iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Glimpse of Ransomware

Faraah M. Dabhoiwala[1]
[1]Information Technology, Vadodara Institute of Engineering

Abstract; Ransomware has become one of the most widespread and damaging threats that internet users face. So basically it is a data kidnapper. It kidnaps your data and demands money from you. In this paper I have put down regarding ransomware and how user becomes victim of ransomware.
Keywords —ransomware, security, internet, virus, malware.

I. INTRODUCTION

Ransomware is one type of malware that encrypts the files on the victim machine using strong cryptography. After that it notifies the user that their files were encrypted and demands money which is known as ransom for decryption. The decryption key is stored on the attacker's server so victims cannot recover their files without paying the amount.

A. Ransomware is rather different from traditional malware:

1) It does not steal victim's information instead it makes it impossible to access your information.
2) It does not try to remain stealthy after files are encrypted because detection would not restore the lost data.
3) It is easy to develop a ransomware as there are a number of well-documented crypto-libraries. [1]

II. A MAJOR DIFFERENCE BETWEEN MALWARE AND RANDSOMWARE

Malware is a program that installs itself on a computer and runs in the background, hiding its presence and stealing passwords, credit card, and other valuable information. User is unaware of the activities of malware. On the other hand, ransomware does not try to hide it. The point at which it encrypts the data, it informs the user of its presence.

A. Cheating with Ransomware

If you try to interfere with the ransomware, for example, entering a wrong payment info, usually results in the remaining time being halved. On the other hand, not paying the ransom within the due time can lead to theransom amount being doubled with a new deadline.
Depending upon the particular version and type of the ransomware, there might beanother pop-up screen showing the list of encrypted files. Users can verify that the filesstill exist, but the contents are merely unreadable garbage. Files are encrypted usingasymmetric (RSA) encryption, where the key used for encryption cannot be used todecrypt the data. RSA algorithm uses two different keys, one (public) for encryption ofdata and one (private) for decryption. Once the data is encrypted, it is generally unrecoverable unless the user decides to pay the ransom. There is no guarantee that once you pay the ransome you will get your data back.Among many other, the most common mode of ransom payment is Bitcoins.
Bitcoin is a digital currency that has been designed to do anonymous online transactions. From the transaction itself, it is impossible to trace the beneficiary. This revolutionary e-currency is specially being used to carry out crimes. [3]

B. Ransomware Attacks

Ransomware prevents the user from using their computer or accessing data.It holds the user's computer and files for ransom.

C. Types Of Ransomware

1) *Locker Ransomware:* Locker ransomware is spread through social engineering and phishing campaigns. According to Symantec, about 36% of binary-based ransomware detected in 2014-2015 was locker ransomware. Computer lockers restrict user access to infected systems by either denying access to the user interface or by restricting the availability of computing resources. Certain capabilities, such as numeric keyboard functionality, might remain unlocked while the rest of the keys and the mouse are locked. This design increases user frustration while restricting user action to following the attacker's instructions. Locker ransomware does not infect files and systems unaffected but it only restricts access to the interface. Thisdesign also means that locker ransomware can often be removed easily by restoring the system toa restore point or by

deploying a commercial removal tool.

2) *Crypto Ransomware:* Crypto ransomware done not lock the user interface but it encrypts the file and data. So the user can interact with the system but he/she cannot access the files. So it leaves the files infected.

III. TARGET SYSTEMS

A. *Personal computers*

Personal computers are most commonly targeted by ransomware because theyare numerous and easily compromised. Users take least care of cyber hygiene and that is the main reason that they are easily caught up by the ransomware. Users get infected generally by visiting social networking websites. Generally Windows operating system is targeted by ransomware but there are other ransomware which target Linux, Mac and Android too.

B. *Mobile devices*

Now a days, mobiles are used by everyone. People keep on visiting various sites and downloading various applicationsunnecessarily which causes much higher risk of infecting the mobiles with ransomware.

