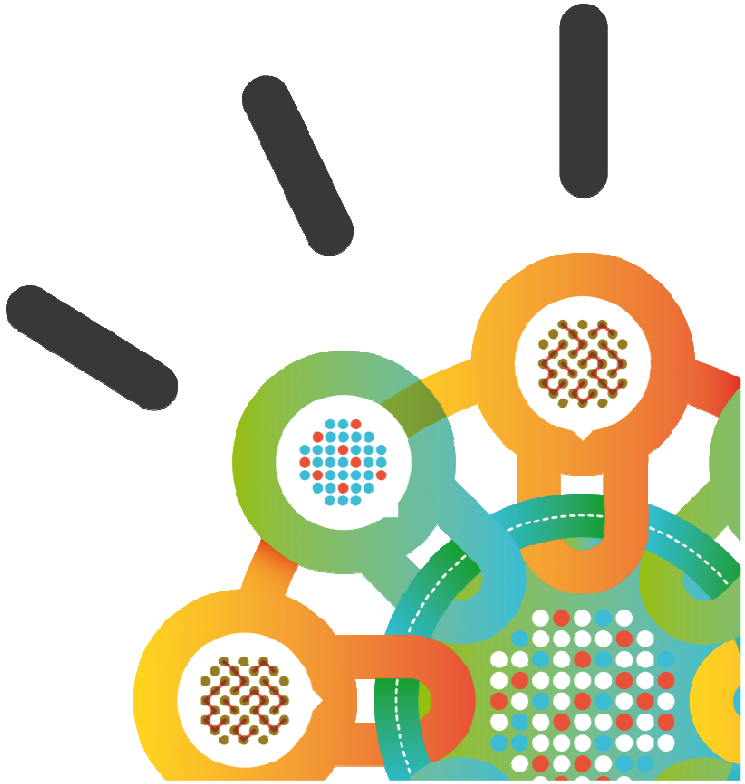
Security Intelligence.
Think Integrated.

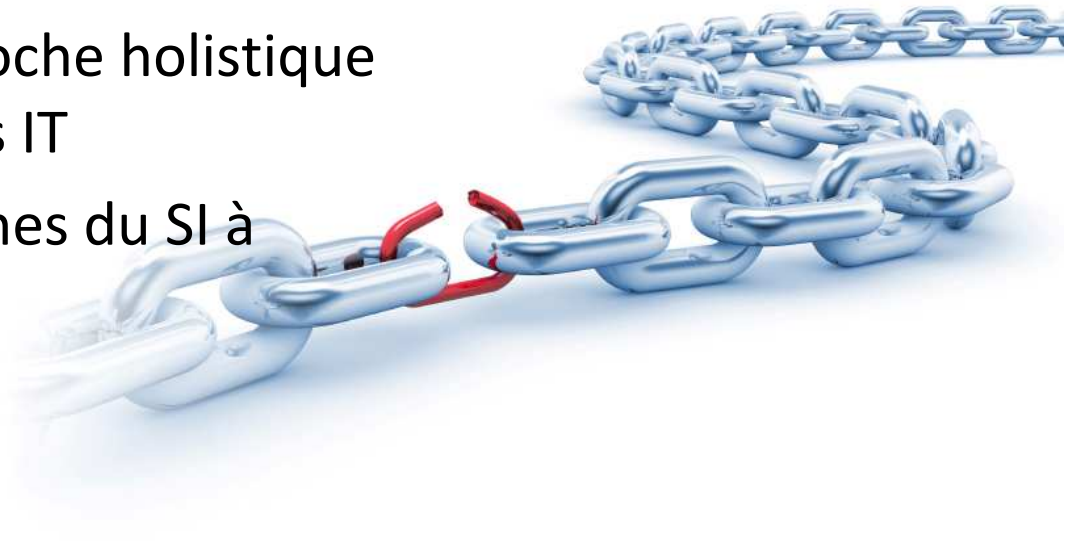
Rationalité et irrationalité dans le gestion des risques informatiques

