Informe trimestral PandaLabs

Julio - Septiembre **2011**

01| Introducción

El verano ya ha pasado y ha llegado el momento de hacer un repaso por todo lo acontecido durando estos tres meses. Veremos cómo la época estival no ha significado un descenso en la creación de malware, con más de 5 millones de nuevos ejemplares creados en este periodo.

Un dato a destacar es que se ha batido el récord de troyanos, llegando al punto en que 3 de cada 4 nuevas muestras de malware creadas durante este trimestre pertenecen a esta categoría, la preferida por los ciberdelincuentes para llevar a cabo sus robos de información.

Haremos un repaso a las noticias del mundo de la seguridad más destacables, desde las últimas andanzas del grupo Anonymous hasta los últimos actos de ciberguerra, sin olvidarnos pasar por los dispositivos móviles, redes sociales, etc.

02| El trimeste de un vistazo

Este trimestre veraniego ha estado plagado de ataques de todo tipo. Uno de los temas populares de este año, Anonymous, ha seguido siendo protagonista de muchas de las noticias de seguridad. Sin embargo, no han sido los únicos en dar que hablar, ya que los ciberdelincuentes siguen haciendo de las suyas con robos a gran escala, además de otros casos que están dentro de lo que podríamos considerar ciberguerra.

Anonymous

El trimestre no pudo empezar peor para este grupo, ya que a principios de mes supimos que en Italia se consiguió arrestar a 15 personas pertenecientes a la "célula" italiana de Anonymous. Es de destacar que sus edades comprendían entre los 15 y los 28 años, siendo 5 de ellos menores de edad. La policía llevó a cabo 30 registros incautándose de diferente material (servidores, etc.) El cabecilla de este grupo se trata de un joven de 26 años residente en Suiza.

Poco después de producirse estos arrestos, supimos que Anonymous había entrado en un sitio web de Universal Music, robando información de usuarios de dicha compañía. Entre la información había nombres de usuario y contraseñas, por lo que Universal urgió a sus usuarios a cambiar sus datos de acceso. Por un lado, esto demuestra que aún hay muchas compañías que no se toman mínimamente en serio la seguridad, ya que almacenar las contraseñas en texto plano es una imprudencia imperdonable. Pero esto no nos debe hacer olvidar que Anonymous actúa como un grupo de vándalos que sólo busca hacer daño; es más, principalmente acaba haciendo daño a los usuarios a los que dice defender, ya que estos datos robados son publicados quedando todos a merced de cualquier persona que quiera utilizar su información.

Volviendo a Italia, en Julio fueron robados y publicados datos de bases de datos de 18 universidades de dicho país.

FIG.01. *TWEET DONDE SE ANUNCIA LA PUBLICACIÓN DE INFORMACIÓN ROBADA.*

En Estados Unidos Anonymous fue un paso más allá entrando en la empresa Booz Allen Hamilton (contratista del Departamento de Defensa –DoD) y robando 90,000 direcciones de correo militares y sus respectivas contraseñas. Consiguieron entrar a través de un servidor que se encontraba completamente desactualizado y desprotegido, ni siquiera contaba con protección antivirus.

Todos estos ataques no quedan sin respuesta, y el FBI detuvo en Estados Unidos a 16 personas relacionadas con Anonymous, enfrentándose a penas de entre 5 y 10 años de cárcel si son declarados culpables.

En cualquier caso ninguna de estas acciones ha conseguido parar a Anonymous, y según pasa el tiempo hemos visto cómo ha ido a más. Días después de estos arrestos Anonymous publicó un documento confidencial de la OTAN. Confirmó que tenía 1 Gb de datos más que no iba a publicar porque sería "irresponsable".

Mientras, en Italia Anonymous volvió a golpear robando más de 8 Gb de datos del CNAIPIC (centro nacional contra el crimen informático para la protección de infraestructuras críticas).

FIG.02. *MENSAJE DE ANONYMOUS VANAGLORIÁNDOSE DE SU ÚLTIMO ROBO DE DATOS.*

Tras esta infinidad de delitos cometidos por Anonymous, un rayo de sensatez iluminó brevemente sus mentes y decidieron hacer activismo real. Denominaron a esta operación #OpPayPal y solicitaron a usuarios de todo el mundo que cerraran sus cuentas de PayPal en forma de protesta contra la compañía. Tuvo algo de eco mediático pero poco efecto real.

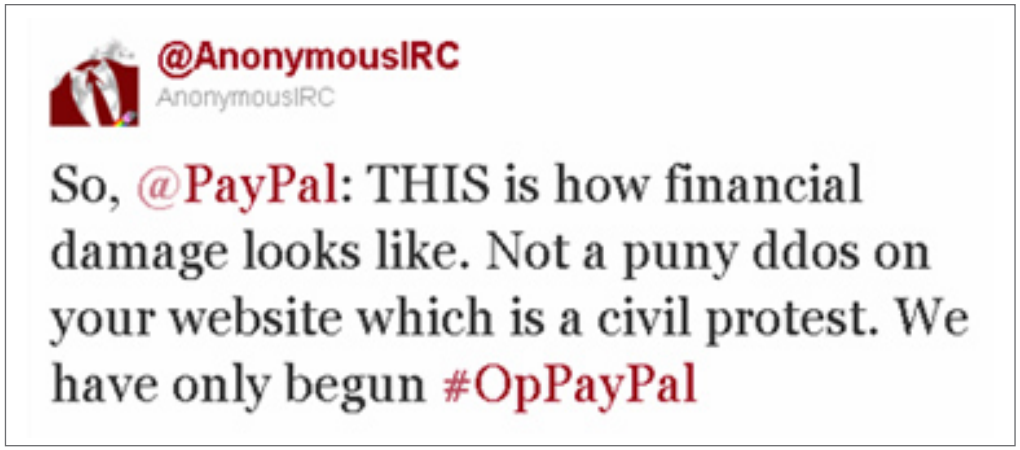


FIG.03. *MENSAJE DE ANONYMOUS ANUNCIANDO SU NUEVA OPERACIÓN.*

Como su operación contra PayPal no obtuvo los resultados deseados, a principios de agosto volvieron a las andadas haciendo lo que mejor saben hacer: robar. Publicaron miles de datos de policías norteamericanos, incluyendo sus direcciones de correo, nombres de usuario, contraseñas y en algunos casos hasta su número de la seguridad social. Semanas más tarde repitieron la operación, en este caso dirigida a policías del metro de San Francisco. Por si no fuera suficiente, volvieron a atacar a una empresa contratista del DoD (Vanguard Defense Industries) robando 1 Gb de datos con correos electrónicos y documentos privados pertenecientes a uno de los ejecutivos de la compañía.

