THE ANNALS OF "DUNĂREA DE JOS" UNIVERSITY OF GALATI
FASCICLE III, 2022, VOL. 45, NO. 1, ISSN 2344-4738, ISSN-L 1221-454X
ELECTROTECHNICS, ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS
Article DOI: ***https://doi.org/10.35219/eeaci.2022.2.04***

DIGITAL VIRUSES VS BIOLOGICAL VIRUSES – A LITERATURE REVIEW

Cătălin Anghel[1], Paul Iacobescu[2], Andreea Alexandra Anghel[3]

[1] Department of Computer Science and Information Technology, University "Dunărea de Jos" of Galati – Romania, 2 Științei, 800146 Galati, Romania*
[2] School for Doctoral Studies in Engineering, University "Dunărea de Jos" of Galati
[3] "Mihail Kogălniceanu" National College, Galati, Romania
[*]Corresponding author e-mail: catalin.anghel@ugal.ro

Abstract: Computer viruses and biological viruses are bugs that make our lives difficult. This paper contains a brief review of the literature aimed to identify the relevant pieces of knowledge, differences and similarities between computer viruses and biological viruses. Also point out the potential intelligent behavior of both biological and computer viruses.

Keywords: computer viruses, biological viruses, artificial intelligence, viruses intelligence, computer malware.

1. INTRODUCTION

The goal of this paper is to conduct a comprehensive literature review comparing human viruses and computer viruses. The purpose of this review is to explore and compare the similarities and differences between these two types of viruses and how they both impact their respective hosts. The paper will examine the nature, transmission, and impact of both human viruses and computer viruses and how these viruses have evolved over time.

This review will also discuss the measures taken to prevent and control the spread of these viruses, including the development of vaccines and antivirus software. Ultimately, the objective of this paper is to gain a deeper understanding of the parallels and contrasts between human viruses and computer viruses and to shed light on the ongoing battle against these dangerous entities.

Viruses seem to exist solely to wreak havoc on society and bring suffering to humanity, whether we are talking about computer viruses or biological viruses. Computer viruses have created problems related to computer systems setting the IT specialists on fire. Biological viruses have always been a great threat for humanity, giving the doctors a hard time.

However, we rely on specialists in both fields. IT and medicine fight a continuous battle and struggle to find methods to prevent, treat, counteract or immunize these threats that affect humanity.

Computer viruses are becoming more intelligent and sophisticated whereas biological viruses are mutating, which makes them harder to diagnose and also more difficult to treat.

"VIRUS" stands for Vital Information Resources Under Siege. A computer virus is a man-made computer-program, or a piece of code that is loaded onto your computer without your knowledge and run against your consent. Virus has a property to replicate itself and spread itself from one computer to another computer.

Computer viruses have the same purpose as the biological viruses and use algorithms in order to multiply, spread and infect. Furthermore, hackers use computer viruses to gain control of computers and obtain vital information stored on it, in order to break them or to obtain financial benefits.

In chapter two we present the history and the most representative computer and biological viruses the impact on society, economy and individuals. Chapter three analyses similarities between computer and biological viruses, how they replicate themselves to spread and infect other systems or organisms, and how they cause harm. Chapter four evaluates the economic and social impact of computer and biological viruses. In chapter five, we present the potential intelligent behavior of both types of viruses and how they can cause harm to human hosts and computer systems and networks. In the final chapter, we conclude the importance of research in the information technology domain and medicine to counter threats in both fields.

2. BIOLOGICAL AND COMPUTER VIRUSES

Biological viruses existed long before computer viruses and have probably existed since living cells first evolved, but the scientific study of viruses and the infections they cause began in the closing years of the 19th century.The first biological virus (Iwanowski D., 1892) has been described as a "non-bacterial pathogen infecting tobacco plants" by the Russian botanist Dimitri Ivanovsky in the year 1892 and discovered (Beijerinck M. W., 1898) as a „tobacco mosaic virus" by the dutch botanist Martinus Beijerinck in the year 1898.

