

PARTE 1

# WSTR

INFORME SOBRE  
LAS AMENAZAS PARA  
LA SEGURIDAD DE  
LOS SITIOS WEB 2016

# ÍNDICE

---

<b>Symantec™ Global Intelligence Network</b>	03
<b>Introducción del WSTR (informe sobre amenazas para la seguridad de los sitios web)</b>	
Los sitios web aún corren el riesgo de infectarse con <i>malware</i> y sufrir fugas de datos	04
Seguridad completa para los sitios web	04
Acontecimientos destacados del año 2015	05
Principales conclusiones	05
Transición a una autenticación más rigurosa	06
Motivos para la esperanza	07
<b>El año 2015 en cifras</b>	
La situación actual	08
Las lagunas de seguridad	09
Las amenazas internas	10
El dinero lo es todo	10
La economía sumergida y las fuerzas de seguridad	14
• Empresas en la sombra	14
• Un negocio viento en popa	14
• Pueden intentar escapar, pero no esconderse	14
• Reducción del riesgo	15
<b>La víctima no es solo el dispositivo o la red, sino también el individuo que está detrás del equipo</b>	
No hay que fiarse de nadie	16
Secretos y mentiras	17
Identidades engañosas	18
Apuesta por el comercio electrónico	18
La confianza de los consumidores se tambalea	19
• La bolsa o la vida	19
• Pero ¿por qué los delincuentes privilegian este tipo de ataques?	19
• Consecuencias de Dyre	20
• El idioma y la ubicación no constituyen obstáculos	20
Leyes de privacidad	21
Evitemos la catástrofe cibernética	22
<b>La víctima no es solo el dispositivo o la red, sino también la entidad que está detrás de la red</b>	
Ataques persistentes	23
Diversidad en las vulnerabilidades de día cero	24
Grupos de ataque activos en 2015	24
Terror global, ataques locales	25
El efecto mariposa	25
Ciberseguridad, ciber sabotaje y cisnes negros	27
La escasa visibilidad no es la solución	27

# Symantec™ Global Intelligence Network

Symantec cuenta con la fuente de datos más completa que existe sobre las amenazas en Internet: Symantec™ Global Intelligence Network, un sistema formado por más de 63,8 millones de sensores de ataque que registra miles de incidencias por segundo.

Esta red supervisa las amenazas existentes en más de 157 países y regiones mediante una combinación de productos y servicios de Symantec, como los siguientes:

- Symantec DeepSight™ Intelligence,
- Symantec™ Managed Security Services,
- productos de consumo Norton™,
- Symantec Website Security
- y otras fuentes de datos externas.

Symantec también mantiene una de las bases de datos sobre vulnerabilidades más completas del mundo. En este momento, hay registradas más de 74 180 vulnerabilidades (a lo largo de dos décadas) que afectan a más de 71 470 productos de más de 23 980 proveedores.

## Los datos de *spam*, *phishing* o *malware* se registran con recursos como los siguientes:

- Symantec Probe Network, un sistema que abarca más de cinco millones de cuentas señuelo;
- Symantec.cloud;
- Symantec Website Security;
- y otras tecnologías de seguridad de Symantec.

La tecnología heurística patentada de Symantec.cloud, denominada Skeptic™, detecta los ataques dirigidos más nuevos y avanzados antes de que lleguen a la red del cliente. En 13 centros de datos, se procesan más de 9000 millones de mensajes de correo electrónico al mes y se filtran más de 1800 millones de solicitudes por Internet al día.

Symantec también recopila información sobre *phishing* a través de una amplia comunidad antifraude de empresas, proveedores de seguridad y más de 50 millones de consumidores.

Symantec Website Security protege más de un millón de servidores web y garantiza una disponibilidad ininterrumpida desde el año 2004. Esta infraestructura de validación permite comprobar si un certificado digital X.509 se ha revocado o no mediante el protocolo de estado de certificados en línea (OCSP) y procesa a diario más de 6000 millones de consultas de este tipo en todo el mundo. El sello Norton™



Secured aparece casi mil millones de veces al día en sitios web de 170 países, así como en los resultados de las búsquedas si se utilizan navegadores compatibles.

Gracias a estos recursos, los analistas de Symantec cuentan con fuentes de información insuperables para detectar, analizar e interpretar las nuevas tendencias en materia de ataques, *malware*, *phishing* y *spam*. Con todos estos datos, elaboran el informe anual sobre las amenazas para la seguridad de los sitios web, que ofrece a las empresas de todos los tamaños y a los consumidores información esencial para proteger sus sistemas de forma eficaz tanto ahora como en el futuro.

# Introducción del WSTR (informe sobre amenazas para la seguridad de los sitios web)

Independientemente de que se trate de hacer compras, trabajar o pagar una factura, hoy en día es imprescindible que los servicios online inspiren confianza. Por suerte, la forma de utilizar y proteger Internet está cambiando para que los internautas se sientan seguros en todo momento, hagan transacciones con plena tranquilidad y no teman por la confidencialidad de sus datos. La seguridad de los sitios web abarca mucho más que los datos que se transfieren entre el servidor y los internautas. Si quieren seguir inspirando confianza, las empresas tienen que considerar su sitio web como parte de un ecosistema que hay que cuidar con atención y constancia.

Ahora que la presencia del comercio electrónico en nuestra vida diaria no deja de aumentar, hay mucho en juego. Cada vez son más las actividades que realizamos en Internet, desde hacer la compra hasta reservar unas vacaciones. De hecho, según [Ecommerce Europe](#), la facturación global del comercio electrónico de la empresa al consumidor aumentó un 24 % para llegar a los 1,943 billones de dólares en el año 2014, mientras que [se prevé](#) que el comercio electrónico entre empresas alcance los 6,7 billones de aquí a 2020. En consecuencia, hoy en día, la seguridad de los sitios web es más importante y pertinente que nunca.

Si una empresa no logra reforzar la protección de su sitio web, no será la única afectada; la confianza de los consumidores también se verá perjudicada y podría haber enormes repercusiones económicas de gran alcance.

## Los sitios web aún corren el riesgo de infectarse con *malware* y sufrir fugas de datos

Los sitios web constituyen un elemento crucial en los ataques de gran envergadura, ya que permiten acceder a la red y a los datos de las empresas, así como a sus clientes y socios.

Por ejemplo, el hecho de que haya aumentado el uso de *malware* contra servidores web Linux (incluidos aquellos que alojan sitios web) demuestra que los delincuentes se han dado cuenta de que la infraestructura que hay detrás de los sitios web es tan valiosa como los datos cifrados con certificados SSL/TLS o incluso más.

Bastaría llevar a cabo un mantenimiento periódico para evitar muchos de los ataques de este tipo, pero las cifras observadas parecen indicar que los propietarios de sitios web no logran estar siempre al día.

Las tres cuartas partes de los sitios web analizados por Symantec en 2015 presentaban vulnerabilidades: un dato que lleva años sin cambiar.

En lugar de pensar solo en la protección, los administradores de los sitios web deberían tener en cuenta también la detección y la respuesta a los ataques. Necesitan herramientas de automatización que permitan supervisar los sitios web de forma constante para detectar indicios de vulnerabilidades o ataques, bloquear los ataques en cuestión y, a continuación, elaborar informes e instalar las actualizaciones y revisiones pertinentes.

## Seguridad completa para los sitios web

En el año 2015 los delincuentes siguieron encontrando vulnerabilidades en la infraestructura subyacente de la seguridad de los sitios web, como «FREAK», que permitía forzar el uso de un protocolo más fácil de descifrar a los atacantes que interceptaran la configuración de una conexión segura.

Si bien es cierto que periódicamente salen actualizaciones para proteger las bibliotecas de protocolos SSL/TLS como OpenSSL, los propietarios de los sitios web tienen que instalarlas si quieren evitar las vulnerabilidades. Asimismo, se está acelerando la transición de SHA-1 a SHA-2, un sistema mucho más eficaz, pero para que el cambio sirva de algo las empresas tienen que implantar correctamente los nuevos certificados.

En 2015 los ataques distribuidos de denegación de servicio (*Distributed Denial of Service* o *DDoS*) han seguido causando estragos en las empresas. Los ataques de gran envergadura, como [el que sufrió la BBC a finales de 2015](#), suelen tener mucho eco, pero en realidad en el punto de mira de los delincuentes están las empresas de todos los tamaños y muchas veces las de pequeñas dimensiones sufren daños colaterales cuando un servidor tiene que cerrar y deja fuera de combate numerosos sitios web solo porque uno de sus clientes ha sido atacado.

[www.ecommerce-europe.eu/news/2015/global-e-commerce-turnover-grew-by-24.0-to-reach-1943bn-in-2014](http://www.ecommerce-europe.eu/news/2015/global-e-commerce-turnover-grew-by-24.0-to-reach-1943bn-in-2014)  
[www.frost.com/sublib/display-report.do?id=MA4E-01-00-00-00](http://www.frost.com/sublib/display-report.do?id=MA4E-01-00-00-00)  
[www.bbc.co.uk/news/technology-35204915](http://www.bbc.co.uk/news/technology-35204915)

La conclusión es evidente: las empresas tienen que adoptar una actitud más proactiva en lo que se refiere a la implantación de los certificados SSL/TLS. No basta con instalarlos una vez y olvidarse del asunto, así que es imprescindible contar con herramientas que automaticen y agilicen el proceso.

### Acontecimientos destacados del año 2015

- Se redujo el precio de los datos robados, como las direcciones de correo electrónico o los números de tarjeta de crédito, lo que parece indicar un aumento en la oferta.
- China fue el origen del 46 % de las actividades realizadas con *bots* maliciosas en 2015 (el año anterior la cifra solo llegaba al 16 %), mientras que Estados Unidos pasó del 16 % al 8 % en ese mismo período.
- Se difundieron las indemnizaciones de los seguros contra ataques cibernéticos, lo que provocó un aumento de las primas y del coste global de las fugas de datos. Según el estudio anual de NetDiligence, las indemnizaciones por ataques cibernéticos llegaron a alcanzar los 15 millones de dólares, mientras que las más habituales oscilaron entre los 30 000 y los 263 000 dólares.
- La media de las identidades afectadas por cada fuga se redujo aproximadamente en un tercio para situarse en 4885. Sin embargo, aumentó en un 85 % el número de fugas registradas sobre las cuales no se reveló cuántas identidades quedaron al descubierto.
- Una víctima especialmente destacada de una incidencia de seguridad fue Hacking Team, empresa italiana que proporciona software de espionaje y vigilancia encubierta a varios clientes gubernamentales. Varias de las vulnerabilidades creadas por estos expertos para usarlas como armas se publicaron en Internet y acabaron en kits de herramientas de ataque web.
- La publicidad dañina sigue invadiendo los sitios web, junto con los servidores Linux en que estos se alojan: el número de infecciones volvió a aumentar en 2015.
- Aumentaron los ataques contra el sector sanitario y las compañías de seguros: por ejemplo, Anthem sufrió una grave fuga de datos en la que se perdieron los historiales médicos de casi 80 millones de pacientes. En 2015, la sanidad fue el subsector que padeció más fugas de datos.
- Ya se habían producido otras veces ataques avanzados provocados por organizaciones dotadas de abundantes recursos y medios económicos, y hace mucho tiempo que sospechamos que cuentan con apoyo gubernamental, pero en 2015 se descubrió el grupo Butterfly, que utilizaba técnicas con un nivel de complejidad similar para enriquecerse.