Sophie Tacchi
sophie_tacchi@fr.ibm.com



Agenda

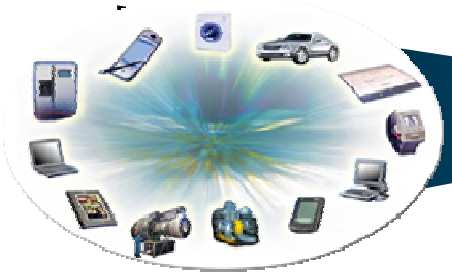
- Evolution technologique, innovation
- Typologie des risques
- Analyse de la nature des menaces
- Qu'en dit le législateur ?
- Nécessité d'une approche holistique de gestion des risques IT
- Les principaux domaines du SI à sécuriser
- Besoins en formation
- Conclusions



Bienvenue dans **une planète plus intelligente** …

Globalisation et virtualisation des ressources, consommation de l'informatique dans le cloud

Milliards d'équipements et d'individus accèdent au web



Accès à l'information

En temps réel

Nouvelles formes d'échange et de collaboration – réseau sociaux

+ de possibilités

+ de complexité

Nouveaux risques

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

▪ Pannes d'électricité ▪ Désastres naturels ▪ Bouleversements politiques ou économiques	▪ Malware ▪ Déni de service ▪ Attaques sophistiquées et organisées
▪ Systèmes non patchés ▪ Vulnérabilité du code ▪ Pas contrôle des changements ▪ Erreur humaine	▪ "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

