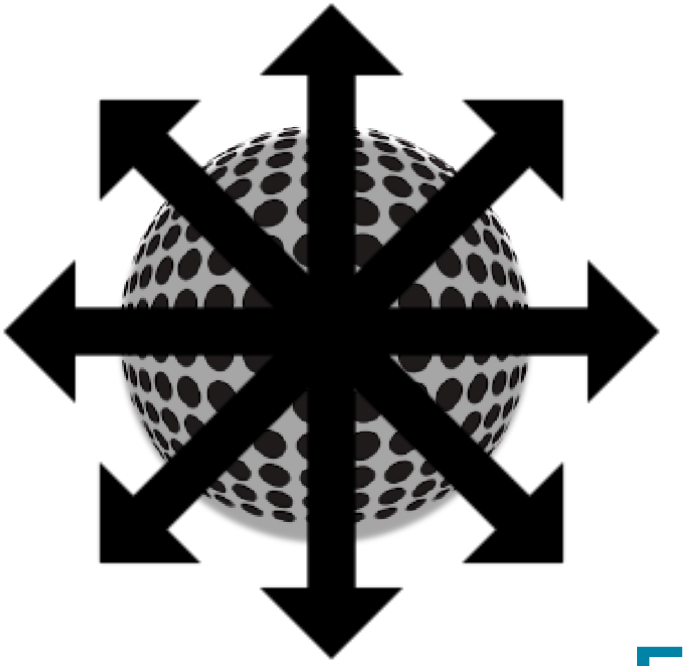
93rd IETF Prague
July 19 – 24, 2015



Groupe de travail DDoS Open Threat Signaling (DOTS)

Exigences opérationnelles

Chris Morrow < morrowc@ops--netman. net>
Ingénieur en sécurité réseau, Google

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

Introduction et contexte

Contexte des DDoS

Qu'est-ce qu'une attaque par déni de service distribué (DDoS) ?

- Une tentative de **consommer des ressources** limitées, d'**exploiter les faiblesses** de la conception ou de la mise en œuvre du logiciel, ou d'**exploiter le manque de capacité de** l'infrastructure.

- Cible la **disponibilité** et l'**utilité** des ressources informatiques et du réseau.

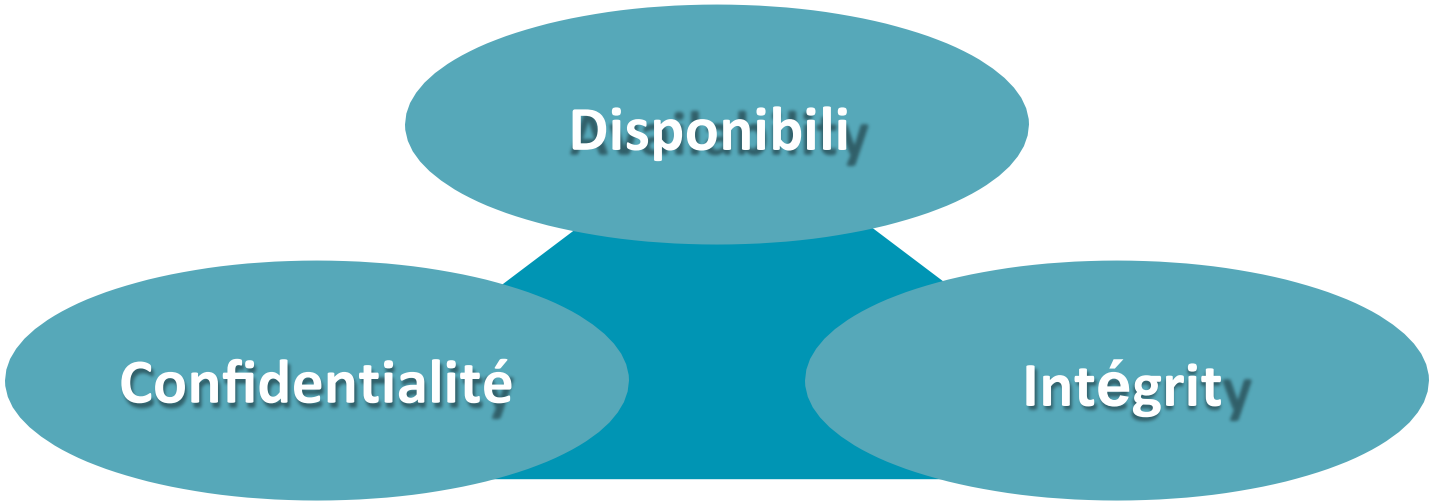
- Les attaques sont presque toujours **distribuées** pour avoir un effet encore plus important (par exemple, DDoS).

