INSIGHTS INTO REGIONAL DEVELOPMENT
ISSN 2669-0195 (online) http://jssidoi.org/IRD/
2022 Volume 4 Number 2 (June)
http://doi.org/10.9770/IRD.2022.4.2(8)

Publisher
http://jssidoi.org/esc/home

RANSOMWARE: A COMPREHENSIVE STUDY OF THE EXPONENTIALLY INCREASING CYBERSECURITY THREAT

Attila Máté Kovács

Doctoral School on Safety and Security Sciences, Óbuda University, Baranyai utca 31c, 1117 Budapest, Hungary

E-mail: *kovacs.attilamate@uni-obuda.hu*

Received 10 April 2022; accepted 27 May 2022; published 30 June 2022

Abstract: Ransomware threats and incidents have exponentially increased causing both financial and reputational losses to organizations of all sizes and sectors. Ransomware attacks became the talk of the news when the world was hit by COVID 19 pandemic and people shifted to remote work in large numbers (Brynjolfsson et al., 2020, p. 13-14). Cybercriminals and threat groups are using various types of social engineering techniques such as email phishing, smishing, spear phishing attacks to spread ransomware infections in systems and networks. To protect organizations, users, and IT infrastructures it is important to understand how ransomware works, and how various threat actors use it to exfiltrate confidential data and information. Hence a critical approach toward ransomware infection and its mitigation by using different techniques is discussed and analyzed in this research paper concerning other scholarly articles and papers.

Keywords: ransomware; cybersecurity threat

Reference to this paper should be made as follows: Kovács, A. M. 2022. Ransomware: a comprehensive study of the exponentially increasing cybersecurity threat. *Insights into Regional Development*, 4(2), 96-104. http://doi.org/10.9770/IRD.2022.4.2(8)

JEL Classification: 033

Additional disciplines: safety and security

1. Introduction

Ransomware is a malicious malware that restricts a user's access to his system by encrypting files and folders that resides on it and demands a payment normally in the form of bitcoin to regain access to the encrypted files and to restore normal functionality. Various social engineering techniques commonly email phishing, spear phishing, smishing, and BEC attacks are used by threat actors to deliver ransomware into users' systems and demand extortion money.

Cyber extortion dates to the 1980s. The PC Cyborg Trojan (Tailor and Patel, 2017), the first ransomware that came into existence in 1989, restarted the target system approximately 90 times. During the process, the Cyborg Trojan encrypted all files and folders in the C drive and rendered the system unusable. Ransomware attacks carried out in the 1990s and early 2000s were conducted by hackers whose main aim was to gain fame through cyber pranks and vandalism (Srinivasan, 2017). More sophisticated and modern ransomware appeared around 2005 and quickly became a new strategy for cybercriminals to infect organizations (Chesti et al., 2020). Various families of ransomware were identified by researchers that inflicted different scales of damage to various industries (Lorenzo,2018). Of these areas, the attacks on health care institutions and hospitals are the best known.

These are carried out primarily by criminals, but in many cases even by members of terrorist organizations (Besenyő at al., 2021).

Ransomware in its different variants is usually aimed at encrypting user data. After data has been encrypted, a ransom is extorted. The data is only released after payment of the mostly digital ransom. With ransomware, a wide variety of organizations have already fallen victim to an extortion attempt: large corporations, medium-sized companies, and even hospitals (see Figure 1).

