**A**

**PROJECT REPORT ON KEYLOGGER**

**Y.NARAYANA REDDY**

**ROLL NO: MT12008**

**IIIT-DELHI.**

**KEYLOGGER:**

**Keystroke logging** (more often called *key logging* or "key loggers") is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. It also has very legitimate uses in studies of human-computer interaction. There are numerous key logging methods, ranging from hardware and software-based approaches to acoustic analysis.

My Focus is on developing software based key logger which is stealth in nature.

**Software Based Key loggers:**

These are software programs designed to work on the target computer’s operating system. From a technical perspective there are five categories:

* **Hypervisor-based**: The key logger can theoretically reside in a malware hyper visor running underneath the operating system, which remains untouched. It effectively becomes a virtual machine.
* **Kernel based**: This method is difficult both to write and to combat. Such key loggers reside at the kernel level and are thus difficult to detect, especially for user-mode applications. They are frequently implemented as root kits that subvert the operating system kernel and gain unauthorized access to the hardware, making them very powerful. A key logger using this method can act as a keyboard device driver for example, and thus gain access to any information typed on the keyboard as it goes to the operating system.
* **API-based**: These key logger hook keyboard API’s; the operating system then notifies the key logger each time a key is pressed and the key logger simply records it. Windows APIs such as GetAsyncKeyState (), GetForegroundWindow (), etc. are used to poll the state of the keyboard or to subscribe to keyboard events. These types of key loggers are the easiest to write, but where constant polling of each key is required, they can cause a noticeable increase in CPU usage, and can also miss the occasional key. A more recent example simply polls the BIOS for pre-boot authentication pin’s that have not been cleared from memory.
* **Form grabbing based**: Form logging based key loggers log web logging submissions by recording the web browsing on submit event functions. This records form data before it is passed over the Internet and bypasses HTTPS encryption.
* **Memory injection based**: Memory Injection based key loggers alter memory tables associated with the browser and other system functions to perform their logging functions. By patching the memory tables or injecting directly into memory, this technique can be used by malware authors who are looking to bypass Windows UAC (User Account Control).
* Packet analyzers: This involves capturing network traffic associated with post events to retrieve unencrypted passwords.

Remote access software key loggers these are local software key loggers with an added feature that allows access to the locally recorded data from a remote location. Remote communication may be achieved using one of these methods:

* Data is uploaded to a website, database or a FTP server.
* Data is periodically emailed to a pre-defined email address.
* Data is wirelessly transmitted by means of an attached hardware system.
* The software enables a remote login to the local machine from the Internet or the local network, for data logs stored on the target machine to be accessed.

**Language used: C Language**

**To Make A Key Logger Stealth:**

To make key logger stealth we followed two approaches

1. While developing a program we added a function stealth() which makes key logger hide while logging the key strokes.
2. The other method is we named our process name in such a way that it appears like a legitimate application. In this case we named it as “chrome tab\*32.exe”.

Various ways to Send Key logger to victim’s computer:

The following procedure combines two exe files and we can send it as legitimate software to the victim:

On your desktop, open your start menu. Then click on Run. Then when the Run window opens, type in “iexpress” and click on OK. The IExpress Wizard program should now open.  
  
1. Click Next  
2. Click Next  
3. It will ask you for a title, put anything in and then click Next  
4. Then Next again  
5. Then Next again  
6. Now you should be at the screen where it asks you to add your files. First add the keylogger.exe. Next add the other .exe file . Then click Next.  
7. Now you’ll be at the “Install Program To Launch”. Make sure to change it to the follow   
Install Program: “legitimatename”.exe  
Post Install Command: “your downloaded EXE file”.exe  
  
Then click Next.  
8. Next again.  
9. Choose where to install this new combined file of yours then click Next.  
10. Now select “No restart” and click Next.  
11. Select “No Save” and Next again.  
12. Now click Next one more time and there, you have your package.

 Choose and install a key logger that best suits your needs. There are a number of programs available out there, but most of them require you to have direct access to the computer in order to install it. Once you've installed it, you will need to manually configure it in order to send you the logs.

 Install the program and configure it. You will need to tell the program which emails you would like to have the logs sent to. To do this, launch the program and then go to "Settings" and "Report Sending." You can put in an email address and the frequency you would like to have them sent. You can also have them sent via FTP.

 Attach it as an email and send it. This is the only way to get a key logger onto a computer if you have no access to it via a network or a direct line to it via the Internet through remote control software. You can attach the program just like any other email attachment. If you're using a web-based application like Gmail, click on "Compose email" and "Attach File," then find which folder you placed the program in, double click on it and click "Open." One problem with this approach is that many spam filters will give warnings about executable files attached to an email. To get the program through the filter, you can embed the file into a document like word and then attach the document to the problem. The second problem you may encounter is that most people know not to download attachments unless they are from a trusted source. So you may have to use the key logger to get into the email account of someone you know the recipient trusts. Label the attachment as a file that the receiver would be interested in such as "Photos" so that you are sure they will download it. Once it is downloaded, the program will automatically install itself and send you an email confirming its installation. This all takes place in the background invisibly.

 Install the key logger using remote software. This is only possible if at some point you have access to the computer that you want to monitor. If you do, then you can install software from GoToMyPC.com that will allow you to control the computer via remote through any computer connected to the Internet. Once you've installed it, you can log on to GoToMyPC.com from any computer and you will be able to control it as if you were sitting in front of it. This way, you can install a key logger directly to it even if you are thousands of miles away.

 Install the key logger over a network. The problem with this is that you will need to have system administrator privileges or be able to get access to the user ID and password to get it. So it's possible that you can use the key logger for this initially and then install it over the network. To do this, go to "Network," find the name of the computer that you would like to install the key logger on and double click on it. Drag and drop the application to the desktop and install it. Again, you will need to configure the application to send the logs to an email address and you will probably want to put it in stealth mode so that the computer's user will not find it.

**References:**

* 1. <http://en.wikipedia.org/wiki/Keystroke_logging>
  2. <http://buffernow.com/2012/10/how-keylogger-works/>
  3. <http://www.appzxor.net/t5049-basic-keylogger-source-code>
  4. <http://www.ehow.com/how_5024016_send-keyloggers-other-computers.html>
  5. <http://www.netadmintools.com/art215.html>
  6. <http://www.securelist.com/en/analysis?pubid=204791931>