Win 32 Sality virus removal

As I said somewhere in this website, I don't have installed any antivirus and I'm running Windows operating system a risky game some of you maybe will say, a true cyber-suicide other are saying. I have never recommended this test to anyone, my intention was only to have a very close look of reality of the threats that Windows are confronted with. Something at the frontier of stupidity and a malware lab. To reproduce exactly the wished environment, that's an unprotected real computer(not a virtual machine because some malware are aware of it) and an unsuspecting user, my kids have full access to this computer to do whatever they want even if they have their own computer. All was OK and believe it or not, very few viruses hit the computer in years until a few days ago when I discovered accidentally that I had not access anymore to Task Manager, it was deactivated, colored in grey. Obviously, the first sign of a malware infection.

Quickly I've done a computer summary audit and discovered these at a first glance:

- Surprisingly, I had access to Registry Editor but any modification I have made there was quickly reversed. For example when I've tried to restore the Task Manager access changing the *DisableTaskMgr* registry key value data from *1 to 0* (this key is in *HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System*), this change was reversed in a few seconds. It's obvious that a process is running in the background supervising the registry.
- Altough it was set to be shown hidden files and folders, the malware changed the settings. I was able to set back to view hidden files and folders for enough time to see in each drive **C:** and **D:** three new files apparently with random names like:

olbl – a shortcut to an MS-DOS program MD5: 3C903788D5438C82F349E679C6A6893F

autorun.inf – with the next content:

```
[AutoRun]
;
;bedRssMexVy JhUSer yvkFTaQMlXxPbKIuivn
Open =aeft.pif
;PlmBvpnebCdgCjIo YsKyY xnGtRvviHj hkuqe
sHElL\expLore\comMANd=aeft.pif
;rnntWndHKJ
sHeLl\OPEn\dEFauLt=1
;hcxyPNmxvaiJlMuf
shEll\oPEN\cOMmANd= aeft.pif
;
SHell\auToPLaY\cOMmand =aeft.pif
```