- Les **dommages collatéraux** causés par une attaque peuvent être aussi graves, voire pires, que l'attaque elle-même.

- **Les attaques DDoS affectent la disponibilitéPas de** disponibilité, no applications/services/ data/Internet! pas de revenus !

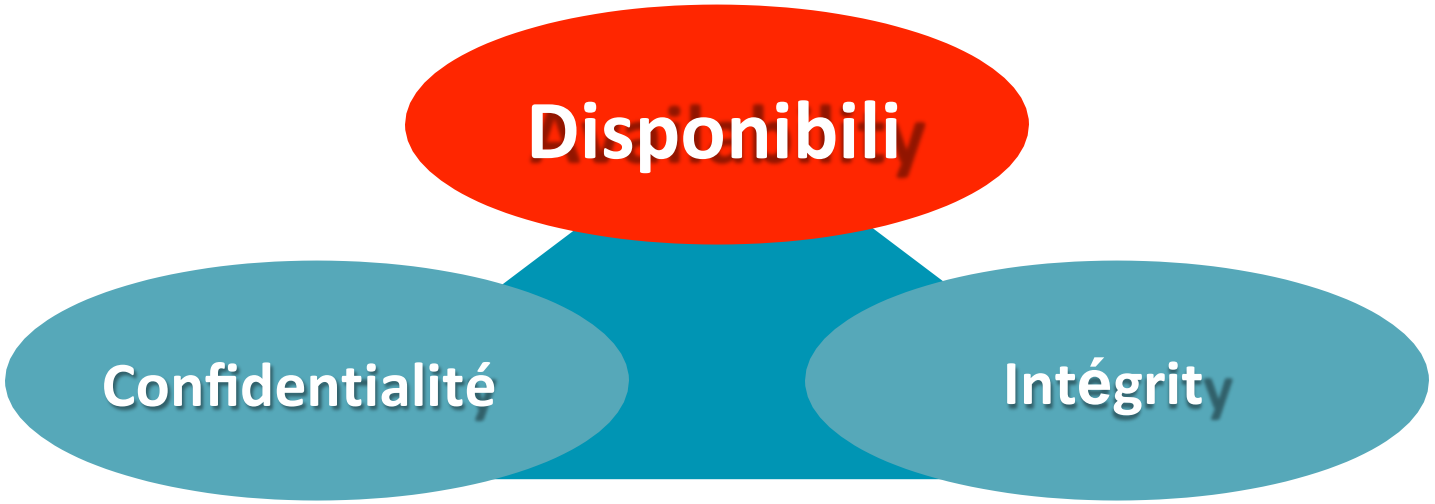
-Les attaques DDoS sont des attaques **contre la capacité et/ou l'état** !

Trois caractéristiques de



L'objectif de la sécurité est de maintenir les trois caractéristiques suivantes

Trois caractéristiques de



L'objectif principal de la défense contre les DDoS est de maintenir la disponibilité face à une attaque.

Réalités de la défense DDoS coordonnée

Perception commune de la posture de sécurité Internet

L'état actuel des défenses sur Internet

Qui peut aider ?

Votre ISP ou MSSP !

Comment pouvez-vous demander de l'aide aujourd'hui ?

Technologie mise au point par Robert Hooke en 1667, mais légèrement améliorée !

Demander de l'aide est difficile !

- La plupart des clients finaux n'ont aucune idée de ce à quoi ressemble leur trafic Internet normal, et encore moins de ce qui se passe réellement lorsqu'ils sont victimes de DDoS (ou même s'ils *comprennent* qu'ils sont attaqués !).
- De nombreux ISP/MSSP ne prévoient pas de défenses DDoS en détail pour leurs clients finaux. Dans de nombreux cas (la plupart ?), les clients finaux ne sont pas en mesure de définir les serveurs/services à protéger, les politiques d'accès au réseau à mettre en place, etc.
- Cela ralentit considérablement les temps de réaction et d'atténuation.
- Cela entrave considérablement l'efficacité de la réaction et de l'atténuation.

