Cyber Sécurité

Les dernières tendances

Conférence ASAGE

19 novembre 2014

Résidence de France – Genève

par **Bruno.KEROUANTON.net**

@kerouanton

©2014 bruno.kerouanton.net

INTERNET

Le pirate, cet être si prévisible

Une étude du comportement des utilisateurs de BitTorrent, menée sur quatre ans, révèle des agissements très répétitifs. La vraie surprise, c'est qu'elle dresse un profil des économies de certains pays à travers le type de fichiers piratés.

COURRIER INTERNATIONAL | VIRGINIE LEPETIT

8 OCTOBRE 2014 | 0 RÉAGIR PARTAGER :

Un garçon devant son ordinateur - Flickr/Nic McPhee

©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

by **Michael Mimoso** Follow @mike_mimoso

December 12, 2013 , 2:34 pm

European diplomats and ministries of foreign affairs have been targeted during recent G20 meetings by Chinese-speaking hackers conducting espionage campaigns using malware to siphon secrets from compromised computers.

The latest incidents came in August when spear phishing messages spiked with attachments promising information on U.S. military options in Syria zeroed in on diplomats

©2014 bruno.kerouanton.net

Opération Ke3chang
Vise les diplomates européens

Operation "Ke3chang": TargetedAttacks Against Ministries of Foreign Affairs

Figure 5:
BS2005 "snake" campaign email attack vector

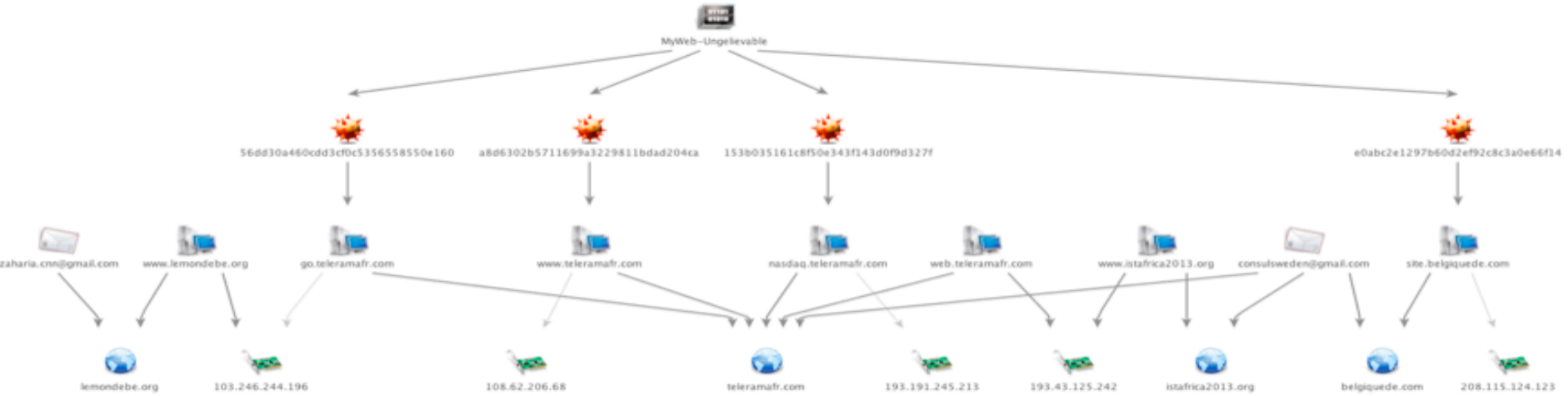
```
From:Consulat [illegible] <consulat.[illegible]@yahoo.fr>
To: [illegible]
Date:10/27/2011 03:10 AM
Subject:RE:French first lady nude photos !


Ladies and Gentlemen,

First Lady Nude Photos: Link-
http://www.allstarpics.sexxxy.biz/pic-gallery/carla-bruni-nude-pics.rar

password:allstarpics

Cheers,

Carlos
```


