ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

INCIDENT RESPONSE PLAYBOOK: A CASE STUDY FOR RANSOMWARE ATTACKS COMPARISIONOF SIEM SOLUTIONS SOURCE

A.Sruthi[1], Jamalpuri Harshitha[2], Chalamala Siddhartha[3], Avuti Abhinay[4], Kunti Ram[5]
[1] Associate Professor, Dept. of CS, Sri Indu College of Engineering and Technology, Hyderabad,
[2 3 4] Research Student, Dept. of CS Sri Indu College of Engineering and Technology, Hyderabad

Abstract: Knowledge about ransomware is important for protecting sensitive data and for participat- ing in public debates about suitable regulation regarding its security. However, as of now, this topic has received little to no attention in most school curricula. As such, it is desirable to analyze what citizens can learn about this topic outside of formal education, e.g., from news articles. This analysis is both relevant to analyzing the public discourse about ransomware, as well as to identify what aspects of this topic should be included in the limited time available for this topic in formal education. Thus, this paper was motivated both by educational and media research. The central goal is to explore how the media reports on this topic and, additionally, to identify potential misconceptions that could stem from this reporting. To do so, we conducted an exploratory case study into the reporting of 109 media articles regarding a high-impact ransomware event: the shutdown of the Colonial Pipeline (located in the east of the USA). We analyzed how the articles introduced central terminology, what details were provided, what details were not, and what (mis-)conceptions readers might receive from them. Our results show that an introduction of the terminology and technical concepts of security is insufficient for a complete understanding of the incident. Most importantly, the articles may lead to four misconceptions about ransomware that are likely to lead to misleading conclusions about the responsibility for the incident and possible political and technical options to prevent such attacks in the future.

Keywords: media analysis; informal education; IT security; ransomware; misconceptions

Introduction

In today's digital age, information security plays a crucial role in protecting both personal and professional data from being accessed, used, or compromised by unauthorized individuals or entities. Without proper security measures being in place, individuals and organizations can be at risk from attacks, such as malware, phishing, and ransomware. With the increasing reliance on technology, such attacks are becoming more frequent; according to the Institute for Security and Technology, "ransomware is a flourishing criminal industry that, not only risks the personal and financial security of individuals, but also threatens national security and human life." (Institute for Security and Technology 2021).

One real-world example of the damage that can be caused by a large ransomware attack is the shutdown of the Colonial oil pipeline in the United States, which led to panic buying and shortages. After the attack, in the evening of 7 May 2021, Colonial Pipeline informed the public about the shutdown of their 5500 mile-long pipeline transporting 45% of the US East Coast's fuel supplies. This led to gas shortages, panic buying, and rising fuel prices in the eastern US. The incident was widely discussed in the media, making it one of the most prominent ransomware attacks of recent times.

The high potential impact of ransomware, both in private and professional lives, makes learning about it important; knowing about ransomware and ransomware prevention is crucial, both for implementing appropriate security measures for one's own sensitive data, as well as for participating in public debates about suitable regulations regarding the protection of data and infrastructure by the industry and government organizations.

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

While knowledge about IT security is considered to be increasingly relevant (c.f. Hu et al. 2022; Yang 2001), there typically is not much time in K-12 education (kindergarten to twelfth grade) for this topic. For example, the influential German Informatics Society (GI) recommends lessons on some aspects of IT security: "students of all years should be able to react appropriately to risks while using computer science systems" (Brinda et al. 2008). However, the curriculum of the southern German state Bavaria, which largely follows the GI recommendations, only devotes up to two mandatory 45-min lessons on "the protection of personal devices (e.g., with firewalls, antivirus programs, and the use of secure passwords)" (Staatsinstitut für Schulqualität und Bildungsforschung München 2023) and "risks of digital communication (e.g., by viruses, malware, identity theft, fake news, and subscription traps)"; very little time compared to the vast amount of content that could be taught in this time. This makes it necessary to strongly condense lessons. It also makes it likely that most students will gather most of their knowledge about ransomware incidents from other information sources, such as news articles. This raises questions about what students can learn from such sources and what limited aspects of ransomware incidents should be addressed in the very limited time provided for this topic within formal education.
To contribute to these questions, we tried to analyze the reporting on ransomware attacks and to identify potential misconceptions that typical readers might get from reading these news articles. Thus, the central research questions of this article are as follows:
RQ (1) What aspects of ransomware are typically explained by typical news articles? RQ (2) What misconceptions (if any) might a typical reader get from this reporting?
Importantly, knowledge about such potential misconceptions can then help educators to prepare their lessons: "Being aware of the typical misconceptions students have in [certain] subject areas can help [teachers] focus [their] instruction to address the most common misconceptions." (Lucariello and Naff 2013). For our analysis, we performed an exploratory case-study into 109 media articles regarding the ransomware incident of the Colonial Pipeline. We analyzed these articles using a qualitative content analysis, following the iterative process of (Kuckartz 2019). This analysis was based on the following leading questions: "How did the articles explain ransomware", "how was the incident reported", and "what misconception might a reader get from this reporting?".
Our analysis shows that most articles focused on the (real-world) consequences of the attack and introduced only its high-level idea; description of technical details and context were rare. Furthermore, many articles omitted essential aspects for a complete understanding of ransomware incidents. Notably, only few articles mention that it is possi- ble to prevent ransomware attacks or negate their effects, both with preventive measures and suitable reaction to attacks. Based on these results, we derived four misconceptions about ransomware attacks that students might get by reading these articles. We show how these misconceptions interfere with the ability to come to an informed opinion about the incident and to derive meaningful conclusions from it. We also highlight what (technical) background knowledge is necessary to address these misconceptions.
Related Work
Research into conceptions and misconceptions (or "alternative conceptions") of subject matters has a long tradition, esp. in physics (e.g., Alwan 2011; Kaltakci and Didis¸ 2007; Uhden 2016) and mathematics (e.g., Mohyuddin and Khalil 2016; Ojose 2015; Vom Hofe and Blum 2016) education. For computer science, most teachers currently lack knowledge about such conceptions: "Most computer science teachers highlight the high importance of relating to prior student knowledge. However, they primarily use their personal experience, rather than theoretical knowledge to report about student conceptions." (Pancratz and Schlegel 2021). They are also unsure how to respond to misconceptions correctly (Pancratz and Schlegel 2021). Thus, identifying (potential) misconceptions, as well as methods to address them, is a desirable research goal. In computer science, projects have already started to do this for

