

Forum:[Hack Forums](#)

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

Moon_Developer - July 15, 2022, 8:34 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.)

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

[u]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]

oryadoo - July 15, 2022, 9:42 pm

amazin crypter i buy it now really bypass wd runtime thanks friend

jmark7 - July 15, 2022, 11:39 pm

I can see finally you got leet upgrade.

BTW You say on thread that its "FUD From 5+ Months" , so we can say it was last updated before 5 months and still FUD?

SIM-5049184 - July 15, 2022, 11:45 pm

I am not registered for as long as you have asked for, nor do I have 100 market contracts. However if you are interested I will gladly provide you a high quality review as I just finished my software I need to protect.

Regardless, best of luck with your sales, excited to see what you build :)

Moon_Developer - July 16, 2022, 12:27 am

(Jul 15, 2022 11:45 PM)Mr. Business Wrote: [\[CITE\]](#) I am not registered for as long as you have asked for, nor do I have 100 market contracts. However if you are interested I will gladly provide you a high quality review as I just finished my software I need to protect.

Regardless, best of luck with your sales, excited to see what you build :)

I have sold already to someone that vouched here, so It's fine. If I find someone that mark my requirements i'll give a vouch too

(Jul 15, 2022 11:39 PM)jmark7 Wrote: [\[CITE\]](#) I can see finally you got leet upgrade.

BTW You say on thread that its "FUD From 5+ Months" , so we can say it was last updated before 5 months and still FUD?

It's updated frequently from 5+ months, but It never got a single detection. And for a crypter is a really good result

nulluser123 - July 16, 2022, 2:32 am

(Jul 15, 2022 08:34 PM)Moon_Developer Wrote: [\[CITE\]](#) BSOD (if closed)

WATCHDOG

Check IsDebuggerPresent (Anti Debug / Attach)

Do you really call this anti debug?

Moon_Developer - July 16, 2022, 2:49 am

(Jul 16, 2022 02:32 AM)nulluser123 Wrote: [\[CITE\]](#) Do you really call this anti debug?

It got a basic anti debugger, it's not the main purpose, bypassing most of AVs from months its the purpose :)

Sticky Bot - July 16, 2022, 10:00 am

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 07-23-2022. 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](#).

hamin390724 - July 16, 2022, 12:02 pm

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.

Moon_Developer - July 17, 2022, 7:42 pm

(Jul 17, 2022 07:32 PM)Dyne Wrote: [\[CITE\]](#) I would be astounded to see an .mp4 extension spoof from .exe bypass AV runtime lol.

Or .pdf.

It's forced to .bat extension atm, and i've also made a lot of work to made it possible, wasn't really easy.

You can bind .pdf / .mp4 and any extensions you prefer tho

obsoletetoaster - July 18, 2022, 12:19 pm

A++ this vendor has top notch products =)

rroki123 - July 18, 2022, 8:17 pm

Hi , can i have vouch copy, i have 10 years here :) i love crypt

Moon_Developer - July 18, 2022, 10:13 pm

(Jul 18, 2022 08:17 PM)rroki123 Wrote: [\[CITE\]](#) Hi , can i have vouch copy, i have 10 years here :) i love crypt

Hi yes DM me

Moon_Developer - July 21, 2022, 9:29 am

1 month : 40\$ public stub

3 month : 100\$ public stub

1 month : 80\$ private stub

Updated price for next 3 customers!

AlphaFace - July 21, 2022, 10:59 am

(Jul 21, 2022 09:29 AM)Moon_Developer Wrote: [\[CITE\]](#) 1 month : 40\$ public stub

3 month : 100\$ public stub

1 month : 80\$ private stub

Updated price for next 3 customers!

Can't DM you as I have a new acc - can you DM me

Moon_Developer - July 21, 2022, 2:37 pm

(Jul 21, 2022 10:59 AM)AlphaFace Wrote: [\[CITE\]](#) Can't DM you as I have a new acc - can you DM me

Done

Moon_Developer - July 22, 2022, 10:04 pm

Last 2 customers for the new offer;

Also updated the c# stub

hamin390724 - July 23, 2022, 2:28 pm

As stated in the contract, the seller violated the terms of the refund if he did not bypass the runtime in Avast.

The product does not bypass Avast and does not even support commercial rat such as Warzone and # other than AsyncRAT.

The seller said that he couldn't get a refund because he was overseas.

A dispute is brought up because the seller did not perform the contract properly.

Fugg - July 23, 2022, 3:16 pm

The seller literally scanned his own stub on virus total.

what the fuck.

Mutant - July 23, 2022, 3:32 pm

(Jul 15, 2022 08:34 PM)Moon_Developer Wrote: [\[CITE\]](#)

[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]

This is a joke right?

You really scanned your stub on VT?

Should edit your post to say 100% detected every single time.

Also, I love how every single "account" that purchased your product is new and only has 1 contract.. with you lol.

Also your vouches to trusted members.. nowhere to be found.

RED FLAGS GALORE.

Fugg - July 23, 2022, 3:36 pm

(Jul 23, 2022 03:32 PM)Mutant Wrote: [\[CITE\]](#) This is a joke right?

You really scanned your stub on VT?

Should edit your post to say 100% detected every single time.

Also, I love how every single "account" that purchased your product is new and only has 1 contract.. with you lol.

Also your vouches to trusted members.. nowhere to be found.

RED FLAGS GALORE.

User can code his own custom encryption algorithm but doesn't understand malware distribution.

Something tells me that OP didn't code any of this shit.