- La seguridad del Internet de las cosas adquirió protagonismo, pues se empezó a atacar a coches, electrodomésticos inteligentes y dispositivos sanitarios, por no hablar de los sistemas de control industrial.
- Se generalizaron los ataques a teléfonos, ya que aumentaron drásticamente las vulnerabilidades de los sistemas móviles y el número de aplicaciones Android maliciosas. Los ataques se volvieron más furtivos y avanzados y, por primera vez, los dispositivos Apple iOS empezaron a caer en las redes de los delincuentes aunque no hubieran sido objeto de jailbreak (proceso que modifica el sistema operativo para permitir la instalación de aplicaciones no autorizadas por el fabricante), como ocurría en los años anteriores.
- El fenómeno del *ransomware* perdió fuerza en 2015, y los atacantes se centraron más en el *crypto-ransomware*. También sufrieron ataques los servidores Linux de alojamiento de sitios web. Asimismo, se detectaron infecciones de *smartphones* y ataques de prueba de concepto a *televisores inteligentes* y relojes inteligentes.
- El sitio web de citas Ashley Madison sufrió un ataque que sacó a la luz los datos de numerosas personas dispuestas a engañar a sus parejas. Este caso tan sonado, junto con la difusión de las sextorsiones en Asia, demuestra que el valor de los datos personales ha adquirido una nueva dimensión que permite sacar más provecho económico a costa de las víctimas.

Existen instrumentos y tácticas eficaces para defenderse de los ataques DDoS, pero es necesario que los administradores de los sitios web dediquen tiempo a conocerlos e implantarlos.

### Principales conclusiones

Este año las vulnerabilidades de día cero han alcanzado niveles sin precedentes. Aunque siguen en el punto de mira las víctimas de siempre, como los complementos web y los sistemas operativos, cada vez son más habituales los ataques contra objetivos como el software de código abierto. Lo más preocupante es que en 2015 se descubrieron graves vulnerabilidades de día cero que se utilizaron para atacar sistemas ICS.

En los ataques dirigidos, siguen siendo fundamentales las maniobras de reconocimiento, que permiten a los atacantes recopilar información discretamente sobre los sistemas que les interesan antes de lanzar el ataque propiamente dicho. Las tácticas de este tipo han tenido mucho peso en ciertos casos de ciberterrorismo de gran repercusión, como los ataques lanzados con los troyanos Trojan.Laziok y BlackEnergy contra centrales eléctricas de Oriente Medio y Ucrania respectivamente.

En 2015 aumentaron prácticamente todos los indicadores relacionados con las fugas de datos; en particular, se batieron récords en la cantidad de ataques, identidades robadas y «megafugas». En cuanto a las fugas de alto riesgo, resulta sorprendente el puesto destacado que ocupan sectores como el de las aseguradoras y el de la hostelería, que despiertan el interés de los delincuentes porque son una fuente de datos privados, como números de tarjeta de crédito o información sanitaria. Es probable que los atacantes aprovechen con más frecuencia estos datos que los de otros sectores.

### Transición a una autenticación más rigurosa

No todo son malas noticias. En 2015 se ha avanzado tanto en lo que se refiere a la eficacia como a la adopción de los certificados SSL/TLS, y las autoridades de certificación han tomado medidas para que el proceso de emisión sea más transparente.

Según un [estudio de Sandvine](#), hoy se cifra casi el 40 % del tráfico de Internet descendente en Estados Unidos, y se prevé que a lo largo del próximo año este dato aumente para superar el 70 % del tráfico mundial.

Por desgracia, según las palabras de Robert Hoblit, vicepresidente de productos emergentes e ingresos de Symantec: «Ahora que se cifra todo, los consumidores tienen una falsa sensación de seguridad y creen que siempre que ven la indicación HTTPS se encuentran en un sitio web de una empresa auténtica que ha superado un proceso de validación».

En realidad, la inmensa mayoría de los fraudes siempre han tenido lugar en sitios web con validación de dominio, es decir, sin que la empresa en cuestión haya superado validación alguna. «Creo que la exigencia de cumplir la normativa relativa a los pagos con tarjeta de crédito va a llevar a las empresas a intensificar los requisitos de la autenticación», comenta Hoblit.

Cuando emite certificados con validación de dominio (DV), la autoridad de certificación comprueba que el contacto del dominio en cuestión apruebe la solicitud del certificado (por lo general, por correo electrónico o por teléfono), algo que suele ser automático. En consecuencia, estas soluciones suelen ser más baratas que los certificados SSL con Extended Validation (EV), los cuales exigen un proceso de validación y autenticación más riguroso.

Es cierto que, cuando se utilizan certificados con DV, se comprueba que el propietario del dominio dé su consentimiento, pero no se verifica quién es realmente dicho propietario, con lo que se deja la pista libre para los delincuentes que quieran lanzar ataques de interposición *Man-in-the-Middle* y de *phishing*. Symantec prevé que las empresas, en especial las que tienen que cumplir la normativa relativa a los pagos con tarjeta de crédito, intensifiquen los requisitos de autenticación y empiecen a adoptar certificados SSL con EV, que garantizan un nivel de seguridad más alto.

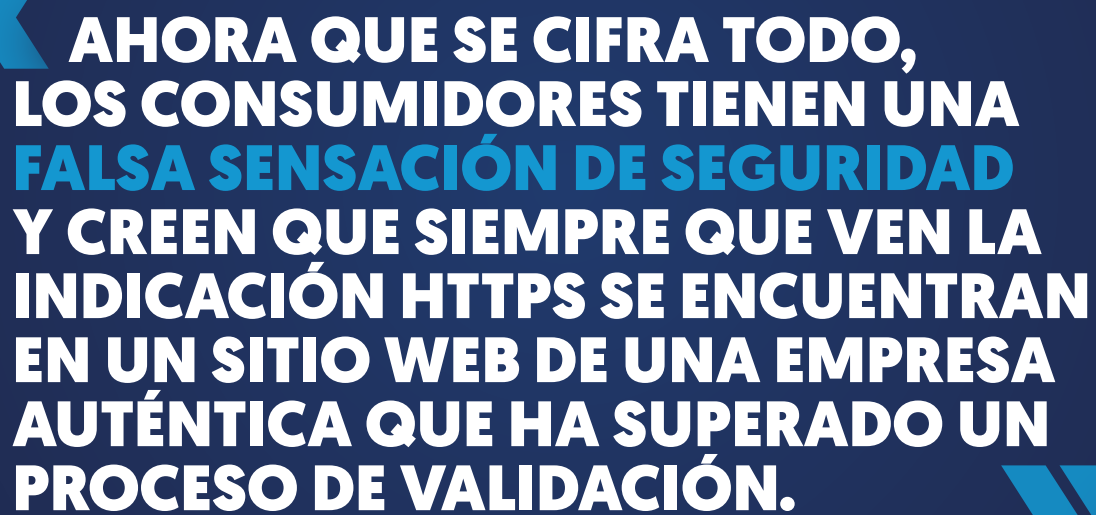
Por otro lado, el cifrado SSL/TLS será más eficaz gracias a la transición del algoritmo SHA-1 a SHA-2. Con la función hash SHA 1, que se ha utilizado con mucha frecuencia, cada hash generado por una fuente debería ser único. En teoría, nunca debería ocurrir que dos fuentes diferentes generaran el mismo hash, pero ya en 2005 se detectaron los primeros puntos débiles de este sistema. La situación llegó a un punto crítico en 2014, cuando [Google anunció](#) que dejaría de admitir los sitios web que utilizaran el algoritmo SHA 1 y que mostraría avisos de seguridad a los internautas que intentasen acceder a sitios web con certificados de este tipo que caducaran después del 1 de enero de 2017. Pronto otros proveedores de navegadores siguieron el ejemplo, con lo que quedó claro que el algoritmo SHA 1 estaba destinado a desaparecer.

En el sector de la seguridad se está avanzando mucho y existe la posibilidad concreta de reducir de forma considerable el número de ataques que se salen con la suya, pero solo se conseguirá si también los propietarios de los sitios web dan un paso al frente y toman medidas.

### Motivos para la esperanza

A pesar de que abundan las malas noticias, si las empresas están bien gestionadas y los usuarios actúan con prudencia, solo las amenazas más implacables se saldrán con la suya. Y hay más motivos para la esperanza. Por ejemplo, hoy se cifra casi el 40 % del tráfico de Internet descendente en Estados Unidos, y se prevé que este dato aumente a lo largo del año. Los estándares más recientes en materia de navegadores y sitios web ponen de relieve la importancia del cifrado y la seguridad.

Asimismo, los desarrolladores de software, teléfonos y sistemas del Internet de las cosas están mejorando la seguridad de sus productos (si bien en ciertos casos partían de un nivel muy bajo). Y, por supuesto, empresas como Symantec están luchando con todos sus medios contra los ciberdelincuentes, espías y malhechores.



**AHORA QUE SE CIFRA TODO,  
LOS CONSUMIDORES TIENEN UNA  
FALSA SENSACIÓN DE SEGURIDAD  
Y CREEN QUE SIEMPRE QUE VEN LA  
INDICACIÓN HTTPS SE ENCUENTRAN  
EN UN SITIO WEB DE UNA EMPRESA  
AUTÉNTICA QUE HA SUPERADO UN  
PROCESO DE VALIDACIÓN.**


Robert Hoblit, vicepresidente de productos emergentes e ingresos de Symantec

## El año 2015 en cifras

En 2015 las fugas de datos, originadas internamente o provocadas por estafadores, siguieron causando estragos tanto en los sitios web como en los dispositivos de los puntos de venta, y salieron más caras que nunca a las víctimas.

### La situación actual

El coste medio total de cada fuga de datos ha aumentado un 23 % en los últimos dos años, hasta alcanzar los 3,79 millones de dólares, tal como revela el [este estudio sobre el coste de las fugas de datos de 2015](#). Como hemos observado una ligera caída en el número total de fugas y la mediana de las identidades afectadas por cada fuga se ha reducido aproximadamente en un tercio para situarse en 4885, podemos concluir que los datos robados en cada ocasión son más valiosos o más confidenciales y las consecuencias para las empresas son más graves que en el pasado.

<b>FUGAS EN TOTAL</b> Fuente: Symantec   CCI 				
2015	Diferencia	2014	Diferencia	2013
305	-2 %	312	+23 %	253

<b>IDENTIDADES AFECTADAS EN TOTAL</b> Fuente: Symantec   CCI 				
2015	Diferencia	2014	Diferencia	2013
429 millones	+23 %	348 millones	-37 %	552 millones

En consecuencia, se están difundiendo las indemnizaciones de los [seguros contra ataques cibernéticos](#) y, según el [estudio de NetDiligence](#), estas han llegado a alcanzar los 15 millones de dólares, mientras que las más habituales se encuentran entre los 30 000 y los 263 000 dólares. Al mismo tiempo, cada vez sale más caro asegurar los activos digitales, lo cual contribuye a que crezca aún más el coste global de las fugas de datos.

En el primer semestre de 2015, [aumentó en un 32 %](#) el valor medio de las primas para comerciantes, mientras que en el sector sanitario algunas de ellas incluso se triplicaron. Además, según Reuters, ahora los deducibles tienden a ser más altos e incluso las mayores aseguradoras no dan pólizas de más de 100 millones de dólares a los clientes en situaciones de riesgo.

<http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF>  
<http://www.symantec.com/cyber-insurance/>  
[http://netdiligence.com/downloads/NetDiligence\\_2015\\_Cyber\\_Claims\\_Study\\_093015.pdf](http://netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf)  
<http://www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN05609M20151012>



## Las lagunas de seguridad

A pesar de que los sistemas de cifrado cada vez son más eficaces, este año muchos de los ataques contra certificados SSL/TLS han aprovechado puntos débiles del ecosistema SSL/TLS general.

«Durante el último año se ha prestado mucha más atención a las bibliotecas de código con relación a las implantaciones de certificados SSL/TLS», comenta Michael Klieman, director general y ejecutivo de gestión de productos en Symantec. «En consecuencia, se han facilitado con una frecuencia razonable actualizaciones y soluciones contra vulnerabilidades».

