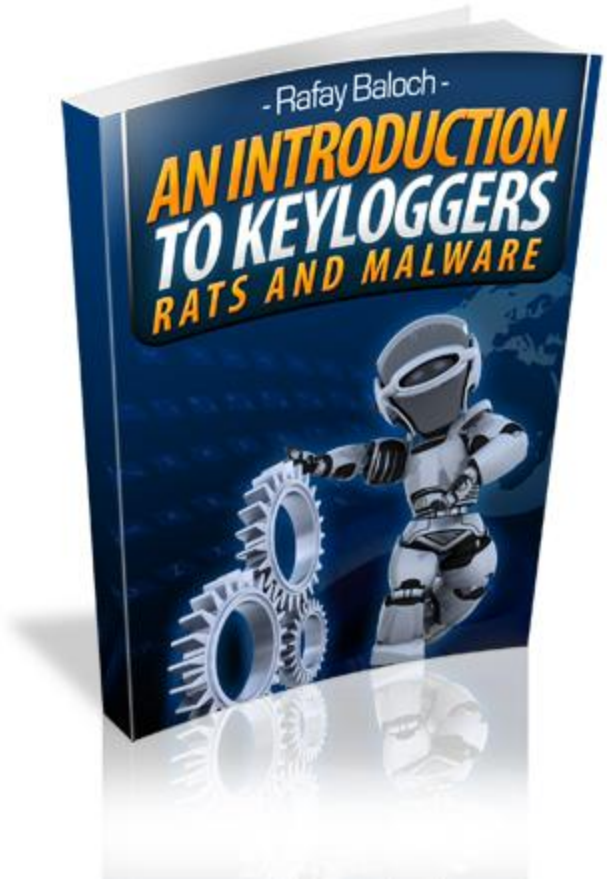


An Introduction To Keyloggers, RATS And Malware

By: Rafay Baloch

www.rafayhackingarticles.blogspot.com

www.hacking-book.com

www.facebookhackingcourse.com

Copyright Notice

Here is the list of the things which you cannot do with this book:

[NO] Can Be Edited Completely

[NO] Can Claim full ownership

[Yes] Can be added to paid membership sites

[Yes] Can be packaged with other products

[NO] Can be sold

[NO] Can be bundled with other products

[NO] Can be broken into multiple chapters

[Yes] Can be given away

[NO] Can sell Resale Rights

[NO] Can sell Master Resale Rights

[NO] Can sell Private Label Rights

[NO] Can be offered through auction sites

[NO] Can sell product as is without changing a thing

Legal Disclaimer

The information provided in this book should be used for educational purposed only. The author holds no responsibility for any misuse of the information provided.

This is not a book which promotes or encourages or exits hackers. But my purpose is to make people aware of security online. I believe that unless you know how to hack (Ethically, you cannot defend yourself from malicious hack attacks). **Know Hacking but no Hacking**.

Warning

Invading some one's privacy is a crime and can experience several penalties if caught.

You implement this information at your own risk!

Resource List

Throughout this e-book the following products are mentioned or discussed

- Keycoabra
- Keysnatch
- Sniperspy
- Winspy
- Spytech Agent
- Allspy keylogger
- Abobo Keylogger For Mac OS
- Sniperspy For Mac
- Spyware cease
- Noadware
- Zemana Antilogger
- A Beginners Guide To Ethical Hacking
- Facebook Hacking Course

Table of Content

Thanks for downloading this book, by downloading this book you have taken a positive step towards your computer security.

What's this book about?

In this book I will discuss about various types of malware, Keyloggers and Rats and tell will explain you the exact methods how hackers can use these keyloggers, Rats and viruses to infect your computer or to control your Pc to steal sensitive information such as username, password, Credit card information etc.

Who Is Rafay Baloch?

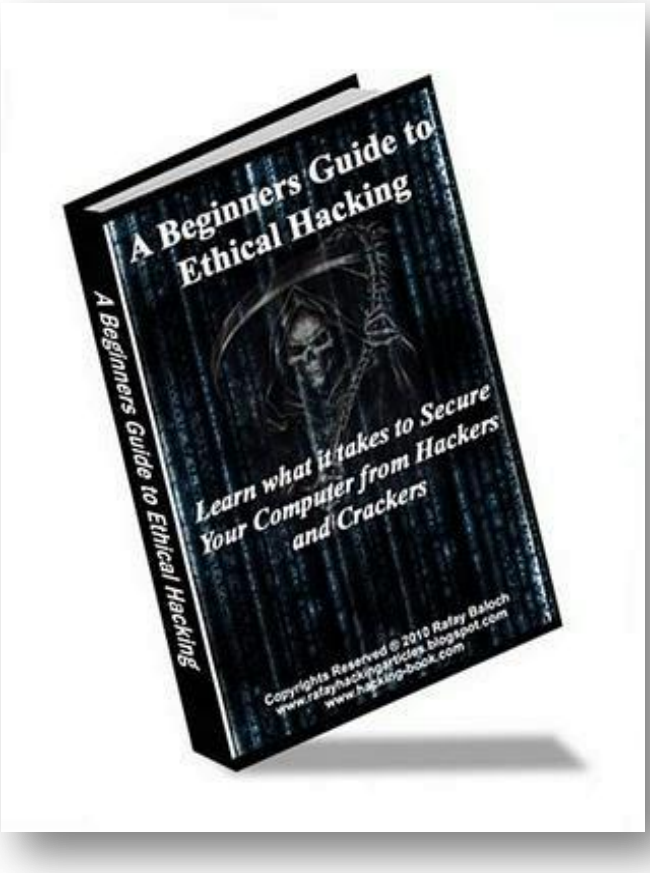
If you have been searching for **"Ethical Hacking and Security"** related content, then the chances are that you might know who I am and the very least you have heard about me, I am the one who runs one of the top and popular Ethical hacking blog **"Rafay Hacking Articles".** I am not a pro hacker or an Expert hacker, but I have been slowly learning and enjoying each and every bit of it.

Unlike other Ethical hackers and Penetration testers I do not keep information to myself that's why I started "**Rafay Hacking Articles**" to educate people about latest security threats and how you can prevent them.

4 Years back when I first got into the "**Hacking Scene**" I asked stupid questions from people and thought that there is some silver bullet to learn hacking, Later when no one helped me I thought do it own my

own, Only after independent research of various topics I came to know what hacking was and how vast this subject really is.

Later I decided to write an E-book to educate newbie's who wanted to learn hacking and had no idea where to start. This is how my book "**A Beginners Guide To Ethical Hacking**" came.



"**A Beginners Guide To Ethical Hacking**" book has been featured on lots of top security blogs and magazines and is one of the few popular Ethical hacking and security books around.

Malware

Malware has been a problem for ages, Malware is short form of malicious software. A Malware is basically a program designed to infect a computer system without owner being informed.

Types of Malware

Malware exists in many forms, below mentioned are some of the common types of malware

1. Trojan Horse – Trojan virus or Trojan horse is one of the most common types of malware, Trojan virus is mostly used to control the victims computer rather than infecting or destroying files on victims computer. A Trojan horse once installed into victims computer can give a hacker complete access to your computer. Trojans are one of the most dangerous forms of malware.

2. Computer Viruses – A computer virus a malicious program which is mostly developed to infect a computer, once it infects a computer it replicates or reproduces itself. A virus is just like a parasite and it needs another host to attach to in order to infect a computer

3. Worms – Worms are almost similar to computer viruses the only difference unlike computer viruses they do not require another host to attach to in order to infect a computer. Once a worm infects a computer it replicates itself. Computer worms are major threats to large networks.

4. Keyloggers - A Keylogger is a hardware or software device which monitors every keystroke, screen shots, chats etc typed on the

computer. A keylogger program does not require physical access to the user's computer. Any person with a basic knowledge of computer can use keylogger

5. RATS – RAT is the short of "**Remote Administration Tool**" and is indeed one of the most dangerous types of malware. It's very similar to a Trojan. Once a RAT is installed in a computer the attacker can do almost anything on the remote computer such as installing a keylogger, shutting down a computer, infecting files etc.

6. Adware – Adware is the short form of Advertisement-supported software. Adware's are commonly designed to display advertisements on your computers. However some of these adwares may contain harmful viruses and spying programs which can bring your computer system to knees.

So these are the most common types of malware, the next chapter will explain you all about keyloggers.

Keyloggers

Keyloggers can be classified into two main types:

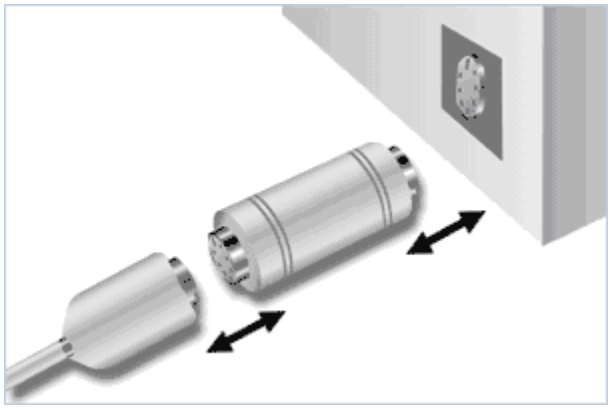
1. Hardware Keylogger

2. Software Keylogger

Hardware Keyloggers

A hardware keylogger is also used for keystroke logging, a hardware keylogger is plugged between the keyboard plug and the USB or PS/2 port socket, and they work with PS/2 keyboards and also usb keyboards,

A hardware keylogger is just like a normal USB drive or any other computer peripheral so that the victims can never doubt that it is a keylogger, Hardware keylogger has any inbuilt memory which stores the typed keystrokes.



The above Image shows you how a hardware keylogger is installed

PS/2 Keylogger

Keycobra – Best Hardware Keylogger

Now you might be wondering where you can find a hardware keylogger, well there are lots of hardware keyloggers available now a days but I would recommend you to use keycobra

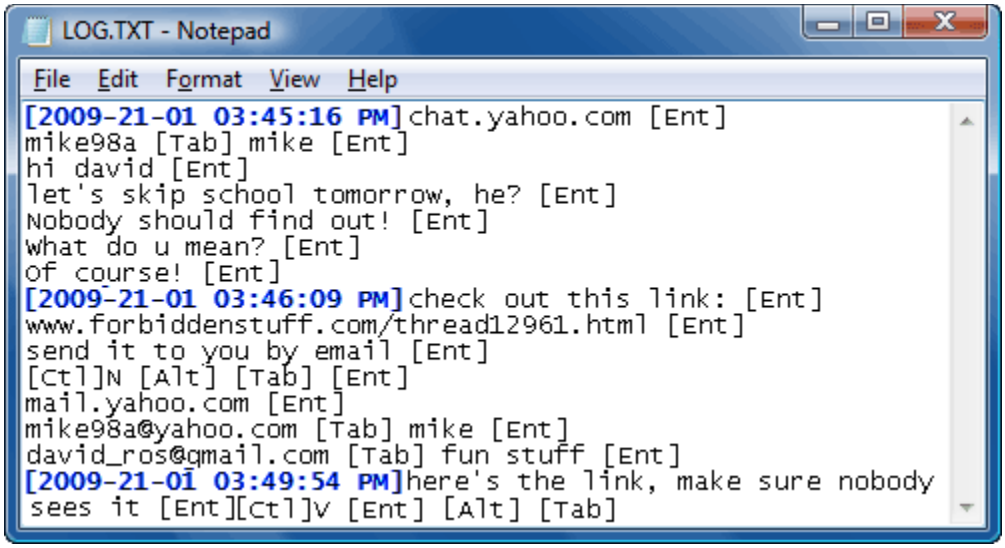
Keycobra is one of my favorite hardware keyloggers as it offers more large amount of storage, Keycoabra keystroke recorder comes in a standard version - 4MB memory capacity, 2,000,000 keystrokes (over 1,000 pages of text), and a Venom version 2 billion keystrokes (over 1 million pages of text), organized into an advanced flash FAT file system. It is compatible with all three operating systems windows,linux and Mac OS, Here are some features of hardware keylogger due to

which keycobra is one of the most popular hardware keyloggers around.

Features

- Record ALL Keystrokes - even Facebook passwords!
- Huge memory capacity, organized as an advanced flash FAT file system
- Advanced text menu for viewing recorded data, includes Net Detective, Phrase Search, Key Filtering, Unplug Counter and more!
- Super fast memory contents download with USB Download Accelerator (included)

Here is the screen shot of logs captured by keycobra as it has captured keystrokes for chat.



Keysnatch

Keysnatch has also a variety of keyloggers including PS/2 keyloggers, USB keyloggers and Wifi keyloggers, The Wifi keylogger has a built in WLAN transceiver and TCP/IP stack, which means that it can connect to the internet through a wifi-acess point

How It Works?

Once the Wifi keylogger has connected to an access point, The **Keysnatch** wifi keylogger will then actively send you all the keystrokes typed by the victim to any email address you provide. The keysnatch wifi keylogger is compatible with all other major operating systems, you name it and it runs on it. Keysnatch keylogger supports all types of keyboards and the best part is that it's completely undetectable by antiviruses.

Software Keyloggers

The hardware keyloggers are extremely useful only in case if you have physical access to victim's computer, but what if you don't have physical access to victim's computer and sometimes the victim might notice it.

