ARTÍCULO DE INVESTIGACIÓN DOCUMENTAL
REVISTA DEL CENTRO DE GRADUADOS E INVESTIGACIÓN. INSTITUTO TECNOLÓGICO DE MÉRIDA. Vol. 31 NÚM. 62. PP. 38 – 43 SEP. 2016 ISSN 0185-6294

ORIGEN Y EVOLUCIÓN DEL CRYPTOVIRUS RANSOMWARE

Martínez-García[1], Holzen Atocha; Moo Medina[1], Melquizedec y Chuc Us[1], Ligia Beatriz

[1] **Ingeniería en Sistemas Computacionales.** Instituto Tecnológico Superior Progreso. Boulevard Víctor Manuel Cervera Pacheco, S/N x 62 Progreso, Yucatán, México. Tel/Fax: 01 969 934 30 23

***Autor contacto:** hmartinez@itsprogreso.edu.mx; mmoo@itsprogreso.edu.mx; lbeatriz@itsprogreso.edu.mx

Recibido: 26/agosto/2016 **Aceptado**: 25/septiembre/2016 **Publicado**: 30/septiembre/2016

RESUMEN

El ransomware es un tipo de malware especializado en el secuestro de datos o equipos informáticos para generalmente solicitar un pago por el rescate de los mismos. En los últimos años, esta variante de malware ha causado pérdidas millonarias a empresas y paralizado hospitales alrededor del mundo, lo que deriva una situación delicada en el ámbito digital. Si bien su utilización es lucrativa con efectividad para los ciberdelincuentes, estos no conformes ahora también lo ofrecen como servicio a disposición de otros para automatizar el proceso de ataque a terceras víctimas, lo que hace que el incremento de riesgo sea mayor. Los administradores de TI y en general, cualquier persona debe estar consciente de los peligros y consecuencias del ransomware.

Palabras Clave: secuestro de datos, servicios en nube, evolución, rescate, seguridad de la información

ABSTRACT

Ransomware is a type of malware specialized in hijacking data or computer equipment generally request a ransom payment thereof. In recent years, this variant of malware has caused millions in losses to businesses and inoperable hospitals around the world, resulting a delicate situation in the digital realm. While their use is effectively lucrative for cybercriminals, these nonconforming now also offer it as a service available to others to automate the process of third attack victims, which causes the increased risk is greater. IT managers and in general, anyone should be aware of the dangers and consequences of ransomware.

Keywords: data kidnapping, cloud services, evolution, ransom, information security

INTRODUCCIÓN

En un mundo globalizado, la importancia de mantener los datos sensibles es cada vez mayor con el avance tecnológico. Cabrera Albornoz [1] toma como referencia la norma ISO 27001:2013 cuando afirma que "La información es un activo que, como otros activos comerciales importantes, tiene valor para la organización y, en consecuencia, necesita ser protegido adecuadamente". Los ciberdelincuentes han adoptado variantes de técnicas para lucrar con este principio, y una de las más actuales y peligrosas es la infección de dispositivos con un tipo de malware llamado ransomware.

El ransomware es un software malicioso que infecta al equipo anfitrión y secuestra al equipo o a los datos, generalmente para solicitar un pago como rescate de los mismos recursos secuestrados. De manera análoga a malware, que viene de las palabras "malicious software" en inglés [2], el término ransomware hace referencia al rescate en cuestión (ransom, en inglés). Se conoce así al malware que pretende lucrarse a través de la extorsión.
El ransomware habitualmente contiene alguna rutina capaz de cifrar archivos y/o bloquear el acceso al sistema. Cifra ficheros en el sistema que infecta con la suposición que sean importantes para la víctima, que se ve obligada a pagar una cantidad de dinero al creador del malware si quiere que el atacante le proporcione el método para poder descifrar los archivos y recuperarlos. De lo contrario los ficheros permanecerán cifrados o incluso, en un momento dado, serán borrados por completo del sistema [3].

