Ransomware and Network Vulnerabilities

1st Raquel Carneiro
Dept. de Ciência de Computadores
FCUP
Porto, Portugal
raquelmcarneiro16@gmail.com

2nd Patrícia Miranda
Dept. de Ciência de Computadores
FCUP
Porto, Portugal
spatricialm37@gmail.com

3rd Tomás Carmo
Dept. de Ciência de Computadores
FCUP
Porto, Portugal
tomas.alportel@gmail.com

***Abstract*—Ransomware, a significant cyber threat, involves malicious software that locks or encrypts data and demands ransoms for its release. The emergence of Ransomware-as-a-Service (RaaS) has democratized the means to conduct such attacks, even for non-technical individuals, thereby increasing the scale and frequency of these threats. High-profile attacks like WannaCry have demonstrated ransomware's destructive capacity, leading to losses in the billions and affecting critical industries. As ransomware tactics continue to evolve, encompassing double and triple extortion and targeting political entities, the urgency for robust cybersecurity defenses becomes paramount. This report explores the historical context, evolution, and current state of ransomware, revealing common vulnerabilities and the urgent need for proactive defense strategies in the face of this dynamic and persistent cyber challenge.**

***Index Terms*—Ransomware, Phishing, Remote Desktop Protocol, Ransomware History, Cryptography, Cryptocurrency, Cyberattacks, WannaCry, NotPetya**

I. Introduction

Cyber criminals recognize that data, files, and digital infrastructure are vital components for the smooth operation and advancement of any business. Given the immense value of these digital assets to a business, the most lucrative and convenient method for attackers to make profits is by seizing control of and demanding a ransom for these resources. [1]

Malware, short for malicious software, refers to a broad category of software designed to harm or exploit any programmable device, service, or network. Within existing malware, ransomware stands out as a particularly subtle strain until its shown to the user. Ransomware sets itself apart from other types of malware by actively extorting victims by data encryption or locking, then charging for the release of the data. Ransomware can be broadly classified into two categories: crypto and locker. The most prevalent type, crypto ransomware, uses advanced algorithms to secretly encrypt important files, in order to prevent people from accessing their own data. The users are met with demands for payment - usually in a hard-to-trace cryptocurrency - in exchange for the decryption key, along with a countdown to induce an atmosphere of urgency. Examples in this category include 'CyproLocker', 'Locky' and 'CryptoWall', which includes the most recognisable ransomware that went viral globally in 2017, named 'WannaCry'. The global financial damage caused by this attack reached 4 billion dollars.[2]

Locker ransomware, on the other hand, takes a more blunt approach; instead of encrypting files, hampers access to the entire system. The screen displays a ransom note prohibiting access to all system functions, rendering the computer inoperable until the ransom is paid, creating a sense of helplessness and panic among users. 'TorrentLocker', 'Locky', 'Winlocker', and 'Reveton' are some examples. [3] Sometimes, even after the ransom has been paid, the attacker refuses to unlock the user's device.

Ransomware is becoming an increasingly important issue as organizations become more reliant on IT infrastructure. This form of malware causes significant damage to organizations and has recently evolved into a new variant known as Ransomware-as-a-Service *(RaaS)*.

RaaS can be defined as a business model between ransomware operators and affiliates, where affiliates pay to launch ransomware attacks developed by the operators. [2] Such a model illustrates the collaborative ecosystem that exists among cybercriminals: one group focuses on creating and managing the ransomware code, while another plans the dissemination and execution of the attacks. Both groups benefit financially from successful ransomware campaigns, sharing the illicit profits generated by extorting victims.

Adapting to the digital age, Ransomware-as-a-service has turned these attacks into a common commodity, allowing individuals with no technical skills to execute ransomware attacks, thereby expanding the range of potential threats. This service includes user-friendly interfaces, customer support, updates, and sometimes even dashboards to track the success of the attacks, further highlighting the paradoxical professionalism that exists within the cybercrime ecosystem.

