Ransomware: seguridad, investigación y tareas forenses

Santiago Trigo[1], Martín Castellote, Ariel Podestá[1], Gonzalo Ruiz de Angeli[1], Sabrina Lamperti[1], Bruno Constanzo[1]

InFo-Lab, Laboratorio de Investigación y Desarrollo de Tecnología en Informática Foren-se (Universidad FASTA, Ministerio Público de la Provincia de Buenos Aires, Municipalidad de General Pueyrredon), Avellaneda 3341, Mar del Plata, Argentina
[1]{santiagotrigo, arieluf, ruizgon, slamperti, bconstanzo}@ufasta.edu.ar
http://www.info-lab.org.ar

Resumen. Las nuevas modalidades delictivas irrumpen en la sociedad con estrategias cada vez más novedosas, llevadas a cabo por personas que buscan obtener beneficios económicos utilizando técnicas de difícil rastreo, aprovechándose del desconocimiento de los usuarios en el uso de las tecnologías de información y comunicación. En este trabajo se busca ahondar en el *ransomware*, un tipo de *malware* que se encuentra actualmente en crecimiento y que representa un desafío tanto para la sociedad misma, en su faceta de prevención, como para los operadores judiciales en la búsqueda de sus potenciales autores.

1 Introducción

Desde tiempos inmemoriales, engañar y ser engañado resultan ser actitudes profundamente enraizadas en los seres humanos, que se manifiestan en los más diversos ámbitos y situaciones. Probablemente, una de las formas más usuales de llevar adelante estos engaños es a través de los fraudes y las falsificaciones.

> Se podrá recordar la historia del caballo de Troya, artilugio utilizado en la Guerra de Troya que, según la Odisea de Homero, fue usado por los griegos como una estrategia para introducirse en dicha ciudad fortificada. Tomado por los troyanos como un signo de su victoria, el caballo fue llevado dentro de los gigantescos muros, sin saber que en su interior se ocultaban varios soldados enemigos. Durante la noche, los guerreros salieron del caballo, mataron a los centinelas y abrieron las puertas de la ciudad para permitir la entrada del ejército griego, lo que provocó la caída definitiva de Troya.

La leyenda ha servido de sustento para dar vida a los *troyanos informáticos*, como un tipo de software malicioso que se presenta al usuario bajo la apariencia de un programa aparentemente legítimo e inofensivo que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

Los *troyanos* se concibieron como una herramienta para causar daños en los equipos infectados. Sin embargo, se observa que, en la actualidad, la tendencia ha cambia-

do hacia el robo de datos bancarios e información personal, ello debido al mayor uso de Internet, en particular, en todo aquel espacio donde se vuelca gran cantidad de este tipo de información sensible.

A las maniobras que se llevan adelante empleando malware para la obtención de beneficios financieros o económicos, se lo conoce como *crimeware*[1]. Dentro de las distintas modalidades que fueron desarrollando estos tipos de malware, encontramos, entre otros, al *adware, pharming, phishing, spoofing, spyware* y *ransomware*[1]. Este último, ha cobrado relevancia desde hace unos años, debido a su especial *modus operandi*, tratándose de aplicaciones orientadas a "secuestrar" el sistema operativo o documentos del usuario para luego cobrar una recompensa por su recuperación.

Debido a las características propias del ransomware y al aprovechamiento de las técnicas de anonimato en Internet, se ha tornado dificultoso, desde el punto de vista judicial, su análisis a la hora de establecer tanto la materialidad delictiva como la posible autoría penalmente responsable. Es por eso que en este trabajo se pretende desarrollar los aspectos de seguridad, de preservación y análisis de la evidencia digital asociada a este delito, para su posible consideración por parte de los operadores judiciales.

2 Marco Teórico

Se puede definir como *malware* a aquellos programas cuyo objetivo es dañar o infiltrarse, sin el consentimiento del propietario, en un sistema de información. En general, se entiende como sinónimo de virus informático, un término que se usó durante mucho tiempo a falta de una mejor descripción, y se refiere a programas que son hostiles, intrusivos y/o molestos. En general, un malware infecta tanto un programa como un sistema, cuando logra alojarse en él y garantizar su ejecución.

Ransomware es el término genérico para referirse a todo tipo de software malicioso que toma el control de un sistema, o de sus datos, y le exige al usuario el pago de un rescate para su liberación. Esta amenaza que ha crecido de forma semi-exponencial en los últimos años[2, 3], lo que hace comúnmente es cifrar ciertos archivos con una determinada clave, que sólo el creador del ransomware conoce y proveerá al usuario que la reclame a cambio del pago de una recompensa.

Desde el punto de vista legal, la modalidad delictiva del *ransomware* puede encuadrarse dentro del tipo penal básico de la **extorsión**, el cual reprime con reclusión o prisión de cinco (5) a diez (10) años, al que con intimidación o simulando autoridad pública o falsa orden de la misma, obligue a otro a entregar, enviar, depositar o poner a su disposición o a la de un tercero, cosas, dinero o documentos que produzcan efectos jurídicos.

