

Etat de la menace 2014

X. Delannoy

Introduction – Exemple 1 (1/2)

Google password cracker

Recherche Environ 4 390 000 résultats

Web

Télécharger Password Cracker - 01net.com - Télécharger.com
www.01net.com/telecharger/windows/Securite/.../120307.html - En cache - Pages similaires
★★★★★ Note : 3 - 20 votes - Windows
Password Cracker permet de retrouver les mots de passe oubliés dans plusieurs logiciels et sous Internet Explorer. Il suffit de déplacer la souris sur le mot de ...

Images correspondant à password cracker

Password Cracker - Télécharger
password-oracker.softonic.fr - En cache - Pages similaires
★★★★★ Note : 2.5 - 40 votes - Windows - Sécurité
7 sept. 2012 ... Password Cracker Télécharger gratuitement - Password Cracker Password Cracker 3.94: Retrouver les mots de passe perdus et oubliés, c'est ... Télécharger - Voir tous - Galerie d'images de Password ...

Password cracking - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Password_cracking - En cache - Pages similaires
In cryptanalysis and computer security, password cracking is the process of recovering passwords from data that have been stored in or transmitted by a ...

John the Ripper password cracker - Openwall
www.openwall.com/john/ - En cache - Pages similaires
A fast password oracker for Unix, Windows, DOS, BeOS, and OpenVMS, with support for Unix, Windows, and Kerberos AFS passwords, plus a lot more with ...

Free Password Crackers - PC Support - About.com
pcsupport.about.com/od/.../password-oracker-recovery.htm - En cache - Pages similaires
A list of free password oracker programs. These freeware password orackers will crack Windows passwords, PDF passwords, Word passwords, and more.

Password Cracker - CNET Download.com
download.cnet.com/Password-Cracker/3000-2092_4-10226556.html - En cache - Pages similaires
★★★★★ Note : 1.5 - 37 avis - Windows
23 Jul 2013 ... Passwords are perhaps the weakest links in the cyber-security chain; if they're complex enough to be secure, you probably won't be able to ...

Télécharger Windows Password Cracker 3.1 (Gratuit) pour Windows
telecharger.somsguide.fr/Windows-Password-Cracker/0301-12924.html - En cache - Pages similaires
4 mars 2012 ... Télécharger Windows Password Cracker 3.1 pour Windows. Retrouvez tous les utilisateurs et mots de passe des différentes versions de ...

Télécharger RAR Password Cracker - Clublo
www.clublo.com/telecharger-fiche/171955-rar-password-oracker.html - En cache - Pages similaires
★★★★★ Note : 2.3 - 15 avis
2 déc. 2007 ... Télécharger RAR Password Cracker : Retrouvez vos mots de passe RAR.

Attaques de mots de passe - Password attack
assiste.com.free.fr/pas/attaque_des_mots_de_passe.html - En cache - Pages similaires
Password Cracker. Ces attaques visent à révéler, décrypter ou découvrir en force les mots de passe. Nous allons trouver plusieurs familles de parasites que les ...

Facebook Hack Password Cracker Télécharger Prime Mises à jour...
www.youtube.com/watch?v=NoXyBLS7IM
16 juin 2013 - 2 min - Ajouté par shennoir88589130
http://www.microracking.com/ Call them (USA): +1-872-228-7997 Télécharger le logiciel ici: http ...

Page 1

Google password cracker

Recherche Page 8 sur environ 4 390 000 résultats

Web

Gmail Password Cracker: How to Crack/Hack Your Gmail Password
www.wondershare.com/disk_.../gmail-password-oracker.html - En cache - Pages similaires
19 Aug 2013 ... This article shows you how to orack Gmail passwords in 3 steps with no hassle. Check in for details.

Oracle Password Cracker - Red-Database-Security
www.red-database-security.com/.../oracle_password_oracker.html - En cache - Pages similaires
Oracle Password-Cracker - V1.04: Oracle Password Tools

How I became a password cracker: technology - Reddit
www.reddit.com/v/.../how_i_became_a_password_oracker/ - En cache - Pages similaires
24 Mar 2013 ... Please read the rules and guidelines before posting: Posts should be on technology (news, updates, political policy, etc), image submissions ...

Prevent Hacking with Password-Cracking Countermeasures - For ...
www.dummies.com/.../prevent-hacking-with-passwordcracking-countermeasu.html - En cache - Pages similaires
Taking some general countermeasures can prevent hacking of your important passwords. A password for one system usually equals passwords for many other ...

Password Recovery Speeds - Lockdown.co.uk
www.lockdown.co.uk/?pg=combi - En cache - Pages similaires
As you can see choosing a password from such a small range of characters is a ... the speed taken to orack various types of passwords with various hardware.

password analysis and cracking kit | projects | sprawl
thesprawl.org/projects/pack/ - En cache - Pages similaires
PACK (Password Analysis and Cracking Toolkit) is a collection of utilities developed to aid in analysis of password lists in order to enhance password oracking ...

Password Cracker | Facebook
https://www.facebook.com/.../Password-Cracker/144794488959972 - En cache - Pages similaires
Password Cracker. 24415 likes · 118 talking about this. This is a Fan page about this tight ass Facebook Password Hacker. To hack people's Facebook Password.

MD5 Cracker | Wordlist Download: Password Cracker
hashreak.blogspot.com/ - En cache - Pages similaires
Password-Cracker, MD5 Cracker, Wordlist download, and Wordlist tools. Online hash:md5 decryption - general password security.

RAR Password Cracker - La dernière version à télécharger...
rar_password_oracker.3download330.com/ - En cache
Télécharger gratuitement RAR Password Cracker 4.49 - Obtenez une nouvelle version de RAR Password Cracker. Un logiciel de récupération des mots de ...

Router Password Cracker: Free Router Password Recovery Software
securitypooled.com/router-password-cracker.php - En cache - Pages similaires
In these cases Router Password Cracker can help you in quickly recovering your lost password. Also Penetration Testers and Forensic Investigators can find ...

Page 8

Google password cracker

Recherche Page 12 sur environ 4 390 000 résultats

Web

Free EXCEL Password Recovery / WORD Password Recovery ...
www.freewarepassword.com/ - En cache - Pages similaires
Download FREE Excel password recovery and Word password recovery / oracking software. Freeware, not just a demo!

Minecraft Password Cracker - A Minecraft Password Recovery Utility ...
www.ign.com/.../minecraft-password-oracker-a-minecraft-password-recovery-utility-452155981/ - En cache
New version available (1.4.3)! See downloads section. Minecraft Password Cracker is a utility that decodes a file called "lastlogint" stored in ...

PDF Password Cracker - AmacPDF Software
www.amacpdf.com/pdf-password-oracker.html - En cache - Pages similaires
PDF Password Cracker can easily help you remove user password and owner password to freely copy, edit, print PDF.

Hack Facebook Mot de passe 2013 Password Cracker on Vimeo
vimeo.com/71534528
1 août 2013 - 3 min
Télécharger http://blacksworld.com/6-comment-hacker-un-compte-facebook.html Vous voulez ...

password cracker pro 3.2
www.echo4.me/stared/995-7400-orack-serial/ - En cache
word-v3-o registration key, pdf password oracker pro 3.0 keygen.

