

The Dirty Dozen

Following several news stories relating to viruses, phishing and general computer security issues, I thought it would be apt to explain in a little more detail what are all these “Viruses”. In fact viruses are actually just one type of Malware. As the name implies, Malware is a software programme that causes harm or problems, most of which has some sort of commercial, if not criminal, basis, depending on the payload that the Malware delivers. There are 11 main types of Malware, but including Adaware, they are often referred to as the Dirty Dozen:

I have delved into Wikipedia somewhat for part of this information, so plenty of credit to a very useful website:

1/ Virus. The type of malware that everybody hears about and that has become the generic term for all types of Malware. A computer virus is a programme that infects executable files, that when run tries to infect other executable software, but also often carries with it a payload that tries to perform other, often malicious actions.

2/ Worm. A close cousin to the virus, the main difference being that a worm is designed to spread itself automatically, whereas a virus requires user intervention for it to spread. Thus viruses hide inside the files of real computer programs (for instance, the macros in Word or the VBScript etc.), while worms do not infect a file or program, but rather stand on their own.

3/ Trojan. As the name implies, their main strength is disguise, and often only get onto your computer when installed by the user himself - arguably the most dangerous kind of malware. You typically pick these up when you download what seems to be legitimate software to which has been added the Trojan, thus installing it yourself on the PC. The Trojan then runs on your PC, using its concealment to hide itself from you and then delivers its payload. Trojans rarely destroy computers or even files because they have bigger targets: your financial information or your computer's system resources, and sometimes even a denial-of-service attack - when thousands of computers all try to connect to a web server at the same time thus rendering it unavailable.

4/ Spyware. Does exactly what it says on the tin - software that spies on you, often tracking your internet activities in order to serve you advertising, encouraging you to buy products that you probably do not want. Also showing you pop up adverts whilst browsing the internet, or even redirecting your browser to their website.

5/ Backdoors – again the name gives it away, these are much the same as Trojans or worms, except that they do something different: they open a "backdoor" onto your computer. This then provides the hacker with a network connection access to your PC, to allow him to install malware or use your PC to send out huge quantities of spam via your own or other email addresses.

6/ Exploits. These attack specific security vulnerabilities. What exploits do is gain access to your computer (via a network or locally) and then increase their own user privileges in order to become super-users. I am sure you have seen Microsoft announcing new updates for its operating system? Often enough the updates are really trying to close the security hole targeted in a newly discovered exploit.

7/ Rootkit. The malware most likely to have a human touch, Rootkits are installed by hackers on other people's computers. The Rootkit is designed to camouflage itself in a system's core processes so as to go undetected, it can hide itself very well with its process not appearing the “system processes”, and also runs ghost

processes that detect when another ghost process has been stopped and restart them within milliseconds. It is the hardest of all malware to detect and also to remove, mainly as it is running on your computer as “root” (administrator) and thus has full access to the system.

8/ Keyloggers. Easy this one: yes, it logs your keystrokes, i.e., it records exactly what you type. Typically, those behind the Keyloggers are out to collect sensitive information such as passwords and financial details that you type on your keyboard that the keylogger software then relays to the hackers.

9/ Wabbits. Not the Bugs Bunny type, but a rare type of malware that concentrates on devastating a single machine, without specifically trying to email or copy itself to another machine.

10/ Dialers. This malware dials telephone numbers via your computer's modem. Dialers either dial expensive premium-rate telephone numbers, often located in small countries far from the host computer; or, they dial a hacker's machine to transmit stolen data.

11/ Browser Hijack. Again, this does exactly what it says on the box, altering your homepage or redirecting your browser to specific websites for advertising purposes, but also some of these websites then allow remote access to your computer.

12/ Adware. The least dangerous and most lucrative malware (lucrative for its distributors). Adware displays adverts on your computer. The Wikipedia entry states that some users choose to allow Adware on his or her machine, and thus it's not really malware. Adware normally comes with software you have downloaded and is installed on your machine totally legally as the terms and conditions you accept before installing the software state that you are also installing the Adware!!! Ever read the full terms and conditions when installing software, there's pages and pages of it so no one notices the references to installing the Adware at the same time!!

So there you go, that's the dirty dozen, just make sure you have an up-to-date antivirus programme running (make sure it actually scans!!) and something that looks for alternative types of malware including the most common – Adware. You can either buy software from the market leaders such as Symantec (Norton), McAfee, or download a free one such as AVG. I would also download a second programme that looks for Adware in particular, my favourite being, Lavasoft's Adaware, which you can then run manually once a week just to be sure you are infection free. However do be careful when you download the antivirus software as there are many rogue sites where you can download a modified version of the software!! I myself, always go to the manufacturer's website or www.download.com, but never go to sites such as www.getfreesoftwarehereandmaybeavirus.com !!

For computer problems and advice, please contact: Edward on 06 26 98 03 12 or by email on ed@emarshall.fr All previous VVV Computer articles can be found at www.emarshall.fr