



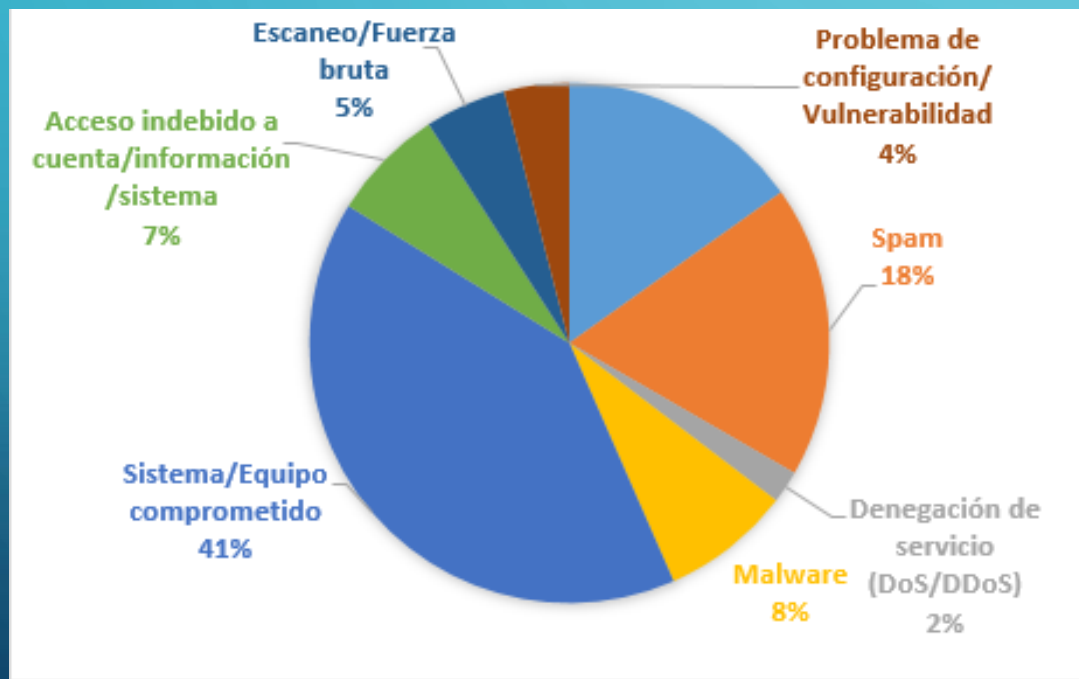
DESDE RANSOMWARE HASTA IOT BOTNETS

¿QUÉ NOS TRAE EL 2017?

Ing. Gabriela Ratti
CERT-PY

ESTADÍSTICAS Y NÚMEROS

TIPOS DE INCIDENTES



✓ Reportes recibidos: **1520**

✓ Incidentes atendidos: **284**

✓ Investigaciones realizadas: **443**

• Fuentes automatizadas:

- > 30,000 eventos por día

RANSOMWARE



RANSOMWARE – MAYOR AMENAZA DEL 2016



Your personal files are encrypted.

Your personal files are encrypted.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' to connect to the secret server and follow instructions.

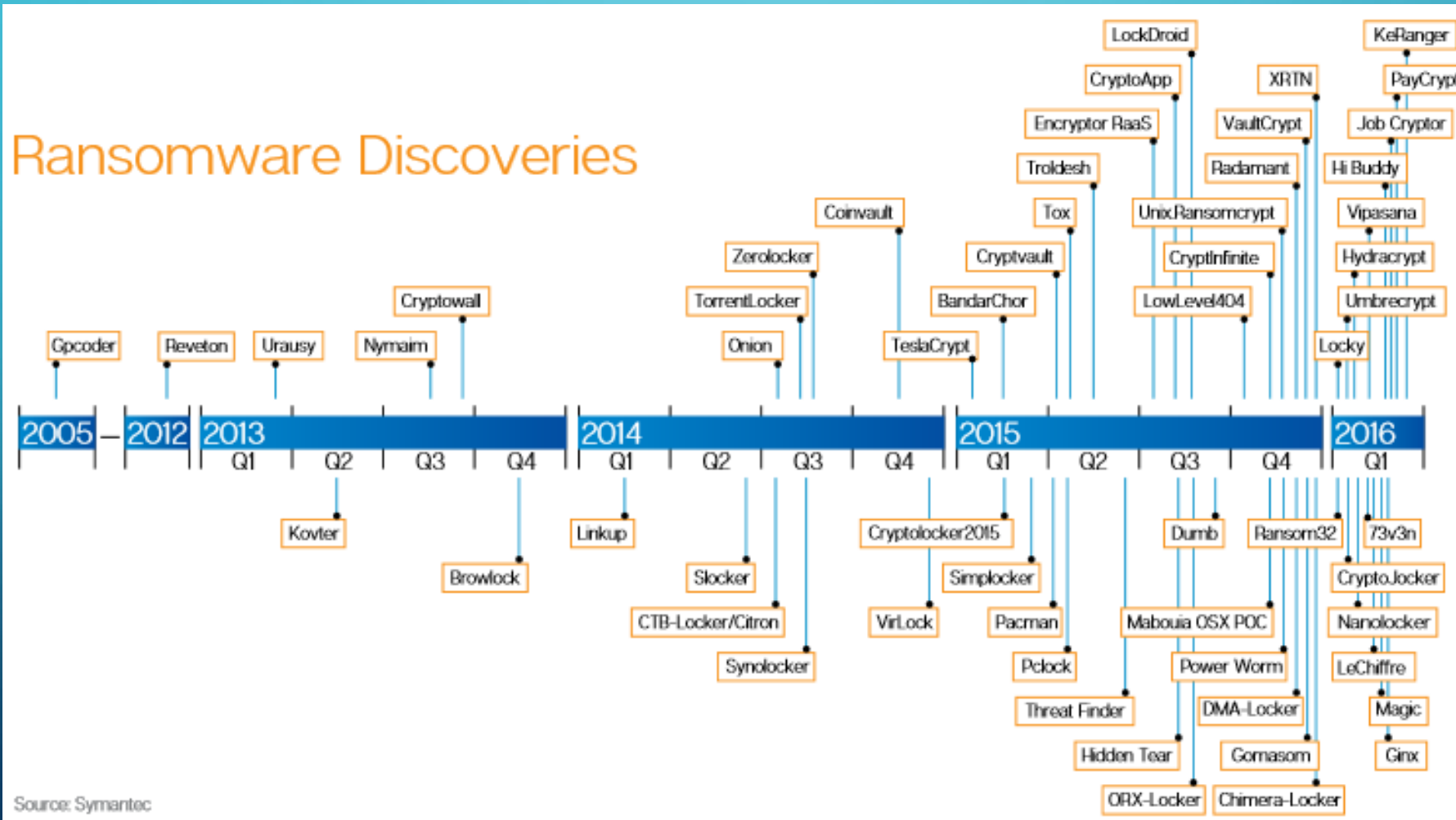
 **WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.**

View **71:59:07** **Next >>**

can open it and use copy-paste for address and key.

