ARBOR NETWORKS
The Security Division of NETSCOUT

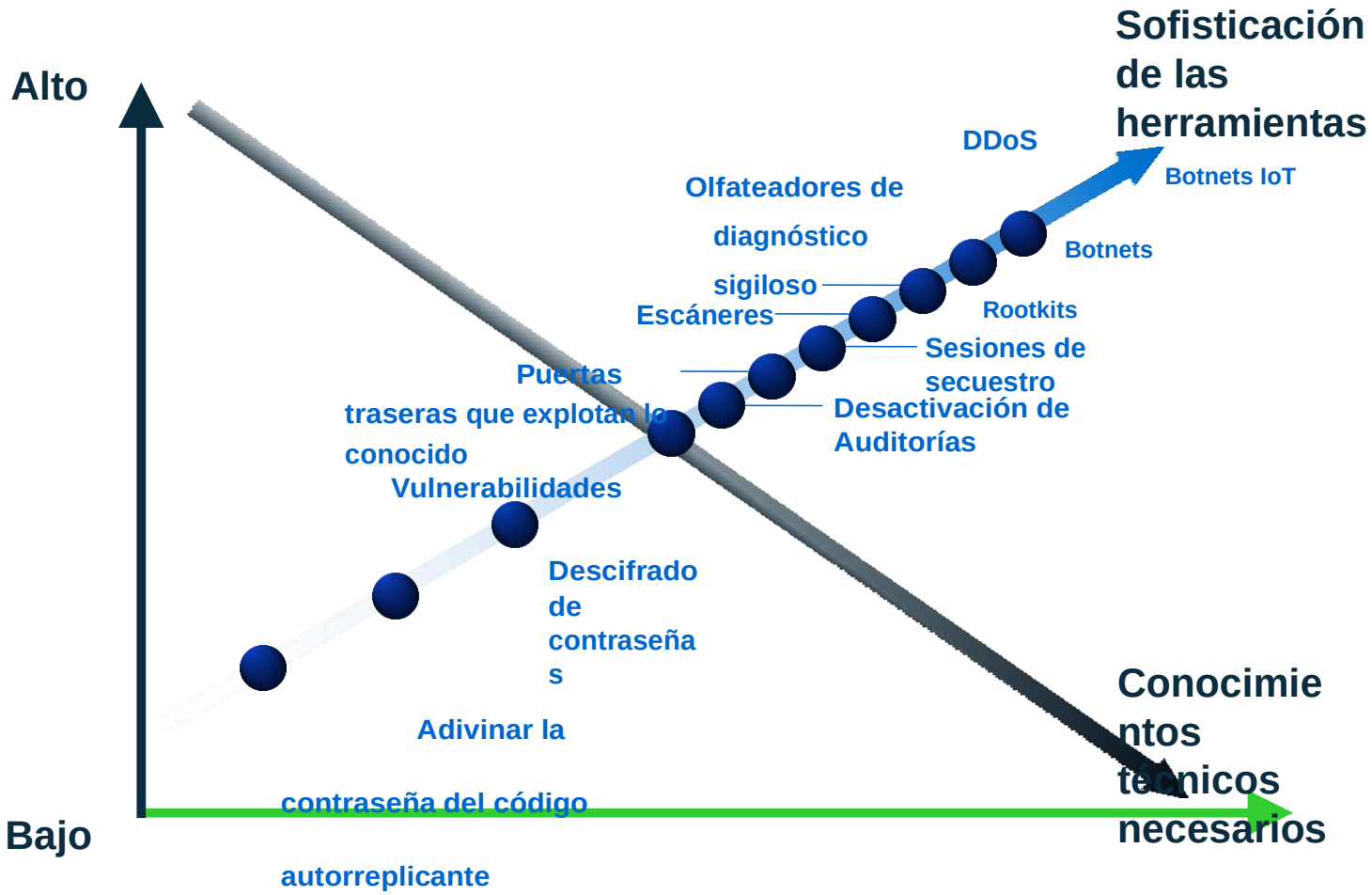
Recogiendo el torbellino

Defensa contra DDoS en la era de Mirai

Roland Dobbins, *ingeniero principal*
<rdobbins@arbor.net>

Introducción y contexto

Evolución de las amenazas y los exploits



Botnets - La amenaza número uno para la seguridad en línea

Wikipedia sobre Botnets: . . . una colección de ordenadores comprometidos (llamados ordenadores zombis) [o bots] que ejecutan programas, normalmente denominados gusanos, troyanos o puertas traseras, bajo una infraestructura común de mando y control.

Las redes de bots son los principales facilitadores de todas estas actividades:

- DDoS
- Extorsión
- Fraude en los clics publicitarios
- Ventas fraudulentas
- Robo de identidad y fraude financiero (suplantación de identidad, robo de información de los ordenadores, etc.)
- Robo de bienes/servicios
- Espionaje/robo de información
- Manipulación bursátil basada en el spam

ARBOR® NETWORKS

Ataques DDoS: una realidad en Internet

- Los ataques DDoS se producen las 24 horas del día y los 365 días del año: son simplemente un hecho de la vida en Internet.
- Cualquier organización, cualquier sitio, cualquier individuo puede verse afectado por un DDoS, ya sea como objetivo directo o a través de daños colaterales.
- Los DDoS salientes pueden ser tan devastadores para los clientes finales y los SP como los DDoS entrantes: los bots en las redes de acceso de banda ancha, en las redes empresariales y en los IDC afectan tanto a las redes de origen como a los objetivos.
- El conocimiento de la situación es clave: ¿qué está ocurriendo en las noticias? ¿Qué aniversarios se celebran este año/mes/semana/hoy?
- Los malhechores se atacan unos a otros con regularidad: ¡daños colaterales!

ARBOR® NETWORKS

La nueva nube del emperador

- Nos basamos en protocolos de hace 34 años diseñados para su uso en un entorno de laboratorio y con poca o ninguna atención a la seguridad como base de nuestra infraestructura global de Internet.
- Aunque existe un gran volumen de trabajo sobre seguridad operativa (opsec) y arquitecturas escalables de Internet, se ha hecho más hincapié en la brecha que en las implantaciones reales.
- Desconexión continua y generalizada entre los arquitectos de redes, los arquitectos de aplicaciones, los grupos operativos, los equipos de seguridad y la dirección.
- Actitud optimista respecto a la seguridad: "¿Por qué iba a *atacarnos* alguien?
- Falta de responsabilidad: ¿se ha despedido a alguien como consecuencia de incidentes de seguridad evitables?
- La omnipresencia del teatro de la seguridad/la serpiente de la seguridad.
- Incapacidad o falta de voluntad para evaluar adecuadamente los modelos abstractos de amenaza: ¿un mecanismo de defensa psicológico necesario?

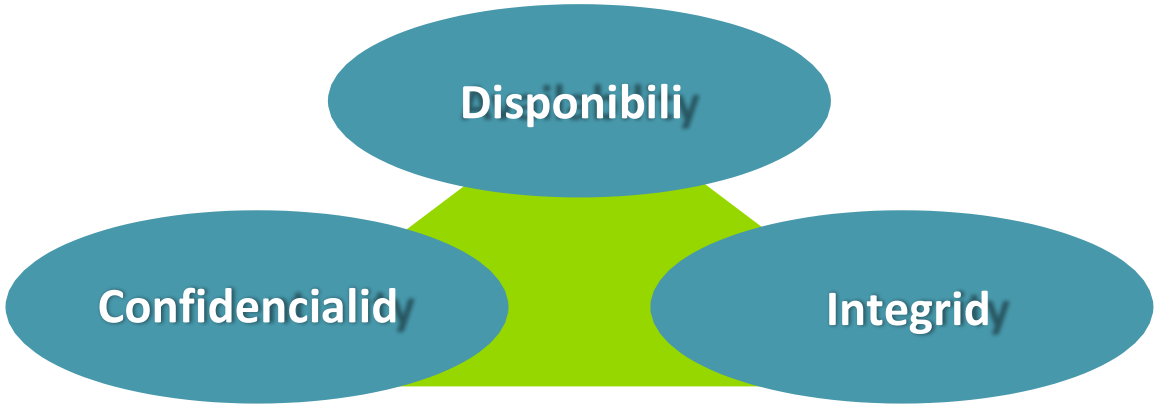
Antecedentes del DDoS

¿Qué es un ataque de denegación de servicio distribuido (DDoS)?

