SECURELIST

Author

Nikolay Grebennikov

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

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.

However the court did not rule in favor of the plaintiff, saying that Mr. Lopez had neglected to take basic precautions when managing his bank account on the Internet: a signature for the malicious code that was found on his system had been added to nearly all antivirus product databases back in 2003.

Joe Lopez's losses were caused by a combination of overall carelessness and an ordinary keylogging program.

- **About keyloggers**
- **Why keyloggers are a threat**
- **How cyber criminals use keyloggers**
- **Increased use of keyloggers by cyber criminals**
- **Keylogger construction**
- **How keyloggers spread**
- **Protection from keyloggers**
- **Conclusions**

About Keyloggers

The term 'keylogger' itself is neutral, and the word describes the program's function. Most sources define a keylogger as a software program designed to secretly monitor and log all keystrokes. This definition is not altogether correct, since a keylogger doesn't have to be software – it can also be a device. Keylogging devices are much rarer than keylogging software, but it is important to keep their existence in mind when thinking about information security.

Legitimate programs may have a keylogging function which can be used to call certain program functions using "hotkeys," or to toggle between keyboard layouts (e.g. Keyboard Ninja). There is

a lot of legitimate software which is designed to allow administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers. However, the ethical boundary between justified monitoring and espionage is a fine line. Legitimate software is often used deliberately to steal confidential user information such as passwords.

Most modern keyloggers are considered to be legitimate software or hardware and are sold on the open market. Developers and vendors offer a long list of cases in which it would be legal and appropriate to use keyloggers, including:

- Parental control: parents can track what their children do on the Internet, and can opt to be notified if there are any attempts to access websites containing adult or otherwise inappropriate content;
- Jealous spouses or partners can use a keylogger to track the actions of their better half on the Internet if they suspect them of “virtual cheating”;
- Company security: tracking the use of computers for non-work-related purposes, or the use of workstations after hours;
- Company security: using keyloggers to track the input of key words and phrases associated with commercial information which could damage the company (materially or otherwise) if disclosed;
- Other security (e.g. law enforcement): using keylogger records to analyze and track incidents linked to the use of personal computers;
- Other reasons.

However, the justifications listed above are more subjective than objective; the situations can all be resolved using other methods. Additionally, **any** legitimate keylogging program can still be used with malicious or criminal intent. Today, keyloggers are mainly used to steal user data relating to various online payment systems, and virus writers are constantly writing new keylogger Trojans for this very purpose.

Furthermore, many keyloggers hide themselves in the system (i.e. they have rootkit functionality), which makes them fully-fledged Trojan programs.

As such programs are extensively used by cyber criminals, detecting them is a priority for antivirus companies. Kaspersky Lab’s malware classification system has a dedicated category for malicious programs with keylogging functionality: Trojan-Spy. Trojan-Spy programs, as the name suggests, track user activity, save the information to the user’s hard disk and then forward it to the author or ‘master’ of the Trojan. The information collected includes keystrokes and screen-shots, used in the theft of banking data to support online fraud.

Why keyloggers are a threat

Unlike other types of malicious program, keyloggers present no threat to the system itself. Nevertheless, they can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cyber criminals can get PIN codes and account numbers for e-payment systems, passwords to online gaming accounts, email addresses, user names, email passwords etc.

Once a cyber criminal has got hold of confidential user data, s/he can easily transfer money from

the user's account or access the user's online gaming account. Unfortunately access to confidential data can sometimes have consequences which are far more serious than an individual's loss of a few dollars. Keyloggers can be used as tools in both industrial and political espionage, accessing data which may include proprietary commercial information and classified government material which could compromise the security of commercial and state-owned organizations (for example, by stealing private encryption keys).

Keyloggers, phishing and social engineering (see 'Computers, Networks and Theft') are currently the main methods being used in cyber fraud. Users who are aware of security issues can easily protect themselves against phishing by ignoring phishing emails and by not entering any personal information on suspicious websites. It is more difficult, however, for users to combat keyloggers; the only possible method is to use an appropriate security solution, as it's usually impossible for a user to tell that a keylogger has been installed on his/ her machine.

According to Cristine Hoepers, the manager of Brazil's Computer Emergency Response Team, which works under the aegis of the country's Internet Steering Committee, keyloggers have pushed phishing out of first place as the most-used method in the theft of confidential information. What's more, keyloggers are becoming more sophisticated – they track websites visited by the user and only log keystrokes entered on websites of particular interest to the cyber criminal.

In recent years, we have seen a considerable increase in the number of different kinds of malicious programs which have keylogging functionality. No Internet user is immune to cyber criminals, no matter where in the world s/he is located and no matter what organization s/he works for.

