جامعة الناصر
AL-NASSER UNIVERSITY

Computer Viruses: Now and Then

Dr. Mohammed Al Muhtadi

AUTHORIZED BY AL-NASSER UNIVERSITY'S RESEARCH OFFICE

Abstract

Our health-conscientious society has come to view any type of virus as an attack, and computer viruses are among the most hated. No computer or network is impervious to an infection, and even a "benign" virus can waste an IT administrator's time while the most dangerous infections can cost consumers and businesses thousands of dollars in hardware, software and man hours. With so many enterprises relying solely on computers for data storage, the cost of serious infections is undeniable.

There's a fine line between proper concern about the potential threat that viruses represent and paranoia, however. People know that a healthy immune system paired with exercise, good diet and routine checkups can prevent infections and prolong life. The same is true for computer viruses, and a few preventative measures can save money in the long term.

- Viruses throughout history
- Who creates viruses? How do they infect?
- Signs of a malware infection
- Statistics about virus proliferation and the cost of viruses
- The anatomy of viruses and inner workings of anti-virus software

A Virus By Any Other Name

Just like a virus that infects your body, malicious computers infections are coded to latch on and propagate, often without leaving any signs of infection at all. Viruses spread by attaching themselves to other programs, including presentations or word documents, or by infecting the boot sector of a hard drive. Viruses often run when the computer boots, making it difficult to remove an infection. A computer virus may then attack and infect the next app that launches as well as other drives and removable media that is connected to the computer.

The true risk of viruses lies in the way that they can cause changes to your computer. Known as "events," these changes may vary from hijacking your browser or changing the computer date to causing lag and using up memory. The worst viruses can modify or delete data, and in some cases a virus is capable of crashing the entire system.

The Spread of Viruses

A virus is simply code like any other program, which means a virus can tag along with any legitimate app. Program installation and booting from floppy disks used to be the origin of many virus attacks. However, the Internet has changed how viruses infect computers. While 87% users pinpointed a floppy disk as the source of a virus in a 1991 study by Dataquest for

the National Computer Security Association, many computers no longer have any optical drives at all, and they're still prime targets for virus infection.

More recently, anti-malware software developer ComboFix cites 5 main sources for virus infections, and four of them involve the Internet directly:

- Downloadable Programs
- Cracked Software
- Email Attachments
- Internet
- Booting From CD

Microsoft also warns of the risk of downloading a virus when browsing the Web.

However, a different mode of infection spread only makes viruses more dangerous. Nearly 75% of infections occur on a computer connected to a network, which means all other devices on that network become vulnerable.

The Real Damage of a Virus

While some viruses use up system resources and simply cause a computer to lag, others are much more dangerous. For the most part, creators of viruses want to use machines to spread infection rather than destroy the computers entirely. However, viruses do not always act as intended and can interact with specific hardware or software on the system to cause further damage. In some cases, the intent is more malicious, and a virus may destroy files and data, interfere with connected hardware and even reformat a hard disk drive.

Signs of a Virus Infection

As long as a virus goes unnoticed, it's free to spread itself; thus, most viruses want to remain invisible. Users can protect their systems from these viruses with use of an anti-virus program. Not all viruses are silent, however. There are several indicators of a virus infection:

- Change in program/file size
- Apps load more slowly
- General system sluggishness
- Unexplained disk or memory usage
- Redirected browser/search pages
- Unresponsive anti-virus programs
- Strange error messages
- Programs not loading
- System not loading
- New programs/icons added

Viruses Litter the Landscape

Are viruses something that people should really be concerned about? The answer is "Yes!" Even the largest companies have experienced an infection, and many enterprises experience repeat infections. Companies with networks made up of 1,000 computers are more likely to experience infections -- an attack four to six times per year -- and the frequency increases the longer the network exists. In a year, viruses could attack monthly.

Indeed, research from Dataquest suggests that successful infections are only growing, and they're growing at exponential rates. In their survey, over 60 percent of respondents had dealt with a small-scale virus infection and 9 percent had experienced infections of more than two dozen machines.

The problem first became noticeable around 1990, and companies with more than 400 computers the experienced a drastic increase -- 600 percent -- of infection in the mid-1990s according to Certus International. A more recent study by Kaspersky shows that 16 million personal households in the United States experienced serious virus problems in 2012.

