Journal of
Information Security and Technologies

Review Article Open Access

Ransomware: Are We Safe on the Web?

Md Sajjad Hosain*

Independent Researcher and Consultant, Bangladesh

***Corresponding author:** Md Sajjad Hosain, Independent Researcher and Consultant, Bangladesh, Tel: 01842957678, Email: sajjad_hosain@yahoo.com

Received Date: June 13, 2022 **Accepted Date:** June 28, 2022 **Published Date:** June 30, 2022

Citation: Hosain S (2022) Ransomware: Are We Safe on the Web?. J Inf Secur Technol 1: 1-9.

Abstract

Ransomware is a modern type of malware that encrypts the files or folders on a targeted device while the attacker demand for certain amount money (ransom) to be paid. The unknown attacker(s) create(s) a hostage-like situation where the victim (user) is severely threatened with the risk of data loss and forced into a monetary negotiation. This paper makes a simple discussion regarding such a malware and makes a few action recommendations for the general users in order to prevent the possibility of being the victims of ransomware. The paper has avoided the technical terms so that the language can be well-understood by the general users who have medium to least levels of expertise about various malwares. The author hopes that this simple paper can be helpful for the ordinary personal users who can be suddenly affected by the hackers as well as organizational policymakers to take some useful precautionary steps in order to avoid any unforeseen attack from the hackers.

Keywords: Ransomware, Malware, Computer virus, Hackers, Bitcoin, Personal data

Introduction

Due to the recent increased use of Internet and electronic devices, a different form of cyber crime has endangered the ordinary (mainly individual) users by hijacking their files or folders accessing through the web. First of all, those cyber criminals (popularly known as hackers) target a specific personal computer (PC) or laptop by its Internet Protocol (IP) address if it is connected to the Internet. Afterwards, they infect the targeted device by injecting 'Malwares' (malicious or infected software, known as computer virus) to infect a user system from different infection vectors such as browser exploit kits, drive-by freeware apps and malicious email attachments. One of the most common and widely discussed malware is 'Ransomware' that is the core theme of this paper. Finally, those hackers ask the owner of that particular IP for a definite sum of money to be paid and in most cases; they ask the victims to pay the ransom money through bitcoin. The practice has taken its acute stage form particularly after 2010.

Damages made by ransomware include data loss, downtime, lost productivity and disclosure of personal files to additional cyber-attacks [1]. As per industry information, the financial cost of ransomware has raised from USD325 million to USD5 billion, between the year 2015 and 2017 [2]. However, one of the unique features of ransomware is that it is both a virus and a business transaction that even a non-technical person can practice. They can generate and tailor their own version of the virus with the help of Ransomware-as-Service (RaaS) software that enables configuring the transaction particulars of the threat, such as price and payment options, in addition to providing a few automation support to the conciliation process [3,4]. Nonetheless, depending on the kind of file contents, attackers may create a variety of threats such as blackmailing victims, leaking the data publicly and even further consequences (e.g., reputation loss and litigations).

Among different malicious software, ransomware is predominantly attractive from a human factors point of view. Differently from other malware that merely attack a host device, ransomware encrypts data and locks down some parts of or complete device operationally till some payment is made to the unknown attacker. Most frequently, such attackers prefer the payment to be made through bitcoin. An ideal ransomware attack operation requires three core technologies: (1) strong and reversible encryption to lock up files (2) unidentified communication keys and decryption tools and finally, (3) concealing the tracks for the ransom deal [5]

In this simple, non-technical paper, the author has made a general discussion on the issue of ransomware such as definition and how it works. Furthermore, he has made some simple practical recommendations in order to avoid such an attack. This paper is intended to the very simple users who have the least knowledge about software or cyber technology. For due reason, the author has used very simple and universally understandable language throughout the paper.

