Welcome

To Our Presentation On Keyloggers

Prepared By: *Suraj shahi*

Content

1. *Definition*
2. *Mode of Infection*
3. *Detecting keylogger activity*
4. *Types of keylogger*
5. *How to Hackers use keylogger data*
6. *Do mobile devices get infected*
7. *Preventive measures*

1)*Definition*

A keylogger, sometimes called a keystroke logger, is a type of surveillance technology used to monitor and record each keystroke on a specific device, such as a computer or smartphone.

2)*Mode of Infection*

- *Surfing suspicious sites and using uncertified software gives way for keyloggers.*
- *Visiting unknown links through emails and text triggers keylogger activity.*
- *Using pop-ups on social sites compels the user to click it and this eventually affects the system.*

3)*Detecting keylogger activity*

- *The keyboard reaction is sluggish due to the monitoring of the keylogger program.*
- *There are instances of system freeze and delayed reaction time.*
- *There are cases of suspicious internet activity where the keylogger may transfer data to its origin.*

4)*Types of keylogger*

1.API-Based keyloggers:

They use API's for keeping log of the keystrokes.

2.Form Grabbing-Based Keyloggers:

They intercept form-based information.

3.Kernel-Based keyloggers:

They hide in system applications and are hard to detect.

4.Hardwar keyloggers:

As name suggest, they are embedded into the keyboard for keylogging.

5)*How hackers use keylogger data*

- *By obtaining the data from the target, hackers use it to "Blackmail" the user.*
- *In the case of company data, it can affect the economic value of the company.*
- *By stealing the government sensitive data, they can breach the security of the country.*

6)*Do mobile devices get infected*

- *There are no specific keylogger programs in hand devices, as they use virtual keyboards for input.*
- *By accessing un-certified websites, there are chances of getting infected by the keylogger programs.*
- *If keyloggers get into the device, they may log typing input and monitor files, photos, emails, etc. and share it with cybercriminals.*

7)*Preventive measures*

- *Use of Antivirus tools and software.*
- *keeping system security protocols updated.*
- *Use the virtual keyboard to input sensitive information, Bank Details, Login Details, etc.*

Thankyou!

Feel Free To Ask Questions.

Email: kingshahi163@gmail.com
Contact: 9809461773