Malware infections — prevention and cure

A simple look at statistics from last 24h in virustotal.com site reveal the fact that only 2% from the files submitted are detected by the ALL antivirus engine, for the rest of 98% one or more antiviruses are failing in detection. There is tests that shows aproximately only 20% of new trojans are detected by an antivirus, any of them, it does not matter but my believing is the percentage is in reality lower than 20%, maybe 1 -5 % of *new trojans – zero day attacks* are detected by an antivirus because speaking of unknown and newly created trojans, only **heuristic** and **file emulation** can be used as detection method, the **signature based** method is out of discussion or this is the method on which antiviruses are relying heavy.

After all these, it is a known fact that **thousands** of new malware are created daily and spreaded in the wild. Until the antiviruses to be updated with new viruses trojans , it will be a period of time while the computer users are without defense–naked. An helpful approach is the *cloud computing* antivirus where a PC send in a cloud, a network in fact, a dubious program for analysis with a few of detecting engines, receiving the results of scanning in real time. **Clam AV** is one of the antivirus software using the cloud technique developed by Immunet company.

If we talk about a *private* malware, ordered and buyed by someone from a virus creator this period of time will be in order of months or years. An example of *private* trojan is Zeus or Zbot used for banking password stealing, it uses a polymorhic engine to bypass antivirus protection and according to Trusteer the leading provider of secure browsing services, it already infected 1% from all the computers, 55% with up-to-date antiviruses software installed. More about Zeus trojan can be found here. But there is a lot of *private* trojans in the wild, other than Zeus, to understand the proportion of this plague it's enough to take the pulse of underground(hidden) hackers forums where a whole malware industry is maintained with an enormous amount of money involved in. What I tell you is not to drop the antivirus software to trash, only it should *not* to be your only line of defense, instead a defense *strategy* must be thought for preventing computer infections.

Ok, this is theory let's talk about some practical approaches. I say above that an antivirus can use file emulation as detecting method, this is achieved by running an executable in an virtual environment and checking the operations executed by the program, this way determining if it's a malware or not. It's kind of a sandbox, or we have **Sandboxie** coming in our help for manual programs analysis. Very often manual analysis of programs, gives better results as an antivirus software especially with new created malware, but must be considered as a secondary option after the traditional antivirus scan and must be considered when we are dealing with programs coming from untrusted sources as forums or blogs.

Returning to the Sanboxie, it creates a folder in the C partition(default) with the name *Sandbox* which contain another folder with the name of the user which are running the program sandboxed, which contain another folder *DefaultBox* and finally inside it is the folders *drive* and *user.* Inside the *drive* folder are the "fake" computer drives e.g. : C,D,E with Program Files ProgramData and Windows folders and so on, which will trick the program making it think it run in the real computer and inside the *user* folder there is folders normally situated in C:\Documents and Settings\%user% as Application Data, Local Settings or any other folder the sandboxed program needs to write in. Supposing we are running a program with a malware embedded in it and checking the folders above mentioned, we can easily see what kind of files the program drop in the folders. The trojans and other malware loves to copy themselves in Temporary, Local Settings, Users profile or Application data folders and if we find there a little executable with strange name and strange File Properties we know that we deal with an malware. The malware creators are often stupid enough to write

“alien” things as “ftyh^&*)w” or “gklti78%$9″ for Company or Legal Copyright, I saw very often this kind of childish behaviour in the malware creations.

No need to say that running sandboxed a program or the browser we prevent the computer infections but this is in the same time a simple analysis method if we know where to look.

Faronics has some interesting software, adding another layer of security with its **Faronics Anti-Executable** or **Faronics Deep Freeze**.

Faronics Anti-Executable, uses a whitelisting method, the same like some antiviruses for preventing unwanted, unauthorised or unlicensed programs to run. Malicious programs as keyloggers or trajans are blocked to run or installing, in conclusion white list method of protection is an effective way to eliminate the threats without the needing of ‘updates” like antimalware software.

Faronics Deep Freeze is like a general sandbox, every change made in a computer malicious or not is deleted at computer reboot. For example if accidentally we mess-up the registry, delete some important files or some viruses made malicious changes to the system, all these nightmares will be gone at computer restart, resulting a truly bulletproof computer.

Similar programs are Clean Slate 6.5 , ShadowProtect or SmartShield. The last one has a special price these days, you might want check it out, and more it protect the CMOS settings as well, being able to recover up to 2 TB of data in seconds.

All these programs are alternatives for clasic back-ups or for cloning partitions methods of “staying on the safe side”. The cloning partitions approach was covered here.

Another security approach for computers are **Rescue Disks**, available as freeware at the most security programs vendors sites. Rescue disks perform a computer disinfect and cleaning from “outside the box”, the computer is booting from CD-ROM or DVD-ROM and having as a big advantage that the operating system and possibly malware programs are “sleeping”, being not able to hide themselves anymore. It’s a known fact that a lot of malware as rootkits are able to hide deeply in a running operating system using the system holes –vulnerabilities or features.

One of the best **Rescue System** are from **Avira GmbH** , and make possible to repair a damaged system, to rescue data or scan and delete the malware found on hard-disk. The download has two variants, and executable or the .ISO file which will be burned to CD. Another free tools from Avira can be found here:

-Avira AntiVir RegistryCleaner(for removing entries of Avira Antivir previously installations)

-Avira AntiVir Boot Sector Repair Tool

-Avira AntiRootkit Tool

Kaspersky also released a Rescue Disk, download from here, able to boot the computer from CD-ROM in a Linux like environment.

Bitdefender vendor released also a rescue CD, with a cool feature, it can auto update the virus definitions when booting from CD with condition that an Internet connection is available of course. The same feature exists also for **F-Secure Rescue CD,** another tool that uses a Linux distribution(Knoppix) to boot and run completely from the CD.

AVG created a free Rescue CD , able to run from a CD or from an USB stick

Trinity Rescue Kit, is a Live Linux CD with tools for recovering data off a formatted disk, for fixing Master Boot Record, for resetting windows passwords, recovery of lost partitions, rootkit detection tools and with 4 virus scanning engines : ClamAV, AVG, F-Prot, BitDefender–all integrated in a single command line. Can be used also with an USB stick and has online update capabilities for the antiviruses definitions database.

More on the next articles.

Share this:

- Share