aeft.pif - MD5: 3C903788D5438C82F349E679C6A6893F

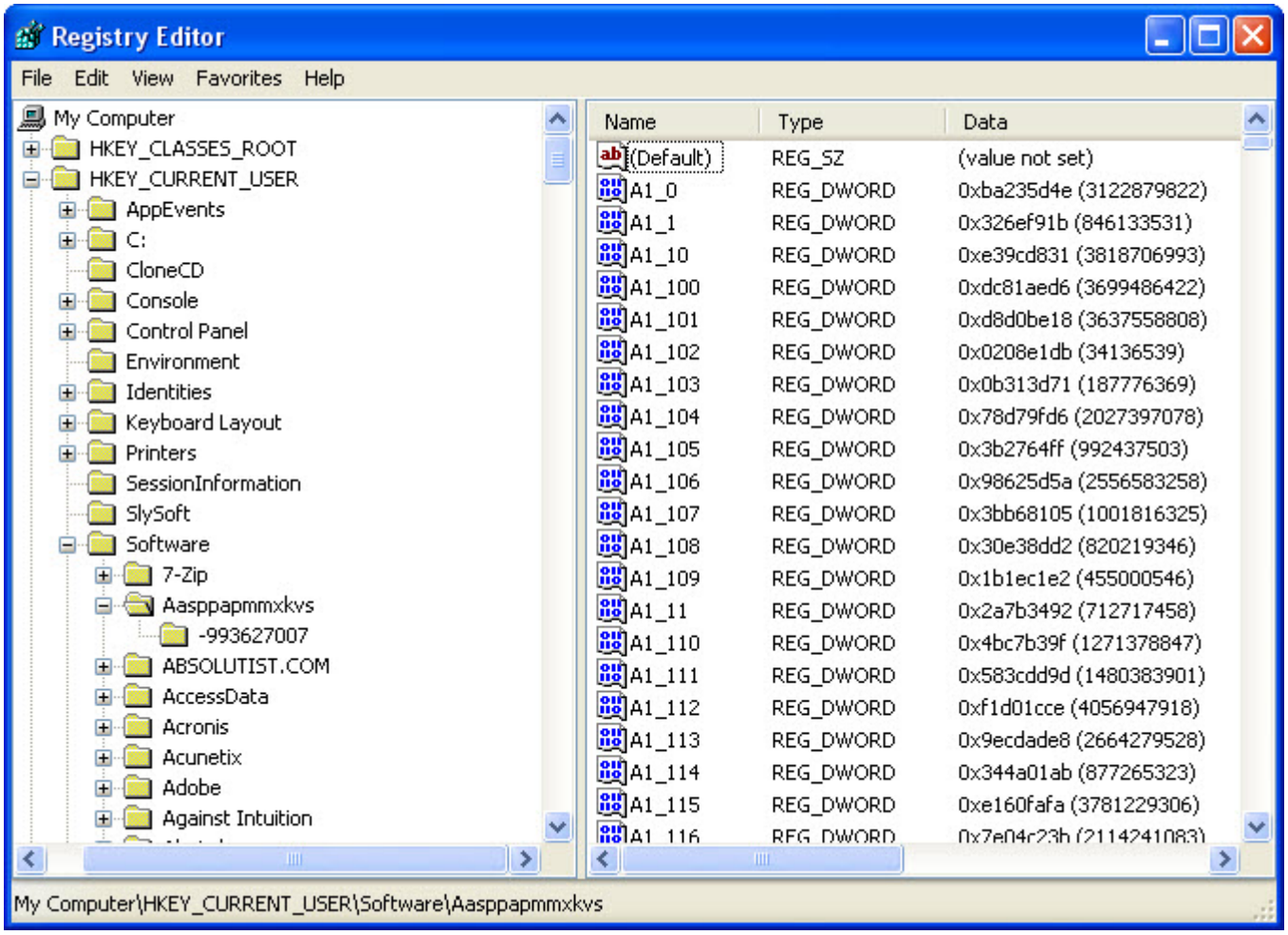
We can notice that **aeft.pif** and **olbl** has the same size and the same MD5 value so it's the same file with other name.

- I am running *Private Firewall* which tells me(pop up a window) each time an executable wants to run with my interaction(double-click) or automatically. This time it said an executable located in

Temporary folder, **winipag.exe** wants to run. I have blocked it.
- Using *Process Hacker* looking for a possible malicious process, I don't saw any, but the majority of legitimate processes were listening to an UDP port which was strange.
- Scanning the **aeft.pif** file to virustotal.com was given a result for *Win32 Sality* malware with a detection ratio of 20/42. A few antivirus big names failed to detect it. For winipag.exe file the detection ratio was higher, of 37/42 detected foe example by Microsoft antivirus as *TrojanProxy:Win32/Pramro.F* or *Spam-Mailbot.z* by McAfee antivirus.

Here is a summary list with Win32 Sality virus features:

- Win32 Sality search for executable files, files with .exe or .scr extension on your hard disk and infects them appending its body to their code in the last section. It changes the code at Entry Point(not Entry Point itself as address) of executables where the code execution starts, redirecting the instructions flow to their own code first, then the control is passed to the host file. If the virus finds a file belonging to an antivirus, it tries to damage or delete it.
- This malware has a polymorphic engine, meaning that its code is changed with every other infection and therefore is almost impossible to be detected based on virus signature.
- Win 32 Sality injects its body to almost all the running processes(those belonging to "system", "local service" and "network service" are excluded.
- Win 32 Sality contains a kernel driver responsible for killing all the processes belonging to an antivirus software. The list of the processes is hard-coded in its body and contains almost all the antiviruses. This driver is also responsible for blocking access to antivirus or security websites being impossible to download malware removal tools from there.
- The users of infected computers with Sality can not use Task Manager anymore, can not boot in Safe Mode, can not view hidden files and folders, can not edit the registry anymore
- Win 32 Sality uses a P2P network over UDP for communications. The number of UDP port is generated based on infected computer name so we can assume it is randomly generated. There is not a central Command&Control server, instead the *list of peers(URL packs)* and other *malware downloaded(EXE packs)* are exchanged between peers. The EXE packs are digitally signed and transferred over TCP because of the reliability of this protocol, these packs contains as I said other malware generally spam generators or spam relays but as well they can be information stealer trojans. The malware has a mechanism able to update continuously the peer list with good, reachable peers, other "bad" non-reachable peers being discarded from the peer list. This list of peers is stored in computer registry in an encrypted form being able to hold maximum 1000 entries. A such list looks like this:



