Ransomware: The Evolution of a Cybercrime

Md Rifat Ahmed, Julia Juremi and Jazrin Ramli

Abstract--- *Ransomware is growing threats that encrypts and lock user's files and holds the decryption key until a ransom is settled by the target. This type of malware is responsible for tens of millions of dollars in extortion annually. Worse still, developing new variants is trivial, facilitating the evasion of many antivirus and intrusion detection systems. This paper discusses the evolution of the Ransomware, which involves types of both computer and mobile device ransomware. The scam has evolved over time, using various techniques to disable the target device. We have identified at least ten different versions of ransomware. In fact, there is not just one single family of ransomware composed of multiple variants, but rather multiple families each with their own unique behavior. This paper also provides the suggestion on how to protect the devices from being infected by this kind of cybercrime.*

Keywords--- *Ransomware, Malware, Trojan, Kill Chain, Wanna Cry, Petya, C2.*

I. INTRODUCTION

Ransomware or ransom malware is a form of malicious software or malware. It is a sub-branch of malware whereby the data of a victim stored in a hard drive or computer is locked by encryption. The only way to retrieve or decrypt this locked information is by paying the ransom via crypto currency like Bitcoin which is digital coin. However, transferring and receiving of payment is done confidentially hence it cannot be traced out [7].

Generally, Ransomware is like a kidnap but in the digital way. That means in kidnap, criminal or criminal groups kidnap someone and similarly in ransomware, criminal lock normal person computer. In other things like demand is also some in kidnap and ransomware. Criminals demand money from their family which is called ransom.

II. EVOLUTION OF RANSOMWARE

The ransomware as we know it know it today is not the same as it was when it first broke out in the technological world. In the year 1989, the first ransomware was a virus which was called the AIDS Trojan or PC Cyborg [1]. This virus was made by Joseph L. Popp.

Popp was a Harvard-trained evolutionary biologist. It was used to encrypt for files name. Later in the year 2005, the first modern ransomware came which called Trojan. Gpcoder, also known as GP code and GP coder.

It was exposed in May 2005 and used to overcome symmetric encryption technique weak. It also used to spread via a spam email attachment claiming. Followed by that, in the year 2007 the definition of ransomware became clear

Md Rifat Ahmed, Faculty of Computing, Engineering & Technology, Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia. E-mail: r.riven.ali.khan@gmail.com
Julia Juremi, Faculty of Computing, Engineering & Technology, Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia. E-mail: julia.juremi@staffemail.apu.edu.my
Jazrin Ramli, Faculty of Computing, Engineering & Technology, Asia Pacific University of Technology & Innovation, Kuala Lumpur, Malaysia. E-mail: jazrin86@gmail.com

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

that was meant for locking (encrypt) files. It was first used against Russia which was like that way displayed a pornographic image on the machine and demanded payment to remove it [1].

The attackers also used SMS text message or calling a premium- rate phone number. The attack spread across Europe and the US. In the year 2008, a new update version of Trojan. Gp coder, which is called GP code used a 1024-bit RSA key. The RSA key is a private key based on RSA algorithm.

This virus was attacked by text file and it asked for payment $100 to $200 in e-gold or Liberty Reserve. Then in 2011, many ransomware samples were created and followed by those samples creation in 2012 many toolkit inventions came for ransomware like Citadel, Lyposi, Reveton etc.

III. Defining the Ransomware Kill Chain

Exabeam company research more than 86 types of ransomware, they see all ransomware attack behavior almost same [2]. They divide these six states which is called Ransomware Killing chain. The six states are;

- Distribution campaign
- Malicious code infection
- Malicious payload staging
- Scanning
- Encryption
- Payday

Distribution Campaign

Distribution campaign is the first states to the Ransomware Kill Chan. In this state hacker trying to install software to victim devise. In that reason, they are tricked or forced to download. In that causes they normally use a malicious dropper or payload via an email, a watering-hole attack, an exploit kit, or a drive-by-download.

