INFORME TRIMESTRAL PANDALABS

JULIO-SEPTIEMBRE 2013

PANDA SECURITY

01| Introducción

02| El trimestre en cifras

03| El trimestre de un vistazo

04| Conclusión

05| Sobre PandaLabs

06| Panda en la Red

01| Introducción

El tercer trimestre de 2013 ha sido uno de los más activos de la historia en cuanto a creación de malware. Prácticamente durante los nueve meses de este año hemos descubierto el mismo número de muestras de malware que a lo largo de todo el año 2012.

Dentro de las diferentes familias de malware, este trimestre destaca la aparición de **CryptoLocker**, un ransomware que secuestra los documentos de nuestro ordenador, y que obliga a pagar a los ciberdelincuentes para poder recuperarlos.

Además, relataremos cómo el grupo "Syrian Electronic Army" continúa en su espiral de ataques, llegando a hackear las cuentas de correo de trabajadores de la mismísima Casa Blanca.

En el terreno móvil veremos algunos ataques contra iPhone, como el que permite infectar los teléfonos de Apple simplemente a través del cargador de corriente. Por su parte, Android sigue protagonizando la mayoría de ataques en este terreno, a pesar de que algunos responsables de Google afirmen que se trata de la plataforma más segura del mercado.

En el ámbito de la ciberguerra y del ciberespionaje, hablaremos principalmente de la NSA y de algunas de las nuevas revelaciones sobre operaciones de ciberespionaje perpetradas por esta agencia norteamericana.

02| El trimestre en cifras

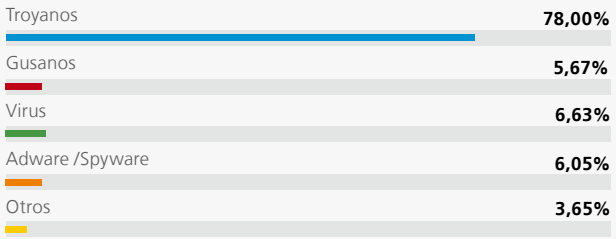
El tercer trimestre de 2013 ha batido un nuevo récord en lo que se refiere a la creación de malware. PandaLabs ha registrado casi 10 millones nuevos de ejemplares en estos tres meses, lo que implica que el número de ejemplares nuevos detectados durante los nueve primeros meses de este año sea casi el mismo que el registrado durante todo el año 2012.

Los troyanos vuelen a encabezar, una vez más, la tabla de tipología de malware creado, con un 76,85% de las nuevas muestras de malware generadas, un porcentaje muy similar al identificado durante el trimestre anterior.

Nuevo malware creado en el tercer trimestre de 2013, por tipo

Troyanos	**76,85%**
Gusanos	**13,12%**
Virus	**9,23%**
Adware /Spyware	**0,57%**
Otros	**0,23%**

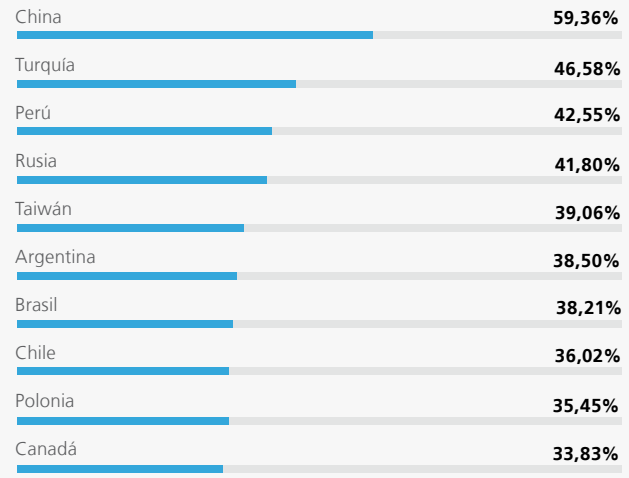
Infecciones por tipo de malware en el tercer trimestre de 2013



Las infecciones de troyanos se mantienen en la cima del ranking, siendo el tipo de malware más utilizado por los ciberdelincuentes para infectar a los usuarios. Cabe destacar un cierto aumento de las infecciones de adware y spyware, aunque con un 6,05% quedan muy lejos del 78% de los troyanos.

