

**Tecnología de Análisis de Spam
Distribuido “En la Nube” de
NETGEAR®**

**Protección de red contra
amenazas vía e-mail**

Durante los últimos años el e-mail se ha convertido en una de las principales fuentes de amenazas de ataque informático tales como spam, virus, troyanos y phishing. Debido a que se pueden realizar e-mailings masivos, los agresores tienen la posibilidad de generar un promedio de unas 40.000 amenazas diarias contra la seguridad informática, es decir: 15 millones de amenazas al año. De acuerdo con la investigación realizada por Ferris el spam ha generado un coste a las empresas americanas de unos 35.000 millones de dólares en 2007, entre costes de productividad y costes de operaciones de ayuda a los clientes. Globalmente esta cantidad ha sido de unos 100.000 millones. De acuerdo a una investigación realizada por Nucleus la gestión del spam supone un coste a las empresas americanas de 71.000 millones adicionales.

Una de las principales razones que llevan a esta situación es que la mayoría de los softwares de seguridad carecen de la capacidad de adaptarse rápidamente a los constantes cambios en este terreno. Los autores de spam y programas malignos están constantemente redefiniendo su forma de distribución para propagar sus amenazas lo más ampliamente posible. La mayoría de los productos anti-spam y de seguridad sólo escanean el e-mail entrante buscando discrepancias en las direcciones y en el título del mensaje. Estos escáneres lo revisan teniendo en cuenta su propia lista de reglas existentes, así que a la hora de detectar inmediatamente amenazas que emplean nuevas técnicas o atributos, éstos fallan. Ya que la mayoría de las amenazas vía e-mail se envían a millones de destinatarios de forma simultánea, es necesaria la detección inmediata y el bloqueo de estas amenazas para poder neutralizar de forma efectiva el ataque.

El dispositivo de Gestión de amenazas Web y e-mail ProSecure™ STM de NETGEAR® utiliza la tecnología de Análisis de Spam Distribuido “en la nube” que está continuamente recopilando información de más de 50 millones de fuentes de todo el mundo. Este dispositivo evalúa de forma efectiva la legitimidad de los e-mails en tiempo real analizando sus patrones de distribución, en vez del título del mensaje solamente. Una vez que un e-mail se clasifica como spam, el escáner le asigna una firma y se genera un fichero de forma inmediata con su correspondiente patrón, deteniendo el ataque de forma efectiva antes de que se propague.

La propuesta de NETGEAR está basada en el conocimiento de que todos los ataques comparten las siguientes características comunes:

- La mayoría de mensajes de e-mail dentro de un ataque han sido alterados para que sea difícil adoptar reglas de bloqueo basándose en el análisis del contenido. Por ejemplo, el contenido de un spam normalmente es una imagen, ya que no puede ser fácilmente analizada por los actuales filtros de contenidos.
- La mayoría de los ataques constan de millones de mensajes de e-mail para poder tener una alta tasa de respuestas y obtener el mayor beneficio posible para el agresor.
- La mayoría de los ataques se llevan a cabo en un corto periodo de tiempo, requiriendo una solución que detecte el ataque en tiempo real para poder limitar o evitar el posible daño.
- Los creadores de los ataques hacen lo posible por disimular su origen para que sea complicado seguir la pista del mensaje de vuelta hacia ellos.

El Ciclo de Vida de un Ataque

Los autores de programas malignos tienen la habilidad de enviar de forma simultánea varios millones de mensajes en cuestión de minutos utilizando *botnets*. Los *botnets* son ordenadores zombi que han sido infectados por programas malignos y que permiten al autor controlar los procesos del sistema de forma remota. Una red *bot* puede tener unos 20.000 zombis de promedio, que se utilizan conjuntamente en un lanzamiento coordinado para una amenaza a gran escala. Hay redes *bot* que pueden tener un millón de zombis. Cuando el autor de un programa maligno lanza un comando de forma remota, cada uno de los equipos de la red infectados cobran vida y llevan a cabo el comando de forma simultánea.

