

Forum:[Hack Forums](#)

Thread: [Development Thread | RustLoader | Advanced and Modern HTTP Loader | Rust](#)

NotKover - June 22, 2022, 6:46 pm

This is a thread to show the progress of the loader i soon plan to sell here on HF, if you have any suggestions or requests of what i should add please send them here

The current functionality it has right now are:

A:Loader

- 1.Drop in WD exclusions folder and run
- 2.Drop in non WD exclusions folder and run

B:Update

C:Startup and persistance

D:UAC exploit

- 1.Adds install paths to WD exclusion & WD exclusions drop folder
- 2.Restarts loader with admin(either on startup or after exploit is ran)

E:Very basic botkiller(wont release till deemed ready aka when its the best killer ik of)

F:Communications over HTTP

Super - June 22, 2022, 7:22 pm

Seems really cool, but I have a couple questions about it.

What does WD exclusions folder mean?

Also, does the UAC bypass work on the latest version of Windows 11, or is it targeting outdated systems?

NotKover - June 22, 2022, 7:39 pm

(Jun 22, 2022 07:22 PM)Super Wrote: [\[CITE\]](#) Seems really cool, but I have a couple questions about it.

What does WD exclusions folder mean?

Also, does the UAC bypass work on the latest version of Windows 11, or is it targeting outdated systems?

WD exclusions folder is a windows defender exclusions folder where windows defender and a alright handful of other AVs will not scan the selected locations, and my UAC exploit i use works on the newest version of w10 and w11 with nearly every AV, i can send some runtime scans using my uac exploit

Scans using the exploit:

<https://checkzilla.io/scan/2319e9a3-69cc-4f28-85aa-c8b692e8e7ef>

<https://checkzilla.io/scan/8b34995d-11f2-41bd-831d-6bf1af453f26>

(Some major changes have happened between those scans with my dropper)

Also when this is ready for sale ill probably move over to one of my better exploits i have saved away to ensure the best results

Super - June 22, 2022, 8:31 pm

(Jun 22, 2022 07:39 PM)NotKover Wrote: [\[CITE\]](#) WD exclusions folder is a windows defender exclusions folder where windows defender and a alright handful of other AVs will not scan the

selected locations, and my UAC exploit i use works on the newest version of w10 and w11 with nearly every AV, i can send some runtime scans using my uac exploit

Scans using the exploit:

<https://checkzilla.io/scan/2319e9a3-69cc-4f28-85aa-c8b692e8e7ef>

<https://checkzilla.io/scan/8b34995d-11f2-41bd-831d-6bf1af453f26>

(Some major changes have happened between those scans with my dropper)

Also when this is ready for sale ill probably move over to one of my better exploits i have saved away to ensure the best results

That's amazing you have a working UAC exploit, most of the ones I know about have gotten patched by now.

Seems like it will be a good product, GLWS.

NotKover - June 22, 2022, 8:36 pm

(Jun 22, 2022 08:31 PM)Super Wrote: [\[CITE\]](#) That's amazing you have a working UAC exploit, most of the ones I know about have gotten patched by now.

Seems like it will be a good product, GLWS.

Thank you very much, if you have any suggestions please let me know because i dont really know what i should and shouldnt add

TheGate - June 23, 2022, 12:36 am

Are you going to give any vouchies for this?

NotKover - June 23, 2022, 1:14 am

(Jun 23, 2022 12:36 AM)TheGate Wrote: [\[CITE\]](#) Are you going to give any vouchies for this? once i think its ready maybe, mainly depends on how well it turns out

__Digital__ - June 23, 2022, 7:55 am

Good luck with your project, i understand why people are using rust. Because it remains fud longer due to avs not caught with it yet. It just reminds me of the good old autoit binary. but with rust they are 10mb easy. As i said good luck with your project hope it is very successful.

