

Forum:[Hack Forums](#)

Thread: [100% FUD Native \[0.00% .NET\] FREE Crypting Guide | Learn to crypt YOURSELF in 1 Week!](#)

RunPE - June 29, 2019, 6:54 am

Want to learn to CRYPT yourself,
Completely FREE with no .NET & with fully open source software?

Benefits of Crypting yourself: Completely Free and no BS licenced software

Know EXACTLY how YOUR files work.

To make sure no one injects their own code into yours..

Just to learn and expand your brain power.

Why I decided to write this?

For anyone wondering why a newbie, no rank, no rep, just over 3 hours online decided to make a "completely free" and "Native FUD" crypting tutorial.. Well, honestly I've been looking at HF for a while now and there is a reason why I didn't sign up ages ago..

HF is good and all, but the people is the problem, I personally feel HF is infected with money sucking users.. People selling crypts for \$100+ just for a simple Native crypt or even \$40 a month for a closed source crypter licence.. So I decided I would try to put it right again, just try to balance out the economy and hopefully people learning from this tutorial will learn and maybe even go into sales but for alot cheaper as there will be just a few more people with crypting knowledge.

Lets Dive In >-0> [<-- a Fish FYI]

I'm hoping people already have some knowledge on at least C++ or some Native language if not, before reading this tutorial I highly recommend you take a look at Code Academy or some other interactive coding tutorial, just to get the basics down. Some sites even have some sort of Cryptography lesson, teaching you the basics of encryption & encoding [AES, Base64 etc.]

So to start with, you need to know a rough idea of the following: [DuckDuckGo is highly recommended for anonymity reasons] The basics of C++

Basics of Cryptography [I highly recommend "The Code Book" its a big read but so useful + some history & stenography if your interested.]

Look into Base64 and other types of Executable Encoding techniques.

Get Visual Studio [Only get the C++ packages, as I said ABSOLUTELY NO .NET]

Get some Music Ready as this is going to take a long time.

Basics of RunPE, Injection and how memory works.

Now once you got all of that done, I HIGHLY recommend looking into ChimeraPE, that's personally how I started.

I honestly cant recommend it enough, so here's the link: github.com/hasherezade/chimera_loader
But anyways, to get started with your first ever crypt.

The TUTORIAL

Convert your PE [Portable Executable | RAT, Worm etc.] to Base64 or whatever encoding you wish to chose.

Encrypt your Base64 in AES, or even make your own encryption. I've seen people making their own Polymorphic Caesar Cipher Encryption

Grab ChimeraPE and create a few functions/variables to load your encrypted Base64, decrypt it, then put it through ChimeraPE or any RunPE of your choosing (Remember dont reinvent the wheel!)

Choose a good place to inject into and a place to store the Encrypted Base64. I highly recommend to store the Base64 in the Registry or maybe you can think of somewhere better? For the Injection/RunPE/ChimeraPE, I recommend choosing either some Native PE in System32 that looks legitimate or just bundle your own injectable PE with your Stub that can be decrypted, saved to disk and injected into.

Add some Randomness [Delays etc.] Personally I use a mining technique, similar to how cryptocurrency works.

Last but not least, add Hooks to common RAT/worm functions, so if your PE moves the mouse, look up what hooks the mouse uses, and look up what hooks antivirus's use to detect it with "behavior detection". Its a bit too complicated to explain so, feel free to search it and look into it as its quite an advanced subject and not 100% necessary to all cases.

Lastly, test, test and test over and over, every single step of the way.

Grab ADVobfuscator to make your file semi-polymorphic: github.com/andrivet/ADVobfuscator <--- HIGHLY RECOMMENDED

Compile the thing, and use a wrapper, it can be as simple as just using a WinRAR SFX archive or even going to the extent of using a NSIS Wrapper and Coding a hidden installer for it!

For anyone having trouble understanding, please contact me on my Jabber @ RunPE@exploit.im
If you really don't understand I would highly appreciate feedback on this tutorial, feel free to ask questions bellow.

If you want me to modify anything or add anything, feel free to PM me on HF.

Anyone wanting a Cheap Crypt under \$15, and cant be bothered to do anything above, contact me either on HF or my jabber stated above.

Again, if ANYTHING is incorrect, please don't hate my thread, I'm open to Ideas and Suggestions!!!

Thanks for Reading! ?

Much appreciated, thanks for sharing something useful to learn from :)

PattyBuckets - July 16, 2019, 4:04 pm

Really looking forward to trying this out! Thank you.

Twistd - July 16, 2019, 6:31 pm

Why are you encoding the payload before encryption?

why are you encrypting with AES and/or recommending making a custom encryption algorithm?

Why are you talking about storing the encrypted payload in registry?

Why do you think making your stub polymorphic will help and what will it help against?

