



## *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*  
Nº de Páginas: *1 de 18*

<i>Informe de divulgación Recursos de Seguridad en Línea</i>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 2 de 18	

## 1 TABLA DE CONTENIDOS

<a href="#"><u>TABLA DE CONTENIDOS.....</u></a>	<a href="#"><u>2</u></a>
<a href="#"><u>OBJETO Y ALCANCE.....</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>INTRODUCCIÓN.....</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>RECURSOS DE SEGURIDAD EN LÍNEA.....</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>ANÁLISIS DE ARCHIVOS SOSPECHOSOS y SANDBOXES.....</u></a>	<a href="#"><u>3</u></a>
<a href="#"><u>ANÁLISIS DE URL's.....</u></a>	<a href="#"><u>8</u></a>
<a href="#"><u>MOTORES DE REPUTACION Y LISTAS NEGRAS.....</u></a>	<a href="#"><u>9</u></a>
<a href="#"><u>BASE DE DATOS DE SPAM Y PHISHING.....</u></a>	<a href="#"><u>11</u></a>
<a href="#"><u>BASES DE DATOS DE SITIOS COMPROMETIDOS.....</u></a>	<a href="#"><u>14</u></a>
<a href="#"><u>BASES DE DATOS DE VULNERABILIDADES.....</u></a>	<a href="#"><u>16</u></a>
<a href="#"><u>CONCLUSIONES.....</u></a>	<a href="#"><u>18</u></a>

<i>Informe de divulgación Recursos de Seguridad en Línea</i>	Código	<i>CERT-IF-6032-010914</i>
	Edición	<i>0</i>
	Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 3 de 18

## 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.

<b>Informe de divulgación</b> <b>Recursos de Seguridad en Línea</b>		Código	CERT-IF-6032-010914
		Edición	0
		Fecha	01/09/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 4 de 18	

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.



The screenshot shows the VirusTotal homepage. At the top is the VirusTotal logo. Below it, a text block states: "VirusTotal es un servicio gratuito que analiza archivos y URLs sospechosas facilitando la rápida detección de virus, gusanos, troyanos y todo tipo de malware." There are three tabs: "Archivo" (selected), "URL", and "Buscar". Below the tabs is a search input field with the text "No hay archivo seleccionado" and a "Seleccionar" button. Underneath, it says "Tamaño máximo: 64MB". At the bottom, there is a blue "Analizar" button and a disclaimer: "Al hacer click en 'Analizar', acepta nuestros Términos del servicio y permite que VirusTotal comparta este fichero con la comunidad de seguridad. Vea nuestra Política de privacidad para más detalles."

<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 5 de 18	

## Wepawet

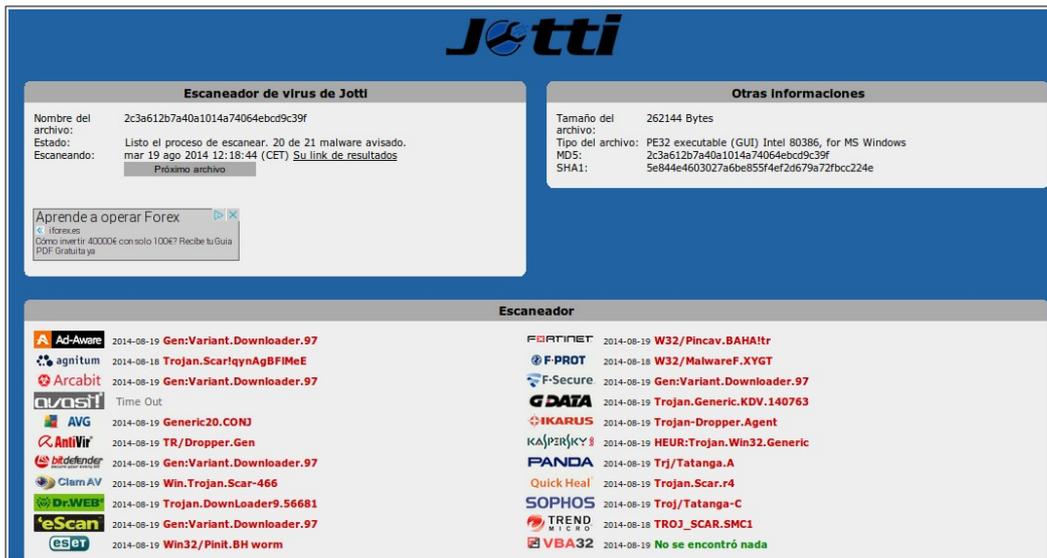
Sitio web: <http://wepawet.cs.ucsb.edu>

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.



