

Experiment-9

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

Date: 28/8/25

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

Step1: Collect Information about malware
How a malware is collected.

Step2: Basic Information about malware:

Name: file.exe
Media Type: application/x-metadownload
SHA-256: f0d08621690cfa6ff16602ex054ff
3f3f586a80a.



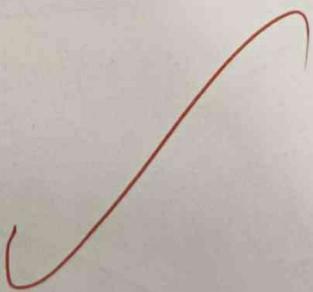
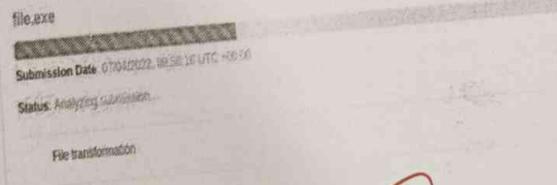
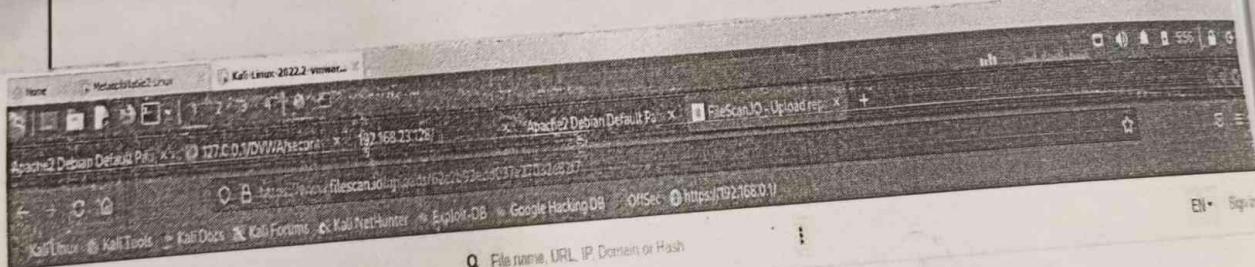
Information and Cyber Security

Report Id : 37cebe6-0978-4c35-9c63-
d177d1evesua

Submission Id : 62c24ef0978441af0d023de

Submission Date : 07/04/2022, 2:24:27

Step 3: Report from filescan.io.



trojan-downloader-implant/MSIL/Trojan-Dropper-MSIL-Arc...
AF2020.Godzilla.A!TrsS16P02390101:AF2-Arc...
020282722

No.: _____

Branch: _____

ASSIGNMENT - I / II
ACADEMIC YEAR : 2022-2023

The due date of each assignment in their login only.

50

① 50 security vendors and 1 suspicious flagged file for analysis

001d008216905ca7a041b001ec02e05d418e66b06cd3cb54fb353ba80a

71.07 KB
2022-07-09 10:00:00 UTC

Detected 2000

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Vendor	Signature	Ad-Aware	Avast
AegisLab-V3	Trojan-Win32-Shell-R1383	AV-Net	Trojan-Crypt2.Gen
Acabit	Trojan-Droj2.Gen	Bitdefender	Win32-Malicious-C.076
AVG	Win32-Meterpreter-0.Tng	Avira	Trojan-Downloader.Gen2
BitDefender	Trojan-Droj2.Gen	BitDefenderFree	Win32-Zoot!-32254-a0120e0c00000000
Box Pro	W32.FamiV3.RoyerNtro.Trojan	CleanAV	Win32-Trojan-Downloader.Gen2
Comodo	Trojan-Win32.Ricotta.AB!Rpsop	CrossStrike Falcon	Win32-Malicious_Perfmon_0000-00
CyberWise	Malicious-BIN6	Cynet	trojan
Qutter	PE32 Malicious-Header-1000	Cloud	PE32-Malicious-ArcorPowershell

File: file.exe

Submission Info

Name: file.exe
Media Type: application/x-msdownload
SHA-256: d01d008216905ca7a041b001ec05d418e66b06cd3cb54fb353ba80a
Report ID: 83554690-be6a-4822-bc88-03fe503c184a
Submission ID: 62c2b93dd037e27032a8217
Submission Date: 07/04/2022, 09:56:16

Download File Download Report

Scan State: ✓

Analysis Overview

Malicious Suspicious Unconfirmed

Verdict: Suspicious Confidence: 20%

Information and Cyber Security

OUTPUT

The screenshot shows a web browser window with the URL <https://filescan.io/>. The page displays the FileScan.io logo and the tagline "RAPID. IN-DEPTH." Below the logo is a large input field with the placeholder text "Drag & Drop For Rapid Analysis. Max file size is 100MB". Underneath the input field, there is a preview section showing a document titled "invoice.doc" from the URL <http://www.webpage.com/invoice.doc>. The preview shows some text and a red checkmark icon. At the bottom of the page, there is a brief description of the service: "FileScan.IO is a free malware analysis service that offers rapid in-depth file assessments, threat intelligence and indicator of compromise (IOCs) extraction for a wide range of executable files, documents and scripts. Learn more".