ITC S.A.

Innovación, Tecnología, Consultoría

URSEC
Unidad Reguladora de Servicios de Comunicaciones

JNT#2017

Primeras Jornadas Nacionales en Telecomunicaciones

21 al 23 de marzo

URSEC
Unidad Reguladora de Servicios de Comunicaciones

JNT#2017

Ciberseguridad y los nuevos desafíos

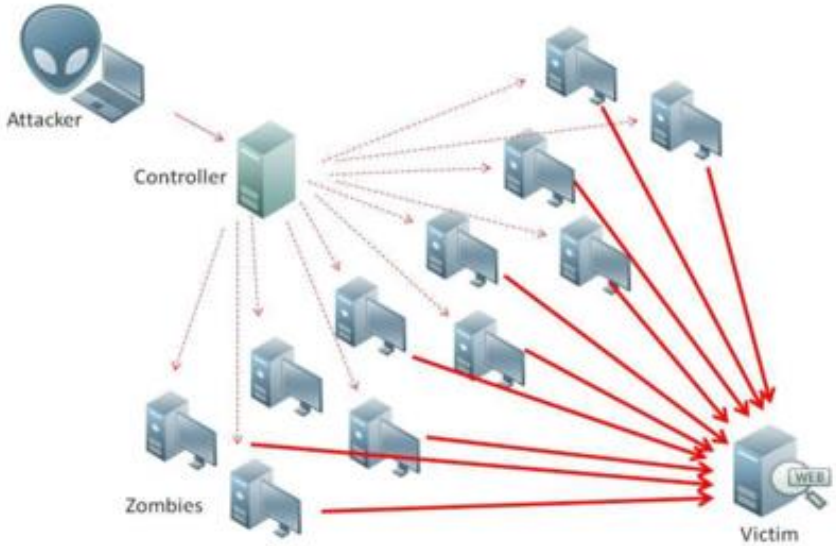
Ing. Leonardo Vidal
Consultor Senior de ITC S.A.
CISSP

Nuevos Desafíos

- Pondremos foco en los *ataques de* ***DDoS basados en IoT***
  - IoT: Internet de las Cosas (*Internet of Things*)
  - DoS (*Denial of Service*): Denegación de Servicio. Agotamiento de recursos asociados a determinado servicio con el objetivo que los usuarios legítimos no puedan acceder a él
  - DDoS: DoS Distribuido (*Distributed Denial of Service*)
  - El DDoS le agrega al DoS que el ataque proviene de muchos orígenes (decenas o centenas de miles)

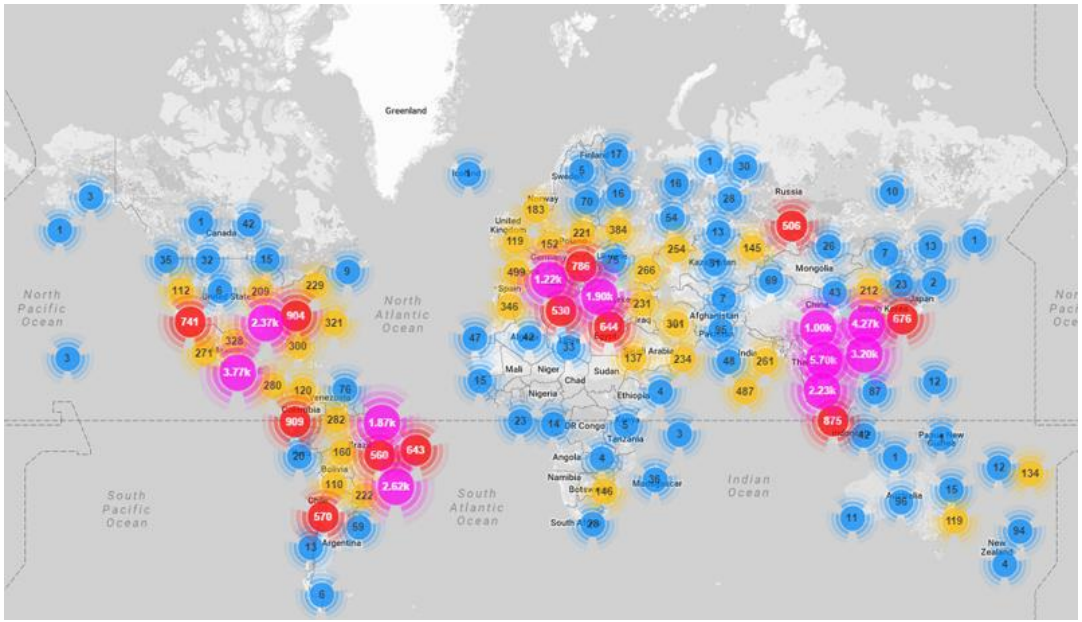
DDoS, botnets, IoT

- Los ataques de DDoS existen desde hace más de 10 años
- Se basan en las redes conocidas como *botnet*: C&C + "zombies" (malware)
  - C&C o C2: Comando y Control de la botnet
- IoT es una excelente ayuda que se le brinda a los atacantes, pues se les ofrecen centenares de miles de dispositivos (y creciendo exponencialmente) que pueden ser, actualmente sin mucho esfuerzo, el origen de los mismos



Ataque recientes (2016) de DDoS basados en IoT

- Mediante botnets que capturaron entre 300.000 y 900.000 *zombies* (DVRs, cámaras IP, routers hogareños, …), han logrado generar picos de tráfico entre **600 Gbps** y **1 Tbps** (1000 Gbps), con ataques que se mantienen durante varias horas
- Servidor con una buena conexión a Internet: **1 Gbps** o **10 Gbps**.



