The Changing Nature of Ransomware

Blair Andrews

University of New South Wales

***Abstract* – Ransomware is one of the most rapidly evolving and challenging forms of malware on the internet – and with emerging trends, we can see that it is becoming more than just a simple malware. The aim of this report is to analyse the impact of ransomware, as well as how rapidly its impact is increasing among not only businesses – but governments and leading essential industries. Ransomware itself is becoming more than just a malware, but a lucrative business scheme for cybercriminals to take advantage of. With the resurgence of remote work from the COVID-19 pandemic, we can find that businesses are now more vulnerable than ever, and the attack surface for ransomware further increases – along with legal and ethical ramifications for both attacker *and* victim(s). This report found that the evolutionary nature of ransomware parallels emerging modern technology such as artificial intelligence and cloud storage – and that ransomware has the potential to evolve past the capabilities of common mitigative technologies.**

I. Introduction

Ransomware is rapidly evolving and utilising emerging technologies and societal changes to strengthen its impact against unknowing victims. The importance of analysing the changing nature of ransomware lies in the dramatic increase of impact that ransomware has had on businesses in the past decade. With the resurgence of remote work due to the COVID-19 pandemic, businesses are left with much more vulnerable systems – as post-pandemic we saw an increase of 13% of worldwide ransomware attacks (Lai, 2024). With this resurgence, we also are beginning to see an emergence of ransomware-as-a-service (RaaS) – a lucrative business model aiming to monetise and allow programmers and criminals to collaborate (Keijzer, 2020). Ransomware is evolving at a rapid rate, as new technologies and encryption techniques surface in the modern world – and the attack surface increases as more 'smart' devices are becoming household commodities. We must analyse the beginnings of ransomware to have a full understanding of just how much ransomware has evolved – and how much it will continue to evolve, and what issues that will arise from that.

II. A Background of Ransomware

Ransomware is a type of malicious software that when installed on a system, it takes the system's files, or the system itself hostage, and demands a payment to be made (usually via Bitcoin) to restore the system back to its previous state (O'Gorman & McDonald, 2012). It is imperative to understand that there are two key types of ransomware – **locker ransomware** and **crypto ransomware**. Locker ransomware denotes malicious software that locks a user out of their system and demands a payment to obtain access back to their system (Richardson & North, 2017). Crypto ransomware is typically the most common of the two and denotes malicious software that encrypts user files and demands payment to obtain a decryption key to gain access back to the files (Richardson & North, 2017).

Ransomware was first conceptualised in 1989, the AIDS Trojan, was distributed via floppy disk and

encrypted user filesystems – the first known example of crypto ransomware (Richardson & North, 2017). As technology rapidly progressed, so did the capabilities of malicious software. Approaching the late 2000s, modern ransomware began utilising more sophisticated forms of encryption, and being able to lock entire systems – with anonymous online payment methods not yet being introduced, ransomware was still in its early developments (Baker, A Brief History of Ransomware [Including Attacks], 2022). With the emergence of Bitcoin and other cryptocurrencies in 2009, ransomware became a lucrative business opportunity for attackers as these cryptocurrencies presented a method to transfer illicit funds with full anonymity (O'Kane, Sezer, & Carlin, 2018).

As time further progressed, encryption methods became more complex, attack methods got more sophisticated, and ransomware has become a business model for criminals to take advantage of in the ever-changing cyber landscape. This, in turn, brings us to the present day, where ransomware is one of the most dangerous and complex cyber-attacks in the world, with unimaginable consequences for a business if targeted (Kumar, 2023).

III. Current Trends

A. Social Engineering the Pandemic

The emergence of COVID-19 made remote work now a pillar of modern workplace requirements and has brought foreseen security complications in its wake. Worldwide, over 2020-2021, ransomware attacks saw a dramatic increase of 13%, which was a larger increase than the past 5 years combined (Lai, 2024). With more individuals working from home, it is much more likely that these individuals would not have adequate security measures – compared to what they would have on-site. This makes these individuals a prime target for any threat actor looking to execute ransomware, and possibly elevate beyond further into the business.

As work-from-home individuals communicate through the internet, this makes them ultimately vulnerable to social engineering attacks – as the challenge increases to educate individuals on identifying genuine websites, contacts, among others (An Duong, Bello, & Maurushat, 2022). During the pandemic, a ransomware attack on the NHS in the United Kingdom targeted patient data, as well as financial data, and brought down emergency services briefly (Milmo, 2022). With healthcare services having a 60% attack rate for ransomware (Swagler, 2023), it is vital to understand that ransomware does not just affect smaller businesses, but industries as important as healthcare.