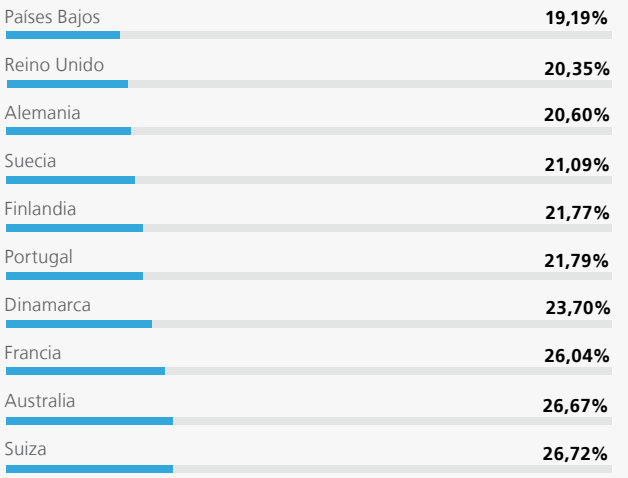
Pasemos a realizar un análisis geográfico de las infecciones: **en este tercer trimestre de 2013 el ratio de infecciones a nivel mundial ha sido del 31,88%**, casi un punto menos si lo comparamos con el segundo trimestre de este año. En cuanto a los datos de los diferentes países, China repite en la primera posición, alcanzando un índice de infección del 59,36%. Le siguen Turquía (46,58%) y Perú (42,55%).

Países con mayor índice de infección



Aunque predominan claramente países de Latinoamérica en este "Top 10", vemos cómo hay países de las principales zonas del mundo. **China bate un récord con un índice de infección muy disparado que supera ampliamente el 50%**.

Países con menor índice de infección



Europa es la zona del mundo donde el índice de infección es más bajo. Países Bajos (19,19%%), Reino Unido (20,35%) y Alemania (20,60%) son los países con un menor índice de Infección a nivel mundial. **El único país no europeo entre los 10 mejores es Australia**, que se sitúa en novena posición con un 26,67%. Otros países que no han conseguido posicionarse en este Top 10, pero que sí han logrado situarse por debajo de la media mundial de infecciones, son: Japón (26,84%), Hungría (27,56%), Venezuela (27,82%), Colombia (29,14%), Bélgica (29,14%), Italia (30,16%), EEUU (30,58%), México (31,49%) y España (31,74%).

03| El trimestre de un vistazo

En muchas ocasiones los ciberdelincuentes se aprovechan de diferentes eventos, fechas señaladas, o noticias de gran impacto para tratar de propagar malware y conseguir nuevas víctimas.

CIBERCRIMEN

Durante este trimestre el grupo **Syrian Electronic Army** ha continuado protagonizando diferentes ataques. En julio, a través de un ataque de phishing, consiguió comprometer las cuentas de Gmail de tres trabajadores encargados de labores de social media en la **Casa Blanca**. Una vez comprometidas estas cuentas, las utilizaron para enviar e-mails fraudulentos a otros objetivos de la Casa Blanca.

En agosto el mismo **Washington Post** publicó una nota confirmando que habían sido víctimas de hacking, y que algunos de sus lectores habían sido redirigidos a páginas de la propia Syrian Electronic Army.

> El Grupo **Syrian Electronic Army** se ha mostrado especialmente activo este trimestre. Entre sus víctimas se cuentan el New York Times, Twitter e incluso trabajadores de la Casa Blanca

Semanas más tarde el **New York Times** y la red social **Twitter** fueron también víctimas de este grupo. En este caso ninguna de las dos empresas fueron hackeadas, sino que se utilizó una técnica denominada DNS poisoning, mediante la cual los usuarios eran redirigidos a otra página cuando tecleaban la dirección web de cualquiera de los dos sitios web. Si se accedía

Semanas más tarde el **New York Times** y la red social **Twitter** fueron también víctimas de este grupo. En este caso ninguna de las dos empresas fueron hackeadas, sino que se utilizó una técnica denominada DNS poisoning, mediante la cual los usuarios eran redirigidos a otra página cuando tecleaban la dirección web de cualquiera de los dos sitios web. Si se accedía a las páginas web utilizando la dirección IP, podía accederse a ambas sin problemas.