artificial intelligence (Axell et al. 2022; Mertala et al. 2022; Wang 2007; Wang et al. 2018), programming Kaczmarczyk et al. (2010); Qian and Lehman (2017), the Internet (Diethelm and Zumbrägel 2010; Hennecke 2015), and conceptions about computing itself as a disci- pline (Beaubouef and McDowell 2008; Hatziapostolou et al. 2008). However, notably, most of these research articles either focused on scholarly arguments about potential conceptions, expert opinion, or interviews with students. To the best of our knowledge, no study in computer science education has used an analysis of material in informal education, such as the reporting in news article, as the basis for such an analysis.

Regarding IT security, a prior study identified the conceptions of young learners (around 8 years old) about computer viruses; already at this young age, almost 90% of par- ticipants knew that computer viruses harm computers. However, the study also identified several misconceptions: only 10% of the students were aware that computer viruses are programs and around 40% assumed that antivirus programs can delete viruses from the Internet (c.f. Tsarava et al. 2020). Another study from 2021 tried to identify conceptions about IT security that experts in the field find worthy of teaching. The conceptions found focused on IT security as a whole, rather than a specific technologies or attacks. Examples include the rule of the weakest link of a technical system, the difference between technical and human attack surfaces, and differentiating between attackers from outside and the inside of a system as two distinct categories (c.f. Schott-Maire et al. 2021).

Technical Background

This section gives an overview of the central principles of IT security necessary to follow this article. We also introduce relevant terminology, as commonly defined in this area.

The CIA-Triad of Information Security

The most crucial framework for IT security is the CIA-triad of information secu- rity (Krutz and Vines 2010). This outlines the goals of IT security in the context of infor- mation. Systems fulfill these criteria if they fulfill confidentiality, integrity, and availability. Confidentiality refers to the fact that information is only available to the entities for which it is intended. Availability describes whether the information can be provided at the time of the request. Integrity indicates that the information provided for requests is complete and accurate.

Cyberattacks

A (digital) attack is any intended maneuver that hinders the functionality of the system as intended. For the purposes of this paper, an attack is an intended action by an external entity that undermines at least one of the goals of the CIA-Triad.[1] An important sub-category of attacks is ransomware attacks (c.f. Section 4). The goal of this attack is to undermine the availability of the system, until a ransom is paid, or to breach its confidentiality unless a ransom is paid. Notably, unlike other attacks, most ransomware attacks do not intend to damage the system permanently (Hassan 2019).

More precisely, the central goal of this type of ransomware is "taking control of critical user resources, and excluding or jeopardizing user's exclusive control" (McIntosh et al. 2021). Therefore, "the primary intrusion principle of ransomware is to stealthily attack and take control of irreplaceable user resources [. . .] before declaring its presence and demanding ransom payments [. . .]" (McIntosh et al. 2021). Notably, it is possible to execute such a ransomware attack by undermining any subcomponent of a computing system (c.f. Proofpoint 2023). However, ransomware attacks most commonly focus on undermining the availability or confidentiality of data (c.f. Kharraz et al. 2015). Indeed, some definitions of ransomware only include these types of ransomware attack, including the definition of the Cybersecurity and Infrastructure Security Agency in the United States (Cybersecurity and Agency 2023). Notably, using this type of attack necessarily leads to "a sudden and significant change in the file system activities" (McIntosh et al. 2018), and it is possible to

detect such attacks with this behavior before the full system is compromised (e.g., Continella et al. 2016).
Prior examples of well-known ransomware attacks include the NotPetya-attack in 2016 (Greenberg 2018) and the WannaCry-attack in 2017 (Newman 2017). Notably, con- trary to the Colonial Pipeline Incident, both focused on the encryption of data, instead of data theft.

