

Forum:[Hack Forums](#)

Thread: [FormBook Formgrabber](#)

ng-Coder - February 13, 2016, 2:16 am

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.

The solely purpose of this tool is for you to be able to spy on your smart kids that knows their way around keyloggers, your smart spouse that superseded all monitoring tools you installed on his/her PC, your smart employee or a computer which you have authority to spy on.

All that been said it is important to note that FormBook should only be use on computer which you own and/or have right/permission to spy. Also check your local laws to see If it's illegally before purchasing FormBook.

In no circumstance shall the Developer of FormBook be held liable for your illegal use of the software, or any damages caused by your use of the software. Please use it responsibly.

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

Skype 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)

Q&A

- Is the bin FUD?

No bin isn't FUD, but that's not suppose to be problem because anything called crypter including .NET ones will crypt the bin just fine and you can also get free fud crypter here:

<https://hackforums.net/showthread.php?tid=5196315>

- Does FormBook come with hosting and domain?

No, FormBook comes with neither of those, you have to provide your domain to have your bin generated.

- Can I get a rebuild if my domain gets banned?

If I'm satisfy with your proof that the domain is really banned under 3 months of purchase you can get a rebuild and if I'm not satisfy you may not have a rebuild.

- What if I lost my primary contact (your email or any account used to register with us).

That means you lost your FormBook customer account too sorry we won't help you.

Note: For max optimization and speed the HTTP/2 header are not decompressed but you can in most of the time figure out the host from the content.

Sample: <https://i.imgur.com/btUksaS.jpg>

.

Benoit balls - February 13, 2016, 2:29 am

Looks pretty nice! Good luck with sales!

N3oNight - February 13, 2016, 3:14 am

looks nice, but you should ask staff in case this is not allowed, you will also loose your account.

ng-Coder - February 13, 2016, 3:30 am

(Feb 13, 2016 03:29 AM)?Leonardo Da Vinci Wrote: [\[CITE\]](#) Looks pretty nice! Good luck with sales! Thank you.

(Feb 13, 2016 04:14 AM)N3oNight Wrote: [\[CITE\]](#) looks nice, but you should ask staff in case this is not allowed, you will also loose your account.

I did read this <https://hackforums.net/misc.php?action=help&hid=21> or I'm missing something?

Cecilia - February 29, 2016, 4:32 am

(Feb 13, 2016 04:14 AM)N3oNight Wrote: [\[CITE\]](#) looks nice, but you should ask staff in case this is not allowed, you will also loose your account.

Formgrabbers have always been allowed. BB had issues because it 'possibly featured web injection and did not block financial fraud'. As long as OP doesn't start fucking with financial things its probably ok.

LordCoder - February 29, 2016, 5:20 am

I believe you should have a strong ToS to sell this, you might have some problems if you don't. Just saying.

Apart from that, glws, looking amazing.

Thomaz000 - February 29, 2016, 5:22 am

This - \$250

And This - " What if I lost my primary contact (your email or any account used to register with us). That means you lost your FormBook customer account too sorry we won't help you."

:(:

Anyway looks nice. GLWS!

cracker007 - February 29, 2016, 5:38 am

Good luck with your sales, vouch for you friend,

ng-Coder - February 29, 2016, 6:57 am

(Feb 29, 2016 05:32 AM)LaPanthere Wrote: [\[CITE\]](#) Formgrabbers have always been allowed. BB had issues because it 'possibly featured web injection and did not block financial fraud'. As long as OP doesn't start fucking with financial things its probably ok.Thx, Yes no extension, plugin or anything like web inject so u have only browser logger..

(Feb 29, 2016 06:20 AM)LordCoder Wrote: [\[CITE\]](#) I believe you should have a strong ToS to sell this, you might have some problems if you don't. Just saying.

Apart from that, glws, looking amazing.Thx will look into adding more Tos note.

(Feb 29, 2016 06:22 AM)thomaz000 Wrote: [\[CITE\]](#) This - \$250

And This - " What if I lost my primary contact (your email or any account used to register with us). That means you lost your FormBook customer account too sorry we won't help you."

:(:

Anyway looks nice. GLWS!Price will go down badly soon when I have time.

Yes if you lost primary contact creating another account for you is long so we decide not do it.

(Feb 29, 2016 06:38 AM)cracker007 Wrote: [\[CITE\]](#) Good luck with your sales, vouch for you friend, Thanks pal. ?

Slavoj Žižek - February 29, 2016, 7:50 am

looks really good, glws - you might need some really strict ToS to cover your ass...

fikky - March 1, 2016, 4:30 pm

might consider buying this when price is reduced

limb3r - March 2, 2016, 2:30 pm

Same as above, and will check back time to time. Bookmarking for keeps though.

?Syria - March 2, 2016, 3:05 pm

I belive form grabbers are against the rules

Cecilia - March 2, 2016, 3:33 pm

(Mar 2, 2016 04:05 PM)?Syria Wrote: [\[CITE\]](#) I belive form grabbers are against the rules
There is nothing in the rules against them, the one that could cover it would be financial crimeware, but that is only if the intended goal is to gain information on the clients bank or card details.

This is not intended for financial fraud.

Cecilia - March 4, 2016, 4:11 pm

Any date on the price drop?

ng-Coder - March 4, 2016, 10:27 pm

(Mar 2, 2016 04:05 PM)?Syria Wrote: [\[CITE\]](#) I belive form grabbers are against the rules
I believe this is no difference to keylogger excluding that it log only browsers and not system-wide.

(Mar 2, 2016 04:33 PM)LaPanthere Wrote: [\[CITE\]](#) There is nothing in the rules against them, the one that could cover it would be financial crimeware, but that is only if the intended goal is to gain information on the clients bank or card details.

This is not intended for financial fraud.
Thanks pal I fixed the TOS

(Mar 4, 2016 05:11 PM)LaPanthere Wrote: [\[CITE\]](#) Any date on the price drop?
The price is updated now :)

limb3r - March 7, 2016, 8:00 am

(Mar 4, 2016 11:27 PM)ng-Coder Wrote: [\[CITE\]](#) I believe this is no difference to keylogger excluding that it log only browsers and not system-wide.

Thanks pal I fixed the TOS

The price is updated now :)
Price going down by half is good but still, shouldn't this be cheaper than stealers? Youssaid it yourself, it's not system-wide. Many stealers can hide process from smart employees too.
I like the small stub size and I assume the bin is built as .exe?

Also what happens when chrome updates?

I'm really interested in this thank you.

ng-Coder - March 7, 2016, 9:13 am

(Mar 7, 2016 09:00 AM)limb3r Wrote: [\[CITE\]](#) Price going down by half is good but still, shouldn't this be cheaper than stealers? Youssaid it yourself, it's not system-wide. Many stealers can hide process from smart employees too.
I like the small stub size and I assume the bin is built as .exe?

Also what happens when chrome updates?

I'm really interested in this thank you.

You're getting it wrong, this is totally different to stealer, stealers don't monitor anything and it only get/show you saved infos(credentials that the target app(s) already saved on the system) will you tell your browser to save your Ashley Madison's password if it ask? ?, stealers are lame than average keylogger in my opinion.

Thanks for your interest, I feel the price is ok at this level.

