

Forum:[Hack Forums](#)

Thread: [FormBook \[Formgrabber\] reviewer wanted](#)

ng-Coder - February 12, 2016, 3:16 am

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

- Coded in C/ASM
- Grab from Iexplore, Firefox and Chrome.
- Support HTTP, HTTPS, SPDY and HTTP/2
- Bin is Balloon Executable. (MPIE + MEE)
I think this is first time any public product will be balloon.
- Ring3 Kit (Lagos Island method)

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

If you're interested plz apply.

Application requirements:

Positive Reputation

Experience with Formgrabbers

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

Questions are welcome if you guys have any, thanks.

ng-Coder - February 12, 2016, 4:19 am

(Feb 12, 2016 05:10 AM)The Watcher?? Wrote: [\[CITE\]](#) FormBook - The Ebook that's actually a Form Grabber! I like it. Not sure if it will be allowed to be sold here though? lol

How much were you thinking about selling this for? I'd be interested in taking a read.

It's not Ebook :,), why will it not allow? many Formgrabber are sold here, I appreciate your interest but I feel you're not having experience with formgrabber ?

FSBN - February 12, 2016, 4:22 am

I would like to get a free copy for a review. Let me know.

ng-Coder - February 12, 2016, 4:35 am

(Feb 12, 2016 05:29 AM)The Watcher?? Wrote: [\[CITE\]](#) For fuck sake I want to read it, how much? ? It's not a book pal...

bluntly - February 12, 2016, 4:37 am

I might seem unexperienced, but I think I know pretty much about formgrabbers. What method do you use? Do you create an Add-On? Or do you simply hook your app. to certain pointers of the browser ? I'm really interested to see how you made it work and see it in action :)

ng-Coder - February 12, 2016, 4:49 am

(Feb 12, 2016 05:37 AM)bluntly Wrote: [\[CITE\]](#) I might seem unexperienced, but I think I know pretty much about formgrabbers. What method do you use? Do you create an Add-On? Or do you simply hook your app. to certain pointers of the browser ? I'm really interested to see how you made it work

and see it in action :)

No Add-On, FormBook first Injects itself into windows trusted process and inject the browsers from there, full PE injection.

bluntly - February 12, 2016, 5:02 am

(Feb 12, 2016 05:49 AM)ng-Coder Wrote: [\[CITE\]](#) No Add-On, FormBook first Injects itself into windows trusted process and inject the browsers from there, full PE injection.

How long have you been coding?

Shoe - February 12, 2016, 5:06 am

FormGrabbers aren't allowed, I do believe. I could be wrong but last time I heard they aren't allowed.

ng-Coder - February 12, 2016, 5:15 am

(Feb 12, 2016 06:02 AM)bluntly Wrote: [\[CITE\]](#) How long have you been coding?

? Does that matter? Well 12 yrs now.

(Feb 12, 2016 06:06 AM)Shoe Wrote: [\[CITE\]](#) FormGrabbers aren't allowed, I do believe. I could be wrong but last time I heard they aren't allowed. We have many Formgrabber out here, they are dead because of lack of update.

bluntly - February 12, 2016, 5:33 am

Just wondered how much experience is put into this FormGrabber :D

Shoe - February 12, 2016, 5:39 am

(Feb 12, 2016 06:15 AM)ng-Coder Wrote: [\[CITE\]](#) We have many Formgrabber out here, they are dead because of lack of update.

That doesn't matter, how dead they are. What matters is whether or not HF allows formgrabbers to be discussed.

Amerikanski - February 12, 2016, 5:45 am

What do you do when chrome updates the functions to be hooked. Can you hook x64 browsers?

Also what is the lagos method? Can I try your software?

ng-Coder - February 12, 2016, 5:52 am

(Feb 12, 2016 06:39 AM)Shoe Wrote: [\[CITE\]](#) That doesn't matter, how dead they are. What matters is whether or not HF allows formgrabbers to be discussed.

Yes it's allowed. formgrabbers are sold here, this is not bot and it has no plugin, external extension nor webinject it's mere browser-keylogger. Plus you're not allow to target unauthorised computer, I never advice you to violate your country's law...

(Feb 12, 2016 06:45 AM)Amerikanski Wrote: [\[CITE\]](#) What do you do when chrome updates the functions to be hooked. Can you hook x64 browsers?

