RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 6 Décembre 2016

Botnet et divination

- A partir du numéro de carte bleue
- Utilisation d'un botnet pour deviner
  - la date d'expiration (60 possibilités)
  - et le CVV2 (1000 possibilités)
  - utilisation de marchands qui ne vérifient que le PAN et la date (26 sur le top 400)
  - puis utilisation de marchands qui vérifient les 3.
- Pas de "centralisation" des échecs.
- Déjà utilisée ? (Tesco Bank avec 2,5 millions de $ de pertes.)

Référence : Université de Newcastle

Je risque rien. J'ai Tor..t ?

- Faille 0 day dans Firefox, et donc dans TorBrowser
- Utilisé activement pour divulguer l'identité de l'utilisateur
- Même "exploit" que celui utilisé par le FBI en 2013.

Référence : torproject

900 000 routeurs ADSL HS

- 900 000 routeurs ADSL de Deutsche Telekom mis hors service.
- Accès au port 7547 (pour manipuler les serveurs NTP)
- Deux jours pour corriger
- Le botnet Mirai semble avoir été utilisé.

Référence : threatpost

Locky in svg

- Images utilisées dans facebook, LinkedIn,
- Format SVG (avec du javascript),
- Récupère automatique une version de Locky,
- Indétecté au moment de sa diffusion.

Référence : checkpoint

J'ai le BLU...

- Firmware "spécial chine" développé par Adups
- Envoie les contacts, messages passés, etc. à un serveur chinois
- Permet de "mettre à jour" le firmware silencieusement
- Sorti sur des smartphones très bon marché dont BLU (Floride).
- Nombre de smartphones touchés : 3 millions !

Référence : AnubisNetworks

PoisonTap : ta session est ma session

- Samy Kamkar réalise une carte réseau
- à partir d'un raspberry pi à 5 dollar
- qui prend le pas sur toute autre connectique
- et qui "activement" pollue le cache d'un navigateur
- avec... ce que l'on veut
- alors que le poste est verrouillé.
- Windows, Mac et Linux impactés.

Référence : samy

Les pirates perdent parfois

- Arrêt d'Avalanche
- Arrestation d'un anonymous pour DDoS

Chute d'Avalanche

- Avalanche : Infrastructure de cybercriminalité à double fastflux depuis 2009
- 1 million de mails nocifs par semaine
- 800.000 domaines
- Les gentils
  - Europol
  - 30 pays impliqués
  - Fraunhofer-Institut (130 To de données analysées)
  - Shadowserver Foundation
- Opération le 30 novembre 2016
- 5 arrestations
- 39 serveurs saisis.

Référence : Europol

Arrêt d'un anonymous pour DDoS

- Déni de service contre EDF.
- préjudice de 162 000 € (selon EDF)
- 6 mois de prison avec sursis
- 29 000€ de dommages et intérêts

Référence : Legalis

Arrêt de zone téléchargement

- zone-téléchargement et DL Protect
- 11ème site français selon Alexa.
- 750 000 visiteurs par jour.
- 1,5 million d'€ de chiffre d'affaire (18000 films, 2500 séries, etc.)
- Lundi 28 novembre : opération Gervais (avec InterPol, Andorre, Allemagne, Islande)
- Arrestation de 7 personnes (5 relâchées)
- Andorre et Toulouse.

Référence : Zataz

Fuites de données

- Dailymotion
- Adultfriendfinder.com
- xHamster

Dailymotion : le leak

- Piratage de comptes dailymotion : 85 millions de mails
- 20% avec des mots de passe (mais avec bcrypt)
- Piratage le 20 octobre
- Conséquence sur ceux qui utilisent le service Oauth2

Référence : dailymotion

Secrets (?) Sex and Fun

- Piratage de Adultfriendfinder.com (339 Ms), Cams (62 Ms), Penthouse (7 Ms)
- Bases de données avec 20 ans d'informations (même les "effacées").
  - email@address.com@deleted1.com
- Octobre 2016
- Bases de données en vente sur le deepweb
- Mots de passe craqués en moyenne à plus de 99,5%

Référence : leakedsource

xHamster nu sur internet

- 380 000 comptes en vente
- login, adresse,
- Mails vérifiés par MotherBoard
- Mots de passe en MD5

Référence : Motherboard

Sujets du jour

La sécurité des blockchains

M. Stéphane Bortzmeyer - AFNIC

Rétro-analyse d'un logiciel malveillant en PHP qui a été installé sur un site Web: désobfuscation, présentation de la fonction.

M. Alexandre Guyon de Chemilly - Apsys