Password oracking or recovery | mozilla-Zine Forums
forums.mozillazine.org/viewtopic.php?t=376&w=2533091 - En cache - Pages similaires
I have just known there is a program openly advertised as attempting to orack Firefox master password: http://www.afterdawn.com/software/secure...master.cfm ...

WinRAR Password Remover And Cracker | Game Hackz
gamehackz.net/rar-password-remover-and-oracker/ - En cache
Use WinRAR password Remover to bypass locked files within 30 seconds, our easy to use program is guaranteed to work on any locked file you may have! We ...

5 Best Free ZIP File Password Recovery Tools for Windows
www.useintapp.com/.../5-best-free-zip-file-password-oracking.html - En cache
4 Aug 2013 ... 5 Best Free ZIP File Password Recovery Tools for Windows. Best computer tips, software and web apps. useintapp.

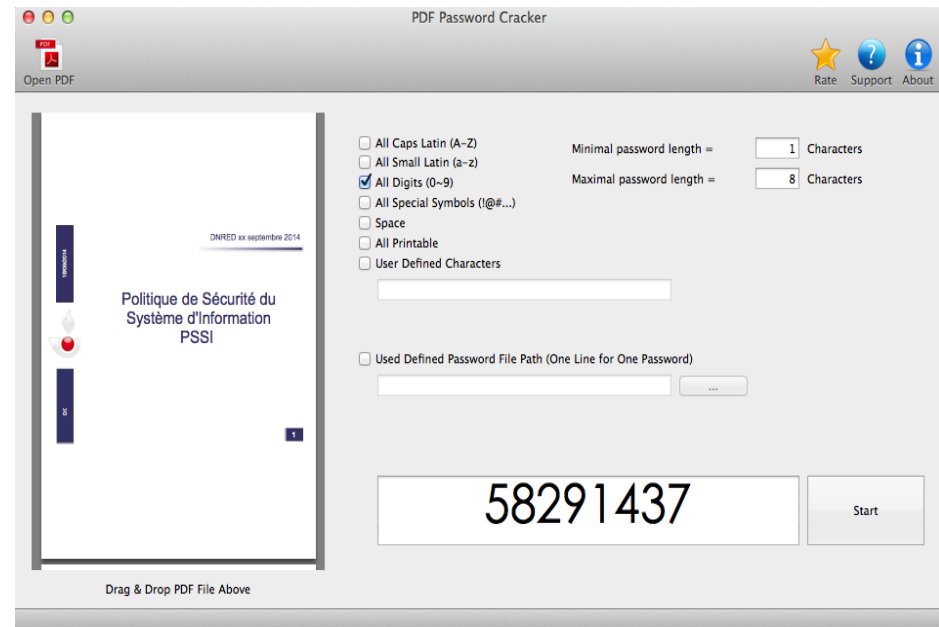
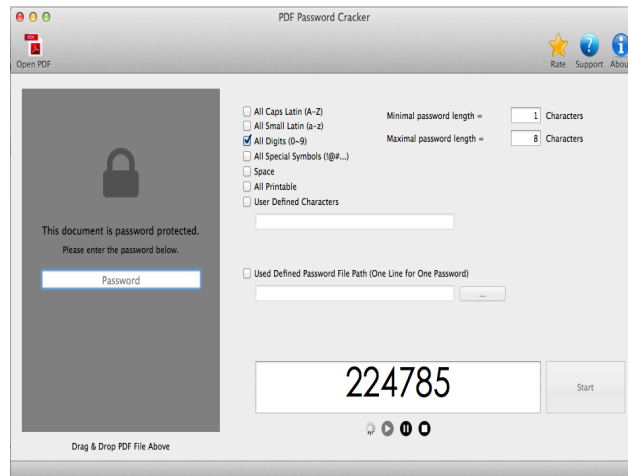
DHS warns of password-oracker targeting industrial networks ...
www.hackgov.com/cybersecurity/...password-oracker/.../60767/ - En cache - Pages similaires
18 Jan 2013 ... Researchers publicized the hacking technique before alerting authorities or the manufacturer.

CrackStation Password Cracking Dictionary (download torrent) - TPB
thelibrary.sx/torrent/.../CrackStation.Password.Cracking.Dictionary - En cache - Pages similaires
18 Feb 2013 ... CrackStation's 15GB 1.5 billion entry password oracking dictionary. The wordlist is being sold by CrackStation using a "pay what you want" ...

Page 13

Résultat d'une recherche Google sur « password cracker »

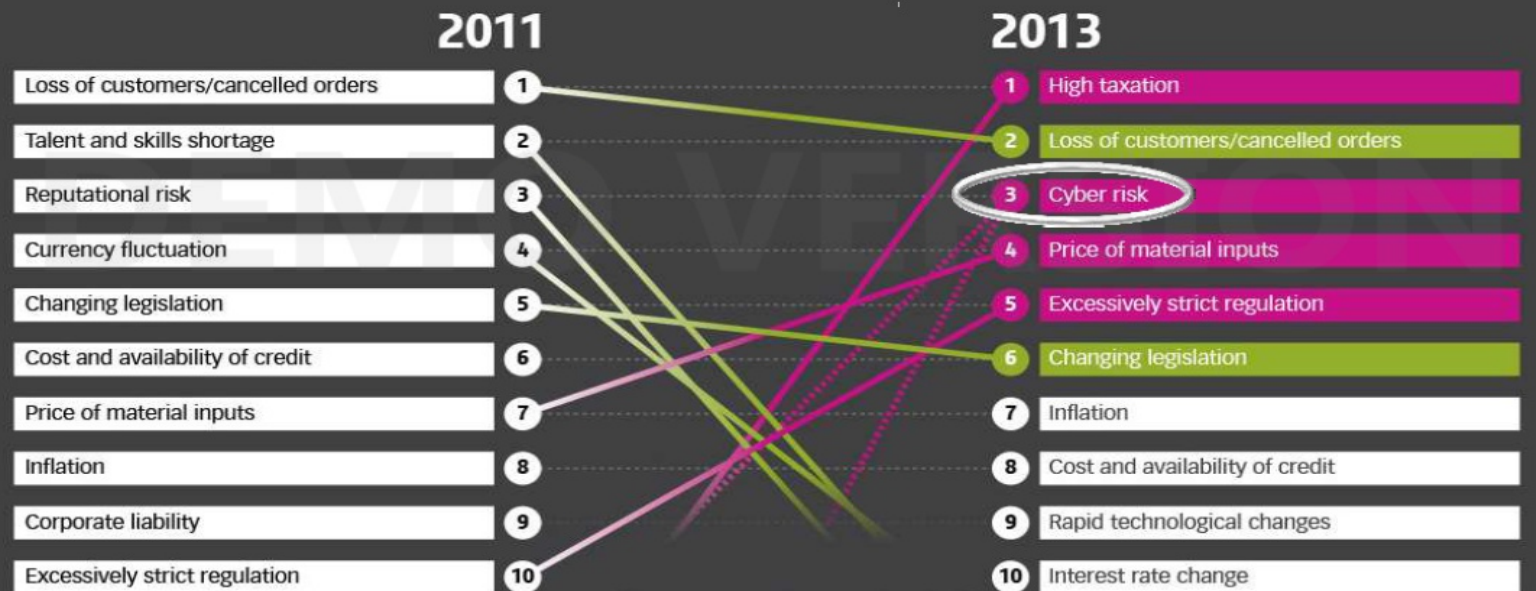
Introduction – Exemple 1 (2/2)