More Viruses, More Problems

With Kaspersky detecting 200,000 new viruses daily, it's hard to believe that there were no more than four viruses in 1986. It took months for new viruses to be created. By 1989, that gap had narrowed to just one week between new viruses, and the 1990s saw viruses created on a daily basis. This has led to millions of different viruses and strains.

Viruses in the Millions

While new viruses arrive every day, it's not just the new strains causing problems. In 1996, most infections were caused by viruses created in 1990. 300 of the original viruses were so resilient that they were still affecting computers six years later. Almost twenty years later, viruses have only continued to proliferate, and there are millions in existence. Pinpointing the exact number of viruses is difficult. Simply looking at virus definition lists paints a telling picture. While Symantec added 303 entries to Norton's definitions during a one-week period in 2012, only 12 of those entries were new. Most of the definition entries were revisions or duplicates of viruses that had begun affecting operating systems other than Windows.

The Very First Viruses

Once upon a time, defending against viruses wasn't accepted as a reality of owning a computer that had network access. Just 30 years ago, viruses didn't exist. The fist handful of viruses were created specifically in computer labs to show the potential threat of such code. However, those viruses spread to other labs just like viruses do now. Of the original viruses, three are the most well-known -- Stoned, Cascade and Friday the 13th -- and they all appeared in the same year.

Computers experienced outbreaks of those viruses for the next two years. The media even gave major coverage to two: Datacrime and Friday the 13th. Later, the general public would

hear about
the Michelangelo virus. Interestingly, the European nation of Bulgaria seemed to be a powerhouse of virus creation despite its tiny size. In 1990, Bulgaria originated over 75 viruses including Dark Avenger, which would become known the world over. This propelled the country to the top of the virus creation leader boards. At the time, Bulgaria had many programmers who were skilled and trained but not employed. They used their talents to created viruses instead of contributing to other projects.

The unprecedented growth meant that computer security suddenly became a very real need for computers connected to the Internet. Manufacturer IBM became the leader of those efforts after creating the High Integrity Computing Laboratory. In addition to this, Symantec would create one of the first anti-virus programs, Symantec Anti-Virus, for anyone who had the money to protect their computers.

The response was right on time. In 1991, viruses became able to adapter to their environments, further eluding computer operators who were attempting to block or remove infections. Total strains numbered over 1,000 as well.

Viruses became part of the fabric of the Internet in the 1990s, with more programmers creating viruses and more consumers investing in computers to provide those viruses with a suitable place to take up residence. In part, young people who were just learning how to code contributed to the astronomical release of new viruses. The United States provided plenty of opportunity for people who were interested in code. Across the ocean, both Germany and Taiwan became prolific at virus creation.

Software creators such as Microsoft would also come to realize that the tools they used to create legitimate apps were ideal for virus creators. In 1992, tools such as Mutation Engine the the Virus Creation Laboratory were created specifically to allow other people to develop new viruses. A GUI in the Virus Creation Laboratory enabled even those who weren't excellent programmers to create pieces of nefarious code to that would adapt and spread on its own.

More Places to Infect Than Ever

Computer ownership is at an all-time high, and mobile devices are everywhere you look as well. Some computers function only when they're connected to the Internet, and wireless networks are a dime a dozen. With both business and home users relying heavily on computers and networks, the number of victims has grown exponentially. Here's a breakdown of PC growth. In 1990, there were 54 million installed computers. In just three years, that number grew to 112 million, and over 40 million computers added to the numbers by 1994.

Technological advancements made business computers more susceptible to attacks, too. Personal computers became more powerful and software more capable, allowing companies to move away from mainframe servers to PCs and client-server computing.

Client-server computing is an especially likely target for virus infections, and one unprotected computer on the network can infect multiple machines connected to the network in rapid succession. This wasn't true two decades ago when businesses still relied on mainframes and networking was less advanced than it is now. After one computer becomes infected, it takes only a few minutes to infect another machine on the network. Even enterprise-sized networks can become completely infected by a virus within hours.

To add to the risk, many of the people who were operating machines on client-server networks were not previously experienced with computers. Laptops and notebooks exacerbated the issue. Portability allowed computers to connect to multiple networks, allowing viruses to spread even further. Cloud-based services require even less computing power, so even tablets are capable enough of handling business processes.

