

Forum:[Hack Forums](#)

Thread: [\[FREE\] FUD HQ Crypting Service](#)

Jean-Jacques Rousseau - October 25, 2019, 2:02 am

Dear members of Hackforums,

Today, I finished building my packer and its infrastructure. To celebrate, I will provide all members on this forum with unlimited free crypts for 3 days (starting now).

Some technical details about the packer:

- always correct entropy (will never reveal it has packed content)
- real runtime bypasses
- slightly unique payload execution method
- bypasses any behavioural/hooks engine by AV, using system calls directly to the kernel (both x86 native and WOW64)
- Written in C and assembly
- Native PE32 exe supported.

The link is: <http://j3bqbosl3z5emesj.onion/>

To reach this link, you need to use the Tor network. Download it here: [Tor Project | Download](#)

Your public key is: "hackforums-3days"

I will update the public stub whenever I see several detections and I have the time for it.

I reserve the right to discontinue the free stubs early, or prolong the free duration, depending on its impact on the private stubs.

Richie Rich - October 25, 2019, 4:53 am

Good job i will try it out

StrikerICA - October 25, 2019, 5:07 am

13/70 results atm. Not bad.

Cyber Coder - October 25, 2019, 5:18 am

(Oct 25, 2019 05:07 AM)StrikerICA Wrote: [\[CITE\]](#) 13/70 results atm. Not bad.70?for sure there isnt any non distributing scanner with that many avs you scanned it somewhere where it distributes. That's why some ppl don't deserve free stuff, they are just going to sh.it all over someone's work for free.

Jean-Jacques Rousseau - October 25, 2019, 5:25 am

Please do not scan on distributing sites again, as it will ruin the detections. I created a new unique public stub, dont ruin it now please.

[Attention Required! | Cloudflare](#)

Defender detection due to bad generation, will fix when I have the time.

Red Vegas - October 25, 2019, 5:34 am

For anyone who's wondering: The website spyralscanner.net is still online and offers non distributing

scanning services for free. I recommend everyone to scan the stub on the site.

Seif Mahmmued - October 25, 2019, 5:35 am

runtime and scantime ?

ii will be fud of node 32 ? at runtime ?

VCRUNTIME140.dll is missing ? ?

Jean-Jacques Rousseau - October 25, 2019, 5:51 am

(Oct 25, 2019 05:35 AM)Seif Mahmmued Wrote: [\[CITE\]](#) runtime and scantime ?

ii will be fud of node 32 ? at runtime ?

VCRUNTIME140.dll is missing ? ?

Yes, packer is currently runtime FUD.

ESET runtime test (#):

[MEGA](#)

My bad, I forgot to remove the link to vcruntime. Updating stub shortly without the dependency.

Seif Mahmmued - October 25, 2019, 5:53 am

(Oct 25, 2019 05:51 AM)Supercut Wrote: [\[CITE\]](#) Yes, packer is currently runtime FUD.

[MEGA](#)

My bad, I forgot to remove the link to vcruntime. Updating stub shortly without the dependency.
Mega??? VLC?

Jean-Jacques Rousseau - October 25, 2019, 5:59 am

Updated stubs without vcruntime dependancy. My mistake.

Seif Mahmmued - October 25, 2019, 6:05 am

i sent to you add in discord

Exe - October 25, 2019, 2:14 pm

Does this work on .NET Rat's?

Junx - October 25, 2019, 2:36 pm

(Oct 25, 2019 05:07 AM)StrikerICA Wrote: [\[CITE\]](#) 13/70 results atm. Not bad.

Are you a fool? Where did you scan it?

Jean-Jacques Rousseau - October 25, 2019, 2:38 pm

(Oct 25, 2019 02:14 PM)Law Wrote: [\[CITE\]](#) Does this work on .NET Rat's?

No! Native PE32 only! You can use a .NET to Native "converter", if you'd like.

learner319 - October 31, 2019, 10:54 pm

(Oct 25, 2019 02:36 PM)Junx Wrote: [\[CITE\]](#) Are you a fool? Where did you scan it?

I think he scanned it on Virustotal :(

learner319 - November 1, 2019, 10:46 am

(Nov 1, 2019 05:33 AM)Wikipedia Wrote: [\[CITE\]](#) VirusTotal submissions get scanned by literally thousands of YARA rules setup by members of VirusTotal Intelligence, a very expensive enterprise offering by Google. You do not need to be an AV vendor to purchase and use this feature, but many AV vendors get it for free nowadays in exchange for providing a version of their engine for use on the platform.

The detection results on VirusTotal are NOT reliable for the real-world. AV vendors do NOT have to provide the same engine as found in their commercial software and more often than not, the engines being put onto VirusTotal are lacking a lot of features that the commercial software will possess as well as being tweaked to have a lower false positive or higher false positive detection ratio.

All of the scanning services like VirusTotal which do not actually share the sample with the AV vendors and do not rely on VirusTotal internally are even more unreliable and all detection ratios should be taken with an even bigger grain of salt.

Any dynamic tests which are performed in a virtual environment without ensuring the use of all default protection layers are also unreliable. AV software tends to watch out for where a file originated from (e.g. whether it came from an online source like a web browser or whether it was already on the machine locally) and this can affect anything from how heuristic analysis treats the file or how dynamic analysis treats the file. It varies because it's vendor-dependent and there is no "rule book" on how each vendor handles cases like these, so there's no single "generic formula" for accurately testing AV software with cases like these, until you reverse-engineer the entire thing or have insider knowledge for the vendor in question.

Furthermore, any dynamic tests which are performed without an active internet connection are unreliable because of cloud reputation scanning, which often are very good at flagging unknown applications as suspicious. The results from a cloud reputation scan may also dictate whether a sample is emulated before being allowed to properly run on the environment or how it is treated with heuristic memory scanning and other forms of dynamic analysis as well, and once again, it's all vendor-dependent with no "generic formula" for accurately testing these cases across all AV software.

That being said, any dynamic tests which are performed with an active internet connection also mess things up for you, because most vendors are not so great on privacy and will upload that unknown program to the cloud so it can be processed by an automated sandbox system. Vendors like Avira use sandbox projects like Cuckoo on the cloud, Fortinet have their own FortiSandbox appliances and several vendors are using Hybrid-Analysis. The results are often processed automatically and when there is an issue, a human analyst will get involved and check the logs or start manually analyzing the sample. This is really bad for you, because detection can be caused by dynamic markers stored on the cloud in sandbox reports as well (Fortinet can do this - detect unknown malware which has been seen in the sandbox before and was considered suspicious based on log output).

I can continue to go on and on with this but I'm probably talking to a brick wall.
Thank you so much for your valuable information.