Symantec

PARTE 2

WSTR

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

ÍNDICE

Vectores de ataque

Ataques web, kits de herramientas y explotación de vulnerabilidades online 3
Linux en la línea de ataque 3
Complementos problemáticos 4
- Se acerca el fin para Flash 4
- Explotación de complementos para servidores web 4

Infección por inyección 4
Kits de herramientas de ataque web 5
Las estafas mediante servicios de asistencia técnica recurren al kit
Nuclear para difundir ransomware 6
Denegación de servicio distribuida 7
- El peligro de los ataques DDoS 7
- Sencillo pero eficaz 9
- Las aplicaciones web cada vez corren más peligro 11

¿Qué dispositivos pueden acabar en una botnet? 12
Publicidad dañina 13
En el cliente 14
Smartphones y otros dispositivos móviles 14
- Un teléfono por persona 14
- Amenazas transversales 14
- Los ataques a dispositivos Android se han vuelto más furtivos 17
- Los usuarios de Android, víctimas del phishing y el ransomware 17
- Ahora los usuarios de Apple iOS corren más riesgo que nunca 17

Protección de los dispositivos móviles 17
¿Qué nos depara el futuro? 18

Amenazas por correo electrónico y otros sistemas de comunicación 18
- Ataques por correo electrónico 18
- *Spam* 19
- *Phishing* 19
- Propagación de malware por correo electrónico 19
- El cifrado del correo electrónico 21
- Ataques que eluden el cifrado 21
- Consejos para garantizar la seguridad al usar el correo electrónico 21

¿Qué nos depara el futuro? 21

Los ordenadores, la informática en la nube y la infraestructura de TI 22
- Sistemas virtualizados y en la nube 23
- Vulnerabilidades en la nube 23
- Protección de la infraestructura de TI 23

Proteja la información esté donde esté 24

La respuesta del sector

La evolución del cifrado 25
Las cifras de la solidez 25
Control y equilibrio 26
El salto a la tecnología SSL Always-On 26
Mayor sensación de seguridad 27

Consejos y prácticas recomendadas

Adopte los estándares del sector 28
Utilice la tecnología SSL/TLS correctamente 28
Adopte una solución completa para la seguridad de los sitios web 28
Conciencie a sus empleados 29
Proteja los dispositivos móviles 29
La seguridad es responsabilidad de todos 29

Vectores de ataque

Ataques web, kits de herramientas y explotación de vulnerabilidades online

Si los servidores web están desprotegidos, también lo están los sitios web que se alojan en ellos y las personas que los visitan. Los delincuentes aprovechan cualquier vulnerabilidad para atacar los sitios web y hacerse con el control de sus servidores host.

Sitios web analizados que presentaban vulnerabilidades
Fonte: Symantec | Trusted Services

2015	Diferencia	2014	Diferencia	2013
78 %	+2 % pts.	**76 %**	-1 % pts.	**77 %**

Porcentaje de vulnerabilidades críticas

2015	Diferencia	2014	Diferencia	2013
15 %	-5 % pts.	**20 %**	+4 % pts.	**16 %**

Una vulnerabilidad crítica es aquella que, en caso de ser explotada, podría hacer que se ejecutara código malicioso sin necesidad de la interacción de un usuario, lo cual podría desembocar en una fuga de datos y poner en peligro a los internautas que visiten los sitios web afectados.

Como siempre, las cifras confirman que los propietarios de los sitios web no instalan las revisiones y actualizaciones en sus sitios web y servidores con la frecuencia que deberían.

Linux en la línea de ataque

En 2015 hemos observado una oleada de uso de *malware* contra Linux, el sistema operativo más habitual en los servidores de los sitios web, entre otros servicios de Internet esenciales

Con frecuencia los ciberdelincuentes contaminan los servidores web afectados con código que lleva a kits de herramientas de ataque, o bien envían mensajes de correo electrónico no deseados y roban nombres de usuario y contraseñas. Además, muchas veces utilizan dichos servidores web como trampolín para seguir causando estragos: por ejemplo, mediante ataques DDoS de gran envergadura, aprovechando que el ancho de banda de un proveedor de alojamiento es mucho mayor que el de un usuario doméstico con una conexión de banda ancha.

Últimamente están proliferando los kits de herramientas de ataque automatizadas y especializadas, que buscan sistemas de gestión de contenidos desprotegidos y otras aplicaciones web en peligro. De este modo, ayudan a los ciberdelincuentes a detectar servidores potencialmente vulnerables y facilitan los ataques a sistemas Linux.

Cómo proteger el servidor

- Manténgalo al día con las actualizaciones y revisiones necesarias.
- Utilice varias capas de seguridad, de forma que si una falla queden otras para proteger distintas áreas del sistema.
- Implante sistemas de detección y prevención de intrusiones en la red y supervise los servicios de correo electrónico que se ejecutan en el servidor.
- Utilice un buen *firewall* y revise periódicamente los registros de acceso para detectar actividades sospechosas.
- Instale un software antivirus, que bloqueará el *malware* que detecte.
- Haga copias de seguridad fuera de las instalaciones.

http://www.symantec.com/connect/tr/blogs/phishing-economy-how-phishing-kits-make-scams-easier-operate

En 2015 también se detectó *ransomware* utilizado contra Linux, en concreto en ciertos archivos con extensiones asociadas a aplicaciones web. Además, el programa cifraba los archivos y directorios que contenían la palabra «backup», con lo que causaba estragos en especial si la víctima no había hecho copias de seguridad fuera de las instalaciones.

Complementos problemáticos

De todos modos, los sistemas operativos no son los únicos que ponen en peligro los servidores web. Si bien durante los últimos años los principales proveedores de sistemas de gestión de contenidos han mejorado sus defensas y han implantado las actualizaciones automáticas, sus complementos siguen constituyendo un grave problema para la seguridad.

Se acerca el fin para Flash

En 2015 aumentó el número de vulnerabilidades de los complementos de Adobe, lo que indica que los atacantes están intentando explotar complementos que se utilicen no solo en varias plataformas, sino prácticamente en todas. La mayoría de las vulnerabilidades de Adobe guardaban relación con Adobe Flash Player (también conocido como Shockwave Flash).

Adobe Flash Player ha sufrido ataques constantemente a lo largo de los años y en 2015 dio origen a 10 vulnerabilidades de día cero (17 %), mientras que en 2014 fueron doce (50 %) y en 2013, cinco (22 %). Como ofrece ganancias tan suculentas, es evidente por qué a los ciberdelincuentes les gusta tanto atacar la tecnología Flash. Apple, Google y Mozilla han expresado su preocupación con respecto al complemento Flash, y tanto Google como Mozilla han anunciado recientemente que Chrome y Firefox dejarán de admitir Flash de forma nativa.

Desde el punto de vista de la seguridad, prevemos que durante el próximo año paulatinamente se vaya dejando de usar Adobe Flash.

Explotación de complementos para servidores web

No solo los complementos para navegadores son vulnerables y sufren ataques. Por ejemplo, baste pensar en WordPress, que hoy se utiliza en la cuarta parte de los sitios web de todo el mundo.

Cualquiera puede crear un complemento de WordPress, con lo que hoy existen complementos de todo tipo, desde los más útiles hasta los más ridículos, como Logout Roulette: «cada vez que se carga una página de administración, existe una posibilidad entre diez de que se cierre la sesión».

Cómo reducir los riesgos que suponen los complementos

- Actualice los complementos periódicamente.
- Consulte las noticias y las listas de seguridad para tener en cuenta las advertencias.
- Para reducir la superficie de ataque, instale solo los complementos realmente útiles.

El problema es que ciertos complementos presentan un nivel de inseguridad sorprendente. Windows es un blanco de ataque frecuente porque cuenta con muchos usuarios, y lo mismo ocurre con WordPress: sus complementos son posibles objetivos y los delincuentes no dejarán escapar esta oportunidad.

Infección por inyección

En 2015 regresó Team GhostShell, que reivindica el ataque de una cantidad considerable de sitios web. En un informe reciente de este mismo año, el equipo de intervenciones de seguridad de Symantec comenta:

«Según las primeras impresiones, la lista de sitios web atacados que se ha publicado recientemente parece aleatoria, los delincuentes no se concentran en un país o sector en especial. Con toda probabilidad, el grupo elige los sitios web que atacar según su vulnerabilidad. Si ha mantenido su anterior modus operandi, seguramente haya infectado las bases de datos mediante la inyección de SQL y los scripts PHP mal configurados».

Una vez más, probablemente estos ataques se podrían haber evitado con una mejor gestión de los servidores y los sitios web. La inyección SQL es un método que se utiliza desde hace mucho tiempo y que sigue funcionando debido a la innecesaria debilidad de los parámetros que establecen los administradores para las consultas.

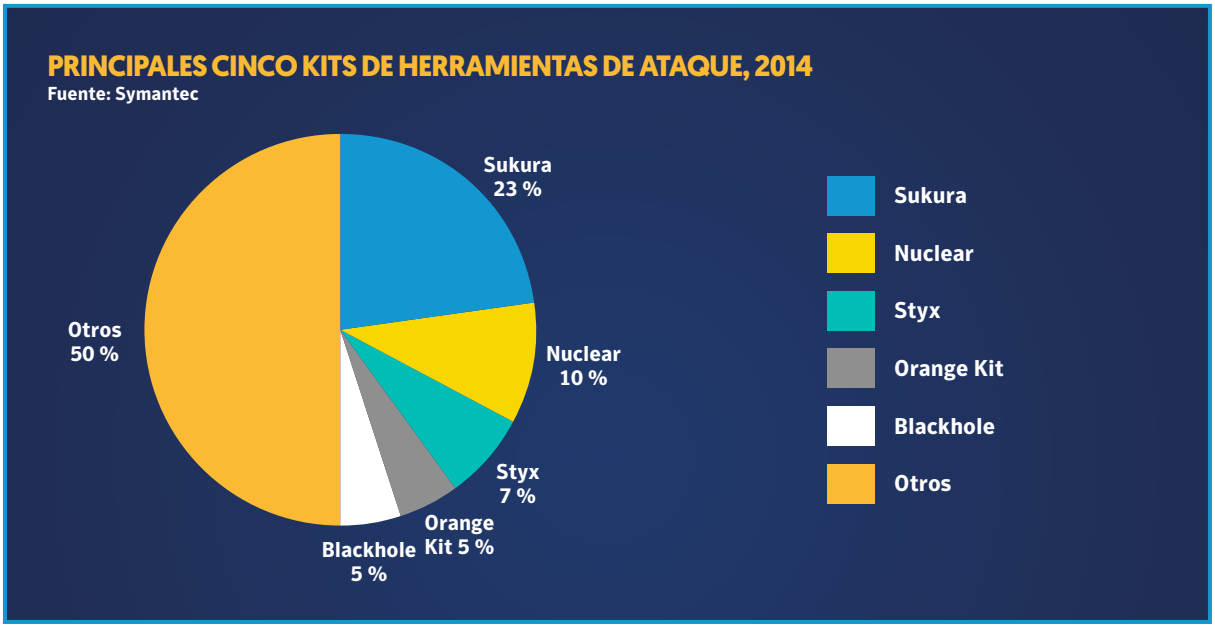
Hay que actualizar periódicamente los complementos, independientemente de que sean para navegadores o para servidores, ya que son proclives a los fallos de seguridad, y las versiones obsoletas se deberían evitar en la medida de lo posible.

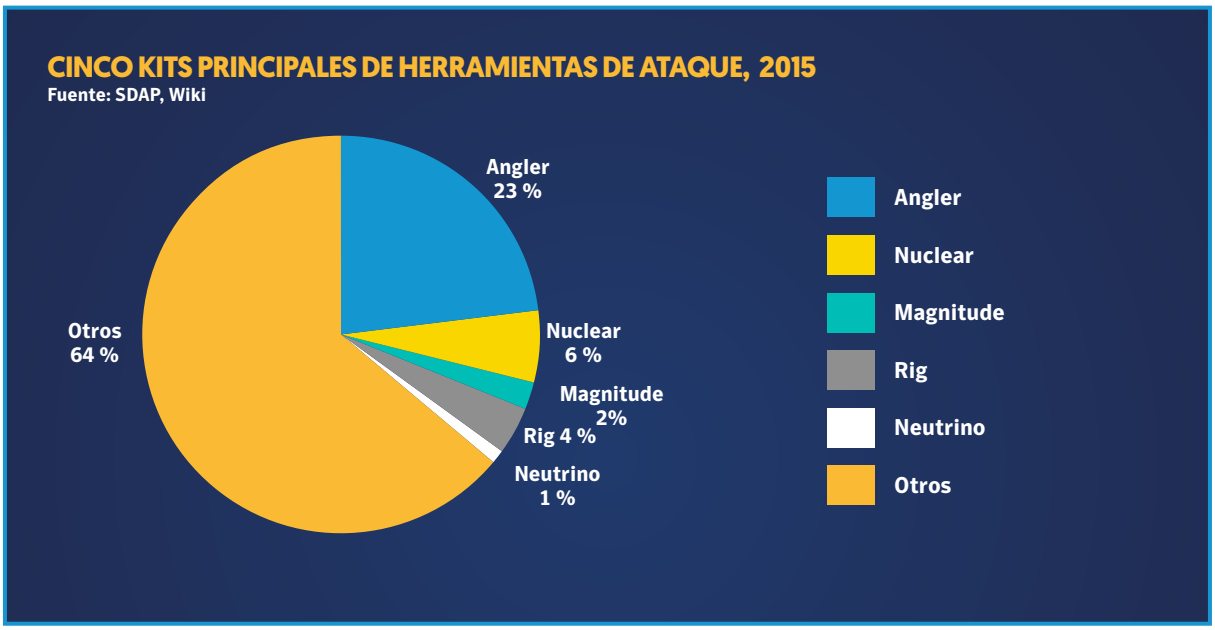
https://www.symantec.com/security_response/writeup.jsp?docid=2015-110911-5027-99
http://w3techs.com/blog/entry/wordpress-powers-25-percent-of-all-websites
https://wordpress.org/plugins/logout-roulette/
http://www.symantec.com/connect/blogs/team-ghostshell-hacking-group-back-bang

Kits de herramientas de ataque web

Es difícil defenderse de las vulnerabilidades nuevas y desconocidas, en especial las de día cero, para las cuales tal vez no existan revisiones de seguridad, y los atacantes hacen todo lo posible por aprovecharlas antes de que los proveedores implanten las revisiones.