With the development of information technology, computer viruses have emerged. The first academic work on the theory of self-replicating computer programs (John von Neumann, 1966) was made by the mathematician John von Neumann in the year 1949 and published in 1966.

The first computer virus (History of malicious programs, Internet Archive), the Creeper virus, was detected on ARPANET, a US military computer network that was the forerunner of the modern Internet, sometime in 1970. This virus was able to gain access independently through a modem and copy itself to the remote system. Infected systems displayed the message, "I'm the Creeper: catch me if you can."

Disease and illnesses have plagued humanity since the earliest days. Vaccines and antiviral drugs helped us prevent wide spreading of some infections. In other cases, there are no vaccines or drugs to treat certain new viruses.

In the case of computers, for known viruses there are antivirus programs that identify and annihilate them, though as for new viruses we are still searching for a solution, until then the possibility of infection is very high.

A top 5 biological (Harding A. & Laneser N., 2020) and computer (www.lifars.com, 2020) viruses are presented as follows:

Number 1

Marburg virus was identified by specialists in 1967, when small outbreaks burst among the workers in a laboratory in Germany, who were exposed to infected monkeys, imported from Uganda. It causes hemorrhagic fever and has a mortality rate of over 80%.

CryptoLocker was launched in September 2013, and it spreads through email attachments and encrypts the user's files. Through this dangerous ransomware, the attacker asks for money to decrypt the files.

Number 2

The Ebola virus was identified in 1976 in Africa and it spreads through contact with the blood or body fluids of infected persons. The disease causes hemorrhagic fever, and has a mortality rate of over 90%.

PlugX malware is a Remote Access Trojan and it was first discovered in 2012. It spreads through email attachments and contains backdoors modules for a wide variety of attacks.

Number 3

The Rabies virus was discovered in 1920, it spreads through the saliva of infected animals and it causes inflammation of the brain, and has a 100% mortality rate.

Zeus Gameover malware was identified in 2011, spreads via spam messages or infected drivers and accesses the victim's sensitive bank account data, to steal money.

Number 4

HIV was discovered in 1980, it is transmitted through blood, genital fluids, and breast milk. It affects the immune system, and untreated, leads to death. It is a deadly virus that currently, doesn't have a permanent cure.

Stuxnet worm was identified in 2010, spread via USB sticks, and was originally targeted at Iran's nuclear facilities.

Number 5

Smallpox was eradicated in 1980, but killed one of three people who contracted the virus. It left survivors with deep, permanent scars, and often, blindness.

Mydoom worm was discovered in 2004. It spreads via email or peer-to-peer networks, and creates a backdoor in the operating system.

3. SIMILARITIES BETWEEN COMPUTER AND BIOLOGICAL VIRUSES

Computer and biological viruses have a lot of similarities when we think about the propagation mechanism and the purpose of the infection. Both types of viruses use the same strategies to spread from one host to another, whether it be through direct contact or exploiting vulnerabilities in software. Table 1 presents those similarities whereas table 2 presents potential similarities between computer viruses and biological viruses (Korthof G., 2006).

Table. 1. Similarities between computer viruses and biological viruses

COMPUTER VIRUSES	BIOLOGICAL VIRUSES
SIMILARITIES	
infection of specific targets (computer files)	infection of specific targets (host cells)
attach to .exe or .com files	integrate into DNA
contains executable code	contains genetic code
virus and host use the same software language	virus and host use the same language (genetic code)
contain information, have length expressed in b(ytes)	contain information, have length expressed in b(ases)
source code causes the behavior of a virus	genotype causes phenotype including behavior
a virus has a small size relative to the host software	small genome relative to the host genome
spread to other computers	spread to other hosts
parasitism: copied by the host	copied by the host cell
one virus per file	no re-infection of the same cell
Initially, the infected file is functional	Initially, the infected cell is functional
user does not immediately notice infection	host organism does not immediately notice infection
the software can be made immune to infection	not every cell is infected
specificity for Operating System (Windows, Unix, Linux) or hardware	host specificity (biological species)
different types (groups) of viruses exist	species, families of viruses exist
degrees of harmfulness	different degrees of virulence
difference in susceptibility of computers	difference in susceptibility of individuals and species
anti-virus software on a computer	immune system of the host (animals, plants, bacteria)
percentage of infected files on a computer	viral load (number of viral particles in host organism)
percentage of computers protected by anti-virus software	percentage of individuals in the population immune to virus (vaccinated or acquired immunity)
PCs came first, viruses later	host organism evolved before infecting virus