The Colonial Incident

A more recent attack was the incident regarding the Colonial Pipeline in 2021: In the evening of 7 May 2021, Colonial Pipeline informed the public about the shutdown of one of their main pipelines, transporting 45% of the US East Coast's fuel supplies.[2] After a consultation with the FBI on the day following the incident, the company Colonial acknowledged that it had been hit by a ransomware attack. A month later, the chief executive of the pipeline company said they believed the hackers gained access to parts of the company's computer systems by exploiting a VPN connection (for which they possessed the credentials) not secured by two-factor authentication. How they acquired valid user credentials remains unclear (Krauss 2021). After gaining access to the system, the attackers executed a program that encrypted files on a computer system after copying them for further use by the criminals. Then, Colonial shut down the operational technology of the pipeline, preventing further fuel transportation. Several articles from different, independent publishers reported that this decision was made because the billing system had been disabled during the attack (Benner and Perlroth 2021; Bertrand et al. 2021; Day 2021; Zetter 2021). However, a spokesperson of Colonial denied these accusations (Nakashima et al. 2021). The authors do not have sufficient information to determine whether these accusations are objectively true or false. Shortly after the incident, the FBI accused the criminal group "DarkSide" of being involved in the attack. This group, presumably located in eastern Europa or Russia, provides ransomware services to third parties (based on their business model, it is unlikely they executed the attack personally). Within just a few days of the attack, DarkSide announced the ceasing of all its activities due to the large-scale impact of the attack. However, this was only after Colonial paid a 75 Bitcoin ransom, 64 of which would be recovered by a new task force of the justice department a month later.

Basic Defensive Concepts

This section briefly summarizes key defensive concepts and best practices used in IT security to defend against attacks. These examples illustrate that there are already established measures and standards (also including ISO 27001) to increase or ensure the security of digital systems. Thus, citizens that are informed about these standards can use their political influence to demand the fulfillment or increase of legislation.

Software Testing

Testing of software enables the detection of unintended behavior of the software. Frequently, such behavior (such as out-of-bounds reads or writes, or missing validation of user data) enables attackers to exploit a program for unintended purposes (such as gaining the ability to execute a program on a system). Established methods of software testing are presented in Hoffmann (2013); Resources such s the OWASP project lists common risks to look out for Open Web Application Security Project (2023).

Regular Updates

Software errors might only be detected at a point in time when the system is already running. New versions of software frequently resolve these errors ("security updates"). Updating software after such updates become available is necessary to ensure security (Aus- tralian Cyber Security Center 2023).

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

Secure Processes

Some attackers gain access to a system by exploiting its interaction with software. To prevent this, certain countermeasures are common. For example, there should be no master passwords that can be leaked or forgotten, and large but seldom changes to the system (such as the deletion or encryption of large amounts of data) should require multifactor authentication by multiple users. A summary of common attacks and countermeasures regarding secure processes are presented in Hadnagy (2010).

Levels of Defenses

Companies can deploy a multi-layered level of defense of a system. For example, they might employ a cybersecurity early warning system that raises alarms in case of extensive data activity (such as in the case of a ransomware attack) (Pohlmann 2019). This enables the company to shut down infected components from the network and prevent infection of other components, by detaching them from the network ("defense in depth", c.f. Smith 2003; Smith and Robinson 1999).

Fail Secure Deployment

Generally, a digital system should not enable a single point of failure. For example, this can be achieved by setting up the relevant components redundantly and backing up the data sets multiple times. Furthermore, failure in one component of the software should not lead to failure in a different component. A summary of common techniques (including "zero trust"-design of software) and advice is presented in Shostack (2014).

Analysis 1: Introducing "Ransomware Attack"

In this first analysis, we examine how the articles introduced the term "Ransomware Attack". This analysis is foundational, as this conceptual knowledge is crucial for under- standing the Colonial Pipeline Incident and sensible (political) consequences. We used Approach B to build the following criteria for introducing the concept. Then, we encoded whether the article explained this aspect or not for each aspect. A definition we considered satisfactory would include all of the following aspects:

A ransomware attack is performed by
gaining access to a computer system and then (11 articles)
executing a program on the victim's computer. (3 articles)
One option (*Data Loss*) to execute a ransomware attack is by
denying access to specific systems or data (42 articles)
by encrypting data with the program and then (23 articles)
demanding money to restore access to this data (41 articles)
by providing the decryption key. (9 articles)
Another option (*Data Breach*) for executing a ransomware attack is
copying sensitive data with the program and then (14 articles)
demanding money for keeping this data confidential. (13 articles)

Almost half of the 109 articles (45) introduced the term ransomware attacks to the readers. Articles that did not explain it focused less on "What happened to the Colonial Pipeline?" and more on "What are the implications of the outage?" (i.e., fuel shortage). However, no article explained all aspects of this definition. A single article introduced all aspects in 1 and 2 but did not present the alternative attacking method in 3. Most articles focused on aspects 2a and 2c. This was frequently phrased as "attackers seize control of a computer until the victim pays a fee." Many articles did not differentiate whether access to a computer, a computer system, or data was locked. Furthermore, the technical details in 2b and especially 2d were omitted. Lastly, the attack requirement (getting access to the system and executing a program) was very often excluded. As such, it remained unclear

what precisely the attack was or how it was executed. Instead, the descriptions focused on the results: lack of access to the data or access to the data by an unwanted source.

Overall, around half of the articles introduced the basic concept of the attack but neglected most technical details.

Analysis 2: Detailed Information on Ransomware Attacks

In this second analysis, we use Approach C to list additional context or background information that could lead to additional insights into ransomware attacks in general.

