SHUBHAM SHARMA

Phone: +91 8894927462
Email: jonusharma59@gmail.com
LinkedIn: https://www.linkedin.com/in/shubham-sharma-1a809b125/
Address: 31/1 V.P.O Thana Bargran Teh. Baroh Distt. Kangra, HP, India.

CAREER OBJECTIVES :

- To work in a firm with professional work is a driven environment where I can utilize and apply my knowledge and skills which would enable me to grow while fulfilling organizational goals.
- To enhance my innovation skills in a dynamicworkplace.

SPECIALIZATION

- Cyber Security
- Malware Domain.
- The main area of Research is Ransomware.
- The threat, Attack, Prevention, and Cure on Window Platform

ADDITIONAL SKILLS

- Researcher.
- Technical Writer.
- Work with Grammarly, Hemingway, Siteliner, Latex, Wireshark, Nmap, Metasploit.
- Work with HTML, CSS, PHP
- Work and Knowledge of Python

ACHIVMENTS

- Best Coordinated and Organized Events as a Chief Coordinator.
- Best Coordinated and Organized an Outside sports Event Basketball and Kabaddi at Central University of Punjab, Bathinda

LANGUAGE KNOWN

- Hindi, Speak Read Write
- English, Speak Read Write
- Panjabi. Speak.

MY RESEARCH LINKS

- https://www.ijitee.org/wp-content/uploads/papers/v9i4/D2035029420.pdf
- https://link.springer.com/article/10.1007/s40031-020-00499-w

STREAM

- Computer Science & Engineering (Diploma, B.Tech)
- Computer Science & Technology Cyber Security (M.Tech)

MY RESEARCH PUBLICATION

- Sharma S., Singh S. (2020). Ransomware Threat, Attack, Prevention and Cure on Window Platform. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(4).
- Sharma, S., & Singh, S. (2020). Texture-Based Automated Classification of Ransomware. Journal of The Institution of Engineers (India): Series B, 1-12.
- Malware Classification, Analysis, Tools, and Techniques on Windows platform. [In communication]

ACADEMIC BACKGROUND

- Masters of Technology (M.Tech.) in Computer Science and Technology with specialization in Cyber Security from the Central University of Punjab, Bathinda. (2018 – 2020)
- Bachelor of Technology Degree (B.Tech.) in Computer Science and Engineering from Himachal Pradesh Technical University, Hamirpur. (2014 –2017)
- Three Years Diploma in Computer Science and Engineering. from Himachal Pradesh Takniki Shiksha Board, Dharamshala.(2010 – 2013)

PERSONALITY TRAITS

- Analytical mind and Skill, Flexible.
- Trained or educated as a Researcher or any relevant area and field.
- Confidence with dealing with members of the public.
- Problem-solving skills,
- Good interpersonal and communication skills
- Writing detailed reports which focus upon the findings of the research. The ability to work both as part of a team, as a Team Leader and on an individual basis too.

WORK EXPERINECE

Total Experience: (2 Year)

- Cyber Security Researcher.
- Research paper & research document reviewer and, Counselor.
- Researcher, Technical Writer, Research Writing & Proposal, Technical documentation Management, Reviewer of Technical Documents & paper, Excellent Technical & Research writing skills, Technical Analysis, Technical Editing, System Administration.
- Proficiency in MS Office.
- MySQL, Php, CSS, HTML (6 months)
- Hemingway, Siteliner, Latex, Python,

WORKED AS ORGANIZER

- Coordinated and Organized a Workshop on “Cyber Security & Network Intelligence” (March-2015).
- Coordinated and Organized a 3 days Annual Fest as a Chief Coordinator. (March-2017).

