No. 28 / abril - mayo 2017

.Seguridad®

Cultura de prevención para TI

28

Buenas prácticas de seguridad

Desarrollo de una cultura de prevención

Tendencias de seguridad para 2017 | Recomendaciones en el uso de la tecnología | Consejos prácticas al comprar en línea | Sanitización de información | Cowrie Honeypot | Recomendaciones para liberar tu página web

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

.Seguridad
Cultura de prevención para TI

Buenas prácticas de seguridad

Desarrollo de una cultura de prevención

El avance de la tecnología, así como la gama de dispositivos que se ofrecen en el mercado, han facilitado que las personas accedan a su información en cualquier lugar y momento.

La Asociación de Internet.MX en su Estudio sobre los Hábitos de los Usuarios de Internet en México 2016 revela que 77% de las personas se conectaron a través de un teléfono inteligente y 23% a través de aparatos electrónicos (tendencia relacionada con el aumento de los dispositivos del Internet de las Cosas). La mayor parte de las actividades realizadas se relacionan con el ocio y el trabajo, pero la Asociación proyecta que actividades como la banca, la realización de trámites gubernamentales y las compras en línea aumentarán en México.

Lo anterior se vuelve un atractivo para los cibercriminales. Las recientes amenazas se están enfocando a tomar control de los dispositivos o recurrir a la ingeniería social para obtener datos de los usuarios; estos últimos se vuelven una puerta de acceso a los círculos sociales, familiares, de trabajo y estudio.

Nuestra vida digital no está desligada de nuestra vida diaria. Por ello es importante conocer los riesgos y las amenazas a las que estamos expuestos, llevar a cabo buenas prácticas de seguridad y saber qué hacer en caso de que se vea comprometida nuestra información personal.

En este número hacemos hincapié en la prevención: abordamos las amenazas que se cree tendrán una mayor presencia en 2017; proporcionamos buenas prácticas de seguridad para comprar en línea, supervisar la navegación de los menores de edad y para sanitizar los datos de nuestros dispositivos; damos sugerencias para realizar un proyecto de sitio web seguro y presentamos el honeypot Cowrie para registrar ataques de fuerza bruta.

El conocimiento es tu mejor defensa.

Katia Rodríguez Rodríguez
Editora
Coordinación de Seguridad de la Información

.Seguridad Cultura de prevención para TI, revista bimestral, abril-mayo 2017 / Certificado de Reserva (en trámite), Certificado de Licitud de Título (en trámite), Certificado de Licitud de Contenido (en trámite), Número ISSN (en trámite), Registro de Marca 1298292 | 1298293 / Universidad Nacional Autónoma de México, Circuito Exterior s/n edificio de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación, Coordinación de Seguridad de la Información, Cd. Universitaria, Coyoacán Ciudad de México, México, C.P. 04510, Teléfono: 56228169

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

DIRECTOR GENERAL
Dr. Felipe Bracho Carpizo

DIRECTOR DE SISTEMAS Y SERVICIOS INSTITUCIONALES
Act. José Fabián Romo Zamudio

COORDINADOR DE SEGURIDAD DE LA INFORMACIÓN/ UNAM-CERT
M. en C. José Roberto Sánchez Soledad

DIRECTORA EDITORIAL
L.A. Célica Martínez Aponte

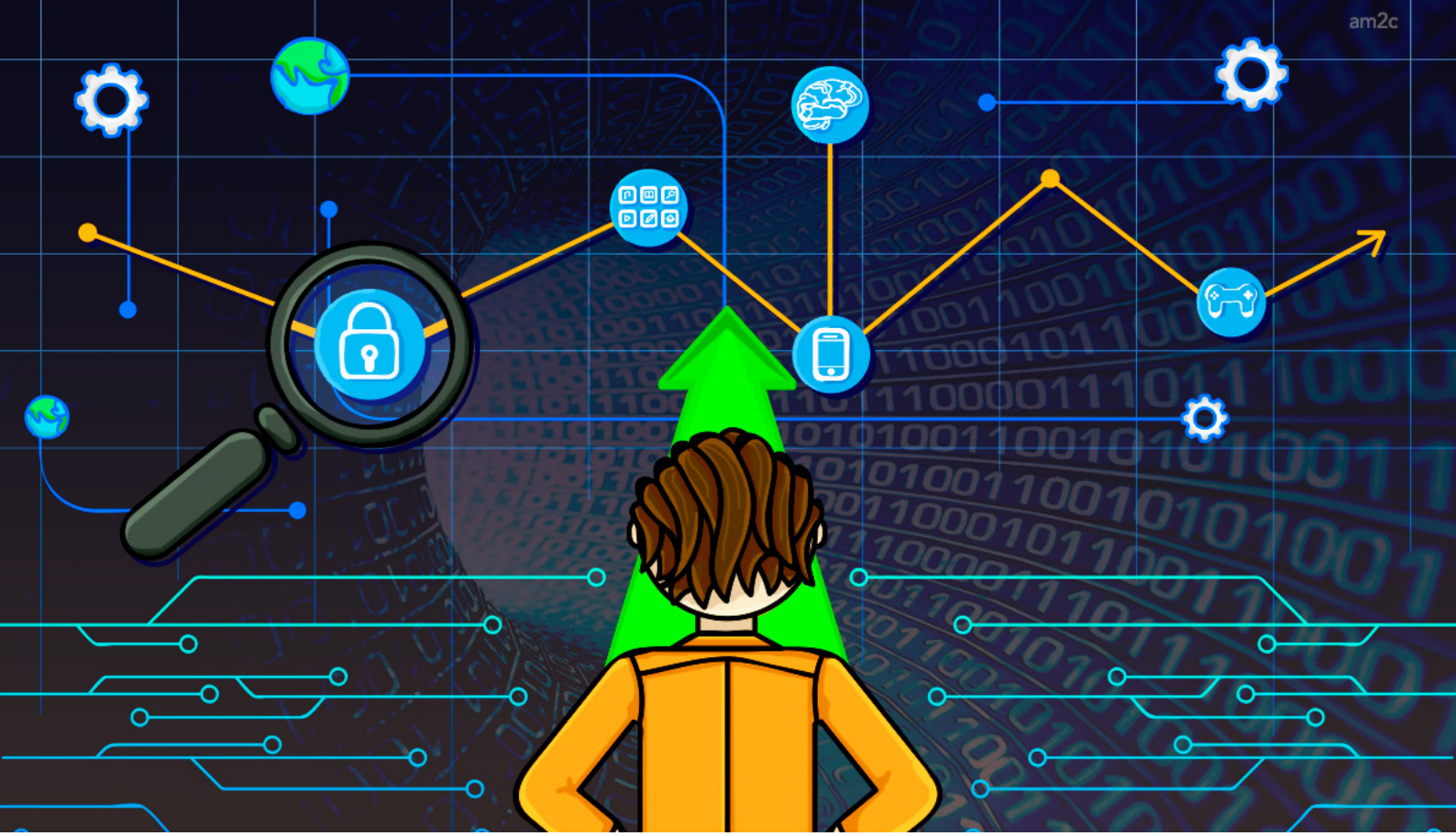
EDICIÓN REALIZADA POR
Katia Rodríguez Rodríguez

ASISTENTES EDITORIALES
Raúl Abraham González Ponce
Abigail Anayeli Vergara Varas

ARTE Y DISEÑO
L.D.C.V. Alicia M. Manjarrez Ceron

REVISIÓN DE CONTENIDO
Angie Aguilar Domínguez
Demian Roberto García Velázquez
Manuel Ignacio Quintero Martínez
Juan López Morales
Célica Martínez Aponte
Javier Ulises Santillán Arenas

COLABORADORES EN ESTE NÚMERO
Israel Andrade Canales
Jesús Mauricio Andrade Guzmán
Camilo Gutiérrez Amaya
Héctor Jesús Pérez Mancilla
Edgar Ríos Clemente
Sergio Anduin Tovar Balderas



Tendencias de seguridad para 2017, ¿estás preparado?

Camilo Gutiérrez Amaya

Desde 2009 el equipo de investigación de ESET realiza el Informe de Tendencias a partir de la revisión de los acontecimientos recientes más importantes en materia de seguridad informática. En 2017 se elaboró un documento con nueve tendencias que abarcan diversos temas como el *Ransomware* de las Cosas, las infraestructuras críticas, las vulnerabilidades, entre otras. En este artículo se resaltarán dos de ellas: la seguridad en dispositivos móviles y las amenazas en plataformas de videojuegos.

En cuanto a los dispositivos móviles, es necesario pensar en los diferentes aspectos de seguridad que deben tener implementadas las plataformas, como el modelo de distribución de aplicaciones, la creciente cantidad de *malware* móvil o el desarrollo seguro en el contexto de incorporación de otras tecnologías, como la realidad aumentada y la realidad virtual a estos dispositivos.

Por otra parte, la industria de los videojuegos ha adquirido cada vez mayor relevancia, con una amplia variedad de usuarios con equipos de gran capacidad de procesamiento a su disposición, convirtiéndolos en un objetivo muy atractivo para los cibercriminales. Si a lo anterior sumamos la tendencia a la integración de consolas con el entorno de equipos de escritorio, se pone de manifiesto la necesidad de hablar sobre seguridad con este público, ya que supone nuevos vectores de ataque.

Por lo tanto, la seguridad debe comenzar a ser considerada en los nuevos desarrollos tecnológicos que día con día se incorporan

a nuestras actividades cotidianas, lo que se traduce en la aplicación de medidas de protección en distintos niveles y en diferentes ámbitos.

Mobile: el *malware* y su realidad... ¿aumentada?

En un principio se esperaba que los dispositivos móviles evolucionaran hasta convertirse en computadoras de bolsillo tan capaces como cualquier equipo de escritorio. Es claro que hoy nuestros teléfonos y tabletas inteligentes han trascendido este propósito, generando nuevas maneras de interacción tecnológica antes impensadas. En el contexto de la revolución socio-tecnológica, los nuevos desarrollos incorporan nuevos riesgos de seguridad que afectan la información digital e incluso al bienestar de los usuarios.

En la actualidad, el *malware* móvil va en aumento y cada vez es más complejo. Ante esta situación, en el desarrollo de software debe implementarse medidas de seguridad desde etapas tempranas y no como hoy en día, que se aplaza hasta etapas tardías del proyecto, en el mejor de los casos, o bien cuando se encuentran en producción. Dejando de lado las aplicaciones que deben cumplir estándares de seguridad, pocos desarrolladores se preocupan por realizar exhaustivos controles sobre sus productos antes de liberarlos al público.

En conjunto con el desarrollo seguro de aplicaciones, las bibliotecas de anuncios publicitarios también tendrán un rol importante en la seguridad, ya que son utilizadas por los desarrolladores en plataformas como una forma de ingresos, donde los usuarios no suelen estar dispuestos a pagar por conseguir la funcionalidad de las aplicaciones. Usualmente encontramos al menos una de ellas por aplicación y muchas veces contienen algún tipo de API insegura que podría ser explotada para la instalación de *malware* o el robo de información.

Adicionalmente, a estos errores involuntarios en el proceso de desarrollo también se suman aquellas creaciones maliciosas cuya propagación en ocasiones es favorecida por las políticas poco restrictivas en repositorios de aplicaciones, que encubren involuntariamente a los cibercriminales bajo la fiabilidad de las tiendas de aplicaciones oficiales. Ante la gran cantidad de potenciales víctimas, los mercados oficiales de aplicaciones sucumben frente a las nuevas campañas de códigos maliciosos que se cuelan en sus repositorios, disponibles para ser descargada por los usuarios.

