Archivo
<< 2013
ene feb mar
abr may

Artículos analíticos más populares

- Desarrollo de las amenazas informáticas en el primer trimestre de 2013
- ¡Felicidades, acabas de ganar! La realidad detrás de las loterías online
- Keyloggers: Qué son y cómo detectarlos (primera parte)
- Kaspersky: Boletín de seguridad 2012. Estadística general de 2012
- El spam en el primer trimestre de 2013

Información para autores potenciales

¿Quiere usted ser uno de nuestros autores y ver su trabajo publicado en nuestro sito web Viruslist.com? ¡Escríbanos!

Home / Análisis

Kaspersky: Boletín de seguridad 2012. Estadística general de 2012

10.12.2012 | Comentar

Denís Máslennikov
Yury Namestnikov

Este informe es parte de Kaspersky Security Bulletin y se basa en los datos obtenidos y procesados por el sistema Kaspersky Security Network. KSN usa una arquitectura "en la nube" en sus productos personales y corporativos y es una de las tecnologías más importantes de Kaspersky Lab.

Kaspersky Security Network permite a nuestros expertos, en tiempo real, detectar los nuevos programas nocivos que todavía no tienen antídoto en forma de identikits o que los métodos heurísticos no pueden detectar. KSN permite desenmascarar las fuentes de propagación de programas nocivos en Internet y evitar que los usuarios se conecten a los sitios infectados.

Al mismo tiempo, KSN permite aumentar la velocidad de reacción ante las nuevas amenazas, ya que se puede bloquear el lanzamiento de un nuevo programa nocivo en los equipos de los usuarios de KSN en una fracción de segundo desde el momento en que se le asigne el dictamen de "peligroso", sin necesidad de actualizar las bases antivirus.

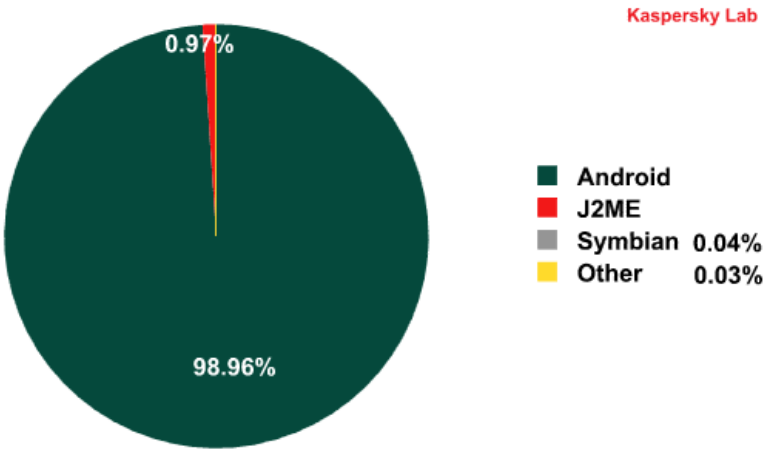
La estadística de este informe se basa en los datos recopilados por los productos de Kaspersky Lab en los equipos de los usuarios que dieron su consentimiento al envío de datos estadísticos.

Amenazas móviles

El desarrollo de las amenazas móviles en 2012 transcurrió bajo la divisa “Toda la atención para Android”. Los creadores de virus se concentraron en el “robot verde”. También se cumplieron nuestros pronósticos sobre el desarrollo de las amenazas móviles en 2012, en los que vaticinábamos la creación de botnets móviles, ataques contra blancos específicos mediante malware móvil y el “espionaje móvil”.

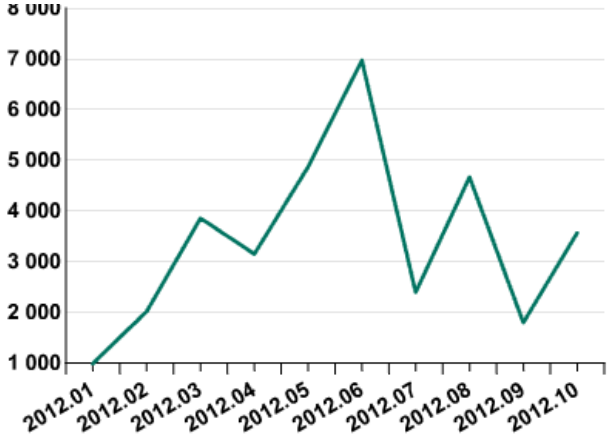
Programas nocivos para Android

En 2012 los esfuerzos de los creadores de virus se concentraron sobre todo a la creación de programas maliciosos para Android. Esto condujo al crecimiento tanto cualitativo como cuantitativo del malware móvil para esta plataforma. El 99% del malware móvil que detectamos cada mes es para la plataforma Android.

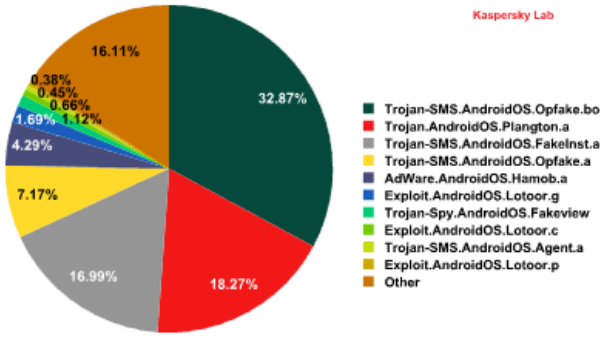


Distribución del malware móvil por plataformas en 2012

Kaspersky Lab



Dinámica de aparición de nuevos programas maliciosos móviles por mes, 2012



TOP 10 de malware para Android

Los objetos más propagados y detectados en los smartphones se pueden dividir en 3 grupos principales: troyanos SMS, módulos publicitarios y exploits para obtener derechos de root en el smartphone.

De ellos, los más propagados eran los troyanos SMS que en su mayoría están dirigidos a los usuarios de Rusia. Esto no es nada sorprendente, si se tiene en cuenta la antigua popularidad de estos programas maliciosos entre los creadores rusos de virus. Los SMS de alto coste siguen siendo el método más lucrativo entre los delincuentes informáticos móviles.