¿Por qué puede ser sencillo capturar los dispositivos IoT?

- Debido a algo que ya se comentó en las sesiones del martes:

  "la seguridad, como siempre, la dejamos para más adelante"

- La enorme mayoría de los dispositivos IoT actualmente se fabrican bajo dos premisas fundamentales:
  - (muy) bajo costo

  - foco (casi) exclusivo en la funcionalidad

Algunas consecuencias

- Por lo tanto, es muy difícil que los fabricantes destinen recursos para el tema seguridad. En consecuencia, los dispositivos salen al mercado y se despliegan con consideraciones de seguridad muy limitadas o casi nulas

- Luego del despliegue masivo, realizarles mejoras en cuanto a seguridad, es muy difícil y/o costoso.

- Adicionalmente, no debemos minimizar las posibles consecuencias en aspectos de confidencialidad de los datos “en poder” de los dispositivos

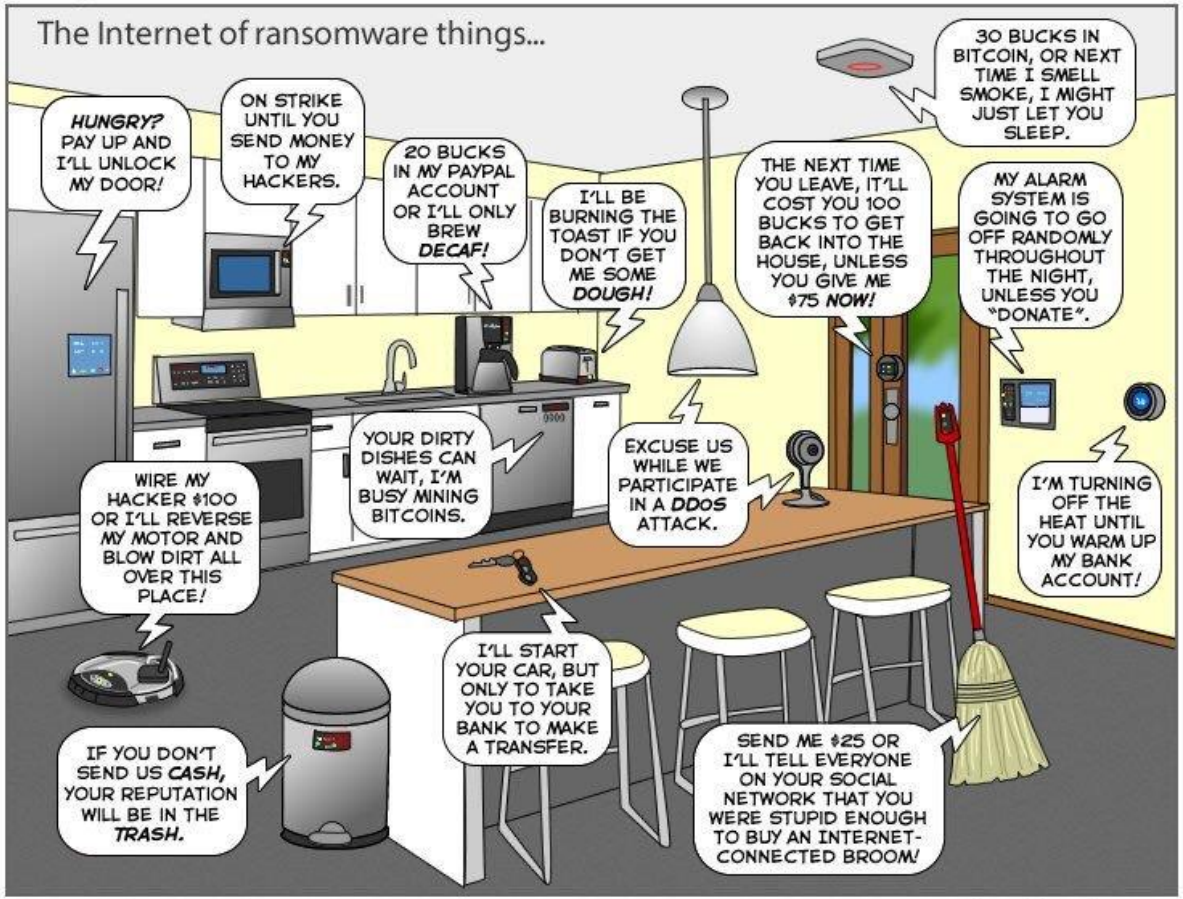
Propuesta

- Que los gobiernos, a través de los organismos adecuados, y con el aporte de todos los involucrados, establezcan las condiciones mínimas de seguridad que deben cumplir los dispositivos que se pretenden introducir al mercado

- Que se puedan “homologar” dispositivos en cuanto a la seguridad

- Que esto se sustente y replique en el ámbito internacional

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

URSEC
Unidad Reguladora de Servicios de Comunicaciones

JNT#2017

¡Gracias!

www.itc.com.uy
itc@itc.com.uy
lvidal@itc.com.uy

Tel: (+598) 2908.2908
Montevideo - Uruguay