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

Septembre 2013

CERT-OSIRIS

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

protection des systèmes d'information = une priorité nationale

AVANT *Défense périmétrique et passive (uniquement ASR)*
MAINTENANT 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

DOCTRINE DE L'ETAT

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. »

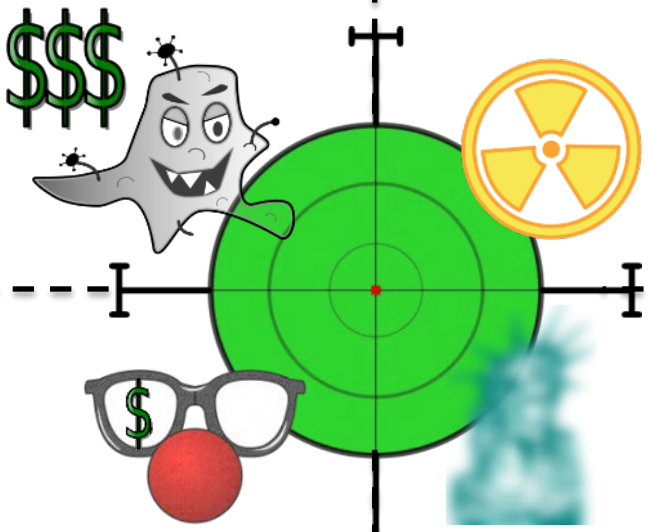
DOCTRINE DE L'ETAT

« ...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

e-Crime organisé

Services d'Etats



Script kiddies

Hacktivistes

LES SERVICES D'ETAT

"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)

Les services d'Etat, le résumé

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

LE E-CRIME ORGANISÉ

STATISTIC

TOTAL INFO

600327 HITED — **461163** HOSTS — **67742** LOADS — **14.69%**

TODAY INFO

2568 HITED — **2531** HOSTS — **285** LOADS — **11.26%**

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

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

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

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

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

Votre ordinateur est bloque.

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 de3 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.
Po ur 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 3era confisqué et votre affaire sera déféré 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 3ur 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)

Ou 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.

Toneo – Ukash est maintenant disponible avec la Carte Toneo.

Becharge – Utilisez Ukash en lign 24/7 avec Visa / MasterCard ou Carte Bancaire.

payer une amende de 100 €

OK

Ukash

LE E-CRIME ORGANISÉ

Lyposit FR (09-2012)

Matsnu FR (05-2012)

Matsnu FR (07-2012)

Matsnu FR (08-2012)

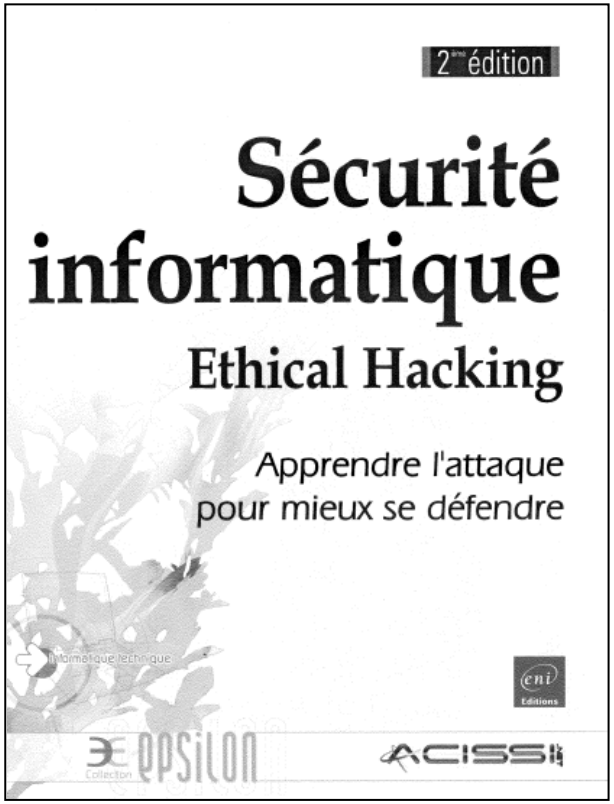
Nertra FR (01-2013)

Nertra FR (10-2012)

Pexby FR (03-2012)

Ransom.IF (FR) (08-2012)

Les Script kiddies



LES SCRIPT KIDDIES

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)

