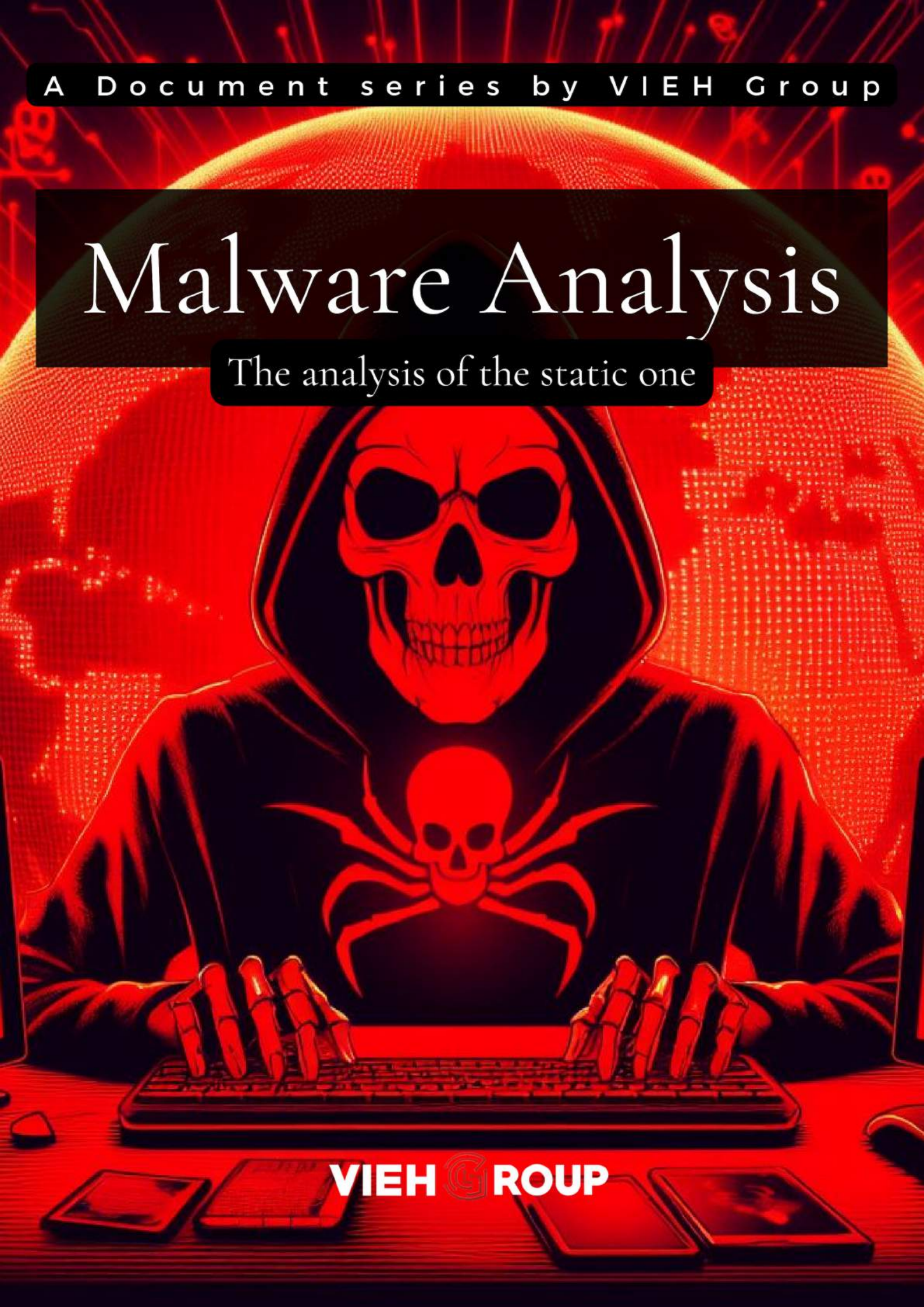
A Document series by VIEH Group

Malware Analysis

The analysis of the static one



VIEH GROUP

Disclaimer

Dear readers,
This document is provided by VIEH Group for educational purposes only. While we strive for accuracy and reliability, we make no warranties or representations regarding the completeness, accuracy, or usefulness of the information presented herein. Any reliance you place on this document is at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. We acknowledge and appreciate the contribution of the source person.

also,
This document is not created by a professional content writer so any mistake and error is a part of great design

Happy learning !!!