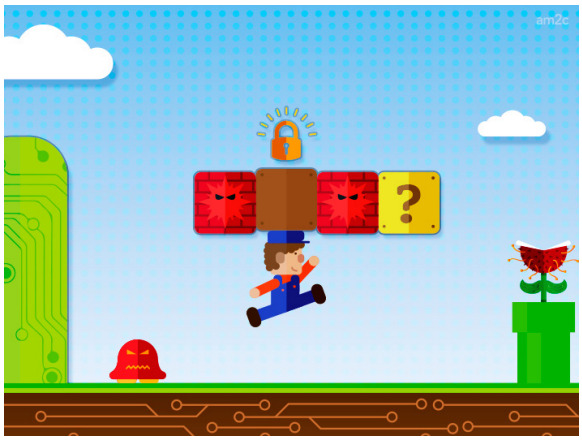
En suma, el crecimiento del *malware* móvil es una realidad innegable que veníamos previendo desde hace algunos años y actualmente se consolida ante nuestros ojos. Durante 2015, la cantidad de nuevas variantes de códigos maliciosos creados para Android promediaba las 200 variantes mensuales; en 2016 este número ascendió a 300 nuevas variantes mensuales (en iOS el número es de dos mensuales), por lo que no debería sorprendernos que este incremento continúe durante los próximos meses y años.

Además del aumento en la cantidad de nuevas variantes de códigos maliciosos, una gran preocupación para los usuarios móviles serán las vulnerabilidades no solo del sistema operativo sino también de las aplicaciones que utilizan. La reciente liberación de iOS 10 y Android 7.0 Nougat plantea algunas mejoras en el estado de la seguridad móvil, especialmente para este último sistema.

Por parte de Google comienzan a vislumbrarse esfuerzos por unificar aspectos de seguridad a través de los distintos modelos de teléfonos y tabletas disponibles en el mercado. Además, la firma continuará depositando esperanzas en su continuo programa de recompensa por errores como un medio para el descubrimiento de vulnerabilidades. Otra característica de Android 7.0 Nougat es que ha introducido diferentes mejoras en el manejo de permisos y aplicaciones que dificultarán la instalación de *malware* dentro del equipo y limitarán el control que estas aplicaciones posean.

En este contexto, a medida que los usuarios desconozcan el peligro de instalar aplicaciones desde fuentes no confiables, la falta de implementación de prácticas de seguridad en el desarrollo de ellas y que los cibercriminales apuesten a nuevas campañas de Ingeniería Social a través de mercados oficiales, durante este año podremos observar más casos de *malware* móvil, aplicaciones falsas y una tendencia creciente a encontrar estafas móviles a través de WhatsApp y las redes sociales. En general, se presentarán riesgos de seguridad en las plataformas móviles, que requerirán la atención de todas las partes involucradas.

Plataformas de juego: los riesgos potenciales de consolas integradas a computadoras



Los juegos emplean tecnologías de última generación compuestas por hardware y software avanzado para ofrecer la mejor experiencia de entretenimiento a los usuarios. Dado que una cantidad innumerable de personas en todo el mundo gasta recursos para jugar en diversas plataformas, ya sean consolas, PC o teléfonos móviles, sin duda, esto las convierte en objetivos sumamente valiosos para los atacantes que buscan obtener fama, beneficios económicos o simplemente por diversión. Por esta razón, la seguridad es un elemento clave para la industria de los videojuegos.

El modelo de negocio de esta industria ha evolucionado en los últimos años. En el pasado, los juegos generaban ingresos principalmente por la venta de software empaquetado, en los cuales los usuarios pagaban una licencia por adelantado y tenían el derecho a jugar todo el tiempo que quisieran. Actualmente, los modelos involucran una mayor cantidad de transacciones monetarias, a través de la integración de consolas con computadoras y dispositivos móviles, lo que podría tener un impacto significativo para la seguridad de la información en los próximos años.

A medida que el modelo de negocio va evolucionando, también atrae nuevos tipos de amenazas. Los juegos online se ven ante la necesidad de hacer frente a las amenazas comunes del mundo cibernético, como el *malware* oculto en los programas de instalación, que incluyen troyanos en el software del juego, o las campañas maliciosas, que se hacen pasar por juegos populares para distribuir códigos maliciosos o robar las cuentas de los jugadores. Sin embargo, también hay otros tipos de conductas ilegales que se aprovechan de los juegos online.

Conforme los jugadores se sumergen en el juego, es común que el mundo virtual se mezcle con la realidad; los cibercriminales se aprovechan de esta transición entre los dos mundos y usan los juegos online para obtener beneficios, principalmente económicos. Esta posibilidad surge cuando se comercializan objetos virtuales en sitios de comercio electrónico, en los cuales los elementos del juego, que fueron robados de las cuentas de otros jugadores o comprados con dinero ilícito, se venden a cambio de dinero real.

Otra forma a través de la cual los delincuentes intentan obtener los datos de los usuarios es atacando directamente a los desarrolladores de juegos, quienes han sido víctimas de brechas de datos; esto ha derivado en incidentes como la pérdida financiera para la empresa y sus clientes, robo de tarjetas de crédito e información personal, entre otros. Además de los riesgos conocidos, se identifican otro tipo de amenazas que se relacionan con el uso popular de los videojuegos.

Tanto hogares como empresas (especialmente hoy en día con la tendencia a permitir los videojuegos en el lugar de trabajo como estrategia para aumentar la productividad) pueden quedar expuestos a las amenazas informáticas solo por habilitar el uso de juegos en sus redes. El simple hecho de tener una consola de juegos dentro de la oficina puede exponer a toda la empresa a ataques dirigidos, los cuales utilizan la plataforma de juego como puerta de entrada a la red corporativa.

Como se observa, existe un panorama amplio de amenazas que atentan contra los gamers, al igual que los dispositivos móviles, resulta necesario que las partes interesadas que van desde los desarrolladores de videojuegos y consolas hasta los jugadores continúen aplicando medidas de seguridad con el propósito de minimizar los riesgos asociados a esta forma de entretenimiento.

Seguridad en diferentes ámbitos y distintos niveles: hacia el desarrollo de la cultura de ciberseguridad

El impacto de la tecnología ha alcanzado a casi todos los aspectos de la sociedad y lo seguirá haciendo en los próximos años. Gran parte de las actividades actuales no se entenderían sin los sistemas de información, los dispositivos electrónicos o las redes de datos, lo que genera una tendencia que conduce hacia la hiperconectividad.

Al analizar el estado y la evolución de la tecnología hay un aspecto a resaltar: cada vez existen más dispositivos, más tecnologías y, por lo tanto, un mayor número de desafíos para mantener la seguridad de la información. Nuevas herramientas que facilitan la comunicación y diversas actividades, como los dispositivos móviles, o que ofrecen entretenimiento, como los videojuegos, se popularizan y evolucionan continuamente.

Sin embargo, de forma paralela aparecen nuevas amenazas y vulnerabilidades, determinantes para los riesgos que siguen aumentado en cantidad, frecuencia o impacto. Por lo tanto, la trascendencia de la tecnología para las sociedades actuales y los riesgos asociados a su uso, muestran la necesidad de proteger la información y otros bienes a distintos niveles y ámbitos.

Ya sea que hablemos de las infraestructuras críticas, el Internet de las Cosas, los dispositivos móviles o los videojuegos, la seguridad de la información adquiere mayor relevancia. Diferentes sectores son requeridos para la mejora y el aumento de la seguridad, desde la iniciativa privada con productos y servicios seguros, los gobiernos con normas y legislaciones, el sector académico con investigaciones y educación, hasta usuarios conscientes de la seguridad. Todo lo anterior para lograr un objetivo de mayor alcance: desarrollar y divulgar la cultura de ciberseguridad.

Si quieres saber más, consulta:

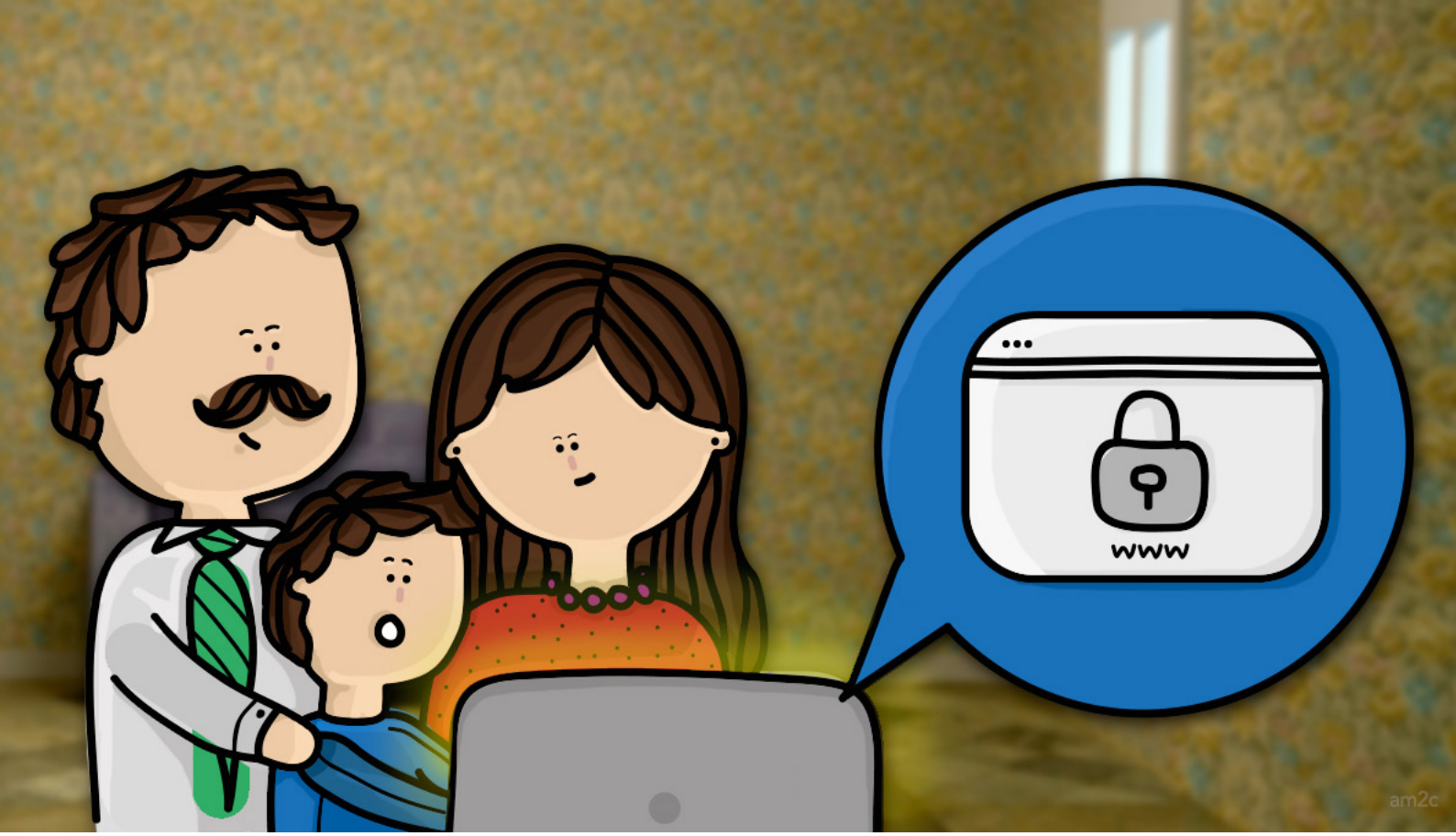
- Riesgos de seguridad en Android
- Información sensible en dispositivos móviles
- Dispositivos móviles: un riesgo de seguridad en las redes corporativas

Camilo Gutiérrez Amaya

Camilo Gutiérrez Amaya se desempeña actualmente como Head of Awareness & Research, liderando el equipo de investigadores de ESET Latinoamérica. Es Ingeniero Electrónico egresado de la Universidad de Antioquia e Ingeniero Administrador graduado de la Universidad Nacional de Colombia.

Cuenta con una especialización en Sistemas de la Información en la Universidad EAFIT y actualmente opta al título de Magister en Data Mining en la Universidad de Buenos Aires, Argentina.

Anteriormente se desempeñó como Coordinador de Riesgo Operativo para una importante compañía de financiamiento y se ha desarrollado modelando y generando sistemas de información.