Yes bin is .exe and it's balloon executable so it's more easier to deal with than average exe.

As for Chrome Update, customers are already receiving optimisation updates even when chrome hasn't change anything, so when they do then customers will also receive update..

I'm surprised how people seems to be scared of Chrome's update like it's WW III ?

.

limb3r - March 9, 2016, 5:15 am

Haha. Touchê

Do you have a video demo or something showing the UI? Seeing that you haven't given any vouch copies out,

As you can tell, formgrabbers aren't my thing but I'm looking to give this a go.

ng-Coder - March 9, 2016, 5:26 am

(Mar 9, 2016 06:15 AM)limb3r Wrote: [\[CITE\]](#) Haha. Touchê

Do you have a video demo or something showing the UI? Seeing that you haven't given any vouch copies out,

As you can tell, formgrabbers aren't my thing but I'm looking to give this a go.

The other reviewer decided to pay and continue using the product without creating report thread ? I gave another vouch copy and he'll do the report maybe today, I don't want testimony on sales thread if it's not about your spouse or kids ?

customers also having this for free <https://hackforums.net/showthread.php?tid=5196315>

limb3r - March 9, 2016, 11:30 pm

Ok. It looks really good. Is the license lifetime for this price?

ng-Coder - March 10, 2016, 12:14 am

(Mar 10, 2016 12:30 AM)limb3r Wrote: [\[CITE\]](#) Ok. It looks really good. Is the license lifetime for this price?

Yes, you will continue receiving update.

Note: you can have update build to new host only if your host have issue under 3 months of purchase, after 3 months you can only have update build for your initial host.

Russ. - March 10, 2016, 9:15 am

Big vouch for NG, great coder. If you want high quality products contact this guy.

ng-Coder - March 10, 2016, 10:28 am

(Mar 10, 2016 10:15 AM)Watson. Wrote: [\[CITE\]](#) Big vouch for NG, great coder. If you want high

quality products contact this guy.
Thanks for the vouch pal, ?

limb3r - March 11, 2016, 1:24 am

This is coded in .net right?

ng-Coder - March 11, 2016, 1:48 am

(Mar 11, 2016 02:24 AM)limb3r Wrote: [\[CITE\]](#) This is coded in .net right?
Lol, are you serious? Why don't you maybe read the thread.

Cecilia - March 12, 2016, 5:33 am

Great product, needs more attention.

ng-Coder - March 14, 2016, 10:35 am

(Mar 12, 2016 06:33 AM)LaPanthere Wrote: [\[CITE\]](#) Great product, needs more attention.
Thank you pal ?

Chan Wong - March 14, 2016, 3:48 pm

Do I need bulletproof server/domain for this?

Cecilia - March 14, 2016, 3:49 pm

(Mar 14, 2016 03:48 PM)Chan Wong Wrote: [\[CITE\]](#) Do I need bulletproof server/domain for this?
Nah just host it on your home server in the usa.
I'm sure it'll be fine
/sarcasm

ng-Coder - March 14, 2016, 11:51 pm

(Mar 14, 2016 03:48 PM)Chan Wong Wrote: [\[CITE\]](#) Do I need bulletproof server/domain for this?
No you don't need bulletproof server/domain for this.

sissy-b - March 17, 2016, 11:58 pm

Always outstanding.. Glws bro.

ng-Coder - March 22, 2016, 3:09 am

(Mar 17, 2016 11:58 PM)keztex Wrote: [\[CITE\]](#) Always outstanding.. Glws bro.
Thank you.

t0mato - March 22, 2016, 9:15 am

Do you need to specify a domain name list to grab forms from , or It will work on every domain being accessed from the machine?!

Bos™ - March 22, 2016, 9:16 am

(Mar 22, 2016 09:15 AM)i-Hmx Wrote: [\[CITE\]](#) Do you need to specify a domain name list to grab forms from , or It will work on every domain being accessed from the machine?!If i remember correctly, op said to me its universal. Although you have a blacklist option to prevent unwanted logs from comming in.

ng-Coder - March 22, 2016, 9:22 am

(Mar 22, 2016 09:15 AM)i-Hmx Wrote: [\[CITE\]](#) Do you need to specify a domain name list to grab forms from , or It will work on every domain being accessed from the machine?!
It will by default grab from every domain but you have option to blacklist domain(s) from control panel, in that case it won't save logs from that blacklisted domain(s) anymore.

Russ. - March 30, 2016, 2:42 pm

\$120 is a great price for this. ng-coder is an amazing programmer. Big Vouch for him!

inc rcx - March 30, 2016, 5:34 pm

Ring3 kit (Lagos Island method)

Doesn't exist, stop trying to use unknown terminology to boost sales.

- Startup (Hidden)

Not from me

- Full PE-Injection (No dll/ No drop)

I hope it's PIC because PE Injection for a formgrabber is overkill.

- Bin is Balloon Executable (MPIE + MEE)

What the fuck is a balloon executable? Why are you making up terms again?

- Doesn't use suspicious windows API (96% of API used are from Lagos)

So wait, this so called 'lagos rootkit' has it's own APIs that windows isn't suspicious against? and you somehow mysteriously calculated that to be 96%?

- No blind hook, all hooks are thread safe so crash is unlikely

'unlikely' ? Why not impossible? Are you initializing mutex's correctly? Before inserting into a list, before reading accessing memory?

Doesn't seem like you're confident with your code.

Internet Explorer - HTTP, HTTPS, SPDY & HTTP/2

Firefox - HTTP, HTTPS, SPDY & HTTP/2

Chrome - HTTPS, SPDY & HTTP/2

Are you manually decompressing SPDY packets, and leaving http/2 header ? or are you Hooking SPDY related routines before compression is called?

ng-Coder - March 30, 2016, 10:49 pm

(Mar 30, 2016 02:42 PM)Russ. Wrote: [\[CITE\]](#) \$120 is a great price for this. ng-coder is an amazing programmer. Big Vouch for him!

Thanks Pal

NoTail - March 31, 2016, 7:47 am

(Mar 30, 2016 05:34 PM)inc rcx Wrote: [\[CITE\]](#) Ring3 kit (Lagos Island method)

Doesn't exist, stop trying to use unknown terminology to boost sales.

- Startup (Hidden)

Not from me

- Full PE-Injection (No dll/ No drop)

I hope it's PIC because PE Injection for a formgrabber is overkill.

- Bin is Balloon Executable (MPIE + MEE)

What the fuck is a balloon executable? Why are you making up terms again?

- Doesn't use suspicious windows API (96% of API used are from Lagos)

So wait, this so called 'lagos rootkit' has it's own APIs that windows isn't suspicious against? and you somehow mysteriously calculated that to be 96%?

- No blind hook, all hooks are thread safe so crash is unlikely

'unlikely' ? Why not impossible? Are you initializing mutex's correctly? Before inserting into a list, before reading accessing memory?

Doesn't seem like you're confident with your code.

