

Forum:[Hack Forums](#)

Thread: [Crypter comparison](#) | [Mega thread](#) | [Runtime Results 2023](#) | [Research](#) | [SCANNER.TO](#)

Ph4n70M Phr34K - February 23, 2023, 9:35 am

Related threads:

<https://hackforums.net/showthread.php?tid=6243986>

<https://hackforums.net/showthread.php?tid=6243938>

<https://hackforums.net/showthread.php?tid=6244180>

<https://hackforums.net/showthread.php?tid=6244776>

Welcome in Crypter comparison mega thread. In this topic we will narrow you everything about crypters to help you understand what is being used nowadays, this would make your work easier. With so many crypters on the market to choose from, it can be overwhelming to make a decision. When you whittle them down, all crypters do essentially the same thing: protect your file from anti-virus software. So when we compare crypters, we have to get down to the most important aspect, detection at runtime.

There are many rumors around, such as that WD cannot be bypassed. In this thread we will debunk those. Before we proceed strictly with tests let us describe in general you what are crypters and how they work.

Crypters are in other words encrypting tools. They are used to obfuscate different type of files in order to protect them from cracking and analyzing and to bypass anti virus software. How does it work? There is many different types of encryption and injection methods and techniques to bypass anti virus software, so it would be really hard to list and describe everything, so in summary the image bellow illustrates very simply what a crypter does to your file.

Spoiler ([Click to View](#))

Additionally you may read short the descriptions for most important terms and details. This introduction to crypters was originally written by KillaMuvz who was developing and selling crypters in the past. It explains features, options, settings, basic knowledge, detections, how to not ruin your payload and ultimately how not to annoy the crypter owner.

Spoiler ([Click to View](#))

Everything you should know about crypters: [Crypter Terms and Definitions](#)

To compare the top crypters against each other, we use the same runtime scanner settings:

Internet ON

Cloud protection ON

Samples submission OFF

Duration 180 seconds

All runtime scans will be completed using <https://scanner.to/> and scantime <https://avcheck.net/>. We will also scan not obfuscated payloads to compare them with different crypting methods. That way we will be able to see what exactly can be bypassed using different combinations of malware + crypter. The results will be presented not only as links but also by screenshots for better visibility. We will use paid and free tools listed below with each crypter tool.

- [BlueLoader Botnet](#)
- [PureMiner Botnet](#)
- [PureHVNC Botnet](#)
- [PureLogs Stealer](#)
- [DarkVision RAT](#)
- [WarZone RAT](#)
- [Babylon RAT](#) (FREE AND NATIVE)

We have also selected some of the most famous obfuscators from two sections:

[Cryptography and Encryption Market](#)
[Cryptography, Encryption, and Decryption](#)

Payloads for each tool will be build with minimal settings to ensure that we get the best results. This is also the most common way to use different malware with crypters, that most features are usually added by crypter. But in our tests we will also try to use minimal settings on crypter side, because we want to get the most accurate results for detections at runtime. Any exception of our standard or these basic rules will be listed for each malware and crypter and will be described and shown with screenshots.

Below you can also see the list of crypters that have been chosen for our tests.

Shared between all customers, monthly subscription crypters:

- [PureCrypter](#)
- [ByteCrypter](#)

Private crypters, handmade crypts:

- [ScrubCrypt](#)
- [RAZ](#)

So far, we have listed many different tools, among others free and paid rats, different botnet loaders, silent mining botnet, stealer and HVNC tool. We did also the same for most famous and known crypters being sold in Hackforums marketplace. All of these are available for purchase by anyone on here but some specified tools are being sold only on russian forums. Additionally if you don't have a general idea what is malware and how to use it you may read old e-book which is about starting up rats and http botnets. This e-book is a bit outdated but there is still a lot of good information's.

Spoiler ([Click to View](#))

Everything you should know about http botnets and rats: [Botnet E-book](#)

Below you can see the starting point for each payload. For better understanding we will also quickly describe each tool in case you never heard about them. Here you can also see runtime scan results for payloads that were not obfuscated yet.

[BlueLoader Botnet](#)Spoiler ([Click to View](#))

BlueLoader is advanced botnet with GUI that can hold large amount of bots and execute tasks with simple click. Coded in NET 4.0. Besides the loader(download & execute/update) it also has some additional features: Bot killer, visit website(hidden and visible) and ddos layer 7.

Runtime results ->[14/20](#) | Scantime results ->[12/26](#)

[PureMiner Botnet](#)Spoiler ([Click to View](#))

PureMiner is advanced cryptocurrency silent miner with GUI support for many different coins. Coded in .NET 4.0. It can auto decide if connected device could use GPU or CPU. It also has build-in proxy and some additional tasks and features.

Runtime results ->[13/20](#) | Scantime results ->[10/26](#)

[PureHVNC Botnet](#)Spoiler ([Click to View](#))

PureHVNC is advanced botnet with GUI that enables you to control any computer remotely and invisibly. Through it, you can use the mouse and keyboard in a hidden way, control the desktop, open browsers and other applications in a hidden way. Coded in NET 4.0.

Runtime results ->[12/20](#) | Scantime results ->[7/26](#)

[PureLogs Stealer](#)

Spoiler ([Click to View](#))

Runtime results ->[12/20](#) | Scantime results ->[10/26](#)

[DarkVision RAT](#)Spoiler ([Click to View](#))

DarkVision is a Windows Remote Administration Tool. It is based on a plugin architecture with memory mapped modules that never touches the disk, which allows for flexible loading of functionality on the remote system. Coded in C++ and ASM.

Runtime results ->[11/20](#) | Scantime results ->[8/26](#)

[WarZone RAT](#)Spoiler ([Click to View](#))

WarZone is advanced Remote Administration Tool packed with a lot of different features. The tool is very intuitive and works flawlessly. Its known from its high reliability and performance. Coded in C++.

Runtime results ->[17/20](#) | Scantime results ->[21/26](#)

[Babylon RAT](#)Spoiler ([Click to View](#))

Babylon is old Remote Administration Tool that was being sold on HF and later it has become free, but not open-source. It has only some basic features such as download and execute, remote desktop, file manager and few more. Coded in C++ and ASM.

Runtime results ->[19/20](#) | Scantime results ->[21/26](#)

As you can see the results of non-obfuscated payloads are pretty much expected. Listed tools are available to buy by pretty much anyone. Most of them have very affordable price and they could compete with more expensive, but similar products. They are being used by a lot of customers, that means they must be bound with heuristic detections. Some crypters might find it hard to make undetectable output, especially when features are utilized or the plugin system that the heuristics kick into gear. One thing could be noticed, DarkVision RAT and PureHVNC Botnet have better

results without obfuscation, because they are quite new on the market and less popular. Anyway such malware is always being used in combination with crypters. So let's move to the main topic - runtime results of different crypters.

Unfortunately we didn't complete the tests with "dummy" payload, for example putty.exe which has no false positives and would give some more clear data.

About the crypters that are missing and initially we were about to test:

- DataEncoder refused to participate and told us that we are not allowed to post results, he also refunded us for the license.

- NanoShield was cooperative and wanted us to finish the tests, but unfortunately we didn't have enough time and the license expired.

In addition to this whole thread, pay special attention to the post linked below, made by [ishop](#), it gives more context, valuable and up-to-date information.

[RE: Crypter comparison | Mega thread | Runtime Results 2023 | Market research](#)

(May 13, 2023 07:48 AM)i.Shop Wrote: [\[CITE\]](#) Not sure this is the right place to post this but I'll give it a try and hope you will forgive me for this long read ?

I would like everyone to exercise your mind with me for a little bit and let me take you into "paranoid of being detected" mode:

Paranoid number One - Crypted file should be clean by itself

Considering the tests results from previous posts and considering that this is a crypter comparison thread then I think an even better test could be performed to eliminate some of the "noise" and variance from these current results.

In order to understand this first let's consider this scenario with a focus on botnet software first:

Coder writes botnet software then distributes this to its fellow users.

Users take some crypt service to crypt the software.

They use it for a while, everyone is happy.

After some time or even at the genesis of the botnet software the coder or the client of this software decides to do a test run to the software without the crypter and launches in the wild his unencrypted but FUD file to some 500-1000 target machines.

Well from the moment the coder/user does that then an invisible chain reaction happens that takes a little time: AV products find this new file with no reputation whatsoever on machine getting executed and send this to its cloud scanning servers for further analysis. Cloud scanning reveals nothing then standard procedure for these files are to be sent to its fellow AV company AV-analysts employees to manually analyse the files then the analyst makes signatures for this unencrypted FUD file. He also trains his machine learning dataset with this file but this will be put into discussion a little bit later.

After some time the unencrypted botnet software is being detected by some AV products

After all of this now the user takes the file again crypts it and it's FUD on scan time and runtime starts to fail on some products and that cannot be reverted. It will be like this like forever or until software developer reFUD's the unencrypted software while doing runtime scan checks iterations as many as necessary. Since this is a large code base then there is a huge attack surface for signatures of AV's so the coder will have a lot of headache to fix this. But most probably the coder will not bother because it thinks it is crypter's job to do that.

The mistake here is of course that developer or client of the software had to launch this file unencrypted just because it worked ? which leads to this irreversible runtime detection which cannot be cleaned with any crypt software/service.

This leaves very few options to fix this like:

Software developer of the botnet could try to fix runtime detections and make his own crypt and deliver both of them always inseparable from each other

Or each botnet owner make his own software and be careful to always distribute the file only crypted.

In the end here is what could be done about the crypter in order to see how good it is statistically speaking:

In order to eliminate the risk that botnet software could be tainted by the previous scenario and most probably is then we should remove botnet software out of the picture for these tests.

We should be making a dummy payload .exe .bat file that is/was never sent in the wild that has 0 runtime detection or close to that (that can be done I have tested it myself) then this file should be crypted with the crypter candidates to see if they are able not to be detected with a dummy file for runtime detection.

Further test iterations can also be made by downloading a malware archive and throwing some parts of the binary of the well know malware into our payload .data then to .code section in order to specifically tune detection for a certain security product at runtime.

Also further iteration for tuning file .data and .code section and imports can be made.

This way I think noise variance is removed from the test results and will show how good a crypter is by itself.

Normaly the crypt that gives close to 0 runtime detections with the dummy file samples should be our best pick.

Then botnet software should have not been released into the wild then we are good to go for the lowest detection of a pair of crypt+software.

Paranoind number Two - Machine Learning already knows you at first sight

Machine Learning(ML) aka Artificial Intelligence(AI) algos have grown very powerful for security products in the last 5 years or so.

ML algos makes uses of scantime and runtime behavior to gather signals in order to get a picture of how a payload looks or behaves.

Some of the signals are:

- Static scanning signals like: size of the file, file sections (.data .text or others) presence or size of those sections, file imports, visible strings in the sample file, icons, certificates, others resources etc..

- Runtime scanning like sensitive API calls, persistence events, network connections or behavior while communicating, files executed or dropped. Sample file name or dropped files name. (BTW this should not be confused with sandbox analysis)

- Environmental context while executing a file and or execution chain that follows. Meaning which app launched the sample file. Was it powershell/cmd execution? Was it being launched from explorer? Was it being launched from a browser ? Was it downloaded from a browser as archive then extracted then executed? And so on.. All of this is also logged by the ML engine running on machine side in realtime.

Now basically ML gathers all those signals without knowing what's under the hood of the crypt actually then compiles sort of fingerprint out of all these signals then some security product analyst manually categorize this fingerprint as good/bad then inserts it into ML database on the product.

By doing this they actually train their ML model to recognize new samples that where never seen

before and based on their signal count match they then put a "tag" on that newly seen sample into being good, suspicious or bad. For example if is an upgraded version of a very used good software then is safe to assume is a good sample, or if is a recrypt/upgrade of a bad malware then is safe to assume that this is a bad sample, or sample is a suspicious one.