Eso es lo bueno, pero la otra cara de la moneda es que los propietarios de sitios web no siempre mantienen al día sus sistemas de seguridad, tal como revelan las vulnerabilidades sin resolver más habituales que se han

observado en los servidores web durante el último año. Es imprescindible que los responsables de gestionar los sitios web mantengan la integridad de las implantaciones SSL/TLS: no basta con instalar los certificados y luego olvidarse del asunto.

Aunque no hemos detectado vulnerabilidades tan peligrosas como Heartbleed, que tanto protagonismo tuvo en 2014, a lo largo de 2015 OpenSSL proporcionó varias actualizaciones y revisiones. Se utiliza OpenSSL en dos tercios de los servidores web, lo que la convierte en una de las implantaciones más difundidas de los protocolos de cifrado SSL y TLS. El objetivo de las actualizaciones mencionadas era resolver vulnerabilidades con distintos niveles de riesgo, que permitían a los delincuentes llevar a cabo ataques de interposición *Man-in-the-Middle* o de denegación de servicio, así como interceptar comunicaciones en teoría seguras.

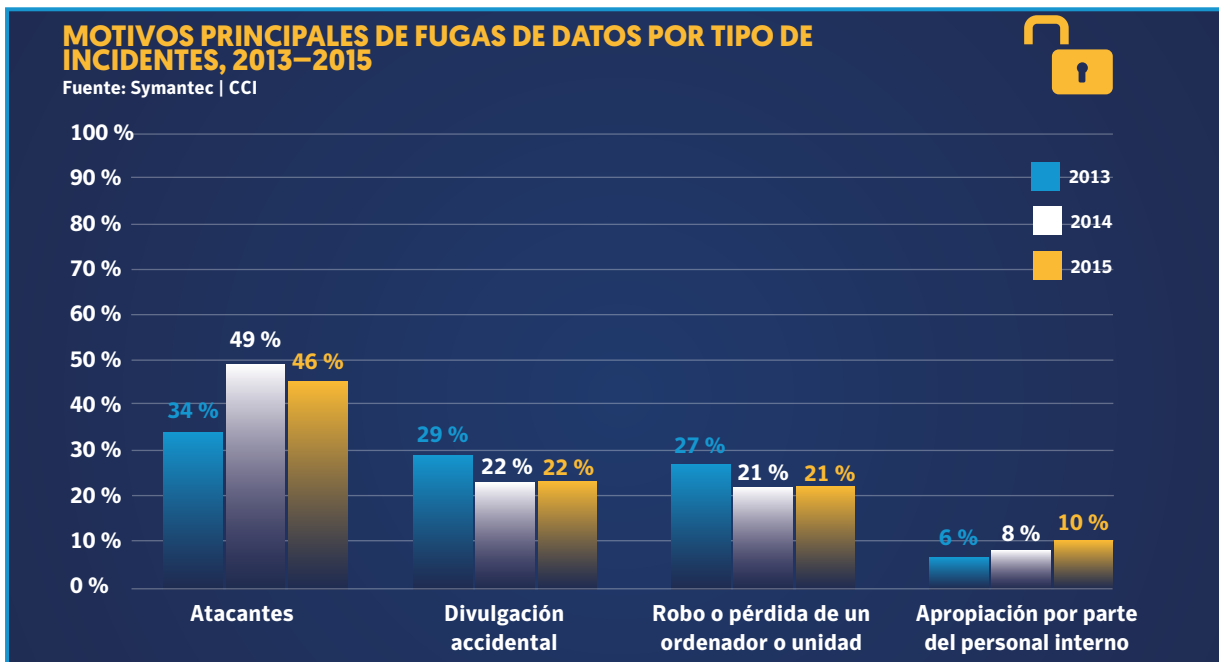
## PRINCIPALES VULNERABILIDADES SIN RESOLVER DETECTADAS EN LOS SERVIDORES WEB ANALIZADOS

Fuente: Symantec | Trusted Services



Puesto	Nombre
1	Vulnerabilidad POODLE (protocolos SSL y TLS)
2	Ausencia del encabezado de opciones X-Content-Type
3	Ausencia del encabezado de opciones X-Frame
4	Certificado SSL firmado con un algoritmo hash débil
5	Vulnerabilidad frente a ataques de secuencias de comandos entre sitios
6	Ausencia del encabezado Strict-Transport-Security
7	Compatibilidad con SSL v2
8	Cookie de sesión SSL cifrada sin el atributo «Secure»
9	Compatibilidad con conjuntos de cifrado SSL poco seguros
10	Vulnerabilidad en el proceso de renegociación de los protocolos SSL y TLS

<http://www.symantec.com/connect/blogs/critical-openssl-vulnerability-could-allow-attackers-intercept-secure-communications>  
<http://www.symantec.com/connect/blogs/new-openssl-vulnerability-could-facilitate-dos-attacks>



#### Las amenazas internas

Si bien solo en torno al 10 % de las fugas de datos de 2015 se debieron a causas internas, el estudio de [NetDiligence](#) revela que, en el 32 % de las indemnizaciones de los seguros contra ataques cibernéticos, intervino algún factor interno. Por ejemplo, [la fuga de datos sufrida en Ashley Madison, una de las más sonadas del año, al parecer fue provocada por alguien descontento que se encontraba dentro de la propia empresa](#), según afirma su director ejecutivo. Si bien no se ha confirmado qué ocurrió exactamente, si la hipótesis mencionada es cierta, este caso destaca el daño que se puede llegar a infligir desde dentro de una empresa.

Las amenazas internas siempre han sido un tema candente en el campo de la seguridad informática, pero en 2015 los organismos gubernamentales, además de percatarse del problema, empezaron a tomar medidas.

- Más de tres cuartos de los organismos gubernamentales estadounidenses encuestados en el [informe federal sobre amenazas internas de MeriTalk](#) aseguran que ahora se esfuerzan más que hace un año por combatir las amenazas internas.
- El Centre for Defence Enterprise del Reino Unido en 2015 patrocinó varios proyectos destinados a supervisar el [comportamiento digital de los empleados](#) para prevenir y [detectar amenazas internas](#) en tiempo real, así como [simuladores de aprendizaje](#) para enseñar a reconocer los riesgos.

[http://netdiligence.com/downloads/NetDiligence\\_2015\\_Cyber\\_Claims\\_Study\\_093015.pdf](http://netdiligence.com/downloads/NetDiligence_2015_Cyber_Claims_Study_093015.pdf)  
<http://uk.businessinsider.com/ashley-madison-ceo-says-hack-was-an-inside-job-2015-7>  
[http://cdn2.hubspot.net/hubfs/407136/PDFs/Symantec/MeriTalk\\_-\\_Symantec\\_-\\_Inside\\_Job\\_Report\\_-\\_FINAL.pdf?t=1445970735623](http://cdn2.hubspot.net/hubfs/407136/PDFs/Symantec/MeriTalk_-_Symantec_-_Inside_Job_Report_-_FINAL.pdf?t=1445970735623)  
<https://www.gov.uk/government/news/protecting-information-from-an-insider-threat>  
<https://www.gov.uk/government/news/identifying-cyber-insider-threats-in-real-time>  
<https://www.gov.uk/government/news/securing-against-the-insider-threat>

#### El dinero lo es todo

El principal motivo que impulsa las fugas de datos sigue siendo económico: cuantos más datos tenga alguien sobre un individuo, más fácil le resultará robar su identidad, así que las aseguradoras, los organismos gubernamentales y las entidades sanitarias están en el punto de mira de los delincuentes, que aspiran a conseguir perfiles personales más completos.

El tipo de información que interesa a los delincuentes no cambió en 2015; únicamente se produjeron pequeños cambios en la clasificación. Los nombres de personas siguen siendo el tipo de dato que sale a la luz con más frecuencia: está presente en más del 78 % de las fugas de datos. Los domicilios, las fechas de nacimiento, los números de identificación de carácter administrativo (por ejemplo, de la seguridad social), los historiales médicos y la información financiera se encuentran entre el 30 y el 40 %, igual que en 2014, aunque el puesto que ocupa cada tipo de dato ha variado ligeramente. Completan la lista de los 10 principales tipos de datos afectados las direcciones de correo electrónico, los números de teléfono, la información relacionada con planes de seguros y los nombres de usuario y contraseñas. Todos ellos vuelven a situarse entre el 10 y el 20 %.

Esto no significa que los datos de las tarjetas de crédito hayan dejado de interesar a los atacantes. Sin embargo, su valor en el mercado negro no es especialmente alto, pues las empresas que emiten las tarjetas, al igual que los propietarios de estas, detectan muy pronto los gastos anómalos, y los datos robados tienen una vida útil limitada. En cualquier caso, el mercado de los datos de tarjetas de crédito no desaparece.

## SECTORES EN LOS QUE SE DEJARON AL DESCUBIERTO MÁS IDENTIDADES (2 CIFRAS)

Fuente: Symantec | CCI



Puesto	Sector	Número de identidades afectadas	Porcentaje de identidades afectadas
1	Servicios sociales	191,035 533	44,5 %
2	Aseguradoras	100 436 696	23,4 %
3	Servicios personales	40 500 000	9,4 %
4	Gestión de recursos humanos	21 501 622	5,0 %
5	Agentes, corredores y servicios de seguros	19 600 000	4,6 %
6	Servicios empresariales	18 519 941	4,3 %
7	Venta al por mayor - Bienes duraderos	11 787 795	2,7 %
8	Servicios ejecutivos, legislativos y generales	6 017 518	1,4 %
9	Servicios de enseñanza	5 012 300	1,2 %
10	Servicios sanitarios	4 154 226	1,0 %

## PRINCIPALES TIPOS DE DATOS AFECTADOS

Fuente: Symantec | CCI



Puesto	Tipo (2015)	2015 %	Tipo (2014)	2014 %
1	Nombres de personas	78,3 %	Nombres de personas	68,9 %
2	Domicilios	43,7 %	Números de identificación de carácter administrativo (p. ej., de la seguridad social)	44,9 %
3	Fechas de nacimiento	41,2 %	Domicilios	42,9 %
4	Números de identificación de carácter administrativo (p. ej., de la seguridad social)	38,4 %	Información financiera	35,5 %
5	Historiales médicos	36,2 %	Fechas de nacimiento	34,9 %
6	Información financiera	33,3 %	Historiales médicos	33,7 %
7	Direcciones de correo electrónico	20,8 %	Números de teléfono	21,2 %
8	Números de teléfono	18,6 %	Direcciones de correo electrónico	19,6 %
9	Información relacionada con planes de seguros	13,2 %	Nombres de usuario y contraseñas	12,8 %
10	Nombres de usuario y contraseñas	11,0 %	Información relacionada con planes de seguros	11,2 %

En cuanto a los sectores más afectados, las empresas de servicios fueron las que sufrieron más fugas de datos, tanto si se tiene en cuenta el número de incidencias como si nos basamos en la cantidad de identidades que salieron a la luz. Sin embargo, dentro de esta clasificación general, el motivo del ataque es diferente en cada subsector.

El número de incidencias más alto se registró en el subsector de los servicios sanitarios, donde se produjeron el 39 % de las fugas del año. Esto entra dentro de lo esperado, dado el rigor de las normas que exigen a las entidades sanitarias informar de las fugas de datos sufridas. Sin embargo, la cantidad de identidades afectadas es relativamente baja en este sector. El hecho de que se produzcan tantas fugas en las que salen a la luz pocas identidades parece indicar que los datos robados son muy valiosos.

El subsector en el que se robaron más identidades fue el de los servicios sociales, pero esto se debe en gran parte a una sola fuga que batió récords al afectar a 191 millones de identidades. Si excluimos este caso concreto, el sector de los servicios sociales pasa al último puesto de la lista. (Por cierto, este es el puesto que ocupa en la clasificación según el número de fugas).

El sector de la venta al detalle sigue siendo muy lucrativo para los delincuentes, aunque ahora que en Estados Unidos se ha adoptado el estándar EMV (es decir, se han empezado a usar tarjetas de pago con chip y PIN), ha perdido valor la información que se puede sacar de los dispositivos de los puntos de venta.

