



INFORME TRIMESTRAL PandaLabs (JULIO-SEPTIEMBRE 2010)

© Panda Security 2010

PANDA
SECURITY

Introducción	03
El trimestre de un vistazo	04
Más clickjacking “Me gusta!”	04
La saga Mariposa continúa...	05
Nuevos ataques a sistemas SCADA y “Here you have”	06
II Barómetro Internacional de seguridad en PYMEs	07
Más infecciones a través de USBs	09
Índice de Riesgo de las Redes Sociales para PYMEs	09
Malware en Smartphones... Android ya es el blanco	11
De vulnerabilidades, exploits y 0-Days	13
Cifras del Q3 2010	16
Incidencia del malware en el mundo	16
Datos de Spam	18
Conclusiones	19
Sobre PandaLabs	20

Cuando cerrábamos la anterior edición de este **informe trimestral**, que publicamos el pasado mes de julio, ya vaticinamos que las Redes Sociales seguirían dando de qué hablar, como ha sido el caso de las técnicas de clickjacking (o aquello que a todos los que estamos en FB nos vuelve locos: decir que algo “Me gusta!”).

Igualmente, comentábamos que tendríamos novedades –en cuanto a seguridad se refiere– respecto a Android, y una vez más, vemos que nuestras predicciones se han cumplido, como podréis leer un poco más adelante.

La saga “Mariposa” continúa, y con buenas noticias, ya que ha habido nuevas detenciones relacionadas con el caso, señal de que las autoridades siguen avanzando en materia de ciberinvestigación.

Este trimestre ha venido bastante cargado de diferentes acontecimientos alrededor del mundo de la seguridad. Quizá uno de los más importantes, del que hemos tenido puntual información a través de los diferentes medios de comunicación, ha sido las infecciones causadas por el gusano “Here you have”.

En las últimas semanas, hemos vuelto a vivir una situación que no habíamos visto en años, el típico gusano de correo, enviándose con el asunto “Here you have”, al más puro estilo *ILoveYou*. Sin llegar a causar una epidemia, sí que logró infectar a grandes compañías. Como hemos explicado en muchas ocasiones, la creación del malware tiene una motivación económica, motivo por el cual este tipo de gusanos prácticamente ha desaparecido.

Entonces, ¿por qué había aparecido este nuevo ejemplar? Pues parece que ha sido, como podrás leer algo más adelante, una posible acción reivindicativa contra Estados Unidos de un grupo llamado “Brigadas de Tariq ibn Ziyad”.

También hemos vuelto a observar que poco se ha avanzado en la seguridad de las PYMEs con respecto al pasado año, ya que siguen infectándose, según los datos de nuestro **II Barómetro Internacional de Seguridad en PYMEs**; eso sí, en el 25% de los casos de infección causada por gusanos, éstos estaban especialmente diseñados para distribuirse a través de dispositivos USB.

También hemos publicado el **Primer Índice Anual de Riesgo en Redes Sociales para PYMEs**. Nos han dicho que el 77% de los empleados las usan, y que el 33% ha sufrido infecciones en el parque corporativo por malware distribuido a través de estas comunidades...

Y más malware: los datos nos indican que siguen creciendo todos los indicadores, y que los países siguen infectándose...

En fin, que además de los movimientos industriales de adquisiciones e inyecciones de capital en diferentes compañías del sector de la seguridad, hemos tenido también mucho movimiento del tipo delictivo. Esperamos que disfrutes leyendo este informe trimestral, porque viene cargadito de información.

Más clickjacking “Me gusta!”

Si tuviéramos que resumir este trimestre en tres palabras, usaríamos las siguientes: clickjacking, BackHat SEO y 0-Day, ya que la mayoría de los ataques sucedidos durante estos meses han tenido al menos una de estas técnicas como protagonista.

Del clickjacking ya os hablamos en el último informe, se trata de una técnica utilizada por los criminales abusando de la característica de “Me gusta!” que existe en Facebook. Durante este trimestre han continuado los mismos ataques, utilizando cualquier tipo de evento, noticia o personaje que pudiera llamar la atención de los usuarios, como el caso del que os informamos en el **blog** sobre la semana del tiburón.

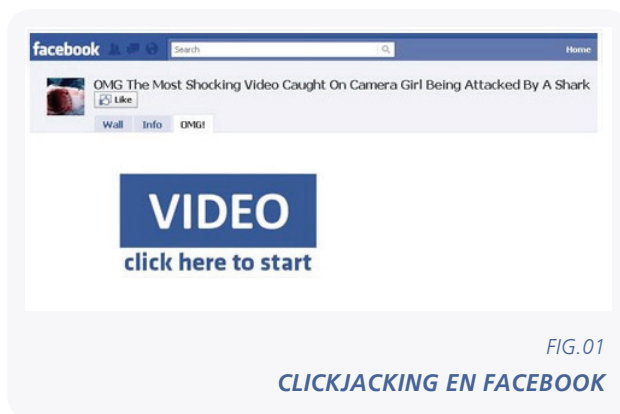


FIG.01
CLICKJACKING EN FACEBOOK

También se han aprovechado de la fama de algunas marcas, como fue el caso de **McDonalds**.



FIG.02
CLICKJACKING EN FACEBOOK

En el caso de los ataques BlackHat SEO sucede lo mismo, los cibercriminales tienen comprobado que les resulta muy sencillo distribuir malware usando este tipo de técnicas. Además, han conseguido automatizarlas para que el llevarlas a cabo no les suponga apenas esfuerzo.

Las redes sociales y los ataques BlackHat SEO siguen siendo los métodos de distribución preferido por los hackers

Hemos visto casos como el de la boda de **Chelsea Clinton**, donde al realizar búsquedas en Google muchos de los resultados redirigían a páginas que distribuían malware, principalmente falsos antivirus o rogueware.

Además debemos ser muy cuidadosos, ya que parece que están ampliando el rango de edades de estos ataques, ya que vimos uno afectando a los **Moshi Monsters**, una mezcla de Tamagochi, Pokemon y NintenDogs bastante popular entre los niños.



FIG.03
BLACK HAT SEO DE MOSHI MONSTERS

Por otro lado, hemos observado que estos ataques se planean con mucha antelación, como pudimos comprobar en agosto cuando vimos un **ataque** dirigido a Halloween y el día de Acción de Gracias en marcha, a pesar de quedar varios meses para que tuvieran lugar estas celebraciones.

La saga Mariposa continúa...

Cuando casi nos habíamos olvidado del caso Mariposa, este verano se anunciaron **varios arrestos** en Eslovenia. La gente se preguntaba si esto estaba realmente relacionado con el **caso Mariposa**, ya que los tipos detrás de Mariposa eran españoles y los arrestados son eslovenos.

El pasado marzo, cuando se hizo pública la historia, hablamos sobre los españoles arrestados, y que ellos habían comprado el bot. Probablemente os disteis cuenta de que no mencionamos nada sobre el vendedor del bot. Esto fue no porque no supiéramos quién estaba detrás, sino porque el FBI nos pidió amablemente que no hiciéramos pública la información, ya que estaban persiguiendo a Iserdo.

¿Quién es Iserdo? Es el apodo de un esloveno que ha sido el desarrollador principal del Butterfly Bot, y el que estaba en contacto con Netkairo. Asimismo, fue el que le vendió a Netkairo el bot con el que montó la red Mariposa.

Según Netkairo, él y Ostiator le dieron a Iserdo un "99%" de la idea para desarrollar el bot. Esto es muy poco probable que sea cierto, recordad además que estábamos teniendo esa conversación porque Netkairo quería que lo contratáramos para trabajar en el laboratorio (sic).

