Asian Journal of Computer and Information Systems (ISSN: 2321 – 5658)
Volume 04– Issue 03, June 2016

Integrating Manual Prevention Techniques with Automated Countermeasures for Effectively Averting Malware

Muhammad Tariq

Head of Section for Networking/Internet & E-Security
Department of IT, Nizwa College of Technology, Nizwa, Oman
Email: mtariqpk [AT] hotmail.com

ABSTRACT— ***In today's world, computer viruses and other forms of malware are among the biggest of the nightmares that haunt information security experts, not to mention a layman. Antivirus programs are the most common, if not the only, relied upon solution available to deal with malware. Different types of antivirus programs offered by multi-billion dollar antivirus industry, signature-based, heuristic-based and hybrid, are still a long way from meeting the expected level of contribution. Significant performance deterioration is also a major downside of antivirus programs. This paper discusses various manual techniques that can be exercised in combination with existing automated countermeasures in order to help in effectively preventing malware with improved performance. The scope of this paper is limited to Microsoft Windows family of operating systems.***

Keywords— Malware, Virus, Worm, Trojan horse, Antivirus

1. INTRODUCTION

The term malware is used to generally refer to a broad category of malicious codes including, viruses, worms, Trojan horses, backdoors, spywares, ad-wares etc. A virus is a self-propagating malicious program that cannot function independently. It needs a host to function to which the virus attaches itself with, like any type of files or programs. A virus is usually spread by sending the infected file or program to other systems in any possible way, like through removable media or as an email attachment. When executed, a virus may damage your hardware, software or data[1].

A worm is an independent self-replicating program that doesn't rely on other executable codes. This stand-alone malicious code is capable of establishing active connections with other systems over the network and transmitting huge no. of copies of itself. A worm takes advantage of vulnerabilities in systems or file/information transport features on a system, which allows it to travel without human aid. The goal of a worm is generally to consume precious computer and network resources including processing power and bandwidth [2,3]. Worms generally do not damage programs or data but there have been some instances of malicious programs in the history which elicited properties of both viruses and worms, e.g. malisia [1].

A Trojan horse is a malicious program that purports to be harmless but surreptitiously performs some malicious function. Unlike viruses or worms, Trojan horses do not propagate from one system to another. Generally, Trojan horses are used for acquiring sensitive information, like passwords, credit card numbers etc. by recording keystrokes.

Backdoors, also termed as trapdoors, are malicious codes that allow an attacker to quickly gain access to a system with great ease [1][2]. Several malicious software combine the functionality of Trojan horses and backdoors in a single package, e.g. beast, sub7 etc. "A blended threat is a more sophisticated attack that bundles some of the worst aspects of viruses, worms, Trojan horses and malicious code into one single threat. Characteristics of blended threats are that they cause harm to the infected system or network, they propagates using multiple methods, the attack can come from multiple points, and blended threats also exploit vulnerabilities"[3].

All these malicious codes are mainly differentiated from each other based upon their purpose, functionality and scope. Over the time, the boundaries of distinction among each of these aforementioned malicious programs have become vague to some extent but still these terminologies are frequently used to address each of them specifically. As their way of working and goal differs, so do the techniques to prevent, detect and recover from each of them. This paper does not addresses specific techniques to deal with each unique type of malware, rather describes a set of manual practices that could be exercised for averting malware. All the malware prevention methods discussed in this paper apply to MS Windows 7 and all the later flavors of MS Windows operating systems including the Server systems.

2. BACKGROUND

An antivirus program is the most commonly employed countermeasure to prevent, detect and remove malware from a system. Antivirus programs are mainly categorized in two types based on their way of working. A signature-based antivirus relies on an inbuilt database that contains virus definition files. Each virus definition file contains virus signatures and characteristics of a specific, already discovered, malicious program. The signature-based antivirus program works by comparing the characteristics and signatures defined in each virus definition file with every file in a system to identify the malicious programs. The database containing virus definition files needs to be frequently updated in order to receive the latest definition files for newly discovered malware. Heuristic-based antivirus programs are the second type. A heuristic-based antivirus relies on several techniques, mainly observing the characteristics and behaviour of programs and files, to detect suspicious activity[6]. Most of the antivirus programs rely on signature-based detection. Even the ones offering a hybrid solution mainly employ signature-based detection with limited heuristic-based features.