The screenshot shows the Jotti Virus Scan interface. At the top, the Jotti logo is displayed. Below it, there are two main sections: 'Escaneador de virus de Jotti' and 'Otras informaciones'.

**Escaneador de virus de Jotti:**

- Nombre del archivo: 2c3a612b7a40a1014a74064ebcd9c39f
- Estado: Listo el proceso de escanear. 20 de 21 malware avisado.
- Escaneado: mar 19 ago 2014 12:18:44 (CET) [Su link de resultados](#)
- Próximo archivo: [Botón]

**Otras informaciones:**

- Tamaño del archivo: 262144 Bytes
- Tipo del archivo: PE32 executable (GUI) Intel 80386, for MS Windows
- MDS: 2c3a612b7a40a1014a74064ebcd9c39f
- SHA1: 5e844e4603027a6be855f4ef2d679a72fbcc224e

Below these sections, there is a link: 'Aprende a operar Forex' with a play button icon.

**Escaneador:**

A grid of antivirus engines and their results:

Ad-Aware	2014-08-19	Gen:Variant.Downloader.97	Fortinet	2014-08-19	W32/Pincav.BAH!tr
agnitum	2014-08-18	Trojan.Scar!qynAgBFMeE	F-PROT	2014-08-18	W32/MalwareF.XYGT
Arcabit	2014-08-19	Gen:Variant.Downloader.97	F-Secure	2014-08-19	Gen:Variant.Downloader.97
avast!	Time Out		GDATA	2014-08-19	Trojan.Generic.KDV.140763
AVG	2014-08-19	Generic20.CONJ	IKARUS	2014-08-19	Trojan-Dropper.Agent
AntiVir	2014-08-19	TR/Dropper.Gen	KASPERSKY	2014-08-19	HEUR:Trojan.Win32.Generic
BitDefender	2014-08-19	Gen:Variant.Downloader.97	PANDA	2014-08-19	Trj/Tatanga.A
ClamAV	2014-08-19	Win.Trojan.Scar-466	Quick Heal	2014-08-19	Trojan.Scar.r4
Dr.Web	2014-08-19	Trojan.Downloader9.56681	SOPHOS	2014-08-19	Troj/Tatanga-C
eScan	2014-08-19	Gen:Variant.Downloader.97	TREND	2014-08-18	TROJ_SCAR.SMCI
eset	2014-08-19	Win32/Pinkt.BH worm	VBA32	2014-08-19	No se encontró nada

## SANDBOXES 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.

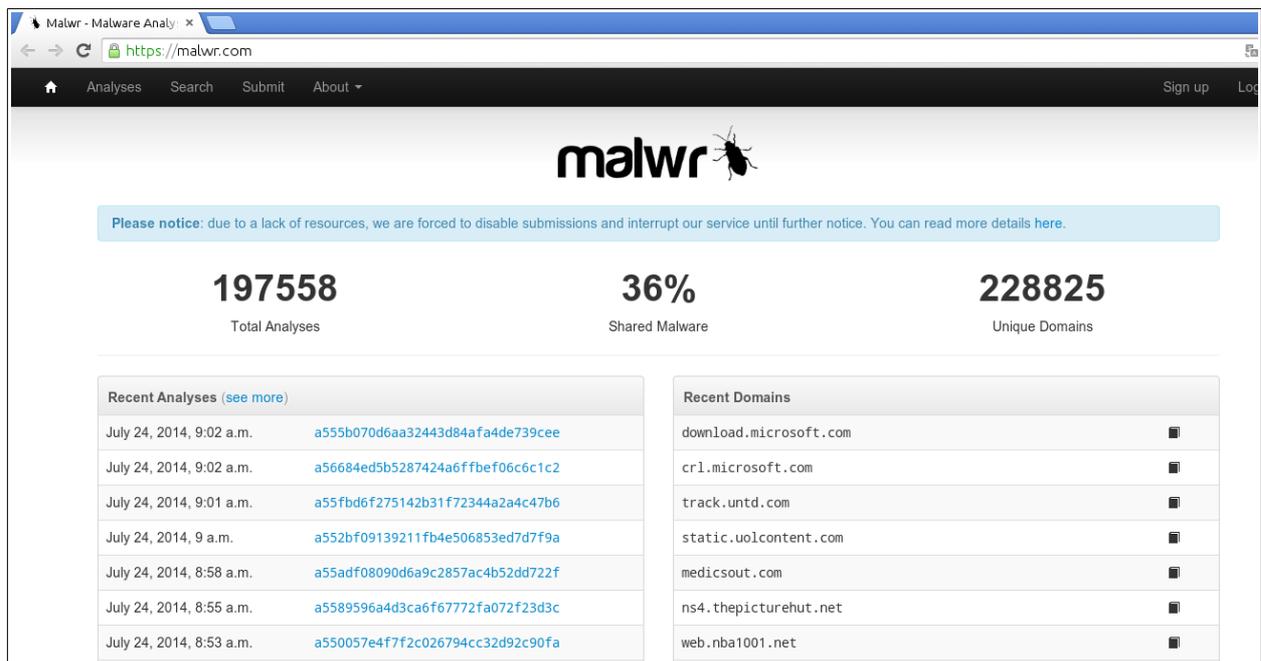
<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	CERT-IF-6032-010914
		Edición	0
		Fecha	01/09/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 6 de 18	