This is where software keyloggers come into play, Software keyloggers can also be classified into two types:

1. Local Keylogger

2. Remote Keylogger

Local Keylogger

Local Keyloggers are used to monitor local computers (May be your own Pc), they are very easy to install and are completely undetectable and it's really hard to figure out once a keylogger is installed on a computer because usually keyloggers hide themselves from taskmanager, Windows Registry etc. Whenever you want to see logs, screenshots etc you just need to press a hotkey which **(ex. Shift+Ctrl+F10).**

There are hundreds of keyloggers available now days but some of them are userfriendly and are actually capable to hide themselves once they are installed, some of the Popular Local Keyloggers are:

1. **Spyagent**
2. **AllSpy Keylogger**
3. **Refog keylogger**

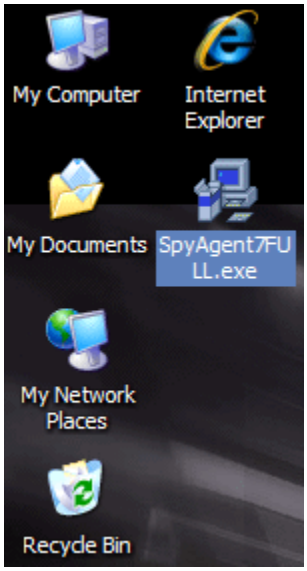
SpyAgent

Spytech agent is an award winning software which can be used to monitor both local and remote computer but it's usually good local monitoring, for remote monitoring there are software better than SpyAgent with far more features than it. Spytech Spyagent runs in total stealth mode and once it is installed on victims computer it's almost impossible to detect it's presence

Spyagent Installation Guide

Here is the complete (Official) installation guide for SpyAgent:

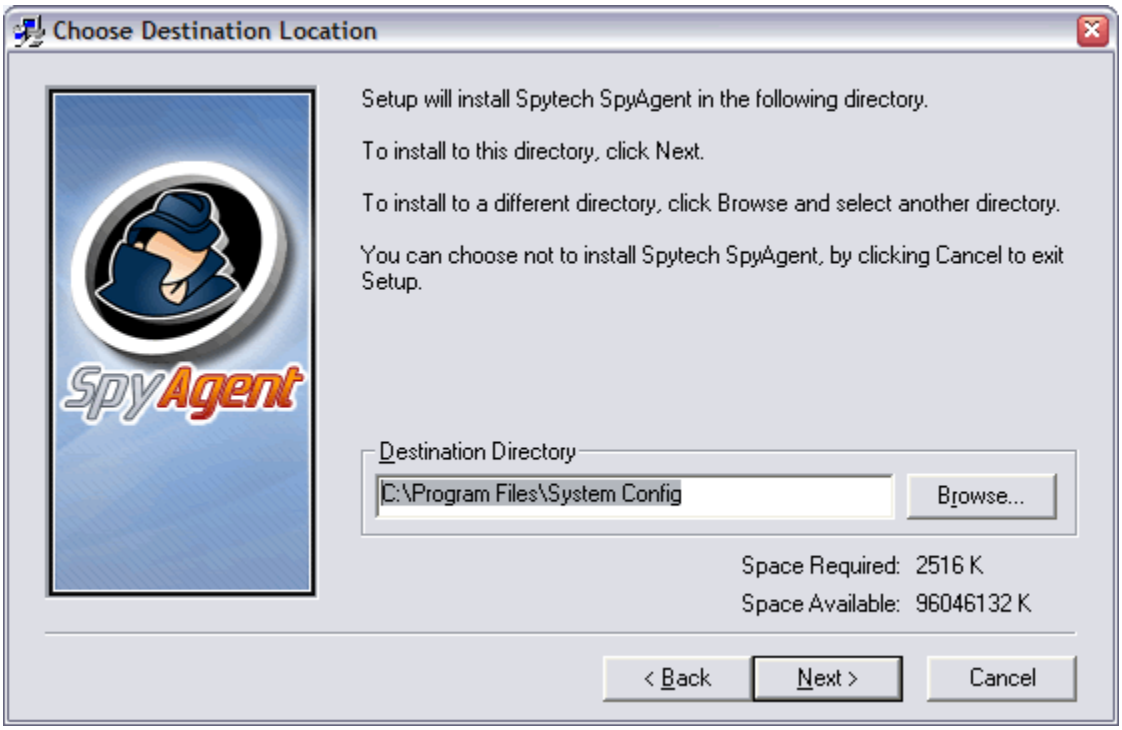
Step 1 - First of all download Spytech Spyagent, after downloading your copy of SpyAgent navigate to where you downloaded (in this case it is on the Windows desktop). Double click the SpyAgent installer file to start the SpyAgent install.



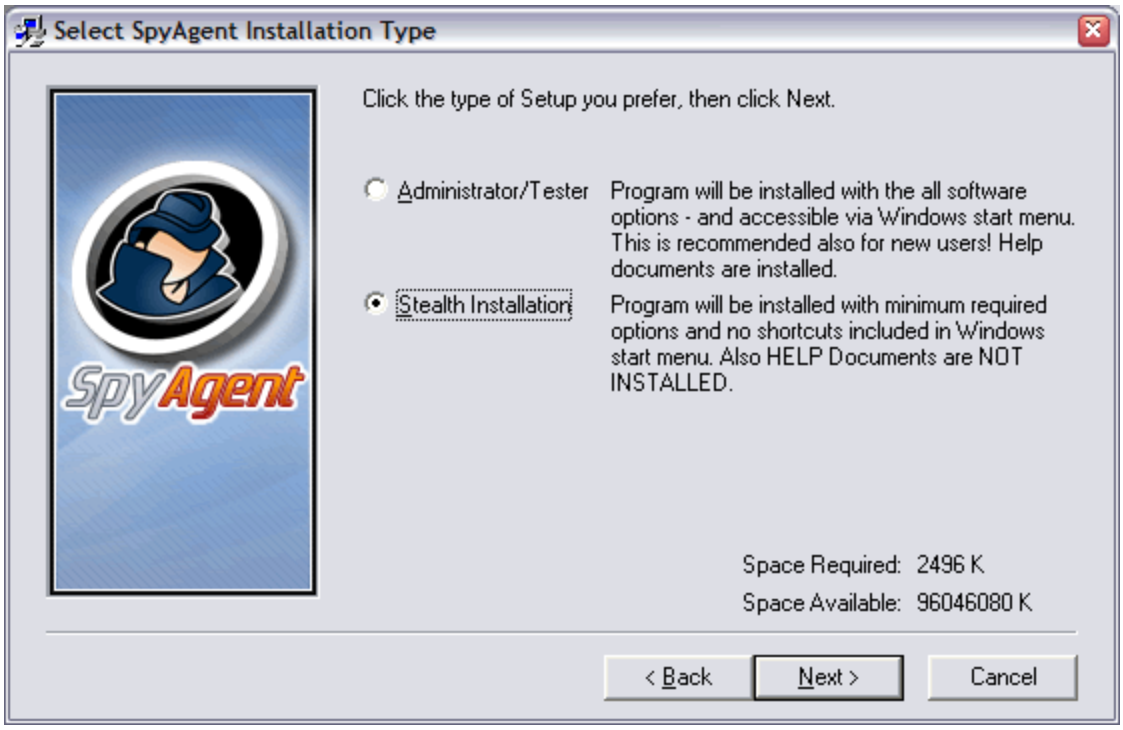
NOTE: After install is complete you can delete this file!

Step 2 - Click through the installer until you come to this screen. This is where you choose the folder location for SpyAgent's install. We recommend you change this from the default (c:\program files\spytech software...) to the path below, or something of your own making. Make sure you remember this path to access the software!

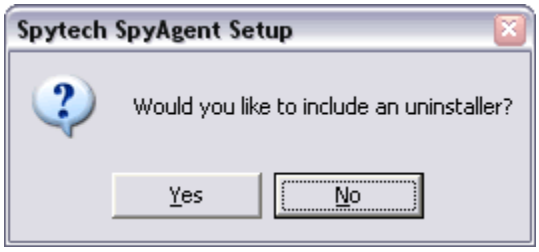
Once you configure the Destination Directory, click the Next button.



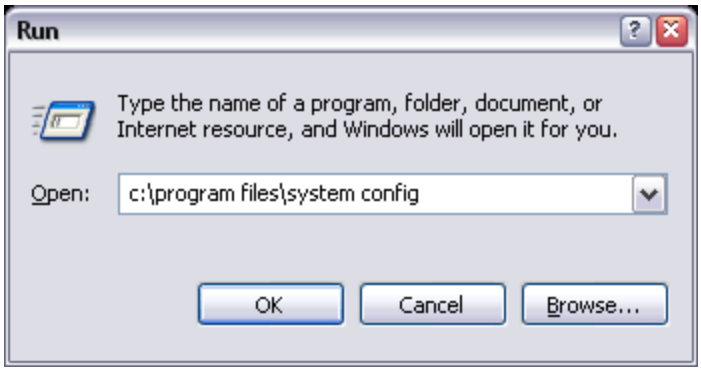
Step 3 - Click through the installer until you come to this screen. This is where you choose the install type for SpyAgent. If you want SpyAgent to not appear in the start menu and install the bare minimum files then choose the Stealth installation, as shown below. Click Next when you have done so.



Step 4 - When you are done configuring the install you will be asked if you want to include an uninstaller. For total stealth choose NO - as shown.

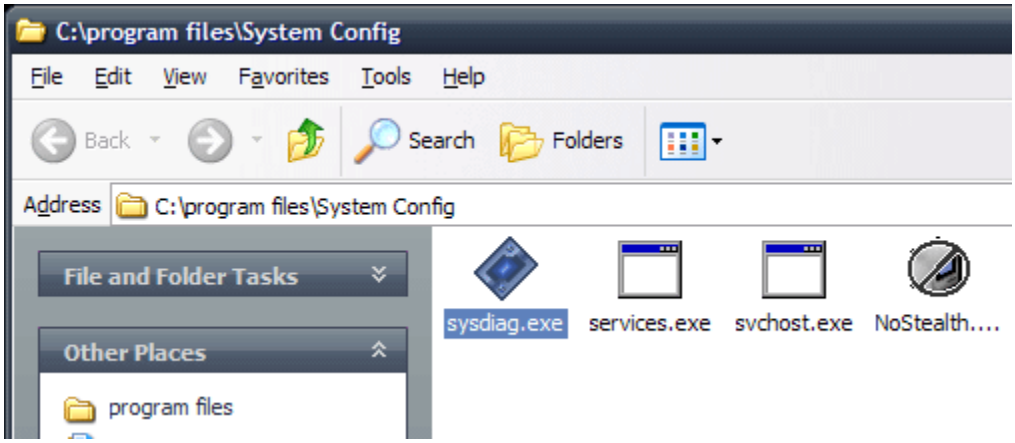


Step 5 - After your install completes you will now have to configure and run SpyAgent! Go to the START button on your desktop and click it once to bring up the Start menu. Choose the RUN... option to get the below window. You will have to enter your installation path (this is the

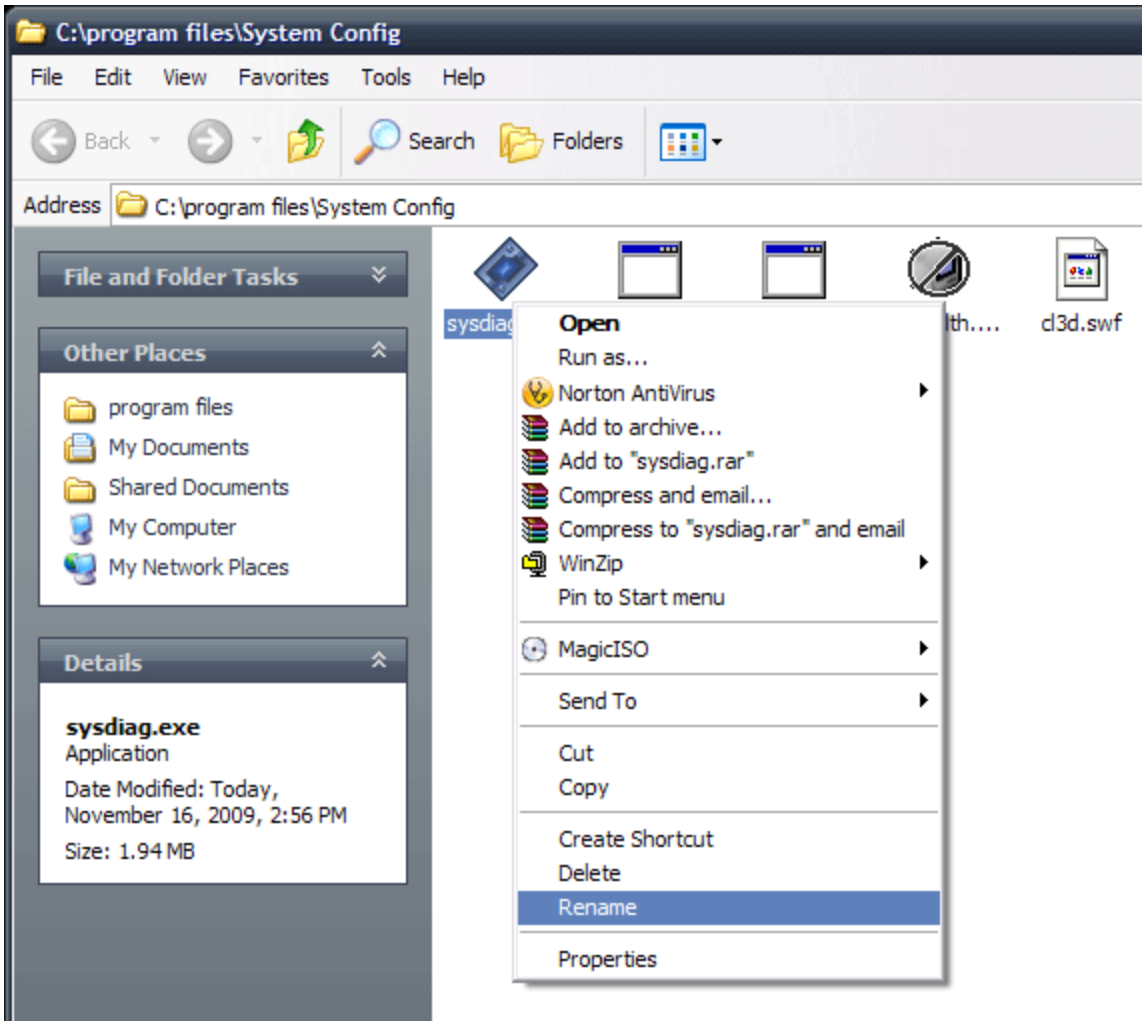


same path from the installer that you just entered!) When you have entered it press OK.

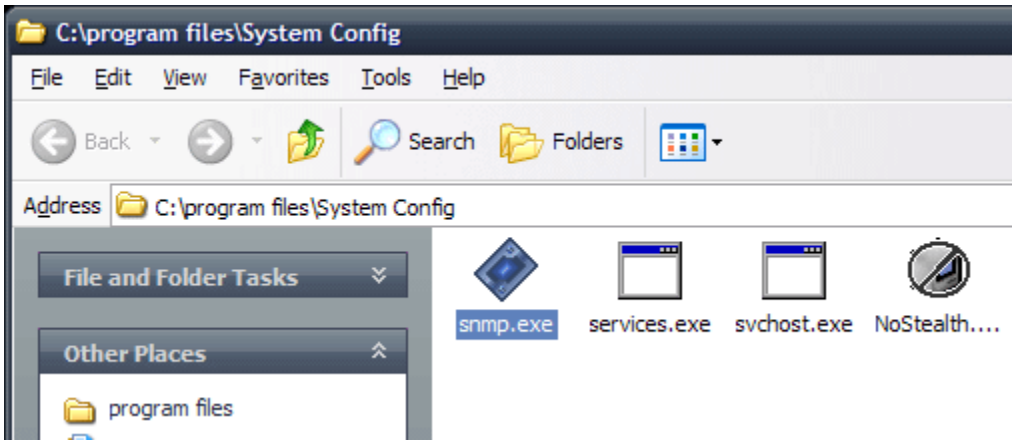
Step 6 (optional) - Once you are in the install directory you will see the SpyAgent files below if you have chosen Stealth install. Now, Highlight the sysdiag.exe file as shown below



Step 7 (optional) - Right click on the sysdiag.exe file and choose RENAME from the menu by clicking on it.

