Malware affects us all
The increasing number of Internet users worldwide creates an equal (or larger) number of opportunities for cyber criminals to take advantage of our systems. As we become more dependent on the online environment, we can clearly see a massive growth in malware and cyber criminal activities all across the globe.

Source: McAfee Labs Threats Report, August 2015
With so many ways out there to access and exploit vulnerable systems, we need to make sure we’re able to recognize a malware infection in order to prevent and defend our systems.

**Because it is a battle and you need to be ready.**

This article will show you what the main symptoms of a malware infected system are. You’ll also learn to correctly evaluate the risk and know where to look for a solution. Let’s get to it!

**Symptoms of a malware infection**

1. **SLOWDOWN**

   Does it take longer than normal for your operating system to boot up? Are you waiting too long for some of your programs to start?

   It is a known fact that malware has the tendency to slow down your operating system, your Internet speed or the speed of your applications.

   If you notice something like this and you’re not using any resource-heavy program or application, check for other causes first. It may be a lack of RAM memory, a fragmented system, a lack of space on your hard drive or maybe a hardware issue affecting your drive. These 10 tips will come in handy when evaluating such problems.

   If you have already thoroughly verified these possible causes and all seems fine, you can start considering a potential malware infection.
One of the most annoying signs of malware is represented by the unwanted pop-up windows. Unexpected pop-ups which appear on the system are a typical sign of a spyware infection.

In this particular case, the main issue is created not only by the numerous pop-up windows that affect your Internet navigation, but also because it is quite difficult to remove them from the system.

Pop-ups are not only annoying, but they usually come bundled with other concealed malware threats, and which could be far more destructive for our systems.

To avoid spyware and its impact on our systems, keep in mind a few security practices:

- don’t click any suspicious pop-up windows
- don’t answer unsolicited emails/messages
- be careful when downloading free applications
3. CRASHES

If your programs or your system crash constantly or the infamous BSOD (Blue Screen of Death) appears regularly, it’s a clear warning that your system is not working properly and you should look into it.

There are two things that can cause this type of issues:

- You could be dealing with a technical issue caused by a potential incompatibility between your software and/or hardware
- Or it may be a malware issue.

If you suspect a technical issue, multiple software problems may lead to this.

*Are you running various programs which may conflict with each other? Are there any orphan registry keys which have not been removed that could down and eventually crash your system?*

If you are checking for malware, simply run a complete scan on the system with a good antivirus product. **It is important to have a reliable security solution on your system,** which should include real-time scanning, automatic update and a firewall.

To find the best solution, check the antivirus test results run by big company names in the security industry, such as AV Comparatives, PC Magazine, AV-TEST or Virus Bulletin and select the best antivirus solution for your system.
4. **SUSPICIOUS HARD DRIVE ACTIVITY**

Another warning sign of a potential malware infection on your system is the **hard drive activity**.

If you notice that your disk continues to exhibit **excessive activity** even when you don’t use it and there is no program or download running at that moment, this could be the right time to check your system for malware.

We have to mention that another possible cause for the abnormal hard disk activity could be a hardware failure of the disk. You should also take this into consideration.

5. **RUNNING OUT OF HARD DRIVE SPACE**

Regarding the hard drive, you also need to check if your physical storage space has been increasing lately or if some of your files disappeared or changed their names.

This is another sign of malware activity, since there are numerous types of malicious software which use various methods to fill up all the available space in the hard drive and cause it to crash.

6. **UNUSUALLY HIGH NETWORK ACTIVITY**
There are cases where the user is not connected to the Internet through his browser, and there is no program that may connect to online servers to download or upload any data, but high network activity can still be observed.

First of all, we need to check the following:

- Is there any Windows update at that moment?
- Is there any program or application that’s downloading or uploading any data?
- Is there any update for a certain app running at that moment?
- Is there a large download that you started and forgot about, which may still be running in the background?

If the answer to all these questions is No, then maybe you should check where all that traffic is going.

- To monitor your network, you can use one of the following programs: GlassWire, Little Snitch or Wireshark.

- To check for a malware infection, use a good antivirus product to check your system.

- If you suspect that your computer has been infected by a dangerous financial malware, you need a specialized security suite designed to address these type of threats.
7. NEW BROWSER HOMEPAGE, NEW TOOLBARS and/or UNWANTED WEBSITES ACCESSED WITHOUT YOUR INPUT

Have you noticed that your home page has been changed and you don’t remember doing it yourself? Did a new toolbar pop out of nowhere and landed at top of your web browser? Have you tried to access your favorite blog, but you were redirected to a different address?

This usually happens when you visit a website and you accidentally click a link or a pop-up window. This triggers unwanted software to download and install on your device. Its effects are not only annoying, but also malicious.

Run a complete scan with your security solution as soon as possible. Because these type of threats don’t go away easily. Make sure you run additional scans with specialized software, such as anti-spyware programs as the ones mentioned above.
8. UNUSUAL MESSAGES OR PROGRAMS THAT START AUTOMATICALLY

A few warning signs should really make you suspicious. If any of these happen, pay closer attention and try finding the cause:

- if, all of a sudden, you see programs opening and closing automatically
- your Windows operating system shutting down without reason
- if you notice strange windows in the booting process
- or if Windows informs you that you’ve lost access to some of your drives.

Though the root cause may be a technical one, it could also be a sign that malware has compromised your system. If this is the case and you lost access to some important areas of your operating system, you need to prepare for the worst. These are the cases when a complete wipe and reinstall of the operating system is taken into consideration.

9. YOUR SECURITY SOLUTION IS DISABLED

If your antivirus solution doesn't seem to work anymore or if the Update module seems to be disabled, then check to see what happened immediately!

You should know that some types of malware are especially designed to disable security solutions, leaving you without any defense. If you already tried to reboot your computer, close and open the security solution and all your troubleshooting efforts were useless, you could consider the malware infection scenario.

This is especially the case since traditional antivirus solutions are sometimes unable to block and remove advanced malware, such as ransomware or financial malware.
10. YOUR FRIENDS TELL YOUR THAT THEY’RE GETTING STRANGE MESSAGES FROM YOU

Are your friends telling you that they received suspicious emails from you or instant messages from your social media account, which often include attachments or links?

Source: Malware spread via Facebook chat

First of all, you need to verify whether those emails or messages were sent from one of your accounts (so check your Sent Items folder in your email/social media account). If there’s nothing there, those messages could have been delivered from an application which is out of your control.

If you discover the messages were sent from one of your accounts, take these steps:

- **Make sure you logged out from all your accounts.** We access the same accounts on our work computers, on our home laptops and of course, on our mobile devices. Since we log in to our

- **Set strong passwords for your accounts.** Don’t use the same password for all your accounts! Even if you are hacked, having different passwords for each account will help you limit a potential loss. Make a habit of managing your passwords safely.

- **Use two-factor authentication.** This option can significantly increase your control over your accounts’ security. Using two-factor authentication means that, besides entering your credentials, you will also need to enter a code sent to your phone.
Knowledge is our best weapon

Knowing how malicious software behaves on a regular system may just prove to be the key element between staying safe and having your system wrecked or your online identity stolen.

Since we live in a connected and complex environment, online security doesn’t end with installing a series of security programs and forgetting about them. It’s essential that we also understand how malware behaves on the system, so we can mitigate its impact.

In the end, it is our knowledge of malware tools and methods that keeps us safe, because it is far easier to prevent a threat from becoming reality than to take actions against it when it’s already too late.