Over time, ransomware extortion techniques improved to incorporate a variety of tactics to compel victims to pay the ransom. Double Extortion Ransomware not only encrypts data but simultaneously exfiltrates it, threatening to release it publicly if their demands are not met, significantly amplifying the potential for reputational damage and regulatory consequences. This dual-threat approach compounds the pressure on victims, making it a powerful weapon in a cybercriminal's arsenal.[3]

The rise of mobile ransomware underlines the adaptability of cybercriminals to the changing digital environment. As mobile devices become ubiquitous and central to both personal and professional activities, they present a lucrative target for attackers. In this way, mobile ransomware takes advantage of the personal and often less secure nature of smartphones and

tablets and the sensitive personal data stored on them. Since the data at danger is personal, the exploitation of these devices puts ransomware directly in the pockets of individuals, who may be more willing to pay ransoms promptly.

Each evolution of ransomware demonstrates the increasing sophistication of these attacks and the critical importance of robust cybersecurity measures, both for individual users and organizations. As such, we found this topic warranted further discussion, which we will address in depth in this report.

This report begins with an overview of ransomware, delineating its varied forms and the mechanisms of attack, to acquaint the reader with the nuances of these cyber threats and their tangible consequences. Subsequent to this foundation, Section 2 explores the historical trajectory of ransomware, chronicling its evolution and the crucial moments in its ascent. Section 3 scrutinizes prevalent vulnerabilities such as phishing and *RDP* compromises, while also shedding light on strategies for fortification against such incursions. This research culminates in Section 4, which encapsulates our findings and imparts concluding reflections.

II. Historic Context

A. Early Stages

The AIDS Trojan, also known as PC Cyborg, is the first known instance of a ransomware attack dating back to 1989. [19] During the World Health Organization (*WHO*) conference in Stockholm, a biologist called Joseph Popp distributed 20,000 floppy disks that contained a Trojan virus that installed itself on the Microsoft Disk Operating System (MS-DOS). After the computer booted up 90 times, it hid all directories and encrypted filenames, only showing an image demanding payment from the victims in order to regain access to their machines. [19]

B. The Advent of Cryptovirology

As technology evolved, ransomware attacks did too. Through time, these attacks kept up with the evolution of cryptography, since encryption was its basis. In 1989, the Trojan was simple to remove using online decryption tools. Although this malicious software resurfaced in 2005, it used asymmetric encryption. [20] GPcode was released in 2006 and is one of the early examples that evolved over time. Some variants started by using symmetric encryption, and then, in 2010, some new versions were discovered using RSA-1024 and AES-256 encryption.

C. The Rise of Police Trojans

In the early 2010s, cyber criminals impersonated law enforcement to intimidate victims and demand payment in order to avoid prosecution, as seen with WinLock and Reventon. [20] For instance, WinLock was used to lock the victim's computer and display pornography until they paid a small ransom. On the other hand, Reventon posed as law enforcement and scared users by implying that they had been watching illegal pornography, and in order to avoid prosecution, victims paid compensation.

D. The Era of Crypto-Ransomware

With the rise of bitcoin, attackers started taking advantage of this easy and untraceable method to extort victims, making ransomware a profitable business. CryptoLocker took full advantage of the bitcoin exchange but combined phishing and more advanced forms of encryption, such as RSA-2048. The success of CryptoLocker led to a surge of new variants and some successors, such as CryptoWall, that, by 2018, had generated US$325 million in damage. [20]

E. The Peak of Ransomware as a Service (RaaS)

As ransomware variants grew more prevalent, they started being offered as a service *(RaaS)*. Ransomware as a Service consists of a partnership where both parties share profits, between the developer of the malicious code and hackers who find vulnerabilities in the systems. [2] Locky and Cerber were two of the most successful *RaaS* variants.

F. Big Game Hunting and Targeted Ransomware

Most recently, a new concept in ransomware was introduced, titled "Big Game Hunting" *(BGH)*. Attackers stopped focusing on the "spray and pay" [21] style of attacks and started focusing on big game hunting. Instead of focusing on small targets, as was the norm, the focus shifted to larger organizations, granting the chance of a bigger payout while having a reduced number of victims. As data plays a crucial role in the operation of an organization, besides encrypting its documents, attackers threatened to release sensitive information to the public in case the companies refused to pay the ransom, introducing double extortion tactics, as seen in Maze. [22]