La tecnología EMV es un estándar global para las tarjetas con microchip, utilizado en varios países desde los años noventa y principios del siglo XXI, que permite autenticar las transacciones mediante una combinación de chip y PIN. Tras las numerosas fugas de datos de gran envergadura que han tenido lugar en los últimos años y la proliferación de estafas con tarjetas de crédito, las entidades que emiten dichas tarjetas en EE. UU. están adoptando este sistema para tratar de paliar los efectos de este tipo de fraudes.

Antes los delincuentes podían hacerse con los datos llamados «Track 2», es decir, la información almacenada en

las bandas magnéticas de las tarjetas, para luego clonarlas y usarlas en tiendas o incluso en cajeros automáticos, si conseguían el PIN. Los datos «Track 1» contienen más información que los «Track 2», como el nombre del titular, el número de cuenta y otros datos discrecionales, que a veces utilizan las aerolíneas al hacer reservas con tarjeta de crédito. El [valor de estos datos](#) se refleja en los precios de venta que alcanzan en el mercado negro de Internet, donde llegan a costar 100 \$ por tarjeta.

Desde octubre de 2015, el 40 % de los consumidores estadounidenses disponen de tarjetas EMV, y se calcula que el 25 % de los comerciantes cumplen el estándar EMV. Sin embargo, con el estándar EMV resulta mucho más difícil clonar tarjetas. Si bien es cierto que [tendrán que pasar unos años](#) antes de que concluya la transición, hay que señalar que el nuevo sistema, junto con otras mejoras de la seguridad de los puntos de venta, debería hacer que este tipo de robos de gran envergadura resultaran más difíciles y sin duda menos rentables para los delincuentes. Esto nos lleva a cuestionarnos la forma de valorar el nivel de riesgo de una fuga de datos. Es posible que en un sector concreto se produzca una gran cantidad de robos o queden al descubierto numerosas identidades, pero ¿significa eso que los datos se estén utilizando para fines delictivos?

Por ejemplo, cabe señalar que el 48 % de las fugas de datos se debieron a descuidos. En estos casos, los datos personales salieron a la luz, bien porque la empresa los compartió con quien no debía o bien porque los registros privados pasaron a ser públicos por un error de configuración del sitio web. Pero ¿llegó la información a manos de personas con intenciones maliciosas? En muchos casos, probablemente no. Si una anciana jubilada recibe por error el historial médico de otra persona en su dirección de correo electrónico, no es fácil que aproveche esta información para robar una identidad. Esto no significa que nunca ocurra, sino que la inmensa mayoría de estas fugas de datos implican un riesgo reducido.

Lo que sí supone un riesgo mucho más alto son los casos en que la fuga de datos se debe a un ataque llevado a cabo por hackers o desde dentro de la propia empresa. Con toda probabilidad, en estas situaciones el objetivo es robar identidades.

<http://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks>  
<http://www.usatoday.com/story/money/personalfinance/2015/09/30/chip-credit-card-deadline/73043464/>  
<http://arstechnica.com/business/2015/10/today-all-stores-in-the-us-should-accept-chip-and-pin-cards-yeah-right/>

## Fuera de lo común

En 2015 el ataque de Hacking Team llamó especialmente la atención porque los delincuentes no buscaban dinero ni identidades, sino armas cibernéticas. También dio mucho que hablar porque fue un ataque de hacking contra hackers.

Hacking Team es un equipo italiano que vende software de espionaje y vigilancia encubierta a usuarios gubernamentales.

En el ataque, salieron a la luz vulnerabilidades de día cero desconocidas hasta entonces.

En cuestión de días, se publicaron en una serie de foros los datos de varias vulnerabilidades del día

cero y numerosos troyanos utilizados como armas por el grupo, mientras que bastaron unas horas para que acabaran entrando en varios kits de herramientas de ataque.



## La economía sumergida y las fuerzas de seguridad

La economía sumergida prospera y la ciberdelincuencia crece a un ritmo vertiginoso, pero tal como hemos visto, en 2015 también aumentaron las detenciones y los desmantelamientos de gran relevancia. En definitiva, estén donde estén los malhechores, ahora las fuerzas de seguridad los encuentran con más rapidez. Es cierto que los ataques de *ransomware* han disminuido, pero también se han diversificado y ahora afectan también a los servidores web Linux.

### Empresas en la sombra

Hoy los ciberdelincuentes son más profesionales y mucho más audaces tanto a la hora de elegir a sus víctimas como en lo que se refiere a las cantidades de dinero que aspiran a amasar. Estas empresas delictivas se consideran negocios propiamente dichos que abarcan una gran variedad de áreas, cada una con sus propios campos de especialización, y que cuentan con colaboradores, socios, distribuidores, proveedores, etc., tal como ocurre en el mercado legal.

### Un negocio viento en popa

Así como durante los últimos años los precios de las direcciones de correo electrónico se han reducido de forma considerable, los de las tarjetas de crédito se han mantenido relativamente bajos pero estables. De todos modos, estos

mismos datos alcanzan un precio muy alto si contienen información «de lujo» (por ejemplo, si se comprueba que las cuentas del vendedor siguen activas o que la tarjeta de crédito no se ha bloqueado).

Por ejemplo, basta pagar entre 100 y 700 dólares estadounidenses a la semana para alquilar un kit de herramientas web que infecte a las víctimas con descargas no autorizadas, con derecho a actualizaciones y asistencia ininterrumpida, mientras que los ataques distribuidos de denegación de servicio (DDoS) cuestan entre 10 y 1000 dólares al día. Por otro lado, en la gama más alta del mercado se encuentran las vulnerabilidades de día cero, que pueden llegar a venderse por cientos de miles de dólares. Cabe señalar que estas cifras han cambiado muy poco desde el año 2014.

## PRINCIPALES FUENTES DE ACTIVIDAD DELICTIVA: BOTS, 2014–2015

Fuente: Symantec | GIN



Puesto	País o región (2015)	Porcentaje de bots (2015)	Puesto	País o región (2014)	Porcentaje de bots (2014)
1	China	46,1 %	1	China	16,5 %
2	Estados Unidos	8,0 %	2	Estados Unidos	16,1 %
3	Taiwán	5,8 %	3	Taiwán	8,5 %
4	Turquía	4,5 %	4	Italia	5,5 %
5	Italia	2,4 %	5	Hungría	4,9 %
6	Hungría	2,2 %	6	Brasil	4,3 %
7	Alemania	2,0 %	7	Japón	3,4 %
8	Brasil	2,0 %	8	Alemania	3,1 %
9	Francia	1,7 %	9	Canadá	3,0 %
10	España	1,7 %	10	Polonia	2,8 %

### Pueden intentar escapar, pero no esconderse

«Durante el último año, los cuerpos de seguridad se han vuelto más eficaces en la lucha contra este tipo de delincuencia —declara Dick O'Brien, desarrollador informático sénior de Symantec—. Las operaciones de este tipo exigen actuar de forma coordinada en el ámbito internacional, porque rara vez el grupo de delincuentes pertenece a un solo país, pero cuando salen bien suponen un duro golpe para los atacantes y hacen que las actividades ilegales se vuelvan más arriesgadas y potencialmente costosas».

<http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services>

**Entre los éxitos logrados en 2015, cabe destacar los siguientes:**

- **El desmantelamiento de la botnet Dridex.** En el marco de una operación de seguridad internacional realizada en octubre, se detuvo a un hombre y se actuó de forma coordinada para arrebatar de las manos de la botnet Dridex miles de ordenadores atacados.
- **El desmantelamiento de Simda.** En abril los cuerpos de seguridad confiscaron la infraestructura en manos de los controladores de la botnet Simda, que abarcaba una serie de servidores de control.
- **La incautación de Ramnit.** En el marco de una operación de seguridad realizada en febrero bajo la batuta de Europol y con la asistencia de Symantec y Microsoft entre otros, las autoridades se incautaron de una serie de servidores y otra infraestructura que estaba en manos del grupo de ciberdelincuentes autores de la botnet Ramnit.
- **La acusación de ataques de hacking contra JP Morgan Chase.** Con relación a varios ataques en los que se robaron más de 100 millones de registros de clientes, las autoridades federales acusaron al menos a cuatro hombres de infiltración en varias instituciones financieras y de manipulación bursátil.

**Reducción del riesgo**

Hay que recordar que gran parte de las fugas de datos se podrían haber evitado con una serie de medidas básicas de sentido común, como las siguientes:

- Aplicar revisiones para resolver vulnerabilidades
- Mantener el software en buen estado
- Implantar filtros de correo electrónico eficaces
- Utilizar software de detección y prevención de las intrusiones
- Limitar el acceso a los datos empresariales por parte de terceros
- Cifrar los datos confidenciales para protegerlos
- Instalar una tecnología de prevención de pérdidas de datos (o DLP)

Obviamente, estas medidas sirven para prevenir los ataques procedentes del exterior. Cuando se trata de evitar las amenazas internas, tanto malintencionadas como involuntarias, las empresas tienen que centrarse en formar debidamente a los empleados e impedir las pérdidas de datos.

Del mismo modo que nos dicen que tenemos que taparnos la boca al toser o lavarnos bien las manos en los hospitales, habría que concienciar a los empleados sobre la importancia de las medidas de seguridad básicas. Además, las empresas deberían contar con herramientas de prevención de pérdidas de datos que permitan localizar, supervisar y proteger su información independientemente de dónde se encuentre, para saber en todo momento quién está utilizando cuáles datos y qué está haciendo con ellos.

La seguridad se debería considerar una parte esencial de las operaciones y del comportamiento de los empleados, y no un mero complemento que sirve para complacer a los auditores. No parece probable que las fugas de datos desaparezcan a corto plazo, pero sin duda podría reducirse su gravedad y los daños que provocan si las empresas comprendieran que la seguridad no es solo responsabilidad del director de sistemas y el gestor de TI, sino que está en manos de todos los empleados.

<http://www.symantec.com/connect/blogs/dridex-takedown-sinks-botnet-infections>  
<http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation>

# La víctima no es solo el dispositivo o la red, sino también el individuo que está detrás del equipo

Algunos de los ataques y tácticas de los ciberdelincuentes en 2015 han sido tan complejos e implacables que han puesto de manifiesto lo vulnerables que son los internautas y, en consecuencia, han hecho que la confianza de los consumidores se tambalee.

En 2015 las fugas de datos, la vigilancia gubernamental y las estafas de toda la vida se aliaron en contra de nuestra privacidad. Ya se trate de fotografías personales, datos de acceso a cuentas bancarias o historiales médicos, podemos tener la certeza de que nuestros datos no tienen nada de privados.

## No hay que fiarse de nadie

En 2015 tuvieron lugar numerosos ataques con *malware* y estafas tradicionales cuyo objetivo era conseguir datos personales. Por ejemplo, uno de los engaños consistía en prometer grandes cantidades de seguidores gratis en Instagram para conseguir que los usuarios revelaran su contraseña o hacerse pasar por Hacienda en un mensaje de correo electrónico para que los destinatarios descargasen archivos adjuntos infectados.

Las estafas más sencillas siguen aprovechando la escasa prudencia que suele tener la gente, pero también hay casos en que los datos de los clientes salen a la luz porque el sitio web en cuestión carece de un buen sistema de seguridad. En este último supuesto, se pueden producir fugas de datos independientemente de lo segura que sea la contraseña que elija el usuario.

De todos modos, quizá sean más preocupantes los ataques producidos en 2015 que recurrieron a técnicas avanzadas de ingeniería social para sortear los sistemas de autenticación de dos factores concebidos para proteger a los usuarios.

Sin embargo, también hubo una estafa que aprovechó precisamente la confianza del público en ciertas entidades: el atacante se hizo pasar por Google en un mensaje de texto imitando el proceso legítimo de recuperación de la contraseña para acceder a la cuenta de correo electrónico de la víctima sin despertar sospechas. (Más información en la columna de la derecha).

