Pontificia Universidad Católica de Chile.
Facultad de Ingeniería.
Departamento de Ciencias de la Computación.
IIC3252 – Criptografía y Seguridad Computacional.
Profesor Jens Hardings.

Criptovirología y Ransomware

Cristóbal Ríos – Daniel Córdova – Fernando González.

Introducción.

Los virus han evolucionado mucho desde sus inicios, de simples bromas hasta elaboradas estafas, evolucionando su forma de infectar, payload, defensa, reproducción y ocultación. [20, 21, 22]

Además ha cambiado mucho el objetivo de los virus y el malware en general, ahora son una nueva forma de conseguir dinero. Si bien la creación de virus comenzó como un reto intelectual para los informáticos de la época, en dónde demostraban sus conocimientos frente al resto; hoy en día la mirada de la mayoría de los creadores de virus o malware no va por ese camino, sino que su prioridad principal es el beneficio financiero. [23]

Para conseguir dinero de forma ilegal se han creado diversas técnicas y amenazas, así por ejemplo hace unos años teníamos a los Dialer, y porqué no nombrar la larga historia que han tenido los Spyware. Viendo las estadísticas de hoy en día, está dando mucho que hablar el Spam, el Phishing y el malware que crean las Botnet. Así principalmente estas amenazas se dedican a obtener los datos bancarios y de las tarjetas de crédito. [20, 21, 22]

Actualmente una nueva amenaza está dando qué hablar, éste es el Ransomware, el cual secuestra los archivos, encriptándolos, y piden una recompensa por la liberación de ellos, es decir por la compra de un software o una clave para poder acceder a ellos, al más puro estilo del una película de ciencia ficción. [24]

En el siguiente documento se explicará a fondo sobre esta amenaza y el estudio de tal. Básicamente el documento se dividiremos en dos partes importantes:

Primero nos adentraremos al mundo de la Criptovirología y el Ransomware, mostrando de dónde surgió esta terminología, la historia del Ransomware y los escasos malware que se catalogan como tal, y finalmente se analizarán dos de los Criptovirus más conocidos, Cryzip y Gpcode. Luego se procede a exponer estudios recientes de los exponentes más grandes en el tema, Young & Yung quienes nos muestran ideas y métodos de crear criptovirus mas seguros haciendo énfasis en métodos criptográficos como lo son criptografía asimétrica y transmisión de información de forma segura a través de la red, las cuales genera un mundo de futuras posibilidades en esta rama.

1. Criptovirología y Ransomware.

En esta primera parte del documento se mostrará a fondo lo que se conoce como Criptovirología y Ransomware. Se iniciará el tema mostrando la terminología de éstos; seguido por la historia, en el cual veremos que no es un tema tan nuevo, y que sólo ha estado oculto por unos años, quizás perfeccionándose; a continuación se verá a fondo dos de los Ransomware más conocidos hoy en día: Cryzip y Gpcode; y finalmente se analizará lo que es el diseño de un Ransomware. En esta parte, la información, principalmente, se extrajo de los principales laboratorios de antivirus y sitios webs dedicados al malware y a la seguridad informática.

1.1 Terminología

Originalmente, el término Ransomware hacía referencia a un tipo de licencia usada para la distribución de software, donde el autor demandaba cierta cantidad de dinero para liberar el código fuente de su programa y si sus condiciones eran cumplidas, el programa pasaba a ser Open Source.

Si analizamos el término Ransomware, éste proviene el vocablo sajón “ransom”, que significa “el pago de dinero para restituir la

libertad de un ser u objeto determinado (secuestro)". Entonces, cuando lo que se secuestra, o se priva de libertad es un componente determinado a través de otros componentes de software, entra en juego lo que se conoce como Ransomware.

Por ello, un Ransomware, podría secuestrar los archivos de un usuario de 3 formas distintas:

- Enviar la información del usuario por la red a otra entidad y eliminársela de su equipo.
- Encriptar la información del usuario, de modo que ésta sea ilegible a simple vista y así necesite un software especial o una clave para poder acceder a ella.
- Ocultar la información en el mismo sistema usando un Rootkit.

No se conoce aún ningún malware que haga lo que se menciona en la primera opción, ya que se necesitaría mucho ancho de banda; y tampoco lo mencionado en la tercera opción, ya que si bien con un rootkit se puede ocultar lo que se desee, se podría obtener nuevamente la información colocando el disco duro infectado en otro equipo; por esto mismo se conoce como Ransomware al tipo de amenaza que hace lo mencionado en la segunda opción, es decir oculta la información encriptándola, y como objetivo es el de obtener dinero, ya sea mediante la compra de un producto o el depósito de una suma en una cuenta bancaria electrónica.

Por otro lado, tenemos el término de criptovirología, el cual se usa para indicar la disciplina de la informática que se dedica al estudio de los criptovirus. Un Criptovirus es básicamente un virus informático que ocupa la criptografía para su modo de operar y producir daño.

Por lo mostrado anteriormente, hoy en día usar los términos Ransomware o Criptovirus para nombrar a esta amenaza es prácticamente lo mismo, pero en un futuro próximo esto puede cambiar; por ejemplo hoy en día ya se están haciendo experimentos de Super-Worms usando la criptovorología [25]; por esto último es más correcto denominar a estas amenazas como: extorsión criptoviral o simplemente Ransomware.

