Keylogger Use for Security of A Personal Computer

Supriya B. Kendhe
IT final year,
JDIET Yavatmal,

Prachi M.Tamgadge
IT final year,
JDIET Yavatmal

Pratiksha D. Sangidwar
IT Final year,
JDIET Yavatmal

Guided By -
Prof. Sandip A. Kahate
Assistant Professor
JDIET Yavatmal

ABSTRACT:

Roaming users who use untrusted machines to access password protected accounts have few good options.An internet cafe machine can easily be running a keylogger. The roaming user has no reliable way of determining whether it is safe, and has no alternative to typing the password. We describe a simple trick the user can employ that is entirely effective in concealing the password. We verify its efficacy against the most popular keylogging programs.

I. INTRODUCTION:

Keylogging is one of the most insidious threats to a user's personal information. Passwords, credit card numbers, PII etc. are potentially exposed; and the incidence of keyloggers in-the-wild is apparently growing rapidly. Unlike Phishing, this is not an attack that alert and sophisticated users can avoid. Writing a keylogger is a trivially easy task , there are numerous freeware offerings, and many of them make efforts to conceal their presence. For example, they will not show up in the Task Manager process list. There's even a feature comparison site for those interested in the hardest to detect keyloggers. Home and enterprise users may be able to trust their systems if they maintain good firewall, anti-virus and update strategies. However roaming users have no control over what is installed. Certain internet kiosks restrict input access to the machine to prevent software installation. This makes it less likely that another user of the machine has installed a keylogger, so long as the administrator has set good policies. But this requires knowing that the administrator is both competent and trustworthy. As things stand a user has no reliable way to determine if a machine is running a keylogger or not. In this environment is there anything a user can do to protect themselves from the possibly catastrophic loss of data.

II. AWRARENESS ABOUT SECURITY TRAININIG:

Fig.1 awareness about security training

In a latest survey it is found that 68% people don't know about security training & 32% know about the security training. taking into consideration of today's world of technology it is important for the people to aware about the facts related to data theft & how to get security from unwanted access.

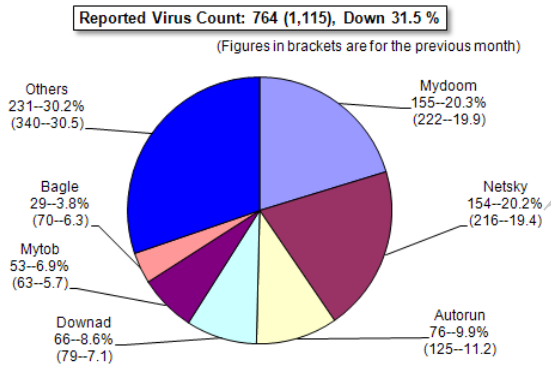

Fig2Reportofviruscount

As shown in the figure 2 , virus count is measured , six types of viruses are found like

1.Mydoom (15.5-20.3%)

2.Netsky (15.4-20.2%)

3.Autorun (7.6-9.9%)

4.Downad (6.6-8.6%)

5.Mytob (63-5.7%)

6.Bagle (7.0-6.3%)

Taking into considerations information about the viruses present in the system, If the user don't know about such type of presence of viruses then it would become difficult for the system to maintain its security.

III.PRIVACY A NEED FOR SECURE INTERNET WORKING:

Privacy has been described in many ways by many people. For the purpose of this discussion we will use the following amalgamation of viewpoints borrowed from industry:

The right of individuals to determine if, when, how, and to what extent data about themselves will be collected, used and shared with others. The fundamental principles within that description that apply to the topic of monitoring software are notice and consent. For monitoring to be appropriate it must be conducted with clear and complete notice provided to the individual prior to the monitoring and informed consent must have been obtained from the person being monitored. Any monitoring done outside of that can be considered inappropriate at best, though many would use considerably stronger and, often, pejorative terminology to describe it. Other privacy considerations must

be taken into account with regard to the data collected during the use of any monitoring software. Is that data stored securely and protected from view or usage outside of what was disclosed when the original notice and consent occurred? Are the people who have access to that data limited only to those with a specific need (a need that is, again, consistent with the notice and consent provided by the individual)? Is the data protected from tampering so as to prevent the attribution of words and deeds to the individual where those words and deeds were not that person's doing? Is the use of the data under the provisions discussed above enforced in some meaningful way with consequences associated with any misuse? It should be mentioned that there are likely to be numerous legal considerations relating to the use of monitoring software. Such software can capture personal data, sensitive data relating to financial, medical or other protected classes of information such as information relating to children. Further, in some instances an individual may have an expectation of privacy which is also protected. Those seeking to use monitoring software for legitimate purposes. Other privacy considerations must be taken into account with regard to the data collected during the use of any monitoring software. Is that data stored securely and protected from view or usage outside of what was disclosed when the original notice and consent occurred? Are the people who have access to that data limited only to those with a specific need (a need that is, again, consistent with the notice and consent provided by the individual)? Is the data protected from tampering so as to prevent the attribution of words and deeds to the individual where those words and deeds were not that person's doing? Is the use of the data under the provisions discussed above enforced in some meaningful way with consequences associated with any misuse?

