Compte rendu BruCon 2013

OSSIR Paris 4 décembre 2013

damien.ressouches AT edelweb.fr

BruCon 2013

- Des origines à la 5ème édition
- De Bruxelles à Gand
- 3 jours d'ateliers
- 2 jours de conférences
- 1 track + des ateliers

HTTP Time bandit

- Vaagn Toukharian, Principal Engineer Qualys
- DOS applicatif
- Approche massivement asymétrique

Cette attaque / les autres

- Attaques classiques GET x 1000
- SlowLoris, PKI abuse, WebSockets…
- Impact de l’utilisation du caractère « % » dans des requêtes sur les bases de données (certaines)

Concept & Méthode

- Identifier la ressource fournie par le serveur la plus « gourmande » en CPU
- Utilisation d’un spider pour parcourir le site
- Volume non pris en compte
- Temps moyen important >> ressources exploitables

Parades évaluées

- Répartisseurs de charge, routeurs : seuils arbitraires
- Utilisation de l’outil

Tests avec Apache

Standard Apache conf = 98% CPU (client = 3%)

Simple mod_security

Advanced mod_security

mod_limitipconn

mod_qos

mod_bwshare

mod_throttle

mod_evasive

mod_httpbl

PCI - Achieving Compliance Through Open Source Solutions

- Erin Jacobs & Zack Fasel
- urbanesecurity.com
- Retour d’expérience, pragmatique
- PCI et solution libres

PCI DSS

- Payment Card Industry Data Security Standard
- 2004 : Visa, MasterCard, AmericanExpress, Discover
- 4 niveaux, en fonction du nombre de transactions
- Primary Cardholder Data & Sensitive Authentication Data

Le constat

- Le besoin : conformité
- Les contraintes : Coût, délais et complexité
- Le comportement : limiter le périmètre

Open Source Software (OSS) : +/-

+ Coûts initiaux
+ Bonne couverture du périmètre
+ Evolutivité
- Coûts cachés
- Support
- Pas « plug & play »

Openpciproject.com

- Partager les bonnes pratiques et retours d’expérience
- Comparer les OSS avec des solutions commerciales
- Fournir des solutions clés en main (procédures, VM…)

Log #1

- **Tout journaliser,** sinon les fondamentaux…
- Centralisation
- Surveillance

Autres OSS

- Contrôle d’intégrité : OpenSource Tripwire, OSSEC, Samhain, Weekly Script + Hash + Diff…
- Patch management : outils intégrés
- AV : ClamAV, liste blanche

Paint by Numbers vs Monet

- Russ Gideon
- Directeur de recherche en malware
- http://www.attackresearch.com/
- Red team
- Retro ingénierie
- Tests d'intrusion / attaques réelles

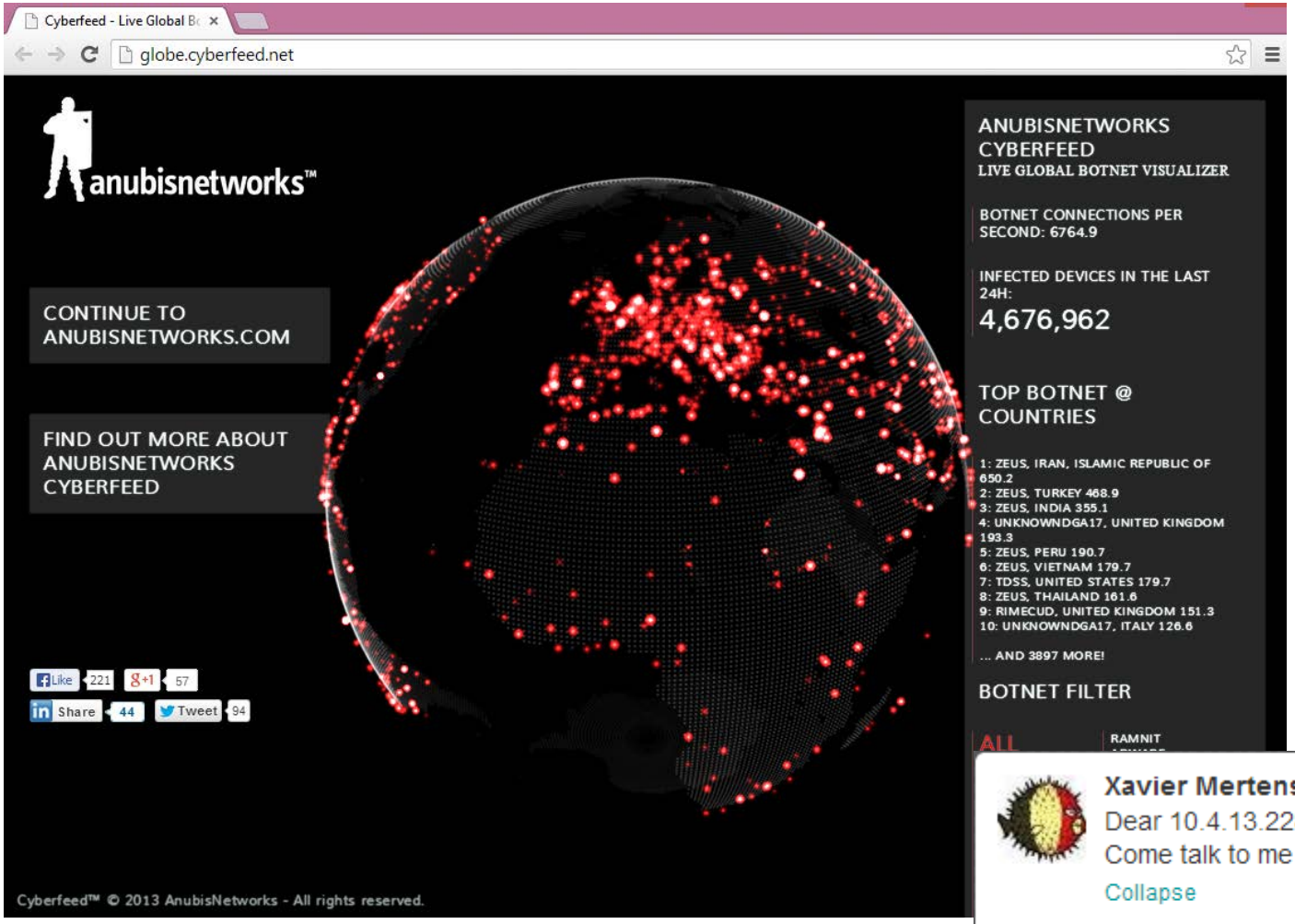
- Industrie de la sécurité
- Différence dans les évolutions
- APT : Advanced... ou pas

