novática
Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*), representa a España en **IFIP** (*International Federation for Information Processing*) y es miembro de **CLEI** (*Centro Latinoamericano de Estudios de Informática*) y de **CECUA** (*Confederation of European Computer User Associations*). Asimismo tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*) y colabora con diversas asociaciones informáticas españolas.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Gutierre de Cetina 24, 28017 Madrid •Tlfn.914029391 <novatica@ati.es>
Administración y Redacción ATI Cataluña
Calle Ávila 50, 3a planta, local 9, 08005 Barcelona
Tlfn.934125235 <secregen@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <novatica.subscripciones@atinet.es>
Publicidad Gutierre de Cetina 24, 28017 Madrid
Tlnf.914029391 <novatica@ati.es>
Imprenta: Impresión Offset Derra S.L., Llull 41, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: "El guardián" - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

sumario

Nº 238, noviembre 2016 - febrero 2017, año XLII

Monografía del próximo número: "Salud y tecnología"

La nueva "*3l1t3*"mediática

Mª José de la Calle
Cofundadora y Directora de Comunicación y Analista Senior del 'think tank' *español Instituto de Tendencias en Tecnología e Innovación (iTTi)*

<mjdelacalle@ittrendsinstitute.org>

Resumen: *A lo largo del artículo, la autora reconoce y traslada el mensaje de que la seguridad digital ha alcanzado su mayoría de edad: las noticias sobre incidentes de naturaleza cibernética, y sus causas, abren hoy los telediarios. Ello aporta una visibilidad, nunca imaginada, sobre una materia como ésta, tradicionalmente exclusiva de cierto ámbito profesional. La nueva audiencia ampliada, constituida por ciudadanos, empresas (y sus empleados) y administraciones (y sus funcionarios), consigue, de este modo, familiarizarse con una serie de elementos (vulnerabilidades y amenazas) y actores (individuos, bandas organizadas y estados) que, como consecuencia, conforman una suerte de nueva élite (3l1t3, en escritura "leet") mediática. Con la excusa de contribuir, también ella, a la divulgación de estos conceptos entre la referida audiencia, la autora hace un repaso de algunas de las amenazas para la seguridad digital más representativas del panorama actual, explicándolas a través de ejemplos y casos reales. Finalmente, se plantea provocadoramente la cuestión de la viabilidad de atajar estos problemas; apuntándose, como una de las soluciones clave, a la necesidad de abordar la seguridad digital desde las etapas más tempranas del diseño de productos y servicios.*

Palabras clave: *calidad, datos personales, DDoS, fiabilidad, funcionalidad, gratuidad, inseguridad digital,* ransomware*, seguridad desde el diseño, seguridad digital.*

Autora

Mª José de la Calle es cofundadora, Directora de Comunicación y Analista Senior del '*think tank*' español Instituto de Tendencias en Tecnología e Innovación (iTTi). Con una experiencia de casi tres décadas en consultoría tecnológica, es una perfecta conocedora de las problemáticas ligadas al papel de la función informática en el seno de las organizaciones. Físico de formación y de corazón, muestra la misma pasión en su intención por hacer llegar el mensaje de la responsabilidad sobre *lo digital* a quienes componen los consejos de administración y otros órganos de gobierno de organizaciones públicas y privadas. En ello refleja, también, su experiencia como miembro de alguno de dichos órganos en entidades sin ánimo de lucro. Escribe regularmente sobre seguridad y tecnologías digitales en diferentes medios y revistas, como lo ha hecho para Novática anteriormente.

1. Contexto

Desde hace algunos años se ha empujado a la sociedad a un empleo masivo (acaso abusivo) de las tecnologías de la información, tanto para un uso personal como laboral. Objetivo que, a la vista está, se ha conseguido con creces[1].

Este uso masivo ha venido acompañado de una gran y creciente inseguridad en los datos y en la información que manejan los dispositivos digitales, que afecta no sólo a la marcha de los negocios y a la intimidad de las personas, sino a la propia integridad física de unos y otras, al haberse encomendado a los algoritmos parte del control de los procesos del mundo real y de las actividades de la vida diaria [2].