Tras el ataque que sufrió en 2015 Hacking Team, una empresa con sede en Italia, salieron a la luz vulnerabilidades de día cero desconocidas hasta entonces y, en cuestión de horas, se integraron en kits de herramientas de ataque.





http://www.symantec.com/connect/blogs/hacking-team-woes-adds-dangers-faced-internet-using-public

El kit de ataque más activo en 2015 fue Angler, y Symantec bloqueó a diario cientos de miles de ataques lanzados con dicho kit, 19,5 millones de ataques en total. El mecanismo de distribución favorito de Angler fue la publicidad maliciosa, con cierta predilección por las vulnerabilidades de Adobe Flash. En 2015 Windows fue la víctima preferida de Angler: en concreto, Windows 7 fue el objetivo del 64 % de los ataques de Angler; y Windows 8.1, del 24 %. Por otro lado, en 2015 Mac OS X no parecía estar en la línea de combate para los atacantes que utilizaban Angler, pero es probable que esto cambie ahora que los ciberdelincuentes tratan de atacar el ecosistema de Apple.

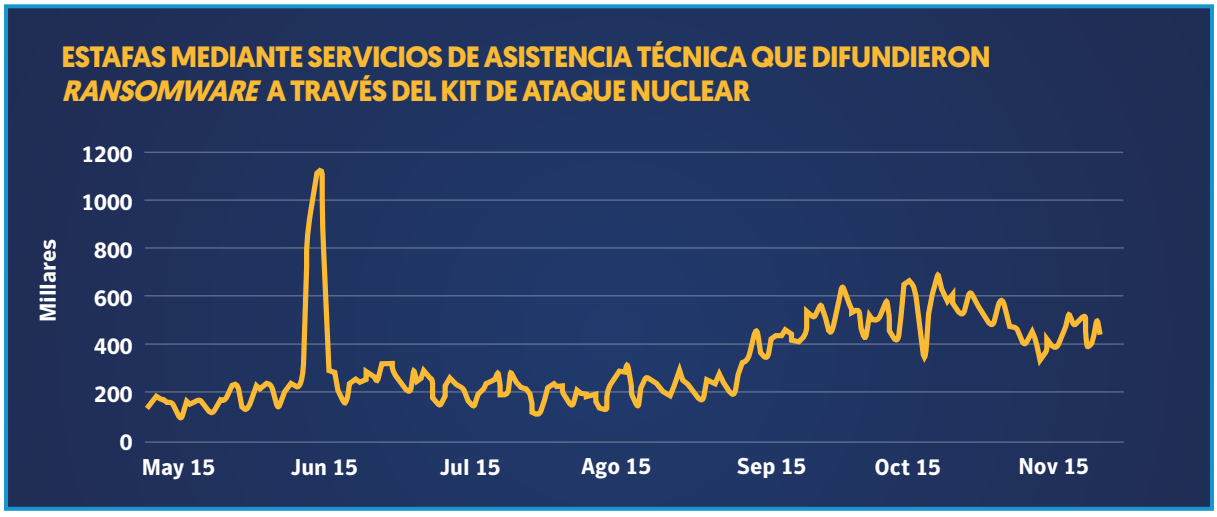
Las estafas mediante servicios de asistencia técnica recurren al kit Nuclear para difundir *ransomware*

En 2015, Symantec registró un aumento del 200 % con respecto al año anterior en el número de estafas mediante servicios de asistencia técnica.

Este tipo de ataques no son nuevos, y cientos de miles de personas en todo el mundo los sufren a diario. Las primeras estafas de este tipo consistían en llamadas por parte de teleoperadores en las que estos trataban de vender paquetes de asistencia técnica a los usuarios para resolver problemas (en realidad inexistentes) que supuestamente había en los ordenadores de las potenciales víctimas.

Con el tiempo, estas estafas han evolucionado y recientemente ha habido casos de mensajes de aviso falsos prácticamente interminables en los que se insta a las potenciales víctimas a llamar a un número gratuito para obtener asistencia. Si llaman, responde una persona aparentemente profesional que trata de convencer al usuario para que instale un software que supuestamente solucionará los problemas, pero en realidad se trata de *malware* y otras aplicaciones indeseadas.

La última novedad ha sido el uso del kit de ataque Nuclear para colocar *ransomware* en los equipos de las víctimas. Los estafadores distraen al usuario mientras el *ransomware* cifra los archivos del ordenador, tratando así de aumentar la probabilidad de que la víctima pague un rescate.



http://www.symantec.com/connect/blogs/what-symantec-s-intrusion-prevention-system-did-you-2015

Si bien no era la primera vez que se usaba *ransomware* en estafas mediante servicios de asistencia técnica, en los casos más recientes se ha añadido un iframe de HTML malicioso en el sitio web que redirigía a los internautas a un servidor en el que se alojaba el kit de ataque Nuclear. Se descubrió que este kit aprovechaba la reciente vulnerabilidad de ejecución de código remoto no especificada de Adobe Flash Player (CVE-2015-7645), entre otras. Si el ataque salía bien, se instalaba Trojan.Cryptowall (*ransomware*) o Trojan.Miuref.B (un troyano que roba información).

Esta ha sido la primera vez que Symantec ha detectado estafas mediante servicios de asistencia técnica combinadas con el kit de ataque Nuclear para distribuir *ransomware* y, si este sistema resulta ser eficaz, sin duda la tendencia continuará. Si bien es plausible que los estafadores de servicios de asistencia técnica y los atacantes que utilizan el kit hayan unido sus fuerzas, también puede ser que los servidores web de los estafadores hayan sido atacados por otro grupo que utilizara el kit de ataque Nuclear. En total, el año pasado Symantec bloqueó más de 100 millones de estafas realizadas mediante servicios de asistencia técnica. Los países más afectados por este tipo de estafas fueron Estados Unidos, Reino Unido, Francia, Australia y Alemania.

Denegación de servicio distribuida

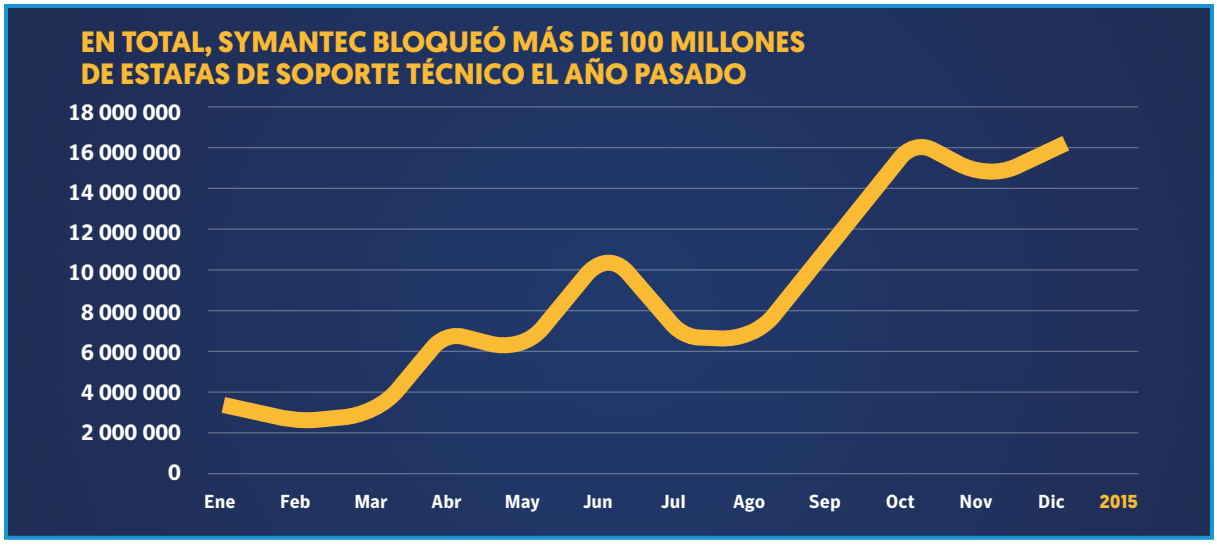
Los ataques de denegación de servicio distribuida (DDoS) se están volviendo más graves y duraderos a medida que aumenta la popularidad de las *botnets* de alquiler y que el Internet de las cosas proporciona más carne de cañón a los ejércitos de dichas redes.

El peligro de los ataques DDoS

Ciertos ataques DDoS aún brindan a los delincuentes numerosas oportunidades para enriquecerse, ya que permiten dañar el sitio web de una empresa con el objetivo de llevar a cabo extorsiones y chantajes. A veces, a la víctima no le queda más remedio que pagar el rescate. Sin embargo, la posibilidad de rastrear el dinero pone las cosas más difíciles a los atacantes, y las tecnologías de mitigación de DDoS hacen que necesiten un ancho de banda cada vez mayor para hacer mella en las víctimas. A pesar de todo, últimamente en algunos de los ataques más graves han intervenido grupos de «hacktivistas» y, a veces, personas que actúan en nombre de algún Estado.

Un ejemplo destacado es el reciente ataque a la BBC, que el 31 de diciembre dejó fuera de combate durante horas el sitio web y sus correspondientes servicios, incluido iPlayer. Según New World Hacking, se trata del ataque DDoS más grave de la historia. La organización anti-Estado Islámico reivindicó su responsabilidad porque el gran alcance de la BBC permitía poner a prueba sus capacidades y el grupo asegura que el ataque llegó a alcanzar los 602 Gbps.

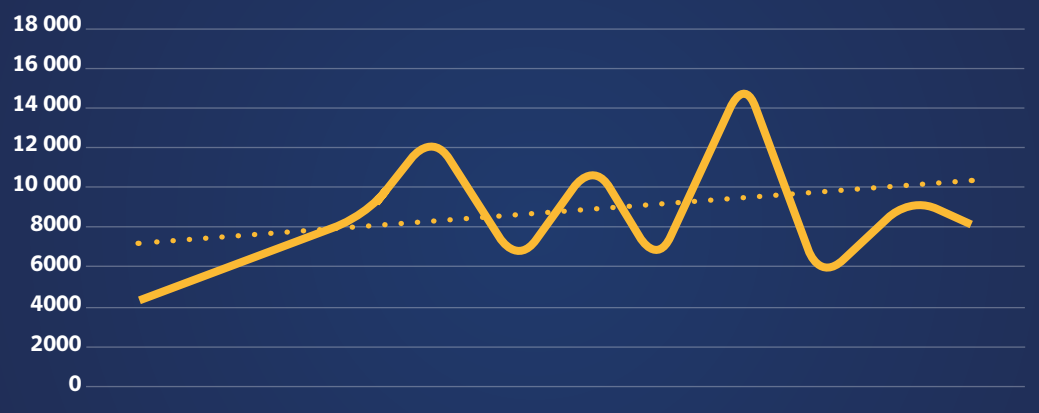
De todos modos, los ataques DDoS también reportan beneficios, como la posibilidad de chantajear a la víctima pidiendo un rescate a cambio de interrumpir el ataque. En 2015 la DDoS también se ha utilizado a veces como herramienta de distracción combinada con ciertos tipos de ataques dirigidos: cuando el equipo de TI descubría que el sitio web de la empresa había sido invadido, pensaba que pronto llegaría la exigencia de pagar un rescate, pero en realidad en ese mismo momento se estaba llevando a cabo otro ataque más furtivo sin que nadie se diera cuenta.



http://www.symantec.com/connect/blogs/when-tech-support-scams-meet-ransomlock
http://www.symantec.com/connect/blogs/tech-support-scams-redirect-nuclear-ek-spread-ransomware
https://www.symantec.com/security_response/vulnerability.jsp?bid=77081
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99
https://www.symantec.com/security_response/writeup.jsp?docid=2015-032402-2413-99
http://www.bbc.co.uk/news/technology-35204915
http://www.techradar.com/news/internet/attack-against-bbc-website-was-the-biggest-volley-of-ddos-fire-ever-seen--1312864
http://www.americanbanker.com/news/bank-technology/banks-lose-up-to-100khour-to-shorter-more-intense-ddos-attacks-1073966-1.html?pg=1
https://www.symantec.com/security_response/writeup.jsp?docid=2014-061923-2824-99

VOLUMEN DE ATAQUES DDOS DETECTADO POR SYMANTEC GLOBAL INTELLIGENCE NETWORK, 2015

Fuente: Symantec | DeepSight



En el gráfico se aprecia cómo aumentó la cantidad de ataques DDoS en el segundo semestre del año, antes de disminuir drásticamente en noviembre y diciembre. En 2015 hubo más picos de actividad, conforme los ataques se volvieron más breves y discretos.