In case file is suspicious then some AV products employs sandboxing of that launched file while letting it launch on the machine. This of course will put some limitations of that sandboxing such as readonly filesystem as a whole or parts of it. Persistence does not hold in this case.

A suspicious execution in a sandboxed environment which could have be avoided should be considered fault of the crypt.

Some security products that employs such sandboxing are: Comodo, Kasperksy, McAfee, Fortinet

Normally ML algos need cloud detection to be enabled in order to work at their full power. Scantime detection services has ML disabled to a considerable degree. That includes services like avcheck and even VirusTotal on some of their AV products.

Controlled runtime scanning even with cloud scanning enabled does not takes into account the environmental context of the sample execution which has been lost or not provided.

When context is lost then runtime detections don't happen in controlled scanning environment and crypt developer thinks he won the battle. But actually when there is context then file has higher chances being detected in the wild as well.

Back on the ML training model we see that AV companies has now a very big database collection of those signal fingerprints. While matching this huge DB against a new sample, even a good benign one you might find it surprisingly that some of them could be detected as malware causing false positive detection even if they ain't and this is because some malware can have similar fingerprint to a benign software file and they will tend to match to a high degree.

This why crypt coder has to find a new recipe for its stub for creating a file fingerprint which by chance dos not cross-interfere with the existing ones in that huge DB.

This of course create a challenge for crypt coder to come up with new out of the box thinking all of the time in order to succeed.

The change of file icon for example that has been talked about to optimize file detection is because of that false positive detection of an already made malware that is similar

Just because some other person out there already used a similar crypt design with similar icon that is why now file is being detected even if has not been spread in the wild yet.

Here is a practical real example of ML into action:

Nowadays WD on Windowns 11 started to be acting differently that WD on Windows 10 when the same sample file is executed on them.

WD 11 now has the same detection algos and signatures as WD 10 but WD 11 has now a more aggressive approach when comes to ML detection.

While creating a undetected file and scanning it and even launching on WD 11 from explorer all could work just fine but after taking it a bit further:

1. making an archive and put file into archive and download this file from a host you might notice that WD 11 pops that payload is detected compared to just bringing the payload in WD 11 by other means and just executing it.

2. launching file from a shell script would make WD 11 change its behavior and consider that payload file is actually a malware

So as you can see its a mixture of how suspicious is a file plus its execution context in order to obtain best results

Now let's sum this up: A crypter is not enough to secure file detection to a maximum. There should be a testing of the whole pairing of: execution chain context + crypt + botnet software

After establishing the real case scenario of execution context we could then crypt the software and

adjust parameters of the crypt and/or botnet software in such a way that ML detection is reduced to a minimum. In such a case good tools like scanner.to cannot control the execution context because is automated. Because of this a crypter coder would have to deploy its whole runtime scanning system for at least the most common security products out there in order to be able to reproduce the exact execution context for each software that is being used with the the crypt.

Based on some study of mine. Having general audience traffic of installs (that does not includes corporations, just regular people target machines) then usually traffic distribution by AV product as follows: has about 30% WD 10 , about 30% WD 11, about 20% McAfee, about 5% Avast/AVG. Products which are the most used.

So at least for these the whole pair of context+crypt+botnet software should be tested and fine tuned on those to obtain the best detection results.

A crypted software that has pass ML as suspicious should be considered as a failure because sandbox will only offer initial execution of that payload because cannot obtain persistence in any way. Crypter+Software should be refined in such a way that ML suspicion status of the file to be removed

To conclude all of this:

I think in order to have best results would be that just one coder to create a monolith software that has it all-in-one, crypt + botnet software + well tested in the wild against all detections technologies of present, that's the only way to control detection at its best

But we can also accept compromise since the perfect outcome is very hard to achieve involving very hard work from the coder perspective which also tries to make his living out of this.

Bringing a sample file to being clean 60-70% on a real case execution scenario is now achievable but the difference of going from that 60-70% to up to a 100% is getting very harder to do by each additional 1% gained on top of that 60-70%.

We can either be "paranoid of being detected" or just make compromise and accept that shared commercial software has its limitations.

Thank you for reading, please leave a QL or HQ post if you enjoyed it.

Stay tuned for more content.

Sincerely, LEGENDS

scanbuddy - February 26, 2023, 8:51 am

Shared between all customers, monthly subscription crypters:

[Contracted customer review](#)

[PureCrypter](#) + Spoiler ([Click to View](#))

+ [BlueLoader Botnet](#) | Runtime results ->[11/20](#) | Scantime results ->[2/26](#)

+ [PureMiner Botnet](#) | Runtime results ->[11/20](#) | Scantime results ->[2/26](#)

+ [PureHVNC Botnet](#) | Runtime results ->[8/20](#) | Scantime results ->[2/26](#)

+ [PureLogs Stealer](#) | Runtime results ->[7/20](#) | Scantime results ->[1/26](#)

+ [DarkVision RAT](#) | Runtime results ->[8/20](#) | Scantime results ->[1/26](#)

+ [WarZone RAT](#) | Runtime results ->[10/20](#) | Scantime results ->[2/26](#)

+ [Babylon RAT](#) | Runtime results ->[11/20](#) | Scantime results ->[2/26](#)

[Contracted customer review](#)

[ByteCrypter](#) + Spoiler ([Click to View](#))

+ [BlueLoader Botnet](#) | We couldn't build a working payload and get these products working together.

+ [PureMiner Botnet](#) | We couldn't build a working payload and get these products working together.

+ [PureHVNC Botnet](#) | We couldn't build a working payload and get these products working together.

+ [PureLogs Stealer](#) | We couldn't build a working payload and get these products working together.

+ [DarkVision RAT](#) | We couldn't build a working payload and get these products working together.

+ [WarZone RAT](#) | Runtime results ->[17/20](#) | Scantime results ->[15/26](#)

+ [Babylon RAT](#) | Runtime results ->[17/20](#) | Scantime results ->[15/26](#)

Private crypters and handmade crypts:

[ScrubCrypt | Contracted customer review](#)

- [ScrubCrypt](#) + [BlueLoader Botnet](#) | Runtime results ->[8/20](#) | Scantime results ->[0/26](#)

Bypassing: Windows Defender, Kaspersky, Malwerbytes, McAfee, Norton

- [ScrubCrypt](#) + [PureMiner Botnet](#) | Runtime results ->[6/20](#) | Scantime results ->[2/26](#)

Bypassing: Windows Defender, Avast, AVG, Kaspersky, Malwerbytes, McAfee, Norton

[RazCrypt | Contracted customer review](#)

- [RAZ Crypt](#) + [BlueLoader Botnet](#) | Runtime results ->[7/20](#) | Scantime results ->[0/26](#)

Bypassing: Windows Defender, Eset, Kaspersky, Malwerbytes, McAfee

- [AAA+ Crypt](#) + [BlueLoader Botnet](#) |

- [Stacks Helium](#) + [BlueLoader Botnet](#) |

SIM-5284310 - February 26, 2023, 9:25 am

nice thread. i'm using nanoshield too and tried to buy another crypters.

the feedback of nanoshield's seller and crypter's bypass quality is the best.

the purecrypter was also useful but the problem is that the bypass method that using powershell can not bypass V3 AV even scantime and runtime test was bypassed.

compare to that, nanoshield can bypass V3 and Windows Defender as well.

Frost Crypt - February 26, 2023, 10:23 am

just few things to add. I see you did some runtime scan with 6/26 scantime, what's the point of doing that since most detections will be scantime not runtime, checking a 1/26 file for runtime is fine, probably a simple icon change would have fix those high detections, you can notice the 1/26 got the best runtime results.

Also my crypter bypassed WD with the right settings, my customers can confirm.

Also I sell private stubs too not only shared.

Other than that, good job

Azx31 - February 26, 2023, 11:02 am

Really interested to see how private stubs perform

Ph4n70M Phr34K - February 26, 2023, 11:11 am

(Feb 26, 2023 11:23 AM)Nano Shield Wrote: [\[CITE\]](#) just few things to add. I see you did some runtime scan with 6/26 scantime, what's the point of doing that since most detections will be scantime not runtime, checking a 1/26 file for runtime is fine, probably a simple icon change would have fix those high detections, you can notice the 1/26 got the

We have tried many different settings and combos with different tools, always trying to get the best and most accurate results possible. At the time of doing latest tests we couldn't get better scantime results. Feel free to let us know when you push a fresh stub, because as we said already we will be doing all the tests again.

Procedure of testing is simple:

1. Crypt payload
2. Check on VM if payload works
3. Check scantime results and try to get best results with different icons and assembly
4. Check runtime scan

We can also give you the same payloads and free runtime scans if you want to.

(Feb 26, 2023 11:23 AM)Nano Shield Wrote: [\[CITE\]](#) Also my crypter bypassed WD with the right settings, my customers can confirm.

Also I sell private stubs too not only shared.

Let us know what tools and settings we should use to get the best results. We will be happy to test your private crypt as well.

(Feb 26, 2023 11:23 AM)Nano Shield Wrote: [\[CITE\]](#) Other than that, good job

Thanks, main purpose of this thread and idea is to make crypter developers to improve their software and make compatible with most of popular malware.

(Feb 26, 2023 12:02 PM)Azx31 Wrote: [\[CITE\]](#) Really interested to see how private stubs perform
In most cases, much better.

POLLUX - February 28, 2023, 8:15 am

Very interesting thread, I'm looking forward to the results.

However, it should be noted, especially for beginners, that the crypt with the least detections is not always the best. I have tested many different crypts from different sellers and at some point I stopped counting with how many I had problems like a low connection rate, not mining bots, not working WD exclusions and more.

Anyway, this thread is good to show people the right way.

scanbuddy - February 28, 2023, 8:30 am

(Feb 28, 2023 09:15 AM)MRKTRK Wrote: [\[CITE\]](#) Very interesting thread, I'm looking forward to the results.

However, it should be noted, especially for beginners, that the crypt with the least detections is not always the best. I have tested many different crypts from different sellers and at some point I

stopped counting with how many I had problems like a low connection rate, not mining bots, not working WD exclusions and more.

Anyway, this thread is good to show people the right way.

Thanks, we only scan working builds as you can see in

<https://hackforums.net/showthread.php?tid=6233658&pid=61888511#pid61888511>

Royal ! - February 28, 2023, 9:22 am

(Feb 26, 2023 09:51 AM)scanbuddy Wrote: [\[CITE\]](#) -Snip-

So you just crypted files using my crypter, then when you have had any detection issue, then you are supposed to contact me for CUSTOMER SUPPORT and get your issue resolved. If am not able to resolve it, then you move on and post these results. But as of now, these results are NOT VALID at all because you NEVER CONTACTED me, At all.

I even see in your so called review you said "We couldn't build a working payload and get these products working together". So what did you do about that?. Your FIRST JOB was that if you couldn't get a file working with byte crypter, you contact me and ask me to get it resolved for you, but you did not?.

All this time you waited and waited just to post results in this thread?. Seriously?. I smell something fishy here.

=====

Further, this is a TOTALLY POINTLESS thread based on few factors-:

*Crypters often get refuted/updated regularly, and so the detection rate changes. So this thread is based on what?. What is the foundation of this thread?. If one crypter is getting good results one day, does not mean the next day it will be same. And same goes for any "bad result".

*Crypter sellers provide customer support to their customers to get their detection issue resolved, if they get detection issues that does not mean the product is "bad" or you are exposing some real "truth" about any product. That means either the crypter is pending REFUD/UPDATE or the Customer is requiring customer support from the seller. Sellers are NOT supposed to keep OP Updated about latest refud scans or results, that again makes this thread pointless.

*@OP, you are NOT a customer of mine. And if you are trying to "sneak in" to produce results, you are doing a clear violation of site policies.