©2014 bruno.kerouanton.net

Opération Ke3chang

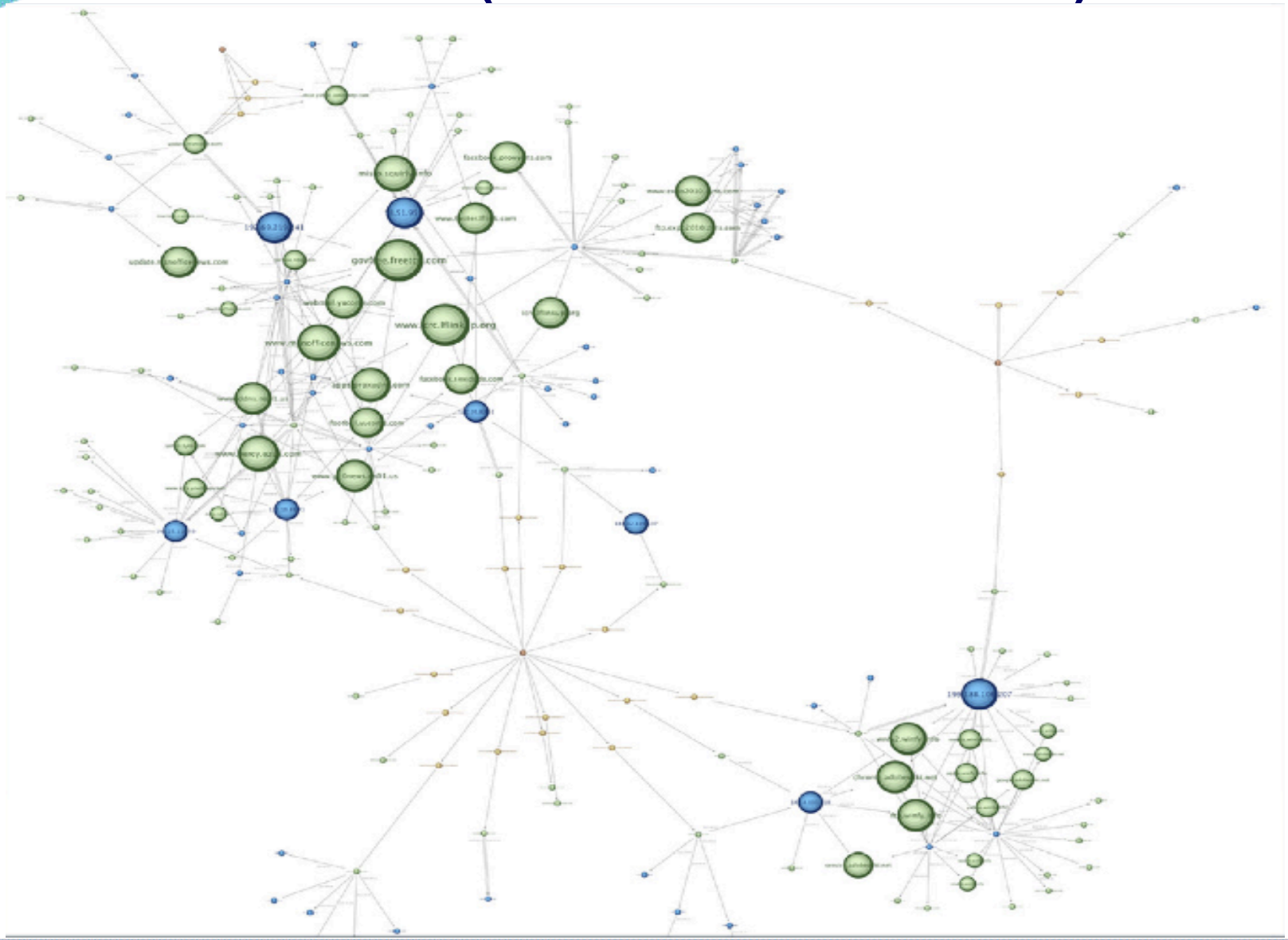
Système d'attaque actif depuis 2010, visant les industries aérospatiales, énergie, technologies de pointe, et gouvernements.

- Août 2013 : attaque avant le sommet du G20 en Russie sur la crise syrienne.
- 23 serveurs de contrôle. 9 ministères européens infiltrés, dont 8 Ministères des Affaires Etrangères.



©2014 bruno.kerouanton.net

C&C (Command & Control)



©2014 bruno.kerouanton.net

APT (Advanced Persistent Threat)

1. RECONNAISSANCE

Attacker leverages information from a variety of factors to understand their target.

2. INCURSION

Attackers break into network by using social engineering to deliver targeted malware to vulnerable systems and people.