Internet Explorer - HTTP, HTTPS, SPDY & HTTP/2

Firefox - HTTP, HTTPS, SPDY & HTTP/2

Chrome - HTTPS, SPDY & HTTP/2

Are you manually decompressing SPDY packets, and leaving http/2 header ? or are you Hooking SPDY related routines before compression is called?

lol , this ?

drewkasp - March 31, 2016, 3:21 pm

(Mar 30, 2016 05:34 PM)inc rcx Wrote: [CITE](#) Ring3 kit (Lagos Island method)

Doesn't exist, stop trying to use unknown terminology to boost sales.

- Startup (Hidden)

Not from me

- Full PE-Injection (No dll/ No drop)

I hope it's PIC because PE Injection for a formgrabber is overkill.

- Bin is Balloon Executable (MPIE + MEE)

What the fuck is a balloon executable? Why are you making up terms again?

- Doesn't use suspicious windows API (96% of API used are from Lagos)

So wait, this so called 'lagos rootkit' has it's own APIs that windows isn't suspicious against? and you somehow mysteriously calculated that to be 96%?

- No blind hook, all hooks are thread safe so crash is unlikely

'unlikely' ? Why not impossible? Are you initializing mutex's correctly? Before inserting into a list,

before reading accessing memory?

Doesn't seem like you're confident with your code.

Internet Explorer - HTTP, HTTPS, SPDY & HTTP/2

Firefox - HTTP, HTTPS, SPDY & HTTP/2

Chrome - HTTPS, SPDY & HTTP/2

Are you manually decompressing SPDY packets, and leaving http/2 header ? or are you Hooking SPDY related routines before compression is called?

Lol...Now that's when his skills needs to be defended...interested but the price is on the high side to try, more vouches will be appreciated from users who have already bought this.

HIGH PAID FELLA - March 31, 2016, 3:22 pm

What do you do to disable SPDY in FF?

inc rcx - March 31, 2016, 4:45 pm

(Mar 31, 2016 03:22 PM)astr Wrote: [\[CITE\]](#) What do you do to disable SPDY in FF?

Disabling SPDY through user preferences isn't the best idea, because it slows down the connection since the point of spdy is to compress packets for faster communication.

Still works though.

ng-Coder - March 31, 2016, 10:20 pm

(Mar 31, 2016 03:21 PM)drewkasp Wrote: [\[CITE\]](#) Lol...Now that's when his skills needs to be defended...interested but the price is on the high side to try, more vouches will be appreciated from users who have already bought this.

No skill need to be defended, ask any question you have and I will answer. As for more customer vouches that's not necessary.

(Mar 31, 2016 03:22 PM)astr Wrote: [\[CITE\]](#) What do you do to disable SPDY in FF?

No, SPDY isn't disabled, FormBook just copy and decompress the data.

inc rcx - April 1, 2016, 2:23 am

Please don't tell me you're one of those people that decompresses GZIP with wininet.

hackgodx - April 1, 2016, 2:34 am

(Feb 29, 2016 05:32 AM)LaPanthere Wrote: [\[CITE\]](#) Formgrabbers have always been allowed. BB had issues because it 'possibly featured web injection and did not block financial fraud'. As long as OP doesn't start fucking with financial things its probably ok.

hey he allowed to post this outside the marketplace? lol

ng-Coder - April 1, 2016, 5:35 am

(Apr 1, 2016 02:23 AM)inc rcx Wrote: [\[CITE\]](#) Please don't tell me you're one of those people that decompresses GZIP with wininet.

I didn't decompress packets with wininet or any other library, I use self crafted snippet which I considered smarter and faster.

FormBook contains so much implementations to handle many other things on its own, that's why the size is soo big ~40kb

Sai Hung - April 1, 2016, 12:19 pm

When you hook chrome most times http data displays correctly but https data are always displayed in form of symbols why is that? Ever had experiences like that? @ngcoder

ng-Coder - April 1, 2016, 1:17 pm

(Apr 1, 2016 12:19 PM)Sai Hung Wrote: [\[CITE\]](#) When you hook chrome most times http data displays correctly but https data are always displayed in form of symbols why is that? Ever had experiences like that? @ngcoder

That's because the https data you got is been encrypted or compressed.

Plz ask such question in code/help thread and not here on sales thread.

inc rcx - April 1, 2016, 2:45 pm

(Apr 1, 2016 05:35 AM)ng-Coder Wrote: [\[CITE\]](#) I didn't decompress packets with wininet or any other library, I use self crafted snippet which I considered smarter and faster.

FormBook contains so much implementations to handle many other things on its own, that's why the size is soo big ~40kb

'self crafted snippet'? Proper implementations use stripped zlib ~ 10kb MAX or IFilter interface.

HIGH PAID FELLA - April 1, 2016, 3:26 pm

(Apr 1, 2016 02:45 PM)inc rcx Wrote: [\[CITE\]](#) 'self crafted snippet'? Proper implementations use stripped zlib ~ 10kb MAX or IFilter interface.

He doesn't know how to disable SPDY, LOL. Probably he can't handle the dynamic functions ?

ng-Coder - April 1, 2016, 10:42 pm

(Apr 1, 2016 02:45 PM)inc rcx Wrote: [\[CITE\]](#) 'self crafted snippet'? Proper implementations use stripped zlib ~ 10kb MAX or IFilter interface.

I wouldn't be explaining/analysing codes here since this is sales thread.

Self crafted, I mean my optimised smaller and faster function to handle compression/inflate/deflates cases. This is balloon you're not allow to link library anyhow, what do you gain from trolling?. seriously you need to change pal.

(Apr 1, 2016 03:26 PM)astr Wrote: [\[CITE\]](#) He doesn't know how to disable SPDY, LOL. Probably he can't handle the dynamic functions ?

Lol, it's better to disable SPDY than to just work flawless with it right?

Dynamic function? I said all hooks are thread safe, you suppose to know the person that does that know far more than just function hooks/calls.

Also SPDY is dead, I support it just for very rear case like 5/100, people that can't stay with HTTP1 and moved to SPDY then has now switched to HTTP2.

.

inc rcx - April 1, 2016, 11:05 pm

(Apr 1, 2016 10:42 PM)ng-Coder Wrote: [\[CITE\]](#) I wouldn't be explaining/analysing codes here since this is sales thread, You can't teach me how to implement my stuffs, least you're far from that level.

Lol, it's better to disable SPDY than to just work flawless with it?

Dynamic function? I said all hooks are thread safe, you suppose to know the person that does that know far more than just function hooks/calls.

I wouldn't be explaining/analysing codes here since this is sales thread, You can't teach me how to implement my stuffs, least you're far from that level.

I can code a better formgrabber in five minutes, using the public symbol servers and a brain.

You skid. ? Oh and i'll definitely make it a space monkey executable file.

ng-Coder - April 1, 2016, 11:39 pm

(Apr 1, 2016 11:05 PM)inc rcx Wrote: [\[CITE\]](#) I wouldn't be explaining/analysing codes here since this is sales thread, You can't teach me how to implement my stuffs, least you're far from that level.

I can code a better formgrabber in five minutes, using the public symbol servers and a brain.

You skid. ? Oh and i'll definitely make it a space monkey executable file.

I forwarded you sample long ago when you were crying you can code such.

I know you have 2% knowledge of what this takes and even with my help you still won't able to code this in 5yrs. all you can do with your life is trolling up and down as you usually do.

Internet mouth drivers like you are nothing new nor strange to me.