CINCO ATAQUES PRINCIPALES DE DDOS DETECTADOS POR SYMANTEC GLOBAL INTELLIGENCE NETWORK

Fuente: Symantec | DeepSight

Puesto	Ataques de 2015	Porcentaje en 2015	Ataques de 2015	Porcentaje en 2014
1	Ataque ICMP Flood genérico	85,7 %	Ataque de amplificacion de DNS	29,44 %
2	Ataque DDoS TCP Syn Flood genérico	6, 4 %	Ataque CMP Flood genérico	17,20 %
3	Ataque DDos Pig Broadcast (Smurf) genérico	2,1 %	Ataque DDos Pig Broadcast (Smurf) genérico	16,78 %
4	Ataque DDoS Teardrop/Land Denial genérico	2,0 %	Ataque DDoS Teardrop/Land Denial genérico	7,17 %
5	Ataque DDoS RFProwl genérico	0,6 %	Ataque DDoS ICMP inaccesible genérico	5,71 %

La mayoría de los ataques DDoS consistieron en avalanchas de ICMP, por lo general mediante envíos masivos de solicitudes de *ping* que sobrecargan el objetivo hasta impedirle gestionar el tráfico legítimo.

https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

Sencillo pero eficaz

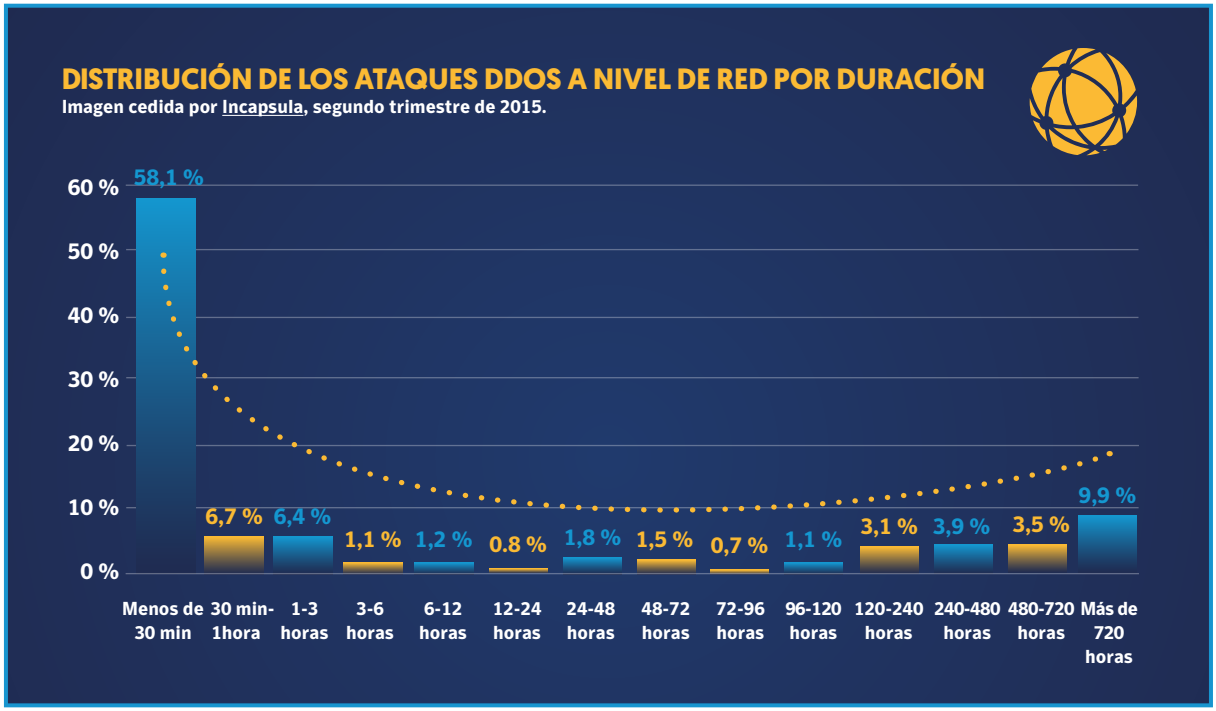
¿Por qué son tan frecuentes los ataques DDoS? La respuesta hoy es la misma que en 2002, cuando hablamos de ellos por primera vez: se configuran fácilmente, resulta difícil detenerlos y causan estragos por naturaleza, sobre todo ahora que proliferan las *botnets* de alquiler.

Según Incapsula, un socio de Symantec, en el segundo trimestre de 2015 aproximadamente el 40 % de los ataques DDoS llevados a cabo en la capa de la red se realizaron con *botnets* de alquiler. A veces los delincuentes se toman la molestia de infectar varios dispositivos vulnerables y crear su propia botnet para luego lanzar el ataque DDoS, pero con frecuencia resulta mucho más fácil alquilar para un periodo de tiempo determinado *botnets* ya preparadas.

Los precios en el mercado negro no sufrieron grandes cambios durante el año: el coste de un ataque DDoS oscila entre los 10 y los 1000 dólares al día.

En cambio, el coste para la empresa atacada es mucho más alto, tal vez hasta mil veces mayor, según la naturaleza del negocio y la importancia del sitio web. En consecuencia, la ganancia que puede conseguir un delincuente compensará con creces el coste del ataque.

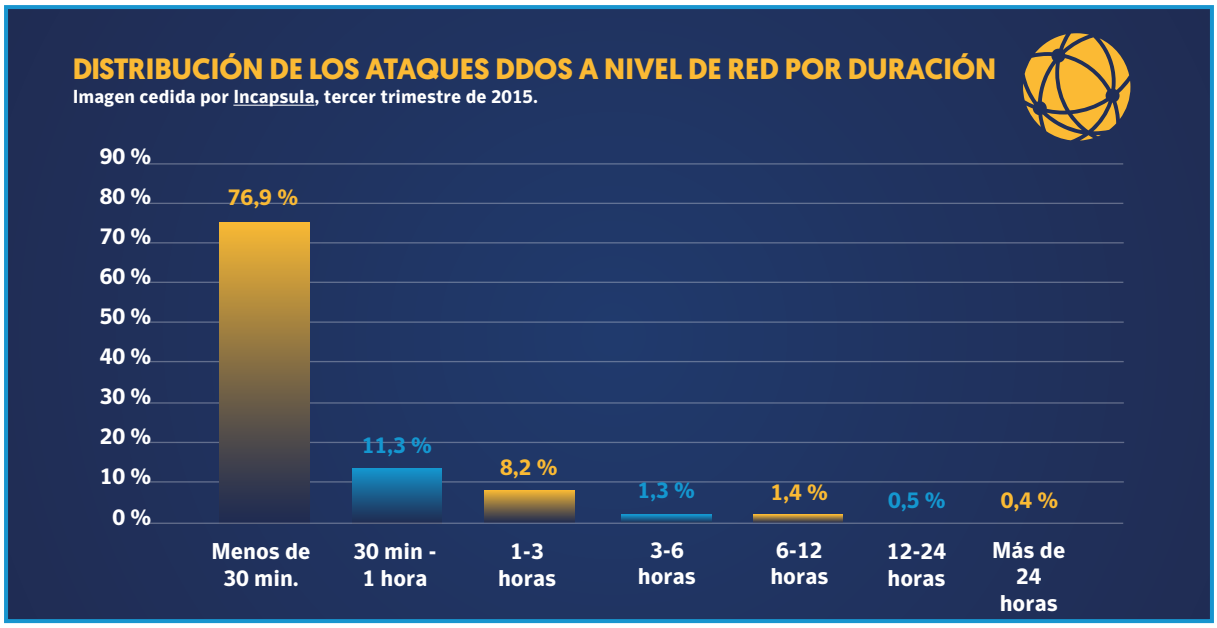
Esta difusión de los ataques relámpago parece indicar que se está recurriendo con más frecuencia a los ataques DDoS ofrecidos como servicio, consistentes en conceder a los suscriptores un acceso limitado a los recursos de la *botnet*, que se comparten con otros suscriptores. Por lo general, de este modo se logra llevar a cabo unos cuantos ataques breves de media envergadura. Además, con este sistema los atacantes descubren hasta qué punto es eficaz la infraestructura de su objetivo a la hora de mitigar los ataques y si tienen que aumentar el volumen. Según los informes de Incapsula, se han generalizado los ataques de más de 100 Gbps y se ha mitigado un ataque de estas características un día sí y otro, no.



En el gráfico se aprecia que, a finales del segundo trimestre de 2015, seguía habiendo una cantidad considerable de ataques DDoS que duraban horas, días, semanas o incluso meses.

http://www.symantec.com/connect/articles/barbarians-gate-introduction-distributed-denial-service-attacks
https://www.incapsula.com/blog/ddos-global-threat-landscape-report-q2-2015.html
http://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-data-malware-and-attack-services

Como se aprecia en el siguiente gráfico, entre el segundo y el tercer trimestre de 2015, el aumento de popularidad de los ataques DDoS como servicio ha ido acompañado de una reducción considerable en la duración de los ataques en la capa de la red. Dado que lanzar un ataque DDoS es ilegal, en ocasiones estos servicios de DDoS de alquiler se presentan como herramientas para realizar pruebas de esfuerzo en el servidor.



Tal como se aprecia en el gráfico, a finales del tercer trimestre prácticamente ya no se producían ataques DDoS que durasen más de un día: no llegaban al 0,5 %.

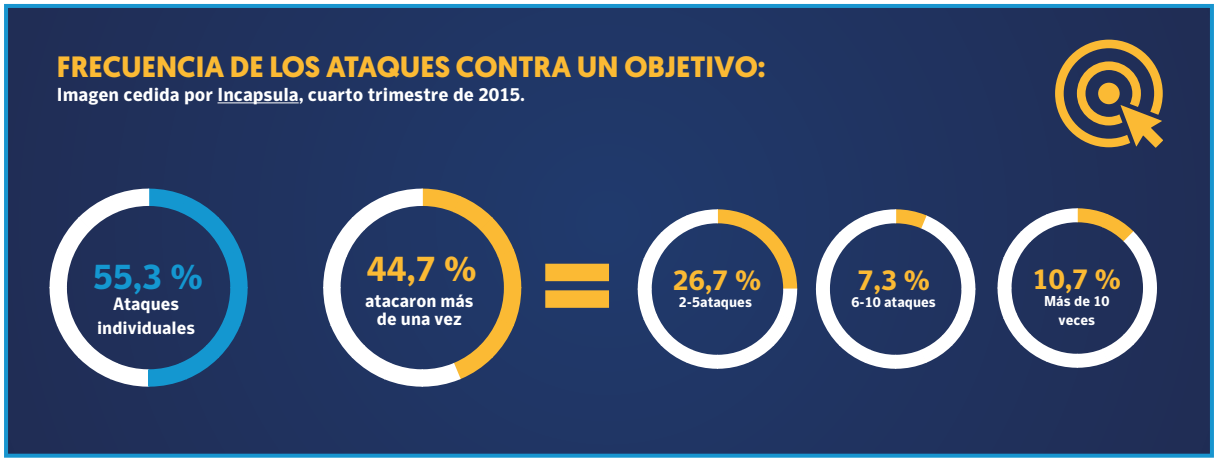
Si bien los ataques cada vez duran menos porque se tiende a preferir las ráfagas de ataques breves, su cantidad cada vez es mayor, tal como ha observado Incapsula, que ha registrado un increíble aumento del 138,8 % en la frecuencia de los ataques a redes en el segundo semestre de 2015.

Las aplicaciones web cada vez corren más peligro

De modo similar a lo que ha ocurrido con los ataques realizados en las capas de la red, también los lanzados contra aplicaciones se han vuelto más breves sin perder ni un ápice de tenacidad. El mayor ataque a la capa de la aplicación mitigado en el cuarto trimestre de 2015 fue una ráfaga muy breve e intensa que alcanzó las 161 300 solicitudes por segundo.

Por un lado, este dato nos recuerda que los ataques DDoS constituyen un problema general que afecta a todo el ecosistema de Internet. Por el otro, demuestra lo fácil que resulta lanzar un ataque de proporciones considerables a la capa de la aplicación, pues bastan unos cuantos dispositivos infectados para generar un tráfico capaz de bloquear un sitio web de tamaño medio durante un largo periodo de tiempo.

En consecuencia, en el cuarto trimestre de 2015 siguieron siendo frecuentes los ataques repetidos en la capa de las aplicaciones: el 44,7 % de los objetivos fueron atacados más de una vez; y el 18 %, más de cinco veces.



https://www.incapsula.com/blog/ddos-report-q4-2015.html

¿Qué dispositivos pueden acabar en una *botnet*?

Las *botnets* desempeñan un papel clave en los ataques DDoS, independientemente de que sean alquiladas o creadas por los propios atacantes. Cuanto mayor sea su tamaño, más solicitudes se podrán enviar al mismo tiempo y más daños sufrirá la víctima.

Pero los ordenadores infectados no son los únicos que ofrecen a los delincuentes un ejército de robots. En octubre se utilizó *malware* contra una serie de servidores MySQL, que ofrecen un ancho de banda mucho mayor que los objetivos convencionales, lo que permite llevar a cabo ataques DDoS contra otros sitios web. Este método no es nuevo, pero demuestra que los delincuentes van a seguir creando *botnets* cada vez más grandes y de mejor calidad.

Otro fenómeno observado en el año 2015 fue el aumento en el uso del Internet de las cosas (o IoT, por sus siglas en inglés) para fortalecer las *botnets*. En concreto, las cámaras de circuito cerrado de televisión se utilizaron con especial frecuencia, probablemente porque constituyen uno de los dispositivos más habituales del Internet de las cosas: en 2014 había en todo el mundo 245 millones de cámaras de videovigilancia operativas instaladas profesionalmente.

Es probable que en el futuro los delincuentes utilicen cada vez más dispositivos vulnerables del Internet de las cosas para lanzar ataques DDoS de gran alcance. Es cierto que existen soluciones para defenderse de los ataques DDoS, pero las empresas también se encuentran con nuevas dificultades a la hora de garantizar la seguridad en dispositivos que no son tradicionales, algo imprescindible si quieren evitar que se conviertan en parte del problema.

Tal vez sea aún más preocupante el hecho de que, sin los debidos sistemas de seguridad, será aún más difícil descubrir que una impresora, frigorífico, termostato o tostadora ha acabado en una *botnet* global tóxica.

SIN LOS DEBIDOS SISTEMAS DE SEGURIDAD, SERÁ AÚN MÁS DIFÍCIL DESCUBRIR QUE UNA IMPRESORA, FRIGORÍFICO, TERMOSTATO O TOSTADORA HA ACABADO EN UNA *BOTNET* GLOBAL TÓXICA.

http://www.symantec.com/connect/blogs/mysql-servers-hijacked-malware-perform-ddos-attacks
https://www.incapsula.com/blog/cctv-ddos-botnet-back-yard.html
https://technology.ihs.com/532501/245-million-video-surveillance-cameras-installed-globally-in-2014
http://www.imperva.com/Products/DDosProtection

Publicidad dañina

En la parte central de 2015, prácticamente todos los segmentos de Internet que se financian con publicidad se han visto afectados por cuentas de publicidad dañina. Una posible explicación es que la publicidad dañina permite infectar a los visitantes de un sitio web con más facilidad que el envío masivo de enlaces a sitios web infectados. Para un delincuente resulta mucho más fácil intentar atacar un sitio web famoso o colocar publicidad dañina en sitios web con mucho tráfico, porque no necesitan tener en cuenta todos los complejos matices de la ingeniería social y «los malos» se ahorran un paso más.