Areva victime d'une intrusion informatique

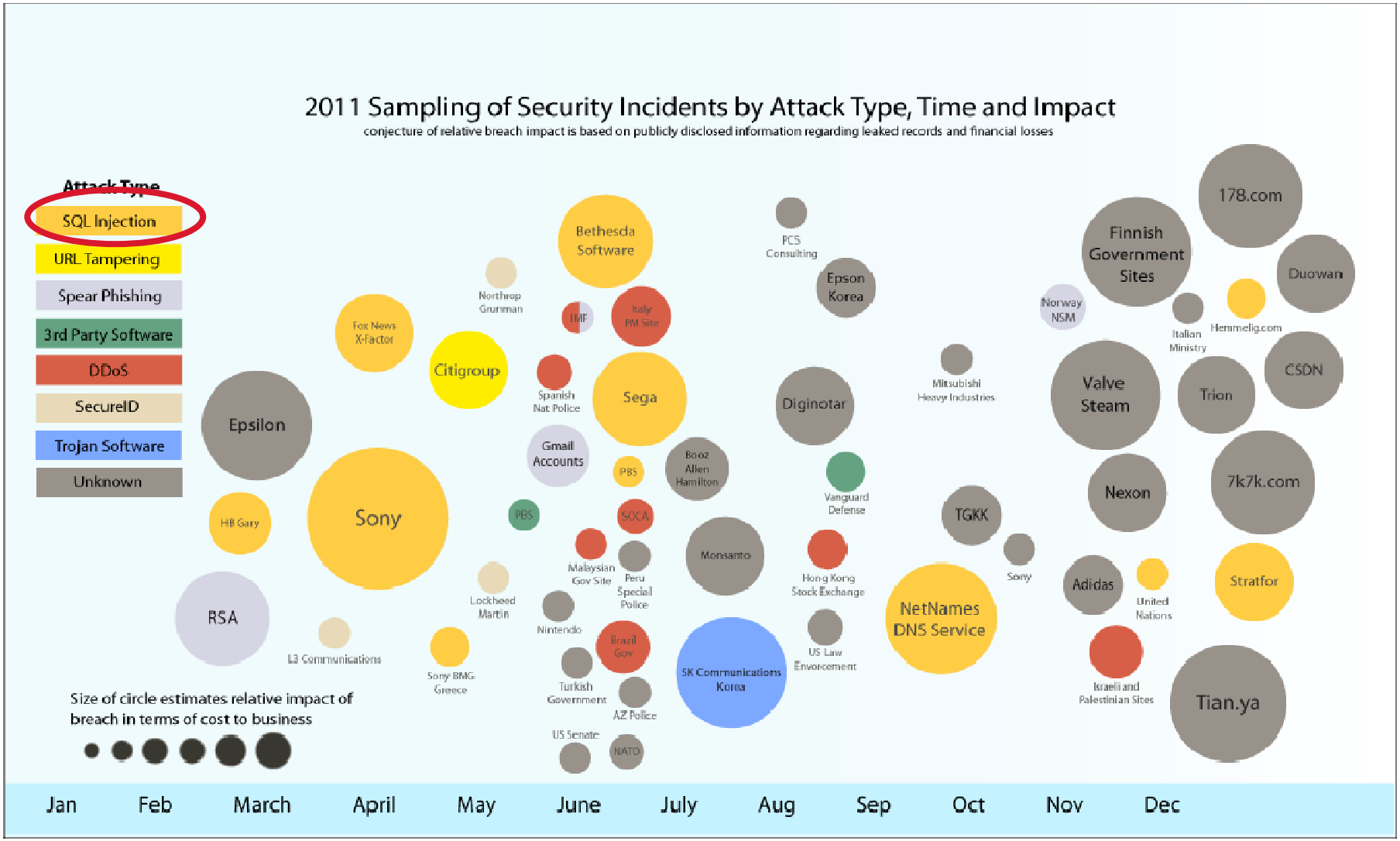
Vaste fuite de données bancaires

Une bombe informatique au Crédit mutuel-CIC

Le système d'information du Crédit Mutuel-CIC est mis à mal

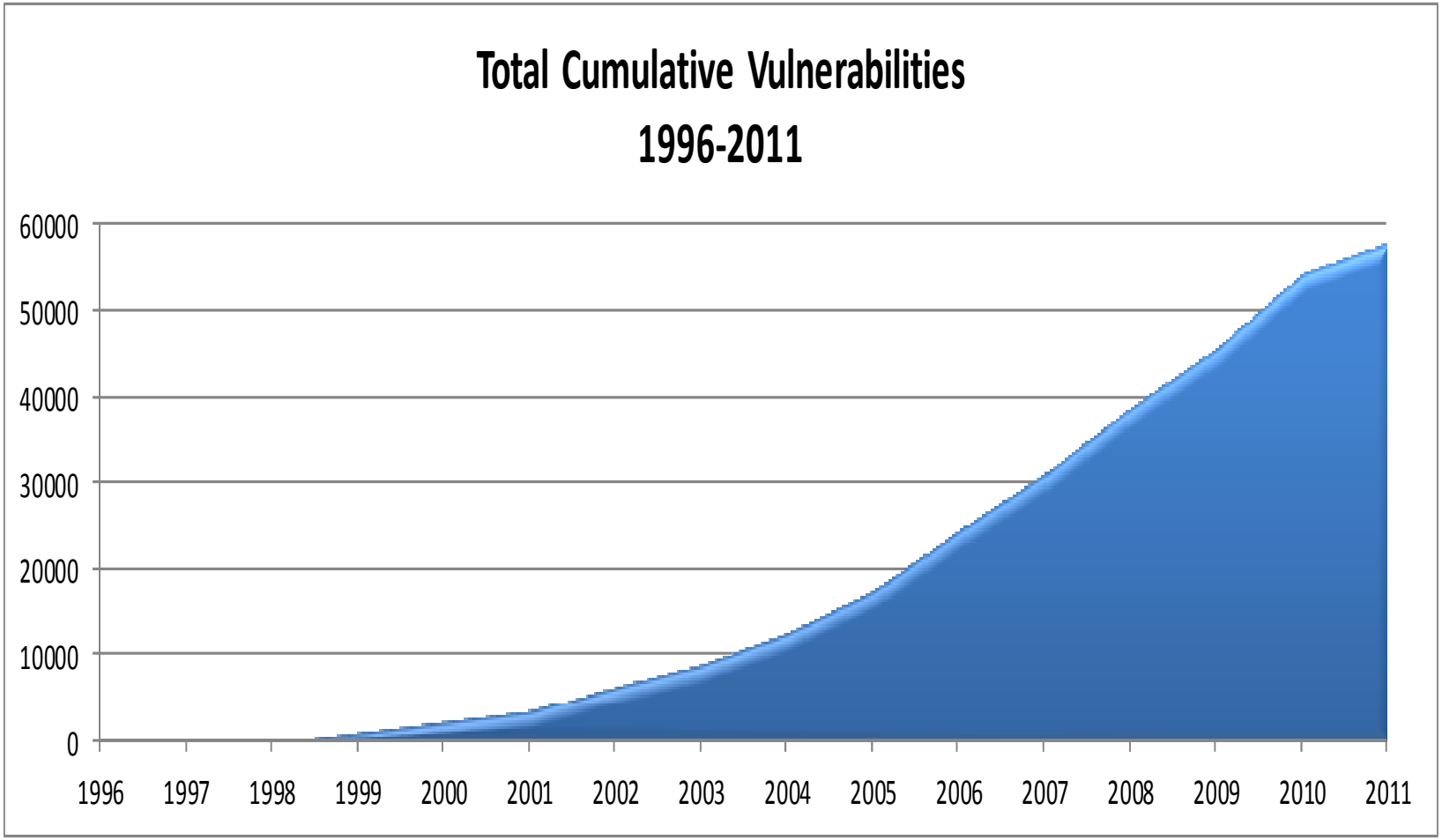
Bercy victime d'une attaque informatique