En otro periódico esloveno, había unas declaraciones diciendo que el precio del bot podría llegar a los 40.000€. No sé de dónde han obtenido esa información, pero parece un poco sobrevalorado. Estos son los precios reales por los que se vendía el bot:

- 
- **BASIC: 350 EUR**
(BFF core with modules: External Downloader, USB Spreader, MSN Spreader)
 - **PREMIUM: 400 EUR**
(BFF core with modules: External Downloader, Basic Flooder, Slowloris Flooder)
 - **BUSINESS: 450 EUR**
(BFF core with modules: External Downloader, Visit, Cookie Stuffer, Adware Simple)
 - **STANDARD: 600 EUR**
(BFF core with modules: External Downloader, USB Spreader, MSN Spreader, Basic Flooder, Visit, Reverse Socks Simple)
 - **SELECTED: 600 EUR**
(BFF core with modules: External Downloader, USB Spreader, MSN Spreader, Basic Flooder, Slowloris Flooder)
 - **PROFESSIONAL: 900 EUR**
(BFF core with modules: External Downloader, Visit, Reverse Socks Simple, Connect Hook, Post Data Grabber, Cookie Stuffer, Adware Simple)
 - **ULTIMATE: 1100 EUR**
(BFF core with modules: External Downloader, Basic Flooder, Slowloris Flooder, USB Spreader, MSN Spreader, Visit, Reverse Socks Simple, Connect Hook, Post Data Grabber, Cookie Stuffer, Adware Simple)
 - **CUSTOM: price depends on chosen modules**
(BFF core with modules you can choose)

FIG.04

PRECIOS BOTS

El "custom" es el que compró Netkairo, estos son los precios de cada módulo:

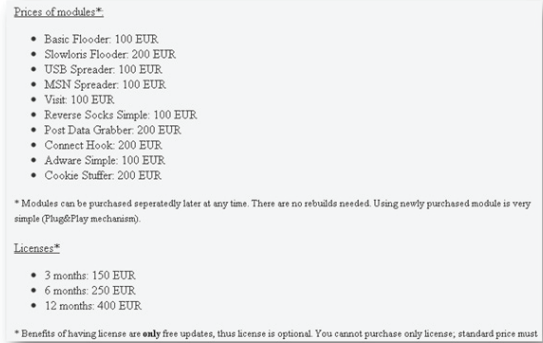
- 
- Prices of modules***
- Basic Flooder: 100 EUR
 - Slowloris Flooder: 200 EUR
 - USB Spreader: 100 EUR
 - MSN Spreader: 100 EUR
 - Visit: 100 EUR
 - Reverse Socks Simple: 100 EUR
 - Post Data Grabber: 200 EUR
 - Connect Hook: 200 EUR
 - Adware Simple: 100 EUR
 - Cookie Stuffer: 200 EUR
- * Modules can be purchased separately later at any time. There are no rebuilds needed. Using newly purchased module is very simple (Plug&Play mechanism).
- Licenses***
- 3 months: 150 EUR
 - 6 months: 250 EUR
 - 12 months: 400 EUR
- * Benefits of having license are **only** free updates, thus license is optional. You cannot purchase only license, standard price most

FIG.05

PRECIOS MÓDULOS BOTS

Pero esto aún no ha acabado. La Guardia Civil está intentando arrestar a más gente sobre el caso Mariposa. Y además Iserdo ha estado vendiendo el bot a diferentes grupos, que están creando sus propias redes de bots (como la que vimos en el "Incidente Vodafone").

La Saga Mariposa continúa: nuevas detenciones en Eslovenia, y las autoridades siguen investigando...

Tras los arrestos en Eslovenia, la policía dio una rueda de prensa donde revelaron información sobre el caso. Habían realizado registros en siete viviendas, donde se incautaron 75 dispositivos (ordenadores, discos duros, memorias, etc.). Confirmaron que habían detenido a 2 sospechosos, de 23 y 24 años. Después de 48 horas fueron puestos en libertad, pero la investigación continúa en curso. La policía confirmó que uno de los arrestados es sospechoso de ser el autor del malware (conocido como ButterflyBot) con el que se creó la red de bots Mariposa. Además, también confirmaron que están investigando 2 delitos: la creación de herramientas que posibilitan crímenes informáticos y el lavado de dinero.

Existe más información, no confirmada por la policía eslovena, pero que diferentes medios han encontrado y publicado: el arrestado de 23 años se cree que es Iserdo, el líder, y es conocido en la vida real como Matjaz Skorjanc, de Maribor, Eslovenia. Es un estudiante de medicina fracasado, cuyo padre tiene una pequeña empresa cerca de Maribor dedicada a la venta y desarrollo de dispositivos electrónicos. Resulta que su alias, Iserdo, deletreado al revés es Odresi, que significa “redimir” en esloveno.

La persona de 24 años es Nusa Coh, también de Maribor, y cuyo alias en el IRC es LOLa. Parece que al menos parte del dinero que Iserdo estaba haciendo con la venta del bot estaba siendo pagado a Nusa Coh, aunque puede que ella no supiera cómo estaba Iserdo consiguiendo ese dinero. Ella recibía transferencias de dinero via Western Union de diferentes personas, como Netkairo, el “dueño” de la red de bots Mariposa.

(Si queréis saber porqué todos los criminales usan Western Union os recomiendo leer [este artículo](#) que publiqué hace unos meses).

Durante la investigación apareció otro nombre, Dejan Janzekovic, de 24 años. Él también es de Maribor y trabaja como administrador de sistemas en “Amis”, una compañía eslovena de telecomunicaciones y proveedor de servicios de Internet (ISP). Algunos medios de comunicación le identificaron erróneamente como Iserdo, pero él no ha sido arrestado.

Dejan contactó con los medios e hizo pública su historia, la policía también registró su casa pero parece que él ha sido más bien una víctima. Los investigadores le conectaron con el caso ya que había sido compañero de clase de Nusa Coh (LOLa) en el instituto (2nd gymnasium Maribor). Dejan ha declarado que no ha estado en contacto con ella desde hace muchos años, y que además Iserdo había utilizado una foto suya como identificación en algunas ocasiones.

La semana que Iserdo y LOLa fueron arrestados, la página web utilizada para anunciar y vender el bot fue cerrada. Una semana después del arresto, la web volvió a estar disponible, y pude tomar unas capturas de pantalla:



FIG.06

RED DE BOTS MARIPOSA

Unos días más tarde, el CERT de Eslovenia (SI-CERT) contactó con la compañía que hospedaba la página (West Hosting Corp). Parece que estuvieron encantados de colaborar, ya que desde entonces la página no está disponible.

Nuevos ataques a sistemas SCADA y “Here you have”

Pero si hay un ataque digno de mencionar este trimestre, este es el que se realizó a sistemas **SCADA**. Lo más relevante, además de las víctimas del ataque, es lo elaborado del mismo. Para llevarlo a cabo se utilizó una vulnerabilidad *0-Day* del sistema operativo Windows, y además instalaba un rootkit que estaba firmado digitalmente. La autoría del ataque no está clara, pero lo que sabemos es que no ha sido llevado a cabo por aficionados.

Para acabar el trimestre, volvimos a vivir una situación que no habíamos visto en años, el típico gusano de correo, enviándose con el asunto “Here you have”, al más puro estilo *ILoveYou*. Sin llegar a causar una epidemia, sí que logró infectar a grandes compañías. Como hemos explicado en muchas ocasiones, la creación del malware tiene una motivación económica, motivo por el cual este tipo de gusanos prácticamente ha desaparecido. Entonces, ¿por qué había aparecido este nuevo ejemplar?

Un nuevo gusano hecho “a la vieja usanza” nos sorprendía a todos llegando a infectar a grandes compañías de Estados Unidos: “Here you have”

El gusano conocido como “Here you have” era la 2ª variante de un gusano aparecido en agosto, y una de las características que tenía es que en el mensaje de correo que se enviaba aparecía como remitente “iraq_resistance”, y parecía estar ligado al grupo terrorista “Brigadas de Tariq ibn Ziyad”.

Tres días después de la aparición de esta variante, una persona que se identifica como el creador del gusano publicó un vídeo en YouTube, firmado por “IRAQ Resistance - Leader of Tarek Bin Ziad Group”, y publicado por un usuario con el alias “iqziad”, de 26 años y desde España, según los datos rellenados por el mismo ciberdelincuente en su perfil de YouTube.

Tariq ibn Ziyad al-Layti (en árabe, **دايز بن قراط**, **Tarik** en la transcripción tradicional española) (muerto en 720) fue un general bereber que lideró la invasión musulmana de la Península Ibérica en el siglo VIII, conquistando la Hispania visigoda, según la historiografía tradicionalmente admitida, basada en crónicas árabes de los siglos X y XI.