1.2 Historia.

La historia comienza en 1989, donde se distribuyeron por correo postal 20.000 copias de un paquete llamado "Aids Information Diskette" a algunas direcciones de usuarios que fueron robadas de la base de datos de "PC Business World" y de "World Health Organization". El paquete contenía un diskette con un programa, con supuesta información del SIDA, que evaluaba ciertas condiciones, y cuando estas se daban, procedía a cifrar el disco rígido y presentaba una factura a la víctima, para que ésta pudiera obtener la clave de cifrado. Por el nombre del paquete, a esta amenaza se le llamó: AIDS, el cual también es conocido como PC Cyborg Trojan. [2, 3, 4, 5]

AIDS, es un troyano que reemplaza el archivo "AUTOEXEC.BAT", que además lo utiliza para contar cuántas veces a arrancado el ordenador, y una vez que éste llega al número 90, oculta los directorios y encripta los nombres de todos los archivos del disco C, dejando el sistema inutilizable. Luego de ello se le pide al usuario que "renueve la licencia" y se contacte con PC Cyborg Corporation, donde se debe pagar la suma de $378 dólares a una cuenta de una dirección en Panamá.

If you install [this] on a microcomputer...
then under terms of this license you agree to pay PC Cyborg Corporation in full for the cost of leasing these programs...
In the case of your breach of this license agreement, PC Cyborg reserves the right to take legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use...
These program mechanisms will adversely affect other program applications...
You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement; your conscience may haunt you for the rest of your life...
and your [PC] will stop functioning normally...
You are strictly prohibited from sharing [this product] with others..

Figura 1: Licencia de usuario final del software AIDS

Fue fácil encontrar al autor, por la cuenta en dónde se debía pagar el dinero. Éste era el Dr. Joseph Popp, el cual fue extraditado al Reino Unido, donde no pudo ser juzgado. Más tarde un tribunal italiano lo declaró culpable, pese a que se le había declarado como demente.

El tema del AIDS, sólo quedó en la memoria colectiva, y no fue sino hasta 1995 cuando Adam Young desarrolló una tesis junto a su profesor a cargo Moti Yung, mediante el cual un virus podía utilizar la criptografía pública para cifrar la información del usuario.

Al año siguiente se realizó otro experimento con éxito, siempre teniendo un cuidado máximo para que el criptovirus no se liberara y causara daños fuera del recinto de investigación. Arrancaba de esta forma el estudio de la aplicación de la criptografía en el desarrollo de programas maliciosos en un proceso de investigación de la manera en la que ésta podía ser utilizada para consolidar, mejorar y desarrollar nuevas versiones de programas.

El estudio de esta nueva modalidad teórica del virus fue bautizada entonces como Criptovirología y desde aquél momento se ha hecho todo lo posible por tener la disciplina limitada a los laboratorios, como una prueba de concepto, aunque el sólo hecho de su existencia ha sido suficiente para que alguien retome el tema y programe un criptovirus que se pueda distribuir por la red.

No fue sino hasta el año 2005, cuando un malware llamado Gpcode apareció [16] y hasta el día de hoy sus versiones han preocupado mucho a los expertos, por su constante evolución. EL cual encripta los archivos usando el algoritmo RSA.

El 2006 apareció otro malware llamado, Crizip [12], el cual sólo usa las librerías públicas de ZIP usando una contraseña. Desde ese momento se encasillaron a todo este tipo de amenazas como Ransomware.

Entre mayo y junio del 2006 aparecen 3 Ransomware más: MayArchive [7], que encripta los archivos como cualquier Ransomware, pero los archivos de rescate sólos los deja en la carpeta de Mis Documentos, Arhiveus [8, 9], que encripta sólo los archivos de la carpeta “Mis Documentos”, y Ransom-A [10, 11], que es un gusano, que a diferencia de los demás Ransomware, esconde los archivos en un directorio oculto, y que una vez terminado el proceso muestra las indicaciones del rescate, unas imágenes porno, y dice que cada 30 minutos elimina un archivo.

En julio del 2007 aparece Sinowal.FY [6], que pertenece a la familia Sinowal, que tradicionalmente se dedican al robo de contraseñas y delitos bancarios. Este malware amenaza con una fecha límite para que se pague la recompensa, declarando que pasada esa fecha borrará todos los archivos cifrados, cosa que no sucede.

Los Ransomware anteriormente mencionados, son los únicos de los que se data su existencia y que caen en esta categoría, eso sí algunos tienen variantes, pero que no han evolucionado mucho, a excepción de Gpcode.

Las deficiencias que tienen este tipo de amenazas es que se tienen que crear desde cero, ya que no existe ningún motor para su creación como para otros tipos de malware, y por lo mismo es que su nivel de infección es muy bajo.

1.3 Cryzip y Gpcode, los Ransomware más conocidos.

A continuación analizaremos a fondo los dos malware más conocidos que caen en la categoría de Ransomware. Por un lado

veremos las características de Cryzip y por otro veremos la evolución de Gpcode.