Ransomware and bitcoin: A general overview

Any program or file that is injurious to a computer (or any other electronic device) is called malware or malicious software. That includes viruses, worms, Trojan horses and spyware. Such malicious programs can carry out a range of malfunctions such as stealing, deleting, modifying, and encrypting. More dangerously, those infected programs can also alter or hijack the core computing functions such as accessing and monitoring users' computer or online actions without their consent and knowledge. There is a variety of a malware which can encrypt the personal files of the users or may lock the computer and prevent the users from accessing it. Based on the capabilities of the ransomware, data might be encrypted in symmetric key (single key), asymmetric key (public key, double key) or combination of both (hybrid key) [6]. After encryption, the data key is sent to the attacker and deleted from the victim's computer. The personal data are encrypted once they are infected with the ransomware and a limited period of time is generally given to the victims to pay an amount of money as ransom. However, there is no guarantee that even after the ransom money is paid to the unknown hacker, the user will get back the key to access his computer and data. The ransomware usually has a high degree of inbuilt capacity to run a 64 bit code from its 32-bit TOR dropper, whereas, a modern malware variants are known to switch the execution context of processor from 32 to 64 bit on a 64 bit environment [7].

The sign of modern ransomware was begun in 2005. Now it is being designed and operated for direct revenue generation from the millions of computer users. The four most common direct revenue generating scams include confusing apps, fake antivirus scams, locker ransomware and crypto ransomware [6]. Such straight revenue generating malware passed through four major turning points in the last decade. Each pivotal point indicates a move from one type of malware to another that has eventually led to ransomware. The top most impacted six countries by all types of ransomware in 2015 are United States, Japan, United Kingdom, Italy, Germany and Russia [6].

The way how the attacker or hacker asks for the ransom money is a way different than those of regular transactions. In case of ransomware, the hacker usually uses a more secure and untraceable transaction system. Presently, in almost all the cases, the hackers ask for the ransomware through bitcoin. Bitcoin is a digital cryptocurrency developed in 2009 by an imaginary creator named Satoshi Nakamoto [8]. It is a decentralized currency that uses peer-to-peer technology, which enables all functions such as currency issuance, transaction processing and verification to be carried out collectively by the same network [9]. Such decentralization renders bitcoin free from Government manipulation or interference, [10]. Bitcoins are created digitally through a "mining" process that requires powerful computers to solve complex algorithms and crunch numbers [11]. Currently, 25 bitcoins are being created in every 10 minutes and is expected to be capped at 21 million in 2140 [12].

An individual can buy bitcoins from online exchanges. Bitcoin transactions are stored in a public ledger known as Blockchain, where money exchange can be seen and recorded by the entire network almost immediately which makes it difficult to identify the owners [7]. Those transactions are not in fact owned by any particular company and are more like email exchanges where no one can block two entities from exchanging emails. Bitcoins are used for sending or receiving money with anyone, anywhere globally at a very small transaction cost. The payments cannot be blocked or frozen. As it is impossible to turn off the entire universal internet, the bitcoin transaction network is apparently unstoppable. Due to such anonymity and lack of tracking sources, the hackers prefer bitcoin as ransom money.

Ransomware: The general types

In general, there are mainly two basic types of ransomware: Locker Ransomware (Computer Locker) which denies access to the computer or mobile device/system and the other one is the Crypto Ramsomware (Data Locker) that prevents access to personal files or data. However, both types of ransomware subsist in present digital lifestyle where the category of malware has been made through the design that prevent and deny access the user to his/her resources: hardware (the device) or software (file or folder). Although, regarding the access to the system or data, they have similar objectives; the operations conducted by each of them are fairly different.

