Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.
CONSEJERÍA DE ECONOMÍA, INNOVACIÓN, CIENCIA Y EMPLEO

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Informe de divulgación
Recursos de Seguridad en Línea

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-6032-010914*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*01/09/2014*
N° de Páginas	*1 de 18*

1 TABLA DE CONTENIDOS

2 OBJETO Y ALCANCE

El objetivo de este documento es dar a conocer un conjunto de recursos disponibles en Internet y de acceso en línea que pueden resultar de utilidad para diferentes tareas relacionadas con el análisis de la seguridad TIC.

Este documento va destinado al personal de la Junta de Andalucía y al público en general.

3 INTRODUCCIÓN

A día de hoy existen a nuestra disposición una gran cantidad de **herramientas sin coste** que nos pueden ayudar en diferentes tareas relacionadas con la seguridad TIC. Desde herramientas que nos ayudan en la prevención de incidentes de seguridad durante nuestro uso cotidiano las TIC hasta otras más orientadas a ser usadas por administradores o especialistas en ciberseguridad.

En este documento vamos a mostrar herramientas de seguridad **disponibles en Internet que podemos usar a través de nuestro navegador**. Éstas se caracterizan por no requerir instalación, ejecutándose a través de la web. Este conjunto de herramientas pueden resultar de gran utilidad para cualquier tipo de usuario, ya que ayudan a prevenir ataques o infecciones en su PC, reparar daños o simplemente facilitar una navegación segura en Internet.

Las herramientas que vamos a mostrar han sido clasificadas en las siguientes categorías:

- Análisis de archivos sospechosos y sandboxes
- Análisis de URL's
- Reputación y listas negras
- Bases de datos de phishing
- Bases de datos de sitios comprometidos
- Bases de datos de vulnerabilidades

4 RECURSOS DE SEGURIDAD EN LÍNEA

4.1 ANÁLISIS DE ARCHIVOS SOSPECHOSOS y SANDBOXES

Existen distintos sitios web de confianza que nos permiten subir y analizar archivos sospechosos. Este tipo de servicios nos pueden resultar útiles para:

- Comprobar si un archivo puede ser malicioso.
- Identificar el código malicioso exacto.
- Buscar códigos maliciosos específicos y conocer sus características.
- Estudiar el comportamiento de los códigos maliciosos.

A continuación se muestran algunos de los sitios web destinados a esta labor y que hemos considerado más interesantes.

VirusTotal

Sitio web: https://www.virustotal.com

VirusTotal es un servicio gratuito y online que analiza archivos y URL's para la detección de virus, gusanos, troyanos, así como cualquier tipo de contenido malicioso identificado por múltiples motores antivirus y de análisis. Al mismo tiempo, puede ser utilizado como un medio para detectar falsos positivos, es decir, recursos inocuos detectados como maliciosos por uno o más escáneres.

Las características de VirusTotal lo han convertido en todo un referente del análisis online de recursos maliciosos. Algunas de sus bondades son:

- Gratuito e imparcial.
- Ejecuta múltiples motores antivirus de diferentes fabricantes y escáneres de sitios web.
- Ejecuta múltiples herramientas de caracterización de archivos y URL.
- Actualizaciones en tiempo real de las firmas de virus y listas negras.
- Ofrece resultados detallados.
- Proporciona estadísticas en tiempo real.
- Proporciona una API para su integración con aplicaciones y ejecución de consultas automatizadas.
- Permite el análisis de URL sospechosas, así como la búsqueda por IP y otros términos, como MD5, SHA256 o determinadas cadenas de textos.
- Comunidad de investigación de malware en línea.
- Aplicaciones de escritorio de diferentes plataformas para interactuar con el servicio.