NotKover - June 23, 2022, 10:24 am

(Jun 23, 2022 07:55 AM)__Digital__ Wrote: [\[CITE\]](#) Good luck with your project, i understand why people are using rust. Because it remains fud longer due to avs not caught with it yet. It just reminds me of the good old autoit binary. but with rust they are 10mb easy. As i said good luck with your project hope it is very successful.

My current binary is only 800KB and has a good handful of functions but once im done the size will probably be like 4MB~ if not more

(Jun 23, 2022 09:58 AM)Dyne Wrote: [\[CITE\]](#) I would love to see how this fares up against HP Wolf Security with dynamic detection. Businesses, banks in the western world have been transitioning workstations to HP infrastructure and subscribing to their dynamic detection modules. Which has proven to be quite good.

A simple subscription costs a proof of business, consultation and about \$5k USD/year for a company.

Not to be confused with HP Wolf Essential Security for home/business use included in newer desktops for free.

The past few months I have been researching this myself and confess myself impressed. Even with

heavily encrypted remote malware (consistent connection) bypassing ZoneAlarm runtime.

Once its ready we can do some testing with it and see, i was thinking about how it would handle to enterprise AVs so we can find out later

Xzedin - June 23, 2022, 7:10 pm

As long as you have the basics down then start adding the sought after functions. So far so good. Seen your posts graduate to a higher level in this forum.

AnonTri - June 23, 2022, 7:54 pm

(Jun 22, 2022 08:36 PM)NotKover Wrote: [\[CITE\]](#) Thank you very much, if you have any suggestions please let me know because i dont really know what i should and shouldnt add

If it does not already it should allow for loading both exe and dll from disk and memory as well as having multiple fallback c2 servers if not giving it a DGA. Though if it does have DGA please allow for fallback c2 to prevent sinkholing. Other than that good persistence and a stable/secure connection will be your biggest selling points for a loader. Anything that makes it more resilient or more likely to last is worth more than any specific features (in terms of logging or proxies or anything not directly related to a loader)

NotKover - June 23, 2022, 9:09 pm

(Jun 23, 2022 07:54 PM)AnonTri Wrote: [\[CITE\]](#) If it does not already it should allow for loading both exe and dll from disk and memory as well as having multiple fallback c2 servers if not giving it a DGA. Though if it does have DGA please allow for fallback c2 to prevent sinkholing. Other than that good persistence and a stable/secure connection will be your biggest selling points for a loader. Anything that makes it more resilient or more likely to last is worth more than any specific features (in terms of logging or proxies or anything not directly related to a loader)

These are planned and i have a good handful of "unique" startup and persistence methods i will implement and test to make sure they dont add any detection vectors but it will be awhile before then

wyvn - June 24, 2022, 9:02 am

how long have you been coding in Rust for and how effective would you say it is to learn for malware development?

I'm currently looking into learning C++ or C, but Rust seems interesting to me also, I'll be learning from the start so i'd rather get locked in to one, which would you recommend?

NotKover - June 24, 2022, 10:26 am

(Jun 24, 2022 09:02 AM)0xj4y Wrote: [\[CITE\]](#) how effective would you say it is to learn for malware development?It can be very effective but is hard to learn from since there isnt like any examples on any already

(Jun 24, 2022 09:02 AM)0xj4y Wrote: [\[CITE\]](#) I'm currently looking into learning C++ or C, but Rust seems interesting to me also, I'll be learning from the start so i'd rather get locked in to one, which would you recommend?personally i would go for rust but i would learn c++ or rust

NotKover - June 26, 2022, 12:56 am

Little update,

I have been working on a rootkit in rust and have a fully ready and functional userland rootkit and will soon try to work on a kernel level rootkit but will need to do further research into finding a driver to load said kit and wont cause a major detection vector

I have also started to work on a AMSI bypass that is not dependent on powershell and will hopefully have it prepared in the next coming days

If you have any suggestions or requests or questions, feel free to comment here to message me via PM/convo or telegram @NotKover

The current binary size is 1.94MB and i will work to reduce the size, i will soon be implementing more complicated functions to then do extensive testing to ensure there is no detection vectors by any of my methods, if you have any suggestions or request, please let me know

Romanus - June 27, 2022, 12:13 am

this is looking very promising, a new loader would definitely be appreciated in the community. talking with kover seperately about more specific details about the loader really has me thinking we've got something promising here, specifically the bot killer here is what's very interesting to me. wont get too much into it here though, as all this will surely be discussed more as kover unravels his product here.

looking forward to future updates & subscribing to this thread.

