analytics

Article

A Comparative Analysis of VirLock and Bacteriophage $\phi 6$ through the Lens of Game Theory

Dimitris Kostadimas [†], **Kalliopi Kastampolidou** [†] and **Theodore Andronikos** [*,†]

Department of Informatics, Ionian University, 7 Tsirigoti Square, 49100 Corfu, Greece; p19kost2@ionio.gr (D.K.); c17kast@ionio.gr (K.K.)

[*] Correspondence: andronikos@ionio.gr

[†] These authors contributed equally to this work.

Abstract: The novelty of this paper lies in its perspective, which underscores the fruitful correlation between biological and computer viruses. In the realm of computer science, the study of theoretical concepts often intersects with practical applications. Computer viruses have many common traits with their biological counterparts. Studying their correlation may enhance our perspective and, ultimately, augment our ability to successfully protect our computer systems and data against viruses. Game theory may be an appropriate tool for establishing the link between biological and computer viruses. In this work, we establish correlations between a well-known computer virus, VirLock, with an equally well-studied biological virus, the bacteriophage $\phi 6$. VirLock is a formidable ransomware that encrypts user files and demands a ransom for data restoration. Drawing a parallel with the biological virus bacteriophage $\phi 6$, we uncover conceptual links like shared attributes and behaviors, as well as useful insights. Following this line of thought, we suggest efficient strategies based on a game theory perspective, which have the potential to address the infections caused by VirLock, and other viruses with analogous behavior. Moreover, we propose mathematical formulations that integrate real-world variables, providing a means to gauge virus severity and design robust defensive strategies and analytics. This interdisciplinary inquiry, fusing game theory, biology, and computer science, advances our understanding of virus behavior, paving the way for the development of effective countermeasures while presenting an alternative viewpoint. Throughout this theoretical exploration, we contribute to the ongoing discourse on computer virus behavior and stimulate new avenues for addressing digital threats. In particular, the formulas and framework developed in this work can facilitate better risk analysis and assessment, and become useful tools in penetration testing analysis, helping companies and organizations enhance their security.

Keywords: game theory; computer virus; biological virus; VirLock; $\phi 6$; polymorphic code

check for updates

Citation: Kostadimas, D.; Kastampolidou, K.; Andronikos, T. A Comparative Analysis of VirLock and Bacteriophage $\phi 6$ through the Lens of Game Theory . *Analytics* **2023**, 2, 853–876. https://doi.org/10.3390/analytics2040045

Received: 29 August 2023
Revised: 16 October 2023
Accepted: 23 October 2023
Published: 6 November 2023

1. Introduction

1.1. Computer Viruses

A computer virus is a widely used term that characterizes malicious computer software. This metaphorical term is based on the observation that the behavior of biological viruses and malicious software has much in common and shares some conceptual characteristics [1].

Biological viruses have many different variations, just like their digital counterparts. Computer viruses have several traits that help in their categorization, usually based on their behavior and infection mechanisms. The way computer viruses infect the host computer also helps in their classification [2,3]. Traits like their target demographic, operational conditions, replication manners, infection mechanisms, infection success rate, and severity, vary considerably, and are used in their categorization and research.

This article investigates the relationship between biological and computer viruses, with a focus on VirLock, a polymorphic ransomware, and its similarities to the $\phi 6$ bacteriophage virus. Linkages between the two viral types are constructed using game theory as a foundation, leading to novel infection management methods and the development of mathematical models for resistance measures. Examining the bio-computational activities of viruses increases our understanding and enables the development of effective computer countermeasures. A computer virus must initially infect the target computer to interact with the host for the first time and begin its replication process. In cases where a virus exhibits traits, such as polymorphic or metamorphic code, or possesses a worm component, the virus's ability to spread appears to be somewhat unpredictable.

It is not necessary for worms to manipulate the target computer software in order to replicate [4]. Unless they consume a significant amount of the computer's resources, their presence will be hinted at by the slow performance. Worms remain active in the computer's memory, and their actions are typically unseen by the user. The most intriguing aspect of worms and viruses with worm components is not merely their rapid self-replication ability but also their capacity to do so without the host computer's user interactions, known as the zero-click type [5,6]. Specific types of computer viruses have the potential to mutate, which in turn leads to better spreading of their population and higher infection rates, while generally improving their already existing traits. This ability to mutate is also observed in biological viruses. Mutation is a typical feature of biological viruses, which has been proven via phylogeny analysis in [7,8]. Mutation is a trait found in viruses with polymorphic and metamorphic codes. Typically, polymorphic code makes unique copies by relying on encryption. The goal of employing polymorphic and metamorphic code is to avoid detection by anti-malware and antivirus technologies. Technically, it is more difficult to achieve the "metamorphic trait" in a virus than the "polymorphic trait." However, the implementation cost may be worth the extra effort because it provides superior protection against antivirus technologies, and evading detection is considerably easier.

1.2. Biological Viruses

Biological viruses are parasitical organisms that gain the ability to reproduce and carry their genetic material, protein, and DNA or RNA, by infecting a host [9]. They translate their RNA into proteins that serve them by using the host's ribosomes since they do not have the ability to synthesize proteins of their own [10]. Viruses can be transmitted through different means, depending on their species [11]. The term "Host range" refers to the number of cells infected by a virus [12]. Usually, a biological virus is dealt with by the immune system of the organism it has infected. Infected organisms could be molecules, animals, plants, as well as humans [13]. Moreover, a good defense method that helps the immune system is the use of vaccines, often used to work against specific viruses. Although the majority of virus mutations have little effect on the general development of the disease, certain alterations may worsen infection severity and undermine current vaccination approaches [14]. Apart from vaccines, as time progresses, antiviral drugs continue to evolve.

When a virus infects a cell, it forces it to directly replicate itself, creating more copies of the virus. What makes up a virus is its genetic material, the capsid, a set of proteins that protect this genetic material, and sometimes external lipids. The extracellular form of the virus is called the virion. Viruses are classified into two types (DNA and RNA, respectively), depending on whether they have a DNA or an RNA genome [15]. The genetic material of an RNA virus is made up of ribonucleic acid (RNA) [16]. A virus can have a lot of different effects on an organism. Causing the death of the host cell is what most of them do. Usually, they do that by using viral proteins to restrict the normal activity of the cell [17,18]. Many viruses cause harm to the host, whereas others may be destroyed without causing adverse effects. There are also viruses that have the ability to infect without causing any changes in the cells [19]. The cells can continue to function normally even when infected, yet they still end up causing the infection to persistently spread. The collection of viruses that infect an organism is termed a virome. The source of infection is identified using a technique called phage typing [20].

Viruses are not transmitted through cell division since they are acellular organisms. Instead, they are transmitted by using the host to create multiple copies of themselves. The host is forced to reproduce the original virus when infected. The interaction of a virus and a host cell is a complex process that takes place in a series of separate phases. Viruses have a basic life cycle [21]. The infection starts once a virus attaches itself to a susceptible host cell. Viruses have attachment proteins or molecules on their surface that recognize and bind to receptors on the surface of the host cells. This attachment is quite selective, with the virus focusing on certain kinds of host cells. That is when the cell type and host range are determined. After that, the virus penetrates the cell. This can happen in a variety of ways, depending on the virus type. Some viruses merge with the host cell membrane directly, whereas others are internalized by endocytosis. In order to disclose its genetic material within the host cell, the virus may need to uncoat itself, losing its outer layers or capsid. After that, the viral genome is exposed and ready for reproduction [22]. The replication and transcription phases of the interaction are where the viral genetic material acquires control of the host cell's machinery. When the virus is replicated, the genome is also multiplied. After they replicate, altered proteins and particles may appear relative to the original form of the virus before the penetration occurred. Newly formed virus particles that are assembled acquire a new final virus structure as well as new functional attributes.

The cycle concludes with the expulsion of mature virions from the host cell. Virus release techniques can vary greatly, involving processes, such as cell lysis, budding from the host cell membrane, or other mechanisms. Once this happens, the cell is killed [23]. The process the host uses to reproduce, so the virus can also be replicated, is called a prophage. Once the virus stops being inactive, lysis happens in the host cell. RNA virus reproduction takes place in the cytoplasm. Each specific virus uses the enzymes it has in order to make copies of the genomes. The virus has the ability to infect a new host cell after lysis, which leads to this cycle repeating itself. Moreover, the virus might mutate during this step [24]. After the immune system of an organism detects a virus, it begins the production of antibodies so that it can suppress the virus. The name of this process is humoral immunity. Whether the body has gotten rid of the virus or not depends on the antibodies that have been produced.

Viruses that can diversify or alter microbial populations are called bacteriophages or phages, and because of those properties, they have been used as antibacterial agents [25]. The host range that some bacteriophages have is only focused on one bacterial strain. Bacteriophages are a group of viruses with double-stranded RNA genomes that infect specific bacteria. RNA viruses consist of segments found in the capsid that form a protein. The virus can be contagious even if different segments are located in different virions [26]. They infect by attaching to the molecules on the surface of the bacterium and entering the cell. Oftentimes, once they enter the cell, they start translating their mRNA into proteins. Virus enzymes assist in destroying the cell membrane. Usually, bacteria use enzymes that can target unknown RNA to protect themselves from this type of infection. Bacteria also have the ability to detect the genomes of viruses that have been encountered in the past, and they can block their reproduction by interfering with the RNA [27,28]. This is what bacteria use to protect themselves from this kind of infection. Bacteria can naturally interfere with the RNA. While a viral RNA is being replicated, certain mutations happen, which could either leave the cell proteins unaffected or contribute to the resistance against antiviral drugs.

1.3. Game Theory

Game theory, along with its extension, evolutionary game theory (EGT), can assist in modeling the behavior of both computer and biological viruses, paving the way for the development of a higher level of protection from them. Its application to realistic scenarios is what makes this concept even more captivating [29]. Characteristics typically found in games have been discerned in the case of biological processes in multicellular organisms like cells and macromolecules (see [30] for an accessible overview). Many biological systems seem to follow certain strategies, as the observation of their moves implies. Of course, during a time span, a player's strategy can change as a result of natural selection. When mutations occur during the cell's lifespan, reversible or irreversible changes to their strategies can take place due to epigenetic transformations. The final outcome of the game is largely determined by the reproductive success of the organism. A succinct introduction to the study of biological systems with the use of evolutionary games can be found in [31]. Numerous traditional games, such as the well-known Prisoner's Dilemma, have been employed to simulate biological circumstances (see [32,33] for references). This extends beyond viruses to include microorganisms and bio-inspired computational models (see [34,35] for more references). Employing nonstandard approaches for analyzing physical systems has deepened our understanding and revolutionized our perspective in many important cases. As an example, we mention that game-theoretic analysis can provide additional insights even when applied to quantum computation (see [36–38] for recent results and more related references).