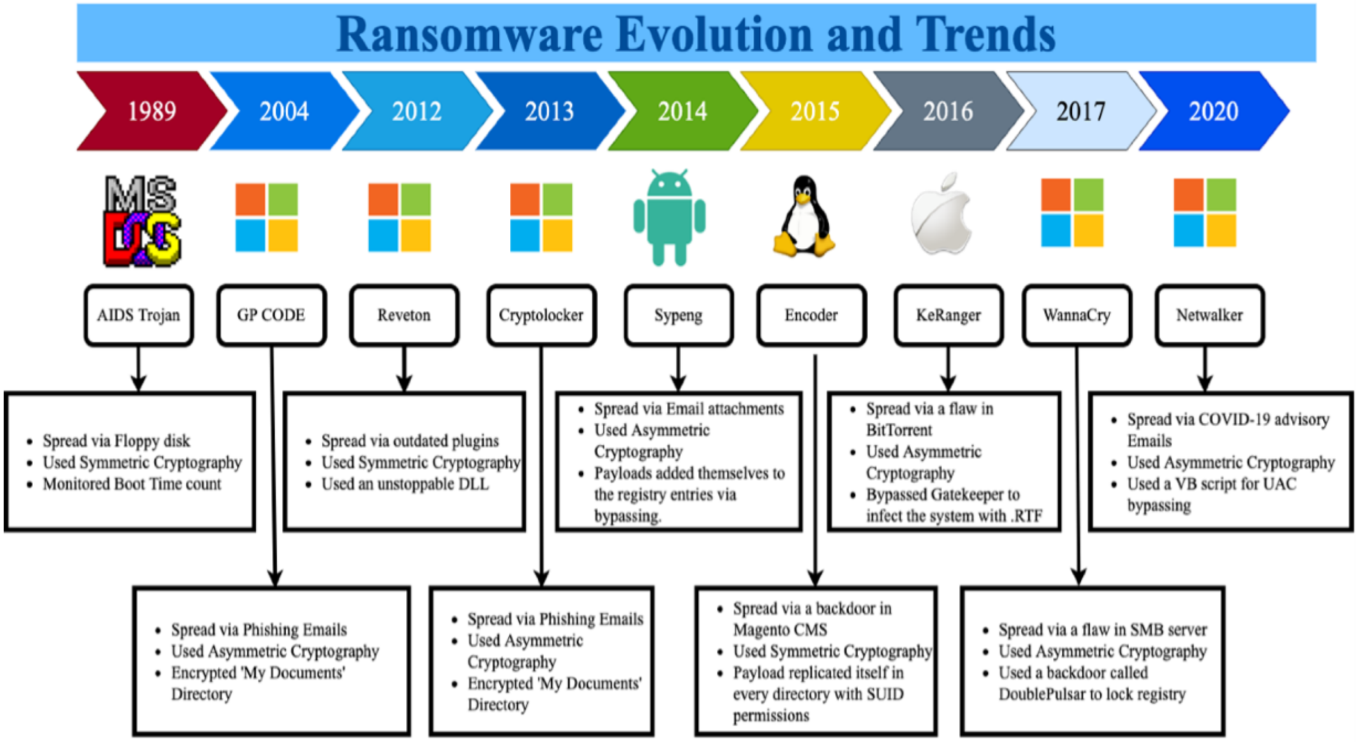
Ransomware Evolution and Trends
1989
2004
2012
2013
2014
2015
2016
2017
2020
AIDS Trojan
GP CODE
Reveton
Cryptolocker
Sypeng
Encoder
KeRanger
WannaCry
Netwalker
Spread via Floppy disk
Used Symmetric Cryptography
Monitored Boot Time count
Spread via outdated plugins
Used Symmetric Cryptography
Used an unstoppable DLL
Spread via Email attachments
Used Asymmetric Cryptography
Payloads added themselves to the registry entries via bypassing.
Spread via a flaw in BitTorrent
Used Asymmetric Cryptography
Bypassed Gatekeeper to infect the system with .RTF
Spread via COVID-19 advisory Emails
Used Asymmetric Cryptography
Used a VB script for UAC bypassing
Spread via Phishing Emails
Used Asymmetric Cryptography
Encrypted 'My Documents' Directory
Spread via Phishing Emails
Used Asymmetric Cryptography
Encrypted 'My Documents' Directory
Spread via a backdoor in Magento CMS
Used Symmetric Cryptography
Payload replicated itself in every directory with SUID permissions
Spread via a flaw in SMB server
Used Asymmetric Cryptography
Used a backdoor called DoublePulsar to lock registry

Figure 1. Evolution of Ransomware

A survey was conducted by Sophos (Sophos, 2021) led by Vanson Bourne across 5400 IT decision-makers in 30 countries. According to the researcher's key findings, it was estimated that 54% of the organizations were hit by ransomware and cybercriminals were able to successfully encrypt their important data. The average ransom paid by mid-sized organizations was US$170,404. The retail and education sector has been severely hit by ransomware attacks. Data is money and adversaries have found ransomware to be very useful in gaining their vendetta to be successful (see Figure 2).