[1] Etimología: *ransom*, del inglés, rescate, y *ware* por *software*.

Por otra parte, teniendo en cuenta que entre las consecuencias más comunes de un ataque por *ransomware* se encuentran la pérdida de información de forma temporal o permanente, la interrupción de los servicios regulares, y las pérdidas financieras asociadas a la restauración de los sistemas; podría pensarse en que a la figura básica de la extorsión se le sume la del **daño informático** (art. 183 del Código Penal) y **entorpecimientos de las comunicaciones** (art. 197 del Código Penal).

Ello así, toda vez que el art. 183 del C.P. establece que será reprimida la conducta de quien *"alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños"*. Inclusive, podría aplicarse la figura agravada del daño, prevista en el art. 184 inc. 5 del C.P. que, de acuerdo al texto legal, aplica cuando la acción se ejecute: *"...en archivos, registros, bibliotecas, museos, o en puentes, caminos, paseos, u otros bienes de uso público (...)"*.

La doctrina ha entendido que el delito de daño no exige que la cosa mueble quede totalmente destruida o inutilizada, bastando para su consumación que la restitución del bien a su estado anterior demande algún gasto, esfuerzo o trabajo. Ese gasto o esfuerzo podría consistir, por ejemplo, en recuperar la información borrada de un backup o en volver a instalar los originales[4].

De igual forma, la jurisprudencia ha receptado que se incluya al "archivo informático" dentro de las previsiones del art. 184 inc. 5 del C.P. -ya que al momento de su redacción original no se encontraba esta posibilidad-, dado que la reforma de la ley de delitos informáticos incluyó dentro de esta figura agravada a los datos, documentos, programas o sistemas informáticos públicos. Así, se ha considerado que *"...un 'archivo informático' queda comprendido en el tenor literal del tipo penal de daño agravado. Ello así por cuanto, el archivo informático, mantiene la sustancia del archivo "tradicional", esto es, las características que permiten describirlo como tal, radicando su novedad sólo en el soporte donde se encuentra almacenada la información"*[6].

Además de las figuras analizadas previamente, podría considerarse aplicable -en algún caso puntual- el art. 197 del C.P. en cuanto penaliza el entorpecimiento de las investigaciones. De acuerdo al texto de la norma: *"Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida."* El agregado *"...de otra naturaleza"* que realiza la ley de delitos informáticos permite pensar en esta posibilidad, dado que una de las consecuencias directas e inmediatas del *ransomware* es el de paralizar la actividad de la empresa que fue atacada. Por ejemplo, para una organización cuya principal actividad se desarrolle a través del intercambio permanente de correo electrónico, o bien cualquier sitio de comercio electrónico, este tipo de ataques puede llegar a constituir un entorpecimiento de sus comunicaciones[2].

[2] En este sentido se consideró en el caso Marchione antes citado, al ser atacada una agencia de publicidad bajo la modalidad de envío masivo de spam.

2.1 Formas de Ataque del *Ransomware*

Existen diferentes formas por las cuales un usuario puede ser infectado por este tipo de malware. A continuación, se describen los más comunes:

- Ingeniería social: comprende los recursos que utilizan los ciberdelincuentes para persuadir a sus víctimas a que realicen ciertas acciones para vulnerar la seguridad de sistemas informáticos o acceder a su información[7]. En la mayoría de los casos, bajo engaños o persuasión, las víctimas instalan algunos programas sin saber que se tratan de *spyware* o algún otro *malware*. El envío de promociones falsas o programas malintencionados forman parte, por ejemplo, de las estrategias que utilizan al aprovechar la ingenuidad y la falta de información de las víctimas. Esta es la principal técnica utilizada por los ciberdelincuentes para engañar a las posibles víctimas e inducirlos a que ejecuten los ransomware. Las principales fuentes de esta destreza, son:
    - Correo electrónico: es una de las principales vías de ataque, con la que se busca que el usuario descargue y ejecute un archivo adjunto. Los contenidos de estos correos usualmente incluyen: algún tipo de premio, notificaciones de que somos buscados por autoridades, envío de documentos u otro tipo de mensajes para incentivar la descarga y ejecución.
    - Descarga Web: es otra forma de Ingeniería Social que busca persuadir al usuario para que descargue y ejecute un programa. En general, se intenta engañar al usuario indicando que debe descargar un antivirus, gestor de descargas o algún otro software “deseable” por él.
    - Redes sociales: por medio de ellas, tanto a través de publicidades, publicaciones o mensajes directos, los ciberdelincuentes buscan persuadir a que el usuario acceda a una página que dispara el ataque. En particular en este caso además de incitar la descarga, el ataque propagarse a los contactos del usuario.
- Vulnerabilidades del Sistema Operativo: Se entiende por vulnerabilidad a un defecto de seguridad de un sistema informático que permite a un atacante aprovecharlo y generar un comportamiento indeseado en el sistema. El recurso utilizado para explotar dicha vulnerabilidad es normalmente un programa o secuencia de comandos, denominado “*exploit*”, que persigue el objetivo de concretar un determinado ataque, como ser: acceso de forma no autorizada, toma de control, consecución de privilegios no concedidos lícitamente o ataques de denegación de servicio. Supongamos entonces que se dispone de un equipo conectado a Internet el cual tiene como sistema operativo Windows XP, del cual se conocen vulnerabilidades que permiten ejecutar software en forma remota. El atacante entonces puede ejecutar el *exploit* e instalar un *ransomware*, y sólo es cuestión de tiempo para que todos los archivos se encuentren cifrados y se pida un rescate por ellos.

