

Forum:[Hack Forums](#)

Thread: [\[\\$150\] Imperium Crypter || Runtime FUD or Refund.](#)

bad_c0de - February 9, 2018, 2:08 pm

Screenshots:

Spoiler [\(Click to View\)](#)

Spoiler [\(Click to View\)](#)

Spoiler [\(Click to View\)](#)

Spoiler [\(Click to View\)](#)

Spoiler [\(Click to View\)](#)

About Imperium:

Tired of "crypters" promising good runtime execution rates yet they fail to comply because of overused old injection methods (dynamic forking also called "RunPE") ? Tired of using shared stubs which get detected in ~6 to 24 hours at best ? If so, you're in the right place.

Imperium was initially a private crypter fully coded in C/ASM then it came to our knowledge that most crypters in this forum doesn't comply with their promises and their fancy threads design, so we decided to give a chance to members here to have a taste of a real crypter under reasonable prices for the community(we are aware that most persons here can't afford the C/ASM version). In this view, we decided to make a low budget version by using a .NET loader instead of the C one and switching some evasions techniques to overcome the gap between price and quality.

What we guarantee:

Completely unique injection method(never used in the field) assuring runtime evasion.

Completely unique stubs(you build your own stub in USG tab).

Small stub size.

Bypassing SSDT hooks(eg. Norton & only AVs based filters) on x86 based machines(no crypter did that til now).

High execution rates.

Refund in case the crypter get caught at runtime by mainstream AVs(Avast, AVG, Bitdefender, KAV, ESET, Norton, TrendMicro, MSE).

Active support.

Plans:

1 Month usage & Ability to build 2 stubs: \$150

1 Month usage & Ability to build 5 stubs: \$280

3 Month usage & Ability to build 10 stubs: \$600

Accepted payment methods:BTC, ETH, BCH(BitcoinCash) & LTC.

Contact us:Jabber: imperium_crypt@jabber.ru

Scan:

Spoiler [\(Click to View\)](#)http://viruscheckmate.com/image/Bi3Z267o8z1f/full/img.png

Runtime videos:

Spoiler ([Click to View](#))Kaspersky:
<https://www.youtube.com/watch?v=2FLo8vhMzN8>

ESET:
https://www.youtube.com/watch?v=DEIye3_e5nQ

Windows Defender:
<https://www.youtube.com/watch?v=C-b7STzQxu8>

Avast:
<https://www.youtube.com/watch?v=mHtlHq7uqSA>

Norton Internet Security:
https://www.youtube.com/watch?v=LTyDQ_gQtTU

360 Total Security:
<https://www.youtube.com/watch?v=SarSUffgtho>

Avira Antivirus:
<https://www.youtube.com/watch?v=UJLmMFeGONQ>

AVG:
<https://www.youtube.com/watch?v=kGpIA-HJzCY>

whendarknesscomes - February 10, 2018, 3:55 am

Can you shoot me a pm with runtime scans?

bad_c0de - February 10, 2018, 5:24 am

(Feb 10, 2018 04:55 AM)whendarknesscomes Wrote: [\[CITE\]](#) Can you shoot me a pm with runtime scans?

Runtime scans ? those runtime online scanners aren't even accurate, you can add me on jabber to test with any AV.

mehtevs - February 10, 2018, 7:19 am

(Feb 10, 2018 06:24 AM)bad_c0de Wrote: [\[CITE\]](#) Runtime scans ? those runtime online scanners aren't even accurate, you can add me on jabber to test with any AV.

why are these online scanners not accurate ?

bad_c0de - February 10, 2018, 7:25 am

(Feb 10, 2018 08:19 AM)mehtevs Wrote: [\[CITE\]](#) why are these online scanners not accurate ? not gonna argue here as i'm not endorsing any service(AVs detections depends on multiple factors like if machines are running on x86 or x64, child processes, cloud options...), but if you wish to see it in action, you can download any AV and we will gladly test it for you via a remote desktop solution.

05317832892 - February 10, 2018, 8:26 am

Screenshot shows injecting into svchost. You say you use a .net loader. Which .net framework does the loader target? Does it work with EOF data or .net files? Ring-3 book evasion, is it manual mapping into current process or syscall extraction? What injection technique is this using? Are you fresh spawning svchost and hollowing it or mapping payload PE and side loading into a currently running svchost? Do you provide any anti-emulation? You say coded in ASM/C yet you have a .net loader? Any explanation on why this is necessary?