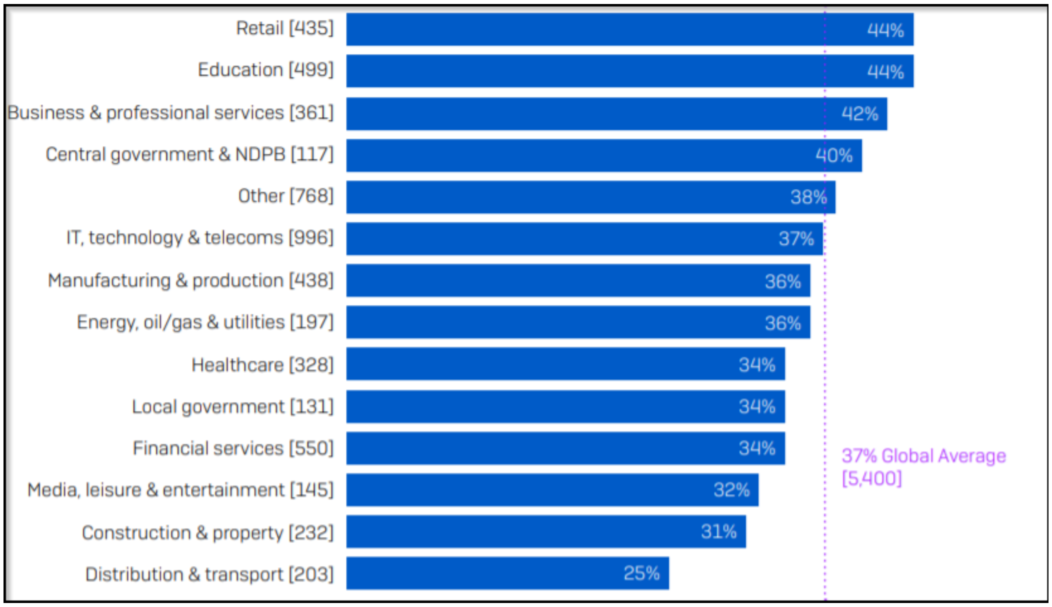

Figure 2. Among various business sectors retail & education sector has been severely hit by Ransomware

Ransomware is a typical attack vector utilized by cybercriminals to carry out nefarious operations such as preventing access to personal data until a ransom is paid. Adversaries demand the ransom in form of cryptocurrency such as bitcoin. The use of cryptocurrencies makes it difficult for law enforcement to track down recipient transactions (Alshaikh et al., 2020). The surge in Ransomware attacks was seen during the Covid 19 pandemic when an Android app called CovidLock was developed to study and analyze heat patterns on Covid-19 (Hama Saeed, 2020). As soon as users installed this application their contacts, gallery, and access to social media accounts were locked and a ransom was asked to be paid, in case of failure to pay the ransom adversaries threatened to make their data public.

In general, ransomware is breakdown into three categories – scareware, locker, and crypto (Atapour-Abarghouei et al., 2019) as shown in Figure 2. Scareware tricks a user into installing software or an executable by using pop-up ads, hence downloading the malware. Adversaries exploit human emotion of fear using scareware rather than encrypting files or locking the system until the ransom amount is paid (Andronio et al., 2015). The locker ransomware aims to disable primary functions of the target system by encrypting files that normally lock the system keyboard or screen. To overcome this malware the system can be rebooted into safe mode or using the on-demand virus scanner which eradicates the infection (Adamu & Awan, 2019). Crypto ransomware encrypts users' sensitive and important files instead of locking the basic functionality of the system. This type of ransomware is relatively hard to decrypt and uses strong encryption techniques which are nearly impossible to crack (see Figure 3).