Demander de l'aide est difficile !

- Cela entraîne des pannes prolongées, des pertes de revenus, des clients finaux frustrés (et les clients de ces clients finaux).

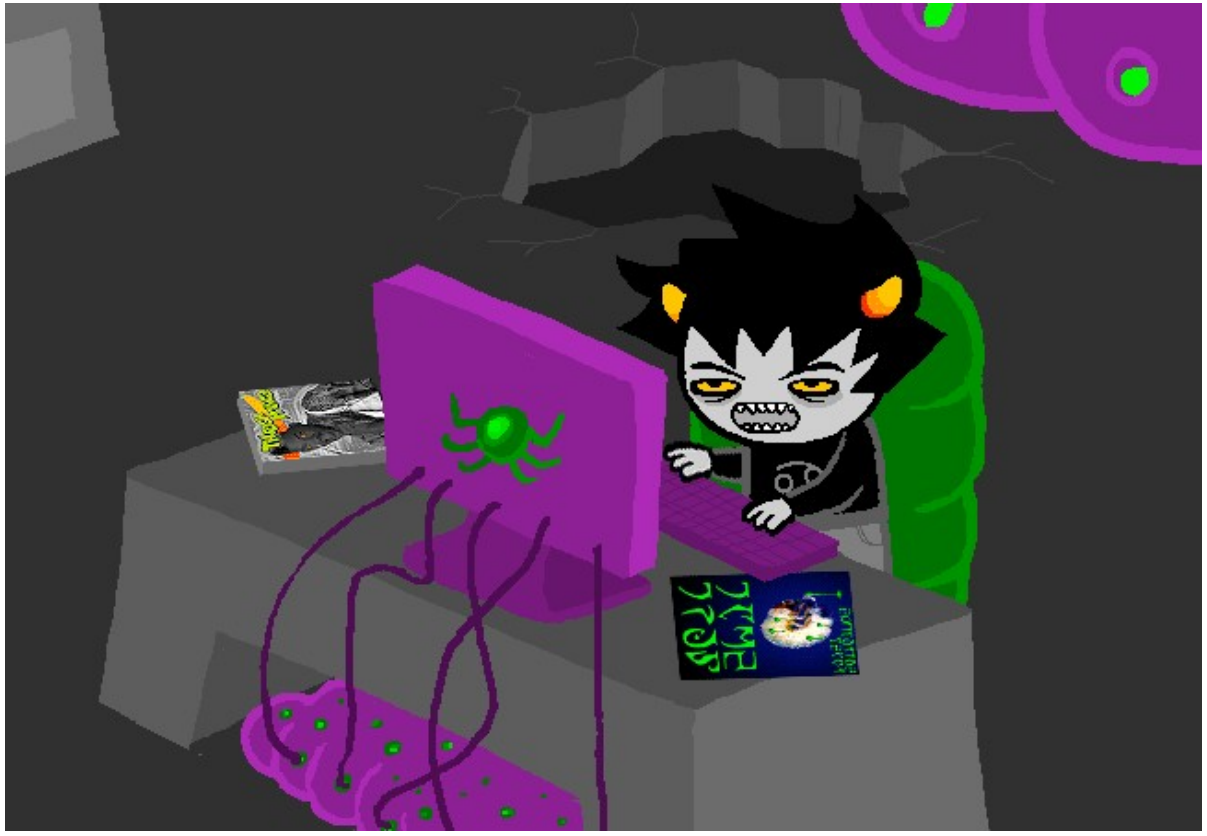
Les méthodes automatisées de notification des attaques

- Mais ils sont propriétaires !
- Les clients finaux ne peuvent pas mélanger les fournisseurs, les fournisseurs d'atténuation en nuage des attaques DDoS des FAI et les fournisseurs d'atténuation en nuage des attaques DDoS des MSSP. Une coordination efficace pendant une attaque est, à toutes fins pratiques, *impossible*.
- Les serveurs/services/infrastructures qui sont la cible de DDoS ne peuvent pas signaler les mesures d'atténuation, même s'ils ont la capacité de détecter et de classifier les attaques DDoS (pensez à Apache mod_security/mod_evasive, BIND RRL).
- Les FAI/MSSP doivent se coordonner (mal, inefficacement) manuellement lorsqu'ils travaillent conjointement pour atténuer les attaques DDoS.
- Comme les attaquants déplacent les vecteurs/ressources DDoS, une latence importante et des erreurs courantes se produisent entre les défenseurs.