Table. 2. Potential similarities between computer viruses and biological viruses

COMPUTER VIRUSES	BIOLOGICAL VIRUSES
POTENTIAL SIMILARITIES	
spread via Trojan horse, external disk, e-mail, internet	spread via vector (mosquitos, bats, rats)
mutating virus	virus mutates
activation of the virus depends on the date	seasonal activity of the virus
software version-dependent action	age-dependent action of the virus
virus infects new host software	infection of new host species
anti-virus software comes at a price	the immune system is costly for the organism
arms race virus and anti-virus software	arms race virus and immune system (vaccines development)
virus disables virus scanner	virus interferes with or inhibits immune reaction
hidden presence of virus	latency; dormancy; symptom free period
polymorphic virus	polymorphic virus
stealth techniques to avoid detection	ability to escape detection by the immune system
Darwinian evolution of mutating viruses	Darwinian evolution of mutating viruses
detected by virus	detected by virus

signature	signature
quarantine of infected file	quarantine of an infected person
delete infected file	programmed cell death as a defense against infection
can cause economic damage	can cause economic damage

4. ECONOMIC AND SOCIAL IMPACT

Apart from infecting the target, biological and computer viruses can weaken or destroy the hosts and create important economic and social implications. These implications are a result of the viruses' effects, but also the emergence of alarmist news, excessive publicity, misinformation, etc.

Y2K Bug.

Many programs represented four-digit years with only the final two digits, making the year 2000 indistinguishable from 1900. Computer systems' inability to distinguish dates correctly had the potential to bring down worldwide infrastructures for industries ranging from banking to air travel. This led to gloomy predictions that all the world's computing systems would cease to function, and the year 2000 will be "The End of The World As We Know It – TEOTWAWKI –" (Quiggin J., 2005).

With the approach of Y2K, governments and other authorities have reassured the public that thanks to multi-billion dollar investments, IT systems are ready for a smooth transition into the new millennium and that the Y2K Bug has been solved. These reassurances failed to convince a significant minority of the population, who stored bottled water and canned food as a precaution against a possible disaster, this reaction being a response to the alarmist news (Quiggin J., 2005).

Despite the fact that around $500 billion was spent globally on the Y2K bug, it was eventually concluded that most of the money was wasted and that the Y2K bug was not a complicated problem, but one that was given too much magnitude (Quiggin J., 2005).

WannaCry ransomware

Ransomwares are not something new for us, the first ransomware, the AIDS Trojan also known as PC Cyborg, was created in 1989 by Joseph L. Popp, now known as the 'father of ransomware' (Ransomware History Timeline, KnowBe4.com). But when the ransomware WannaCry arrived on 12 May 2017, chaos was unleashed. In just a few days, this virus infected over 230,000 computers that use Microsoft Windows from 150 countries. The cyberattack affected countless sectors but the medical system was the more damaged part. Operating room equipment, refrigerators for blood storage, MRI scanners, and even the patient care was troubled because a lot of non–critical cases that were not considered an emergency, were diverted of care from certain facilities, impacted by the crisis the ransomware started (Ehrenfeld, J. M., 2017).