Contribution. This paper introduces a novel perspective, namely that biological and computer viruses, despite their obvious differences, exhibit many common behavioral traits. Through the correlation of computer viruses to their biological counterparts, this paper aims to offer a fresh viewpoint and advocate for a new and promising vein of research. In this work, we build upon the preliminary investigation of [39], and we demonstrate that the association between the behavioral traits of biological viruses and computer viruses is possible and fruitful. In this research, we focus on VirLock, a ransomware-type computer virus, and its similarities to biological viruses, especially with the well-documented and studied $\phi 6$ bacteriophage virus. Our approach culminates in a thorough examination and analysis of the main similarities and anticipated differences between these two viruses. VirLock is a well-known virus from which many people have suffered. It had a massive impact, which was one of the reasons it was preferred over other ransomware viruses, like WannaCry or Petya. Many respected sources and studies on the subject have extensively investigated VirLock; most antivirus vendors provide particular tools, while other sources exploit the virus in a variety of ways, allowing us to correlate numerous cleaning strategies. Other viruses spread via networks, but VirLock is an excellent non-zero-click example. VirLock has mutable and polymorphic code. This is a crucial trait that not all computer viruses have. $\phi 6$ covers the multidisciplinary length since it has been further addressed in an easily understood manner by a wide range of audiences. $\phi 6$ is also very well-known, with numerous citations, and can be figuratively associated with VirLock's behavior. In addition to improving the variety of tools for evaluating the efficacy of the strategies employed to counter viruses, we anticipate that this line of research will lead to the implementation of novel strategies that, in the end, have proven efficient for combating certain virus types. Of course, there are numerous types of computer viruses, and the same is true for biological ones. To be effective, any framework must have an in-depth understanding of a virus and its method of infection. Worms, for example, have a very similar infectious pattern, and the proposed framework, with appropriate extensions and modifications, could be applied to worms too. Therefore, we believe that the analytical approach presented here can be generalized and adopted to tackle more general scenarios. The formulas and framework can assist in better risk analysis and assessment. For this purpose, they could be integrated into a penetration testing suite, and utilized in penetration analysis reports for digital security assessment. The interested reader is referred to [40–43] for introductory presentations of the scope and capabilities of some of the most well-known and popular modern penetration testing tools. Therefore, the approach initiated in this work can assist companies and organizations to thoroughly evaluate their security risks and enhance the prioritization of their vulnerability management procedures, leading to improved security and facilitating early and safe recovery from such attacks.

1.4. Organization

This paper is organized as follows. Section 1 presents an introduction to the subject and gives many references to previous related works. The introduction contains Sections 1.1–1.3, which provide a succinct overview of computer viruses, biological viruses, and game theory, respectively. Section 2 provides a comprehensive analysis of the VirLock virus and includes subsections describing the most important characteristics of the virus. Section 3 explains how game theory can be used to model VirLock. Section 4 provides a concise introduction to the $\phi 6$ virus, and Section 5 demonstrates how $\phi 6$ can be modeled using game theory. An extensive comparison of VirLock with $\phi 6$, highlighting similarities and differences, is presented in Section 6. Section 7 is devoted to the analytical exposition of the formal mathematical framework. Section 8 briefly touches on the ethical considerations and dilemmas arising when dealing with viruses. Finally, Section 9 summarizes this work and discusses some limitations and prospective future research.

2. The VirLock Virus

2.1. Introduction

VirLock [44] is a computer virus that, when it manages to infect the victim's computer, encrypts the majority of the user's precious files while essentially locking the system. Then, it demands a ransom from its victims to grant them access back to their system and data. This behavior is what classifies this virus as ransomware. VirLock is usually spread through cloud storage and exhibits parasitic behavior as it infects certain supported computer files. From the moment it executes in the host computer, it begins to infect the supported files. It is noteworthy that the way it alters the files differs slightly from what is normally observed from similar types of malware. Instead of embedding malware within clean code, VirLock embeds clean code within malware. This implies that every encrypted file will be embedded into the malware. The file then functions as a VirLock mutation, and it can be used to further infect and spread the virus.

The first VirLock detection took place in 2014 [45]. Naturally, as the virus is polymorphic, numerous distinct mutations have been discovered throughout the course of many years, up until the present. Numerous differences in VirLock's core functions as well as the decoration code, have been discovered as it continued to evolve. VirLock is capable of propagating through networks and due to the growing popularity of cloud storage nowadays, which VirLock takes advantage of, it is able to achieve better spreadability. Its capability to spread and infect is amplified by its inherent behavior, as outlined in the next subsection.

2.2. Behavior

VirLock has the ability to take over the entire screen area of the computer and terminate the Windows `explorer.exe` process, which controls the graphical user interface [46]. By the time it infects the computer, it has been rendered nearly unusable because there is no way to access the operating system's core features as the virus message covers up the entire screen while binary files and files with specific extensions are "encrypted" in the background. In certain VirLock variants, the user's geolocation is also breached, and based on this, VirLock is able to display special lock screen messages that pretend to be local authorities instead of generic ones [47]. This helps persuade the user even more that the message is legitimate and that they should cooperate. While all the above take place, the typical user is unable to utilize antivirus software in the traditional manner, which requires access to the graphical user interface. The best technique to clean a computer from VirLock, as advised by several antivirus vendors, is to boot into Safe Mode with Networking in the Windows OS, or use a VirLock cleaner provided by certain companies, along with manuals for the disinfection operations. These strategies will probably prevent VirLock from launching itself at startup. If the OS boots up properly, and the OS files are not "encrypted," the user can try to disinfect the computer by running a virus scan with antivirus software or anti-malware software. The type of VirLock variant that infected the host will obviously affect the likelihood of successful detection and removal of the virus, as it is quite likely that a new variant may not be recognized yet. This additional complexity is the result of VirLock's ability to mutate, as explained in the following subsection.

2.3. Mutations

VirLock's exceptional ability to evade detection and defenses has been partially attributed to its adaptive coding structure. This malware employed polymorphic code, allowing it to mutate with each execution, while preserving its primary function [48]. Better live behavioral analysis capabilities in antivirus solutions, as well as the use of AI, may provide a distinct advantage over the signature-based approach in combating such types of viruses, but detection is not totally certain. Mutations are not completely different from the core code as they retain certain traits. The core behavior and infection strategy, in many cases, appears to remain the same, if it is not altered by a third party. It is possible that the level of protection can be increased by focusing on the way viruses react to scenarios. There are various mutations and variations of VirLock in the databases of most digital security companies. Data from the well-known website VirusTotal suggest that the virus's mutations and variations have different detection rates from a variety of antivirus software. In VirusTotal, VirLock can be seen under the names PolyRansom.b, Nabucur.A (the letter after the dot refers to the variation, and different ones can be seen), Win32.Cryptor, and more (some of the results can be found in [49–51]). Even though behavioral analysis from antivirus and anti-malware software is considered important (see [52–55] for further details), there are still ways that VirLock evades their emulations, e.g., by employing techniques like payload encryption and generic obscure code [56,57]. In view of this fact, being familiar with viable countermeasures becomes even more important.

2.4. Possible Countermeasures

As previously mentioned, for known VirLock variants, certain companies provide a VirLock cleaner [58] that claims to be able to remove the virus's leftovers and "decrypt" the majority (if not all) of the infected files. The user is warned that false positives might also be detected and should proceed with caution. Others even suggest a cloud access security broker (CASB) that could protect the cloud storage by setting limits on certain activities and/or breaking connections when needed [59,60]. Analyzing the behavior of this type of malware appears to be the most effective approach for its detection and prevention, as its numerous variants usually challenge anti-malware software.

The best practical protection against this type of infection is to keep regular backups of the files that are of critical importance. Other measures that could also help prevent infection and further transmission are network segmentation and keeping antivirus software up to date [61,62]. As mentioned, another great proactive measure that could protect against VirLock and similar attacks involves the use of a CASB. However, due to the complex set-up that most of these services require, it does not appear to be the best 'maximum payoff' solution for users with little computer knowledge. On the other hand, a known exploit of VirLock, and an easy route to safety in the case of an infection, is its disregard of Windows volume shadow copies; this technology, which is included in Microsoft Windows operating systems, captures backup copies or snapshots of files or volumes, while they are in use. One may consult [63,64] for a comprehensive introduction to this topic. Therefore, the harm can be undone if this feature of Windows OS is enabled in order to revert to a previous backup [46]. Security specialists have also found that VirLock has a flaw that can be exploited. Specifically, VirLock can be misled to act as if the ransom has been paid, if 64 consecutive zero-bits are input in the description key field [65]. Immediately afterward, decryption can be initiated by simply clicking a file, so that the original file could be manually recovered. The drawback of this strategy is that the user will have to do this for every single file in the computer, with the risk of infecting the computer once again. The process should be conducted by moving the recovered files to an external drive and then formatting the one with the infected files. Following a thorough review of the literature on VirLock and existing recovery processes, a list of disinfection strategies, with both proactive and reactive measures, is provided in the forthcoming tables. This will help construct a better framework and keep track of possible scenarios and the resulting outcomes since not every technique is as effective in any given scenario. The concept is further explained in later sections.

2.5. Technical Background

As we delve deeper into understanding VirLock's behavior and countermeasures, it is essential to take a look into its technical aspects as well. Some well-known ransomware tend to use one-way encryption algorithms like RSA or AES. VirLock, on the other hand, implements a two-stage encryption based on XOR and XOR-ROL operations [46]. The fact that VirLock does not utilize well-known encryption algorithms explains why many researchers do not consider VirLock's mechanism as encryption. This also accounts for the fact that, with VirLock, the Shannon entropy is not as high as when RSA or AES are employed because enhanced encryption always results in more entropy (see standard cryptography textbooks, such as reference [66]). The infection occurs when the user attempts to run the infectious file. By the time it is executed, it drops 3 randomly named executables in random folders. The executables appear to carry different hashes as they are polymorphic [67]. One of them disguises itself as a Windows service, while the others encrypt and infect the computer's files. The task manager process is also disabled, providing an extra layer of protection to the virus, preventing the user from taking control and killing the virus process that attempts to alter the Windows registry. These are VirLock's trademark actions. Initially, VirLock disables the user access control (UAC) so as to gain full permission to access and modify files and folders without needing administration privileges. Afterward, VirLock obfuscates the known file extensions, preventing the user from detecting the `.exe` extension. This can have dire consequences, as the user will consider these files safe and eligible for backup, execution, or transfer to another system. Finally, VirLock modifies the registry so as to render hidden files invisible [46]. This action significantly complicates the user's awareness of the state of critical operating system files and hinders any recovery effort.

2.6. Propagation

Later variations of VirLock seem to be able to spread through networks with the help of cloud storage, as illustrated in Figure 1. VirLock can infect other computers through the files it has infected. One possible infection scenario could be one where a company makes use of cloud storage for easier file access among its employees. The first infection occurs by an employee clicking the link of a malicious email. This will trigger the execution of the malicious software. If one of the computers becomes infected with VirLock, this variant can also infect the files stored in the cloud as it will scan for such folders connecting to the network. Consequently, when other co-workers access/use these infected files in the cloud storage, they may also become infected as the files act similar to a virus "mutant" [68].