Wepawet

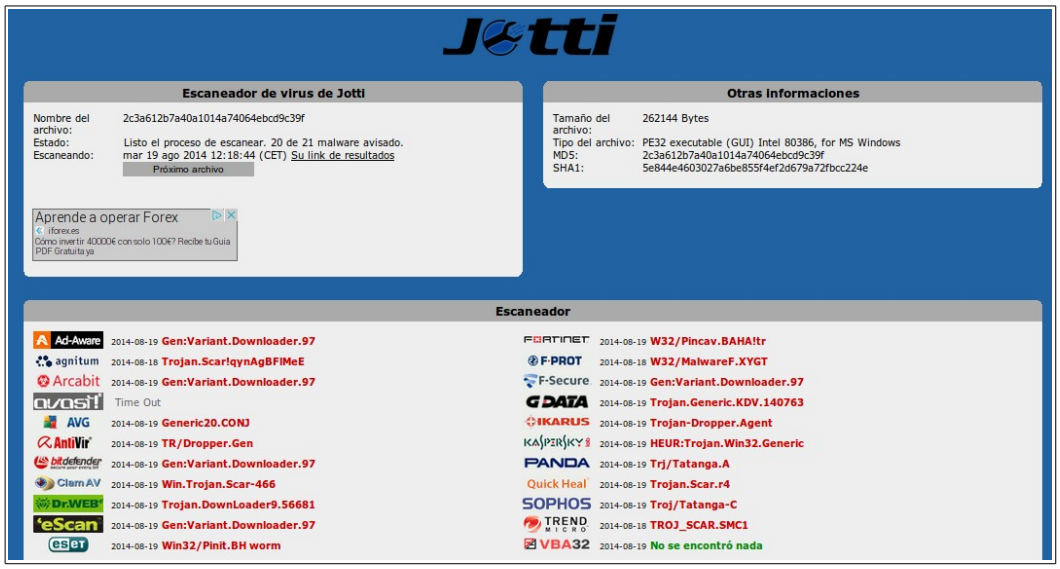
Sitio web: http://wepawet.cs.ucsb.edu

Wepawet es una plataforma para el análisis de amenazas en archivos Javascript, PDF y Flash. Es posible realizar el análisis a partir de una URL o subiendo directamente el archivo.

Jotti Viruscan

Sitio web: http://virusscan.jotti.org

A través de este sitio web podemos subir un archivo y analizarlo con múltiples motores antivirus.



SANDOBOXES ONLINE

El concepto de sandbox suele asociarse a "entorno de pruebas" en diferentes áreas. En el ámbito del análisis de malware, una sandbox se refiere a un entorno aislado donde podemos ejecutar programas potencialmente peligrosos o desconocidos para poder estudiarlos

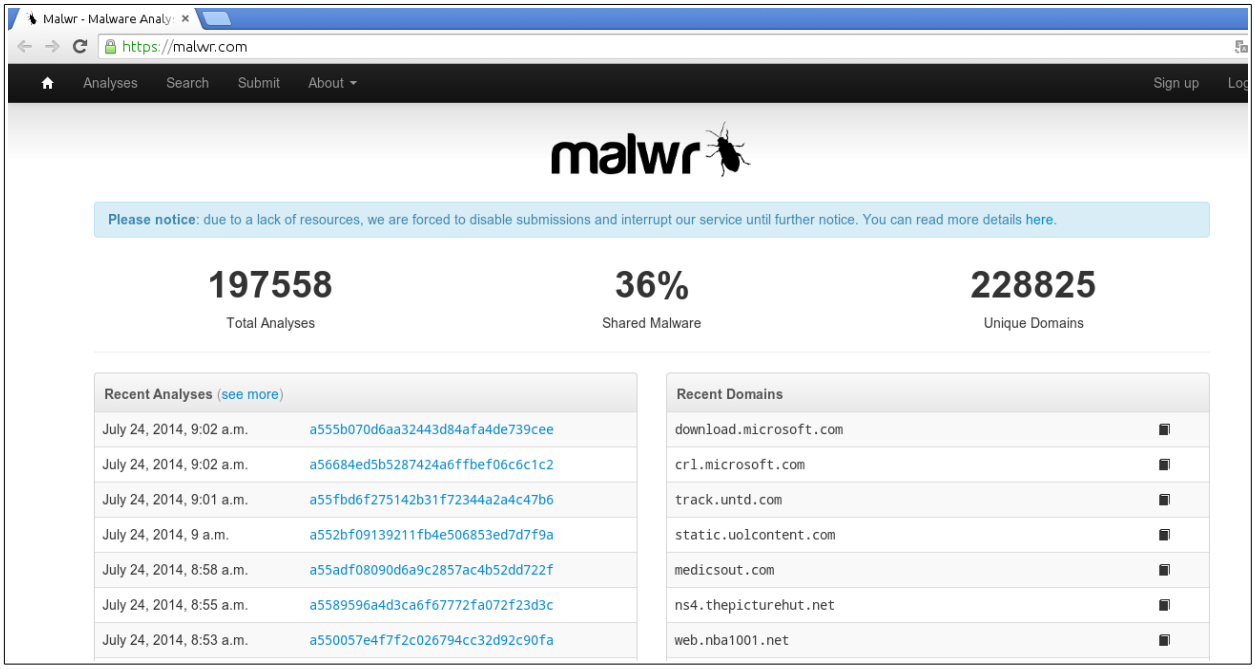
Usando técnicas de virtualización, una sandbox proporciona un sistema dotado de un conjunto muy controlado y limitado de recursos, como por ejemplo, espacio reservado en disco y memoria, acceso a la red, etc. Todo ello se monitoriza con el objetivo de determinar que comportamiento tiene ese programa.

