ARBOR NETWORKS

The Security Division of NETSCOUT

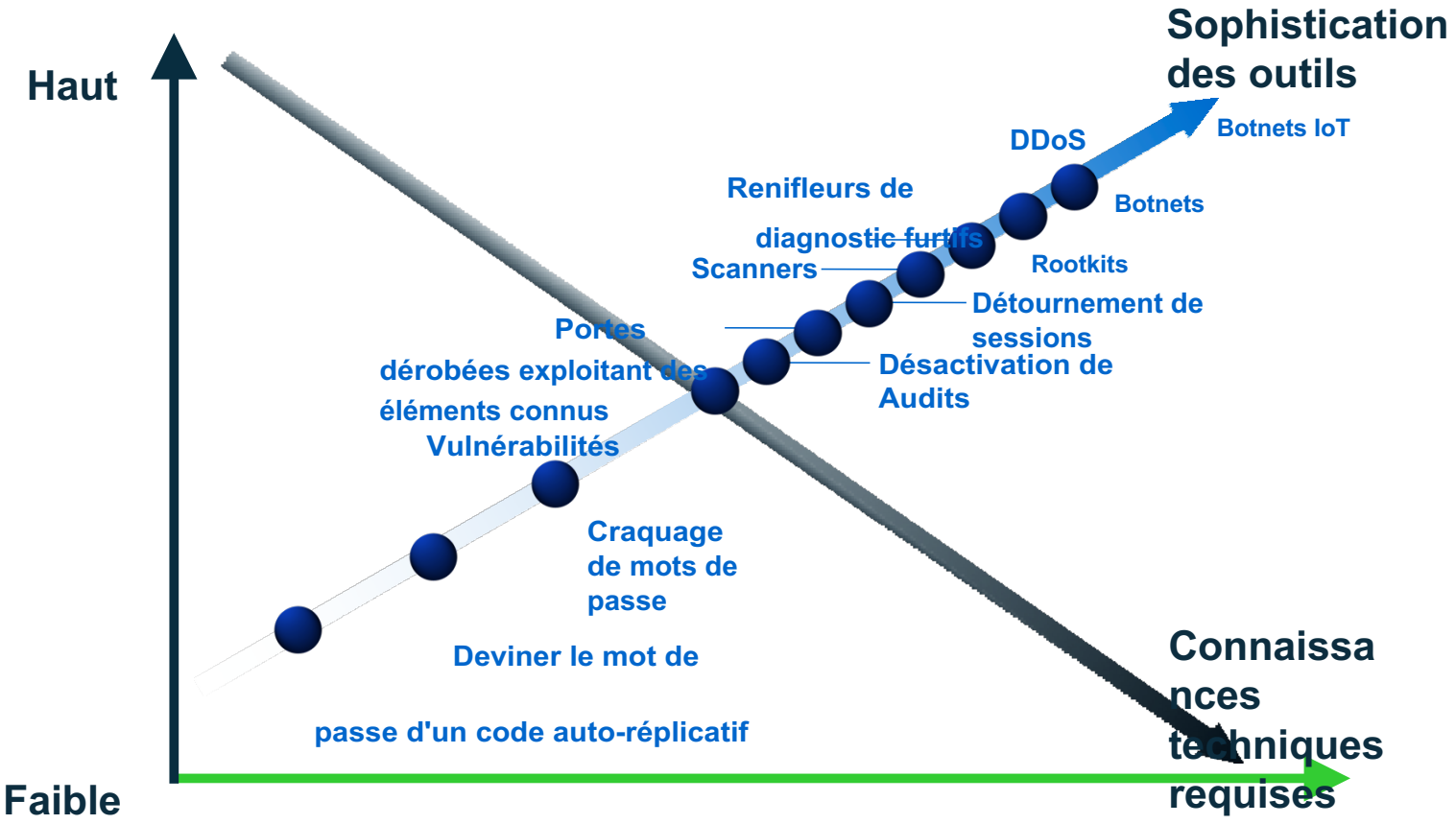
Récolter le tourbillon

La défense contre les DDoS à l'ère de Mirai

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

Introduction et contexte

Évolution des menaces et des exploits



Botnets - La première menace pour la sécurité en ligne

Wikipedia sur les botnets : ... une collection d'ordinateurs compromis (appelés ordinateurs zombies) [ou bots] exécutant des programmes, généralement appelés vers, chevaux de Troie ou portes dérobées, sous une infrastructure commune de commande et de contrôle.

Les botnets sont les principaux catalyseurs de toutes ces activités :

- DDoS
- Extorsion
- Fraude aux clics publicitaires
- Ventes frauduleuses
- Vol d'identité et fraude financière (hameçonnage, vol d'informations sur les PC, etc.)
- Vol de biens/services
- Espionnage/vol d'informations
- Manipulation boursière basée sur le spam

ARBOR NETWORKS

Attaques DDoS - Une réalité sur l'internet

- Les attaques DDoS ont lieu 24 heures sur 24, 7 jours sur 7 et 365 jours par an : elles font partie intégrante de la vie sur Internet.
- Toute organisation, tout site, tout individu peut être affecté par un DDoS, que ce soit en tant que cible directe ou par le biais de dommages collatéraux.
- Les attaques DDoS sortantes peuvent être tout aussi dévastatrices pour les clients finaux et les fournisseurs de services que les attaques DDoS entrantes - les hôtes botté sur les réseaux d'accès à large bande, sur les réseaux d'entreprise et dans les IDC affectent à la fois les réseaux sources et les cibles.
- La connaissance de la situation est essentielle - que se passe-t-il dans l'actualité ? Quels sont les anniversaires qui ont lieu cette année/mois/semaine/jour ?
- Les mécréants s'attaquent les uns aux autres avec régularité - dommages collatéraux

ARBOR® NETWORKS

Le nouveau nuage de l'empereur

- Nous nous appuyons sur des protocoles vieux de 34 ans, conçus pour être utilisés dans un environnement de laboratoire et avec peu ou pas de considération pour la sécurité, comme base de notre infrastructure Internet mondiale.
- Bien qu'il existe un grand nombre de travaux sur la sécurité opérationnelle (opsec) et les architectures Internet évolutives, ils sont davantage mis à l'honneur dans les brèches que dans les déploiements réels.
- Déconnexion permanente et généralisée entre les architectes de réseau, les architectes d'application, les groupes opérationnels, les équipes de sécurité et la direction.
- Attitude hypocrite à l'égard de la sécurité - "Pourquoi quelqu'un *nous* attaquerait-il ?
- Absence de responsabilité - quelqu'un a-t-il déjà été licencié à la suite d'incidents de sécurité évitables ?
- L'omniprésence du théâtre de la sécurité/de l'illusion de la sécurité.
- L'incapacité/la réticence à évaluer correctement les modèles de menace abstraits - un mécanisme de défense psychologique nécessaire ?

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).

