RéSIST : Tour d'horizon

Fabrice Prigent

RéSIST

Mardi 21 Juin 2017

La sécurité coûte cher... Essayez le piratage

Référence : Commitstrip

It's not a bug, it's a feature

- Cloak and Dagger
- Découverte par 2 chercheurs du Georgia Institute of Technology
- Utilisation sur Android
- Mécanisme standard de "surrimpression" d'alerte
- Combiné au mécanisme pour handicapés visuels.
- Utilisé pour "surimprimer" sur les demandes d'autorisations
- Pas de solution "générique", hormis les précautions habituelles

Référence : Science Daily

1 million de dollars de rançon pour un web hoster

- Nayana, Web hoster sud coréen
- 153 Serveurs Linux
- 3400 clients cryptolockés
- Malware utilisé : variante Erebus + Faille Dirty Cow
- Infrastructure : Apache 1.3.36 + PHP 5.1.4
- Rançon de 1 million de dollars (4,4 millions initialement)

Référence : Ars Technica

ShadowBroker, WikiLeaks : même combat ?

- Le groupe de pirates ShadowBrokers annonce des leak NSA réguliers
- Ils auraient, selon leur dire, 75% de l'arsenal NSA.
- Abonnement à 21000 $ (en Zcash)
- Cas de conscience pour les whitehats
- Crowd Founding (échoué) pour les whitehats
- La question est pourquoi (Eternal Blue, utilisé, pouvait rapporter bien plus)

Référence : Steemit

Wannacry : rire ou pleurer ?

- Ver utilisant une faille provenant du leak NSA (SMB Exploit)
- Désactivé par un simple domaine (killswitch).
- 139 K$ de rançon (au 16 juin 2017)
- n'a touché que 200 à 300 000 machines (1,7 M pour Conficker, 13 M pour Mariposa) dont quelques grosses entités (Renault, Fedex, NHS, etc.).
- Propagation par port 445 donc soit accessible du net, soit par l'interne).
- A été largement devancé par un ver plus ancien faisant du mining : Adylkuzz.
- A poussé Microsoft à changer sa politique de patch sur Windows XP.

Stackslash : faille sur les unix

- Existe depuis 2005, redécouverte en 2010, puis en 2017
- Chercheurs de Qualys
- Touche Linux, FreeBSD, Solaris.
- Permet à un simple utilisateur de passer root.
- Des contournements existent, mais peuvent casser une machine chargée.
  - RLIMIT_STACK
  - RLIMIT_AS
  - pour les utilisateurs locaux et les services distants
- Correctifs en cours de distribution

Référence : Qualys

Phishing : Remplissage de nom de domaine

- Nouvelle technique de phishing
- On complète le nom de domaine avec des tirets
- Découverte par Phislabs
- Cible particulièrement les mobiles.
- Les mobiles sont plus vulnérables, et plus attaqués (double authentification SMS, compte, etc.)

http://m.facebook.com————————-validate—-step1.rickytaylk.com/sign_in.html *Référence : Phishlabs*

Fuites de données

- Electeurs Américains
- Withings
- YahooBleed

Elections US

- 1,1 To d'informations sur des électeurs américains disponibles
- Société Deep Root Analytics, spécialisée dans la publicité politique
- un peu moins de 200 Millions de fiches (Tél, religion, etc.)
- accessible sur un compte amazon S3
- Mécanisme des "AWS S3 Bucket" qui sont souvent laissés sans sécurité.

Référence : UpGuard

Withings

- Racheté récemment par Nokia
- Quantify yourself
- Plusieurs centaines de comptes, majoritairement français.

Référence : Zataz

YahooBleed

- Faille ImageMagick (datant de Janvier 2015).
- Problème de correctif inapplicable.
- Retrait de la bibliothèque
- En fait ce sont 2 failles.

Référence : ScaryBeastSecurity

Petites actualités

- Par l'intermédiaire du protocole Serial-Over-LAN, on peut prendre le contrôle de machines Intel *Référence : Intel*
- Reality Leigh Winner trahie par les points jaunes sur les impressions d'un leak concernant les piratages russes *Référence : The Intercept*
- Le CCC casse l'identification par Iris du Samsung Galaxy S8 avec des bouts de ficelle *Référence : CCC*
- 98 % de 3087 étudiants du MIT se font piéger et donnent leur contacts pour une pizza (mais 86% le font pour rien du tout, plus 6% qui mentent) *Référence : NBER*

Petites actualités 2

- Les nouveaux phishing demandent une photographie avec une carte d'identité (Paypal) : *Référence : Phishme*
- Les élèves de Rhodes Island ont un PC (programme 1:1), mais perdent leur intimité : *Référence : PDF de l'ACLU*
- 2 millions de machines dans le monde proposent du SMBv1, dont 42% avec un accès Guest. Entre wannacry et sambacry... *Référence : BleepingComputer*

Sujets du jour

La prédation informationnelle

Damien Teyssier

Phishing, le retour

Doriane Pérard