

Are You Infected? Detecting Malware Infection

Jong Purisima 2003-02-13

The day starts normally. You wake up, drive to work, go to your desk, turn on your computer, take a sip from your coffee, and proceed to check your email. Reminders here, spam there, pictures here, stories there, a couple of games, and some animation. Classify your mail: work related here, from friends, families and acquaintances there. Then you take your morning break.

Break is over so you get back to your computer and suddenly notice that it is busy with something you are not aware of. So you decide to close all applications, one at a time, and try to figure out what is going on. Then you notice that closing applications is slower than usual.

You get nervous and then think that it is best to restart your system. Perhaps restarting would bring things back to normal. As your computer boots up, nothing seems to have changed. You log on to it and then find that everything *is* back to normal. Tension naturally eases up but then you ask yourself, "What could have caused the earlier malfunction? Is my computer infected?"

When users suspect that a malware has caused a system problem, they are usually wrong nine out of ten times. There are a lot of reasons for a system to malfunction. It is always assumed, however, that a malfunction is caused by something external to a system, something that has the intention and the effect of disrupting the normal system operation, something that is related to a virus or malware. Most of the time, however, the cause of a malfunction is not in any way related to malware.

Discussing all causes of system malfunction is not easy due to the diversity of systems in terms of hardware, software, firmware, and other configurations. The end of a discussion about one system usually opens discussions about other systems. It is then reasonable that we discuss here how a malware causes systems to malfunction. Once in a while, malware tends to introduce technological innovations but the approaches and concepts remain the same.

Malware Strategy and Tactics

It is only apt to discuss the strategy of a malware. First, a malware causes unusual behavior on a system. It may have been designed to propagate, as in the case of viruses, or to inflict havoc or damage on a system, which is what trojans actually do. Other types of malware such as

droppers introduce other malware to systems. Virus kits generate malware for other malicious purposes on a system.

So, what are some of the tactics that various malware employ. Malware is designed to execute on a system. For this to happen, the malware is often packaged in interesting forms such as games, cool animation, and often as pornographic movies or images. Since it cannot get onto a system without user intervention, it uses any means necessary to fool the victim end user into executing its file on their system. Most of the safe computing tips suggest that any new file or attachment should always be scanned before it is executed or opened.

Once executed, malware can perform its intended malicious function on a system. Unfortunately, it may not always be apparent to users that their system is indeed infected. The remainder of this article will discuss how to determine whether or not the system has been infected and will offer some tips on to manually disinfect the system.

Memory Residency

Memory-resident programs are those that can be placed in, and remain in, an affected system's main memory space after execution. Memory residency enables a piece of malware to be readily available whenever needed, ensuring that the malware is easily accessible or can monitor every event on an affected system. This is a malware's way of controlling every activity on an affected system when a condition is satisfied.

To find out if a malware is resident in the memory, you may need to invoke system tools like the Task Manager in Windows NT-based systems. On Windows 95- or 98-based systems, you can press CTRL-ALT-DEL, which displays a window containing all the running processes in memory. Once you have full view of the things that are currently in memory, check if a malware is there or not.

This is tricky and at the same time risky. Terminating a memory-resident program that is critical to a system may cause some undesirable results, such as displaying the Blue Screen of Death or even triggering the system to restart. It is advisable to check if a specific memory-resident program is indeed alien to the system, which is not an easy task. You can either consult your operating system manual or search for that program in an Internet search engine. If the search returns no results or does not indicate a relation to any recent malware, it is best that you leave it alone. This is rather too risky to tinker with but may be used for checking if

worst comes to worst.

Spoofed Process Names

Contemporary malware tends to use process names that look strikingly similar to common process names. It's more like spoofing them into a name that you might think is the real thing but it's not. For example, `WSOCK32.DLL`, a common process in memory handling the library of socket functions, can be spoofed as `WSOCK33.DLL`. Another is `KERNE132.dll` (notice that the L in `KERNEL` is actually the number 1) can be mistaken for the real `KERNEL32.DLL`. Sometimes the names are actually valid but the path is different. The `KERNEL32.DLL` is always found in the `\Windows\System32` directory but some malware puts it in `\Windows\System`.