How cyber criminals use keyloggers

One of the most publicized keylogging incidents recently was the theft of over $1million from client accounts at the major Scandinavian bank Nordea. In August 2006 Nordea clients started to receive emails, allegedly from the bank, suggesting that they install an antispam product, which was supposedly attached to the message. When a user opened the file and downloaded it to his/ her computer, the machine would be infected with a well known Trojan called Haxdoor. This would be activated when the victim registered at Nordea's online service, and the Trojan would display an error notification with a request to re-enter the registration information. The keylogger incorporated in the Trojan would record data entered by the bank's clients, and later send this data to the cyber criminals' server. This was how cyber criminals were able to access client accounts, and transfer money from them. According to Haxdoor's author, the Trojan has also been used in attacks against Australian banks and many others.

On January 24, 2004 the notorious Mydoom worm caused a major epidemic. MyDoom broke the record previously set by Sobig, provoking the largest epidemic in Internet history to date. The worm used social engineering methods and organized a DoS attack on www.sco.com; the site was either unreachable or unstable for several months as a consequence. The worm left a Trojan on infected computers which was subsequently used to infect the victim machines with new modifications of the worm. The fact that MyDoom had a keylogging function to harvest credit card numbers was not widely publicized in the media.

In early 2005 the London police prevented a serious attempt to steal banking data. After attacking a banking system, the cyber criminals had planned to steal $423 million from Sumitomo Mitsui's London-based offices. The main component of the Trojan used, which was created by the

32-year-old Yeron Bolondi, was a keylogger that allowed the criminals to track all the keystrokes entered when victims used the bank's client interface.

In May 2005 in London the Israeli police arrested a married couple who were charged with developing malicious programs that were used by some Israeli companies in **industrial espionage**. The scale of the espionage was shocking: the companies named by the Israeli authorities in investigative reports included cellular providers like Cellcom and Pelephone, and satellite television provider YES. According to reports, the Trojan was used to access information relating to the PR agency Rani Rahav, whose clients included Partner Communications (Israel's second leading cellular services provider) and the HOT cable television group. The Mayer company, which imports Volvo and Honda cars to Israel, was suspected of committing industrial espionage against Champion Motors, which imports Audi and Volkswagen cars to the country. Ruth Brier-Haephrati, who sold the keylogging Trojan that her husband Michael Haephrati created, was sentenced to four years in jail, and Michael received a two-year sentence.

In February 2006, the Brazilian police arrested 55 people involved in spreading malicious programs which were used to steal user information and passwords to banking systems. The keyloggers were activated when the users visited their banks' websites, and secretly tracked and subsequently sent all data entered on these pages to cyber criminals. The total amount of money stolen from 200 client accounts at six of the country's banks totaled $4.7million.

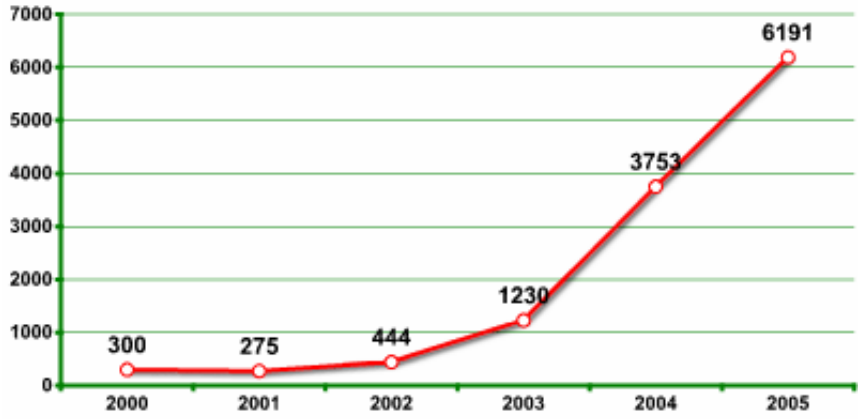
At approximately the same time, a similar criminal grouping made up of young (20 – 30 year old) Russians and Ukrainians was arrested. In late 2004, the group began sending banking clients in France and a number of other countries email messages that contained a malicious program – namely, a keylogger. Furthermore, these spy programs were placed on specially created websites; users were lured to these sites using classic social engineering methods. In the same way as in the cases described above, the program was activated when users visited their banks' websites, and the keylogger harvested all the information entered by the user and sent it to the cyber criminals. In the course of eleven months over one million dollars was stolen.

There are many more examples of cyber criminals using keyloggers – most financial cybercrime is committed using keyloggers, since these programs are the most comprehensive and reliable tool for tracking electronic information.

Increased use of keyloggers by cyber criminals

The fact that cyber criminals choose to use keyloggers time and again is confirmed by IT security companies.

