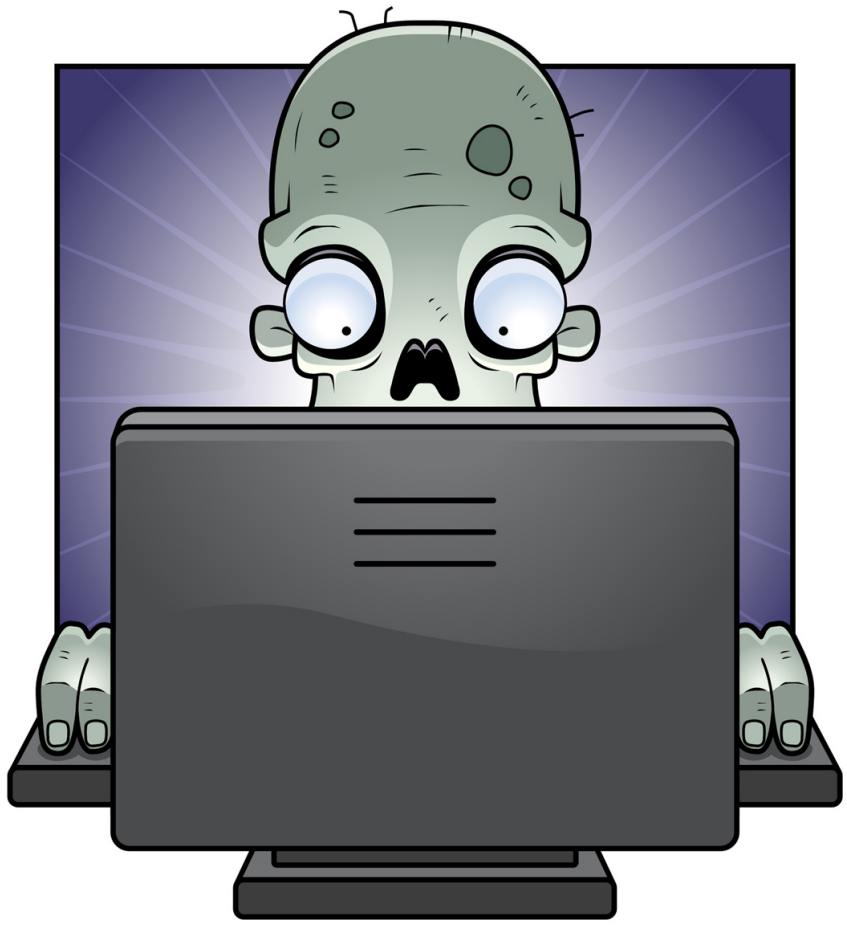
Cyber-Criminalité

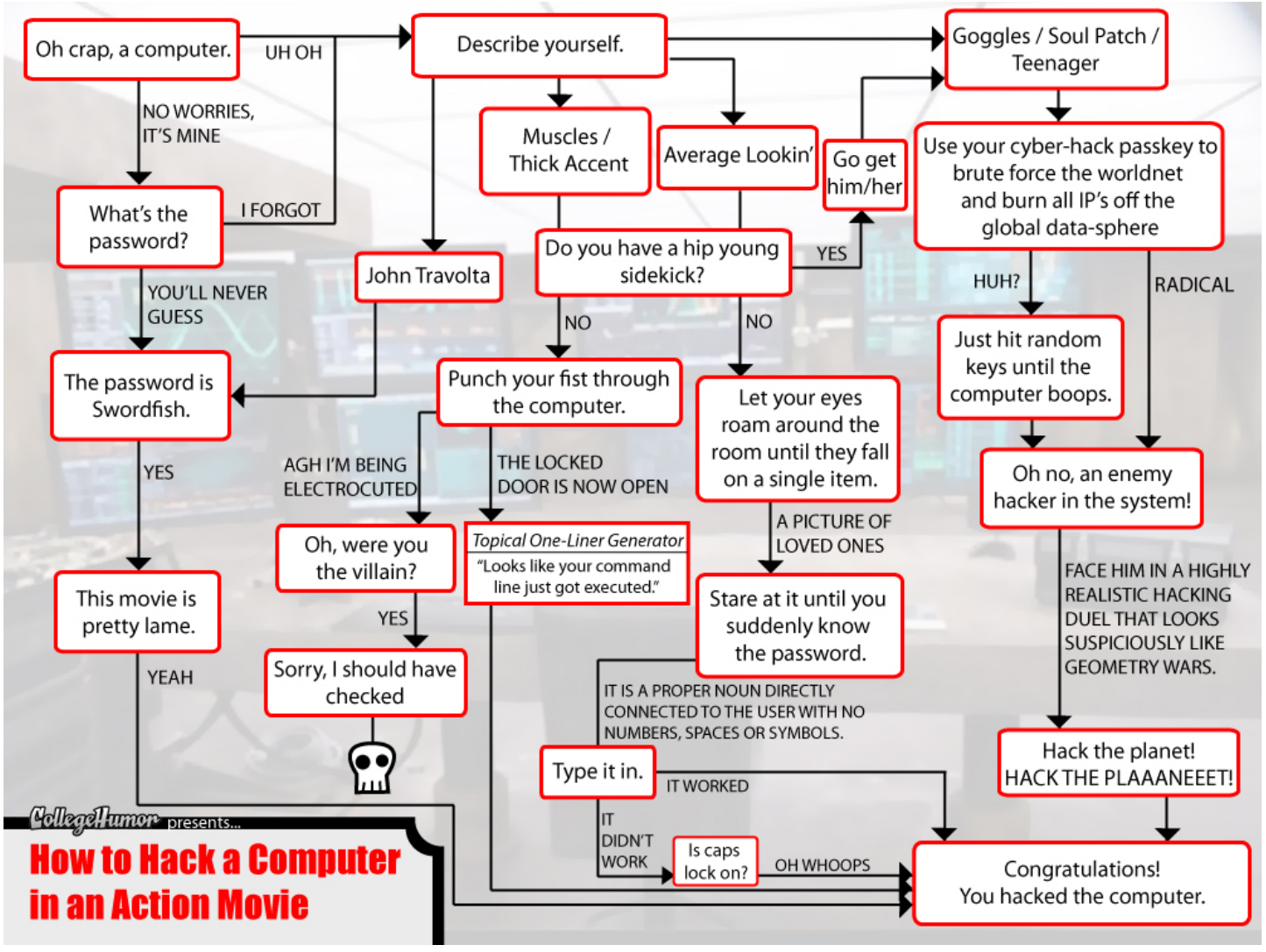
Contes et légendes du cyberespace

Nicolas Rougier



Hollywood

Mais puisque je vous dis que je l'ai vu à la télé...



Sécurité Informatique

Qui fait quoi où comment ?

Données

- Collecte
- Echange / Vente
- Copie / Refus
- Modification

Acteurs / Cibles

- Gouvernements
- Entreprises
- Particulier
- Vous

Enjeux

- Economique
- Politique
- Militaire
- Sociétal

Vecteurs

- Systèmes informatiques
- Systèmes embarqués
- Réseaux
- etc.

Historique.zip

1970 John Draper découvre qu'un son de 2600Hz autorise la connexion gratuite aux lignes AT&T.

1981 Ian Murphy, alias *Captain Zero* est la première personne inculpée pour crime informatique.

