



Institutional Sign In

All



ADVANCED SEARCH

Conferences > 2020 2nd International Confer...

Evolution, Mitigation, and Prevention of Ransomware

Publisher: IEEE

Cite This

Cite This

PDF

Ikra Afzal Chesti; Mamoon Humayun; Najm Us Sama; NZ Jhanjhi All Authors

Export to Collabratec

Alerts

Manage Content Alerts

Add to Citation Alerts

More Like This

Knowing the ransomware and building defense against it - specific to healthcare institutes

2017 Third International Conference on Mobile and Secure Services (MobiSecServ) Published: 2017

Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing

2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS) Published: 2016

Show More

Top Organizations with Patents on Technologies Mentioned in This Article

Abstract

Document Sections

- I. Introduction
- II. The Ransomware Timeline
- III. More than Software Is Required
- IV. To Pay or Pay Not
- V. Data on Infection

Show Full Outline ▾

Authors

Figures

References

Keywords

More Like This

Downl

PDF

Abstract: Tremendous growth of ransom malware demands valuable security methods to protect individuals and organizations. Ransomware or ransom malware is a type of malware that res... **View more**

Metadata**Abstract:**

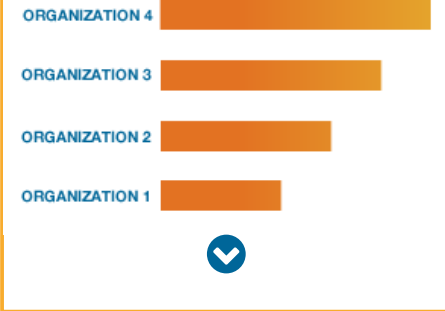
Tremendous growth of ransom malware demands valuable security methods to protect individuals and organizations. Ransomware or ransom malware is a type of malware that restricts users from accessing their files or system and demands a ransom payment to get back access to files. The hacked files are encrypted and asked for payment to decrypt and redeliver the files back to the user. To regain access back to hacked files one has to make digital payment. Ransomware of this type is dangerous as it hacks all the files and fails all the security methods available on the system also the possibility for retrieving your file is zero percent. Even if the payment is done still one cannot be sure that files will be delivered back to the user. The earliest ransomware came into existence in 1980, at that time one has to pay through snail mail. Ransomware is considered as the most widespread malware since 1989 and had caused global financial losses both to individuals and big organizations. Every year this loss is increasing. Therefore, protection of our data from ransomware is necessary. Today, originators of ransomware demand for payment via bitcoins or cryptocurrency. This paper provides the detailed overview about ransomware, its evolution, the reasons for paying or not paying a ransom, the existing approaches to avoid this problem, and the recovery techniques in case of infection.

Published in: 2020 2nd International Conference on Computer and Information Sciences (ICCIS)

Date of Conference: 13-15 Oct. 2020

DOI: 10.1109/ICCIS49240.2020.9257708

Publisher: IEEE



Date Added to IEEE Xplore: 24 November
2020

Conference Location: Sakaka, Saudi
Arabia, Saudi Arabia

ISBN Information:
Citation Map

1.A. Muhammad and A.S. Ejjyime, "Analysis of Ransomware Origin Threats and Economic Lost on Victims", *International Journal of Pure and Applied Sciences*, 2017.

Show Context Google Scholar

2.S. Maniath, P. Poornachandran and V. Sujadevi, "Survey on Prevention Mitigation and Containment of Ransomware Attacks" in Book Survey on Prevention Mitigation and Containment of Ransomware Attacks, Springer, pp. 39-52, 2018.

Show Context Google Scholar

3.D. Sgandurra, L. Munoz-Gonzalez, R. Mohsen and E.C. Lupu, Automated dynamic analysis of ransomware: Benefits limitations and use for detection, 2016.

Show Context Google Scholar

4.S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm", *Computers*, vol. 8, no. 4, pp. 79, 2019.

Show Context CrossRef Google Scholar

5.A.L.Y. Ren, C.T. Liang, S.N.B. ImJun Hyug and N. Jhanjhi, "A Three-Level Ransomware Detection and Prevention Mechanism", *Eai Endorsed Transactions on Energy Web*, 2019.

Show Context Google Scholar

6.R. Richardson and M.M. North, "Ransomware: Evolution mitigation and prevention", *International Management Review*, vol. 13, no. 1, pp. 10, 2017.

Show Context Google Scholar

7.M.H.U. Salvi and M.R.V. Kerkar, "Ransomware: A cyber extortion", *Asian Journal For*

Convergence In Technology (AJCT), 2 2016.

[Show Context](#) [Google Scholar](#)

8.N. Hampton and Z.A. Baig, Ransomware: Emergence of the cyber-extortion menace, 2015.

