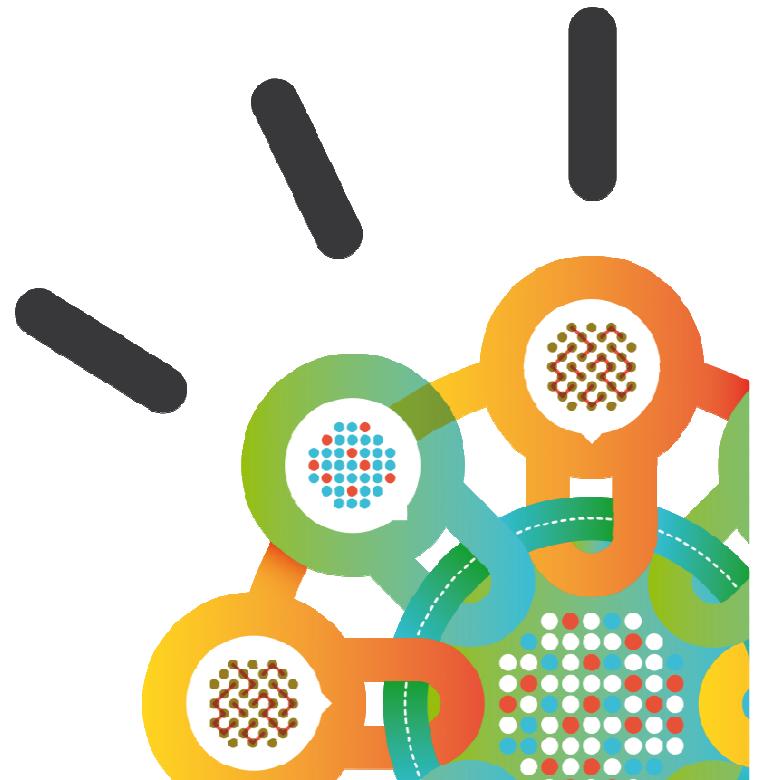


Security Intelligence.
Think Integrated.

