keylogger

is a hidden program that is sent via e-mail or you download it from an untrusted site or it is among free programs and you are not aware of it, as the spyware transmits all what is written on the keyboard to remote destinations, usually to the owner of the spying or the sender of the program, and this is the most dangerous These objects, whose work is similar to that of a Trojan horse, a type of spy virus, is used to monitor certain devices and see what is written on them. Such as passwords, passwords, and credit card numbers. The keylogger can also take screenshots of the computer screen at specific times that the programmer sets and then sends them with the type that he recorded to the programmer.

How it works(1)

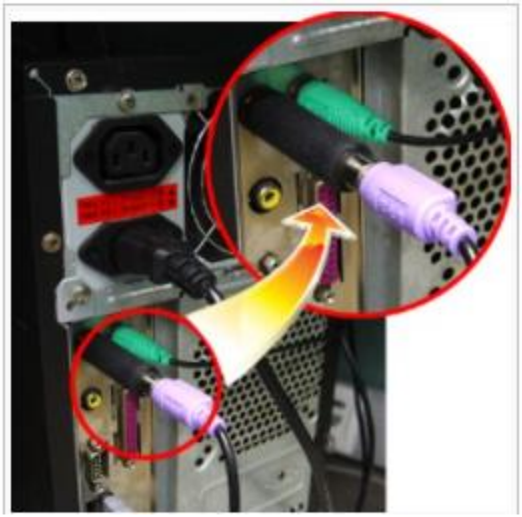
Its mechanics are not very different from the mechanics it follows. most computer virus; It enters through security holes and monitors the path that information takes Security Flaws towards the keyboard parts on its way from the keyboard, processing and transforming this data in the computer...

A keylogger infiltrates your device by downloading untrusted software, or it can reach you through an applet that is sent to you via email. Or it may reach you by sharing computer applications with another infected device.

The keylogger records everything that is typed on the keyboard, or it can come up to taking screenshots of the computer screen every period of time specified by the programmer for that malicious programming, then the keylogger sends all this data to the programmer.

Types of keylogger

We used to think that the keylogger has one type, which is malicious software, but there are many more dangerous types, including the panel monitor, which is a piece that connects the keyboard and the motherboard, so when using any device in a public place or a cafe, make sure that the keyboard is connected directly and there is no piece or connection between the keyboard and the device



Keylogger use by cybercriminals

In February 2005, Joe Lopez, a businessman from Florida, filed a suit against Bank of America after unknown hackers stole $90,000 from his Bank of America account. The money had been transferred to Latvia.

An investigation showed that Mr. Lopez’s computer was infected with a malicious program, Backdoor.Coreflood, which records every keystroke and sends this information to malicious users via the Internet. This is how the hackers got hold of Joe Lopez’s user name and password, since Mr. Lopez often used the Internet to manage his Bank of America account.

According to research conducted by John Bambenek, an analyst at the SANS Institute, approximately 10 million computers in the US alone are currently infected with a malicious program which has a keylogging function. Using these figures, together with the total number of American users of e-payment systems, possible losses are estimated to be $24.3 million.

How keyloggers spread

Keyloggers spread in much the same way that other malicious programs spread. Excluding cases where keyloggers are purchased and installed by a jealous spouse or partner, and the use of keyloggers by security services, keyloggers are mostly spread using the following methods):

- a keylogger can be installed when a user opens a file attached to an email;
- a keylogger can be installed when a file is launched from an open-access directory on a P2P network;
- a keylogger can be installed via a web page script which exploits a browser vulnerability. The program will automatically be launched when a user visits a infected site;
- a keylogger can be installed by another malicious program already present on the victim machine, if the program is capable of downloading and installing other malware to the system.

How to protect yourself from keyloggers

Most antivirus companies have added keyboard loggers to their databases, which makes protecting against them no different from protecting against other types of malware, so you should check your antivirus product if it isn't

These are some of the methods that help protect against unknown keyloggers or are designed to target a specific system

1- Use one-time passwords or two-step authentication

Using a one-time password can help minimize losses if the password you enter is intercepted, as the password generated can be used one time only, and the period of time during which the password can be used is limited. Even if a one-time password is intercepted, a cyber criminal will not be able to use it in order to obtain access to confidential information.

2-

2- Using a system with proactive protection designed to detect keyloggers

3- Ensure that the keyboard wire is connected directly to the device and that there are no connections between the device and the keyboard, and you should avoid entering important data using a wireless keyboard

resources and references

1-

Keyloggers: How they work and how to detect them (Part 1) | Securelist

2-

Amazon.com: Yubico FIDO Security Key NFC - Two Factor Authentication USB and NFC Security Key, Fits USB-A Ports and Works with Supported NFC Mobile Devices – FIDO U2F and FIDO2 Certified - More Than a Password : Electronics