Cryzip

Cryzip, también conocido como Zippo, el cual está escrito en Visual C++, fue detectado en marzo del 2006, y afecta a la familia de SO Windows. Tiene una peligrosidad y daño mediana, y una propagación muy baja, el cual ha afectado principalmente a usuarios de Estados Unidos y Gran Bretaña. [12, 13, 14, 15].

Cryzip es un troyano que comprime en formato ZIP con contraseña todos los archivos con permisos de lectura y escritura, en todas las unidades de disco, con cualquiera de las siguientes extensiones: ARH, ARJ, ASM, BAS, C, CDR, CGI, CHM, CPP, DB, DB1, DB2, DBF, DBT, DBX, DOC, DPR, DSW, FRM, FRT, FRX, GTD, GZ, GZIP, JPG, KEY, KWM, LST, MAN, MDB, MMF, MO, OLD, P12, PAK, PAS, PDF, PEM, PGP, PL, PWL, PWM, RAR, RTF, SAFE, TAR, TXT, XLS, XML y ZIP.

Sus alias son: Zippo.10, Troj/Zippo-A, TROJ_CRYZIP.A, Virus.Win32.Zippo.10, Win32/Zippo.10, Win32/Cryzip.A.

Al momento de ejecutarse, crea un archivo de nombre “ZIPPO_CRYPTOR.ZIP”, en todas las unidades de disco. Además inyecta su componente DLL, “ZIPPO.DLL”, en todas las aplicaciones que se estén ejecutando.

Los archivos que encuentra, con las extensiones antes mencionadas, los comprime en un archivo .ZIP con contraseña y cambia su nombre finalizándolos con “_CRYPT.ZIP”.

Además, sobre-escribe el archivo en el momento que está comprimiéndolo con el texto “Erased by Zippo! GO OUT!!!” y después, los elimina. De esta manera, no se pueden recuperar estos archivos incluso si se utiliza una herramienta especial para recuperar archivos eliminados.

Una vez comprimido un archivo, crea en todas las carpetas un archivo de texto, “AUTO_ZIP_REPORT.TXT”, con instrucciones para que el usuario pague $300 dólares, a través de E-Gold, para la contraseña que puede descomprimir los archivos.
Aunque el código de cifrado de un ZIP es fuerte, un ataque de fuerza bruta aún es

```
OUR E-GOLD ACCOUNT: [número de cuenta]

INSTRUCTIONS HOW TO GET YUOR FILES BACK READ
CAREFULLY. IF YOU DO NOT UNDERSTAND, READ AGAIN.

This is automated report generated by auto archiving
software.

Your computer catched our software while browsing
illigal porn pages, all your documents, text files,
databases was archived with long enought password.

You can not guess the password for your archived
files - password lenght is more then 10 symbols that
makes all password recovery programs fail to
bruteforce it (guess password by trying all possible
combinations).

Do not try to search for a program what encrypted
your information - it is simply do not exists in your
hard disk anymore. If you really care about documents
and information in encrypted files you can pay using
electonic currency $300.
Reporting to police about a case will not help you,
they do not know password. Reporting somewhere about
our e-gold account will not help you to restore
files. This is your only way to get yours files back.

------------------------------
How to pay to get your information back.

1. click on this link to open your free e-gold
account - the first screen is the e-gold "terms and
conditions" page. You need to agree to these by
clicking on the "I AGREE" button on the bottom on the
```

factible para conseguir la clave.

Figura 2: Extracto de la recompensa pedida por Cryzip

El texto del archivo “AUTO_ZIP_REPORT.TXT” está codificado dentro de la DLL de Cryzip, usando una simple codificación de XOR (0x13). La contraseña con que se comprimen los archivos también se encuentra dentro de la DLL, pero no es encriptada, es por ello que se conoce, y es la siguiente: “C:\Program Files\Microsoft Visual Studio\VC98”.

Cryzip no se propaga por sus propios medios, sino que precisa de la intervención de un usuario atacante para su propagación, por ello el contagio con la amenaza principalmente se da en los archivos recibidos vía clientes P2P, IRC, email o cualquier otro medio de intercambio de archivos.

Gpcode.

Gpcode [16] es sin lugar a duda el más famoso de su especie, el cual marcó el principio de una era de delitos en el crimen cibernético y ha llegado a una evolución tal, que está preocupando a muchos, entre ellos a los laboratorios de los antivirus.

Este malware comenzó a ser visto como tal en el año 2005, pero sus primeras apariciones fueron en diciembre del 2004, donde varios usuarios vieron que sus archivos no podían ser abiertos, ya que habían sido encriptados, pero no había ningún rastro de algún programa que haya hecho eso, y la única pista que había dejado era un archivo de texto de nombre !_Vnimanie_!.txt (Vnimanie es una palabra rusa que significa "atención"), el cual básicamente describía que los archivos habían sido encriptados y que debía comprarse un programa para ello.

En junio 2005, apareció una nueva ola de este malware, pero con una clave de cifrado más compleja. Fue en este instante que se tuvieron muestras del virus, y se pudo clasificar como tal.

En enero del 2006, apareció una nueva variante Gpcode.ac, el cual fue el primero en usar clave de cifrado RSA, de 56 bits, cosa que fue una gran mejora en cuanto a los métodos de encriptación usados anteriormente. Además fue aquí cuando se descubrió cómo se infectaban los usuarios con este malware.