El problema de la inseguridad en el mundo virtual se conoce desde los inicios de la Informática. Ya en 1949, Von Neumann habló por primera vez de programas auto-replicantes y unos años después, en la década de los sesenta, verían la luz los primitivos predecesores de los actuales *virus* de naturaleza software [20]. Desde entonces, todo apunta a que no se ha sabido hacer las cosas mucho mejor. Reiteradamente ha primado la presión del *time-to-market* y, en lugar de producirse la evolución/revolución digital con una razonable seguridad, las prisas por situar nuevos productos en el mercado han llevado a ponderar, por encima de cualquier otro aspecto, su funcionalidad. Unos productos que, carentes de la debida calidad (y consiguiente seguridad; aunque sobrados de funciones), habitualmente han tenido que arreglarse (parchearse), a posteriori.

Peor aún, esa falta de seguridad innata ha venido acompañada de una *exigencia* que obliga al propio usuario a responsabilizase de mantener sus equipos seguros (para lo que se le ha venido dirigiendo una gran cantidad de advertencias y consejos sobre lo que debe hacer o lo que ha de evitar).

Tal enfoque, aun carente de toda lógica, parece haberse interiorizado. Y procedimentado: 1) vender productos defectuosos; 2) asignar al comprador la responsabilidad de utilizarlos correctamente para padecer los mínimos fallos; y, 3) al mismo tiempo, producir y comunicar (el fabricante) mejoras y parches.

No se trata de un tema tecnológico. Es una cuestión de moral y disciplina de mercado; de madurez del consumidor, quien debe despertar del ensueño inducido de productos buenos, seguros, gratis (o muy baratos), y sin otras contrapartidas.

Los ciberdelincuentes no son más listos que los desarrolladores de esos productos, no vienen de otro planeta. Y además, supuestamente, los desarrolladores pueden/deben conocer mejor que nadie dichos productos. ¡Son suyos! Por tanto, si, como parece evidente, disponen de la capacidad para arreglarlos después, ¡por favor, háganlo antes!

Como se ha dicho, lo que se está viendo es una carrera por sacar al mercado el producto antes que la competencia. Un gran plan para convertir a la ingente masa de usuarios/clientes (algunas empresas los cuentan, hoy, por miles de millones) en su departamento de calidad. ¡Y, encima, gratis! (O, siendo más precisos, con costes encubiertos para los propios usuarios/clientes, cual puede ser tener que hacer entrega de sus datos personales).

Hay en todo ello un trasfondo de regulación y voluntad política. Ambas escasas, dado que los propios gobiernos se benefician (cuando no las promueven), de las vulnerabilidades intrínsecas a las tecnologías digitales, para fines diversos, entre los que gozan de una posición de privilegio los de naturaleza militar y los de vigilancia/espionaje.

2. Nuevas celebridades: la jet set digital

Diariamente, la prensa generalista muestra, junto a noticias y comentarios sobre personajes políticos, futbolistas, artistas y otros protagonistas de la crónica informativa y social, términos que, hasta hace bien poco, nadie había visto (nadie habría imaginado ver) fuera de determinados ámbitos estrictamente profesionales. Hoy las menciones a anglicismos y/o neologismos relacionados con *lo digital* (algunos tan nuevos que aún no se tiene, apenas, referencia de ellos)

> “ El colectivo ciudadano es, precisamente, el que se muestra más expuesto ante las consecuencias de la inseguridad digital ”

como *ransomware*, *DDoS*, u otros, aparecen con regularidad en los titulares de noticias en televisión, en páginas web y en otros medios.

Muchos de dichos titulares juegan con la baza de contar con una audiencia entregada, por tratarse de noticias que se antojan propias de la crónica rosa y de la órbita de los paparazzi. Ejemplos de ello pueden ser casos como el del robo de fotografías comprometedoras de famosas, albergadas en la nube de Apple [5], o el de los ataques a páginas de contactos, como el portal AshleyMadison.com [15]. Otros están cargados de lecciones que deberían contribuir a que la opinión pública tomase conciencia de la ciberdebilidad (como efecto de la ciberdependencia) de la sociedad actual y de su estado del bienestar. Al menos, es el efecto pedagógico que debería tener el dar a conocer cómo más de doscientas mil personas se quedaron sin suministro eléctrico, hace poco más de un año, en Ucrania [21], tras un ciberataque. La revelación de los contenidos de mensajes de correo electrónico relacionados con la campaña de la candidata Clinton [24] y sus aparentes efectos sobre los resultados electorales en EE.UU., el pasado noviembre, deberían provocar, igualmente, más de una reflexión sobre lo *ciber-influenciable* que pueden llegar a ser las sociedades más conectadas.

