AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Estudio realizado por AV-TEST:
Correo basura (spam) peligroso

Correo basura, ahora más peligroso que nunca

Los spammer o personas que envían correos no deseados hacen uso de botnets para enviar millones de correos basura al día. El Instituto AV-TEST de Magdeburgo ha recopilado y analizado medio millón de correos basura, o spam en inglés, para un estudio que han llevado a cabo durante 18 meses: El peligro proveniente del correo basura es actualmente mayor que nunca.

Markus Selinger

Parece que el tema del correo basura se haya tranquilizado. Aunque sigue siendo pesado, nos hemos acostumbrado a ello. Y esto es lo que lo hace tan peligroso. En un estudio realizado durante 18 meses, entre agosto de 2011 y febrero de 2013, el laboratorio de AV-TEST ha recopilado medio millón de correos basura clasificados y los ha analizado. El resultado es decepcionante: Uno de cada tres correos basura con archivos adjuntos está infectado con un software malintencionado. Otros correos, por el contrario, intentan seducir al usuario a que visite una página web infectada.

Pero lo peor de todo es que el 25 % de los envíos de correos basura se realizan desde las oficinas, e incluso desde las alemanas.

Más de 500.000 correos basura sometidos a análisis de laboratorio

El Instituto AV-TEST ha analizado un total de 550.000 correos clasificados con anterioridad como correos basura. De ellos, casi 14.000 correos estaban infectados, lo que corresponde a casi el 2,5 %.

Los correos basura se recopilaron gracias a 90 cuentas de correo electrónico vigiladas. En parte, las direcciones de correo electrónico se inscribieron en foros y en concursos. Una vez preparado el estudio, tras una corta puesta en marcha, las cuentas de correo empezaron a recibir docenas de correos basura al día.

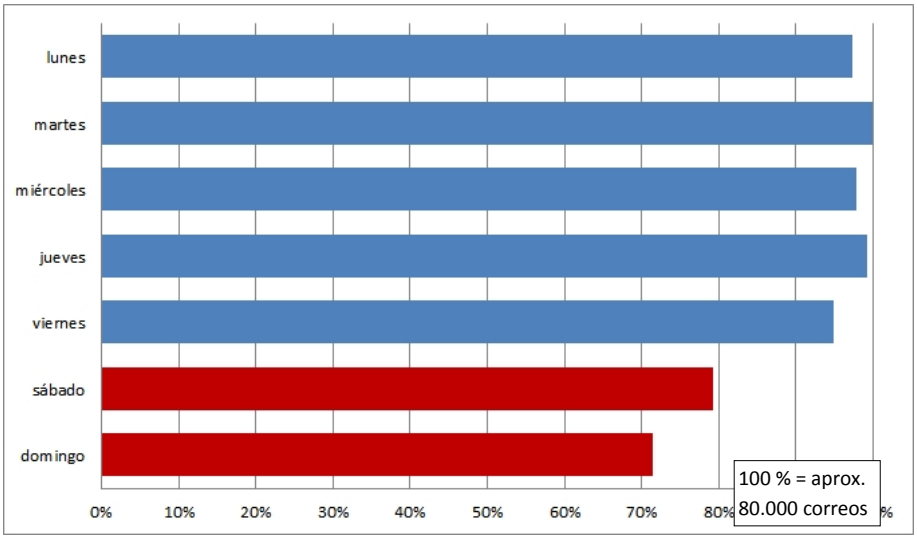
Muchos archivos adjuntos infectados

Por lo menos 30.000 correos basura de los 550.000 analizados tenían un archivo adjunto, de entre los que más de 10.000 estaban dotados de un componente malicioso, esto es más del 30 %. 400.000 correos contenían texto y también URL o enlaces a páginas de internet. En el caso de los correos con enlaces, casi el 1 % de éstos llevaban directamente a páginas infectadas con software malicioso. Las demás solían ser ofertas fraudulentas de productos falsificados, como pueden

Encontrará más información en:
www.av-test.org

En la página web de AV-TEST GmbH siempre encontrará información sobre la prueba, otros estudios y las estadísticas más actuales sobre spam y malware.