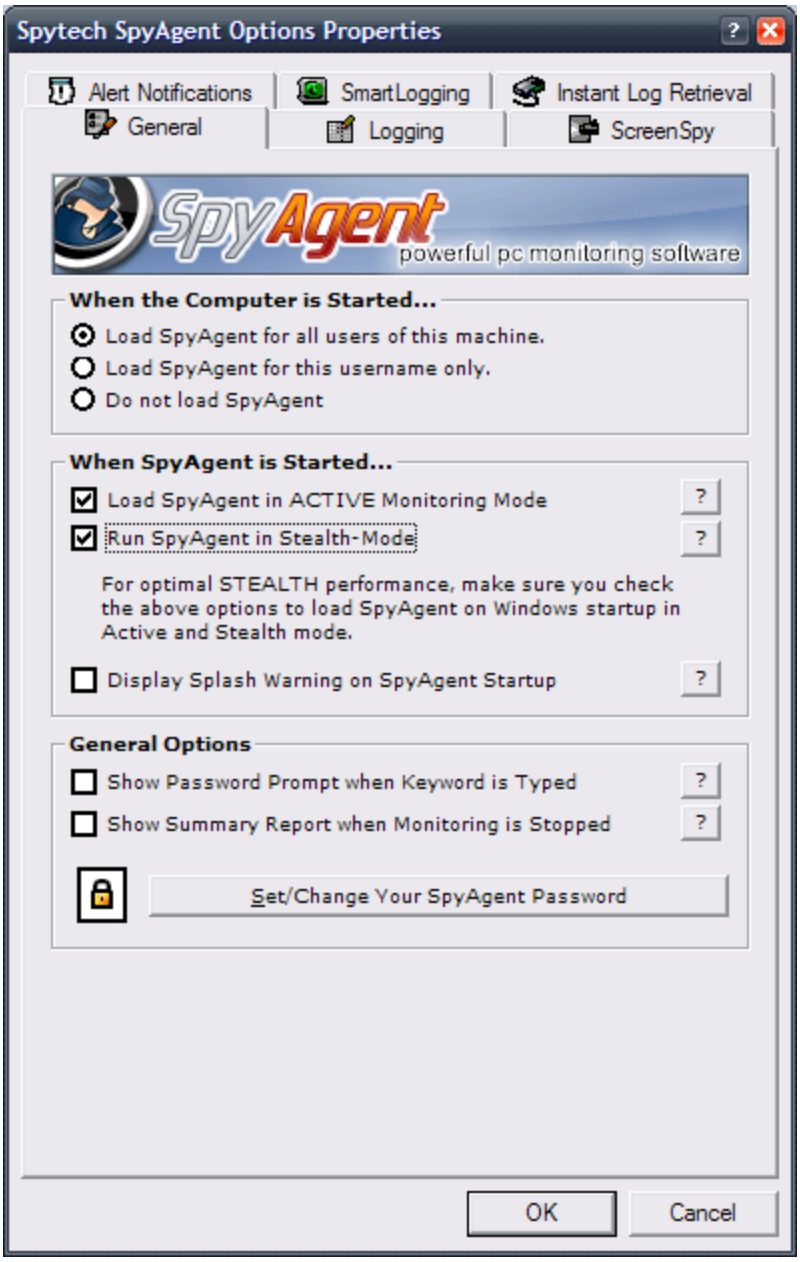


Step 8 (optional) - You will now be able to type a new name in for sysdiag.exe. As you can see below we chose to name it "snmp.exe". Use the below name, or something of your making to conceal SpyAgent's identity.



Step 9 - After renaming you can now run SpyAgent by double clicking the file you renamed! You will be prompted to configure your password - do so. Once inside SpyAgent click on the 'GENERAL' button on the right side of the SpyAgent window. The below window will appear - enable the options exactly as you see in the below window.

After you configure the General options you can click the LOGGING tab and configure the logging options as well! When you are done click OK to save your options!

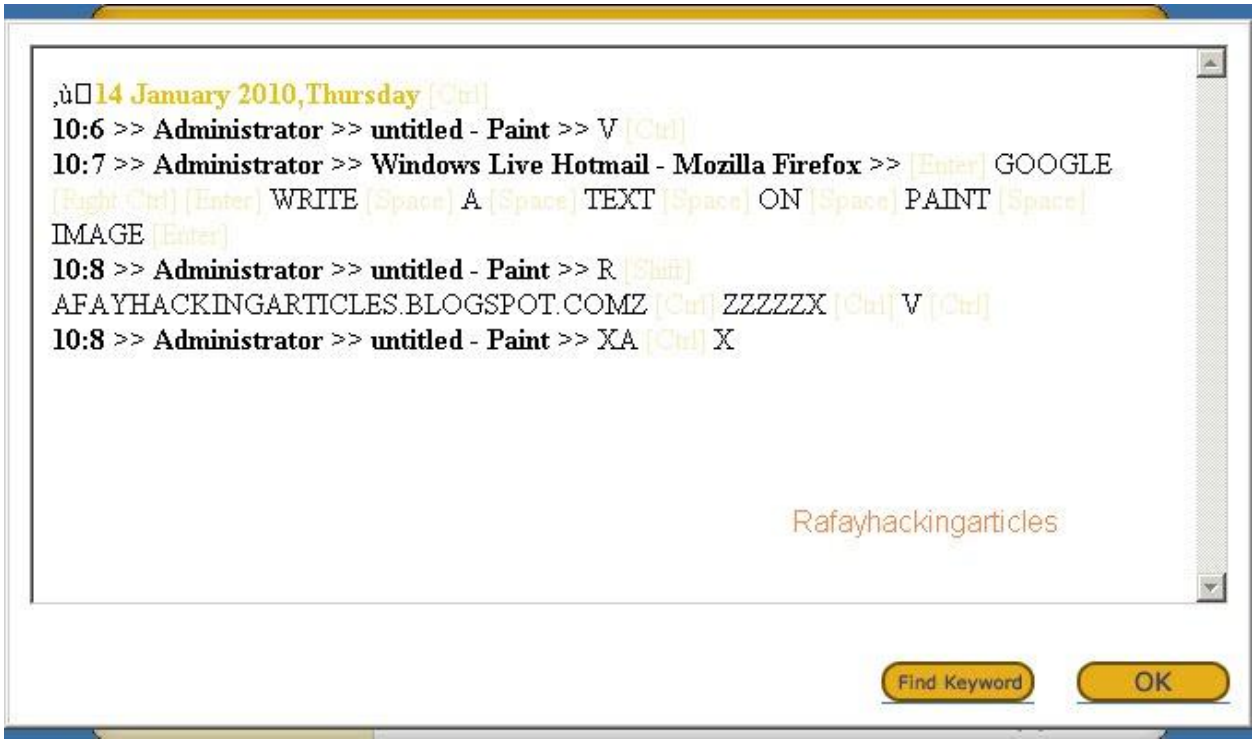


Step 10 - Almost done! Now all that is left to do is click the Start Monitoring button that is highlighted below! You will be prompted for your password - enter it, and click OK. You will receive a notification message on how to bring SpyAgent out of stealth mode to later view logs - read this message carefully!

Now SpyAgent is in total stealth. When you restart your PC it will run invisibly as well. To stop stealth mode run the nostealth.exe in the SpyAgent installation directory, or press CONTROL+SHIFT+ALT+M on your keyboard to bring up the password window!

AllSpyKeylogger

Allspy keylogger is best known for it user friendly interface, It can record keystrokes, Chatlogs, websites visited etc(Nothing Special), I guess all the other keyloggers have the ability to record all above things. The only thing I like about Allspy keylogger is that it has a very user-friendly interface and a person even with basic knowledge computer can use Allspy keylogger



Remote Keyloggers

Remote keyloggers are used for the purpose of monitoring a remote pc, Once a remote keylogger is installed on your computer the attacker can get your keystrokes, your webcam shots, chat logs etc sitting in any part of the world.

You can find tons of Remote keyloggers on web but lots of them are either not capable of properly recording keystrokes or they have a high antivirus detection rate, With my experience of 4 years in the field of Ethical hacking and security I have tested over 50 different keyloggers and have found just these two keyloggers worth the price:

1. **Sniperspy**
2. **Winspy**

Winspy Keylogger

WinSpy Software is a Complete Stealth Monitoring Software that can both monitor your Local PC and Remote PC. It includes Remote Install and Real-time Remote PC Viewer. Win Spy Software will capture anything the user sees or types on the keyboard.

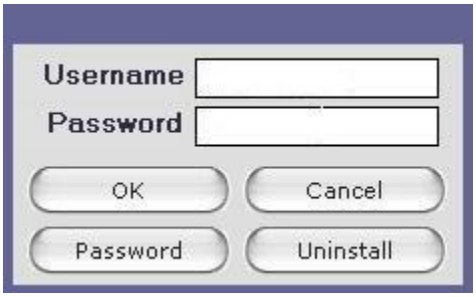
Below I will show you the exact method to how hackers can install a winspy keylogger on a victim's computer remotely.

Step 1 - First of all you need to **Download winspy keylogger**

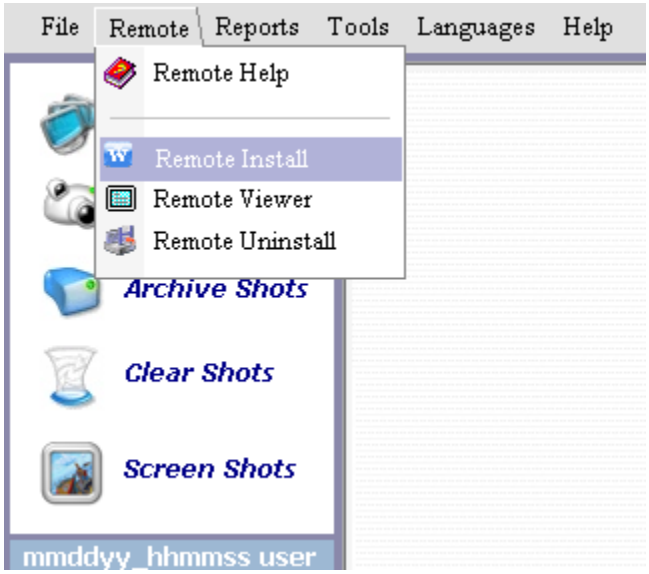
Step 2 - After downloading winspy keylogger run the application. On running, a dialog box will be prompted. Now, create a user-id and password on first run and hit apply password. Remember this password as it is required each time you start Winspy and even while uninstalling.

Step 3 - Now, another box will come, explaining you the hot keys(**Ctrl + Shift +F12)** to start the Winspy keylogger software.

Step 4 - Now pressing on the hot keys will take you a login box asking you to enter the username and password. Enter the username and password and click ok.



Step 5 - On entering the username and password you will be taken to winspy main screen. Now select **Remote at top** and **click on Remote install**.



Step 6 - On doing this you will be taken to the Remote install file creator. Enter the following things there:

User – Type in the victim's name.

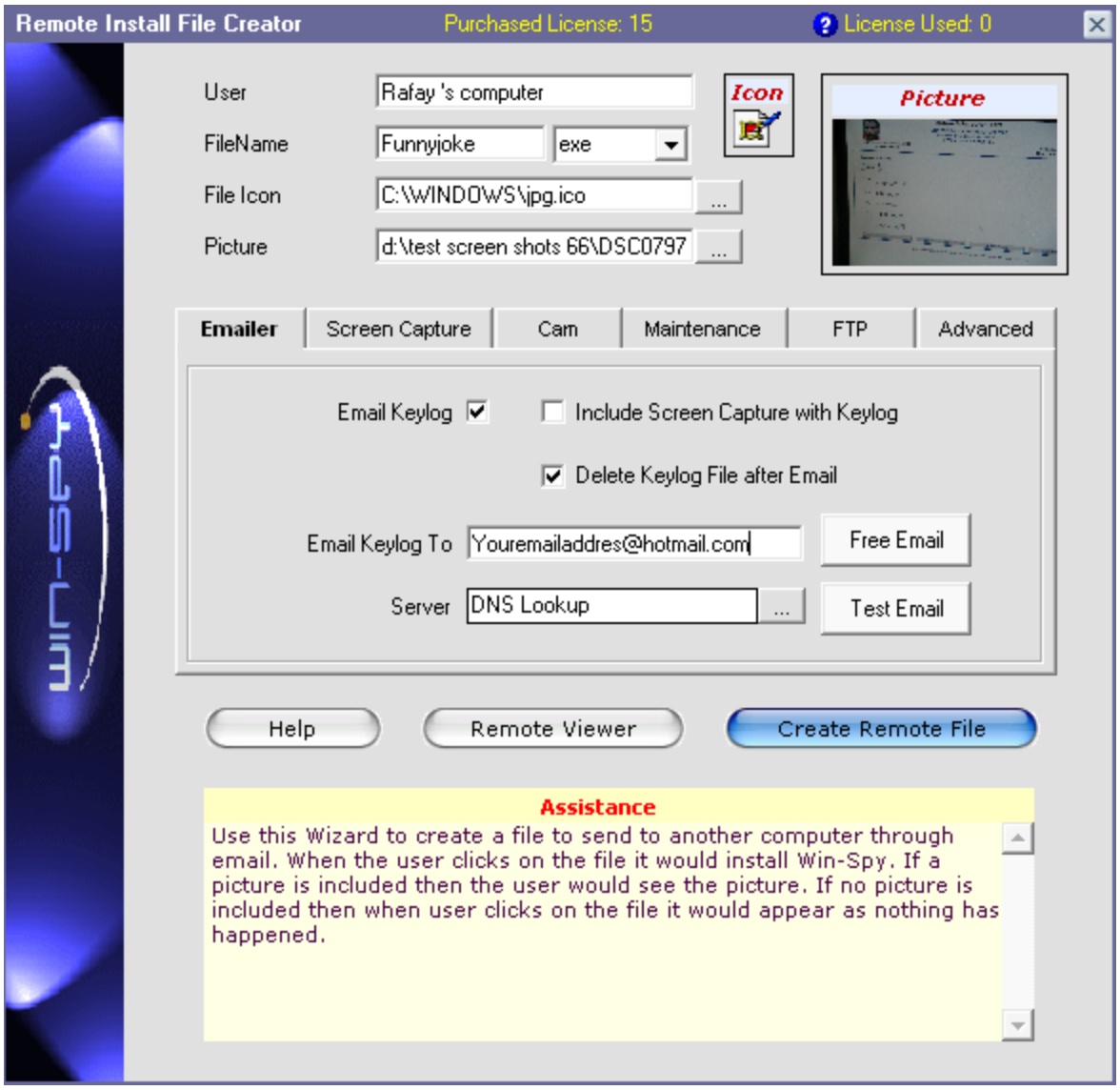
File Name – Here you need to enter the name of file needs to be sent. Like I have kept the name "**Funny joke**" which the victim will love to accept.

File icon – You really don't need to change this.

Picture – Select the picture you want to insert to the remote file.

Email log to – In this field enter your email address which you will use to receive the

Keystrokes - As hotmail account do not accept remote logs so it's necessary to use a Gmail account instead.

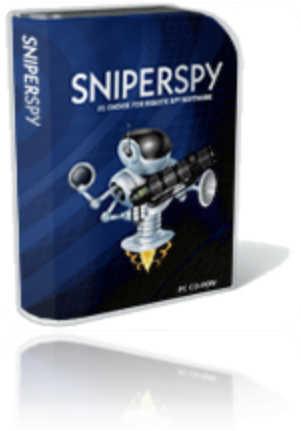


Step 7 - After you have done all the above steps, click on "**Create remote file**". Now the remote file will be created, it will look something like this.