Las empresas de publicidad no suelen pedir mucha información a quienes envían anuncios, con lo que a los delincuentes les resulta fácil hacerse pasar por empresas legítimas y cargar anuncios dañinos, que podrán aparecer en numerosos sitios web.

Además, gracias al uso de cookies, los creadores de *malware* pueden adaptar su código malicioso o redireccionamientos para atacar prácticamente al subconjunto de usuarios que quieran, ya sea por ámbito geográfico, hora del día, empresa, intereses o actividad reciente en Internet.

Como se sabe, por desgracia la publicidad dañina es difícil de detectar y los delincuentes cada vez son más astutos, hasta el punto de que, después de una o dos horas, eliminan el código malicioso de los anuncios, que se vuelve casi invisible. Como es tan eficaz y difícil de analizar, «es previsible que el uso de la publicidad dañina siga aumentando. En consecuencia, es posible que la mayor demanda de herramientas de bloqueo de anuncios contribuya a reducir los efectos negativos de la publicidad dañina».

SITIOS WEB EXPLOTADOS CON MÁS FRECUENCIA, 2014-2015

Fuente: Symantec | SDAP, Safe Web, Rulespace

Puesto	Categorías más explotadas en 2015	Porcentaje	Categorías más explotadas en 2014	Porcentaje
1	Tecnología	**23,2 %**	Tecnología	**21,5 %**
2	Negocios	**8,1 %**	Alojamiento web	**7,3 %**
3	Búsquedas	**7,5 %**	Blogs	**7,1 %**
4	Blogs	**7,0 %**	Negocios	**6,0 %**
5	Dínamicas	**6,4 %**	Anonimizador	**5,0 %**
6	Educativas	**4.0 %**	Entretenimiento	**2,6 %**
7	Parking de dominios	**3,2 %**	Compras	**2,5 %**
8	Entretenimiento	**2,6 %**	Ilegal	**2,4 %**
9	Compras	**2,4 %**	Parking de dominios	**2.2 %**
10	Ilegal	**2,1 %**	Comunidad virtual	**1.8 %**

En 2015, la mayoría del contenido malicioso y de la publicidad dañina afectó a sitios web relacionados con tecnologías y negocios.

http://www.symantec.com/connect/blogs/malvertising-campaign-targets-brazilian-users

En el cliente

Smartphones y otros dispositivos móviles

En pocas palabras, los smartphones cada vez son un objetivo más atractivo para los ciberdelincuentes. En consecuencia, estos están invirtiendo en ataques más avanzados que sean más eficaces a la hora de robar datos personales valiosos y extorsionar a las víctimas. Aunque los usuarios de Android son el principal objetivo, en 2015 también hubo ataques contra dispositivos Apple, y los dispositivos 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).

Un teléfono por persona

Según el seguimiento realizado por IDC de las ventas mundiales de teléfonos móviles por trimestre, «en 2015 se compraron más de 1400 millones de smartphones en el mundo, lo que supone un aumento del 10 % con respecto al año anterior, cuando se vendieron 1300 millones» (27 de enero de 2016). Cinco de cada seis teléfonos nuevos funcionan con Android, y uno de cada siete utiliza el sistema operativo iOS de Apple (IDC, cuotas de mercado de los sistemas operativos de los smartphones, segundo trimestre de 2015). Según el fabricante de móviles Ericsson, a finales del año 2020 el número de smartphones registrados podría llegar a los 6400 millones, lo que equivale a casi uno por persona.

Además, las tabletas y los teléfonos de alta gama cuentan con procesadores potentes y, gracias a la red 4G, disponen de conectividad de banda ancha. También contienen datos personales muy valiosos. Por ejemplo, en 2015 llegó al mercado Apple Pay, y pronto aparecerán otros sistemas de pago móviles del mismo tipo. Todos estos factores hacen que se trate de dispositivos muy atractivos para los delincuentes.

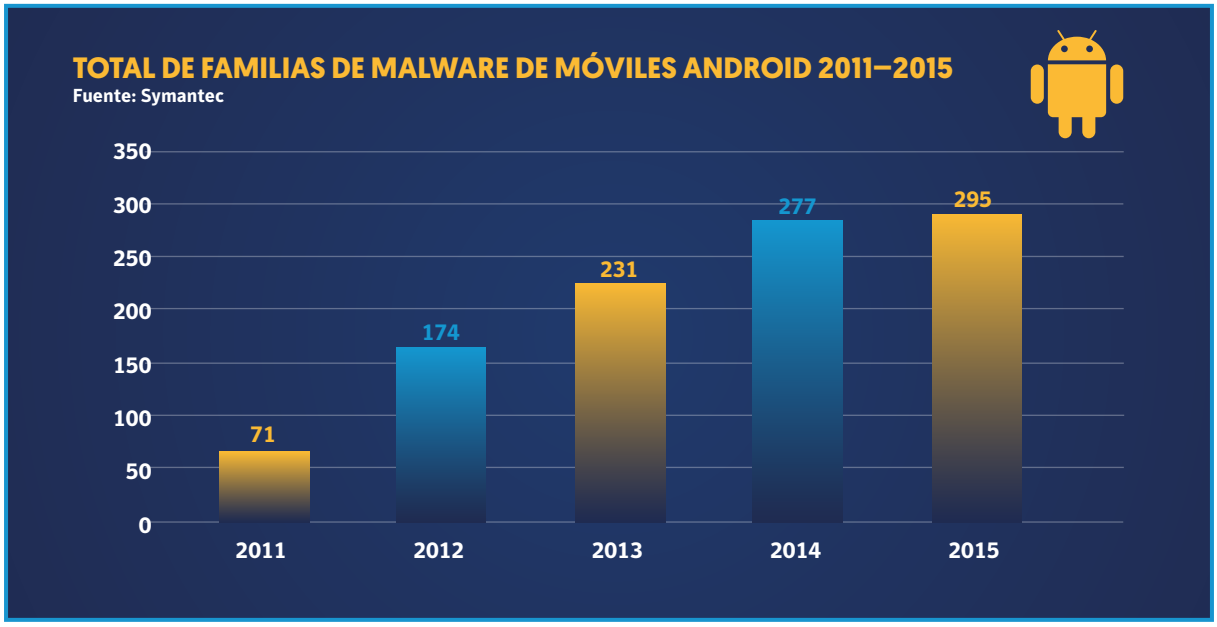
Amenazas transversales

Muchas tiendas de aplicaciones permiten a los usuarios navegar, comprar aplicaciones e instalarlas a distancia desde su equipo de sobremesa, lo que brinda a los delincuentes una oportunidad de oro. Por ejemplo, con Google Play, los clientes pueden navegar desde su ordenador con normalidad e instalar las aplicaciones directamente en el teléfono. Recientemente ha habido casos de *malware* en Windows que han aprovechado este sistema: una vez infectado el equipo de sobremesa, se han robado las cookies del navegador para sesiones de Google Play, que prácticamente son las credenciales de los usuarios, con lo que permiten a los ciberdelincuentes hacerse pasar por el usuario para instalar aplicaciones a distancia en los teléfonos y las tabletas de las víctimas sin que estas lo sepan ni lo autoricen.

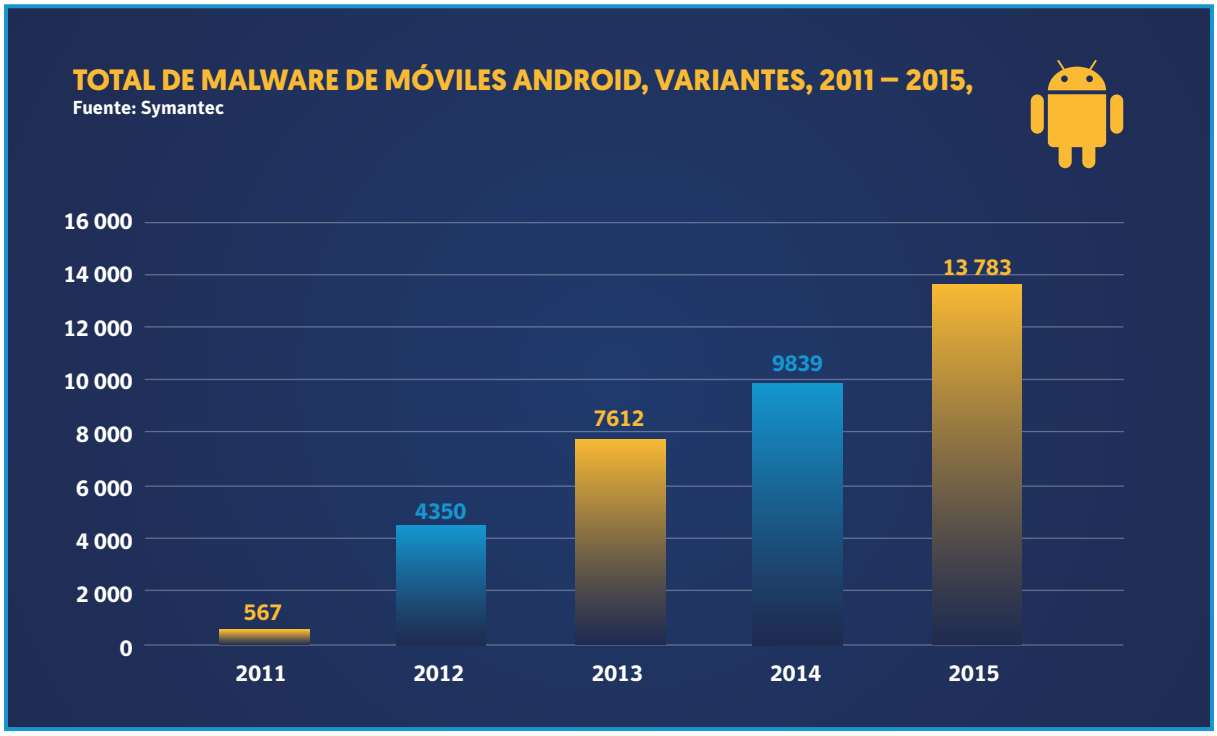
ANÁLISIS DE APLICACIONES DE SYMANTEC NORTON MOBILE INSIGHT
Fuente: Symantec | SDAP

	2015	2014	2013
Total de aplicaciones analizadas	10,8 millones	6,3 millones	6,1 millones
Total de aplicaciones clasificadas como *malware*	3,3 millones	1 millón	0,7 millones
Total de aplicaciones clasificadas como *grayware*	3 millones	2,3 millones	2,2 millones
Total de grayware clasificado como *madware*	2,3 millones	1,3 millones	1,2 millones
Definición de *malware*	Programas y archivos creados para causar daños, como virus, gusanos y troyanos.		
Definición de *grayware*	Programas que no contienen virus y no son claramente maliciosos pero pueden resultar molestos o incluso dañinos para el usuario [por ejemplo, herramientas de ataque, herramientas de acceso (*accessware*), programas espía (*spyware*), publicidad no deseada (*adware*), marcadores y programas de broma].		
Definición de *madware*	Técnicas agresivas para colocar publicidad en el calendario y los álbumes fotográficos de un dispositivo móvil y para insertar mensajes en la barra de notificación. El *madware* puede llegar incluso a sustituir un tono por un anuncio.		

http://www.idc.com/getdoc.jsp?containerId=prUS40980416
http://www.idc.com/prodserv/smartphone-os-market-share.jsp
http://www.ericsson.com/mobility-report
https://www.census.gov/population/international/data/idb/worldpopgraph.php



La cantidad de tipos de *malware* utilizados contra Android en 2015 aumentó un 6 %, mientras que el año anterior el crecimiento había sido del 20 %.

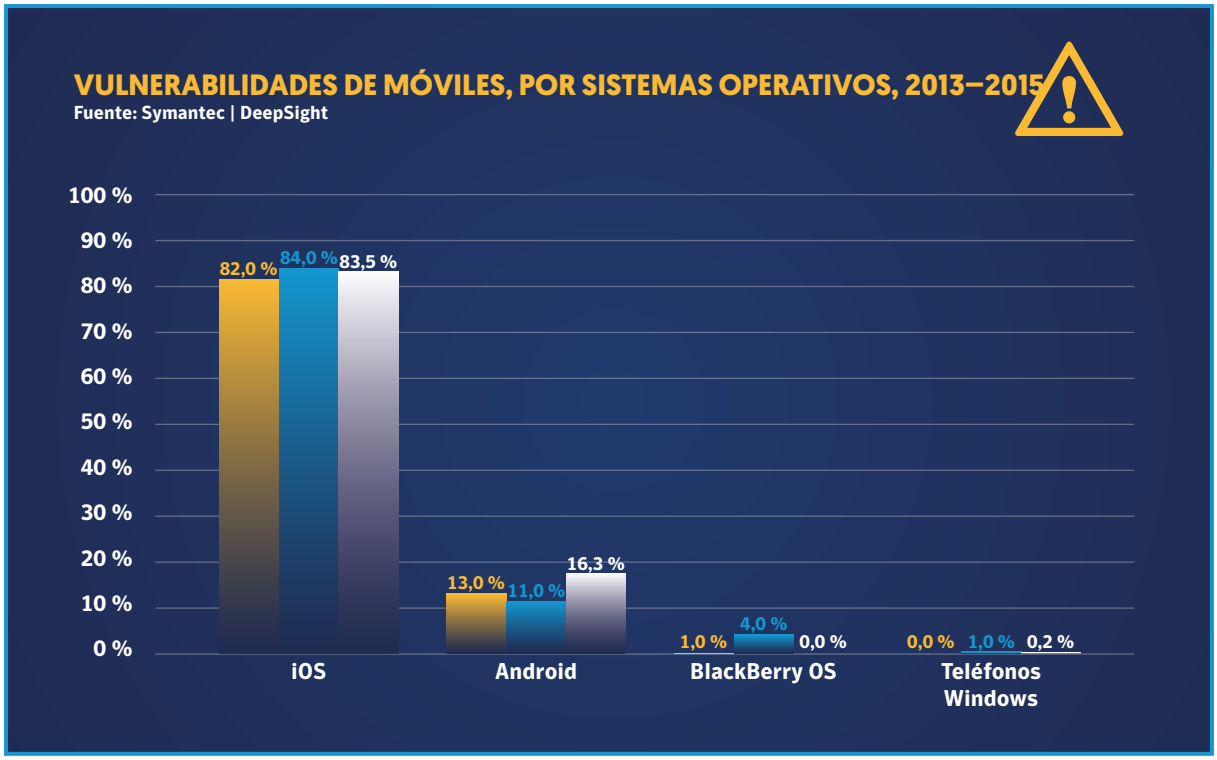


Por otro lado, el volumen de variantes de Android aumentó un 40 % en 2015, mientras que el año anterior había crecido un 29 %.

