Global Advanced Research Journal of Educational Research and Reviews (ISSN: 2315-5132) Vol. 10(2) PP. 252-256, April 2023
Available online http://garj.org/garjerr

Review

Mitigating Ransomware through Cybersecurity Law Enforcement

Philip Nnamdi Egbo

University Graduate School Bloomington, Cybersecurity Risk Management, Indiana University, Bloomington, U.S.A.
E-mail: egbophil@yahoo.com

Accepted 30 April 2023

Cybersecurity is a hot topic in our present-day society because of the role it plays especially in this era of Internet of Things (IoT) where there is a rapid growth in the network of connected computing devices. The internet has made the world a global village by bringing various nations, businesses, governments, and people together. The Covid19 pandemic has also contributed to the huge dependence on the internet as most organizations in both the public and private sectors were forced to operate virtually to contain the spread of the pandemic. The dependence on the internet by several individuals, governments, companies including financial institutions and health care industries for daily business operations have created multiple avenues for cybercrime. Some of these cybercrimes have escalated to become national security issues because of their impact on critical infrastructures. Ransomware is a prevalent cybercrime that was predicted by the European Union Agency for Cybersecurity to rise to 150 percent between April 2020 and July 2021. Due to the challenges of enforcing laws across various borders and attribution amongst other issues have created difficulties in managing ransomware attacks and other forms of cybercrime. Ransomware perpetrators have progressed from incoherent splinter factions to a sophisticated operation. The aim of this paper is to focus on some of the cybersecurity law enforcements that can mitigate ransomware attacks.

Keywords: Cybersecurity and Law Enforcement

OVERVIEW OF RANSOMWARE

Ransomware is a malicious software that prevents an individual or an organization from gaining access into their computer by locking it or deters the individual or organization from accessing the data on their computer, systems, or networks by encrypting the individual's sensitive data until the user pays a ransom to the ransomware actor to have their data decrypted (Federal Bureau of Investigation (FBI), 2020). Some of the critical data that is captured by the ransomware actors include the personal identifiable information (PII) of their victims and their authentication credentials. The ransomware actors in some cases exfiltrate this data and threaten to leak or sell the information if the ransom is not paid (Ransomware Task Force, 2021). The probability of the individuals getting back their data after making the payment for the ransom is uncertain.

There are two major forms of ransomware, and they include the Crypto ransomware, it is the most common type of ransomware that prevents the individual or organization from accessing their files or data by encrypting them and demanding that a ransom is paid to the threat actor to regain access to the files or data (Savage, Coogan and Lau, 2015). However, it is important to note that the majority of crypto ransomware utilizes encryption to deny individuals or organizations access to their data, but some do not (Savage et al., 2015). A survey conducted on 5000 Information Technology Managers in 2020 revealed that 51% of them had suffered a ransomware attack in the previous year and that 73% of those attacks had the victim's data encrypted (Ransomware Task Force, 2021). The second form of ransomware is known as the Locker

ransomware, it prevents the individual or organization from accessing their computers or systems by locking it, and it also requires a payment of ransom to the threat actor to unlock the system (Savage et al., 2015). Crypto ransomware operates by targeting the individual or organizations critical data and encrypts them (Richardson and Max, 2017). The crypto ransomware does not infect the individual or organizations system files, rather it allows the system to continue to function after being infected with the malware to allow communication between the data owner and the ransomware actor, such that if the malware is removed, the individual's data will still be encrypted (Richardson and North, 2017). Locker ransomware is targeted at the device or system which it locks to prevent the individual or organization from gaining access to the device or system (Richardson and North, 2017). At first, the locker ransomware targeted users of home computers until it later progressed to mobile devices (Ransomware, 2022). Unlike crypto ransomware, the locker ransomware only locks the device. The user can recover their files or data if the malware is removed or by relocating the storage of the device to a new system which makes the locker ransomware to be inefficient for ransomware actors (Richardson and North, 2017).

Doxware is malware that acts like a ransomware, it threatens to leak the user or organizations sensitive data or have them sold on the dark web if the ransom is not paid (Anchor, 2022).

EVOLUTION OF RANSOMWARE

The Cybersecurity Ventures have predicted that there will be a new ransomware attack on individuals and organizations every 2 seconds by 2031 as the ransomware actors are continually modifying their tactics and extortion schemes to capture their victims (Braue, 2022). Ransomware propagates in several ways, one of the methods of infection is by exploiting the vulnerabilities on the individuals or organizations devices, systems, or network (Ransomware Task Force, 2021). Another approach used by ransomware is through social engineering techniques such as phishing emails that deceive an individual or employees of an organization to open attachments that launch the malware to infect the systems and compromise the network (Ransomware Task Force, 2021). Other methods of ransomware proliferation include clicking on a malicious link or opening an ad on a computer that directs the system to a website that is embedded with the malware (FBI, 2020).