Now all the hacker has to do is just to send the remote file to the victim via email attachment or by uploading it to a web-hosting site and then sending victim the download link. Once the remote file gets installed into victim's computer, you will receive keystrokes on your Gmail ID you entered in step 6.

Sniperspy Keylogger

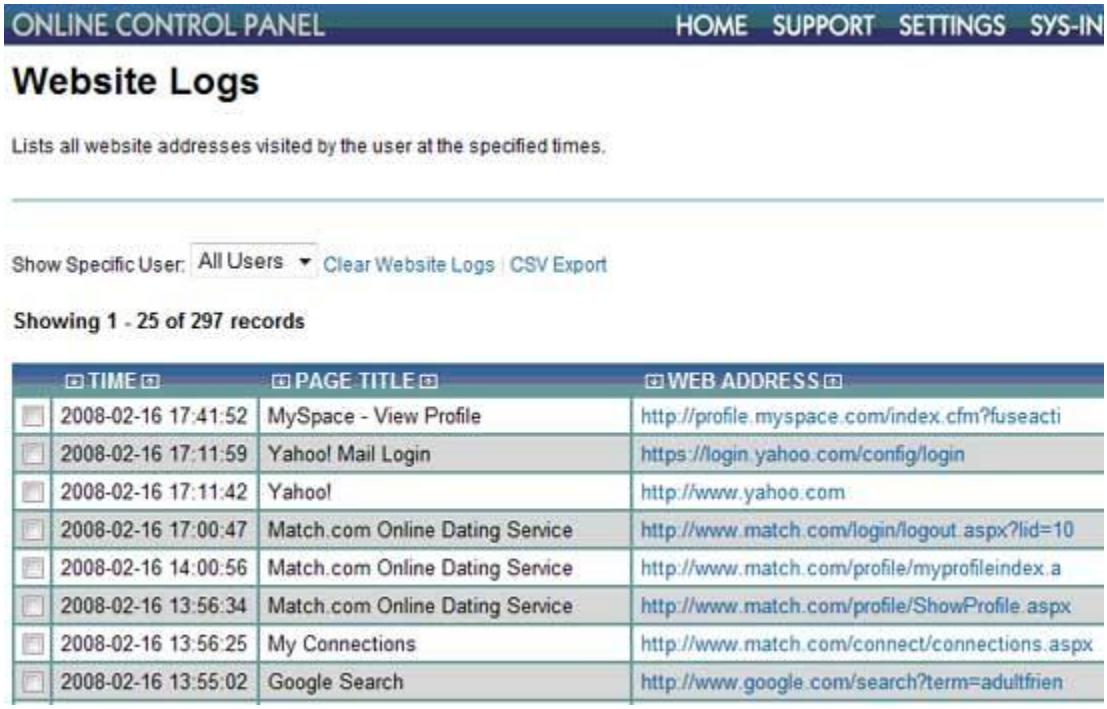
Sniperspy is one of my most favorite keyloggers, It is extremely powerful and has a very low antivirus detection rate. SniperSpy is the industry leading Remote password hacking software combined with the Remote Install and Remote Viewing feature.



Once installed on the remote PC(s) you wish, you only need to login to your own personal SniperSpy account to view activity logs of the remote PC's! This means that you can view logs of the remote PC's from anywhere in the world as long as you have internet access!

Do you want to Spy on a Remote PC? Expose the truth behind the lies! Unlike the rest, SniperSpy allows you to remotely spy any PC like a television! Watch what happens on the screen LIVE! The only remote PC spy software with a SECURE control panel!

This Remote PC Spy software also saves screenshots along with text logs of chats, websites, keystrokes in any language and more. Remotely view everything your child, employee or anyone does while they use your distant PC. Includes LIVE admin and control commands!



Screen shot of website logs for victims computer on sniperspy control panel

Which software keylogger is better Sniperspy or Winspy?

I recommend Sniperspy for the following reasons:

1. Sniperspy is Fully compatible with windows vista,but winspy has known Compatibility issues with Windows vista

2. It has low antivirus detection rate

3. Sniperspy can bypass firewall but Winspy cant.

4. Sniperspy is recognized by CNN,BBC,CBS and other popular news network,

Hence it is reputed and trustworthy.

Keyloggers for Mac

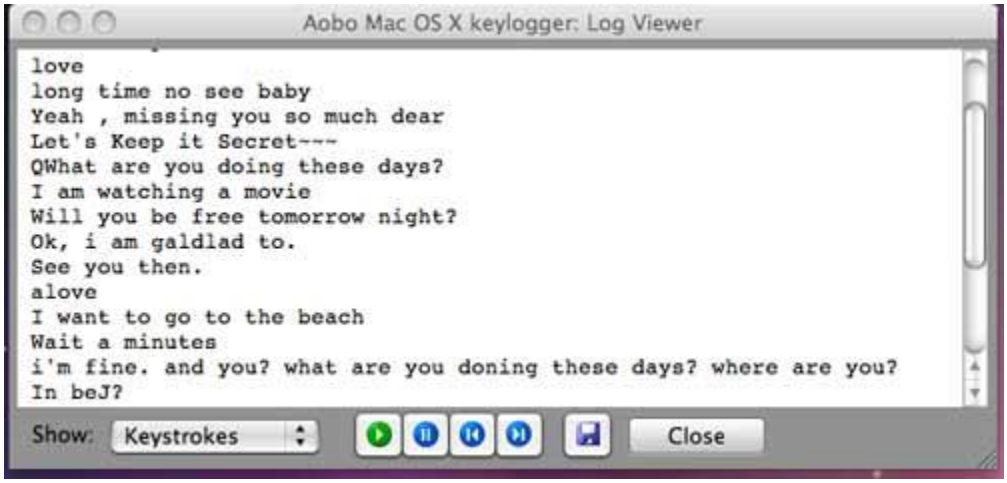
At this point you might be wondering if these above said keyloggers work on Mac OS or not, the answer is no because almost all keyloggers are made for windows platform, you will hardly find a free keylogger for Mac OS. So let's look at few popular keylogger softwares for Mac OS.

Abobo Mac OS X

A year back Abobo used to be the only keylogger for monitoring mac os boxes. But now there are lots of Keyloggers available for mac but honestly lots of them are not capable for recording passwords.

Features

- Record keystrokes typed except passwords
- Record desktop screenshots by interval Typed
- Record websites visited, chat conversations typed
- Record keystrokes typed in Email content
- Stealth & undetectable Monitoring, Recording
- Secretly send logs to email box or FTP space



Screen shot of MSN chat recorded by Abobo Keylogger For Mac

There are two versions of Abobo Mac OS:

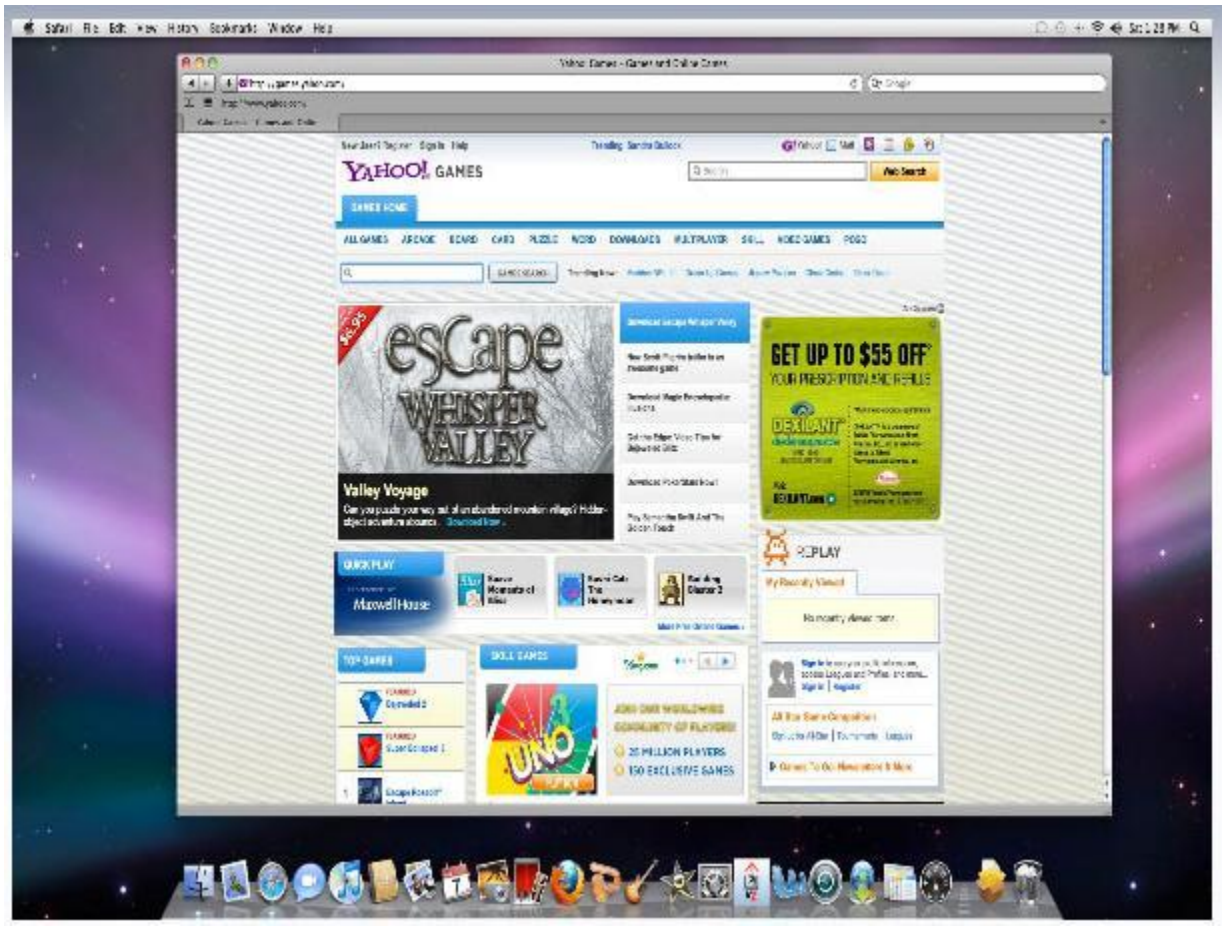
1. Abobo Mac OS Standard Edition (79.95 USD)

2. Abobo Mac OS Professional Edition (399.95 USD)

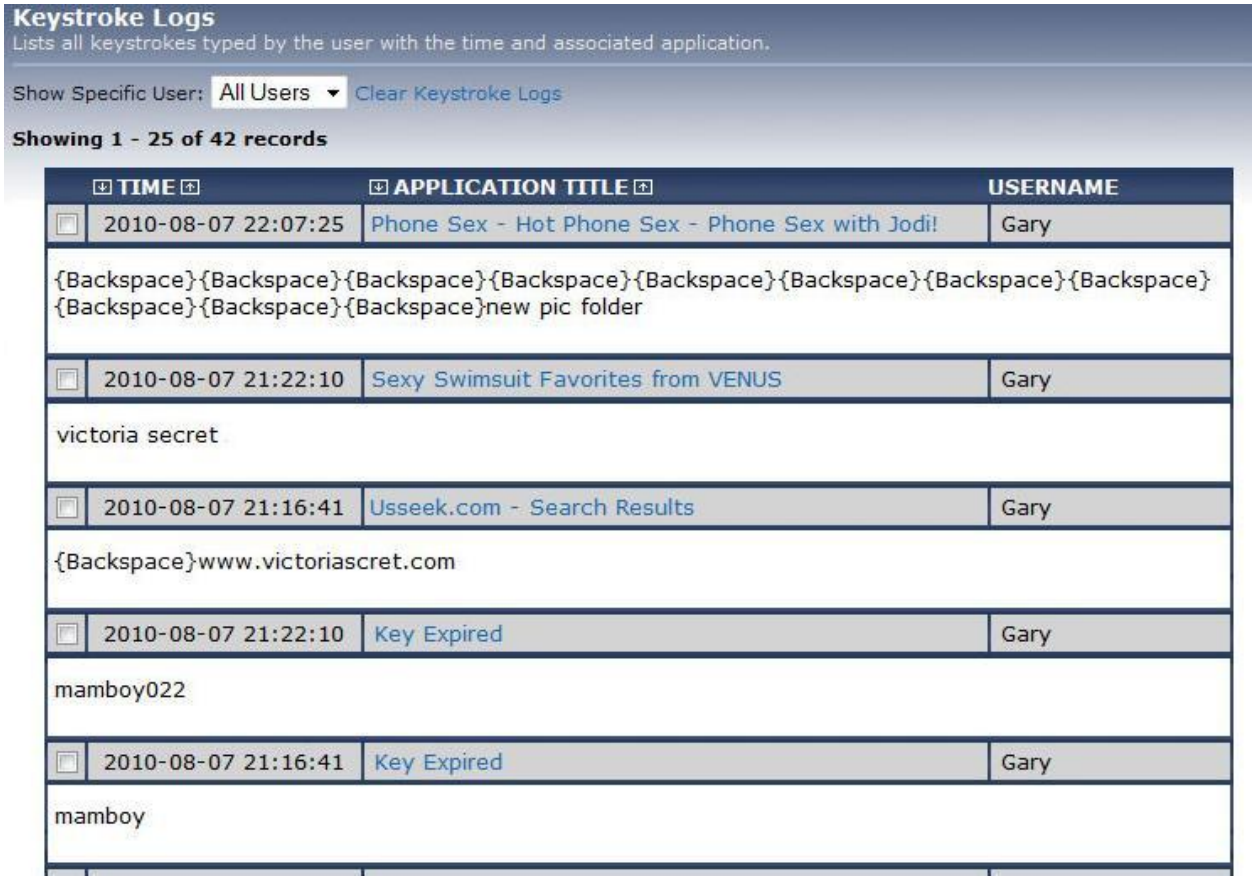
The problem with the standard edition is that it does not record passwords and thus it's of no use, However if you want to record screenshots, Chats etc then you should go for it, Talking about Professional edition I think it's quite expensive and frankly speaking not worth the cost.

Sniperspy for Mac

Sniperspy mac is the ideal choice for those who are looking to monitor a Mac computer. SniperSpy is the only software that allows you to secretly watch your Macintosh like a television! Login from ANYWHERE using another computer, smartphone or iPad



Screen capture by sniperspy mac



Keystroke Logs
Lists all keystrokes typed by the user with the time and associated application.

Show Specific User: All Users Clear Keystroke Logs

Showing 1 - 25 of 42 records

TIME	APPLICATION TITLE	USERNAME
2010-08-07 22:07:25	Phone Sex - Hot Phone Sex - Phone Sex with Jodi!	Gary
{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}{Backspace}new pic folder		
2010-08-07 21:22:10	Sexy Swimsuit Favorites from VENUS	Gary
victoria secret		
2010-08-07 21:16:41	Usseek.com - Search Results	Gary
{Backspace}www.victoriascret.com		
2010-08-07 21:22:10	Key Expired	Gary
mamboy022		
2010-08-07 21:16:41	Key Expired	Gary
mamboy		

Keystrokes recorded by Sniperspy mac

Keylogger for Linux

Lots of people actually believe that Trojans are invalid against linux operating systems but the reality is that Trojan are valid against linux operating systems but they infect in a different manner

LKL is a famous linux keylogger that runs under Linux on the x86 arch. LKL sniffs and logs everything that passes through the hardware keyboard port (0x60). It translates keycodes to ASCII with a keymap file.

