# Computer virus: 20 years look back

In the three decades of computer development, there has been a twenty-year silence: computer viruses. People have spent a lot of effort to develop computer science and have no less effort to eliminate the virus. Like

**In the three decades of computer development, there has been a twenty-year silence: computer viruses. People have spent a lot of effort to develop computer science and have no less effort to eliminate the virus. Like a serious illness, computer viruses still don't get better. They continue to grow with increasing scale and harm.**

What solution for computer viruses? A question that seems simple but still has no satisfactory answer. Let us turn over the timeline, analyze and ponder to find a solution to this "inter-century" problem.

**Computer virus, persistent joke**

In fact, computer viruses have been around since the early 1970s. Creeper viruses (1970), Rabbit (1974) and Animal (1980) are considered the ancestors of computer viruses. However, due to being born on large computers, they only spread around in laboratories, not many people are interested in other than computer experts. Computer viruses only have a strong impact on society when they transfer from a large computer to a

personal computer. Brain is the first computer virus (1986) to perform this task. Brain's original purpose was to serve advertising for Brain Computer Service in Lahore (Pakistan). When the computer is infected with a virus, a screen suddenly appears introducing the name and address, including the company's contact phone! The parasite entered the boot sector of 360KB type floppy disk, the most popular data exchange media at the time, Brain virus infected worldwide. Although not harmful to computers, Brain made many computer users panic.

After Brain, other virus-boot (B-virus) sectors appear in turn such as Lehigh, Vienna, Cascade, Pingpong . Viruses of this period are "benign", mostly originating from universities where There are many good and active students who like to joke. However, their gentleness does not last for long. To make a strong impression, hackers are keen to put malicious code into B-virus making them more violent. Representatives of this type are Disk Killer virus. After 30 hours of infection, the virus will encrypt the location data of the disk partitions causing the system to be paralyzed, and all data is destroyed.

Due to the attack of the computer before the operating system starts, even though it is small (512-2048 bytes), B-Virus easily controls BIOS-based disk access tasks, independent of the operating system. The biggest disadvantage of B-virus is that the activation capacity is not high (because not all computers start from the floppy disk). To combat B-virus, ROM-BIOS manufacturers have taken a very timely move: providing the option to disable the booting of the computer from a floppy disk. Some chip manufacturers also integrate procedures to identify B-virus-like behaviors into ROM-BIOS.

Before this situation, the hackers tried to resist by expanding the object to the executable file COM and EXE of the operating system, giving birth to new viruses: virus file (F-virus). Although it depends on the operating system, F-virus solves the basic disadvantages of B-virus. Using the operating system script, F-virus not only disables virus-like behavioral identification programs in ROM but also enhances the ability to create multiple parasitic copies on other objects on the system. Vietnamese people in the 1990s still remember the impressive attacks of Friday 13th, Datalock, Little Girl, White Rose . on MS-DOS operating system which had a simple structure with many serious security holes important.

But the worst is just beginning. Along with F-virus, bisexual viruses (including boot sectors and executable files) such as BFD, Compback, Invader, Junkie, Natas . wear on both ROM-BIOS directives and operating systems. onions. Viruses spread on disk structures such as Dir2 / FAT, Weichan . also jumped into battle, making the situation more confused and gloomy.

Recognizing the weakness of 16-bit products, Microsoft decided to stop developing MS-DOS and Windows 3.x. In 1995 the company unveiled a 32-bit operating system with a graphical interface. The advent of Windows 95 marked the turning of the color of the global information technology scene and shook the world of computer viruses. If MS-DOS applications run in single-session real-time mode, the Windows 95 application works in a multitasking protection mode. Each process is granted a separate space by Windows, completely separate from other applications. This model has disturbed hackers' F-virus design techniques. In a unified environment, from its own permanent memory, F-virus can freely interfere in the space of other applications. In a multitasking environment, F-virus itself can only work around the application's virtual machine space. However, some F-viruses on Windows (such as Spenna Spy, Bodgy, Bolzano, Pate .) also try to exploit directory search functions to insert code into files that are "sleeping" on the system. This method only improves the situation temporarily because the virus is easily detected (hard disk is continuously accessed, the disk space increases suspiciously, the speed of the machine is significantly reduced . ).