El segundo grupo de amenazas móviles del TOP 10 son los módulos publicitarios Plangton y Hamob. No es casualidad que la primera familia se detecte como troyano. Plangton suele encontrarse en las aplicaciones gratuitas y en efecto muestra publicidad, pero también puede suplantar la página de inicio del navegador. La cuestión es que la suplantación ocurre sin avisar al usuario y sin su consentimiento, por lo que se considera que es un comportamiento malicioso. En lo que atañe a Hamob, bajo el nombre de AdWare.AndroidOS.Hamob se detectan las aplicaciones que se hacen pasar por programas útiles, pero en realidad sólo muestran anuncios publicitarios al usuario.

Y, para finalizar, el tercer grupo. Aquí están las diferentes modificaciones de los exploits para obtener privilegios de root en los smartphones con diferentes versiones de Android.

Esta popularidad de los exploits está condicionada por el hecho de que diferentes modificaciones de backdors pertenecientes a diversas familias, cuyo número ha crecido este último año, usan las mismas modificaciones de exploits para obtener altos privilegios (de root).

Crecimiento del número de incidentes con programas maliciosos en las tiendas oficiales de aplicaciones, sobre todo en Android Market

A pesar de que Google ha implementado el módulo Google Bouncer, que efectúa el análisis automático de todas la nuevas aplicaciones en Google Play (ex Android Market), no hay cambios sustanciales en el promedio de incidentes. La atención pública suele sentirse atraída por los casos con gran cantidad de infecciones, por ejemplo, el incidente causado por el programa malicioso Dougalek, cuyas copias descargaron decenas de miles de usuarios (sobre todo de Japón). Esto provocó una de las más grandes fugas de información personal de los usuarios de dispositivos móviles. Para tampoco hay que olvidar los

fugas de información personal de los usuarios de dispositivos móviles. Pero tampoco hay que olvidar los cientos de otros incidentes con menor cantidad de víctimas.

También cabe destacar el primer caso de detección de software malicioso para iOS en App Store. A principios de julio se descubrió una aplicación sospechosa llamada "Find and Call", tanto en App Store como en Android Market. Al descargar e instalar este programa, el usuario veía una solicitud de registro, que le pedía ingresar su dirección de correo electrónico y número de teléfono. Después del registro, los datos ingresados y la libreta telefónica se enviaban a un servidor remoto.

Parte del procedimiento de envío de la libreta telefónica al servidor remoto

Después de cierto tiempo, a cada uno de los números de teléfono robados llegaba spam SMS que incitaba a seguir un enlace para descargar "Find and Call".

Las primeras botnets móviles

El primer síntoma fue el descubrimiento a principios de año del bot IRC para Android llamado Foncy, que funcionaba en conjunto con el troyano SMS del mismo nombre. Era precisamente el bot IRC el que podía tomar el control del smartphone después de la infección. Y es que además del troyano SMS en el droper APK había un root exploit que se usaba para obtener altos privilegios en el sistema infectado. Y después de conectarse con el servidor de administración el bot podía recibir y ejecutar instrucciones shell. De hecho, todos los smartphones infectados por el bot IRC Foncy formaban una verdadera botnet y estaban dispuestos a realizar prácticamente cualquier cosa que les ordenara su "dueño".

Los creadores de virus chinos lograron crear una botnet de entre 10.000 a 30.000 dispositivos activos, pero el total de smartphones infectados alcanzaba varios cientos de miles. La base de esta botnet era el backdoor RootSmart, que tiene varias funciones de control remoto de dispositivos con Android. Para propagar RootSmart, los delincuentes informáticos usaron un truco conocido y efectivo: empaquetaron un programa legítimo y lo pusieron en el sitio de una popular tienda china extraoficial de aplicaciones para Android. Como resultado, los usuarios que descargaban el programa, que supuestamente servía para configurar el teléfono, recibían junto con él un backdoor que agregaba sus dispositivos a la botnet.

Las dimensiones de la infección causada por RootSmart permitieron a los delincuentes convertir en dinero contante y sonante la red creada con los teléfonos infectados. Para este fin eligieron el método más popular entre los delincuentes informáticos móviles, que consiste en enviar mensajes SMS de pago a números cortos. Los delincuentes usaban los números más baratos para que las víctimas no se dieran cuenta de sus pérdidas durante el máximo tiempo. El control total que los delincuentes obtenían sobre los dispositivos móviles les daba la posibilidad de ocultar por largo tiempo la presencia del programa malicioso y aprovecharlo para robar más dinero.

Ataques contra blancos específicos mediante malware móvil

En 2012 se usaron algunos nuevos programas maliciosos para sistemas operativos diferentes a Android en ataques contra blancos específicos.

Un buen ejemplo de estos ataques son los lanzados mediante ZitMo y SpitMo (Zeus- y SpyEye-in-the-Mobile). Nuevas versiones de ZitMo y SpitMo aparecían con regularidad, tanto para Android como para otros sistemas operativos. Los escritores de virus siguen usando los mismos métodos de camuflaje que hace dos años. O bien los disfrazan de "certificados de seguridad", o bien los hacen pasar como software para proteger smartphones.

Métodos tradicionales de camuflaje de ZitMo/SpitMo

A pesar de que los sistemas operativos diferentes a Android no son tan populares, esto no significa que ya nadie los use. A los escritores de virus, por ejemplo, les da lo mismo los rumores de la pronta muerte de Blackberry. En 2012 también aparecieron nuevas versiones de ZitMo para esta plataforma, y los delincuentes usaron al mismo tiempo este programa malicioso para Blackberry y para Android. Por lo menos, los números de los servidores de administración de ambas versiones eran los mismos.

Espionaje mediante malware móvil

El año pasado pronosticamos que el espionaje móvil – el robo de datos de los teléfonos móviles y el seguimiento de las personas mediante su teléfono móvil y servicios de geolocalización- se convertiría en un fenómeno ampliamente difundido, saliendo de los límites del uso común que hacen los órganos del estado y algunas compañías de detectives de estas tecnologías.

Por desgracia, así fue. La cantidad de programas maliciosos que por su comportamiento son troyanos-espía o backdoors ha crecido en cientos de veces. También merece la pena destacar la creciente cantidad de aplicaciones comerciales de monitorización, que a veces son difíciles de diferenciar de los programas maliciosos.

El ejemplo más claro de espionaje con el uso de programas maliciosos móviles es el incidente del módulo

publicitario FinSpy. Este módulo fue desarrollado por la compañía británica Gamma International, que se especializa en la creación de software de monitorización para organizaciones estatales. De hecho, este programa tiene funcionalidades de troyano-espía. La compañía The Citizen Lab logró descubrir versiones móviles de FinSpy en agosto de 2012. Se descubrieron modificaciones del troyano para las plataformas Android, iOS, Windows Mobile y Symbian. Sin lugar a dudas, existen diferencias entre ellos, pero todos pueden hacer un seguimiento de casi todas las actividades de los usuarios en el equipo infectado, seguir su paradero, hacer llamadas en secreto y enviar información a servidores remotos.