This whole situation could have been prevented easily because the security patch update needed to protect the computers against the virus was available before the attack. The patch was released on March 2017 and Microsoft Security Bulletin MS17-010 flagged the patch as a critical update for Windows but, in May 2017, when the WannaCry attack began, many systems were unpatched, therefore vulnerable to the virus (Fruhlinger J., 2022).

The WannaCry ransomware is a good example of how cyberterrorism affects everyday life even though, usually it is not lethal, still impacts our society because it exacerbate perceptions of threat that leads to personal insecurity, fear and anxiety (Gross M.L., Canetti D., Vashdi D.R., 2017).

Covid-19 virus.

A virus that spread globally and caused a pandemic in a very short time.

In addition to the actual SARS-CoV-2 disease, this virus has also created panic among the population. Many people have stocked up on canned goods, flour, sugar, toilet paper, disinfectants, or face masks.

As the number of Covid-19 cases rises, governments are banning large gatherings of people, closing shops, and taking measures to enforce social distancing. This is causing the so-called "panic-buying" that's emptying store shelves quicker than they can be restocked because panic-buying supplies are one way humans have coped with uncertainty over epidemics since at least 1918 during the Spanish flu (McKeever A., 2020).

Diverse international responses to the COVID-19 pandemic have included containment measures including lockdowns, quarantines, and curfews; these have caused numerous industries, including tourism and the hospitality sector, to cease operations. The COVID-19 coronavirus epidemic has devastating human repercussions, but it has also caused economic uncertainty that will probably cost the world economy $1 trillion in 2020 (UN Audiovisual Library, 2020).

Quarantine and preventive measures for SARS-COV-2 have altered people's lives which has affected the young population as follows: according to the report, of the 731 participants aged 18 through 24 years, 49.1% reported anxiety disorder; 52.3%, depressive

disorder; and 46%, Trauma and Stressor-related Disorders. Of the 1911 participants aged 25 through 44 years, 35.3% reported anxiety disorder; 32.5%, depressive disorder; and 36% for TSRD. (Vahia I.V., Jeste D.V., Reynolds C.F., 2020).

The current epidemic is a relatively new stressor or trauma for mental health professionals from a psychopathological perspective. Although the effects of the coronavirus on mental health have not been thoroughly studied, it is anticipated that COVID-19 will have rippling effects, especially based on current public reactions raising concerns of widespread panic and increasing anxiety. (Kontoangelos K., Economou M., and Papageorgiou C., 2020)

Schools, training institutes, and higher education institutions have been forced to shut down in the majority of countries as a result of lockdown and social isolation measures brought on by the COVID-19 epidemic. Both learners and teachers may experience a completely different learning environment when switching from traditional face-to-face learning to online learning, yet they are forced to adjust because there are few or no other options. Through a variety of online channels, the educational system and the teachers implemented "Education in Emergency," forcing them to adopt a system for which they are not prepared (Pokhrel S., & Chhetri R., 2021).

Students, parents, and educators all over the world have been affected by the unforeseen ripple effect of the COVID-19 epidemic as schools have been closed to deal with the global pandemic. Many students are experiencing psychological and emotional distress at home or in their living environment, making it difficult for them to function efficiently. The ideal methods for homeschooling children online have not yet been developed (Pokhrel S., & Chhetri R., 2021).

5. INTELLIGENCE OF VIRUSES

"Viruses are very intelligent. They can think. They do things that we do not expect. They adapt to the environment. They change themselves in order to survive" – Michael Lai, professor of molecular microbiology and immunology and a Howard Hughes Medical Institute Investigator (Cohen J.J. & Foote S., 2021).

However, the intelligence of the biological viruses have always been under question because of the scientist debate about whether they are alive or not.

Because viruses do not use their own energy, some scientists do not consider them alive. But giant viruses like Mimivirus, a causative agent of some forms of pneumonia, can behave in some ways like the one-celled life forms do. The Mimivirus is very complex, is able to repair it's own DNA, can correct reproduction errors, can create mRNA and translate it into proteins, like living cells do. (Lief J., 2012).

