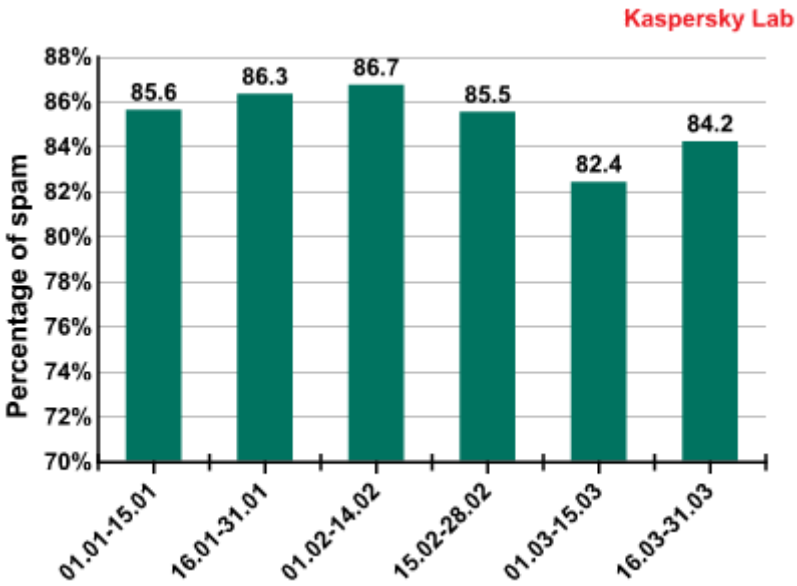
Estudio realizado por Kaspersky Lab.

La evolución del Spam: enero-marzo 2010

Tendencias recientes:

- En el primer trimestre, el porcentaje de spam en el correo electrónico de tráfico promedio de 85,2%.
- Enlaces a sitios de phishing se encuentra en el 0,57% de todo el tráfico electrónico.
- accesorios gráfica figuran en el 11,7% de todos los mensajes de spam.
- Los tres principales fuentes de spam incluidos los EE.UU., India y Rusia.
- Los spammers transferido dominios de la zona cn. A la zona ru.

El spam en el tráfico de correo



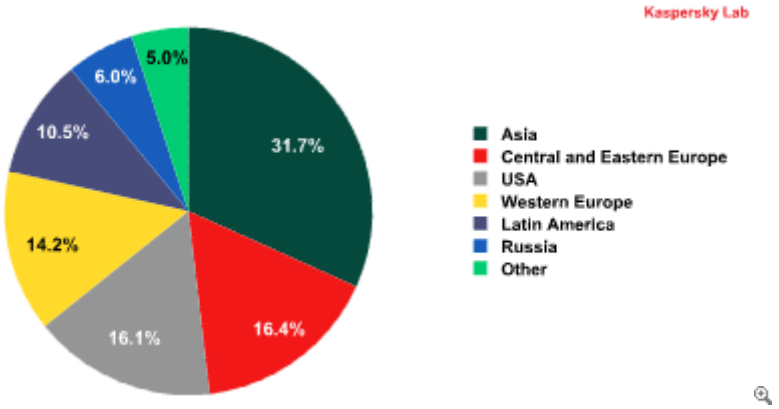
El spam en el tráfico de correo

En el primer trimestre de 2010, el porcentaje de spam en el correo electrónico de tráfico promedio de 85,2%. Esta cifra coincide con el resultado final para 2009. La primera quincena de marzo registró un descenso considerable en la cantidad de spam. Esto podría haber sido causado por el cierre de 277 dominios que pertenecen a la botnet Waledac spammer al final de febrero . Sin embargo Waledac no es el jugador más activo en el mercado de spam y por lo tanto probablemente no es la causa de tal descenso notable en la cantidad de spam, al contrario que en el caso de McColo.

Ya hemos mencionado la formación del mercado de spam en nuestros informes anteriores. Ahora podemos pasar a hablar de estabilización en la cantidad de spam en el tráfico postal, que se mantiene prácticamente sin cambios, fluctuando en algún lugar entre 84-87%. La tendencia a la baja de spam del año pasado el tráfico de correo se desprende de este año también, lo que significa un porcentaje de este tipo de spam está cerca de sus figuras máximas. Un elevado de 90,8% se registró el 21 de febrero, con una baja de 78% el 5 de marzo.