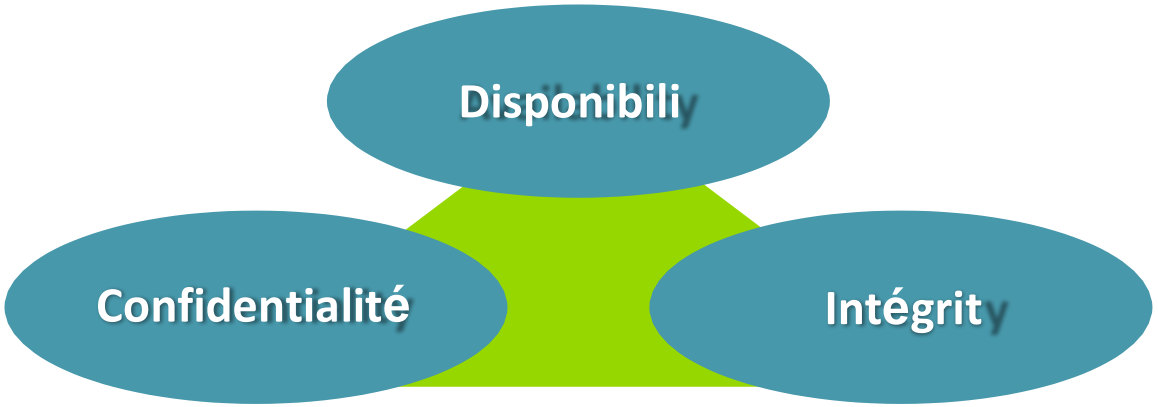
- Les **dommages collatéraux** causés par une attaque peuvent être aussi graves, voire pires, que l'attaque elle-même.

- **Les attaques DDoS affectent la disponibilité** ! Sans disponibilité, pas d'applications/services/données/Internet ! Pas de revenus !

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

ARBOR NETWORKS

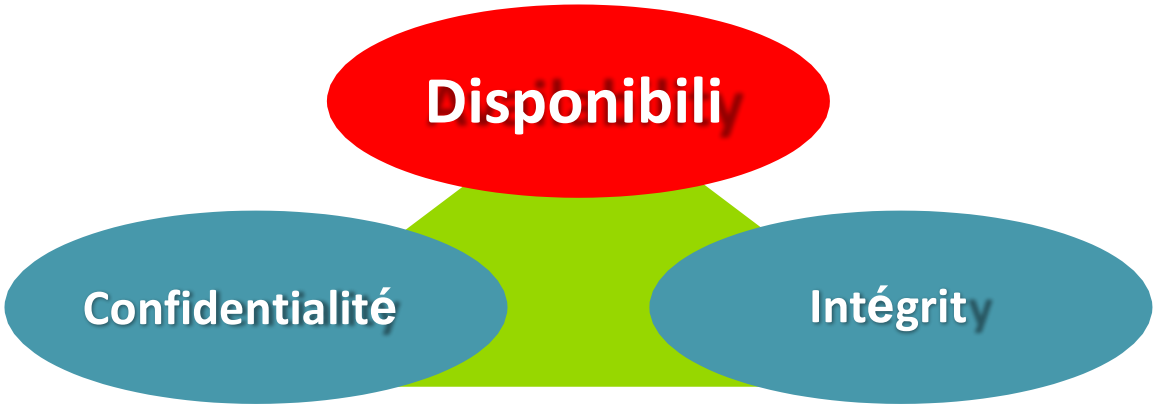
Trois attributs de sécurité



- L'objectif de la sécurité est de maintenir ces trois attributs.

ARBOR NETWORKS

Trois attributs de sécurité



- L'objectif principal de la défense contre les DDoS est de maintenir la disponibilité face aux attaques.

ARBOR NETWORKS

La quasi-totalité des dépenses et des efforts en matière de sécurité sont axés sur la confidentialité et l'intégrité.

- La confidentialité et l'intégrité sont des concepts relativement simples, faciles à comprendre pour les non-spécialistes.
- Dans la pratique, la confidentialité et l'intégrité équivalent à peu près au cryptage, ce qui est facile à comprendre pour les non-spécialistes.
- En réalité, ils ne se limitent pas au cryptage, mais il est facile de crier victoire : "Nous avons un antivirus, nous avons le cryptage des disques, nous sommes conformes aux normes PCI, woo- hoo ! "
- Et pourtant, des centaines de millions d'hôtes infectés par des robots, des réseaux d'entreprises de toutes tailles et de tous secteurs ont été complètement pénétrés, la propriété intellectuelle a été volée, des secrets militaires ont été divulgués, etc.
- La disponibilité ne peut pas être modifiée - le serveur Web, le serveur DNS et le PBX VoIP sont soit en service, soit hors service. Il n'y a aucun moyen d'obscurcir, d'exagérer ou de tergiverser en ce qui concerne la posture de sécurité réelle, dans le monde réel.
- La disponibilité exige des praticiens de la sécurité opérationnelle (opsec) qui comprennent le TCP/IP et le routage/commutation ; qui comprennent les serveurs Web ; qui comprennent les serveurs DNS ; qui comprennent la sécurité ; qui comprennent la couche 7.
- Ces personnes sont rares et ne sont pas bon marché. La plupart des organisations ne connaissent même pas les compétences requises et l'étendue de l'expérience à rechercher afin d'identifier et d'engager les bonnes personnes.

ARBOR NETWORKS

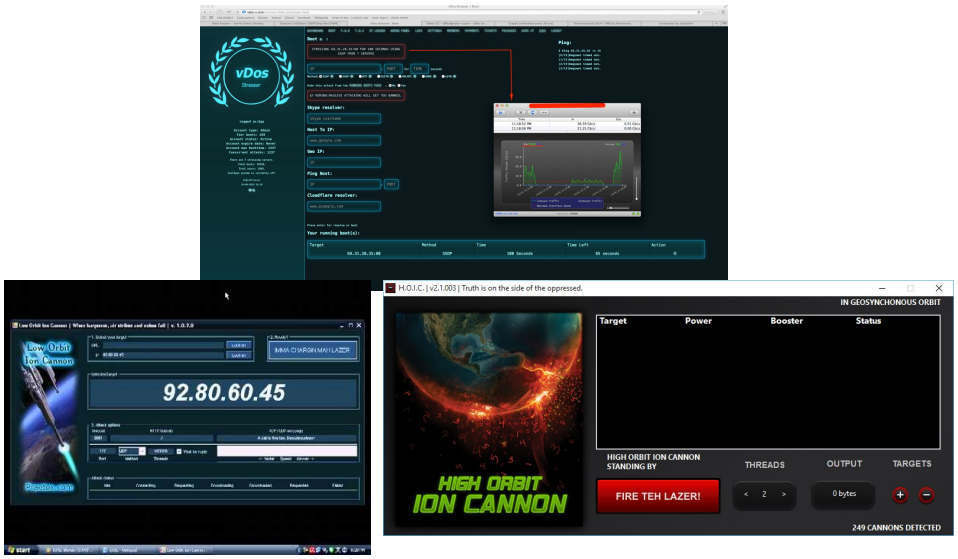
La disponibilité est difficile !

- Le maintien de la disponibilité face à une attaque nécessite une combinaison de compétences, d'architecture, d'agilité opérationnelle, de capacités d'analyse et d'atténuation que la plupart des organisations ne possèdent tout simplement pas.
- En pratique, la plupart des organisations ne tiennent jamais compte de la disponibilité lorsqu'elles conçoivent/spécifient/construisent/déploient/testent des applications/services/propriétés en ligne.
- Dans la pratique, la plupart des organisations ne font jamais le lien logique entre le maintien de la disponibilité et la continuité des activités.
- Dans la pratique, la plupart des organisations ne soumettent jamais leurs piles d'applications/services à des tests de stress afin de déterminer les lacunes en matière d'évolutivité/résilience et de les corriger.
- En pratique, la plupart des organisations n'ont pas de plan d'atténuation des DDoS.