Existen sitios web que proporcionan servicios de sandbox online. Veamos algunos de los más interesantes.

Malwr

Sitio web: https://malwr.com

Malwr es un servicio de sandbox gratuito, no comercial, basado en Cuckoo Sandbox. Permite el envío de archivos (ejecutables, pdf, dll, ...), recibiendo como resultado un análisis de la ejecución del mismo en un entorno controlado. En éste se realiza un análisis del programa bajo estudio (se suele denominar "muestra") extrayendo características de su comportamiento tanto en ejecución (análisis dinámico), como sin ser ejecutado (análisis estático). Los resultados pueden ser además compartidos con el resto de la comunidad de usuarios.



Anubis

Sitio web: https://anubis.iseclab.org

Anubis es otros servicio de sandbox gratuito. Permite analizar el comportamiento de archivos ejecutables de Windows. Genera como resultado un informe con gran cantidad de información sobre el análisis realizado.

En el siguiente enlace podrá encontrar un ejemplo informe realizado tras el análisis de un malware de Android.

Threat Expert

Sitio web: http://www.threatexpert.com

Threat Expert es un sistema de análisis de amenazas online basado en una tecnología sandbox propietaria.

En el siguiente enlace podrá encontrar un ejemplo informe realizado tras el análisis de un malware.

4.2 ANÁLISIS DE URL's

Las herramientas que veremos a continuación permiten identificar amenazas en sitios web accesibles a través de Internet. Para este análisis sólo basta con indicar la dirección web de la página que se desea analizar.

Anteriormente hemos visto algunas herramientas como VirusTotal, que además de analizar archivos, nos ofrecen este otro tipo de servicio.

Veamos otras herramientas que nos permiten realizar esta tarea.

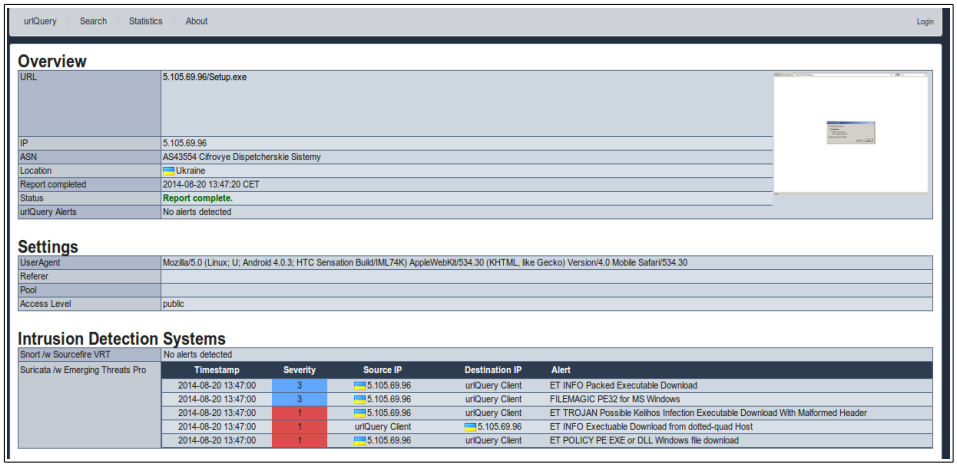
URLQuery

Sitio web: http://urlquery.net

Realiza la petición al sitio sospechoso, actuando como intermediario y detectando si existe alguna amenazas en el mismo. Actúa como si se tratara de un usuario que navega por todas las páginas que ofrece un determinado sitio web. Esto es conocido como HoneyClient.

