Denegación de Servicio y su impacto en el negocio bancario: cómo prepararse y responder a esta amenaza

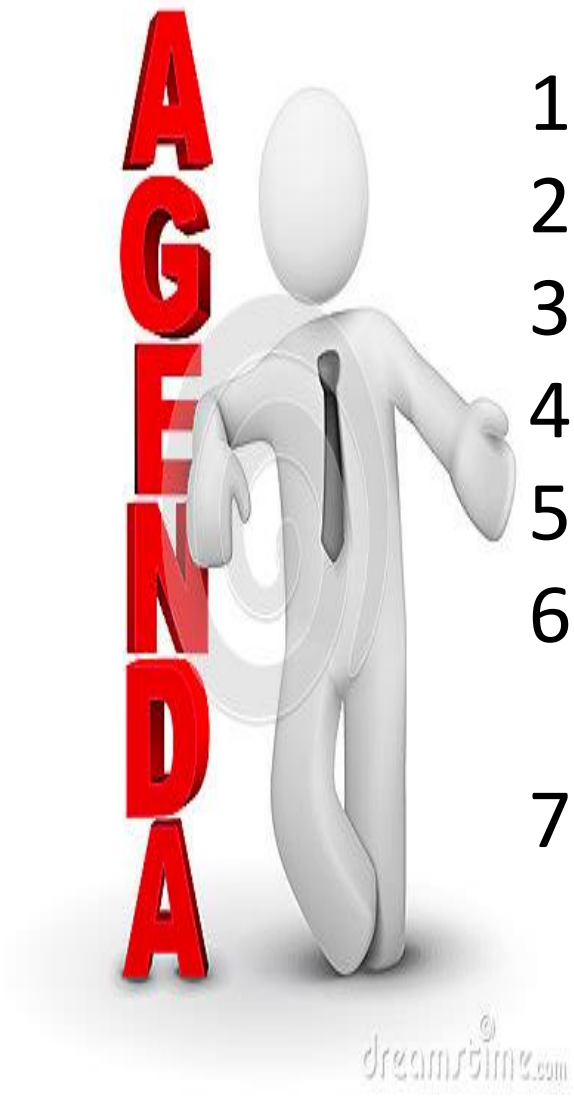
Carlos Luis Vidal, MBA, CISA, CISM, CISSP, CFE, CIA, Security+

CELAES 2016
31st Financial Security Conference

FIBA

FELABAN

FOLLOW US
@fiba_bankers



1. Introducción a los DDos
2. Razones y motivación de un DDos
3. Tipos de DDos
4. Ddos y Botnets: Retos y tendencias
5. Impacto al negocio
6. Herramientas, Medidas Proactivas y Reactivas contra los DDos
7. Conclusiones

CELAES 2016
31st Financial Security Conference

FIBA

FELABAN

FOLLOW US
@fiba_bankers

1. Introducción a los DDos

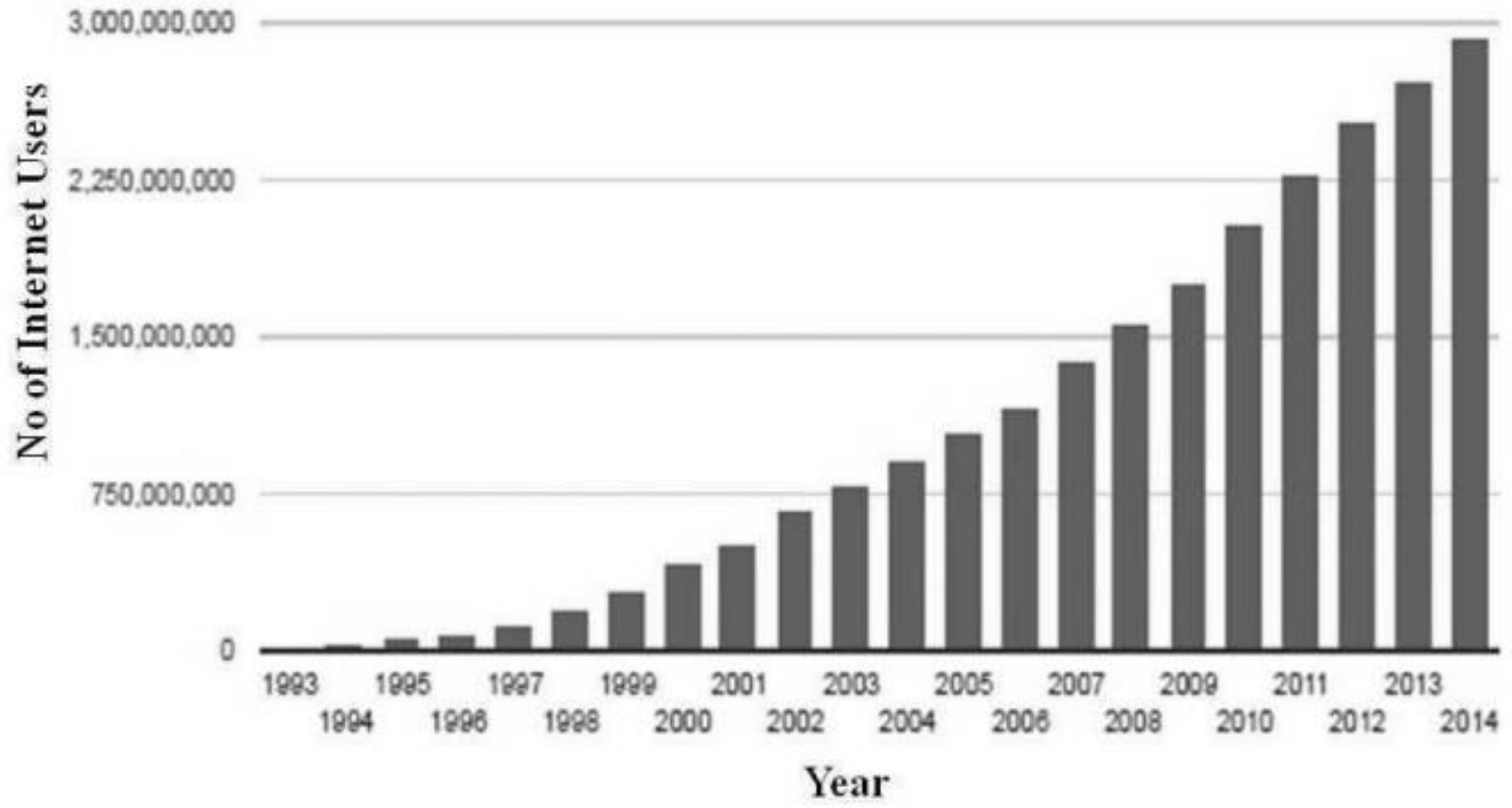
Definición:

Un DDos es un ataque coordinado llevado a cabo usando un largo número de host comprometidos con el fin de interrumpir un servicio.