Procedure of General Ransomware Attacks

Most articles included no additional information regarding the procedure of ran- somware attacks. Eleven articles noted at least one of the following aspects:

Payment of the ransom incentives further attacks. (9 articles)

Access to the encryption key does not automatically enable one to get the system to run again. Instead, this can be a complex activity. (3 articles)

Paying the ransom to access the decryption key cannot guarantee access to the (right) decryption key(s). (2 articles)

The company behind the Colonial Pipeline paid the ransom but still struggled to rebuild the system. (1 article)

Three articles explained two of these aspects. The remaining articles explained one each. No article explained why a statement was true.

Vulnerabilities Enabling Ransomware Attacks

Five articles contained some information regarding vulnerabilities that enable ran- somware attacks:

Frequently, access to computer systems is gained by phishing. (3 articles)

Leaked password lists might enable access to computer systems. (2 articles)

Notably, no article noted software vulnerabilities as a potential entry point for ransomware attacks. No article explained how exactly these aspects enable attackers to execute an attack.

Defenses against Ransomware Attacks

Thirteen articles explained possible defenses against ransomware attacks.:

Multi-factor authentication. (8 articles)

Backups of data. (6 articles)[3]

Zero-trust design of software. (4 articles)

Utilization of firewalls. (1 article)

Protecting the company data with encryption. (1 article)[4]

Regular security updates. (1 article)

Most articles include no explanations of possible defenses and countermeasures. Most articles did not explain how or why these mechanisms would help defend against ransomware attacks or against what aspect of an attack they would help. Notably, they also did not specify whether they would have helped in the Colonial incident or if they are practical for businesses.

Analysis 3: Presentation of the Incident

The third analysis discusses how articles presented the incident and how many articles used which approach. This presentation is essential, as citizens without prior knowledge of ransomware attacks likely derive answers for questions such as “What happened?”, “Who is to blame?”, and “What should be done?” from these articles.

Chain of Events of the Incident

We used approach A to analyze how the articles described the chain of events between the ransomware attacks and the shutdown of fuel transport. The following categories of descriptions emerged:[5]

First, there was a ransomware attack. Then, there was no fuel transport anymore. (14 articles)

First, there was a ransomware attack. Then, the Pipeline shut down and there was no fuel transport anymore. (18 articles)

First, there was a ransomware attack. Then, Colonial shut down the Pipeline, stopping the fuel transport. (5 articles)

First, there was a ransomware attack. Then, Colonial shut down the Pipeline because their billing system was disabled. Then, there was no fuel transport. (5 articles)

The vast majority of articles focused on the result of the incident (a lack of fuel transport). Only ten articles highlighted that the *direct* cause of the shutdown was a decision to shut down by Colonial. Notably, 32 articles denoted that the pipeline was attacked and that it shut down, without an explicit connection between both events.

Framing of the Incident

No article framed the responsibility for the incident differently from "Colonial was the victim of a ransomware attack". One article also included the perspective that companies have a responsibility to secure their digital systems: "The shutdown of the Colonial Pipeline by cyber criminals highlights a massive problem — many of the companies running our critical infrastructure have left their systems vulnerable to hackers through dangerously negligent cybersecurity," Sen. Ron Wyden (D-OR) said in a statement. "Congress must take action to hold critical infrastructure companies accountable and force them to secure their computer systems" (Morrison 2021).

Attributing for the Incident

Attributing the attacker was limited to attribution to the creator of the software. Earlier articles did not include any attribution. We used method A to classify the 25 articles that denoted an attacker:

The attack was executed by DarkSide. (18 articles)

The attack was executed with the software of DarkSide. (4 articles)

The attack was executed either by DarkSide or by hackers using the software of DarkSide. (2 articles)

The attack was executed by a criminal group. (1 article)

Attribution was done either by referring to the FBI (13 articles), unnamed sources (4 articles), to the ransom demand (1 article), as a publicly known fact (4 articles), or without a source (3 articles).

Only one article highlighted that attributing cyberattacks is difficult; another one even deemed it impossible.

Political Consequences of the Incident

Last, we used method C to analyze the political consequences of the incident that were proposed or explained by the articles. The following consequences were mentioned more than five times:[6]

Companies must now report cybersecurity incidents. (10 articles)[7]

Companies are now being demanded to assess the security of their systems. (10 articles, no further details were provided)

The USA should pressure Russia because they do not act against ransomware groups in their territory. (9 articles)

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

Biden signed a new executive order for more security. (8 articles, no further details were provided in these articles)
There should be higher mandatory and technical security standards. (7 articles, all gave at least one example)[8]
The government should go after cryptocurrencies (7 articles, two of which outlined
how this would be possible)
There is now a task force at the justice department. (6 articles, no further details were provided)
More money should be invested. (5 articles, no details)

Analysis 4: Potential Misconceptions

The prior analysis showed that most media articles focused on the real-world conse- quences of the ransomware attack, i.e., primarily the fuel shortages (c.f. Section 4). Notably, this focus was true even if the corresponding article defined the term ransomware attack, i.e., tried to explain the concept to its readers. Only a few articles explained in detail how ransomware attacks are executed and, consequently, focused a little on what can be done to prevent them (c.f. Section 5)—both regarding critical infrastructure such as Colonial and privately for ones own systems. Unfortunately, this lack of explanation can lead to several misconceptions about ransomware attacks. In this section, we derive four such potential misconceptions, argue why these misconceptions are wrong, and explain how they can be countered.

