Reputación en la Red: Gestión de Lista Blanca en RedIRIS

Carlos Sánchez[1], Jesús Sanz de las Heras[2], Francisco Monserrat[2], Rafael Capilla[1]

[1]Universidad Rey Juan Carlos, c/ Tulipan s/n, 28933, Madrid, Tlf: (34) 91 488 81 19
Email: CJSQ84@GMAIL.COM, RAFAEL.CAPILLA@URJC.ES

[2]RedIRIS, Plaza de Manuel Gómez Moreno s/n, Madrid, Tlf: (34) 91 212 76 25
Email: JESUS.HERAS@REDIRIS.ES, FRANCISCO.MONSERRAT@REDIRIS.ES

***Abstract* — Actualmente, el uso masivo de Internet como herramienta de trabajo permite que las organizaciones pueden mejorar su productividad a través de herramientas en tiempo real, como son: correo electrónico, mensajería instantánea, VoIP y Web. En este contexto, la sensibilidad de la información que circula por estos canales se está incrementando y las organizaciones se encuentran cada vez están más expuestas a problemas de seguridad. Actualmente, debido a que el correo electrónico es una de las aplicaciones más utilizadas en la Red, éste se ha visto afectado en los últimos diez años por problemas de seguridad tales como: spam, virus, o phishing entre otros. Algunos de los esfuerzos de hoy en día que están resultando más efectivos para garantizar la seguridad del correo se basan en la reputación de las direcciones IP mediante las denominadas Listas Blancas. En este trabajo proponemos la creación de una plataforma de gestión Web para agilizar y automatizar las tareas cotidianas que forman parte de la gestión de listas blancas que permitan garantizar la reputación de las direcciones IP provenientes de servidores de correo electrónico.**

I. Introducción

Durante mucho tiempo, el término *spam* se ha definido como “la distribución masiva de correo electrónico no deseado", es decir, como un problema que afectaba exclusivamente a los buzones de los usuarios. Sin embargo, en la actualidad supone un serio problema para las propias infraestructuras de servidores de correo electrónico. Asimismo, en los últimos años el spam se ha consolidado como el canal más efectivo para llevar a cabo actividades de ingeniería social maliciosa. Los objetivos vienen siendo la propagación de gusanos a través de enlaces Web y adjuntos para capturar nuevas maquinas (“zombies”) y poder llevar a cabo diferentes actividades delictivas en la red, como por ejemplo: ataques DoS, campañas de phishing, e-marketing, etc. De esta manera, el spam puede utilizarse como uno de los mejores detectores de máquinas comprometidas (“zombies”) que si bien son usadas para campañas de spam pueden ser utilizadas para cualquier otro tipo de ataques a mayor escala. En este contexto, podemos formular diversas preguntas que constituyen auténticos desafíos en la gestión del correo electrónico. Por ejemplo, la protección de los buzones de usuarios de máquinas zombies podría hacerse analizando los contenidos o la reputación de la IP de donde procede el mensaje. En este sentido, una de las primeras medidas para solucionar el problema es poder analizar la “reputacion” de la máquina que envía un mensaje, lo que ha dado lugar a listas “negras” (BlackListings) [6] que consisten en listas de direcciones IP con mala reputación en contraposición a las listas blancas (“Whitelisting”) que contienen direcciones con buena reputación. Con el fin de responder estos desafíos, estructuramos este trabajo de la siguiente manera. La sección II describe los aspectos más relevantes sobre la problemática de la gestión en la red. La sección III describe el estado actual de nuestra propuesta consistente en una plataforma Web para gestionar la reputación de las direcciones IP. La sección IV describe de forma resumida las experiencias preliminares llevadas a cabo. Finalmente, en la sección V proporcionamos las conclusiones

II. Reputación en la red

En la Internet de hoy en día, el correo electrónico se configura como una herramienta fundamental y necesaria para mejorar y acelerar las comunicaciones electrónicas como parte del funcionamiento de una organización, por lo que la no recepción de un mensaje debido a que éste pueda ser rechazado por considerarse un falso positivo (spam) debe ser evitado, Por otro lado las técnicas empleadas por los generadores de spam son cada vez más sofisticadas, ya que tratan que los mensajes enviados lleguen hasta el usuario final.

