

Forum:[Hack Forums](#)

Thread: [Eagle Monitor RAT Updates](#)

arsium - November 13, 2022, 12:08 pm

Hello all,

As you probably saw, I closed the old thread concerning Eagle. All updates and changelogs will be posted here !

And here is the changelog for new version (3-2.3.0) !

[New][Client] Patch AMSI
[New][Client] Patch ETW
[New][Client] Randomize PE from PEB
[New][Client] Anti-Debug
[Tweaks] Added 'Optimize' attribute for csc compiler
[New] Added Remote CMD
[New] Added Remote Powershell
[Fix] BSOD was not working (wrong status code)
[Fix] Null reference with keylogger socket

Release & Code for 3-2.3.0 : [GitHub](#)

Pictures :

drpc1070 - November 13, 2022, 2:23 pm

nice working bro keep good work , i would let you know i try it but its crash so match hope fix it soon and i would chat with you if you dont mind

arsium - November 13, 2022, 11:57 pm

(Nov 13, 2022 03:23 PM)drpc1070 Wrote: [\[CITE\]](#) nice working bro keep good work , i would let you know i try it but its crash so match hope fix it soon
and i would chat with you if you dont mind
When does it crash ? I've tested in vm and got no prob

arsium - November 14, 2022, 7:08 am

(Nov 14, 2022 05:27 AM)Dyne Wrote: [\[CITE\]](#) Congratulations.

RAT tested on VPS Server 2019 and connecting local and external. Nothing is broken and it looks great. Reminds me very much of parallax.

Please consider adding .reloc table to the stub. It will make it much easier for encryption providers to work with you in the future.

If you consider releasing your own tool in the future, please reach out for help with a marketing plan.

Thx !

Yes here I'm learning quite much stuff with PE and here I'm trying to figure out how to work with relocations

If you have some advices, pdfs, books or resources to name I'll be happy :)

Also curious about improving Eagle :

Do you think it's interesting to implement RSA-2048/4096 with AES for communication or only AES is good for you ?

Applet - November 15, 2022, 5:27 am

thanks for the free release.

Sir what is "Patch ETW"

Royal ! - November 15, 2022, 6:00 am

Goodluck with your Project mate, sounds nice.

arsium - November 15, 2022, 9:01 am

(Nov 15, 2022 06:27 AM)Applet Wrote: [\[CITE\]](#) thanks for the free release.

Sir what is "Patch ETW"

Event Tracing for windows.

To know more about it : [IredTeams](#)

Applet - November 15, 2022, 9:56 am

(Nov 15, 2022 10:01 AM)arsium Wrote: [\[CITE\]](#) Event Tracing for windows.

To know more about it : [IredTeams](#)

Went through the link, Its interesting.

Sorry for noob question but does it help bypass detection?

arsium - November 15, 2022, 1:16 pm

(Nov 15, 2022 10:56 AM)Applet Wrote: [\[CITE\]](#) Went through the link, Its interesting.

Sorry for noob question but does it help bypass detection?

Not for bypassing here more for 'anti-debug' if you want

Warune79 - November 15, 2022, 4:15 pm

Great News! Verry HQ work..

naxster - November 16, 2022, 3:11 am

Nice release!!

Out of curiosity, when using the "File Manager" is it possible to download a folder that contains files?

arsium - November 16, 2022, 4:15 am

(Nov 16, 2022 04:11 AM)naxster Wrote: [\[CITE\]](#) Nice release!!

Out of curiosity, when using the "File Manager" is it possible to download a folder that contains files?

Thx !

Nope but I could add it (even I've never seen that)

CrypterHQ - November 18, 2022, 6:00 am

(Nov 13, 2022 01:08 PM)arsium Wrote: [\[CITE\]](#) Hello all,

As you probably saw, I closed the old thread concerning Eagle. All updates and changelogs will be posted here !

And here is the changelog for new version (3-2.3.0) !