ARBOR NETWORKS

L'armement des DDoS

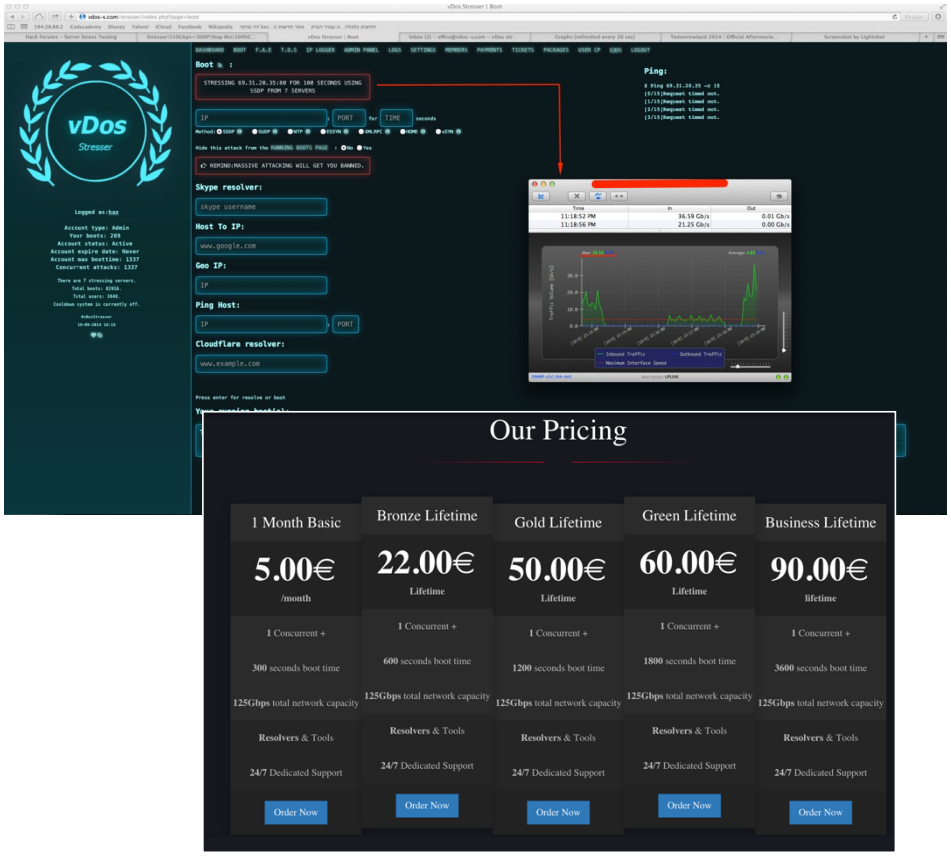
"Weaponize" : *convertir pour utiliser comme une arme / simplifier l'utilisation comme une arme.*



- Disponibilité accrue de "Stresser Tools"/"Booters" qui réalisent des attaques hautement distribuées en utilisant une combinaison d'attaques d'amplification avec ou sans spoofing. Ils sont souvent liés à des fermes à robots.
- Développement d'outils destinés à être utilisés par des attaquants ayant choisi de participer volontairement :
  - Canon à ions en orbite basse utilisé pour effectuer des attaques UDP/ICMP non dissimulées.
  - Le canon ionique à haute orbite envoie des requêtes HTTP non usurpées contre plusieurs sites.

ARBOR NETWORKS

Des outils DDoS pour les masses

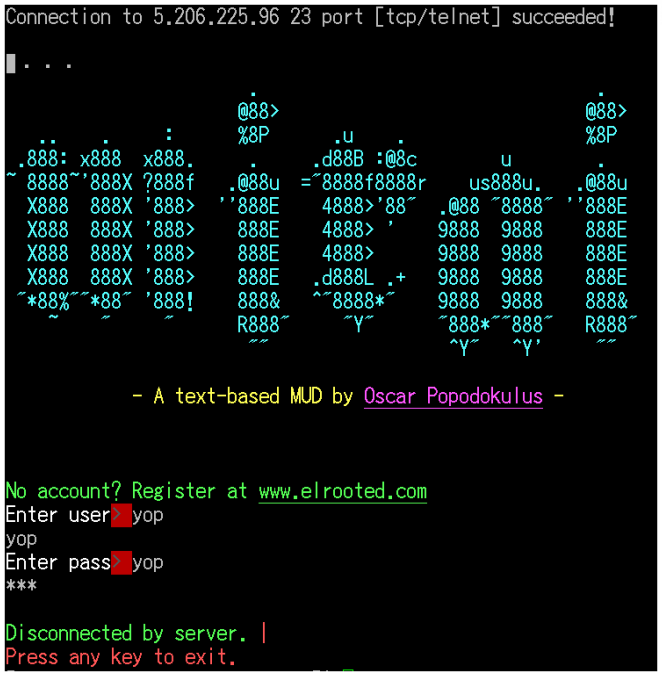


- Quiconque a la possibilité de cliquer sur un bouton peut désormais lancer une attaque DDoS.
- Bon marché et simple à utiliser :
  - Comptes VIP !
  - Abonnement à vie !
  - Un support client 24x7 !
- Principalement utilisés par les joueurs qui s'attaquent les uns aux autres, ils ont récemment été utilisés pour attaquer des cibles très visibles.

ARBOR NETWORKS

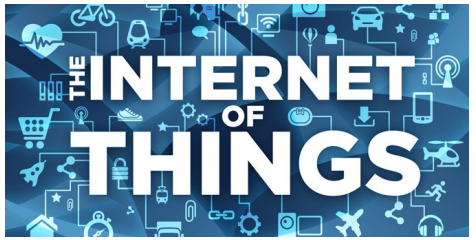
La situation de l'IdO

L'INTERNET DES OBJETS



ARBOR NETWORKS

L'internet des objets (IoT)



Wikipedia : *L'internet des objets (IoT) est le réseau d'appareils physiques, de véhicules, de bâtiments et d'autres objets - dotés d'électronique, de logiciels, de capteurs et de connectivité réseau - qui permet à ces objets de collecter et d'échanger des données.*

Mais s'agit-il de quelque chose de nouveau ou simplement de marketing

- Par exemple, la "cafetière de la chambre de Troie" a été connectée à Internet en 1993.

Définition plus précise : *Un dispositif IoT (dispositif intégré) est essentiellement un ordinateur doté d'une unité centrale, d'une mémoire, d'un logiciel et d'un ensemble d'interfaces qui sont dédiés à des rôles ou des tâches spécifiques.*

NOMS D'UTILISATEUR ET MOTS DE PASSE PAR DÉFAUT !!!