EVOLUCIÓN DEL RANSOMWARE

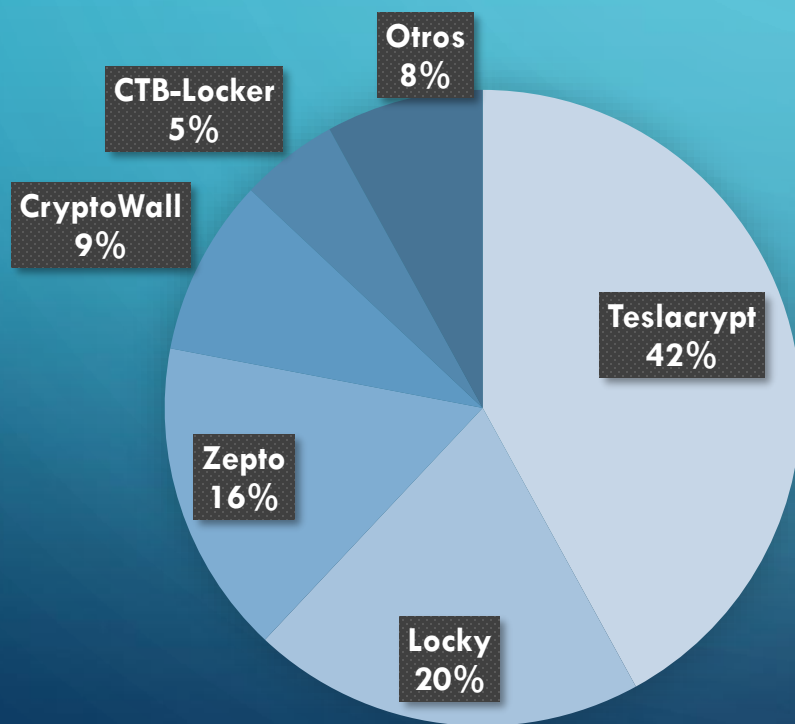
Ransomware Discoveries



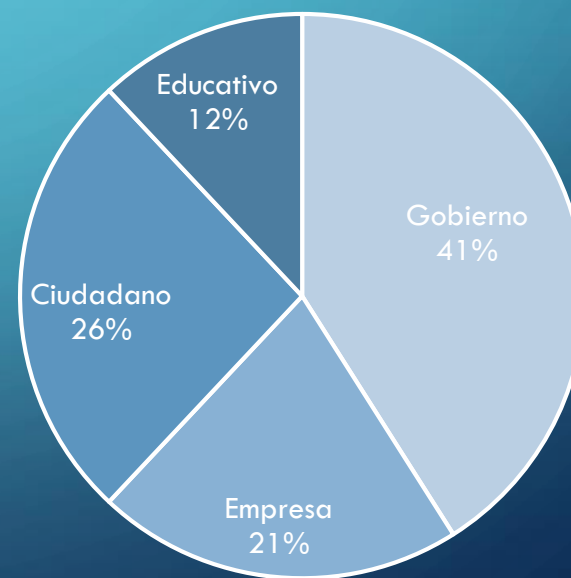
Source: Symantec

EVOLUCIÓN DEL RANSOMWARE

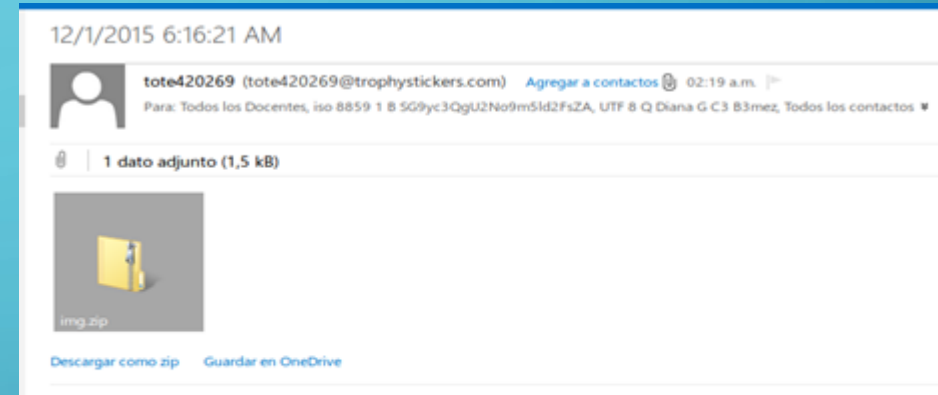
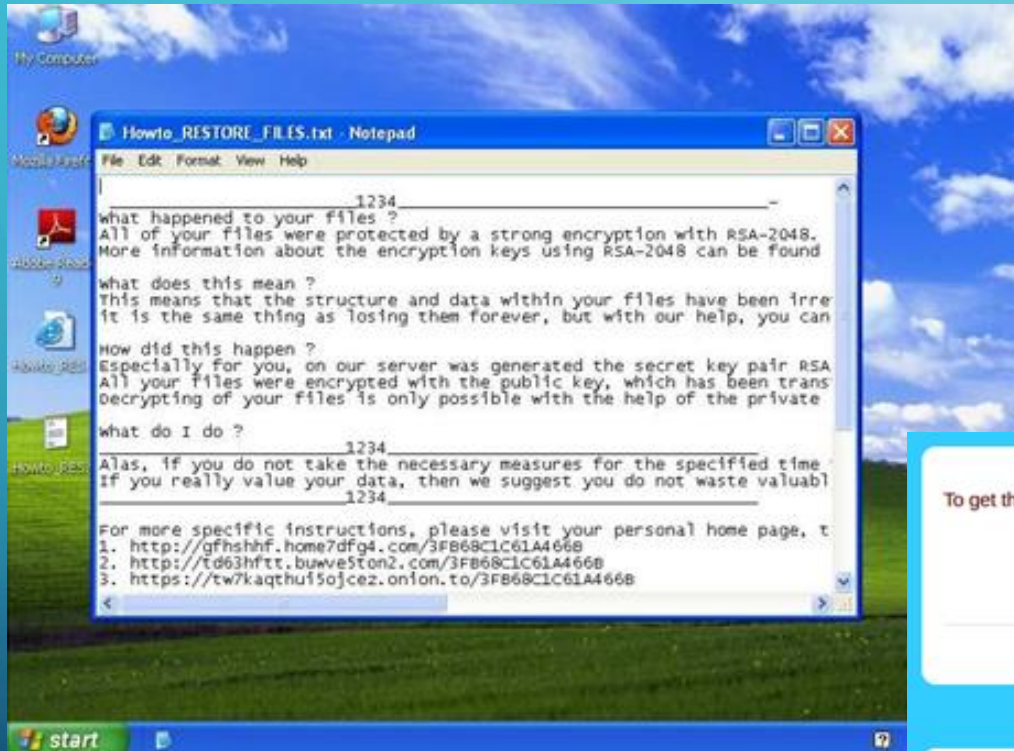
VARIANTES DE RANSOMWARE



SECTOR AFECTADO



TESLACRYPT, UN CASO DE ÉXITO... PARCIAL



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD**. If payment is not made before **02/11/15 - 07:31** the cost of decrypting files will increase **2 times** and will be **1000 USD/EUR**

Prior to increasing the amount left:
167h 50m 13s

Your system: Windows 7 (x64) First connect IP: 186.17.146.251 Total encrypted **21218** files.

[Refresh](#) [Payment](#) [FAQ](#) [Decrypt 1 file for FREE](#) [Support](#)

We give you the opportunity to decipher **1 file** free of charge! You can make sure that the service really works and after payment for the CryptoWall program you can actually decrypt the files.

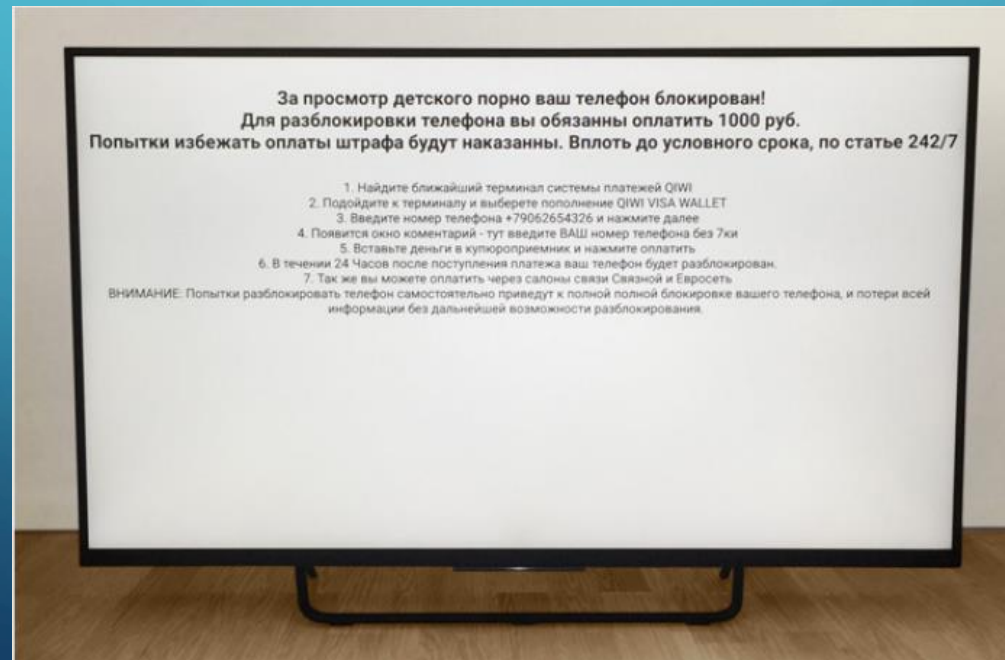
Please select a file to decrypt and load it to the server

Ningún archivo selecciona

Note: file should not be more than 512 kilobytes

TENDENCIAS CON RESPECTO AL RANSOMWARE

- ✓ Los ciberdelincuentes buscan aumentar la presión
- ✓ Vectores de infección con mínima interacción del usuario: drive-by download, fuerza bruta RDP, explotación de vulnerabilidades en la red, etc.
- ✓ No solo computadoras: móviles, servidores web (ransomweb), SmartTV