AWARDS

- 2 times LAN gaming runner-up Bronze Medal in (Feb-2019 & 2020).
- 3 times Kabaddi runner up Silver Medal in (Feb-2012, 2017 & 2020).
- 2 times Basketball Winner Gold Medal in (Feb-2019 & 2020).
- Best Coordinator and Organized Events as a Chief Coordinator. (March-2015,2016 & 2017).
- Best Organizer & Anchor trophy in (Feb-2015, 2017 &2020).
- Best Organizer Trophy for outside Sports in (Feb-2020).

International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-9 Issue-4, February 2020

Ransomware Threat, Attack, Prevention and Cure on Window Platform

Shubham Sharma, Satwinder Singh

Abstract: *With the advancement of digitization in every domain, the dependency of individuals on these digitized softwares has also increased. Although these softwares can perform storage, transfer, and security of digital media easily, the threat of hardware/software failure, data tapping and breaching data has always been there. Most of these threats have been introduced by the development of malicious softwares that can provide unauthorized access of machine's data. This malicious software was termed as malware. The development of any antimalware software to prevent the machine from malware triggers the attacker to generate new malicious operations to infect the machine. Ransomware is, however, a novel and one of the dangerous malware invented recently that restricts the user from accessing their system by locking the operating system files using strong encryption algorithms in the system unless and until a ransom is paid. Seeing the emergence of this ransomware threat and also the increasing usage of digital media, many techniques have been developed to detect the presence of different types of ransomware in different environments. Since the importance of developing techniques to prevent our machines from such attacks is increasing substantially, further research in the respective domain require thorough analysis of all the techniques that have been developed in this regard. This paper introduces the concept of ransomware and how it has been evolved. Along with various methods of handling the ransomware, thorough analysis of techniques that have been developed until now for the prevention and detection of different ransomwares is also performed. The analysis shows that there has been a big improvement in coding techniques utilized by ransomware which will eventually turn out a good detection system that considerably reduces the quantity of victim information loss.*

Keywords: Ransomware attack, Security, Detection, Prevention and Cure

I. INTRODUCTION

Malware is a malicious software package or computer code which can infect the computer to destroy or lock your data. Ransomware is a specific type of malware [1] that restricts the access of machine's data to its own user and then demands a ransom to release the restriction. The main difference between ransomware and malware is that, while a malware tries to remain hidden in your pc, laptop, computer just like a hidden file and do their work at backend without knowing the user or client and undetectable to the users, whereas ransomware upon encrypting your whole file which is in system and your PC, laptop and computer too is compromised, and tells the user of its presence [2]. However, the restriction or locking is performed using the encryption mechanism which encrypts the necessary information of the machine, computer, tablets or any kind of other electronic device. However, these encryption mechanisms were primarily developed to encrypt the user information for system security.

Ransomware attacks are rapidly growing in popularity and cybercriminals are earning to a great extent using these attacks. Businesses and individuals worldwide are currently under attack by ransomware [3]. According to the annual cybercrime report, businesses were targeted after every 14 seconds with ransomware in 2019 and this estimate will rise in 2021 by 11 seconds [4]. Usually, the amount of money that the victim pays as a ransom to decrypt or save their data from any kind of stealing canbe$300 to $700 or some time it can be increased $10,000 to $30,000 [5]. This payment is commonly requested in Bitcoin (a cryptocurrency payment system) or any other alternative invisible currency; which mostly depends on the location, local language, the language you are familiar with and your preference and suitability for traveling. However, sometimes even after paying the whole ransom, cybercriminals can break their promises of releasing the original version of data and disappear, leading to bigger losses. These types of attacks happen because of a lack of cyber security knowledge and consciousness of backing up important files by normal users. However, Ransomware-as-a-Service (RaaS) has emerged recently as the worst type of attack that allows nontechnical criminals to make attacks at a very low cost [6].

