Informe trimestral PandaLabs

Abril - Junio **2011**

01| Introducción

El título de la canción de Guns N' Roses "Welcome to the Jungle" (en español, "Bienvenidos a la Jungla") es el mejor resumen que podemos hacer sobre lo sucedido en el mundo de la seguridad este segundo trimestre de 2011. La cantidad de ataques sufridos por grandes empresas y corporaciones ha hecho saltar la alarma, al ver que sistemas que considerábamos confiables, o empresas en las que depositábamos nuestra confianza, y aún más importante, nuestra información personal, nos han defraudado.

Está claro que el principal culpable es y siempre será el delincuente que perpetra el robo, pero si quien guarda tu información se deja la puerta abierta y no tiene unas mínimas medidas de seguridad es una negligencia que no debe pasarse por alto.

Pero no todos los ataques han tenido como objetivo el robo de información personal para enriquecerse, hemos visto actos de posible ciberespionaje como el ocurrido en el Fondo Monetario Internacional (FMI), y vandalismo como el perpetrado por Anonymous y más recientemente por esa especie de spin-off del grupo autodenominado "LulzSec", afectando tanto a empresas privadas como a entidades oficiales como el Senado de Estados Unidos o la mismísima CIA.

02| El trimeste de un vistazo

Ciberactivismo, ciberguerra, ciberdelincuencia… son conceptos que cada día utilizamos más. De hecho, en los últimos informes que hemos realizado han tenido sus apartados propios. Normalmente es relativamente sencillo clasificar los diferentes ataques/incidentes de seguridad en función del objetivo perseguido: está muy claro que sabotear una centrifugadora de uranio en Irán es un acto de ciberguerra, o que el robo de datos de personales de una empresa es un acto de ciberdelicuencia. Además, el ciberactivismo como tal no es algo malo, aunque la comisión de delitos en su nombre le haya otorgado una connotación negativa.

Sin embargo, este trimestre vemos cómo algunas de estas líneas imaginarias se difuminan, y vemos ataques que se podrían incluir en varios apartados, si no en todos.

De ‘hacktivistas’ a ‘estupidistas’

El grupo Anonymous parece que para protestar tiene que llevar a cabo actos ilegales. Si sus integrantes fueran mínimamente inteligentes, se darían cuenta de que su incapacidad de protestar sin violar la ley hace que sus denuncias pierdan legitimidad. Durante los últimos meses han perpetrado ataques contra la web de la Cámara de Comercio de Estados Unidos, Sony, la Policía Nacional española, webs de diferentes gobiernos y un largo etcétera.

Además se justifican publicando comunicados en los que indican que sus actos son “protestas pacíficas”, a pesar de las pérdidas económicas que causan y las ilegalidades que cometen. Dicen representar y ser la voz de “el pueblo”, a pesar de lo cual no son capaces de dar la cara, escondiéndose tras seudónimos.

Por si no tuviéramos bastante con Anonymous, ha aparecido otro grupo autodenominado LulzSec, que opina que el vandalismo y la delincuencia es algo divertido (sic). Si los más inconscientes de Anonymous se juntaran para formar un grupo, parecerían caballeros de exquisita educación al lado de LulzSec.

FIG.01. *IMAGEN DE PERFIL UTILIZADA POR LULZSEC EN SU PERFIL DE TWITTER.*

Su principal método de "trabajo" ha sido robar bases de datos de diferentes empresas (PBS, Fox, etc.) además de alguna denegación de servicio (como el llevado a cabo a la página web de la CIA). Por si esto no fuera suficiente, han publicado los datos personales de usuarios que previamente habían robado, incluyendo direcciones de correo, contraseñas, etc. lo que ha facilitado que se realicen todo tipo de secuestros de cuentas y robos.

A finales de junio, LulzSec y Anonymous lanzaron una operación conjunta llamada "Operation: Anti-Security" con el objetivo de atacar a páginas de cualquier gobierno o entidad gubernamental que se cruce en su camino.

La incoherencia de Lulzsec queda claro en un suceso que relato más adelante, donde le robaron a Sega datos de más de un millón de sus clientes: al principio hubo quien pensó que era obra de Lulzsec, pero enseguida salieron a desmentirlo y de hecho ofrecieron sus servicios a Sega para dar con los culpables del delito. Como buenos defensores del totalitarismo, cometer delitos es bueno sólo si ellos los protagonizan, en caso contrario está muy mal y hay que destruir al "competidor".

FIG.02. *MENSAJE DE LULZSEC A SEGA ENVIADO A TRAVÉS DE TWITTER.*

La escalada de actos vandálicos siguió imparable, alcanzando su punto álgido con su "operación Chinga la Migra" en la que robaron y publicaron información de la fuerzas del orden del estado de Arizona. Entre la información hecha pública se encontraban documentos confidenciales y todo tipo de información personal de agentes de las patrullas fronterizas.

```
So with those last thoughts, it's time to say bon voyage. Our planned 50 day cruise has expired, and we
must now sail into the distance, leaving behind - we hope - inspiration, fear, denial, happiness,
approval, disapproval, mockery, embarrassment, thoughtfulness, jealousy, hate, even love. If anything,
we hope we had a microscopic impact on someone, somewhere. Anywhere.
```

FIG.03. ÚLTIMO COMUNICADO *DE LULZSEC.*

A continuación se comenzaron a ver movimientos "anti-LulzSec", donde grupos similares comenzaron a trabajar para desenmascarar a LulzSec. Se cree que como consecuencia de la información obtenida por estos grupos la policía británica detuvo a Ryan Cleary, un adolescente de 19 años, que administraba un servidor de IRC relacionado con LulzSec.