Also what is the lagos method? Can I try your software?

If Chrome update and FormBook hook is patched, all customer will have update for free in less than 24hrs.

X64 browser works with only iexplore, there is no x64 Firefox, I'll add x64 Chrome-Beta if I see it ever getting popular.

Lagos Island is a neat and yet very effective userland rootkit You can learn more about it in some underground forum you can try to search.

Green Goblin - February 12, 2016, 7:57 am

this is pretty cool, if its legit lmao

NTTITONV326 - February 12, 2016, 7:59 am

What about the quic protocol? How are you bypassing Spdy?

RootBite - February 12, 2016, 8:01 am

I would love to review this :p

NTTITONV326 - February 12, 2016, 8:02 am

(Feb 12, 2016 06:39 AM)Shoe Wrote: [\[CITE\]](#) That doesn't matter, how dead they are. What matters is whether or not HF allows formgrabbers to be discussed.

Formgrabber are fine you delinquent

NTTITONV325 - February 12, 2016, 8:12 am

The QUIC Protocol is now in use, read the RFCs. SPDY is redundant, and quite frankly will be discontinued in the future.

How are you handling SPDY?

Amerikanski - February 12, 2016, 8:40 am

(Feb 12, 2016 06:52 AM)ng-Coder Wrote: [\[CITE\]](#) there is no x64 Firefox

Yes there is they are offering it now.

ng-Coder - February 12, 2016, 8:45 am

(Feb 12, 2016 09:12 AM)NTTITONV325 Wrote: [\[CITE\]](#) The QUIC Protocol is now in use, read the RFCs. SPDY is redundant, and quite frankly will be discontinued in the future.

How are you handling SPDY?

QUIC is a UDP version of protocol like SPDY and HTTP/2

Do you know any site that receive form-log through QUIC? I guess no.

Yes SPDY is already deprecated and people have moved to HTTP/2 which is the present industry standard it's not even required and many people won't leave HTTP 1.1 anyway.

I'm not handling SPDY any special, just copy the log from him and let him go.

NTTITONV325 - February 12, 2016, 8:46 am

(Feb 12, 2016 09:45 AM)ng-Coder Wrote: [\[CITE\]](#) QUIC is a UDP version of protocol like SPDY and HTTP/2

Do you know any site that receive form-log through QUIC? I guess no.

Yes SPDY is already deprecated and people have moved to HTTP/2 which is the present industry standard it's not even required and many people won't leave HTTP 1.1 anyway.

I'm not handling SPDY any special, just copy the log from him and let him go.

No, are you disabling SPDY, hooking SPDY or decompressing SPDY packets?

Same thing goes for HTTP/2

ng-Coder - February 12, 2016, 8:48 am

(Feb 12, 2016 08:57 AM)Green Goblin Wrote: [\[CITE\]](#) this is pretty cool, if its legit lmao
Yes it's legit Escrow will be welcome. Factor8

Armada - February 12, 2016, 8:49 am

@OP This honestly looks sick, but yea, form grabbers fall in the disallowed blackhat activity as they are almost always used for financial fraud. I would contact a staff member to clarify this but I am near certain this is the case.

You might need to sell this off site in that event. But on that note, if your still looking for someone to give a review hmu in PM.

ng-Coder - February 12, 2016, 9:01 am

(Feb 12, 2016 09:40 AM)Amerikanski Wrote: [\[CITE\]](#) Yes there is they are offering it now.
? yes I see just in beta version like chrome, haven't compatible with standard plugins, I'll add it before it get to stable. Thx pal.

(Feb 12, 2016 09:46 AM)NTTITONV325 Wrote: [\[CITE\]](#) No, are you disabling SPDY, hooking SPDY or decompressing SPDY packets?

Same thing goes for HTTP/2
I just copy the log from SPDY I say, same thing to HTTP2.?

(Feb 12, 2016 09:49 AM)Armada Wrote: [\[CITE\]](#) @OP This honestly looks sick, but yea, form grabbers fall in the disallowed blackhat activity as they are almost always used for financial fraud. I would contact a staff member to clarify this but I am near certain this is the case.

