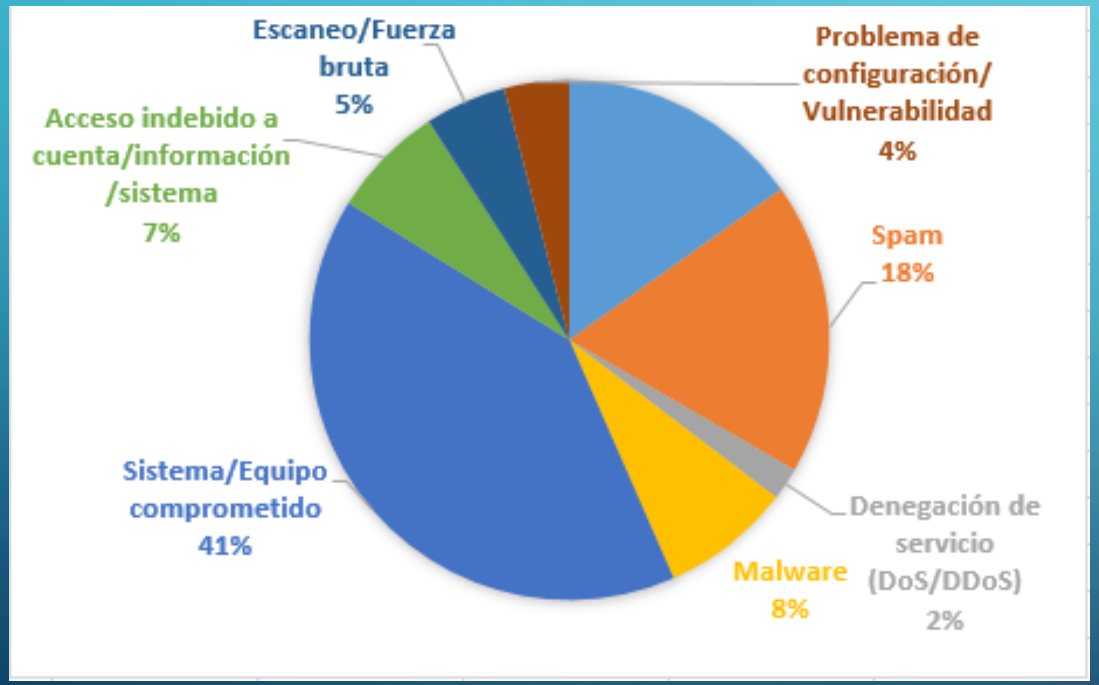
DESDE RANSOMWARE HASTA IOT BOTNETS

¿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**

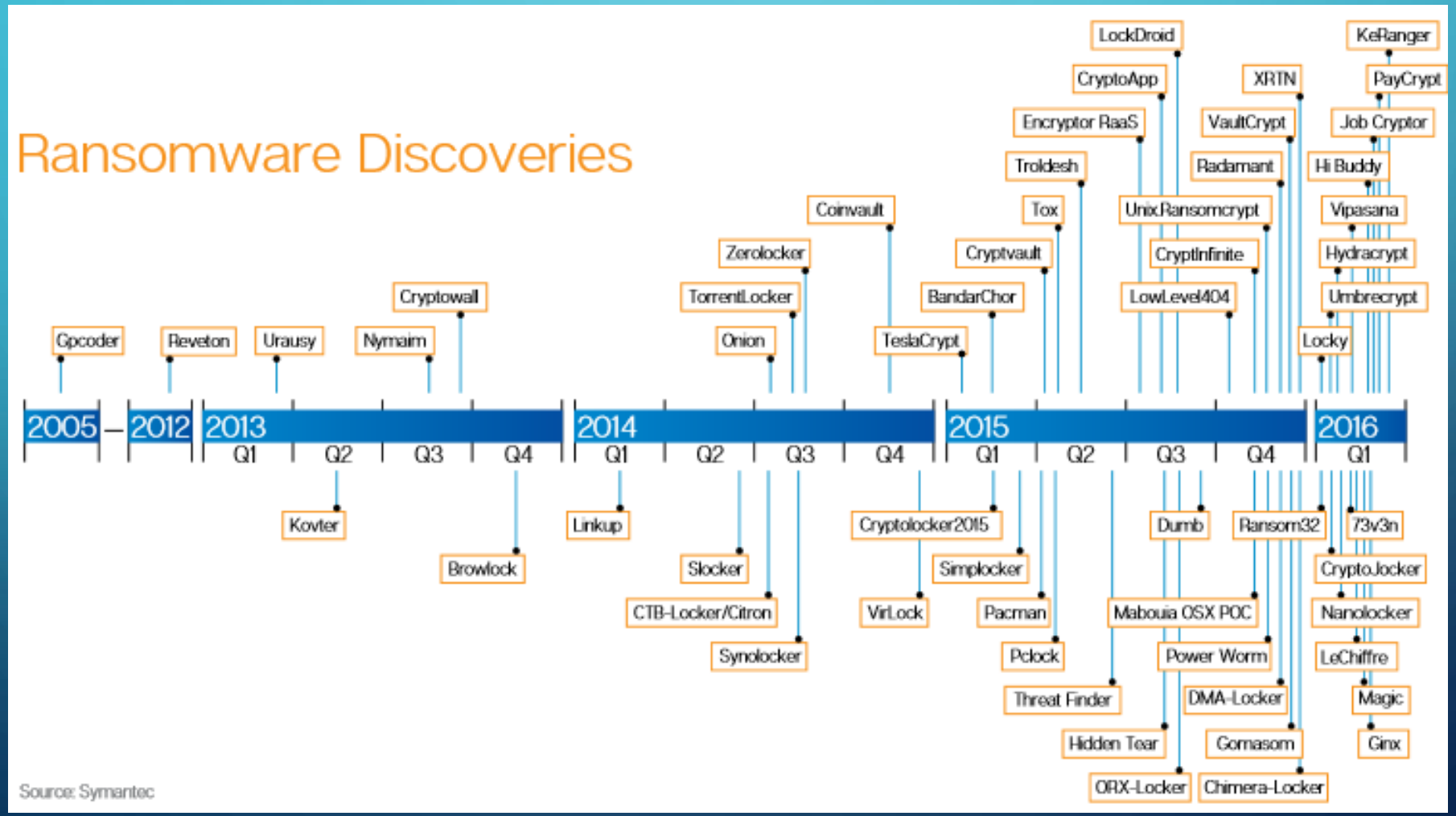
- **Fuentes automatizadas:**
  - > 30,000 eventos por día