El día 26 de junio, a través de su cuenta de Twitter, LulzSec anunció su disolución en un comunicado. En su cuenta de Twitter animaron a la gente a continuar la operación Anti-Security (#Antisec) y unirse al canal de IRC de Anonymous.

FIG.04. *LULZSEC PIDIENDO A LA GENTE SU APOYO A ANONYMOUS.*

No todo son malas noticias, ya que se han producido varios arrestos de miembros de Anonymous en este trimestre, como 3 personas en España que estaban muy involucradas en la organización, y otros 32 en Turquía.

El trimestre negro

Además de los lamentables sucesos protagonizados por Anonymous y LulzSec, nos encontramos ante uno de los peores trimestres de la historia si analizamos la cantidad de diferentes ataques que han sucedido. En marzo RSA hizo público que habían detectado una intrusión que había conllevado el robo de información sobre el diseño de su conocido sistema de doble factor de autenticación "SecureID".

FIG.05. *ROBO DE INFORMACIÓN DEL SISTEMA DE AUTENTIFICACIÓN "SECUREID".*

En mayo Lockheed Martin, el primer contratista del Departamento de Defensa de Estados Unidos sufrió una intrusión gracias al uso de la información robada meses atrás a RSA. Parece que los que robaron la información han conseguido comprometer el algoritmo utilizado para generar las claves. RSA tendrá que cambiar los más de 40 millones de SecurID que tienen sus clientes, entre los que se encuentran las más importantes empresas del mundo.

Este mismo mes se conoció que ordenadores militares de Noruega habían sido atacados en marzo: unos 100 militares –muchos de ellos de alto rango- recibieron un correo electrónico en noruego, que incluía un fichero adjunto. Este fichero era un troyano creado para robar información. Según la información hecha pública, uno de los ataques tuvo éxito aunque desde ese ordenador no se tenía acceso a información crítica.

En junio se descubrió que el Fondo Monetario Internacional había estado comprometido durante meses, aunque debido a la escasa información que se ha hecho pública desconocemos la motivación detrás del ataque. Es bastante probable, debido al tipo de delicada información que maneja la institución, que se trate de un ataque dirigido. Sin embargo tampoco podemos descartar que se trate de un caso de cibercrimen común.

El sitio web de la Agencia Espacial Europea fue hackeada y todos los datos robados fueron hechos públicos. Entre los datos se encontraban nombres de usuario, cuentas ftp, e incluso las contraseñas de las cuentas ftp que se encontraban ¡en texto plano!
Citigroup ha protagonizado otro incidente vergonzoso, donde información de 360.000 cuentas ha sido comprometida. Lo peor de este ataque, es que ni siquiera hubo la necesidad de hackear un servidor, simplemente "jugando" con la URL podías acceder a la información de otra cuenta.

Sega, la popular compañía japonesa de videojuegos, ha sido otra de las víctimas: los datos de 1,3 millones de usuarios de su red Sega Pass fueron robados el pasado mes de junio, incluyendo nombres de usuario, fechas de nacimiento, direcciones de correo y contraseñas, aunque éstas estaban cifradas, por lo que se minimiza algo el riesgo si el cifrado utilizado es fuerte, algo que vistas experiencias pasadas no está suficientemente extendido.

Sonygate

Pero si hay un ataque que debe figurar en el muro de la vergüenza, es el que sufrió Sony. Empezó con el robo de datos en su red PlayStation Network (PSN) que afectó a los datos de 77 millones de usuarios de todo el mundo. No sólo se trata del mayor robo de datos de usuarios de la historia, sino que el manejo que hizo la compañía fue catastrófico: ocultó el problema durante días, y cuando lo hizo público dijo que datos de usuarios podrían haber sido comprometidos cuando sabían fehacientemente que habían sido robados.

Para agravar aún más la situación, los datos robados eran especialmente sensibles, ya que incluían el nombre, dirección completa del usuario, dirección de correo electrónico, ID de PSN, contraseña (todo parece indicar que no estaba cifrada), fecha de cumpleaños, historial de compras, nº de la tarjeta de crédito (sólo de los usuarios que tenían almacenada esta información, se calcula que es un 10%), fecha de caducidad de la misma…