.

inc rcx - April 1, 2016, 11:54 pm

(Apr 1, 2016 11:39 PM)ng-Coder Wrote: [\[CITE\]](#) I forwarded you sample long ago when you were crying you can code such.

I know you have 2% knowledge of what this takes and even with my help you still won't able to code this in 5yrs. all you can do with your life is trolling up and down as you usually do.

Internet mouth drivers like you are nothing new nor strange to me.

.Yet I wrote rombortik a week after I learned, and I proved you wrong in all circumstances. You don't even understand what metamorphism is. I doubt the code of this shitty fg is quality of any nature.

I've already fucked you up because you can't code.

You probably failed all your math classes you mathematically inept fuck.

Spdy is deprecated and I've already pointed that out in your shitty dev thread. The fact that you don't seem to understand how google manages the network protocols baffles me. Spdy isn't even needed to begin with.

ng-Coder - April 2, 2016, 12:32 am

(Apr 1, 2016 11:54 PM)inc rcx Wrote: [\[CITE\]](#) Yet I wrote rombortik a week after I learned, and I proved you wrong in all circumstances. You don't even understand what metamorphism is. I doubt the code of this shitty fg is quality of any nature.

I've already fucked you up because you can't code.

You probably failed all your math classes you mathematically inept fuck.

Spdy is deprecated and I've already pointed that out in your shitty dev thread. The fact that you don't seem to understand how google manages the network protocols baffles me. Spdy isn't even

needed to begin with.

Lol, ofcourse I know you coded rombershit kid. You don't need to disgrace yourself and you could've just leave this thread for good.

Non of my student will compile a code as shitty as rombertik and call it malware and I can imagine how many years it took you to compile that skidded shit. It will take you least 10yrs to write a code close to level of FormBook.

To start with, FormBook is asm and a balloon executable, you don't need to be a reverser to see clearly that this is far different to skidded shit.

I will not be replying you on this thread anymore, do you mind to see my mathematics awards?

.

inc rcx - April 2, 2016, 12:34 am

(Apr 2, 2016 12:32 AM)ng-Coder Wrote: [\[CITE\]](#) Lol, ofcourse I know you coded rombershit kid. You don't need to disgrace yourself and you could've just leave this thread for good.

Non of my student will compile a code as shitty as rombertik and call it malware and I can imagine how many years it took you to compile that skidded shit. It will take you least 10yrs to write a code close to level of FormBook.

To start with, FormBook is asm and a balloon executable, you don't need to be a reverser to see clearly that this is far different to skidded shit.

I will not be replying you on this thread anymore, do you mind to see my mathematics awards?

.It took me 1 day to make, with 7 days of learning to code, better than what you'll ever accomplish in your life and more importantly i made more money from that project alone than you'll ever make in your life.

There's no such thing as a balloon executable, you down syndrome fucking retard. (PIC is nothing impressive, stop acting like it is, you compile with no random base address, therefore no relocations, you either merge .data or don't use globals, you don't reference characters as strings to avoid .rdata, and more importantly you pass a local pointer with dynamic functions). Anyone with an IQ of 90 can write PIC. It's all relative.

Your shit is skidded shit, you use mainstream techniques of walking the PEB and traversing the EAT. You're just like every other wannabe.

Students? Glad to see there will be a bunch of shitty malware developers that excel in failing at mathematics.

I repeat, it will take me FIVE minutes to write something better than your shitty 'formbook' Not only that i'll actually DECOMPRESS http2 headers because i understand RFCs

```
symchk.exe /r c:\progra~1\mozill~1\* /s SRV*C:\symcache\*symbols.mozilla.org/  
symchk.exe /r c:\progra~1\chrome\* /s  
SRV*C:\symcache\*chromium-browser-symsrv.commondatastorage.googleapis.com/
```

Sai Hung - April 2, 2016, 9:28 am

@inc rcx, hay mate, why don't you cool down.

It's his sales thread, allow him to show what he's got, not saying you insulting here, don't ruin his show. Ng coder is someone who maybe wouldn't want to show u everything, but I believe one way or the other he's good at what he does, same thing as you.

So relax, don't spoil the fun pls, let him sell what he has and let's meet you who knows how to code. I believe you would be willing to share ideas.

Kindly don't see it that I want to insult you here, just calm down, and let him sell what he has.

Remix - April 2, 2016, 1:09 pm

(Apr 1, 2016 11:54 PM)inc rcx Wrote: [\[CITE\]](#) Yet I wrote rombortik a week after I learned Yet no one cares.

I'm wondering why you still come back to HF every time you get banned/closed.

Didn't you say you're done with HF?

I see.

Tell me how bad I am in C/C++

I couldn't give less fucks

inc rcx - April 2, 2016, 3:26 pm

(Apr 2, 2016 01:09 PM)Teh Remix Wrote: [\[CITE\]](#) Yet no one cares.

I'm wondering why you still come back to HF every time you get banned/closed.

Didn't you say you're done with HF?

I see.

Tell me how bad I am in C/C++

I couldn't give less fucks

Good, that's how most bad programmers are they've taken enough criticism.

Remix - April 3, 2016, 3:23 am

(Apr 2, 2016 03:26 PM)inc rcx Wrote: [\[CITE\]](#) Good, that's how most bad programmers are they've taken enough criticism.

Please stick to the topic

No need to tell me how bad programmers are since I'm a bad programmer

And stop sales trashing please

inc rcx - April 3, 2016, 3:45 am

(Apr 3, 2016 03:23 AM)Teh Remix Wrote: [\[CITE\]](#) Please stick to the topic

No need to tell me how bad programmers are since I'm a bad programmer

And stop sales trashing please

Sales trashing versus exposing a shit coder?

lol ok keep buying skid products, you skids. you'll never learn logic.

Mcbride - April 3, 2016, 4:08 am

' Wrote:FormBook Features

- Coded in C/ASM

- Startup (Hidden)

- Full PE-Injection (No dll/ No drop)

- Ring3 kit (Lagos Island method)
- Bin is Balloon Executable (MPIE + MEE)
- Doesn't use suspicious windows API (96% of API used are from Lagos)
- 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 balloon), ~20kb (compressed)
- Intuitive PHP Panel
<https://i.imgur.com/rKPVSnA.jpg>
- Bugfix, Updates and Support is free.hahaha! horse shit... "lagos island method" GTFO

Remix - April 3, 2016, 6:11 am

(Apr 3, 2016 03:45 AM)inc rcx Wrote: [\[CITE\]](#) lol ok keep buying skid products, you skids. you'll never learn logic.

I will because I'm a skid that will never learn logic

Now leave HF

Nobody wants you here and you're just crying how bad everyone is

Sai Hung - April 3, 2016, 8:09 am

(Apr 3, 2016 06:11 AM)Teh Remix Wrote: [\[CITE\]](#) I will because I'm a skid that will never learn logic
Now leave HF

Nobody wants you here and you're just crying how bad everyone is

Stop talking to him. Just leave him alone, he hasn't even asked himself this, ngcoder makes a lot of money from these things, he criticises, other than make his own dough, he's there ranting. Just ignore him.

You do know how to decompress https traffic yeh? In formgrabbers?