A lo largo de septiembre se han producido nuevos arrestos, tanto en Estados Unidos como en el Reino Unido, aunque Anonymous no parece que vaya a dejar de cometer delitos.

Cibercrimen

El mundo de la seguridad sigue en su habitual espiral creciente, donde las buenas noticias son que cada vez se consigue arrestar a más ciberdelincuentes. En julio, Rogelio Hackett, de 25 años, fue condenado a 10 años de cárcel y pagar una multa de 100.000$ por haber robado datos de 675.000 tarjetas de crédito. El hablar de condenas en firme es un paso muy importante, ya que es una de las mejores medidas disuasorias que demuestran que la impunidad no es una opción.

Aún así no todo son buenas noticias, y se siguen cometiendo delitos en todo el mundo. Los ciberdelincuentes utilizan técnicas de ingeniería social para tratar de infectar y robar información a los usuarios, y como siempre en cuanto se produce alguna noticia relevante tratan de aprovecharse de la misma, como ha sido el caso del fallecimiento de la cantante Amy Whinehouse o la masacre de Oslo.

Una de las claves en la lucha contra la ciberdelincuencia es la colaboración entre los diferentes países, ya que la mayoría de los delitos se dan en diferentes países al no existir fronteras en Internet. A este respecto, una buena noticia la tuvimos este trimestre cuando el US-CERT y el CERT-In (de Estados Unidos e India respectivamente) firmaron un acuerdo de colaboración que abre un rayo de esperanza. Si acuerdo de este tipo se generalizan podría suponer un importante paso adelante en la lucha contra la delincuencia en Internet.

Ciberguerra

En julio, el adjunto al secretario de defensa estadounidense, Bill Lynn, hizo público un ataque recibido en marzo, durante el que habían robado 24.000 documentos pertenecientes a un sistema armamentístico secreto. El DOD dijo que lo más posible es que se tratara de un ataque perpetrado por el servicio de inteligencia de una potencia extranjera.

FIG.04. ***EL DEPARTAMENTO DE DEFENSA DE ESTADOS UNIDOS SUFRIÓ UN ROBO DE 24.000 DOCUMENTOS.***

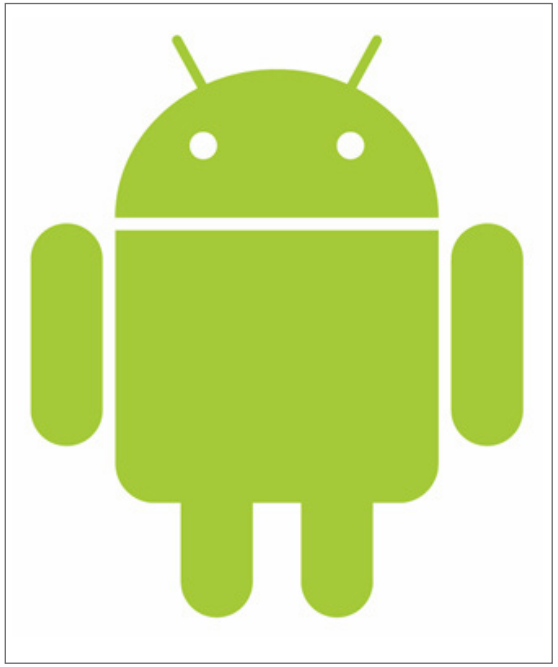
Unos días más tarde, el general de los Marines James 'Hoss' Cartwright hizo unas declaraciones en las que decía que el departamento de IT del DOD estaba en la edad de piedra.

Cuando ya casi nos habíamos olvidado de Stuxnet, la web DEBKAfile publicó un informe citando "fuentes de inteligencia" en el que se afirmaba que Irán había tenido que sustituir miles de centrifugadoras de uranio debido al ataque sufrido el año pasado, y que desde entonces no han conseguido volver a enriquecer uranio al ritmo normal. El gobierno iraní, de hecho, confirmó a través de su ministro de asuntos exteriores que está instalando "nuevas y más rápidas" centrifugadoras para acelerar el proceso de enriquecimiento de uranio.

En julio, el Departamento de Interior norteamericano, refiriéndose al caso Stuxnet, dijo al Congreso que temen que el mismo tipo de ataque pueda ser utilizado contra infraestructuras críticas de su país. El hecho de que cada vez haya disponible más información hace temer que se creen variantes que puedan atacar a otro tipo de sistemas del país.

Si algo se puede decir de los ataques de ciberguerra o ciberespionaje, es que en la mayoría de los casos se mira hacia China como la gran sospechosa que está detrás de todos ellos. Sin embargo es obvio que por una parte China no es la responsable de todos los ataques, y por otra en China tienen que estar recibiendo ataques.

Cuando por ejemplo la Unión Europea recibe un ataque cibernético, o tantos otros casos que han sucedido este mismo año, llegan al conocimiento de los ciudadanos porque se hacen públicos. Sin embargo, en otros países no se conocen casos. ¿Es esto debido a que no sufren ataques? En absoluto, normalmente se debe al oscurantismo informativo. Y China, por una vez, se ha abierto y en agosto confesó que el año pasado recibió 500.000 ataques, la mayoría de ellos con procedencia de países extranjeros.



Mac, móviles…

Las "nuevas" plataformas en las que el malware se está fijando cada vez más son los ordenadores Mac y los móviles basados en el sistema operativo Android, tal y como os hemos contado en anteriores informes. Este trimestre no ha sido una excepción, y hemos visto como la escena de las amenazas para Mac va avanzando, con ataques cada vez más sofisticados que conjugan el uso de vulnerabilidades con la instalación de backdoors que permiten el acceso al sistema comprometido.

FIG.05. ***ANDROID SE HA CONVERTIDO EN EL SISTEMA OPERATIVO MÓVIL PREFERIDO POR LOS CIBERDELINCUENTES.***

En el terreno de Android, hemos visto durante este trimestre una nueva variante de Zitmo, la versión del troyano bancario Zeus que tiene un componente para móviles. En esta ocasión, cuando el teléfono móvil de la víctima se infecta con Zitmo el troyano reenvía los mensajes remitidos por la entidad bancaria con un password de un solo uso a los ciberdelincuentes, de tal forma que así pueden realizar cualquier transacción on-line desde la cuenta de la víctima.