## Cómo funciona la estafa de Gmail

1. Un atacante consigue la dirección de correo electrónico y el número de teléfono de la víctima (ambos suelen ser públicos).
2. El atacante se hace pasar por la víctima y pide a Google que le envíe su contraseña.
3. A continuación, el atacante envía a la víctima el siguiente mensaje de texto (o uno similar): «Google ha detectado actividad inusual no autorizada en su cuenta. Para impedirla, responda con el código que hemos enviado a su dispositivo móvil».
4. Así, la víctima se espera recibir el código para restablecer la contraseña que envía Google y se lo pasa al atacante.
5. El atacante restablece la contraseña y, cuando ha conseguido lo que buscaba o ha configurado el reenvío, comunica la nueva contraseña temporal (de nuevo, haciéndose pasar por Google) a la víctima, que no se dará cuenta de lo que ha ocurrido.

<http://www.symantec.com/connect/blogs/free-instagram-followers-compromised-accounts-phishing-sites-and-survey-scams>  
<http://www.symantec.com/connect/blogs/australians-beware-scammers-are-impersonating-australian-taxation-office>  
<http://www.symantec.com/connect/blogs/password-recovery-scam-tricks-users-handing-over-email-account-access>



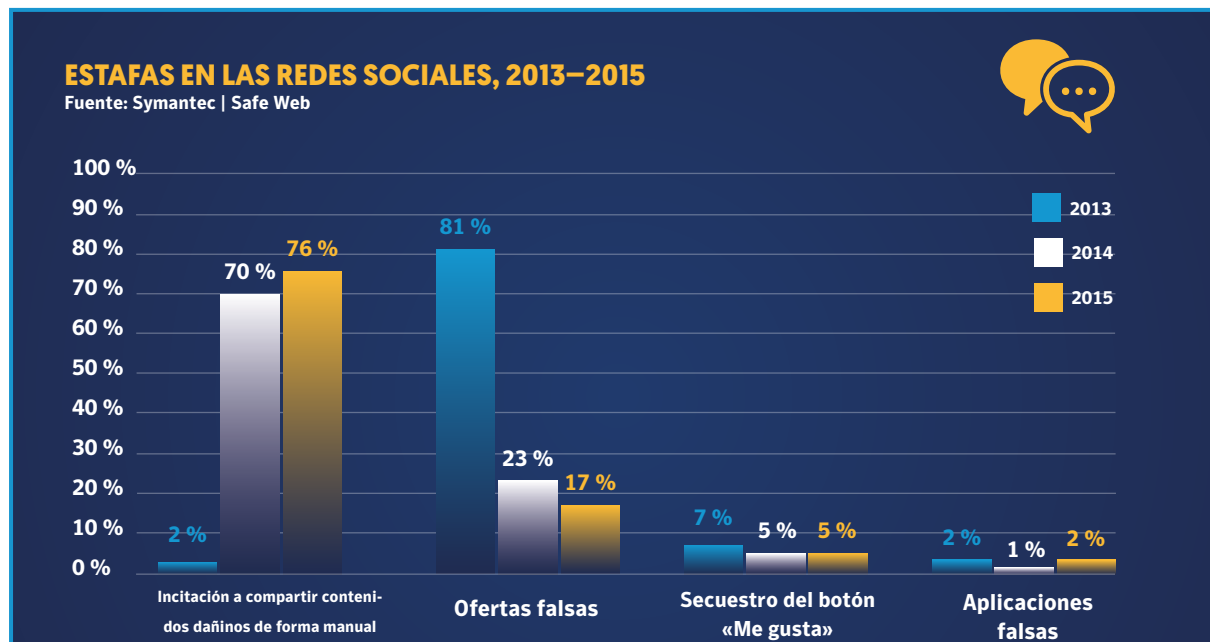
## Secretos y mentiras

En 2015 las estafas tradicionales siguieron al orden del día, pero además aparecieron amenazas a la privacidad más maliciosas.

Por ejemplo, las sextorsiones, especialmente habituales en Asia, consisten en usar un alias atractivo para que la víctima acceda a enviar vídeos sexualmente explícitos. A continuación, los delincuentes piden al internauta que descargue una aplicación para continuar con la relación y, de este modo, consiguen los datos telefónicos y los contactos de la víctima.

Por último, el malhechor amenaza con enviar el contenido sexual a toda la lista de contactos de la víctima a menos que pague una cantidad de dinero. Debido a la naturaleza tan delicada del contenido afectado, a las víctimas les suele costar denunciar el ataque y acaban enviando al hacker cientos de dólares, si no miles.

En la misma línea, el ataque a Ashley Madison provocó un pico de mensajes no deseados con asuntos como los siguientes: «¿Cómo comprobar si el ataque a Ashley Madison te ha afectado?» o «Ashley Madison, víctima de un ataque: ¿quieres saber si tu cónyuge te engaña?». Este ataque fue inusual, pues sus repercusiones llegaron mucho más allá de la esfera económica para afectar a las relaciones personales y la reputación de la gente.



<http://www.symantec.com/connect/blogs/online-criminal-group-uses-android-app-sextortion>  
[http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html?\\_r=0](http://www.nytimes.com/2015/07/21/technology/hacker-attack-reported-on-ashley-madison-a-dating-service.html?_r=0)  
<http://www.symantec.com/connect/blogs/scammers-quick-capitalize-ashley-madison-breach>

## Identidades engañosas

Las redes sociales siguieron siendo un terreno fértil para los delincuentes en 2015, pues estos lograron difundir estafas, enlaces falsos y ataques de *phishing* aprovechando la confianza que tiene la gente en sus contactos.

Ahora los atacantes utilizan tácticas más ingeniosas y avanzadas y, para salirse con la suya, tienen que recurrir a una ingeniería social convincente.

Hubo una estafa en concreto que llegó a crear toda una red de cientos de miles de cuentas de Twitter falsas, en la que cada nivel reforzaba la credibilidad del nivel superior, para conseguir seguidores y retuiteos entre los usuarios de Twitter auténticos. En la cumbre de dicha red había cuentas falsas que se hacían pasar por cabeceras de prensa y personajes famosos, y los delincuentes incluso llegaron a imitar las publicaciones de las cuentas auténticas para que los tuiteos resultaran más creíbles.



Para decidir quién es digno de confianza en las redes sociales, tenga en cuenta los siguientes consejos:

- **Busque el símbolo azul de verificación.** Antes de empezar a seguir a un personaje famoso o una marca, los usuarios de Twitter deberían siempre ver si aparece el símbolo azul de verificación, que indica que Twitter ha comprobado la autenticidad del propietario de la cuenta en cuestión.
- **No se fie de los nuevos seguidores.** Si una persona cualquiera se suma a sus seguidores, no corresponda automáticamente siguiéndola a ella. Antes, observe sus publicaciones. ¿Retuitea contenido de aspecto sospechoso? Si es así, lo más probable es que se trate de un *bot*.
- **A veces los números engañan.** Aunque los usuarios que empiecen a seguir su cuenta tengan a su vez miles de seguidores, no se base en este dato para decidir si son de fiar, pues es muy fácil falsificar estas cifras.

## Apuesta por el comercio electrónico

En el fin de semana de Acción de Gracias de 2015, el número de consumidores que compraron por Internet superó al de quienes acudieron a las tiendas, según los cálculos de la National Retail Foundation (fundación nacional de venta al detalle).

Según Ecommerce Europe, la facturación global del comercio electrónico de la empresa al consumidor aumentó un 24 % para llegar a los 1943 millones de dólares en 2014, pero eso no es gran cosa en comparación con los 6,7 billones que, según los cálculos de Frost and Sullivan, alcanzará de aquí al año 2020 el comercio electrónico entre empresas. Esta última previsión abarca todo tipo de comercio electrónico, incluido el uso de sistemas de intercambio de datos electrónicos y de Internet.

Incluso los gobiernos cada vez recurren más a los servicios digitales para cuadrar las cuentas. Por ejemplo, el gobierno británico ha revelado recientemente que en 2014 se ahorró 1700 millones de libras esterlinas gracias a la transformación digital y tecnológica.

Si bien es cierto que los certificados SSL/TLS, los distintivos de confianza y la protección de los sitios web contribuyen a mantener la economía online, todo este negocio podría correr peligro si la gente deja de fiarse de los sistemas de seguridad en que se basa el sector.

### La confianza de los consumidores se tambalea

Otros ataques perpetrados en 2015 también demuestran el grado de maldad y complejidad al que se puede llegar para hacer dinero.

#### La bolsa o la vida

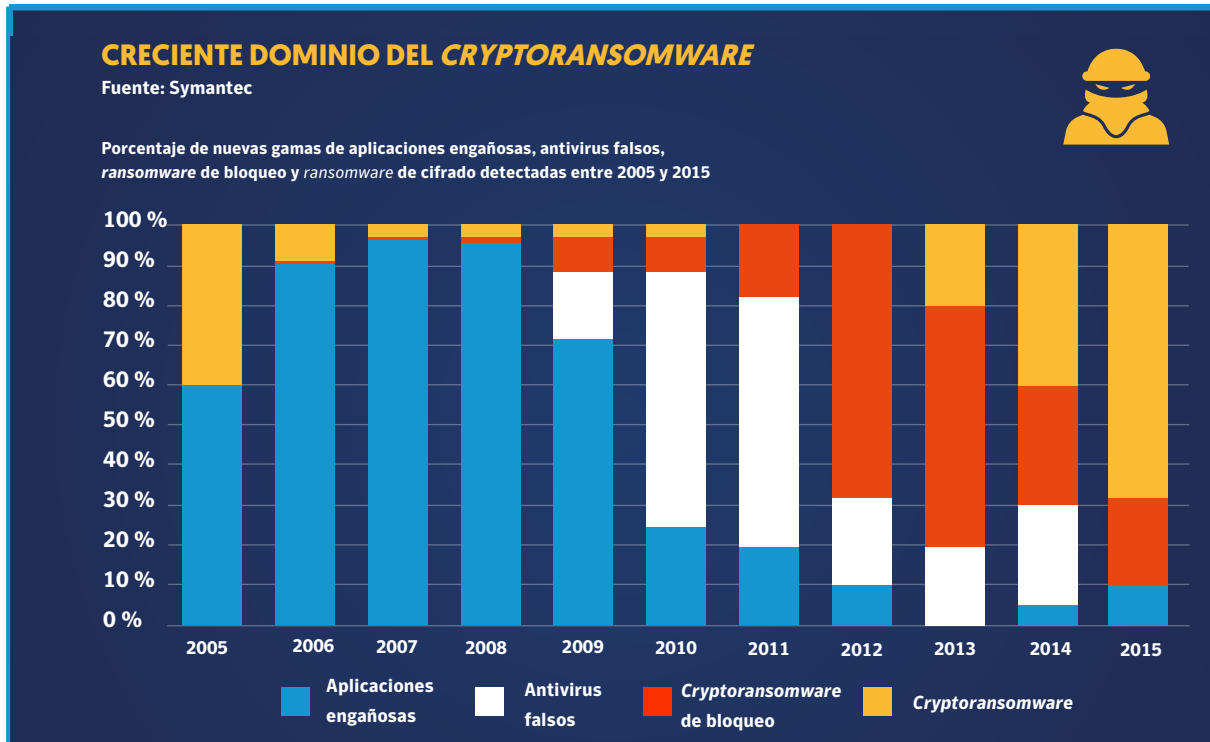
El *ransomware* se ha difundido cada vez más en los últimos años y en 2015 muchos preveían que la tendencia continuase. Sin embargo, los ataques de este tipo se han diversificado, pero su volumen no ha aumentado. Ahora los ciberdelincuentes cifran archivos almacenados en dispositivos móviles y cualquier recurso por el que la víctima esté dispuesta a pagar. De hecho, un estudio de Symantec ha llegado a demostrar que también la televisión inteligente puede ser víctima de este tipo de ataques.

