Journal of Advanced Research in Computer Graphics and Multimedia Technology
Volume 2, Issue 1 - 2020, Pg. No. 17-19
Peer Reviewed Journal

Article

An Analysis on Ransomware and System Safety

Arpit Kumar Sharma[1], Sayar Singh Shekhawat[2], Charchit Sharma[3], Chirayu Mehta[4]

[1]Research Scholar,[1]Computer and Communication Engineering, Manipal University Jaipur, Jaipur.
[2,3,4]Department of Computer Science, Arya Institute of Engineering Technology, Jaipur.

I N F O

Corresponding Author:
Arpit Kumar Sharma, Computer and Communication Engineering, Manipal University Jaipur, Jaipur
E-mail Id:
er.aks31@gmail.com

How to cite this article:
Sharma AK, Shekhawat SS, Sharma C et al. An Analysis on Ransomware and System Safety. *J Adv Res Comp Graph Multim Tech* 2020; 2(1): 17-19.

Date of Submission: 2020-02-12
Date of Acceptance: 2020-03-18

A B S T R A C T

As we can see computer has start playing a big role in our daily life. From the very beginning if we see we humans are not much dependent on computers but if we see nowadays it is like our own fragment that we can't work without computer. While use of computers in our life is increased with this our cyber securities complexities are also increased as well. Very next day we hear new kind of cyber-attacks on our computers it not just only affects our daily life but it also disturbs our digital world also. As the cyber-attacks are increasing day by day, different kinds of attacks are introduced yet among all the dangerous attacks one is rated high known as Ransomware. In this paper we will explore and learn more about Ransomware that how it attacks and affect your computer and how it actually works like and how dangerous it is.

Keywords: Ransomware, System Security, malicious file, Attacks

Introduction

Our computers are getting more advanced and enhanced by new tech. day by day. This enhancement is leading and affecting our daily life as well, nowadays it is like our daily lives or our daily routine.[1-3] No one or nobody is there who is not using online services these services start playing an significant role in our daily life and from easy to easy and hard to hard work we use computer amenities to save time but to save time sometime we lose our securities.[4-5] As the graph of digitalization is getting increase day by day in our daily routine and the cybercrimes as well proportionally.[6-7] Among all the threats there is a dangerous threat which was very active from few last year's known as Ransomware. Well moving forward on the threat lets know how Ransomware works.[8-10] what ransomware do is that the attacker sends a miscellaneous mail or any miscellaneous message or link to the user and when user click on the received link a malware file start downloading in the background and that file is ransomware. What this file does is that it converts the user's data like their photos videos their documents and many more data by attacking the system's security system. It stops user to access his /her own data and lock the data permanently and to get back the access for users own data user have to ask the hacker for the key to unlock or get the access of data back. It sounds funny that you have to pay money to access your own data after attacked by such kind of threats.[11,12] Attacker attacks on the user's side to by attacks like phishing, PHP etc. by a mail and when all data get encrypted then the attacker the user for money for the key and when attacker receives the money then he gives the user the decryption code or key. Ransomware is classified into 2 types.

Methodology

- **Working_Method** Ransomware attacks your computer from different networks or in varieties of ways, among all the ways or path there is a most popular way which is downloads an attached file through a spam mail.[9] The attached file after receiving downloaded then it launches itself in the background to attacks your system's security.[10] Including some other methods like downloading some software from non-trustable

sites from browser or by clicking on a malvitsing advertisement leads to download such kind of files looking on the additional methods like getting self-copied from chat messages or by removable disks etc. In general, this malicious file introduced by a no trustable website in an executable format in your computer and that can be in different file formats like .zip and others. Or this type of file can be also be received by fax or via any attachment.[13] After the file gets downloaded it starts encrypting your data and adds its own extension to your file to lock them and make them inaccessible.[14] More complicated software start working without accepting the command by the user that's how it affect your sophisticated software. It's also called drive-by as per attacks.[15]

- Ransomware and its Statistics

Table 1.Statistics Data Report

S.No	Statistics
1	A survey report by FBI was that there are 4,000 ransom ware attacks launched every day. Every 40 seconds attack is launched.
2	The WanaCryptor incident in May is estimated to have infected over two-lac systems in seventy countries in just a few days.
3	Pundits estimate that the payout to ransomware pirates for 2017 eclipsed $3 billion.
4	More than 97% of phishing emails sent in 2016 contained ransomware
5	Ransome ware hit the 60% program.
6	Causing massive disruption, 63% said their system was shut down for more than a day.
7	IBM-X coz the done 70%.
8	In the report of computer ransomware was 40% approximately.
9	Only 4% of organizations feel "very confident" in their ability to stop ransomware.
10	According to CBR Online 28% of companies find out the lost listed into the list.

- **Shielding from Ransomware** Whether you need to know how defend against Crypto Locker or any of the other 4,000 daily attacks; the first component of the solution is to warn co-workers against downloading suspicious file attachments.[11] They won't prevent all attacks, but it will help. It is also critical to ensure that your servers are being patched regularly, as many security gaps that ransomware hackers take advantage of are often protected in the latest Microsoft patches.[12-13] Failing to stay up to date can cause major issues down the line. No matter what, you have to prepare to be hit. So it's critical you not only have backups, but secure, tested backups and a well-documented, secure disaster recovery plan if the attack is pervasive enough. On the data protection side of things, keep these 5 components in mind. Use backup for the Follow the 3-2-1 rule.[14] Three copies of your data, 2 different types of media and 1 version stored off-site. If you do get hit by ransomware, you'll have an easy escape. You can even consider keeping a backup offline (on tape or rotational media), but recovery times are longer from offline backups, and offline backups are more difficult to test.