[Show Context](#) [Google Scholar](#)

9.A. Mauraya, N. Kumar, A. Agrawal and R. Khan, "Ransomware: Evolution target and safety measures", *International Journal of Computer Sciences and Engineering*, vol. 6, no. 1, pp. 80-85, 2017.

[Show Context](#) [Google Scholar](#)

10.B. Amro, "Malware detection techniques for mobile devices", *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, vol. 2017, no. 7.

[Show Context](#) [Google Scholar](#)

11.M. Ameer, S. Murtaza and M. Aleem, "A Study of Android-based Ransomware: Discovery Methods and Impacts", *Journal of Information Assurance & Security*, vol. 13, no. 3, 2018.

[Show Context](#) [Google Scholar](#)

12.P. Zavarsky and D. Lindskog, "Experimental analysis of ransomware on windows and android platforms: Evolution and characterization", *Procedia Computer Science*, vol. 94, pp. 465-472, 2016.

[Show Context](#) [Google Scholar](#)

13.D. Rendell, "Understanding the evolution of malware", *Computer Fraud & Security*, vol. 2019, no. 1, pp. 17-19, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

14. *System and Method for Protecting Information from Unauthorized Access*, October 2018.

[Show Context](#) [Google Scholar](#)

15.M. Karami and D. McCoy, "Understanding the emerging threat of ddos-as-a-service" in Book Understanding the emerging threat of ddos-as-a-service, 2013.

[Show Context](#) [Google Scholar](#)

16.K. Cabaj, P. Gawkowski, K. Grochowski and D. Osojca, "Network activity analysis of CryptoWall ransomware", *Przegląd Elektrotechniczny*, vol. 91, no. 11, pp. 201-204, 2015.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

17. Jason Cameron Bays, *Reactions To Ransomware Variants Among Internet Users: Measuring Payment Evocation*, 2019.

[Show Context](#) [Google Scholar](#)

18.J. Mitchell, Ransomware Characteristics by Country, 2018.

[Google Scholar](#)

19.N. Scaife, P. Traynor and K. Butler, "Making sense of the ransomware mess (and planning a sensible path forward)", *IEEE Potentials*, vol. 36, no. 6, pp. 28-31, 2017.

[View Article](#) [Full Text: PDF \(1882KB\)](#) [Google Scholar](#)

20.N. Roberts, "Ransomware: an evolving threat", *Utica College*, 2018.

[Google Scholar](#)

21.K. Jochem, LockerGoga. Mysterious and Dangerous. Part One.

[Google Scholar](#)

22.U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal and A. Kumar, Ransomware Threat and its Impact on SCADA, 2019.

[Show Context](#) [View Article](#) [Full Text: PDF \(294KB\)](#) [Google Scholar](#)

23.J.C. Sipior, J. Bierstaker, P. Borchardt and B.T. Ward, "A Ransomware Case for Use in the Classroom", *Communications of the Association for Information Systems*, vol. 43, no. 1, pp. 32, 2018.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

24.E. Cartwright, J. Hernandez Castro and A. Cartwright, "To pay or not: game theoretic models of ransomware", *Journal of Cybersecurity*, vol. 5, no. 1, pp. tyz009, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

25.G. Hull, H. John and B. Arief, "Ransomware deployment methods and analysis: views from a predictive model and human responses", *Crime Science*, vol. 8, no. 1, pp. 2, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

26.H. Gupta and M. Singh, "Cyber Threat Analysis of Consumer Devices" in Book *Cyber Threat Analysis of Consumer Devices*, Springer, pp. 32-45, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

27.B. Schneier, *Click here to kill everybody: Security and survival in a hyper-connected world*, WW Norton & Company, 2018.

[Show Context](#) [Google Scholar](#)

28.T. Anjana, "Discussion On Ransomware Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks", *International Journal for Research Trends and Innovation*, no. 2, pp. 310-314, 2017.

[Show Context](#) [Google Scholar](#)

29.J.E. Thomas, *Using Digital Forensic Techniques to Investigate and Detect Ransomware Infection*, 2018.

[Show Context](#) [Google Scholar](#)

30.R. Brewer, "Ransomware attacks: detection prevention and cure", *Network Security*,

no. 9, pp. 5-9, 2016.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

31.Y. Klijnsma, "The history of Cryptowall: a large scale cryptographic ransomware threat" in Book The history of Cryptowall: a large scale cryptographic ransomware threat, 2019.

[Show Context](#) [Google Scholar](#)

32.S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Ransomware threat and detection techniques: A review", *Int. J. Computer Science and Network Security*, vol. 19, no. 2, pp. 136, 2019.

