How to detect computer viruses in pirated software

The software, music, movies piracy is a reality of our days, we like it or not. Although it's illegal, some argue the use of pirated software(warez) mentioning the high cost of it, the lack of money or simply is using it because "it is there", on some warez forums or blogs, without thinking too much at legal issues. This article has not as topic this debate if the warez use is justified or not, it's everyone's responsibility how they answer to this question and what are their actions. Certainly, embedding malware, especially computer trojans in program's setup files and spreading the links via warez forums is one of the different methods used by bad boys to steal emails accounts, banking or other important accounts credentials.

The warez forums are the perfect environment to launch computers infecting campaigns for a good reason: anybody can upload to a files sharing website whatever he wants and post the link, nobody including forum staff can guarantee that the posted program is clean of malware unless somebody download the program and scan it with an antivirus but who does that? The forum users, assuming for themselves huge computer infections risks because very often a single antivirus it does not matter who are its developers, fails to detect the newly created trojans. Using an online scan service like *virustotal.com* is a better alternative than scanning with a single antivirus because this service are using many antivirus engines but it has its limitation, it can scan files with maximum size of 32 MB and bad boys know it. What to do if a file is larger than 32 MB?

To be honest, the warez forums are not the only websites spreading infected software, a program downloaded legally from its established website can spy on your computer, can collect for statistics data about how you use your computer, what websites are you visiting or other private information, a behaviour which is perceived as a privacy threat by many users and even more, such programs are detected as malware by a few security programs.

If you deal with a suspicious program the simplest option is to use *virustotal.com* to scan the file– if the file is smaller than 32 MB of course and you have the advantage over your installed antivirus to see the results of many more antivirus engines, so a more accurate result.

The next thing you can do is to check the file(setup) properties, if a malevolent person embed a trojan into an installer, the digital signature will be missing. Also, a lot of "wannabe" hackers are neglectful when they build the new installers and add different strange things as *File Properties* or the file properties fields are missing completely.

Let's see how is looking the file properties of a modified installer–**easyHDR PRO, High Dynamic Range photo processing software**, found on a warez forum compared with the original setup file:

Installer with trojan contained

1. File version: 2.20.1.0
2. Description: Setup Application
3. Copyright: Setup Engine Copyright © 1992-2012
4. Comments: Created with….
5. Company: easyHDR PRO
6. Internal name: sf_rt
7. Original File name: suf_launch.exe
8. Product name: easyHDR PRO

And now the original installer:

1. File version: 2.20.1.0
2. Description: easyHDR PRO 2 installer
3. Copyright: (C) 2006-2012 Bartlomiej Okonek
4. Company: SIMPARTEK – Bartlomiej Okonek

You can see the differences, the *so-called* hacker was simply too lazy to add the proper file properties when he was building his infected installer. Even the icons were different.

The next thing you can check is the file hashes, the original has **MD5 0FA5244E5F9606AAA10070002AB1B7C8** and the infected installer **MD5 8B78190E81E32C46C94B7C34A9B3C81E**. The file hashes are of a great help for quick file analysis, a free tool called *HashTab* used for calculating them is found at:

http://implbits.com/HashTab.aspx

This tool add an entry to the context menu(right-click menu) and the result hashes can be used to compare files or to verify file integrity and authenticity. Or you can google for hashes, some online security services use the hashes to determine if a file was previously detected as malware.

What about scanning this file at virustotal.com? Well, not laudable results:

https://www.virustotal.com/file/ac60202365b59b05d6eb04cfe00f301cb9801e119495bc72ff127c5070194485/analysis/1334599798/

Detection ratio: 5 / 42, a lot of big names antiviruses fail to detect it, grrrrr, is not good for you if it happens to use one of them.

