National College of Ireland

Configuration Manual

MSc Research Project
MSc Cyber Security

Naresh Mantipally
Student ID: 22183973

School of Computing
National College of Ireland

Supervisor: Michael Pantridge

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Naresh Mantipally

Student ID: x22183973

Programme: MSc Cyber Security **Year:** 2023-2024

Module: Research Project

Lecturer: Michael Pantridge

Submission Due Date: 25.04.2024

Project Title: Empowering Ransomware Detection: Leveraging Splunk and Sigma Rules for Enhanced Security

Word Count: 864 **Page Count: 11**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Naresh.M

Date: 20.04.2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Empowering Ransomware Detection: Leveraging Splunk and Sigma Rules for Enhanced Security

Naresh Mantipally
Student ID:22183973

1 Introduction

This research enhances ransomware detection in Splunk by aligning strategies with MITRE ATT&CK. It develops Sigma rules focusing on File Overwrite and File Renaming tactics, mapped to MITRE techniques. A custom Go script aids in encryption/decryption testing. This empowers security teams with actionable insights, advancing cybersecurity.

2 System Requirements

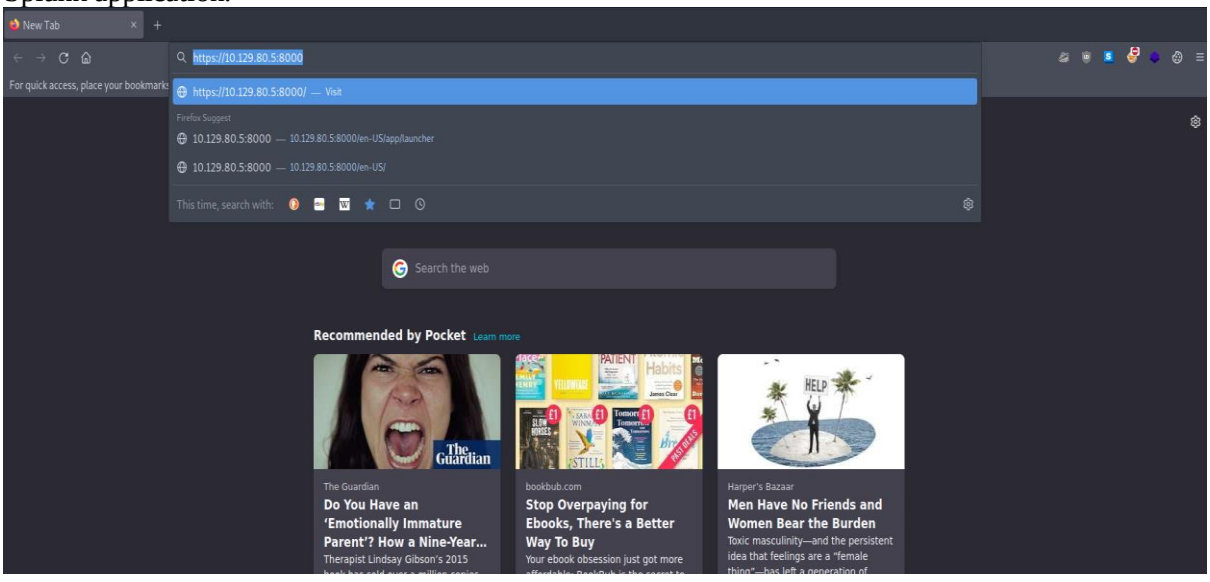
To implement this project, we require a cloud instance from Hack the box platform, which can be assessed through the link below. It expires every 120 minutes.
https://vnc.htb-cloud.com/?host=proxy-uk.htb-cloud.com/bird/htb-qevhd7m1lv.htb-cloud.com&password=oXt6vycz

2.1 Software Configuration

Hack the Box Setup:

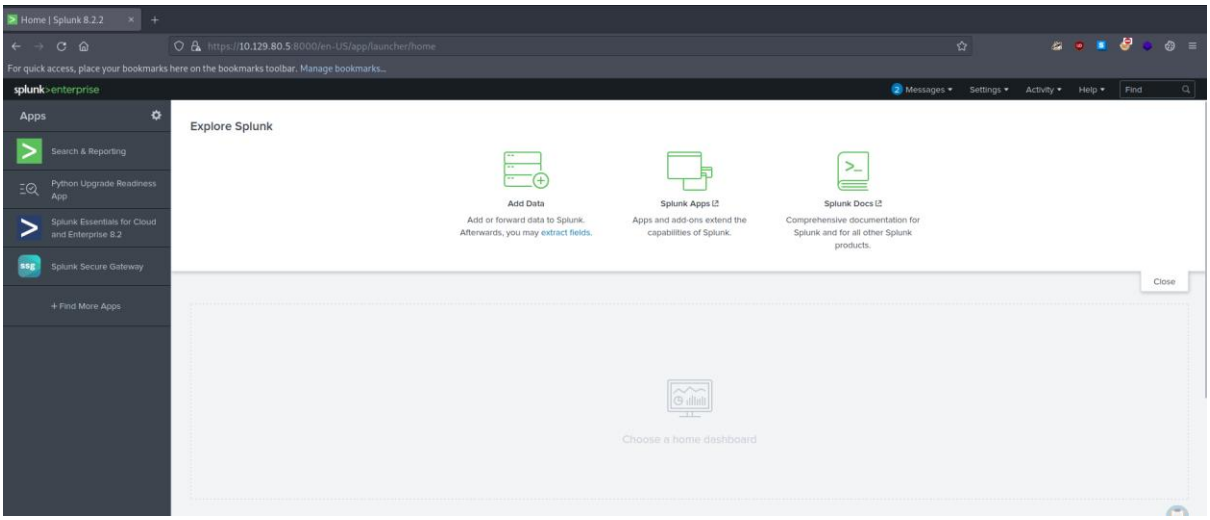
- Go to above link we can see a Linux based virtual machine.

Then, access the Splunk interface at https://10.129.80.5:8000 and launch the Search & Reporting Splunk application.

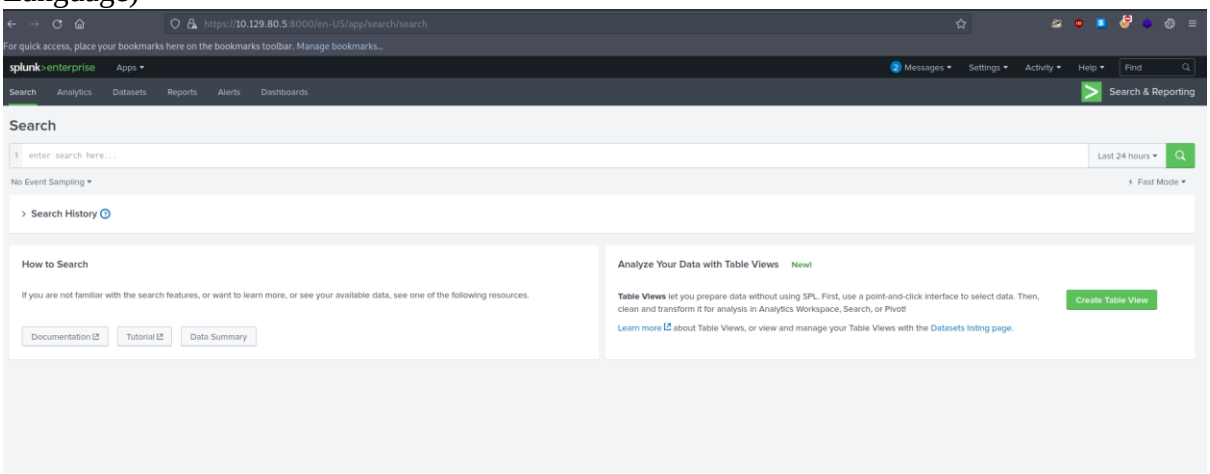


Seach and Reporting application

- Using the Splunk enterprise application by clicking on search and reporting application we can address the logs which are stored in another Linux machine which can access through RDP.