2.7. Infected File Structure

The structure of the aforementioned files involves the following: the polymorphic code appears at the beginning and end of the code, undergoing changes in every iteration/infection. The polymorphic code is essentially "wrapped" around the main code blocks. This part of the code is also referred to as "decoration code" as it "decorates" the main code with operations like random API calls from random modules. The malicious code, which runs every time, appears after the first piece of polymorphic code, and it is usually the same among different variations of the code. Right after the malicious code, VirLock embeds the encrypted data of the original file it infected, often referred to as "clean code." The last piece of polymorphic code appears at the end of the code [62,69,70]. In the case of an infection, and depending on the technical expertise of the user, the user may prefer to pay the ransom rather than engage in disinfection operations that might appear complicated. There are several major reasons as to why one should reconsider making the ransom payment. First, there is a compelling ethical justification, especially in light of the exorbitant price the ransomware may demand. Second, according to a number of sources [71], just 8% of those who pay the ransom successfully recover the grand total of the data. Ransomware preys on its victims' urgency to regain their data, pushing them to a ransom payment strategy. Of course, as it appears, there are other significantly more efficient ways for victims to recover their data while achieving a high pay-off as players.

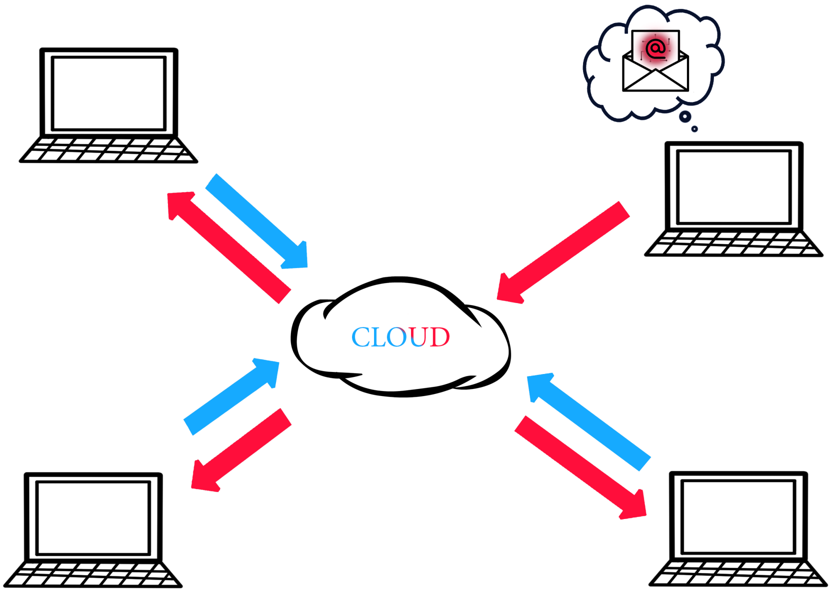
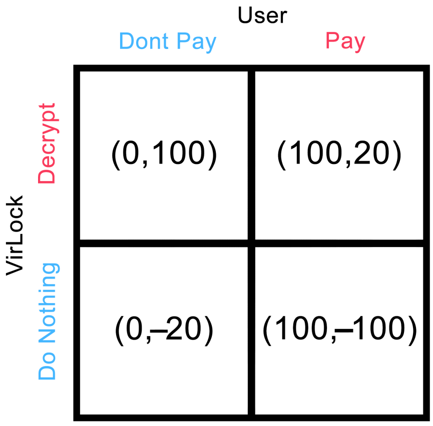


Figure 1. This figure illustrates the VirLock cloud storage spread and infection. In this example, the user of the top right computer opened a malicious email attachment that infected the PC with the VirLock malware. The files in the network share of the cloud storage will also become infected. The malware may eventually spread to other machines in the network. The blue arrows represent interaction with the cloud, while the red ones show the route of the infection.

3. Modeling VirLock with Game Theory

It is fruitful to assess the strategies that benefit the user the most in the case of a VirLock infection by employing game theory tools to model various scenarios. The use of game theory can bridge the gap between technical solutions and decision-making by taking a more analytical approach to a complex problem [72]. This paper introduces a modification of the well-known susceptible infected recovered (SIR) and susceptible infected susceptible (SIS) models. These models are capable of capturing the relationships among nodes within a network, as well as their impact on malware dissemination. They employ game theory to calculate optimal strategies that can limit the impact of malware proliferation and decrease security costs [73].

The game-theoretic analysis of ransomware in this paper assumes that the defender can invest in two types of ransomware protection: (1) general protection due to deterrence effort, which reduces the probability of infection, and (2) a backup plan that enables the user to recover from the infection [74]. Based on the general consensus among security experts [71] that "96% of those whose data were encrypted obtained their data back in the most significant ransomware attack," and that "only 8% (of those who paid) obtained all their data back," we constructed a payoff matrix, as seen Figure 2. This indicates that paying the ransom may not be the best choice since there are alternative methods of recovering the data. The following game theory matrix pictures a scenario where the user who is infected by ransomware has to decide whether paying the ransom or not is worth it.



		User	
		Dont Pay	Pay
VirLock	Decrypt	(0,100)	(100,20)
	Do Nothing	(0,–20)	(100,–100)

Figure 2. Game theory payoff matrix of the ransom payment. VirLock may or may not decrypt the user's data (or at least not in its entirety). The user has the choice of agreeing or refusing to pay the ransom. It is clear that paying the ransom will generally result in an advantageous position for the malware creator(s) and that doing so entails extra risks.

In this game, the VirLock malware and the user are considered as the players. The user has two possible moves and so does VirLock. The user can choose to pay or not to pay the ransom, and VirLock can "choose" to decrypt or not to decrypt the files. VirLock's moves are technically predetermined since there is usually an algorithm that offers the user the decryption key, but we can still roughly calculate the possible outcomes of the scenario. The maximum payoff is considered to be 100. For the user, 100 means that all their files were decrypted without losing any money (which does not appear here since we do not consider certain disinfection techniques but only ransom payment). For VirLock, 100 means that the entirety of the ransom is paid. We consider that the data are of some importance.

Each table cell represents the outcome of the game after the players have chosen their strategies. On the top left cell, we have the statistically improbable case where the files are decrypted while the user does not pay. This case may occur if VirLock fails to encrypt the data or the user employs a proactive strategy so no damage is taken from the attack. Because of this, the payoff for the user is taken to be 100 since not only no money is spent but all the data are unaffected while tackling the attack and preventing further spread. On the other hand, in the bottom left cell, we have the case where the user does not pay and VirLock does not decrypt. This could be considered a neutral state, but in reality, if VirLock manages to encrypt the data, the user is at a disadvantage. Of course, based on the data criticality and the possible disinfection techniques per case, the negative number could go even lower, meaning bigger losses for the user. We will further demonstrate the effects of such factors in the following sections. The top right cell captures the case where the user chooses to pay the ransom and VirLock decrypts the files. As the available statistics suggest, only a portion of the data is usually decrypted. Moreover, considering that the ransom is quite high, the user benefits only in theory, since, usually, not all files are rescued, and only some of the data are recovered, despite the significant amount paid. Again, considering the importance of the files, the payoff is proportional to the cost of money and the data criticality that are encrypted. The benefit could even go below 0, depending on the circumstances. The bottom right cell represents the case, where the user pays the whole ransom and VirLock does nothing to decrypt the data or a second infection takes place from the user error or VirLock's inability. In this case, the user loses everything in the context of this game, with a cost of -100, while VirLock obtains it all (100).

4. The Pseudomonas Virus $\phi6$

Bacteriophage $\phi6$, also known as a Pseudomonas phage $\phi6$, is a lytic virus and a member of the Cystoviridae family that infects Pseudomonas bacteria [75]. Specifically, this type of virus infects Pseudomonas syringae and legume-infecting bacteria. The bacteriophage $\phi6$ has been widely referenced in the literature, and has been studied via classical and evolutionary game theory [76–79]. It is classified as a dsRNA (double-stranded RNA) virus, and its double-stranded genome consists of twelve protein codes and three segmented parts. A lipid membrane covers the nucleocapsid of this species.

4.1. Genome Structure

The infection cycle begins by attaching to the host bacterium using receptor-binding proteins on its surface. With its unique protein, named P3, designed for this function, $\phi 6$ finds the bacterium and sticks to it. In addition to the protein above, many other proteins participate in the process of cell infection. Upon attachment, $\phi 6$ injects its segmented, tripartite genome into the host cell, where replication and transcription occur [80]. Unlike many other bacteriophages, $\phi 6$ carries a segmented, tripartite genome, consisting of three separate RNA segments. These segments are denoted as L (large), M (medium), and S (small), and they contain the encodings of essential viral proteins and enzymes. The L segment encodes the RNA-dependent polymerase and capping enzyme, the M segment encodes structural proteins and a maturation protease, while the S segment encodes non-structural proteins involved in replication and transcription. This segmented genome structure allows $\phi 6$ to undergo genetic reassortment, enhancing its adaptability and diversity as it primarily infects Pseudomonas syringae, a plant-pathogenic bacterium [80].

4.2. Infection Cycle

This process synthesizes viral RNA and proteins needed for the construction of new phage particles. $\phi 6$ displays a high degree of host specificity, primarily targeting Pseudomonas bacteria, particularly Pseudomonas syringae strains. This specificity is mediated by specific receptor-binding proteins on the phage's surface that recognize and attach to receptors on the bacterial cell surface. The virus's outer lipid envelope is derived from the host cell membrane during the assembly of new phage particles. After assembling and maturation, the host cell undergoes lysis, releasing progeny-phage particles that can infect other Pseudomonas bacteria, perpetuating the infection cycle [80]. This cycle of attachment to the host cell, entry, replication, and transcription of viral RNA, assembly, maturation, cell lysis, and the release of new phage particles, continues, allowing the $\phi 6$ bacteriophage to propagate and spread in populations of Pseudomonas bacteria. The ultimate goal of the propagation is to generate a large number of progeny phage particles that, capable of infecting additional host cells, ensuring the survival and spread of the phage within its bacterial host population. $\phi 6$ bacteriophages compete with each other to gain capsid proteins in their common bacterial targeted host. When different strains of $\phi 6$ bacteriophages are assembled, with varying numbers of bacteriophage particles that can simultaneously infect a single bacterial cell, different results are obtained. The result of infection of the bacterial cell by the virus directly depends on the combination and proportions that will be chosen in the phage and bacteria populations. A strain can infect a cell alone, or infection can result from a combination of viruses and their counterparts or even their mutations [77].

The behavior of the bacteriophages, as well as the role that each one will take and whether they will cooperate with their neighbors or show selfish behavior plays a catalytic role in the fitness of the population against the virus. $\phi 6$ is found in cases of polymorphism mixes with helper viruses. From a game-theoretic perspective, some behaviors can be interpreted with the help of the prisoner's dilemma game, and others with the help of the snowdrift game (also called the chicken game), with different results, depending on the ratio of infecting viruses to bacterial cells [76]. Due to its unique genome and well-understood life cycle, $\phi 6$ serves as a valuable model organism in virology research, aiding investigations in virus–host interactions, RNA biology, and viral replication.

