

SPLUNK

Conclusion:

In this fun exercise, as a SOC Analyst, we have investigated a cyber-attack where the attacker had defaced a website 'imreallynotbatman.com' of the Wayne Enterprise. We mapped the attacker's activities into the 7 phases of the Cyber Kill Chain. Let us recap everything we have found so far:

Reconnaissance Phase:

We first looked at any reconnaissance activity from the attacker to identify the IP address and other details about the adversary.

Findings:

IP Address 40.80.148.42 was found to be scanning our webserver.

The attacker was using Acunetix as a web scanner.

Exploitation Phase:

We then looked into the traces of exploitation attempts and found brute-force attacks against our server, which were successful.

Findings:

Brute force attack originated from IP 23.22.63.114.

The IP address used to gain access: 40.80.148.42

142 unique brute force attempts were made against the server, out of which one attempt was successful

Installation Phase:

Next, we looked at the installation phase to see any executable from the attacker's IP Address uploaded to our server.

Findings:

A malicious executable file 3791.exe was observed to be uploaded by the attacker.

We looked at the sysmon logs and found the MD5 hash of the file.

Action on Objective:

After compromising the web server, the attacker defaced the website.

Findings:

We examined the logs and found the file name used to deface the webserver.

Weaponization Phase:

We used various threat Intel platforms to find the attacker's infrastructure based on the following information we saw in the above activities.

Information we had:

Domain: prankglassinebracket.jumpingcrab.com

IP Address: 23.22.63.114

Findings:

Multiple masquerading domains were found associated with the attacker's IPs.

An email of the user Lillian.rose@polson1vy.com was also found associated with the attacker's IP address.

Deliver Phase:

In this phase, we again leveraged online Threat Intel sites to find malware associated with the adversary's IP address, which appeared to be a secondary attack vector if the initial compromise failed.

Findings:

A malware name MirandaTateScreensaver.scr.exe was found associated with the adversary.

MD5 of the malware was c99131e0169171935c5ac32615ed6261

Volatility

Volatility is a free memory forensics tool developed and maintained by Volatility Foundation, commonly used by malware and SOC analysts within a blue team or as part of their detection and monitoring solutions. Volatility is written in Python and is made up of python plugins and modules designed as a plug-and-play way of analyzing memory dumps.

Simple example of using a plugin.

PID	PPID	ImageFileName	Offset	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
998	652	svchost.exe	0x2029ab8	9	226	0	False	2012-07-22 02:42:33.000000	N/A	Disabled
664	608	lsass.exe	0x202a3b8	24	330	0	False	2012-07-22 02:42:32.000000	N/A	Disabled
652	608	services.exe	0x202ab28	16	243	0	False	2012-07-22 02:42:32.000000	N/A	Disabled
1640	1484	reader_sl.exe	0x207bda0	5	39	0	False	2012-07-22 02:42:36.000000	N/A	Disabled
1512	652	spoolsv.exe	0x20b17b8	14	113	0	False	2012-07-22 02:42:36.000000	N/A	Disabled
1588	1004	wuauctl.exe	0x225bda0	5	132	0	False	2012-07-22 02:44:01.000000	N/A	Disabled
788	652	alg.exe	0x22e8da0	7	104	0	False	2012-07-22 02:43:01.000000	N/A	Disabled
1484	1464	explorer.exe	0x23dea70	17	415	0	False	2012-07-22 02:42:36.000000	N/A	Disabled
1056	652	svchost.exe	0x23dfa0	5	60	0	False	2012-07-22 02:42:33.000000	N/A	Disabled
1136	1004	wuauctl.exe	0x23fcda0	8	173	0	False	2012-07-22 02:43:46.000000	N/A	Disabled
1220	652	svchost.exe	0x2495650	15	197	0	False	2012-07-22 02:42:35.000000	N/A	Disabled
608	368	winlogon.exe	0x2498700	23	519	0	False	2012-07-22 02:42:32.000000	N/A	Disabled
584	368	cssrss.exe	0x24a0598	9	326	0	False	2012-07-22 02:42:32.000000	N/A	Disabled
368	4	smss.exe	0x24f1020	3	19	N/A	False	2012-07-22 02:42:31.000000	N/A	Disabled
1004	652	svchost.exe	0x25001d0	64	1118	0	False	2012-07-22 02:42:33.000000	N/A	Disabled
824	652	svchost.exe	0x2511360	20	194	0	False	2012-07-22 02:42:33.000000	N/A	Disabled
4	0	System	0x25c89c8	53	240	N/A	False	N/A	N/A	Disabled

Exercise.

For case 1

Most things were straightforward in answering , we just had to use the required plugins however to find the user agent requires a special command which could be confusing.

```
lthmanalyst@ubuntu:/Scenarios/Investigations$ strings /Scenarios/Investigations/*Investigation-1.vmem | grep -i "user-agent"
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
User-Agent: RPC
User-Agent: RPC
User-Agent: Mozilla/5.0 (Windows; U; MSIE 7.0; Windows NT 6.0; en-US)
User-Agent
user-agent
USER-AGENT:
User-Agent:
cs(User-Agent)
User-Agent
User-Agent
lthmanalyst@ubuntu:/Scenarios/Investigations$ █
```

Case2

In addition, there were outside OSINT that were required to find some of the solutions. Because we were dealing with a suspicious process called **@WanaDecryptor@**, OSINT was required. Some notable sources were virus total and blogs to find the correct mutex for the known indicator of the malware.

(MsWinZonesCacheCounterMutexA0x0)

One important thing to note is that this suspicious process is part of the famous malware **wannacry**. Finally to summarize, it's important to recognize the suspicious pid and parent process PID, so that we can trace and link things up.

Velociraptor

In this room, we will explore Rapid7's newly acquired tool known as [Velociraptor](#).

Per the official Velociraptor [documentation](#), "*Velociraptor is a unique, advanced open-source endpoint monitoring, digital forensic and cyber response platform. It was developed by Digital Forensic and Incident Response (DFIR) professionals who needed a powerful and efficient way to hunt for specific artifacts and monitor activities across fleets of endpoints. Velociraptor provides you with the ability to more effectively respond to a wide range of digital forensic and cyber incident response investigations and data breaches*".

This tool was created by Mike Cohen, a former Google employee who worked on tools such as [GRR](#) (GRR Rapid Response) and [Rekall](#) (Rekall Memory Forensic Framework). Mike joined Rapid7's Detection and Response Team and continues to work on improving Velociraptor. At the date of this entry, the latest release for Velociraptor is [0.6.3](#).

Learning Objectives

- Learn what is Velociraptor
- Learn how to interact with agents and create collections
- Learn how to interact with the virtual file system
- Learn what is VQL and how to create basic queries
- Use Velociraptor to perform a basic hunt

ct.thymecode@thm-velociraptor: ~

```
config.yaml velociraptor velociraptor.config.yaml velociraptor-v0.5.8-linux-amd64
ct.thymecode@thm-velociraptor: ~$ ./velociraptor-v0.5.8-linux-amd64 --config velociraptor.config.yaml frontend -v
```

Administrator Command Prompt - velociraptor-v0.5.8-windows-amd64.exe --config velociraptor.config.yaml client -v

Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

Digging deeper!
This is Velociraptor 0.5.8 built on:2021-04-11T22:11:10Z (e46bf54c)
Loading config from file velociraptor\ls' is not recognized as an internal or external command,
Starting Frontend. [build_time]:"operable program or batch file.

Error increasing limit invalid argc:Users\Administrator> cd C
Starting Journal service. The system cannot find the path specified.
Starting the notification service.
Starting Inventory Service C:Users\Administrator>cd "C:\Program Files\Velociraptor"
Loaded 250 built in artifacts in 1
Starting Label service. C:\Program Files\Velociraptor\velociraptor-v0.5.8-windows-amd64.exe --config velociraptor.config.yaml client -v
Selected frontend configuration lo[INFO] 2023-08-28T17:31:13Z
Starting Client Monitoring Service[INFO] 2023-08-28T17:31:13Z
Reloading client monitoring tables[INFO] 2023-08-28T17:31:13Z
Starting Hunt Dispatcher Service. [INFO] 2023-08-28T17:31:13Z
Starting the hunt manager service. [INFO] 2023-08-28T17:31:13Z
server monitoring: Starting Server [INFO] 2023-08-28T17:31:13Z
Closing Server Monitoring Event ta[INFO] 2023-08-28T17:31:13Z Digging deeper! https://www.velocidex.com
server monitoring: Updating monitor[INFO] 2023-08-28T17:31:13Z This is Velociraptor 0.5.8 built on 2021-04-11T22:11:10Z (e46bf54c)
Starting Enrollment service. [INFO] 2023-08-28T17:31:13Z Loading config from file velociraptor.config.yaml
server monitoring: Collecting Servi[INFO] 2023-08-28T17:31:13Z Loading writeback from C:\Program Files\Velociraptor\velociraptor.writeback.yaml
Starting VFS writing service. [INFO] 2023-08-28T17:31:13Z Setting temp directory to C:\Program Files\Velociraptor\Tools

Velociraptor

Search clients Show All thm-velociraptor.eu-west-1 compute internal connected thmadmin

State	FlowId	Artifacts	Created	Last Active	Creator	Mb	Rows
✓	F CJMGlO2JVI10M	Generic.Client.Info	2023-08-28 20:53:52 UTC	2023-08-28 20:53:54 UTC		8	