Los ataque DDos, han comenzado a tener mayor notoriedad en los sistemas bancarios desde el 2010 (Operación Abibal). Este año Anonymus lanzó una operación llamada OpIcarus.

1. Introducción a los DDos

Aumento creciente de usuarios de Internet



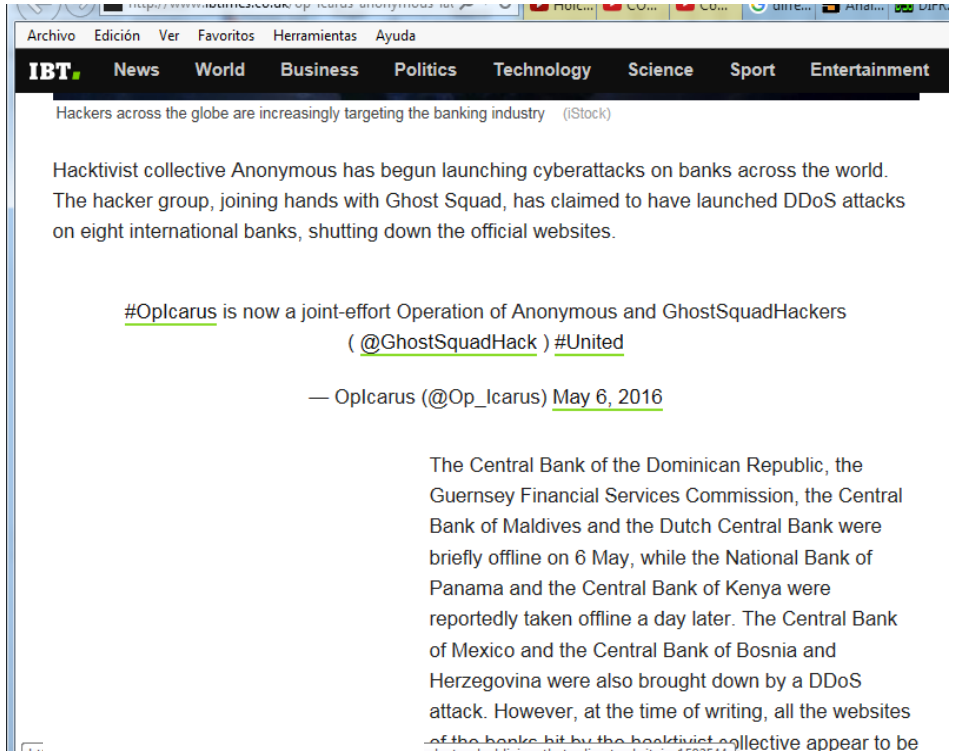
CELAES 2016
31st Financial Security Conference

FIBA

FELABAN

FOLLOW US
@fiba_bankers

1. Introducción - Noticias



Archivo Edición Ver Favoritos Herramientas Ayuda

IBT. News World Business Politics Technology Science Sport Entertainment

Hackers across the globe are increasingly targeting the banking industry (iStock)

Hacktivist collective Anonymous has begun launching cyberattacks on banks across the world. The hacker group, joining hands with Ghost Squad, has claimed to have launched DDoS attacks on eight international banks, shutting down the official websites.

#OpIcarus is now a joint-effort Operation of Anonymous and GhostSquadHackers (@GhostSquadHack) #United

— OpIcarus (@Op_Icarus) May 6, 2016

The Central Bank of the Dominican Republic, the Guernsey Financial Services Commission, the Central Bank of Maldives and the Dutch Central Bank were briefly offline on 6 May, while the National Bank of Panama and the Central Bank of Kenya were reportedly taken offline a day later. The Central Bank of Mexico and the Central Bank of Bosnia and Herzegovina were also brought down by a DDoS attack. However, at the time of writing, all the websites of the banks hit by the hacktivist collective appear to be

Pietro Romano @tribal_sec · 9 jun.
#Anonymous shut down the #Bank of #Greece website with #DDoS #attack techworm.net/2016/05/anonym… #OpIcarus #cyberattack #Legion

Anonymous shut down the Bank of Greece website…

Anonymous DDoS Bank of Greece website to protest against the global corruption in finance and banking sector The online hacktivist group, Anonymous has rec

techworm.net

AMERICAN BANKER | Bank Technology

Recent Issues | Magazine | Video | Web Seminars | White Papers | Women in Banking | FinTech Forward

DEALMAKING & STRATEGY | COMMUNITY BANKING | NATIONAL/ REGIONAL | LAW & REGULATION | CONSUMER FINANCE | BANK TECHNOLOGY | BANKTHINK

Banks Lose Up to $100K/Hour to Shorter, More Intense DDoS Attacks

By Penny Crosman
April 23, 2015

Twitter LinkedIn Facebook Google + Email Comments Print Reprints

Distributed denial of service attacks have morphed from a nuisance to something more sinister.

In a DDoS attack, heavy volumes of traffic are hurled at a website to halt normal activity or inflict damage, typically freezing up the site for several hours. Such exploits achieved notoriety in the fall of 2012 when large banks were hit by a cyberterrorist group.

But the Operation Ababil attacks were simply meant to stop banks' websites from functioning. They caused a great deal of consternation among bank customers and the press, but little serious harm.

