INTRODUCTION TO THE THEORY OF COMPUTER VIRUSES

Andreia-Cristina SIREȚANU[1], Andrei-Cristian SĂRĂTEANU[2*], Gabriel GÎTLAN[2]

[1]*Department of Software Engineering and Automation, Software Engineering FAF-211, Faculty of Computers Informatics and Microelectronics, Chișinău, Republic of Moldova*
[2]*Department of Software Engineering and Automation, Software Engineering FAF-213, Faculty of Computers Informatics and Microelectronics, Chișinău, Republic of Moldova*

*Corresponding author: Andrei-Cristian Sărăteanu, andrei-cristian.sarateanu@isa.utm.md

Summary: *This article contains structural descriptions about the most popular viruses that have touched the world. Some of them could damage your computer hardware, steal your money or just have access to your personal data. All viruses are classified in exact types in dependence of their harm effect and way of infection. As technologies are evolving, computer diseases become more dangerous, that's why the world needs higher levels of security and more qualified antiviruses.*

Keywords: *computer virus, hardware, damage, security*

Introduction

The problem with computer viruses started in 1971, when the first virus named “Creeper” was created. Viruses differ from each other with the level of infection and risk that all computer users face. It may happen to people when they receive an email with an attachment to be downloaded, then their computer has slowed to a crawl or a fraudulent charge on credit card could happen. Computer viruses can cause millions or even billions of dollars in economic damage and even information theft.

The worst case of virus aftermath is damaging or even destroying the hardware of the computer, which can lead to data loss. In personal use it does not have very high danger, but when a server computer is damaged it can lead to vulnerability of money stealth and other already known teracts. To avert contact with a virus, people should exercise caution when surfing the web, downloading files, and opening links or attachments. A computer infection can remain numb on the computer, without giving any significant indications or harmful effects. In case it happens When an infection enters your computer Infections can infect other computers in the same organization. Getting passwords or information, logging keystrokes, misinterpreting registration, sending spam emails to your email contacts and taking control of your device are just some of the confusing and annoying things that can cause infection. To assist stay safe, they should never download text or email attachments that you’re not expecting, or files websites that they don’t trust.

The technologies were evolving in a very fast way during the last 50 years,the softs was evolving and computer viruses were doing the same. So, the history of viruses becomes bigger every year and figure 1 represents the most dangerous and famous viruses arranged on the chronological axis.