Durante los últimos tres años, no ha dejado de aumentar el número de vulnerabilidades de los sistemas móviles. A diferencia de lo que ocurre con los dispositivos Android, las vulnerabilidades de iOS han sido clave para acceder a los teléfonos con iOS, en especial a los que se han sometido a *jailbreaking*, proceso que permite a un usuario instalar aplicaciones no autorizadas en el Apple Store, eludiendo el sistema de seguridad de iOS. En cambio, resulta mucho más difícil atacar un dispositivo en el que no se haya practicado *jailbreaking*, pues en ese caso la aplicación que se quiera instalar se tendrá que descargar del App Store. Los procesos de control de Apple son conocidos por su rigor, motivo por el que la cantidad de software malicioso utilizado contra iOS es mucho menor que la del *malware* para Android.

En 2012, IOS.Finfish se convirtió en el primer caso de aplicación iOS maliciosa detectada en el Apple Store. Finfish permitía robar datos contenidos en el dispositivo atacado. En 2014 apareció OSX.Wirelurker, que atacaba aprovechando las conexiones USB a un equipo Mac o PC, para luego instalar aplicaciones en dispositivos iOS que no se hubieran sometido a *jailbreaking*.

Sin embargo, en 2015 se descubrió la posibilidad de utilizar XcodeGhost y YiSpecter contra dispositivos iOS sin necesidad de que el sistema atacado presentara vulnerabilidades ni se hubiera sometido a *jailbreaking*.



Durante los últimos años, la mayor parte de las vulnerabilidades detectadas en sistemas móviles se han encontrado en la plataforma iOS, y ha habido un gran interés por realizar jailbreaking en los dispositivos o instalar *malware*.

http://www.symantec.com/security_response/writeup.jsp?docid=2012-083015-4511-99&tabid=2
https://www.symantec.com/security_response/writeup.jsp?docid=2014-110618-0523-99

Los ataques a dispositivos Android se han vuelto más furtivos

El *malware* usado contra Android cada vez es más difícil de detectar. Por ejemplo, los creadores de *malware* empezaron a camuflar el código para eludir el software de seguridad basado en firmas antes de lanzar sus ataques y actualmente existe *malware* que comprueba si se está ejecutando en teléfonos auténticos o en el tipo de emuladores que utilicen los expertos en seguridad.

Los usuarios de Android, víctimas del *phishing* y el *ransomware*

Además de los trucos de siempre como vender aplicaciones falsas que no son lo que prometen, ahora los atacantes recurren a técnicas más avanzadas para sacar dinero a sus víctimas. Por ejemplo, los expertos de Symantec han descubierto un nuevo troyano utilizado para lanzar ataques de *phishing* en Android que muestra una página de inicio de sesión falsa superpuesta a las aplicaciones de banca online legítimas, para conseguir así que los usuarios les revelen sus credenciales bancarias. Asimismo, el *ransomware* para Android más reciente imita el estilo de Google para parecer más legítimo e intimidatorio al mostrar falsos avisos del FBI en las pantallas de bloqueo. Otra novedad reciente es el uso de *ransomware* para cifrar archivos (por ejemplo, fotografías), en lugar de simplemente para cambiar el PIN de acceso al teléfono.

Ahora los usuarios de Apple iOS corren más riesgo que nunca

Gracias al rigor con el que Apple controla su sistema operativo y su tienda de aplicaciones, las amenazas contra los iPhones y iPads han sido poco frecuentes y de alcance limitado, pero en 2015 la situación cambió:

- En 2015 se detectaron nueve gamas nuevas de amenazas para iOS, mientras que hasta entonces solo se conocían cuatro en total.
- El software para desarrolladores de contrabando denominado XcodeGhost infectó 4000 aplicaciones.
- El *malware* YiSpecter eludió la tienda de aplicaciones gracias al marco de distribución de aplicaciones empresarial.
- Los expertos en seguridad encontraron Youmi incrustado en 256 aplicaciones iOS. Se trata de un software utilizado para mostrar anuncios publicitarios, pero también envía datos personales a una ubicación remota sin el consentimiento de los usuarios.
- Las vulnerabilidades detectadas en AirDrop, el sistema inalámbrico de transferencia de archivos de Apple, podrían permitir a un atacante instalar *malware* en un dispositivo Apple.

Conforme aumenta la cantidad de iPads y iPhones que vende Apple, probablemente interesarán cada vez más a los ciberdelincuentes, en parte porque sus propietarios disponen (por término medio) de mayores ingresos. Tanto las empresas como los particulares deberían abandonar la idea de que los dispositivos Apple son inmunes a los ataques.

El *ransomware* llega a los dispositivos móviles

Imagínese la frustración de un usuario que, al descargar una fantástica aplicación nueva para el teléfono, se encuentra el dispositivo bloqueado y un aviso del FBI en la página de inicio. Lo único que puede hacer es pagar un rescate y esperar que los atacantes desbloqueen el teléfono o despedirse para siempre de sus fotografías, contactos y recuerdos.

Protección de los dispositivos móviles

Recomendamos tanto a los particulares como a las empresas que traten los dispositivos móviles como lo que son: potentes ordenadores de pequeñas dimensiones. Para protegerlos como les corresponde, tome las siguientes medidas:

- Controle el acceso, incluso con tecnología biométrica cuando sea posible.
- Adopte un sistema para evitar las pérdidas de datos (por ejemplo, el cifrado en el dispositivo).
- Haga copias de seguridad del dispositivo de forma automatizada.
- Implante un sistema que permita encontrar el dispositivo y borrar sus datos a distancia, lo cual resultará muy útil en caso de extravío.
- Actualice el software periódicamente. Por ejemplo, la última versión de Android, lanzada en octubre con el nombre en clave de Marshmallow (versión 6.0), incluye una serie de funciones diseñadas especialmente para detener a los atacantes. Según Statista, en octubre de 2015 la versión de Android más difundida seguía siendo KitKat (la 4.4), utilizada en un 38,9 % de los casos, mientras que un 15,6 % de los dispositivos Android funcionaban con Lollipop (versión 5.0).

http://www.symantec.com/connect/blogs/android-banking-trojan-delivers-customized-phishing-pages-straight-cloud
http://www.symantec.com/connect/blogs/android-ransomware-uses-material-design-scare-users-paying-ransom
http://www.symantec.com/security_response/landing/azlisting.jsp?azid=I
http://www.symantec.com/connect/tr/blogs/new-xcodeghost-malware-variant-discovered
http://www.bbc.co.uk/news/technology-34338362
http://www.symantec.com/connect/blogs/yispecter-threat-shows-ios-now-firmly-attackers-agenda
http://www.symantec.com/connect/blogs/ad-library-behind-pulled-ios-apps-also-used-android-development
http://www.symantec.com/connect/blogs/airdrop-vulnerability-poses-threat-iphone-and-mac-users
http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/

- No descargue aplicaciones en sitios web desconocidos, instálelas solo desde fuentes de confianza y no recurra al *jailbreaking*.
- Preste especial atención a los permisos que solicita una aplicación.
- Actualice las aplicaciones con la mayor frecuencia posible y, si detecta algo sospechoso, elimínela y espere a que salga una nueva versión.
- Si sospecha que su cuenta ha sufrido un ataque, cambie la ID de Apple o la contraseña de Google Play. Este consejo también se refiere a la protección de las credenciales para cualquier tienda de aplicaciones de otros fabricantes.
- Tenga mucho cuidado si recibe notificaciones o mensajes de correo electrónico sospechosos que le pidan sus credenciales o cualquier tipo de datos de identificación personal.
- Hasta que se aplique una revisión, sea prudente a la hora de acceder mediante el navegador móvil a archivos de vídeo o audio no solicitados.
- Si utiliza Android, instale las actualizaciones de seguridad en cuanto se las ofrezca su operador o el fabricante de su dispositivo.
- Existen más soluciones de seguridad para sistemas móviles que contribuyen a defenderse del software malicioso, y toda empresa debería plantearse implantar herramientas de gestión de la movilidad que ayuden a proteger y controlar los dispositivos móviles de sus empleados.

¿Qué nos depara el futuro?

Según nuestras previsiones, las amenazas a dispositivos móviles seguirán proliferando en 2016. Tal vez pronto se vendan en el mercado negro kits de intrusión para teléfonos similares a los que se utilizan para atacar ordenadores.

Al mismo tiempo, Apple y Google están haciendo todo lo posible por proteger sus sistemas operativos y sus ecosistemas en general. En concreto, prevemos que mejoren tanto las técnicas utilizadas para validar y firmar las aplicaciones como la forma de distribuirlas. Los usuarios tendrán que acostumbrarse a que las aplicaciones y el sistema operativo de sus teléfonos se actualicen con frecuencia, automáticamente de forma predeterminada, y asumirán que los dispositivos móviles necesitan software de seguridad.

Tal vez esto sea un indicio de avance más que un motivo de alarma: si los expertos en seguridad, los desarrolladores de sistemas operativos y los creadores de aplicaciones detectan y resuelven más problemas, es porque prestan más atención a la seguridad móvil. Aunque se prevé que durante el próximo año aumenten los ataques contra estos dispositivos, también se espera que, si toman las medidas preventivas adecuadas y siguen invirtiendo en seguridad, los usuarios gocen de un buen nivel de protección.

Amenazas por correo electrónico y otros sistemas de comunicación

Los sistemas informáticos (ordenadores y redes) siguen siendo víctimas de un *malware* que evoluciona con rapidez. El correo electrónico sigue siendo el medio preferido de los ciberdelincuentes y la cantidad de mensajes que se envían no deja de aumentar. Al mismo tiempo, el *phishing* y el *spam* están disminuyendo, aunque más de la mitad de los mensajes que se reciben son no deseados. El número de mensajes de correo electrónico maliciosos ha aumentado desde el año 2014 y estos siguen constituyendo un sistema eficaz para los ciberdelincuentes, aunque el *spam* farmacéutico no lo sea.

Ataques por correo electrónico

El correo electrónico sigue dominando la comunicación digital, al tiempo que aumenta la popularidad de las tecnologías de mensajería instantánea, tanto para usos empresariales como de consumo. Según los cálculos de Symantec, en 2015 se enviaron aproximadamente 190 000 millones de mensajes de correo electrónico al día, una cifra que prevemos que aumente en un 4 % de aquí a finales de 2016. Por término medio, cada usuario empresarial envió y recibió 42 mensajes de correo electrónico al día, y cada vez son más los individuos que leen el correo en dispositivos móviles. Para los ciberdelincuentes que quieran contactar electrónicamente al mayor número posible de personas, este sigue siendo el mejor sistema.

No es de extrañar que los ciberdelincuentes sigan utilizándolo con tanta frecuencia para enviar mensajes no deseados, lanzar ataques de *phishing* y transmitir *malware*. Sin embargo, en 2015 disminuyeron las amenazas por correo electrónico, limitándose al 1 % del correo no deseado. Symantec cuenta con análisis más detallados sobre el *malware* y el *phishing*, pues dado que estas amenazas tienen consecuencias dañinas que pueden llegar a ser considerables, resulta útil conocerlas mejor.

Symantec analiza una parte considerable del correo electrónico empresarial que se envía en el mundo, con lo que disponemos de información privilegiada sobre este medio y sobre las amenazas que supone para la seguridad. Muchos de los mensajes de correo electrónico empresariales nunca salen de la empresa, mientras que aproximadamente tres cuartas partes del tráfico de correo electrónico exterior son mensajes entrantes, más de la mitad de ellos no deseados.

https://support.apple.com/en-us/HT201355/
https://support.google.com/accounts/answer/41078?hl=en

Spam

En 2015 más de la mitad de los mensajes de correo electrónico empresariales recibidos eran no deseados, a pesar de que durante los últimos años la cantidad de *spam* ha ido disminuyendo paulatinamente y, de hecho, en 2015 llegó al nivel más bajo registrado desde el año 2003. De todos modos, el problema del *spam* sigue ahí: simplemente, se envía por otros canales, como las redes sociales y la mensajería instantánea, dos de los tipos de aplicaciones más difundidas en los dispositivos móviles. Así, al aprovechar estos sistemas además del correo electrónico, los atacantes perfeccionan sus tácticas.

Phishing

Con el tiempo, gracias a la evolución del mercado de la ciberdelincuencia, las campañas de *phishing* se han simplificado mucho para los atacantes. Ahora estos colaboran entre sí: algunos se especializan en kits de *phishing*, mientras que otros los venden a quien quiera llevar a cabo ataques de este tipo.

Por lo general, estos kits se venden a un precio de entre 2 y 10 USD, y no se necesitan grandes competencias técnicas para utilizarlos ni para personalizar sus páginas web según las necesidades particulares de cada uno. A continuación, los estafadores pueden utilizar los datos robados con estos ataques para sus propios propósitos o bien venderlos en el mercado negro.