METODOLOGÍA

Este trabajo de investigación documental proporciona a personas especializadas en el tema, académicos y hombres de negocios un tema para reflexionar y tomar las medidas pertinentes ante esta evolución hasta el momento imparable del ransomware, cuyos efectos negativos alrededor del planeta han sido evidentes y documentados por un tiempo considerable.

El alcance de este trabajo es describir la evolución del ransomware, desde sus primeras variantes hasta su evolución a servicio en la nube. Para eso, la investigación se basó en fuentes diversas tales como artículos de investigación, libros, portales de internet y una

experimentación propia con el ransomware "Hidden Tear", liberado originalmente con fines educativos.

Orígenes del ransomware

De acuerdo a Gazet [4] el ransomware tiene sus inicios en 1989, cuando se propagó por primera vez un malware de este tipo en aquella época. La forma de propagación se dio mediante el envío masivo de discos flexibles de 3 ½ pulgadas a través del correo postal. Estos discos se presentaban como portadores de información privilegiada que ayudaría a encontrar una cura contra el Síndrome de Inmuno Deficiencia Adquirida. Al ingresarlos al equipo, el troyano se activaba e internamente colocaba un contador que esperaba el reinicio del anfitrión para ir en aumento. Cuando el equipo anfitrión tenía su reinicio número 90, el malware cifraba los nombres de los archivos, lo que dejaba inutilizable el equipo anfitrión y las aplicaciones.

Las víctimas podían ver el archivo de licencia, el cual solicitaba dos tipos de pago de rescate diferentes, ya sea por 365 aplicaciones funcionales o por el disco duro completo. El pago debía hacerse vía cheque bancario con unos datos específicos a la compañía "Pc Cyborg Corporation". Por eso este malware fue conocido como "AIDS info disk" o "PC Cyborg Trojan".

El cifrado resultó ser débil, utilizando un algoritmo de cifrado monoalfabético, pero el primer antecedente de ransomware había surgido, aunque propiamente no se le nombraba de esa manera.

Auge y popularidad

A partir de ese momento, los investigadores en seguridad tomaron interés en este campo, y a pesar de que surgían nuevas variantes de este malware, los cambios tecnológicos y las regulaciones en los sistemas de pago hacían que la efectividad de este ataque mermase. Durante algunos años se mantuvo bajo el índice de ataques con este comportamiento. Sin embargo, el uso de cifrado cada vez más complejo y los sistemas de moneda digitales y por ende, el Bitcoin, harían que resurgiese el uso de ransomware.

Bitcoin, a diferencia de la mayoría de monedas digitales que no son tomadas como serias en el mundo de la economía, es una moneda digital viable, con capitalización de mercado creciente y ventajas tales como la descentralización y la anonimidad bidireccional en el sistema de transferencias [5]. Los ciberdelincuentes se han dado cuenta de esto, y han adoptado nuevas estrategias de extorsión digital altamente lucrativa y con niveles de efectividad superiores a los esperados en otro tipo de malware.

El crecimiento de este malware ha sido exponencial, de tal manera que en 2013 fue de 500% en proporción comparada con los ataques lanzados en 2012 [6] (Symantec, 2014). Esta cifra aumenta año con año, lo que permite proyectar un aumento importante en ataques de este tipo. De acuerdo a estadísticas actualizadas de Intel Security [7] (2016), el número de muestras nuevas de ransomware tuvo un breve descenso en 2014, repuntando al siguiente año con un crecimiento de ataques con variantes nuevas en el año 2015, y siguiendo la tendencia en 2016. Esto es representado en la Figura 1.

