ESWL: Plataforma Web para la Gestión de Lista Blanca en RedIRIS

ESWL: Web platform for RedIRIS White List Management

Carlos Javier Sánchez, Rafael Capilla, Jesús Sanz de las Heras, Francisco Monserrat

Resumen

En la última década, el uso masivo del correo electrónico ha incrementado el valor y cantidad de la información transmitida por este medio, generando al mismo tiempo numerosos problemas de seguridad, tales como: spam, virus, o phising entre otros. El spam se presenta actualmente como uno de los mayores enemigos del correo electrónico y supone un serio problema para las infraestructuras de los propios servidores de correo así como para la reputación de las organizaciones que los mantienen. Algunos esfuerzos que tratan de garantizar la seguridad del correo se basan en listas de reputación de direcciones IP, denominadas también listas blancas. En este trabajo proponemos la creación de una plataforma Web de gestión, dentro de RedIRIS, que agilice y automatice parte de las tareas cotidianas que forman parte de la gestión de listas de reputación IP.

Palabras clave: Spam, listas de reputación IP, listas blancas.

Summary

In the last decade, the massive use of e-mail has increased the value and amount of the information transmitted via this media, while generating several security problems, such as: spam, virus or phishing, among others. Spam is currently one of the greatest enemies of e-mail and poses a serious problem to the infrastructure of mail servers themselves, in addition to the reputation of the organisations that maintain them. Some of the efforts aimed at guaranteeing e-mail security are based on IP address reputation lists, also called white lists. In this paper we propose the creation of a Web-based management platform, within RedIRIS, to expedite and automate part of the daily tasks that form part of IP reputation list management.

Keywords: Spam, IP reputation lists, white lists.

En este trabajo proponemos la creación de una plataforma Web de gestión, dentro de RedIRIS, que agilice y automatice parte de las tareas cotidianas que forman parte de la gestión de listas de reputación IP

Uno de los mecanismos más eficaces y conocidos para mitigar el spam son las denominadas listas negras que contienen direcciones IP emisoras de spam

1. Introducción

En los últimos años, el spam se ha consolidado como uno de los canales más efectivos para el envío de información electrónica no deseada así como de nuevas formas delictivas (DoD, Phising) mediante la captura de servidores ("zombies") a través de la propagación de gusanos que se distribuyen en la red. Algunas de las soluciones actuales se basan en el análisis de contenidos y en la reputación (buena o mala) de las direcciones IP de donde procede el mensaje. La reputación IP ha dado lugar tanto a tecnología basada en listas negras (BlackListing) [6], que consisten en ofrecer acceso a direcciones IP con mala reputación, como a listas blancas ("Whitelisting"), direcciones IP con buena reputación. Con el fin de responder a estos desafíos, describimos en este trabajo una plataforma Web para la gestión de listas blancas dentro de RedIRIS.

2. Reputación en la red

El interés por las listas de reputación IP se basa en la confianza o no de las direcciones IP que forman parte de ella, de manera que los administradores de las organizaciones de correo puedan decidir aceptar o rechazar correo procedente desde ciertas direcciones IP y tratar de reducir al máximo los falsos positivos (spam). Uno de los mecanismos más eficaces y conocidos para mitigar el spam son las denominadas listas negras (DNSbl - DNS BlackList) que contienen direcciones IP emisoras de spam. El

principal problema de este tipo de listas es la arbitrariedad empleada para incluir o excluir direcciones IP [1] [2], provocando falsos positivos y una disminución de su eficacia. Con el fin de mitigar este impacto, se hace necesario definir una lista de excepciones o lista blanca que indique aquellas direcciones que no deben ser filtradas. Actualmente, la unión de listas blancas y negras ha mejorado los sistemas de reputación, donde las direcciones IP reciben una puntuación que refleja la confianza en la misma en base a criterios más amplios. Ese valor es utilizado por los ISP para aceptar o rechazar un correo electrónico. A nivel internacional existen diversas iniciativas de listas blancas, como por ejemplo la iniciativa alemana denominada DNS Whitelist [3], de carácter abierto y no comercial.