1986 Premier virus informatique, *Brain*, Pakistan. Infecte les systèmes IBM/MSDOS.

1987 Virus *Jérusalem*, capable d'infecter et de détruire.

1988 Premier ver internet, Robert T. Morris, 3 mois de prison (sursis), 10 000$ d'amende.
Première condamnation de Kevin Mitnick.

1989 *Dark Avenger*, virus se propageant d'un ordinateur à un autre. A peu près 30 virus en circulation.

1990 Kevin Poulsen est condamné (détournement d'appels téléphoniques)

1991 Plus de 1000 virus en circulation.
Phil Zimmerman met PGP à disposition de la communauté.

1994 Vladimir Levin vole éléctroniquement 10 000 000$ à la CityBank. 3 ans de prison.

1995 Arrestation de Kevin Mitnick (7 ans de cavale). 5 ans de prison.

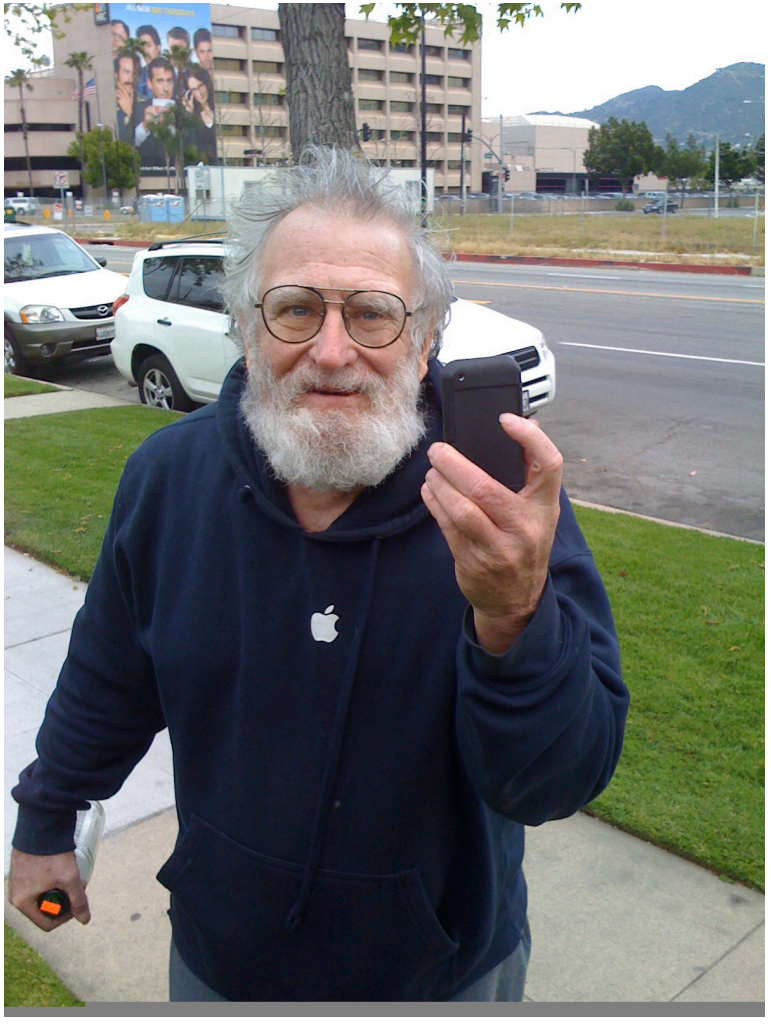
1998 Explosion du piratage (Back Orifice, sites militaires, New York Times).