Y así comenzó a perfeccionarse el malware. Al poco tiempo usó una clave de encriptación de 67 bits. Y a principios de junio del mismo año, en 5 días, aparecieron 3 variantes más, Gpcode.ae que tenía una clave RSA de 260 bit, Gpcode.af que usaba una clave de 330 bits, y finalmente Gpcode.ag [19] con una clave de 660 bits.

EL autor de Gpcode, planificó los ataques con mucho cuidado, utilizando técnicas de ingeniería social para difundir el virus.

AL comienzo se envió un Spam a las direcciones de correo electrónico de job.ru, el cual es uno de los de los principales sitios web de contratación de Rusia. El correo contenía un archivo adjunto de nombre anketa.doc (anketa significa formulario de solicitud en ruso), y además decía que llenaran este formulario y reenviaran el mail. Al abrir el documento Word, un macros malicioso de nombre "Tored.a" comienza a ejecutarse e instala otro troyano de nombre "Small.crb" en el ordenador de la víctima, cuya función es descargar el troyano Gpcode desde el sitio "msk.ru/services.txt" y lo instala en el equipo.

Una vez Gpcode está instalado escanea todos los directorios escanea los directorios accesibles y cifra archivos con ciertas extensiones. Una vez terminada su función, los tres troyanos son eliminados, para así no dejar rastros, y se muestra una ventana Pop-pup indicando que se ha terminado de encriptar los archivos con el algoritmo de encriptación respectivo. Además deja en cada carpeta que contenga los archivos cifrados un archivo de nombre "readme.tex" con un texto como el siguiente:

"Algunos archivos están codificados por el método RSA. Para comprar un decodificador escriba a: k47674@mail.ru con el tema: RESPUESTA".

El cual luego le respondía, diciéndole una cuenta de paypal donde debía depositar el dinero para obtener el software que descifra los archivos. Comenzó pidiendo 2000 rubios (aproximadamente 70 dólares), y así ha ido bajando precio, hasta llegar a los 500 rubios.

Si bien el creador del virus sigue con la misma modalidad para infectar con Gpcode, sus técnicas de encriptación como vimos han evolucionado, así fue como en junio de este año (2008) apareció una nueva versión Gpcode.ak [17, 18], el cual continúa ocupando el algoritmo RSA para encriptar, pero esta vez usando una clave de 1024 bits, el cual es la única versión hasta el momento de la cual no se conoce la clave y se teme que se demoren en conocerla.

Aunque Gpcode es hoy en día el Ransomware más temido, tiene un pequeño defecto, que es muy probable que cambie a futuro: no sobre-escribe los archivos antes de eliminarlos; por ende, muchos de los archivos se pueden rescatar usando alguna herramienta de recuperación de archivos. Para lo cual se han creado herramientas como StopGpcode2 de Kaspersky Lab [20], que puede recuperar muchos de los archivos encriptados por Gpcode.

1.3 Diseño y Análisis de Ransomwares.

La creación de un Ransomware es una tarea un tanto difícil, puesto que existen muchas dificultades en su diseño, que las analizaremos a continuación.

La principal dificultad que existe para los creadores de Ransomwares es que no existe una aplicación generadora de Ransomwares, así como lo hay para virus, troyanos, worms y demás es. Es por esto mismo que los creadores de Ransomwares deben programar su aplicación desde cero, y por lo mismo podemos ver que no son tan infecciosos.

Al momento de crear un Ransomware, lo primero que debe tenerse claro son las reglas de los archivos que se encriptarán, estás pueden ser, por ejemplo: límite superior e inferior para el tamaño de los archivos, ubicaciones de éstos, permisos de escritura y lectura, las extensiones, y otros, como por ejemplo que no estén ocultos.

Luego de definir las reglas de los archivos que deseamos encriptar, se nos viene la primera dificultad, ésta es la rapidez con la que tenemos que actuar, ya que la víctima no debe enterarse de que estamos encriptando sus datos en el momento del proceso; por ello se deben usar una cantidad suficientes de Threads que trabajen en paralelo, y que a la vez no colapsen el sistema, por ello la cantidad debería ser relativa a la memoria del sistema y a la memoria disponible en el momento del proceso de encriptación.

Como segunda y principal dificultad es la elección del método de encriptación y tamaño de la llave. La criptografía simétrica y asimétrica tiene sus ventajas y desventajas, a la vez. Por un lado si ocupamos criptografía asimétrica, tendremos la ventaja de que la clave para desencriptar no se encontrará en el código, pero como desventaja que el proceso de encriptación es muy lento, y si ocupamos criptografía asimétrica es lo contrario. Además debemos ocupar una llave de gran tamaño, para que sea casi imposible encontrarla por fuerza bruta. Por esto mismo, vemos que los Ransomwares usarán sólo criptografía asimétrica a futuro, como Gpcode, ya que la velocidad en los equipos cada vez es mayor.
Otro punto a mencionar, es la elección de las llaves, la cual debiera ser dinámica, o seudo-dinámica, es decir con algún algoritmo conocido por el atacante, ya que si se encontrase la llave para los archivos encriptados en un equipo, sea difícil encontrar la llave para los archivos encriptados en otro equipo. Finalmente se debe remarcar que hasta hoy, todos los Ransomwares al momentos de señalarle a la víctima que ha sido infectada, le indica el algoritmo de encriptación y el tamaño de la llave, cosa que a futuro puede cambiar, dificultando más aún la labor de desencriptación.