You might need to sell this off site in that event. But on that note, if your still looking for someone to give a review hmu in PM.

formgrabbers are sold here you can search, this is not bot and it has no plugin, external extension nor webinject it's mere browser-keylogger. Plus you're not allow to target unauthorised computer, I never advice you to violate your country's law...

NTTITONV325 - February 12, 2016, 9:49 am

(Feb 12, 2016 10:01 AM)ng-Coder Wrote: [\[CITE\]](#) ? yes I see just in beta version like chrome, haven't compatible with standard plugins, I'll add it before it get to stable. Thx pal.

I just copy the log from SPDY I say, same thing to HTTP2.?

formgrabbers are sold here you can search, this is not bot and it has no plugin, external extension nor webinject it's mere browser-keylogger. Plus you're not allow to target unauthorised computer, I never advice you to violate your country's law...

How does one just copy the log from spdy? What is this? decompressed SPDY packets going through SSL_WRITE?

Are you lost?

ng-Coder - February 12, 2016, 10:13 am

(Feb 12, 2016 10:49 AM)NTTITONV325 Wrote: [\[CITE\]](#) How does one just copy the log from spdy? What is this? decompressed SPDY packets going through SSL_WRITE?

Are you lost?

?, Ok here is the thing, SPDY body is not yet compressed nor encrypted by the time I copy it only the header is compressed, then I just decompress the header.

And for optimisation I don't even decompress HTTP/2 header because

1. I don't have my own thread, all the hook are just passage, that's how you archive fully thread-safe hook.
2. Host is most of time included in the body content so I don't need to create unnecessary overhead or delay any thread by wasting time decompressing header.

ng-Coder - February 12, 2016, 10:38 am

(Feb 12, 2016 11:25 AM)The Watcher?? Wrote: [\[CITE\]](#) Forgive me but, I feel you're not experienced enough in this area. Spoiler [\(Click to View\)](#)? Lol, revenge ?

Lucifer Morningstar - February 12, 2016, 10:45 am

To be honest I'd just give a review copy to NITTITION whenever he creates a new account.

He's probably one of the most experienced people in this section when it comes to formgrabbers. ?

NTTITONV327 - February 12, 2016, 11:18 am

(Feb 12, 2016 11:13 AM)ng-Coder Wrote: [\[CITE\]](#) ?, Ok here is the thing, SPDY body is not yet compressed nor encrypted by the time I copy it only the header is compressed, then I just decompress the header.

And for optimisation I don't even decompress HTTP/2 header because

1. I don't have my own thread, all the hook are just passage, that's how you archive fully thread-safe hook.
 2. Host is most of time included in the body content so I don't need to create unnecessary overhead or delay any thread by wasting time decompressing header.
- then I just decompress the header.

that's the answer i was looking for.

And for optimisation I don't even decompress HTTP/2 header because

1. I don't have my own thread, all the hook are just passage, that's how you archive fully thread-safe hook.
2. Host is most of time included in the body content so I don't need to create unnecessary overhead or delay any thread by wasting time decompressing header.

Correct.

And to clarify, what functions are you hooking? For Firefox and Chrome.

When I wrote my formgrabber, I hooked Sslwrite I believe, and Spdy related functions. I used the symbol server to find them, same goes along with http/2

Amerikanski - February 12, 2016, 8:00 pm

(Feb 12, 2016 12:18 PM)NTTITONV327 Wrote: [\[CITE\]](#) then I just decompress the header.

that's the answer i was looking for.

And for optimisation I don't even decompress HTTP/2 header because

1. I don't have my own thread, all the hook are just passage, that's how you archive fully

thread-safe hook.

2. Host is most of time included in the body content so I don't need to create unnecessary overhead or delay any thread by wasting time decompressing header.

Correct.

And to clarify, what functions are you hooking? For Firefox and Chrome.

When I wrote my formgrabber, I hooked Sslwrite I believe, and Spdy related functions. I used the symbol server to find them, same goes along with http/2
chrome doesn't use ssl_write anymore they use ssl_write_app and if you need webinjects too
ssl_read_app

ng-Coder - February 13, 2016, 2:19 am

(Feb 12, 2016 09:00 PM)Amerikanski Wrote: [\[CITE\]](#) chrome doesn't use ssl_write anymore they use ssl_write_app and if you need webinjects too ssl_read_app
yes it's now ssl_write_app, no webinject plz this has nothing like that..