Why are you recommending cryptography books for this task?

juzioo09524 - August 7, 2019, 1:45 pm

thank you for doing something for free for new people :)

_ap0g - August 11, 2019, 2:23 am

Nice one.. gonna try this out

Anonz8 - August 11, 2019, 11:31 pm

thank you for doing something free for new people :)

slipperyneck - October 9, 2020, 2:27 pm

(Jun 29, 2019 06:54 AM)RunPE Wrote: [\[CITE\]](#) Want to learn to CRYPT yourself, Completely FREE with no .NET & with fully open source software?

Benefits of Crypting yourself: Completely Free and no BS licenced software

Know EXACTLY how YOUR files work.

To make sure no one injects their own code into yours..

Just to learn and expand your brain power.

Why I decided to write this?

For anyone wondering why a newbie, no rank, no rep, just over 3 hours online decided to make a "completely free" and "Native FUD" crypting tutorial.. Well, honestly I've been looking at HF for a while now and there is a reason why I didn't sign up ages ago..

HF is good and all, but the people is the problem, I personally feel HF is infected with money sucking users.. People selling crypts for \$100+ just for a simple Native crypt or even \$40 a month for a closed source crypter licence.. So I decided I would try to put it right again, just try to balance out the economy and hopefully people learning from this tutorial will learn and maybe even go into sales but for alot cheaper as there will be just a few more people with crypting knowledge.

Lets Dive In >-0> [<-- a Fish FYI]

I'm hoping people already have some knowledge on at least C++ or some Native language if not, before reading this tutorial I highly recommend you take a look at Code Academy or some other interactive coding tutorial, just to get the basics down. Some sites even have some sort of Cryptography lesson, teaching you the basics of encryption & encoding [AES, Base64 etc.]

So to start with, you need to know a rough idea of the following: [DuckDuckGo is highly recommended for anonymity reasons]The basics of C++

Basics of Cryptography [I highly recommend "The Code Book" its a big read but so useful + some history & stenography if your interested.]

Look into Base64 and other types of Executable Encoding techniques.

Get Visual Studio [Only get the C++ packages, as I said ABSOLUTELY NO .NET]

Get some Music Ready as this is going to take a long time.

Basics of RunPE, Injection and how memory works.

Now once you got all of that done, I HIGHLY recommend looking into ChimeraPE, that's personally how I started.

I honestly cant recommend it enough, so here's the link: github.com/hasherezade/chimera_loader
But anyways, to get started with your first ever crypt.

The TUTORIAL

Convert your PE [Portable Executable | RAT, Worm etc.] to Base64 or whatever encoding you wish to chose.

Encrypt your Base64 in AES, or even make your own encryption. I've seen people making their own Polymorphic Caesar Cipher Encryption

Grab ChimeraPE and create a few functions/variables to load your encrypted Base64, decrypt it, then put it through ChimeraPE or any RunPE of your choosing (Remember dont reinvent the wheel!)

Choose a good place to inject into and a place to store the Encrypted Base64. I highly recommend to store the Base64 in the Registry or maybe you can think of somewhere better? For the Injection/RunPE/ChimeraPE, I recommend choosing either some Native PE in System32 that looks legitimate or just bundle your own injectable PE with your Stub that can be decrypted, saved to disk and injected into.

Add some Randomness [Delays etc.] Personally I use a mining technique, similar to how cryptocurrency works.

Last but not least, add Hooks to common RAT/worm functions, so if your PE moves the mouse, look up what hooks the mouse uses, and look up what hooks antivirus's use to detect it with "behavior detection". Its a bit too complicated to explain so, feel free to search it and look into it as its quite an advanced subject and not 100% necessary to all cases.

Lastly, test, test and test over and over, every single step of the way.

Grab ADVobfuscator to make your file semi-polymorphic: github.com/andrivet/ADVobfuscator <---
HIGHLY RECOMMENDED

Compile the thing, and use a wrapper, it can be as simple as just using a WinRAR SFX archive or even going to the extent of using a NSIS Wrapper and Coding a hidden installer for it!

For anyone having trouble understanding, please contact me on my Jabber @ RunPE@exploit.im
If you really don't understand I would highly appreciate feedback on this tutorial, feel free to ask questions bellow.
If you want me to modify anything or add anything, feel free to PM me on HF.
Anyone wanting a Cheap Crypt under \$15, and cant be bothered to do anything above, contact me either on HF or my jabber stated above.

Again, if ANYTHING is incorrect, please don't hate my thread, I'm open to Ideas and Suggestions!!!

Thanks for Reading! ?
Saving for later

currentlytheradersbn - October 10, 2020, 1:39 am
rThanks... untime or scantime?

Whocares12345 - October 10, 2020, 12:47 pm
Nice tutorial! thanks for the High quality post!

artson1990 - February 2, 2021, 3:08 pm
hi thanks for the High quality post.
i want ask you something if you can pm me still dont have 25 posts :)

xyz147258 - March 8, 2021, 11:44 am
I really need your help
bro Are you a telegram?

