Ransomware Threat

Simon Lowry
CISO, Cybersecurity
HealthTechCompanyLtd
Dublin, Ireland
x21168938@student.ncirl.i
e

***Abstract*— this is a report for the board of directors of HealthTechCompanyLtd related to the Ransomware Threat presented by the CISO. It covers details about the impact of the Ransomware threat, a description of the threat, high profile incidents related to the threat, some lessons for our organization based on that, and then more considerations based on our organization and finally, methods of detection and prevention.**

I. Introduction

Cybercrime is becoming increasingly regular, having greater impact, and in some cases rising it's level of sophistication. One of the most virulent forms of threats businesses, organizations and nations face is ransomware. Every 11 seconds another ransomware attack is said to have occured. In 2021 analysis of ransomware by FinCEN showed that $590 million was paid in ransomware transactions in the US alone exceeding the amount that was paid in ransomware transactions the previous year. [1] For 2022, the total loss expected to come from ransomware is projected to reach $20 billion worldwide. The fallout from dealing with ransomware is prolonged, complex and costly to both revenue and many other aspects of running a business. Some of the latest research shows that companies are effected on the bottom line as well as loss of customer trust, reputational damage, having to lay off various employees and in some cases, the shutting down of businesses of small and medium sized businesses shutting down completely. [2]

The average downtime is 13 days and the average ransom demanded was $170000 according to a report done by Group IB. [3] For some though as this report will outline the impact can go on for months as they look to recover and protect their systems from further attacks. It can systematically cripple many organisations' ability to operate. Ransomware is not some flash in the pan form of malware it's been around since it's 1989 and it's variants and it's effects are still growing more and more pronounced

II. Description of Ransomware Threat

Ransomware is a type of malware that encrypts your computer and makes a demand of a fee to be paid with the alleged promise of having the device unencrypted by the attackers after doing so. It stops the user from being able to use their device regardless of the type of device whether it be a laptop or tablet, IOT device. It's a form of digital extortion that threatens to either delete the users data or release sensitive information online in what's known as a double extortion. [4]

Currently many are distracted by the covid pandemic and working from their own home networks and with this some security researchers believe that the risks are even greater with a hugely broader attack surface with each user on their own individual home networks some of which may not be nearly as well protected as the corporate network. Even with the use of VPNs, when an attacker has infiltrated a user's device at home, all they needs to do is wait until that user goes into their VPN session before looking to perform their nefarious activities and now they have access to whatever that user has access to and could look to move laterally in the network and potentially detonate ransomware and other malware on a whole host of devices. [5]

Not only are these attacks extremely disruptive and destructive for businesses and organizations, but nowadays they can also be implemented and executed by people with little understanding of how to actually make this kind of malware or how it fully operates. This can be done with through RaaS aka Ransomware as a Service. Individuals or organised crime can leverage ransomware attacks and hacking tools to gain high volume of return from their investment through the ransoms that are paid from infected machines that they have attacked. Such services are available from businesses like REvil and Darkside lowering the barrier for entry to so many more people being able to carry out these attacks easily. The payments for these ransoms are also carried out through bitcoin giving the attackers greater degree of anonymity when they look to attack our networks and any other networks across the globe. What this all highlights is that it's not if we will be attacked and infiltrated by malware. The actions we take and continue to take in prevention, detection and recovery and good training to the weakest link in cyber security which are our employees..

Next we'll look at some high profile attacks, analyze them and look to take some lessons from them.

III. High-Profile Ransomware Attacks

A. HSE Ireland Attack

On May 14th 2021, ransomware was activated in the HSE and cause a huge amount of complications in running and operating services and the accrued costs anticipated to be in the region of €100 million. The attackers had demanded almost €18 million in bitcoin for their ransom fee but the Irish Government decided and stuck to their guns of not paying the ransom. The initial infection had been a malicious attachment that came in through a phishing email opened on site at the HSE. [7]

This attack caused a tremendous and catastrophic impact with the HSE deciding to shut down all of their IT systems and shut down all of their networks crippling the nations healthcare system..This was in the midst of the pandemic when the resources of the HSE was already stretched and this put further strain on an already aching health system. The attackers may have believed that due to the pandemic already waging and no doubt being aware of the impact it was having on hospital that they would sucuumb to their demands but they were wrong.