As the attack surface for ransomware increases with more remote workers in businesses becoming the standard, security policies must be implemented and governed within such businesses. Prior to the COVID-19 pandemic, remote work was typically uncommon. In the United States Census, 7.3% of employees stated they worked from home prior to 2020, in 2021 however, that number rose to 17.9% (Silver, 2023). This dramatic increase in remote workers further increased the attack surface for businesses – making it more difficult to compete with opportunistic cybercriminals. This further emphasises the point of proper security implementations, and further governance to ensure the risks leading to ransomware are mitigated – typically social engineering. By fooling an unknowing employee into downloading malicious files, an attacker can gain uninterrupted remote access to a system, and potentially elevate their privileges to an administrative position through faulty access control, misconfigured networks, and other vulnerabilities. This allows an attacker to easily disable and potentially encrypt important files and information that could have serious consequences on the business' reputation and finances, and more importantly, user information.

The biggest challenge with ransomware as noted, is the lack of knowingness and understanding among users – which is why security policy implementation and governance must be a priority in businesses switching to remote work. However, there are also other challenges to face, such that there is a clear lack and need of open-source ransomware libraries (Beaman, Barkworth, Akande, Hakak, & Khan, 2021). Similar to existing libraries that enable research and development on zero-day vulnerabilities, a library containing ransomware with origin information would

be crucial to researchers and would be vital to mitigative strategies for ransomware.

The danger of ransomware has been substantiated, especially in current trends following the COVID-19 pandemic – and we have found that ransomware is becoming a generic business model for cybercriminals; and something that is easily attainable for a criminal entrepreneur.

B. Ransomware-as-a-Service

With the emergence of untraceable anonymity online, ransomware has become a lucrative business opportunity for cybercriminals looking to make easy money. Ransomware-as-a-service (RaaS) models allow attackers with little programming abilities to communicate and purchase services from skilled ransomware developers (O'Kane, Sezer, & Carlin, 2018). By allowing cybercriminals to work with skilled developers, you have the collusion of two parties that are missing key skills to launch a ransomware attack – thereby emphasising the dangers of RaaS. In 2021, a survey of 5,600 IT professionals detailed that 66% had suffered a ransomware attack, with that number having grown from 37% in the previous year (Sophos, 2022). This considerable increase indicates that threat actors are becoming much more capable in launching a ransomware attack – further indicating the mass production and utilisation of RaaS.

Within a typical RaaS, there are four revenue models – flat fee monthly subscription, affiliate programs, one time license fee, and pure profit sharing (Baker, What is Ransomware as a Service (RaaS)?, 2023). RaaS has become so sophisticated in fact, that some providers are offering user-friendly portals to view the progress of their ransomware attack (Keijzer, 2020), highlighting the ease of accessibility of launching a ransomware attack regardless of your computer literacy level. As noted, more workers than ever are working from home, and at the same time, there are more IoT (Internet of Things) devices in every home. With more devices connected to the internet, the attack surface for cybercriminals increases – which has ultimately led to RaaS, as more criminals are understanding this as time progresses and are looking for accessible sources of illicit income.

Over the course of 2020-2021, average ransom demands increased from $170,000 to $812,360 (based on 282 surveyed businesses), with fifteen of those businesses reporting ransom demands of over $1,000,000 (Sophos, 2022). Along with that, the common ransomware attack ten years ago typically had lower demands like $100 for decryption access – which that has now increased dramatically to figures 500x and greater (Trend Micro, 2023). We can understand from these figures that there has been a dramatic increase in demands from ransomware attacks – indicating the increase in capabilities from attackers, being confident enough to increase their demands by such an upward trajectory. DarkSide is an RaaS operation that focuses on finding vulnerabilities in unpatched VMware operating systems, and in May of 2021 the service was linked with the ransomware attack of Colonial Pipeline – an American oil infrastructure company, which paid $5,000,000 to retrieve over 100 gigabytes of encrypted company data (Sood, Hurley, & Arsene, 2021). Ransomware moving from a simple locking malware to a multi-million-dollar industry in a little under a decade is a cause for extreme concern for the rapidly changing nature of ransomware. As the outreach of cyberspace changes – so does the importance of user privacy, and through ransomware it is being exploited in rapidly advancing emerging concepts.

C. Double Extortion Ransomware, to Pay or Not to Pay

The legal ramifications are not typically considered when handling a ransomware attack, and when a business is extorted, they believe they have no other option. Double extortion ransomware is an emerging layered ransomware attack that involves the typical encryption of data – but includes another layer where the business is threatened with publication of confidential documents (Sukianto, 2023). Through this method, the attacker has further leverage and can possibly demand further payments. However, it is important to note that in some countries, it is illegal to pay a ransom and conduct “business” with an illicit trader. For instance, in the United States, it isn’t

outright illegal to pay a ransom – however – it *is* illegal to conduct "business" with an individual or organisation on a sanctioned list, which may include hackers, hacker groups, or governments known to be affiliated with hackers (Huffman, Lowell, Bartnick, & Nowicki, 2018), with penalties of up to 20 years in prison, or a $1,000,000 fine (Cahill, 2023).