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:W1phozQZURUJ: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
```

Sécurité de l'IOT (ou son absence)

Les problèmes de sécurité de l'IdO :

- Les dispositifs IoT ont généralement des capacités embarquées limitées et nécessitent souvent une configuration et un contrôle externes.
- Beaucoup de ces piles de dispositifs ne sont pas correctement sécurisées :
  - Noms d'utilisateur/mots de passe codés en dur
  - Services inutiles activés par défaut (Chargen, SSDP, DNS forwarder)
  - Interfaces de gestion non sécurisées (Web, SNMP, TR-069 et autres)
  - Capacités limitées ou inexistantes de mise à jour du logiciel
  - Très peu de correctifs ou de mises à jour après le déploiement
- Billion. Le nombre de dispositifs IoT en 2020 est estimé à environ 20-30Billion Cependant, plus de 6 milliards de dispositifs sont déjà en ligne et 5,5 millions sont ajoutés chaque jour1.

ARBOR NETWORKS

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

Des millions de dispositifs IoT vulnérables + Armement = ?

Botnets IoT !

L'histoire des botnets IoT

Les botnets IoT ne sont en fait pas nouveaux :

- Le premier botnet a été créé en 1993 lorsque Robey Pointer a créé un bot IRC (Internet Relay Chat) appelé "eggbot" qui était utilisé pour défendre les canaux IRC en lançant des attaques par inondation contre les utilisateurs indésirables. Le bot était également utilisé pour attaquer d'autres canaux en utilisant les protocoles CTCP et DCC. Plusieurs instances du bot pouvaient unir leurs efforts et travailler ensemble dans des "botnets".
- En 2003, la première attaque DDoS (non intentionnelle) contre l'université du Wisconsin à l'aide de dispositifs IoT a eu lieu à cause d'une adresse NTP codée en dur dans 700 000 modems DSL/câble Netgear. Même après la sortie d'un nouveau logiciel, l'attaque s'est poursuivie pendant des années, jusqu'à ce que le dernier appareil soit mis à la poubelle.
- En 2008, la première attaque DDoS par botnet IoT enregistrée a été réalisée à l'aide d'un botnet de routeurs à large bande CPE basés sur Linux.
- In 2012, an unknown researcher published a report called the “Internet census of 2012”. Les données utilisées dans le rapport ont été recueillies en piratant environ 420 000 dispositifs CPE dans le monde entier à l'aide d'informations d'identification In 2012, an unknown researcher published a report called the “Internet census of 2012”. par défaut1.

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

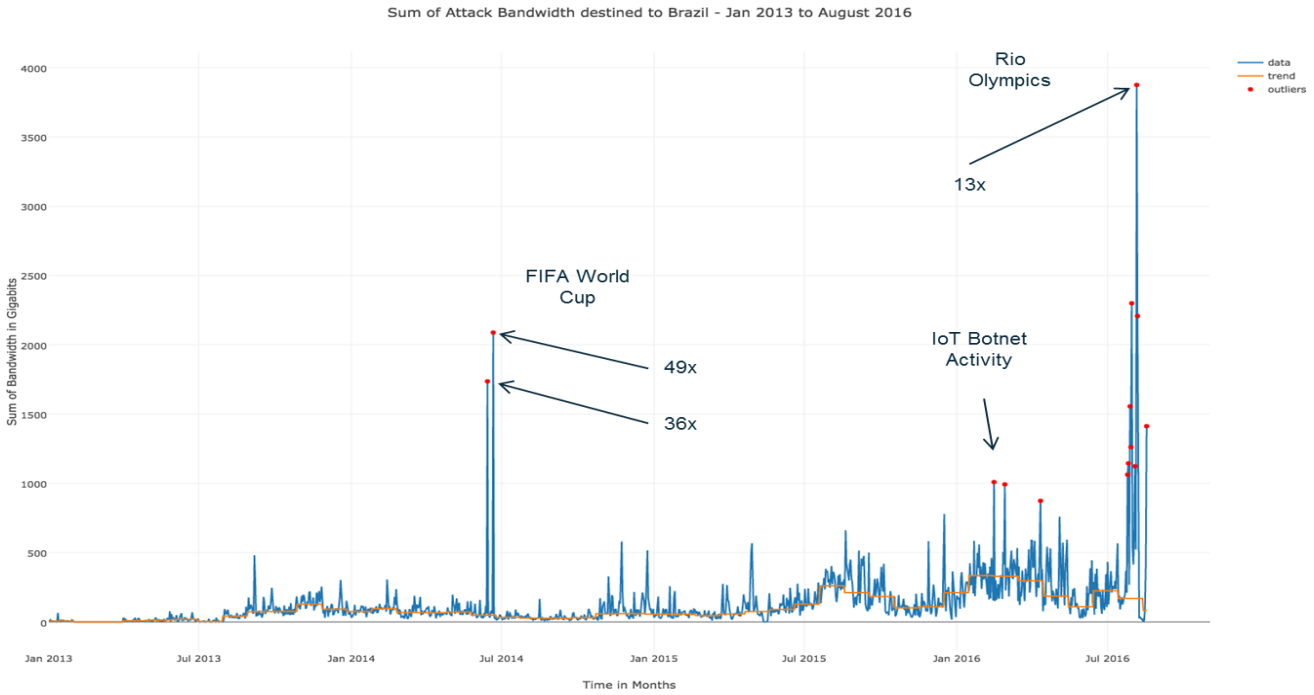
Situation actuelle des botnets IoT

Les botnets IoT ont maintenant été militarisés et sont disponibles via des services de booter/stresser :

- Un botnet IoT utilisant le code Lizardstresser a été utilisé pour attaquer des sites au Brésil en 2016, avec des volumes d'attaque atteignant 400gb/sec.
- Le même botnet, composé d'environ 10 000 webcams, a été utilisé pour lancer des attaques soutenues de 540gb/sec contre des organisations affiliées aux Jeux olympiques au cours de l'été 2016.
- Un botnet IoT basé sur la base de code Mirai a été utilisé dans les attaques DDoS réalisées en novembre 2016 contre le journaliste spécialisé dans la sécurité Brian Krebs, qui ont culminé à 620gb/sec.
- Des botnets IoT utilisant le code Mirai ont été utilisés dans les attaques contre le fournisseur de DNS faisant autorité Dyn en novembre 2016.

Le code source des bots LizardStresser et Mirai a été diffusé dans la nature et a donné naissance à de multiples nouvelles variantes.

Le bot LizzardStresser attaque le Brésil



- Des attaques ont été lancées non seulement contre l'infrastructure des événements sportifs, mais aussi contre les sponsors associés et les institutions financières et gouvernementales.

ARBOR NETWORKS

Lutte contre les botnets IoT

Vecteurs d'infection des botnets IoT - exemple de Mirai

1. Un dispositif compromis créera un fil d'analyse séparé pour rechercher d'autres dispositifs sur les ports TCP 23, 2323, 23231, 37777 et 7547 (+5555) (interface SOAP TR- 069/TR-064) en utilisant des IP aléatoires.
2. Si un appareil répond, une tentative de connexion sera effectuée à l'aide d'un ensemble de combinaisons nom d'utilisateur/mot de passe courantes.
3. En cas de succès, l'adresse IP de l'appareil vulnérable est envoyée au serveur C&C.
4. Le serveur C&C se connectera à l'appareil, téléchargera le malware approprié et compromettra l'appareil. L'appareil va maintenant commencer à scanner, allez au numéro 1.

- Dans l'état actuel des choses, un appareil vulnérable sera infecté **quelques minutes** après avoir été connecté à Internet.