Integra diferentes funcionalidades que resultan de gran utilidad:

- Permite configurar distintos User-Agents, lo que permite "simular" distintos clientes. Esto es útil para ciertos casos en los que las páginas se comportan de manera diferente según el cliente que realice la petición.
- Muestra las redirecciones que realiza el sitio, lo cual nos permite comprobar si existe alguna redirección maliciosa.
- Nos muestra los scripts Javascript que se ejecutan en el navegador.
- Integra motores de detección de intrusos.
- Proporciona información WHOIS sobre la IP.



Sucuri SiteCheck

Sitio web: http://sitecheck.sucuri.net

Analizador online de sitios web. Permite identificar amenazas como malwares o páginas dedicadas a actividades fraudulentas. También identifica errores en el sitio web analizado, si está presente en alguna lista negra o si existen recursos desactualizados o vulnerables.

BrowserDefender

Sitio web: http://www.browserdefender.com/es/

Analiza un sitio web en busca de amenazas contra la seguridad de los usuarios. Ofrece la descarga de plugins para diferentes navegadores que nos permiten identificar en tiempo real, mientras navegamos por Internet, amenazas en los sitios web por los que naveguemos o incluso en los resultados que nos ofrecen los buscadores.

4.3 MOTORES DE REPUTACION Y LISTAS NEGRAS

Las amenazas varían en el tiempo. A veces no es posible determinar en un momento concreto la existencia de una de ellas en un determinado sitio de Internet, bien porque haya sido desmantelada o porque haya cambiado de servidor, o cualquier otro motivo. Sin embargo, basándonos en otros criterios, como por ejemplo su historial de actividades, podría ser posible identificar actividad maliciosa asociada a una determinada IP o una página.

Bajo esta premisa nacen los motores de reputación. Este tipo de sistemas permiten marcar como peligroso, inofensivo, sospechoso o cualquier otro criterio a un determinado recurso de Internet en función de múltiples factores como las opiniones de los usuarios, su historial, contenido que publica, y un largo etcétera.

A este tipo de sistemas se suman las listas negras. Una lista negra es un sitio donde se registran direcciones IPs, dominios o sitios web que están implicados en acciones potencialmente dañinas, ya sea de forma voluntaria o involuntaria. Originariamente surgen para combatir el spam y ayudar a los proveedores de servicios de correo electrónico.

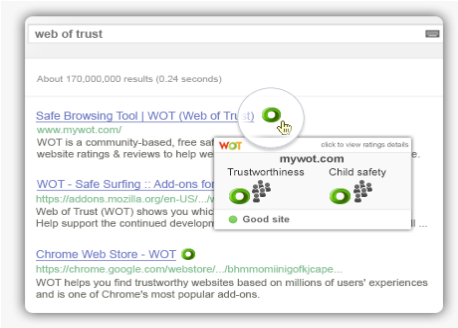
Este tipo de servicios, además de ser útiles para los usuarios en su uso cotidiano de Internet, o para los profesionales de la seguridad, también son útiles en sistemas de protección perimetrales como IDS o cortafuegos los cuales, si lo soportan, pueden conectarse a ellos, y a partir de la información que proporcionan afinar y mejorar sus tareas de protección.

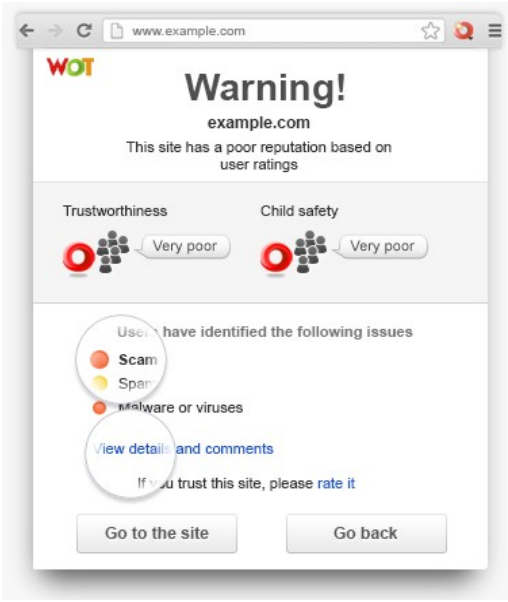
WOT (Web Of Trust)

Sitio web: https://www.mywot.com

WOT es un servicio que se usa para marcar páginas web dependiendo de su reputación. Esto ayuda a los usuarios durante la navegación por Internet a estar informados sobre la confianza en las páginas que visitan y sobre las que realizan trámites.

