

Sensibilisation aux menaces Internet & Formation aux bonnes pratiques pour les utilisateurs (BPU) de systèmes informatiques



Module 1
Panorama des menaces SSI

Module 2
Les règles élémentaires de
protection

SOMMAIRE

P. 2

<http://tomnichols.net/blog/2011/11/16/meeting-cyber-attacks-with-military-force/>



- Doctrine de l'Etat
- Origines des menaces
- Vos données personnelles
- Quelles réponses ?

DOCTRINE DE L'ETAT, LE RÉSUMÉ

P. 3



protection des systèmes d'information = **une priorité nationale**



**AVANT
MAINTENANT**

Défense périphérique et passive (uniquement ASR)
Défense active en profondeur (tout le monde)



pas de parade absolue contre les attaques évoluées
Se doter d'une capacité de gestion de crise et d'après-crise



la sécurité informatique est
largement dépendante des comportements des utilisateurs
des systèmes d'information

RAPPORT D'INFORMATION SUR LA CYBERDÉFENSE (Juillet 2012) « *La cyberdéfense : un enjeu mondial, une priorité nationale* »



 « ...il est complexe de se protéger contre les attaques informatiques, car les techniques évoluent sans cesse et il n'existe pas de parade absolue dans le 'cyberespace' »

 « ...la sécurité informatique est largement dépendante des comportements des utilisateurs des systèmes d'information, qui considèrent souvent les règles de sécurité comme autant de contraintes. »

« La conclusion que je tire de tout cela est que nous voyons bien s'ouvrir, pour les années qui viennent, un nouveau champ de bataille, avec des stratégies et des effets très spécifiques. »

« ...la sécurité de l'ensemble de la société de l'information nécessite que **chacun soit sensibilisé aux risques et aux menaces et adapte ses comportements et ses pratiques** »
(p 107)



CLASSEMENT DES MENACES

P. 6



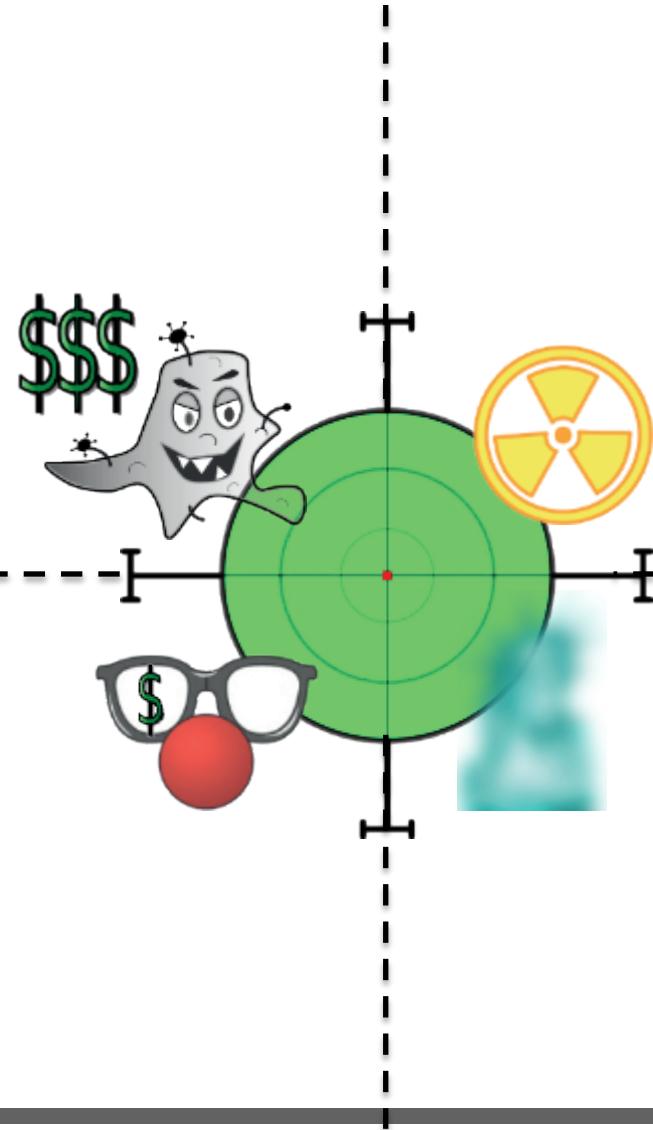
e-Crime organisé



Services d'Etats



Script kiddies



Hacktivistes

"The first known major cyberattack authorized by a U.S. president,"
David E. Sanger, New-York Times 1er juin 2012



2010 - IRAN

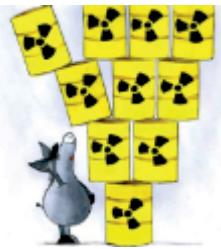
Destructions matérielles dans des usines de traitement de l'uranium
(ver Stuxnet)

2012 - FRANCE

Intrusion dans l'intranet de l'Elysée, extorsion de documents

2013 - USA

Programme de surveillance étatique et collecte d'informations chez les opérateurs et fournisseurs de service (PRISM)



2021 - Monde

Société PEGASSUS



9 juin -> 21 octobre 2013

Le Monde : **306 articles** citent Edward Snowden

Une équipe de 10 journalistes travaillent sur l'histoire du programme PRISM et la surveillance de la France par les services secrets US

Editorial du 21 octobre

« Les "révélations Snowden" ne visent pas à affaiblir les sociétés démocratiques mais à les consolider, à éveiller les consciences sur les risques que comportent pour nos valeurs ce gigantesque ratissage de données permettant de lire dans nos vies, nos contacts, nos opinions, comme à livre ouvert. »

LUNDI 21 OCTOBRE 2013

P. 9

Le Monde*Edition du lundi 21 octobre 2013*

Comment la NSA espionne la France

Les documents que "Le Monde" a pu consulter montrent comment le renseignement américain a ciblé la France, ses institutions, ses entreprises et ses citoyens.



Inside the NSA's web of surveillance

In the course of the summer, the documents forwarded to several of the media by Edward Snowden have contributed to lifting the veil on the extent of the surveillance and espionage carried out by the NSA, the American National Security Agency and its allies.



Editorial du "Monde" : combattre Big Brother

Les "révélations Snowden" ne visent pas à affaiblir les sociétés démocratiques mais à les consolider.



Les services secrets américains très intéressés par Wanadoo et Alcatel-Lucent

Les adresses de messagerie de l'entreprise franco-américaine de télécommunications et celles de l'ancienne filiale d'Orange, qui compte encore 4,5 millions d'utilisateurs, ont été espionnées.



Plongée dans la "pieuvre" de la cybersurveillance de la NSA

Infographie interactive. Les documents rendus publics par Edward Snowden dressent le portrait complexe de la cybersurveillance américaine, pilotée par la toute-puissante NSA.



