Analysis of AutoPlay Feature via the USB Flash Drives

Ruhma Tahir, Zara Hamid and Hasan Tahir

***Abstract*—USB flash worms represent a persistent threat to the growing Internet in an increasingly networked world. However, their evolution has been somewhat limited and they still rely on the same basic paradigms, which contain fundamental laws. This paper analyzes the Autoplay vulnerability commonly exploited by flash worms to infect removable drives and further applies this analysis to the OpenWith worm found in flash drives. Preventive measures which need to be employed to restrict flash worms and techniques for removing these worms have been discussed in this paper.**

***Index Terms*—Autoplay, Computer Forensics, Flash drive worms.**

I. Introduction

The security landscape is shifting from large and widespread outbreaks to quiet threats. Computer viruses pose a serious threat to computer and network security. Fighting computer viruses is a critical but daunting task. The potential for damage from computer viruses and worms has increased in direct relationship to the importance of legitimate software in our lives.

Traditionally, all forms of viruses and worms were solely introduced via rogue executables downloaded off the Internet, but now these can also be introduced via removable devices. USB flash drives have become vastly popular during recent times. Almost everyone, now-a-days, possesses one of these magic sticks. Ease of use, good performance and large capacity have made the flash drives a must for the individuals. Though USB flash drives are gaining much popularity, but they could cause serious security breaches ranging from some malware sneaking into a PC and screwing a computer to destroying your important data.

Various security incidents indicate the advent of new worms that propagate via USB flash memory devices. These worms are seen to search for removable drives on a computer and then make copies of itself on these devices. Once the drive is connected to another computer these worms automatically install themselves on the new computer and repeat the exercise in an attempt to spread further. If an audio player, flash drive
or USB stick becomes infected; the user could plug it into the corporate network and unknowingly unleash a crippling virus.

USB flash drives have opened up new avenues to infect computer environments; as a result of which the virus writers have become keener to create USB flash drive viruses. Their newer creations are significantly more complex and difficult to detect and remove. As antivirus products improve and detect the latest and greatest viruses, the virus authors invent new and more devious ways to hide their progeny.

Keeping in mind the plus points, the other side of the picture is also grim. USB flash drives are vulnerable to *the OpenWith Virus* which attempts to spread by copying itself to removable storage drives and thus creating problems for the user in the form of not being able to access the contents of removable storage drive. This virus simply cannot be detected using traditional antivirus software.

In this paper, we analyze the commonly spreading OpenWith Virus through USB-flash drives and propose control strategies for preventing virus infections within the flash drives.

II. Worms and Viruses

A computer virus attaches itself to a program or files so as to spread from one computer to another, and leaves infections as it travels [1]. Some viruses cause only mild but annoying effects while others can damage the hardware, software or files. Almost all viruses are attached to an executable file, which means that the virus may exist on a computer but it cannot infect it unless the malicious program is run or opened.

A worm is similar to a virus by its design and is considered to be a sub-class of a virus. Worms spread from one computer to the other computer, but unlike a virus, it has the capability to travel by its own. A worm takes advantage of file or information transport features on a system, which allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on the system. So rather than a computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

A. Flash Drive Worms

The growing number of high capacity portable storage media devices poses a potentially huge security threat to individuals as well as to large organizations. Such devices bypass traditional safeguards and open the underlying systems to a range of threats because they remain invisible to normal perimeter-based security. Flash drives, which can transport

Manuscript received March 20, 2008.