Another virus that can be considered intelligent is HIV. Although an enormous amount of research has been done on it, still, there is a lot of unknown about its incredible adaptability. But it is now clear that this very clever virus is able to escape the immune system by directly invading the most intelligent immune cells, attacking the immune system directly and weakening the host.

Throughout all the history of medicine, viruses caused scientists lots of trouble due to their ability to adapt to their hosts, overcome defense mechanisms and take over cellular metabolism. Another characteristic of viruses is their ability to spread from one host to another or from one species to another, leading to the appearance of mutations that can create more efficient ways to exploit the new hosts.

The ability of biological viruses to attack the hosts in the most effective ways, could be compared with the behavior of computer viruses, which learn and adapt to overcome anti-malware tools, and infect computers.

Today's computers are becoming more and more powerful. The evolution of computer hardware and software has allowed hackers to develop more complex malware, capable of analyzing and exploiting large amounts of data.

The development of such applications requires skills, experience and in-depth knowledge but, at the same time create great challenges for cybersecurity professionals to protect networks, systems and software from cyberattacks.

Diogo O. Beltran has predicted that –"By the year 2040, AI will appear on computer viruses that will communicate with each other using a universal Internet language and will be programmed to fuse and mutate into Computer Organs that will later be controlled by powerful search engines (Systems) diffused throughout the Internet" (Sharma S., 2016).

Malware that extends its capabilities is nothing new. Artificial Intelligence technologies such as Machine Learning, allow developers to create adaptive software, capable of revising their source code to adapt to the changes in the real world, changes that were not anticipated when the malware source code was first written.

Artificial Intelligence can be used to build self-learning malware capable of completely altering its tasks as it spreads. This type of virus can analyze security defenses and develop its methods of exploiting vulnerabilities, constantly updating itself as it learns more about the target environment.

Because virus adaptation can occur without human intervention, the task of the anti-malware software to detect, neutralize or eradicate malware software, becomes more and more challenging.

Malware is getting more complex as it can use heuristic algorithms to dynamically change the source code to prevent detection. The past decade and particularly the past few years has been transformative for artificial intelligence. Considering the evolution of Artificial Intelligence technologies, it is an impossible task to predict how intelligent malware will affect us when developed on a big scale, using these techniques (Baddeley M., *et al*., 2019).

There is very little literature that explicitly mentions the use of artificietal intelligence in malware development. However, the computer virus called Zellome, contained genetics algorithms as a form of brute force approach to generate decryption routine to facilitate its polymorphic behavior. Although this virus was considered a weak one, this approach should be considered as a red flag, because AI-enabled malware could soon be the newest weapon in the threat hacker's arsenal (Pan J.Y. and Fung C.C., 2008).

Although there are currently not many examples of AI-enabled malware documented, the threats that utilize machine learning and AI to find vulnerable systems, evade detection from security products and enhance social engineering techniques, is an important matter we should focus on and a probable scenario that we should to take into consideration (Roy. M., 2019).

Similar to healthcare, where researchers, health care providers and public health authorities work together to describe genetic sequence mutations and find cures for biological viruses, Cyber Security companies spend big money on research and development of products with built-in artificial intelligence to counter such malware.

6. CONCLUSION

This paper is a literature review that compares and analyses the similarities, differences, characteristics and social economic impact between computer viruses and biological viruses. Also point out the potential intelligent behavior of both biological and computer viruses.

Humanity is in a continuous transformation and can no longer conceive its existence without research in information technology domains, implemented in all socio-economic fields and in medicine, to counter biological threats.

The responsibility of researchers active in both fields of activity is closely linked to innovation, research and technological evolution.

The battle against biological and computer viruses continues in both medical and cyber security fields.

7. REFERENCES

Baddeley M., et al., (2019). *Towards a New Enlightenment? A Transcendent Decade*.

