

Recepción: 22 de noviembre de 2016**Aceptación:** 08 de diciembre de 2016**Publicación:** 14 de diciembre de 2016

INFECCIÓN CON RANSOMWARE EN EL SERVIDOR DE BASE DE DATOS DEL SISTEMA ONSYSTEC ERP

RANSOMWARE INFECTION ON THE ONSYSTEC ERP SYSTEM DATABASE SERVER

Raúl Armando Ramos Morocho¹Enrique Gallegos Mosquera²

1. Universidad Técnica de Babahoyo. Facultad de Administración, Finanzas e Informática. Babahoyo, Los Ríos (Ecuador). E-mail: rrosamos@utb.edu.ec

2. Universidad Técnica de Babahoyo. Facultad de Administración, Finanzas e Informática. Babahoyo, Los Ríos (Ecuador). E-mail: enriquedgallegos@gmail.com

Citación sugerida:

Ramos Morocho, R.A. y Gallegos Mosquera, E. (2016). Infección con ransomware en el servidor de base de datos del sistema Onsystem ERP. *3C Tecnología: glosas de innovación aplicadas a la pyme*, 5(4), 56-76. DOI: <http://dx.doi.org/10.17993/3ctecno.2016.v5n4e20.56-76/>.

RESUMEN

Se presenta un estudio de caso de una infección efectuada en un servidor de base de datos con Windows Server, con un tipo de software mal intencionado denominado ransomware; una situación alarmante, porque la empresa víctima de este ataque no pudo realizar sus operaciones y transacciones a causa de la infección. El virus no solo detuvo el motor de la base de datos, sino también aplicó un cifrado (no conocido) en todos los archivos del sistema, y solicitaba que se contacte a un email para negociar la devolución del acceso a las bases de datos y archivos encriptados.

ABSTRACT

We present a case study of an infection performed on a Windows Server database server, with a type of malicious software called ransomware. It is an alarming situation because the company that was the victim of this attack could not carry out its operations and transactions because of the infection. The virus not only stopped the database engine, but also applied an encryption (not known) in all files of the system, and requested that an email be contacted to negotiate the return of access to encrypted files and databases.

PALABRAS CLAVE

Ransomware, cifrado, servidor.

KEY WORDS

Ransomware, encryption, server.

1. INTRODUCCIÓN

La inclusión de las TIC en las empresas privadas, en los últimos años ha crecido exponencialmente, esto ha hecho posible que la productividad aumente; y como ilustrativamente se dice que “la cizaña crece junto con el trigo”, así como aumentan las herramientas de gestión de negocios, también aparece en el escenario el famoso software mal intencionado, cuyo objetivo es obtener beneficio (generalmente económico) introduciendo malware en un ordenador empresarial, aprovechando las vulnerabilidades y bugs de los sistemas de información o utilizando ingeniería social.

Cuando se trata el tema de “virus informáticos”, la tendencia es restarles importancia y suponer que son algún tipo de software que crea accesos directos en una unidad USB extraíble, o simplemente que es un programa que ralentiza el funcionamiento de un computador; si bien la tecnología aumenta para beneficiar las organizaciones en general, lo cierto es que a la par, evolucionan también los ataques de los delincuentes informáticos; las unidades de TIC de las empresas, tienen ahora la responsabilidad de actualizar su conocimiento respecto a este tema y capacitar a los usuarios de los sistemas de información, para potenciar los recursos de software disponibles y para tener conciencia que una red de computadoras suele ser “una calle sin semáforos” para los ciberdelincuentes.

Este trabajo tiene como título “*infección con ransomware en el servidor de base de datos del sistema Onsystem ERP*”, la información ha sido recopilada por medio de la entrevista a las personas que estuvieron directamente involucradas en el caso. El objetivo de este estudio de caso es analizar y aumentar el conocimiento de los ataques con ransomware a los sistemas de información; para mitigar los casos de infección con este tipo de virus, como bien se sabe es mucho más sencillo entender un tema cuando se presenta en la vida real, por esa razón se utilizan este tipo de trabajos como técnica de aprendizaje.

2. DESARROLLO

La compañía Onsystem S.A. es una empresa dedicada a brindar soluciones informáticas a sus clientes, desde el año 2009, su sede es en la ciudad de Ventanas, en la provincia de Los Ríos. El producto estrella de la compañía es el sistema llamado Onsystem® ERP 6.0, este es un sistema informático empresarial que gestiona funciones de integración y administración de los negocios relacionados con las tareas de producción, automatizando los procesos y controlando la disponibilidad de los productos (inventario) y los flujos de trabajo.

