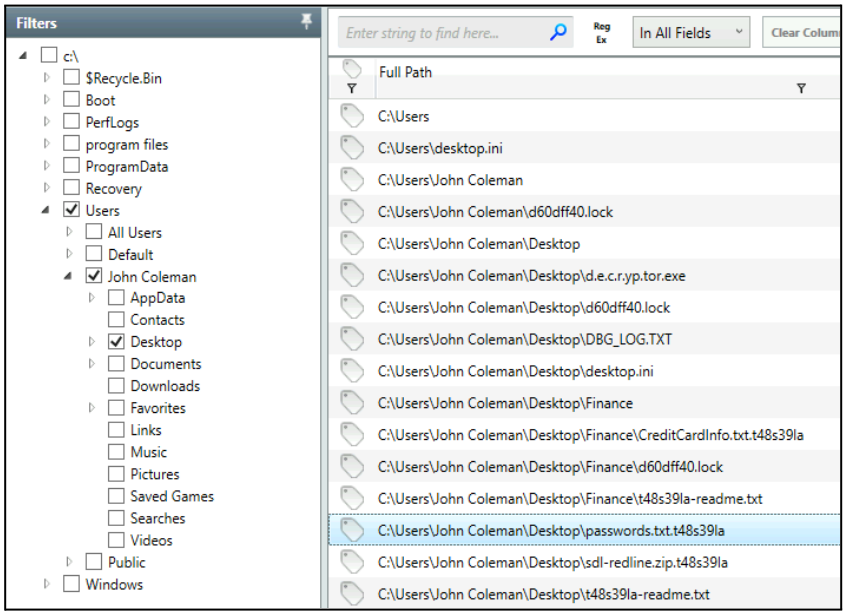


Image 8: Files renamed.

In the same section we can find a descriptor file and a readme me file with some extra characters.

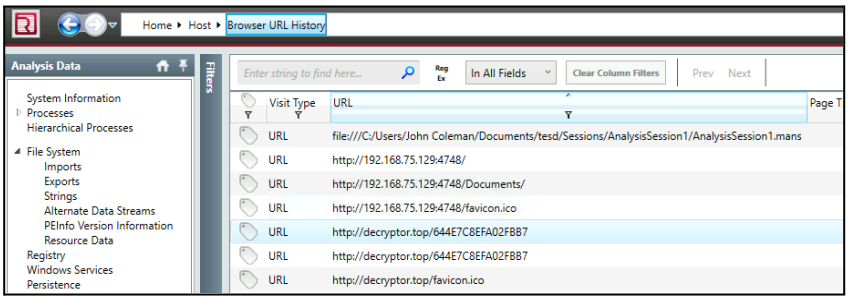


Image 9: Decrypt file.

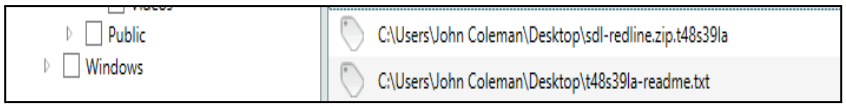


Image 10: Readme file.

Note: In such a readme file, it contains the same name format as the extensions so that’s a sign for a possible decryption attempt for free.

Step 4:
Click “Time Line” followed by adding “.t48s39la” in the search bar, we are able to see the total amount of files changed with this extension and are encrypted.

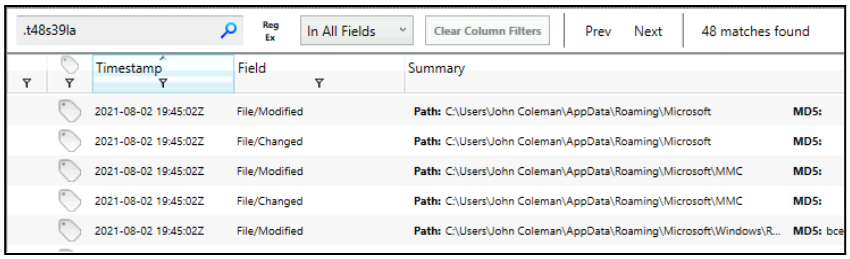


Image 11: Total matches.

Note: 48 was the total amount of coincidences but we might need to consider some files are replicated so they might even see less.

Step 5:
Locate yourself one more time in “File System " section followed by checking boxes for “Users”, “John Coleman” and “Downloads”.

Step 6:
Find and select the “WinRAR2021” file.

