CyberSoft White Papers

Environmental Impact:

Microsoft Operating Systems and the Computer Virus Threat

by: Joseph Wells

www.cyber.com.

CyberSoft, Inc.
1948 Butler Pike, Conshohoken, PA, USA
Tel: +1 610 825 4748 * Fax: +1 610 825 6785 * Email info@cyber.com.

Thesis

Biological life forms depend on their environment to survive. In a friendly environment they flourish, but if their environment suddenly becomes hostile, they must either adapt or die.

This model applies to computer viruses.

Evidence of Extinction Level Events

In the mid-1990's I developed a theory about the effect of Microsoft Windows 3.1 on various types of computer viruses. The theory was intended to explain an observed phenomenon. In the early 1990's there was a decrease in the number of file viruses being reported in actual incidents. At the same time there was an increase of boot virus incidents. [1]

My conjecture was that most of the older DOS file-infecting viruses couldn't spread effectively under Windows 3.1, while most boot viruses could. The theory was subsequently tested and proven by the

antivirus research group at IBM's Thomas J Watson research center. [2] Others also adopted it. [3]

This paper is intended to explain to users how change in the computing environmen-specifically change introduced by versions of Microsoft Windows-has had a direct impact on the nature of the virus threat.

Much of the information given here is based on historical data from the WildList. [4]

The Paleozoic Era of Computer Viruses-DOS

When I analyzed my first virus in 1989, the primary virus threat involved memory-resident DOS viruses that infect program files (file viruses). DOS is file-infector-friendly. Back then, Jerusalem.1808 was the most common virus. Another, secondary class of viruses was the class of viruses that infect boot sectors (boot viruses). These were around, but they required users to accidentally boot from an infected floppy. File viruses were spreading faster. [5]

The first boot virus to become well known (actually well hyped) was Michelangelo in early 1992. During that same period, researchers were seeing a change in which class of viruses was more common. They were seeing more boot virus reports and fewer file-virus reports. Looking back, the reason was a change in environment.

The Mesozoic Era of Computer Viruses-Windows 3.1

The Jerusalem virus crashes Windows. Moreover, it infects Windows executables incorrectly-overwriting the start of the Windows portion of the file. [6] File viruses needed to be run from the DOS command line, but people were now running Windows programs.

Boot viruses, however, infect on system startup, before any operating system is running. When you accidentally boot from an infected floppy, the virus infects either your master boot record (MBR) or your DOS boot sector. Booting from an infected MBR or DOS boot sector puts the virus in memory. Once in memory, the virus infects floppies when they're accessed. Boot viruses infect via the system BIOS.

When do you accidentally boot from a floppy? Usually when there's a data diskette in the A: drive, your system hangs for some reason, and you hit [Ctrl] [Alt] [Del] or the switch. Talk about a boot-virus-friendly environment. In this new environment where file viruses began dying, boot viruses had everything going for them.

Several boot viruses infect well under Windows 3.1. Most notable of these are FORM, AntiEXE, and Monkey.B. Before the first macro virus appeared, these were the most prevalent viruses. Monkey.B has especially made life difficult for users and MIS people. This is because the conventional wisdom in dealing with viruses involves booting the infected system from an uninfected DOS disk and scanning the hard drive, but Monkey.B causes the infected hard drive to be invalid and invisible to DOS. It is extremely difficult to remove without an antivirus product.

But systems change and, from a boot-virus point of view, an environmental disaster was on the horizon. To paraphrase Dr. Emilio Lizardo, "Laugh while you can Monkey.B." [7]

The Cenozoic Era of Computer Viruses-Win32

Earlier versions of Windows were 16-bit operating systems-later versions are 32-bit operating systems. While boot viruses breed like rabbits by using system BIOS, Windows NT, Windows 95, and Windows 98 don't depend on system BIOS to function. (Windows 2000 which is based on NT technology.)

Viola! Boot virus birth control.

Note however: Windows NT doesn't make a system immune to viruses. Rather, it prevents the system from being a virus vector. The system can still get a boot virus, but it will no longer spread it to floppies.

Here's how it works: On system startup, the BIOS will run regardless of which operating system will ultimately load. It there is an infected floppy in the A: drive on startup, the hard drive will become infected at this stage. DOS and Windows 3.x used this system BIOS and viruses could spread. Windows NT, however, does not rely on system BIOS. NT comes with NT-specific disk drivers to perform low-level disk functions. So when the NT devices take over, the virus loses control.

Still, there is this brief window of opportunity in which the virus can take action. Herein lies the real danger of boot viruses under Windows NT. Some malicious boot viruses cause damage before NT takes control.

