МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МАТЕРИАЛЫ
VIII Международной молодежной научной
конференции
«МАТЕМАТИЧЕСКОЕ
И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
ИНФОРМАЦИОННЫХ,
ТЕХНИЧЕСКИХ
И ЭКОНОМИЧЕСКИХ СИСТЕМ»

Томск, 26–30 мая 2021 г.

Под общей редакцией И.С. Шмырина

Томск
Издательство Томского государственного университета
2021

VIII. ПРОГРАММНЫЕ И АППАРАТНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

DOI: 10.17223/978-5-907442-42-9-2021-34

EVOLUTION OF COMPUTER VIRUSES

Chikalova S.V., Tkachuk P.R., Lavrinenko M.D.

Tomsk State University

chikalova.sveta@mail.ru, tkachuk_polina@bk.ru, mila-gygy@mail.ru

Introduction

Today, the massive use of personal computers, unfortunately, is associated with the emergence of self-replicating virus programs that interfere with the normal operation of the computer, destroy the file structure of disks and damage the information stored in the computer. Increasingly, there are reports in the media about all sorts of pirate tricks by computer hooligans, about the emergence of more and more sophisticated self-distributing programs.

A computer virus is a type of malware that can inject itself into the code of other programs, system memory areas, boot sectors, and distribute copies of itself through various communication channels.

The creation and distribution of malicious programs (including viruses) is prosecuted in Russia in accordance with the Criminal Code of the Russian Federation (Chapter 28, Article 273).

Nowadays, things are changing too quickly, so we consider it necessary to compare one of the first computer viruses with one of the last.

1. Formulation of the problem

This paper examines one of the first computer viruses, the Morris worm, and one of the latest computer viruses, WannaCry. On the basis of the studied theoretical aspects and generalization of theoretical material, viruses are compared, their similarities and differences are assessed. The aim of the work is to study the influence of computer viruses on the operation of computers, this study will help to deepen knowledge in the field of the theory of computer viruses.

2. Morris worm

One of the earliest computer viruses is the Morris Worm, which was written by Cornell University graduate student Robert Tappan Morris and launched at about 6:00 pm on November 2, 1988 at the Massachusetts Institute of Technology [1].

Morris's father was an outstanding programmer. He has worked in cryptography, worked at Bell Labs, and helped develop Multics and Unix. At the time of the cyberattack, Robert's father was in a senior position in the division responsible for IT security of federal government systems. That is, the future programmer had someone to learn from.

2.1. Morris worm attack method

The Morris worm only infected the Unix operating system, exploiting known vulnerabilities in programs such as: Sendmail – email of the time, Finger is a utility that allows users to obtain information about other users, as well as weak passwords, which were often a repetition of a login consisting of a name and the user's last name, or some popular word. The worm completely paralyzed the system by repeatedly rewriting its own code and launching several copies of itself at the same time, which clogged memory and clogged network channels. A peculiarity of the Morris worm is that the computer could become infected several times, gradually reducing the system's performance, eventually disabling it.

Attempts to investigate the problem and eliminate malicious files failed for a long time due to the fact that system files were frequently updated, changed, or information was destroyed.

2.2. The purpose of the Morris worm

Interestingly, the worm was not originally designed as a super-effective virus; according to Robert Morris, it was only for educational purposes, as an experimental project. It all happened because of the carelessness of the administrators and the mistake of the creator. The error was that the virus had a special spreading mechanism: the program, before introducing itself into the system, had to ask if there is already a copy of it in this system, but instead of giving a positive answer with an unambiguous command, Morris added a randomizer to the code, which in one of the seven cases of a positive answer still loaded the program into the system. This led to the fact that many devices were infected several times.

2.3. Removing the Morris worm

The activity of the worm was easy to detect due to specific security flaws in standard servers. As a result, within twelve hours after the beginning of the infection, the worm was able to catch, decompile, and develop a number of countermeasures (the simplest is to rename the cc compiler so that the worm cannot compile its "head"). For troubleshooting, leading American information technology specialists were assembled, who managed to completely fix the problem in two days, creating a special program that ultimately destroyed the virus.

2.4. Morris worm damage

Robert Morris really had no idea that he would create a virus of this magnitude and was himself afraid of what he had done. As follows from the report on the results of the investigation of the incident, he made some attempts to stop the epidemic, although the "switch" was not provided. Robert, as soon as he learned about the seriousness of the situation, called his friend with a request to publish an anonymous apology and a guide to "treatment", but he did not go into direct contact and did not inform those in charge.

The Morris worm practically paralyzed computers on the network for up to five days. Computers were paralyzed for at least 8 million hours and over 1 million hours [2] were spent restoring systems to work. Total losses in monetary terms were estimated at about \$98 million, they were the sum of direct and indirect losses.

Direct losses included (\$32 million): stopping, testing and rebooting 42700 machines; identification of the worm, deleting, cleaning memory and restoring the performance of 6200 machines (this is about 10% of all computers connected to the network at that time); analysis of the worm's code, disassembling and documenting; fixing UNIX systems and testing.