Les révélations d'Edward Snowden, un séisme planétaire

L'affaire de la NSA a déclenché des crises diplomatiques entre les Etats-Unis et leurs alliés et secoué les géants de l'Internet.

En images**ABONNEZ-VOUS**

Les révélations d'Edward Snowden, un séisme planétaire

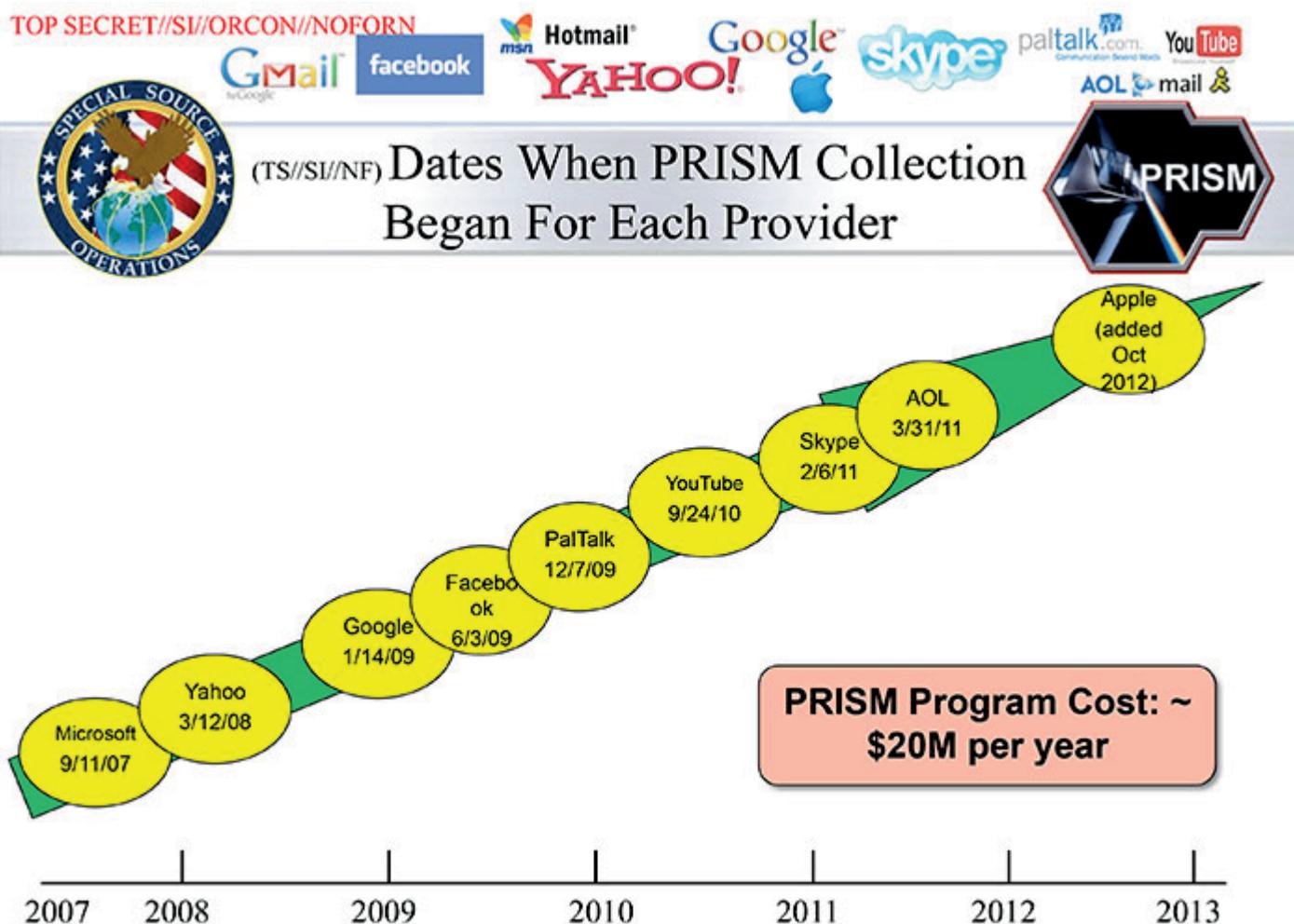
Le Monde.fr | 21.10.2013 à 06h01 • Mis à jour le 21.10.2013 à 08h55 |

Par Philippe Bernard et Marie Jégo (Moscou, correspondante)



Alcatel•Lucent

- 62,5 millions de données téléphoniques sont collectés en France du 10 décembre 2012 au 8 janvier 2013
- Cibles : Alcatel Lucent, Wanadoo
- Intrusion massive de la NSA, via Upstream, sur l'adresse wanadoo.fr
- Utilisation de 45 000 « sélecteurs »
- *Interception de SMS en fonction de mots clés*



TOP SECRET//SI//ORCON//NOFORN

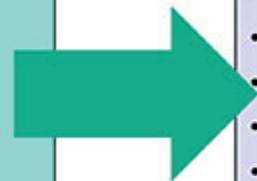


(TS//SI//NF) PRISM Collection Details



Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple



What Will You Receive in Collection
(Surveillance and Stored Comms)?
It varies by provider. In general:

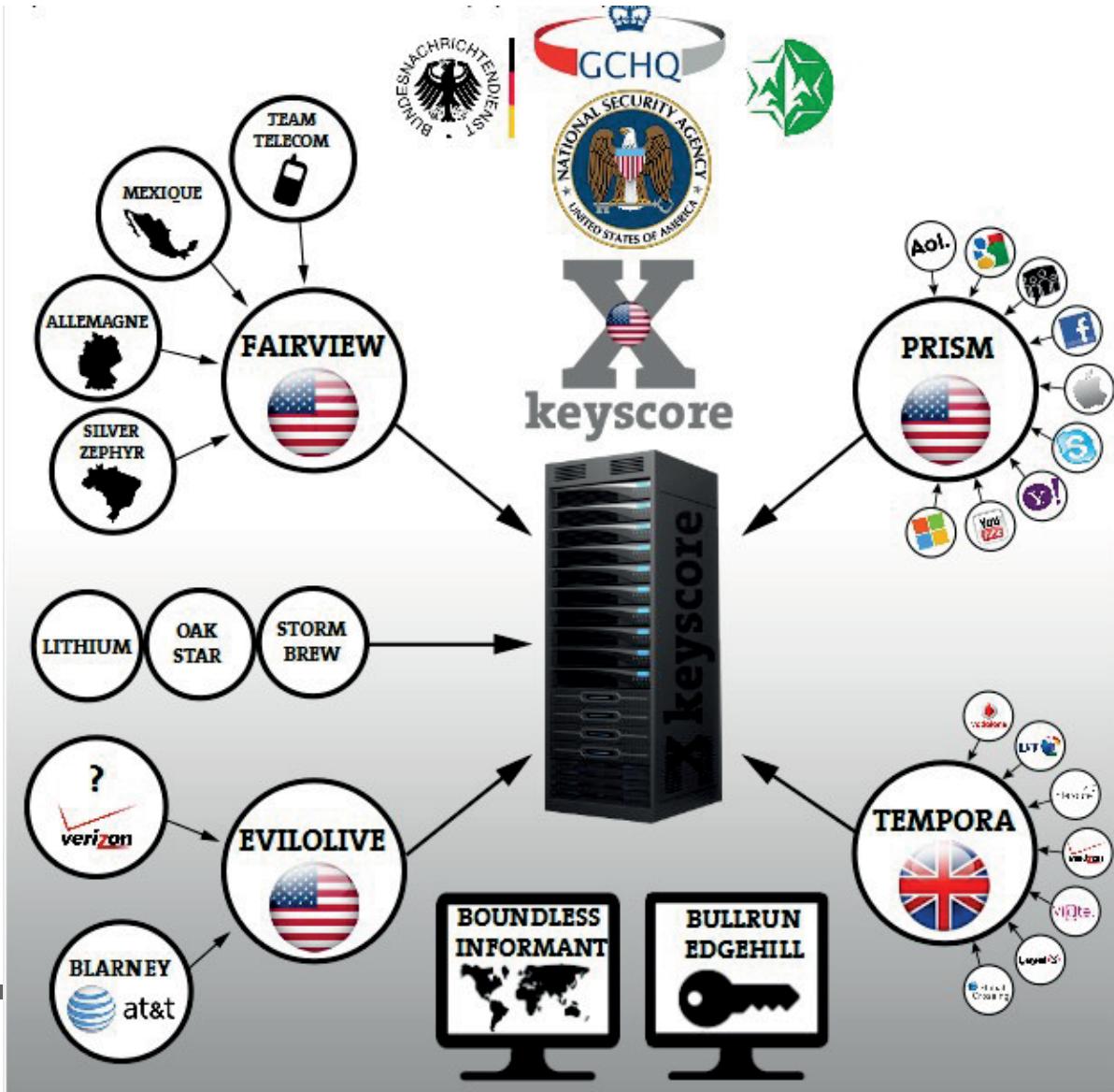
- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:

[Go PRISMFAA](#)

TOP SECRET//SI//ORCON//NOFORN

XKeyscore, l'outil de la NSA pour examiner "quasiment tout ce que fait un individu sur le Web"



http://www.lemonde.fr/technologies/visuel_interactif/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html

des recherches extrêmement précises

P. 14

- Show me all the encrypted word documents from Iran
- Show me all PGP usage in Iran



- My target speaks German but is in Pakistan – how can I find him?



- I have a Jihadist document that has been passed around through numerous people, who wrote this and where were they?



850 000 employées et contractuels de la NSA possèdent l'accréditation top secret

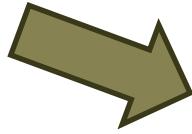


Le 25 Novembre 2013

La NSA a infiltré 50 000 réseaux informatiques avec des malwares

- utilise un processus connu sous le nom de « Computer Network Exploitation » (CNE)
- exploité dans plus de 50 000 localisations.
- Pour se faire, ce système installe des malwares chargés de récupérer des données sensibles.
- Création d'une unité spéciale appelée TAO (Tailored Access Operations) qui regroupe une centaine de hackers
- les malwares sont dormants et peuvent être activés à distance par simple clic.

http://en.wikipedia.org/wiki/Tailored_Access_Operations



« L'espionnage serait peut-être tolérable s'il pouvait être exercé par d'honnêtes gens. »

Montesquieu, *De l'esprit des lois*

LES SERVICES D'ETAT, LE RÉSUMÉ

P. 17



Vers une force de dissuasion numérique ?



Les mécanismes d'infection sont connus

Les attaques évoluées
d'origine étatiques sont
indétectables



Advanced
Persistent
Threats

- Furtivité
- Stratégie d'attaque
- Reproduction, évolution et disparition programmées
- Aucun outil conventionnel de sécurité ne permet de déceler un APT



BOTNET WADELAC, DÉMANTELÉ EN 2009

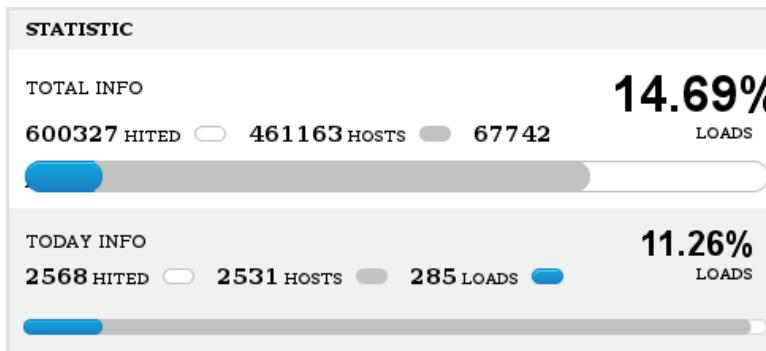
P. 18



LE E-CRIME ORGANISÉ

P. 19

Copie d'écran d'une console *BLACKHOLE Exploit Kit*



EXPLOITS		LOADS	% ↑
Java Rhino >		54430	79.89
PDF LIBTIFF >		8771	12.87
PDF ALL >		1983	2.91
Java OBE >		1396	2.05
FLASH >		571	0.84
HCP >		503	0.74
MDAC >		475	0.70

OS	HITS	HOSTS	LOADS ↑	%
Windows 7	290890	219291	28879	13.17
Windows XP	163899	128063	23110	18.05
Windows Vista	107408	81266	15648	19.26
Windows 2003	700	529	158	29.87
Windows 2000	342	290	27	9.34
Windows NT	173	145	6	4.14
Windows 98	79	75	4	5.41
Mac OS	32982	30799	1	0.00
Linux	3803	3672	1	0.03
Windows 95	8	8	0	0.00

BROWSERS ↓	HITS	HOSTS	LOADS	%
Aol >	4	4	0	0.00
Chrome >	27574	23726	576	2.43
Firefox >	174630	142879	25778	18.05
MSIE >	348070	256067	40008	15.63
Mozilla >	3889	3594	11	0.31
Opera >	7900	5429	882	16.25
Safari >	38213	35387	681	1.92

THREADS ↓	HITS	HOSTS	LOADS	%
10k US >	1775	1729	135	7.81
2k loads AU >	18956	17345	1493	8.61
2k uk loads >	29509	26810	3506	13.08
3k UK loads mattew >	22449	20091	3010	14.98
50k AU >	14244	12949	1920	14.83
50k CA i EU >	9159	8547	1807	21.14

COUNTRIES	HITS ↑	HOSTS	LOADS	%
France	306438	209039	30779	14.72
United Kingdom	103352	89037	11190	12.57
United States	98661	86664	14679	16.95
Australia	53145	46296	5925	12.80
Germany	10476	9874	1468	14.88
Russian Federation	9871	4149	532	12.83
Canada	6994	5958	1041	17.47
Spain	4636	4367	1200	27.48
Italy	3471	3190	409	12.83
Romania	856	603	115	19.13

LMI LEMONDE INFORMATIQUE

Le 18 Octobre 2013

Oracle corrige 127 vulnérabilités sur ses produits



Crédits Photo: D.R.