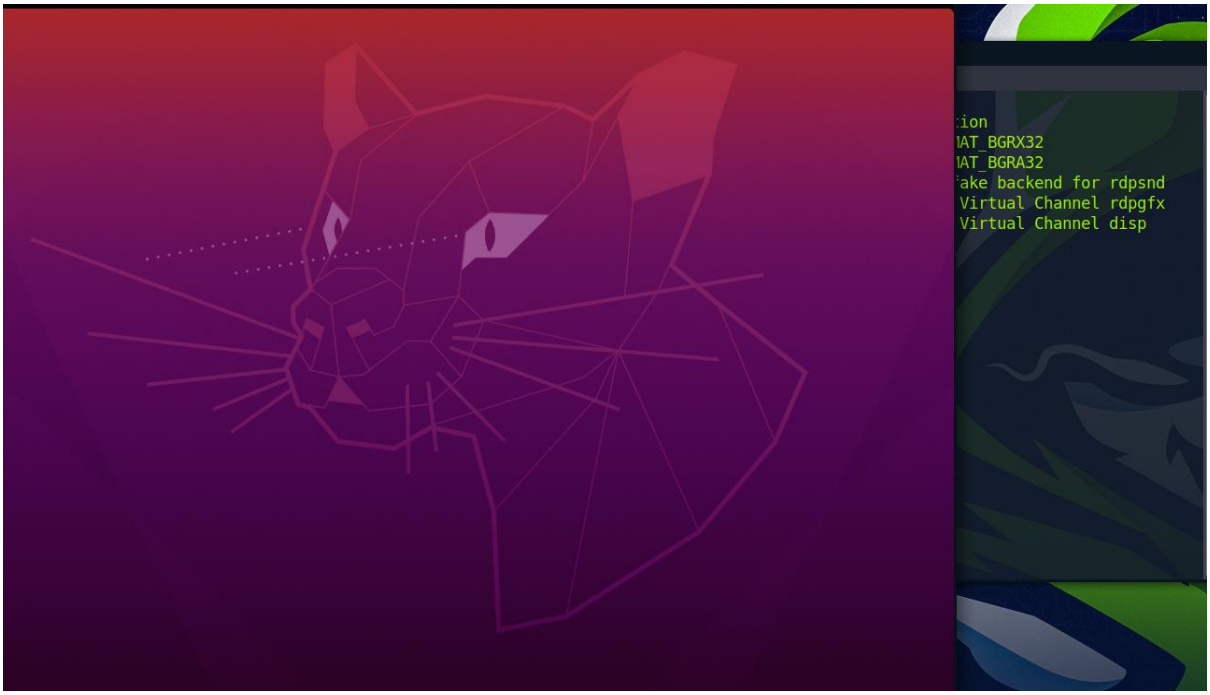


In search and reporting application we can find specific logs by using SPL (Splunk processing Language)

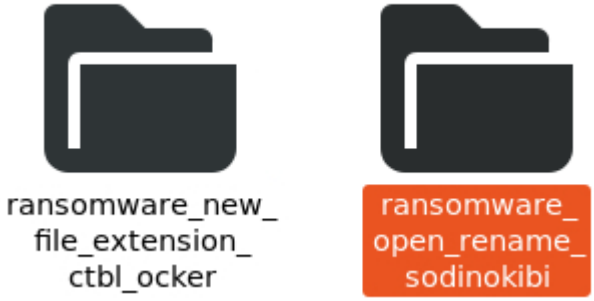


Other Linux machines can access by the spawned target via RDP as outlined below. All files, logs, and PCAP files related to the covered attacks can be found in the /home/htb-student and /home/htb-student/module_files directories.
Steps:
Step 1: Open the Parrot Terminal
Step 2: Enter the command as below.
xfreerdp /u:htb-student /p:'HTB_@cademy_stdnt!' /v:10.129.80.5 /dynamic-resolution

Step 3: Spawn the Linux based machine.



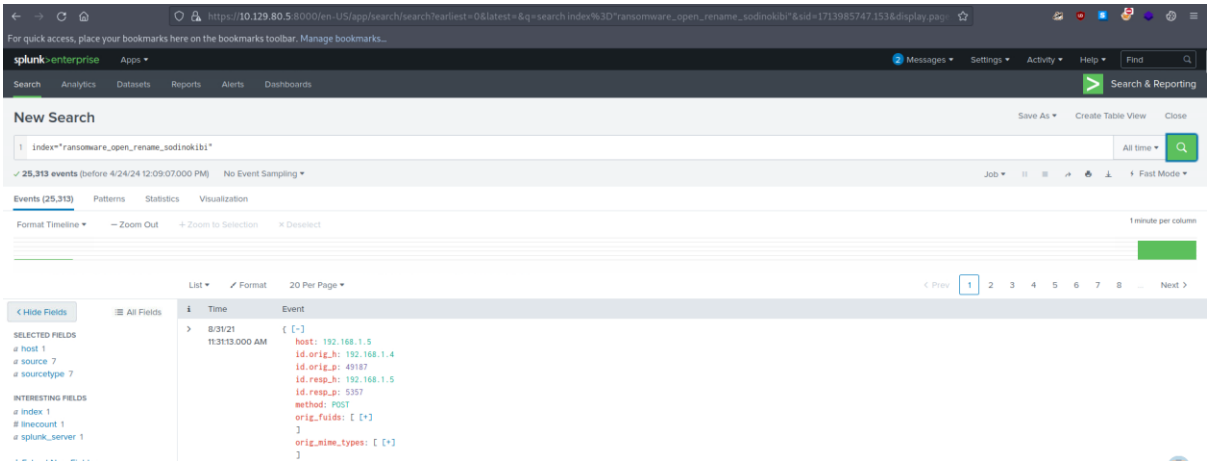
Step 4: All files, logs, and PCAP files related to the covered attacks can be found in the /home/htb-student and /home/htb-student/module_files directories.