Por el momento no hay respuesta a la interrogante sobre quién pidió a FinSpy atacar a víctimas en concreto, y es poco probable que lo sepamos en el futuro. Pero incluso sin esta información la aparición de FinSpy marca el inicio de un nuevo capítulo en la historia del malware móvil: al igual que las ordenadoras comunes y

marca el inicio de un nuevo capítulo en la historia del malware móvil: al igual que los ordenadores comunes y corrientes, los dispositivos móviles se están convirtiendo en blancos de ataques contra objetivos específicos y ataques espía.

Programas maliciosos para Mac

En 2012 se derrumbaron todos los mitos sobre la seguridad de los equipos Mac. Este año mostró que el malware para Mac constituye una seria amenaza a la seguridad.

A principios de año se descubrió Flashfake, una botnet de 700.000 bots formada exclusivamente por equipos Mac. (El análisis completo de este troyano-descargador se publicó en viruslist.es).

Después, no hubo más epidemias de FlashFake, pero los delincuentes usaron el malware para Mac durante todo el año para hacer sus ataques. La razón es que los productos de la compañía Apple son populares entre muchos políticos influyentes y hombres de negocios, y la información que guardan sus ordenadores representa interés para determinada categoría de delincuentes.

En 2012 nuestros expertos antivirus agregaron un **30%** más de firmas para detectar troyanos para Mac que en 2011. Si comparamos con 2010, la cantidad de firmas agregadas por año se ha multiplicado por 6.

Número de firmas antivirus para Mac OS X, por año

El programa malicioso para Mac más propagado es FlashFake, y sus primeras versiones se descubrieron ya en 2011. FlashFake fue el líder absoluto, según la estadística del primer semestre de 2012. Pero veamos cuales fueron los programas maliciosos para Mac OS X más propagados en el segundo semestre de 2012.

TOP 10 de programas maliciosos para Mac OS X, segundo semestre de 2012

Puesto	Nombre	% del total de ataques
1	Trojan.OSX.FakeCo.a	52%
2	Trojan-Downloader.OSX.Jahlav.d	8%
3	Trojan-Downloader.OSX.Flashfake.ai	7%
4	Trojan-Downloader.OSX.FavDonw.c	5%
5	Trojan-Downloader.OSX.FavDonw.a	2%
6	Trojan-Downloader.OSX.Flashfake.ab	2%
7	Trojan-FakeAV.OSX.Defma.gen	2%
8	Trojan-FakeAV.OSX.Defma.f	1%
9	Exploit.OSX.Smid.b	1%
10	Trojan-Downloader.OSX.Flashfake.af	1%

En el primer puesto tenemos a Trojan.OSX.FakeCo.a (52%). Este programa malicioso se disfraza de fichero de instalación de un códec de video. Después de la instalación, no aparecen nuevos códecs en el sistema, y el programa instalado se comporta como un programa AdWare, que recopila información de marketing sobre el usuario y se la envía a los delincuentes.

El segundo puesto de la lista lo ocupa el troyano Jahlav (8%), conocido desde hace cuatro años. Este

programa malicioso también se disfraza de fichero de instalación de un códec de video. Pero en vez de un códec, instala un programa malicioso que, sin que el usuario se dé cuenta, se conecta al servidor de los delincuentes y puede descargar otros ficheros al equipo infectado. Como regla, este programa malicioso trata de descargar un troyano que suplanta las direcciones de DNS por las de los servidores de los delincuentes (Kaspersky Lab lo detecta como Trojan.OSX.Dnscha).

En el cuarto y quinto lugar están los programas de la familia TTrojan-Downloader.OSX.FavDonw, que suman el 7% de las incidencias. Estos programas tienen un sólo objetivo: después de instalarse en el Mac, descargan falsos antivirus.

En los puestos 7 y 8 se encuentran los antivirus falsos de la familia Trojan-FakeAV.OSX.Defma, que extorsionan a los clientes exigiéndoles dinero por curar supuestos programas maliciosos.

En el noveno puesto está el exploit Exploit.OSX.Smid.b, dirigido a una vulnerabilidad en Java y que permite al delincuente ejecutar cualquier código en los equipos que no tienen Java actualizado.

Después de que descubriéramos la botnet FlashFake, la compañía Apple ha empezado a poner más empeño en las cuestiones de seguridad de su sistema operativo. Por ejemplo, publicó los parches críticos para Oracle Java al mismo tiempo que las versiones para Windows y anunció las funciones de defensa de la siguiente versión de Mac OS X: sólo se podrán instalar de forma predeterminada programas de la tienda oficial, se usará una máquina virtual para los programas descargados de la tienda, la instalación de las actualizaciones será automática, etc.

Programas nocivos en Internet (ataques por la Web)

La cantidad de ataques mediante navegadores web en un año subió de 946.393.693 a **1.595.587.670.** De esta manera, nuestros productos protegieron a los usuarios de los peligros de navegación en Internet un promedio de 4.371.473 veces al día.

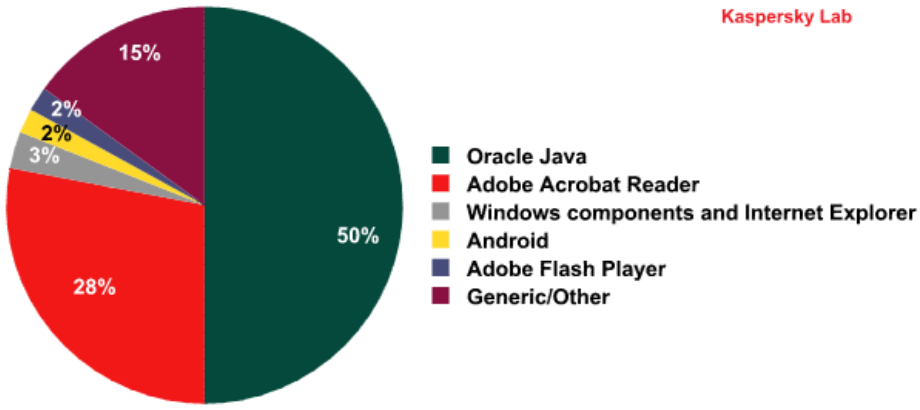
En comparación con el año pasado, el ritmo de crecimiento de la cantidad de ataques a través de navegadores web casi no ha cambiado. La cantidad de ataques neutralizados en 2012 supera a la de 2011 en 1,7 veces, mientras que 2011 superó a 2010 en 1,6 veces. El principal método de ataque (mediante exploits packs) da a los delincuentes una garantía casi total de infectar equipos, si estos no cuentan con protección y tienen por lo menos una aplicación popular vulnerable.