Oracle a corrigé mardi 127 vulnérabilités dans Java, sa base de données et d'autres produits qui auraient pu permettre aux pirates de prendre la main sur les systèmes.

Dans le cadre du plan annoncé précédemment par Oracle et visant à augmenter la fréquence des mises à jour de sécurité Java d'une tous les quatre mois à une tous les trois mois, l'éditeur a intégré Java dans son Critical Patch Update (CPU) trimestriel. La nouvelle version Java SE 7 Update 45 (7u45) publiée mardi contient ainsi 51 des 127 correctifs de sécurité présents dans le CPU. Cinquante de ces correctifs concernent d'ailleurs des failles qui peuvent être exploitées à distance sans authentification. 12 d'entre elles sont en outre marquées du

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir.

- CERTA-2013-AVI-421 Multiples vulnérabilités dans Oracle Database Server (17 juillet 2013)
- CERTA-2013-AVI-420 Vulnérabilité dans Oracle Industry Applications (17 juillet 2013)
- CERTA-2013-AVI-419 Multiples vulnérabilités dans Oracle MySQL (17 juillet 2013)
- CERTA-2013-AVI-418 Vulnérabilité dans Oracle iLearning (17 juillet 2013)
- CERTA-2013-AVI-417 Multiples vulnérabilités dans Oracle Virtualization (17 juillet 2013)
- CERTA-2013-AVI-416 Multiples vulnérabilités dans Oracle Solaris (17 juillet 2013)
- CERTA-2013-AVI-415 Multiples vulnérabilités dans Moodle (17 juillet 2013)
- CERTA-2013-AVI-414 Vulnérabilité dans PHP (16 juillet 2013)
- CERTA-2013-AVI-413 Multiples vulnérabilités dans Juniper Junos (15 juillet 2013)



- CERTA-2013-ALE-002 Vulnérabilités dans Adobe Reader et Acrobat (Corrigée le 21 février 2013)**

- CERTA-2013-AVI-408 Multiples vulnérabilités dans Google Chrome (10 juillet 2013)
- CERTA-2013-AVI-407 Multiples vulnérabilités dans Adobe ColdFusion (10 juillet 2013)
- CERTA-2013-AVI-406 Vulnérabilité dans Adobe Shockwave Player (10 juillet 2013)**
- CERTA-2013-AVI-405 Multiples vulnérabilités dans Adobe Flash Player (10 juillet 2013)**
- CERTA-2013-AVI-404 Vulnérabilité dans Microsoft Windows Defender (10 juillet 2013)
- CERTA-2013-AVI-403 Vulnérabilité dans Microsoft Windows Media Format Runtime (10 juillet 2013)
- CERTA-2013-AVI-402 Vulnérabilité dans Microsoft DirectShow (10 juillet 2013)
- CERTA-2013-AVI-401 Multiples vulnérabilités dans Microsoft Internet Explorer (10 juillet 2013)
- CERTA-2013-AVI-400 Vulnérabilité dans Microsoft GDI+ (10 juillet 2013)
- CERTA-2013-AVI-399 Multiples vulnérabilités dans le noyau Microsoft Windows (10 juillet 2013)
- CERTA-2013-AVI-398 Multiples vulnérabilités dans Microsoft Framework .net et Silverlight (10 juillet 2013)
- CERTA-2013-AVI-394 Vulnérabilité dans Citrix XenServer (08 juillet 2013)
- CERTA-2013-AVI-393 Multiples vulnérabilités dans Apple OS X (08 juillet 2013)



- CERTA-2013-AVI-361 Multiples vulnérabilités dans Oracle Java (19 juin 2013)**



- CERTA-2013-AVI-354 Vulnérabilité dans Microsoft Office (12 juin 2013)**



BOTNET FLASHBACK : 600 000 MAC OSX INFECTÉS

P. 22

Découvert par l'éditeur antivirus russe Dr. Web (avril 2012)

Faille : logiciel JAVA

Vecteur d'infection : + 4 000 000 pages web compromises (dont dlink.com)

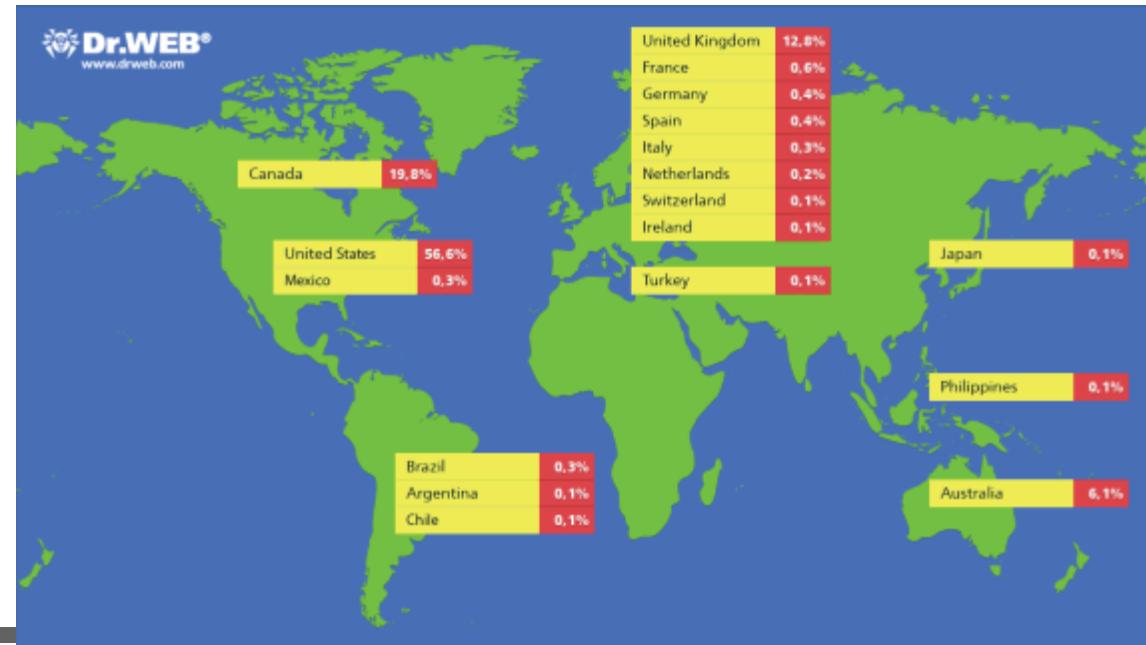
Une visite d'un site infecté suffit à contaminer le Mac

« Apple en faute ?