Exemples d'attaques ciblées visant des entreprises et des gouvernements

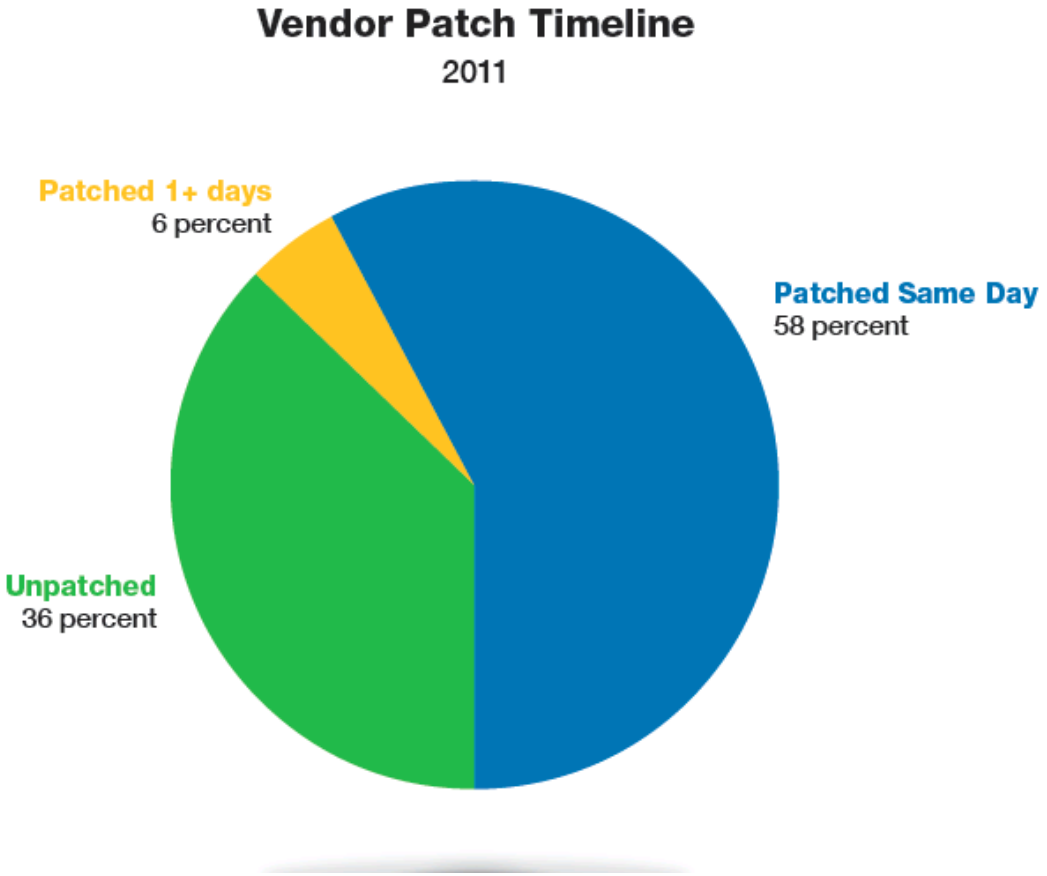


IBM Security X-Force® 2012 Trend and Risk Report

Vulnérabilités cumulées – XForce 2012



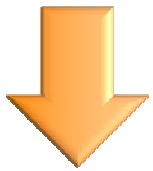
Les vulnérabilités sont peu « patchées » mais la tendance s'améliore.