Aplicaciones vulnerables usadas por los delincuentes

Aplicaciones vulnerables usadas por los delincuentes

Si bautizamos 2011 como “el año de las vulnerabilidades”, podemos llamar con tranquilidad a 2012 “el año de las vulnerabilidades Java”: este año la mitad de los ataques registrados se realizaron mediante exploits dirigidos a Java.

Hoy en día Java está instalado en más de 3.000.000.000 dispositivos que usan diferentes sistemas operativos. Por lo tanto, para algunos errores de Java se pueden crear exploits que funcionen en múltiples plataformas. En el transcurso del año hemos analizado tanto ataques masivos con conjuntos de exploits, como ataques para blancos específicos en los que usaban exploits Java dirigidos a PC y a Mac.

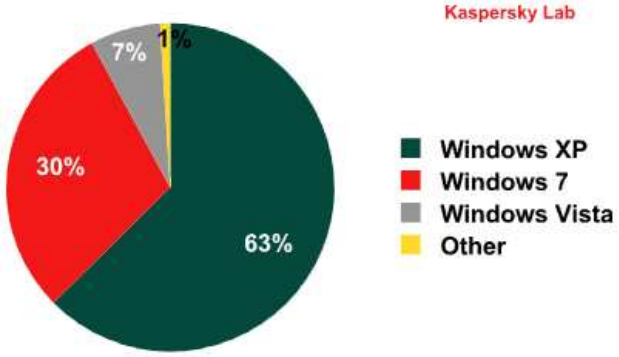


Aplicaciones cuyas vulnerabilidades usaron los exploits web, 2012

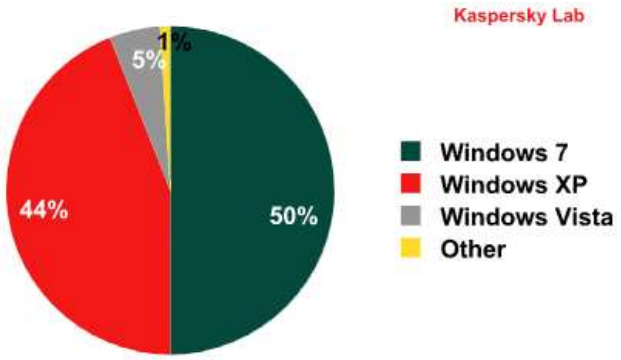
En 2012 bajó la popularidad de los exploits para Adobe Reader, que este año causaron el 28% de todos los incidentes. Como resultado, Adobe Reader ocupó el segundo puesto de la estadística. Hacemos notar que en las últimas versiones de Adobe Reader se prestó mucha atención al problema de las vulnerabilidades. En particular, se implementaron nuevos mecanismos que protegen la aplicación contra los exploits. Estas medidas hacen que sea mucho más difícil crear exploits efectivos.

En el tercer lugar se ubican los programas que usan vulnerabilidades para diferentes componentes de Windows e Internet Explorer. Durante el año se usaron de forma activa exploits para vulnerabilidades ya detectadas en 2010: MS10-042 en Windows Help and Support Center y MS04-028, relacionada con el procesamiento incorrecto de ficheros jpeg.

En el cuarto puesto, con un 2%, están los exploits para la plataforma móvil Android OS. Los delincuentes usan estos exploits para obtener privilegios de root, que les dan posibilidades casi ilimitadas para hacer manipulaciones sobre el sistema.



Distribución de versiones del SO Windows instalado en los equipos de los usuarios, 2011



Distribución de versiones del SO Windows instalado en los equipos de los usuarios, 2012

En este año, la cantidad de usuarios de Windows 7 aumentó del 30% al 50%. A pesar de que Windows 7 se actualiza a intervalos regulares, los ataques contra los equipos de los usuarios siguen teniendo lugar: como ya hemos mencionado, las intrusiones en el sistema no se hacen mediante los componentes de Windows, sino a través de las aplicaciones de otros fabricantes.

Programas maliciosos en Internet: Top 20

De todos los programas maliciosos que tomaron parte en ataques a los usuarios, hemos destacado 20 que fueron los más activos. Ellos son los responsables del 96% de los ataques en Internet.

Puesto	Nombre*	Cantidad de ataques	% del total de ataques**
1	URL maliciosas	1 393 829 795	87.36%
2	Trojan.Script.Iframer	58 279 262	3.65%
3	Trojan.Script.Generic	38 948 140	2.44%
4	Trojan.Win32.Generic	5 670 627	0.36%
5	Trojan-Downloader.Script.Generic	4 695 210	0.29%
6	Exploit.Script.Blocker	4 557 284	0.29%
7	Trojan.JS.Popupper.aw	3 355 605	0.21%
8	Exploit.Script.Generic	2 943 410	0.18%
9	Trojan-Downloader.SWF.Voleydaytor.h	2 573 072	0.16%
10	AdWare.Win32.IBryte.x	1 623 246	0.10%
11	Trojan-Downloader.Win32.Generic	1 611 565	0.10%
12	AdWare.Win32.ScreenSaver.e	1 381 242	0.09%
13	Trojan-Downloader.JS.Iframe.cxk	1 376 898	0.09%
14	Trojan-Downloader.JS.Iframe.cyq	1 079 163	0.07%
15	Trojan-Downloader.JS.Expack.sn	1 071 626	0.07%
16	AdWare.Win32.ScreenSaver.i	1 069 954	0.07%
17	Trojan-Downloader.JS.JScript.ag	1 044 147	0.07%
18	Trojan-Downloader.JS.Agent.gmf	1 040 738	0.07%
19	Trojan-Downloader.JS.Agent.gqu	983 899	0.06%
20	Trojan-Downloader.Win32.Agent.gyai	982 626	0.06%

** Veredictos de detección del módulo antivirus para la web. Información prestada por los usuarios de productos de Kaspersky Lab que han dado su consentimiento para el envío de datos estadísticos.*
*** Porcentaje del total de ataques web registrados en los equipos de usuarios únicos.*

Los sitios maliciosos detectados con la ayuda de métodos heurísticos "en la nube", sin mediar actualizaciones de las clásicas bases antivirus, ocupan el primer puesto de la estadística. El desarrollo de las nuevas tecnologías de detección que se fundamentan en las posibilidades de KSN, ha permitido aumentar la detección de amenazas por estos métodos del 75% al 87%. Una importante parte de las detecciones de URLs maliciosas corresponde a sitios con exploits.