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.



The screenshot shows the Malwr website interface. At the top, there is a navigation bar with 'Analyses', 'Search', 'Submit', and 'About' links, along with 'Sign up' and 'Log' options. The main header features the 'malwr' logo with a bug icon. Below the header, a blue notice box states: 'Please notice: due to a lack of resources, we are forced to disable submissions and interrupt our service until further notice. You can read more details here.' The main content area displays three large statistics: '197558 Total Analyses', '36% Shared Malware', and '228825 Unique Domains'. Below these statistics are two tables: 'Recent Analyses (see more)' and 'Recent Domains'. The 'Recent Analyses' table lists several entries with timestamps and hashes. The 'Recent Domains' table lists domains like 'download.microsoft.com', 'cr1.microsoft.com', 'track.untd.com', 'static.uolcontent.com', 'medicsout.com', 'ns4.thepicturehut.net', and 'web.nba1001.net'.

## Anubis

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

Anubis es otro 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.

<i>Informe de divulgación Recursos de Seguridad en Línea</i>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 7 de 18	

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.



The screenshot shows the ThreatExpert website. At the top, there is a navigation menu with links for Home, ThreatExpert Reports, Tools, Threat Browser, Submit Sample, and About ThreatExpert. Below the menu, a 'Welcome to ThreatExpert' section describes the system as an advanced automated threat analysis tool. To the right, there is a search bar and links for 'Sign In' and 'Register'. The main content area features a 'Geographic Distribution of Threats' section with a world map and a donut chart. The donut chart shows the distribution of threats by country, with the Russian Federation being the largest category, followed by the United States, Spain, Germany, United Kingdom, and Brazil. A list of malware samples is displayed on the left side of the page.

Malware	Adware
Trojan.Llineage.Gen1Pac.3	
Trojan.Popuper	
Worm.IM.Sohanad	
Application.Ardamax_Keylogger	
Email-Worm.Brontok	
Win32.Virut.Gen.5	
RogueAntiSpyware.AntiVirusPro	
Worm.Hamweg.Gen	
Win32.Salty.AM.Gen	
Rootkit.Podnuha.Gen.2	

En el siguiente [enlace](#) podrá encontrar un ejemplo informe realizado tras el análisis de un malware.