The Future of Viruses

At first, people focused on the positive possibilities of the Internet, once known as the "data superhighway." Few people were concerned over possible security implications. However, the truth remains the same. Any networking means more computers become susceptible to infection than before. The allure of cost-effective data transfer, including video, voice and data traffic, led to more computers and devices connecting to the Internet. Now, government agencies, the military, non-profits, small businesses, schools and individual consumers all have access to the Internet. As the Internet grows more populated, the threat of virus infections also grows.

It's not just about numbers, however. Viruses will continue to become more dangerous, and more strains will come into existence. Tools such as Mutation Engine and the Virus Creation Laboratory were used to create a boom of boot sector viruses that remain especially difficult to remove. The evolution of viruses has also lead to polymorphic boot sector viruses that are able to adapt to avoid detection and removal. Many virus creators focused on Windows computers, but the threat has expanded to Mac OS and programmers continue to target mobile devices such as Android smartphones. As developers attempted to thwart viruses, virus creators simply became more creative, resilient and intelligent when it came to coding malware.

Anti-virus and security companies faced a specific hurdle when computers began running 32-bit software. Software such as DOS and Windows 3.1 still used 16-bit architecture were already equipped with anti-virus solutions while newer 32-bit programs such as UNIX and Windows NT were on the way. McAfee and Symantec were among the biggest names in the security industry, and the companies were prepared for the upcoming 32-bit applications that would arise after Microsoft released Windows 95 for home use. August 1995 came and went, and the release of Windows 95 was a bumpy road for everyone involved.

Existing anti-virus solutions worked best with 16-bit applications, and they couldn't detect infections in the newer 32-bit programs. There was a lack of anti-virus solutions available to home users at the release of Windows 95. However, both McAfee and Symantec released

their own tools, Virus Scan 95 and Norton Antivirus 95, respectively. The release of Windows 95 demonstrated how anti-virus creators would have to keep up with advances in hardware and software for computers to remain protected against new threats.

Digital Infections Have Real-World Costs

The cost of computer virus infections during the first several years in the 1990s was more than anyone would have estimated. A survey by IBM's High Integrity Computing Laboratory and Dataquest shows that businesses lost almost two billion dollars in the first three years of the decade. In 1994 alone, companies lost 1.9 billion dollars to virus infections. While anti-virus applications helped to steady the rate at which costs of infections climbed, the price remains undeniable. In 2004, the MyDoom virus caused $38 billion in damage. A survey by the FBI reported that the average company lost $24,000 on computer viruses, spyware and computer-related crime.

Much of the high price of virus infections is due to the costs for cleaning up infected computers, networks and drives. Loss of productivity also contributes to the rising costs of a virus infection when you consider that one virus can easily affect 1,000 computers. Attached devices and drives for each computer must also requires scanning and cleanup when infected.

Virus Plan of Recovery for 25 Computers

The original study that Dataquest performed in 1991 about computer viruses was telling. American companies typically required four days to fully recover from a virus attack. Some companies needed as much a month to recover. To add to the cost and frustration of a successful attack, some companies experienced relapses after infected drives or disks remained infected and those infections were able to attack the network once more. 25% of networks would experience a relapse like this within a month of the original attack.

In 1993, cleanup of a computer virus infection cost companies an average of $177,000. That amount continued to grow. In the next year, the cost skyrocketed to $254,000 per company with 1,000 computers. Every machine that required cleanup would cost an organization hundreds of dollars.

Companies began to take note in the early 1990s. NYNEX, a large telecommunication company, appeared before the U.S. Congress in 1993. The briefing detailed viruses and infections over the previous four years. NYNEX had experienced 50 reports events with viruses, and the company believed many other virus infections had gone unreported. The company's briefing revealed that it was unlikely for a single computer to experience a single infection. Rather, viruses tended to affect more than a dozen computers and 50 disks at a time. In one incident on a 3Com
network, personnel did not become aware of an infection until after 17 computers had already become infected. The network experienced a week's worth of downtime during cleanup.

In comparison, annoying viruses that are intended to exact less damage are less costly, but the prices are still high. For example, the Jerusalem-B virus infected 10 executable files on just one computer. However, the computer was connected to a network so all the computers on the network required scanning. The process cost the company two shift plus overtime for four IT technicians scanning the network, and the LAN experienced frequent interruptions during those two days of damage control.