3. DISCOVERY

Once in, the attackers stay "low and slow" to avoid detection.

They then map the organization's defenses from the inside and create a battle plan and deploy multiple parallel kill chains to ensure success.

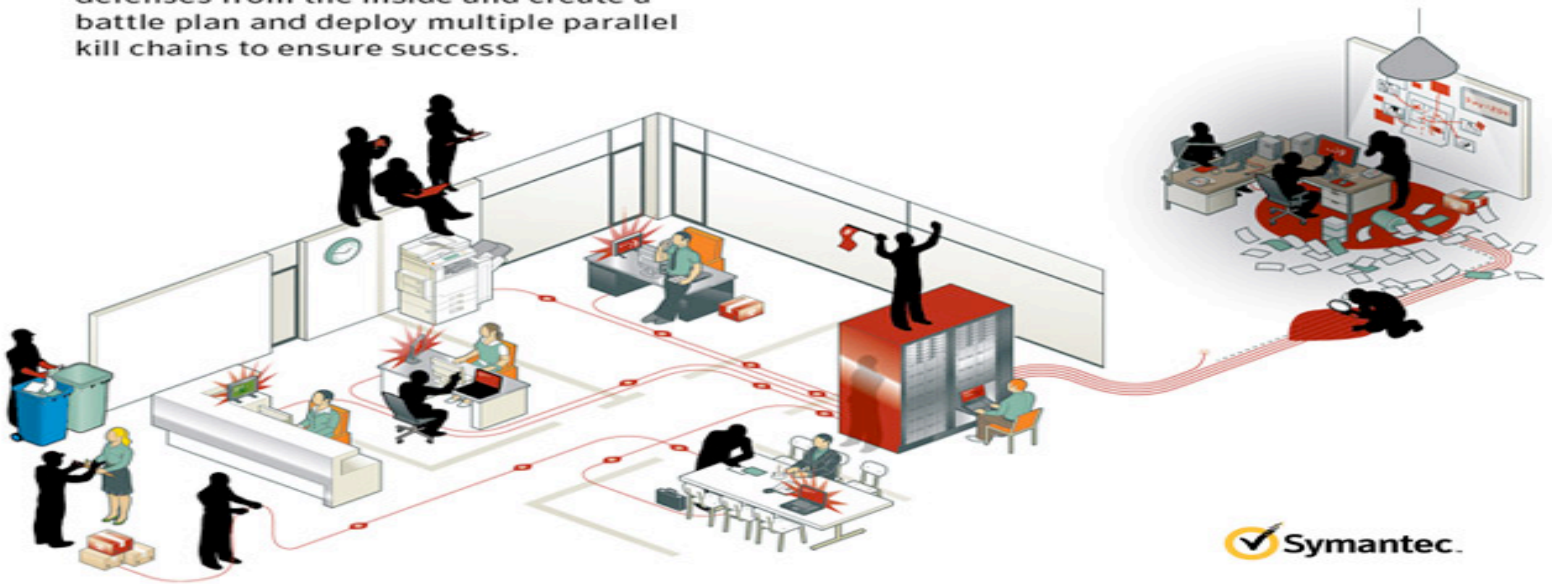
4. CAPTURE

Attackers access unprotected systems and capture information over an extended period.