Lista blanca en RedIRIS: El actual diseño de la lista blanca desplegada en RedIRIS dispone de los siguientes módulos, tal y como muestra la Figura 1. El módulo de (i) gestión de direcciones IP se encarga de las altas y bajas de las direcciones IP de los servidores de correo que desean ser incluidos en la lista y que han superado las comprobaciones establecidas. El módulo (ii) accesos es responsable de generar los distintos formatos que se ofrecen para servir las IP: a) zonas DNS para consultas vía DNS y b) ficheros con formato greylist y postfix/sendmail. El módulo de (iii) vigilancia chequea periodicamente las direcciones IP de la Lista con el fin de que éstas sean confiables, de manera que se puedan eliminar aquellas que hayan dejado de serlo. Finalmente, el módulo (iv) gestión de usuarios no está implementado en la solución actual, siendo el Administrador de la lista el encargado de introducir nuevos usuarios de forma manual. La lista blanca de RedIRIS dispone de zonas de reputación máxima, media y de ninguna confianza. Las altas de la zona de máxima confianza se coordinan a través del Foro ABUSES (alianza entre universidades y proveedores españoles) [4] que contienen direcciones IP de confianza. La zona de media confianza corresponde a direcciones IP de terceros conocidas por los miembros del Foro ABUSES. La zona de ninguna confianza consiste en una lista de IP peligrosas basada en la captura de IPs a través de buzones trampa (spamtraps). Los spamtraps consisten en sistemas de captura de mensajes para comprobar que los equipos no reciben un volumen considerable de correo basura.

FIGURA 1. ELEMENTOS PRINCIPALES DE LA GESTIÓN DE LISTAS BLANCAS EN REDIRIS

Se hace necesario definir una lista de excepciones o lista blanca que indique aquellas direcciones que no deben ser filtradas

Los spamtraps consisten en sistemas de captura de mensajes para comprobar que los equipos no reciben un volumen considerable de correo basura

3. ESWL: Plataforma web de gestión de listas blancas en RedIRIS

Debido a una carencia de gestión centralizada y automatizada de los módulos descritos anteriormente, en este artículo se describe el estado actual de la plataforma Web ESWL (Email Spanish White Listing) para la gestión de listas blancas de direcciones IP dentro de la comunidad del foro Abuses de RedIRIS y fruto de la colaboración entre RedIRIS y la Universidad Rey Juan Carlos (URJC) de Madrid. El objetivo de ESWL es mejorar esta gestión que hasta ahora se realizaba de forma manual y reducir el coste de administración de la lista. Además, se pretende la integración con otras listas blancas mediante el uso de formatos de intercambio estándar, con el fin de incrementar el valor de la información almacenada. El objetivo de la plataforma ESWL es permitir que los responsables de cada dominio actualicen sus propias IPs, fundamentalmente de la zona ESWL. Por el contrario, la zona MTAWL es muy variada ya que incorpora

rangos de direcciones de Google, Hotmail o Yahoo, siendo éstas gestionadas por RedIRIS. La plataforma se enfoca a la comunidad de responsables de seguridad y correo de RedIRIS y de los ISP españoles afiliados al foro ABUSES. Las partes principales de la plataforma ESWL son las siguientes.