Step 7:
Scroll right the bottom slidebar and find the MD5 column in there we are able to get file MD5 hash value.

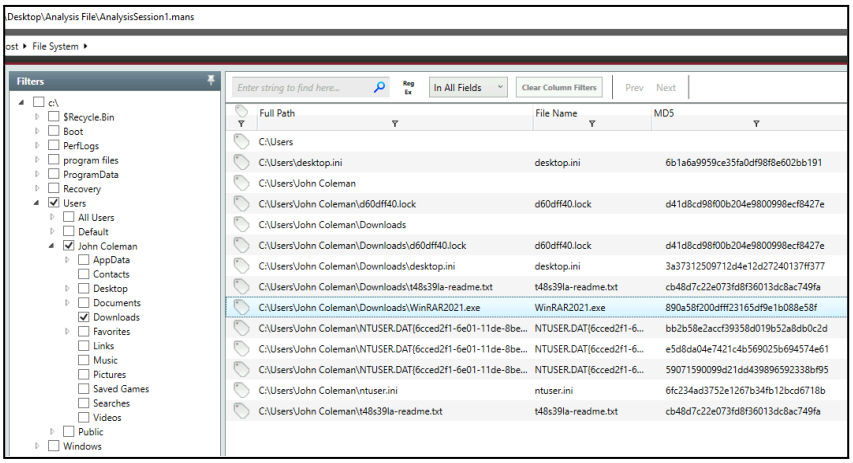


Image 12: MD5 hash value.

VirusTotal Result:
Step 1:
Copy MD5 hash value “890a58f200dfff23165df9e1b088e58f” and navigate to virus total website. Link in links section.

Step 2:
Select “Search” option and paste the previous MD5 hash value.

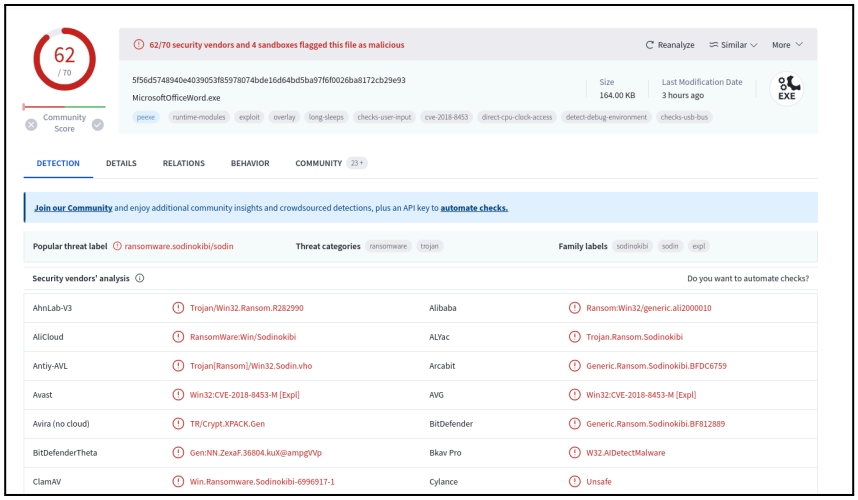


Image 13: Analysis result.

We can see a total of 62 from 70 antiviruses were able to detect it as malicious and it is denoted under “Sodinokibi” name by the community

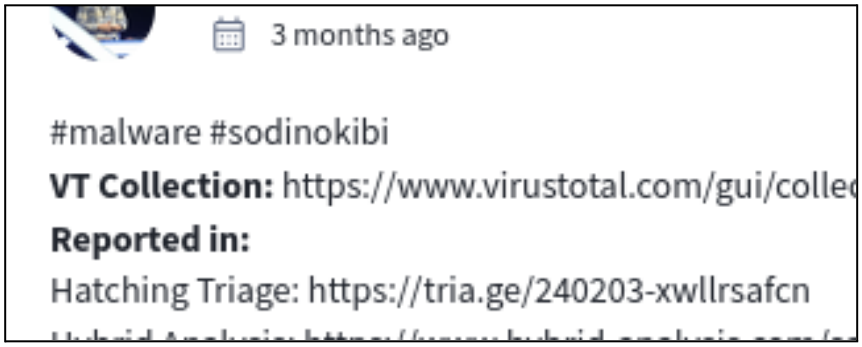


Image 14: Community.

Recommendations.

Restore backups files to retrieve as much information as possible before the inicident.

Links.

Installation:
https://fireeye.market/apps/211364
https://www.virustotal.com/gui/home/upload