Rationalité et irrationalité dans le gestion des risques informatiques

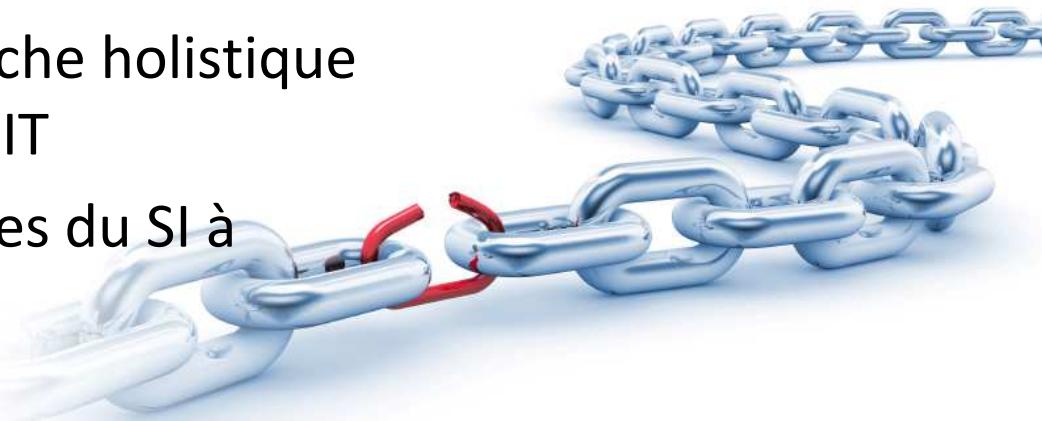
Sophie Tacchi

sophie_tacchi@fr.ibm.com

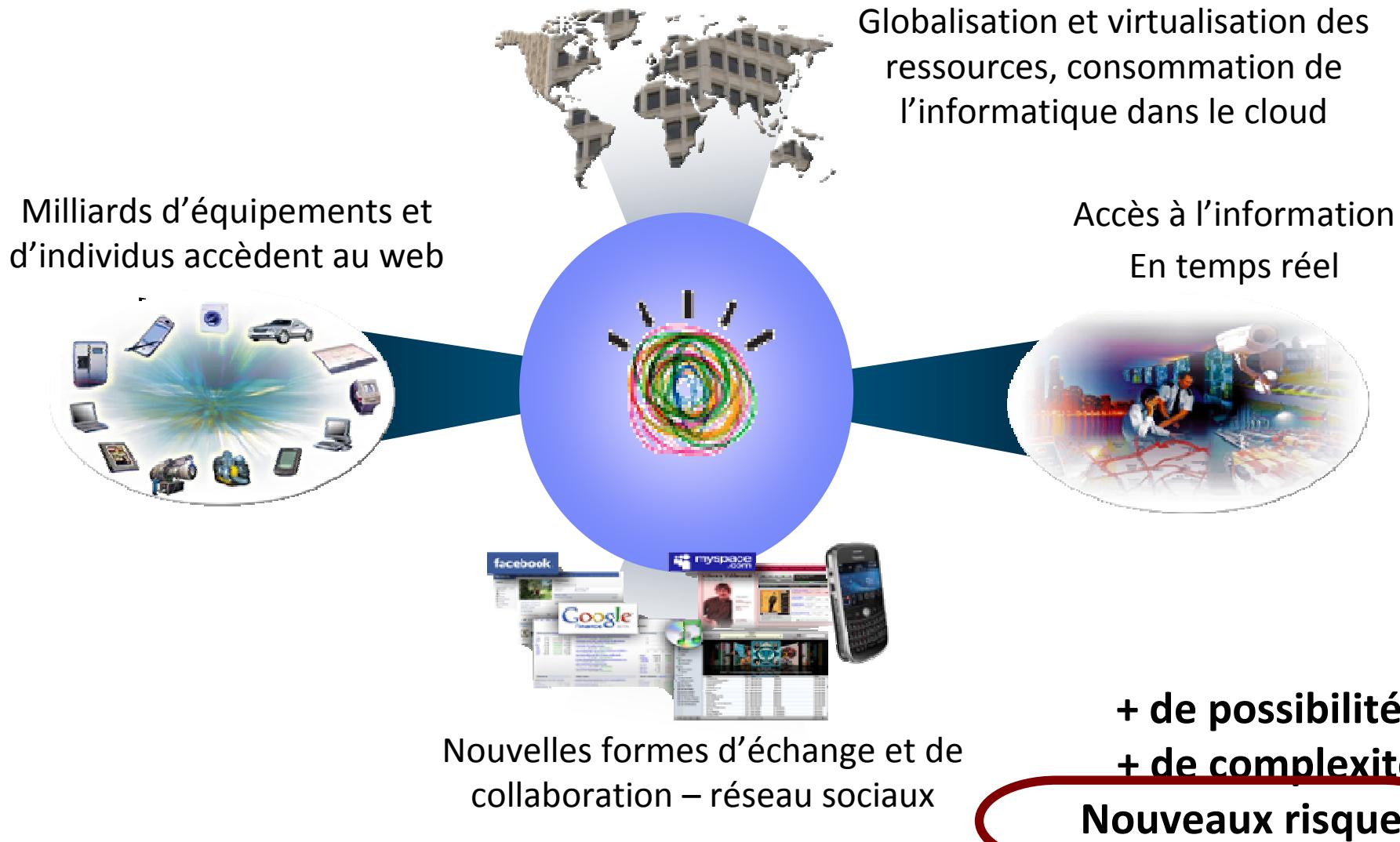


Agenda

- Evolution technologique, innovation
- Typologie des risques
- Analyse de la nature des menaces
- Qu'en dit le législateur ?
- Nécessité d'une approche holistique de gestion des risques IT
- Les principaux domaines du SI à sécuriser
- Besoins en formation
- Conclusions



Bienvenue dans une planète plus intelligente ...



Les menaces augmentent.. Impactant les niveaux de services, les coûts et l'activité. Il existe une multitude de scénarios de menaces ...

Menaces Externes

Par inadvertance

<ul style="list-style-type: none">■ Pannes d'électricité■ Désastres naturels■ Bouleversements politiques ou économiques	<ul style="list-style-type: none">■ Malware■ Déni de service■ Attaques sophistiquées et organisées
<ul style="list-style-type: none">■ Systèmes non patchés■ Vulnérabilité du code■ Pas contrôle des changements■ Erreur humaine	<ul style="list-style-type: none">■ “Back doors” créées par des développeurs■ Vol de données■ Fraudeurs internes

Intentionnelles

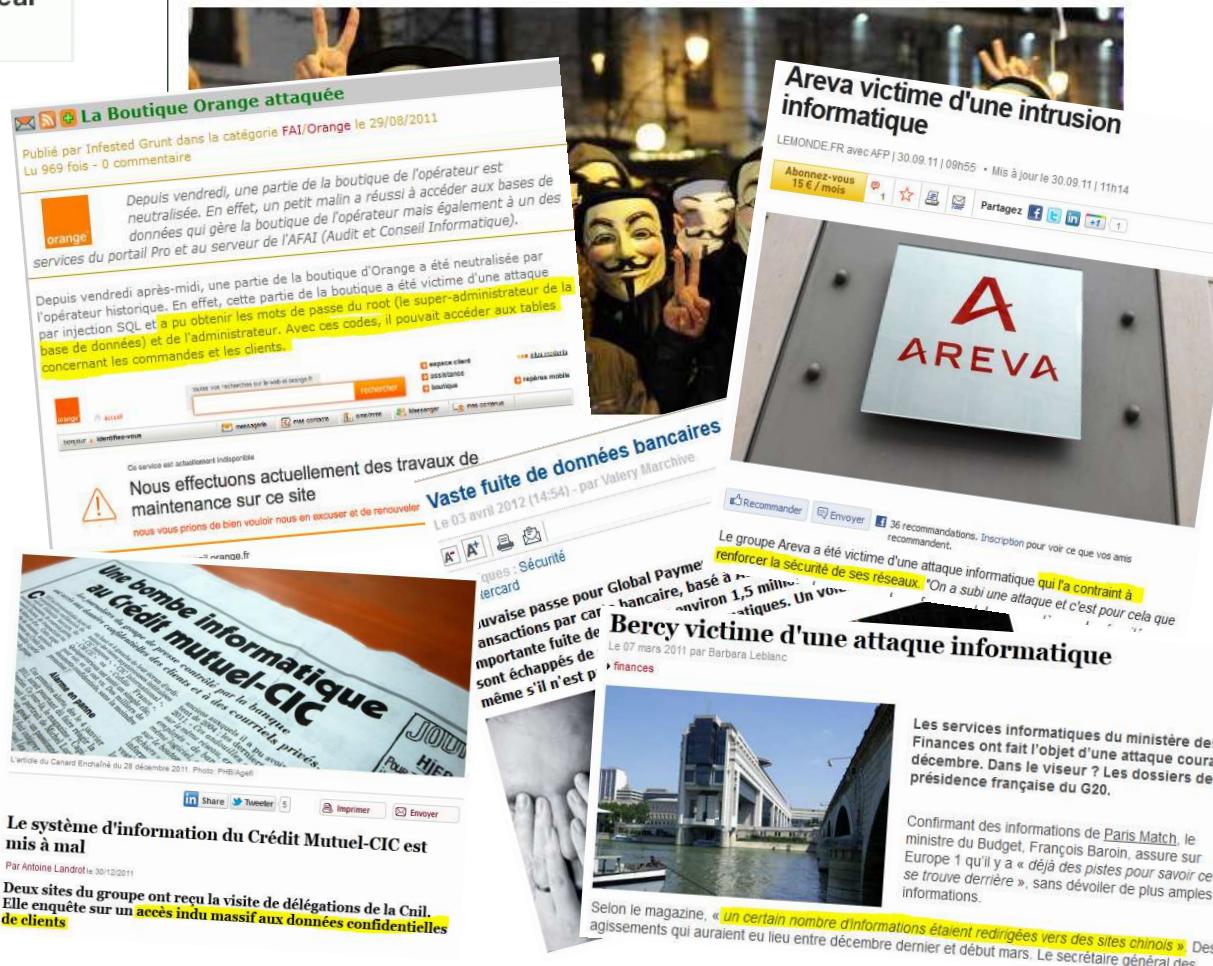
Menaces internes

Evolution des menaces : Les récentes attaques amènent à se poser des questions sur l'efficacité des mécanismes de sécurité traditionnels



Les Anonymous s'attaquent à l'Élysée

Le site internet du gouvernement a été piraté vendredi.