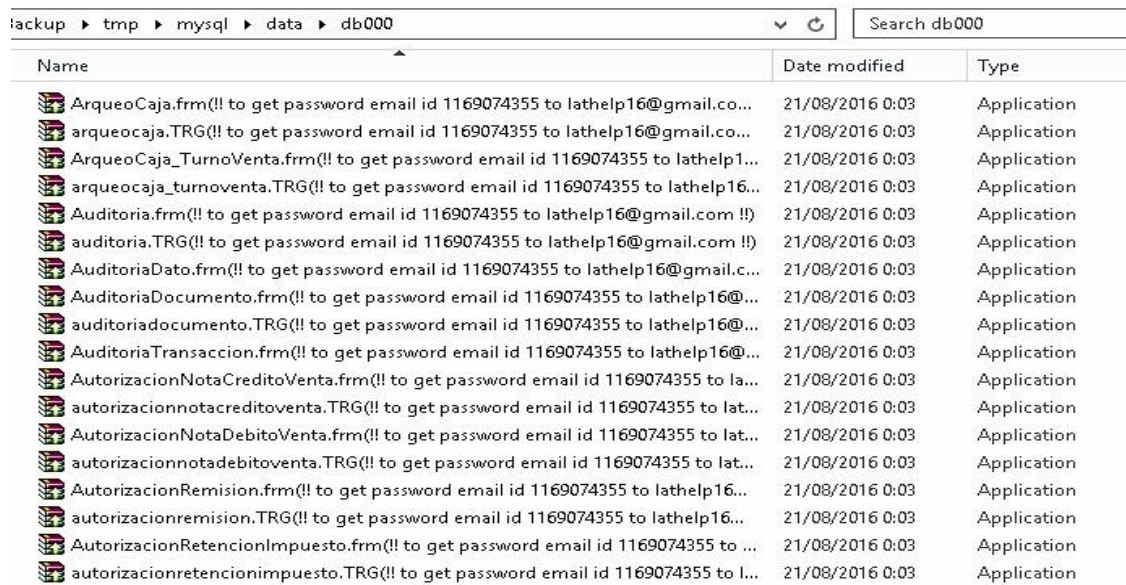
A inicios del año 2016, Onsystem implementó su sistema ERP en una empresa llamada Agroxven, que se dedica a la compra, selección y exportación de productos de agricultura, en especial el cacao; sin embargo, por ser una empresa grande, en la que participan en realidad doce compañías anexas, el proceso de implementación había sido evolutivo y parsimonioso, es decir, se había visto la necesidad de ajustar o personalizar ciertos requerimientos, por lo que el proceso se desarrolló en un tiempo más o menos prolongado, ya que hasta el octavo mes del año aún se estaban precisando detalles, agregando funciones o capacitando a los usuarios; pese a seguir en el proceso de implementación, Agroxven ya estaba trabajando con normalidad, haciendo uso del sistema ERP de Onsystem.

En el mes de agosto del 2016, un día sábado, los usuarios del sistema en Agroxven, notaron que no pudieron acceder al servidor de la base de datos, o sea, no podían facturar, ingresar información o generar reportes. Todos los servicios de los sistemas que utilizan habían sido dados de baja, por lo tanto, no podían acceder a la información almacenada en la base de datos, que se encontraba en un ordenador con Windows Server.

Hasta ese momento nadie sabía lo que ocurría, todos pensaban que era un fallo en el sistema ERP, sin embargo, los otros sistemas que usaban tampoco respondían, por lo que descartaron esa opción. Pensaron también que era un error en algún recurso de la red; bueno, el caso es que ellos dejaron pasar ese día y no comunicaron a Onsystem lo sucedido, por lo que ese día no se pudo solucionar el problema.

El día lunes de la semana siguiente todavía continuaba el problema por lo que ahora si le notificaron a Onsystem que el sistema no se podía conectar al servidor; entonces fue el equipo de soporte técnico a revisar cual era el problema. Después de analizar el asunto, se dieron cuenta que el servicio de Mysql, que es el SGBD que utiliza Onsystem ERP, había sido detenido, es decir, el motor de la base de datos no estaba funcionando, pero también había en ese equipo otros servidores de otras bases de datos: Postgresql y Cobol, y todos estos fueron también detenidos.

Después notaron que exactamente todos los archivos como: documentos, ficheros comprimidos, y todo lo que estaba almacenado en el disco duro, en ambas particiones, aparecían con extensión de una aplicación, es decir, un archivo ejecutable; como bien se conoce, por ejemplo: un documento de Microsoft Word, tiene una extensión de un documento, de igual manera una música o un video, éstos no pueden ser una aplicación, por lo que el ingeniero de soporte técnico supo que se trataba de algún tipo de virus; hay una gran cantidad de virus en la red que hacen casi lo mismo, la mayor parte de estas infecciones se producen mediante unidades de USB extraíbles, la diferencia es que, algunos de estos virus, son algo inofensivos, pues ocultan los verdaderos archivos y crean otros con los mismos nombres pero con otra extensión, generalmente con una extensión de aplicación o accesos directos, en esos casos el problema se resuelve con un simple comando en la consola de comandos de Windows, y se eliminan los archivos creados por el virus que en realidad no pasan de los 2kb cada uno. El caso Agroxven no era tan sencillo, porque los archivos mantenían su peso original, eso significa, que no eran archivos creados por el virus para engañar al usuario, sino que eran los ficheros originales, pero el malware había aplicado sobre ellos un algoritmo de encriptación, para cambiar el nombre y la extensión, pero manteniendo internamente su contenido verdadero, de alguna manera, modificaron el código hexadecimal para alterar su arquitectura, y hacerlos ilegibles, pues se convirtieron en una aplicación, provocando que al hacer clic para leerlos, se ejecuten para solicitar una clave de descifrado o para causar una mayor propagación del virus.