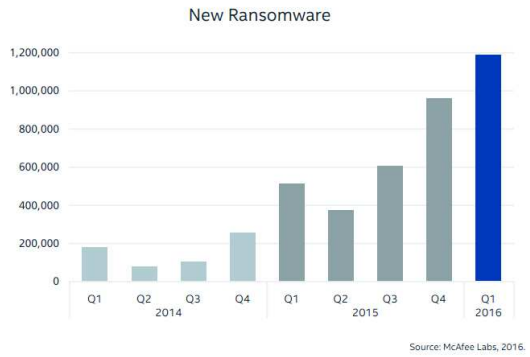

Figura 1. Crecimiento de nuevo ransomware entre 2014 y el primer cuarto de 2016. Fuente: [7]

El total de casos de ransomware es aún más preocupante, ya que como lo muestra la Figura 2, la tendencia es el aumento de variantes de ransomware a un ritmo acelerado.

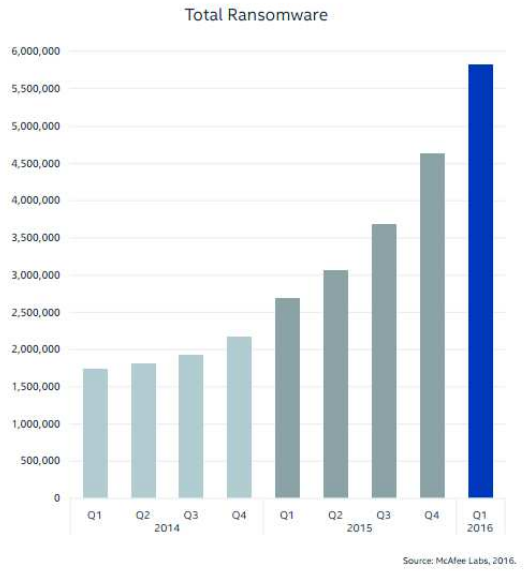

Figura 2. Total de muestras de ransomware entre 2014 y primer cuarto de 2016. Fuente: [7]

Comportamiento del ransomware

La forma de extorsionar a la víctima básicamente está clasificada en dos comportamientos similares. Es por eso que el ransomware puede ser clasificado en dos variantes: Ransomware-Crypto y Rasomware-Locker. [8]

Un Ransomware está clasificado en Crypto cuando su comportamiento está orientado a cifrar los datos y los archivos para dejarlos inservibles e ilegibles para cualquiera y así exigir un rescate económico en bitcoins. Esto obliga al usuario final a pagar hasta obtener la clave de descifrado. No se afectan los archivos del sistema operativo ni sus funcionalidades, a fin de que el usuario pueda abrir y comprobar que los archivos se encuentran cifrados e ilegibles. Las imágenes, los videos, archivos de texto, y archivos con extensiones comunes son los objetivos de esta categoría.

El ransomware-locker por el contrario se centra en el sistema operativo o sus funcionalidades, dejando una funcionalidad mínima. Los usuarios con conocimientos técnicos en computación se percataron que es posible rescatar los datos y reinstalar la funcionalidad de la parte afectada. El impacto y efectividad de este ransomware es menor en comparativa con el crypto, por lo cual cada vez es menor la tasa de ataques de este tipo.

Éxito y consolidación del ransomware

El ransomware-crypto representa la infección por ransomware más esparcida en la actualidad. El éxito y la efectividad de este ataque se consolidan en gran porcentaje gracias a la ingeniería social. La ingeniería social en el campo de la seguridad informática es definida por Jara & Pacheco [9] como "la práctica para obtener datos confidenciales a través de la manipulación psicológica de usuarios legítimos". Aunque esta definición no es única, es un hecho que esta técnica explota ciertas características propias del ser humano [10], manipulándolo psicológicamente o mediante el engaño para instarlo a hacer (o dejar de hacer) alguna operación sensible y que permite al ciberdelincuente proseguir con el ataque. Las técnicas de ingeniería social pueden ser variadas, pero no necesariamente exclusivas entre sí [11].