RELATED

Enlarge This Image

What Banks Need to Know from Verizon's Comprehensive Breach Report

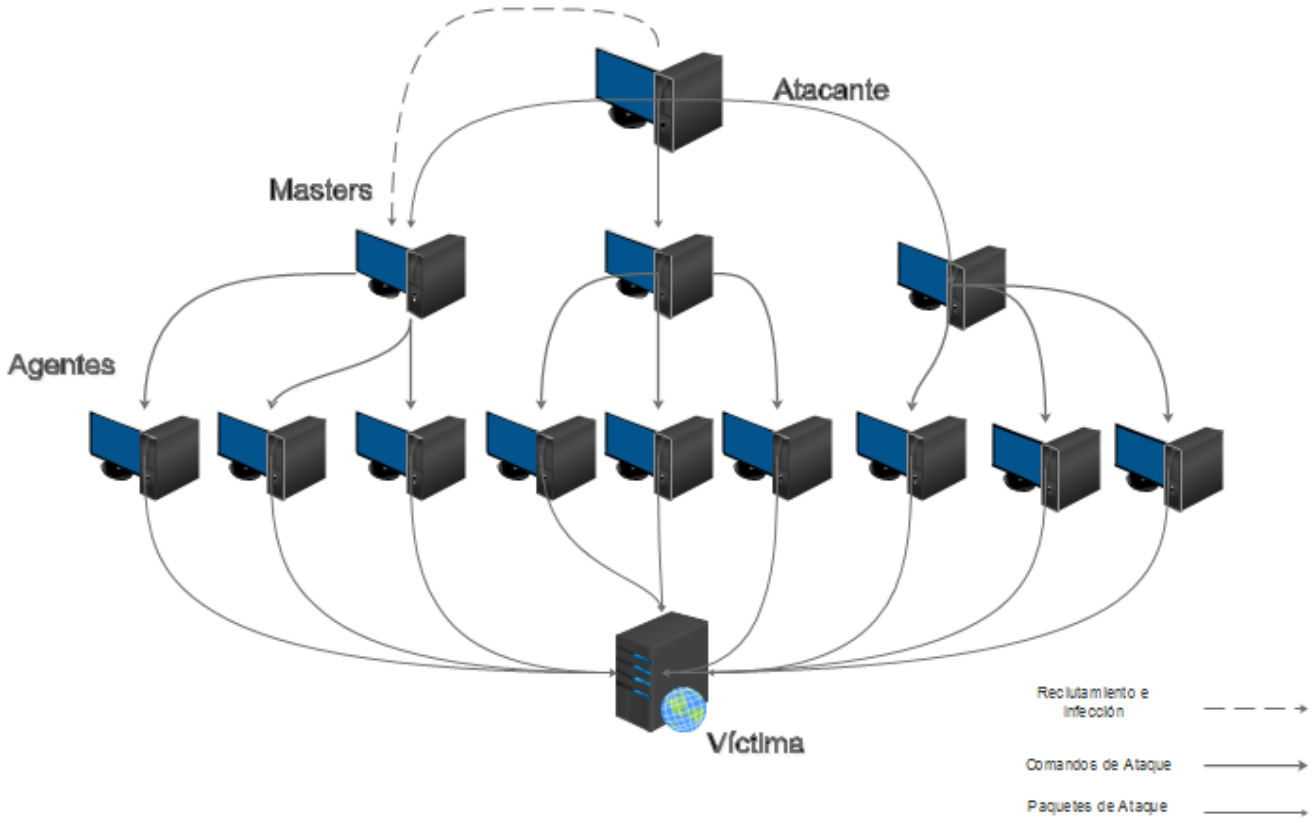
DDoS Attacks Are Still Happening — and

1. Introducción a los DDos

Ejecución de un DDos:

Consta de 4 pasos básicos:

Reclutamiento, Infección, Comandos de ataque y paquetes (tráfico) de ataque.



2. Razones y Motivación de un DDos

- **Competencia:** Su empresa es competidora de la empresa del atacante.
- **Ideológicos**: los mensajes y/o valores no correspondes con los de los atacantes, por lo cual desean silenciarlo.
- **Chantaje:** alguien quiere que usted pague una cantidad de dinero, no es diferente de la extorsión "la vida real".
- **Política:** un grupo de individuos quiere vengarse de un Estado (instituto, organización) debido a sus opiniones políticas diferentes. Muchas veces, es impulsado por un Estado.
- **Desafío:** alguien quiere mostrar su nivel de conocimientos
- **DDos No intencionales:** Productos, canal o servicio nuevo donde no se estimó bien la capacidad.

3. Tipos de DDos

Existen varios tipos de Ddos, sin embargo se podrían agrupar en 3 grupos:

1. **Ataques volumétricos :** Sobrecargar ancho de red**.**

2. **Ataques de tráfico:** Sobrecargar capacidad de recursos del servidor o componentes de red.

3. **Ataques de Capa Aplicación:** Aprovechar vulnerabilidades de los aplicativos web.

4. DDOS y BOTNETS – Tendencias y Retos

Categorías:

Características	Móvil	Fijo
Uso de Dirección IP	Private	Público
Poder de Batería	Limitado	Ilimitado
Ancho de Banda	Limitado	Ilitimado
Colección de	Dispositivos Móviles	Dispositivos Fijos
Gestión de seguridad Centralizado	NO	SI
C & C protocol	SMS, MMS, Bluetooh	HTTP, DNS, P2P, IRC