En el segundo puesto están los scripts maliciosos que los delincuentes incrustan en el código de sitios legítimos hackeados con la ayuda de programas especiales. Esto es un indicio de que en muchos sitios legítimos hay inyecciones de código malicioso en forma de tags iframe invisibles. Estos scripts remiten al usuario, sin que se dé cuenta, a páginas web maliciosas durante los ataques drive-by. Scripts maliciosos similares se asentaron en los puestos 13 y 14.

Las posiciones 3, 4 y 5 las ocupan diferentes veredictos heurísticos que detectan scripts maliciosos y ficheros ejecutables PE, que se pueden dividir en dos categorías. El malware de la primera categoría descarga y ejecuta otros programas maliciosos. Los objetos maliciosos de la segunda categoría roban datos de banca en Internet, cuentas de redes sociales, servicios, etc.

En el noveno puesto está Trojan-Downloader.SWF.Voleydaytor.h, descubierto en diferentes sitios de la categoría "Para adultos". Bajo la apariencia de una actualización de un programa de reproducción de vídeos, se instalan diferentes programas maliciosos en los equipos de los usuarios.

En la estadística hay dos representantes de los exploits, Exploit.Script.Generic, cuya descarga se bloqueó casi tres millones de veces, y Exploit.Script.Bloker, con 4,5 millones de descargas bloqueadas. En la absoluta mayoría de los casos, los usuarios no se topan con exploits solitarios, sino con conjuntos de exploits. Estos son una parte integrante de los ataques drive-by. Uno de los rasgos importantes es que los paquetes de exploits se modifican y actualizan todo el tiempo para integrarles vulnerabilidades recientes y métodos de evadir los medios de defensa.

Tres posiciones del TOP 20 las ocupan programas publicitarios de las familias iBryte y ScreenSaver. El programa publicitario AdWare.Win32.IBryte.x, se propaga como un descargador de programas populares gratuitos. Después de iniciarse, descarga el programa gratuito solicitado por el usuario y al mismo tiempo instala un módulo publicitario. El programa se puede descargar del sitio oficial con el mismo éxito y así evitar la instalación del módulo publicitario. El año pasado los representantes de la familia AdWare eran el doble. La disminución de la cantidad de estos programas se debe a que se los sustituye por nuevos métodos de visualización de publicidad más efectivos y, lo que es más importante, legales, como la publicidad de contexto en los sistemas de búsqueda y las redes sociales.

A diferencia de 2011, en la estadística no hay programas usados para estafas con números SMS cortos, de la familia Hoax.Win32.ArchSMS. Estos programas exigen enviar SMS a un número corto para recibir el código para descifrar un archivo descargado por el usuario. En 2011 los delincuentes crearon sitios similares a los repositorios de ficheros, pero los archivos ofrecidos no tenían ningún contenido. En 2012 los delincuentes empezaron a crear sitios que dan la posibilidad de utilizar el mismo esquema de estafa sin descargar ningún fichero al disco. Los programas de Kaspersky Lab ponen estos programas en la lista negra de forma automática.

Países en cuyos recursos se hospedan programas nocivos: Top 20

Para lanzar **1.595.587.670** ataques mediante Internet los delincuentes usaron 6.537.320 hosts únicos, dos millones menos que en 2011. En 202 países y territorios del mundo se encontraron servidores que contenían códigos maliciosos. El 96,1% de los ataques que detectamos en Internet se lanzaron desde hostings maliciosos situados en veinte países.

Puesto	País*	Cantidad de ataques**	% del total de ataques*
1	Estados Unidos	413 622 459	25.5%
2	Federación Rusa	317 697 806	19.6%
3	Países Bajos	271 583 924	16.8%
4	Alemania	184 661 326	11.4%
5	Inglaterra	90 127 327	5.6%
6	Ucrania	71 012 583	4.4%
7	Francia	56 808 749	3.5%
8	China	31 637 561	2.0%
9	Islas Vírgenes, Inglaterra	26 593 331	1.6%
10	Canadá	19 316 279	1.2%
11	República Checa	13 311 441	0.8%
12	Israel	9 953 064	0.6%
13	Suecia	9 093 053	0.6%
14	Rumania	6 881 404	0.4%
15	Vietnam	6 624 570	0.4%
16	España	6 543 135	0.4%
17	Polonia	6 325 848	0.4%
18	Luxenburgo	5 669 370	0.3%
19	Irlanda	4 854 163	0.3%
20	Letonia	4 685 861	0.3%

La presente estadística contiene los veredictos de detección del módulo del antivirus web que enviaron los usuarios de los productos de Kaspersky Lab que dieron su consentimiento para el envío de datos estadísticos.
Para determinar la fuente geográfica de los ataques se usaba el método de yuxtaponer el nombre de dominio a la dirección IP real, en la cual se encuentra este dominio y determinar la ubicación geográfica de esta dirección IP (GEOIP).
*** Suma de los ataques únicos registrados por el antivirus web desde los recursos web ubicados en el país.*

EE.UU. (25,5%) y Rusia (19,6%) ocupan los dos primeros puestos en la estadística. La presencia de los Países Bajos (16,8%) y Alemania (11,4%) entre los cinco primeros es estable y este es el tercer año consecutivo que ocupan el tercer y cuarto puesto respectivamente. Si bien el índice de EE.UU. este año aumentó en sólo un 0,1%, los índices de hosting malicioso de Rusia (+5%), Holanda (+7%) y Alemania (+2,7%) han crecido notablemente.

Hasta 2010 China ocupaba el primer puesto, porque en sus servidores se encontraba más del 50% de todos los hostings maliciosos del mundo. En 2010 el gobierno de China pudo eliminar una gran cantidad de hostings maliciosos y al mismo tiempo hizo más duras las reglas de registro de dominios en la zona .cn. Después de esto, la cantidad de hostings maliciosos en China se redujo drásticamente y desde entonces observamos la progresiva consolidación de los hostings en EE.UU, Rusia, Países Bajos y Alemania.