- Un intento de **consumir recursos** finitos, **explotar las debilidades** del diseño o la implementación del software, o **aprovechar la falta de capacidad de** la infraestructura
- Se centra en la **disponibilidad** y **utilidad** de los recursos informáticos y de red
- Los ataques casi siempre se **distribuyen** para lograr un efecto aún más significativo (es decir, DDoS)
- Los **daños colaterales** causados por un ataque pueden ser tan graves, o incluso peores, que el propio ataque
- **Los ataques DDoS afectan a la disponibilidad**. Si no hay disponibilidad, no hay aplicaciones/servicios/datos/Internet. No hay ingresos!
- **Los** ataques DDoS son ataques **contra la capacidad y/o el estado**.

ARBOR NETWORKS

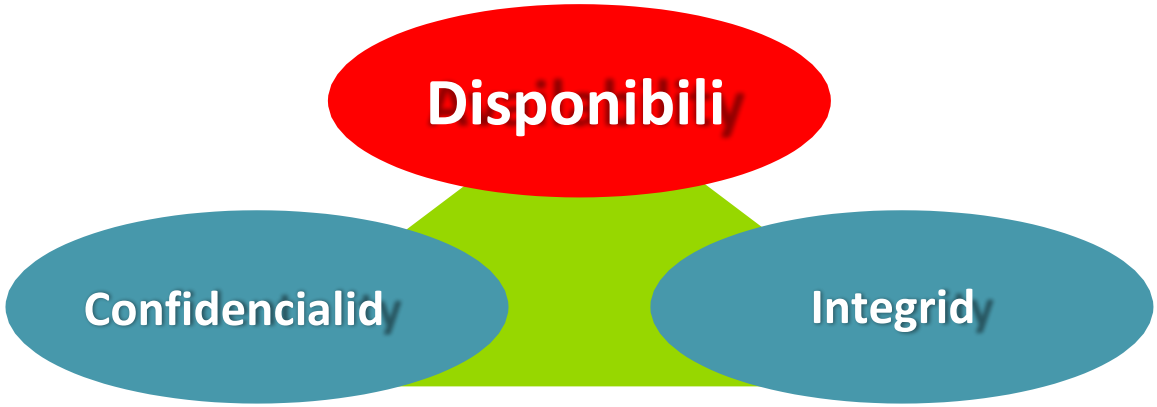
Tres atributos de seguridad



- El objetivo de la seguridad es mantener estos tres atributos.

ARBOR NETWORKS

Tres atributos de seguridad



- El objetivo principal de la defensa DDoS es mantener la disponibilidad frente a los ataques

ARBOR NETWORKS

Casi todo el gasto/esfuerzo en seguridad se centra en la confidencialidad y la integridad

- La confidencialidad y la integridad son conceptos relativamente sencillos, fáciles de entender para los no especialistas
- En la práctica, la confidencialidad y la integridad equivalen prácticamente a la encriptación.
- La realidad es que hay algo más que la encriptación, pero es fácil proclamar la victoria: "Tenemos antivirus, tenemos encriptación de disco, cumplimos con la PCI, ¡woo- hoo! "
- Y sin embargo, cientos de millones de hosts bots; redes empresariales de todos los tamaños en todos los verticales completamente penetradas, propiedad intelectual robada, secretos de defensa filtrados, etc.
- La disponibilidad no puede ser refinada - el servidor Web/Servidor DNS/PBX VoIP o está en funcionamiento o no lo está. No hay manera de ofuscar/exagerar/prevaricar con respecto a la postura de seguridad real del mundo.
- La disponibilidad requiere profesionales de la seguridad operativa (opsec) que comprendan TCP/IP y el enrutamiento/conmutación; que comprendan los servidores web; que comprendan los servidores DNS; que comprendan la seguridad; que comprendan la capa 7.
- Estas personas son raras y no son baratas. La mayoría de las organizaciones ni siquiera entienden las habilidades requeridas y el alcance de la experiencia que deben buscar para identificar y contratar a las personas adecuadas.

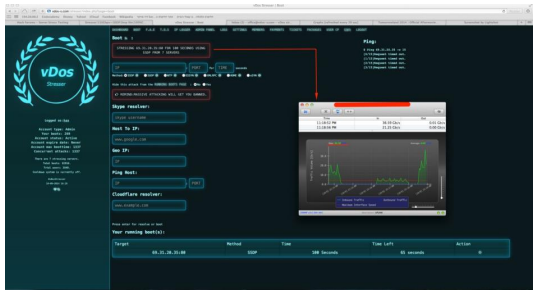
La disponibilidad es difícil.

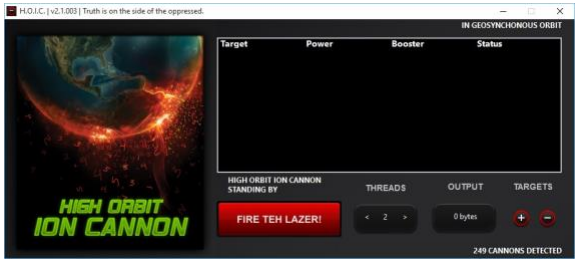
- Mantener la disponibilidad frente a los ataques requiere una combinación de habilidades, arquitectura, agilidad operativa, capacidades analíticas y capacidades de mitigación que la mayoría de las organizaciones simplemente no poseen
- En la práctica, la mayoría de las organizaciones nunca tienen en cuenta la disponibilidad a la hora de diseñar/especificar/construir/desplegar/probar aplicaciones/servicios/propiedades en línea
- En la práctica, la mayoría de las organizaciones nunca establecen la conexión lógica entre el mantenimiento de la disponibilidad y la continuidad del negocio
- En la práctica, la mayoría de las organizaciones nunca hacen pruebas de estrés de sus pilas de aplicaciones/servicios para determinar las deficiencias de escalabilidad/resiliencia y proceder a solucionarlas
- En la práctica, la mayoría de las organizaciones no tienen planes de mitigación de DDoS - o si tienen un plan, ¡nunca lo ensayan!