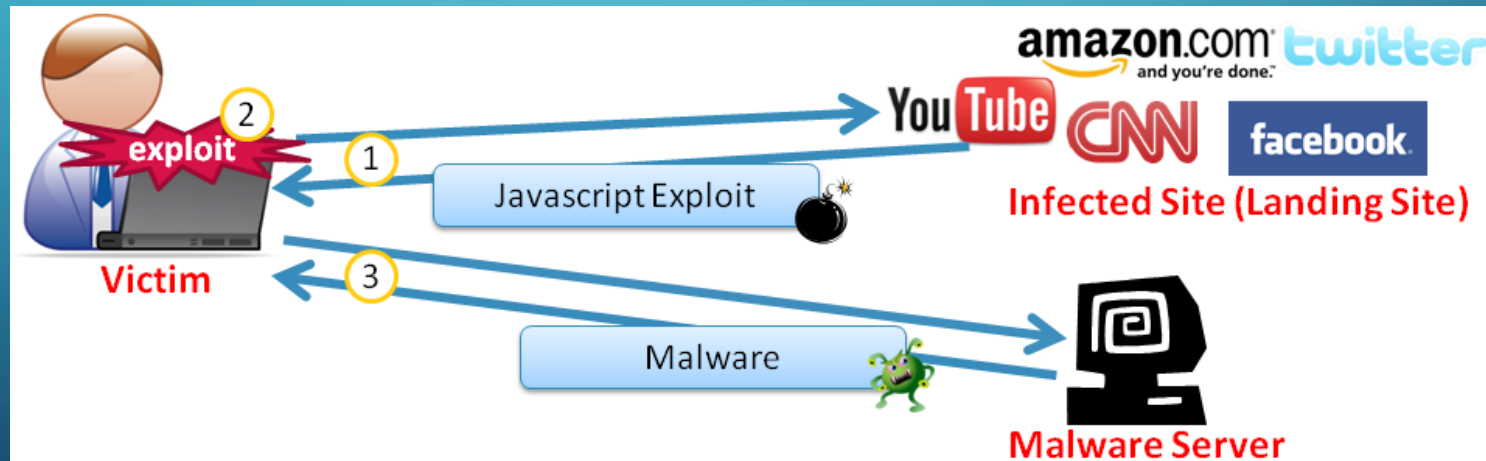


DRIVE-BY DOWNLOAD Y EXPLOIT KITS



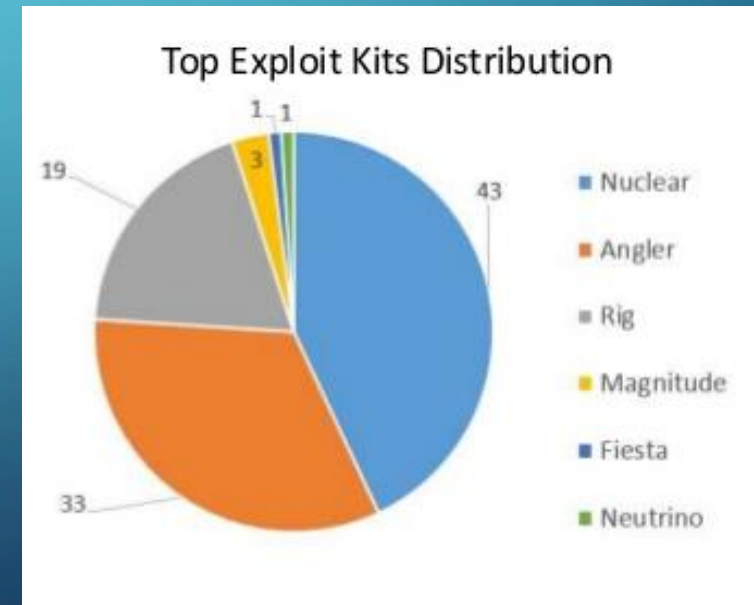
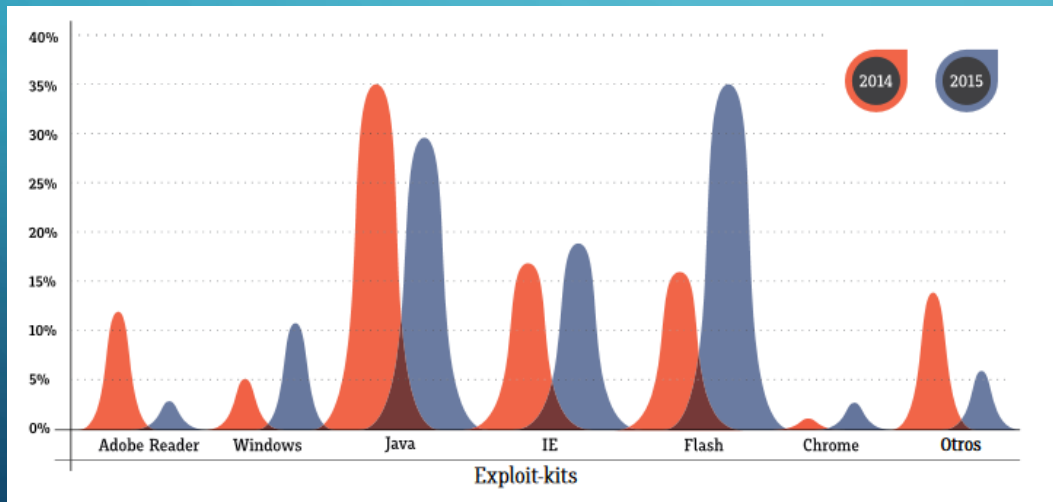
DRIVE-BY DOWNLOAD

Existen técnicas a través de las cuales sólo se requiere que un usuario abra una página web en el navegador para infectarlo.

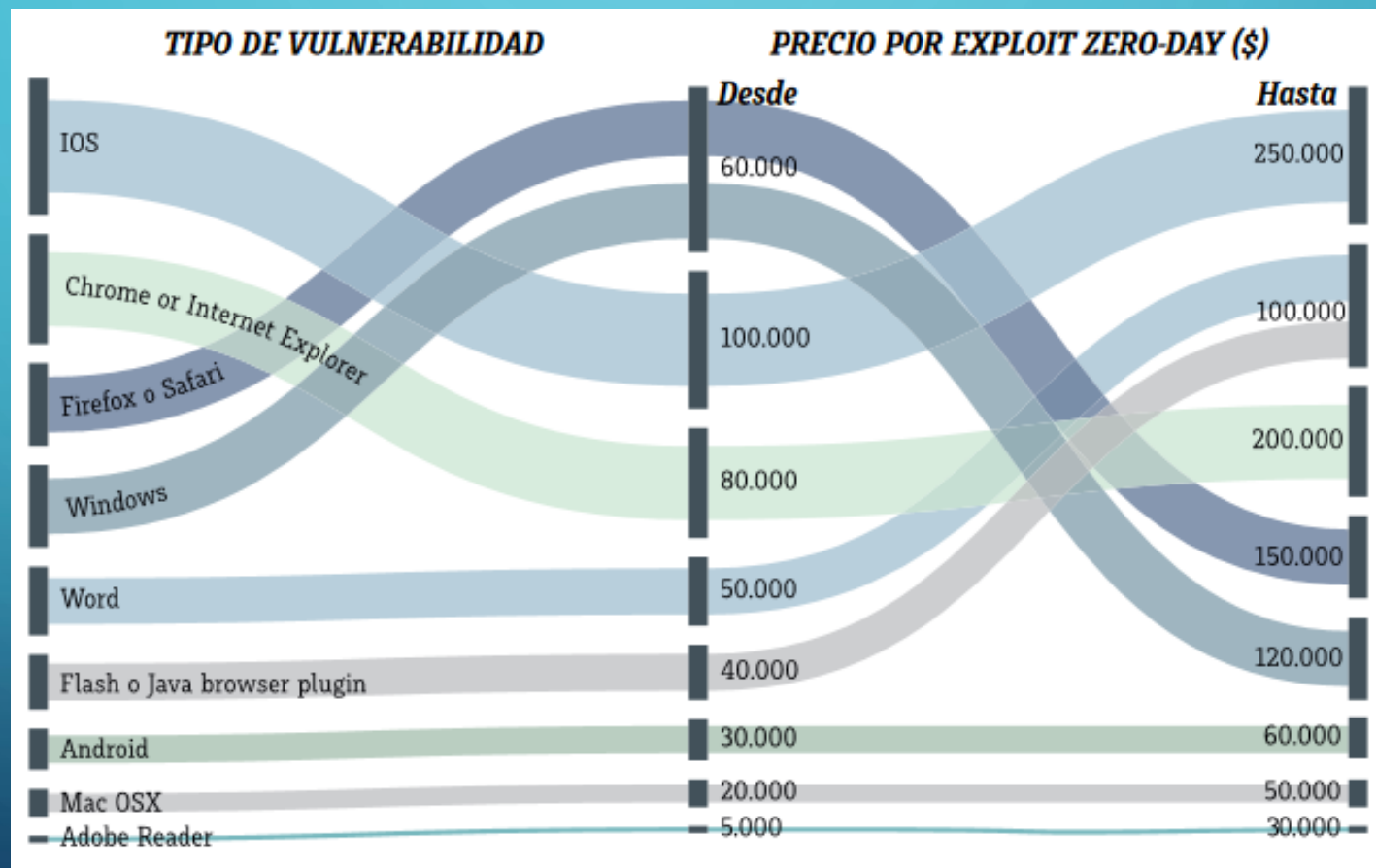


EXPLOIT KITS

Conjunto de herramientas que busca explotar vulnerabilidades en la máquina objetivo, por lo general para instalar malware, extraer información u otras acciones maliciosas.



VULNERABILIDADES ZERO-DAY Y SUS COSTOS



APT's Y ATAQUES DIRIGIDOS



ADVANCED PERSISTENT THREAT

Ataque **dirigido**, con altos niveles **sofisticación** y **recursos**, a través del cual un atacante, por medio de múltiples vectores de ataque (malware, vulnerabilidades, ingeniería social, etc.), intenta de forma **persistente** penetrar la seguridad de un **objetivo específico**, para un **fin específico**.