El estable crecimiento de los índices de Rusia tiene dos motivos. En primer lugar, por desgracia no son raras las intrusiones en sitios legítimos, entre ellos los mayores portales de la zona .ru. El segundo motivo es que los delincuentes cibernéticos rusos se sienten muy cómodos en el espacio informático ruso y crean muchos sitios maliciosos. Los castigos previstos por las leyes rusas para los delitos informáticos son bastante suaves (la mayor parte de las veces con libertad condicional) y es raro que ordenen clausurar los servidores de administración. Si el ritmo de crecimiento de la cantidad de hostings maliciosos situados en servidores rusos se conserva en el nivel actual, Rusia puede alcanzar el primer puesto por cantidad de hostings maliciosos ya el próximo año.

En Holanda y Alemania los delincuentes actúan con mucho más cuidado: registran o hackean una gran cantidad de sitios y cuando las direcciones de éstos aparecen en las listas negras de los proveedores, de inmediato trasladan el contenido malicioso a otros servidores.

Amenazas locales

Un factor de primordial importancia es la estadística de las infecciones locales que afectan a los equipos de los usuarios. Aquí se reflejan los datos de los objetos que penetraron en los equipos sin usar la Web, el correo electrónico o los puertos de red.

Nuestras soluciones antivirus detectaron más de tres mil millones de incidentes virales en los equipos que integran Kaspersky Security Network.

En estos incidentes se pudo registrar 112.474 diferentes programas nocivos y potencialmente indeseables.

Programas maliciosos detectados en los ordenadores de los usuarios: Top 20

Los programas maliciosos que integran el primer TOP 20 son las amenazas más propagadas de 2012.

Puesto	Objeto detectado	Cantidad de usuarios únicos	%%
1	Trojan.Win32.Generic	9,761,684	22.1%
2	DangerousObject.Multi.Generic	9,640,618	21.9%
3	Trojan.Win32.AutoRun.gen	5,969,543	13.5%
4	Trojan.Win32.Starter.yy	3,860,982	8.8%
5	Virus.Win32.Virut.ce	3,017,527	6.8%
6	Net-Worm.Win32.Kido.ih	2,752,409	6.2%
7	Net-Worm.Win32.Kido.ir	2,181,181	4.9%
8	Virus.Win32.Sality.aa	2,166,907	4.9%
9	Hoax.Win32.ArchSMS.gen	2,030,664	4.6%
10	Virus.Win32.Generic	2,017,478	4.6%
11	Virus.Win32.Nimnul.a	1,793,115	4.1%
12	HiddenObject.Multi.Generic	1,508,877	3.4%
13	Trojan.WinLNK.Runner.bl	1,344,989	3.1%
14	Worm.Win32.AutoRun.hxw	948,436	2.2%
15	Virus.Win32.Sality.ag	841,994	1.9%
16	Virus.Win32.Suspic.gen	408,201	0.9%
17	Trojan.Win32.Patched.dj	367,371	0.8%
18	Email-Worm.Win32.Runouce.b	295,887	0.7%
19	Trojan-Dropper.Script.Generic	232,007	0.5%
20	AdWare.Win32.GoonSearch.b	196,281	0.4%

La presente estadística contiene los veredictos de detección del módulo del antivirus web que enviaron los usuarios de los productos de Kaspersky Lab que dieron su consentimiento para el envío de datos estadísticos.
** Cantidad de usuarios únicos en cuyos equipos el antivirus detectó este objeto.*

En 13,5 millones de equipos se bloquearon intentos de infección detectados mediante diferentes métodos heurísticos: Trojan.Win32.Generic (primer puesto), Virus.Win32.Generic (octavo puesto), HiddenObject.Multi.Generic (puesto 12), Trojan-Dropper.Script.Generic (puesto 19).

El segundo puesto de la estadística lo ocupan diferentes programas maliciosos detectados mediante tecnologías “en la nube” y detectados como DangerousObject.Multi.Generic. Estas tecnologías se activan cuando en las bases antivirus todavía no existen firmas ni heurísticas que detecten el programa malicioso, pero la compañía antivirus ya tiene información sobre el objeto "en la nube". De hecho, esta es la forma en que se detectan los programas maliciosos más nuevos. Gracias al sistema de detección instantánea de amenazas UDS, que es parte de Kaspersky Security Network, más de 9.600.000 equipos gozaron de protección en tiempo real.

Ocho integrantes del TOP 20 tienen mecanismos de autopropagación o se usan como uno de los componentes en el esquema de propagación de gusanos: Trojan.Win32.Starter.yy (cuarto puesto), Net-Worm.Win32.Kido.ih (sexto puesto), Net-Worm.Win32.Kido.ir (séptimo puesto), Virus.Win32.Sality.aa (octavo puesto), Virus.Win32.Nimnul.a (puesto 11), Virus.Win32.Sality.ag (puesto 15) y Virus.Win32.Suspic.gen (puesto 16).

En 2012 más de dos millones de usuarios se toparon con estafas que usaban números SMS cortos (Hoax.Win32.ArchSMS.gen, noveno puesto). Bajo diferentes pretextos, sobre todo prometiendo acceso al contenido de un archivo o un instalador de juegos, programas, libros o cosas similares, los delincuentes tratan de obligar a los usuarios a enviar SMS a números premium cortos. En la mayoría de los casos, después de enviar el mensaje, el usuario no recibe nada a cambio.

Trojan.WinLNK.Runner.bl (puesto 13) y Worm.Win32.AutoRun.hxw (puesto 14) son detecciones de ficheros lnk (accesos directos) maliciosos. En los ficheros lnk de estas familias se ejecuta cmd.exe con los parámetros de lanzamiento de un fichero exe malicioso. Los gusanos los usan activamente para propagarse mediante memorias usb.

Trojan.Win32.Patched.dj (puesto 17) es interesante. Se trata de una detección de ficheros exe y dll infectados.

Su funcionalidad maliciosa se reduce a enviar por correo al creador de virus información sobre la infección, para después abrir un puerto en el equipo y quedar a la espera de instrucciones del hacker, que a su vez puede descargar ficheros, ejecutarlos, detener programas lanzados en el equipo, etc. Al final, el programa malicioso se usa para construir una botnet.

