Virus Bulletin :: VB2018 paper: Inside Formbook infostealer

Gabriela Nicolao

Deloitte, Argentina

Abstract

Formbook [1] is an infostealer that has been advertised for sale in public hacking forums since February 2016 by a user with the handle 'ng-Coder'. It is more advanced than a keylogger as it can retrieve authorization and login credentials from a web data form before the information reaches a secure server, bypassing HTTPS encryption. Formbook is effective even if the victims use a virtual keyboard, auto-fill, or if they copy and paste information to fill the form. The author of Formbook affirms that it is 'browser-logger software', a.k.a. form-grabbing software. Formbook offers a PHP panel, where the buyers can track their victims' information, including screenshots, keylogged data, and stolen credentials. Hosting and domain services are provided for low prices with a bin only available in the Pro version.

Formbook was used in a spam campaign in late 2017, targeting the aerospace, defence contractor and manufacturing sectors in South Korea and the USA. It includes hiding, persistence, anti-analysis, deletion and termination mechanisms along with several commands that the C&C (command-and-control) server can receive. The 'ng-Coder' user indicated that Formbook should not be used for malicious purposes and blocked sales until further notice after the spam campaigns became known. According to 'ng-Coder', Formbook should only be used to spy on family members or employees if the user has the explicit right to do so. However, this claim is dubious given the barely legitimate nature of the use of such software.

About formgrabbers

Formgrabbers intercept HTTP(S) data and use inline hooking to redirect the function to one within the formgrabber before transferring the execution flow back to the HTTP function to complete the request. This technique allows formgrabbers to capture a user's information before the user submits it over the Internet to a secure server. While keyloggers focus mainly on capturing the user's input, formgrabbers collect pasted information and/or information selected via a drop-down option, which makes them more efficient than keyloggers.

A formgrabber injects a DLL (Dynamic Link Library) into a browser and monitors for calls to the HttpSendRequest API within WININET.DLL in order to intercept the data before encryption and send all requests to its own code, prior to sending the data onwards. Andromeda (aka Gamarue), Tinba and Weyland-Yutani BOT are some malware families that use this technique.

Formbook background

Prior to advertising it for sale, a user with the handle 'ng-Coder' offered Formbook for free in public hacking forums so that other users could review it.