Según lo que cuenta el vídeo, este gusano ha sido creado y distribuido para afectar principalmente a Estados Unidos por dos razones: para conmemorar los atentados del 11-S y reivindicar el respeto al Islam, haciendo referencia al intento de quema del Corán del pastor Terry Jones.

El vídeo, muestra una imagen estática de Andalucía junto a una foto y un escudo, presumiblemente identificativo del propio grupo. Esta es la traducción al español de la locución del vídeo:

“Hola. Mi Nick es Iraq Resistance. Escuchar las razones que hay detrás del virus del 9 de septiembre que ha afectado a la NASA, Coca-Cola, Google y a muchos jugadores americanos. Lo que quiero decir que es los Estados Unidos no tienen derecho a invadir a nuestra gente y robar el petróleo bajo el nombre de armas nucleares. ¿Lo habéis visto? No hay evidencias de ningún proyecto. Es muy fácil matar y destruir. Segundo, sobre el Cristiano, Terry Jones. Lo que ha intentado hacer el mismo día en que este gusano se distribuyó tampoco es justo. Sé que no todos los Cristianos son iguales, y muchos periódicos han escrito que yo soy un hacker terrorista porque he hecho un virus informático, pero no que Mr. Terry Jones lo es. ¿Y no es él terrorista por haberse metido contra el comportamiento musulmán? Creo, América, venga ya! Sé justo. ¿Dónde está vuestra libertad, que debería acabar contigo??? Como dice tu gente educada y moderna. No sé si realmente hay otro y realmente no quiero “machacar” ordenadores y realmente no hay ninguno afectado como sabéis del informe. Podría “machacar” a todos los infectados, pero no lo haré y no uséis la palabra terrorista, por favor. Espero que la gente entienda que no soy una persona negativa. Gracias por publicarlo”.

II Barómetro Internacional de Seguridad en PYMEs

Por segundo año consecutivo, hemos publicado la segunda edición de nuestro **Barómetro Internacional de Seguridad en PYMEs**. Para su elaboración, este año hemos consultado a 10.470 compañías de diferentes países europeos, latinoamericanos y de Estados Unidos y Canadá, con un tamaño de hasta 1.000 PCs.

En él, y comparado con las cifras de la pasada edición, las compañías españolas han mejorado en la adopción de medidas de seguridad y se sitúan por encima del resto de cifras (92%), pero sin embargo, han registrado un mayor número de infecciones en el último año comparado con la media europea y norteamericana (59% frente a 49 y 65%, respectivamente). Este dato sólo se ve superado por la media latinoamericana, que se sitúa en el 65%.

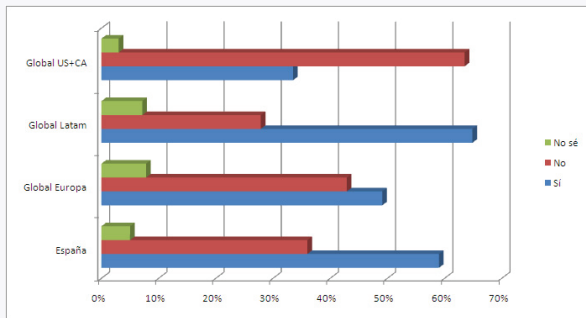


FIG.07

¿SE HA VISTO ALGUNO DE LOS ORDENADORES DE TU EMPRESA AFECTADO POR ALGUNA AMENAZA DE INTERNET?

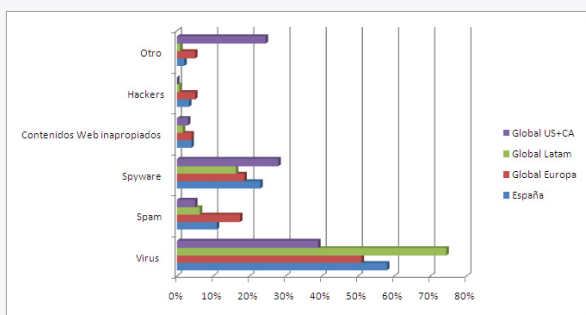


FIG.08

¿POR QUÉ TIPO DE AMENAZA TE HAS VISTO AFECTADO?

La percepción acerca de la necesidad de protegerse es muy alta prácticamente en todas las regiones y países, aunque una media del 7% de usuarios todavía piensa que no es nada importante, razón que ponderan por encima del precio. Entre el 11 y el 13% de los encuestados manifiesta no tener instalado ningún sistema de seguridad.

El 17% de promedio afirma protegerse con soluciones gratuitas. Aún a pesar de que las empresas cuentan con una mayor concienciación y manifiestan estar protegidas en un ratio mayor, el porcentaje de éstas que confirman haber sufrido infecciones en el último año se sitúa en el 52% de media global.

El 52% de las PYMEs se ha infectado en 2010, en su mayoría, a través de dispositivos USB

El correo sigue siendo la vía de entrada de malware más común, junto con la navegación de Internet. Este año, sin embargo, han crecido exponencialmente las infecciones causadas por dispositivos USBs o memorias externas, situándose en una media del 27% de compañías afectadas por esta vía en detrimento de las derivadas del uso de redes P2P, chats o aplicaciones similares.

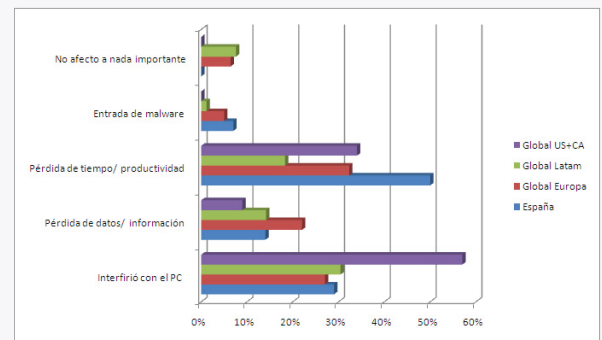


FIG.09

¿CÓMO TE AFECTÓ LA INFECCIÓN?

La pérdida de tiempo y de productividad, así como la interferencia con el PC son las principales consecuencias de haber sido infectados que señalan los usuarios preguntados, a la que sigue la pérdida de datos e información.

En términos generales, las compañías manifiestan haber mantenido la misma inversión en seguridad que el pasado año, aunque a la pregunta de si cuentan con un responsable de seguridad, el 58% en España, el 67% de media en el resto de los países de la Unión Europea, el 68% en Latinoamérica y el 60% en US y Canadá cuentan con esta figura, cifras ligeramente superiores a las de la pasada edición.

El informe completo está disponible en: <http://prensa.pandasecurity.com/wp-content/uploads/2010/07/2ndbarometro.pdf>.

Más infecciones a través de USBs

La distribución de amenazas de Internet a través de dispositivos USB con almacenamiento de memoria es una tendencia al alza de los últimos meses. La infección de las pequeñas y medianas empresas por malware que viaja en estos gadgets y que se ejecuta de forma automática, es ya una realidad. Y es que, además, estudiando las nuevas amenazas creadas en lo que va de año, encontramos que el 25% de los nuevos gusanos están especialmente diseñados para distribuirse a través de dispositivos USB.

Esta información cuadra con los datos expuestos anteriormente del II Barómetro Internacional de Seguridad en PYMEs, en el que el 48% de las PYMEs encuestadas (de 2 hasta 1.000 PCs) confiesa haber resultado infectadas por algún tipo de malware en el último año, y el 27% afirma que la fuente de su infección ha sido un dispositivo con memoria extraíble conectado mediante USB al ordenador.

De momento, este método de infección no supera a las amenazas que utilizan el correo electrónico para distribuirse, pero la tendencia es a aumentar. Prácticamente, cualquier cosa que nos compramos, viene preparada para enchufar al USB del ordenador: cámaras digitales, teléfonos móviles, reproductores MP3 o MP4. Y es una práctica habitual hacerlo, ya que resulta bastante cómodo. Todos estos dispositivos llevan tarjetas de memoria o memorias internas. Por lo tanto, es sumamente sencillo que nuestro teléfono sea portador, sin que lo sepamos, de un virus.