Name	Date modified	Type
ArqueoCaja.frm(! to get password email id 1169074355 to lathelp16@gmail.co...	21/08/2016 0:03	Application
arqueocaja.TRG(! to get password email id 1169074355 to lathelp16@gmail.co...	21/08/2016 0:03	Application
ArqueoCaja_TurnoVenta.frm(! to get password email id 1169074355 to lathelp1...	21/08/2016 0:03	Application
arqueocaja_turnoventa.TRG(! to get password email id 1169074355 to lathelp16...	21/08/2016 0:03	Application
Auditoria.frm(! to get password email id 1169074355 to lathelp16@gmail.com !!)	21/08/2016 0:03	Application
auditoria.TRG(! to get password email id 1169074355 to lathelp16@gmail.com !!)	21/08/2016 0:03	Application
AuditoriaDato.frm(! to get password email id 1169074355 to lathelp16@gmail.c...	21/08/2016 0:03	Application
AuditoriaDocumento.frm(! to get password email id 1169074355 to lathelp16@...	21/08/2016 0:03	Application
auditoriadocumento.TRG(! to get password email id 1169074355 to lathelp16@...	21/08/2016 0:03	Application
AuditoriaTransaccion.frm(! to get password email id 1169074355 to lathelp16@...	21/08/2016 0:03	Application
AutorizacionNotaCreditoVenta.frm(! to get password email id 1169074355 to la...	21/08/2016 0:03	Application
autorizacionnotacreditoventa.TRG(! to get password email id 1169074355 to lat...	21/08/2016 0:03	Application
AutorizacionNotaDebitoVenta.frm(! to get password email id 1169074355 to lat...	21/08/2016 0:03	Application
autorizacionnotadebitoventa.TRG(! to get password email id 1169074355 to lat...	21/08/2016 0:03	Application
AutorizacionRemision.frm(! to get password email id 1169074355 to lathelp16...	21/08/2016 0:03	Application
autorizacionremision.TRG(! to get password email id 1169074355 to lathelp16...	21/08/2016 0:03	Application
AutorizacionRetencionImpuesto.frm(! to get password email id 1169074355 to ...	21/08/2016 0:03	Application
autorizacionretencionimpuesto.TRG(! to get password email id 1169074355 to l...	21/08/2016 0:03	Application

Figura 1. Captura de los datos mysql encriptados.

Fuente: Elaboración propia.

Se observa como los comprobantes electrónicos y demás datos están como tipo aplicación y el nombre ha sido modificado, agregando el email y el id de la infección, con los cuales se podía contactar con el creador del virus.

Se continuó revisando todo el equipo, entonces aparece la parte más trágica de todas, toda la información de la base de datos estaba también encriptada, o sea, los archivos sql, y los que tenían la información de la empresa; ¡un desastre total!, habían perdido toda la información de años en tan solo horas. Onsystem ERP, posee una herramienta que efectúa respaldos de la base de datos todos los días de manera automática, y los almacena en una carpeta en el servidor, pero todos los backups de la base de datos habían sido guardados en el mismo equipo, ¡qué problema más grande!, esto significa que ellos también estaban bajo el efecto de la infección, el caso era grave porque no podían restaurar esos respaldos ya que eran inaccesibles por el SGBD.

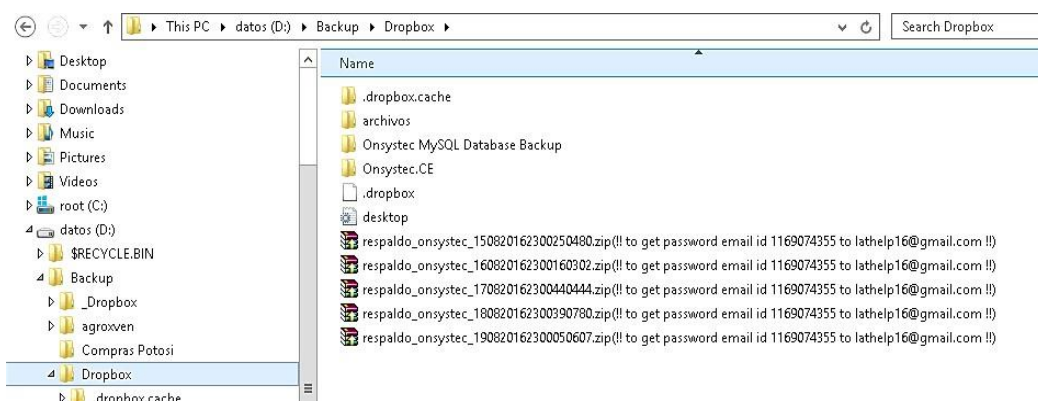


Figura 2. Captura de los backups encriptados.

Fuente: Elaboración propia.

Ahora bien, los respaldos se almacenaban en una carpeta en el mismo equipo, pero esa carpeta estaba sincronizada con una cuenta de Dropbox, el famoso software de almacenamiento en la nube, que proporciona una capacidad que va desde 5 hasta 15Gb de almacenamiento gratuito pero aumentable comprando uno de los planes que ofertan, en este caso era una cuenta gratuita, el ingeniero de Onsystemec previendo que algo como esto podía suceder, incluso algún daño físico en el equipo, o alguna otra situación; con los backups en la nube, se evitaría la pérdida de la información.

Entonces cada vez que Onsystemec backups realizaba los respaldos en la carpeta donde se guardaban, automáticamente se actualizaba en la nube, hasta allí todo bien, el problema era que los respaldos no se almacenaban por versiones en la nube, sino que los reemplazaba, es decir, por ejemplo: el backup del miércoles en la noche se subía a la nube a las 12:00 de la noche, al día siguiente a la misma hora se realizaba el nuevo backup, el cual reemplazaba al anterior. Por lo tanto, lo más lógico era pensar que si el virus encriptó los archivos el viernes en la noche, antes de que se realizara el backup automático, el respaldo se iba a subir a la nube encriptado y éste reemplazaría el respaldo del jueves, provocando el deterioro total de ese respaldo, y aunque Onsystemec tenía respaldos aparte, que había copiado del Dropbox manualmente, pero estaban guardados en el mismo servidor; ahora bien, en otro caso, si el virus encriptaba la información después del backup automático, la situación era similar, solo con la diferencia de un día, ya que el sábado también se haría el respaldo automático a la misma hora, por lo que el resultado habría sido el mismo.

