

1.0 Summary

Findings and observations: Sample is a .PDF file that was received in an Hotmail account that has been compromised multiple times over the years. This sample contains several links to download files from a few different sites, however upon trying to activate these links they had already been taken down. The sites linked to were generic file sharing sites, and file types included .EXE, .ACE, .RTF, .ZIP and .SCR files. The email was received from a domain currently registered in Malaysia and associated with a person purported to be living in Kansas, which could lead to further information about the source.

Recommendations: Try to examine samples within 72 hours of receipt next time. Upgrade licenses to enable better analysis of 64-bit code.

Conclusion: Missed the window to obtain additional files that would have been downloaded/launched by this document. Act faster on similar samples in the future. Online virus scanning sites may be ineffective in detecting malicious files such as these, and can also produce false positives and/or flag normal program behavior as suspicious.

1.1 Identification

File name: Seminar_Cyber_Security_2016.pdf

File Type: PDF / 1.4

Malware name(s): Unknown

Current detection: Sophos (1/55 ratio on Virustotal)

Malware type: Trojan/Downloader/Launcher

Size: 973,253 bytes

Packer: Not packed

Encryption/encoding: N/A

Origin: Malaysia

Compile time: N/A

Hashes

MD5: e34be1974edb9f4e5da79341e1e37ba0

SHA1: 1850e0df012645032a3c3590321c3724ef79a894

SHA256: 13ece20c212f01cff1532c25d2635aeb04aef432e63a161ac6a0953f6929de9a

ssdeep: 24576:WZN4hqDYFuf9SZm+QbgmOMmF/USoyZY4VlhZyzNOa:WNsCaBQeM01e4VIuNOa

Test environment details: Win 7 Home Premium SP1 running in VirtualBox 5.0.18_Ubuntu r106667 on Ubuntu 16.04. Hardware is an Acer Aspire 5742 (Intel i3).

1.2 Dependencies

OS: N/A

Imports: N/A

Exports: N/A

Other: N/A

2.0 Characteristics

2.1 Behavior

File links to various other files on several different filesharing websites. Links were dead at time of analysis so no further information available. No other behaviors noticed locally, no network traffic

observed besides when the user followed links in the document. SQLite db dropped in one of the local user Acrobat directories, appears to be normal part of Acrobat Reader operation.

2.2 Infection

None observed. Presumed that any infection would have been accomplished with one of the other files linked to in the document.

2.3 Persistence

None observed.

2.4 Movement

None observed.

2.5 Data Exfiltration

None observed.

2.6 C²

None observed.

2.7 Signatures

Network signatures include HTTP activity on ports 80 and 443 to these addresses (when links followed):

https://volafire.io/get/pUdLP3Rpw64zZA/doc_PO-0930.scr

<http://fastfglobal.coxslot.com/scan-copy%E2%80%AEfdp.zip>

<http://fastfglobal.coxslot.com/password.rtf>

<http://buffet.honor.es/PcCleanUp.exe>

http://buffet.honor.es/Invitation_CS_Training.ace

3.0 Recommendations

From the user perspective, oft-repeated recommendations about not opening strange documents or following links from unsolicited email would apply. This particular file does not appear to do anything besides serve malicious links, so this practice alone could help prevent issues from this malware. Malicious code execution upon opening the document has not been ruled out, however, so the recommendation against opening strange files stands.

From the administrative perspective, various recommendations could be formed depending on the environment. Executables could be whitelisted to prevent the execution of strange files such as the above-mentioned PcCleanUp.exe file. These and similar file-sharing sites could be blocked in favor of other file sharing methods. Rules could be developed regarding the sender and email body itself to block similar messages from being delivered. Antivirus solutions may have success in preventing some of the payload files above from being opened/executed.