Fuentes de spam

Fuentes de spam por región

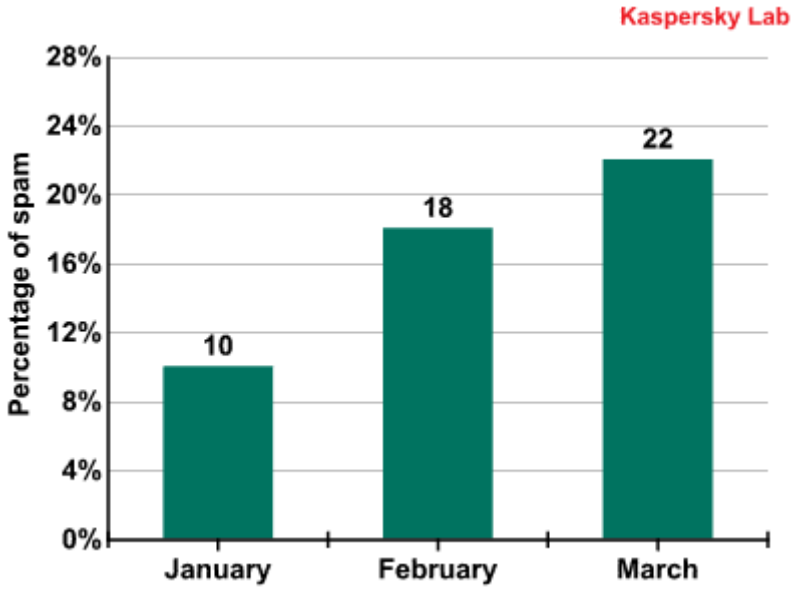


Fuentes de spam por región

Asia sigue siendo la principal fuente de spam, ya que el año pasado (31,7%). Europa no se queda atrás - con un 30,6% del spam que se distribuye desde su territorio. Si combinamos Rusia con el resto de Europa, esta región entonces tomaría la iniciativa, con un 36,6%.

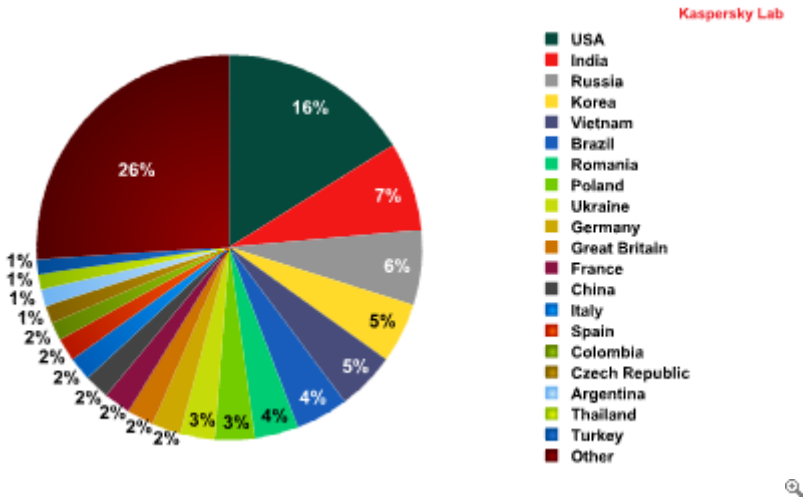
La cantidad de spam se distribuye desde América del Sur ha disminuido. En el primer semestre de 2009 alcanzó el 15% y quedó en segundo lugar. En la actualidad América del Sur salidas del 10,5%, que fue cerca de su figura 2008 (11%).