Both aforementioned types of antivirus programs suffer from several shortcomings. Principally, a signature-based antivirus cannot detect a zero-day-attack or the malware whose corresponding definition file is not present in the database. Heuristic-based antivirus programs are just too far from being mature enough to be solely relied upon. In terms of performance, signature-based detection is very processor-intensive, whereas heuristic-based are even worse.

A host-based firewall is a software program that filters incoming and outgoing traffic in a system. A firewall principally works by comparing the source and destination IP addresses of inbound or outbound traffic with a pre-specified set of rules[9]. Since a firewall doesn't have a signature database like an antivirus program and it doesn't monitor application layer data, it cannot protect a system from incoming viruses or Trojan horses. However, a firewall does offer a limited ability to thwart worms trying to establish connections from or to a system from the external network.

The, not very commonly used, host-based intrusion detection/prevention systems function the same way as a firewall, but also contain a signature database. They are able to detect/prevent a broad range of attacks, including malware to some extent. These systems offer a limited ability to filter the malware trying to attack our devices over a network, but not against other sources like USB-drive, CD/DVD's etc[8].

The, even much lesser utilized, honeypot programs are used by professional security experts to attract the attackers towards a system in an attempt to learn the methods used by them in order to develop approaches to thwart them[7]. Honeypots are far from being a practical solution to malware for a common user.

3. MANUAL MALWARE PREVENTION TECHNIQUES

The previous section discusses several currently utilized automated countermeasures that may be used to handle malware. Antivirus programs clearly dominate in terms of relevance and practicability in implementation against malware, along with a firewall to some extent. The previous section also identifies the limitations of available solutions and the need to fill the gap in security against malware.

This section describes various manual approaches that can be used, or integrated with existing automated solutions, to strengthen the defence against malware.

3.1 Hiding and Execution Methods Used by Malware

One of the most common sources of malware is removable media including USB-drives, CD/DVDs etc. Other common sources include WWW, email attachments, macros attached with MS Office documents etc.

It is important to note that a malicious program present in a hard drive, removable USB-drive, CD/DVD or elsewhere cannot perform the associated malicious function unless it, or the file it is attached with, gets executed. Among many possible examples, following are two ways commonly used by malicious programs to hide themselves and get executed in CD/DVDs and USB-disks.

1) Autorun.inf

Autorun.inf is a text-based configuration file that is mostly present in the root directory of a CD/DVD or USB-drive. MS Windows OS's look for this file to see which program to automatically execute when the media is connected[4]. Most of the malware take advantage of autorun.inf to get executed, either when the USB/CD is inserted or when the user double-clicks to open the drive. The malware is located somewhere in the drive, generally in a hidden folder, and the path of that malware is present in 'autorun.inf'[5]. This is one of the most common methods employed by malware to spread infections in MS Windows based systems.

2) Benign icons and filenames

Many malicious codes hide themselves in USB-disks and CD/DVD's by using a 'folder icon' and use the name of some other folder already present in that drive. Frequently, malicious program hides the folder whose name is used by it. These malicious programs also hide the extensions of all the files in the drive in order to hide their own extension. The purpose is to appear as a folder belonging to the user, making the user unintentionally double-click and execute the malicious program. When executed, the malicious program often opens the hidden folder by itself that the user intended, in order to maintain stealth. It has also been observed that when CD's or USB-drives are infected, sometimes you'll see a 'folder icon' instead of a regular 'drive icon' used by MS Windows OS. If you observe this, you can almost be sure that your drive is infected.

3.2 Preventing Malware from Execution

Follow the instructions below to safely access your content from infected USB-drives, CD/DVD's and hard drives. However, it is important to mention that following these steps is of no use in an already infected system. In this case, detection and recovery procedures must be executed first to remove the infection from the system.

1. In order to prevent against the threat of infected Autorun.inf files, never double-click or right-click any root drive. Instead get all the root drives listed in the left-pan in MS Windows' 'My Computer' section (In Windows XP, this can be achieved by clicking the 'Folders' button in the top bar of Windows Explorer. Available by default in Windows 7/Vista/8/10). Select (single left-click) the intended drive in the left-pan to browse the drive contents in the right-pan. This ensures bypassing of Autorun.inf file.