Remix - April 3, 2016, 11:45 am

(Apr 3, 2016 08:09 AM)Sai Hung Wrote: [\[CITE\]](#) Stop talking to him. Just leave him alone, he hasn't even asked himself this, ngcoder makes a lot of money from these things, he criticises, other than make his own dough, he's there ranting. Just ignore him.

You do know how to decompress https traffic yeh? In formgrabbers?

He needs to tell me how bad I am

That's the only purpose of his life

ng-Coder - April 3, 2016, 12:06 pm

(Apr 3, 2016 11:45 AM)Teh Remix Wrote: [\[CITE\]](#) He needs to tell me how bad I am

That's the only purpose of his life

Just ignore the kid my buddy, I'm busy moving forward and making money, let him keep crying cos he can't code this in 10years, I wonder why he feels it's anybody's fault that he's a looser, lol.

Just keep coding for living ?, Don't reply him again please.

.

Sai Hung - April 3, 2016, 1:47 pm

(Apr 3, 2016 11:45 AM)Teh Remix Wrote: [\[CITE\]](#) He needs to tell me how bad I am

That's the only purpose of his life

Nah, don't waste time talking to him. Just forget him.

inc rcx - April 3, 2016, 3:44 pm

(Apr 3, 2016 08:09 AM)Sai Hung Wrote: [\[CITE\]](#) Stop talking to him. Just leave him alone, he hasn't even asked himself this, ngcoder makes a lot of money from these things, he criticises, other than make his own dough, he's there ranting. Just ignore him.

You do know how to decompress https traffic yeh? In formgrabbers?

You don't decompress https traffic.

(Apr 3, 2016 12:06 PM)ng-Coder Wrote: [\[CITE\]](#) Just ignore the kid my buddy, I'm busy moving forward and making money, let him keep crying cos he can't code this in 10years, I wonder why he feels it's anybody's fault that he's a looser, lol.

Just keep coding for living ?, Don't reply him again please.

.

Yes because hooking exported functions and calling inflate is hard, and using terms like balloon & lagos island rootkit are just as difficult.

(Apr 3, 2016 06:11 AM)Teh Remix Wrote: [\[CITE\]](#) I will because I'm a skid that will never learn logic
Now leave HF

Nobody wants you here and you're just crying how bad everyone is

I don't even know you, that's the funny part. The only people that DONT want me here are the incompetent ones i tend to expose, you, the OP, and a few others on this forum.

I wonder what functions i'd hook for ssl on chrome?

code.google.com/p/chromium/codesearch#chromium/src/third_party/boringssl/src/ssl/ssl_lib.c&q=ssl_write&sq=package:chromium&type=cs&l=629

What about spdy & http/2?

code.google.com/p/chromium/codesearch#chromium/src/net/spdy/spdy_http_stream.cc&sq=package:chromium&type=cs :: << spdystream::sendrequest

Functions located in memory for Chrome ::

Zlib:

sendspace.com/file/f1cmv9

Now anyone in this thread can make a better formgrabber than your shitty poorly written "formbook" bullshit.

Or hell if you're lazy and don't feel like decompressing

code.google.com/p/chromium/codesearch#chromium/src/net/http/http_network_session.h&q=enable_http2&sq=package:chromium&type=cs&l=92

xor r12 r12 - April 3, 2016, 10:09 pm

I overlooked http/2 and managed to decompress all headers.

"A receiving endpoint reassembles the header block by concatenating its fragments and then decompresses the block to reconstruct the header list."

This is simple enough, every type 0x01 received needs to be concatenated in your formgrabber, then once the request is HEADERS END in the flags you know that's the end of the block and you can proceed to decode the block.

You seem incompetent, this took me 20 minutes.

3 Bytes = frame payload size

1 byte = type

1 byte = flags

R + Stream Identifier = 4 bytes

Then framepayload.

not difficult.

Example data frame host: facebook.com [9704]

lsd=AVoPGAdO&display=&enable_profile_selector=&isprivate=&legacy_return=1&profile_selector_id=&skip_api_login=&signed_next=&trynum=1&timezone=360&lgndim=eyJ3J3ljozMzY2LCJoljo3NjgsImF3ljozMzY2LCJhaCI6NzI4LCJljoyNH0%3D&lgnd=231604_I7gK&lgns=1459750577&email=fuckyou%40facebook.com&pass=fuckyeah&default_persistent=0&qstamp=W1tbNywxOSw0MSw0Nyw2MSwxMTMsMTE2LDExNywxMjAsMTI5LDEzNSwxNTcsMTgxLDE4NCwxOTMsMTk2LDE5NywyMjQsMjM2LDE1MCwyODgsMzA4LDMxMSwzMjMsMzQ1LDM0NywzNTAsMzY4LDM3MiwzNzMsMzk0LDQwMiw0NjlsNDY4LDQ5NCw1NTAsNTYwLDU2OCw1NzEsNTk1LDY0OCw3ODFdXSwiQVprWmRoeXlFVVVetbjFsV1RHM3c0Z21vQksxeUtRTHlxUUtySzJGeEpybng4Qk9wb2RPQ3dVaDdxUE9pTWxmdGxpRHY0RGdZQzN4bEk2VTk5WGNua2xfN2pGYmRPb290UzFtYXNfQkl5SEhaVnVwekNaSENYWHBCdFpVTGVXa05aQ3JsWVFmOXJtUkhLOVltMDQ0UjYycTI2OGxKN0NJSWYwX1EwWXBVZlpRaG1DdDFEYzQ5Z0J6SWxFTUFfS3paT3dsS0dUdWcyZkxkFa0lGTG00VUtPM2NJII0%3D

yunohpackdecompress? ?

SREE - April 7, 2016, 12:47 am

Vouch For the Form Book. One and only Simple and Powerfull Form grabber and bug less one .. i have used so many form grabber but this one is cool the user wont even notice this infected their system becoz it wont affect system performances and wont crash browsers.. works well with ff and crome latest versions.. thanks man :) keep the good work up..

xor r12 r12 - April 7, 2016, 12:36 pm

(Apr 7, 2016 12:47 AM)SREE Wrote: [\[CITE\]](#) Vouch For the Form Book. One and only Simple and Powerfull Form grabber and bug less one .. i have used so many form grabber but this one is cool the user wont even notice this infected their system becoz it wont affect system performances and wont crash browsers..

works well with ff and crome latest versions.. thanks man :) keep the good work up..
and yet OP can't implement HPACK decompression for http/2.

ng-Coder - April 8, 2016, 2:20 am

(Apr 7, 2016 12:47 AM)SREE Wrote: [\[CITE\]](#) Vouch For the Form Book. One and only Simple and Powerfull Form grabber and bug less one .. i have used so many form grabber but this one is cool the user wont even notice this infected their system becoz it wont affect system performances and wont crash browsers..

works well with ff and crome latest versions.. thanks man :) keep the good work up..
Thanks ?.

xor r12 r12 - April 8, 2016, 2:41 am

(Apr 8, 2016 02:20 AM)ng-Coder Wrote: [\[CITE\]](#) Thanks ?.
pm me, i'll sell u the hpack decompressor i wrote for \$25.