Los virus y demás amenazas vía e-mail se autopropagan en el momento en que éstos infectan el equipo del usuario. Cuantos más equipos se infecten al principio, mayor será su propagación. Por esta razón es crucial detectar el ataque tan pronto como sea posible. Deteniendo el ataque en sus minutos iniciales, se puede interrumpir de forma efectiva el ataque a gran escala.

Los Patrones de los Mensajes

El spam, phishing y demás amenazas vía e-mail constan de millones de mensajes diferentes realizados de forma intencionada para escapar de los filtros más utilizados. Sin embargo los mensajes que componen un mismo ataque comparten al menos un valor único identificable que puede ser usado para poder distinguir el ataque. Los diferentes ataques spam se lanzan normalmente desde la misma red de máquinas zombis. Los ataques de phishing normalmente lo encabezan destinatarios de las mismas páginas Web fraudulentas. Y cada vez que un virus específico se lanza vía e-mail siempre contiene el mismo código malicioso. Estas características comunes se pueden identificar incluso en una nueva técnica llamada “Whaling” o “caza de ballenas”.

Botnet

Una red *bot* o *botnet* es una colección de ordenadores que han sido infectados por software robots o “bots”. Un “bot” normalmente se ejecuta de manera autónoma utilizando la vulnerabilidad existente en la seguridad del sistema operativo o en una de las aplicaciones del usuario. El “bot” puede instalarse en el sistema de forma automática sin necesidad de la intervención del usuario. Un bot también puede ejecutarse mediante un gusano o troyano que haya llegado a través de spam. Una vez que el bot está instalado, el ordenador se une a una gran conjunto de ordenadores infectados por el bot denominados “zombis” y pueden ser controlados por usuarios maliciosos de forma remota sin el consentimiento ni el conocimiento del dueño legal del equipo.

Caza de Ballenas (Whaling)

El “Whaling” (o caza de ballenas) es un tipo de phishing cuyo objetivo son los altos ejecutivos dentro de una empresa. El “whaling” consiste en confeccionar cuidadosamente un e-mail que se envía a objetivos individuales para tentarles a pulsar en el link incluido en el mensaje que les llevará a una página Web maliciosa. Una vez en la Web, puede que se descargue un software espía en sus equipos o los usuarios puede que sean engañados para que rellenen formularios con información sensible sobre ellos o sus negocios. Un e-mail típico de “whaling” puede hacerse pasar por una factura procedente del “Better Business Bureau” (Oficina de mejoras) u otro contenido relacionado con su negocio.

Cada uno de estos valores recurrentes se denominan “patrones del mensaje” del ataque. Cada mensaje que contenga uno o más de estos patrones únicos tiene muchas posibilidades de ser parte del mismo ataque.

La mayoría de los ataques tienen un ciclo de vida relativamente corto, normalmente unas pocas horas. Así que el auténtico valor de una solución de escaneado debe ser que sea capaz de detectar y clasificar los mensajes en tiempo real, antes de que el ataque produzca algún daño. Además desde que la mayoría de los ataques intentan disfrazar los mensajes para que parezcan correspondencia legítima, las soluciones basadas en el análisis de patrones deben distinguir entre comunicación legítima y amenazas vía e-mail.

Para llevar a cabo ambos objetivos, los patrones de mensajes deben extraer del envoltorio del mensaje, los títulos, y el cuerpo del mismo sin tener en cuenta el contenido propiamente dicho. El análisis de patrones se puede aplicar para identificar ataques en cualquier idioma, formato de mensaje o tipo de código. Los patrones de mensaje pueden dividirse en patrones de distribución o patrones de estructura. Analizando la forma en que se distribuye el mensaje a sus destinatarios, los patrones de distribución determinan si el mensaje es legítimo o una amenaza potencial, mientras que los patrones de estructura determinan el volumen de la distribución.

