Malware Traffic Analysis

Introduction

You have been hired as a security analyst. You were tasked to determine any malicious activity associated with a malware attack.

You will have access to the internet to learn more about the events. You can use websites, such as VirusTotal, to upload and verify threat existence.

The tasks below are designed to provide some guidance through the analysis process.

You will practice and be assessed on the following skills:

- Evaluate event alerts using Squil.
- Use Google search as a tool to obtain intelligence on a potential exploit.
- Use VirusTotal to upload and verify threat existence.

Instructions

Part 1: Gather the Basic Information

In this part, you will review the alerts listed in Security Onion VM and gather basic information for the interested time frame.

Step 1: Verify the status of services

a. Log into Security Onion VM.

b. Open a terminal window. Enter the **sudo so-status** command to verify that all the services are ready.

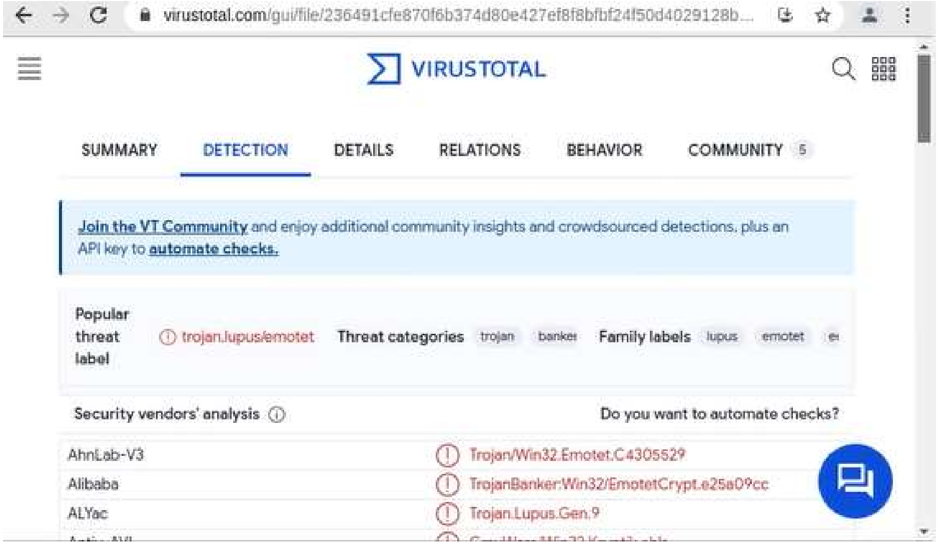
c. When the nsm service is ready, log into Sguil.sud

d. Download the .pcap file of yours and replay the malware packet capture. Before replaying the packet capture, update IDS rules using the command **sudo rule-update**.

Step 2: Gather basic information.

a. **What is the name of the trojan? Identify the time frame of the attack, including the date and approximate time.**

Trojan's name is trojan.lupus/emotet.



virustotal.com/gui/file/236491cfe870f6b374d80e427ef8f8bfbf24f50d4029128b...

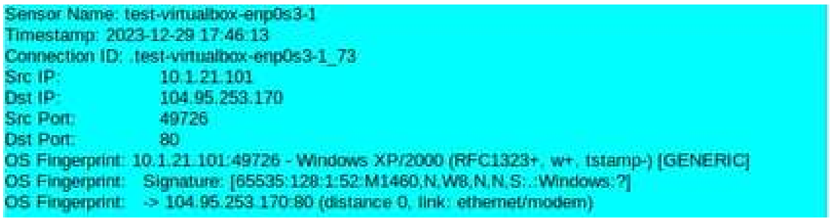
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.lupus/emotet   Threat categories: trojan, banker   Family labels: lupus, emotet, e

Security vendors' analysis   Do you want to automate checks?

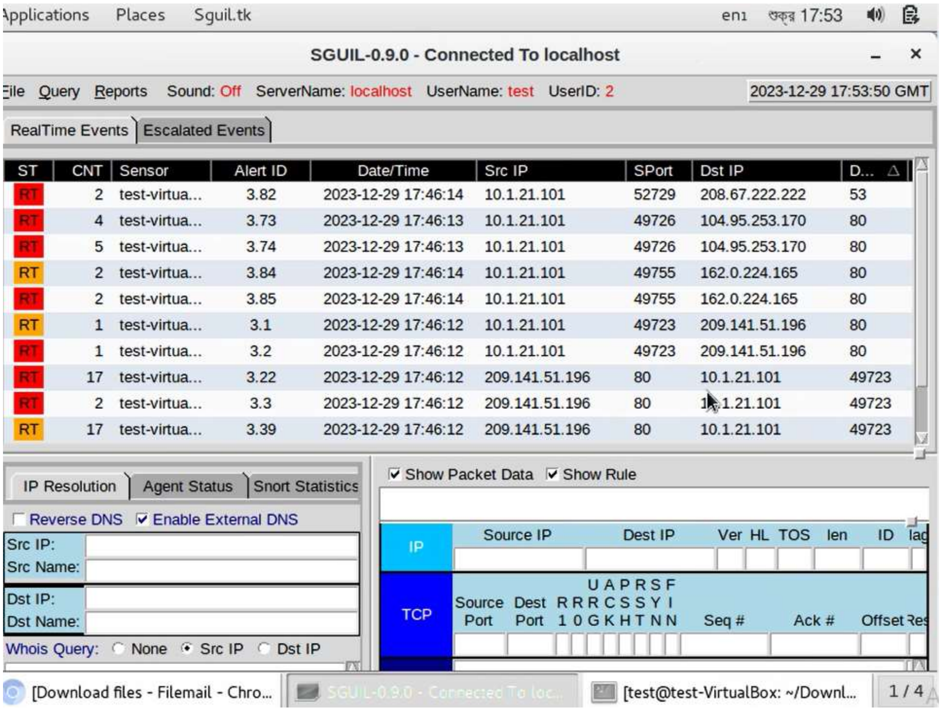
AhnLab-V3	Trojan/Win32.Emotet.C4305529
Alibaba	TrojanBanker:Win32/EmotetCrypt.e25a09cc
ALYac	Trojan.Lupus.Gen.9