Binders

A binder is small piece software used to bind or combine to or more files under one name and extension. Powerful keyloggers such as sniperspy have build in binders. As some of you might know that most of viruses come with .exe extension so the victim can get suspicious and is less likely to run the file. With binders you can easily bind a file with .exe extension with other extensions such as .mp3, .bat, .jpeg.

Some of the popular binders are as follows:

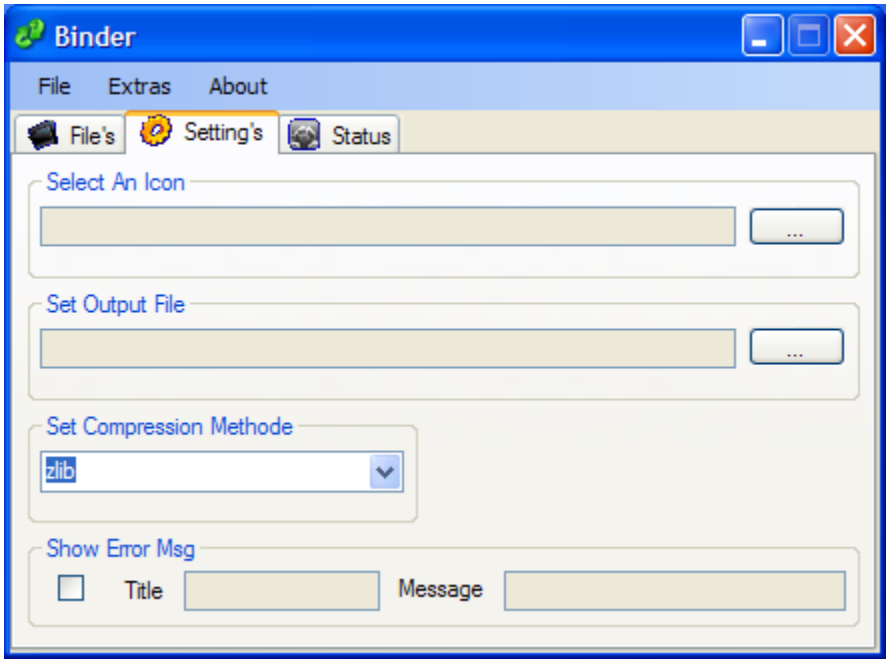
Simple Binder

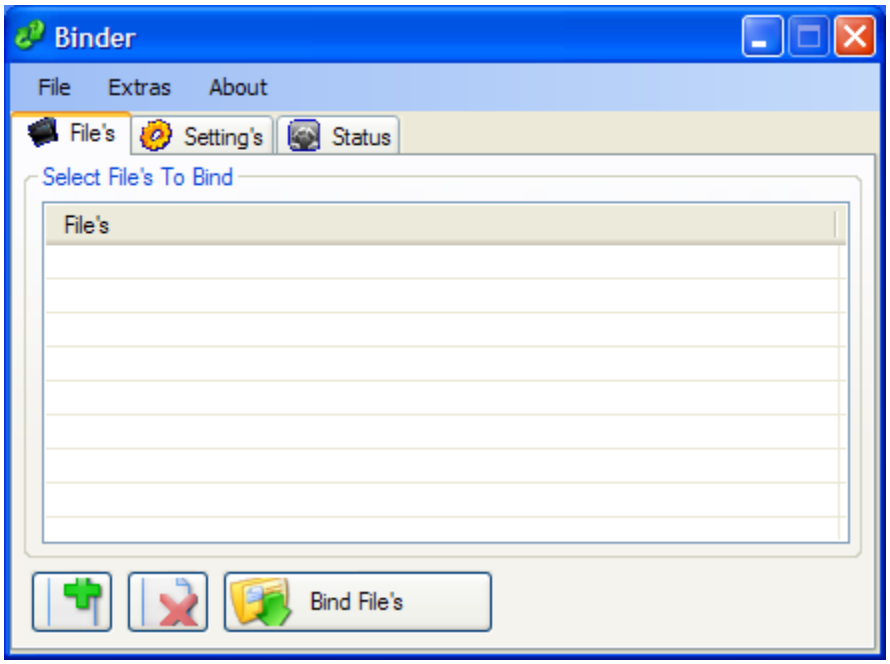
Simple binder is one of my favorite binders of all time, I give thumbs up to the maker "Nathan", It's so easy to use and even a script kiddie can easily use it to bind keylogger or backdoors with other files

Weekend Binder

Weekend Binder can be used to bind two or more files under one extension and icon, if the binded file contains an application, the application also runs along with the actual binded files.

Easy Binders





As the name reveals the meaning that it is a simple binder and very easy to use. Easy Binder has capability to combine or bind unlimited, it doesn't matter the file is of which type easy binder has the ability to bind it. The best part is that the icon of the Host file can be changed

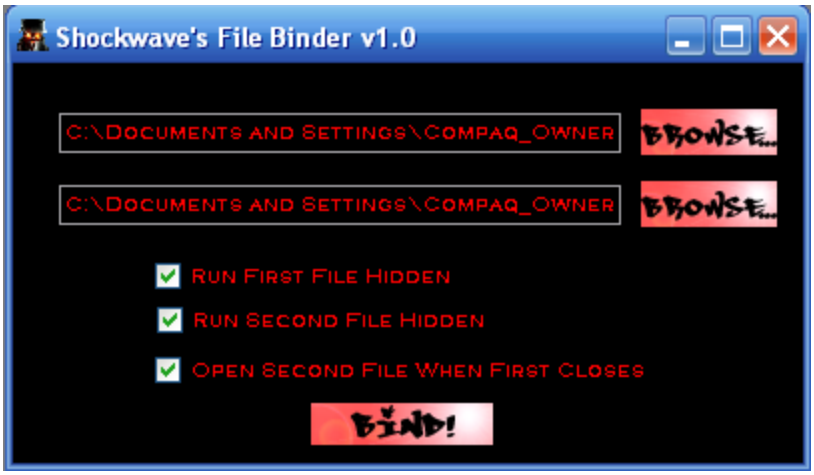
Shockwave File Binder

Shockwave file binder is one of very popular binders, it is self explanatory and has a user friendly design, here is how you can use a shockwave file binder.

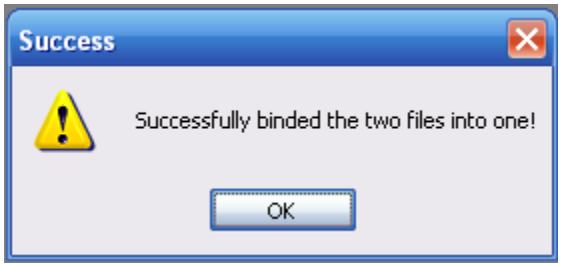
1. Once you have opened shockwave's file binder it will look like this:

2. Now in the first form select original file

3. In the second form select the file you wish to bind with it.



4. Once you have completed the first three steps the following screen will appear:



How Does Antivirus Work?

Before I tell you some techniques which hackers use to bypass antivirus detection while installing keyloggers, you need to understand first that how keyloggers work.

An antivirus uses a variety of strategies to detect malicious programs, the most common method is a **signature based detection** method, An antivirus has a database of antivirus signatures which basically are the sample malware codes, when a program is scanned by an antivirus the antivirus compares the malware code or malicious code with the code of the program being scanned and thus reports if the program is malicious or not.

Now signature based detection method is good but you need to update your antivirus regularly in order to add protection against latest malwares.

The other method which an antivirus uses is **Heuristic-based method** where a malicious program is identified by its suspicious behavior. This approach can be helpful against new types of malwares.

Now as you know how an antivirus software works, I will introduce you to some of antivirus bypassing techniques which hackers use to evade antivirus detection while installating a malicious program such as a Trojan or keylogger.

Crypters

Crypting is one of the popular methods used for antivirus evading due to it's simplicity and also because it does not require any prior knowledge about any programming language.

How Crypters Work?

A crypter is a small program that allows the attacker to crypt the source code of a Trojan or any form of malware, A crypter basically jumbles the source of the file to make it undetectable, As I told you before that an antivirus use a signature based detection, the crypter jumbles the source so when an antivirus scans the virus it cannot detect it.

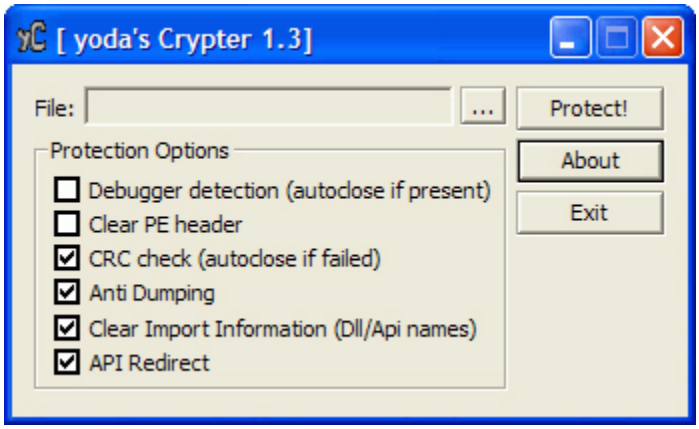
What is a FUD?

You might hear about "**FUD Virus**", "**FUD Trojan**" and might be wondering what this "**FUD**" thing is. FUD basically stands for "**Fully Undetectable**" which simply means that a server, Trojan or a virus which cannot be detected by an antivirus. FUD server is very difficult to achieve, you are very lucky if you can find any binders or crypters out there which is FUD. Free Crypters lose their affectivity as antivirus makes or composes a signature for them, however paid crypters are said to be Fully undetectable.

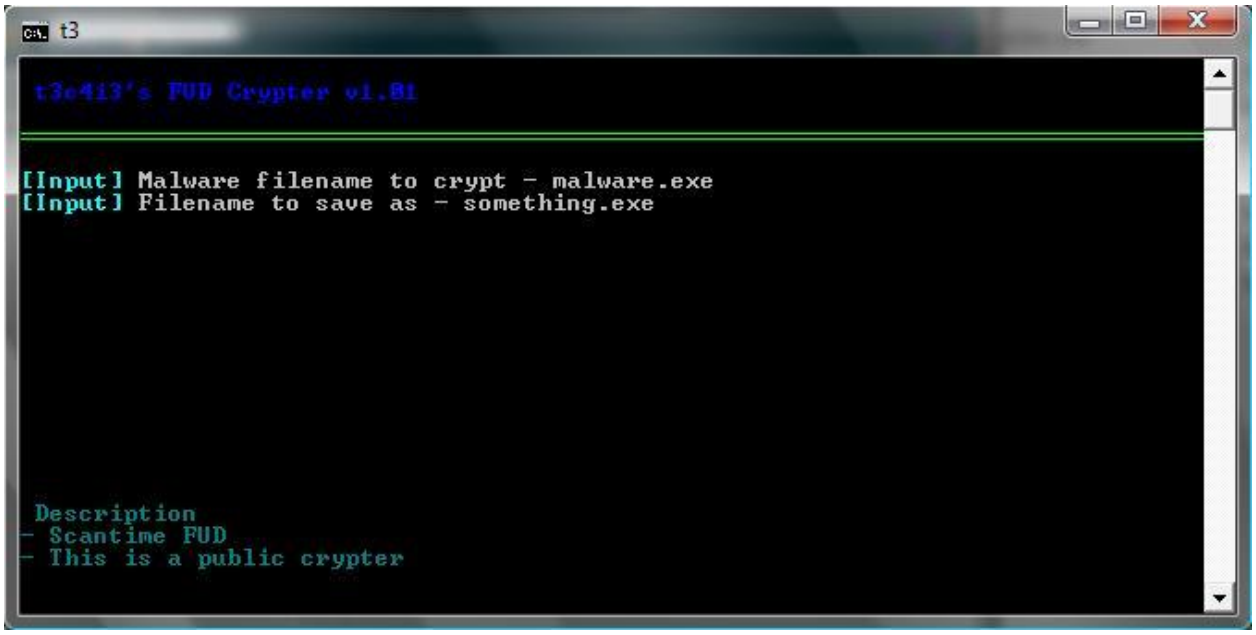
Here are some of the commonly used crypters:

Ultimate Crypter – Ultimate crypter is one of the most commonly used crypters around, Ultimate crypter may not be able to achieve a FUD server but it has a very low detection rate. It has a paid version too which claims to make the server FUD however I haven't tried it

Yoda's Crypter – Yoda's crypter has a lower antivirus detection rate than ultimate crypter, it has a user friendly graphical representation and is very easy to use.



T3c4i3 Crypter - [T3c4i3 crypter](#) used to be fully undetectable when I used it couple of months ago but now antiviruses have composed signatures for it, The way it works it that it crypts the source code of the program and assigns individual code within the code and therefore antiviruses do not detect it



There are lots of crypters available online just google for them and you will find tons of them for free.

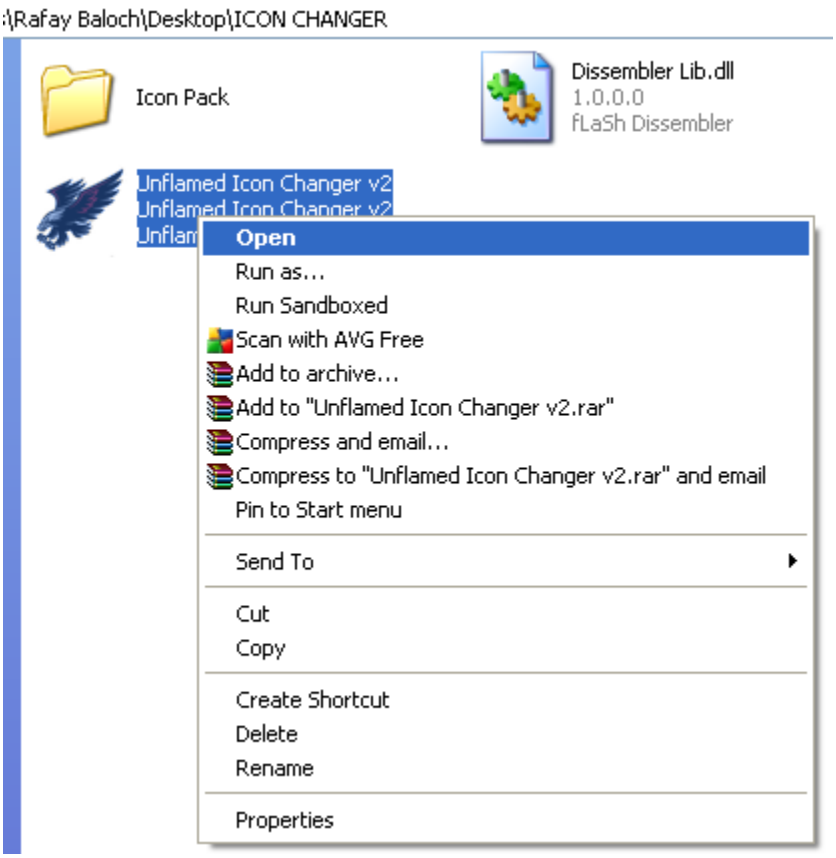
Icon changing

Icon changing is another method adopted by hackers to make a server undetectable. There are lots of servers, Trojans and viruses which are recognized by antivirus because their icon contains virus signatures so it's not a good option to use the default Icon.