Amenazas y recomendaciones para menores de edad en el uso de la tecnología

Héctor Jesús Pérez Mancilla

En la actualidad, vivimos en un mundo gobernado por la campaña mediática del consumo y la facilitación de las tecnologías de información. Cada día, en cualquier parte del mundo, las personas consumen diversos productos y servicios al hacer uso de nuevas tecnologías de información, sin que los usuarios se den cuenta de la gran cantidad de datos personales que son compartidos y muchas veces sin que estén conscientes de la forma en que permiten que estos sean difundidos. Los menores de edad están expuestos en este contexto.

En este artículo abarcaremos los delitos informáticos más utilizados por las diferentes organizaciones criminales y los más combatidos por las organizaciones gubernamentales y sociales.

Riesgos

Cada día es más frecuente la tendencia de regalar a los menores de edad dispositivos electrónicos sin ninguna concientización previa o sin alguna recomendación de uso, manejo y cuidado de la información personal.

Es de esperarse que la delincuencia organizada, como grupos enfocados en el sector de la pedofilia, la trata de personas o en la recolección de datos personales para campañas mediáticas, también estén enterados de este tipo de vulnerabilidades en prácticas inculcadas a los menores de edad:

- Entregar información a quien les pregunte
- Obedecer a los adultos
- No cuestionar a los adultos

- Los que son más atentos en sus respuestas, son mejor catalogados por los adultos
- Deben ser agradecidos y corresponder a los adultos por educación (*Rosas, Florentina, 2010*).

Estas vulnerabilidades son buenas costumbres que enseñan los padres o familiares a los menores y las organizaciones delictivas hacen uso de ellas, explotándolas y convirtiendo el riesgo en una amenaza latente contra los menores, porque hay una clara falta de concientización en cómo deben manejar estos la información que saben.

El Programa de Inclusión y Alfabetización Digital del gobierno federal mexicano es una gran campaña que otorga tabletas inteligentes a los niños para dar un acercamiento tecnológico a las diferentes escuelas en diferentes grados escolares. Sin embargo, el único problema que se debería contraatacar es la falta de implementación de un programa de concientización para los maestros, los padres de familia y los estudiantes a los cuales se les entregan estas tecnologías de la información, ya que corren el riesgo de revelar información y datos personales en un nivel de exposición peligrosa, que va desde conceder permisos excesivos a aplicaciones gratuitas o con costo.

Por ejemplo, existen casos bien documentados y muy conocidos (*Trend Micro, 2011*) de aplicaciones que solicitan acceso a muchas características cuando el único recurso al que deberían acceder en un dispositivo móvil como un smartphone o una tableta es a la linterna, pero se le asignan permisos excesivos tales como la localización, acceso a la cámara fotográfica y de video, a los contactos y a las modificaciones al sistema del dispositivo; el usuario, con la finalidad de utilizar la aplicación, accede a la concesión de los permisos sin una previa concientización. Cualquier persona, no necesariamente un niño, proporcionará los permisos con tal de obtener y utilizar la aplicación en ese momento.

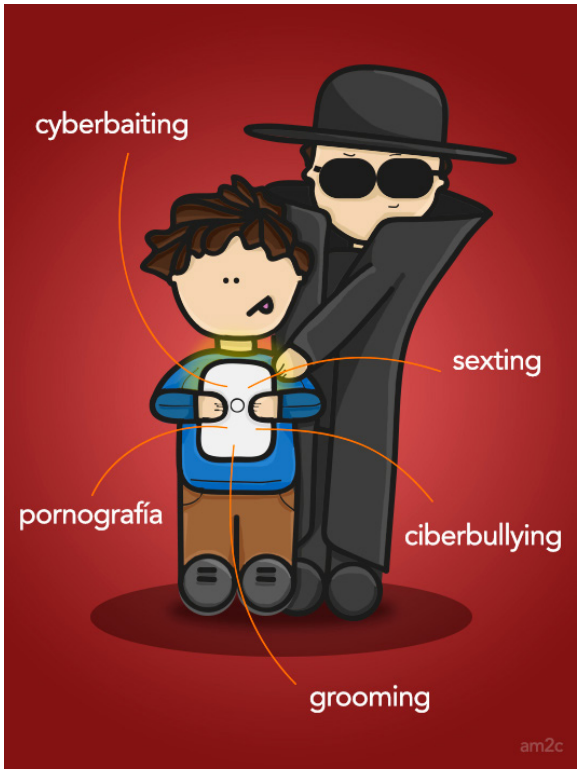
El otorgar tantos permisos a una aplicación podrá permitir el uso y difusión de la información del dispositivo electrónico, más allá de la toma de imágenes, en ocasiones en las que el usuario no esté utilizando la cámara fotográfica de su dispositivo. Una fotografía de un menor de edad desnudo en el mercado negro no puede valer más allá de un dólar americano y un video en la misma situación no valdrá más allá de cinco dólares americanos (*García, Colmenares, 2015*), pero la problemática a combatir es que las fotografías y los videos se convertirán en parte de bibliotecas con un amplio repertorio que diferentes organizaciones criminales comercializarán en todo el mundo, propagando los datos, las imágenes y los videos de los menores, pudiendo haber prevenido la captura de estos con una correcta concientización por parte de los padres, los maestros y los adultos.

Los delitos informáticos más utilizados por organizaciones criminales son:

- *Sexting*: es el uso de dispositivos móviles y computadoras para el intercambio de mensajes o contenido sexual. Este contenido debe considerarse inapropiado en el momento en que el canal de conversación es abordado por menores de edad y existe una revelación inadecuada de la información por parte de algún integrante del canal de conversación.
- *Ciberbullying*: acoso, amenazas y agresión son algunos de los componentes de este delito a través de Internet. Esta situación entre menores de edad semejante es más compleja por la impotencia que experimentan los jóvenes al no poder ejercer ninguna acción o tener miedo a lo que puedan realizar los padres de familia al conocer la situación.
- *Grooming*: es la acción de desnudar a menores de edad por medio de engaños y recopilar sus imágenes por una *webcam*. La mayoría de los atacantes que realizan este delito son adultos adoptando la falsa identidad de menores (utilizando el factor psicológico de confianza denominado "factor espejo"), ganando la confianza del menor simulando tener su edad, problemas y gustos similares. Ahora, con el uso de los dispositivos móviles se ha in-

crementado el *grooming* ya que, con la utilización de estos mismos, no existe la supervisión o vigilancia continua de los padres o un adulto responsable. En muchas ocasiones, ya no se requiere la interacción directa del atacante al poder establecer una interacción por medio de aplicaciones maliciosas, programadas para la recolección de imágenes.

- Pornografía: aunque en algunos países es un entretenimiento legal, siempre y cuando los participantes o actores sean considerados mayores de edad y las relaciones sexuales se lleven a cabo con consentimiento, la pornografía de menores de edad es muy recurrente y existe la distribución de este material sin autorización.
- *Ciberbaiting*: Esta práctica es una forma de *ciberbullying*, con la diferencia de que son los menores quienes acosan a sus maestros por medio de Internet. En estas prácticas se burlan de los docentes, los violentan verbalmente y humillan públicamente.



Contramedidas a los delitos informáticos

La prevención concreta al *sexting* es indicar a los menores de edad que la información que se proporciona por medio de dispositivos móviles, equipos de cómputo o a través de la distribución a pedimento de contenido es sensible y podría poner en riesgo su integridad o afectar su imagen.

Para el *ciberbullying* la forma de prevención es a través de la concientización sobre el uso correcto de los dispositivos móviles con los menores, así como el abordar a tiempo el acoso verbal y físico que es muy frecuente en los centros de estudio, evitando que el acoso se convierta en formas físicas de agresión.

El *grooming* es inversamente proporcional a la supervisión de padres de familia, por lo que se debe vigilar la instalación de aplicaciones en los dispositivos móviles de los menores y monitorear recurrentemente a los contactos en redes sociales.

Si deseamos evaluar si los menores están protegidos contra estos ataques o delitos o, aún mejor, si deseamos saber si nuestros hijos son o no generadores de estos delitos, debemos de poder contestar las siguientes preguntas:

- ¿Sabemos qué hacen nuestros hijos con sus dispositivos electrónicos?
- ¿Para qué los utilizan?
- ¿Qué usos les dan a las características de los dispositivos?
- ¿Sabemos el contenido de los dispositivos de nuestros hijos?
- ¿Sabemos qué redes sociales consultan?
- ¿Cómo obtuvieron el acceso a las redes sociales?
- ¿Quiénes son sus amigos o contactos en sus redes sociales?
- ¿Quiénes son sus contactos en su dispositivo móvil?
- ¿Cuidamos sus datos personales?
- ¿Qué información personal tienen autorizado entregar?
- ¿Han compartido imágenes o informa-

ción de ellos en forma que les dé pena contar?
- ¿Sabemos que no incurren en algún delito a través de sus dispositivos electrónicos?
- ¿Sabemos si son generadores de *ciberbaiting*, *sexting* y *ciberbullying*?

Conclusiones

Entre las recomendaciones que deben darse a los padres de familia, maestros y personas que interactúan de alguna forma con menores de edad o niños que hacen uso de dispositivos móviles se encuentran:

1. La responsabilidad de un dispositivo electrónico no termina con la entrega o regalo de uno, esta apenas comienza y debe darse un seguimiento constante de su uso correcto.
2. Enseñar al menor a utilizar el dispositivo correctamente e indicarle para qué fue diseñado, con el fin de evitar un mal uso del smartphone o tableta que conlleve al menor a un delito cibernético.
3. Concientizar al menor para que no proporcione información a personas desconocidas o que conoció en alguna red social.
4. Educar al menor de edad a no compartir imágenes o fotografías de sí mismos en ninguna red social. Enseñarles a que las personas pueden compartir fotografías de él o ella siempre y cuando no involucren imágenes deshonrosas o que lo hagan sentir en un estado incómodo.
5. Los padres pueden realizar una revisión periódica de los dispositivos electrónicos del menor de edad, como las computadoras, los teléfonos inteligentes y las tabletas, a las listas de contactos, a los accesos a redes sociales, el uso de la cámara fotográfica y la geolocalización del dispositivo en las aplicaciones y las fotografías tomadas.
6. Concientizar de forma constante sobre los delitos más comunes a los que están expuestos, cómo cuidarse de estos y cómo no generar los mismos.
7. Formar grupos integrados por padres de familia, maestros y autoridades en los cuales se puedan concientizar sobre los delitos a los que están expuestos los menores de edad.
8. Mantener un contacto constante con autoridades especializadas en temas de ciberdelincuencia enfocados a menores de edad, para que apoyen en el desarrollo correcto de un programa de vigilancia permanente a maestros y alumnos. Aunado a esto, seguir cualquier comunicado de fuentes confiables sobre amenazas y vulnerabilidades detectadas en dispositivos electrónicos y aplicaciones que nos afecten de forma directa.
9. Tener una comunicación clara, sincera y abierta entre padres, maestros y menores de edad para atender cualquier duda o interés.
10. El más importante es que la responsabilidad de la educación no es únicamente de los maestros y directivos escolares, conlleva un compromiso de todos los adultos involucrados en la sana convivencia en el medio del menor de edad. Ellos deben de atribuirse y asumir la responsabilidad y compromiso del buen uso de los dispositivos móviles y de cómputo a los cuales tenga acceso.

Referencias

García, J.C., Colmenares, L.E. (Abril-Junio 2015). Pornografía y explotación sexual infantil, efectos sociales y la tecnología. Pornography and child explotation. Revista Visión criminológica-criminalística. Año 2 número 10 Abril-Junio 2015. Recuperado de: http://revista.cleu.edu.mx/new/descargas/1503/Art%C3%ADculo2_pornograf%C3%ADa_infantil.pdf

Rosas, RF.; Florentina, R. (2010). Aspectos Generales y Jurídicos de la Pederastia. Recuperado de: http://repositaI.cuaed.unam.mx:8080/jspui/bitstream/123456789/880/1/Pederastia.pdf

Trend Micro. (2011). Cuando las aplicaciones de Android piden más de lo que necesitan. Recuperado de: http://www.trendmicro.es/media/br/ebook-when-android-apps-want-more-es.pdf

Si quieres saber más, consulta:

- Redes sociales en la escuela
- Reputación en línea
- Criminalística aplicada en la seguridad de tecnologías de información y comunicaciones

Héctor Jesús Pérez Mancilla

Ingeniero en Computación por parte del Instituto Politécnico Nacional, egresado de la Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán. Posee las certificaciones Certified Ethical Hacker, Certified Hacking Forensics Investigator, Certified Network Security y Certified System Administrator por pate del EC-Council; y las Certified Information Systems Auditor y COBIT por parte de ISACA.