Malware Traffic



```
Sensor Name: test-virtualbox-enp0s3-1
Timestamp: 2023-12-29 17:46:13
Connection ID: .test-virtualbox-enp0s3-1_73
Src IP:          10.1.21.101
Dst IP:          104.95.253.170
Src Port:        49726
Dst Port:        80
OS Fingerprint: 10.1.21.101:49726 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:   Signature: [65535:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:   -> 104.95.253.170:80 (distance 0, link: ethernet/modem)
```

Timestamp: 2023-12-29 17:46:13



Applications Places Squil.tk
en1 শুক্র 17:53
SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: test UserID: 2 2023-12-29 17:53:50 GMT

RealTime Events
Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	D...
RT	2	test-virtua...	3.82	2023-12-29 17:46:14	10.1.21.101	52729	208.67.222.222	53
RT	4	test-virtua...	3.73	2023-12-29 17:46:13	10.1.21.101	49726	104.95.253.170	80
RT	5	test-virtua...	3.74	2023-12-29 17:46:13	10.1.21.101	49726	104.95.253.170	80
RT	2	test-virtua...	3.84	2023-12-29 17:46:14	10.1.21.101	49755	162.0.224.165	80
RT	2	test-virtua...	3.85	2023-12-29 17:46:14	10.1.21.101	49755	162.0.224.165	80
RT	1	test-virtua...	3.1	2023-12-29 17:46:12	10.1.21.101	49723	209.141.51.196	80
RT	1	test-virtua...	3.2	2023-12-29 17:46:12	10.1.21.101	49723	209.141.51.196	80
RT	17	test-virtua...	3.22	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723
RT	2	test-virtua...	3.3	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723
RT	17	test-virtua...	3.39	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723

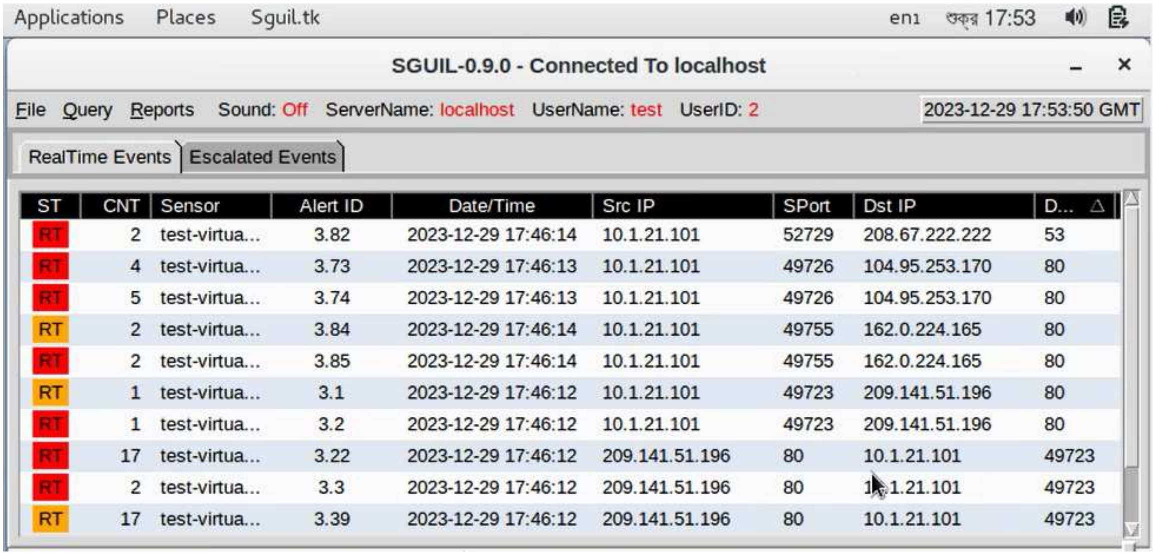
☐ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ○ None ● Src IP ○ Dst IP

☑ Show Packet Data ☑ Show Rule

b. List the alerts noted during this time frame associated with the trojan.