La Boutique Orange attaquée
Publié par Infested Grunt dans la catégorie FAI/Orange le 29/08/2011
Lu 969 fois - 0 commentaire

Depuis vendredi, une partie de la boutique de l'opérateur est neutralisée. En effet, un petit malin a réussi à accéder aux bases de données qui gère la boutique de l'opérateur mais également à un des services du portail Pro et au serveur de l'AFAI (Audit et Conseil Informatique).

Depuis vendredi après-midi, une partie de la boutique d'Orange a été neutralisée par l'opérateur historique. En effet, cette partie de la boutique a été victime d'une attaque par injection SQL et a pu obtenir les mots de passe du root (le super-administrateur de la base de données) et de l'administrateur. Avec ces codes, il pouvait accéder aux tables concernant les commandes et les clients.

Areva victime d'une intrusion informatique
LEMONDE.FR avec AFP | 30.09.11 | 09h55 • Mis à jour le 30.09.11 | 11h14

Abonnez-vous 19 €/mois Partagez

Vaste fuite de données bancaires
Le 03 avril 2012 (14:54) - par Valery Marchive

Le groupe Areva a été victime d'une attaque informatique qui l'a contraint à renforcer la sécurité de ses réseaux. On a subi une attaque et c'est pour cela que

Bercy victime d'une attaque informatique
Le 07 mars 2011 par Barbara Leblanc

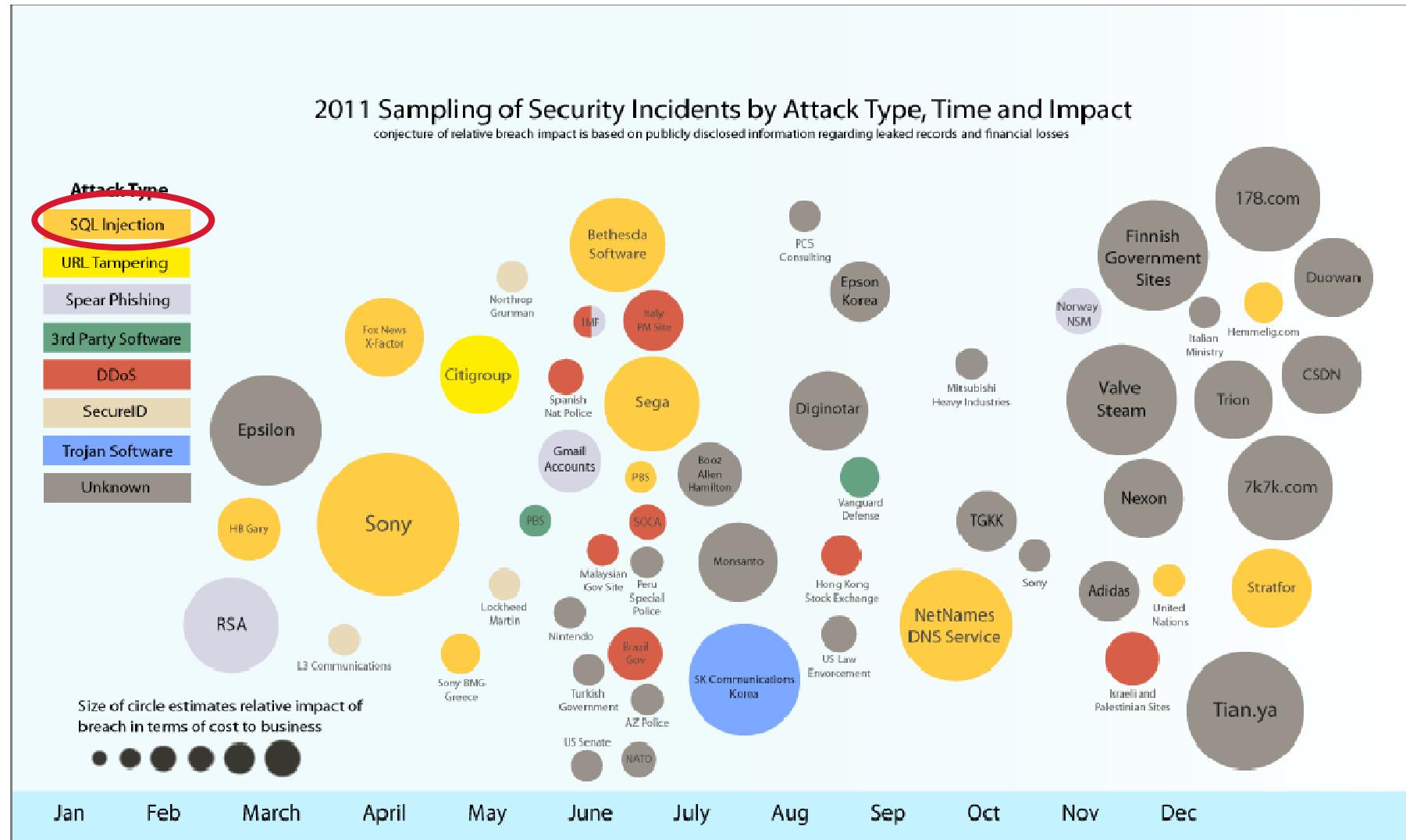
Les services informatiques du ministère des Finances ont fait l'objet d'une attaque courant décembre. Dans le viseur ? Les dossiers de la présidence française du G20.

Confirmant des informations de Paris Match, le ministre du Budget, François Baroin, assure sur Europe 1 qu'il y a « déjà des pistes pour savoir ce qui se trouve derrière », sans dévoiler de plus amples informations.