CELAES 2016
31st Financial Security Conference

FIBA

FELABAN

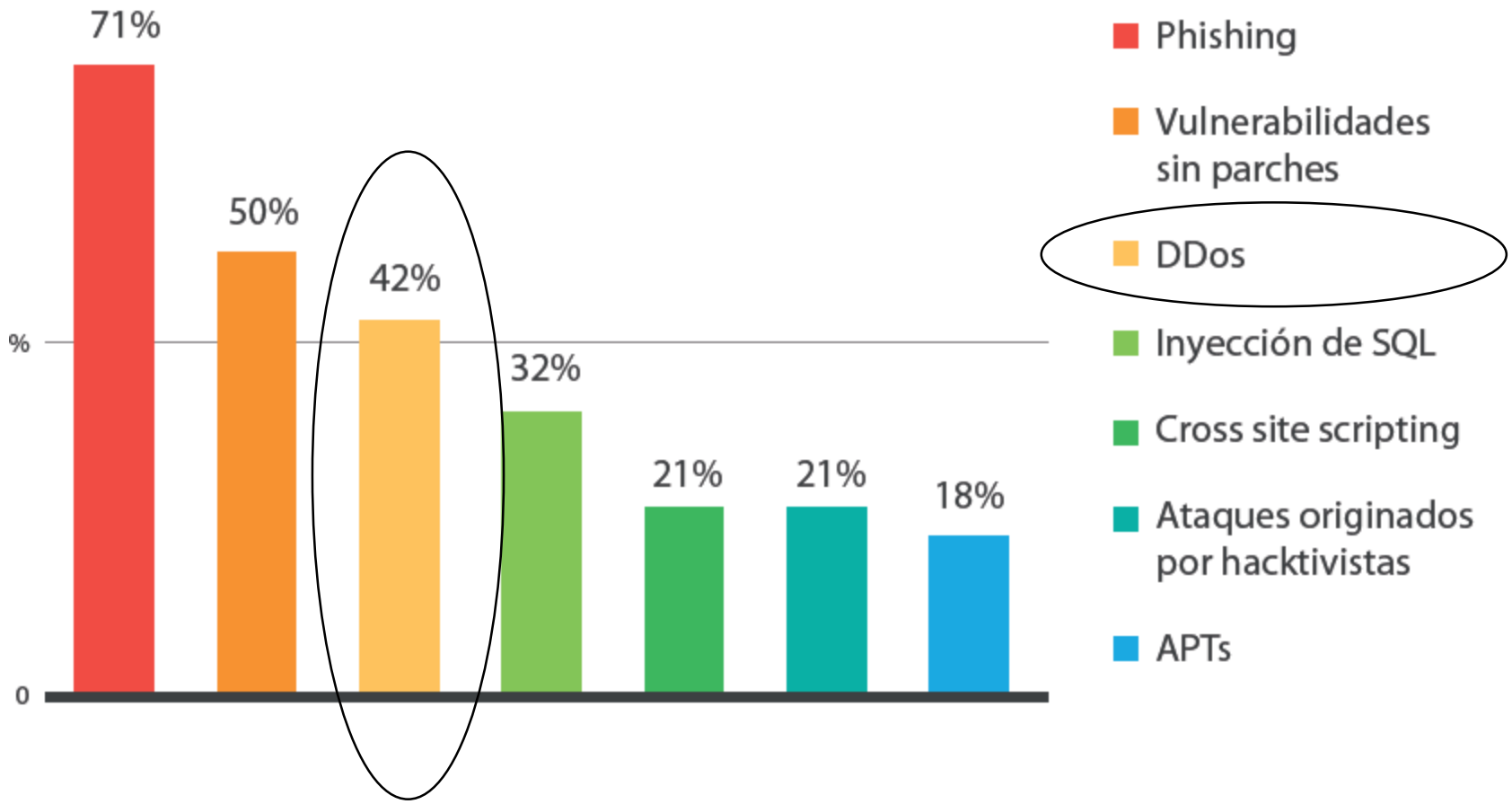
FOLLOW US
@fiba_bankers

4. DDOS y BOTNETS – Tendencias y Retos

Ataques DDos por Industria: 3° Servicios Financieros

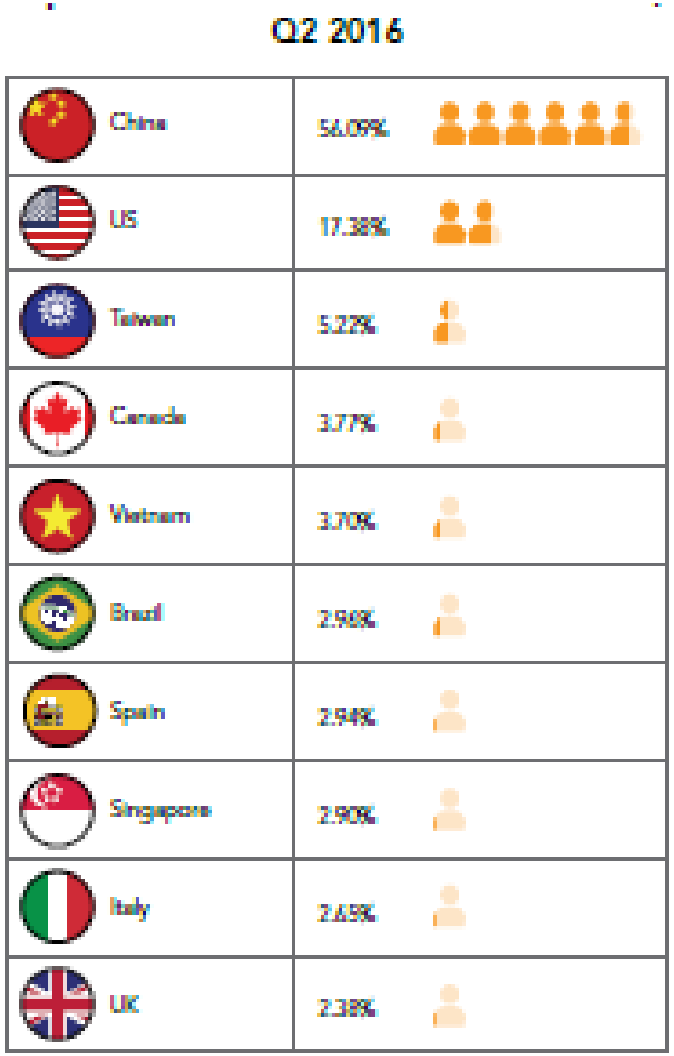
4. DDOS y BOTNETS – Tendencias y Retos

Frecuencia por tipo de ataques informáticos