G. The Sophistication of Double Extortion and Beyond

Following this, Maze leaked 700MB of data belonging to Allied Universal after missing the deadline for a payment, showing that they have access to the data and are not afraid to release it. [23] This combination of ransomware and malware posed an even bigger threat to users, backing up data was not a solution anymore, and on the other hand, it increased the chances of the victim not paying the ransom, resulting in having their data leaked. [24]

H. Triple Extortion and Multiparty Ransomware Attacks

Triple Extortion is an extension of double extortion. [25] By stealing data from companies, attackers gain access to client or supplier information. Besides contacting companies for a ransom, they also got in touch with the costumers, demanding a payout so that their data would not get leaked. AvosLocker is one of the groups that pressured victims with *DDoS* attacks to create a more hostile situation and increase the ransom payout. [20]

I. Political and Ideologically Motivated Ransomware

Some Russian-based ransomware groups have been associated with attacks motivated by political objectives. For instance, some groups were known to attack before the elections took place in various democracies. [26] In the same way, various companies were prone to experiencing ransomware attacks or retaliation for removing or canceling operations in Russia due to Russia invading Ukraine. [27]

J. Ransomware: Evolving Threats and Future Trends

The global pandemic of COVID-19 created an upsurge in ransomware invasions across various industries. Since organizations had to transition to remote working, the number of ransomware attacks escalated 148% in March compared to February 2019. [28] The third quarter of 2023 is the most successful quarter in the ransomware industry. So, it is crucial for organizations to maintain vigilance and establish strong cybersecurity protocols in order to protect against this ever-present threat.

Therefore, ransomware accompanied the latest technological evolution, and it is expected that it will keep up with all the future innovations that are still being explored and developed, such as AI, and grow with them.

III. Common Vulnerabilities

A. Phishing Vulnerability

This well known and straightforward attack is one of the most common ways to spread ransomware software. It relies on deceiving the victim with a convincing email or pop-up impersonating a reputable business or alerting for a fake emergency, for example. When clicked by the user, the ransomware is downloaded into the victims machine, compromising it.

1) Countermeasures Against Phishing: Despite the fact that human error plays a significant role in the success of phishing attacks, there are several preventative measures that can effectively mitigate such security issues by proactively identifying potential phishing threats.

a) ***Blacklist and Whitelist approach****:* By classifying emails or websites as malicious or not, based on the information that is not part of these, such as the domain name or URL, we can arrange blacklists to block or stop access to misleading links and whitelists (for example to restrict a system from accessing any domain other than the one in the whitelist). The primary drawback of this strategy is that it does not identify every phishing website because it is quite simple for an attacker to register on an other domain if their prior one was reported. [10]

b) ***Data Mining, Deep Learning and Machine Learning based approach****:* Another method to distinguish these malicious links or websites is from a machine learning point of view. By analysing various HTML, URL and other page features (such as CSS for example) and noticing their patterns, strong classification models were created. [9] Anti-phishing tools were developed based on these models so they can filter these malicious emails or websites and even detect new ones. [10] These can be used to update the blacklist or whitelist above as well.

c) ***Authentication Reinforcement approach****:* Even when a victim's credentials are compromised, with a more robust authentication system, an attacker can be stopped from accessing a protected resource. A commonly used type is multi-factor authentication, which requires not only the username and password but another form of identity. Normally a combination of something you know, something you are, and something you have. [10]

Along other methods, a prevention tactic that could minimize the dissemination of this attack is the implementation of an enhanced email filtering system that utilizes the machine learning techniques previously described. Although these solutions offer strong defenses and proactive steps to ward off phishing attacks, no amount of preparation can entirely avert all of these. [10]

2) Impact and Consequences of the WannaCry Ransomware Outbreak: As previously mentioned, the famous attack that relied in phishing emails as its initial infection technique was the 2017 WannaCry attack. It spread through computers all across the globe, being one of the most destructive ransomware attacks in history. This particular strain of malware capitalized on a breach in Microsoft's implementation of the Server Message Block *(SMB)* protocol, known as "EternalBlue," allowing it to proliferate swiftly across the network of the affected party and self-propagate to each connected machine. [12]

One of the most acutely impacted sectors was healthcare, with the National Health Service (*NHS*) in the United Kingdom standing as a stark example of the vulnerability inherent in modern digital infrastructures. The *NHS* endured extensive operational interruptions as the ransomware encrypted data on computers across the service, rendering critical systems and medical equipment inoperable. Consequently, there was a marked cancellation of appointments and a delay in routine services, as detailed by BBC News. [4] In many places, the *NHS* was compelled to turn away non-critical crises and resort to manual processes such as pen and paper.