En realidad, lo que sucedió fue que el equipo donde estaban los servidores de las bases de datos había sido infectado con un Ransomware, este es un tipo de software mal intencionado que básicamente “secuestra” (encripta) toda la información que hay en un ordenador, como archivos, documentos, etc., y después pide una remuneración económica para su “rescate” (descifrar). La manera de cómo este equipo se infectó con este virus, a ciencia cierta no se conoce aún, sin embargo, se puede sugerir que era un virus que ya estaba en el equipo desde antes de la instalación del sistema ERP, aunque aún no se activaba, pero estaba monitoreando la información, capturando contraseñas, datos etc., para ver qué tan lucrativo pudiera ser el ataque, y en el momento que le pareció oportuno, lo ejecutó; primero deteniendo el servicio del SGBD, esto significa que el malware tenía privilegios de usuario administrador para poder detener el servicio.

Esto pudo ser posible utilizando una vulnerabilidad del software SMBD o S.O., o simplemente habiendo obtenido la contraseña del usuario administrador previamente, por medio del mismo software mal intencionado, haciendo uso de un keylogger o un aplicativo similar, y después cifró toda la información con un algoritmo desconocido; dando lugar a que la única manera de recuperar información de extrema importancia, sea pagando la suma de dinero que ellos solicitan.

Este tipo de virus es muy peligroso y dañino, con la capacidad de enviar a la bancarrota a una empresa, en tan solo minutos. El nombre de este Ransomware se desconoce hasta el momento, puesto que existen una gran cantidad, para nombrar algunos: Satana, CTB Locker, Locky, Zepto, entre muchos otros. Otra teoría con respecto a la manera en que se infectó el equipo, pudo haber sido por medio del mismo Dropbox, ya que éste se actualizaba a tempranas horas de la madrugada, y el malware pudo haberse introducido por el mismo puerto del Dropbox, y no sería la primera vez

que los softwares mal intencionados utilicen estos medios, que son muy utilizados por los usuarios, para infectar ordenadores y para capturar información que les puede proporcionar eventos para alcanzar sus objetivos lucrativos.

Otra teoría, pero poco probable es que algún usuario haya revisado algún correo electrónico o descargado alguna aplicación en el servidor, y ejecutó el malware sin darse cuenta, pero de acuerdo a los usuarios, dicen que nadie maneja ese ordenador, solo el administrador de la base de datos que es el ingeniero a cargo, y es de Onsystemec. Seguidamente de que Onsystemec descubrió que se trataba de un ransomware, unos de los virus más lucrativos que existen, consideraron pagar por el rescate, pues los archivos eran indescifrables, y era información con la que la empresa trabaja y la necesitaban con urgencia, más allá de cómo se infectaron, había que resolver el problema.

El caso es que existen un tipo de ransomware que después que el usuario paga el monto económico solicitado por el delincuente informático, éste de todas maneras elimina la información y la víctima no tendrá acceso a ella jamás a pesar de haber pagado el rescate; considerando esta situación, Onsystemec empezó a analizar otras opciones, entonces se dan cuenta que el respaldo almacenado en Dropbox, no estaba encriptado, y entonces se fijaron en la fecha y era el backup realizado el día viernes, el mismo día que el virus se activó, eso significa que efectivamente el virus se ejecutó después de la sincronización de Dropbox. La explicación es que una vez que el virus encriptó todos los archivos, inmediatamente bloqueó los puertos de comunicación, incluido el de Dropbox, por ello el backup no se pudo actualizar en la nube el día siguiente, ya que había perdido la conexión.

Fue así como se pudo salvar la información de la base de datos, y en realidad no se perdió casi nada, sólo lo que trabajaron el día sábado, pero no ingresaron al sistema, desde ese punto de vista, ciertamente no se perdió nada de la base de datos, gracias a ese error del ransomware de bloquear los puertos de comunicación. La solución que tuvo este caso, realmente se puede decir que fue buena fortuna o una acción torpe del ransomware, aun así, sirve como un ejemplo claro para concientizar que la información es lo más valioso de una empresa y es necesario tomar todas las precauciones preventivas y correctivas para evitar estos ataques a futuro.

Los antecedentes de este tipo de casos son muchos en Ecuador y en otros países, si se lee una revista de tecnología o alguna fuente de noticias, existe una variedad de eventos dados en diferentes empresas o simplemente en usuarios convencionales, sin tener el debido conocimiento para evitar una infección y/o para emplear medidas de recuperación de la información después de haber sido infectados, y sencillamente asumiendo la pérdida de ella. Para no citar un antecedente demasiado lejano, se narrará una experiencia que se dio en el año 2014, en el GADPLR (Gobierno Autónomo Descentralizado Provincial de Los Ríos) en la ciudad de Babahoyo.

En una ocasión un usuario del área de administración notificó a la unidad de TIC que no podía trabajar porque un programa se ejecutaba en primer plano y no era posible detenerlo, también comentó que el S.O. estaba ralentizado y algunos archivos no se encontraban ni se podía abrir su contenido, el jefe del área envió a alguien a revisar el asunto; entonces se revisó el equipo y se supo que era un virus, en ese momento no fue relevante el mensaje que mostraba la ventana emergente del programa que estaba en primer plano (que estaba en inglés), la cual si la detenía

con el administrador de tareas, al instante volvía a aparecer; se sugirió que era un programa de esos que se descargan de páginas como *softonic*, entre otras, que a veces engañan a los usuarios haciéndoles creer que son los programas que buscan, pero en realidad son un grupo de malware que se instalan en el ordenador, son algún tipo de trojanos o gusanos de internet, pero con objetivos no tan dañinos.