Cómo funciona

Cada vez son más los ejemplares de malware, entre ellos el peligroso gusano Conficker, que se propagan mediante la infección de dispositivos y unidades extraíbles como llaves de memoria, reproductores MP3, cámaras de fotos, etc. La técnica utilizada por estos ejemplares es la siguiente: el sistema operativo Windows utiliza el archivo Autorun.inf de las unidades extraíbles con el fin de saber qué acciones debe llevar a cabo cuando un nuevo dispositivo de almacenamiento externo, como una unidad USB o un CD / DVD, se inserta en el PC.

Este archivo, ubicado en el directorio raíz de los dispositivos extraíbles, ofrece, entre otras cosas, la posibilidad de definir un programa que ejecute automáticamente parte del contenido del dispositivo extraíble cuando éste sea conectado a un PC. Esta funcionalidad está siendo utilizada por los ciberdelincuentes para propagar sus virus, mediante la modificación de ese fichero Autorun.inf con órdenes para que el malware que se ha copiado, por ejemplo, en una llave de memoria USB se ejecute automáticamente en cuanto ésta sea conectada a un PC. Así, ese PC quedaría infectado inmediatamente.

Para prevenir esto, Panda Security ha desarrollado Panda USB Vaccine un producto gratuito que permite llevar a cabo una doble protección preventiva, o vacuna, tanto del mismo PC para deshabilitar la funcionalidad AutoRun, como de unidades y llaves USB individuales, disponible en <http://www.pandasecurity.com/spain/homeusers/downloads/usbvaccine/>.

Índice de Riesgo de las Redes Sociales para PYMEs

Y hablando de informes sobre amenazas y riesgos en empresas, también hemos lanzado en este trimestre el **Primer Índice Anual de Riesgo de las Redes Sociales para PYMEs**. Para esta primera edición, hemos realizado el estudio en Estados Unidos, hablando con responsables de seguridad de 315 empresas de hasta 1.000 empleados hasta el mes de julio.

El 77% de los empleados de PYMEs en EE.UU. utiliza redes sociales en horas de trabajo. El 33% dice que se ha infectado la compañía por malware distribuido a través de estas comunidades

Uno de los primeros datos resultantes es que el uso de redes sociales durante horario de trabajo es una práctica habitual (el 77% de los empleados lo hace), y consecuentemente, el 33% dice que se ha infectado el parque corporativo por malware que se ha distribuido por estas comunidades.

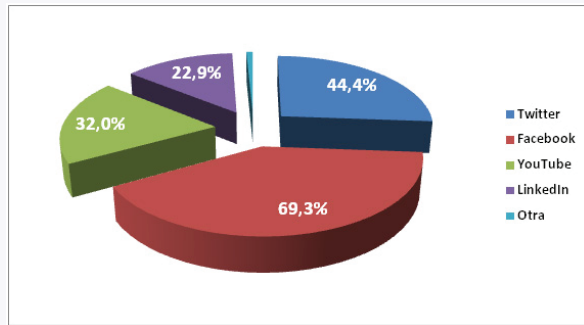


FIG. 10

REDES SOCIALES MÁS UTILIZADAS POR LOS EMPLEADOS DE PYMES EN EE.UU.

Los beneficios de las redes sociales minimizan las preocupaciones

Según el estudio, las mayores preocupaciones de las PYMES respecto a las redes sociales incluyen la privacidad y las pérdidas económicas (74%), infecciones de malware (69%), pérdida de productividad de los empleados (60%) y las relacionadas con la reputación de la empresa (50%), seguida de los problemas del rendimiento y uso de la red (29%).

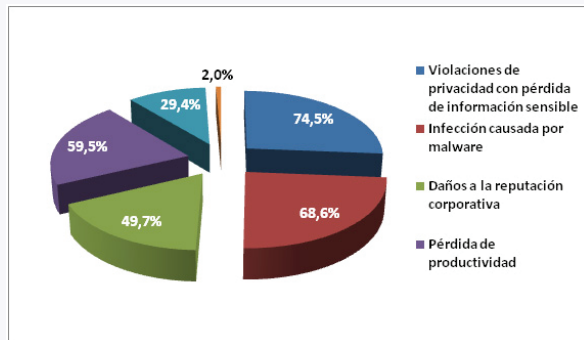


FIG. 11

PRINCIPALES PREOCUPACIONES DE LOS RESPONSABLES DE SEGURIDAD DE LAS PYMES DE EE.UU. DEBIDO A LA UTILIZACIÓN DE LAS REDES SOCIALES POR PARTE DE SUS TRABAJADORES

Sin embargo, esta preocupación no impide a las PYMES la utilización de los beneficios de las redes sociales ya que un 78% de los encuestados reporta que utilizan estas herramientas para apoyar la investigación y la inteligencia competitiva, mejorar su servicio de soporte al cliente, implementar las relaciones públicas y las iniciativas de marketing y generar beneficios directos. Facebook es la herramienta social más popular utilizada por las PYMES: 69% de las empresas tienen cuentas activas en este sitio, seguido por Twitter (44%), YouTube (32%) y LinkedIn (23%).

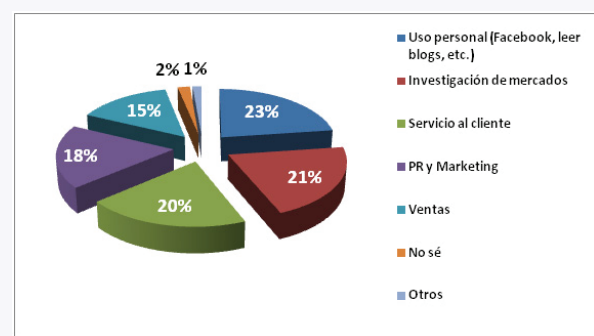


FIG. 12

OBJETIVOS DE UTILIZACIÓN DE LAS REDES SOCIALES POR LAS PYMES DE EE.UU.

Facebook se convierte en la fuente principal de infecciones de malware

Facebook es mencionado como el principal culpable para las compañías que han experimentado infecciones de malware (71,6%) y violaciones de privacidad (73,2%). YouTube ocupa el segundo lugar en cuanto a infecciones (41,2%), mientras que Twitter contribuyó a una cantidad significativa de violaciones de privacidad (51%). Para las compañías que han reportado pérdidas económicas debido a violaciones de privacidad por parte de los empleados, Facebook, fue una vez más el sitio más mencionado como el sitio social en el que se originaron las pérdidas (62%), seguido de Twitter (38%), YouTube (24%) y LinkedIn (11%).

Políticas y educación prevalecen entre las PYMES

Para minimizar los riesgos asociados con las redes sociales, 57% de las compañías tienen en la actualidad políticas de regulación, con un 81% de estas empresas que tienen personal para poner en marcha estas políticas. Además, el 64% de las compañías encuestadas reporta haber tenido programas de formación para educar a los empleados en los riesgos y beneficios de las redes sociales en el trabajo. La mayoría de los encuestados (62%) no permite el uso personal de las redes sociales en el trabajo.

Las restricciones más comunes incluyen: juegos (32%), publicar contenido no apropiado en las redes sociales (31%) e instalar aplicaciones no autorizadas (25%). Además el 25% de las compañías dice bloquear activamente los sitios populares para los empleados, mayoritariamente a través de appliances y/o servicios de seguridad basados en servicios web (45%).

Además, el 35% de las empresas infectadas ha sufrido pérdidas económicas, y más de un tercio de éstas, estima las pérdidas en más de 5.000\$.

El estudio completo puede consultarse en <http://prensa.pandasecurity.com/wp-content/uploads/2010/06/%C3%8Dndice-de-riesgo-de-las-Redes-Sociales-para-PYMES2.pdf>.

Malware en Smartphones... Android ya es el blanco

En artículos anteriores analizábamos la situación del mercado de los smartphones e indicábamos que era más probable que Android se convirtiera en el terminal smartphone más popular. Parece ser que las previsiones se están cumpliendo y, con un parque de terminales aún no excesivamente grande en calle, también están surgiendo las primeras aplicaciones con intenciones maliciosas y por tanto considerables como malware.