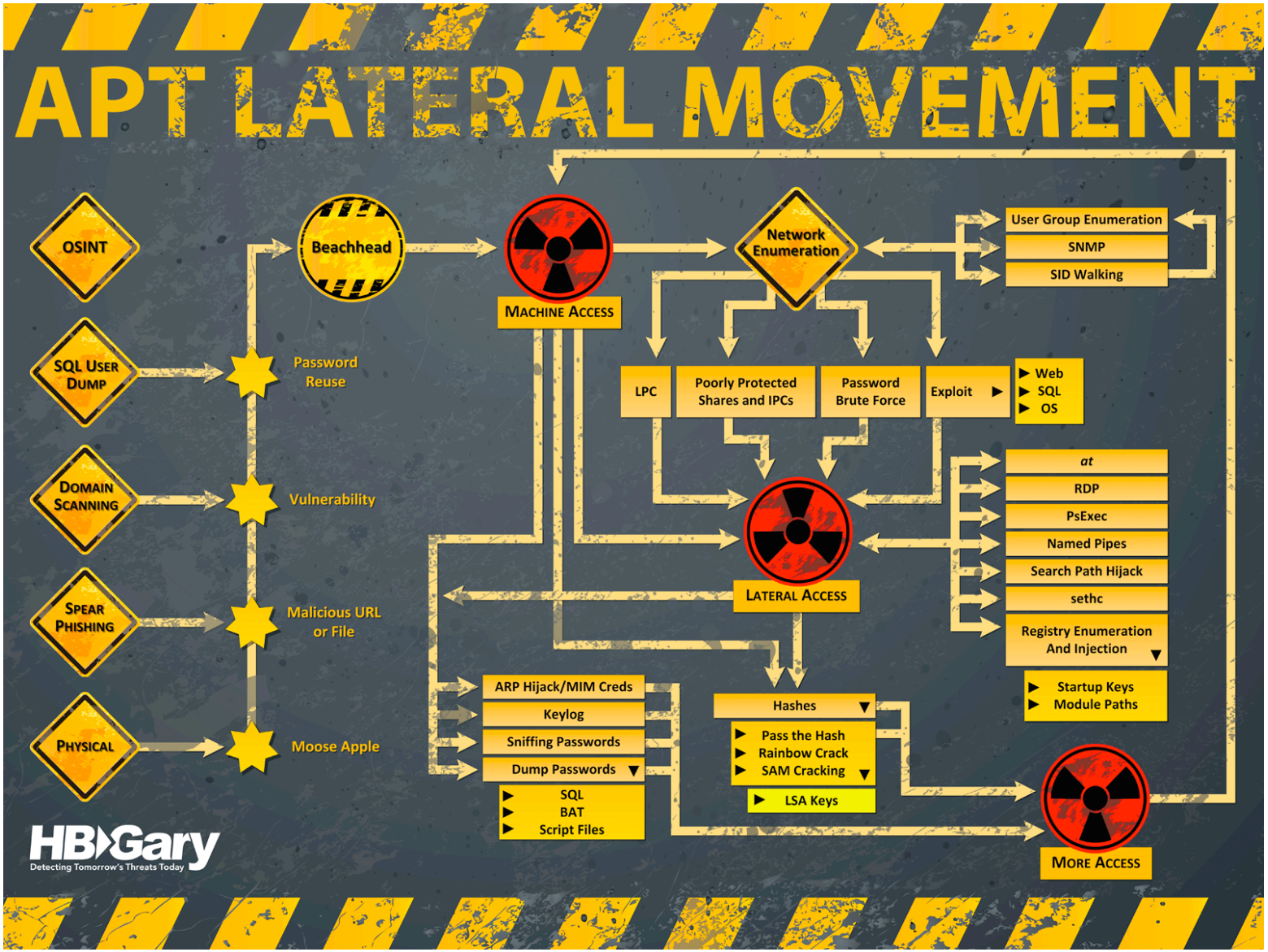
They may also install malware to secretly acquire data or disrupt operations.

5. EXFILTRATION

Captured information is sent back to attack team's home base for analysis and further exploitation fraud—or worse.



©2014 bruno.kerouanton.net



©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign

By Stephen Ward | October 14, 2014 | iSIGHT Partners

SandWorm Team Zero-day impacting all versions of Microsoft Windows – used in Russian cyber-espionage campaign targeting NATO, European Union, Telecommunications and Energy sectors

UPDATE – 10/21/14

©2014 bruno.kerouanton.net

Sandworm Windows zero-day vulnerability being actively exploited in targeted attacks

Critical new Windows zero-day has reportedly been used in a limited number of targeted cyberespionage attacks to deliver a back door on to the victim's computer.

Created: 14 Oct 2014 15:38:06 GMT • Updated: 17 Oct 2014 11:51:07 GMT • Translations available: 日本語, 한국어, Português

Symantec Security Response SYMANTEC EMPLOYEE

+3 3 Votes

Symantec. | Official Blog

Tweet

A critical new vulnerability in the Windows operating system is reportedly being exploited in a limited number of attacks against targets in the US and Europe. The Microsoft Windows OLE Package Manager Remote Code

©2014 bruno.kerouanton.net

Faille dans Certicode : des millions d'euros dérobés à la Banque Postale

Sécurité : *Une faille dans le système Certicode de la Banque Postale a été exploitée par des escrocs pour virer illégalement des fonds depuis des comptes clients. Plusieurs interpellations ont eu lieu cette semaine. Le préjudice total serait de 25 millions d'euros.*

Par La rédaction de ZDNet.fr | Vendredi 07 Novembre 2014
Suivre @zdnetfr

Censé sécuriser les opérations réalisées sur téléphone mobile par les clients de la Banque Postale, le système Certicode de la banque française aurait comporté une faille, largement exploitée par des escrocs pour détourner des fonds.