RANSOMWARE


YOUR personal files
are encrypted
Pay Ransom
Back
Purchase

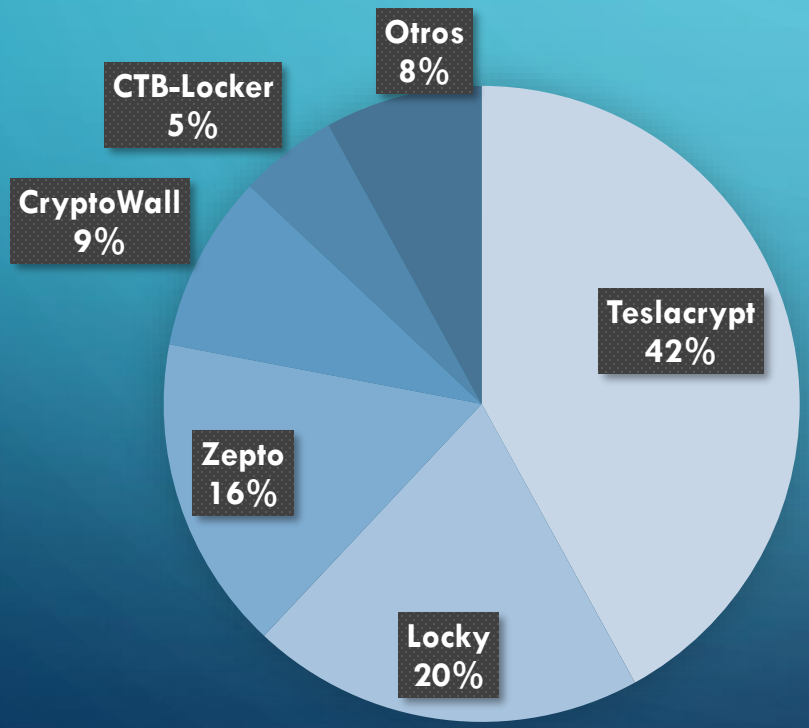
RANSOMWARE – MAYOR AMENAZA DEL 2016

EVOLUCIÓN DEL RANSOMWARE

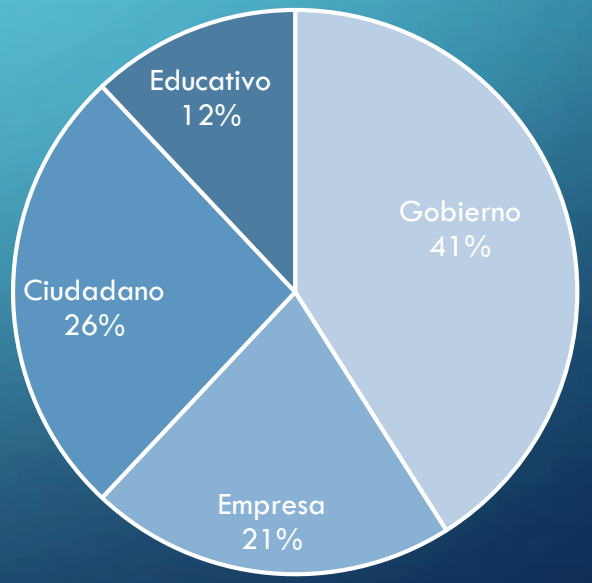


EVOLUCIÓN DEL RANSOMWARE

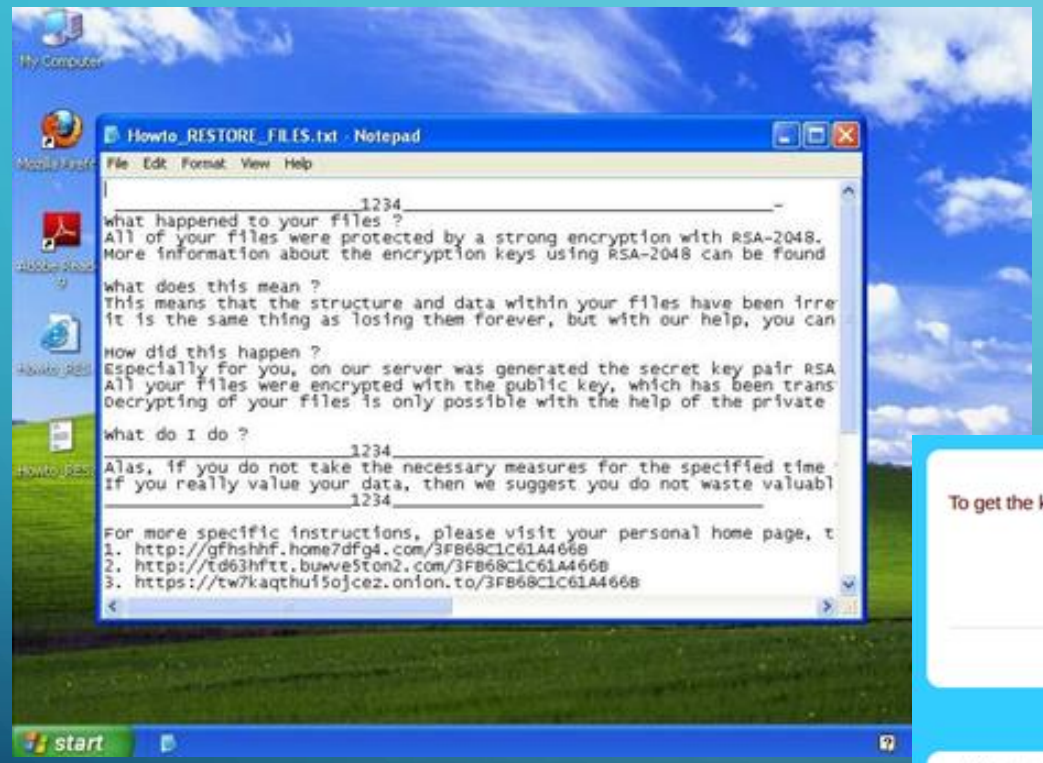
VARIANTES DE RANSOMWARE

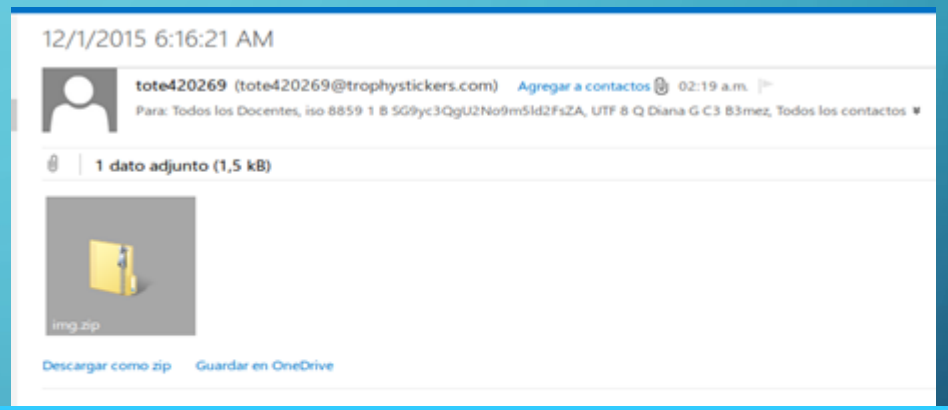


SECTOR AFECTADO



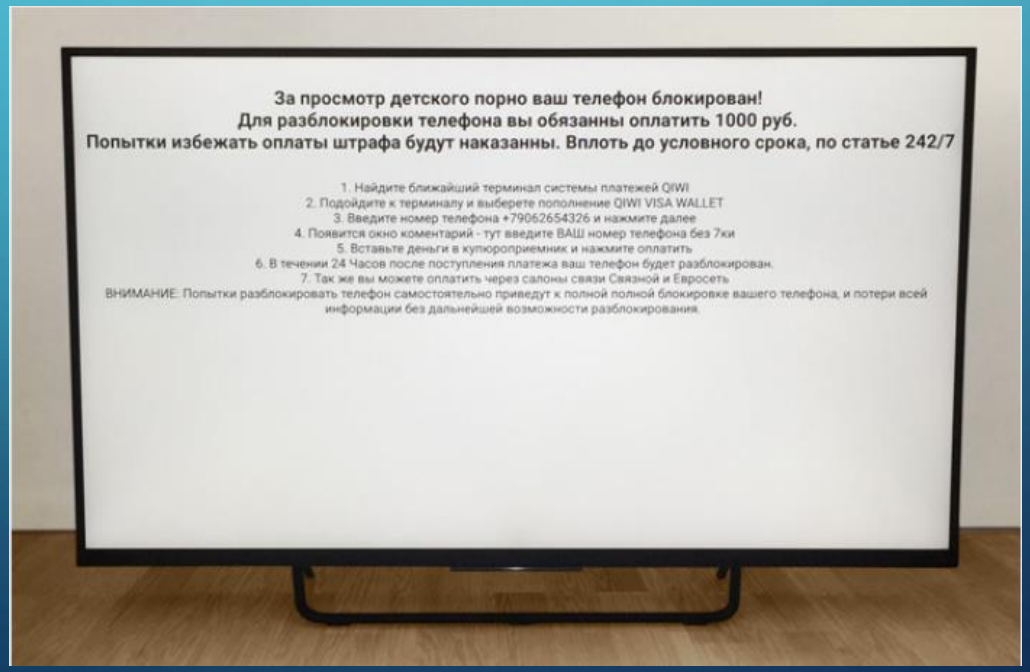
TESLACRYPT, UN CASO DE ÉXITO… PARCIAL





TENDENCIAS CON RESPECTO AL RANSOMWARE

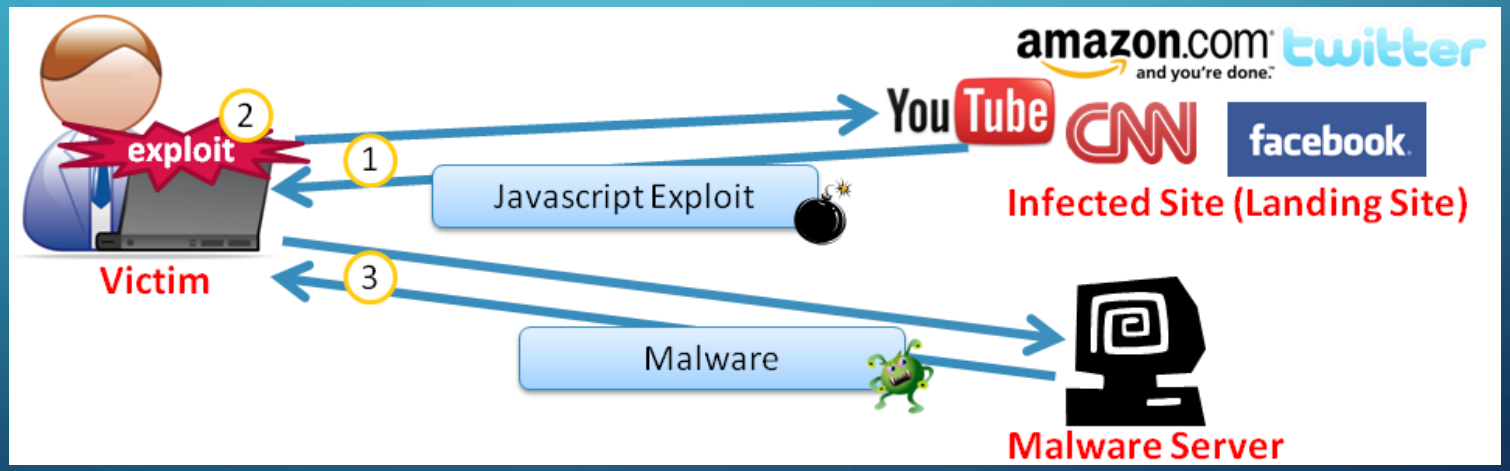
- ✓Los ciberdelincuentes buscan aumentar la presión
- ✓Vectores de infección con mínima interacción del usuario: drive-by download, fuerza bruta RDP, explotación de vulnerabilidades en la red, etc.
- ✓No solo computadoras: móviles, servidores web (ransomweb), SmartTV



