RECENT TRENDS

THE RISE OF CRYPTO-RANSOMWARE IN THE CYBER-ATTACK WORLD

PhD Research Lab
Industry ⇄ Research

EXECUTIVE SUMMARY

- Digitisation has improved the lifestyle of internet user, and all tasks can be performed effectively, easily and efficiently.
- Each pillar has two sides, this facility in the digitisation trend towards cyber-attacks.
- The ransomware attack is one of the latest popular cyber-attacks.

INTRODUCTION

In the digital world where all data is stored digitally, 24X7 data can be easily accessed at a lower cost at any time. In one click, all functions are performed quickly, effortlessly and effectively. Digitization has improved the internet user's lifestyle. But, "There are two sides to each pillar." Where, digitalization creates security issues like cyber-attacks for the government (public) and private confidential information (Mohurle & Patil, 2017). The various cyber-attacks on the network are ransomware, spyware, adware, phishing, spam, malware, Trojan, virus, intruders, etc. to steal confidential data. In that, the ransomware is one of the popular data theft methods. The few types of ransom ware attacks are Crypto Locker, TeslaCrypt, Reveton, TorrentLocker, CryptoTear, KeyRanger, CryptoWall, Fusob, Locky, SamSam and WannaCry. Ransomware is a kind of malware infection; it is injected to the user's system and infects all important information and files. It is hard to get out once it is transferred. Once ransomware is activated in the user system then it will encrypt files like .mp3, .jpg, .doc,.xls, etc. then, the ransom is demanded to release the data. It is like system hostage to the hackers. In this case, the user has two options, pay ransom, and collect all the files or format the system. But there is no guarantee that the data will be received in decrypt format. Ransomware has become one of the largest scams to hit businesses over the past few years. The Federal Bureau of Investigation (FBI) predicts that damages in 2016 is around $1 billion (Brewer, 2016).

Digital Transformation and Cyber Attacks

How is the Ransomware infect the system?

The ransomware Trojan mostly sends to victim system through a malicious website or as a phishing spam message in email. Once the message is downloaded and opened by the victim then the attacker takes control of the victim system. The intruder then demands the Bitcoin as a ransom, mostly; the ransom is in bitcoin form, because it is cryptocurrency. Further, the intruder provides only short period of time to pay the ransom amount. That’s because, to stop victim finding alternative data recovery solution. Generally, most victims ask for more time to pay the bitcoin or they negotiate for less price.

Old Ransomware Attack

The concept of ransomware has been around for quite a while. In 1989, Dr. Joseph Popp published a Trojan named AID. It is also known as PC Cyborg Trojan or Aids Info Disk. The Trojan has encrypted all files and folders and hidden them on the PC's C: drive. This attack is in the form of license renewal, where, personal computer (PC) permission is blocked. A script message is delivered to the victim, requesting a $189 ransom and it should be transferred to the Corporation of PC Cyborg through post office box in order to renewal the license. The infected PC didn't function until the ransom is paid and the acts of the malware have been reversed once payment done (Brewer, 2016).

Recent Ransomware attacks

The Wannacry is one of the worst ransomware attacks in 2017. Wannacry spread all over the world in one day, 150 countries were infected and more than 230,000 computer systems were corrupted causing $4 billion financial loss (Petrenko, Petrenko, Makoveichuk, & Chetyrbok, 2018). The Wannacry is one kind of software malicious; it targeted the British National Health Service, where clinics and hospitals were shut down, and almost 20,000 appointments had been cancelled. This ransomware malware blocks user access to the system. It encrypted and held the entire device as hostage until they release the ransom amount. Once payment is done the decryption key is provided to access the system (Mohurle & Patil, 2017).

In May 2019, the ransomware attack called Robbin Hood occurred in the American city, Baltimore. Baltimore is the second US town targeted for the ransom attack (Fisher, 2019). The government computer systems of Baltimore are attacked by the RobbinHood virus for ransom. Essential services and all servers were taken offline with ransom note demanding $76,280 approximately (13 bitcoin) to release the encryption key. But the government refuses to pay the amount to the intruder. But the government spent nearly $18 million to recover the system (Threat, May, & Bell, 2019).