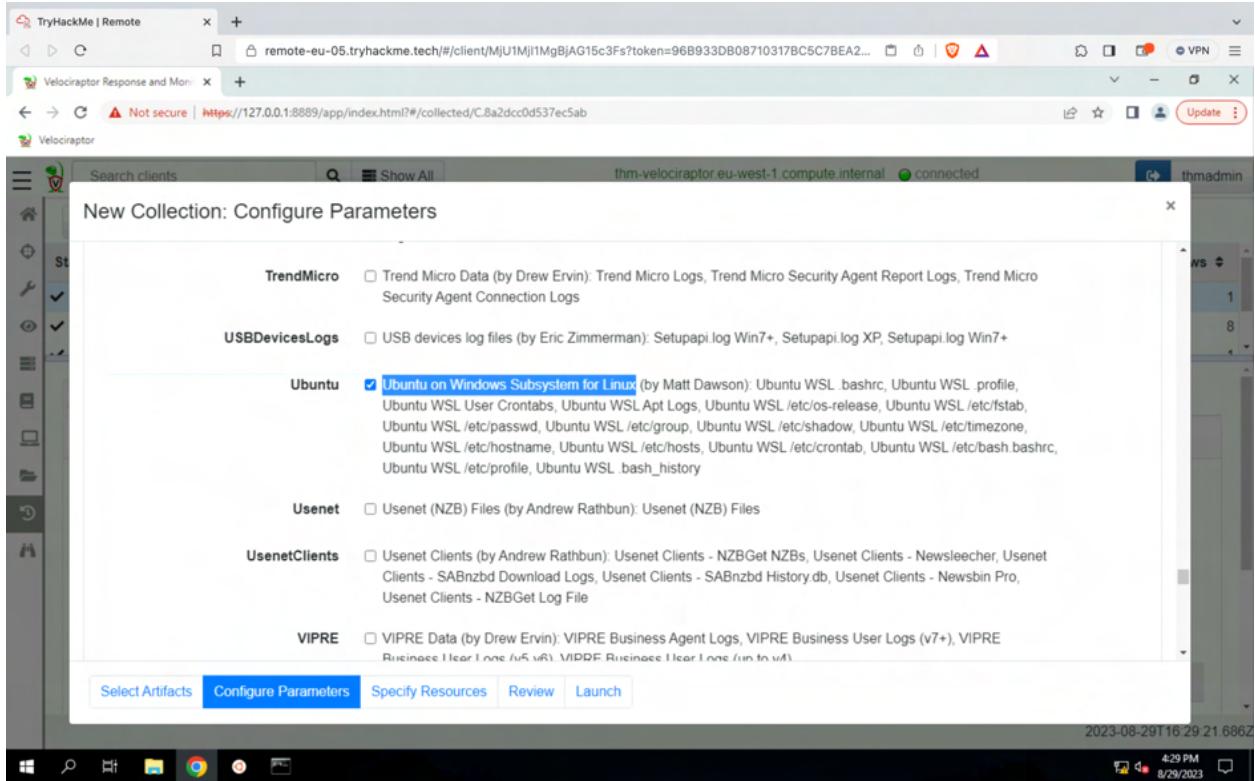
Artifact Collection Uploaded Files Requests Results Log Notebook

Request sent to client

```
14     "max_row": "1000"
15   }
16   {
17     "query_id": "1",
18     "task_id": "1693256032508714",
19     "VQLClientAction": {
20       "precondition": "SELECT OS From info() where OS = 'windows'",
21       "Query": [
22         {
23           "VQL": "LET precondition_Generic_Client_Info_Users_0=SELECT OS FROM info() WHERE OS = 'windows'"
24         },
25       ],
26     }
27     "VQL": "LET Generic_Client_Info_Users_0=SELECT Name, Description, Htme AS Lastlogin FROM Artifact.Windows.SYS.Users[]"
28   },
29   {
30     "Name": "$4b3003c65600da3c4ca73094cf23e1d4c63c719330d3604ea3cad424f6e2c7f",
31     "VQL": "SELECT * FROM if(then=Generic_Client_Info_Users_0, condition=precondition_Generic_Client_Info_Users_0, else= { SELECT * FROM scope() WHERE log(message+`Query sk"
32   }
```

Windows.sys.Users() 1 of 1 . Aa \b S

2023-08-28T21:15:46.626Z 9:15 PM 8/28/2023



The screenshot shows a web browser window titled "The VFS :: Velociraptor" open in a Brave browser. The URL is docs.velociraptor.app/docs/gui/vfs/. The page displays the Velociraptor logo and navigation links for announcements, documentation, and various training modules. A sidebar on the left lists "The Admin GUI" sections: "Inspecting clients", "The VFS", "Artifacts", and "Hunting". The "The VFS" section is currently selected. The main content area shows a screenshot of a Windows File Explorer-like interface titled "DESKTOP DESKTOP\...\Windows\system32\cmd.exe". It lists files like "cmd.exe", "cmdkey.dll", and "cmdkey.dll~\$". Below this is a "Registry Accessor" section with a table showing registry keys and their properties. The table includes columns for Name, Value, Mode, and Action. A red box highlights the "Value" column for the "Software\Microsoft\Windows\CurrentVersion\Run" key, which contains the value "RunOnce". The bottom of the page features a footer with "VQL Reference", "Brought to you by RAPID7", and a copyright notice from 2022.

The screenshot shows a web browser window with the URL docs.velociraptor.app/docs/forensic/filesystem/. A modal dialog titled "Raw Response JSON" displays the following JSON data:

```

1+ [
2+   {
3+     "Name": "ChromeSetup.exe",
4+     "ModTime": "2020-05-31T17:38:42Z",
5+     "FullPath": "C:\\Users\\mike\\downloads\\ChromeSetup.exe",
6+     "Mtime": "2020-05-31T17:38:42Z",
7+     "Btime": "2021-01-19T08:52:33.1732915Z",
8+     "Ctime": "2020-05-31T17:38:42Z",
9+     "Atime": "2021-01-22T14:23:00.5879832Z",
10+    "Data": {},
11+    "Size": 1995576,
12+    "IsDir": "false",
13+    "IsLink": "false",
14+    "Mode": 438,
15+    "Sys": {
16+      "fileAttributes": 32,
17+      "CreationTime": {
18+        "LowDateTime": 1832406963,
19+        "HighDateTime": 308642912
20+      },
21+      "LastAccessTime": {
22+        "LowDateTime": 1832406963,
23+        "HighDateTime": 308642912
24+      }
25+    }
26+  }
27+ ]
  
```

The modal has a "Close" button at the bottom right. Below the modal, the text "Glob output" is visible.

Some of the more important columns available are `lPath` is the complete path to the matching file, whereas the `Name` is just the filename.

The screenshot shows a Firefox browser window with the URL <https://127.0.0.1:8889/app/index.html#/notebooks/N.CJOGPUACOD69C>. The page displays a table of notebook metadata and a detailed view of a specific file's PE header.

NotebookId	Name	Description	Creation Time	Modified Time	Creator	Collaborators
N.CJOGPUACOD69C	notebook	notebook	2023-08-31 21:58:17 UTC	2023-08-31 21:58:17 UTC	admin	admin

Below the table, a file viewer shows the details for `FXSDRV.DLL` from `C:/Windows/System32/spool/drivers/x64/3/FXSDRV.DLL`. The file's PE header is expanded, showing fields like `FileHeader`, `GUIDAge`, `PDB`, `Sections`, and `VersionInformation`.

```
SELECT "C:/" + FullPath AS Full_Path,FileName AS  
File_Name,parse_pe(file="C:/" + FullPath) AS PE  
  
FROM parse_mft(filename="C:/$MFT", accessor="ntfs")  
  
WHERE NOT IsDir  
  
AND FullPath =~ "Windows/System32/spool/drivers"  
  
AND PE
```

Utilized VQL Query to find a suspicious DLL.

Malware Analysis

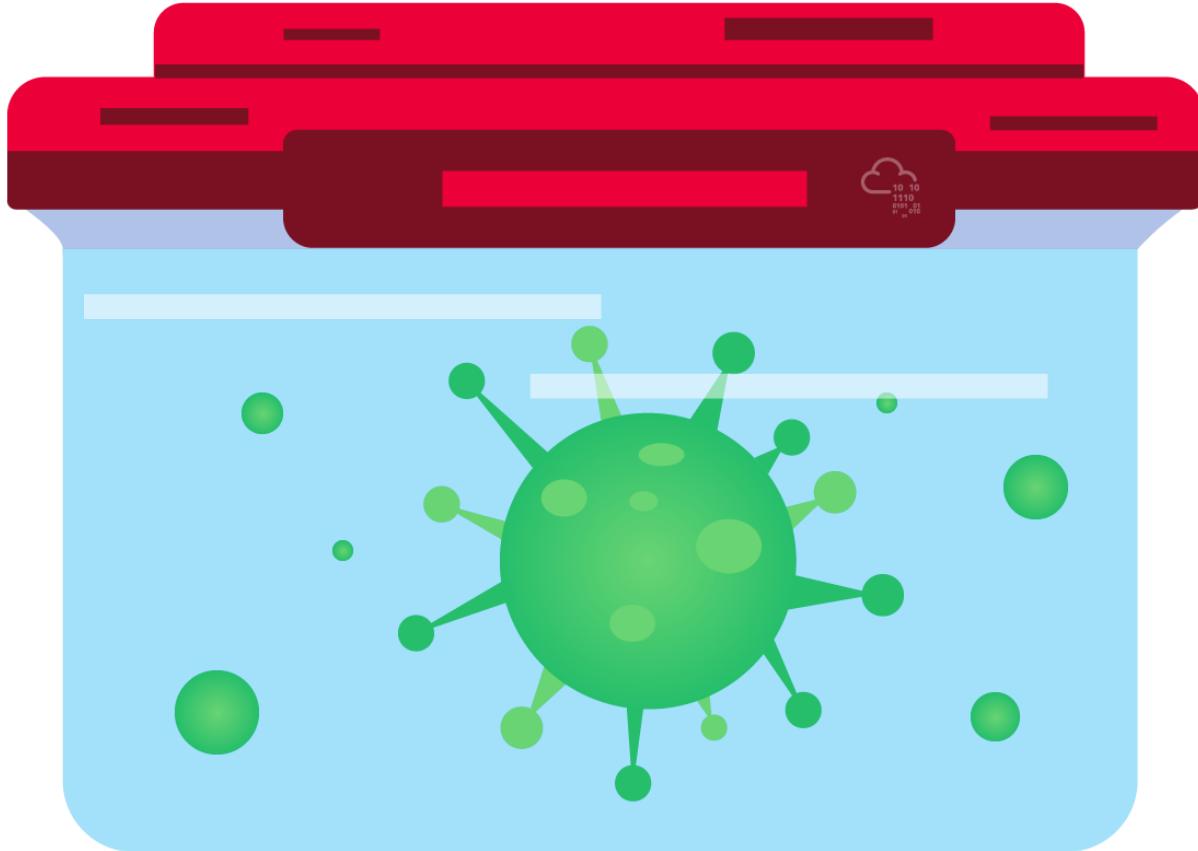
- Never analyze malware or suspected malware on a machine that does not have the sole purpose of analyzing malware.
- When not analyzing or moving malware samples around to different locations, always keep them in password-protected zip/rar or other archives so that we can avoid accidental detonation.
- Only extract the malware from this password-protected archive inside the isolated environment, and only when analyzing it.
- Create an isolated VM specifically for malware analysis, which has the capability of being reverted to a clean slate once you are done.
- Ensure that all internet connections are closed or at least monitored.
- Once you are done with malware analysis, revert the VM to its clean slate for the next malware analysis session to avoid residue from a previous malware execution corrupting the next one.

Malware Analysis is like solving a puzzle. Different tools and techniques are used to find the pieces of this puzzle, and joining those pieces gives us the complete picture of what the malware is trying to do. Most of the time, you will have an executable file (also called a binary or a PE file. PE stands for Portable Executable), a malicious document file, or a Network Packet Capture (Pcap). The Portable Executable is the most prevalent type of file analyzed while performing Malware Analysis.