En definitiva, se trata en todos los casos de sucesos que, independientemente del contexto en el que se producen, adquieren cada vez una mayor visibilidad y una mayor presencia mediática, por cuanto afectan, de forma creciente, al buen nombre, a la actividad y a la vida cotidiana de instituciones, empresas y ciudadanos en general.

Parece tratarse de una suerte de jet set digital que ensombrece al *establishment* y a la jet set tradicional. Es la nueva élite mediática.

El colectivo ciudadano es, precisamente, el que se muestra más expuesto ante las consecuencias de la inseguridad digital. La revelación de los datos médicos personales que cualquiera había confiado a su centro sanitario; la de la deuda contraída con determinada entidad, cuyas bases de datos se han podido ver comprometidas; o la aparentemente más inocente publicación, en la cuenta de Instagram de un antiguo compañero de universidad, de determinadas fotografías tomadas, entonces, tras una noche en la que compartieron algunas cervezas de más, son reflejo de la referida exposición.

Ventajas de *lo digital* como la disponibilidad, a precios cada vez más asequibles, de los más variopintos dispositivos de almacenamiento o la facilidad de replicación, con impecable exactitud, de la información en formato electrónico, convierten la *huella digital* de cualquier individuo (el detallado rastro de sus acciones en Internet) en imborrable. Y ello, más allá del *derecho al olvido* con cuya invocación ese mismo individuo puede demandar de los buscadores la retirada de las pistas de su paso por Internet. ¡Una batalla perdida! En esta coyuntura, situaciones como las descritas en el párrafo anterior pueden jugar a la contra ante la solicitud de un préstamo, la posibilidad de un nuevo contrato de trabajo, etc., en tanto que aquellas circunstancias pasadas (quizás ya olvidadas por sus protagonistas), pueden cobrar una actualidad no deseada y tener unas consecuencias de pesadilla para los interesados.

Los fallos de seguridad, naturalmente, afectan también a las organizaciones (empresas e instituciones), que pueden ver deterioradas sus cuentas y su imagen pública como resultado de cualquier incidente que suponga revelación no autorizada de su información, interrupción de sus operaciones o servicios, etc.

Los actores que se encuentran tras ese tipo de incidentes tienen perfiles y nombres muy diversos. Hasta cierto punto, hoy la figura del ciberdelincuente solitario parece un rastro del pasado. Es cierto que la actual disponibilidad y facilidad de uso de multitud de herramientas ciberofensivas permiten hablar de *ejércitos de un solo hombre*; pero no lo es menos que la imagen (en ocasiones, idílica) del atacante autónomo, hoy, deja paso, por una cuestión de eficacia y rentabilidad, a grupos más numerosos, organizados y jerarquizados. Se trata de bandas delictivas en toda regla, cuando no estructuras al servicio directo de estados soberanos o pseudo-soberanos (piense en los esfuerzos que dedica Daesh a su promoción y a sus acciones en el ciberespacio [18]).

Y al igual que los actores, también sus motivaciones y objetivos son diversos, desde el clásico incentivo económico (hoy, por ejemplo, el espionaje industrial resulta inconcebible sin el apoyo de *lo digital*), pasando por el ideológico (el citado ciberterrorismo de Daesh puede ser un inmejorable ejemplo), hasta el político en el que son los estados soberanos, sus gobiernos, quienes explotan las posibilidades del ciberespacio para vigilar a sus propios ciudadanos, para materializar sus estrategias geo-políticas o, simplemente, para abortar las de sus adversarios (en 2010 las pretensiones nucleares iraníes se vieron seriamente afectadas por los efectos de una ofensiva cibernética).