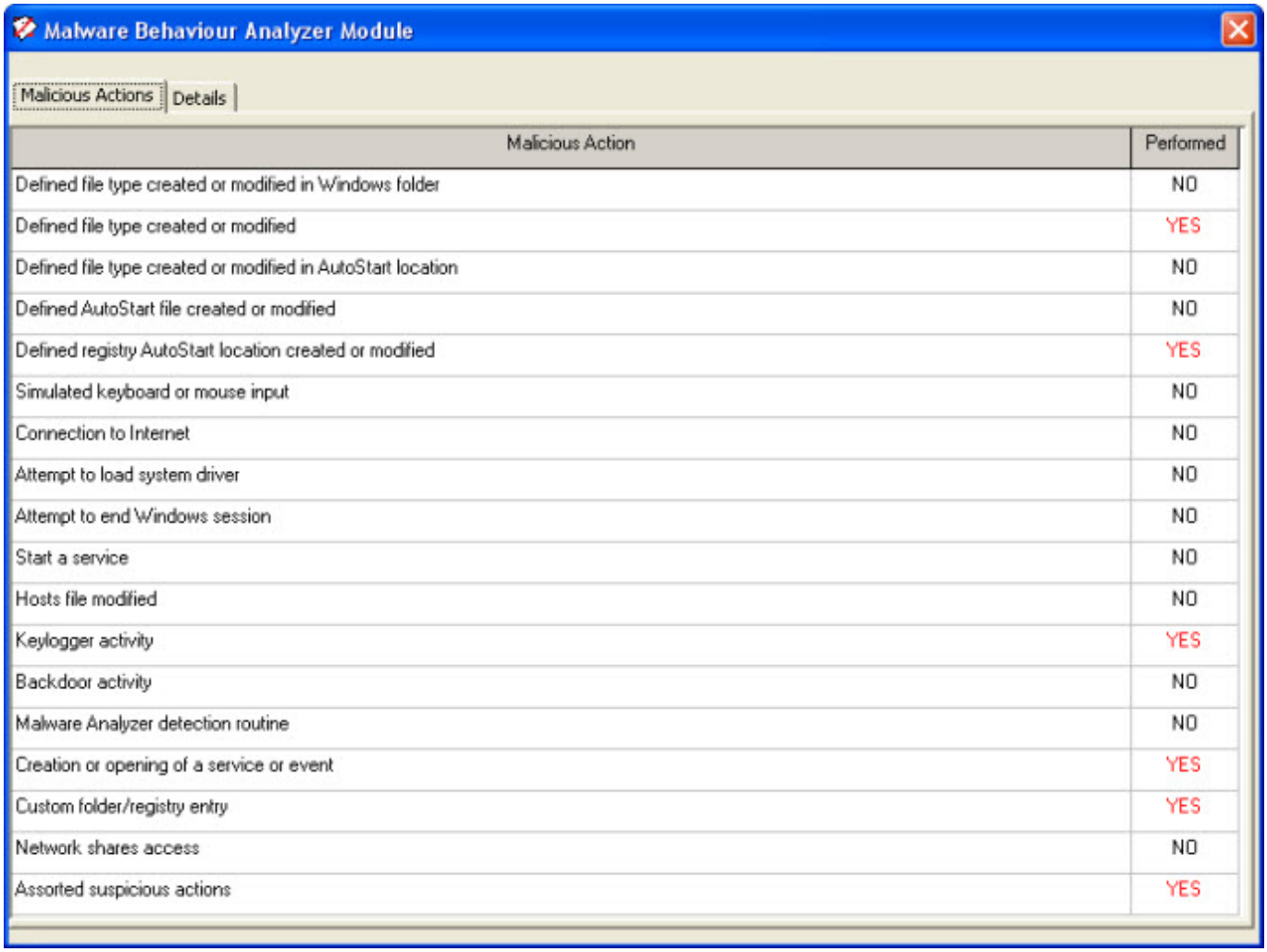
You can try also to extract the files from inside an installer using a tool like *Uniextract* and view them, but you need some experience to recognize a trojan file.

In my opinion, the best option to decide about an executable, is to run it in a virtual environment like a “sandbox” and to monitor its actions, what it does. You don’t need a virtual machine for this, *Sandboxie* accompanied by *Buster Sandboxie Analyzer*(BSA) module is one of the most powerful and convenient sandboxing tool. Sandboxie because a presumed infected program can not perform permanent changes to your system and BSA because it offers detailed information about the analyzed program behaviour and even it tries to decide whether it is malicious or not. Of course, these combination can be used also on “legitimate” but dubious software, not only on those provided by warez forums.

Now let’s see our infected setup file running in a sandbox.