Los niveles de afectación del ransomware son cada vez mayores. Entre abril de 2014 y junio de 2015, el Internet Crime Complaint Center (IC3), del FBI, recibió 992 reportes relacionados a CryptoWall y otras variantes de ransomware [12], cuyas víctimas tuvieron pérdidas económicas que llegaron a los 18 millones de dólares. CryptoWall y sus variantes se han estado utilizando activamente desde abril de 2014, para infectar víctimas que incurren en gastos no solo por el rescate que piden los cibercriminales detrás, sino también por otros costos asociados. A este rescate, que oscila entre 200 y 10 mil dólares, se suman la pérdida de productividad, la mitigación del riesgo en la red, los servicios de Tecnologías de Información, tasas legales, y más [13]. Tal como señala el informe del IC3, estos fraudes financieros afectan tanto a individuos como a compañías del sector empresarial.

Los ciberdelincuentes que utilizan el ransomware como herramienta han encontrado un nicho de mercado atractivo para ellos: los hospitales. En febrero de 2016, el Hollywood Presbyterian Medical Center en Estados Unidos fue extorsionado con la cantidad de 9000 bitcoins para desbloquear los recursos secuestrados, lo que equivalía en ese momento a 3.6 millones de dólares [14]. Después de una negociación, se logró reducir la cifra al equivalente de 17,000 dólares, pagados en bitcoins. Los sistemas y datos estuvieron fuera de línea durante 10 días. Allen Stefanek, CEO del Hospital, afirmó que pagando era la forma más rápida y eficaz de restaurar las funciones administrativas y de manejo de datos de los pacientes [15].

Otros hospitales fueron atacados a partir de entonces, tales como el Hospital Metodista en Henderson en el estado de Kentucky, el cual fue declarado en estado de emergencia [16], MedStar, la red de salud de 10 hospitales de Maryland [17], y el Kansas Heart Hospital, el cual efectuó el pago solicitado por los ciberdelincuentes a fin de recibir la clave de descifrado, pero en cambio recibió una segunda solicitud por un pago de rescate mayor [18].

Los hospitales son el blanco perfecto para este tipo de extorsión, ya que proporcionan cuidados críticos y se basan en información actualizada de los registros de pacientes. Sin un acceso rápido a las historias de drogas, las directivas de cirugía y otros datos, la atención al paciente puede quedar retrasado o paralizado, lo que hace que los hospitales se vean obligados a pagar un rescate en lugar de los retrasos de riesgo que podrían resultar en la muerte de alguien y también demandas millonarias. Otro motivo para considerarlos ideales a este ataque, es que los empleados son entrenados para proteger la confidencialidad y privacidad del paciente, pero no se les educa digitalmente en seguridad de la información [16].

Ransomware as a Service

Algunos ciberdelincuentes han evolucionado el concepto de ransomware, y lo han convertido en un esquema de distribución afiliado, lo que da lugar al RaaS (Ransomware as a Service). Esto es, ponen a disposición de terceros un panel o kit de creación de ransomware, donde el afiliado tiene la oportunidad de personalizar la dirección bitcoin, el tipo de cifrado, la cantidad de rescate a solicitar, entre otros. El esquema general como se muestra en la Figura 3 es simple: El proveedor del servicio genera el malware, el afiliado lo distribuye y los dos obtienen ganancias. Así, se genera una relación ganar-ganar, pues el ciberdelincuente no se preocupa de la distribución, y el afiliado no necesita conocimientos técnicos de programación.

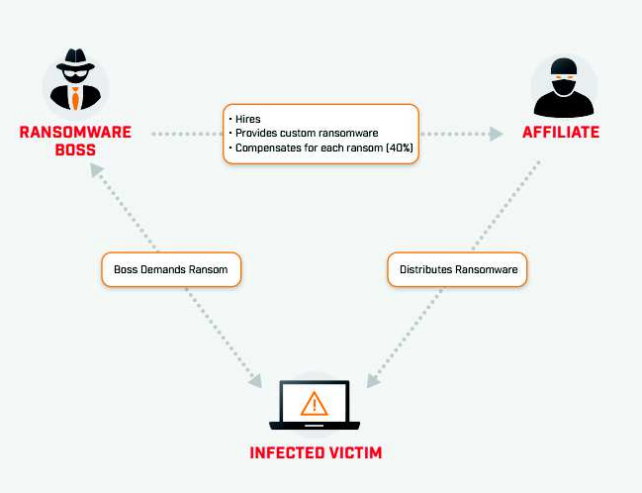

Figura 3. Esquema del Ransomware as a Service. Fuente: [19]