This document is credited to **Unknown (Can mail us for credit),** whose exceptional insights elevate its value. Their contribution is deeply appreciated, underscoring their significant role in its creation.

Our newsletter: **Cyber Arjun**

Scan QR:

STATIC ANALYSIS OF A MALWARE

File name:-
4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c.bin / Ransomeware-Petya

File type:- executable

Cpu type:- 32 bit

Okay let's go to analysis part...

❖ Steps that I have choose for my analysis

➢ First take a malware sample

➢ Check the hash value for the malware

➢ Check the file type whether it is executable or dll

➢ Check the malware whether it is packed or unpacked

➢ If the malware is packed then unpacke it

➢ Check the strings for the malware and search for any intresting strings is there or not

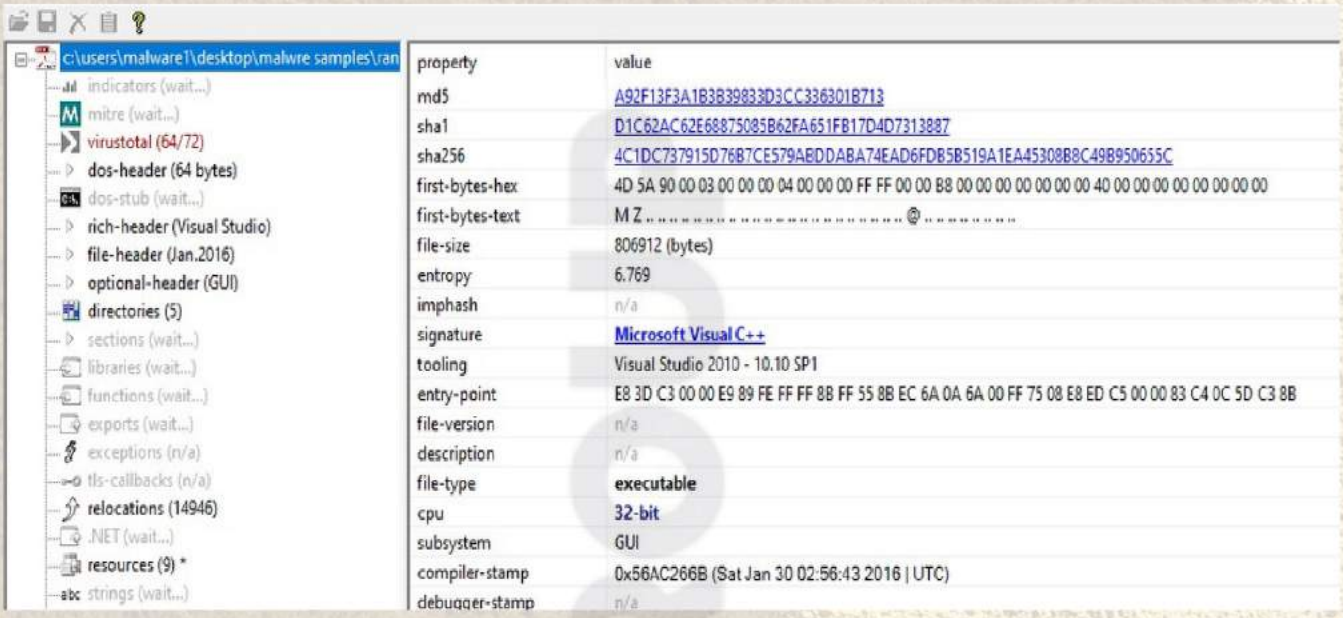
➢ Look for icons in the malware means which icons that the malware are using

➢If we want more information Look in to virus total for the best results

First check the hash of the malware it will help the other reseachers to do work and researching for that