Aunque no se leyó lo que decía el mensaje, lo que sí se pudo observar fue el nombre de esa aplicación, ésta se llamaba “*CTB Locker*”, hasta ese momento la persona que revisó el equipo desconocía por completo la existencia de ese tipo de virus, por lo que se hizo respaldo de los archivos y datos, formateó el disco duro y reinstaló el sistema operativo, aunque se notó que los archivos todos presentaban una extensión aleatoria y tenían el icono de fichero desconocido de Windows, pero pareció irrelevante ese detalle.

Después de formatear el equipo y reinstalar el sistema, funcionaba todo correctamente, ahora el problema era que se había hecho una copia de seguridad a archivos encriptados, por eso tenían una extensión aleatoria y eran desconocidos para Windows.

Nombre	Fecha de modifica...	Tipo	Tamaño
CARATULA COTIZACION.DOCX.jagsxta	01/09/2014 9:11	Archivo JAGSXTA	12 KB
CARATULA SUBASTA INVERSA.DOCX.jagsxta	21/03/2014 9:42	Archivo JAGSXTA	12 KB
CEDULA JOSELIM.DOCX.iczatqb	08/12/2014 14:49	Archivo ICZATQB	2.128 KB
COBRO DE LEVANTAMIENTO DE TEXTO 2013.XLSX.jagsxta	18/06/2014 14:03	Archivo JAGSXTA	34 KB
Copia de CONTROL GENERAL (Recuperado).XLS.jagsxta	06/01/2015 14:52	Archivo JAGSXTA	700 KB
COSTO LEVANTAMIENTO DE TEXTO 2012.XLSX.jagsxta	16/06/2014 12:02	Archivo JAGSXTA	37 KB
COSTO LEVANTAMIENTO DE TEXTO PROVEEDORES.XLSX.jagsxta	11/06/2014 16:08	Archivo JAGSXTA	24 KB
DESCARGO EQUIPO INFORMatico.DOCX.jagsxta	22/12/2014 12:27	Archivo JAGSXTA	13 KB
Ficha_Confidencial_2014_new.XLSX.jagsxta	07/07/2014 14:40	Archivo JAGSXTA	66 KB
FIRMAS ESCANEADAS.DOCX.iczatqb	23/10/2014 11:59	Archivo ICZATQB	1.804 KB
Formato de car+itula de caja (cart+In).XLSX.jagsxta	12/12/2014 13:36	Archivo JAGSXTA	13 KB
FRIMA COMISION TECNICA.DOCX.iczatqb	25/09/2014 9:42	Archivo ICZATQB	109 KB
LEVANT TEXTO 2014.XLSX.jagsxta	17/06/2014 9:57	Archivo JAGSXTA	22 KB
OFICIO 2015.DOCX.jagsxta	06/01/2015 15:09	Archivo JAGSXTA	20 KB

Figura 3. Captura de los documentos encriptados por CTB Locker.

Fuente: Elaboración propia.

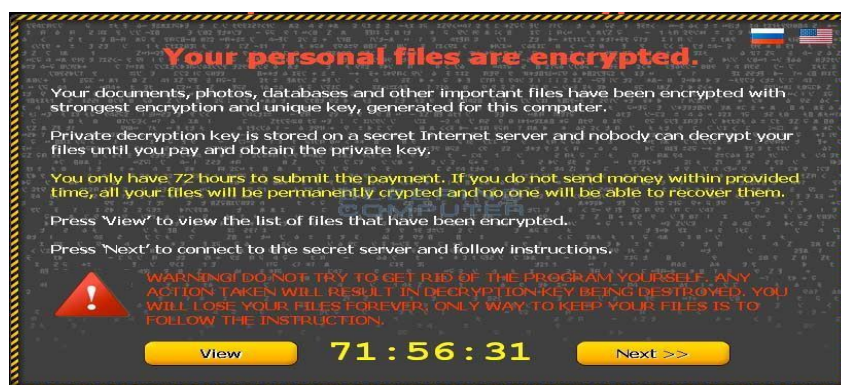


Figura 4. Captura de la ventana emergente de CTB Locker, llamado también Critroni.

Fuente: Elaboración propia.

Cuando se investigó el CTB Locker, entonces se supo que se trataba de un ransomware que había empezado a difundirse el mes de julio del 2014, que realizaba un ataque más sofisticado que lo que hacían los virus normalmente, pero ahora ya no había esperanza de recuperar la información ya que el virus había sido eliminado; el error fue haber formateado el equipo, ¿por qué?, porque después de investigar sobre el asunto, es un malware relativamente sencillo de eliminar con una herramienta antimalware o algún antivirus, entre ellos podemos mencionar: Hitman Pro, SpyHunter, y muchos más; la solución hubiera sido más sencilla, ya que si se eliminaba el ransomware con un antivirus, se podía utilizar una herramienta llamada *Shadow Explorer* con la cual se podían restaurar los archivos a una fecha anterior, pero eso no funcionó porque se formateó el sistema, debió haberse realizado antes de formatear para poder recuperar la información, aunque los ficheros se restaurarían a una versión anterior.