La atención que se ha prestado a Stuxnet, nombre dado al código informático dañino empleado contra el programa nuclear iraní, no sólo ha servido para conocer la complejidad que pueden llegar a alcanzar los ciberataques, habitualmente, ejecutados por fases (recogida previa de información, acceso al sistema objetivo, introducción del código dañino que permitirá, posteriormente, obtener el control remoto del citado sistema, ataque propiamente dicho, etc.), sino que también ha permitido evidenciar el posicionamiento mediático que las amenazas cibernéticas son capaces de alcanzar. En el caso de Stuxnet, su supuesta condición de *primera ciberarma de la Historia* le ha permitido venir copando portadas y titulares desde entonces [11] [14].

Como ocurrió con Stuxnet, actualmente son otras las amenazas que han logrado colarse entre la ciberélite mediática: el *ransomware*, los ataques DDoS o las *botnet* son destacados ejemplos.

3. *Ransomware*, la estrella del momento

Esta forma de código informático dañino que *secuestra* los datos de los sistemas que infecta, los cifra, dejándolos inaccesibles, para liberarlos posteriormente sólo previo pago de un rescate (*ransom*, en inglés) no es nueva; no obstante, en los últimos años, está adquiriendo una enorme relevancia: entre septiembre de 2013 y junio de 2014 el virus CryptoLocker infectó alrededor de medio millón de ordenadores en todo el mundo, afectando, entre otras entidades a la NASA y al Departamento de Sanidad y Servicios

> “El *ransomware* se ha extendido a todo tipo de víctimas, desde el usuario residencial a las redes corporativas, desde la microempresa a las grandes corporaciones, sin olvidar las entidades del sector público”

Sociales de los EE.UU. (HSS, por sus siglas en inglés) [16].

El *ransomware* se ha extendido a todo tipo de víctimas, desde el usuario residencial a las redes corporativas, desde la microempresa a las grandes corporaciones, sin olvidar las entidades del sector público [8].

En el caso de los dispositivos personales y domésticos, un informe de TrendMicro publicado el pasado mes de enero [26] describía cómo un televisor inteligente LG había sido infectado por una variante del virus *Flocker* creado para el sistema operativo Android y descubierto en mayo de 2015.

El 29 de septiembre de ese mismo año [12], Google anunciaba que había mil cuatrocientos millones de dispositivos Android (de propósito, tanto personal, como profesional) activos en el mundo; mil cuatrocientos millones de dispositivos susceptibles de ser atacados.

De hecho, en el ámbito corporativo las noticias sobre este tipo de ciberataques también han ocupado permanentemente los titulares durante todo 2016. Así, en marzo, un artículo de la BBC daba a conocer que tres hospitales de EE.UU. habían sido extorsionados en los dos primeros meses del año [3].

En suma, el alcance y el crecimiento que está experimentando el *ransomware* hacen de él la ciberamenaza estrella del momento actual. El reciente *Informe Anual de Amenazas 2017* de SonicWall habla de *crecimiento explosivo* en la distribución de *ransomware* [4], lo que la convierte, posiblemente, en el segmento de mayor crecimiento de la ciberdelincuencia. Concretamente, las cifras indican que este tipo de ataques crecieron 167 veces en un año, desde los 3,8 millones en 2015 a los 638 millones en 2016. El informe apunta, como causa de ese crecimiento, a una confluencia de factores como la aparición del *ransomware-como-servicio* (RaaS) y la normalización/popularización del acceso al Bitcoin.

Es, nuevamente, TrendMicro quien señala que el modelo de negocio RaaS permite a los creadores de este tipo de código nocivo ganar dinero con él, apoyándose en redes de distribuidores, los cuales no requieren, apenas, conocimientos técnicos [25]. Por tanto, cualquiera que pretenda hacer dinero rápido a costa de terceros (individuos, empresas u otras entidades) no tendrá más que contratar este servicio.

4. DDoS y *botnet*, coprotagonistas

El ampliamente divulgado (aquel día abrió los telediarios) ataque de denegación distribuida de servicio (del inglés “*Distributed Denial of Service*”, DDoS) que tuvo lugar el pasado 21 de octubre de 2016 sobre la empresa estadounidense Dyn no buscó dañar un dominio o sitio web específicos [22].

