RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 17 Février 2015

Je (ne) suis (pas) Charlie

- Attentat du 7 Janvier
- Répercussions informatiques
  - Anonymous #OpCharlieHebdo
    - Sites Alintibaha et ansar-alhaqq.net HS
    - Liste de "cyberdjihadistes" diffusée sur PasteBin
    - Comptes piratés ou fermés
  - Cyberdjihadisme #opFrance
  - Loi(s) renseignement
    - Tendance à interdire le chiffrement
    - Installation de backdoor obligatoires
    - Fermeture de sites sans juge
    - Rapprochement doctrinal Occident / Chine.

#opFrance

- Plus de 20 000 sites "défacés"
  - Mairies,
  - Universités,
  - CNRS,
  - Mais surtout Monsieur tout le monde (et même une mosquée).
- Failles "élémentaires"
  - Joomla,
  - Drupal,
  - Wordpress,
  - Spip,
- Vingtaine de groupes (recouvrant)
  - "Fallaga Team" arrêté en Tunisie
  - AnonGhost,
  - Moroccan Hassan,
  - etc.

#opFrance : Conclusions

- Des mises à jour simples non appliquées
- Niveau bas des attaquants
- Prise de conscience ?
  - Rétablissement "en l'état" ! ? !, d'où des "redefacement"
  - Rarement des analyses approfondies (backdoor ?)
- Impact public assez important.

DDoS Chinois : poivre du Sichuan

Changement de comportement du GFW

- Principe : DNS Menteur
- Problème
  - Les résultats "mentis" sont connus.
  - Ils sont "contournés" VPN ou autres
- Solution
  - Renvoyer vers de vrais serveurs "aléatoires" (sur 5589 tests, 1856 IP uniques)
- Résultats
  - DDoS sur des serveurs quelconques
  - Saturation des connexions
    - Complète (pas de syncookies),
    - Non répétitives (inutilité "relative" des blacklists),
    - Très nombreuses ($>$ 5700 /16)
- Prémisses
  - Interrogation DNS sur ces mêmes serveurs

source : https://benjamin.sonntag.fr source : http://www.bortzmeyer.org

Google Zéro

- Programme Google de "full disclosure"
- 3 mois pour corriger (45 jours pour le CERT, 120 pour HP zéro day initiative)
- 83% des failles le sont,
- 90% depuis le 1er Octobre 2014 (Adobe : 100% !)
- Mais ire de Microsoft (faille Windows 7 et Windows 8.1, 3 jours avant le correctif)
- Délai de grâce de 14 jours si demande et confirmation de correction

source : http://googleprojectzero.blogspot.jp
source : http://www.zerodayinitiative.com

Piratage Bancaire d'envergure

- Découverte à cause d'un distributeur "généreux" à Kiev en 2013.
- 100 banques concernées de plus de 30 pays
- 300 millions de dollars, minimum
- Malware sur les postes des employés (envoyé par spearphishing) : carbanak, (RAT)
- Analyse des comportements, puis reproduction