2000- Répression accrue, effet 11/01.

Phreaking

Alors, c'est l'histoire d'un gars qui achète une boîte de céréale...

Cap'n Crunch alias John Draper



Hacking

Un peu d'astuce, d'espièglerie, c'est la vie de Kevin...

Black Hat

White Hat

Somecolor Hat

A lire : `korben.info/interview-black-hat.html`

Cracking

Voilà ! Avec cette protection, personne ne pourra... ah zut !

DeCSS vs DMCA, 1998

DeCSS permet de décrypter les contenus d'un DVD.

Sony vs. George Hotz, 2010

Ne lisez pas la ligne suivante

```
46 DC EA D3 17 FE 45 D8 09 23 EB 97 E4 95 ...
```

Trop tard, vous êtes coupable !

Voir aussi

`www.jeuxvideo.com/dossiers/00016383/les-protections-anti-copie-qui-font-rire-ou-pleurer.htm`

Scamming

419, escrocs et croque-escrocs

From : Martins Jide
Date : Thursday, September 23, 2004 11 :02 AM
Subject : URGENT REPLY

It is obvious that this proposal will come to you as a
suprise. This is because we have not met before but I am inspired to
sending you this email by the huge fund transfer opportunity that
will be of mutual benefit to the two of us.

However, I am Barrister Martins jide,the personal
attorney to the late Engr. Suk Hun Wufei flody, a Citizen of
Japan, who used to work with Nigerian National
Petrolum Co-operatrion (NNPC).

On the 26th of August 2003, my client,his wife and
their three were involved in a fatal house explossion at
Nigerian National Petrolum Co-operatrion (NNPC)
quaters Lagos.

blah blah blah...

Hoaxing

et autres légendes urbaines...

Subject : FW : FW : Free Shoes
Date : 01/03/1998

Just a quick note to tell you about a program that Nike started to help make fields and playgrounds for the underprivileged from old tennis shoes.

All YOU have to do is send in your old tennis shoes (NO MATTER WHAT THEY LOOK LIKE) with a piece of paper that has your name and address on it, and Nike will send you a brand new pair back FREE OF COST!!! The tennis shoes you send DO NOT have to be Nike. Just as long as they are tennis shoes. It really is a worthwhile project, and it's helping a lot of young kids.

Phishing

Votre biote mail est trop pleine de plein de lettres...

Il a été porté à notre attention que vous avez dépassé votre limite de quota de boîte aux lettres ensemble. Vous ne pouvez pas être en mesure d'envoyer ou de recevoir de nouveaux courriels toute fraction de seconde à partir de maintenant, jusqu'à ce que vous mettez à niveau votre quota de boîte aux lettres email.

Cliquez ici http ://everstats.cjbb.net/ mettre à jour votre limite de quota

Merci pour votre coopération
Copyright © 2010 de l'administrateur système.

RAPPEL
Suite à l'incident de sécurité survenu à l'Université de Lorraine, il est nécessaire de changer de suite pour celles et ceux qui ne l'ont pas encore fait, votre mot de passe, en vous rendant à l'adresse suivante :

https ://xxxxxxx.xxxx.xx

Puis, après authentification, de cliquer sur "mot de passe".

