

Forum:[Hack Forums](#)

Thread: [Crypter Help Desk | Crypter 101 |](#)

Cyph Jr - February 24, 2015, 5:48 pm

Crypters 101

An in depth guide providing you with everything you need to know about crypters.

What is a crypter?A crypter is a program that hides detection rates commonly identified by Anti Viruses by encrypting data. Crypters are most likely used for encrypting Malware programs such as rats, keyloggers and other malicious files.

A crypted file that isn't detected by anti-viruses is considered FUD which stands for fully undetectable. A crypted file that is detected by anti-viruses is considered UD which stands for undetectable. It's considered UD because it's not detected by all anti viruses but by some.

Types Of Crypters

There are two different types of crypters; Runtime and Scantime.A Scantime crypter is fully undetected from all Anti-Viruses when you scan it.

A Runtime Crypter can keep the file from being recognized during and after startup of the computer. Files crypted with a Runtime Crypter are decrypted in memory. Most runtime crypters use a RunPe.

Languages A Crypter Can Be Coded InVb.net

C++

C#

ASM

VB 6

Delphi

Features of a crypter; What they mean/do?USG – Unique Stub Generator makes each stub different and to crypt the selected file.

EOF – End of File is required for some rats such as Cybergate, bifrost to be successfully crypted or else the crypted file.

Extension Spoofer – spoofer is where you can change the end of your crypted file into a .JPG, .PNG or any supported extensions.

Icon Changer – Will change the icon of the crypted file.

File Pumper – Pumps the file to make it larger.

File Binder – Will bind your crypted file to another program of your choice.

RunPE – Injects your file into another process.

Anti-Sandboxie – When added to a crypted file and file is being attempted to run in the sandboxie it will refuse.

Anti-VM – When added to a crypted file, the file will refuse to run on a VM.

Startup – Runs the file every time the computer starts.

Obfuscate – To make harder to understand.

Persistence – Makes the crypted harder to end or be killed by botkillers.

Botkiller – Used to kill other malware on a machine.

Hide File – After a crypted file with hide file is executed it changes the program from visible to hidden.

Melt File – After a crypted file with melt file is executed it deletes itself from the machine.

Delay – Slows down the execution of the file for a few seconds.

Stub – The stub is undetected code that helps your file stay FUD. The stub is also the code that decrypts and runs the file.

Assembly changer – Changes the assembly to what you specify.

Disable Task manager – Disables access to task manager.

Disable System restore – Disables system restore.

Cloner – Clones the icon of a file.

Backdoor – A feature that allows unauthorized access to data.

Where to scan crypted files?Scan4you

RazorScanner

Avdetect

refud.me

Any other site that doesn't distributes

Where NOT to scan crypted files?VirusTotal

Any other site that distributes

What to look for when buying cryptersMake sure the product you're buying isn't a scam or rip off.

FUD you're buying a crypter because you want to make your rat FUD. Contact the seller asking for a test crypt.

Legit. Check the vouches and product reviews.

DefinitionsMalware - A malware is a software that is made to harm/damage or disable computers.
Ex Rats.

Keylogger - A keylogger is a software that is intended to track the keystrokes of the infected person. Keyloggers are mostly used to gain logins for a victim on a specific site.

Credits to [Saturday](#) for formatting this thread.

Credits to [Abide](#) for helping me with 2 definitions.

Hidden Pain. - February 25, 2015, 12:36 am

Very nice guide, will definitely help new members that want to get into this ?

LynS - February 25, 2015, 4:10 am

Nice tutorial mate, this will surely help the newbies :D

Cyph Jr - March 1, 2015, 6:55 pm

Bumping this thread. Looking for more suggestions.

Cyph Jr - March 1, 2015, 7:00 pm

(Mar 1, 2015 07:58 PM)Tweety. Wrote: [\[CITE\]](#) I would update the features, most of the definitions are wrong.

Don't just say that elaborate be more specific.

tweety - March 1, 2015, 7:07 pm

EOF – End of File is data that is required for some malware to run, it typically consists of settings etc

File Pumper – Pumps the file with junk code adding it to the EOF to make it larger.

Obfuscate – Changes the control flow and readability of the malware.

Persistence – locks, respawns processes, recreates registry keys for malware to ensure it isn't killed.

Melt File – after installing the malware, it will run the installed version and kill itself, then deleting itself, leaving the installed version behind.

Delay – delays itself from being executed.

Stub – a template of the malware without the payload.

Just a few.

NggZAreReal - April 18, 2015, 5:55 am

nice crypter :) , good work and thanks :)

?I??? ??t - April 19, 2015, 3:40 am

you missing autoit on your thread ;)