Along with making a server undetectable it prevents the victim from being suspicious, there are various softwares for icon changing however we will look at software called "**Icon changer V2**", Icon changer also allows you to change icons for binded files which makes your work a lot easier.

Here is how you can use "Icon changer v2" to change icon for your server:

1. First of all download and install Icon changer
2. Next extract the files into a folder
3. Now run the file "**Unflamed Icon changer**"



4. Now simply select the icon you want to use and click on **change** and the icon will be changed.

You can also use your own icon, simply make your icon and add the image to **"icon pack"** folder.

Hexing

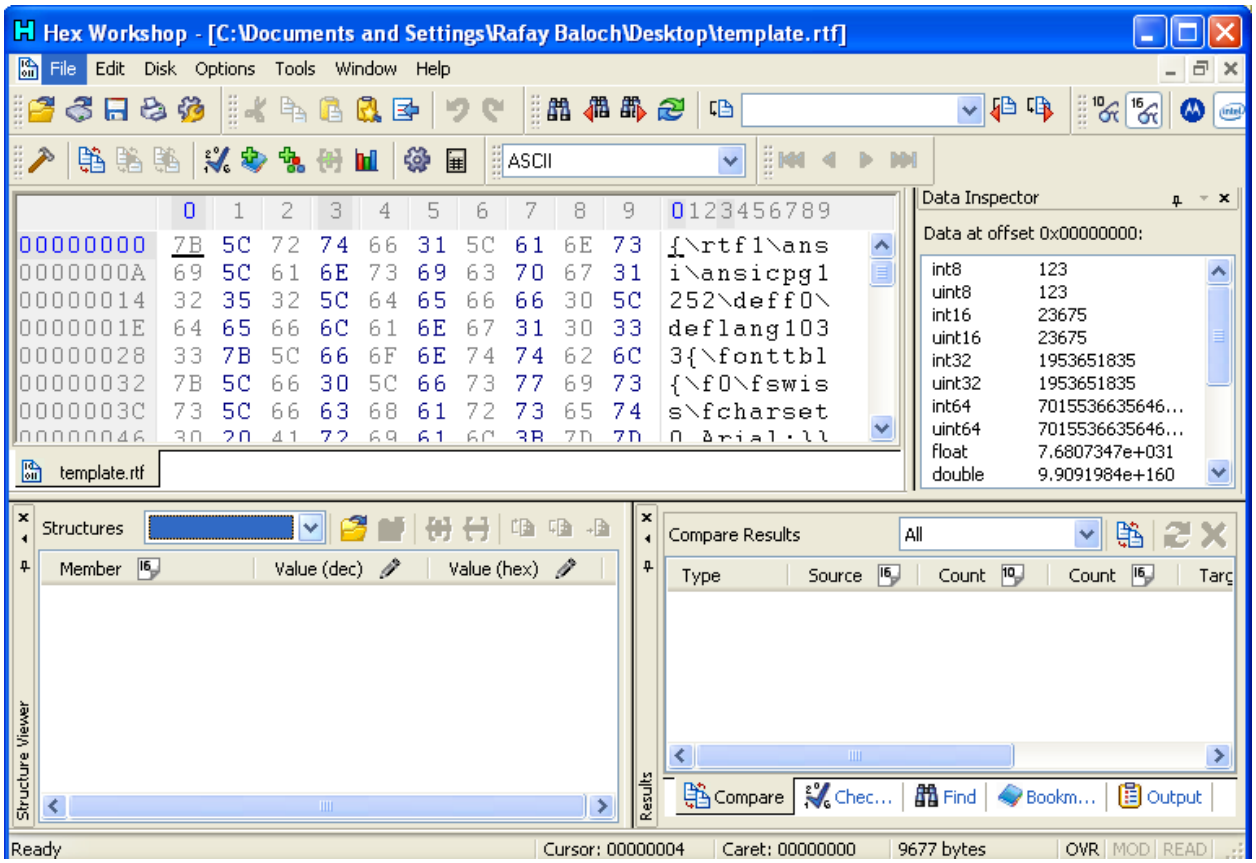
Hexing is another method used to achieve a fully undetectable server, Compared to Crypting, icon changing and binding this method has a greater success rate. Hexing or hex editing is not commonly used due to the complexity of this method.

How does Hexing work?

As you have learnt before that antiviruses use signature detection method. As I have told you before that an antivirus use various methods to detect a virus or a malicious software, In hex editing we search for the flagged signature and change it so the antivirus cannot detect it

What is a Hex Editor?

A hex editor is simply a program which is used for editing binary files. A hex editor is one of the most important program of your toolkit for Hexediting.



Stealers

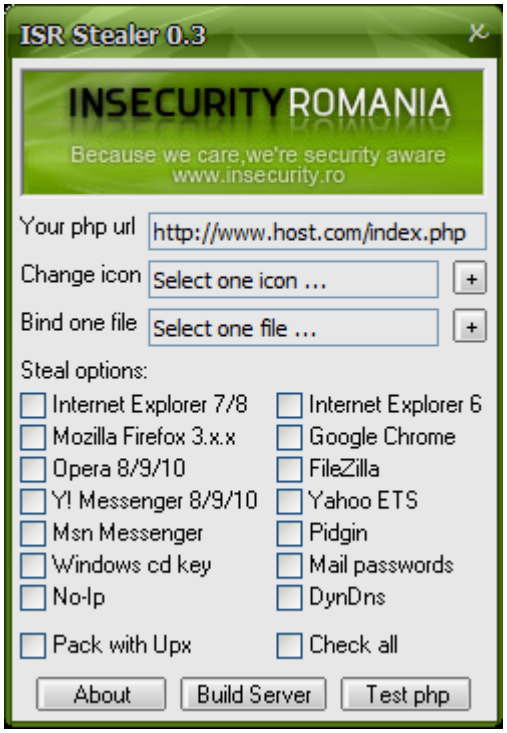
Stealers are a very common form of malware and at times are a major threat to your browser security. Almost all browsers have "**Remember My Password**" feature and almost 90% of users use this feature so they don't need to type username and password again but this could be very dangerous if you a hacker has used a stealer against your system.

The function is a stealer is just to steal saved passwords and send it to the attacker's server or his FTP account. Like keyloggers stealers are easily detected by antivirus software, you can use methods such as crypting, Hexing or icon changing to bypass antivirus detection.

ISTEALER –

Istealer is one of the most commonly used stealer due to its user friendly interface. It has also a paid version which is claimed to b undetectable by many antivirus softwares.

ISR STEALER –



ISR stealer is made by Romanian security team. ISR stealer can stael passwords from many applications such as FileZilla, Pidgin, MSN, yahoo etc

IStealer Server Setup

Setting up an Istealer server or ISR stealer server can be a bit complicated for users who are not familiar with web hosting stuff but once the server is up it's very easy to use.

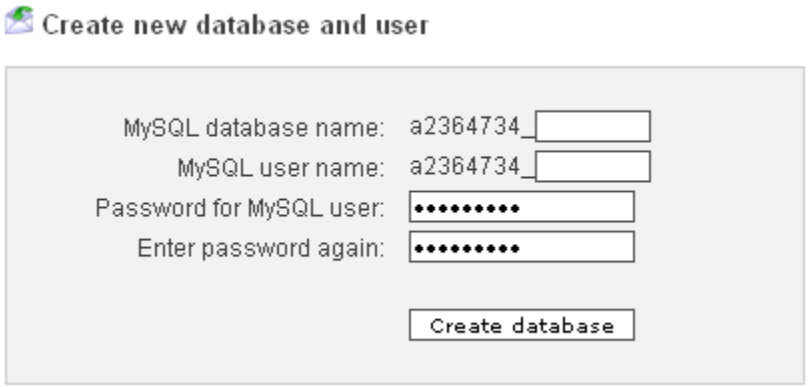
Requirements

1. IStealer

2. Freewebhosting account

1. First of all you need to create an account on a free webhosting site such as **freehostia.com**, **000webhost.com** etc.

2. Next you need to create a **mysql database**, To create a mysql server login to your free webhosting account(In my case it's 000webhost.com) and click on "**mysql**" select an appropriate username and password and click on "**Create database**"



3. Next open index.php in your PHP logger folder and paste the database information you received when you created your mysql database in step 2.

```
// CONFIGURATION ************************************************

$dbHost     = "localhost";       // (1)MySQL host
$dbUser     = "rafaybaloch";     // (3)MySQL username
$dbPass     = "password";  // (4)MySQL password
$dbDatabase = "username_db";     // (2)MySQL database name

$username   = "user";            // Login Username
$password   = "pass";            // Login Password

$logspage   = 100;               // Number of logs per page

// ************************************************************
```

Note: $username=”user” $password=”pass” are your username and password for istealer login

4. Once you have completed step number 3 save your index.php file.

5. Next upload your both files index.php and style.css, To upload go to file manager browse to the appropriate location of the files and click on upload button

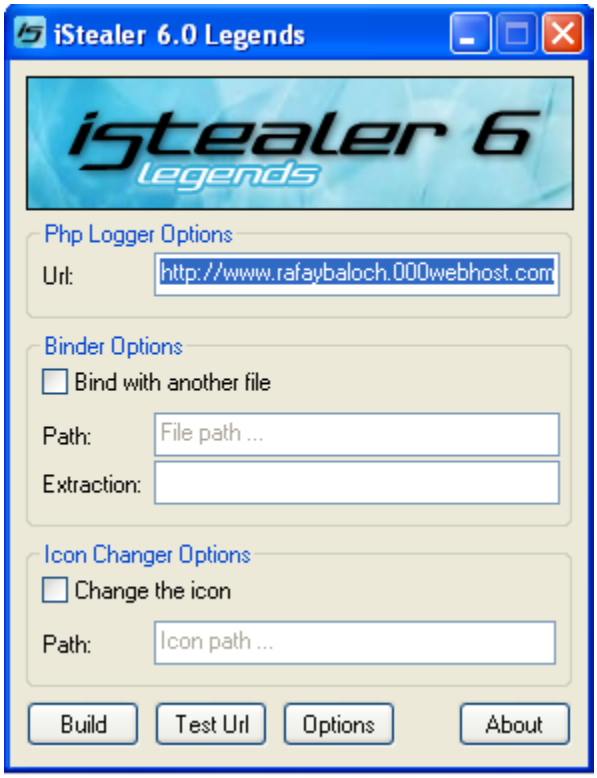
6. Next goto the filemanager again and click on index.php as you look at the address bar you will find a link similar to the below one:

   http://username.000webhost.com

7. Next login in with your username and password which you choose in the step 3

8. Next open Istealer.exe and replace the existing url with the following url:

   http://www.yourusername.000webhost.com



9. Now press “test” and check if your stealer is working correctly or not and then click on build to create a server.

RATS

RAT is the short form of "**Remote Administration Tool**". It's very similar to a Trojan. Once a RAT is installed in a computer the attacker can do almost anything on the remote computer such as installing a keylogger, controlling a computer, infecting files etc.

Commonly Used RATS

1. ProRat
2. Turkojan
3. Cybergate

PRORAT

ProRat is a Remote administration tool(RAT). Prorat opens a port on infected computer which allows the client to perform various operations on the infected computer. Once Prorat is installed on a computer it's very difficult to remove it without an updated Antivirus program. Below I will show the procedure which a hacker will take to take control of victims computer using Prorat.

1. First of all download Prorat. The password of zip file will be "Pro".

Note:Disable your Antivirus before using Prorat

Once you have downloaded it launch the program. You will see the following screen:

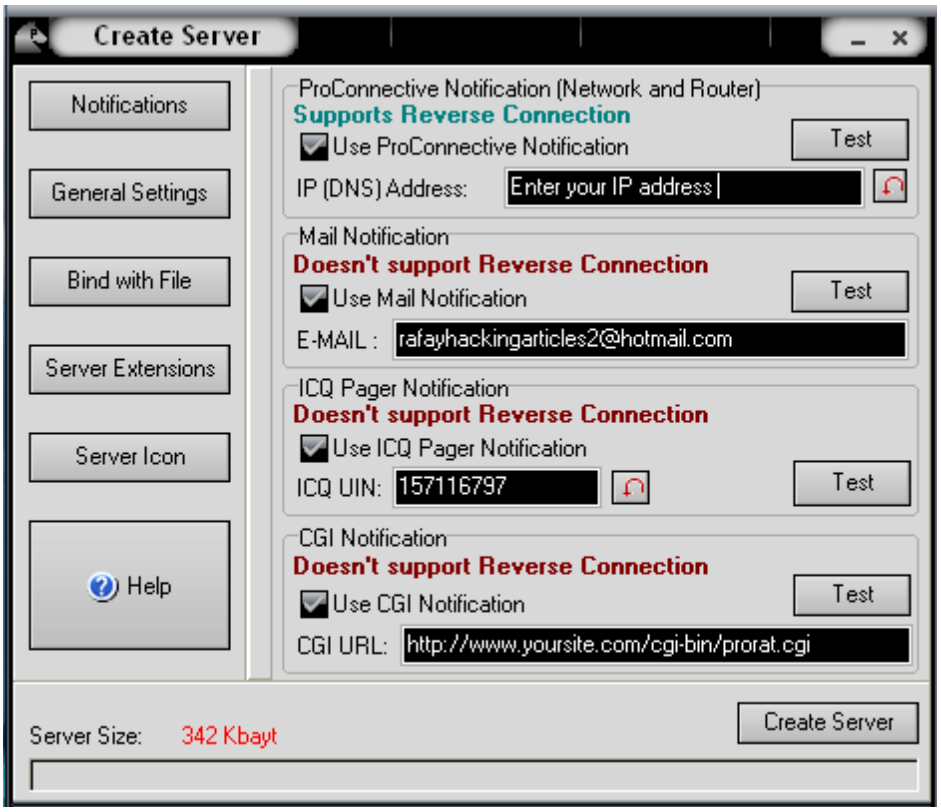
3. Click on the Create button at bottom to create the Trojan file and choose the Create prorat server.

4. Put your IP address in the IP(DNS) Address box so the server could connect you.

If you don't know you IP address click the red arrow and It will fill you IP address automatically.

5. Now open Notifications at the sidebar and select the second option "Mail

Notifications".Here you will an email address "**bomberman@yahoo.com**" change this to the email address where you want to receive notifications when the server is installed into your victims computer.