Lockpicking

Ne vous souciez plus jamais de vos clés

Defcon 2011

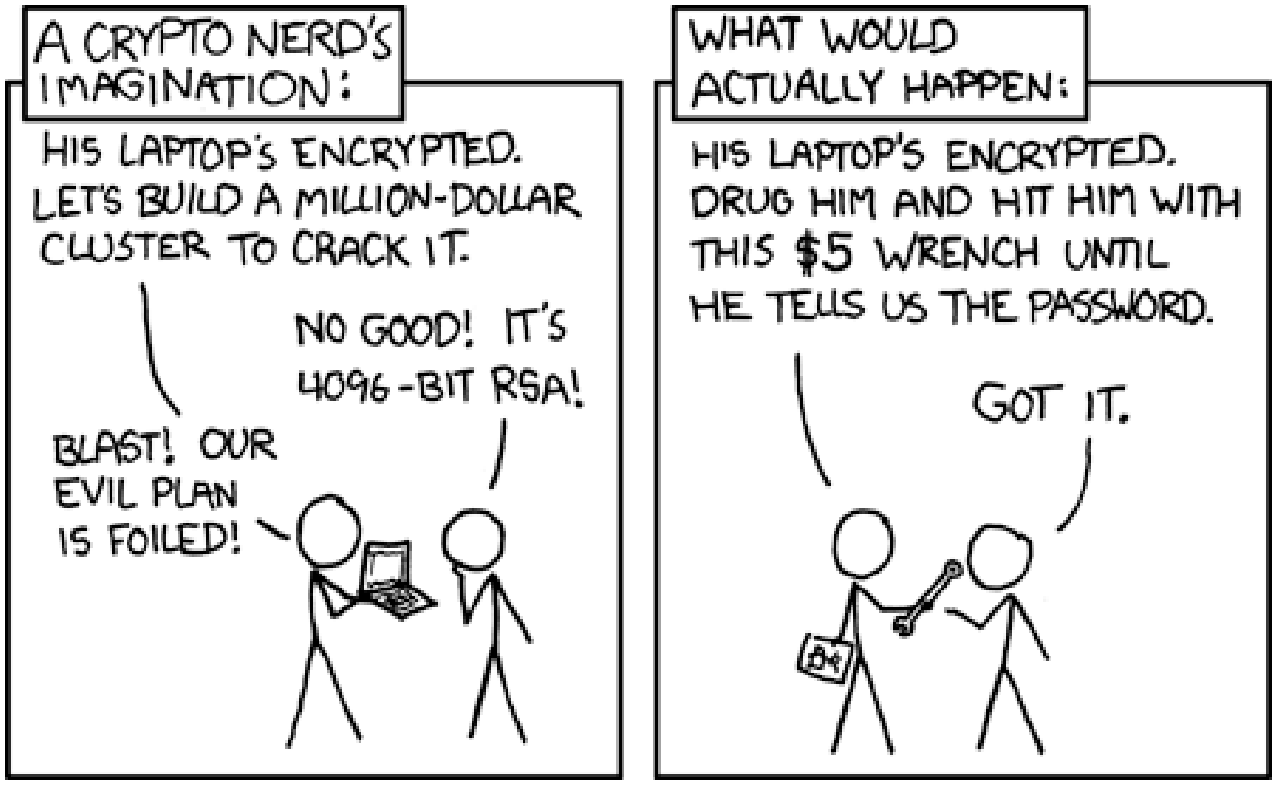
Une serrure éléctronique à 1300$, certifiée par le département de la sécurité (Homeland security), a été ouverte en quelques secondes en utilisant 5 techniques différentes. La plus simple utilisant un trombone, la plus drôle utilisant un maillet...

Social engineering

``Bugs in the human hardware''

De l'art d'extirper frauduleusement des informations à l'insu de son interlocuteur

De l'art de manipuler un interlocuteur à son insu



Skimming

La préhistoire

Les temps modernes

Virus(ing)

Du gâteau à l'ours bogué...

The cookie monster, 1970

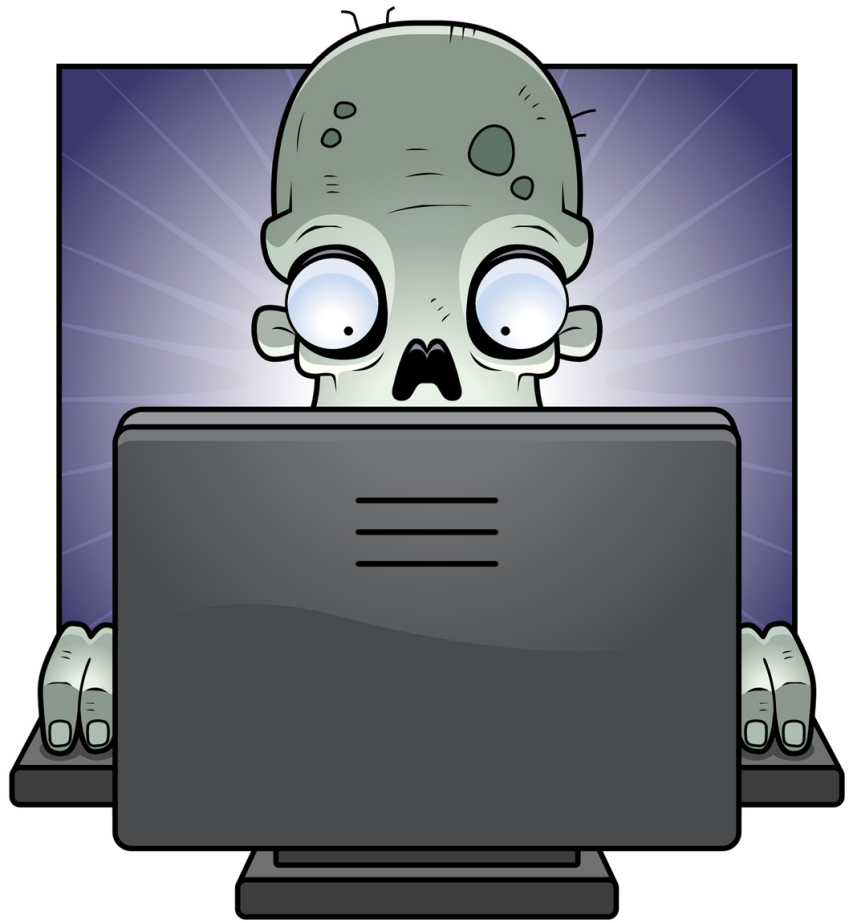
```
Cookie, cookie, give me a cookie.
...
Oh, Thank you
```