Best Regards,
~Roma

NotKover - June 27, 2022, 12:16 am

(Jun 27, 2022 12:13 AM)Romanus Wrote: [\[CITE\]](#) this is looking very promising, a new loader would definitely be appreciated in the community. talking with kover seperately about more specific details about the loader really has me thinking we've got something promising here, specifically the bot killer here is what's very interesting to me. wont get too much into it here though, as all this will surely be discussed more as kover unravels his product here.

looking forward to future updates & subscribing to this thread.

Best Regards,
~Roma

Thank you, if you have any suggestions, please tell me because i am going all out on this project and i want to try to make it as useful as possible and feature rich without any detection vectors

Another little update, the new binary size is now 244KB after major optimizations and cleaning code

DI?E - June 27, 2022, 5:16 pm

(Jun 23, 2022 07:10 PM)Xzedin Wrote: [\[CITE\]](#) As long as you have the basics down then start adding the sought after functions. So far so good. Seen your posts graduate to a higher level in this forum.

This most definitely needs to be implemented.

NotKover - June 27, 2022, 6:20 pm

(Jun 27, 2022 05:16 PM)DI?E Wrote: [\[CITE\]](#) This most definitely needs to be implemented. The base of the botnet is finished(comms, basic tasks etc and persistence) but i will be adding more methods of startup and persistance that are uncommon etc and later today or tomorrow i will start implementing other functions and then start working on the php panel

Carve - June 28, 2022, 9:16 am

Very interesting little project you have going. Will it only have HTTP or will you have a fallback c2c? Need any help with a nice web interface?

NotKover - June 28, 2022, 3:41 pm

(Jun 28, 2022 09:16 AM)Carve Wrote: [\[CITE\]](#) Very interesting little project you have going. Will it only have HTTP or will you have a fallback c2c? Need any help with a nice web interface? it will have fall over domains in case one gets suspended etc

bananaj Juice - June 29, 2022, 4:59 am

It's very interesting and I see that you are already selling a dropper also developed in Rust. Seems that is a good choice.

Can you tell me what the differences are between the loader and the dropper?

Thanks @NotKover

AnonTri - June 29, 2022, 4:53 pm

(Jun 29, 2022 04:59 AM)bananaj Juice Wrote: [\[CITE\]](#) It's very interesting and I see that you are already selling a dropper also developed in Rust. Seems that is a good choice.

Can you tell me what the differences are between the loader and the dropper?

Thanks @NotKover

The loader is a piece of malware that allows you to create a botnet and allows remote access to computers, the dropper just downloads/drops and executes your malware/payload on a victim so you don't send the actual malware for it to get caught/detected as easily.

Kover can ofc add on if his are different but those will be the basic answers

NotKover - June 29, 2022, 5:46 pm

(Jun 29, 2022 04:53 PM)AnonTri Wrote: [\[CITE\]](#) The loader is a piece of malware that allows you to create a botnet and allows remote access to computers, the dropper just downloads/drops and executes your malware/payload on a victim so you don't send the actual malware for it to get caught/detected as easily.

Kover can ofc add on if his are different but those will be the basic answers

this is a perfect answer, some people get confused between dropper and loader because some languages translate loader to dropper etc but yes your answer is correct

Mutant - July 3, 2022, 2:06 pm

Can't wait to see it! Would love to know an ETA on this. I've been looking for a new loader to implement as everything I have touched is anything but FUD, regardless of what crypt I use.

