Departamento de Seguridad Informática MINSAP

Junio 2017

Volumen 1, nº 1

Boletín de Seguridad Informática

Contenido:

Puntos de interés especial:

-Los ciberataques han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. .

-Desde que surgieron los primeros exámenes de **WannaCry** se empezó a sospechar sobre los posibles vínculos de este malware con el polémico régimen de Corea del Norte.

-Este jueves entra en vigor la nueva y polémica ley sobre ciberseguridad en China, entre quejas de las empresas extranjeras acerca de posibles limitaciones a su capacidad de negocio en el país

Los ciberataques a infraestructuras estratégicas se multiplican por siete en solo dos años

Los ciberataques a las infraestructuras extracríticas de España —centrales eléctricas y nucleares, plantas de agua, aeropuertos y hospitales, entre otras— no paran de aumentar. A un ritmo mayor del previsto por el Gobierno. Según los datos del Instituto Nacional de Ciberseguridad (Incibe), las ofensivas a través de la red contra los operadores de estas instalaciones se han multiplicado por siete en solo dos años. Han pasado de 63 en 2014, a 134 en 2015 y a 479 en 2016. Y, además, en el primer cuatrimestre de 2017 se han registrado 247, por lo que de seguir así se superarán los 700 incidentes este ejercicio y se batirá otro récord.

En este acristalado edificio de cuatro plantas, a las afueras de León, la primera alerta saltó a las nueve y cuarto de la mañana. "Nos enteramos, de manera oficiosa, de que algo estaba ocurriendo en Telefónica", explica Marcos Gómez, subdirector del Incibe, al recordar el pasado 12 de mayo, cuando el virus WannaCry desató una alarma mundial. Más de 350.000 operadores —empresas, particulares y administraciones— de 180 países se vieron afectados por un *ransomware* (cibersecuestro) que encriptaba los documentos de los equipos y pedía un rescate a cambio de descifrarlos. Entre los objetivos, además de la compañía española de telecomunicaciones, se encontraban 16 hospitales británicos, que quedaron totalmente paralizados. Estas infraestructuras estratégicas, denominadas en el argot como "críticas", se vieron obligadas a suspender su actividad y a desviar a sus pacientes de urgencias a otros centros, evidenciando el peligro que entraña un ciberataque de estas características.

Aunque ninguno adquirió una trascendencia similar al del Reino Unido, en España se han descubierto cerca de un millar de ofensivas contra operadores de instalaciones críticas en apenas tres años, según los datos del Incibe. La mayor parte, a infraestructuras energéticas. Una cifra al alza, que evidencia los retos de seguridad a los que se enfrenta el país. "Las amenazas que encontramos en el mundo real, como el espionaje, terrorismo o extorsión; ahora son también ciberamenazas. Y las motivaciones son las mismas que antes", dice Alberto Hernández, director general del Incibe.

El ministro de Interior, Juan Ignacio Zoido, lo advertía también el pasado diciembre en una comparecencia en el Congreso: "La gravedad [de este problema], de potenciales consecuencias, entre ellas la pérdida de vidas humanas, amén de severos daños económicos y de trastornos de todo tipo que puede provocar un evento de esta envergadura, justifica con creces que para el Gobierno sea una de nuestras prioridades en materia de seguridad".

Los ciberataques a infraestructuras se multiplican por siete en solo dos años.

Los virus, los troyanos (*software* malicioso que permite el acceso remoto desde otro equipo) y los *spyware* (programas espía) son la amenaza más común. También destacan los accesos no autorizados; y los ataques de denegación de servicio (DoS), que provocan que una plataforma sea inaccesible para sus usuarios. "La protección de las infraestructuras críticas está vinculada cada vez más a una dimensión

digital, de cuya protección depende cada vez más nuestra seguridad", señala el último informe de Seguridad Nacional del Ejecutivo.

Toda esta batería de incidencias que, según las previsiones, marcará este 2017 un nuevo récord. Pero Hernández matiza esta continua subida. "Para explicarla, debemos conjugar tres factores. Es cierto que están sucediendo más ataques. Pero también tenemos mejores capacidades para detectarlos y, a su vez, los afectados nos las están notificando más", detalla el máximo responsable del Instituto nacional de Ciberseguridad, sentado en un despacho de la cuarta planta. Desde esta habitación y a través de un cristal, se observa la sala de la tercera donde trabaja el equipo de detección de ciberataques. En una gran pantalla, un mapa de España muestra en tiempo real el número de equipos comprometidos en el país —de todo tipo: ciudadanos, compañías e infraestructuras críticas— y su localización. A las seis de la tarde del martes, Madrid destaca con 9.715 IP en peligro. Le siguen Barcelona, con 5.276; y Sevilla, con 1.529. El nivel de alerta nacional es del 29%. Muy lejos del 72% que se alcanzó durante la crisis de WannaCry.