This paper highlights the evolution of major ransomware attacks that have occurred over the years as follows:

1989 – The first ransomware attack was launched by Joseph L. Pop, a biologist that was Harvard trained. The ransomware was named Aids Trojan also known as PC Cyborg (Humayun et al., 2021). The ransomware was distributed through a floppy disk drive at a World Health Organization international conference on AIDS, the ransomware made use of a simple symmetric cryptography to encrypt file names, and this enabled an easy decryption of the data (Humayun et al., 2021). The ransomware infected 20,000 floppy disks that were distributed at the conference. Ransomware did not gain much popularity then because of the limited number of people that were utilizing the internet (Humayun et al., 2021).

2005 - A ransomware named Trojan.GPCoder was launched in May 2005, it infected the victim's computer through phishing emails and encrypted the Microsoft Office application and media files on the computers (Humayun et al., 2021). This was the first modern ransomware, and it used an unsophisticated symmetric encryption technique that enabled the decryption and recovery of the data (Oz et al., 2021). In 2005, the International Telecommunications Union in their report proposed the term Internet of Things (IoT) as a way of using technology to connect the world (Humayun et al., 2021). As the IoT developed, it increased the growth and scope of ransomware (Humayun et al., 2021).

2006 – The Trojan.Cryzip was launched in March 2006, it copied the data files of the victim into a password protected archive file and deleted the original data files (Richardson and North, 2017). The malware code was included in the password which allowed easy data recovery. Trojan.archiveus was released in the same year, it was the first malware that requested a ransom of purchasing medications from a certain online pharmacy (Humayun et al., 2021).

2007 – The first locker ransomware was launched in 2007 and it was targeted at Russia. The ransomware locked the victim's computer with a pornographic image display that required a payment of ransom through a Short Message Service (SMS) or by calling a premium rate phone number to have the computer unlocked (Richardson and North, 2017).

2008 – A modified version of the Trojan.GPCoder known as GPCode.AK was released (Humayun et al., 2021). The GPCode.AK encrypted the targets data using a 1024-bit RSA key and demanded the ransom payment of $100 to $200 in electronic gold currency (Richardson and North, 2017).

2010 – Another version of locker ransomware known as WinLock was released (Humayun et al., 2021). The ransomware disabled the input-output interface of the victim's computer and asked for the payment of $10 via a premium rate short message service (SMS) to obtain the unlock code (Humayun et al., 2021). After arresting a group of 10 people involved in the attack, it was discovered that they earned over 16 million dollars from the SMS program (Humayun et al., 2021).

2011 – Prior to the emergence of cryptocurrencies, ransomware actors faced a major challenge on ransom payments as these payments were limited to certain geographical terrains, liable to local legal sanctions and nothing protected their identities and allowed payments of large ransom (Oz et al., 2021). The prevalence of cryptocurrencies such as bitcoin after 2009 enabled the ransomware actors to overcome this challenge and this led to a widespread of ransomware attacks where about 60,000 new variants of ransomwares were identified in 2011 (Oz et al., 2021).

2012 – A variant of the locker ransomware known as Reveton was launched, the target computer was locked once it accessed the malicious website (Humayun et al., 2021). The ransomware used a coercion method through a screen display with a message that the victim was responsible for violating cyber regulations, to force the individual to pay the ransom (Humayun et al., 2021). Similarly, a toolkit known as Citadel was introduced at a cost of $3,000, it enabled efficient ways of generating and distributing ransomware (Richardson & North, 2017). Likewise, a new toolkit identified as Lyposit was released in 2012, the ransomware pretended to originate from the law enforcement agency (just like Reveton) to deceive its victims (Richardson and North, 2017).

2013 – CryptoLocker ransomware was launched in August 2013, it made use of asymmetric cryptography to encrypt the victim's data files (Richardson and North, 2017). The original version was transmitted through a Gameover ZeuS banking Trojan botnet, and it encrypted about 67 data file types that included all data files of the Microsoft Office. The later version was released through an email that disguised to come from the United Parcel Service (UPS) or FedEx (Richardson and North, 2017). It demanded that ransom payment be made in bitcoin (Oz et al., 2021). Another ransomware known as Dirty decrypt was launched in July 2013, it targeted computers that were running different versions of the Windows operating system (Humayun et al., 2021).

