UNIVERSIDAD D CÓRDOBA
ESPAÑA

I Congreso Internacional y Multidisciplinar de INVESTIGADORES EN FORMACIÓN

18 al 21 Febrero de 2019 | Manta - Ecuador

Impacto de la masificación de IoT en el poder de los ataques DDoS

Gabriel Agustín Cotera Ramírez
Docente de la Universidad Técnica de Manabí
Formación:
Magister en Informática de Gestión y Nuevas Tecnologías
Por la Universidad Técnica Federico Santa María.
Analista de Sistemas
Por la Universidad Laica «Eloy Alfaro» de Manabí

e-mail: gcoteras@utm.edu.ec
gabriel.cotera@fci.edu.ec

Introducción

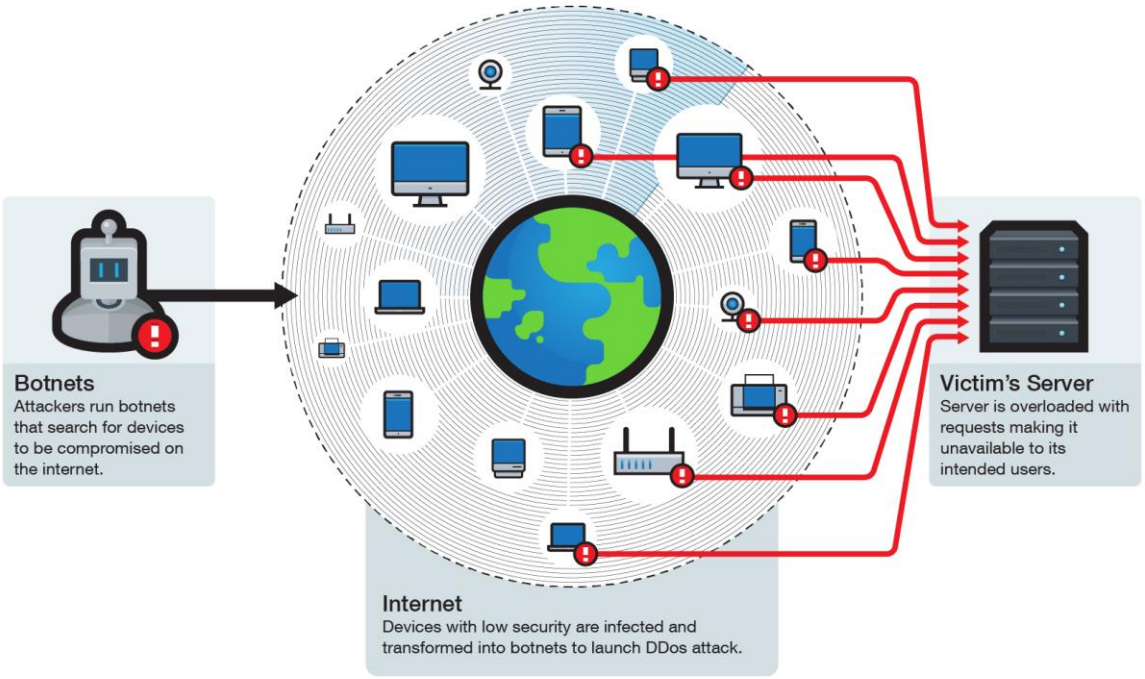
Los dispositivos relacionados al término Internet de las cosas (IoT) son “inteligentes”, consumen poca energía y necesitan poca o ninguna interacción humana para establecer comunicación entre ellos y transmitir datos por Internet.

Tienen el potencial para facilitar las tareas de captura de datos en tiempo real y de forma autónoma con precisión, ya sea, del ambiente, de un paciente de hospital, de un equipo industrial o una cámara de vigilancia. Esta versatilidad a hecho que se masifique su uso.