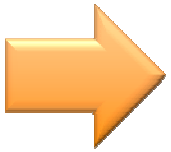
	2011	2010	2009	2008	2007	2006
Unpatched %	36.0%	43.3%	45.1%	51.9%	44.6%	46.6%

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

Un Utilisateur

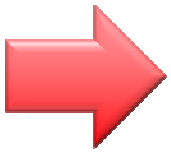


Surfe sur internet



Serveur Web qui intègre un iframe

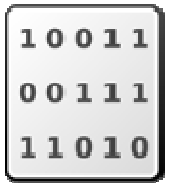
Serveur iframe malicieux



Téléchargement sur le poste de l'utilisateur

Malware installé et activaté

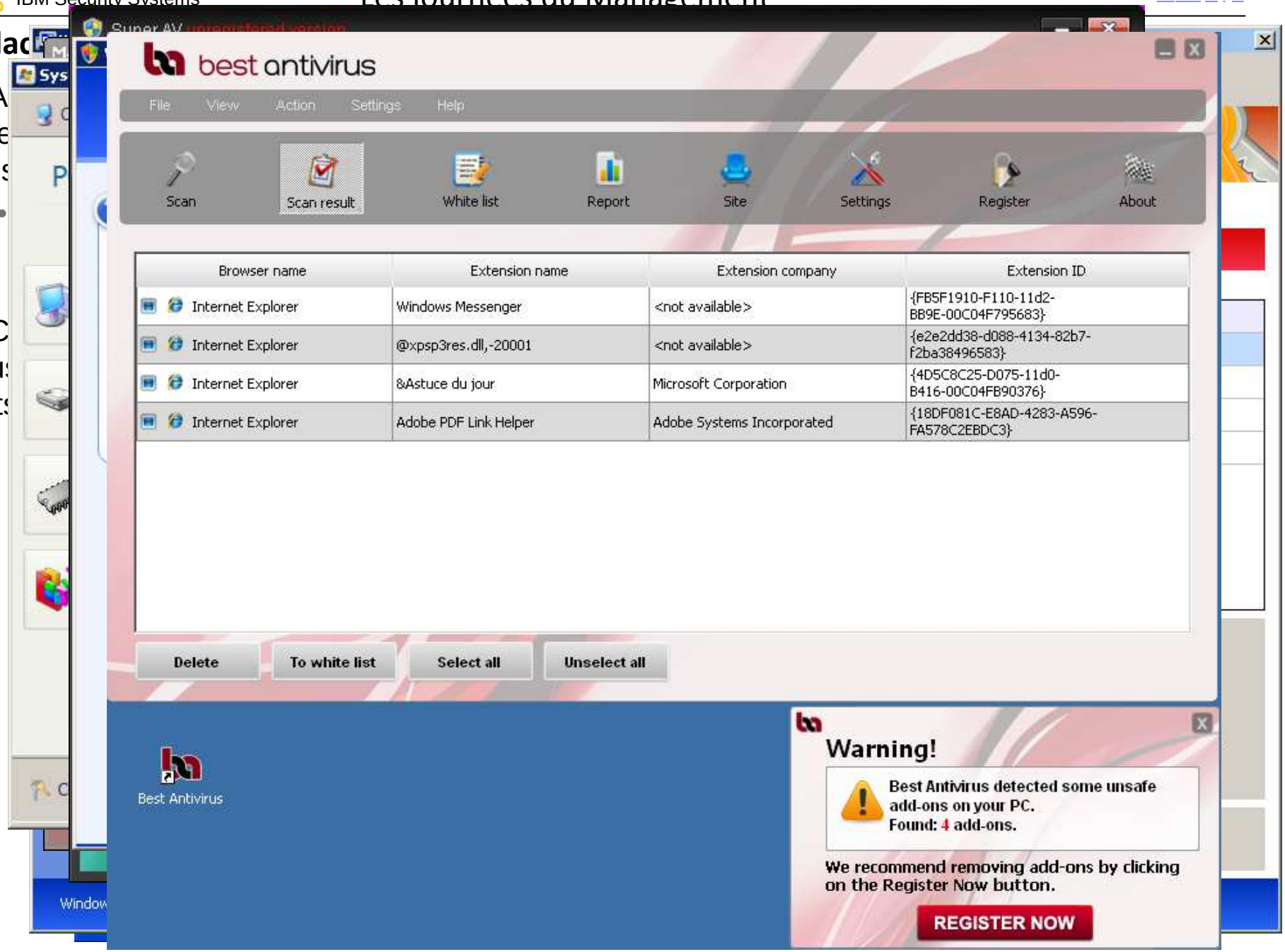
« Downloader » installé



Code malicieux téléchargé

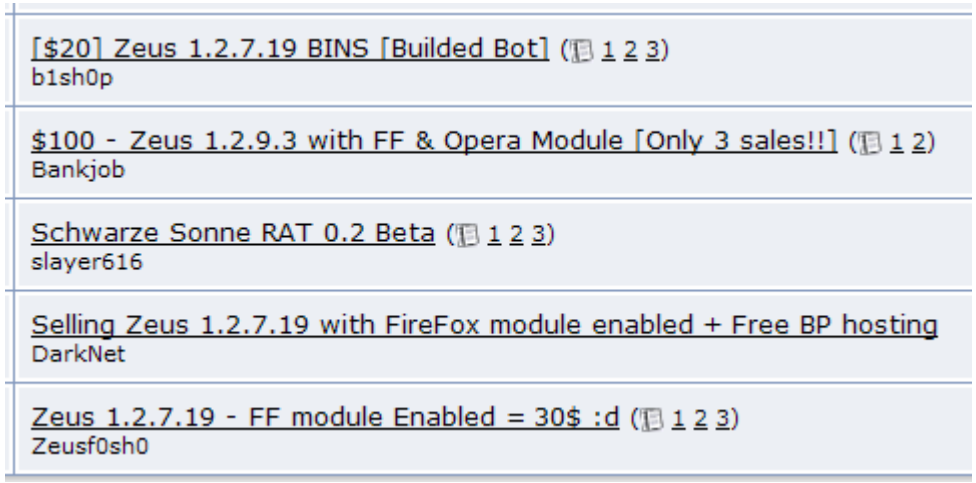
Blac

- A
  te
  lis
  -
- C
  us
  its

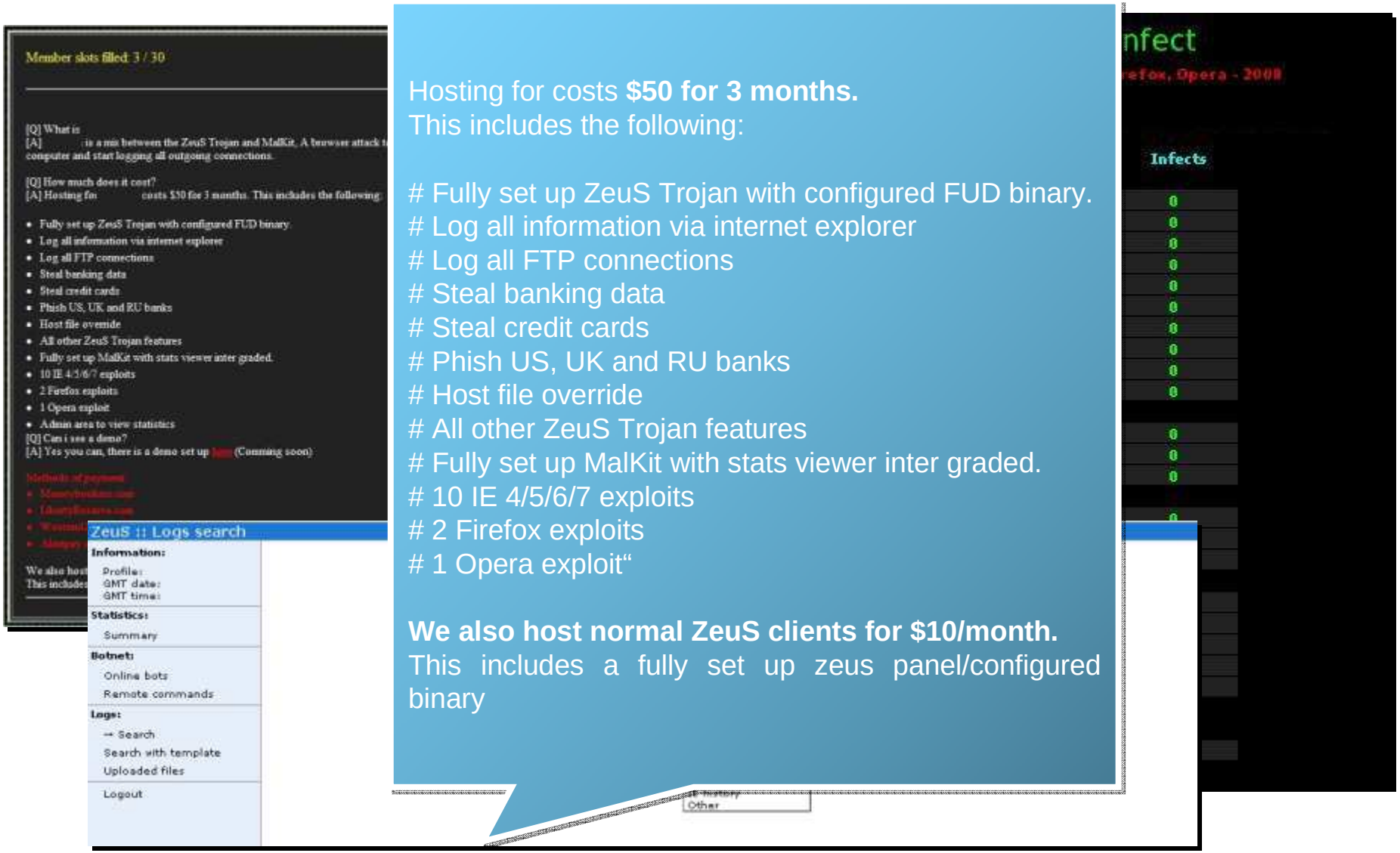


Tendances en terme de malware

- 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



Zeus Services de cybercriminalité



Hosting for costs **$50 for 3 months.**