(i) Locker Ransomware (Computer Locker): This type of ransomware is used by the hackers to lock the system and prevent the users from accessing to its resources. With such a locked system, the user can only perform specific limited operations such as typing arithmetic digits for verifying the payments instructed by the hacker. Afterwards, the hacker forces the user by adopting diverse psychological technique in order to pay the ransom. Locker ransomware can co-exist with a variety of systems in different types of operating systems such as Microsoft Windows, Linux, OS X and Android. A few versions of the Locker ransomware for Android Phones and Android Smartwatches can exist and infect a wide variety of users' data as discussed. In such a case, it is not possible for the user to access its settings to delete the malware application. According to the a few samples which have been found from research papers and throughout the Internet search are Lockdroid and SimpLocker [6] that are, in fact, fake applications, and really are ransomware only. Such locker ransomware may possibly grow more and more while the user enters to the Internet, same as an intelligent car that does some of its operation like open/lock doors and turn on/off. Once it is infected, it might be out the of control of the user and the user has to pay the ransom in to unlock it again.

(ii) Crypto Ransomware (Data Locker): With the increased necessity, every PC or other electronic devices are becoming more connected to the Internet and web than ever before. Crypto ransomware or data locker particularly targets the personal data rather than the system itself that can encrypt or lock the data focused on individual files. Such a ransomware uses variety of encryption and cryptography algorithms as defined in design phase of the development.

It is usual and understandable that the users might have vital private information on his/her device such as documents, database, academic researches and projects, valuable personal data like photos and videos of the loved ones etc. After completing the encryption on the infected files on the system, the unknown attacker usually sends a message through the system that can be linked to website or a simple text file containing the instructions regarding later processes of payment; or decryption of some random files as demo [6].

Ransomware: Systems that can be affected

The latest versions of ransomware can affect on or crash different types of systems or devices ranging from personal computer to mobile devices and servers. It is a serious and significant threat to Internet of Things (IoTs) if those (IoTs) are infected by

the malware particularly ransomware. Electronic devices such as domestic appliances like TVs, refrigerators or portable devices like mobile phones, media players, tablets, cameras, routers which contain a lightweight version of operating system such as Linux, might be as well targeted by ransomware.

(i) Personal computers: Most of the updated ransomware are designed to target personal computers that run through Microsoft Windows Operating System, Linux Operating System and OS X Operating System [6]. Among those operating systems, Microsoft Windows is the most vulnerable against malware particularly ransomware. The ransomware may use the Application Programming Interface (API) that exist in the system for encrypting and decrypting of the data. Although, both types of ransomware, the system locker or browser locker and crypto locker which encrypt personal data can exist in personal computer, those ransomware are more destructive for Microsoft Windows operating system but less harmful for other operating systems.

(ii) Mobile devices: Almost every single individual now-a-days uses mobile device such as phones, tablets and notebooks. Those devices are operated by a variety of operating systems where the most famous of them are Android, iOS and Windows. Among all those operating systems, Android has the most users around the globe having more applications in this system than others. In case of iOS, the users who did not jailbreak their phone may enjoy some security protection layer while installing new third party applications. In this regard, Android is weak and more vulnerable to malware. The cyber security analysts have identified a number of ransomware in Android applications that locks the device and ask for money. For instance, Lockdroid and Simplocker are some fake antivirus for found android device which are basically ransomware usually disguised pretending as fake defenders [10].

(iii) Servers or databases: Servers or databases of companies and organizations may contain vital, sensitive and important information such as critical company information, customer details, records and other sensitive information. The cybercriminals who think to target servers for earning money can spread malicious ransomware and force the managements to pay the ransom. It is a significant requirement for organizations to have their own strategies such as plan for disaster recovery and efficient back up. There are a few Internet and network security companies that keeps monitoring on the local networks implemented within an organization. Those companies have their own strategies and plans for keeping the clients' data secure against malware or physical loss, accidental loss, or even from natural disasters such as storm, earthquake and fire. Therefore, it is better for any organization to have contracts with such Internet security companies. They may collect several backups of the files in different locations which can be recovered later.

Cybercriminals who attack servers with ransomware may ask for more money as they are well informed regarding the business that worth more than a normal home user. As the hackers retain the decryption key, there might be no other way in that critical situation as the whole system is down and no one can access the data.