NotKover - July 3, 2022, 4:25 pm

(Jul 3, 2022 02:06 PM)Mutant Wrote: [\[CITE\]](#) Can't wait to see it! Would love to know an ETA on this. I've been looking for a new loader to implement as everything I have touched is anything but FUD, regardless of what crypt I use.

it will be a few weeks before anything since i will be doing a lot of tests to make sure nothing ads a detection vector thats to grate to risk etc

Sicario P - July 9, 2022, 8:25 pm

I would like to see this working

NotKover - July 10, 2022, 6:35 am

(Jul 9, 2022 08:25 PM)Sicario P Wrote: [\[CITE\]](#) I would like to see this working

It is currently functional but is being tested greatly right now

DI?E - July 11, 2022, 3:46 pm

(Jul 10, 2022 06:35 AM)NotKover Wrote: [\[CITE\]](#) It is currently functional but is being tested greatly

right now
IF you need help let me know.

NotKover - July 11, 2022, 4:19 pm

(Jul 11, 2022 03:46 PM)DI?E Wrote: [\[CITE\]](#) IF you need help let me know.
Send me a message and we can talk about it

nulluser123 - July 13, 2022, 1:04 pm

(Jun 23, 2022 07:55 AM)___Digital___ Wrote: [\[CITE\]](#) Good luck with your project, i understand why people are using rust. Because it remains fud longer due to avs not caught with it yet. It just reminds me of the good old autoit binary. but with rust they are 10mb easy. As i said good luck with your project hope it is very successful.

What? The rust compiler uses LLVM, exactly like C and C++ (on clang). It doesn't matter that it is written in Rust, they all compile through LLVM to similar output lmao.

To OP: how does the loader bypass firewall solutions? If the runtime of the loader is good - I could be interested.

NotKover - July 15, 2022, 7:31 pm

Update: I am currently working on a "recovery" system for a addon to the loader, if anyone has suggestions please let me know and i will consider them

Mutant - July 15, 2022, 7:41 pm

(Jul 15, 2022 07:31 PM)NotKover Wrote: [\[CITE\]](#) Update: I am currently working on a "recovery" system for a addon to the loader, if anyone has suggestions please let me know and i will consider them

Idk if it's allowed here but I'm sure it would be widely popular if your recovery system could detect trezor suite downloaded on the computer as well as Ledger.

NotKover - July 24, 2022, 11:42 am

A small update on the loader, i am currently cleaning up the code to attempt to make some of the module addon sizes smaller, currently with all modules added the file size is 4.1MB and my goal will to get the file size down to around 2MB or less

If anyone has any suggestions or requests of functions to be added please let me know here or through HF messages or telegram @NotKover

As per request i will be adding a shellcode loader to it if there is anything else feel free to contact me

Practise - July 26, 2022, 6:35 am

Can you program a loader for Android?

NotKover - July 26, 2022, 7:22 am

(Jul 26, 2022 06:35 AM)Practise Wrote: [\[CITE\]](#) Can you program a loader for Android?
Maybe after im done with this i can look into one fpr android

Practise - July 26, 2022, 7:33 am

(Jul 26, 2022 07:22 AM)NotKover Wrote: [\[CITE\]](#) Maybe after im done with this i can look into one fpr android

Really?!? You are a High Quality Member!!!!

Ph4n70M Phr34K - July 31, 2022, 1:37 pm

how its going my friend ?

NotKover - August 1, 2022, 1:04 am

(Jul 31, 2022 01:37 PM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) how its going my friend ?

Going good, my ISP has been having issues and just came back online for the first time in nearly 4-5 days nice

(Jul 31, 2022 02:09 PM)Incog Wrote: [\[CITE\]](#) Hi, I'm writing a reply for Kover as he asked me to check for any new posts on certain threads and reply back with what he says ?