<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. <b>8</b> de 18	

## 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.

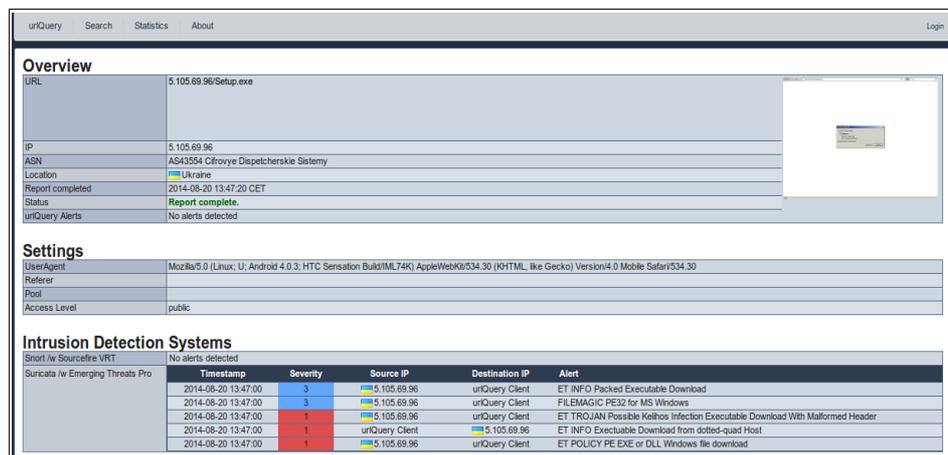
### URLQuery

Sitio web: <http://urlquery.net>

Realiza la petición al sitio sospechoso, actuando como intermediario y detectando si existe alguna amenaza 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.



The screenshot shows the URLQuery web interface. The 'Overview' section displays details for a URL: 5.105.69.96/Setup.exe, including its IP, ASN (AS43554), location (Ukraine), and report completion time (2014-08-20 13:47:20 CET). The 'Settings' section shows the UserAgent string: Mozilla/5.0 (Linux; U; Android 4.0.3; HTC Sensation Build/ML74K) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30. The 'Intrusion Detection Systems' section shows a table of alerts detected by Suricata Iw Emerging Threats Pro.

Timestamp	Severity	Source IP	Destination IP	Alert
2014-08-20 13:47:00	3	5.105.69.96	urlQuery Client	ET INFO Packed Executable Download
2014-08-20 13:47:00	3	5.105.69.96	urlQuery Client	FILEMAGIC PE32 for MS Windows
2014-08-20 13:47:00	1	5.105.69.96	urlQuery Client	ET TROJAN Possible Keilhos Infection Executable Download With Malformed Header
2014-08-20 13:47:00	1	urlQuery Client	5.105.69.96	ET INFO Executable Download from dotted-quad Host
2014-08-20 13:47:00	1	5.105.69.96	urlQuery Client	ET POLICY PE EXE or DLL Windows file download

<i>Informe de divulgación Recursos de Seguridad en Línea</i>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 9 de 18

### **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.

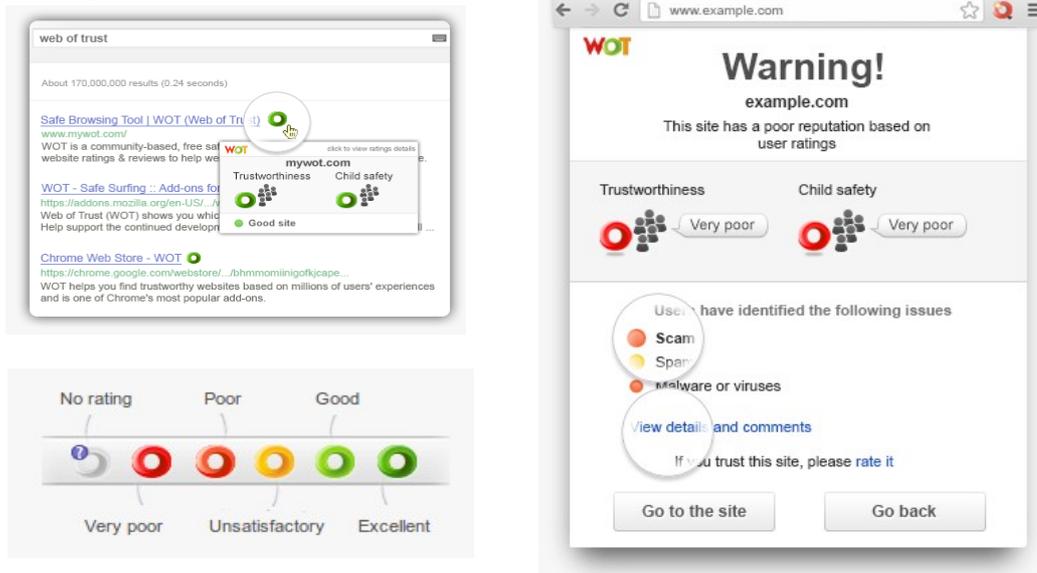
<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	CERT-IF-6032-010914
		Edición	0
		Fecha	01/09/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 10 de 18	