- Intrusion
- Déplacement latéral : APT / pentester
  - Persistance des accès
  - Récupération des identifiants
- Exploiter l’attaque
  - Pentest : peu de C&C
  - Attacker : processus automatisé

Realtime analysis and visualization of internet status

- João Gouveia, Tiago Balgan Henriques, Tiago Martins
- Architecture de la solution SteamForce
- Résultats du scan distribué :
  - HTTP
  - telnet
  - HTTPS
  - 5555
  - FTP
  - SSH
  - SMTP

Realtime analysis and visualization of internet status



Exploit Intelligence Project

- Dan Guido
  - Trail of bits
  - NYU.poly

- Rappels sur 2011
  - 4 crimepacks leaders
  - Vulnérables face à DEP, ASLR, EMET
  - Le potentiel de Java
  - Recommandations

2013

- Evolution des configurations
- Crimepacks pour IE, Reader & Flash ➔ XP sinon Java
- DEP + Reader sécurisé + EMET – Java = ?
- Elderwood Exploit Kit

Ses étudiants + Davis

- Elderwood : plugins, IE8 / XP ➔ 50%
- Davis : pas de plugin, IE9 / W7 ➔ 99%
- Facilité de développer une attaque / complexité de protection

Analyzing Internet Attacks with Honeypots

- Ioannis Koniaris
- DevOps, IT
- Botnet tracking, malware analysis
- Kippo-Graph, Honeyd-Viz, HoneyDrive

Vulnérabilité des composants

- Pare-feux
- IDS

…. Les honeypots à la rescousse

Présentations

- « un composant du système d'information dont la valeur repose sur l'utilisation non autorisée et illicite de cette ressource » Lance Spitzner
- Particularités
  - Pas de valeur
  - Pas de raison d'être contacté
  - Pas de raison de contacter d'autres ressources
  - Retarder l'attaquant
  - Alerter
  - Tromper l'attaquant : fingerprint, emulation

Les types de Honeypot

- Finalité : Production / Recherche
- 3 niveaux d’interaction
- 3 positionnements
- Autres types d’honeypots :
  - Honeytoken
  - Honeypages
  - Shadow honeypots, ADS
  - Client honeypots

(des) avantages

- ✓ Pas de faux positifs <-> IDS
- ✓ Système d’alerte
- ✓ Nouvelles menaces
- ✓ Défense en profondeur
- ✗ Périmètre très limité
- ✗ Risque de rebond (compromission)
- ✗ Vulnérabilité et manque de furtivité
- ✗ Complexe

…. Et attention aux aspects légaux

Geolocation of GSM mobile devices

- José Pico & David Perez / Taddong
- Enjeu : geolocaliser un terminal
- OpenDNS, 2 antennes

- Triangulation basée sur le temps de réponse
- Usurpation du réseau
- Identifier la direction du téléphone

Merci

- BruCon 6 : 25-26 septembre 2014
- http://www.brucon.org
- http://blog.brucon.org/
- https://twitter.com/brucon
- http://www.linkedin.com/groups?gid=1777141
- http://www.youtube.com/user/brucontalks/
- http://files.brucon.org/2013/