Indirect losses were attributed (\$66 million): loss of computer time due to lack of access to the network; loss of user access to the network.

As for the punishment of Robert himself, then in 1989, Robert appeared in court, becoming the very first person charged under a new article on computer crimes – the Computer Fraud and Abuse Act. He faced up to five years in prison and a quarter of a million dollars in fines. But he eventually received 3 years and a \$10 thousand fine, and was also sentenced to 400 hours of community service (the programmer considered this punishment excessive, but the appeal was rejected).

Why did Morris avoid the real deadline that the public demanded? Because Robert had no criminal plan and was not hiding anything.

3. WannaCry Computer Virus

Among the huge number of malicious programs, there are unique individuals. Having studied the most famous ones, we present you one of the most dangerous viruses of the last decade.

WannaCry (also known as WannaCrypt, WCry, WanaCrypt0r 2.0, and Wanna Decryptor) is a malware, network worm, and ransomware that only infects computers running Microsoft Windows. After infecting a computer, the worm's program code encrypts almost all files stored on the computer and offers to pay a ransom in cryptocurrency to decrypt them. If the ransom is not paid within 7 days from the moment of infection, the ability to decrypt files is lost forever [3].

An early version of this virus, called WeCry, appeared in February 2017 and extorted 0.1 bitcoin (\$177 at current exchange rates). WanaCrypt0r is an improved version of this malware, in which attackers can specify any amount and increase it over time. The developers of the virus are unknown and it is not a fact that they are behind the attacks. They may well sell malware to anyone who wants it for a one-time payment.

The mass distribution of WannaCry began on May 12, 2017 – first of all, they attacked computers in Spain, and then in other countries. In Russia, ministries (Ministry of Internal Affairs of Russia), MegaFon suffered. The information systems of Russian Railways were affected, but the worm quickly localized and did not affect train traffic. In addition, computers in the UK, Spain, Italy, Germany, Portugal, Turkey, Ukraine, Kazakhstan, Indonesia, Vietnam, Japan and the Philippines were affected by the virus.

Over 98% of WannaCry ransomware infections occur on computers running Windows 7, with over 60% of infections affecting the 64-bit version of the OS. Such data were released by Kaspersky Lab analysts. According to statistics, less than 1% of infected computers are running Windows Server 2008 R2 and Windows 10 (0.03%).

The WannaCry worm exploits a vulnerability in Windows operating systems to infect computers. The WannaCry worm itself was created and launched by unknown attackers using information stolen from the National Security Agency.

After penetrating the folder with documents and other files, the virus encrypts them, changing the extensions to .WNCRY. The malware then requires the purchase of a special key, which costs between \$300 and \$600, threatening to delete the files otherwise.

In general, WannaCry is an exploit that is used to infect and spread, plus an ransomware that is downloaded to the computer after the infection has occurred.

This is an important difference between WannaCry and most other ransomware. In order to infect your computer with an ordinary, let's say, ransomware, the user must make some mistake – click on a suspicious link, allow executing a macro in Word, download a dubious attachment from a letter. You can get infected with WannaCry without doing anything at all.

3.1. WannaCry attack method

The malware scans Internet sites for computers with open TCP port 445, which is responsible for supporting the SMBv1 protocol. Having found such a computer, the program makes several attempts to exploit the EternalBlue vulnerability on it and, if successful, installs the DoublePulsar backdoor, through which the executable code of the WannaCry program is loaded and launched. On every attempt to use it, the malware checks for the presence of DoublePulsar on the target computer and, if detected, downloads directly through this backdoor.

It encrypts files of various types, including office documents, photographs, films, archives and other file formats, which may contain potentially important information for the user. Encrypted files are given the .WCRY extension (hence the name of the ransomware) and become completely unreadable.

After that, he changes the desktop wallpaper, displaying there a notification about the infection and a list of actions that supposedly need to be performed in order to return the files. WannaCry scatters the same notifications in the form of text files among folders on the computer so that the user does not miss it.

After completing the encryption process, the program displays a window with a request to transfer a certain amount in bitcoins (equivalent to \$300) [4] to the specified wallet within three days. If the ransom is not received in a timely manner, its amount will be automatically

doubled. On the seventh day, if WannaCry is not removed from the infected system, the encrypted files are destroyed.

The ransom payments are pointless, as the individual keys will never be sent and the files will remain encrypted.

3.2. The purpose of WannaCry

The action of the Wanna Cry virus is aimed at getting on a computer, encrypting the files on it, and extorting a ransom for their decryption.

3.3. Removing WannaCry

The 22-year-old blogger known on the Internet as MalwareTech was analyzing the malware code and noticed that the software was trying to reach an unusual web address – iu-qerfsodp9ifjaposdfjhgosurijfaewrwergwea.com – but that address was not linked to the website because it was not identified [5].

Whenever the malware tried to connect to the mysterious website, an error would occur and the virus would act, causing damage.

As an experiment, MalwareTech decided to spend \$10 69 cents and registered the specified web address. As the owner of the web address, he gained access to analytical data and gained an understanding of the scale of online extortion.