Ransomware: Who are the victims of?

Those unknown hackers who write the malicious code to victimize the users and getting ransom generally do not care who is or will be the victim. One thing is very obvious that anyone who has a digital device might be infected no matter what the device is. It can be virtually anything such as a mobile phone, tablet, laptop, personal computer, server, or even a smartwatch which use lightweight android operating system. If the operations of sending and receiving the decryption key are automated, any device is vulnerable to do the job of an attacker. Such an automated device can well act as a money collecting machine and it is possible.

(i) Private or individual users: Individual users are the most susceptible category to be infected with of malware particularly ransomware. The knowledge and technical expertise of personal users are not usually adequate regarding computer systems, network communication and information security. In most cases, typically they save all their personal data files in their digital devices such as phones, tablets, laptops, or desktops computers that they use in offices, workplaces or homes. They can be the best targets for ransomware by the cybercriminals as easy prey and earn money. Such a ransomeware can be bought even author from some sites such as Darknet [6].

(ii) Businesses organizations: Digital data that is stored in any businesses organizations contains most important knowledge and information. For example, banks, online shopping stores such as Amazon & Ebay, software firms or any other types of companies use digital systems and their data can be vulnerable to any types of malware specially ransomware. Sometimes the attackers or cybercriminals dedicates months for attacking an organization, encrypt data or lock systems. Afterwards, the money they ask for as the amount of ransom, worth more than

their time spent. Modern ransomware are smarter than the old or traditional ones as they are designed intelligently to run on any environment without giving a little clue to the network security mechanisms exist.

(iii) Public agencies and Governments: It is obvious that in some extreme cases, the attackers or cybercriminals may target the public agencies and Government servers such as research centers, law enforcement offices and even military servers as they did in the history of malware. Lately, they have targeted some of the above noted organizations with ransomware too where they have asked for ransom according to the organizations' data value.

Ransomware: How it victimizes?

The procedure of earning money by having ransom money from the victims is not a very simple process for the cybercriminals who design and implement it. It is watchfully planned that covers multiple elements. A small hole or weakness in the process can cause the failure of whole procedure.

(i) Propagation: Modern ransomware require special skills to have a successful implementation, this is not the job of amateur cybercriminals. Those ransomwares might be distributed through some of malware distributors where they do that by taking a definite fee. As an example, pay-per-click is a business website for advertisers similar to Google. Very similarly, the professional malware distributors also conduct their businesses adopting different unique methods such as pay-per-download or pay-per-install.

(ii) Traffic Distribution System (TDS): Cybercriminals may buy redirected traffic from a traffic distribution system (TDS) vendor, and point it to a website that contains or hosts malware including ransomware. It's a very common method and the malware might be downloaded to the users' systems easily.

(iii) Malvertisement: Malvertisement (Malicious advertisement) user may click an advert in a legitimate website while such an advertisement may redirect him/her to another website that is hosting or containing the malware.

(iv) Spam email: Everyone who have an electronic mail (e-mail) account, may have experience of receiving bulk amount of spam e-mails. Propagation of malware through spam is an easy way by using some social engineering and psychological techniques [6].

Cybercriminals may send unwanted e-mails to the users to infect them with the malware where such e-mails may have fake attachments. Spam mails might contain the issues like job adverts and offerings, tax rebates, lottery wining notifications, business proposals and many more unusual surprising news.

(v) Unsecured downloaders or downloading: While searching for downloading some files on the Internet, sometime we may experience some websites that want us to install its own downloader. By using that downloader, we can download our desired files. In such a case, occasionally, the downloader itself might be a malware, or after downloading such applications, the user may download the malware including ransomware without knowing.