- Les appareils vulnérables proviennent principalement de 3 fabricants en Chine, l'un d'entre eux a publié un patch en 2014 mais uniquement pour la version anglaise de son SW.

LE BOTNET MIRAI

Environ 500 000 appareils dans le monde

- De fortes concentrations en Chine, à Hong Kong, à Macao, au Vietnam, à Taiwan, en Corée du Sud, en Thaïlande, en Indonésie, au Brésil et en Espagne.

Le même logiciel malveillant de botnet utilisé dans les attaques de Krebs, OVH Dyn et Liberia.

- Cela n'implique pas qu'il s'agissait des mêmes adversaires.

Multiples vecteurs d'attaque DDoS possibles

Au moins une variante a été vermifugée !

Capacités d'attaque DDoS d'un botnet IoT - Mirai

Mise à jour flash du 15 décembre 2016
Une nouvelle variante de Mirai a été observée dans la nature, émettant du trafic usurpé. Les attaques comprennent des inondations SYN-, des attaques de réflexion/amplification DNS et des attaques d'amplification de réflexion TCP.

Types d'attaques :

- inondation UDP
- Inondation du moteur d'origine des soupapes
- Inondation TCP ACK
- Attaque TCP "Stomp" (inondation ACK sur une connexion TCP établie, conçue pour contourner les dispositifs d'atténuation DDoS)
- Inondation TCP SYN
- Inondation de paquets GRE
- Inondation des requêtes HTTP (GET, POST, HEAD)
- Préparation pseudo-aléatoire des étiquettes DNS ("DNS Water Torture")

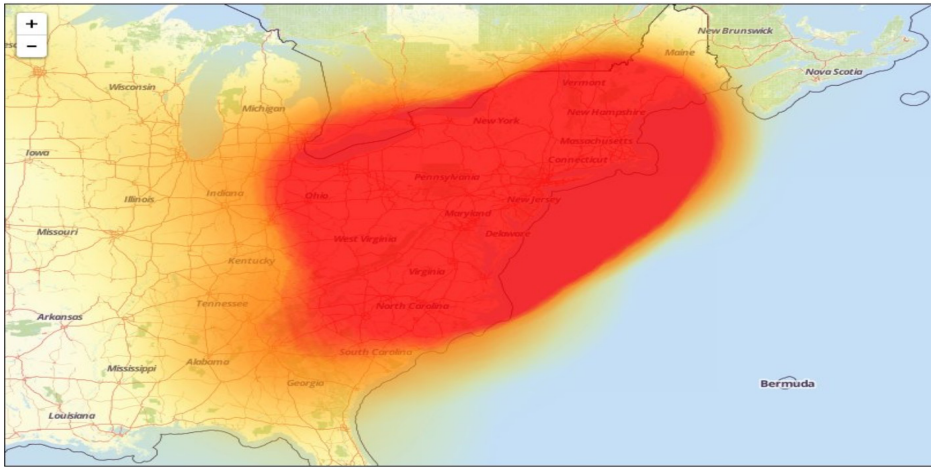
Le logiciel malveillant Mirai s'exécute dans l'espace utilisateur et n'a pas, jusqu'à présent, utilisé d'adresses IP usurpées, ce qui lui interdit d'effectuer des attaques par usurpation et par réflexion.

DYN ATTACKS ON OCTOBER 21st

Trois attaques visant l'infrastructure DNS gérée de Dyn
Les clients de Dyn comprennent

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

Ces attaques ont entraîné des pannes à grande échelle pour les clients de Dyn, même si ces derniers n'ont pas été attaqués directement.



ARBOR NETWORKS

CHRONOLOGIE DE L'ATTAQUE DYN

Attaque 1
Début : 11:10 UTC

Durée : 2 heures et 20 minutes

Attaque 2
Début : 15:50 UTC

Durée : 1 heure et 10 minutes

Attaque 3
Atténuation dès le départ

Destinations : APAC, Amérique du Sud, Europe de l'Est, US-West, US-East
Les pannes étaient régionales

ARBOR NETWORKS

Comprendre et atténuer les attaques

Vecteurs d'attaque multiples et hautement distribués
Dyn a d'abord signalé "des dizaines de millions d'adresses IP".

Plus tard corrigée à une estimation de 100.000

Effet de cascade
La perturbation du service DNS due à l'attaque originale génère une activité de réessai légitime.

C'est ce qui a poussé Dyn à surévaluer le nombre d'adresses IP attaquantes.

Atténuations :

ACLs, S/RTBH, flowspec, IDMS

ARBOR NETWORKS

ATTAQUES AU LIB LIB LIB LIB LIB LIB LIB LIB DÉBUT DÉBUT 31 OCTOBRE

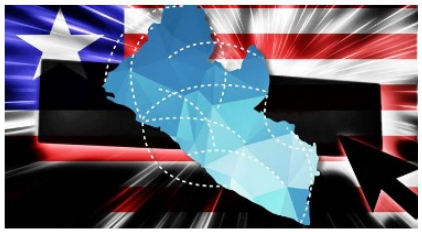
SC Magazine US > News > Analysts mixed on reason for Liberia Mirai attack

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.

AI NETWORKS

Atténuation des attaques DDoS du botnet IoT

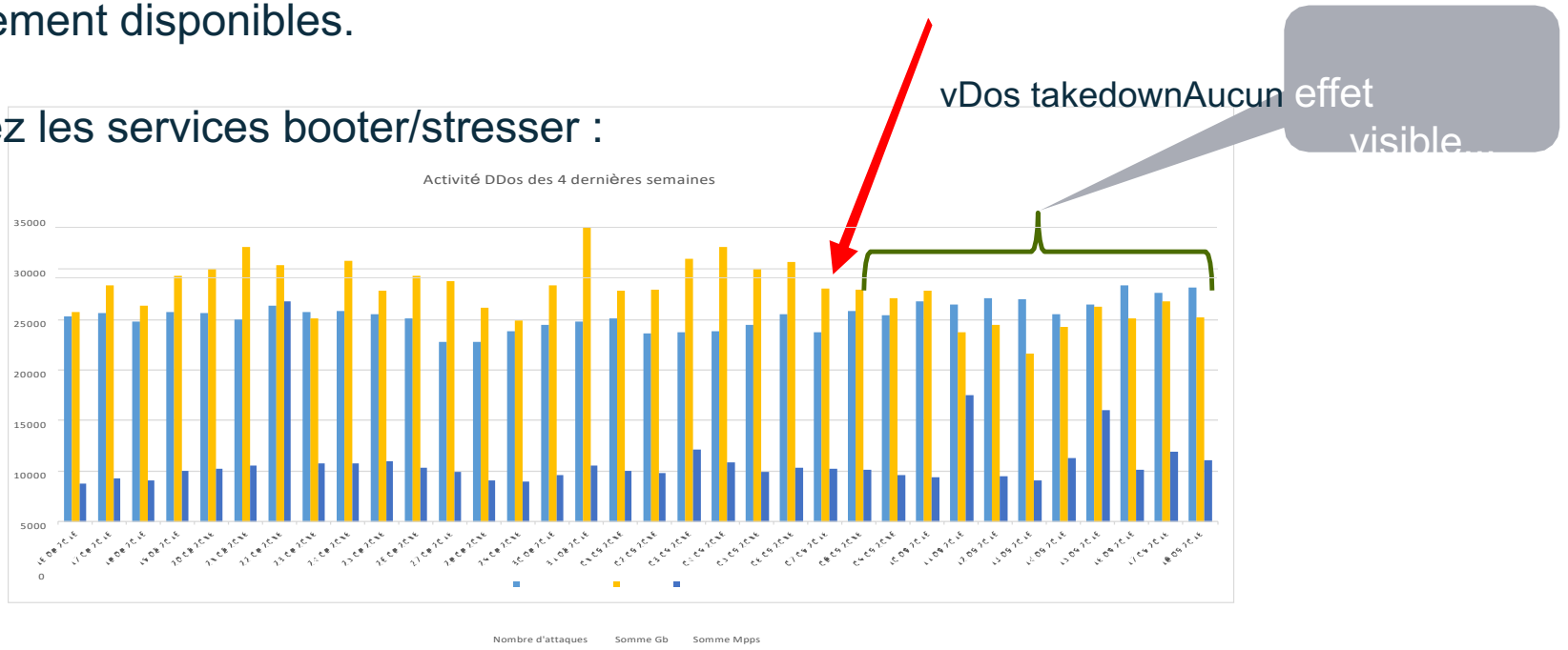
Les botnets IoT n'ont rien de nouveau et les attaques utilisées n'ont rien de nouveau non plus. Les mêmes approches d'atténuation des attaques DDoS s'appliquent toujours !

- Mettre en œuvre les meilleures pratiques actuelles (BCP's) pour l'infrastructure, les hôtes/applications/services et les serveurs DNS. Il s'agit notamment de spécifier les politiques d'accès au réseau pour les types de serveurs courants.
- Utiliser la télémétrie des flux pour détecter, classer et retracer le trafic DDoS.
- Utilisez S/RTBH, flowspec, des solutions intelligentes d'atténuation des DDoS (IDMS) pour atténuer les attaques.
- Planifiez et entraînez-vous à faire face aux attaques DDoS.

Comment réduire la menace des botnets IoT ?

Les botnets IoT sont populaires aujourd'hui car les appareils IoT sont vulnérables et les outils pour les infecter et les subvertir à des fins d'attaques sont facilement disponibles.

1. Arrêtez les services booter/stresser :



Comment réduire la menace des botnets IoT (suite)

2. Arrêtez de vendre et de déployer des dispositifs IoT vulnérables :
   - Qui va faire appliquer cette loi ?
   - Qui va payer pour cela ?
   - Les gens se soucient-ils du fait que leur webcam attaque quelqu'un d'autre ?

3. Corrigez les dispositifs IoT vulnérables :
   - Quand avez-vous mis à niveau votre dispositif CPE pour la dernière fois ? Télévision intelligente ? Votre cafetière ? Vos ampoules intelligentes ?
   - Les routeurs Netgear qui attaquaient l'université du Wisconsin n'ont JAMAIS été corrigés et l'attaque n'a cessé que lorsque le dernier appareil a été jeté à la poubelle.