La reputación se basa en distintos factores como la presencia de malware, la identificación de páginas de phishing alojadas o la existencia de contenido ofensivo. Sin embargo, la valoración que más se tiene en cuenta es la opinión de los usuarios. Éstos pueden votar y establecer valoraciones que influirán positiva o negativamente al sitio web.

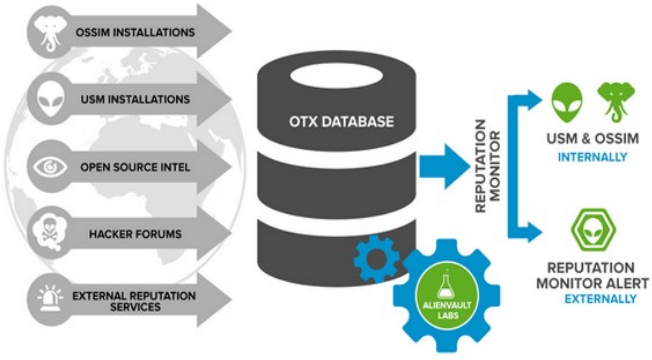




AlienVault Reputation Monitor Alert

Sitio web: http://www.alienvault.com/open-threat-exchange/reputation-monitor

Se trata de un servicio gratuito que permite alertarte cuando tus IPs y dominios aparecen en la base de datos de reputación de IPs de AlienVault, en alguna lista negra o incluso si está siendo objeto de conversación en algún foro de hackers (lo cual podrían indicar que fuera comprometida). También permite monitorizar registros DNS y certificados SSL para asegurar que no hay ningún tipo de cambio en ellos que desconociese.



Para poder usarlo debemos crearnos una cuenta en el sitio web indicado, donde tendremos acceso a un panel en el que podremos registrar nuestras IPs o dominios. El sistema de reputación nos avisará en caso de que detecte que nuestros activos registrados están implicadas en algún tipo de actividad maliciosa identificada por este motor.

URLVoid

Sitio web: http://www.urlvoid.com

Permite conocer la reputación de un sitio web en función de los resultados ofrecidos por varios analizadores de sitios web.

MultiRBL

Sitio web: http://multirbl.valli.org/lookup

Buscador de listas negras. Contiene más de 300 listas de diferentes proveedores donde buscar.

4.4 BASE DE DATOS DE SPAM Y PHISHING

De entre las amenazas más persistentes y continuadas, el spam y el phishing siguen ocupando un lugar en lo más alto. Su efectividad como medio para el fraude, propagar otras amenazas o simplemente inundarnos de anuncios no deseados es muy elevada.

Una de las formas de evitar ser víctimas de ello es hacer uso responsable de los servicios que las TIC ponen a nuestra disposición y actuar con responsabilidad. Pero para aportarnos un poco más de ayuda también existen páginas web dedicadas a combatirlo donde se registran tanto sitios web como direcciones de correo que han sido observados en actividades de spam o phsihing. Esto nos permite tenerlos identificados o denunciarlos.