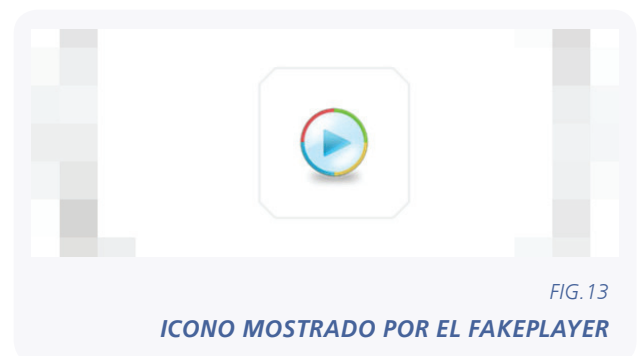
Primeras amenazas

Las primeras amenazas fueron intentos de aplicaciones falsas de acceso a banca online, y estas desaparecieron del Market en poco tiempo ya que fueron denunciadas por usuarios. Estas aplicaciones eran muy simples ya que básicamente mostraban un formulario de acceso en el que el usuario introducía su usuario y contraseña. Se trataban de los primeros intentos de phishing orientados a terminales Android.

Android comienza a ser blanco de hackers, gracias a la popularización de la plataforma y su uso por una gran cantidad de usuarios

Ha sido este verano cuando han empezado a surgir las primeras y más complejas aplicaciones que realizaban acciones maliciosas en el terminal con perjuicio para el usuario.

El primero en salir a la luz fue el Android/FakePlayer.A. Se trataba de una falsa aplicación para reproducir vídeos que lo que realmente hacía era enviar mensajes de texto a números Premium. El usuario infectado con este troyano veía cómo a final de mes su factura de teléfono había engordado considerablemente debido a que el coste de estos mensajes puede ser diez o incluso más veces más caro que un mensaje normal.



El FakePlayer.A era una primera versión muy beta del troyano, ya que analizándolo internamente había código de pruebas e incluso la clase HolaMundo que crean IDEs usados para programar en java como Eclipse.

Posteriormente se distribuyó la variante B del troyano, más depurada y sin código "basura", aun así la aplicación base era la misma y realizaba las mismas acciones.

El mercado del espionaje

La integración de sistemas GPS en los smartphones ha permitido dotar de información geográfica del usuario al terminal para que éste pueda adecuar o adaptar la información a las necesidades del usuario. A su vez, esta información puede ser utilizada con intenciones más oscuras, como el espionaje tanto con fines delictivos como para satisfacer la curiosidad de parejas celosas.

Para cubrir esta demanda existen aplicaciones comerciales orientadas al espionaje y si bien se sitúan en la frontera de lo que es una aplicación legítima: quiero localizar mi móvil si me lo roban, o distribuir mi posición por si me pierdo y me tienen que buscar o controlar la posición de personas vulnerables que pueden estar en peligro en caso de perderse. Pero en el caso de que el terminal sea monitorizado sin el conocimiento o consentimiento del propietario o usuario de éste, podemos decir que se trata de malware malintencionado y más aún cuando este se disfraza de una falsa aplicación o juego como es el caso del TapSnake.

TapSnake es un supuesto juego basado en el famoso Snake, que aparte de permitirte disfrutar del juego geoposiciona el terminal y envía dicha posición a los servidores de la empresa que ofrece los servicios de espionaje. Dicha empresa ofrece otra aplicación también para Android donde podemos ver la posición de los usuarios infectados por TapSnake que hayan sido registrados con una cuenta de correo determinada.

Por tanto, para poder monitorizar a una persona el espía debe animar a la víctima a instalarse el juego en cuestión y registrarlo con una cuenta determinada.

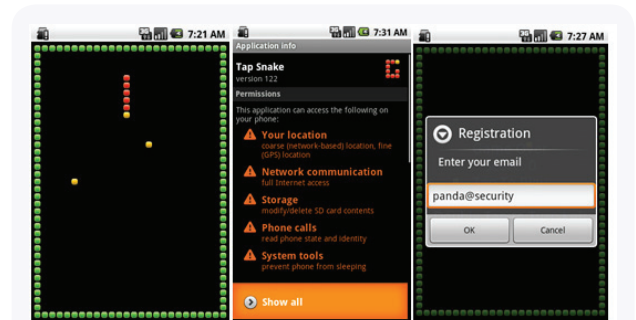


FIG. 14

PANTALLAS DE TAPSSNAKE

Como podemos ver el malware en la plataforma Android sólo acaba de empezar a dar sus primeros pasos pero la fácil distribución de aplicaciones a través del Market hace que los usuarios no tengan mucha necesidad de instalar aplicaciones que no sean distribuidas por el Market.

Por tanto queda por ver qué política de distribución/seguridad va a ser más atacada si la de Market/Store limitado que hace que los usuarios busquen otras fuentes menos seguras de software o un Market/Store más abierto que aunque a primera vista puede parecer más vulnerable a la larga permite que la distribución de software esté más controlada.

Android como reclamo

Por último, comentar que en las últimas semanas están apareciendo aplicaciones de Android legítimas comprimidas con autoextraíbles que infectan las máquinas en las que se trata de descomprimir la aplicación. Es decir, se están empezando a usar las aplicaciones de Android como reclamo para infectar PCs a través de autoextraíbles.

De vulnerabilidades, exploits y 0-Days

A lo largo de este tercer trimestre del año se ha hablado, y se sigue hablando, principalmente de 2 errores de diseño importantes en el sistema operativo de Microsoft Windows.

La historia comienza el 16 de junio de este año cuando se descubre un nuevo *0-Day*, CVE-2010-2568¹, que afecta a todas las versiones de Windows a partir de Windows XP e incluso a las versiones beta de Windows 7 Service Pack 1 y Windows Server 2008 R2 Service Pack 1 y es clasificada por Microsoft como crítica en todas sus versiones.

La vulnerabilidad se produce porque Windows analiza incorrectamente los ficheros de acceso *directo* (ficheros con extensión .lnk y .pif) permitiendo a un usuario malicioso la ejecución remota de código si un usuario visualiza el icono del acceso directo que ha sido modificado para ese fin. Esta vulnerabilidad se empezó a explotar "*In-The-Wild*" utilizando el malware *Rootkit/TmpHider*. Debido a las características de su explotación, al igual que para el malware de la familia autorun, los dispositivos USB son las principales vías para la distribución de malware utilizando esta vulnerabilidad.

Microsoft no tardó en publicar una solución temporal para mitigar esta vulnerabilidad. La solución consistía en eliminar el valor predeterminado de las siguientes entradas de registro de Windows:

```
HKEY_CLASSES_ROOT\lnkfile\shell\IconHandler
HKEY_CLASSES_ROOT\piffile\shell\IconHandler
```

Al eliminar esta funcionalidad del sistema operativo, la vulnerabilidad era corregida, pero se dejaban de visualizar todos los iconos representativos de las aplicaciones que hacían referencia en cada acceso directo dentro del sistema.

Posiblemente debido a que no se consideraba adecuada esta solución temporal propuesta por Microsoft, la comunidad de seguridad en Internet se movió, y se crearon otras soluciones para proteger el sistema sin la necesidad de eliminar los iconos de acceso directo de Windows. Entre ellas, el investigador Didier Stevens conocido por su herramienta de análisis de PDF desarrollada en Python, creó la herramienta *Ariad*² para mitigar la explotación de la vulnerabilidad.

Casi 2 meses después, el 2 de agosto, Microsoft puso fin a esta brecha de seguridad publicando la actualización³ (MS10-046) que corrige finalmente la vulnerabilidad. Desde el departamento de **PandaLabs** recomendamos que se aplique esta actualización a la mayor brevedad posible.

El 28 de agosto, es decir, 26 días después de que Microsoft publicase su solución para la vulnerabilidad antes comentada, se publicaba nuevamente una nueva vulnerabilidad⁴ crítica, que permitía la ejecución remota de código.

La vulnerabilidad se produce debido al orden de búsqueda en las carpetas del sistema que utiliza Windows para la carga de una librería donde no se ha indicado su ruta de la librería en el disco.

Orden de búsqueda de las librerías:

1. Directorio desde el que la aplicación ha sido cargada.
2. Directorio del sistema (%system%).
3. Directorio del sistema para 16 bits.
4. Directorio de Windows.
5. Directorio de trabajo actual (Current Working Directory CWD).
6. Directorios contenidos en la variable de entorno PATH.