4. Si les dispositifs IoT ne peuvent pas être réparés (ou faire confiance), isolez-les d'Internet et créez des barrières !

Exemple de la façon d'isoler les dispositifs IoT - le réseau domestique de Steinthor !

En 2011, Steinthor connected 3 IP Web Cams to his home network. ces appareils communiquent avec un NAS Synology qui fournit un portail vidéo et stocke tous les enregistrements vidéo.

Le réseau est segmenté en 2 zones :

- VLAN utilisateur
- Sous-réseau vidéo où un (vieux) Cisco ASA 5505 contrôle toutes les communications entre les webcams et le NAS.

VideoCameras (5 incoming rules)

1	☑	any	SynologyNAS	ip	Permit	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

Le VPN L3 est utilisé pour permettre l'accès à distance au portail de la webcam fonctionnant sur le Synology.

1) Voir aussi http://robert.penz.name/1341/ready-your-home-network-for-iot/

Quelle est la prochaine étape ?

Quelle est la prochaine étape ?

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	1	hGz3p9773	1	lVKN5o4792	1	Q5yeRg1199	1	sEYrYO0	1	s6udvo1201
2	NEWdMf773	2	fDyRFB4792	2	0C0Z9L1199	2	zq9Tyo0	2	Cn4R3Y1201	2	L7MbXd4808
3	nAwk4f4792	3	2DxRlK1199	3	AuKUG00	3	9Quiam1201	3	VCAg4G4808	3	3bvZ2e827
4	HcB4Qs1199	4	LyJ59Q0	4	g28cfK1201	4	SgtyKo4808	4	ogVNVQ827	4	7Lhs4l9264
5	hdiQl80	5	bDNPUL1201	5	zbKby54808	5	BBrc1u827	5	fXClL49264	5	k6MTRC125
6	Irl0bG1201	6	GR6Y0e4808	6	OjkvHG827	6	zla2ot9264	6	HxxjEv125	6	8aWgfy3416
7	FKLw0j4808	7	7lj6yy827	7	zgmlOO9264	7	hgJ9hA125	7	z3W1cr3416	7	G88v639143
8	nGtzCB827	8	xn2uyV9264	8	f7m2mH125	8	5u291A3416	8	SQdqja9143	8	gC1L7c7312
9	eEo3T59264	9	u7uUQh125	9	yUSxLs3416	9	jTDUSC9143	9	461WuM7312	9	W4DDYM7929
10	Q0WbaW9136	10	UA10mR773	10	lAHSge4792	10	xbvwZo1199	10	YjTJ6N0	10	t5hkC31201
11	XgQ6xl773	11	Snqh6u4792	11	Lr1zBn1199	11	R7SzfG0	11	StkbAJ1201	11	tMwcc54808
12	4gv8me4792	12	KJ2ZQJ1199	12	yGBiVQ0	12	7oQTzk1201	12	pmieOL4808	12	XiFigk827
13	lluKNB1199	13	aF0lvv0	13	hUNJPK1201	13	MUuie34808	13	sloanv827	13	FyPZsK9264
14	xePfVg0	14	0Wenhi1201	14	K6VMzn4808	14	00JZUo827	14	40Qbtk9264	14	U0Tu8U125
15	9EhuEg1201	15	ao1SyT4808	15	pfDRXS827	15	WTnOip9264	15	1UDPr5125	15	HV38sg3416
16	8UTjLW4808	16	JlOdAl827	16	2hyMU39264	16	ShaEtt125	16	6ot6RO3416	16	G9vOqh9143
17	Q1rm8O827	17	ijyw6A9264	17	jNBLAL125	17	V5O52Y3416	17	LmKVnJ9143	17	pleWQA7312
18	tuJjLc9264	18	KFQ9jX125	18	u87vdt3416	18	ZhnWO29143	18	VjH2sG7312	18	j2xFTC7929
19	KCHQN6125	19	L9ZAuy3416	19	0UPVab9143	19	gWQZRu7312	19	B5u2JZ7929	19	Guo3ui1000
20	l4iuaN773	20	Yz8KUc4792	20	Dq62je1199	20	Kw47Bv0	20	Fu55LG1201	20	jluOx54808
21	A32uFl4792	21	cTRiX81199	21	bO5KeD0	21	CISW201201	21	vUrT844808	21	xfLkDe827
22	QGT2Va1199	22	4CJmnz0	22	oWBhP11201	22	jsafKF4808	22	FWQ9Kg827	22	c8dmJm9264
23	zaRezi0	23	VqlQwB1201	23	29ksvt4808	23	pw5Z6R827	23	T6TwM49264	23	wwWlrr125
24	fiSajA1201	24	cblgGR4808	24	n9gTZa827	24	FN2RCM9264	24	RXPxrK125	24	1kvRVX3416

Quelle est la prochaine étape ?

De très nombreuses autres catégories d'appareils "IoT" de qualité grand public - ampoules, thermostats, "compteurs intelligents", etc.

De grands routeurs de classe opérateur et d'entreprise ont déjà été compromis, utilisés pour des attaques DDoS par inondation ICMP, le détournement de route pour DDoS et pour le spam (cisco/cisco creds, même pour les routeurs Juniper).

Scanner/compromettre en plusieurs étapes des dispositifs IoT *derrière des* NATs/firewalls !

Maintenant, nous avons NETCONF, et diverses API SDN . . .et la possibilité d'exécuter un code arbitraire sur les routeurs eux-mêmes.

Les PCA d'infrastructure de réseau sont plus importants que jamais !

Tous les routeurs sont des appareils intégrés à l'IdO, même les plus gros ! Les smartphones aussi !

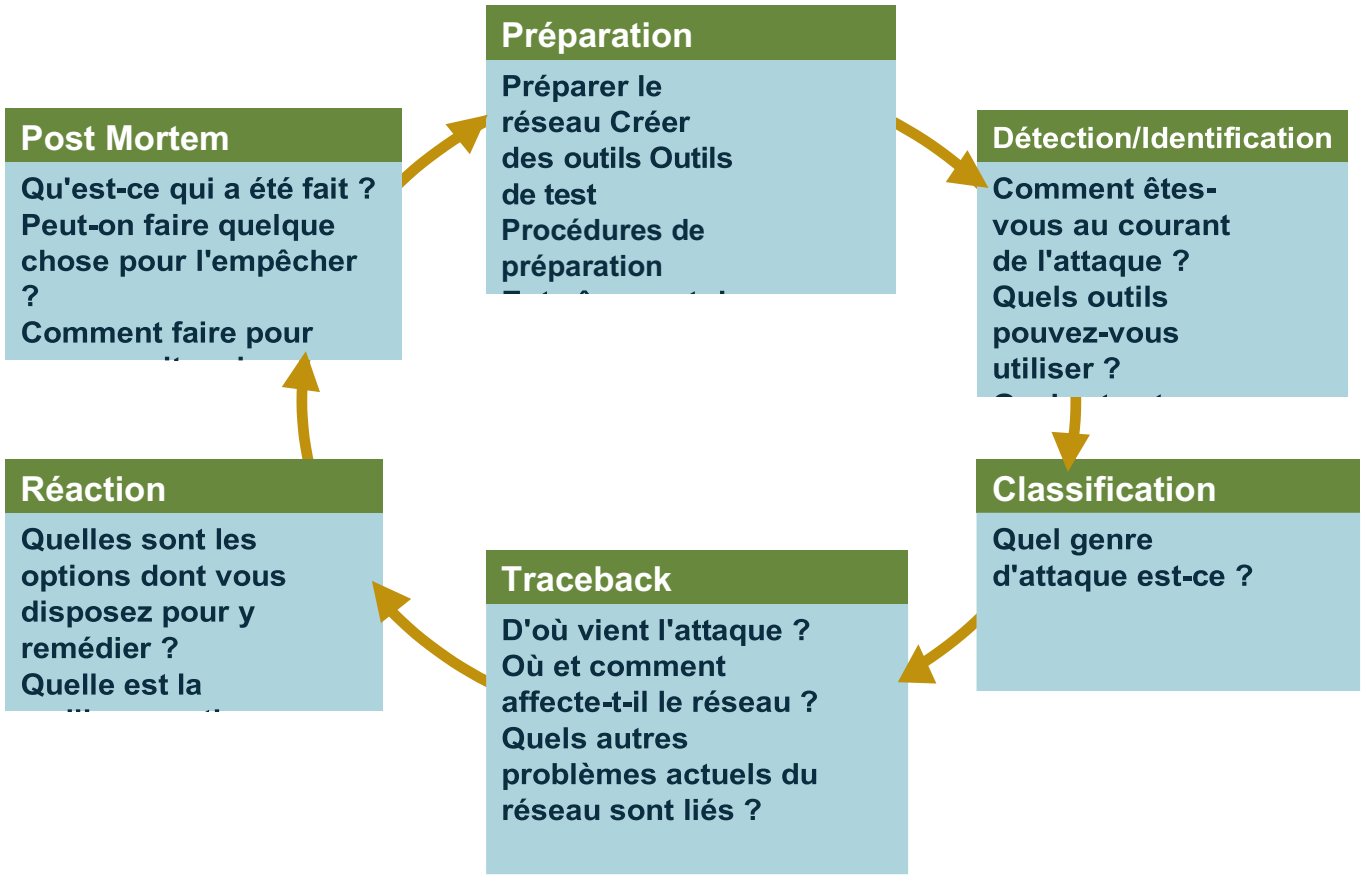
Que pouvons-nous faire ?

Disponibilité des réseaux et des applications : Protéger l'infrastructure

- La sécurité est au cœur de l'avenir de l'interréseautage ; nous sommes passés d'un internet de confiance implicite à un internet de méfiance généralisée.
- Aucun paquet n'est fiable ; tous les paquets doivent mériter cette confiance grâce à la capacité d'un périphérique réseau à inspecter et à appliquer la politique.
- La protection de l'infrastructure est l'exigence de sécurité la plus fondamentale.
- La protection de l'infrastructure doit être incluse dans toutes les conceptions de haute disponibilité.
- Une infrastructure sécurisée constitue la base d'une prestation de services continue.

ARBOR® NETWORKS

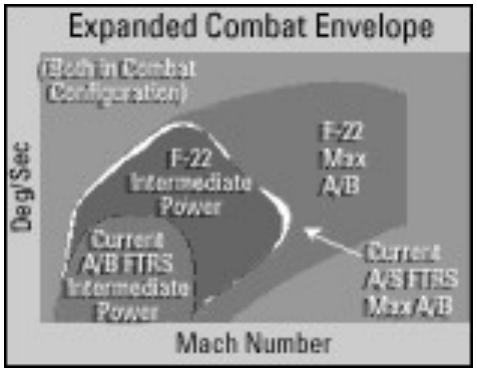
Les six phases de la réponse aux incidents

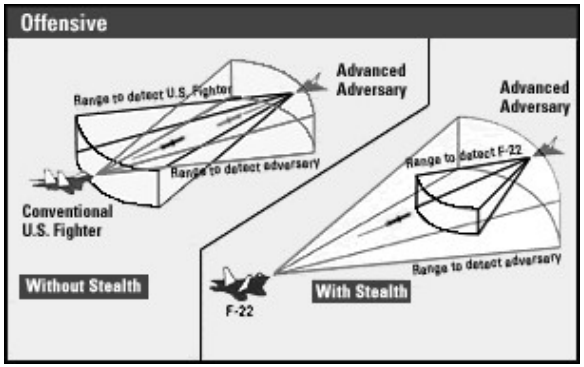