(vi) Social engineering and self-propagation: Along with other main functionalities that ransomware possess, they have the capability to spread itself to other systems. Such a case is possible through a connected network link where the infected device is connected to other specific ways of connectivity or transmission of files. As an example, a mobile phone may contain the operation to read the contact books of the device and can spread itself among the other users. Message may contain the links to the location where ransomware is available or spread via social media/networks as an attachment.

(vii) Affiliate schemes of spreading: When a ransomware runs as a service and infect many devices, it can also increase the chances of extracting ransom from the victims. In such a case, all the affiliated members have the task or job of spreading the ransomware to any number of the systems that are capable of. The same concept exists for denial of service attacks where multiple systems attack a server as agents of an attack [6].

Ransomware: Countermeasures to prevent

In case of malware, prevention is obviously better that cure. In this section of the paper, some of the useful and helpful tips and techniques have been discussed in order to prevent our systems against malware particularly ransomware. The author expects that such tips and techniques will help to reduce the risk of the system being infected and recovery in case of infection.

(i) Inform, educate and train: In order to be protected from, ransomware must be studied regarding how it works, spreads and infects a system. It is important for organizations, agencies and public or government institutions to inform, educate and train their employees about ransomware. Learning and

becoming aware of such malware is a good way to know and being protected from the infection of such viruses.

(ii) Update the operating system or software from authentic sources: Updating or using the latest version of systems or software is imperative. One very common scenario is that most of the organizations, businesses and Government agencies neglect the issue of updating their systems and often use the old versions of operating systems, application and services. As an example, many universities, colleges as well as Government offices are still using old versions of the various operating systems such as Microsoft Windows XP, 7 or 8. This is similar with other operating systems such as Linux, OS X.

For example, a system using Microsoft Windows XP in an organization is more vulnerable to be virus infection than an organization that uses the latest version such as Microsoft Windows 10 that have the latest security patches. The reason is obvious since having 100% secured is not possible at all. In this digital world, the users face new types of malware and other threats everyday from different perspectives. Furthermore, the operating system used must be always updated with latest security features. Usually most of the systems need Adobe Flash Player, Shockwave player for playing audio and video types (such as extension & formats). Here the cybercriminals may target those application and infect them with the malicious codes. Afterwards, when the user updates, they install the updated version from an unknown source and the system can be infected from that source too. So, it is important to update those applications with latest security patches from their original official websites. Microsoft Software was, is and will be a superb target for cybercriminals, who are doing experiment and research on vulnerabilities, finding security holes in MS Operating systems as well as for the software. The users of digital systems particularly those who are using Microsoft products such as Microsoft Windows with different versions are much vulnerable and there are large numbers of known and unknown malware in their devices. They should be more aware about how to secure and prevent their systems against malware including ransomware.

One of the primary measures for being safe is to update regularly on time as the users find out a notification related to new release or update of their operating systems or other software from the authentic official resources. Most of the software companies or organizations they have their own specific release date for new products as well as for the security or other patches of the existed software. The users, particularly the system administrators who are responsible for protecting the data and systems, must have adequate updated knowledge regarding these important issues such as the release time of new versions or patch for the software products. Database administrators, system administrators, network administrators and security administrators should know how to take care of their own scope of tasks.

(iii) Use a layered defense approach: As discussed before, a ransomware can spread through various ways. One of them is the spam e-mail. Therefore, it is important for the organization to have messaging check points and e-mail security solutions to protect the e-mails that will be sent and received. There is a variety of such mail protection software available in the market. As an example, Google use a particular e-mail security for Gmail, in which a user cannot send an email attachment that contains a malicious executable file. However, such a protection system may know only about the known file (malware), it may fail regarding zero-day malware or attacks which are new and unknown to the security system. In no way, an unknown mail or an e-mail with susceptive file should be opened as those e-mails, in most cases, contain malware.