R. T. Ruhma Tahir is with Department of Information Security, College of Signals, National University of Sciences and Technology (NUST), Lalkurti, Rawalpindi Cantt, Pakistan.(phone: 0092-051-2113672; fax: 0092-051-9257201; e-mail: ruhma@mcs.edu.pk)

Z. H. Zara Hamid is with the Department of Software Engineering, College of Signals, National University of Sciences and Technology (NUST), Lalkurti, Rawalpindi Cantt, Pakistan.(e-mail: xarahamid@yahoo.com)

H. T. Hasan Tahir is with the Computer Science and Engineering Department, Bahria Institute of Management and Computer Sciences, Shangrilla Road, E-8, Bahria University, Islamabad, Pakistan (e-mail: hasanmailbox@ yahoo.com).

very large quantities of data, pose a constant threat because of the fact that there is no way to control what is already on the devices when they are connected to the system or a network. Also it is not easy to control what is transferred onto them. A family of worms spreads by copying itself onto removable drives such as USB memory sticks, and then automatically running when the device is next connected to a computer. Consequently trojans, hacking tools, viruses, worms or malware infections simply walk in the door and bypass corporate security systems and procedures. A single infected file on a USB flash drive could cause large amounts of damage.

III. Autoplay Feature

Autoplay is the feature built into Windows that automatically runs a program specified by the file AutoRun.inf whenever a CD-ROM, DVD or USB drive is plugged into a Windows-based computer. Autoplay is intended as a convenience feature to automatically start an installer when removable media is inserted into a computer system.

Flash drive infections usually involve malware that loads an AutoRun.inf file into the root folder of all drives (internal, external, and removable) which automatically runs a malicious .exe file on the computer. When an infected USB flash drive is inserted, the trojan infects the system; if Autoplay has not been disabled.

Keeping Autoplay enabled on USB and other removable drives has become a security risk due to the increasing number of malware variants that can infect them. When removable media is inserted, system looks for AutoRun.inf which automatically can run a malicious .exe file.

There are a number of things which can be done with an AutoRun.inf file, and is a major vulnerability that the virus writers try to exploit.

A. *Openwith Worm*

The OpenWith worm might seem like a new tactic, but it's really an old hacker trick rehashed for a new generation. Evolution of computer viruses came into place by infecting files on floppy disks. The dispersion of these viruses was done when these floppy disks were taken from one PC to another. The same strategy is used by the OpenWith worm to infect the PCs of unsuspecting users via their flash drives. The OpenWith worm targets USB flash drives by creating a hidden file to ensure that a copy of the worm is run the next time the media is connected to a Windows PC. It also changes the open menu of USB flash drive to append garbage characters instead of the actual open options. This disables the user to open the contents of the flash drive.

The OpenWith worm takes advantage of windows Autoplay feature that automatically runs a program specified by the file AutoRun.inf whenever the USB drive is plugged into a Windows-based computer. The OpenWith worm loads an infected AutoRun.inf file into the root directory of the flash drive, which automatically runs the malicious code in the AutoRun.inf file on the computer. When a USB flash drive becomes infected, the trojan infects a system when the flash drive is inserted, if Autoplay feature of the flash drive has not been disabled.

IV. Computer Forensics

Computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law. Computer forensics activities commonly include [3]:

1. the secure collection of computer data
2. the identification of suspect data
3. the examination of suspect data to determine details such as origin and content
4. getting rid of the causes of the incident, vulnerabilities or the residue
5. post mortem analysis

The Figure 1 below illustrates the sequence of steps taken to study, examine and eradicate the OpenWith worm.

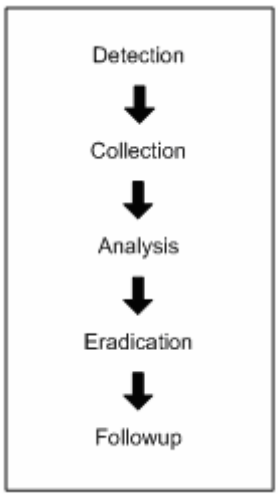

Figure 1. Incident Response Methodology

A. *Detection of Worm*

There are a few annoying changes in the normal functioning of flash drive, which lead to the detection of the worm.

A USB flash drive can be accesses by two ways – either by double-clicking or selecting ‘open’ from the open menu. The OpenWith worm disturbs the normal execution of USB access and results in the following problems.