I personally know some nurses who working in a hospital affected by this attack and it completely devastated their ways and means of performing their duties such was their dependence on these systems. They were forced to resort to using pens and paper and the operating of the hospital grinded to a halt in many ways with a host of appointments needing to be cancelled due to the pervasive impact of the attack. Diagnostic services were badly effected as well as laboratory systems and radiotherapy services preventing these treatments from taking place and the software being used to manage and keep track of patient data.

Another alarming thing here was that the attackers had actually penetrated the HSE network since 18th of March 2021 and continued to sustain their presence on the network and exfiltrating sensitive data and further propagating with lateral movement to other servers on the network. Gaining this sensitive information again could provide them with another means of leverage that they would hope to exploit the HSE and Irish Government. These movements were logged on some of the systems but were not detected for the duration of the time. Here we see the importance of proper infrastrucutre in place to detect this kind of operating and alerting that would be triggered and followed up by some cyber security analysts. Proper defenses need to be in place in the diferent parts of the cyber kill chain, there is no such thing as being immune to a breach. In fact, many breaches are only found 6 months to a year after the attacker has made their way onto the networks.

The HSE invoked its Critical Incident Process, which began a sequence of events leading to the decision to switch off all HSE IT systems and disconnect the National Healthcare Network ("NHN") from the internet, in order to attempt to contain and assess the impact of the cyber attack. These actions removed the threat actor's (the "Attacker") access to the HSE's environment.

The chain of occurrences brought about by this attack led to the HSE needing to call on it's Critical Incident Process and subsequently turning off all of their IT systems and completely stop the National Healthcare. This would be applied as a mitigation strategy in order to stop the threat actor from looking to continue to operate in the HSE network and potentially looking to escalate privileges, or move laterally throughout the network and infect even more systems and amplify the damage being caused. Staff as a result of this lost the ability to communicate through networked phones or email and operate on their systems. The attacker was looking to disrupt the availability of the systems and services of the HSE with this ransomware in order to both ideally obtain a ransom and otherwise gain access to the sensitive information which they could potentially threaten to release online. The data was encrypted by the ransomware and would only be decrypted in the event that the ransom was paid.

The scope and impact of the attack was that significant that the National Cyber Security Centre, An Garda Siochana and the army were involved in reaction to the compromise and aiming to regain normal operations.

Even with such a robust retrospective response with the various agencies involved, the HSE report mentioned that four months on from the attack there were still lingering impacts from in their recovery. This is despite the fact that they obtained the key to decrypt the data there was still a devastating and pervasive impact to operations for months after. It perfectly highlights that prevention, detection and avenues of recovery are absolutely pertinent to protect against these attacks in the first place. Even when you decide to pay or manage to decrypt the data, the legacy of it's impact rumbles on and the business or hospital in this case is left with a huge amount of long lasting. Investing in proper security controls that can stop these attacks

In Q1 of 2019 a risk assessment was undertaken on the HSE and based on that there was a 75% likelihood of an attack occuring with the impact of that very attack assigned to be of major impact. This risk assessment was brought to the attention of the board and it was not taken seriously. This is a lesson for all of us in our company. We ought to take the valuable insight from their lessons learned. Fail to prepare and prepare to fail. It's not if these attacks take place or compromise some of our systems, it's when. Proper strategy, resources, security controls and training must take place to protect our assets, our brand, revenue and customers and their trust in us. This attack highlighted how woefully unprepared the Irish health care system was to protect itself. There wasn't even core staff in place like a CISO to take responsibility for the security of their network and systems. They had a shortage of any real cyber staff, their staff hadn't been properly trained and prepared for these kinds of eventualities and the price was paid for this. The report highlighted that their cyber security capabilities needed a complete overhaul and this would be a multi-year process to get all of the pieces in place to make it more robustly capable of preventing attacks like this from happening or at least mitigating them and their impact to the best degree possible when they do. They would benefit from utilizing setting out policies, standards, guidelines, adopting frameworks like NIST to help to focus their procedures being implemented in some of the most effective routes of properly setting up a cyber security programme which would not only help against ransomware attacks but also protect the whole organization. [8]

B. Wannacry

In 2017, WannaCry Ransomware created a frenzy infecting more than 230,000 systems across the world and costing billions of dollars in it's carnage..[9]

It takes advantage of Windows vulnerability related to the Server Message Block Protocol which helps systems on a network communicate and could instead be filled into running code. When it infects the computers it encrypts the files on the computers and demangs a ransom in bitcoin. [10]