¹ <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2568>.

² <http://blog.didierstevens.com/2010/07/18/mitigating-lnk-exploitation-with-ariad/>.

³ <http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx>.

⁴ <http://www.microsoft.com/technet/security/advisory/2269637.mspx>.

Utilizando la función `LoadLibrary`⁵ se puede cometer este descuido. Como se puede observar en el siguiente ejemplo, el programador no indica la ruta completa de la librería `mylibrary.dll`.

```
HMODULE handle = LoadLibrary("mylibrary.dll");
```

Bajo estas circunstancias, la librería maliciosa será cargada por el programa si se encuentra en una ruta anterior al orden de búsqueda en la que se encuentra la librería original del programa.

Para evitar esta posible amenaza se muestra el siguiente código que no es vulnerable porque se está indicando la ruta de la librería.

```
HMODULE handle = LoadLibrary("c:\\windows\\system32\\mylibrary.dll");
```

Un ejemplo real es la aplicación iTunes de Apple que es vulnerable a este ataque. Si un usuario malicioso comparte una carpeta con diferentes ficheros multimedia en una ruta accesible por otros usuarios y si uno de estos usuarios intenta reproducir uno de los ficheros ubicado en ese recurso compartido, cuando iTunes necesite cargar una librería de forma dinámica comenzará su búsqueda en ese mismo directorio, donde está ubicado el fichero que desea reproducir. En este caso, si el usuario malicioso ha copiado en esa ubicación una librería similar a la que necesita cargar iTunes, el sistema podría quedar comprometido al ejecutarse el código de la librería maliciosa en vez de la librería solicitada.

A diferencia de otras vulnerabilidades publicadas por Microsoft en sus boletines de seguridad donde nos proporciona una actualización para los entornos vulnerables, en esta situación, es el propio fabricante de la aplicación quien debe ser el encargado de publicar la solución, p.e., a través de una actualización del software vulnerable.

En su ayuda por corregir el problema, Microsoft ha creado una nueva entrada de registro con el nombre `CWDIllegalDllSearch` que permite a los usuarios controlar el algoritmo de ruta de búsqueda de la librerías que serán cargadas de forma dinámica por los programas.

La información actualizada de esta nueva funcionalidad introducida por Microsoft la podemos encontrar en el siguiente enlace <http://support.microsoft.com/kb/2264107>.

Continuando con la empresa Apple, el día 29 de Agosto el investigador Rubén Santamarta publicó un nuevo *0-Day* que permite la ejecución arbitraria de código en la aplicación Quicktime Player 7.x y 6.x. La vulnerabilidad es aprovechada debido a un despiste del programador al no eliminar el parámetro `__Marshaled_pUnk` del plugin "QTPlugin.ocx" que había sido utilizado en versiones anteriores del plugin.

Con su investigación Rubén Santamarta no solo ha conseguido descubrir un nuevo *0-Day*, sino que además ha creado un exploit capaz de saltarse las protecciones ASLR⁶ y DEP⁷ para demostrar de forma exitosa la explotación de esta vulnerabilidad en las diferentes versiones de sistema operativo de Microsoft incluyendo Windows 7.

Toda la información de este descubrimiento ha sido detallada por el propio autor en la siguiente página: http://reversemode.com/index.php?option=com_content&task=view&id=69&Itemid=1.

Vamos a cerrar el informe para este trimestre con el último *0-Day* que se ha descubierto en los programas Adobe Acrobat y Adobe Reader. Aunque ésta pueda parecer una de las habituales noticias que podemos leer sobre este producto, la peculiaridad de esta vulnerabilidad ha sido la forma en la que el atacante se las ha ideado para explotarla.

La vulnerabilidad es un *buffer overflow* en la librería `CoolType.dll`. Esta librería llama a la función del sistema `strcat`⁸ la cual es insegura al no tener la capacidad de indicar el tamaño de buffer que se quiere añadir al buffer destino.

5 [http://msdn.microsoft.com/en-us/library/ms684175\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms684175(VS.85).aspx).

6 http://en.wikipedia.org/wiki/Address_space_layout_randomization.

7 http://en.wikipedia.org/wiki/Data_Execution_Prevention.

8 [http://msdn.microsoft.com/en-us/library/bb759925\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb759925(VS.85).aspx).

Si el buffer que se desea añadir es superior al espacio libre restante donde se desea copiar, se producirá un *buffer overflow*. Es como intentar llenar 1,5 litros de agua en una botella que tiene capacidad para solo 1 litro.

Microsoft, en su página de información de API de Windows, ya está indicando que no se debe usar (mirar el enlace citado sobre la función `strcat`).

```
LPTSTR StrCat(  
    __inout LPTSTR psz1,  
    __in LPCTSTR psz2  
);
```

Note: Do not use. See Remarks for alternative functions.

VUPEN especialista en la creación de exploits para esta aplicación nos muestra en este artículo "Criminals Are Getting Smarter: Analysis of the Adobe Acrobat/ Reader 0-Day Exploit"⁹ cómo el atacante ha sido capaz de evitar las protecciones ASLR y DEP en Windows utilizando un método nunca antes visto.

Sin entrar en muchos detalles técnicos, cuando se produce un *buffer overflow*, normalmente se intenta sobrescribir la dirección de retorno o el manejador de excepciones para cambiar el flujo de la ejecución del programa y así el usuario malicioso puede ejecutar su código inyectado. No obstante, en esta ocasión no es factible, debido a la protección de Microsoft que verifica los posibles *buffer overflow* (opción `/GS`¹⁰ del compilador de Visual Studio) y al manejo de las excepciones, el conjunto y la configuración de ambas protecciones en el código impiden, en esta ocasión, una explotación satisfactoria de la vulnerabilidad.

No obstante, el atacante va más allá y descubre una vía para poder explotar la vulnerabilidad de forma satisfactoria sin la necesidad de sobrescribir la dirección de retorno o el manejo de excepciones para llegar a controlar el flujo de la ejecución. Sin embargo, el usuario malicioso aún tenía que solventar las protecciones de ASLR y DEP. Superar ASLR fue "sencillo", utilizó la librería `icucnv36.dll` que no es compatible con este sistema de protección y creó un *exploit* utilizando la técnica ROP¹¹. No obstante, esta librería no importa las funciones `VirtualAlloc`, `VirtualProtect`, `HeapCreate`, `WriteMemory` ni siquiera `LoadLibrary`, necesarias para evitar la última protección, DEP. Así que el usuario se las ingenió para utilizar las funciones `CreateFileA`, `CreateFileMappingA`, `MapViewOfFile` y `memcpy` que éstas sí que estaban importadas por la librería para poder ejecutar el código malicioso en la máquina comprometida. Un análisis más detallado de cómo el usuario pudo explotar la vulnerabilidad se encuentra en el artículo que antes hemos citado.

En este exploit se puede observar los altos conocimientos técnicos de los creadores de malware en su carrera por infectar el mayor número de máquinas, evitando las últimas protecciones que proporciona Microsoft en su sistema Windows. ASLR y DEP son dos protecciones muy competentes frente a este tipo de vulnerabilidades siempre y cuando ambas estén activadas y todos los módulos del programa sean compatibles con ASLR. En esta ocasión la librería `icucnv36.dll` ha sido el talón de Aquiles y causante de una explotación satisfactoria de la vulnerabilidad.

⁹ <http://www.vupen.com/blog/>.

¹⁰ [http://msdn.microsoft.com/en-us/library/8dbf701c\(VS.80\).aspx](http://msdn.microsoft.com/en-us/library/8dbf701c(VS.80).aspx).

¹¹ http://en.wikipedia.org/wiki/Return-oriented_programming.

Incidencia del malware en el mundo

Hace poco, nos preguntaban a través de Twitter qué habría que hacer para acabar con el malware... La verdad es que la pregunta se las trae, porque la respuesta más adecuada sería parecida a las que hacen las misses en los concursos de belleza: "Quiero la paz en el mundo".

