5 best free security tools you may not know yet

You may already know that online security is important, but you use the right security tool. Different online attacks target computers every minute a day and although standard anti-virus software is very good, they are not designed to solve everything.

You may already know that online security is important, but you use the right security tool. Different online attacks target computers every minute a day and although standard anti-virus software is very good, they are not designed to solve everything.

The following security tools will help you improve your system and network security. You may not have heard of them, but they are very important for online security.

Why haven't you heard of these tools?

Perhaps you think: I installed an online security suite, why do I need these tools?

The answer is simple: the online security suite cannot control each component of the computer. Certainly it can solve viruses, malware, firewalls and sometimes ransomware, but in general these tools can perform different tasks but are not professional.

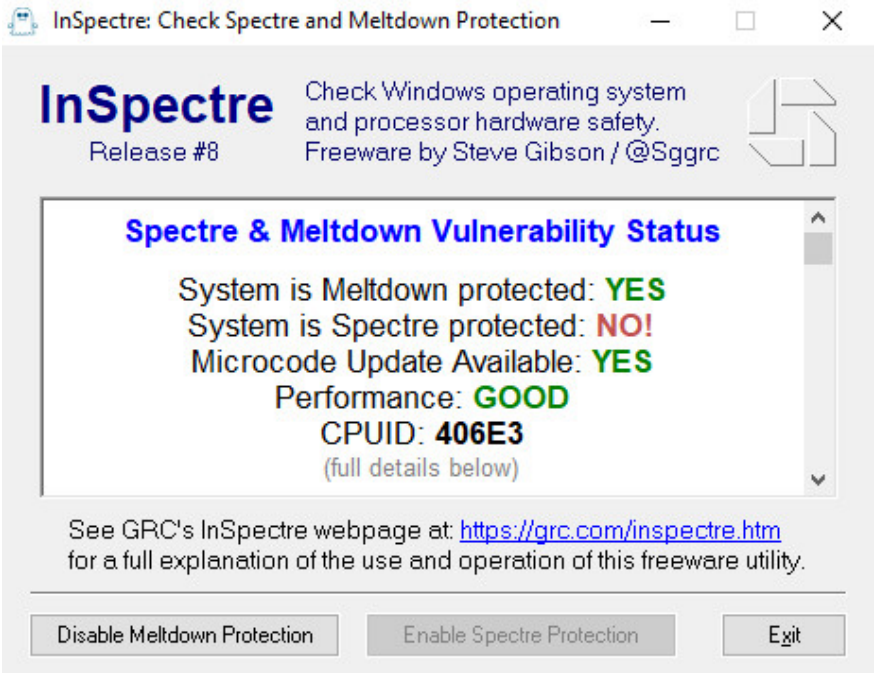
1. 5 signs of computer infection with malware

Whether you use an online security suite or not, install these tools and see how helpful they are in your online security.

1. **InSpectre** : Check the computer for Specter error.
2. **Angry IP Scanner** : Check your network for unauthorized access and bandwidth blocking (using a lot of bandwidth).
3. **Cybereason RansomFree** : Scan the device to find ransomware.
4. **Disconnect** : Monitor connections to your browser.
5. **Malwarebytes Anti-Rootkit:** Removes dangerous rootkits and fixes the damage they cause.

Below are details about each of these important tools and why you should use them in addition to the security tools in use.

1. InSpectre



You've probably heard about Specter and Metldown, CPU holes with exploits still in theory. Not many computers are immune to these vulnerabilities and patches, and operating system updates only slow down the process.

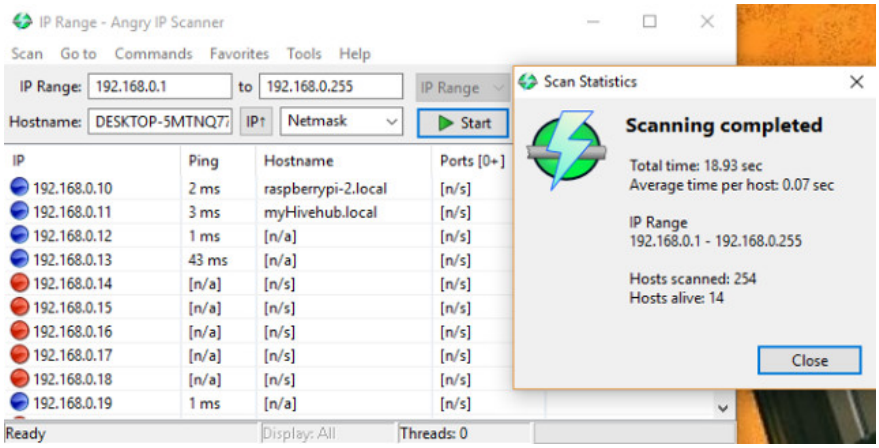
1. All you need to know about Meltdown and Specter - two dangerous vulnerabilities are present on billions of devices running Intel, AMD and ARM chips.

Although Microsoft has released their tool to test the Specter / Metldown vulnerability, it is still very difficult to use. Inpectre is designed to clarify the current status of each system, perform system software and hardware updates to ensure maximum security and performance.

InSpectre is easy to use and informs users immediately if the CPU is affected by CPU errors. In addition, InSpectre notifies if the problem has been patched or has an update. You can disable security, although this is not wise unless your system is experiencing specific performance problems. If disabling can fix the problem, you should upgrade the hardware.