One of VeriSign's recent reports notes that in recent years, the company has seen a rapid growth in the number of malicious programs that have keylogging functionality.



Source: iDefense, a VeriSign Company

One report issued by Symantec shows that almost 50% of malicious programs detected by the company's analysts during the past year do not pose a direct threat to computers, but instead are used by cyber criminals to harvest personal user data.

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.

Kaspersky Lab is constantly detecting new malicious programs which have a keylogging function. One of the first virus alerts on www.viruslist.com, Kaspersky Lab's dedicated malware information site, was published on 15th June 2001. The warning related to TROJ_LATINUS.SVR, a Trojan with a keylogging function. Since then, there has been a steady stream of new keyloggers and new modifications. Kaspersky antivirus database currently contain records for more than 300 families of keyloggers. This number does not include keyloggers that are part of complex threats (i.e. in which the spy component provides additional functionality).

Most modern malicious programs are hybrids which implement many different technologies. Due to this, any category of malicious program may include programs with keylogger (sub)functionality. The number of spy programs detected by Kaspersky Lab each month is on the increase, and most of these programs use keylogging technology.

Keylogger construction

The main idea behind keyloggers is to get in between any two links in the chain of events between when a key is pressed and when information about that keystroke is displayed on the monitor. This can be achieved using video surveillance, a hardware bug in the keyboard, wiring or the computer itself, intercepting input/ output, substituting the keyboard driver, the filter driver in the keyboard stack, intercepting kernel functions by any means possible (substituting addresses in system tables, splicing function code, etc.), intercepting DLL functions in user mode, and, finally, requesting information from the keyboard using standard documented methods.

Experience shows that the more complex the approach, the less likely it is to be used in common Trojan programs and the more likely it is to be used in specially designed Trojan programs which are designed to steal financial data from a specific company.

Keyloggers can be divided into two categories: keylogging devices and keylogging software. Keyloggers which fall into the first category are usually small devices that can be fixed to the keyboard, or placed within a cable or the computer itself. The keylogging software category is

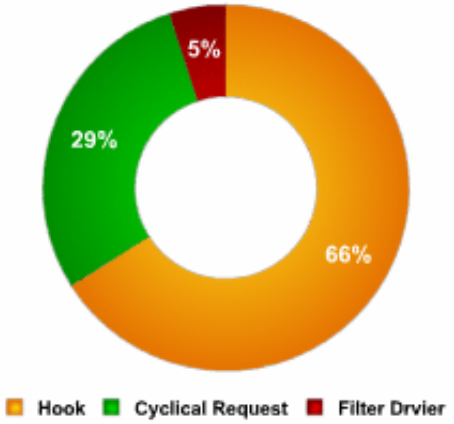
made up of dedicated programs designed to track and log keystrokes.

The most common methods used to construct keylogging software are as follows:

- a system hook which intercepts notification that a key has been pressed (installed using WinAPI SetWindowsHook for messages sent by the window procedure. It is most often written in C);
- a cyclical information keyboard request from the keyboard (using WinAPI Get(Async)KeyState or GetKeyboardState – most often written in Visual Basic, sometimes in Borland Delphi);
- using a filter driver (requires specialized knowledge and is written in C).

We will provide a detailed explanation of the different ways keyloggers are constructed in the second half of this article (to be published in the near future). But first, here are some statistics.

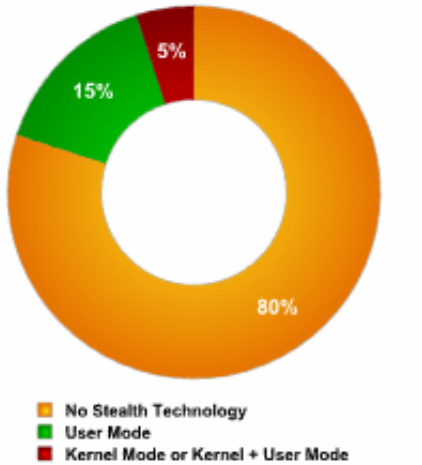
A rough breakdown of the different types of keyloggers is shown in the pie chart below:



Recently, keyloggers that disguise their files to keep them from being found manually or by an antivirus program have become more numerous. These stealth techniques are called rootkit technologies. There are two main rootkit technologies used by keyloggers:

- masking in user mode;
- masking in kernel mode.

A rough breakdown of the techniques used by keyloggers to mask their activity is shown in the pie chart below:



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 already added known keyloggers to their databases, making protecting against keyloggers no different from protecting against other types of malicious program: install an antivirus product and keep its database up to date. However, since most antivirus products classify keyloggers as *potentially malicious*, or *potentially undesirable programs*, users should ensure that their antivirus product will, with default settings, detect this type of malware. If not, then the product should be configured accordingly, to ensure protection against most common keyloggers.