4.0 Raw Notes

4.1 Static Analysis

Using strings and pdf-parser, observed the following URLs in the document:

https://volafire.io/get/pUdLP3Rpw64zZA/doc_PO-0930.scr

<http://fastfglobal.coxslot.com/scan-copy%E2%80%AEfdp.zip>
<http://fastfglobal.coxslot.com/password.rtf>
<http://buffet.honor.es/PcCleanUp.exe>
http://buffet.honor.es/Invitation_CS_Training.ace

PDFiD information

- This PDF file contains an open action to be performed when the document is viewed. Malicious PDF documents with JavaScript very often use open actions to launch the JavaScript without user interaction.
- This PDF document has 1 page, please note that most malicious PDFs have only one page.
- This PDF document has 72 object start declarations and 72 object end declarations.
- This PDF document has 25 stream object start declarations and 25 stream object end declarations.
- This PDF document has a cross reference table (xref).
- This PDF document has a pointer to the cross reference table (startxref).
- This PDF document has a trailer dictionary containing entries allowing the cross reference table, and thus the file objects, to be read.

4.2 Dynamic Analysis

Sandbox observed a SQLite file dropping. Found this file in C:\Users\[USER]\AppData\Local\Adobe\Acrobat\DC, header is below:

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	53	51	4C	69	74	65	20	66	6F	72	6D	61	74	20	33	00	SQLite format 3
00000010	04	00	01	01	00	40	20	20	00	00	00	01	00	00	00	03	@
00000020	00	00	00	00	00	00	00	00	00	00	00	02	00	00	00	04	
00000030	00	00	00	00	00	00	00	00	00	00	00	01	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	01	
00000060	00	2D	E2	22	0D	00	00	00	02	02	80	00	02	EC	02	80	-â" € i €
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

4.3 Disassembly

From IDA Pro:

```

* seg000:000ECD A7 6F
* seg000:000ECD A8 62
* seg000:000ECD A9 6A
* seg000:000ECD AA 0D
* seg000:000ECD AB 3C
* seg000:000ECD AC 3C
* seg000:000ECD AD 2F
* seg000:000ECD AE 50
* seg000:000ECD AF
seg000:000ECD AF 72 6F
seg000:000ECD AF
* seg000:000ECDB1 64
seg000:000ECDB2
seg000:000ECDB2 75 63
seg000:000ECDB4
* seg000:000ECDB4 65 72 28
seg000:000ECDB4

```

```

db 6Fh ; 0
db 62h ; b
db 6Ah ; j
db 0Dh
db 3Ch ; <
db 3Ch ; <
db 2Fh ; /
db 50h ; P

```

```

; -----
;         jnb     short loc_ECE20      ; Jump if Below (CF=1)
; -----
;         db      64h ; d
; -----
;         jnz     short near ptr loc_ECE16+1 ; Jump if Not Zero (ZF=0)
;         db      65h
;         jnb     short loc_ECDDF      ; Jump if Below (CF=1)
; -----

```

```

seg000:000ECDDF
seg000:000ECDDF
seg000:000ECDDF
+ * seg000:000ECDDF 00 68 00
* seg000:000ECDE2 74 00
* seg000:000ECDE4 74 00
* seg000:000ECDE6 70 00
* seg000:000ECDE8 3A 00
* seg000:000ECDEA 2F
* seg000:000ECDEB 00 2F
* seg000:000ECDED 00 77 00
* seg000:000ECDF0 77 00
* seg000:000ECDF2 77 00
* seg000:000ECDF4 2E 00 72 00
* seg000:000ECDF8 61
* seg000:000ECDF9 00 64 00 70
* seg000:000ECDFD 00 64 00 66
* seg000:000ECE01 00 2E
* seg000:000ECE03 00 63 00
* seg000:000ECE06 6F
* seg000:000ECE07 00 6D 29
* seg000:000ECE0A 2F |
* seg000:000ECE0B 41
- * seg000:000ECE0C 75 74
* seg000:000ECE0E 68 6F 72 28 FE
* seg000:000ECE13 FF 00
* seg000:000ECE15 41
seg000:000ECE16
seg000:000ECE16
* seg000:000ECE16 00 63 00
* seg000:000ECE19 63 00
* seg000:000ECE1B 65 00 72 29