Dyn administra un servicio de traducción de nombres de dominio (direcciones de Internet en formato alfanumérico, como las habituales *.com*, por ejemplo), convirtiéndolos a un nuevo formato cuasi-numérico denominado dirección IP (éstas actúan como identificadores de los ordenadores conectados a Internet), facilitando la comunicación, esto es, la transmisión de paquetes de datos, entre unos ordenadores y otros. Por tanto, cualquier acción de sabotaje sobre el sistema a cargo de esa traducción/casación de nombres-direcciones truncará, no sólo su operativa normal, sino el acceso a cuantos dominios cuyos nombres no hayan podido ser traducidos. Todo esto constituye, sin duda, un paso hacia un nuevo nivel en la productividad de los ataques.

En el caso del ataque a Dyn las páginas web de numerosas empresas, entre ellas algunas de las más relevantes empresas de Internet (Netflix, PayPal, Sony PlayStation, Twitter, …), quedaron inaccesibles durante horas, como si se hubiera ejecutado un ataque particular sobre cada una de ellas de forma independiente.

El éxito de los ataques DDoS se basa en la capacidad del atacante para colapsar los servidores atacados (afectando a su ancho de banda) de forma que éstos no puedan seguir dando respuesta a las solicitudes/peticiones que reciben desde otros nodos o dispositivos. Cuanto más ancho de banda haya disponible, más peticiones simultáneas se requerirán; o, lo que es lo mismo, más dispositivos lanzándolas.

Esto último no parece constituir, hoy, un reto infranqueable. La existencia de multitud (miles de millones) de dispositivos conectados a Internet y débilmente protegidos frente a posibles intrusiones, favorece un escenario en el que hacerse con el control de tales dispositivos, no será sino una primera fase antes de utilizarlos para el lanzamiento, sobre el sistema que se pretende colapsar, de un número de peticiones lo suficientemente elevado como para que se llegue con holgura a los niveles pretendidos de saturación.

Ese escenario es el que ofrece la llamada *Internet de las Cosas* (IoT, por sus siglas en inglés), paradigma bajo el cual todo tipo de *máquinas* conectadas a Internet (cámaras de tráfico o de vigilancia, dispositivos vigila-bebés, termostatos, encaminadores, televisores, frigoríficos, relojes y pulseras que miden pulsaciones, el ritmo cardíaco y/o la calidad del sueño, contadores de luz, agua o gas, etc.), son capaces de comunicarse entre sí, a menudo de forma autónoma.

Con el oportuno software de control, ese comportamiento autónomo, podría moldearse, reorientando la voluntad de las máquinas hasta convertirlas en una suerte de red de autómatas, o red de zombis (*botnet* en la bibliografía inglesa), que lanzase peticiones al servidor objetivo, con el fin de colapsarlo. En el *Caso Dyn*, con ayuda del software nocivo *Mirai*, se logró alcanzar una tasa de peticiones del orden de 1,2 terabits de información por segundo.

Mirai ya había saltado a las portadas el mes anterior, cuando fue utilizado para atacar la página del periodista y divulgador de la seguridad digital, Brian Krebs[2]. En el *Caso Krebs* unos 380.000 dispositivos, *a las órdenes de Mirai*, lograron colapsar el servidor enviándole peticiones, a razón de 665 Gbits/seg.

Poco después del ataque a Krebs, se publicaría el código fuente de *Mirai* [7], provocando que el número de *botnets* aumentara.

El 14 de octubre de 2016, a tan sólo una semana del ataque a Dyn, el Departamento de Seguridad Interior de los EE.UU. había publicado una alerta sobre *Mirai* [9] y sobre los peligros de los ataques DDoS ejecutados por *botnets* compuestas por dispositivos de la IoT. La alerta también preveía posibles ataques futuros.