Sorry if I come off as aggressive. Your crypter is new on this forum and lacks technical details. PM if you want testing/vouch.

bad_c0de - February 10, 2018, 8:54 am

(Feb 10, 2018 09:26 AM)ROOTED Wrote: [\[CITE\]](#) Screenshot shows injecting into svchost. You say you use a .net loader. Which .net framework does the loader target? Does it work with EOF data or .net files? Ring-3 book evasion, is it manual mapping into current process or syscall extraction? What injection technique is this using? Are you fresh spawning svchost and hollowing it or mapping payload PE and side loading into a currently running svchost? Do you provide any anti-emulation? You say coded in ASM/C yet you have a .net loader? Any explanation on why the this is necessary?

Sorry if I come off as aggressive. Your crypter is new on this forum and lacks technical details. PM if you want testing/vouch.

- "Which .net framework does the loader target?"

It targets any version you want.

- "Does it work with EOF data or .net files?"

Works with .NET files, but we don't support EOF since no modern malware use that.

- "Ring-3 hook evasion, is it manual mapping into current process or syscall extraction?"

Usermode hooks are not really needed to be bypassed im my case, but i'm doing it anyway(i map a new ntdll from the disk) and no it's not manual mapping.

- "What injection technique is this using? "

Technique is a mix between basic RunPE and Process Doppelganging(it's compatible with all windows versions in both arch).

- "Are you fresh spawning svchost and hollowing it or mapping payload PE and side loading into a currently running svchost?"

i spawn wermgr by default because it's usually spawned when a crash happens and is signed by Microsoft but it works with svchost too.

- "Do you provide any anti-emulation?"

yeah we do.

- "You say coded in ASM/C yet you have a .net loader? Any explanation on why the this is necessary?"

Answer is on the thread: to make a low budget version, there is a C/ASM version already in sales(not here).

- "Sorry if I come off as aggressive"

Not at all.

- "PM if you want testing/vouch."

We may provide vouch copies but not for now.

05317832892 - February 10, 2018, 11:11 am

(Feb 10, 2018 09:54 AM)bad_c0de Wrote: [\[CITE\]](#) - "Which .net framework does the loader target?"
It targets any version you want.

- "Does it work with EOF data or .net files?"

Works with .NET files, but we don't support EOF since no modern malware use that.

- "Ring-3 hook evasion, is it manual mapping into current process or syscall extraction?"
Usermode hooks are not really needed to be bypassed in my case, but i'm doing it anyway(i map a new ntdll from the disk) and no it's not manual mapping.

- "What injection technique is this using? "
Technique is a mix between basic RunPE and Process Doppelganging(it's compatible with all windows versions in both arch).

- "Are you fresh spawning svchost and hollowing it or mapping payload PE and side loading into a currently running svchost?"
i spawn wermgr by default because it's usually spawned when a crash happens and is signed by Microsoft but it works with svchost too.

- "Do you provide any anti-emulation?"
yeah we do.

- "You say coded in ASM/C yet you have a .net loader? Any explanation on why the this is necessary?"
Answer is on the thread: to make a low budget version, there is a C/ASM version already in sales(not here).

- "Sorry if I come off as aggressive"
Not at all.

- "PM if you want testing/vouch."
We may provide vouch copies but not for now.
Nicely layed out reply, and you gave all the answers I want to hear. You have my vouch.

Your injection method intrigues me. I have seen an interesting implementation of doppelgänger live in the wild, it uses the second half of the traditional PoC, creating the process from the section object, however it's obtains the section object differently without using the transaction APIs. Maybe similar to your work, I have no idea.

One last thing, for most people, the definition of manual mapping is just that, imitating LoadLibraryA() reading a clean copy of ntdll.dll from the disk and mapping it into memory so the functions can be executed without any hooks, which sounds like what you're doing.

Regardless, you have my vouch, good luck with sales.

DexterGO - February 10, 2018, 11:14 am
(Feb 10, 2018 11:27 AM)_GodLike Wrote: [\[CITE\]](#) use dyncheck for your runtime scan...
hello

<https://run4me.net/result/0857447d667e3e19ad8d61f8716bac7f2c32ce73c691eaeca41d871ca3d5797a>

bad_c0de - February 10, 2018, 11:18 am
(Feb 10, 2018 12:11 PM)ROOTED Wrote: [\[CITE\]](#) Nicely layed out reply, and you gave all the answers I want to hear. You have my vouch.