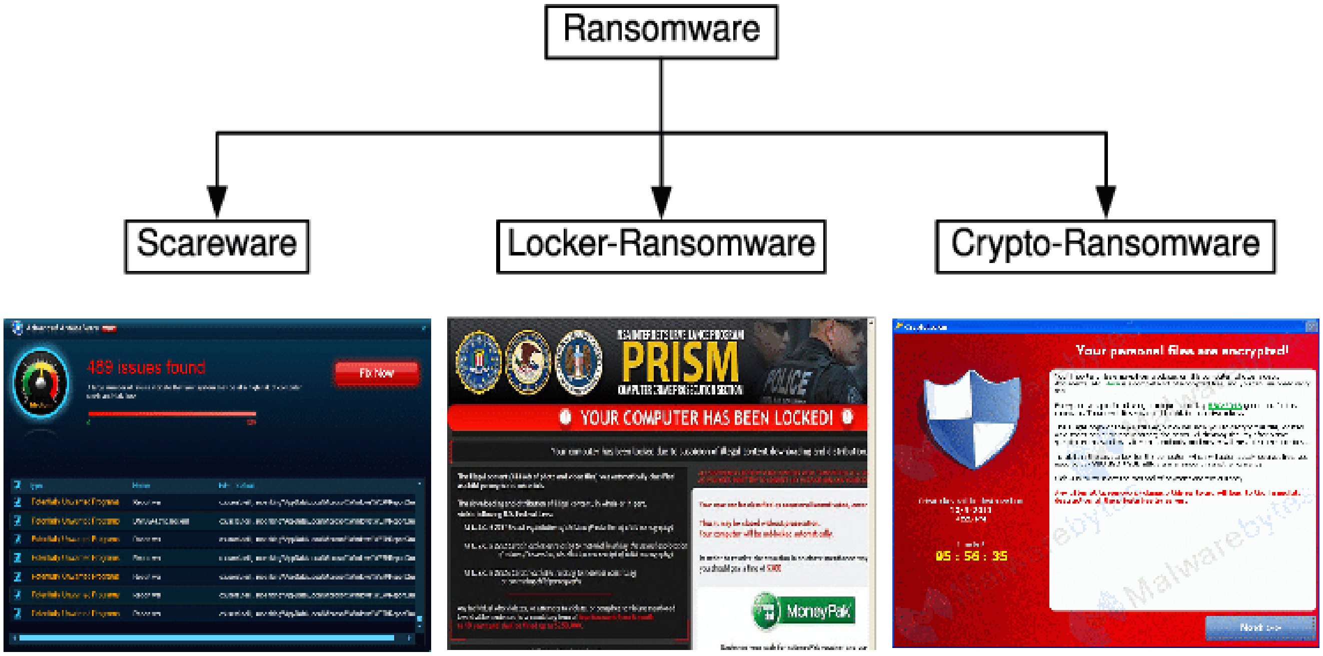

Figure 3. Categories of Ransomware

2. Literature review

A relatively higher number of scholarly research has been conducted on Ransomware, its propagation, and mitigation. Attacks using ransomware have become increasingly complex and have been adopting enhanced encryption techniques, which make it nearly impossible to retrieve data unless the ransom is paid.
Researchers created awareness among unskilled users of the organization regarding the dangers of ransomware (Gupta & Tripathi, 2017). The researchers listed down the threats due to ransomware such as system shutdown, loss of sensitive information, and financial loss. The study proposed mitigation techniques such as email security, intrusion detection, security policies, and the adoption of best practices.