[Show Context](#) [Google Scholar](#)

33.M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb and S. Mahmood, "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study", *Arabian Journal for Science and Engineering*, pp. 1-19, 2020.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

34.S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach", *Int. J. Eng. Res. Technol*, vol. 12, no. 1, pp. 9-16, 2019.

[Show Context](#) [Google Scholar](#)

Contents

I. Introduction

Ransomware is a particularly malicious strain of malware that has become enormously prevalent and is proving to be especially damaging to organizations and individuals alike [1]. Ransomware can attack hardware of the victim by locking their screens thereby preventing users from accessing their system and demanding a ransom payment to get access back to their hardware. It can also hack the user files using

encryption and demanding ransom payment from the user to redeliver the files [2]. It can also attack mobile devices by altering the PIN of the device and demands a ransom payment to get the new pin. The ransom payment is usually done in bitcoins or crypto currency. Ransomware is immensely increasing business. The computer security company Symantec assesses that ransomware obtains under duress millions of currency from targets each year. Symantec also reports that there is no guarantee that an encrypted file will be delivered back to the targeted user in case of ransom payment is done[1]. Based on their behavior ransomware is divided into two basic categories [3] as shown in the below Fig. 1. Fig. 1.

Types of ransomware

Authors



Figures



References



Citation Map

1.A. Muhammad and A.S. Ejyime, "Analysis of Ransomware Origin Threats and Economic Lost on Victims", *International Journal of Pure and Applied Sciences*, 2017.

Show Context Google Scholar

2.S. Maniath, P. Poornachandran and V. Sujadevi, "Survey on Prevention Mitigation and Containment of Ransomware Attacks" in Book Survey on Prevention Mitigation and Containment of Ransomware Attacks, Springer, pp. 39-52, 2018.

Show Context Google Scholar

3.D. Sgandurra, L. Munoz-Gonzalez, R. Mohsen and E.C. Lupu, Automated dynamic analysis of ransomware: Benefits limitations and use for detection, 2016.

Show Context [Google Scholar](#)

4.S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Prevention of Crypto-Ransomware Using a Pre-Encryption Detection Algorithm", *Computers*, vol. 8, no. 4, pp. 79, 2019.

Show Context [CrossRef](#) [Google Scholar](#)

5.A.L.Y. Ren, C.T. Liang, S.N.B. ImJun Hyug and N. Jhanjhi, "A Three-Level Ransomware Detection and Prevention Mechanism", *Eai Endorsed Transactions on Energy Web*, 2019.

Show Context [Google Scholar](#)

6.R. Richardson and M.M. North, "Ransomware: Evolution mitigation and prevention", *International Management Review*, vol. 13, no. 1, pp. 10, 2017.

Show Context [Google Scholar](#)

7.M.H.U. Salvi and M.R.V. Kerkar, "Ransomware: A cyber extortion", *Asian Journal For Convergence In Technology (AJCT)*, 2 2016.

Show Context [Google Scholar](#)

8.N. Hampton and Z.A. Baig, Ransomware: Emergence of the cyber-extortion menace, 2015.

Show Context [Google Scholar](#)

9.A. Mauraya, N. Kumar, A. Agrawal and R. Khan, "Ransomware: Evolution target and safety measures", *International Journal of Computer Sciences and Engineering*, vol. 6, no. 1, pp. 80-85, 2017.

Show Context [Google Scholar](#)

10.B. Amro, "Malware detection techniques for mobile devices", *International Journal of Mobile Network Communications & Telematics (IJMNCT)*, vol. 2017, no. 7.

[Show Context](#) [Google Scholar](#)

11.M. Ameer, S. Murtaza and M. Aleem, "A Study of Android-based Ransomware: Discovery Methods and Impacts", *Journal of Information Assurance & Security*, vol. 13, no. 3, 2018.

[Show Context](#) [Google Scholar](#)

12.P. Zavarisky and D. Lindskog, "Experimental analysis of ransomware on windows and android platforms: Evolution and characterization", *Procedia Computer Science*, vol. 94, pp. 465-472, 2016.

[Show Context](#) [Google Scholar](#)

13.D. Rendell, "Understanding the evolution of malware", *Computer Fraud & Security*, vol. 2019, no. 1, pp. 17-19, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

14.*System and Method for Protecting Information from Unauthorized Access*, October 2018.

[Show Context](#) [Google Scholar](#)

15.M. Karami and D. McCoy, "Understanding the emerging threat of ddos-as-a-service" in Book Understanding the emerging threat of ddos-as-a-service, 2013.