MD5	a92f13f3a1b3b39833d3cc336301b713
SHA-1	d1c62ac62e68875085b62fa651fb17d4d7313887
SHA-256	4c1dc737915d76b7ce579abddaba74ead6fdb5b519a1ea45308b8c49b950655c

Then after take a sample of the malware and check it's file type in pestudio

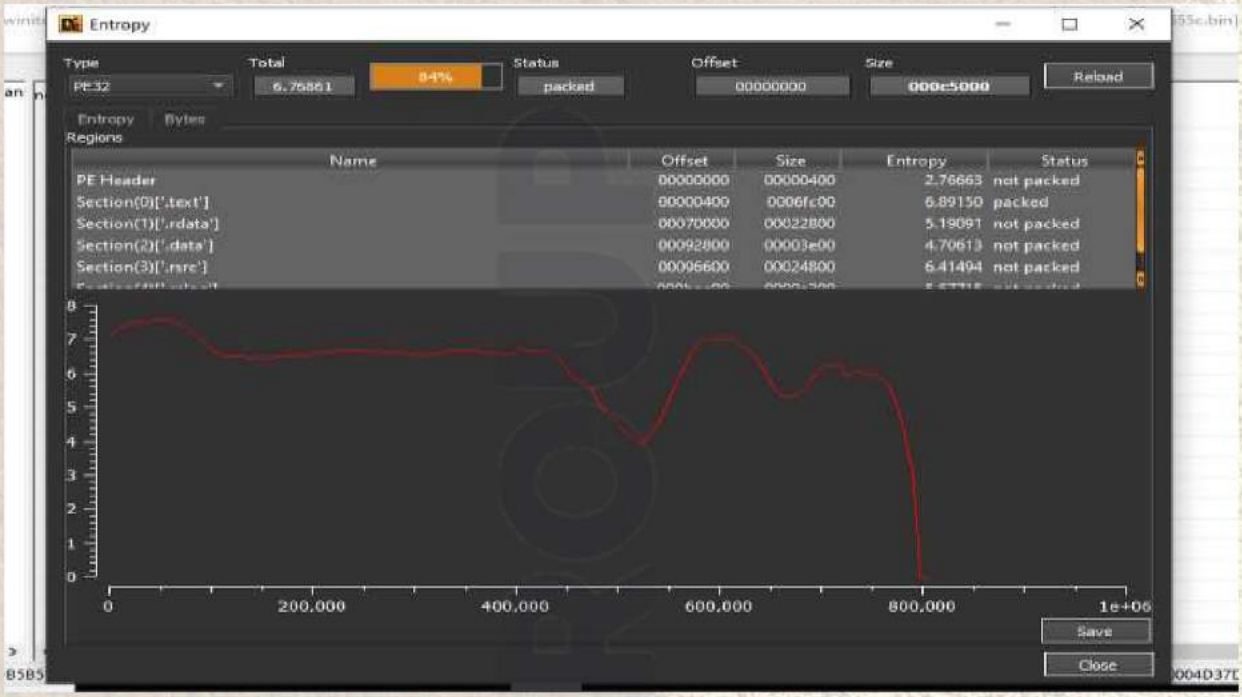


Ok the file is a .exe file and its cpu type is 32 bit

- Check the malware if it is packed or not in this we will be using exe pe info

Ok the malware is not packed

- Ok for our confirmation we will see another tool to check the malware is packed or not for this iam using tool called detect it easy



Yeah the malware is not packed

- After that we go to pe studio and search for the intresting strings

HttpConnection::connect
InternetCrackUrl failed
Invalid scheme
Http is disabled
InternetOpen failed
InternetConnect failed
HttpOpenRequest failed
HttpSendRequest failed
cannot get response status code
Export Denied
HttpConnection::connect succeeded
, size:
bytes
) returned unexpected size:
getHeaderValue(
HttpConnection::Response::getIntHeaderValue
, name=
Cannot get header value (
HttpConnection::Response::getHeaderValue
HttpConnection::Response::readContent
InternetReadFile failed
HttpConnection::Response::saveToBuffer
Http error, status:
MB), size is
Content size exceeds maximum size (
unknown