DRIVE-BY DOWNLOAD Y EXPLOIT KITS

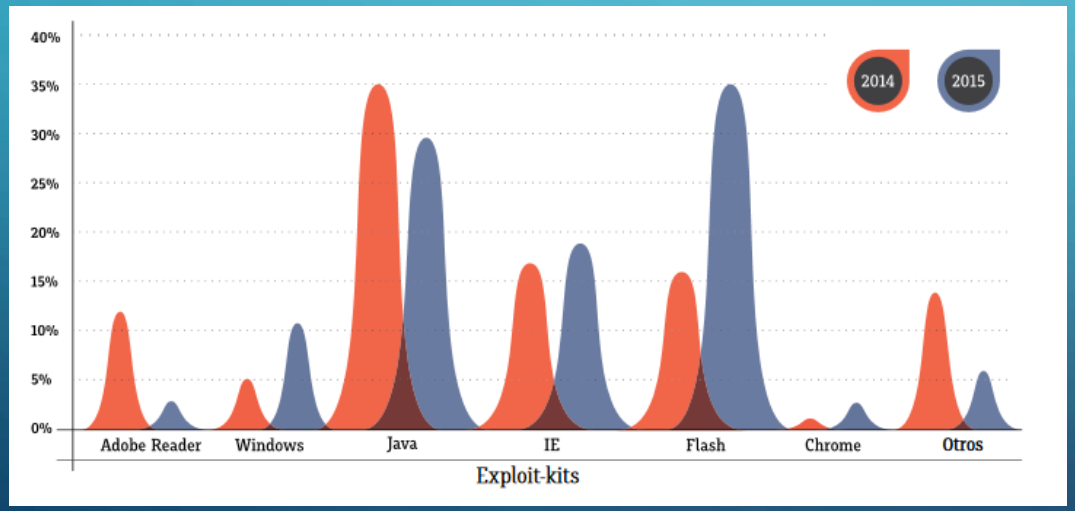
DRIVE-BY DOWNLOAD

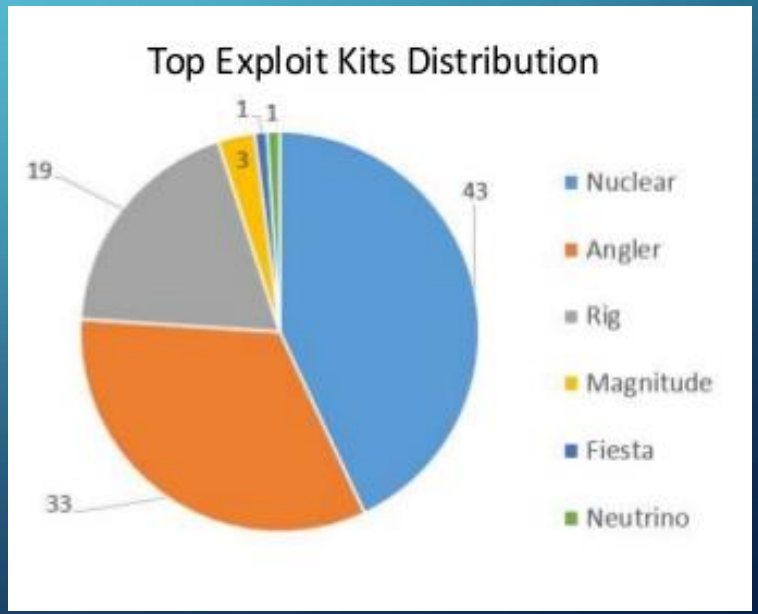
Existen técnicas a través de las cuales sólo se requiere que un usuario abra una página web en el navegador para infectarlo.



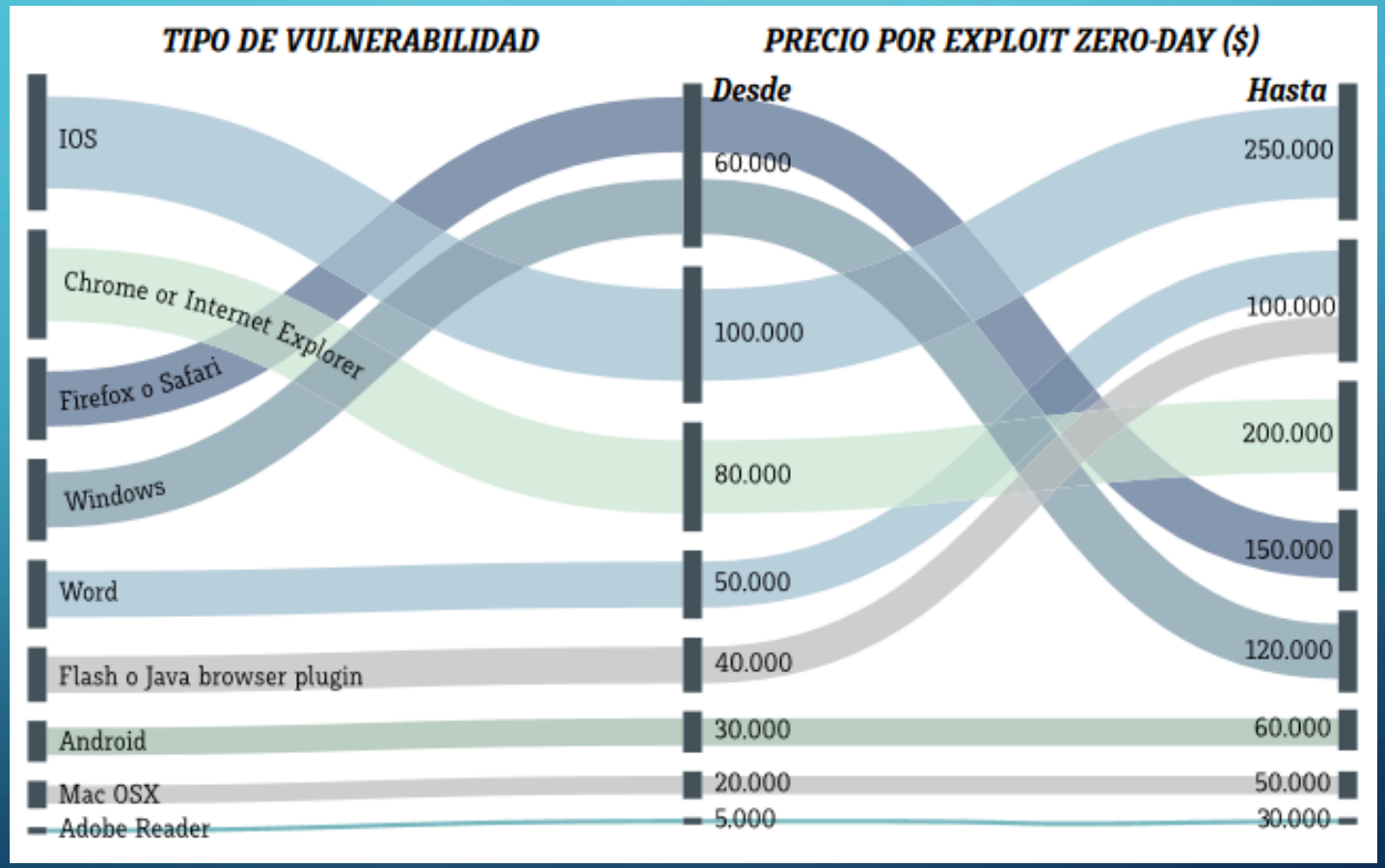
EXPLOIT KITS

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



APTs 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**.

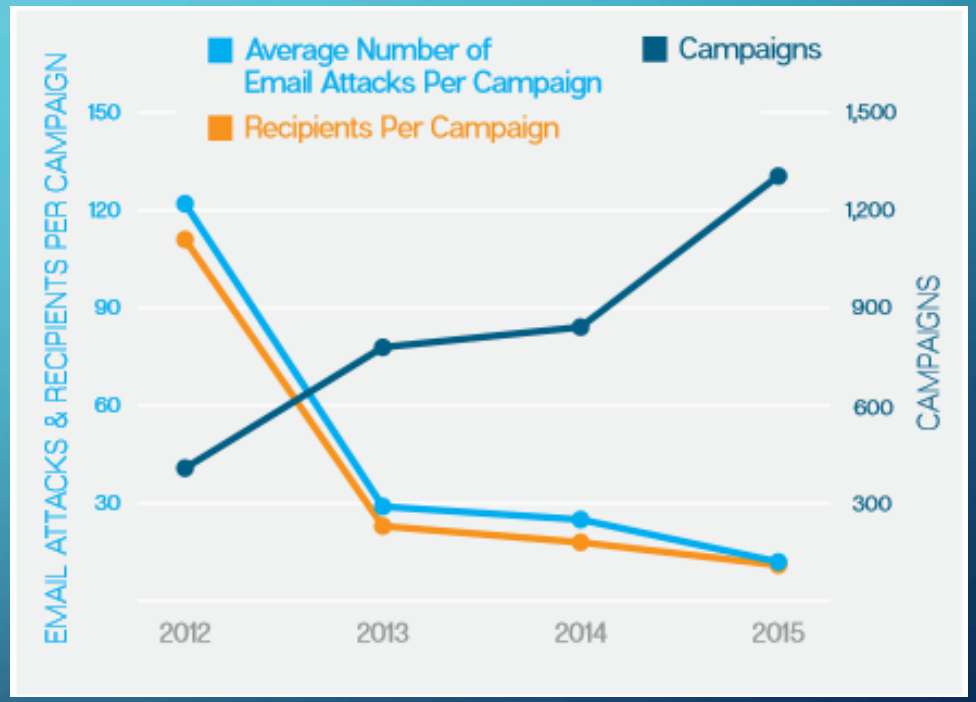
Ejemplo:

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

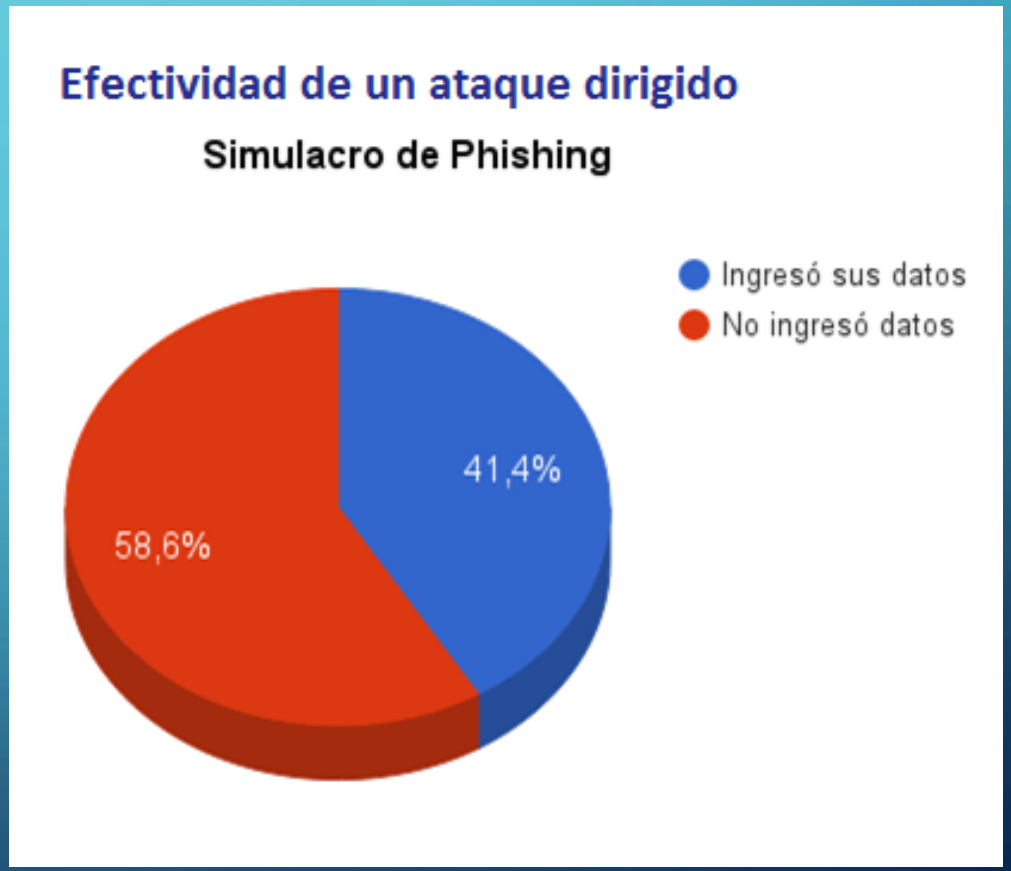
VECTORES DE ATAQUE DE UN APT

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

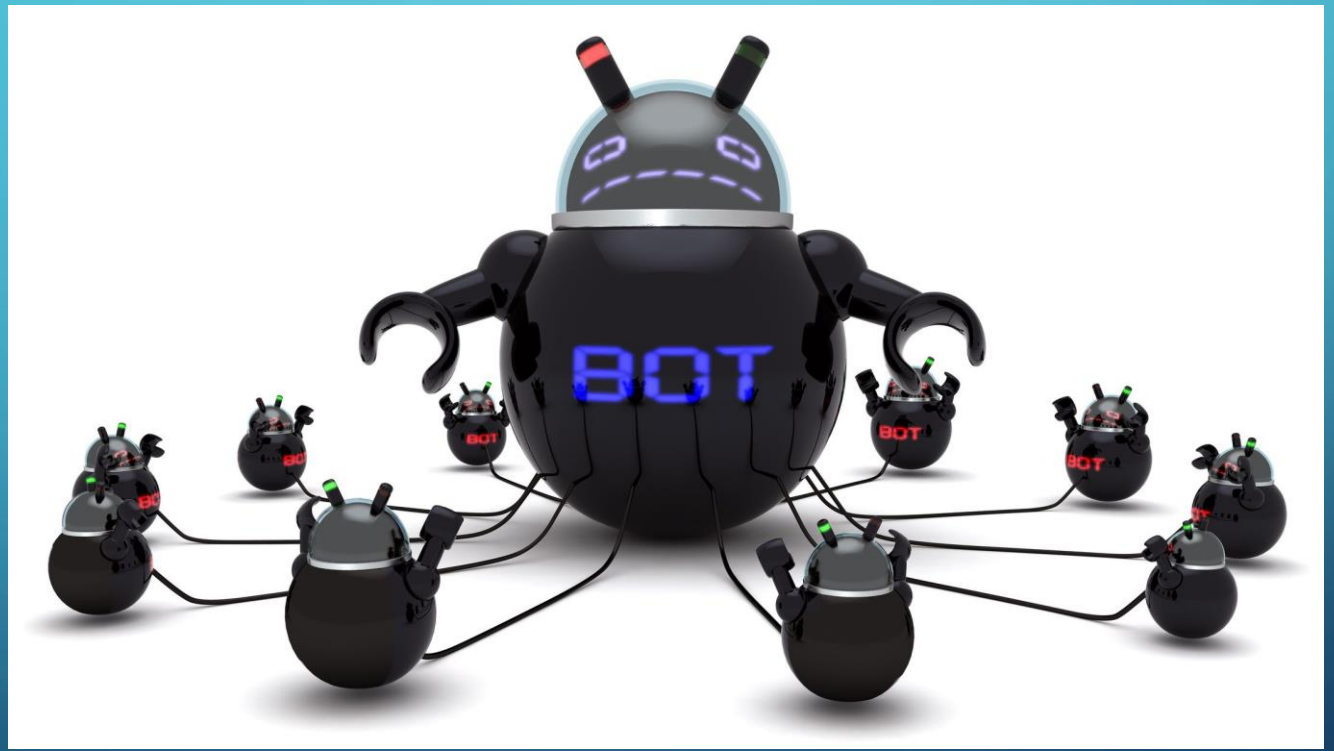


EVOLUCIÓN DE LOS OBJETIVOS

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