A) Gestión de usuarios

Este módulo representa una mejoría con respecto a otras implementaciones de listas blancas, a través del cual se pretende involucrar a los responsables de direcciones IP dentro de la propia lista para mantener actualizada la información con direcciones de servidores de correo activos. ESWL define varios tipos de usuarios con diferentes perfiles según el nivel de confianza de la zona DNS a la que se asocian sus direcciones IP. Inicialmente hemos considerado los siguientes perfiles: Administrador, Abuses y MTA. El perfil Administrador, posee todos los privilegios y es el encargado de configurar los distintos parámetros de la aplicación, gestionar los restantes tipos de usuarios y las direcciones IP de la lista blanca. El perfil Abuses se asocia a la zona DNS de mayor confianza mientras que el usuario tipo MTA a la de menor confianza. A los nuevos usuarios se les asocia el perfil MTA, que puede ser elevado de categoría por el administrador. La plataforma ESWL exhibe una gran usabilidad gracias a los distintos colores utilizados y a la facilidad para administrar la información. Asimismo, la plataforma elimina de forma automática, en un tiempo configurable por el administrador, aquellos usuarios no confirmados, y permite enviarles un correo electrónico para que actualicen sus datos personales, con el fin de que todas las direcciones IP existentes en la lista blanca se encuentren asociadas a un usuario activo. En caso de no actualización de los datos, los usuarios y sus direcciones IP se eliminan. De esta manera se automatiza esta funcionalidad y se descarga de trabajo al administrador de la lista.

El objetivo de la plataforma ESWL es permitir que los responsables de cada dominio actualicen sus propias IPs, fundamentalmente de la zona ESWL

B) Gestión de Direcciones IP

Constituyen el eje central de la plataforma por el cual los usuarios pueden gestionar las direcciones IP que se encuentren bajo su responsabilidad. Esta actualización se refleja en tiempo real en los diferentes formatos suministrados. Cada dirección IP tiene asociada dos direcciones de correo tipo abuses, una pública y otra privada, debido a que los rangos IP requieren de un atributo con una dirección abuse [7] que es pública y puede conocerse mediante IP Whois o vía Web. La dirección abuses se utiliza para un contacto más seguro en caso de surgir algún problema con la IP que se pretende registrar, por ejemplo, en caso de coincidencia con el módulo spamtraps. Resulta necesario que ambas direcciones abuses sean confirmadas para que una dirección IP pueda formar parte de la Lista Blanca de RedIRIS. Además, ESWL define de forma automática estados para las direcciones IP que se pueden modificar posteriormente. Los estados que se permiten son: activada, desactivada, no actualizada, aviso, y bloqueada, tal y como muestra la Figura 2.

La dirección abuses se utiliza para un contacto más seguro en caso de surgir algún problema con la IP que se pretende registrar

FIGURA 2. ESTADO DE LAS DIRECCIONES IP EN LA LISTA BLANCA DEFINIDOS EN ESWL

Cada dirección IP debe superar un conjunto de comprobaciones para poder formar parte de la lista, siendo éstas las siguientes: (i) Disponer de resolución inversa en el DNS, (ii) No formar parte de ninguna lista negra y, (iii) El dominio de la dirección IP debe poseer un registro SPF en el DNS. Estas comprobaciones son realizadas por ESWL de forma automática, de manera que en caso de no superar alguna de las comprobaciones, se informe al usuario responsable de la IP del problema encontrado. De manera adicional, existe una serie de direcciones IP consideradas especiales y que son dadas de alta por el administrador. Estas direcciones corresponden a servidores de correo especiales como puede ser gmail, estando incluidas en la zona del DNS de menor confianza. La plataforma permite a los usuarios administradores o del foro ABUSES la agregación de direcciones IP por rangos, mientras que los usuarios MTA deberán añadirlas una a una. Finalmente, ESWL permite importar direcciones IP recolectadas provenientes de otras fuentes [5] de confianza y que encajen en las políticas de la lista blanca, como por ejemplo [3].

C) Zonas DNS
ESWL permite generar zonas DNS para que puedan ser consultadas por cualquier servidor de correo. Por defecto se definen dos zonas: ESWL (direcciones IP de servidores de correo gestionados por miembros del foro abuses) y MTAWL (direcciones IP de servidores de correo validadas por miembros del foro abuses). Además, permite formatos disponibles para: postfix, sendmail, spamassassin y greylisting, con la intención de que la lista blanca pueda ser utilizada en el mayor número de servidores.