Fuente: Akamai's state of the internet / security

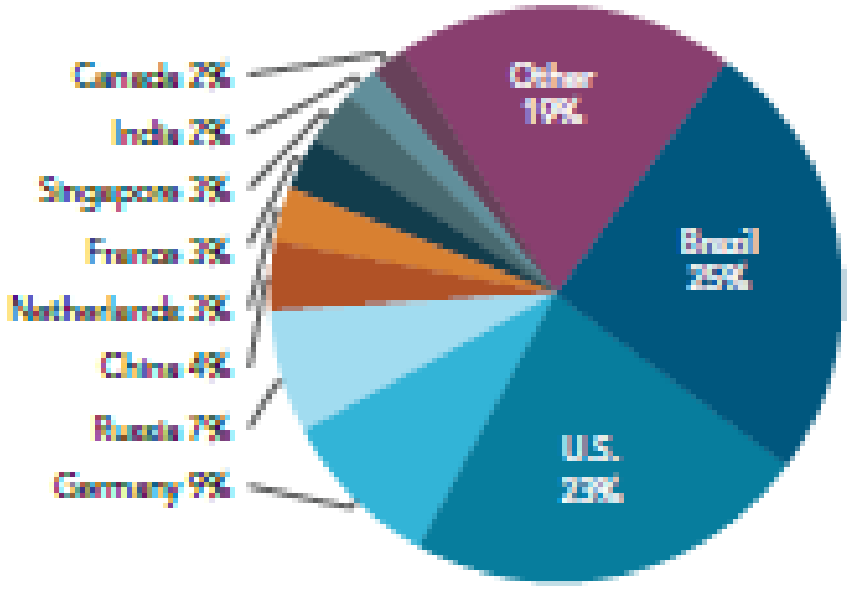
4. DDOS y BOTNETS – Tendencias y Retos



Top 10: Países Origen de Ataques DDos
2 Semestre del 2016

4. DDOS y BOTNETS – Tendencias y Retos

Fuentes de ataques Web Application por Industria
Segundo Semestre 2016

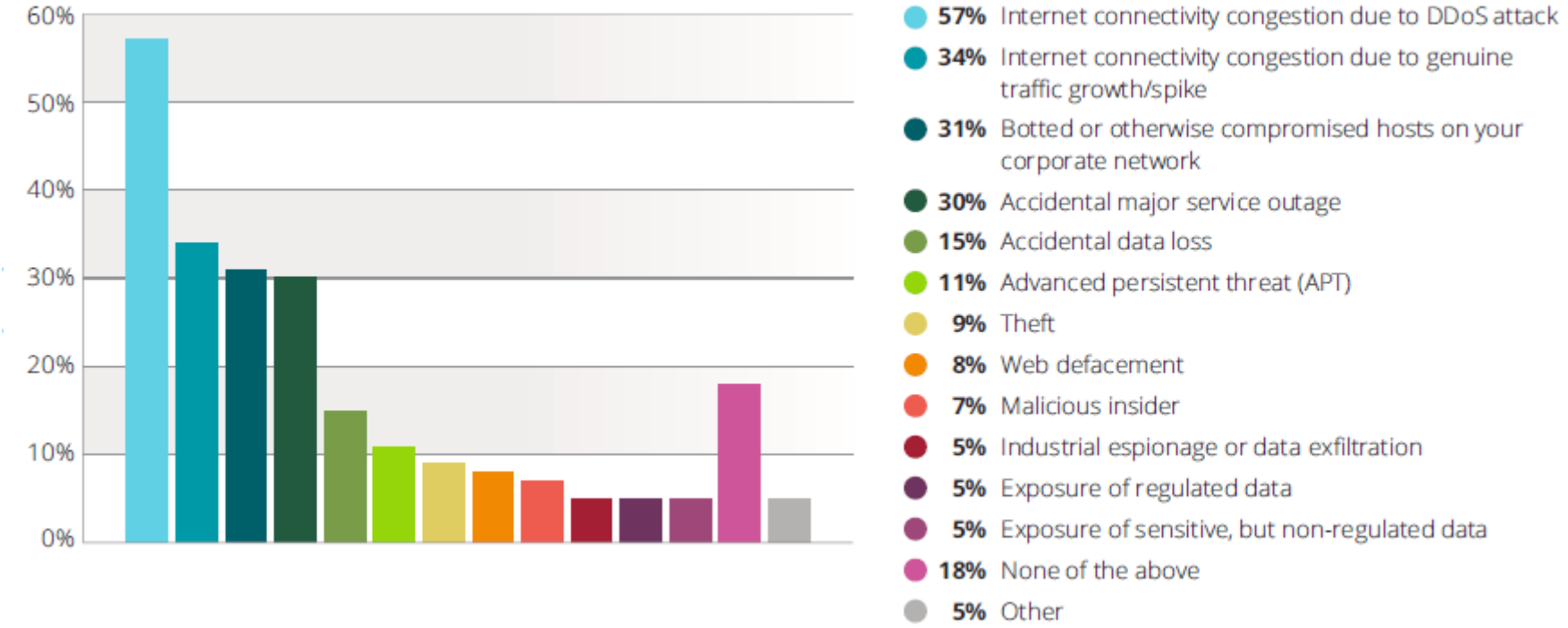


Brasil desplazó a USA el ultimo trimestre del año.

