SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

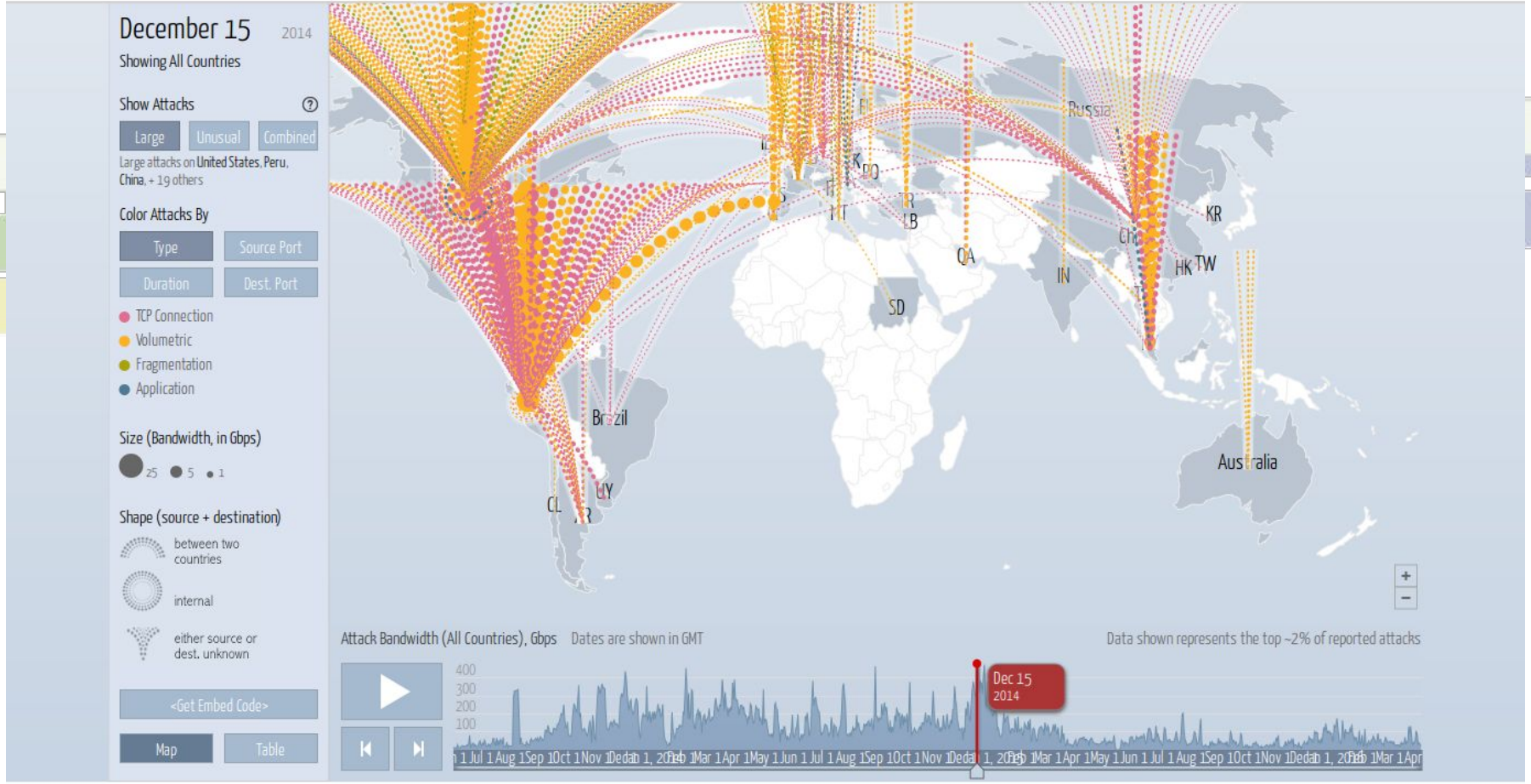
CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

