PANDA CLOUD EMAIL PROTECTION

Simply... Evolution

CÓMO EVITAR SPAM Y MALWARE EN CORREO DE LA FORMA MÁS EFICIENTE

PANDA CLOUD OFFICE PROTECTION

PANDA CLOUD EMAIL PROTECTION

PANDA CLOUD INTERNET PROTECTION

PANDA SECURITY | 20 Aniversario 1990-2010

Indice

1. ¿Por dónde atacan los virus?

La mayoría de las amenazas que llegan a una empresa lo hacen a través de su servidor de correo y esto es así por diferentes motivos:

- El servicio de correo es el medio más empleado para comunicación entre personas a través de Internet.

- Un correo es una postal fácilmente accesible y manipulable.

- El protocolo de correo SMTP es sencillo y puede ser emulado por cualquier internauta.

- Muchas de las comunicaciones confidenciales de las empresas siguen pasando a través del correo electrónico.

- Los dispositivos de seguridad de las empresas tipo cortafuego no filtran el tráfico SMTP, que alcanza el servidor de correo.

- Los directorios de correo suelen aportar información altamente sensible de la empresa: estructura organizativa, funciones claves, directorios con informa-ción estratégica, etc.

- Es un medio de infección masivo, mediante gusanos y troyanos que se replican en cada destino, utilizando los ordenadores infectados leyendo las listas de correo del ordenador huésped.

- Un ataque dirigido de manera intencionada al servidor de correo de una empresa puede tener serias consecuencias económicas, y se convierte en un potencial objetivo.

Las empresas requieren que sus servidores de correo estén protegidos frente a los ataques de otros servidores. Normalmente se diseñan estrategias de protección por capas, que permiten incrementar la eficiencia de la protección ante posibles infecciones por virus y demás malware (dialers, spyware, hoaxes, gusanos troyanos, etc.)

Otro elemento importante es el tiempo de reacción ante una nueva infección no conocida. Se define la ventana de vulnerabilidad como el tiempo que transcurre desde que se presenta una nueva amenaza hasta que se liberan los primeros ficheros de firmas para detectarlos. Un ejemplo claro fue el virus **MyDoom**, en pocas horas (las que se tardó en aislar) infectó varios millones de ordenadores en todo el mundo.

Para reducir esta exposición al mínimo se emplean técnicas predictivas, basadas en métodos heurísticos o bayesianos, que permiten identificar comportamientos anómalos de los correos y de los ficheros que adjuntan y de esta forma aislar aquellos correos que resulten sospechosos. Lógicamente cuanto antes se aíslen estos correos, menor será la probabilidad de infección de la infraestructura IT.

2. El problema del spam

El correo electrónico se ha convertido en una herramienta indispensable para la gestión de las empresas e incluso de nuestras relaciones personales, sustituyendo en gran medida en la actualidad a otros medios de comunicación tradicionales.

Como toda herramienta con un alto grado de implantación, es susceptible de un uso intencionado cuya finalidad sea perjudicar a los usuarios del servicio de correo.

Uno de estos malos usos del servicio de correo es el denominado spam. El envío masivo de correos, se ha demostrado como una poderosa herramienta de marketing de muy bajo coste. Además los Spammers (generadores de spam) pueden llevar a cabo un negocio muy rentable en poco tiempo, siendo retribuidos en función del número de correos que envían en la red.

Esto ha motivado un efecto avalancha en el desarrollo de este tipo de correo, alcanzando en ciertos países cifras exorbitantes. Según Messaging Anti-Abuse Working Group (MAAWG), entre el 82-87% de todo el correo entrante es categorizado como spam o "correo basura"[1].

El spam provoca una molestia personal puesto que hay que gestionarlo (abrirlo, borrarlo, a veces puede producir equívocos en los destinatarios) y también un claro perjuicio económico, derivado del manejo de altos volúmenes de correo sin utilidad para la empresa. Todo el tiempo utilizado por el personal de una empresa (empleados usuarios, administradores de IT, etc) y los recursos de servidores y comunicaciones son costes para la empresa.