Ahora también hay *ransomware* que amenaza con publicar los archivos de la víctima en Internet a menos que pague una suma de dinero: se trata de una interesante y siniestra novedad que con toda probabilidad está destinada a generalizarse, ya que en estos casos no sirve de nada el típico consejo de hacer copias de seguridad.

«En la historia de la humanidad, nunca hasta ahora se ha sometido a la gente a una extorsión a tan enorme escala».

#### Pero ¿por qué los delincuentes privilegian este tipo de ataques?

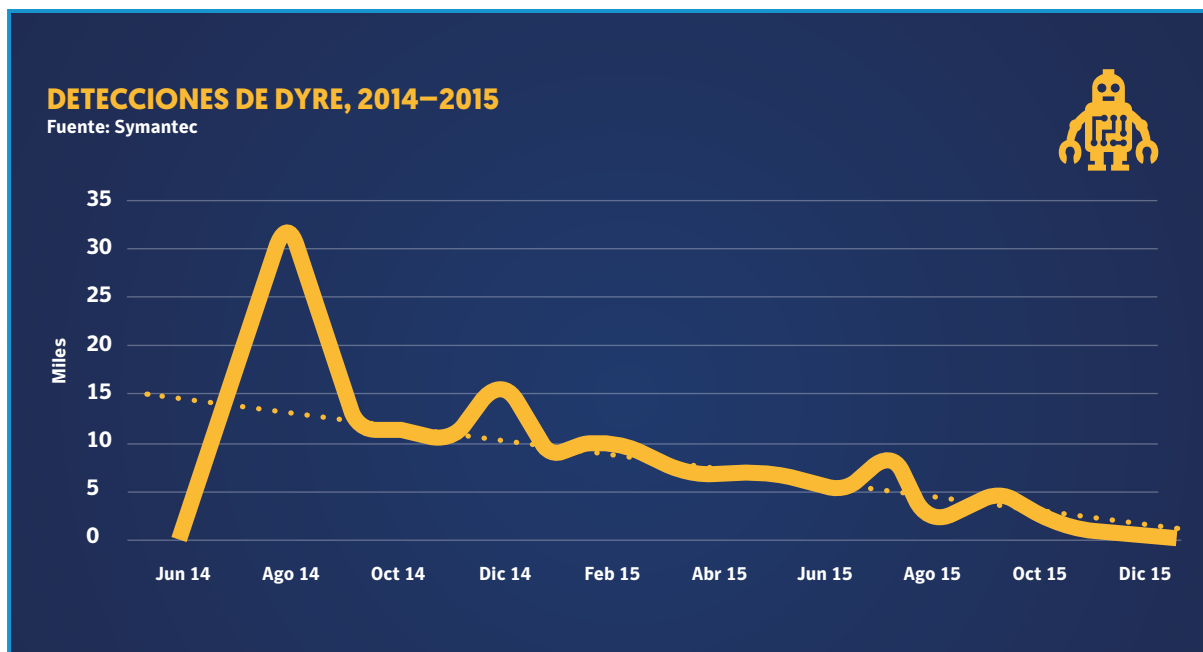
- Ante el exceso de oferta de datos robados en el mercado negro y la aparición en Estados Unidos del estándar EMV, que mejora la seguridad de los pagos con tarjeta, se han reducido las ganancias que se pueden conseguir mediante el robo de datos de tarjetas de crédito.
- Los fraudes con tarjetas de crédito implican la intervención de muchas personas y la legislación al respecto garantiza que la pérdida económica de la víctima sea mínima. En cambio, es muy fácil conseguir en el mercado negro un kit de herramientas de *ransomware* para atacar a las víctimas, que con toda probabilidad acabarán pagando. El delincuente no tendrá que gastar en los servicios de ningún intermediario y no hay ningún sistema que limite las pérdidas de la víctima, con lo que la ganancia será máxima.



<http://www.symantec.com/connect/blogs/how-my-tv-got-infected-ransomware-and-what-you-can-learn-it>  
<http://www.computerworld.com/article/3002120/security/new-ransomware-program-threatens-to-publish-user-files.html>  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-evolution-of-ransomware.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf)

## Consecuencias de Dyre

Después de que la policía cerrara varias *botnets* financieras muy importantes, *Dyre* ha ocupado su lugar.



Además de secuestrar navegadores web de uso habitual e interceptar sesiones de banca online para robar datos, *Dyre* también consiguió instalar *malware* en el ordenador de la víctima y, muchas veces, añadir el equipo en cuestión a la *botnet* del atacante.

En un principio, *Dyre* surgió como una de las operaciones de fraude financiero más peligrosas de todos los tiempos, ideada para estafar a los clientes de más de 1000 bancos y otras empresas de todo el mundo.

Sin embargo, los ciberdelincuentes que controlaban el troyano *Dyre* sufrieron un duro golpe tras una operación de seguridad rusa que tuvo lugar en noviembre. Tal como se destaca en el [blog Security Response](#), según la telemetría de Symantec el grupo prácticamente ha dejado de actuar. *Dyre* (detectado por Symantec como [Infostealer.Dyre](#)) se difundió mediante campañas por correo electrónico y, desde el 18 de noviembre de 2015, no se han observado mensajes de correo electrónico relacionados con *Dyre*. Poco después, se redujo drásticamente la cantidad de detecciones del

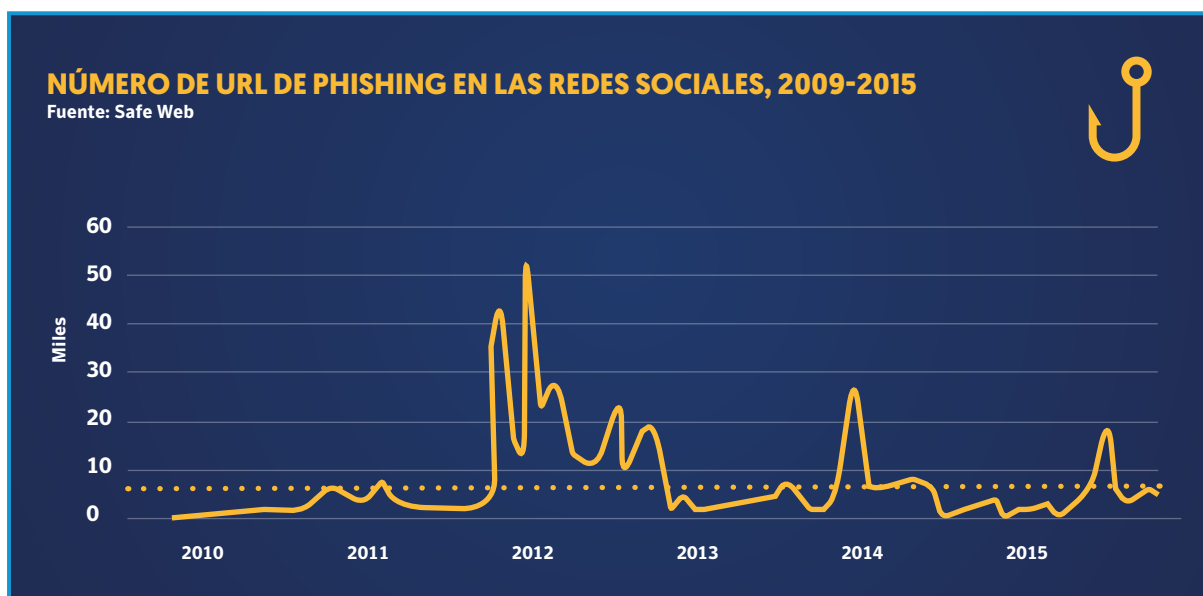
troyano *Dyre* y otro *malware* relacionado. Anteriormente, a principios de 2015, se calculaba que el número de infecciones al mes superaba las 9000, mientras que en noviembre del mismo año no llegaba a las 600.

### El idioma y la ubicación no constituyen obstáculos

Otros ataques perpetrados en 2015 también demuestran el grado de maldad y complejidad al que se puede llegar para hacer dinero. Independientemente de dónde viva y del idioma que hable, corre peligro de sufrir un ataque cibernético. Por ejemplo, baste pensar en *Boleto*, un sistema de pago que se utiliza solo en Brasil. A pesar de lo específico que es, este año han aparecido [tres tipos de malware](#) creados en especial para atacarlo.

En todo el mundo se están llevando a cabo ataques localizados similares, lo que demuestra que los ciberdelincuentes hacen todo lo posible por manipular a las víctimas estén donde estén y sea cual sea su idioma.

<http://www.symantec.com/connect/blogs/dyre-emerges-main-financial-trojan-threat>  
<http://www.symantec.com/connect/blogs/dyre-operations-bank-fraud-group-grind-halt-following-takedown>  
[http://www.symantec.com/security\\_response/writeup.jsp?docid=2014-061713-0826-99](http://www.symantec.com/security_response/writeup.jsp?docid=2014-061713-0826-99)  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/boleto-malware.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/boleto-malware.pdf)



En la tabla se muestra el papel crucial que han desempeñado las redes sociales en los ataques de ingeniería social del pasado. Durante los últimos años, estos sitios web han tomado medidas drásticas al respecto y ahora a los ciberdelincuentes les resulta mucho más difícil atacarlos.

Con los kits de herramientas de *phishing*, es facilísimo llevar a cabo una campaña en un país concreto y, a continuación, cambiar de plantilla para atacar a otro objetivo. Muchas veces el idioma utilizado en dichos ataques localizados se traduce automáticamente mediante las plantillas y, para un destinatario que no sea nativo, resulta suficientemente convincente.

### Leyes de privacidad

«A la gente no solo le interesa quién puede atacar, sino también quién puede filtrar información», explica Shankar Somasundaram, director ejecutivo de gestión de productos e ingeniería en Symantec.

En mayo de 2014 el eco la resolución del Tribunal de Justicia Europeo sobre el «derecho al olvido» se propagó entre quienes recopilan datos y, a finales de 2015, Google ya había recibido 348 085 solicitudes de eliminación de resultados de búsquedas.

Aunque muchos pensaban que esto solo resultaría ventajoso para quienes quisieran ocultar escándalos o evitar acusaciones, según las preguntas frecuentes de Google, entre las solicitudes más habituales se encontraban las que

pedían eliminar datos de contacto, direcciones postales o «contenido relativo únicamente a la salud, orientación sexual, raza, etnia, religión, y afiliación política y sindical de un individuo».

Además, este año el Tribunal de Justicia Europeo volvió a hacer que aumentara el interés de la opinión pública en la cuestión de la privacidad cuando declaró nulo el acuerdo de «puerto seguro» del año 2000. Según explicó Monique Goyens, directora general de la Organización de Consumidores Europea, esta resolución confirma que «un acuerdo que permite a las empresas estadounidenses declarar que respetan las normas de protección de datos de la Unión Europea sin que ninguna autoridad compruebe que eso es cierto no vale ni siquiera el papel en el que está escrito».

Tal como comentó en su momento el periódico The Guardian, tal vez esto «contribuya a evitar que el gobierno estadounidense acceda a datos de usuarios en manos de la Unión Europea» y «abra las puertas a más investigaciones, reclamaciones y juicios por parte de los usuarios y de las autoridades encargadas de cuestiones relativas a los datos».