La aparición de nuevas familias de malware para Android es algo cada vez más frecuente, cada una con diferentes objetivos, aunque todas comparten un objetivo en común: el robo de información. Así, hemos visto diferentes variantes que no sólo copian datos del terminal y los envían a los ciberdelincuentes, sino que son capaces de grabar las conversaciones que tengamos en el móvil.

Redes Sociales

El mayor evento que ha sucedido en este campo es el lanzamiento en junio de Google+, un directo competidor de Facebook. Mucho más sencillo y con menos opciones, ha conseguido millones de usuarios en apenas 3 meses.

Aún así, los ciberdelincuentes no han comenzado a bombardear a los nuevos usuarios de Google+ con campañas de engaños y distribución de malware como hacen regularmente en Facebook. Sin embargo, al poco tiempo de lanzarse, como las invitaciones no estaban abiertas a todo el público y había mucha expectación y ganas por parte del público de conseguir una, vimos un caso muy curioso que tuvo lugar… en Facebook. Crearon una página llamada "Get Google Plus Invitation FREE" (Consigue gratis invitación a Google Plus) donde sólo tenías que dar a "Me gusta" para conseguir dicha invitación. Por supuesto, también había que facilitar la dirección de correo para que te pudieran enviar dicha invitación, aunque realmente se trataba de un engaño y dicha invitación no existía.

Este tipo de engaños, de hecho, está muy extendido en Facebook, la plataforma favorita de los delincuentes para lanzar sus ataques mediante técnicas de ingeniería social, siempre usando noticias reales o bulos en los que muchísimos usuarios siguen cayendo.

Y por supuesto, no podemos cerrar este apartado de redes sociales sin nombrar a Twitter, que aunque en menor medida que Facebook, sigue siendo una plataforma muy utilizada para enviar tanto spam como links maliciosos. Otra técnica que está siendo muy utilizada por los ciberdelincuentes es el hackeo de cuentas. Así, vimos como la cuenta de Twitter de Fox News fue hackeada y comenzó a publicar el 4 de julio, una falsa noticia anunciando la muerte de Obama. También hemos visto como la cuenta de PayPal UK fue hackeada comenzando a enviar mensajes en tono jocoso riéndose de la seguridad que tienen.

Pero no todos los ataques son realizados en plan bromista, ya que vimos hackeo a la cuenta de Twitter de una entidad financiera, donde los ciberdelincuentes comenzaron a enviar DMs (mensajes directos) a los seguidores de su cuenta, indicándoles que debían pinchar en un link debido a un problema de seguridad en su cuenta. Este link dirigía al usuario a una página de phishing que imitaba la del banco, donde le solicitaba todos los datos necesarios para poder posteriormente hacerse pasar por dicho cliente y robarle el dinero.

03| El trimeste en cifras

Vamos a proceder al análisis de las cifras de malware de este trimestre. En este periodo vacacional en muchos países del mundo, los creadores de malware no se han tomado ningún descanso, creando más de 5 millones de nuevas muestras. Si analizamos en detalle los datos veremos que como viene siendo habitual desde la popularización del cibercrimen, los troyanos son el tipo de malware más prevalente. En cualquier caso cabe destacar que este trimestre se ha alcanzado una cifra récord, donde de cada 4 nuevos ejemplares de malware creados 3 son troyanos, un 76,76%.

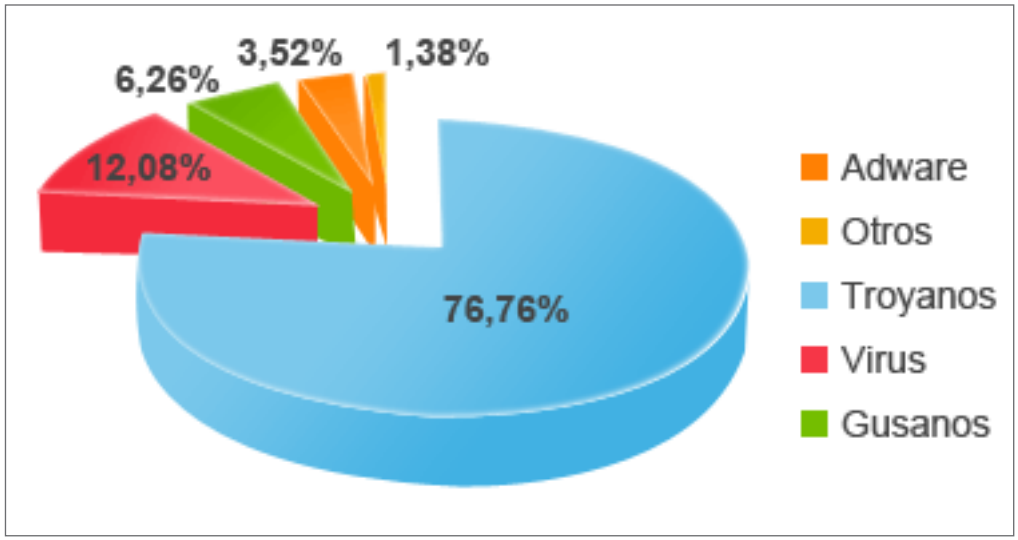


FIG.06. *NUEVAS MUESTRAS DE MALWARE DETECTADAS EN PANDALABS.*

La segunda posición la ocupan los virus, con un 12,08%, seguidos de los gusanos (6,26%) y el adware (3,53%) categoría que engloba a los falsos antivirus y que también repunta respecto al trimestre anterior.

Los números de los que estamos hablando recogen la cantidad de muestras creadas y su tipología, lo que no siempre se traduce en infecciones reales. Para analizar lo que realmente sucede en el mundo, vamos a ver los datos obtenidos por nuestra red de sensores que forman la Inteligencia Colectiva.