Malicious Code Infection

In this state, hacker made a tricked by using dropper and victim download that .exe files or another way hacker attacked victim devise by connecting to a predefined list of IP addresses that host the C2 server, or by using DGA to connect via pseudo random domains.

Then the dropper usually copies the malicious executable to a local directory such as Temp folder or %App Data%/local/temp. Finally, the dropper script is terminated, removed, and the malicious payload is executed.

Staging

Staging is three states of ransomware killing Chain. It is middle states of virus inject and scanning files. It is checking the local configuration and registry keys for various rights, such as proxy settings, user privileges, accessibility, and other potentially meaningful information.

There are also several steps on system, for example: running at boot, run when in recovery mode, disabling recovery mode, etc. Finally, it uses various commands to delete shadow copies of the files from the system.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

Scanning

In this state's ransom ware scanning all system files. It is take several time which is depends of many files have in system. It normal prepares to take files hostage. The ransomware scans and maps the locations containing those files, both locally and on both mapped and unmapped network-accessible systems. Many ransomware also took cloud files, drop box and searching some interesting data or information.

Encryption and Payday

Encryption is fifted state in Ransomware Killing Chain. In these states, all files systems are encrypted and all file or browser is locked. Payday is the last states of ransomware killing Chain. Payday happens after encryption phase. When it happens, desktop screen will be replaced with a note. The note will state the bitcoin address and time to pay. Example: if you give 300 bit coins into first week, otherwise give 600 bit coins into next two weeks. Your file will all be deleted if the payment is failed to be performed in three weeks time.

IV. TYPES OF RANSOMWARE

Crypto-Malware

Crypto-malware is a common type of ransomware. It is also called encryptor ransomware, as the name proposes. It encodes your file. Crypto-malware have many types. Those are;

Crypto Locker

Encrypting ransomware reappeared in September 2013 with a Trojan which is known as Crypto Locker. Its peak in 2013 and 2014. Crypto Locker was isolated by the seizure of the Game over ZeuS botnet as part of Operation Tovar, as officially announced by the U.S. Department of Justice on 2 June 2014. But In this time, it was attacked over 500,000 machines and took over $3 million form victim. Normally it is used a botnet, spread through spam email, to encrypt user files and take such as the user's name, birthday, location, Facebook information, system details and IP address. It then locks the user out of their computer entirely and demands a payment within 24 hours. Crypto Locker was also propagated using the Gameover ZeuS Trojan and botnet.

Crypto Wall

Another major ransomware Trojan targeting Windows, which is Crypto Wall. It was first appeared in 2014. In this time Crypto wall came with different versions, such as Crypto Defense, Cryptor Bit, Crypto Wall 2.0, Crypto Wall 3.0 and Crypto Wall 4.0. It works like CrypLocker. In late 2015, Crytpo Wall 4.0 was introduced with a new feature. It was attacked user computer by email and web page and show advertisements. Sometime variations of Crypto Wall's ransom note are also unusual, containing text such as: "Congratulations!!! You have become a part of large community Crypto Wall. Together we make the Internet a better and safer place." The ransom demanded is a hefty $700, doubling after about a week to $1,400. The FBI reported in June 2015 that nearly 1,000 victims had contacted the bureau's Internet Crime Complaint Center to report Crypto Wall infections, and estimated losses of at least $18 million [11]. The most recent version, Crypto Wall 4.0, enhanced its code to avoid antivirus detection, and encrypts not only the data in files but also the file names.

CTB-Locker

In mid 2014, a new encryption come which is called CTB-Locker. People use this to command and control systems, while affiliates pay a monthly fee to access the ransomware, taking on the responsibility for finding victims through their own spam email campaigns or by running malicious web sites linked to exploit kits. The name CTB-Locker comes from Curve-Tor-Bitcoin-Locker, alluding to the Elliptic Curve encryption and ransomware employs use Tor network for communications and the payment demanded in Bitcoins. CTB-Locker's ransom note displays several flag icons in the top right corner, in that reason the victim can read the note in different European languages.

