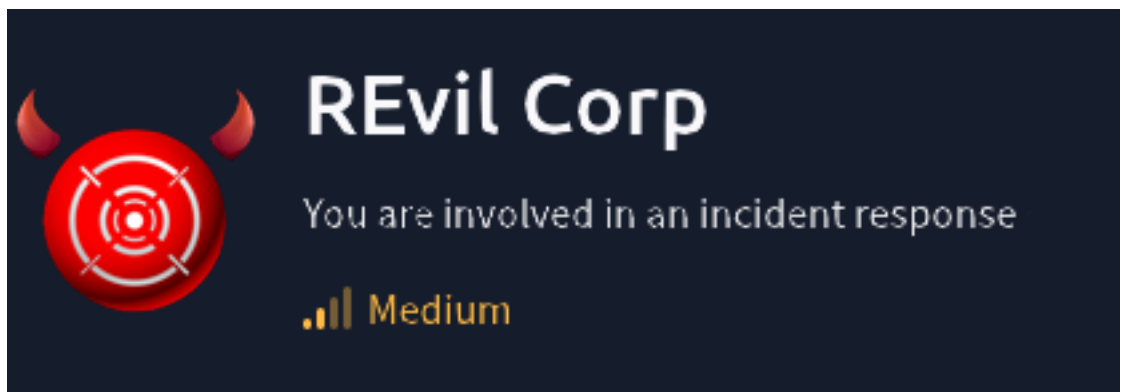


Incident Report

Client: Lockman Group



TeamWork:
- Sh3llr1ck0

Content.

Executive	03
Incident Report	
Investigation	04
Configuration Steps.	
Running and Importing Script.	
Analysis Incident.	
VirusTotal Result.	
Recommendations.	
Links	10

Lockman Group

Incident Report

EMPLOYEE DETAILS

NAME	John Coleman
DEPARTMENT	Operations
PHONE NUMBER	N/A

DESCRIPTION OF INCIDENT

Location: Reserved	
Date: 11/04/2023	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.
Time: 9:00 a.m.	
Police Notified: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	

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

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: Independent

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.

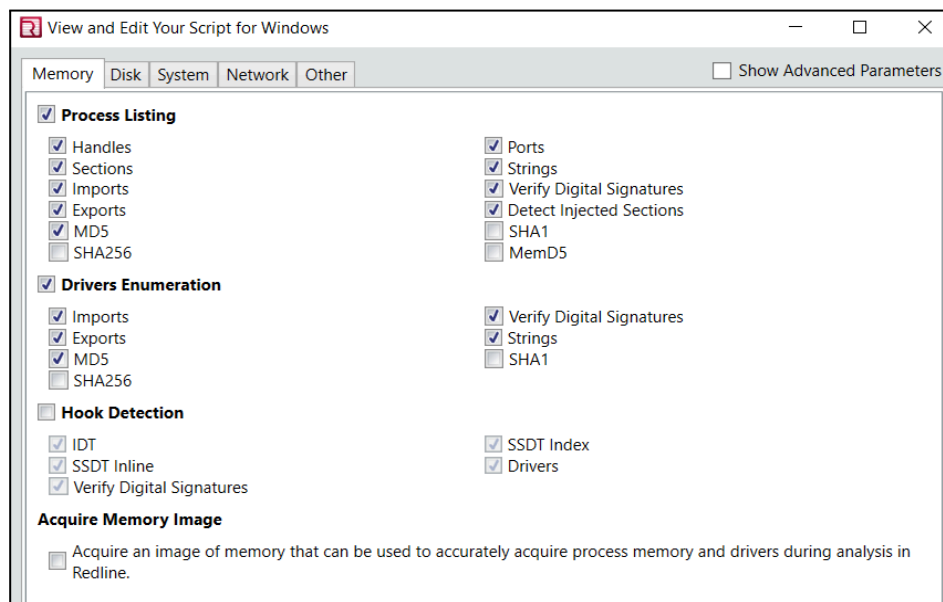


Image 1: Memory section configuration.