Durante los últimos meses hemos constatado un aumento de ataques utilizando la técnica **DNS poisoning**

El "**Virus de la Policía**" ha seguido causando estragos a través de numerosas variantes que han tratado de infectar a los usuarios. Nos ha llamado especialmente la atención una de ellas, debido al alto coste de la "multa", ya que aunque el precio habitual suele rondar los 100 $/€, en este caso la suma solicitada ascendía a 300.

En España, la Brigada de Delitos Informáticos de la Policía Nacional ha detenido en Madrid a dos ciudadanos ucranianos relacionados con el blanqueo de dinero de una de las bandas que está detrás de estos ataques protagonizados por el Virus de la Policía. Entre los diferentes bienes incautados a estos ciberdelincuentes, se encontraban bitcoins, siendo esta la segunda vez en la historia que un cuerpo policial se incauta de la famosa moneda virtual.

Si una amenaza se ha ganado un nombre propio durante este trimestre esta es sin duda **CryptoLocker**. Se trata de un troyano que utiliza tácticas de ransomware, cifrando todos los ficheros de datos importantes del usuario y pidiendo un rescate para poder volver a recuperarlos.

CryptoLocker es una nueva familia de malware que secuestra documentos y pide un rescate por ellos

Si bien este tipo de ataques no es nuevo, existen ciertas características que han conseguido que tenga más éxito a la hora de cobrar el rescate solicitado a las víctimas:

- En vez de cifrar todo tipo de ficheros, se centra solamente en aquellos que los usuarios más pueden valorar: fotos, vídeos, documentos de texto, etc.
- No sólo cifra ficheros en el disco, sino que también puede hacerlo en unidades que estén en la misma red local.
- El cifrado es asimétrico, por lo que se necesita obligatoriamente la clave que los ciberdelincuentes tienen para recuperar los datos, siendo inviable la utilización de herramientas específicas para poder recuperar los ficheros.
- En el mensaje que se muestra para pagar el rescate aparece una cuenta atrás, lo que fuerza a la víctima a tener que tomar una decisión: pagar o perder todos sus datos.

En la lucha contra la ciberdelincuencia, el Parlamento Europeo ha aprobado que se apliquen penas más severas a delitos relacionados con los ciberataques. Por ejemplo, el simple hecho de crear o utilizar una botnet (red de bots) podrá acarrear penas de al menos tres años, sin contar otros crímenes que hayan podido cometerse mediante el uso de dichas botnets.

REDES SOCIALES

En el terreno de las redes sociales, Facebook ha completado este trimestre la migración de todos sus usuarios a navegación segura, y ahora todos los usuarios de la más grande red social del mundo se conectan a la misma mediante HTTPS, de tal forma que todas las comunicaciones entre los dispositivos de los internautas y Facebook van cifradas, pudiendo así evitar el robo de los datos mediante la captura de la información que viaja por la Red.

Todos los usuarios de Facebook se conectan ya mediante **HTTPS**

MÓVILES

A pesar de que **Android** es la plataforma más popular, y por tanto suele protagonizar esta sección, este trimestre vamos a comenzar hablando de su principal competidor: iOS, el sistema operativo de Apple para teléfonos (iPhone) y tabletas (iPad). En julio, un grupo universitario de investigadores de la Georgia Tech Information Security Center (GTISC) mostraron un ataque mediante el que podían infectar un iPhone simplemente enchufándolo a un cargador.

Se ha demostrado cómo se puede infectar un **iPhone** simplemente conectándolo a un cargador

En septiembre, **Apple** lanzó la nueva versión de iOS, la 7, que además de cambios estéticos y de funcionalidad, corregía 80 vulnerabilidades diferentes, entre las que se encontraba la aquí descrita. Sin embargo, en unas pocas horas aparecieron nuevos problemas de seguridad en iOS 7: uno de ellos, por ejemplo, permitía saltarse el código de desbloqueo.