- Vulnerabilidades de Red: Normalmente un equipo que se conecta a Internet se encuentra en un entorno de red que actúa como intermediario entre origen y destino de las comunicaciones que involucran al mismo. En este contexto existirán diversos dispositivos cuya tarea fundamental es simplemente la de transmitir la información de un punto a otro sin alterarla. Pero diversos sucesos indeseados podrían ocurrir sin que el usuario lo note. Por ejemplo, uno de los dispositivos intermediarios podría encontrarse infectado redirigiendo todo el tráfico hacia un equipo intermedio que modifique el contenido original generando vulnerabilidades sobre el equipo que finalmente lo recibe. Este ataque se conoce como *"man in the middle"* y brinda un escenario fértil para la introducción de *ransomware* en los equipos destino y origen.

2.2 *Modus Operandi* del *Ransomware*

Por lo general, el *ransomware* tiene cinco fases esenciales:

1. El ciberdelincuente debe infiltrarse en el sistema informático víctima o de alguna forma inducir a la víctima para que realice la ejecución del *malware*.
2. Una vez que comienza la ejecución, el *ransomware* busca en el sistema los archivos de interés (de acuerdo a extensiones de los archivos, o algún patrón determinado en base a su nombre o ubicación) y comienza la operación de cifrado.
    a. El cifrado de los archivos puede consistir en la eliminación o corrupción de la tabla de particiones o estructuras del sistema de archivos, el cifrado débil con mecanismos tipo XOR o ROR/ROL de los datos, o el cifrado criptográfico (con variantes de AES y alguna forma de negociación de claves).
    b. Algunos *malwares* de este tipo no se molestan en aplicar un cifrado fuerte, simplemente basta con que el usuario no pueda acceder a sus archivos y generar en él el pánico necesario para inducir al pago.
    c. En aquellas variantes que si utilizan cifrado fuerte y claves aleatorias, es necesario que el equipo está conectado a internet y así poder guardar en los servidores de *Command-and-Control (C&C)* las claves para que luego sea posible descifrar los archivos.
3. Informar a la víctima de lo ocurrido y pedir un rescate para la recuperación de los datos cifrados. Además, se instruye al usuario (de manera resumida) sobre cómo adquirir Bitcoins y la utilización de la red Tor para comunicarse con los "secuestradores virtuales".

4. Una vez que se realiza el pago, el usuario debe comunicarse con los ciberdelincuentes para informar del mismo y solicitar la (o las) claves de descifrado. En algunas ocasiones, los ciberdelincuentes utilizan distintas estrategias para fomentar el pago, por ejemplo:
    a. Indicar una fecha límite luego de la cual se eliminarán las claves de cifrado. En realidad, es una fecha arbitraria que se utiliza para aumentar la presión sobre el usuario, o aumentar el monto de rescate que piden luego de pasado un tiempo.
    b. Algunos ciberdelincuentes descifran uno o dos archivos del usuario "gratis" para demostrar que cuentan con las claves adecuadas para recuperar la información del usuario.
    c. Otros *malwares* utilizan figuras o personajes de la cultura popular para inducir miedo en sus víctimas, por ejemplo el *ransomware* conocido como *Jigsaw*[8] (y sus variantes).
5. Finalmente, queda en la "buena voluntad" u "honestidad" del ciberdelincuente en aportar las claves y/o herramientas que van a realizar la recuperación de la información cifrada.

El *modus operandi* del *ransomware* es muy simple. Lo más habitual, es que el ciberdelincuente encuentre la forma de ejecutar el malware en el sistema informático de la víctima mediante las técnicas descriptas en la sección anterior. Una vez que logró su ejecución es sólo una cuestión de tiempo hasta que todos los datos hayan sido cifrados.

Bitcoin es un tipo de moneda que sirve para intercambiar bienes y servicios. Sin embargo, a diferencia de otras monedas tal como las usamos a diario, el Bitcoin es una divisa electrónica que presenta novedosas características, destacándose por su eficiencia, seguridad y facilidad de intercambio. Su mayor diferencia frente al resto de monedas, es que se trata de una moneda descentralizada, por lo que escapa al control estatal de emisión y circulación. Ello así, porque el Bitcoin no tiene un emisor central como sucede con los dólares, los euros o el peso; la criptomoneda es producida por las personas y empresas de alrededor del mundo dedicando gran cantidad de recursos a la minería[3].