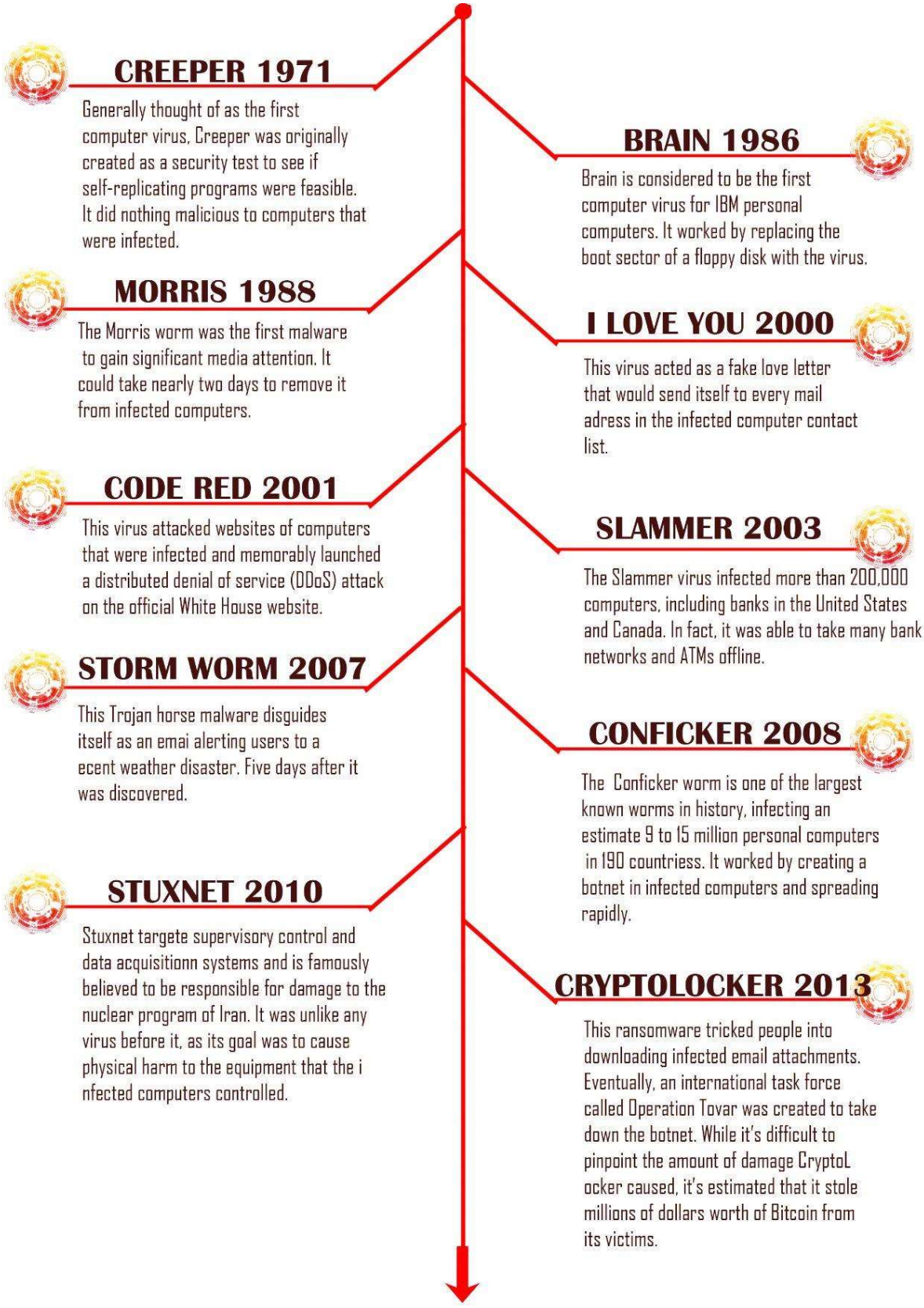

Figure 1. History of Computer Viruses

For years, in the IT sphere appeared a big variety of viruses, each having special features and, of course, having their own target. So it was necessary to divide them in types, that is represented in the following table 1:

Table 1

Computer Viruses Classification

Type	Description
Executable Virus	*Viruses are self-replicating programs that are embedded in software programs. Once a virus infects a host program, it waits for a predetermined time to deliver its download while it replicates on the computer or network it has compromised. Executable viruses are no longer as common in modern operating systems as they used to be. Although rare, they are still found in the wild.*
Macro Virus	*A macro virus is a class of infection that infects Microsoft Office-based products using built-in Visual Basic functionality to spread across a company's network and email system. This class of viruses was seen in the wild in the late 1990s before finally being brought under control by a series of security updates to Microsoft products and improved detection methods from antivirus vendors.*
Boot-Sector Virus	*In the late 1980s and late 1990s, boot sector viruses were known to be the hardest to detect and remove. Their ability to mount and then camouflage with sophisticated detection techniques has allowed them to flourish longer than other types of viruses. This style of attack has seen a resurgence in nature over the past 2 years and is often not noticed by even the highest rated antivirus providers.*
WORM	*Computer worms are a class of computer viruses that can spread not only through an internal network but also through external networks such as the internet. A worm can be a standalone program that runs independently of the executing host.*
Trojan horse	*Trojan horse viruses are so named because the actual malware is programmed into innocent software which is one of the browser's toolbar's many technologies. After the carrier software installs a virus on the host system, the virus delivers its payload. Trojan viruses do not always reproduce, they often expect the end user to initiate an action that allows them to install themselves.*
Malware	*Malware refers to a category of viruses that appeared in the first decade of the 21st century with the advent of social networks and the everyday use of computers. The damage that can spread and occur over the Internet has increased exponentially. This has caused malicious programmers to create sophisticated programs that take control of your computer, flood advertising systems and other malicious programs, and create chaos. This morphed into another version of malware, sometimes called ransomware, these sophisticated programs would mimic legitimate antivirus and security programs in an attempt to extort money from the computer user.*
Browser redirects	*Browser redirects are malicious code embedded in websites that govern your browser's website and search standards on websites that are not chosen by the end user, which generates search revenue for the entity responsible for the malicious code.*

Worst Computer Viruses

There are a ton of PC infections that show up from one side of the planet to the other. The most well-known are viewed as those that truly hurt more individuals. The absolute most perilous infections are thought of: Morris Worm, njRAT, ILOVEYOU.

1) Morris Worm, a virus that is also considered the most established PC worm appropriated by means of the Internet. It likewise brought about the first lawful offense conviction in quite a while under the 1986 Computer Fraud and Abuse Act.

This worm was composed by an alumni understudy at Cornell University, Robert Tappan Morris, and sent off on November 2, 1988. The expense of the harm was $100,000-$10,000,000. Clifford Stoll[1], a frameworks head known for finding and hence following the programmer Markus Hess three years sooner, helped battle the worm, writing in 1989 that, "I studied the organization, and observed that 2,000 PCs were contaminated in fifteen hours or less. These machines were dead in the water, pointless until cleaned. Also, eliminating the infection frequently took two days."[2] Stoll remarked that the worm showed the risk of monoculture, as "Assuming every one of the frameworks on the ARPANET ran Berkeley Unix, the infection would have handicapped each of the 50,000 of them [3]. The Morris worm has in some cases been alluded to as the "Incomparable Worm," because of the overwhelming impact it had on the Internet around then, both in by and large framework personal time and in mental effect on the impression of safety and dependability of the Internet. The name was derived from the "Incomparable Worms" of Tolkien: Scatha and Glaurung. The code of infection can be found on github [4].