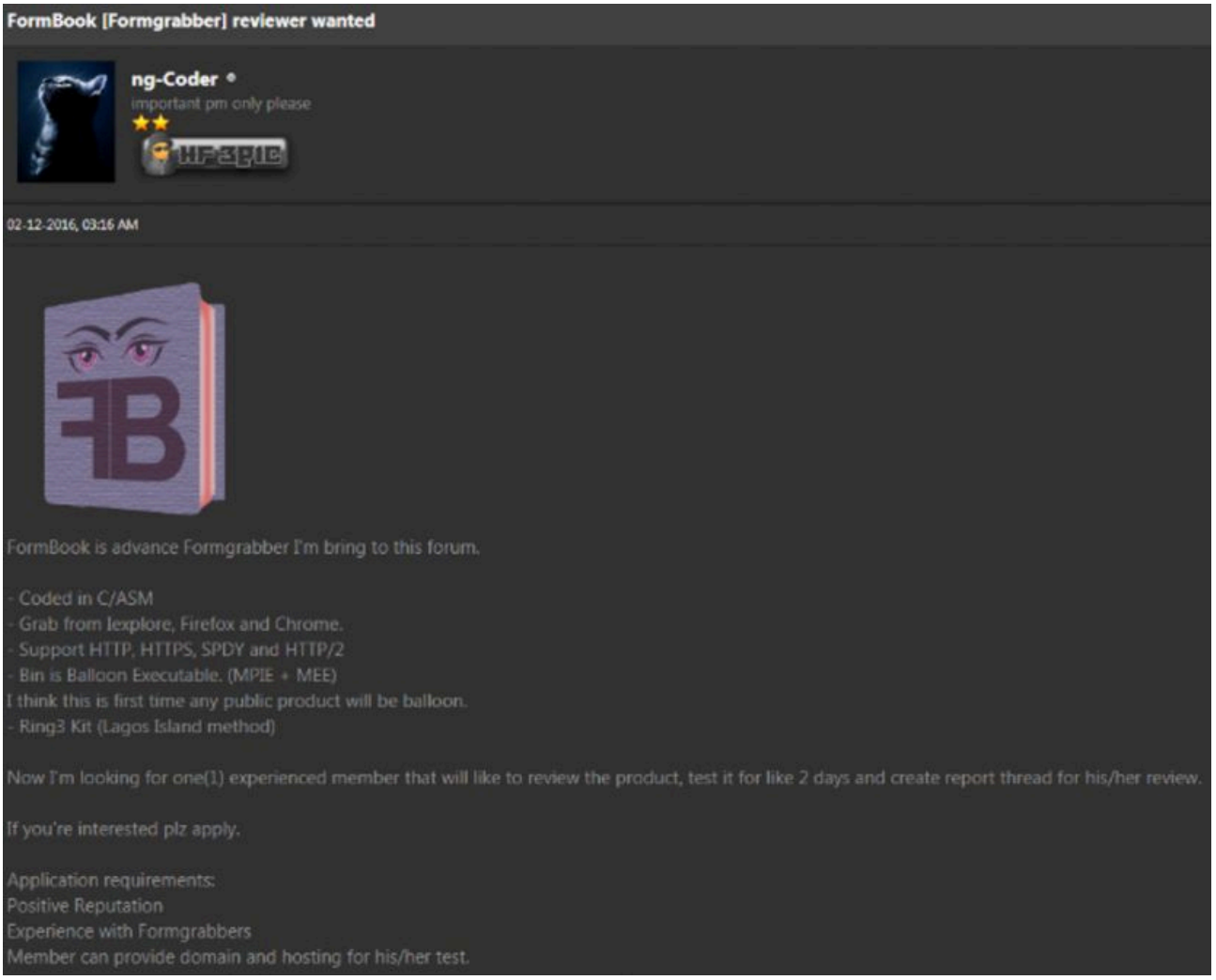


Figure 1: First mention of Formbook in a forum.

Soon after the free version was released, the user 'ng-Coder' advertised Formbook for sale at an initial price of 250 USD. However, the author reduced the price to 120 USD in early March 2016 after receiving several complaints about the price from forum members. The current pricing list and payment methods offered in the forum are displayed in Figure 2.

Figure 2: Pricing list and payment methods for Formbook.

Characteristics

According to the user 'ng-Coder', Formbook boasts the following features:

- Coded in ASM/C (x86_x64)
- Startup (hidden)
- Full PE-injection (no DLL/no drop/both x86 and x64)
- Ring3 kit
- Bin is Balloon Executable (MPIE + MEE)
- Doesn't use suspicious Windows APIs
- No blind hook, all hooks are thread safe including the x64, so crash is unlikely
- All communications with the panel are encrypted
- Install manager
- File browsing (FB Connect)
- Full Unicode support.

Control panel

Formbook works as a botnet, infecting victims that are shown in a web panel in order to manage the information that is retrieved from them. Figure 3 shows the web panel.