Según la tecnóloga Morgen E. Peck, la manera más sencilla de entender a Bitcoin es pensarlo como un registro contable digital[9]. Peck propone imaginar el sistema como una mesa donde se sientan los individuos y llevan entre todos el mismo registro contable, donde se indica el número de criptomonedas de cada uno de ellos. Los saldos de cada cuenta constituyen información pública, y las transferencias de fondos se anuncian como transacciones a todos los presentes, que deben verificar su autenticidad. Aunque las criptomonedas no tienen un respaldo físico, los intentos de gastar más de una vez la misma moneda serán detectados por los demás participantes, que no autorizarán la transacción. Esta ilustración muestra el mecanismo general con el que

[3] Explicar el mecanismo de minería de Bitcoins excede los propósitos de este trabajo, para profundizar en la temática en general se recomienda leer *"Bitcoin for the Befuddled"*[10].

opera Bitcoin, pero en lugar de una mesa se comparte una red *peer-to-peer*, y las transacciones se dan entre direcciones cuya posesión se verifica por medio de criptografía.

3 Aspectos de seguridad: prevención y planes de contingencia

Dado el nivel de riesgo que presenta este tipo de malware es fundamental considerar el uso de todo mecanismo de **prevención** disponible. Los mismos se sintetizan a continuación:

- ***Backups*:** La realización de copias de resguardo periódicas es una de las mejores medidas de prevención que se pueden tomar. No sólo son efectivos contra *ransomware*, sino para otras situaciones donde la información de un sistema pueda verse comprometida.

  La eficiencia del *backup* depende principalmente de tres factores: la frecuencia con que se realizan, los contenidos que abarcan, y el modo en que se llevan a cabo (ya sean completos o incrementales). Otro punto de suma importancia es que se debe verificar, de forma regular idealmente, que los *backups* realizados efectivamente tienen la capacidad de restaurar la información ante un ataque.

  Finalmente es preciso atender al modo en el cual debe restablecerse el *backup*. Es inapropiado hacerlo desde el mismo sistema operativo infectado por el *ransomware*, ya que podría suceder que el mismo aún permaneciera activo y también el *backup* resulte cifrado. La más recomendable es utilizar un sistema operativo cargado por primera vez en memoria (por ejemplo, una distribución de Linux tipo *"live"*) solo para el restablecimiento del *backup*.

  Si bien tener resguardo en un sistema de *cloud computing* es una alternativa válida, no se recomienda esta estrategia cuando éste se encuentra sincronizado con una carpeta del sistema a proteger, dado que existen algunos tipos de *ransomware* que cifran este tipo de carpetas, y, en consecuencia, al sincronizarse también afecta a la información que se encontraba alojada en la nube.

- **Uso de antivirus residentes:** es un recurso útil que reduce la probabilidad de ataque de un virus de este tipo. Es importante que precisamente sea "residente", es decir que se ejecute permanentemente a fin de impedir el acceso del *malware* en el momento que intenta ingresar al sistema o que, al menos, detecte su intrusión antes de que cifre toda la información.

- **Estudios de seguridad y puesta a punto por expertos:** debe considerarse contratar expertos en esta temática, para que realicen un estudio de vulnerabilidades sobre el sistema, a fin de dejarlo en un estado que reduzca las posibilidades de recibir ataques.

- **Capacitación preventiva de usuarios:** Uno de los puntos más vulnerables de una organización o empresa, es probablemente la cantidad de usuarios que uti-

liza sus sistemas. El usuario, usualmente inexperto en cuestiones de seguridad informática, desconoce los recursos que un atacante puede utilizar para intentar tomar el control sobre los dispositivos. Frente a este escenario es importante capacitarlos a fin de proveerles directivas claras para el uso diario que reduzcan esta debilidad.

En cuestiones de configuración de los equipos, algunas de las recomendaciones podrían comprender:

- Muestra de extensiones ocultas de los archivos. Esto podría evitar que, por ejemplo, un archivo ejecutable cuyo nombre es "archivo.pdf.exe" se visualice como "archivo.pdf" confundiendo al usuario y dando la oportunidad al *malware* de ser ejecutado.
- Filtro de tipos de archivo ejecutables en casillas de email.
- Puntualmente en el caso de contar con un equipo con sistema operativo Windows, es recomendable deshabilitar la ejecución desde las carpetas "AppData" y "LocalAppData" de cada usuario[11]. Estas carpetas suelen ser utilizadas por malwares para ocultar archivos ejecutables.
- Deshabilitación de acceso por escritorio remoto. Comúnmente los equipos suelen tener habilitada esta funcionalidad. Si bien su uso requiere del ingreso de credenciales de usuario, un malware podría automáticamente probar secuencialmente todas las contraseñas posibles hasta tanto encuentre la correcta y así ingresar ilegítimamente al sistema.