Here some of interesting strings it will makes connection to the internet

	registry	-	-	RegOpenKeyTransacted
	registry	-	-	RegCreateKeyTransacted
	registry	Defense Evasion	Modify Registry	RegDeleteKeyTransacted
	registry	Defense Evasion	Modify Registry	RegDeleteKeyEx
	registry	Defense Evasion	Modify Registry	RegSetValueEx
	registry	Discovery	Query Registry	RegQueryInfoKey
	registry	Defense Evasion	Modify Registry	RegDeleteKey
	registry	Discovery	Query Registry	RegEnumKeyEx
	registry	-	-	RegCreateKeyEx
	registry	-	-	RegOpenKeyEx
	registry	Defense Evasion	Modify Registry	RegDeleteValue
	registry	Discovery	Query Registry	RegQueryInfoKey
	registry	Discovery	Query Registry	RegQueryValueEx
	registry	Discovery	Query Registry	RegEnumKey
	registry	-	-	REGISTRY

And after that we see some more intresting strings in the above picture are modifying the registry

data-exchange	-	-	PeekNamedPipe
data-exchange	-	-	CreatePipe

This is how the malware can exchange the data with the help of these functions

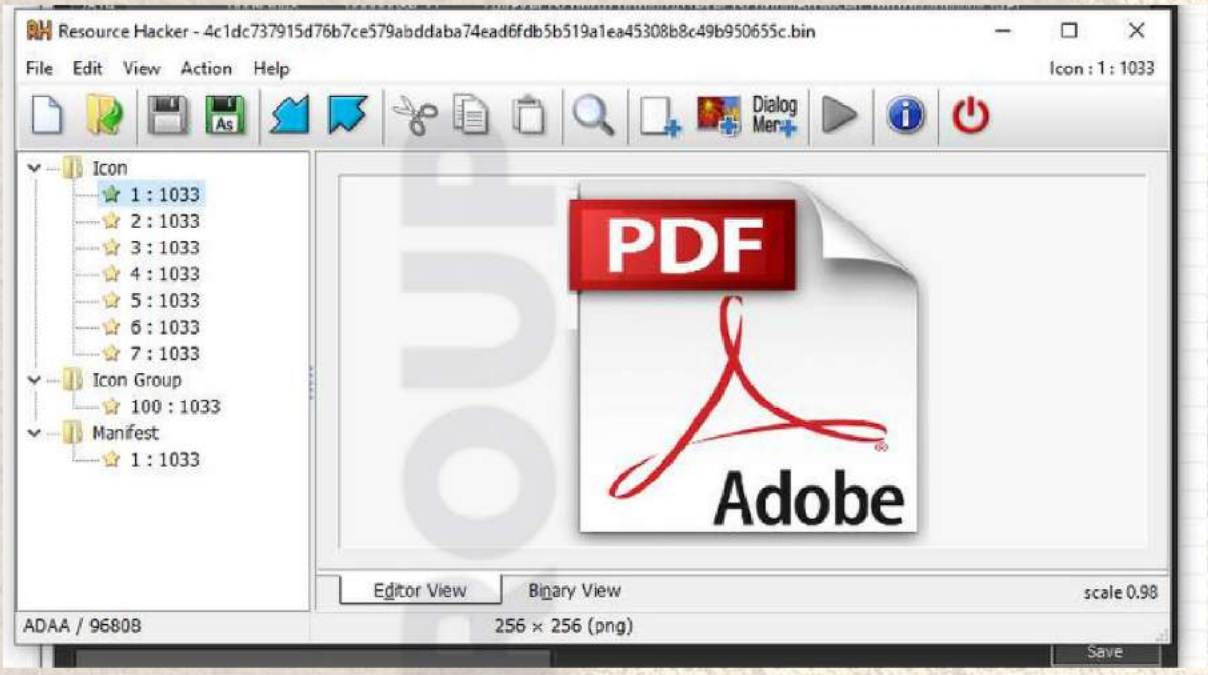
cryptography	-	-	CryptMsgGetParam
cryptography	-	-	CertFindCertificateInStore
cryptography	-	-	CryptCreateHash
cryptography	-	-	CryptHashData
cryptography	-	-	CryptGetHashParam
cryptography	-	-	CryptGetHashParam
cryptography	-	-	CryptReleaseContext
cryptography	-	-	CryptCreateHash
cryptography	-	-	CryptDestroyHash
cryptography	-	-	CryptHashData
cryptography	-	-	WinVerifyTrust
cryptography	-	-	CryptQueryObject
cryptography	-	-	CertFindCertificateInStore
cryptography	-	-	CertCloseStore
cryptography	-	-	CryptMsgGetParam
cryptography	-	-	CryptProtectData
cryptography	-	-	CryptUnprotectData
console	-	-	GetConsoleCP
console	-	-	GetConsoleMode
console	-	-	GetStdHandle
console	-	-	SetStdHandle