- Sur i7 quadri-coeur génération 2012 (Mac) :
 - **1,5 minute** pour casser le mot de passe 291437 (6 chiffres)
 - **2h30 heures** pour casser le mot de passe **58291437** (8 chiffres) (AES128)
 - 708 jours (estimation) pour un code secret alpha numérique (0-9 ; a-z ; A-Z) à 8 positions
- Un serveur Xeon E7-8837 est 7 fois plus rapide
 - **25 minutes** (estimation) pour le code à 8 chiffres
 - **100 jours** (estimation) pour le code alphanumérique → **10 jours** avec 10 serveurs

Quel niveau de risque ?

This is the third biennial Risk Index, commissioned by Lloyd's to assess corporate risk priorities and attitudes among business leaders across the world.





https://www.youtube.com/watch?feature=player_detailpage&v=v1yb-wWwAEQ

Voir aussi le groupes de hacker chinois à louer « Hidden Lynx »

- **Objet**
 - Appréhender la prévalence des attaques/infractions en conditions réelles
- **Sources**
 - nombreuses, mais pas de vision globale/agrégée
 - Sophos, Imperva, Symantec, IBM, Juniper research, Verizon, McAfee, IDC, ... (Anssi?)
 - chaque éditeur fait une synthèse sur les menaces qu'il propose de couvrir (éditeurs antivirus → malwares)
 - parfois partisans, voire contradictoires
 - rester vigilant et corréler les résultats
 - seule étude relativement générale :
 - Verizon : 47000 incidents de sécurité, 19 organisations dont plusieurs CERT, 671 infractions.
- **Utilité**
 - évaluer la vraisemblance des scénarios de menace pesant sur une application et plus généralement sur le SI.

- L'état de la menace est pollué par des mythes entretenus
 - par les opportunités commerciales
 - le cloud est sûr (dixit un vendeur de cloud)
 - le confort que procure un statu quo largement accepté même s'il est faux
 - les attaques sont bloquées par l'antivirus du poste de travail
 - l'usurpation d'adresse IP (IP spoofing) est une attaque facile à mener
 - des effets d'annonce spectaculaires mais non représentatifs
 - Stuxnet vise les cibles industrielles iraniennes : pas la France ni l'informatique de gestion

- Événement de sécurité
 - potentielle tentative de compromission de l'intégrité, la confidentialité et la disponibilité du SI
- Incident de sécurité
 - l'intention de compromission est confirmée (attaque)
- Infraction
 - la compromission est avérée

Chaine SSL



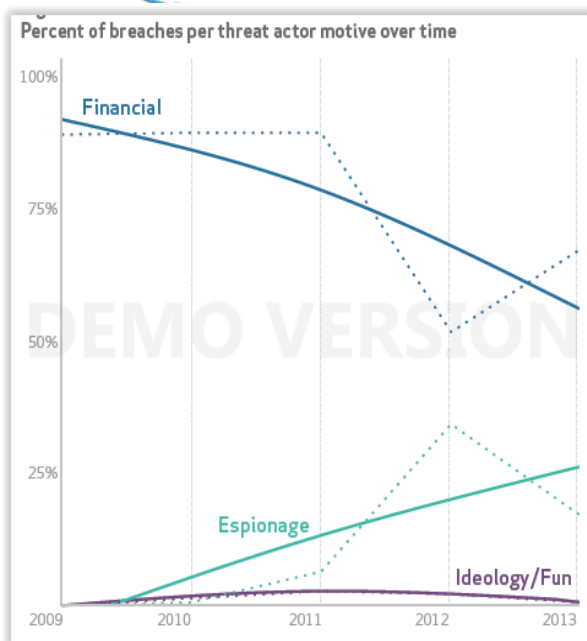
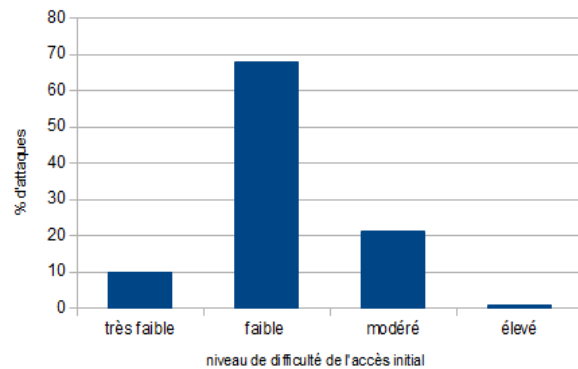
Mythe 1 : La Sophistication (1/2)

- Mythe

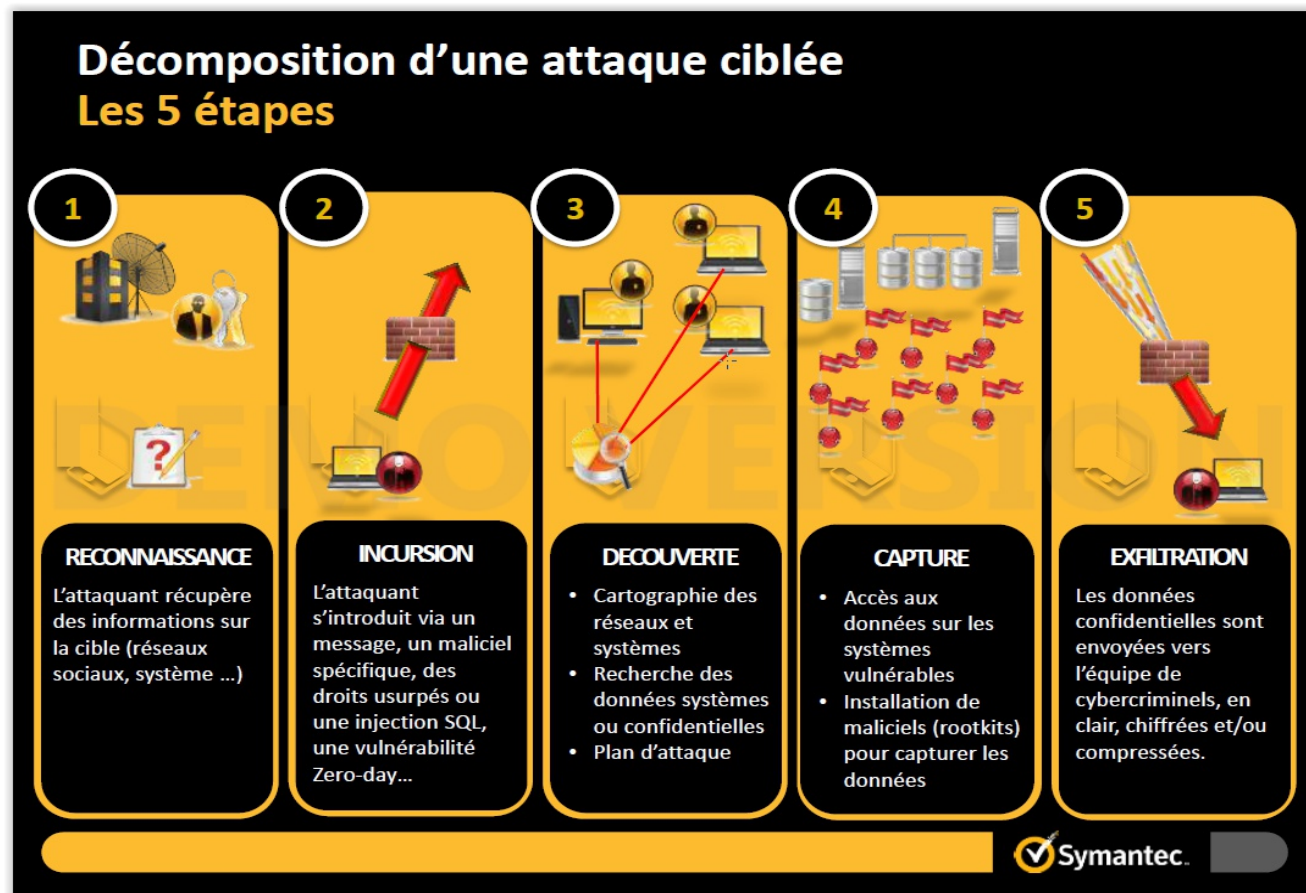
- les attaques sont désormais très sophistiquées