Wanna Cry

Wanna Cry is also known as known as Wanna Crypt and Wanna cry. It is normally encrypted victims file. It started global attack in on Friday 12 May 2017 and every attack they demand $300 in bitcoin for unlocking encrypted files. More than 300,000 victims in over 150 countries fell victim to the ransomware over the course of one weekend, with businesses, governments, and individuals across the globe all affected.

National Health Service (NHS) England, and Telefonica, one of the largest telecom providers in the world, have each given out statements indicating that their systems have been brought to a grinding halt by a ransomware that Malware bytes detects as Ransom.

WanaCrypt0r. The ransomware has also been observed hitting companies in Spain, Russia, Ukraine, and Taiwan. The ransomware is spread using a known, and patched, vulnerability (MS17-010) that came from a leaked NSA set of exploits. And the encryption is done with RSA-2048 encryption. That means that decryption will be next to impossible, unless the coders have made a mistake that we haven’t found yet.

Petya

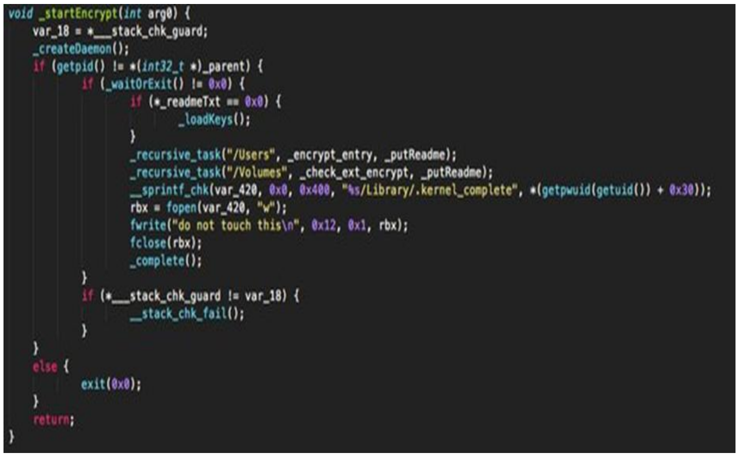
Petyaransomware which is create in July, 2016. It is also called Not Petya/Golden Eye. This virus first hit targets in Ukraine, including its central bank, main international airport, and even the Chernobyl nuclear facility, before quickly spreading around the globe, infecting organisations across Europe, Russia, the US, and Australia.

Locker

Reventon is types of locker ransomware which is made in 2012. It is based on the Citadel Trojan which is based on the Zeus Trojan. Victim computer affect when they go illegal activities, such as downloading unlicensed software or child pornography. The warning informs the user that to unlock their system, they would have to pay a fine using a voucher from an anonymous prepaid cash service such as Ukash or pay safe card. It is also called "Police Trojan".

Mac ransomware

No operator system is safe from ransomware. Mac OS also affected by a ransomware in 2016 called KeRanger. Figure 1 shows the KeRanger code. Usually, Mac OS gets infected by a ransomware through an app. The app name is Transmission which is copied malicious filed and encrypted files. When Apple Company discovered the malware, they soon released an anti-malware program called X Protect. With the release of XProtect, the ransomware could not affect anymore Mac OS.



```
void _startEncrypt(int arg0) {
    var_18 = *___stack_chk_guard;
    _createDaemon();
    if (getpid() != *(int32_t *)_parent) {
            if (_waitOrExit() != 0x0) {
                    if (*_readmeTxt == 0x0) {
                            _loadKeys();
                    }
                    _recursive_task("/Users", _encrypt_entry, _putReadme);
                    _recursive_task("/Volumes", _check_ext_encrypt, _putReadme);
                    ___sprintf_chk(var_420, 0x0, 0x400, "%s/Library/.kernel_complete", *(getpwuid(getuid()) + 0x30));
                    rbx = fopen(var_420, "w");
                    fwrite("do not touch this\n", 0x12, 0x1, rbx);
                    fclose(rbx);
                    _complete();
            }
            if (*___stack_chk_guard != var_18) {
                    ___stack_chk_fail();
            }
    }
    else {
            exit(0x0);
    }
    return;
}
```

Figure 1: KeRanger Code

Mobile Ransomware

Mobile ransomware is not a very common and due to this many people do not know the existence of this ransomware. Mobile ransomware normally blocks all message and requires a certain ransom amount to be paid in order unlock the entire message. Mobiles can be infected via malicious app. If your mobile is affected by this malware, you can boot app to safe mode and delete infect apps [3]. Figure 2 shows the mobile attack time needed.