To find the different puzzle pieces, you will often use various tools, tricks, and shortcuts. These techniques can be grouped into the following two categories:

- Static Analysis
- Dynamic Analysis

Static Analysis

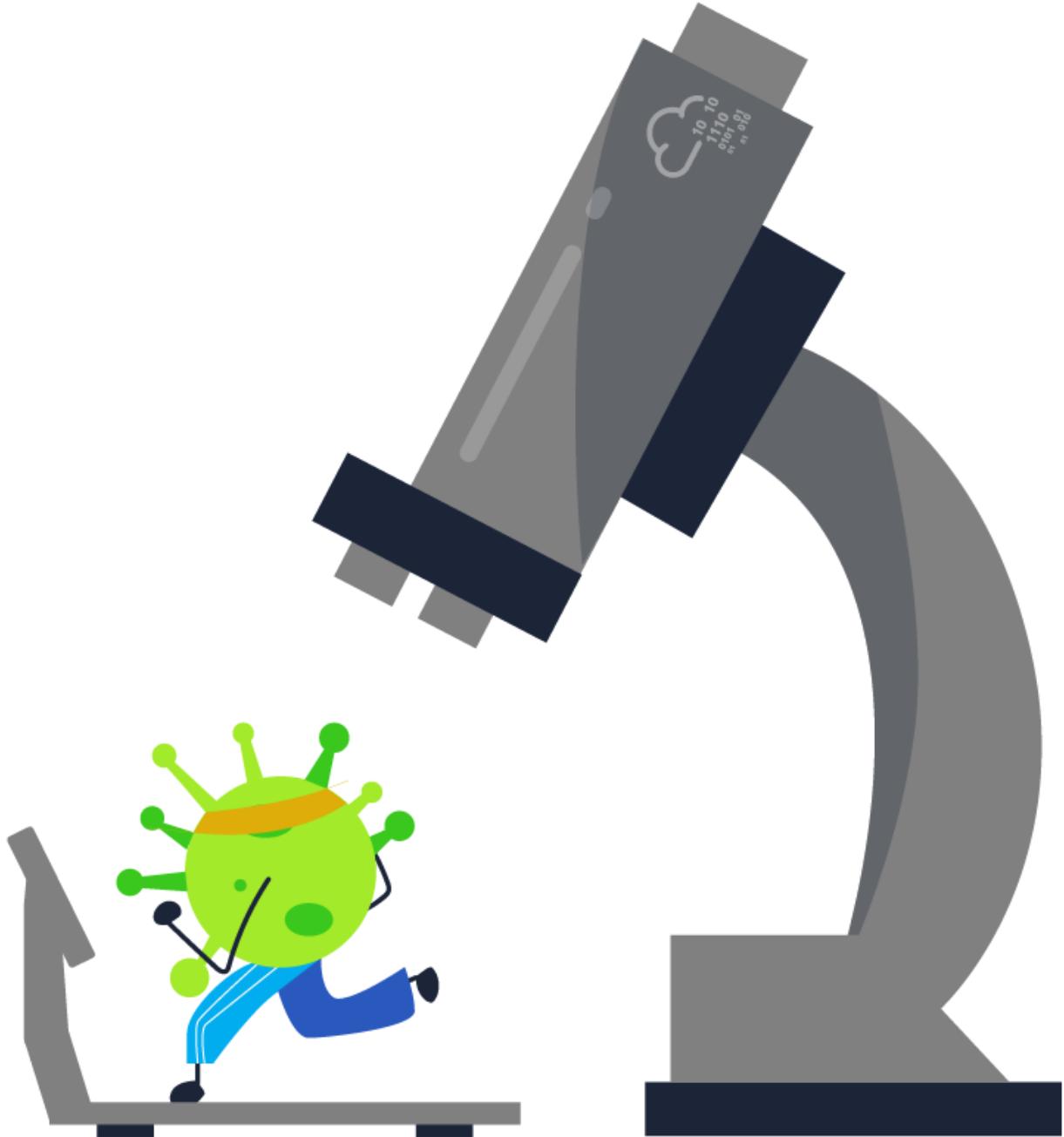


When malware is analyzed without being executed, it is called Static Analysis. In this case, the different properties of the PE file are analyzed without running it. Similarly, in the case of a malicious document, exploring the document's properties without analyzing it will be considered Static Analysis. Examples of static analysis include checking for strings in malware, checking the PE header for information related to different sections, or looking at the code using a disassemble. We will look at some of these techniques later in the room.

Malware often uses techniques to avoid static analysis. Some of these techniques use obfuscation, packing, or other means of hiding its properties. To circumvent these techniques, we often use dynamic analysis.

Dynamic Analysis

Malware faces a dilemma. It has to execute to fulfill its purpose, and no matter how much obfuscation is added to the code, it becomes an easy target for detection once it runs.



Static analysis might provide us with crucial information regarding malware, but sometimes that is not enough. We might need to run the malware in a controlled environment to observe what it does in these cases. Malware can often hide its properties to thwart Static Analysis. However, in most of those cases, Dynamic Analysis can prove fruitful. Dynamic analysis techniques include running the malware in a VM, either in a manual fashion with tools installed to monitor the

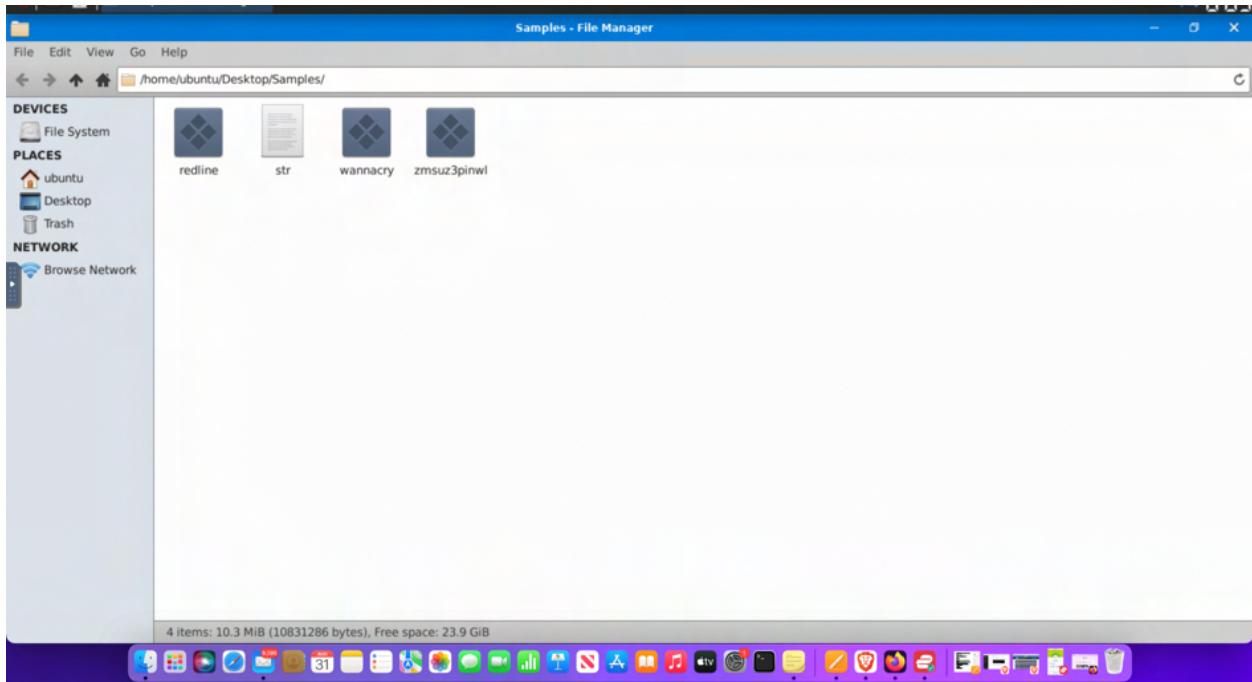
malware's activity or in the form of sandboxes that perform this task automatically. We will learn about some of these techniques later in this room. Once we run the malware in a controlled environment, we can use our knowledge from the Windows Forensics rooms to identify what it did in our environment. The advantage here is that since we control the environment, we can configure it to avoid noise, like activity from a legitimate user or Windows Services. Thus, everything we observe in such an environment points to malware activity, making it easier to identify what the malware did in this scenario.

Malware, however, often uses techniques to prevent an analyst from performing dynamic analysis. Since most dynamic analysis is performed in a controlled environment, most methods to bypass dynamic analysis include detecting the environment in which it is being run. Therefore, in these cases, the malware uses a different, benign code path if it identifies that it is being run in a controlled environment.