SUMMARY

Digitalisation has become a worldwide cornerstone of technology, the same trend towards cyber-attacks like ransomware. The ransomware is malware that exploits and infects the computer system. Mostly the ransomware attack is in the encrypted form. It will not allow the data to be retrieved or backed up. Even if a system holds a lock on those files, it will kill the process and proceed to attack the file. Where the Internet is needed for some ransomware malware attacks and some do not need it. Some malware is capable of destroying the data without internet. The malware is program in such a way that it will clean up itself from the victimised device without leaving any forensic evidence. In three ways we can prevent some assaults on ransomware, they are software applications that are insecure or outdated should be updated, then executable file placing position like %TEMP% or %APPDATA should be clean up regularly and finally backup should be taken regularly in the computer system. In the future, to resolve cyber-attacks like ransomware, cyber security should be strengthened.

REFERENCES

- Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. Network Security, 2016(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1

- Fisher, C. (2019). A ransomware attack is holding Baltimore's networks hostage. Retrieved October 4, 2019, from engadget website: https://www.engadget.com/2019/05/08/baltimore-city-government-ransomware-attack/

- Lie-Bjelland, O. (2019). Digital transformation – Is cyber threat really the greatest risk of all? Retrieved October 4, 2019, from Corporater website: https://corporater.com/en/digital-transformation-is-cyber-threat-really-the-greatest-risk-of-all/

- Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science (IJARCS), 8(5), 1938–1940. https://doi.org/10.26483/ijarcs.v8i5.4021

- Petrenko, A. S., Petrenko, S. A., Makoveichuk, K. A., & Chetyrbok, P. V. (2018). Protection model of PCS of subway from attacks type «wanna cry», «petya» and «bad rabbit» IoT. 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 945–949. https://doi.org/10.1109/EIConRus.2018.8317245

- Threat, C., May, R., & Bell, P. (2019). Cyber Threat Report May 06, 2019. Retrieved from https://digitalcommons.usmalibrary.org/cgi/viewcontent.cgi?article=1044&context=aci_rp

Format type: E-Book

UK: 10 Park Place,
Manchester M4 4EY.
UK: +44-1143520021
Email:info@phdassistance.com
Web:www.phdassistance.com

ABOUT THE DEPARTMENT

Engineering and Technology Lab at PhD Assistance is involved in exploring novel research areas by conducting dynamic research. It promotes innovation in all fields of engineering by advancing the technology with structured and continuous research. The problems and challenges faced by the existing technologies and trends are explored by our researchers exist in scholarly literature, in theory, or in practices that needs deliberate investigation These problems are identified and fixed by our researchers by suggesting better novel alternatives with appropriate tools, technologies and approaches, thereby proving their effectiveness in real time applications.

ABOUT US

PhD Assistance, is world's reputed academic guidance provider for the past 15 years have guided more than 4,500 Ph.D. scholars and 10,500 Masters Students across the globe. We support students, research scholars, entrepreneurs, and professionals from various organizations in providing consistently high-quality writing and data analytical services every time. We value every client and make sure their requirements are identified and understood by our specialized professionals and analysts, enriched in experience to deliver technically sound output within the requested timeframe. Writers at PhD Assistance are best referred as 'Researchers' since every topic they handle unique and challenging. We specialize in handling text and data, i.e., content development and Statistical analysis where the latest statistical applications are exhausted by our expert analysts for determining the outcome of the data analysed. Qualified and experienced researchers including Ph.D. holders, statisticians, and research analysts offer cutting edge research consulting and writing services to meet your business information or academic project requirement. Our expertise has passion towards research and persona l assistance as we work closely with you for a very professional and quality output within your stipulated time frame. Our services cover vast areas, and we also support either part or entire research paper/service as per your requirement at competitive prices.