Selon La Dépêche, la Banque Postale a alerté la direction centrale de la police judiciaire. Le préjudice serait estimé à plusieurs millions d'euros. RTL.fr évoque lui un préjudice total de 25 millions d'euros. Et différents escrocs auraient ainsi exploité cette faille ces derniers mois.

Des suspects fichés par la DGSI

Ce serait notamment le cas de sept individus, interpellés mercredi par la PJ de Toulouse. Ils sont soupçonnés d'avoir ainsi détourné plusieurs

©2014 bruno.kerouanton.net

La poste américaine victime d'une cyberattaque

Le Monde | 10.11.2014 à 18h37 • Mis à jour le 10.11.2014 à 20h31

L'US Postal Service, la poste américaine, a annoncé lundi 10 novembre avoir été victime d'une cyberattaque. L'entreprise a annoncé craindre que les données personnelles de ses 800 000 employés ou sous-traitants et de certains clients aient été volées.

« Le service postal a récemment appris qu'une cyberintrusion avait visé certains de nos systèmes d'information. Nous avons lancé une enquête sur cet incident dès que nous en avons été informés », a déclaré le groupe dans un communiqué.

LE FBI ENQUÊTE

©2014 bruno.kerouanton.net

Darkhotel, quand les pirates visent les cadres en voyage d'affaires

Sécurité : *Cette campagne d'espionnage révélée par Kaspersky cible les connexions de cadres dirigeants dans leurs chambres d'hôtel. Les attaques auraient débuté il y a 4 ans.*

Par La rédaction de ZDNet.fr | Mercredi 12 Novembre 2014
Suivre @zdnetfr

Article mis à jour le 13 novembre à 12h30

Si les connexions Internet en Wi-Fi sont devenues dans les hôtels une commodité au même titre que la télévision ou le téléphone, se pose la question de la sécurisation de ces accès. Or, il semble que des carences à ce niveau soient allègrement exploitées par des pirates.

En effet, les experts du GReAT de Kaspersky Lab ont découvert une vaste campagne d'espionnage à travers ce vecteur. Bien sûr, il ne s'agit pas de fouiller dans n'importe quel PC de voyageur en transit mais bien de cibler les machines connectées de cadres dirigeants afin de mettre la main sur des informations sensibles.

©2014 bruno.kerouanton.net

Surveillance généralisée

Publié le 12 Novembre 2014

Piratage massif de webcams dans le monde : votre chambre et votre salon font-ils partie des 73 000 flux diffusés en direct sur un site russe ?

La faiblesse des mots de passe informatiques a permis ce piratage qui concerne plus de 3000 caméras en France.

Security Response

Operation CloudyOmega: Ichitaro zero-day and ongoing cyberespionage campaign targeting Japan

The campaign was launched by an attack group that has communication channels with other notorious attack groups including Hidden Lynx and the group responsible for LadyBoyle.

Created: 13 Nov 2014 05:49:55 GMT • Updated: 13 Nov 2014 10:26:26 GMT • Translations available: 日本語

Symantec Security Response SYMANTEC EMPLOYEE

0 Votes

Symantec. | Official Blog

Tweet

JustSystems has issued an update to its Ichitaro product line (Japanese office suite software), plugging a zero-day vulnerability. This vulnerability is being actively exploited in the wild to specifically target Japanese organizations.

The exploit is sent to the targeted organizations through emails with a malicious Ichitaro document file attached, which Symantec products detect as Bloodhound.Exploit.557. Payloads from the exploit may include Backdoor.Emdivi, Backdoor.Korplug, and Backdoor.ZXshell; however, all payloads aim to steal confidential information from the compromised computer.

©2014 bruno.kerouanton.net

LA TRIBUNE ECONOMIE BOURSE ENTREPRISES & FINANCE HI-TECH VO

Airbus Helicopters a-t-il été victime d'un piratage informatique américain ?