Beyond its role as a model organism, $\phi 6$ has garnered attention for its potential application in phage therapy, an emerging approach that employs phages to target and eliminate specific pathogenic bacteria, potentially offering an alternative to antibiotics. Additionally, $\phi 6$'s natural presence in the environment can play a role in controlling the population of Pseudomonas bacteria by causing cell lysis and reducing bacterial abundance. In biotechnology, $\phi 6$ and related phages find utility, particularly in phage display technology, where they assist in the selection of specific proteins with desired properties.

4.3. Possible Countermeasures

Eliminating $\phi 6$ bacteriophage, a type of virus that infects Pseudomonas bacteria, can be a complex endeavor due to its ability to infect and replicate within host bacteria. Several approaches can control or reduce the presence of $\phi 6$ in various settings. One approach involves the use of antibiotics, which primarily target bacterial infections. While antibiotics will not directly eliminate phages, they can indirectly help by reducing the population of susceptible host bacteria. This can limit the hosts available for $\phi 6$, potentially slowing down its propagation [81]. Another strategy is phage therapy, which involves using other bacteriophages known as "phage predators", which specifically target and infect $\phi 6$ or similar bacteriophages. This approach relies on predatory phages to reduce the population of $\phi 6$ in a bacterial culture.

Developing bacterial strains that are resistant to $\phi 6$ infection is a long-term strategy. Genetic engineering can be used to create bacteria lacking the receptors to which $\phi 6$ attaches. However, this method may not be feasible for all applications and should be approached with caution [81]. In certain environments, like water treatment facilities or industrial processes, controlling environmental conditions, such as temperature, pH, or nutrient availability, can help limit the growth of $\phi 6$ and its host bacteria. Understanding the environmental factors that support $\phi 6$ propagation and modifying them can be effective. Additionally, thorough disinfection, using appropriate chemicals, heat, or UV radiation, can help inactivate and eliminate $\phi 6$ particles, particularly in environments where $\phi 6$ contamination poses a risk, such as laboratory equipment [82].

Preventive measures, such as strict hygiene and biosecurity protocols, are crucial for preventing the introduction and spread of $\phi 6$, particularly in laboratory and industrial settings where bacterial cultures are used. Implementing these measures can help minimize the risk of $\phi 6$ contamination. In some biotechnological applications, modifying or controlling the culture conditions can limit the growth of $\phi 6$. Optimizing the growth medium composition or temperature, for example, may reduce the impact of $\phi 6$ in bioprocesses [78]. The specific approach to eliminating or controlling $\phi 6$ bacteriophage will depend on the context, objectives, and available resources. It is essential to consider the potential risks and benefits of each strategy, especially in research or industrial settings, and seek guidance from experts in virology, microbiology, or biotechnology when dealing with $\phi 6$.

5. Modeling $\phi 6$ with Game Theory

While game theory is primarily applied to economics, social sciences, and political science, it can also be used as an analogy or conceptual framework to understand certain aspects of biological systems, including the interactions between viruses like $\phi 6$ bacteriophage and their host bacteria [77]. In this context, we can perceive the co-evolutionary dynamics between the two as a strategic "game." Bacteria develop defense mechanisms to resist viral infections, while viruses like $\phi 6$ evolve to overcome these defenses. This ongoing adaptation can be viewed as a strategic interaction where both parties are adapting their strategies (genetic makeup) over time in response to each other's moves [78]. Furthermore, game theory provides a framework to conceptualize the strategies employed by viruses like $\phi 6$ and to maximize their chances of successful infection and replication within a host cell. Similarly, it can be used to model the strategies employed by host organisms (in this case bacteria) to defend against viral infections, such as activating antiviral defense mechanisms.

Another perspective involves resource allocation within the host cell. Both $\phi 6$ and the host bacterium may compete for limited resources like energy and raw materials to support their own reproduction and survival. Game theory concepts, such as the prisoner's dilemma or the tragedy of the commons, can be applied to understand how these competing entities allocate resources and interact within the host environment [79]. Additionally, game theory can help in exploring the trade-off between viral virulence (the ability to cause harm to the host) and host resistance (the ability to defend against infection). This trade-off can be analyzed in the context of the evolutionary strategies of both the virus and the host. It is essential to recognize that while game theory offers a useful paradigm for understanding the strategic aspects of virus–host interactions, these interactions are inherently complex. They encompass various genetic, molecular, and ecological factors that go beyond the simplified models presented by game theory. Nonetheless, applying game theory concepts enriches our perspective on how viruses like $\phi 6$ and their host cells engage in a dynamic interplay of strategies and adaptations.

6. Comparison of VirLock with $\phi 6$

It is of considerable interest, and may yield new insights, to compare the properties of biological and computer viruses and how they behave during and after the invasion of the host. Computer viruses continue to evolve in tandem with the development of computers, just like their biological counterparts. Biological viruses mutate, and when they do, generations can be observed over time. Similarly, computer viruses may also mutate and replicate themselves or can be altered by a third party. To follow this metaphor even further, we may correlate the immune system of a bacterium with the antivirus, other security software installed on a computer, and other digital security properties (like privileges, actions, settings, etc.). A computer infection can be associated with the infection of a bacterium by a biological virus. Computer viruses attempt to weaken the computer's "immune system" in order to replicate themselves and increase their population. In addition to the above, VirLock and worm-type viruses try to infect more than just a single individual and spread their population through the network, which in turn can be correlated with a population of bacteria in close proximity.

As we attempt to compare and correlate computer viruses with their biological counterparts, we choose a representative from each group. We deem the bacteriophage $\phi 6$ as a suitable representative of biological viruses since its behavior and structure have been extensively modeled in terms of classical and evolutionary game theory. It is worth noting that $\phi 6$ bacteriophage has been extensively studied in virology and is used as a model organism to investigate various aspects of virus–host interactions, viral replication, and RNA biology due to its unique segmented genome and well-documented life cycle. Studying $\phi 6$ helps researchers gain insight into the broader field of virology and molecular biology. In other words, $\phi 6$ bacteriophage stands out as a unique and extensively studied virus with distinct characteristics, making it a valuable tool for understanding virology and virus–host interactions, and exploring various practical applications, from phage therapy to biotechnology.

The most important characteristics of VirLock that can be associated with the bacteriophages $\phi 6$ are listed below.

($\mathbf{P}_1$) Rapid growth due to self-replication.
($\mathbf{P}_2$) Self-protection via host manipulation.
($\mathbf{P}_3$) Ability to gain full access to the host functions.
($\mathbf{P}_4$) Affinity for certain host types.
($\mathbf{P}_5$) Parasitic behavior, code manipulation, and embedding into replicants/mutants.
($\mathbf{P}_6$) Ability to spread upon contact with other hosts.
($\mathbf{P}_7$) Existence of a core structure.
($\mathbf{P}_8$) Capability for rapid mutation.
($\mathbf{P}_9$) Ability to avoid initial detection and resistance to elimination efforts.

Table 1 summarizes the main thesis of our approach regarding the fundamental correlation between computer and biological viruses. Tables 2 and 3 elaborate on the main similarities and differences between VirLock and $\phi 6$, respectively.

Table 1. The correlation hypothesis between computer and biological viruses.

General Correlation Hypothesis	
Computer networks	Cities/Countries
PC in a computer network	Individual in a city or country
Infected files in a computer system	Infected cells in a human organism
Security software and properties (e.g., antivirus, privileges, actions)	Immune system of a human individual

Table 2. This table highlights the similarities between VirLock and $\phi 6$.

Similarities	
VirLock	$\phi 6$
Infection of specific file types	Pseudomonas bacteria
Parasitic	Parasitic
Propagation process	Propagation process
Exposure to the virus	Exposure to the virus
Hijacking the host's machinery for replication	Hijacking the host's machinery for replication
Malware code mutates	Both virus and host cells mutate
Replication follows infection	Replication follows infection
Embedding of clean code in malware	Alteration of the RNA of host ribosomes
Antivirus and anti-malware	Immune system, RNA interference
Specifically designed VirLock cleaners	Specifically designed vaccines and antiviral drugs
Impairs computer files	Impairs host cells
Infection spreads via infected files	Infection spreads via infected cells

Table 3. This table highlights the differences between VirLock and $\phi 6$.

Differences	
VirLock	$\phi 6$
Infection through infected files	Virus enzymes
Multiple attributes	P12 proteins
Polymorphic code	RNA, Capsid, Virion

Tables 4–8 detail the recovery steps after infection. They capture the complexity involved in each step compared to the effectiveness and risks entailed in order to obtain better insight into the overall costs and benefits that could be used in this type of game.

Table 4. This table shows the complexities of VirLock recovery strategies.

The Complexities of the Recovery Strategies			
Strategy	Complexity (out of 10)	Effectiveness	Risk of reinfection
Ransom payment	1	Low	High
Decryption based on VirLock's flaw	5	Medium	High
Recovery based on shadow volume copies	4	High (depends)	Medium
Removal	6	High	Low
Removal plus cleanup	8	High	Low

Table 5. This recovery strategy exploits VirLock's flaw.

Decryption Based on VirLock's Flaw	
Stages	Complexity (out of 10)
Enter 64 zeros in the decryption key	1
Process every file	8 (Possibly prohibitively slow)

Table 6. This recovery strategy uses shadow volume copies.

Recovery Based on Shadow Volume Copies	
Stages	Complexity (out of 10)
Enable shadow volume service	2
Boot into Windows Safe Mode	4
Recover to a previous shadow copy	4

Table 7. The recovery strategy of using simple malware removal with antivirus software.

Removal with Antivirus Software	
Stages	Complexity (out of 10)
Boot into Windows Safe Mode	4
Install antivirus on external disk	4 (not always necessary)
Scan the computer	2

Table 8. The recovery strategy when using virus removal and a cleaner with recovery features.

Recover Using Antivirus plus Cleaner	
Stages	Complexity (out of 10)
Boot into Windows Safe Mode	4
Install antivirus on external disk	4 (not always necessary)
Install VirLock cleaner on external disk	4 (not always necessary)
Run the cleaner (requires several steps and might result in deleting files that are not infected	5
Scan and clean the computer	2

We rated the above stages by considering the difficulty encountered by a typical computer user when implementing these operations. Complexity ranges from 0 to 10; 0 means that any average user could complete this task without any issues, whereas 10 means that the steps are either time-consuming, dangerous, or too complex (requiring special knowledge and having sub-steps), or there are factors that have other requirements. Depending on the relative success rate of a certain technique and the percentage of the files that may be recovered (assuming that it is usually impossible to recover all of the files), the effectiveness variable can have one of three possible values: low, medium, or high. When employing a specific recovery method, the user might be susceptible to contracting the virus once more. To quantify the risk in such an eventuality, the reinfection variable can be used as an indicator of whether the user is more or less susceptible to reinfection and uses the same scale as the effectiveness variable.