Salesforce - March 15, 2021, 1:12 am
Hi i need your help and pay your service pm me :)

onimant - April 7, 2021, 3:26 am
(Jun 29, 2019 06:54 AM)RunPE Wrote: [\[CITE\]](#) Want to learn to CRYPT yourself,
Completely FREE with no .NET & with fully open source software?

Benefits of Crypting yourself:Completely Free and no BS licenced software

Know EXACTLY how YOUR files work.

To make sure no one injects their own code into yours..

Just to learn and expand your brain power.

Why I decided to write this?

For anyone wondering why a newbie, no rank, no rep, just over 3 hours online decided to make a "completely free" and "Native FUD" crypting tutorial.. Well, honestly I've been looking at HF for a while now and there is a reason why I didn't sign up ages ago..

HF is good and all, but the people is the problem, I personally feel HF is infected with money sucking users.. People selling crypts for \$100+ just for a simple Native crypt or even \$40 a month for a closed source crypter licence.. So I decided I would try to put it right again, just try to balance out the economy and hopefully people learning from this tutorial will learn and maybe even go into sales but for alot cheaper as there will be just a few more people with crypting knowledge.

Lets Dive In >-0> [<-- a Fish FYI]

I'm hoping people already have some knowledge on at least C++ or some Native language if not, before reading this tutorial I highly recommend you take a look at Code Academy or some other interactive coding tutorial, just to get the basics down. Some sites even have some sort of Cryptography lesson, teaching you the basics of encryption & encoding [AES, Base64 etc.]

So to start with, you need to know a rough idea of the following: [DuckDuckGo is highly recommended for anonymity reasons]The basics of C++

Basics of Cryptography [I highly recommend "The Code Book" its a big read but so useful + some history & stenography if your interested.]

Look into Base64 and other types of Executable Encoding techniques.

Get Visual Studio [Only get the C++ packages, as I said ABSOLUTELY NO .NET]

Get some Music Ready as this is going to take a long time.

Basics of RunPE, Injection and how memory works.

Now once you got all of that done, I HIGHLY recommend looking into ChimeraPE, that's personally how I started.

I honestly cant recommend it enough, so here's the link: github.com/hasherezade/chimera_loader
But anyways, to get started with your first ever crypt.

The TUTORIAL

Convert your PE [Portable Executable | RAT, Worm etc.] to Base64 or whatever encoding you wish to chose.

Encrypt your Base64 in AES, or even make your own encryption. I've seen people making their own Polymorphic Caesar Cipher Encryption

Grab ChimeraPE and create a few functions/variables to load your encrypted Base64, decrypt it, then put it through ChimeraPE or any RunPE of your choosing (Remember dont reinvent the wheel!)

Choose a good place to inject into and a place to store the Encrypted Base64. I highly recommend to store the Base64 in the Registry or maybe you can think of somewhere better? For the Injection/RunPE/ChimeraPE, I recommend choosing either some Native PE in System32 that looks legitimate or just bundle your own injectable PE with your Stub that can be decrypted, saved to disk and injected into.

Add some Randomness [Delays etc.] Personally I use a mining technique, similar to how cryptocurrency works.

Last but not least, add Hooks to common RAT/worm functions, so if your PE moves the mouse, look up what hooks the mouse uses, and look up what hooks antivirus's use to detect it with "behavior detection". Its a bit too complicated to explain so, feel free to search it and look into it as its quite an advanced subject and not 100% necessary to all cases.

Lastly, test, test and test over and over, every single step of the way.

Grab ADVobfuscator to make your file semi-polymorphic: github.com/andrivet/ADVobfuscator <---
HIGHLY RECOMMENDED

Compile the thing, and use a wrapper, it can be as simple as just using a WinRAR SFX archive or even going to the extent of using a NSIS Wrapper and Coding a hidden installer for it!

For anyone having trouble understanding, please contact me on my Jabber @ RunPE@exploit.im
If you really don't understand I would highly appreciate feedback on this tutorial, feel free to ask questions bellow.

If you want me to modify anything or add anything, feel free to PM me on HF.

Anyone wanting a Cheap Crypt under \$15, and cant be bothered to do anything above, contact me either on HF or my jabber stated above.

Again, if ANYTHING is incorrect, please don't hate my thread, I'm open to Ideas and Suggestions!!!

Thanks for Reading! ?

Good tutorial buddy, Thanks alot..

futbol33 - April 11, 2021, 4:58 pm

This post helped me understand how the crypter works. thank you

speedyboy17 - April 16, 2021, 8:07 am

Can i get your discord or something would like you to teach me more about this (am a noobie but know how to code in weblanguage) would pay you if you could learn me :D

maki000124k - April 22, 2021, 11:32 am

Good one. It helped me understand how it works. Thanks.

Treppy. - April 22, 2021, 12:06 pm

I would like to crypt with my private crypter which will not be used on internet

hunter x hunter - April 22, 2021, 1:43 pm

hi sir ,would you like to make a video tutorial for this please ? thank you i'm struggling