Sécurité, protection des sources, what else ?

Pierre-Yves Bonnetain
py.bonnetain@ba-consultants.fr

B&A Consultants – BP 70024 – 31330 Grenade-sur-Garonne

7 décembre 2015

B&A Consultants

- Cabinet de conseil en sécurité informatique créé en 1996.
- Conseils, suivi et assistance en sécurité informatique.
- Audits de sécurité, de configurations, de code...
- Tests d'intrusion, tests d'applications.
- Réponse à incidents, analyses *post-mortem*.
- Analyses de risques, gestion des risques sur l'information.
- Ingéniérie de la sécurité informatique, recherche de solutions.
- Formations à la sécurité informatique.
- Expertise judiciaire (civile ou pénale) et expertises privées.
- Animateur de ReSIST, groupe de travail régional de l'OSSIR (`www.ossir.org/resist`)

B&A CONSULTANTS SECURITE INFORMATIQUE

Dans les films et dans la vie

(C) King Features Syndicate – Bill Holbrook

`www.onthefastrack.com`

C'est drôle. . .

Et malheureusement terriblement réaliste.

Petit dicton

Le problème de sécurité se trouve entre le clavier et la chaise.

Des réflexes de base à avoir

- Mettez à jour vos systèmes et les outils dont vous vous servez
- Rien d'inutile sur les systèmes
- Pas de mélange éléments sensibles/éléments publics : machines différentes
- Ne faites spontanément confiance à personne, surtout de façon dématérialisée
- Chiffrez de façon efficace tout votre système (disque/partition)
- Sauvegardez de façon sécurisée vos systèmes
- Gérez vos mots de passe, **sans doublons**
- Gardez vos secrets secrets !

B&A CONSULTANTS SECURITE INFORMATIQUE

Le mot de passe : je peux le deviner

2012, Yahoo !

Le mot de passe : je peux le deviner

Most Common & Worst Passwords of 2014

Rank	Password	Change from 2013
1	123456	Unchanged
2	password	Unchanged
3	12345	Up 17
4	12345678	Down 1
5	qwerty	Down 1
6	123456789	Unchanged
7	1234	Up 9
8	baseball	New
9	dragon	New
10	football	New
11	1234567	Down 4
12	monkey	Up 5
13	letmein	Up 1
14	abc123	Down 9
15	111111	Down 8
16	mustang	New
17	access	New
18	shadow	Unchanged
19	master	New
20	michael	New
21	superman	New
22	696969	New
23	123123	Down 12
24	batman	New
25	trustno1	Down 1

via Splashdata analysis

B&A CONSULTANTS SECURITE INFORMATIQUE

Smartphone, tablette : j'ai déjà votre mot de passe

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

- En supposant que ce n'est pas simplement « faire glisser pour déverrouiller » (15% environ)
- Près de 25% des mots de passe numériques sur ces vingt valeurs
- Très nombreuses analyses statistiques sur les mots de passe numériques :
  - dates de naissance (jour/mois, 19xx),
  - répétitions (4545, 6363),
  - circuits sur pavé numérique (2580, 1397, 1458)
  - sur le premier chiffre (ligne supérieure ou colonne gauche : 70%, dont chiffre 1 : 30%)
- Les « codes graphiques », c'est pire !

B&A CONSULTANTS SECURITE INFORMATIQUE

Si j'ai votre mot de passe

Je suis « vous »

- Utilisation de **votre** identité sur les systèmes ou logiciels
- Que ces systèmes ou logiciels soient privés ou professionnels
- Conséquences :
  - Accès à tout ce à quoi vous avez accès
  - Possibilité d'agir à votre place (messages ? usurpation d'identité ?)
- Smartphone/tablette se connectent souvent **automatiquement** aux applications (messagerie, Facebook, WhatsApp. . .)