Ha dirigido diversas gerencias de sistemas en el sector privado y dedicado en los últimos 10 años de experiencia en preservar la seguridad de la información en diferentes áreas desde formar parte de equipos de pruebas de penetración hasta dirigir equipos de cumplimiento de seguridad y auditoría de sistemas en roles como Oficial de Seguridad de la Información en diversas industrias desde la iniciativa privada y la banca en México.

Consejos prácticos de seguridad para proteger los datos bancarios al comprar en línea

Israel Andrade Canales

Uno de los atractivos más importantes de Internet es el comercio electrónico. En México, esta actividad aumentó su valor de mercado un 59% de 2014 a 2015, como lo demuestran estudios recientes sobre los hábitos de los usuarios de Internet en nuestro país (*AMIPCI, 2016*). Ya sea desde el celular o la PC, el internauta cuenta con una gran variedad de tiendas y métodos de pago, pero al mismo tiempo, de riesgos informáticos.

Lo anterior ha provocado que una de las resistencias más importantes al comercio electrónico esté relacionada con la seguridad informática (*AMIPCI, 2016; Pagnotta 2016*). Sin embargo, hoy el usuario tiene al alcance varios mecanismos que pueden ayudarle a tener más confianza en las tecnologías de comercio electrónico: desde buenas prácticas de seguridad hasta tecnologías que protegen sus datos bancarios.

En este artículo se presentan un conjunto de consejos, buenas prácticas y herramientas que reducen el riesgo de robo de información bancaria durante el pago de bienes y servicios en línea, y al mismo tiempo, se explica al usuario el porqué de dichos consejos.

Para lograr lo anterior, se describe de manera sencilla el proceso de compra en línea, y durante cada etapa se mencionan los principales riesgos de los datos bancarios y las mejores prácticas que puede emplear el usuario del comercio electrónico.

Protección de los datos bancarios

La información más importante durante la compra de productos y servicios por Internet son los datos que hacen posible el pago

en línea. En México, los métodos de pago más populares durante 2016 fueron Paypal y las tarjetas de crédito y débito (*AMIPCI, 2016*). Los datos bancarios de interés en estos tres métodos son (*Ali, Arief, Emms, & van Moorsel, 2016*):

- Las credenciales de acceso a las carteras digitales como Paypal.
- El número de tarjeta bancaria, el cual es una cifra única de 16 dígitos que vincula una tarjeta bancaria con el tarjetahabiente.
- El código verificador de tarjeta (CVV, por sus siglas en inglés), el cual es un número de tres dígitos impreso en el reverso de la tarjeta. Este dato se supone secreto y no debe ser almacenado por ningún sistema de compra en línea legítimo.
- La fecha de vencimiento de la tarjeta de crédito/débito.
- El código postal que registró el tarjetahabiente.

La información mencionada anteriormente es el objetivo principal que tiene un defraudador electrónico, el cual intentará obtenerla desde cualquier lugar donde se ingrese, almacene, procese y transfiera.

¿Cómo proteger los datos bancarios mientras están en tu computadora?

Al comprar productos o servicios por Internet requerimos varias tecnologías que se interconectan para realizar las mismas acciones que un cliente realizaría en una tienda física, esto es: solicitar el producto o servicio y realizar el pago.

De manera simplificada, para que un cliente indique a la tienda lo que desea comprar requerirá de un programa que será su interlocutor con la tienda: en los equipos de escritorio, el navegador web; y en los dispositivos móviles, la aplicación de la tienda.

Por lo anterior, el sistema operativo de tu dispositivo, el navegador web y las aplicaciones son herramientas clave para una compra menos riesgosa y su buen funcionamiento también es tu responsabilidad. Por ello:

1. **Nunca instales *software* pirata, de escasa reputación o de fuentes no confiables en los dispositivos donde realices las compras, ¡estos deben ser de tu absoluta confianza!** Tu navegador cuenta con mecanismos para identificar si los sitios que visitas son confiables y si modificas su configuración, podrías afectar esta protección.
2. Es muy importante actualizar el sistema operativo, tu navegador web y la aplicación de la tienda. De esta manera reparas las posibles debilidades de este *software*, además de agregarle nuevas funcionalidades que mejoren la experiencia de compra.

Adicionalmente, no debes realizar compras desde dispositivos en los cuales no tengas pleno control o que varios usuarios comparten. Existe *software* capaz de registrar lo que tecleas o envías por Internet. En este sentido:

3. No utilices computadoras de sitios como salas de Internet públicas o de renta. Del mismo modo, no te conectes desde redes públicas o compartidas, ya que la red informática debe ser de plena confianza. Esto ayudará a reducir los riesgos asociados a la intercepción de los datos bancarios sobre la red.

Finalmente, si almacenas tus datos bancarios en tu computadora o dispositivo móvil, asegúrate de lo siguiente:

4. Utiliza llaveros[1] que cifren tus datos bancarios y evita que estos se encuentren almacenados en texto claro. Si los datos bancarios están en tu dispositivo portátil, asegura que tu dispositivo cuente con mecanismos de autenticación. **Debes estar consciente del lugar donde tienes almacenados tus datos bancarios y asegurarte de reducir estos sitios al mínimo necesario.**

¿Cómo proteger tus datos bancarios cuando están en la tienda digital?

Hoy en día, la mayoría de los negocios apuestan al comercio electrónico (*López, 2016*) y por ello existe una gran variedad de tiendas en línea. No todas son confiables. Hay sitios creados intencionalmente para la obtención de los datos bancarios a través del engaño, y por tal motivo, la tienda donde realizas la compra debe tener una buena reputación; por lo anterior se recomienda hacer un poco de investigación sobre la tienda antes de comprar:

1. Verifica que la URL del comercio sea legítima. También revisa la fecha de creación del sitio web; prefiere aquellos que tengan algún tiempo considerable en el mercado.
2. Una tienda electrónica de buena reputación invertirá en su plataforma de venta, por lo tanto, si el sitio que visitas es de poca calidad, con contenido desactualizado o generado automáticamente, evítalo.

Sin embargo, lo anterior no es suficiente. Los ataques informáticos ocurren en casi cualquier tipo de servicio electrónico (correo electrónico, almacenamiento en la nube, comercio electrónico, entre otros). Empresas importantes como Yahoo! y Dropbox han sufrido ataques informáticos escandalosos (puedes consultar aquí algunos casos). Por tal motivo, no podemos confiar en que los datos que almacenan serán resguardados de manera segura.

3. Preferentemente, elige comercios que no almacenen los datos de tu tarjeta de crédito o débito (lo anterior puedes consultarlo en las políticas de privacidad del sitio), o bien, prefiere las tiendas que cuenten con sistemas de pago administrado por terceros de confianza (como el caso de Paypal y otras carteras virtuales[2]).

Otra opción interesante es contar con una tarjeta virtual, la cual es una tarjeta de crédito o débito ofrecida por algunos bancos, cuyo CVV u otro dato bancario, cambia en cada transacción, haciéndola temporal y de un solo uso (*Rubenking, 2014*). De esta manera, si la tienda es comprometida, tus datos bancarios no pueden ser aprovechados por cibercriminales.

En un reciente estudio realizado por un grupo de investigadores de la Universidad de Newcastle se analizó la seguridad de los métodos y redes de pago. Se descubrió que es muy factible realizar un ataque coordinado en diversas tiendas electrónicas **para deducir el CVV de un número de tarjeta a través de técnicas de prueba y error** (*Ali, Arief, Emms, & van Moorsel, 2016*). Por lo tanto:

4. Las herramientas más útiles en la realización del pago son las que reducen el tiempo de validación, como la funcionalidad que ofrecen algunos bancos para activar y desactivar temporalmente las tarjetas de crédito; así como los mecanismos para variar dinámicamente los datos bancarios por medio de tarjetas virtuales.

Conclusiones

De la misma manera que tomamos medidas de seguridad para comprar en una tienda física, es necesario hacerlo en línea. En este artículo se presentaron algunas recomendaciones que los usuarios pueden seguir al pagar productos o servicios por Internet. Estos consejos de seguridad van desde buenas prácticas en el uso de dispositivos electrónicos, hasta el manejo menos riesgoso de los datos bancarios durante el pago mediante tecnologías de seguridad bancaria.

La adopción de mejores prácticas durante la compra por Internet reducirá el riesgo de ser víctima de fraudes por esta vía, lo que favorecerá la confianza y el uso frecuente de las tecnologías de comercio electrónico.

Referencias

[1] Un llavero electrónico o gestor de contraseñas es un programa que almacena contraseñas u otros datos sensibles, los cuales protege con algoritmos criptográficos. Se recomienda la utilización de estas herramientas en lugar de almacenar los datos sensibles en archivos de texto plano. Algunos gestores de contraseñas populares son KeePass y LastPass, este último es un servicio ofrecido en línea y accesible desde dispositivos móviles.

[2] Las carteras virtuales son servicios electrónicos que concentran los datos de tarjetas de créditos o débito y realizan el cobro de productos o servicios evitando que los datos bancarios sean almacenados por tiendas en línea. Algunos ejemplos son Google Wallet, Apple Pay, Paypal, entre otros.

Ali, M. A., Arief, B., Emms, M., & van Moorsel, A. (2016). Ne?. IEEE Security & Privacy.

Asociación Mexicana de Internet (AMIPCI). (2016). Estudio AMIPCI de Comercio Electrónico en México 2016, Asociación Mexicana de Internet. Asociación de Internet. Recuperado de https://www.asociaciondeInternet.mx/es/estudios

López, J. (7 de abril de 2016). Sitios de e-commerce en México aumentan y abandonan tiendas físicas. El Economista. Recuperado de http://www.elfinanciero.com.mx/tech/aumentan-sitios-de-e-commerce-que-estan-dejando-el-mundo-offline.html

Pagnota, S. (28 de diciembre de 2016). El 41,3% cree que las compras online son "altamente peligrosas". WeLiveSecurity en Español. Recuperado de: http://www.welivesecurity.com/la-es/2016/12/28/compras-online-peligrosas/

Rubenking, N. (17 de septiembre de 2014). 5 Things You Should Know About Virtual Credit Cards. PC Magazine. Recuperado de: http://www.pcmag.com/article2/0,2817,2468612,00.asp

Si quieres saber más, consulta:

Algunos productos bancarios que ofrecen tarjetas virtuales son Pago móvil de Banorte, Bancomer Wallet de BBVA Bancomer y Entropay. Para mayor información se invita al lector a seguir los sitios electrónicos de dichos productos.

- https://www.banorte.com/cms/banorte/banortemovil/#!/pagomovil
- http://bancadigital.bancomer.com/wallet/
- https://www.entropay.com/

Israel Andrade Canales

Fue becario y colaborador del UNAM-CERT de 2009 a 2012. Estudió la carrera de Ingeniería en Computación en la FES Aragón y posteriormente la Maestría en Investigación de Operaciones en el Posgrado de Ingeniería. Ha trabajado como consultor y auditor de seguridad informática para gobierno e iniciativa privada. Actualmente se desempeña como Académico en la UNAM en dicha materia.

Sanitización de información

Edgar Ríos Clemente

La información es uno de los activos más importantes de las organizaciones. Durante su ciclo de vida debe ser protegida mediante diversos controles de acuerdo a su estado (en reposo, en tránsito o en uso). Una vez que finaliza su ciclo de vida, se debe contar con procesos de destrucción segura para que dicha información no pueda ser reutilizada con otros fines.