ARBOR NETWORKS

El armamento de los DDoS

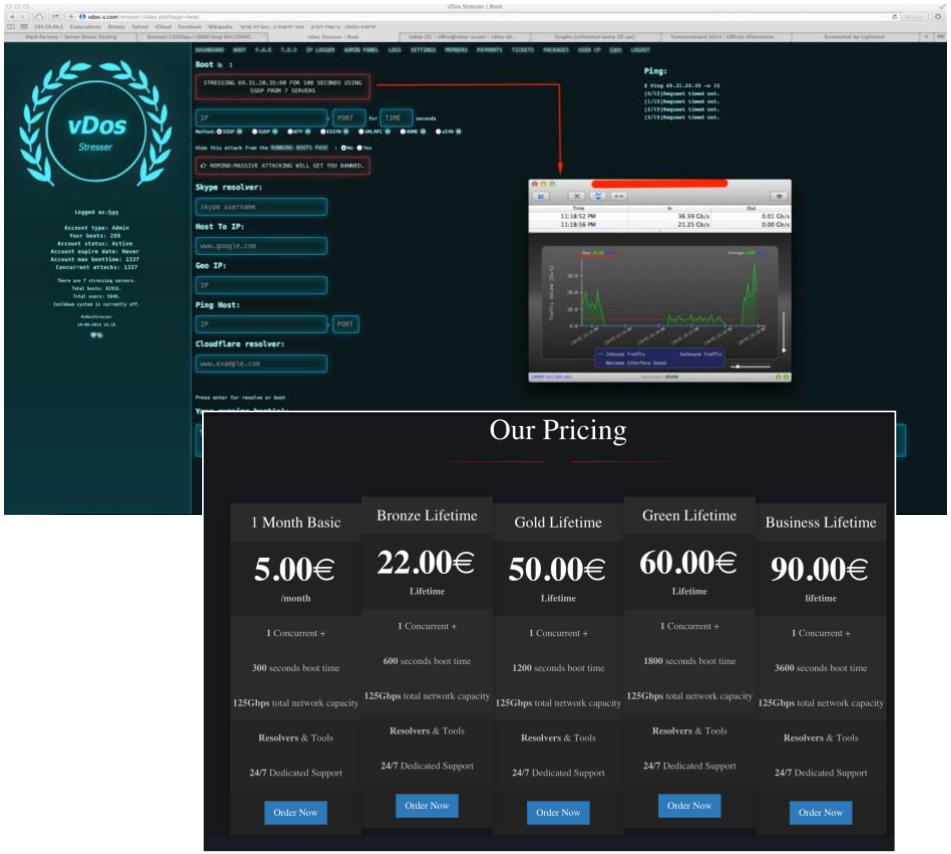
"Weaponize" : *Convertir para usar como arma / simplificar el uso como arma*





- Aumento de la disponibilidad de "Stresser Tools"/"Booters" que realizan ataques altamente distribuidos utilizando una combinación de ataques de amplificación no suplantados y suplantados. A menudo están vinculados a las granjas de bots.
- Desarrollo de herramientas para su uso por parte de los atacantes voluntarios:
  - Cañón de iones de órbita baja utilizado para realizar ataques UDP/ICMP no suplantados
  - El cañón de iones de alta órbita envía peticiones HTTP no suplantadas contra varios sitios

Herramientas DDoS para las masas

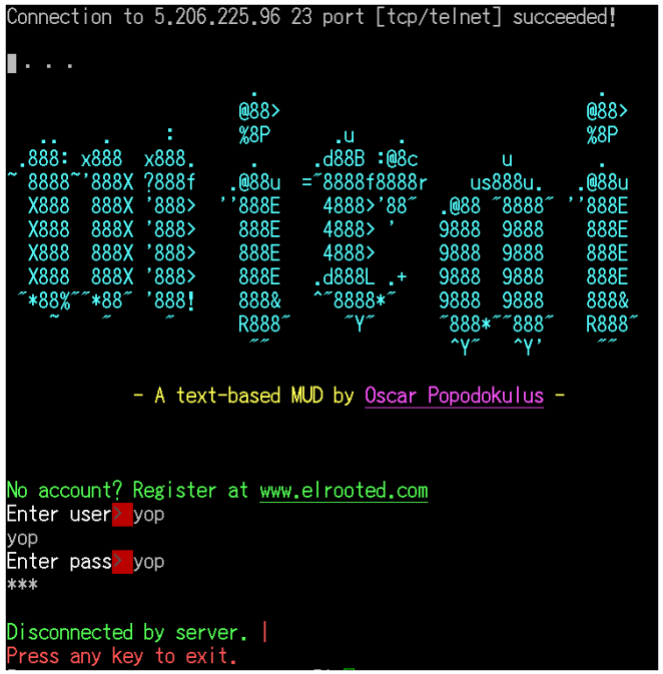


- Cualquiera que tenga la capacidad de pulsar un botón puede ahora lanzar un ataque DDoS.
- Barato y sencillo de usar:
  - Cuentas VIP!
  - Suscripción de por vida!
  - Atención al cliente 24 horas al día, 7 días a la semana.
- Principalmente son utilizados por los jugadores que se atacan entre sí, pero recientemente hemos visto que se utilizan para atacar objetivos muy visibles.

ARBOR NETWORKS

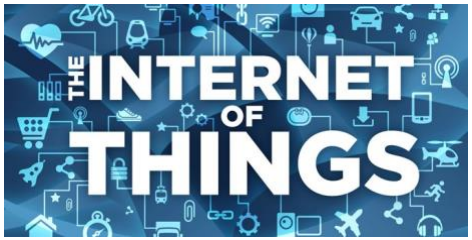
La situación del IoT

INTERNET DE LAS COSAS



ARBOR NETWORKS

Internet de los objetos (IoT)



Wikipedia: *El internet de las cosas (IoT) es la red de dispositivos físicos, vehículos, edificios y otros elementos -integrados con electrónica, software, sensores y conectividad de red- que permite a estos objetos recoger e intercambiar datos*

Pero, ¿se trata de algo nuevo o sólo de marketing?

- Por ejemplo, la "cafetera de la sala de Troya" se conectó a Internet en 1993.

Una definición más exacta: *Un dispositivo IoT (dispositivo integrado) es esencialmente un ordenador con una CPU, memoria, software y un conjunto de interfaces que se dedican a funciones o tareas específicas.*

NOMBRES DE USUARIO Y CONTRASEÑAS POR DEFECTO!!!

https://krebsonsecurity.com/wp-content/uploads/2016/10/IoTbadpass-Sheet1.csv

```
Username/Password,Manufacturer,Link to supporting evidence
,,
admin/123456,ACTi IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko,ANKO Products DVR,http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass,"Axis IP Camera, et. al",http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv,Dahua Camera,http://www.cam-it.org/index.php?topic=5192.0
root/888888,Dahua DVR,http://www.cam-it.org/index.php?topic=5035.0
root/666666,Dahua DVR,http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv,Dahua IP Camera,http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin,Dahua IP Camera,http://www.cam-it.org/index.php?topic=9396.0
666666/666666,Dahua IP Camera,http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox,Dreambox TV receiver,https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx,EV ZLX Two-way Speaker?,?
root/juantech,Guangzhou Juan Optical,https://news.ycombinator.com/item?id=11114012
root/xc3511,H.264 - Chinese DVR,http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518,HiSilicon IP Camera,https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd,HiSilicon IP Camera,https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin,IPX-DDK Network Camera,http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system,"IQinVision Cameras, et. al",https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm,Mobotix Network Camera,http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321,"Packet8 VOIP Phone, et. al",http://webcache.googleusercontent.com/search?q=cache:WlphozQZURUJ:community.freepbx.org/t/packet8-atas-
phones/4119+&cd=21&hl=en&ct=clnk&gl=us
root/00000000,Panasonic Printer,https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek,RealTek Routers,
admin/1111111,Samsung IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc,Shenzhen Anran Security Camera,https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin,SMC Routers,http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb,Toshiba Network Camera,http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt,Ubiquiti AirOS Router,http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor,VideoIQ,https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>,Vivotek IP Camera,https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111,"Xerox printers, et. al",https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521,ZTE Router,http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html
```

Seguridad del IoT (o falta de ella)

Problemas de seguridad del IoT:

- Los dispositivos IoT suelen tener capacidades limitadas a bordo y a menudo necesitan una configuración y un control externos.
- Muchas de estas pilas de dispositivos no están bien aseguradas:
  - Nombres de usuario/contraseñas codificadas
  - Servicios innecesarios activados por defecto (Chargen, SSDP, DNS forwarder)
  - Interfaces de gestión no seguras (Web, SNMP, TR-069, etc.)
  - Capacidades de actualización de software limitadas o inexistentes
  - Rara vez se parchea o se actualiza después de la implantación
- Se calcula que el número de dispositivos IoT en 2020 será de unos 20-30Billion. Sin embargo, ya tenemos más de 6.000 millones de dispositivos en línea, a los que se suman 5,5 millones cada día1.

ARBOR NETWORKS

1) Investigación de Gartner: http://www.gartner.com/newsroom/id/3165317

Millones de dispositivos IoT vulnerables

+ Arma de fuego = ?

Botnets IoT!

