This translation is a joint initiative of MAAWG (www.maawg.org) and ITU (www.itu.int/ITU-D/cyb/cybersecurity).

Recomendación del MAAWG

Gestión del puerto 25 en el espacio de direcciones IP fijas o dinámicas Beneficios de la adopción de medidas y riesgos de la inacción

Introducción

Quienes envían correo basura (o *spammers*) y otros delincuentes cibernéticos utilizan cada vez más virus y programas espía ("spyware") como medio de obtener el control de un gran número de computadoras. El aumento incesante de computadoras que mantienen conexiones permanentemente activadas, como ocurre con la DSL, los sistemas de cable o las redes de empresa, favorece la propagación de esas prácticas y su capacidad para causar estragos. Con pocos cambios tecnológicos y educando al usuario para incentivarlo, entre otras cosas, a utilizar programas antivirus y con sistemas cortafuegos, los proveedores de correo electrónico pueden ejercer un mayor control del posible tráfico malicioso procedente de los sistemas de sus usuarios. Si gestionan el envío de correo electrónico de las computadoras personales, los proveedores podrán reducir los costos derivados de sus actividades, dar mayor satisfacción a los usuarios y reducir el grado de abusos por Internet asociado con sus servicios.

Amenazas y abusos en la transmisión de correo electrónico

Con el acceso constante (envío de correo electrónico) de las computadoras personales a servidores de correo electrónico sin control ni vigilancia por parte del proveedor de correo electrónico, tanto los proveedores como sus clientes están más expuestos a sufrir las consecuencias de personas mal intencionadas o de aplicaciones perjudiciales. Las computadoras personales controladas por terceros no autorizados e imposibles de detectar, conocidas con el nombre de "zombis" o "botnets" (grupos de programas informáticos robots), favorecen el anonimato de quienes luego las utilizan para conectarse directamente a servidores de intercambio de correo (MX) y a servidores de retransmisión del protocolo simple de transferencia de correo (SMTP) no protegidos con objeto de enviar aún más correo basura y virus. Prácticamente el 80% de mensajes de correo basura circula por computadoras zombis sin el conocimiento ni la autorización de sus propietarios.

Riesgos de la inacción

Las consecuencias negativas para los propietarios de las computadoras afectadas son inmediatas y graves. A menudo, sus computadoras marchan con extrema lentitud durante varios días, en especial cuando quieren entrar en Internet. Sin que lleguen a saberlo, es posible que el emisor de correo basura esté saturando en sus equipos la anchura de banda de la transmisión "ascendente" y, además, limitando sensiblemente la anchura de banda de la transmisión "descendente".

Aunque el proveedor al que está conectada la computadora puede haber advertido apenas la anchura de banda suplementaria que se está utilizando, suele sufrir también las consecuencias negativas de esa intrusión. Puede llegar a ocurrir que el cliente afectado solicite apoyo técnico, lo cual entrañará para el proveedor la pérdida de un mes o más de ingresos, o que simplemente considere que el funcionamiento de los programas informáticos, del sistema de marcación o de los servicios de banda ancha es deficiente y decida cancelarlos.

Mientras la conexión del usuario siga infectada, el proveedor acumulará quejas de quienes están recibiendo mensajes de correo basura extraídos del cliente en cuestión. Las quejas recibidas por las unidades encargadas de la atención al cliente, de los abusos y de las operaciones de red pueden elevar los costos a niveles críticos debido a la presencia de incluso un pequeño número de computadoras "zombis". Además, el proveedor puede llegar a

comprobar que toda su red figura en la "lista negra" o que no está autorizada para enviar mensajes de correo electrónico a destinos muy solicitados ya que se considera que su red es la fuente de los abusos. Naturalmente, cada mensaje de correo basura enviado es también un mensaje recibido más. Permitir que este tipo de abusos se ejerza sin restricciones tiene consecuencias proporcionalmente negativas a escala mundial para *todos* los usuarios de Internet y proveedores de acceso porque los clientes pierden confianza y están menos dispuestos a utilizar Internet en las comunicaciones, el comercio o el esparcimiento.