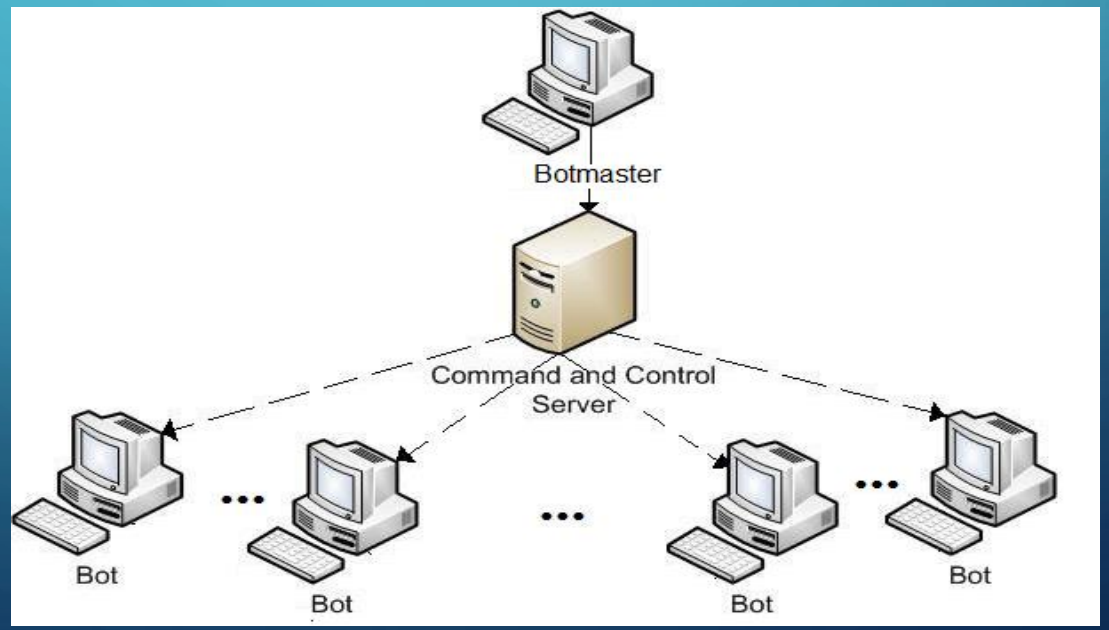


BOTNETS

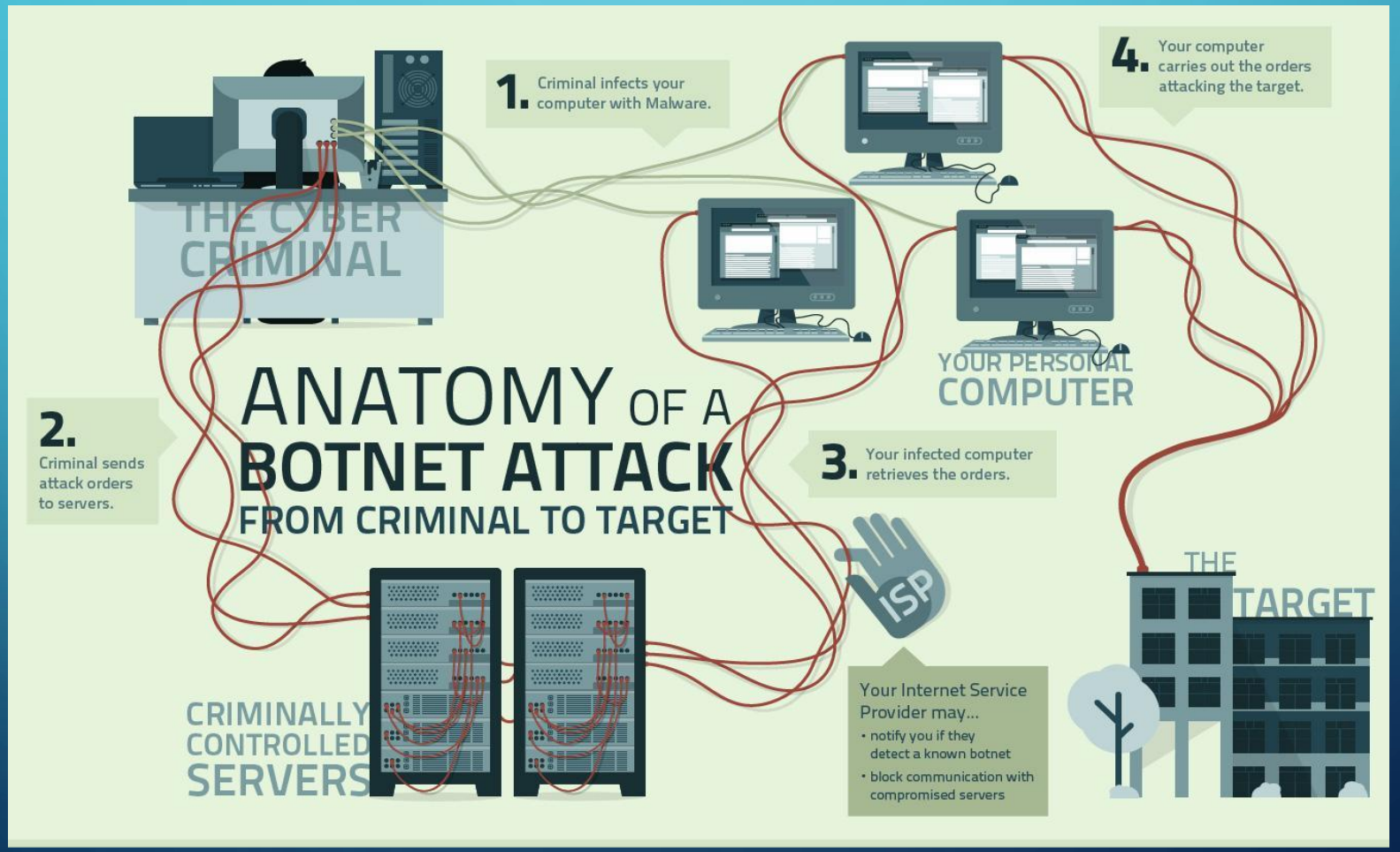


BOTNETS

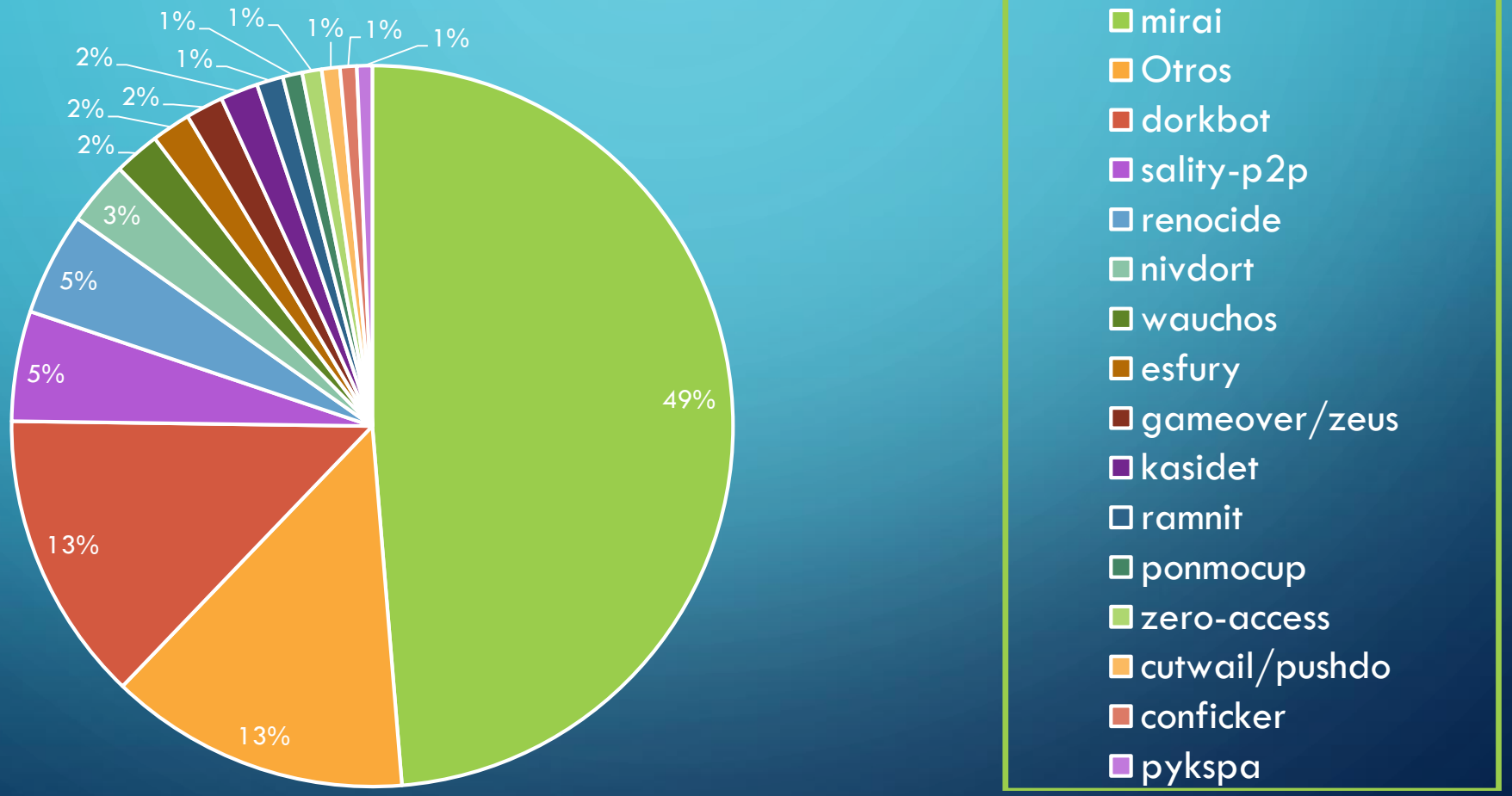
Red de equipos infectados (bots o zombies) controlada por el artífice de la botnet (botmaster) de forma remota, por lo general a través de servidores de Comando y Control (C&C).