Con relación a recomendaciones directas al usuario podría considerarse:

- Evitar realizar click sobre cualquier enlace que se encuentre en un email cuyo remitente es desconocido.
- Si se descarga un archivo, porque se confía del remitente, es recomendable verificar que no se trate de un archivo del tipo ejecutable (ej: .exe)
- Si, en cambio, el usuario ejecuta el archivo sospechoso, poder desactivar las conexiones de red inalámbricas y quitar bien el cable de red inmediatamente, es una acción acertada a fin de reducir riesgos y dar tiempo a realizar un análisis de antivirus.

- **Arquitecturas de red bien definidas:** Es indudable que, si "seguridad informática" es lo que se pretende lograr en una organización, entonces una correcta diagramación del esquema de redes debe llevarse a cabo. Cuando un equipo se encuentra en un segmento de red aislado del resto, es muy poco probable entonces que se vea infectado desde algún otro que se encuentra fuera de dicho segmento. En este sentido deben considerarse diversos aspectos tales como:

- Control de uso de canales compartidos. Debe evitarse el uso de redes de tipo Wi-Fi ya que todo equipo que se encuentre en las cercanías podría ser víctima de malware o atacante del sistema. En un caso así resultará mucho más difícil controlar el alcance, que en un caso de conexiones por cable físico.
- Control de visibilidad. Es recomendable el uso de subredes que representen áreas lógicas, en donde los equipos dentro de ellas no tengan acceso a otros ubicados en otras subredes. De todas maneras, la forma más efectiva de generar esa segmentación es directamente evitar la conexión física entre estos segmentos.
- Uso de *firewalls* (o cortafuegos) donde se bloquee todo tráfico de red que no tenga un propósito útil para el objetivo de la organización o empresa.

Por otra parte, con relación a los planes de contingencia, se puede recomendar:

- **Evitar el pago de rescate:** El usuario afectado suele caer la desesperación por recuperar sus datos, que ciertamente pueden ser indispensable para el desarrollo de su actividad. Ante uno de estos ataques el primer paso efectuado usualmente es consultar a expertos en la materia. Cuando el diagnóstico técnico no es alentador, el usuario entonces comienza a evaluar cualquier alternativa que esté a su alcance para restablecer lo que ha perdido.

  Si bien lo último que desearía hacer la víctima es pagar el rescate al ciberdelincuente, también ocurre que es, aparentemente, el único recurso del que dispone. Es así que gran parte de los usuarios afectados termina cayendo en el pago, lo que fomenta un contexto aún mucho peor.

  Cuando un usuario paga lo primero que ocurre es que queda registrado como uno con voluntad de pagar. Esto genera más posibilidad de volver a ser víctima porque el ataque ya rindió fruto para el ciberdelincuente.

  Otra consecuencia de este acto, que trasciende la situación particular, es que fomenta el crecimiento de este mecanismo perverso de obtención de dinero vía extorsión. Es un problema que afecta a cualquier usuario, en cualquier parte del mundo y que va en crecimiento a medida que cada víctima accede al pago por el rescate de su información. Cada vez existen más tipos de *ransomware* que superan a los anteriores en complejidad y capacidad de ataque. Esto es lo que debe procurar evitarse y el camino es no acceder a la demanda del ciberdelincuente.

- **Alta de *backups*:** Como se mencionó previamente, tener una correcta política de *backups* es uno de los métodos de prevención más efectivos en este contexto. Cuando un *ransomware* finalmente logra encriptar los datos de una empresa u organización, y su ataque tiene la suficiente eficacia como para no dejar alternativa más que el pago del rescate, la recuperación de la información a partir de un *backup* es la única herramienta realmente efectiva que puede dar solución completa al problema. Pero este método verdaderamente útil, debe

llevarse a cabo respetando ciertas consideraciones. Durante el restablecimiento de un *backup* se debe garantizar absolutamente que el mismo no sea también afectado por el *ransomware* que provocó el incidente. Para ello, podrían aplicarse las siguientes políticas:

- Realizar la operación en un entorno desconectado. Tanto el equipo contenedor de las copias de seguridad como el que las recibe, deben encontrarse desconectados físicamente de cualquier red cuyo alcance exceda a estos dos.
- Durante el proceso no se debe utilizar, bajo ningún concepto, el sistema operativo infectado. En lugar de ello debe utilizarse un sistema operativo cargado en memoria por primera vez exclusivamente para el caso puntual. Aquellos que funcionan en modo *"live"* (que no requieren instalación previa), pueden ser una opción viable para este punto.
- Reinstalar completamente el sistema operativo infectado. Es menester asegurarse que el virus no persista en el equipo.