Fuente: Akamai's state of the internet / security

4. DDOS y BOTNETS – Tendencias y Retos

Amenazas Observadas en Redes corporativas

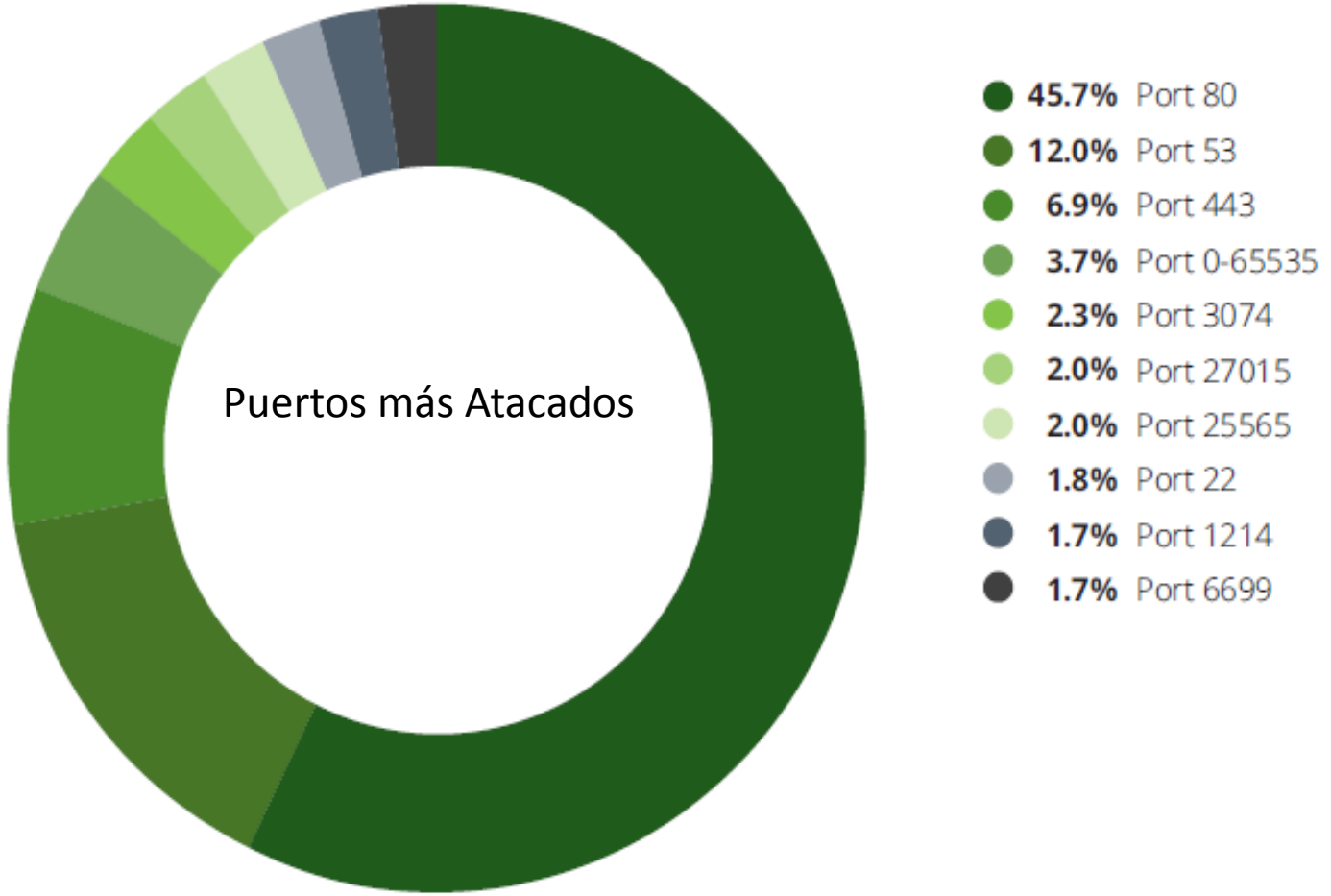


Fuente: Akamai's state of the internet / security

4. DDOS y BOTNETS – Tendencias y Retos

Puertos (Servicios) más atacados por los DDos

El 65 % de ataques es dirigido a los puertos 80 (web) , 53 (dns) y 443(Https)



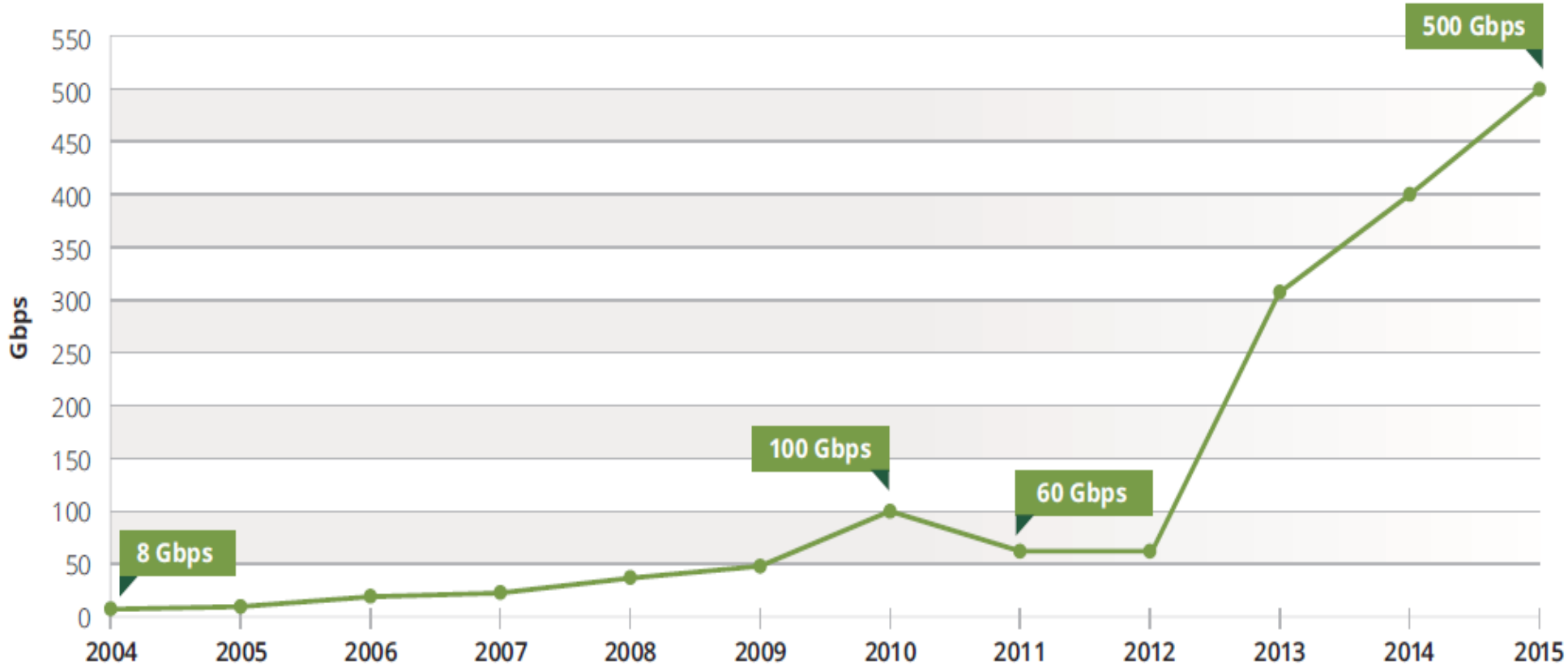
Fuente: Arbor Network Infraestructure Report ATLAS 2016,,.

CELAES 2016
31st Financial Security Conference
FIBA
FELABAN
FOLLOW US
@fiba_bankers

4. DDOS y BOTNETS – Tendencias y Retos

Crecimiento del tamaño de los ataques Ddos por Año .

En los últimos años la tendencia es un crecimiento agresivo del tamaño de ataques.



Aumento de los ataques de Ddos en 73% con respecto al 2015.

Fuente: Arbor Network Infraestructure Report, Q2 2016.

4. DDOS y BOTNETS – Tendencias y Retos

Tamaño pico de ataques, hace una semana….

IoT: no solo se usa host, sino también camaras ip y grabadoras de video digital

Fuente: Arbor Network Infraestructure Report, Q2 2016.

5. Impacto al negocio de los DDos

- Daño a la **marca** y reputación.
- Incumplimiento de **contratos** y violaciones a los **SLA**s.
- Pérdida de confianzas de los **stakeholders.**
- Interrrupción del servicio que afectaría, por ejemplo, la emisión de créditos, no renovación de servicios y pérdida en ventas/servicios (**lucro cesante**)
- Costos de **marketing** y **publicidad** asociados para minimizar el daño en los medios.

5. Impacto al negocio de los DDos

Compañias tienen **costos** asociados a las caídas de sus sistemas de alrededor del **3.6 % de sus utilidades**.

Fuente: Infonetics' survey, The Cost of Server, Application, and Network Downtime. 2015.

Un **tercio (1/3)** de los incidentes de **caídas de los sistemas**, se encuentran atribuidos a **Ddos attacks**.

Fuente: Verisign/Merril Research. 2015

El **costo promedio** de ataque de DDos es **$5,600/minuto** o más de **$300K/hora**.