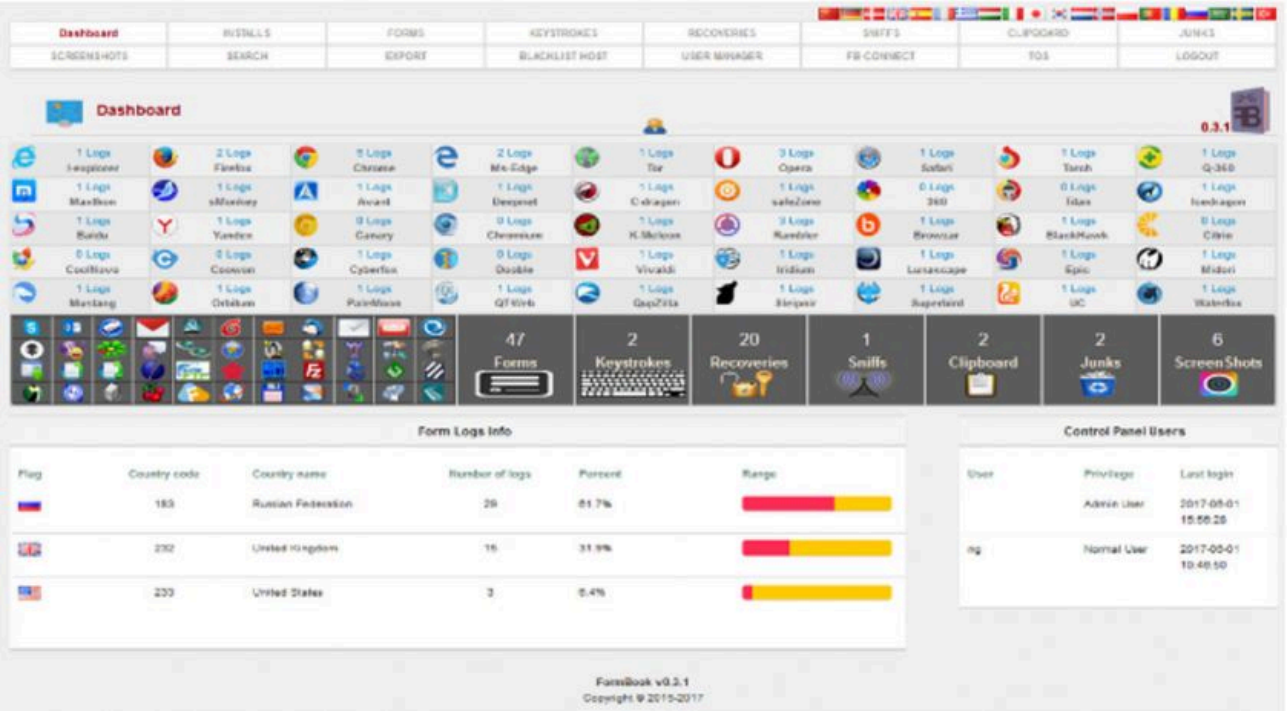


Figure 3: Formbook web panel.

Each bot can receive the following commands from the C&C server:

- Download and execute
- Update
- Uninstall
- Visit URL
- Clear cookies
- Restart system
- Shut down system
- Force upload keystroke
- Take screenshot
- FB Connect (file browsing)
- Download and execute from FB Connect
- Update bin from FB Connect