> “Sí, hay remedio. ¡Debe haberlo! Con el importante matiz de que la seguridad total no existe”

Y así ocurrió. A mediados de noviembre pasado 900.000 clientes de la operadora alemana Deutsche Telecom vieron como su servicio quedaba interrumpido por una variante de *Mirai* introducida en los encaminadores que la compañía tiene distribuidos por los domicilios de sus clientes. Ello se había logrado gracias a una vulnerabilidad en el proceso que permitía a la operadora actualizar remotamente el *firmware* de sus equipos. También en el Reino Unido, la compañía de telefonía TalkTalk sufría la infección de *Mirai* en 2.400 de sus encaminadores. Además, en esos días, se daba a conocer la noticia de que más de ochenta modelos de cámaras Sony eran vulnerables a *Mirai*, pudiéndose tomar el control de ellas [17].

Se trata, por tanto, de un panorama en el que hasta los fabricantes legítimos de hardware/software/firmware quedan en entredicho, cuando sus propios mecanismos de actualización de equipos y dispositivos pierden toda fiabilidad, abriendo la puerta a riesgos de seguridad digital de cualquier tipo.

Por si todo esto no fuera suficiente, de nuevo se trata de servicios que, como se ha indicado para el caso del *ransomware*, se pueden comprar, alquilar o contratar [19] [23] [6].

5. El reto: ¿hay remedio a todo este desastre?

Sí, hay remedio. ¡Debe haberlo! Con el importante matiz de que la seguridad total no existe.

Sí, parece haber un primer remedio en la propia tecnología, en la aplicación de más tecnología. Lo parece porque es el tipo de remedio que más adeptos demuestra tener en el ámbito corporativo: los gastos en seguridad digital en las empresas no hacen más que aumentar. No obstante, no es un remedio que, hasta la fecha, se haya mostrado del todo eficaz (salvo para quienes viven de él, ofreciendo soluciones y servicios de seguridad digital): a pesar de que la inversión, año a año, va a más, los incidentes y sus consecuencias no van a menos. Es lo que el analista Garrett A. Bekker, III, denomina *La Gran Desconexión* [10].

Por tanto, añadir tecnología complementaria o *de subsanación* (se da por sentado que habrá vulnerabilidades y se opta, tanto preventiva, como reactivamente, según el tipo de soluciones que se apliquen, por *subsanarlas* mediante apósitos) no es suficiente.

Frente a esta frustración, una solución que se antoja más eficaz es la de considerar la seguridad como un requisito más de los productos y servicios de naturaleza digital. Todo dispositivo electrónico y cualquier software pueden ser razonablemente seguros. No obstante, por desgracia, no es éste un requisito que suela recogerse en las especificaciones de fabricación/desarrollo. No siempre se contempla la *seguridad desde el diseño*, como ocurre con otras especificaciones funcionales, de rendimiento, etc.

De hecho, la seguridad no sólo debería estar presente en las etapas más tempranas del diseño, debería formar parte de todos los procesos de la organización.

Finalmente, ponerle remedio a la actual situación pasa, necesariamente también, por una mayor exigencia del consumidor a la hora de adquirir productos seguros. Y por la obligación ciudadana de demandar de los representantes políticos legislaciones que obliguen a comercializar productos y servicios digitalmente seguros, dentro de lo razonable; como ocurre con otras seguridades, más tradicionales, en determinados sectores industriales.

Si no se le pone remedio, lo digital podría quedar relegado a su aplicación en actividades poco relevantes, poco críticas. Y a su sustitución en éstas, por mecanismos que, hoy, resultarían estrafalarios. Sirvan como aviso la vuelta a la máquina de escribir del Kremlin [13], ya anunciada en 2013; o el más reciente anuncio del hotel *Romantik Seehotel Jaegerwirt* de sustituir su moderno sistema informático de gestión de apertura y cierre de puertas, basado en el uso de tarjetas, por las más convencionales cerraduras con la llave de toda la vida [1].

Referencias

[1] A. Martí. “Cuando no puedes entrar a tu habitación de cuatro estrellas porque tu hotel ha sufrido un ciberataque”. *Xataka, 20 de enero de 2017.* <https://www.xataka.com/seguridad/cuando-no-puedes-entrar-a-tu-habitacion-de-cuatro-estrellas-porque-tu-hotel-ha-sufrido-un-ciberataque>. Último acceso: 19 de febrero de 2017.