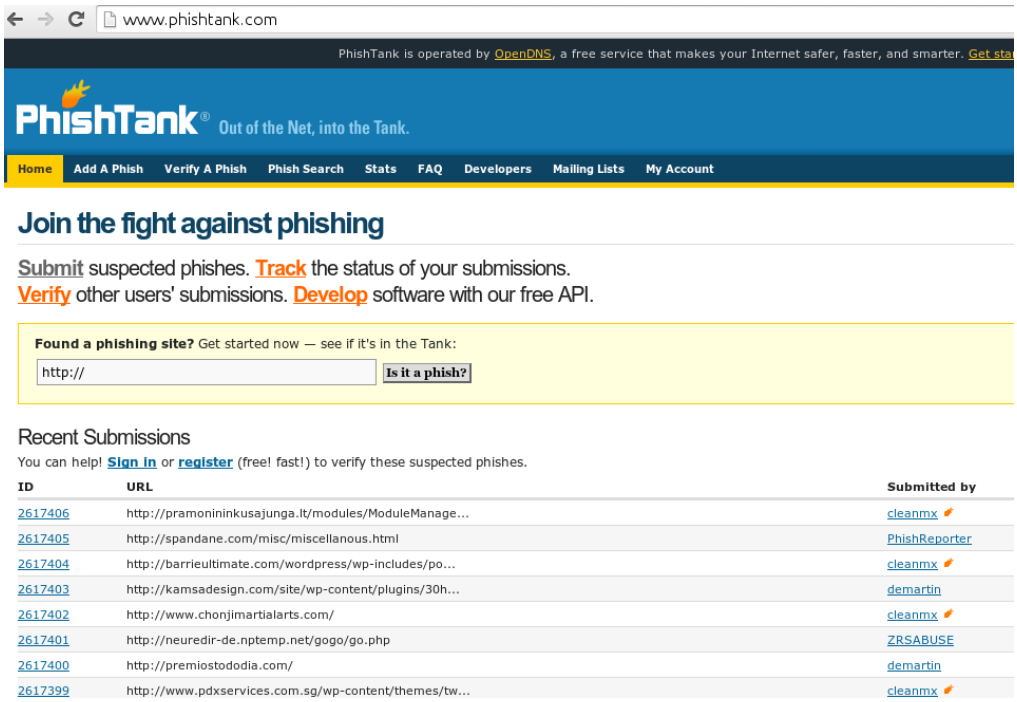
Phistank

Sitio web: http://www.phishtank.com

Impulsado por la iniciativa OpenDNS, PhishTank es un sitio web dedicado a almacenar casos de **phishing web**. Ofrece un espacio de intercambio colaborativo de datos e información sobre el phishing.

En la web se pueden realizar distintas operaciones como enviar una notificación sobre un caso de phishing, buscar en la base de datos los casos de phishing registrados o verificar si un sitio o servidor web contiene tiene alojada una página de phishing.

PhishTank ofrece además una API abierta que podemos integrar en nuestras aplicaciones, o para su uso de forma automatizado. Nos permite obtener sus datos en distintos formatos para su manejo (xml, csv, json...).



Phishtank ofrece además un complemento que se puede instalar en el navegador FireFox y que nos permitirán detectar en tiempo real mientras navegamos por la web, si una página está identificada como phishing. Éste se llama **PhishTank SiteChecker**.

Firefox: https://addons.mozilla.org/es/firefox/addon/phishtank-sitechecker/

OpenPhish

Sitio web: http://www.openphish.com

OpenPhish es un repositorio libre de sitios web detectados como phishing obtenidos con la tecnología de detección de phishing de la compañía FraudSense. Además de consultar los casos de phishing identificados desde el propio sitio web, es posible descargar la lista completa de los sitios recopilados en formato txt.

SpamCop

Sitio web: http://www.spamcop.net

SpamCop centra su misión en combatir las amenazas que se propagan a través del correo electrónico.