Let's take a closer look at the methods that can be used to protect against unknown keyloggers or a keylogger designed to target a specific system.

Since the chief purpose of keyloggers is to get confidential data (bank card numbers, passwords, etc.), the most logical ways to protect against unknown keyloggers are as follows:

1. using one-time passwords or two-step authentication,
2. using a system with proactive protection designed to detect keylogging software,
3. using a virtual keyboard.

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.

In order to get one-time passwords, you can use a special device such as:

1. a USB key (such as Aladdin eToken NG OTP):

2. a ‘calculator’ (such as RSA SecurID 900 Signing Token):

In order to generate one-time passwords, you can also use mobile phone text messaging systems that are registered with the banking system and receive a PIN-code as a reply. The PIN is then used together with the personal code for authentication.

If either of the above devices is used to generate passwords, the procedure is as described below:

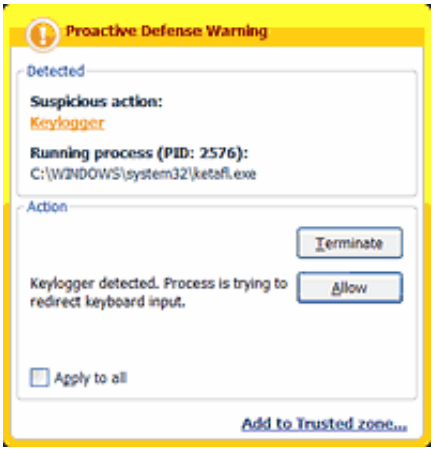
1. the user connects to the Internet and opens a dialogue box where personal data should be entered;
2. the user then presses a button on the device to generate a one-time password, and a password will appear on the device’s LCD display for 15 seconds;
3. the user enters his user name, personal PIN code and the generated one-time password in the dialogue box (usually the PIN code and the key are entered one after the other in a single pass code field);
4. the codes that are entered are verified by the server, and a decision is made whether or not the user may access confidential data.

When using a calculator device to generate a password, the user will enter his PIN code on the device 'keyboard' and press the ">" button.

One-time password generators are widely used by banking systems in Europe, Asia, the US and Australia. For example, Lloyds TSB, a leading bank, decided to use password generators back in November 2005.

In this case, however, the company has to spend a considerable amount of money as it had to acquire and distribute password generators to its clients, and develop/ purchase the accompanying software.

A more cost efficient solution is proactive protection on the client side, which can warn a user if an attempt is made to install or activate keylogging software.



Proactive protection against keyloggers in Kaspersky Internet Security

The main drawback of this method is that the user is actively involved and has to decide what action should be taken. If a user is not very technically experienced, s/he might make the wrong decision, resulting in a keylogger being allowed to bypass the antivirus solution. However, if developers minimize user involvement, then keyloggers will be able to evade detection due to an insufficiently rigorous security policy. However, if settings are too stringent, then other, useful programs which contain legitimate keylogging functions might also be blocked.

The final method which can be used to protect against both keylogging software and hardware is using a **virtual keyboard**. A virtual keyboard is a program that shows a keyboard on the screen, and the keys can be 'pressed' by using a mouse.

The idea of an on-screen keyboard is nothing new - the Windows operating system has a built-in on-screen keyboard that can be launched as follows: Start > Programs > Accessories > Accessibility > On-Screen Keyboard.

An example of the Windows on-screen keyboard

However, on-screen keyboards aren't a very popular method of outsmarting keyloggers. They were not designed to protect against cyber threats, but as an accessibility tool for disabled users. Information entered using an on-screen keyboard can easily be intercepted by a malicious program. In order to be used to protect against keyloggers, on-screen keyboards have to be specially designed in order to ensure that information entered or transmitted via the on-screen keyboard cannot be intercepted.

Conclusions

This article has provided an overview of how keyloggers – both keylogging software and hardware - function and are used.

- Even though keylogger developers market their products as legitimate software, most keyloggers can be used to steal personal user data and in political and industrial espionage.
- At present, keyloggers – together with phishing and social engineering methods – are one of

the most commonly used methods of cyber fraud.

- IT security companies have recorded a steady increase in the number of malicious programs that have keylogging functionality.
- Reports show that there is an increased tendency to use rootkit technologies in keylogging software, to help the keylogger evade manual detection and detection by antivirus solutions.
- Only dedicated protection can detect that a keylogger is being used for spy purposes.
- The following measures can be taken to protect against keyloggers:
  - use a standard antivirus that can be adjusted to detect potentially malicious software (default settings for many products);
  - proactive protection will protect the system against new ,modifications of existing keyloggers;
  - use a virtual keyboard or a system to generate one-time passwords to protect against keylogging software and hardware.