Different types of ransomware have also been analyzed based on their ransom value (Hernandez-Castro et al., 2017a). The analysis was done on Cryptolocker, CryptoWall, and TeslaCrypt based on the price of ransom and the data available to the hackers. This encourages adversaries to adopt strategies that enable them to gain more financial value by targeting organizations.

The most popular and common environment targeted by cybercriminals is android due to its popularity among users of all kinds (Mercaldo et al., 2016). The research proposed the analysis of ransomware attacks on android mobile environments by taking malware samples and then analyzing them based on their behavior by applying a set of logical rules. The analysis aided in the identification of different types of ransomware. Mobile environments are more prone to ransomware attacks and its detection can be achieved by using approaches such as static, dynamic, and hybrid approaches (Manish, 2020). The static approach used techniques such as Linear regression, SVM, Code analysis, etc. At the same time, the dynamic and hybrid approaches used taint analysis, encryption, foreground, obfuscation, text, and image classification respectively. The research pointed out the accuracy of the proposed methodologies to be in the range of 95% - 98% which is quite a good score in the detection of ransomware in the android environment.

Various types of approaches have been used to detect ransomware. The most effective and common ones include the signature-based approach and the behavior-based approach. The signature-based approach detects unique patterns in ransomware source code and analyzes function calling sequences in ransomware code. The patterns are saved into a database that is used by an anti-malware solution for malware detection in executables. Signature-based approaches are effective and convenient as they have fewer false positives. According to research this approach is ineffective against obfuscated code in ransomware and is unable to detect new patterns unless manual hunting is used (Goyal et al., 2019).

In a behavior-based approach, researchers created an artificial virtualized environment to see the behavior of ransomware when it interacts with the system (Grant & Parkinson, 2018). The researchers analyzed the behavior of ransomware when it interacts with the file system of the operating system. The analysis was conducted through a file monitoring system that helped in monitoring the interaction of the malware with files. The research concluded that every ransomware has a unique ability to interact with file systems and files and can be distinguished by an individual or shared patterns.

Another approach was employed to study ransomware behavior on networks using reverse engineering (Zimba et al., 2018). The research focused on uncovering the interaction of the famous WannaCry ransomware interactions with the network. Dynamic analysis was used to detect the interaction of the malware with the network. The code analysis fetched the adapter properties of the infected network to extract information about the malware whether it resides on the private or public subnet to assess the propagation level and damage inflicted.

Similar research was conducted on the WannaCry ransomware based on an analysis of two components (Akbanov et al., 2019). The first component extracts a list of IP addresses based on local and public subnet and scans the internal and external network for MS17-010 vulnerability. The second component was based on the ransomware encryption process as it uses RSA keys for encrypting the files.

Prevention techniques for ransomware included categorizing ransomware characteristics of different variants (Singh, 2017). The research focused on analyzing different families of ransomware and its characteristics. The research concluded that many families of ransomware exhibited similar characteristics which made the detection and prevention relatively easier for known patterns of malware infection.

A new technique to recover from ransomware was introduced which assumed that the ransomware that targeted the windows system used the CNG cryptographic library to encrypt user files and folders (Lee et al., 2017). As per the research, the ransomware uses the same keys that are on the host so the retrieval can be achieved by using the same keys to decrypt the files.

The use of machine learning has aided in the detection of ransomware by using reverse engineering, static analysis, and machine learning techniques (Poudyal et al., 2018). The framework proposed in the research used analysis techniques that analyzed raw binaries, libraries, function calls, and assembly code.

3. Methodologies and Techniques

The research community has put earnest efforts into analyzing ransomware of different variants and has presented different methods of preventing ransomware. The main objective of doing this research is to present ransomware prevention techniques for organizations that can be easily adopted and implemented by organizations including common users.

4. User Training

The major cause of ransomware infecting organizations is the lack of user awareness of such cybersecurity threats. An organization can adopt state-of-the-art frameworks and security controls but still fail to protect its confidential data if its users are not aware. Adversaries always go for low-hanging fruits and use social engineering techniques (Hinson, 2008) such as email phishing, BEC attacks, smishing, etc. that entice the users into clicking malicious links and installing malware that results in a ransomware infection. Another way that the network or system may get infected is by using cracked or unpatched software (Kumar et al., 2016) downloaded from unverified sources.