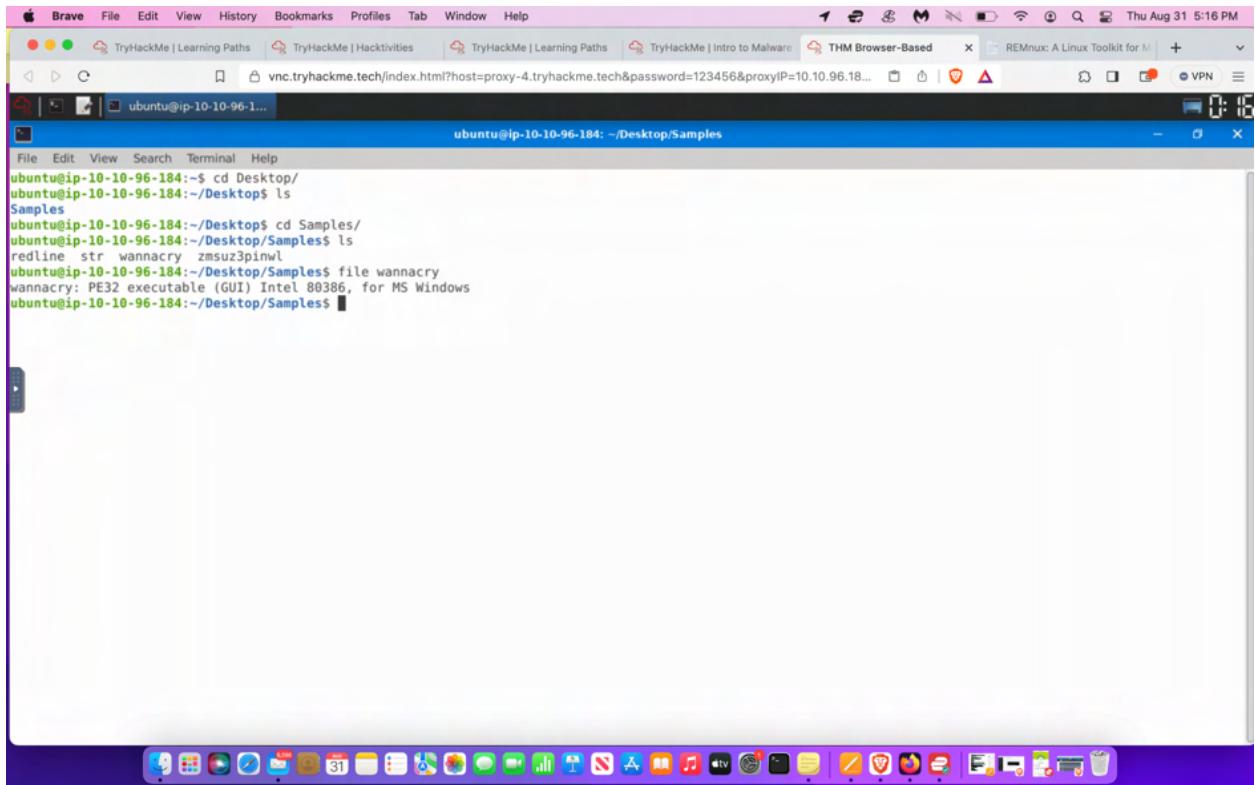
Advanced Malware Analysis

Advanced Malware Analysis Techniques

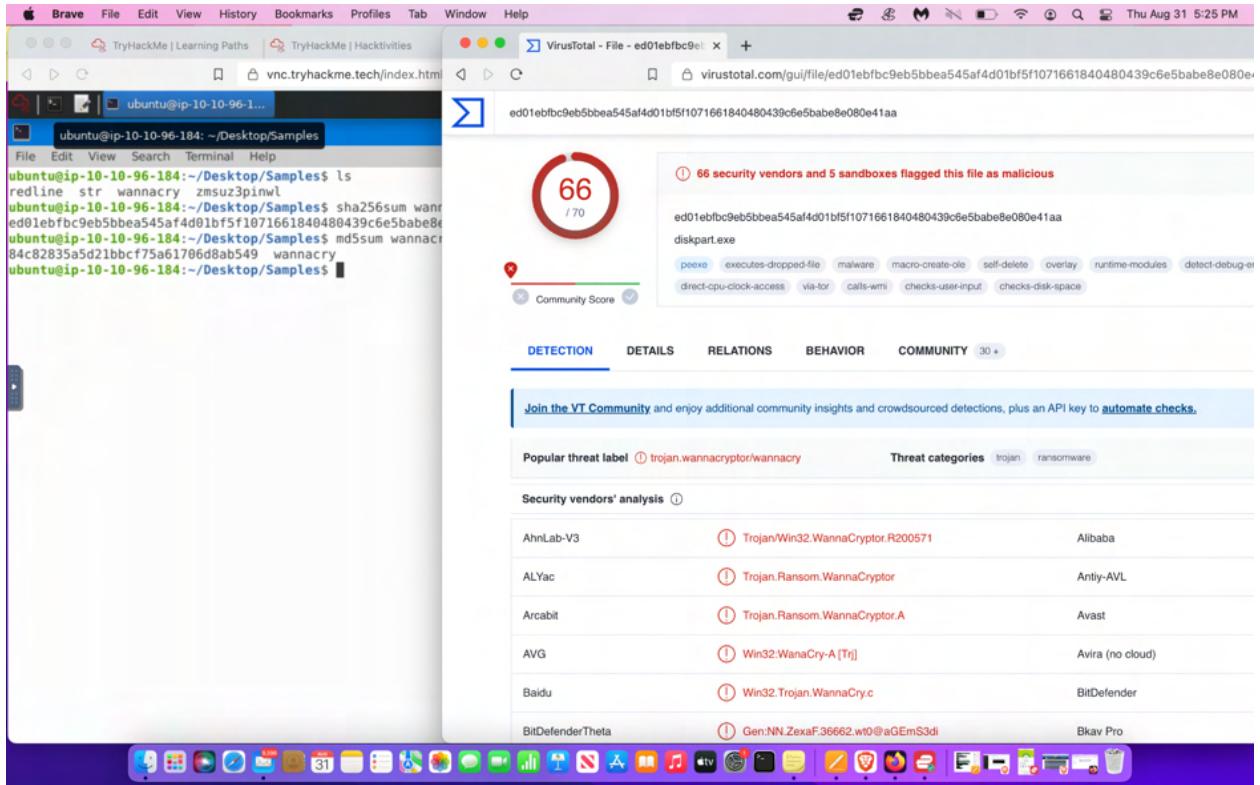
- Objective: Analyze malware that evades basic static and dynamic analysis.
- Tools: Disassemblers and debuggers.
- Disassemblers: Convert malware code from binary to assembly language.
 - Allows static examination of malware instructions.
- Debuggers: Attach to a program and monitor malware instructions during runtime.
 - Enables starting and stopping malware at different points.
 - Identifies crucial information.
 - Provides insights into system memory and CPU utilization.



Remnux the linux distribution used for malware analysis.

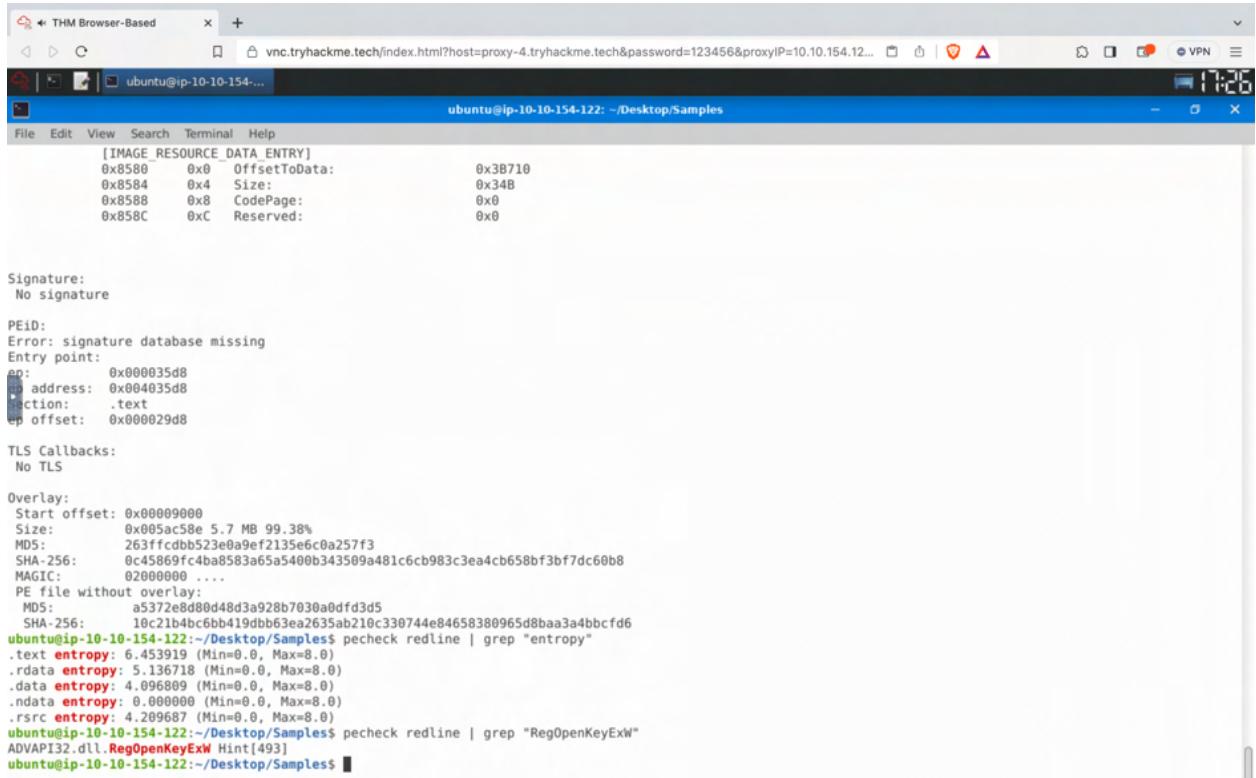


Details for the famous wannacry malware present in samples directory. uses the X-86. It is a PE32 Executable GUI for windows.



Calculate md5 or sha256 hash and look up the hash on virus total.

Analysed the PE header using the pecheck command to find various sections such as .text , .data, .rdata, .ndata, .rsrs



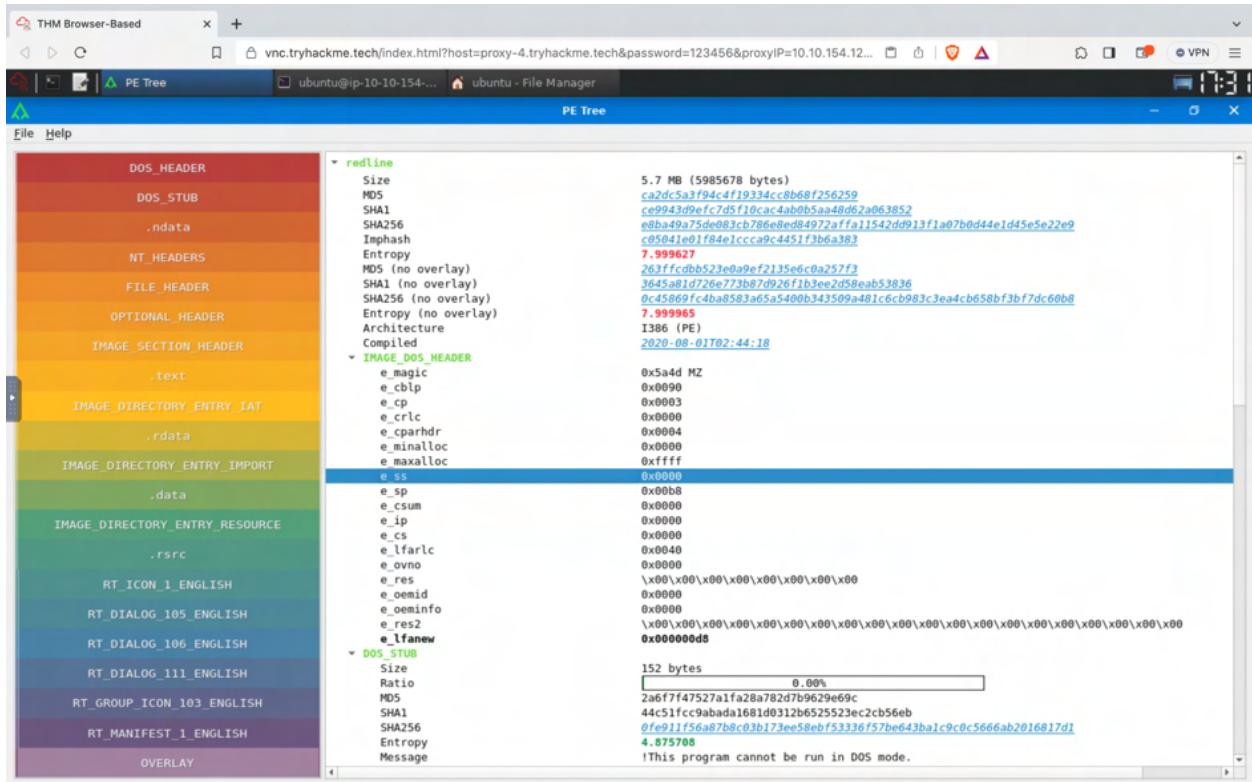
```

ubuntu@ip-10-10-154-122: ~/Desktop/Samples$ pecheck redline | grep "entropy"
.text entropy: 6.453919 (Min=0.0, Max=8.0)
.rdata entropy: 5.136718 (Min=0.0, Max=8.0)
.data entropy: 4.096889 (Min=0.0, Max=8.0)
.ndata entropy: 0.000000 (Min=0.0, Max=8.0)
.rsrc entropy: 4.209687 (Min=0.0, Max=8.0)
ubuntu@ip-10-10-154-122: ~/Desktop/Samples$ pecheck redline | grep "RegOpenKeyExW"
ADVAPI32.dll.RegOpenKeyExW Hint[493]
ubuntu@ip-10-10-154-122: ~/Desktop/Samples$ 

```

Executed the pe-tree command on the terminal `pe-tree redline`

for the redline sample given to view a GUI based interface in a more readable format. Ultimately this contains metadata which can be helpful for our malware analysis.