La historia de los botnets del IoT

Las redes de bots de IoT no son nada nuevo:

- La primera red de bots se creó en 1993, cuando Robey Pointer creó un bot de Internet Relay Chat (IRC) llamado "eggbot", que se utilizaba para defender canales de IRC lanzando ataques de inundación contra usuarios no deseados. El bot también se utilizaba para atacar otros canales utilizando los protocolos CTCP y DCC. Varias instancias del bot podían unir esfuerzos y trabajar juntas en "botnets".
- En 2003, el primer ataque DDoS (no intencionado) contra la Universidad de Wisconsin utilizando dispositivos IoT se produjo debido a una dirección NTP codificada en 700.000 módems DSL/cable de Netgear. Incluso después de que se lanzara un nuevo software, el ataque continuó durante años hasta que el último dispositivo fue tirado a la basura.
- En 2008, el primer ataque de botnet DDoS IoT del que se tiene constancia se realizó mediante una botnet de routers de banda ancha CPE basados en Linux.
- In 2012, an unknown researcher published a report called the “Internet census of 2012”. Los datos utilizados en el informe se obtuvieron pirateando unos 420.000 dispositivos CPE de todo el mundo con credenciales predeterminadas1

1) https://en.wikipedia.org/wiki/Carna_botnet

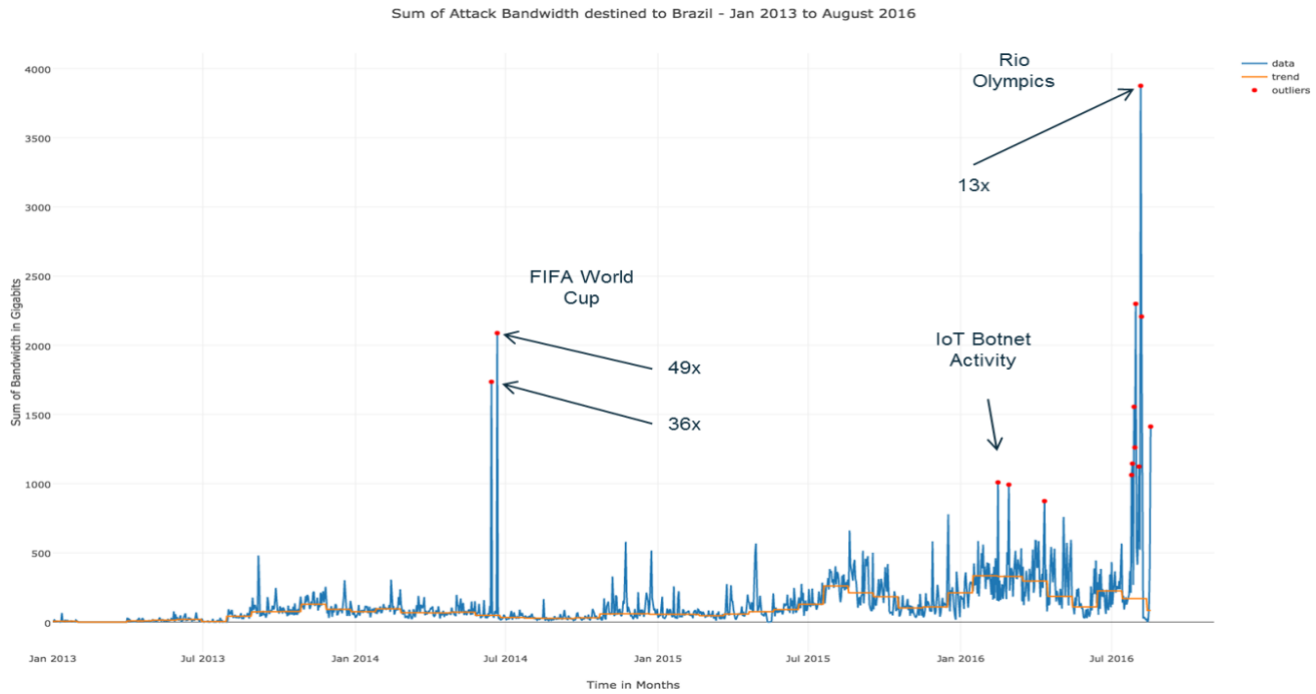
Situación actual de las redes de bots de Internet de las Cosas

Las redes de bots IoT se han convertido en un arma y están disponibles a través de los servicios de booter/stresser:

- Una red de bots IoT que utiliza el código de Lizardstresser se utilizó para atacar sitios en Brasil en 2016 con volúmenes de ataque que alcanzaron los 400gb/seg.
- La misma red de bots, compuesta por unas 10.000 cámaras web, se utilizó para lanzar ataques sostenidos de 540gb/seg contra organizaciones afiliadas a los Juegos Olímpicos en el verano de 2016.
- En los ataques DDoS realizados en noviembre de 2016 contra el periodista de seguridad Brian Krebs, que alcanzaron un máximo de 620gb/seg, se utilizó una red de bots IoT basada en la base de código Mirai.
- Las redes de bots IoT que utilizan el código Mirai se utilizaron en los ataques contra el proveedor de DNS autorizado Dyn en noviembre de 2016.

  El código fuente de los bots LizardStresser y Mirai se ha liberado en la naturaleza y ha generado múltiples variantes nuevas.

El bot LizzardStresser ataca Brasil



- Ataques lanzados no sólo contra la infraestructura de los eventos deportivos, sino también contra los patrocinadores asociados y las instituciones financieras y gubernamentales.

Cómo hacer frente a las redes de bots del IoT

Vectores de infección de la red de bots IoT - Ejemplo de Mirai

1. Un dispositivo comprometido creará un hilo de escaneo separado para buscar otros dispositivos en los puertos TCP 23,2323,23231,37777 y 7547 (+5555) (interfaz TR- 069/TR-064 SOAP) utilizando IP's aleatorias.
2. Si un dispositivo responde, se intentará iniciar la sesión utilizando un conjunto de combinaciones comunes de nombre de usuario y contraseña
3. Si tiene éxito, la dirección IP del dispositivo vulnerable se envía al servidor C&C
4. El servidor de C&C se registrará en el dispositivo, descargará el malware apropiado y comprometerá el dispositivo. El dispositivo empezará a escanear, pasa al nº 1

- Tal y como está la situación ahora, un dispositivo vulnerable se infectará a los **pocos minutos** de estar conectado a Internet.
- Los dispositivos vulnerables provienen principalmente de 3 fabricantes de China, uno de ellos lanzó un parche en 2014 pero solo para la versión inglesa de su SW.

LA RED DE BOTS MIRAI

Aproximadamente 500.000 dispositivos en todo el mundo

- Altas concentraciones en China, Hong Kong, Macao, Vietnam, Taiwán, Corea del Sur, Tailandia, Indonesia, Brasil y España

El mismo malware botnet utilizado en los ataques de Krebs, OVH Dyn y Liberia

- No implica que fueran los mismos adversarios

Múltiples vectores de ataque DDoS posibles

Al menos una variante ha sido desparasitada.

Capacidades de ataque DDoS de IoT Botnet - Mirai

Actualización del flash el 15 de diciembre de 2016

Una nueva variante de Mirai ha sido vista en la naturaleza emitiendo tráfico falsificado. Los ataques incluyen inundaciones SYN, ataques de

Tipos de ataque:

- Inundación UDP
- Inundación del motor de origen de las
- Inundación TCP ACK
- Ataque TCP "Stomp" (inundación ACK en una conexión TCP establecida, diseñada para eludir los dispositivos de mitigación DDoS)
- Inundación TCP SYN
- Inundación de paquetes GRE
- Inundación de solicitudes HTTP (GET, POST, HEAD)
- Preparación de etiquetas pseudoaleatorias DNS ("Tortura de agua DNS")

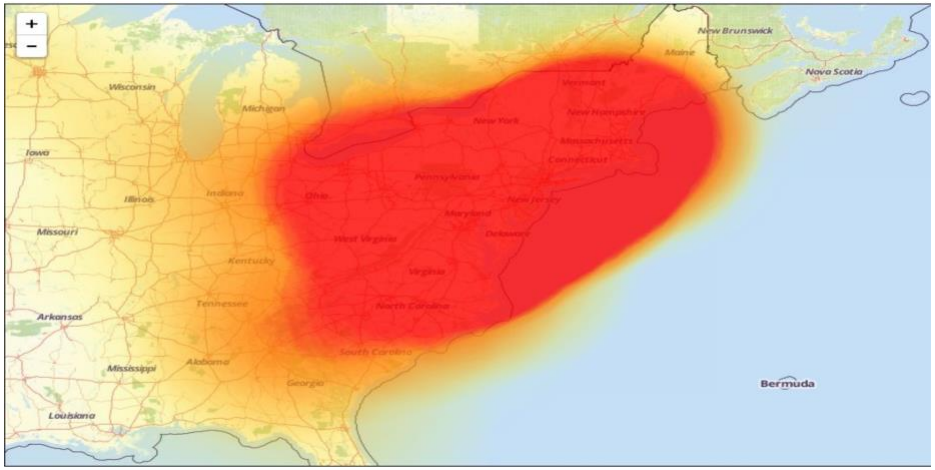
El malware Mirai se ejecuta en el espacio de usuario y, hasta ahora, no ha utilizado direcciones IP falsas, lo que le impide realizar ataques de suplantación y reflexión.

DYN ATACA EL 21 DE OCTUBRE

Tres ataques dirigidos a la infraestructura de DNS gestionada por Dyn
Los clientes de Dyn incluyen

- Netflix Twitter, Reddit, Github, Spotify, PayPal, Airbnb, NYT, etc.

Estos ataques provocaron cortes a gran escala para los clientes de Dyn, aunque los clientes no fueron atacados directamente



ARBOR NETWORKS

CRONOLOGÍA DE LOS ATAQUES DE DYN

Ataque 1
Comienza: 11:10 UTC

Duración: 2 horas y 20 minutos

Ataque 2
Comienza: 15:50 UTC

Duración: 1 hora y 10 minutos

Ataque 3
Mitigado desde el principio

Destinos: APAC, Sudamérica, Europa del Este, Estados Unidos-Oeste, Estados Unidos-Este
Los cortes fueron regionales

ARBOR NETWORKS

Entender y mitigar los ataques

Múltiples vectores de ataque altamente distribuidos
Dyn informó originalmente de "10s de millones de direcciones IP"

Posteriormente se corrigió a una estimación de 100.000

Efecto cascada
La interrupción del servicio DNS por el ataque original genera una actividad legítima de reintentos

Esto es lo que causó que Dyn sobreinformara inicialmente el número de IP's atacantes

Mitigación:

ACLs, S/RTBH, flowspec, IDMS

ARBOR NETWORKS

ATAQUES EN LIBERIA - A PARTIR DEL 31 DE OCTUBRE

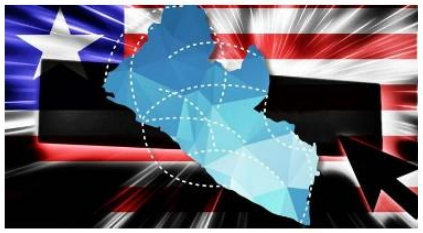
SC Magazine US > News > Analysts mixed on reason for Liberia Mirai attack

by Bradley Barth, Senior Reporter

November 04, 2016

Analysts mixed on reason for Liberia Mirai attack

A barrage of Mirai botnet-fueled distributed denial of service (DDoS) attacks reportedly incapacitated Internet operations across the West African coastal nation of Liberia earlier this week, bu industry researchers had mixed views on the rationale behind the attack and damage inflicted.



A large botnet operation dubbed Shadows Kill targeted Liberian IP addresses with a DDoS attack over several days this past week, prompting speculation as to the perpetrators' true motive.

In a Thursday post on the publishing site *Medium*, independent researcher Kevin Beaumont reported a series of "continued short duration attacks" – perpetrated by a Mirai botnet composed of Internet of Things devices such as CCTV cameras – that may have crippled Liberia's Internet infrastructure. Beaumont linked the attacks to the same actor that launched a massive attack against the DNS service Dyn on Oct. 21, knocking out such websites as Amazon, Reddit and Twitter.

Mitigación de DDoS de IoT Botnet

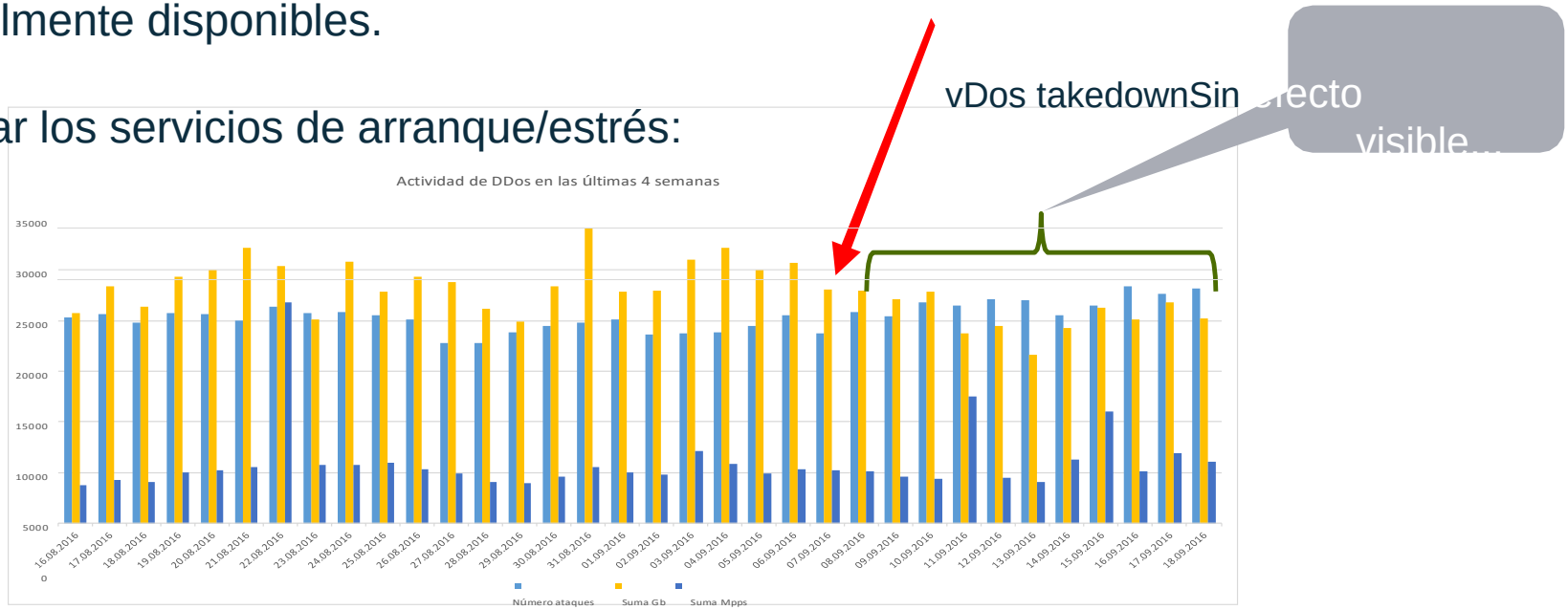
Las redes de bots IoT no son nada nuevo y los ataques utilizados tampoco lo son. Se siguen aplicando los mismos enfoques de mitigación de DDoS.

- Aplicar las mejores prácticas actuales (BCP) para la infraestructura, los servidores de host/aplicación/servicios y DNS. Esto incluye la especificación de las políticas de acceso a la red para los tipos de servidores comunes.
- Utilice la telemetría de flujo para detectar, clasificar y rastrear el tráfico DDoS.
- Utilice S/RTBH, flowspec, soluciones inteligentes de mitigación de DDoS (IDMS) para mitigar los ataques.
- Planifique y practique cómo hacer frente a los ataques DDoS.

Cómo reducir la amenaza de los botnets del IoT

Las redes de bots IoT son populares hoy en día porque los dispositivos IoT son vulnerables y las herramientas para infectarlos y subvertirlos con fines de ataque están fácilmente disponibles.

1. Apagar los servicios de arranque/estrés:



Cómo reducir la amenaza de los botnets del IoT (cont.)

2. Dejar de vender e instalar dispositivos IoT vulnerables:
   - ¿Quién va a hacer que esto se cumpla?
   - ¿Quién va a pagar esto?
   - ¿Le importa a la gente que su cámara web esté atacando a otra persona?

3. Parchee los dispositivos IoT vulnerables:
   - ¿Cuándo fue la última vez que actualizó su dispositivo CPE? ¿Televisión inteligente? ¿La cafetera? ¿Sus bombillas inteligentes?
   - Los routers Netgear que atacaron la Universidad de Wisconsin NUNCA fueron parcheados y el ataque murió sólo cuando el último dispositivo fue arrojado a la basura.

4. Si los dispositivos IoT no pueden ser reparados (o no son de confianza), ¡aíslelos de Internet y cree barreras!

Ejemplo de cómo aislar dispositivos IoT: ¡la red doméstica de Steinthor!

En 2011, Steinthor connected 3 IP Web Cams to his home network. estos dispositivos se comunican con un NAS de Synology que proporciona un portal de vídeo y almacena todas las grabaciones de Steinthor connected 3 IP Web Cams to his home network. vídeo.

La red está segmentada en 2 áreas:

- VLAN de usuario

VideoCameras (5 incoming rules)

1	☑	any	SynologyNAS	ip	Permit	TOP 10	3975813		
2	☑	any	any	echo-reply	Permit		0		
3	☑	any	any	domain	Permit		0		
4	☑	any	any	ntp	Permit		160		
5		any	any	ip	Deny				Implicit rule

- Subred de vídeo donde un (viejo) Cisco ASA 5505 controla toda la comunicación entre las cámaras web y el NAS.

L3 VPN se utiliza para permitir el acceso remoto al portal de la cámara web que se ejecuta en el Synology.

¿Qué es lo siguiente?

¿Qué es lo siguiente?

ZYSECURITY
CCTV products OEM, your own factory

ZYSECURITY CO.,LIMITED | www.zysecurity.com
Add: 5F,3th Building,HuBeiBaoFeng industrial area,LongGang district,Shenzhen,China
TEL:(86) 755-33561429 | Mob:+86 18320850260 | E-mail:Daisy@zysecurity.com | Contact:Daisy

XMEYE SYSTEM - SUPER PASSWORD - FOR DVR NVR IPC

	2017 January	2017 February	2017 March	2017 April	2017 May	2017 June
1	y6rEnN9136	hGz3p9773	lVKN5o4792	Q5yeRg1199	sEYrYO0	s6udvo1201
2	NEWdMf773	fDyRFB4792	0C0Z9L1199	zq9Tyo0	Cn4R3Y1201	L7MbXd4808
3	nAwk4f4792	2DxRlK1199	AuKUG00	9Quiam1201	VCAg4G4808	3bvZ2e827
4	HcB4Qs1199	LyJ59Q0	g28cfK1201	SgtyKo4808	ogVNVQ827	7Lhs4l9264
5	hdiQl80	bDNPUL1201	zbKby54808	BBrc1u827	fXClL49264	k6MTRC125
6	Irl0bG1201	GR6Y0e4808	OjkvHG827	zla2ot9264	HxxjEv125	8aWgfy3416
7	FKLw0j4808	7lj6yy827	zgmlOO9264	hgJ9hA125	z3W1cr3416	G88v639143
8	nGtzC8827	xn2uyV9264	f7m2mH125	5u291A3416	SQdqja9143	gC1L7c7312
9	eEo3T59264	u7uUQh125	yUSxLs3416	jTDUSC9143	461WuM7312	W4DDYM7929
10	Q0WbaW9136	UA10mR773	lAHSge4792	xbvwZo1199	YjTJ6N0	t5hkC31201
11	XgQ6xI773	Snqh6u4792	Lr1zBn1199	R7SzfG0	StkbAJ1201	tMwcc54808
12	4gv8me4792	KJ2ZQJ1199	yGBiVQ0	7oQTzk1201	pmieOL4808	XiFigk827
13	lluKNB1199	aF0lvv0	hUNJPK1201	MUuie34808	sloanv827	FyPZsK9264
14	xePfVg0	0Wenhi1201	K6VMzn4808	00JZUo827	40Qbtk9264	U0Tu8U125
15	9EhuEg1201	ao1SyT4808	pfDRXS827	WTnOlp9264	1UDPr5125	HV38sg3416
16	8UTjLW4808	JlOdAl827	2hyMU39264	ShaEtt125	6ot6RO3416	G9vOqh9143
17	Q1rm8O827	ijyw6A9264	jNBLAL125	V5O52Y3416	LmKVnJ9143	pleWQA7312
18	tuJjLc9264	KFQ9jX125	u87vdt3416	ZhnWO29143	VjH2sG7312	j2xFTC7929
19	KCHQN6125	L9ZAuy3416	0UPVab9143	gWQZRu7312	B5u2JZ7929	Guo3ui1000
20	l4iuaN773	Yz8KUc4792	Dq62je1199	Kw47Bv0	Fu55LG1201	jluOx54808
21	A32uFI4792	cTRiX81199	bO5KeD0	CISW201201	vUrT844808	xfLkDe827
22	QGT2Va1199	4CJmnz0	oWBhP11201	jsafKF4808	FWQ9Kg827	c8dmJm9264
23	zaRezi0	VqlQwB1201	29ksvt4808	pw5Z6R827	T6TwM49264	wwWlrr125

¿Qué es lo siguiente?

Hay muchas más categorías de dispositivos de consumo de la "IO": bombillas, termostatos, "contadores inteligentes", etc.

Los grandes routers de clase portadora y de empresa han sido comprometidos antes, utilizados para ataques DDoS de inundación ICMP, secuestro de rutas para DDoS y para spam (credenciales de cisco/cisco, incluso para routers Juniper)

Escaneo/compromiso en varias etapas de dispositivos IoT *detrás de* NATs/firewalls.

Ahora tenemos NETCONF, y varias API de SDN...

. . y la capacidad de ejecutar código arbitrario en los propios routers.

Los planes de continuidad de la infraestructura de red son más importantes que nunca.

Todos los routers son dispositivos integrados en el IoT, incluso los grandes.También lo son los smartphones.

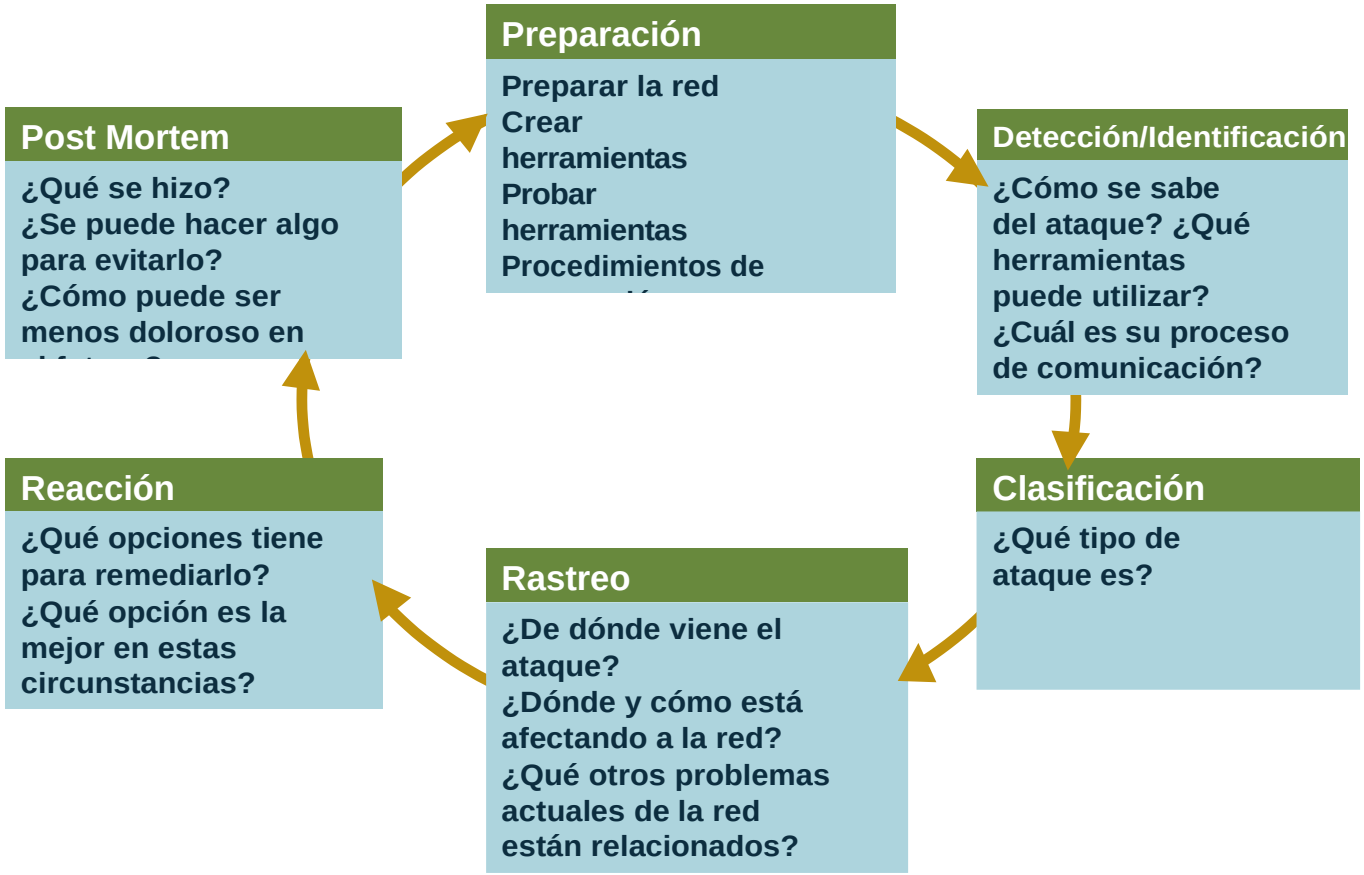
¿Qué podemos hacer?

Disponibilidad de la Red/Aplicación: Proteger la infraestructura

- La seguridad es el corazón del futuro del trabajo en red; hemos pasado de una Internet de confianza implícita a una Internet de desconfianza generalizada
- No se puede confiar en ningún paquete; todos los paquetes deben ganarse esa confianza mediante la capacidad de un dispositivo de red para inspeccionar y aplicar la política
- Proteger la infraestructura es el requisito de seguridad más fundamental
- La protección de la infraestructura debe incluirse en todos los diseños de alta disponibilidad
- Una infraestructura segura es la base de la prestación continua de servicios

ARBOR NETWORKS

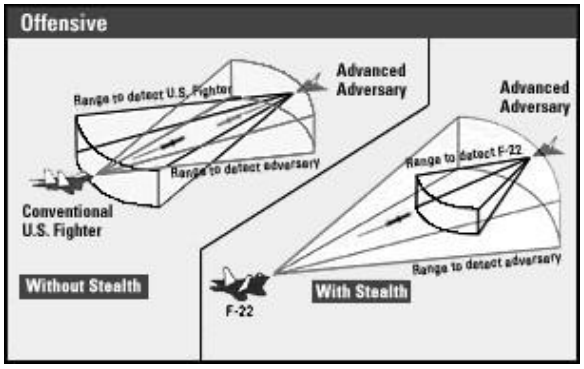
Seis fases de la respuesta a incidentes

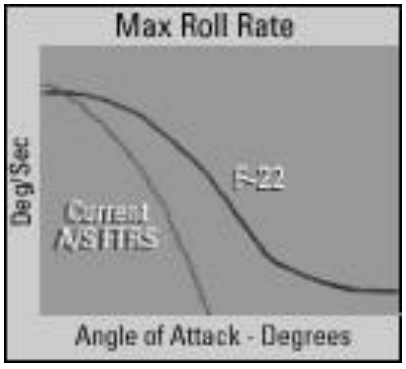


¿SE ESTÁ SUPERANDO EL LÍMITE?

Conozca su equipo e infraestructura

- Conozca el rendimiento de todos sus equipos (routers, switches, servidores, etc.). Tienes que saber lo que tu equipo es realmente capaz de hacer.
- Conozca las capacidades de su red. Si es posible, pruébela. Las sorpresas no son divertidas durante un incidente de seguridad
- pps vs. bps vs. qps vs. cps vs. tps - y, cómo influye la habilitación de características



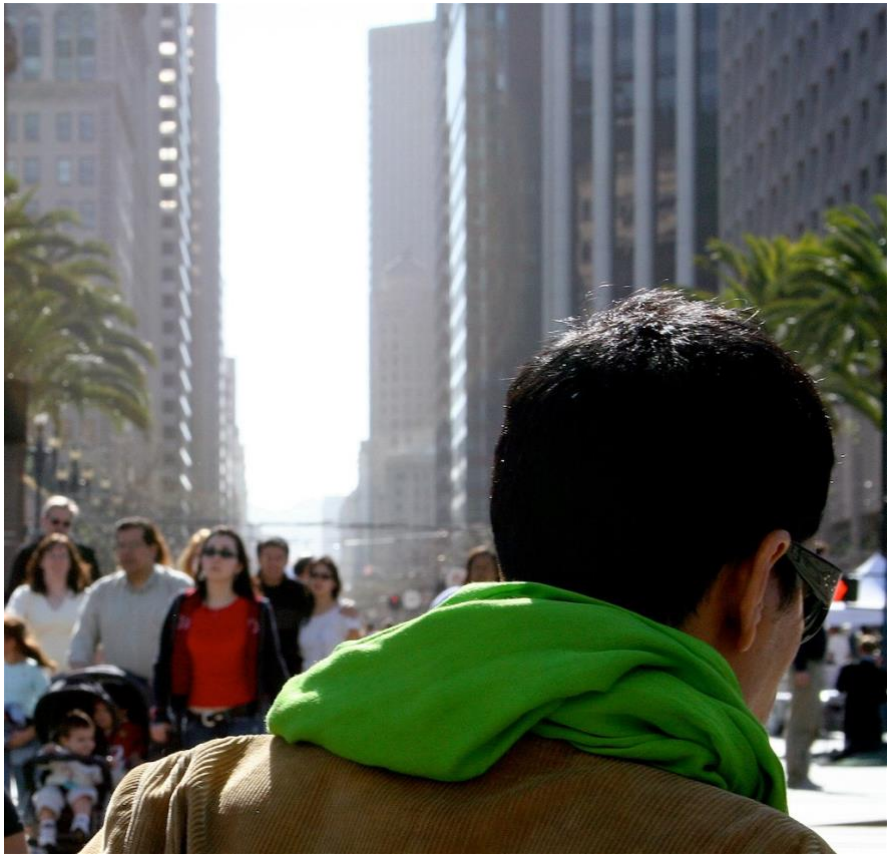


ARBOR NETWORKS

Arquitectura

Las herramientas adecuadas para el trabajo adecuado

Las personas adecuadas para el trabajo adecuado



Requisitos de habilidades del equipo OPSEC

El equipo OPSEC necesita saberlo:
Todo lo que sabe un ingeniero de Backbone

Todo lo que sabe un ingeniero de gestión de redes

Todo lo que sabe un sysadmin/webmaster Todo lo

que sabe un postmaster de correo electrónico

Todo lo que sabe un ingeniero de

DNS/DHCP/Direccionamiento Todo lo que sabe un

ingeniero de CERT

Todo lo que sabe un especialista en infoseguridad empresarial

En esencia, se buscan superingenieros que sean híbridos de Backbone/Ingenieros de Seguridad.

