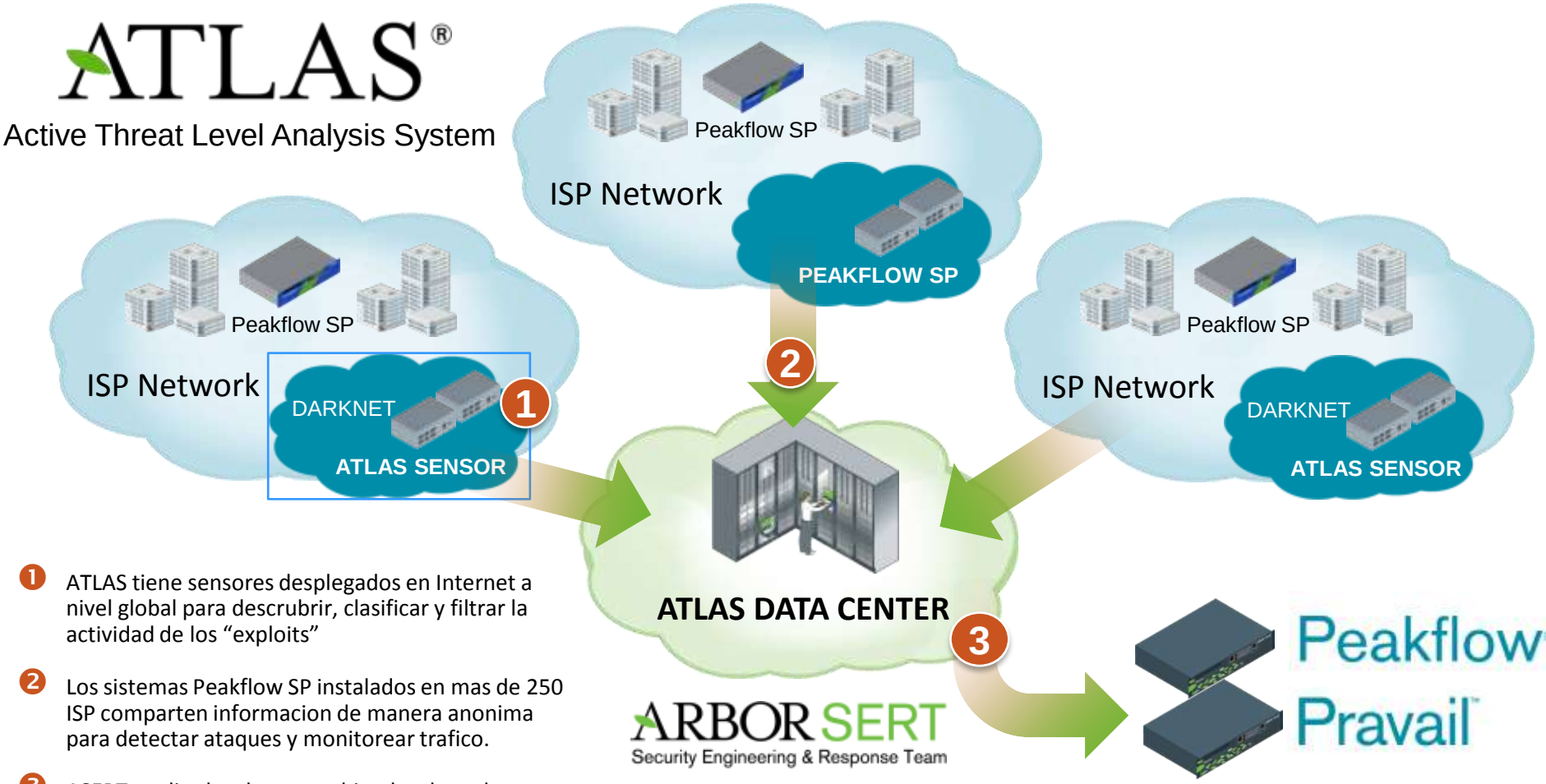
La Problematica de DDOS: Lo que importa no es el tamaño, es la complejidad.