BOTNETS, ROOTKITS Y BACKDOORS

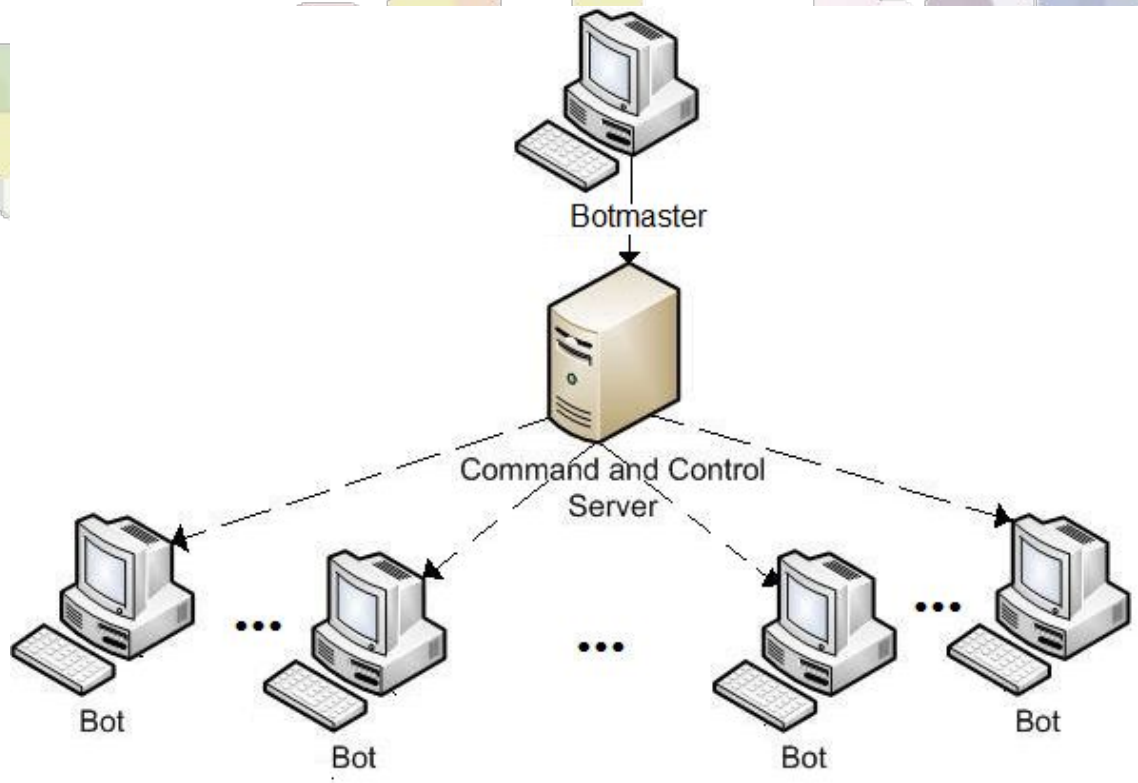
SERVIDORES EN LA MIRA DEL CIBERCRIMEN

Ataques DDoS en el mundo

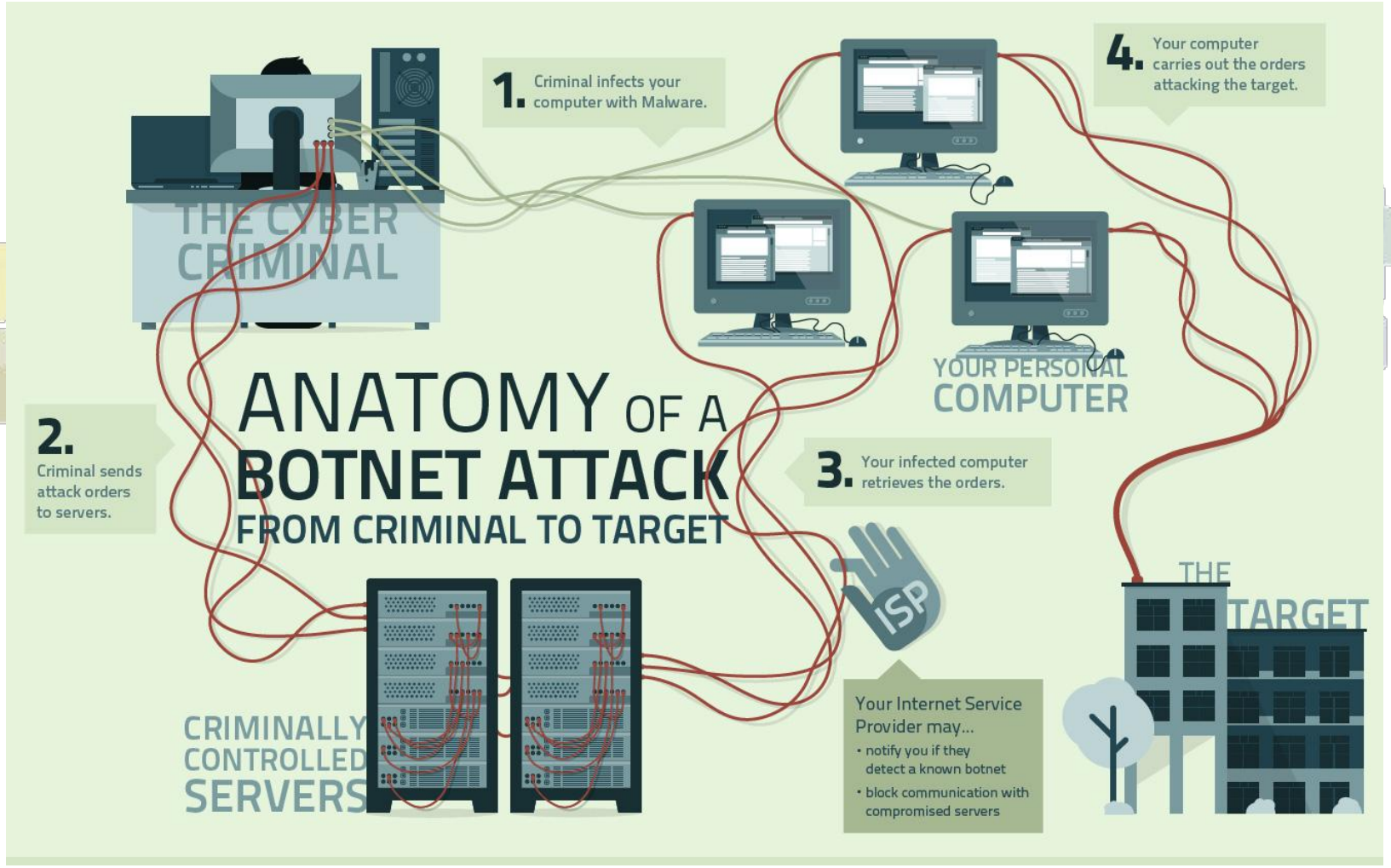


Botnets