LES SCRIPT KIDDIES

Attack sophistication vs. intruder knowledge

ema

DDoS attacks

"stealth"/advanced scanning techniques

increase in worms

widespread attacks using NNTP to distribute attack

sophisticated command & control

widespread attacks on DNS infrastructure

executable code attacks (against browsers)

anti-forensic techniques

automated widespread attacks

home users targeted

GUI intruder tools

distributed attack tools

hijacking sessions

increase in wide-scale Trojan horse distribution

Internet social engineering attacks

widespread denial-of-service attacks

Windows-based remote controllable Trojans (Back Orifice)

techniques to analyze code for vulnerabilities without source code

automated probes/scans

packet spoofing

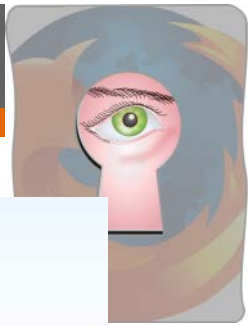
1990

Intruder Knowledge

2004

Attack Sophistication

LE BUSINESS DES DONNÉES PERSONNELLES



LE BUSINESS DES DONNÉES PERSONNELLES

Détails de votre sélection

Ciblage géographique

Régions (1)

ALSACE

Propriétaire de piscine (1)

Oui

919 contacts

551,4 € HT

659,47 € 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

Exclure les contacts déja achetés

Voir l'aperçu du fichier

Etape suivante : Critères

FACEBOOK STOCKE

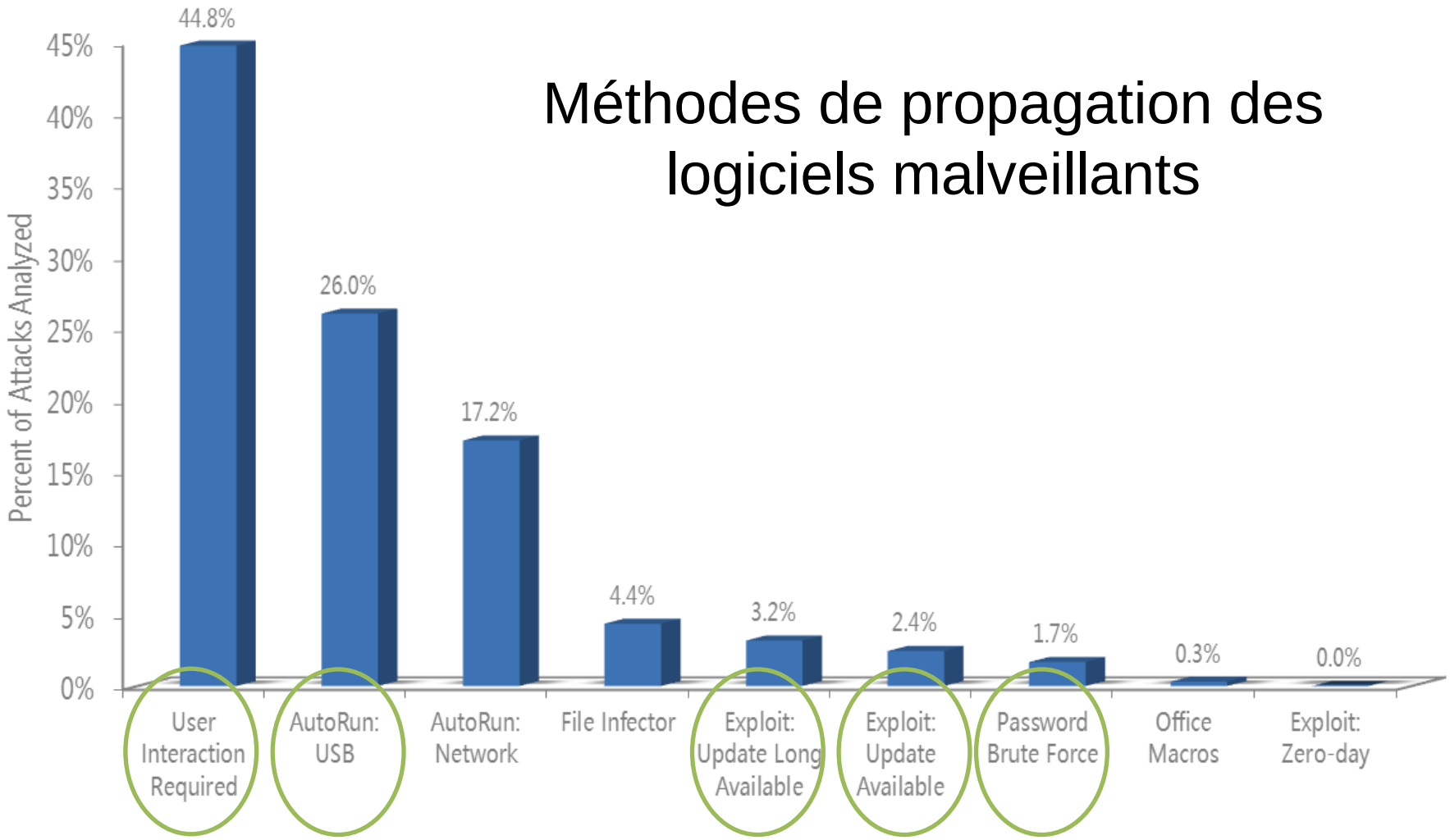
EUROPE - *Facebook* attaqué en justice pour non-respect de la vie privée : après avoir demandé la communication des données le concernant auprès du réseau social, un étudiant autrichien a constaté que **Facebook conserve les données personnelles supprimées par l'utilisateur** et **collecte des informations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