Federico Chaniz – Channel Director
fchaniz@arbor.net

ATLAS: Inteligencia Global de Amenazas

ATLAS®

Active Threat Level Analysis System

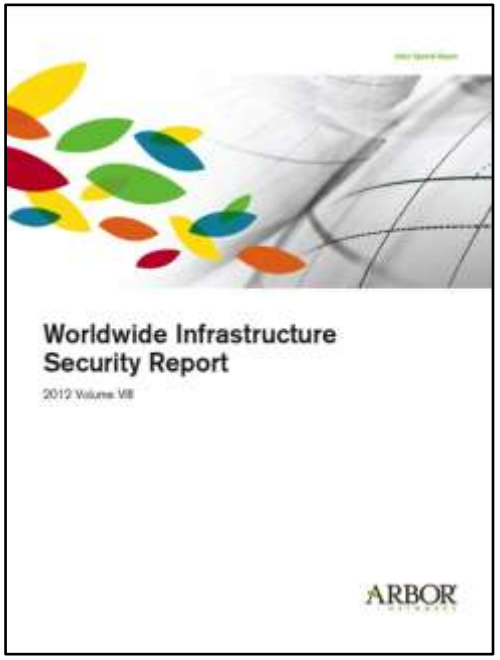


1. ATLAS tiene sensores desplegados en Internet a nivel global para descrubrir, clasificar y filtrar la actividad de los “exploits”
2. Los sistemas Peakflow SP instalados en mas de 250 ISP comparten informacion de manera anonima para detectar ataques y monitorear trafico.
3. ASERT analiza los datos combinados de malware y nuevos vectores de ataques detectados, y los convierte en informacion que alimenta las soluciones de Arbor.

DDOS y la Disponibilidad de Servicio

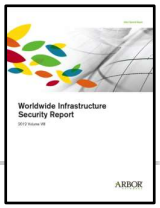
- La Disponibilidad de Servicios es critica.
  - Los ataques de DDoS sacan a las empresas de Internet y no le permiten acceder a los servicios.
  - La mayoria de las organizaciones cuentan con la Internet para mantener la continuidad del negocios.

- Los ataques de DDOS.
  - Existen mayores motivaciones para la generacion de ataques.
  - Los ataques de DDOS son muy faciles de realizar.
  - Estan altamente desarrollados a nivel social.



ARBOR NETWORKS

Que motiva los ataques de DDOS?



33% Ideological

31%
Online gaming

33%

27%
Vandalism/nihilism

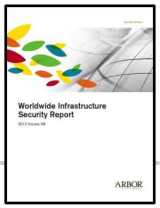
What drives DDoS attacks?

One third of reported attacks were
driven by political or ideological disputes

ARBOR NETWORKS

Source: Arbor Networks 8th annual Worldwide Infrastructure Security Report; time period: Oct 2011 - Sept 2012

La Nuevos Patrones de Ataques de DDOS



Mas Complejos

- Los ataques de Nivel de Aplicacion y Multi Vectoriales son cada vez mas comunes.
- El Malware usa ahora mecanismos mas complejos de infiltracion.

Mayor Capacidad

- Mayor cantidad de Botnets disponibles para lanzar ataques distribuidos y a nivel de aplicacion.
- Las herramientas disponibles hacen que generar un ataque sea cada vez mas simple.

Coordinados

- Los ataques de DDOS se usan para cubrir o iniciar otro tipo de actividades criminales..
- Las campañas para ataques complejos y multi vecoriales estan cada vez mas organizadas.


Major U.S. banks still under DDoS attack

Posted on 28 September 2012.

PNC Bank seems to be the latest target of the organized DDoS attacks against major U.S. financial institutions such as JPMorgan Chase, Bank of America, Wells Fargo, Citigroup, U.S. Bancorp, New York Stock Exchange and others.

In the week, the banks' websites have been intermittently bombarded with a flood of requests that left their own customers unable to reach them and perform financial transactions via internet banking.