Existe tanto dinero moviéndose en el underground generado por las actividades delictivas de las cibermafias de las que hablamos continuamente, que la cantidad de malware que se genera buscando nuevas víctimas sigue creciendo.

Además, las infecciones se mantienen también en niveles muy altos, debido a que cada vez utilizan diferentes canales de distribución, buscando sorprender y, a la vez, engañar a los usuarios: cuando ya te has acostumbrado a reconocer amenazas que llegan por el correo electrónico, de repente te infectas a través de una red social, o por una falsa web...

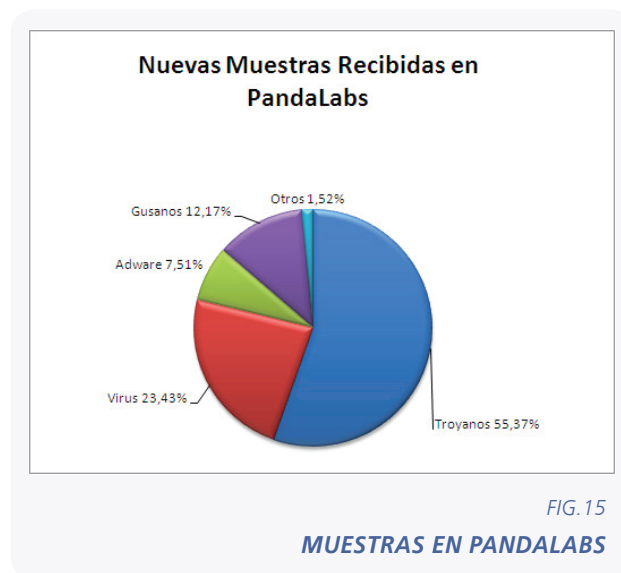
Pero he de decir que la pregunta, que puede parecer genérica y global, sí tiene una respuesta válida: el cibercrimen al menos se frenará cuando se consiga una mayor colaboración internacional y se detengan a más ciberdelinquentes. Y cuando a éstos, además, no les compense cometer sus crímenes, porque las penas impuestas sean adecuadas al acto cometido.

Mientras las entidades gubernamentales y las autoridades no dediquen más atención y foco en la investigación, no se cultiven las relaciones internacionales para fomentar la cooperación y no se endurezcan las penas impuestas a los hackers detenidos, la situación seguirá la misma tendencia: es decir, seguirá creciendo.

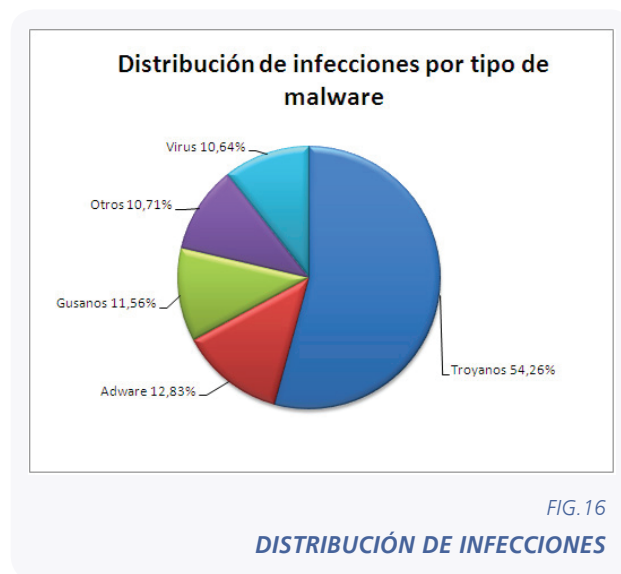
Y eso es precisamente lo que encontramos revisando las cifras de lo que ha ocurrido con el malware en este tercer trimestre.

Echando un vistazo al reparto por tipo de amenazas que hemos recibido en **PandaLabs** durante estos tres meses, podemos observar que más o menos se mantiene el reparto de la tarta, aunque los troyanos crecen 4 puntos en peso de su categoría comparándolo con el pasado trimestre.

Es lógico: los troyanos están, en su mayoría, destinados a conseguir beneficio económico, y por eso son los que mayor ROI (Retorno de la Inversión) dan a sus creadores.

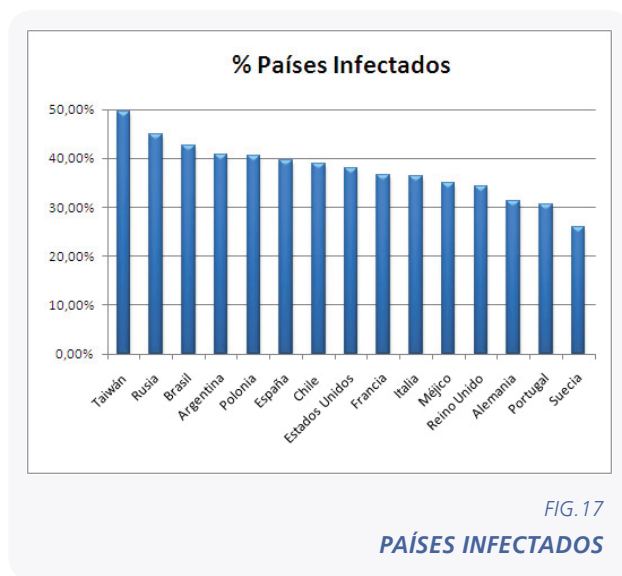


Consecuentemente, el índice de infecciones a nivel mundial tiene su correspondencia con el nuevo malware creado, ya que los usuarios y empresas afectados por la categoría de Troyanos sigue aumentando. Incluso ha subido 5 puntos, comparado con el trimestre anterior.



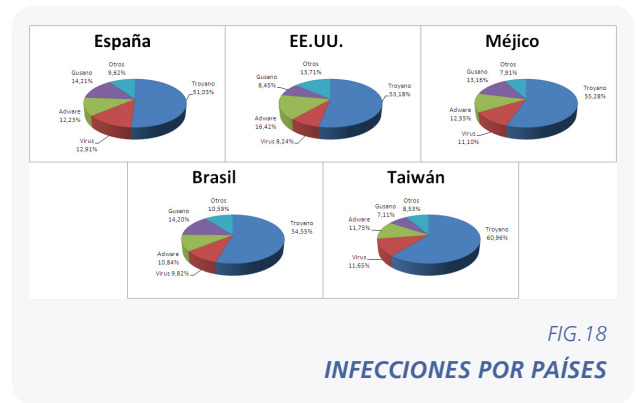
Estos datos son extraídos de nuestro antivirus online y gratuito Panda ActiveScan (www.activescan.com). Las cifras no solo tienen en cuenta el malware activo, es decir, aquel que está en ejecución en el momento de realizar el análisis, sino también el malware latente, que es aquel que está alojado en el ordenador pero que aún no ha sido ejecutado. Puede ser ejecutado por el propio usuario o puede estar a la espera de ser ejecutado remotamente.

Y mirando cómo están los países, éste es el ranking por porcentaje de infecciones:

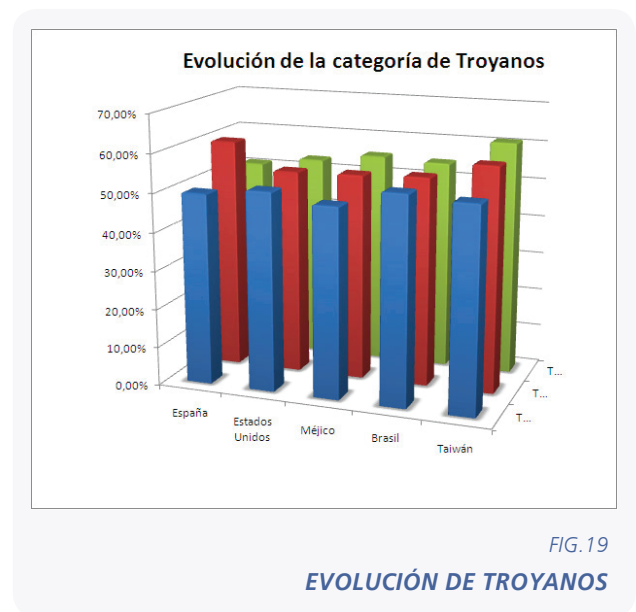


Nos llama particularmente la atención la escalada de Brasil, que en el anterior informe trimestral se encontraba en el puesto número 6, y ha ascendido hasta el 3; y el caso de Chile, que en el anterior no aparecía en este ranking, pero se ha situado súbitamente en el puesto número 7.