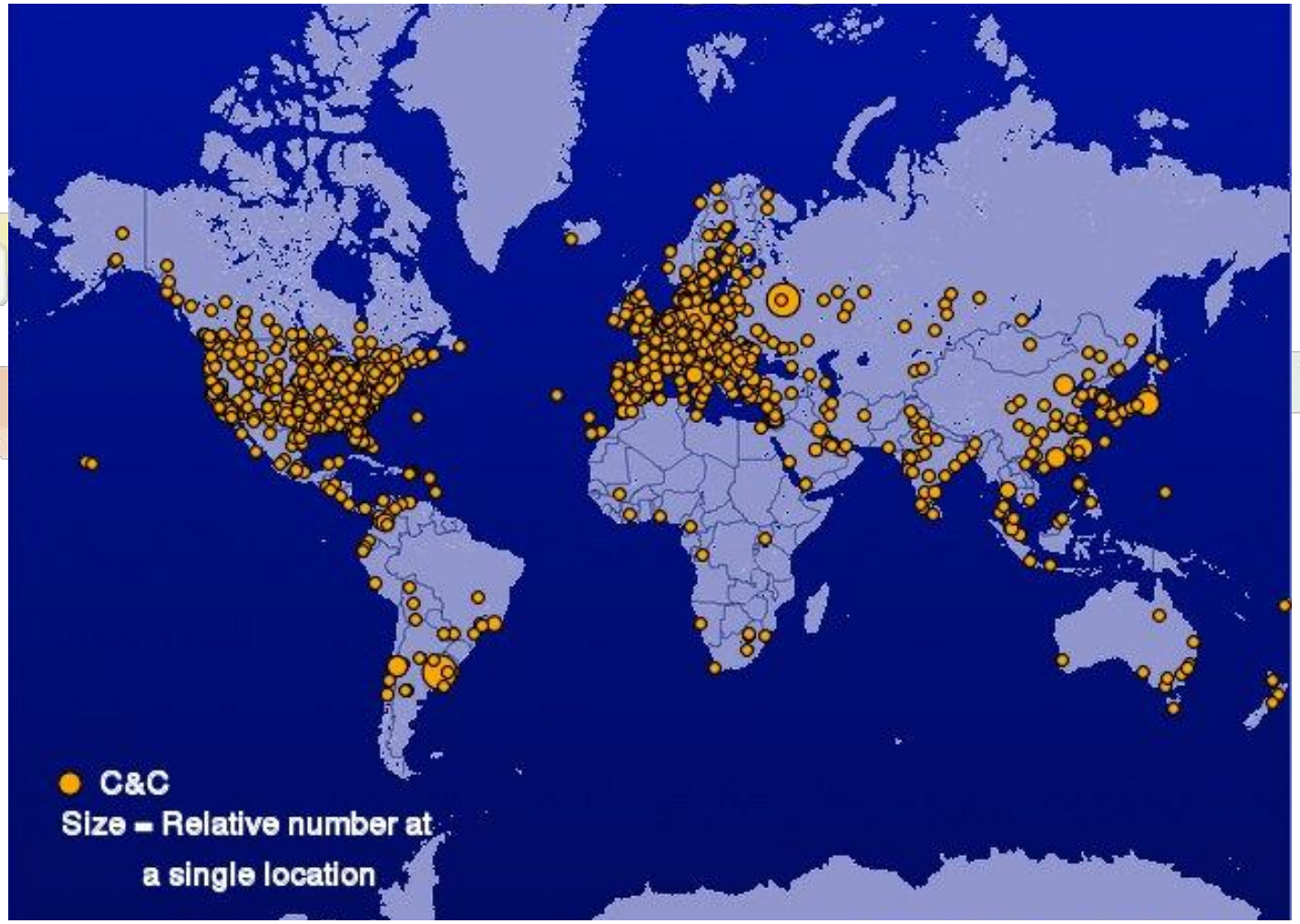
Red de equipos infectados (bots o zombies) controlada por el artífice de la botnet (botmaster) de forma remota, por lo general a través de servidores de Comando y Control (C&C).