Al mismo tiempo, la cantidad de spam distribuido de Europa del Este ha aumentado (16,4%). Es fácil seguir la dinámica de crecimiento en la cantidad de spam enviado desde esta región en el primer trimestre de 2010:



Spam distribuye desde el territorio de Europa central y oriental: la dinámica del crecimiento

Fuentes de spam por país



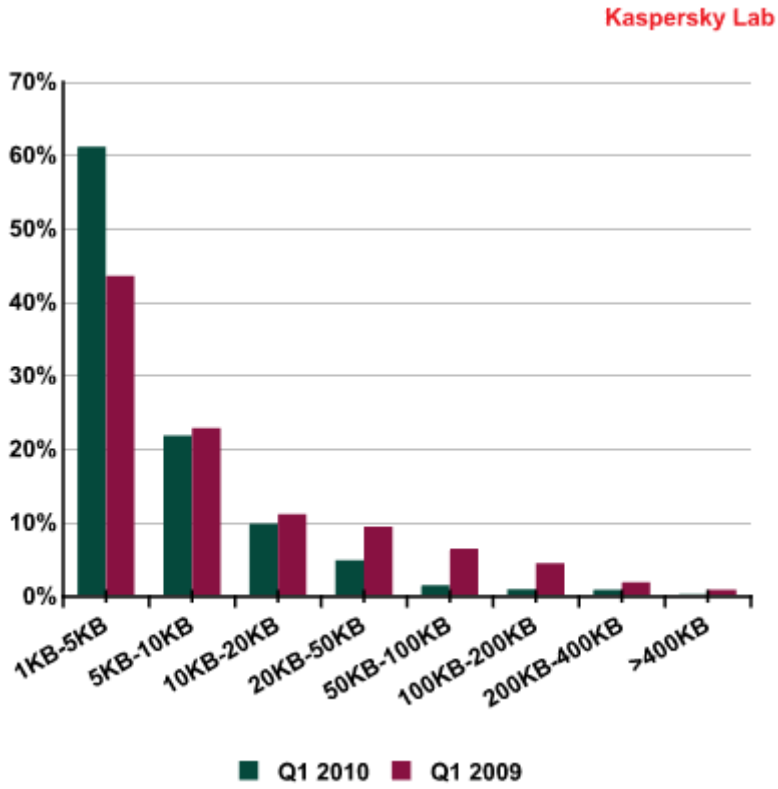
Fuentes de spam

No hay grandes cambios en las fuentes de la calificación de spam - no hay líderes inesperado aparecido. Los EE.UU. mantuvo su posición en la parte superior, con la India y Rusia viene segundo y tercero. Ellos fueron seguidos principalmente por los países del Este de Asia y Europa del Este. Casi todos los participantes anteriores se mantuvo en el Top 10, se limita a intercambiar lugares.

La situación en Brasil mejoraron significativamente: se bajó del tercer al sexto lugar. Turquía y China abandonó el Top 10. Con China, esto puede haber sido causada por un endurecimiento de la política del gobierno de registro de dominios. Ucrania y Alemania, en cambio, volvió a entrar en el Top 10 de nuevo. En 2008, han estado siempre entre los distribuidores de spam diez primeros, pero en 2009 no pudieron mantener sus posiciones.

Cabe señalar que el idioma en el que el spam es distribuido a partir de un determinado país a menudo no refleja el idioma oficial de ese país. Por ejemplo, una gran cantidad de spam en ruso viene de la India, mientras que Brasil se extiende una gran cantidad de spam en alemán y hay un montón de correo basura que sale de Alemania que está en español. Esto ocurre porque el lenguaje de spam no se define por la localización geográfica de la propiedad intelectual. Se define por la botnet que los equipos pertenecen.