- **Uso de antivirus:** Para realizar la limpieza de los equipos infectados será necesaria la utilización de algún antivirus, o una herramienta especializada en remover el *malware* del que se fue víctima. De no realizarse esta tarea, cabe la posibilidad que algún componente siga activo en el equipo y continúe con la propagación e infección de nuevos equipos, o vuelva a activarse en el mismo equipo.
- **Uso de herramientas de descifrado:** frente al auge del *ransomware* algunas empresas, investigadores y expertos de seguridad han analizado y aplicado ingeniería inversa a varias amenazas de este tipo, y proveen servicios y herramientas que permiten identificar qué *malware* realizó el ataque e, idealmente, ayudar en el proceso de descifrar la información[12, 13].

4 Denuncia, preservación de la evidencia, y tareas forenses

"¿Qué debo hacer cuando el sistema informático ha sido infectado por un ransomware?" Esa es la pregunta fundamental que le surge a una víctima cuando ha tomado conocimiento de que su sistema ha sido vulnerado. Como primera medida y acción principal a tomar, se debe apagar el o los sistemas informáticos infectados para evitar que el malware siga propagándose, no volviéndolo a encender hasta contactar a un técnico idóneo en este tipo de infecciones.

Como se ha explicado anteriormente, todo aquel que haya sido infectado por este malware es víctima de un delito y como tal puede hacer la **denuncia** correspondiente en la comisaría cercana al domicilio o en la fiscalía abocada a este tipo de casos, para que se realice la investigación correspondiente.

Es fundamental que el medio de almacenamiento del equipo informático que fue infectado no sea manipulado, a fin de preservar -de la mejor manera posible- la evidencia digital del delito. Además, como el ciberdelincuente aporta un mail de contacto para negociar con él, recomendamos no mantener ningún tipo de contacto y dejar que la investigación tome su curso una vez realizada la denuncia.

Al momento de realizar la denuncia, ya sea en la comisaría o fiscalía, es preciso establecer la fecha y el modo en el cual ha sido infectado por el *ransomware*. Los puntos fundamentales que deben mencionarse, además de las preguntas de rigor que efectuará el funcionario público, son:

1. Fecha exacta y hora aproximada de cuando tuvo conocimiento que fue infectado.
2. Acciones que estaba realizando al tener conocimiento de la infección.
3. Acciones previas inmediatas realizadas al ser infectado.
4. Si mantuvo contacto vía mail con los ciberdelincuentes, aportar dichos mails con el encabezado completo[4]. Es fundamental el encabezado ya que posee datos del remitente y pueden ser de utilidad para la investigación.
5. Aportar el/los medio/s de almacenamiento del equipo informático infectado.

Con dicha información, se abrirá una investigación donde una de las primeras medidas a tomarse será la realización de una **pericia informática forense** sobre el medio de almacenamiento que se ha aportado.

Dicho procedimiento será realizado por un perito informático oficial, ya sea este miembro del Ministerio Público Fiscal o de la Policía de acuerdo a la intervención y facultades que se asignan en cada jurisdicción.

Las partes intervinientes en la investigación serán notificadas del procedimiento y de la fecha de inicio de la pericia, con el objeto de ejercer los derechos acordados por las normas procesales. Las tareas del perito serán las siguientes[14]:

1. Realizar la imagen forense del medio de almacenamiento afectado.
2. Hacer la comprobación de hashes[5] del dispositivo original y su copia forense.
3. Analizar la imagen forense en busca de las causas de la infección.

Una vez que se obtiene la imagen forense, comienza la etapa de preparación del entorno forense y análisis. En ese sentido, primero se debe verificar cuál es el grado de cifrado de los datos alcanzado por el *ransomware*. Para ello, se debe utilizar una má-

[4] El encabezado de un email siempre acompaña al mensaje y lleva consigo evidencia digital que puede resultar útil. Si el usuario no sabe recuperarlos, deberá pedir ayuda al instructor o perito informático.

[5] Los algoritmos de hash son funciones matemáticas que resumen un bloque de datos de tamaño variable en una cadena alfanumérica representativa de tamaño fijo.

quina o estación de trabajo totalmente aislada de cualquier red de datos y sin conexión a Internet. Esto es para evitar que, si por alguna razón el *ransomware* que está alojado en la imagen forense, intenta propagarse, no pueda hacerlo.

Cuando el ambiente de trabajo está preparado, lo primero que se debe hacer es montar lógicamente la imagen forense como si fuese un disco y analizar su estructura. Aquí pueden presentarse dos escenarios:

1. Que el *ransomware* haya cifrado o eliminado la tabla de particiones del dispositivo, por lo cual, no será posible ver la estructura del mismo de una manera sencilla. En este caso, será necesario reconstruir la tabla antes de proceder[15].
2. Que no se haya cifrado la tabla de particiones del dispositivo, por lo tanto, será posible ver la estructura de directorios del mismo.