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

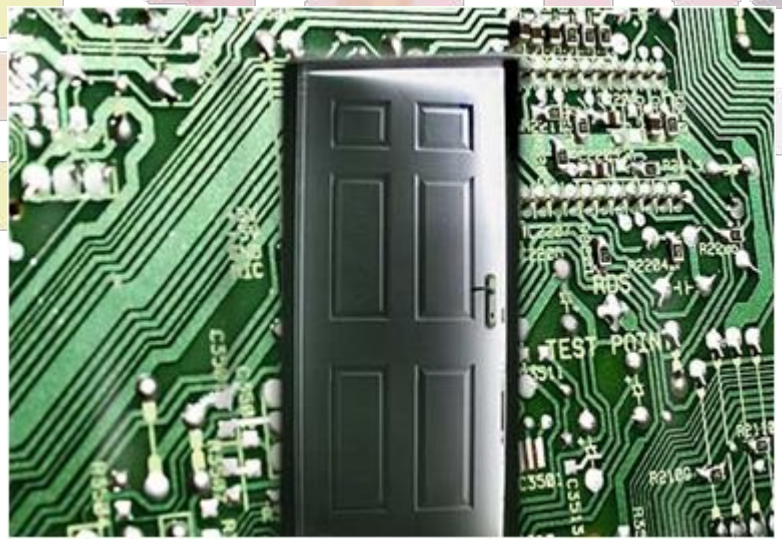
¿Cómo entran? ...