Misconception 1: Bad Weather

The first misconception can be stated as follows: "Unfortunately, computer systems are sometimes shut down by ransomware attacks." We call this the *Bad Weather* misconception, as it is similar to how a leisure activity can fall through because of bad weather. This misconception implicates that ransomware attacks are just unfortunate and random events, because they are both unforeseen and inevitable. This is wrong, as ransomware attacks are neither random, nor inevitable, nor necessarily unforeseen (c.f Pohlmann 2019). However, this misconception might by caused by the fact that most articles did not explain the prerequisites of the attack (system access and insufficient levels of defenses), only its effect after completion (c.f. Section 4). Instead, there are established measures to prevent, detect, and counter ransomware attacks—both prior, during, and after an incident (c.f. Section 3.4). To counter this misconception, one should know about (the existence of) such measures and the requirements for an attack (system access).

Misconception 2: Bank Robbery

The second misconception can be stated as follows: "In a ransomware attack, the helpless victim has no choice but to do as the attackers bid". We call this the *Bank Robbery* misconception, as it is similar to a situation where a bank employee has to do as a bank robber orders because they have a gun pointed towards their chest. This is a misconception, as security preparations are crucial for determining possible choices: With sufficient prepa- rations, it can be possible to restore systems (e.g., with a backup, c.f. Shostack 2014). This misconception might by caused by the fact that only a few articles explained the options available to Colonial and instead focused on the fact that they paid the ransom (while frequently not reporting the fact that, despite this, they were unable to restore access to their systems, c.f. Section 5.1). To counter this misconception, one needs to know about measures to prevent and react to ransomware. Applying this knowledge also requires technical details of the attack (which systems were affected and how) and the procedure (when and who decided to shut down which system).

Misconception 3: Easy Attribution

The third misconception can be stated as follows: "It is easy to attribute an attack to a real-world entity". This would imply that denying responsibility for an attack is hard

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

and suggests that false-flag attacks are infrequent. This is a misconception, as there is no direct or objectively verifiable connection between data (such as code to be executed on the victim machine or a network stream containing said code) to the technical entity that created it. Furthermore, there is also no direct connection between that technical entity and a real-life entity. In fact, a common way to hide an attack is by first compromising an intermediate entity and performing the actual attack from that entity. However, only two articles highlighted that making an attribution is hard, while 18 articles denoted an attacker with certainty; frequently using arguments from authority in this process (c.f. Section 6.3). To counter this misconception, it is sufficient to know that there is no direct connection between data and real-world entities. However, deeper knowledge about the methods used to infer these entities (e.g., by using a log of all network activity to trace a stream of data back to the first sender) is beneficial to better understand why digital attribution might sometimes be possible, why it is hard, and how likely it is to succeed.

Misconception 4: Innocent Victim

The fourth *Innocent Victim* misconception can be stated as follows: "A company hit by ransomware is an innocent victim of an evil attacker." The unspoken implication is that asking about the responsibility of the company would be "victim-blaming" (Eigenberg and Garland 2008) and, as such, morally wrong. This is a misconception, as companies are responsible for securing their systems and preventing attacks. In fact, the "dangerously negligent cybersecurity" (Morrison 2021) of companies, or "systems [that] weren´t properly secured" (Bustillo 2021), are frequently used as justification for laws demanding certain technical standards. Notably, the view that companies must raise their security standards is almost undisputed by experts: "The time has come for government to mandate that companies vital to U.S. national and economic security meet basic cybersecurity standards, according to a vast majority of cybersecurity experts" (Marks 2021). To counter this misconception, one can point towards this responsibility and the consensus that current software frequently lacks security. It might also be advisable to differentiate between "the incident" (including everything that happened) and "the attack" (focused on the technical attack and its direct, i.e., technical, consequences).

Implications

As shown in the analysis, only a few articles contained the information necessary to counter the misconceptions presented in the last analysis. Furthermore, some aspects that are both relevant for reflecting on the incident and uncontroversial among experts (e.g., companies are responsible for securing their systems) were widely ignored in both the content and presentation of the articles. This impacts perceptions: After reading the story "Colonial was, unfortunately, an innocent victim of Russian hackers and helplessly watched as their pipeline was disabled", one might argue that a sensible consequence might be to pressure Russia to do something about "their" hackers. However, after reading the story "Colonial neglected its security which enabled unknown attackers to deactivate their billing system. Then, Colonial shut down their pipeline voluntarily", one might ask for higher technical standards and discuss whether companies should be allowed to issue such a shutdown.

In the articles we read, most framed the incident closer to the first story.[9] Notably,
knowing about the four proposed misconceptions enables a more critical reflection of this story; it is apparent that many details are not typical for ransomware incidents. Thus, readers might be inclined to search for more information to understand the situation, fostering their ability to meaningfully participate in the corresponding political debates. Overall, given the significant consequences of ransomware attacks (both for indi- viduals, companies, and society), we argue that the general education of citizens should enable them to reflect on ransomware incidents critically. Furthermore, given some of the proposed political consequences (such as new laws or pressuring another state), we argue that citizens should also critically reflect on the reporting of public incidents. However, as

shown earlier, the articles we analyzed explained the concept insufficiently for political mature participation in the corresponding political debates.