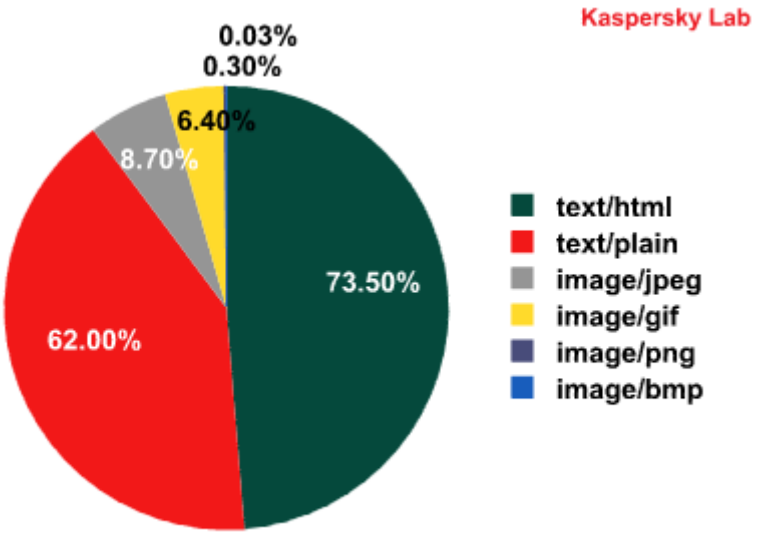
Tamaño de mensajes de spam



Tamaño de mensajes de spam

Los spammers prefieren enviar correos electrónicos pequeños, a menudo no superior a 1 KB. Esto puede ser fácilmente explicada por el hecho de que dichos correos electrónicos contienen un único enlace, lo que crea dificultades para los filtros de contenido orientado a la detección de ellos. Además, se necesitan menos recursos para distribuir dicho "ligero", mensajes de correo electrónico. Además, la mayoría de los usuarios actuales y elimine inmediatamente un correo electrónico si lo ven es spam. Es por eso que los spammers tratan de encapsular la información de publicidad en una frase, de modo que un usuario tendrá tiempo de leerlo antes de que se presione el botón "Borrar". En el primer trimestre de 2010 el porcentaje de correos electrónicos pequeños promedio un tercio de la cantidad total de spam (31,3%). Los correos electrónicos de más de 50 KB de tamaño representaron sólo el 2,9% de todo el spam en el 1er trimestre de 2010.

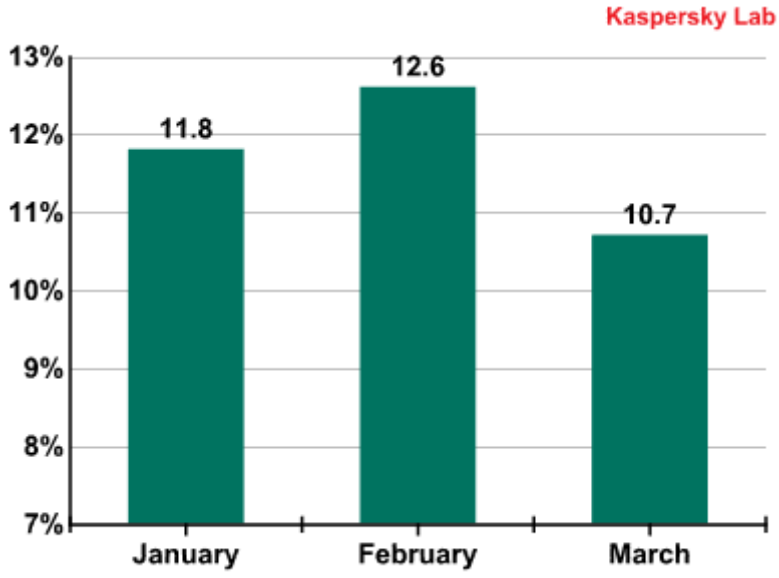
Tipos de archivos adjuntos en los correos electrónicos de spam malicioso



Tipos de archivos adjuntos en los correos electrónicos de spam malicioso

En el primer trimestre de 2010 la mayoría de mensajes de correo electrónico contiene un adjunto en formato HTML. Notablemente, más pequeño correo electrónico con un adjunto en formato HTML pueden contener sólo un enlace. Los mensajes con archivos adjuntos en formato jpeg se encontraron en el 8,7% de todos los correos spam y el 6,4% para el formato gif. Algunos mensajes de correo electrónico que figura tanto en formato JPEG y GIF en un elemento: el contenido del mensaje fue en formato jpeg, mientras que el darse de baja forma fue en gif.