- Réalité

- les attaquants vont au plus simple :
 - ils utilisent ce qui est simple et qui marche tant que ça marche
 - l'objectif n'est plus le « challenge » technique mais d'arriver rapidement à l'objectif qui n'est pas technique : gain financier, espionnage, ...
- la création de nouvelles menaces sur les mobiles s'est ralentie car les auteurs préfèrent améliorer celles déjà existantes
- 84 % des infractions sont réalisées en quelques minutes ou quelques heures (Verizon2013)
- 80 % des attaques de type injection SQL sont automatisées (Havij, SQLmap, ...) (Integra2012)
- le niveau de difficulté des infractions augmente mais reste simple



- Les attaques sophistiquées combinent des techniques simples



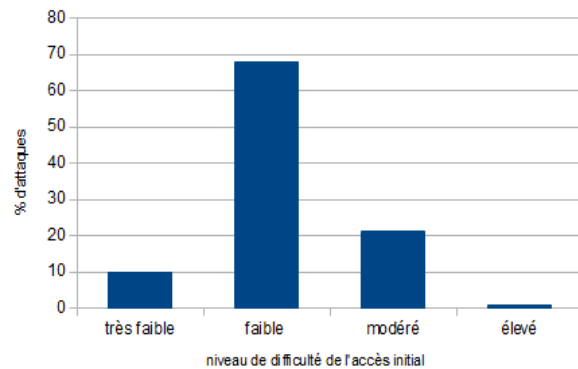
Mythe 1 : La Sophistication (1/2)

- Mythe

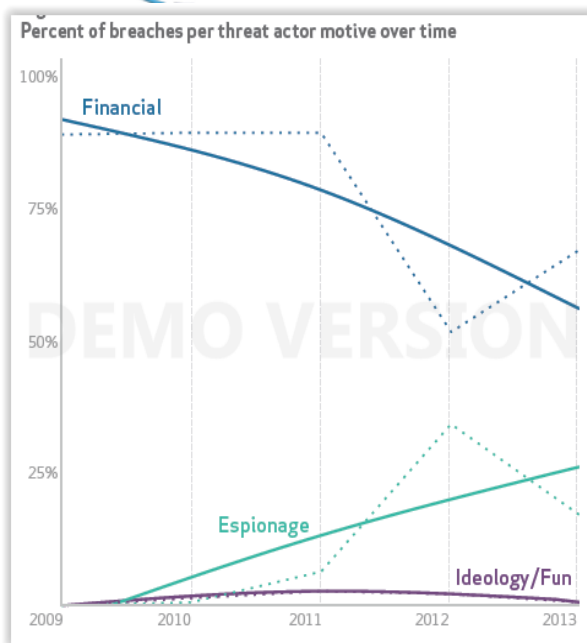
- les attaques sont désormais très sophistiquées

- Réalité

- les attaquants vont au plus simple :
 - ils utilisent ce qui est simple et qui marche tant que ça marche
 - l'objectif n'est plus le « challenge » technique mais d'arriver rapidement à l'objectif qui n'est pas technique : gain financier, espionnage, ...
- la création de nouvelles menaces sur les mobiles s'est ralentie car les auteurs préfèrent améliorer celles déjà existantes
- 84 % des infractions sont réalisées en quelques minutes ou quelques heures (Verizon2013)
- 80 % des attaques de type injection SQL sont automatisées (Havij, SQLmap, ...) (Integra2012)
- le niveau de difficulté des infractions augmente mais reste simple



AUPHINE
IVERSITÉ PARIS



Mythe 2 : Le centre de production

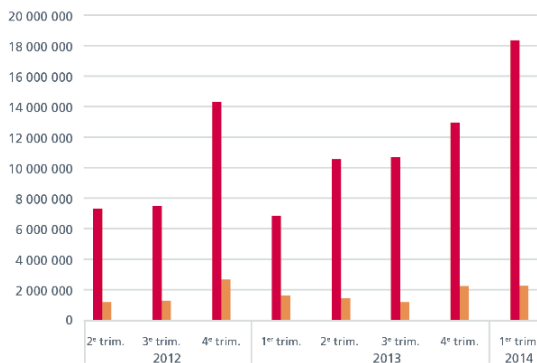
- Mythe

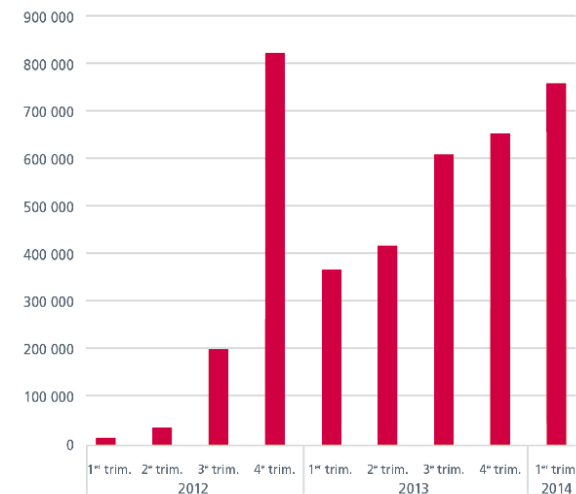
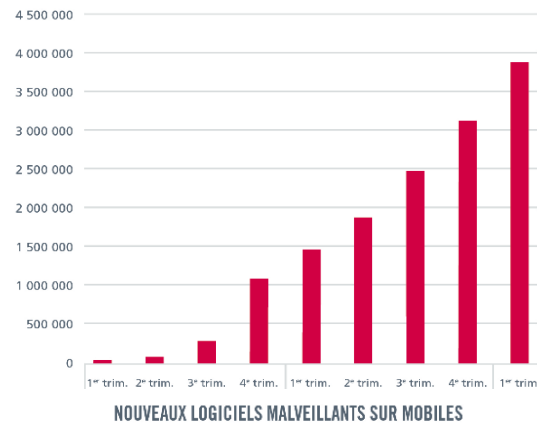
- les centres de production sont la cible privilégiée des attaquants