To make the user aware of all the threats associated with ransomware a user awareness session should be conducted by organizations twice or thrice a month. Cyber drills should be conducted in which internal phishing campaigns should be launched to test the user's knowledge related to ransomware.

5. High damages caused by Emote and Wannacry

The Emotet malware program represents a possible attack vector. It is able to read contact relationships from mailboxes and subsequently send very authentic spam mail automatically. As a result, it has a high level of distribution and, at the same time, a comparatively high success rate in infecting corporate networks. Emotet and reloaded malware have thus already caused high damage to those affected in business and administration - and regularly reappear with new functions to cause damage supplemented by further techniques and malware.
Advanced attacks are characterized by the fact that they use malicious functions that used to be deployed manually in selected attacks, but are now deployed semi-automatically over a wide area. A variety of malicious functions means that advanced variants pose a significantly greater threat. In addition to the widespread use of increasingly sophisticated spam by malware such as Emotet, in many cases, the perpetrators are now taking a phased approach.

Whereas some time ago individual computers were encrypted and a ransom was demanded per encrypted PC, today affected corporate networks are first spied on in a targeted manner. In the process, data is often extracted and an assessment of the respective victim is made. The perpetrators then tailor their ransom demands to the affected organization. Encryption is often targeted and may include existing backups. Corporate networks are often completely compromised. The previously leaked data is often used to increase pressure on victims to act by threatening to publish or resell the data if the ransom for the encrypted data is not paid. The cleanup of affected networks can take months depending on the size of the affected network. Most recently, in several cases non-payment was threatened with the publication of previously stolen data, and in some cases, this was carried out.
Against this background, consistent preventive action is becoming increasingly important.

Two other relevant examples connected to mass effects and psychology can be WannaCry and Jigsaw.
On Friday, May 11, 2017, the world was shaken by a series of huge cyber attacks that brought several hospital systems in the UK to a standstill and led to the suspension of emergency care. These attacks occurred on the same day. It was identified as a ransomware virus and named WannaCry being followed by further variations (WanaCrypt0r 2.0, WCry), which locked down infected PCs and issued a screen message telling the users that the only way to bring the system back online was to pay $300 in cryptocurrency. According to cybersecurity companies, the vulnerability that was exploited in the attack was leaked shortly before WannaCry went viral by a team of hackers who used the name Shadow Brokers. The Shadow Brokers claimed to have obtained valuable data from the United States National Security Agency (NSA) in the time leading up to the attack. In just a single day, the number of infected computers surpassed the 100,000 mark.

The Jigsaw ransomware virus, if not the biggest attack, is probably the scariest, and the best example of psychological warfare; the malware, like the character in the horror film Saw, does not kill instantly, but "plays" with the victims, who are given 24 hours to pay the equivalent of one hundred and fifty dollars in bitcoins and get the unlock key. If they do not pay within the first hour, the ransomware deletes a file. After the second hour, one more, and so on for 72 hours. Because that's when everything is destroyed. Jigsaw even warns users not to try to restart the computer, or they can kiss the files goodbye immediately. And at the end of the message, a countdown timer starts, adding to the fear.

6. Understanding Shadow IT

Shadow IT as a phenomenon and term is defined as any hardware, software, or solution that is being utilized by users without the formal knowledge of the IT department (Silic & Back, 2014). Since the software or application being used by users is unknown to the IT department, this software can be a major cause of ransomware infection. Non-IT users may download software from unverified sites that could lead to malicious backdoor installation and may infect the system with ransomware.

The overcome the problem of users installing unverified software, all the users should be connected to the company domain and should not be allowed to install any type of software without the approval of the IT department. This can be reached via clearly defining the access control rules and authorization rules on the authentication mechanisms such as RADIUS or Domain.

