

Forum:[Hack Forums](#)

Thread: [\[Guide\] NooB Friendly Guide to Keyloggers! \[Guide\]](#)

Deciever - July 17, 2012, 9:47 pm

Welcome to a Beginner's Guide to Keyloggers! In this guide I will go through all the common topics that you may need to know. When you finish reading this topic you will know everything you will ever need to get started keylogging. I cover every topic related to keyloggers as well as cover terminology and definitions. I'll explain how a keylogger works and how to even get started making your own! So let's get started!

What is a keylogger?

Learning the lingo and definitions.

Common features keyloggers have.

How do I use a keylogger?

What is a "stub"?

What is the "server"?

What is crypting?

What is the difference between a stealer and a keylogger?

What is .net framework and why do I care?

What are some good keyloggers?

What are some upsides to keyloggers?

What are some downsides to keyloggers?

I want to make my own keylogger. Where do I start?

I think I've been infected with a keylogger! What do I do?

Conclusion

A keylogger is a program that logs a keyboards keystrokes. It can be used for several purposes, both black hat and white hat. The most common use is black hat. A keylogger functions by grabbing a keystroke, triggered by when the slave presses a key on their keyboard, and saving it to a variable. This process is called "keyboard hooking". It then will take this long variable and send it via a SMTP or FTP server. You can then view these logs and use it for whatever your intention may be. Keyloggers have several different features that I will go into in a later section. The most basic ones only include keyboard hooking and a way to send the logs.

One of the most confusing things about starting something new is not understanding the lingo. If you don't understand the lingo, how will you know what people are talking about? In this section I'll be explaining the common terms people use concerning keyloggers. I'll be going over some other more general things as well.

Logger

Slang term for keylogger. See the "What is a keylogger" section.

Hooks

Slang term for keyboard hooks. These are also explained in the "What is a keylogger section"

Keystrokes

Section of code that is triggered when the slave types something on the keyboard.

Logs

Compilation of all the keystrokes over a period of time.

FTP

A webhost that stores files that allows the user to connect and retrieve said files. Files in this case are logs.

SMTP

A way that logs are sent via email. Example, MSN, Gmail, Yahoo, etc.

FUD

Full Un-Detected. This means that antiviruses will not detect your file as a virus. This will be further explained in the "What is crypting section".

UD

Undetected. This means that some antiviruses will not detect your files as a virus, while others will.

Server

A server is the output of your keylogger. I will take this in-depth in the "What is a server?" section.

Crypter

A crypter crypts your file removing detections. I'll take this in-depth in the "What is crypting" section.

Detection

A detection is a term used when an antivirus detects, or thinks your file is a virus. You always want to have the least amount of detections possible to increase your success rate and to reduce errors.

Black hat

A black hat is someone who uses their knowledge of computers and security for malicious reasons.

White hat

A white hat is someone who uses their knowledge of computers and security for helpful reasons. They help disinfect and improve others security to combat black hat hackers.

Grey hat

A grey hat is a mixture between a black and white hat. They will infect innocent people and then help them get rid of it, for free or a price (the latter being more common).

Backdoored

When a file is backdoored it has a virus binded to it. This means that the file will act normally and the user will be infected without their knowledge. This has become extremely common in the keylogger section. Always be wary of new releases.

As I've said before, most keyloggers have two basic settings. Keyboard hooking and log sending (by FTP or SMTP). Most keylogger developers (myself included) like to include more settings to help ease the user experience. Below is a list of common settings you may find, and what they do:

Icon Changers

This will change your viruses icon without corrupting it like some third party programs can do.

MuteX

MuteX is a unique string that you generate. It helps prevent multiple logs from being sent.

Add to Startup

This will add a registry (or other ways) that will cause your virus to start when the computer is turned on.

Antis

Antis are a feature that help keep your virus on the slaves computer for as long as possible. They disable or stop certain white hat programs such as antiviruses, sandboxie, and keyscramblers from running or removing your file.

Disable CMD/Taskmanager/Registry

This feature will change the registry value for each of these system tools to disable them.

Logging interval

This allows the user to chose how often logs are sent.

Fake Error Message

This will cause a fake error message to pop up, making it seem less suspicious.

File pumper

This will add to the size of your virus. This helps making it seem less suspicious as a game won't be a few kilobytes.

Assembly Editing

This allows you to change things found in the properties menu when right clicking a file. This helps it seem more like a real file rather than a virus.

Encrypted user information

This encrtyps your information so that others cannot steal it by decompiling your virus.

Test connection

This will test your credentials that you've entered to make sure they are correct.

Using a keylogger is a lot easier than it sounds. All you need to do is find one that you want to use, download it, and then chose your settings. Once you have entered all your information and chosen your settings, click the build button. The builder will create your server. This is what you give to people. Give them this file and when they run it they will be infected and you will start receiving logs. Pretty self explanatory. If you ever have a question contact the creator and they should be able to help you.