Simple technique:

Hook ssl_free/ssl_write

Determine HTTP/2 Header prefix socket, if so, decompress 0x00 headers, and then concatenate data until received headers-terminate flag, or whatever it's referred to. Once i've assembled the block i decompress the entire block and parse the host.... simple, effective, thread safe and clean. You could choose how to implement the compression, if you're not associating each PR structure with a linked list node... it's fine

rep movsb - April 9, 2016, 12:14 am

almost forgot to include proof
i.imgur.com/BBItOoM.png

TERRORISST-- - April 13, 2016, 1:17 am

I don't see how this formgrabber can parse Google Requests from Google Chrome since google chrome uses QUIC for it's own services (Packet's are encrypted under TLS).

ng-Coder - April 13, 2016, 2:32 am

(Apr 13, 2016 01:17 AM)TERRORISST-- Wrote: [\[CITE\]](#) I don't see how this formgrabber can parse Google Requests from Google Chrome since google chrome uses QUIC for it's own services (Packet's are encrypted under TLS).

FormBook works with gmail on google Chrome, proof is there on the tread.

<https://i.imgur.com/btUksaS.jpg>

As for the header you can see it's senseless and unnecessary overhead.
I do what I consider to be best and most efficient.

Also, FormBook create/spawn no thread to archive flawless speed then it will be senseless making those real process threads do additional work.

.

TERRORISST-- - April 13, 2016, 3:26 am

(Apr 13, 2016 02:32 AM)ng-Coder Wrote: [\[CITE\]](#) FormBook works with gmail on google Chrome, proof is there on the tread.

As for the header you can see it's senseless and unnecessary overhead.
I do what I consider to be best and most efficient.

Also, FormBook create/spawn no thread to archive flawless speed then it will be senseless making those real process threads do additional work.

1. Chrome Will occasionally switch to http / 2.0 at times, other than that it's TLS under QUIC for it's own services (GMAIL,YOUTUBE,etc..). As you can see below. (That screenshot proves nothing, except for the fact that you might have disabled cookies and logged into GMAIL several times for it to authenticate through TCP & http / 2.0)

2. Huffman decompression takes up no noticeable performance time, there will come time when HTTP 2.0 is the new standard, not all of the payload information will give you the host. For instance, tribot dot ORG, or twitter (perhaps?)

Here is what the payload looks like under QUIC:

i.imgur.com/z1c0MdA.png << Here you can see the alternate service negotiation and the switch between h2 to QUIC
i.imgur.com/AH14hIS.png
i.imgur.com/KhcGAb5.png -- FOLLOWED BY PAYLOAD IN NEXT PACKET

3. HTTP 2.0 is simple to parse the payload.

As for parsing the headers, well that's a different story. Huffman algorithm is long, extensive, and could up your binary by 10 KB. But in the end it's worth it, and skids can't do it.

ng-Coder - April 13, 2016, 5:24 am

(Apr 13, 2016 03:26 AM)TERRORISST-- Wrote: [\[CITE\]](#) 1. Chrome Will occasionally switch to http / 2.0 at times, other than that it's TLS under QUIC for it's own services (GMAIL,YOUTUBE,etc..). As you can see below. (That screenshot proves nothing, except for the fact that you might have disabled cookies and logged into GMAIL several times for it to authenticate through TCP & http / 2.0)

2. Huffman decompression takes up no noticeable performance time, there will come time when HTTP 2.0 is the new standard, not all of the payload information will give you the host. For instance, tribot dot ORG, or twitter (perhaps?)

Here is what the payload looks like under QUIC:

i.imgur.com/z1c0MdA.png << Here you can see the alternate service negotiation and the switch between h2 to QUIC
i.imgur.com/AH14hIS.png
i.imgur.com/KhcGAb5.png -- FOLLOWED BY PAYLOAD IN NEXT PACKET

3. HTTP 2.0 is simple to parse the payload.

As for parsing the headers, well that's a different story. Huffman algorithm is long, extensive, and could up your binary by 10 KB. But in the end it's worth it, and skids can't do it.

Oh you've changed your nameset again? I didn't know it's you this useless loser, I repeat! It will take you 10yrs to code anything close to FormBook.

This is your 999th account here, can't you simply see you're the most retarded loser!?

No reply for you again but you're free to keep bumping for me.

.

TERRORISST-- - April 13, 2016, 5:34 am

(Apr 13, 2016 05:24 AM)ng-Coder Wrote: [\[CITE\]](#) Oh you've changed your nameset again? I didn't know it's you this useless loser, I repeat! It will take you 10yrs to code anything close to FormBook.

This is your 999th account here, can't you simply see you're the most retarded loser!?

No reply for you again but you're free to keep bumping for me.

.

You ignored my entire post because you know I'm right, and why would it take me 10 years? I just proved to you that QUIC is necessary, and have shown you that i'm more capable than you.

you can't even huffman/quic, skid.

MrBorAo - April 14, 2016, 2:10 pm

PM me your jabber.

Interested in buying.

ng-Coder - April 15, 2016, 1:34 am

(Apr 14, 2016 02:10 PM)MrBorAo Wrote: [\[CITE\]](#) PM me your jabber.

Interested in buying.

Skype is what I use, Ng.Coder

.

TERRORISST---- - April 15, 2016, 3:30 am

(Apr 15, 2016 01:34 AM)ng-Coder Wrote: [\[CITE\]](#) Skype is what I use, Ng.Coder

.

ur formgrabber is broken i repeat ur shitty formgrabber is broken

MrBorAo - April 15, 2016, 4:48 am

(Apr 15, 2016 01:34 AM)ng-Coder Wrote: [\[CITE\]](#) Skype is what I use, Ng.Coder

.

And I dont use skype so send me your jabber.

TERRORISST---- - April 15, 2016, 4:56 pm

(Apr 15, 2016 04:48 AM)MrBorAo Wrote: [\[CITE\]](#) And I dont use skype so send me your jabber.

how fucking dumb are you? Read what i posted above, clearly the OP doesn't indicate any signs of intelligence.

You're buying a broken piece of shit that doesn't decompress headers, nor support QUIC.

CosmicTheGod - April 15, 2016, 5:05 pm

Ballon Executable ??!!?? Lagos Island ???

Shit where do you get your drugs my friend ?

elipheleht - April 17, 2016, 12:25 am

haters gonna hate. i'm gonna still buy this...i don't care what any hater thinks. this product seems ubber legit. ng coder PM me about payment and your yahooo messenger id or naija number. also accept my add request on skype . my skype id is elipheleh

keep flying that flag.

TERRORISST----- - April 17, 2016, 1:29 am

(Apr 17, 2016 12:25 AM)elipheleht Wrote: [\[CITE\]](#) haters gonna hate. i'm gonna still buy this...i don't care what any hater thinks. this product seems ubber legit. ng coder PM me about payment and your yahooo messenger id or naija number. also accept my add request on skype . my skype id is elipheleh

keep flying that flag.

Haters going to Hate? I'm providing discrete proof that this grabber does NOT work.

Continue to waste your money, dumb fucking skid.

Telling by your signature, you're some down syndrome dick riding moron.

ng-Coder - April 17, 2016, 3:12 am

(Apr 17, 2016 12:25 AM)elipheleht Wrote: [\[CITE\]](#) haters gonna hate. i'm gonna still buy this...i don't care what any hater thinks. this product seems ubber legit.