The above files related to ransomware with Excessive Overwriting and excessive renaming with same Extension.

Detecting Ransomware with Splunk & Zeek Logs (Excessive Overwriting)

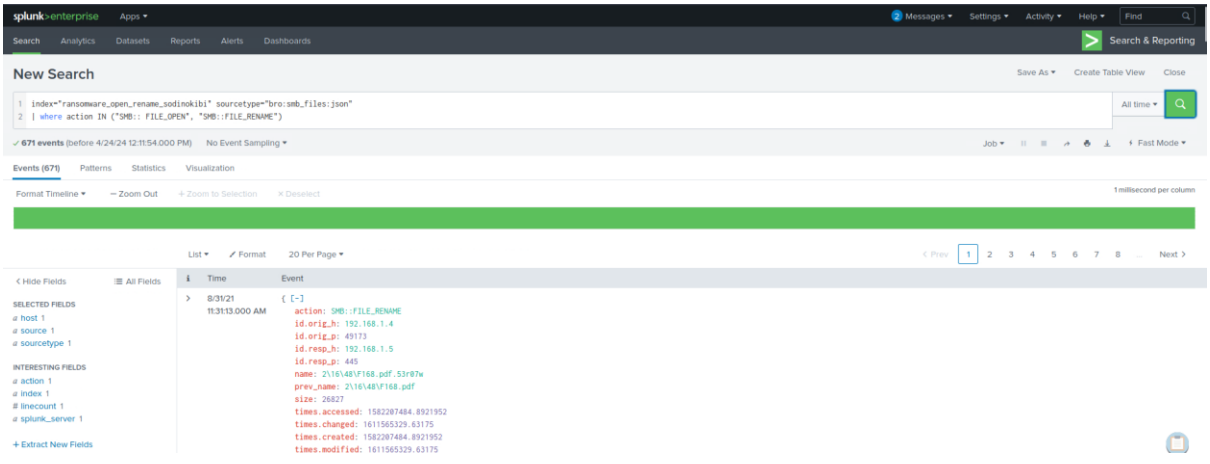
index="ransomware_open_rename_sodinokibi" sourcetype="bro:smb_files:json" action=" `SMB::FILE_OPEN` ,SMB::FILE_RENAME": This line filters the events based on the index, ransomware_open_rename_sodinokibi a specific sourcetype bro:smb_files:json, and the action SMB::FILE_RENAME. This effectively narrows the search to SMB file rename actions in the specified index.

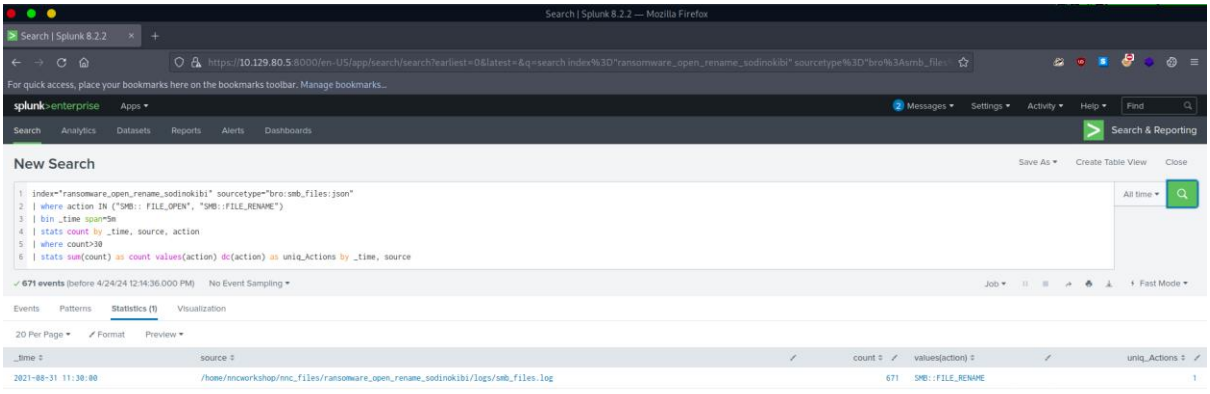


By following below query we can filter the logs to find the ransomware.