For example, if your system became infected with Michelangelo, it would quietly reside in the MBR and spread no farther. But when you boot your system next March 6th, the virus code will run, overwrite much of your hard drive, and NT will never get around to starting. [8]

Consider also the One Half virus. Each time you boot, it encrypts a portion of your hard disk. Under previous operating systems, the virus would be active in memory. While memory-resident the virus dynamically decrypts affected sectors; so you have access to your programs and data. With NT, however, the NT drivers take control away from the virus and parts of your system remain encrypted and inaccessible. With each boot you lose more sectors.

Monkey.B is a disaster on an NT system. On infection it makes the MBR invalid by overwriting it with virus code. It encrypts and stores the original MBR. While the virus is resident, it decrypts the original MBR and provides it whenever the operating system requests it. When you attempt to boot an NT system, you'll end up with the message "Inaccessible boot device" and a halted system. [9]

Statistics began to indicate a downward trend in boot viruses and a leveling out of file viruses (but at a low level). This statistical trend was seen primarily in the United States. Interestingly though, the drop in boot viruses seems to have appeared at about the same time that Windows 95 was released. However, antivirus software companies didn't go out of business. In fact, they were feverishly trying to

keep up to date, because a new virus threat type was created-one well adapted to the new environment.

The Eocene Epoch-Office 97

This adaptation appeared just before the downward boot virus trend began. Concept, the first macro virus written for the Microsoft Word environment, was "released" around the same time that Windows 95 was. [10] This virus gave us a whole new perspective on our statistics. It blew everything else away. In one year it became (by far) the most common virus.

So Concept, and the other macro viruses, became the primary virus threat in the Windows environment. These viruses were written in WordBasic-a macro language built into Word 6.0 and Word for Windows 95. We soon began seeing new WordBasic virus variants appearing on the WildList. Because these were the ones best adapted to spread in the new Windows/Office 95 environment. Then in 1996 the first Microsoft Excel virus appeared. Excel viruses have also spread, but not as efficiently as Word viruses.

But the environment was by no means static. With the appearance and widespread usage of Microsoft Office 97, we started to see a leveling off of the WordBasic macro viruses. In Office 97 WordBasic was replaced by Visual Basic for Applications (VBA). But this time extinction was not as imminent. This time some of the viruses could actually adapt (dare I say evolve).

Word 97 allowed the user to translate (or upconvert) macros from WordBasic to VBA. Some WordBasic macro viruses successfully upconvert others don't. Those that could adapted. [11] So some of these viruses that did successfully adapt by upconversion began to appear in the wild. In addition, viruses specifically written in VBA macro language began to appear, as did the first VBA "class" viruses.

In 1999, we began to see this evolution reflected in the WildList. In the April release of the WildList, Concept was still at the top of a section of the WildList called the frequency list. [12] At that time, the only VBA virus on the Frequency list was the newly discovered Melissa virus. But by August, Concept had dropped to number seven, and five VBA viruses were on frequency list-two being more frequently reported than Concept.

At the time of this writing, another change is becoming evident. The April WildList had 34 WordBasic viruses and 16 Word/VBA. [13] However, August has 19 WordBasic viruses and 27 VBA viruses. The ratio is reversing because there is now a VBA-friendly and WordBasic-hostile computing environment.

The Eocene Epoch-A New Era in File Viruses

At the same time, the August WildList shows that something else new was happening. Three other viruses, of another new type, were reported more frequently than Concept. The top two viruses on the August 1999 list actually represent two new virus types-both are specifically designed to function in

the Windows 32-bit environment.

Many researchers call the top virus on the list a "worm" rather than a virus. Whatever you call it W32/Ska.A is incredibly common (you may know it as the Happy 99 virus). It was the number one reported virus in August-and another, similar virus that beat out Concept is called W32/ExploreZip.

The number two virus in August was W95/CIH. 1003-a virus created for Windows 95. This one got a lot of press in early 1999-and for some reason the press took it upon themselves to rename the virus "Chernobyl" -even though no antivirus product uses that name.

Note the increase of this new breed of file-infecting viruses. There were seven Win32 viruses reported in April of 1999. By August there were 13. Yet even some of these may already be doomed-they're specific to Windows 95 and won't infect under Windows NT. [14]

In Perspective

In 1996, IBM proved my theory that old DOS file-infecting viruses began moving toward extinction in the early 1990's, when the environment (Windows 3.1) became hostile to them. Next came Window 32-bit operating systems, which bypass BIOS-and boot viruses depend upon BIOS to spread. Thus, we're now seeing a decrease in boot viruses. Finally, Office 97 created an environment that was hostile to many of the original Word macro viruses and it appears that these have begun to drop off the WildList.