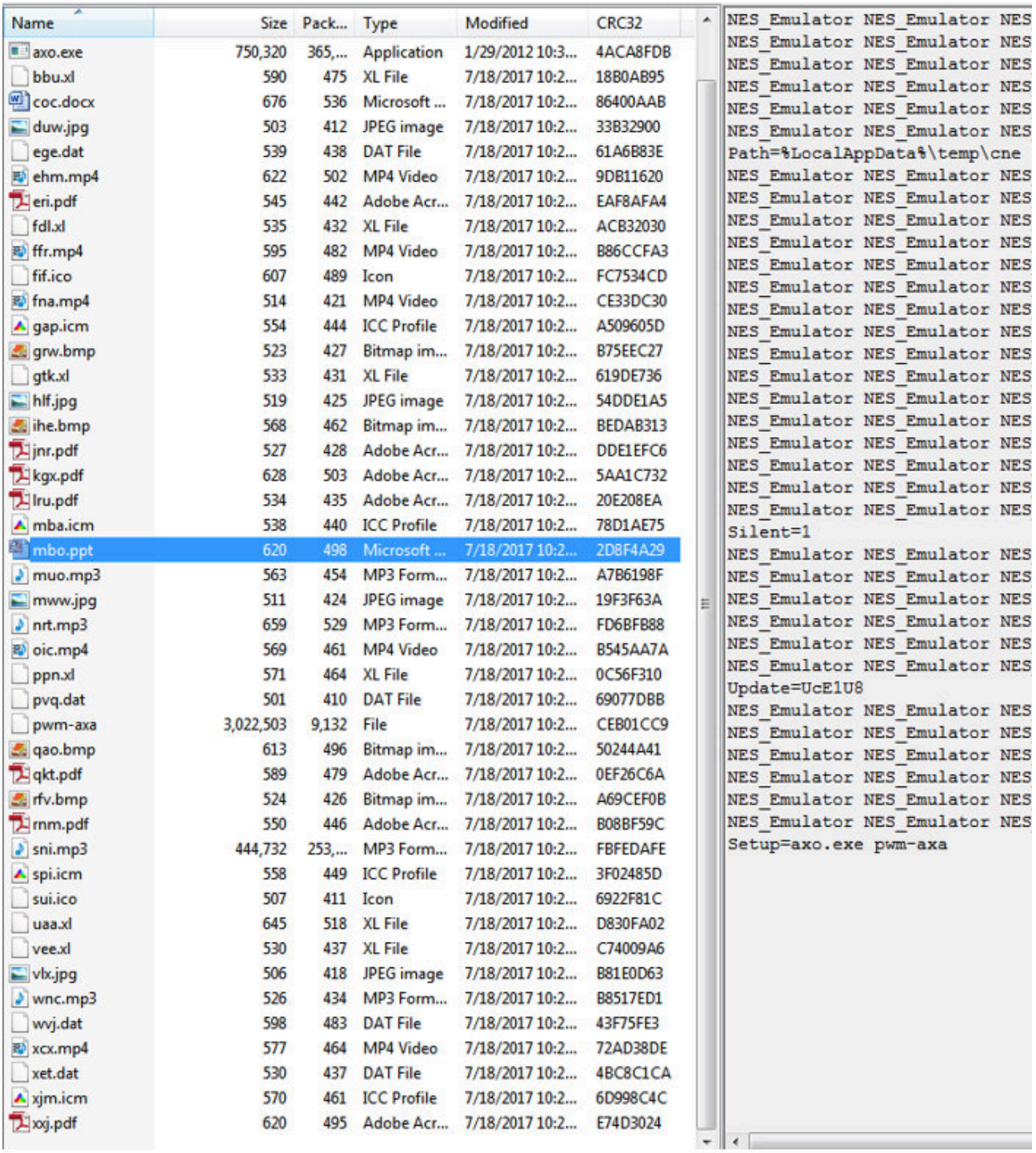
Campaigns

Formbook was used in spam campaigns targeting the aerospace, defence contractor and manufacturing sectors within the US and South Korea in 2017 [2]. It was distributed via PDFs with embedded links, DOC and XLS files with malicious macros, and compressed files containing the executable.

It was also observed in 2018, distributed via emails with DOCX files that contained a URL [3]. This URL downloaded an RTF file that exploits CVE-2017-8570 and drops an executable. This executable downloads the Formbook sample.

Analysis

The analysed sample is a RAR self-extracting archive (SFX) that contains several files, as shown in Figure 4.