El 25 % de los envíos de correo basura se realizan desde las oficinas



Para realizar el estudio, se han registrado los correos basura obtenidos durante todos los días de la semana. El número máximo de correos al día alcanzó unos 80.000 correos electrónicos. El envío de correo basura de lunes a viernes siempre ha sido constante, y disminuye considerablemente durante el fin de semana. Esto demuestra que estos ordenadores, que se apagan durante los fines de semana, están en oficinas. Por lo que el 25 % de los ordenadores que envían correo basura desde botnets están en oficinas, incluso en las alemanas.

de ellos estaban infectados con software malicioso. Y si el correo electrónico provenía de la India, estaba infectado el 78 % de los archivos adjuntos recibidos durante el estudio. Seguido muy de cerca de los correos con archivos adjuntos provenientes de Vietnam: 77 %. La mitad de los 30.000 correos basura con archivos adjuntos registrados provenían de los EE UU, China, la India e incluso Alemania. Los correos basura con archivos adjuntos provenientes de Alemania no eran tan peligrosos: El 10 % de los correos venían acompañados de software malintencionado.

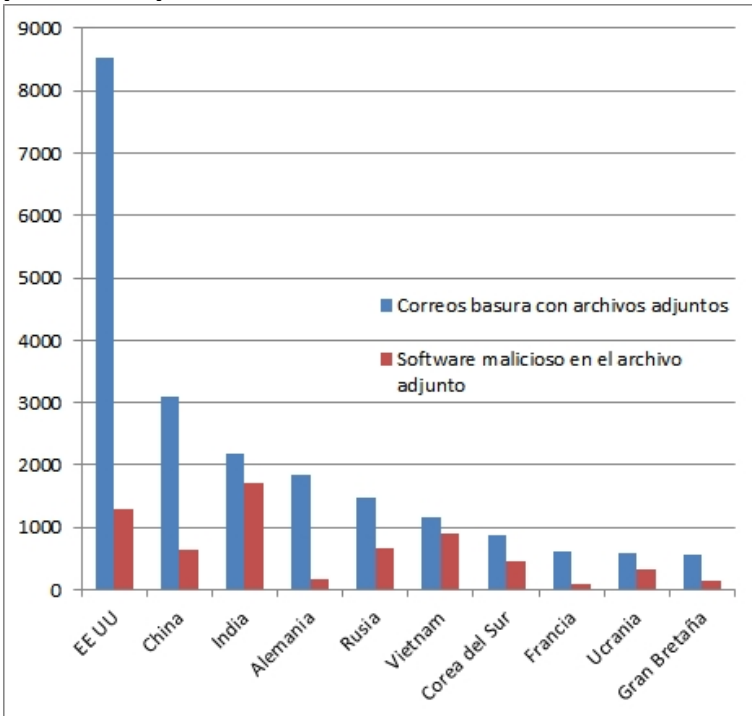
ser productos farmacéuticos.

Los archivos adjuntos infectados de los correos solían ser los que siempre son responsables de un ataque: archivos ZIP, archivos ejecutables EXE, COM, SCR, BAT y PIF y documentos HTML. También los archivos PDF y las fotos siguen siendo objetos infectados apreciados. El estudio ha demostrado que los correos basura con archivos ZIP estaban infectados casi al 100 %. Lo mismo ocurre con los archivos ejecutables EXE o PIF. Durante el estudio, más del 80 % de los documentos HTML adjuntos a los correos basura estaban infectados.

El spam de la India siempre es peligroso

Aunque la mayoría de correos basura con archivos adjuntos provienen de los EE UU, solo el 15 %

Correos electrónicos con archivos adjuntos según los países de procedencia



Aunque los EE UU era el país que ha enviado más correos basura con archivos adjuntos, si se compara con otros países, sus correos no solían venir acompañados de tantos componentes peligrosos. Mientras que los correos provenientes de la India o de Vietnam casi siempre venían acompañados de un software malintencionado. El 10 % de los correos basura con archivos adjuntos provenientes de Alemania solían estar infectados.

