

# VB2018 paper: Inside Formbook infostealer

---

 [virusbulletin.com/virusbulletin/2019/01/vb2018-paper-inside-formbook-infostealer/](https://virusbulletin.com/virusbulletin/2019/01/vb2018-paper-inside-formbook-infostealer/)

**Gabriela Nicolao**

---

Deloitte, Argentina

*Copyright © 2018 Virus Bulletin*

---

Table of contents

[Abstract](#)

[About formgrabbers](#)

[Formbook background](#)

[Characteristics](#)

[Control panel](#)

[Campaigns](#)

[Analysis](#)

[1. Hiding mechanism](#)

[2. Persistence mechanism](#)

[3. Protection disabling and anti-analysis](#)

[4. Check default browser](#)

[5. Formbook deletion and termination](#)

[Conclusion](#)

[IOCs](#)

[References](#)

## **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.

FormBook [Formgrabber] reviewer wanted



ng-Coder \*

important pm only please



02-12-2016, 03:16 AM



FormBook is advance Formgrabber I'm bring to this forum.

- Coded in C/ASM
- Grab from Iexplore, Firefox and Chrome.
- Support HTTP, HTTPS, SPDY and HTTP/2
- Bin is Balloon Executable. (MPIE + MEE)

I think this is first time any public product will be balloon.

- Ring3 Kit (Lagos Island method)

Now I'm looking for one(1) experienced member that will like to review the product, test it for like 2 days and create report thread for his/her review.

If you're interested plz apply.

Application requirements:

Positive Reputation

Experience with Formgrabbers

Member can provide domain and hosting for his/her test.

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.

PRICING	
\$29 / Week <i>Full Package/Hosted</i>	\$59 / Month <i>Full Package/Hosted</i>
\$99 / 3 Month <i>Full Package/Hosted</i>	\$299 - Pro <i>Bin for your domain</i>
PAYMENT METHOD	
Bitcoin -&- PM Perfect Money	

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.

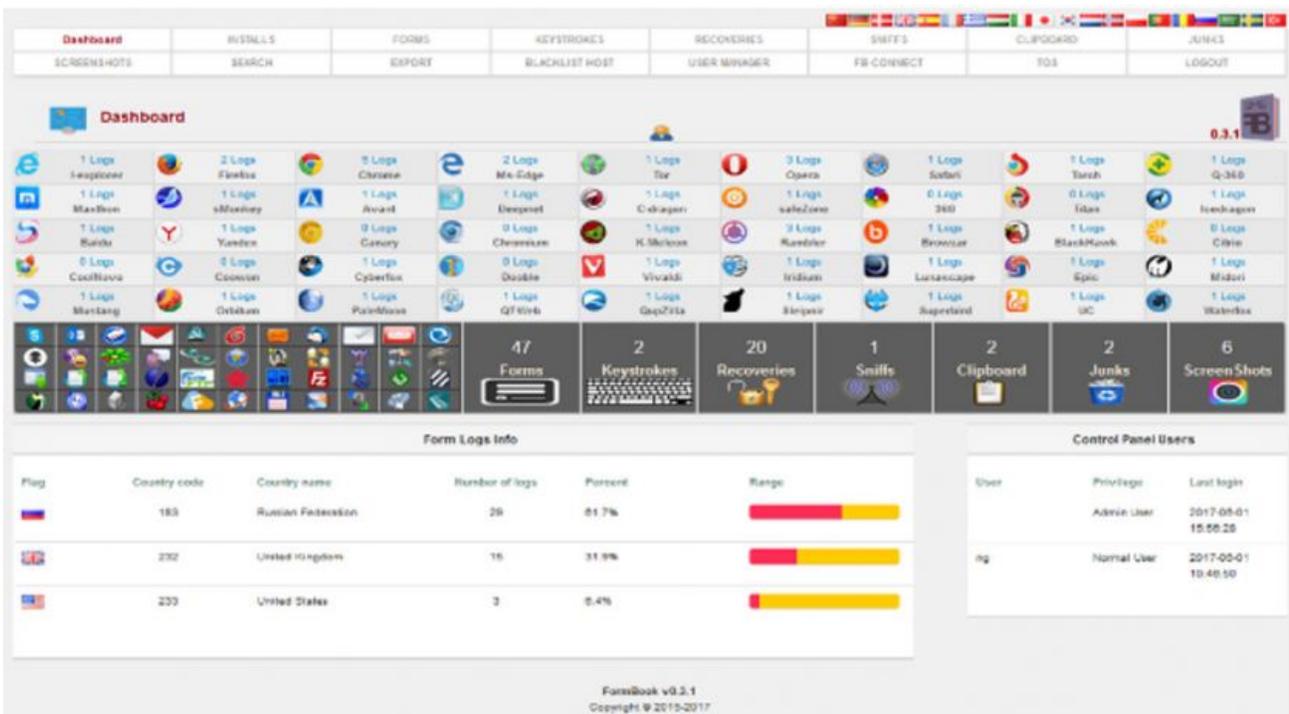


Figure 3: Formbook web panel.