Fuente: The Cost of Downtime, Lerner (November, 2014)

6. Herramientas, medidas proactivas y reactivas anti-DDos

Proactivas (tendencias y posibilidad de ocurrencia)

- Firmas
- Basado en comportamiento anómalo
- Híbridos

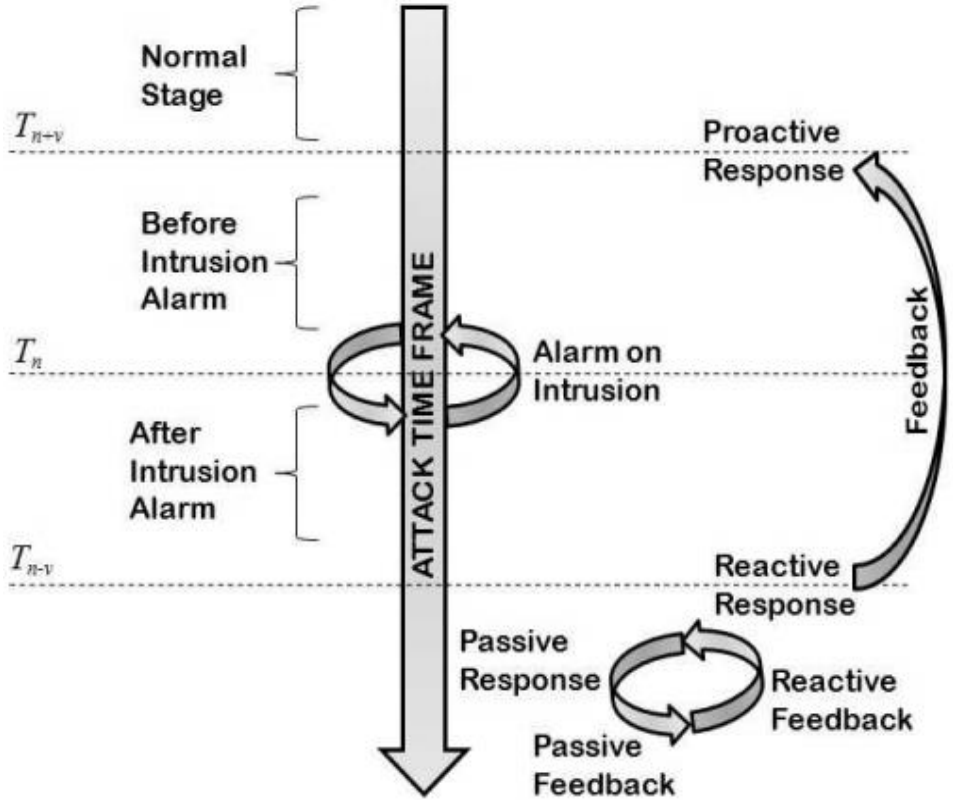
Reactivas (cuando el ataque es confirmado)

- Emiten alarmas
- Bloquean paquetes
- Bloquean Ips

  Basado:

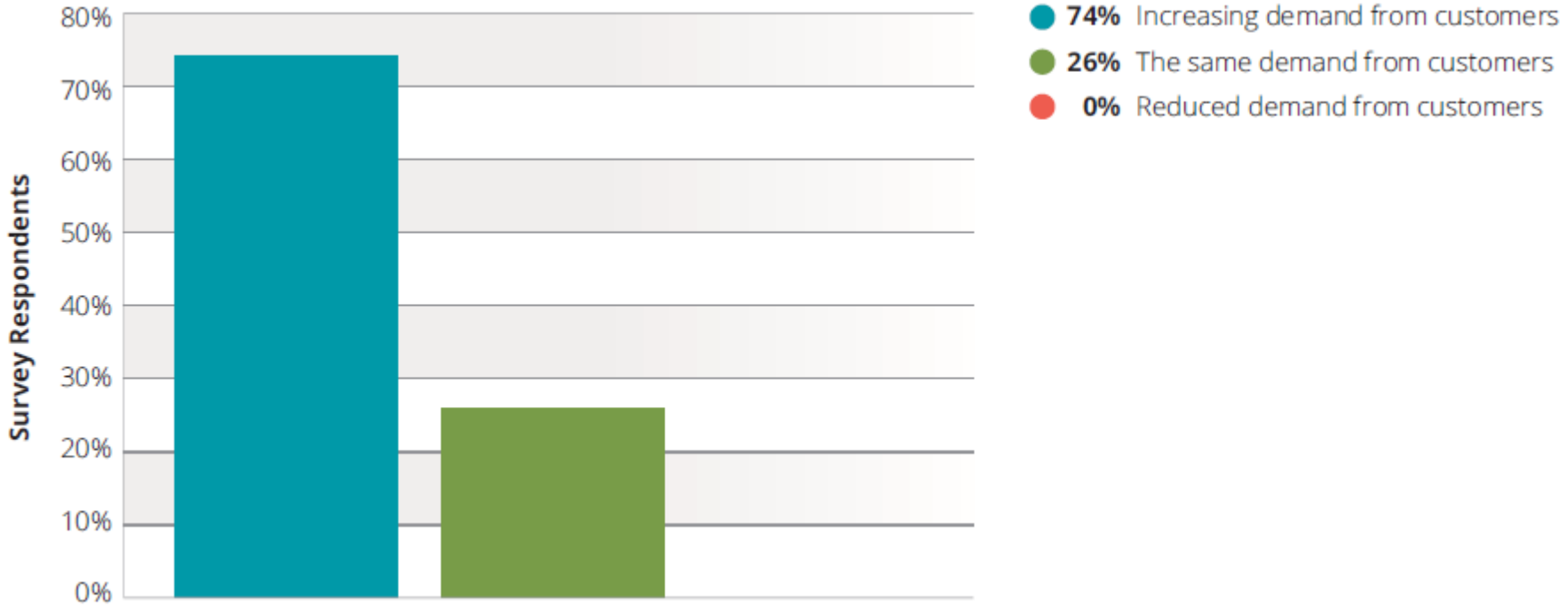
  Reconocimiento de IPS

  Basado en filtros (Ingress and Egress)



