Malware Analysis

OF A WORD DOCUMENT FILE

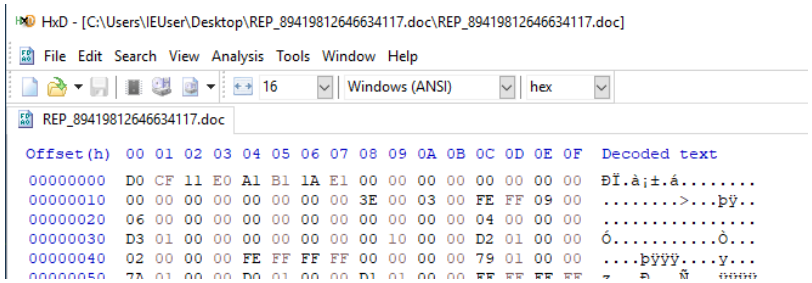
Robert Christopherson | Blue-Team | 12.20.2022

Overview

- Tools used
    - HxD
    - PEStudio
    - olevba.py
    - FakeDNS
    - Wireshark
    - Remnux
    - Cyber Chef
    - Fiddler
    - inetsim
    - Procmon
- Objective
    - Using a suite of tools, determine if a word document is malicious or not.
    - Perform the analysis is a contained environment for security and safety.

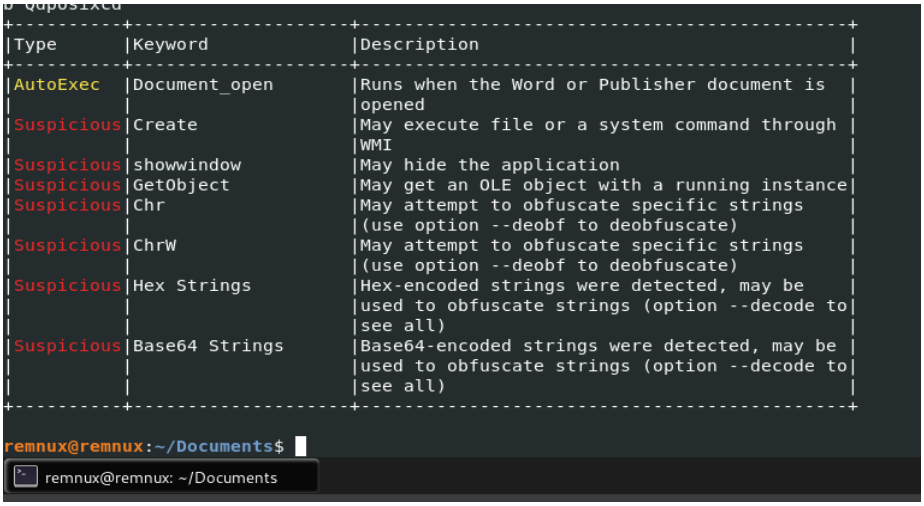
Method

- Static Analysis
    - Load up a Remnux Virtual Machine and ensure the target file is on that machine.
        - The safest way to move malicious files around is in a zipped file.
    - Using HxD we can view the Word document in hexadecimal.
        - The first characters of the file are “D0 CF 11 E0”.
        - This is the unique marker for “Doc File” (Word Document File).
        - The file is a legitimate Word Doc file.



    - Using PEStudio in our initial assessment we can view artifacts of any executables such as macros.
        - Receiving 12 indicators we can dig deeper
    - Running olevba.py against the file returns suspicious actions.
        - The file will autorun macros at open

- It appears that the script will attempt to open a system command such as CMD in hidden mode and immediately try to run its payload.



- Dynamic Analysis
  - Set up and configured a Windows 10 Virtual Machine to run the malware on.
    - Installed Procmon, Wireshark and fiddler to catch the processes and traffic created from executing the malware.
  - Ensure that your virtual machines are first fully sandboxed and not connected to any external network interfaces.
  - For this lab, I set up inetsim and FakeDNS to simulate a real network connection.
  - Execute the malware on the Windows VM.
  - Immediately we see a CMD window open then disappear.
    - Confirmed by Procmon as we can see a PowerShell process created.