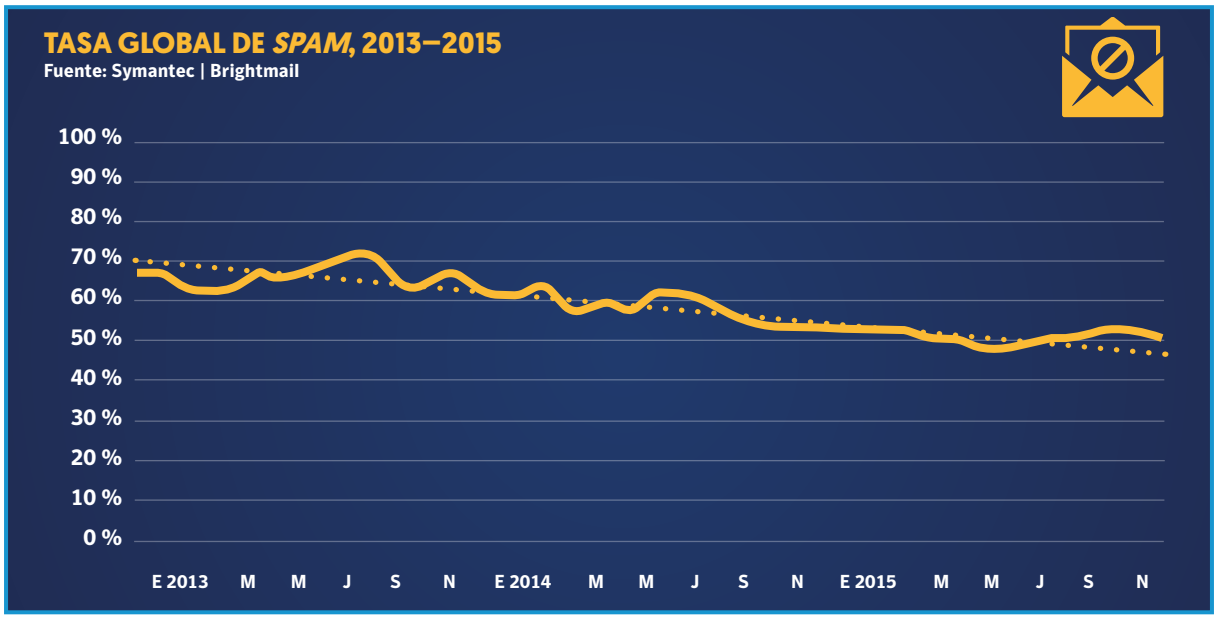
Propagación de *malware* por correo electrónico

Como ocurre con el *phishing*, cuando se distribuye *malware* por correo electrónico, se necesitan ciertos conocimientos de ingeniería social para lograr que el destinatario abra un archivo adjunto o haga clic en un enlace. Los adjuntos pueden ser facturas falsas, documentos de trabajo u otro tipo de archivos y, por lo general, es necesario que el software utilizado para abrirlos presente alguna vulnerabilidad sin resolver. De forma similar, los enlaces maliciosos dirigen al usuario a un sitio web infectado mediante un kit de herramientas de ataque para instalar algún tipo de *malware* en su equipo.

Las amenazas como Dridex recurren exclusivamente a los ataques mediante correo electrónico no deseado y muestran nombres de empresas reales tanto en la dirección del remitente como en el cuerpo del mensaje. La inmensa mayoría del *spam* de Dridex se camufla en forma de mensaje con contenido financiero, como facturas, recibos y pedidos. Estos mensajes llevan adjuntos archivos de Word o Excel maliciosos, con una carga útil que instala el *malware* propiamente dicho con el fin de robar datos de banca online.

El grupo de ciberdelincuentes responsables de este ataque en concreto ha utilizado todo tipo de *spam* y de vectores de difusión de *malware*: desde simples archivos adjuntos maliciosos hasta enlaces en el cuerpo del mensaje que llevan a la página de entrada de un kit de ataque, pasando por archivos PDF dañinos y macros.

La propagación de *malware* por correo electrónico no se ha reducido como el *spam* general y, dado su volumen relativamente bajo, es más proclive a las fluctuaciones. Se producen picos cuando se llevan a cabo campañas de gran envergadura.

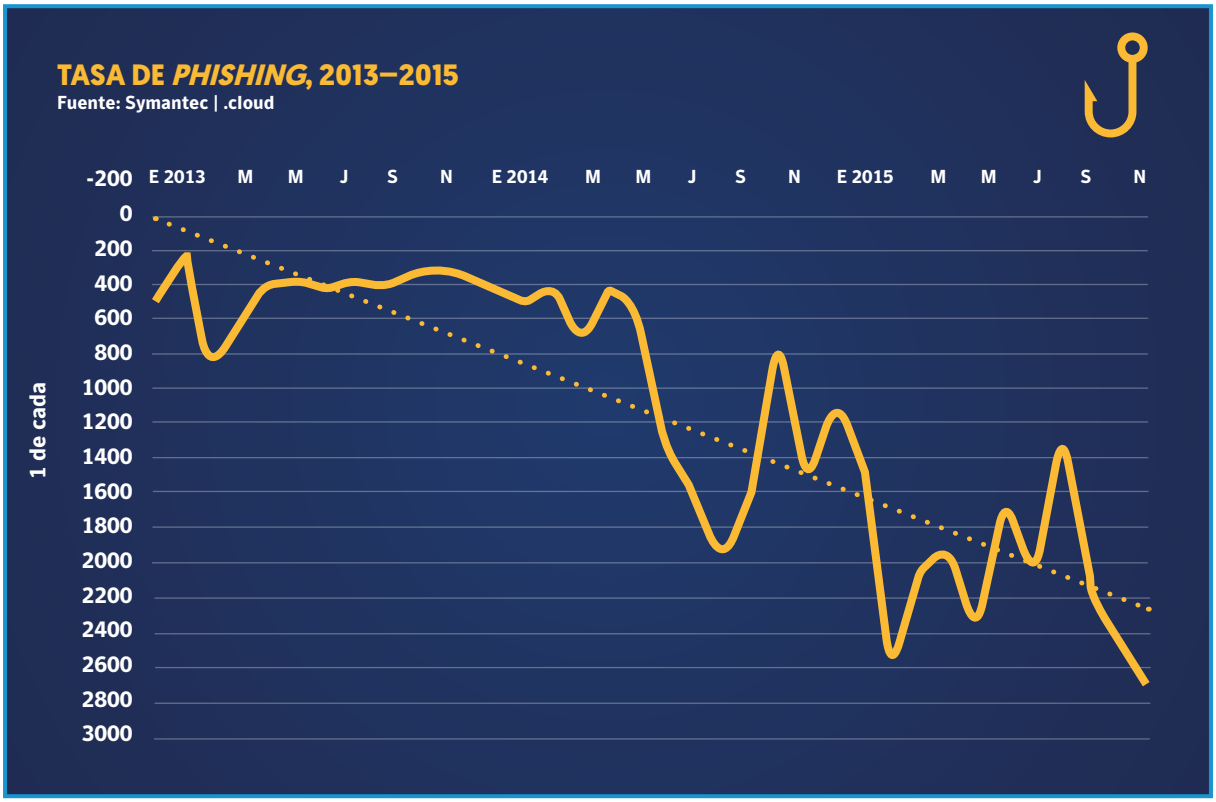


No es de extrañar que siga siendo uno de los métodos preferidos de los cibercriminales para enviar *spam*, *phishing* y *malware*. Sin embargo, en 2015 estas tres técnicas declinaron.

http://www.symantec.com/connect/blogs/phishing-economy-how-phishing-kits-make-scams-easier-operate
http://www.symantec.com/connect/blogs/dridex-and-how-overcome-it
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf

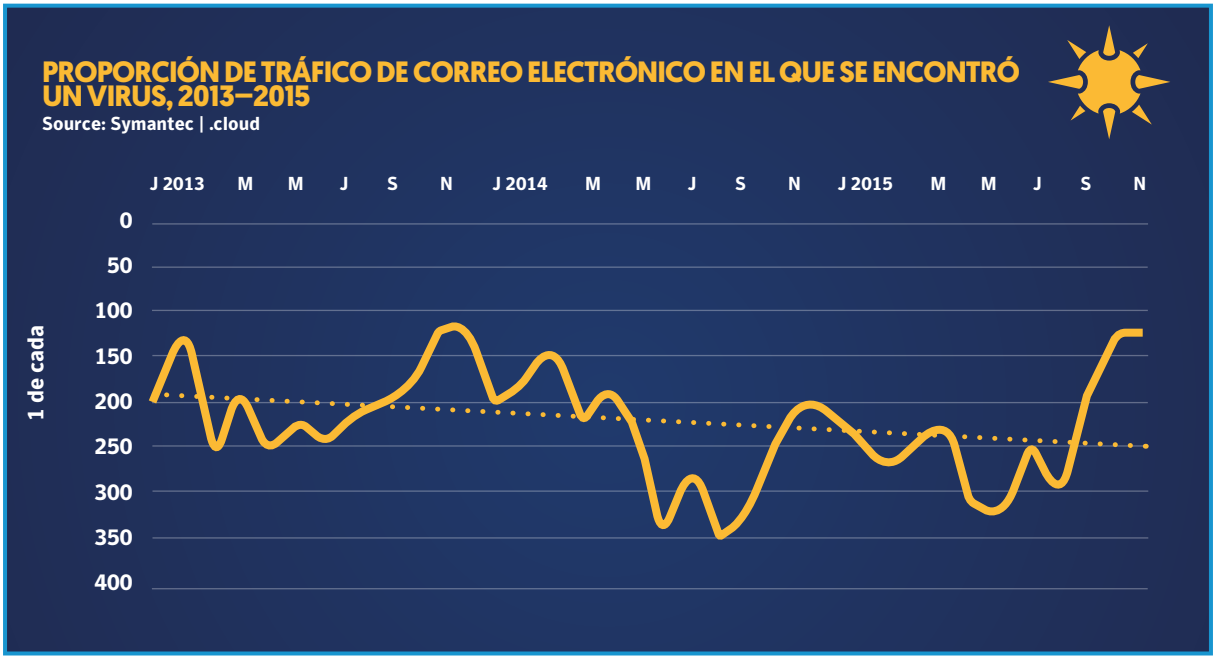
TASA DE *PHISHING*, 2013–2015

Fuente: Symantec | .cloud



PROPORCIÓN DE TRÁFICO DE CORREO ELECTRÓNICO EN EL QUE SE ENCONTRÓ UN VIRUS, 2013–2015

Source: Symantec | .cloud



El cifrado del correo electrónico

Resulta muy útil cifrar el correo electrónico, porque de este modo se protege la confidencialidad de los mensajes y se facilita la autenticación de los emisores. Existen vulnerabilidades en la tecnología subyacente (como se aprecia en los datos expuestos), pero parte del problema de seguridad se debe a que no se utiliza de forma generalizada.

Aunque los sistemas de correo electrónico en línea (como Outlook.com, de Microsoft, y Google Mail) cifran los datos en los clientes y casi todos los sistemas de correo electrónico dan prioridad a la transmisión cifrada, todavía queda una sorprendente cantidad de correo electrónico que se envía mediante transferencias SMTP sin cifrar. Por ejemplo, según datos de Google, en torno al 40 % de los mensajes entrantes del año pasado no estaban cifrados.

Existen herramientas eficaces para cifrar el correo electrónico en los equipos de escritorio y en las pasarelas (por ejemplo, las de Symantec), pero las empresas tienen que aprender a utilizar mejor la tecnología disponible para proteger el correo electrónico tanto durante las transferencias como una vez recibido.

Ataques que eluden el cifrado

Hemos observado una serie de ataques y vulnerabilidades en el cifrado subyacente utilizado para proteger las transmisiones por correo electrónico. Por ejemplo, el ataque Logjam aprovecha un defecto del mecanismo de intercambio de claves con que inicia cualquier intercambio cifrado.

Con la herramienta SSL Toolbox de Symantec, nuestros clientes pueden analizar sus dominios para comprobar la presencia de Logjam y otras importantes vulnerabilidades. Este recurso gratuito permite detectar problemas importantes como POODLE o Heartbleed, así como errores que pueda haber en la instalación de certificados SSL/TLS.

Consejos para garantizar la seguridad al usar el correo electrónico

Aunque muchos particulares y empresas consideran que no son un objetivo especialmente interesante para los ciberdelincuentes, tal vez se equivoquen.

La clave está en no bajar la guardia nunca. En el ámbito personal, esto significa:

- No abrir mensajes de correo electrónico procedentes de emisores desconocidos
- Buscar siempre el símbolo del candado y comprobar el certificado SSL/TLS antes de escribir información confidencial en un sitio web
- No utilizar redes desprotegidas para acceder a datos confidenciales

En el ámbito empresarial, hay que hacer lo siguiente:

- Implantar software de detección y prevención de las intrusiones
- Saber qué información valiosa posee la empresa y utilizar tecnología de prevención de pérdidas de datos
- Controlar dónde están los datos y quién tiene acceso a ellos
- Contar con un plan de respuesta a las incidencias para cuando se detecte un ataque

¿Qué nos depara el futuro?

Tras tres años de reducción constante del *phishing*, prevemos que la cantidad de ataques de este tipo se mantenga en el nivel actual o incluso siga bajando. Ahora los ataques de phishing son más dirigidos y menos masivos. Además, en muchos casos ya se ha empezado a utilizar las redes sociales, lo que contribuye a la disminución del número de mensajes de correo electrónico. De todos modos, en ciertas partes del mundo los ataques de *phishing* por correo electrónico son más frecuentes que en otras: así, la disminución ha sido más acusada en numerosos países de habla inglesa, en América del Norte y en ciertas zonas de la Europa Occidental.