SECRETARÍA
NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

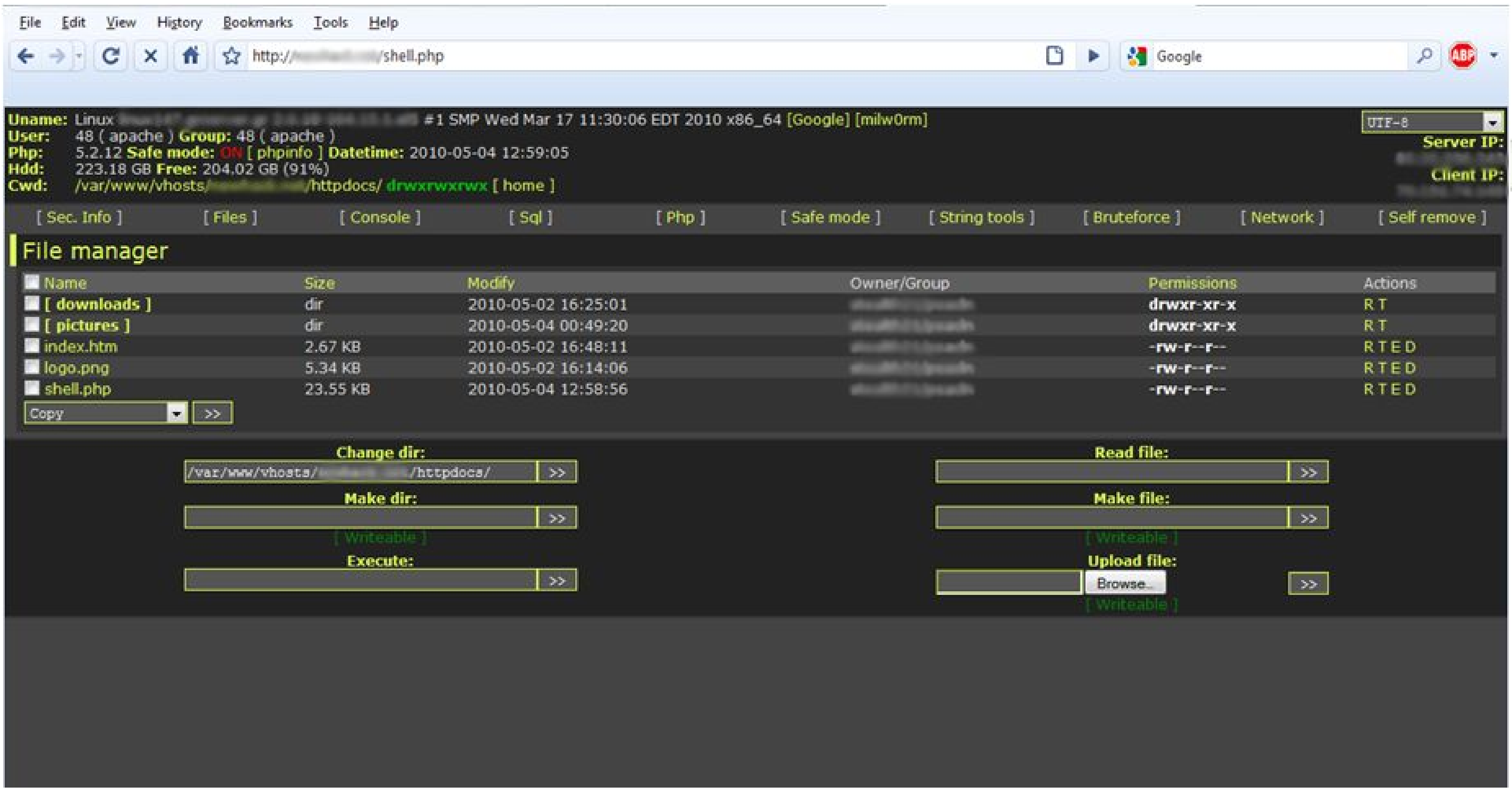
CERT-PY

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@IBTeam:~# nc -lvp 4444
listening on [any] 4444 ...
192.168.1.33: inverse host lookup failed: Unknown server error : Connectio
connect to [192.168.1.34] from (UNKNOWN) [192.168.1.33] 1057
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
[root@dvwa ~]# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program n
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN      3146/mysqld
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN      1798/sshd
tcp        0      0 127.0.0.1:25                0.0.0.0:*                   LISTEN      999/sendmail:
tcp        0      0 0.0.0.0:4444                0.0.0.0:*                   LISTEN      3473/nc
tcp        0      0 :::80                       :::*                        LISTEN      2743/httpd
tcp        0      0 :::22                       :::*                        LISTEN      1798/sshd
```

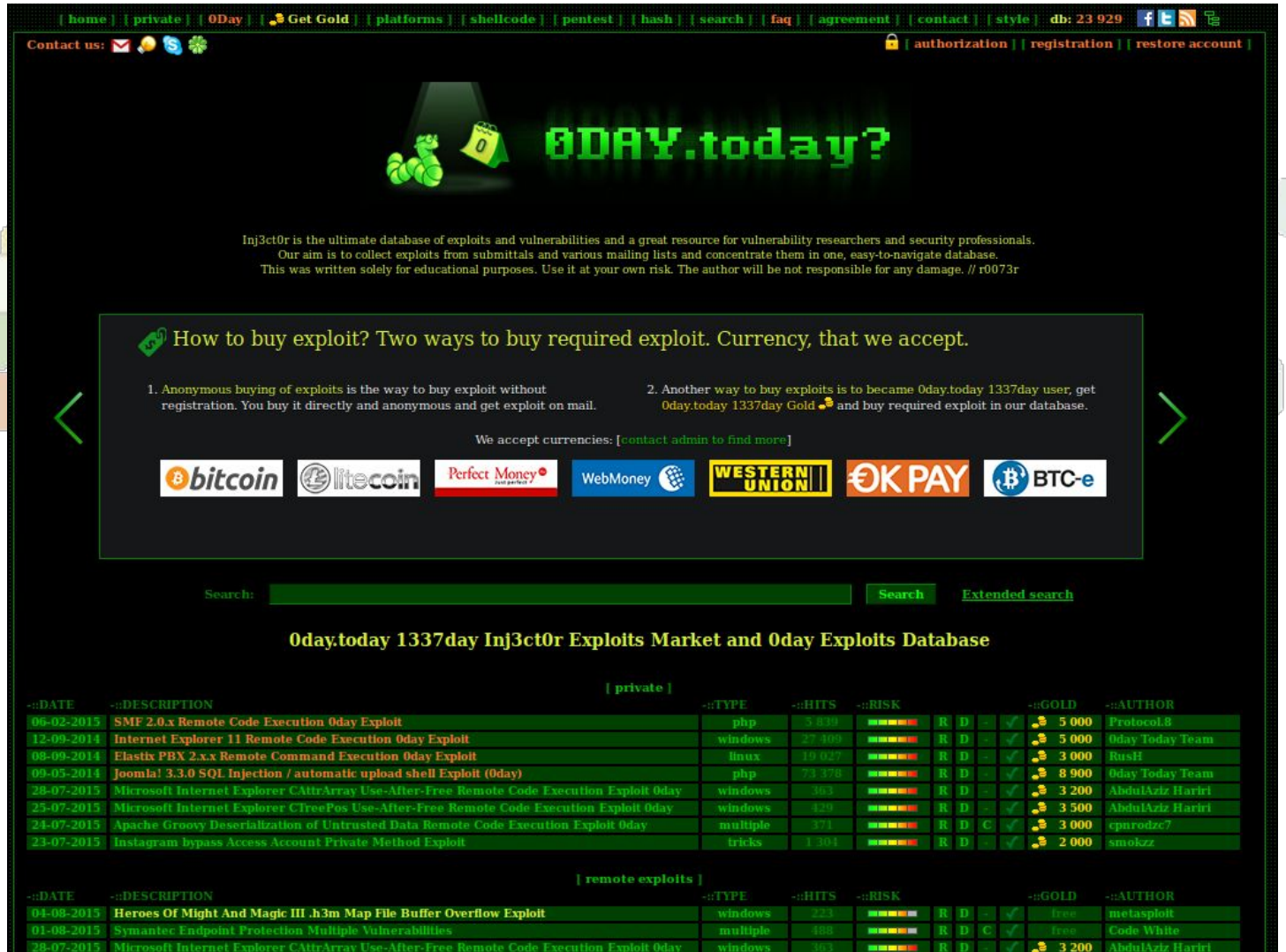
Cuando la webshell no es suficiente..

SECRETARÍA NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

CERT-PY

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo
agendaDigital

Vulnerabilidades y exploits



Escalación de privilegios

Para realizar un daño real y persistente en un sistema, se requiere privilegios de **root**

Explotación de vulnerabilidades → Escalación de privilegios

```
$gcc cve_2016_0728.c -o cve_2016_0728 -lkeyutils -Wall
$./cve_2016_0728 PP1
uid=1000, euid=1000
Increfing...
finished increfing
forking...
finished forking
caling revoke...
uid=0, euid=0
#
# whoami
root
#
```

WELCOME TO HACKER-DEMO

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
- Volatility

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, BIND
  - Zimbra
  - Librerías: OpenSSL, glibC, etc.
  - Paquetes adicionales
- Aplicaciones Web:
  - CMS, Plugins, Plantillas

Contraseña robustas y Buenas prácticas

- Longitud: mínimo 12 caracteres
- 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**

Autenticación de doble factor

Medida de seguridad adicional al usuario y contraseña

Usuario + Contraseña + CÓDIGO DE SEGURIDAD

- Implementación 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:~#
```