According to the statement posted online by the self-styled Izz ad-Din al-Qassam Cyber Fighters group, the attacks are a way of forcing the takedown of the controversial video that, according to the group, mocks the prophet Muhammad.

The hacktivists have also provided links to two sites that, when visited by volunteers, automatically use their computers to flood the aforementioned sites with requests.


New DDoS Warning Issued by Regulator

Second Alert Recommends Defensive Steps

The National Credit Union Administration is the second federal banking regulator to issue an alert about fraud risks linked to distributed denial of service attacks.

In late December, the Office of the Comptroller of the Currency also issued an alert about DDoS activity.

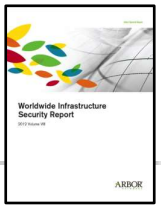
Attorney Joseph Burton, a cybercrime and information security expert and managing partner of law firm Duane Morris LLP, says banking institutions should heed these notices as warnings that DDoS strikes will continue this year.

"In the attacks we're talking about, there have definitely been account transfers," Burton says, adding that banks and credit unions have an obligation and responsibility to address these risks and ensure they have the right types of programs in place.

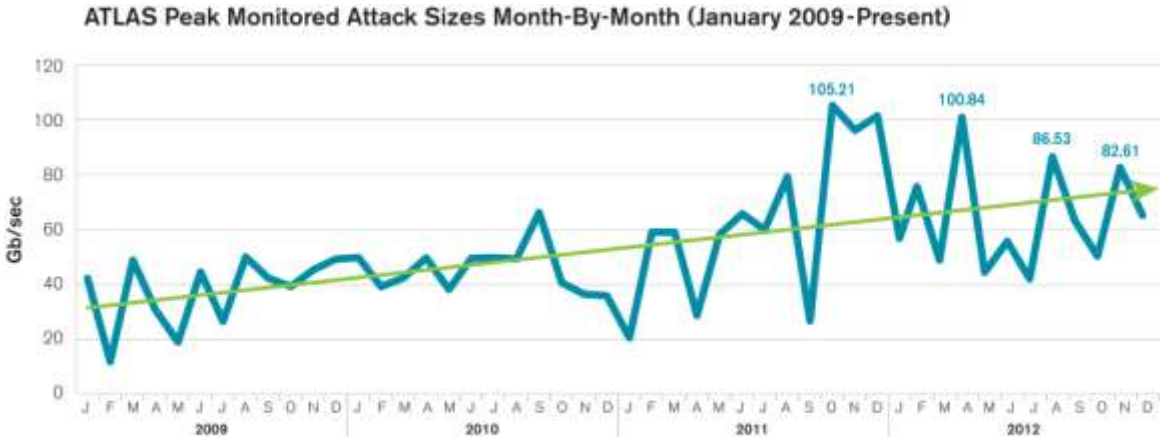
RELATED CONTENT

ARBOR NETWORKS

Tamaño de los Ataques Volumetricos

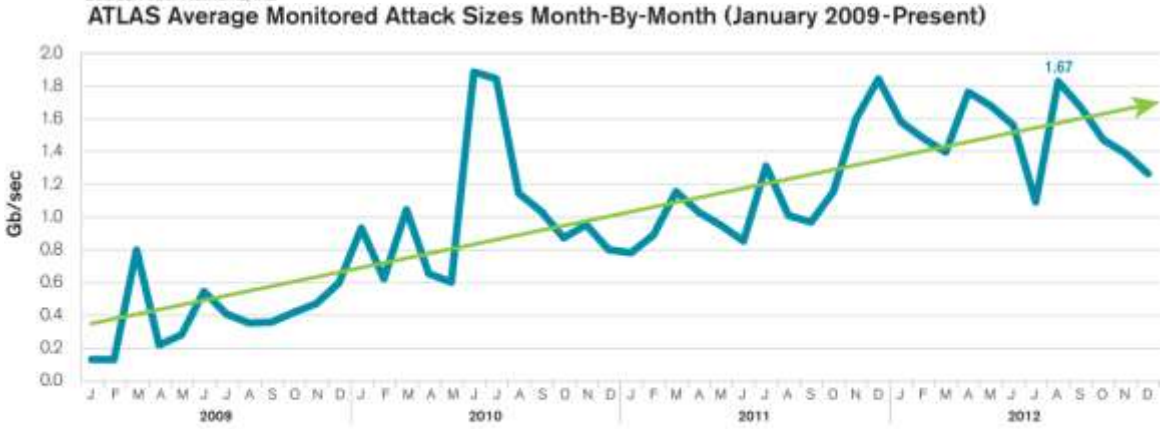


- Los “**Peaks”** de Trafico en 2012 fueron de 80 a 100Gbps.



Source: Arbor Networks, Inc.

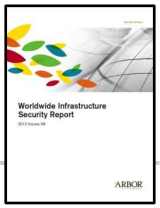
- El **Promedio** de trafico de un ataque Volumetrico esta por encima de 1Gb/sec