Fuente: https://www.ssh.com/iot/

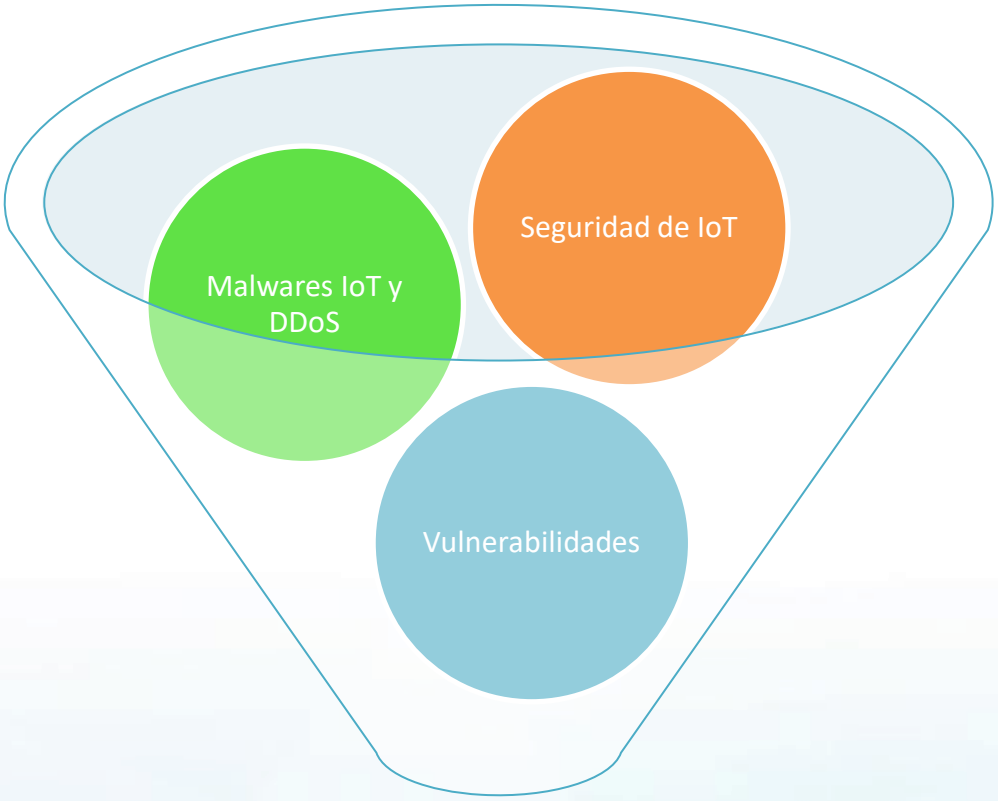
OBJETIVO DE ESTUDIO

Determinar la influencia del incremento masivo de los dispositivos de IoT en el poder de los ataques DDoS.



Fuente: https://blog.trendmicro.com/trendlabs-security-intelligence/internet-things-ecosystem-broken-fix/

METODOLOGÍA DE LA INVESTIGACIÓN



Informes de ataques recientes

Relación entre el crecimiento de IoT y el poder de los ataques de DDoS, influenciados por las vulnerabilidades