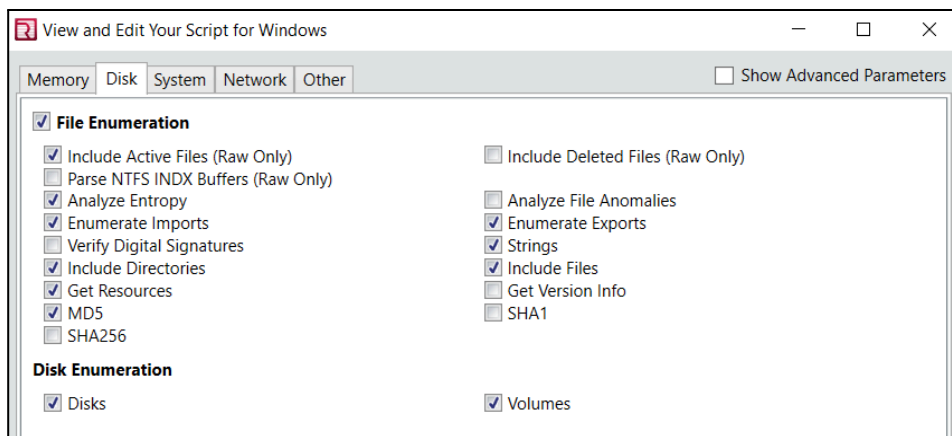


Image 2: Disk section configuration.

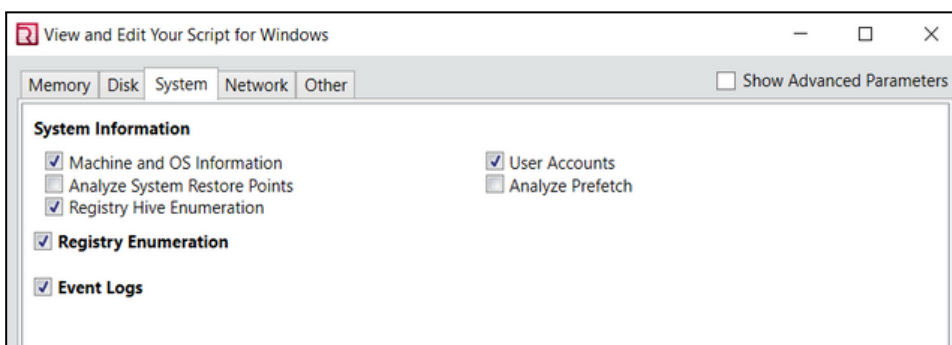


Image 3: System section configuration.

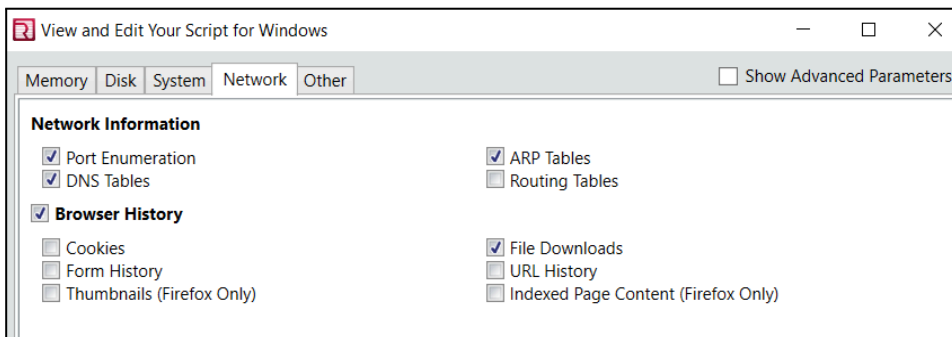


Image 4: Network section configuration.