Entre los servicios documentados se encuentran los siguientes [20]:

Tox: Uno de los primeros kits de creación de ransomware. Es gratuito, basta con un registro y configurar el monto de rescate, el texto a desplegar después de la infección y un código de verificación. Genera un archivo .scr ejecutable de alrededor de 2 mb. Ganancia: 80% Afiliado, 20% Creador del ransomware.

Fakben: Kit no gratuito, se necesita pagar 50 dólares como suscripción única. Más configurable que Tox, ofrece algunos servicios extra de hacking. Ganancia: 90% Afiliado, 10% Creador del ransomware.

Encryptor RaaS: Cuota de 5% para el servicio, se puede configurar fecha límite de pago y un precio distinto dependiendo si se efectúa el pago antes o después de esa fecha. El cliente obtiene una dirección Bitcoin única que actúa como un identificador en toda la campaña.

Hidden Tear: Este ransomware originalmente fue distribuido como código abierto y para fines meramente educativos. Fue liberado en el portal Github en agosto de 2015 por el experto en seguridad informática Utku Sen. El autor ha escrito el código de fuente abierta en GitHub para que todos los interesados podría comprender la anatomía de un ataque ransomware. Hidden Tear utiliza el bloque de cifrado AES para cifrar los datos, tiene un muy pequeño cargador de tan sólo 12 KB, y cuenta con capacidades de evasión antivirus. Actores de delitos informáticos, por desgracia, utilizan este kit para construir ransomware en el mundo real.

ORX Locker: Tiene como regla poner el precio de desbloqueo en al menos $75 dólares, y para evitar malos entendidos con el afiliado, un tercero procesa los datos estadísticos como número de máquinas infectadas y número de pagos realizados.

Ransom32: La comisión de este kit es de 25% del total. Sin embargo, el estar escrito en javascript lo hace multiplataforma y atractivo para los afiliados.

Janus: Es de las plataformas más recientes. Porcentaje variante dependiendo el número de Bitcoins logrados. Requiere privilegios de administrador para instalarse y efectuar su proceso.

AlphaLocker: A diferencia de otros casos RAAS que simplemente alojan las campañas de afiliación, las personas que están detrás AlphaLocker venden, literalmente, un paquete con una copia única del ransomware real, el descifrador binario principal, y el panel de administración por 65 dólares en promedio (pagados en Bitcoin). El cliente, por lo tanto, consigue el control total del ransomware y puede albergar, distribuir o incluso revenderlo.

Cabe destacar que la mayoría de estos servicios se encuentran en la Deep Web o Web Profunda, utilizan métodos de ofuscación para evadir antivirus y garantizan la anonimidad mediante el pago en Bitcoins.

RESULTADOS Y DISCUSIÓN

Para comprobar personalmente el comportamiento de un ransomware-crypto, los autores de este trabajo realizaron pruebas con un ransomware gratuito, el cual fue nombrado "Hidden Tear", liberado con fines didácticos. Este malware pasó de ser open source a ser considerado RaaS. Hidden Tear tiene dos formas de operar: el modo online, tradicional de los ransomware actuales, y el modo offline, el cual es demostrativo.

