Departamento de Seguridad Informática MINSAP

Agosto 2017

Volumen 1, nº 1

# Boletín de Seguridad Informática

Contenido:



Puntos de interés especial:

- **Tres fallos de seguridad** (CVE-2017-3108, CVE-2017-3107 y CVE-2017-3110), cuya gravedad varía entre moderada e importante
- El Instituto Jinan de Tecnología Cuántica en **China planea lanzar un nuevo sistema de mensajería que aseguran es imposible de "hackear"**

## Adobe parchea 80 vulnerabilidades presentes en productos como Flash Player, Reader y Acrobat

**Adobe** ha publicado un paquete con **80 actualizaciones de seguridad** para los productos Flash Player, Adobe Acrobat, Adobe Reader, Digital Editions y Experience Manager.

Para **Flash Player**, que actualmente se encuentra en su versión 26.0.0.151, se han corregido dos vulnerabilidades importantes que han llegado a las implementaciones para **Windows, Mac, Linux y Chrome OS**. Una (CVE-2017-3085) se trataba de un fallo que permitía filtrar información, mientras que la otra (CVE-2017-3106) era una confusión de tipos que abría la puerta a la ejecución de código en remoto.

La mala prensa que tiene Flash en términos de seguridad ha motivado a muchos usuarios a evitar su uso en lo máximo posible. Lejos de ser esto una costumbre de paranoicos o *geeks*, ha llegado hasta a ser implementada en Google Chrome. Los detractores de esta tecnología se habrán alegrado tras saber que Adobe tiene planeado ponerle fin en 2020.

**69 vulnerabilidades** han sido corregidas en las versiones 2017.009.20058, 2017.008.30051, 2015.006.30306 y anteriores de **Reader y Acrobat tanto para Windows como Mac**. Algunas de las vulnerabilidades más importantes permitían a un hacker tomar el control del sistema afectado.

Como es lógico, la gran cantidad de fallos corregidos hace entrever que hay vulnerabilidades de todo tipo. Los parches publicados también van dirigidos a corrupciones de memoria, vulnerabilidades de usar después de liberar memoria, desbordamientos y confusiones de tipos. La compañía ha comentado que estas pueden ser explotadas para la ejecución de código en remoto y en algunos casos podrían llevar a una filtración de información.

**Tres fallos de seguridad** (CVE-2017-3108, CVE-2017-3107 y CVE-2017-3110), cuya gravedad varía entre moderada e importante, han sido corregidas en el producto de gestión de contenido empresarial **Experience Manager**. Fueron reportados de forma anónima y permitían a los atacantes filtrar información y ejecutar código arbitrario.

Otras **nueve vulnerabilidades** han sido corregidas en el lector de libros electrónicos **Digital Editions** en sus versiones para **Windows, Mac, Android e iOS**. Dos de los fallos (CVE-2017-11274 y CVE-2017-11272), que han sido marcado como críticos, abrían la puerta a la ejecución de código y al filtrado de información.

## TrickBot es un troyano que se propaga de forma similar a WannaCry y NotPetya

Utilizar el protocolo SMB se ha convertido en buen recurso para ayudar a esparcir un malware. Después de ver los estragos causados por WannaCry y NotPetya, está apareciendo malware que usa el mismo mecanismo para difundirse y conseguir así un mayor impacto, como es el caso de la nueva versión del troyano bancario **TrickBot**.

La última versión de TrickBot, conocida como "1000029" (v24) , ha sido encontrada haciendo uso del protocolo SMB (Windows Server Message

Block), utilizado por Microsoft Windows para compartir recursos a través de red (ficheros, impresoras, unidades de red… ), pudiendo compartir también con sistemas operativos Unix y Unix-like mediante Samba, una implementación software libre del mismo protocolo.

Las versiones anteriores de TrickBot tuvieron el año pasado como objetivo a entidades financieras de todo el mundo, usando el método de phishing para infectar a sus víctimas. Sin embargo, según Flashpoint, el troyano ha **evolucionado para propagarse localmente a través de las redes mediante SMB, aunque carece de algunas de las características más avanzadas vistas en WannaCry y NotPetya**, como la capacidad de escanear de forma aleatoria IP externas para buscar conexiones SMB, las cuales fueron incorporadas en un exploit de la NSA llamado EternalBlue.

Flashpoint comenta que la actual versión del troyano bancario ha sido modificado para escanear dominios incluidos en una lista de servidores vulnerables a través de la API NetServerEnum de Windows, además de enumerar otras computadoras conectadas a la red a través de LDAP (Lightweight Directory Access Protocol).

