Understanding Keylogger Techniques

Name:meghana Lalam

Date:07-06-2024

Introduction to Keyloggers

- What is a Keylogger?
- - Definition: A keylogger is a type of surveillance software that records keystrokes made by a user.
- - Purpose: Typically used to steal sensitive information like passwords and personal data.

Types of Keyloggers

- Hardware Keyloggers
- - Examples: Keyboard overlays, USB keyloggers.
- - Characteristics: Physically attached to a computer.

- Software Keyloggers
- - Examples: Application keyloggers, Kernel-based keyloggers, API-based keyloggers.
- - Characteristics: Installed on the computer's

How Keyloggers Work

- Basic Mechanism
- - Monitoring and logging keystrokes.
- - Data transmission to the attacker.

- Methods of Operation
- - Capturing keyboard strokes via software.
- - Intercepting input at the kernel level.

Installation Methods

- Social Engineering Techniques
- - Phishing emails, malicious downloads.

- Physical Access
- - Direct installation of hardware keyloggers.

- Malware and Exploits
- - Using other malware to deploy keyloggers.

Detection of Keyloggers

- Symptoms of a Keylogger Infection
- - Slow system performance.
- - Unusual network activity.

- Detection Tools and Techniques
- - Anti-malware software.
- - Regular system scans and monitoring.

Prevention Strategies

- Best Practices
- - Using up-to-date anti-virus and anti-malware software.
- - Regular software updates and patches.

- Physical Security
- - Ensuring physical access control to devices.

- Behavioral Measures

Legal and Ethical Implications

- Legality
- - Laws surrounding the use of keyloggers vary by jurisdiction.

- Ethical Considerations
- - Consent and privacy concerns.
- - Legitimate uses in parental control or corporate monitoring.

Case Studies

- Real-world Examples
- - Notable incidents of keylogger attacks.
- - Impact and aftermath.

Summary and Conclusion

- Recap of Key Points
- - Definition and types of keyloggers.
- - How they work and how they are installed.
- - Detection and prevention methods.

- Final Thoughts
- - Importance of awareness and proactive security measures.

Questions and Discussion

- Invite Questions
- - Open the floor for audience questions.

- Discussion Points
- - Engage the audience in a discussion on keylogger-related experiences or concerns.

References

- List any references or resources used to compile the presentation.