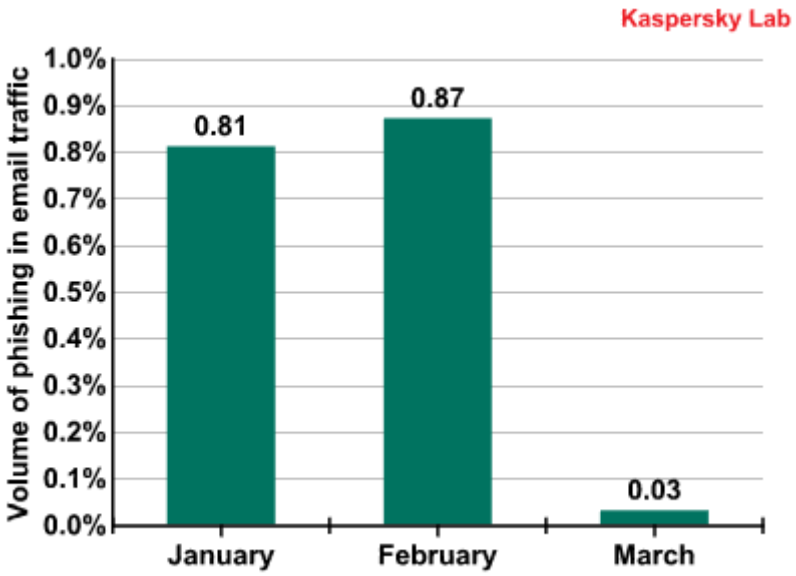
La cantidad total de spam gráfico (mensajes con imágenes) de media el 11,7% de todos los correos spam. La mayoría de los mensajes que contengan imágenes se distribuyeron en febrero.



Los correos electrónicos con archivos adjuntos gráfica

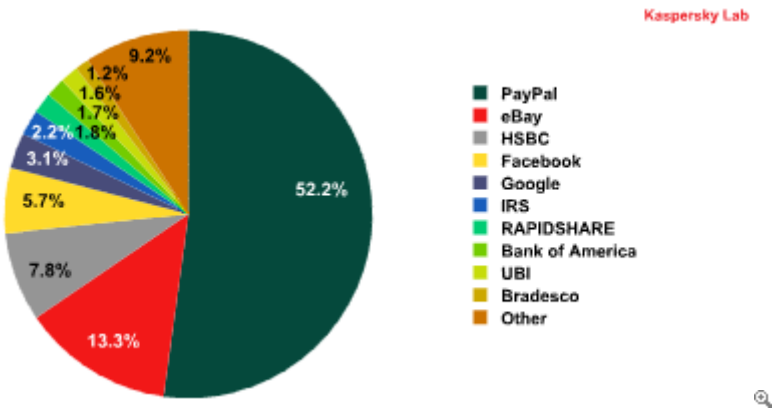
Phishing

En el primer trimestre de 2010 enlaces a sitios de phishing se encuentra en el 0,57% de todo el tráfico electrónico. En enero y febrero, la proporción de correos electrónicos de phishing casi igualó la cifra del año anterior, mientras que en marzo disminuyeron drásticamente y un promedio de sólo 0,03% de todo el tráfico electrónico. No es fácil explicar este hecho, pero vamos a ver cómo evoluciona la situación.



Los correos electrónicos que contienen enlaces a sitios de phishing

Una vez más, el objetivo más atractivo para los phishers se PayPal, quedando en el extremo receptor de más de la mitad de todos los ataques de phishing durante el primer trimestre de 2010. El segundo lugar, como era de esperar, cayó a eBay con el 13,3%.



Las 10 organizaciones blanco de ataques de phishing

Facebook apareció inesperadamente en el cuarto lugar. Esta fue la primera vez desde que comenzamos a monitorear que los ataques a un sitio de redes sociales han sido tan prolíficos. Actualmente, Facebook es uno de los sitios de redes sociales más populares con más de 400 millones de usuarios y su número está en constante crecimiento. Después de haber robado las cuentas de usuarios, a continuación, los estafadores pueden usar para distribuir spam, el envío de correos electrónicos masivos a los propietarios de cuentas y sus amigos en la red. Este

