Experiment-9

Implementation of IT Audit, Malware Analysis and Vulnerability Assessment and Generate the Report

Date: 11-11-24

AIM

Implementation of IT Audit, malware analysis and Vulnerability assessment and generate the report.

PROCEDURE

Step-1: Collect information about malware

Step-2: Get the basic information about malware

Step-3: Get the report from filescan.io and virustotal.com

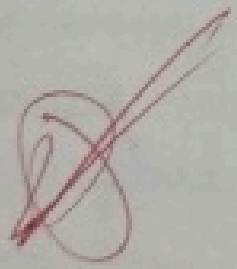
Step-4: Perform IT Audit to get the port information

SOURCECODE

Steps

1. Download the malware file from github / browser.
2. Go to the downloaded location of the malware file.
3. Give right click on the malware file and click on "extract here" now file.exe appears.

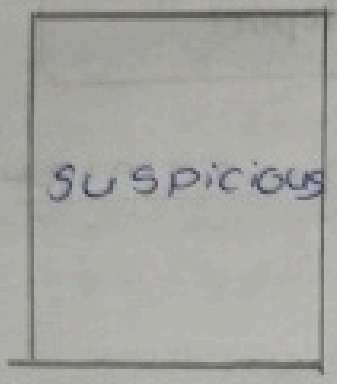
4. Now open browser and type filescan.io.
5. Now Drag and Drop the file.exe in it.
6. It shows the a dialog box it shows 4 ~~dio~~ options in that just select last option "I consent to the Terms of Use and Privacy Policy"
7. Click on upload.
8. Now it checks uploaded file whether it is malicious or not.



term and policy.
report of filescan.io

https://www.filescan.io/upload

overview;
verdict:



confidence:
100%

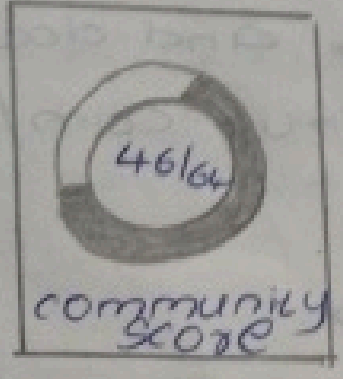
name: malwar.rar
SHA 256: d0168261c1a7aa
f4bb08a80a3cdf
f68b06

Report ID: 8355dc96-bea0-
4822-bc86-03fe
50ccd84b

submission date: 25/10/2024.
11:33:38 pm

now open virustotal.com browser

https://www.virustotal.com/gui/file



① 46/64 security vendor flagged this file

8440177dd7590d103
f9189999233f10
size 3fe506cd
42.5KB 846

malware.rar
rar

DETECTION	DETAILS	RELATION	BEHAVIOR	COMMUNITY
Popular threat ⓘ	Trojan.Swort/Cryptz		Threat: hacktool	
Security vendor's analysis ⓘ				
AhnLab-V3	ⓘ Trojan/Win32.Shell.R1283	Alicloud	ⓘ Trojan:Win/Rozena.A	
ALYac	ⓘ Trojan.CryptZ.Marte.1.Gen	Antiy-AVL	ⓘ Array Wasel/Win32.Tamp-ering.a	
Arcabit	ⓘ Trojan.CryptZ.Marte.1.Gen	Avast	ⓘ Win32:Meterpe-ter-C [Trj]	
AVG	ⓘ Win32-meterp-reter-C [Trj]	Avira (no cloud)	ⓘ TR/Patched.Gen2	
Bit Defend-er	ⓘ Trojan.Cryptz.Marte.1.Gen	ClamAV	ⓘ Win.Trojan.Swort.5710536-0	

25/9/24