Mick Krause, the Program Manager for Information Security at Rockwell International, submitted the cost a virus infection that her company had experienced:

Technical Overview

How Computer Viruses Work

Viruses are small pieces of code. At the base of this code is an instruction to replicate. Viruses are able to do this by exploiting processes already on the infected computer, or host. During infection, a virus can makes it homes in any software component of a computer environment. This includes programs, the operating system, the boot sector of a disk and a driver for a piece of hardware. Viruses are able to take control over the host in a variety of ways. This brief details the common types of viruses, their function and how we can fight them.

Types of Viruses: File

Although there are multiple types of viruses, most of those that are currently known, including the Friday the 13th virus, are file viruses. This means that infection occurs because the virus has attached itself to another file much like a parasite. These files are typically .EXE or .COM files that execute or control another program. The code belonging to the virus inserts into the overall application code. When the program launches, the virus executes before or instead of the intended program.

File viruses typically store themselves in a computer's memory, which allows the virus to monitor the computer. When the user launches another program, the file virus can then infect that application as well. A simple type of file virus will overwrite the host application, causing it not to load at all. However, this alerts computer users of the virus. The sooner an infection comes apparent, the less time the virus has to spread. This is why more complex viruses act in a more subtle way. It allows the virus grater opportunity to spread before detection.

The increased usage of client-server environments had less to an increase in file viruses as well. Networks provide the challenge of adequate detecting and cleaning viruses from memory without having to reboot from a clean disk. When a virus spreads through a host computer, it becomes more difficult to remove the infection. Sometimes, the method used to scan a computer can even cause further infection if the scan opens files, allowing viruses to infect those new files. Well-known virus "Hundred Years" was able to infect non-executable data files, too.

Types of Viruses: Boot Sector

There are only about 200 strains of boot sector viruses currently. However, these viruses make up 3/4 of all computer infections. Stoned, the most common computer virus up until this point, is a boot sector virus. Michelangelo is another notorious boot sector virus. These reason boot sector viruses are so common is because they are difficult to detect. This type of virus doesn't frequently affect computer performance or change file size in a noticeable way. Users may not be aware of a boot sector virus until their computer begins to reformat. Boot sector viruses are known for their ability to rapidly spread and infect removable media such as floppy disks, which allows the disk to transfer itself to the hard drive. Boot sector viruses launch with the boot of the hard rive or disk, and the virus gains control of the host before MS-DOS has even loaded. This type of virus is able to infect a variety of environments because MS-DOS doesn't have to load. These includes MS-DOS, Windows, OS/2, PC-NFS, or Windows NT.

Boot sector viruses enter RAM, where they remain to infect the hard disk until the computer restarts. Restarting requires the virus to enter memory again, which allows tools such as CHKDSK to detect the virus when the program is used to analyze memory usage. Boot sector viruses typically use a few kilobytes of RAM. Partition table viruses are similar to boot sector viruses, but they attack the hard drive petition, move that partition and replace the original partition with infected codes. Partition table viruses are able to spread to the boot sector when floppy disks are used.

Types of Viruses: Multi-Partite Viruses

Multi-partite viruses are the worst of both boot sector and partition table viruses. These viruses infect any components of the host software, and multi-partite viruses can spread as easily as a file virus while retaining the ability to infect the partition table or boot sector of a computer. For this reason, removal of multi-partite viruses is especially difficult. One example of this type of virus is Tequila.

Types of Viruses: Trojan Horses

Just like the classical Trojan horse, this type of code presents to be something that it's not. Often, Trojans pretend to be software that the user would actually install. Initially, this type of virus didn't replicate; however, advanced Trojan Horses were created with that intent. After a specific event, the Trojan Horse infection perform a specific task such as displaying an error to the user, destroying data or reformatting the disk. While some researchers do not consider Trojans to be the same as computer viruses, the damage and cost remains high to users.

Types of Viruses: File Overwriters

File overwriters are parasitic viruses that attach themselves to a specific application. While the program's code remains the same, the virus attempts to infect as many files as possible. Some overwriters are created to do nothing more but replicate, using hard drive space and

causing a computer to run more slowly. When viruses of this type are flawed, they can have more damaging effects, including destroying data and files. The most dangerous file overwriters are completely invisible until the trigger event. At this point, the virus can deliberately wreak havoc on the system.