## 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.

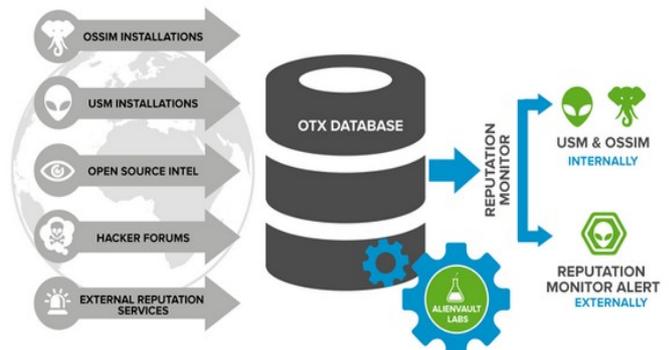
La reputación se basa en distintos factores como la presencia de malware, la identificación de páginas de phishing alojadas o la existencia de contenido ofensivo. Sin embargo, la valoración que más se tiene en cuenta es la opinión de los usuarios. Éstos pueden votar y establecer valoraciones que influirán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



<i>Informe de divulgación Recursos de Seguridad en Línea</i>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. <b>11</b> de 18	

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 phishing. Esto nos permite tenerlos identificados o denunciarlos.

### Phistank

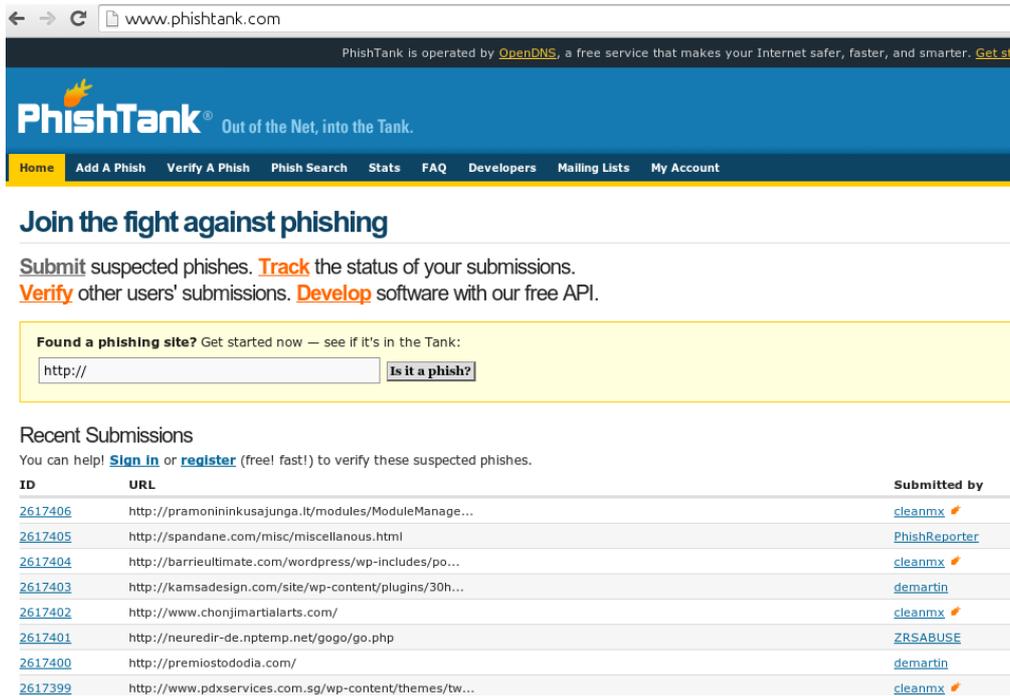
Sitio web: <http://www.phishtank.com>

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.

<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	CERT-IF-6032-010914
		Edición	0
		Fecha	01/09/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 12 de 18	

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...).



www.phishtank.com

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started](#)

# PhishTank®

Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

## Join the fight against phishing

**Submit** suspected phishes. **Track** the status of your submissions.  
**Verify** other users' submissions. **Develop** software with our free API.

**Found a phishing site?** Get started now — see if it's in the Tank:

[Is it a phish?](#)

### Recent Submissions

You can help! [Sign in](#) or [register](#) (free! fast!) to verify these suspected phishes.