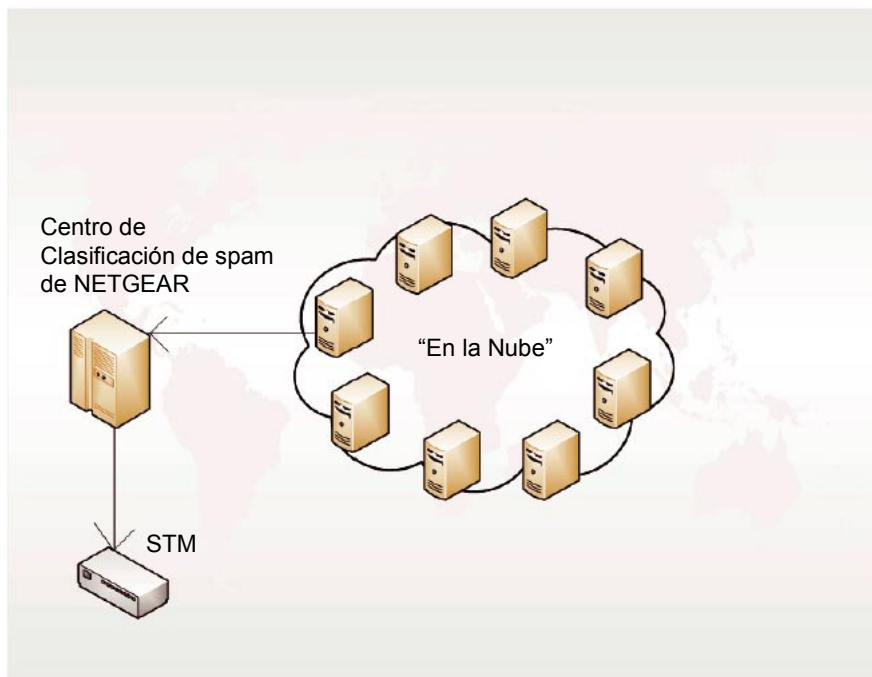


Imagen 1: Tecnología de Análisis de Spam Distribuida “en la Nube” de NETGEAR

La detección de los patrones representa una nueva forma de entender cómo se crean y propagan las amenazas vía e-mail. A través de esta detección y análisis, NETGEAR puede identificar de forma proactiva nuevos y únicos patrones en tiempo real, bloqueando nuevas amenazas en cuanto éstas sean lanzadas.

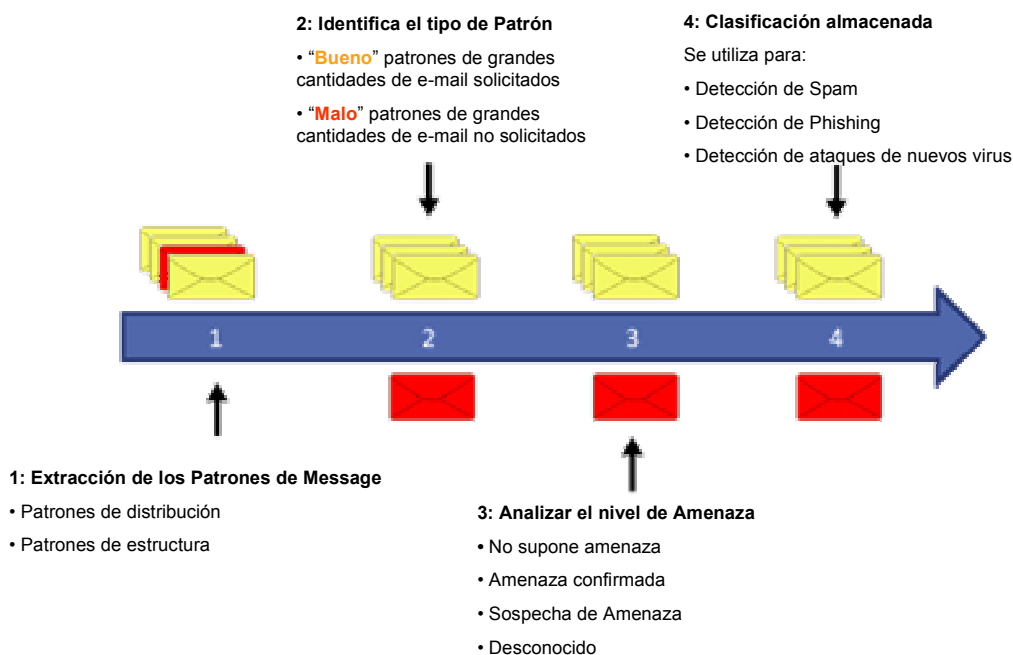


Imagen 2: Tecnología de Análisis de Spam Distribuida “en la Nube” de NETGEAR

Tecnología de Análisis de Spam Distribuido “En la Nube”