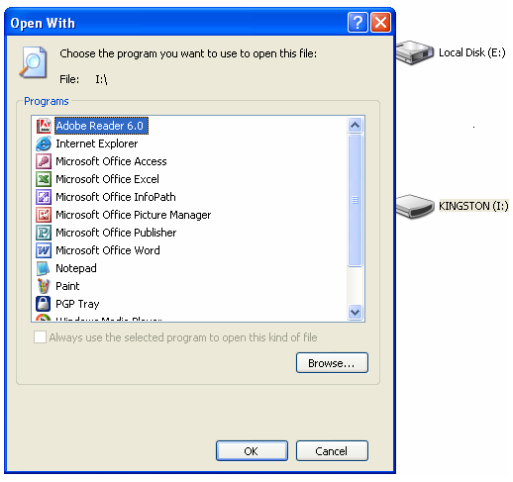

Figure 2. Infected OpenWith Dialog Box

The flash drive responds to a double click by opening an OpenWith dialog box, instead of opening the contents of the flash drive seen in example Figure 2 below, upon selecting Internet Explorer from the 'choose program options', it opens the contents of the flash drive, but the problem remains because 'Always run the selected program to open this kind of file' option/checkbox is disabled. As the result, whenever the flash drive is double-clicked an OpenWith dialog box repeatedly appears.

Selecting 'Open' or 'Explore' from the open menu, it opens the contents of the flash drive. The worm corrupts both the 'Open' and 'Explore' options by displaying garbage characters instead of actual options within the open menu. The corrupted open menu is shown in Figure 3.

Figure 3. Infected Open Menu

B. *Collection of Evidence*

The only visible evidence of the presence of a worm is the existence of Ravmon.exe file, which does not give any clue as to how the worm is working and infecting the opening of the flash drive.

Our next step is to search for the hidden files and operating system files, which could have been infected. Upon analysis an AutoRun.inf file is discovered, which is not present otherwise. The examination of the contents of AutoRun.inf file revealed the true cause of the annoying changes in open menu. The comparison of an infected AutoRun.inf file with an uninfected AutoRun.inf file leads us to the conclusion that this is the actual source of infection. The contents of the infected AutoRun.inf file are shown below.

```
[AutoRun]
open=RavMon.exe
shell\open=´ò¿ª(&O)
shell\open\Command=RavMon.exe
shell\explore=×ÊÔ´¹ÜÀíÆ÷(&X)
```

Figure 4. Infected AutoRun.inf file

C. *Analysis*

We performed an in-depth analysis of the infection by observing its response under various scenarios.

Scenario-1: Infected System and Uninfected Flash Drive

In this scenario the system is infected with Ravmon.exe file which exists in the C:\Windows folder of the system. As soon as a flash drive is plugged into the system, the Ravmon.exe file executes, replicates itself and creates an infected AutoRun.inf file into the flash drive. Ultimately the clean flash drive is infected with the worm when the flash drive is next plugged in and Chinese like characters appear on the open menu.

Scenario-2: Uninfected System and Infected Flash Drive

In this particular scenario, the system is clean, while the flash drive contains Ravmon.exe and infected AutoRun.inf file. The Autoplay feature is enabled in the flash drive and when the infected flash drive is plugged into the system, the AutoRun.inf file automatically executes thus running the Ravmon.exe file.

Upon execution, it creates a copy of itself into the windows system directory: %Windir%\RAVMON.EXE. It also creates a non-malicious RavMonLog file that contains the port number on which its backdoor component listens. The worm adds the following values to the registry to auto start itself when Windows starts, HKEY_LOCAL_MACHINE\ Software\Microsoft\Windows\CurrentVersion\Run"RavAV" =%Windir%\RAVMON.EXE [4].