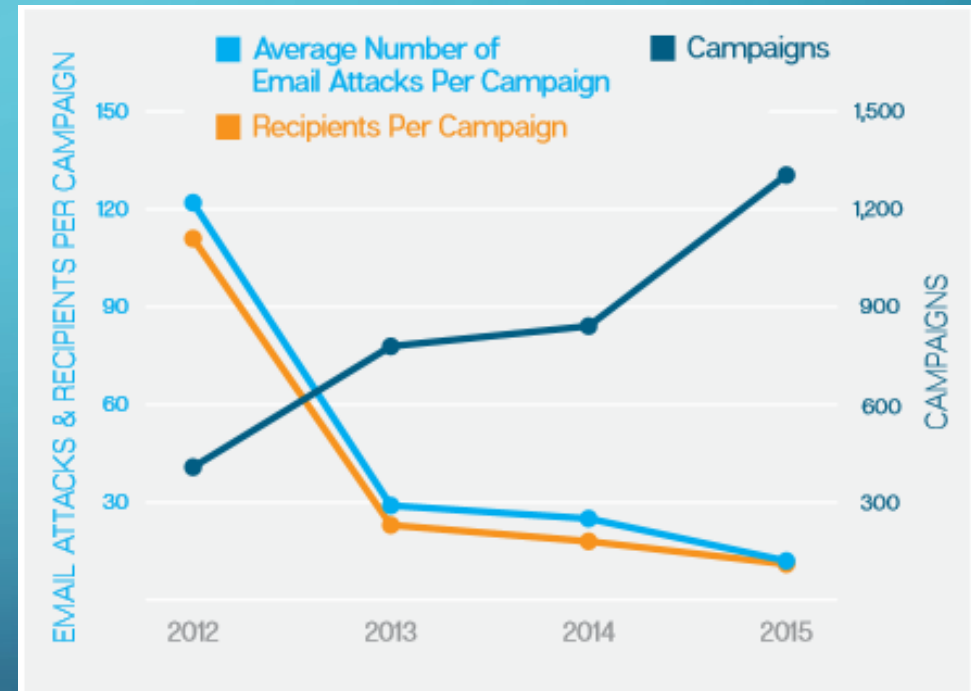
Ejemplo:

STUXNET

- Específico para sistemas SCADA – WinCC/PCS 7 Siemens
- Programado para infectar únicamente la planta de Natanz, Irán
- Aprovechaba 4 vulnerabilidades 0-day
- Estuvo operando como mínimo 5 años antes de ser descubierto

VECTORES DE ATAQUE DE UN APT

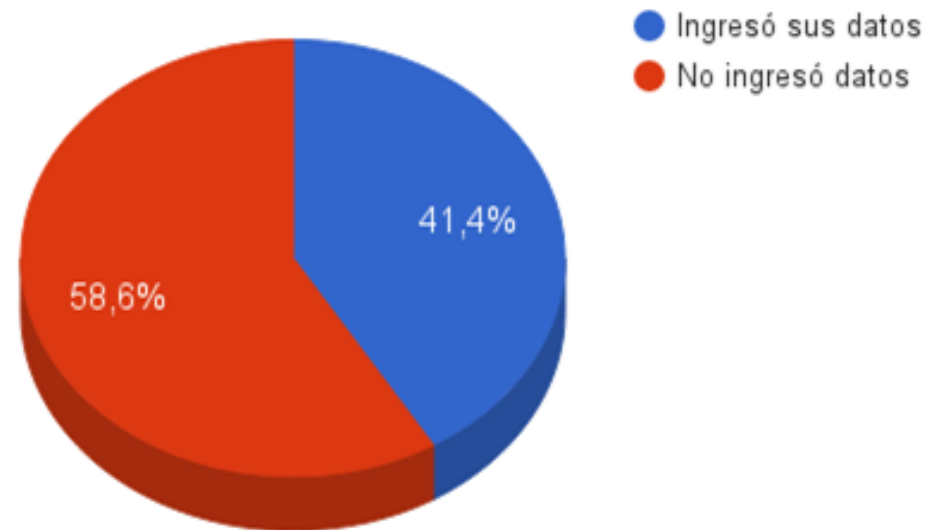
- Spear-phishing
- Watering Hole
- Técnicas de ingeniería social muy dirigidas
- Insiders



