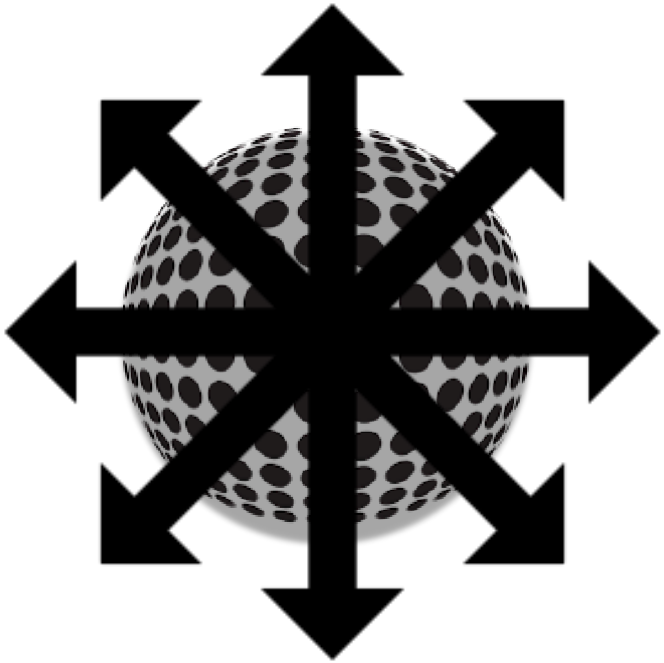
93rd IETF Prague
July 19 – 24, 2015



Grupo de trabajo de señalización de amenazas abiertas DDoS (DOTS)

Requisitos operativos

Chris Morrow < morrowc@ops--netman. net> *Ingeniero de seguridad de redes*, Google

Roland Dobbins < rdobbins@arbor.net> *Ingeniero principal*, Arbor Networks

Introducción y contexto

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

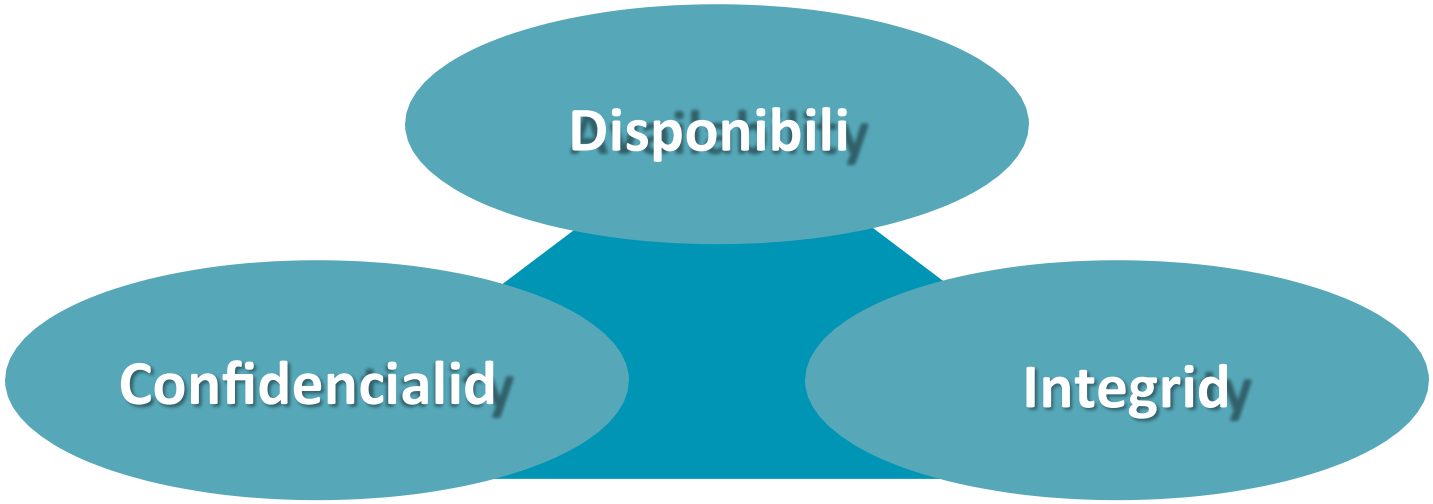
- Los ataques casi siempre se **distribuyen** para lograr un efecto aún más significativo (es decir, DDoS)

- 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¡Sin** disponibilidad no applications/services/ data/Internet! no hay ingresos!

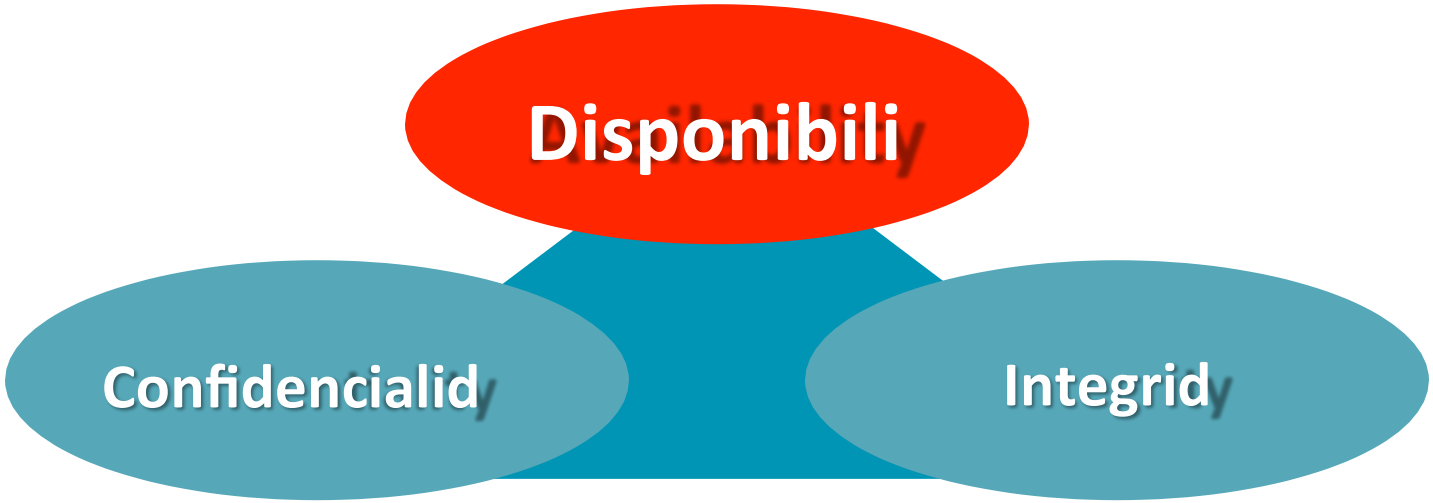
-¡Los ataques DDoS son ataques **contra la capacidad y/o el estado**!

Tres características de seguridad



El objetivo de la seguridad es mantener estas tres características

Tres características de seguridad



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

Realidades de la defensa DDoS

Percepción común de la postura de seguridad en Internet hoy en día

Estado actual de las defensas en Internet

¿Quién puede ayudar?

Su ISP o MSSP.

¿Cómo puede pedir ayuda hoy?

Tecnología iniciada por Robert Hooke en 1667, ¡sólo ligeramente mejorada!

Pedir ayuda es difícil Saber cómo ayudar es más difícil

- La mayoría de los clientes finales no tienen ni idea de cómo es su tráfico de Internet normal, y mucho menos de lo que está ocurriendo realmente cuando están siendo atacados por DDoS (¡o incluso *entender* que están siendo atacados!).
- Muchos ISPs/MSSPs no proveen defensas DDoS en detalle para sus clientes finales**.** En muchos casos (¿la mayoría?), los clientes finales no pueden articular qué servidores/servicios necesitan protección, qué políticas de acceso a la red deben aplicarse, etc.
- Esto ralentiza drásticamente los tiempos de reacción/mitigación.
- Esto impide drásticamente la eficacia de la reacción/mitigación.
- Esto conduce a interrupciones prolongadas, pérdida de ingresos, clientes finales frustrados (y clientes de esos clientes finales)

Hoy en día existen métodos automatizados de notificación de ataques DDoS

- Pero son de propiedad.
- Los clientes finales no pueden mezclar vendedores, proveedores de mitigación de DDoS en la nube ISP, proveedores de mitigación de DDoS en la nube MSSP. La coordinación efectiva durante un ataque es prácticamente *imposible*.
- Los servidores/servicios/dispositivos de infraestructura que son el objetivo de los DDoS no pueden señalar la mitigación, incluso si tienen la capacidad de detectar y clasificar los ataques DDoS (piense en Apache mod_security/mod_evasive, BIND RRL).
- Los ISP/MSSP deben coordinarse (mal, ineficientemente) manualmente cuando trabajan conjuntamente para mitigar los ataques DDoS.
- A medida que los atacantes cambian los vectores/recursos DDoS, se produce una latencia severa, un error común entre los defensores.
- Los portales web existen; son específicos de los proveedores/ISP/MSSP, tienen diversos grados de configurabilidad de la mitigación (la mayoría de los clientes finales no sabrían qué configurar), y pueden ser difíciles de acceder durante un ataque cuando se confunden el IDC y el tránsito de la LAN del cliente.

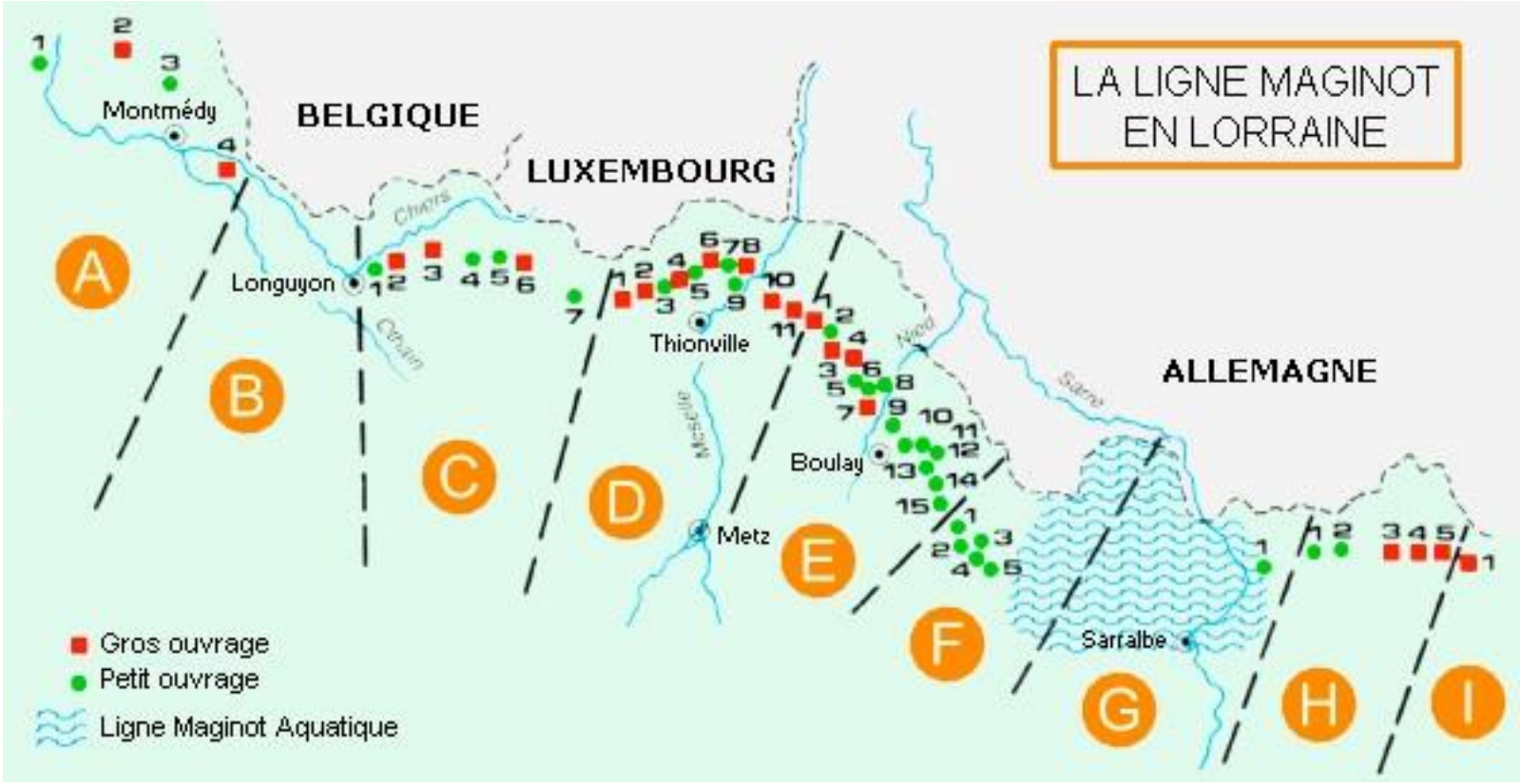
La defensa contra el DDoS se convierte en un concurso de mecanografía...

Atacante.

La defensa contra el DDoS se convierte en un concurso de mecanografía...

Defensor.

Defensas en gran parte estáticas y de baja agilidad . .



. . . Llevar a resultados predecibles.

Coordinación de las defensas DDoS, Circa 1995.

```
 PINE 4.64   MAIN MENU [A]                        Folder: INBOX  13 Messages

      ?     HELP              -  Get help using Pine
      C     COMPOSE MESSAGE   -  Compose and send/post a message
      I     MESSAGE INDEX     -  View messages in current folder
      L     FOLDER LIST       -  Select a folder OR news group to view
      A     ADDRESS BOOK      -  Update address book
      S     SETUP             -  Configure Pine Options
      Q     QUIT              -  Leave the Pine program


   Copyright 1989-2005.  PINE is a trademark of the University of Washington.
                 [Folder "INBOX" opened with 13 messages - 1 new]
? Help                    P PrevCmd                 R RelNotes
O OTHER CMDS > [ListFldrs] N NextCmd                K KBLock
```

Coordinación de las defensas DDoS, circa 2005.

```
 PINE 4.64   MAIN MENU [A]                        Folder: INBOX  13 Messages

      ?     HELP              -  Get help using Pine
      C     COMPOSE MESSAGE   -  Compose and send/post a message
      I     MESSAGE INDEX     -  View messages in current folder
      L     FOLDER LIST       -  Select a folder OR news group to view
      A     ADDRESS BOOK      -  Update address book
      S     SETUP             -  Configure Pine Options
      Q     QUIT              -  Leave the Pine program


   Copyright 1989-2005.  PINE is a trademark of the University of Washington.
                [Folder "INBOX" opened with 13 messages - 1 new]
? Help                    P PrevCmd                 R RelNotes
O OTHER CMDS > [ListFldrs] N NextCmd                K KBLock
```

Coordinación de las defensas DDoS, alrededor de 2015.

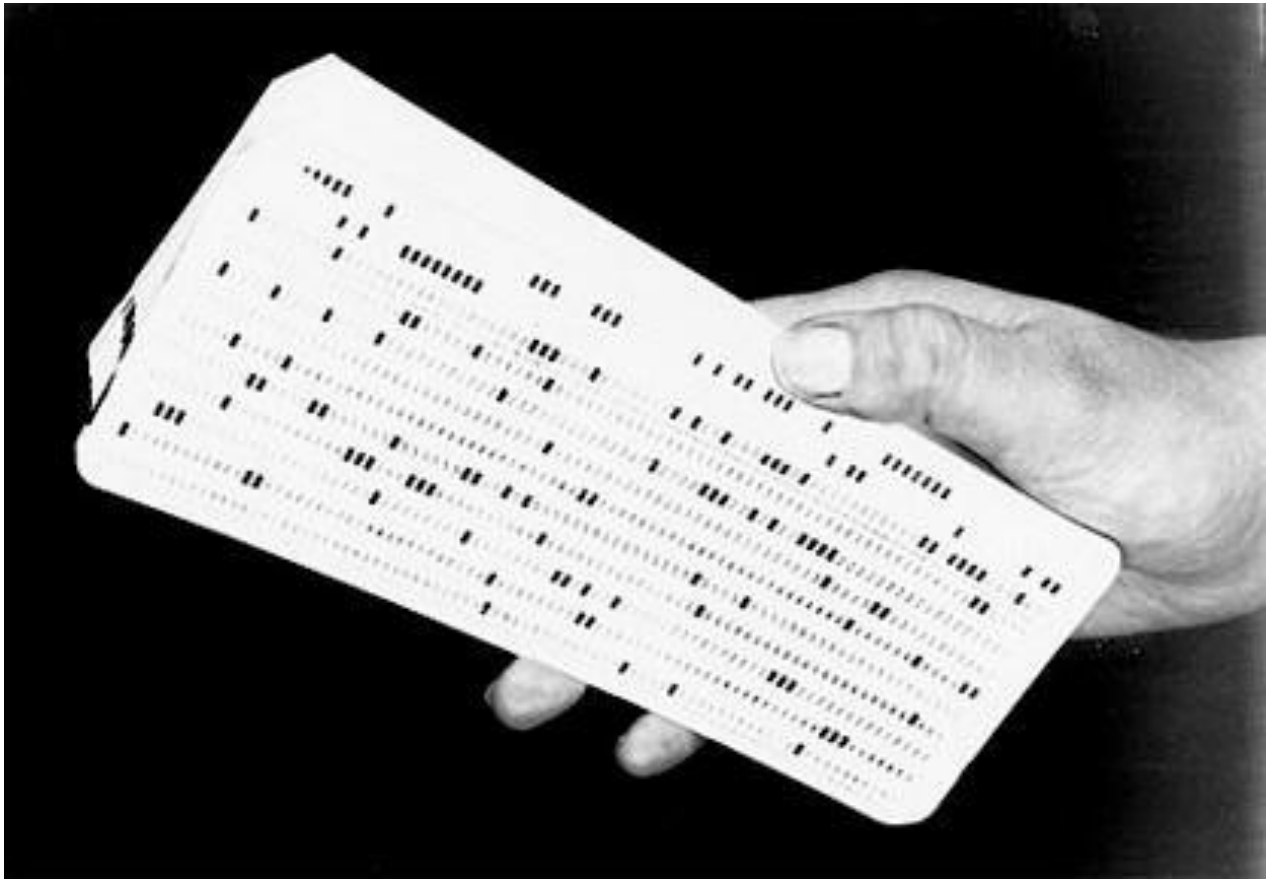
```
 PINE 4.64   MAIN MENU [A]                        Folder: INBOX  13 Messages

      ?     HELP              -  Get help using Pine
      C     COMPOSE MESSAGE   -  Compose and send/post a message
      I     MESSAGE INDEX     -  View messages in current folder
      L     FOLDER LIST       -  Select a folder OR news group to view
      A     ADDRESS BOOK      -  Update address book
      S     SETUP             -  Configure Pine Options
      Q     QUIT              -  Leave the Pine program


   Copyright 1989-2005.  PINE is a trademark of the University of Washington.
                [Folder "INBOX" opened with 13 messages - 1 new]
? Help                    P PrevCmd                 R RelNotes
O OTHER CMDS > [ListFldrs] N NextCmd                K KBLock
```

Podemos -y debemos- hacerlo mejor.

Necesitamos una forma estandarizada de compartir la información...



. . . A través de un transporte rápido, de baja latencia y *poco fiable* . .

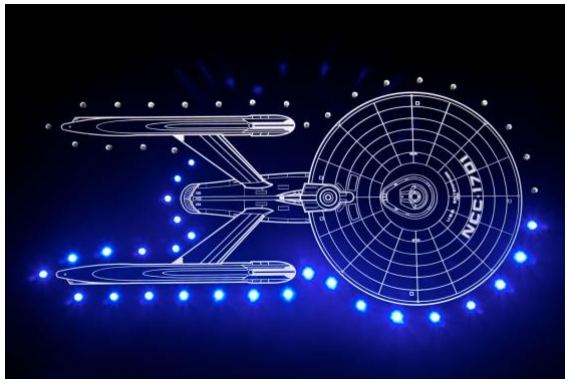
. . . A través de un transporte *fiable* que hará que *las políticas . .*

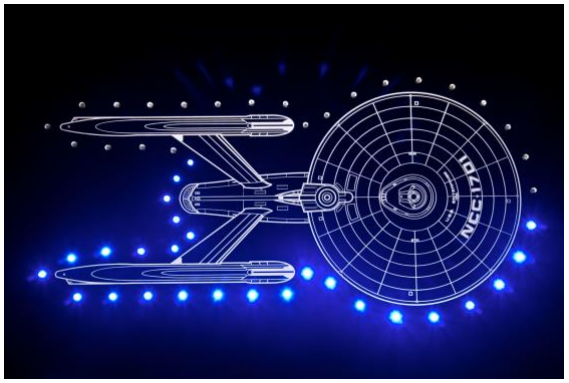
. . . Háblenos de sí mismo, de sus problemas y de sus acciones deseadas. . .

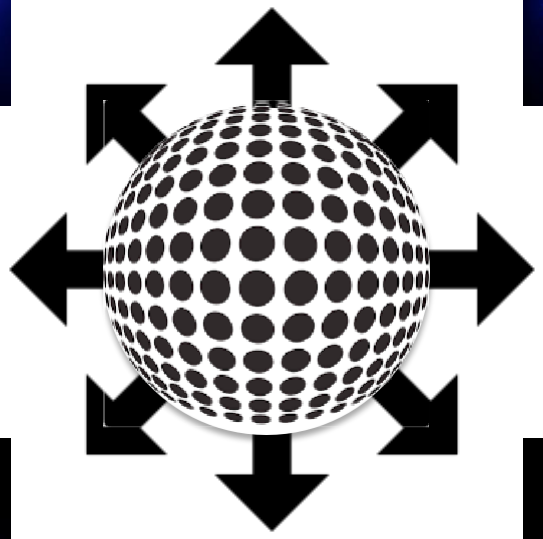
. . . Que puede ser transmitido interna y externamente según sea necesario . .

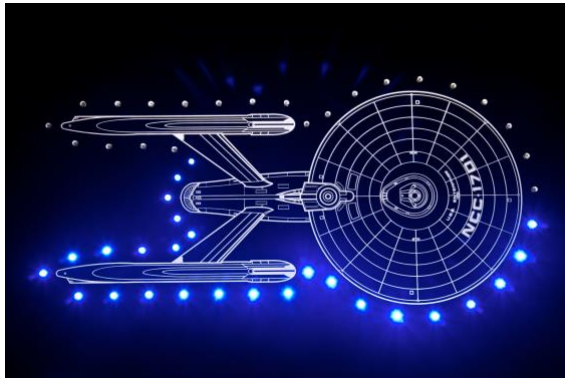
. . . Todos y todo en la red pueden participar . .

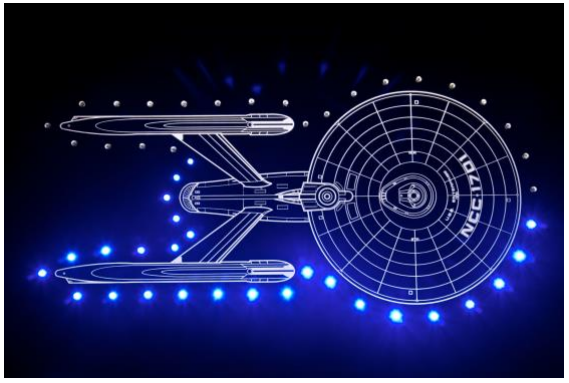
. . . En Defensa coordinada y a la carta contra DDoS.











Resumen de los requisitos operativos del DOTS

Requisitos operativos del DOTS

- Intercambio de información sobre ataques DDoS y su mitigación basado en estándares.
- No debe asumir las capacidades de detección/clasificación orgánica del suplicante.
- Debe trabajar en transportes comunes, tanto fiables como no fiables.
- Debe soportar la autenticación mutua y la criptografía opcional.

Requisitos operativos del DOTS (cont.)

- Debe describir el objetivo atacado (rango de direcciones IP, puertos/protocolos/servicios que se ejecutan en el objetivo, etc.).
- Debe describir el resultado deseado en términos generales (bloquear, redirigir, fregar, limitar la velocidad, etc.).
- Debe actualizar al solicitante con las acciones implementadas y el estado, el solicitante debe hacer lo mismo.
- Debe apoyar los relevos intra e interorganizacionales.

Requisitos operativos del DOTS (cont.)

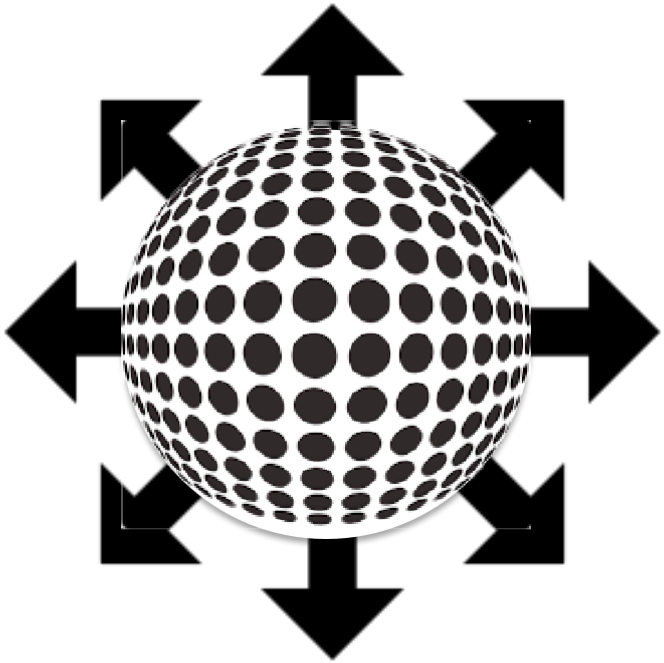
- Debe admitir el filtrado y la transformación de acciones/resultados basados en políticas.
- Debe ser extensible.
- Debe centrarse en el DDoS inicialmente, otros usos pueden venir después.
- Debe minimizar la complejidad de la implementación y la interacción de los nodos.

Requisitos operativos del DOTS (cont.)

- Debe incluir una función de "latido".
- Debe ser agnóstica a la tecnología de detección/clasificación/mitigación.
- Debe soportar el ámbito de distribución permitido (TLP?).
- Debe utilizar los protocolos y modelos de información existentes siempre que sea posible y adecuado.

Esta presentación - http://bit.ly/1I2IVrF

93rd IETF Prague
July 19 – 24, 2015



Grupo de trabajo de señalización de amenazas abiertas DDoS (DOTS)

Gracias.

Chris Morrow < morrowc@ops--netman. net>
Ingeniero de seguridad de redes, Google

Roland Dobbins < rdobbins@arbor.net>
Ingeniero principal, Arbor Networks