sality_peerlist

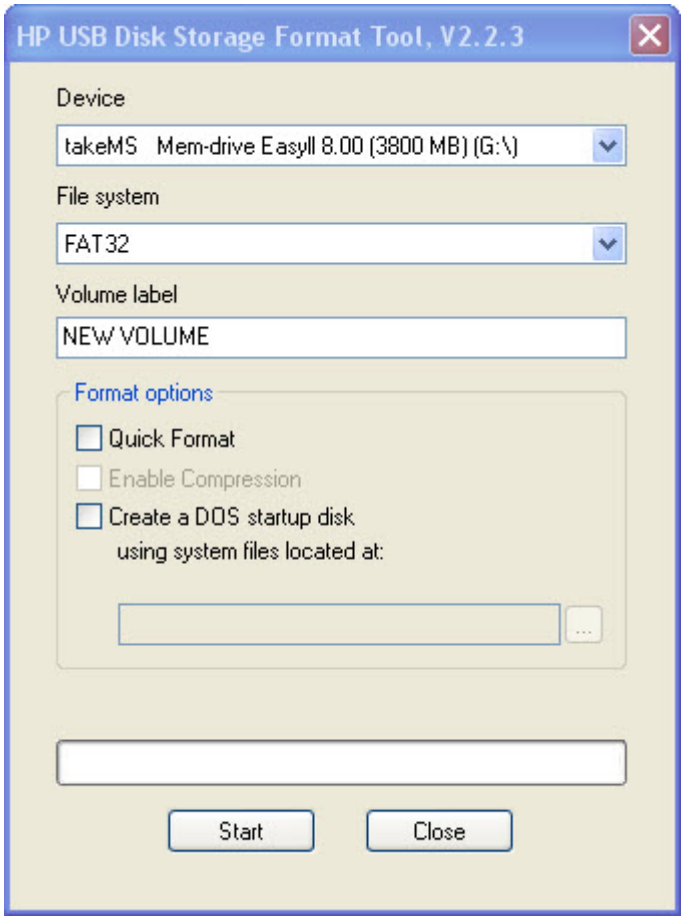
Win 32 Sality virus was first seen in 2003 in russian space, since then it was continuously improved by its creators resulting a top virus if I can say so, a strong competitor of Conficker. In the real conditions is impossible to take down its botnet, it's very hard for an antivirus and for some impossible to disinfect a computer infected with Sality using traditional methods.

Returning to my computer infected with this virus, after I search for help with Google I decided to use *Kaspersky Win32/Sality Remover* downloaded from softpedia.com because the Kaspersky official website was not accesible. After I run it two times it was obvious that the tool had not effect upon malware I don't know why, maybe it is outdated. Another recommendation that I found was to use *Avira AntiVir Rescue System*. I thought it's a good idea to install it to an USB flash drive, for this you need:

- The .iso file of *Avira AntiVir Rescue System*(further I will name it AVRS) – it's based on a small Linux distribution and Avira engine itself
- *UNetbootin for Windows* for installing Avira AVRS on USB flash drive
- *HP USB Disk Storage Format Tool* for formatting the USB flash in FAT32 format