Uno de los pasos que hay que tomar en cuenta cuando un dispositivo o la información que contiene deja de ser útil, es realizar una eliminación de manera segura.

La sanitización de datos, de acuerdo con el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST, por sus siglas en inglés), se refiere a un proceso que no permite el acceso a los datos sobre los medios para un determinado nivel de esfuerzo, es decir, que los datos no se recuperen fácilmente.

Riesgos de no sanitizar los datos

Cuando la información no es eliminada de forma segura, la información importante puede remanecer, lo cual puede derivar en probables riesgos como:

- Datos privados o personales de los clientes o empleados pueden ser utilizados para cometer fraude o robo de identidad.
- Datos críticos pueden ser recuperados y usados por adversarios o competidores.

- Fuga de datos privados o personales que deriven en grandes multas y acciones legales para las organizaciones, por no cumplir con las leyes de protección de datos personales.
- La propiedad intelectual puede ser recuperada y publicada, derivando en pérdida de reputación y/o ganancias.

La **clasificación** contribuye en la valuación y protección de los activos de información; esto incluye también los procesos y procedimientos para reclasificarla, porque después de un periodo la información considerada como sensible puede declinar en valor o criticidad (de esta forma se evita que haya controles de protección excesivos). Por lo anterior, dentro de las políticas de clasificación de información, deberá también incluirse la reclasificación de información física y digital.

Por otra parte, en México el robo de identidad es un tema importante. Según datos del Banco de México, nuestro país ocupó en 2015 el octavo lugar a nivel mundial en este delito; debido a esto, como una medida de control, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) ha creado una guía completa para prevenir el robo de identidad, la cual se puede consultar en el siguiente enlace, que hace referencia a métodos para sanitizar la información.

Motivos para sanitizar

Algunas de las razones por las que se requiere sanitizar los medios de almacenamiento son:

- **Reutilizar:** Cuando se quiere reubicar el dispositivo a un usuario diferente o utilizarlo con otro propósito.
- **Revender:** Cuando se quiere revender el dispositivo y ya cuenta con nuestros datos personales, principalmente si son identificables.
- **Reparar:** Cuando se tiene que llevar a reparación, pero ya cuenta con información personal delicada.
- **Eliminar:** Al desechar o al donarlo, dar de baja el dispositivo.
- **Destruir:** Cuando se cuenta con información confidencial, la cual requiere que sean destruidos físicamente los dispositivos.
- **Regulatorio:** Por cumplimiento de regulaciones como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) o la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO).

Actualmente existen diversas organizaciones que cuentan con programas de donación o reciclaje de dispositivos electrónicos que incluyen celulares, computadoras portátiles, servidores, consolas de videojuegos y tabletas.

Empresas como Microsoft sugieren contactar a sus socios comerciales para apoyarse en la eliminación de información personal identificable; desafortunadamente, en México no se cuenta con *partners* que realicen este servicio de acuerdo con su sitio web pero, por otra parte, existen empresas nacionales que realizan esta labor.

En el país, los servicios más comunes que se ofrecen para la destrucción física de los documentos y los dispositivos físicos (discos magnéticos) son la desmagnetización, la trituración y la incineración.

Administrando los riesgos de medios de almacenamiento

Para contar con un mejor manejo de riesgos asociados con el almacenamiento de información sensitiva, el Centro Nacional de Ciberseguridad (NCSC, por sus siglas en inglés) del Reino Unido recomienda:

- Entender los datos y su valor potencial fuera de la organización.
- Comprender el costo de la sanitización de la información y añadirlo a los costos de adquisiciones para asignar un presupuesto.

- Contar con una política de reutilización y eliminación, con roles clave entendidos por todos en la organización.
- Conocer las tecnologías que se están empleando.
- Conservar los manuales de fabricantes para conocer cómo desechar y sanitizar.
- Establecer el ciclo de vida del medio de almacenamiento (qué se almacena, dónde y por cuánto tiempo).
- Usar terceros confiables que se apeguen a estándares internacionales.
- Obtener certificados de destrucción de los servicios de terceros (algunos proveedores adicionalmente proporcionan el video de la destrucción).
- Supervisar que los procesos de destrucción y equipo son probados periódicamente.
- Verificar que los datos son sanitizados apropiadamente.
- Remover las etiquetas o marcas indicando pertenencia del dispositivo o de los datos contenidos.
- Clasificar y etiquetar la información para que tenga el proceso adecuado y reducir posibles fugas o pérdidas.

Debido a estos escenarios, se requiere el uso de diferentes tecnologías y/o métodos para que se elimine la información de forma segura.

Estándares de sanitización y destrucción de datos

El Reino Unido cuenta con el estándar Her Majesty's Government (HMG) Infosec Standard 5 (IS5) para destrucción de datos; en Europa se tiene el estándar de destrucción de la información EN15713; en Alemania cuentan con el estándar DIN-66399; mientras que en los Estados Unidos de América se pueden seguir las guías de sanitización de medios del Instituto Nacional de Estándares y Tecnología NIST-800-88.

En México aún no contamos con una norma o estándar, pero una propuesta es la guía para el Borrado Seguro de Datos Personales desarrollada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), la cual es muy completa.

Actualmente, las organizaciones líderes de ciberseguridad, como el NIST, ya no cuentan con una lista de herramientas aprobadas, tal vez debido a la existencia de métodos más sofisticados para recuperación de información, al grado de que ya no es recomendable únicamente la sobreescritura en los discos magnéticos (aunque en la práctica es mejor siempre hacerlo). Sin embargo, el equipo de ciberseguridad de la Organización del Tratado del Atlántico Norte (OTAN) cuenta con un catálogo de productos para eliminación de discos magnéticos que puede ser de utilidad cuando se buscan opciones de eliminación más robustas.

Conclusiones

Los medios de almacenamiento evolucionan muy rápido, por lo cual habrá que identificar las nuevas tecnologías y los métodos de sanitización de datos más actuales para proteger los datos de las organizaciones.

Es importante mencionar que el contar con los procesos y el presupuesto para la sanitización de información ayudará a administrar diversos riesgos asociados a la falta de protección de información, sin olvidar que deben ir de la mano con las políticas de clasificación y retención de información. Por esta razón, se han mencionado en el artículo diversos estándares internacionales, así como las mejores prácticas nacionales. De esta forma, los encargados de proteger

la información pueden apoyarse en ellos para la generación de políticas, procesos y estándares que mejor se adapten a las necesidades de cada organización.

Es importante que al finalizar el ciclo de vida de la información, se aplique alguna (o varias) de las técnicas de sanitización de datos, de acuerdo con el tipo de información. De este modo se minimizará el riesgo de que dicha información sea reutilizada con otros fines.

Para organizaciones que requieran contratar servicios de destrucción de datos (incluyendo medios magnéticos e información física) en el país, una opción es elegir una empresa que pertenezca a una asociación internacional como la National Association for Information Destruction (NAID) de los Estados Unidos de América.

Referencias

Arch Linux. (13 de noviembre de 2016). Securely wipe disk. Arch Linux. Recuperado de: https://wiki.archlinux.org/index.php/Securely_wipe_disk

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (Junio de 2016). Guía para el Borrado Seguro de Datos Personales. Recuperado de: http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf

----------. (2016). Guía para Prevenir el Robo de Identidad. Recuperado de: http://inicio.inai.org.mx/nuevo/Guia%20Robo%20Identidad.pdf

Microsoft. (2017). How to more safely dispose of computers and other devices. Microsoft. Recuperado de: https://www.microsoft.com/en-us/safety/online-privacy/safely-dispose-computers-and-devices.aspx

National Cyber Security Centre. (24 de septiembre de 2016). Secure sanitisation of storage media. Guidance. Recuperado de: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media

National Institute of Standards and Technology. (Diciembre 2014). Guidelines for Media Sanitization. Recuperado de: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

North Atlantic Treaty Organization. (2014). Disk Erasure. Information Assurance Product Catalogue. Recuperado de: http://www.ia.nato.int/niapc/Category/Disk-Erasure_11

Rothke, B. (24 de febrero de 2009). Why Information Must Be Destroyed. CSO. Recuperado de: http://www.csoonline.com/article/2123705/privacy/why-information-must-be-destroyed.html

----------. (5 de mayo de 2009). Why Information Must Be Destroyed, Part Two . CSO. Recuperado de: http://www.csoonline.com/article/2123985/data-protection/why-information-must-be-destroyed--part-two.html

Wikipedia. (26 de marzo de 2017). Persistencia de datos. Wikipedia. Recuperado de: https://es.wikipedia.org/wiki/Persistencia_de_datos

----------. (19 de noviembre de 2016). Sanitización de datos. Wikipedia. Recuperado de: https://es.wikipedia.org/wiki/Sanitizaci%C3%B3n

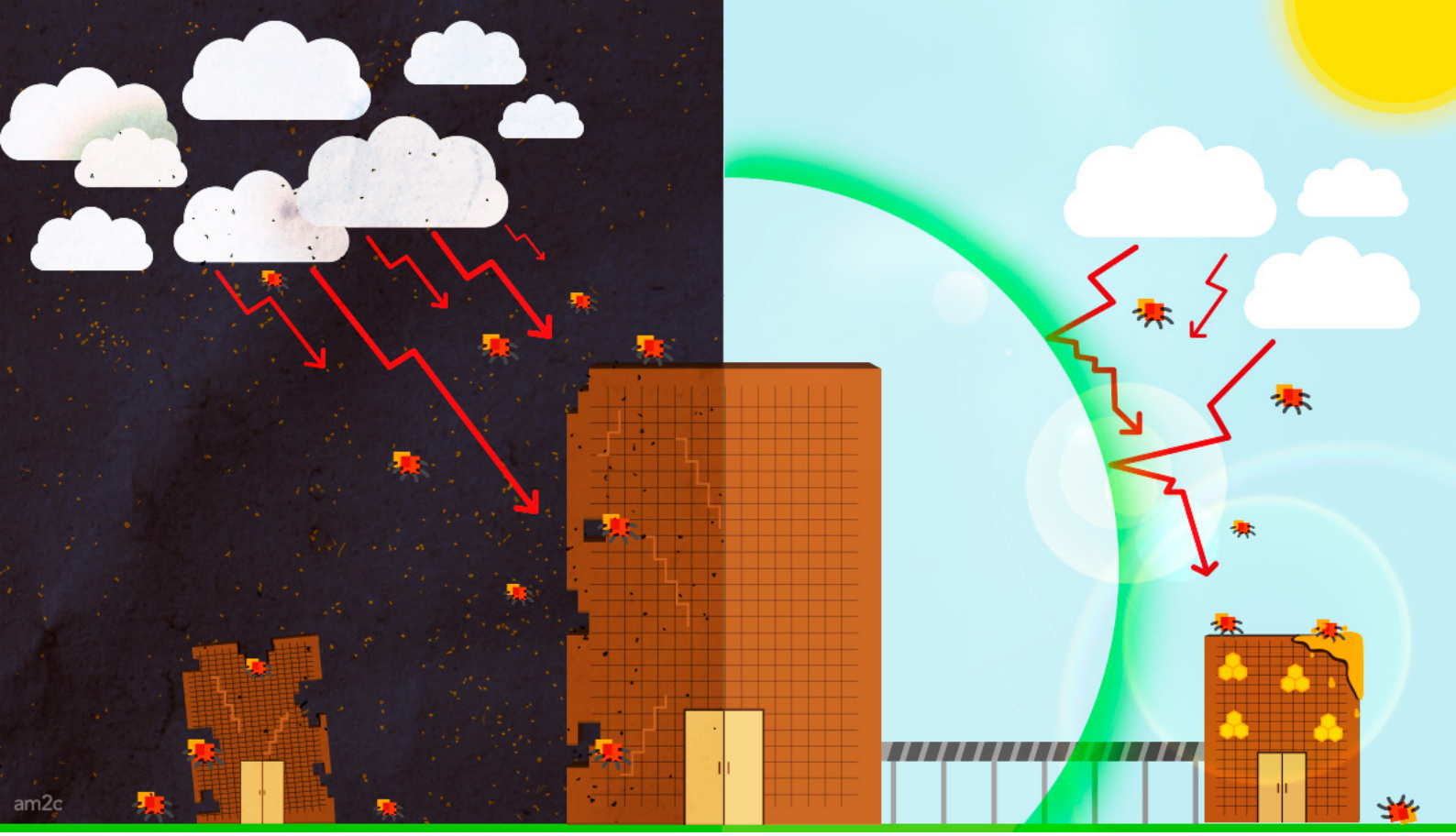
Si quieres saber más, consulta:

- Guía de sanitización segura de medios de almacenamiento del Centro Nacional de CiberSeguridad del Reino Unido (NCSC)
- Guía para el Borrado Seguro de Datos Personales del Instituto Nacional de

Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)
- Guía de destrucción de información EN15713:2009 de la british security industry association (BSIA)
- Directrices para sanitización de medios del Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América (NIST)

Edgar Ríos Clemente

Maestro en Ciencias en Cyber Security and Management de la Universidad de Warwick del Reino Unido. Es Ingeniero en Computación de la UNAM, ex becario de la segunda generación de seguridad Informática (CSI/UNAM-CERT) y ex becario del Consejo Nacional de Ciencia y Tecnología (CONACYT). Cuenta con más de 11 años de experiencia en Seguridad de la Información en los sectores de telecomunicaciones, financiero y público. Posee la certificación CISM.