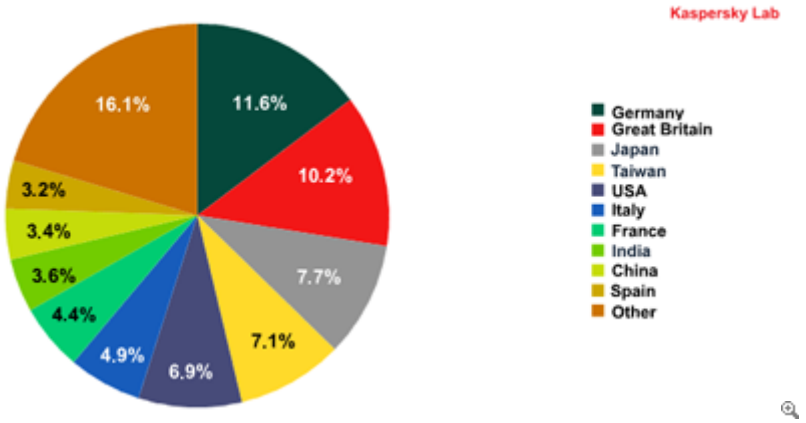
método de distribución de correo no deseado permite a enormes audiencias que se alcance. Además, permite que los defraudadores aprovechan de las opciones de los sitios de redes sociales adicionales, como ser capaz de enviar peticiones diferentes, enlaces a fotos y las invitaciones, todos con el anuncio adjunto, tanto dentro de la red y las bandejas de entrada de los usuarios. Asimismo, si bien el registro de usuarios de cuentas de introducir sus datos (por ejemplo, una dirección de correo electrónico) que los spammers pueden agregar a sus bases de datos.

Curiosamente, en marzo, la red social de Rusia se llevó a cabo Vkontakte 25a entre las organizaciones dirigidas por los ataques de phishing. Esta red ha superado los límites del sector ruso de Internet y sigue creciendo.

Los mensajes con archivos adjuntos maliciosos

Durante el primer trimestre de 2010 archivos maliciosos se encuentran en el 0,68% del total del tráfico de correo, un descenso del 0,3% con respecto al último trimestre de 2009.

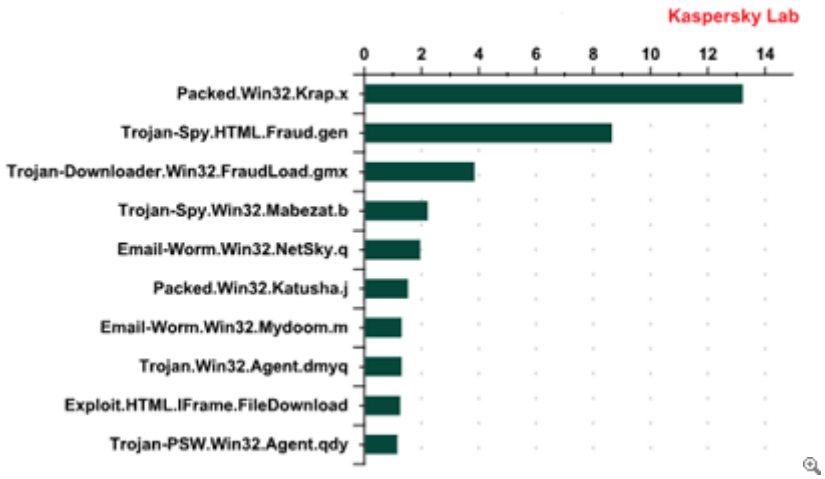
La distribución geográfica de los intentos de infectar las computadoras de los usuarios a través de correo electrónico se puede ver en el siguiente gráfico:



Informática infección por la geografía

Más del 35% de los mensajes recibidos por los usuarios en Alemania, el Reino Unido, Italia, Francia y España (es decir, los países de la zona UE) contenía archivos adjuntos maliciosos. Japón recibió el 7,6% de todos los correos electrónicos infectados y el 13% se enviaron a otros países asiáticos, como Taiwán, India y China. Cerca del 7% de los mensajes maliciosos llegado a sus destinatarios EE.UU..