Los métodos de infección evolucionan activamente y hoy en día vemos que ninguna nueva familia ha entrado

en el TOP 20: aquí dominan Sality, Virut, Numnul (el del año pasado) y Kido. Los delincuentes informáticos han dejado sus métodos anteriores para usar de forma masiva botnets mediante infecciones por Internet con el uso de exploits. Las técnicas de infección de ficheros ejecutables no gozan de popularidad entre los creadores de virus orientados a los negocios, debido a que es muy difícil controlar el proceso de autopropagación de virus y gusanos, y las grandes botnets no tardan mucho en atraer la atención de la policía.

"Un cuadro del mundo"

Para calcular en qué países los usuarios se topan con más frecuencia con las amenazas cibernéticas, hemos contado para cada país la frecuencia con que durante el año los usuarios observaron activaciones del programa antivirus. Los datos obtenidos caracterizan el nivel de riesgo de infección de los ordenadores en diferentes países del mundo y son una muestra de la agresividad del entorno en que funcionan los ordenadores en diferentes países.

Amenazas web

El riesgo de infección por Internet, que es la principal fuente de objetos maliciosos para los usuarios de la mayoría de los países, es el índice que representa mayor interés.

Puesto	País	% de usuarios únicos**
1	Federación Rusa	58.6
2	Tayikistán	58.5
3	Azerbaiyán	57.1
4	Armenia	55.7
5	Kazajistán	55.5
6	Bielorrusia	51.8
7	Bangladesh	51.7
8	Sri Lanka	51.5
9	India	51.1
10	Sudán	51.0
11	Turkmenistán	51.0
12	Omán	48,0
13	Uzbekistán	47.5
14	Malasia	47.3
15	Moldavia	47.2
16	Maldivas	46.8
17	Ucrania	46.8
18	Italia	45.6
19	Estados Unidos	45.1
20	España	44.7

*La presente estadística contiene los veredictos de detección del módulo del antivirus web que enviaron los usuarios de los productos de Kaspersky Lab que dieron su consentimiento para el envío de datos estadísticos. *En los cálculos hemos excluido a los países en los cuales la cantidad de usuarios de los productos de Kaspersky Lab es relativamente pequeña (menos de 10.000).*
***Porcentaje de usuarios únicos que fueron víctimas de ataques web, de entre todos los usuarios únicos de los productos de Kaspersky Lab en el país.*

Por segundo año consecutivo Rusia lidera la presente estadística. Para los usuarios rusos, este año el riesgo durante la navegación en Internet ha crecido del 55,9% hasta el 58,6%. Por desgracia, en el sector ruso de Internet se usa una gran cantidad de esquemas de delincuencia informática. Debido a que entre los usuarios privados y los empresarios está creciendo la popularidad de la banca en Internet, en 2012 los delincuentes informáticos propagaron activamente los programas maliciosos correspondientes. Otro tipo de estafa que con frecuencia se encuentra en el sector ruso de Internet es la monetización con el uso de SMS de pago: los estafadores piden al usuario que pague por compras o servicios mediante SMS, pero éste no recibe nada de lo prometido.

Tayikistán ha subido del puesto 17 al 2 con un índice del 58,5%. En el tercer puesto está Azerbaiyán, que subió del sexto puesto con el 57,1% de usuarios atacados.

Italia, EE.UU. y España han ocupado los últimos tres lugares del TOP20 de países del 2012.

EE.UU. que según los resultados de 2011 ocupó el tercer puesto, en 2012 bajó de golpe al 19: la cantidad de usuarios atacados en este país se redujo del 50,1% al 45,1%. Esto está condicionado por el éxito de la lucha contra la delincuencia informática y la clausura de varias grandes botnets, entre ellas DNSChanger, Hlux y varias ZeuS (Zbot).

Italia y España han entrado por primera vez en el TOP 20 de países por la cantidad de usuarios atacados mientras navegaban en Internet. En estos países la cantidad de incidentes por usuario ha sido bastante grande durante todo el año, lo que, en primer lugar, está relacionado con los ataques de los troyanos bancarios.

Todos los países del mundo se pueden distribuir según el grado de riesgo de infección durante la navegación por Internet.

1. **Grupo de alto riesgo**
   En este grupo, con resultados de41-60%, han ingresado 31 países. Además de los países del TOP 20, también han ingresado Australia (44,4%), Indonesia (44,2%), Canadá (42,8%), Georgia (42,3%) e Inglaterra (41,1%).
2. **Grupo de riesgo**
   En este grupo, con índices del21-40%, han ingresado 110 países, entre ellos Turquía (39,9%), Francia (39,8%), Chile (39,4%), China (38,4%), Polonia (37,1%), Letonia (35,3%), Suecia (34,1%), Austria (34%), Ecuador (33,3%), Alemania (31,8%), Finlandia (27,9%), Noruega (27,3%), Japón

(22,8%) y Dinamarca (21,6%).

3. **Grupo de países más seguros para navegar en Internet** (0-20%)
   En 2012 han entrado en este grupo 10 países: Gabón (20,6%), Togo (20,5%), Reunión (20,2%), Nigeria (19,6%), Mauricio (18%), Guadalupe (17,8%), Martinica (17,7%), Benín (17,2%), Burundi (16,9%) y Congo (16,7%).

El primer grupo ha aumentado en 8 países. La mayor parte del grupo son países del espacio postsoviético y de Asia. Es una pena que haya aumentado la cantidad de países europeos en este grupo.

Del grupo de países de navegación segura en Internet han salido todos los países europeos, y ahora sólo quedan países de África. Hacemos notar que los países que se sumaron al grupo de países de navegación segura en Internet, estaban en los grupos de nivel de infección alta y máxima por el número de infecciones locales. El que estén en el grupo de países de navegación segura en Internet se explica por el carácter de propagación de ficheros en estos países: como en ellos Internet no está muy desarrollado, los usuarios usan diferentes tipos de memorias extraíbles para compartir información. Como resultado, en estos países nuestros radares casi no registran amenazas web, pero sí una gran cantidad de virus y gusanos que se difunden mediante memorias USB e infectan ficheros.

En promedio mundial, el nivel de peligrosidad de Internet sigue creciendo por segundo año consecutivo y según los resultados de 2012, constituye el 34,7%, un 2,4% más que el año pasado. Uno de cada tres usuarios de Internet en el mundo sufre un ataque informático por lo menos una vez al año.