He said it's going good, but his ISP is having issues so he can't access HF atm

Thank you for checking up for me, im happy the internet is back and i am going to continue this project

NotKover - August 18, 2022, 4:04 pm

Doing a little update, i was away from my PC since the 9th~ and was not able to do any work after then but before hand i rewrote my runpe since it was being buggy but seems to be working efficiently now and i have not seen any bugs with it anymore, i also improved the shellcode loader and reduced its weight by 600kb making its current weight 300kb, i plan to release in the next few days but i am unsure if i will feel it ready by then

If you have any function suggestions please post here or pm/convo me or message me on telegram @NotKover

trojohn - August 24, 2022, 4:40 pm

Sounds very interesting. Good luck with the release.

NotKover - August 25, 2022, 12:32 pm

(Aug 24, 2022 03:09 PM)shatter Wrote: [\[CITE\]](#) Can you explain to me what the UAC bypass does? Is it an exploit, PoC, or just a misconfiguration? I've been following this thread for a hot minute now and have now finally decided to make a post in regards to the project.

I PMed you about it and if you have more questions feel free to ask

(Aug 24, 2022 04:40 PM)trojohn Wrote: [\[CITE\]](#) Sounds very interesting. Good luck with the release. Thanks man, im going to try to release soon but ive been running into a good amount of errors

A little update, Im having a little bit of issues with the RunPE i made and am probably going to delay the release of the run in memory function but i will have run from disk but i will add it as soon as i fix the bugs

NotKover - September 3, 2022, 1:37 pm

Small update, the first loader version is ready and is in final testing before sales will be open

NotKover - September 3, 2022, 10:28 pm

(Sep 3, 2022 06:32 PM)Dyne Wrote: [\[CITE\]](#) Just a minor update. indeed but its also big since yk sales are going to be opened up

LeadPal - September 4, 2022, 10:43 am

So excited to see how this will turn out, posting to keep an eye on this

SIM-23882 - September 7, 2022, 9:12 am

Hey there, is there a price on this yet ? Thanks

NotKover - September 8, 2022, 1:07 pm

(Sep 7, 2022 09:12 AM)Cbuts05 Wrote: [\[CITE\]](#) Hey there, is there a price on this yet ? Thanks
For the first variant, i would probably charge around \$200-\$300 since the bot isn't finished but the customers would get rebuilds of updates etc till the final version of the bot is done

SIM-23882 - September 8, 2022, 1:12 pm

(Sep 8, 2022 01:07 PM)NotKover Wrote: [\[CITE\]](#) For the first variant, i would probably charge around \$200-\$300 since the bot isn't finished but the customers would get rebuilds of updates etc till the final version of the bot is done

Thanks for the info, keep up the good work

burer - September 27, 2022, 1:15 pm

CnC is just HTTP panel? Is there a recovery mechanism in case panel is busted?

3127707 - September 27, 2022, 1:27 pm

Hello, please contact me @rat_999, I need your help. I hope to cooperate with you. I am an Internet enthusiast in China

NotKover - October 1, 2022, 6:55 pm

(Sep 27, 2022 01:15 PM)burer Wrote: [\[CITE\]](#) CnC is just HTTP panel? Is there a recovery mechanism in case panel is busted?

The cnc and communications are over http(s) and yes, you can have up to 3 domains per build of it to reduce the chances of the botnet being lost

(Sep 27, 2022 01:27 PM)3127707 Wrote: [\[CITE\]](#) Hello, please contact me @rat_999, I need your help. I hope to cooperate with you. I am an Internet enthusiast in China
replied.

NZT48 - October 3, 2022, 1:21 am

Hello,

Do bots communicate over the TOR network?

NotKover - October 4, 2022, 6:57 pm

(Oct 3, 2022 01:21 AM)NZT48 Wrote: [\[CITE\]](#) Hello,

Do bots communicate over the TOR network?

The botnet will communicate via http over clear net

Stanley - November 2, 2022, 2:53 pm

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley

NotKover - November 2, 2022, 2:55 pm

A happy and sad update, a user has contacted me via telegram 1.5h ago and purchased the source code of my loader and has requested i no longer sell/use it so i will be stopping development on it and will start from scratch on a new loader on c++ i will not be selling source code to since i am no

longer in need of a large sum of money, i am sorry for any inconvenience of users who wanted to purchase builds of it.