7. Keeping Operating systems, applications & Services updated

Cybercriminals exploit older versions of operating systems, applications, and services. The security loopholes in unpatched or older versions of OS or applications running on the system are exploited by cybercriminals. They utilize various techniques such as remote code execution (Sharma & Singh Tomar, 2015) which allows initial access to the system. The adversary can then install the malware that will encrypt all files and folders of the target user.

It is strongly recommended to the organization keep their systems, applications, and services updated to the latest version. The latest software and applications have built-in auto-update options that automatically update their selves. This is true for both mobile devices and PCs.

8. Implementing Endpoint Detection Response Solution

Endpoint Detection Response (EDR) is an integrated solution that can continuously monitor real-time data of endpoints with rule-based automated detection and response. The whole point of implementing an EDR solution is to monitor each activity on the endpoint so that the risk of being infected by ransomware is minimized. EDR solution helps to analyze data patterns collected from various endpoints and automatically respond to threats to mitigate, contain, and notify the users.

9. Segmentation and Zero Trust Network

It is very important to segment your network based on trust boundaries, the type of data that is shared both internally and over the internet. Each network segment should be properly divided, and a clear information flow should be established with the right access control techniques. By setting up clear boundaries, in case of a ransomware infection, the malware will be restricted to that target system rather than propagating in the entire network.

The Zero Trust network is based on the principle that trust is nothing and validates everything (Sheikh et al., 2021). By validating traffic at every level of the IT infrastructure there will be a less likely chance that a system or host would be compromised by a ransomware attack.

10. Conclusion

Ransomware attacks will continue to rise and will become more complex and sophisticated with each passing day. It is very important to employ appropriate security controls that leverage ransomware attacks. Pattern Detection, behavior analysis, and code analysis are some of the most common ways that can detect, analyze and prevent ransomware attacks. These techniques can be embedded into enterprise tools that will help organizations protect their sensitive and critical data. By following a systematic plan that not only emphasizes using state-of-the-art tools but also basic security controls that may get missed by IT and security departments. Organizations and individuals should follow the discussed approach in the previous section to minimize the rate at which ransomware infections occur and to protect their organization's critical assets and data from adversaries.

References

Besenyő, J., Márton, K., & Shaffer, R. (2021): Hospital Attacks Since 9/11: An Analysis of Terrorism Targeting Healthcare Facilities and Workers, *Studies in Conflict & Terrorism*, https://doi.org/10.1080/1057610X.2021.1937821

Brynjolfsson, E., Horton, J., Ozimek, A., Rock, D., Sharma, G., & TuYe, H.-Y. (2020). *COVID-19 and Remote Work: An Early Look at US Data*. National Bureau of Economic Research. https://doi.org/10.3386/w27344

Sophos. (2021). The State of Ransomware 2021. https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf

Tailor, J. & Patel, A. (2017). A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control. *International Journal of Scientific Research*, 4.

Srinivasan, C. (2017). Hobby hackers to billion-dollar industry: the evolution of ransomware. *Computer Fraud & Security*, (11), 7-9. https://doi.org/10.1016/s1361-3723(17)30081-7

Fernández Maimó, L., Huertas Celdrán, A., Perales Gómez, Á.L., García Clemente, F.J., Weimer, J., & Lee, I. 2019. Intelligent and Dynamic Ransomware Spread Detection and Mitigation in Integrated Clinical Environments. *Sensors*. 19(5):1114. https://doi.org/10.3390/s19051114

Chesti, I. A., Humayun, M., Sama, N. U., & Jhanjhi, N. (2020a). Evolution, Mitigation, and Prevention of Ransomware. In *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*. IEEE. https://doi.org/10.1109/iccis49240.2020.9257708

Alshaikh, H., Ramadan, N., & Ahmed, H. (2020). Ransomware Prevention and Mitigation Techniques. *International Journal of Computer Applications*, 177(40), 31–39. https://doi.org/10.5120/ijca2020919899

Hama Saeed, M. A. (2020). Malware in Computer Systems: Problems and Solutions. *IJID (International Journal on Informatics for Development)*, 9(1), 1 https://doi.org/10.14421/ijid.2020.09101

Adamu, U., & Awan, I. (2019). Ransomware Prediction Using Supervised Learning Algorithms. *In 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE.* https://doi.org/10.1109/ficloud.2019.00016

Gupta, G., & Tripathi, D. K. (2017). Study on ransomware attack and its prevention. *Computer Science*, 3(5).