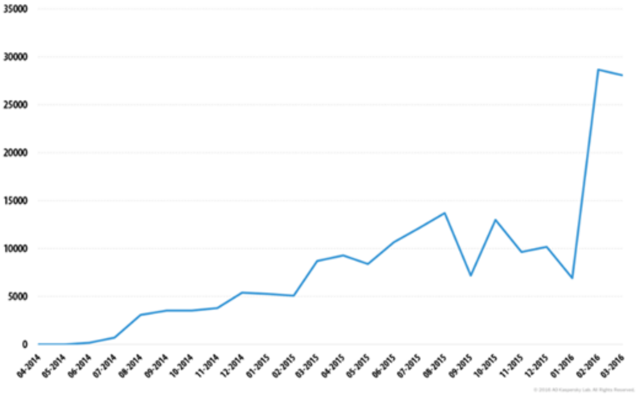


Figure 2: Mobile Attack Time

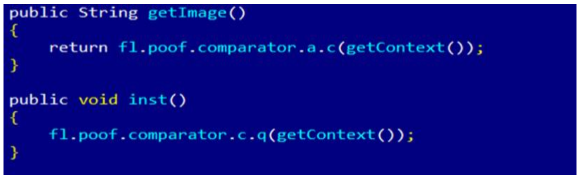
V. TYPES OF MOBILE RANSOMWARE

Fusobransomware

In April 2016, a new Trojan-Ransom program attacked more than 100 countries user mobile which is called Trojan-Ransomn. AndroidOS. Fusob [3]. This ransomware was first discovered by Kaspersky lab experts which was in early January 2015.This Trojan collects information about the device and sends it to the attackers. In doing so, it uploads two different sets of data to the Command and Control (C&C) server.

The first set of data contains information about the device, such as device model, the version of the operating system, etc. This ransomware uses Base64 algorithm for sending data by encoding and uploaded to the criminals' server.

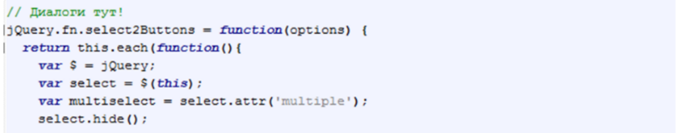
The second data set, among other things, contains the user location and the call log with names from the contact list. This set is encrypted by the AES algorithm and loaded to a malicious C&C server. The Trojan then waits for the attackers' command with the necessary data to block the device. For this purpose, the Trojan uses an HTML file received from the C&C. The Trojan itself includes functionality that can be activated from this file. Figure 3 and Figure 4 show the example of Fusobransomware code.



```
public String getImage()
{
    return fl.poof.comparator.a.c(getContext());
}

public void inst()
{
    fl.poof.comparator.c.q(getContext());
}
```

Figure 3: Example of Fusobran Somware Code



```
// Диалоги тут!
jQuery.fn.select2Buttons = function(options) {
  return this.each(function(){
    var $ = jQuery;
    var select = $(this);
    var multiselect = select.attr('multiple');
    select.hide();
```

Figure 4: Fusobransomware Code

There are two ways of how this ransomware works:

I. Take photo from front camera

II. Install a previously downloaded APK file

Normally user phone affect this ransomware by visiting the porn sites. The criminals usually demand between $100 and $200 to unblock the device [6]. The ransom has to be paid in the form of codes from pre-paid iTunes cards.

The Small Ransomware

In April, 2016, another new virus attacked over 12% mobile users which are called as Trojan-Ransomn. Android OS. Small. This virus was second most popular in that time and it has on our radar since mid-June 2014. This ransomware was worked by three group:

The First Group

This ransomware Trojan-Ransom. Android OS. Small family includes small and very basic ransom Trojans. This ransomware asks to devices owner and if he say yes, then it send a message and make too hard to use that mobile.

The Second Group

The second group is Trojan-Ransom. Android OS. Small family are encryptors. This virus first blocking devices, then start to encrypting files on the memory card.

The Third Group

The third group of the Trojan-Ransom. Android OS. Small family which is a multifunctional ransomware Trojan. It works depends on command which was received from C&C. This virus asked to device administrator for run. If administrator says yes, then it takes information from devices. Such as the phone number, the device model, the IMEI, and the version of the operating system. Trojan can receive commands from both the C&C and via GCM. It can perform the following commands:

- START – start the main service of the Trojan
- STOP - stop the main service of the Trojan
- RESTART – restart the main service of the Trojan
- URL – change the C&C address
- MESSAGE – send an SMS to a specified number with a specified text
- UPDATE_PATTERNS – update the rules for processing incoming SMSs
- UNBLOCK – disable the device administrator rights
- UPDATE – download a file form the specified URL and install it
- CONTACTS – send out a specified SMS to all contacts from the list of contacts PAGE – address a specified C&C for a command
- ALLMSG – upload all SMSs from the device to the criminals’ server
- ALLCONTACTS - upload all contacts from the device to the criminals’ server
- ONLINE – address the C&C - NEWMSG – save a specified SMS on the device
- LOCKER – display text with the ransom demand
- LOCKER_UPDATE – update the text with the ransom demand
- LOCKER_BLOCK – block the device
- LOCKER_UNBLOCK – unblock the device
- CHANGE_GCM_ID – change GCM ID

Once launched, the Trojan also intercepts incoming SMSs by rules which was received from the C&C. It can also receive the following commands via SMS:

- 3458 – disable the device administrator rights
- Deblock – unblock the device
- hi - enable mobile data transfer
- ask - disable mobile data transfer
- privet – enable WiFi
- ru – disable WiFi
- 393838 – in addition to the command the message should contain a new encrypted C&C address

Svpengransomware

Svpengransomware attacked over 97% user which was located in the US. Kaspersky Lab detected this family in a total of 9 countries in April, 2016. The creator of this virus who also create the banking Trojan Svpeng. This virus allows permission to devices as administrato. It then take lists of calls , history of visiting site by browser and it also take picture by front camera. The Trojan blocks the device by overlaying all windows with an HTML file and demand $500 for unlock devise.

1. How the Ransomware does affect the Device?

Ransomware attacks computers and mobile devices in many ways [5].

Exploit Kits

Exploit kits is a software which is designed to run ransomware on web servers. Once you click on these web servers, your computer will be affected.

Social Engineering

It is other types of exploit kits. In social engineering main technique is email. It is also affected by the file like a PDF or Excel/Doc record, however, it’s extremely an executable record. The client downloads the document clicks on it, and this way the system gets infected.

C2

C2 is quit stander for command and control. C2s are servers or networks used by machines infected with malicious code to receive commands and stolen data. C2 servers can be distributed in layers to prolong their activity and hide the origin of commands.

2. How to Protect Device from Ransomware?

Ransomware today has become a huge problem in the world we live in today. Many companies and home desktops can be prone to being infected by the ransomware [6]. There are several ways to prevent a device from being harmed by the ransomware. The first step is to always do a back-up. Ransomware normally attacks on your data and wants a certain amount of money to be paid to unlock that data. If the data has already been backed-up, then there is of no need to pay the ransom to unlock it. Instead it can be recovered from back- up storage such as a drive or a cloud. When doing back up, ensure to use multiple back up storage types and use different devices. This is very important because if the same device or clouds is used then that too can be affected by ransomware [7]. Keep to the 3-2-1 rule whereby keep three backups of your data, on two different storage types, and at least one backup offsite.

Secondly is to always update. Update is very important to save computer from ransomware. We use different software for easy and quickly control. For an example, in the Operator system there are different kinds of browsers such as Opera, Chrome, Firefox and Microsoft Edge etc. These companies add in new features from time to time in conjunction with the latest of technology to ensure surfing the web is ever safe to use. Hence, if you constantly update these types of software, you are guaranteed that your computer or device is safe to use all the time.

Thirdly is the use of an antivirus application. An Antivirus application helps in ensuring that one’s device is safe from any sort of ransomware attacks. Avoid email links and attachments. Email is a common way to spread ransomware easily. Hacker sends a link in victim email, when victim click the link, the computer will be effect. In that reason, every person should avoid unknown e-mail [6].

3. How to Stop Ransomware Attacks

In the last few years, ransomware attack increased at a high rate. For that reason, different companies and people try to create an anti-virus to test and find out how to stop or control ransomware attack. The standard procedure is as follows:

1. Look for unregistered or expired C2 domains belonging to active botnets and point it to a sinkhole (a sinkhole is a server designed to capture malicious traffic and prevent control of infected computers by the criminals who infected them).

2. Gather data on the geographical distribution and scale of the infections, including IP addresses, which can be used to notify victims that they're infected and assist law enforcement.

3. Reverse engineer the malware and see if there is any vulnerability in the code which would allow us to take-over the malware/botnet and prevent the spread or malicious use, via the domain we registered.

VI. Conclusion

Ransomware is a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer ransom and extortion to the victims. As awareness of these scams increases, the attackers and their malware are likely to evolve and use more sophisticated techniques to evade detection and prevent removal. The "ransom letter" will likely also evolve and the attackers will use different hooks to defraud innocent users. Even if we take every possible precaution to try and prevent ransomware from gaining entry and to swiftly detect attacks, there may still be times when our defenses fall short. The best way to safeguard against ransomware attacks and lessen the potential impact on our side is to maintain a regular, secure backup system alongside a clear recovery plan that allows us to restore a recent backup immediately. Take the right steps to prevent, detect and recover from ransomware and we can dramatically reduce its potential impact on our business.

References

[1] Gazet, A., 2010. Comparative analysis of various ransomwarevirii. *Journal in computer virology*, 6(1), pp.77-90.

[2] Kaspersky lab Report. Accessed on https://media.kasperskycontenthub.com/wpcontent/uploads/sites/43/2018/03/07190822/KSN_Report_Ransomware_2014-2016_final_ENG.pdf.

[3] Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L. and Kirda, E., 2015, July. Cutting the gordian knot: A look under the hood of ransomware attacks. *In International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 3-24).

[4] Marcus Hutuchins. How to Stop Ransomware Attacks. Accessed on https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.

[5] O'Gorman, G. and McDonald, G., 2012. Ransomware: A growing menace. *Symantec Corporation.*

[6] Ronny Richardson and Max North. How to protect device from ransomware. Accessed on 2 Jan 2019. Link: http://scholarspress.us/journals/IMR/pdf/IMR-1 2017.%20pdf/IMR-v13n1art2.pdf.

[7] Scaife, N., Carter, H., Traynor, P. and Butler, K.R., 2016, June. Cryptolock (and drop it): stopping ransomware attacks on user data. *In 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS)* (pp. 303-312). IEEE.

[8] P. Mary Jeyanthi, Santosh Shrivastava Kumar "The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region", *Theoretical Economics Letters,* 2019, 9, 752-760.

[9] P. Mary Jeyanthi, "An Empirical Study of Fraudulent and Bankruptcy in Indian Banking Sectors", *The Empirical Economics Letters,* Vol.18; No. 3, March 2019.

[10] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Hybrid Metaheuristic techniques", *International Journal of Business Intelligence Research,* Volume 5, Issue 1, April-2014.

[11] P. Mary Jeyanthi, "INDUSTRY 4.O: The combination of the Internet of Things (IoT)and the Internet of People (IoP)", *Journal of Contemporary Research in Management,* Vol.13; No. 4 Oct-Dec, 2018, ISSN: 0973-9785.

[12] P. Mary Jeyanthi, "The transformation of Social media information systems leads to Global business: An Empirical Survey", *International Journal of Technology and Science (IJTS),* issue 3, volume 5, ISSN Online: 2350-1111.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019

[13] P. Mary Jeyanthi," An Empirical Study of Fraud Control Techniques using Business Intelligence in Financial Institutions", *Vivekananda Journal of Research* Vol. 7, Special Issue 1, May 2018, ISSN 2319-8702(Print), pp. 159-164.

[14] Mary Jeyanthi, S and Karnan, M.:"Business Intelligence: Artificial bear Optimization Approach", International *Journal of Scientific & Engineering Research,* Volume 4, Issue 8, August-2013.

[15] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Optimization techniques for Decision Making", International *Journal of Engineering Research and Technology,* Volume 2, Issue 8, August-2013.

[16] Mary Jeyanthi, S and Karnan, M.: "A New Implementation of Mathematical Models with metaheuristic Algorithms for Business Intelligence", *International Journal of Advanced Research in Computer and Communication Engineering,* Volume 3, Issue 3, March-2014.

[17] Dr. Mary Jeyanthi: "Partial Image Retrieval Systems in Luminance and Color Invariants: An Empirical Study", *International Journal of Web Technology* (ISSN: 2278-2389) – Volume-4, Issue-2.

[18] Dr. Mary Jeyanthi: "CipherText Policy attribute-based Encryption for Patients Health Information in Cloud Platform", *Journal of Information Science and Engineering* (ISSN: 1016-2364)

[19] Mary Jeyanthi, P, Adarsh Sharma, Purva Verma: "Sustainability of the business and employment generation in the field of UPVC widows" (ICSMS2019).

[20] Mary Jeyanthi, P: "An Empirical Survey of Sustainability in Social Media and Information Systems across emerging countries", *International Conference on Sustainability Management and Strategy"* (ICSMS2018).

[21] Mary Jeyanthi, P: "Agile Analytics in Business Decision Making: An Empirical Study", *International Conference on Business Management and Information Systems"* (ICBMIS2015).

[22] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence – soft computing Techniques", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).

[23] Mary Jeyanthi, S and Karnan, M.: "A Comparative Study of Genetic algorithm and Artificial Bear Optimization algorithm in Business Intelligence", *International Conference on Mathematics in Engineering & Business Management* (ICMEB 2012).

[24] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Optimization for Decision Making ", *2011 IEEE International Conference on Computational Intelligence and Computing Research* (2011 IEEE ICCIC).

[25] Mary Jeyanthi, S and Karnan, M.: "Business Intelligence: Data Mining and Decision making to overcome the Financial Risk", *2011 IEEE International Conference on Computational Intelligence and Computing Research (2011 IEEE ICCIC).*

[26] Dr. Mary Jeyanthi, S: "Pervasive Computing in Business Intelligence", *State level seminar on Computing and Communication Technologies.* (SCCT-2015)

[27] Dr.P.Mary Jeyanthi, "Artificial Bear Optimization (ABO) – A new approach of Metaheuristic algorithm for Business Intelligence", ISBN no: 978-93-87862-65-4, *Bonfring Publication*. Issue Date: 01-Apr-2019

[28] Dr.P.Mary Jeyanthi , "Customer Value Management (CVM) – Thinking Inside the box" – ISBN : 978-93-87862-94-4, *Bonfring Publication,* Issue Date: 16-Oct-2019.

[29] Jeyanthi, P. M., & Shrivastava, S. K. (2019). The Determinant Parameters of Knowledge Transfer among Academicians in Colleges of Chennai Region. *Theoretical Economics Letters,* 9(4), 752-760.

Received: 17 Sept 2019 | Revised: 19 Oct 2019 | Accepted: 20 Nov 2019