Si os estáis preguntando por qué tipo de malware se han infectado los usuarios de estos países, a continuación podréis verlo con detalle, pero no hay sorpresas: la categoría que más infecta, por encima del resto, es la de troyanos, como cabía esperar, por las razones anteriormente expuestas:



Y ya que tenemos unos protagonistas de excepción, vamos a echar un vistazo a la evolución de las infecciones por país de la categoría de los troyanos:



La situación es variable: en unos países crece y en otros, decrece, pero con una variación tan leve, que no se puede hablar ni de tendencia a la baja ni de repunte: vemos que los métodos de infección les siguen funcionando a los hackers, ya que con los troyanos, siguen consiguiendo su objetivo.

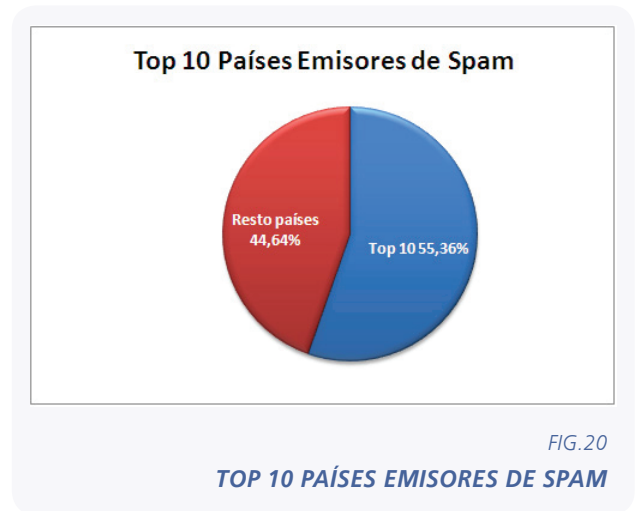
En términos globales, podemos decir que de cada 10 potenciales víctimas que reciben troyanos, 5 –es decir, la mitad– se infecta a causa de éstos. Estaría bien saber finalmente de ese 50%, cuántos son víctimas de fraude financiero o de robo... Pero para tener estos datos, creo que todavía tendremos que esperar un poco a que desde los organismos o cuerpos de seguridad que reciben las denuncias por país, se ofrezca un mayor flujo de información.

Datos de Spam

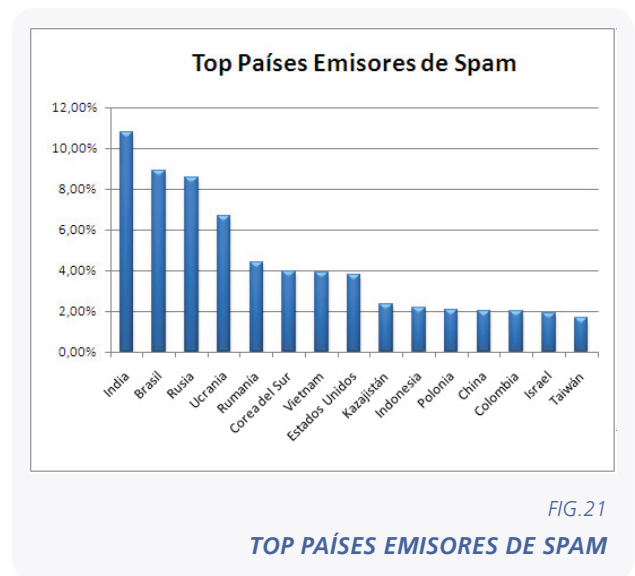
Bueno, la situación del spam tampoco ha mejorado, la verdad. Como siempre decimos, los cibercriminales buscan mil y una maneras para que el spam llegue a su destinatario, y a medida que las soluciones de seguridad son capaces de detectarlos, van variando sus técnicas para saltarse estos filtros y alcanzar sus objetivos.

La verdad es que cada vez que observamos este tipo de spam, nos sorprende más que pueda haber víctimas que caigan en la trampa, porque estos delincuentes ya no pierden mucho tiempo en esmerarse con el diseño ni con el mensaje. Pero eso sí, se esmeran probando nuevas formas de distribución, incluso enviándolo como un fichero .mp3.

En estos tres meses, el 95% del correo que circulaba por la red era spam. En su mayoría, son las redes de bots (ordenadores "secuestrados" que esperan órdenes de un hacker) las que se encargan de su distribución, sin que el dueño del PC sepa siquiera que está enviándolo y, por lo tanto, cometiendo un delito. Y en este período, el Top 10 de países se ha llevado el 55% de todo el spam mundial que ha circulado por la red.



¿Cuáles son estos países? Los que puedes ver a continuación:



Tampoco hay excesivas sorpresas, si lo comparamos con el anterior trimestre. Quizá lo más reseñable sea la desaparición del ranking (de momento) del Reino Unido, que algo estará haciendo para evitar clasificarse en este top.

Sinceramente, nos gustaría en algún momento cerrar una de las ediciones de este informe (ya sea trimestral o anual) con un mensaje positivo porque la situación hubiese mejorado, pero el Consejo de Redacción que elabora este dossier, tras un rato de deliberación, ha acordado que no es todavía el momento...

Creo que las razones están bien claras: sigue habiendo más malware, las cibermafias siguen consiguiendo infectar, cada vez hay nuevos métodos que sorprenden a los usuarios, ya están haciendo target en Smartphones... En fin, nada que nos sorprenda.

Sin embargo, sí cabe reseñar el éxito que se está teniendo, en diferentes países, con la desarticulación de la botnet Mariposa primero, y del "negocio" de venta del kit original, Butterfly. La colaboración que comenzó el pasado año, sigue dando sus frutos, y creemos que todavía quedan algunas detenciones por llevar a cabo. Sin duda, éste sigue siendo un excelente ejemplo de trabajo en equipo y colaboración internacional.

Nosotros seguimos haciéndolo, focalizándonos en diferentes casuísticas y con diferentes cuerpos de policía de diversos países. Esperamos que en próximas ediciones podamos contaros algunos de los casos, porque querrá decir que han resultado exitosos y han acabado con algunas detenciones y desarticulaciones.

En los próximos meses estaremos cerrando el año... Todos, también los cibercriminales, que en su organización empresarial querrán sacar el máximo beneficio posible antes de retirarse a celebrar el cambio de año (si es que lo celebran).

Por lo tanto, ¿qué veremos? Más malware, nuevos métodos de distribución, más ataques de BlackHat SEO, más bichos para las nuevas plataformas...

Ojo con Mac, que empieza a despegar en cuanto a malware se refiere... y no solo para ordenadores, sino para iPads, iPhones, etc... Lo tendremos en nuestro radar para sucesivos informes. Siempre hemos dicho que comenzará a despuntar el cibercrimen para usuarios Mac cuando Apple consiga una respetable cuota de mercado mundial, y ya lo está haciendo. Y en el momento en que se convierta en blanco, creemos que va a pillar a su comunidad de usuarios desprevenida. Así que nuestra recomendación es que más vale protegerse por el "por si acaso" que después tener que lamentar...

Y también tendremos varios ojos puestos en los dispositivos móviles (ya hemos visto que Android empieza a despegar en el mundo del malware...).

No nos extrañaría que de aquí a final de año veamos más gusanos hechos a la antigua usanza como el "Here you have"... Pero estaremos prevenidos para minimizar su impacto.

Y como la próxima cita que tenemos será ya en 2011 (a primeros de año sacaremos nuestro informe-resumen anual), dejadme que sea el primero en deciros "Feliz Navidad" (aunque sea pronto, en algunos países no se celebre, etc...) ;-).

Gracias por seguirnos. ¡Espero que lo hayáis disfrutado!

PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- Desde **PandaLabs** se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.
- **PandaLabs** se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.
- Del mismo modo, **PandaLabs** mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad. Su objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.
- Se puede obtener información sobre las últimas amenazas descubiertas en el blog de **PandaLabs** en: <http://pandalabs.pandasecurity.com/>.