This outrightly makes handling ransomware much more complex, as there is no guarantee that the attackers will restore your data if you pay them, and you may be imprisoned. At the same time, especially with the emergence of double extortion ransomware, businesses must be aware of notifying proper authorities of data breaches – as it is illegal to not declare a data breach in most countries. Typical passive mitigative measures in businesses are becoming not enough to deal with modern ransomware (Payne & Mienie, 2021), and the capabilities of attackers are proving to increase year-after-year, as the rate of ransomware attacks are becoming increasingly more prevalent, and increasingly more expensive. As it evolves, ransomware is beginning to interact with more legal and ethical issues and is becoming a more central focus in cyber security because of the potential ramifications of simply being a victim – *you* could be the one imprisoned in an attack on *you*.

IV. Future Prospects

The future of ransomware can cast a concerning and poisonous perspective on the developing technologies of the modern world. Many modern businesses are switching to a cloud environment, typically to store their data. Ransomware development could potentially see a cloud-based variant of ransomware – possibly targeting cloud administrator accounts or locking use of cloud databases entirely (Hacquebord, Hilt, & Sancho, 2022). As well as that, as more IoT devices join networks (both at home and in the workplace), further security measures would be needed to properly protect devices from being intruded – in the future, ransomware will take advantage of home devices, and seeing the increase in remote work, this is a huge vulnerability. Ransomware has already begun being used through home devices such as smart thermostats (Fitzpatrick & Griffin, 2016), which further indicates possible routes of attack. Not only would these home devices be used as routes, but potentially as victims – smart watch ransomware, smart car ransomware, smart television ransomware (Richardson & North, 2017), the list goes on of potential devices that could be attacked.

The current development and evolution of AI tools is becoming increasingly concerning for the development of ransomware – specifically social engineering. Recently, individuals around the world have been receiving phone calls from family members in distress but have been fooled by an AI algorithm designed to imitate voices based off short voice clips (Ovide, 2023). This, paired with the rapidly evolving nature of artificial intelligence, is a great cause of concern for the future of social engineering. Using AI tools, it would be possible to mass-produce believable scam emails, texts, calls, among other forms of communication. Social engineering is the first stage of a ransomware attack, and with the help of AI, ransomware could become rampant – and businesses would *need* to focus on making sure their employees are educated and understand the difference between genuine and ingenuine communications. Not only would AI be used for social engineering, but also to potentially produce modular ransomware, further contributing to the ransomware-as-a-service model. AI tools are becoming increasingly expansive, so much so that there are several potential dangers for the future of cybersecurity, and the power of AI needs to be harnessed to ensure that it does not fall into the wrong hands.

As time progresses, ransomware developers will become more opportunistic and focus more on zero-day exploitation to gain a larger attack surface – producing malware more efficiently to bypass standard mitigative software (Zugec, 2024). By weaponizing new vulnerabilities, attackers will be able to gain access to systems more frequently and implant ransomware much more efficiently. Along with that, ransomware developers are also beginning to take advantage of new and emerging encryption technologies, such as quantum-resilient encryption (Zugec, 2024). Ransomware developers leaning toward more secure

programming techniques, as well as effective encryption technologies would mean more dominance over their victims – and less chance for remediation without paying the ransom.

V. Conclusion

Ransomware has evolved from a simple locker malware to one of the most, if not *the most* dangerous and concerning cyber-attacks in the world. It has evolved from an individual seeking small amounts of petty cash – to a lucrative business model raking in $2.59 billion annually in Australia alone (Urquhart, 2021). The study of the changing nature of ransomware is a necessity, as technology develops and evolves, so will the capabilities of attackers. Especially as ransomware-as-a-service develops further, the number of potential attackers will highly increase – and so will payment demand. Not only will ransomware fall further into illicit business models, but emerging strategies dictate the cunning methods of monetisation that attackers will use further in the future – such as multi-layer extortion ransomware. Ransomware becoming further monetised and increasingly popular with criminals around the world means more impact and alignment with legal and ethical issues in governments, and soon the focus must shift to protect victims in such attacks.

Ransomware is one of the fastest evolving forms of cyber attack in the current era, and businesses – and individuals – must look to protect themselves at all costs: first by combatting social engineering and educating and understanding phishing techniques. From there, focus needs to be shifted to mitigative technologies – antivirus, firewalls, cyber hygiene. Ransomware, like any malware, is only effective against the unprepared. As it evolves rapidly, we must combat it by understanding what new weaknesses it may target – and implement and govern.