En el terreno de Android siguen aumentando los ataques. Sin embargo, uno de los titulares más llamativos de este trimestre nos lo dio Google, donde Adrian Ludwig, responsable de seguridad de Android, mostró datos que aseguran que menos del 0,001% de las instalaciones de aplicaciones de Android son capaces de saltarse las defensas multi-capa que tiene el sistema. Las estadísticas pueden mostrar diferentes realidades,

pero lo que es innegable es que Android es la plataforma móvil más atacada.

Android continúa siendo la plataforma móvil más atacada

Android está en el punto de mira de los ciberdelincuentes que están buscando continuamente nuevas formas de atacar a la plataforma e infectar a los usuarios. Como resultado hemos visto durante este trimestre un nuevo tipo de ataque en el que modificando un fichero APK legítimo (instalador de aplicaciones de Android) se consigue que éste instale cualquier tipo de código malicioso sin que el sistema se dé cuenta de lo que está sucediendo.

CIBERGUERRA

Dentro del ámbito del ciberespionaje, este trimestre continúa teniendo el mismo protagonista que el anterior: la Agencia Nacional de Seguridad norteamericana, más conocida por sus siglas en inglés NSA (National Security Agency). A principios de 2013, Edward Snowden, que había trabajado para la NSA como administrador de sistemas, finiquitó su relación con la agencia llevándose consigo un número importante de documentos que reveló a diferentes medios de comunicación. Gracias a ello se desveló un programa de la **NSA** denominado PRISM, mediante el que la agencia podía obtener datos de usuarios de grandes empresas norteamericanas: Microsoft, Google, Apple, Facebook, etc.

Nuevas revelaciones conocidas a través de documentos filtrados por Edward Snowden han situado a la **NSA** como protagonista de las mayores acciones de ciberespionaje

Si bien las primeras informaciones resultaban escandalosas, aparecieron diferentes datos que podían limitar el alcance de los documentos filtrados, como que sólo podían acceder a datos de objetivos mediante la obtención previa de una orden judicial. Sin embargo, no todo era tan inocente como parecía en un primer momento.

Ante el escándalo del espionaje realizado por la NSA, grandes empresas han demandado al gobierno norteamericano una mayor transparencia en los programas de vigilancia. En concreto, están pidiendo que les dejen hacer público la cantidad de peticiones de información que reciben del gobierno, y diferente información relacionada con estas peticiones.

La **NSA** incluyó un backdoor en un conocido algoritmo de generación de números pseudoaleatorios, cuyo uso era recomendado por importantes organismos oficiales

Dentro de las nuevas revelaciones que han sido dadas a conocer durante estos tres meses, se ha sabido que la NSA había incluido un backdoor en el Dual EC_DRBG, un algoritmo de generación de números pseudoaleatorios que había sido certificado por los más importantes organismos internacionales. De hecho, días más tarde la compañía de seguridad RSA envió un comunicado a sus clientes para que no utilizaran dicho algoritmo, que estaba implementado por defecto en dos de sus productos.

04| Conclusión

Cerramos este tercer trimestre de 2013 con la creación de malware batiendo cifras récord, alcanzando ya la cifra de nuevo malware generado durante todo el año 2012.

Hemos visto cómo se popularizan cada vez más los ataques utilizando técnicas de DNS posioning, algo que seguramente sigamos presenciando durante los próximos meses.

En el ámbito del ciberespionaje, Estados Unidos ha robado todo el protagonismo a China debido al escándalo destapado por Edward Snowden, y todo parece indicar que seguiremos conociendo detalles de diferentes programas llevados a cabo por la NSA para poder espiar de forma indiscriminada y con todo tipo de técnicas ilegales a usuarios, empresas y gobiernos de todo el mundo.

05| 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 de 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/

06| Panda en la Red

facebook
https://www.facebook.com/PandaSecurity

twitter
https://twitter.com/PandaComunica

google+
https://plus.google.com/b/114692356211770437886/114692356211770437886/posts

youtube
http://www.youtube.com/pandasecurity1

linkedin
http://www.linkedin.com/company/panda-security