En el primer trimestre de 2010, el Top 10 ficheros maliciosos más populares que se encuentran en el tráfico postal ha sido el siguiente:



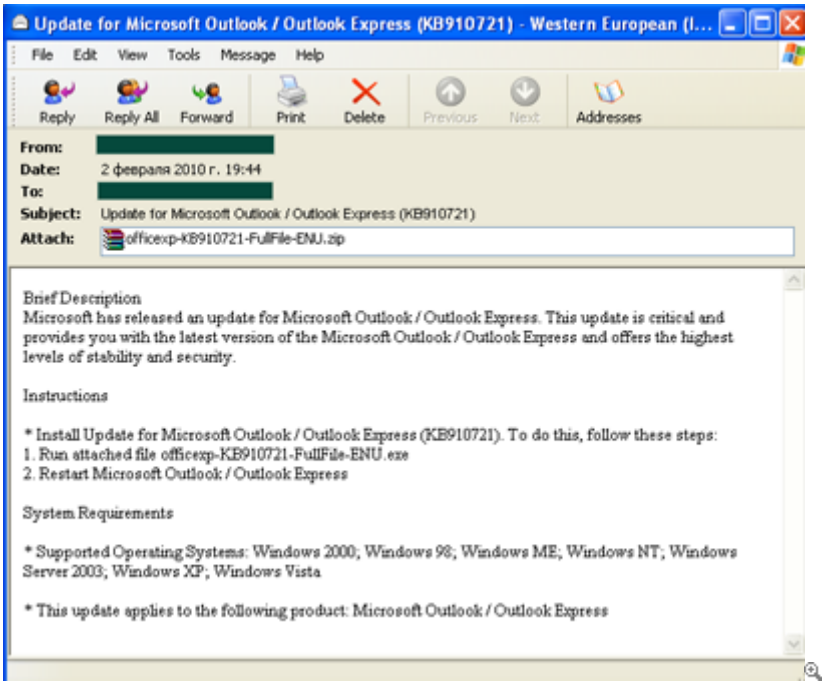
Top 10 más populares archivos maliciosos en el tráfico postal

En primer lugar está el Packed.Win32.Krap.x envasador. En el trimestre anterior que fue cuarto en la clasificación. A principios de 2010 Krap.x fue encontrado en mensajes de correo electrónico dos veces más que a finales de 2009. Este no es el envasador sólo en la calificación. Packed.Win32.Katusha.j (sexto lugar) es de hecho un representante de la nueva generación de Packed.Win32.Krap.ah, el programa de más amplia distribución en el último trimestre.

En general, Krap.ah (Katusha.j) y Krap.x se emplean para embalar el troyano espía y otros programas Zbot falso antivirus. Además Krap.x es un empaquetador de Iksmas, un gusano de correo con la función integrada de robo de datos y distribución de spam.

Curiosamente, más del 55% de todos los mensajes de correo electrónico con un archivo adjunto que contiene Packed.Win32.Krap.x fueron enviados a los países desarrollados, entre ellos el 16,7% a Japón, el 12,7% a Alemania y cerca del 8% a los Estados Unidos.

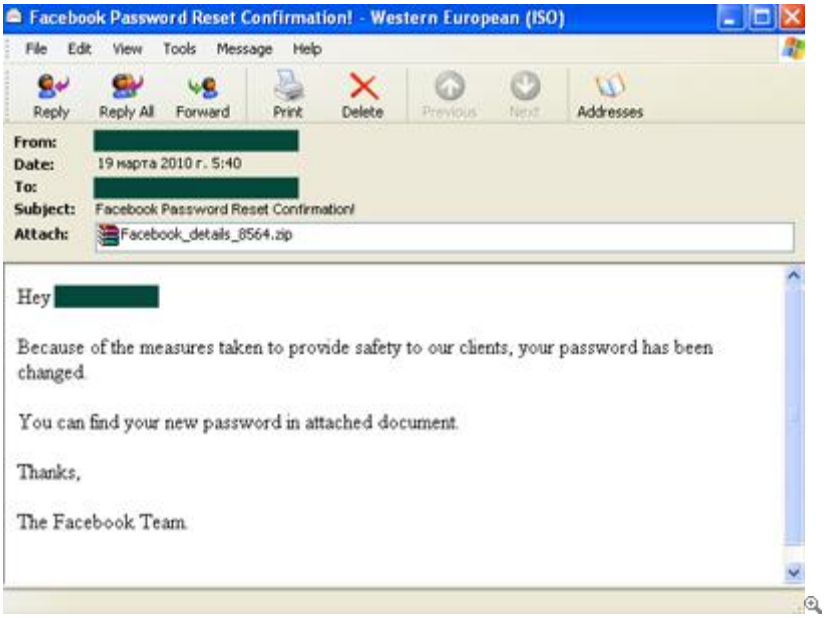
Los programas maliciosos incluidas con la ayuda de Krap.x también se distribuyeron en los correos electrónicos que ofrecen a los usuarios la posibilidad de instalar una actualización de Microsoft Outlook.