Lastly, if you have had posted this thread about some mainstream tools like a remote admin tool, any miner, any other one time "buy and use forever" type product I would have understood the point of this thread.

But creating such threads about "crypters" makes no sense whatsoever.

Good luck with this thread.

Ph4n70M Phr34K - February 28, 2023, 9:58 am

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) So you just crypted files using my crypter, then when

you have had any detection issue, then you are supposed to contact me for CUSTOMER SUPPORT and get your issue resolved. If am not able to resolve it, then you move on and post these results. But as of now, these results are NOT VALID at all because you NEVER CONTACTED me, At all. I even see in your so called review you said "We couldn't build a working payload and get these products working together". So what did you do about that?. Your FIRST JOB was that if you couldn't get a file working with byte crypter, you contact me and ask me to get it resolved for you, but you did not?.

The thing is that besides the "detection issue", the crypter doesn't work at all with most of the tools, we have tried almost all possible combinations of settings. It only worked with WarZone and Babylon, which are a bit obsolete being honest. Statement that "We couldn't build a working payload and get these products working together" fully describes in short our experience. We didn't have this issue with any other crypter. This is all besides ~20 scantime detections. It is worth mentioning that you are encouraging people to use two cracked obfuscators on top of your crypter.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) All this time you waited and waited just to post results in this thread?. Seriously?. I smell something fishy here.

Being honest, no idea what you mean. We have been testing many tools with different crypters, it took a lot of effort, time, money to complete. This is how a market research should be done.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) *@OP, you are NOT a customer of mine. I think this is the only true thing in your entire post

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) And if you are trying to "sneak in" to produce results, you are doing a clear violation of site policies. I'm not trying anything, i didn't use your product.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) Lastly, if you have had posted this thread about some mainstream tools like a remote admin tool, any miner, any other one time "buy and use forever" type product I would have understood the point of this thread.

Again i have no clue what you mean, this is exactly what you said, a thread about some mainstream tools, rats, botnets, crypters and other popular malware. Basic market research for newcomers.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) But creating such threads about "crypters" makes no sense whatsoever.

So far everyone mentioned in this thread liked the idea and some even contributed with discounts and licenses. With that being said i think that creating such threads makes hell a lot of sense.

scanbuddy - February 28, 2023, 10:26 am

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) So you just crypted files using my crypter, then when you have had any detection issue, then you are supposed to contact me for CUSTOMER SUPPORT and get your issue resolved. If am not able to resolve it, then you move on and post these results. But as of now, these results are NOT VALID at all because you NEVER CONTACTED me, At all.

In the crypting test we have followed the 8 minutes long video guide included in the product files. In 4th minute you guide us to obfuscate the crypted file with Confuser 1.9.0.0 (open source tool from 2012)

and .NET Reactor 4.9.0.0 (cracked tool from 2015).

How would updating the crypter help if we obfuscate the crypted file with detected obfuscators? Not to mention that rarely will any file work after crypting and obfuscating with 2 obfuscators.

If there is new crypting guide, please send it to us and we will test again.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) I even see in your so called review you said "We couldn't build a working payload and get these products working together". So what did you do about that?. Your FIRST JOB was that if you couldn't get a file working with byte crypter, you contact me and ask me to get it resolved for you, but you did not?.

We did tests with the products we received. We can test again if you send us an update.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) All this time you waited and waited just to post results in this thread?. Seriously?. I smell something fishy here.

We had many tests to do, not just Byte Crypter.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) Further, this is a TOTALLY POINTLESS thread based on few factors:-

*Crypters often get refuted/updated regularly, and so the detection rate changes. So this thread is based on what?. What is the foundation of this thread?. If one crypter is getting good results one day, does not mean the next day it will be same. And same goes for any "bad result".

Scantime will not change if you obfuscate the file after crypting.

If scantime is not FUD then runtime will not be either.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) *Crypter sellers provide customer support to their customers to get their detection issue resolved, if they get detection issues that does not mean the product is "bad" or you are exposing some real "truth" about any product. That means either the crypter is pending REFUD/UPDATE or the Customer is requiring customer support from the seller. Sellers are NOT supposed to keep OP Updated about latest refud scans or results, that again makes this thread pointless.

We tried updating the crypter stub several times. It seems to be "pending REFUD/UPDATE" for a while now.

(Feb 28, 2023 10:22 AM)Royal ! Wrote: [\[CITE\]](#) *@OP, you are NOT a customer of mine. And if you are trying to "sneak in" to produce results, you are doing a clear violation of site policies.

I am your customer.

Order ID: 883b3b37-0732-47a0-a4b6-f29e4c3ae0a6

Amount Gateway Date purchased

US\$35.00 BTC February 18, 2023

Contract: <https://hackforums.net/contracts.php?action=view&cid=361075>

YAK_CODER - February 28, 2023, 11:02 am

this thread is sick

what the point of all of this?

every crypter have its users that are happy

so dont judge what u dont or cant own

simple

YAK_CODER - February 28, 2023, 11:24 am

(Feb 28, 2023 12:11 PM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) This is just a market research as it says.

We own crypter licences, we bought them and reviewed.

We would be happy to review YAK Crypt.

(Feb 28, 2023 12:17 PM)Dyne Wrote: [\[CITE\]](#) No disrespect to you, as I acknowledge and respect your previous accolades and accomplishments, however;

Discussion about smart purchase decisions is allowed and should be allowed. Market research and understanding is allowed.

When you purchase an item, do you rely solely on what the listing tells you? or do you look to consumer reviews first?

These users actively purchased licenses to extract a market sample. This is not wrong and should be encouraged.

I bid you good luck in your journeys and hope you have been well.

I can agree if you arrange the test with the coder (not a user that can be a newbe) at least as some guys say 1/26 scantime file is good for next step the runtime test but as i know the thread writer with all respect we just need fair review (with the coder help) so u give him all the chance

wtfpop - March 1, 2023, 6:13 am

(Feb 26, 2023 09:51 AM)scanbuddy Wrote: [\[CITE\]](#) [ScrubCrypt | Contracted customer review](#)

- [ScrubCrypt](#) + [BlueLoader Botnet](#) | Runtime results ->[8/20](#) | Scantime results ->[0/26](#)
Bypassing: Windows Defender, Kaspersky, Malwerbytes, McAfee, Norton

- [ScrubCrypt](#) + [PureMiner Botnet](#) | Runtime results ->[6/20](#) | Scantime results ->[2/26](#)
Bypassing: Windows Defender, Avast, AVG, Kaspersky, Malwerbytes, McAfee, Norton
We have since updated ScrubCrypt to fix the Bitdefender and Adaware scantime detection. ?
Steps have been taken to improve consistency with runtime results.

cesilia732 - March 1, 2023, 7:53 am

Do you plan to add more crypters in the future to this thread ?

I would love to see yakuza crypter and warzone crypter
and thanks for all the work for this thread mate

YAK_CODER - March 1, 2023, 10:09 am

i will join with no doubt
just contacted the thread owner
for a test

POLLUX - March 1, 2023, 10:31 am

(Mar 1, 2023 11:09 AM)YAK_CODER Wrote: [\[CITE\]](#) i will join with no doubt
just contacted the thread owner
for a test

Good decision, someone who is not participating in something like this can't be really convinced of his own product.

pepperJelly - March 1, 2023, 11:44 am

Thanks for this thread. Vey usefull.

Geofry Handsome - March 1, 2023, 11:50 am

I love this thread, and all the answers and claims speak for them self. Lots of future customers of crypters will be thankful to have this as a help to make a decision weather they buy a crypter and from whom.

I am very thankful for all the efforts which are done here to help the community to figure out which product fits their desires.

Personally I won't use any crypter from Hackforums or elsewhere. It's just pointless as soon as you figured out how to make your files FUD or UD. But it will help those, who are not able or willing to do this work on their own.

Thanks a lot.

pepperJelly - March 1, 2023, 11:53 am

I wonder when we are going to start seeing software to change the signature of malware with AI.
I also wonder when the first AI antivirus will come out.

POLLUX - March 1, 2023, 12:28 pm

(Mar 1, 2023 12:53 PM)pepperJelly Wrote: [\[CITE\]](#) I wonder when we are going to start seeing software to change the signature of malware with AI.
I also wonder when the first AI antivirus will come out.
I am looking forward to the first AI crypter thread ?

pepperJelly - March 1, 2023, 12:30 pm

I'll be scared of the first AI crypter thread

YAK_CODER - March 1, 2023, 12:50 pm

(Mar 1, 2023 11:31 AM)MRKTRK Wrote: [\[CITE\]](#) Good decision, someone who is not participating in something like this can't be really convinced of his own product.

A test file have been sent to thread owner

(Mar 1, 2023 01:50 PM)YAK_CODER Wrote: [\[CITE\]](#) A test file have been sent to thread owner
As expected

crypted file sent to them since 21 hours

still didnt tested

and hope they dont do as it must be dirty on all this time

as its public stub

Ph4n70M Phr34K - March 2, 2023, 10:47 am

(Mar 1, 2023 01:50 PM)YAK_CODER Wrote: [\[CITE\]](#) A test file have been sent to thread owner

As expected

crypted file sent to them since 21 hours

still didnt tested

and hope they dont do as it must be dirty on all this time

as its public stub

I'm not online 24/7. You could have just scan it yourself as i advised you. You only sent me a random file, without even saying what it is.

I would need to be a "contracted customer" of yours if you want me to post results for your crypter.
You would need to take my payloads and send them back encrypted...

POLLUX - March 2, 2023, 11:06 am

(Mar 1, 2023 01:50 PM)YAK_CODER Wrote: [\[CITE\]](#) A test file have been sent to thread owner

As expected

crypted file sent to them since 21 hours

still didnt tested

and hope they dont do as it must be dirty on all this time

as its public stub

Not sure what to think if your crypts have an expected FUD time of less than 24 hours. However, maybe you go the "official" way with OP, start a contract, use his payload and then he is able to test and review it.

Ph4n70M Phr34K - March 2, 2023, 11:10 am

(Mar 2, 2023 12:06 PM)MRKTRK Wrote: [\[CITE\]](#) Not sure what to think if your crypts have an expected FUD time of less than 24 hours. However, maybe you go the "official" way with OP, start a contract, use his payload and then he is able to test and review it.

Thanks. One post with results has been removed because it was a marketplace violation.

To comply with hackforums rules, i need to have active contract and review need to be posted in sales thread. Then it could be copied and linked in my thread. Thats the only way.

HogWild - March 10, 2023, 9:23 pm

Really interesting, thanks for sharing!

?{ RadioActive Hack }? - March 15, 2023, 4:29 pm

Quality thread. Really interesting, for someone like me that hasn't used a cypher in many many years it's interesting to so how effective they are.

Great job boys.

affairsector - March 16, 2023, 8:46 am

Thank you for your contribution; you have saved me a significant amount of research time.

You may call me V - March 16, 2023, 3:13 pm

Thanks for sharing this, i really enjoyed it

scanbuddy - March 16, 2023, 5:25 pm

Unfortunately [Data Encoder](#) insisted on refunding my order thus refused to be reviewed in this comparison thread.

berserk3r - March 19, 2023, 4:32 am

Wow! amazing thread thank you man, this will help a lot to avoid false advertising and claiming!