VI. Future Research

Future work in the evolution of ransomware must analyse current and previous studies, and by analysing new forms of ransomware, mitigative techniques will improve. Focus must be shifted to the analysis of emerging technologies that may be used in ransomware, and the prevention of allowing them to be used.

VII. References

An Duong, A., Bello, A., & Maurushat, A. (2022). Chapter 3 - Working from home users at risk of COVID-19 ransomware attacks. In *Cybersecurity and Cognitive Science* (pp. 51-87). Academic Press.

Baker, K. (2022, October 10). *A Brief History of Ransomware [Including Attacks]*. Retrieved from CrowdStrike: https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/

Baker, K. (2023, January 30). *What is Ransomware as a Service (RaaS)?* Retrieved from CrowdStrike: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*.

Cahill, J. (2023). *Pay The Ransom, Risk Jail Time?* Retrieved from INFIMA Sec: https://infimasec.com/blog/pay-your-ransom-go-straight-to-jail

Fitzpatrick, D., & Griffin, D. (2016, August 27). *Cyber-extortion losses skyrocket, says FBI*. Retrieved from CNN: http://money.cnn.com/2016/04/15/technology/ransomwarecyber-security

Hacquebord, F., Hilt, S., & Sancho, D. (2022). *The Near and Far Future of Ransomware Business Models.* Trend Micro Research.

Huffman, B. W., Lowell, M. J., Bartnick, W. J., & Nowicki, J. K. (2018). *Is Paying a Ransom to Stop a Ransomware Attack Illegal?* Reed Smith.

Keijzer, N. (2020). *The new generation of ransomware - An in depth study of Ransomware-as-a-Service*. Twente: University of Twente.

Kumar, D. I. (2023). Emerging Threats in Cybersecurity: A Review Article. *International Journal of Applied and Natural Sciences*, 1-8.

Lai, B. (2024). *The threat of ransomware - Parliament of Australia*. Retrieved from Parliament of Australia: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook47p/ThreatRansomware

Milmo, D. (2022, August 11). *NHS ransomware attack: what happened and how bad is it? | Guardian Australia*. Retrieved from The Guardian: https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it

O'Gorman, G., & McDonald, G. (2012). *Ransomware: A Growing Menace.* California: Symantec.

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *Special Issue: Privacy, Data Assurance, Security Solutions for Internet of Things (PASS4IoT)*, 321-327.

Ovide, S. (2023, October 17). *Should you have a family 'safe word' against AI voice-spoofing scams?* Retrieved from The Washington Post: https://www.washingtonpost.com/technology/2023/10/17/should-you-have-family-safe-word-against-ai-voice-spoofing-scams/

Payne, B., & Mienie, E. (2021). Multiple-Extortion Ransomware: The Case for Active Cyber Threat Intelligence . In D. T. Eze, D. L. Speakman, & D. C. Onwubiko, *ECCWS 2021 20th European Conference on Cyber Warfare and Security* (pp. 331-336). Chester: University of Chester.

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, 10-21.

Silver, H. (2023). Working from Home: Before and After the Pandemic. *SAGE - PMC COVID-19 Collection*, 66-70.

Sood, K., Hurley, S., & Arsene, A.-L. (2021, May 18). *Darkside Ransomware: Falcon Protects Customers*. Retrieved from CrowdStrike: https://www.crowdstrike.com/blog/falcon-protects-from-darkside-ransomware/

Sophos. (2022). *The State of Ransomware 2022*. England: Sophos.

Sukianto, A. (2023, November 15). *What is Double Extortion Ransomware? And How to Avoid It*. Retrieved from UpGuard: https://www.upguard.com/blog/double-extortion-ransomware

Swagler, C. (2023, December 9). *Top 13 Ransomware Targets of 2023*. Retrieved from Speartip: https://www.speartip.com/top-13-ransomware-targets-in-2023

Trend Micro. (2023, February 21). *A Deep Dive into the Evolution of Ransomware Part 1*. Retrieved from Trend Micro: https://www.trendmicro.com/en_za/research/23/b/ransomware-evolution-part-1

Urquhart, A. (2021, August 12). Ransomware Payment Bills 2021. *Senate Hansard*. Tasmania: Parliament of Australia.

Zugec, M. (2024, January 3). *2024 Cybersecurity Forecast: Ransomware's New Tactics and Targets*. Retrieved from Bitdefender: https://www.bitdefender.com.au/blog/businessinsights/2024-cybersecurity-forecast-ransomwares-new-tactics-and-targets/