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.



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.

0040A6A8	. mov	cl,byte ptr ds:[eax]	eax: "gxo.exe"	
0040A6AA	. mov	byte ptr ds:[eax],cl	[ebp+8]: "gxo.exe"	
0040A6AD	. inc	eax	eax: "gxo.exe"	
0040A6AE	. mov	dword ptr ss:[ebp+8],eax	[ebp+8]: "gxo.exe"	
0040A6B1	. mov	eax,dword ptr ss:[ebp+C]	[ebp+C]: "grw.bmp"	
0040A6B4	. inc	eax	eax: "gxo.exe"	
0040A6B5	. mov	dword ptr ss:[ebp+C],eax	[ebp+C]: "grw.bmp"	
0040A6B8	. ^	jmp 524e1011c26b6bf7e23f5d107222397129f9		
0040A6BA	>	mov	eax,dword ptr ss:[ebp+8]	[ebp+8]: "gxo.exe"
0040A6BD	. mov	byte ptr ds:[eax],0	eax: "gxo.exe"	
0040A6C0	. mov	eax,dword ptr ss:[ebp+8]	[ebp+8]: "gxo.exe"	

Figure 5: File

extraction.

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

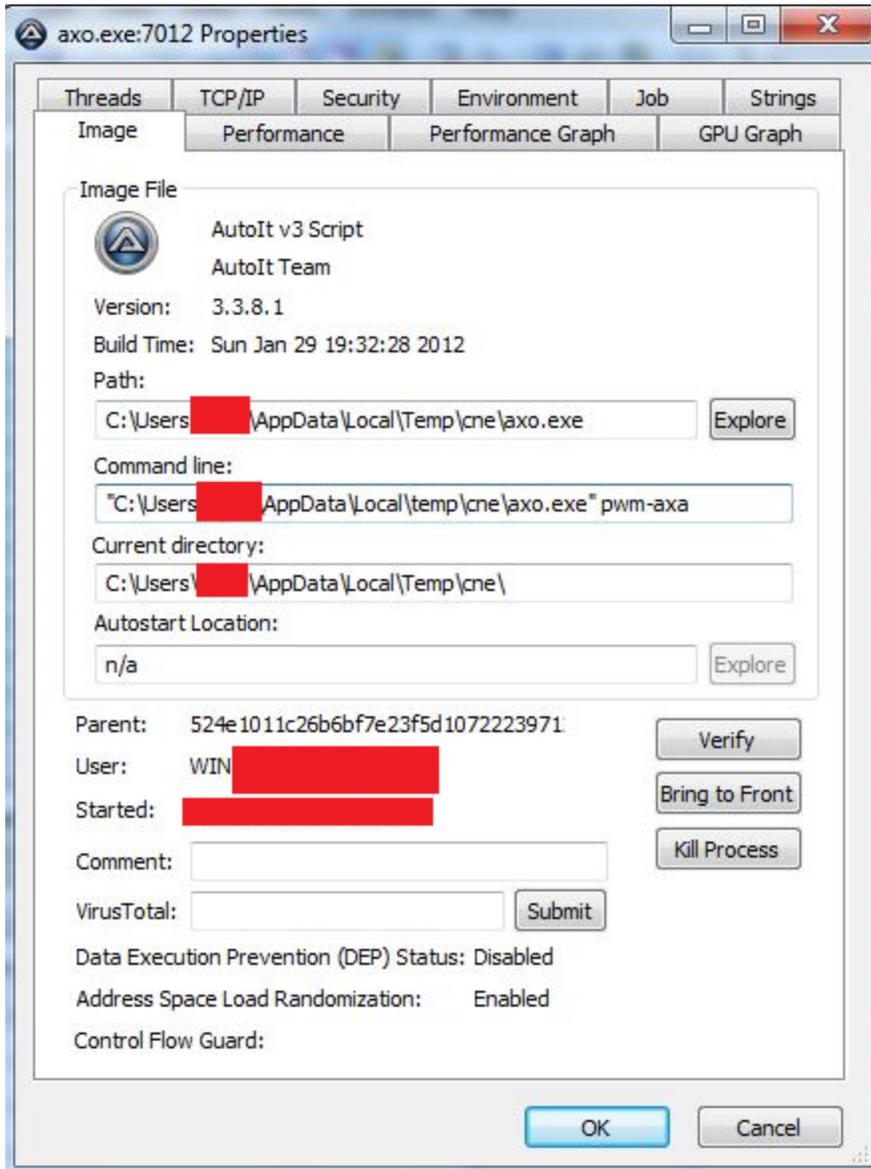


Figure 6: Properties of the

axo.exe Autolt 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=31344534393434353534323530434242373641383738383736424642434538453337424445313341333842443845433332393835
Keys=fju
Dir=cne
Key=WindowsUpdate
AuEx=pwm-axa
ExEc=axo.exe
StartUps=nuq-BZeoa17C68j1BF884Xr52nF6mviO538823d9uwkELR34Us
RP=fgy.hmf
sK=858
sN=gl1.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

---

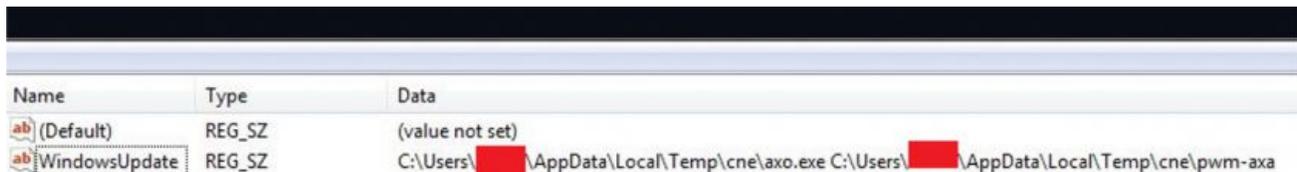
The script changes the cne folder attributes to hide its content by executing the command `FileSetAttrib($cne_Folder_Path, "+H")`.

## 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", $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))
RegWrite("HKCU64\Software\Microsoft\Windows\CurrentVersion\Run", $WindowsUpdate,
"REG_SZ", $cne_Folder_Path & "\" & $axo.exe & " " &
FileGetShortName($cne_Folder_Path & "\" & $pwm-axa))
EndIf
Sleep(1000)
Sleep(1000)
EndFunc
```



The screenshot shows the Windows Registry Editor with the following table of registry values:

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

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>.