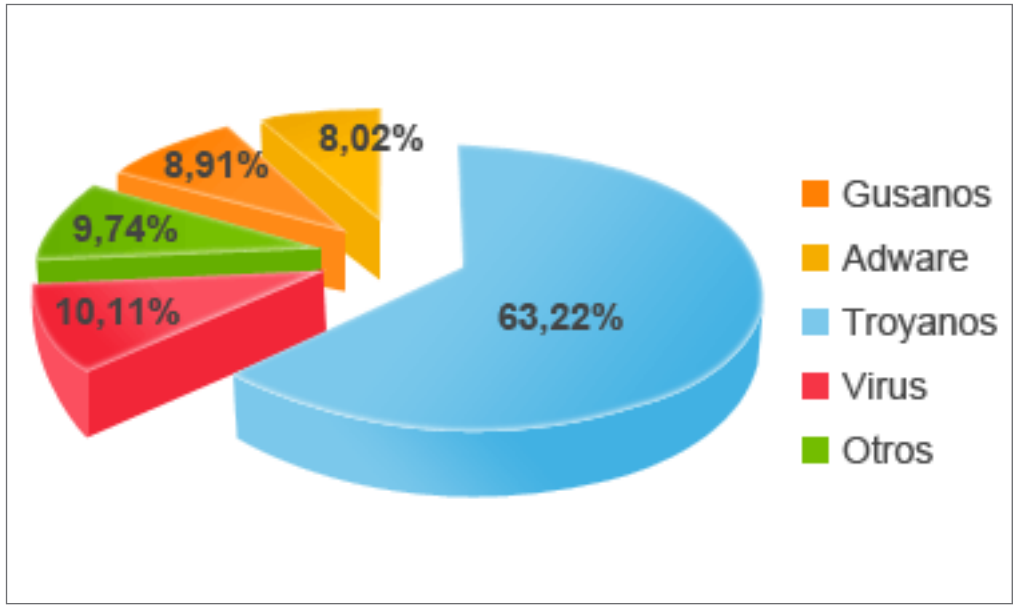


FIG.07. *DISTRIBUCIÓN DE INFECCIONES POR TIPO DE MALWARE.*

Podemos observar cómo los troyanos son los protagonistas de nuevo, siendo los responsables de un 63,22% del total de las infecciones que se han producido durante este tercer trimestre de 2011. Curiosamente, a pesar de que hemos visto cambios notables en la creación de nuevo malware (con un importante crecimiento en las cifras de troyanos) , las cifras recogidas por PandaLabs en este periodo muestran que la distribución de infecciones por tipo de malware apenas han sufrido cambios respecto al trimestre anterior.

Si vamos al detalle para ver qué malware está causando más infecciones, vemos que el Top 10 causa el 49,97% de las infecciones. Sin embargo, esta cifra puede resultar engañosa, ya que viendo el detalle de estos 10 primeros 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:

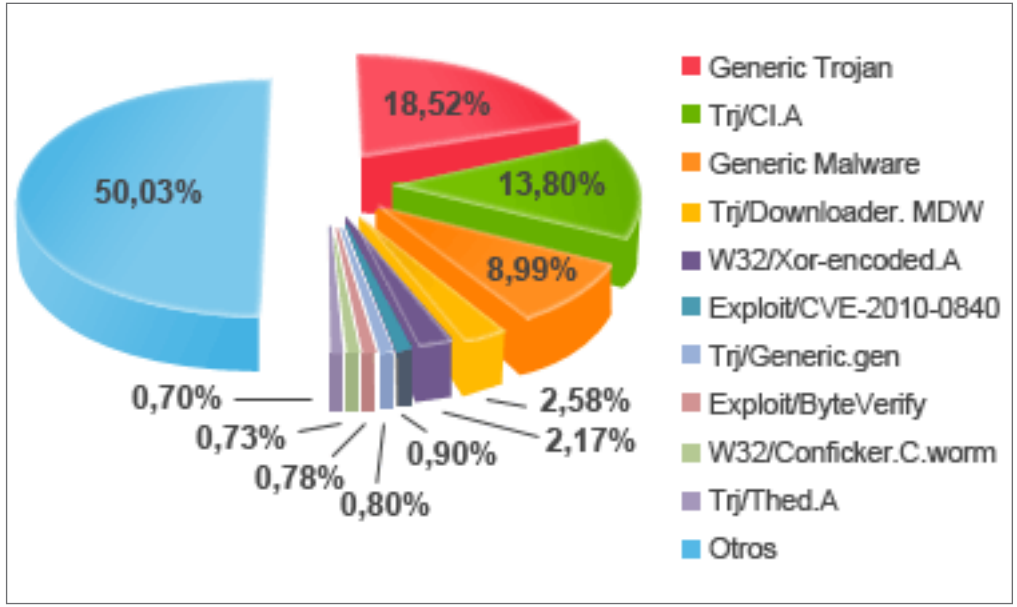


FIG.08. *FAMILIAS DE MALWARE.*

Ahora echemos un vistazo al porcentaje de equipos infectados en cada país. Usando de nuevo los datos de Inteligencia Colectiva, veremos el porcentaje de equipos infectados a nivel mundial y por país. En la siguiente gráfica mostramos los 15 países con mayor ratio de infección del mundo en el segundo trimestre de 2011:

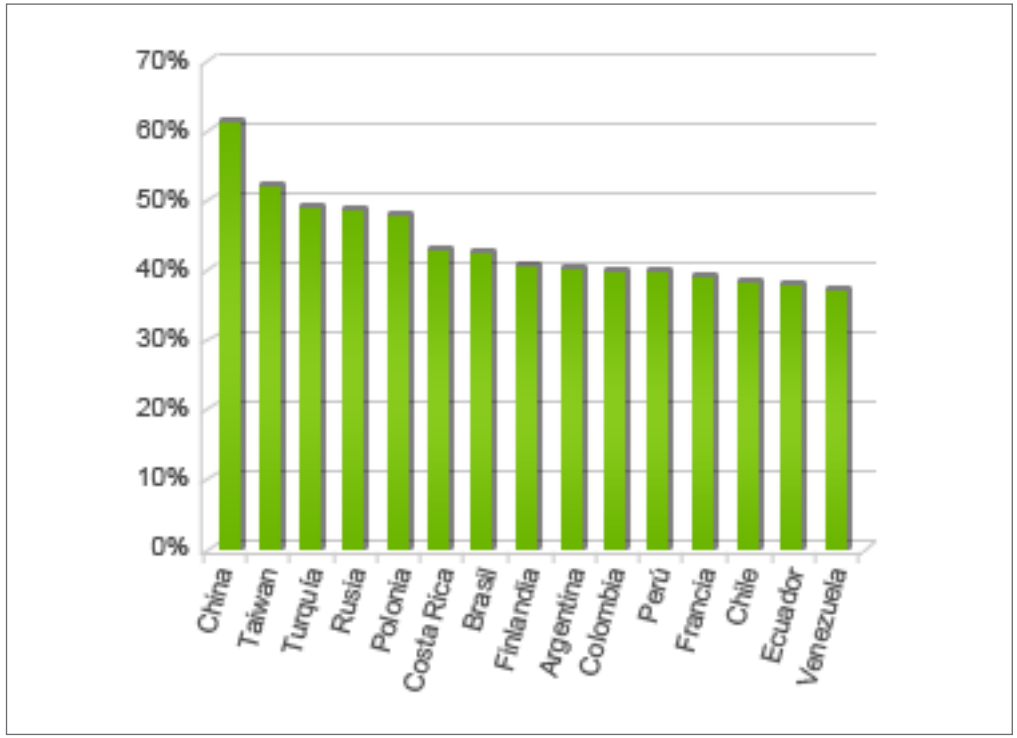


FIG.09. *PORCENTAJE DE INFECCIÓN POR PAÍSES.*

La media mundial de infecciones se sitúa en el 37,87%, un 2% menos que en el trimestre anterior. De nuevo China sigue liderando el ranking de países con mayor índice de ordenadores infectados, con un 62,47%. A cierta distancia le siguen Taiwán (50,93%), Turquía (46,68%) y Rusia (45,73%).

Respecto a los países con menor índice de infección, Suecia vuelve a ser el país del mundo mejor situado, con un 23,36%, seguido de Reino Unido (26,53%), Suiza (26,57%) y Alemania (28,20%). En el siguiente gráfico tenemos los 10 países con menor índice de infección, todos ellos europeos salvo Japón y Australia:

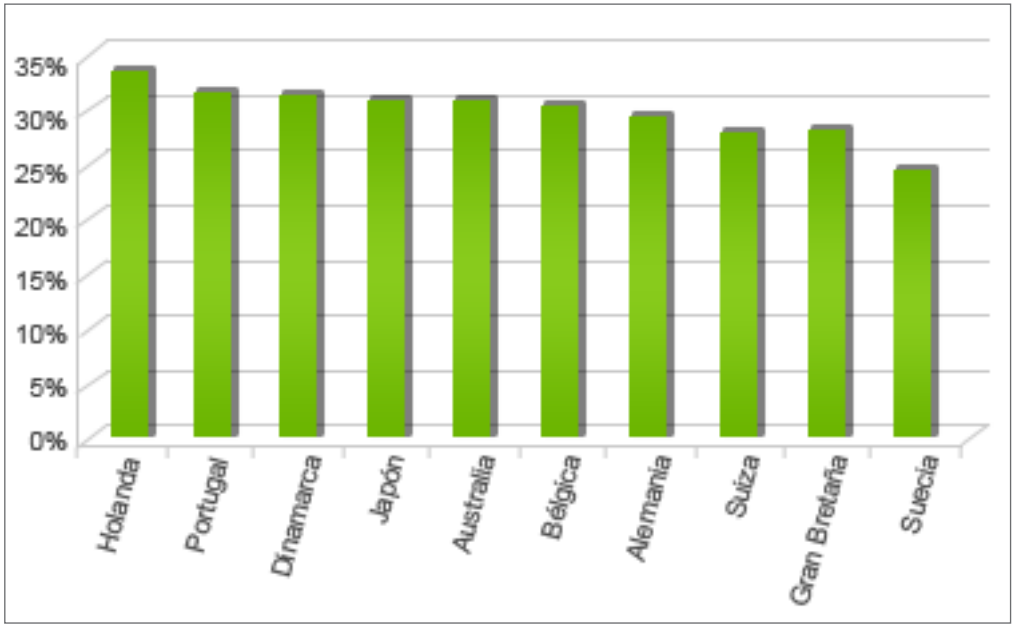


FIG.10. *LOS DIEZ PAÍSES CON MENOR RATIO DE INFECCIÓN DEL MUNDO.*

04| Exploits: cómo funcionan

En la gran mayoría de los artículos de esta sección hemos ido mostrando cada trimestre las diferentes vulnerabilidades que han ido apareciendo y el impacto que han podido tener en el mundo real.

Sin embargo, en los 2 últimos artículos decidimos modificar un poco la información que íbamos a mostrar y hablar sobre el concurso Pown2Own y la supuesta seguridad de las últimas versiones de los navegadores web. Si recordamos, en el primer trimestre mencionábamos como el navegador Google Chrome había salido victorioso de dicho concurso y teóricamente los mejores hackers más prestigiosos del mundo no habían conseguido hacerle frente. Parecía que Google Chrome era el navegador más seguro del mundo, ¿Era realmente cierta esa afirmación? En el segundo trimestre se dio respuesta a esta importante cuestión sobre seguridad, 2 meses tardaron los investigadores de la empresa VUPEN en conseguir hacerle frente y nuevamente los hackers mostraban cuan cierta es la frase que “La seguridad al 100% es inexistente”.

Esto no indica que tengamos que dejar de utilizar una herramienta tan importante como es Internet. Pero sí nos hace ver, que tenemos que dificultar por todo los medios las acciones que pueda realizar un software malicioso. En muchas ocasiones hemos recomendado tener actualizado el sistema operativo, el antivirus y cualquier otro software de seguridad. No es lo mismo para un corredor una carrera de 100 metros lisos que una de 100 metros vallas. Las empresas de seguridad nos debemos encargar de crear esas vallas que dificulten o eviten al software malicioso realizar sus acciones. Pero el usuario tiene que concienciarse que estas “vallas” son necesarias para la seguridad de sus recursos.

En este articulo vamos a explicar por qué existen las vulnerabilidades y como son aprovechadas para ejecutar código malicioso desde un punto de vista más técnico.

Este puede ser el primero de varios artículos que muestren el estado del arte de las vulnerabilidades actuales y las diferentes técnicas de explotación que existen hoy día, y si los sistemas de protección actuales son suficientes para hacerle frente. Empecemos por el principio ¿Por qué existen las vulnerabilidades?

Qué son las vulnerabilidades

Las vulnerabilidades en el campo informático y según la Wikipedia son:
Las Vulnerabilidades son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario.

