Beating the Keylogger at its Own Game

Keyloggers are specifically installed to trap account passwords and credit card information. This article is an attempt to beat these malicious pieces of code at their own game!

The fact is that we have been living with keyloggers for many years now. For the uninitiated, a keylogger is a small piece of code that traps every key that you press on the keyboard. Pranksters or online thieves can use these to capture account passwords, credit card information and more! With more and more people using credit cards online these days, the threat that these keyloggers pose to innocent Net users is real.

So what's a keylogger, anyway?

The working of a keylogger is pretty simple—it makes a copy of everything you type on the keyboard and saves it in a file. Some advanced keyloggers can even mail the logged file to the e-mail ID entered by the hacker who installed it. There have been many incidents on the Web where people recall the losses they suffered thanks to these keyloggers. Two simple ideas that deceive keyloggers are explained in this article.

The key-less solution

Before we begin with the two solutions, let's consider something very simple that can be of use. Since this is not very practical, we shall only deal with it briefly.

A keylogger logs the keys that we type. What if we could enter a password without having to type it? The logic is simple—do a perfect copy-paste! Simply type your password in a file that you can carry on a floppy, USB drive, etc. Whenever you need to enter a password, simply copy-paste from the file. This way the keylogger will not be able to log your sensitive information.

Trick 1—The haphazard poem method

Let's consider the password *firE19@*. I have chosen this with a purpose. The password contains small letters, capital letters, numbers, and special characters as well. What we will do here is allow the keylogger to log whatever we type. So we key in a message like this.

Etti was a fat lady
she bought some butter
the butter was bitter
so she bought
some more better butter
to make the
bitter butter bitter.

Once you have typed the above text, you need to copy one character at a time and paste it into the password field.

Our password is *firE19@*. Since our first alphabet is 'f', copy the 'f' from the word 'fat' and paste it into the password box. Our next alphabet is 'i'. So copy only 'i' from the word 'bitter' and paste it into the password box. Follow this step for all the characters/number/symbols in the password and 'synthesise' the password right under the nose of the keylogger.

The text logged by the key logger will be as follows:

```
Etti was a fat lady
she bought some butter
the butter was bitter
so she bought
some more better butter
to make the
bitter butter bitter.
cv cv cv cv cv cv cv
The line of cvs register the ctrl+c
and ctrl+v operations,
i.e., the copy and paste commandsÖ
```

Trick 2: The eraser at the back of the genius's pencil

Speaking plainly, Trick 1 should be able to fool an ordinary keylogger. What if the keylogger also monitors the clipboard? It will also log the copied text. This trick is better than the previous two. Here we shall not do any copy-paste operations. Another example will help you understand.

Let's suppose *cooljeba* is the password that we wish to enter. So what we do now is type *coolorhotjeba* in the text field. And then with the help of the mouse, we select the *orhot* part and delete it by pressing the delete button (or by using Ctrl+x to cut it).

This is what we enter:
Cool**orhot**jeba

It appears on the password field as: **********

So what the keylogger logs is:
Coolorhotjebax

That's all! I personally use the second trick to enter my passwords, as it is feasible and consumes little time.

Although the Internet is a wonderful medium of communication, it also offers innumerable opportunities for your data to be stolen. There are goons out there who wish to gather information that you have always kept secret. Their success could cost you money, time and your reputation. Keyloggers are a common tool that crackers employ to fish out information. Using the tricks explained in this article, you could protect your passwords and critical information without many hassles. The tricks are easy, inexpensive and can be implemented by almost anyone—even the absolute newbie! END

By: Allwin Samuel Jeba. *The author is a graphic designer from Bangalore. He can be reached at jeba@cooljeba.com*

NEWS LIGHT

Linspire Professional in the pipeline

Linspire, the popular user-friendly distribution of Linux, is testing the beta of its enterprise offering, Linspire Professional, at a number of enterprise organizations—including the State of Indiana's Access program in the USA. The new Linspire product will face stiff competition from some established names in the enterprise desktop segment—Red Hat, Novell, etc. The new version of Linspire will take advantage of the CNR software delivery subscription technology. This will allow administrators in an organisation to control the desktops in the company, remotely.

Linspire hopes their new offering will be a wake up call for Red Hat and Novell—the leaders in this vertical of the market. The user-friendliness of Linspire Professional is expected to be a big plus on the side of the product.

There are three factors that Linspire thinks are important to further Linux desktop solutions: technology, the channel, and end user demand. Demand is the singlemost important factor that they identify.