The previous tables (as well as the ransom payment payoff matrix of Figure 2) strive to help users whose computers have been compromised by VirLock to choose a strategy that may offer them the highest pay-off against VirLock in their unique infection scenario. Additionally, individuals who have been infected by similar software may find the tables informative. The user can clearly benefit from having a well-considered plan beforehand, such as one of the plans provided in the previous tables. The recovery technique utilizing shadow volume copies has a high success rate. However, whether it is possible depends on how proactive the user is in terms of keeping shadow volume copies beforehand and how old they are. Moreover, depending on how many files the user stores in their computer, the "click on every file in your computer" step may not be a great option, but it might not be needed at all depending on the situation. We point out that antivirus or anti-malware software is not always necessary after the infection has taken place if it has been installed beforehand and is still operational. The strategies above are broken into steps, and the difficulty value associated with each step is chosen with the average computer user in mind. Of course, these values are subject to change based on the characteristics of the individual user, since a computer science graduate or a high-prestige company employee would significantly lower the value of the complexity variable.

7. Mathematical Formulation

7.1. Intuition and Derivation

Taking into account all the aforementioned facts, and real-life factors, like the common behavior of a user during a computer virus infection scenario, enables us to develop a series of conceptual mathematical formulas. The proposed formulation not only supports procedures like the simple calculation of the severity of a virus but can also estimate the importance of those realistic factors. An analogous approach is taken by the industry standard common vulnerability scoring system (CVSS), which is designed to identify key technical aspects of software, hardware, and firmware vulnerabilities. It utilizes a scoring system to indicate the severity of a vulnerability in comparison to other vulnerabilities. The scores are based on realistic characteristics of viruses and vulnerabilities, like the scope of the vulnerability, the user interaction, the availability, the level of possible remediation, and many more. All the above metrics take similar values to the ones we used in the tables previously introduced. CVSS uses special formulas to calculate a severity score that ranges from 0 to 10, with 10 being the critical severity level. Further info about CVSS can be found in this specification document [83], and a CVSS calculator is also provided in [84]. Even though CVSS ratings for the severity levels are approximate [85], the system allows "players" to prepare more and obtain the necessary resources (for example a CASB or an antivirus) to achieve maximum payoff against the known threats. As CVSS claims on its site [86], they aim to "provide a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity."

The existence of precise mathematical formulas allows further tests and experiments that may lead to a definitive conclusion regarding the importance of the factors during the infection, apart from the importance of the technical and technological ones. Games can be based on these formulas in order to simulate certain infection scenarios. Then, by observing the players and the outcomes of the employed strategies, new strategies may be devised that offer advantages over the existing ones. To this end, we propose a series of formulas that take into account the different types of end users and are specific to certain scenarios, so they can be more accurate than formulas utilizing the one-size-fits-all approach. In the field of biological viruses, there are several cases where formulas that factor in realistic data are being used. An obvious case that comes to mind is the recent COVID-19 virus pandemic outbreak, where certain equations have been proposed [87,88]. Unfortunately, it would seem that such formulas that constitute a precautionary measure are not being used widely in the field of computer virus attacks.

At this point, taking into account some of the factors that are extensively analyzed in the literature, which can affect the behavior and the outcome of a possible infection, formulas that fit certain scenarios can be designed. The following example is based on a hypothetical ransomware attack (identical or similar to VirLock). For demonstration purposes, one might draw a parallel between a small city's population getting infected by a biological virus and a computer network succumbing to a computer virus. Inspired by the CVSS and other formulas from the computer and the biological world, as well as the typical model of a commercial company, the average user profile, and their characteristic behavior, we propose a group of novel formulas. These formulas, combined with the standard mechanics of game theory, are useful in the continuous endeavor to discover better strategies to cope with viral infections. Below, we list the factors we have taken into account in our formulas, specifically based on VirLock and, more generally, on ransomware.

- A: User's awareness of the computer virus/user's computer literacy knowledge/ Sudden anxiety from the attack.
- B: Economical state of the user/company.
- C: Criticality of the encrypted data/amount of the critically encrypted data.
- D: Amount of data.
- E: Amount of data the virus infects.
- F: Percentage of infected computers in the network.
- G: Known ways of effective disinfection/possible ways of data recovery.
- H: The effectiveness of the known disinfection strategies altogether (percentage based on users who attempted the strategies).
- I: Safety of operations during/after the infection.

The following formula is used to estimate the spreadability score, denoted by SPS:

$$SPS = 0.7(100 - A) + 0.3F \tag{1}$$

Given the spreadability score, the severity of the infection, denoted by SF, can be computed by the next formula, in which the parameter G is assumed to be > 0.

$$SF = 0.1C + 0.25E + 0.1F + 0.25\,SPS + 0.3G \tag{2}$$

Analogously, assuming that $G \neq 0$, the disinfection probability DP is given by

$$DP = 0.15A + 0.2B + 0.1(100 - E) + 0.15(100 - F) + 0.3H + 0.1I \tag{3}$$

Finally, the disinfection payoff, denoted by DC, can be computed by the Algorithm 1, given below, where $S = \frac{e}{d}$.

Algorithm 1: Disinfection payoff

```
if ($C \leq 0.2$ OR $S < 0.2$) then
    $DC = 0$
else if ($C > 0.8$) then
    $DC = C$
else if ($S \leq 0.8$) then
    $DC = C * S$
else if ($S \leq 1$) then
    $DC = C$
return $100 * DC$
```

The above formulas almost always return a decimal number that represents the corresponding score on a scale of 1–100 (percentage). The values of the variables range from 1 to 100 and determine the final probability. For example, if only 1/4 of the computers in the network are infected, the value of the F variable would be 25. If the encrypted data of a company or an individual are of extreme critical importance, where the loss would mean huge drawbacks, then high criticality could range from 90 to 100 for variable C. Having a certain percentage scale could provide more accurate numbers in pay-off matrices, ensuring that both players have benefits that they can use to their advantage.

7.2. Test Case Scenario

To obtain a better understanding of the previous mathematical concepts, we visualize them in the figures that follow. This allows us to compile the general profiles of the players, which in this scenario are 2 companies with different behaviors against VirLock. The difference between the companies is captured by the different values of the variables, as shown in Table 9. The data creation and calculations were carried out by a custom computer program, written in C, based on the mathematical concepts introduced above. We paid special attention to whether or not to pay the ransom because it is the most essential question in the context of ransomware. In addition to this core issue, we present preventive and reactive techniques, followed by an analysis of why choosing to pay may be a good or poor idea, depending on the circumstances.

Table 9. The values of the variables used to model the profiles of fictional companies A and B used in the example scenarios that follow.

Variables and Their Values		
Variable	Company A	Company B
A	20	90
B	25	60
C	25	90
D	100	100
E	80	10
F	90	15
G	25	25
H	60	60
I	15	75

Figure 3 shows the different results produced based on 2 different fictional companies: company A, which is technologically illiterate, and company B, which is technologically literate. In this case, ransomware like VirLock could be much more effective against company A. This is because viruses like VirLock aim for this characteristic in their victims. When VirLock is sent via email, pretending to be an important document that one should forward, employees of company A may be tricked into spreading the virus. This will affect the spreadability score and the severity. Assuming that the volume and criticality of data are basically the same in both companies, and that both are attacked by the same virus, we can understand the advantages and disadvantages of these 2 players against the virus.

In the case of company A, variables A, F, and I differ compared to company B since most of the employees would not be able to identify a candy-wrapped scam email and would probably forward it to the rest of the network, i.e., the F variable assumes higher values. By the time they realize that an infection has occurred, they might not have a well-planned disinfection strategy, and attempts to disinfect operations could have a worse effect. In contrast, a company with well-trained and up-to-date employees would probably have less of a problem and would restrict the spread much faster. Variable F would be lower and variable I higher, leading to a less severe attack, lower spreadability, and a higher payoff. Company B probably has much more data that are of critical importance but maintains a much better data-to-infected data ratio due to their proactive strategy against attacks. Company A has a much higher data-to-infected data ratio, but their data may not be of such critical importance. In such a scenario, one may modify the values of B, C, D, and E accordingly.

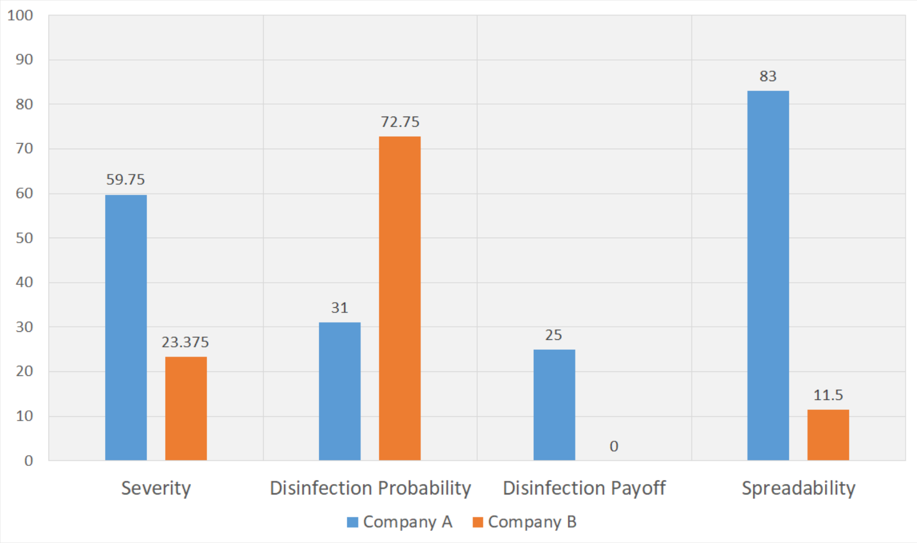


Figure 3. Graphical representation of the results given by the preceding formulas for 2 different companies. It is clear that the technologically illiterate company (company A) faces a significantly more severe problem compared to company B. The spreadability also rises significantly in the case of A.

Additionally, we ran extensive tests in which a single trait was fixed to a constant value. This approach enabled us to evaluate how a certain variable corresponding to a trait affects the remaining variables, and to what extent. In the following figures, a variable is chosen as constant while all other variables take values from 0 to 100. Examining the charts can visually illustrate the effects of the traits.

Figure 4 makes it clear that the increase in the values of the severity output from the formulas depends heavily on the value of variable A. The conclusion is that a technologically illiterate company or individual is more susceptible to infections and finds it harder to disinfect and not spread the virus (especially in the scenario of VirLock), which is also why the spreadability line is much higher. Note that the severity line is slightly higher but steeper, and the disinfection probability is also higher. A simple comparison between Figures 4 and 5 demonstrates that the disinfection payoff is the same in both cases, i.e., when $A = 20$ and when $A = 80$, since this formula does not make use of variable A.