Continuará la tendencia de hacer cada vez más cosas online (pagar facturas, pedir citas médicas, solicitar plaza en la Universidad, gestionar cuentas de programas de fidelización, contratar un seguro, etc.), lo cual proporciona un terreno jugoso para el *phishing*. Además, como el acceso a Internet y las transacciones electrónicas cada vez son más habituales en los países en vías de desarrollo, incluso es posible que en estas zonas aumente la cantidad de ataques de este tipo.

http://www.google.com/transparencyreport/saferemail/
http://www.symantec.com/en/uk/desktop-email-encryption/
http://www.symantec.com/en/uk/gateway-email-encryption/
http://www.symantec.com/connect/blogs/logjam-latest-security-flaw-affect-secure-communication-protocols
https://ssltools.websecurity.symantec.com/checker/views/certCheck.jsp
http://www.symantec.com/connect/blogs/when-defenses-fail-case-incident-response

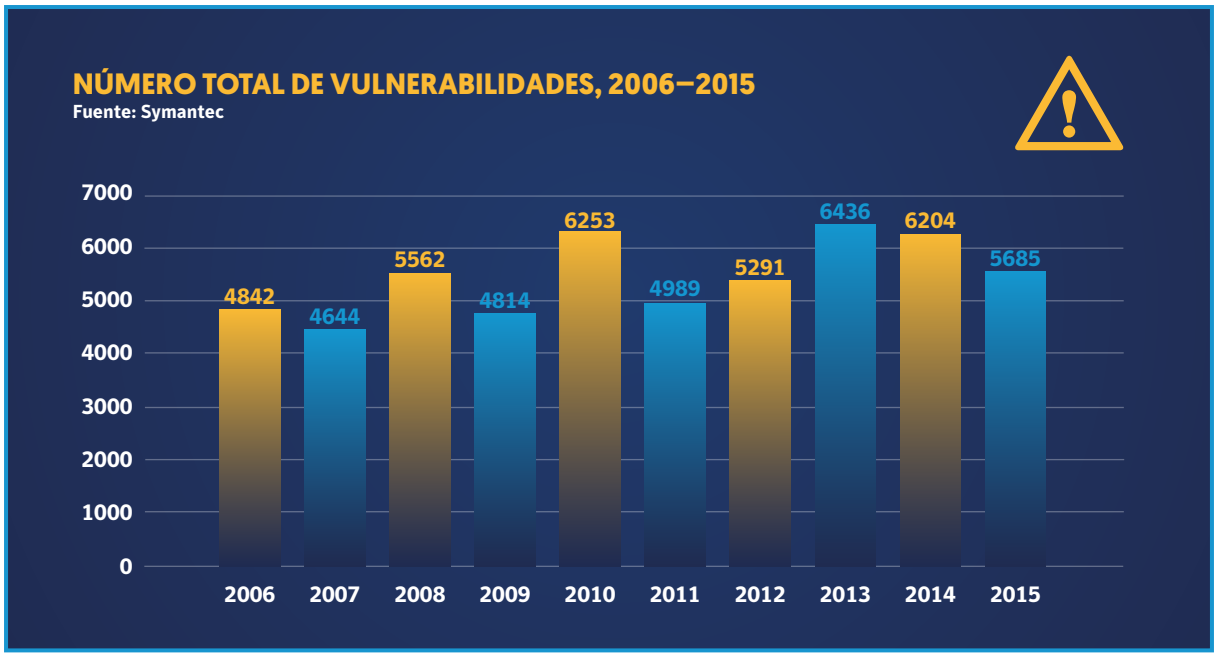
Los ordenadores, la informática en la nube y la infraestructura de TI

Los sistemas informáticos (ordenadores y redes) siguen siendo víctimas de un *malware* que evoluciona con rapidez. Los sistemas Linux y Mac OS X cada vez están más amenazados por el *malware*: no hay ningún sistema operativo que sea inmune automáticamente y, de hecho, incluso los sistemas virtualizados y alojados en la nube son vulnerables. Ahora el *malware* consigue detectar entornos virtualizados e infectarlos.

La ciberseguridad afecta a todo el mundo. Las empresas tienen que proteger sus equipos y su infraestructura de TI para impedir los robos de datos, los fraudes y los ataques con *malware*. Asimismo, tanto las empresas como los consumidores deberían tener en cuenta las amenazas que los acechan: los ciberdelincuentes podrían cifrar sus datos y exigir el pago de un rescate para descifrarlos, robarles la identidad o usar sus equipos como trampolín para atacar a otros objetivos.

En general, la ciberseguridad consiste en proteger los pilares de las TI: los ordenadores, los servidores y las redes. El problema es que el *malware* está en todas partes. En 2015, han sufrido ataques una mayor cantidad de sistemas diversos, como Linux, Mac, equipos virtualizados y sistemas en la nube. Cada año aumenta el volumen de datos que se gestionan en la nube, para fines asociados a la gestión de las relaciones con los clientes, los servicios de facturación, las redes sociales, el correo electrónico móvil y un largo etcétera.

Una de las formas de atacar un sistema consiste en aprovechar las vulnerabilidades que presenta, y son pocos los que carecen de ellas. Estas vulnerabilidades, un aspecto muy importante de la ciberseguridad, se encuentran tanto en los sistemas operativos como en las aplicaciones que se ejecutan en ellos. Si no se resuelven, dejan la pista libre a todo el que quiera atacar un sistema, que podrá aprovecharlas y utilizarlas con fines maliciosos. Cada año los expertos descubren nuevas vulnerabilidades de distintos tipos: las más codiciadas son las de día cero, es decir, aquellas para las que todavía no existe una revisión de seguridad.



Tal como se aprecia en el gráfico, parece que desde el año 2013 se impuso una tendencia a la baja, que se ha acentuado claramente en 2015.

Sistemas virtualizados y en la nube

El término «cloud computing» o «informática en la nube» abarca una gran variedad de soluciones y entornos técnicos, como los modelos de software como servicio (SaaS), plataforma como servicio (PaaS) o infraestructura como servicio (IaaS). Este último cada vez se utiliza más en las empresas y, a medida que se transfiere a la nube una mayor cantidad de datos y servicios, despierta más interés entre los ciberdelincuentes y los expertos en seguridad. Como ocurre con cualquier sistema, cada vez que se añade una capa nueva al conjunto de servicios, aumenta la superficie de ataque. Los entornos en la nube a veces presentan vulnerabilidades comunes, como la inyección SQL, pero también pueden verse afectados por otro tipo de problemas. Por ejemplo, en 2015 Symantec comprobó que, cuando los usuarios (no los proveedores de servicios) cometen errores de configuración y gestión, existe el riesgo de que accedan a los sistemas en la nube personas no autorizadas. Además, también se descubrieron 11 000 archivos accesibles públicamente, algunos de ellos con datos personales confidenciales. En el mercado negro, es habitual la compraventa de credenciales robadas para acceder a sistemas en la nube por un precio que no suele alcanzar los 10 $.

Vulnerabilidades en la nube

Los sistemas en la nube no tienen por qué ser menos seguros que los servicios de TI tradicionales, pero en cualquier caso los administradores tienen que asegurarse de que los servicios en la nube estén bien configurados y de que todos los datos cuenten con la suficiente protección. Además, deberían controlar el acceso a los sistemas en la nube, a ser posible mediante autenticación de dos factores.

Hay vulnerabilidades, como VENOM, que permiten a un atacante salir de una máquina virtual huésped y acceder al sistema operativo anfitrión nativo, así como a otras máquinas virtuales que se ejecuten en la misma plataforma. Así, los atacantes que aprovechen VENOM podrían llegar a robar datos confidenciales presentes en cualquiera de las máquinas virtuales del sistema afectado, además de acceder a la red local del anfitrión y a sus sistemas. VENOM (CVE-2015-3456) existió desde el año 2004 en el hipervisor de código abierto QEMU, que suele estar instalado de forma predeterminada en numerosas infraestructuras virtualizadas que utilizan Xen, QEMU y KVM. Hay que señalar que VENOM no afecta a los hipervisores de VMware, Microsoft Hyper-V y Bochs.

Hasta la fecha, no se ha tenido conocimiento de que la vulnerabilidad VENOM haya sido aprovechada y, desde que se sabe de su existencia, los desarrolladores de QEMU junto con otros proveedores afectados han creado y distribuido revisiones de seguridad para VENOM.

Hoy uno de cada seis (el 16 %) tipos de *malware* es capaz de detectar la presencia de un entorno de máquinas virtuales, mientras que en 2014 lo lograba uno de cada cinco (el 20 %). Esta capacidad hace que sea más difícil detectar el malware, en especial en los sistemas de espacios aislados de seguridad que utilicen la virtualización. Pero es más preocupante el hecho de que el ciberdelincuente sepa cuándo puede atacar e infectar a otras máquinas virtuales del mismo sistema.

Aproximadamente, el 16 % del *malware* es capaz de detectar un entorno de máquinas virtuales, y en el cuarto trimestre la cifra llegó a rondar el 22 %.
Hoy es más importante que nunca contar con un perfil de seguridad eficaz para los sistemas virtuales. Es necesario proteger las máquinas virtuales y los servicios en la nube tanto como otros servicios y dispositivos. Las políticas de seguridad deberían abarcar tanto la infraestructura virtual como la física y, si se implantan sistemas de protección integrados en todas las plataformas, será más fácil mitigar este tipo de problemas en el futuro.

Protección de la infraestructura de TI

Ante estas amenazas y otras muchas similares, siguen siendo válidos los consejos de siempre para cualquier tipo de servicio de infraestructura, como los servidores de archivos, los servidores web y otros dispositivos conectados a Internet:

- Manténgase al día acerca de las amenazas que van surgiendo.
- Instale siempre en los sistemas las últimas revisiones de seguridad y actualizaciones.
- Implante un software de seguridad integrado que incluya tecnología contra el *malware*.
- Adopte un *firewall* eficaz que permita solo el tráfico conocido y revise los registros de acceso periódicamente para detectar actividad que parezca sospechosa.
- Utilice varias capas de seguridad, de forma que si una falla queden otras para proteger distintas áreas del sistema.
- Aplique las políticas correctas y forme bien a los empleados.
- Controle los accesos según un principio de privilegios mínimos.
- Implante sistemas de detección y prevención de intrusiones en la red y supervise los servicios de correo electrónico que se ejecutan en el servidor.
- Guarde siempre las copias de seguridad fuera de las instalaciones.

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/mistakes-in-the-iaas-cloud-could-put-your-data-at-risk.pdf
http://www.symantec.com/connect/blogs/venom-vulnerability-could-expose-virtual-machines-unpatched-host-systems

A continuación añadimos una serie de consideraciones que se deben tener en cuenta en lo que se refiere a los sistemas en la nube:

- Proteja las credenciales utilizadas para acceder a las funciones de administración en la nube y asegúrese que solo acceda a los datos quien realmente lo necesite.
- Asegúrese de comprender bien la configuración de los recursos en la nube y elija los parámetros idóneos.
- Habilite el registro de eventos para saber siempre quién accede a los datos en la nube.
- Lea los acuerdos de nivel de servicio de los proveedores de informática en la nube para saber cómo se protegen los datos almacenados en la nube.
- Asegúrese de que las direcciones IP en la nube se incluyan en los procesos de gestión de vulnerabilidades y someta a auditorías cualquier servicio que se preste en la nube.

Proteja la información esté donde esté

Cuando las empresas transfieren sus sistemas de TI a entornos virtuales y en la nube, se encuentran con dificultades nuevas en materia de seguridad. Además, como siempre, la propia naturaleza humana es una amenaza en sí misma, y la mala gestión de la seguridad lleva a la aparición de sistemas de TI en la sombra, es decir, sistemas y soluciones que se utilizan dentro de una empresa sin la aprobación explícita de esta, o bien soluciones implantadas por personas que no pertenecen al departamento de TI. A veces, resulta facilísimo que un grupo de empleados recurra a productos externos para resolver de inmediato una exigencia concreta. Los responsables de la infraestructura de TI de la empresa deberían tratar de entender por qué el personal actúa sin consultar al departamento informático para que lo oriente en este tipo de decisiones.

Es importante que el director de sistemas esté informado de lo que se hace en la empresa y que sepa si ciertos equipos buscan servicios o aplicaciones de los que carecen. A continuación, tendrá que decidir cómo satisfacer esa exigencia y prestar el servicio necesario de forma segura. Contar con los procesos adecuados es esencial para proteger la información y los datos, incluso cuando no estén almacenados en la empresa.

http://www.symantec.com/connect/blogs/monitoring-shadow-it

La respuesta del sector

La tecnología SSL/TLS sigue siendo crucial para el cifrado, la autenticación y la confidencialidad en Internet, pero en torno a ella hay una infraestructura de confianza que se debe mantener y vigilar para que siga siendo eficaz, y el sector tiene que aprender y adaptarse constantemente.

La evolución del cifrado

El 11 de agosto de 1994 Daniel Kohn vendió un CD a un amigo de Filadelfia. Este pagó 12,48 $ más los gastos de envío con tarjeta de crédito, en la primera transacción de la historia protegida con tecnología de cifrado.

Al día siguiente, en el New York Times se publicaba lo siguiente: «Como cada vez se habla más de las incidencias de seguridad que tienen lugar en Internet, muchas personas y empresas son reticentes a enviar datos confidenciales, como números de tarjeta de crédito, información sobre ventas o mensajes de correo electrónico privados».

Veinte años después, las preocupaciones siguen siendo las mismas, pero parece que estamos dispuestos a asumir el riesgo, con la esperanza de que el banco venga en nuestro auxilio si algo sale mal. Sin embargo, sin una infraestructura SSL/TLS segura y sólida, esta frágil confianza se derrumbará y el comercio electrónico sencillamente dejará de funcionar.

Las cifras de la solidez

La eficacia de la tecnología SSL/TLS ha avanzado muchísimo desde 1994, y lo sigue haciendo: este mismo año el sector ha pasado del estándar SHA-1 al SHA-2.

Gracias al aumento de la potencia de procesamiento, ahora a los *hackers* les resulta más fácil descifrar algoritmos hash mediante ataques de fuerza bruta y, según numerosos expertos, los certificados basados en SHA-1 serán vulnerables dentro de muy poco tiempo. Por eso, los principales navegadores han decidido dejar de admitir los certificados SHA 1 durante los próximos dos años, así que si un internauta intenta acceder a un sitio web que los utilice, verá una advertencia de seguridad.

«Coincidimos con Microsoft y Google en que se debería dejar de emitir certificados SHA-1 a partir del 1 de enero de 2016, y que pasado el 1 de enero de 2017 ya no se deberían considerar fiables», comentan fuentes de Mozilla. Incluso se ha hablado de adelantar estas fechas para acelerar el cambio.

Symantec ofrece un servicio de actualización gratuito, pero las grandes empresas tienen que garantizar que cuentan con un plan de migración para poner al día todos los dispositivos y aplicaciones que en este momento no reconozcan el algoritmo SHA 2.

¿Hay motivos para el pánico?

