*THINK INDIA (Quarterly Journal)*

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

# Awareness Of Ransomeware Attacks-Detection And Prevention Parameters

S. Swapna
Asst. Professor, M. Tech,
Pallavi Engineering College
*vooreswapna205@gmail.com*

R.Keerthana
B.Tech-CSE
Pallavi Engineering College

P.Poojitha
B.Tech-CSE,
Pallavi Engineering College

**Abstract:** In this paper, cybercrime activities have grown significantly, compromising device security and jeopardizing the normal activities of enterprises. The profits obtained through intimidation and the Limitations for tracking down the illegal transactions have created a lucrative business based on the of users' files. In this context, ransomware takes advantage of cryptography to compromise theuser information or deny access to the operating system. Then, the attacker extorts the victim to pay a ransom in order to regain access, recover the data, or keep the information private. Nowadays, the adoption of Situational Awareness (SA) and cognitive approaches can facilitate the rapid identification of ransomware threats. SA allows knowing what is happening in compromised devices and network communications through monitoring, aggregation, correlation, and analysis tasks. The current literature provides some parameters that are monitored and analyzed in order to prevent these kinds of attacks at an early stage. However, there is no complete list of them. To the best of our knowledge, this paper is the first proposal that summarizes the parameters evaluated in this research field and considers the SA concept. Furthermore, there are several articles that tackle ransomware problems. However, there are few surveys that summarize the current situation in the area, not only regarding its evolution but also its issues and future challenges. This survey also provides a classification of ransomware articles based on detection and prevention approaches.

**Keywords***:* information security; prediction; ransomware; situational awarenes

*****

## INTRODUCTION

### Ransomeware

Ransom malware, or Ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card.

### Types of ransomware

There are three main types of ransomware, ranging in severity from mildly off-putting to Cuban Missile Crisis dangerous. They are as follows:

**Scareware**: As it turns out, is not that scary. It includes rogue security software and tech support scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe.A legitimate cybersecurity software program would not solicit customers in this way. If you don't already have this company's software on your computer, then they would not be monitoring you for ransomware infection. If you do have security software, you wouldn't need to pay to have the infection removed—you've already paid for the software to do that very job.

**Screen lockers**: Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine. However, the FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

**Encrypting ransomware**: This is the truly nasty stuff. These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get ahold of your files, no security software or system restore can return them to you. Unless you pay the ransom—for the most part, they're gone. And even if you do pay up, there's no guarantee the cybercriminals will give you those files back.

## BACKGROUND STUDY AND RELATE WORK

### Ransomware:

Ransomware became very popular because of U.S. businesses and consumers approximately $209 million during the first quarter of 2016[1]. Topics about privacy with the legal and very public battle between Apple and the FBI. The strike down of the Safe Harbor Act by a European High Court and its replacement with the EU-U.S. Privacy Shield framework has focused businesses to re-examine the impact of privacy going forward[1]. After usage of internet ,the requirement of cyber security was increased by as more connections between the physical and the digital worlds. But companies and government agencies did not followed guidelines which left everyone vulnerable. Due to the innovative approaches of research scientists and the policy leadership of elected officials, we feel that together we can identify bold, new technologies and strategies to ensure the safety and security of government, industry and each other[1].

According to previous surveys ransomware different companies in the first five months of 2016 are more than all of 2015. Based on these facts we can say ransomware in 2016 would be very high. Ransomware attackers will use different means to attack users by focusing on phishing

### History of Ransomware

The first ransomware, known as PC Cyborg or AIDS, was created in the late 1980s. PC Cyborg would encrypt all files in the C: directory after 90 reboots, and then demand the user renew their license by sending $189 by mail to PC Cyborg Corp. The encryption used was simple enough to reverse, so it posed little threat to those who were computer savvy. With few variants popping up over the next 10 years, a true ransomware threat would not arrive on the scene until 2004, when GpCode used weak RSA encryption to hold personal files for ransom. In 2007, Winlock heralded the rise of a new type of ransomware that, instead of encrypting files, locked people out of their desktops. Winlock took over the victim screen and displayed pornographic images. Then, it demanded payment via a paid SMS to remove them. With the development of the ransom family Reveton in 2012 came a new form of ransomware: law enforcement ransomware. Victims would be locked out of their desktop and shown an official-looking page that included credentials for law enforcement agencies such as the FBI and Interpol. The ransomware would claim that the user had committed a crime, such as computer hacking, downloading illegal files, or even being involved with child pornography. Most of the law enforcement ransomware families required a fine be paid ranging from $100 to $3,000 with a pre-paid card such as UKash or PaySafeCard.

Average users did not know what to make of this and believed they were truly under investigation from law enforcement. This social engineering tactic, now referred to as implied guilt, makes the user question their own innocence and, rather than being called out on an activity they aren't proud of, pay the ransom to make it all go away. In 2013 Crypto Locker re- introduced the world to encrypting ransomware—only this time it was far more dangerous.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

Crypto Locker used military grade encryption and stored the key required to unlock files on a remote server. This meant that it was virtually impossible for users to get their data back without paying the ransom. This type of encrypting ransomware is still in use today, as it's proven to be an incredibly effective tool for cybercriminals to make money. Large scale outbreaks of ransomware, such as WannaCry in May 2017 and Petya in June 2017, used encrypting ransomware to ensnare users and businesses across the globe. In recent news, the criminals behind the Sodinokibi ransomware (an alleged offshoot of GandCrab) have started to use managed service providers (MSP) to spread infections. In August of 2019, hundreds of dental offices around the country found they could no longer access their patient records. Attackers used a compromised MSP, in this case a medical records software company, to directly infect upwards of 400 dental offices using the record keeping software softw.
Ransomware.

**Mac Ransomware**

Learn about KeRanger, the first true Mac ransomware. Learn about KeRanger, the first true Mac ransomware.
Not ones to be left out of the ransomware game, Mac malware authors dropped the first ransomware for Mac OSes in 2016. Called KeRanger, the ransomware infected an app called Transmission that, when launched, copied malicious files that remained running quietly in the background for three days until they detonated and encrypted files. Thankfully, Apple's built-in anti-malware program XProtect released an update soon after the ransomware was discovered that would block it from infecting user systems. Nevertheless, Mac ransomware is no longer theoretical.

**Mobile ransomware**

It wasn't until the height of the infamous Crypto Locker and other similar families in 2014 that ransomware was seen on a large scale on mobile devices. Mobile ransomware typically displays a message that the device has been locked due to some type of illegal activity. The message states that the phone will be unlocked after a fee is paid. Mobile ransomware is often delivered via malicious apps, and requires that you boot the phone up in safe mode and delete the infected app in order to retrieve access to your mobile device.

**What to do if infected**

The number one rule if you find yourself infected with ransomware is to never pay the ransom. (This is now advice endorsed by the FBI.) All that does is encourage cybercriminals to launch additional attacks against either you or someone else. However, you may be able to retrieve some encrypted files by using free decryptors.
To be clear: Not all ransomware families have had decryptors created for them, in many cases because the ransomware is utilizing advanced and sophisticated encryption algorithms. And even if there is a decryptor, it's not always clear if it's for right version of the malware. You don't want to further encrypt your files by using the wrong decryption script. Therefore, you'll need to pay close attention to the ransom message itself, or perhaps ask the advice of a security/IT specialist before trying anything.
Other ways to deal with a ransomware infection include downloading a security product known for remediation and running a scan to remove the threat. You may not get your files back, but you can rest assured the infection will be cleaned up. For screenlocking ransomware, a full system restore might be in order. If that doesn't work, you can try running a scan from a bootable CD or USB drive. If you want to try and thwart an encrypting ransomware infection in action, you'll need to stay particularly vigilant. If you notice your system slowing down for seemingly no reason, shut it down and disconnect it from the Internet. If, once you boot up again the malware is still active, it will not be able to send or receive instructions from the command and control server. That means without a key or way to extract payment, the malware may stay idle. At that point, download and install a security product and run a full scan.


**Protect from ransomware**

Security experts agree that the best way to protect from ransomware is to prevent it from happening in the first place.

The first step in ransomware prevention is to invest in awesome cybersecurity—a program with real-time protection that's

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

designed to thwart advanced malware attacks such as ransomware.

You should also look out for features that will both shield vulnerable programs from threats (an anti-exploit technology) as well as block ransomware from holding files hostage (an anti- ransomware component). Customers who were using the premium version of Malwarebytes for Windows, for example, were protected from all of the major ransomware attacks of 2017.

Next, as much as it may pain you, you need to create secure backups of your data on a regular basis. Our recommendation is to use cloud storage that includes high-level encryption and multiple-factor authentication. However, you can purchase USBs or an external hard drive where you can save new or updated files—just be sure to physically disconnect the devices from your computer after backing up, otherwise they can become infected with ransomware, too.

Then, be sure your systems and software are updated. The WannaCry ransomware outbreak took advantage of a vulnerability in Microsoft software. While the company had released a patch for the security loophole back in March 2017, many folks didn't install the update—which left them open to attack. We get that it's hard to stay on top of an ever-growing list of updates from an ever-growing list of software and applications used in your daily life. That's why we recommend changing your settings to enable automatic updating.

Finally, stay informed. One of the most common ways that computers are infected with ransomware is through social engineering. Educate ourself on how to detect malspam, suspicious websites, and other scams.

### Steps To Avoid Ransomeware

Cyber security has never been more important. Thankfully, there are several inexpensive and simple steps that anyone can take to avoid becoming a victim of ransomware.

1. Be Careful — The simplest step is often the one that people overlook. Most ransomware requires the victim to perform an action to activate it, such as clicking a link or opening a file. Don't interact with anything that looks suspicious, even if it appears to come from a friend or family member.
2. Make Regular Backups — Backups on external hard drives are essential. They're relatively inexpensive (costing far less than paying a ransom demand) and will allow you to keep a copy of your important files and documents. Don't keep these hard drives plugged in at all times; otherwise, they could become infected too.
3. Disable Autoplay — Autoplay can be very convenient when trying to open a file type that you're familiar with. However, hackers can often disguise a virus as a regular media file, so you're best not letting your computer open them automatically.
4. Stay Secure — Stay away from dodgy websites (for example, piracy-based websites) and always have firewall and anti-virus programs running in the background. Even free programs are better than nothing and some of them are actually pretty good, for example AVG and Avast.
5. Install Updates — Don't ignore updates for your programs and operating system — they're often there to patch out security vulnerabilities and combat new threats.
6. Enable File Extensions — This will allow you to always know what a file actually is before opening it. Windows operating systems have this feature turned off by default. Enabling it will help you to notice odd file types that could contain something malicious.
7. Don't Pay — More often than not, hackers won't hold up their end of the bargain. Paying them sends a clear message that you can be victimized, and could also fund future criminal activities.
8. Stay Informed — Read up on the latest news about ransomware, viruses and cyber-attacks so you're always 100% informed and prepared.
9. Make a Plan — If your computer or device does become infected, immediately disconnect from the internet. Also, don't pull the power or restart — this could actually help the ransomware spread further.
10. Seek Expert Assistance — There are many websites dedicated to decrypting files that have been encrypted by ransomware. Not all types of ransomware can be fixed, but it's certainly worth trying to find a decryption key before giving up and restoring a backup.

## Ransomware Life Cycle

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

The ransomware life cycle can be described in seven steps, as follows:
1.Ransomware design
2.Ransomware dissemination
3.Ransomware arrival
4.Command and Control communication (C&C) 5.Search user's information
6.Encryption
7.Extortion and financial claiming


**Fig:Steps of Ransomware Life Cycle**

The following are some defense methods suggested by Symantec Corporation (Sherman, 2015).
A. User education: Most of the attacks occur through "Spear Phishing" attempts, that is, an unsolicited email comes with an attachment from an unknown sender. Users should be educated to properly handle such attachments, especially when the mail is from a suspicious or an unknown sender.
B. Block end users from executing the malware:This includes policies that prevent launch attempts by the files that come from compression formats, blocking auto-run, execution of files from removable devices and access to script files.
C. Limit user access to mapped devices:Most frequent ransomware variants have the capability to browse and encrypt files stored on mapped drives. Restricting user's permission to such drives will limit the ransomware's ability to encrypt.

## Proposed architecture

We propose a multi-layered architecture to detect and prevent ransomware attacks. Each layer works independently on different phases of the ransomware's execution. Process monitoring is an effective technique against ransomware that is used in many of the current tools and strategies. Even with present techniques ransomware is still on the rise, which means we still need some strategy or architecture that will enable in mitigating this increasing threat to the users worldwide.

## Architectural overview

**Layer 1:** Policies The main weakness in any system is the user itself. Creating better policies for process execution and macros extensions will help the users to know what it will do in their system. For example, other than just asking user permissions, the process functionality and detailed access requirements should be shown to the user. Furthermore, showing the URL from which it is downloaded can help the user to identify unknown processes or nefarious websites.
**Layer 2**: Creating recursive folder to detect ransomware Detecting ransomware in its early phase will avoid the risk of encrypting even a single file on the victim's machine. For this, we propose creating a recursive folder in each directory on user's system (Figure 6). We set the depth of this folder to be one more than the maximum folder depth in that directory. If ransomware passes Layer 1 then by default it has LocalSYS privileges, which means it has directory access and it can also communicate with external servers. However, on this layer, before the process is given LocalSYS privilege we give only directory access to it to see its functionality. Every process in a system is confined within maximum directory depth, i.e., they have a path associated with them that is on the system. In short, we will check whether the process is traversing our directory or not. If the process reaches the final folder in the recursive directory that means it was traversing and can be shut down before giving any other access to it. At this stage, it does not matter

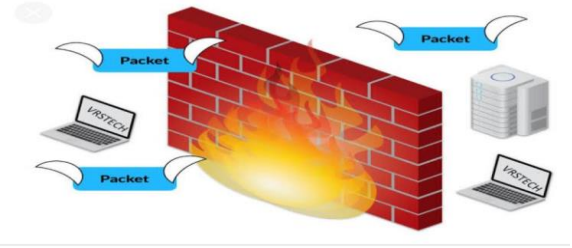
ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

even if the ransomware traverses directories on the user's system, as it will not be able to encrypt them without encryption keys that it receives from C&C server.

**Layer 3**: Process monitoring This technique is being used as a primary defense mechanism against ransomware. Once the process has passed Layer 2, it has given all the LocalSYS privileges. At this stage, we can monitor the process for behavior like how frequently it is creating handlers to access directories or its communication with external servers. Layer 4: Backup and recovery This is one of the most important aspects in recovering encrypted files. Most of the case studies that have not paid the ransom amount had their files backed up. Time plays an important role in backups, i.e., how frequently data is being backed up. Furthermore, how quickly it can be recovered is crucial. Oracle has provided a solution for frequent backups and the backup can be taken to 12 locations simultaneously. Although this is an expensive solution requiring multiple additional devices, it will solve the issue of frequent backups and once a system is compromised by ransomware, the backup machine itself can be made the primary system.

## Firewall :

In computing, a firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.




## Advantages of Firewall Security:

• Monitors Traffic: A firewall monitors all of the traffic entering your computer network.
• Blocks Trojans: A firewall helps block Trojan horses.
• Stops Hackers: Having a firewall keeps hackers out of your network.
• Stops Key loggers: Having firewall security will reduce the risk of key loggers monitoring you.

Firewall security in ransomware protection softwareAside from protection it gives, there are a lot of benefits that you can get by having a ransomware protection software.

• System Security-New strains of ransomware keep on innovating and upgrading. …
• No Downtime
• Easy Deployment
• File Recovery Provide
• Alerts
• Built-in Backup Tool
• Cleaning Utility

## Situational awareness

Situational awareness or situation awareness (SA) is the perception of environmental elements and events with respect to time or space, the comprehension of their meaning, and the projection of their future status.

## Ransomware Situational Awareness Model

The situational awareness model helps to know the real status of network and devices and facilitate the decision-making process. For this purpose, SA includes activities not only related to the identication and monitoring of specic elements or parameters but also the aggregation, correlation, analysis, and forecasting activities. The decision-making process takes advantage of historical and new data in order to execute countermeasures over the compromised environment. The SA model proposed by Endsley [10] is based on three stages as follows:

- **Perception** -This stage identies and monitors specic assets and network parameters. It also reports ordinary events as well as new incidents. The perception phase gathers raw data related to the protected system. Then, this

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

information must be organized in individual structures inorder to facilitate the management and access of it.

- **Comprehension** -Collected information is correlated and aggregated in order to simplify analysis and prediction tasks. Firstly, non-sensitive and redundant data are discarded and then a preliminary analysis is done.
- **Projection** -This stage applies analysis techniques to forecast the behavior of the system and track sits evolution. This phase takes into account countermeasures previously applied and their impact on the environment. Combining historical and current information proactive and reactive actions or responses are executed.

**Figure 2. Endsley Situational Awareness Model and Ransomware Protection & Mitigation**

Firstly, the perception layer is implemented in different tools responsible for gathering information. The obtained metrics can include C&C communications, lesystem activity, MBRcommunications, System API calls, among others. Then, the

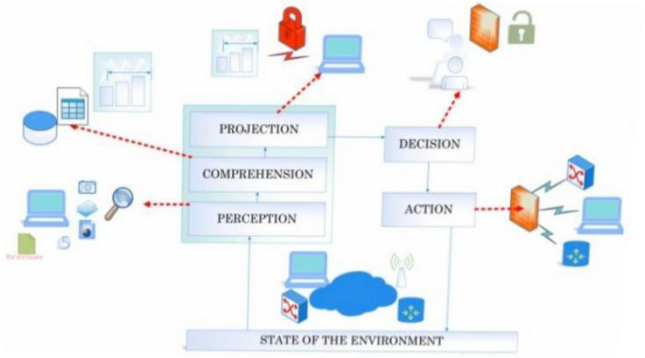


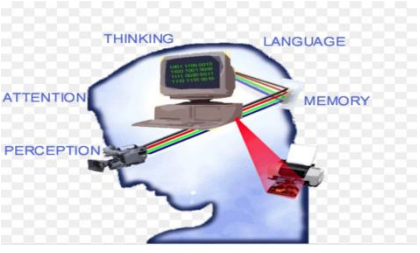
Figure 2. Endsley Situational Awareness Model and Ransomware Protection & Mitigation.

comprehension layer uses the collected data to gain knowledge about the actual situation of the monitored elements. This is achieved through the use of interpretation, evaluation, and pattern recognition techniques. Since ransomware requires to gather user information, connect to the C&C server, obtain an encryption key, search for user les, its particular behavior could be detected. In this regard, given the complexity of ransomware attacks, there is an evident need for correlating different metrics in order to identify suspicious behavior. Meanwhile, the main objective of the projection level is to take advantage of the actual knowledge of the system in order to make predictions about the future status of the analyzed elements. A reliable prediction is one of the most critical features in the context of ransomware attacks because it is difcult to recover the les once they are encrypted. Consequently, a timely and reliable prediction of a ransomware attack is fundamental to design an efcient, proactive response.

The Decision layer receives the projection ransomware alerts and establishes a response plan to avoid/mitigate the attack. The action plan depends on the access to different mitigation tools and the privileges to modify/recongure the system. For instance, it can include a new Firewall/IDSreconguration, insert a new rule in the switch to block suspicious packets, insert a honeypot in a specic network location, among others. In the Action layer, the action plan is executed. Depending on the network type, the actions can be accomplished in a specic point or in a distributed way. If the action plan is correct and the actions are correctly implemented, the State of the Environment of the system could avoid/mitigate the effect of a ransomware attack.

## Cognitive approach

The cognitive approach in psychology is a relatively modern approach to human behaviour that focuses on how we think. It assumes that our thought processes affect the way in which we behave.



ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

## Advantages of cognitive approach

The cognitive approach has a key advantage of practical and useful applications, but a key disadvantage of not being able to observe the supposed causes of behaviour. The scientific nature of the approach is one worthy of discussing as it can be both a strength and weakness, as is its reductionist nature.

**Conclusion**: Finally, this paper proposes that as the attempts of firewall were doesn't seemed in a success, so if there is a security layer in a firewall then there could be a huge impact on prevention of ransomware attack.Ransomware is one of the critical threats facing not only end users but also organizations. The number of enterprises and organizations affected by ransomware is growing and the financial losses and reputation damage are extensive. Also, the evolution of new markets and business models such as mobile communication, IoT, Cloud-based services, and the perception of anonymity provided by digital currencies have promoted the development of new variants of ransomware. Although the research community is working hard on novel methods to prevent and avoid ransomware attacks, there is a marked tendency towards the utilization of more cognitive mechanisms in order to gain real knowledge not only of end devices but also of network elements. The key idea is to find the right characteristics that have been changing in the system, allowing the identification of suspicious behavior and, consequently, the detection and prevention of threats. Ransomware attacks are not going to disappear in the medium term because they are carried out when the attacker discovers a new configuration weakness in end devices. For that reason, it is necessary to implement a progressive security strategy and discuss the legal issues in order to track this kind of attack. The community must be aware of the current situation in each country and how it could impact the third parties involved.The primary objective of the present article is to facilitate the research work in this area through the presentation of updated studies that summarize the current investigations and show a holistic ransomware view. For this purpose, a complete description of the ransomware evolution, its life cycle, and its relation with the Situational Awareness concept are presented. It includes a complete description of the ransomware life cycle from the attacker’s design and dissemination to the extortion of the victim. Similarly, a description of the common payments methods, like bitcoin, is included. Moreover, in order to facilitate the testing phase of future investigations, a detailed summary of several parameters that have been evaluated in the current research is introduced. To the best of our knowledge, the present contribution is the first work that covers this aspect. Furthermore, an updated state of the art in prevention, detection, and protection, as the main areas related to minimizing the impact of ransomware threats, is presented. The work concludes with an analysis of the main challenges and hot topics in the ransomware research field.The internet has become a strategic ecosystem for different human activities, such as production, communication, entertainment, and economy, among others. Therefore, building and maintaining a secure digital network environment are a central topic in different research areas. Despite the fact that ransomware has evolved as one of the most common cybersecurity threats, the analysis and development of new prevention, detection, and protection methods will help to reduce the attacker revenues and decrease the incentive behind this illegal activity.

**Conslusion:**

This paper gives an overview of the threat Ransomeware and proposes a model by which one can avoid the cyber attack.It also gives the complete information of life cycle of ransomeware.The paper provides information to design an efficient model which protects from cyber treats.

ISSN:0971-1260
Vol-22-Issue-4-October-December-2019

**References**:

*1. https://www.mdpi.com/2072-4292/11/10/1168/htm*
*2.www.academia.edu/Documents/in/ransomware*

*3.Stopping Ransomware Attacks on User Data*