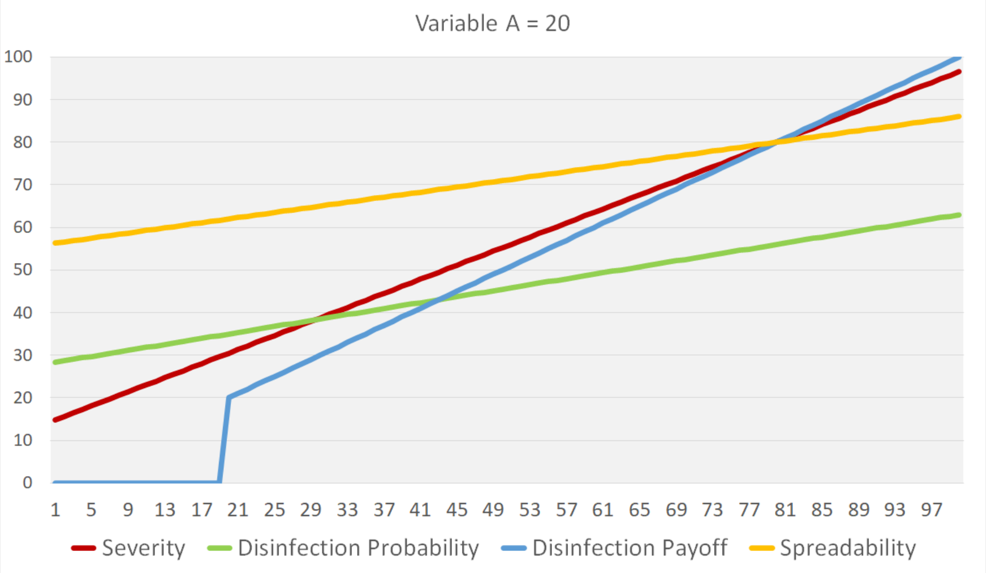


Figure 4. This chart displays a graphic plot of the formulas in the case where variable A is constant with a value of 20, while the values of the rest of the variables range from 0 to 100.

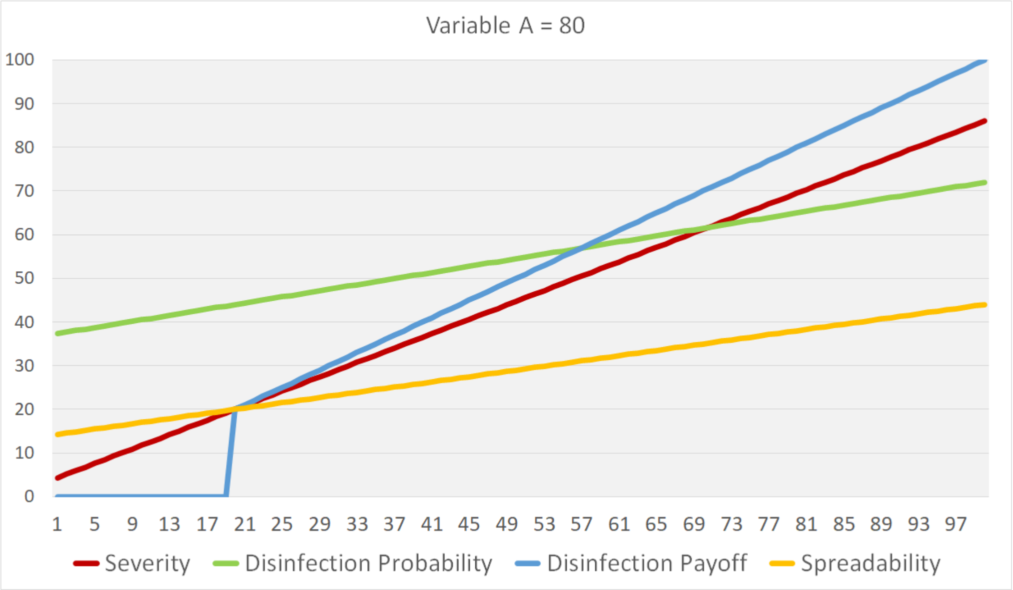


Figure 5. This chart plots the formulas, where variable A is constant with a value of 80, while the values of the rest of the variables range from 0 to 100.

In Figures 6 and 7, we can observe a cross-shape between severity and disinfection payoff when $C = 10$ and $C = 90$. The cross is obviously higher in the $C = 90$ chart since the data criticality is extremely high, something that makes attacks more severe. The main difference between the two charts lies in the disinfection payoff associated with employing any strategy to recover their data. The intuition behind this is that, given the data's high criticality, it is extremely important (with a value proportionate to the data criticality) to employ any strategy to recover the data. This is the exact opposite of the chart when $C = 10$, where $DP = 0$, indicating that it is not worth it to employ anything with such low-level data criticality.

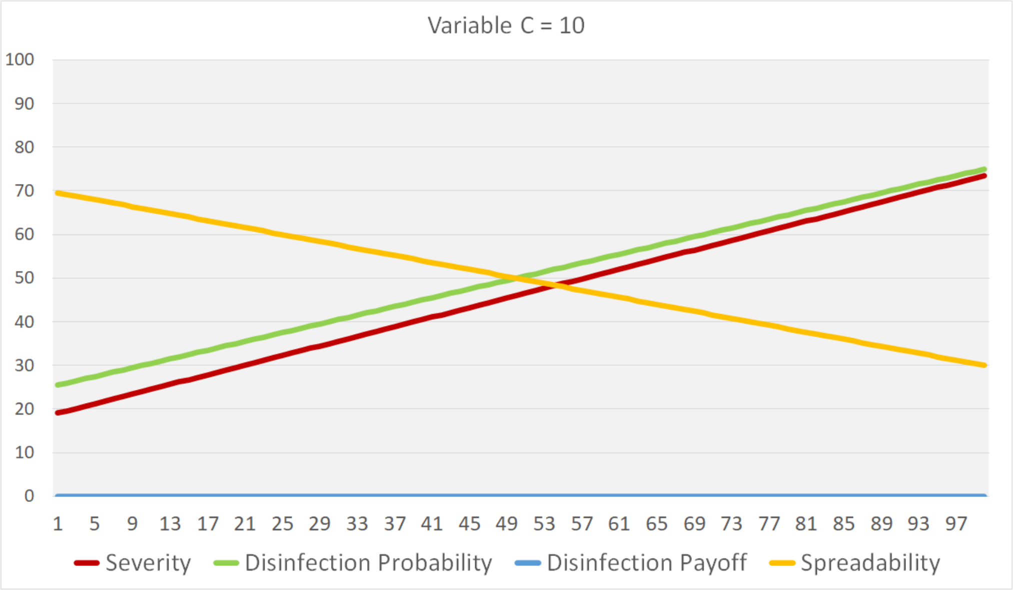


Figure 6. The above figure contains a graphic plot of the formulas in the case where variable C is constant with a value of 10 while the values from the rest of the variables range from 0 to 100.

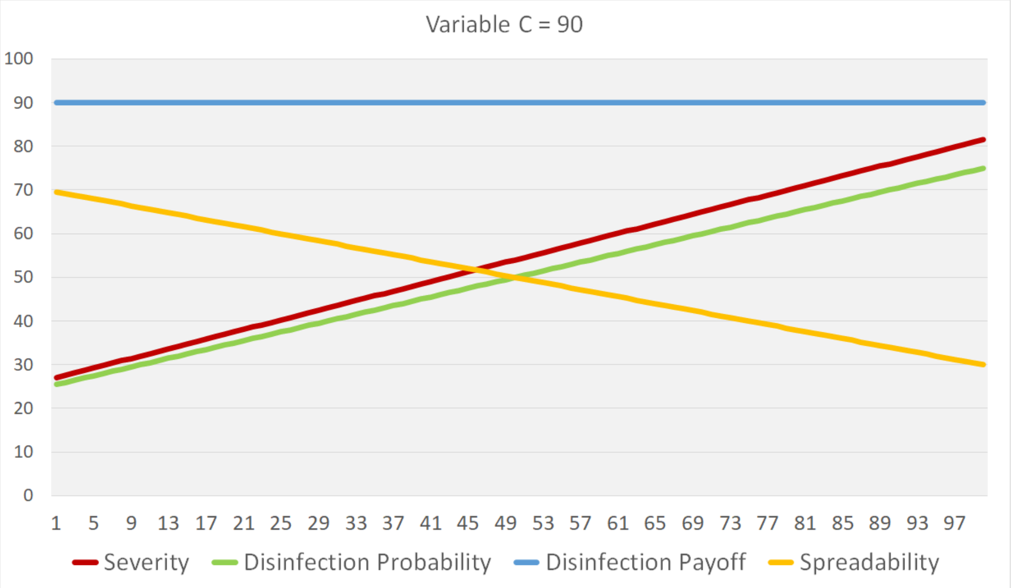


Figure 7. Chart presenting the output of the formulas where variable *C* is constant with a value of 90 while the values from the rest of the variables range from 0 to 100.

8. Ethical Considerations

The emergence of ransomware attacks in the digital era is a growing threat that poses significant ethical dilemmas. While the motivation behind paying ransoms to cybercriminals is often driven by the urgent need to regain access to crucial data or systems, it brings forth apprehensions about inadvertently endorsing criminal behavior and nurturing the ransomware industry [89]. Furthermore, these payments come with no data recovery assurance, and, as we mentioned in the previous section, the possibility of such a scenario is very high, thus potentially leaving victims in a precarious situation [90]. This ethical dilemma raises fundamental questions about the prudence of acquiescing to extortion without a guaranteed resolution [91]. From an ethical standpoint, organizations must critically evaluate the consequences of indirectly supporting an ecosystem of illegal activities and the repercussions of indirectly funding criminal acts. Moreover, paying a ransom sets a dangerous pattern, making organizations more susceptible to future attacks, and potentially prolonging the cycle of victimization. Ethical considerations also encompass the neglect of investments in cybersecurity and the potential legal repercussions [92]. Prioritizing alternative solutions, such as employing proactive and reactive cybersecurity measures, implementing effective incident response protocols, and collaborating with law enforcement agencies, aligns more closely with ethical principles and the well-being of society, thus safeguarding the interests of stakeholders and preserving the rule of law in the digital realm [93].

9. Discussion and Conclusions

This work advocates a new perspective and offers a starting point for future experimentations. Through the correlation of computer viruses with biological ones, we set the groundwork for further research involving the game-theoretic perspective. The study of characteristics and behaviors, along with their similarities, can enhance our understanding of the impact factors in a game, showing that remedies and disinfection mechanics that work well in the biological world could be effective through proper correlations in the computer world. Game theory is a unifying tool, given the growing need for behavioral analysis, especially as most anti-malware software consistently enhances their analysis tools. Analyzing the behavior of viruses and the users' actions can lead to the formulation of more effective strategies against an opponent. Alternative strategies for dealing with biological and computer viruses can appear through the study of their relationships using appropriate tools and methodologies. The proposed game-theoretic tools and methods could prove useful in enhancing penetration testing, and vice versa, since the results of penetration testing could adjust the values of variables used in games. The topic of threat assessment is very important both in theory and in practice when attempting to tackle multiple scenarios, especially in environments where data are critical. Moreover, risk analysis, as shown in the previous tables and charts, is equally important in order to select a strategy that will offer the ultimate payoff. There are factors that are sometimes not taken into account, even though they are important and could change the possible outcome of an attack. The specific users and their traits should be taken into account when picking a strategy in order to achieve an optimal outcome, since just picking the ultimate security does not factor in costs like price, complexity, application, etc.