W32/Bugbear.B@mm, 2003

```
1natbanker.com 1nationalbank.com 1stbk.com 1stfed.com 1stfederal.com
1stnatbank.com1stnationalbank.com 1stnb.com 1stnewrichmond.com
1stsecuritybank.com 1stsource.com 365online.com 53.com
abbeynational.co.uk abbybank.com abingtonbank.com abnamro.be
abramsbank.com abtbank.com accbank.ie acommunitybk.com...
```

Votre ordinateur est-il un zombie ?

Spppaaammmmm... Je veux du spaaaaaaaaammmm



Place a bowl full of brains in front of it and see if you get a response (slashdot).

Script Kiddies

et l'incommensurable pouvoir de l'ignorance

```
...
<bitchchecker> shut up i hack you
<Elch> ok, i'm quiet, hope you don't show us how good a hacker you are ^^
<bitchchecker> tell me your network number man then you're dead
<Elch> Eh, it's 129.0.0.1
<Elch> or maybe 127.0.0.1
<Elch> yes exactly that's it : 127.0.0.1 I'm waiting for you great attack
<bitchchecker> in five minutes your hard drive is deleted
<Elch> Now I'm frightened
<bitchchecker> shut up you'll be gone
<bitchchecker> i have a program where i enter your ip and you're dead
<bitchchecker> say goodbye
<Elch> to whom?
<bitchchecker> to you man
<bitchchecker> buy buy
<Elch> I'm shivering thinking about such great HackOrs like you
* bitchchecker Quit (Ping timeout#)
```

Quelques minutes après...

```
* bitchchecker  has joined #stopHipHop
<bitchchecker> dude be happy my pc crashed otherwise you'd be gone
<Metanot> lol
```

Et ça continue encore et encore...

(C'est que le début d'accord, d'accord...)

2001-2002

- Noms de domaine parasites
- Attaque des DNS primaires (9/13)
- Vote éléctronique
- YES cards

2003-2004

- Peer to peer et malware
- Attaque sur GNU et linux
- Vol de données
- Loi Economie Numérique

2005-2006

- Nouvelles cibles : GSM, WiFi, etc.
- Botnets et attaques commanditées
- Attaques 0-day
- Les mules

2007-2008

- MMORPG
- Réseaux sociaux
- Piratage du hardware
- Contrefaçon

(36 15) EULA

End User License Agreement

Gamestation.co.uk

By placing an order via this Web site on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant Us a non transferable option to claim, for now and for ever more, ***your immortal soul****. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamesation.co.uk or one of its duly authorised minions... We reserve the right to serve such notice in 6 (six) foot high letters of fire, however we can accept no liability for any loss or damage caused by such an act. If you a) do not believe you have an immortal soul, b) have already given it to another party, or c) do not wish to grant Us such a license, please click the link below to nullify this sub-clause and proceed with your transaction.*

Tuto4pc

`http://streisand.me/tuto4pc.htm`

Les informations communiquées par les utilisateurs seront conservées dans un fichier informatisé appartenant à la société tuto4pc et sont susceptibles d'être communiquées aux partenaires commerciaux de tuto4pc, et/ou a tout tiers...

Kill games

Dexter est un amateur...

Elvis Pressley est vivant !

Des hackers ont trouvé des techniques permettant de faire des copies de passeports RFID et contourner les procédures d'authentification RFID.

Assassinats ciblés

En lisant à distance la puce, ... BOOM !