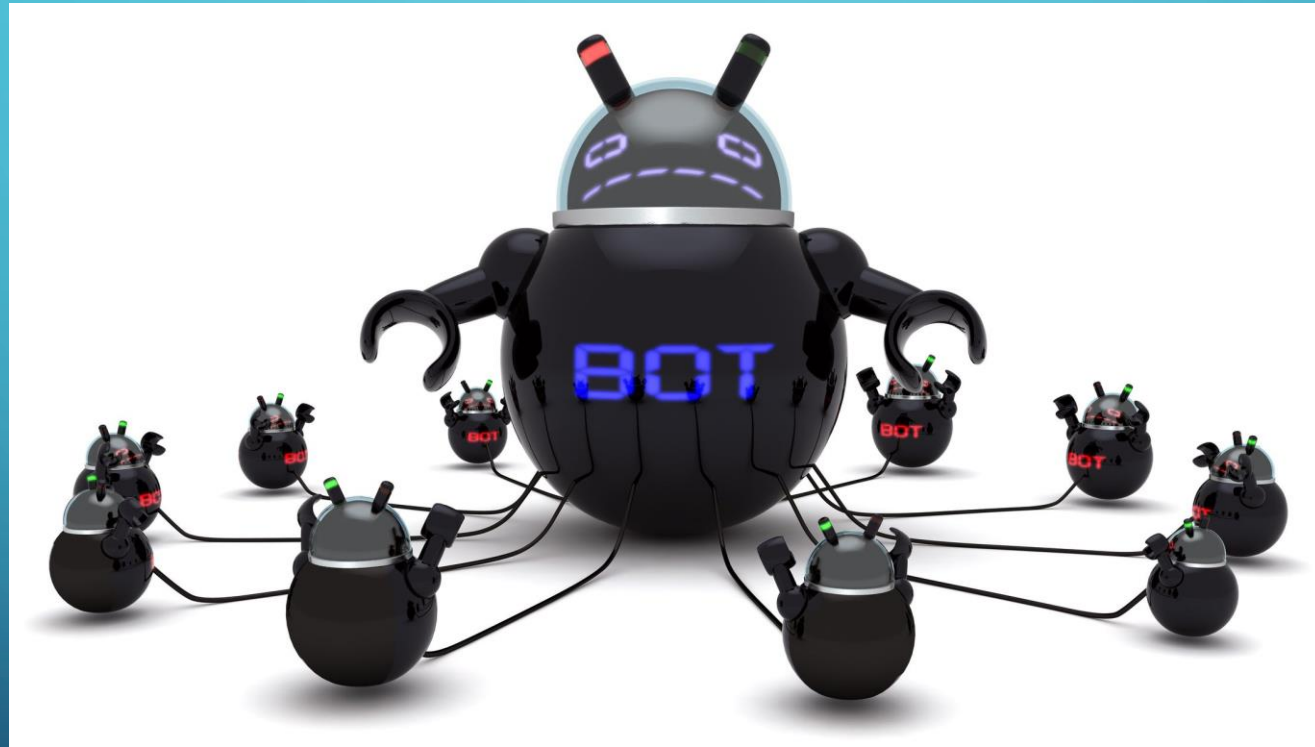
EVOLUCIÓN DE LOS OBJETIVOS

1. Gobierno
2. Sector financiero
3. Servicios críticos
4. Empresas grandes

Efectividad de un ataque dirigido
Simulacro de Phishing

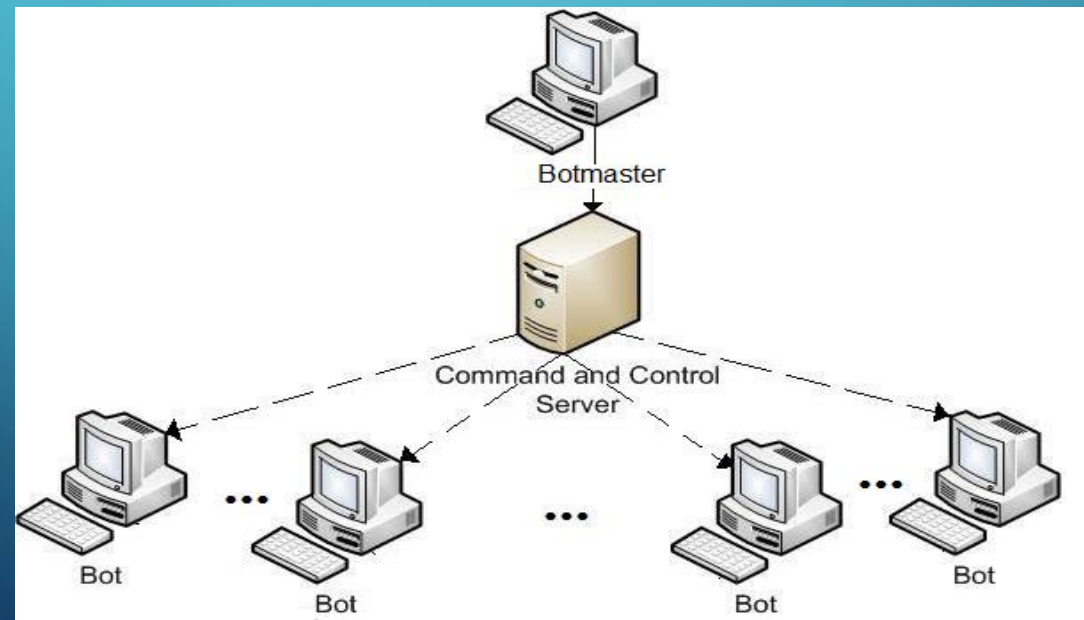


BOTNETS

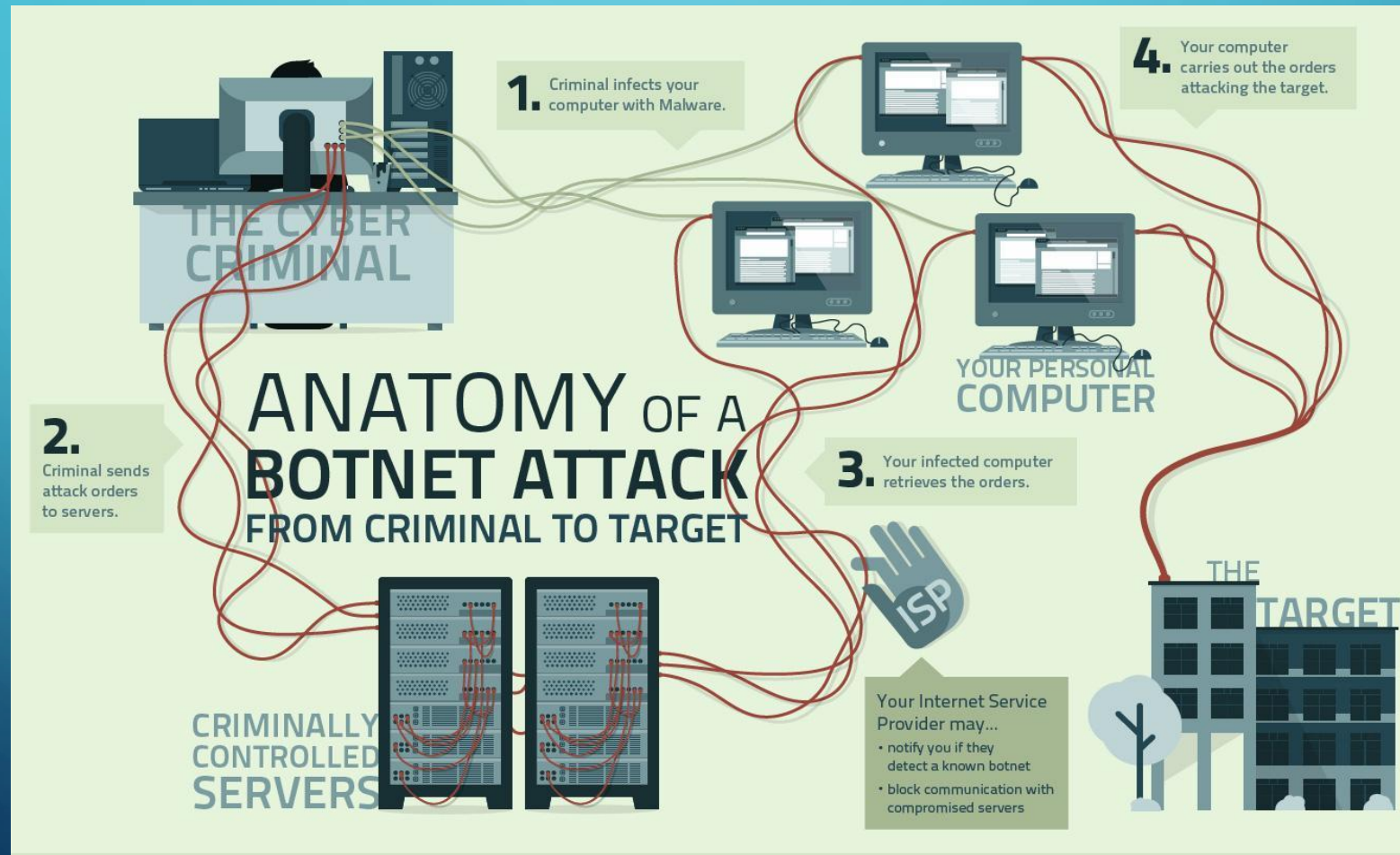


BOTNETS

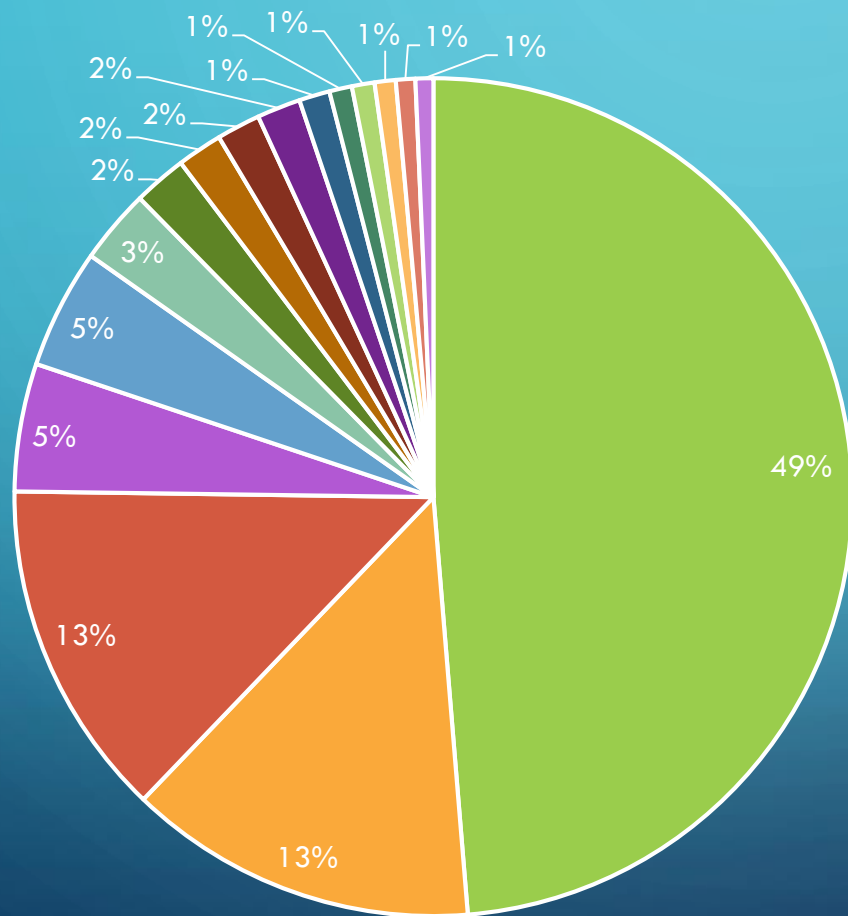
Red de equipos infectados (bots o zombies) controlada por el