Además, el spam puede llegar a ralentizar las comunicaciones de una empresa: si el servidor de correo se ve forzado a procesar un volumen de correo de spam elevado, puede llegar a no tener suficiente capacidad de proceso para procesar convenientemente los correos útiles.

Lamentablemente el spam crece anualmente, alimentado por un número creciente de Spammers que generan un mayor volumen de tráfico. Esto obliga a tratar de una forma efectiva el filtrado y posterior eliminación de este tipo de correos.

La bondad de un sistema Anti-spam se mide por su exactitud a la hora de diagnosticar qué es y qué no es spam. Para ello se emplea el parámetro de falsos positivos.

Debemos tener en cuenta que el criterio de declarar un correo como spam, no carece de subjetividad, por lo que no se debe obviar el criterio del usuario al que va dirigido el supuesto correo.

El hecho de eliminar spam con criterios muy severos (alta parada de spam) puede tener consecuencias más negativas que positivas pues se puede aumentar de forma indeseada la tasa de falsos positivos (correos útiles tratados como spam).

1. http://www.maawg.org/about/MAAWG20072Q_Metrics_Report.pdf

Por tanto una técnica efectiva de filtrado debe proporcionar un alto rechazo del spam y simultáneamente un bajo nivel de falsos positivos. Este factor es crítico pues el usuario muestra una gran sensibilidad a que sean borrados correos que le eran útiles.

Para evitar efectos no deseados y simultáneamente parar un alto porcentaje de spam hay que mantener actualizado los criterios de filtrado y recibir información sobre nuevos orígenes de spam, de cuántas más fuentes mejor. Además, una técnica de almacenamiento por cuarentena es de especial ayuda para reducir la tasa de falsos positivos.

De todo lo anterior se deduce que la gestión del spam de una compañía no es un asunto sencillo y requiere de un procesado laborioso para alcanzar cuotas de calidad aceptables.

3. El servidor de correo. Una vulnerabilidad crítica

El tráfico de correo electrónico está basado en un protocolo SMTP, que reúne pocos o ningún requisito para el intercambio de información entre dos nodos de la red de manera confiable. Además, es un protocolo que se puede emular con facilidad, siendo factible generar tráfico SMTP intercambiando información de protocolo por un nodo de red (un simple PC) que no tiene intención de enviar correos sino saturar las comunicaciones de un servidor.

Los Firewalls de las empresas no pueden bloquear el tráfico de correo, pues constituye una fuente fundamental de sus comunicaciones, por lo que ha originado que sea un medio ideal para el envío de todo tipo de virus y malware (spyware, hoaxes, phishing, etc.)

A continuación vamos a tratar algunos casos de ataques que pueden resultar en un claro perjuicio para los usuarios del servicio de correo.

3.1 Ataques de Denegación del Servicio

Un ataque a un servidor de correo puede consistir en un envío masivo de demandas de comunicación hacia ese servidor. Esto significa que se genera protocolo de comunicación en volumen (frecuentemente desde orígenes diferentes) sin llegar a producirse siquiera el envío de un correo. El servidor que es interrogado, puede tomar diferentes opciones:

- **Opción A**: No responder a solicitudes de comunicación dirigida a direcciones de correo no registradas en el servidor de correo.
- **Opción B**: Responder con un mensaje de error al remitente.
- **Opción C**: Aviso de que se encuentra ocupado.

Si se toma la **Opción A** estamos aplicando una política que discrimina no sólo el correo malicioso sino también el correo útil, donde el remitente simplemente se ha equivocado al teclear la dirección de destino. No es por tanto recomendable configurar el servidor de correo en esta forma.

La **Opción B** supone que por cada inicio de protocolo SMTP, el servidor va a ser interrogado por una dirección y este va a declarar al nodo remitente si existe o no en su dominio. Es la manera normal de trabajo de los servidores de correo pues proporciona un grado de certidumbre sobre la recepción en el destinatario.