Secure

Ransomware mainly targets Windows OS. As backup arrangements can necessitate abundant role-based examples for unified organization, data measure, reportage, exploration and analytics, safeguarding all those machineries can be multifaceted. Consider fastening them down to do only what they are compulsory, and nonentity more.[14] Innovative solutions grounded on integrated backup appliances characteristically remove that difficulty and come toughened out of the place of work. So, safekeeping can be far modest in individuals' newer architectures.

Test

Test the feasibility of your holdup and tragedy retrieval tactic regularly. A ration of issues can affect retrieval, as well as backups of technologies that formerly include ransomware. Test mechanization is fetching a tendency in the data management and data protection manufacturing.[15] It is significant those topographies are cast-off extra as security pressures become extra impactful to IT.

Detect

Primary ransomware detection incomes previous recovery.[8] Supplementary holdup sellers are preliminary to usage prognostic analytics and machine learning to classify possible attacks and attentive managers of uneven differences of data as holdups are swallowed.[9]

Instant_Recovery

If you have efficiently sponsored up your data and verified its mend ability you will be prepared to roll back your system to a innocuous reinstate point and circumvent downtime, data failure and income loss.[10] Ransomware occurrences have been violent. If you have not been criticized yet, it's not a substance of it, but when be equipped with unitrends thorough line of protection.[11-13]

Conclusion

Ransomware is very hazardous software for our system. To defend our personal data or any business-related data to safe our data we should keep taking backup our data time

to time. We should keep up to date our antivirus so it can detect such unwanted files and delete them to protect our computer. It is hard to be infected by a ransomware. The different strains of ransomware could do a lot of things to your computer, from locking the screen to encrypting the files. Which is why it's important to know how to identify ransomware and learn on how to properly address the ransomware issue? In order to protect your computer, it is better to have a regular backup and install legitimate security software.[14,15]

Future_Goals

Yet there is no permanent technique has developed till now to protect our computers and our data. So in future we should create an algorithm or technique which can detect such kind of malicious program or files to prevent our computer from such attacks.

References

1. Aidan JS, Verma HK, Awasthi LK. Comprehensive Survey on Petya Ransomware Attack. International Conference on Next Generation Computing and Information Systems (ICNGCIS), Jammu, 2017; 122-125.
2. Ko JJJD, Kim SC, Kwak J. Real Time Android Ransomware Detection by Analyzed Android Applications. International Conference on Electronics, Information, and Communication (ICEIC), Auckland, New Zealand, 2019; 1-5.
3. Almashhadani AO, Kaiiali MSS, Kane OP. A Multi-Classifier Network-Based Crypto Ransomware Detection System: A Case Study of Locky Ransomware. *IEEE Access* 2019; 7: 47053-47067.
4. Agrawal R, Stokes JW, Selvaraj K et al. Attention in Recurrent Neural Networks for Ransomware Detection," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Brighton, United Kingdom, 2019; 3222-3226.
5. Sheen S, Yadav A. Ransomware detection by mining API call usage," 2018 International Conference on Advances in Computing. *Communications and Informatics (ICACCI), Bangalore,* 2018; 983-987.
6. Naik N, Jenkins P, Savage N et al. Cyberthreat Hunting - Part 2: Tracking Ransomware Threat Actors using Fuzzy Hashing and Fuzzy C-Means Clustering," 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, LA, USA, 2019; 1-6.
7. Kara I, Aydos M. Static and Dynamic Analysis of Third Generation Cerber Ransomware," 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), ANKARA, Turkey, 2018; 12-17
8. Saxena S, Soni HK. Strategies for Ransomware Removal and Prevention. 2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2018; 1-4.
9. Naik N, Jenkins P, Savage N et al. Cyberthreat Hunting - Part 1: Triaging Ransomware using Fuzzy Hashing, Import Hashing and YARA Rules. 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, LA, USA, 2019; 1-6.
10. Butt UJ, Abbod M, Lors A et al. Ransomware Threat and its Impact on SCADA," 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, United Kingdom, 2019; 205-212.
11. Ferreira A. Why Ransomware Needs A Human Touch," 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, 2018; 1-5.
12. Aidan JS, Zeenia , Garg U. Advanced Petya Ransomware and Mitigation Strategies. 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC), Jalandhar, India, 2018; 23-28.
13. Lokuketagoda B, Weerakoon MP, Kuruppu UM et al. R - Killer: An Email Based Ransomware Protection Tool," 2018 13th International Conference on Computer Science & Education (ICCSE), Colombo, 2018; 1-7.
14. Butt UJ, Abbod M, Lors A et al. Ransomware Threat and its Impact on SCADA," 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), London, United Kingdom, 2019; 205-212.
15. Naik N, Jenkins P, Savage N et al. Cyberthreat Hunting Part 1: Triaging Ransomware using Fuzzy Hashing, Import Hashing and YARA Rules. 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), New Orleans, LA, USA, 2019; 1-6.