Les méthodes automatisées de notification des attaques

- Les portails Web existent ; ils sont spécifiques aux fournisseurs/ISP/MSSP, ont des degrés variables de configuration de l'atténuation (la plupart des clients finaux ne sauraient pas quoi configurer), et peuvent être difficiles d'accès pendant une attaque lorsque l'IDC et le transit LAN du client sont confondus.

La défense contre les DDoS devient un concours de dactylographie . .

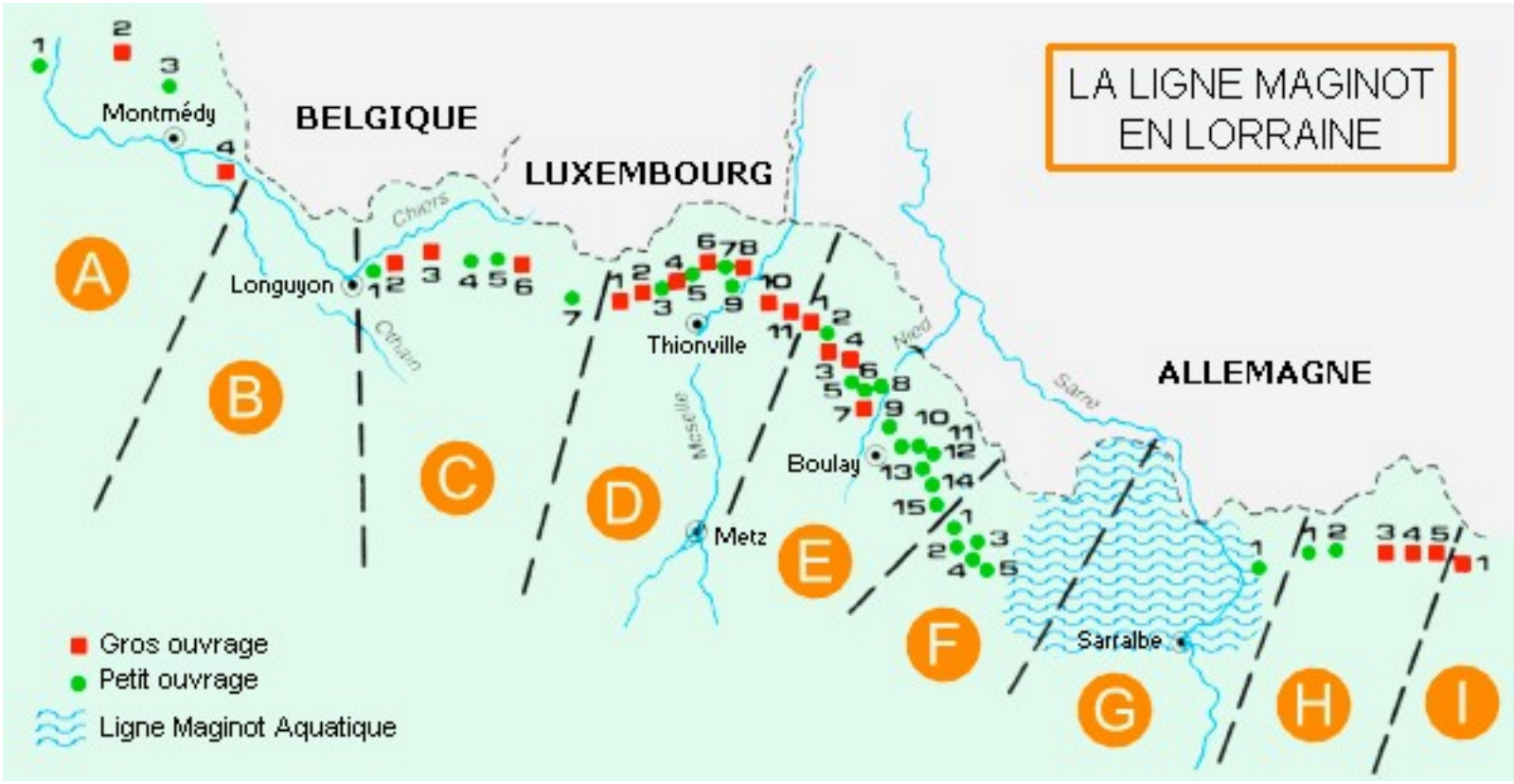


Attaquant.