Como infección no debiera considerarse mucho la infección usando vulnerabilida-

des de los sistemas o aplicaciones, así como los virus o worms, y como lo hacía anteriormente Gpcode, ya que estas vulnerabilidades están disponibles para el atacante por un tiempo determinado, y cuando se solucionen estas vulnerabilidades y las posibles víctimas actualicen su sistema, el malware no tendrá valor. Por esto debiera considerarse la técnica más usada, y la que más resultados otorga, esto es la infección de archivo; es decir, como un verdadero troyano; esto es por ejemplo, infectando ejecutables, donde se ocupan las técnicas de los Joiners (un Joiner es una aplicación juntadora de archivos, y que los guarda, separados por firmas, en un ejecutable), o bien infectando archivos Microsoft Office por medios de las macros, o como se está haciendo últimamente q es infectando archivos multimedia, y así usar otros tipos de Malwares, que sólo descarguen nuestra aplicación de algún sitio web y la ejecuten.

Si hablamos de ocultación, hablamos de Rootkit, que es la otra gran amenaza de la cual debemos preocuparnos, y que el tema está más allá de este texto. Es por ello, que si queremos que el proceso del Ransomware, se inicie y termine sin ningún problema debemos usar éstas herramientas, ya que con ellos podemos ocultar el proceso tanto para el usuario, como para el antivirus.

Como consideración al momento de diseñar un Ransomware, se debe tener en cuenta eliminar el archivo que fue encriptado, y sobre-escribirlo, cosa que no hace Gpcode, ya que existen herramientas de recuperación de archivos, y no serviría de nada todo lo que hizo el Ransomware.

Como último paso y el más fácil, cuando ya se ha infectado a la víctima, el Ransomware debe eliminar sus huellas, usando otro ejecutable que elimine todos los archivos que participaron en el ataque. Y por último éste debe mostrarse al usuario, indicándole las reglas que debe seguir para recuperar sus archivos.

Finalmente, hay que tener en cuenta la existencia de programas como OllyDGB, el cual es un desensamblador y debugger, por ende la herramienta perfecta de los crackers:

- Si la ocupamos como desensamblador, podríamos ver el código fuente del Ransomware, en lenguaje assembler, encontrando las llaves que se usan para el proceso de encriptación, o bien información sensible en cuanto al Ransomware, como por ejemplo si éste envía un mail al momento de infectar un equipo, se encontraría la dirección del mail con su clave, etc., en síntesis se puede visualizar todo su código. Es por ello, que el Ransomware, o cualquier otra aplicación debiera ocupar 3 medidas de seguridad para esto, primero, encriptar todas las variables, de modo que no sean entendibles a simple vista, segundo ocupar un ofuscador, ya que éste optimiza y cambia toda la estructura del código, haciéndolo más inentendible, y tercero ocupando un UPX, el cual empaqueta y comprime el ejecutable del Ransomware, y luego permite ejecutar éste sin tener que descomprimirlo
- Si lo ocupamos como debugger, podemos interceptar la aplicación del Ransomware en tiempo de ejecución, por ende, podemos determinar todas sus variables en un momento determinado, y por ende darle toda la información de la aplicación al que está analizando el Ransomware, es por ello que debiera trabajarse con las variables encriptadas, haciendo no deducible el estado de cada una de las variables.

Teniendo en cuenta todas estas medidas, y el trabajo que conlleva, se puede crear un Ransomware, el cual como se ve, es una tarea un poco difícil si es que se quiere lograr hacer un Ransomware que cumpla todos sus objetivos y que no sea descubierto en el intento.

Por todo esto, no deberíamos sorprendernos si ha futuro aparecen generadores de Ransomwares, donde uno podría las reglas de los archivos a encriptar, la cantidad de Threads que se quieren correr en el proce-

so de encriptación, el algoritmo de encriptación y la llave a usar, los métodos de ocultación e infección que se quieren usar, etc.

2 Estudios Expuestos por Young & Yung [1]

Los más grandes exponentes, y creadores de la vez, de la Criptovirología son Adam Young y Moti Yung. A continuación se da una reseña de sus estudios más aplicables a los criptovirus.

2.1 Criptocontadores

Una condición común usada por los virus para decidir cuándo atacar es el valor de un contador, típicamente usado para comenzar el ataque sólo cuando se ha propagado una mínima cantidad de copias. La desventaja que esto presenta para el atacante es que el mismo código de su virus le está proporcionando información valiosa al defensor sobre la población actual del malware. Para resolver este problema se propone el uso de "criptocontadores", o contadores que cualquiera pueda incrementar o decrementar, pero sólo el creador pueda leer.