- Réalité

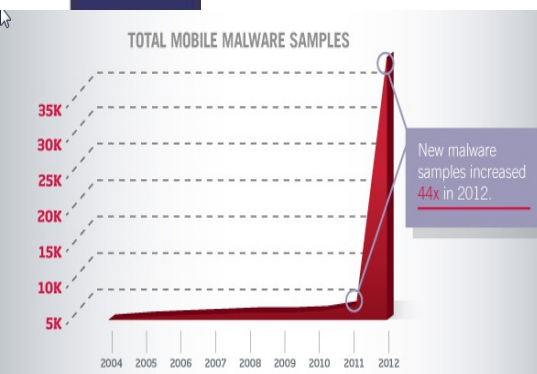
- l' « informatique locale » est un des vecteurs d'attaque significatif pour s'introduire dans le système d'information
 - 25 % des infractions impliquent un ordinateur de bureau^(Verizon2013)
 - 22% des infractions impliquent un portable^(Verizon2013)
 - 22 % des infractions impliquent un serveur de fichier^(Verizon2013)
- 28 % des attaques reposent sur un serveur Web compromis^(Sophos2013+IBM2013)
- une application Web est attaquée en moyenne 4 fois par mois, certaines attaquées en permanence^(Imperva 2013)

NOUVELLES URL SUSPECTES





Source : McAfee Labs, 2014



• Mythe

- les attaques sur les systèmes Android croissent mais sont peu répandues dans l'absolu

• Réalité

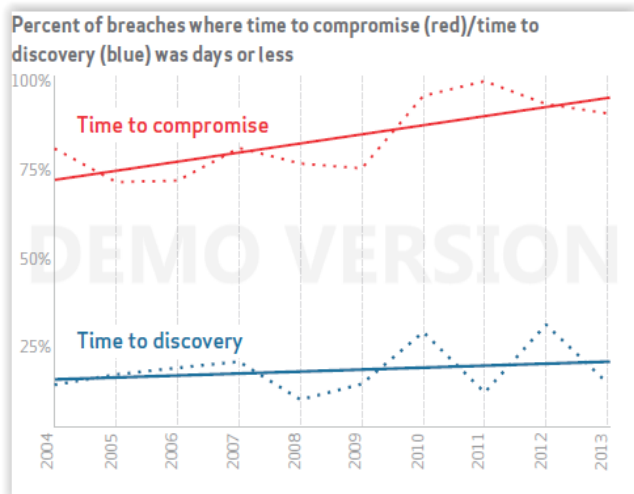
- en Australie et aux Etats Unis les systèmes Android ont une probabilité d'être attaqué supérieure aux systèmes windows ^(Sophos 2013)
- +/- équivalent en France, Allemagne et Pays Bas ^(Sophos 2013)
- 80 % des malwares pour mobile ciblent le système d'exploitation Android ^(JuniperResearch 2013) :
 - 73 % de part de part de marché et 83% des ventes ^(gartner2013)
- Les malwares Android utilisent désormais les mêmes techniques que sur Windows

- Mythe
 - les données sont piratées durant leur transport sur Internet
- Réalité
 - très peu d'infractions sur des données en transit sur les réseaux^(Verizon 2013)
 - les données sont principalement vulnérables^(Verizon 2013)
 - au repos (dans les bases de données et les serveurs de fichiers)
 - en cours de traitement (dans les serveurs applicatifs)
 - Sécuriser un lien est relativement facile. Voir la démarche de Galileo qui cible la source ou la destination

The Solution

In modern digital communications, encryption is widely employed to protect users from eavesdropping. Unfortunately, encryption also prevents law enforcement and intelligence agencies from being able to monitor and prevent crimes and threats to the country security.

Remote Control System (RCS) is a solution designed to evade encryption by means of an agent directly installed on the device to monitor. Evidence collection on monitored devices is stealth and transmission of collected data from the device to the RCS server is encrypted and untraceable.



Mythe 5 : Visibilité

- Mythe

- Les attaques sont visibles (si je suis piraté, je le sais)

- Réalité

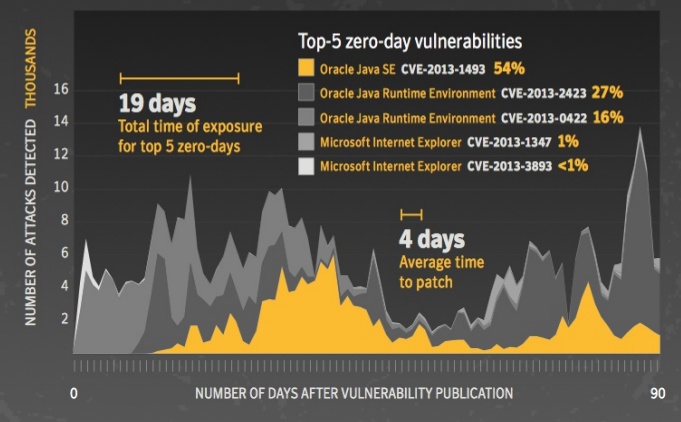
- les attaques sont furtives
- 69 % des infractions sont repérées par un tiers indirectement^(Verizon 2013)
- 66 % des infractions restent ignorées pendant des mois (ce qui augmente l'impact)^(Verizon 2013)
- 4 % des infractions sont détectées après plusieurs années^(Verizon 2013)

Zero-day Vulnerabilities

14 2012 +64% 23 2013

23 software vulnerabilities were zero-day,
5 of which were for Java

97% of attacks using exploits for vulnerabilities
identified as zero-day were Java-based



DA
UNIVE



ADOBE READER	\$5,000-\$30,000
MAC OSX	\$20,000-\$50,000
ANDROID	\$30,000-\$60,000
FLASH OR JAVA BROWSER PLUG-INS	\$40,000-\$100,000
MICROSOFT WORD	\$50,000-\$100,000
WINDOWS	\$60,000-\$120,000
FIREFOX OR SAFARI	\$60,000-\$150,000
CHROME OR INTERNET EXPLORER	\$80,000-\$200,000
IOS	\$100,000-\$250,000

Mythe 6 : les correctifs de sécurité

• Mythe :

- les attaques exploitent des systèmes non patchés (correctifs de sécurité non appliqués)

• Réalité

- les correctifs de sécurité permettent de se protéger des attaques opportunistes (50% des attaques^(IBM2013)) mais ...
- pas des attaques basées sur des 0-day
 - 0-day :vulnérabilité exploitée mais pas de correctif disponible
 - 14 vulnérabilités publiées 0-day en 2012^(symantec2013)
 - non publiées ?
 - forte hausse de l'exploitation des 0-day en 2013^(F-secure2013)
- certains logiciels courants sont mal développés et contiennent beaucoup de vulnérabilités et donc un fort potentiel de 0-day
 - Adobe reader : 58 vuln critiques depuis le début de l'année
 - Par comparaison, Microsoft word : 15 vuln critiques depuis le début de l'année