Perhaps those who develop computer viruses understand very well the meaning of the proverb "the hard-to-reach difficulty". Concept is one such virus. Exploiting the macro script file (VB Application) in Microsoft Office

office suite, this virus author has created a new virus just to "prove my point", prove his point: the virus also has can infect data files! Although not destructive, the worst thing the hacker has done is publish the entire code of the virus. This triggered the "post-Concept" phase with the emergence of macro viruses CAP, Gold Fish, CyberHack, JohnMMX . Do not stop there, macro viruses also "encroach" to Microsft Excel with " Life products "like Laroux, HalfCross, After-5h . Both Power Point presentation files are infected by TriState virus.

Dissatisfied with the VBA script, hackers also study other types of destructive spreads. A wide range of malicious codes such as worm, Trojan horse, backdoor . appear. Do not transmit directly to F-virus executable files, they exist and act as a standalone application. Taking advantage of network communication, they send themselves to the addresses collected on intermediate stations on the line. DemiURG, the type of virus dubbed "7 in 1" is a typical. Spread through the network to the destination machine, DemiURG spreads into 7 infectious forms of BAT, EXE-DOS, EXE-16, EXE-32, DLL, XLS and VBS. When a sample finds "prey", it gathers 7 brothers and spreads to the object. When a sample is destroyed, other patterns will be applied to the defeated.

In the face of unfavorable situation, Microsoft had to "press the stomach" to add "Warning virus macro" in MsOffice 97. This move has reduced the number of macro viruses but also caused the giant to sweat profusely. Credit is declining: customers are no longer interested in VBA scripts, each advertised as a powerful customization tool for advanced users.

Aware of Internet growth, 1998 Microsoft introduced a version of Windows 98 that added many important network services. It can be said that the Windows 98 and MSOffice 97 product suites have handled their role very well in a collaborative and shared environment. However, the virus cloud does not really dissolve. Although it proved to be superior to MS-DOS in terms of security, Windows 9x also had certain weaknesses. CIH (aka Chernobyl) is a testament to the laxity of this operating system. CIH was discovered in July 1998 in Southeast Asia. Its author argues that the level of devastation of this virus is similar to the one that leaked the Chernobyl nuclear reactor on April 26, 1986 in Russia where humanity must be vigilant. The CIH variants spread into the EXE-32 file of Windows 9x. When activated, CIH checks the current day of the system to decide to "hand out" or just infect other EXEs. If it is on April 26 (for version 1003 and 1049) or 26 monthly (for version 1019), CIH format track 0 all hard drives on the machine, then CIH writes "garbage" into flash ROM makes the machine completely destroyed. Exploiting the weakness of Windows 95, CIH has changed the subjective perception of users that "computer viruses only destroy logical data, they cannot touch the hardware of the machine". With its sinful scenario, CIH has spoiled millions of "brand name" computers around the world (kind of using die-chip ROM chips on the motherboard).

While Microsoft has not "recovered" after CIH's attack, the macro virus "shriveled" is disruptive. In March 1999, Melissa (relative to VicodinES) made a spectacular shot. Using only the VBA script, Melissa is the first macro virus capable of sending its code to email addresses in the victim's address book. Thanks to the email service, Melissa infected hundreds of thousands of computers in a few hours, a remarkable transmission rate that hackers longed for. In turn, Melissa "set an example" for other viruses like Sircam and Nimda to study. However our scenario is different from Melissa. When taking control of the system, they flocked to the My Documents folder to browse the user's private documents and then send them to other computers. This attack caused many people to "stand dead", especially businessmen because the company's secrets were exposed to people.

