Filtración del correo del spoofed ESA

Contenido

Introducción

Este documento describe un problema que se encuentre en el dispositivo de seguridad del email de Cisco (ESA) cuando el Spam y el email fraudulento ingresa en la red.

Problema

Tentativa de los impostores de personificar el correo electrónico. Cuando el correo electrónico personifica (los significados de ser de) a un miembro de su personal de la compañía, puede ser determinado engañoso y tiene el potencial para causar la confusión. En un intento por solucionar este problema, los administradores del correo electrónico pudieron intentar bloquear el correo entrante que aparece originar dentro de la compañía (correo del *spoofed*).

Puede ser que parezca lógico que si usted bloquea el correo entrante de Internet que tiene la dirección de retorno de la compañía en el Domain Name, soluciona el problema. Desafortunadamente, cuando usted bloquea el correo de esta manera, puede también bloquear el correo electrónico legítimo al mismo tiempo. Considere estos ejemplos:

- Un empleado viaja y utiliza un Proveedor de servicios de Internet (ISP) del hotel que transparente reorienta todo el tráfico del Simple Mail Transfer Protocol (SMTP) a los servidores del correo ISP. Cuando se envía el correo, puede ser que parezca que fluye directamente a través del servidor SMTP de la empresa, pero está enviado realmente a través de un servidor SMTP de tercera persona antes de que se entregue a la empresa.

- Un empleado inscribe a una lista de discusión del correo electrónico. Cuando los mensajes se envían a la lista de correo electrónico, se vuelven a todos los suscriptores, al parecer del terminal original.

- Un sistema externo se utiliza para monitorear el funcionamiento o el accesibilidad de los dispositivos externo-visibles. Cuando ocurre una alerta, el correo electrónico tiene el Domain Name de la compañía en la dirección de retorno. Los proveedores de servicio de tercera persona, tales como WebEx, hacen esto bastante con frecuencia.

- Debido a un Error de configuración de la red temporaria, el correo desde adentro de la compañía se envía vía el módulo de escucha entrante, bastante que el módulo de escucha saliente.

- Alguien fuera de la compañía recibe un mensaje ese ellos remite nuevamente dentro de la compañía con un agente de usuario del correo (M.U.A.) ese las nuevas líneas del encabezado de las aplicaciones bastante que el encabezado original.

- Una aplicación Internet-basada, tal como las **páginas del envío de** Federal Express o Yahoo **envía por correo electrónico esta** página del **artículo**, crea el correo legítimo con una dirección de retorno esas puntas de nuevo a la compañía. El correo es legítimo y tiene una dirección de origen desde adentro de la compañía, pero no origina desde adentro.

Estos ejemplos muestran que si usted bloquea el correo entrante basado en la información sobre el dominio, puede dar lugar a los falsos positivos.

Solución

Esta sección describe las acciones recomendadas que usted debe realizar para solucionar este problema.

Aplique los filtros

Para evitar la pérdida de correos electrónicos legítimos, no bloquee el correo entrante basado en la información sobre el dominio. En lugar, usted puede marcar el asunto con etiqueta de estos tipos de mensaje mientras que ingresan la red, que indica al beneficiario que los mensajes potencialmente están forjados. Esto se puede lograr con los filtros del mensaje o con los filtros contentos.

La estrategia básica para estos filtros es marcar las líneas del encabezado al revés-acentuadas del cuerpo (de los datos es el más importante), así como el remitente del sobre del RFC 821. Estas líneas del encabezado se muestran en MUAs y son lo más comúnmente posible las que son más probable ser forjado por una persona fraudulenta.

El filtro del mensaje en el próximo ejemplo muestra cómo usted puede marcar los mensajes con etiqueta que potencialmente se personifican. Este filtro realiza varias acciones:

- Si el asunto tiene ya **"{forjado posiblemente}"** en él, después otra copia no es agregada por el filtro. Esto es importante cuando las contestaciones se incluyen en el flujo de mensajes, y un asunto pudo moverse con el mail gateway varias veces antes de que un hilo del mensaje sea completo.

- Este filtro busca para el remitente del sobre o de la encabezado que tiene un direccionamiento ese los extremos en el Domain Name **@yourdomain.com.** Es importante observar que correo-de la búsqueda es automáticamente sin diferenciación entre mayúsculas y minúsculas, pero de - la búsqueda de la encabezado no es. Si el Domain Name se encuentra en cualquier ubicación, el filtro inserta "**{forjado posiblemente}" en el** extremo del asunto.

Aquí está un ejemplo del filtro:

```
MarkPossiblySpoofedEmail:

   if ( (recv-listener == "InboundMail")       AND
        (subject != "\\{Possibly Forged\\}$") )
```

```
{
    if (mail-from == "@yourdomain\\.com$") OR
       (header("From") == "(?i)@yourdomain\\.com")
    {
        strip-header("Subject");
        insert-header("Subject", "$Subject {Possibly Forged}");
    }
}
```

Medidas adicionales

Porque no hay método simple de identificar el correo del spoofed del correo legítimo, no hay manera de eliminar el problema totalmente. Por lo tanto, Cisco recomienda que usted habilita la exploración del Anti-Spam de IronPort (IPA), que identifica con eficacia el correo fraudulento (phishing) o el Spam y lo bloquea positivamente. El uso de este escáner del anti-Spam, cuando está juntado con los filtros descritos en la sección anterior, proporciona los mejores resultados sin la pérdida de correo electrónico legítimo.

Si usted debe identificar los correos electrónicos fraudulentos que entran en su red, después considere el uso de la tecnología identificada las claves del correo del dominio (DKIM); requiere más la configuración, pero es una buena medida contra el phishing y los correos electrónicos fraudulentos.

> Nota: Para más información sobre los filtros del mensaje, refiera al **guía del usuario de AsyncOS** en la página de soporte del dispositivo de seguridad del correo electrónico de Cisco.