(Feb 12, 2016 12:18 PM)NTTITONV327 Wrote: [\[CITE\]](#) And to clarify, what functions are you hooking? For Firefox and Chrome.

When I wrote my formgrabber, I hooked Sslwrite I believe, and Spdy related functions. I used the symbol server to find them, same goes along with http/2

I can only say it hook the post functions, I won't be analyzing the hook process because I think it's not public.

NTTITONV330 - February 13, 2016, 12:49 pm

(Feb 13, 2016 03:19 AM)ng-Coder Wrote: [\[CITE\]](#) yes it's now ssl_write_app, no webinject plz this has nothing like that..

I can only say it hook the post functions, I won't be analyzing the hook process because I think it's not public.

The symbol servers are public. It's pretty much public.

ng-Coder - February 13, 2016, 1:05 pm

(Feb 13, 2016 01:49 PM)NTTITONV330 Wrote: [\[CITE\]](#) The symbol servers are public. It's pretty much public. You can see more about it here: <https://hackforums.net/showthread.php?tid=5168562>

Armada - February 13, 2016, 1:21 pm

OP PMed me with the offer, Sadly I am just too damn busy this weekend to give it a whirl and test. ?

I was actually really looking forward to the opportunity. If our still looking for someone I might be available Monday bro. Otherwise I look forward to the review(s) ?

Zettabit - February 13, 2016, 4:19 pm

If you're still looking for somebody to test, I have a domain and hosting in which I can test this for you. I also know exactly what sites to test this on.

micdonand - February 17, 2016, 3:49 pm

(Feb 12, 2016 06:06 AM)Shoe Wrote: [\[CITE\]](#) FormGrabbers aren't allowed, I do believe. I could be

wrong but last time I heard they aren't allowed.
It is allowed I think, as long it's not bot

KardoseR - February 17, 2016, 4:43 pm

why in every fucking thread that contains the word formgrabber the "wannabe moderator" members go haywire full retard HURR I THINK FORMGRABBERS ARENT ALLOWED ON HF HURRR, and then 10 more people say the same thing and im yet to see the admin say anything about this, cmon stop being retarded, if you classify formgrabbers as banking/carding then you must aswell ban keyloggers you retards. stop trying to sound smart like you know the rules of this skid forum

Thomaz000 - February 29, 2016, 3:59 am

Is this still in development? I don't see what the problem is myself. I'm not happy with the keyloggers or smart keyloggers that are available on the market. I just want to get general details but I find keyloggers inneficient at this. I'm not interested in getting fininancial blackhat stuff but just something more efficient than the current keyloggers

ng-Coder - February 29, 2016, 4:28 am

(Feb 29, 2016 04:59 AM)thomaz000 Wrote: [\[CITE\]](#) Is this still in development? I don't see what the problem is myself. I'm not happy with the keyloggers or smart keyloggers that are available on the market. I just want to get general details but I find keyloggers inneficient at this. I'm not interested in getting fininancial blackhat stuff but just something more efficient than the current keyloggers
<https://hackforums.net/showthread.php?tid=5168562>

limb3r - March 11, 2016, 1:09 am

Where are the reviews? C'mon guys.

NotRandom - March 11, 2016, 3:03 am

Never mind found my answer

ng-Coder - March 14, 2016, 10:33 am

(Mar 11, 2016 02:09 AM)limb3r Wrote: [\[CITE\]](#) Where are the reviews? C'mon guys.
<https://hackforums.net/showthread.php?tid=5200139>

push rdx - March 14, 2016, 10:48 am

I'll review it, pm me the bin.

?Syria - March 14, 2016, 10:50 am

(Mar 14, 2016 10:48 AM)push rdx Wrote: [\[CITE\]](#) I'll review it, pm me the bin.
You are a comedian

push rdx - March 14, 2016, 11:29 am

(Mar 14, 2016 10:50 AM)?Syria Wrote: [\[CITE\]](#) You are a comedian
And you're an idiot.

?Syria - March 14, 2016, 11:49 am

(Mar 14, 2016 11:29 AM)push rdx Wrote: [\[CITE\]](#) And you're an idiot.
How am i an idiot? explain

push rdx - March 14, 2016, 4:01 pm

(Mar 14, 2016 11:49 AM)?Syria Wrote: [\[CITE\]](#) How am i an idiot? explain
You're basing user knowledge and integrity on post count , join date and reputation.

