Author: DonP1r3lly

Disclaimer: I have created a guide on security and practical advice. The use of this guide is entirely at your own risk, and I disclaim any responsibility for misuse. Please exercise discretion and seek professional advice if needed. If you are in physical danger, contact the authorities in your country.

Incident Responders Personal devices

If you have downloaded a program or file that you are unsure about or has been reported, what can I do?

1. The first step is to use your **antivirus software**; ensure it is up to date and perform a full scan.

2. Check on **VirusTotal.com** or upload the downloaded file to the website to see if there are any reports.

3. Several antivirus vendors offer a **SysRescue Live** on their official websites, which is a Linux image you can burn. It runs independently of your Windows or Mac system and can remove persistent files that compromise the system.

If you want to go further and have some knowledge of computer science, I will now show you various advanced analysis tools.:

4. For Windows, we have SysInternals, always available on the Microsoft website with its documentation. It allows you to view numerous parameters of the computer, including RAM, hard drive, connections, and the registry in real time, and to record all that data.

5. PeStudio: This software can provide you with static property information, the SHA256 hash that you can verify online, etc.

6. Use a lab with Linux/Windows; there are numerous forensic distributions available. I will mention two: Kali Linux and REMnux, which come with pre-installed analysis tools.

7. Within the laboratory, the most common tools include Wireshark, ProcDOT, Process Monitor, and Process Hacker. There are many tools available; use the ones you feel most comfortable with or find easiest to use.

Okay, you've completed all the steps and found nothing. However, if you still feel uneasy about using the computer because you suspect it might be compromised, create a live Linux image, boot from it, and use an available program to overwrite all sectors of the suspected infected disk with a single pass. You will lose all your stored data, but it's always better to ensure that you are clean.

If you have found the guide helpful, please recommend it to your friends.