- Filename: eccouncil-ceh31250-v10-6-3-1-covert_data_gathering.md
- Show Name: CEHv10 (312-50)
- Topic Name: Attacks and Exploits
- Episode Name: Covert Data Gathering
- Description: In this episode, Daniel and Zach look at ways to clandestinely gather information from target systems and users. Here you'll see how to use keyloggers and implement spyware to record sensitive information through keystrokes, screenshots, and even video/audio capture.

==========

Covert Data Gathering

- **What do we mean by "Covert Data Gathering"?**
- Keyloggers
    - Hardware
        - KeyGrabber
        - KeyGhost
        - *DEMO: Airdrive Keylogger*
    - Software
        - Spyrix
        - *DEMO: Revealer Keylogger Free*
- Spyware
    - Meant to be stealthy
        - Doesn't show in Task Manager
        - Smuggled in with some kind of freeware
        - Does more than keylogging
    - Spytech SpyAgent
        - *DEMO*
        - Install
        - Hotkey access <Shift + Ctrl + Alt + M>
- **Is this the only kind of Spyware that we need to be aware of?**
    - Other types of Spyware
        - Mobile device specific
            - Cell phone
        - GPS
            - https://mspy.com
            - Uses GPS to track device
            - Creates log of GPS data
                - Where/When data
                - Location info
        - USB
            - USBDview
                - https://www.nirsoft.net/utils/usb_devices_view.html
        - A/V
            - Utilizes webcam and/or microphone to record
- **How does Spyware end up on a user's computer?**
    - Smuggled

        - Freeware
        - Games
        - Add-ons
    - Guile
        - Pretends to be some other kind of legit software
    - Drive-by download
    - Exploit browser vulns
    - Social Engineering
- **Is there any way to prevent Spyware and Keyloggers from being installed?**
    - Anti-Spyware software
    - Anti-Keylogger software
    - Prevent unauthorized physical access
    - End User Security Awareness training
    - Updates and Patches
    - Pop-up blockers