ESWL permite generar zonas DNS para que puedan ser consultadas por cualquier servidor de correo

D) Sistema de vigilancia mediante Spamtraps
Las direcciones Ip son comprobadas mediante un módulo de vigilancia basado en direcciones trampa. Este modulo comprueba si la dirección origen del SPAM está dentro las direcciones incluídas en la lista blanca. En caso de estar en la lista, se avisa a los administradores de esta dirección y se cambia el estado de la dirección IP , de forma que no este incluído en los ficheros generados de las zonas DNS. Esta comprobación asegura que la información proporcionada por la plataforma es confiable.

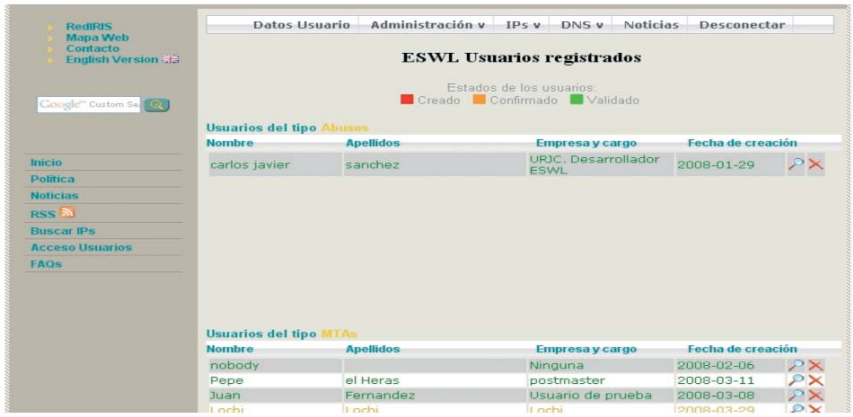
Las direcciones Ip son comprobadas mediante un módulo de vigilancia basado en direcciones trampa

4. Implantación y pruebas en RedIRIS

A partir del trabajo descrito en [8], se realizó la implantación en las instalaciones de RedIRIS en el mes de Octubre de 2008. Para ello se contó con un servidor Linux RedHat Enterprise, reservándose en un espacio de 10GB de disco. La implantación ha necesitado un tiempo considerable debido a ciertos problemas con unos módulos de seguridad interna (SElinux). Las dos personas involucradas directamente en el servicio participaron en la instalación. En la configuración inicial de ESWL se han definido cuatro zonas DNS, dos de ellas con 2.000 direcciones IP de máxima confianza (zona ESWL) y alrededor de 60.000 direcciones con calidad o confianza aceptable (zona MTAWL). Asimismo, todos los ficheros se encuentran en formato DNS.

En cuanto a las pruebas realizadas hasta el momento el objetivo ha sido doble: por un lado probar la funcionalidad de los distintos módulos de la aplicación y por otro lado la compatibilidad con los datos de la lista blanca existente. En cuanto a la gestión de usuarios, la Figura 3 muestra un ejemplo de usuarios con distintos roles. Los diferentes colores de la herramienta facilitan la distinción de los usuarios creados, confirmados y validados. Hemos observado que el procedimiento de verificación de la cuenta de correo electrónico es muy satisfactorio.

