Information Stealer Using Python

By Inlighn Tech

Objective:

The objective of this project is to develop an **Information Stealer** that extracts sensitive information such as **saved browser passwords, clipboard data, and system information.** This project helps students understand **cybersecurity vulnerabilities, data extraction techniques, and how attackers steal personal data.**

Project Overview:

This Python script performs the following malicious (yet educational) tasks:

1. **Extracts Saved Browser Passwords:**
    - Retrieves stored credentials from Google Chrome.
    - Decrypts saved passwords using system encryption keys.
2. **Captures Clipboard Data:**
    - Reads and stores the latest copied text.
    - Can include sensitive data like passwords and credit card numbers.
3. **Steals System Information:**
    - Gathers OS details, IP address, MAC address, hostname, and processor information.
    - Retrieves public IP using an external API.

How the Project Works:

1. **Decrypting Saved Passwords:**
    a. **The script locates Chrome's encrypted password database.**
    b. **It extracts and decrypts saved passwords using the system's encryption key.**

2. **Clipboard Data Extraction:**
    a. **The script reads the clipboard using `pyperclip` to capture copied text.**

3. **System Information Gathering:**
    a. **The script collects system details like OS version, architecture, IP address, and MAC address.**
    b. **Uses `requests` to fetch the public IP from an external service.**

Key Concepts Covered:

- **Browser Forensics:** Extracting and decrypting saved credentials from Chrome.
- **Cryptography:** Using Windows API (`CryptUnprotectData`) and AES decryption.
- **SQLite Database Handling:** Accessing and reading stored browser credentials.
- **Clipboard Hijacking:** Capturing clipboard data using Python.
- **System Reconnaissance:** Gathering system and network details.
- **Ethical Hacking & Cybersecurity:** Understanding and mitigating real-world threats.

Step-by-Step Implementation:

1. Extracting Saved Passwords

- Retrieves the encryption key from the Chrome `Local State` file.
- Opens the Chrome `Login Data` SQLite database.
- Decrypts saved credentials and displays them.

2. Capturing Clipboard Data

- Uses `pyperclip` to retrieve copied text.
- Displays clipboard content if available.

3. Gathering System Information

- Retrieves OS name, version, IP, MAC address, and processor details.

- Uses an external API to get the public IP address.

Expected Outcomes:

By completing this project, students will:

- Learn **how password storage and encryption work** in web browsers.
- Understand **cryptographic decryption techniques** using AES and Windows API.
- Gain hands-on experience in **extracting system and network information.**
- Understand **how attackers steal data and how to defend against it.**
- Develop a foundational knowledge of **penetration testing and cybersecurity.**

Next Steps:

Students should implement their own version of the Information Stealer using the outlined concepts. A video tutorial will be provided later to demonstrate the correct implementation and security countermeasures.

For further enhancements, students can:

- **Add Keylogging: Capture keystrokes to log user activity.**
- **Stealth Techniques: Hide the script in system startup for persistence.**
- **Remote Data Exfiltration: Send stolen data to a remote server.**
- **Multi-Browser Support: Extend password extraction to Firefox, Edge, etc.**
- **Real-Time Clipboard Monitoring: Continuously capture clipboard changes.**

Disclaimer: This project is for educational and ethical hacking purposes only.

Unauthorized data collection without consent is illegal and violates cybersecurity laws. Always obtain permission before testing these techniques on any system.