La tecnología de Análisis de Spam Distribuido “en la Nube” de NETGEAR consiste en dos elementos: el dispositivo Gateway de seguridad ProSecure STM instalado dentro de la red de la empresa, y el Centro de Clasificación de Spam de NETGEAR para el Análisis de Spam Distribuido “en la Nube”. EL STM se comunica con el Centro de Clasificación de Spam en tiempo real, obteniendo información, al segundo, sobre ataques de spam y programas malignos (ver imagen 1)

A través de una comunicación constante y coordinada entre ambos sistemas, NETGEAR detecta y clasifica de forma proactiva todo tipo de patrones de amenazas vía e-mail en tiempo real, basándose en el análisis de más de 50 millones de fuentes de todo el mundo. La tecnología de Análisis de Spam Distribuido extrae y analiza patrones relevantes de mensajes que se utilizarán posteriormente para identificar y clasificar, la distribución y estructura de los patrones de los ataques vía e-mail (ver imagen 2). Además para identificar nuevos patrones la tecnología de Análisis de Spam Distribuido se utiliza para modificar y mejorar las clasificaciones de los patrones de mensajes realizados con anterioridad.

Aplicando el análisis de forma inversa, el Análisis de Spam Distribuido puede distinguir los patrones de distribución entre grandes cantidades de e-mail solicitados que representen correspondencia de negocio legítima y de entre aquellos que no lo sean. Como resultado, la tecnología de Análisis de Spam Distribuido identifica cerca del 100 por cien de los mensajes de riesgo recibidos con casi ningún caso de falso positivo. Al sistema le resultan irrelevantes los idiomas y es igualmente efectivo con todos los tipos de formatos y códigos utilizados.

RESUMEN

Para combatir de forma efectiva las amenazas vía e-mail, una solución satisfactoria debe abarcar un gran número de objetivos. El Análisis de Spam Distribuido es una tecnología de detección proactiva que no se fía del contenido del mensaje y es capaz de detectar spam en cualquier idioma y formato de mensaje, incluyendo imágenes y código HTML así como caracteres extraños. El Análisis de Spam Distribuido analiza y clasifica de forma proactiva nuevas amenazas vía e-mail y desarrolla un fichero de patrones a pocos minutos después de haberse lanzado el ataque. La tecnología de Análisis de Spam Distribuido ofrece:

- Alto porcentaje de detección de spam con casi ningún caso de falso positivo.
- Detección inmediata de nuevas amenazas via e-mail
- Protección contra tentativas de phishing
- Protección contra amenazas en el contenido del mensaje. Contenido irrelevante.
- Detección de amenazas multi-idioma.
- Detección de amenazas multi-formato

Debido al análisis avanzado de patrones, la tecnología de Análisis de Spam Distribuido ofrece la mejor protección contra amenazas vía e-mail.

Solución de Gestión ProSecure™ STM contra Amenazas Web y E-mail de NETGEAR®

El dispositivo ProSecure STM utiliza una tecnología única que detecta y bloquea las intrusiones basadas en un comportamiento de distribución rápido y a gran escala. De este modo se puede detectar intrusiones de spam y programas malignos tan pronto como se produzcan y bloquear todos los mensajes asociados en tiempo real.

El dispositivo ProSecure STM con tecnología Stream Scanning, está diseñado para escanear flujos de información a medida que van entrando en la red. NETGEAR STM con la tecnología Stream Scanning es capaz de procesar grandes volúmenes de información en tiempo real, utilizando un simple escáner para identificar spam, programas malignos, brechas de seguridad o aplicaciones innecesarias. Así se asegura que los usuarios de la red reciban su e-mail y los contenidos Web limpios y sin retrasos.

El dispositivo ProSecure STM utiliza un sistema de comportamiento de defensa proactivo que soluciona las vulnerabilidades. La solución NETGEAR utiliza un análisis forense para identificar características sospechosas tanto en el tráfico de entrada como de salida de la red y neutralizarlas hasta que puedan ser examinadas más detenidamente.