Qu'il soit dangereux ou non, Flashback-k révèle un problème dans la façon dont on pense la sécurité au sein d'Apple.

La faille qu'il exploite est loin d'être inconnue. Depuis le mois de février, Oracle propose [une mise à jour critique pour la corriger](#). Les utilisateurs de Windows qui utilisent Java l'ont par exemple obtenue grâce à l'outil de mise à jour de Java. Mais sur Mac, c'est Apple qui centralise ces mises à jour de sécurité et qui les distribue par l'intermédiaire d'un outil intégré à Mac OS X. Or la marque à la pomme n'avait pas publié ce correctif ! »

<http://www.01net.com/editorial/563178/le-botnet-flashback-met-a-mal-le-sentiment-d-invulnerabilite-sur-mac/>





 **Votre ordinateur est bloqué.**

ATTENTION!

Votre ordinateur est bloqué en raison du délit de la loi de la France

On révélait les violations suivantes :

- le fait d'une prise de vues du film, l'inscription ou la transmission des documents du contenu pornographique avec la participation des mineurs, la pornographie mettant en scène des enfants, de la sodomie et des actions violentes en ce qui concerne les enfants. La punition est prévue par l'article (art. 227-23) du Code pénal de la France. Cela est puni par une réclusion pendant de 2 à 5 ans.
- l'exploitation du logiciel avec la violation des droits d'auteur. La punition est prévue par l'article (art 323-2) du Code pénal de la France. Cela est puni par une réclusion pendant de 1 à 3 ans.
- l'envoi de 3 fichiers multimédia avec la violation des droits d'auteur. La punition est prévue par l'article (art. 323-3) du Code pénal de la France. Cela est puni par une réclusion pendant de 1 à 3 ans.

Pour débloquer l'ordinateur, il vous faut payer l'amende conformément par la législation française dans la mesure de 100 euros aux 3 jours à venir. La punition en forme de l'amende est possible seulement à la première violation. À la violation réitérée suivra la responsabilité pénale. Si vous ne payez pas l'amende au délai exactement indiqué, votre ordinateur sera confisqué et votre affaire sera déférée au tribunal. Vous pouvez payer l'amende à notre partenaire avec l'aide des vouchers Ukash. Acquérez ces vouchers Ukash sur la somme 100 euros, puis remplissez une forme avec les codes et les sommes des vouchers. appuyez sur un bouton «Payer l'amende». Votre ordinateur sera débloqué à la fois après un contrôle de l'authenticité Ukash du voucher. D'habitude 1-4 heures. Trouvez un point de vente plus proche Commandez Ukash: 100 euros Recevez un code Ukash (de 19 chiffres)

Où puis-je acheter un voucher Ukash?

Acheter Ukash dans plus de 20.000 points de vente en France. Vous pouvez Obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques GAB, y compris les bureaux de tabac, Presse et stations service.

 Tabac presse – Ukash est disponible dans des milliers Bureaux de tabac.

 Tonéo – Ukash est maintenant disponible avec la Carte Toneo.

www.beCHARGE.BE Becharge – Utilisez Ukash en ligne 24/7 avec Visa / MasterCard ou Carte Bancaire.

payer une amende de 100 € **OK** 

LE E-CRIME ORGANISÉ

P.



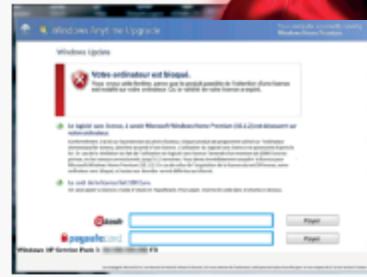
Lyposit FR (09-2012)



Metsnu FR (05-2012)



Metsnu FR (07-2012)



Metsnu FR (08-2012)



Netsu FR (01-2013)



Netsu FR (10-2012)



Pexby FR (03-2012)



Ransom.IF (FR) (08-2012)

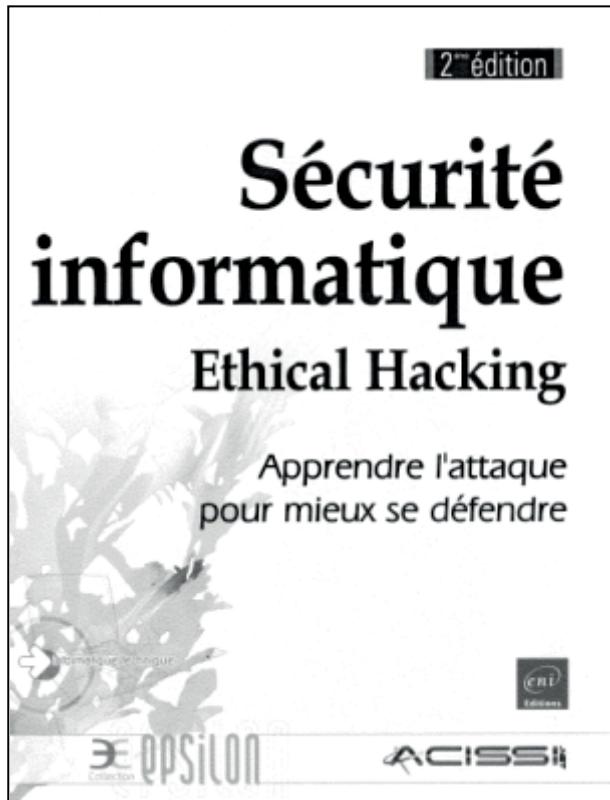


C.