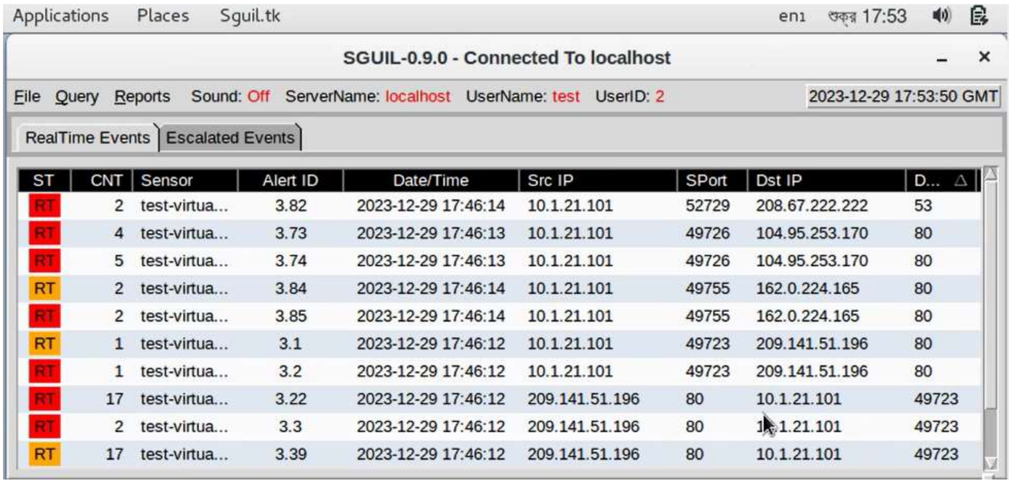
Applications Places Squil.tk
en1 শুক্র 17:53
SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: test UserID: 2 2023-12-29 17:53:50 GMT

RealTime Events Escalated Events

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	D...
RT	2	test-virtua...	3.82	2023-12-29 17:46:14	10.1.21.101	52729	208.67.222.222	53
RT	4	test-virtua...	3.73	2023-12-29 17:46:13	10.1.21.101	49726	104.95.253.170	80
RT	5	test-virtua...	3.74	2023-12-29 17:46:13	10.1.21.101	49726	104.95.253.170	80
RT	2	test-virtua...	3.84	2023-12-29 17:46:14	10.1.21.101	49755	162.0.224.165	80
RT	2	test-virtua...	3.85	2023-12-29 17:46:14	10.1.21.101	49755	162.0.224.165	80
RT	1	test-virtua...	3.1	2023-12-29 17:46:12	10.1.21.101	49723	209.141.51.196	80
RT	1	test-virtua...	3.2	2023-12-29 17:46:12	10.1.21.101	49723	209.141.51.196	80
RT	17	test-virtua...	3.22	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723
RT	2	test-virtua...	3.3	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723
RT	17	test-virtua...	3.39	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723

c. **List the internal IP addresses and external IP addresses involve**



Sound: Off ServerName: localhost UserName: test UserID: 2 2023-12-29 17:53:50 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	D... △
RT	2	test-virtua...	3.82	2023-12-29 17:46:14	10.1.21.101	52729	208.67.222.222	53
RT	4	test-virtua...	3.73	2023-12-29 17:46:13	10.1.21.101	49726	104.95.253.170	80
RT	5	test-virtua...	3.74	2023-12-29 17:46:13	10.1.21.101	49726	104.95.253.170	80
RT	2	test-virtua...	3.84	2023-12-29 17:46:14	10.1.21.101	49755	162.0.224.165	80
RT	2	test-virtua...	3.85	2023-12-29 17:46:14	10.1.21.101	49755	162.0.224.165	80
RT	1	test-virtua...	3.1	2023-12-29 17:46:12	10.1.21.101	49723	209.141.51.196	80
RT	1	test-virtua...	3.2	2023-12-29 17:46:12	10.1.21.101	49723	209.141.51.196	80
RT	17	test-virtua...	3.22	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723
RT	2	test-virtua...	3.3	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723
RT	17	test-virtua...	3.39	2023-12-29 17:46:12	209.141.51.196	80	10.1.21.101	49723

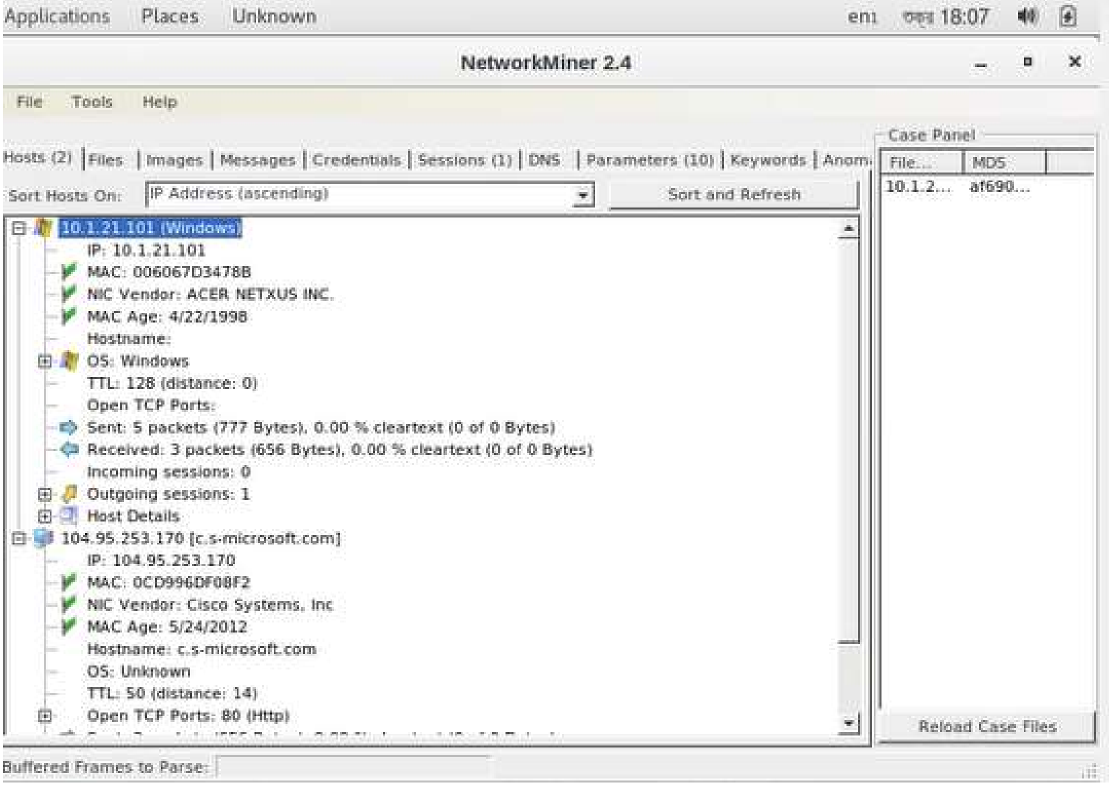
ere.