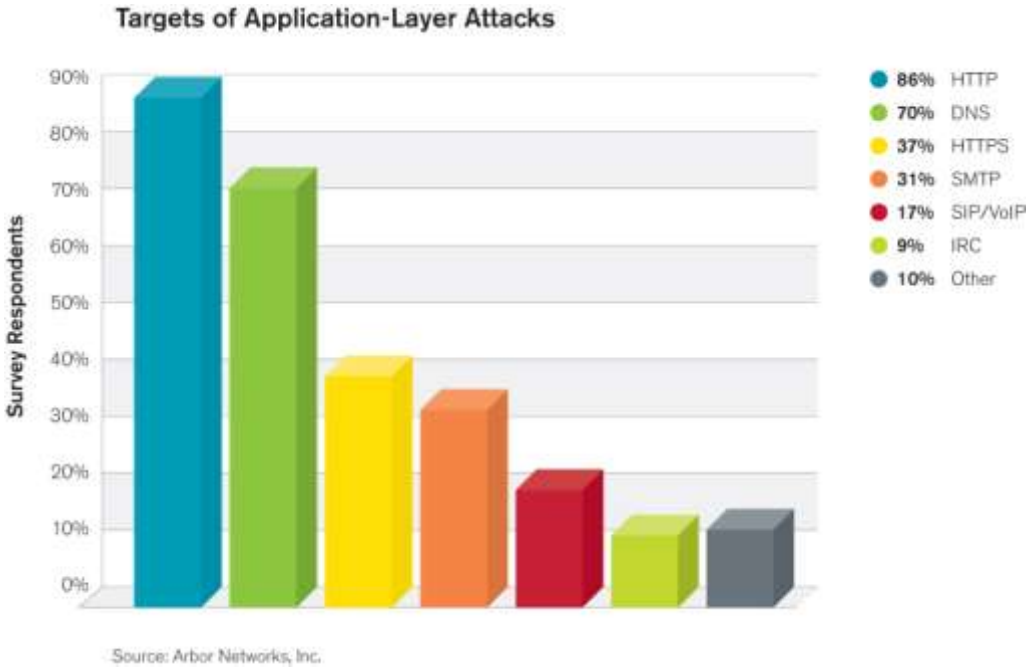


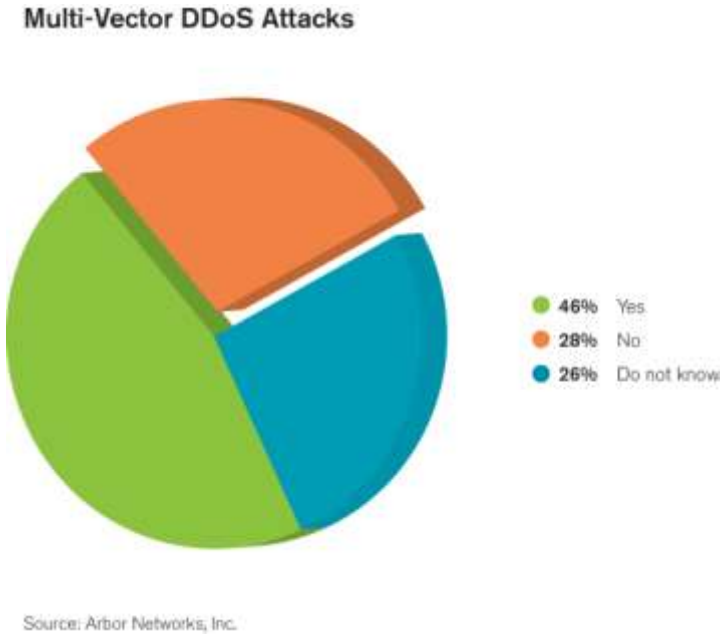
Source: Arbor Networks, Inc.

ARBOR NETWORKS

Ataques de Aplicacion y Multi-Vectoriales



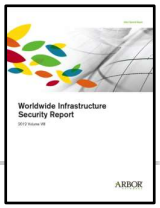


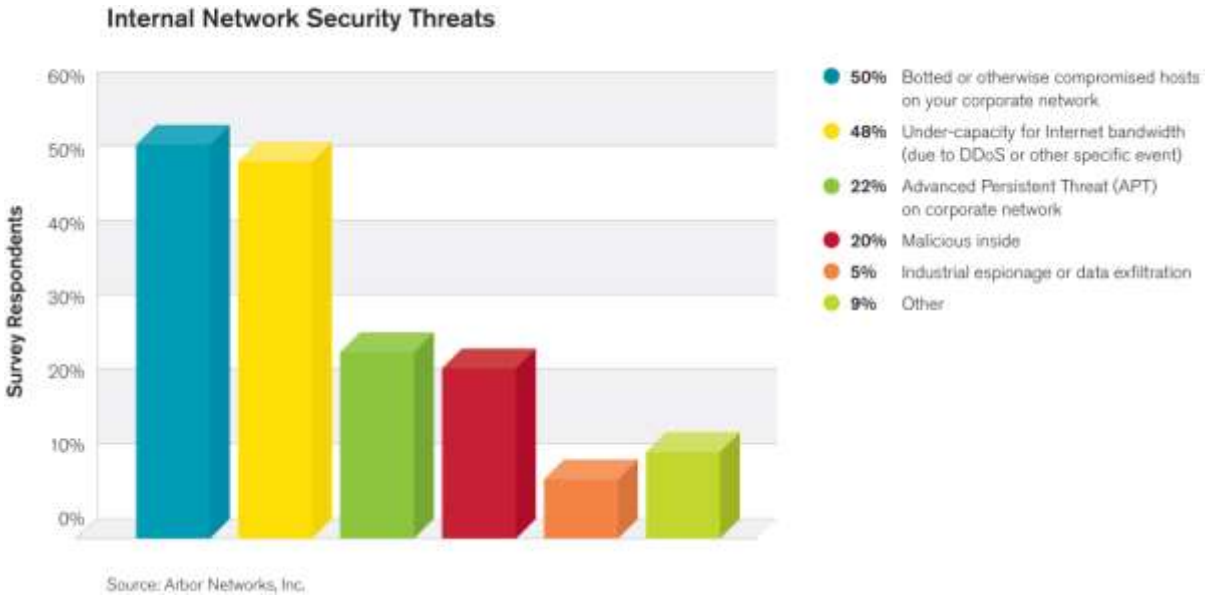


- Los servidores HTTP y de DNS son los blancos mas comunes para los ataques a nivel de aplicacion.
- Cerca del 50% de los clientes reportaron ataques multivectoriales. Un incremento del 60% respecto de 2011.
  - Los ataques Multivectoriales son complejos, pues requieren una estrategia de defensa de varias capas.