TrickBot también puede ser distribuido mediante un falso fichero *setup.exe* y enviado a través de un script de PowerShell para propagarse por la comunicación entre procesos y descargar así versiones adicionales de TrickBot en unidades compartidas.

Evitar abrir ficheros o enlaces sospechosos o de origen desconocido, hacer copias de seguridad de forma rutinaria, tener el antimalware y el resto del software con las últimas actualizaciones de seguridad instaladas e inhabilitar SMB en caso de no usarlo son buenos consejos a seguir para evitar la infección por TrickBot.

## Microsoft publica el primer parche para una vulnerabilidad hallada en WSL

Microsoft publicó el miércoles de esta semana su paquete de parches para corregir vulnerabilidades halladas en sus productos. Lo más destacable es que por primera vez vemos una corrección para un fallo de seguridad hallado en **WSL** (Windows Subsystem for Linux), el subsistema que permite ejecutar una cantidad limitada de distribuciones Linux sobre Windows y que recientemente ha llegado a Windows Server.

La vulnerabilidad (CVE-2017-8622) hallada en WSL **radicaba en cómo manejaba dicha tecnología las tuberías con nombres utilizadas para las comunicaciones entre procesos, abriendo así la puerta a la ejecución de código con permisos de administrador**. Sin embargo, para ser explotada requería de acceso local al sistema, por lo que su posible impacto quedaba minimizado. Microsoft la ha etiquetado como una escalada de privilegios que afecta la versión 1703 de Windows 10 64-bit.

Recordamos que WSL apareció en la conferencia Build 2016 como "Ubuntu Bash para Windows 10", ya que este subsistema lo que permite es la ejecución de programas y aplicaciones Linux con un interfaz de línea de comandos. Aunque la distribución de Canonical tomó la delantera, más tarde aparecieron openSUSE, SUSE Enterprise Linux y Fedora.

Otros fallos importantes de los corregidos por Microsoft el día de ayer fueron unos problemas de corrupción de memoria hallados en el motor de scripts utilizado por **Internet Explorer y Microsoft Edge**, los cuales están acompañados de otras 17 vulnerabilidades que abrían la puerta a la ejecución de código en remoto a través de los mencionados navegadores. Para su explotación solo era necesaria la utilización de páginas web con código JavaScript malicioso.

Otros componentes parcheados han sido el motor de bases de datos JET, Windows Search, componentes como los relacionados con el despliegue de documentos PDF, el protocolo de escritorio remoto, la herramienta de colaboración Sharepoint, SQL Server y Adobe Flash Player.

## Delitos informáticos causan pérdidas superiores a los 100 mil millones de dólares.

**El alcance de las tecnologías de la información lleva hoy a nuevos delitos como la usurpación de identidad, fenómeno que ocasionó en los últimos seis años pérdidas superiores a los 100 mil millones de dólares.**

La consultora Javelin Strategy y Research señaló en su investigación que las modalidades más vulneradas son los documentos oficiales, tarjetas de crédito, teléfonos móviles, fraude bancario, así como los datos personales y los préstamos.

Entre las preocupaciones de la entidad, destaca la carencia de estadísticas globales, lo cual impide conocer el alcance del delito a nivel mundial, y resaltó que **solo en Estados Unidos hubo cerca de 15,4 millones de víctimas en 2016, cifra que superó en 16 por ciento el dato de 2015.**

Analistas del tema alertan a los usuarios sobre la información que publican

en la red, pues en ella existe un mercado virtual e ilegal donde se compran y venden todo tipo de datos, entre los cuales se encuentran pasaportes, tarjetas de identidad, direcciones de correo electrónico, contraseñas y, por supuesto, claves bancarias.

Ese incremento de los casos de robo de identidad y las pérdidas millonarias impulsaron la creación de una guía para que las organizaciones que procesan, almacenan o transmiten datos de tarjetas de pago aseguren la información y eviten el fraude.

Dicha iniciativa se conoce como Estándar de seguridad de datos de la industria de tarjetas de pago, pero aún se encuentra en vías de implementación.

Advirtió la investigación que en esta era, donde el empleo de las redes sociales -Facebook, Instagran, Linkedin, entre otras-, tienen mayor alcance, algunos usuarios publican información sensible que puede ser empleada por los estafadores y facilitar sus ataques.