Este caso en realidad no se resolvió, puesto que no se pudo descryptar los archivos (aunque quedaron guardados), ya han pasado dos años y ya han creado herramientas para descifrar esos archivos. La empresa de antivirus *Kaspersky* y otras empresas similares han creado aplicaciones para descifrar archivos de algunos de los ransomware más conocidos, así que, en cualquier momento es posible recuperar información que se haya perdido a causa de estas infecciones; este como otros antecedentes, enriquecen el conocimiento y la experiencia en este tipo de situaciones que son muy comunes en las TIC.

¿Son frecuentes los ataques con software malicioso en las empresas?

La creación de programas maliciosos aumenta exponencialmente, esto representa una amenaza constante a las empresas, ya que éstas son el blanco prioritario de los cibercriminales, la evolución del malware en los últimos años ha sido abrumadora.

Los expertos de *G DATA Security Labs* descubrieron 1.84 millones de nuevas amenazas informáticas en la primera mitad de 2014, lo que significa que el cibercrimen alumbró un nuevo malware para entornos Windows cada 8.6 segundos, es decir, más de 10,200 nuevos tipos de programas maliciosos cada día. (Computerworld, 2014, p. 26)

Por otra parte, el software mal intencionado no tiene sentido sino utiliza medios de propagación y maneras para introducirse en los dispositivos para comprometer la información de los usuarios y sacar provecho; y una parte de esas infecciones se producen en Ecuador.

Al día hay 10.5 millones de ataques cibernéticos en el mundo, el 1.8% es en Ecuador; cada 34 segundos un malware desconocido es descargado, cada 5 minutos una aplicación de alto riesgo es utilizada. A nivel regional, Ecuador es el segundo país más atacado por cibercriminales. (CHECKPOINT, 2015, p. 59)

Hay que tener presente los códigos maliciosos como botnets, bitcoinsminers y ransomware, los nuevos códigos se enfocan en generar una ganancia económica para los atacantes, en lugar de realizar un daño como hacían los antiguos virus. Los objetivos principales de estas amenazas son:

robo de información para obtener dinero vendiéndola a la competencia, secuestro de los datos para pedir una compensación económica como rescate y uso de ataques DOS (denegación de servicios) para detener la producción de una empresa. (Pérez, 2016).

¿Qué se necesita saber sobre un ransomware?

Para entender con mayor precisión la naturaleza, la propagación y la amenaza que representa un ataque ransomware, es necesario analizar un poco que tan frecuente se producen este tipo de ataques, dónde y cómo se realizan. Cuáles son los medios más comunes que utiliza para introducir su código malicioso en un dispositivo, en que plataformas se ejecutan, y qué se pronostica sobre ellos para los siguientes años.

De acuerdo con el gobierno de los Estados Unidos, unos 4,000 ataques ransomware se llevan a cabo todos los días, un aumento del 300% desde el año pasado, y el número sigue en aumento. Esto se debe a que el ransomware se ha convertido en unos de los negocios más rentables para los cibercriminales. (Acronis, 2016)

Para este análisis vamos a ver cómo evolucionan las detecciones de diferentes familias de ransomware durante los primeros seis meses del año 2016.

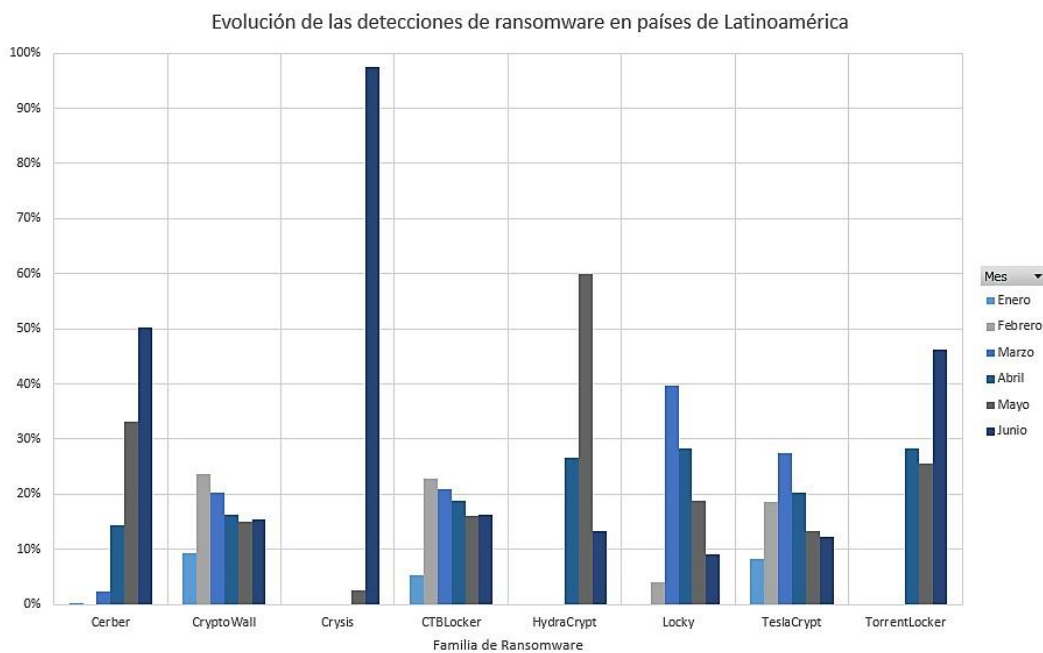


Figura 5: Cuadro estadístico de las infecciones producidas por la familia ransomware, desde enero a junio de 2016, en los países de Latinoamérica.