Name	Size	Pack...	Type	Modified	CRC32
axo.exe	750,320	365,...	Application	1/29/2012 10:3...	4ACA8FDB
bbu.xl	590	475	XL File	7/18/2017 10:2...	18B0AB95
coc.docx	676	536	Microsoft ...	7/18/2017 10:2...	86400AAB
duw.jpg	503	412	JPEG image	7/18/2017 10:2...	33B32900
ege.dat	539	438	DAT File	7/18/2017 10:2...	61A6B83E
ehm.mp4	622	502	MP4 Video	7/18/2017 10:2...	9DB11620
eri.pdf	545	442	Adobe Acr...	7/18/2017 10:2...	EAF8AFA4
fdl.xl	535	432	XL File	7/18/2017 10:2...	ACB32030
ffr.mp4	595	482	MP4 Video	7/18/2017 10:2...	B86CCFA3
fif.ico	607	489	Icon	7/18/2017 10:2...	FC7534CD
fna.mp4	514	421	MP4 Video	7/18/2017 10:2...	CE33DC30
gap.icm	554	444	ICC Profile	7/18/2017 10:2...	A509605D
grw.bmp	523	427	Bitmap im...	7/18/2017 10:2...	B75EEC27
gtk.xl	533	431	XL File	7/18/2017 10:2...	619DE736
hlf.jpg	519	425	JPEG image	7/18/2017 10:2...	54DDE1A5
ihe.bmp	568	462	Bitmap im...	7/18/2017 10:2...	BEDAB313
jnr.pdf	527	428	Adobe Acr...	7/18/2017 10:2...	DDE1EFC6
kgx.pdf	628	503	Adobe Acr...	7/18/2017 10:2...	5AA1C732
lru.pdf	534	435	Adobe Acr...	7/18/2017 10:2...	20E208EA
mba.icm	538	440	ICC Profile	7/18/2017 10:2...	78D1AE75
mbo.ppt	620	498	Microsoft ...	7/18/2017 10:2...	2D8F4A29
muo.mp3	563	454	MP3 Form...	7/18/2017 10:2...	A7B6198F
mww.jpg	511	424	JPEG image	7/18/2017 10:2...	19F3F63A
nrt.mp3	659	529	MP3 Form...	7/18/2017 10:2...	FD6BFB88
oic.mp4	569	461	MP4 Video	7/18/2017 10:2...	B545AA7A
ppn.xl	571	464	XL File	7/18/2017 10:2...	0C56F310
pvq.dat	501	410	DAT File	7/18/2017 10:2...	69077DBB
pwm-axa	3,022,503	9,132	File	7/18/2017 10:2...	CEB01CC9
qao.bmp	613	496	Bitmap im...	7/18/2017 10:2...	50244A41
qkt.pdf	589	479	Adobe Acr...	7/18/2017 10:2...	0EF26C6A
rfv.bmp	524	426	Bitmap im...	7/18/2017 10:2...	A69CEF0B
rnm.pdf	550	446	Adobe Acr...	7/18/2017 10:2...	B08BF59C
sni.mp3	444,732	253,...	MP3 Form...	7/18/2017 10:2...	FBFEDAFE
spi.icm	558	449	ICC Profile	7/18/2017 10:2...	3F02485D
sui.ico	507	411	Icon	7/18/2017 10:2...	6922F81C
uaa.xl	645	518	XL File	7/18/2017 10:2...	D830FA02
vee.xl	530	437	XL File	7/18/2017 10:2...	C74009A6
vlx.jpg	506	418	JPEG image	7/18/2017 10:2...	B81E0D63
wnc.mp3	526	434	MP3 Form...	7/18/2017 10:2...	B8517ED1
wvj.dat	598	483	DAT File	7/18/2017 10:2...	43F75FE3
xcx.mp4	577	464	MP4 Video	7/18/2017 10:2...	72AD38DE
xet.dat	530	437	DAT File	7/18/2017 10:2...	4BC8C1CA
xjm.icm	570	461	ICC Profile	7/18/2017 10:2...	6D998C4C
xxj.pdf	620	495	Adobe Acr...	7/18/2017 10:2...	E74D3024

Figure 4: SFX file.

The description to the right of the files shows the following strings:

- Path=%LocalAppData%\temp\cne
- Silent=1
- Update=UcE1U8

- Setup=axo.exe pwm-axa

Files with a size below 1K contain a few strings that are probably used during decompression.

After executing the SFX file, Formbook extracts the files in %LocalAppData%\temp\cne using CreateDirectoryW. It then deletes the SFX file. Figure 5 shows the file extraction.

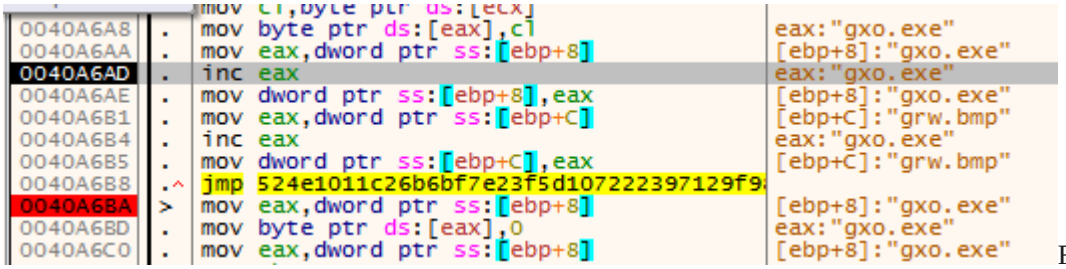


Figure 5: File extraction.

The axo.exe file is an AutoIt script that is executed with the pwm-axa file as a parameter. Figure 6 shows the properties of the axo.exe file.