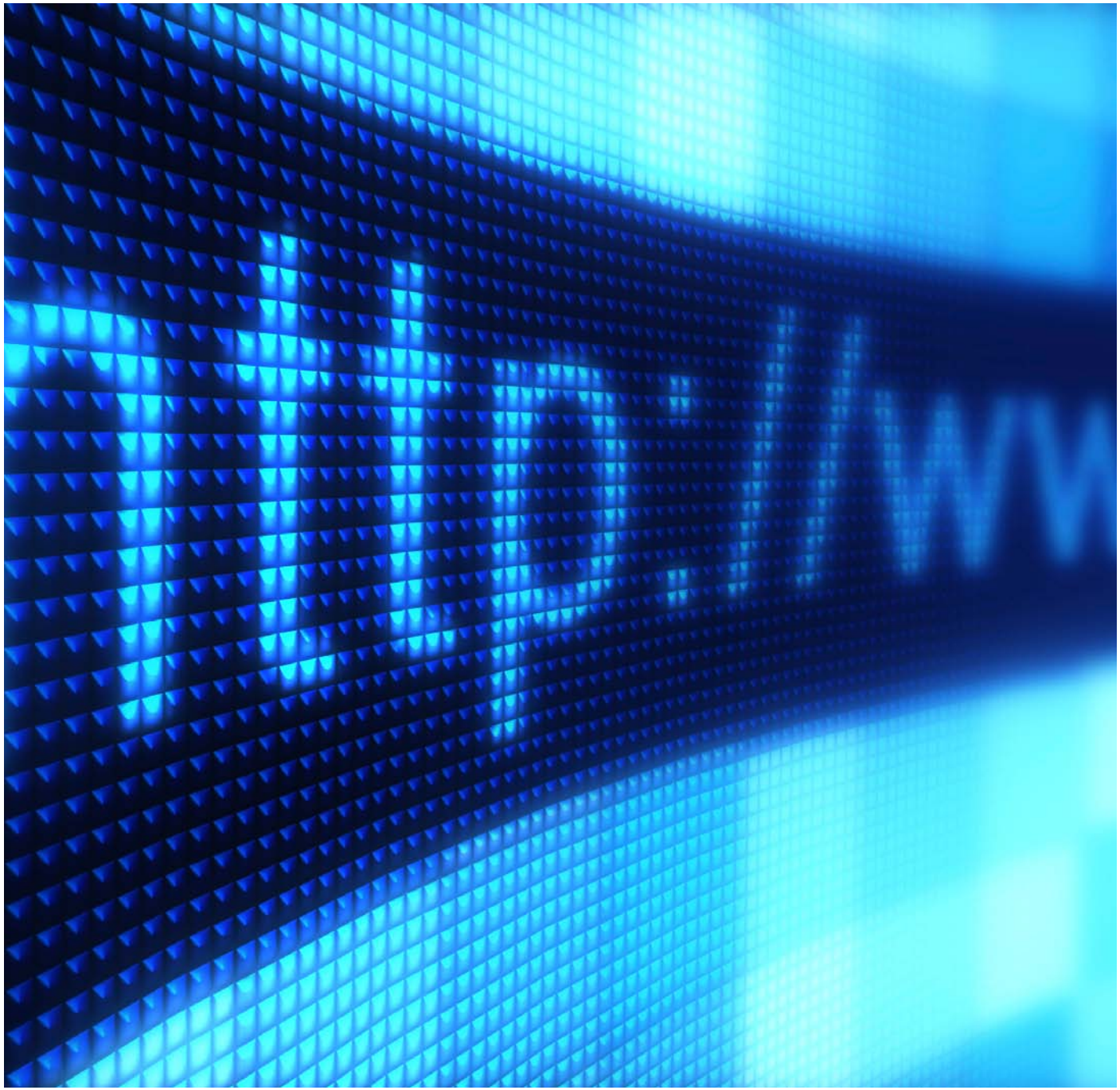
Si esto no fuera suficiente, días después sufrió otro ataque Sony Online Entertainment, sufriendo un robo de datos similar que afectó a otros 24 millones de usuarios.

Malware

Además de todos los ataques que hemos contado, hemos visto cómo este trimestre se han repetido los ataques "tradicionales" de los que también somos víctimas los usuarios. Las tendencias respecto a los últimos tiempos se mantienen, en plataformas Mac hemos visto por primera vez un ataque a gran escala, protagonizada (¡cómo no!) por falsos antivirus. A pesar de que la instalación del falso antivirus (llamado MacDefender) afectó a miles de usuarios de todo el mundo, Apple quiso escurrir el bulto negando la evidencia. Días después reculó, y publicó una "actualización de seguridad" (sic) que protegía contra este malware. En cuestión de minutos comenzaron a aparecer nuevas variantes, como MacShield, que se saltaban esta actualización de Apple, algo lógico si vemos que se basa en tecnología que tiene más de 20 años y que hoy en día está claramente superada, siendo inservible a no ser que se combine con técnicas modernas como el análisis por comportamiento.

En el mundo de los móviles todo transcurre "sin novedad", es decir, siguen incrementándose los ataques de malware a plataformas Android. No llegan ni mucho menos a los niveles de los ataques que ha sufrido Apple con los falsos antivirus pero como algo no cambie en breve empezará a ser un problema con mayúsculas.

El mundo de las redes sociales deja claro que los usuarios somos capaces de chocar con la misma piedra una y otra vez. Hemos visto como las típicas campañas en Facebook de "Descubre quién visita tu perfil" y similares consiguen un gran éxito afectando a miles de usuarios cada vez.