A. Listas de reputación

Actualmente, una de las técnicas más populares para evitar o controlar mejor el spam son las denominadas *listas de reputación*. La reputación en la Red define un valor de confianza para cada dirección IP que emita un correo electrónico. Así, este valor se convierte en una información de gran valor para que los ISPs decidan aceptar o rechazar dicho correo. En este sentido, uno de los mecanismos más eficaces para mitigar el spam son las denominadas *listas negras* (DNSbl – DNS BlackList) que contienen direcciones IP de emisores de spam (reputación negativa). Estas listas se utilizan para evitar la recepción de mensajes originados desde una dirección IP incluida en ellas. Las listas negras almacenan direcciones IP en

base a muy diversos criterios, como pueden: ser denuncias de usuarios, configuración del servidor de correo electrónico, uso de direccionamiento especifico (rango IP de usuarios residenciales), localización geográfica de la dirección IP emisora, incumplimiento de estándares RFC, etc. En general, la arbitrariedad para la inclusión o eliminación de direcciones IP en estas listas sigue siendo el principal problema [1] [2], ya que puede provocar falsos positivos y una disminución de su eficacia. En este sentido, con el fin de reducir el impacto de falsos positivos en listas negras, se hace necesario definir una lista de excepciones o *lista blanca* que nos indique qué emisores de correo no deberían ser filtrados, con el fin de mitigar el perjuicio provocado por el bloqueo de una dirección IP respecto al spam que ésta pudiera generar.

Actualmente, la unión de listas blancas y negras ha hecho evolucionar los sistemas hacia modelos de reputación, donde al final se puntúa con un determinado valor la calidad de una dirección IP en base a un criterio más amplio. A nivel internacional existen varias iniciativas de listas blancas, sobre todo en USA y son de carácter comercial. La lista blanca más importante a nivel europeo es una iniciativa alemana denominada DNS Whitelist [3] que tiene carácter abierto y no comercial. Con el fin de sumar esfuerzos y promocionar el uso de listas blancas, a nivel español RedIRIS ha puesto en marcha una iniciativa similar que trata de ser el embrión de lista blanca distribuida cuyo ámbito se circunscribe a las redes académicas europeas. Los objetivos y el estado actual de desarrollo de esta lista blanca se describen en el siguiente apartado.

B. Gestión de lista blanca en RedIRIS

Actualmente, la lista blanca desplegada en RedIRIS (red académica española) dispone de los siguientes elementos: (i) Gestión de direcciones IP, (ii) Accesos vía DNS, (iii) Módulo de gestión de usuarios y (iv) Sistema de vigilancia de cumplimiento de las políticas establecidas, tal y como se describe en la **Figura 1**. El módulo de *gestión de direcciones IP* se encarga principalmente de las altas y bajas de las direcciones IP de los servidores de correo que se pretende almacenar en la lista blanca. Asimismo, este módulo es el encargado de realizar los chequeos necesarios de forma automática para que las direcciones pasen con éxito una serie de filtros. El módulo de *accesos DNS* es el encargado de generar las distintas zonas DNS que son utilizadas para las consultas a través del DNS y en formatos greylist y postfix/sendmail. Las zonas DNS se generarán de forma periódica en función de las direcciones IP asociadas a cada zona y que se encuentren en estado activo. El módulo de *altas y bajas de usuarios* permite gestionar los distintos usuarios de la plataforma ESWL y con distintos privilegios. Estos usuarios serán las personas responsables de los servidores de correo que deseen formar parte de la lista blanca. Finalmente, el módulo de vigilancia se encarga de chequear de forma periódica las direcciones IP con el fin de que sean confiables y eliminar de la lista aquellas que hayan dejado de serlo.

Fig. 1. Elementos principales de la gestión de listas blancas en RedIRIS.

La lista blanca de RedIRIS dispone de zonas de reputación máxima, media y ninguna confianza. La zona de máxima confianza esta articulada a través del Foro ABUSES (alianza entre universidades y proveedores españoles) [4] que contienen direcciones IP gestionadas por personas de confianza. La zona de media confianza son direcciones IP de terceros conocidas por los miembros del Foro ABUSES. La zona de ninguna confianza es una lista negra basada en captura de IPs a través de buzones trampa (más conocido como sistema de spamtraps) que vigila y comprueba que las direcciones de las restantes zonas no envíen spam. Los spamtraps consisten en emplear sistemas de captura de mensajes que luego se utilizan para comprobar que los equipos que aparecen en esta lista blanca no reciben un volumen considerable de correo basura. El uso de spamtraps nos permite usar muestras reales de spam para comprobar que las direcciones contenidas en otras zonas no envían spam, y en caso de detectarlo poder contactar con los responsables.