Primero se analizó el código, y se hizo constar de las configuraciones propias en el código fuente, con la posibilidad de configurar el sitio donde se enviará el password de descifrado, el tipo de cifrado a aplicar a los archivos, la ubicación a cifrar por carpetas o por unidad y las extensiones de los archivos a cifrar, con la opción de agregar o modificar alguno. Un fragmento de código donde se puede ver la configuración de los archivos a cifrar se muestra a continuación en la Figura 4.

```
117  //encrypts target directory
118  public void encryptDirectory(string location, string password)
119  {
120    //extensions to be encrypt
121    var validExtensions = new[]
122    {
123    ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png",
124    ".csv", ".sql", ".mdb", ".sln", ".php", ".asp", ".aspx", ".html", ".xml", ".psd"
125    };
126    string[] files = Directory.GetFiles(location);
127    string[] childDirectories = Directory.GetDirectories(location);
128    for (int i = 0; i < files.Length; i++)
129    {
130      string extension = Path.GetExtension(files[i]);
131      if (validExtensions.Contains(extension))
132      {
133          EncryptFile(files[i],password);
134      }
135    }
136    for (int i = 0; i < childDirectories.Length; i++)
137    {
138      encryptDirectory(childDirectories[i],password);
139    }
140  }
```

Figura 4. Fragmento de código para configurar y validar extensiones de archivo. Fuente: Elaboración propia

Analizando el fragmento, es posible ver que, si coincide la extensión del archivo con las que el ransomware quiere

cifrar, se dispone a hacerlo, mediante el método EncryptFile tal y como lo muestra la Figura 5.

```
//Encrypts single file
public void EncryptFile(string file, string password)
{
  byte[] bytesToBeEncrypted = File.ReadAllBytes(file);
  byte[] passwordBytes = Encoding.UTF8.GetBytes(password);
  // Hash the password with SHA256
  passwordBytes = SHA256.Create().ComputeHash(passwordBytes);
  byte[] bytesEncrypted = AES_Encrypt(bytesToBeEncrypted, passwordBytes);
  File.WriteAllBytes(file, bytesEncrypted);
  System.IO.File.Move(file, file+".locked");
}
```

Figura 5. Fragmento de código que cifra el archivo. Fuente: Elaboración propia

Resultados de prueba de comportamiento

Finalizando la configuración, se realizó la prueba en un entorno controlado con una máquina virtual, se procedió a infectar el anfitrión y en task background los archivos con extensiones comunes de los folders configurados previamente fueron cifrados con algoritmo AES, lo que hacía prácticamente imposible su descifrado. También fue posible observar que no ataca archivos que no hayan sido configurados previamente. Esto se verificó con archivos pdf almacenados en las carpetas objetivo.

Por otra parte, se recibió en el servidor que simulaba ser del atacante la clave de descifrado, además de datos como nombre del equipo y nombre de usuario. El análisis de Hidden Tear puede ser revisado en otro trabajo relacionado [21].

CONCLUSIONES

Este trabajo ha presentado un panorama general del ransomware y su evolución. Las pérdidas financieras, así como del factor tiempo, son una realidad de este malware. Las empresas, hospitales, instituciones y en general, cualquier persona que haga uso de los datos y la información, debería tener conocimiento de este riesgo latente para tomar las medidas pertinentes. La evaluación de la seguridad de la información a menudo es tomada en cuenta después de sufrir las consecuencias de un desastre. El desconocimiento o desinterés pueden poner en jaque a las entidades que se infecten con este malware. Como se ha mencionado, el ransomware es un peligro que cada vez más aumenta en cantidad y complejidad, por lo que se requiere un análisis situacional en cada entidad con infraestructura tecnológica para determinar si se está preparado o no ante una eventual infección o ataque. Para finalizar, mencionar otro aspecto a tomar en cuenta: la educación de los usuarios finales en cuanto a seguridad. Si se les educa adecuadamente en gestión de riesgos, es posible dirigir al punto mínimo el riesgo de ser impactados por este malware, y por otras amenazas latentes.

AGRADECIMIENTOS

Los autores agradecen al Tecnológico Nacional de México por financiar el proyecto de investigación “Cloud Storage para neutralizar los efectos del ransomware en datos sensibles” del cual forma parte este estudio.