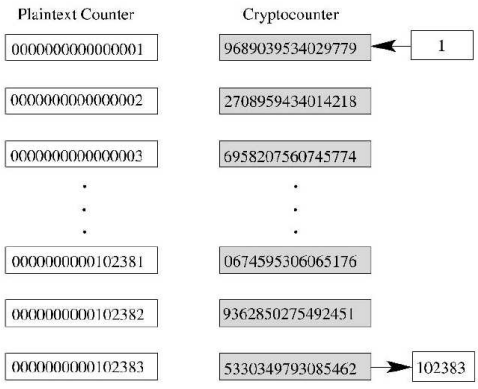

Figura 3: Ejemplo del funcionamiento de un criptocontador

Para esto, un primer enfoque es usar llaves pública/privada, tal que sólo el usuario con la llave privada pueda conocer el valor actual del contador, pero cualquier usuario pueda modificar su valor "a ciegas". Con esto se consigue que el malware pueda usar contadores libremente, y para cualquier agente externo que trate de leerlos, conocer su valor real en un determinado punto sea extremadamente difícil.

2.2 Robo de Información de manera segura

Al tratar de usar un virus para robar información se dan 2 escenarios típicos. En el primero, el virus almacena el nombre del dato que quiere robar (por ejemplo, si se desea extraer el sueldo de Juan Pérez de una DB, el virus almacenara un string con el valor "Juan Perez"), y en el segundo, una vez extraído dicho valor de la DB, el virus lo almacena en una de sus variables (en el ejemplo anterior, un ejemplo podría ser "$100.000"). En cualquiera de los dos casos, el defensor podría averiguar algunas señas de la información que fue robada.

Para resolver el 2do problema, bastaría encriptar el dato obtenido con un par de llaves privada/pública. Pero para el 1er caso, el problema no es tan fácil, ya que si se quiere proteger el nombre en todo momento, se debería poder consultar por "Juan Perez" sin tener en ningún momento dicho texto plano entre el código.

2.3 Criptocomputación

Es un área reciente de la criptografía. Su objetivo es poder operar directamente sobre datos encriptados sin necesidad de decriptarlos, no simplemente almacenar y transportar datos encriptados. Esta ciencia podría aplicarse, por ejemplo, para prevenir la piratería.

3 Problemas para el autor de un Ransomware [1]

Al tratarse de un nuevo enfoque para hacer virus, aparecen nuevos problemas, tanto para el atacante como para el defensor. A continuación se presentan una serie de ideas desarrolladas por los autores para poder realizar un ataque efectivo tratando tecnologías actuales como posibles desarrollos a futuro que podría ayudar a refinar estos ataques.

3.1 Redes mixtas

Posiblemente, el aspecto más débil del ataque de extorsión desde la perspectiva de quienes crean virus es obtener el rescate sin ser atrapado. Existen métodos que permiten a dos partes que desconfían mutuamente comunicarse sobre una red de una forma anónima en donde el vehículo básico para hacer esto es llamado una red Mixta. Una red mixta forma la base para un sistema de reenvió anónimo y es un bloque fundamental de construcción para muchos protocolos criptográficos. Hay dos categorías, síncrona y asíncrona, la asíncrona es ideal para trafico de emails de forma anónima en cambio las síncronas son mejores para el trafico de mensajes de forma aleatoria.

Una red mixta consiste en una colección de N nodos netos. La idea básica detrás de una red mixta asincrónica es tomar un mensaje de entrada, enviarlo de nodo a nodo a lo largo de un camino al azar elegido, y luego enviarlo a su destino final. Es necesario usar la codificación para prevenir correlaciones basadas en el contenido así como fijar la longitud de cada mensaje de tal manera que las correlaciones basadas en el tamaño no sean posibles. Esto implica que los mensajes grandes tienen que ser divididos en piezas más pequeñas, y los mensajes cortos tienen que ser rellenados a la longitud necesaria. Los mensajes clasificados fijos son codificados usando un criptosistema probabilístico de llave pública. Por lo tanto, aun si el mismo mensaje es enviado por la red en más de una ocasión parecerá diferente con una alta probabilidad.

Una red mixta asincrónica debe tener un mensaje de tamaño suficientemente grande siempre. Si sólo unos pocos mensajes viajan por la red entonces la correlación es trivial. Es por esto que se ha propuesto una solución nueva a este problema, la idea es considerar los nodos de red mixta como algoritmos probabilísticos y dejarles afectar los caminos que toman los mensajes. Cuando un desvío ocurre tiene el efecto de añadir nuevas capas en el mensaje en cuestión. Este mecanismo tiene la propiedad que hasta el remitente no sabe qué camino tomará su mensaje dentro de la red mixta. Los métodos que han sido ideados no sólo permiten que mensajes anónimos sean enviados, sino también permitan respuestas anónimas.

En el ataque de cryptovirus, el virus puede instruir a la víctima de colocar la dirección de correo electrónico de la víctima en un tablón de anuncios público. Para evitar la vergüenza, el virus puede decir a la víctima codificar primero la dirección de correo electrónico usando la llave pública del virus. La dirección de correo electrónico puede ser elegida expresamente para tratar con el creador de virus y por lo tanto no revelar la personalidad de la víctima.