Might as well start basing off skin color as well.

retard.

?Syria - March 14, 2016, 4:17 pm

(Mar 14, 2016 04:01 PM)push rdx Wrote: [\[CITE\]](#) You're basing user knowledge and integrity on post count , join date and reputation.

Might as well start basing off skin color as well.

retard.

Not that moron, im saying no one is gonna trust a new member

RISC - March 14, 2016, 8:08 pm

(Mar 14, 2016 04:17 PM)?Syria Wrote: [\[CITE\]](#) Not that moron, im saying no one is gonna trust a new member

That "new" member has more knowledge on malware development than this entire forum's knowledge combined. You really are retarded.

?Syria - March 14, 2016, 8:59 pm

(Mar 14, 2016 08:08 PM)RISC Wrote: [\[CITE\]](#) That "new" member has more knowledge on malware development than this entire forum's knowledge combined. You really are retarded.

NO ONE CARES! Hes not trusted

ng-Coder - March 15, 2016, 12:02 am

(Mar 14, 2016 08:08 PM)RISC Wrote: [\[CITE\]](#) That "new" member has more knowledge on malware development than this entire forum's knowledge combined. You really are retarded.

?

push rdx - March 15, 2016, 12:16 am

(Mar 15, 2016 12:02 AM)ng-Coder Wrote: [\[CITE\]](#) ?

"Oh hai there I use words like balloon executable to make myself look like a knowledgable coder when in reality it's independant position code that raises false positives due to merged sections"

Great idea

ng-Coder - March 15, 2016, 12:24 am

(Mar 15, 2016 12:16 AM)push rdx Wrote: [\[CITE\]](#) Am I going to get this bin.. Or is your skid ass going to keep stalling?

How will I give bin to you kid? you know I know you and you understand this isn't in the level of your skidded C code.

(Mar 15, 2016 12:16 AM)push rdx Wrote: [\[CITE\]](#) "Oh hai there I use words like balloon executable to make myself look like a knowledgable coder when in reality it's independant position code that raises false positives due to merged sections"

Great idea

Lol, team duqu! here you are with your 0 knowledge about lots of things you talking about, FormBook is real balloon nothing is packed, merged nor encrypted yet good luck for skid buddy like you in cracking it.

kid why don't you just leave this forum for good!

push rdx - March 15, 2016, 12:45 am

(Mar 15, 2016 12:24 AM)ng-Coder Wrote: [\[CITE\]](#) How will I give bin to you kid? you know I know you and you understand this isn't in the level of your skidded C code.

Lol, team duqu! here you are with your 0 knowledge about lots of things you talking about, FormBook is real balloon nothing is packed, merged nor encrypted yet good luck for skid buddy like you in cracking it.

kid why don't you just leave this forum for good! Oh yes, hips will never suspect anything...

ng-Coder - March 15, 2016, 1:17 am

(Mar 15, 2016 12:45 AM)push rdx Wrote: [\[CITE\]](#) Oh yes, hips will never suspect anything... There are varieties of HIPS, just as there are varieties of Firewall most that I know of are bypassed.

logan.john - November 22, 2017, 3:21 am

pls i will like to buy 1mth license for this formbook contact me via skype elvisborrow80 or boitest.ua@gmail.com

slyraptor - November 23, 2017, 1:06 am

good product bro. seemss to be a very stable botnet. although am yet to try it but based on the feature sets , it asm/c so crypting it will require native crypter

Spearhead - November 26, 2017, 11:41 am

Excellent product from a very experienced code. Please PM me your skype I would like to purchase this?

macspeed - June 6, 2018, 2:17 pm

get back to me if you have working form grabber, that is active or where to buy

sahil131 - July 26, 2018, 9:07 am

Are you reselling formbook? let me know how you do it

Njord - July 26, 2018, 9:37 am

id love a vouch copy bro :P

Jack? - July 26, 2018, 10:21 am

(Jul 26, 2018 09:37 AM)Njord Wrote: [\[CITE\]](#) id love a vouch copy bro :P thread is 2 years old

Njord - July 26, 2018, 10:22 am

(Jul 26, 2018 10:21 AM)Jack? Wrote: [\[CITE\]](#) thread is 2 years old oh well rip