SPL Query:

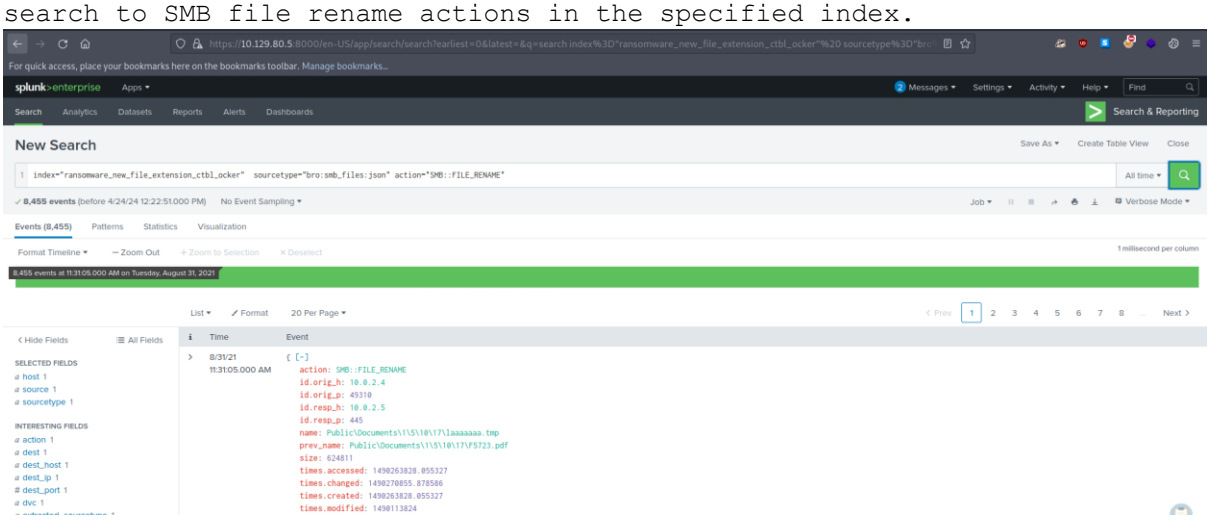
```
index="ransomware_open_rename_sodinokibi" sourcetype="bro:smb_files:json"
| where action IN ("SMB::FILE_OPEN", "SMB::FILE_RENAME")
| bin _time span=5m
| stats count by _time, source, action
| where count>30
| stats sum(count) as count values(action) dc(action) as uniq_actions by _time,
source
| where uniq_actions==2 AND count>100
```





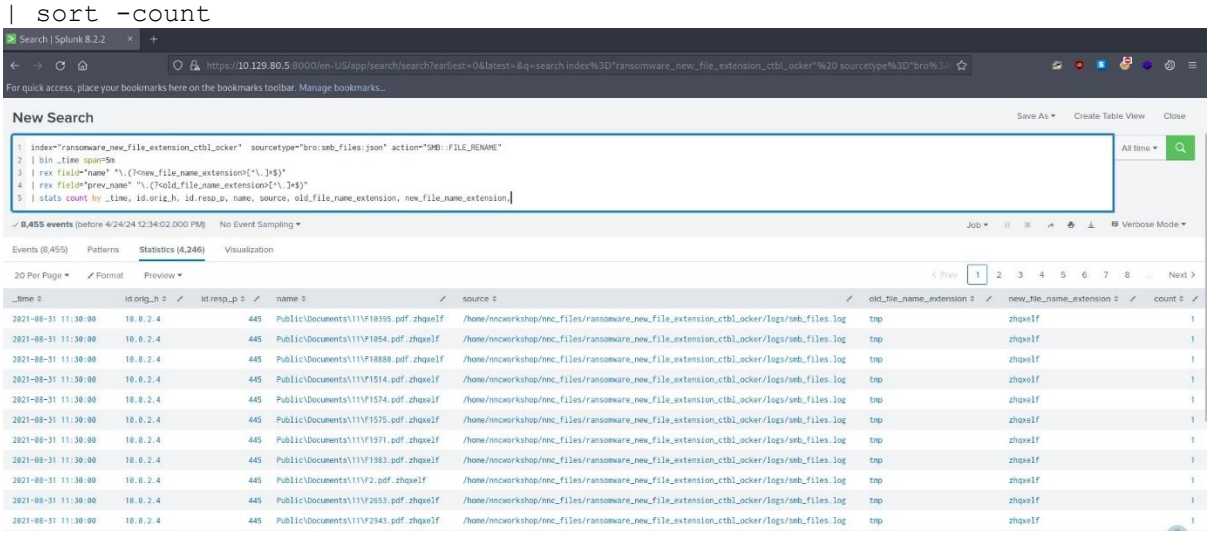
Detecting Ransomware with Splunk & Zeek Logs (Excessive Renaming With The Same Extension)