FUNCIONAMIENTO DE UNA BOTNET



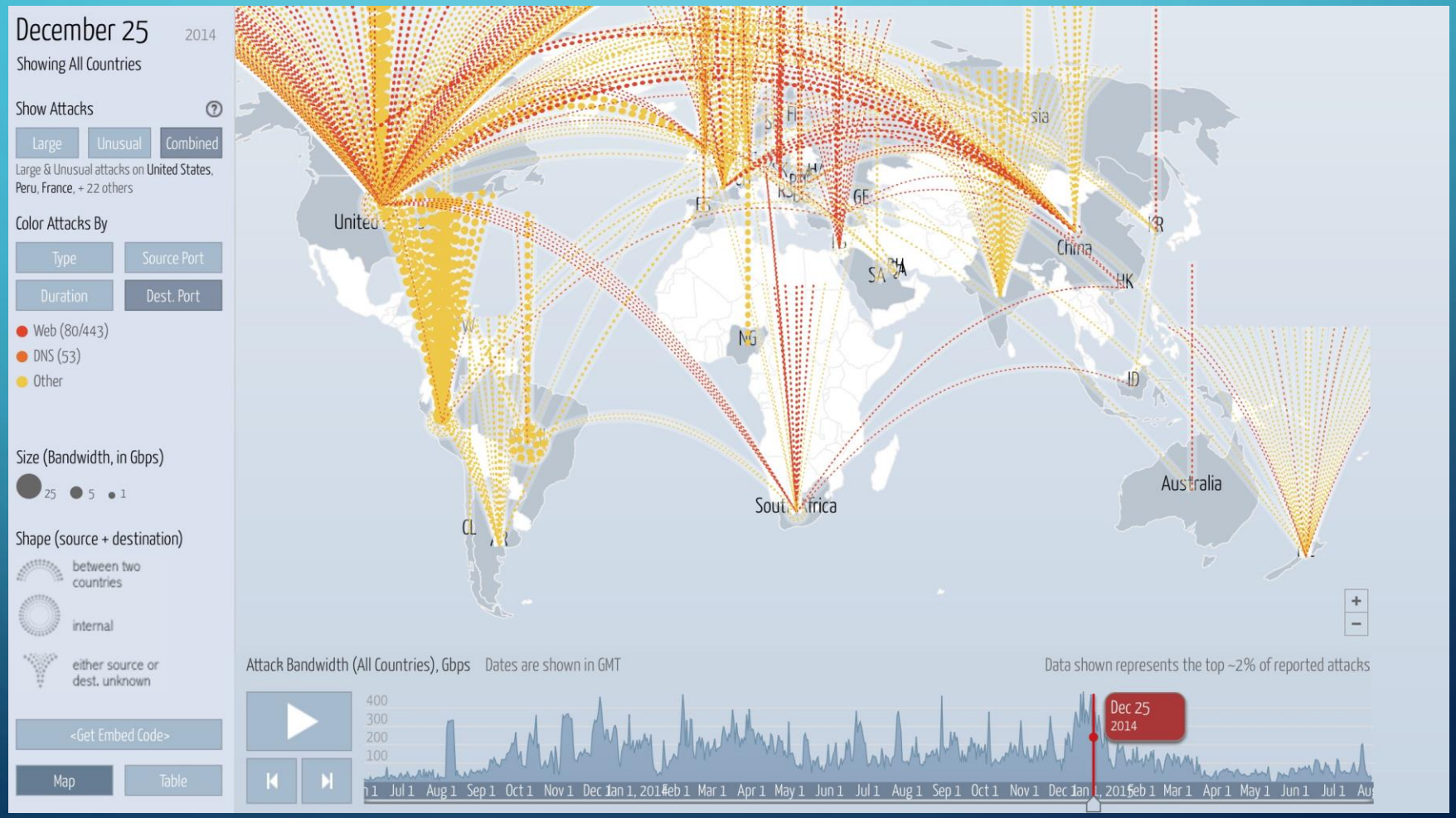
PRINCIPALES INFECCIONES EN PARAGUAY



¿PARA QUÉ BOTNETS?

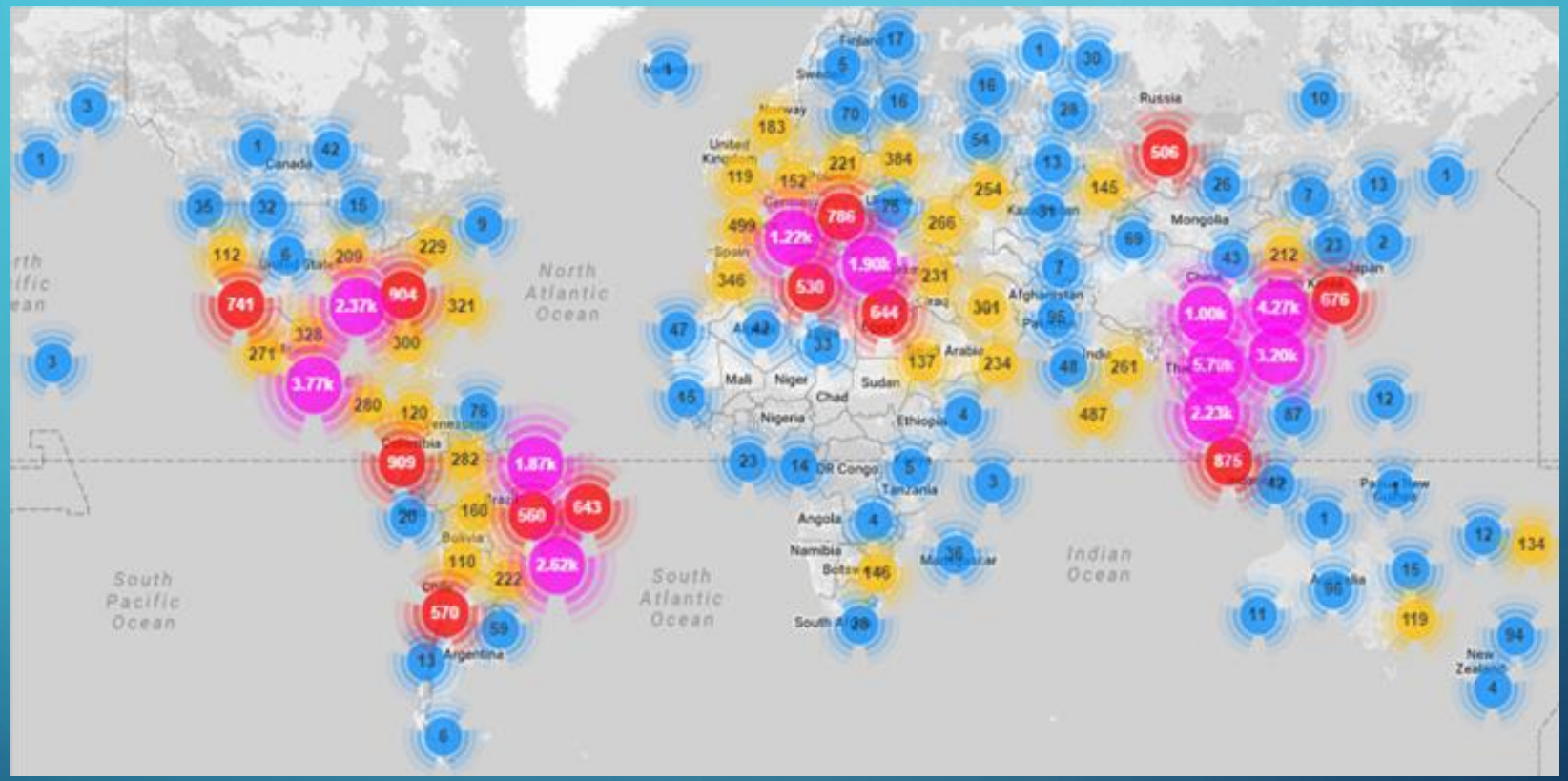
- DoS/DDoS
- Spam
- Distribución de malware
- Proxies maliciosos
- Click-Fraud
- Phishing
- Hacktivismo