Dynamic Analysis

Uploaded samples on hybrid analysis to analyze the report given for the redline sample. This was done my using the md5 hash as opposed to uploading an actual sample.

The screenshot shows a web browser window with the Hybrid Analysis interface. The URL in the address bar is <https://hybrid-analysis.com/sample/e8ba49a75de083cb786e8ed84972affa11542dd913f1a07b0d44e1d45e5e22e9/>. The page title is "redline". The main content area displays the analysis results, starting with a "Risk Assessment" section. The "malicious" label is prominently displayed at the top right. The "Incident Response" sidebar on the right lists various artifacts and tools used for analysis, such as CrowdStrike AI, File Details, Screenshots, and Notifications. The "Back to top" link is located near the bottom of the sidebar.

Risk Assessment

- Spyware**: Found browser information locations related strings
Hooks API calls
POSTs files to a webserver
Sets a computer-based training (CBT) hook
Tries to steal browser sensitive information (file access)
- Persistence**: Installs hooks/patches the running process
Spawns a lot of processes
Writes data to a remote process
- Fingerprint**: Queries kernel debugger information
Queries process information
Queries sensitive IE security settings
Queries the display settings of system associated file extensions
Queries the internet cache settings (often used to hide footprints in index.dat or internet cache)
Reads the windows installation language
Tries to identify its external IP address
- Evasive**: Contains ability to adjust token privileges
Contains ability to check if a debugger is running

Incident Response

- Related Sandbox Artifacts
- Indicators
- CrowdStrike AI
- File Details
- Screenshots (3)
- Hybrid Analysis (50)
- Network Analysis
- Extracted Strings
- Extracted Files (35)
- Notifications
- Community (0)

[Back to top](#)

The screenshot shows the Hybrid Analysis interface with the following sections:

- Contacted Hosts:** A table listing contacted hosts with columns: IP Address, Port/Protocol, Associated Process, and Details. The table includes rows for various IP addresses, ports (e.g., 443, 80), protocols (TCP), processes (e.g., 62237fa56f568_satt5e879a0c5.exe), and details indicating the United States, United Kingdom, Germany, or Russian Federation.
- Contacted Countries:** A world map showing connections between the United States and other countries like the United Kingdom, Germany, and Russia.
- Network Analysis:** A sidebar menu with options like Incident Response, Related Sandbox Artifacts, Indicators, CrowdStrike AI, Screenshots (3), Hybrid Analysis (50), Network Analysis (selected), DNS Requests (17), Contacted Hosts (10), Contacted Countries, HTTP Traffic (22), Memory Forensics (1), Extracted Strings, Extracted Files (35), Notifications, and Community (0).
- Bottom Bar:** A toolbar with various icons for file operations and navigation.

Contacted hosts findings in the network analysis of the incidence response.

Summary

Malware analysis. However, this was just scratching the surface.

- Static and Dynamic analysis of malware
- Finding strings, calculating hashes, and running AV scans on malware
- Introduction to the PE header and how to use information from it in malware analysis
- Sandboxing and different online sandboxes that we can use
- How malware evades the techniques we just discussed.

PHISHING

Email Protocols and Message Flow

Email Protocols:

- Email transactions involve specific protocols designed for network-related tasks.
- Three main protocols facilitate outgoing and incoming email messages.

SMTP (Simple Mail Transfer Protocol):

- Handles the sending of emails.

POP3 (Post Office Protocol):

- Responsible for transferring email between a client and a mail server.
- Emails are downloaded and stored on a single device.
- Sent messages are stored on the same device.
- Accessible only from the device where emails were downloaded.
- Enable "Keep email on server" to retain messages on the server.

IMAP (Internet Message Access Protocol):

- Also responsible for transferring email between a client and a mail server.
- Emails are stored on the server and can be downloaded to multiple devices.
- Sent messages are stored on the server.
- Messages can be synced and accessed across multiple devices.

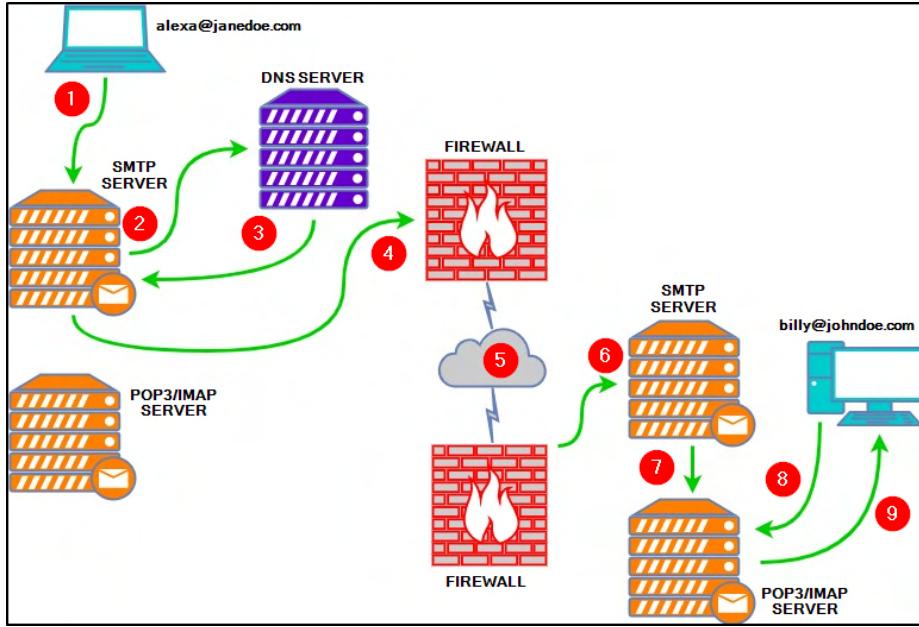
Email Transmission Steps:

Below is an explanation of each numbered point from the above diagram:

1. Alexa composes an email to Billy (billy@johndoe.com) in her favorite email client. After she's done, she hits the send button.

- 2 . The **SMTP** server needs to determine where to send Alexa's email. It queries **DNS** for information associated with johndoe.com.
- 3 . The **DNS** server obtains the information johndoe.com and sends that information to the **SMTP** server.
- 4 . The **SMTP** server sends Alexa's email across the Internet to Billy's mailbox at johndoe.com.
- 5 . In this stage, Alexa's email passes through various **SMTP** servers and is finally relayed to the destination **SMTP** server.
- 6 . Alexa's email finally reached the destination **SMTP** server.
- 7 . Alexa's email is forwarded and is now sitting in the local **POP3/IMAP** server waiting for Billy.
- 8 . Billy logs into his email client, which queries the local **POP3/IMAP** server for new emails in his mailbox.
- 9 . Alexa's email is copied (**IMAP**) or downloaded (**POP3**) to Billy's email client.

Lastly, each protocol has its associated default ports and recommended ports. For example, **SMTP** is port 25.



Email Body

So far everything has been straightforward . One important thing to note is that contents within a pdf file that are encoded from base64 data have to be decoded in human readable format. One notable for example is a email , which consists of a pdf file. Since the base 64 data is very lengthy , we simply just copied the contents and pasted in in cyberchef.

The screenshot shows the CyberChef interface on a Mac OS X desktop. The title bar reads "Brave" and "gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B%3D',true,false)&input=CgpKVkJFU...". The main area has a sidebar with various operations like "Operations", "Search...", "Favourites", "To Base64", "From Base64", etc. The "Recipe" section is set to "From Base64" with the alphabet "A-Za-z0-9+=". The "Input" section contains a very long base64 encoded string. The "Output" section shows the decoded PDF content, which includes a header "%PDF-1.6\n", some binary data, and a footer "%EOF". The status bar at the bottom indicates "47715 ⌂ 623".

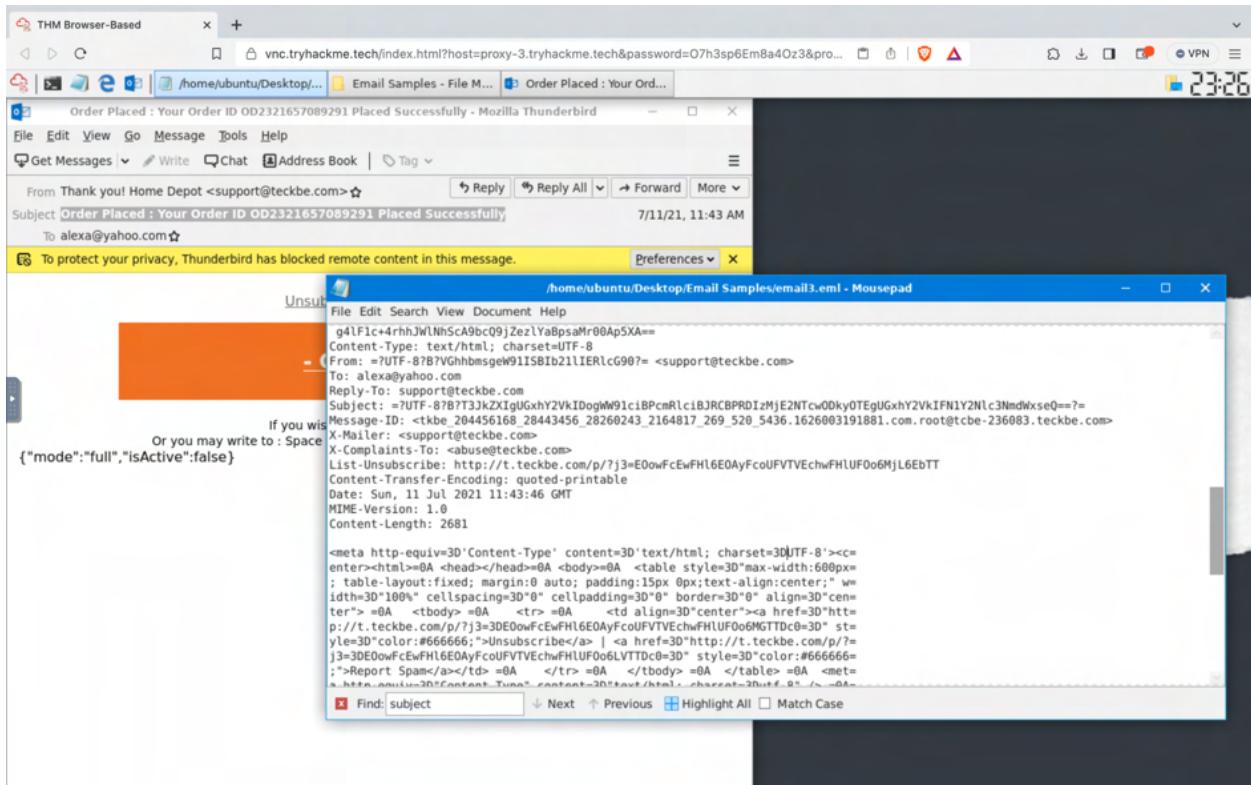
Then we selected the from base64 recipe and dragged it, and bake. We then saved the output to a pdf file .