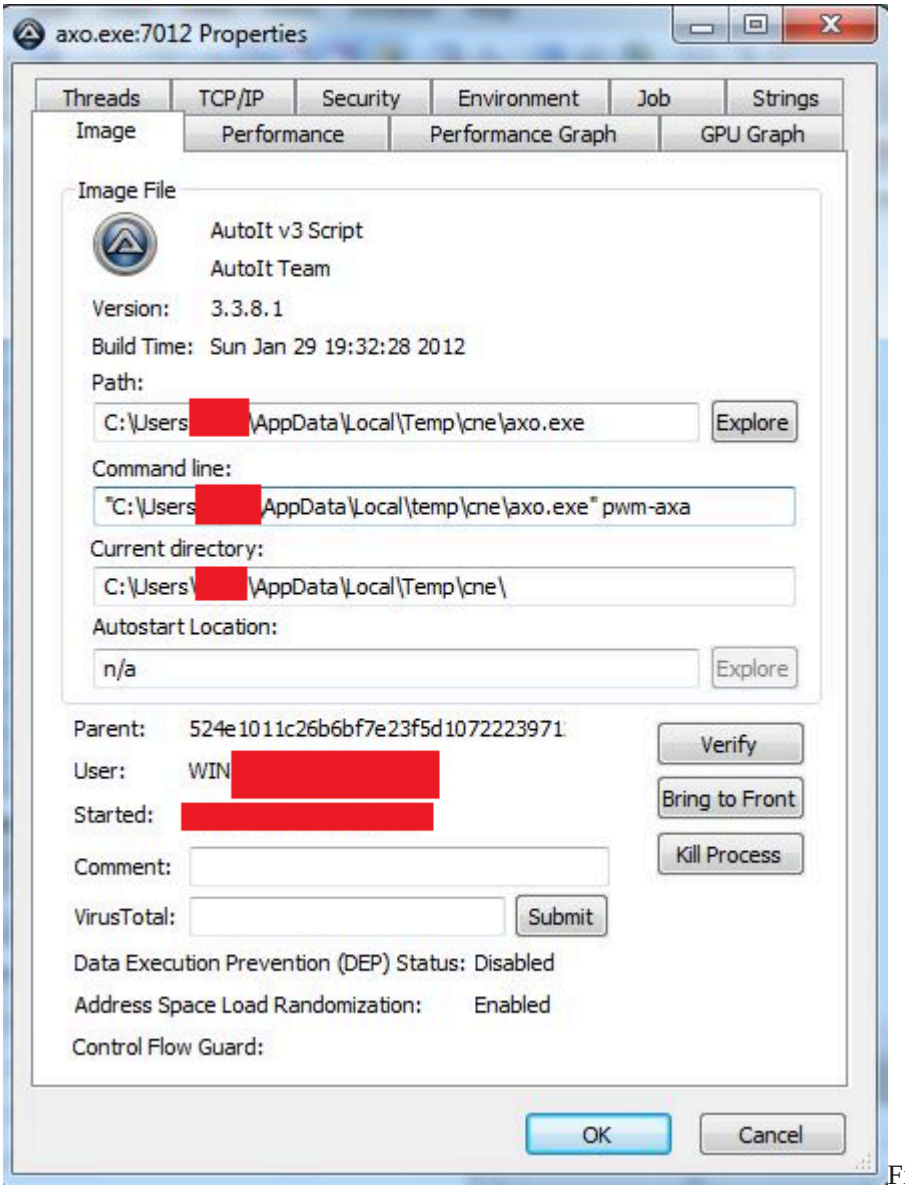


Figure 6: Properties of the axo.exe AutoIt executable.

The script decrypts Formbook and loads it in memory. In order to do this, 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 44 functions with obfuscated names. The sni.mp3 file includes interesting strings that were used during the execution, as shown in Figure 7.

```
[Setting]
sd_Keys=3134453439343435353432353043424237364138373838373642464243453845333742444531334133384244384543333239383 5
Keys=fiu
Dir=cne
Key=WindowsUpdate
AuEx=pwm-axa
ExEc=axo.exe
StartUps=nug-BZeoal7C68j1BF884Xr52nF6mvI0538823d9uwkELR34Us
RP=fgv.hmf
sK=858
sN=sli.hxp
eof=hmf
inc=meq.cxe
```

Figure 7: Interesting strings found in the sni.mp3 file.