```

```

; -----
loc_ECDDF:
; CODE XREF: seg000:000ECDB4↑j
; Add
add [eax+0], ch
; Jump if Zero (ZF=1)
jz short $+2
; Jump if Zero (ZF=1)
jz short $+2
; Jump if Overflow (OF=1)
jo short $+2
; Compare Two Operands
cmp al, [eax]
; Decimal Adjust AL after Subtraction
das
; Add
add [edi], ch
; Add
add [edi+0], dh
; Jump if Above (CF=0 & ZF=0)
ja short $+2
; Jump if Above (CF=0 & ZF=0)
ja short $+2
; Add
add cs:[edx+0], dh
; Pop all General Registers
popa
; Add
add [eax+eax+70h], ah
; Add
add [eax+eax+66h], ah
; Add
add [esi], ch
; Add
add [ebx+0], ah
; Output Byte(s) to Port
outsd
; Add
add [ebp+29h], ch
; Decimal Adjust AL after Subtraction
das
; Increment by 1
inc ecx
; Jump if Not Zero (ZF=0)
jnz short near ptr loc_ECE7E+4
; Increment by 1
push 0FE28726Fh
; Increment by 1
inc dword ptr [eax]
; Increment by 1
inc ecx

loc_ECE16:
; CODE XREF: seg000:000ECDB2↑j
; Add
add [ebx+0], ah
; Adjust RPL Field of Selector
arpl [eax], ax
; Add
add gs:[edx+29h], dh

```

onlinedisassembler.com

```

.data:0000062d 37
.data:0000062e 383520303030
.data:00000634 3030
.data:00000636 206e0d
.data:00000639 0a30
.data:0000063b 3030
.data:0000063d 3030
.data:0000063f 3030
.data:00000641 393431
.data:00000644 2030
.data:00000646 3030
.data:00000648 3030
.data:0000064a 206e0d
.data:0000064d 0a30
.data:0000064f 3030
.data:00000651 3030
.data:00000653 3031
.data:00000655 3032
.data:00000657 37

```

```

- - -
(bad)
cmp BYTE PTR [rip+0x30303020],dh # 0x30303030
xor BYTE PTR [rax],dh
and BYTE PTR [rsi+0xd],ch
or dh,BYTE PTR [rax]
xor BYTE PTR [rax],dh
xor BYTE PTR [rax],dh
xor BYTE PTR [rax],dh
xor BYTE PTR [rax],dh
cmp DWORD PTR [rcx+rsi*1],esi
and BYTE PTR [rax],dh
xor BYTE PTR [rax],dh
xor BYTE PTR [rax],dh
xor BYTE PTR [rax],dh
and BYTE PTR [rsi+0xd],ch
or dh,BYTE PTR [rax]
xor BYTE PTR [rax],dh
xor BYTE PTR [rax],dh
xor BYTE PTR [rcx],dh
xor BYTE PTR [rdx],dh
(bad)
- - -

```

4.4 Debugging

N/A

4.5 Other

This file was sent as an attachment to an email on 28APR2016, of all things, pretending to be an email from SANS:

The link leads to buffet.honor.es/PcCleanU=p.exe which is defunct. There is a link to the actual SANS site further down in the email, and the malicious .PDF file is an attachment.

From: testa@rarejet.com
Subject: CS SEMINAR (JOB SECURITY)

To= p of the day,

SANS cyber security training is an essential element in the development of individuals and teams that are prepared to protect governmental, military, and commercial institutions from cyberattacks. To be part of this enlightenment program, simply download this invitation form fill and send back to me your (CS instructor). If you are not sure of the security of your computer, use our Pc Clean Up tool (sold \$320) for free (7days free) by following the link below...

PC CleanUp tool: CLEAN UP YOUR PC FROM MALWARE= S NOW

The SANS Institute is the most trusted, and by far the largest, provider of training, certification, and research to cybersecurity professionals globally.

- In 2015, SANS trained over 30,000 people, including professionals from 91% of the Fortune 100, nearly every US government agency

Virustotal detects virtually nothing:




SHA256: 13ece20c212f01cff1532c25d2635aeb04aef432e63a161ac6a0953f6929de9a

File name: Seminar_Cyber_Security_2016.pdf

Detection ratio: 1 / 55

Analysis date: 2016-05-13 20:38:29 UTC (1 minute ago)



Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
Sophos	Troj/PDFUri-CH	20160513
ALYac	✓	20160513
AVG	✓	20160513