C. *Servers*

An organization's servers and databases store all of their critical information. The secured information is stored on the server which should not be accessible to everyone. If the server is attacked by ransomware the highly secured information gets stolen and it may harm the reputation of the organization. So it is very much important to safeguard the servers from ransomware.[2]

IV. BACKUP IS THE BEST OPTION FOR RECOVERY OF DATA

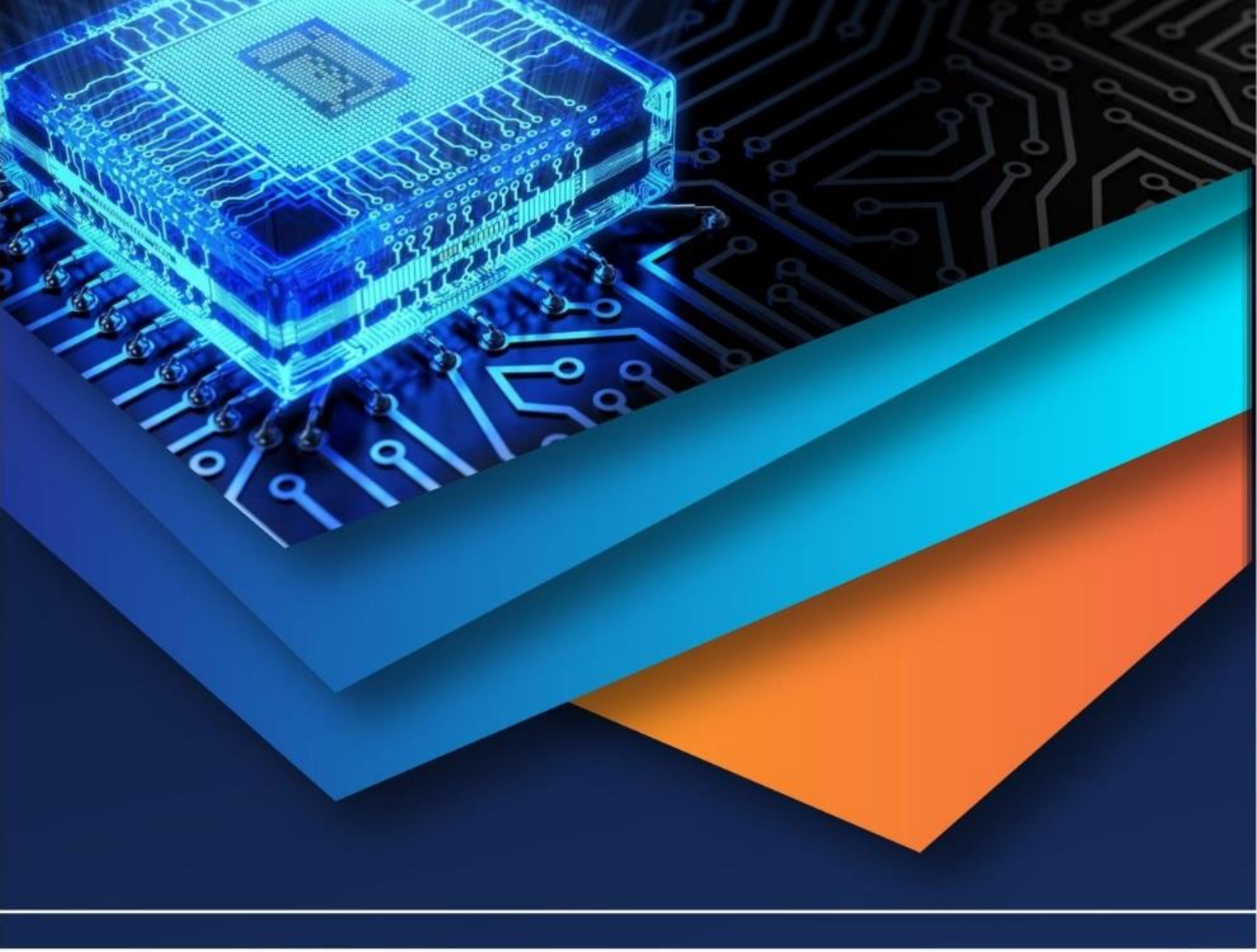
Paying the ransom does not seem to be a proper option because there is no guarantee that the data will be recovered even after paying the ransom. So it is advisable to take backup of the data offline in the computer which is not connected to the internet. Offline backup is required because if the computergoes online then it is possible that ransomware might attack the backup files also.

V. ACKNOWLEDGMENT

I would like to thank my Parents for their endless support and my husband, Mr.Rahil Barafwala for constantly encouraging me to work on research paper and this work is the result of the same.

REFERENCES

[1] Vadim Kotov and Mantej Singh Rajpal, "Understanding Crypto-Ransomware", November 2014.
[2] James Scott and Drew Spaniel, "The ICIT Ransomware Report ", March 2016.
[3] ShafqatMehmood, "Enterprise Survival Guide for Ransomware Attacks", April,2016.
[4] A report on RansomwareA Growing Enterprise Threat.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY