



JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS

**PROJECT TITLE: CURBING RANSOMWARE USING FILE MONITORING
APPLICATION**

A project submitted in Partial Fulfillment of the Requirements for the award of the

DEGREE OF

BACHELOR OF SCIENCE

In

COMPUTER SECURITY AND FORENSICS

Authors:

CAVENDISH WACHERA MWANGI - I132/0857/2013

Under the Guidance of

PROF . ANTHONY RODRIGUES

DECLARATION

I hereby declare that this project report entitled
CURBING RANSOMWARE USING FILE MONITORING APPLICATION

Is written by me and is my own effort and that no part has been plagiarized without citations

STUDENT

NAME: CAVENDISH WACHERA MWANGI

REG NO: I132/0857/2013

SIGNATURE: _____ DATE: _____

SUPERVISOR

NAME: PROF. ANTHONY RODRIGUES

SIGNATURE: _____ DATE: _____

DEDICATION

I dedicate this project to my family and close friends who have shown unconditional support and provided all the help I needed to accomplish my goals.

ACKNOWLEDGEMENT

I wish to acknowledge my brother Patrick Mugambi who tirelessly helped me create my application. I acknowledge my parents for their unconditional love and moral and financial support to facilitate my project. I also acknowledge my supervisor Prof. Rodriguez for his intensive guidance and assurance I deliver what was required in the project. In addition I cannot forget to acknowledge the multiple cups of caffeine I consumed which helped me burn the midnight oil in order to achieve the goals and objectives pertaining this project.

Contents

DECLARATION	i
DEDICATION	ii
ACKNOWLEDGEMENT	iii
List of Abbreviations	iv
List of figures	v
Table of Contents	vi
Abstract	vi
CHAPTER 1	1
1.0 Background Information	1
1.1 Problem Statement	1
1.2 Objectives	2
1.3 Research Questions	2
1.4 Significance of the study	2
1.5 Delimitations of the project	3
CHAPTER 2	4
2.0 Literature Review	4
2.1 What is ransomware	4
2.2 Motives behind ransomware attacks	5
2.3 Types of ransomwares	5
2.4 Infection vectors	7
2.5 Attack methodologies	9
2.6 Anatomy of a ransomware attack	10
Phase 1: Exploitation and infection	10
Phase 2: Delivery and installation	10
Phase 3: Contacting headquarters, handshake and key generation	10
Phase 4: Destroying Backup	10
Phase 5: File Encryption	10
Phase 6: Extortion	10
2.7 Effects of ransomware attacks	11
2.8 File System Activity	12
2.9 Psychological Aspect of Ransomware	13

CHAPTER 3	18
3.0 Methodology	18
3.1 Types of System Development Life Cycle (SDLC) methodologies	19
CHAPTER 4	21
4.0 System/Software Development	21
4.1 Analysis and Requirements	21
4.2 Design	22
4.2.2 Deployment model.....	25
Phase 1: Launching ransomware sample on a set of documents	25
Phase 2: Capturing of I/O Request Packets generated.....	25
Phase 3: Capturing Master File Table (MFT) entries	25
Phase 4: Notifications upon detection of malicious file changes	26
Phase 5: Response Tactics	26
4.3 Implementation.....	26
4.4 Testing.....	27
4.4.1 Unit Testing.....	27
4.4.2 Integration Testing.....	27
4.4.3 System Testing.....	27
CHAPTER 5	29
5.0 Findings.....	29
5.1 Hypothesis.....	30
CHAPTER 6	31
6.0 Conclusion.....	31
6.2 Recommendation	32
REFERENCES.....	33

Abstract

Most organizations and consumers all over the world are running losses in hundreds of millions due to the quick emergence of one of the most dangerous cyberthreats which is the ransomware. Ransomware is the technology and modern enabled way of extortion a subject that affects people across the globe on a very large scale. Being the most profitable type of attack with added modules like Ransomware-as-a-service, the number of attackers has significantly increased and cybercriminals with little skills are able to target innocent users in order to make money. Chapter1 of this project gives background information on ransomware attacks and addresses the specific problem of the ransomware attack on the file system. It also contains the objectives of the project, importance of the project as well as its limitations. Chapter 2 of this project gives a brief history of related methods used to curb ransomware attacks, as well as the statistical figures of the impact of the ransomware attacks on the sectors of the economy. In addition motives behind ransomware attacks, types of ransomware families, infection vectors, attack methodologies, anatomy of a ransomware attack, file system activity and the psychological aspect of ransomware are discussed. Chapter3 of this project highlight the methodology used to develop the project and Chapter 4 explains the different system requirements design models used to develop this project. Chapter 5 discusses the findings acquired after the application is implemented. Chapter 6 concludes the project and gives recommendations for future works.

CHAPTER 1

1.0 Background Information

No one is safe. Cybercriminals are always fast, smart and impressively adaptive and are always on the outlook for new techniques and tricks and opportunities to compromise and make damage. Ransomware is a piece of pernicious software that exploits a user's computer vulnerabilities to sneak into the victim's computer and encrypt his or her files; then the attacker keeps the files locked unless the victim agrees to pay a ransom. The main motive behind ransomware attack is and has always been for profit purposes. Victims are infected when they unknowingly download ransomware from compromised websites, spammed email and other malwares. The most common types of ransomwares are those that lock up a victims computer screen and only unlock it once the ransom is paid and the other type is the one that encrypt victim's files and information and decrypts it upon payment. Data encrypted is locked using strong, often unbreakable encryption which leaves most victims with no other choice but to pay up the ransom. Despite the fight put up by the anti-virus, anti-malware and anti-ransomware companies it still poses a challenge due to the increase in the creation of new ransomware families which they are unable to keep up with. Payment is made through bitcoins which promote anonymity since they are hard to trace and this has led to many attackers cashing in for the ransomware business.

1.1 Problem Statement

Ransomwares that lock up screen aren't as disturbing as those that encrypt ones data. Failure to understand clearly the attack methodology carried out on the file system structure has made it difficult to create a solution once the infection has taken place. Fighting an infection is time-consuming and expensive and there is no guarantee of getting ones data back even in the events of paying the ransom. In addition most people don't backup their files and information, thus are faced with a lot of problems once their computers are infected. Protecting systems and preventing infections is the most sure way of fighting ransomware thus there is need for an application that can offer an analysis environment to enable monitoring and preventing suspicious file changes that can be brought about by the infection.

1.2 Objectives

Main Objectives

-To create a proper model of ransomware prevention by creating an application that will monitor abnormalities on the changes in a file system.

Specific Objectives

-Describing how a malicious process interact with the file system in order to gain a better understanding on how ransoms infect file systems

-Investigate the common characteristics of ransomware attacks from a file system perspective regardless of the technical differences the attack happens; capturing execution sequences I/O Request Packets and Master File Table.

-To reduce the chances of fighting infections caused by the ransomware attack.

1.3 Research Questions

1. How does ransomware attack take place?
2. What does the ransomware do to the file system?
3. How can we prevent the ransomware attack from taking place?

1.4 Significance of the study

This research project will provide a deeper and clearer understanding of analogy of ransomware attack on the file system thus enabling implementation of a proper prevention measure. The research project will thus reduce the chances of ransomware attacks from taking place. By offering a platform to analyze a ransomware's infrastructure, this research project will provide more material for analyzers involved in the fight against ransomware. By this there is a chance its trend will be observed thus stronger prevention measures will be created. Designing effective defense mechanisms is not practically possible without having an insightful understanding of these attacks.

1.5 Delimitations of the project

Capturing I/O Request packets require execution of low level operation for the purposes of accessing all object of an operating object through privileged kernel mode. This was not achievable since I created my application using C# programming language which requires high level operations.

CHAPTER 2

2.0 Literature Review

2.1 What is ransomware

Ransomware is no longer just a scareware. It has gone a long way from just issuing empty threats and is now known for its data-kidnapping capabilities and file-encrypting abilities. This is a malware that prevent or limit users from accessing their computers or even files. They then force the victims to pay ransom usually in the form of Bitcoins before they can access back.

2.1.1 How big is the ransomware problem

The earlier variants of ransomware started by mainly preying on individuals but have since become a huge threat to even the largest organizations. Small businesses, individual and government agencies have been seen giving in to the ransom demand just to get back their files and systems.

Back in 2013, Russia suffered 250,000 instances of ransomware attacks; a 100% increase from 2012. Between September 2015 and April 2016 over 100 million ransomware threats were blocked with an approximated number of 50 different families of ransomware being discovered. In addition an approximated figure of \$325 million was lost due to the attacks in 2015.

A report generated by AVAST security software showed that users encountered ransomware-infected websites 18 million times. Upon analyzing an attack for a month, they discovered that the ransomware infected around 5,700 computers per day amounting to 68,000 computers in a month. The ransomware charged \$60-\$200 for users to regain access to their files. In addition 2.9% of the victims paid the ransom; that's roughly 168 victims per day. For instance the CryptoLocker ransomware and its variants extorted \$100 million from its victims in just 10 months.

Infection numbers are significantly increasing too and so have the ransomware families amounting to 100 families in 2015. The average ransom demanded today has jumped to \$679 from \$294 in 2015.

Curbing Ransomware Attacks Using File Monitor Application

The most affected business sector is the services sector with 38% of organization infected, 17% in the manufacturing sector along with Real Estate, Insurance and Finance. Public Administration is at an estimated 10% infection. In addition Retail trade has 4% infection, mining at 1%, Agriculture, Forestry and Fishing at 1%, Construction at 4%, Wholesale Trade at 9% and Transportation, Communications and Utilities at 7%. A large number of cybercriminals have been able to acquire their ransomware, even those with low levels of expertise due to the rise of ransomware-as-a-service (Raas).

Regionally, US is the most affected with 28% of global infections followed by Canada(16%), Australia(11%), India(9%), Japan(4%), Italy(4%), UK(3%), Germany(2%), Netherlands(2%) and Malaysia(2%).

2.2 Motives behind ransomware attacks

The ultimate goal of ransomware attacks is to get money from victims, which is why the payment method is an important aspect. Reliable payment methods should contain the following properties: difficulty in tracing the recipient of the payment and the ease of exchanging payments into a preferred currency. Online payment systems such as MoneyPak are used since they provide limited possibilities to trace the money because the services aren't tied to any banking authority and the owner of the money is anonymous. The other payment method is through bitcoins. The transactions are cryptographically signed messages that exemplify a fund transfer from one public key to another and only the corresponding private key can be used to authorize the fund transfer.

2.3 Types of ransomwares

New families of ransomware are appearing every month due to the shifting of the ransomware landscape. In addition older ransomware families are disappearing with the emergence of the new threats. The following are several but common ransomware families as well as their attack methods:

2.3.1Locky

Being the most prolific variant created and having emerged in February this year, locky encrypts a victim's data and offer instruction on how to acquire the decryption program. Ransom rates were \$200-\$400 (0.5 to 1 bitcoin).

2.3.2CryptXXX

This ransomware emerged in April primarily spread by compromised websites that redirected users to exploit kits. CryptXXX gathers bitcoin wallet data and sends it to the attackers. CryptXXX asks for a ransom of \$500.

2.3.3Cerber

Managed to make a significant impact due to its ransom rates when it emerged in March this year. One of its novel features is reading the ransom note aloud to the victim using a text-to-speech (TTS) module. Its ransom rate stood at \$513 to \$1,026.

2.3.4Reveton

Mostly referred to as the police Ransomware because of impersonating local police.

Other types include:

- BitCrypt
- CRIBIT
- FAREIT
- Critroni or Curve-Tor-Bitcoin Locker

2.4 Infection vectors

Ransomware can infect a computer in multiple ways broadly explained as follows:

Malicious Email

This is one of the most common methods of spreading ransomware especially through spam email. The email use social-engineering tactics to trick and deceive recipient. Infection occurs in several ways; ransomware installs directly when a malicious attachment is opened, upon opening a malicious attachment a second-stage delivery is initiated through a downloader which subsequently downloads and installs the ransomware and lastly upon clicking a link which points to an exploit kit which ultimately leads to the ransomware being installed on the computer. The email poses as an important email from a known organization. Individual spam variation relies on recipient's inherent to act on messages that appear to be urgent. In addition, the attack succeeds as it exploits the primeval urge to explore the unknown inherent in human nature. Careless clicking on links and attachments remains the most common infection vector.

Exploit Kits

Being the second predominant method, they take advantage of vulnerabilities (especially favor zero-day vulnerabilities) in softwares in order to install ransomware. For instance they compromise web servers and inject iframes into the web pages hosted which then direct browsers to the exploit kit servers. The kits rely on users running outdated softwares on their computers who unfortunately are an overabundance. Attackers redirect users to the exploit kit in several ways like malicious social media post, malvertisement and redirecting web traffic. In most cases cybercriminal pay Exploit Kit operators to propagate ransomware. Due to this threats served by each kit change over time. For example the Neutrino Exploit Kit distributed the CryptXXX ransomware and Magnitude delivered Cerber.

Infected removable drives

These include USBs and portable hard drives. Malware spreads through removable storage if a user uses the same device for multiple computers.

Program and server vulnerabilities

Includes weaknesses caused by other forms of malware already infecting the machine and browsers or operating systems that haven't been updated recently. Also vulnerable softwares running on servers.

Infected software bundles

Some applications have bundles with malware including browser toolbars, software key generators, and instant messenger applications, third-party executable files especially from non-trusted sources and files shared through peer-to-peer file sharing sites.

Malvertising

Malicious ads are distributed through trusted websites with a high volume of visitors who by simply loading the web page hosting the malvertisement redirects to an exploit kit leading to an infection. Malicious components of ads are short lived and once removed; traces of its presence disappear.

Brute-forcing passwords

Attackers have also turned to a way of brute-forcing login credentials of software used on servers. A good example is the criminals behind the Bucbi ransomware who used this method to gain access to remote desktop protocol servers.

Self-propagation

Some ransomware infect removable drives with a copy of itself before it starts encrypting thus increasing its chances of spreading to other computers. For example the ZCrypto ransomware and Cryptorbot ransomware.

SMS messages and untrusted-party app stores

Some ransomware threats spread through SMS messages like the android ransomware. They can also make it onto a device through untrusted third party app stores.

2.5 Attack methodologies

The methods used to attack systems by ransomware have advanced over the years to more sophisticated methods as you will see below. The attack methodologies entail:

- Copying of different types of files to hidden folder producing a pseudophase to deceive the victim.
- Linking all selected file to 1 file and deleting the original files followed by the creation of a text file with instruction on how to get back the files directing how the decryption key can be received.
- Encrypting certain files and threatening to destroy them by a deadline. For instance notification windows that pops up to distract a victim and bluff of deleting a file every half an hour.
- Another methodology is compressing document files, multimedia files and database files into a password-protected ZIP file after overwriting them before leaving a notification.
- Targeting of the Master Boot Record preventing the operating system from loading and displays a notification.
- Impersonating local police and informing victims that they have been caught doing illegal activities online. Mostly adapt their messages depending on the users GPS location. For instance an infected American computer displays a message from FBI.
- Locking the screen of the infected computer preventing it from booting up and preventing detection by behavioral monitoring tool and projecting a ransom message or notification.
- The other methodology which also adds as the most common to be used today is encrypting all file using algorithms such as RSA that are becoming stronger and unbreakable as time moves on and also deleting backup files to prevent restoration of encrypted files.

2.6 Anatomy of a ransomware attack

There are several stages that take place in order for ransomware attack to be fully carried out and they are as follows:

Phase 1: Exploitation and infection

For an attack to be successful, the malicious ransomware file needs to be executed on a computer. This is mainly done through the common infection vectors like phishing emails and exploits kits.

Phase 2: Delivery and installation

The ransomware executables are delivered to the victims system. Upon installing itself, the ransomware sets keys in the windows Registry to start automatically every time the victim's computer boots up.

Phase 3: Contacting headquarters, handshake and key generation

Before the ransomware can attack it contacts a command and control server operated by the attackers that owns it. Ransomware client and server identify each other through a handshake and thereafter the server generates two cryptographic keys. One key is kept on the victim's computer while the second key is stored securely on the criminals' server.

Phase 4: Destroying Backup

The ransomware targets the backup files and folders on the victims system and removes them to prevent restoring; a unique feature of ransomware as compared to other type of malwares. On the light of this action, some ransomware do not spoil the backup but do so as a way of scaring the victims into paying the ransomware.

Phase 5: File Encryption

With the cryptographic keys established and the backup completely removed, the ransomware starts encrypting every file it finds with important productivity and file extensions like .doc, .xls, with a key for each file and then writes the encrypted key at the beginning of all files.

Phase 6: Extortion

With the encryption dirty work done, the demand instructions for extortion and payment are presented as the ransomware displays a screen giving the victims a time limit to pay up before

the decryption key is destroyed. The payment is made in untraceable bitcoins or other electronic payment methods. The victim purchases bitcoins and transfers it to the attacker's bitcoin address. The victim then sends a transfer ID to the attacker as proof of statement who then sends the decryption key and instruction to the victim. However it is important to note that paying the ransom does not guarantee that the victim will regain access to his or her file and system. Instead this can encourage the attackers to extort more money from the victim. In addition to that, ransomware authors are usually not the best software developers thus their code may contain a number of flaws such that the compromised data can crash for good.

2.7 Effects of ransomware attacks

Organizations may be forced to shut down their system to deal with the infection. The organizations services may be impacted thus affecting the customers. In addition the organization will experience financial losses and reputation damages.

Organization may be hit with large legal bills if customers are affected. Also they may have to pay for incident-response and other-security solution once the attack has taken place. Penalty and fines due to violation of policy like HIPAA can apply to health institutions like hospitals

Loss of records, customers' personal information or intellectual property can impact an organization's brand, finances and reputation. Even if a victim pays the ransom and the files are decrypted, there is still a risk that data may be corrupted during the decryption process. Attackers can also threaten to post the stolen data online in order to extort more money from the victim.

Upon a ransomware attack, patients' records including medical history may be inaccessible leading to delays in treatment or even administration of the wrong medication.

2.8 File System Activity

In this report I am going to analyze broadly what happens to a file system when under a ransomware attack happens; how the malicious malware interact with the file system. By this I will be able to analyze common characteristic of ransomware attacks from a file system perspective and also be able to distinguish multiple attack strategies used by some of the ransomware families

File level activity is a common characteristic of ransomware samples that target users file. Monitoring interesting function calls. Register callback routines to capture all types of I/O Request Packets generated on behalf of processes to access the file system as well as monitor changes in Master File Table (MFT). Different call backs routines allow us to capture the entire read, write and attribute change requests to the file system. Malicious processes generate requests to access file system is significantly different from benign processes. Attackers use both customized (decreases the chances of being easily detected by common malware analysis techniques) and standard cryptosystem to encrypt users' data. In order to minimize the chances of recovering the original data, most ransomware families carry out both encryption and deletion mechanisms.

Encryption mechanism

Some families use windows function to perform their encryption; they call *CryptEncrypt* with a handle to the encryption key and a pointer to a buffer that contains the plaintext to be encrypt. Plaintext in the buffer is directly overwritten with the encrypted data created by the function. I/O manager generates IRP_MJ_CREATE on behalf of the malicious process to open the users' files. File content is read via IRP_MJ_READ for encryption and is overwritten with the cipher text buffer using the IRP_MJ_WRITE function each time a file encryption occurs.

Another method of attacking a file other than the standard cryptosystem; Ransomware 1st generates an encrypted version of a file using an AES-256 encryption key and then overwrites the original files data with the encrypted file. The encrypted file is then encrypted using a 1024-bit RSA public key.

In NTFS file system, file has an entry in the Master File Table (MFT) that reflects the changes of the corresponding file or folder core file attributes can be found in the STANDARD_INFORMATION attribute and \$DATA attribute that contains the content of the corresponding file. A significant number of changes occur in a very short time in MFT entries with encrypted content in the \$DATA files attribute of files that do not share the same path. A malicious MFT entry is a MFT entry that is generated/ modified in a system under a ransomware attack.

In order to distinguish between benign and malicious file system activity, defining a file system activity model that reflects the normal interaction with the file system is possible. In addition a classifier can be trained on benign and malicious MFT entries to detect abnormal file system activities when the system is under an attack. A system with protection capabilities can intercept all requests and discard the suspicious requests before they reach the file system driver.

2.9 Psychological Aspect of Ransomware

Ransomware operation is simple. Through the years, ransomware has tremendously developed into a very effective cyber threat that no longer just “scares” its would-be victims with a locked screen but a notorious malware that knows the weak points of its targets. Online threats are evolving to rely more on mastering the psychology behind each scheme than mastering the technical aspects of the operation. Psychological aspect of ransomware makes the problem so malicious and increases its success rate. The understanding of the victim’s psyche has largely contributed to the spread and effectiveness of ransomware which has consistently banked on exploiting its victims fear to make for an effective extortion scheme. Fear is used as a major component of the scheme, as it has proven to be effective in the past and still remains the biggest factor for its success. The ransomware variants take advantage of its victim’s fear, prodding them to pay the ransom instead of having to find an alternative solution. Police Trojan incited fear among its targets by feigning legitimate federal law violation warnings to trick users into clicking on a poisoned link.”When people see the ransomware notice on their work PC, they panic afraid they might lose their job. They think it’s their fault for triggering the attacks so they pay.

Ransomware developers have developed a variety of ways to convince users that paying the ransom is the best option. Take for instance, time-based threats. Some ransomware involve a timer showing how much time the victim has left to pay the ransom. To further heighten the sense of urgency, each hour of failure to pay the ransom leads to a deletion of a portion of the victims file. Some ransomware also use shame to coerce users into paying the ransom. For example a particular sample used a locked ransomware that said “YOU ARE A PORN ADDICT” disrupting a victim in a certain way and they’re more likely to pay up. Given that lives are on the line when a hospital’s system is locked down, the hospital has limited choices. It cannot waste valuable time safely removing the malware so its often forced to bite the bullet and pay the ransom in the name of patients.

To understand how ransomware attacks can succeed in extracting payment from a rational population, we must consider some of the behavioral, economic, psychological and social-engineering techniques used in ransomware.

Deception

The human cognitive mechanism is known to take representational shortcuts (assumptions that we generally hold to be true) in order to gain efficiency. Deception is designed to exploit this tendency in the cognitive system. The use of legitimate-looking themes such as those mimicking law enforcement agencies helps to deceive victims.

Central and peripheral route to persuasion

The Elaboration Likelihood Model (ELM) proposes that there is a central route and a peripheral route to persuasion. With persuasion through the central route, an individual is persuaded through careful and thoughtful considerations of the merits presented. With peripheral persuasion, an individual is persuaded through associations with positive or negative cues in the stimulus. Positive associations may be that of a reward for carrying out some action, while a negative association is the threat of punishment for not complying.

Authority & social compliance

Society has trained people to behave in accordance with established patterns and norms, such as trusting and obeying known authorities like the police. The use of nationally localized law

enforcement themes along with other relevant authority cues makes the extortion demand seem all the more real.

Visceral triggers

The accusation of committing a crime and the authorities knowing their location can provoke an intuitive reaction of fear within a victim. This can influence the victim's cognitive information processing and their decision-making abilities, making it less likely that they will make a rational decision when it comes to the ransom payment.

Influence of framing

The way in which a risk is framed or described can influence the individual's perception of risk. Prospect theory is a behavioral economic theory that states that people make decisions that are risk-averse over prospects involving gains, while they become risk-loving over prospects involving losses. This means people are more likely to take risks when they are given a proposition that plays up risk of losses. False messages threatening the deprivation of liberty for 5 to 11 years are designed to take advantage of these human characteristics and could unduly influence a victim into paying the ransom.

Dishonesty principle

If you have broken the law, it can be used against you. With ransomware messages threatening prosecution for "downloading of pirated music, video, warez", some victims are less likely to seek help from others or to contact law enforcement once they realize they have been scammed

Preference for confirmatory rewarding information

Information search bias describes a tendency for individuals to seek information that confirms their initial hypothesis, rather than seeking out information to disprove it. This has been found to be a persistent human error and reduces the quality of decision outcomes. After the initial shock of seeing the ransomware message, victims may erroneously seek out information to confirm the existence of the organizations and laws presented in the ransomware messages, rather than trying to disprove the claims. This can lead to a bias and influence the decision to make a ransom

payment. Since most people are not legal experts, they can be confused and, instead of seeking help, resort to paying the ransom instead.

Ransomware relies more on the users' sentiments towards the encrypted data and what effect the loss of this information might have.

Time

Time pressure has been shown to influence the decision strategy used. When under time pressure, an individual is more likely to reduce the cognitive resources available for an analytic judgment. Crypto ransomware employs time-pressure tactics accompanied with temporal monetary penalties in an effort to force payment of the ransom.

Endowment effect

As a result of ownership, people ascribe more value to their own possessions. This can lead to people paying more to retain something they already own rather than obtaining something owned by someone else. For example, having a victim's personal photos encrypted by ransomware could potentially invoke this effect.

Loss aversion

People have a stronger tendency to avoid losses than to acquire gains. If a victim is unsure what risks are associated with the loss of their information, it can lead to loss-aversion decision-making which increases the likelihood of the victim making the ransom payment

Sunk costs

Sunk costs influence decisions and can lead to irrational behavior because individuals are prone to loss aversion and framing effects. If a victim's personal work which they have invested a lot of time and effort into has been encrypted and is threaten with loss, it can unduly influence the ransom payment. The decision-making process in this case is a tradeoff between the value of the work that is potentially lost versus the ransom amount.

Ellsberg paradox

This is the idea of how people make decisions under conditions of ambiguity or uncertainty. Basically people overwhelmingly prefer and will choose known probabilities of winning in risky situations. Without fully knowing how the loss of data might affect a victim, they may opt for the safer probability of paying the ransom to get their data back. In ransomware situations, the victim is potentially faced with two unequal probabilities. On the one hand, they are unsure about whether they would actually get the data back even if they paid the ransom. On the other hand, they could be even more uncertain about how the loss of data would impact them. Faced with these unequal uncertainties, people have a tendency to choose the option that they perceive to have a more definite outcome.

Fear of regret

When faced with an ambiguous decision, individuals may take into account the possibility of feeling regret and may attempt to reduce this possibility through the choice that they make. Fear of regret around the possible loss of data may influence any decisions around the ransomware payment.

Anxiety, risk and decision making

It has been shown that surges in anxiety can be correlated with surges in general risk perception, which can lead to errors in risk assessment. A victim's anxiety around the potential loss of data may affect their risk perception and assessment, leading to a higher probability of paying the ransom demand.

CHAPTER 3

3.0 Methodology

The methodology used in this project is **System Development Life Cycle (SDLC)**. The phases of SDLC and their potential deliverables are:

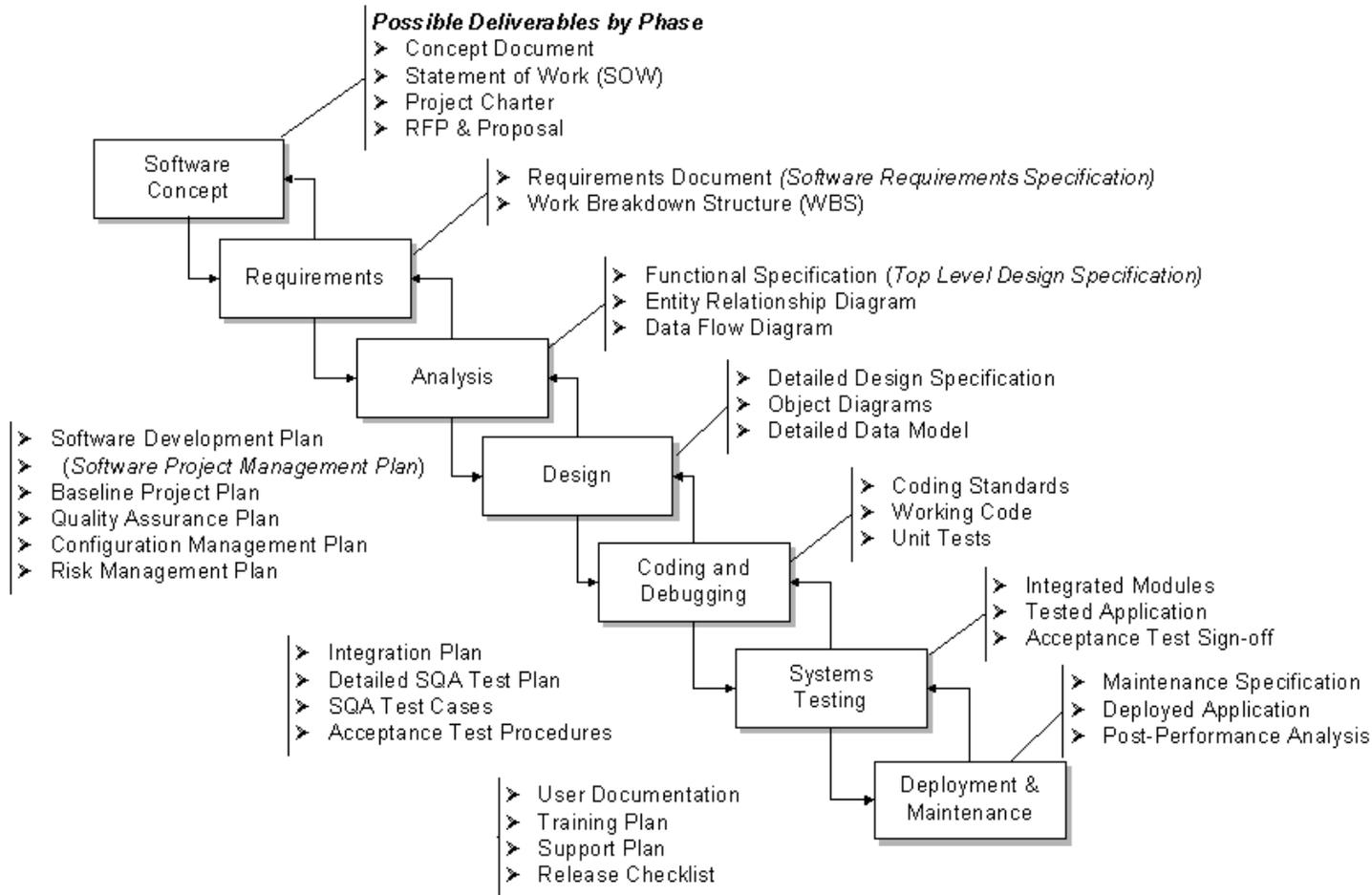


Figure 1 Phases of the System Development Life Cycle (SDLC)

3.1 Types of System Development Life Cycle (SDLC) methodologies

Waterfall model

Progress is seen as flowing steadily downwards through the phases of software implementation. Any phase in the development process begins only if the previous phase is complete.

V-shaped model

Is an extension of waterfall model; instead of moving down in a linear way, the process steps are bent upwards after coding phase to form the V shape.

Evolutionary prototyping Model

Incomplete versions of the software program are developed and evolve into the final system through iterative incorporation of user feedback.

Spiral Method (SDM)

It combines the features of the prototyping model and the waterfall model. Favored for large, expensive and complicated projects.

Iterative and incremental Method

Entails developing a system through repeated cycles and in smaller portions at a time, allowing developers to take advantage of what was learned during development of earlier parts.

Extreme programming (Agile development)

It is based on iterative and incremental development where requirements and solutions evolve through collaboration between cross-functional teams.

3.2 Methodology Used for this project

The type of methodology used for this project is **Agile development**.

Reasons for this are because agile development decreases the time required to avail the system features. It offers room for continuous inputs which leaves no room for guesswork and the end result is a high quality application. The working application is delivered frequently in weeks

rather than month. In addition there is regular adaptation to changing circumstances as even late changes in requirements are welcomed.

As an agile development method, Scrum methodology will be implemented. Scrum is the leading agile development method for completing projects with an innovative scope of work

Scrum process



Figure 2 Tasks are done in sprints

CHAPTER 4

4.0 System/Software Development

4.1 Analysis and Requirements

4.1.1 System requirements

Hardware Requirements

- A computer for the purposes of launching both the ransomware variant and the file monitoring application.

Software requirements

- Ransomware variant to launch in the analysis environment.
- Handler application to capture I/O requests.
- FileSystemWatcher to monitor for file changes.
- A specific folder containing the files and documents to be monitored.

4.1.2 Compatibility

The application is currently compatible with Windows Operating System

4.1.3 Programming Language

The application was developed using C# programming language.

4.1.4 Development Platform

The application was developed with Visual Studio application

4.2 Design

4.2.1 Architectural design model



Figure 3 User Interface Design

Components

Live monitor

Entails a radar scans that scans for changes that occur in the file level activity both benign and malicious. Also detects occurrences of abnormal changes and alerts the system if any are founds.

Reports

Displays the neutralized threats that have been detected and are associated with abnormal changes in the file systems.

Logs

Collect and stores logs of the actions executed by the application for later analysis. In addition there is also zip samples of the ransomwares detected and neutralized.

4.2.2 Activity Diagram

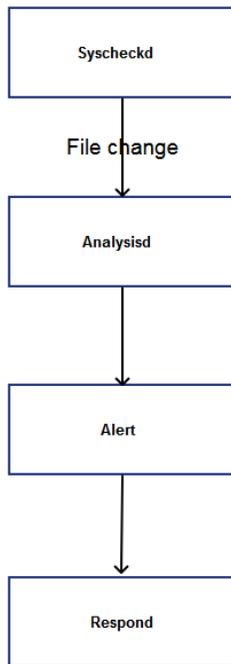


Figure 4 Activity Diagram

Syscheckd

There is a define file system activity model that reflects the normal interaction with the file system. In addition there is a file watcher that keeps a look out for abnormal or suspicious file changes.

Analysisd

Decoding and analyzing of the noted file change is carried out. There exists an analytics engine that has a classifier that has been trained on benign and malicious MFT entries and IRP generation to detect abnormal file system activities

Alert

The application notifies the system of detected threats by producing reports after abnormal file changes have been detected

Respond

This module intercepts all requests and discards the suspicious requests before they reach the file system.

4.2.3 Use Case diagram

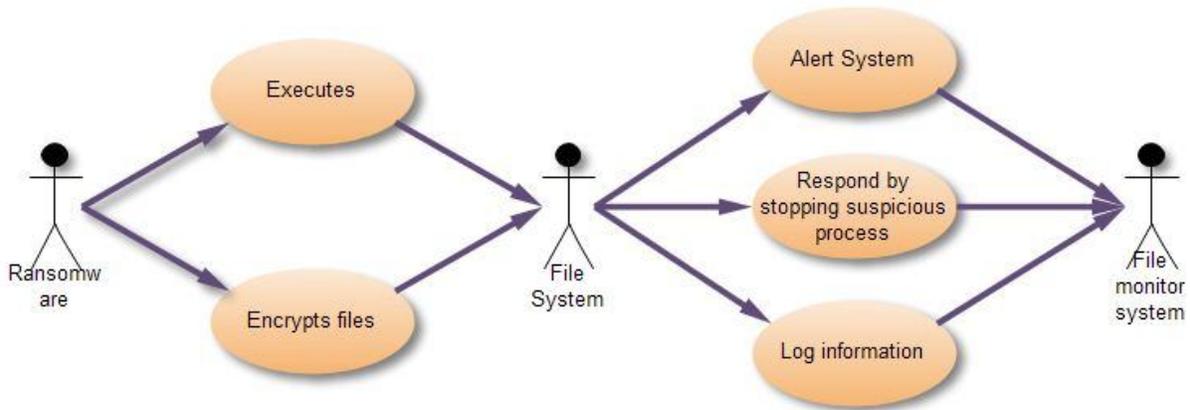
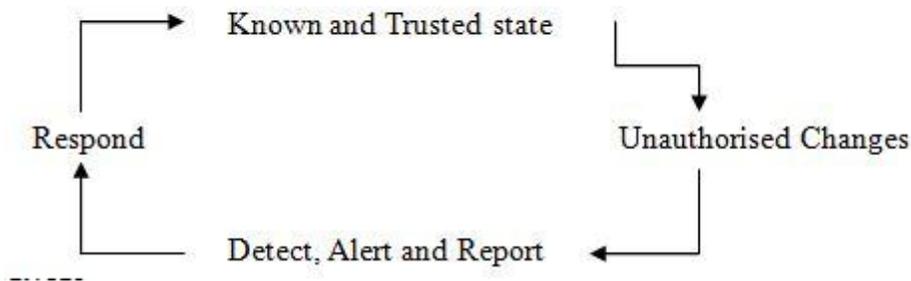


Figure 5 Use Case Diagram

The actors are the ransomware variant, file system and the file monitoring system and the use case showcase the activities carried out by the ransomware and those carried out by the file monitoring system on the file system

4.2.4 Design Pattern



4.2.2 Deployment model

Phase 1: Launching ransomware sample on a set of documents

This phase entails launching a sample ransomware to a sample set of a file system in order for the attack to take place which will entail encryption and deletion mechanisms.

Phase 2: Capturing of I/O Request Packets generated

Access to file resources by a user generates I/O Request Packets thus this phase will entail acquiring the I/O Request packets generated when a file system is under a ransomware attack in terms of frequency of generation and the type of request generated.

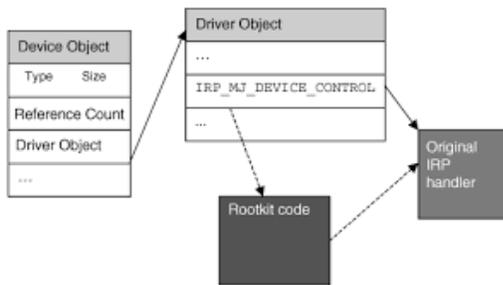


Figure 6 I/O Request Packet

Phase 3: Capturing Master File Table (MFT) entries

This phase will entails monitoring of the Master File Table entries generated when a file system is accessed and changes are made. In this phase malicious Master File Table entry generated will be captured.



Figure 7 Master File Table of a file system

Phase 4: Notifications upon detection of malicious file changes

This phase will entail alerting the system upon detect of a suspicious file change by the classifier in the analytics engine in terms of the types of IRPs generated by malicious processes and generation of malicious Master File Table (MFT) entries.

Phase 5: Response Tactics

This phase will entail neutralizing threats detected by killing the suspicious process before they attack the file system driver. This phase will also entail generating logs of the activities carried out by the file monitor in terms of the ransomware sample stored for the purposes of later analysis. In order this phase will also entail archiving of the reports generated when a threat is detected.

4.3 Implementation

4.3.1 Risk Mitigation

The ransomware variant is launched on a specific folder to avoid spread of risks to other folders within the drive.

The risk mitigation options implemented by the program are:

- (i) **Watch/Monitor** - Monitor the environment for changes that affect the nature and/or the impact of the risk.
- (ii) **Avoid** - Adjust program requirements or constraints to eliminate or reduce the risk.
- (iii) **Control** - Implement actions to minimize the impact or likelihood of the risk.

4.3.2 Programming language used

C# is faster to develop in and it is full of features that make development faster and easier, usually at the cost of flexibility and runtime performance. It is an object oriented language that allows one to build a breadth of applications.

4.3.3 Development tools

- (a) Pencil application – for creation of User Interface Design.
- (b) Visual Studio – for coding the file monitoring program.
- (c) Edraw Max – for drawing the activity diagram and use case diagram

4.4 Testing

4.4.1 Unit Testing

Verifies modules function properly. Done by the development Team.

	Components tested	Status
(i)	Live monitor radar	Working
(ii)	Archive report button	Working
(iii)	Reports window	Working

4.4.2 Integration Testing

Ensure that code is implemented and designed properly.

	Components tested	Status
(i)	FileSystemWatcher class	Working
(ii)	Handler application	Working

FileSystemWatcher listens to the file system change notifications and raises events when a directory files in a directory changes. This component watches files in a specified folder (AAAAFld) in Local Disk C. For each file system request, we collected the process name and process id of the operation. Handler application captures the process name and process id of the malicious process

4.4.3 System Testing

Ensures that the system does what the requirements specify.

	Components tested	Status
(i)	Alerting of threats seen	Working
(ii)	Displaying the number of threats	Working
(iii)	Neutralizing the threats	Working
(iv)	Zipping of ransomware samples	Working



Figure 8 Testing all system components

Curbing Ransomware Attacks Using File Monitor Application

Name	Date modified	Type	Size
 notepad_Sample_Ransomware.zip	12/4/2016 3:45 PM	WinRAR ZIP archive	37,427 KB
 RansomwareProj_Sample_Ransomware.zip	12/4/2016 4:55 PM	WinRAR ZIP archive	76 KB

Figure 9 Zipped malware samples.