La défense contre les DDoS devient un concours de dactylographie . .

Défenseur.

Des défenses largement statiques et à faible agilité . . .



GT DOTS

. . . Conduisent à des résultats prévisibles .

Coordination des défenses DDoS, vers 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
```

Coordination des défenses DDoS, vers 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
```

Coordination des défenses DDoS, vers 2015.

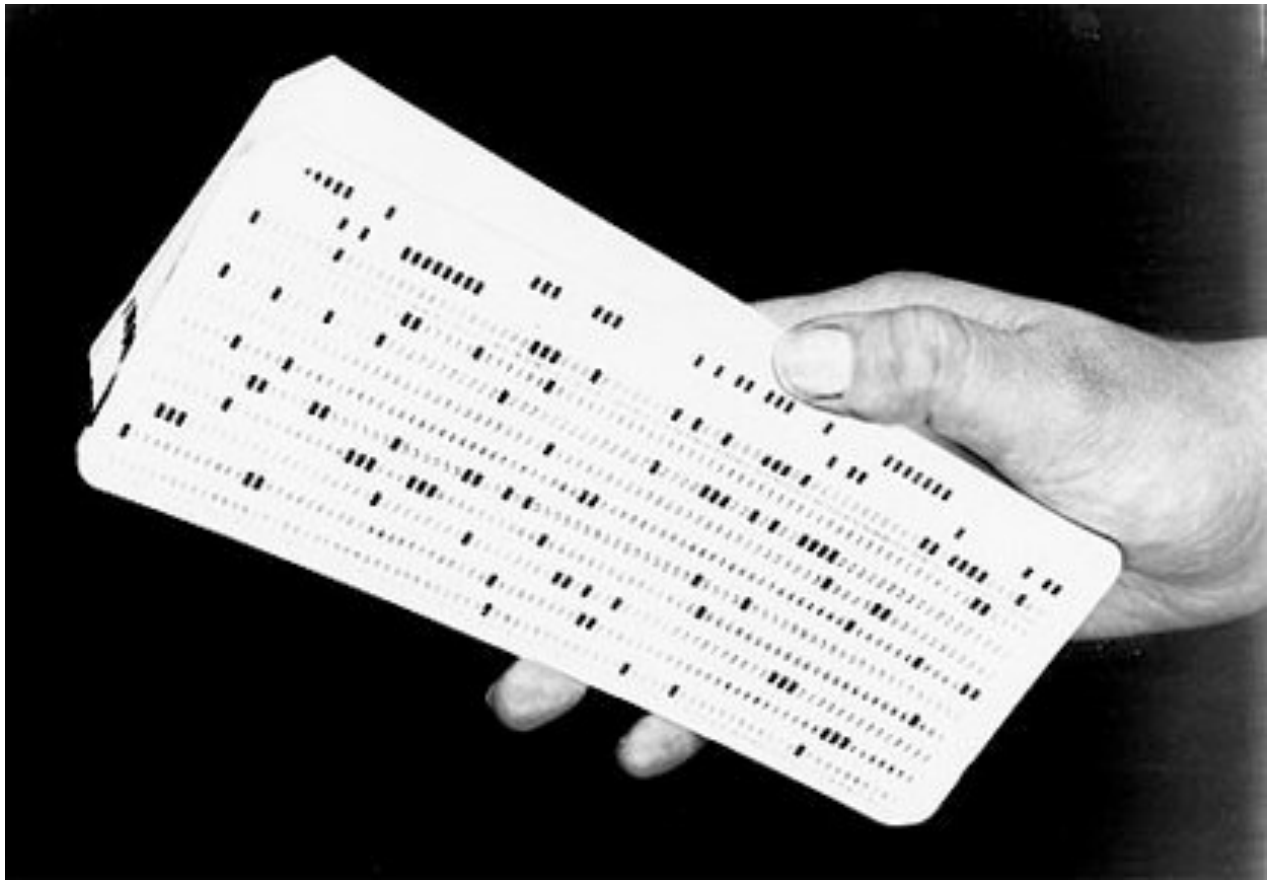
```
 PINE 4.64   MAIN MENU [A]                        Folder: INBOX  13 Messages

     ?     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
```

Nous pouvons - et *devons* - faire mieux que cela !