War games

Pour une frappe légère, presser A

Estonie (2007)

- Vise les sites web des banques, journaux, ministères, etc.
- La Russie suspectée (en représaille au déplacement d'une statue)
- Conduit la plupart des pays à reconsidérer leur position

STUXNET (2010)

- Attaque ciblée sur les systèmes Siemens-SCADA iraniens (60% des infections)
- 4 attaques zero-day incluses
- Modification de la vitesse des centrifugeuses
- Les Etats-Unis et Israël sont largement "suspectés"

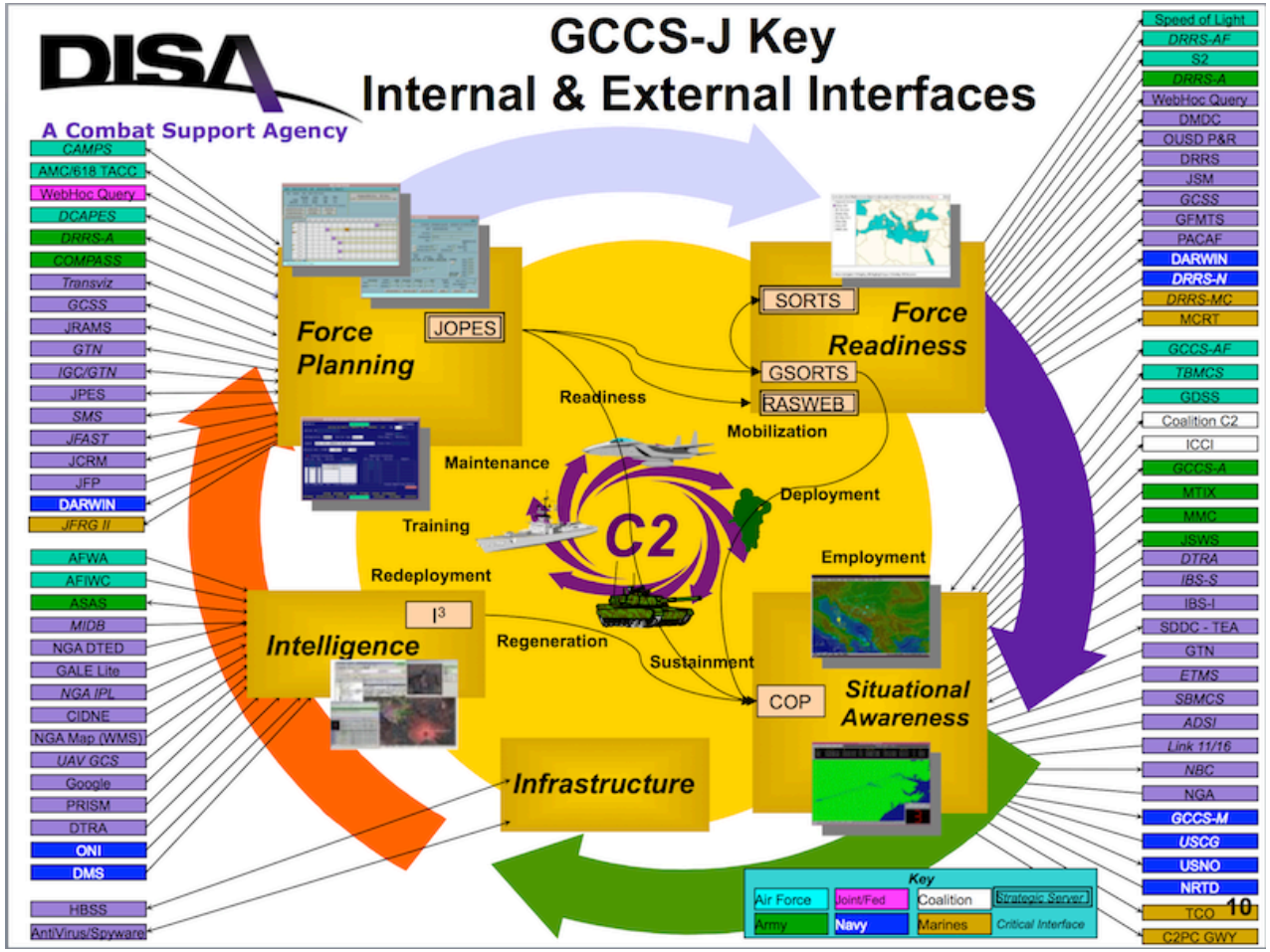
Data games

Vos meilleurs ennemis...

L'Agence nationale de sécurité américaine (NSA) et le FBI ont accès aux serveurs de neuf géants américains de l'internet, dont Microsoft, Yahoo !, Google et Facebook, pour y surveiller les activités d'étrangers, ont révélé le Washington Post et le Guardian **jeudi 6 juin 2013**.

Où est Charlie (PRISM) ?

reflets.info/prism-lets-have-a-look-at-the-big-picture/



Vie privée

Vie publique

Eric Schmidt (Google)

"If you have something you don't want anyone to know, maybe you shouldn't be doing it in the first place."