There are other things you can do to check for infection. For example, you can check if a recently executed and supposedly terminated program is still in memory when it should not be. Another indication is when a program appears to have multiple copies of itself in memory even if no application with that name is currently.

Lastly, if upon closing all applications and checking the memory usage of a certain entry in memory, it is using up almost all the memory resources you may have to check it out. This is particularly true if there is no indication that there is a memory activity for that entry. The memory space may be deemed safe by just viewing but, tinkering with it, like terminating entries, may produce unwanted results. However, if you find out that certain malware is indeed on your system after verifying with the AV vendors' reports, you can terminate the malware in memory and proceed to find out what other things it has added or modified on your system.

Gaining Control

Before a malware becomes memory-resident, it needs to be executed first, as mentioned previously. The initial execution, a user executing the file, is only the first step. Malware often employs other techniques to make sure that it is executed at least once in every system session. It does this by putting links to itself in places where the system initializes or pre-configures the Operating System. These are places or configuration files where it is accessed by an Operating System upon startup. For a malware, it is rather important for it to be executed every time and to advocate its aim to be memory resident. What better way to be executed, or to be triggered to reside in memory, than to be executed upon computer startup.

There are plenty of places where a malware can use this technique. One of the earliest techniques used was to infect the Command Interpreter, more commonly known as `command.com`. Upon infecting this file, the malware can assure that it gets executed and can reside in memory even before the command interpreter is executed. A malware can also try to accomplish this by adding links to itself in the `autoexec.bat` or `config.sys`, which are configuration files used by DOS and even Windows systems on its basic start up scheme.

Registries

Contemporary malware has found new ways to position itself on a system and ensure its execution. One way is by adding or modifying Registry entries. The Registry is a repository of system configuration settings and includes links to applications that need to be executed once the system has been established. This is a good place for malware to exploit and this is what we will look at.

To access the registry, click "Start" then "Run" and then type "Regedit" beside the "Open:" box. This opens the Registry editor. A word of caution, similar to terminating processes in memory, modifying or deleting registry entries can lead to unwanted system problems. Since the registry is the repository of configuration settings, a minor change here can cause your system to not start or boot up properly or sometimes render some applications to be unusable. It is recommended that you follow these instructions with care.

In the registry editor, you will see that registry keys are organized similarly to the File/Folder structure. The location, `\HKEY_LOCAL_MACHINE\ SOFTWARE\ Microsoft\ Windows \CurrentVersion`, contains 3-6 folders that are part of the Autostart Registries as follows:

```
"Run "  
"RunOnce "  
"RunOnce\Setup "  
"RunOnceEx "  
"RunServices "  
"RunServicesOnce "
```

The applications in these folders are what Windows executes immediately after a system is started up. Another similar location and privilege that may contain these 3-6 Autostart registries are in `\HKEY_CURRENT_USER\ Software\ Microsoft\ Windows\ CurrentVersion`

You may have to check and familiarize yourself with each entry. The total number of entries is different for every system and is often proportional to the number of system tray entries that you have. The system tray is usually located at the lower right section of the Windows desktop and contains small icons beside the clock.

These applications are usually Windows-based executable files that have an .EXE extension, and are thus assumed that these have File Properties just as typical Windows executables do. You may check each file that is associated in the AutoRun Registry by opening a File Manager (also known as Windows Explorer) to view the file properties of each entry. To do this, right-click the files, choose "Properties", and then check out the entries in the "Version" tab of each file. The "Company" and "Product Version" often tell you a lot about the file. Registry entries in these locations without the full path are located in the Windows Directory, Windows\System, or Windows\System32 Directory. Keep in mind that some malware sets the Hidden file attribute on files it drops on the system. If this is the case, you will have to set Windows Explorer to show hidden files (Tools->Folder Options, click the View tab, then select the Show hidden files and folders radio button).