Los fraudes electrónicos

El lenguaje que usan los técnicos del Incibe recuerda al policial. Hablan de rastrear la web en busca de "movimientos" sospechosos y de "declaraciones" de *hackers* que desvelen amenazas; de los "cebos" que colocan a los "malos"; y de las "muestras" de virus que analizan para comprender su funcionamiento y combatirlos. Porque su actividad no se limita a las infraestructuras críticas. En 2016, aquí se contabilizaron más de 115.000 ciberataques a ciudadanos, universidades, empresas e instituciones. Esa cifra se duplicó respecto a 2015, cuando se registraron 60.400. En el primer cuatrimestre de 2017, sumaron más de 50.000.

En este contexto general, las amenazas más habituales son los *bots* (programas que infectan equipos para que pueda controlarlos un hacker), los *ramsonware* y los delitos de fraude electrónico e intento de robo de credenciales personales (tarjetas bancarias y cuentas de correo), entre otros. Hasta los equipos del Congreso los han sufrido, según confirman fuentes parlamentarias. Aunque estos ataques no causan excesiva preocupación en los expertos. Su pesadilla es otra.

Es el 23 de diciembre de 2015 la fecha que está marcada en rojo en el sector de la ciberseguridad. Ese día, por primera vez en la historia, un ataque informático provocó un corte de suministro eléctrico masivo. Durante horas, el troyano BlackEnergy tumbó la red que abastecía a 600.000 hogares de la región de Ivano-Frankivsk, al sureste de Ucrania. En pleno invierno. Un ejemplo que usó Zoido en el Parlamento para aseverar que el terrorismo y el crimen organizado "tienen capacidad para causar daños catastróficos". Y un suceso al que también se refiere Hernández: "Las infraestructuras críticas, al igual que se protegen de ataques físicos, también hay que hacerlo de los ciberataques. Aquí juegan un papel muy importante los dueños de estas instalaciones; que deberán tomar medidas para combatir estas amenazas. Igual que contratan vigilantes de seguridad".

El soplo que permitió preparar la ofensiva contra WannaCry

"El mundo de la ciberseguridad, al final, es muy pequeño", destaca Marcos Gómez, pasada ya una semana desde el "frenético" viernes en que WannaCry irrumpió en su vida. Una “larga” jornada que se complicó a las 9.15 horas, cuando saltó la primera alerta en el Incibe. No fue una llamada oficial. Fue un soplo. "Alguien nos comentó que algo pasaba en Telefónica", apostilla el subdirector del Instituto Nacional de Ciberseguridad, que comenzó a trabajar de inmediato. El equipo de detección de incidentes inició un rastreo de la red en busca de pistas: movimientos o declaraciones de intenciones de *hackers* en los días previos. A las 11.15, la compañía de telecomunicaciones les confirmó oficialmente el ataque.

"Contactamos con otros centros de seguridad y también con operadores similares a Telefónica para saber si les estaba ocurriendo lo mismo", apostilla Gómez. Enviaron ya las primeras recomendaciones para frenar el avance del *ransomware*. Y sobre las 12.30 se envió el informe interno a los operadores con los primeros análisis. También se elaboraron documentos ejecutivos para la Secretaría de Estado y para el Ministerio de Industria, del que depende el Incibe. Eran los primeros pasos de un trabajo que duraría días.

El negocio de la ciberdelincuencia

El negocio de la ciberseguridad mueve más de 76.000 millones de euros al año en el mundo, según el director general del Incibe, que recalca que los ciberataques generan más de un billón en pérdidas. El Instituto Nacional de Ciberseguridad ha identificado en España casos de cibersecuestros que piden como rescate desde 300 a 3.000 euros.

El National Cyber Security Centre confirma el origen norcoreano de WannaCry

Desde que surgieron los primeros exámenes de **WannaCry** se empezó a sospechar sobre los posibles vínculos de este malware con el polémico régimen de Corea del Norte.

Sin embargo, por entonces todavía quedaban muchos cabos sueltos por atar para determinar quién era el verdadero responsable de WannaCry. Han sido oficiales del National Cyber Security Centre (NCSC) de Reino Unido los que, tras examinarlo minuciosamente, se han visto en condiciones para **confirmar que el temido ransomware tiene su origen en Corea del Norte**, apuntando concretamente al grupo de hackers **Lazarus**, que presuntamente trabaja para el régimen de ese país.