Beyond the confines of healthcare, the ramifications of the WannaCry ransomware manifested across a diverse array of industries. Major international corporations such as Renault and Nissan in the automotive industry, and FedEx's subsidiary *TNT* Express in logistics, experienced substantial operational challenges. As a result, production and assembly lines were halted in several of Renault's factories in France and Nissan's manufacturing in the Uk. [5] In like manner, FedEx experienced serious economic harm and service delays forthwith of the TNT Express system infection, underscoring the vulnerability of supply chains to cyberattacks. [6] Additionally, the telecommunications sector, represented by Spain's Telefónica, was among the early casualties, illustrating the indiscriminate reach of the ransomware. [7]

3) Comparative Analysis of the Global Impact: WannaCry vs NotPetya Cyberattack: In contrast, the NotPetya attack, which followed shortly after in June 2017, was initially perceived as a ransomware outbreak but was later identified

as a more malicious state-sponsored act of cyber warfare, primarily targeting Ukraine but quickly spreading globally. [11] NotPetya's design was much more destructive; it aimed not just to ransom but to wipe data, leading to permanent loss of data and significant disruption of operations. While industries similar to those affected by WannaCry — such as logistics, healthcare, and manufacturing — were impacted, NotPetya is often cited as being the more devastating of the two due to its intent to destroy rather than profit. Notably, shipping giant Maersk reported a complete halt of operations as a consequence of NotPetya, causing a ripple effect on global shipping and ports. Multinational companies like Merck & Co., Mondelez International, and others suffered hundreds of millions in damages, far exceeding the costs of WannaCry.[8]

4) Contrasting Cyber Catastrophes: Lessons from WannaCry and NotPetya: Ultimately, the juxtaposition of WannaCry and NotPetya reveals two pivotal cyber incidents with different motivations but similarly far-reaching implications, demonstrating the evolving landscape of cyber threats. They serve as a compelling narrative of the growing severity of cyberattacks and the expanding scope of their consequences, emphasising a pressing imperative for vigorous and dynamic cybersecurity measures. NotPetya, in particular, serves as a reminder of how cyberattacks can transcend economic disruption to act as instruments of geopolitical strategy, with the capacity to inflict systemic harm and inject chaos into the physical realms of society and commerce. [11]

B. Remote Desktop Protocol Vulnerabilities

Remote Desktop Protocol *(RDP)* is a Microsoft network communication protocol that allows communication with a Windows Server. It is widely used in working environments where staff needs to access its work desktop from home, for example. However this remote access protocol has its security flaws that can prove to be very damaging to users and corporations involved. Some of this include weak authentication (man-in-the-middle and password guessing attacks in this context are quite common) and default port exposure. With these two combined, an attacker can scan *IP*'s, intercept the default port if open, and deploy the desired ransomware. [13]

1) Countermeasures Against RDP Attacks: RDP attacks were especially on the rise during the COVID-19 pandemic, since so many people were working remotely from home and relied heavily on this connection. [14] As an illustration of how to lessen this issue, consider:

a) ***Strengthening credentials****:* Changing the username to something more unique and creating a more complex password to prevent brute force attacks is a simple but effective change.

b) ***Changing the default port****:* Another clear alternative is to switch the default port for *RDP* to an alternate port, diminishing the possibility of the attack.

c) ***Using Virtual Private Network (VPN)****:* Utilizing a *VPN* before accessing *RDP* can be highly beneficial, though it does require the upkeep of the *VPN* infrastructure and essentially transfers the responsibility of securing the entry point for users from *RDP* to the *VPN* itself. [16]

2) Real World Examples: A notable ransomware attack that specifically targeted *RDP* servers was the 2019 Nemty attack, which threatened to leak the victim's important files, including their credentials. This leak of *RDP* credentials would then feed other attacks, such as the Crysis ransomware attack that aimed at large organisations in New Zealand and Australia. [15]