Cowrie Honeypot: Ataques de fuerza bruta

Sergio Anduin Tovar Balderas

Los protocolos de SSH y Telnet son muy utilizados para la administración remota de diversos equipos de telecomunicaciones (como son un switch o un router), dispositivos de almacenamiento en red, puntos de acceso inalámbrico, entre otros. Los atacantes están aprovechando la falta de mecanismos de seguridad en estos dispositivos creando un nuevo vector de ataque para realizar Denegaciones de Servicio Distribuidas (DDoS) u otras actividades maliciosas.

Actualmente muchos dispositivos conectados a Internet utilizan los protocolos de Telnet y SSH, por lo tanto son susceptibles a ataques de fuerza bruta. Este artículo tiene como objetivo presentar la instalación, configuración y una prueba de concepto de Cowrie, un honeypot Telnet y SSH de interacción media, diseñado para registrar la interacción de la terminal y ataques de fuerza bruta realizados por los atacantes.

A través del tiempo se han desarrollado diferentes honeypots para el servicio de SSH como Kojoney de baja interacción que emula este servicio. Posteriormente, Upi Tamminen desarrolló Kippo inspirado en Kojoney, sin embargo, no está basado en su diseño o arquitectura.

Michel Oosterhof es el desarrollador de Cowrie y decidió renombrarlo como "Cowrie" para distinguirlo del honeypot original (Kippo), ya que él agregó características con las que Kippo no contaba o tenía deficiencias, tales como mejoras en el registro de bitácoras de algunos ataques, soporte para comandos y herramientas adicionales que son parte del protocolo SSH. Algunas de las nuevas caracterísi-

cpu, reboot, entre otras), uso de "*" y "!" para la autenticación de usuarios (userdb), bitácoras en texto, una base de datos, el formato JSON, entre otras. Las características antes mencionadas permiten mejorar la emulación y ampliar la interacción del honeypot, haciéndole pensar a los atacantes que es un servicio real; esto posibilita una mayor ejecución de comandos de los atacantes logrando obtener mayor información y mejores resultados al procesar y analizar las bitácoras.

Cuando un atacante, malware o intruso intenta entrar a un equipo a través del servicio (SSH o Telnet) y no cuenta con los datos de acceso (usuario y contraseña), intentará realizar un ataque de fuerza bruta o de diccionario para identificar las credenciales válidas. Posteriormente ingresará al sistema e intentará realizar otras actividades como la infección del equipo, ataques de denegación de servicio o la identificación de equipos para efectuar un movimiento lateral. Una vez iniciada la sesión, los módulos del honeypot identifican, controlan y procesan el comando ejecutado para generar una respuesta adecuada simulando ser un sistema real. Por ejemplo: si el comando ejecutado es cat/etc/shadow, Cowrie verificará que existe el comando, consultará el archivo shadow en su sistema de archivos y lo desplegará en pantalla. Todo este proceso es registrado en las bitácoras y los archivos descargados (generalmente malware) desde el honeypot son almacenados para su análisis posterior. El siguiente diagrama muestra el panorama general del funcionamiento de Cowrie.

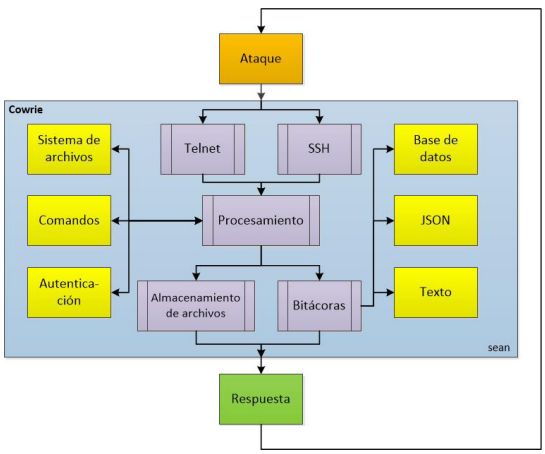


Figura 1. Panorama general de funcionalidad (de Sergio Anduin Tovar Balderas)

Instalación

Es posible instalar Cowrie en diversos sistemas operativos como Debian, Ubuntu, entre otros. Para esta prueba de concepto se utilizará Debian; primero se deberán configurar los parámetros de red y tener los repositorios actualizados para instalar las dependencias que requiere para su funcionamiento.

Los requisitos para la instalación son:

- Sistema Operativo Linux Debian 8.7.1 – Jessie
- Conexión a Internet
- Cowrie

El archivo */etc/apt/sources.list* contiene la lista de los repositorios donde se pueden obtener los paquetes necesarios para la instalación de Cowrie. Se recomienda utilizar la réplica de Debian más cercana para descargar más rápido los paquetes.

```
sean@honeypot: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
sean@honeypot:~$ su -
Password:
root@honeypot:~# cat /etc/apt/sources.list
deb http://mmc.geofisica.unam.mx/debian/ jessie main contrib non-free
deb-src http://mmc.geofisica.unam.mx/debian/ jessie main contrib non-free
deb http://security.debian.org/ jessie/updates main
deb-src http://security.debian.org/ jessie/updates main
root@honeypot:~# apt-get update
```

Figura 2. Configuración de los repositorios

Cowrie necesita los siguientes paquetes.

```
sean@honeypot: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@honeypot:~# apt-get install -y git virtualenv libmpfr-dev libssl-dev \
> libmpc-dev libffi-dev build-essential libpython-dev \
> python2.7-minimal
```

Figura 3. Instalación de paquetes para Cowrie

Una parte importante durante la instalación y configuración de honeypots es la creación de un usuario normal para que el honeypot se ejecute sin privilegios. Esto ayuda a prevenir que los atacantes se aprovechen de alguna falla en el diseño del honeypot y puedan obtener privilegios de súper usuario en el equipo.

Continuando con la instalación del honeypot, se requiere crear un usuario con el cual se ejecutará. También se descargará el código fuente de Cowrie desde su repositorio en GitHub.

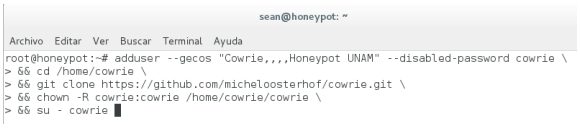


Figura 4. Creación de usuario y descarga de Cowrie

Existen diversas formas instalar Cowrie, una de ellas es utilizar virtualenv. Este módulo de Python permite crear un ambiente virtual en una carpeta particular sin interferir con los paquetes de Python del sistema nativo. Cada ambiente contiene su conjunto independiente de paquetes y su propio binario de Python.

Posteriormente, se instalan los paquetes de Python en el ambiente virtual (honeypot-unam) que Cowrie necesita para su funcionamiento.

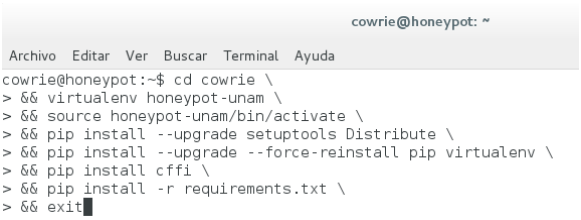


Figura 5. Instalación de paquetes de Python para Cowrie

Configuración

El archivo principal de configuración (cowrie.cfg) contiene secciones para habilitar diferentes opciones; es posible modificar el archivo con un editor como vi, nano o gedit.

- Nombre: la línea 23 define el nombre del equipo (`hostname = svr04`).
  El siguiente comando modifica la variable `svr04 por unam`.
  sed -i '23 s/svr04/unam/' /home/cowrie/cowrie/cowrie.cfg
- Habilitar el servicio: la línea 267 habilita el soporte para Telnet.
  El siguiente comando modifica la variable `false` por `true`.
  sed -i '267 s/false/true/' /home/cowrie/cowrie/cowrie.cfg
- Configuración de puertos: la línea 180 y 280 especifican el puerto para escuchar las conexiones entrantes de SSH y Telnet respectivamente.
  El siguiente comando modifica la variable `#listen_port = 2222` quitando el signo #
  sed -i '180 s/#listen_port = 2222/listen_port = 2222/' /home/cowrie/cowrie/cowrie.cfg
  El siguiente comando modifica la variable #listen_port = 2223 quitando el signo #
  sed -i '280 s/#listen_port = 2223/listen_port = 2223/' /home/cowrie/cowrie/cowrie.cfg
- Reglas: es necesario realizar esta configuración debido a que Cowrie se ejecuta sin permisos de súper usuario y no puede poner en escucha los puertos 22 y 23 correspondientes a SSH y Telnet respectivamente. Se utiliza iptables para hacer una redirección del puerto 22 al 2222 y del 23 al 2223.
  iptables -t nat -A PREROUTING -p tcp --dport 22 -j REDIRECT --to-port 2222
  iptables -t nat -A PREROUTING -p tcp --dport 23 -j REDIRECT --to-port 2223
- Permisos: se asigna el dueño y grupo cowrie a todos los archivos y carpetas.
  chown -R cowrie:cowrie /home/cowrie/cowrie

Figura 6. Configuración de variables en el archivo principal de configuración

Iniciar Cowrie

Existen diferentes formas iniciar Cowrie. El script start.sh se utiliza para iniciar el honeypot dependiendo de los argumentos pasados a través de la línea de comandos. Cuando se usa un ambiente virtual de Python, el primer argumento es el nombre del ambiente. La imagen 7 muestra los pasos para iniciar Cowrie cuando se ejecuta el comando *./start.sh honeypot-unam* con el usuario que se creó previamente.

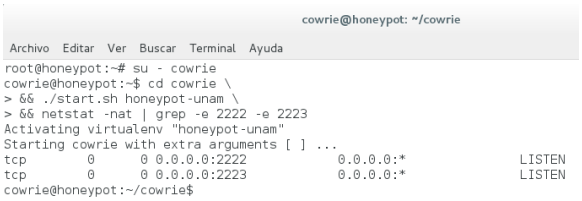


Figura 7. Iniciar Cowrie

Es importante verificar que los puertos 2222 y 2223 se encuentran en escucha (LISTEN), esto significa que el honeypot está ejecutando los procesos necesarios para abrir el socket en espera de conexiones entrantes.

Bitácoras

Es posible configurar Cowrie para registrar los eventos en archivos de texto, JSON, base de datos, entre otros. En la ruta de instalación se encuentra la carpeta log que contiene las bitácoras, una de ellas es cowrie.log. Este archivo contiene el registro de la actividad, configuraciones habilitadas, errores e inicio de los servicios indicando el puerto y la interacción de los atacantes con el honeypot.

Figura 8. Bitácora cowrie.log

Prueba de concepto

A continuación, se muestra un ataque de fuerza bruta realizado al servicio de SSH. Se podrá observar la combinación de usuarios y contraseñas, así como los intentos de autenticación fallidos y satisfactorios.