DI?E - March 21, 2023, 11:47 am

(Mar 1, 2023 01:28 PM)MRKTRK Wrote: [\[CITE\]](#) I am looking forward to the first AI crypter thread ? Should go check out the Dark AI section. Already a few users who have managed to do so. I have as well. As far as the OP's thread I think this is a good thread to base decisions on and crypter sellers should join in on the discussion. Not only would it clear up a lot of questions it would also point out your products flexibility and quality.

youdigitalzdotcom - March 21, 2023, 10:51 pm

but how much can really be made from this as I have not really seen any one shown proof of earnings in this forum

iCasher - March 21, 2023, 11:14 pm

i would like to test my obfuscation method so can you pm me your patch and i will pm you back with the encrypted file but if it's not good don't share XD XD not looking to sell anytime soon anyway just testing if i am on the right path or not

nice thread btw

SIM-4716536 - April 2, 2023, 8:42 pm

good work and nice thread looking forward for more results and tests

wojack - April 2, 2023, 9:05 pm

damnnn thank you for your explanation and time!

johnpenta - April 9, 2023, 5:18 pm

Two questions:

- Is there a way to crypt a keylogger the way it will get executed even though user has no admin rights?

- Is there a way to crypt an android RAT that instead of installing an APK file the user will run an excel file or similar?

Thanks!

YAK_CODER - April 22, 2023, 7:00 am

i waste 45 \$ on

<https://scanner.to/>

Tested crypted # runtime internet on scan 180 sec

first test 4/21

<https://scanner.to/result/exES9PyXeA>

second test is wanna test how accurate is the site

so i just scan other file same stub

and do second scan 11/21

<https://scanner.to/result/Ua09f8BnAD>

the site is not helpful nor accurate

SIM-5300886 - April 22, 2023, 8:05 am

(Apr 22, 2023 07:00 AM)YAK_CODER Wrote: [\[CITE\]](#) i waste 45 \$ on

<https://scanner.to/>

Tested crypted # runtime internet on scan 180 sec

first test 4/21

<https://scanner.to/result/exES9PyXeA>

second test is wanna test how accurate is the site

so i just scan other file same stub

and do second scan 11/21

<https://scanner.to/result/Ua09f8BnAD>

the site is not helpful nor accurate

How can it not be accurate with video proof?

YAK_CODER - April 22, 2023, 9:10 am

you check video time

its 12 sec or 1 minute not 3 minus

something wrong and need be fixed

scanbuddy - April 22, 2023, 9:55 am

(Apr 22, 2023 07:00 AM)YAK_CODER Wrote: [\[CITE\]](#) i waste 45 \$ on

<https://scanner.to/>

Tested crypted # runtime internet on scan 180 sec

first test 4/21

<https://scanner.to/result/exES9PyXeA>

second test is wanna test how accurate is the site

so i just scan other file same stub

and do second scan 11/21

<https://scanner.to/result/Ua09f8BnAD>

the site is not helpful nor accurate

Hello, you scanned 2 different files. Check MD5 hash.

Video recording is stopped when detection appears.

No detection = video is 3 minutes.

YAK_CODER - April 22, 2023, 11:01 am

same crypter stub bro

with some change on junk

the idia here not attacking you or the site

we just need things to be better

very helpful on crypter work

to check how every line can make difference on runtime

(Apr 22, 2023 09:55 AM)scanbuddy Wrote: [\[CITE\]](#) Video recording is stopped when detection appears.

this is another point to talk about

lets say wd show msg that say

security scan required

why its counted as detection?

no dection appear

scanbuddy - April 22, 2023, 3:38 pm

(Apr 22, 2023 11:01 AM)YAK_CODER Wrote: [\[CITE\]](#) same crypter stub bro

with some change on junkApparently your edits affected AV behavior.

(Apr 22, 2023 11:01 AM)YAK_CODER Wrote: [\[CITE\]](#) the idia here not attacking you or the site

we just need things to be better

very helpful on crypter work

to check how every line can make difference on runtime

this is another point to talk about

lets say wd show msg that say

security scan required

why its counted as detection?

no dection appearWe will try to fix this rare notification problem.

Frost Crypt - April 23, 2023, 1:24 pm

(Apr 22, 2023 07:00 AM)YAK_CODER Wrote: [\[CITE\]](#) i waste 45 \$ on

<https://scanner.to/>

Tested crypted # runtime internet on scan 180 sec

first test 4/21

<https://scanner.to/result/exES9PyXeA>

second test is wanna test how accurate is the site

so i just scan other file same stub

and do second scan 11/21

<https://scanner.to/result/Ua09f8BnAD>

the site is not helpful nor accurate

but crypting different files can have different results, is 1 thing to crypt putty and another thing to crypt darkcomet, being the same stub

md5 is not the same

YAK_CODER - April 23, 2023, 4:31 pm

I JUST WANNA SAY THANKS TO

scanner.to

God bless you

i test every line

still work though

<https://scanner.to/result/SnQcW6DTHn>

thats rmcoss

no start up

added msg box to my stub itself

just to be sure thing executed

before main package

r**mcoss +startup no wd exclude code

<https://scanner.to/result/fUjAes7qdF>

im so happy to get this

all happen coz of this amazing runtime scanner

thx men

Cooligan - May 9, 2023, 2:17 am

Fantastic thread [Ph4n70M Phr34K](#), and very much so needed during today's crypter market.

I really hope this reaches a large majority of potential crypter customers on HF.

This would actually do really well as a sticky thread.

ElfSquad - May 9, 2023, 5:10 am

The topic is useful...but also not very

due to the fact that coders are updated every day, and no one wants to do a more up to date review

maybe the thread has some probability of truth, but consider the progress of encryption

Ph4n70M Phr34K - May 9, 2023, 5:19 am

(May 9, 2023 05:10 AM)ElfSquad Wrote: [CITE](#) The topic is useful...but also not very

due to the fact that coders are updated every day, and no one wants to do a more up to date review

maybe the thread has some probability of truth, but consider the progress of encryption

Without going into much details, you are totally wrong.

You need to fully read this thread to understand it.

ElfSquad - May 9, 2023, 5:29 am

(May 9, 2023 05:19 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) Without going into much details, you are totally wrong.

You need to fully read this thread to understand it.

I read the whole thing and realized that every cryptor updates his software every 3-4 days

although I agree with a lot of people.

Ph4n70M Phr34K - May 9, 2023, 5:59 am

(May 9, 2023 05:29 AM)ElfSquad Wrote: [\[CITE\]](#) I read the whole thing and realized that every cryptor updates his software every 3-4 days

although I agree with a lot of people.

You need to read the replies, not only OP.

Updates, doesn't mean that the crypter has been improved.

In most cases update is just about cleaning scantime detections.

In most cases it is just about slightly modifying the stub, changing encryption algorithm a bit, adding junk code and so on.

In most cases, i would say ALWAYS, the crypter performs exactly the same, runtime result is basically the same.

Take a look at ByteCrypter example. He doesn't update anything, even if he would push a new stub, he is encouraging people to use two cracked obfuscators on top of his crypter, so his update would be meaningless. It is indeed a drastic example, but straightforward.

ElfSquad - May 9, 2023, 7:19 am

(May 9, 2023 05:59 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) You need to read the replies, not only OP.

Updates, doesn't mean that the crypter has been improved.

In most cases update is just about cleaning scantime detections.

In most cases it is just about slightly modifying the stub, changing encryption algorithm a bit, adding junk code and so on.

In most cases, i would say ALWAYS, the crypter performs exactly the same, runtime result is basically the same.

Take a look at ByteCrypter example. He doesn't update anything, even if he would push a new stub, he is encouraging people to use two cracked obfuscators on top of his crypter, so his update would be meaningless. It is indeed a drastic example, but straightforward.

Re-read the thread, you're right. It's a shame, even.

I understand that the best crypt is a handheld crypt.

Bodyrot - May 11, 2023, 8:10 am

very HQ info here i read the entire post thanks for all the useful post, although its been a few months since posting this is bytencrypter still having issues creating useable stubs i was recently viewing that one only cause of price but mind kinda changed after reading this

i.Shop - May 13, 2023, 7:48 am

Not sure this is the right place to post this but I'll give it a try and hope you will forgive me for this long read ?

I would like everyone to exercise your mind with me for a little bit and let me take you into "paranoid of being detected" mode:

Paranoid number One - Crypted file should be clean by itself

Considering the tests results from previous posts and considering that this is a crypter comparison thread then I think a even better test could be performed to eliminate some of the "noise" and variance from these current results.

In order to understand this first let's consider this scenario with a focus on botnet software first: Coder writes botnet software then distributes this to its fellow users.

Users take some crypt service to crypt the software.

They use it for a while, everyone is happy.

After some time or even at the genesis of the botnet software the coder or the client of this software decides to do a test run to the software without the crypter and launches in the wild his unencrypted but FUD file to some 500-1000 target machines.

Well from the moment the coder/user does that then an invisible chain reaction happens that takes a little time: AV products finds this new file with no reputation whatsoever on machine getting executed and sends this to its cloud scanning servers for further analysis. Cloud scanning reveals nothing then standard procedure for these files are to be sent its fellow AV company AV-analysts employees to manually analyse the files then the analyst makes signatures for this unencrypted FUD file. He also trains his machine learning dataset with this file but this will be put into discussion a little bit later.

After some time the unencrypted botnet software is being detected by some AV products

After all of this now the users takes the file again crypt it and it's FUD on scantime and runtime starts to fail on some products and that cannot be reverted. It will be like this like forever or until software developer reFUD's the unencrypted software while doing runtime scan checks iterations as many as necessary. Since this is a large code base then there is a huge attack surface for signatures of AV's so the coder will have a lot headache to fix this. But most probably the coder will not bother because it thinks it is crypter's job to do that.

The mistake here is of course that developer or client of the software had to launch this file unencrypted just because it worked ? which leads to this irreversible runtime detection which cannot be cleaned with any crypt software/service.

This leaves very few options to fix this like:

Software developer of the botnet could try to fix runtime detections and make his own crypt and deliver both of them always inseparable from each other

Or each botnet owner make his own software and be careful to always distribute the file only crypted.

In the end here is what could be done about the crypter in order to see how good it is statistically speaking:

In order to eliminate the risk that botnet software could be tainted by the previous scenario and most probably is then we should remove botnet software out of the picture for these tests.

We should be making a dummy payload .exe .bat file that is/was never sent in the wild that has 0 runtime detection or close to that (that can be done I have tested it myself) then this file should be crypted with the crypter candidates to see if they are able not to be detected with a dummy file for

runtime detection.

Further test iterations can also be made by downloading a malware archive and throwing some parts of the binary of the well know malware into our payload .data then to .code section in order to specifically tune detection for a certain security product at runtime.

Also further iteration for tuning file .data and .code section and imports can be made.

This way I think noise variance is removed from the test results and will show how good a crypter is by itself.

Normaly the crypt that gives close to 0 runtime detections with the dummy file samples should be our best pick.

Then botnet software should have not been released into the wild then we are good to go for the lowest detection of a pair of crypt+software.

Paranoind number Two - Machine Learning already knows you at first sight

Machine Learning(ML) aka Artificial Intelligence(AI) algos have grown very powerful for security products in the last 5 years or so.

ML algos makes uses of scantime and runtime behavior to gather signals in order to get a picture of how a payload looks or behaves.

Some of the signals are:

- Static scanning signals like: size of the file, file sections (.data .text or others) presence or size of those sections, file imports, visible strings in the sample file, icons, certificates, others resources etc..
- Runtime scanning like sensitive API calls, persistence events, network connections or behavior while communicating, files executed or dropped. Sample file name or dropped files name. (BTW this should not be confused with sandbox analysis)
- Environmental context while executing a file and or execution chain that follows. Meaning which app launched the sample file. Was it powershell/cmd execution? Was it being launched from explorer? Was it being launched from a browser ? Was it downloaded from a browser as archive then extracted then executed? And so on.. All of this is also logged by the ML engine running on machine side in realtime.

Now basically ML gathers all those signals without knowing what's under the hood of the crypt actually then compiles sort of fingerprint out of all these signals then some security product analyst manually categorize this fingerprint as good/bad then inserts it into ML database on the product.