Prácticas idóneas para la transmisión de correo electrónico

La autorreglamentación del sector industrial es la medida más eficaz para resolver el abuso en las transmisiones de correo electrónico, y la magnitud que ha alcanzado el problema del correo basura exige una acción inmediata. Los organismos gubernamentales en todo el mundo han comprendido perfectamente el mensaje: sin una acción inmediata ni resultados que la avalen, la industria se confronta a un examen más minucioso y a una mayor reglamentación. Por lo tanto, el MAAWG recomienda a los proveedores de Internet y de servicios de correo electrónico el siguiente conjunto de prácticas idóneas para la transmisión de correo electrónico:

1) Proporcionar servicios de entrega de correo electrónico en el puerto 587, como se describe en RFC 2476.
2) Exigir la autenticación en la entrega de correo electrónico, como se describe en RFC 2554.
3) Abstenerse de interferir la conectividad con el puerto 587.
4) Configurar el programa informático del cliente de correo electrónico para que admita el puerto 587 y la autenticación en la entrega de correo electrónico.
5) Bloquear el acceso al puerto 25 de todos los equipos anfitriones de la red, excepto los que se hayan autorizado explícitamente para efectuar las funciones de retransmisión del SMTP. En los equipos anfitriones los proveedores incluirán seguramente sus propios servidores de entrega de correo electrónico y tal vez los servidores de entrega de correo electrónico legítimos de los clientes responsables.
6) Bloquear el tráfico que llega a la red desde el puerto 25, lo cual evitará el posible abuso de quienes envían correo basura utilizando el encaminamiento asimétrico y piratean las direcciones IP en la red del operador.

Estas prácticas han sido adoptadas por proveedores de diferente envergadura, entre ellos muchos de los proveedores de servicio más reclamados en el mundo entero y numerosos miembros del MAAWG, sin que ello redundara en una reducción apreciable de la cartera de clientes.

Beneficios de la adopción de medidas

Con la exigencia de autenticación y la agrupación del tráfico para la transmisión de correo electrónico a través de retransmisores de SMTP, el ISP logra numerosas ventajas interesantes. Gracias a la adopción de esas medidas, el ISP podrá:

- Identificar la parte responsable de los mensajes entregados.
- Filtrar la cabida útil de correo basura, virus y otros mensajes abusivos.
- Vigilar y limitar, por cliente y/o en conjunto, las velocidades de transmisión.
- Hacer cumplir políticas en materia de utilización y condiciones de servicio aceptables aplicadas a la entrega de correo electrónico.

Por otra parte, el ISP obtendrá las siguientes ventajas competitivas:

- Mejoras en la entrega de mensajes de correo electrónico legítimos dado el menor riesgo de figurar en la "lista negra" de proveedores de servicios de correo electrónico y de Internet receptores.
- Menores costos en los centros de ayuda por cuestiones de abuso, de atención al cliente y de operaciones de la red.
- Capacidad para ofrecer servicios de primera categoría a los clientes que tienen verdadera necesidad de utilizar servidores de correo electrónico con acceso directo al puerto 25.
- Costos de infraestructura más bajos gracias a reducciones en la utilización del puerto y el consumo de anchura de banda.

- Participación del destinatario en la reducción del volumen de mensajes de correo basura a nivel mundial.

En cuanto se apliquen estas medidas, los equipos infectados ya no podrán favorecer el anonimato. Se podrán identificar rápidamente las computadoras afectadas, que se pondrán en cuarentena hasta que el propietario comprenda el origen del problema y lo corrija. Mientras tanto, se informará a los clientes de cuáles son las amenazas en materia de seguridad, alentándolos a que se protejan de ellas. Cada uno de estos cambios aumentará la seguridad y reforzará la privacidad de *todos* los usuarios.

Educación del cliente

El MAAWG no insistirá nunca demasiado en la importancia de mantener el contacto con los clientes y poner en su conocimiento esas amenazas y las medidas que se están adoptando para resolverlas, así como el papel que deben desempeñar los propietarios de las computadoras en este paso hacia un método de transmisión de correo electrónico más seguro. Los proveedores de Internet y de servicios de correo electrónico deben comunicar a sus clientes qué medidas están tomando, por qué lo hacen y por qué para la enorme mayoría de ellos, serán transparentes. Se insta enérgicamente a todos los proveedores de correo electrónico que adopten estas prácticas tecnológicas cuanto antes, para recuperar el control del puerto 25, y a que sigan informando adecuadamente a sus clientes, con objeto de proteger sus servicios contra los abusos.

Bibliografía

SMTP Service Extension for Authentication, J. Meyers, marzo de 1999: http://www.ietf.org/rfc/rfc2554.txt

Message Submission, R. Gellens and J. Klensin, diciembre de 1998: http://www.ietf.org/rfc/rfc2476.txt

Operation Spam Zombies, Federal Trade Commission, mayo de 2005:
http://www.ftc.gov/bcp/conline/edcams/spam/zombie/

Anti Spam Technical Alliance Technology and Policy Proposal, Anti Spam Technical Alliance, 11 de junio, 2004:
http://www.postmaster.aol.com/asta/proposal_html.html

Stopping Spam - Creating a Stronger, Safer Internet, Industry Canada, abril de 2005:
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00329e.html