Cuando el atacante encuentra una víctima envía la demanda anónimamente a la víctima, la víctima puede incluir el rescate dentro de la respuesta anónima. Mientras el rescate en sí mismo no revela la personalidad de la víctima, el ataque conserva el anonimato de la víctima. Una red mixta es

por lo tanto un componente básico para realizar ataques de cryptovirus.

Para detener al atacante, la ley puede procurar citar a los administradores de cada nodo en la red mixta. Tal citación podría pedir la llave privada actual y todas las llaves privadas anteriores de cada uno de los administradores. Si todas las llaves privadas necesarias y tráfico de mensaje fueran obtenidas, esto permitiría que la ley rastree cualquier mensaje enviado. Sin embargo, si cada nodo estuviera adherido a un protocolo estándar de la red mixta, generaría nuevos pares de claves regularmente y suprimiría todas las llaves privadas anteriores, entonces la citación no ayudaría probablemente a la aplicación de la ley.

Se ha propuesto un método reciente conocido como la nueva codificación universal la cual tendrá como base una red mixta probablemente segura. Usando un cryptosystem, como el ElGamal que permite la nueva codificación sin el primer descifre, es posible enviar los mensajes de entrada aleatoriamente de forma inconsciente a través de la red mixta. Con respecto al ataque de virus, esto implica que no hay ningún administrador llaves privadas que pueda cooperar con la ley

Si un nodo de red mixta con la nueva codificación no almacena la permutación arbitraria que usó en una operación de mezcla, entonces la permutación se pierde para siempre. Esta propiedad hace las redes mixtas con la nueva codificación muy atractiva para criminales que tienen que comunicarse anónimamente.

3.2 Las dos caras del anonimato

La capacidad de comunicarse anónimamente y hacer cosas de una forma anónima es de gran utilidad. Los criminales que realizan operaciones criminales de un modo anónimo minimizan su riesgo de ser agarrado pero también tiene su lado bueno, por ejemplo los votantes que participan en votaciones anónimamente se libran del miedo de la persecución. La necesidad de comunicarse anónimamente y realizar actividades anónimas se ha extendido en el reino digital y actualmente existen algoritmos criptográficos avanzados para enviar anónimamente correos electrónicos, votación, y artículos adquisitivos sobre Internet.

3.3 Dinero electrónico

El dinero electrónico es una tecnología que combina el anonimato del dinero efectivo con la seguridad y conveniencia ofrecida por tarjetas de debito. El concepto del dinero electrónico implica que las corrientes de ceros pueden sustituir el papel moneda. El dinero electrónico es una de las aplicaciones más complicadas de la criptografía de clave pública. Una de las ventajas del dinero electrónico es que puede ser protegido de la destrucción. Considerando la evolución de dinero, la migración al dinero electrónico tiene sentido. Los problemas asociados con el cambio de productos perecederos a productos no perecederos fueron solucionados usando monedas. El problema de arrastrar aproximadamente cientos de monedas fue minimizado usando el papel moneda, es por eso que el dinero electrónico puede hacerse un medio de pago más barato comparado con el papel moneda.

3.4 Delito Perfecto

Considere el problema de un secuestrador cuando afronta el momento de recoger el dinero del rescate. Esta situación es arriesgada de la perspectiva del secuestrador ya que esto hace ciertas asunciones sobre las capacidades de vigilancia y esfuerzos de la ley por atrapar al secuestrador. Pero con el dinero electrónico, esto no es el caso. El secuestrador puede insistir que el rescate sea pagado usando el dinero electrónico que es codificado bajo la llave pública del secuestrador. El secuestrador puede insistir que el dinero electrónico criptografiado sea enviado usando un reenvió anónimo en una respuesta anónima. Esto es conocido como el delito perfecto. Sin embargo cuando es necesario, las autoridades pueden colaborar y así rastrear el flujo de dinero electrónico. Ellos por lo tanto tienen la capacidad de revocar el anonimato proporcionado por el sistema.

Considerando la existencia de esquemas de dinero efectivo electrónico anónimos que aseguran el anonimato revocable, uno podría suponer que la amenaza de política de asesinato y delitos perfectos sea eliminada. Sin embargo, esta suposición es fundamentalmente estropeada ya que hace la asunción implícita que hay una entidad que es capaz de controlar todos los medios de pago. Esto no tiene que ser el caso. Suponga que una organización (por ejemplo, un pequeño país extranjero) crea un dinero digital. Usando codificación, firmas, y redes mixtas sería posible comprar y vender productos y servicios usando el dinero en Internet de una forma confidencial y no detectable (similar a "BlackNet").Esta organización puede diseñar el sistema de pago para ser completamente anónima. Cualquier país u organización que hace esto probablemente prosperará. Se haría un depósito para corporaciones de delito por todo el mundo y acumularía grandes ganancias en el corto plazo que le permitiría invertir en negocios legítimos. Otros países podrían crear una legislación que haría la utilización del dinero electrónico extranjero ilegal, pero la criptografía inhibiría enormemente la capacidad de la aplicación de la ley para hacer cumplir tales leyes.