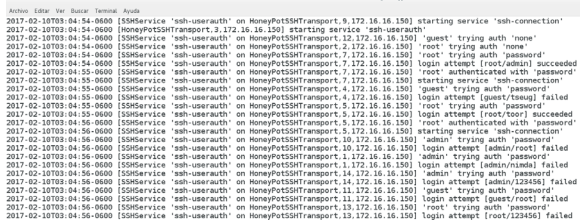


Figura 9. Ataque de fuerza bruta a SSH

Después de que el ataque de fuerza bruta o de diccionario fue satisfactorio, se conoce el usuario y contraseña válido para ingresar al honeypot. El atacante iniciará sesión y ejecutará comandos (interacción) creyendo que se trata de un equipo real, cuando en realidad toda actividad está siendo registrada y controlada por el honeypot para su análisis posterior.

La imagen 10 muestra la ejecución de algunos comandos (ls /, lscpu, cat /et/shadow, entre otros) realizados por los atacantes o malware.

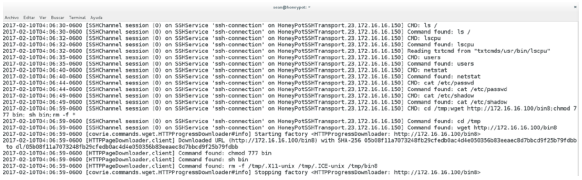


Figura 10. Registro de los comandos ejecutados

La información generada y almacenada en las diferentes bitácoras por Cowrie es de vital importancia ya que puede ser utilizada para generar ciberinteligencia en nuestra organización.

Una de las principales ventajas de Cowrie es el uso de JSON, esto posibilita procesar todos los datos obtenidos por el honeypot en un SIEM o en herramientas que permitan este formato como entrada.

El archivo de registro *cowrie.json* muestra los eventos de la interacción con cada uno de los comandos ejecutados en formato JSON.

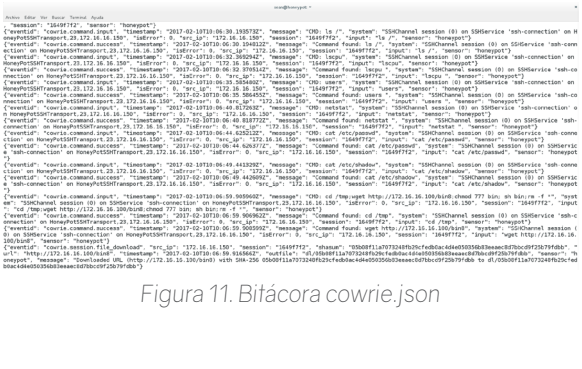


Figura 11. Bitácora cowrie.json

En la imagen 11 se puede observar el siguiente registro.

{“eventid”: “cowrie.session.file_download”, “src_ip”: “172.16.16.150”, “session”:

"1649f7f2", "shasum": "05b08f11a7073248fb29cfedb0ac4d4e-050356b83eeaec8d7bbcd9f25b79fdbb", "url": "http://172.16.16.100/bin8", "timestamp": "2017-02-10T10:06:59.916566Z", "outfile": "dl/05b08f11a7073248fb29cfedb0ac4d4e-050356b83eeaec8d7bbcd9f25b79fdbb", "sensor": "honeypot", "message": "Downloaded URL (http://172.16.16.100/bin8) with SHA-256 05b08f11a7073248fb29cfedb0ac4d4e-050356b83eeaec8d7bbcd9f25b79fdbb to dl/05b08f11a7073248fb29cfedb0ac4d4e-050356b83eeaec8d7bbcd9f25b79fdbb"}

Este evento muestra la descarga del archivo bin8 desde el servidor web http://172.16.16.100. El honeypot es capaz de almacenar el archivo en la carpeta dl dentro del directorio de instalación de Cowrie renombrando el archivo bin8 con su firma SHA256.

Es posible buscar el archivo sospechoso en el servicio web de VirusTotal a través de su firma SHA256 o subir el archivo para tener otra opinión de múltiples antivirus. Para determinar si el archivo sospechoso es algún tipo de malware es necesario realizar un análisis de malware. Se puede buscar el archivo sospechoso en esta URL.

La Red Distribuida de Honeypots (RDH) es un proyecto colaborativo de detección de eventos de seguridad implementado y administrado por el Proyecto Honeynet de UNAM-CERT. Los eventos de seguridad que se pueden observar en el mapa son conexiones de malware, SSH y Telnet dirigidas hacia los honeypots que forman parte de la RDH. Este honeypot forma parte de los sensores de UNAM-CERT en la RDH. Si desea ver los eventos en tiempo real dirigidos a los honeypots de la RDH puedes consultar http://map.cert.unam.mx.

Conclusión

Este artículo mostró la implementación de Cowrie. Las nuevas características del honeypot mejoran a Kippo debido a la capacidad de interacción, registro de eventos e integración con otras herramientas. La prueba de concepto muestra cómo se registran en dos bitácoras diferentes los eventos de un ataque de fuerza bruta y los comandos ejecutados cuando ingresan al honeypot.

A través del procesamiento, análisis e interpretación de la información generada por Cowrie se puede identificar equipos que están distribuyendo malware o realizando ataques de fuerza bruta y poder mitigar actividades maliciosas para mejorar la seguridad en una organización.
Antes de desplegar un sistema con servicios de Telnet o SSH, es recomendable cambiar las contraseñas preestablecidas por unas seguras, utilizar una red de administración, crear reglas de firewall y/o listas de control de acceso (ACL), complementar con TCPwrapper, firewall de host y programas como fail2ban o SSHGuard en los dispositivos.

SI deseas ver el video del artículo consulta el canal SeguridadTV de UNAM-CERT o entra directamente aquí.

Referencias

Botezatu, B. (2016, 23 de octubre). Unprotected IoT devices killed the US Internet for hours. Bitdefender BOX. Recuperado de https://www.bitdefender.com/box/blog/iot-news/mirai-iot-security-alert/

Cisco. (2016). Cisco 2016 Annual Security Report. Recuperado de http://www.cisco.com/c/dam/assets/offers/pdfs/cisco-asr-2016.pdf

Coret, J.A. (2006, 1 de abril). Kojoney - A Honeypot For The SSH Service. Recuperado de http://kojoney.sourceforge.net/

Khalimonenko, A., Strohschneider, J., Kupreev, O. (2017, 2 de febrero). DDoS attacks in Q4 2016. Securelist. Recuperado de https://securelist.com/analysis/quarterly-malware-reports/77412/ddos-attacks-in-q4-2016/

----------. (2016, 31 de octubre). Kaspersky DDOS intelligence report for Q3 2016. Securelist. Recuperado de https://securelist.com/analysis/quarterly-malware-reports/76464/kaspersky-ddos-intelligence-report-for-q3-2016/

Oosterhof, M. (2017). Cowrie Honeypot - Security Intelligence. Cowrie Honeypot. Recuperado de http://www.micheloosterhof.com/cowrie/

----------. Cowrie SSH/Telnet Honeypot. GitHub. Recuperado de https://github.com/micheloosterhof/cowrie

Tamminen, U. (2016, 30 de septiembre). Kippo –SSH Honeypot. GitHub. Recuperado de https://github.com/desaster/kippo

VirusTotal. (s.f.). VirusTotal - Free Online Virus, Malware and URL Scanner. Recuperado de https://www.virustotal.com/

Si quieres saber más:

- La importancia de las pruebas de penetración
- Glastopf: Honeypot de aplicaciones web - I
- ¿Qué es y cómo funciona un ataque DDoS?

Sergio Anduin Tovar Balderas

Es egresado de la carrera de Ingeniería en Computación con módulo de salida en Redes y Seguridad por la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM).

Labora desde 2014 en la Coordinación de Seguridad de la Información (CSI/UNAM-CERT) en el área de Detección de Intrusos y Tecnologías Honeypot, donde lleva a cabo actividades de desarrollo, instalación y pruebas de tecnologías honeypot para análisis y detección de actividad maliciosa.

Fue instructor de la línea de especialización Detección de Intrusos y Tecnologías Honeypot en el Congreso Seguridad en Cómputo UNAM 2014.

Egresado de la octava generación del Plan de Becas en Seguridad Informática de UNAM-CERT. Ha participado como instructor de nuevas generaciones en este mismo plan de capacitación. Laboró en el proyecto Seguridad en UNIX de la misma organización, además ha impartido cursos y participado en proyectos con dependencias de la UNAM y entidades externas del sector público.

Cuenta con la certificación IPS-ESE (IPS Express Security for Engineers) de Cisco.

Recomendaciones antes de liberar tu página web

Jesús Mauricio Andrade Guzmán

Proteger tu página web y los datos de tus usuarios es una tarea cada vez más complicada. El desarrollo de páginas web se ha convertido en un gran negocio, pero la alta demanda implica una oferta en aumento que, desafortunadamente, baja la calidad del producto final. La presión de entregar una página web en tiempo y forma hace que los desarrolladores cada vez inviertan menos tiempo en cuestiones que perciben menos "críticas", como la seguridad o el rendimiento del sitio.

El propósito de este artículo es proporcionar consejos generales de rendimiento y defensa para aplicaciones web. Estas recomendaciones aplican para cualquier tipo de proyecto web, ya sea que esté basada en un gestor de contenidos o en otro tipo de desarrollo. Quizás el único requisito es que sea una página pública a través de un servidor web como Apache, Ngnix, IIS, entre otros.

Las consideraciones de administración de sistemas o desarrollo de aplicaciones dependen en gran medida de los recursos que los actores involucrados tengan a la mano. Un estudio independiente de diseño web o incluso desarrolladores independientes (freelancers), no tienen acceso a los mismos recursos que una universidad o una empresa de mayor tamaño. La tendencia del mercado es la reducción de costos y tiempos, pero es importante tener en cuenta los riesgos e implicaciones de las decisiones que se toman. Incluso si hablamos de una universidad o empresa grande, los equipos de desarrollo web no están necesariamente en contacto directo

con los administradores de sistemas. Para estos equipos de desarrollo, las siguientes recomendaciones pueden ser de utilidad.

A modo de ejemplo, hoy en día los servicios de hospedaje web ya incluyen muchas opciones de protección, como servicios de firewall de red, firewall de aplicaciones, protección para DDoS, entre otros; sin embargo, los equipos de desarrollo no tienen acceso a la configuración de estas funciones, las opciones disponibles se reducen a "encendido" y "apagado".

Figura 1. No siempre es posible acceder a la tabla de reglas de ModSecurity

El servicio de hospedaje es un material de trabajo, más que parte de un proyecto en sí; y no es posible acceder a configuraciones como las que se comentan en artículos previos de la revista .Seguridad [1] y [2], porque los desarrolladores son también clientes del proveedor de servicios de hosting. Esta situación se complica un poco más con servicios de hosting compartido en los que únicamente se tiene acceso a la consola del gestor de contenido, y si hay suerte, a la base de datos. En la mayoría de los casos, hay que trabajar con versiones de software no actualizado o configuraciones de rendimiento sin optimización.

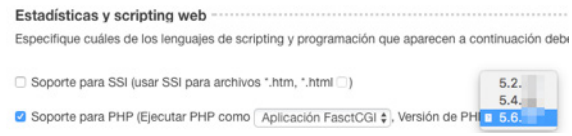


Figura 2. A veces la versión más reciente de PHP disponible es 5.6.X

¿Qué puedo hacer?

Si te has encontrado en esta situación, no todo está perdido. Las siguientes tres consideraciones te pueden ayudar a agregar características de seguridad y rendimiento a tus proyectos con una inversión mínima de tiempo, conocimientos o de dinero. Es posible que estés a punto de liberar tu siguiente proyecto web y esta lista puede serte útil como guía por si no has considerado estas tres opciones en tu proyecto. Recuerda que sin importar si el proyecto es un desarrollo propio, una aplicación web basada en gestores de contenido o cualquier otro tipo de servicio en línea que utilice Internet, puedes aplicar alguna de estas recomendaciones con relativa facilidad.