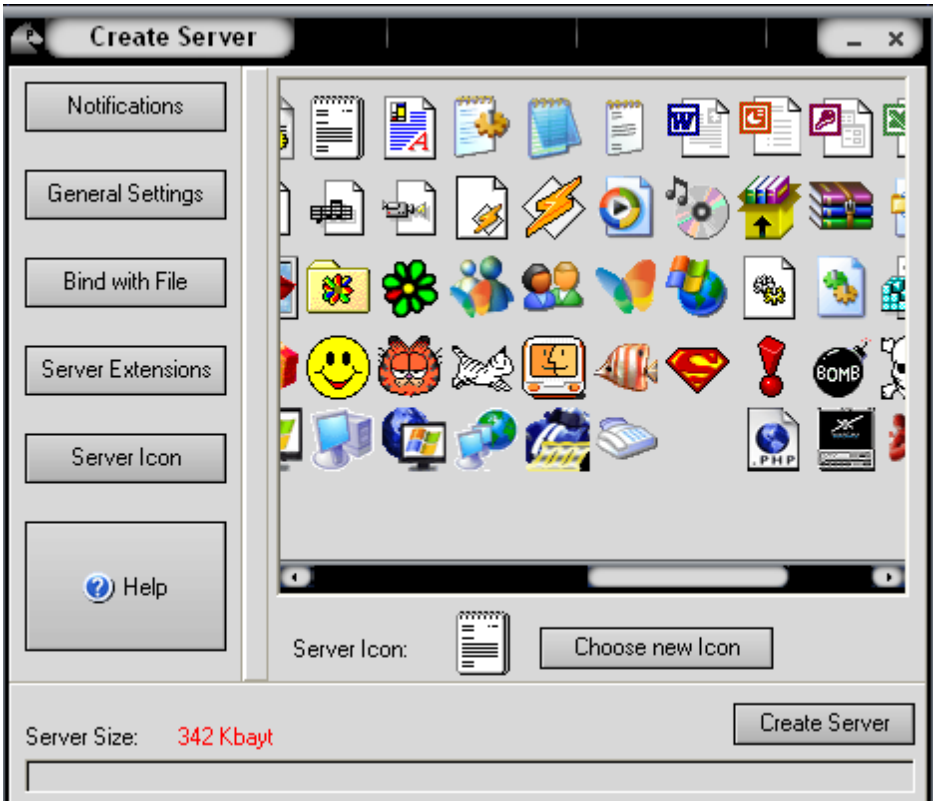


6. Now click on the General Setting option. Enter the server port you would like to connect through. Enter the server password, you will be asked for server password when the victim gets infected and you would like to connect to them and then choose the victim name. You can also tick the "**Give a fake error**" message option when the victim will open the server he will get a fake error message which you configure making victim think that the file is damaged or corrupted.

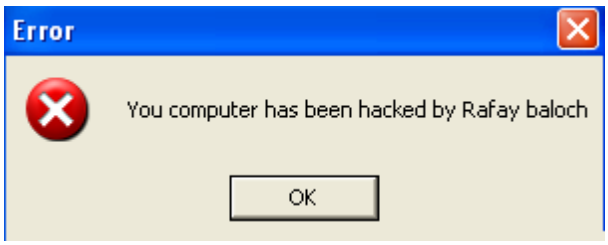
7. Click on Bind with file on the sidebar. You can bind it with a text document or any other file you may increase chances of victim to click it.

8. Now Click on Server extensions option. Here you can change the desired extension. I will use EXE because it has Icon support or you can also use SCR too it also has icon support too.

9. Now Click on server Icon and choose the desired icon you would like to display for the server and click on Create server.



Now you have successfully created a server. The hacker could rename it something like “Funny joke” and sent it via email attachment or alternatively the hacker could upload it to a webhosting site and just ask the victim to manually download it. Once the victims runs the server on his/her computer he will get an error message which I configured in the general settings tab.



The server gets installed silently in the computer background and the hacker will be sent a notification to the email address he described in the notification tab whenever the victim is infected.

Reversing a Keylogger, RAT Server

Till now you must have known and understood basic techniques which attackers use to evade antivirus detection of a virus, keylogger and a Trojan.

This section will explain you various techniques which can be used to reverse a keylogger, what reversing here means is extracting the passwords from a server. Now reversing a keylogger or a RAT server at some times be extremely complicated

Bintext

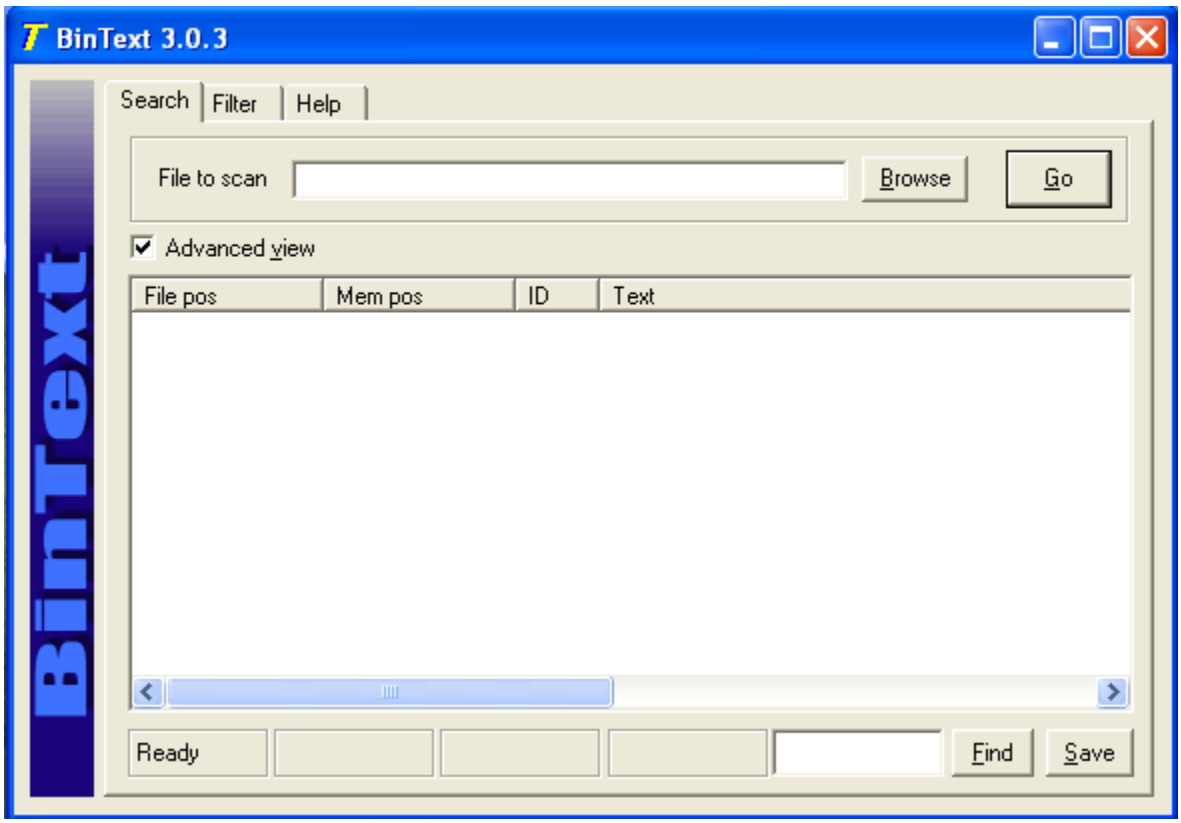
Now as you know that hotmail does not accept keystroke logs so therefore hackers use a gmail account to accept logs as I told you earlier in winspy installation guide. Bintext is extremely awesome software used for reversing a keylogger.

Bin Text a text extractor software used to extract text from application or any file, with bintext you can easily reverse a keylogger or a RAT server and extract the userid and password of the gmail account which on which the logs will be sent.

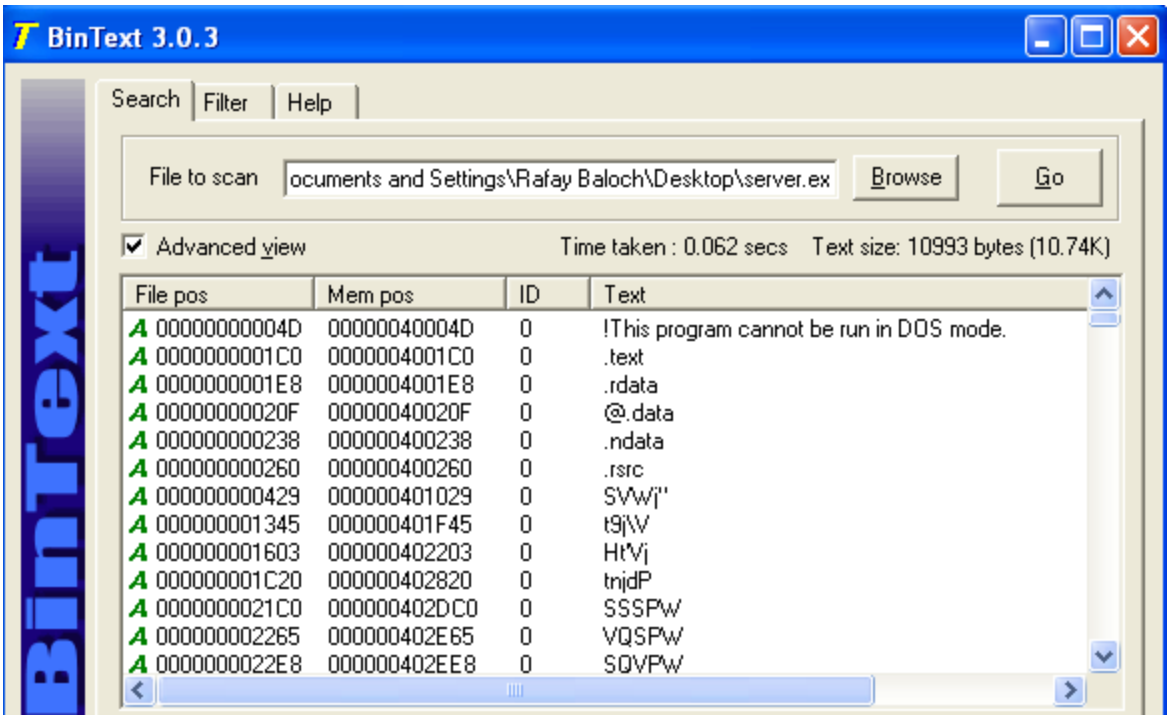
Requirements

1. Bintext
2. A Keylogger or a RAT server

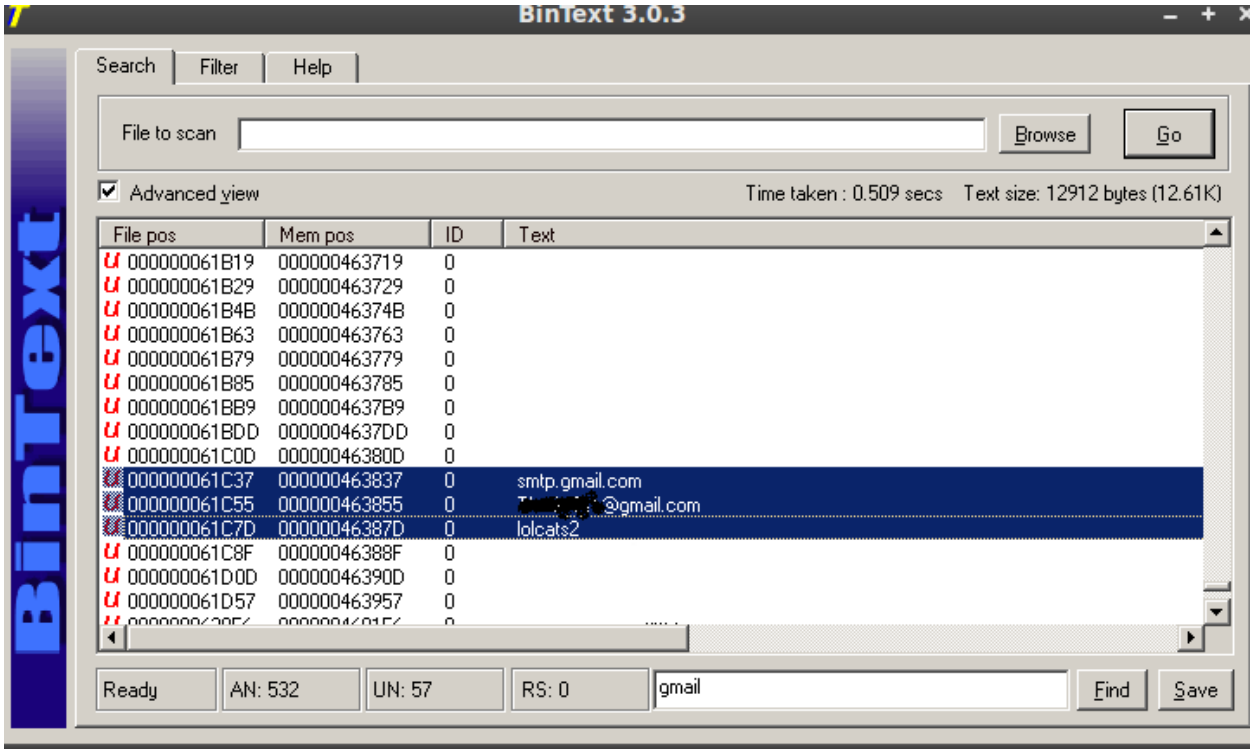
1. Once you have fulfilled the above requirements go ahead and start bintext



2. Next click on browse and locate the appropriate server file and click on the go button to load the program code.



3. Next go to the search bar at the bottom and search for the keyword “Gmail” and it will display the attacker’s Gmail username and password and you will come across a screen similar to the below one:


BinText 3.0.3
Search
Filter
Help
File to scan
Browse
Go
Advanced view
Time taken : 0.509 secs
Text size: 12912 bytes (12.61K)
File pos
Mem pos
ID
Text
000000061B19 000000463719 0
000000061B29 000000463729 0
000000061B4B 00000046374B 0
000000061B63 000000463763 0
000000061B79 000000463779 0
000000061B85 000000463785 0
000000061BB9 0000004637B9 0
000000061BDD 0000004637DD 0
000000061C0D 00000046380D 0
000000061C37 000000463837 0 smtp.gmail.com
000000061C55 000000463855 0 [redacted]@gmail.com
000000061C7D 00000046387D 0 lolcats2
000000061C8F 00000046388F 0
000000061D0D 00000046390D 0
000000061D57 000000463957 0
Ready
AN: 532
UN: 57
RS: 0
gmail
Find
Save

Wireshark

Wireshark previously called **Ethereal** is basically a packet sniffing tool but it can be used for various purposes, here I will tell you how you can use wireshark to reverse and find out its Ftp password.