Airbus Helicopters a-t-il subi une attaque informatique des Etats-Unis dans le cadre de l'appel international lancé par la Pologne qui veut acquérir 70 hélicoptères de transport (Crédits : DGA)

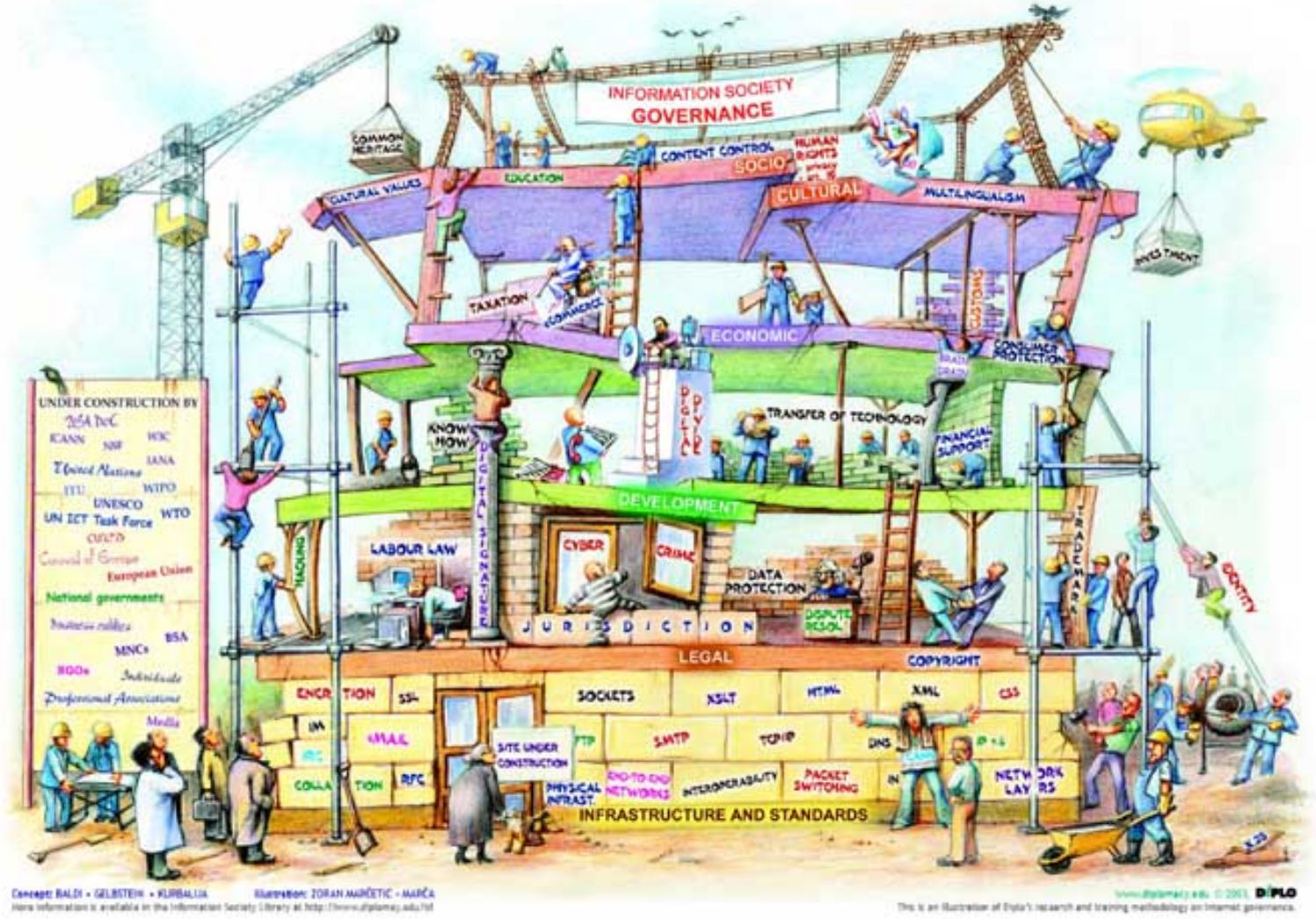
Michel Cabirol | 13/11/2014, 6:56 - 671 mots

Selon des sources concordantes, Airbus Helicopters a été victime d'une attaque informatique. Le constructeur a de "fortes suspicions" d'une attaque venant des États-Unis.