artífice de la botnet (botmaster) de forma remota, por lo general a través de servidores de Comando y Control (C&C).



FUNCIONAMIENTO DE UNA BOTNET



PRINCIPALES INFECCIONES EN PARAGUAY



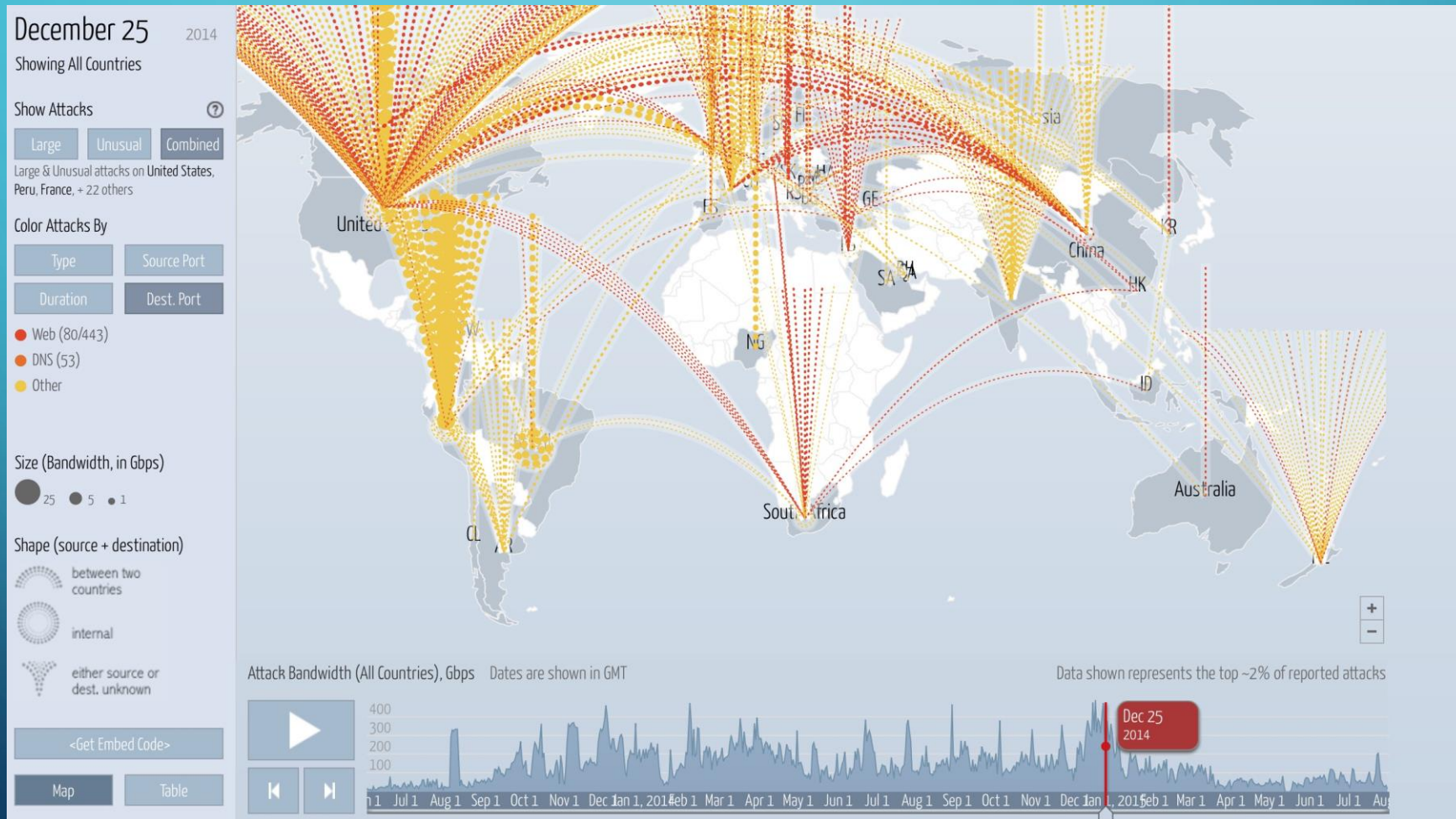
- mirai
- Otros
- dorkbot
- sality-p2p
- renocide
- nivdort
- wauchos
- esfury
- gameover/zeus
- kasidet
- ramnit
- ponmocup
- zero-access
- cutwail/pushdo
- conficker
- pykspa