LES SCRIPT KIDDIES

P. 25



LES SCRIPT KIDDIES

P. 26

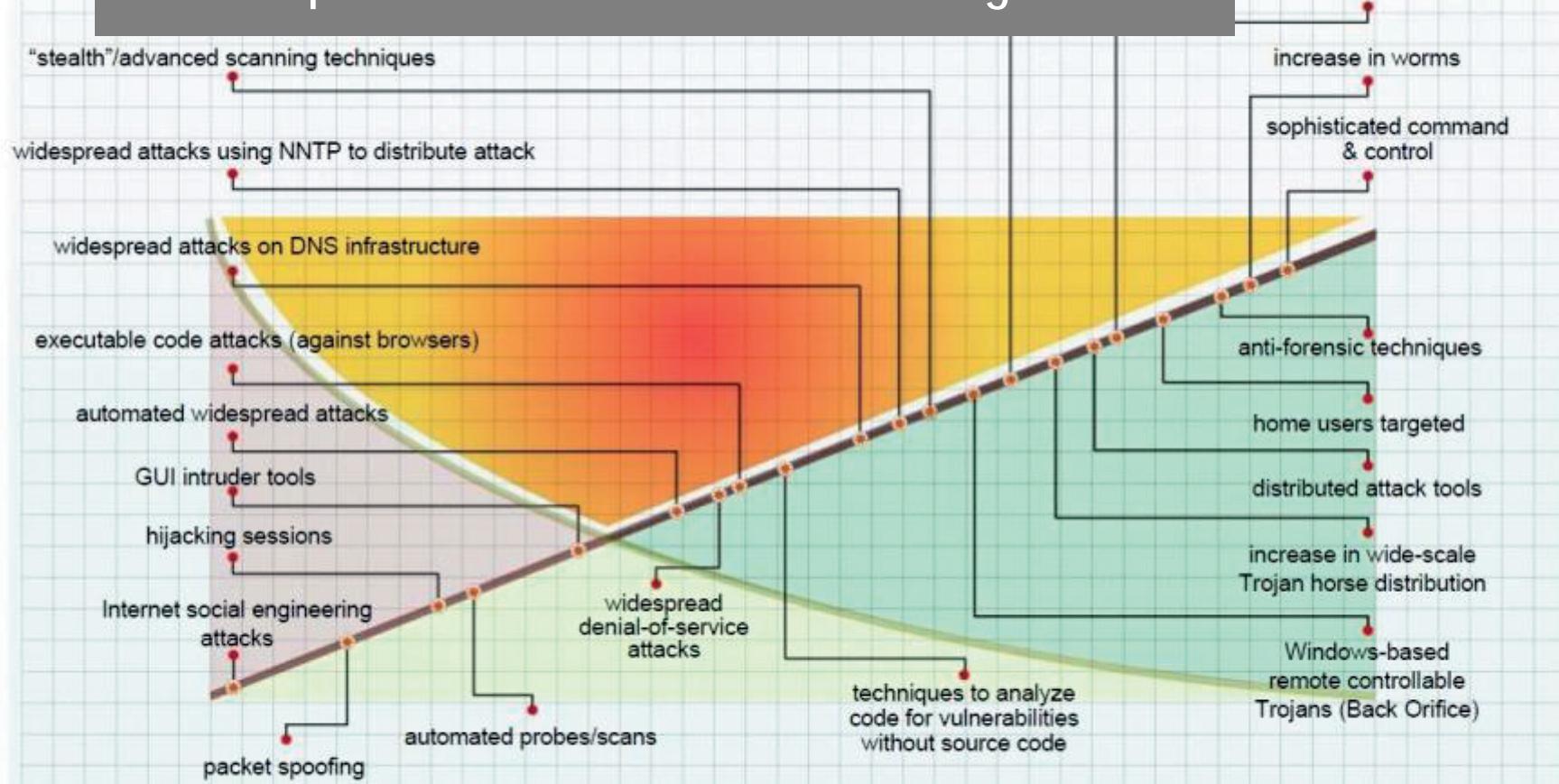


AUTRICHE - Arrestation d'un adolescent soupçonné d'avoir attaqué les serveurs de 259 sociétés en trois mois : âgé de 15 ans, il a été arrêté par la police autrichienne qui l'accuse de défigurations de sites Internet et d'exfiltrations de données sensibles. Il a utilisé plusieurs **logiciels largement diffusés sur internet** dont certains logiciels d'anonymisation.

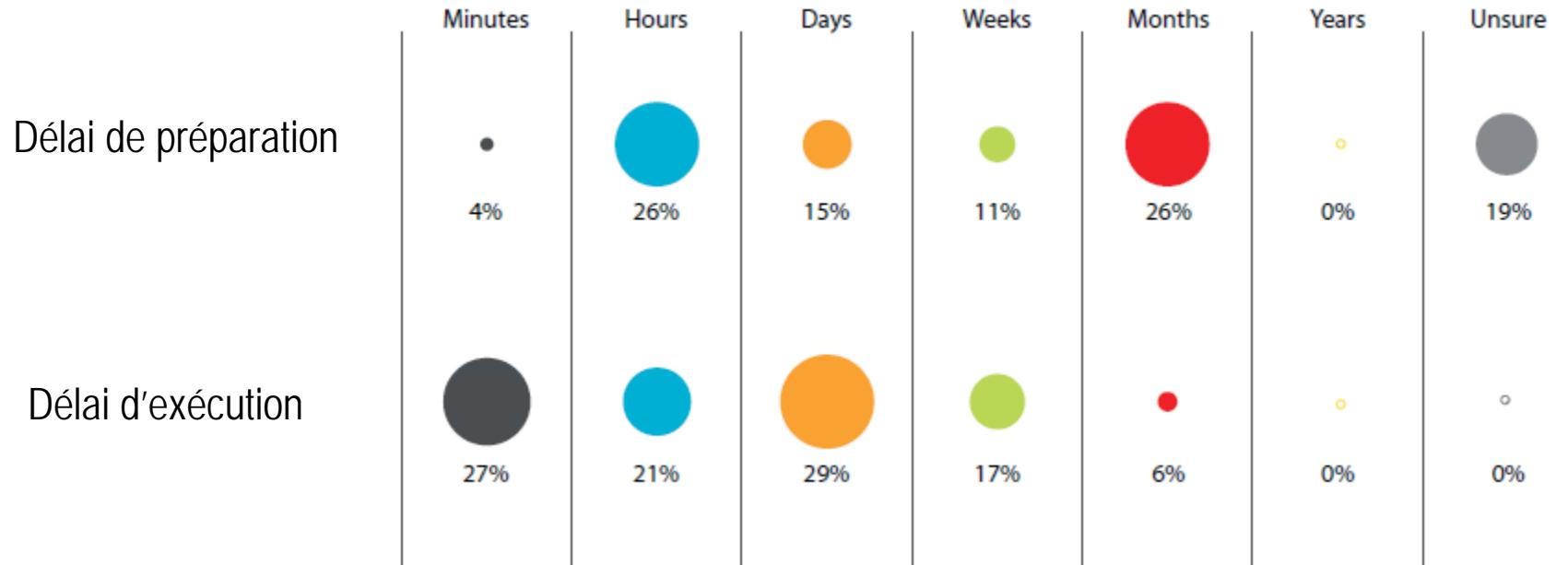
([Kurier](#) du 13/04/12, [ZDNet](#) du 17/04/12)



