Student: Lucas George Sipos
Student ID: 24292215

Table of Contents

Student: Lucas George Sipos
Student ID: 24292215

Comparative Analysis of Cyberattack Reporting Across Diverse Media Outlets

Introduction

Cyberattacks have been growing in frequency in the digital age, affecting people and organisations from all over the world. An important case study for getting to know how different outlets of journalism describe cybersecurity unfortunate events is the recent cyberattack on Orange Group, one of the most significant French telecom service providers. The analysis below focuses on the press coverage of the Orange cyberattack with regard to three different categories of news outlets: mainstream media, technical news sources, and cybersecurity news platforms. The study will look into the attack vector, the compromised entities, suggestions for countermeasures, and the more general cybersecurity consequences.

Background of Orange Group

Orange Group is one of the largest telecommunications providers in Europe, serving millions of customers across various countries. The company supplies many different types of services, which include digital solutions, internet services, and mobile communications. Orange Group has become an international player in the telecommunications industry, making their customer data and infrastructure extremely intriguing targets for cybercriminals. This incident is especially important because the most recent breach has demonstrated just how vulnerable such well-established companies can be to cyberattacks.

Attack Vector and Technical Details

Mainstream Media: Capacity Media

The full details of the cyberattack can be found in Capacity Media's report[3]. According to the article, a "non-critical application" that was utilized by Orange's Romanian branch was actually the source of the breach. Despite this, the report simply points out that approximately 12,000 files were stolen and does not contain significant technical details. The media outlet seems to have focused on providing simple to understand news to a larger audience, considering that it provides absolutely no mention of the exact vulnerabilities exploited or the attacker's method of access. This lack of technical detail could make it more complicated for the reader to fully understand how the breach happened and whether there are security vulnerabilities in Orange's infrastructure.

Student: Lucas George Sipos
Student ID: 24292215

Technical News Source: BleepingComputer

A much more detailed explanation of the attack vector is to be observed on BleepingComputer[1]. According to the report, the hacker, known as Rey, took advantage of compromised credentials and vulnerabilities in Orange's Jira software, which tracks bugs and issues. BleepingComputer also verifies that the attacker was actually able to access the system for more than a month before they started stealing data during a three-hour timeframe. Such technical information has been included to appeal to a more informed audience who are familiar with cybersecurity concepts. The post provides additional information to the report by emphasising that, despite the attacker sending out a ransom note, the breach was not a ransomware attack.

Cybersecurity News Source: CyberNews

CyberNews publishes in-depth technical analysis as well, supporting their claim that compromised credentials plus Jira software vulnerabilities were used[2]. Similarly with the hacker's own claim that the breach was not a HellCat ransomware operation, the report also highlights the hacker's technique to indicate that no ransomware was deployed. Concerns on similar vulnerabilities in other companies are further addressed by CyberNews' analysis of the larger implications of exploiting Jira software, a popular project management application.

Entities Compromised and Impact

Mainstream Media

Capacity Media briefly mentions that employee and customer information was compromised and focuses on the quantity of stolen files. The report does not, however, distinguish between the different information categories compromised or analyse any potential impact on Orange's business or clients. This limited analysis may reduce the risks to the affected people by giving the false impression that the breach was less serious than it actually was.

Technical News Source

The article on BleepingComputer goes into more details regarding the leaked data, claiming that it comprised 380,000 different email addresses, invoices, contracts, partial payment card information, and customer records. Furthermore, the report pointed out that the majority of the stolen data was outdated, which helped minimize some of the immediate risks related to the breach. Still, the existence of any customer data, even outdated data, remains a serious privacy issue and emphasizes the importance of strong data security measures.

Student: Lucas George Sipos
Student ID: 24292215

Cybersecurity News Source

In spite of publishing a similar analysis of the stolen data, CyberNews goes a bit further and mentions Yoxo customers, Orange's subscription service without a contract period, as being impacted. This focus on specifics draws attention to the type of services that are at risk as well as the breach's larger effects. Concerns are also raised in the report over the public release of internal project plans, which can have long-term effects on Orange's position on the market and business operations.

Mitigation Efforts and Resolutions

Mainstream Media

According to Capacity Media, Orange responded right away to protect the private data of its partners, customers, and employees. The article, however, doesn't go into additional detail about what has been done to minimize the breach or any type of collaboration with cybersecurity authorities. Readers might not completely understand the company's response to the attack as a result of this lack of given information.

Technical News Source

Orange's IT and cybersecurity teams are actively investigating the scope of the attack and trying to minimize the impact, as reported by BleepingComputer. According to the publisher, Orange is committed to giving frequent updates and is working with law enforcement. The outlet's more technical and analytical approach can be seen in the inclusion of mitigation measures. The article also emphasizes the importance of communication and transparency of the following days after the cyberattack.

Cybersecurity News Source

BleepingComputer's findings were also reported by CyberNews, which highlights that Orange's cybersecurity teams are collaborating closely with authorities to assess the damage. The article also emphasizes Orange's commitment to meeting its legal responsibilities regarding data breaches, highlighting the ethical implications of the company's response. CyberNews also looks at some long-term actions Orange could be taking in order to prevent breaches in the future, like strengthening access controls and fixing vulnerabilities in third-party software.

Student: Lucas George Sipos
Student ID: 24292215

Evaluation of Reporting Depth, Accuracy, and Bias

There are considerable differences in the depth, accuracy, and bias of the media's coverage of the Orange Group cyberattack. Platforms for technical and cybersecurity news, like BleepingComputer and CyberNews, provide in-depth analysis to an experienced audience. Technical details such as the attack vector, exploited vulnerabilities, and the scope of the data breach are presented by these outlets. On the other hand, mainstream media outlets such as Capacity Media tend to focus on readability and present basic coverage, and frequently leave out important technical information.

The accuracy of reporting aligns with the depth of coverage. CyberNews and BleepingComputer support each other's conclusions, increasing their credibility. Though not incorrect, Capacity Media's general summary is not detailed enough to fully capture the complexity of the attack. This difference shows how the media outlet's level of experience influences the amount of information it publishes.

These sources are further distinguished by bias. In order to avoid public panic, mainstream media usually takes a calm and unbiased approach, sometimes minimising the gravity of the breach. Technical and cybersecurity news sources, on the other hand, target a more skilled and analytical audience by highlighting the risks and vulnerabilities exposed by the breach. This difference in viewpoint shows how the media influences the public's perception of cybersecurity threats with both technical analysis and general understanding being important parts of accurate reporting.

Conclusion

The different methods used by technical, mainstream, and cybersecurity news outlets to report the cyberattacks are shown by this assessment. Technical and cybersecurity platforms provide more in-depth and critical insights, while mainstream media focuses on accessibility and comfort. Having a better understanding of cybersecurity threats and the media's influence on public opinion needs an understanding of these distinctions. Accurate, complete, and honest reporting will be more and more important as cyberattacks continue to increase in complexity and frequency.

Student: Lucas George Sipos
Student ID: 24292215

Works Cited

1. **Ilascu, Ionut.** *BleepingComputer.* [Online] February 25, 2025. https://www.bleepingcomputer.com/news/security/orange-group-confirms-breach-after-hacker-leaks-company-documents/.

2. **Mous, Anton.** *CyberNews.* [Online] February 2025, 2025. https://cybernews.com/security/orange-group-confirms-data-breach/.

3. **Sensi, Jasdip.** *Capacity Media.* [Online] February 27, 2025. https://www.capacitymedia.com/article/orange-cyberattack.