Le système d'information du Crédit Mutuel-CIC est mis à mal
Par Antoine Landrot le 30/12/2011

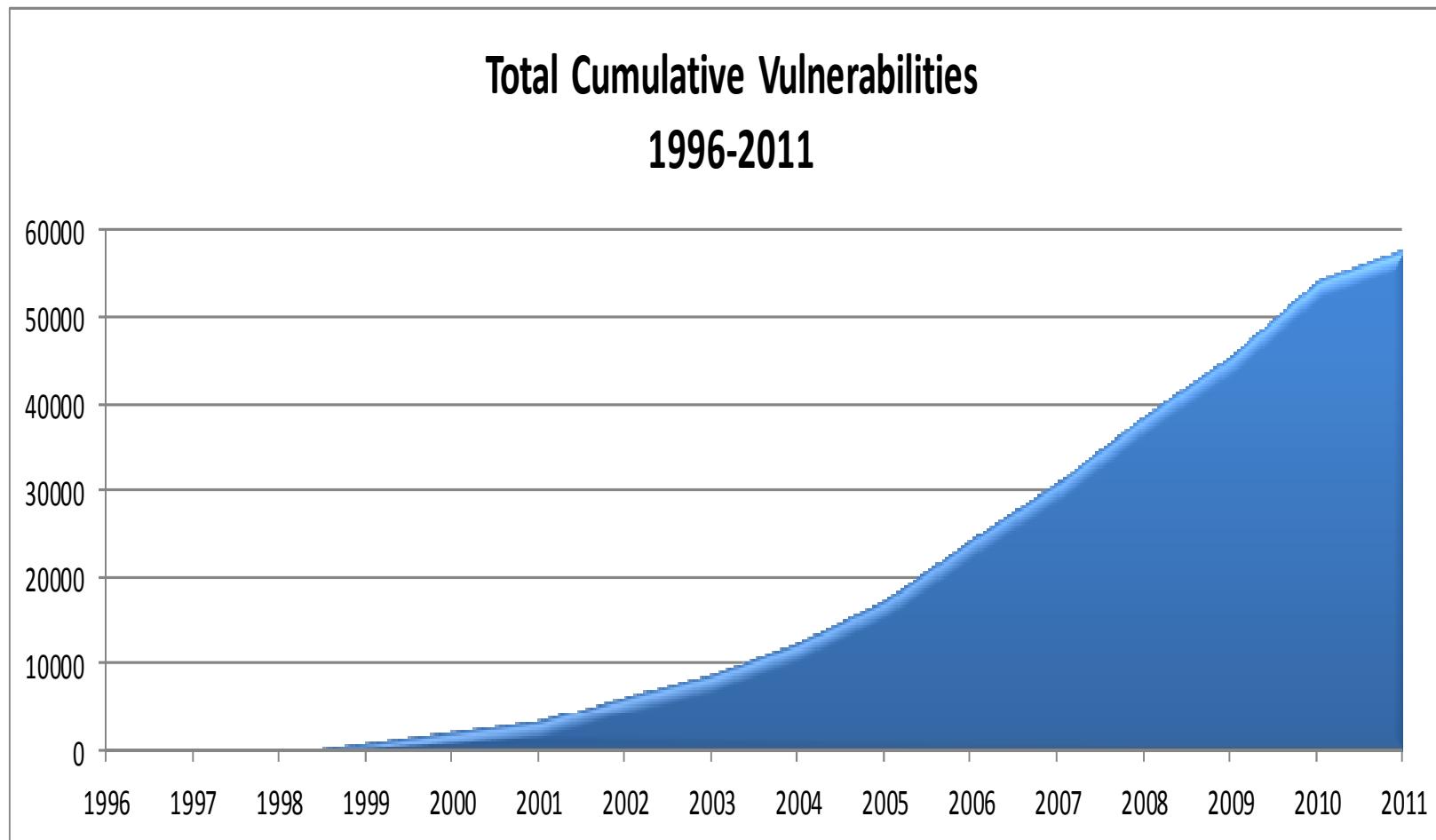
Deux sites du groupe ont reçu la visite de délégations de la Cnil. Elle enquête sur un accès indu massif aux données confidentielles de clients.