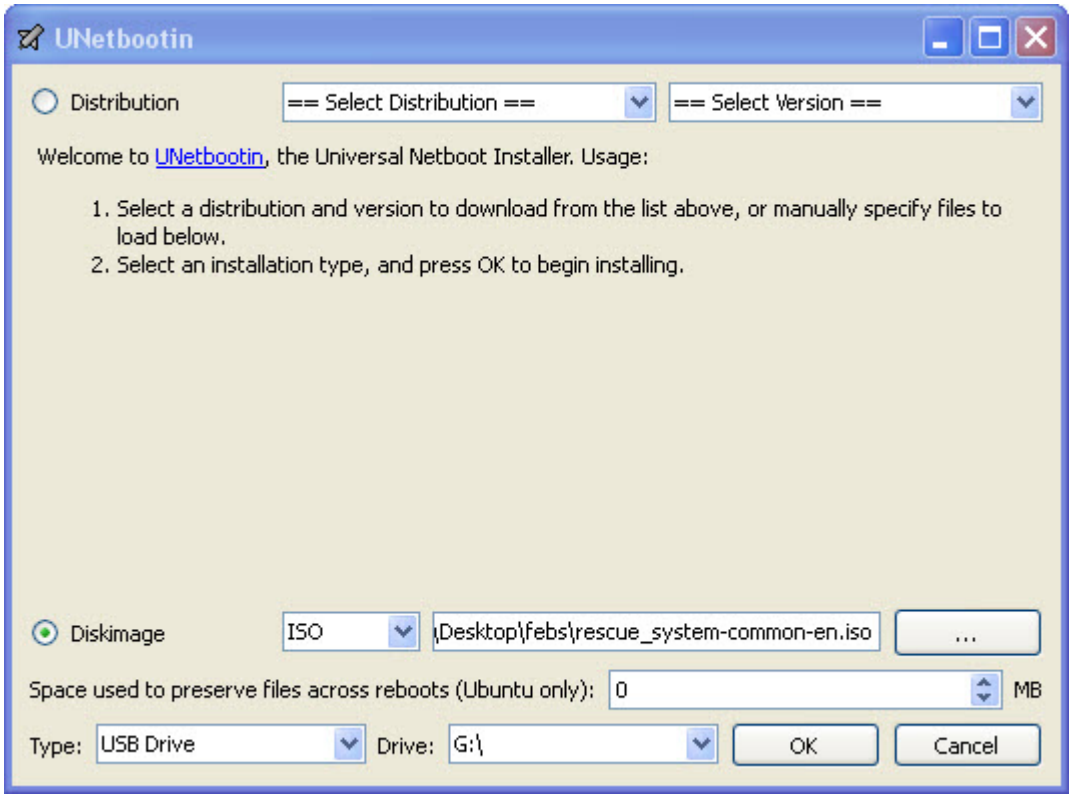
The steps are very simple and are described below in images.

First we need to format the USB flash drive, G:\ is the drive letter for USB flash drive:



hp-usb-disk-storage-format-tool

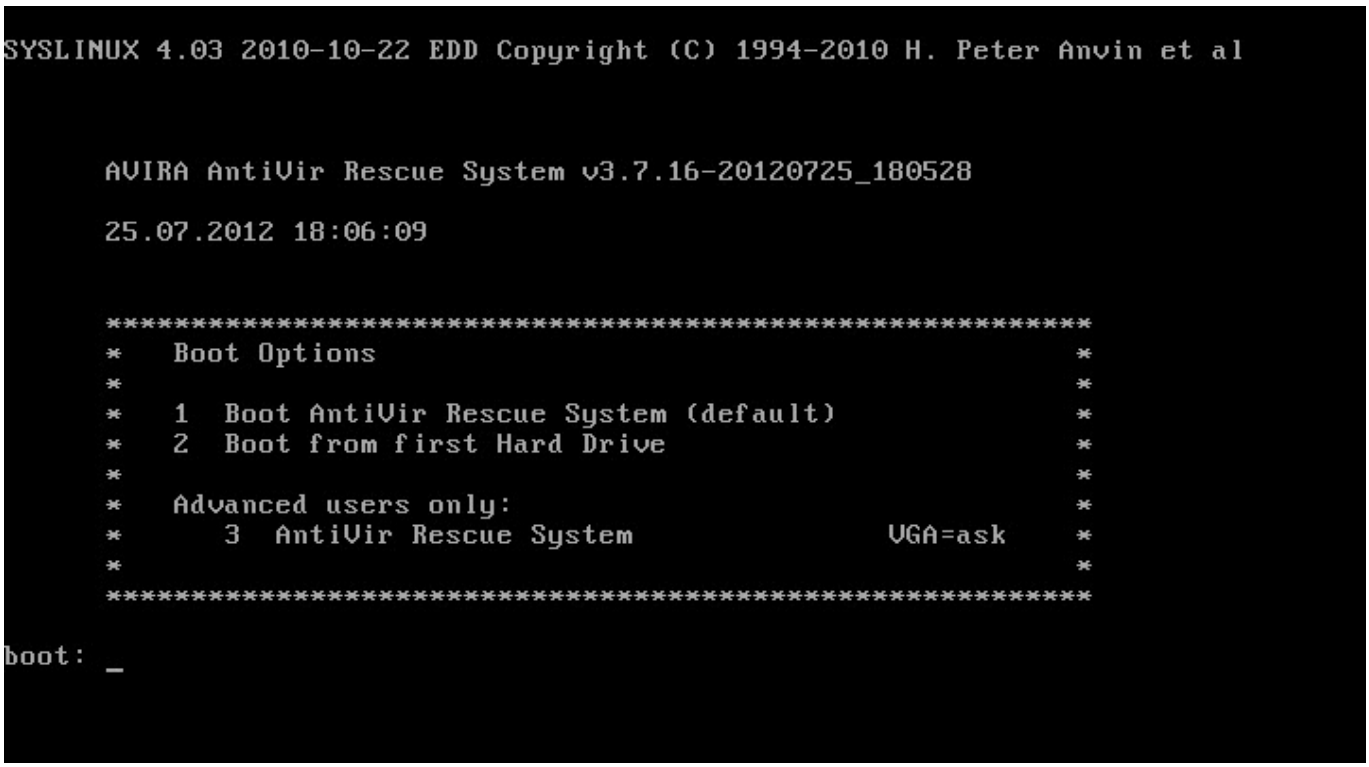
Press start button and the USB drive will be formatted. Next, run UNetbootin, choose *Diskimage* and point to the .iso file downloaded, click OK:



UNetbootin

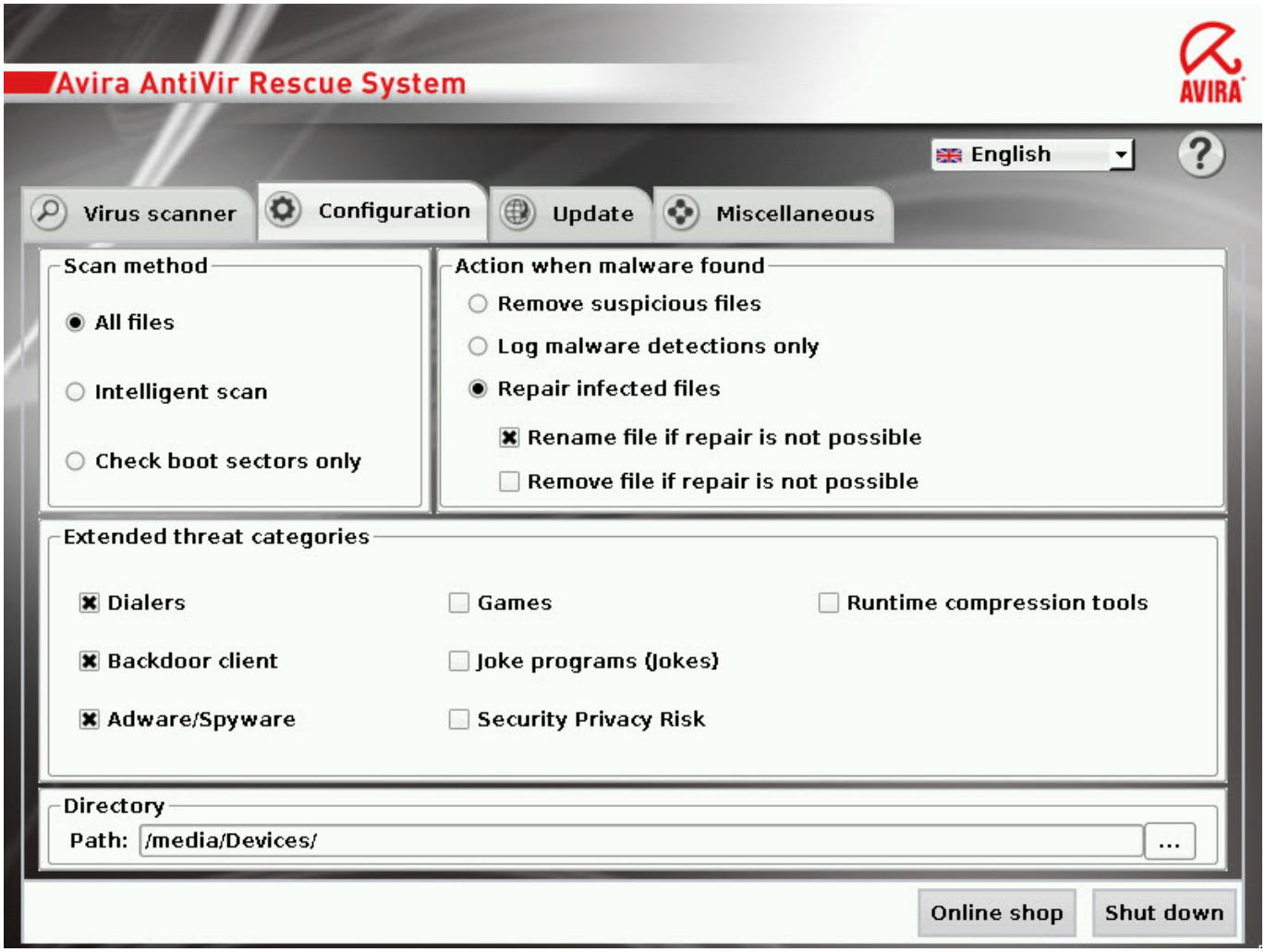
OK, after finishing our bootable USB stick, its time to change the setting in BIOS and make the computer at next boot to boot from USB drive. Here , or here are good tutorials how to do this if you don't know. One more good tutorial here.

You will be presented with this screen:



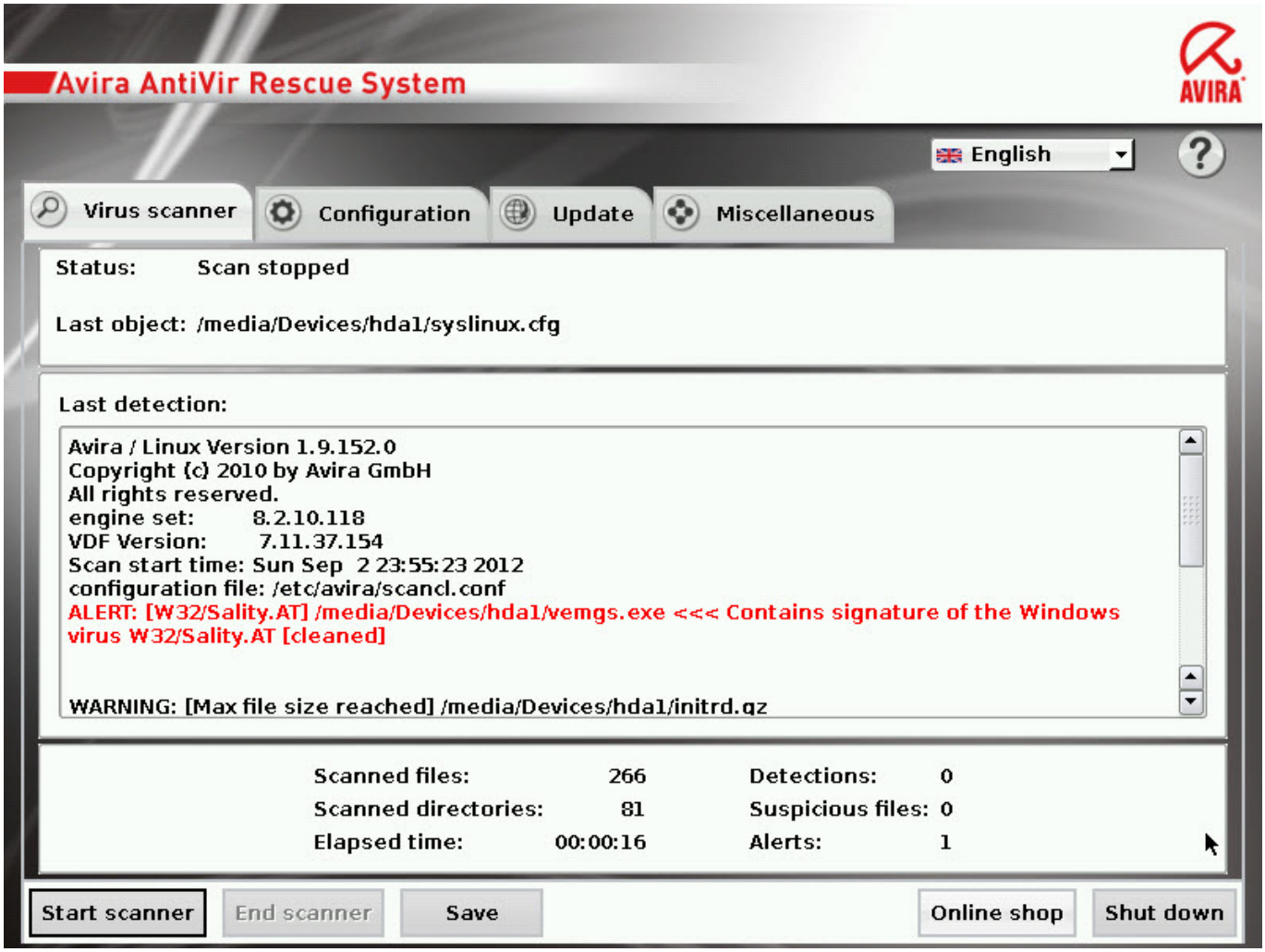
avira_rescue_system_boot

The default boot option is set to Antivir Rescue System so you can hit Enter. Also the configuration of the system is set, you can leave it as it is:



avira_rescue_system_configuration

And start the scanner, as you can see below that it finds the files infected with Win32 Sality and other malware if it’s the case and tries to disinfect them:



avira_rescue_system_scanner

And that's all, after finishing its job you can shut down Antivir Rescue System, remove USB drive from the computer, change the BIOS to boot normally from the hard disk and you will have a completely clean of Win32 Sality computer. At least that was my case. Of course you can try as well other Rescue Disks:

- *Kaspersky Rescue Disk*
- *Dr.Web LiveCD*
- *BitDefender Antivirus Rescue CD*
- *AVG Rescue CD*

The best chances to get rid of Win32 Sality virus is to use a Rescue CD and act from outside of Windows when it is asleep, this virus injects a lot of legitimate processes with its code, some of the processes being used even by Windows versions of antivirus software therefore being impossible for these antivirus software to stop the processes and clean the files.

Dirk Knop, Technical Editor at Avira said here:

> The removal of W32/Sality isn't as easy as we like it to be though. It should be done using our Rescue CD which also includes the updated engine. This is due to the fact that

> it’s not possible to kill all processes at runtime to get hold of the binary files and disinfect them. It is always a good idea to clean an infected system with the Rescue CD as the malware isn’t active when the computer is started from the CD.

For an extended read about Win32 Sality you can go here, it’s a very comprehensive PDF document written by **Nicolas Falliere** from Symantec.

Keep Safe !

Share this:

- Share