**Para protegerse, el estudio sugirió emplear los programas antivirus y otros de protección de datos, y estimó que cerca del 80 por ciento de los cibercrímenes pueden evitarse si las personas actúan con mayor discreción.**

Otras vías de defensa, aconsejó, pueden ser no emplear fechas de nacimiento en contraseñas y códigos PIN (Personal Identification Number), no dejar los datos importantes por escrito, así como destruir los documentos importantes antes de botarlos.

Las empresas también pueden ser estafadas cuando, por ejemplo, el delincuente suplanta la identidad de un alto directivo, envía un correo electrónico al contable y solicita una transferencia a determinada cuenta. Con esta técnica a inicios de año un banco belga perdió 70 millones de euros.

Expertos aconsejan adoptar algunas medidas ante la sospecha de suplantación de identidad, como recopilar toda la información posible, guardar los mensajes de texto, revisar las redes sociales, avisar a los contactos sobre el perfil falso y realizar la denuncia a las autoridades.

El hackeo de identidad puede tener intenciones alejadas del lucro y varía desde el acoso a una persona en nombre del usurpado, la compra de productos ilegales en la llamada red oscura o sencillamente vender información sobre la víctima.

La denominada suplantación o usurpación de identidad es el delito mediante el cual una persona se hace pasar por otra para llevar a cabo actividades de carácter ilegal, como pueden ser pedir un crédito o préstamo hipotecario, contratar nuevas líneas telefónicas o atacar a terceras personas.

Las víctimas de este delito -personas o empresas- pueden perder su patrimonio en caso de robo, ser objetos de chantaje o verse involucrados en hechos delictivos que ni siquiera imaginan.

## China lanzará un sistema de mensajería “imposible de hackear”

El Instituto Jinan de Tecnología Cuántica en **China planea lanzar un nuevo sistema de mensajería que aseguran es imposible de “hackear”**, informa *The Telegraph*.

**El funcionamiento del servicio se basa en una tecnología cuántica mucho más segura que los cables de Internet o de teléfono que transmite los mensajes incrustados en partículas de luz**.

En caso de que una tercera persona intentara acceder a la información enviada, el sistema cortaría automáticamente la comunicación y el mensaje sería imposible de interpretar.

**El nuevo programa fue probado a principios del julio y estará disponible para 200 miembros del personal gubernamental, financiero y militar de la ciudad de Jinan** (provincia de Shandong). Los autores del proyecto estiman empezar a comercializar el producto en el mes de agosto.

El subdirector del instituto, Zhou Fei, afirmó que **su intención es utilizar el servicio para “la defensa nacional, las finanzas y otros campos”**. Además, los creadores estiman que si el sistema tiene éxito, se extenderá a toda China y por el mundo entero, indica el *Financial Times*.

Según *China Daily*, **el proyecto tendrá un costo de 19,5 millones de dólares y será capaz de cifrar hasta 4 mil datos por segundo**.

## Confirman ataques cibernéticos contra funcionarios de Gran Bretaña y Alemania

**Este sábado se produjeron ataques cibernéticos contra funcionarios y legisladores del Parlamento británico cuando varios hackers intentaron acceder a varias cuentas de correo electrónico.**

**También emails personales de varios funcionarios alemanes fueron objeto de un ciberataque** similar al que padeció el año pasado el Partido Demócrata estadunidense, informó el Departamento Federal de Seguridad de Técnica Informativa de Alemania (BSI, por sus siglas en alemán).

La ofensiva contra el Parlamento es investigada por funcionarios británicos, luego de descubrir “intentos no autorizados de acceder a cuentas de legisladores”. Por razones de seguridad, se comunicó, los parlamentarios no tendrán acceso a su correo electrónico

fuera de Westminster.

**Una vocera de la Cámara de los Comunes informó que el hackeo afectó la capacidad de los parlamentarios y de personal auxiliar para acceder al sistema y usar su email. Al momento del informe no había datos sobre cuántos legisladores resultaron perjudicados, ni cuál es la magnitud de la agresión.**

"Seguimos investigando este incidente y adoptaremos nuevas medidas para asegurar la red de computadoras en colaboración con el Centro Nacional de Ciberseguridad", señaló la portavoz.

El Centro Nacional de Ciberseguridad y la Agencia Penal Nacional ya indagan el incidente. Liam Fox, ministro para el Comercio Internacional, dijo que el ataque "no es sorpresa y debería servir como advertencia" para los británicos. Este hackeo es el segundo en los pasados dos meses. El primero se reportó el pasado 12 de mayo, cuando el Sistema Nacional de Salud fue blanco de un ciberataque que infectó a la red computarizada y obligó a algunos hospitales a frenar la admisión de pacientes y a desviar ambulancias.