Part 2: Learn about the Exploit

In this part, you will learn more about the exploit.

Step 1: Infected host

a. **Based on the alerts, what is the IP and MAC addresses of the infected computer? Based on the MAC address, what is the vendor of the NIC chipset? (Hint: NetworkMiner or internet search**



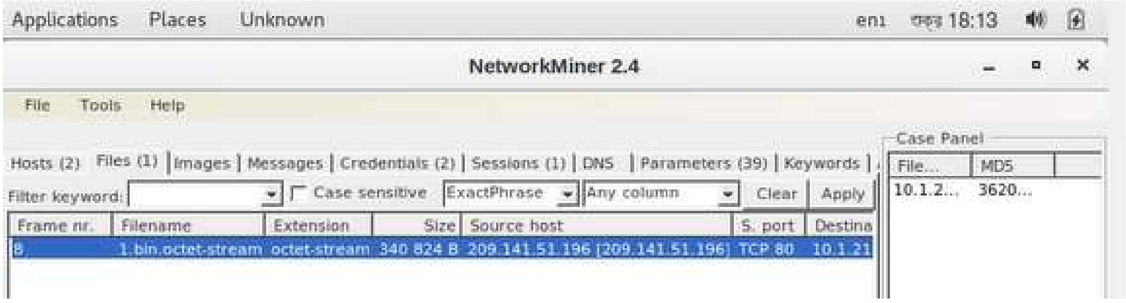
Sort Hosts On: IP Address (ascending)

```
10.1.21.101 (Windows)
    IP: 10.1.21.101
    MAC: 006067D3478B
    NIC Vendor: ACER NETXUS INC.
    MAC Age: 4/22/1998
    Hostname:
    OS: Windows
    TTL: 128 (distance: 0)
    Open TCP Ports:
    Sent: 5 packets (777 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Received: 3 packets (656 Bytes), 0.00 % cleartext (0 of 0 Bytes)
    Incoming sessions: 0
    Outgoing sessions: 1
    Host Details
104.95.253.170 [c.s-microsoft.com]
    IP: 104.95.253.170
    MAC: 0CD996DF08F2
    NIC Vendor: Cisco Systems, Inc
    MAC Age: 5/24/2012
    Hostname: c.s-microsoft.com
    OS: Unknown
    TTL: 50 (distance: 14)
    Open TCP Ports: 80 (Http)
```

10.1.2... af690...

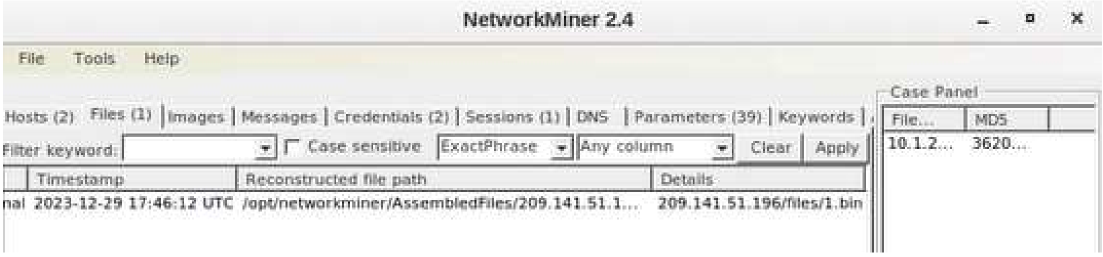
Buffered Frames to Parse:

b. **Based on the alerts, when (date and time in UTC) and how was the PC infected? (Hint: Enter the command date in the terminal to determine the time zone for the displayed time**



Frame nr.	Filename	Extension	Size	Source host	S. port	Destina
8	1.bin.octet-stream	octet-stream	340 824 B	209.141.51.196 [209.141.51.196]	TCP 80	10.1.21

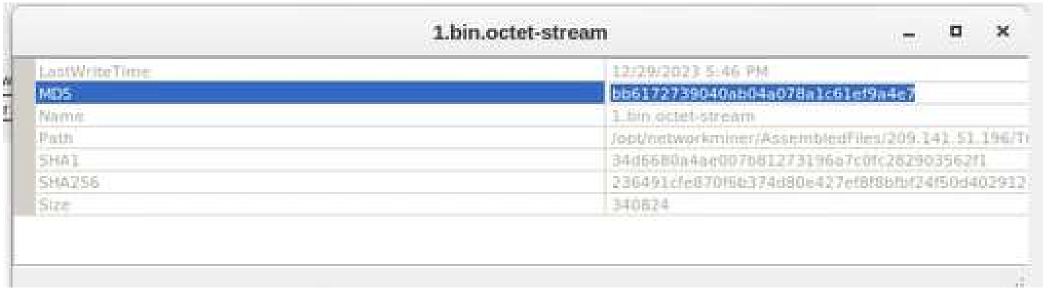
File...	MD5
10.1.2...	3620...



