

Forum:[Hack Forums](#)

Thread: [~~ The Ultimate Keyloggers Guide for Beginners ~~](#)

Profit Margin - November 30, 2013, 8:04 am

Information:

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 we will be going over:

- ? 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?
- ? How to spread your keylogger
- ? Conclusion

What is a keylogger?:

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.

The Lingo

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.

Common features of a keylogger

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 encrypts 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.

How to use a keylogger:

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 choose 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.

What is a Stub?

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.

What is a server?

A server is the output of your keylogging builder. It takes your user information (the builder) and the actual malicious code (the stub) and merges the two (via either CodeDOM which I'll explain later in this section, or by filesplitting, which I will also cover) to make one bad ass file. There are several ways that this is accomplished, and both ways have their ups and downs. The server is also what you distribute to infect people. It is your "virus"

CodeDom is a type of building that generates the code during runtime. This allows the user to only have to download one file (just a builder). After inputting your information, the builder will take this and combine it with the malicious code (already inside the builder). This helps lower detection rates, but overall is harder to do, and is harder to reFUD (you have to re distribute the entire builder, instead of just providing another stub).

Filesplitting is the old school way to do things. It requires taking your information (the builder) and combining it with a separate file that contains the malicious code. While this makes it easier to detect, it's easier to update as you can simply give your users another file (same thing, just with less detections).

Crypting:

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 choose 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.

Stealers vs Keyloggers

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.

Framework:

.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).

Some keyloggers:

This is like asking what your favorite ice cream flavor is! There is no "correct" answer. It's best to go and figure things out for

yourself. Being spoon fed information doesn't help you grow intellectually. Figure out which keylogger you like the best, and fits your needs.

Paid keyloggers:

[Limitless Logger](#)

[Legacy Log](#)

[Cyborg](#)

Free keyloggers:

[Limitless Logger Lite](#)

[Dracula Logger](#)

[SysLogger](#)

[Unknown Logger](#)

Advantages of Keyloggers

Keyloggers are great for having massive amounts of slaves. They will constantly send you their info and passwords without you having to do anything. They are more stable that other types of malware and are easier to write. They are also extremeley beginner friendly, and that is why they are so popular.

Downsides to Keyloggers

There's one major downside to keyloggers. Well two, but the second is a downside for all types of malware. The first is that (most) keyloggers don't allow you to have any control once you've infected your slave. You have no control, you can't stop logs, you can't do anything really. Keyloggers are starting to add in remote logging and this is slowly growing to be more and more advanced. The second downside is the .Net dependancy for most keyloggers. This is actually a downside for a lot of malware.

Where do I start to make my own Keylogger?

Well, aren't you ambitious!? It's great that you want to learn, but please...please do not copy and paste public source! Actually learn it for yourself! Once you've done that and made one, don't release it unless it's actually advanced/totally yours. There are plenty of ones on the market.

Anyway, to learn how to make a keylogger, you'll need to figure out what language. For beginners I recommend Visual Basic .Net. Learn about SMTP mailing, and keyboard hooks. Then learn about filesplitting. There are plenty of guides on this forum, just search around!

Spreading:

Spreading is self explanatory, its spreading your keylogger around so you get more slaves. There is multiple ways you can spread your keylogger. Below are some good ways.

Chat Rooms - This is slow but you get adult people (You can get credit cards and paypals from this). First of all , go to any chat room from any of these below:

Code 1.<http://www.chat-avenue.com/teenchat.html>

2.<http://www.chat-avenue.com/adultchat.html>

3.<http://www.321teenchat.com/>

4.<http://www.javachatrooms.net/>

5.<http://www.freechatnow.com/>

And then , upload your file to any free file hosting such as sharesend and then go to chat rooms , and start spamming "16/F/uk huge boobs wanna see my naked pics ? go here <insert link> and tell me if u like it!!

Torrents - This is the most effective way. First you need a torrent client, I use uTorrent, because it's the easiest. Once you get your torrent client, Get some fake stuff , like Steam games Keygen or Cracks or w/e and then put them in a .rar file and put the RAT on it. (BIND IT) . Now you gotta create the torrents. Open uTorrent , and then go to File -> Create New Torrent And add your .rar file on it, okay so now trackers are needed... These are some good ones:

Code <http://open.tracker.#.org/announce>

<http://www.torrent-downloads.to:2710/announce>

<http://denis.stalker.h3q.com:6969/announce>

<udp://denis.stalker.h3q.com:6969/announce>

<http://www.sumotracker.com/announce>

Then click START SEEDING. Now .. Click Create -> Save AS... and save anywhere u want

After you saved , go to <http://www.#.org>, Register and upload your torrent

Conclusion:

Well, this tutorial was a lot longer than I anticipated, it covers everything you could possibly need to know about keylogging. Hopefully this will help some people out and will reduce the amount of pointless threads in this section. If this tutorial helped you, please post what you thought of it! If you have a suggestion, feel free to PM or post here!

Marwix - November 30, 2013, 8:32 am

Very big thread about keyloggers and stuff, Good work buddy :)

Profit Margin - November 30, 2013, 8:33 am

(Nov 30, 2013 09:32 AM)Noname Fail Wrote: [CITEI](#) Very big thread about keyloggers and stuff, Good work buddy :)

Thanks, hopefully there isnt as many questions now in this section

stdio - November 30, 2013, 10:05 am

Very nicely written guide, if you allow me.. can i include it in my free ebook guide for keylogger newbies?

I have made a thread about it here, i am sure this will help many members

<https://hackforums.net/showthread.php?tid=3379490>

Thanks

Profit Margin - November 30, 2013, 10:14 am

(Nov 30, 2013 11:05 AM)Homi Wrote: [\[CITE\]](#) Very nicely written guide, if you allow me.. can i include it in my free ebook guide for keylogger newbies?

I have made a thread about it here, i am sure this will help many members

<https://hackforums.net/showthread.php?tid=3379490>

Thanks

Yes you can use it for your ebook guide ?

Big Bird - November 30, 2013, 11:04 am

Thanks for the release! This will help many!

Profit Margin - November 30, 2013, 11:22 am

(Nov 30, 2013 12:04 PM)Big Bird Wrote: [\[CITE\]](#) Thanks for the release! This will help many!

I hope it will help many, and no problem

bjskatebj - December 1, 2013, 8:26 am

Thanks for making this it had helped me a lot

tahareal - December 1, 2013, 10:43 am

thanks for sharing now i understand keyloggers a lot :)

princep786 - December 3, 2013, 8:30 am

Thanks for the guide...Do you know of any fud keyloggers that allow remote control. I used winspy and it doesnt really work.

GTST - December 4, 2013, 7:50 pm

great guide that will come in handy

born2rock - December 5, 2013, 10:14 pm

nice info of keyloggers and stuff, Good work buddy :)

tomatojoe - December 6, 2013, 3:25 am

Very thorough and noob-friendly. Well written guide which I will certainly refer to. Nice work!

Evil_Wevil - December 6, 2013, 8:40 am

it was long but great

very nice each and every thing is in detail

tnxs for this great thread

NewFlash - December 7, 2013, 9:20 am

Thank you for this tutorial. This is exactly what we are looking!!

StThomasAquinas - December 11, 2013, 6:50 am

This is an excellent guide for n00bs.

Very nicely written and easy to understand.

salesman1960 - December 11, 2013, 2:21 pm

Could you include also in your guide for anyone wondering that SysLogger is currently not working :O