[Download PDF](#)

## Latest articles:

---

### **Cryptojacking on the fly: TeamTNT using NVIDIA drivers to mine cryptocurrency**

TeamTNT is known for attacking insecure and vulnerable Kubernetes deployments in order to infiltrate organizations' dedicated environments and transform them into attack launchpads. In this article Aditya Sood presents a new module introduced by...

### **Collector-stealer: a Russian origin credential and information extractor**

Collector-stealer, a piece of malware of Russian origin, is heavily used on the Internet to exfiltrate sensitive data from end-user systems and store it in its C&C panels. In this article, researchers Aditya K Sood and Rohit Chaturvedi present a 360...

### **Fighting Fire with Fire**

In 1989, Joe Wells encountered his first virus: Jerusalem. He disassembled the virus, and from that moment onward, was intrigued by the properties of these small pieces of self-replicating code. Joe Wells was an expert on computer viruses, was partly...

### **Run your malicious VBA macros anywhere!**

---

Kurt Natvig wanted to understand whether it's possible to recompile VBA macros to another language, which could then easily be 'run' on any gateway, thus revealing a sample's true nature in a safe manner. In this article he explains how he recompiled...

### **Dissecting the design and vulnerabilities in AZORult C&C panels**

---

Aditya K Sood looks at the command-and-control (C&C) design of the AZORult malware, discussing his team's findings related to the C&C design and some security issues they identified during the research.

#### Bulletin Archive

We have placed cookies on your device in order to improve the functionality of this site, as outlined in our [cookies policy](#). However, you may delete and block all cookies from this site and your use of the site will be unaffected. By continuing to browse this site, you are agreeing to Virus Bulletin's use of data as outlined in our [privacy policy](#).