2014 – Curve-Tor-Bitcoin (CTB) Locker ransomware was released; the name was derived from the technologies the ransomware was using. The malware used Elliptic Curve Cryptography for encryption, Tor for anonymity web browsing method used during the ransom payment and Bitcoin representing the mode of payment (Oz et al., 2021). Similarly, the Cryptowall cryptographic ransomware was launched, it used the same technology and compromised over 600,000 systems (Oz et al., 2021). Over a million dollars was generated from this version of malware (Richardson and North, 2017). Android Defender: the first locker ransomware for mobile devices was also introduced in 2014, it disguised as genuine antivirus software to infect its victim (Oz et al., 2021). The cryptographic version of the ransomware appeared a year later, it scanned the SD Card of mobile devices and used an Advanced Encryption Standard (AES) to encrypt files with certain extensions.

2015 – Ransomware-as-a-Service emerged in 2015 and it was designed to generate ransomware kits that could be easily modified and deployed by anyone that purchased it (Oz et al., 2021). So many ransomwares were detected in 2015 and this growth in scale could be linked to the widespread of the Internet of Things (IoT), some of this ransomwares include Tesla Crypt that targeted gaming files of its victims computer and demanded a ransom payment of $500, the first ransomware that targeted GNU/Linux operating systems known as Linux.Encoder was released and Cryptowall 3.0 was also launched (Humayun et al., 2021). A total sum of $27 million dollars was estimated to be paid in 2015 as ransom by the Federal Bureau of Investigation (FBI) (Richardson and North, 2017).

2016 – Petya ransomware was introduced, it was designed to overwrite the master boot record (MBR) of the targeted computer (Richardson and North, 2017). The malware demanded a $300 Bitcoin ransom payment (Humayun et al., 2021). CryptXXX ransomware was also launched in 2016, it targeted and encrypted the windows operating system. A ransom of 2.4Bitcoins was requested by the threat actors (Humayun et al., 2021).

2017 – WannaCry ransomware was released, and it was recorded to be the worst cybercrime in 2017 as it impacted 150 countries and infected over 250,000 systems, exploiting the vulnerability in the Microsoft Windows SMB Server Remote Code (Oz et al., 2021). NotPetya ransomware was also launched in 2017, it affected different sectors in multiple nations and encrypted the victims' windows operating system's master boot record (Cybersecurity and Infrastructure Security Agency (CISA), 2022).

2018 – PureLocker ransomware was released, it made use of a hybrid encryption and displayed a ransom note to the victims instructing them to contact the threat actor through an untraceable email service (Oz et al., 2021).

2019 – Ryuk ransomware appeared in 2019, it was programmed to target and disrupt specific companies including newspapers such as the Tribune papers and a North Carolina water utility company (Check Point Software, 2022). The malware demanded a payment of 15-50 Bitcoins (Check Point Software, 2022). REvil was another ransomware that was released in September 2019, REvil was responsible for shutting down about 22 towns in Texas (Check Point Software, 2022). It went further to shut down a United Kingdom currency exchange provider known as Travelex and demanded $6 million ransom (Check Point Software, 2022). Robinhood ransomware was also reported in 2019, a ransom of $76,000 was demanded (Check Point Software, 2022).

2020 – Corona ransomware emerged, targeting health organization during the COVID19 pandemic (Oz et al., 2021). It encrypted the medical records of patients (Oz et al., 2021). PureLocker ransomware was also identified in 2020, it was programmed to target the servers of large organizations whom the malware actors presumed will pay a huge ransom (Check Point Software, 2022).

2021 – A ransomware attack was launched that prompted Colonial Pipeline company to shut down 5,500 miles of its pipeline that accounted for 45% of the gas used on the East Coast of the United States (Dudley and Golden, 2021). The attack compromised the personal identifiable information of about 6000 people and $4.4 million was paid as ransom (Fung, 2022). According to research conducted by Checkpoint, it was observed that the global ransom cases had doubled in the first half of 2021 when compared to the ransomware cases experienced in 2020 (Check Point Software, 2022).

2022 – On February 27, 2022, Bridgestone detected a security breach on their network, the LockBit ransomware group was responsible for the breach, and they threatened to leak the data that was stolen from the company if the ransom was not paid (Saraie, 2022).