La **Opción C** se da en circunstancias de operación especiales, bien por que el servidor de correo está saturado o porque se ha decidido como táctica de respuesta a un ataque identificado.

El objetivo de estos ataques es claro: ralentizar el servidor de correo del cliente, incluso si es posible volverlo no operativo, con el consiguiente perjuicio económico.

3.2 Ataques de Directorio DHA

DHA (Directory Harvest Attack) es la técnica empleada por Hackers para hacerse con los directorios de correo de la organización a la que dirigen el ataque. Para ello emplean un software que genera direcciones de correo aleatorias mediante el envío de combinaciones factibles (nombres comunes, cargos, nombres de departamentos, etc.).

Mediante el envío masivo de ese tipo de direcciones y utilizando una técnica de prueba y error, pueden llegar a capturar no sólo las direcciones de correo de la organización sino también información sensible: su estructura organizativa, discos con información reservada, etc.

Las consecuencias que esto puede tener son fácilmente imaginables y pueden incluso derivar en responsabilidades a terceros de la empresa atacada si se demuestra falta de diligencia en el tratamiento de la información por su parte.

3.3 Phishing

Término que ilustra la acción de un Hacker para hacerse pasar por otro (generalmente una empresa) y de esta forma conseguir información confidencial del destinatario del correo. Un ejemplo reciente son los e-mails que se envían haciéndose pasar por el envío de un determinado Banco y bajo cualquier pretexto solicitar al destinatario datos personales, por ejemplo su Código de Cuenta Cliente. La emulación de la página del tercero (a la que las víctimas son dirigidas a través de un link en el e-mail) a veces alcanza una gran verosimilitud y el engaño tiene un alto grado de aciertos, con las consecuencias económicas que ello conlleva.

3.4 Spyware

Otra forma de obtener con información confidencial de los destinatarios del correo es enviar ficheros que al ejecutarse dejan residentes un troyano que graba y luego envía a determinado destino información de identificación del cliente cuando, por ejemplo, éste accede a determinadas páginas.

4. Protección efectiva del servicio de correo

Se puede proporcionar la seguridad del correo en diferentes niveles de la red. Distinguimos cincos casos:

- **Seguridad de Correo en el PC.** No es una solución efectiva desde el punto de vista de administración para eliminar el spam o problemas de ataques de Denegación de Servicio o de Directorio. De hecho todos los ataques se producirían tal como se han descrito en el apartado anterior sin protegerse el servidor de correo. Además los criterios para el filtrado de spam pueden carecer de la efectividad requerida según la máxima: "alto rechazo + bajo falsos positivos", quedan a discreción del usuario.

- **Seguridad en el Servidor de Correo.** Todo el tráfico no deseado atraviesa la red de cliente hasta el servidor de correo, lo que ya supone una sobrecarga de proceso en otros elementos de la red. El grado de conocimiento de fuentes y tipos de ataques se limita a la experiencia de la red del cliente. Además se carga con un procesamiento adicional al servidor de correo.

- **Seguridad en el Gateway del Cliente.** Se puede proceder con una argu-mentación similar al caso anterior. La mejora se produce por ser el Gateway un elemento más externo de la red del cliente.

- **Seguridad mediante Hardware específico en el perímetro de la red del cliente.** No soluciona la sobrecarga en los recursos de comunicaciones, pues el SPAM viaja por las líneas de comunicaciones del cliente, pero sí elimina la carga de proceso en los elementos de red.

- **Seguridad en Red mediante un Servicio Gestionado.** Aporta una solu-ción a todos los problemas anteriores:

  - El spam es eliminado en un punto externo a la red del cliente sin utilizar sus recursos.

  - Los ataques de Denegación de Servicio o DHA no se dirigen al servidor de correo.

  - No carga con procesamiento adicional los elementos de red del cliente.

  - No requiere de la inversión en Hardware adicional.

  - Y además se dispone de información actualizada a nivel de red, lo que permite reaccionar de manera más rápida ante nuevos ataques de red.