Exemples d'attaques ciblées visant des entreprises et des gouvernements

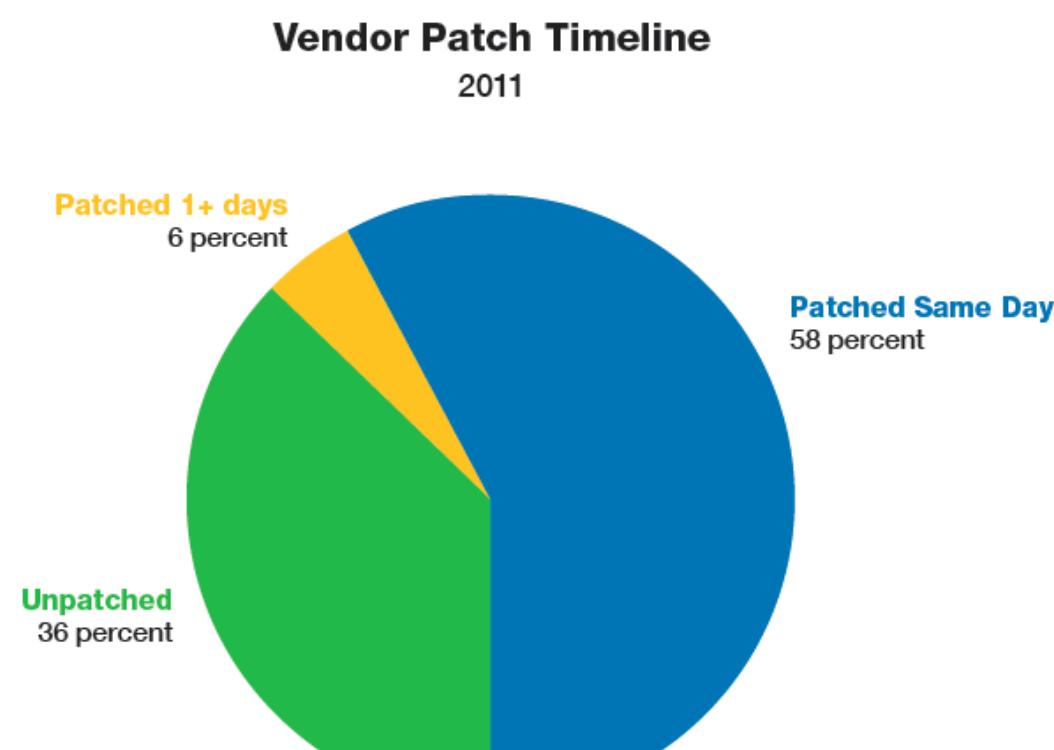


IBM Security X-Force® 2012 Trend and Risk Report

Vulnérabilités cumulées – XForce 2012

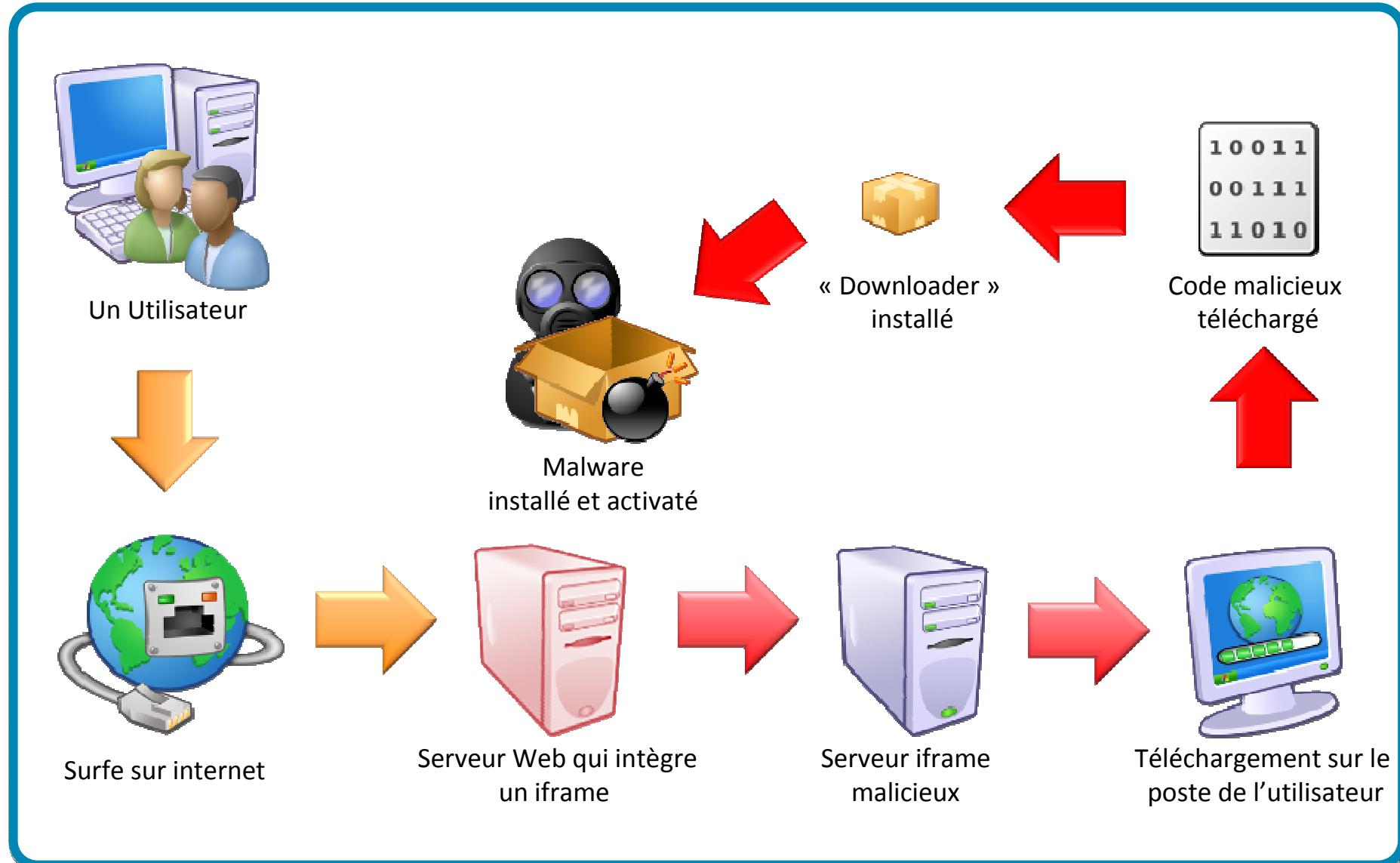


Les vulnérabilités sont peu « patchées » mais la tendance s'améliore.



	2011	2010	2009	2008	2007	2006
Unpatched %	36.0%	43.3%	45.1%	51.9%	44.6%	46.6%

Une technique d'infection parmi d'autres : navigation sur le web !!!!





Black

- A
te
lis
-

C Us its

The screenshot shows the Best Antivirus software interface. The main window title is "best antivirus". The menu bar includes File, View, Action, Settings, and Help. The toolbar contains icons for Scan, Scan result, White list, Report, Site, Settings, Register, and About. The main content area displays a table of browser extensions:

Browser name	Extension name	Extension company	Extension ID
Internet Explorer	Windows Messenger	<not available>	{FB5F1910-F110-11d2-BB9E-00C04F795683}
Internet Explorer	@xpsp3res.dll,-20001	<not available>	{e2e2dd38-d088-4134-82b7-f2ba38496583}
Internet Explorer	&Astuce du jour	Microsoft Corporation	{4D5C8C25-D075-11d0-B416-00C04FB90376}
Internet Explorer	Adobe PDF Link Helper	Adobe Systems Incorporated	{18DF081C-E8AD-4283-A596-FA578C2EBDC3}

At the bottom of the main window are buttons for Delete, To white list, Select all, and Unselect all. A small "Best Antivirus" logo is in the bottom left corner. A "Warning!" dialog box is overlaid on the bottom right, stating: "Best Antivirus detected some unsafe add-ons on your PC. Found: 4 add-ons." It includes an exclamation mark icon and a "REGISTER NOW" button.