By doing this they actually train their ML model to recognize new samples that where never seen before and based on their signal count match they then put a "tag" on that newly seen sample into being good, suspicious or bad. For example if is an upgraded version of a very used good software then is safe to assume is a good sample, or if is a recrypt/upgrade of a bad malware then is safe to assume that this is a bad sample, or sample is a suspicious one.

In case file is suspicious then some AV products employs sandboxing of that launched file while letting it launch on the machine. This of course will put some limitations of that sandboxing such as readonly filesystem as a whole or parts of it. Persistence does not hold in this case.

A suspicious execution in a sandboxed evnironment which could have be avoided should be considered fault of the crypt.

Some security products that employs such sandboxing are: Comodo, Kasperksy, McAfee, Fortinet

Normally ML algos need cloud detection to be enabled in order to work at their full power. Scantime detection services has ML disabled to a considerable degree. That includes services like avcheck and even VirusTotal on some of their AV products.

Controlled runtime scanning even with cloud scanning enabled does not takes into account the environmental context of the sample execution which has been lost or not provided.

When context is lost then runtime detections don't happen in controlled scanning environment and

crypt developer thinks he won the battle. But actually when there is context then file has higher chances being detected in the wild as well.

Back on the ML training model we see that AV companies has now a very big database collection of those signal fingerprints. While matching this huge DB against a new sample, even a good benign one you might find it surprisingly that some of them could be detected as malware causing false positive detection even if they ain't and this is because some malware can have similar fingerprint to a benign software file and they will tend to match to a high degree.

This why crypt coder has to find a new recipe for its stub for creating a file fingerprint which by chance dos not cross-interfere with the existing ones in that huge DB.

This of course create a challenge for crypt coder to come up with new out of the box thinking all of the time in order to succeed.

The change of file icon for example that has been talked about to optimize file detection is because of that false positive detection of an already made malware that is similar

Just because some other person out there already used a similar crypt design with similar icon that is why now file is being detected even if has not been spread in the wild yet.

Here is a practical real example of ML into action:

Nowadays WD on Windowns 11 started to be acting differently that WD on Windows 10 when the same sample file is executed on them.

WD 11 now has the same detection algos and signatures as WD 10 but WD 11 has now a more aggressive approach when comes to ML detection.

While creating a undetected file and scanning it and even launching on WD 11 from explorer all could work just fine but after taking it a bit further:

1. making an archive and put file into archive and download this file from a host you might notice that WD 11 pops that payload is detected compared to just bringing the payload in WD 11 by other means and just executing it.

2. launching file from a shell script would make WD 11 change its behavior and consider that payload file is actually a malware

So as you can see its a mixture of how suspicious is a file plus its execution context in order to obtain best results

Now let's sum this up: A crypter is not enough to secure file detection to a maximum. There should be a testing of the whole pairing of: execution chain context + crypt + botnet software

After establishing the real case scenario of execution context we could then crypt the software and adjust parameters of the crypt and/or botnet software in such a way that ML detection is reduced to a minimum. In such a case good tools like scanner.to cannot control the execution context because is automated. Because of this a crypter coder would have to deploy its whole runtime scanning system for at least the most common security products out there in order to be able to reproduce the exact execution context for each software that is being used with the the crypt.

Based on some study of mine. Having general audience traffic of installs (that does not includes corporations, just regular people target machines) then usually traffic distribution by AV product as follows: has about 30% WD 10 , about 30% WD 11, about 20% Mcafee, about 5% Avast/AVG. Products which are the most used.

So at least for these the whole pair of context+crypt+botnet software should be tested and fine tuned on those to obtain the best detection results.

A crypted software that has pass ML as suspicious should be considered as a failure because sandbox will only offer initial execution of that payload because cannot obtain persistence in any way. Crypter+Software should be refined in such a way that ML suspicion status of the file to be removed

To conclude all of this:

I think in order to have best results would be that just one coder to create a monolith software that has it all-in-one, crypt + botnet software + well tested in the wild against all detections technologies of present, that's the only way to control detection at its best

But we can also accept compromise since the perfect outcome is very hard to achieve involving very hard work from the coder perspective which also tries to make his living out of this.

Bringing a sample file to being clean 60-70% on a real case execution scenario is now achievable but the difference of going from that 60-70% to up to a 100% is getting very harder to do by each additional 1% gained on top of that 60-70%.

We can either be "paranoid of being detected" or just make compromise and accept that shared commercial software has its limitations.

Frost Crypt - May 18, 2023, 12:15 am

latest windows updates gave me some trouble with defender but bypasses it again

<https://vimeo.com/828407356>

Ph4n70M Phr34K - May 20, 2023, 2:29 pm

(May 13, 2023 07:48 AM)i.Shop Wrote: [\[CITE\]](#) Not sure this is the right place to post this but I'll give it a try and hope you will forgive me for this long read ?

I would like everyone to exercise your mind with me for a little bit and let me take you into "paranoid of being detected" mode:

Paranoid number One - Crypted file should be clean by itself

Considering the tests results from previous posts and considering that this is a crypter comparison thread then I think a even better test could be performed to eliminate some of the "noise" and variance from these current results.

In order to understand this first let's consider this scenario with a focus on botnet software first:

Coder writes botnet software then distributes this to its fellow users.

Users take some crypt service to crypt the software.

They use it for a while, everyone is happy.

After some time or even at the genesis of the botnet software the coder or the client of this software decides to do a test run to the software without the crypter and launches in the wild his unencrypted but FUD file to some 500-1000 target machines.

Well from the moment the coder/user does that then an invisible chain reaction happens that takes a little time: AV products finds this new file with no reputation whatsoever on machine getting executed and sends this to its cloud scanning servers for further analysis. Cloud scanning reveals nothing then standard procedure for these files are to be sent its fellow AV company AV-analysts employees to manually analyse the files then the analyst makes signatures for this unencrypted FUD file. He also trains his machine learning dataset with this file but this will be put into discussion a little bit later.

After some time the unencrypted botnet software is being detected by some AV products

After all of this now the users takes the file again crypt it and it's FUD on scantime and runtime starts to fail on some products and that cannot be reverted. It will be like this like forever or until software developer reFUD's the unencrypted software while doing runtime scan checks iterations as many as necessary. Since this is a large code base then there is a huge attack surface for signatures of AV's so the coder will have a lot headache to fix this. But most probably the coder will not bother because it thinks it is crypter's job to do that.

The mistake here is of course that developer or client of the software had to launch this file

uncrypted just because it worked ? which leads to this irreversible runtime detection which cannot be cleaned with any crypt software/service.

This leaves very few options to fix this like:

Software developer of the botnet could try to fix runtime detections and make his own crypt and deliver both of them always inseparable from each other

Or each botnet owner make his own software and be careful to always distribute the file only crypted.

In the end here is what could be done about the crypter in order to see how good it is statistically speaking:

In order to eliminate the risk that botnet software could be tainted by the previous scenario and most probably is then we should remove botnet software out of the picture for these tests.

We should be making a dummy payload .exe .bat file that is/was never sent in the wild that has 0 runtime detection or close to that (that can be done I have tested it myself) then this file should be crypted with the crypter candidates to see if they are able not to be detected with a dummy file for runtime detection.

Further test iterations can also be made by downloading a malware archive and throwing some parts of the binary of the well know malware into our payload .data then to .code section in order to specifically tune detection for a certain security product at runtime.

Also further iteration for tuning file .data and .code section and imports can be made.

This way I think noise variance is removed from the test results and will show how good a crypter is by itself.

Normaly the crypt that gives close to 0 runtime detections with the dummy file samples should be our best pick.

Then botnet software should have not been released into the wild then we are good to go for the lowest detection of a pair of crypt+software.

Paranoind number Two - Machine Learning already knows you at first sight

Machine Learning(ML) aka Artificial Intelligence(AI) algos have grown very powerful for security products in the last 5 years or so.

ML algos makes uses of scantime and runtime behavior to gather signals in order to get a picture of how a payload looks or behaves.

Some of the signals are:

- Static scanning signals like: size of the file, file sections (.data .text or others) presence or size of those sections, file imports, visible strings in the sample file, icons, certificates, others resources etc..

- Runtime scanning like sensitive API calls, persistence events, network connections or behavior while communicating, files executed or dropped. Sample file name or dropped files name. (BTW this should not be confused with sandbox analysis)

- Environmental context while executing a file and or execution chain that follows. Meaning which app launched the sample file. Was it powershell/cmd execution? Was it being launched from explorer? Was it being launched from a browser ? Was it downloaded from a browser as archive then extracted then executed? And so on.. All of this is also logged by the ML engine running on machine side in realtime.

Now basically ML gathers all those signals without knowing what's under the hood of the crypt actually then compiles sort of fingerprint out of all these signals then some security product analyst manually categorize this fingerprint as good/bad then inserts it into ML database on the product.

By doing this they actually train their ML model to recognize new samples that where never seen before and based on their signal count match they then put a "tag" on that newly seen sample into being good, suspicious or bad. For example if is an upgraded version of a very used good software

then is safe to assume is a good sample, or if is a recrypt/upgrade of a bad malware then is safe to assume that this is a bad sample, or sample is a suspicious one.

In case file is suspicious then some AV products employs sandboxing of that launched file while letting it launch on the machine. This of course will put some limitations of that sandboxing such as readonly filesystem as a whole or parts of it. Persistence does not hold in this case.

A suspicious execution in a sandboxed environment which could have be avoided should be considered fault of the crypt.

Some security products that employs such sandboxing are: Comodo, Kaspersky, McAfee, Fortinet

Normally ML algos need cloud detection to be enabled in order to work at their full power. Scantime detection services has ML disabled to a considerable degree. That includes services like avcheck and even VirusTotal on some of their AV products.

Controlled runtime scanning even with cloud scanning enabled does not takes into account the environmental context of the sample execution which has been lost or not provided.

When context is lost then runtime detections don't happen in controlled scanning environment and crypt developer thinks he won the battle. But actually when there is context then file has higher chances being detected in the wild as well.

Back on the ML training model we see that AV companies has now a very big database collection of those signal fingerprints. While matching this huge DB against a new sample, even a good benign one you might find it surprisingly that some of them could be detected as malware causing false positive detection even if they ain't and this is because some malware can have similar fingerprint to a benign software file and they will tend to match to a high degree.

This why crypt coder has to find a new recipe for its stub for creating a file fingerprint which by chance dos not cross-interfere with the existing ones in that huge DB.

This of course create a challenge for crypt coder to come up with new out of the box thinking all of the time in order to succeed.

The change of file icon for example that has been talked about to optimize file detection is because of that false positive detection of an already made malware that is similar

Just because some other person out there already used a similar crypt design with similar icon that is why now file is being detected even if has not been spread in the wild yet.

Here is a practical real example of ML into action:

Nowadays WD on Windows 11 started to be acting differently that WD on Windows 10 when the same sample file is executed on them.

WD 11 now has the same detection algos and signatures as WD 10 but WD 11 has now a more aggressive approach when comes to ML detection.

While creating a undetected file and scanning it and even launching on WD 11 from explorer all could work just fine but after taking it a bit further:

1. making an archive and put file into archive and download this file from a host you might notice that WD 11 pops that payload is detected compared to just bringing the payload in WD 11 by other means and just executing it.

2. launching file from a shell script would make WD 11 change its behavior and consider that payload file is actually a malware

So as you can see its a mixture of how suspicious is a file plus its execution context in order to obtain best results

Now let's sum this up: A crypter is not enough to secure file detection to a maximum. There should be a testing of the whole pairing of: execution chain context + crypt + botnet software

After establishing the real case scenario of execution context we could then crypt the software and adjust parameters of the crypt and/or botnet software in such a way that ML detection is reduced to a minimum. In such a case good tools like scanner.to cannot control the execution context because

is automated. Because of this a crypter coder would have to deploy its whole runtime scanning system for at least the most common security products out there in order to be able to reproduce the exact execution context for each software that is being used with the the crypt.