In this situation, Microsoft decided to replace Windows 9x with Windows 2000 operating system using Windows NT technology with NTFS disk format, which was rated better than FAT32 in terms of organization and security. After the cluttered Windows 2000 "guy", the red-glazed Windows XP girl is "merry" by Microsoft boss with many outstanding features: support for multiple CPUs, tight memory management, better disk access , ActiveX executable code protection, powerful multimedia support, remote access control . In 2003, Microsoft

officially announced to stop technical support for Windows 9x users, meaning operating systems Windows 95, Windows 98 and Windows Me were "deadly".

Despite Microsoft's attempts to improve security, hackers still do not break down. In 2001 the Blaster worm, then Sasser, exploited the vulnerability of Remote Access Control to issue a command to shut down the victim's computer remotely. This scenario is also implemented by Slammer (2003) with a more dangerous level: closing down SQL Server by sending messages through the communication port without writing the virus code to the hard disk.

2005 was a turbulent year with 2 outstanding events in the security field. Most notable is the counterfeiting and theft of international credit cards. Security experts believe that in this case there is a strong need for software to act as computer viruses, secretly entering the database storage system, stealing the user account ID number. issued to pirated card printing establishments. The second case was less popular but brought another meaning: confrontation between hacker organizations Mydoom and Netsky. Mutating and mutually exclusive, hacker groups from different countries have disturbed the information technology world. Up to now, although the war has been less stressful, the names of these viruses are still in the "top-hot" ranking list of security companies.

**Look for antivirus solutions**

In the fight against computer viruses, the virus scanning software (also called anti-virus) plays the most active role. Using a sample library of known viruses, anti-viruses quickly detect the presence of viruses in the user's computer. When the number of viruses is low, the frequency of strange virus occurrence is low, the pattern-based identification method is quite effective. As the number of viruses increases, anti-viruses are at a disadvantage: the world has only about 25 large companies confronting 150,000 different viruses. Against this situation, anti-viruses seek to take the initiative when an outbreak occurs. This plan includes two main areas: increasing the speed of updating and proactively detecting strange diseases. The first segment is tasked with increasing the team of new virus update experts and this is a strong policy to support online customers. The second array focuses on the research of advanced new intelligent virus identification algorithms, promptly blocking them before they spread. Each anti-virus selects a separate research path: Symantec has Bloodhount, Sophos chooses the genetic direction, McAfee studies hashing, BitDefender uses heuristic . Because the results of the predictions are always wrong, Customers must accept the risk: sometimes anti-viruses detect a virus on the clean data. Although difficult and complicated, this strategy is the inevitable trend of anti-viruses.

Although the anti-virus has made a lot of efforts, the battle's situation has not changed. During the 20 years of existence and development, the virus has not (and does not need to) change the attack scenario: it is to take advantage of loopholes (security vulnerabilities of the system, innocence of trust, and fondness). user period) to implement intentions of destructive infection. There are two notable factors: the system (including operating system and applications) and computer users. The fact that tight systems are less likely to be attacked by viruses. Patchwork operating systems (fix, patch) are always fertile ground for computer virus development. Every time the system is consolidated, some viruses return to the backstage, and the security situation temporarily settles for a while. Soon the epidemic broke out again with new, more dangerous viruses. Therefore, network security and security have always been Microsoft's top priority in the future 64-bit operating system development plan.

Users are crucial to the survival of information technology companies. Users choose and spend money on quality IT products, so that new companies can continue to exist to produce better products. However, due to differences in income of each country, due to differences in consumer psychology, due to inadequate price policy and many other reasons . not all users are willing to pay a purse. . The use of pirated software in many countries around the world not only causes damage to manufacturers but also helps to develop illegal activities. A quick look at the

black websites of hacker groups, people can find countless software cracking tools, unauthorized network penetration pages, embedded Trojans to websites, even teaching how to create virus with extremely rich source program library.

Observing the 20-year panorama of the world virus, we cannot help but wonder. Social development, large information technology entails increasing activity in the underground world of hackers. Nowadays, no one dares to guarantee the absolute safety of any system, including those that were once called "inviolable". If not, why are the most advanced networks of highly developed countries such as the US, Europe and South Korea still being attacked by hackers?