Mark Zuckerberg (Facebook)

"The age of privacy is over."

Scott McNealy (Sun)

"You have zero privacy anyway. Get over it."

L'utilisateur et ses mots de passes

azerty, gandalf, toto, ...

Utilisateur lambda

Porte d'entrée privilégiée dans le système et accès aux ressources.

Les (très) mauvais mots de passes

- Nom ou prénom de vous ou mari/femme/parents/chien/chat/tortue...
- Nom de personnages (Bond, Gandalf, Wizard, ...)
- Nom ou prénom en général
- Date de naissance, immatriculation, sécurité sociale, lieu
- Nom commun (français ou étranger) / noms propres
- Motifs clavier ou numérique (azerty, 9876543210, etc.)
- Inversion des lettres(1/i, 0/O, @/a)

Toute combinaison de ces motifs est un mauvais mot de passe.

Tout mot de passe rendu public doit être changé.

L'utilisateur et ses mots de passes

!NvRMd19.5940!AyS01(

Les bons mots de passes

- Première lettre de chaque mot d'une phrase.
- Utilisation de signes de ponctuation.
- Utilisation de majuscules et chiffres.
- Facile à retenir pour vous, difficile à trouver pour quelqu'un.
- Facile à taper au clavier.
- Ne jamais écrire un mot de passe où que ce soit.

Exemples

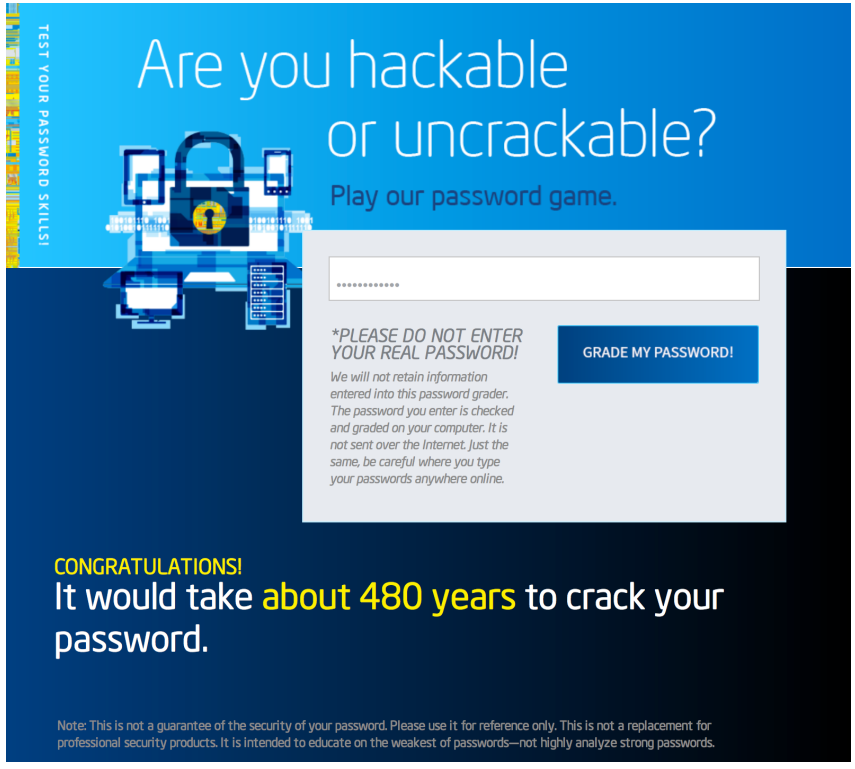
- "Ma tortue s'appelle Achille" $\longrightarrow$ **`Mts'aA`**
- "Et mon chien c'est Toto" $\longrightarrow$ **`Emcc'eT`**

`Mts'aA Emc'eT` est maintenant un mauvais mot de passe.

Analyse d'un hack

(`arstechnica.com/security/2013/05/`)

- 16449 mots de passes "hashés", MD5
- `5f4dcc3b5aa765d61d8327deb` → "password"
- Cracker inexperimenté : 47%
- Cracker expert : 90%
- `k1araj0hns0n`
  `Sh1a-labe0uf,`
  `gonefishing1125`



("Mot de Passe" est donc un bon mot de passe...)

L'utilisateur lambda

oui, oui, encore lui...