Owing to this, it is desirable to have a public debate about the relevance of formalized teaching on this topic, or other measures to increase awareness and background knowledge of ransomware attacks and suitable defense mechanisms and regulation to prevent or mitigate the damage caused by them. As of now, it seems likely that the knowledge necessary for meaningful public discussion is neither conveyed in schools, nor by other means of informal education, such as in news articles.

Limitations

This article analyzed the reporting on an ransomware incident and potential miscon- ceptions that might stem from it. However, there are limitations that demand reflection.

First and foremost, only 45 of the articles we analyzed introduced the concept of ransomware attacks. As such, it might have been sensible to only use those articles as the baseline for the percentage of articles that introduced certain concepts. Nevertheless, even with this lower baseline, the majority of articles failed to introduce technically relevant concepts and details.

Second, we did not analyze whether the different types of articles (from newspapers and tech blogs) influenced the way the information was presented. During our analysis, we got the impression that the tech blogs presented slightly more detailed information. However, we assumed that the overall quality would not have increased by much if focusing this analysis only on articles from tech blogs.

Third, we focused on the consequences of the misconceptions for political participation. An additional analysis might have highlighted the consequences for *personal* decisions of citizens. For example, the articles we read included almost no information relevant for the security of systems the readers might possess (such as, a NAS that should be updated regularly).

Last, there were technical problems with the article selection[10] and one could argue that more articles from more publishers should have been analyzed. However, after reading over 100 articles, we assumed that more or different articles would not influence the overall results too much. However, we argue that such an analysis should be repeated with a different ransomware incident or even a different type of security incident, to obtain a more representative picture of the corresponding media reporting.

Conclusions and Future Work

This article analyzed the reporting on the Colonial Pipeline incident. We showed that the majority of articles focused on the consequences of the shutdown, rather than the attack, even if focusing solely on the articles that introduced the concept of ransomware attacks. Importantly, several crucial aspects such as technical countermeasures were introduced only in a handful of articles. Based on this lack of background information, we derived four misconceptions that readers might receive from this reporting about ransomware attacks. We showed the relevance of these misconceptions to the reflection on the incident and desirable political consequences following from it. We also outlined technical knowledge relevant to countering these misconceptions in formal education. This knowledge can help teachers in preparing their lessons and focusing on important aspects. As a next step, it is desirable to analyze the prevalence of these misconceptions in practice (both by citizen and the journalists writing these articles) to allow a better understanding of the scope of the problem.

Supplementary Materials: The following supporting information can be downloaded at: https: //www.mdpi.com/article/10.3390/socsci12050265/s1.

Author Contributions: Conceptualization, A.G. and D.A.; methodology, A.G.; software, A.G. and D.A.; validation, A.G. and D.A. and M.H.; formal analysis, A.G. and D.A. and M.H.; investigation,
A.G. and D.A.; resources, M.H.; data curation, A.G. and D.A.; writing—original draft preparation,

A.G. und D.A.; writing—review and editing, A.G.; visualization, Not Applicable; supervision, M.H.; project administration, A.G.; funding acquisition, M.H. 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: An Excel Table containing URLs to all articles is available in the supplementary material section. Due to copyright constraints, the articles themselves (or the phrases extracted) cannot be published by the authors.

Conflicts of Interest: The authors declare no conflict of interest. No author is affiliated with Colo- nial or any of the publishers analyzed in this publication. The authors only had access to public information.

Notes

[1] Usually, (cyber-)attacks are defined more abstractly. However, this definition is both sufficient for this paper and compatible with common definitions (c.f. Bay 2016; Kissel 2011).

[2] The following summary of this incident is derived from the consensus of all media articles we read for our analysis. It represents our best effort to summarize the incident based on our knowledge at the time of submission. We have neither original data nor first-person insights, and some of the information provided here might turn out to be incomplete, misleading, or even wrong.

[3] The articles did not mention that this does not help against the second attack option.

[4] The article does not mention this does not help against the first attack option.

[5] Articles are classified by the most detailed description that applies.

[6] Consequences are only denoted in this list, if they were presented as consequences. Phrases such as "The attackers profited from low cybersecurity standards" do not count towards "There should be higher cybersecurity standards". Ten additional consequences were denoted in fewer articles, including one article arguing that companies should be liable for damages caused to customers because of cyberattacks.

[7] This demand, as well as the second and last in this list stems from an executive order issued by Biden after the attack.

[8] Four more articles mentioned that low standards are a problem. Three further articles demanded higher standards, but it is unclear whether these articles refer to technical standards or proposals such as having to report incidents. One further article mentioned that some companies do not treat security earnestly enough.

[9] We do not claim that either of the stories are objectively appropriate for this specific incident: The contextual information to objectively and definitely judge one way or the other is either disputed or not available to the public (including the authors).

[10] Due to these problems, rather than using the programmable search engine, the second author used the internal search engine of the tech blogs and manually collected all articles between 6 May 2021 and 1 August 2021. The same was true for the Houston Chronicle and the Star Tribute. For unclear reasons, only a total of five articles could be found for the Star Tribune, among a large number of dead links.

References

Alwan, Almahdi Ali. 2011. Misconception of heat and temperature among physics students. *Procedia-Social and Behavioral Sciences* 12: 600–14.

Australian Cyber Security Center. 2023. How to update your device and software. Available online: https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-update-your-device-and-software (accessed on 27 April 2023).