Based on some study of mine. Having general audience traffic of installs (that does not includes corporations, just regular people target machines) then usually traffic distribution by AV product as follows: has about 30% WD 10 , about 30% WD 11, about 20% McAfee, about 5% Avast/AVG. Products which are the most used.

So at least for these the whole pair of context+crypt+botnet software should be tested and fine tuned on those to obtain the best detection results.

A crypted software that has pass ML as suspicious should be considered as a failure because sandbox will only offer initial execution of that payload because cannot obtain persistence in any way. Crypter+Software should be refined in such a way that ML suspicion status of the file to be removed

To conclude all of this:

I think in order to have best results would be that just one coder to create a monolith software that has it all-in-one, crypt + botnet software + well tested in the wild against all detections technologies of present, that's the only way to control detection at its best

But we can also accept compromise since the perfect outcome is very hard to achieve involving very hard work from the coder perspective which also tries to make his living out of this.

Bringing a sample file to being clean 60-70% on a real case execution scenario is now achievable but the difference of going from that 60-70% to up to a 100% is getting very harder to do by each additional 1% gained on top of that 60-70%.

We can either be "paranoid of being detected" or just make compromise and accept that shared commercial software has its limitations.

Im quoting this to make it visible. High quality post that should be read by everyone.

tamburro - May 22, 2023, 8:07 am

Wonderful post, It was just what I looking for....

I'm an old user since 2009 and quitting the scene, and now what I saw Is FUD became quite impossible to reach, unless you write your own Rat and offuscate It by code.

I see all the AVs have started to Scan the memory and Is quite simple to detect the sign of a PE file....

That Is my 50cent opinion....

Captain Pre - May 24, 2023, 2:29 am

Awesome thread.

I love how you are actively purchasing licenses to these products and not expecting freebies.

Great work!

MitsosMd - May 24, 2023, 6:49 am

So which crypter would you recommend me for pureminer I am kinda newbie

Ph4n70M Phr34K - May 24, 2023, 6:52 am

(May 24, 2023 06:49 AM)MitsosMd Wrote: [\[CITE\]](#) So which crypter would you recommend me for pureminer I am kinda newbie

For PureMiner i would recommend [CHRONOS](#)

I didnt use his service, but i know [mention=4873170] been using him for long time, combined with PureMiner.

Friendz - May 31, 2023, 8:11 am

A very comprehensive thread.

Nicely detailed report.

7 - May 31, 2023, 8:44 am

(Feb 23, 2023 10:35 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) Welcome in Crypter comparison mega thread. In this topic we will narrow you everything about crypters to help you understand what is being used nowadays, this would make your work easier. With so many crypters on the market to choose from, it can be overwhelming to make a decision. When you whittle them down, all crypters do essentially the same thing: protect your file from anti-virus software. So when we compare crypters, we have to get down to the most important aspect, detection at runtime.

There are many rumors around, such as that WD cannot be bypassed. In this thread we will debunk those. Before we proceed strictly with tests let us describe in general you what are crypters and how they work.

Crypters are in other words encrypting tools. They are used to obfuscate different type of files in order to protect them from cracking and analyzing and to bypass anti virus software. How does it work? There is many different types of encryption and injection methods and techniques to bypass anti virus software, so it would be really hard to list and describe everything, so in summary the image bellow illustrates very simply what a crypter does to your file.

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

Additionally you may read short the descriptions for most important terms and details. This introduction to crypters was originally written by KillaMuvz who was developing and selling crypters in the past. It explains features, options, settings, basic knowledge, detections, how to not ruin your payload and ultimately how not to annoy the crypter owner.

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

Everything you should know about crypters: [Crypter Terms and Definitions](#)

To compare the top crypters against each other, we use the same runtime scanner settings:

Internet ON

Cloud protection ON

Samples submission OFF

Duration 180 seconds

All runtime scans will be completed using <https://scanner.to/> and scantime <https://avcheck.net/>. We will also scan not obfuscated payloads to compare them with different crypting methods. That way will be able to see what exactly can be bypassed using different combinations of malware + crypter. The results will be presented not only as links but also by screenshots for better visibility. We will use paid and free tools listed below with each crypter tool.

- [BlueLoader Botnet](#)
- [PureMiner Botnet](#)
- [PureHVNC Botnet](#)
- [PureLogs Stealer](#)
- [DarkVision RAT](#)
- [WarZone RAT](#)
- [Babylon RAT](#) (FREE AND NATIVE)

We have also selected some of the most famous obfuscators from two sections:

[Cryptography and Encryption Market](#)
[Cryptography, Encryption, and Decryption](#)

Payloads for each tool will be build with minimal settings to ensure that we get the best results. This is also the most common way to use different malware with crypters, that most features are usually added by crypter. But in our tests we will also try to use minimal settings on crypter side, because we want to get the most accurate results for detections at runtime. Any exception of our standard or these basic rules will be listed for each malware and crypter and will be described and shown with screenshots.

Below you can also see the list of crypters that have been chosen for our tests.

Shared between all customers, monthly subscription crypters:

- [PureCrypter](#)
- [ByteCrypter](#)

Private crypters, handmade crypts:

- [ScrubCrypt](#)
- [RAZ](#)

So far, we have listed many different tools, among others free and paid rats, different botnet loaders, silent mining botnet, stealer and HVNC tool. We did also the same for most famous and known crypters being sold in Hackforums marketplace. All of these are available for purchase by anyone on here but some specified tools are being sold only on russian forums. Additionally if you don't have a general idea what is malware and how to use it you may read old e-book which is about starting up rats and http botnets. This e-book is a bit outdated but there is still a lot of good information's.

Spoiler ([Click to View](#))

Everything you should know about http botnets and rats: [Botnet E-book](#)

Below you can see the starting point for each payload. For better understanding we will also quickly describe each tool in case you never heard about them. Here you can also see runtime scan results for payloads that were not obfuscated yet.

[BlueLoader Botnet](#) Spoiler ([Click to View](#))

BlueLoader is advanced botnet with GUI that can hold large amount of bots and execute tasks with simple click. Coded in NET 4.0. Besides the loader(download & execute/update) it also has some additional features: Bot killer, visit website(hidden and visible) and ddos layer 7.

Runtime results ->[14/20](#) | Scantime results ->[12/26](#)

[PureMiner Botnet](#) Spoiler ([Click to View](#))

PureMiner is advanced cryptocurrency silent miner with GUI support for many different coins. Coded in .NET 4.0. It can auto decide if connected device could use GPU or CPU. It also has build-in proxy and some additional tasks and features.

Runtime results ->[13/20](#) | Scantime results ->[10/26](#)

[PureHVNC Botnet](#)Spoiler ([Click to View](#))

PureHVNC is advanced botnet with GUI that enables you to control any computer remotely and invisibly. Through it, you can use the mouse and keyboard in a hidden way, control the desktop, open browsers and other applications in a hidden way. Coded in NET 4.0.

Runtime results ->[12/20](#) | Scantime results ->[7/26](#)

[PureLogs Stealer](#)

Spoiler ([Click to View](#))

Runtime results ->[12/20](#) | Scantime results ->[10/26](#)

[DarkVision RAT](#)Spoiler ([Click to View](#))

DarkVision is a Windows Remote Administration Tool. It is based on a plugin architecture with memory mapped modules that never touches the disk, which allows for flexible loading of functionality on the remote system. Coded in C++ and ASM.

Runtime results ->[11/20](#) | Scantime results ->[8/26](#)

[WarZone RAT](#)Spoiler ([Click to View](#))

WarZone is advanced Remote Administration Tool packed with a lot of different features. The tool is very intuitive and works flawlessly. It's known from its high reliability and performance. Coded in C++.

Runtime results ->[17/20](#) | Scantime results ->[21/26](#)

[Babylon RAT](#)Spoiler ([Click to View](#))

Babylon is old Remote Administration Tool that was being sold on HF and later it has become free, but not open-source. It has only some basic features such as download and execute, remote desktop, file manager and few more. Coded in C++ and ASM.

Runtime results ->[19/20](#) | Scantime results ->[21/26](#)

As you can see the results of non-obfuscated payloads are pretty much expected. Listed tools are available to buy by pretty much anyone. Most of them have very affordable price and they could compete with more expensive, but similar products. They are being used by a lot of customers, that means they must be bound with heuristic detections. Some crypters might find it hard to make undetectable output, especially when features are utilized or the plugin system that the heuristics kick into gear. One thing could be noticed, DarkVision RAT and PureHVNC Botnet have better results without obfuscation, because they are quite new on the market and less popular. Anyway such malware is always being used in combination with crypters. So let's move to the main topic - runtime results of different crypters.

Unfortunately we didn't complete the tests with "dummy" payload, for example putty.exe which has no false positives and would give some more clear data.

About the crypters that are missing and initially we were about to test:

- DataEncoder refused to participate and told us that we are not allowed to post results, he also refunded us for the license.
 - NanoShield was cooperative and wanted us to finish the tests, but unfortunately we didn't have enough time and the license expired.
- I would like to see this thread progress.
Not sure how I feel about refusing to participate.. is that because they are too good and don't want to show anyone else up or the opposite.
Shame you didn't get to test with TOM hahahaha..... idiot
He only negged me because I said he can't crypt

Ph4n70M Phr34K - May 31, 2023, 9:02 am

(May 31, 2023 08:44 AM)NulldB Wrote: [\[CITE\]](#) I would like to see this thread progress.
There will be no progress, unless, someone is willing to pay for malware and crypts.

(May 31, 2023 08:44 AM)NulldB Wrote: [\[CITE\]](#) Not sure how I feel about refusing to participate.. is that because they are too good and don't want to show anyone else up or the opposite.
He didn't want to get exposed. Worth to mention that he refused to accept the contract after the sale. At this point it's pretty clear.
If he does accept the contract we would obviously post the results anyway.

7 - May 31, 2023, 9:03 am

(May 31, 2023 09:02 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) There will be no progress, unless, someone is willing to pay for malware and crypts.

He didn't want to get exposed. Worth to mention that he refused to accept the contract after the sale. At this point it's pretty clear.
who would you use now then? your personal choice

Ph4n70M Phr34K - May 31, 2023, 9:04 am

(May 31, 2023 09:03 AM)NulldB Wrote: [\[CITE\]](#) who would you use now then? your personal choice
I'm not up-to-date since I haven't been doing anything in that area for almost a year now

7 - May 31, 2023, 9:08 am

(May 31, 2023 09:04 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) I'm not up-to-date since I haven't been doing anything in that area for almost a year now
Yeah I wanna get my amadey up and running again
Need some solid crypter not one full of idiot skids

BadMoney - June 3, 2023, 6:04 pm

Wow, I just read through the entire thread
and I must say, THANK YOU. Thanks for
doing all the "Market Research" for us.
I'm as new as can be to this and so far
you guys have been the most helpful.
*Still confused, but we all gotta start somewhere!!

Ph4n70M Phr34K - June 15, 2023, 4:05 pm

(Jun 3, 2023 06:04 PM)BadMoney Wrote: [\[CITE\]](#) Wow, I just read through the entire thread

and I must say, THANK YOU. Thanks for doing all the "Market Research" for us. I'm as new as can be to this and so far you guys have been the most helpful. *Still confused, but we all gotta start somewhere!! At your service, sir. If you enjoyed this, then you would love to read my other threads.

SecuredNet - June 17, 2023, 12:21 am

Thanks you :) you guides are very nices

what is best
Babylon 1.6.0.0 or Babylon 1.7.0.0

Ph4n70M Phr34K - June 18, 2023, 10:40 am

(Jun 17, 2023 12:21 AM)SecuredNet Wrote: [\[CITE\]](#) Thanks you :) you guides are very nices

what is best
Babylon 1.6.0.0 or Babylon 1.7.0.0
The Babylon is already on its 23.4.0.18 stage, seems like you been missing a lot of updates.