3.5 Futuras Posibilidades

Ideas básicas que forman la base de ataques usando criptovirología:

1. Realización del virus como un algoritmo distribuido. El virus reside en máquinas múltiples que son conectadas a la red. Esto da la robustez contra la posibilidad que el ataque de virus sea terminado desde la supresión o el comprometimiento de un o dos virus puede no parar el ataque.
2. El virus utiliza una tabla de anuncios. Esto permite que los virus se comuniquen el uno al otro leyendo y escribiendo a una sola posición de la cual todos ellos son conscientes.
3. El virus utiliza una red mixta. Esto permite que los virus oculten sus posiciones de cada uno incluso de los otros y por lo tanto ayuda a impedirles ser descubierto.
4. El virus emplea la codificación dividida. Esto protege la intimidad de la víctima. Sin alguna medida de privacidad de ciertas víctimas pueden no dudar en no hacer caso de las demandas virales.
5. El virus emplea la criptografía asimétrica. Esto permite que los virus cambien llaves públicas, digitalmente firmen datos, y codifiquen datos usando una llave pública. De ahí, los virus pueden establecer canales certificados y confidenciales el uno con el otro por la red mixta y sobre el tablón de anuncios.

6. Los virus generan la aleatoriedad compartida. Los protocolos criptográficos basados en tirar una moneda permiten que los virus generen la aleatoriedad en un camino que es robusto contra un pequeño número de virus puestos en peligro.

Varios métodos indirectos existen para conseguir la ganancia financiera usando este tipo de malware. Por ejemplo, un atacante decidido puede premeditar una tentativa de extorsión comprando varias acciones de una pequeña empresa pública, a condición de esto un número considerable de acciones aumentara para la venta. Una vez que el ataque es realizado la víctima puede ser obligada a comprar una gran cantidad de acciones de la pequeña compañía. Esto tiene una tendencia de hacer subir el precio de cada acción, en donde el atacante puede cobrar en efectivo. El inconveniente obvio a este método consiste en que todos los accionistas excepcionales pueden ser considerados como sospechosos.

Conclusión

En este documento se introdujo un concepto quizás nuevo para el lector: Los criptovirus. Se detalló su historia desde sus comienzos hasta sus aplicaciones más actuales.

Pero por sobre todo se explicó la forma de uso que, a nuestro juicio, es la más peligrosa en la actualidad: Los Ransomware. Este tipo de malware, que funciona encriptando los archivos de la víctima para luego pedir un "rescate", puede llegar a ser muy nocivo para los defensores, y muy lucrativo para los atacantes.

En este trabajo se presentaron las formas de Ransomware más conocidas, junto con los aportes más notables que, para bien o para mal, han hecho en el tema los dos autores más destacados: Young & Yung.

Uno podría sostener que el primer paso en la obtención del poder es la acumulación de riqueza. El desastre total es una posibilidad previsible, ya que permitimos cada vez más que máquinas tomen decisiones por nosotros. Los ataques de cryptovirus distribuidos pueden parecer sensacionales, y para nuestro tiempo seguramente lo son. Sin embargo, ellos son quizás menos sensacionales de lo que le habría parecido un par de teléfonos celulares al inventor del telégrafo. Hoy estos ataques quizás son más relevantes como inspiración que amenazas realizables, sin embargo cuando se desarrollen criptovirus más evolucionados usando nuevas técnicas de cifrado, hará imposible el decifrado de archivos encriptados.

Referencias

[1] Adam Young , Moti Yung, "Malicious Cryptography, Exposing Cryptovirology"

[2] http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.pdf

[3] http://www.ciac.org/ciac/bulletins/a-10.shtml

[4] http://www.nationmaster.com/encyclopedia/AIDS-(trojan-horse)

[5] http://www.viruslist.com/en/viruses/encyclopedia?chapter=153311160

[6] http://www.pandasecurity.com/spain/hom

eusers/security-info/about-mal-ware/encyclopedia/overview.aspx?lst=det&idvirus=168350

[7] http://www.sophos.com/security/analyses/viruses-and-spyware/trojarhiveusa.html

[8] http://www.secureworks.com/research/threats/arhiveus/

[9] http://www.sophos.com/security/analyses/viruses-and-spyware/trojarhiveusa.html

[10] http://www.sophos.com/security/analyses/viruses-and-spyware/trojransoma.html

[11] http://vil.nai.com/vil/content/v_140057.htm

[12] http://www.secureworks.com/research/threats/cryzip/

[13] http://www.viruslist.com/en/viruses/encyclopedia?virusid=115215

[14] http://www.symantec.com/security_response/writeup.jsp?docid=2006-031314-5208-99

[15] http://www.vsantivirus.com/cryzip-a.htm

[16] http://www.viruslist.com/sp/analysis?pubid=188965655

[17] http://www.viruslist.com/sp/viruses/encyclopedia?virusid=313444

[18] http://www.kaspersky.com/sp/news?id=207732671

[19] http://www.viruslist.com/sp/viruses/encyclopedia?virusid=123921

[20] http://www.viruslist.com/sp/analysis?pubid=207270972

[21] http://www.viruslist.com/sp/analysis?pubid=207270984

[22] http://www.viruslist.com/sp/analysis?pubid=207270947

[23] http://www.viruslist.com/sp/news?id=187033544

[24] http://www.nod32-es.com/download/files/docs/ransomware.pdf

[25] wwwcsif.cs.ucdavis.edu/~balepin/files/**worms-cryptovirology**.pdf