IV.METHODS OF WATCHING OVER DIFFERENT ACTIVITIES :

As we've seen, there are many approaches to monitoring an individual's computer activities. These techniques include the use of commercial software as well as more rudimentary spying techniques such as password-guessing. There are also hardware-based attacks such as the use of a small camera overlooking a keyboard or ATM PIN entry keypad as well as hardware devices designed either to be installed in series with the keyboard or soldered inside the keyboard itself (such as the one used by the FBI in the Scarfo case). These hardware solutions boast capacities of as many as 2 million keystrokes (more than 600 typewritten pages).

Hardware-based keystroke logging is nearly impossible to detect through the use of software, as even advanced techniques, such as monitoring for voltage variances in the hardware path, require foreknowledge of what keyboard is being used and what is 'normal' for that keyboard in all use scenarios. In addition to the methods described previously there are also a growing number of instances of malicious software which include monitoring components Although key loggers are useful for collecting digital evidence, this monitoring process results in invasion of the student's right to privacy: a personal profile could be built for a specific student. Special consideration should be given to a person's right to privacy; especially if that right is invaded.

The key logger software logs five result files, represented as HTML files, and a varying number of JPEG files per workstation and can deliver the logs to a pre-determined destination. The result files log the following: file and folder manipulation, application accesses, web site visits, keystrokes and screen shots captured. Each file contains various entries associated with each category.

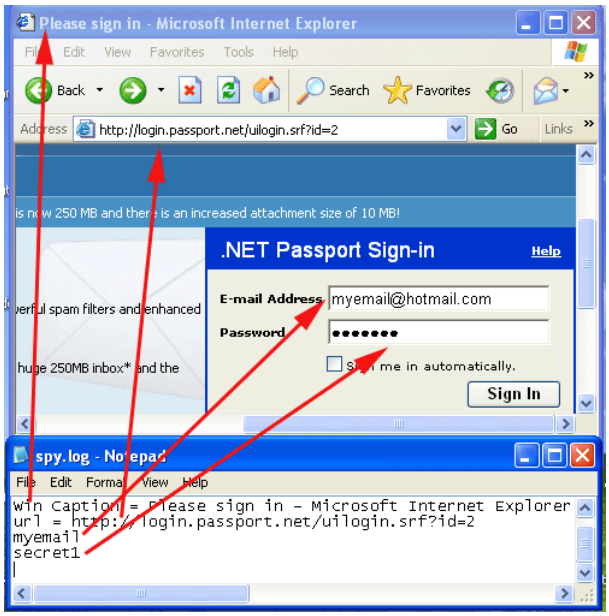

Fig 3. how does a keylogger work?

In the figure shown above we can see that in spy.log text document is created for all the keystrokes recorded and the activities done. For example in this figure "please sign in" window is opened in the Microsoft internet explorer. Also the em.comail id "my email@hotmail" and password "secret1" is also displayed in the spy.log though it is in the form of dot and not visible.

A keylogger captures all keystrokes that the user types on the computer keyboard, including passwords, personal information entered into an online registration form (e.g., a mailing address or telephone number), financial information submitted as part of an online transaction, and the contents of emails or instant messages.

One can have firewall installed in a computer, however normally firewalls are designed to block specific kinds of threats and look only at certain attributes of incoming transmissions, much like the post office looks only at the addresses or attributes on a letter, but does not look at, or attempt to evaluate, the letter's content. Some of the major spyware categories are adware, malware, keylogger, browser helper objects, worms, Trojans, password hijackers, E-mail flooders, firewall killers, spoofers, hacking tools, dialers, tracking cookies, remote administration tools, backdoors and annoyance tools. The password hijackers and Keylogger spywares are the most insidious threats to a user's personal information. Passwords, credit card numbers, and other sensitive or personally identifying information are potentially exposed.

V.CONCLUSION:

Thus using this technology of Monitoring & working by a Keylogger it becomes easy for the user to have a watch on his system whatever activites going on the system .If any one of the hacker or any user performs some undesired activities like related to hacking or harming through viruses , then the user will get acknowledgment of that through the screenshots and recording of the keystrokes in the text file created which contains all the log.

REFERENCES:

[1]Nairit Adhikary, Rohit Shrivastava, Ashwini Kumar, Sunil Kumar Verma, Monark Bag, Vijenndra Singh "*Battering Keyloggers and Screen Recording Software by Fabricating Passwords"* International Journal Computer Network and Information Security, June 2012.

[2] Ankit Parekh, Ajinkya Pawar, Pratik Munot, Piyush Mantri, "*Secure Authentication Using Anti-Screenshot Virtual Keyboard*", International Journal of Computer Science Issues, September 2011.

[3] M. Agarwal , M. Mehra, "*Secure Authentication using Dynamic Virtual Keyboard Layout*", ICWET – TCET, Mumbai, India, 2011

[4] S. Gong, "*Design and Implementation of Anti-Screenshot Virtual Keyboard Applied in Online Banking"* E-Business and E-Government (ICEE), 2010 International Conf., 7-9 May 2010, pp-1320-1322

[5]L. Keun-Gi ,"*USB PassOn: Secure USB Thumb Drive Forensic Toolkit*" , Future Generation Communication and Networking, 2008. FGCN '08. Second International Conf., 13-15 Dec. 2008.

[6] L. Valeri, "*Screen Recording System For Windows Desktop*" Russian-Korean International Symposium Science and Technology conf., 2004, pp.107-109