Your injection method intrigues me. I have seen an interesting implementation of doppelgänger live

in the wild, it uses the second half of the traditional PoC, creating the process from the section object, however it's obtains the section object differently without using the transaction APIs. Maybe similar to your work, I have no idea.

One last thing, for most people, the definition of manual mapping is just that, imitating LoadLibraryA() reading a clean copy of ntdll.dll from the disk and mapping it into memory so the functions can be executed without any hooks, which sounds like what you're doing.

Regardless, you have my vouch, good luck with sales.

Thanks for your reply!

you can add me on jabber for more information.

(Feb 10, 2018 12:14 PM)mike10 Wrote: [\[CITE\]](#) hello

<https://run4me.net/result/0857447d667e3e19ad8d61f8716bac7f2c32ce73c691eaeca41d871ca3d5797a>

Thanks for buying !

I hope you enjoy it, even though as i said before those online scanners aren't accurate(yeah it's FUD on them, but i still insist on accuracy fact).

mehtevs - February 10, 2018, 12:05 pm

(Feb 10, 2018 12:14 PM)mike10 Wrote: [\[CITE\]](#) hello

<https://run4me.net/result/0857447d667e3e19ad8d61f8716bac7f2c32ce73c691eaeca41d871ca3d5797a>

scan with internet access on.

SIM-2212192 - February 10, 2018, 2:28 pm

(Feb 10, 2018 02:57 PM)_GodLike Wrote: [\[CITE\]](#) mfw

>too poor to afford \$30 dyncheck

>uses a shitty excuse like "its not accurate!" to avoid providing runtime proof

GLWS THOUGH BUDDY!!

dude sick burn

bad_c0de - February 11, 2018, 2:34 am

updated with some runtime videos for Avast & ESET & Kaspersky yesterday.

gonna do the rest today.

mehtevs - February 11, 2018, 2:58 am

what about CIS (<https://www.comodo.com/home/internet-security/free-internet-security.php>) with hips enabled. & 360 Total security (<https://www.360totalsecurity.com/en/>)

bad_c0de - February 11, 2018, 5:25 am

(Feb 11, 2018 03:58 AM)mehtevs Wrote: [\[CITE\]](#) what about CIS (

<https://www.comodo.com/home/internet-security/free-internet-security.php>) with hips enabled. & 360 Total security (<https://www.360totalsecurity.com/en/>)

We tested CIS and as you see, it didn't handled my code correctly in the isolation mode(enabled by default) for native files... we will fix this soon.

For 360, yeah we bypass it.

Meedman - February 11, 2018, 9:21 am

(Feb 10, 2018 12:50 PM)_GodLike Wrote: [\[CITE\]](#) run4me is the most inaccurate runtime scanner there is. If you want results you use dyncheck. \$30 per check, not \$30 per month (run4me).

Thank you for your feedback I take what you say,
If you have any idea how Run4Me can be better send me message !

Kind Regards,
Meedman

Guccitive - February 11, 2018, 10:59 am

Sounds like the new deal gl & hf

SoveitUnion - February 11, 2018, 11:02 am

Long hesitated, but bought this crypter. This is a really high-quality product, I received 100% scantime and runtime FUD. Pleasantly surprised by small size output file. Support is almost always online and helps with any questions. It's expensive, but the quality is worth it. I recommend 5+

bad_c0de - February 11, 2018, 11:09 am

(Feb 11, 2018 12:02 PM)VolodyaPutin Wrote: [\[CITE\]](#) Long hesitated, but bought this crypter. This is a really high-quality product, I received 100% scantime and runtime FUD. Pleasantly surprised by small size output file. Support is almost always online and helps with any questions. It's expensive, but the quality is worth it. I recommend 5+

Thanks for your comment ! i hope you enjoy it.