A stub is a separate binary that contains special code that is required for the keylogger to function. There are usually two things in a keylogger. The builder and the stub. Some keyloggers will have a stub built in. A builder takes the information and settings you've chosen and merges it with a stub. The stub contains keyhooks and the workings of each feature. These two merge to create your virus, containing all of the information. I'll cover this file in the next section.

Crypting can be very complex, though it isn't necessary for you to know all of this information. So for this section I'll keep things to what you need to know. Crypting involves taking a stub (sometimes it's CodeDOM) and using that to FUD (or lower your detection rate) your file. The entire process can get a bit confusing, and I won't bother getting into it. What you do need to know is that crypting can easily corrupt your keylogging sever making it no longer work. A corrupt keylogger may not be detected (the crypter at least did it's job) but it will not send logs making it useless. Because of this you should chose your crypters carefully and it may take a while to find one that works (for free) with your keylogging server. If you are buying a crypter (which I recommend) then be sure to ask the seller to either test or verify your server. In short, crypting is used to lower detection rate, and raise execution rates. That's all you need to know.

There is one major defining difference between a stealer and a keylogger. A stealers purposes is to steal passwords that have been saved in the browser/application. Ever logged into something and your browser prompted you to save the password? This is what stealers steal. They are good for massivley grabbing passwords and quickly. Once run they do not continue to steal until run again.

.Net Framework is a very in-depth concept from Microsoft. While you don't need to know (or should you really care) you should know that most keyloggers are written in Visual Basic .Net, giving it a dependancies. Depending on who made it (whether they suck or not) you may have to install a specific version (.Net 4.0). Most computers (99%) come with .Net 2.0 installed. Your output will also requie a specific framework (depending on which one you use).

Hope this helps any new people that want to learn! If you have any questions about keyloggers, please feel free to reply below or pm me :)

CSGHOST - July 17, 2012, 9:51 pm

Thanks for the lingo section it really is going to help me out

Alside - July 17, 2012, 9:58 pm

Interesting I learned some new information thanks.

Deciever - July 17, 2012, 9:59 pm

(Jul 17, 2012 09:58 PM)Alside Wrote: [\[CITE\]](#) Interesting I learned some new information thanks. Of course! We learn something new everyday :)

Curel - July 17, 2012, 10:03 pm

didnt know about the black hat and white hat stuff thats pretty cool :)

Deciever - July 17, 2012, 10:05 pm

(Jul 17, 2012 10:03 PM)Curel Wrote: [\[CITE\]](#) didnt know about the black hat and white hat stuff thats pretty cool :)

Im glad you took time to read my guide, it makes me feel like people enjoy my hard work :P

lilybear199814 - July 18, 2012, 10:52 pm

I am a noob and this was soo helpful! I wanna learn coding and if you have any information on that let me know! Btw I dont wanna download anything

Deciever - July 18, 2012, 11:05 pm

(Jul 18, 2012 10:52 PM)lilybear199814 Wrote: [\[CITE\]](#) I am a noob and this was soo helpful! I wanna learn coding and if you have any information on that let me know! Btw I dont wanna download anything

If you are trying to gain slaves via your keylogger, you will need download the keylogger/binder/crypter and find someone with a ftp host. Or you can have someone with the stuff already that will TeamView with you and set it up. You can PM my friend [??Dong???](#) he can help you set one up, but he will have charge fee. Otherwise you can find someone who does it for free on the forums, but I doubt you will find a free service like that :P

Quality_k1nG - July 18, 2012, 11:05 pm

hi this is very great guide definitely it will help many people

Tman1531 - July 18, 2012, 11:19 pm

Definitely helped me since i am new to using loggers.Thanks and hopefully this will come in handy

for me soon!

kr4NK - July 18, 2012, 11:59 pm

Nice dude, learned some new stuff^^
Good job

loser386 - July 19, 2012, 1:03 am

really awesome tut
thx for sharing :)

tlozoot - July 19, 2012, 1:56 am

thanks for the guide it will help me ! :D

Deciever - July 19, 2012, 11:20 am

Thanks guys! If yall really enjoyed this TUT feel free to +1 rep

And I will be out soon with some awesome free money making ebooks! Working on them now :D

wraithcranzz - July 19, 2012, 12:05 pm

Thanks For the Great Guide. gained Some new Knowladge xD

japheth08 - July 19, 2012, 2:11 pm

but is there any way to remove a keylogger without any programs?

Deciever - July 19, 2012, 2:17 pm

(Jul 19, 2012 02:11 PM)japheth08 Wrote: [CITE](#) but is there any way to remove a keylogger without any programs?

If you know the process image name then yes, otherwise if you dont know if you are infected you can check with a free malwarebyte trial.

Or you can check out this thread <https://hackforums.net/forumdisplay.php?fid=115>

ChefHacker - July 19, 2012, 2:48 pm

thanks a lot, it help me tons and know im not so clueless