This was originally reputed to be an a zero day that the NSA had developed an exploit for called Eternal Blue which ended up being stoled by a hacking group called the Shadow Brokers who then released it online. This caused a lot of consternation when it was revealed with Microsoft criticisizing the NSA for not reporting the vulnerability to them. However, this is something the NSA is known to do, stockpiling zero days in what they would deem as the interest of the country. Microsoft did release a patch but the reality is a huge amount of systems and companies are not paying attention to these things and don't have a patching policy in place and as a result pay the price for that. [10]

The attackers usually requested $300 dollars worth of bitcoin and increased that ransome to $600 if they did not pay within three days and then they would threaten to delete the files if they didn't. The prevalence of WannaCry eventually caused havoc in over 150 countries and aronud 4 billion dollars. [11]

As a former cybersecurity analyst, I've seen first hand the impact of wannacry. I've seen it take systems out of operation and how extremely incessant and rapid it is in its attempts to spread throughout the network. It can send out thousands upon thousands of attempts to connect to other systems both on our network and outside the network all within every few minutes and this doesn't stop. It's impact cannot be underestimated and it's mitigation needs to be swift to prevent it spreading and causing further damage. For us in our cyber soc that meant performing actions like putting in a port 445 block to stop those external attempts as initial mitigation steps.

What we can learn from the wannacry attacks is really about the potency of many kinds of ransomware when it comes to spreading and the massive loss of revenue. We see the importance of keeping our systems up to date with proper and effective patching. Security engineers need to monitor the latest vulnerabilities, have a proper inventory of the services, operating systems, applications and dependencies being run on the systems through the organization and what versions they are at. Using this information combined with keeping abreast of security vulnerabilities and performing threat modelling with risk management processes like DREAD they can determine the best path forward with dealing with the various vulnerabilities in the wild.

We can learn about how vital it is to detect these compromises as swiftly as possible in order to reduce the impact and spread. The importance of having a big enough security team to cover the span of the networks that are needed to protect. The earlier we can stop the attacks the more likely we are to decrease the impact. They also need to keep abreast of the latest security vulnerabilities their attack vectors, techniques and how to remediate them. We also know that this was targeted heavily to those in the healthcare sector and as a result as a company we could very well be a priority target at this very moment for a number of ransomware groups. We also note that again the need for proper cybersecurity training for regular staff to ensure that they don't get exploited by phishing links with attachments or links in them. Even today there are still millions of machines that have not updated to cover the Wannacry attack vector..[12]

C. Fed Ex Attack

FedEx reported an estimated $300 million loss in its first quarter earnings report Tuesday, attributing the loss mostly to a computer virus that impacted the company's operations across Europe in July. The package delivery company's Dutch subsidiary, TNT Express, was infected with the NotPetya ransomware virus in late June. NotPetya hit companies in Ukraine and soon spread to other countries. Much of TNT Express's operations are based in Ukraine. The attack froze users' computers, encrypted their files and demanded a ransom of $300 in bitcoin to regain access. [15]

Like the earlier WannaCry outbreak, NotPetya used a Windows_exploit stripped from an NSA leak to spread across networks. For this attack, the majority of those who were infected were in Ukraine and the attack vector was exploiting a vulnerability in M.E. Doc an accounting piece of software created by a kiev based software company Intellect Service. An interesting point found by cybersecurity researchers is that for those who did pay it didn't matter. This was actually a wiper making it impossible for the files and data to go back to their original state and as a result were no longer useful. TNT Express, a part of FedEx, made use of this software and was affected badly by it leading to a temporary suspension of tradining it's shares on the New York Stock Exchange. [16]

While FedEx reported a $1.24 billion operating profit for the quarter, that came in about $300 million below what was expected due to the hack. The earnings report released Tuesday by FedEx notes that most of TNT's services resumed after the attack and "substantially all" its critical operational systems are back up and running, but volume, revenue and profits were negatively impacted.. [15]

What we can learn from this attack is the importance of proper assessment of third party tools that are used within the company. Is this a reputable company that regularly updates it's software? Do they respond to problems with their software in a timely manner? Are they security conscious? We see a different attack vector with accounting software being the vehicle from which the attack is launched. Again, it emphasises the need to keep up to date with latest releases of software and ensuring that these third parties are properly vetted not only for the purpose of what they bring but these additional security considerations are also needed to ensure we are not introducing some transitive risk. Like previous attacks we see that prevented measures could have stopped the drastic impact to operating and the huge sum of revenue that was lost.