(Feb 11, 2018 11:59 AM)Guccitive Wrote: [\[CITE\]](#) Sounds like the new deal gl & hf
thanks but i'm not sure what you meant by "new deal", i assume you're talking about runtime FUD policy and yeah i take those detections seriously... a crypter that can't bypass at runtime AVs must not be sold in the first place.

bad_c0de - February 13, 2018, 8:25 am

Added a video for AVG & Fixed some issues with old malwares.
Should be fine now.

jackbaur57 - February 13, 2018, 9:59 am

Added you on Jabber , kindly accept and let talk there . Thank

kauf - February 13, 2018, 10:53 am

how long FUD is the crypter?

bad_c0de - February 13, 2018, 11:07 am

(Feb 13, 2018 10:59 AM)jackbaur57 Wrote: [\[CITE\]](#) Added you on Jabber , kindly accept and let talk there . Thank

yeah i accepted you

(Feb 13, 2018 11:53 AM)hostbob Wrote: [\[CITE\]](#) how long FUD is the crypter?
FUD time is long enough since the stubs you get are mutated at each build.

Electron - February 13, 2018, 2:25 pm

Vouch for bad_c0de, he's an amazing coder!

Smile? - February 14, 2018, 6:44 am

So what rat did you use for those videos and stub analyze?

bad_c0de - February 14, 2018, 7:08 am

(Feb 14, 2018 07:44 AM)dâFu™ Wrote: [\[CITE\]](#) So what rat did you use for those videos and stub

analyze?

netwire & #, can do anything you want too.

(Feb 13, 2018 03:25 PM)Noxious™ Wrote: [\[CITE\]](#) Vouch for bad_c0de, he's an amazing coder! Thanks ! although my pseudo says my code is bad.

Smile? - February 14, 2018, 7:24 am

(Feb 14, 2018 08:08 AM)bad_c0de Wrote: [\[CITE\]](#) netwire & #, can do anything you want too.

Thanks ! although my pseudo says my code is bad.

Better upload some more proofs with netwire & # appear on screen.

bad_c0de - February 14, 2018, 7:26 am

(Feb 14, 2018 08:24 AM)dåFu™ Wrote: [\[CITE\]](#) Better upload some more proofs with netwire & # appear on screen.

appears on the screen lol, and for netwire showing the RAT getting connected is enough. you can add me jabber if you want to see it live.

Smile? - February 14, 2018, 8:12 am

(Feb 14, 2018 08:26 AM)bad_c0de Wrote: [\[CITE\]](#) # appears on the screen lol, and for netwire showing the RAT getting connected is enough.

you can add me jabber if you want to see it live.

Okay thanks , it wasn't clear at eset video what rat are you using.

I will wait for some vouches and will buy later.

bad_c0de - February 16, 2018, 6:25 am

Update: reduced stub size to ~30kb and cleaned a bitdefender startup detection.

PerfectStorm - February 16, 2018, 6:29 am

(Feb 10, 2018 12:50 PM)_GodLike Wrote: [\[CITE\]](#) run4me is the most unaccurate runtime scanner there is. If you want results you use dyncheck. \$30 per check, not \$30 per month (run4me). 30 per check, gtfo here with that

blackdark22 - February 16, 2018, 2:31 pm

adding u on jabber and if I can see proof, buying this straight away. About time we get some real runtime FUD crypters in here

bad_c0de - February 17, 2018, 6:25 am

(Feb 16, 2018 03:31 PM)blackdark22 Wrote: [\[CITE\]](#) adding u on jabber and if I can see proof, buying this straight away. About time we get some real runtime FUD crypters in here i've accepted you, and yeah you're welcome to ask for any proof.

Zenk69 - February 17, 2018, 12:33 pm

(Feb 17, 2018 07:25 AM)bad_c0de Wrote: [\[CITE\]](#) i've accepted you, and yeah you're welcome to ask for any proof.

check my pm please

kauf - February 18, 2018, 10:27 pm

(Feb 13, 2018 12:07 PM)bad_c0de Wrote: [\[CITE\]](#) yeah i accepted you

FUD time is long enough since the stubs you get are mutated at each build.

is this private stub for each customers? as you said every stubs are mutated.

bad_c0de - February 19, 2018, 2:07 am

(Feb 17, 2018 01:33 PM)Zenk69 Wrote: [\[CITE\]](#) check my pm please
replied to you on jabber.

(Feb 18, 2018 11:27 PM)hostbob Wrote: [\[CITE\]](#) is this private stub for each customers? as you said
every stubs are mutated.

each customer have the right to generate a unique stub depending on his license, that stub is also
mutated as an extra step at each crypt to make the FUD time longer.

bad_c0de - February 23, 2018, 4:11 am

Sales paused for now due to a new nod32 runtime detection(
http://www.virusradar.com/en/MSIL_Injector.TKT/description), days will be added for all clients with
new stubs.