Nous avons besoin d'un moyen normalisé de partager l'information . . .



. . . À travers un transport rapide, à faible latence et *peu fiable* . . .

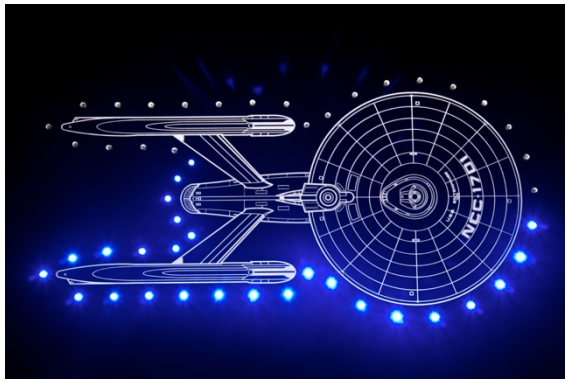
. . . À travers un transport *fiable* qui fera passer les *politiques* . . .

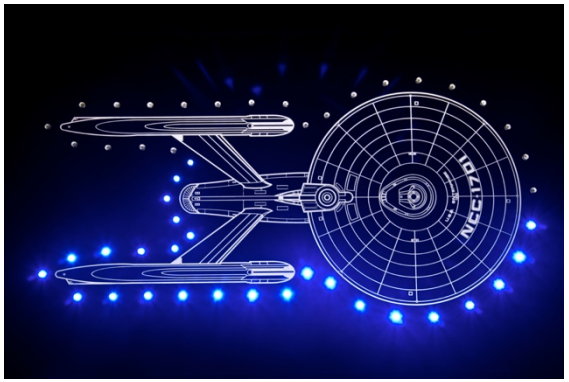
. . . Nous parler de lui-même, de ses problèmes et de ses

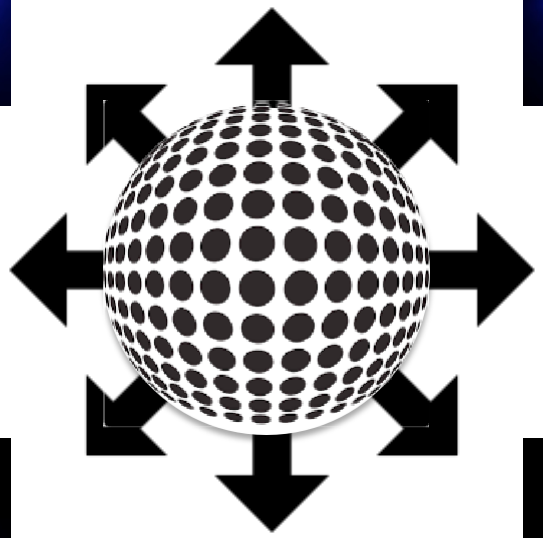
. . . Qui peuvent être relayés à l'intérieur et à l'extérieur en cas de besoin . .

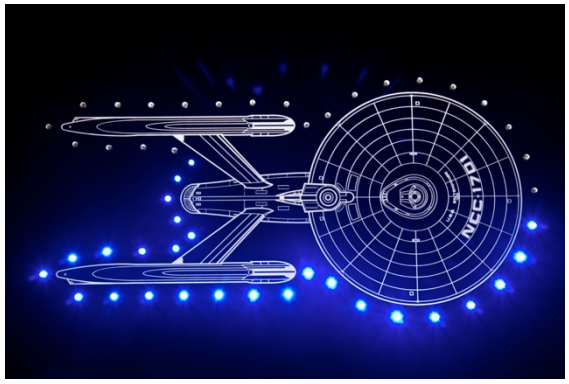
. . . Tout le monde et tous les éléments du réseau peuvent participer . .