5. Seguridad en red mediante un servicio gestionado

Esta solución se realiza mediante un sistema de filtrado del correo en un nodo externo a la red del cliente. Para ello todo el tráfico de un mismo dominio de cliente se debe redirigir hacia el sistema de filtrado, modificando el campo MX del DNS del dominio del cliente.

A partir de ese momento, los correos con dirección de destino, la del dominio del cliente, son previamente enviados al sistema de filtrado. Éste los procesa y analiza mediante uno o varios motores antivirus, antispam y opcionalmente los filtra también por su contenido, siguiendo criterios de diccionario, por tipo de ficheros o tipo de imágenes.

Los correos que se clasifican como spam pueden ser tratados siguiendo diferentes políticas:

- Los correos que son claramente spam (por ejemplo proceden de direcciones incluidas en listas negras) son eliminados.

- Los correos que responden claramente a un perfil de spam, pero que no se puede garantizar con toda seguridad, se guardan en una cuarentena, notificando al destinatario de que dispone de correo considerado spam y que, por ejemplo, dispone de una semana para leerlo antes de ser borrado.

- Los correos que pudieran dar lugar a un falso positivo se marcan, por ejemplo, modificando la cabecera del correo, para que sean procesados por el receptor del correo.

Dentro de un ámbito de Servicio Gestionado, el administrador del dominio del cliente puede establecer la política que considere más conveniente o puede delegar la configuración al proveedor del Servicio Gestionado, según sea el caso.

El Servicio Gestionado también aporta una mejor defensa ante ataques de denegación de servicio o de directorio. Los expertos que gestionan el sistema de filtrado van a detectar comportamientos anómalos en el tráfico de un dominio y pueden utilizar "contramedidas" para luchar ante esos ataques. Un ejemplo: ante un ataque de denegación de servicio, el sistema de filtrado puede ralentizar su respuesta a esa dirección, provocando que el ataque no sea efectivo al aumentar los tiempos de respuesta y, por tanto, de espera del nodo que realiza el ataque. Esta ralentización puede desembocar en "cortar" cualquier tipo de respuesta a determinadas direcciones.

El hecho de ser un servicio en red gestionado permite acopiar una gran cantidad de información acerca de los ataques a la seguridad. Esta posición de observatorio,

aporta una clara ventaja para la detección temprana de nuevas amenazas. Por ejemplo, se empieza a propagar un nuevo correo de "phishing" en Internet que solicita en nombre de una entidad bancaria los datos de código de cuenta cliente a los destinatarios. La dirección del remitente está falseada y la página web a la que la víctima es dirigida designa a la supuesta entidad bancaria.

Un servicio gestionado en red va a detectar más rápidamente esta nueva amenaza y podrá emplear los medios de seguridad para que no afecte a los dominios de sus clientes.

La Seguridad Gestionada desde un nodo de red también proporciona una información completa a los clientes tanto de los ataques que ellos reciben como de los ataques más peligrosos que se producen.

Cada vez más, los ataques son más sofisticados y dirigidos a objetivos concretos, por lo que tienen un alto riesgo de producir más daño. La mejor técnica para combatirlos es mediante un servicio gestionado en red, por el alto grado de especialización del servicio prestado.

6. Panda Cloud Email Protection

Panda Cloud Email Protection es una solución de seguridad para email basada en software como servicio (SaaS), que garantiza la entrega de correo seguro y limpio. Panda Cloud Email Protection ofrece las siguientes funciones: antimalware, antispam, filtrado de contenidos y continuidad del servicio de correo:

- **Protección antimalware:** usando las más avanzadas tecnologías de protección preventiva, Panda Cloud Email Protection detecta todo tipo de malware, tanto conocido como desconocido, contenido dentro de los emails. Detecta los virus conocidos a través del motor de firmas y las nuevas amenazas a través de las últimas tecnologías proactivas y mediante el análisis directo de los ficheros sospechosos por PandaLabs.