Any viable framework must exhibit a better understanding of a virus and its method of infection in order to be effective. Worms, for example, have an infectious pattern that is extremely similar, and the proposed framework could work for them too. If we consider a simple malware that does not spread, the damage to a company would be minor, but it could be terrible for an individual, and the entire formulation would change. These could be addressed by correctly extending the proposed framework. Obviously, the proposed framework, being a starting point, has certain limitations. There is bias in this work because we prioritize some factors over others based on the overall damage that could be done. Following considerable testing, we focused our attention on these parameters that appeared to return acceptable—or at least rational—scores. We believe that any similar approach will always be biased because we are dealing with practically infinite and unforeseen events. In future work, we intend to further study the spreadability of viruses in medium- and small-sized networks. For this purpose, the introduction of new games and pay-off matrices, based on real-life scenarios for a wider range of users, will be instrumental. We believe that evolutionary game theory offers the necessary tools to monitor virus mutations more effectively and outline strategies for fending off infections. To this end, we plan to extend the current formulas and further evaluate their usefulness for disinfection, spreadability, and severity. Hopefully, this will allow us to obtain even more objective and realistic measurements from the corresponding games regarding the severity of a computer virus in certain scenarios, the probability of disinfection, and the effectiveness of specific strategies for such viruses. Furthermore, we would like to verify whether processes like natural selection and its properties also apply to computer environments.

Author Contributions: Conceptualization, D.K. and K.K.; methodology, T.A.; software, D.K.; validation, K.K.; formal analysis, D.K. and T.A.; investigation, D.K. and K.K.; writing original draft preparation, D.K. and K.K.; writing review and editing, T.A. and K.K.; visualization, D.K.; supervision, T.A.; project administration, T.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The source code used for the parametrization, data creation, and testing processes of the concept in this study, as well as the exports, are available upon request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cohen, F. Computer viruses: Theory and experiments. *Comput. Secur.* **1987**, *6*, 22–35. https://doi.org/https://doi.org/10.1016/0167-4048(87)90122-2.
2. Kaspersky. What's the Difference between a Virus and a Worm?, **2021**. Available online: https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms (accessed on 31 October 2023).
3. Uniserve IT Solutions. What Are the Different Types of Computer Viruses?. Available online: https://uniserveit.com/blog/what-are-the-different-types-of-computer-viruses (accessed on 31 October 2023).

4. Norton. What is a Computer Worm, and how Does It Work?, **2019**. Available online: https://us.norton.com/blog/malware/what-is-a-computer-worm (accessed on 31 October 2023).
5. Taylor, K. What Is A Worm Virus?, VIPRE, **2017**. Available online: https://vipre.com/resources/articles/what-is-a-worm-virus/ (accessed on 31 October 2023).
6. Latto, N. Worm vs. Virus: What's the Difference and Does It Matter?, Avast, **2022**. Available online: https://www.avast.com/c-worm-vs-virus (accessed on 31 October 2023).
7. Forster, P.; Forster, L.; Renfrew, C.; Forster, M. Phylogenetic network analysis of SARS-CoV-2 genomes. *Proc. Natl. Acad. Sci. USA* **2020**, *117*, 9241–9243.
8. Stojanov, D. Phylogenicity of B. 1.1. 7 surface glycoprotein, novel distance function and first report of V90T missense mutation in SARS-CoV-2 surface glycoprotein. *Meta Gene* **2021**, *30*, 100967.
9. Stent, G.S. Molecular biology of bacterial viruses. *Mol. Biol. Bact. Viruses* **1963**, 143, 345.
10. Boase, J.; Wellman, B. A plague of viruses: Biological, computer and marketing. *Curr. Sociol.* **2001**, *49*, 39–55.
11. Löwer, R.; Löwer, J.; Kurth, R. The viruses in all of us: Characteristics and biological significance of human endogenous retrovirus sequences. *Proc. Natl. Acad. Sci. USA* **1996**, *93*, 5177–5184.
12. Stewart, F.M.; Levin, B.R. The population biology of bacterial viruses: Why be temperate. *Theor. Popul. Biol.* **1984**, *26*, 93–117.
13. Mettenleiter, T.C.; Sobrino, F. *Animal Viruses: Molecular Biology*; Caister Academic Press: Norfolk, UK, **2008**; Volume 1.
14. Stojanov, D. Structural implications of SARS-CoV-2 Surface Glycoprotein N501Y mutation within receptor-binding domain [499-505]–computational analysis of the most frequent Asn501 polar uncharged amino acid mutations. *Biotechnol. Biotechnol. Equip.* **2023**, *37*, 2206492.
15. Salazar-Gonzalez, J.F.; Salazar, M.G.; Keele, B.F.; Learn, G.H.; Giorgi, E.E.; Li, H.; Decker, J.M.; Wang, S.; Baalwa, J.; Kraus, M.H.; et al. Genetic identity, biological phenotype, and evolutionary pathways of transmitted/founder viruses in acute and early HIV-1 infection. *J. Exp. Med.* **2009**, *206*, 1273–1289.
16. Wagner, E.; Hewlett, M. *Basic Virology*; Blackwell Science: Amsterdam, The Netherlands, **2004**.
17. Koonin, E.V.; Wolf, Y.I. Evolution of microbes and viruses: A paradigm shift in evolutionary biology? *Front. Cell. Infect. Microbiol.* **2012**, *2*, 119.
18. Feschotte, C.; Gilbert, C. Endogenous viruses: Insights into viral evolution and impact on host biology. *Nat. Rev. Genet.* **2012**, *13*, 283–296.
19. Hayes, W. *The Genetics of Bacteria and Their Viruses: Studies in Basic Genetics and Molecular Biology*; Blackwell Scientific: Oxford, UK, 1964.
20. Baggesen, D.L.; Sørensen, G.; Nielsen, E.; Wegener, H.C. Phage typing of Salmonella Typhimurium—Is it still a useful tool for surveillance and outbreak investigation? *Eurosurveillance* **2010**, *15*, 19471.
21. Wasik, B.R.; Turner, P.E. On the biological success of viruses. *Annu. Rev. Microbiol.* **2013**, *67*, 519–541.
22. Blaas, D. Viral entry pathways: The example of common cold viruses. *Wien. Med. Wochenschr.* **2016**, *166*, 211–226.
23. Birtles, D.; Oh, A.E.; Lee, J. Exploring the pH dependence of the SARS-CoV-2 complete fusion domain and the role of its unique structural features. *Protein Sci.* **2022**, *31*, e4390.
24. Rogers, K. *Bacteria and Viruses*; Britannica Educational Publishing: Chicago, IL, USA, 2010.
25. Onodera, S.; Olkkonen, V.; Gottlieb, P.; Strassman, J.; Qiao, X.; Bamford, D.H.; Mindich, L. Construction of a transducing virus from double-stranded RNA bacteriophage phi6: Establishment of carrier states in host cells. *J. Virol.* **1992**, *66*, 190–196.
26. Douglas, T.; Young, M. Viruses: Making friends with old foes. *Science* **2006**, *312*, 873–875.
27. Falk, B.W.; Tsai, J.H. Biology and molecular biology of viruses in the genus Tenuivirus. *Annu. Rev. Phytopathol.* **1998**, *36*, 139–163.
28. Bouvier, N.M.; Palese, P. The biology of influenza viruses. *Vaccine* **2008**, *26*, D49–D53.
29. Weibull, J.W. *Evolutionary Game Theory*; MIT Press: Cambridge, MA, USA, **1997**.
30. Kastampolidou, K.; Andronikos, T. Microbes and the Games They Play. In *GeNeDis 2020*; Springer International Publishing: Springer, Cham, **2021**; pp. 265–271. https://doi.org/10.1007/978-3-030-78787-5_32.
31. Kastampolidou, K.; Andronikos, T. A Survey of Evolutionary Games in Biology. In *Advances in Experimental Medicine and Biology*; Springer International Publishing: Springer, Cham, 2020; pp. 253–261. https://doi.org/10.1007/978-3-030-32622-7_23.
32. Kastampolidou, K.; Nikiforos, M.N.; Andronikos, T. A Brief Survey of the Prisoners' Dilemma Game and Its Potential Use in Biology. In *Advances in Experimental Medicine and Biology*; Springer International Publishing: Springer, Cham, 2020; pp. 315–322. https://doi.org/10.1007/978-3-030-32622-7_29.
33. Archetti, M.; Pienta, K.J. Cooperation among cancer cells: Applying game theory to cancer. *Nat. Rev. Cancer* **2019**, *19*, 110–117.
34. Theocharopoulou, G.; Giannakis, K.; Papalitsas, C.; Fanarioti, S.; Andronikos, T. Elements of Game Theory in a Bio-inspired Model of Computation. In Proceedings of the 2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA), Patras, Greece, 15–17 July 2019; pp. 1–4. https://doi.org/10.1109/iisa.2019.8900768.
35. Giannakis, K.; Papalitsas, C.; Kastampolidou, K.; Singh, A.; Andronikos, T. Dominant Strategies of Quantum Games on Quantum Periodic Automata. *Computation* **2015**, *3*, 586–599. https://doi.org/10.3390/computation3040586.
36. Andronikos, T.; Sirokofskich, A.; Kastampolidou, K.; Varvouzou, M.; Giannakis, K.; Singh, A. Finite Automata Capturing Winning Sequences for All Possible Variants of the PQ Penny Flip Game. *Mathematics* **2018**, *6*, 20. https://doi.org/10.3390/math6020020.
37. Giannakis, K.; Theocharopoulou, G.; Papalitsas, C.; Fanarioti, S.; Andronikos, T. Quantum Conditional Strategies and Automata for Prisoners' Dilemmata under the EWL Scheme. *Appl. Sci.* **2019**, *9*, 2635. https://doi.org/10.3390/app9132635.