- Mythe

- les attaques exploitent des vulnérabilités techniques

- Réalité

- Oui, mais ...
- l'humain joue souvent le rôle de catalyseur pour leur exploitation
- 29 % des infractions utilisent de l'ingénierie sociale (Verizon 2013)
- 95 % des attaques d'espionnage soutenues par un état s'appuient sur du hameçonnage (phishing) ou du harponnage (spear phishing) (Verizon 2013)
- les vecteurs d'installation des malwares utilisés dans les infractions sont principalement liés à l'utilisateur
 - Installation directe: 74 % (app malicieuse) (Verizon 2013)
 - Pièce jointe d'un mail : 47 % (Verizon 2013)

*Une même attaque
peut utiliser plusieurs
vecteurs*

EMAIL CAMPAIGNS

2011 – 2013

Source: Symantec



	2013	2012	2013 vs 2012	2011	2013 vs 2011
SUBJ: Campaigns	779	408	+91%	165	+472%
Average Number of Email Attacks Per Campaign	29	122	-76%	78	-62%
Recipients per Campaign	23	111	-81%	61	-62%
Average Duration of a Campaign (in days)	8.2	3	+173%	4	+105%

Top-Ten Industries Targeted in Spear-Phishing Attacks, 2013

Source: Symantec



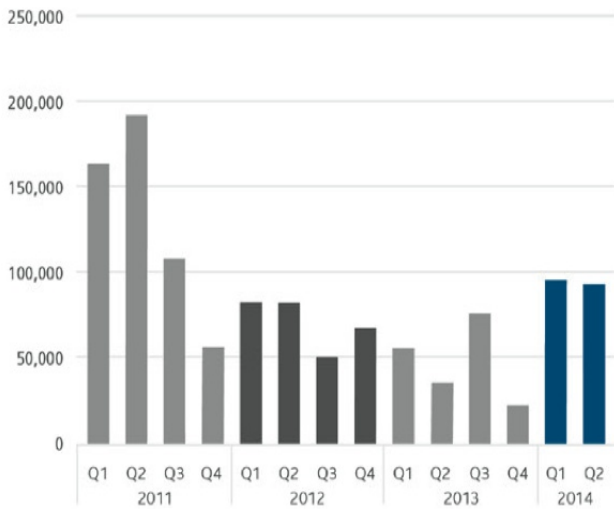
Public Administration (Gov.)	16%
Services – Professional	15
Services – Non-Traditional	14
Manufacturing	13
Finance, Insurance & Real Estate	13
Transportation, Gas, Communications, Electric	6
Wholesale	5
Retail	2
Mining	1
Construction	1

Mythe 7 : « tout » technique (2/3)

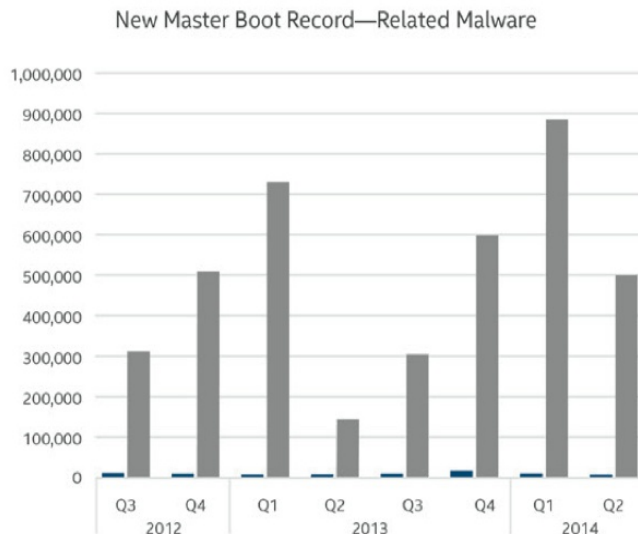
• Spear phishing

- Phishing ciblé (APT)
- 91% de campagne en plus par rapport entre 2012 et 2013 (symantec 2014)
- 472% de campagnes de plus entre 2011 et 2013 (symantec 2014)
- Les administrations sont particulièrement visées (symantec 2014)
- De mieux en mieux ciblées
 - de moins en moins de mail pour une attaque : -76% entre 2012 et 2013 (symantec 2014)
- De plus en plus discret
 - Mails étalés sur une période plus longue : de trois jours en 2012 à huit jours en 2013 (symantec 2014)

- Les mails de spearfishing peuvent renvoyer vers un site infecté ou contenir directement une charge malveillante dans un document joint
- Format des documents joints (symantec 2014)
 - .exe reste une valeur sure
 - .pdf, .doc, .xls en baisse
 - .class et .jpeg en hausse
- Etapes d'une attaque
 - **l'intrusion** : l'attaquant prend pied sur un système informatique ;
 - **la persistance** : l'attaquant met en place les moyens lui permettant de régulièrement se connecter en toute discrétion à ce système ;
 - **le déplacement latéral** : l'attaquant accède à des systèmes liés à celui compromis. Scénario classique: l'attaquant capture les identifiants des utilisateurs des systèmes compromis et les utilise à leur insu pour accéder aux données des applications.
 - **l'exfiltration** : l'attaquant rapatrie discrètement les données sur son serveur.



Source: McAfee Labs, 2014.



- Mythe

- la sécurité du poste de travail est assurée par son antivirus

- Réalité

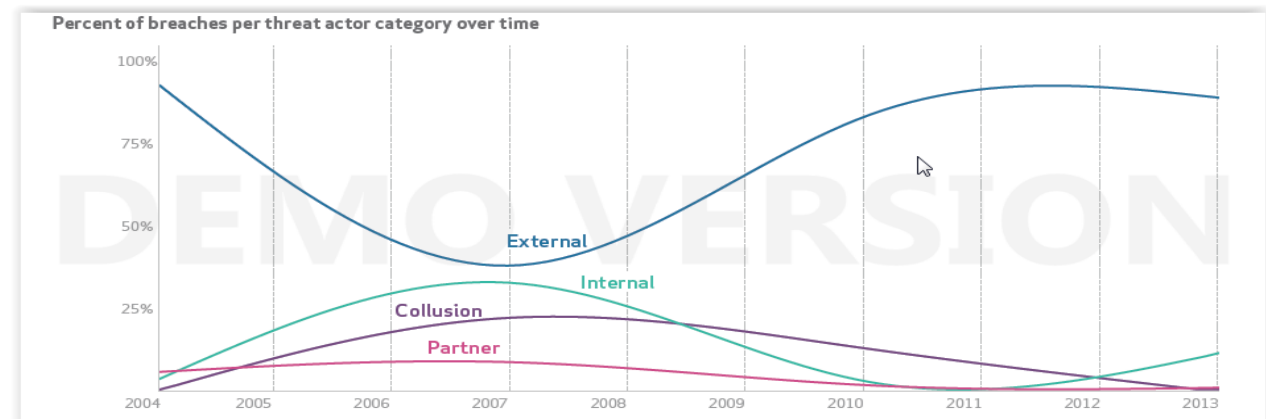
- 75% des malwares ne sont trouvés que dans une seule organisation^(Verizon 2013)
 - les attaquants sont en capacité de construire des malwares spécifiques adaptés à la cible et donc difficilement détectables par l'AV.
- dans 39 % des infractions mettant en œuvre un malware celui-ci est un root-kit donc difficilement détectable par l'antivirus^(Verizon 2013)
- les fichiers de signature « débordent » et doivent être purgés des anciennes signatures^(McAfee-Platinum)

- Mythe

- les attaques sont fréquemment menées par des personnes internes à l'organisation.