El segundo lugar en el Top 10 va a Trojan-Spy.HTML.Fraud.gen . Esta pieza de malware está diseñado para recopilar datos de los usuarios de registro personal y. En enero y marzo de 2010 este programa malicioso liderado el campo del malware distribuido por correo electrónico.

muestras de más de 70% de los Trojan-Spy.HTML.Fraud.gen (al igual que Packed.Win32.Krap.x) malware encontrado se encuentra en los países desarrollados, entre ellos el 39% detectado en el Reino Unido.

Trojan-Downloader.Win32.FraudLoad.gmx se encuentra en tercera posición. Este troyano descarga otros programas maliciosos en la computadora de un usuario, por ejemplo programas antivirus deshonestos diseñado para extorsionar a su víctima. Este troyano fue más a menudo a los usuarios en su idioma oficial es el Inglés - en el Reino Unido, EE.UU., Australia y Canadá. Más de la mitad de todas las muestras Trojan-Downloader.Win32.FraudLoad.gmx detectamos procedían de esos países. En marzo fue especialmente activo en la mayor parte falsos correos electrónicos enviados en nombre de Facebook.



Migración de dominios spammer a la zona ru.

El año pasado, los spammers usan activamente los dominios chinos para implementar sitios de publicidad de Viagra, o que contienen otros tipos de ofertas spammer tradicionales. Los remitentes de spam distribuido grandes cantidades de spam que contienen enlaces a esos dominios. A finales de 2009, el gobierno chino endurecido su política en materia de registro de dominio en China. Esto provocó una considerable disminución de la cantidad de spam que contienen enlaces a dominios chinos. Por desgracia, el spam en sí no ha desaparecido y los dominios spammer han emigrado de la zona cn. A la zona ru..

Las actividades de las autoridades de China registró el cierre en marzo de dos importantes empresas chinas de registro de dominios, Go Daddy y Network Solutions. Esto se debía a la introducción de requisitos para algunos proveedores de dirección IP para proporcionar a los funcionarios chinos con documentos y fotografías que acrediten su identidad.

Conclusión

El comienzo de 2010 fue bastante tranquila para la industria del spam. La cantidad de spam en el tráfico postal dejado de crecer y durante el primer trimestre de 2010 no superaron las cifras del año pasado. Tomando las recientes tendencias de desarrollo en consideración, ya podemos hablar de la saturación del tráfico de correo con spam. Análisis demuestra que la proporción de spam en el tráfico postal ha seguido una curva parabólica en los últimos 10 años.

A principios de 2000, la proporción de spam duplicado cada año: 15% en 2001, 30-40% en 2002, el 50% a mediados de 2003 y 70-80% a finales de 2003. A finales de 2004, la industria del spam y se había formado un mayor crecimiento de su participación en el tráfico de correo lento: a continuación, durante el período 2004-2009 el incremento fue de 75% a 85%. Esto también puede ser causada por la aparición de nuevas plataformas de Internet para los spammers, como los blogs y redes sociales.

Aunque por lo general la cantidad de spam es estable, "migra" de región a región. Por ejemplo, en el primer trimestre de 2010 la cantidad de spam procedente de América Latina fallecido, mientras que más spam fue distribuido de Europa Central y Oriental.

Los spammers no se desarrollan nuevas tecnologías. Continúan utilizando pequeños mensajes que se pueden distribuir de forma rápida y en grandes cantidades.

Los estafadores y creadores de virus activamente aprovechar las tecnologías de spam, con los creadores de virus a través de redes sociales para distribuir sus programas maliciosos.

Cuando a finales de 2009, el gobierno chino reforzado su nombre de dominio política de registro, el contenido de spam migran desde la zona cn. A la zona ru.. Si las agencias de aplicación de la ley tanto en Rusia como en todo el mundo fueron más activas en la lucha contra este problema, habría muchos menos incidentes negativos resultantes de spam.