Fuente de la imagen: https://www.nauler.com/

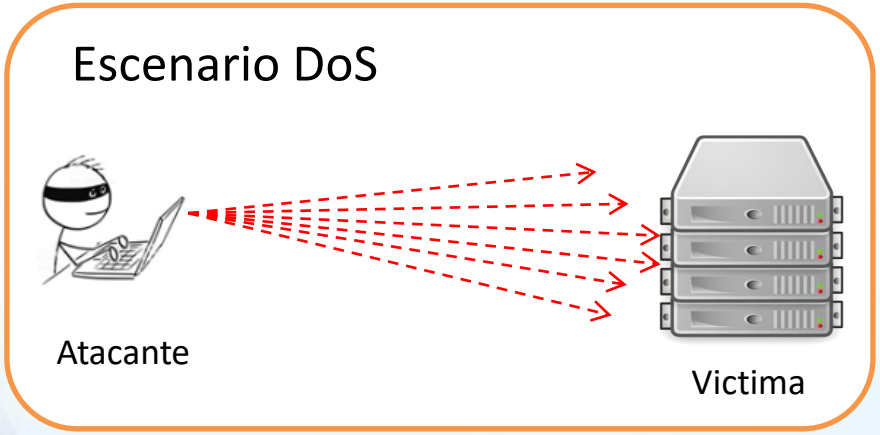
Seguridad

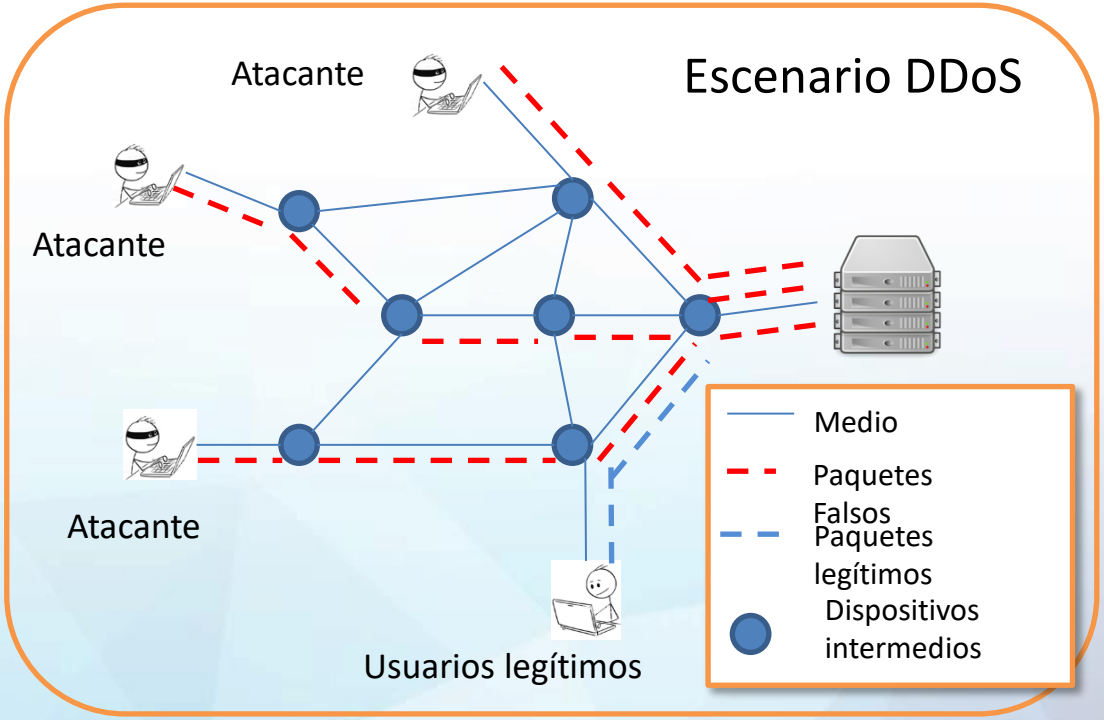
La capacidad de cómputo limitada, el número masivo de dispositivos de IoT inseguros que están en línea sumado a varias vulnerabilidades conocidas hacen que éste entorno sea terreno fértil para los cibercriminales (Silva, Silva, Pinto, & Salles, 2013) (Vlajic & Zhou, 2018) y un desafío para la ciberseguridad.

Perspectiva	Estratégia
Aplicación	Clave pública
	Hashing y extracción de elementos.
Arquitectura	SDN
Comunicación	Mejora de capas y protocolos
Datos	Seguridad E2E

Ataque DDoS

Consiste en enviar una gran cantidad de paquetes “falsos” que consumen los recursos de red o de computo de la víctima hasta dejarla temporalmente fuera de servicio (Nur & Tozal, 2018) (Singh, Singh, & Kumar, 2016) o con servicio de forma intermitente.