Tendances en terme de malware

- Zeus anime une e-économie souterraine et vend :
 - Des versions privées de l'outil avec des plugins additionnels
 - Des services de configuration Zeus
 - Des services hébergés et gérés
 - Des add-on Zeus avec packages additionnels

[\$20] Zeus 1.2.7.19 BINS [Builded Bot] (1 2 3) b1sh0p
\$100 - Zeus 1.2.9.3 with FF & Opera Module [Only 3 sales!!] (1 2) Bankjob
Schwarze Sonne RAT 0.2 Beta (1 2 3) slayer616
Selling Zeus 1.2.7.19 with FireFox module enabled + Free BP hosting DarkNet
Zeus 1.2.7.19 - FF module Enabled = 30\$:d (1 2 3) Zeusf0sh0

 5-XXXX-XXXX-XXXX-31
 setupservice@XXXX.ru
 BL:146 TL:0
Setup Public Zeus - free
Setup Private Zeus - Details in icq\msn
<i>(Opera 10.10 & FF 3.5.5)</i>
Private Exploit System - Details in icq\msn
I will help to rent hosting for Zeus - cheap and quickly

Zeus Services de cybercriminalité

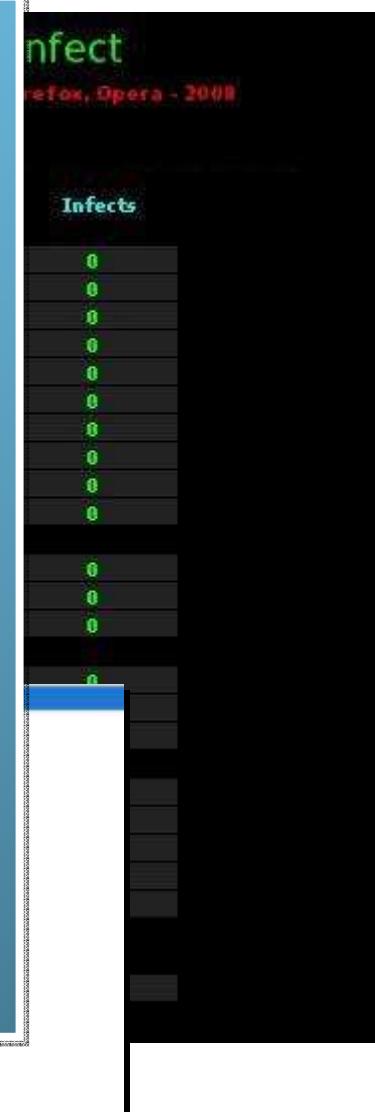


Hosting for costs \$50 for 3 months.

This includes the following:

- # Fully set up ZeuS Trojan with configured FUD binary.
 - # Log all information via internet explorer
 - # Log all FTP connections
 - # Steal banking data
 - # Steal credit cards
 - # Phish US, UK and RU banks
 - # Host file override
 - # All other ZeuS Trojan features
 - # Fully set up MalKit with stats viewer inter graded.
 - # 10 IE 4/5/6/7 exploits
 - # 2 Firefox exploits
 - # 1 Opera exploit
 - # Admin area to view statistics
- [Q] Can i see a demo?
 [A] Yes you can, there is a demo set up [here](#) (Coming soon)
- Methods of payment:
 • Moneybookers
 • Click2Pay
 • Western Union
- Zeus :: Logs search
- Information:
 Profiles:
 GMT date:
 GMT time:
 Statistics:
 Summary
 Botnets:
 Online bots
 Remote commands
 Logs:
 → Search
 Search with template
 Uploaded files
 Logout

We also host normal ZeuS clients for \$10/month.
 This includes a fully set up zeus panel/configured binary



En parallèle arriva SpyEye...

- Un concurrent de Zeus – SpyEye a été conçu pour être plus “grand public”
 - Ses robots avaient la capacité d’effacer **Zeus**
 - Il introduit de nouvelles fonctionnalités comme – Keylogger, et « sniffer » de réseaux



2010 - Zeus et SpyEye ont fusionné

CP :: Summary statistics

Information:

Current user: **Administrator**
GMT date: 30.01.2011
GMT time: 12:51:41

Statistics:

- **Summary**
- OS**

Botnet:

- Bots**

Reports:

- Search in database
- Search in files

System:

- Information
- Users

Logout

Information

Total imports in database: **6098**
Time of first activity: **2011-01-29 00:51:41**

Total bots: **6098**
Total active bots in 24 hours: **54.90% - 3348**
Minimal version of bot: **Any**
Maximal version of bot: **Any**

Botnet [All] >>

Actions: Reset imports

Installed (6098)	Online (912)
Germany	442
Korea, Republic of	157
Unknown	87
Austria	66
Switzerland	25
Peru	25
Italy	17
Netherlands	17
Spain	9
Chile	7
United States	7
Belgium	5
Ecuador	5
France	5
United States	4
Mexico	3
Argentina	3
Turkey	3
Thailand	3
Taiwan	3
United Kingdom	2
Colombia	2
Poland	2
Thailand	2
Russian Federation	2
Czech Republic	2
Serbia	1
India	1
Japan	1
Iran, Islamic Republic of	1
Slovenia	1
Venezuela	1
Ukraine	1
Romania	1

