

Forum: [Hack Forums](#)

Thread: [Moon Crypter \[FUD 5+ MONTHS\] VT PROOF | EXTENSION SPOOFING](#)

Moon_Developer - July 15, 2022, 6:52 pm

[Video: <https://vimeo.com/728174071>]

BSOD (if closed)
WATCHDOG
Check IsDebuggerPresent (Anti Debug / Attach)
Check MouseMovements (Close if user is a VM)
AES / XOR / Custom Encryption
Support .NET / Native / ASM / Python / Java (x64 - x86)
File is compressed and reduced of size (Max 300kb for 1/2mb file)
Destroy payload ("Melt")
Melt file (self delete)
Bind files (ALL extensions. e.g mp4 / pdf / etc)
AMSI / EFW / AV evasion and hooking

VIRUSTOTAL LINK - >

<https://www.virustotal.com/gui/file/cbc988436005a79d12c786a4483c78f91a72eb22b59c03c289f63053eb21d598/details>

**Also single crypt available for PUBLIC stub (25\$ for crypt.)

Telegram @LordCokage

PROVIDING 2 VOUCH COPIES TOO (ONLY TO USERS THAT ARE REGISTERED FROM MORE THEN 5+ years or with 100+ contracts!

We are using an extension spoofing (forced to .batch)

The "mechanism" is exactly this :

- > Batch file - > Powershell (RunPE) -> Decrypt* - > c++ stub - > Decrypt - > Execute (public stub is c++, private stub is c++ with mASM, low size)
[contract=tid]Start Contract[/contract]

Sticky Bot - July 15, 2022, 8:29 pm

Hi, I'm Sticky Bot. The owner of this thread has purchased a Paid Sticky. Hack Forums does not get involved in deals or deal disputes. We do not vouch for the product or the service offered by members. Please note that all deals are at your own risk. The sticky will expire on 07-22-2022. If you or a loved one are interested in buying a sticky please visit this page: [Buy Sticky](#). For more information about Paid Stickies you can read our [Help Doc](#).

SIM-3281006 - July 16, 2022, 4:50 am

I need to check out this...

hamin390724 - July 16, 2022, 11:53 am

I bought this seller's product. (public / 1 month)

Since there are few reviews for this seller, I will kindly write a review for other users of HF.

I have completed the payment and am waiting for the delivery of the product.(Delivery scheduled within 24 hours)

After receiving the crypter, I will focus on bypassing AV on runtime and whether it works well.

localhost247 - July 18, 2022, 6:19 am

Did you think is a good idea to make the file in .batch after crypting.
because it will be easy to decrypt.

Please can anyone confirm if it bypass WD.

Moon_Developer - July 18, 2022, 8:10 am

(Jul 18, 2022 06:19 AM)localhost247 Wrote: [\[CITE\]](#) how much did you paid for it?
Hi, do you mean prices? Read post again

Moon_Developer - July 20, 2022, 12:37 am

(Jul 18, 2022 06:19 AM)localhost247 Wrote: [\[CITE\]](#) Did you think is a good idea to make the file in .batch after crypting.
because it will be easy to decrypt.

Please can anyone confirm if it bypass WD.

The main goal of crypting with this method, is that isn't easy for them to recognize file as .executable on scantime, and while for runtime it decrypt and allocate memory dynamically , so , it's not easy to decrypt, or to detect!

Check it out video, and uploaded VT link for scan!

Moon_Developer - July 20, 2022, 2:25 am

(Jul 20, 2022 02:21 AM)kysse Wrote: [\[CITE\]](#) refused to provide a vouch copy because he posted "proof/virus total links" on the thread.

Uploading to virus total eventually will get this method patched.
I'm not forced to give a vouch copy, you can read again the rules. Also, it's safe from the first time I posted it here , also uploading new links,
and due to this method of extension spoofing used, it won't get detected anytime soon

And i've already sold product here (and as my other thread , all are liked by users.)

Also, after begging for a vouch (while you got also open disputes.) it's not really a trustworthy thing.

You are probably the last person that (noone here) will give a vouch copy too

go away and stop trying to shitpost :)

dublib - July 20, 2022, 2:33 am

(Jul 20, 2022 02:25 AM)Moon_Developer Wrote: [\[CITE\]](#) I'm not forced to give a vouch copy, you can read again the rules. Also, it's safe from the first time I posted it here , also uploading new links,
and due to this method of extension spoofing used, it won't get detected anytime soon

Thanks

eh that's funny it's like you didn't upload to virustotal where they distribute to all AVs
same guy @elmundo sold the same thing and it was detected week after

Avi- - July 20, 2022, 2:58 am

(Jul 20, 2022 02:25 AM)Moon_Developer Wrote: [\[CITE\]](#) I'm not forced to give a vouch copy, you can read again the rules. Also, it's safe from the first time I posted it here , also uploading new links, and due to this method of extension spoofing used, it won't get detected anytime soon

And i've already sold product here (and as my other thread , all are liked by users.)

Also, after begging for a vouch (while you got also open disputes.) it's not really a trustworthy thing.

You are probably the last person that (noone here) will give a vouch copy too

go away and stop trying to shitpost :)

looks like his open dispute is resolved on his end and the other guy is just offline to mark it as resolve lol and it's a dispute over him leaving a negative b-rating on his service + you prob shouldn't offer vouch copies on the post and not want to provide them to members who are 5+ years onsite and like he mentioned uploading to virustotal, this will just end up being patched.

Moon_Developer - July 20, 2022, 9:48 am

(Jul 20, 2022 02:58 AM)Avi- Wrote: [\[CITE\]](#) looks like his open dispute is resolved on his end and the other guy is just offline to mark it as resolve lol and it's a dispute over him leaving a negative b-rating on his service + you prob shouldn't offer vouch copies on the post and not want to provide them to members who are 5+ years onsite and like he mentioned uploading to virustotal, this will just end up being patched.

Its not gonna get patched, if it Was the case, it should have been time ago, and not after 5 months, also I have my own methods to keep updating it

1 month : 40\$ public stub

3 month : 100\$ public stub

1 month : 80\$ private stub

~~~~~ Updated Price for next 3 customers

Stanley - July 24, 2022, 9:33 am

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

Moon\_Developer - August 7, 2022, 3:51 pm

20% discount on all sales till 10/08

**wtfpop** - August 17, 2022, 7:44 am

You know, i'd appreciate it if you stopped pasting my stuff.

Anyways, my github got suspended so good luck finding someone else to paste from if you feel like scamming more people.

**justalemon** - August 17, 2022, 1:49 pm

Virus total shows Microsoft Defender detection "VirTool:BAT/lalive.E!MTB". Is that correct? Btw, this is exe output or .bat?

**sjonnietamponie** - September 12, 2022, 11:05 am

WARNING DON'T BUY FROM MOON\_DEVELOPER

He sent me a p\_moon.exe and private\_stub\_loader\_login.exe which dropped a TEAMSPEAK.exe in my roaming directory. I decompiled the code and it was a information stealer (Stealerium) to be exact. the file shows a fake error message like: File cannot be inside a ZIP directory. Please extract.

skillless script kiddie who claims to have made a crypter but is full of shit. be aware (reported)

<https://ibb.co/vJYspyS> <-- screenshot