? don't mind that animal, he's just trying to make me reply him.

His stupidity is unimaginable and he doesn't worth talking to, Omni is trying his best to get rid of him though.

He can't even afford a copy of FormBook to know what the code looks like left alone to know if there is any bug, then he started crying when I refused to give him a review copy, lol what a loser.

.

TERRORISST----- - April 17, 2016, 4:25 am

(Apr 17, 2016 03:12 AM)ng-Coder Wrote: [\[CITE\]](#) ? don't mind that animal, he's just trying to make me reply him.

His stupidity is unimaginable and he doesn't worth talking to, Omni is trying his best to get rid of him though.

He can't even afford a copy of FormBook to know what the code looks like left alone to know if there is any bug, then he started crying when I refused to give him a review copy, lol what a loser.

.Says the guy who's incapable of decompressing http2.0 headers, implementing quic, and makes up terms.

I'll let the customers speak for your shitty malware.

Dw once I'm finished with my final exams I'll knock this shit out of hf.

stackoverflowin - April 17, 2016, 4:29 am

(Apr 17, 2016 04:25 AM)TERRORISST----- Wrote: [\[CITE\]](#) Says the guy who's incapable of decompressing http2.0 headers, implementing quic, and makes up terms.

I'll let the customers speak for your shitty malware.

Dw once I'm finished with my final exams I'll knock this shit out of hf.

Wait, in the OP it says he supports HTTP/2.0 but he doesn't decompress the headers?

Sai Hung - April 18, 2016, 12:56 am

@Terrorist, and yet I sent you a mail and asked you to assist on how to send logs to a php server since I didn't know much and you didn't gimme a reply even till date.

I wonder why,

Hoodie+ - April 18, 2016, 11:26 am

(Apr 18, 2016 12:56 AM)Sai Hung Wrote: [\[CITE\]](#) @Terrorist, and yet I sent you a mail and asked you to assist on how to send logs to a php server since I didn't know much and you didn't gimme a reply even till date.

I wonder why,

He's banned and can't send PMs if he doesn't have 25 posts.

locit - April 18, 2016, 3:36 pm

(Apr 17, 2016 04:25 AM)TERRORISST----- Wrote: [\[CITE\]](#) Says the guy who's incapable of decompressing http2.0 headers, implementing quic, and makes up terms.

I'll let the customers speak for your shitty malware.

Dw once I'm finished with my final exams I'll knock this shit out of hf.

<TERRORISST> Anyone here know what a lagos island rootkit is?

And yet you dont know anything

TERRORISST- - April 18, 2016, 4:01 pm

(Apr 18, 2016 03:36 PM)locit Wrote: [\[CITE\]](#) <TERRORISST> Anyone here know what a lagos island rootkit is?

And yet you dont know anything
it's that bad isnt it

drewkasp - April 20, 2016, 1:57 am

would have bought this tool but seeing the ups and downs and doubts involved..i'd rather stay clear.
GLWS OP.

ng-Coder - April 20, 2016, 6:28 am

(Apr 20, 2016 01:57 AM)drewkasp Wrote: [\[CITE\]](#) would have bought this tool but seeing the ups and downs and doubts involved..i'd rather stay clear.

GLWS OP.
? thanks pal.

I have much customers and they are all satisfied so I don't care about a single low life kid hating, I'm damn busy ?.

neo da matrix - April 20, 2016, 8:32 am

ng coder reply your pm's, i sent you a message

ng-Coder - April 21, 2016, 3:19 am

(Apr 20, 2016 08:32 AM)neo da matrix Wrote: [\[CITE\]](#) ng coder reply your pm's, i sent you a message
Replied. ?

okobino1 - April 22, 2016, 3:07 am

Omo Niaja, NG-Coder, Lagos Island Root kit... I hailzzz

In_Case_You_Need_Help - April 23, 2016, 9:48 am

(Apr 22, 2016 03:07 AM)okobino1 Wrote: [\[CITE\]](#) Omo Niaja, NG-Coder, Lagos Island Root kit... I hailzzz
lol.. lekki nko ?

ng-Coder - April 23, 2016, 5:03 pm

(Apr 22, 2016 03:07 AM)okobino1 Wrote: [\[CITE\]](#) Omo Niaja, NG-Coder, Lagos Island Root kit... I hailzzz

(Apr 23, 2016 09:48 AM)In_Case_You_Need_Help Wrote: [\[CITE\]](#) lol.. lekki nko ?
Lol, it's not what you guys think.

MalwareTech - April 24, 2016, 3:02 pm

Usually I don't concern myself with threads like these, but I've now had multiple people who are just trying to learn contacting me to ask about "MEE", "MPIE" and "Balloon Executables" so I'll say here what I said to them.

These are not real terms, they are acronyms and words you've literally just made up to try and seem intelligent and well informed, a quick google for both "Multiple Entry Executable" and "Mapped Position Independent Executable" returns no results other than this thread you've authored and "Balloon Exeuctable" returns 88 results, only 2 of which are relevant and guess who authored both of those (yes, you!). "MEE" and "Balloon Executable" are complete bullshit terms you've coined for no good reason and "MPIE" is just stupid new way you've made up to say "shellcode". The proper term is PIC (position independent code) or shellcode (same as PIC), kindly please find another way to portray your superior intellect other than confusing people who just want to learn with made up terminology, it's not fair on them and it's not fair on the people like me who have to explain to them they were trolled.

VisualSoft - April 24, 2016, 3:04 pm

despite this terms which do not exit , does this really work?

CosmicTheGod - April 24, 2016, 3:28 pm

(Apr 24, 2016 03:04 PM)VisualSoft Wrote: [\[CITE\]](#) despite this terms which do not exit , does this really work?

Doesn't support QUIC doesn't decompress HTTP/2 headers so it doesn't work correctly plus there's no such thing as Lagos Island Rootkit .

It's just a Nigerian Scam 419 guys doing malware stuff .

GTFO NG Coder pfffffffff

HIGH PAID FELLA - April 24, 2016, 3:39 pm

Lmao ^

Calling it a Nigerian scam, yeah it is actually getting annoying.

Master in Online Business - April 24, 2016, 3:49 pm

Good work and all the best bros

ng-Coder - April 25, 2016, 12:55 am

(Apr 24, 2016 03:02 PM)# Wrote: [\[CITE\]](#) Usually I don't concern myself with threads like these, but I've now had multiple people who are just trying to learn contacting me to ask about "MEE", "MPIE" and "Balloon Executables" so I'll say here what I said to them.

These are not real terms, they are acronyms and words you've literally just made up to try and seem intelligent and well informed, a quick google for both "Multiple Entry Executable" and "Mapped Position Independent Executable" returns no results other than this thread you've authored and "Balloon Exeuctable" returns 88 results, only 2 of which are relevant and guess who authored both of those (yes, you!). "MEE" and "Balloon Executable" are complete bullshit terms you've coined for no good reason and "MPIE" is just stupid new way you've made up to say "shellcode". The proper term is PIC (position independent code) or shellcode (same as PIC), kindly please find another way to portray your superior intellect other than confusing people who just want to learn with made up terminology, it's not fair on them and it's not fair on the people like me who have to explain to them they were trolled.