Una vez que se puede ver la estructura de directorios del dispositivo, será necesario tratar de recolectar la siguiente información del mismo:

- Sistema operativo principal instalado en el dispositivo: Si se observa una carpeta que se llama "home", da la pauta que se está bajo una distribución de "Linux"; si, en cambio, se visualiza una carpeta con el nombre "Windows", se tratará de un sistema operativo en entorno de Windows[6].
- Luego verificar cuántos usuarios hay en el sistema operativo. Cada usuario tiene una carpeta con su nombre dentro del directorio "Users" para el caso de los sistemas operativos más modernos como Windows 7, 8 o 10 o "Documents and Settings" para versiones antiguas de Windows como es el caso de Windows XP.
    - Dentro de cada carpeta con el nombre de los usuarios existe un archivo denominado "NTUser.DAT" el cual describe toda la actividad del usuario, como por ejemplo los archivos recientemente ejecutados por el mismo. Dicho archivo es fundamental para determinar cuáles fueron los movimientos del usuario en el momento de la infección. Es posible que este archivo haya sido alcanzado por el ransomware y sea imposible su visualización. Si esto sucede, esta operación no podrá ser realizada.
- Analizar el registro de eventos del sistema operativo: el registro de eventos de Windows se encuentra dentro del directorio "windows\system32\winevt". Dicho registro contiene y describe todos los eventos que el sistema operativo detectó, como por ejemplo los inicios de sesión de los diferentes usuarios del sistema, las acciones realizadas por dichos usuarios como así también los inicios de sesión remotos. Es muy importante analizar este contenido, debido a que puede dar indicios de qué usuario estaba utilizando el sistema al momento de la infección y las acciones realizadas por el mismo.

[6] Para este trabajo, se supondrá que el sistema operativo a analizar es Windows, ya que es el escenario más común en este tipo de casos.

- Analizar el Registro de Windows[7]: Si estos archivos no han sido cifrados, es posible analizarlos. Los más importantes aquí serán las ramas SOFTWARE, SYSTEM, SECURITY y SAM, ya que en ellas se podrán obtener datos como: cuál fue el último usuario que estuvo operando el sistema y a qué hora, qué software fue instalado en el sistema, y los archivos que fueron ejecutados recientemente.

Una vez analizados estos puntos, se tendrá un mejor conocimiento de cómo fue el ataque recibido, si se produjo mediante un archivo que se descargó de Internet (mail o descarga de la web) o si fue por un ataque remoto. Si es este último se podrá informar desde qué dirección IP[8] se recibió el ataque. En ambos casos se podría identificar el archivo malicioso que dañó el sistema, qué tipo de cifrado fue utilizado y la fecha y hora del ataque. Cabe destacar que estos datos podrán ser obtenidos siempre y cuando dicha información no haya sido alcanzada por el *ransomware* y la misma no haya sido cifrada.

Es muy importante poder identificar el archivo malicioso que infectó al sistema para poder analizarlo y eventualmente realizar pruebas aisladas[16]. En lo posible se debe extraer el archivo (generalmente un ejecutable) de la imagen forense y tratar de ejecutarlo para tratar de determinar a qué C&C se conecta y también tratar de establecer si la clave de cifrado utilizada es una clave fija. Es primordial ejecutar este tipo de malware en una computadora que esté totalmente aislada de la red de trabajo dónde se está actuando. Además, debe ser una computadora destinadas a pruebas, con lo cual, no debe contener ningún tipo de dato o información relevante, ya que es posible que resulte secuestrada. Existen dos técnicas a realizar en esta prueba:

1. **Análisis de paquetes de red** una vez ejecutado el archivo malicioso, se podrá determinar a qué C&C se intenta comunicar el proceso malicioso disparado en la prueba, así identificarlo, saber su dirección IP y el modus operandi del mismo. Cabe mencionar que saber su dirección de IP es de utilidad para poder determinar en qué país se encuentran los posibles atacantes.
2. **Volcado de la memoria RAM** consiste en crear un archivo que contenga la información que se encuentra en la memoria principal en el momento en que el archivo malicioso comienza a cifrar los datos de la computadora. Esto es importante para que, si el proceso de cifrado utilizado por el archivo malicioso utiliza una clave fija para secuestrar los datos, luego se podrá analizar dicho archivo y quizás así, poder obtener la clave para descifrar los datos.

Por estas dos técnicas mencionadas es que es importante ejecutar el archivo malicioso y así, poder dar una respuesta más detallada del incidente que se está analizando.

[7] El registro de Windows es una base de datos jerárquica que almacena los ajustes de configuración y opciones en los sistemas operativos Microsoft Windows.

[8] Una dirección IP es un número que identifica en un momento determinado a un dispositivo conectado a Internet.

Una vez culminadas todas las tareas descriptas en esta sección, se elaborará un informe detallado con todos los resultados y conclusiones obtenidas del acto de pericia llevado a cabo, el cual se elevará a la Fiscalía u organismo actuante que interviene.