But this discovery was not the only one – he soon found that after registering the web address, the spread of the malware stopped.

MalwareTech believes that the malware did not self-destruct, but was "frightened" by the so-called virtual machine – a protected platform used, among other things, to detect viruses and read their program code.

A real computer cannot access the meaningless address iu-qerfsodp9ifjaposdfjhgosurijfaewrwergwea.com, unlike a virtual machine, which is able to simulate connecting to it as a genuine website.

Recently, malware creators have been embedding a special verification code in them to see if the machine they have entered is virtual. If so, the virus is not activated so as not to be destroyed.

"The malware stops immediately to prevent further analysis," MalwareTech writes on its blog. "Because of my logging, all these viruses thought they had entered the virtual machine and logged out. ... So we are inadvertently prevented the spread of ransomware. "

The WannaCry virus can be removed, but all files that were encrypted with WannaCry are still not decrypted.

Experts also warn of the possible appearance of new, more advanced modifications of WannaCry.

Experts from Kaspersky Lab and the antivirus company Symantec, based on a tweet published by Google researcher Neil Mehta, noted that the WannaCry code signatures coincide with a code signature allegedly used in February 2015 by the Lazarus Group, an alleged connection with the DPRK government.

Linguistic analysis of the text of the ransom demand by specialists from the American cybersecurity company Flashpoint showed that the main language of the authors of WannaCry is most likely the southern dialect of Chinese.

3.4. Damage from WannaCry

According to experts, in the first four days of a large-scale cyberattack, about 300 thousand users in 150 countries of the world were affected. The total damage is estimated at \$1 billion.

4. Comparison and analysis of these two viruses

The development of technology does not stand still, computers have changed a lot since the beginning of their first appearance (1927), their capabilities have expanded, they have become more productive, faster, and multifunctional.

Thanks to technological progress, PCs have fewer weaknesses, which is why viruses are becoming more dangerous and sophisticated.

We are comparing two network worms, the Morris worm and the WannaCry worm, for more accurate analysis.

Similarity of viruses:

The Morris worm and WannaCry belong to the same type of malware. Both viruses are worms.

Explanation: A worm is a subclass of a virus, meaning every worm is a virus, but not every virus is a worm. The virus multiplies on its own, it can gradually infect files not only within one computer, but also spread to other devices. The worm, on the other hand, multiplies without infecting other files; it is injected onto a specific PC. The main difference is in the code. The worm has its own code, while the virus injects itself into files that are already in the system [6].

Differences between viruses:

1. The WannaCry code is ahead of the Morris worm in complexity. As described earlier, a bug was made in the code of the first virus, leading to an overflow of memory, which simply showed the imperfection of computers of that time. The WannaCry code was deliberately complex.

2. The goals of the creators of network worms were different. The creators of WannaCry demanded a ransom for decrypting the data, and Robert Morris, creating the Morris worm, acted solely for educational purposes.

3. Elimination of WannaCry happened only partially, since the virus is new and its modifications are still taking place. If we talk about the Morris worm, after the discovery of the problem, the specialists found a solution within 2 days.

4. The consequences of the impact of WannaCry are more global, since even if the network worm is removed, the files will not be decrypted. To remove the Morris worm, it was necessary to take a number of countermeasures, after which the system was not disrupted or data was lost.

5. The total monetary damage caused by the Morris worm and WannaCry, adjusted for inflation, is different. At the 2017 rate for the Morris worm, the damage would be approximately \$217 million, which is about 21.7% of WannaCry's total damage.

Conclusion

Thus, with each passing year, viruses become more sophisticated and more difficult to get rid of. They cause serious financial damage and cause PC crashes, so users need to be vigilant. There are viruses, but there are also antiviruses that must be installed and used to avoid data loss, collection of personal information about you, and computer malfunctions. After collecting data and conducting a comparative analysis, we came to the conclusion that our hypothesis was indeed confirmed. The WannaCry virus is more dangerous than the Morris worm.

REFERENCES

1. Morris worm [Electronic resource]: website / Wikipedia – URL: https://en.wikipedia.org/wiki/Morris_worm (date accessed: 29.04.2021)
2. Morris worm — он был первым [Electronic resource]: website / Habr – URL: <https://habr.com/ru/post/160337/> (date accessed: 29.04.2021)
3. WannaCry ransomware attack [Electronic resource]: website / Wikipedia – URL: https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (date accessed: 29.04.2021)
4. Эпидемия шифровальщика WannaCry: что произошло и как защититься [Electronic resource]: website / kaspersky.ru – URL: <https://www.kaspersky.ru/blog/wannacry-ransomware/16147/> (date accessed: 30.04.2021)
5. "Случайный герой" рассказал, как он остановил вирус WannaCry [Electronic resource]: website / bbc.com – URL: <https://www.bbc.com/russian/news-39909763> (date accessed: 01.05.2021)
6. Eugene H. Spafford The Internet Worm Program: An Analysis [Electronic resource]: website / spaf.cerias.purdue.edu – URL: <https://spaf.cerias.purdue.edu/tech-reps/823.pdf> (date accessed: 03.05.2021)