También mencionar al Instituto Tecnológico Superior Progreso por las facilidades otorgadas en los recursos de tiempo y espacio.

REFERENCIAS BIBLIOGRÁFICAS

[1] Sánchez, S. (2014). Importancia de implementar el SGSI en una empresa certificada BASC.

[2] Moure, M. (2013). Secuestro de información por medio de malware.

[3] Cercas, J. Diagnóstico de ataques de seguridad mediante redes bayesianas.

[4] Gazet, A. (2010). Comparative analysis of various ransomware virii. Journal in computer virology, 6(1), 77-90.

[5] Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013, May). Zerocoin: Anonymous distributed e-cash from bitcoin. In Security and Privacy (SP), 2013 IEEE Symposium on (pp. 397-411). IEEE.

[6] Symantec. (2014) Internet Security Threat Report 2014::Volume 19. Recuperado de http://www.symantec.com/es/mx/security_response/publications/threatreport.jsp

[7] Intel Security. (2016). McAffee Labs Threats Report. June 2016. Recuperado el 10 de Julio de 2016, a partir de http://www.mcafee.com/mx/resources/reports/rp-quarterly-threats-may-2016.pdf

[8] Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware Digital Extortion: A Rising New Age Threat. Indian Journal of Science and Technology, 9, 14.

[9] Jara, H., & Pacheco, F. G. (2012). Ethical Hacking 2.0. Usershop.

[10] Mieres, J. (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas). Recuperado http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

[11] Zhou, Y., & Jiang, X. (2012, May). Dissecting android malware: Characterization and evolution. In 2012 IEEE Symposium on Security and Privacy (pp. 95-109). IEEE.

[12] Internet Crime Complaint Center (IC3) | Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes. (s/f). Recuperado el 12 de Junio de 2016, a partir de https://www.ic3.gov/media/2015/150623.aspx

[13] Sabrina Pagnotta. (2015, June 24). CryptoWall, el ransomware más activo: reportan pérdidas por 18 millones de dólares. Recuperado el 26 de diciembre de 2015, a partir de http://www.welivesecurity.com/la-

es/2015/06/24/cryptowall-ransomware-activo-millones-dolares/

[14] Narinder Purba. (2016, febrero 15). Hospital de Estados Unidos fue víctima de un ransomware "al azar". Recuperado el 24 de febrero de 2016, a partir de http://www.welivesecurity.com/la-es/2016/02/15/hospital-estados-unidos-victima-ransomware/

[15] Yadron, D. (2016, febrero 18). Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers. The Guardian. Recuperado a partir de https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center

[16] Zetter, K. (2016, marzo 30). Why Hospitals Are the Perfect Targets for Ransomware. Recuperado el 14 de junio de 2016, a partir de https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/

[17] Gallagher, S. (2016, abril 7). Maryland hospital: Ransomware success wasn't IT department's fault. Recuperado el 24 de junio de 2016, a partir de http://arstechnica.com/security/2016/04/maryland-hospital-group-denies-ignored-warnings-allowed-ransomware-attack/

[18] Hospital pays ransomware, but doesn't get files decrypted. (s/f). Recuperado el 24 de junio de 2016, a partir de http://www.extremetech.com/extreme/229162-hospital-pays-ransomware-but-doesnt-get-files-decrypted

[19] Kremez, V. (2016, abril) Ransomware as a Service: Inside an Organized Russian Ransomware Campaign. Recuperado el 20 de agosto de 2016, a partir de https://www.flashpoint-intel.com/home/assets/Media/Flashpoint_Ransomware_April2016.pdf

[20] Ransomware as a Service: 8 Known RaaS Threats - InfoSec Resources. (s/f). Recuperado el 14 de agosto de 2016, a partir de http://resources.infosecinstitute.com/ransomware-as-a-service-8-known-raas-threats/

[21] Martínez, H., & Chuc, L. Hidden Tear: Análisis del primer Ransomware Open Source. Avances y perspectivas de la innovación, investigación y vinculación, 31.