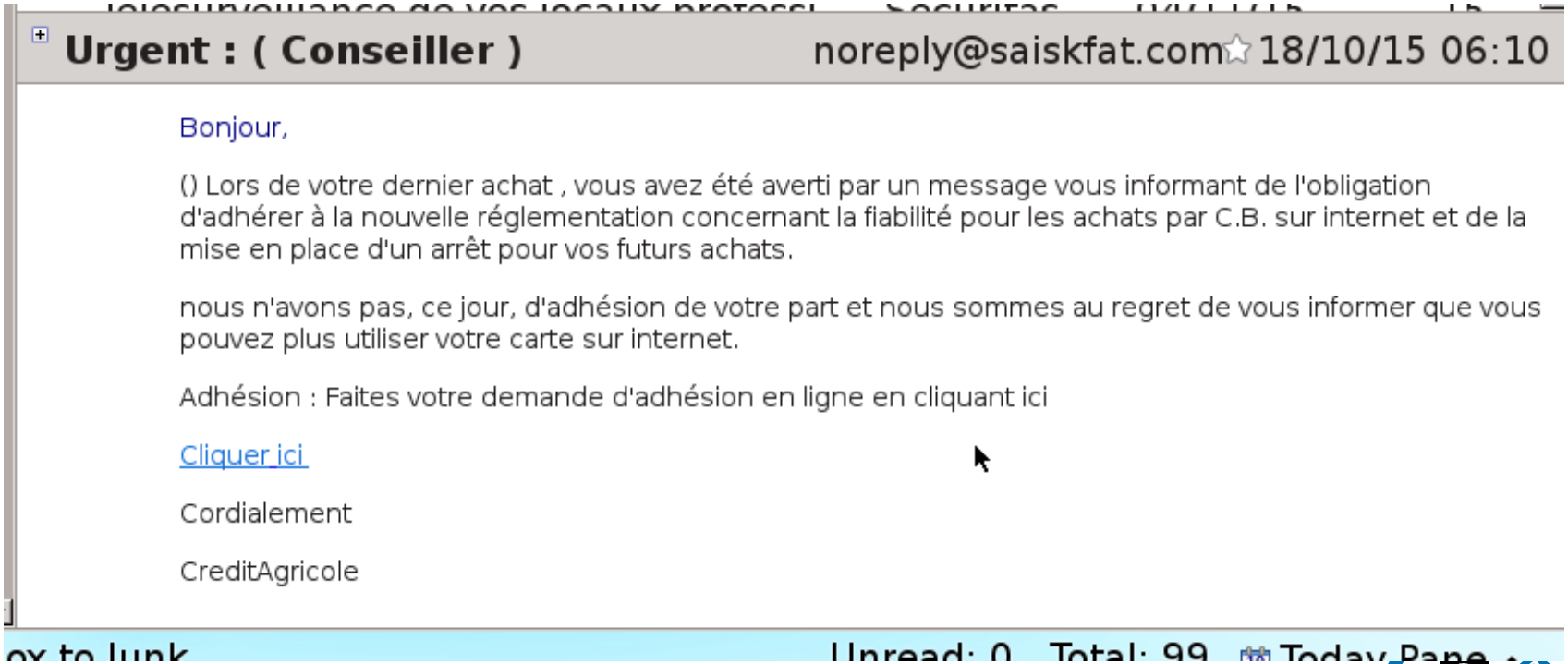
J'en veux plus

Tentatives de connexions sur **tous** les systèmes ou logiciels où vous pourriez avoir un compte, en utilisant le même mot de passe.

CONSULTANTS
SECURITE INFORMATIQUE

Etre trop confiant, c'est être naïf

- Informatique = dématérialisation
- Dématérialisation ⇒ perte de repères
- Perte de repères = « qui est *vraiment* derrière ce message/ce site ? »



Un mail, un site, une info sensible

Saturation de votre espace disque

Nous vous rappelons les consignes pour votre messagerie :

- Nettoyer les spams
- Effacer les mails de blagues (powerpoint et autres) qui prennent **beaucoup** de place.
- Vider régulièrement votre corbeille
- Hormis cas exceptionnel, les mails de plus de 1 an ne servent à rien

login :

Mot de passe :