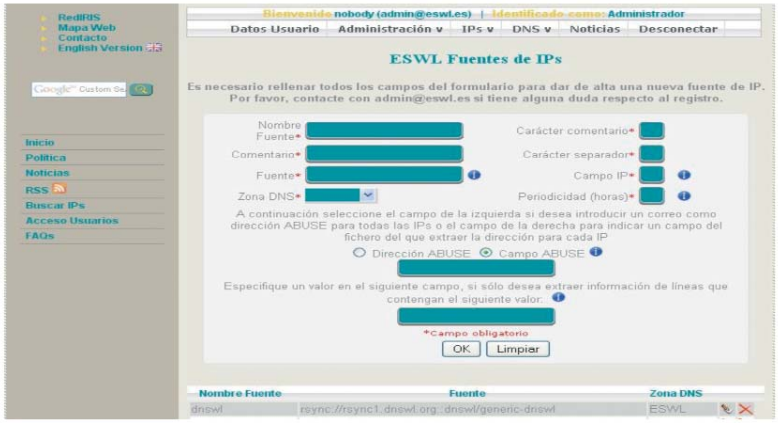
FIGURA 3. GESTIÓN DE USUARIOS DE LA LISTA BLANCA DE REDIRIS MEDIANTE LA PLATAFORMA ESWL



Una vez dados de alta los usuarios se procedió a introducir un conjunto de direcciones de IP y fuentes de IP

Una vez dados de alta los usuarios se procedió a introducir un conjunto de direcciones de IP y fuentes de IP (bloques completos de direcciones). Posteriormente, se generó la información de reputación que proporciona la lista para acceso vía consultas DNS ó mediante archivos de postfix/sendmail y greylist. De manera adicional, se verificó que la información generada corresponde con los datos introducidos y que la sintaxis de los ficheros es correcta. La Figura 4 muestra la interfaz para importar direcciones IP de una fuente externa.

FIGURA 4. DEFINICIÓN DE FUENTES DE IPS A TRAVÉS DE LA PLATAFORMA ESWL



La facilidad de ESWL permite gestionar de manera efectiva y con menor esfuerzo la lista blanca en RedIRIS, gracias a la implementación de procesos automatizados, así como la integración con listas blancas internacionales

5. Conclusiones

La facilidad de ESWL permite gestionar de manera efectiva y con menor esfuerzo la lista blanca en RedIRIS, gracias a la implementación de procesos automatizados, así como la integración con listas blancas internacionales. Las pruebas iniciales auguran un uso extensivo de la plataforma que debe ser contrastado por los usuarios externos. Como trabajos futuros se pretende: (i) tender a un sistema distribuido que permita el intercambio de direcciones IP en el entorno académico europeo mediante la

unificación de criterios, (ii) ampliación del mirror DNS para soportar las consultas vía DNS, (iii) incrementar la automatización de todo el proceso de gestión de la lista y, (iv) mejorar la gestión de grandes rangos de IPs mediante la inclusión de máscaras.

Referencias

[1] The Spamhaus Project from Wikipedia. http://en.wikipedia.org/wiki/The_Spamhaus_Project (2008).

[2] The Spamhaus Project. http://www.spamhaus.org/ (2008).

[3] DNS Whitelist. http://www.dnswl.org/ (2008).

[4] Foro ABUSES. http://www.RedIRIS.es/abuses/ (2008).

[5] Dutch Whitelist. http://noc.bit.nl/dnsbl/nlwhitelist/ (2008).

[6] Guidelines for Management of DNS Blacklists for Email. http://www3.tools.ietf.org/html/draft-irtf-asrg-bcp-blacklists-02 (2008).

[7] RFC 2142 Mailbox names for common services, roles and functions. http://www.rfc-ignorant.org/rfcs/rfc2142.php (2008).

[8] C. J. Sánchez, J. Sanz de las Heras, F. Montserrat, R. Capilla. "Reputación en la Red: Gestión de Lista Blanca en RedIRIS". XVIII Jornadas Telecom i+d, Bilbao, 29-31 Oct, ISBN: 978-84-9860-135-0, (2008).

Carlos Javier Sánchez
cjsq84@gmail.com
Rafael Capilla
rafael.capilla@urjc.es

Universidad Rey Juan Carlos

Jesús Sanz de las Heras
jesus.heras@rediris.es

Francisco Monserrat
francisco.monserrat@rediris.es

RedIRIS