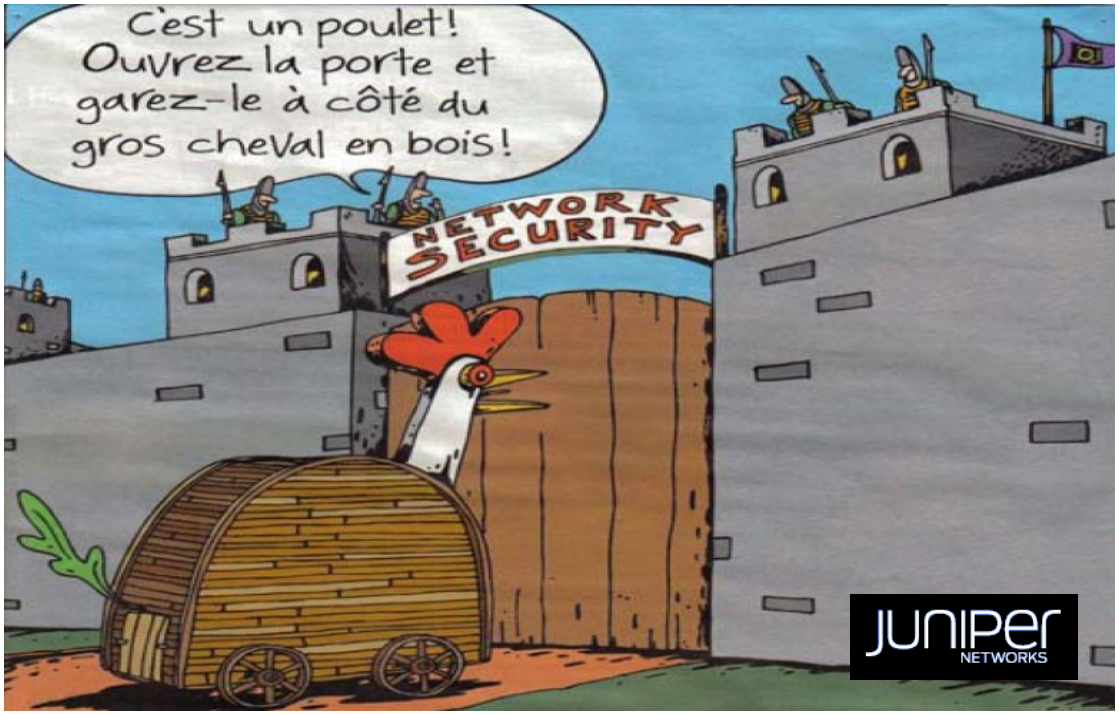
MONDE - Comme l'iPhone et Android, Windows Phone 7 collecte les données de géolocalisation des utilisateurs : l'ordiphone transmet à *Microsoft* son numéro de série, ses coordonnées GPS et des informations sur les réseaux GSM (2G et 3G) et Wi-Fi environnants. (*Cnet* du 25/04, *Microsoft*)

QUE FAIRE ?

Méthodes de propagation des logiciels malveillants



QUE FAIRE ?



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

QUE FAIRE ?

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