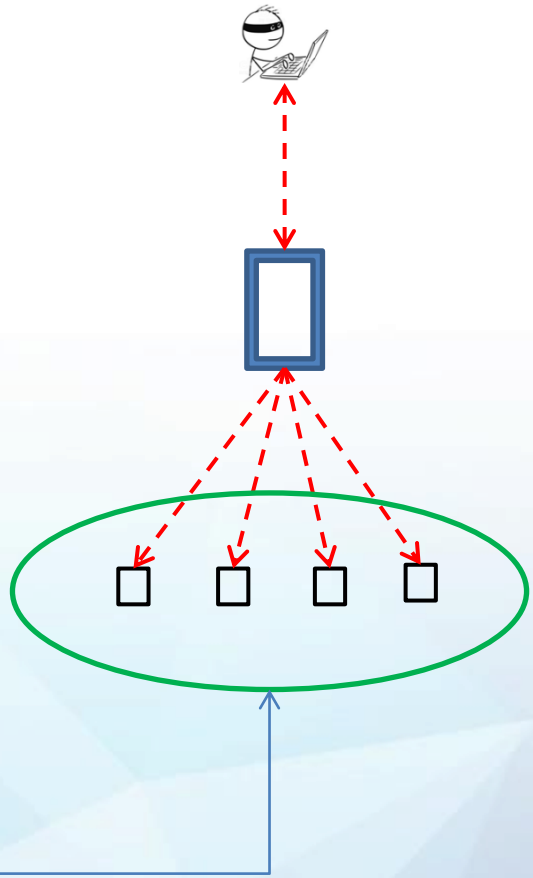
Componentes de un ataque DDoS

Atacante : Cibercriminal que ejecuta el ataque. Inicialmente infecta computadores que servirán de manejadores.

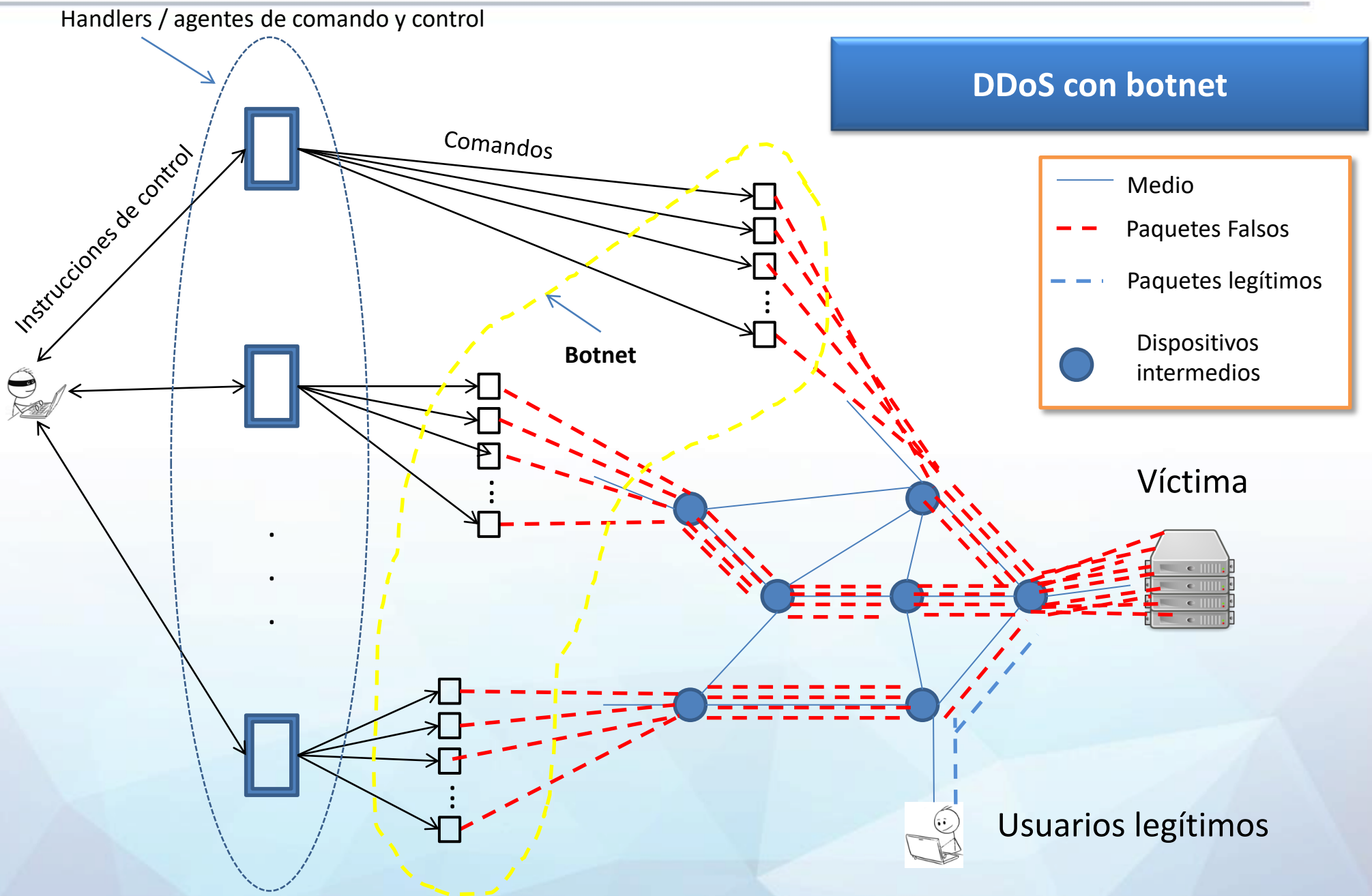
Manejadores (handlers / masters) : Computadores comprometidos que propagan el malware a otros dispositivos convirtiéndolos en bot y transmiten los comandos de control y ataque.