[http://www.cio.com/article/3008661/google-receives-steady-stream-of-right-to-be-forgotten-requests.html#tk.rss\\_all](http://www.cio.com/article/3008661/google-receives-steady-stream-of-right-to-be-forgotten-requests.html#tk.rss_all)  
[http://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#common\\_delisting\\_scenarios](http://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#common_delisting_scenarios)  
[http://www.beuc.eu/publications/beuc-pr-2015-020\\_historic\\_victory\\_for\\_europeans\\_personal\\_data\\_rights.pdf](http://www.beuc.eu/publications/beuc-pr-2015-020_historic_victory_for_europeans_personal_data_rights.pdf)  
<http://www.theguardian.com/technology/2015/oct/06/safe-harbour-european-court-declare-invalid-data-protection>

A medida que proliferan las fugas de datos y que aumenta la parte de nuestra vida personal que tiene lugar en Internet, es probable que en 2016 aumente el interés judicial por la protección de la privacidad individual, así como la cantidad de normas sobre la cuestión.

En cuanto al mundo empresarial, hay que empezar a abordar la seguridad desde el punto de vista de la formación y la epidemiología. Todos los empleados tienen que colaborar para garantizar el buen estado de las tecnologías digitales, mientras que los directores informáticos y los

responsables de TI tienen que ser conscientes de los riesgos que corren y supervisar los síntomas de forma proactiva con el fin de diagnosticar las enfermedades digitales antes de que pongan en peligro los datos y la tranquilidad de los clientes.

Symantec cree firmemente en la confidencialidad y la defiende con uñas y dientes en todo el mundo. No deberíamos resignarnos a la idea errónea de que la privacidad ya no existe: al contrario, se trata de algo muy valioso que hay que proteger con atención.

### Evitemos la catástrofe cibernética

Según un informe de BofA Merrill Lynch Global, la ciberdelincuencia roba 575 000 millones de dólares al año a la economía global y, en una hipotética catástrofe cibernética de alcance universal, en 2020 podría llegar a llevarse un quinto del valor creado por Internet.

Nos corresponde a todos a hacer cuanto esté en nuestra mano por evitar que ocurra algo así.

En lo que se refiere a los consumidores, ha llegado el momento de abandonar las malas costumbres. Mucha gente conoce las normas básicas para garantizar la ciberseguridad y, sin embargo, más de un tercio de los estadounidenses que comparten contraseñas han revelado la que permite acceder a su cuenta bancaria online. Si queremos reforzar la seguridad en Internet, es imprescindible que todo el mundo asuma su parte de responsabilidad.

**LA CIBERDELINCUENCIA TIENE  
UN COSTE DE HASTA 575 000  
MILLONES DE DÓLARES AL AÑO  
PARA LA ECONOMÍA GLOBAL**

**575 000  
MILLONES DE DÓLARES**

[http://us.norton.com/cyber-security-insights?id=us\\_hho\\_nortoncom\\_clp\\_norton-hp-ribbon-award\\_nrpt](http://us.norton.com/cyber-security-insights?id=us_hho_nortoncom_clp_norton-hp-ribbon-award_nrpt)

## La víctima no es solo el dispositivo o la red, sino también la entidad que está detrás de la red

En resumen, los ataques tan frecuentes, persistentes y avanzados contra organismos gubernamentales y empresas de todos los tamaños constituyen una amenaza más grave para la seguridad y la economía nacionales. El número de vulnerabilidades de día cero ha aumentado y se sabe que se han utilizado como armas. Las campañas de spear-phishing se han vuelto más difíciles de detectar, pues se utilizan para atacar a menos individuos dentro de una menor cantidad de entidades previamente seleccionadas.

### Ataques persistentes

La importante fuga de datos que sufrió Anthem, el segundo proveedor de servicios sanitarios más grande de Estados Unidos, afectó a los historiales médicos de 78 millones de pacientes. El ataque salió a la luz en febrero de 2015 y, según averiguó Symantec, fue perpetrado por un grupo llamado Black Vine que cuenta con recursos económicos considerables y colabora con Topsec, una empresa de seguridad informática con sede en China. Black Vine utiliza *malware* avanzado hecho a medida para llevar a cabo campañas de ciberespionaje contra distintos sectores, como el aeroespacial y el de la energía.

Entre las víctimas de ciberespionaje del año 2015, también se encuentran la Casa Blanca, el Pentágono, el Bundestag alemán y la Oficina de Gestión del Personal del gobierno estadounidense, que perdió 21, 5 millones de archivos personales con datos confidenciales como historiales sanitarios y financieros, registros de detenciones e incluso huellas dactilares.

Todo esto se enmarca en una creciente oleada mundial de ataques de ciberespionaje avanzados, persistentes y dotados de importantes recursos. En el punto de mira de los espías se encuentran los secretos de Estado, la propiedad intelectual empresarial (como diseños, patentes y planos) y, tal como se ha observado en recientes fugas de datos, la información personal.

Las vulnerabilidades de día cero son especialmente valiosas para los atacantes. En el pasado hemos visto cómo han conseguido aprovecharlas para atacar un organismo gubernamental a través de un simple documento de Word infectado enviado por correo electrónico. Es más, son tan

interesantes para los delincuentes que estos hacen todo lo posible por evitar que salgan a la luz y mantener así su posición de ventaja. Por ejemplo, a veces los atacantes diseñan *malware* que se activa solo en un momento concreto o en ciertas zonas geográficas. De este modo, no lo descubren los expertos en seguridad que ejecuten el software en otro lugar o a otra hora.

Como las vulnerabilidades de día cero son una fuente de riqueza aparentemente tan difícil de conseguir, los delincuentes las protegen como oro en paño para poder usarlas más tiempo sin que nadie las detecte.

En los ataques *watering hole* avanzados, los sitios web afectados se activan solo cuando el visitante procede de una dirección IP en concreto. Al reducir así los daños colaterales, es menos probable que salga a la luz la vulnerabilidad. Es más, este sistema también dificulta la tarea de los expertos en seguridad que visiten el sitio web desde un lugar diferente. Cuando el proveedor interesado revela un ataque, con frecuencia estos sitios web infectados pasan a usar otra vulnerabilidad aún desconocida para seguir actuando sin que nadie se dé cuenta.

Symantec sigue investigando el troyano Regin y analiza las capacidades técnicas de los atacantes que cuentan con apoyo estatal. Así, se han detectado 49 nuevos módulos, cada uno de los cuales añade nuevas funciones como el registro de pulsaciones de teclas, el acceso a archivos y al correo electrónico, y una amplia infraestructura de control. Según nuestros analistas, el troyano Regin es tan avanzado y complejo que podría ser fruto de meses o incluso años de trabajo por parte de equipos de desarrolladores dotados de buenos recursos.

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-black-vine-cyberespionage-group.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf)  
<http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/>  
<http://www.wsj.com/articles/nsa-chief-says-cyberattack-at-pentagon-was-sophisticated-persistent-1441761541>  
<http://ca.reuters.com/article/technologyNews/idCAKBN002GA20150610>  
<http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/>  
<http://www.symantec.com/connect/blogs/regin-further-unravelling-mysteries-cyberespionage-threat>  
[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/regin-analysis.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf)

En la actualidad, los ataques de *spear phishing* y *watering hole* que utilizan sitios web infectados son los sistemas preferidos para llevar a cabo ataques dirigidos. De todos modos, a medida que una empresa añade capas de tecnología, se amplía también su superficie de ataque. Ahora que cada vez se utilizan más sistemas en la nube y que se van imponiendo los dispositivos del Internet de las cosas, prevemos que durante los próximos dos años los ataques dirigidos traten de aprovechar las vulnerabilidades de estas tecnologías. Con toda probabilidad, se empezará por atacar a los servicios en la nube especialmente vulnerables a ataques como la inyección SQL. Los atacantes se saldrán con la suya fácilmente mediante campañas de *spear phishing* que explotarán la seguridad insuficiente y los errores de configuración debidos a los usuarios, más que a los proveedores de servicios en la nube.

Para evitar ser detectadas, ahora las campañas de *spear phishing* son más numerosas pero afectan a menos individuos cada una. Es posible que muy pronto cada una ataque solo a un objetivo o a varios individuos concretos de una misma empresa. Por otro lado, las campañas de *spear phishing* de mayor envergadura probablemente se lleven a cabo con ataques *watering hole*, mediante sitios web infectados aprovechando codiciadas vulnerabilidades de día cero.

### VULNERABILIDADES DE DÍA CERO

Fuente: Symantec I SDAP, Wiki

2013	Cambio	2014	Cambio	2015
23	+4 %	24	+125 %	54

### Diversidad en las vulnerabilidades de día cero

En 2015 se detectaron 54 vulnerabilidades de día cero, una cifra sin precedentes que duplicaba la del año anterior. Es evidente que descubrir vulnerabilidades desconocidas y dar con la forma de aprovecharlas se ha convertido en una de las técnicas preferidas de los delincuentes más avanzados, y nada parece indicar que la tendencia vaya a cambiar.

**Las vulnerabilidades de día cero alcanzan precios muy altos en el mercado negro. Por este motivo y por su propia naturaleza, creemos que el número de vulnerabilidades de día cero detectadas no refleja la magnitud real del problema.**

La mayoría de las vulnerabilidades de día cero detectadas en 2015 se utilizaron contra tecnologías «de toda la vida» que sufren ataques desde hace años. A lo largo del año, los ciberdelincuentes acumularon diez vulnerabilidades de día cero contra Adobe Flash Player. También Microsoft despertó el interés de los malhechores, si bien las 10 vulnerabilidades de día cero que se estaban usando contra su software se distribuyeron mediante Microsoft Windows (6), Internet Explorer (2) y Microsoft Office (2). El sistema operativo Android también sufrió ataques con cuatro vulnerabilidades de día cero a lo largo de 2015.

### Grupos de ataque activos en 2015

Algunos de los grupos más destacados que llevaron a cabo ataques dirigidos en 2015 fueron los siguientes:

- **Black Vine:** grupo con sede en China que ha atacado principalmente a entidades de los sectores aeroespacial y sanitario, como Anthem y la Oficina de Administración de Personal (ambas estadounidenses), en busca de propiedad intelectual e identidades.
- **Rocket Kitten:** grupo iraní con apoyo estatal que lanza ataques de espionaje a periodistas, activistas defensores de los derechos humanos y científicos.
- **Cadelle and Chafer:** grupo iraní que ha atacado principalmente aerolíneas y empresas de los sectores de la energía y las telecomunicaciones en Oriente Medio, así como una empresa estadounidense.
- **Duke y Seaduke:** grupo con apoyo estatal que al parecer actúa desde 2010 y ataca principalmente a agencias gubernamentales europeas, individuos muy destacados, así como organizaciones de investigación privadas y de política internacional.
- **Emissary Panda:** grupo chino que ataca con el fin de robar propiedad intelectual a entidades de varios sectores (financiero, aeroespacial, inteligencia, telecomunicaciones, energía e ingeniería nuclear). Se lo conoce sobre todo por haber aprovechado la vulnerabilidad de día cero CVE-2015-5119, que salió a la luz en el ataque de Hacking Team.
- **Waterbug y Turla:** grupo ruso de espionaje que lanza ataques de *spear phishing* y *watering hole* contra embaixadas e instituciones gubernamentales. Se cree que lleva activo desde el año 2005.
- **Butterfly:** ataques a grandes empresas multimillonarias de varios sectores (TI, farmacéutico y materias primas), como Facebook y Apple, con el objetivo de obtener información privilegiada para aprovecharse en el mercado bursátil.

[http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/the-black-vine-cyberespionage-group.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-black-vine-cyberespionage-group.pdf)  
<http://www.symantec.com/connect/blogs/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets>  
<http://www.symantec.com/connect/blogs/forkmeiamfamous-seaduke-latest-weapon-duke-armory>  
[https://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/waterbug-attack-group.pdf](https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf)  
<http://www.symantec.com/connect/blogs/butterfly-profiting-high-level-corporate-attacks>  
<http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats>



## Terror global, ataques locales

«Los ciberdelincuentes se están volviendo más profesionales y más osados en cuanto a las víctimas que eligen y las cantidades de dinero que manejan», comenta Stephen Doherty, analista sénior de información sobre amenazas de Symantec.