2. Once inside the root drive, verify that file extensions are visible and hidden folders are showing. Check/uncheck the associated checkboxes from Windows Explorer path "Tools -> Folder Options -> View" in order to fulfill these requirements.

3. If System or Hidden attributes are set for any files/folders in your drive, you may still not be able to see them in your drive, even if you've correctly followed the previous step. In order to view them, un-set the Read-only, Hidden and System attributes of all the files, folders and sub-folders by executing the 'ATTRIB' command once in DOS Command Prompt program with switches '-s', '-h', '-r', '/D' and '/S'. All the files and folders should now be visible.

4. If you see Autorun.inf and other strange files, especially with exe, com, bat, vbs or pif extensions, delete them unless you specifically recognize them as trusted files. If you see any files with any extension but icons similar to the 'folder icon', delete them. Folders do not have any extension. In an infected system, you may still not be able to see the extensions of your files in the drive you are currently browsing, as the malware in the memory might hide file extensions again as soon as you un-hided them. In this case, before double-clicking any folder, check the properties of that folder by right-clicking it. If you notice 'Application (.exe)', or anything else other than 'File Folder', in the 'Type of File' field, what you are assuming to be a folder is not actually a folder, delete it immediately.

5. Rule of thumb – keep the curiosity under control. It is as dangerous for a computer, as it is for a cat. If you intend to access content from your own USB-drive, most likely you recognize your content as well. Restrain your curiosity about any suspicious files (especially with dangerous extensions like exe, com, bat, vbs, pif etc.) you see in your drive and delete them before your system pays the price.

6. Alternate Method: Create a simple text file on your desktop and write the command 'del H:\*.inf /F /S /Q' inside (considering that 'H' is the drive letter assigned to your USB-drive when it is connected to the system. Change the Drive letter accordingly). Now change the extension of this file from .txt to .bat. Execute this batch file before accessing your USB-drive to automatically remove the autorun.inf file from your USB-drive. Safely remove your drive and connect it back again. Keeping in mind the 'rule of thumb', feel free to browse and even directly open your USB-drive by double-clicking.

3.3 Other Manual Prevention Techniques

1. Keep the operating system up-to-date. Make sure that 'Automatic Updates' are enabled and the system is automatically downloading latest security patches and services packs when it is connected to the Internet. This automatic online maintenance ensures that all known vulnerabilities are regularly fixed in the system.

2. Uninstall all unnecessary programs. They may not only deteriorate system performance, instead also make the system insecure by offering vulnerabilities to be exploited by malware.

3. Disable unnecessary services and startup programs. Unnecessary services not only deteriorate system's performance by consuming system's memory, rather also make the system more vulnerable by offering holes to be exploited by the attackers. The most convenient way to do this is to access the System Configuration utility in MS Windows 7 by typing 'msconfig' command in the run menu. Under the 'Services' Tab, check the checkbox stating 'Hide all Microsoft Services' and then uncheck all the unnecessary services. Observe the service name and manufacturer to take the decision. Even if you uncheck all of these services, after checking the 'Hide all Microsoft Services' checkbox, your system would still boot and function properly. If any program, like antivirus, creates any issue later, you may repeat the procedure to start the respective service again. A more comprehensive and better approach would be to disable unnecessary OS services also, which can be done by accessing 'Services Console' through 'Administrative Tools' in the control panel. Similarly, for disabling unnecessary startup programs, use the 'Startup' Tab in the System Configuration utility.

4. Ensure that the default Windows Firewall, or any other host-based firewall, is enabled for prevention against worms.

5. Disable Macros in MS office documents.

6. Frequently observe the startup folders of all the user accounts, specifically the default user, in your system to identify any malware present in your system. Any file/program placed in a startup folder gets automatically executed at system startup when the associated user logins into his account. Startup folders are one of the most common places exploited by malware to get executed on system startup. Following is the path to the startup folder of the default user.

   (Root):\Users\Default\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup (Windows 7 and Vista)

   (Root):\Documents and Settings\All Users\Start Menu\Programs\Startup (Versions prior to Vista)

   Where 'Root' refers to the hard disk partition in which OS is installed.

7. Frequently observe the startup folders in Windows Registry and remove malicious entries. Execute 'regedit' command in run menu to access Windows Registry editor and observe the following paths.