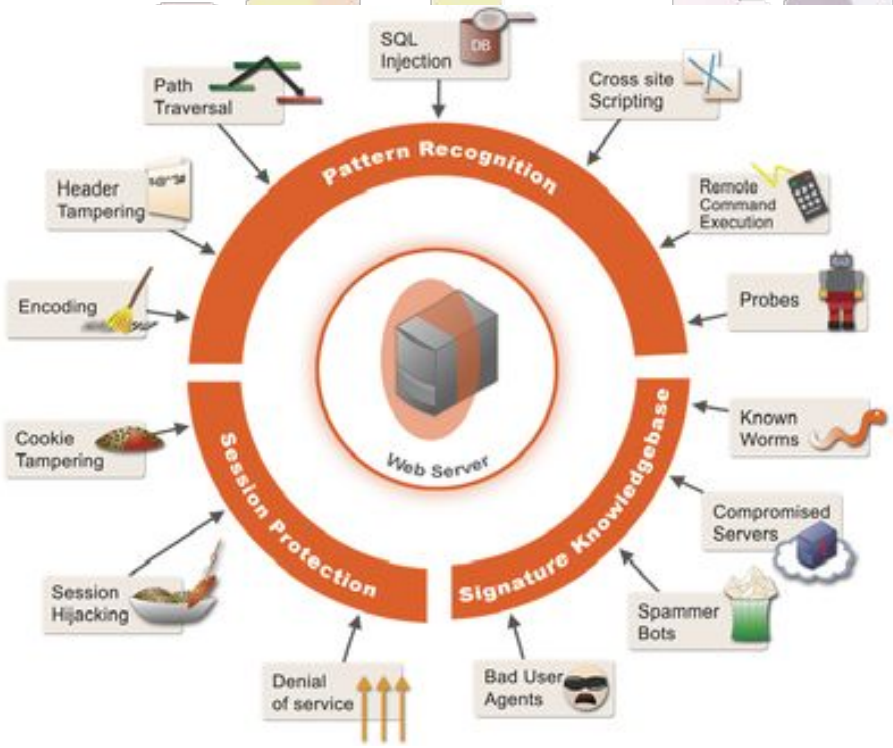
Hardening de SO y aplicaciones

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)

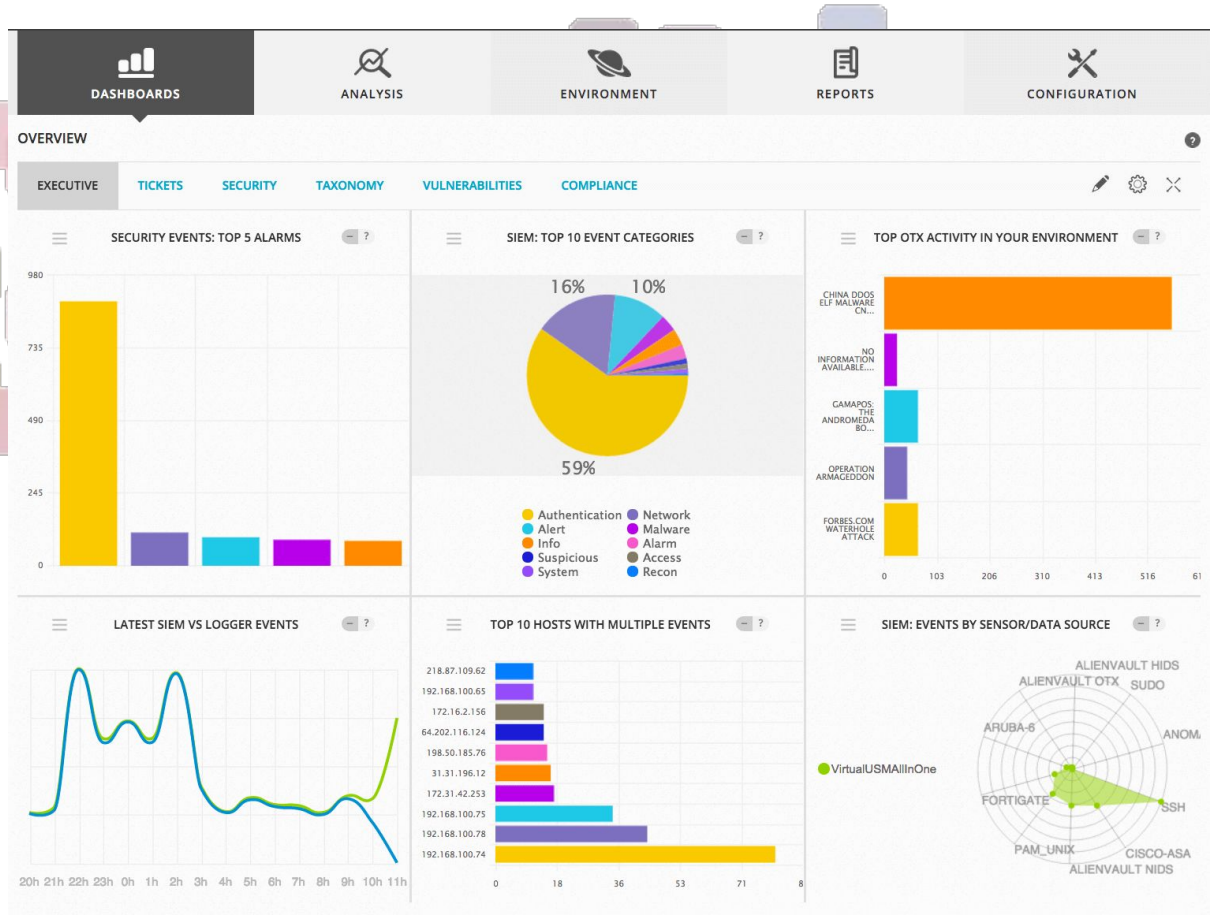
- ModSecurity
- OpenWAF
- Ironbee
- ESAPI WAF