Beijerinck, M. W. (1898). *Über ein Contagium vivum fluidum als Ursache der Fleckenkrankheit der Tabaksblätter*. Verhandelingen der Koninklijke Akademie van Wetenschappen Te Amsterdam, 65: pg. 1–22.

Cohen J.J. & Foote S. (2021). *The Cambridge Companion to Environmental Humanities*, Cambridge University Press.

Ehrenfeld, J. M. (2017). *WannaCry, Cybersecurity and Health Information Technology: A Time to Act*, Journal of medical systems – Springer, DOI 10.1007/s10916-017-0752-1.

Fruhlinger J., 2022. *WannaCry explained: A perfect ransomware storm*, https://www.csoonline.com /article/3227906/wannacry-explained-a-perfect-ransomware-storm.html.

Gross M.L., Canetti D., Vashdi D.R. (2017). *Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes*, Journal of Cybersecurity, Volume 3, Issue 1, pg. 49–58.

Harding A. & Laneser N. (2020). *The 12 deadliest viruses on Earth*, www.livescience.com, 04.03.2020.

Iwanowski, D. (1892). *Über die Mosaikkrankheit der Tabakspflanze*. Bulletin Scientifique Publié Par l'Académie Impériale des Sciences de Saint-Pétersbourg. Nouvelle Serie III, St. Petersburg. 35: pg. 67–70.

Internet Archive. *History of malicious programs*. https://web.archive.org/web/20061016141708/http://www.viruslist.com/en/viruses/encyclopedia?chapter=153310937.

John von Neumann (1966). *Theory of Self-Reproducing Automata.* Essays on Cellular Automata, University of Illinois Press, pg. 66–87.

KnowBe4.com. *Ransomware History Timeline*, https://www.knowbe4.com/ransomware.

Kontoangelos K., Economou M., and Papageorgiou C. (2020). *Mental Health Effects of COVID-19 Pandemia: A Review of Clinical and Psychological Traits*, Psychiatry Investigation Volume 17, Issue 6, pg. 491-505.

Korthof G., (2006). *Similarities and Dissimilarities of Computer Viruses and Biological Viruses*, https://wasdarwinwrong.com/korthof78.htm.

Lief J., (2012). *Virus Intelligence: Are Viruses Alive and Sentient?*, https://jonlieffmd.com/blog/are-

viruses-alive-are-viruses-sentient-virus-intelligence.

lifar.com (2020). *Top 10 Most Dangerous Cyber Viruses of All Time*, 22.04.2020.

McKeever, A. (2020). *Coronavirus is spreading panic. Here's the science behind why*, www.nationalgeographic.com.

Pan J.Y. and Fung C.C. (2008). *Artificial intelligence in malware - Cop or culprit?*, Ninth Postgraduate Electrical Engineering and Computing Symposium, (PEECS2008), pp. 181-184.

Pokhrel S., & Chhetri R. (2021). *A Literature Review on Impact of COVID-19 Pandemic on Teaching and Learning*, Higher Education for the Future, Volume 8, Issue 1, pg. 133–141.

Quiggin, J. (2005). *The Y2K scare: Causes, Costs and Cures*, Australian Journal of Public Administration, Volume 64, Issue 3, pg. 46-55, 2005. DOI: 10.1111/j.1467-8500.2005.00451.x.

Roy. M., (2019). *AI-enabled malware is coming, Malwarebytes warns*, https://www.techtarget.com/searchsecurity/news/252465971/AI-enabled-malware-is-coming-Malwarebytes-warns.

Sharma S. (2016). *Fighting virus and malware with artificial intelligence.* Insights Success, https://insights success.com /fighting-virus-and-malware-with-artificial-intelligence.

UN Audiovisual Library (2020). *Geneva/ Covid-19 Economic Impact.* https://www.unmultimedia.org/avlibrary/asset/2539/2539212/.

Vahia I.V., Jeste D.V., Reynolds C.F. (2020). *Older Adults and the Mental Health Effects of COVID-19*, JAMA, doi:10.1001/jama.2020.21753.