SecuredNet - June 18, 2023, 3:32 pm

(Jun 18, 2023 10:40 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) The Babylon is already on its 23.4.0.18 stage, seems like you been missing a lot of updates.

Wtf ^^
have you a link?

Ph4n70M Phr34K - June 24, 2023, 12:22 pm

(Jun 18, 2023 03:32 PM)SecuredNet Wrote: [\[CITE\]](#) Wtf ^^
have you a link?
Yes, [here you go](#)

Ren And Stimpy - June 27, 2023, 11:41 am

Great thread! Thank you for reviewing all the software!

satisgam - June 28, 2023, 8:40 am

Thanks for the thread

Ph4n70M Phr34K - June 29, 2023, 9:41 am

Im seriously thinking about buying more crypts and doing tests.

ablationvector - July 6, 2023, 12:57 am

The user TOM scammed me out of \$135 euro for his "private crypt" service.

He is exploiting the "ignore member" feature so that you cannot dispute a contract. He was planning on scamming me from the start as he put me on his ignore list even before I was questioning if he had scammed me or not. I made the mistake of ignoring all the warning signs, please please don't make the same mistake I did and get scammed.

He first said it would take 6-48 hours, and then after 48 hours he said it would take 72 hours, and after that he said 5 more hours and then just completely stopped responding to me at all.

I don't care about the money I got scammed out of, I just really hope that other people don't have to

go through what I went through.

Please, please do yourself a favor and do not deal with this member; don't make the same mistake I did.

If anyone wants proof of telegram messages, just PM me.

Hopefully staff can fix this loophole so that other members don't get scammed like I did.

There are many more people he's scammed and gotten away with, please please save your money and do not get scammed by this user.

rooneyleo - July 9, 2023, 2:47 am

(Jul 6, 2023 12:57 AM)Joestar Wrote: [\[CITE\]](#) The user TOM scammed me out of \$135 euro for his "private crypt" service.

He is exploiting the "ignore member" feature so that you cannot dispute a contract. He was planning on scamming me from the start as he put me on his ignore list even before I was questioning if he had scammed me or not. I made the mistake of ignoring all the warning signs, please please don't make the same mistake I did and get scammed.

He first said it would take 6-48 hours, and then after 48 hours he said it would take 72 hours, and after that he said 5 more hours and then just completely stopped responding to me at all.

I don't care about the money I got scammed out of, I just really hope that other people don't have to go through what I went through.

Please, please do yourself a favor and do not deal with this member; don't make the same mistake I did.

If anyone wants proof of telegram messages, just PM me.

Hopefully staff can fix this loophole so that other members don't get scammed like I did.

There are many more people he's scammed and gotten away with, please please save your money and do not get scammed by this user.

tom is a fraud everyone knows that

coldhot1234 - July 12, 2023, 2:55 am

Thing most of the crypter in this forum are using opensource stuffs from github without changing anything and making fools to people including the crypter named R***C*** (people can understand i dont wanna take full name) how crypters like him are making fool to people.

A good crypter will always update the stub in every 1-2days and will always bypass atleast wd+cloud runtime

because in real life no one will download a file just to scan that file with avs they all gonna execute the file so concept of scantime does not get valid here only runtime matters.

In my personal exp i have seen that wd runtime varies from region to region say for example a file is

clean with runtime in COUNTRY X so it does not guarantee that the the same file will be clean in the COUNTRY Y.

So the overall summary is always check the crypt manually by your hand in your vm/vds with runtime and dont trust online scanners they never give any accurate results

OceanCrypter - July 13, 2023, 4:25 am

Legends? This guy should be kidding, the free crypters I make are better than the shitty products this guy sells, you have to stop smearing me. Or I'll make you regret it. These products have been of no use to the market and forum for years. The free crypter I made is better than these. Trust me lol

Ph4n70M Phr34K - July 13, 2023, 8:57 am

(Jul 13, 2023 04:25 AM)OceanCrypter Wrote: [\[CITE\]](#) Legends? This guy should be kidding, the free crypters I make are better than the shitty products this guy sells, you have to stop smearing me. Or I'll make you regret it. These products have been of no use to the market and forum for years. The free crypter I made is better than these. Trust me lol

You are not welcomed here.

Just go and scam people outside HF.

On HackForums you will always be exposed and banned.

For context: <https://hackforums.net/showthread.php?tid=6222007&page=3>

YAK_CODER - July 16, 2023, 9:04 am

i feel its bad days regarding this bloody war of russia an ukrainaia
its affect our fuckin work
affect all crypto market
even affect us on real life
wtf or its me only

Sowry - July 18, 2023, 4:39 am

This is really helpful.

I need the same test with the crypter of @Nano Shield.

It seems to be a serious competitor :)

P17CH - July 18, 2023, 7:58 am

Hey does anyone know how i would hide malware in an image, so when the image is opened the malware is run?

Ph4n70M Phr34K - July 18, 2023, 8:08 am

(Jul 18, 2023 07:58 AM)P17CH Wrote: [\[CITE\]](#) Hey does anyone know how i would hide malware in an image, so when the image is opened the malware is run?

That's only possible in movies, not in reality.

P17CH - July 19, 2023, 12:37 am

then how would i hide malware and trick people into downloading and executing it?

Ph4n70M Phr34K - July 25, 2023, 12:08 pm

Important read: <https://hackforums.net/showthread.php?tid=6222007&pid=62026435#pid62026435>

Poor scumbag going to be more active again.

drewkasp - July 25, 2023, 5:35 pm

Nice work OP...you the best!

neon_light - July 28, 2023, 1:53 pm

Many of us crypter sellers (aegistools.pw) also sell private stubs by the way.
It would be best to review the private stubs

Ph4n70M Phr34K - July 29, 2023, 2:32 am

(Jul 28, 2023 01:53 PM)neon_light Wrote: [\[CITE\]](#) Many of us crypter sellers (aegistools.pw) also sell private stubs by the way.

It would be best to review the private stubs

A while back ago you took 50\$ from me and blocked instantly. You have the nerve to self advertise in this thread?

The contract that you never accepted so i couldn't open a dispute:

<https://hackforums.net/contracts.php?action=view&cid=323733>

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

I couldn't care less about the 50\$, but you forgot about that?

You have been banned for 6 months and i thought you ditched this account already, seems like you continue your scamming practice instead.

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

You should not post in this thread.

Perhaps, i have another thread that fits you more:

<https://hackforums.net/showthread.php?tid=6222007>

picpic - August 5, 2023, 2:30 am

Wow ... Seeing the truth finally come out about all those scammers who've been ruining this site for years is a real pleasure ... A sort of revenge against their bad faith, where we usually got a -10 in popularity as soon as we dared to reveal the scam (Hello TOM !)

A few years ago, such a thread wouldn't have stayed online for long. Glad to see things are changing!

I also tested aegistools about two years ago and I can confirm that it was crap!

...What I don't understand, however, is how people like Royal! can still sell their product with impunity!

SIM-5084802 - August 7, 2023, 7:16 am

Wow, what a nice post! Many thanks for the time taken to do this, much appreciated!!

loadman - August 22, 2023, 10:20 am

this is my normal 50\$ crypt with customer's payload

<https://checkzilla.io/scan/fd776c40-4e87-4400-9d8e-19bf4b3e865d>

with internet on 180 seconds

<https://hackforums.net/showthread.php?pid=62063141#pid62063141>

probably the best results you can get with ur payload IN ENTIRE HF

open for review anytime

Nz1W0rm - September 19, 2023, 5:29 pm

This is very useful thread for nood like me, thanks for sharing your knowledge and time to test these cryptors

martigo333 - September 26, 2023, 1:54 pm

very nice thread, you guys are the best.

Transporter007 - September 27, 2023, 10:40 am

(Jul 29, 2023 02:32 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) A while back ago you took 50\$ from me and blocked instantly. You have the nerve to self advertise in this thread?

The contract that you never accepted so i couldn't open a dispute:

<https://hackforums.net/contracts.php?action=view&cid=323733>

Spoiler ([Click to View](#))

I couldn't care less about the 50\$, but you forgot about that?

You have been banned for 6 months and i thought you ditched this account already, seems like you continue your scamming practice instead.

Spoiler ([Click to View](#))

You should not post in this thread.

Perhaps, i have another thread that fits you more:

<https://hackforums.net/showthread.php?tid=6222007>

Same happened with me he took money and never reply.

raymundo - October 5, 2023, 7:57 am

(Feb 26, 2023 11:23 AM)Nano Shield Wrote: [\[CITE\]](#) just few things to add. I see you did some runtime scan with 6/26 scantime, what's the point of doing that since most detections will be scantime not runtime, checking a 1/26 file for runtime is fine, probably a simple icon change would have fix those high detections, you can notice the 1/26 got the best runtime results.

Also my crypter bypassed WD with the right settings, my customers can confirm.

Also I sell private stubs too not only shared.

Other than that, good job

Does nano shield have UAC bypass?

07days - October 5, 2023, 11:51 pm

Great post. I'll get back to it a bit later. Thanks!

vancy - October 23, 2023, 9:22 am

Very helpful thread.

scanbuddy - November 16, 2023, 3:14 pm

(Sep 21, 2023 12:28 AM)m0hx Wrote: [\[CITE\]](#) If anyone got scanner.to or checkzilla accounts dm me for testing. ty!

Post/DM your username to get 10 free scans at scanner.to!

xc0de - November 22, 2023, 7:21 am

do you sell silent exploit pdf,jpg,xls,docx?

Ph4n70M Phr34K - November 22, 2023, 8:34 am

(Nov 22, 2023 08:21 AM)xc0de Wrote: [\[CITE\]](#) do you sell silent exploit pdf,jpg,xls,docx?

Yes i do.

I also sell aliens and vehicles which are using light speed.

xc0de - November 22, 2023, 8:44 am

(Nov 22, 2023 09:34 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) Yes i do.

I also sell aliens and vehicles which are using light speed.

?????

celejpepa - November 29, 2023, 11:27 am

(Feb 26, 2023 10:25 AM)g0san Wrote: [\[CITE\]](#) nice thread. i'm using nanoshield too and tried to buy another crypters.

the feedback of nanoshield's seller and crypter's bypass quality is the best.

the purecrypter was also useful but the problem is that the bypass method that using powershell can not bypass V3 AV even scantime and runtime test was bypassed.

compare to that, nanoshield can bypass V3 and Windows Defender as well.

is this that nanoshield u talked about <https://nanoshield.pro>?

cltrade - December 11, 2023, 5:34 pm

Glad to see this thread.

Any updated suggestions on recommended crypter(s) to use now?

ScrubspooF - December 12, 2023, 5:56 am

(Dec 11, 2023 06:34 PM)cltrade Wrote: [\[CITE\]](#) Glad to see this thread.

Any updated suggestions on recommended crypter(s) to use now?

ScrubCrypt is for sale again, new 2.0 release on <https://scrubcrypt.ru>

ScrubspooF - December 12, 2023, 6:12 am

(Dec 12, 2023 07:06 AM)ZELOS Wrote: [\[CITE\]](#) Haven't you sold the source code to reggie?

Reggie and I agreed that it could continue to be sold. He also only paid me less than half the money for what he received.

RobinHood - December 12, 2023, 6:23 am

(Dec 12, 2023 06:56 AM)ScrubspooF Wrote: [\[CITE\]](#) ScrubCrypt is for sale again, new 2.0 release on <https://scrubcrypt.ru>

Can you please check your telegram?

cltrade - December 12, 2023, 6:26 am

(Dec 12, 2023 06:56 AM)ScrubspooF Wrote: [\[CITE\]](#) ScrubCrypt is for sale again, new 2.0 release on <https://scrubcrypt.ru>

Does it work with Darkvision and Rhadamanthys

ScrubspooF - December 12, 2023, 6:42 am

(Dec 12, 2023 07:23 AM)RobinHood Wrote: [\[CITE\]](#) Can you please check your telegram?