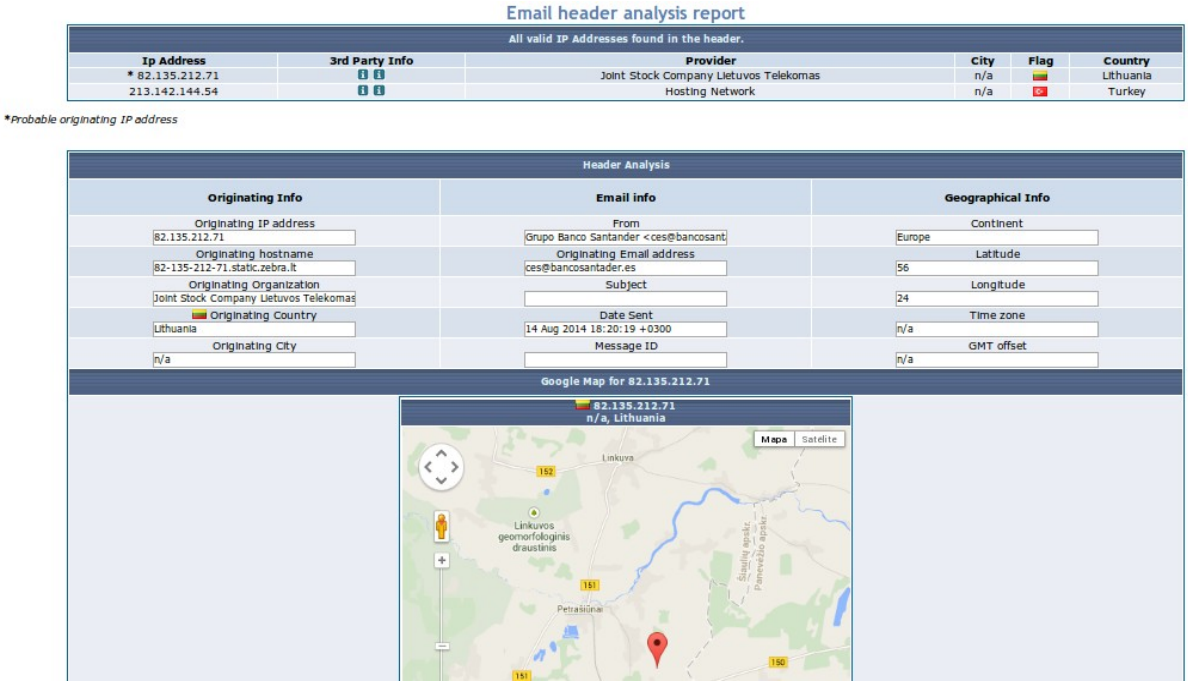
Ofrece a los usuarios un servicio a través del que pueden informar de casos de correos electrónicos no deseados. Con éstos, SpamCop determina el origen del correo electrónico no deseado y lo notifica a los proveedores de servicios de Internet pertinentes.

También ofrece una lista negra de IPs emisoras de SPAM llamada SCBL (SpamCop BlackList).

IpTrackerOnline.com - Email Header Analysis

Sitio web: http://www.iptrackeronline.com/email-header-analysis.php

Se trata de una herramienta que nos permite analizar una cabecera de un correo electrónico de forma automática. Desglosa la información de la cabecera del correo y muestra de forma clara los servidores de correo que ha atravesado hasta llegar a nosotros, el origen de la IP del emisor o su localización.



Stop Forum Spam

Sitio web: http://www.stopforumspam.com

Según los propios creadores del sitio web:

"*Te ofrecemos un listado de spammers que insisten al abusar de foros y bitácoras mediante ataques de spam, timos, explotaciones de vulnerabilidades, y otras molestias. Ofrecemos un sitio de "uso libre" donde puedes comprobar altas y comentarios nuevos en nuestra base de datos. Mostramos spammers conocidos de foros y bitácoras, con sus direcciones IP y correo-e, nombres de usuario, su grado de actividad, y en algunos casos, evidencia de su spam.*

Hay dos formas de acceder a esta información: o bien mediante búsquedas, o utilizando el API que se ofrece para búsquedas automáticas. El API permite que tu sitio (mediante un "mod" o un plugin/extensión) decida sobre cómo gestionar la actividad de los spammers.".

4.5 BASES DE DATOS DE SITIOS COMPROMETIDOS

Existen una serie de sitios en Internet dedicados a publicar sitios web que tienen problemas de seguridad. Desde sitios web con malwares hasta sitios web que han sido atacados por algún grupo organizado de ciberdelincuentes.

Este tipo de portales son útiles para detectar si alguno de nuestros sitios web ha podido ser víctima de un ataque y éste ha sido publicado en la red.

Zone-H

Sitio web: http://www.zone-h.org

Los ciberdelincuentes son humanos, y como tales suelen contar con las mismas virtudes y defectos humanos que nos caracterizan. Uno de ellos es el deseo de reconocimiento.

Zone-H es una base de datos de sitios web que han sido víctimas de un ataque de deface o modificación ilegítima. Este sitio web es comúnmente usado por ciberdelincuentes para publicar sus ataques exitosos de defacement y mostrarlos al mundo. Esto es especialmente útil para detectar la existencia de un sitio web de nuestro entorno que pueda haber sido comprometido por un ataque de este tipo.