03| El trimeste en cifras

Vamos a proceder al análisis de las cifras de malware de este trimestre. La aparición de malware sigue siendo masiva, y es que la creación de 42 nuevas muestras de malware al minuto no nos augura nada bueno. Si echamos un vistazo a qué tipo de malware es el que se está creando, vemos que no hay un cambio de tendencia, teniendo en primer lugar a los troyanos, tipo de malware al que pertenecen el 68,34% de las muestras. El motivo del protagonismo de este tipo de malware, como hemos comentado en anteriores informes, es que es el idóneo para ser utilizado por los ciberdelincuentes para llevar a cabo robos de información, su principal fuente de ingresos.

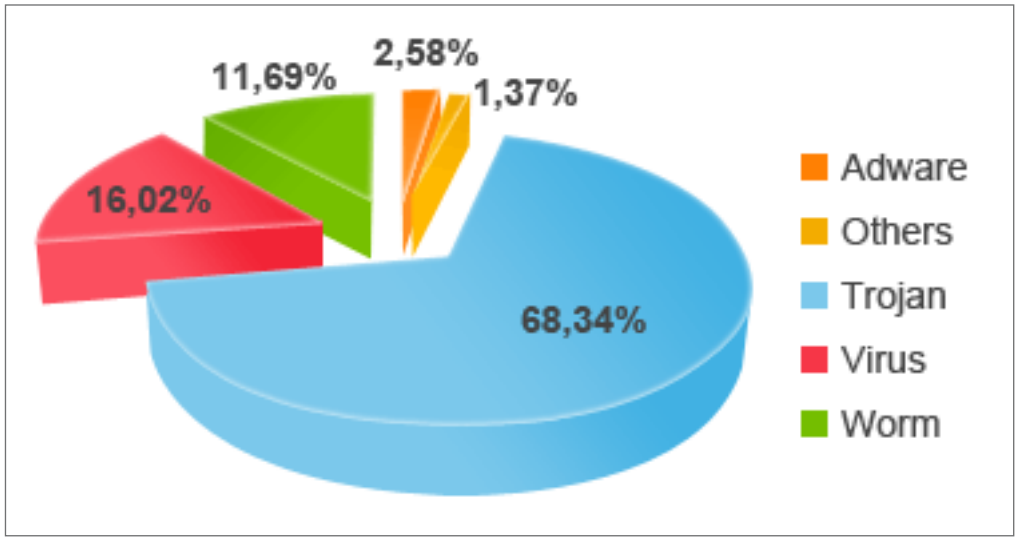


FIG.06. *NUEVAS MUESTRAS DE MALWARE DETECTADAS EN PANDALABS.*

La segunda posición la ocupan los virus, con un 16,02%. Aunque los virus parecen cosa del pasado, su resurgir tiene una fácil explicación: hay unas pocas familias muy activas, apareciendo continuamente nuevas variantes que infectan a los usuarios. ¿Por qué existe esta actividad, cuando lo que buscan los creadores de malware es robar información? Porque estas familias de

virus tienen características de troyano, y roban información de los usuarios, como en el caso del Sality o del Viking.

En tercer lugar nos encontramos con los gusanos, y en cuarto con el Adware, principalmente debido a que dentro de esta categoría se incluyen los falsos antivirus, también conocidos como rogueware. Se tratan de programas que simulan ser antivirus u otras herramientas de seguridad y mantenimiento del PC, buscando que la víctima les pague por un servicio que realmente no existe. Ya en 2009 realizamos un estudio en el que estimamos que los ciberdelincuentes hacían más de 400 millones de dólares sólo con la venta de falsos antivirus.

En cualquier caso, los números de los que estamos hablando recogen la cantidad de muestras creadas y su tipología, pero no las infecciones. Veamos a continuación la distribución del tipo de malware que ha infectado ordenadores durante el segundo trimestre de 2011, en base a los datos obtenidos por nuestra herramienta gratuita Panda ActiveScan:

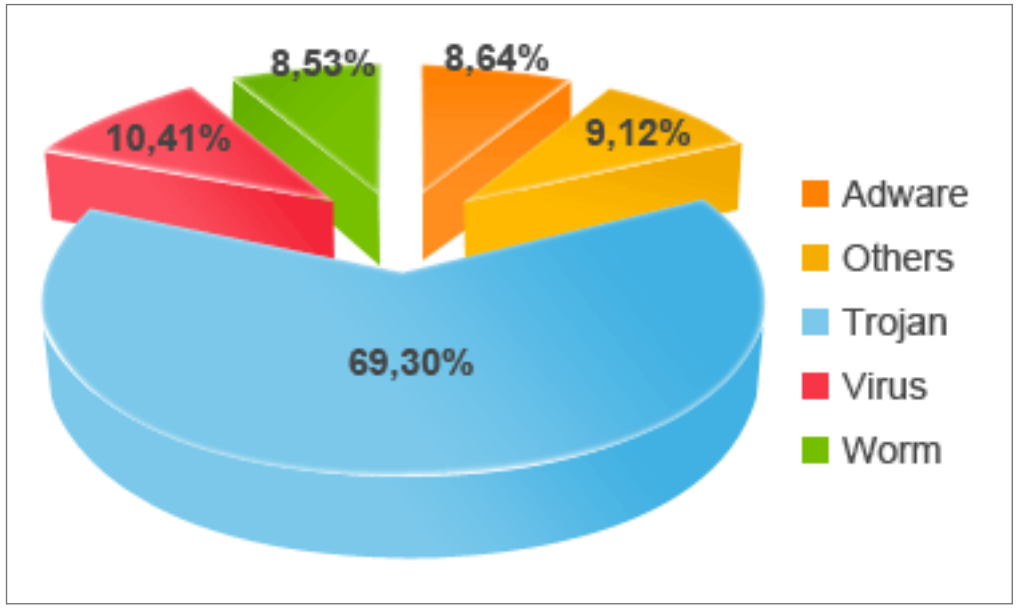


FIG.07. *DISTRIBUCIÓN DE INFECCIONES POR TIPO DE MALWARE.*

Como podemos observar, hay diferencias notables entre los ejemplares de malware creados en el trimestre y la distribución de infecciones. La lógica nos haría llegar a la conclusión de que los virus y gusanos deberían tener un mayor porcentaje, ya que poseen una característica que no posee el resto: son capaces de replicarse, por lo que su potencial de expansión es infinito comparado con el de un troyano o un falso antivirus. ¿Por qué no es así? Bien, el disparador de la infección es un ciberdelincuente, por lo que dependerá dónde ponen el foco. Así, vemos que con diferencia son los troyanos los que causan la mayor parte de las infecciones (tampoco es que sea una gran sorpresa). Los virus y los gusanos, en cambio, reducen su "cuota de mercado" en comparación a las muestras creadas y recogidas por PandaLabs en este periodo.

Pero si en una categoría podemos ver una clara diferencia, es en la de Adware, ya que aunque sólo un 2,58% de las nuevas muestras de malware pertenecen a esta categoría, son responsables de un 8,64% de las infecciones. Esto demuestra el interés y el trabajo que dedican los ciberdelincuentes en la "promoción" de estas herramientas. Desde un punto de vista de coste/beneficios es fácil de comprender, ya que sólo tienen que distribuir sus falsos antivirus y esperar a que los engañados usuarios les den su dinero de forma voluntaria.

Si vamos al detalle para ver qué malware está causando más infecciones, vemos que el Top 10 causa el 52,03% de las infecciones. Sin embargo, esta cifra puede resultar engañosa, ya que viendo el detalle de estos 10 primero vemos que se tratan de detecciones genéricas (detrás de las cuales está la Inteligencia Colectiva) que engloban numerosas familias de malware. Este es el detalle:

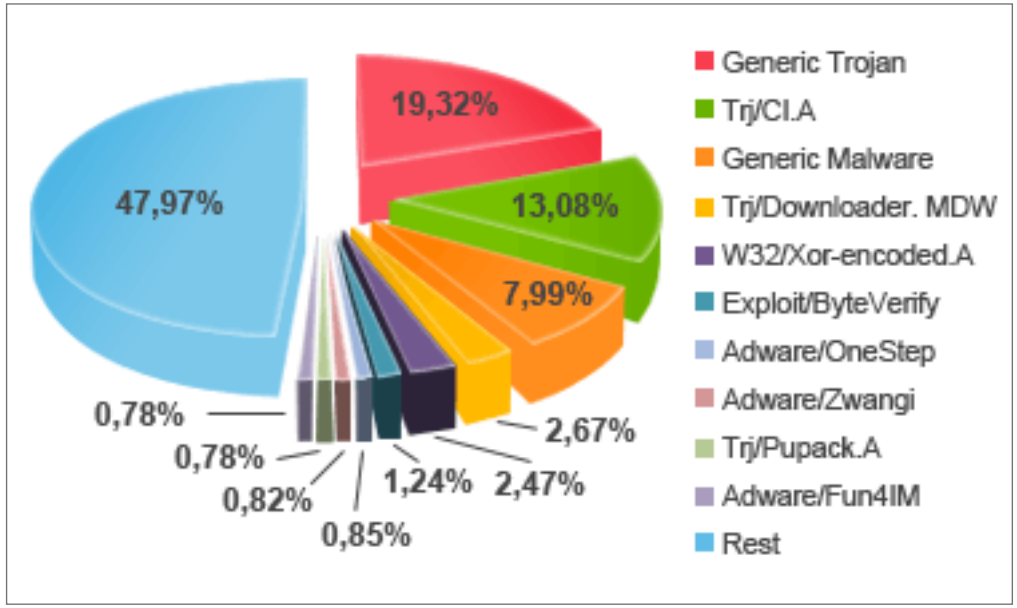


FIG.08. *FAMILIAS DE MALWARE.*

Ahora echemos un vistazo al porcentaje de equipos infectados en cada país. Usando de nuevo los datos de Panda ActiveScan, veremos el porcentaje de equipos infectados a nivel mundial y por país. Este tipo de datos suelen dar pie a polémicas, ya que hay quien apunta que ActiveScan (un antivirus online de análisis bajo demanda) es utilizado por usuarios que sospechan que están infectados y buscan una segunda opinión.