My telegram is @scrubspooF, you might be talking to the old one that someone hijacked.

(Dec 12, 2023 07:26 AM)cltrade Wrote: [\[CITE\]](#) Does it work with Darkvision and Rhadamanthys
Yes

ashsim - December 17, 2023, 5:46 pm

has anyone used atilla crypter here and the url exploit, if yes what were the results like?

shoto4meeee - December 24, 2023, 2:59 pm

please does anyone know FUD Crypter one can use

ogmack - December 25, 2023, 7:19 am

Thank you for taking the time to share this information with us Ph4n70M, from everything I've read

and understood, it's worth taking the time to create your own malware rather than buying one that's already known to anti-virus software, very interesting in any case, thank you.

Binance - January 7, 2024, 8:23 pm

The effort that went into this thread is amazing... thx for ur contribution...

Ph4n70M Phr34K - January 9, 2024, 10:49 am

(Jul 29, 2023 02:32 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) A while back ago you took 50\$ from me and blocked instantly. You have the nerve to self advertise in this thread?

The contract that you never accepted so i couldn't open a dispute:

<https://hackforums.net/contracts.php?action=view&cid=323733>

Spoiler ([Click to View](#))

I couldn't care less about the 50\$, but you forgot about that?

You have been banned for 6 months and i thought you ditched this account already, seems like you continue your scamming practice instead.

Spoiler ([Click to View](#))

You should not post in this thread.

Perhaps, i have another thread that fits you more:

<https://hackforums.net/showthread.php?tid=6222007>

Just a quick reminder, since this guy is still active and recently visited my profile.

Disgusting scum.

GOELU - January 17, 2024, 5:20 am

Guys can you recommend me 3 crypters right now that are staying long time

?BADMAN? - January 17, 2024, 5:36 am

(Jan 17, 2024 06:20 AM)GOELU Wrote: [\[CITE\]](#) Guys can you recommend me 3 crypters right now that are staying long time

I doubt that you will get something here that lasts longer than 2 days.

Tentco - January 17, 2024, 5:41 am

(Jan 17, 2024 06:36 AM)?BADMAN? Wrote: [\[CITE\]](#) I doubt that you will get something here that lasts longer than 2 days.

really?

alejandro752ska - January 19, 2024, 7:40 pm

what a HQ Thread thank u!

Basically almost any crypter (except one or two) here cant even bypass defender xD

Hacker2245 - January 21, 2024, 8:38 pm

time long i not read thread like this .. last thread i read like this maybe from 2009 2010 .. this thread UHQ for newbies devloper in world crypter , This is a great reference for beginners in this field .. i hope the moderators to pin this topic to this section because of its importance
thank you Ph4n70M Phr34K

(May 13, 2023 07:48 AM)i.Shop Wrote: [\[CITE\]](#) Not sure this is the right place to post this but I'll give it a try and hope you will forgive me for this long read ?

I would like everyone to exercise your mind with me for a little bit and let me take you into "paranoid of being detected" mode:

Paranoid number One - Crypted file should be clean by itself

Considering the tests results from previous posts and considering that this is a crypter comparison thread then I think a even better test could be performed to eliminate some of the "noise" and variance from these current results.

In order to understand this first let's consider this scenario with a focus on botnet software first:

Coder writes botnet software then distributes this to its fellow users.

Users take some crypt service to crypt the software.

They use it for a while, everyone is happy.

After some time or even at the genesis of the botnet software the coder or the client of this software decides to do a test run to the software without the crypter and launches in the wild his unencrypted but FUD file to some 500-1000 target machines.

Well from the moment the coder/user does that then an invisible chain reaction happens that takes a little time: AV products finds this new file with no reputation whatsoever on machine getting executed and sends this to its cloud scanning servers for further analysis. Cloud scanning reveals nothing then standard procedure for these files are to be sent its fellow AV company AV-analysts employees to manually analyse the files then the analyst makes signatures for this unencrypted FUD file. He also trains his machine learning dataset with this file but this will be put into discussion a little bit later.

After some time the unencrypted botnet software is being detected by some AV products

100% any devloper read your post will make a great crypter .. your post a Great source for newbies devloper crypter I hope everyone practices this ?

this is really problem ..

earthwonder442 - January 22, 2024, 4:33 pm

hey buddy, How's it going?

I need Crypter ASAP plus RAT.....How much?

Ph4n70M Phr34K - February 20, 2024, 11:54 am

Little update. BaitCrypter continues.

Roughly 2 years ago: Version 3.7.27

<https://hackforums.net/showthread.php?tid=6233658&pid=61888511#pid61888511>

Spoiler ([Click to View](#))

Today: Version 3.7.27

<https://hackforums.net/showthread.php?tid=6264283&pid=62283975#pid62283975>

Spoiler ([Click to View](#))

He is blatantly false advertising and deceiving people:

<https://hackforums.net/showthread.php?tid=6264283&pid=62284064#pid62284064>

"Why would I change the version or change the way how bytencrypter works?. I have bought selling rights to an already perfectly working product so why would I bother to change anything on the crypter?. I have just bought the rights to officially sell it and maintain it, simple."

No fucks given anymore.

Spoiler ([Click to View](#))

Ph4n70M Phr34K - February 28, 2024, 1:42 am

Its a misery for me how can someone be lying and deceiving people so blatantly.

Literally posting fake scan results in public, but in private acknowledging the fact its fake. Not worth

to mention it was proven by multiply members.

Poor Royal.

Spoiler ([Click to View](#))

Recent victim, one of the hundreds if not thousand:

Spoiler ([Click to View](#))

berserk3r - February 28, 2024, 4:59 am

All of those crypter are complete sh*t and useless I don't know why they pay for them, they worse no thing and just waste of money and time

CryptProvider - March 1, 2024, 10:09 pm

Hi I would like to participate, free crypt of course!

Voidlight - March 2, 2024, 5:29 am

would also like to offer a free crypt for a vouch/comparison

Ph4n70M Phr34K - March 2, 2024, 7:09 am

(Mar 1, 2024 11:09 PM)CryptProvider Wrote: [\[CITE\]](#) Hi I would like to participate, free crypt of course!

(Mar 2, 2024 06:29 AM)Voidlight Wrote: [\[CITE\]](#) would also like to offer a free crypt for a vouch/comparison

Sure folks ! There is a dedicated thread where you are welcomed

<https://hackforums.net/showthread.php?tid=6261188>

Cheers.

CryptProvider - March 2, 2024, 7:15 am

(Mar 2, 2024 08:09 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) Snip

Wishing you success.

I will never understand rep ABUSE, but to each their own.

Stanley - March 17, 2024, 9:44 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

Ph4n70M Phr34K - April 5, 2024, 10:18 am

Another victim of BaitCrypter aka Royal / Eladictocosity / gangushbo / neon_light / bigbronlet / SIM-2362145 / perhaps many more accounts.

Saving it here below before it gets deleted.

kabospy - July 1, 2024, 5:34 am

Please which crypter works perfectly with DarkVision RAT, I really need help

Luc1fer - July 6, 2024, 6:34 am

(Apr 5, 2024 10:18 AM)Ph4n70M Phr34K Wrote: [\[CITE\]](#) Another victim of BaitCrypter aka Royal / Eladictocosity / gangushbo / neon_light / bigbronlet / SIM-2362145 / perhaps many more accounts.

Saving it here below before it gets deleted.

Appreciate your thread.

"bigbronlet" contacted me on an account with a crypting thread since 2016 offering private crypts for only \$100 LIFETIME.

Knew anyone with 8 years experience crypting wouldn't do that, but how can he remain active since this has been "known" for apparently years?

Deterra - July 8, 2024, 2:25 pm

I always saw the use of public use crypter software as less efficient as hand made, but the best way is if crypts are maintained by hand rather than generated on the fly.

messi goat - October 20, 2024, 9:51 am

After reading several of your comments and interventions, your publications and your analyses on the different types of encrypting your interventions on scammers.

Your statistics are wonderful. As quoted on your profiles on hackforums for more information, I will want your advice more brief to buy an effective encrypter .thank you for giving me a name of an encrypter to buy the best of all.

thank you for your bra I am waiting for your return impatiently

.Thank you

warjero - October 25, 2024, 8:39 am

Hi, I'm having trouble connecting my DarkVision stub to PureCrypt. The server won't connect after I put it through the crypter.

I think I've tried all the settings correctly.

The server connects fine without encryption, but when I encrypt it it doesn't connect anymore.

Can anyone help me out?

Thanks a lot.

Backpack-Rucksack - October 30, 2024, 6:38 pm

After all, which one can you guys recommend?

Binance - November 14, 2024, 5:48 pm

(Oct 30, 2024 06:38 PM)Backpack-Rucksack Wrote: [\[CITE\]](#) After all, which one can you guys recommend?

The best recommendation is your own research.

This market changes daily, and understand WHAT you're buying. This is not magic button that says "crypt".

warjero - November 17, 2024, 7:13 am

I have contracted an encryption for my client VenomRat from the telegram user @asgard_bot_support but the file does not work, I have paid \$45 for an encryption. The file does not connect and they do not give me any solution. I do not trust this seller.

With PureCrypter it does work well but most of the time it is detected by WD.

I have contacted @R_A_Z_1 and I am going to try it now.
I will let you know how it goes when I have tried it.

Any encryption recommendations for venomrat?
Cheers

elcharro - December 12, 2024, 6:12 pm

how can I access to the software

(Nov 17, 2024 08:13 AM)warjero Wrote: [\[CITE\]](#) I have contracted an encryption for my client VenomRat from the telegram user @asgard_bot_support but the file does not work, I have paid \$45 for an encryption. The file does not connect and they do not give me any solution. I do not trust this seller.

With PureCrypter it does work well but most of the time it is detected by WD.

I have contacted @R_A_Z_1 and I am going to try it now.
I will let you know how it goes when I have tried it.

Any encryption recommendations for venomrat?
Cheers
did you try @R_A_Z_1 ? how was going?

woo097878781 - December 29, 2024, 4:54 am

I read a lot of your articles
thank you for your attentiveness

Hope you can publish an article about the latest encryptor tests in 2024
Hahaha

Many encryption devices are no longer what they used to be.
Most are impossible to get around, but all sell for high prices.
Meaningless and unhelpful to the market

I bought and tried many

everything is still there
Public stubs are pointless
This is still the case for runtime and static scans. I find such sales pointless.

(They can't be bypassed, it's best to use legal obfuscation code, the result will be the same)
Hahaha XDD

(Dec 12, 2024 07:12 PM)elcharro Wrote: [\[CITE\]](#) how can I access to the software

did you try @R_A_Z_1 ? how was going?
I have contacted and am waiting for shipment.

duck2 - January 1, 2025, 1:06 am

(Dec 29, 2024 05:54 AM)woo097878781 Wrote: [\[CITE\]](#) I read a lot of your articles
thank you for your attentiveness

Hope you can publish an article about the latest encryptor tests in 2024
Hahaha

Many encryption devices are no longer what they used to be.
Most are impossible to get around, but all sell for high prices.
Meaningless and unhelpful to the market

I bought and tried many

everything is still there
Public stubs are pointless
This is still the case for runtime and static scans. I find such sales pointless.

(They can't be bypassed, it's best to use legal obfuscation code, the result will be the same)
Hahaha XDD

I have contacted and am waiting for shipment.
what service did you try ?

woo097878781 - January 1, 2025, 4:57 am

(Jan 1, 2025 02:06 AM)duck2 Wrote: [\[CITE\]](#) what service did you try ?
Many encryption services

ettacuty - January 2, 2025, 4:30 pm

Contact @mayorofbrit on telegram a malware expert he may be able to recommend the best for you