bot : Equipo infectado con malware que envía los paquetes de datos fraudulentos durante el ataque.

Una botnet es una colección de bots que están conectados a un manejador (Spognardi, Donno, Dragoni, & Giaretta, 2017) (Silva et al., 2013).



DDoS con botnet



Vulnerabilidades comunes

- **Contraseñas débiles**
- **Servicios de red inseguros**
- Interfaces de ecosistemas inseguros
- Mecanismos de actualización inseguros
- Componentes obsoletos
- Protección de privacidad insuficiente
- Almacenamiento y transferencia de datos inseguros
- Falta de gestión de dispositivos
- **Configuración predeterminada insegura**

Bertino & Islam, 2017) (OWASP Foundation, 2018)

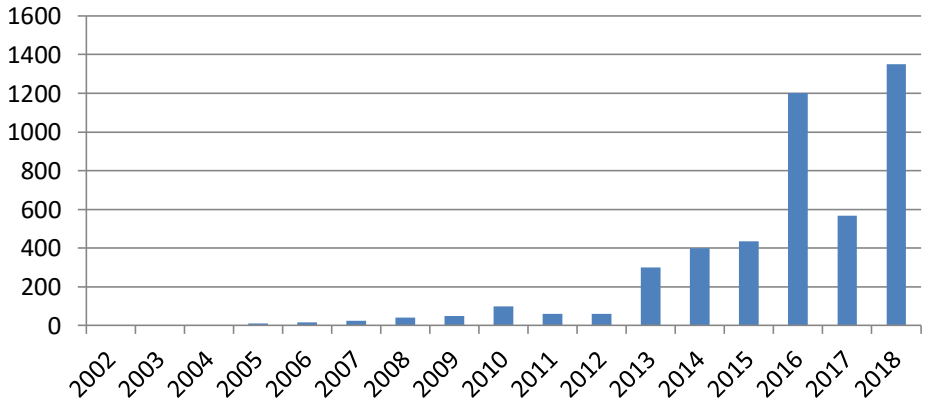
Malwares de IoT con capacidades de ataques de DDoS

Malwares de IoT con capacidad de ataque DDoS	Año de descubrimiento	Protocolo comprometido
Linux.Hydra	2008	UDP
PsyB0t	2009	UDP, ICMP
Chuck Norris	2010	UDP
Tsunami, Kaiten	2010	UDP,HTTP
Aidra, LightAidra, Zendran	2012	TCP XMAS
Spike, Dofloo, MsBlack, Wrkatk, Sotdas, AES.DdoS	2014	UDP, ICMP,
BASHLITE, LizKebab, Torlus, Gafgyt	2015	UDP
Elknot, BillGates Botnet	2015	UDP, ICMP, HTTP
XDOR.DdoS	2015	TCP
LUABOT	2016	HTTP
Remaiten, KTN-RM	2016	UDP,
NewAidra, Linux.IRCTelnet	2016	TCP XMAS
Mirai	2016	IP, HTTP
Amnesia, IoT Reaper, Reaper	2017	UDP, HTTP