ATAQUES DDOS EN EL MUNDO



INTERNET OF THINGS

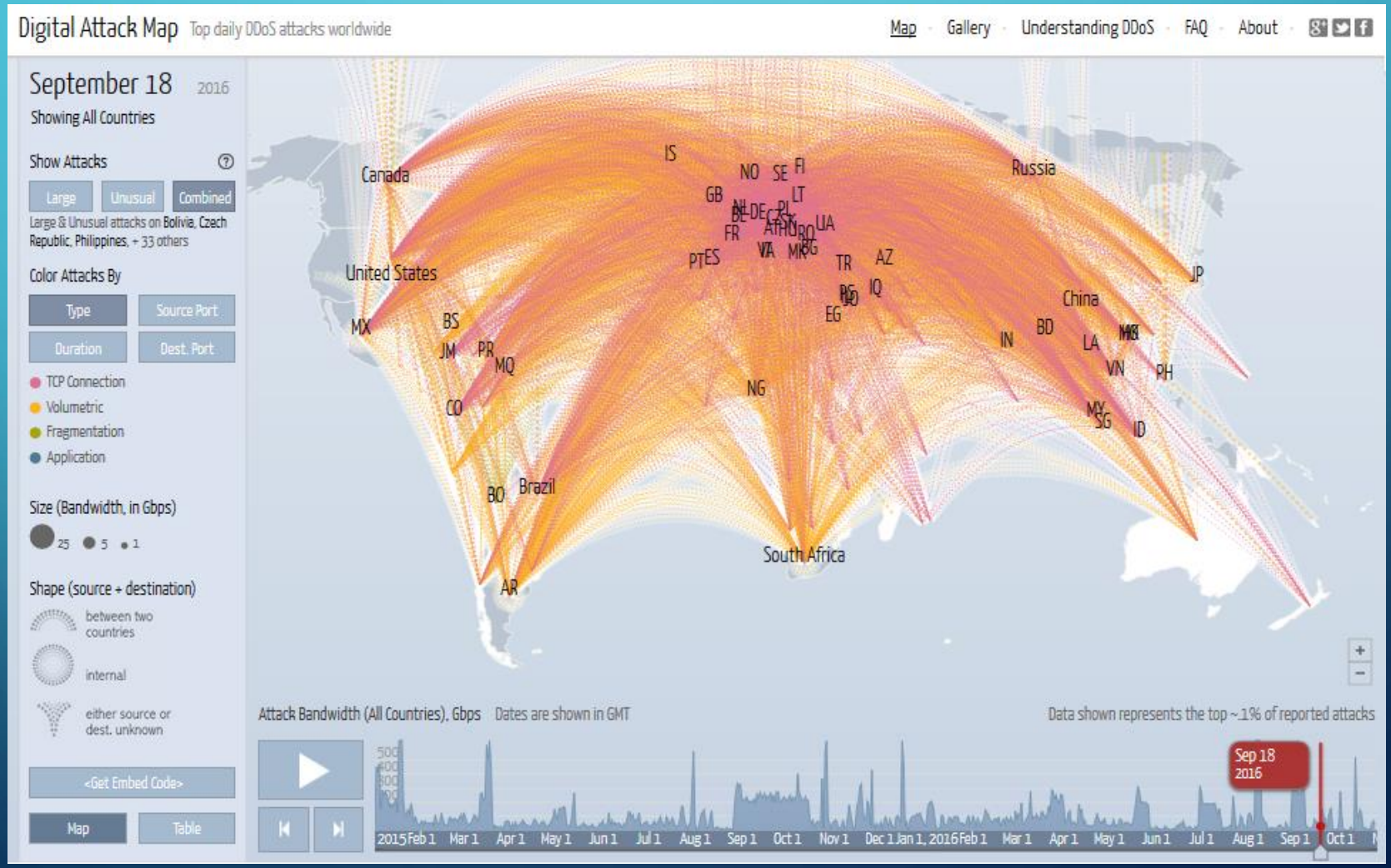
MIRAI BOTNET



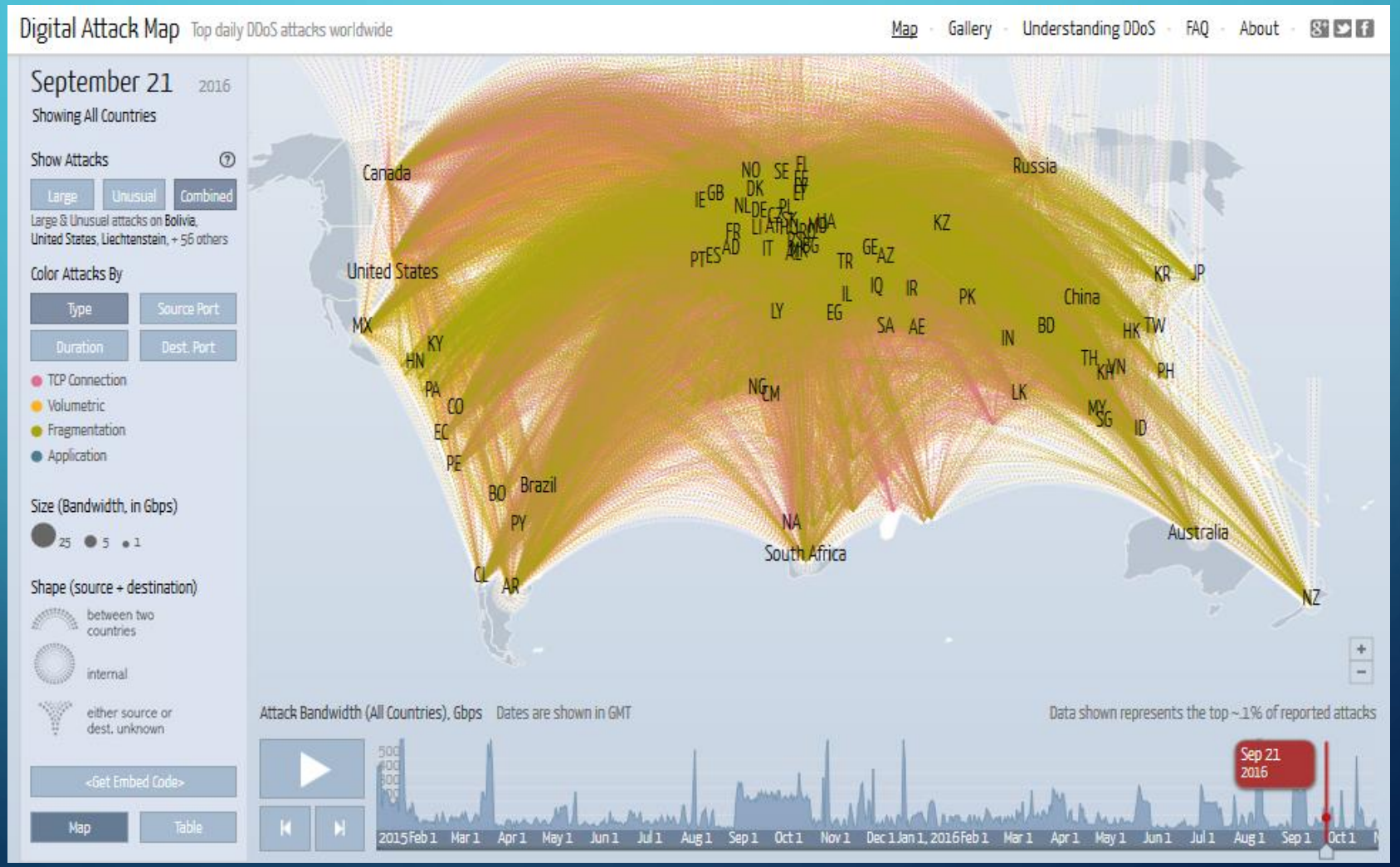
~ 150.000 equipos → > 1.5 Tbps

Al menos **780** IPs de Paraguay

ATAQUES DDOS – BOTNET MIRAI



ATAQUES DDOS – BOTNET MIRAI

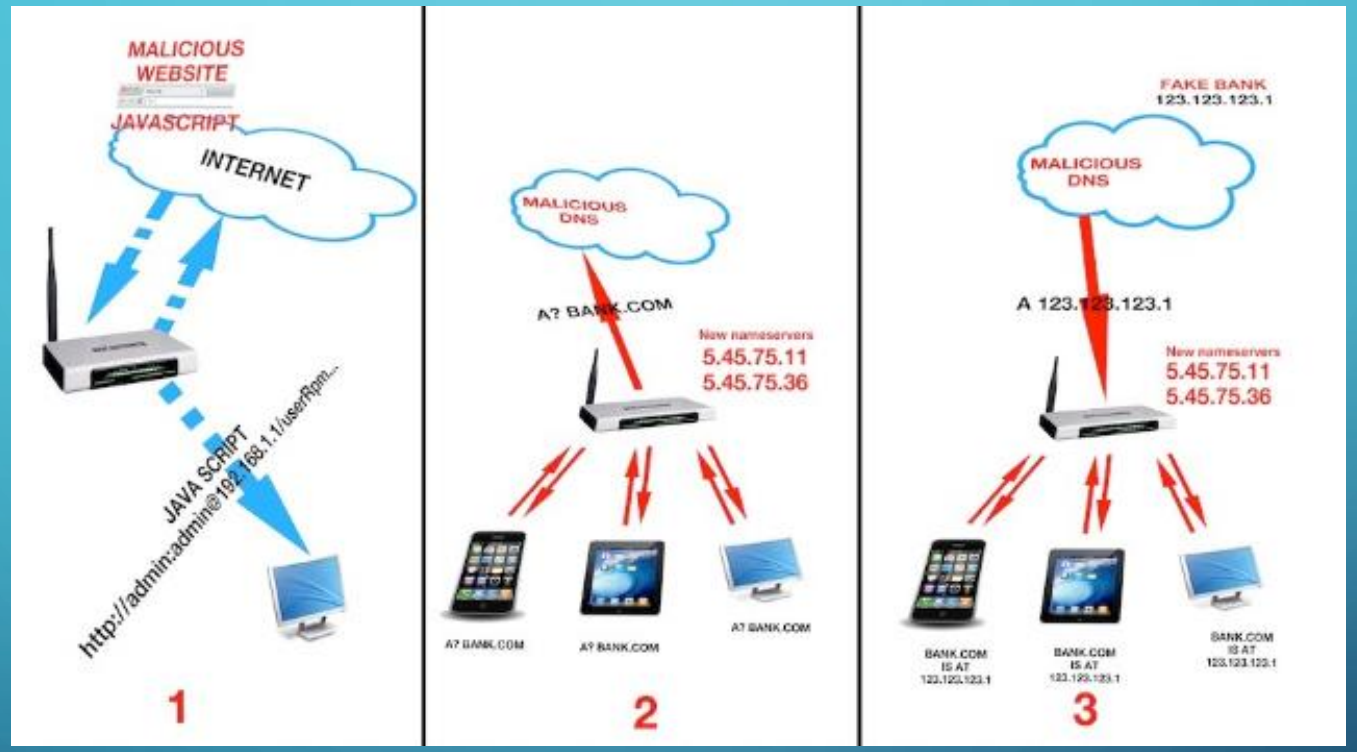


MIRAI BOTNET

```
th_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                    // root      admin
th_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                // admin     admin
th_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                // root      888888
th_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);            // root      default
th_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5); // support   support
th_entry("\x50\x4D\x4D\x56", "", 4);                                        // root      (none)
th_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);    // admin     password
th_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                        // root      root
th_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                    // root      12345
th_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                        // user      user
th_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                    // admin     (none)
th_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                        // root      pass
th_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                        // root      1111
```