[New][Client] Patch AMSI
[New][Client] Patch ETW
[New][Client] Randomize PE from PEB
[New][Client] Anti-Debug
[Tweaks] Added 'Optimize' attribute for csc compiler
[New] Added Remote CMD
[New] Added Remote Powershell
[Fix] BSOD was not working (wrong status code)
[Fix] Null reference with keylogger socket

Release & Code for 3-2.3.0 : [GitHub](#)

Pictures :

Thank you for the good work you doing for the community. Can your RAT hold up to 2-5k connection

arsium - November 18, 2022, 8:04 am

(Nov 18, 2022 07:00 AM)CrypterHQ Wrote: [\[CITE\]](#) Thank you for the good work you doing for the community. Can your RAT hold up to 2-5k connection

I really did not test

Max I've tested is 100-200 client while using simultaneous commands

CrypterHQ - November 18, 2022, 8:44 am

(Nov 18, 2022 09:04 AM)arsium Wrote: [\[CITE\]](#) I really did not test

Max I've tested is 100-200 client while using simultaneous commands

Thanks for the update, but it should hold 20-500 connection perfectly?

arsium - November 18, 2022, 8:47 am

(Nov 18, 2022 09:44 AM)CrypterHQ Wrote: [\[CITE\]](#) Thanks for the update, but it should hold 20-500 connection perfectly?

No tested as said above. In theory yes. Practically idk :)

CrypterHQ - November 18, 2022, 9:54 am

(Nov 18, 2022 09:47 AM)arsium Wrote: [\[CITE\]](#) No tested as said above. In theory yes. Practically idk :)

Alright bro, I've picked my point thanks for the explanation.

zelus - December 4, 2022, 12:50 pm

It crashes for me. Maybe cos i tried testing the stub on same PC

node01 - December 5, 2022, 3:44 am

i been off for couple of months in that short term the project matured very well, nice job bro

Richest. - December 5, 2022, 5:09 am

Played around with this RAT a couple times now and it works great! Everything works fine.
Good luck with the rest of the project OP!

arsium - December 12, 2022, 9:57 am

New update ! (and maybe the last)

[New][Client] BypassUAC
[New] Added TCP Connection view [Tweaks][UI] Optimization (imagelist, tabcontrol...)
[New] Added total clients on main UI [Fix] Some logs could cause crash/be not displayed
[Tweaks] Optimization for PacketHandler (methods full static) [Tweaks] Optimization for
ClientHandler (methods full static)
[Tweaks] Optimization for ServerHandler (methods full static)

DI?E - December 13, 2022, 9:19 am

Nice to see you being active with this. Keep it up.

Warune79 - February 13, 2023, 11:07 pm

(Dec 12, 2022 10:57 AM)arsium Wrote: [\[CITE\]](#) New update ! (and maybe the last)

[New][Client] BypassUAC
[New] Added TCP Connection view [Tweaks][UI] Optimization (imagelist, tabcontrol...)
[New] Added total clients on main UI [Fix] Some logs could cause crash/be not displayed
[Tweaks] Optimization for PacketHandler (methods full static) [Tweaks] Optimization for
ClientHandler (methods full static)
[Tweaks] Optimization for ServerHandler (methods full static)
Verry nice updates, why is this the last update?

arsium - February 13, 2023, 11:14 pm

(Feb 14, 2023 12:07 AM)Warune79 Wrote: [\[CITE\]](#) Verry nice updates, why is this the last update?
Because I'm tired that people don't wanna learn. And I'm working on a derivated rat from eagle with
fully new communication's protocol :)

jmark7 - February 16, 2023, 3:09 pm

Its sad to see end of such a nice project.

arsium - February 16, 2023, 3:14 pm

(Feb 16, 2023 04:09 PM)jmark7 Wrote: [\[CITE\]](#) Its sad to see end of such a nice project.
New project will be easier to encrypt (no plugin system) and some advanced things will be added :)

It's easier to begin a new derivated project than fully modifying the old one (but will try anyway)

Monxiwnl - February 16, 2023, 7:27 pm

When i launch my builder, it doesnt come up as a client. Why is this the case? I launched my builder
on my laptop that runs windows 11

arsium - February 17, 2023, 5:06 am

(Feb 16, 2023 08:27 PM)Monxiwnl Wrote: [\[CITE\]](#) When i launch my builder, it doesnt come up as a
client. Why is this the case? I launched my builder on my laptop that runs windows 11
Check your av or your firewall
Maybe and surely your firewall with server

jmark7 - February 18, 2023, 10:03 am

(Feb 16, 2023 04:14 PM)arsium Wrote: [\[CITE\]](#) New project will be easier to encrypt (no plugin
system) and some advanced things will be added :)

It's easier to begin a new derivated project than fully modifying the old one (but will try anyway) sounds interesting, what will be the new features added to it?
Also it was not hard to crypt eagle.