ARBOR NETWORKS

Mejores prácticas actuales de infraestructura (BCP)

- Las ACLs de interfaz (iACLs) deben emplearse en los bordes de la red pertinentes (peering/tránsito, borde de agregación del cliente, etc.) para proteger la propia infraestructura de la red; deben utilizarse secciones adicionales específicas de los servicios para restringir el tráfico destinado a los servidores orientados a Internet a los puertos y protocolos asociados a los servicios y aplicaciones de dichos servidores.

- El uso de GRE -Protocolo IP 47- en estos ataques es notable como un mecanismo común utilizado por los atacantes para eludir las ACLs que sólo contienen declaraciones de política relacionadas con protocolos comunes como TCP, UDP e ICMP; hay 254 protocolos válidos de Internet, y los protocolos irrelevantes deben ser filtrados en los bordes a través de ACLs.

- También deberían desplegarse otros BCP de la infraestructura de red, como los mecanismos de autoprotección del plano de control y de gestión (rACL, CoPP, GTSM, clave MD5, etc.).

- Todos los dispositivos de la infraestructura de red deben ser accesibles únicamente a través de los hosts de gestión designados, y este acceso debe facilitarse a través de una red de gestión dedicada fuera de banda (OOB). Durante los ataques DDoS de alto impacto, una red de gestión dedicada garantiza que los dispositivos puedan ser gestionados independientemente de las condiciones de la red de producción, y también garantiza que los mecanismos vitales como la telemetría de flujo y SNMP no se interrumpan, lo que asegura la visibilidad continua del tráfico de ataque durante un incidente

PBC de infraestructura (cont.)

- La telemetría de flujo, como Cisco NetFlow, Juniper cflowd y sFlow, debería estar habilitada en todos los bordes de la red y exportada a un sistema de recopilación/análisis.
- El blackholing basado en la fuente (S/RTBH) es una poderosa técnica de reacción que permite que decenas o incluso cientos de miles de IPs de origen de ataque (clasificadas a través del análisis de flujo, archivos de registro, etc.) sean rápidamente bloqueadas en base a sus direcciones de origen. S/RTBH aprovecha BGP como mecanismo de plano de control para indicar instantáneamente a los dispositivos de borde que empiecen a descartar el tráfico de ataque. Flowspec permite una granularidad de capa 4: ¡despliegue instantáneo de ACL a través de BGP!
- Los sistemas inteligentes de mitigación de DDoS (IDMS) deben desplegarse en centros de limpieza topológicamente adecuados para proteger los servidores/servicios/aplicaciones. Deberían colocarse al norte de los equilibradores de carga; si una organización insiste en colocar cortafuegos e IDS/'IPS' en línea delante de los servidores, ¡proteja estos puntos de estrangulamiento de DDoS con estado y todo lo que hay detrás de ellos!
- No coloque cortafuegos ni IDS/'IPS' delante de los servidores: no aportan ningún valor de seguridad en entornos de servidores en los que cada conexión entrante es, por definición, no solicitada. Son puntos de estrangulamiento DDoS, y degradan la postura de seguridad operativa de la red y las aplicaciones.

ARBOR NETWORKS

Acoge las mejores prácticas actuales (BCP)

- Los servidores de cara al público deben estar configurados de forma reforzada, con servicios innecesarios desactivados, acceso a la gestión OOB, endurecimiento de la configuración específica del servicio, ajuste de la pila IP y otros mecanismos relevantes.

- El filtrado sin estado en el servidor a través de tcpwrappers es un mecanismo útil de aplicación de políticas; para los servidores web, los módulos de Apache como mod_security y mod_evasive aportan capacidades adicionales.

- El despliegue de cortafuegos con estado u otros dispositivos de inspección como IDS/'IPS' frente a los servidores orientados a Internet está contraindicado; como cada conexión entrante a los servidores orientados a Internet es, por definición, no solicitada, la inspección con estado no añade nada a la postura de seguridad de los servidores, y sirve para debilitar su capacidad de soportar el tráfico DDoS debido al tamaño limitado de la tabla de estados incluso de los cortafuegos e IDS/IPS más grandes/rápidos del mercado actual.

  Durante estos ataques en particular y muchos otros, se observó que los cortafuegos situados frente a los servidores objetivo fallaban mientras recibían cantidades relativamente bajas de tráfico de ataque, lo que permitía que el DDoS lograra dejar los servidores fuera de servicio con poco esfuerzo por atacante

PBC de acogida (cont.)

- Los balanceadores de carga también instancian estado que hace que los servidores reales detrás de los balanceadores de carga sean más vulnerables a los DDoS; durante estos ataques, se observó que los balanceadores de carga fallaban debido al agotamiento del estado como resultado del tráfico de ataque. S/RTBH, flowspec, cachés de proxy inverso e IDMS deberían utilizarse para proteger el equilibrador de carga y los servidores reales detrás de él.

- La infraestructura del DNS debe desplegarse en una arquitectura modular, con separación de funciones como servidores autoritativos, resolutores internos, resolutores externos, resolutores de sólo caché, etc., y debe escalarse adecuadamente empleando técnicas como el direccionamiento IPv4 anycast. Deberían emplearse mecanismos de autodefensa de los servidores DNS, como RRL e IDMS, para proteger el DNS de ataques deliberados y/o daños colaterales.

¿Estamos condenados?

- ***No. La*** implementación de herramientas/técnicas/BCPs existentes y bien conocidas da lugar a una postura de seguridad muy mejorada con resultados medibles.
- La evolución de las defensas contra estos ataques demuestra que es posible un cambio positivo: las organizaciones objetivo y los ISP/MSSP defensores han modificado las arquitecturas, las técnicas de mitigación, los procesos y los procedimientos para mitigar con éxito estos ataques.
- Las capacidades de mitigación se están ampliando para satisfacer y superar los volúmenes de ataques: la arquitectura de despliegue, el ancho de banda de desviación/reinyección y el aprovechamiento de la infraestructura de red son fundamentales.

- La automatización es una buena cosa, pero no sustituye a una arquitectura resistente, una planificación perspicaz y un personal de operaciones inteligente, que son más importantes ahora que nunca.

Resumen

- La situación actual es similar a la de cuando Windows XP era el sistema operativo más utilizado: muchos dispositivos vulnerables y poca defensa contra el peligro. Esto se solucionó lanzando software más resistente y, poco a poco, el número de dispositivos vulnerables se redujo. Sin embargo, todavía tenemos ordenadores vulnerables con Windows XP conectados a Internet.   ¡y ahora tenemos órdenes de magnitud de dispositivos IoT más vulnerables!
- Los bots son cada vez más inteligentes y tienen capacidades más avanzadas. El bot Medusa, basado en Windows, genera hilos del navegador IE para realizar ataques HTTP y HTTP/S avanzados. Se necesita más inteligencia para hacer frente a estos ataques, ¡y nosotros la tenemos!
- Las defensas deben implementarse ***antes de que*** se produzcan los ataques.
- El éxito de la defensa DDoS contra ataques de gran capacidad y complejidad tiene lugar ***todos los días***!
- ***Sabemos cómo hacerlo.***

Gracias.

Roland Dobbins, *ingeniero principal*
< rdobbins@arbor.net>

ARBOR NETWORKS
The Security Division of NETSCOUT