5 Conclusiones

Como se ha visto en el trabajo, el problema del *ransomware* es complejo, y si bien puede haber soluciones y medidas de protección para las víctimas, es complicado de analizar e investigar desde el punto de vista judicial. Resumiendo lo expuesto, podemos decir que:

- Son múltiples los puntos a tener en cuenta para evitar ser víctima de un *ransomware*, los cuales van desde el uso del antivirus, la topología de red hasta la capacitación de los usuarios.
- Un *backup* bien realizado es la mejor forma de evitar la pérdida datos ante un ataque de *ransomware*.
- El pago de la recompensa no es recomendado, ya que alienta a la economía de los ciberdelincuentes, dándoles lugar para seguir apostando a códigos cada vez más complejos y eficientes que nos llevarán a un panorama más comprometido en un futuro. En su lugar, se recomienda llevar a cabo la denuncia y tratar de recuperar la información con herramientas provistas por expertos.
- La guía de procedimientos aquí presentada asiste tanto a la víctima como al perito informático. Esto permite aumentar las probabilidades de obtener información acerca del ataque realizando y el atacante, y también disminuye las probabilidades de que la víctima pierda una parte de su información.
- Incluso en el caso que no sea posible recuperar la información, presentar la denuncia a las autoridades sirve para que los peritos oficiales e investigadores armen un mapa de la situación que permita detectar posibles patrones en común, a partir de otras evidencias que se reúnan en las investigaciones, que permitan establecer más información acerca del ataque y eventualmente, del atacante.

Si bien el escenario es complejo y desafiante, utilizando metodologías correctas, y aplicando estrategias y políticas de seguridad adecuadas, es posible hacerle frente a la amenaza del *ransomware*.

Agradecimientos

Se agradece a la Universidad FASTA, al Ministerio Público Fiscal de la Provincia de Buenos Aires y a la Municipalidad de General Pueyrredon por brindar un espacio

único de trabajo como es el Laboratorio de Investigación y Desarrollo de Tecnología en Informática Forense. En particular, a Ana Haydée Di Iorio, Fernando Greco, Hugo Curti, Juan Ignacio Iturriaga, Juan Ignacio Alberdi y Sebastián Lasia, investigadores del Grupo de Investigación en Informática Forense y Sistemas Operativos de la Universidad FASTA.

Referencias

1. Cristian Borghello, *"Crimeware: el crimen del Siglo XXI"*, ESET Latinoamérica (2009). Disponible en: https://www.welivesecurity.com/wp-content/uploads/2014/01/crimeware_crimen_siglo_xxi.pdf.
2. *"The Next Tier - 8 Security Predictions for 2017"*, Trend Micro USA (2016). Disponible en https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017.
3. *"Kaspersky Security Bulletin 2016 - The ransomware revolution"*, Kaspersky lab (2016). Informe y datos adicionales disponibles en https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/.
4. Pablo Palazzi, *"Delitos Informáticos"*, Ed. Ad-Hoc (2000), pág. 139.
5. Ley 26.388 de la República Argentina.
6. *Caso "Marchione, Gabriel"* - Cámara Nacional Criminal y Correccional Federal, Sala 2°, 15/11/2005.
7. Cristian Borghello, *"El arma infalible: la Ingeniería Social",* ESET Latinoamérica (2009). Disponible en: http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf.
8. Lawrence Abrams, *"Jigsaw Ransomware Decrypted: Will delete your files until you pay the Ransom"* (blogpost, Abril 2016). Disponible en: https://www.bleepingcomputer.com/news/security/jigsaw-ransomware-decrypted-will-delete-your-files-until-you-pay-the-ransom/.
9. Morgen Peck, *"Bitcoin: The Cryptoanarchists' Answer to Cash"*. IEEE Spectrum (2012). Disponible en: http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash.
10. Conrad Barski, Chris Wilmer, *"Bitcoin for the Befudled"*. (2015). no starch press, San Francisco, EEUU.
11. Lysa Myers, *"11 formas de protegerte del ransomware, incluyendo Cryptolocker"*. Revista digital welivesecurity en español. (2015). ESET Latinoamérica. Disponible en: https://www.welivesecurity.com/la-es/2015/07/08/11-formas-protegerte-del-ransomware-cryptolocker/.
12. Servicio online *"ID Ransomware"* https://id-ransomware.malwarehunterteam.com/.
13. Decrypters de Emsisoft https://decrypter.emsisoft.com/.
14. Ana H. Di Iorio et al., *"Guía Integral de Empleo de la Informática Forense en el Proceso Penal"*. (2016). Universidad FASTA, Mar del Plata.
15. Documentación de TestDisk (software). *"TestDisk Step by Step"*. Disponible en http://www.cgsecurity.org/wiki/TestDisk_Step_By_Step.
16. Michael Sikorski, Andrew Honig, *"Practical Malware Analysis"*. (2012). no starch press, San Francisco, EEUU.