Types of Viruses: Polymorphic

Viruses are increasingly of the polymorphic variety, which means that they can adapt to avoid to detecting. Thanks to Mutation Engine, which allows even non-programmers to easily create polymorphic viruses, the numbers of this type of virus will only continue to rise. Polymorphic viruses in computers are comparable to the AIDS virus that infects humans. Both mutates to make it difficult for the host to detect and defend against the virus. In the case of the polymorphic virus, it's an anti-virus program and not the body that the virus eludes because the virus does not compare to known infections. Polymorphic viruses contain encryption code that allows the virus to remain hidden for longer. In addition to this, these viruses have a decryption routine that runs when the file executes. There is no type of software that polymorphic viruses can't infect. They're commonly seen as file viruses, but boot sector polymorphic viruses also exist.

Fortunately some of these viruses can only mutate a limited number of times, which helps anti-virus programs to detect infection by the virus. For example, the Whale virus has only 32 forms that a security program can compare a suspected infection to. When anti-virus applications can account for wildcard variations of the virus, detection and removal becomes easier. However, Mutation Engine allows virus creators to devise polymorphic viruses with as many as four billion strains.

Types of Viruses: Stealth Viruses

Just like stealth airplanes are designed to avoid detection by radars, stealth viruses have been engineered to avoid detection by security "radars" or anti-virus software. Despite the fact that the file exists as part of another application or in the boot sector, scanning tools are unable to locate anything amiss. A stealth virus remains in the computer's memory where it can monitor the system. When the host opens a file that the virus has infected, the virus quickly removes traces of infection and allows the computer to execute the file normally. When MS-DOS closed the file, the virus once against infects it.

Stealth viruses that target the boot sector are even more tricky because they change the position of the actual boot sector code on the disk. These viruses allow the computer to boot normally by "passing along" the actual boot code. To the untrained eye, everything appears normal. However, users aren't seeing the normal boot. As long as the stealth virus is on a computer, it will take up space and cause the computer to perform poorly. Stealth viruses might delete data or files as well.

Scans from security software can help the virus spread itself to other files on the host computer by opening files during the scan. Stealth viruses can then infect those files while

they are open. The same process makes it difficult for the anti-virus software to locate the virus.

Security Software for Virus Detection and Removal

Anti-virus software like that from Symantec and McAfee can rely on an every-growing pool of resources to fight viruses. These tools include signature-based scanning, monitoring of the system, checksum comparisons and generic expert systems. Through a combination of these tools, programs can reduce a host computer's vulnerabilities to virus infection. Software that relies on only a couple of these methods won't cover all the possible methods of infiltration. Thus, the best method to prevent computer virus infection is to utilize all these methods to create a barrier between the computer and viruses.

Signature-Based Virus Removal Tools

A virus scanner will inspect every file on a hard drive and can use any of the mentioned methods. The most commonly used tactic is signature-based analysis. Every virus leaves a signature containing unique lines of code. Like a human fingerprint, these signatures are unique, and anti-virus software can identify viruses based on the signatures that they leave behind. Anti-virus applications like Norton contain libraries of viruses and their signatures. Entries in these catalogs are known as definitions

The most comprehensive security software will use this method to scan for potential infections and update their definition databases frequently. The best scanners look in files, the boot sector, memory and partitions to find possible traces that match the known signature of a virus. After a match is located, the scanner can pinpoint the location of the virus to remove it from the system. The ability to identify a virus goes a long way toward virus removal. This same method also enables programs to prevent viruses from infecting a system in the first place.

However, the signature-based scanner isn't without its flaws. Only viruses with signatures known to the program can be detected or removed with this method. Viruses that have yet to be discovered, analyzed and added to the database can elude these scanners. Polymorphic viruses are especially capable of avoiding detection by these scanners because they can mutate their signatures.

Resources

http://www.microsoft.com/security/pc-security/virus-whatis.aspx

http://www.combofix.org/top-5-sources-of-computer-virus-attack.php

http://www.statisticbrain.com/computer-virus-statistics/

http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_Kaspersky_Lab_now_detects_200000_new_malicious_programs_every_day

http://www.investopedia.com/financial-edge/0512/10-of-the-most-costly-computer-viruses-of-all-time.aspx

http://news.cnet.com/2100-7349_3-6028946.html

http://www.zdnet.com/blog/bott/the-malware-numbers-game-how-many-viruses-are-out-there/4783