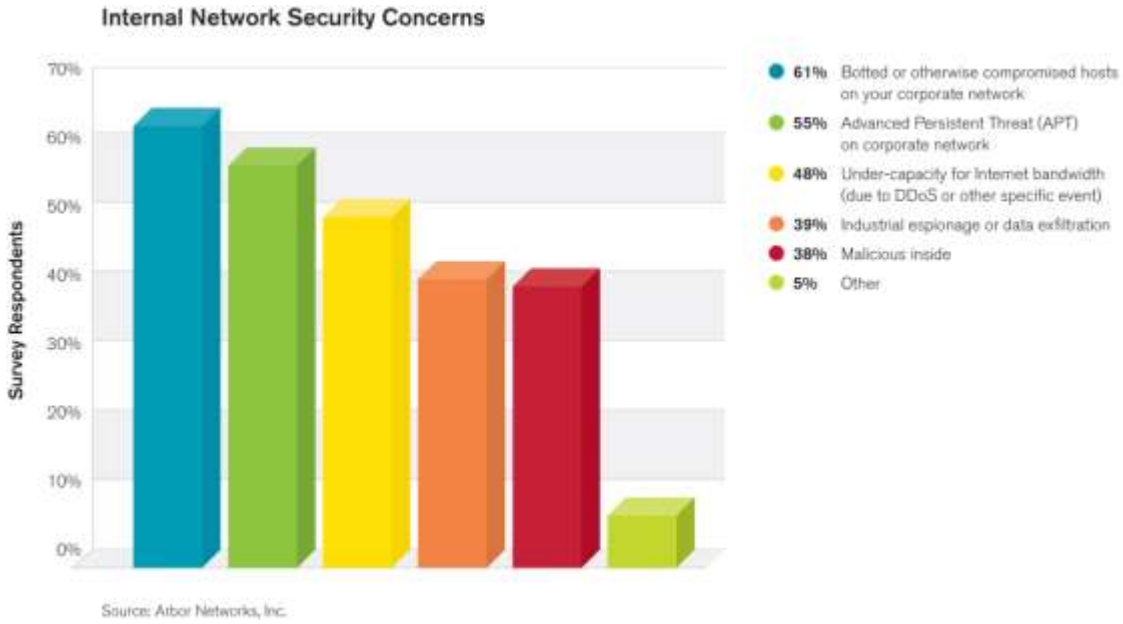
ARBOR® NETWORKS

Amenazas en las Redes Internas





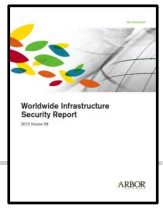
- La mitad de los clientes han experimientado la existencia de Botnets y servidores comprometidos en sus redes internas



- Aumento de la preocupacion en APT como metodo para el espionaje industrial, mas alla de haberlos experimentados.

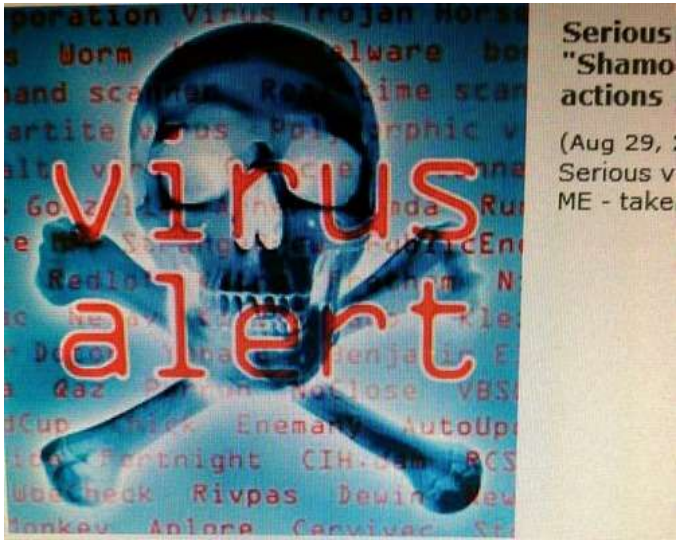
ARBOR NETWORKS

Malware en las Redes Internas



Xtreme RAT – 2012

Remote Access Trojan (RAT) que permite a usuarios remotos robar datos de las maquinas infectadas. La infeccion se realizo a traves de una campania de “spear phishing” y fue dirigida a institucion de gobierno de US and Israeli.