2) njRAT is a remote access apparatus (RAT) or trojan which permits the holder of the program to control the end-client's PC. It was first found in June 2013 for certain variations followed by November 2012. It was made by a hacking association from various nations called Sparclyheason and was regularly utilized against focuses in the Middle East [5]. It can be spread through phishing and tainted drives. This device is publicly released at the github page [6].

The main features of njRAT are to:

- Manipulate and change files
- Open a remote shell through SSH, allowing the attacker to use system commands
- Take passes stored in apps and web browsers
- Kill processes with task managers
- Record the computer's microphone and camera
- Manipulate the registry
- Log keystrokes

In the current days it's exceptionally challenging to arrive at documentation[7] on the best way to utilize it, on the grounds that the organization of the most well-known destinations are eliminating the articles about this, to reduce the quantity of robotic assaults. Some of them are:

- A flood of njRAT assaults was accounted for in India in July two thousand fourteen. While trying to handicap njRAT's abilities, Microsoft brought down 4.000.000 sites in two thousand-fourteen while endeavoring to channel traffic through no-ip.com spaces.
- In March two thousand sixteen, Softpedia announced that spam crusades spreading remote access trojans, for example, njRAT were focusing on Discord. In October two thousand twenty, Softpedia additionally announced the presence of a broke VMware download that'd download njRAT by means of Pastebin. Ending the cycle would crash the PC.
- An Islamic State site was hacked in March two thousand seventeen to indicate a phony Adobe Flash Player download, which rather downloaded the njRAT trojan[8].

3) *ILOVEYOU,* sometimes called Like Bug or Like Letter for you, is a computer worm infecting two out of ten million Windows computers as of May 5, at a cost of two thousand. It started spreading like an email titled "ILOVEYOU" and "LOVE-LETTER-FOR-YOU.TXT.vbs.". Opening the connection initializes the Visual Basic content. First, the worm damages nearby machines by overwriting non-standard documents. (including Office Notes and Picture Notes) but will hide the MP3 recording instead of delete it) Then, at this point, the worm reproduces itself in all Windows address books used by Microsoft Outlook, allowing it to spread much faster than other email worms of the past. The source code of the virus can be found on github[9].

Conclusions

Virus attacks seem simple to expand in a very brief time, can be designed to leave tiny traces in most modern systems, are effective against modern security policies for multi-level , and only require a minimal experience to be implemented. Their potential threat is serious and they can spread very quickly through a computer system. It appears that they can spread through computer networks in the same way as they spread through individual computers, and thus pose a widespread and fairly direct threat to many systems today.

Acknowledgements. We want to show our deepest gratitude for the perseverance, integrity and people-loving nature of Mrs. Gogoi Elena, these are just a few of her qualities that continue to inspire us.

References:

1. GRAHAM, P., "FWIW the article on the worm is mistaken". [online]. [accessed: 05.03.2022]. Available: https://twitter.com/paulg/status/1323246618326507524
2. BRENDAN P., "Zen and the Art of the Internet: A Beginner's Guide to the Internet, First Edition". [online]. [accessed: 06.03.2022]. Available: https://archive.org/details/zenartofinternet00keho
3. FBI DEPARTMENT, "FBI data about Morris Worm attacks". [online]. [accessed: 01.03.2022]. Available: https://www.fbi.gov/history/famous-cases/morris-worm
4. ARIALDO M., "Morris Worm source code". [online]. [accessed: 03.03.2022]. Available: https://github.com/arialdomartini/morris-worm, https://github.com/CSE3320/Morris-Worm
5. CIMPANU C., "RAT Hosted on PasteBin Leads to BSOD". [online]. [accessed at 03.03.2022]. Available: http://news.softpedia.com/news/rat-hosted-on-pastebin-leads-to-bsod-509803.shtml
6. SPARKLY H., "njRAT Source Code". [online]. [accessed at 03.03.2022]. Available: https://github.com/mwsrc/njRAT
7. SPARKLY H., "njRAT Documentation". [online]. [accessed at 03.03.2022]. Available: https://any.run/malware-trends/njrat
8. SPARKLY H., "njRAT Download Page". [online]. [accessed at 03.03.2022]. Available: https://github.com/OneParsec/njRAT
9. ONEL DE GUZMAN, "ILOVEYOU Source Code". [online]. [accessed: 03.03.2022]. Available: https://github.com/onx/ILOVEYOU