Ransomware usually operates by locking the desktop of the victim to render the system inaccessible to the user, or by encrypting, overwriting, or deleting the user's files from their storage drive. This is performed by first transferring the parent file of ransomware to perform all operations to the victim's computer either by using e-mail or online advertisements or some external drives. Some commonest ways employed by cybercriminals to unfold ransomware are Spam or fake email campaigns that contain malicious links or attachments; web traffic redirects to compromised websites; Drive-by downloads, infected softwares, contaminated external storage devices like USB drive, memory card, hard drive etc. Sometimes, attacks also use remote desktop protocols like approaches that don't have confidence in any kind of user interaction. This parent file first creates a connection with the C&C server which provides keys for encrypting the stored data of the victim's computer. Once it receives the encryption key, it looks for specific files and folders to encrypt.

Revised Manuscript Received on February 06, 2020.

* Correspondence Author

Shubham Sharma*, Department of Computer Science & Technology (Cyber Security), Central University of Punjab, Bathinda, India. Email: jonusharma59@gmail.com

Satwinder Singh, Department of Computer Science & Technology (Cyber Security), Central University of Punjab, Bathinda, India. Email: satwinder.singh@cup.edu.in

Retrieval Number: D2035029420/2020©BEIESP
DOI: 10.35940/ijitee.D2035.029420

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

J. Inst. Eng. India Ser. B
https://doi.org/10.1007/s40031-020-00499-w

ORIGINAL CONTRIBUTION

Texture-Based Automated Classification of Ransomware

Shubham Sharma[1] · Satwinder Singh[1]

Received: 28 May 2020 / Accepted: 2 October 2020

Abstract Reliance on digital data has been increased with easy availability of user friendly software to store and manipulate data with much less effort. This digital data can become very hard to maintain if no security mechanisms has been implemented to protect it from unauthorized access. Even the whole machine is on the verge of being infected if not being secured. Data and the whole machine can be easily infected or lost if any malicious operation is being executed on the machine by some unauthorized user. This is possible, by injecting some malicious operations in the byte code of the source file that is being transferred into the machine. These malicious operations, according to the harm they caused, have been categorized into different categories of malware. Among various malwares, Ransomware is a harmful malware that can restrict the user's access to his own computer's data, using encryption mechanism. Until the required ransom is not paid the decryption key is not provided. Unlike other techniques discussed in the literature, the technique proposed in this paper analyse irregularity in the texture of the image. Proposed technique used local binary pattern generated from the file to be analysed which has the ability to detect the same immediately on the transfer of file into the victim's computer before its execution. This analysis detects the injection of some abnormal operations inserted into the byte code of the respective file to make the ransomware execute. The technique was tested on 1738 window based and 179 android based different ransomware and benign samples which generated an accuracy of 87.9% at maximum.

Keywords Ransomeware · Convolutional Neural Network · SVM · LBP · Texture

Introduction

The advancement in computer and internet technology has ushered in this information age. As computers have become increasingly powerful and easily accessible, our reliance on them has also grown immensely. Nowadays, IoT devices such as smartphones, smart TV, etc., are no longer limited for phone calling or message transmission but are also being used for social networking, web browsing, meeting scheduling, file downloading, gaming and online bank transaction in just a single click. To certain extent, for all of the IoT devices which are connected with the internet either directly or indirectly over the network through any kind of service provider, confidential information of users such as contacts, online banking credential details, bank account number, credit card number, private pictures are kept in these devices. There are various types of operating systems such as Windows, Mac, iOS, Android, etc. And every IoT device can have its own running environment while using internet over the network. This has become one of the main targets for attackers to escalate any kind of malware. To prevent a full access of your organization's ability to confront to ransomware attacks, specialized users, applications, and infrastructure are utilized, and tailored recommendations are received for attractive security.

Criminals ruthlessly target organizations, demanding ransoms in any form to recover stolen information and stop

✉ Shubham Sharma
jonusharma59@gmail.com

Satwinder Singh
satwindercse@gmail.com

[1] Central University of Punjab, Bathinda, Punjab, India

Published online: 31 October 2020

Shubham Sharma.