En resumen: Debido a una programación insegura por parte del programador, por lo tanto siempre van a existir, un usuario puede aprovecharse de esta falla en el código para ejecutar acciones para las que no fue diseñado dicho programa.

```
1  #include <stdio.h>
2  #include <stdlib.h>
3  #include <string.h>
4
5
6  void copy_string(char * string)
7  {
8      char buffer[10];
9      strcpy(buffer, string);
10     printf("this is your buffer %s", buffer);
11     return;
12
13 }
14
15
16 int main(int argc,char *argv[])
17 {
18
19     if (argc == 2)
20     {
21         copy_string(argv[1]);
22         return 1;
23     }
24     printf("%s <buffer>", argv[0]);
25     return 0;
26 }
```

FIG.11. *IMAGEN 1.*

Ahora la pregunta sería ¿Pero cómo consigue el usuario ejecutar acciones (código) para las que no fue diseñada una aplicación? Para dar respuesta a esta pregunta tenemos que comprender cómo se ejecuta el código de una aplicación en el sistema operativo y posteriormente podremos dar respuesta a la pregunta planteada.

Para comenzar, hemos programado la siguiente aplicación utilizando el lenguaje C[1].

NOTA: El código ha sido compilado con el compilador LCC –Win32
http://www.cs.virginia.edu/~lcc-win32/

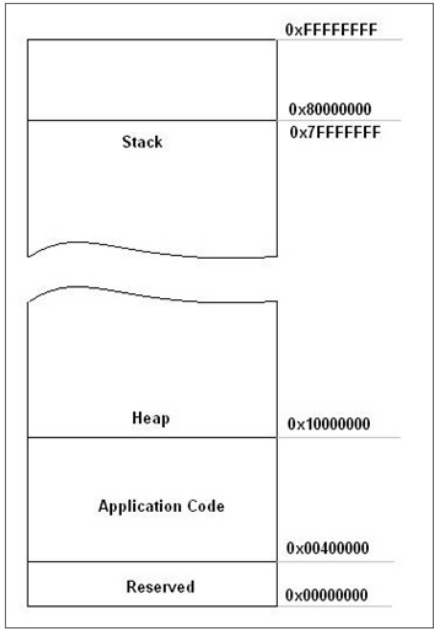
Como podemos observar, el programa es muy simple, su misión es recoger el primer parámetro que el usuario le ha introducido por consola (línea 21), copiar el valor a la variable ***buffer*** (línea 9) y mostrar el contenido de esta variable al usuario por la consola (línea 10).

Una vez compilado el programa, lo ejecutamos, le pasamos como parámetro la cadena AABBCCDD, vemos que nos devuelve el siguiente resultado esperado. Es decir la operación para la que ha sido diseñado.

```
C:\WINDOWS\system32\cmd.exe

C:\lcc\projects\lcc>example.exe AABBCCDD
this is your buffer AABBCCDD
C:\lcc\projects\lcc>
```

FIG.12. *IMAGEN 2.*



¿Qué ha sucedido? El programa ha sido cargado en memoria por el sistema operativo, entre otras cosas ha creado la ***pila*** o ***stack***[2], también el espacio de memoria ***heap***[3] y otras operaciones para empezar a ejecutar su código en el procesador o ***CPU***[4] de la máquina.

En la siguiente figura mostramos una aproximación de cómo queda estructurado el proceso en memoria de programa ejecutado.

FIG.13. *IMAGEN 3.*

La ***pila***, el ***heap*** y los ***registros***[5] del procesador son los elementos más importantes que el investigador de seguridad tiene que tener en cuenta para poder desarrollar su exploit. Además de estos factores también intervienen otros elementos que hay que tener en cuenta para poder conseguir una explotación satisfactoria de la vulnerabilidad, algunos de estos elementos son:

- Versión del sistema operativo
- Protecciones propias del sistema operativo (ASLR , DEP)
- Compatibilidad de la aplicación con las protecciones propias del sistema operativo
- Protecciones implementadas por el compilador. (/GS)
- Protecciones implementadas por el desarrollador.

La explotación de vulnerabilidades es un tema muy amplio del cual ya hay varios libros e innumerables artículos en Internet donde se habla exclusivamente de este fascinante mundo. Hay que recordar que este tema empezó a finales de los 80 y desde entonces la situación ha cambiado mucho. No obstante, en este primer artículo sólo queremos exponer las bases de cómo es posible ejecutar código arbitrario a través de una vulnerabilidad descubierta en una aplicación, y ya en próximos artículos iremos adentrándonos con más información técnica para ver cuál es el estado del arte actual de la explotación y mitigación de vulnerabilidades.

Comencemos por el principio. Una vez que se crea el proceso en memoria de la aplicación que hemos programado y cuando el sistema operativo lo considere oportuno, el procesador irá ejecutando cada una de las instrucciones que componen nuestro programa hasta finalizar con la ejecución del mismo. Cada una de estas instrucciones se irá pasando al procesador para ser ejecutada mediante el registro ***EIP***.

```
0x004012EA    PUSH DWORD PTR [EBP+8]
0x004012ED    LEA  EDI, DWORD PTR [EBP-A]
0x004012F0    PUSH EDI
0x00401302    CALL strcpy
```

FIG.14. *IMAGEN 4.*

Es decir las siguientes intrusiones se ejecutarán en el procesador y el registro ***EIP*** ira tomando los siguiente valores ***0x004012EA***, *0x004012ED* y *0x004012F0*, *0x00401302*. Por ejemplo cuando el registro ***EIP*** tome el valor 0x004012F0 el procesador pasará a ejecutar la instrucción ***"PUSH EDI"***.

Teniendo esto en mente, el objetivo de nuestro ***exploit***[9] será conseguir alterar el contenido al que apunta una de las direcciones que va a ser utilizada por el registro ***EIP***. De esta forma conseguiremos que la nueva instrucción a la que apuntará el registro ***EIP*** sea la ejecución de nuestra ***shellcode***[10] y por lo tanto habremos conseguido la ejecución del código arbitrario que hemos hablado al principio de este artículo.

Pasemos a responder ahora la pregunta que seguramente nos está rondando por la cabeza ¿Cómo se altera el contenido al que va apuntar el registro ***EIP***? Bien, es esencial saber el funcionamiento de los registros del procesador y también como se almacenan las variables del programa en la pila durante de la ejecución de un programa entre otras cosas. Para dar respuesta a esa pregunta vamos analizar lo que está sucediendo en la pila antes de la llamada a la función ***strcpy*** (linea 10) dentro de ***copy_string*** (linea 21).