38. Andronikos, T.; Sirokofskich, A. The Connection between the PQ Penny Flip Game and the Dihedral Groups. *Mathematics* **2021**, *9*, 1115. https://doi.org/10.3390/math9101115.
39. Kostadimas, D.; Kastampolidou, K.; Andronikos, T. Correlation of biological and computer viruses through evolutionary game theory. In Proceedings of the 2021 16th International Workshop on Semantic and Social Media Adaptation & Personalization (SMAP), Corfu, Greece, 4–5 November 2021. https://doi.org/10.1109/smap53521.2021.9610778.
40. Okeke, F. 8 Best Penetration Testing Tools and Software for 2023. 2023. Available online: https://www.techrepublic.com/article/best-penetration-testing-tools (accessed on 31 October 2023).
41. 19 Powerful Penetration Testing Tools Used By Pros in 2023. 2023. Available online: https://www.softwaretestinghelp.com/penetration-testing-tools (accessed on 31 October 2023).
42. Saeed, H. 17 Best Security Penetration Testing Tools The Pros Use. 2023. Available online: https://www.redswitches.com/blog/penetration-testing-tools (accessed on 31 October 2023).
43. Fruhlinger, J.; Porup, J. 11 Penetration Testing Tools the Pros Use. 2021. Available online: https://www.csoonline.com/article/551957/11-penetration-testing-tools-the-pros-use.html (accessed on 31 October 2023).
44. Malwarebytes. Ransom.VirLock. Available online: https://www.malwarebytes.com/blog/detections/ransom-virlock (accessed on 22 September 2023).
45. Aurangzeb, S.; Aleem, M.; Iqbal, M.A.; Islam, M.A. Ransomware: A survey and trends. *J. Inf. Assur. Secur.* **2017**, *6*, 48–58.
46. Sophos. *The Current State of Ransomware: VirLock, ThreatFinder, CrypVault and PowerShell-Based*; Sophos: Abingdon, UK, **2016**.
47. The BlackBerry Cylance Threat Research Team. Threat Spotlight: Virlock Polymorphic Ransomware, **2019**. Available online: https://blogs.blackberry.com/en/2019/07/threat-spotlight-virlock-polymorphic-ransomware (accessed on 31 October 2023).
48. Ryan, M. *Ransomware Revolution: The Rise of a Prodigious Cyber Threat*; Advances in Information Security; Springer: Berlin/Heidelberg, Germany; 2021. https://doi.org/10.1007/978-3-030-66583-8.
49. VirusTotal. Analysis of b3f70c6224b38f445ce2d2538ada604094de65165c84218798bfc4fd3ff11ac7. Available online: https://www.virustotal.com/gui/file/b3f70c6224b38f445ce2d2538ada604094de65165c84218798bfc4fd3ff11ac7 (accessed on 31 October 2023).
50. VirusTotal. Analysis of 58d003a53890d6192e803c0cc2aa4f4ae35f7432d9600f1c60bd00323e50198b. Available online: https://www.virustotal.com/gui/file/58d003a53890d6192e803c0cc2aa4f4ae35f7432d9600f1c60bd00323e50198b (accessed on 31 October 2023).
51. VirusTotal. Analysis of 29e40e7bd619110e8adbf99cbc48c09d03a8c4bebb49e5e583dd1ce35b5deea9. Available online: https://www.virustotal.com/gui/file/29e40e7bd619110e8adbf99cbc48c09d03a8c4bebb49e5e583dd1ce35b5deea9 (accessed on 31 October 2023).
52. Lee, D.; Larose, R.; Rifon, N. Keeping our network safe: A model of online protection behaviour. *Behav. Inf. Technol.* **2008**, *27*, 445–454.
53. Rhee, H.S.; Kim, C.; Ryu, Y.U. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Comput. Secur.* **2009**, *28*, 816–826.
54. Gandotra, E.; Bansal, D.; Sofat, S. Malware analysis and classification: A survey. *J. Inf. Secur.* **2014**, *2014*.
55. Shijo, P.; Salim, A. Integrated static and dynamic analysis for malware detection. *Procedia Comput. Sci.* **2015**, *46*, 804–811.
56. Staff, T.E. 70% of Malware Infections Go Undetected by AV Software. 2015. Available online: https://www.tripwire.com/state-of-security/70-of-malware-infections-go-undetected-by-antivirus-software-study-says (accessed on 31 October 2023).
57. Taylor, C. Polymorphic Virus, CyberHoo. 2020. Available online: https://cyberhoot.com/cybrary/polymorphic-virus/ (accessed on 31 October 2023).
58. ESET. VirLock: The First Shape-shifter Among Ransomware, 2014. Available online: https://www.eset.com/int/about/newsroom/press-releases/research/virlock-the-first-shape-shifter-among-ransomware/ (accessed on 31 October 2023).
59. Singh, A. Virlock's Resurgence Poses Bigger Threat to File Syncing Over the Cloud, Netskope. 2017. Available online: https://www.netskope.com/blog/virlocks-resurgence-poses-bigger-threat-file-syncing-cloud (accessed on 31 October 2023).
60. Netskope. Cloud Access Security Broker (CASB). 2023. Available online: https://www.netskope.com/products/casb (accessed on 31 October 2023).
61. Howells, J. Protecting Yourself Against the Scourge of Ransomware, Orange Business, 2017. Available online: https://www.orange-business.com/en/blogs/connecting-technology/security/protecting-yourself-against-the-scourge-of-ransomware (accessed on 31 October 2023).
62. Stu, S. Weird Ransomware Strain Spreads Like a Virus in the Cloud, The Spiceworks Community. 2016. Available online: https://community.spiceworks.com/topic/1855433-this-weird-ransomware-strain-spreads-like-a-virus-in-the-cloud-mitigation (accessed on 31 October 2023).
63. Microsoft. Volume Shadow Copy Service. 2022. Available online: https://learn.microsoft.com/en-us/windows-server/storage/file-server/volume-shadow-copy-service (accessed on 31 October 2023).
64. Wikipedia. Shadow Copy. 2023. Available online: https://en.wikipedia.org/wiki/Shadow_Copy (accessed on 31 October 2023).
65. NJCCIC. VirLock NJCCIC Threat Profile. 2016. Available online: https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants/virlock (accessed on 31 October 2023).
66. Hoffstein, J.; Pipher, J.; Silverman, J.H. *An Introduction to Mathematical Cryptography*; Springer: New York, NY, USA, **2014**. https://doi.org/10.1007/978-1-4939-1711-2.
67. Vamshi, A. Cloud Malware Fan-out with Virlock Ransomware. Netskope, 2017. Available online: https://www.netskope.com/blog/cloud-malware-fan-virlock-ransomware (accessed on 31 October 2023).

68. KnowBe4. Virlock Ransomware. Available online: https://www.knowbe4.com/virlock-ransomware (accessed on 31 October 2023).
69. Sjouwerman, S. This Weird Ransomware Strain Spreads Like a Virus in the Cloud. Available online: https://blog.knowbe4.com/new-virlock-ransomware-strain-spreads-stealthily-via-cloud-storage (accessed on 31 October 2023).
70. Craciun, V.; Nacu, A.; Andronic, M. It's a file infector... It's ransomware... It's VirLock. In Proceedings of the Virus Bulletin Conference, Prague, Czech Republic, 30 September–2 October 2015.
71. Adam, S. The State of Ransomware 2021. Sophos News, 2021. Available online: https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021/ (accessed on 31 October 2023).
72. Li, Z.; Liao, Q. Game theory of data-selling ransomware. *J. Cyber Secur. Mobil.* **2021**, *10*, 65–96.
73. Spyridopoulos, T.; Maraslis, K.; Mylonas, A.; Tryfonas, T.; Oikonomou, G. A game theoretical method for cost-benefit analysis of malware dissemination prevention. *Inf. Secur. J.: A Glob. Perspect.* **2015**, *24*, 164–176.
74. Yin, T.; Sarabi, A.; Liu, M. Deterrence, backup, or insurance: A game-theoretic analysis of ransomware. In Proceedings of the Annual Workshop on the Economics of Information Security (WEIS). Virtual. 28–29 June 2021
75. NCBI. National Center for Biotechnology Information. Available online: https://www.ncbi.nlm.nih.gov/Taxonomy/Browser/wwwtax.cgi?lvl=0&amp;id=2928686 (accessed on 22 September 2023).
76. Turner, P.E.; Chao, L. Escape from prisoner's dilemma in RNA phage Φ6. *Am. Nat.* **2003**, *161*, 497–505.
77. Turner, P.E. Cheating Viruses and Game Theory: The theory of games can explain how viruses evolve when they compete against one another in a test of evolutionary fitness. *Am. Sci.* **2005**, *93*, 428–435.
78. Wolf, D.M.; Arkin, A.P. Motifs, modules and games in bacteria. *Curr. Opin. Microbiol.* **2003**, *6*, 125–134.
79. Klarreich, E. Generous players: Game theory explores the golden rule's place in biology. *Sci. News* **2004**, *166*, 58–60.
80. Sinclair, J.F.; Tzagoloff, A.; Levine, D.; Mindich, L. Proteins of bacteriophage phi6. *J. Virol.* **1975**, *16*, 685–695.
81. Bohl, K.; Hummert, S.; Werner, S.; Basanta, D.; Deutsch, A.; Schuster, S.; Theißen, G.; Schroeter, A. Evolutionary game theory: Molecules as players. *Mol. BioSyst.* **2014**, *10*, 3066–3074.
82. Silverman, A.I.; Boehm, A.B. Systematic review and meta-analysis of the persistence and disinfection of human coronaviruses and their viral surrogates in water and wastewater. *Environ. Sci. Technol. Lett.* **2020**, *7*, 544–553.
83. FIRST. Common Vulnerability Scoring System v3.1: Specification Document. Available online: https://www.first.org/cvss/specification-document (accessed on 31 October 2023).
84. FIRST. Common Vulnerability Scoring System Version 3.1 Calculator. Available online: https://www.first.org/cvss/calculator/3.1 (accessed on 31 October 2023).
85. Wikipedia Common Vulnerability Scoring System. 2023. Available online: https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System (accessed on 31 October 2023).
86. FIRST. Common Vulnerability Scoring System SIG. Available online: https://www.first.org/cvss/ (accessed on 31 October 2023).
87. Fokas, A.S.; Dikaios, N.; Kastis, G.A. COVID-19: Predictive mathematical formulae for the number of deaths during lockdown and possible scenarios for the post-lockdown period. *Proc. R. Soc. A* **2021**, *477*, 20200745.
88. Balak, N.; Inan, D.; Ganau, M.; Zoia, C.; Sönmez, S.; Kurt, B.; Akgül, A.; Tez, M. A simple mathematical tool to forecast COVID-19 cumulative case numbers. *Clin. Epidemiol. Glob. Health* **2021**, *12*, 100853.
89. Botes, M.; Lenzini, G. When cryptographic ransomware poses cyber threats: Ethical challenges and proposed safeguards for cybersecurity researchers. In Proceedings of the 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 6–10 June 2022; pp. 562–568.
90. Mierzwa, S.; Drylie, J.; Bogdan, D. Ransomware Incident Preparations with Ethical Considerations and Command System Framework Proposal. *J. Leadersh. Account. Ethics* **2022**, *19*, 110.
91. Broucek, V.; Turner, P. Technical, legal and ethical dilemmas: Distinguishing risks arising from malware and cyber-attack tools in the 'cloud'—A forensic computing perspective. *J. Comput. Virol. Hacking Tech.* **2013**, *9*, 27–33.
92. Hofmann, T. How organisations can ethically negotiate ransomware payments. *Netw. Secur.* **2020**, *2020*, 13–17.
93. Pawlicka, A.; Choraś, M.; Pawlicki, M.; Kozik, R. A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic. *Bus. Horiz.* **2021**, *64*, 729–734.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.