1. What is your chosen malware?

Keylogger

1. How does it work?

It works by recording the keystrokes of a keyboard from a user without their knowledge. The information gathered can be used to find out sensitive information like, passwords, and credit card information.

1. How does social engineering figure into its distribution?

Social engineering is used to first trick the person into installing the keylogger.

1. What are some real-world examples?

Olympic Vision is a keylogger used to attack businessman and uses phishing business emails into tricking them into installing the keylogger.

1. How is it prevented and/or removed?

Methods of prevention varies because there are many ways that a keylogger can be installed in a device. The rule of thumb is to never fall for phishing emails and never click on suspicious links or visit unsecured websites. After you have recognized a keylogger in your computer, you can try to find the file location and delete it or use anti-virus software to remove it.