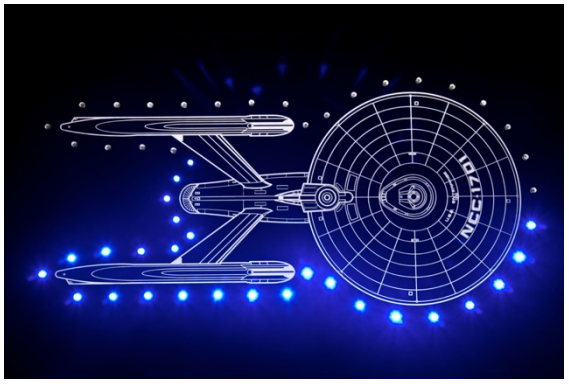
. . . Dans Coordinated, On-Demand DDoS Defense.











Résumé des exigences opérationnelles du DOTS

Exigences opérationnelles du DOTS

- Échange normalisé d'informations sur les attaques DDoS et leur atténuation.
- Ne doit pas présumer des capacités de détection/classification organiques du suppliant.
- Doit travailler sur des transports communs fiables et non fiables.
- Doit supporter l'authentification mutuelle et la cryptographie facultative.

Exigences opérationnelles du DOTS

- Doit décrire la cible de l'attaque (plage d'adresses IP, ports/protocoles/services fonctionnant sur la cible, etc.)
- Doit décrire le résultat souhaité en termes généraux (bloquer, rediriger, scrub, limiter le débit, etc.).
- Doit mettre à jour le supplicant avec les actions mises en œuvre et le statut, le supplicant doit faire de même.
- Doit supporter les relais intra- et inter-organisationnels.

Exigences opérationnelles du DOTS

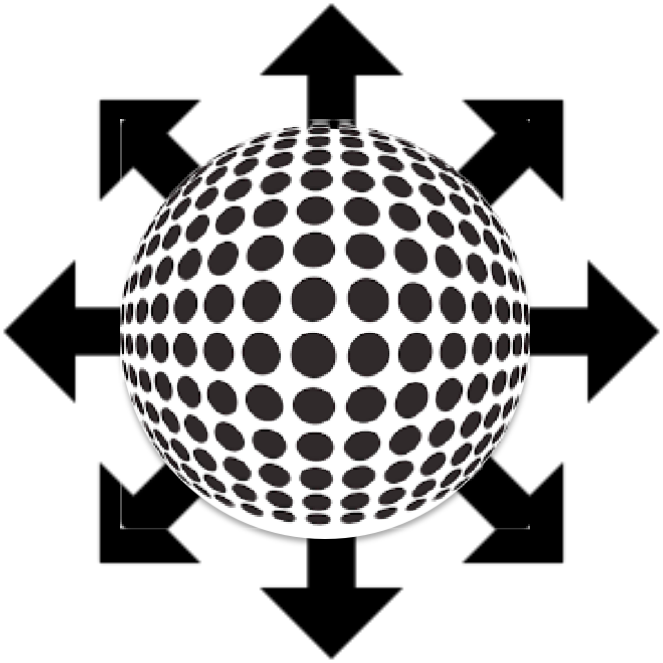
- Doit prendre en charge le filtrage et la transformation des actions/résultats basés sur des politiques.
- Doit être extensible.
- Doit se concentrer sur les DDoS dans un premier temps, les autres utilisations peuvent venir plus tard.
- Doit minimiser la complexité de la mise en œuvre et de l'interaction des nœuds.

Exigences opérationnelles du DOTS

- Doit inclure une fonction de "battement de cœur".
- Doit être agnostique en matière de technologie de détection/classification/atténuation.
- Doit supporter la portée de la distribution autorisée (TLP ?).
- devrait utiliser les protocoles et les modèles d'information existants dans la mesure du possible et chaque fois que cela est approprié.

Cette présentation - http://bit.ly/1I2IVrF

93rd IETF Prague
July 19 – 24, 2015



Groupe de travail DDoS Open Threat Signaling (DOTS)

Merci !

Chris Morrow < morrowc@ops--netman. net>
Ingénieur en sécurité réseau, Google

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