Este punto de vista es válido y cierto, sin embargo no es lo único que debemos tener en cuenta. Por ejemplo, la gran mayoría de usuarios que utiliza ActiveScan tiene un antivirus instalado y actualizado en su ordenador, lo que hace que la cifra de infecciones sea menor que si aumentáramos el uso de PCs desprotegidos para equipararlo a la situación real.

En la siguiente gráfica mostramos los 20 países con mayor ratio de infección del mundo en el segundo trimestre de 2011:

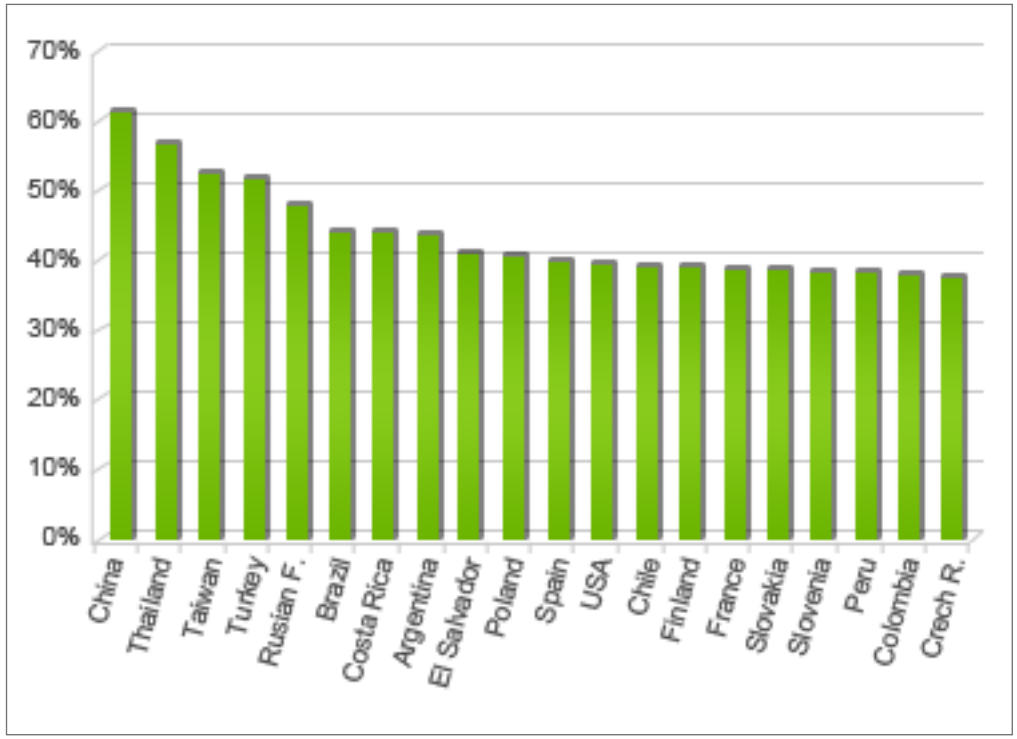


FIG.09. *PORCENTAJE DE INFECCIÓN POR PAÍSES.*

Vemos que los 3 primeros puestos pertenecen a países asiáticos. En primer lugar nos encontramos con China, país que tiene ni más ni menos que un 61,33% de sus PCs infectados con malware. En segunda posición está Tailandia, con un 56,67% de ratio de infección. Taiwán y Turquía también superan el 50% de infecciones, con un 52,92% y un 51,75% respectivamente.

La media mundial de infecciones se sitúa en el 39,79%. Suecia es el país del mundo con menos PCs infectados, un 27,29%, seguido por Suiza (29,02%), Noruega (29,13%) y Alemania (30,96%), todos ellos países europeos. En el siguiente gráfico tenemos los 10 países con menor índice de infección:

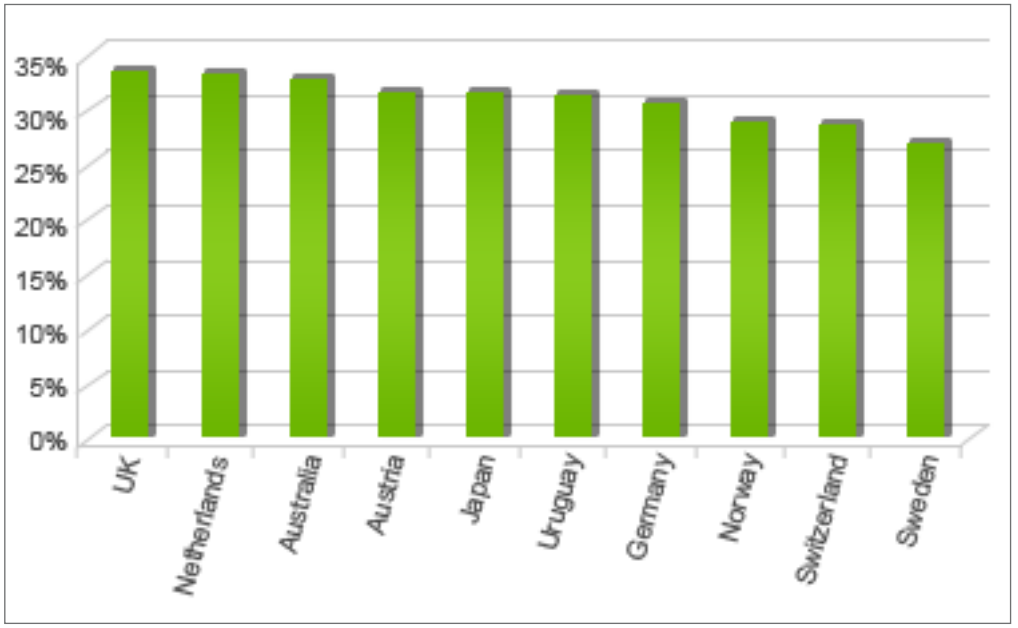


FIG.10. *LOS DIEZ PAÍSES CON MENOR RATIO DE INFECCIÓN DEL MUNDO.*

04| Vulnerabilidades

En esta sección vamos a seguir con la temática del trimestre pasado, que es mostrar información interesante, así como datos curiosos dentro de la temática de las vulnerabilidades.

No obstante, los que quieran información detallada sobre las vulnerabilidades y parches que han aparecido este segundo trimestre en los productos más relevantes del mercado como Microsoft, Adobe y Oracle pueden encontrarla en los siguientes enlaces.

- http://www.microsoft.com/technet/security/current.aspx
- http://www.adobe.com/support/security/
- http://www.oracle.com/technetwork/topics/security/alerts-086861.html#SecurityAlerts

Si también queréis información de las vulnerabilidades que afectan a éstos y otros productos podemos visualizarlas en el siguiente enlace:

- http://cve.mitre.org/cve/

Empezamos el artículo recordando como en el trimestre pasado hablábamos del concurso Pwn2Own organizado por el equipo ZeroDay Inciative[1] de la compañía TippingPoint. Donde ya mencionamos que Investigadores de la empresa VUPEN se aprovecharon de una vulnerabilidad en la última versión del motor WebKit[2] de Safari para saltarse las protecciones de ASLR[3] y DEP[4] en la versión de 64bit de un MacOSX Snow Leopard totalmente parcheado y así ganar el premio. Lo mismo hizo Stephen Fewer investigador

de la empresa Harmony Security con un Internet Explorer 8 ejecutándose bajo Windows 7 Service Pack 1. Para conseguir la hazaña necesito nada más y nada menos que 3 vulnerabilidades desconocidas.

Sólo el navegador Google Chrome ha salido victorioso de los ataques de los mejores hackers. Es posible que el éxito de este navegador frente a los hackers sea debido a las actualizaciones previas realizadas por Google días antes del comienzo del concurso para arreglar ciertos fallos de seguridad detectados y esto ha hecho que los investigadores no participasen en el intento al ver que sus exploits ya no funcionaban.

Puestos ya en contexto, podríamos decir que según los resultados del concurso, Google Chrome sería la mejor opción para realizar una navegación más segura por Internet. No obstante, los hechos muestran que este navegador puede ser comprometido al igual que los 2 anteriores. Porque 2 meses después de que finalizase el concurso Pown2Own, el 4 de mayo, la empresa VUPEN anunciaba mediante un mensaje en su cuenta de Twitter (@VUPEN) que estaban trabajando duramente en una posible vulnerabilidad que afectaba al imbatido navegador Google:

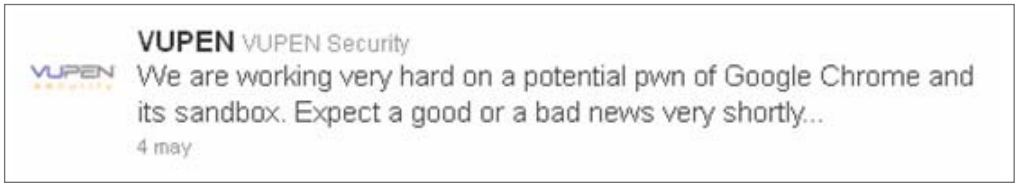


FIG.11. *MENSAJE DE VUPEN VÍA TWITTER DONDE COMENTA QUE ESTÁ TRABAJANDO EN UNA VULNERABILIDAD QUE AFECTA A GOOGLE CHROME.*

Dicho y hecho, 5 días después VUPEN vuelve a publicar un mensaje en Twitter indicando que dispone de un exploit que se salta la seguridad de Google Chrome (versión 11). El mensaje hace referencia a un post que han creado en su página web donde dan algo más de información e incluyen un video[5] para demostrar la gran hazaña conseguida.