Download : InSpectre

2. Angry IP Scanner



With over 23 million downloads and available for Windows, Mac and Linux operating systems, Angry IP Scanner is a must-have tool for your home router.

As a free and open source tool, Angry IP Scanner will scan local networks, using the IP range you specify. Then, the IP address is pinged and data is collected on each responding device. You can export the result of this scan to text file (as well as XML and CSV).

1. How to export Chrome browsing history to HTML, CSV or TXT file

Note, Angry IP Scanner runs on Java, so you should ensure Java updates if you run this tool regularly. Java has its own security issues, so only regular updates solve this problem.

1. 7 free network tools for Admin

Download : Angry IP Scanner

3. Cybereason RansomFree

You already know about ransomware, this is a type of malware that locks the system, encrypts data and forces you to pay if you want to access it again. It makes it impossible for you to use anything on your computer and perhaps data on the cloud.

1. List of the 3 most dangerous and scary Ransomware viruses

In many cases, after the ransom is paid, the scammers do not comply with the agreement. Although there are a number of tools that can kill ransomware, not all are effective, so you should be prepared.

RansomFree of the Cybereason protects against 99% of ransomware according to its website. RansomFree is available in Windows 7 and new versions, it creates canary files used to detect ransomware behaviors. These files are usually located where the ransomware starts and the ransomware key is locked so that it cannot encrypt data. This software is designed to work with other security software.

Download : RansomFree

4. Disconnect

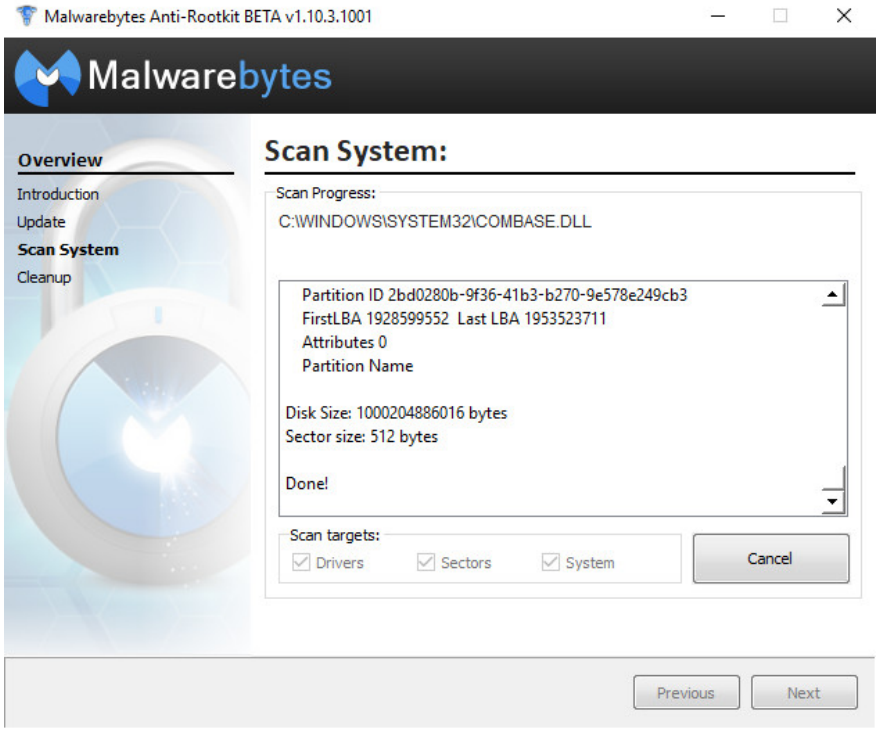
When browsing the web, not only the websites you visit communicate with your browser, ads, analytics, social networks, and many other things that follow you. But with the add on Disconnect browser, you can find out who is following you and act promptly.

By displaying and blocking websites that track you, Disconnect can accelerate your browser 44% faster. And more importantly, it protects when you're online. Although you should not block ads, Disconnect can block invisible monitors from being linked to ad networks or social networks, which are things you should be careful of. In addition, Disconnect has a whitelist option to ensure the content you want to view is still loaded.

Download :

1. Disconnect for Chrome
2. Disconnect for Firefox
3. Disconnect for Opera
4. Disconnect for Safari

5. Malwarebytes Anti-Rootkit



Rootkits can be extremely dangerous, this is a powerful malware that can close anti-virus software, provide administrator privileges and take complete control of your system, rootkits operate at the hardware level.

This means they can control BISO systems as well as operating systems. There are a number of possible solutions to deal with rootkits, but the real tool can help you with Malwarebytes Anti-Rootkit (MBAR). After installation, MBAR will scan the computer and look for threats. Then you just need to press the **Cleanup** button to let the tool resolve the threats and this can be done while restarting the computer.

Currently the software is only beta, it has not been fully supported by developers. However, if you are worried about rootkits, use this tool now.

1. These Anti-Rootkit tools should and should be in the system

Download : Malwarebytes Anti-Rootkit

Are you really as safe as you think? The home network has vulnerabilities that you don't know, Specter errors can attack your devices when unexpected and operate online with the risk of malware attacks.

These tools are free, easy to use and can help you solve a lot of problems. Install them with effective VPN software (such as ExpressVPN or CyberGhost) and high-quality security suite like Bitdefender Internet Security to really secure your online security.

See more:

1. Free Wi-Fi security tools
2. 10 best Hacking and security tools for Linux
3. 5 Security application you should consider removing and replacing