¿PARA QUÉ BOTNETS?

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



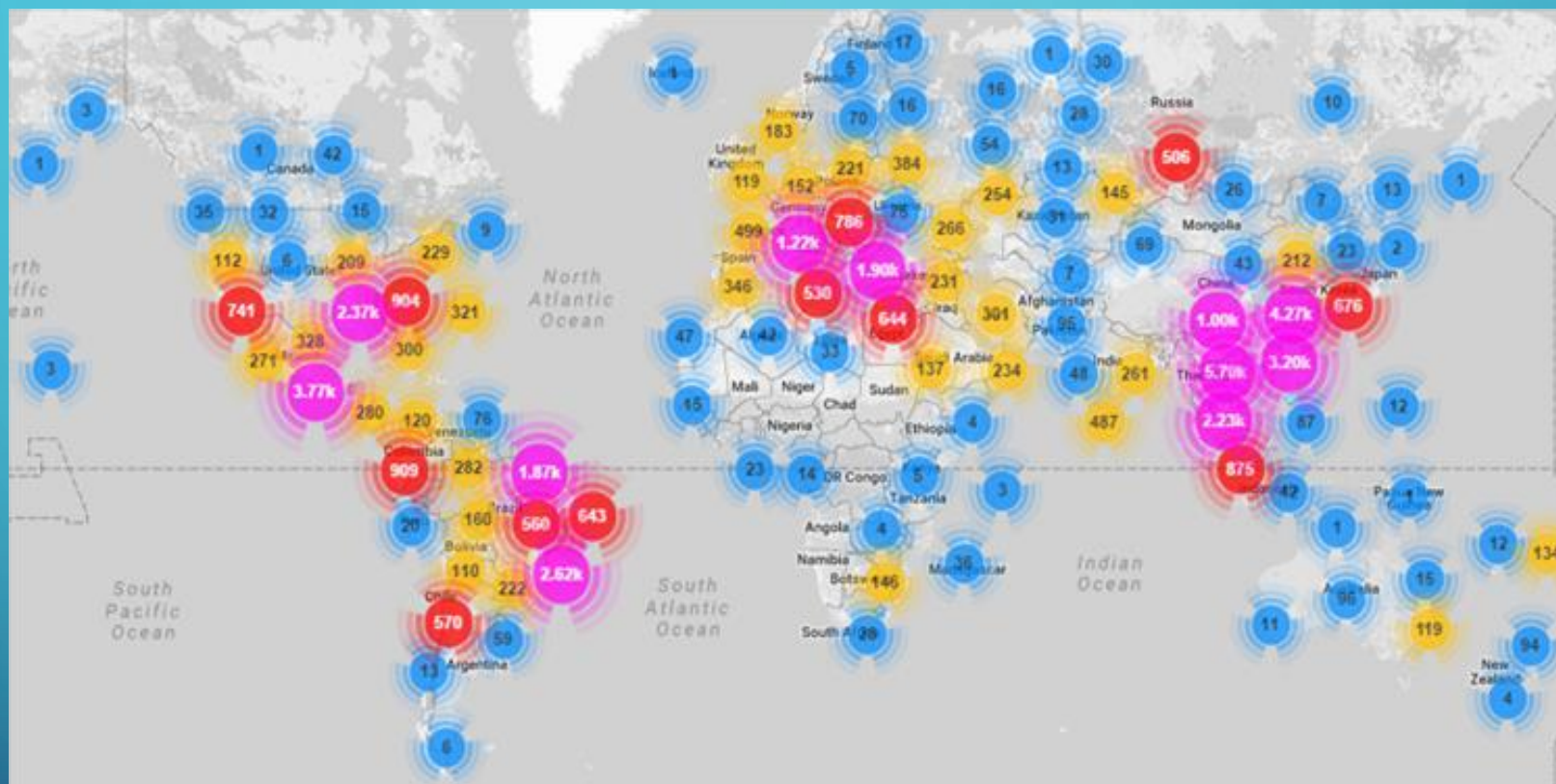
ATAQUES DDOS EN EL MUNDO



INTERNET OF THINGS



MIRAI BOTNET



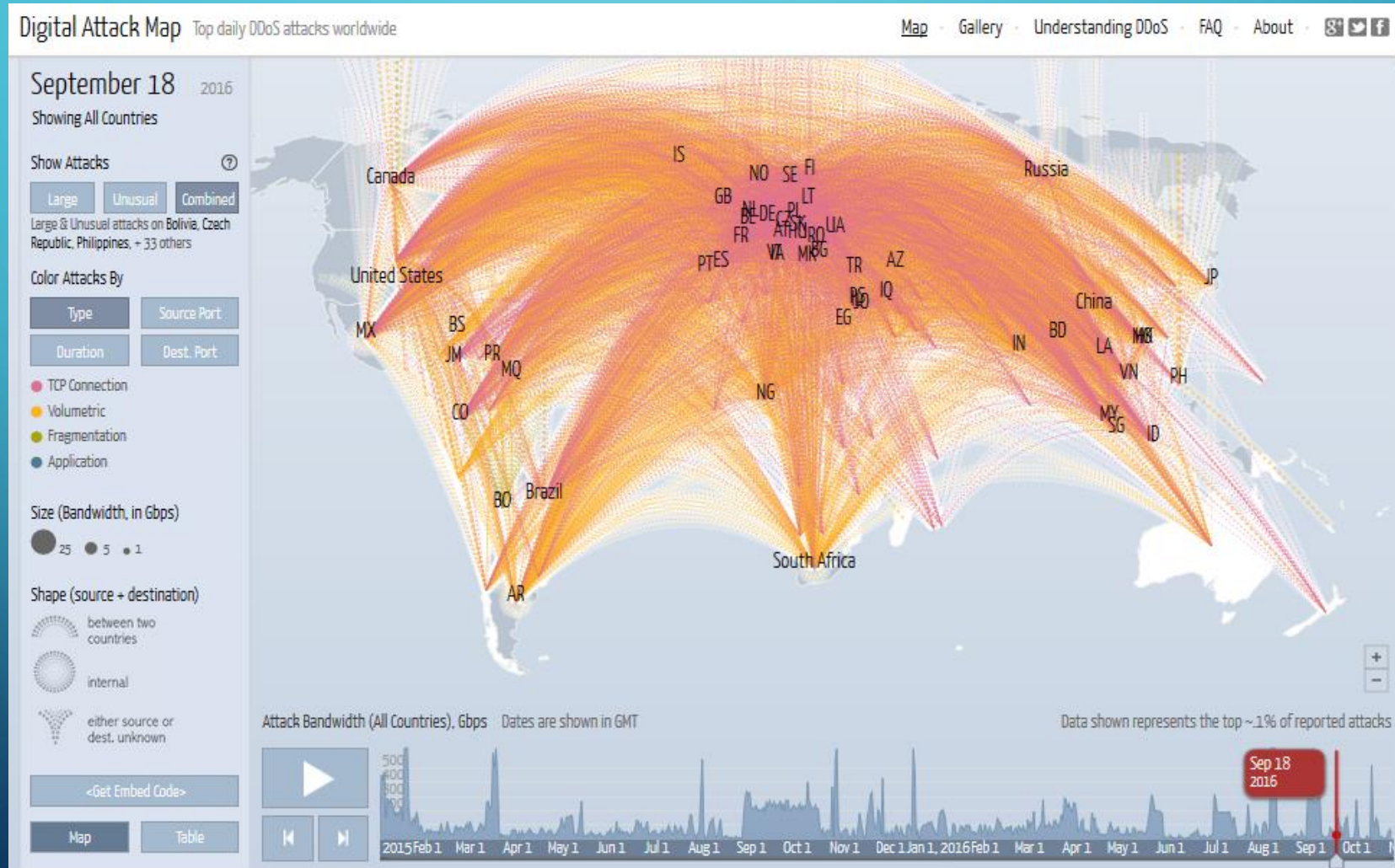
~ 150.000 equipos



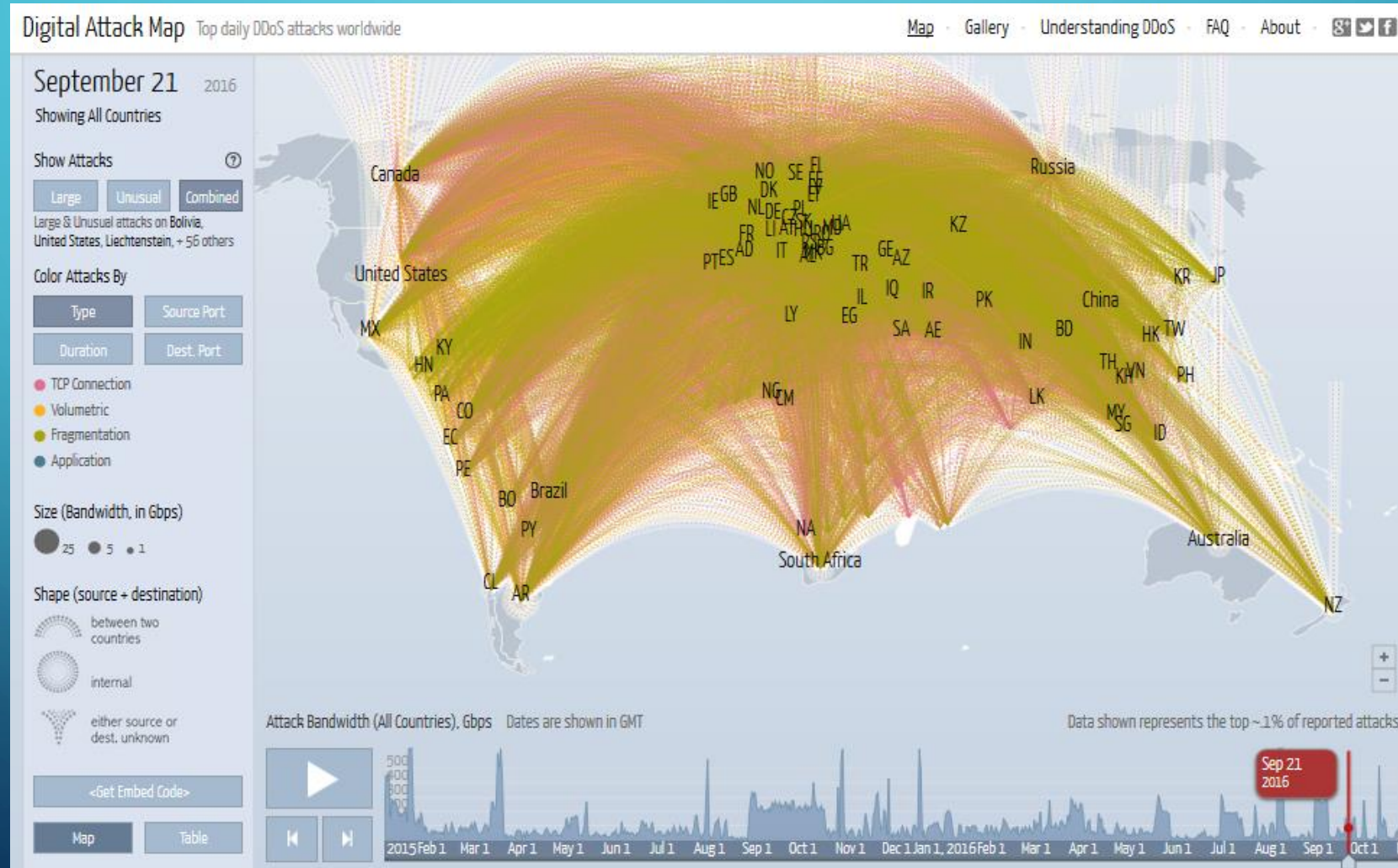
> 1.5 Tbps

Al menos **780** IPs de Paraguay

ATAQUES DDOS – BOTNET MIRAI



ATAQUES DDOS – BOTNET MIRAI



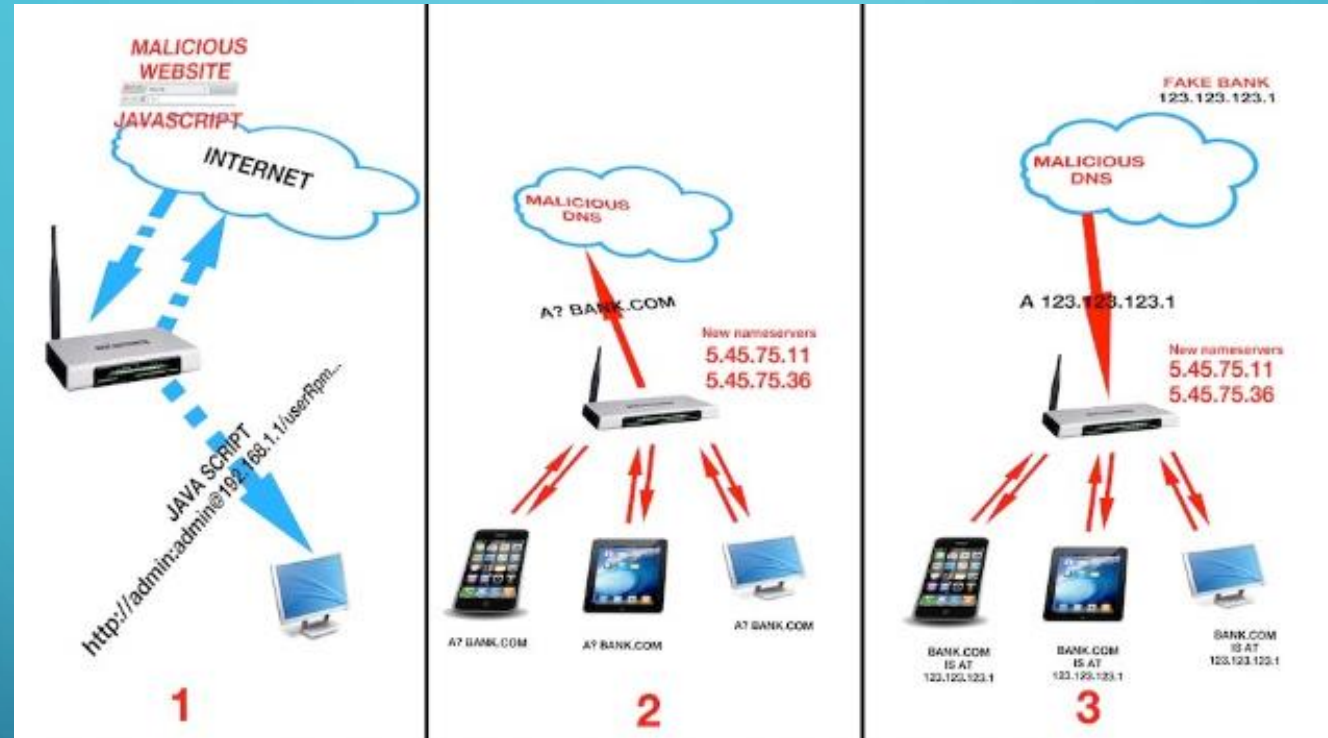
MIRAI BOTNET

```
th_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);
th_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);
th_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);
th_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);
th_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);
th_entry("\x50\x4D\x4D\x56", "", 4);
th_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);
th_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);
th_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);
th_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);
th_entry("\x43\x46\x4F\x4B\x4C", "", 3);
th_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);
th_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);
```

// root	admin
// admin	admin
// root	888888
// root	default
// support	support
// root	(none)
// admin	password
// root	root
// root	12345
// user	user
// admin	(none)
// root	pass
// root	1111