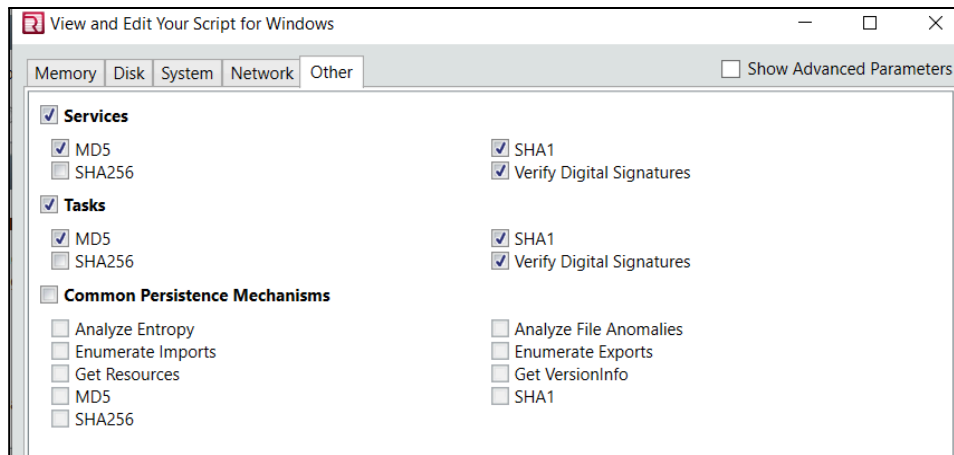
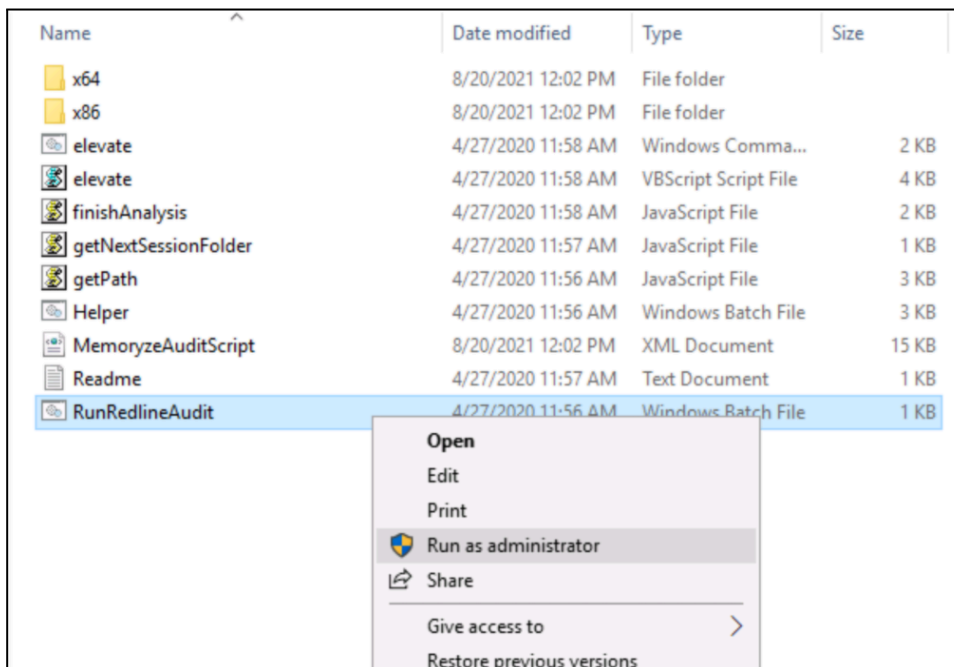


Image 5: Other section configuration.

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.

Operating System Information	
Operating System:	Windows 7 Home Premium 7601 Service Pack 1
Product Name:	Windows 7 Home Premium
Patch Level:	Service Pack 1
OS Build:	7601
Product ID:	00359-112-0000007-85772
System directory:	C:\Windows\system32
Install Date:	2021-08-02 19:04:38Z
Operating System Bitness:	32-bit

User Information	
Registered Owner:	Windows User
Registered Organization:	Not Available
Domain:	WORKGROUP
Logged in User:	John Coleman
Logged on User:	WIN-HKKQB6M7FTQ\John Coleman,WORKGROUP\WIN-HKKQB6M7FTQ\$

Image 6: System information

Step 2:

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

Host ▶ File Download History ▶ Full Detailed Information	
File Download Information	
Type:	Auto
Source URL:	http://192.168.75.129:4748/Documents/WinRAR2021.exe
Target Directory:	C:\Users\John Coleman\Downloads\WinRAR2021.exe
Filename:	Not Available
Temporary Path:	Not Available
File Size:	164 Kilobytes
Bytes Downloaded:	164 Kilobytes
State:	Not Available
MIME Type:	Not Available
Referrer:	Not Available
Can Auto Resume:	Not Available
Cache Flags:	Not Available
Cache Hits:	0
Full HTTP Header:	Not Available

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.

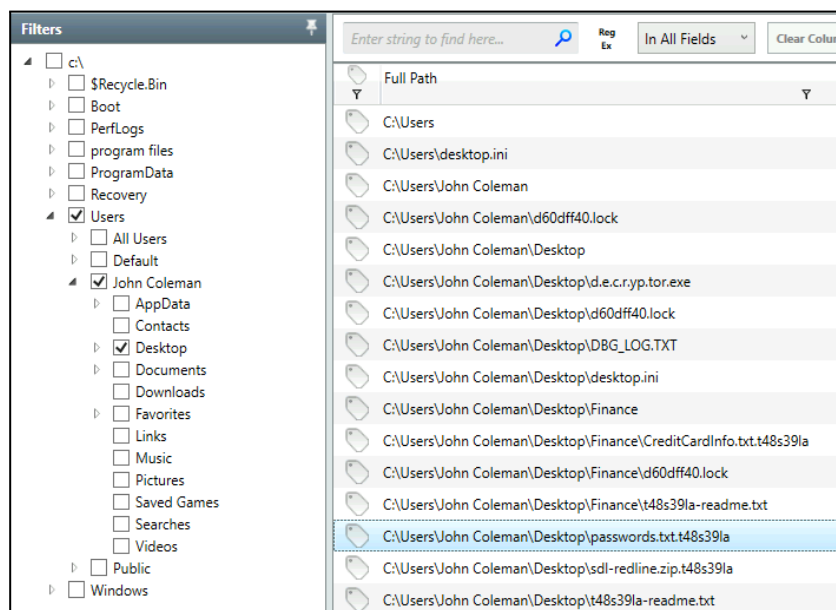


Image 8: Files renamed.