source : http://blog.kaspersky.com/

MongoDB dans le monde

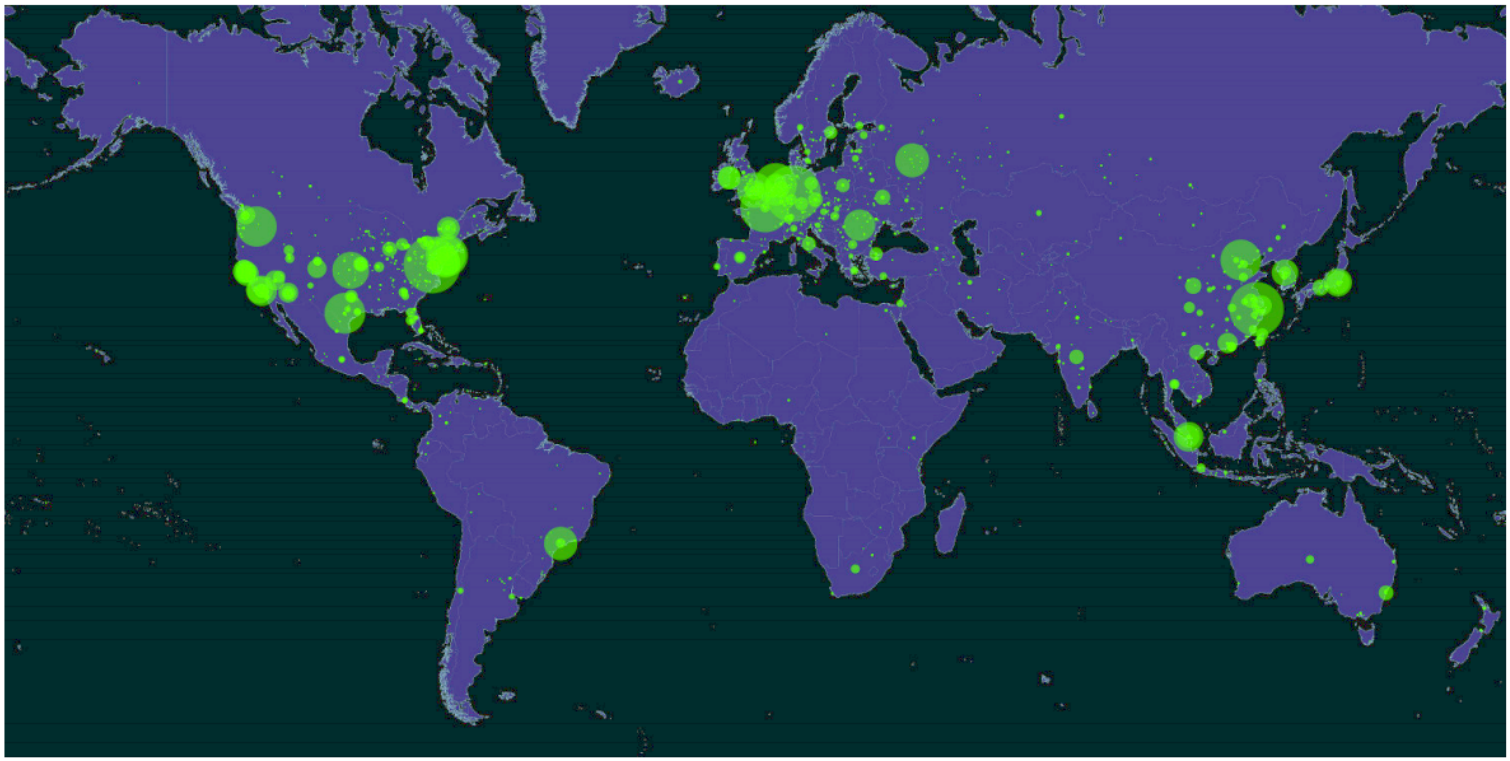

Figure 1: World-wide distribution of openly accessible MongoDBs

MongoDB mal configuré

- Test d'étudiants sur internet pour trouver des bases MongoDB (port TCP/27017)
- Des entreprises avaient leur MongoDB accessibles sur le net (39 890 instances)
  - Dont une base de 8 millions de clients chez un FAI Français
- Cela nécessitait une modification de la configuration du SGBD
- Mais ont oublié de protéger l'accès à la base.

source : http://cispa.saarland

Communication autour du piratage de l'IAE Lyon3

- Origine : un mail envoyé à 2200 étudiants, avec par erreur des données administratives
- Problème : concomitance avec des événements sécurité, dans la même sous-entité.
  - Serveur piraté (88000 contacts)
  - Envoi de spams

source : http://etudiant.lefigaro.fr

Festival Flash

- 3 patch Flash en 2 semaines
- 22/1/2015, 30/1/2015, 5/2/2015
- Couvrant 30 signatures CVE, dont
  - 1 de sévérité 5,
  - 1 de sévérité 8.5,
  - 1 de sévérité 9.5,
  - les 27 autres à 10 !
- Exploitées "massivement" en 0 day (vecteur : Dailymotion)

source : http://www.cvedetails.com/

Faille JAsbug

- Faille de 15 ans
- Vient d'être corrigé
- Attaque MiTM sur l'active directory

Faille IE 11.x/Spartan

- Faille XSS contournant le SOP (Same Origin Policy)
- Injecter du code dans n'importe quel site

source : http://www.cvedetails.com

Sujets du jour

M. Benjamin DELPY

Présentation et utilisation avancées de Mimikatz

MM. Vincent FARGUES et David BERARD - Thalès Group

Solution du Challenge NoSuchCon 2014