[2] A. Reid. “Here’s how we can protect ourselves from the hidden algorithms that influence our lives”. *The Conversation, 20 de diciembre de 2016.* <https://theconversation.com/heres-how-we-can-protect-ourselves-from-the-hidden-algorithms-that-influence-our-lives-70674>. Último acceso: 16 de febrero de 2017.

[3] BBC. “Three US hospitals hit by ransomware”. *BBC News, 23 de marzo de 2016.* <http://www.bbc.com/news/technology-35880610>. Último acceso: 18 de febrero de 2017.

[4] B. Conner. “SonicWall Annual Threat Report reveals the state of the cybersecurity arms race”. *SonicWall, Blog, 6 de febrero de 2017.* <https://blog.sonicwall.com/2017/02/sonicwall-threat-report-reveals-cybersecurity-arms-race/>. Último acceso: 18 de febrero de 2017.

[5] C. Athur. “Naked celebrity hack: security experts focus on iCloud backup theory”. *The Guardian, 1 de septiembre de 2014.* <https://www.theguardian.com/technology/2014/sep/01/naked-celebrity-hack-icloud-backup-jennifer-lawrence>. Último acceso: 16 de febrero de 2017.

[6] C. Doctorow. “Two hackers are selling DDoS attacks from 400,000 IoT devices infected with the Mirai worm”. *BoingBoing, 28 de noviembre de 2016.* <http://boingboing.net/2016/11/28/two-hackers-are-selling-ddos-a.html>. Último acceso: 19 de febrero de 2017.

[7] C. Osborne. “Source code of Mirai botnet responsible for Krebs On Security DDoS released online”. *ZDnet/ZeroDay, 3 de octubre de 2016.* <http://www.zdnet.com/article/source-code-of-mirai-botnet-responsible-for-krebs-on-security-ddos-released-online/>. Último acceso: 19 de febrero de 2017.

[8] Departamento de Justicia de los EE.UU. “How to protect your networks from ransomware”. *Gobierno de los EE.UU., 2016.* <https://www.justice.gov/criminal-ccips/file/872771/download>. Último acceso: 18 de febrero de 2017.

[9] DHS/US-CERT. “Heightened DDoS Threat Posed by Mirai and Other Botnets”. *Department of Homeland Security/US Computer Emergency Readiness Team. Alert (TA16-288A), 14 de octubre de 2016.* <https://www.us-cert.gov/ncas/alerts/TA16-288A>. Último acceso: 19 de febrero de 2017.

[10] G. A. Bekker. “The 2017 Data Threat Landscape”. *451 Research, 14 de febrero de 2017.* <https://www.youtube.com/watch?v=N1uV9QYsxoI&feature=youtu.be>. Último acceso: 19 de febrero de 2017.

[11] G. Julián. “Stuxnet: historia del primer arma de la ciberguerra”. *Genbeta, 2 de diciembre de 2013.* <https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra>. Último acceso: 18 de febrero de 2017.

[12] J. Callaham. “Google says there are now 1.4 billion active Android devices worldwide”. *Android-Central, 29 de septiembre de 2015.* <http://www.bbc.com/news/technology-35880610>. Último acceso: 18 de febrero de 2017.

> “ Frente a esta frustración, una solución que se antoja más eficaz es la de considerar la seguridad como un requisito más de los productos y servicios de naturaleza digital ”

[13] J. Mendiola. “El Kremlin recupera la máquina de escribir como herramienta de inteligencia”. *El Confidencial, 16 de julio de 2013.* <http://www.elconfidencial.com/tecnologia/2013-07-16/el-kremlin-recupera-la-maquina-de-escribir-como-herramienta-de-inteligencia_766293/>. Último acceso: 19 de febrero de 2017.

[14] K. Zetter. “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon”. *Wired, 3 de noviembre de 2014.* <https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>. Último acceso: 16 de febrero de 2017.

[15] K. Zetter. “Hackers Finally Post Stolen Ashley Madison Data”. *Wired, 18 de agosto de 2015.* <https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/>. Último acceso: 16 de febrero de 2017.