(iv) Endpoint security solution: Using Endpoint security solution is another way to prevent and protect of the system against the malware including ransomware. A huge number of endpoint security products exist in the market for securing the system, monitoring functions and operations on the systems. As an instance, Kaspersky is a well-known for good endpoint security products. A further little higher level of such endpoint security solutions might be the host based intrusion detection systems, host based intrusion prevention system, honeypots and firewalls for securing the systems against known and unknown malware or other types of threats [6].

(v) Mobile/tab users should use only authentic and verified distributor products: Now-a-days, almost everyone may have mobile phone or tab for their own personal use. For securing such devices against ransomware, the user must be well informed regarding the applications they use and install those applications only and only from a verified official distributor. The users must not install untrusted, free or cheap mobile or tablet applications from any unknown source that can otherwise infect their device with the malware including ransomware. Further, those users must check the permission that is required to gain access to those applications.

(vi) Use network protection: A well securing network is vital and critical in preventing and protecting the system which is connected to each other in an organization. In a secured network protection system, all the inflow and outflow of data should be monitored and controlled via firewall or other centralized or decentralized security systems to protect the entire system properly against the malware, malicious traffic, known or unknown threats and vulnerabilities. Intrusion detection systems and intrusion prevention systems have important roles in network security. Additionally, firewalls and honeypot/honeynet systems are quite useful. Some of the honeypot systems today used for capturing malware mostly focused on capturing and hunting of new, zero-day, unknown malware including ransomware.

(vii) Make backups and have a streamlined plan: Having a proper backup is not only a good idea to evade the threat of ransomware only, it is necessary to protect important information from all other types of threats of natural and men-made disasters such as flood, physical loss, fire, earthquake, damage, steal etc. The disaster recovery is easy if the users have a disciplined and regular back up procedure of their data. It's better to have backups separately from the system itself or in another location (such as external hard disk), preferably online (such as Google Drive) that can be available anywhere at any point of time and it will reduce the risk of data loss. In case of worst scenario, if all the prevention techniques fail and the overall system is infected with ransomware, the user can recover his/her data that he/she has backed up.

(viii) Use tools to remove the ransomware: Various anti-virus packages are available in the market that can detect and prevent the malware including ransomware from different vendors such as Kaspersky, Symantec, Norton etc.

(ix) Shadow copies: Even if complete system is infected and all the data is encrypted, the ransomware does not interfere with some inbuilt applications that can be recovered and restored. The user can recover or restore at least some files. Those recovery points are typically called shadow copies. If the user installs another separate application for doing this to take restore points as he/she is using the system daily, he/she can recover most of the data even in case of infection without paying to the cybercriminals.

However, there is not absolute 100% or bulletproof solution to be safe from ransomware. Some of the more advanced intelligent crypto ransomware are well conscious of all those explained techniques. Once the system is infected, the viruses might delete even the shadow copies. Other ransomware may also delete and pass through the security mechanisms which already run on the system, or they may delete, deactivate the files. Such an attack can reduce the detection and prevention ransomware on the system. In this situation, the only viable way for this is to keep proper and disciplined backup solution since there is not any practical way to access files or recover them without having the decryption key.

Ransomware: Future trend

Right at this moment, the users may face being infected with ransomware on their systems such as mobile devices, laptops or even on their wrist or smartwatches. However, later in the future, with the expansion and growth of Internet of things, the users may experience it on the other gadgets that run with a lightweight version operating system and the malicious code can run on that environments. The household appliances such as TVs, refrigerators, personal computers or other devices may be interconnected via a wifi access point. Therefore, once any of these devices got infected with ransomware, the percentage of possibilities of spreading to other system is quite high.

Huang et al. [11] estimated that the overall revenue generated by the hackers for the past two years was over 16 million USD extorted from on the order of 20,000 victims. They anticipated that the amount will increase with the mounting use of Internet and web. The economists and financial experts warns that such a distorted and tax evaded black money can be used for any illegal and unethical purposes such as terror financing. Therefore, it is now upto the users on how they protect or save their systems and avoid paying the hackers.