I respect you and I never thought you could go this low, here isn't a patent office, least you could've talk to me.

.
(Apr 24, 2016 03:04 PM)VisualSoft Wrote: [\[CITE\]](#) despite this terms which do not exit , does this really work?

This formgrabber works perfectly as advertised and all customers are satisfied as you can see no customer made complain that any of the said claims isn't correct.

.
Malwaretechchatparticipan - April 25, 2016, 1:57 am

(Apr 25, 2016 12:55 AM)ng-Coder Wrote: [\[CITE\]](#) I respect you and I never thought you could go this low, here isn't a patent office, least you could've talk to me.

.
This formgrabber works perfectly as advertised and all customers are satisfied as you can see no customer made complain that any of the said claims isn't correct.

.Doesn't matter, doesn't support QUIC, nor decompress HTTP2. Have fun parsing google services on chrome / chromium / opera. ?

No customers complained because:

1. You don't have any.

2. All other vouches are your friends.

(You probably won't add support for another ten years, it's fine)

MalwareTech - April 25, 2016, 2:27 am

(Apr 25, 2016 12:55 AM)ng-Coder Wrote: [\[CITE\]](#) I respect you and I never thought you could go this low, here isn't a patent office, least you could've talk to me.

I don't see how exactly it's low, I am just looking out for the beginner reverse engineers who are getting confused by your made up terms for shellcode and self relocating executables. At least to some extent "MEE" and "MPIE" can be made sense of, but "balloon executable"? You could have at least explained where you pulled the word balloon from, because that term makes literally no sense whatsoever.

You need to understand how infuriating it is when we're trying to help people and they're asking about a bunch of gibberish terms they heard from some guy who heard it from some guy on hackforums.

ng-Coder - April 25, 2016, 3:34 am

(Apr 25, 2016 02:27 AM)# Wrote: [\[CITE\]](#) I don't see how exactly it's low, I am just looking out for the beginner reverse engineers who are getting confused by your made up terms for shellcode and self relocating executables. At least to some extent "MEE" and "MPIE" can be made sense of, but "balloon executable"? You could have at least explained where you pulled the word balloon from, because that term makes literally no sense whatsoever.

You need to understand how infuriating it is when we're trying to help people and they're asking about a bunch of gibberish terms they heard from some guy who heard it from some guy on hackforums.

Low in the sense that you didn't query me directly before concluding and made this post, ofcourse I would've explain, show you and even provide sample.

The term Balloon executable is used by at least two different coding team that I know, never even noticed it's this strange until recently.

Yes:

Balloon executable means a standard executable that can be use as shellcode and it's having multiple enrypoint.

But:

Shellcode is not a standard executable which have PE headers and use the header nor necessary have multiple entries.

What I understand as balloon executable is not self relocating because it relocates nothing as it's doesn't even use import table nor do any type of dynamic relocation.

I'm surely a learner and not trying to pose supirior to anybody, I feel you could've ask me whatever you want through pm/chat and correct what you feel should be corrected amicably.

.

MalwareTech - April 25, 2016, 4:08 am

(Apr 25, 2016 03:34 AM)ng-Coder Wrote: [\[CITE\]](#) Low in the sense that you didn't query me directly before concluding and made this post, ofcourse I would've explain, show you and even provide sample.

The term Balloon executable is used by at least two different coding team that I know, never even noticed it's this strange until recently.

Yes:

Balloon executable means a standard executable that can be use as shellcode and it's having multiple enrypoint.

But:

Shellcode is not a standard executable which have PE headers and use the header nor necessary have multiple entries.

What I understand as balloon executable is not self relocating because it relocates nothing as it's doesn't even use import table nor do any type of dynamic relocation.

I'm surely a learner and not trying to pose supirior to anybody, I feel you could've ask me whatever you want through pm/chat and correct what you feel should be corrected amicably.

.
Sorry if I mistook your intent. I just assumed you were trying to look smart by making up terms, didn't realize you were the victim of someone else's foolery.

For the record, it's still just considered PIC or shellcode even if it's a PE file. The term refers to the fact the code can be run anywhere in memory and format is generally unimportant (though if it requires a relocation table it would usually be considered self relocating rather than position independent). There's also direct code injection, where you inject parts of your executable (usually a few functions) then pass them some kind of table containing runtime data they will need.

I really wouldn't pay any attention to these "coding teams" using ridiculous terms like "balloon executable", they're either strolling or stupid. Anyway, I'm happy to delete my posts, just please don't confuse any more people with these ridiculous terms.

ng-Coder - April 25, 2016, 4:33 am

(Apr 25, 2016 04:08 AM)# Wrote: [\[CITE\]](#) Sorry if I mistook your intent. I just assumed you were trying to look smart by making up terms, didn't realize you were the victim of someone else's foolery.

For the record, it's still just considered PIC or shellcode even if it's a PE file. The term refers to the fact the code can be run anywhere in memory and format is generally unimportant (though if it requires a relocation table it would usually be considered self relocating rather than position independent). There's also direct code injection, where you inject parts of your executable (usually a few functions) then pass them some kind of table containing runtime data they will need.

I really wouldn't pay any attention to these "coding teams" using ridiculous terms like "balloon executable", they're either strolling or stupid. Anyway, I'm happy to delete my posts, just please don't confuse any more people with these ridiculous terms.

Thanks anyway, I'll review the thread.

.
_Devil - April 25, 2016, 1:40 pm

I am so confused with all this talk on the thread, Can some one please explain me what is Boolean Executable.

topLevel - April 25, 2016, 2:51 pm

(Apr 25, 2016 01:40 PM)_Devil Wrote: [\[CITE\]](#) I am so confused with all this talk on the thread, Can some one please explain me what is Boolean Executable.
go up 2 posts. he explains it.

ng-Coder - May 8, 2016, 4:11 pm

(Apr 25, 2016 01:40 PM)_Devil Wrote: [\[CITE\]](#) I am so confused with all this talk on the thread, Can some one please explain me what is Boolean Executable.
Don't worry about balloon executable pal, it says nothing than you can use any crypter for it ?.

ng-Coder - June 13, 2016, 11:31 am

(Jun 13, 2016 10:32 AM)khanisgr8 Wrote: [\[CITE\]](#) Today i have found short time to do small Review of Second Version of This form grabber..

I have already done

Review of old version : <https://hackforums.net/showthread.php?tid=5200139>

Lets continue talking about this second version. what is changed ? and is the quality improved or no ?

I tested This version in

Windows 8.1 Pro(64bit)

Windows 7 Ultimate(32bit)

Windows 10 x64

In this version

Browser-Keylogger is very useful and working very good .

Their was bug in old version It send to much junk to panel but in this version there is strong filter (To filter junk requests)

It is tested in

windows 10 x64 chrome 32bit

Windows 10 x64 bit and internet explorer edge x64

Windows 10 x64 bit and Firefox 64bit

Windows 8 x62 bit and Firefox 63bit

In all my tests injection was succesfull..

It will terminate and will not inject if comodo or vmware or wireshark or any other monitoring tool is running

Peace ?

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>