The above highlighted evolution of ransomware shows that the threat actors constantly modify their strategies to exploit even the latest technologies. Ransomware has

developed from malware that was distributed through a floppy disk drive to a large-scale enterprise that has the capability of exploiting zero-day vulnerabilities (Ransomware, 2022). Furthermore, ransomware has also progressed from demanding ransom payments in the form of gift cards or money to millions of dollars in cryptocurrencies, thereby making it the most profitable cybercrime (Ransomware, 2022). This indicates that ransomware will continue to prevail in our society if there are no cybersecurity law enforcements that ensure that ransomware perpetrators and other actors of cybercrime are brought to justice. Following the widespread use of the Internet of Things (IoT), computing devices, organizations, businesses, and people are becoming more dependent on the internet (Humayun et al., 2021). This advancement of IoT has also opened a wide opportunity for ransomware actors to exploit. Constant technological innovations are developed and launched by security researchers to protect individuals and organizations from ransomware attacks, however, it comes with its limitations. Some of these limitations include zero-day vulnerabilities and human factors because these factors are sometimes beyond control. Not everyone is technological savvy to know how to protect their digital life, similarly, a newly discovered zero-day vulnerability in a software could take a while to be patched if it requires certain privileges and affects confidentiality (Roumani, 2021). Developing and enforcing cybersecurity law turns out to be a formidable approach to mitigate ransomware and other forms of cybercrime.

IMPACTS OF RANSOMWARE

Ransomware is a global challenge as an attack could spread across countries and affect various sectors and institutions, a typical example of this is the WannaCry ransomware attack in 2017 that affected over 250,000 systems in 150 countries (Ransomware Task Force, 2021). Ransomware damages are estimated to cost the world $265 billion dollars annually by 2031 (Braue, 2022). Some of the major impacts of ransomware are summarized as follows:

Economy – Millions of dollars are paid yearly as ransom payments towards criminal organizations, $350 million was paid by the victims of ransomware attack in cryptocurrency, there by recording a 311% increase in ransom payments in 2020 (Ransomware Task Force, 2021). These payments exclude the actual cost of damages that are suffered by the victims. The Robinhood ransomware attack in Baltimore demanded $76,000 for ransom but the damages suffered cost the city of Baltimore $18 million (Check Point Software, 2022).

Loss of Data and Privacy – Ransomware attacks often lead to the loss of data and privacy (Ransomware Task Force, 2021). The colonial pipeline attack did not only steal 100 gigabytes of data (Kerner, 2022), but it also compromised the personal identifiable information (PII) of about 6000 individuals (Fung, 2022). This has also provided opportunities for the ransomware actors to carry out double extortions by demanding ransom payment for the decryption of the encrypted data and later threatening to leak the data or compromised PII's on the internet or the dark web (Ransomware Task Force, 2021). Only one major ransomware group was observed to exfiltrate data at the beginning of 2020, but by the end of that year, 17 other ransomware groups had adopted this approach (Ransomware Task Force, 2021).

Critical Infrastructure – The Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation reports have indicated that 14 out of the 16 critical infrastructures sectors in the United States have experienced a form of ransomware attack with healthcare and public health sector facing the most attacks (Waldman, 2022). In May 2021, the Federal Bureau of Investigation detected 16 CONTI ransomware attacks that targeted emergency medical services, First Responder networks, US Healthcare sector, 9-1-1 dispatch center, municipalities, and law enforcement agencies (FBI, 2021). It is important to note that attacks on nuclear facilities or power grids could cause significant consequences (Ransomware Task Force, 2021).

LIMITATIONS OF CURRENT CYBERSECURITY LAW

The current legal framework in the United States has a limited mention of the word "cybersecurity" in its laws, the word cybersecurity was first mentioned as a footnote in a published 2007 Seventh Circuit opinion in the US (Kosseff, 2017). Furthermore, the legal framework of the United States is fragmented as the US does not have a national law that governs cybersecurity (Li, 2018). The General Data Protection Regulation (GDPR) of the European Union (EU) has enabled the EU to develop a uniform data security law on all its member states, however, the passage of a GDPR-inspired state legislation has increased the complexities for compliance (Li, 2018). The Budapest convention on Cybercrime was a strategic approach to address cybercrimes such as ransomware in a global context, nevertheless, the non-participation of Russia, China and other nation states limits the scope of the convention (Kosseff, 2017). Moreover, a lot of the cybercrimes originate from Russia, China, North Korea, and Iran that are not part of the 50 nations that sanctioned the Budapest Convention that laid out procedures of extradition for cybercrime cases (Kosseff, 2017). Finally, most of the current cybersecurity laws are focused on confidentiality, not taking the other security triads; integrity and availability into account (Kosseff, 2017). Some of the ransomware attacks that were highlighted in the evolution of ransomware in this research paper showed that they deleted the user's data after comprising the system. This borders on integrity, similarly, the colonial pipeline ransomware attack led to the shutdown of its fuel distributions reducing the availability of gas along the east coast of the United States (Fung, 2022).