- Réalité

- 86 % des infractions n'ont pas d'origine interne (Verizon 2013)
- 1 % des infractions ont pour origine un partenaire (Verizon 2013)
- 8 % des fuites de données sont dues à un attaquant interne (symantec 2013)
- 13 % des infractions ont une origine interne (Verizon 2013)



Verizon, 2014

Mythe 10 : une navigation sur des sites « tous publics » permet d'éviter tout risque

- Mythe

- Les principaux sites web infectés sont ceux pour Adulte. Donc pas de risque lorsque les utilisateurs naviguent sur des sites « tout publics ».

- Réalité

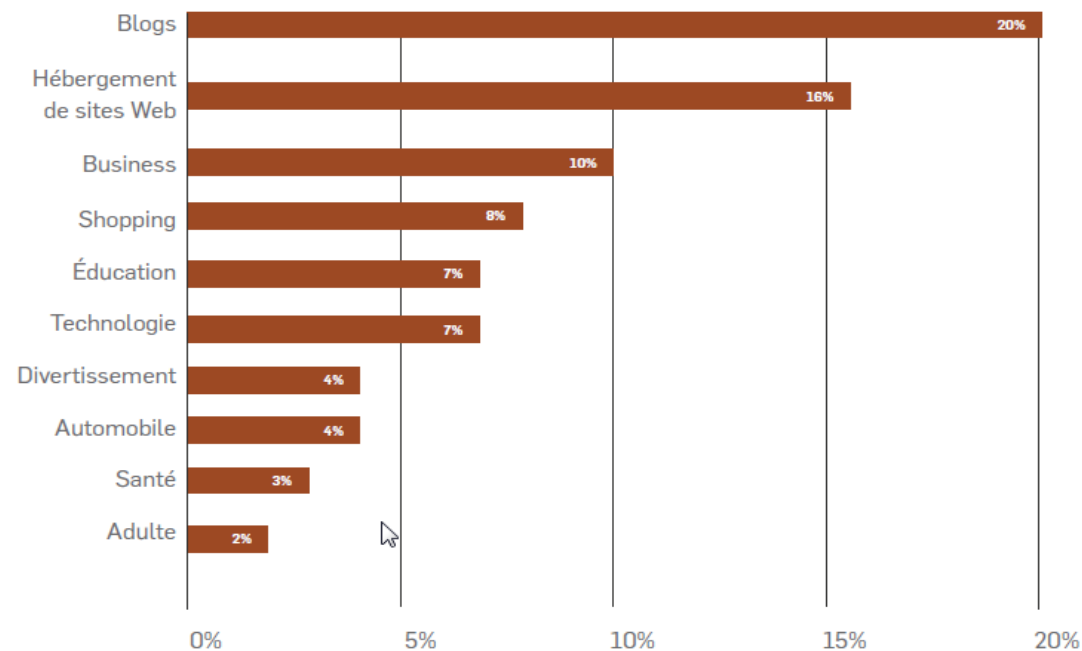


Figure 3 : Les 10 catégories de sites les plus infectées Source : TechNewsDaily

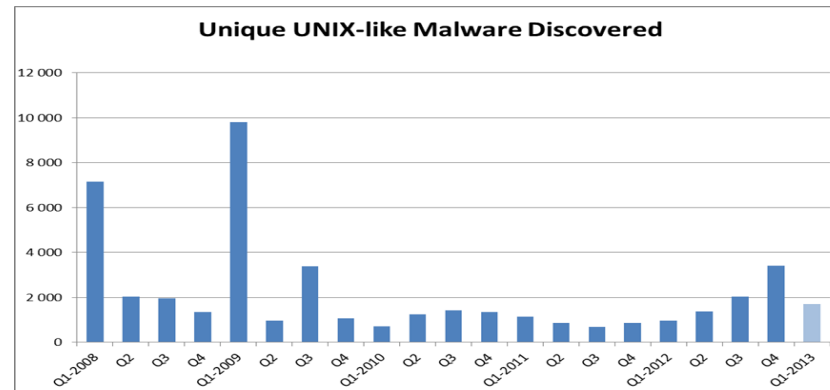
- Mythe :
 - OS X n'est pas attaqué/attaquable
- Réalité :
 - **Modèle de sécurité robuste** :
 - Construit sur Unix BSD
 - 10.6 introduit capacités de détection et de suppression de malwares (Xprotect)
 - 10.8 introduit les permissions d'exécution de code. L'utilisateur doit donner son accord pour l'exécution de toute application non signée par un développeur Apple.
 - **Printemps 2012 : *Flashback* infecte 600000 macs. Propagation de type « drive by download »**
 - **Juillet 2012 : diffusion de *Morcut***
 - Permet de surveiller : frappe clavier, presse papier, applications en cours d'exécution, copies d'écran, web cam, micro, carnet d'adresse, les méta données du système de fichier, les URL consultées, la position de la souris, la localisation, ...
 - **Sophos découvre 4900 nouveaux malwares pour OS X chaque semaine ...**