- ✓ Credenciales por defecto
- ✓ Puertos de administración expuestos a Internet

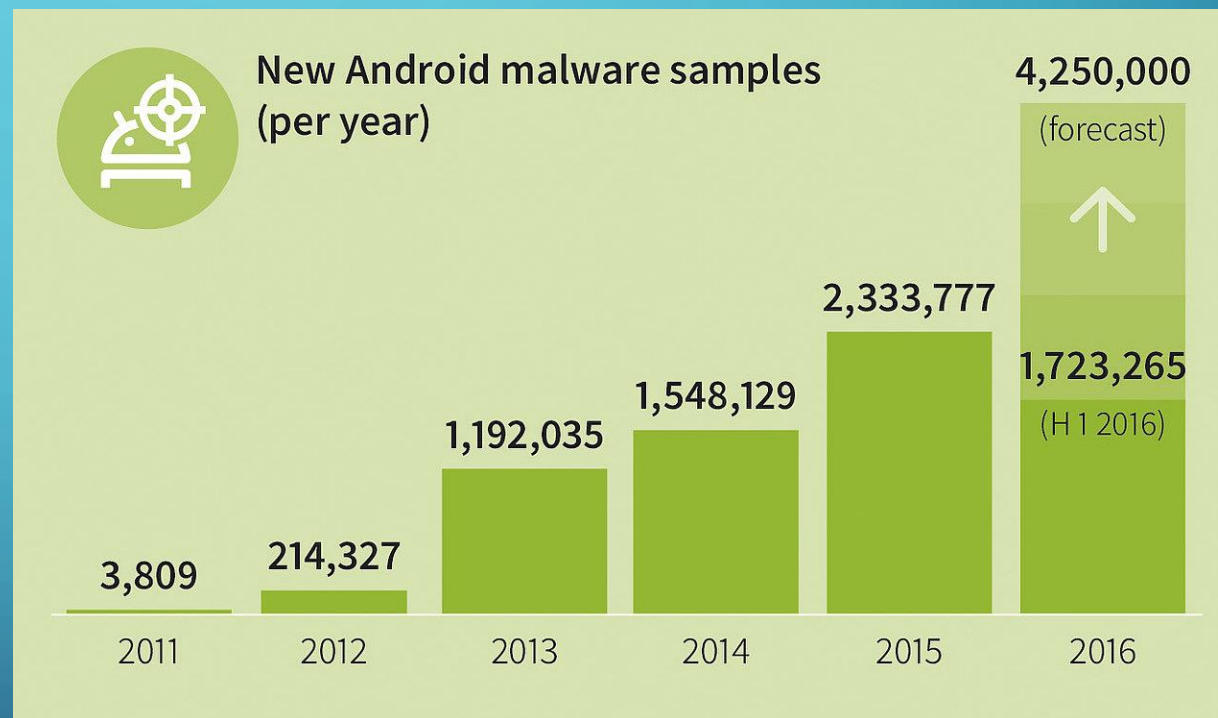
ROUTER BOTNETS



- ✓ Botnets de routers comprometidos mediante gusanos (self-replication)
- ✓ Vulnerabilidad CSRF y credenciales por defecto

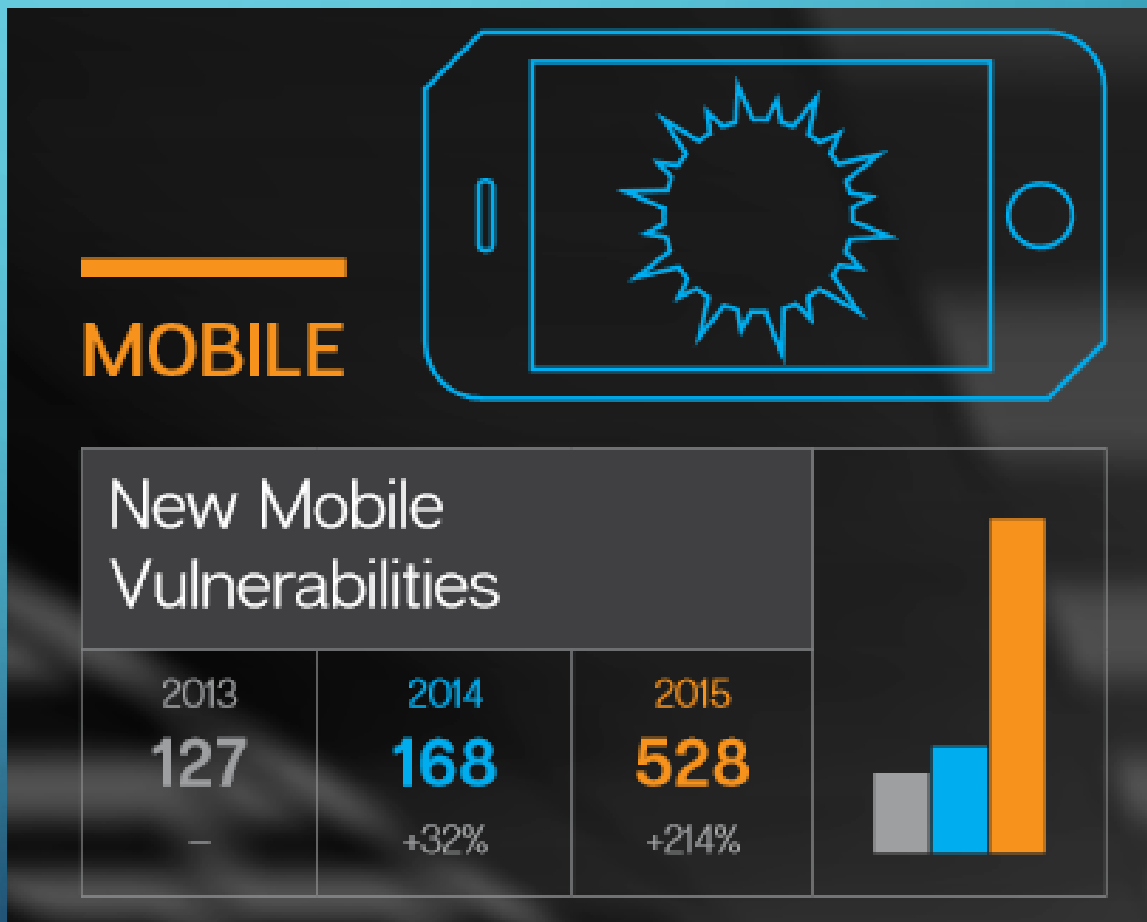
DISPOSITIVO MÓVILES

- Robo de información
- Click-fraud
- RATs – ataques dirigidos
- Ransomware



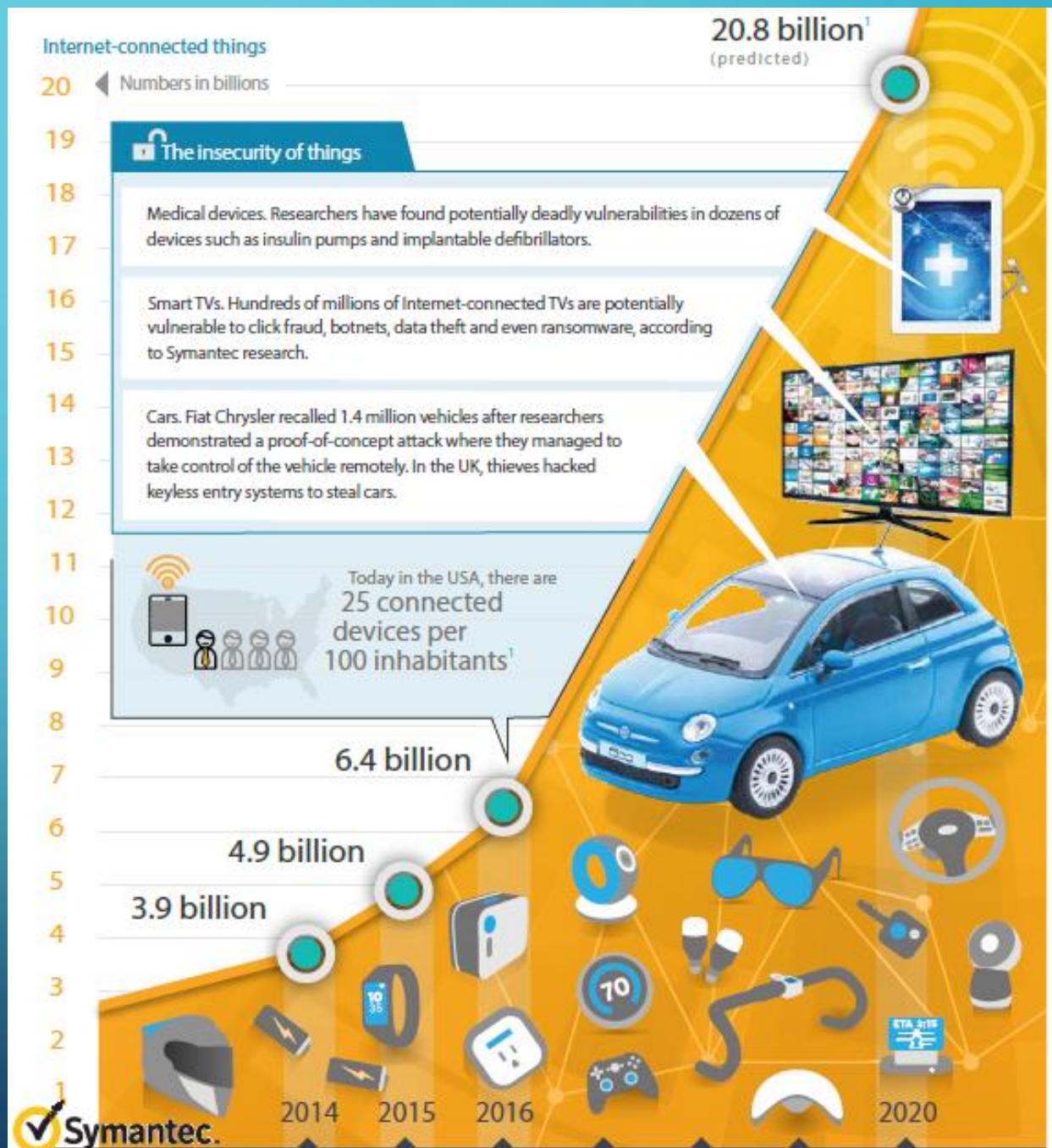
VULNERABILIDADES EN DISPOSITIVO MÓVILES

- Stagefright
- Drammer
- QuadRooter (4 en 1)
- Dirty COW



OTROS RIESGOS EN IOT

- Ataques disruptivos
- Ransomware en dispositivos
- Ataques dirigidos
- Interferencia y daños físicos



MUCHAS GRACIAS!



CERT-PY



www.cert.gov.py

denuncias: abuse@cert.gov.py

contactos: cert@cert.gov.py