(Feb 17, 2023 06:06 AM)arsium Wrote: [\[CITE\]](#) Check your av or your firewall
Maybe and surely your firewall with server
you should consider adding AV and Firewall Disabler as most of user dont know how to disable firewall.

arsium - February 19, 2023, 1:45 am

(Feb 18, 2023 11:03 AM)jmark7 Wrote: [\[CITE\]](#) sounds interesting, what will be the new features added to it?
Also it was not hard to crypt eagle.

you should consider adding AV and Firewall Disabler as most of user dont know how to disable firewall.

Fully new network protocol, no fancy features only advanced features like you could find in some tools like cobalt strike and the like.

I'm not there to learn people using remote access tool or others ?

jmark7 - February 20, 2023, 11:38 pm

(Feb 19, 2023 02:45 AM)arsium Wrote: [\[CITE\]](#) I'm not there to learn people using remote access tool or others ?
Thats True.

OPCLOSURE - February 21, 2023, 6:00 am

does it still crash all the time or is it more stable now

rhg2323 - February 22, 2023, 9:47 am

Any suggestion for what crypter is best for this RAT? Looks great by the way!

jmark7 - February 24, 2023, 7:06 am

You Planing to add hvnc in the new rat/update you making?

arsium - February 24, 2023, 7:43 am

(Feb 24, 2023 08:06 AM)jmark7 Wrote: [\[CITE\]](#) You Planing to add hvnc in the new rat/update you making?

No. I don't think hvnc is meaningful. Gathering information, Low-Level bypass and the like are most interesting stuff. Any hvnc is a derivated version of Tiny nuke nowadays. See pandora hvnc, venom hvnc and the like.

jmark7 - February 24, 2023, 7:52 am

(Feb 24, 2023 08:43 AM)arsium Wrote: [\[CITE\]](#) No. I don't think hvnc is meaningful. Gathering information, Low-Level bypass and the like are most interesting stuff. Any hvnc is a derivated version of Tiny nuke nowadays. See pandora hvnc, venom hvnc and the like.

I was going through your Github Repositories and found hvnc forked there and made me think you are adding it.

would be interesting as a Plugin though or a separate project like Pegasus.

Sanel - February 25, 2023, 8:44 am

Thats nice keep going but I get a Crash when someone disconnects and I'm like Between folders I turn off the folder browser and it crashes + when I turn off eagle and turn it on it only connects to my

computer but not the surrounding ones but nice updates ?

demesur - February 27, 2023, 4:51 am

Getting back to malware dev :) . is it okay if I reuse some of the code? I want to write a C++ server for this.

MSBuild path seems to be old or at least variant between Windows versions. On what version of windows have you tested this ?

I'm getting back to malware dev :) . is it okay if I reuse the code? I want to write a C++ server for this.

arsium - February 27, 2023, 9:17 am

(Feb 27, 2023 05:51 AM)demesur Wrote: [\[CITE\]](#) Getting back to malware dev :) . is it okay if I reuse some of the code? I want to write a C++ server for this.

MSBuild path seems to be old or at least variant between Windows versions. On what version of windows have you tested this ?

I'm getting back to malware dev :) . is it okay if I reuse the code? I want to write a C++ server for this.

Yes yes you can.

It has been tested on Windows 10 & 11 latest version.

hkdd - March 19, 2023, 6:59 pm

Very nice rat, I am very interested, how can I contact you?

maka0001111 - May 10, 2023, 12:51 pm

Nice project, make a darker theme

murado - May 11, 2023, 9:43 am

looking good so far, will you add ddos feature? i am really interested in what kind of method you would use there.