6. Herramientas, medidas proactivas y reactivas anti-DDos

Demanda por servicios de Detección/Mitigación de Ataques DDos

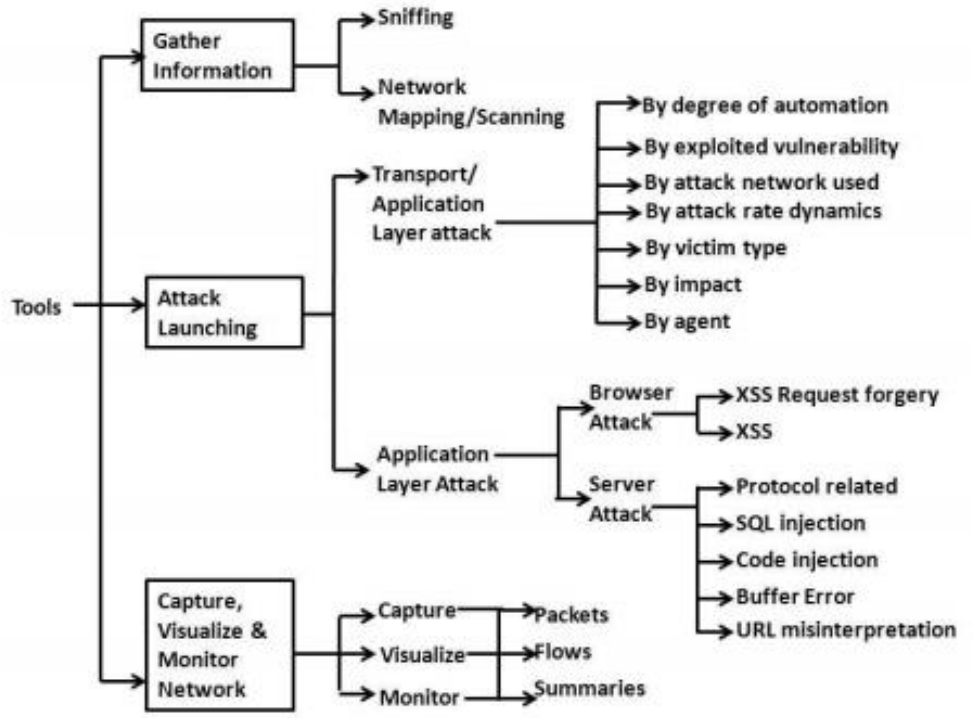


Fuente: Akamai's state of the internet / security

6. Herramientas, medidas proactivas y reactivas anti-DDos

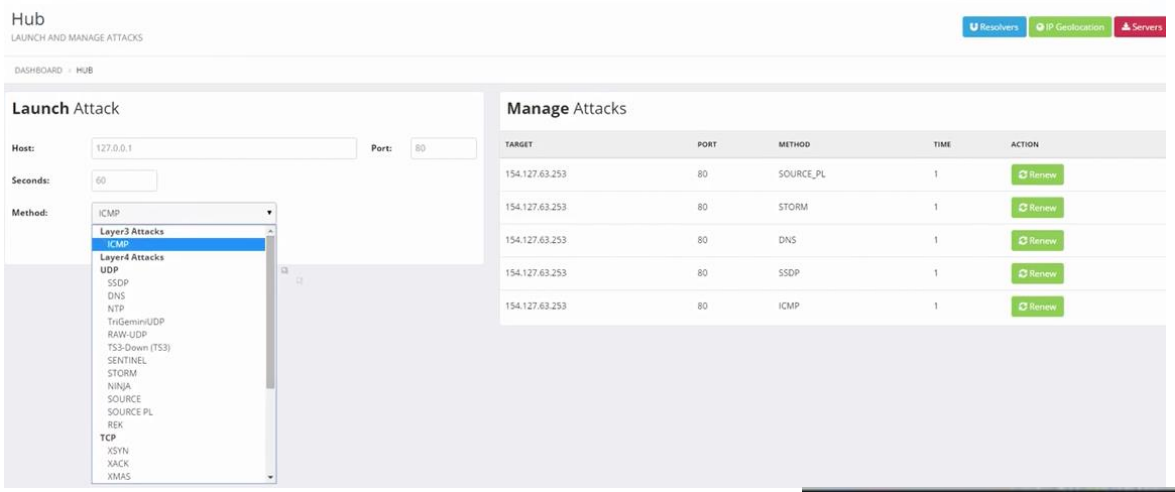
Pueden ser de 3 tipos:

- ✓ Herramientas de captura de información
- ✓ Herramientas de ejecución de ataque (LOIC y HOIC)
- ✓ Herramientas de captura, monitoreo y visualización



Fuente: Ddos Attacks: Detección, Prevención, Reacción y Tolerancia, Dhruba Kumar Bhattacharyya, Jugal Kumar Kalita, 2016

6. Herramientas, medidas proactivas y reactivas anti-DDos



7. Conclusiones sobre Ddos en el sistema bancario

1. Protección tradicional contra ataques Ddos actuales **resulta ser ineficaz.** Recordar diversas soluciones **(y su alcance)** considerar: Firerwalls, IDS, NOC (**rendimiento y disponibilidad**), WAF (Protocolos de capa 7), SIEM (**timestamp**), Hardening, Un proveedor de Servicio Anti DDOs- SOC (Seguridad) **24/7**. **Nuevas** amenazas, soluciones que deben **evolucionar**.

2. Los ataques DDoS han entrado en una nueva fase peligrosa: ataques con mayor número de Host comprometidos (miles) y mayor pico de tráfico (**> 1 000 GBs). Aumento del 73% con respecto al 2015.**

3. **Menos dinero y personas** atacantes **son necesarios, pero mayor cantidad de voluntarios (cómplices) y/o involuntarios. Dificultad de trazabilidad.**

CELAES 2016
31st Financial Security Conference
FIBA
FELABAN
FOLLOW US
@fiba_bankers

7. Conclusiones sobre Ddos en el sistema bancario (continuación..)

4. Además de la **pérdida monetaria**, considerar el daño a **la reputación de la marca** por los ataques DDoS. Tomar en cuenta que ahora la comunicación es en tiempo real para los clientes **(redes sociales).**

5. Existencia en internet de diversas herramientas DDos/Botnets **libres y/o bajo costo.** Así como i**nterfaces** y/o comandos **sencillos.**

6. Bancos **de todo tamaño** son vulnerables a los ataques DDoS.

7. Plan de Manejo ante Crisis y Gestión de Incidentes. ¡**No sólo aspectos técnicos**!!

8. Los ataques demuestran la necesidad de prevención, detección, reacción (corrección) y **tolerancia (recuperación)** anti-DDoS.

¡Muchas gracias!

cluisv@intercorp.com.pe
cluis@pucp.edu.pe