The script contains the following features:

1. Hiding mechanism

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

2. 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
Else
RegWrite("HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", $WindowsUpdate, "REG_SZ"
RegWrite("HKCU64\Software\Microsoft\Windows\CurrentVersion\Run", $WindowsUpdate, "REG_SZ", $cne_Fold
EndIf
Sleep(1000)
Sleep(1000)
EndFunc
```

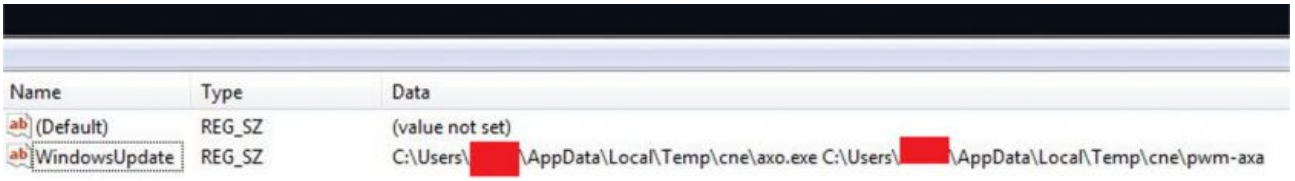


Figure 8: Persistence mechanism.

3. Protection disabling and anti-analysis

The script tries to modify the following registry keys:

- RegWrite("HKCU64\Software\Microsoft\Windows\CurrentVersion\Policies\System", "DisableTaskMgr", "REG_DWORD", "1")
- RegDelete("HKLM64\Software\Microsoft\Windows NT\CurrentVersion\SPP\Clients")
- RegWrite("HKLM64\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System", "EnableLUA", "REG_DWORD", "0")

And it:

- Disables Task Manager
- Turns off the system protection
- Disables UAC (User Account Controls)

Formbook will terminate if it finds *VMware* or *VirtualBox* processes running in the victim's system and if the 'D' drive has space of less than 1MB:

- 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

4. 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.

5. Formbook deletion and termination

Formbook will look for the svshost.exe process and terminate if it finds more than two svshost.exe processes running, as shown in Figure 9.

```
If UBound(ProcessList("svshost.exe")) > 2 Then Exit ; COMMENT: ProcessList Returns array of process names and PIDs. UBound returns size of array.
ProcessSetPriority("svshost.exe", 5) ; COMMENT: 5=REALTIME
```

Figure 9: Termination.

Conclusion

Despite Formbook infostealer having been around for a couple of years now, it only came to public attention after it was extensively used in spam campaigns in late 2017. The fact that Formbook wasn't noticed before is probably because its developers didn't release the builder to the public, so it was easy for them to track its activities and turn it off if they found that it was being used for purposes for which it was not intended 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 the Agent Tesla remote access trojan (RAT), the author of Formbook initially offered a beta version of the product free of charge in order 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 'ng-Coder', Formbook should only be used to spy on family members or employees if the user has the explicit right to do so. However, this claim itself is dubious given the barely legitimate nature of the use of such software.

IOCs

The SHA256 hash of the SFX file that was analysed is: 2f74f8518bd14a882a870f3794a76dba381b59c1e40247a2483468959b572d82.

References

[1] Schwarz, D. The Formidable FormBook Form Grabber. Arbor Networks, 20 September 2017. https://www.arbornetworks.com/blog/asert/formidable-formbook-form-grabber/.

[2] Villeneuve, N.; Eitzman, R.; Nemes S.; Dean, T. Significant FormBook Distribution Campaigns Impacting the U.S. and South Korea. FireEye, 5 October 2017. https://www.fireeye.com/blog/threat-research/2017/10/formbook-malware-distribution-campaigns.html.

[3] Urgent server alert malspam delivers formbook trojan via CVE-2017-8570 word doc. My Online Security, 16 February 2018. https://myonlinesecurity.co.uk/urgent-server-alert-malspam-delivers-formbook-trojan-via-cve-2017-8570-word-doc.