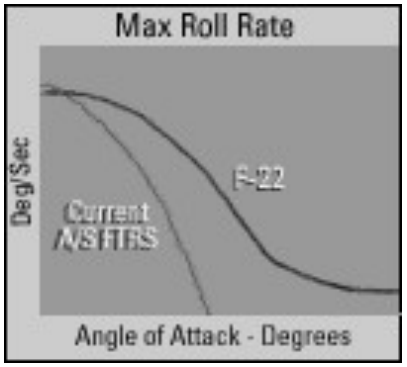
REPOUSSEZ-VOUS LES LIMITES ?

Connaissez votre équipement et votre infrastructure !

- Connaissez l'enveloppe de performance de tous vos équipements (routeurs, commutateurs, serveurs, etc.). Vous devez savoir ce que votre équipement est réellement capable de faire !
- Connaissez les capacités de votre réseau. Si possible, testez-le. Les surprises ne sont pas amusantes lors d'un incident de sécurité.
- pps vs. bps vs. qps vs. cps vs. tps - et comment l'activation des fonctionnalités les influence







ARBOR NETWORKS

Architecture

Les bons outils pour le bon travail

Les bonnes personnes pour le bon travail

Compétences requises pour l'équipe OPSEC

L'équipe OPSEC doit savoir :
Tout ce que sait un ingénieur Backbone

Tout ce qu'un ingénieur en gestion de réseau sait

Tout ce qu'un administrateur de

système/webmaster sait Tout ce qu'un

administrateur de courrier électronique sait

Tout ce qu'un ingénieur DNS/DHCP/Adressing sait Tout

ce qu'un ingénieur CERT sait

Tout ce que sait un spécialiste de l'Infosec d'entreprise

En substance, vous recherchez des super-ingénieurs qui sont des ingénieurs hybrides Backbone/Sécurité.

ARBOR NETWORKS

Meilleures pratiques actuelles en matière d'infrastructure (BCP)

- Des listes de contrôle d'accès d'interface (iACL) doivent être utilisées aux extrémités pertinentes du réseau (homologue/transit, périphérie d'agrégation des clients, etc.) pour protéger l'infrastructure du réseau elle-même ; des sections supplémentaires spécifiques aux services doivent être utilisées pour limiter le trafic destiné aux serveurs faisant face à l'Internet aux ports et protocoles associés aux services et applications sur ces serveurs.
- L'utilisation du protocole GRE (IP Protocol 47) dans ces attaques est remarquable car il s'agit d'un mécanisme commun utilisé par les attaquants pour contourner les listes de contrôle d'accès qui ne contiennent que des déclarations de politique relatives aux protocoles courants tels que TCP, UDP et ICMP ; il existe 254 protocoles Internet valides et les protocoles non pertinents doivent être filtrés aux extrémités par des listes de contrôle d'accès.
- Des PCA supplémentaires pour l'infrastructure du réseau, tels que les mécanismes d'autoprotection des plans de contrôle et de gestion (rACL, CoPP, GTSM, clé MD5, etc.), doivent également être déployés.
- Tous les dispositifs de l'infrastructure du réseau doivent être accessibles uniquement via des hôtes de gestion désignés, et cet accès doit être facilité par un réseau de gestion hors bande (OOB) dédié. Lors d'attaques DDoS à fort impact, un réseau de gestion dédié garantit que les dispositifs peuvent être gérés indépendamment des conditions sur le réseau de production, et garantit également que les mécanismes vitaux tels que la télémétrie des flux et le SNMP ne sont pas interrompus, ce qui assure une visibilité continue du trafic d'attaque pendant un incident.

PCA d'infrastructure

- La télémétrie des flux, comme Cisco NetFlow, Juniper cflowd et sFlow, doit être activée à toutes les extrémités du réseau et exportée vers un système de collecte et d'analyse.

- Le "Source-based remotely-triggered blackholing" (S/RTBH) est une technique de réaction puissante qui permet à des dizaines, voire des centaines de milliers d'adresses IP sources d'attaques (classées par l'analyse des flux, les fichiers journaux, etc.) d'être rapidement blackholées en fonction de leur adresse source. S/RTBH utilise BGP comme mécanisme du plan de contrôle pour signaler instantanément aux périphériques de commencer à abandonner le trafic d'attaque. Flowspec permet une granularité de couche 4 - déploiement instantané des ACL via BGP !

- Les systèmes intelligents d'atténuation des attaques DDoS (IDMS) doivent être déployés dans des centres de nettoyage adaptés sur le plan topologique afin de protéger les serveurs/services/applications. Ils devraient être placés au nord des équilibreurs de charge ; si une organisation insiste pour placer des pare-feu et des IDS/'IPS' en ligne devant les serveurs, protégez ces points d'étranglement DDoS étatiques et tout ce qui se trouve derrière eux !

- Ne placez pas de pare-feu et d'IDS/'IPS' devant les serveurs - ils n'apportent aucune valeur de sécurité dans les environnements de serveurs où chaque connexion entrante est par définition non sollicitée. Ce sont des points d'étranglement DDoS et ils dégradent la posture de sécurité opérationnelle du réseau et des applications.
- La politique devrait être appliquée par des ACL sans état dans les routeurs/commutateurs basés sur le matériel .