Le mail

- Vérifier la provenance des emails
- Ne pas cliquer sur les liens
  → `JessicaAlbaNue.jpg.vbs`

Logiciels divers et variés

- `WoWKeyGen.exe`
- Fonctionnalités exactes ?
- Vérification des fichiers : MD5

Utilisation des logiciels

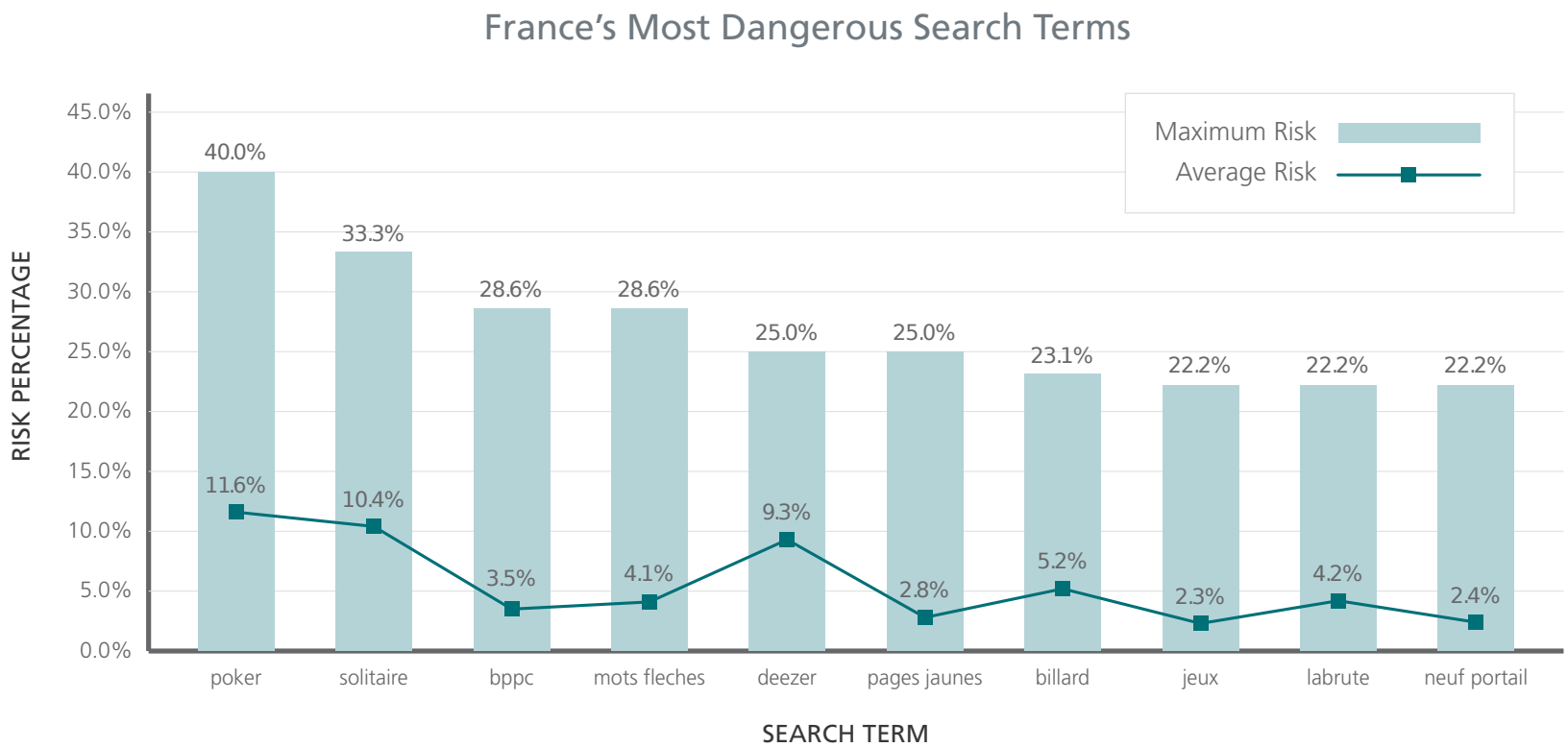
- Droits root requis ?

Web & mots fléchés

Mais où va t'on ?

McAfee®

Europe



arstechnica.com/information-technology/2013/06/download-me-saying-yes-to-the-webs-most-dangerous-search-terms/

Retour à Hollywood

Alors, ça, c'est fait...

Hacker les caméras de surveillance

2012 - http ://chess.bitnik.org/about.html

Hacker un immeuble

1995 - et faire un tetris géant...

Hacker une voiture

Avril 2011 - Une chanson piégée permet de prendre le contrôle d'une voiture

Hacker un avion

Avril 1013 - Un chercheur montre comment prendre le contrôle des systèmes de vol

Hacker un satellite

Avril 2009 - Attaque "man in the middle", écoute des flux

Hacker un drône

Juin 2012 - Prise de contrôle d'un drône militaire

Hacker un humain

Octobre 2012 - Un hacker parvient à pirater un pacemaker

Pour en savoir plus...

Informations générales

- korben.info
- www.slashdot.org
- www.clusif.asso.fr
- www.laquadrature.net
- reflets.info
- bugbrother.blog.lemonde.fr
- security.ngoinabox.org/fr
- arstechnica.com

Cryptographie

- www.truecrypt.org/
- www.gnupg.org/

Anonymat

- www.vpnblog.net
- www.torproject.org