What does this evidence demonstrate? The nature of the virus threat is by no means static, because their environment affects the various virus types. The world's computing climate has gone through dramatic changes as a result of changes in the computing environment-specifically changes in Microsoft operating systems. Except for a few WordBasic viruses that survived upconversion in the wild, computer viruses, unlike true life forms, have not been able to adapt to these changes.

As a result, WordBasic viruses are now threatened. Many boot viruses are on the endangered species list. And all but a few DOS file viruses are virtually extinct. Thus the very nature of the virus threat has changed drastically because of changes in the computing environment. We have seen the threat primary type shift from file viruses, to boot viruses, to WordBasic viruses, to VBA and Win32 viruses.

What does this mean for users?

This means that the chance of someone getting the older types of computer viruses is steadily decreasing. DOS file-infecting viruses and, to a lesser extent, BIOS-based boot viruses simply can't cut it in today's computing environment. In the real world, they are moving toward extinction. In a similar manner, the older WordBasic macro viruses that cannot successfully adapt (upconvert) will follow suit-as will viruses specific to Windows 95.

Antivirus product developers must keep these facts in mind. Research must keep pace with the reality of the changing virus threat. Development must optimize product size and speed by removing any

viruses that are not a real-world threat. [15] Yet, many antivirus products were originally developed to handle viruses that are now nearing extinction. As newer threats have appeared, products have been patched to handle the change, but none have been completely redesigned and built from the ground up.

The computer world is still changing. Can "adapted" patchwork products cut it, or do we need a whole new species of antivirus?

[1] White, Steve R., Kephart, Jeffrey O., and Chess, David M. "The Changing Ecology of Computer Viruses," ***Proceedings of the Sixth International Virus Bulletin Conference***, Brighton, UK. September 19-20, 1996

[2] Ducklin, Paul, "Anti-Virus Research: What's Over the Next Hill?" ***Proceedings of the Seventh International Virus Bulletin Conference***, San Francisco, October 2-3, 1997

[3] White, Steve R., Kephart, Jeffrey O., and Chess, David M. "The Changing Ecology of Computer Viruses," 1996 Acknowledgements.

[4] The ***WildList*** is a monthly report on viruses reported in the wild (i.e. actually spreading on user's systems). It was founded by Joe Wells in 1993 and is under the control of the WildList Organization International. Copies of the WildList are available for free at www.wildlist.org.

[5] The first PC virus was a boot virus, however file viruses soon outnumbered boot viruses by 1991. For example, of the 118 known viruses listed in the August 1990 ***Virus Bulletin***, only 13 were boot viruses.

[6] Jerusalem calculated the file size in .EXE program files by using the size stored in the file header. Windows EXE files have a DOS stub file and the Windows program follows directly after the stub. So when Jerusalem infects it writes its own code right after the stub, thus overwriting the header information for the Windows program.

[7] Dr. Emilio Lizardo (also called John Warfin) was the red lectroid leader in the cult movie, ***The Adventures of Buckaroo Bonzai-Across the 8th Dimension***. What he actually said was "Laugh while you can, monkey boy."

[8] Aubrey-Jones, David, "What Threat are Viruses on Windows NT?" ***Proceedings of the Sixth International Virus Bulletin Conference***, Brighton, UK. September 19-20, 1996. This paper discusses the effect of various boot (and other) viruses under Windows NT.

[9] Aubrey-Jones, David, "What Threat are Viruses on Windows NT?" 1996

[10] Gordon, Sarah, "What a (WinWord.)Concept," ***Virus Bulletin***, September 1995,

pp. 8-9.

[11] Concept, and a few other WordBasic viruses, were actually recognized by Office 97. These were not up converted (however, some were reportedly upconverted by a beta version that had the detection disabled), others failed upconversion and resulted in invalid VBA code modules that would not run, and still others, including some Wazzu variants, successfully upconverted and spread in the wild.

[12] The frequency list portion of the WildList shows viruses reported by 15 or more participants. It is sorted by frequency.

[13] Word/VBA is used here because other office viruses written in VBA also appear on the list. These are primarily viruses that infect Excel spreadsheets.

[14] Such viruses depend on Windows 95 specific DLLs.

[15] For exhaustive evidence that certain viruses should be removed from antivirus products-and that this would improve those products-see my paper "A Radical New Direction in Virus Scanning." Available from CyberSoft's web site, www.cyber.com.