D. Baltimore Attack

WannaCry and NotPetya was not the last ransomware to exploit the Enternal Blue in Windows. In the US city of Baltimore RobinHood ransomware managed to take most of the city government's computers offline. The hackers sought out a payment of over $76000 to restore their access. This came along with threats to increase that very ransom within 4 days and permanently the data if their demands were not within the time frame. These demands were refuted. [13]

The estimated damages of this attack totalled around £18.2 million for a vulnerability that had been about for some time and critically, there was an assessment report that came out which highlighted security gaps and the failure to act resulted in dire consequences for the city on a number of fronts.. [14]

What we can see here from this attack is that ransomware is a threat to all, whether is an organisation, a government, a regular everyday user browsing the internet or an entire region and it's infrastructure can be infiltrated. We note that even that again we see the use of a vulnerability Eternal Blue that had been known about for quite some time and Microsoft had released a patch for but like many many other systems across the globe, these systems were not updated to protect themselves from these kinds of attacks. This is the very same vulnerability that wannacry exploited. The thought that it will never happen to me or us is a dangerous one and leaves any and all of us at risk to these threats. It shows that many many organizations and businesses are not doing enough to keep on top of cyber risks and that hackers are more than happy to keep exploiting the same vulnerabilities if they are protected against or patched against. It's a low hanging fruit for them and makes for an easy entry point to cause trouble and compromise systems and networks.

Also, another takeaway from this incident is that even when you rid yourself of the malware it's not any point of celebration. You are still at risk to further attacks until action is taken to remediate your systems and networks. Otherwise and especially with high profile attacks, the previous attackers know you are vulnerable and now everybody else does as well. If you haven't taken that as a warning to get yourself properly secured from this, further attacks will be imminent. There was not enough budget and proper security in place for the baltimore protection. This is all despite the fact that the cities of Atlanta and San Antonio were also hit by ransomware attacks and the warnings from their failures to act were not taken seriously enough. Ignorance is no longer bliss in these situations and without proper resource allocation and defenses in place, devastating attacks like this can and will happen. Being proactive about security controls instead of retrospectively regretting and reacting is key. The cost could be catastrophic otherwise.

IV. More On How This Threat Affects Our IT Landscape

By now I'm hoping that it's clear that our organization creating healthcare software and being a large organization that could potentially be able to afford a large ransom makes us an ideal target. When healthcare organizations are attacked it weighers heavier and for longer in the minds of people for sustained periods of time making the news and putting a costly toll and that toll would be played out within our organization if it was due to one of our applications. They shown to attackers to be a successful route to obtain a substantial ransom since they are part of critical infrastructure. We are inticately bound with these organizations.

In terms of our systems in our organisation we are predominantly windows with the latest asset inventory check (70% windows machines). A study done by Virus Total in 2021 showed that 95% of ransomware files were Windows based executable or dynamic link libraries. [17] If this is anything to go by this also puts us at a higher risk with being software for healthcare organization providers, a global organisation and the fact that our cyber programme is only starting to mature of late. However all devices from your Android devices, iOS systems, or Windows systems all are still a risk of this type of exploitation via ransomware. [4]

We have a wide attack surface with selling a number of different variants of our applications and hosting some of these in our own data centres and then others with our cloud provider. We do have firewalls in place which is of some help here. The patching that occurs for our systems is sporadic and not systematic. We have a small number of staff in cyber security teams however currently this number is not sufficient to manage all of the areas we need to cover, they are primarily based in our security operations centre. We are also facing budgetary constraints with revenue only marginally growing which adds to our challenges in attracting and retaining cyber security staff. Regular employees are not given proper training on things like phishing and other cybersecurity threats. As the incoming CISO, I'm currently in the process of outlining new Policies, Standards, Guidelines and Procedures to increase our security posture and the more fine-grained details of protecting against these attacks. Nearly 75% of those breached by ransomware in the Cybereason Ransomware Research report felt that they had good security policy, however going from an abstract security policy to effective security being concretely implemented requires tangible security controls, processes, training for staff and many other facets to be truly effective. [2] The weakest link in cyber security is people and with ransomware this is particular true and so our employees and their actions will be very important for our organization.

Taking a baseline prior to introducing and actively measuring the difference from the security changes will help us know that we're doing is making a difference as well. We must pay attention to lessons learned from the high profile cases above where those organizations who failed to sufficiently act and take these threats seriously, suffered greatly.