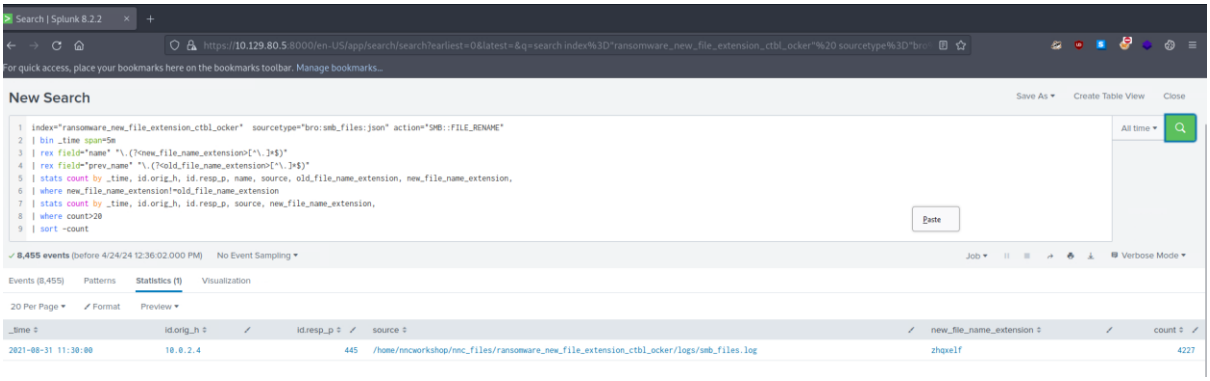
```
index="ransomware_new_file_extension_ctbl_ocker" sourcetype="bro:smb_files:json"
action="SMB::FILE_RENAME": This line filters the events based on the index
ransomware_new_file_extension_ctbl_ocker, a specific sourcetype
bro:smb_files:json, and the action SMB::FILE_RENAME. This effectively narrows the
search to SMB file rename actions in the specified index.
```



By following below query we can filter the logs to find the ransomware.

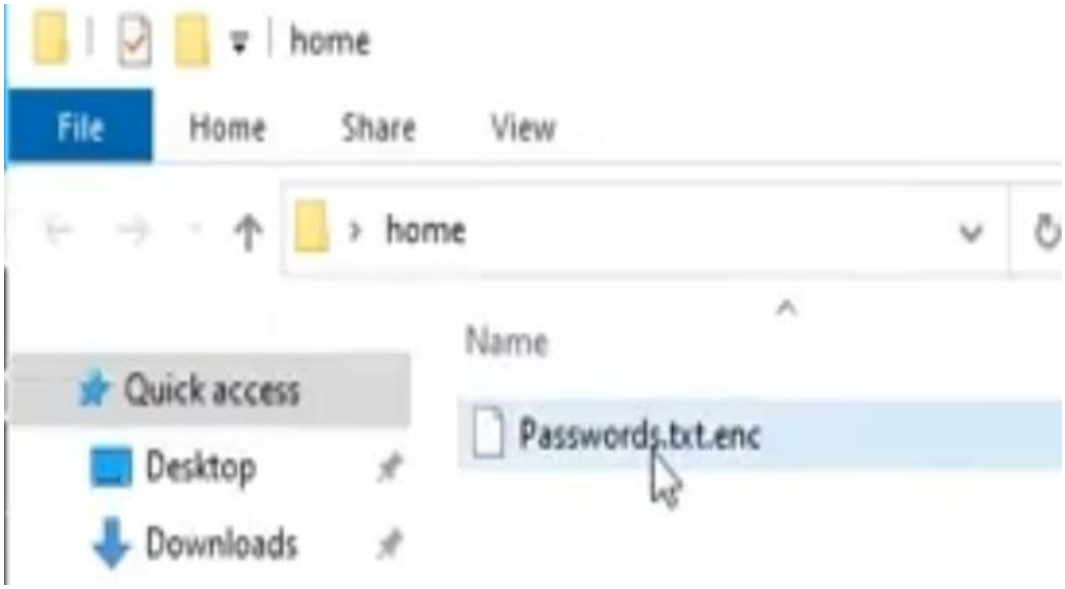
```
index="ransomware_new_file_extension_ctbl_ocker" sourcetype="bro:smb_files:json"
action="SMB::FILE_RENAME"
| bin _time span=5m
| rex field="name" "\.(?<new_file_name_extension>[^\.]*$)"
| rex field="prev_name" "\.(?<old_file_name_extension>[^\.]*$)"
| stats count by _time, id.orig_h, id.resp_p, name, source,
old_file_name_extension, new_file_name_extension,
| where new_file_name_extension!=old_file_name_extension
| stats count by _time, id.orig_h, id.resp_p, source, new_file_name_extension
| where count>20
| sort -count
```