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

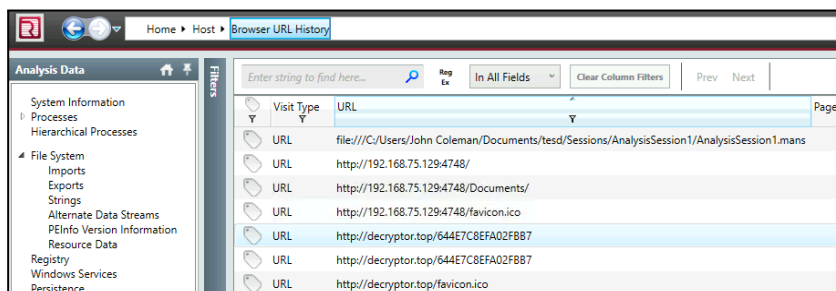


Image 9: Decrypt file.

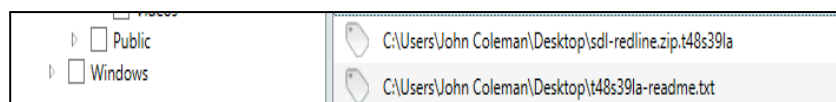
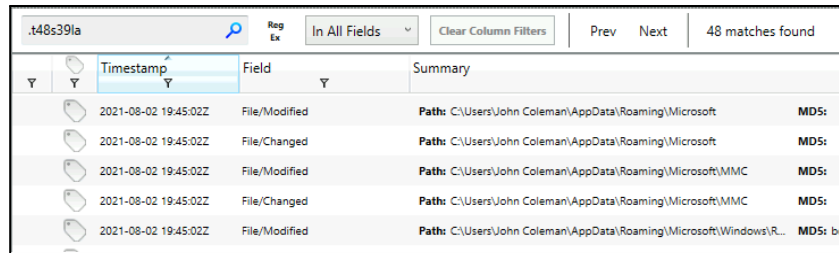


Image 10: Readme file.

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 “.t48s391a” in the search bar, we are able to see the total amount of files changed with this extension and are encrypted.



Timestampt	Field	Summary
2021-08-02 19:45:02Z	File/Modified	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft MD5:
2021-08-02 19:45:02Z	File/Changed	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft MD5:
2021-08-02 19:45:02Z	File/Modified	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\MMC MD5:
2021-08-02 19:45:02Z	File/Changed	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\MMC MD5:
2021-08-02 19:45:02Z	File/Modified	Path: C:\Users\John Coleman\AppData\Roaming\Microsoft\Windows\I... MD5: bce

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:

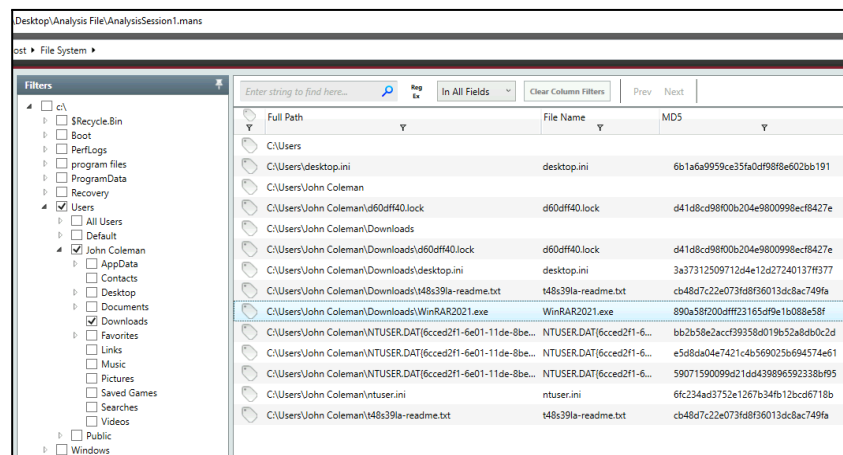
Locate yourself one more time in “File System ” section followed by checking boxes for “Users”, “John Coleman” and “Downloads”.