El procesador va a ejecutar la línea 9 de nuestro programa y entonces llamará a la función ***strcpy*** pasando las variables **buffer** (de tipo array de caracteres) y string como parámetros a la función, antes de esta llamada la pila (ver stack en la imagen 5) tendrá el siguiente aspecto:

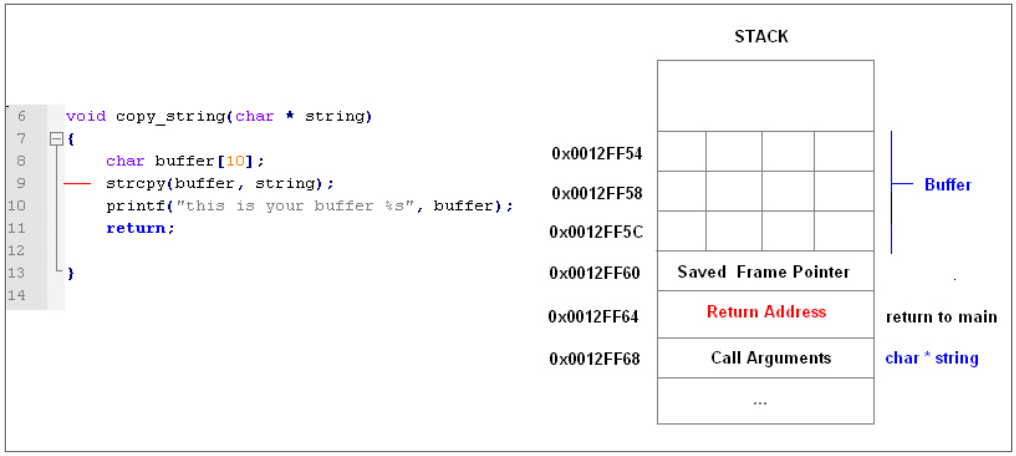


FIG.15. *IMAGEN 5.*

El primer dato almacenado en la pila en 0x0012FF68 es la dirección al parámetro ***string*** pasado a la función ***copy_string*** (linea 6 y 21) que realmente hace referencia al parámetro del usuario introducido por la consola como primer argumento para el programa que estamos ejecutando. El siguiente parámetro almacenado es ***Return Address***. Este valor es la dirección que será utilizada por el registro ***EIP*** para volver a la función ***main***, realmente es la dirección de memoria que apunta a la siguiente instrucción (línea 22 del código) dentro de main una vez que retorne de la llamada a ***copy_string***.

La siguiente instrucción a ejecutarse como hemos comentado será la línea 9, donde se pasarán los argumentos ***buffer*** y ***string*** a la función ***strcpy***. Esta función está definida en Microsoft como:

FIG.16. *IMAGEN 6.*

Su funcionamiento es muy sencillo, copia el contenido de la cadena origen al contenido de la cadena destino, además nos advierte que el comportamiento puede ser impredecible en el caso de que se superpongan ¿Cómo puede suceder esto? ***strcpy*** es una función que se encarga de copiar cadenas, es insegura porque no verifica si la cadena destino tiene suficiente capacidad para guardar el contenido de la cadena origen. Si se da esa situación, se estaría sobrescribiendo una zona de memoria destinada a otros datos y por lo tanto, se podría producir un comportamiento inesperado en la ejecución del programa, porque podría estar trabajando con unos datos incorrectos a los esperados en esa dirección de memoria que tiene contenido modificado.

Pasemos a ver cómo se comporta la aplicación si la cadena introducida es un valor inferior en tamaño a 10 bytes que es la capacidad de la variable ***buffer*** (linea 8)

Ejecutamos el comando: ***example AAAAA***

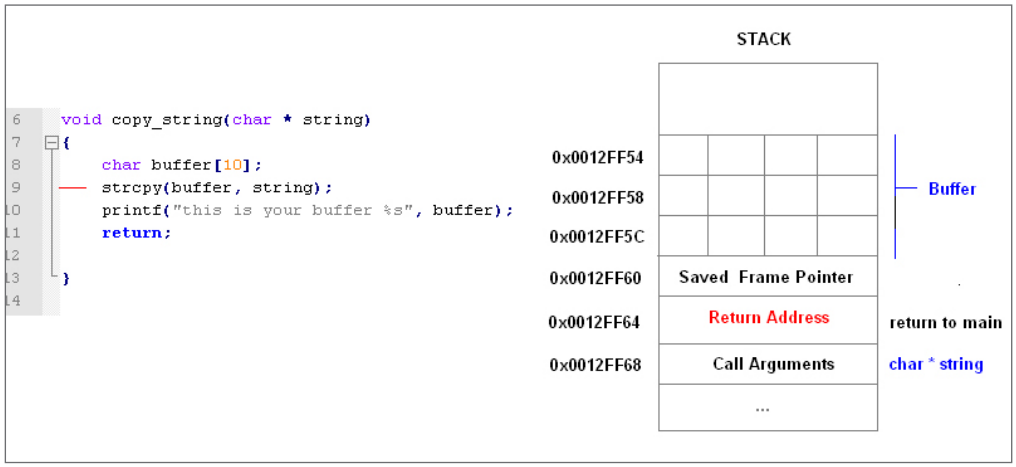


FIG.17. *IMAGEN 7.*

Como observamos en la ilustración se han rellenado 6 (en la imagen aparece el número 41 que es el valor del carácter A en formato hexadecimal y 00 como valor NULL indicando el final de una cadena de caracteres) de las 10 "celdas" (bytes) que contiene la variable ***buffer***. Es decir tal y como está programada la aplicación y al haber usado la función insegura ***strcpy***, ocuparemos tantas celdas en la memoria de la pila como longitud tenga la cadena pasada como argumento independientemente de la longitud de nuestra variable ***buffer***.

Con esta última idea ¿Se nos ocurre una forma de cómo cambiar el flujo de la aplicación sabiendo que ***strcpy*** es una función insegura? ¿No? Seguro que si, sencillamente tenemos que enviar una cadena lo suficientemente grande para ocupar el máximo de "celdas" posibles en la memoria de la ***pila*** y así modificar el valor almacenado en la dirección 0x0012FF64 que representa al valor ***Return Address*** y será ejecutado por el procesador bajo el registro ***EIP*** en el retorno a la función ***main***.

Según nuestra teoría la pila debería quedar de la siguiente forma, si le pasamos a la aplicación una cadena con una longitud de 20 caracteres.