Valider Effacer

ANTS
SECURITE INFORMATIQUE

Un mail, un site, une info sensible

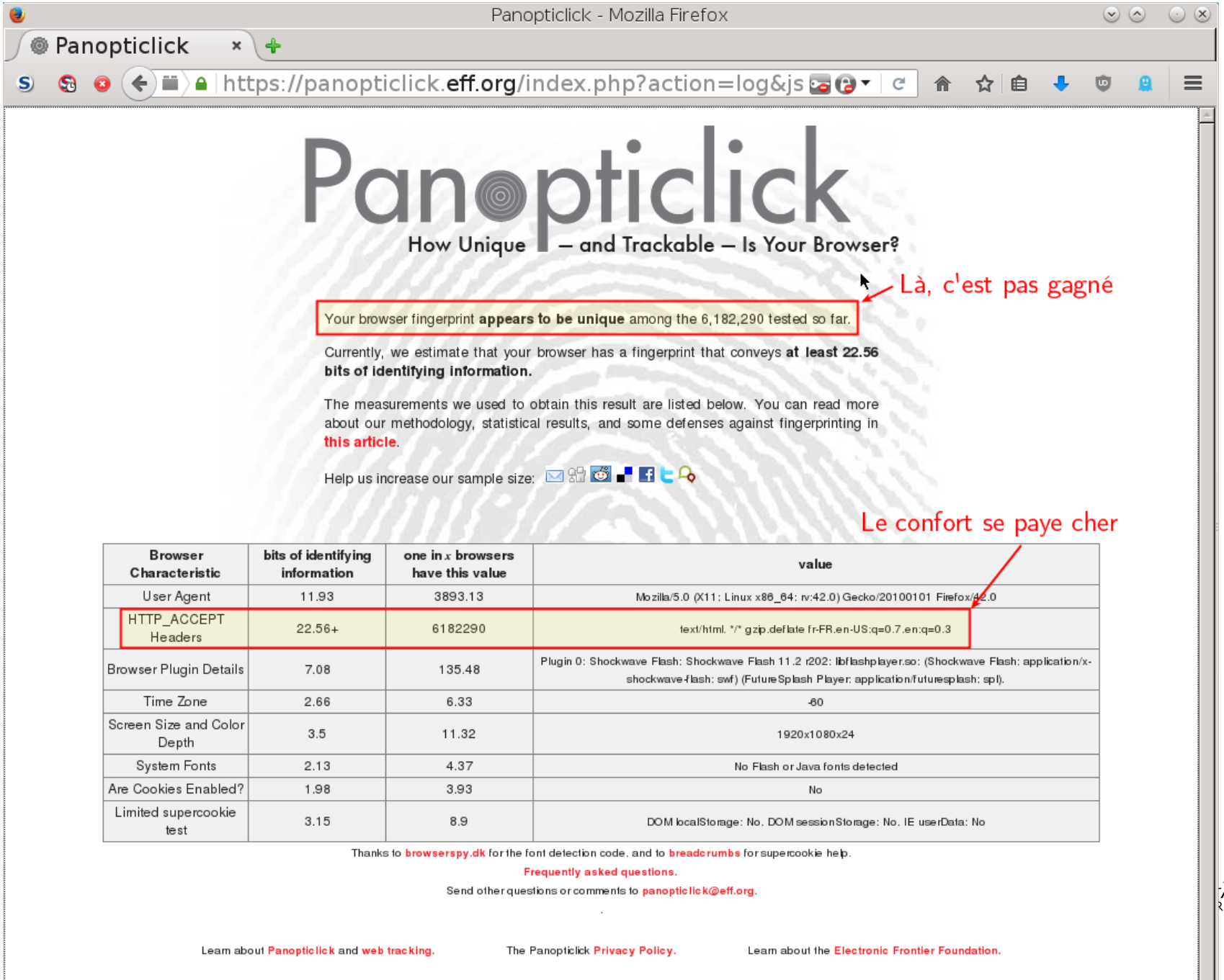
B&A CONSULTANTS SECURITE INFORMATIQUE

Chiffrer, oui mais...

- Les données seront consommées en clair, par vous ou vos correspondants
- La très grande majorité des attaques/fuites se fera à ce moment-là
- Bon outil $\Rightarrow$ impossible de récupérer les données sans la clé de déchiffrement $\Rightarrow$ ne pas se rater !
- Chiffrement ici, pas de chiffrement là-bas $\rightarrow$ c'est là-bas que se fera l'attaque (typique : sauvegardes)

B&A CONSULTANTS SECURITE INFORMATIQUE

Des traces, des traces



Quelques outils

Firefox avec les extensions HTTPS Everywhere, Perspectives, Ghostery, Ublock-Origin, Flash Block

OpenPGP pour le chiffrement ponctuel (emails et fichiers)

Bitlocker, Luks, Truecrypt pour le chiffrement global (disque, partitions)

Tails distribution Linux (clé USB, DVD) garantissant l'absence de traces sur la machine (incorpore les éléments précédents)

Keepass, PasswordSafe Outils de gestion des mots de passe

B&A CONSULTANTS SECURITE INFORMATIQUE