Shamoon – 2012

Malware ejecutable que se distribuye a traves de los recursos compartidos de la red. Corrompe archivos y mecanismos de booteo en una fecha determinada. El grupo "Cutting Sword of Justice" reclama la responsabilidad por este ataque a 30,000 estaciones de Saudi Aramco. La empresa paso 1 semana reestableciedo los servicios.

ARBOR NETWORKS

DDOS en Operacion “Ababil”

- Comprometieron servidores de PHP, WordPress, & Joomla
- Multiples vectores de ataques concurrentes
  - Ataques GET/POST a nivel de Aplicacion sobre servidores HTTP/S
  - Ataques de Aplicacion del tipo DNS Query
  - Floods de protocolos UDP, TCP SYN e ICMP

DDoS Attacks on Banks Resume

Experts Warn Botnet Getting Stronger

By Tracy Kitten | February 26, 2013 | Follow Tracy @FraudBlogger

Credit Eligible | Email | Tweet | Like | Share | Get Permission

WELLS FARGO, PNC, CapitalOne, BB&T, US bank, HSBC, SunTrust, CHASE, Bank of America, REGIONS

Izz ad-Din al-Qassam Cyber Fighters has launched a new wave of **distributed-denial-of-service** attacks against U.S. banks and credit unions, and experts say institutions can expect more incidents in the coming days.

Just after 10 a.m. ET on Feb. 25, the opening day of **RSA Conference 2013**, a handful of U.S. banking institutions were reportedly targeted as part of the latest attacks.

KrebsonSecurity

In-depth security news and investigation

19 DDoS Attack on Bank Hid $900,000 Cyberheist

A Christmas Eve cyberattack against the Web site of a regional California financial institution helped to distract bank officials from an online account takeover against one of its clients, netting thieves more than $900,000.

At approximately midday on December 24, 2012, organized cyber crooks began moving money out of corporate accounts belonging to **Ascent Builders**, a construction firm based in Sacramento, Calif. In short order, the company's financial institution – San Francisco-based **Bank of the West** – came under a large distributed denial of service (DDoS) attack, a digital assault which disables a targeted site using a flood of junk traffic from compromised PCs.

Otras caracteristicas unicas del ataque.

- Un alto valor de “paquetes por segundo” por cada fuente.
- Attaques simultaneos a diferetnes empresas del mismo mercado.
- Monitoreo en tiempo real de los resultados.
- Agilidad inusual para modificar el ataque cuando eran mitigados.

ARBOR NETWORKS

Lecciones Aprendidas

Que hace a los ataques tan efectivos?

DESAFIOS

- Los atacantes cambian de tacticas en tiempo real.
- Definen objetivos “fragiles” usando ataques de Aplicacion de L4/7
- Inline Firewall/IPS no son efectivos.
- La oferta de los ISP para brindar MSS es limitada.
- Falta de una proteccion de DDOS en varios niveles.

Que se necesita cambiar?

RECOMENDACONES

- Inversion en soluciones de defensa especifica para DDOS.
  - Falta de “practica” en DDOS.
  - Foco en Mantener la Disponibilidad
  - Estrecha Colaboracion con el Service Provier al momento de un ataque.
- DDoS debe ser parte de los Planes de Continuidad. No estan incluidadas en las Planes de Disaster Recovery.

ARBOR NETWORKS

La Solucion para este tipo de Amenazas

Basada en Visibilidad Global de la Red y en Inteligencia de Seguridad

Visibilidad de Internet & Corportiva

Conoce tu Red y tu Trafico.

Inteligencia de Seguridad

Conoce la Amenaza

Proteccion

Mitiga las Amenazas

ARBOR NETWORKS

ARBOR NETWORKS

Gracias