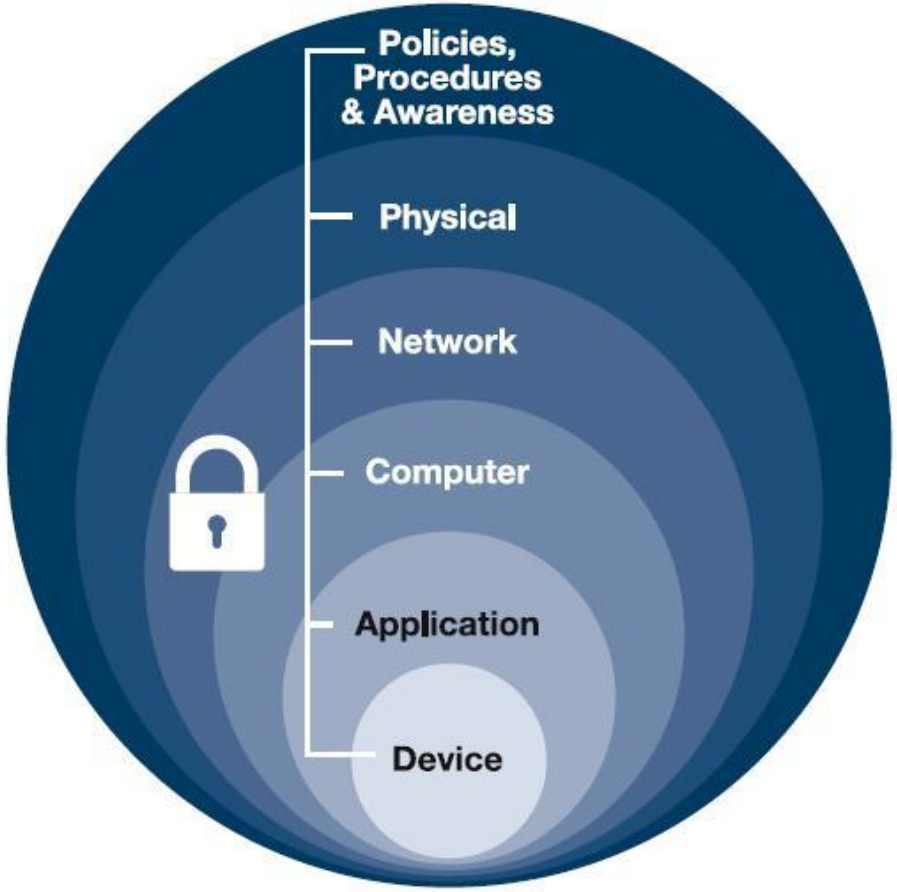
Seguridad Perimetral

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