- Mythe

- Unix n'est pas attaqué/attaquable

- Réalité

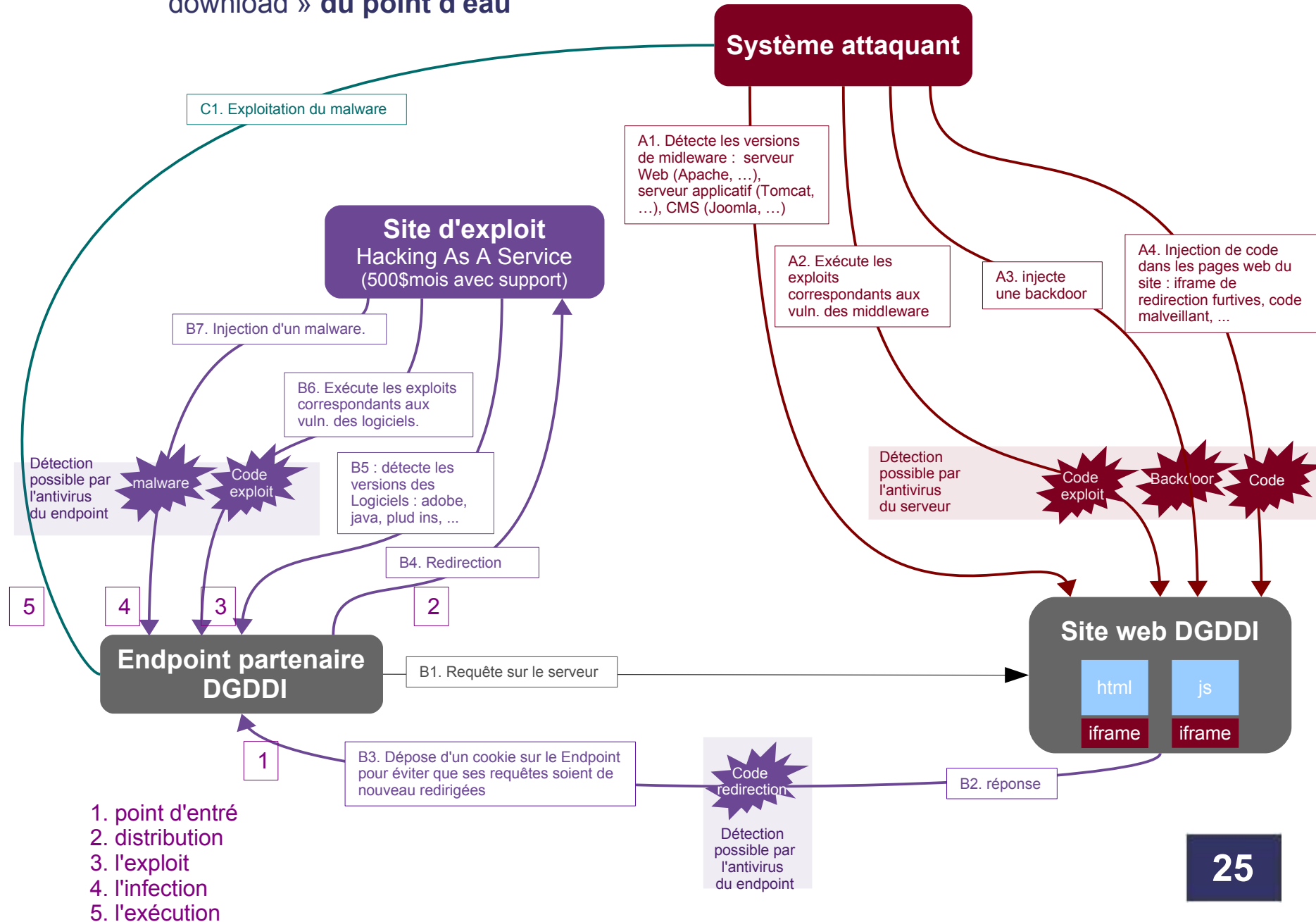
- Plus de 500 malwares découverts par mois sur les Unix like



- Ces malwares ciblent en particulier les middlewares qui s'exécutent sur Linux (apache, tomcat, joomla, ...)
 - (présentation AV serveurs de fichier)

Mythe 12 : Unix est sûr (2/5)

Cinématique simplifiée d'une attaque « drive by download » du point d'eau



- Variations

- L'attaquant peut aussi injecter du Javascript, des PDF et des objets flash.
- Le javascript peut être obfusqué ce qui rend l'injection indétectable à la relecture du code (encode avec des outils libres).
- Le serveur peut contenir directement le code de l'exploit à exécuter sur le navigateur
- L'injection peut aussi exploiter un mot de passe d'administration faible qui permet d'ajouter des modules malins à Apache. Ou un « rogue » Apache.

- Responsabilité pénale : l'hébergeur d'un serveur de redirection est responsable
 - « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende. »
article 323-2 du code pénal
 - « Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »
article 323-3 du code pénal
 - la loi n'est pas strictement appliquée ... pour l'instant

- L'exploitation des vulnérabilités des applications sur Linux est rapidement intégrée par les antivirus
 - par exemple la backdoor *Darkleech* (*Apache/Tomcat*)

THREAT DETAILS

Linux/Backdoor-Appmod
MTIS13-062-A

THREAT IDENTIFIER(S)

Linux/Backdoor-Appmod

THREAT TYPE

Malware

RISK ASSESSMENT

Undetermined

MAIN THREAT VECTORS

Web

USER INTERACTION REQUIRED

Yes

Darkleech is a malicious Apache server module that currently is infecting highly visited websites. First appearances date from August 2012, and through February 2013 the malware has attacked an estimated 20,000 victims. Its method of spreading is unknown, but it is known that it infects Apache installations with invisible code that exposes visitors to third-party sites used to spread malware and exploit kits like Blackhole. The malware is under continuous development; multiple versions of the injected modules have been reported. Apart from injecting iframes modules, the attack takes control of the SSH binaries, giving access to the infected site even after it has been disinfected. The malware does not attack every visitor, instead selecting victims randomly and constantly changing domains to avoid detection. The US media company Los Angeles Times and Seagate are its latest victims.

DESCRIPTION

- *Shell bash (sept 2014)*

McAfee Mitigations

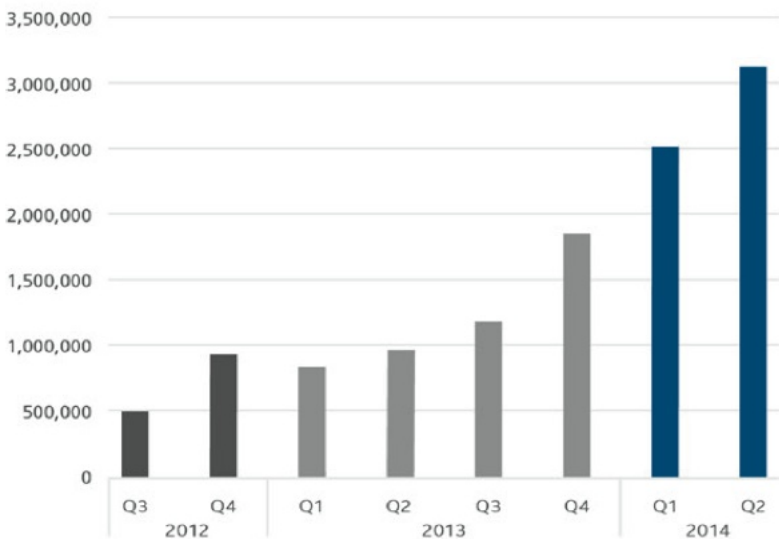
Several McAfee products have signatures to help mitigate this vulnerability. These include:

- **AV - AntiVirus**
 - Includes all McAfee AntiVirus products, including VSE, McAfee AntiVirus Plus, MWG, etc.
 - 7573 DAT – Detects all payload samples seen from exploit of the Bash vulnerability
 - Samples are detected as "Linux/Dingle"

Mythe 13 : applications et modules signés

- Mythe :
 - les applications/modules signés sont fiables
- Réalité :
 - Globalement vrai ...
 - mais de moins en moins

New Malicious Signed Binaries



Source: McAfee Labs, 2014.

- La menace est complexe car elle
 - est en forte augmentation
 - porte sur tous les biens du SI
 - évolue
 - est polymorphe
- Formaliser et d'organiser la réponse à la menace
==> la politique de sécurité