Mercaldo, F., Nardone, V., & Santone, A. (2016). Ransomware Inside Out. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE. https://doi.org/10.1109/ares.2016.35

Android Ransomware and Its Detection Methods. (2020). *International Journal of Innovative Technology and Exploring Engineering*, 9(4), 1252–1255. https://doi.org/10.35940/ijitee.d1632.029420

Goyal, P. S., Kakkar, A., Vinod, G., & Joseph, G. (2019). Crypto-Ransomware Detection Using Behavioural Analysis. In *Reliability, Safety and Hazard Assessment for Risk-Based Technologies* (pp. 239–251). Springer Singapore. https://doi.org/10.1007/978-981-13-9008-1_20

Grant, L., & Parkinson, S. (2018). Identifying File Interaction Patterns in Ransomware Behaviour. In *Computer Communications and Networks* (pp. 317–335). Springer International Publishing. https://doi.org/10.1007/978-3-319-92624-7_14

Zimba, A., Wang, Z., & Chen, H. (2018). Multi-stage crypto ransomware attacks: A new emerging cyber threat to critical infrastructure and industrial control systems. *ICT Express*, *4*(1), 14–18. https://doi.org/10.1016/j.icte.2017.12.007

Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms. *Journal of Telecommunications and Information Technology*, 1, 113-124. https://doi.org/10.26636/jtit.2019.130218

Singh, T. (2017). Evolving Threat Agents: Ransomware and their Variants. *International Journal of Computer Applications*, 164(7), 28–34. https://doi.org/10.5120/ijca2017913666

Poudyal, S., Subedi, K. P., & Dasgupta, D. (2018). A Framework for Analyzing Ransomware using Machine Learning. In *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE. https://doi.org/10.1109/ssci.2018.8628743

Hinson, G. (2008). Social Engineering Techniques, Risks, and Controls. *EDPACS*, 37(4-5), 32–46. https://doi.org/10.1080/07366980801907540

Kumar, S., Madhavan, L., Nagappan, M., & Sikdar, B. (2016). Malware in Pirated Software: Case Study of Malware Encounters in Personal Computers. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE. https://doi.org/10.1109/ares.2016.101

Silic, M., & Back, A. (2014). Shadow IT – A view from behind the curtain. *Computers & Security*, 45, 274–283. https://doi.org/10.1016/j.cose.2014.06.007

Sheikh, N., Pawar, M., & Lawrence, V. (2021). Zero trust using Network Micro Segmentation. In *IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE. https://doi.org/10.1109/infocomwkshps51825.2021.9484645

Attila Máté KOVÁCS works at Óbuda University Doctoral School on Safety and Security Sciences; Cognizant [CEHv11 Certified Ethical Hacker; Certified Chief Information Security Officer and ISO27000 auditor]. After earning a post-graduate degree in Energy Economics from the Regional Centre for Energy Policy Research, Budapest Corvinus University, for a thesis on Electricity Capacity Mechanisms, he also deepened his knowledge in two proficiency fields of his interests, Artificial Intelligence and Machine Learning, at Kürt Academy and Stanford. At the start of his career, he worked as a strategy consultant at Roland Berger Strategy Consultants and Accenture and later at Cyber Services Plc in international information security Research & Development projects.Before joining Cognizant in 2021 in an Information Security Management position, he worked at the air navigation service provider Hungarocontrol, personally contributing to the remote tower and remotely controlled aerial vehicle development and regulatory initiatives.
ORCID ID: 0000-0001-5088-5749
