Talking points for the presentation:

1. Slide 1 - Introduction
    a. We will be talking about keyloggers and its functionalities, how they are used ethically and unethically.
2. Slide 2 - what are keyloggers
    a. Keyloggers are usually in the form of usb drives and once plugged in they record the keystrokes of the user.
3. Slide 3 - Key Research Findings
    a. DarkHotel – is a hacker org that targets anything government related,
    b. The olympic vision - The Olympic Vision Keylogger has the capacity to route stolen information to the attacker via email, FTP, or HTTP
4. Slide 4 - DarkHotel
    a. DarkHotel can then collect any private data entered or stored in the device that they want.
    b. use a combination of spear phishing, dangerous malware, and botnet to collect data.
5. Slide 5 - Olympic Vision Keylogger
    a. The Olympic Vision Keylogger has the capacity to route stolen information to the attacker via email, FTP, or HTTP.
    b. The Olympic Vision Keylogger is capable of gathering and exfiltrating system data, keystrokes, clipboard contents, screenshots, and credentials stored.
6. Slide 6 - Ethical Use Cases
    a. parental control purposes
    b. companies using keyloggers to monitor computer activity for security purposes.
7. Slide 7 - Unethical Use Cases
    a. A large portion is for cybercrime, to steal sensitive data
    b. RATs which are remote access trojans, attackers can monitor and fully control the infected computer
8. Slide 8 - conclusion
    a. In conclusion keyloggers functionally are both a massive security risk and help for security testers.

Slide 1: Introduction

Welcome and grab audience attention - keyloggers are easy to program, which basic knowledge of python you can make one yourself

Overview of Keyloggers - keyloggers come in a lot of forms. Software based, usb, and they can be combined into other malware to further cause damage.

Definition - it is a type of malware that records the keystrokes of the users keyboard.

Purpose of the presentation - the purpose of our presentation is to show how ethical and unethical keyloggers are.

Slide 2: What are Keyloggers

1. Definition and types
    a. Hardware-based Keyloggers:
    b. Software-based keyloggers:
    c.

Hardware-based (USB drives)
Software-based
Activation process
USB drive insertion triggers recording

Slide 3: Key Research Findings

DarkHotel
Introduction
Target: Government entities
Tactics
Spear Phishing
Malware
Botnet
Data collection methods
Olympic Vision Keylogger
Introduction
Data routing options
Comprehensive capabilities
System data
Keystrokes
Clipboard contents
Screenshots
Credentials

Slide 4: DarkHotel

DarkHotel's keyloggers are designed not only to record keystrokes but also to exfiltrate the captured data. The stolen information is sent to remote servers controlled by the attackers. This enables them to gather intelligence, sensitive documents, or login credentials for further malicious activities.

Slide 5: Olympic Vision Keylogger

The Olympic Vision keylogger is not a sophisticated malware. Once installed on a device it will steal information including the computer name, Windows product keys, keystrokes, network information, clipboard text, and data saved in browsers, messaging clients, FTP clients, and email clients.

Slide 6: Ethical Use Cases

- Parental control purposes
- Monitoring children's online activity
- Ensuring online safety
- Companies using keyloggers
- Monitoring employee computer activity
- Enhancing cybersecurity measures

Slide 7: Unethical Use Cases

- Cybercrime
- Stealing sensitive data
- Financial fraud
- Remote Access Trojans (RATs)
- Full control and monitoring of infected computers
- Invasion of privacy

Slide 8: Conclusion

- Recap of key points
- Balancing act: Security risk vs. security testing aid
- Importance of awareness and vigilance
- Call to action: Promote responsible use and security measures.