RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

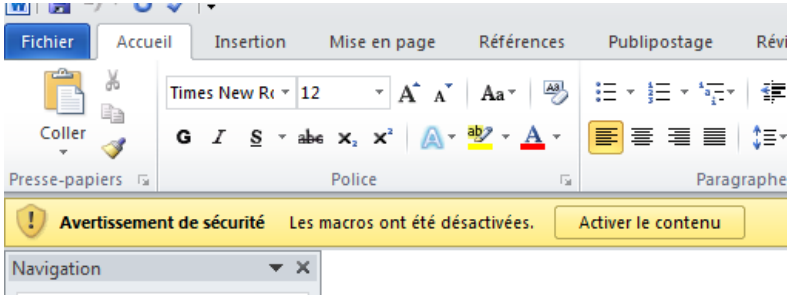
Mardi 2 Juin 2015

Les piratages et attaques

Les piratages et attaques

Macro is Back

- Virus macro Word Dridex
  - Malgré la nécessité de valider les macros



- 3 temps :
  - Infection VBS
  - Recherche de binaires sur une IP, puis sur pastebin
  - Connexion en SSL
- Entreprises françaises touchées
- Français correct
- Virus non détecté (3 sur 57)
- Mais parfois bloqué par certaines signatures clamav
- 6 campagnes différentes

Microsoft Digital Constitution

- Site web microsoft "digital constitution" piraté
- Site sur la vie privée en ligne
- Symptômes
  - Installation de liens de jeux en ligne
- Raisons
  - Version obsolète de Wordpress

Piratages de OPM

- Office of personnel Management de l'armée américaine
- 2 piratages successifs
  - 10 millions de personnes
  - 4 millions le second (les plus "intéressantes" ont été ciblées)
- Attribution à "deep panda" (groupe chinois)
- Les raisons
  - Du code cobol (pas de chiffrement possible)
  - Windows + jrun (abandonné en 2013 par adobe)
  - Des contractants employant des chinois (en Chine)
  - *"Everything is focused on box checking"* et pas de *"Train like you fight"*
- Les solutions
  - "Sprint sécuritaire" de 30 jours
  - Généralisation de l'authentification multifacteurs
  - Abandon de "adobe jrun"

arstechnica.com

Piratage de Kaspersky

- Kaspersky, société antivirale réputée, domiciliée en Russie.
- Duqu 2.0 (ciblant aussi les iraniens)
- Plusieurs zéro days (dont MS15-061)
- Des certificats de drivers Foxconn volés
- Découverte par un produit anti-APT "en test"
- Supputations
  - Equation group
  - NSA et GHCQ (documents Edward Snowden concernant le warrant gpw/1160 de 2008)

fistlook.org

kaspersky.com

securlist.com

army.mil piraté par la SEA

- Piratage du site web US par la syrian electronic army (SEA) (army.mil)
- Le lundi 8 juin
- Installation de Popups
- Passage de tous les sites web en HTTPS Only

Eweek.com

Piratage de lastpass

- Site d'hébergement de mot de passe
- Nécessité de changer les mots de passe "master"
- *"Mais les données ne risquent rien"*
  - Chiffrement des données (with a random salt and 100,000 rounds of server-side PBKDF2-SHA256, in addition to the rounds performed client-side,)
- A replacer dans le contexte des gestionnaires de mots de passe "dans le cloud"

threatpost.com

devd.me

Les failles

Les failles

Faille Apple

- Permet le vol de mot de passe
- Faille dans l'application mail
  - Utilisation de code html dans un mail.
- Pas de correction immédiate

github.com

youtu.be

Faille venom

- Touche les systèmes de virtualisation
  - xen,kvm, qemu
- Se trouve dans le contrôleur de disquette virtuel

blog.erratasec.com

Faille IE

- Décrite depuis février 2015
- Microsoft ne patchera pas.
- Détectée par équipe HP, pour un concours Microsoft (ont gagne 125000 $)

hp.com

Faille samsung

- Faille dans le mécanisme de mise à jour de Swiftkey
- L'éxécutable est récupéré en HTTP, donc interceptable
- Mais l'application n'est pas vulnérable sur le store

blackhat.com

LogJam

- Similarité avec freak
- Faille "downgrade" dans diffie-helman
- On descend le chiffrement à 512 bits
- tls(https, imaps, smtps, etc.)

weakdh.org

Informations diverses

Informations diverses

Autres Nouvelles

- Reddit, Wikipédia passent en HTTPS
- Blackmirror
  - Sourceforge copie des outils (nmap, vlc,gimp) qui n'étaient pas (ou plus) sur sourceforge
  - Intégration de "crapware" dans les installeurs.

Sujets du jour

MM. Stéphane TONELLI et Patrice REVEILLAC - Gendarmerie Nationale - SR Midi-Pyrénées

Les bitcoins : principes, fonctionnement et utilisation