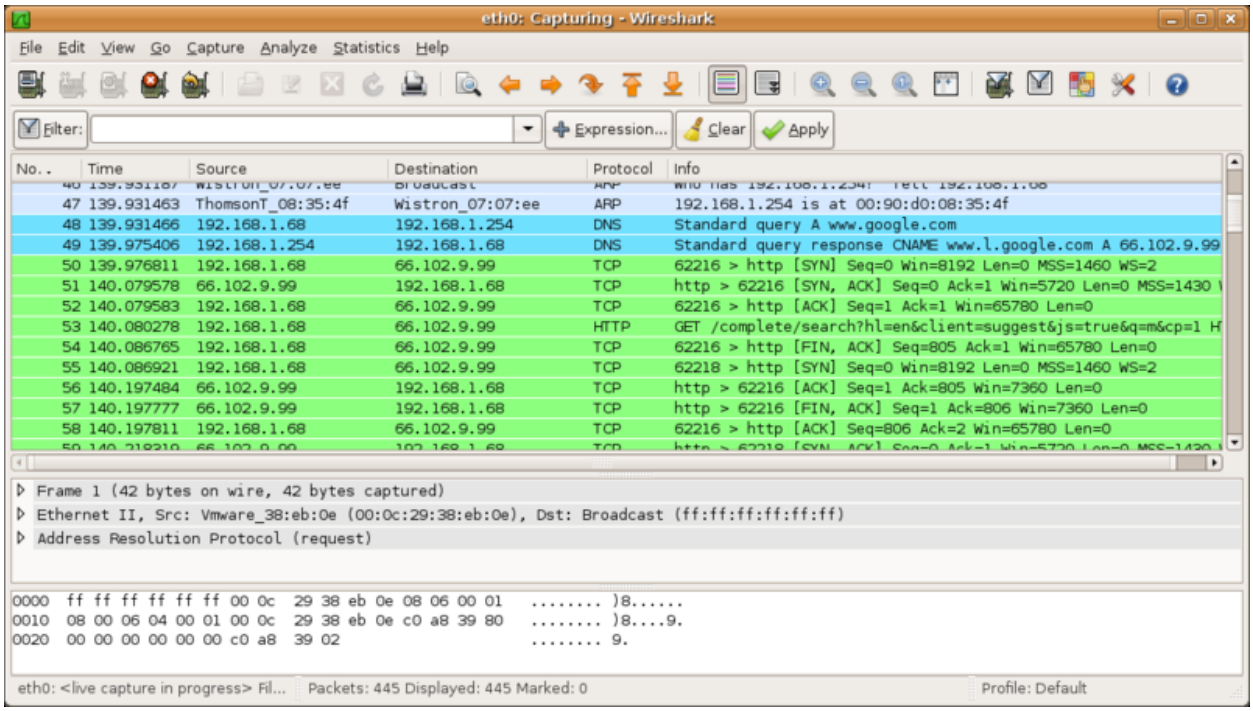
Usually if you are infected with a keylogger, the keylogger sends the keystrokes to the FTP in the time interval which is set by the attacker usually 10 to 15mins

We can monitor our own network with wireshark to figure out what network connections it is making with other iP addresses. As you might already know that FTP uses Port 21, We can filter out all FTP connections in wireshark and can get the FTP username and password for the keylogger server.

So here are the steps you can follow to find out the FTP password for a keylogger server:

Procedure

1. First of all download Wireshark and install it on your computer also make sure to install Winpcap which comes with wireshark installation package.

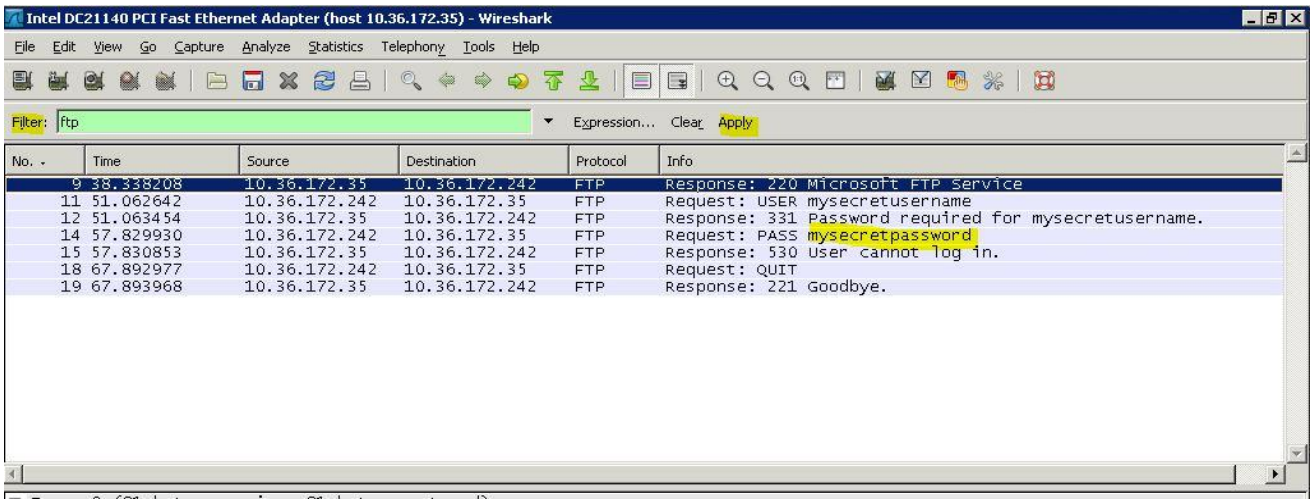


Sample screen shot of wireshark running on Ubuntu linux

2. Now go to capture button at the top and start monitoring

3. Now type **"FTP"** at the filter and it will filter out all ftp connections

4. As you scroll down you will find the "**FTP username**" and "**Password**" for victims ftp account and that's it.


Intel DC21140 PCI Fast Ethernet Adapter (host 10.36.172.35) - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: ftp
Expression... Clear Apply
No. Time Source Destination Protocol Info
9 38.338208 10.36.172.35 10.36.172.242 FTP Response: 220 Microsoft FTP Service
11 51.062642 10.36.172.242 10.36.172.35 FTP Request: USER mysecretusername
12 51.063454 10.36.172.35 10.36.172.242 FTP Response: 331 Password required for mysecretusername.
14 57.829930 10.36.172.242 10.36.172.35 FTP Request: PASS mysecretpassword
15 57.830853 10.36.172.35 10.36.172.242 FTP Response: 530 User cannot log in.
18 67.892977 10.36.172.242 10.36.172.35 FTP Request: QUIT
19 67.893968 10.36.172.35 10.36.172.242 FTP Response: 221 Goodbye.

Protection against Keyloggers and Trojans

Keyloggers and Troajans sometimes are extremely difficult to detect as hackers can use methods such as crypting, binding and hexing to evade antivirus detection, below are some of the methods you can use to protect your computer from harmful keyloggers and Trojans

Antivirus

Antivirus is one of the best counter measure against a keylogger but antivirus protection is not enough you need a good antispyware to keep yourself on the safe side, One mistake I see people doing is not updating the antivirus regularly. New Trojans and viruses are created every day so you need to update your antivirus regularly to avoid getting infected with them.

Recommended Antivirus

1. AVG Antivirus

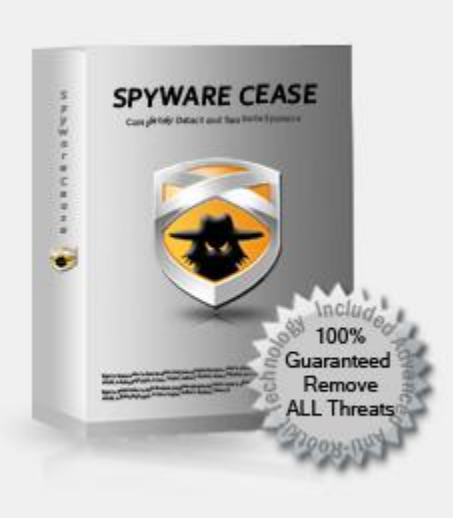
2. Kaspersky Antivirus

Antispyware

Like I told above antivirus protection is not very enough and you need an antispyware, Antispywares are specially made for the purpose of protecting your computer from spywares such as keyloggers and Rats.

Recommend Antispywares

1. **Spyware cease –** [Spyware cease]() is one of my most favorite antispywares. The reason why I like is that it has a very user-friendly interface and it can protect your computer against 99% spyware threats. So if you are looking for a good antispyware software I recommend Spyware cease



No Adware - Another alternative to Spyware cease is **noadware**, It is constantly updated to identify he latest threats to your privacy. The software will scan your PC for different Spyware, Adware, Dialers, and Web Bug traces. These items not only create nuisances in the form of popups, system slowdowns and crashes, but many items actually record personal information about you, such as credit cards, social security numbers, or other sensitive information.

For more information on this program and download details visit the following link:

Noadware

Antiloggers

Antiloggers are programs which are specially used for detecting the presence of keylogger, One of the popular antilogger is **a zemana antilogger** which claims to detect almost any keylogger. Antliloggers can even detect the presence of keylogger even if your system is infected with a keylogger.

Online virus Scanners

Online file scanners have capability to scan the given file with many antivirus, Online virus scanners is one of the best and effective way to detect suspicious virus files. Hackers also take advantage of these virus scanners and use it for scanning their virus files to check whether it's fully undetectable or not

Some of the popular online virus scanners are as follows:

1.http://novirusthanks.org

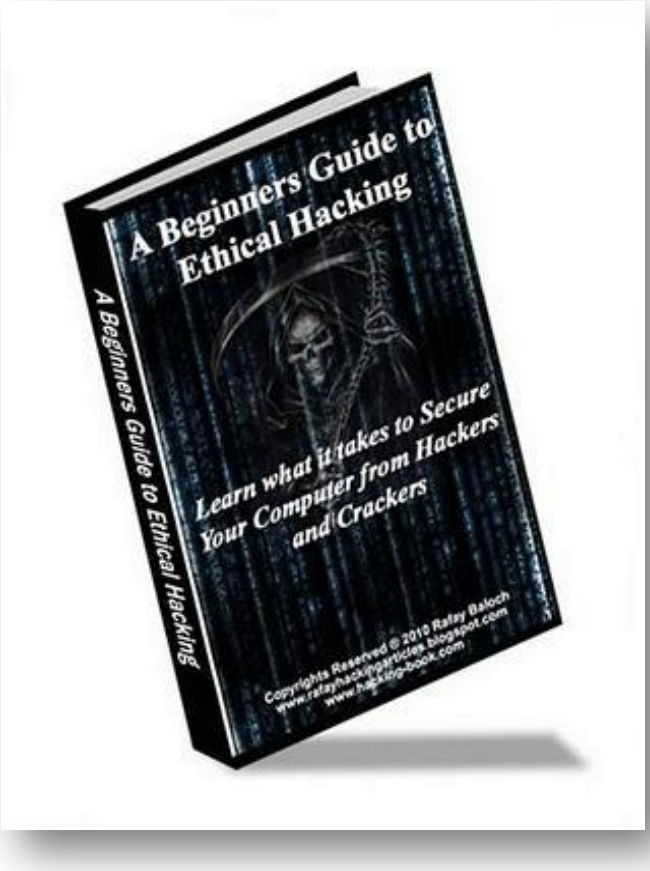
2. http://onlinescan.avast.com/

3. http://www.virustotal.com/

A Beginners Guide to Ethical Hacking

I hope you have enjoyed reading this book and you might want to get deeper in this subject and learn some advanced Ethical hacking techniques.

A Beginners Guide to Ethical hacking book is a complete path for a newbie hacker to become a master in this subject. A beginner's guide to ethical hacking.



How will the information in the book affect me?

- You will learn latest Ethical hacking techniques and also you will learn to apply them in real world situations
- You will start to think like hackers
- Secure your computer from trojans,worms, Adwares etc
- Amaze your friends with your newly learned tricks
- You will be able to protect yourself from future hack attacks

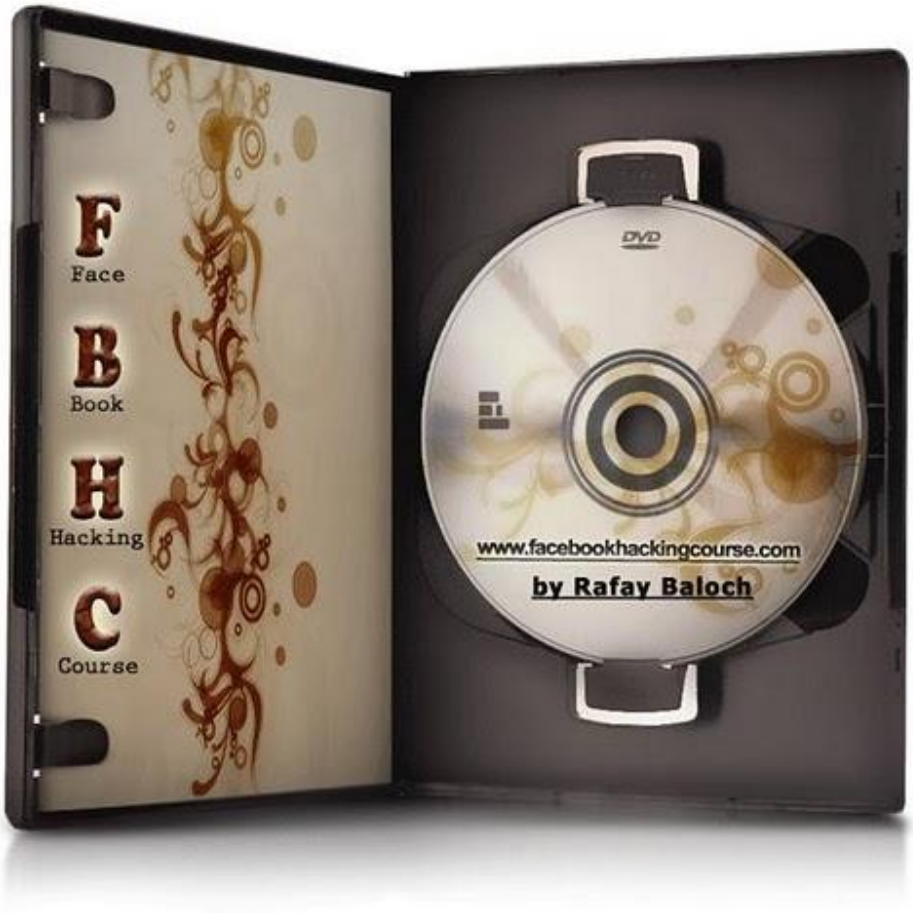
And much more...

For more information and download links, kindly visit the links below:

A Beginners Guide To Ethical Hacking

Facebook Hacking Course

Facebook hacking Course is a series of videos which will tell you exactly how hackers hack facebook accounts, What methods they use and how you can avoid falling for these kinds of attacks, You will watch my computer screen as I show you exactly how it's done, Each video contains a pre made lab so you can practice what you learned



How is the course presented?

The course contains video modules which will tell you about Facebook hacking and security and with each part there is a lab where you can practice what you learned.

For more information and download links, kindly visit the links below:

Facebook Hacking Course

Rafay Hacking Articles

As I have already mentioned earlier that I also run a blog http://rafayhackingarticles.blogspot.com where I post related to latest security stuff and security issues. Feel free to ask any questions related to hacking directly on my blog and I would love to answer it.

Congratulations

We have reached the end of this book, Hope you have enjoyed reading it, I would love to hear from you about the things you liked in this book and about the things you didn't like in this book.

Kindly send your Feedback at: **rafaybaloch@gmail.com**

Get In Touch With Me:

- **Twitter.com/rafayb1**
- **Facebook.com/rafaybalochofficialpage**