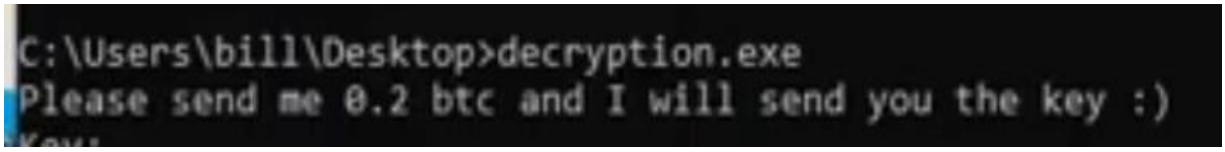
TESTING IN WINDOWS:
Custom GO script:

- Run the script in windows vm command prompt.
  We have a file called password.txt on my Desktop.
- 

- It will change the password.txt which is encryption file to password.txt.enc
- 

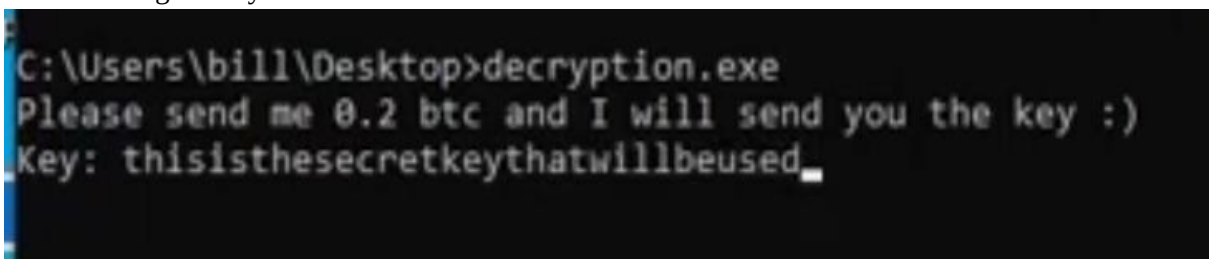
- Open the file with Notepad.

- We can see that file got encrypted when we try to decrypt it by command prompt.