The screenshot shows the Mac OS X Finder window titled "Downloads". It lists a single file named "download.pdf". The file is a PDF document, as indicated by the icon and the "Kind" column in the list view.

Once we saved it to a pdf file, then we should be able to view the BASE64 contents decoded of the pdf file

The screenshot shows a web browser window displaying the PDF file "download.pdf". The content of the PDF is visible as a single page with the text "THABENOR_PP_ATTACHMENT".

EMAIL ANALYSIS PHISING



From the given samples we can find some useful information given the email headers. We can find the sender's address which is stated in the above screen shot. A way to find other valuable information such as which entity the sender has masqueraded as or in other words spoofed, we can use the given platform to open the email sample. From the analysis we can see in the email that the sender has spoofed using home depot. This information apparently was not visible within the sample file. Another factor was subject, that was encoded, we learned that the subject of the email could be retrieved by simply opening the email through the thunderbird application. A link was placed by the sender, which was also retrieved through the thunderbird application.

PHISHING CASE

Used email headers to find relevant information. There are many useful tools one can use to find useful information from a phishing email. The one listed below is from google, called message header. It appears to be user friendly and one can navigate through the findings to for analysis

Messageheader

Received: from 10.197.37.234 by atlas105.free.mail.bf1.yahoo.com with HTTPS; Wed, 7 Jul 2021 02:14:46 +0000

Return-Path: <postmaster@teknko.xyz>

X-Originating-Ip: [209.85.167.226]

X-Spam-Score: none (domain of etekno.xyz does not designate permitted sender hosts)

Authentication-Results: atlas105.free.mail.bf1.yahoo.com; dkim=unknown; spf=none smtp.mailfrom=metekno.xyz;

Created at: 7/6/2021, 7:14:40 PM PDT (Delivered after 6 sec)

From: Netflix <JGQ47wazXe1YVBrkeDg-J0g700DQwWdr@J0g700DQwWdr-ykV

To: redacted@yahoo.com

Subject: Your Netflix Account is Hold

SPF: none
Learn more

DKIM: unknown with domain Unknown!
Learn more

DMARC: unknown
Learn more

File Edit Search View Document Help

Delay From

6 sec

CSV To JSON

CSV To PDF

CSV To XML

CSV To CSV

HTML Lines To CSV

HTML To CSV

HTML To PDF

HTML To XML

HTML To JSON

HTML To CSV

HTML To PDF

HTML To XML

HTML To JSON

Data Tools

CSV Template Engine

CSV To JSON

CSV To PDF

CSV Editor

CSV To XML

CSV To CSV

CSV Extractor

Phone Extractor

CSV To PDF

URL Extractor

CSV To XML

CSV Extractor

CSV Home

Step 2: Choose output options (optional)

Step 3: Extract URLs

Extract Extract To Excel

Result Data

<http://schema.org/>

<https://>

https://www.rapidapi.com/us/rapidapi/icons/icon_plain_white.json

<https://fonticons.com>

<https://quickanddirtytools.com/icon/icon.php?icon=play&size=16>

<https://imagekit.io/email/ibfa9bf1372754d00707d1516/kgoge>

<https://i.imgur.com/2DnD9mgTemp0D1>

<https://i.imgur.com/2DnD9mgTemp0D0>

Save your result: convertcsv.cdr | Download Result | EOL | CRLF |

The url extractor is a pretty useful tool for finding all of the urls that are listed. Typically this could also be located in the e-mail body.

The screenshot shows a Firefox browser window with several tabs open, including 'Using the Blind Carbon', 'TryHackMe | Learning', 'TryHackMe | Phishing', 'Message Header Analyzer', 'TryHackMe | Phishing', and 'Private browsing'. The main content area is titled 'Message Header Analyzer' and contains a large block of encoded text starting with 'g(77, 77);color:inherit;">' followed by various header fields. Below this is a table with 14 rows, each representing a header field with its value. The table includes columns for 'Header', 'Value', and 'Type'. The 'Value' column for X-Google-OKM-Signature contains a very long string of characters.

Header	Type	Value
7-X-Header		//ayAHH10H9XoIPcAn_MasOsVUH8MNqsjenZAAJNhzvPtu1WdpyqdsAugusuz pwrJHdu/dsobt/qvbyK yplzazuzrVwI8VXuHv2YU_yvw8XLH2RjLJXqHPQwzLMJHienJ4CjstAUJre/uk3ity+QyptN3aHkYb33.SOMHprRuQqYi0jUkzev0S3XWhp27SiQjwM7HOgva-
7-X-Google-OKM-Signature		v=1; anno=sha256; c=related;relaxed; d=1e100.net; s=20161025; hr=x-gm-message-state message-id=date to from subject:mime-version; bh=HLZRRPrbarLnjceKEGgNmzTn4kOdad8jRPQ2QPMEm; b=hPz6oyzaNDXDeDdURm56t*X+p72n#f29p4XmJndpws2BMZYohf3k+30Ne3 3dECPmIEOnvAegzrhJLtaTe4rhJhqv2J2B6g119mYIKSEN+yyIGOs1qph1Z6TwvUIMCkeymfEPsJuQ9J78r++/VX1YRA4D0T/KoFNT1CGxJtZQkIDhNuJxAbpKZMaPsf#[2lPOQuaOC6YVWP78859WOS9HMaAvBjYwPTMXZMNV1T1K1ESCW1Qodf1MPCQwVYb0YA2JZ9JTrgSN33JrwVutbxpCu+HVR/DBz0JUtmWQJlo4cvg==
8-X-Gm-Message-State		AOAM533EZsiaMkM3IewHUBGUujhifEr1gPuAbhEfJWIKu2wn4r+yJnjqmCnQkUypnZ7wp/WbqyadB9Q8Bsq2S/dspqOO==
9-X-Google-Smtb-Source		ABdhpJz6YR00AT7zgRfB2ugW7RJ203BYkm4HFIBuawJapAdMqALah5wGCRAB13lZk9h5o9wVEct
10-X-Received		by 2002.aca.eff0: with SMTP id nfm16727904oh.66.1625624086463; Tue, 06 Jul 2021 19:14:46 -0700 (PDT)
11-X-Relaying-Domain		elektro.ng
12-X-Mailer		Microsoft Office Outlook, Build 11.0.5510
13-X-ContentID		19380
14-X-ContentBase		/Portal/content/DollarGeneral

The message header analysis is also a useful tool to find important information such as domain of interest, submitting host, received host, protocols and IP addresses.

Phishing case 2 lab

In this lab we analyzed a malicious attachment from a phishing email through a online malware sandbox platform for analysis, we can analyze the network and discover other important details. In summary we discovered how the email was classified which was suspicious. We discovered a pdf file, SHA 256 of the pdf file was available. A windows process file was flagged as potentially bad traffic. In addition we can click and view screen shots of the live e-mail, in terms of how a potential victim could be a target.

The screenshot shows a Firefox browser window with the URL <https://app.any.run/tasks/8bfd4c58-ec0d-4371-bfeb-52a334b69f59/>. The main content is a phishing page for Netflix, prompting the user to update payment details. The page includes a message to the customer, a 'MOVE YOUR MOUSE TO VIEW SCREENSHOTS' instruction, and a warning about trouble with current billing information. Below the main content is a table of network traffic and processes.

HTTP Requests	Connections	DNS Requests	Threats	PCAP
14	41	20	1	
Timeshift	Protocol	PID	Process name	CN IP Port Domain ASN Traffic
55661 ms	TCP	3228	explorer.exe	176.34.132.62 443 help.netflix.com Amazon.com 351 b
56657 ms	TCP	1840	explorer.exe	45.57.90.1 443 assets.netflix... Netflix Stream... 505 b
56658 ms	TCP	1840	explorer.exe	45.57.90.1 443 assets.netflix... Netflix Stream... 771 b
57760 ms	TCP	1776	svchost.exe	2.16.107.83 443 ardownload3... Akamai Intern... 133 b
57761 ms	TCP	1776	svchost.exe	2.16.107.83 443 ardownload3... Akamai Intern... 58 b
58745 ms	TCP	3812	AdobeAEM.exe	2.16.107.83 443 ardownload3... Akamai Intern... 524 b

Suspicious activity

MD5: 4A2775EA2B8EF41901A3F08D3B857C8
Start: 21.07.2021, 20:45 Total time: 60 s
Win7 32 bit Complete generated.doc

Indicators:

- Get sample
- IOC
- MalConf
- ATT&CK matrix
- Restart
- Text report
- Process graph
- ATT&CK matrix
- Export

Processes

PID	Process Name	Type	File Path	RAM
2088	AcroRd32.exe	-type=renderer	"C:\Users\admin\AppData\Local\Temp\Payment-updated.pdf"	15k 8k 141
3368	RdrCEF.exe	-backgroundcolor=16514043		3k 1k 122
2940	RdrCEF.exe	-type=renderer -log-file="C:\Program Files\Adobe\Acrobat Reader D...	444 11 75	
700	RdrCEF.exe	-type=gpu-process -field-trial-handle=1168,7591836415733672309...	362 5 73	
3752	RdrCEF.exe	-type=gpu-process -field-trial-handle=1168,7591836415733672309...	363 5 73	
2304	RdrCEF.exe	-type=gpu-process -field-trial-handle=1168,7591836415733672309...	364 5 73	
2836	RdrCEF.exe	-type=renderer -log-file="C:\Program Files\Adobe\Acrobat Reader D...	364 5 73	

The screenshot shows a Firefox browser window with the address bar pointing to <https://any.run/report/cc6f1a04b10bcb168aeecc8d870b97bd7c20fc161e8310b5bce1af8ed420e2c2>. The main content is a malware analysis report from ANY.RUN. At the top, there are promotional banners for "Huge database of samples and IOCs", "Custom VM setup", "Unlimited submissions", and "Interactive approach". A "Sign up, it's free" button is also visible. Below this, the "Connections" section lists network activity:

PID	Process	IP	Domain	ASN	CN	Reputation
384	RdrCEF.exe	3.233.129.217:443	p13n.adobe.io	—	US	unknown
980	explorer.exe	35.244.149.249:443	lihi1.com	—	US	unknown
3228	explorer.exe	93.184.220.29:80	ocsp.digicert.com	MCI Communications Services, Inc. d/b/a Verizon Business	US	whitelisted
3228	explorer.exe	2.18.232.136:443	help.netflix.com	Akamai International B.V.	—	whitelisted
3228	explorer.exe	176.34.132.62:443	help.netflix.com	Amazon.com, Inc.	IE	unknown
3228	explorer.exe	104.16.149.64:443	cdn.cookielaw.org	Cloudflare Inc	US	unknown
3228	explorer.exe	104.20.184.68:443	geolocation.onetrust.com	Cloudflare Inc	US	shared
1776	svchost.exe	2.16.107.83:443	ardownload3.adobe.com	Akamai International B.V.	—	malicious
3812	AdobeARM.exe	2.16.107.83:443	ardownload3.adobe.com	Akamai International B.V.	—	malicious
1840	explorer.exe	45.57.90.1:443	assets.netflixext.com	Netflix Streaming Services Inc.	US	suspicious

Below the connections table, there is a "DNS requests" section with a table header:

Domain	IP	Reputation
--------	----	------------

At the bottom of the browser window, the Mac OS X Dock is visible, showing various application icons.