And here also some of intresting strings are these will do the process of cryptography functions encryptions

- The below are also some of intresting and strings

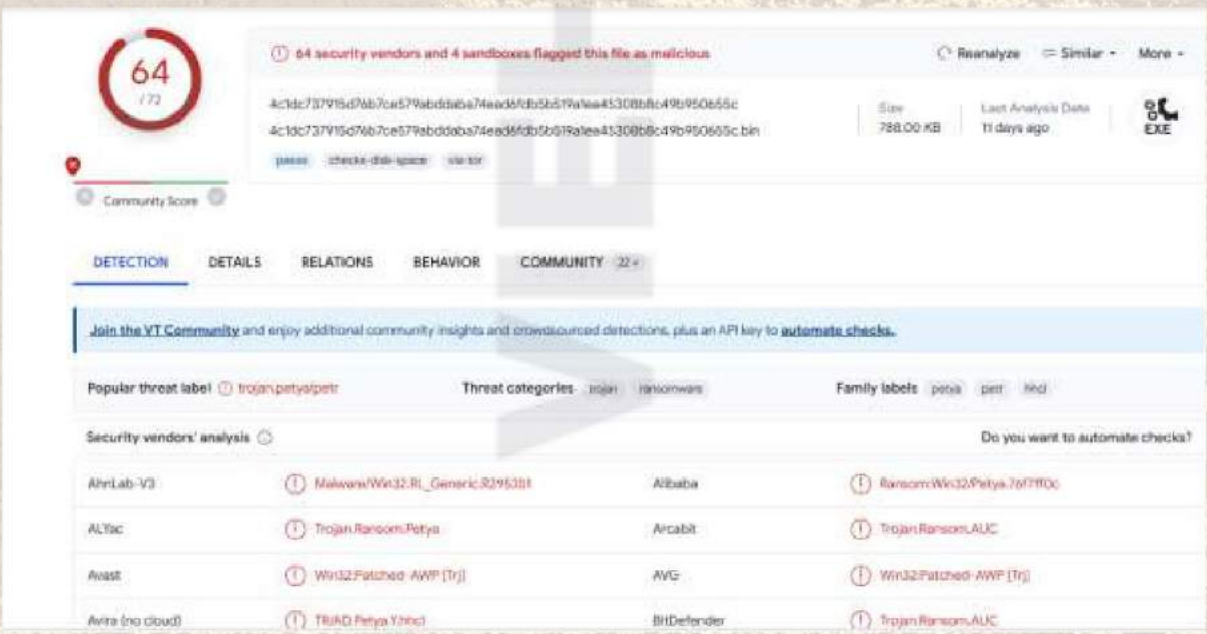
This makes the malware execute and exit the process

• And search for the icons is there any icons are usong the malware or not



Ok the malware is using the adobe pdf logo to fool the victims Using double extension methods

- Ok lets go to in to virus total to check how many av are detects the malware



Ok the virus total detects it and marks as score of 64/72

In that type of method we considered as the malware is ransomeware named as petya

We ill go to another process to see any domains are ther or not

Contacted Domains (3)