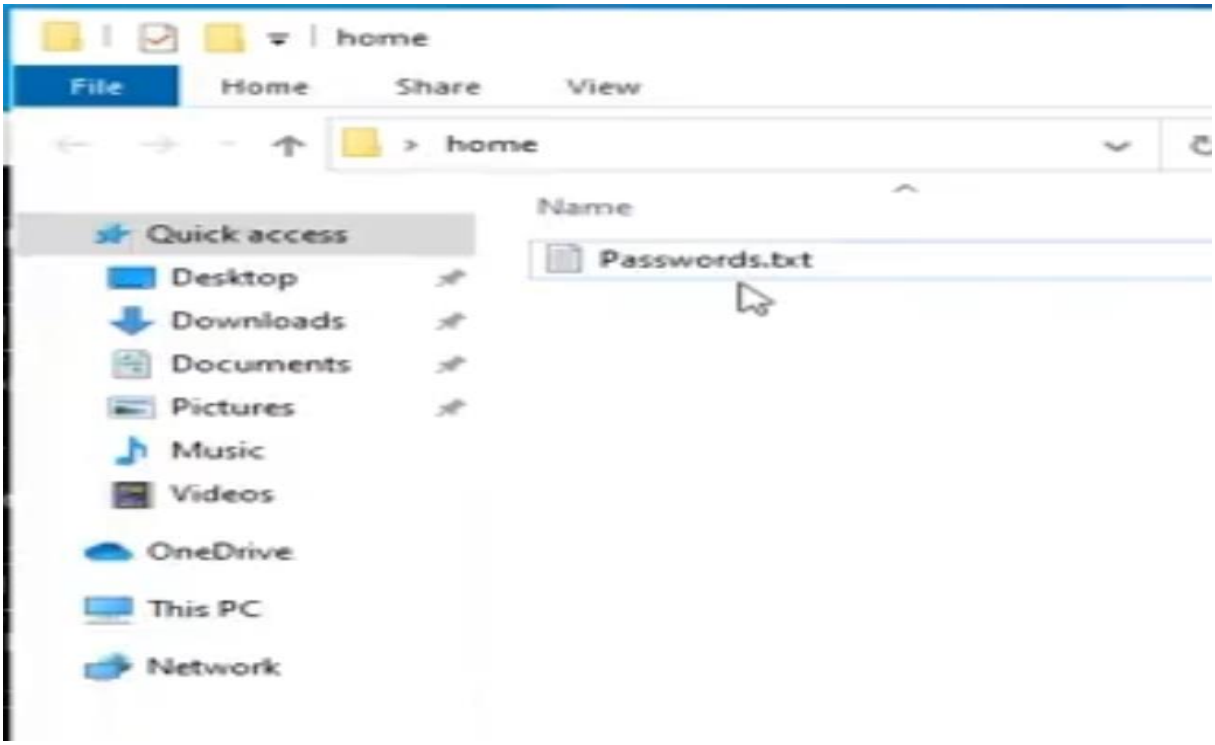


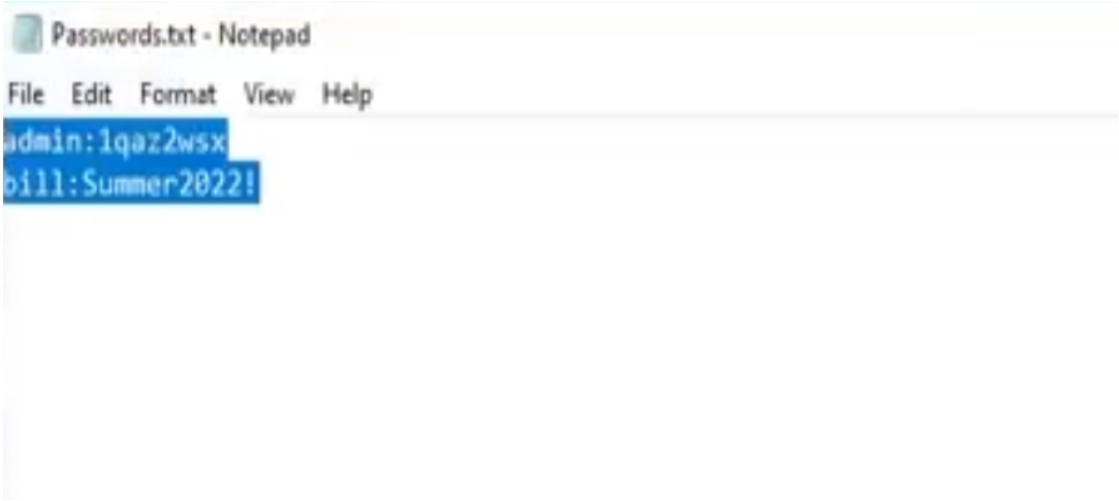
It ask for ransom, victim pay ransom it give the secret key which is "thisissecretkeythatwillbeused"

Decryption of file:
After entering the key

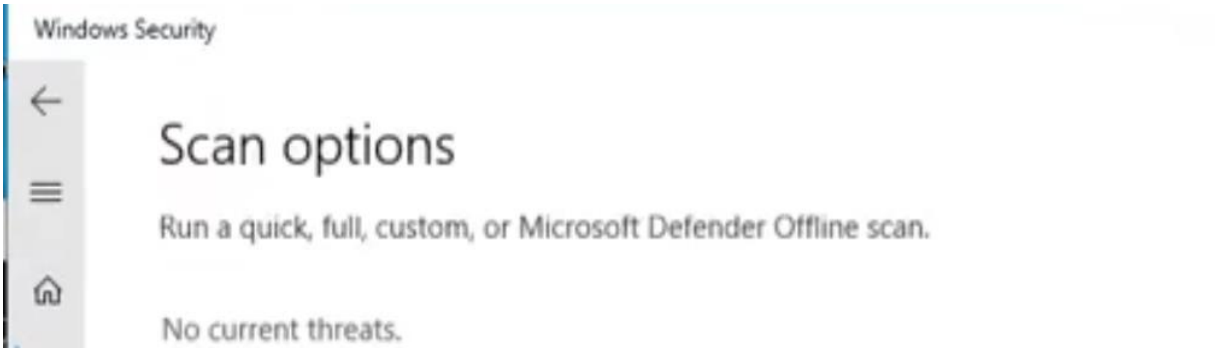


File changes from password.txt.enc to password.txt and the file content is decrypted.





Windows Defender evading.
It didn’t detect ransomware. It shows no threats.



Virus Total Results:

Surprisingly, we can only two of 75 vendors detected that encryption.exe is malicious.