CONCLUSION

The 2017 WannaCry ransomware revealed that ransomware attacks have evolved to now become a global challenge that knows no borders. Mitigating ransomware will require the improvement of the current cybersecurity laws at the national and international level because a coordinated global action is needed to achieve this purpose. There is an urgent need to create an international law that defines the criteria to determine when cyber activities directed towards a nation violates its sovereignty. The legal framework for the international law can be developed to include actions for extradition and attribution to ensure that ransomware actors in foreign states are extradited or prosecuted. New regulations that monitor the cryptocurrency sector that enable ransomware attacks should be developed, as this will unmask the identities of the threat actors. Lastly, developing and enforcing a uniform cybersecurity law at the national and international level will also enable standardization, collaboration, and compliance.

REFERENCES

Braue D (2022). *Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031*. Cybercrime Magazine. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

Dixon VK (2009). Understanding the implications of a global village. *Inquiries J. 1*(11).

Dudley R, Golden D (2021). *The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-Promoting Cybersecurity Firms*. ProPublica. https://www.propublica.org/article/the-colonial-pipeline-ransomware-hackers-had-a-secret-weapon-self-promoting-cybersecurity-firms

Federal Bureau of Investigation (2022). *Ransomware*. Retrieved from https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

Federal Bureau of Investigation. “Internet Crime Report 2021”. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Fung B (2021). *Colonial Pipeline says ransomware attack also led to personal information being stolen | CNN Business*. CNN. https://www.cnn.com/2021/08/16/tech/colonial-pipeline-ransomware/index.html

Humayun M, Jhanjhi NZ, Alsayat A, Ponnusamy V (2021). Internet of things and ransomware: Evolution, mitigation, and prevention. *Egyptian Informatics J. 22*(1): 105-117.

Kerner SM (2022). *Colonial Pipeline hack explained: Everything you need to know*. Whatls.com. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

Kosseff J (2017). Defining cybersecurity law. *Iowa L. Rev.*, *103*: 985.

Li C (2018). A repeated call for omnibus federal cybersecurity law. *Notre Dame L. Rev.*, *94*: 2211.

Li S, Xu LD, Zhao S (2015). The internet of things: a survey. *Inf Syst Front* **17**: 243–259. https://doi.org/10.1007/s10796-014-9492-7

Osborne C (2021). *Ransomware in 2022: We're all screwed*. ZDNET. https://www.zdnet.com/article/ransomware-in-2022-were-all-screwed/

Oz H, Aris A, Levi A, Uluagac AS (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, *54*(11s): 1-37.

Petya Ransomware. (2018, February 15). https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware.

Ransomware Security Software | Anchor. (n.d.). Anchor. https://anchormydata.com/ransomware/

Recent Ransomware Attacks. (n.d.). https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/recent-ransomware-attacks/.

Richardson R, North MM (2017). Ransomware: Evolution, mitigation and prevention. *Int. Manage. Rev. 13*(1): 10.

Roumani Y (2021). Patching zero-day vulnerabilities: an empirical analysis. *J. Cybersecurity*, *7*(1): 023.

RTF Report: Combating Ransomware. (n.d.). Institute for Security and Technology. https://securityandtechnology.org/ransomwaretaskforce/report/

Saraie C (2022). Five ransomware attacks in 2022 so far you should know about. https://www.cshub.com/attacks/articles/five-ransomware-attacks-in-2022-so-far-you-should-know-about

Savage K, Coogan P, Lau H (2015). The evolution of ransomware. *Symantec, Mountain View*.

Schmitt MN, Vihul L (2017). Sovereignty in cyberspace: lex lata vel non?. *Am. J. Int. Law*. *111*: 213-218.

Shackelford S (2014). Defining the Cyber Threat in Internet Governance. In *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (pp. 3-51). Cambridge: Cambridge University Press. doi:10.1017/CBO9781139021838.004

The History of Ransomware? Understand | Prevent | Recover. (n.d.). Ransomware.org. https://ransomware.org/what-is-ransomware/the-history-of-ransomware/

Waldman A (2022). *FBI: Ransomware hit 649 critical infrastructure entities in 2021 | TechTarget*. Security. https://www.techtarget.com/searchsecurity/news/252515076/FBI-Ransomware-hit-649-critical-infrastructure-entities-in-2021