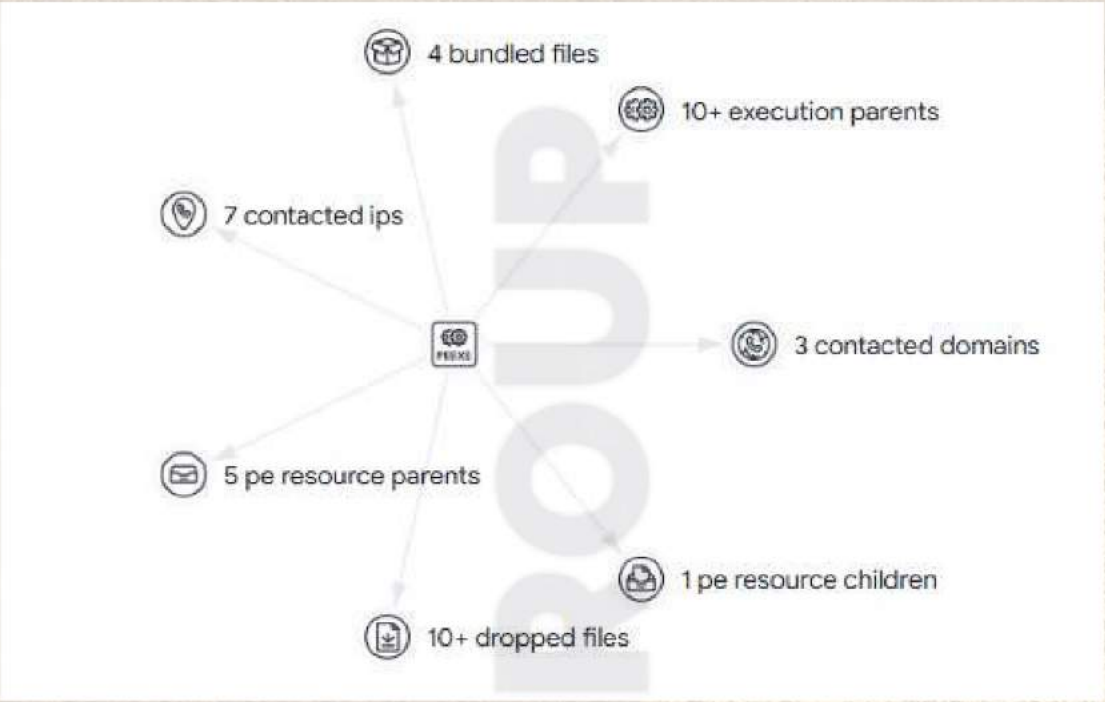
Domain	Detections
canonical-bos01.cdn.snapcraftcontent.com	0 / 88
canonical-lgw01.cdn.snapcraftcontent.com	0 / 88
www.msftconnecttest.com	0 / 88

Ok the malware connecting with these domains

Lets see is ther any ip's are there or not

IP	Detections	Autonomous System	Country
13.107.4.52	1 / 88	8068	US
185.125.188.57	0 / 88	41231	GB
185.125.190.26	0 / 88	41231	GB
185.125.190.27	0 / 88	41231	GB
185.125.190.28	0 / 88	41231	GB
91.189.91.42	0 / 88	41231	US
91.189.91.43	0 / 88	41231	US

Ok it will have some of ip's that to ping and communicate



This is the graph for the malware for wher the actions for that goes on

This is the overview of static analysis

Presenting the dynamic analysis of petya malware

Summary:- the malware is a ransomeware named as petya

What happens is when the the victim downloads any adobe document and any other document files in a malicious page the petya ransomeware is downnloaded with that

When the malware excutes it performs different function

Like:- send the data to the attacker

Lock the scrren and demand for the ransome

Cretes the files and deletes the files automatically

Changing the registries of the windows

And drooping some other malwares

And binding to other files in the computer

This is the overview of the dynamic analysis.

Thank you

Thank you for taking the time to read through our publication. Your continued support is invaluable.

Jai Hind!