This includes the following:

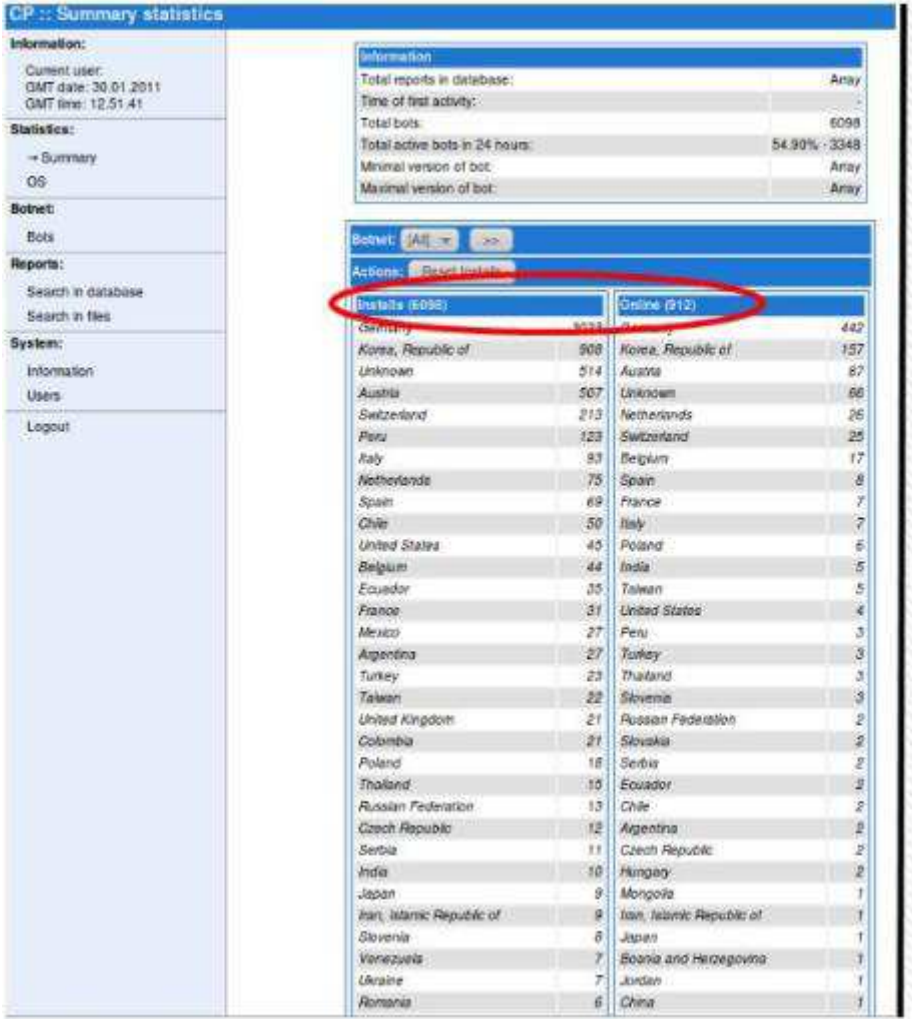
Fully set up ZeuS Trojan with configured FUD binary.
Log all information via internet explorer
Log all FTP connections
Steal banking data
Steal credit cards
Phish US, UK and RU banks
Host file override
All other ZeuS Trojan features
Fully set up MalKit with stats viewer inter graded.
10 IE 4/5/6/7 exploits
2 Firefox exploits
1 Opera exploit“