Tasks Statistic

Update Bot

VIRTEST

SOCKS 5

Bots Monitoring

Plugins

RDP

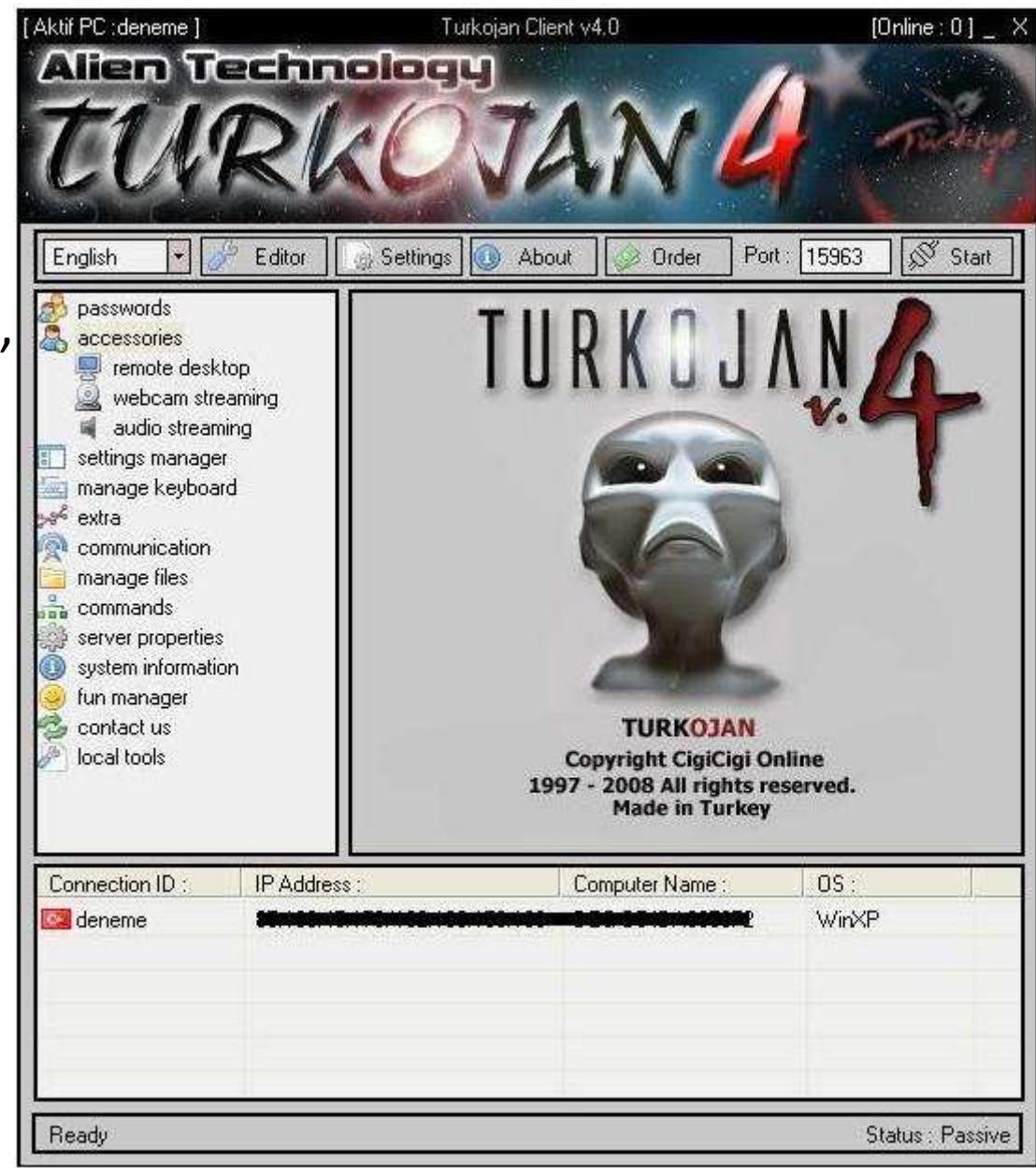
Settings

GEO Info

Flag	Country	Online Bots/ All Bots	Detail
	Argentina	(2/ 27)	
	Aruba	(0/ 1)	
	Austria	(0/ 6)	
	Azerbaijan	(87/ 507)	
	Belarus	(1/ 2)	
	Belgium	(17/ 44)	
	Bosnia and Herzegovina	(1/ 2)	
	Brazil	(0/ 1)	
	Bulgaria	(0/ 3)	
	Canada	(0/ 6)	
	Chile	(2/ 50)	
	China	(1/ 1)	
	Colombia	(0/ 21)	
	Croatia	(0/ 1)	
	Czech Republic	(2/ 12)	
	Denmark	(1/ 4)	
	Ecuador	(2/ 35)	
	Egypt	(0/ 2)	
	Estonia	(1/ 2)	
	Finland	(7/ 31)	
	Germany	(441/ 3023)	
	Greece	(1/ 5)	
	Guatemala	(0/ 4)	
	Hungary	(2/ 6)	
	Iceland	(1/ 1)	
	India	(5/ 10)	
	Ireland	(0/ 1)	
	Iran, Islamic Republic of	(1/ 9)	
	Israel	(0/ 4)	
	Italy	(7/ 93)	

Trojan Creator Kits

- Constructor/Turkojan
- V.4 New features
 - Accéder à un poste en “Remote Desktop”
 - Activer la webcam et enregistrer à l’insu de l’utilisateur
 - Audio Streaming
 - Récupérer tous les mots de passe
 - MSN Sniffer
 - Online & Offline keylogger
 - Etc..



Un commerce en pleine expansion...

	<p>Bronze Edition</p> <ul style="list-style-type: none"> ■ This product is the improved version of Turkojan 3.0 and it has some limitations(Webcam - audio streaming and msn sniffer doesn't work for this version) ■ 1 month replacement warranty if it gets deducted by any antivirus ■ 7/24 online support via e-mail ■ Supports only Windows 95/98/ME/NT/2000/XP ■ Realtime Screen viewing(controlling is disabled) <p>Price : 99\$ (United State Dollar)</p>
	<p>Silver Edition</p> <ul style="list-style-type: none"> ■ 4 months (maximum 3 times) replacement warranty if it gets deducted by any antivirus ■ 7/24 online support via e-mail and instant messengers ■ Supports 95/98/ME/NT/2000/XP/Vista ■ Webcam streaming is available with this version ■ Realtime Screen viewing(controlling is disabled) ■ Notifies changes on clipboard and save them <p>Price : 179\$ (United State Dollar)</p>
	<p>Gold Edition</p> <ul style="list-style-type: none"> ■ 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets deducted by any antivirus (you can choose 6 months or 9 months) ■ 7/24 online support via e-mail and instant messengers ■ Supports Windows 95/98/ME/NT/2000/2003/XP/Vista ■ Remote Shell (Managing with Ms-Dos Commands) ■ Webcam - audio streaming and msn sniffer ■ Controlling remote computer via keyboard and mouse ■ Notifies changes on clipboard and save them ■ Technical support after installing software ■ Viewing pictures without any download(Thumbnail Viewer) <p>Price : 249\$ (United State Dollar)</p>

Que dit le législateur?

Soucieux de la protection de la vie privée des citoyens et des actifs immatériels de l'entreprise (dont le Capital intellectuel), le législateur étoffe les contraintes légales avec le temps.