If the folders contain unusual entries such as misspelled company names or grammatical errors, then this should give you more reason to investigate that application. Check out some manuals or refer to search engines. If these files are verified as being malicious, then you can start removing their links. Let me remind you again that removing critical entries, by mistake, in the registry produces undesirable results. It is important that you thoroughly examine and verify that the links you will remove from your system are links to a malware file.

Another way for a malware to gain control of systems is by modifying the association of commonly used file extensions. Windows is typically file extension-based and uses the HKEY_CLASSES_ROOT entries to determine which applications or programs to run for certain extensions. .EXE, .DLL, .COM, and other readily infectable files are commonly modified. These entries or registry keys are often not associated with programs and indicate internal system commands or contain the appropriate applications typically associated with it.

It is also advisable to back up a registry entry first by exporting its registry key to a file. To do this, right click the folder-like entry in the registry and then select "Export". Agree when prompted to save it to a file. After creating a backup, you can now delete or modify the registry key. If you find that what you deleted is a normal entry and not that of a malware, restore it from your backup.

Other StartUp locations

Other areas where AutoStart entries can be found are in the files, System.ini and Win.ini. A malware often modifies these with links to itself added to the "run=" or "load=" sections of the files. These files are located at the Windows Directory (typically C:\Windows).

Following the same approach that you followed with the registry entries, you can remove them from the AutoStart entries after you have verified that they are malicious. Again, back up these files before making any modification just in case the entries are not malicious and you have to restore the files to their original form.

All the necessary system configuration files can be accessed, viewed and edited with the Sysedit program. To invoke the program, click "Start", and then "Run", and then type "Sysedit" in the "Open:" box.

Another place where you can find autostart entries are in the Start > (All) Programs > Startup folder. The entries here are also referenced and are executed immediately after system startup. Similarly, you may need to back up these files before tinkering with them.

Macros

Applications like word processing, spreadsheets or PowerPoint presentations are often vulnerable to macro viruses. You can check for malicious activities by checking for macros within these files. To do this, access the macros organizer (you may refer to your applications help file) and check if there are any unknown macros inside, press the ALT-F11 keys in the more recent offerings of Microsoft Office Family (beginning in Office 97 and up). However, some macro viruses tend to hide themselves from users by changing the foreground/background of the macro font display or by adding multiple tabs to make the text invisible to the default view pane.

The following is an explanation of procedures readers can use for two different applications that use macros: MS Word and Excel.

MS Word

Search your hard drive for any file named NORMAL.DOT, which is the global template of this application. Rename it to make sure that you have a backup and this will trigger Word to recreate a new NORMAL.DOT and the assurance that it is clean of any macro viruses. Open Microsoft Word and then turn on the Macro Virus Protection. After which, you may now try and open the file that you suspect has a macro virus. If there are any macros inside these files, you will be prompted by the Macro Virus Protection. It may also help if you can jot down the file size of the NORMAL.DOT so that in the future, you can just refer to this size in comparing it with the existing global template. This way you can easily spot the difference.

MS Excel

Search your hard drive for any folder name XLStart. For Excel, this folder contains all the things necessary for customization and this includes macros as well. You can transfer the contents of this folder to a temporary directory. Open Excel and turn on the Macro Virus Protection. After doing so, you can now open the Excel file that may be infected and then the Macro Virus Protection should be able to figure that out for you.

So What Now?

Now that you have removed the link to the suspects, you can send your suspected file to your preferred Antivirus Vendor for analysis. You may send it via email and attach the suspected file in a password-protected zip file (don't forget to include the password in the mail so that the zip file can be extracted and analyzed). The vendor's response usually takes a matter of days, depending on your subscription. You can do the same to the files that you have seen in memory and fear to be malicious.

If after reading this article twice, you still cannot comprehend what has been discussed or is not willing to risk your system to be broken by the modifications suggested, it may be better for you to use an Antivirus software and allow that software to check your system for malicious codes or programs.

The best ways to keep your system from infection are found in safe computing guides that are available on most AV Vendors' Web sites. These discussions include the basic things you must do to minimize the risk of being infected. Not only are these helpful, they are also a good venue for you to know more about your system and making you a better citizen of Cyberspace.

[Privacy Statement](#)

Copyright 2006, SecurityFocus