  - Reports from inetsim, Wireshark and fiddler all confirm the malware was attempting to access 5 malicious sites with the visible DNS queries.
    - amelano.net
    - 911concepts.com
    - anyonschoools.com
    - beech.org
    - fireelabo.com

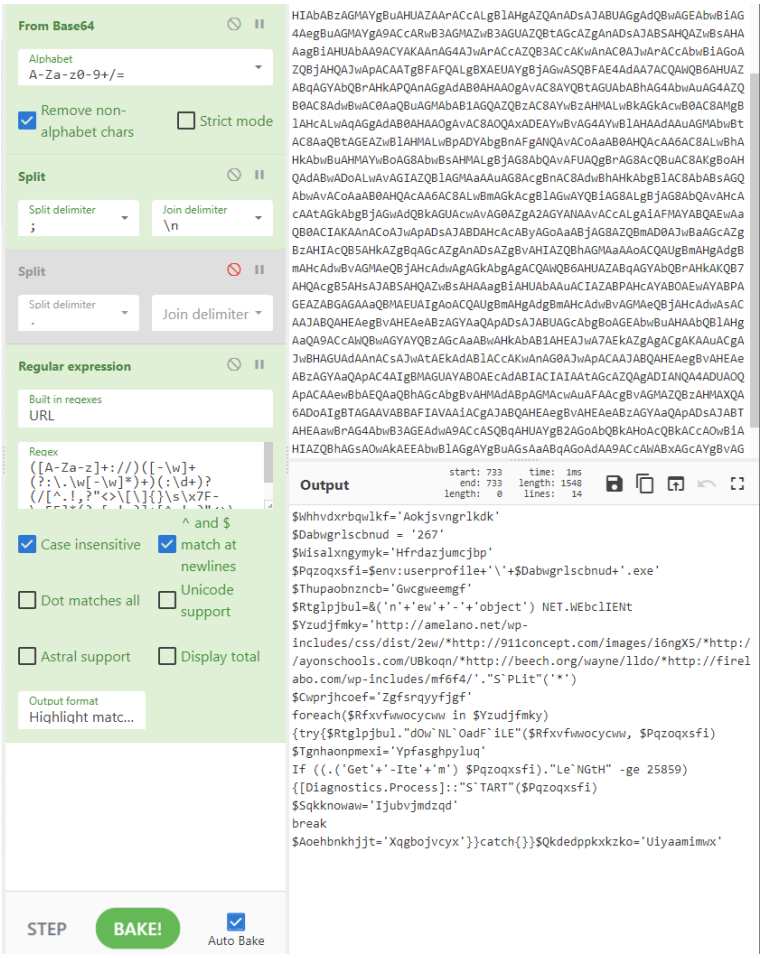
6	200	HTTP	amelano.net	/wp-includes/css/dist/2ew/
7	200	HTTP	911concept.com	/images/i6ngX5/
8	200	HTTP	ayonschools.com	/UBkoqn/
9	200	HTTP	beech.org	/wayne/lldo/
10	200	HTTP	firelabo.com	/wp-includes/mf6f4/
11	200	HTTP	Tunnel to	self.events.data.microsof...

```
remnux@remnux:~$ sudo cat /var/log/inetsim/report/report.66282.txt
=== Report for session '66282' ===

Real start date            : 2022-12-17 19:11:45
Simulated start date       : 2022-12-17 19:11:45
Time difference on startup : none

2022-12-17 19:12:14  First simulated date in log file
2022-12-17 19:12:14  HTTP connection, method: GET, URL: http://amelano.net/wp-includes/css/di
st/2ew/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2022-12-17 19:12:14  HTTP connection, method: GET, URL: http://911concept.com/images/i6ngX5/,
 file name: /var/lib/inetsim/http/fakefiles/sample.html
2022-12-17 19:12:14  HTTP connection, method: GET, URL: http://ayonschools.com/UBkoqn/, file
name: /var/lib/inetsim/http/fakefiles/sample.html
2022-12-17 19:12:14  HTTP connection, method: GET, URL: http://beech.org/wayne/lldo/, file na
me: /var/lib/inetsim/http/fakefiles/sample.html
2022-12-17 19:12:14  HTTP connection, method: GET, URL: http://firelabo.com/wp-includes/mf6f4
/, file name: /var/lib/inetsim/http/fakefiles/sample.html
2022-12-17 19:12:14  Last simulated date in log file

===
remnux@remnux:~$
```



- Using CyberChef to decode the Base64 code that was contained within the malware we can see all 5 of these sites listed in the code.

Conclusion

- This Word document was an initial attack via a phishing attempt that once executed would call out to multiple servers
- Presumably this would download and execute more payloads.
- We did not see any attempts at data exfiltration.

Resources

- pestudio
- HxD
- olevba.py
- FakeDNS
- Wireshark
- Remnux
- Cyber Chef
- Fiddler
- inetsim
- Procmon