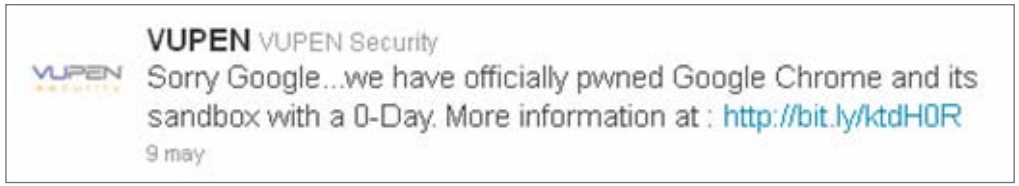


FIG.12. *MENSAJE DE VUPEN VÍA TWITTER DONDE ANUNCIA QUE HA PODIDO COMPROMETER EL NAVEGADOR GOOGLE CHROME.*

Parecía que la versión 12 de Google Chrome no era vulnerable a dicho ataque, pero 2 días más tarde, el 11 de Mayo, VUPEN lo volvía a conseguir y confirmaba nuevamente en Twitter que la versión 12 del navegador también había sido comprometida.

FIG.13. *MENSAJE DE VUPEN VÍA TWITTER DONDE ANUNCIA QUE TAMBIÉN HA PODIDO COMPROMETER AMBAS VERSIONES.*

En su blog VUPEN comenta que el exploit que consigue explotar la vulnerabilidad en Google Chrome es unos de los más sofisticados que han visto y creado. Este es capaz de saltarse las últimas mitigaciones de seguridad, ASLR y DEP, implementadas ambas en las versiones actuales del sistema operativo Windows 32 y 64 bits además de evitar la sandbox desarrollada por Google en su navegador y explotarse de forma silenciosa, es decir, no hay ningún comportamiento anómalo que alerte al usuario durante el proceso de la explotación de la vulnerabilidad que algo malicioso esta ocurriendo en la máquina comprometida. Debido a su gravedad, la información técnica de dicha información sólo estará disponible para las agencias gubernamentales que están dentro del programa de clientes de la propia empresa.

Parece ser que los investigadores de seguridad de esta empresa se han tomado como reto descubrir fallos de seguridad en los sistemas que han sobrevivido a concursos como Pwn2Own. Mencionamos esto porque VUPEN también ha dicho que está trabajando en otro 0day que afecta a otro de los productos que también salió inmune del concurso. En este caso es el sistema operativo para móviles de Google, Android, donde mencionaban que un usuario malicioso podría hacerse con el control de un Nexus S si el usuario afectado visitaba una página web maliciosa. Posiblemente el nuevo 0day habrá sido descubierto en el motor de renderizado WebKit[6] utilizado en el navegador web de Android y principal foco y objetivo de vulnerabilidades en Safari y Google Chrome.

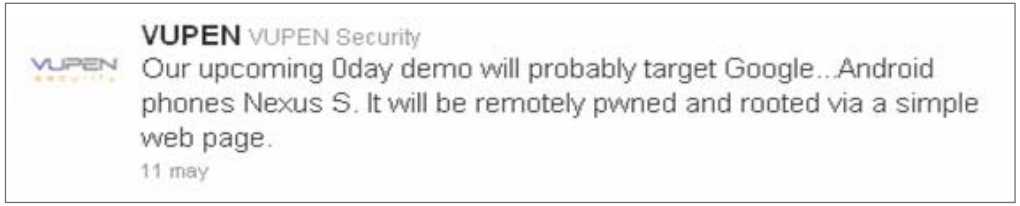


FIG.14. *VUPEN SE PONE EL RETO DE EXPLOTAR EL SISTEMA ANDROID.*

Aún no hay información de si VUPEN ha conseguido este último reto, ¿se atreverán los chicos de VUPEN también con ChromeOS el sistema operativo de Google para netbooks? Tendremos que estar atentos a sus movimientos, actualmente VUPEN está reconocida como una de las empresas líder a nivel mundial en el campo de la investigación y asesoramiento de vulnerabilidades.

Esto nos hace ver nuevamente que un sistema operativo totalmente actualizado a día de hoy no es suficiente. Por lo tanto tenemos que hacer uso de otras tecnologías y herramientas que complementen dicha seguridad para evitar una posible intrusión, infección o robo de información privada de nuestros equipos de casa y empresas.

1 http://zdi.tippingpoint.com/
2 http://www.webkit.org/
3 http://cansecwest.com/
4 http://en.wikipedia.org/wiki/Data_Execution_Prevention
5 http://www.vupen.com/demos/VUPEN_Pwning_Chrome.php
6 http://www.webkit.org/

05| Conclusión

Todos estos ataques de los que estamos siendo testigos nos pueden dar una sensación de inseguridad, pero de todo podemos aprender, y esto es lo positivo de la situación. Grandes empresas como Sony han descubierto que no tomarse en serio su seguridad ha afectado de forma directa a su negocio e incluso al precio de sus acciones en bolsa.

Algo así obliga a todas las empresas a dar a la seguridad la importancia que se merece, y lo más importante, los usuarios debemos exigir estas medidas ya que es nuestra información la que está en juego, y si no responden a nuestras expectativas tendremos que buscar competidores que nos den garantías.

06| Sobre PandaLabs

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 por en el blog de **PandaLabs** en: **http://pandalabs.pandasecurity.com/**

PANDA SECURITY