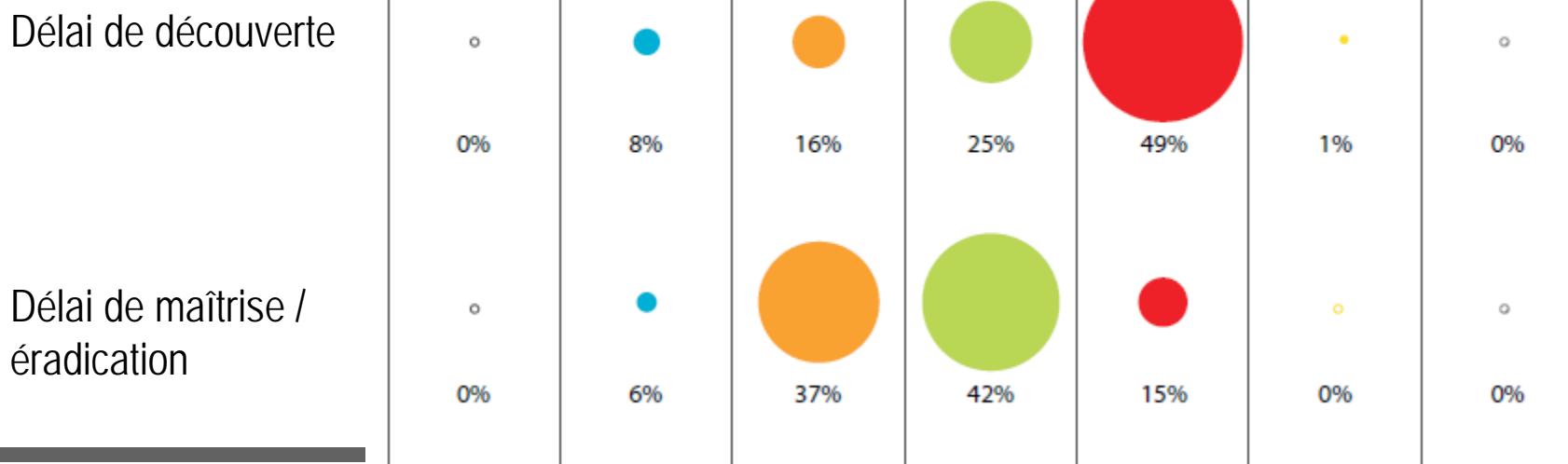
Attack sophistication vs. intruder knowledge



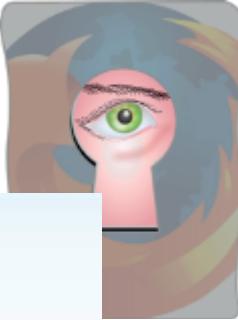
Phase d'attaque



Infection - Compromission



LE BUSINESS DES DONNÉES PERSONNELLES



P. 29

The screenshot shows the homepage of EasyFichiers.com. At the top, there is a navigation bar with a house icon, a user icon, and dropdown menus for "Fichiers de Particuliers" and "Fichiers d'Entreprises". A search bar is also present. Below the navigation, a breadcrumb trail shows the user has navigated from "Accueil" to "Fichiers de Particuliers" and then to "Fichier Propriétaires de piscines".

The main content area features a product image for "Propriétaires de piscines", which is a database of residential addresses and phone numbers for individuals who own a home with a pool. The image includes a small logo and two orange starburst badges labeled "Source Officielle". To the right of the image, the title "Fichier Propriétaires de piscines" is displayed, followed by a description: "Fichier d'adresses postales et téléphones de particuliers qui ont une maison avec une piscine." Below this, there are icons for a magnifying glass, a mail envelope, and a telephone receiver. An orange button labeled "Devis immédiat ▶" is prominently featured. At the bottom, there are two options: "Mensuelle" (Monthly) with a number 5 inside a box, and "Contacts nominatifs" (Nominal contacts) with a small icon.

LE BUSINESS DES DONNÉES PERSONNELLES

P. 30



Détails de votre sélection

Ciblage géographique ALSACE

Régions (1) ALSACE

Propriétaire de piscine (1) Oui

919 contacts
551,4 € HT
669,47 € TTC

Adresse postale + Téléphone
919 contacts **551,4 € HT**

Adresse postale
1 406 contacts **492,1 € HT**

Téléphone
919 contacts **413,55 € HT**

[Maitrisez votre budget](#) >

[Exclude les contacts déjà achetés](#) >

[Voir l'aperçu du fichier](#) >

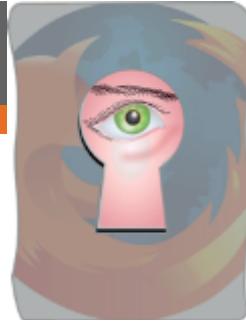
Etape suivante : Critères ►

07 février 2014, par Jérôme Marin

Susan Wojcicki, une spécialiste de la pub à la tête de YouTube



YouTube a une nouvelle patronne: Susan Wojcicki, l'une des employées vedette de Google, la maison-mère de la plate-forme de vidéos. Cette nomination, confirmée mercredi 5 février, pourrait marquer une nouvelle étape dans l'histoire du site, racheté en fin 2006 par le moteur de recherche pour 1,65 milliard de dollars et qui peine encore à s'imposer dans la création de contenus originaux.



EUROPE - *Facebook attaqué en justice pour non-respect de la vie privée* : après avoir demandé la communication des données le concernant auprès du réseau social, un étudiant autrichien a constaté que **Facebook conserve les données personnelles supprimées par l'utilisateur et collecte des informations portant sur des personnes non membres**.

([Écrans.fr](#) du 22/10, [The Register](#) du 23/10, [Europe vs. Facebook](#))

[Les plaintes relatives au respect de la vie privée se multiplient contre Facebook, mais les amendes encourues sont trop peu dissuasives pour que le réseau social modifie ses pratiques.]