A helpful feature from the platform was a self generated report one could create . This lists important details such as PID, and ip address. Luckily it was readable and important labels such as malicious IP were available to analyze from the given report.

Phishing Case 3 lab.

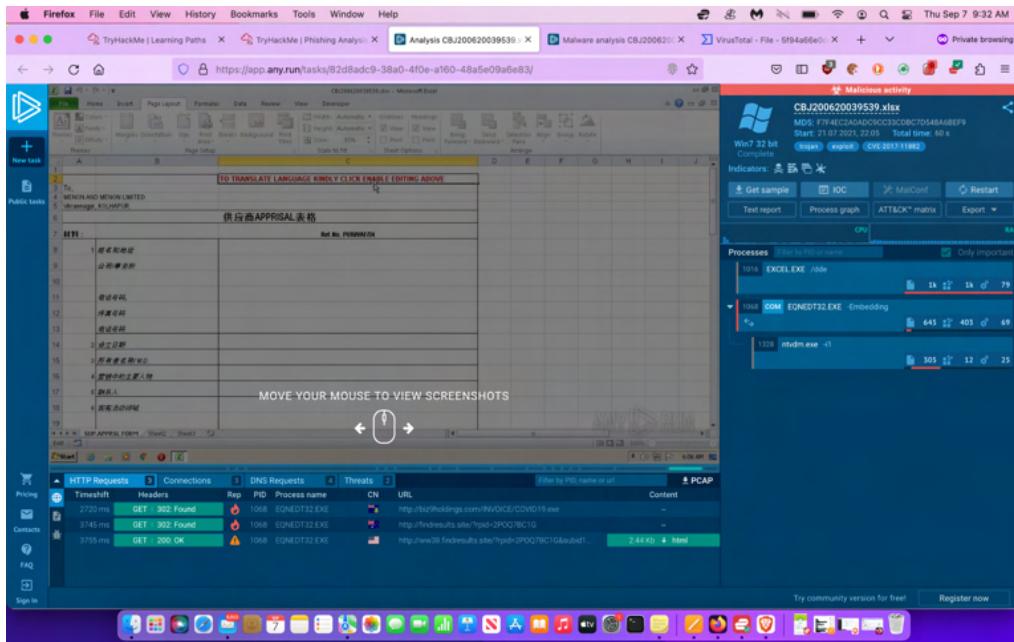
For this case , a sandbox with the suspicious email was provided. We retrieved the details , and we discovered a Malicious activity had been classified. From the given report generated, We learned that this time there was an excel file present. We traced 3 malicious domains, along with 3 malicious IP addresses. In addition we discovered the vulnerability that the malicious attachment attempted to exploit. That vulnerability happens to be **CVE-2017-11882**.

The screenshot shows the ANY.RUN malware analysis interface. At the top, it displays various tabs and a search bar. Below the tabs, there's a summary section with counts for HTTP(S) requests, TCP/UDP connections, DNS requests, and Threats. The main area contains three tables: 'HTTP requests', 'Connections', and 'DNS requests'. The 'HTTP requests' table lists three entries, all associated with process ID 1068 and labeled as 'malicious'. The 'Connections' table lists three entries, also associated with process ID 1068 and labeled as 'malicious'. The 'DNS requests' table is partially visible at the bottom. The interface has a dark theme with some light-colored sections and red buttons for 'malicious' detections.

HTTP(S) requests		TCP/UDP connections		DNS requests		Threats	
3		3		4		0	

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
1068	EQNEDT32.EXE	GET	302	204.11.56.48.80	http://bizHoldings.com/INVOICE/COVID19.exe	VG	—	—	malicious
1068	EQNEDT32.EXE	GET	302	103.224.182.251.80	http://findresults.site/?pid=2PQ7BC1G	AU	—	—	malicious
1068	EQNEDT32.EXE	GET	200	75.2.11.242.80	http://www38.findresults.site/?pid=2PQ7BC1G&subId=20210722-15052609-bee9-RbcB329e748d	US	html	2.44 Kb	malicious

PID	Process	IP	Domain	ASN	CN	Reputation
1068	EQNEDT32.EXE	204.11.56.48.80	bizHoldings.com	Confluence Networks Inc.	VG	malicious
1068	EQNEDT32.EXE	103.224.182.251.80	findresults.site	Trellian Pty. Limited	AU	malicious
1068	EQNEDT32.EXE	75.2.11.242.80	www38.findresults.site	AT&T Services, Inc.	US	malicious



VULNERABILITIES

CVE-2017-11882 Detail

Description

Microsoft Office 2007 Service Pack 3, Microsoft Office 2010 Service Pack 2, Microsoft Office 2013 Service Pack 1, and Microsoft Office 2016 allow an attacker to run arbitrary code in the context of the current user by failing to properly handle objects in memory, aka "Microsoft Office Memory Corruption Vulnerability". This CVE ID is unique from CVE-2017-11894.

Severity	CVSS Version 3.x	CVSS Version 2.0
CVSS 3.x Severity and Metrics:		
NIST: NVD	Base Score: 7.8 HIGH	Vector: CVSS:3.1/AV:L/AC:L/PR:N/U:R/S:U/C:H/I:H/A:H

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

QUICK INFO

CVE Dictionary Entry: CVE-2017-11882
NVD Published Date: 11/14/2017
NVD Last Modified: 03/16/2021
Source: Microsoft Corporation

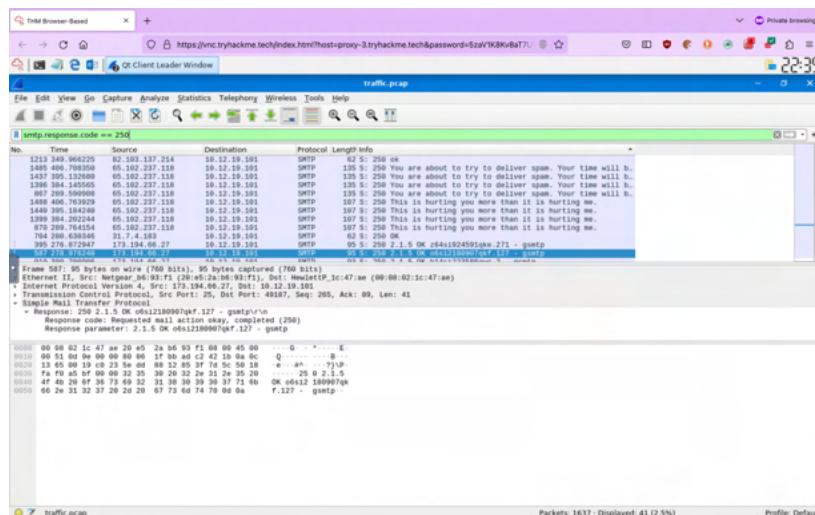
Phishing Prevention

In this lab we explored the various the various methods defenders can take to protect users from falling as a victim. The main focus for the first portion was email security using SPF, DKIM, DMARC. We explored mitigations as per the MITRE ATTA&CK Framework in terms of tricking targets.

A notable concept we explored was S/MIME which is an important concept learned from our SECURITY+ studies. We briefly touched on digital signatures and encryption, not ignoring the importance of public key cryptography.

SMTP STATUS CODES

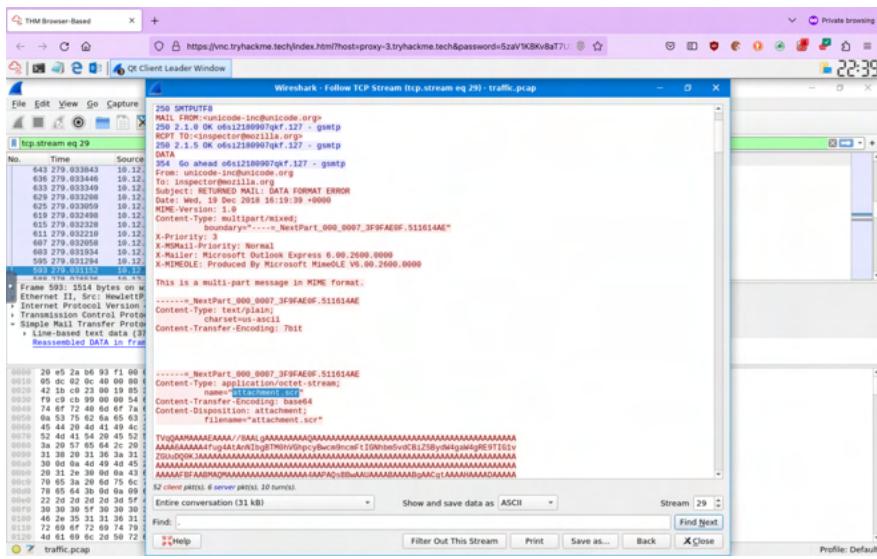
We proceeded on to the lab portion which involved SMTP status codes. We deployed wireshark, and completed the given scenario. Most of the portions were straightforward because we had our trusty wireshark documentation to guide us when filtering to analyze the given packet capture.