ID	URL	Submitted by
<a href="#">2617406</a>	<a href="http://pramonininkusajunga.it/modules/ModuleManage...">http://pramonininkusajunga.it/modules/ModuleManage...</a>	<a href="#">cleanmx</a>
<a href="#">2617405</a>	<a href="http://spandane.com/misc/miscellaneous.html">http://spandane.com/misc/miscellaneous.html</a>	<a href="#">PhishReporter</a>
<a href="#">2617404</a>	<a href="http://barrieultimate.com/wordpress/wp-includes/po...">http://barrieultimate.com/wordpress/wp-includes/po...</a>	<a href="#">cleanmx</a>
<a href="#">2617403</a>	<a href="http://kamsadesign.com/site/wp-content/plugins/30h...">http://kamsadesign.com/site/wp-content/plugins/30h...</a>	<a href="#">demartin</a>
<a href="#">2617402</a>	<a href="http://www.chonjimartialarts.com/">http://www.chonjimartialarts.com/</a>	<a href="#">cleanmx</a>
<a href="#">2617401</a>	<a href="http://neuredir-de.nptemp.net/gogo/go.php">http://neuredir-de.nptemp.net/gogo/go.php</a>	<a href="#">ZRSABUSE</a>
<a href="#">2617400</a>	<a href="http://premiostododia.com/">http://premiostododia.com/</a>	<a href="#">demartin</a>
<a href="#">2617399</a>	<a href="http://www.pdxservices.com.sg/wp-content/themes/tw...">http://www.pdxservices.com.sg/wp-content/themes/tw...</a>	<a href="#">cleanmx</a>

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.

<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	CERT-IF-6032-010914
		Edición	0
		Fecha	01/09/2014
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 13 de 18	

## 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.

**Email header analysis report**

All valid IP Addresses found in the header.

IP Address	3rd Party Info	Provider	City	Flag	Country
* 82.135.212.71	 	Joint Stock Company Lietuvos Telekomas	n/a		Lithuania
213.142.144.54	 	Hosting Network	n/a		Turkey

\*Probable originating IP address

---

Header Analysis

Originating Info	Email info	Geographical Info
Originating IP address 82.135.212.71	From Grupo Banco Santander <ces@bancosant>	Continent Europe
Originating hostname 82-135-212-71.static.zebra.lt	Originating Email address ces@bancosantader.es	Latitude 56
Originating Organization Joint Stock Company Lietuvos Telekomas	Subject	Longitude 24
Originating Country Lithuania	Date Sent 14 Aug 2014 18:20:19 +0300	Time zone n/a
Originating City n/a	Message ID	GMT offset n/a

Google Map for 82.135.212.71



<i>Informe de divulgación Recursos de Seguridad en Línea</i>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. <b>14</b> de 18

## **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.

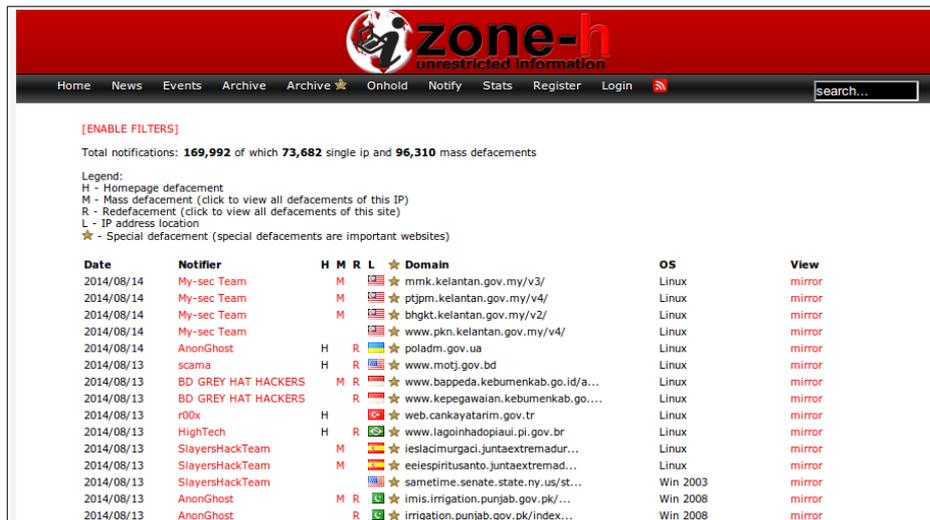
## **Zone-H**

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.

