

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

- 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.
- Ingénierie 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)

Dans les films et dans la vie



©2015 King Features Syndicate, Inc. World rights reserved



<http://www.onthefastrack.com>

Dans la
vraie
vie :



E-mail: bholbrook1@gmail.com

(C) King Features Syndicate – Bill Holbrook
www.onthefastrack.com

C'est drôle...

Et malheureusement terriblement réaliste.

Petit diction

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 !

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

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 !

Je suis « vous »

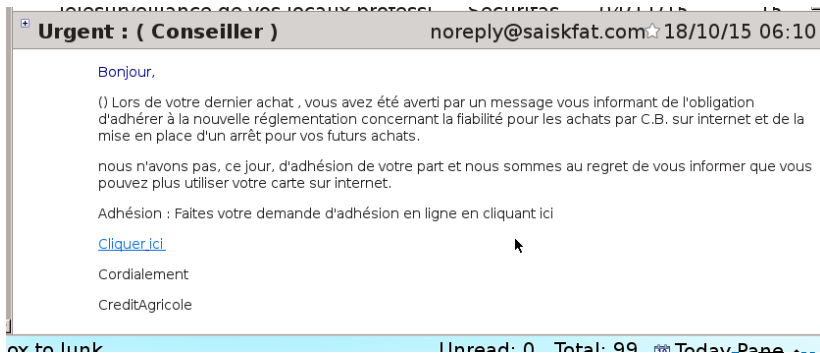
- Utilisation de **votre** identité sur les systèmes ou logiciels
- Que ces systèmes ou logiciels soient privés ou professionnels
- Conséquences :
 - Accès à tout ce à quoi vous avez accès
 - Possibilité d'agir à votre place (messages ? usurpation d'identité ?)
- Smartphone/tablette se connectent souvent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

Etre trop confiant, c'est être naïf

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



URGENT : (Conseiller) noreply@saiskfat.com 18/10/15 06:10

Bonjour,

() Lors de votre dernier achat , vous avez été averti par un message vous informant de l'obligation d'adhérer à la nouvelle réglementation concernant la fiabilité pour les achats par C.B. sur internet et de la mise en place d'un arrêt pour vos futurs achats.

nous n'avons pas, ce jour, d'adhésion de votre part et nous sommes au regret de vous informer que vous pouvez plus utiliser votre carte sur internet.

Adhésion : Faites votre demande d'adhésion en ligne en cliquant ici

[Cliquer ici](#)

Cordialement

CreditAgricole

Unread: 0 Total: 99 Today Page 1



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 :

Piratage en cours Changez IMMEDIATEMENT votre mot de passe

Changement de mot de passe

Login :

Ancien mot de passe :

Nouveau mot de passe

Nouveau Mot de passe (Confirmation)

Valider

Effacer

- 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)

Des traces, des traces

Panoptick - Mozilla Firefox

Panoptick x +

https://panoptick.eff.org/index.php?action=log&js

Panoptick

How Unique – and Trackable – Is Your Browser?

Your browser fingerprint **appears to be unique** among the 6,182,290 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 22.56 bits of identifying information**.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size:

Là, c'est pas gagné

Le confort se paye cher

Browser Characteristic	bits of identifying information	one in <i>x</i> browsers have this value	value
User Agent	11.93	3893.13	Mozilla/5.0 (X11; Linux x86_64; rv:42.0) Gecko/20100101 Firefox/42.0
HTTP_ACCEPT Headers	22.56+	6182290	text/html,*/* gzip deflate fr-FR,en-US;q=0.7,en;q=0.3
Browser Plugin Details	7.08	135.48	Plugin 0: Shockwave Flash: Shockwave Flash 11.2 r202; Ibfshpplayer.so; (Shockwave Flash: application/x-shockwave-flash; swf) (FutureSplash Player: application/futuresplash; spl)
Time Zone	2.66	6.33	-60
Screen Size and Color Depth	3.5	11.32	1920x1080x24
System Fonts	2.13	4.37	No Flash or Java fonts detected
Are Cookies Enabled?	1.98	3.93	No
Limited supercookie test	3.15	8.9	DOM localStorage: No. DOM sessionStorage: No. IE userData: No

Thanks to [browserspy.dk](#) for the font detection code, and to [breadcrumbs](#) for supercookie help.

[Frequently asked questions.](#)

Send other questions or comments to panoptick@eff.org.

Learn about [Panoptick](#) and [web tracking](#). The [Panoptick Privacy Policy](#). Learn about the [Electronic Frontier Foundation](#).

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