Ransomware Attack Vectors and Kill Chain

There are a number of different threat vectors for ransomware to make it's way onto your system, some of the more common ones are phishing and exploiting publicly facing applications or external reomte services. [3]

Many are leveraging social engineering in it's different formats however Virus Total research suggests that there are few associated with exploits with only 5% of their samples and those were making use of them. They did however note that tools such as Mimikatz, Cobaltstrike, Powerfshell and many different kinds of remote access trojans (RATs) were used to elevate privileges and as a way of lateral movement. [17]

Microsoft Word document macros and can be used as part of the delivery mechanism and the same with exploit kits. There are also different mechanism from a user clicking on a malicious link to malware being placed in advertising networks. These can be downloaded with the user even realizing or performing any actoin. [4]

Detection, Mitigation and Recovery with an Outbreak

As the majority of Internet-based threats target common vulnerabilities, simply plugging these gaps can considerably improve security. It's not a simple fire-and-forget solution, however, because the Internet is a constantly evolving battleground. Cyber hygiene is something that needs to be monitored and reviewed, much like any other business activity: if something isn't working, or costs too much, you should be checking to see how it can be improved. [18]

However ransomware does not stay static, there are wide families and attackers are always looking to expand the capabilities and utilize different methods to ensure that their ransomware and malware in general can be undergoing metamorphosis in order to avoid detection and exploit vulnerable systems. [19]

There are free services available such as ID Ransomware that can identify the strain of malware and can offer information as to whether there are decryptors available or not. Also there is VirusTotal which is a great tool for uploading any suspicious files and can check a whole host of different tools to see if they contain a hash of known ransomware or any other known malware.

Should you pay the Ransom?

One of the common topics that arises in relation to ransomware is whether or not you should pay the ransom in the event that your system. I am of the opinion that we should not pay the ransom. 80% according to the report come back again. Why? Because they know that that the same systems are still vulnerable. As the saying goes, there is no honour among thieves and many of these ransomware gangs would fall into this category. [2]

Some organizations when they do pay the ransom could face the scenario where they don't release the data or it's been damaged in some way or they could face a second impending. Regular backups are a must here however even where backups are present some ransomware gangs can threaten to post sensitive information online with double extortion tactics. Thus this mitigation strategy can be rendered less effective with GDPR fines, loss of reputation, customer trust, as well as others threatening stock manipulation to short the company stock against an impending release of that sensitive information. Or it could be completely removed if they are capable of removing the backups. Hence why it's important to keep this backups offline and out of the networks completely air gapped from any system on the corporate network.

Even in the best possible scenario where our systems are now back able to be in operation and our data is back available, this would not be a point of celebration. These systems would still be vulnerable and could be attacked again. Bringing them back online without properly addressing these already exploited vulnerability could be a reckless approach and bring about further compromise and devastation to the confidentiality and availability of our systems and data. These vulnerabilities would need to be mitigated with little undue delay.

Prevention

Prevention of this kind of threat must involve a defence in depth approach to increase the likelihood of being. With multiple types of security controls in place we can reduce the attack surface for potential attack vectors being exploited.

The best approach in my opinion lies within this focused prevention and recovery. This requires investment from our company and that investment is paid back by developing the security of our systems and services as an asset to the company. This can help as a marketing selling point to customers who can know that they can trust our services, our brand and have the confidence to know that their data is also safe with us. We've taken the necessary steps because we know how important it is to continue a focused security process that remains vigilant and adapting to the evolving threat landscape we face as an organization. Security is a responsibility that takes a cultural adoption to be truly successful while also accepting that there is no such thing as being 100% secure. Some level of risk is always there.

Some things we can introduce for all employee could be 6 month/yearly training on cybersecurity and good cyber hygiene, phishing campaigns run by SOC to check the level of employees actions based on that training, Regular emails to employees so that their cyber awareness regularly has the chance to increase, discouraging the use of external devices on corporate systems, and training users, so they can identify and report phishing attacks. give users a way of reporting an outbreak, dedicated phone number and email to the cybersoc.