El 25 % de los envíos de correo basura se realizan desde las oficinas

En el estudio se registró el envío de correo basura durante cada uno de los días de la semana, y finalmente se analizaron los resultados transcurridos 18 meses. El resultado fue que de lunes a viernes, el nivel de correo basura enviado siempre ha sido constante. Y durante el fin de semana, sábado y domingo, el envío disminuye un 25 %. El estudio llega a la conclusión de que el 25 % de los envíos de correo basura se realizan desde las oficinas que cierran los fines de semana. Y el lunes vuelve a aumentar el nivel de correo basura.

Tras analizar los meses, no despuntó ninguno. Solamente se ha constatado que en julio y agosto la mayoría de los correos tenían la mayor tasa de infección. Pero no se ha podido reconocer ningún modelo.

Botnets: activas y traidoras

El envío de los correos basura se realiza casi exclusivamente desde ordenadores controlados de forma remota y discreta por botnets. De esta manera, los correos siempre llegan desde otra dirección IP. Por esta razón, los proveedores tienen dificultades a la hora de identificar rápidamente los correos sospechosos partiendo de su dirección IP.

Para el usuario, los ordenadores infectados con un troyano controlado son traicioneramente discretos. Pues el usuario no debe darse cuenta de que su ordenador está siendo usado para enviar correos. Existen botnets de distintos tamaños. Las redes que se han bloqueado en los últimos años estaban compuestas de 1 a 10 millones de ordenadores controlados. De los que no todos estaban siempre online. Pero, incluso con unos pocos cientos de miles de ordenadores se pueden enviar muchos correos basura en poco tiempo.

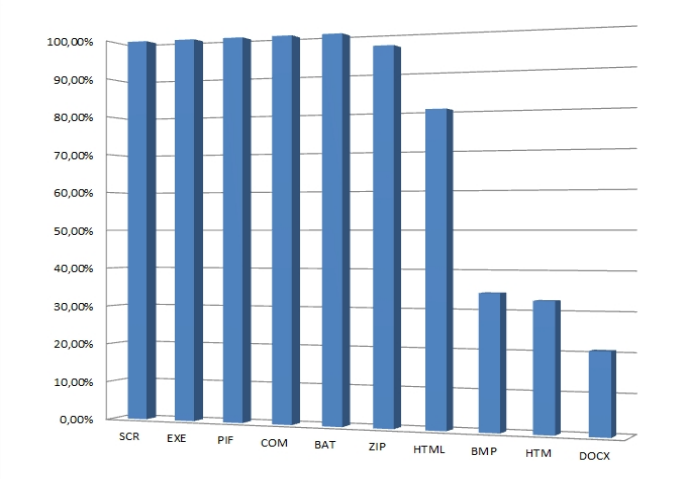
"¿Mi ordenador parte de una botnet?" ¡Realiza la prueba online!

La Oficina Federal para la Seguridad en colaboración con la Asociación de la Industria de Internet alemana ha puesto a disposición del público la página www.botfrei.de, donde encontrará numerosos enlaces de proveedores con los que podrá comprobar si su ordenador forma parte de una botnet.

Los software antivirus protegen

Si en un ordenador se hace uso de un paquete de seguridad actual, es casi imposible que sea controlado por una botnet hostil. Pues los paquetes de protección llevan incluido un escáner contra rootkits y troyanos, los cuales son las herramientas más apreciadas por los gestores de botnets. Encontrará las pruebas actuales de los paquetes de seguridad de forma gratuita en www.av-test.org

Los 10 archivos adjuntos infectados más populares



En el estudio se han contabilizado un total de 30 tipos diferentes de archivos adjuntos. Los cinco más populares demuestran que siempre que un correo basura lleva un archivo ejecutable, éste está infectado con un software malicioso.

Encuéntranos en facebook Síganos en twitter

Magdeburgo, 11 de abril de 2013
Autor: Markus Selinger

Si desea más información, póngase en contacto con el equipo de AV-TEST GmbH:
Correo electrónico: presse@av-test.de
Tlf.: +49 391 6075460
Página web: www.av-test.de