The Maze attack, as mentioned in section 2, used a new extortion method that would leak the data if the victim refused to pay the ransom. One of its main ways of propagation was also through *RDP* brute force attacks making victims of an *IT* services firm, the Hammersmith Medicine Research during the COVID-19 pandemic and many others. [17,18]

As shown above, the mutuality in these ransomware attacks lies in the exploitation of *RDP* connections, leading to comparable preventative strategies such as strengthening the complexity of credentials, safeguarding the default *RDP* port by restricting access from unknown public *IP*s, allowing connections solely from verified *IP*s, closing off any unused ports, and enhancing security with an additional layer of encryption through a *VPN*.

IV. CONCLUSION

The relentless evolution of ransomware, as evidenced by the devastating impacts of WannaCry and NotPetya, highlight the extreme importance of cybersecurity as a critical component of global security and economic stability. From the exploitation of *RDP* vulnerabilities to the commoditization of ransomware through *RaaS* models, the sophistication of these cyberattacks reveal that cybercriminals are always innovating and adapting.

This article has emphasised the importance of understanding ransomware's historical context, the mechanisms by which it exploits technological and human vulnerabilities, and the profound consequences of its attacks. The shift towards more targeted and destructive campaigns, such as those seen in "Big Game Hunting," and the emergence of double and triple extortion techniques, demonstrate the increasing audacity and strategic planning of threat actors.

As we navigate an increasingly interconnected world, the imperative for robust, proactive, and adaptive cybersecurity defenses has never been more pronounced. Organizations and individuals alike must prioritize the implementation of comprehensive security protocols, and foster collaboration across sectors to mitigate the risks posed by these cyber threats.

In conclusion, the cybersecurity community must remain vigilant and innovative, anticipating the next iteration of ransomware tactics and preparing for the inevitable convergence of cyber threats with emerging technologies such as artificial intelligence and quantum computing. The battle against ransomware is not just about protecting data; it is about safeguarding our societal, economic, and political pillars against the insidious reach of cyber warfare.

REFERENCES

[1] N. K. Verma and A. K. Ghosh, *Computational intelligence: Theories, applications and future directions* - volume II ICCI-2017, Singapore: Springer Singapore, 2019, pp. 65–80.

[2] K. Baker.(2023, January 30) *What is ransomware as a service (raas)? - crowdstrike* [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

[3] S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Ransomware, Threat and Detection Techniques: A Review", School of Computer and Information Technology, Taylor's Univ., Malasya, Rep. 2, 2019.

[4] BBC News. (2017)*NHS cyber-attack: GPs and hospitals hit by ransomware* [Online]. Available: https://www.bbc.com/news/health-39899646

[5] G. Cohen, "Throwback attack: Wannacry ransomware takes Renault-Nissan Plants Offline," Industrial Cybersecurity Pulse, https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-wannacry-ransomware-takes-renault-nissan-plants-offline/ (accessed 2023).

[6] Reuters Staff. "Fedex says Cyber Attack to hurt full-year results," Reuters, https://www.reuters.com/article/us-cyber-attack-fedex-idUSKBN1A21D7 (accessed Nov. 5, 2023).

[7] J. C. Wong and O. Solon, "Massive ransomware cyber-attack hits nearly 100 countries around the world," The Guardian, https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs (accessed 2023).

[8] M. Heller, "Notpetya ransomware impact costs Maersk Hundreds of Millions: TechTarget," Security, https://www.techtarget.com/searchsecurity/news/450424681/NotPetya-ransomware-impact-costs-Maersk-hundreds-of-millions (accessed 2023).

[9] A. Sadiq et al, "A review of phishing attacks and counter-measures for internet of things-based smart business applications in industry 4.0", Dep. Computer Science, NFC Institute of Engineering and Fertilizer Research, Pakistan, 2021. Available: https://onlinelibrary.wiley.com/doi/epdf/10.1002/hbe2.301

[10] Z. Alkhalil, C. Hewage, L. Nawaf, I. Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy", Cardiff School of Technologies, Cardiff Metropolitan University, United Kingdom, 2021. Available: https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

[11] S.Y.A. Fayi, "What Petya/NotPetya Ransomware Is and What Its Remidiations Are", in Latifi, S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham. Available: https://doi.org/10.1007/978-3-319-77028-4_15