- **Protección antispam:** Panda Cloud Email Protection combina varios motores antispam diferentes para alcanzar un ratio de detección por encima del 98.5%, garantizando que los usuarios no reciben spam. Aun más, el ratio de falsos positivos ronda sobre el 1 entre 30.000, alcanzando el máximo nivel de eficiencia.

- **Filtrado de contenidos:** permite a los clientes definir las políticas de seguridad de la compañía, estableciendo qué adjuntos pueden ser recibidos y cuales deben ser bloqueados.

- **Continuidad del servicio de correo:** Panda Cloud Email Protection evita que cualquier posible fallo en la red afecte a la continuidad del negocio. En previsión de cualquier fallo de los servidores del cliente o la propia red, el correo estaría accesible durante varios días, a la espera de la recuperación del sistema habitual.

6.1 Como funciona

Panda Cloud Email Protection scanea y ejecuta las acciones previamente definidas para cada uno de los buzones, antes de que esos lleguen a la red del cliente.

Si el correo está limpio, esté será inmediatamente entregado al buzón. Si por el contrario se detecta un comportamiento sospechoso o surge algún conflicto con las políticas establecidas, Panda Cloud Email Protection eliminará el mensaje o lo almacenará en el área de cuarentena. El área de cuarentena permite almacenar de forma segura mensajes sospechosos o inválidos, y de ser necesario, ser analizados lejos del sistema del cliente.

Panda Cloud Email Protection está directamente conectado a la Inteligencia Colectiva de Panda Security. Esto implica que todo el conocimiento sobre nuevas amenazas de PandaLabs está incluido en tiempo real y de forma transparente para los usuarios.

Panda Cloud Email Protection ofrece:

- **Máxima confidencialidad y seguridad en la información:** Panda Cloud Email Protection utiliza las más rigurosas medidas para garantizar la seguridad y confidencialidad de la información y datos de los clientes. El scaneo del correo se lleva a cabo bajo la más estricta confidencialidad, en línea con las políticas de seguridad ISO/17799, aplicándose tanto en la gestión de datos como en la seguridad física. Se monitoriza tanto el correo entrante como saliente para evitar que material confidencial entre o abandone la compañía.

- **Sencillo interfaz:** Los administradores y los usuarios de los buzones tienen acceso a la consola web, en la que en función de sus correspondientes permisos pueden realizar toda una serie de acciones. Esta consola es altamente intuitiva y existe una guía de usuario para resolver cualquier duda.

- **Configuración personalizable:** Panda Cloud Email Protection permite un alto nivel de configuración sin disminución de su simplicidad. Se pueden establecer políticas de seguridad para las cuentas de los usuarios e incluso permitiendo a dichos usuarios configurar sus propias listas blancas y negras de spam.

- **Gestión de la cuarentena:** Panda Cloud Email Protection almacena todo el spam o los mensajes que podrían contener virus en su propia cuarentena. De esta forma, se garantiza que los servidores de los clientes no va a estar nunca saturados de spam, ahorrando en recursos y capacidad de almacenaje. Sin embargo, los gusanos conocidos de envío masivo (mass-mailing), son eliminados directamente, sin ser enviados a la cuarentena, aunque se mantiene un registro para datos estadísticos. En el caso de adjuntos sospechosos de contener virus, son enviados a PandaLabs para que se realice un análisis detallado. PandaLabs tomará medidas inmediatas tanto para liberarlo como para confirmar que está infectado.

Panda Cloud Email Protection no requiere de inversiones iniciales ni en hardware ni en tecnología, los clientes no tiene que instalar ningún sofware complejo y caro y no implica ningún coste de mantenimiento.

Para usar este sistema, los clientes sólo necesitan redirigir su servidor de correo a Panda Cloud Email Protection mediante una simple redirección de DNS. El servicio está disponible en 24 horas.

7. Inteligencia Colectiva. Un nuevo modelo de seguridad

Panda Cloud Email Protection clasifica el malware en tiempo real basándose en la Inteligencia Colectiva. Pero ¿cómo funciona la Inteligencia Colectiva?