Fuente: (Amaya, 2016).

Los cibercriminales se enfocan en propagar sus amenazas en donde se encuentra la mayor cantidad de usuarios potenciales, es decir, las grandes empresas en los países con la mayor cantidad de manejo y producción de información, ya que los ataques en estas empresas son más rentables para ellos:

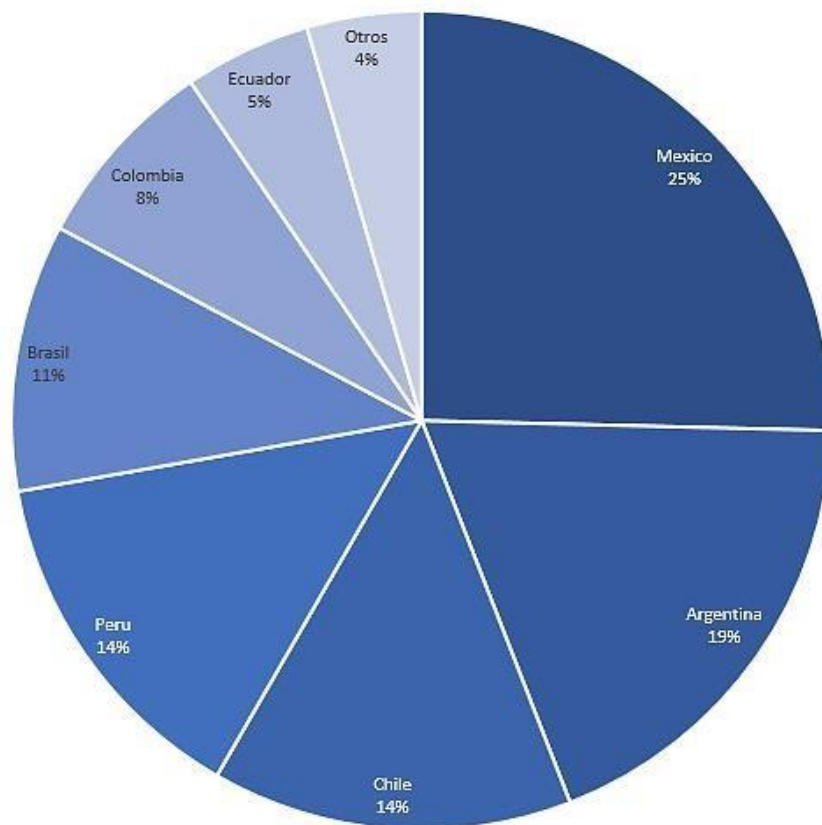


Figura 6. Gráfica de los países más atacados con ransomware.

Fuente: (Amaya, 2016).

A pesar que los ataques ransomware evolucionan con el tiempo, los medios de propagación básicamente siguen siendo los mismos:

Dispositivos USB, correos electrónicos, puertas de acceso; es decir, vulnerabilidades en el sistema lo que permite la introducción de malware. También se debe considerar la nube o “Cloud” como medio de propagación, ya que de esta manera la infección se produce de manera más rápida por toda la red.

El código malicioso ransomware en la actualidad no solo infecta a ordenadores con Windows también ataca a MAC OS el sistema operativo de Apple y se han visto algunos casos en Linux, pero no con tanto éxito como en los dos anteriores, eso con respecto a computadores, pero si hablamos de dispositivos tecnológicos en general, ransomware ha también migrado a otras plataformas, por ejemplo: los dispositivos móviles han sido también blanco; después de haber causado pérdidas financieras en un gran número de empresas en el mundo, ahora ataca a la plataforma Android.

Existen dos tipos generales de malware que entran en la categoría de ransomware para Android: el ransomware de bloqueo de pantalla, y el criptográfico. En el de bloqueo de pantalla, el recurso

secuestrado es el acceso al sistema comprometido, en cambio, en el criptográfico el recurso secuestrado son los archivos del usuario. (LIPOVSKY, 2016).

Pero también el ransomware está afectando ahora a los automóviles, por medio del software denominado *jackware*.

Defino como *jackware* al software malicioso que intenta tomar el control de un dispositivo cuyo objetivo principal no es el procesamiento de datos ni la comunicación digital. Un automóvil, por ejemplo, sería uno de estos dispositivos. (COBB, 2016)

Existen cada vez nuevas variantes de ransomware que pueden tener efectos más severos, es el caso del nuevo malware de esta familia que se denomina *Jigsaw* que muestra una imagen de la marioneta *Billy*, que es una identidad de la serie de películas de terror *Saw*.

Además de este recurso gráfico, la verdadera amenaza de esta variante de ransomware reside en que cada hora se van eliminando algunos de los ficheros cifrados. Esto hace que el tiempo sea un factor fundamental si se quieren recuperar los archivos. De hecho, si se intenta detener el proceso o reiniciar el sistema, *Jigsaw* eliminará 1000 ficheros, por lo que limita las acciones que puede realizar el usuario para tratar de recuperar su información sin pagar el rescate. (Albors, 2016)

En realidad, *Jigsaw* es solo un ejemplo de la gran cantidad de variantes que se producen en la familia ransomware, lo que da lugar a que estos ataques sean cada vez más agresivos y sus planes de extorsión puedan tener éxito. Aun así, existen herramientas de descifrado de archivos por ransomware, que han sido creadas por empresas de la seguridad informática, generalmente son gratuitas, que pueden permitir recuperar la información que fue encriptada, aunque cada vez existen esas variantes mencionadas que incluyen nuevas características que complejizan el proceso de restitución de los datos.