	Timestamp	Reconstructed file path	Details
nal	2023-12-29 17:46:12 UTC	/opt/networkminer/AssembledFiles/209.141.51.1...	209.141.51.196/files/1.bin

File...	MD5
10.1.2...	3620...

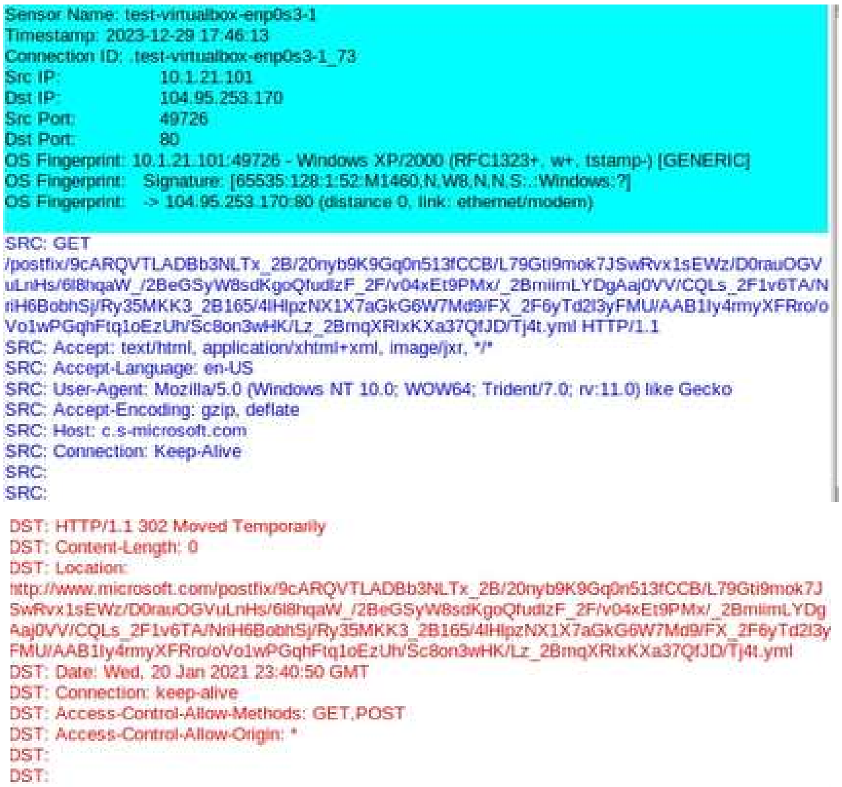
c. **How did the malware infect the PC? Use an internet search as necessary.**



LastWriteTime	12/29/2023 5:46 PM
MD5	bb6172739040ab04a078a1c61ef9a4e7
Name	1.bin.octet-stream
Path	/opt/networkminer/AssembledFiles/209.141.51.196/Tr
SHA1	34d6680a4ae007b81273196a7c0fc282903562f1
SHA256	236491cfe870f6b374d80e427ef8f8bfbf24f50d402912
Size	340824

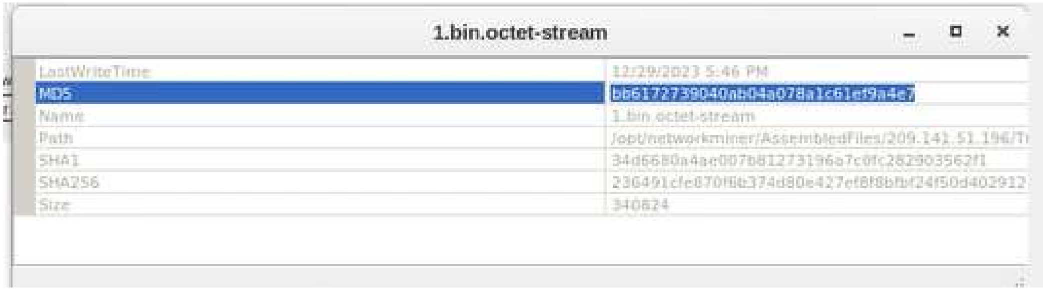
Step 2: Examine the exploit.

a. **Based on the alerts associated with HTTP GET request, what files were downloaded? List the malicious domains observed and the files downloaded.**



