RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 21 Février 2017

2 millions de petits Wordpress, et moi, et moi.

- Faille dans wordpress 4.7.1 permettant de modifier toute page.
- Patchée en catimini en 4.7.2... Dommage.
- 2 millions de sites web piratés
- Très grosse utilisation par les pirates.

Référence : Sucuri

Vizio : chérie, on passe à la télé.

- Fournisseur de Smart TV
- Observait, par l'intermédiaire de 11 millions de télé
- Ce que regardait les clients
- Qu'il s'agisse de streaming, ou de fichiers sur USB
- Devinait grâce à l'analyse de plusieurs millions de points.
- 2,2 millions de dollars d'amende.

Référence : ArsTechnica

Piratage de MongoDB

- Des bases MongoDB disponibles directement sur Internet
- Le pirate (Harak1r1) copie puis efface les bases (vrai ou faux ?).
- 220 $ (0.2 BTC)
- Très peu payent (Souvent de simples tests).

Référence : Krebs on Security

La sécurité.. j'imprime pas.

- Chercheurs de l'université de la Ruhr
- Analyse des possibilités de pirater des imprimantes
- Utilisation du langage postscript
- Même les imprimantes les plus récentes sont vulnérables
- DoS, copie de document
- Outil PRET disponible pour rechercher
- Utilisé par un "whitehat" sur toutes les imprimantes accessibles depuis internet.

Référence : Université de Ruhr

L'ail au Tea, ben c'est pas bon

- Verizon fait un retour de son équipe de sécurité
- 5000 ampoules, chauffages, machines à café, etc. connectés
- Piratés et utilisés pour... rechercher des restaurants de crustacés
- Changement des mots de passe par le pirate
- Saturation des DNS locaux (environ 1000 requêtes de sous domaines toutes les 15 minutes)
- Solution : capture des dialogues pour récupérer les nouveaux mots de passe.

Référence : Verizon

Opération Bugdrop

- 70 organisations majoritairement ukrainiennes piratées (depuis 2015)
- Plus de 600 GB téléchargées sur Dropbox
- Conversations audios, screenshot, fichiers (sur USB ou non)
- Débute par un word infecté
- DLL (reflective injection) chiffrées par XOR récursif.

Référence : cyberx-labs

Un malware, sans les mains dans le disque dur

- Découverte d'un code meterpreter dans la mémoire d'un DC d'une banque
- Utilisation massive des outils "in situ"
- 140 organisations dans 40 pays pour ce malware.
- Des ressemblances avec cabarnak et GCMAN.

Référence : ThreatPost

Faille Microsoft GDI

- Faille connue par Microsoft depuis 1 an
- Touche (encore) GDI
- Exploitable par un fichier EMF
- Découverte par le projet zéro de Google
- Après Full disclosure, et PoC, Microsoft devait le corriger au dernier patche Tuesday
- Ne le sera pas finalement pas avant le 14 Mars.

Référence : Projet zéro

Vous ne pouvez pas comprendre, j'ai un Mac..

- Virus Macro sur MacOS
- Cible : Word.
- Rapatriement d'une backdoor depuis securitychecking.org:443/index.asp
- Code de faible niveau.

Référence : ThreatPost

Vous ne pouvez vraiment pas comprendre, j'ai un Mac..

- X-agent spyware.
- Origine APT28 (Groupe Russe)
- Utilisé précédemment sur Windows, Android, Linux
- Du lourd.

Référence : The HackerNews

Les antivirus, tous de la m..de (sauf Microsoft)

- Billet d'humeur de Robert O'Callahan,
- Ex développeur Mozilla
- Très forte critique des antivirus
  - Ne détectent quasiment plus rien
  - Introduisent des failles de sécurité
  - Introduisent des bugs et des ralentissements
  - Désactivent certains mécanismes de sécurité des navigateurs.
- Préfère les bonnes pratiques de sécurité.

Référence : Robert O'Callahan

Guide ANSSI sur la collecte des données Windows 10

- Après la sécurisation,
- Un nouveau guide pour restreindre la collecte de données
- Des désactivations en série
- Des tweaks (avec un niveau supérieur de "non collecte");
- Des GPO pour l'entreprise.
- Et un Windows 10 moins sexy au final.

Référence : ANSSI

Google sans firewall

- Google présente son fonctionnement
  - Sans Firewall
  - Sans VPN
- grâce à
  - L'identification des postes
  - L'identification des personnes
- mais c'est 3 ans de travail.. avec les moyens de Google.

Référence : Kaspersky

Les pirates perdent parfois

- Anna Senpaï

Who is Anna Senpaï

- Excellente analyse de Krebs
- En anglais.
- Un roman d'une dizaine de pages
- Passionnant.

Référence : Krebsonsecurity

Fuites de données

- Denuvo
- Yahoo

Denuvo

- Spécialisée dans la protection de jeux vidéos.
- Piratage de messages privés, dont certains de studios de création de jeux.
- Accessibilité de fichiers (dont certains de jeux)

Référence : ArsTechnica

Yahoo : Chef, je crois que j'ai encore glissé

- Yahoo annonce que des cookies forgés ont été utilisés
- Yahoo ne sait pas "vraiment" qui est concerné.
- N'a pas de lien avec les 2 autres problèmes.
- Après les 300 Millions de $ de réduction, Verizon va-t-il demandé un autre rabais ?

Référence : Yahoo

Petites actualités

- On peut tracker un utilisateur à 99,7% depuis son PC sans possibilité de blocage *Référence : hackernews*
- LeadedSource stoppé par le FBI. Les bases piratées devront être achetées ailleurs.*Référence : Zdnet*
- Récupérer des informations personnelles grâce à l'auto-remplissage des formulaires *Référence : GitHub*
- TicketBleed : Faille "HeartBleed" sur les F5 *Référence : filippo.io*
- Faille en cours sur les OS microsoft par utilisation de SMB *Référence : cert.org*

Sujets du jour

Des records de vulnérabilité

M. Rodolphe ORTALO, Carsat MP