Amenazas locales

Además de las infecciones a través de la web, representan interés los datos sobre los programas maliciosos detectados directamente en los ordenadores de los usuarios o en las memorias extraíbles conectadas a los mismos: memorias USB, tarjetas de memoria de cámaras fotográficas, teléfonos y discos duros externos. En esencia, esta estadística refleja el nivel de infección de los ordenadores personales en diferentes países del mundo.

Puesto	País	%*
1	Bangladesh	99.7
2	Sudán	88.2
3	Malawi	78.0
4	Tanzania	77.4
5	Ruanda	76.5
6	Afganistán	75.6
7	India	75.2
8	Laos	73.3
9	Nepal	72.9
10	Angola	72.0
11	Vietnam	70.4
12	Mauritania	69.8
13	Iraq	69.6
14	Maldivas	69.2
15	Uganda	69.0
16	Sri Lanka	68.5
17	Mongolia	68.0
18	Yibuti	67.4
19	Mali	67.3
20	Costa de Marfil	67.0

*La presente estadística contiene los veredictos de detección del módulo del antivirus web que enviaron los usuarios de los productos de Kaspersky Lab que dieron su consentimiento para el envío de datos estadísticos. *En los cálculos hemos excluido a los países en los cuales la cantidad de usuarios de los productos de Kaspersky Lab es relativamente pequeña (menos de 10.000).*
***Porcentaje de usuarios únicos en cuyos ordenadores se detectaron amenazas locales, de entre la cantidad total de usuarios de productos de Kaspersky Lab en el país.*

El TOP 20 de 2012 está formado por países de África y Asia. La situación en los países líderes de la estadística no ha mejorado. Como hace un año, en Sudán y Bangladesh, 9 de cada 10 ordenadores se toparon por lo menos una vez con infecciones traídas por programas maliciosos. Todavía no está desarrollada la cultura de utilizar antivirus y el poco conocimiento de los usuarios sobre las posibles amenazas informáticas hace que los ordenadores en estos países sean vulnerables a los programas maliciosos.

En el caso de las amenazas locales también podemos poner los países en diferentes categorías.

1. **Nivel máximo de infección (más del 75%):** 7 países de Asia y África, entre ellos India (75,2%) y Bangladesh (99,7%), que también estaban en el grupo de alto riesgo de navegación en Internet.
2. **Nivel de infección alto (56-75%):** 41 países, entre ellos Indonesia (64,7%), Etiopía (58,2%) y Kenia (58%).
3. **Nivel de infección medio 35-55%:** 67 países, entre ellos China (52,7%), Kazajistán (52,6%), Rusia (48,7%), Turquía (48,67%), Brasil (43,5%), Corea del Sur (39,8%), España (39,8%), Portugal (35,8%) y Letonia (35,7%).
4. **Nivel de infección mínimo** (0-35%)**:** 38 países. Entre ellos están EE.UU. (33,3%), Francia (32,8%), Inglaterra (30,9%), Letonia (31,4%) y Bélgica (27,2%). La cantidad de países que integran este grupo en comparación con 2011 ha crecido 2,7 veces, ya que el año pasado tenía sólo 14 países. En primer lugar los cambios están relacionados con la progresiva extinción de los virus clásicos y los gusanos de autoinicio.

TOP 10 de países con porcentaje mínimo de ordenadores infectados:

Puesto	País*	%
1	Dinamarca	15.0
2	Japón	19.5
3	Finlandia	19.8
4	Suecia	22.9
5	República Checa	23.5
6	Países Bajos	23.9
7	Noruega	24.0
8	Luxemburgo	24.2
9	Alemania	24.3
10	Suiza	24.4

En el grupo de los países más seguros, sufrieron ataques un promedio del 25,4% de los ordenadores de los usuarios. En comparación con el año pasado, este índice bajó en 4 puntos porcentuales.

Conclusión

2012 ha sido el año en que los delincuentes informáticos han empezado a experimentar un gran interés por nuevas plataformas, sobre todo por Mac OS X y Android OS. La posibilidad de infectar con facilidad una gran cantidad de equipos y dispositivos de los usuarios siempre ha atraído a los delincuentes y por eso está en crecimiento la cantidad de ataques contra los usuarios de Mac y Android.

A principios de año se descubrió una enorme botnet de 700.000 ordenadores Mac creada por el programa Flashfake. Los delincuentes podían instalar módulos maliciosos adicionales en los equipos infectados. Se sabe que uno de los módulos se ocupaba de suplantar el tráfico en el navegador. Pero los ataques masivos no fueron los únicos que afectaron a Mac. Durante todo el año hemos venido detectando ataques dirigidos a blancos específicos mediante backdoors que tenían como blanco a los usuarios de Mac OS X. Esta tendencia se reflejó en nuestras cifras: la cantidad de firmas antivirus para Mac OS X creció en un **30%** en comparación con2011.

La epidemia del troyano para Mac y la serie de malware para Android hizo que el asunto de la protección de las nuevas plataformas cobrara especial actualidad. La necesidad de esta protección se hizo evidente para la mayoría de la población de Internet en el planeta. Los mitos sobre la invulnerabilidad de Mac ante los virus se derrumbaron. Los fabricantes empezaron a prestar más atención a la defensa de las plataformas: en la nueva versión de Mac OS X se implementaron varias funciones que mejoraban la seguridad, mientras que por su parte Google organizó el escaneado de las aplicaciones agregadas a su tienda. La industria antivirus, que estaba lista ante estos avatares, desde hace cierto tiempo ofrece soluciones como Kaspersky One, dirigidas a la protección de una serie de dispositivos, desde PC y Mac hasta teléfonos y *tabletas*.

Por desgracia, a pesar de los éxitos en la lucha contra la delincuencia cibernética, en 2012 el porcentaje de usuarios atacados en Internet ha seguido creciendo y alcanzó el 34%. Ningún país europeo ha entrado en el grupo de países en el que el porcentaje de usuarios atacados durante su navegación en Internet sea menor al 20%.

Si bautizamos 2011 como “el año de las vulnerabilidades”, podemos llamar con tranquilidad a 2012 “el año de las vulnerabilidades Java”. Según nuestra estadística, la mitad de los ataques mediante exploits en 2012 corresponde a las vulnerabilidades de Java. Y es importante el hecho de que los delincuentes usaron vulnerabilidades tanto durante ataques masivos, como en ataques contra blancos específicos y los exploits funcionaron tanto contra PC como contra Mac.

Fuente:
- Kaspersky Lab

Correo electrónico: webmaster@viruslist.com