Sirhofiio - July 26, 2018, 4:47 pm

ive had 1k bots on this shit once ata a time they stop typing anything even when they active on real pc

sherbet - July 28, 2018, 4:34 pm

Is this still in development? lmk

int - July 28, 2018, 7:47 pm

(Jul 28, 2018 04:34 PM)sherbet Wrote: [\[CITE\]](#) Is this still in development? lmk

No you retard its a 2 year old thread

keemodas - July 29, 2018, 12:52 pm

Does formbook still work?i know is over 2 years now...

kisore1 - September 19, 2018, 1:52 am

Ng.coder is a ripper, please beware and don't buy anything from him, i was ripped few days ago for formbook. For all those vouching for him, you are responsible too for his actions, Admin you equally must take part of the blame for allowing post and comments from confirmed rippers still standing on the forum. please do something about this, it is destroying the credibility of this forum.

NOTE: Skype: Ng.Coder is a RIPPER!!!!!! don't buy anything from him

LordDragon - September 19, 2018, 2:01 am

(Sep 19, 2018 01:52 AM)kisore1 Wrote: [\[CITE\]](#) Ng.coder is a ripper, please beware and don't buy anything from him, i was ripped few days ago for formbook. For all those vouching for him, you are responsible too for his actions, Admin you equally must take part of the blame for allowing post and comments from confirmed rippers still standing on the forum. please do something about this, it is destroying the credibility of this forum.

NOTE: Skype: Ng.Coder is a RIPPER!!!!!! don't buy anything from him

Wow is my only comment for now.

z3ro-cool - September 19, 2018, 4:25 am

(Sep 19, 2018 02:01 AM)LordDragon Wrote: [\[CITE\]](#) Wow is my only comment for now.
why ? this guy has been scammed by IMPOSTER because he is dumbass.

LordDragon - September 19, 2018, 5:57 am

(Sep 19, 2018 04:25 AM)z3ro-cool Wrote: [\[CITE\]](#) why ? this guy has been scammed by IMPOSTER because he is dumbass.

Why I said "wow" is that I added him months ago and we discussed about his product.

guccifer30 - September 19, 2018, 7:31 am

I heard that formbook is only being sold privately? Can someone confirm ?

Polymorphin - September 19, 2018, 8:53 am

Do you still need some beta testers? to test it

YAK_CODER - September 19, 2018, 9:22 am

(Sep 19, 2018 07:31 AM)guccifer30 Wrote: [\[CITE\]](#) I heard that formbook is only being sold privately? Can someone confirm ?I Test form book formgrabber many times when i was working on my crypter what i can say

- 1- This guy is very friendly have alot skills that appear on his work
- 2- Very stable malware better than anything you have test before
- 3-Native with no Dependency at all
- 4- To buy pm him for icq or skype

YaKuza Usq Crypter

<https://hackforums.net/showthread.php?tid=5861395>

guccifer30 - September 19, 2018, 9:26 am

(Sep 19, 2018 09:22 AM)crypt4u Wrote: [\[CITE\]](#) I Test form book formgrabber many times when i was working on my crypter

what i can say

- 1- This guy is very friendly have alot skills that appear on his work
- 2- Very stable malware better than anything you have test before

3-Native with no Dependency at all

4- To buy pm him for icq or skype

YaKuza Usg Crypter

I know, i used it in the past, i just lost my domain. Im trying to contact ng-coder again but so far i get in touch only with dumb scammers.

YAK_CODER - September 19, 2018, 9:34 am

(Sep 19, 2018 09:26 AM)guccifer30 Wrote: [\[CITE\]](#) I know, i used it in the past, i just lost my domain. Im trying to contact ng-coder again but so far i get in touch only with dumb scammers.will pm you his icq

3DES - September 19, 2018, 10:48 am

(Sep 19, 2018 08:53 AM)Polymorphin Wrote: [\[CITE\]](#) Do you still need some beta testers? to test it
Dude how fucking late can you be?

keemodas - September 20, 2018, 4:48 am

We don't even know what to believe if FB project is still selling or not some people say selling some say its a scam...

paki12 - November 29, 2018, 3:37 am

Hi ngcoder i want this can you please tell me how to buy this