La NHS, servicio público de salud del Reino Unido, fue uno de los primeros entes conocidos afectados por WannaCry, del cual se pensó en un principio que era un ataque dirigido a empresas e instituciones concretas. Pero ahora se sabe que el ataque no fue ni mucho menos dirigido, sino que fue indiscriminado, o que incluso a los atacantes se les pudo ir de las manos.

Lazarus fue el grupo de hackers encargado del brutal ataque contra Sony Pictures en 2014, el cual provocó grandes daños y pérdidas a la productora y que fue motivado sobre todo por la película The Interview, una comedia que resulta una crítica explícita al régimen de Corea del Norte y a la figura de Kim Jong-Un. Aunque muchos señalan que Lazarus trabaja para el gobierno norcoreano, nadie es capaz de afirmar esto en firme debido a que no hay pruebas contundentes de que eso sea verdad.

Para llegar a la conclusión de vincular WannaCry con Lazarus, se ha **encontrado código en el ransomware que coinciden tanto en la base como en los autores** con el empleado en otros malware creados por el mismo grupo de hackers.

La polémica ley de ciberseguridad entra en vigor en China

Este jueves entra en vigor la nueva y polémica ley sobre ciberseguridad en China, entre quejas de las empresas extranjeras acerca de posibles limitaciones a su capacidad de negocio en el país y promesas de Pekín de que no trata de restringir la libre competencia. La medida, que el Legislativo aprobó el pasado noviembre, busca, según las autoridades del país, proteger la privacidad de los datos e y reducir la vulnerabilidad a ataques como el del virus WannaCry que afectó a centenares de miles de sistemas informáticos en todo el mundo.

"No hay seguridad nacional sin ciberseguridad", ha dicho el presidente chino, Xi Jinping, en una muestra de la importancia que Pekín atribuye a la medida. Desde la llegada de Xi al poder, el régimen chino ha incrementado la censura y el control sobre Internet, ha reclamado la soberanía nacional en el ciberespacio y ha puesto en marcha una serie de regulaciones sobre las empresas tecnológicas.

El objetivo de la nueva ley es, según la Administración del Ciberespacio de China (CAC), "salvaguardar la soberanía en el ciberespacio, la seguridad nacional y el interés público, así como los derechos y los intereses de los ciudadanos". Una meta que la hace tan amplia como vaga, y por tanto complicada de cumplir, señalan sus críticos. Aunque oficialmente entrará en vigor este jueves, Pekín tiene dos años para ir poniendo en marcha sus distintos elementos clave. Entre otros aspectos positivos, la nueva ley regula la protección de datos, hasta ahora una zona gris en China. Los proveedores de servicios de Internet no podrán recabar y vender sin autorización la información personal de sus usuarios, y sus clientes podrán exigir que se borren sus datos en caso de abuso. Pero también prohíbe que los usuarios de Internet puedan publicar contenido que perjudique "el honor nacional" o del que se sospeche que pueda intentar "deponer el sistema socialista" o la alteración del orden social y económico vigente.

Otras provisiones han suscitado también el escepticismo, o directamente la preocupación de analistas y empresas extranjeras que habían solicitado el aplazamiento de la entrada en vigor de la medida hasta que se aclarasen algunos de sus puntos más polémicos. En su opinión, partes de la ley amenazan con excluir a firmas foráneas de sectores que Pekín define como "clave" pero que no están claramente delimitados.

"La ley debería ser proporcional, consistente, no discriminatoria y transparente, y no vemos que cumpla esos requisitos, al menos desde fuera", sostenía este miércoles en un acto público Mats Harborn, presidente de la Cámara de Comercio Europea en China, una de las organizaciones que ha criticado la norma con mayor dureza. Michael Chang, el número dos de esta entidad, ha advertido por su parte del "enorme coste y dificultad de cumplimiento" para las empresas.

Las cláusulas de la ley prevén revisiones de seguridad periódicas para los productos de aquellas empresas autorizadas a operar en sectores "clave". Entre estos, se enumeran específicamente áreas como la energía, las finanzas o los servicios públicos, pero también "cualquier otra infraestructura de información clave que pueda causar graves daños a la seguridad nacional, la economía o el interés público si se destruyeran, quedaran inutilizadas o se filtraran". Es decir, casi cualquier sector puede entenderse como "clave".