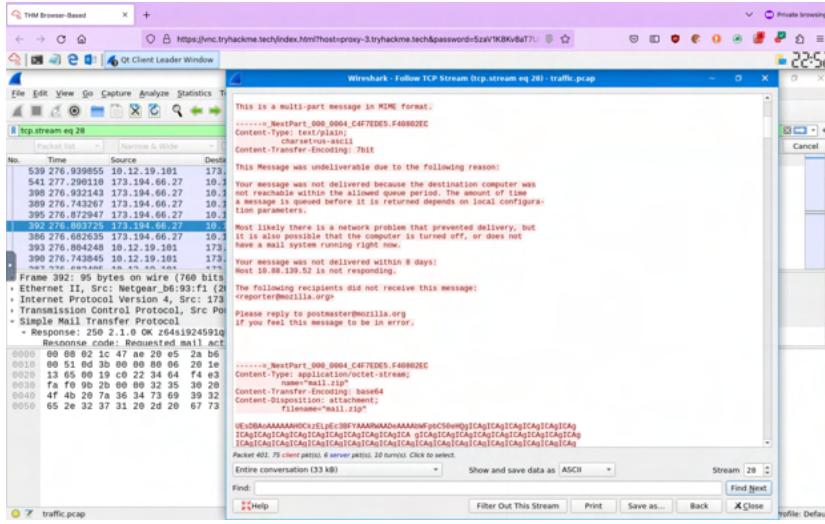
SMTP TRAFFIC ANALYSIS

In this portion of the lab we again explored packet capture analysis using wireshark on a virtual machine. Again most of it was straight forward using the given wire shark documentation. However, during our analysis we discovered some interesting findings which i will share.

During our analysis we discovered an attachment file



During our analysis we discovered an attachment file, we simply followed the tcp stream to retrieve the finding. We learned that the port the traffic was using was 25 catered to SMTP. The source ip address was 10.12.19.101 involved for all SMTP traffic. Finally relating to this we discovered the final attachment , which was mail.zip



Conclusion

Finally in conclusion an important aspect for SOC analysts to study was a given phishing IR playbook. The phishing playbook <https://www.incidentresponse.org/playbooks/phishing> summarizes an incident response by the NIST incident process. It covers **Prepare, Detect , Analyze, Contain , Eradicate , Recovery, Post-Incident Handling**.

Lab Scenario:

Here we investigated a E-mail sample via a virtual machine to determine if it was legitimate. The e-mail also contained an attachment . One important thing to note here is that it was a generic email with a generic good day greeting. We analyzed the email headers using thunderbird as the application.

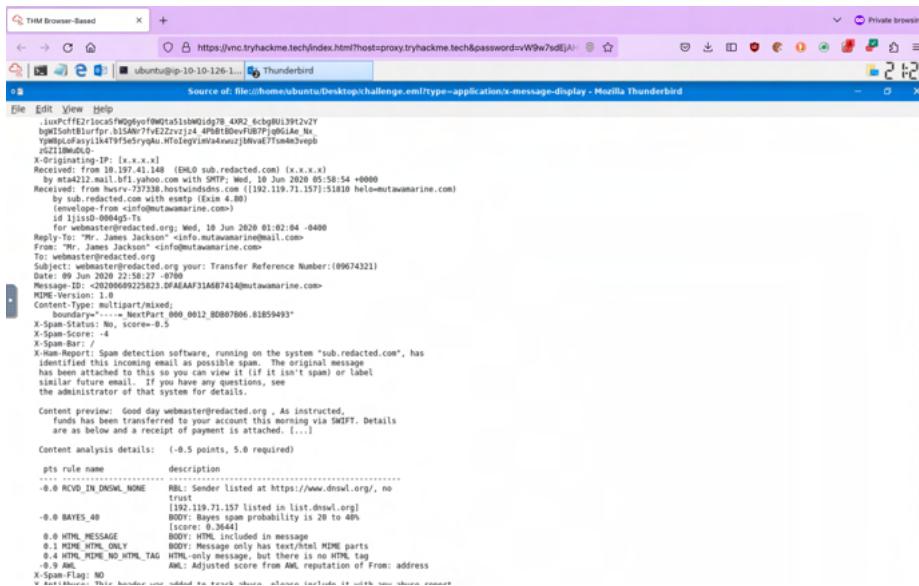
From the analysis we notice the date the e-mail was received, which was 6/10/20.

Email was from Mr James. Jackson

Email address: info@mutawamarine.com

Email address to receive a reply of email: info@mutawamarine.com

Originating ip address: 192.119.71.157



Next during our analysis we needed to run the whois command on our local terminal , so as we went ahead and did that .

Command : whois 192.119.71.157

From the terminal output , we notice that the owner of the originating IP address is Hostwinds LLC.

```
remarks: 192.168.0.0/16 are found Indiana-IPv4-Special-Registry.
remarks: 192.0.0/24 reserved for IANA IPv4 Special Purpose
remarks: Address Registry (RFC5736). Complete registration
REMARKS: details for 192.0.0/24 are found
REMARKS: Indiana-IPv4-Special-Registry.

whois: whois.arin.net

changed: 1993-05
source: IANA

# whois.arin.net

NetRange: 192.119.64.0 - 192.119.127.255
CIDR: 192.119.64.0/18
NetName: HOSTWINDS-18-2
NetHandle: NET-192-119-64-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: Direct Allocation
OrgASes: ASS4396
Organization: Hostwinds LLC. (HL-29)
RegDate: 2012-11-12
Updated: 2021-09-23
Comment: https://www.hostwinds.com
Comment: Abuse Contact: abuse@hostwinds.com
Ref: https://rdap.arin.net/registry/p/192.119.64.0

OrgName: Hostwinds LLC
OrgId: HL-29
Address: 12101 Tukwila International Blvd, 3rd Floor, Suite 320
City: Seattle
StateProv: WA
PostalCode: 98168
Country: US
RegDate: 2011-11-30
Updated: 2021-09-23
Comment: https://www.hostwinds.com
Comment: Abuse Contact: abuse@hostwinds.com
Ref: https://rdap.arin.net/registry/entity/HL-29

ReferralServer: rwhois://rwhois.hostwinds.net:4321

OrgTechHandle: HNOC9-ARIN
OrgTechName: Hostwinds Network Operations Center
OrgTechPhone: +1-206-886-8665
OrgTechEmail: support@hostwinds.com
OrgTechRef: https://rdap.arin.net/registry/entity/HNOC9-ARIN

OrgAbuseHandle: HAC3-ARIN
OrgAbuseName: Hostwinds Abuse Center
OrgAbusePhone: +1-206-886-8665
OrgAbuseEmail: abuse@hostwinds.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/HAC3-ARIN

OrgNOCHandle: HNOC9-ARIN
OrgNOCName: Hostwinds Network Operations Center
OrgNOCPhone: +1-206-886-8665
OrgNOCEmail: support@hostwinds.com
OrgNOCRef: https://rdap.arin.net/registry/entity/HNOC9-ARIN

(base) Faizs-MacBook-Pro:~ Faizs
```

To find SPF record for return path

Command: nslookup -type=txt mutamarine.com

```
(base) Faizs-MacBook-Pro:~ faiz$ nslookup -type=txt mutamarine.com
Server:      100.64.100.1
Address:     100.64.100.1#53

** server can't find mutamarine.com: NXDOMAIN

(base) Faizs-MacBook-Pro:~ faiz$ nslookup -type=txt mutawamarine.com
Server:      100.64.100.1
Address:     100.64.100.1#53

Non-authoritative answer:
mutawamarine.com      text = "MS=ms97822417"
mutawamarine.com      text = "MS=842BCB91F2AB2807BE05D25DC690D1226B349676"
mutawamarine.com      text = "v=spf1 include:spf.protection.outlook.com -all"

Authoritative answers can be found from:

(base) Faizs-MacBook-Pro:~ faiz$
```

To find the DMARC record for the return path domain we used the dig command

Command: dig TXT _dmarc.mutawamarine.com

We notice that it is **v=DMARC1; p=quarantine; fo=1**

```
(base) Faizs-MacBook-Pro:~ faiz$ dig TXT _dmarc.mutawamarine.com
; <<>> DiG 9.10.6 <<>> TXT _dmarc.mutawamarine.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62614
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;_dmarc.mutawamarine.com.      IN      TXT
;;
;; ANSWER SECTION:
_dmarc.mutawamarine.com. 3600    IN      TXT      "v=DMARC1; p=quarantine; fo=1"
;;
;; Query time: 111 msec
;; SERVER: 100.64.100.1#53(100.64.100.1)
;; WHEN: Mon Sep 11 17:34:45 PDT 2023
;; MSG SIZE  rcvd: 93
(base) Faizs-MacBook-Pro:~ faiz$ █
```

Finally from our analysis we were found out that the attachment was named **SWT_#09674321_PDF_.CAB**. From there on we used the hybrid analysis to find out the **SHA256: 2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f**
File Extension: RAR

Analysis Overview

Submission name: **SWT_#09674321_PDF_.CAB**
 Size: 400KB
 Type: **unknown**
 Mime: application/x-rar
 SHA256: **2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f**
 Last Anti-Virus Scan: 07/21/2023 18:13:12 (UTC)
 Last Sandbox Report: 01/02/2022 16:57:41 (UTC)

Anti-Virus Results

Scanner	Threat Score	Malware Label
MetaDefender	3%	Multi Scan Analysis
VirusTotal	60%	Multi Scan Analysis

From our analysis we can infer that the file attachment was indeed malicious , marked as a **Trojan.Generic**

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
March 11th 2023 10:01:01 (UTC)	SWT_#09674321_PDF_.CAB_INFECTED.zip Zip archive data, at least v2.0 to extract c1d3c0b-4270f484-07559458d7ed9bddd621a4d0fa2993649fd9d06ca59fd	no specific threat	AV Detection: Marked as clean	-	Windows 7 32 bit	<input type="checkbox"/>
January 2nd 2022 16:57:41 (UTC)	attachment.pdf.cab RAR archive data, v8.7. 2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f	malicious	AV Detection: 32% Trojan.Generic	-	Windows 7 64 bit	<input type="checkbox"/>
December 31st 2021 20:30:12 (UTC)	SWT_#09674321_PDF_.CAB RAR archive data, v8.7. 2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f	malicious	AV Detection: 32% Trojan.Generic	-	Windows 7 64 bit	<input type="checkbox"/>

Finally we utilized virus total to find the exact file size of the pdf attachment (SWT_#09674321_PDF_.CAB) plugging in the SHA-256 we discovered on hybrid analysis.

We discovered that the file size of the attachment was actually 400.26 KB

The screenshot shows a Firefox browser window with the address bar pointing to <https://www.virustotal.com/gui/file/2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f>. The page content includes:

- Basic properties:**
 - MD5: f4dd3456cd976a145c1179ad4d461ec
 - SHA-1: 5a2bb0188377c15c036843b4a6ab9bc0f2c1607
 - SHA-256: 2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f
 - SSDEEP: 12288:Mj6ygt8RoYqManuL8lOA81a8Yolm9-X3B4k5:EgoRJCul87tolC+X3O
 - TLSH: T12C94238893562439A8F7385DAFD0CFB5EFE898E74E8F97709CFD609E5D140446205AC2
 - File type: RAR compressed rar
 - Magic: RAR archive data, v5
 - TrID: RAR compressed archive (v5.0) (61.5%) RAR compressed archive (gen) (38.4%)
 - File size: 400.26 KB (409868 bytes)
- History:**
 - First Submission: 2020-06-10 07:06:14 UTC
 - Last Submission: 2023-08-17 17:23:53 UTC
 - Last Analysis: 2023-09-07 17:45:53 UTC
- Community:** A section encouraging users to join the VT Community.