III. PLATAFORMA WEB DE GESTIÓN DE LISTAS BLANCAS EN REDIRIS

Debido a una carencia de gestión centralizada y más automatizada de los módulos descritos anteriormente, en este artículo se describe el estado actual de una herramienta Web (denominada **ESWL**) orientada a la gestión de listas blancas de direcciones IP dentro de la comunidad del foro Abuses de RedIRIS, fruto de la colaboración entre RedIRIS y la Universidad Rey Juan Carlos de Madrid. Por este motivo, este proyecto trata de mejorar y ofrecer soluciones a un conjunto de problemas que permitan mejorar el funcionamiento de la lista blanca que a nivel nacional mantiene RedIRIS. Actualmente, la lista blanca dentro de RedIRIS se gestiona por completo de forma manual, siendo altamente costoso el mantenimiento y actualización tanto de direcciones IP registradas como de los contactos asignados a cada una de ellas. Además, se pretende mejorar la integración con otras listas blancas para que información administrada por RedIRIS resulte más valiosa y efectiva dentro de la comunidad a la que se orienta. En este sentido se persigue el uso de un formato estándar que permita un intercambio de información con otras listas. La plataforma Web que constituye la herramienta que trata de integrar la funcionalidad antes mencionada y mejorar la gestión de la lista blanca incluye como novedad una gestión de usuarios con diferentes características que puedan dar de alta direcciones IP y gestionarlas durante su el ciclo de vida, descargando así el trabajo realizado por el administrador de la lista.

A. Gestión de usuarios

En todo momento se pretende que la información de la lista blanca esté actualizada y no existan usuarios inactivos con información no válida o direcciones IP que ya no pertenezcan a los servidores de correo activos. La plataforma Web define distintos tipos de usuarios con diferentes perfiles que se basan en el nivel de confianza de la zona DNS a la que se asocian sus direcciones IP. Cada perfil tiene asociados unos permisos y consideramos inicialmente 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 MTA a la de menor confianza. Para el registro en la aplicación, cualquier persona debe introducir sus datos personales y confirmar su dirección de correo electrónico. Tras la confirmación, es necesario que los administradores de la lista blanca validen al usuario. Todos los usuarios entran en la aplicación con el perfil que menos privilegios tiene (MTA), pudiendo los administradores elevar el nivel de confianza de dicho perfil. Por otra parte, la herramienta elimina de forma automática, en un tiempo configurable por el administrador, aquellos usuarios no confirmados, y puede enviar un correo electrónico a los usuarios para que actualicen sus datos personales, de forma que todas las direcciones IP existentes en la lista blanca estén asociadas siempre a un usuario activo. En caso de no actualización de los datos, los usuarios y sus IP se eliminan. De esta manera se automatiza esta funcionalidad y se descarga de trabajo al administrador de la lista.

B. Gestión de Direcciones IP

Constituyen el eje central de la plataforma. Los usuarios pueden gestionar las direcciones IP que se encuentren bajo su responsabilidad. El alta de direcciones se realiza a través del formulario de la **Figura 2**. En el formulario de la Figura 2, la dirección IP dispone de dos direcciones de correo *abuses*, una pública y otra privada. Esto es así debido a que todos los rangos IP requieren de un atributo con una dirección *abuse* [7] que es pública y puede conocerse mediante *IP Whois* o vía Web.

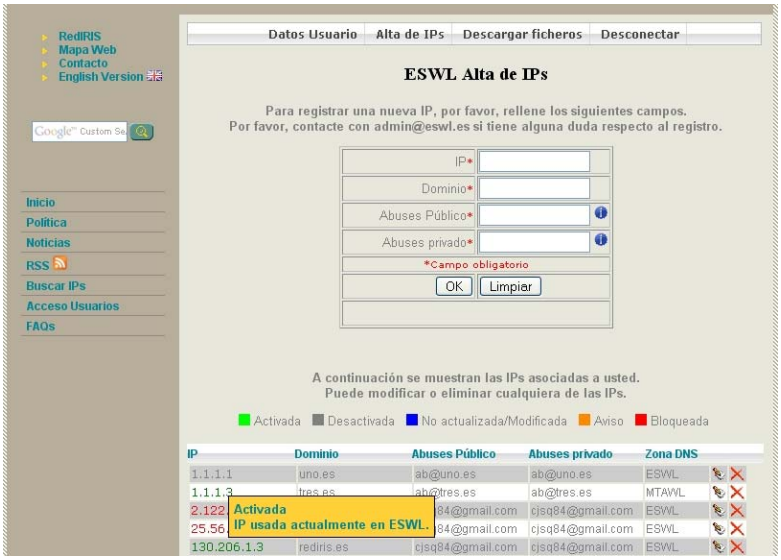

Fig. 2. Alta de direcciones IP en la lista blanca a través de la plataforma de gestión ESWL.