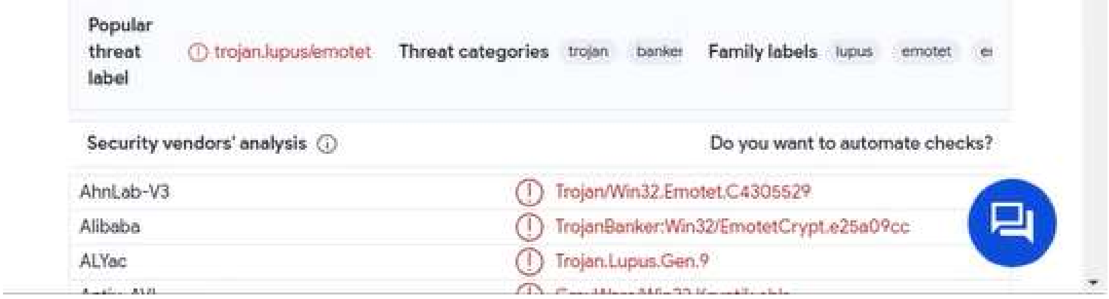
```
Sensor Name: test-virtualbox-enp0s3-1
Timestamp: 2023-12-29 17:46:13
Connection ID: .test-virtualbox-enp0s3-1_73
Src IP:            10.1.21.101
Dst IP:            104.95.253.170
Src Port:          49726
Dst Port:          80
OS Fingerprint: 10.1.21.101:49726 - Windows XP/2000 (RFC1323+, w+, tstamp-) [GENERIC]
OS Fingerprint:    Signature: [65535:128:1:52:M1460,N,W8,N,N,S:.:Windows:?]
OS Fingerprint:    -> 104.95.253.170:80 (distance 0, link: ethernet/modem)

SRC: GET
/postfix/9cARQVTLADBb3NLTx_2B/20nyb9K9Gq0n513fCCB/L79Gti9mok7JSwRvx1sEWz/D0rauOGV
uLnHs/6l8hqaW_/2BeGSyW8sdKgoQfudlzF_2F/v04xEt9PMx/_2BmiimLYDgAaj0VV/CQLs_2F1v6TA/N
riH6BobhSj/Ry35MKK3_2B165/4lHlpzNX1X7aGkG6W7Md9/FX_2F6yTd2l3yFMU/AAB1ly4rmyXFRro/o
Vo1wPGqhFtq1oEzUh/Sc8on3wHK/Lz_2BmqXRlxKXa37QfJD/Tj4t.yml HTTP/1.1
SRC: Accept: text/html, application/xhtml+xml, image/jxr, */*
SRC: Accept-Language: en-US
SRC: User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
SRC: Accept-Encoding: gzip, deflate
SRC: Host: c.s-microsoft.com
SRC: Connection: Keep-Alive
SRC:
SRC:

DST: HTTP/1.1 302 Moved Temporarily
DST: Content-Length: 0
DST: Location:
http://www.microsoft.com/postfix/9cARQVTLADBb3NLTx_2B/20nyb9K9Gq0n513fCCB/L79Gti9mok7J
SwRvx1sEWz/D0rauOGVuLnHs/6l8hqaW_/2BeGSyW8sdKgoQfudlzF_2F/v04xEt9PMx/_2BmiimLYDg
Aaj0VV/CQLs_2F1v6TA/NriH6BobhSj/Ry35MKK3_2B165/4lHlpzNX1X7aGkG6W7Md9/FX_2F6yTd2l3y
FMU/AAB1ly4rmyXFRro/oVo1wPGqhFtq1oEzUh/Sc8on3wHK/Lz_2BmqXRlxKXa37QfJD/Tj4t.yml
DST: Date: Wed, 20 Jan 2021 23:40:50 GMT
DST: Connection: keep-alive
DST: Access-Control-Allow-Methods: GET,POST
DST: Access-Control-Allow-Origin: *
DST:
DST:
```

Use any available tools in Security Onion VM, determine and record the SHA256 hash for the downloaded files that probably infected the computer?



LastWriteTime	12/29/2023 5:46 PM
MD5	bb6172739040ab04a078a1c61ef9a4e7
Name	1.bin.octet-stream
Path	/opt/networkminer/AssembledFiles/209.141.51.196/Tr
SHA1	34d6680a4ae007b81273196a7c0fc282903562f1
SHA256	236491cfe870f6b374d80e427ef8f8bfbf24f50d402912
Size	340824

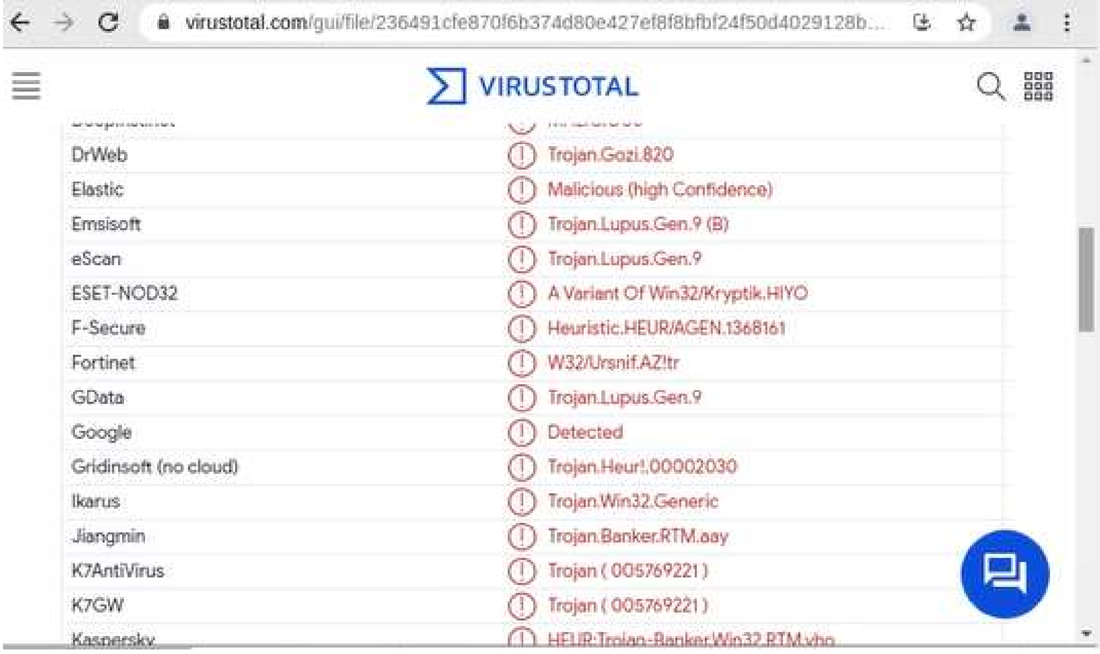
b. **Navigate to www.virustotal.com input the SHA256 hash to determine if these were detected as malicious files. Record your findings, such as file type and size, other names, and target machine. You can also include any information that is provided by the community posted in VirusTotal.**