<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	CERT-IF-6032-010914
		Edición	0
		Fecha	01/09/2014
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. 15 de 18



Date	Notifier	H	M	R	L	Domain	OS	View
2014/08/14	My-sec Team		M			mmk.kelantan.gov.my/v3/	Linux	mirror
2014/08/14	My-sec Team		M			ptjpm.kelantan.gov.my/v4/	Linux	mirror
2014/08/14	My-sec Team		M			bhgt.kelantan.gov.my/v2/	Linux	mirror
2014/08/14	My-sec Team		M			www.pkn.kelantan.gov.my/v4/	Linux	mirror
2014/08/14	AnonGhost	H		R		poladm.gov.ua	Linux	mirror
2014/08/13	scama	H		R		www.motj.gov.bd	Linux	mirror
2014/08/13	BD GREY HAT HACKERS		M	R		www.bappeda.kebumekab.go.id/a...	Linux	mirror
2014/08/13	BD GREY HAT HACKERS		R			www.kepegawaian.kebumekab.go...	Linux	mirror
2014/08/13	r00x	H		R		web.cankayatarim.gov.tr	Linux	mirror
2014/08/13	HighTech	H		R		www.lagoindahopiaui.pi.gov.br	Linux	mirror
2014/08/13	SlayersHackTeam		M			ieslacimurgaci.juntaextremadur...	Linux	mirror
2014/08/13	SlayersHackTeam		M			eeiespirtusanto.juntaextremad...	Linux	mirror
2014/08/13	SlayersHackTeam		M			sametime.senate.state.ny.us/st...	Win 2003	mirror
2014/08/13	AnonGhost		M	R		imis.irrigation.punjab.gov.pk/...	Win 2008	mirror
2014/08/13	AnonGhost		R			irrigation.punjab.gov.pk/index...	Win 2008	mirror

## 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.

<i>Informe de divulgación Recursos de Seguridad en Línea</i>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>		Categoría: <i>Público</i>	Pág. <b>16</b> de 18

## 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.



...[<Vulnerabilities: Latest>]

Status	Type	Name	URL
Unreported	Cross Site Scripting	Clinica Santa Maria	<a href="http://www.clinicasantamaria.cl/">http://www.clinicasantamaria.cl/</a>
Fixed	Source Code Disclosure	Banco BCI	<a href="http://www.bci.cl/">http://www.bci.cl/</a>
Unreported	Cross Site Scripting	E-Pagos, EFT Group (Nextel)	<a href="https://nextel.e-pagos.cl/">https://nextel.e-pagos.cl/</a>
Unreported	Cross Site Scripting	E-Pagos, EFT Group (ScotiaBank)	<a href="https://scotiabank.e-pagos.cl/">https://scotiabank.e-pagos.cl/</a>
Unreported	Cross Site Scripting	E-Pagos, EFT Group (Entel)	<a href="https://entelpcseftgestion.e-pagos.cl/">https://entelpcseftgestion.e-pagos.cl/</a>
Fixed	Data Leak	EFT Group	<a href="https://www.eftgroup.cl/">https://www.eftgroup.cl/</a>
Fixed	Cross Site Scripting	EFT Group	<a href="https://www.eftgroup.cl/">https://www.eftgroup.cl/</a>
Unreported	Cross Site Scripting	Banco Itau Chile	<a href="https://www.itau.cl/">https://www.itau.cl/</a>
Unreported	Cross Site Scripting	Gangas	<a href="http://www.gangas.cl/">http://www.gangas.cl/</a>
Unreported	Full Path Disclosure	Municipalidad de Santiago	<a href="http://tramites.munistgo.cl/">http://tramites.munistgo.cl/</a>
Unreported	Data Leak	Municipalidad de Santiago	<a href="http://tramites.munistgo.cl/">http://tramites.munistgo.cl/</a>
Reported	Data Leak	Casino Express	<a href="http://www.casinoexpress.cl/">http://www.casinoexpress.cl/</a>
Unreported	Cross Site Scripting	Claro Chile	<a href="http://hogar.clarochile.cl/">http://hogar.clarochile.cl/</a>
Unreported	SQL Injection	Paris Porn Movies	<a href="http://www.parispornmovies.biz">http://www.parispornmovies.biz</a>
Unreported	Cross Site Scripting	Just Milf GFS	<a href="http://www.justmilfgfs.com">http://www.justmilfgfs.com</a>

## 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.

<b>Informe de divulgación Recursos de Seguridad en Línea</b>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. 17 de 18	

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.

<i>Informe de divulgación Recursos de Seguridad en Línea</i>		Código	<i>CERT-IF-6032-010914</i>
		Edición	<i>0</i>
		Fecha	<i>01/09/2014</i>
Tipo de documento: <i>Informe</i>	Categoría: <i>Público</i>	Pág. <b>18</b> de 18	

## 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.