

**Janardan Bhagat Shikshan Prasarak Sanstha’s**

**CHANGU KANA THAKUR**

**Arts, Commerce, Science College**

**New Panvel (W)**

**CASE STUDY**

**DEVELOPED BY**

**Mr. ROHAN KIRAN THAKUR**

**UNDER THE GUIDENCE OF**

**PROF.MRS. Pratibha Jadhav**

**ACEDEMIC YEAR**

**2019-2020**

**PROJECT TITLE**

**Presentation on “Keyloger”**

**Presentation:**

**Contents:**

* What is a Keylogger?
* What information keylogger collect?
* Why Keyloggers Are A Threat?
* Objectives of keylogger.
* How Keyloggers Spread?

**How To Protect Yourself From Keyloggers?**  
 What is a Keylogger?

* At its most basic definition, a keylogger is a function which records or keystrokes on a computer. Taken at this basic level, a keylogger looks absolutely harmless. In the hands of a hacker or a cybercriminal, a keylogger is a potent tool to steal away your information.
* We'll talk about how a keylogger works, how cybercriminals install it on your computer, and what you can do to avoid being a victim. You'll know what is a keylogger when we're done.

**WHY KEYLOGGERS ARE A THREAT**

* Keyloggers are a serious threat to users and the users' data, as they track the keystrokes to intercept passwords and other sensitive information typed in through the keyboard. This gives hackers the benefit of access to PIN codes and account numbers, passwords to online shopping sites, email ids, email logins, and other confidential information, etc.
* When the hackers get access to the users' private and sensitive information, they can take advantage of the extracted data to perform online money transaction the user's account. Keyloggers can sometimes be used as a spying tool to compromise business and state-owned company's data.

**How does Keylogger work?**

If a computer has a Keylogger install, then it saves the activity of that computer secretly. For example.

* Save any password entered by the user in Computer.
* Save all website URLs searched for
* Record all applications running on the computer.
* Record all Instant Messaging.
* Store Email Remote Location.

**Objectives of keylogger**

* The main objective of keyloggers is to interfere in the chain of events that happen when a key is pressed and when the data is displayed on the monitor as a result of a keystroke.
* A keylogger can be done by introducing a wiring or a hardware bug in the keyboard, to achieve video surveillance; terminating input and/or output; or by also implementing the use of a filter driver in the keyboard stack; and demanding data from the user's keyboard using generalized documented methods

**HOW KEYLOGGERS SPREAD Keyloggers can be installed**

* when a user clicks on a link or opens an attachment/file from a phishing mail
* Keyloggers can be installed through webpage script. This is done by exploiting a vulnerable browser and the
* keylogger is launched when the user visits the malicious website.
* 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 an infected site

**HOW TO PROTECT YOURSELF FROM KEYLOGGERS**

* Take caution when opening attachments: Keyloggers can be present in files received through email, chats, P2P networks, text messages or even social networks. If someone sends you an email out of the cold or the contents of the email are asking for your personal information, chances are there's a keylogger in there somewhere.
* **Use a comprehensive security system:** Install a good Antivirus Product with the latest virus definitions
* **Use of Virtual Keyboard:** Virtual Keyboard helps to avoid personal data interception by the hackers. It is a software used to allow the users to input characters without the actual need for physical keys.
* **Implement Two Factor Authentication:** Strict implementation of Two-factor authentication through one time passwords would help users protect their sensitive credentials, as one-time password is momentary and the hackers cannot use the same detected password the next time.