MONDE - Comme l'iPhone et Android, Windows Phone 7 collecte les données de géolocalisation des utilisateurs : l'ordiphone transmet à *Microsoft* son numéro de série, ses coordonnées GPS et des informations sur les réseaux GSM (2G et 3G) et Wi-Fi environnants. ([Cnet](#) du 25/04, [Microsoft](#))

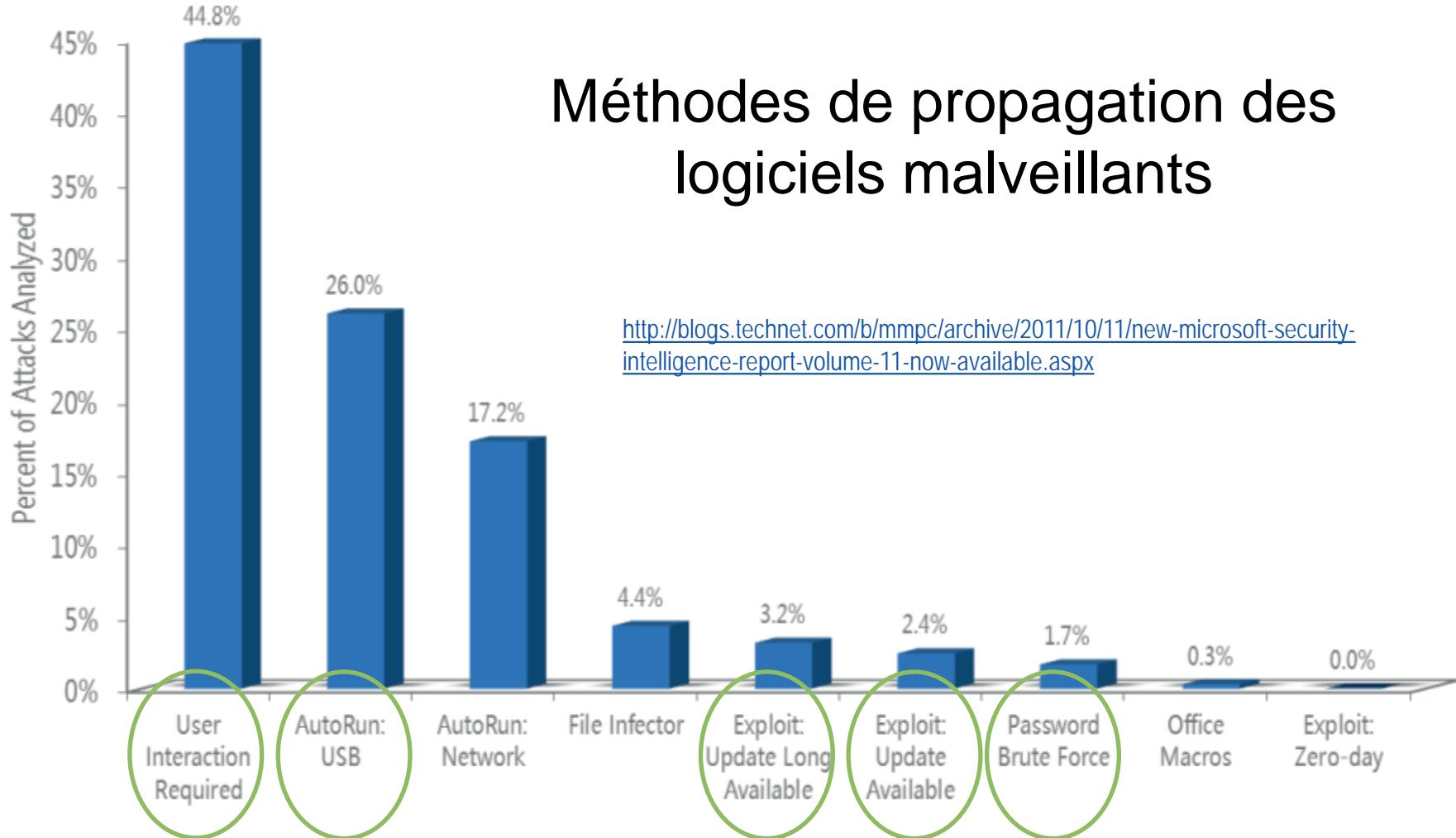


CAMPAGNE ANTI-GOOGLE DE MICROSOFT

P. 34

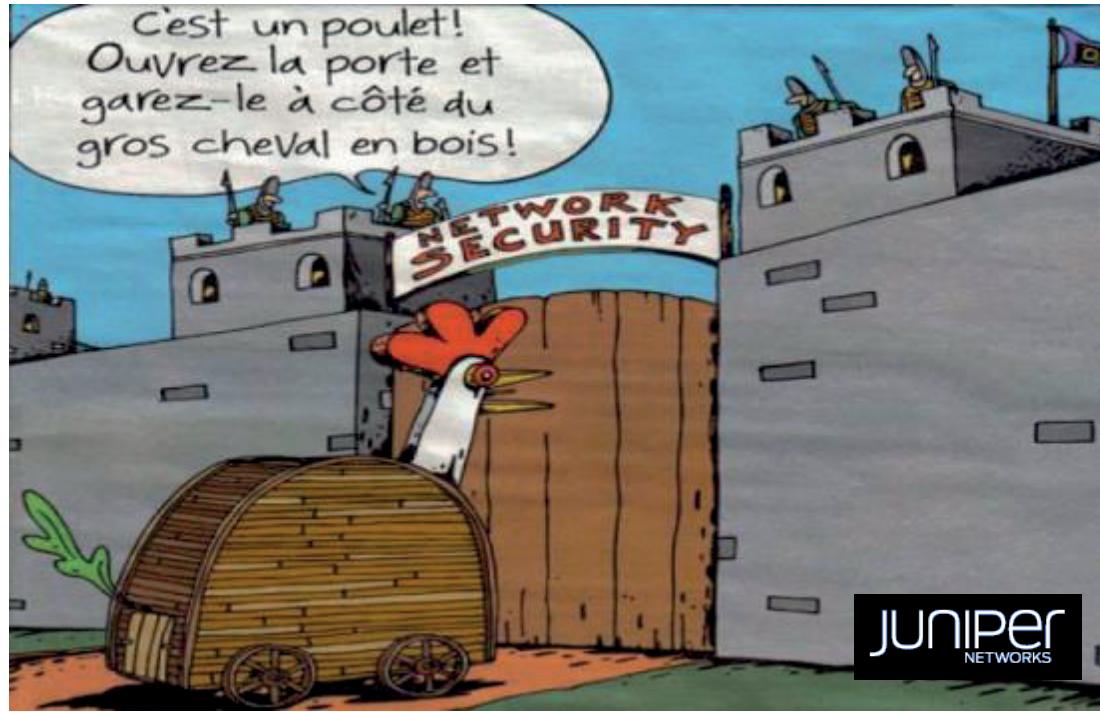


<http://www.scroogled.com/>



QUE FAIRE ?

P. 36



L'attaque d'un poste client est aujourd'hui le moyen le plus utilisé pour pénétrer dans un réseau informatique.

QUE FAIRE ?

P. 37



Tous les internautes sont exposés en permanence à des menaces



Les attaques les plus sophistiquées (APT) sont indétectables



Les autres attaques : protection par l'application des bonnes pratiques (BPU)



Module 2
Les règles élémentaires de
protection