- France : CNIL loi n° 78-17 du 6/1/1978 – modifiée en 2004
- Cadre réglementaire Européen
 - Directive de protection des données 95/46/EC,
 - Directive ePrivacy 2002/58/EC
 - Directive « Privacy by Design » applicable au 1^{er} Janvier 2015

Cible : organisations de plus de 250 personnes

Pour tous les **nouveaux développements** intégrant des données privées et des données de l'entreprise

Amende : 2 % du chiffre d'affaires mondial de l'entreprise

- Décret de confidentialité pour les données médicales/ hébergeur de données de santé
- Les données personnelles appartiennent à leurs titulaires, tout accès non autorisé doit leur être notifié par courrier « papier » !

Pour innover et opérer en toute confiance, les organisations doivent gérer leurs risques Informatiques de bout en bout.

Gouvernance Risque et Conformité

Définir sa politique de sécurité

Gérer ses risques

Surveillance intelligente et conformité

Sécuriser les identités

- Fournir les ressources informatiques nécessaires à l'instant t à un utilisateur donné
- Gérer les accès

Protéger les Données

- Protéger les données
- Structurées en Bases de Données et
- non structurées dans des fichiers xls, pdf, ...

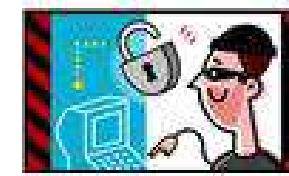
Protéger les Applications

- Concevoir des applications sécurisées dès la conception
- Corriger les vulnérabilités des applications en production
- Sécuriser les web services

Protéger les Infrastructures

- Réseaux
- Ordinateurs
 - Centraux
 - Serveurs
- Les postes de travail fixes/mobiles
 - Tablettes
 - Smartphones

Exemple : ce n'est pas parce que l'on dispose d'une carte à puce que l'intégralité de la chaîne du paiement par carte est sécurisée



Données sensibles : #CB,
Date de validité, CVV

Il existe plusieurs chemins pour accéder aux données cartes, le dupliquer pour les revendre ou pour acheter frauduleusement sur internet.

VISA, MC, AMEX, JCB ont défini le standard PCI DSS auquel toutes banques ou e-marchands « doivent » se conformer.



Gouvernance – Risques – conformité



Répondre aux questions urgentes

Quels sont les risques ?

Quels contrôles mettre en place ?

Comment démontrer la conformité ?

Comment surveiller de manière
proactive mon système ?



Gestion des accès et des identités des personnes (et des objets)

Répondre aux questions urgentes

Est-ce que le registre des identités est précis et à jour ?

Quelle gestion des identités dans un cloud?

Comment re-certifier les habilitations ?

Comment contrôler les utilisateurs privilégiés?

Qui accède à quoi?



Protéger les données contre les accès non autorisés

Répondre aux questions urgentes

Où sont les données sensibles?
Sous quelles formes sont-elles ?
Comment les protéger ?
Que font les administrateurs de bases de données ?

Web Application Vulnerabilities
as a Percentage of All Disclosures in 2012 H1

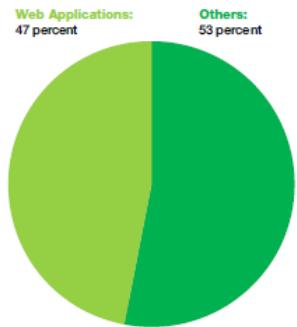


Figure 35: Web Application Vulnerabilities as a Percentage of All Disclosures in 2012 H1

Sécuriser les applications “by design”

Répondre aux questions urgentes

Les nouvelles applications sont-elles
“sécurisées” ?

Comment corriger les vulnérabilités
existantes ?

Comment sécuriser les webservices ?



Fermer la porte aux hackers

Répondre aux questions urgentes

Qui attaque mon système ?
Quelles sont les dernières mesures de protection ?
Comment se protéger des nouvelles attaques ?



Maîtrise ses postes de travail et équipements connectés sur le réseau

Répondre aux questions urgentes

Comment protéger les postes de travail ?

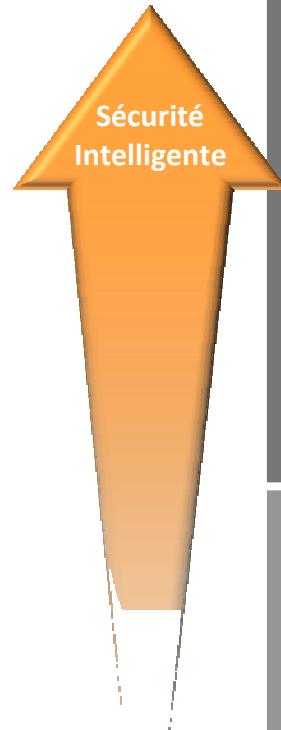
Comment vérifier la conformité par rapport aux politiques de sécurité ?

Comment protéger les terminaux mobiles ?

Comment gérer le BYOD ?

Les besoins en formation pour les années à venir

- Spécialistes Juridiques de la sécurité numérique / CNIL + « privacy by design »
- Spécialistes en sécurité informatique – white hats
- Architectes Sécurité
- Analystes Sécuritaires
- Spécialistes sécurité Réseaux, IAM, Données, Applications,
- Gestionnaires de risques informatiques
-



Niveaux/ domaines	Identités	Données	Applications	Sécurité Intelligente:
				Corrélation de Logs en temps réel et analyse comportementale des flux sur le réseaux Assistance externe d'un service de recherche en menaces
Basique	Annuaire centralisé	Chiffrement Contrôle d'accès	Scanner d'application	Sécurité périphérique Anti virus/anti malware
Avancé	Provisionning des Utilisateurs Gestion des accès Authentification forte	Surveillance des accès aux données Prévenir contre le vol de données	Pare feu applicatif Scanner de code source	Sécurité de la virtualisation Gestion Sécuritaire des équipements et terminaux/ Réseaux
Optimisé	Analyse en fct des rôles Gouvernance ID Gestion des Utilisateurs privilégiés	Analyse des flux de données Gouvernance des données	Procesus d'ingénierie d'applications Détection de la fraude	Surveillance avancée du réseau Investigation / data mining Systèmes sécurisés

Questions?



Merci

http://www.ibm.com/smarterplanet/us/en/business_resilience_management/article/security_essentials.html

<https://www-935.ibm.com/services/us/iss/xforce/trendreports/>