Ahora que se acercan las elecciones presidenciales de Estados Unidos, han circulado mensajes de correo no deseado que utilizan como cebo el tema de las primarias para infectar al destinatario con *malware*. Los ciberdelincuentes que recurren al spam saben jugar con las emociones y las reacciones viscerales de los destinatarios recurriendo a temas como los eventos globales, la crisis de los refugiados de Oriente Medio, la inmigración, la política exterior, la economía e incluso el terrorismo.

En una campaña reciente de correo no deseado llevada a cabo en Oriente Medio y Canadá, los malhechores se hacían pasar por agentes de policía y recomendaban a los destinatarios que descargasen supuestas soluciones de seguridad, que en realidad no eran más que *malware*. Todos los nombres utilizados correspondían a funcionarios reales en activo y, en muchos casos, en el asunto del mensaje aparecía el nombre de un empleado de la empresa atacada.

Para que un ataque de este tipo resulte convincente, es necesario investigar previamente, como hizo este grupo antes de enviar los mensajes de *phishing*. Además, como no tenían los datos de los empleados, en primer lugar enviaron mensajes a otras personas de la empresa, como el personal informático o de atención al cliente.

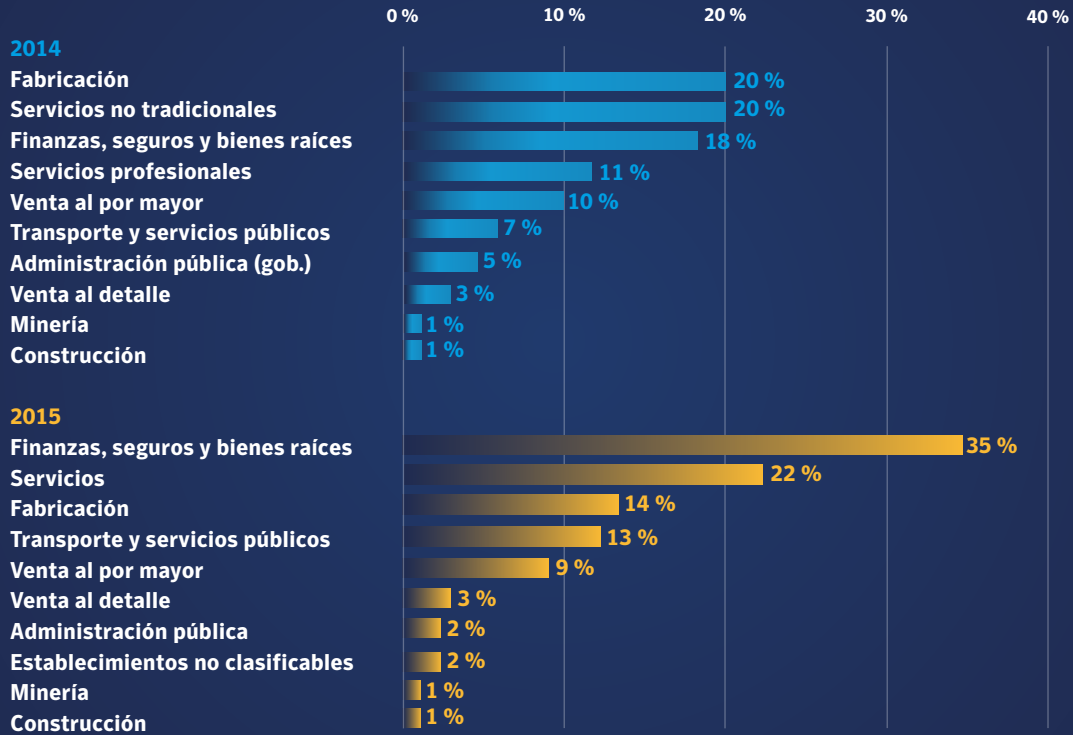
Este nivel tan avanzado de investigación y localización, que podría exigir la intervención de cientos de personas, se está volviendo cada vez más habitual en las estafas con botnets. La economía sumergida no consiste solo en vender bienes robados, sino que constituye todo un sector con organizaciones y profesionales tan preparados como los que cabe esperarse de las empresas legítimas. Y como ocurre en otros muchos sectores, las economías con más futuro, como la china, llegan pisando fuerte.

## El efecto mariposa

Butterfly (literalmente, mariposa) es un grupo de *hackers* muy bien organizados y con una excelente preparación que se dedican a espiar a las empresas con el objetivo de aprovecharse en el mercado bursátil, ya sea vendiendo datos confidenciales o realizando ellos mismos operaciones con información privilegiada. Los primeros ataques de este tipo que se conocen tuvieron lugar en 2013 y afectaron a empresas tan famosas como Apple, Microsoft y Facebook. De todos modos, los delincuentes suelen tomar medidas estratégicas para no dejar rastro, como el uso de servidores de control virtuales cifrados. El hecho de que estos *hackers* aprovechen vulnerabilidades de día cero revela un nivel de complejidad nunca visto hasta ahora en los ataques realizados con fines comerciales.

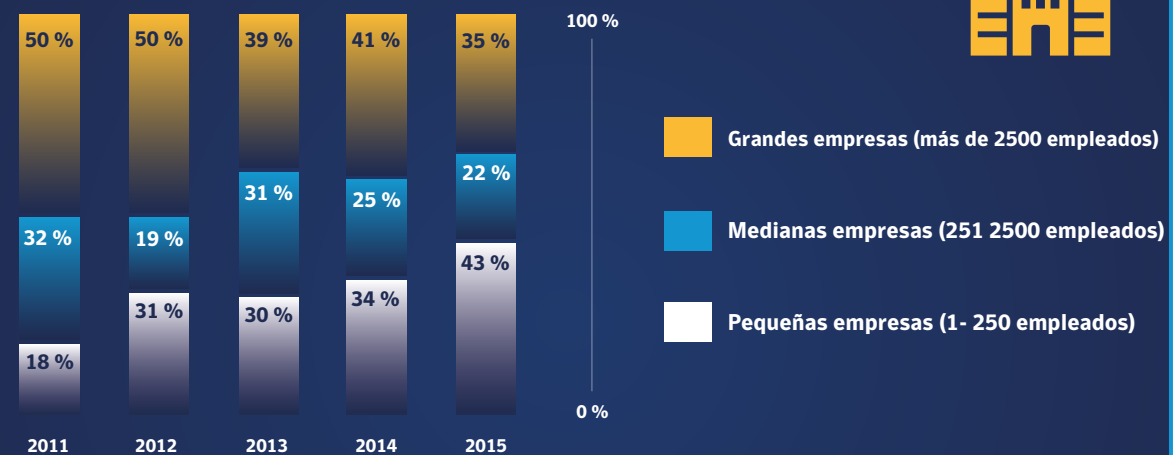
### LOS 10 SECTORES MÁS ATACADOS CON SPEAR PHISHING (2014-2015)

Fuente: Symantec I cloud



### ATAQUES DE SPEAR PHISHING SEGÚN EL TAMAÑO DE LA EMPRESA ATACADA (2011-2015)

Fuente: Symantec I cloud



## Ciberseguridad, cibernegros y ciberespionaje

Si el ciberespionaje avanzado está tan extendido, resulta curioso que no lo esté el cibernegros. Lo que se necesita para infligir daños físicos es similar a lo que se usa en el ciberespionaje, y la cantidad de potenciales víctimas está aumentando gracias a la proliferación de dispositivos con conexión a Internet, incluidos los sistemas de control industrial.

En su análisis de seguridad y defensa de 2015, el gobierno británico resume con claridad los desafíos actuales:

«La gama de ciberdelincuentes que amenazan al Reino Unido se ha ampliado. El peligro es cada vez más asimétrico y global. Por lo general, para defenderse de forma constante y fiable, se necesitan competencias avanzadas y una inversión considerable. Pero cada vez más países están desarrollando, con recursos estatales, capacidades avanzadas que se podrían utilizar en conflictos, incluso contra la infraestructura nacional crítica y las instituciones gubernamentales. Por otro lado, los actores no estatales, como los terroristas y los ciberdelincuentes, pueden conseguir con facilidad tecnología e instrumentos cibernéticos y utilizarlos con fines destructivos».

El uso de Stuxnet contra el programa nuclear iraní es el ejemplo más conocido de ataque cibernético contra una infraestructura física. Es posible que ya se hayan llevado a cabo con éxito más ataques que aún no han salido a la luz o que haya más infecciones en curso por ahora inactivas. En cualquier caso, parece improbable que la infraestructura crítica mundial sea inmune a estas amenazas. De hecho, a finales de 2014, una planta siderúrgica alemana fue víctima de lo que parece un aviso de futuros ataques que podrían ser más graves.

## La escasa visibilidad no es la solución

La forma más eficaz de protegerse del ciberespionaje es, sencillamente, ser consciente del peligro. Cualquier empresa podría ser víctima de un ataque dirigido que recurra a técnicas de watering hole o abrevadero y spear phishing. El hecho de ser pequeña o poco conocida no reduce su vulnerabilidad.

Así es, pues en 2015 las pequeñas empresas sufrieron un mayor porcentaje (43 %) de ataques de spear phishing, pero disminuyó su probabilidad de ser atacadas. Es decir, se produjeron más ataques contra ese tipo de víctimas, pero se centraron en un número de empresas menor (3 %).

En cambio, el 35 % de los ataques de spear phishing fueron contra grandes empresas, y 1 de cada 2,7 (el 38 %) estuvieron en el punto de mira de los delincuentes al menos una vez. Estos datos parecen indicar que se lanzaron campañas más masivas a una escala mucho mayor.

Una vez reconocido el riesgo, las empresas pueden tomar medidas para protegerse: revisar sus planes de seguridad y de respuesta a las incidencias, pedir consejo y ayuda si fuera necesario, actualizar sus defensas técnicas, implantar programas de formación y políticas de personal eficaces, y estar siempre al día de las novedades.



## PRÓXIMAMENTE: WSTR 2016, SEGUNDA PARTE

PARTE 2

# WSTR

INFORME SOBRE  
LAS AMENAZAS PARA  
LA SEGURIDAD DE  
LOS SITIOS WEB 2016

En la segunda parte de nuestro exhaustivo informe sobre amenazas para la seguridad de los sitios web, examinamos las nuevas y siniestras formas de ataque a las que recurren los ciberdelincuentes. Además, analizamos a fondo la rápida proliferación de los ataques DDoS, que cada vez tienen mayor alcance, y comentamos las nuevas oportunidades que brinda a los delincuentes el Internet de las cosas.

La respuesta del sector a estas nuevas amenazas ha sido alentadora, pero todavía se puede hacer más. Descubra cómo está reaccionando el sector e infórmese sobre nuestros consejos y prácticas recomendadas para garantizar la seguridad de los sitios web.

**EN LAS PRÓXIMAS SEMANAS LE ENVIAREMOS LA  
SEGUNDA PARTE DEL WSTR 2016: NO SE LA PIERDA.**

Si desea los números de teléfono de algún país en concreto, consulte nuestro sitio web.

**Para obtener información sobre productos, llame al:**

900 931 298 o al +353 1 793 9076

**Symantec España**

Symantec Spain S.L.

Parque Empresarial La Finca – Somosaguas

Paseo del Club Deportivo, Edificio 13, oficina D1, 28223

Pozuelo de Alarcón, Madrid, España

[www.symantec.es/ss](http://www.symantec.es/ss)

Queda prohibida la reproducción total o parcial de este documento técnico sin el consentimiento previo por escrito de su autor.

Copyright © 2016 Symantec Corporation. Reservados todos los derechos. Symantec, el logotipo de Symantec, el logotipo de la marca de comprobación, Norton Secured y el logotipo de Norton Secured son marcas comerciales o marcas comerciales registradas en los Estados Unidos y en otros países por Symantec Corporation o sus filiales. Los demás nombres pueden ser marcas comerciales de sus respectivos propietarios