[Show Context](#) [Google Scholar](#)

16.K. Cabaj, P. Gawkowski, K. Grochowski and D. Osojca, "Network activity analysis of CryptoWall ransomware", *Przegląd Elektrotechniczny*, vol. 91, no. 11, pp. 201-204, 2015.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

17.Jason Cameron Bays, *Reactions To Ransomware Variants Among Internet Users: Measuring Payment Evocation*, 2019.

[Show Context](#) [Google Scholar](#)

18.J. Mitchell, Ransomware Characteristics by Country, 2018.

[Google Scholar](#)

19.N. Scaife, P. Traynor and K. Butler, "Making sense of the ransomware mess (and planning a sensible path forward)", *IEEE Potentials*, vol. 36, no. 6, pp. 28-31, 2017.

[View Article](#) [Full Text: PDF \(1882KB\)](#) [Google Scholar](#)

20.N. Roberts, "Ransomware: an evolving threat", *Utica College*, 2018.

[Google Scholar](#)

21.K. Jochem, LockerGoga. Mysterious and Dangerous. Part One.

[Google Scholar](#)

22.U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal and A. Kumar, Ransomware Threat and its Impact on SCADA, 2019.

[Show Context](#) [View Article](#) [Full Text: PDF \(294KB\)](#) [Google Scholar](#)

23.J.C. Sipiør, J. Bierstaker, P. Borchardt and B.T. Ward, "A Ransomware Case for Use in the Classroom", *Communications of the Association for Information Systems*, vol. 43, no. 1, pp. 32, 2018.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

24.E. Cartwright, J. Hernandez Castro and A. Cartwright, "To pay or not: game theoretic models of ransomware", *Journal of Cybersecurity*, vol. 5, no. 1, pp. tyz009, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

25.G. Hull, H. John and B. Arief, "Ransomware deployment methods and analysis: views from a predictive model and human responses", *Crime Science*, vol. 8, no. 1, pp. 2, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

26.H. Gupta and M. Singh, "Cyber Threat Analysis of Consumer Devices" in Book Cyber Threat Analysis of Consumer Devices, Springer, pp. 32-45, 2019.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

27.B. Schneier, Click here to kill everybody: Security and survival in a hyper-connected world, WW Norton & Company, 2018.

[Show Context](#) [Google Scholar](#)

28.T. Anjana, "Discussion On Ransomware Wannacry Ransomware and Cloud Storage Services Against Ransom Malware Attacks", *International Journal for Research Trends and Innovation*, no. 2, pp. 310-314, 2017.

[Show Context](#) [Google Scholar](#)

29.J.E. Thomas, Using Digital Forensic Techniques to Investigate and Detect Ransomware Infection, 2018.

[Show Context](#) [Google Scholar](#)

30.R. Brewer, "Ransomware attacks: detection prevention and cure", *Network Security*, no. 9, pp. 5-9, 2016.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

31.Y. Klijnsma, "The history of Cryptowall: a large scale cryptographic ransomware threat" in Book The history of Cryptowall: a large scale cryptographic ransomware threat, 2019.

[Show Context](#) [Google Scholar](#)

32.S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "Ransomware threat and detection techniques: A review", *Int. J. Computer Science and Network Security*, vol. 19, no. 2, pp. 136, 2019.

[Show Context](#) [Google Scholar](#)

33.M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb and S. Mahmood, "Cyber

Security Threats and Vulnerabilities: A Systematic Mapping Study", *Arabian Journal for Science and Engineering*, pp. 1-19, 2020.

[Show Context](#) [CrossRef](#) [Google Scholar](#)

34.S. Kok, A. Abdullah, N. Jhanjhi and M. Supramaniam, "A Review of Intrusion Detection System using Machine Learning Approach", *Int. J. Eng. Res. Technol*, vol. 12, no. 1, pp. 9-16, 2019.

[Show Context](#) [Google Scholar](#)

Keywords



IEEE Personal Account

[CHANGE USERNAME/PASSWORD](#)

Purchase Details

[PAYMENT OPTIONS](#)

[VIEW PURCHASED DOCUMENTS](#)

Profile Information

[COMMUNICATIONS PREFERENCES](#)

[PROFESSION AND EDUCATION](#)

[TECHNICAL INTERESTS](#)

Need Help?

[US & CANADA: +1 800 678 4333](#)

[WORLDWIDE: +1 732 981 0060](#)

[CONTACT & SUPPORT](#)

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE Account

» [Change Username/Password](#)

» [Update Address](#)

Purchase Details

» [Payment Options](#)

» [Order History](#)

» [View Purchased Documents](#)

Profile Information

» [Communications Preferences](#)

» [Profession and Education](#)

» [Technical Interests](#)

Need Help?

» **US & Canada:** +1 800 678 4333

» **Worldwide:** +1 732 981 0060

» [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.