

Forum: [Hack Forums](#)

Thread: [Madonna Crypt | C/ASM | No dependencies | LoadPE | RunPE](#)

donatellaversace - May 26, 2021, 12:05 pm

Madonna Crypts

Dear members of Hackforums,

I offer my private crypting service.

Technical information

Fully optimized for attacks

Full unicode support

Stubs are written in C/ASM

Stubs supports the entire line of modern windows

Native 100% with no dependencies (not depending on .NET framework.)

Anti-emulation

Great heuristics of binary

Great entropy of binary

Unique binaries for each customer

Unhooks antivirus hooks in ntdll.dll, so that your malware performs better during runtime.

Hard to reverse engineer statically

Compression

I can crypt x64 and x86. x64 is preferred for longer FUD times and better scantime performance.

Two execution methods:

LoadPE - no API call, fully clean runtime

RunPE - unique call chain with unhooked calls. Use for binaries that are not supported by LoadPE.

Each customer receives a unique stub. The stubs are hand-made and then ran through my plethora of utilities such as source-code scrambling as well as LLVM IR bitcode obfuscation. The outputs are extremely unique from eachother.

I can crypt most .NET binaries as well - using a CLR loader. Ask me, and we test.

I will crypt using LoadPE for best runtime. Some binaries are not supported by my LoadPE, for example BitRat. For these options, I offer RunPE into itself. BitRAT has been tested and working with RunPE in itself. Are you unsure if your binary is supported, ask, and we test.

Crypter purity & detections

Each crypt you will get will be scantime FUD. I will prove this with a scan (either dyncheck or avcheck). If I am unable to generate a FUD output you will have the option to not pay, pay a smaller amount, or wait til I can generate a FUD output. If the file is undetected on scanner - I will treat it as undetected.

The crypter is runtime clean. Here is a link to dyncheck scan:

https://dyncheck.com/scan/id/af6f2062058d8dc6d221ba85591f1b53#collapse_info

According to dyncheck, comodo and symantec detects the file during execution. There is no screenshot of this, so it might be fault of dyncheck, the file might still be running inside sandbox, or it might've been detected. Either way consider the runtime of LoadPE execution to be 0-2/23. RunPE execution has a higher chance of detection. The binary has been saved and is available for trusted members or staff to confirm, it is the real crypted binary that has ben used in dyncheck scan.

The crypter is clean in runtime, but your binary may not be. Often, the developer of your payload will provide runtime scans of their payload so you know what the runtime footprint is of binary. For example, Smoke loader has a runtime footprint of 4-6/23, Godzilla has a runtime footprint of 2/12. You must take into consideration the runtime footprint of your binary as well. My crypter helps improve the footprint of your payload by unhooking hooks that the AV has placed; but this is no guarantee. If your file is using bad behavior, such as dropping files to disk, or encrypting files, there is a larger chance of it getting detected. There is nothing a crypter can do to prevent this; contact the developer of your payload. Use good or private malware for optimal runtime results.

I do not offer additional features. I do not add melt, watchdog, persistence, etc. Those are the features of your bot. Startup might be an option in the future, that is all. Please disable code mutation / UPX in your builder to prevent conflicts with the crypter.

30 EUR / 1 crypt: if detected within 4 hours you get free recrypt

50 EUR / 1 crypt: if detected within 8 hours you get free recrypt

100 EUR / 1 crypt : if detected within 24 hours you get free recrypt

If we work long-term or want another payment plan (discounts), ask me, and we discuss.

You get recrypts only if your file hash is not on scanners like virustotal.

In case of refunds, I will refund the amount with a small fee to cover the BTC transaction fee.

Write to me on jabber/XMPP: donatellaversace@xmpp.jp

Please have OTR encryption enabled.

[contract=tid]Start Contract[/contract]

I sell the product under the assumption that it shall not be misused in any illegal or unethical way. It is unforgettable that the use of this product in combination with illegal malware on computers that

you do not have explicit consent to is in clear violation of Article 273 of the Criminal Code of the Russian Federation (or the equivalent of your jurisdiction). Each buyer carries the responsibility of using this product in line with the law.

PandaLord69 - May 26, 2021, 12:10 pm

Glad to see you started the services. Been a beta tester of your services.

Crypted my bitrat & miner came out awesome still using it. Will buy for sure <3.

Bypasses WD st/rt am happy with this.

bellodipapa - May 28, 2021, 7:11 am

sounds good, good luck with sales !

donatellaversace - May 28, 2021, 11:40 am

(May 28, 2021 06:28 AM)Fulya Donmez Wrote: [\[CITE\]](#) Join Date: 05-09-2021. That gonna be an issue

Absolutely wouldn't be. Please refrain from low-quality posting on my thread. My service was available free for all users on this forum for several days to try out before I started this thread. I already have satisfied customers, and furthermore, the stub used in dyncheck has been saved and can be confirmed by any reverse engineer/trusted moderator on this thread. Additionally, this forum has a contract system that conveniently makes it impossible me to scam someone without consequences. As a final note, those who are serious in following the market already recognize me from underground forums where I sell the same product.

I could go on and on, but I am probably talking to a brick wall. You're clearly not here to purchase my product or leave a review, so please refrain from posting on my thread. This incident has been reported.

wolterkam - May 28, 2021, 1:05 pm

connect on jabber please.

donatellaversace - May 31, 2021, 9:19 am

Crypter service temporarily paused while I develop code for a Red Team.

Message will be edited and thread will be bumped when the service can continue in its normal state.

Aekras1a - June 8, 2021, 11:02 pm

Very interested in your services, have added on jabber. Good luck with sales and regarding the Red Team work.

Look forward to hearing from you soon, take care.

justalemon - January 20, 2022, 1:33 am

Good luck with sales! I will add you now