Por otra parte, la dirección *abuse* 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. Asimismo, se definen diferentes estados para las direcciones IP. Estos estados son establecidos por la aplicación automáticamente, aunque el administrador puede cambiar el estado de cualquier dirección IP para el correcto funcionamiento de la lista blanca. Los estados que se permiten son: activada, desactivada, no actualizada, aviso, y bloqueada. Cada estado se asigna a un color de manera que sea fácilmente identificable.

Por otra parte, una dirección IP deberá 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. Nuestra plataforma mejora esta gestión ya que realiza estas comprobaciones de forma automática y sin intervención por parte del administrador. En el caso de no superar alguna de las comprobaciones mencionadas, se informa al usuario responsable de la IP, del problema encontrado. De esta manera, se agiliza enormemente la gestión de IPs que van a formar parte de la lista blanca. De manera adicional, existen un conjunto serie de direcciones IP consideradas especiales y que son dadas de alta por el administrador. Estas direcciones corresponden a servidores de correo especiales como pueden ser *gmail, o hotmail.* Estas direcciones forman parte de la zona del DNS de menor confianza puesto que el usuario que las da de alta no es el responsable real de las mismas. Además, la herramienta permite a los usuarios administradores o del foro ABUSES la agregación de direcciones IP por rangos (127.0.0.2/24), mientras que los usuarios MTA deberán añadirlas una a una. Finalmente, otra de las mejoras consiste en incluir direcciones IP provenientes de otras listas blancas. La plataforma Web trata de sincronizar de forma masiva direcciones IP recolectadas provenientes de otras fuentes [5] que dispongan de direcciones IP de confianza que encajen en las políticas de la lista blanca, como por ejemplo [3].

C. Zonas DNS

La generación de las zonas DNS es uno de los objetivos de la aplicación para que éstas puedan ser consultadas por cualquier servidor de correo del mundo lanzando consultas de direcciones IP sobre ellas. Por defecto, en la aplicación se definen dos zonas DNS: **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), las cuales indican la confianza sobre las direcciones IP que las componen. También se permite definir nuevas zonas y modificar las existentes. Al definir una nueva zona, se ha de indicar el perfil de usuario cuyas direcciones IP nutren a la nueva zona. Por otra parte, existen formatos disponibles para: *postfix, sendmail, spamassassin y greylisting,* con la intención de que la lista blanca pueda ser utilizada en la mayor cantidad de servidores de correo posibles.

D. Sistema de vigilancia mediante Spamtraps

Todas las direcciones IP de la aplicación serán chequeadas contra el módulo de vigilancia basado en spamtraps. Este módulo comprueba si alguna de las IPs envía spam recogidos en los sistemas de spamtrap. En caso positivo, se deberá eliminar la dirección IP de la base de datos. Si por cualquier motivo la IP no puede ser eliminada en un momento determinado, la aplicación ESWL permite cambiar su estado *Aviso*, que implica que esta dirección IP no formará parte de los ficheros generados de las zonas DNS. Si el usuario dueño de una determinada IP considera que se trata de un falso positivo, podrá contactar con los administradores e incluso volver a insertar la dirección IP en la plataforma ESWL El objetivo del chequeo proporcionado por el módulo de vigilancia es que la información proporcionada por la plataforma sea totalmente confiable, de forma que no exista ningún indicio de que las direcciones IP incluidas en los ficheros de salida de ESWL han enviado spam en algún momento.

IV. EXPERIENCIAS PRELIMINARES

Las experiencias preliminares a nivel práctico que se están llevando a cabo en RedIRIS se han dirigido a la prueba del correcto funcionamiento de los siguientes módulos: (i) Gestión de usuarios, (ii) Gestión de direcciones IP, (iii) Generación de listas de reputación. En cuanto a la gestión de usuarios, además del usuario administrador existente por defecto, se han almacenado 2 usuarios administradores adicionales para las dos personas responsables en RedIris del futuro servicio, y para las pruebas a realiza, 2 usuarios con perfil Abuses y otros 2 con perfil MTA. 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, con el fin de mejorar la gestión al administrador y elevar la usabilidad de la interfaz. Asimismo, hemos podido observar que algunos campos del formulario pueden requerir algunas modificaciones, por ejemplo el tamaño del número de teléfono no permite incluir teléfonos internacionales ni hacer referencia a extensiones, aunque el procedimiento, con verificación de la cuenta de correo electrónico es muy satisfactorio.