La vulnerabilidad denominada FREAK, descubierta en marzo de 2015, permitía forzar el uso del cifrado de exportación (mucho menos eficaz del que se suele usar hoy) a los atacantes que interceptaran la configuración de una conexión segura entre un cliente y un servidor afectado. De este modo, resultaba fácil descifrar el mensaje de la transacción con los recursos informáticos disponibles en la actualidad.

SE CALCULA QUE INICIALMENTE ERAN VULNERABLES A ESTE ATAQUE LOS SERVIDORES DEL 9,6 % DEL MILLÓN DE DOMINIOS DE SITIOS WEB PRINCIPALES. NUEVE MESES DESPUÉS, LO SIGUE SIENDO EL 8,5 %.

http://www.fastcompany.com/3054025/fast-feed/youll-never-guess-what-the-first-thing-ever-sold-on-the-internet-was?partner=rss
http://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html
http://www.infoworld.com/article/2879073/security/all-you-need-to-know-about-the-move-to-sha-2-encryption.html
https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/
http://www.symantec.com/connect/blogs/freak-vulnerability-can-leave-encrypted-communications-open-attack
https://freakattack.com

Control y equilibrio

Con el objetivo de fortalecer el ecosistema SSL/TLS, Symantec también ha propugnado la adopción generalizada de la autorización de la autoridad de certificación (CAA) DNS, que permite a una empresa o propietario de DNS especificar la autoridad de certificación (CA) que debe emitir los certificados que compre. Si una persona malintencionada o un empleado que no conozca la política empresarial intenta comprar un certificado de una CA que no esté presente en la lista de entidades aprobadas, dicha CA podrá comprobar la CAA y avisar de la solicitud al propietario de DNS.

De este modo, se reduce el riesgo de que se emitan certificados de origen dudoso en nombre de una empresa legítima sin que esta lo sepa, lo cual a su vez contribuirá a evitar que los delincuentes consigan crear sitios web certificados para lanzar ataques de *phishing*.

Además, para mejorar la detección de los certificados de origen dudoso, Symantec cumple con la exigencia de Google de registrar todos los certificados EV emitidos en su registro Certificate Transparency y, desde marzo de 2016, registra también los certificados OV y DV. De este modo, junto con un software que supervisa y audita los certificados y el uso que se hace de ellos, este sistema crea «un marco abierto que permite a quien lo desee observar y verificar prácticamente en tiempo real los certificados SSL/TLS existentes y recién emitidos», tal como dicen sus autores.

El salto a la tecnología SSL Always-On

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 año este dato aumente para superar el 70 % del tráfico mundial. Este aumento tan repentino se debe a una serie de factores:

- **Adopción por parte de grandes empresas.** Varios de los nombres con más peso en Internet (como Facebook, Twitter y, recientemente, Netflix) ya han adoptado el protocolo HTTPS.
- **Preferencia por parte de los buscadores.** En 2014 Google anunció que los sitios web que protegieran con el protocolo HTTPS todas sus páginas tendrían un mejor posicionamiento en los resultados de las búsquedas, lo cual ha animado a numerosos propietarios de sitios web a adoptar este sistema.
- **Mejora de Internet.** El Internet Engineering Task Force o IETF (grupo de trabajo de ingeniería de Internet), entidad encargada de crear estándares para Internet, publicó en 2015 una nueva versión del protocolo de transferencia de hipertexto conocido como HTTP/2, que con toda probabilidad a corto plazo se convertirá en el estándar del sector. Tal como especifica el borrador, el protocolo HTTP/2 hace posible «un uso más eficiente de los recursos de la red», lo que significa que está diseñado para garantizar un rendimiento más alto y una capacidad de respuesta más rápida para los sitios web. Además, todos los principales navegadores solo admitirán el protocolo HTTP/2 con tecnología SSL/TLS. En la práctica, esto obliga a los sitios web que adopten el nuevo estándar a cifrar toda la información.

Se espera que dentro de unos pocos años todas las páginas de Internet cuenten con un certificado SSL/TLS. Symantec incluso está colaborando con los proveedores de alojamiento web para ayudarlos a incluir el cifrado en el servicio que prestan a los propietarios de sitios web.

Tipo de certificado	Validación del dominio	Cifrado «https»	Validación de la identidad	Validación de la dirección	Símbolo del candado en la interfaz de usuario del navegador	Barra de direcciones verde*
DV	Sí	Sí	Ninguna	No	Sí	No
OV	Sí	Sí	Buena	Sí	Sí	No
EV	Sí	Sí	Muy buena	Sí	Sí	Sí

*O un candado verde o algún signo verde en la barra de direcciones.

https://casecurity.org/2013/09/25/what-is-certification-authority-authorization/
https://knowledge.symantec.com/support/ssl-certificates-support/index?page=content&id=AR2177
https://www.certificate-transparency.org
https://www.sandvine.com/pr/2016/2/11/sandvine-70-of-global-internet-traffic-will-be-encrypted-in-2016.html
http://fortune.com/2015/04/30/netflix-internet-traffic-encrypted/
http://googlewebmastercentral.blogspot.co.uk/2014/08/https-as-ranking-signal.html
http://tools.ietf.org/pdf/draft-ietf-httpbis-http2-17.pdf
https://www.mnot.net/blog/2015/06/15/http2_implementation_status
https://www.hostpoint.ch/en/ssl/freessl.html

Mayor sensación de seguridad

Varios de los principales navegadores también están mejorando sus indicadores de seguridad (los colores y símbolos utilizados en la barra de direcciones para indicar a los internautas el nivel de seguridad del sitio web), para que resulte claro cuándo una página protegida con tecnología SSL/TLS incluye contenido desprotegido vulnerable a los ataques de interposición «Man-in-the-Middle». Dicho de otro modo, resultarán más evidentes los casos en que el sitio web no garantiza la seguridad de la conexión y el peligro que esto implica.

Se trata solo de un ejemplo de la tendencia a tranquilizar a los internautas y a las personas que compran por Internet mediante indicadores de seguridad. Así, los distintivos de confianza y las garantías de compra contribuyen a disipar los temores que tienen numerosos consumidores cuando compran por Internet y no ven al propietario de la tienda en persona ni pueden tocar los productos que están adquiriendo.

https://blog.mozilla.org/security/2015/11/03/updated-firefox-security-indicators-2/
https://www.nortonshoppingguarantee.com/

Consejos y prácticas recomendadas

Para que los sistemas que garantizan la seguridad de los sitios web sean eficaces, hay que implantarlos con cuidado, así como llevar a cabo una supervisión y mantenimiento constantes. Existen herramientas que contribuyen a proteger el ecosistema del sitio web, pero todo empieza por la formación. Ahora que ya conoce los riesgos, descubra lo que puede hacer al respecto.

Adopte los estándares del sector

- **Utilice la tecnología SSL Always-On.** Proteja con el protocolo SSL/TLS todas las páginas para que se cifren todas las interacciones entre el sitio web y el internauta. Al adoptar este sistema, también llamado «HTTPS Everywhere», con certificados SSL/TLS OV o EV, demostrará su credibilidad y mejorará su posicionamiento en los resultados de las búsquedas. Además, allanará el camino para la adopción de HTTP/2, que mejora el rendimiento.
- **Migre al algoritmo SHA-2.** Tal como se explica en este informe, las autoridades de certificación deberían haber dejado de emitir certificados SHA-1 a partir del 1 de enero de 2016, pero tiene que comprobar que se actualicen también todos los certificados antiguos, al igual que los dispositivos y las aplicaciones que en este momento no reconozcan el algoritmo SHA-2.
- **Considere la posibilidad de adoptar el algoritmo ECC.** Symantec también ofrece la posibilidad de usar el algoritmo de cifrado ECC. Los principales navegadores, incluidos los móviles, admiten certificados ECC en todas las plataformas recientes, y las claves ECC de 256 bits son 64 000 veces más difíciles de descifrar que las claves RSA de 2084 bits de uso estándar en el sector.

Utilice la tecnología SSL/TLS correctamente

Los certificados SSL y TLS son eficaces solo si se instalan y mantienen correctamente, así que no olvide lo siguiente:

- **Mantenga actualizadas las bibliotecas de protocolos.** La implantación de SSL/TLS es una tarea constante y resulta imprescindible instalar lo antes posible las actualizaciones y revisiones del software que utilice.
- **No permita que sus certificados caduquen.** Tenga siempre bajo control los certificados con los que cuenta, la autoridad de certificación que los ha emitido y su fecha de caducidad. Symantec ofrece una serie de herramientas de automatización que facilitan esta tarea, con lo que tendrá más tiempo para abordar cuestiones de seguridad de forma proactiva.
- **Muestre distintivos de confianza conocidos** (como el sello Norton Secured) en zonas bien visibles de su sitio web para demostrar a los clientes que se toma en serio su seguridad.
- **Gestione las claves SSL/TLS correctamente.** Limite el número de personas con acceso a ellas; compruebe que quien se ocupa de administrar las contraseñas del servidor donde se guardan las claves no sea el mismo que gestiona los sistemas en los que se almacenan las claves; y utilice sistemas automatizados de gestión de claves y certificados para reducir la necesidad de intervenciones humanas.

Adopte una solución completa para la seguridad de los sitios web

- **Haga análisis periódicos.** Vigile sus servidores web para detectar posibles vulnerabilidades o infecciones con *malware*. Para ello, resultan muy útiles las herramientas de automatización.
- **Utilice un antivirus.** El software antivirus no es solo para los ordenadores y smartphones, sino también para los servidores, y podría ayudar a evitar un grave ataque con *malware* contra toda la infraestructura del sitio web.
- **Instale solo los complementos realmente útiles.** También el software que utiliza para gestionar el sitio web presenta vulnerabilidades. Cuantos más programas de terceros utilice, mayor será la superficie de ataque, así que implante solo lo que sea imprescindible.
- **Tenga en cuenta todo el ecosistema.** ¿Ha implantado un *firewall* para aplicaciones web que evite los daños de los ataques de inyección? ¿Su sistema de firma de código garantiza la seguridad de sus aplicaciones web? ¿Cuenta con herramientas automatizadas que detecten y eviten los ataques DDoS, un problema cada vez más habitual?

Symantec ofrece una gama de herramientas con las que la tarea de garantizar la seguridad completa de los sitios web resulta sencilla y eficiente.

http://www.symantec.com/connect/blogs/introducing-algorithm-agility-ecc-and-dsa
https://www.symantec.com/en/uk/complete-website-security/
http://www.symantec.com/page.jsp?id=seal-transition

Conciencie a sus empleados

Como siempre, para que sus sitios web y servidores estén bien protegidos este año, guíese por el sentido común y adopte los hábitos de seguridad que le recomendamos a continuación.

- Asegúrese de que los empleados no abran archivos adjuntos de gente que no conozcan.
- Ayúdeles a reconocer los peligros que acechan en las redes sociales. Explíqueles que, si una oferta parece falsa, seguramente lo sea; que la mayoría de las estafas están relacionadas con noticias de actualidad; y que las páginas de inicio de sesión a las que conducen algunos enlaces pueden ser una trampa.
- Si un sitio web o aplicación ofrece autenticación de dos factores, dígales que elijan siempre esta opción.
- Pídales que usen contraseñas distintas para cada cuenta de correo electrónico, aplicación, sitio web o servicio (sobre todo si están relacionados con el trabajo).
- Recuérdeles que usen el sentido común. No por tener un antivirus es menos grave visitar sitios web dañinos o de naturaleza dudosa.
- Aplique controles de acceso eficaces para proteger los servidores y las claves privadas según un principio de privilegios mínimos.

Proteja los dispositivos móviles

Recomendamos tanto a los particulares como a las empresas que traten los dispositivos móviles como lo que son: potentes ordenadores de pequeñas dimensiones. Para protegerlos como les corresponde, tome las siguientes medidas:

- Controle el acceso, a ser posible con tecnología biométrica.
- Adopte un sistema para evitar las pérdidas de datos (por ejemplo, el cifrado en el dispositivo).
- Haga copias de seguridad del dispositivo de forma automatizada.
- Implante un sistema que permita encontrar el dispositivo y borrar sus datos a distancia.
- Actualice el software periódicamente. Por ejemplo, la última versión de Android, cuyo nombre en clave es Honeycomb, incluye una serie de funciones diseñadas especialmente para detener a los atacantes.
- No recurra al llamado «jailbreak» (consistente en modificar el sistema operativo para permitir la instalación de aplicaciones no autorizadas por el fabricante) y compre las aplicaciones solo en mercados de confianza.
- Forme a los usuarios, especialmente en lo que se refiere a tener cuidado con los permisos que solicita una aplicación.
- Implante soluciones de seguridad como Symantec Mobility o Norton Mobile Security.

La seguridad es responsabilidad de todos

La confianza de los consumidores se construye con numerosas interacciones que tienen lugar en diferentes sitios web pertenecientes a innumerables empresas. Pero basta una mala experiencia (un robo de datos o una descarga no autorizada) para manchar la reputación de todos los sitios web en la mente de la gente.

Como decíamos al comienzo del informe, este año es un buen momento para reducir el número de ataques cibernéticos que se salen con la suya y para limitar los riesgos que puede suponer su sitio web para los consumidores, pero es imprescindible que se implique y tome medidas concretas.

Adopte Symantec Website Security en 2016 y, con nuestra ayuda, haga que sea un año positivo para la seguridad informática y pésimo para los ciberdelincuentes.

http://www.symantec.com/connect/blogs/how-android-s-evolution-has-impacted-mobile-threat-landscape
http://www.symantec.com/mobility/
https://us.norton.com/norton-mobile-security

Symantec

PRÓXIMAMENTE: WSTR 2016, VERSIÓN COMPLETA

INFORME COMPLETO

WSTR

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

En la última entrega del WSTR 2016, podrá descargar todo el informe y encontrará una nueva sección sobre lo que cabe esperar a partir de 2016. Abordamos una amplia gama de temas relacionados con la seguridad de los sitios web, desde las tendencias emergentes hasta los debates que siguen de actualidad o que han surgido últimamente, para que sepa lo que nos depara el futuro y vaya siempre un paso por delante.

Además, podrá ver nuestra infografía, en la que se resumen los datos más destacados del informe de este año.

EN LAS PRÓXIMAS SEMANAS LE ENVIAREMOS LA VERSIÓN COMPLETA 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/ssl