[16] L. Franceschi-Bicchierai. “Even NASA got infected with ‹CryptoLocker› ransomware”. *Motherboard, 5 de junio de 2015.* <https://motherboard.vice.com/en_us/article/even-nasa-got-infected-with-cryptolocker-ransomware>. Último acceso: 18 de febrero de 2017.

[17] L. H. Newman. “The botnet that broke the Internet isn’t going away”. *Wired, 9 de diciembre de 2016.* <https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away/>. Último acceso: 19 de febrero de 2017.

[18] M. Montgomery. “ISIS and the Internet. Turning a tool into a weapon”. *Radio Canada International, 20 de septiembre de 2016.* <http://www.rcinet.ca/en/2016/09/20/isis-and-the-internet-turning-a-tool-into-a-weapon/>. Último acceso: 17 de febrero de 2017.

[19] M. Wilson. “Want to launch your own DDoS attacks? Just buy them from Lizard Squad”. *BetaNews, 2015.* <https://betanews.com/2014/12/31/want-to-launch-your-own-ddos-attacks-just-buy-them-from-lizard-squad/>. Último acceso: 19 de febrero de 2017.

[20] Panda Security Internacional. “(I) Evolution of computer viruses: history of viruses”. *Communication USA. Nota de prensa, 12 de abril de 2004.* <http://www.pandasecurity.com/about/press/viewnews.htm?noticia=4944&entorno=&ver=&pagina=&producto=>. Último acceso: 16 de febrero de 2017.

[21] S. Khandelwal. “Hackers cause world’s first power outage with malware”. *The Hacker News, 5 de enero de 2016.* <http://thehackernews.com/2016/01/Ukraine-power-system-hacked.html>. Último acceso: 16 de febrero de 2017.

[22] S. Khandelwal. “Massive DDoS attack against Dyn DNS service knocks popular sites offline”. *The Hacker News, 21 de octubre de 2016.* <http://thehackernews.com/2016/10/dyn-dns-ddos.html>. Último acceso: 16 de febrero de 2017.

[23] T. Fox-Brewster. “Hackers Sell $7,500 IoT Cannon To Bring Down The Web Again”. *Forbes, 23 de octubre de 2016.* <http://www.forbes.com/sites/thomasbrewster/2016/10/23/massive-ddos-iot-botnet-for-hire-twitter-dyn-amazon/#dae9914c9156>. Último acceso: 19 de febrero de 2017.

[24] T. Hamburger, K. Tumulty. “WikiLeaks releases thousands of documents about Clinton and internal deliberations”. *The Washington Post, 22 de julio de 2016.* <https://www.washingtonpost.com/news/post-politics/wp/2016/07/22/on-eve-of-democratic-convention-wikileaks-releases-thousands-of-documents-about-clinton-the-campaign-and-internal-deliberations/?utm_term=.7863428b8545>. Último acceso: 16 de febrero de 2017.

[25] TrendMicro. “Ransomware-as-a-Service: Ransomware operators find ways to bring in business”. *TrendMicro, 2 de septiembre de 2016.* <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-as-a-service-ransomware-operators-find-ways-to-bring-in-business>. Último acceso: 18 de febrero de 2017.

[26] TrendMicro. “Ransomware Recap: Dec. 19 - Dec. 31, 2016”. *TrendMicro, 10 de enero de 2017.* <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-dec-19-dec-31-2016>. Último acceso: 18 de febrero de 2017.

Notas

[1] Seguramente, habrá llamado la atención del lector el uso de la palabra “3l1t3” en el título del artículo, la cual viene a significar “élite” en escritura “leet”. Este tipo de escritura alfanumérica es propia de algunas comunidades de Internet, y consiste en la sustitución de caracteres alfabéticos (letras, principalmente vocales) por dígitos numéricos. Considerada una forma de comunicación sólo para iniciados, debe su nombre, leet speak (1337 5p34K) precisamente a eso: la forma de hablar de la élite (elite speak, en inglés).

[2] “KrebsOnSecurity. In-depth security news and investigation” (KrebssobreSeguridad. Noticias e investigación en profundidad sobre seguridad). <https://krebsonsecurity.com/>. Último acceso: 19 de febrero de 2017.