The more society develops, the more complex human relationships are. If in the twentieth century, world wars were only to resolve conflicts of two forces, then in the 21st century, people must suffer more disasters: ethnic war, religious conflict, violence terror, terrorism . Opposition forces themselves have deep differentiation. In the information technology world too, today's security war is not simply a battle between computer viruses and anti-viruses but also a tense confrontation among hacker groups. The fact that the US Air Force mistakenly shot the Chinese embassy in Yugoslavia triggered a fierce battle among hacker groups in many countries on the Internet. After 9/11, the results of an investigation by US security agencies revealed that terrorist groups had once contacted each other by the Internet. There is a theory that they used computer viruses to steal intelligence from various sources in preparation for the attack. Some hackers use the name Bin Laden to name the virus to issue a warning message to the world! Military militants expect future wars to separate the attack on the opponent's computer network, paralyzing the communication system and controlling the enemy's military hardware. This is not fiction because isn't the Internet originating from the military network of the US military?

So the answer to the human factor belongs to the problem of awareness. If you say that, you will have to say: "The problem of computer viruses eventually returns to the social problem?". Indeed, when people will give up their evil ambitions, crime will decrease, society will be more stable and safe. It is also an ideal social image that people desire to build for thousands of years. Every state is based on a certain philosophical doctrine. Each theory has a way to resolve conflicts in different human social life. But they all want to build a stable and sustainable society. Only remaining issue is time.

We can believe in the future of a society that is absent from hackers. This is completely grounded in the past few years when the ranks of Vietnamese hackers have made important changes. Instead of writing viruses to destroy the world, Vietnamese hackers have joined the famous IT companies, or switched to security research. This is a very good sign for Vietnam Internet in the context of world hackers constantly attacking and destroying domestic systems. The fact that Vietnamese hackers participated in clarifying the case of iCMS in 2005 is also a microcosm of the safe information technology world. Through this event, some hackers gave up the underworld to come to light, asking for the return of fairness for the game.

**Epilogue**

Over the past twenty years humanity has witnessed many great events, including achievements and losses.The world seems more fragile, more risky.Computer viruses are also more malicious.If mankind has to deal with terrorism, riots and natural disasters every day, computer users must be vigilant with all kinds of attacks and harassment of abusive computer networks and computers. Mobile device.Where does the future of computer viruses go?Obviously they will go along with the development of human society.Computer virus is a product of human beings, embodying human sin.When people clean up their sins, the virus will have no reason to exist.

SAFETY INFORMATION 2006 WHAT IS NEW?

In early 2006, the annual international conference on information security (ATTT) was organized by IBC - a member of the Information Systems Audit and Control Association - at Bangkok (Thai Land).Mr. Vu Quoc Thanh, director of Misoft company, the first Vietnamese to attend this conference, said:
The 2006 ATTT conference forecasted the main risks this year. That is:
1. Mail bombs and malicious mail (related to email)
2. Spyware
3. Attack phishing and pharming
4. Hackers attack Google users
5. Risk of using peer applications
6. The risk of wireless local area network
7. Quick message (spam IM)
8. Attack of viruses and computer worms
9. The risk of mobile devices.

Many speakers emphasized on two types of particularly dangerous attacks: Botnet and Zero-day-attack. A botnet is a network of many computers infected with "bot" (shortened from the robot), which is a piece of code capable of hiding itself in a computer and executing remote commands. Sometimes, after infection, it stays in the system for several years waiting for the opportunity to function, so it is difficult to detect.
Zero-day-attack only attacks can appear on the same day of announcing new weaknesses (usually with the corresponding patch but sometimes not enough). The likelihood of success of these attacks is very high because even when the new patch is published, not everyone can "patch" on the first day. Since the new weakness, in 6 days the "crook" researched the attack code, and the manufacturer must after 54 days to release the patch.
In terms of ATT services, it is said that the trend of outsourcing network security management services, especially those that require high network security and require fast response (like financial institutions goods and government).
**PV implementation**

**Truong Minh Nhat Quang**