No está claro si, en estas revisiones de seguridad, las empresas tendrán que revelar a las autoridades chinas los códigos fuente de sus programas u otros datos altamente confidenciales, algo que ha hecho saltar las alarmas sobre la posibilidad de espionaje industrial o de robo de la propiedad intelectual.

Además**,** las empresas —tanto nacionales como extranjeras— tendrán que almacenar los datos obtenidos en China en servidores que se encuentren en territorio de este país. Para trasladar al exterior datos que impliquen a más de un millón y medio de personas será necesario someterse a una revisión de seguridad.

La relación que establece Xi entre la seguridad nacional y la ciberseguridad "refleja una visión ampliamente aceptada en China", ha apuntado en un reciente análisis Nabil Alsabah, del centro de estudios alemán MERICS. "La dirección que están adoptando los líderes chinos está clara: regular estrictamente tecnologías extranjeras en las que no se puede confiar y esforzarse por desarrollar sustitutos nacionales".

Un grupo de hackers está explotando SambaCry para minar ordenadores Linux

A finales del mes pasado cubrimos el caso de **SambaCry**, una vulnerabilidad descubierta en versiones recientes de Samba (implementación libre de los protocolos SMB y CIFS) que dejaba la puerta abierta hasta al control remoto del sistema afectado en caso de ser explotada por un hacker habilidoso.

Aunque la comunidad de Samba reaccionó a gran velocidad para **parchear la vulnerabilidad, su aplicación depende del usuario final**, lo que abre la puerta a su explotación por parte de los hackers. El número de ordenadores afectados por este problema ha ido en aumento y ha alcanzado los 458.000. Además, investigadores avisan que la vulnerabilidad ha abierto la puerta a la creación de mecanismos de difusión similares a los empleados por WannaCry, el ransomware que causó estragos a nivel mundial hace un mes.

La compañía de ciberseguridad rusa Kaspersky Lab ha detectado una campaña de malware para explotar SambaCry, la cual infecta ordenadores Linux con software de minado de criptodivisas (como Bitcoin). Omri Ben Bassat, investigador en seguridad de Intezer, decidió poner a esta campaña el nombre de **EternalMiner**.

Según los investigadores, un grupo de hackers todavía sin identificar ha empezado a **secuestrar ordenadores Linux** solo una semana después de destaparse el caso de SambaCry para **instalar una versión reciente de CPUminer**, un software de minado de criptodivisas que está siendo usado para la divisa Monero en este caso.

Después de comprometer un ordenador Linux a través de la explotación de SambaCry, los atacantes ejecutan dos cargas en el sistema:

- INAebsGB.so: Una shell invertida que ofrece acceso remoto a los atacantes.
- cblRWuoCc.so: Una puerta trasera que incluye utilidades de minado de criptodivisas, como CPUminer.

El minado de criptodivisas puede requerir de una gran inversión y una elevada potencia de computación, por eso los cibercrminales utilizan malware para hacerse con computadoras ajenas y obtener así beneficios.

Los cibercriminales han ganado hasta el momento 98 XMR a través de la explotación de SambaCry, lo que vendrían a ser unos 5.380 dólares.

Ubuntu 17.10 mejorará el soporte de Secure Boot para arrancar Windows desde GRUB

Ubuntu es un sistema operativo en constante desarrollo. A pesar de lanzar cada dos años una versión LTS con 5 años de soporte (siendo estas las recomendadas para los usuarios finales), cada seis meses nos encontramos con un nuevo lanzamiento de esta popular distribución Linux.

Para **Ubuntu 17.10** llegarán grandes cambios al sistema, destacando la vuelta de la interfaz gráfica GNOME en su versión 3. Sin embargo, esta no va a ser la única novedad de calado, ya que **la carga de cadena de Secure Boot está siendo mejorada para arrancar Windows correctamente desde el gestor de arranque GRUB**. Otros parches que van a ser añadidos harán que los usuarios no tengan que inhabilitar Secure Boot cuando usen módulos DKMS.

Los desarrolladores de Ubuntu también están trabajando para añadir algunas características como la habilitación por defecto del soporte para PIE (Position Independent Executables) en las arquitectura i386, armhf y arm64. Esto hará que los **binarios habilitados por PIE se carguen automáticamente en ubicaciones aleatorias en la memoria virtual**, junto con todas sus dependencias, cada vez que las respectivas aplicaciones son ejecutadas, volviendo así más difícil la ejecución de ataques ROP (Return Oriented Programming).

Otro cambio importante que llegará con Ubuntu 17.10 será la utilización de Netplan para la configuración de redes cuando se instale la versión Server de esta distribución a través del instalador de Debian (distribución madre de Ubuntu).