**Paralelamente, Alemania "está observando un agresión cibernética profesional contra correos personales de funcionarios de instituciones económicas y la administración", comunicó el BSI.** Añadió que esta agresión es de características similares a los padecidos por el Comité Nacional Demócrata estadunidense en 2016 y el movimiento político La República en Marcha en las pasadas elecciones francesas, supuestamente ejecutados por hackers rusos para presuntamente intervenir en los procesos electorales en Estados Unidos y Francia.

Las acusaciones contra Rusia fueron esgrimidas frecuentemente por políticos durante campañas efectuadas en los pasados dos años, aunque sin ninguna prueba.

Mientras tanto, la Agencia Central de Inteligencia estadunidense concluyó que sí existió inferencia ilegal, vía ataques cibernéticos, en la elección presidencial de 2016.

## Nuevo ciberataque golpea a gigante del petróleo y bancos en Rusia y Ucrania

Una **gran ola de ataques cibernéticos** que recuerda el modo de acción del virus WannaCry ha golpeado este martes a diferentes **empresas en Ucrania, alternado el funcionamiento de los bancos y aeropuertos, y Rusia**, donde incluso ha sido atacado el **gigante petrolero Rosneft**. Una información que incluso ha dado a conocer el viceprimer ministro de Ucrania, **Pavlo Rozenkoe**, a través de Twitter.

Según la información reportada por varias compañías, un nuevo virus tipo «ramsonware», una vez que ha infectado los ordenadores, exige un rescate de 300 dólares en Bitcoins y de momento ha afectado al Banco Nacional de Ucrania (NBU), metro de Kiev, los servicios informáticos del Gobierno ucraniano y el gigante petrolero estatal ruso.

El Centro Criptológico Nacional (CCN-CERT) ha identificado ya que el ataque «contra varias multinacionales con sede en España que afecta a sistemas Windows, cifrando el sistema operativo o disco y cuya propagación es similar a la de WannaCry; es decir, una vez ha infectado una máquina puede propagarse por el resto de sistemas conectados a esa misma red».

CCN-CERT asegura que el «malware» utilizado en la campaña es una variante de la familia Petya y aunque se ha detectado ya en empresas ubicadas en Ucrania, también en algunas multinacionales con sede en España.

Así, debido a este ataque, los pasajeros del **metro de Kiev** no podían pagar con tarjeta de crédito y los bancos han tenido que suspender su actividad en determinados servicios.En Rusia, **Rosneft**, uno de los mayores productores de petróleo del mundo, ha asegurado haber sido víctima de un «fuerte ataque», pero ha indicado que su producción no había sido interrumpida por un servidor de copia de seguridad. La **siderúrgica Evraz** también ha sido atacado, según ha declarado un portavoz de la agencia de noticias RIA-Novosti. De acuerdo con la empresa especializada en la seguridad informática Grupo IB, «cerca de 80 empresas fueron blanco» en Rusia y Ucrania. Entre ellos, Rosneft y grandes bancos de Ucrania, sino también compañías como **Nivea, Auchan** y las estructuras de gobierno de Ucrania.

Según la misma fuente, el nuevo ciberataque se estaría llevando a cabo con una «**versión modificada recientemente**» del virus informático Petia.

En un comunicado, el **banco central de Ucrania** ha asegurado que «informó a los bancos y otros agentes del mercado financiero de un ataque informático externo este lunes contra bancos de Ucrania y empresas públicas y comerciales». A raíz de estos ataques, «los bancos tienen dificultades para mantener a sus clientes y hacer su trabajo», ha dicho el NBU.

«Todos los participantes en el mercado financiero han tomado medidas para fortalecer la seguridad y contrarrestar estos ataques cibernéticos», ha dicho la NBU, que «no tiene ninguna duda de que la infraestructura bancaria sabe defenderse» de este «malware». Varios bancos han confirmado un ataque informático contra de sus servicios. La entidad financiera **Oschadbank** ha dicho en un comunicado «se ve obligado a recurrir a los servicios limitados para sus clientes». El sitio web oficial y, con la excepción de uno, de los paneles del **Aeropuerto Internacional de Boryspil**, Kiev, asegura que «ya no funcionan», según ha declarado la dirección del aeropuerto en su página de Facebook, agregando que debido a estas deficiencias, los vuelos pueden retrasarse.