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

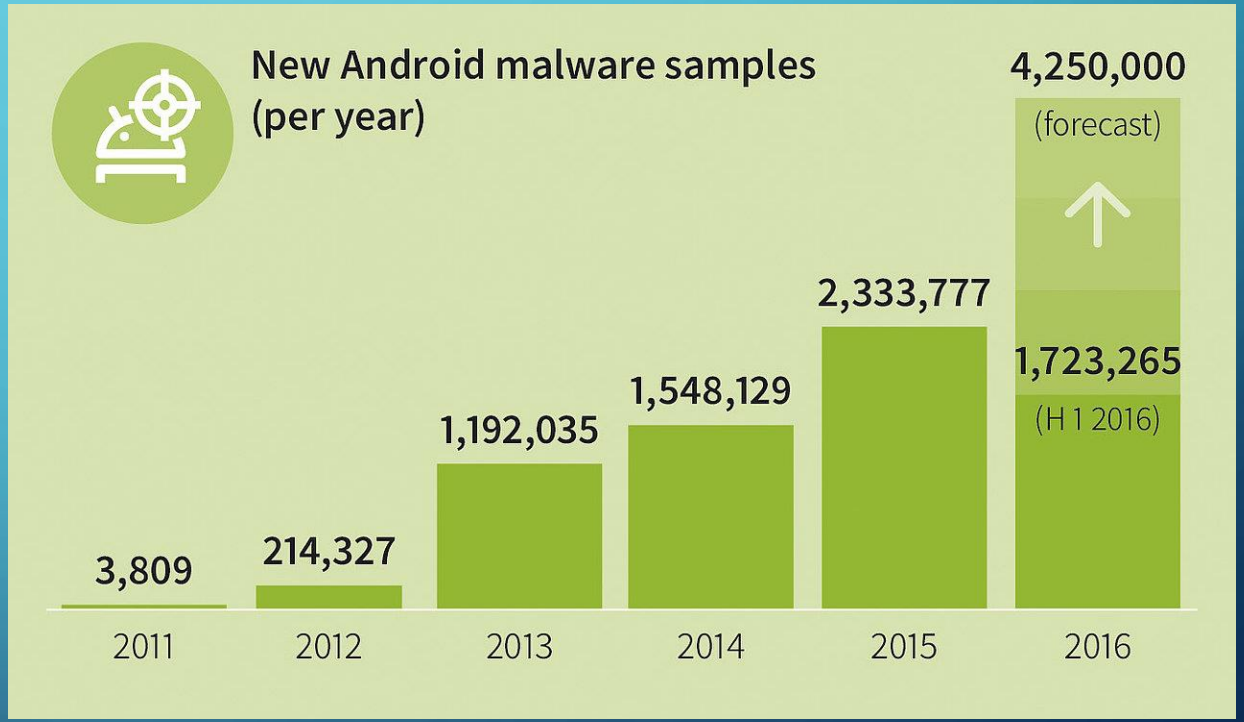
ROUTER BOTNETS



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

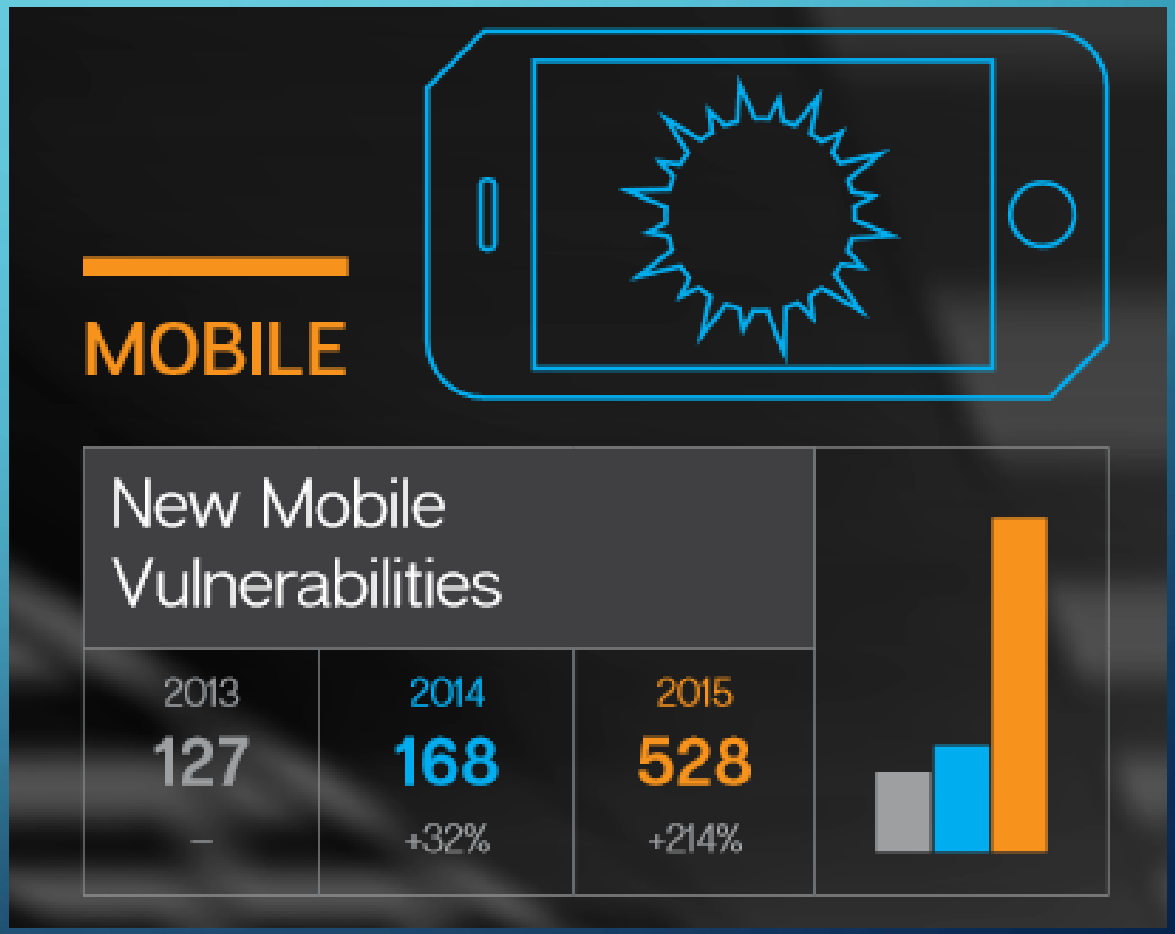
DISPOSITIVO MÓVILES

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



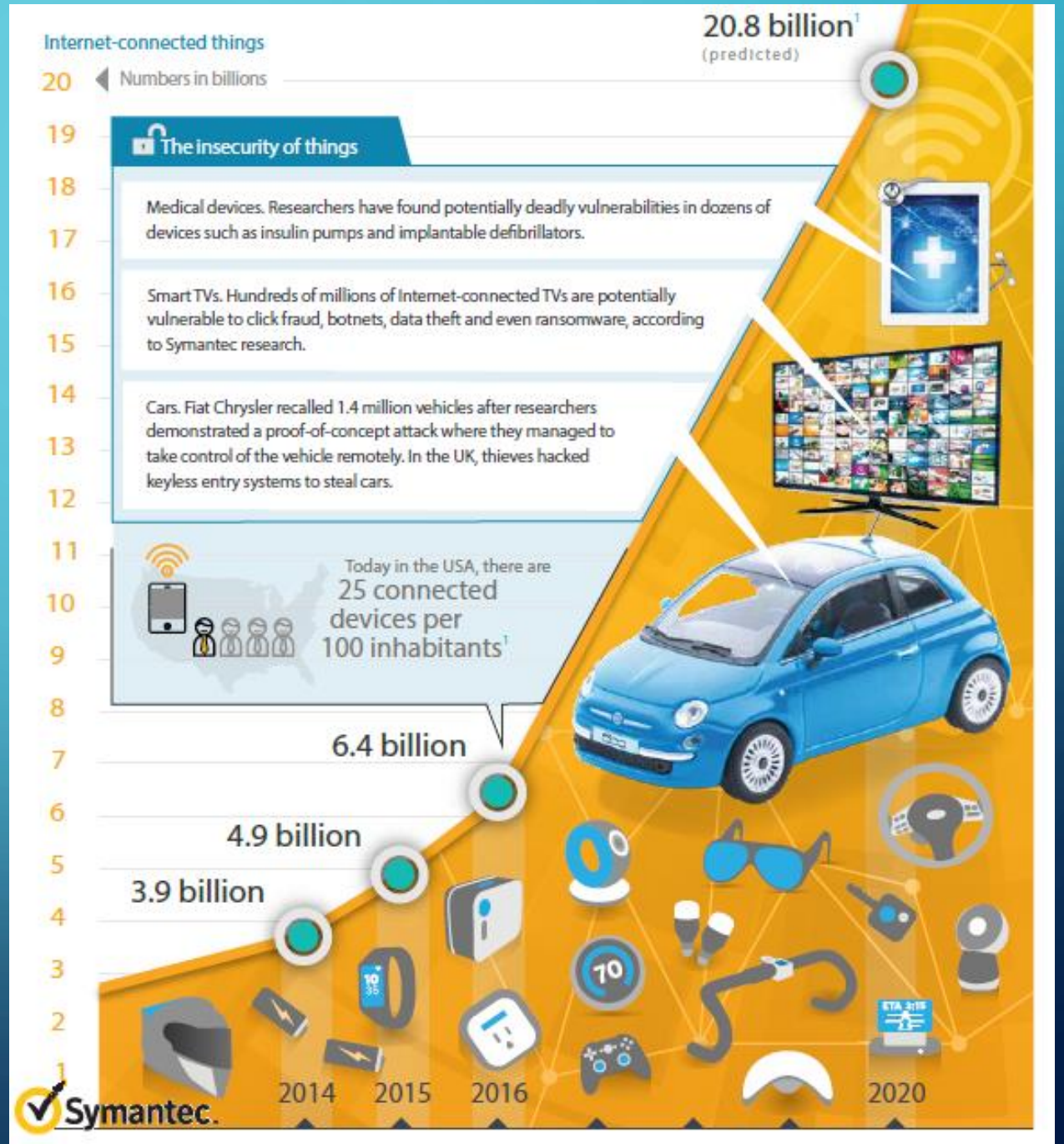
VULNERABILIDADES EN DISPOSITIVO MÓVILES

- 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!

@CERTpy

/CERT-Py

www.cert.gov.py

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