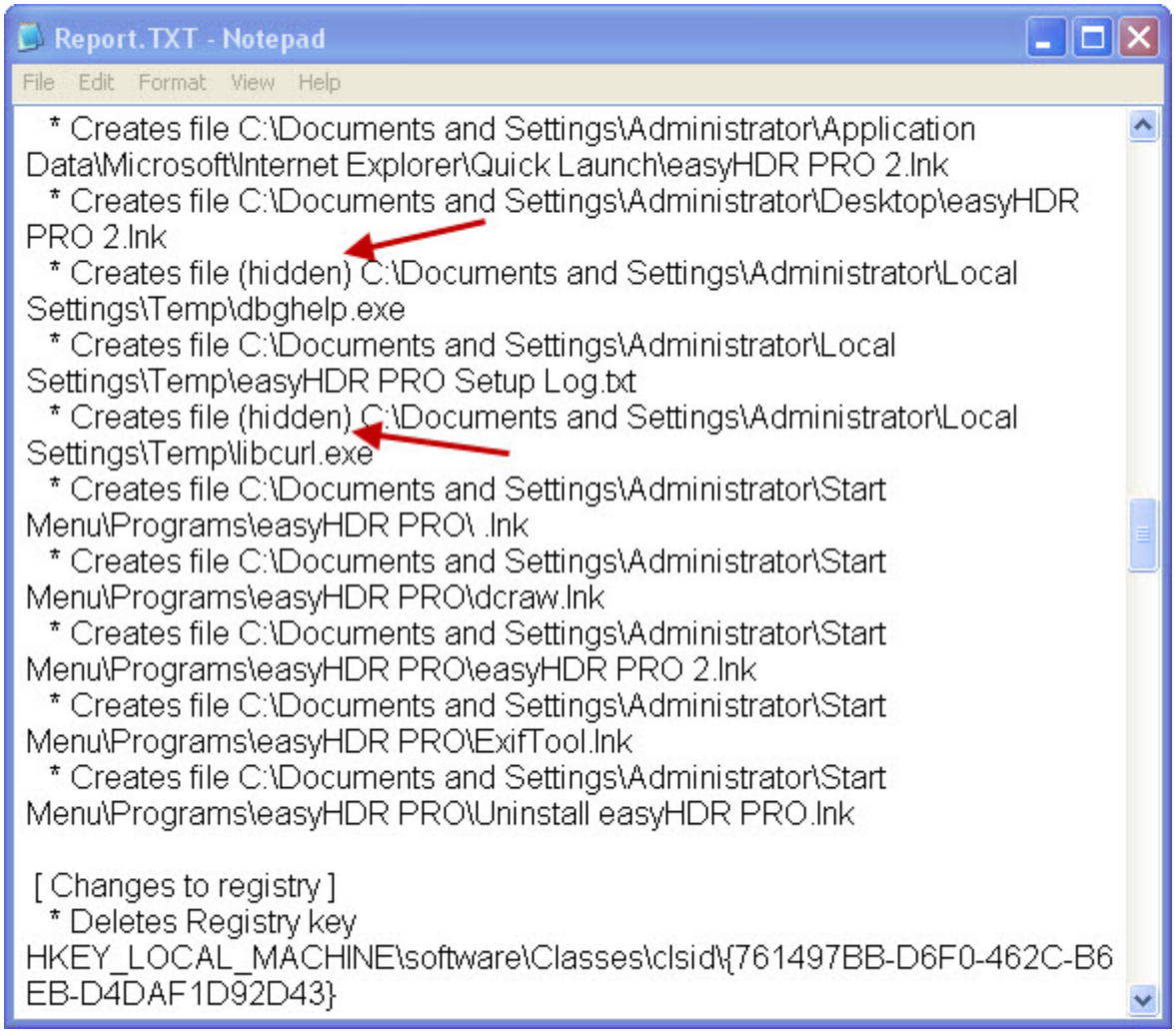
First of all, we can notice in *Malware Behaviour Analyzer(BSA)* three factors of risk, enough to make an idea for yourself about this analyzed program:

1. An autostart registry entry created
2. Keylogger activity
3. Assorted suspicious actions



malware behaviour analyzer

The read of the report reveals the creation of two hidden files in *Temporary directory*, or there is not reason for this other than to hide the files from user so we can guess these are malware files:



report hidden files

These two suspicious files are:

1. *dbghelp.exe* MD5 1A9E6ACF61D24E829059F5595EDAB9BF
2. *libcurl.exe* MD5 15E63AA1A22AFA8481D3DE1DC34F039B

The first one, *dbghelp.exe* is detected as *Trojan.Generic*(13/42 detection ratio) at www.virustotal.com, see report and the second one, *libcurl.exe* is detected as *Win32/Fignotok.A Trojan*(32/41 detection ratio) see report.

However, remember that the setup which included these two trojans and the original **easyHDR PRO** program, has a poor detection ratio of 5/42, that's because it was compressed and packed especially to avoid the antivirus detection. The unsuspecting user can run the infected installation and the appearances are ok because the wanted program installs as expected, what the user does not know is what happens behind the scene: he just won two computer trojans as a bonus.

Keep safe !

Share this:

- Share