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



Trojan Creator Kits

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

Un commerce en pleine expansion…

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 1er Janvier 2015

    Cible : organisations de plus de 250 personnes

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

    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	**Protéger les Données**	**Protéger les Applications**	**Protéger les Infrastructures**
•Fournir les ressources informatiques nécessaires à l'instant t à un utilisateur donné •Gérer les accès	Protéger les données • Structurées en Bases de Données et • non structurées dans des fichiers xls, pdf, …	• Concevoir des applications sécurisées dès la conception • Corriger les vulnérabilités des applications en production • Sécuriser les web services	•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 chaine du paiement par carte est sécurisée

Télecollecteur

Banque du commerçant

Boutique e commerce

Données sensible : #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.

PCI Security Standards Council


Gouvernance – Risques - conformité
IBM
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 privilégies?
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 ?

Sécuriser les applications “by design”

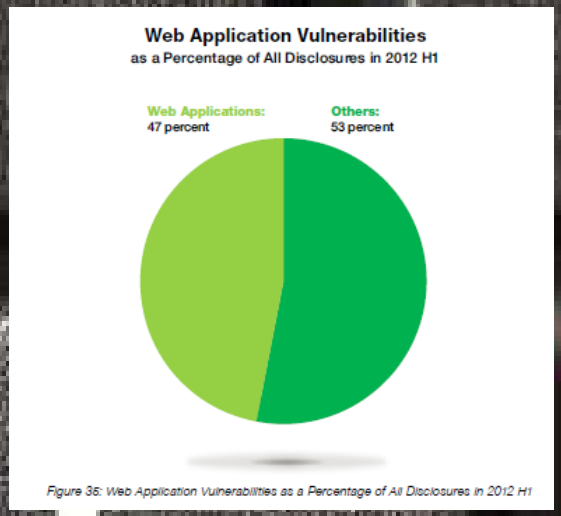


Figure 35: Web Application Vulnerabilities as a Percentage of All Disclosures in 2012 H1

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 ?

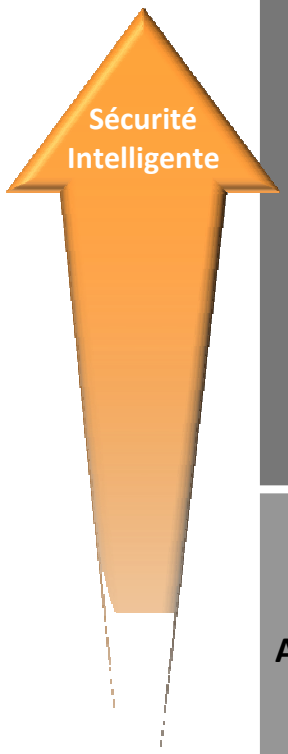
Comment protéger les terminaux mobiles ?

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
- ……..

Recommandations : mettre en œuvre les points de contrôles suivants pour devancer les menaces et mieux protéger son SI



	Sécurité Intelligente: Gestion des événements et des information de sécurité Corrélation de Logs en temps réélet analyse comportementale des flux sur le réseaux Assistance externe d'un service de recherche en menaces			
Optimisé	Analyse en fct des rôles Gouvernance ID Gestion des Utilisateurs privilégiés	Analyse des flux de données Gouvernance des données	Procesus d'ingéniérie d'applicatoins Détection de la fraude	Surveillance avancée du réseau Investigation / data mining Systèmes sécurisés
Avancé	Provisionning des Utilisateurs Gestion des accès Authentificaiton 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
Basique	Annuaire centralisé	Chiffrement Contrôle d'acces	Scanner d'application	Sécurité périmétrique Anti virus/anti malware
Niveaux/ domaines	**Identités**	**Données**	**Applications**	**Infrastructure**

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/