Theoretical and practical implications

The theoretical and practical research focusing on ransomware is still quite scarce. The author expects this paper will assist in informing the basic users to get to know and protect their devices from ransomware. He further expects that this paper can be a basic guideline for further researches to be conducted in upcoming times.

Limitations and further research scope

The paper is a basic paper written in a very simple language. It is not an empirical research paper. However, the author is hopeful that even though the paper is a very basic one, it can motivate in contributing to conduct further theoretical and empirical research initiatives.

Conclusions

Internet and cyber-security are two of the hottest information security topics in recent years. This paper has discussed the nature, type, systems that can be affected, the targets as well as the ways to protect the electronic devices connected online from malware particularly from ransomware. Each of the point has been discussed elaborately in this theoretical paper. Ransomware is not merely a malware as it covers other dimensional aspects such as economics and psychologies as well. In case of economic aspects, we can think of the hackers' targets and the value of the data. The attackers or hackers have some economic strategies. For example, they demand comparatively less amount of money from home or normal users; and more amount of money from an organization. On the other hand, regarding the psychological part, those same hackers usually give very short period of time to the victims after infecting their systems or capturing the data. Such a pressure put the users in a critical situation to decide where they have a very limited period of time. If, unfortunately, the user whose system is infected does not have a proper backup or other prevention strategies has to pay the ransome amount or take the risk of losing data. This is the psychological aspect about the ransomware.

The future of ransomware is unpredictable. Although, the experts are introducing unique and effective ways to avoid and protect from such malware, the hackers are as well investing their time and resources to upgrade their malware versions with higher capabilities and performance resulting in less failure than before. The cybercriminals are also constantly working on various ways to make the ransomware more intelligent and efficient as desired. In the future, along with the growth of digitalization and Internet of things (IoT), this issue will certainly grow along both in terms of academia and obviously, in practice among the cyber security experts.

Source of Funding

There is no source of funding to report.

Conflict of Interest

The author declares no conflict on interest.

References

1. Caporusso N, Chea S, and Abukhaled R (2019) A Game-Theoretical Model of Ransomware. In: Ahram T., Nicholson D. (eds) Advances in Human Factors in Cybersecurity. AHFE 2018. Advances in Intelligent Systems and Computing 782.

2. Hammill A (2017) The rise and wrath of ransomware and what it means for society. Doctoral dissertation, Utica College.

3. Nieuwenhuizen D (2017) A behavioural-based approach to ransomware detection. MWR Labs Whitepaper 655.

4. Tuttle H (2016) Ransomware attacks pose growing threat. Risk Management 63: 4-10.

5. Hampton N, & Baig ZA (2015) Ransomware: Emergence of the cyber-extortion men-ace. 13th Australian Information Security Management Conference, held from the 30 November – 2 December, 2015 (47-56), Edith Cowan University Joondalup Campus, Perth, Western Australia.

6. Herati DA, Bojamma AM, and Gandhi MPI (2018) Countermeasures to Ransomware Threats. 5th Annual Conference on Cyber-security, Banglalore, India.

7. Bhardwaj A, Subrahmanyam GV, Avasthi V, & Sastry HG (2015). Ransomware: A rising threat of new age digital extortion. Indian Journal of Science and Technology 9: 1-27.

8. Hosain MS (2020) Cryptocurrencies: The ultimate fate. Journal of Systems Integration 11: 34-45.

9. Hossin MA, & Hosain MS (2018) Bitcoin: Future Transaction Currency? International Journal of Business and Information 13: 385-404.

10. Cohen L, Montague VB, & Yuen M (2016) OCR Releases HIPAA Guidance on Ransomware.

11. Huang DY, Aliapoulios MM, Li VG, Invernizzi L, McRoberts K, et al. (2018) Tracking Ransomware End-to-end. 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA 618-631.

12. Investopedia.com (2019). Determining the intrinsic value of Bitcoin.