For a cyber team, knowledge sharing, regular lessons learned on different incidents, dedicated analysts monitoring and dealing with phishing incidents, means of shutting down specific ports e.g. 445 for SMB, unplanned simulations for both the SOC and executive teams, tabletop exercises, examine ransomware that does make it into the network and try to determine it's behaviour, awareness of obfuscation techniques used to avoid detection

Systems and networks

They can contain some simple more important tips on cyber hygiene and specifically on ransomware

also notifying about recent attacks and their impact and how it was caused and if possible could have been prevented.

- *Sufficient investment in Email filtering systems:* It needs to examine and scan email attachments. A lot of ransomware can be transmitted via .zip or .rar or .7z extensions. Older file types like .doc and .docm should also be blocked since they use macros. Blocking ought to be applied to .js and .wsf files a swell. A good vendor option to go with here would be Proofpoint which have some very effective tools for email filtering.
- *Anti-virus software* that runs regularly and reports when malware has been detected and raises an alert to the security operations team.
- *MFA (Multi-Factor Authentication)* which can stop lateral movement if the ransomware has made it's way onto the system.
- *Network segmentation* can also help for a similar reason, confining the malware or intruder to a given subnet for example.
- *Patch systems:* one of the most important things to keep ransomware at bay is keeping all systems and services properly patched and enforcing deadlines to have these done by.
- *Blocking sites* deemed to be a threat and ones with drive-by attacks that could contain ransomware.
- *Disable any external facing remote services and ports not needed.* This includes removing powershell from any system that doesn't require it and for those that do, enforcing that only signed powershell scripts can run as an additional mitigation strategy.

REFERENCES

[1] Financial Trend Analysis: Ransomware Trends [Online] Avaiilable: https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

[2] B. Keeler, 'Ransomware: The True Cost of Business, [Online] Available::

https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

[3] Group I-B, Ransomware Uncovered: 2020-2021,

[Online] Available:

https://explore.group-ib.com/ransomware-reports/ransomware_uncovered_2020

[4] A Liska, Ransomware, 2016

[5] D. Palmer, Ransomware vs WFH: How remote working is making cyberattacks easier to pull off

[Online]Available: https://www.zdnet.com/article/ransomware-vs-wfh-how-remote-working-is-making-cyberattacks-easier-to-pull-off/

[6] Allianz, Ransomware Insights: Risks and Resilience

https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/agcs-ransomware-trends-risks-and-resilience.pdf

[7] N. O'Leary, Irish Times,

[Online] Available:

https://www.irishtimes.com/news/politics/ireland-is-taking-measures-over-potential-cyberattacks-taoiseach-says-1.4806509

[8] PricewaterhouseCoopers, Conti Cyber Arttack on the Hse - Independent Post Incident Review

[Online] Available:

https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

[9] Imprvera, Wannacry Ransomware, [Online] Available:

https://www.imperva.com/learn/application-security/wannacry-ransomware/

[10] J. Fruhlinger, What is WannaCry ransomware, how does it infect, and who was responsible?, [Online] Available:

https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[11] Kaspersky, What is WannaCry Ransomware, [Online] Available:

https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[12] Z Whittaker, Two Years After Wannarcy, a million Computers Remain At Risk, [Online] Available:

https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAEX

[13] N2WS, The Baltimore Ransomware Attack, [Online] Available: https://n2ws.com/blog/aws-disaster-recovery/baltimore-ransomware-attack

[14] A. Petcu, The Curious Case of the Baltimore Ransomware Attack: What You Need to Know, [Online] Available: https://heimdalsecurity.com/blog/baltimore-ransomware/

[15] Z. Shorbajee, FedEx attributes $300 million loss to NotPetya ransomware attack, [Online] Available:

https://www.cyberscoop.com/fedex-attributes-300-million-loss-notpetya-attack/

[16] I. Arghire, NotPetya Operators Accessed M.E.Doc Server Using Stolen Credentials: Cisco, [Online] Available:

https://www.securityweek.com/notpetya-operators-accessed-medoc-server-using-stolen-credentials-cisco

[17] Virus Total, Virus Total Ransomware Report, October 2021, [Online] Available:

https://storage.googleapis.com/vtpublic/vt-ransomware-report-2021.pdf

[18] A. Calder, The Ransomware threat landscape, 2021

[19] McAfee, Advanced Threat Report October 2021, [Online] Available:

https://www.mcafee.com/enterprise/en-us/lp/threats-reports/oct-2021.htm

Link to slides and recordings:
https://drive.google.com/drive/folders/1qISE4vwJzfCulwwyIJCU3R9F1fkpQXX9?usp=sharing