The first command in the AutoRun.inf file executes the Ravmon.exe file, enabling Ravmon to replicate itself to the existing system. The second command changes the open option within the open menu to ò¿ª(&O). As part of their routine, many worms and trojans make changes to the registry. Some of them change one or more of the shell\open\command keys. If these keys are changed, the worm or trojan runs each time certain files are run. In this case Ravmon. exe will run each time AutoRun.inf is run [5]. The fourth command changes the Explore option within the open menu to ×ÊÔ´¹ÜÀíÆ÷(&X).

Scenario-3: Recovered System and Recovered Flash Drive but with infected AutoRun.inf file

In the third scenario, Ravmon.exe is removed from the system as well as the flash drive by an anti-virus tool. Now the remaining problem is the existence of infected AutoRun.inf file because of which the Chinese like characters in the open menu persist. But since the Ravmon.exe file has been removed from both the flash drive as well as the system the worm do not propagate to other systems via flash drives.

We see that although the Ravmon.exe file is successfully removed from the system as well as the flash drive, the AutoRun.inf remains infected. This motivates us to further explore techniques to successfully remove the infection in the AutoRun.inf file.

D. *Eradication/ Repair Recovery*

The eradication repair and recovery measures involve restoring the normal functioning of flash drives, by either removing the AutoRun.inf file or overwriting its contents. Removal of AutoRun.inf file consists of the following steps:

1. Open the *folder options* of your flash drive by navigating into *Tools* and then *Folder Options*.

2. In the *View* tab, under the *Hidden Files and Folders* option select *Show Hidden Files and Folders*.

3. Then also uncheck the *Hide Protected Operating System Files.*

4. A file with the name of AutoRun.inf will appear. Select the file, and then open using *Notepad*. Check if the following lines are present in the file:
shell\open=´ò¿ª(&O)
shell\explore=×ÊÔ´¹ÜÀíÆ÷(&X)

5. If the lines are present, delete the file.

The same effect can be achieved on the command prompt with the following commands [6]:

Type the command

C:\attrib -R -S -H C:\AutoRun.inf
C:\del AutoRun.inf
where C:\ represents the drive letter which you are attempting to correct. Overwriting AutoRun.inf file can also be performed to achieve the normal functioning of Auto play feature.

E. Follow up

After carrying out the recovery procedures the flash drive was restored to its normal functioning. Although the worm is completely removed from the system, as well as the flash drive but we still recommend certain preventive measures which should be taken to protect the system from being compromised by the attack.

The vulnerability that the attacker tries to exploit is the Autoplay feature of removable devices. We recommend disabling the Autoplay feature on USB drives as a method of prevention before plugging in the USB flash drive into the system. The Autoplay feature can be disabled by following the steps enlisted below:

1. Open Windows Explorer by pressing the Windows + "e" key.
2. Right-click the desired flash drive and select Properties from the menu.
3. Select the Autoplay tab

Select each item from the pulldown list and for the action to perform, select "Take no action" to disable Autoplay.

V. CONCLUSION

Memory sticks present no more of a risk than any other transferable data format. Banning memory sticks is a bit drastic and means not taking advantage of the technological advancements and its benefits. People need to be aware of secure and safe practice regarding viruses and data, and then there shouldn't be a problem. Various precautionary measures and available solutions should be employed to control the use of these flash drives.

REFERENCES

[1] “The Difference Between a Virus, Worm and Trojan Horse”, http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp
[2] “Coding VBS Flash Drive Worm”, http://forum.darkc0de.com/index.php?action=vthread&forum=4&topic=1856
[3] “Computer forensics”, http://en.wikipedia.org/wiki/Computer_forensics
[4] “W32/RJump.worm”, http://vil.nai.com/vil/content/v_139985.htm
[5] “Symantec Security Response”, http://www.symantec.com/security_response/writeup.jsp?docid=200 4-050614-0532-99
[6] “Flash drive Worms”, http://pakfellows.com/forums/messagepost.cfm?postaction=reply&ca tid=45&threadid=30990&messid=896812&startpage=1&parentid=896812