   H_K_L_M\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
   H_K_L_M\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
   H_K_L_M\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
   H_K_L_M\Microsoft\Windows\CurrentVersion\RunServices
   H_K_L_M\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
   H_K_C_U\Software\Microsoft\Windows\CurrentVersion\Run
   H_K_C_U\Software\Microsoft\Windows\CurrentVersion\Runonce

8. In order to prevent against email infections, refer to the rule of thumb discussed previously. Refrain from downloading any attachment with dangerous file extensions or coming from some unknown source.

9. For prevention over the WWW, keep the anti-phishing software enabled in your browser/ system. Refrain from unnecessarily clicking any tempting banners/links on doubtful websites or downloading suspicious stuff. If available, verify the hashes/digital signatures of files before downloading. Disable 'automatic execution of unsigned ActiveX Controls and Applets' in your web browser and set the security level of your browser to high.

3.4 Advance Prevention Approaches

1. Execute a suspicious program in a 'Sand Box' (virtual machine) and observe, before executing it in your system. Sometimes, viewing the Hex Dump of a file also helps in identifying whether it is malicious or not.

2. Enable 'System Restore', especially for the OS partition. In case of observing any suspicious events in the system, try restoring your system to a back-date, when the system was fine. If the malware prevents you from accessing System Restore, perform a 'Clean Boot' using 'System Configuration' Console (msconfig) and try accessing System Restore utility in 'Safe Mode'.

3. Many malicious programs replace legitimate DLL files of core OS processes (e.g. svchost.exe, smss.exe, crss.exe, winlogon.exe, lsass.exe etc). Using the signature verification utility, frequently verify the signatures of programs and DLL files in Windows directory (and all sub-directories) and observe unverified and unsigned files. The signature verification utility can be accessed by executing 'sigverif' command in the run menu, in all the versions of MS Windows.

4. Frequently observe open ports of your system using third party utilities (like Diamond CS Port Explorer) for identifying any Trojan horses or Worms in your system. Remove the associated programs if malicious ports are

identified.

5. Frequently observe running processes using Task Manager or any third party utility (like Process XP) for identifying any malicious processes. Observe the path of suspicious processes. Take help of a search engine for identifying the purpose and nature of suspicious processes.

6. Use the Autoruns utility (third-party) provided by Sysinternals to identify the DLL’s and processes loaded at startup. Also use this utility for signature verification of all the files loaded at system startup.

4. CONCLUSION & FUTURE EXTENSIONS

This paper discusses existing automated countermeasures and several manual techniques that can be integrated to strengthen the defense against malware. The described manual approaches for malware prevention will not only significantly enhance the security of the system, rather also result in significant performance enhancement. Disabling of lesser important processor-intensive modules of antivirus program may also be considered for further performance enhancement. This paper mainly presented manual techniques for prevention only. Manual detection and recovery measures present the scope for future extension.

5. REFERENCES

[1] J. E. Canavan, Fundamentals of Network Security, Library of Congress Cataloging-in-Publication Data, Artech House, Boston London, 2001

[2] John Aycock, Advances in Information Security, Computer Viruses and Malware, Springer, 2006

[3] Vangie Beal. (2010) The Difference between a Computer Virus, Worm and Trojan Horse. [Online]. Available: http://www.webopedia.com /DidYouKnow/internet/2004/virus.asp

[4] (2012) Autorun.inf: Structure and Making. [Online]. Available: http://www.autoruntools.com/autorun-inf.php

[5] Mikko. (2009). When is Autorun.info Really an Autorun.inf?. [Online]. Availble: http://www.f-secure.com/weblog/archives/00001575.html

[6] (2012) Antivirus. [Online]. Available: http://www.scribd.com/doc/47040815/Antivirus

[7] M. T. Qassrawi, “Client Honeypots: Approaches and Challenges, New Trends in Information Science and Service Science (NISS)”, in IEEE Conference Publications, Gyeongju, China,, PP. 19-25, 2010

[8] L. Ying, Z. Yan, O. Yang-gia, “The Design and Implementation of Host-based Intrusion Detection System”, in Third International Symposium on Intelligent Information Technology and Security Informatics (IITSI), IEEE Conference Publications, pp. 595-598, April 2010

[9] (2011). Firewalls. [Online]. Available: http://www.vicomsoft.com
/learning-center/firewalls/