ARBOR NETWORKS

Accueillir les meilleures pratiques

- Les serveurs faisant face au public doivent être configurés de manière renforcée, avec des services inutiles désactivés, un accès de gestion OOB, un renforcement de la configuration spécifique au service, un réglage de la pile IP et d'autres mécanismes pertinents.

- Le filtrage apatride sur serveur via tcpwrappers est un mécanisme utile de mise en œuvre des politiques ; pour les serveurs Web, les modules Apache tels que mod_security et mod_evasive apportent des capacités supplémentaires.

- Le déploiement de pare-feu à état ou d'autres dispositifs d'inspection tels que les IDS/IPS devant les serveurs tournés vers l'Internet est contre-indiqué ; comme chaque connexion entrante vers les serveurs tournés vers l'Internet est par définition non sollicitée, l'inspection à état n'ajoute rien à la posture de sécurité des serveurs et sert à affaiblir leur capacité à résister au trafic DDoS en raison de la taille limitée des tables d'état des pare-feu et des IDS/IPS les plus grands/rapides sur le marché aujourd'hui.
  Au cours de ces attaques et de nombreuses autres, il a été observé que les pare-feu situés devant les serveurs ciblés tombaient en panne alors qu'ils recevaient des quantités relativement faibles de trafic d'attaque, ce qui permettait aux DDoS de réussir à rendre les serveurs indisponibles sans grand effort attaquant.

PCA de l'hôte

- Les équilibreurs de charge instancient également un état qui rend les serveurs réels derrière les équilibreurs de charge plus vulnérables aux attaques DDoS ; au cours de ces attaques, on a observé que les équilibreurs de charge échouaient en raison de l'épuisement de l'état dû au trafic d'attaque. S/RTBH, flowspec, reverse-proxy caches, & IDMS devraient être utilisés pour protéger l'équilibreur de charge et les serveurs réels derrière lui.

- L'infrastructure DNS doit être déployée dans une architecture modulaire et cloisonnée, avec une séparation des fonctions telles que les serveurs faisant autorité, les résolveurs internes, les résolveurs externes, les résolveurs en cache uniquement, etc., et doit être mise à l'échelle de manière appropriée en utilisant des techniques telles que l'adressage anycast IPv4. Flowspec, S/RTBH, les mécanismes d'autodéfense des serveurs DNS tels que RRL et IDMS devraient être utilisés pour protéger le DNS contre les attaques délibérées et/ou les dommages collatéraux.

Sommes-nous condamnés ?

- ***Non ! Le*** déploiement d'outils/techniques/BCP existants et bien connus permet d'améliorer considérablement la sécurité et d'obtenir des résultats mesurables.
- L'évolution des défenses contre ces attaques montre qu'un changement positif est possible - les organisations ciblées et les ISP/MSSP qui les défendent ont modifié leurs architectures, leurs techniques d'atténuation, leurs processus et leurs procédures afin d'atténuer ces attaques avec succès.
- Les capacités d'atténuation s'adaptent pour répondre et dépasser les volumes d'attaques - l'architecture de déploiement, la bande passante de déviation/réinjection, l'exploitation de l'infrastructure de réseau sont essentielles.
- L'automatisation est une bonne chose, mais elle ne remplace pas une architecture résiliente, une planification perspicace et un personnel de sécurité opérationnelle intelligent, qui sont plus importants que jamais !

ARBOR NETWORKS

Résumé

- La situation actuelle est similaire à celle de l'époque où Windows XP était le système d'exploitation le plus utilisé : beaucoup de dispositifs vulnérables et peu de moyens de défense contre les compromis. Le problème a été résolu par la sortie de logiciels plus résistants et, progressivement, le nombre de dispositifs vulnérables a diminué. Cependant, nous avons toujours des ordinateurs Windows XP vulnérables connectés à Internet  ... et maintenant nous avons des ordres de grandeur de dispositifs IoT plus vulnérables !
- Les bots deviennent de plus en plus intelligents et disposent de capacités plus avancées. Le bot Medusa, basé sur Windows, génère des threads de navigateur IE pour réaliser des attaques HTTP et HTTP/S avancées. Il faut plus d'intelligence pour faire face à ces attaques - et nous l'avons !
- Les défenses doivent être mises en place ***avant que*** les attaques ***ne*** se produisent !
- Une défense DDoS réussie contre les attaques à haute capacité et à haute complexité a lieu ***tous les jours*** !
- ***Nous savons comment faire !***

Merci !

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

ARBOR NETWORKS
The Security Division of NETSCOUT