1. Caché

La utilización de sistemas de caché en un proyecto debe estar acompañada de un entendimiento, al menos en términos generales, de las implicaciones de seguridad que debe tener disponible una sección del contenido de esta manera.[1] Sin embargo, a veces es inevitable el uso de estos sistemas porque el rendimiento del servidor es insuficiente, la carga de peticiones es mayor a la esperada o el presupuesto de ancho de banda es limitado. Esta recomendación asume que existe alguna justificación para utilizar servicios de caché en un proyecto web, por ejemplo, que la tecnología en la que se desarrolla un proyecto web incluye estas funciones y desactivarlas afectaría el rendimiento del sistema.

Las funciones de caché para aplicaciones web muchas veces están ya incluidas en la configuración de tu servidor web o son una función automática del lenguaje que utilizas para servir contenido dinámico. Otra manera de utilizar caché en una página web es aprovechando las funciones de los navegadores, que pueden guardar datos en la computadora de tus usuarios para evitar la consulta remota lo más posible. En "Caching Tutorial for Web Authors and Webmasters" [4], puedes encontrar una reseña sobre lo que puede hacer el caché para tu página.

Sobre las opciones de caché en el servidor, básicamente se trata de configurarlo para que guarde una copia estática de los

archivos de tu página. Este tipo de caché almacena las secciones de tu sitio en un formato que no puede ser procesado por el lenguaje para servir contenido dinámico (pensemos que las páginas PHP o Java se guardan como HTML), lo que libera la carga de procesamiento de tu servidor y responde más rápido.

Activar configuraciones de caché puede ser cuestión de instalar un complemento para tu gestor de contenidos. Algunas opciones para Wordpress son W3 Total Cache, WP Super Cache, WP Rocket, de los que puedes consultar esta lista comparativa [5]; para Drupal puedes consultar [6]. Sin embargo, esta opción no siempre está disponible, porque supone al menos acceso al directorio de la aplicación (FTP, SFTP, SSH, entre otros), o incluso privilegios para instalar módulos para el servidor (como Apache y Nginx) o para el lenguaje (como PHP y Java).

2. CDN (Redes de Distribución de contenido)

Otra opción para mejorar el rendimiento son las redes de distribución de contenido (CDN) que se encargan, en términos generales, de servir como intermediarios para una parte del contenido (o todo) que se distribuye en tu sitio. La idea es que estos servicios respondan a los usuarios desde una ubicación optimizada, de forma que el tiempo de espera para una solicitud sea menor.

Una manera común de integrar esta tecnología es accediendo a bibliotecas comunes como jQuery, Bootstrap, Google, Font Awesome, entre muchas otras. Puedes consultar cómo incluir en tu proyecto las versiones CDN de las bibliotecas de funciones que utilices para evitar la descarga desde tu servidor. Por ejemplo, para incluir jQuery desde su versión CDN alojada por Google, debes agregar esto a la cabecera de tu página:

```
<script src="https://ajax.google-
apis.com/ajax/libs/jquery/3.1.1/
jquery.min.js"></script>
```

Lo anterior descargará la versión 3.1.1 de jQuery desde un servidor de Google, evitando la consulta a tu servidor para jQuery. Revisa la documentación de las bibliotecas que utilizas, es muy probable que puedas ahorrar tiempo de procesamiento y de respuesta con esta estrategia.

Por otro lado, las redes CDN pueden servir también para distribuir el contenido completo de tu proyecto web. Puedes consultar [7] y [8] donde se explica el funcionamiento general y se enlistan las más populares. Cabe destacar que el funcionamiento de este tipo de servicios puede estar integrado incluso al registro DNS del dominio de tu proyecto, sin afectar tu servicio de hosting. Lo que ocurre es que esta red se encarga de distribuir tu contenido y evitar que la petición llegue a tu servidor. La ubicación de los nodos de estas redes globales garantiza que tu contenido se servirá desde el sitio geográfico que más le convenga a tus usuarios.

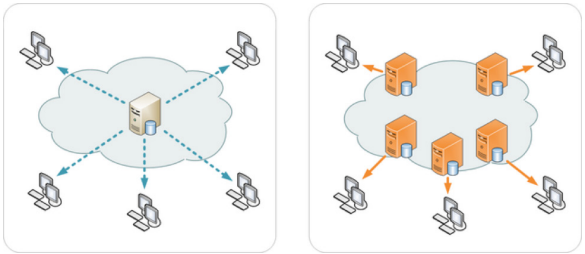


Figura 3. A la izquierda, un servidor web normal, a la derecha una red de distribución de contenido [https://en.wikipedia.org/wiki/File:NCDN_-_CDN.png]

Las empresas que ofrecen los servicios de distribución de contenido también ofrecen opciones de seguridad para sus usuarios. Debido a que estas redes están en una capa anterior a la infraestructura del servidor web principal, se pueden colocar servicios de firewall de aplicaciones, protecciones de DDoS, cifrado SSL, entre otros.

Por ejemplo, para protección de DDoS, un servicio CDN puede soportar una carga significativamente mayor a un servidor alojado en hospedajes de capacidad estándar.

Cuando un ataque de este tipo se detecta por la CDN, el usuario puede recibir alertas y, literalmente, presionar un botón de pánico para informar a sus usuarios que el sitio está bajo un ataque. La función de la CDN es responder a las peticiones masivas con la posibilidad de distinguir entre las peticiones de ataque y las legítimas, como se muestra en la figura 4.

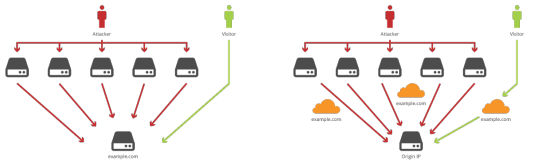


Figura 4. A la izquierda, el esquema de ataque DDoS; a la derecha, la protección de CDN ante DDoS [9]

Para mayor información, puedes consultar otros riesgos que puedes evitar con esta tecnología en [10], [11] o [12].

Al utilizar una CDN es de suponer que confías en el distribuidor de contenidos; esto es importante porque este tipo de servicios puede incluir condiciones por parte de estas empresas, lo que implica la recopilación de información de tu página (por ejemplo, para estadísticas de uso). Estar en un punto intermedio entre el usuario y el servidor principal también otorga a este tipo de servicios privilegios muy interesantes: pueden permitir a la CDN mostrar publicidad a los usuarios (ads) o modificar el código que se envía desde tu página sin que tengas ningún control sobre el proceso. Si decides utilizar este tipo de servicio, asegúrate de comprender sus implicaciones e investiga las opciones disponibles con base en tus necesidades específicas, así como consultar con cuidado los términos y condiciones de uso.

3. Herramientas anti *spam*

La manera de proteger una página web contra el spam es relevante cuando el proyecto considera datos de entrada de parte de los usuarios, ya sea en forma de formularios de contacto, foros de discusión, listas de correo, entre otros. Al permitir que una página reciba datos de entrada, es necesario añadir algún mecanismo para evitar mensajes de spam, o ataques que vulneren el sistema que soporte la página web.

No siempre es posible integrar al desarrollo un sistema de monitoreo o moderación de comentarios a una página web, porque esta función muchas veces es secundaria para el objetivo principal del proyecto. Sin embargo, considerar un mecanismo de moderación o protección contra el spam, hará que esté mejor protegido y evitará problemas futuros, mantenimientos inesperados o corrección de fallas no programadas.

En este caso, tu mejor opción es transferir la operación de los comentarios a una plataforma de terceros, como Facebook [13], Disqus [14] o Wordpress [15] con Akismet [16], o lo que dependerá de cada proyecto, además de que se debe considerar la privacidad de los usuarios al elegir alguno de estos servicios.

Conclusión

Claramente, esta no es una lista exhaustiva de características de seguridad o de las herramientas para atender estas cuestiones. Reconocer posibles amenazas que puedan afectar a tu aplicación es un primer paso muy importante para evitar estos problemas. Los cuidados y medidas que puedas adoptar dependerán de tu proyecto y de los usuarios a los que esté orientada tu página web. Recuerda que la seguridad y privacidad de la información de los usuarios de tu página estará bajo tu cuidado, al consultar tu sitio y posiblemente después, si almacenas información.

Referencias

[1] Los riesgos de utilizar caché se pueden consultar en [3], en la sección "Browser Cache".

[1] Díaz, S. S. (Enero-febrero 2013). Firewall de Aplicación Web - Parte I. .Seguridad

Cultura de prevención para TI. Recuperado de: http://revista.seguridad.unam.mx/node/2167

[2] Díaz, S. S.; Ramírez, D. O. (Marzo-abril 2013). Firewall de Aplicación Web - Parte II. .Seguridad Cultura de prevención para TI. Recuperado de: http://revista.seguridad.unam.mx/node/2175

[3] OWASP. (30 de junio de 2016). OWASP Application Security FAQ - OWASP. OWASP. Recuperado de: https://www.owasp.org/index.php/OWASP_Application_Security_FAQ#Browser_Cache

[4] Nottingham, M. (6 de mayo de 2013). Caching Tutorial for Web Authors and Webmasters. mnot. Recuperado de: https://www.mnot.net/cache_docs/

[5] Ewer, T. (28 de febrero de 2017). The Top 3 WordPress Caching Plugins Compared and Choosing the Best One for Your Site. WPMU DEV- The WordPress Experts. Recuperado de : https://premium.wpmudev.org/blog/top-wordpress-caching-plugins/

[6] Drupal. (s.f.). Caching to improve performance. Drupal. Recuperado de: https://www.drupal.org/docs/7/managing-site-performance-and-scalability/caching-to-improve-performance [Consultado: 06-mar-2017].

[7] Wikipedia. (1 de enero de 2017). Red de entrega de contenidos. Wikipedia, La enciclopedia libre. Recuperado de: https://es.wikipedia.org/wiki/Red_de_entrega_de_contenidos

[8] Wikipedia. (22 de marzo de 2017). Content delivery network. Wikipedia, The Free Encyclopedia. Recuperado de: https://en.wikipedia.org/wiki/Content_delivery_network

[9] Sullivan, N. (30 de julio de 2013. DDoS Prevention: Protecting The Origin. Cloudflare Blog. Recuperado de: http://blog.cloudflare.com/ddos-prevention-protecting-the-origin/

[10] Cloudfare. (s.f.). Security. Cloudflare. Recuperado de: https://www.cloudflare.com/security/

[11] KeyCDN. (2017). CDN Features | API, Raw Logs, HTTP/2, Free Custom SSL, Real-time Analytics and many more. KeyCDN. Recuperado de: https://www.keycdn.com/features

[12] Imperva. (2017). Website Security | Bot Filtering | Anti-DDoS | PCI Compliance. Imperva Incapsula. Recuperado de: https://www.incapsula.com/website-security/

[13] Facebook for Developers. (s.f.). Plugin de comentarios. Facebook for Developers. Recuperado de: https://developers.facebook.com/docs/plugins/comments/

[14] Disqus. (2017). Disqus – The #1 way to build your audience. Disqus. Recueprado de: https://disqus.com/

[15] WordPress. (s.f.). Comments in WordPress. WordPress.ORG. Recuperado de: https://codex.wordpress.org/Comments_in_WordPress

[16] Akismet. (s.f.). Akismet: Spam Protection for WordPress. Akismet. Recuperado de: https://akismet.com/

Si quieres saber más, consulta:

- ¿Es la seguridad de la información un freno o un facilitador de la expansión del negocio?
- Consejos para desarrolladores web con enfoque a comercio electrónico
- Ataques web

Jesús Mauricio Andrade Guzmán

Maestro en Ciencias (Computación), egresado del Posgrado en Ciencia e Ingeniería de la Computación, de la Universidad Nacional Autónoma de México.

Colaboró con la Coordinación de Seguridad de la Información de 2003 a 2013. Especialista en defensa de aplicaciones web (GIAC GWEB), administración de servicios y desarrollo de software.

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM CERT®

Revista .Seguridad *Cultura de prevención para* TI
No.28 / abril - mayo 2017