Popular threat label ⓘ trojan.lupus/emotet Threat categories trojan banker Family labels lupus emotet e

Security vendors' analysis ⓘ Do you want to automate checks?

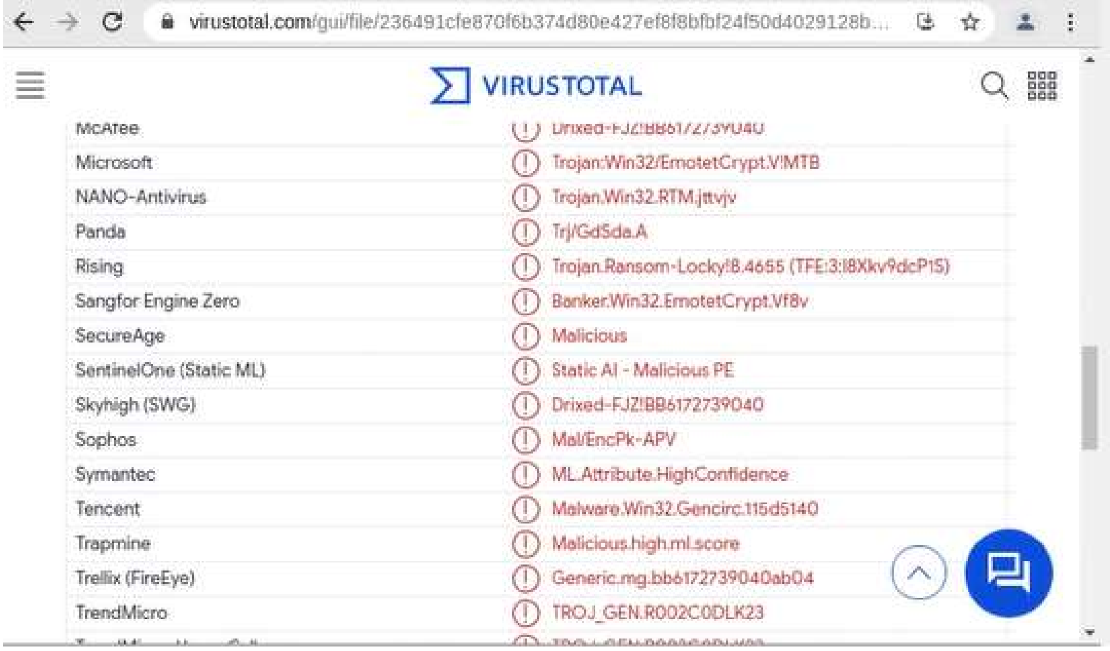
AhnLab-V3	ⓘ Trojan/Win32.Emotet.C4305529
Alibaba	ⓘ TrojanBanker:Win32/EmotetCrypt.e25a09cc
ALYac	ⓘ Trojan.Lupus.Gen.9



virustotal.com/gui/file/236491cfe870f6b374d80e427ef8f8bfbf24f50d4029128b...