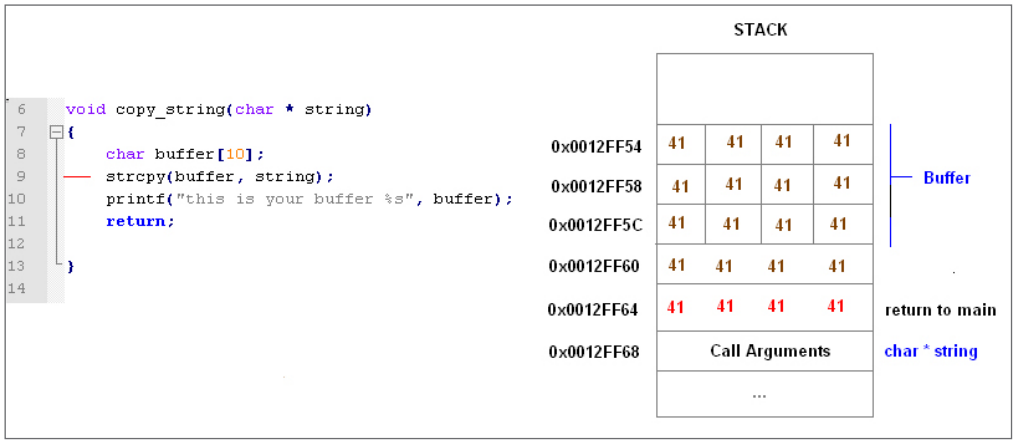


FIG.18. *IMAGEN 8.*

¡¡Hagamos la prueba!!.
Ejecutamos el comando: ***example AAAAAAAAAAAAAAAAAAAA***

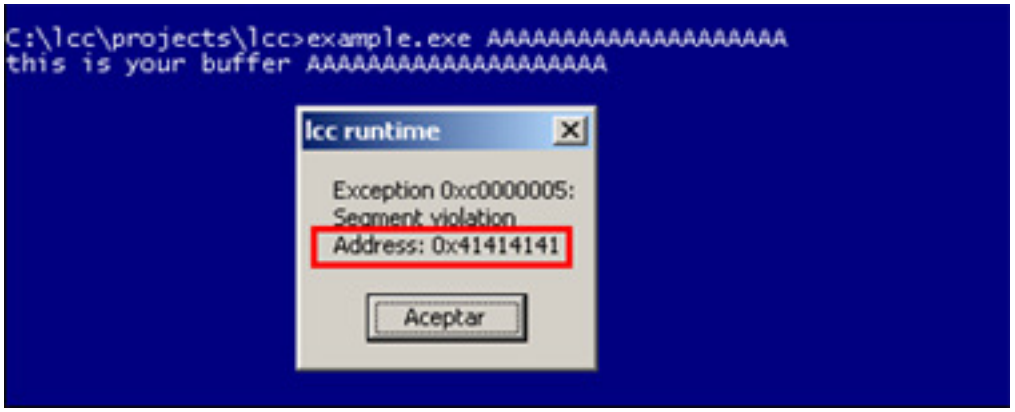


FIG.19. *IMAGEN 9.*

¡¡Perfecto!! lo hemos conseguido, se ha ejecutado la dirección ***0x41414141***. Y se ha lanzado una excepción porque no es una dirección válida para nuestro proceso.

En el mundo de la seguridad informática esta vulnerabilidad se denomina DoS[11] o (de) negación de servicio, el objetivo es paralizar el servicio de una aplicación. Esto puede tener graves consecuencias, imaginaos si los servidores de Internet de un banco quedaran paralizados, se perderían seguramente millones de euros por cada minuto que esté caído el servicio.

No obstante al principio hemos mencionado cómo se podría ejecutar código arbitrario a través de una vulnerabilidad. La respuesta llegados a este punto es sencilla, en vez de utilizar la dirección ***0x41414141*** que es inválida, el usuario se las tendría que ingeniar para ser capaz de utilizar una dirección válida de memoria que este apuntando a la shellcode o código que queramos ejecutar. Ahora bien ¿Cómo introducimos la shellcode en la memoria del programa?¿Cómo se salta la shellcode?¿Es posible ejecutar código arbitrario en todas las vulnerabilidades encontradas? Esta parte la dejamos para que investiguéis y os la responderemos en próximos artículos.

Si quieres más información sobre este tema puedes leer The Shellcode Handbook, un libro muy recomendado para adquirir más conocimiento sobre la creación de exploits y vulnerabilidades.

1 http://en.wikipedia.org/wiki/C_%28programming_language%29
2 http://en.wikipedia.org/wiki/Stack_%28abstract_data_type%29
3 http://en.wikipedia.org/wiki/Heap_%28data_structure%29
4 http://en.wikipedia.org/wiki/Central_processing_unit
5 http://en.wikipedia.org/wiki/Processor_register
6 http://en.wikipedia.org/wiki/ASLR
7 http://en.wikipedia.org/wiki/Data_Execution_Prevention
8 http://en.wikipedia.org/wiki/Stack-smashing_protection#Microsoft_Visual_Studio_.2FGS
9 http://en.wikipedia.org/wiki/Exploit_%28computer_security%29
10 http://en.wikipedia.org/wiki/Shellcode
11 http://en.wikipedia.org/wiki/Denial-of-service_attack

05| Conclusión

Vivimos en un mundo cada vez más conectado, donde estar actualizando tu estado en Facebook o en Twitter ya no sólo corresponde a nuestro rato de ocio en casa o por motivos laborales en la oficina, sino que los dispositivos móviles nos llevan cada vez más a estar conectados permanentemente.

Esto no sólo nos beneficia a los usuarios, sino que abre una nueva ventana de oportunidad para los ciberdelincuentes que, como hemos podido comprobar, no pierden su oportunidad. Esta ciberdelincuencia cada vez más profesionalizada no deja de buscar nuevos métodos con los que optimizar su trabajo, que no es otro que robar información a los usuarios.

Por otro lado, parece que la idea de "ciberguerra" se asienta más que nunca, y que el caso Stuxnet no fue algo aislado, sino la punta del iceberg, y que vamos a ser testigos de una carrera "ciberarmamentística" que nada tendrá que envidiar a los tiempos de la Guerra Fría, aunque esta vez a través de Internet.

Esto ha sido todo lo que ha dado de sí el tercer trimestre de este año en lo que a seguridad informática se refiere. En el próximo número daremos un repaso a todo lo acontecido a lo largo de 2011, y nos asomaremos a lo que nos deparará el próximo.

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