XSSed

Sitio web: http://www.xssed.com

Se trata de una base de datos de sitios web que son vulnerables a ataques de XSS.

Clean-MX

Sitio web: http://support.clean-mx.com

Se trata de una base de datos de amenazas en tiempo real. En ésta podemos consultar una lista de sitios web que han sido relacionados con algún tipo de amenaza:

- Sitios web con malwares.
- Sitios web con phishing.
- Sitios web comprometidos por algún tipo de ataque.

Por cada una de las entradas ofrece enlaces a otros recursos de análisis (p.Ej: VirusTotal, ThreatExpert, Avira, Comodo, ...) que nos permiten profundizar en un análisis.

El equipo de Clean-MX además, en caso de detectar una amenaza manda una notificación a la cuenta de correo "abuse" asociada al dominio afectado.

Secureless

Sitio web: http://secureless.org

Se trata de una base de datos de sitios web que son vulnerables y han sido víctimas de algún ataque. Es posible acceder a diferentes categorías de ataques como modificaciones ilegítimas (defacement), inyecciones SQL, XSS, subida de ficheros, etc.

4.6 BASES DE DATOS DE VULNERABILIDADES

A diario se publican una gran cantidad de vulnerabilidades. Un equipo de seguridad debería estar al día de las vulnerabilidades que se publican para los sistemas y programas que se usan en la organización. Contar por tanto con recursos que nos permitan acceder a información detallada de las vulnerabilidades que nos afectan es de gran utilidad.

MITRE CVE

Sitio web: https://cve.mitre.org

Lista de información registrada sobre conocidas vulnerabilidades de seguridad, donde cada referencia tiene un número de identificación único. De esta forma provee una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

Fue definido y es mantenido por The MITRE Corporation (por eso a veces a la lista se la conoce por el nombre MITRE CVE List) con fondos de la National Cyber Security Division del gobierno de los Estados Unidos de América. Forma parte del llamado Security Content Automation Protocol.

NVD (National Vulnerability Database)

Sitio web: http://web.nvd.nist.gov

Es el repositorio del gobierno de los EEUU de información sobre vulnerabilidades.

CVE Details

Sitio web: http://www.cvedetails.com

Se trata de un sitio web con una base de datos de vulnerabilidades que nos permite buscarlas de forma rápida y ofrecernos información detallada al respecto. Tiene un interfaz basado en un estilo de hoja de cálculo, que te permite navegar fácilmente por los expedientes CVE asociados a fabricantes de software y productos. Además, por cada listado, puedes clasificar los expedientes CVE por criticidad del mismo, número de exploits públicos o fecha, lo que permite acceder a datos interesantes de manera muy rápida. También,permite buscar por otros códigos de expedientes como los BID, los códigos de Microsoft y en todo momento enlaza con la base de datos de Metasploit para indicarte si existe un exploit asociado a ese CVE en el framework. Además de Metasploit, los expedientes CVE tienen asociadas las referencias a exploits en Internet, en webs de exploits, por ejemplo Exploit-db.

OSVDB

Sitio web: http://osvdb.org

Es una base de datos abierta e independiente de vulnerabilidades. Proporciona información técnica, detallada, actual e imparcial sobre vulnerabilidades que pueden afectar a diversas plataformas y aplicaciones.

Este proyecto Open Source tiene por objetivo que la comunidad internauta disponga de una base de datos de vulnerabilidades de libre distribución, que sea actualizada con el esfuerzo de todo aquel que desee aportar su granito de arena y que sea independiente de fabricantes y necesidades comerciales.

5 CONCLUSIONES

Actuar de forma responsable y ser cautos mientras nos movemos por la red es algo básico para mantenernos seguros. Pero además, al igual que en nuestros hogares tenemos un botiquín con material sanitario para las emergencias, es muy recomendable contar con nuestro "botiquín" especial para los peligros que acechan por Internet.

En este documento hemos querido aportar unas pocas herramientas que nos podrán ser de utilidad cuando, por ejemplo, nos envíen un archivo en un correo un conocido o cuando entremos en un sitio web que no conocemos. Así, en caso de tropezar con algo que pudiese ser dañino podamos contar con recursos que nos ayuden a identificarlos a tiempo y prevenir el mal que pudiera causarnos.