Step 6:

Find and select the “WinRAR2021” file.

Step 7:

Scroll right the bottom sidebar and find the MD5 column in there we are able to get file MD5 hash value.



Full Path	File Name	MD5
C:\Users		
C:\Users\desktop.ini	desktop.ini	6b1a6a9959ce35fa0df98f8e602bb191
C:\Users\John Coleman		
C:\Users\John Coleman\desktop.ini	desktop.ini	d41d8cd98f00b204e9800998ecf8427e
C:\Users\John Coleman\Downloads		
C:\Users\John Coleman\Downloads\desktop.ini	desktop.ini	3a37312509712d4e12d27240137f9377
C:\Users\John Coleman\Downloads\t48s391a-readme.txt	t48s391a-readme.txt	cb48d7c22e073f8f96013dc8ac749fa
C:\Users\John Coleman\Downloads\WinRAR2021.exe	WinRAR2021.exe	890a58f200df9f23165d9e1c088e58f
C:\Users\John Coleman\NTUSER.DAT(6cced2f1-6e01-11de-8be...	NTUSER.DAT(6cced2f1-6...	bb2b58e2accf39358d019b52a8db0c2d
C:\Users\John Coleman\NTUSER.DAT(6cced2f1-6e01-11de-8be...	NTUSER.DAT(6cced2f1-6...	e5d8da04e7421c4b569025b694574e61
C:\Users\John Coleman\NTUSER.DAT(6cced2f1-6e01-11de-8be...	NTUSER.DAT(6cced2f1-6...	59071590099d21dd439896592338b995
C:\Users\John Coleman\ntuser.ini	ntuser.ini	6fc234ad3752e1267b34fb12bccd67118b
C:\Users\John Coleman\t48s391a-readme.txt	t48s391a-readme.txt	cb48d7c22e073f8f96013dc8ac749fa

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.

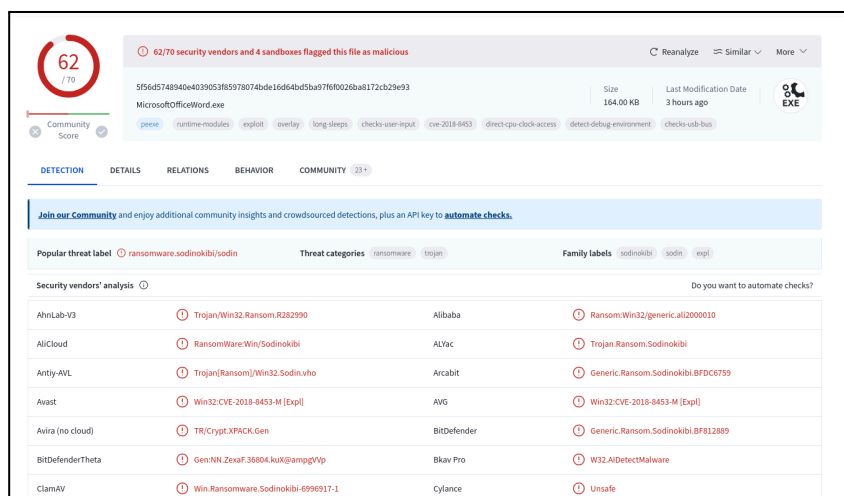


Image 13: Analysis result.

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

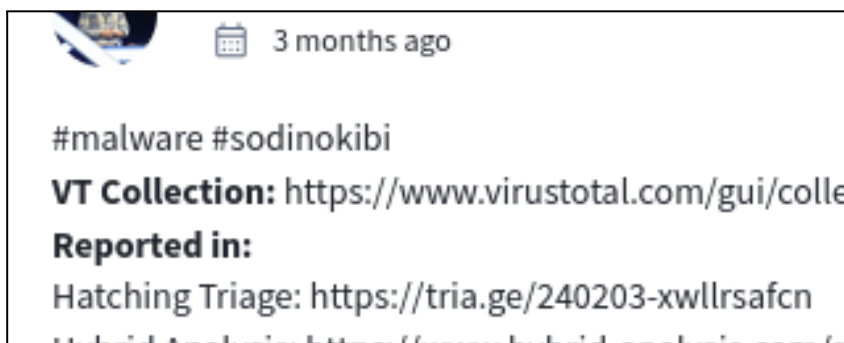


Image 14: Community.

Recommendations.

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

Links.

Installation:

<https://fireeye.market/apps/211364>

<https://www.virustotal.com/gui/home/upload>