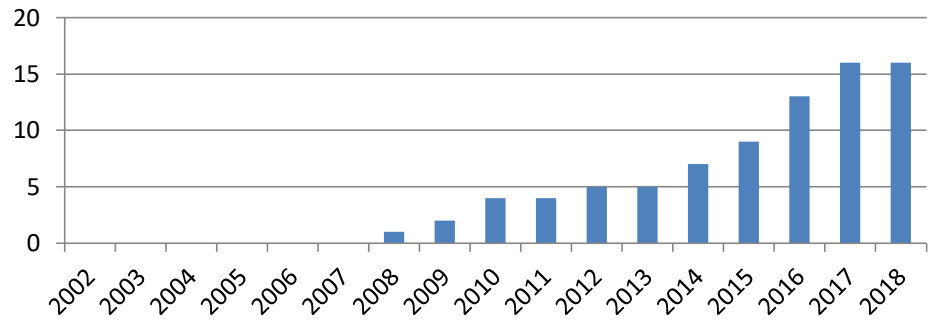
Fuente: adaptación de (Spognardi et al., 2017)

RESULTADOS

Ancho de banda de ataques DDoS en Gbps



Malwares del IoT con capacidades ataques DDoS



Capa	Protocolos con vulnerabilidad registrada en la NVD	Vulnerabilidades	Vulnerabilidades relacionadas con actividad DoS
Física / MAC	UMTS, GSM, GPRS, IrDA, LTE, WiMAX, 802.11, NFC, Bluetooth, 802.15.4, 6LoWPAN	295	45
Red	IPv4, IPv6, uIP,RPL, UPnP, ZigBee	491	451
Transporte	TCP, UDP, SSL / TLS	1429	1215
Aplicación	AMQP, WebSockets, MQTT, SOAP, Alljoyn	281	95

DISCUSIÓN

Los ataques DDoS son un problema serio para la cibereguridad, se están potenciando con el desarrollo de IoT (Spognardi et al., 2017) caracterizándolo de forma negativa. El gran número de dispositivos de IoT que han sido comprometidos están ayudando a los cibercriminales a perpetrar ataques sigilosos y difíciles de detectar, logrando un ancho de banda cada vez mayor. En el 2010 es el primer ataque DDoS de gran magnitud (para la época), el ancho de banda solo fue de un poco más de 100 Gb / s, pero representó el doble de lo alcanzado en el 2009.

Los ataques permiten que las organizaciones de seguridad, investigadores y científicos determinen el crecimiento y actualización de los malwares que se encuentran en Internet reclutando dispositivos de IoT.

Las capas de red y transporte tienen un mayor número de vulnerabilidades conocidas. En estas capas están los protocolos más antiguos y que se encuentran en toda la infraestructura de Internet..

CONCLUSIONES

Después de 20 años del primer ataque de DoS estos tipos de amenaza siguen latentes. Evolucionaron en los ataques DDoS que se lanzan utilizando botnets que en la actualidad están conformadas mayormente por dispositivos de IoT.

Aunque en la pila de protocolos de IoT la mayoría tiene identificada al menos una vulnerabilidad en los ataques DDoS se utilizan unos pocos.

Basándonos en la literatura científica previa e informes de ataques DDoS, mostramos que éstos han incrementado el poder de ataque en el tiempo que se detectaron malwares de IoT nuevos o la evolución de uno existente. Aún así, no podemos precisar exactamente cuántos malwares para IoT están “sueltos” en el Internet y mucho menos el número de dispositivos comprometidos.

UNIVERSIDAD D CÓRDOBA
ESPAÑA

I Congreso Internacional y Multidisciplinar de INVESTIGADORES EN FORMACIÓN

18 al 21 Febrero de 2019 | Manta - Ecuador