Axell, Cecilia, Astrid Berg, Jonas Hallström, Sam Thellman, and Tom Ziemke. 2022. Artificial intelligence in contemporary children's culture: A case study. In *PATT 39. PATT on the Edge Technology, Innovation and Education. St. John's, Newfoundland and Labrador, Canada June 21st–24th, 2022*. St. John's: Memorial University of Newfoundland, pp. 376–86.

Bay, Morten. 2016. What is cybersecurity? *French Journal for Media Research* 6: 1–28.

Beaubouef, Theresa, and Patrick McDowell. 2008. Computer science: student myths and misconceptions. *Journal of Computing Sciences in Colleges* 23: 43–48.

Benner, Katie, and Nicole Perlroth. 2021. U.S. seizes share of ransom from hackers in colonial pipeline attack. *The New York Times*, June 7.

Bertrand, Natasha, Evan Perez, Zachary Cohen, Geneva Sands, and Josh Campbell. 2021. Colonial pipeline did pay ransom to hackers, sources now say. *CNN*, May 12.

Brinda, Torsten, Michael Fothe, Steffen Friedrich, Bernhard Koerber, Hermann Puhlmann, Gerhard Röhner, and Carsten Schulte. 2008. *Grundsätze und standards für die informatik in der schule-bildungsstandards informatik für die sekundarstufe i*. Bonn: Gesellschaft für Informatik eV.
Bustillo, Miguel. 2021. Cyberattack forces closure of largest U.S. refined-fuel pipeline. *Wall Street Journal*, May 8.
Continella, Andrea, Alessandro Guagnelli, Giovanni Zingaro, Giulio De Pasquale, Alessandro Barenghi, Stefano Zanero, and Federico Maggi. 2016. Shieldfs: A self-healing, ransomware-aware filesystem. Paper presented at 32nd Annual Conference on Computer Security Applications, Los Angeles, CA, USA, December 5–8, pp. 336–347. https://doi.org/10.1145/2991079.2991110.
Cybersecurity and Infrastructure Security Agency. 2023. Stop Ransomware|cisa. Available online: https://www.cisa.gov/stopransomware (accessed on 23 April 2023).
Day, Lewin. 2021. The colonial pipeline is finally back online and pumping gas. *The Drive*, May 12.
Diethelm, Ira, and Stefan Zumbrägel. 2010. Wie funktioniert eigentlich das internet?-empirische untersuchung von schülervorstellun- gen. In *Didaktik der Informatik. Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik*. Bonn: Gesellschaft für Informatik e.V.
Eigenberg, Helen, and Tammy Garland. 2008. Victim blaming. In *Controversies in Victimology*. London: Routledge, pp. 33–48. Greenberg, Andy. 2018. The untold story of notpetya, the most devastating cyberattack in history. *Wired*, August 22.
Hadnagy, Christopher. 2010. *Social Engineering: The Art of Human Hacking*. Hoboken: John Wiley & Sons. Hassan, Nihad. 2019. *Ransomware Revealed*. Cham: Springer.
Hatziapostolou, Thanos, Anna Sotiriadou, and Petros Kefalas. 2008. Promoting computer science programmes to potential students: 10 myths for computer science. Paper presented at the 3rd Informatics Education Europe, Venice, Italy, December 4–5.
Hennecke, Martin. 2015. Modellvorstellungen zum aufbau des internets. In *Informatik Allgemeinbildend Begreifen*. Bonn: Gesellschaft für Informatik e.V.
Hoffmann, Dirk. 2013. *Software-Qualitat*. Berlin: Springer.
Hu, Siqi, Carol Hsu, and Zhongyun Zhou. 2022. Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems* 62: 752–64.
Institute for Security and Technology. 2021. Combating Ransomware. Available online: https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf (accessed on 27 April 2023).
Kaczmarczyk, Lisa C., Elizabeth R. Petrick, J. Philip East, and Geoffrey L. Herman. 2010. Identifying student misconceptions of programming. Paper presented at 41st ACM Technical Symposium on Computer Science Education, Milwaukee, WI, USA, March 10–13, pp. 107–111.
Kaltakci, Derya, and Nilüfer Didis¸. 2007. Identification of pre-service physics teachers' misconceptions on gravity concept: a study with a 3-tier misconception test. In *AIP Conference Proceedings*. College Park: American Institute of Physics, vol. 899, pp. 499–500.
Kharraz, Amin, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. 2015. Cutting the gordian knot: A look under the hood of ransomware attacks. Paper presented at 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Milan, Italy, July 9–10, pp. 3–24.
Kissel, Richard. 2011. *Glossary of Key Information Security Terms*. Collingdale: Diane Publishing.
Krauss, Clifford. 2021. Colonial pipeline chief says an oversight let hackers into its system. *The New York Times*, June 8.
Krutz, Ronald L., and Russell Dean Vines. 2010. *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Hoboken: John Wiley & Sons Inc.
Kuckartz, Udo. 2019. *Qualitative Text Analysis: A Systematic Approach*. Cham: Springer International Publishing, pp. 181–97. https://doi.org/10.1007/978-3-030-15636-7_8.
Lucariello, Joan, and David Naff. 2013. *How Do I Get My Students over Their Alternative Conceptions (Misconceptions) for Learning*. Washington, DC: American Psychological Association.
Marks, Joseph. 2021. The cybersecurity 202: Our expert network says it's time for more cybersecurity regulations. *The Washington Post*, June 11.
McIntosh, Timothy, A. S. M. Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. 2021. Ransomware mitigation in the modern era: A comprehensive review, research challenges, and future directions. *ACM Comput. Surv.* 54: 197. https://doi.org/10.1145/3479393.
McIntosh, Timothy R., Julian Jang-Jaccard, and Paul A. Watters. 2018. Large scale behavioral analysis of ransomware attacks. In *Neural Information Processing*. Edited by Long Cheng, Andrew Chi Sing Leung, Seiichi Ozawa. Cham: Springer International Publishing, pp. 217–29.
Mertala, Pekka, Janne Fagerlund, and Oscar Calderon. 2022. Finnish 5th and 6th grade students' pre-instructional conceptions of artificial intelligence (ai) and their implications for ai literacy education. *Computers and Education: Artificial Intelligence* 3: 100095.
Mohyuddin, Rana Ghulam and Usman Khalil. 2016. Misconceptions of students in learning mathematics at primary level. *Bulletin of Education and Research* 38: 133–62.
Morrison, Sara. 2021. How a major oil pipeline got held for ransom. *Vox*, June 8.
Nakashima, Ellen, Lori Aratani, and Douglas MacMillan. 2021. Colonial hack exposed government's light-touch oversight of pipeline cybersecurity. *Houston Chronicles*, May 30.
Newman, Lily Hay. 2017. The ransomware meltdown experts warned about is here. *Wired*, May 12.
Ojose, Bobby. 2015. Students' misconceptions in mathematics: Analysis of remedies and what research says. *Ohio Journal of School Mathematics* 72: 30–34.