[12] S. Algarni, "Cybersecurity Attacks: Analysis of "WannaCry" Attack and Proposing Methods for Reducing or Preventing Such Attacks in Future", in Tuba, M., Akashe, S., Joshi, A. (eds) ICT Systems and Sustainability. Advances in Intelligent Systems and Computing, vol 1270. Springer, Singapore. Available: https://link.springer.com/chapter/10.1007/978-981-15-8289-9_73

[13] C. Longzheng, Y. Shengsheng, Z. Jing-li, "Research and implementation of remote desktop protocol service over SSL VPN," IEEE International Conference onServices Computing, 2004. (SCC 2004). Proceedings. 2004, Shanghai, China, 2004, pp. 502-505, Available: https://ieeexplore.ieee.org/abstract/document/1358052

[14] Splashtop Team. "The Role of VPN and RDP in Ransomware Attacks," Splashtop, https://www.splashtop.com/blog/role-of-vpn-rdp-in-ransomware-attacks (accessed 2023).

[15] S. Jimada, T.D.L. Nguyen, J. Sanda, S.K. Vududala (2021). Analysis of Ransomware, Methodologies Used by Attackers and Mitigation Techniques. In: R. Kumar, N.H. Quang, V. Kumar Solanki, M. Cardona, P.K. Pattnaik, Research in Intelligent and Computing in Engineering. Advances in Intelligent Systems and Computing, vol 1254. Springer, Singapore. Available: https://link.springer.com/chapter/10.1007/978-981-15-7527-3_37

[16] P. Arntz, "How to protect RDP," Malwarebytes, https://www.malwarebytes.com/blog/news/2022/03/protect-rdp-access-ransomware-attacks (accessed 2023).

[17] P. Arntz, "Maze: The Ransomware that introduced an extra twist: Malwarebytes labs," Malwarebytes, https://www.malwarebytes.com/blog/news/2020/05/maze-the-ransomware-that-introduced-an-extra-twist (accessed 2023).

[18] C. Dinu, "Maze ransomware: Origins, operating mode, attacks," Heimdal Security Blog, https://heimdalsecurity.com/blog/maze-ransomware-101/ (accessed 2023).

[19] J. Dossett, "A timeline of the biggest ransomware attacks," CNET, https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/ (accessed 2023).

[20] V. Drake, "The history and evolution of ransomware attacks," Flashpoint, https://flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/ (accessed 2023).

[21] "A brief history of ransomware [including attacks] - CrowdStrike," crowdstrike.com, https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/ (accessed 2023).

[22] "Allied universal breach by Maze Ransomware," Binary Defense, https://www.binarydefense.com/resources/threat-watch/allied-universal-breach-by-maze-ransomware/ (accessed 2023).

[23] "Triple extortion ransomware: The DDoS flavour," Packetlabs, https://www.packetlabs.net/posts/triple-extortion-ransomware/ (accessed 2023).

[24] The CrowdStrike Intel Team, "Ransomware + data leak extortion: Origins and adversaries, pt. 1," crowdstrike.com, https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/ (accessed 2023).

[25] K. Nershi, S. Grossman (2022). "Assessing the Political Motivations Behind Ransomware Attacks", Stanford Internet Observatory. Available: https://bahamasamlconference.centralbankbahamas.com/assets/images/pdf/conferences/2023/nershi-grossman_ransomware.pdf

[26] V. P. Nangineni and S. Winterfeld, "Defeating Triple Extortion Ransomware: The Potent Combo of Ransomware and DDoS Attacks," Akamai, https://www.akamai.com/blog/security/defeating-triple-extortion-ransomware (accessed 2023).

[27] K. Nershi and S. Grossman, "New paper: Assessing political motivations behind Ransomware attacks," FSI, https://cyber.fsi.stanford.edu/io/news/new-paper-assessing-political-motivations-behind-ransomware-attacks (accessed 2023).

[28] J. L. Hardcastle, "Ransomware Attacks Spike 148% Amid COVID-19 Scams", sdxcentral, https://www.sdxcentral.com/articles/news/ransomware-attacks-spike-148-amid-covid-19-scams/2020/04/ (accessed 2023).