CHAPTER 5

5.0 Findings

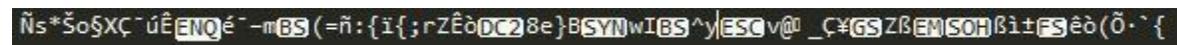
The ransomware sample captured generates an encrypted version of a file using an AES-256 encryption key and then overwrites the original file's data with the encrypted file. In most cases when files are encrypted using AES 256 encryption algorithm, the decryption key is generated with the same machine so if found, it can be used to decrypt the encrypted content. To prevent this from happening, attackers encrypt the decryption key using a unique key found on their servers which they trade for with ransom.

```
public void encryptFile(string filePath,string encryptionKey){
    //convert file to byte array and key to bytes too
    byte[] encryptable = File.ReadAllBytes(filePath);
    byte[] encrypted = null;
    byte[] keyBytes = Encoding.UTF8.GetBytes(encryptionKey);
    byte[] salt = new byte[] {1,5,6,2,8,2,5,8,4,6,5,7,4,2,1};
    //create a hash for the key
    keyBytes = SHA512.Create().ComputeHash(keyBytes);

    using(MemoryStream memStream = new MemoryStream()){
        using(AesCryptoServiceProvider aes = new AesCryptoServiceProvider()){
            aes.KeySize = 256;
            aes.BlockSize = 128;
            var key = new Rfc2898DeriveBytes(keyBytes, salt, 1000);
            aes.Key = key.GetBytes(aes.KeySize / 8);
            aes.IV = key.GetBytes(aes.BlockSize / 8);
            aes.Mode = CipherMode.CBC;
            using(var cryptoStream = new CryptoStream(memStream,aes.CreateEncryptor(),CryptoStreamMode.Write)){
                cryptoStream.Write(encryptable,0,encryptable.Length);
                cryptoStream.Close();
            }
            encrypted = memStream.ToArray();
        }
    }
}
```

Figure 10 AES Encryption algorithm used by the ransomware sample

In addition, the ransomware changes the filenames entirely. A file encrypted by this ransomware looks like this:



Ñs*Šo\$XÇ`úÊ[ENQ]é`-mBS(=ñ:{i{;rZÊò[DC2]8e}B\$YNwIBS^y|ESCv@_C¥GSZBEMSOHβi±FSêò(Ö·`{

Figure 11 Contents of the encrypted file

5.1 Hypothesis

On I/O Request Packets, the ransomware sample, calls CryptEncrypt with a handle to the encryption key and a pointer to a buffer that contains the plaintext to be encrypted. The plaintext is directly overwritten with the encrypted data. IRP_MJ_CREATE is generated when the malicious process opens the files. File content is read via IRP_MJ_READ for encryption and is overwritten using IRP_MJ_WRITE function. IRP_MJ_SET_INFORMATION function is used to delete the original file and to also overwrite the original file with the encrypted file.

On MFT (Master File Table) file, when a file is deleted, the clusters that are used to keep the files' data are set to unallocated in \$BITMAP attribute. In addition the MFT entry is updated thus we can detect ransomware attacks that target user's files based on the changes in the MFT table.

CHAPTER 6

6.0 Conclusion

The following chapter concludes this report. A summary of the research is presented, and findings of the study are discussed and interpreted. The significance of this research in the immediate context of file monitoring is examined. Recommendations for further research end the chapter.

As per the main objective a file monitoring application was created which monitored the files in a specified folder. The application used specified file attributes to distinguish suspicious sequences and benign processes in a file system. The application was able to neutralize the noted threats and zipped them for later in depth analysis. It was also able to log the events carried out by the file monitoring application.

As per the specific objective of describing how a malicious process interacts with the file system, we launched the ransomware sample on a specified directory of files and we were able to capture the encrypted files after the ransomware attack had taken place. Furthermore we were able to have a look at the encrypted content of the encrypted files as shown in figure 9.

In relations to analyzing the characteristics of the ransomware attacks to a file system, we were able to capture the encryption algorithm used by the ransomware variant which was AES-256 encryption algorithm and carried out a further study on how it is used to encrypt the file system as shown in figure 8.

Upon analyzing the ransomware sample with a special focus on its destructive functionality which is encrypting original files, we were able to build the file monitoring application in a way that it would stop the malicious process before it preceded to the other files in the system thus reduced the chances of fighting infections. Monitoring files in a decoy folder is a multilayered type of defense against ransomware attacks which are one of the most arising threats worldwide. Either produced using little technical effort or sold as a service to those less skilled, ransomware has created negative impact in all sectors of an economy thus war against ransomware begin from mitigation strategies with minimal impact such as to an individuals' computers to those strategies with huge impact such as servers and networks of big organizations in order to ensure that the ransomware issue becomes a thing of the past.

6.2 Recommendation

We recommend creation of a way to integrate low level operation with the file monitoring application for the purposes of deploying privileged kernel mode to gain access to all objects of the operating system in order to capture the I/O Request Packets and Master File Table entries.

We also recommend future integration of the application with a classifier for the purposes of automated identification of benign and malicious processes for proper efficiency and better performance in file monitoring.

REFERENCES

1. Amin Kharraz, W. R. (2014). *Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks*.
2. Kharraz, W. R. (2015). *UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware*.
3. Atkinson, S. (2015, June). *Psychology and the hacker - Psychological Incident Handling* SANS Institute..
4. Corporations, S. (2016). *Ransomware and Businesses 2016*.
5. Dr.P.B.Pathak. (2016). A Dangerous Trend of Cybercrime: Ransomware Growing Challenge. *International Journal of Advanced Research in Computer Engineering & Technology* , 371-373.
6. Kevin Savage, P. C. (2015, August 6). SECURITY RESPONSE. *The evolution of Ransomware* , pp. 47-49.
7. Liao, Q. (2007). *RANSOMWARE: A GROWING THREAT TO SMES* , pp. 360-365.
8. Mehmood, S. (2016, April 30). *Enterprise Survival Guide For Ransomware Attacks*. SANS Institute .
9. Saiyed, C. (2016). CRYPTOLOCKER. *ISSA Journal* .
10. Thakkar, S. (2014). Ransomware - Exploring the Electronic form of Extortion. *International Journal for Scientific Research & Development* , 123-125.
11. Wisniewski, C. (2015). *CryptoLocker, CryptoWall and Beyond: Mitigating the Rising Ransomware Threat*. SOPHOS.
12. Xin Luo, Q. L. (2007). *Awareness Education as the Key to Ransomware Prevention*.