VIRUSTOTAL

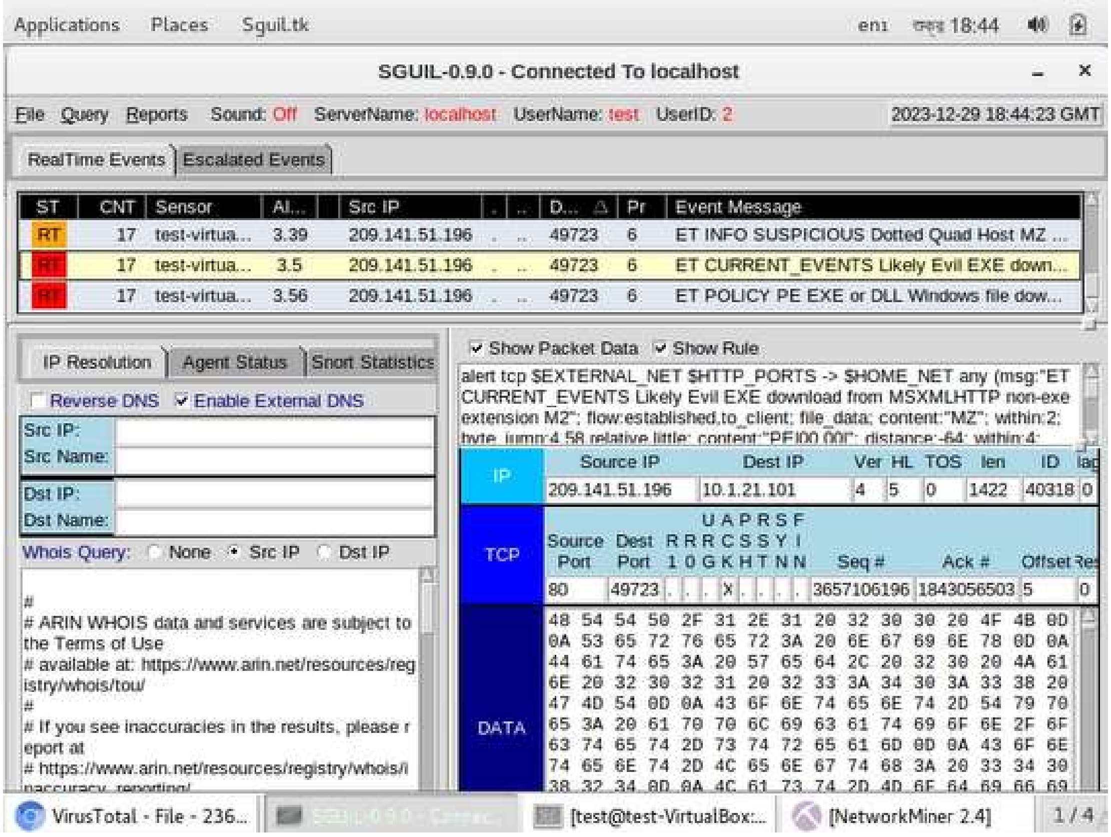
DrWeb	ⓘ Trojan.Gozi.820
Elastic	ⓘ Malicious (high Confidence)
Emsisoft	ⓘ Trojan.Lupus.Gen.9 (B)
eScan	ⓘ Trojan.Lupus.Gen.9
ESET-NOD32	ⓘ A Variant Of Win32/Kryptik.HIYO
F-Secure	ⓘ Heuristic.HEUR/AGEN.1368161
Fortinet	ⓘ W32/Ursnif.AZ!tr
GData	ⓘ Trojan.Lupus.Gen.9
Google	ⓘ Detected
Gridinsoft (no cloud)	ⓘ Trojan.Heur!.00002030
Ikarus	ⓘ Trojan.Win32.Generic
Jiangmin	ⓘ Trojan.Banker.RTM.aay
K7AntiVirus	ⓘ Trojan (005769221)
K7GW	ⓘ Trojan (005769221)
Kaspersky	ⓘ HEUR:Trojan-Banker.Win32.RTM.vho



virustotal.com/gui/file/236491cfe870f6b374d80e427ef8f8bfbf24f50d4029128b...

McAfee	Drixed-FJZ!BB6172739040
Microsoft	Trojan:Win32/EmotetCrypt.V!MTB
NANO-Antivirus	Trojan.Win32.RTM.jttvjv
Panda	Trj/GdSda.A
Rising	Trojan.Ransom-Locky!8.4655 (TFE:3:I8Xkv9dcP1S)
Sangfor Engine Zero	Banker.Win32.EmotetCrypt.Vf8v
SecureAge	Malicious
SentinelOne (Static ML)	Static AI - Malicious PE
Skyhigh (SWG)	Drixed-FJZ!BB6172739040
Sophos	Mal/EncPk-APV
Symantec	ML.Attribute.HighConfidence
Tencent	Malware.Win32.Gencirc.115d5140
Trapmine	Malicious.high.ml.score
Trellix (FireEye)	Generic.mg.bb6172739040ab04
TrendMicro	TROJ_GEN.R002C0DLK23

c. **Examine other alerts associated with the infected host during this timeframe and record your findings**



SGUIL-0.9.0 - Connected To localhost

Sound: Off ServerName: localhost UserName: test UserID: 2 2023-12-29 18:44:23 GMT

ST	CNT	Sensor	Al...	Src IP	.	..	D... △	Pr	Event Message
RT	17	test-virtua...	3.39	209.141.51.196	.	..	49723	6	ET INFO SUSPICIOUS Dotted Quad Host MZ ...
RT	17	test-virtua...	3.5	209.141.51.196	.	..	49723	6	ET CURRENT_EVENTS Likely Evil EXE down...
RT	17	test-virtua...	3.56	209.141.51.196	.	..	49723	6	ET POLICY PE EXE or DLL Windows file dow...

□ Reverse DNS ☑ Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: ○ None ● Src IP ○ Dst IP

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
```

☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS Likely Evil EXE download from MSXMLHTTP non-exe extension M2"; flow:established,to_client; file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4;
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	lag
	209.141.51.196	10.1.21.101	4	5	0	1422	40318	0

TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res
	80	49723	.	.	.	X	.	.	.	.	3657106196	1843056503	5	0

DATA

```
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D
0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 0D 0A
44 61 74 65 3A 20 57 65 64 2C 20 32 30 20 4A 61
6E 20 32 30 32 31 20 32 33 3A 34 30 3A 33 38 20
47 4D 54 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70
65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6F
63 74 65 74 2D 73 74 72 65 61 6D 0D 0A 43 6F 6E
74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 33 34 30
38 32 34 0D 0A 4C 61 73 74 2D 4D 6F 64 69 66 69
```

Step 3: Report Your Findings

Summarizes your findings based on the information you have gathered from the previous parts, summarize your findings.

The trojan.lupus/emotet was installed on the host, a Windows computer with IP 10.1.21.101, after it sent a DNS query to a malicious domain. By listening on port 80, the trojan.lupus/emotet malware poses as an Apache web server. Following infection, a variety of malware is downloaded via trojan.lupus/emotet. The majority of sources confirmed that these files were malware after they were examined on virustotal.com using their SHA256 hash.