Fig. 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 (bloques completos de direcciones), observado que la interacción entre el sistema y los usuarios responde a los requisitos especificados inicialmente. La generación de las listas de reputación se basa en las direcciones IP dadas de alta por los usuarios y que son verificadas por la aplicación antes de proceder a su activación en el sistema de reputación. Posteriormente, se procedió a generar, mediante la opción habilitada a tal efecto en el menú *"DNS"* del usuario Administrador, la información de reputación que proporcionará la lista para acceso vía consultas DNS ó mediante los archivos de postfix/sendmail y greylist). Además, se verificó que la información generada corresponde con los datos introducidos y que la sintaxis de los ficheros es correcta. La generación y descarga de los datos contenidos en la lista blanca en los tres formatos disponibles se realiza desde la interfaz gráfica mostrada en la **Figura 4**.

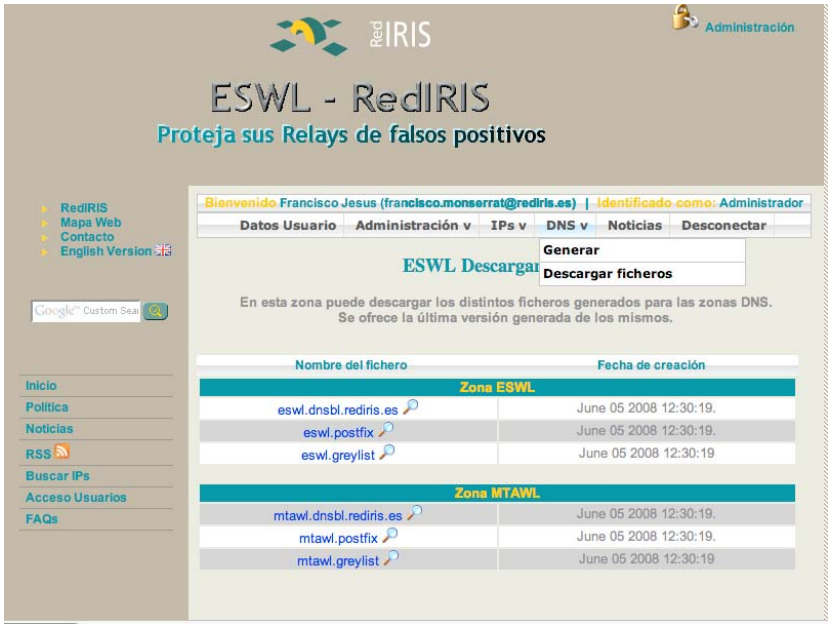

Fig. 4. Descarga y visualización de los ficheros generados por la plataforma ESWL.

V. Conclusión

Entre las conclusiones principales podemos destacar que el trabajo propuesto pretende ser un avance en la gestión de listas blancas en la comunidad académica española pero también con posibilidad e integración a nivel internacional, para lo cual se implantará próximamente en RedIRIS. Esta plataforma Web proporciona una gran usabilidad y facilidad para la gestión de listas blancas al automatizar e integrar parte de los procesos que actualmente se encuentran dispersos. De esta manera se facilita y descarga la tarea de los administradores de listas. Por otra parte, con esta iniciativa no hemos pretendido hacer una comparativa en cuanto a funcionalidades con otros sistemas parecidos, sino agilizar la gestión de listas blancas, principalmente en el ámbito español. Asimismo, como trabajos futuros, además de la explotación de esta plataforma, se pretenden otros aspectos como: (i) Tender a un sistema distribuido que permita el intercambio de direcciones IP en el entorno académico europeo mediante la unificación de criterios con iniciativas similares, (ii) Ampliación del mirror DNS para soportar el número de consultas vía DNS de la lista blanca, (iii) Aumentar la automatización de todo el proceso de gestión de la lista y, (iv) Mejora de la gestión de grandes rangos de IPs como por ejemplo mediante la inclusión de máscaras para direcciones IP.

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).