Millones de ordenadores repartidos por el mundo, sobre los que corren soluciones de Panda Security, están continuamente enviando información sobre posible malware a PandaLabs. Cuando aparece un fichero sospechoso, éste es enviado a PandaLabs y es clasificado como desconocido por defecto. Otro fichero sospechoso puede aparecer en cualquier otro sitio y a su vez es enviado a PandaLabs de la misma manera.

En PandaLabs, ambos ficheros y otros más, son enviados a un proceso de inteligencia artificial de correlación y clasificación que determina si es malware o no. Este proceso permite definir firmas en malware en cuestión de segundos. Solamente con ficheros muy complejos es necesaria la intervención humana.

Cuando un fichero es clasificado como nuevo malware es automáticamente incluido en el fichero de firmas de Panda Security e inmediatamente desplegado a todas las soluciones Panda. Si es goodware, también es clasificado, para evitar falsos positivos posteriores.

Panda Cloud Protection está directamente conectado a PandaLabs y todas las nuevas firmas están disponibles en tiempo real. Las ventajas de la Inteligencia Colectiva son notorias:

- La inteligencia reside en Internet (Inteligencia desde la nube).

- Panda obtiene visibilidad global sobre nuevas amenazas.

- El malware y el goodware se clasifican automáticamente.

- El proceso es completamente transparente para el usuario.

8. Beneficios del uso de Panda Cloud Email Protection

Panda Cloud Email Protection afrece a los usuarios el mejor ratio calidad-precio gracias a ser un servicio gestionado y reduciendo el tráfico entrante. Esta solución ofrece ventajas sólo disponibles a través de un servicio gestionado de limpieza de correo, beneficios no posibles con un software tradicional de servidor de correo o appliances dedicados.

Los beneficios incluidos son los siguientes:

- **Incremento de la productividad,** eliminando el spam y el malware de los mensajes recibidos con la máxima garantía.

- **Reducción de los costes operativos,** gracias a la reducción de las incidencias causadas por el malware o el spam y el tiempo de atenderlas.

- **Elimina la complejidad,** dado que la gestión es llevada a cabo por un tercero y la infraestructura interna de hardware es eliminada.

- **Simplifica la gestión de riesgos,** eliminando al email como origen de amenazas.

- **Permite la continuidad del negocio,** manteniendo los emails incluso durante un fallo interno de servidores y entregándolos una vez los sistemas se han recuperado.

- **Cumplimiento de la normativa,** garantizando correo limpio entrante y saliente y bloqueando los daños causados por un envío involuntario de spam desde la organización.

9. Conclusión

El spam y los ataques de malware están ganando en sofisticación y enfocados en perseguir objetivos específicos, por ello, el riesgo de que causen daños extensivos es mayor que nunca. La mejor técnica para combatir estas amenazas es a través de un servicio gestionado, utilizando los servicios de alta especialización que sólo un proveedor de servicio especializado puede ofrecer. Un servicio gestonado para el filtrado de correo es el método más efectivos y menos caro para aquellas compañías cuyos recursos de IT puedan verse comprometidos por las amenazas que se transmiten vía email.

Panda Cloud Email Protection ofrece la metodología de seguridad más avanzada de la industria. Actúa fuera de la red del cliente, utilizando una plataforma redundante y sistemas preventivos de detección que pueden resistir y aislar ataques de nuevas amenazas, incluso antes de que hayan sido identificadas. Este es un método efectivo dado que no requiere de inversiones en sistemas específicos y además, reduce la inversión en infraestructura de comunicaciones.

Con el equipo de expertos en seguridad de Panda Security gestionando la protección de correo, la disponibilidad y la confidencialidad, los clientes pueden focalizar sus recursos internos en las actividades centrales de su negocio.

Para más información sobre Panda Cloud Email Protection, visite por favor www.pandasecurity.com.

PANDA SECURITY

902 24 36 54
www.pandasecurity.com

 0610-WP-Cómo evitar spam y malware en correo de la forma más eficiente

PANDA SECURITY | 20 Aniversario 1990-2010