Las infecciones de ransomware siguen creciendo y sus efectos en constante evolución, lo que sugiere que las empresas y usuarios que crean y procesan información importante, tengan el conocimiento y la experiencia requerida para evitar este tipo de ataques. Las detecciones de ransomware en ESET Live Grid, sistema que reúne información de amenazas detectadas en equipos de usuarios ESET alrededor del mundo, muestran una tendencia creciente desde el último trimestre del 2015 y el primero del 2016:

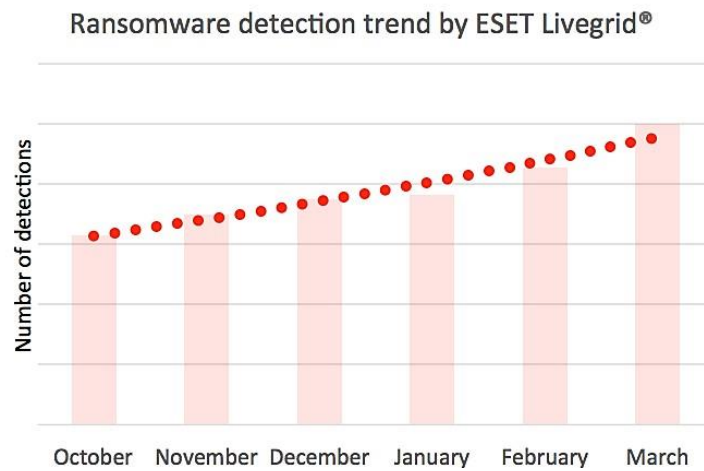


Figura 7. Crecimiento de las infecciones detectadas por ESET.

Fuente: (Pagnotta, 2016).

3. CONCLUSIONES

El caso de Onsystem tuvo una solución afortunada debido a las copias de seguridad efectuadas en Dropbox y a una acción torpe del ransomware ya que bloqueó los puertos lógicos, impidiendo que se actualizara en la nube los archivos infectados. Ahora bien, en cualquier otra situación de infección con ransomware no es recomendable de ninguna manera “pagar” por el “rescate”, ya que no hay garantías de que será restituido en su totalidad el acceso a la información comprometida; además, pueden quedar vestigios del malware que darán lugar a manifestaciones futuras con fines iguales.

Por medio de este estudio se ha concluido que los casos de infección con software mal intencionado, en particular: el ransomware, son una realidad en el mundo de la informática y es necesario tomar medidas preventivas y correctivas para hacer frente a este tipo de ataques. Si se trata de un usuario convencional, el riesgo disminuye considerablemente, pero si es una empresa de producción masiva de información importante, la unidad de TIC tiene la ardua tarea de aislar los eventos y actividades que puedan dar lugar a que se produzca una infección de ransomware.

Por medio de esta experiencia, Onsystem está tomando las medidas requeridas para evitar y corregir este tipo de casos en sus clientes, por eso, está ahora desarrollando una herramienta (software) que va a permitir realizar copias de seguridad de las bases de datos del sistema ERP, por separado, automáticamente, todos los días, por versiones, que se almacenarán en una carpeta que luego se subirán a un servidor FTP (Protocolo de Transferencia de Ficheros) en otro equipo y en otra ubicación geográfica. Si bien este es un tema de constante investigación y evolución, este trabajo será el acicate que va a permitir considerar la seguridad de los datos como realmente importante en la productividad de una empresa o usuario que hace un uso notable de la información.

4. REFERENCIAS BIBLIOGRÁFICAS

- Acronis. (2016). *Ransomware va viral*. Recuperado de: <http://www.computerworld.com/article/3123041/backup-recovery/ransomware-goes-viral-what-you-need-to-know.html/>.
- Albors, J. (2016). *Wlive Security*. Obtenido de Jigsaw y cómo el ransomware se vuelve más agresivo con nuevas capacidades: Recuperado de: <http://www.wlivesecurity.com/la-es/2016/04/15/jigsaw-ransomware-mas-agresivo-nuevas-capacidades/>.
- Amaya, C. G. (2016). *Nuevas variantes de ransomware en evolución constante*. Recuperado de: <http://www.wlivesecurity.com/la-es/2016/07/08/variantes-de-ransomware-evolucion/>.
- Checkpoint. (2015). *Security Everywhere, una estrategia en la ciberguerra*. *Computerworld EC*, 59.
- COBB, S. (2016). *Wlive Security*. Obtenido de Jackware: cuando los autos conectados conocen al ransomware: Recuperado de: <http://www.wlivesecurity.com/la-es/2016/07/21/jackware-autos-conectados-ransomware/>.
- Computerworld. (2014). *8 Segundos malware en Windows*. *Computerworld EC*, 26.
- Lipovski, R. (2016). *Wlive Security*. Obtenido de El auge del ransomware para Android: criptográfico y de bloqueo de pantalla: <http://www.wlivesecurity.com/la-es/2016/02/18/auge-ransomware-para-android/>.
- Pagnotta, A. (2016). *Wlive Security*. Obtenido de Tu seguridad depende de ti: aprende a evitar el ransomware: <http://www.wlivesecurity.com/la-es/2016/05/02/tu-seguridad-evitar-el-ransomware/>.
- Pérez, I. (2016). *El malware empresarial crece en el mundo*. Obtenido de Computerworld: <http://computerworld.com.ec/actualidad/tendencias/30-el-malware-empresarial-crece-en-el-mundo.html/>.