Open Web Application Security Project. 2023 Open Web Application Security Project: Owasp Top Ten. Available online: https://owasp.org/www-project-top-ten/ (accessed on 27 April 2023).
Pancratz, Nils, and Alexander Schlegel. 2021. Lehrerperspektiven auf die rekonstruktion von schüler-vorstellungen im informatikunterricht. In *INFOS 2021-19. GI-Fachtagung Informatik und Schule*. Bonn: Gesellschaft für Informatik.
Pohlmann, Norbert. 2019. *Cyber-Sicherheit: das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Wiesbaden: Springer Fachmedien Wiesbaden GmbHSpringer Vieweg.
Proofpoint. 2023. What Is Ransomware? Available online: https://www.proofpoint.com/threat-reference/ransomware (accessed on 25 April 2023).
Qian, Yizhou, and James Lehman. 2017. Students' misconceptions and other difficulties in introductory programming: A literature review. *ACM Transactions on Computing Education (TOCE)* 18: 1–24.
Schott-Maire, Ulrike, Manuel Riel, and Ralf Romeike. 2021. Expertenmeinungen über bildung zur it-sicherheit: Was jeder mensch wissen sollte! In *INFOS 2021-19. GI-Fachtagung Informatik und Schule*. Edited by Ludger Humbert. Bonn: Gesellschaft für Informatik, pp. 83–92. https://doi.org/10.18420/infos2021_f258.
Shostack, Adam. 2014. *Threat Modeling: Designing for Security*. Indianapolis: John Wiley and Sons.
Smith, Clifton L. 2003. Understanding concepts in the defence in depth strategy. Paper presented at IEEE 37th Annual 2003 International Carnahan Conference onSecurity Technology, Taipei, Taiwan, October 14–16, pp. 8–16. https://doi.org/10.1109/CCST.2003.1297528.
Smith, Clifton L., and Robinson, Mike. 1999. The understanding of security technology and its applications. Paper presented at IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology (Cat. No. 99CH36303), Madrid, Spain, October 5–7, pp. 26–37.
Staatsinstitut für Schulqualität und Bildungsforschung München. Lehrplan Natur und Technik (Informatik). 2023 Available online: https://www.lehrplanplus.bayern.de/fachlehrplan/gymnasium/7/nt_gym (accessed on 15 January 2022).
Tsarava, Katerina, Manuel Ninaus, Tereza Hannemann, Kristina Volná, Korbinian Moeller, and Cyril Brom. 2020. Fostering knowledge of computer viruses among children: The effects of a lesson with a cartoon series. Paper presented at Koli Calling'20: Proceedings of the 20th Koli Calling International Conference on Computing Education Research, Koli, Finland, November 19–22, pp. 1–9.
Uhden, Olaf. 2016. Verständnisprobleme von schülerinnen und schülern beim verbinden von physik und mathematik. *Zeitschrift für Didaktik der Naturwissenschaften* 22: 13–24.
Vom Hofe, Rudolf and Werner Blum. 2016. "grundvorstellungen" as a category of subject-matter didactics. *Journal für Mathematik-Didaktik* 37: 225–54.
Wang, Pei. 2007. Three fundamental misconceptions of artificial intelligence. *Journal of Experimental & Theoretical Artificial Intelligence* 19: 249–68.
Wang, Pei, Kai Liu, and Quinn Dougherty. 2018. Conceptions of artificial intelligence and singularity. *Information* 9: 79.
Yang, T. Andrew. 2001. Computer security and impact on computer science education. *Journal of Computing Sciences in Colleges* 16: 233–46.
Zetter, Kim. 2021. Us gov issues emergency order while colonial pipeline is down. *Zero Day*, May 9.

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.