©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

La complexité du problème



©2014 bruno.kerouanton.net

Le périmètre de la sécurité

…du point de vue du «RSSI»

Postes de travail

Conformité réglementaire

Réseaux

Systèmes

Bases de données

Plans de secours

Pandémies

PKI

Gestion d'incident

Sauvegardes

Messagerie

Politiques

Téléphonie

Plan de continuité

Architecture

Contrôle d'accès

Documentations

Mobilité

Veille

Audits

Procédures

Nomadisme

Fournisseurs

Physique

Sensibilisation

Dans les projets

Applicative

De l'information

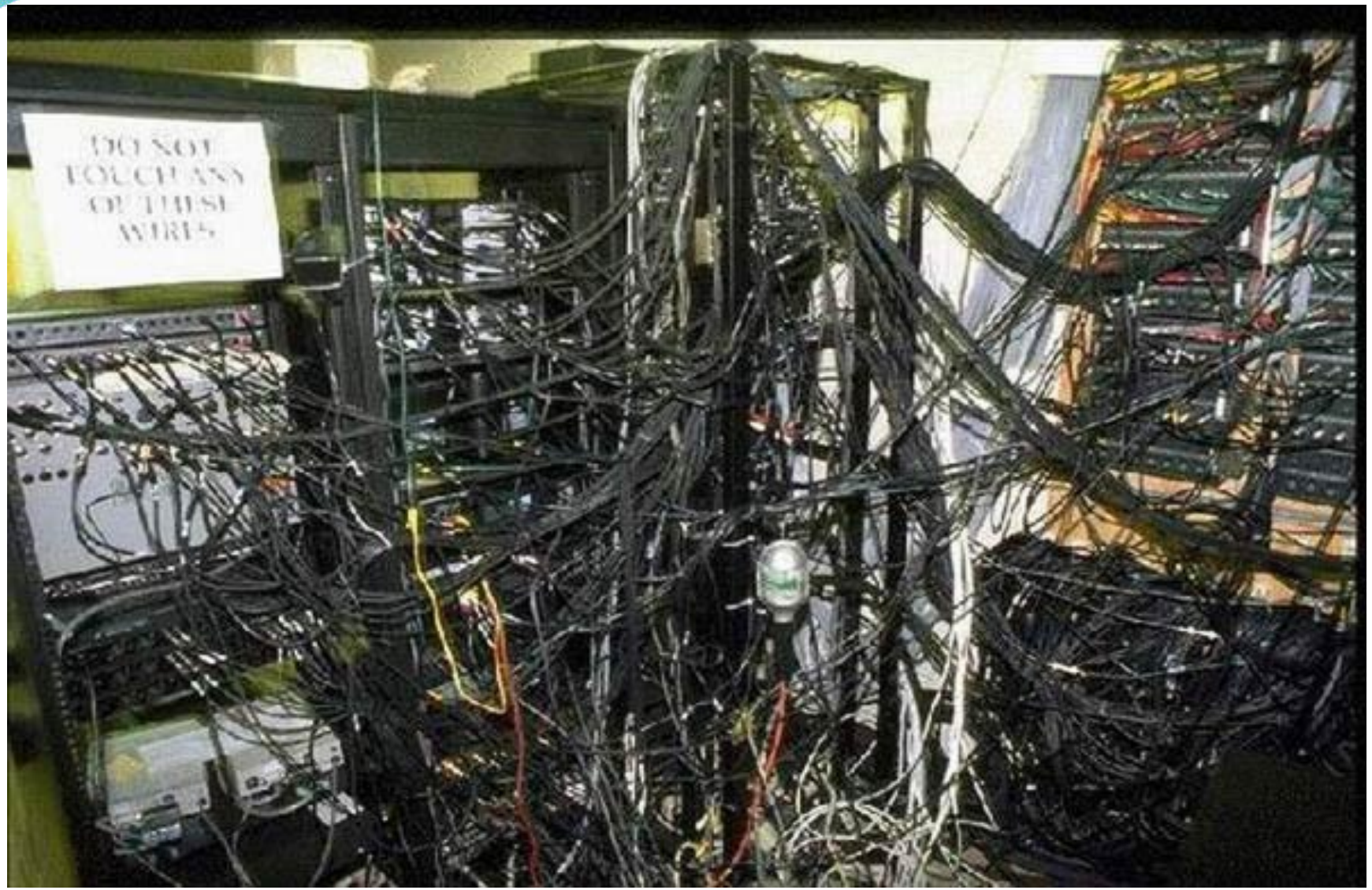
Archivage

Contrats

Web

etc…etc…etc…

©2014 bruno.kerouanton.net

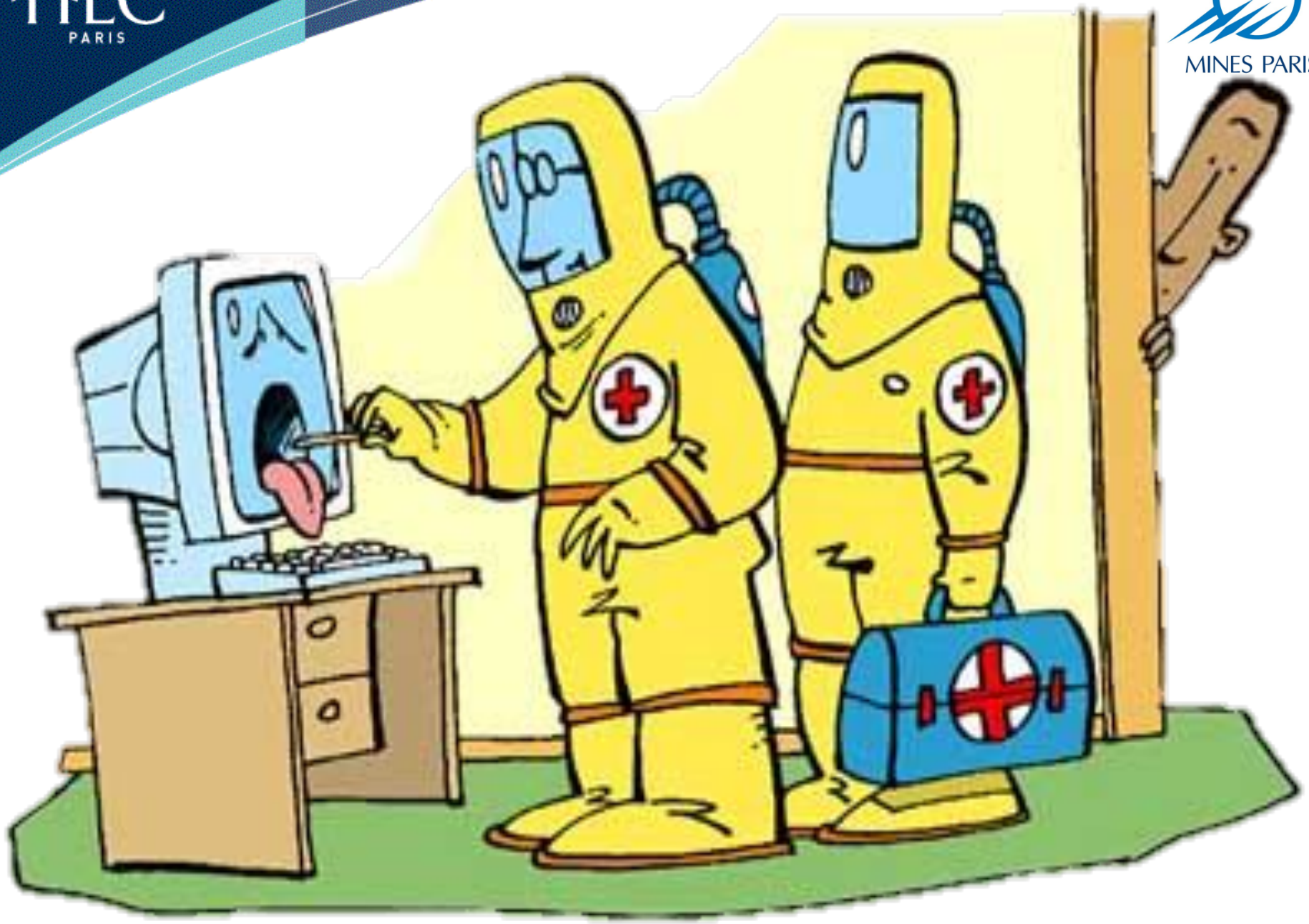


©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

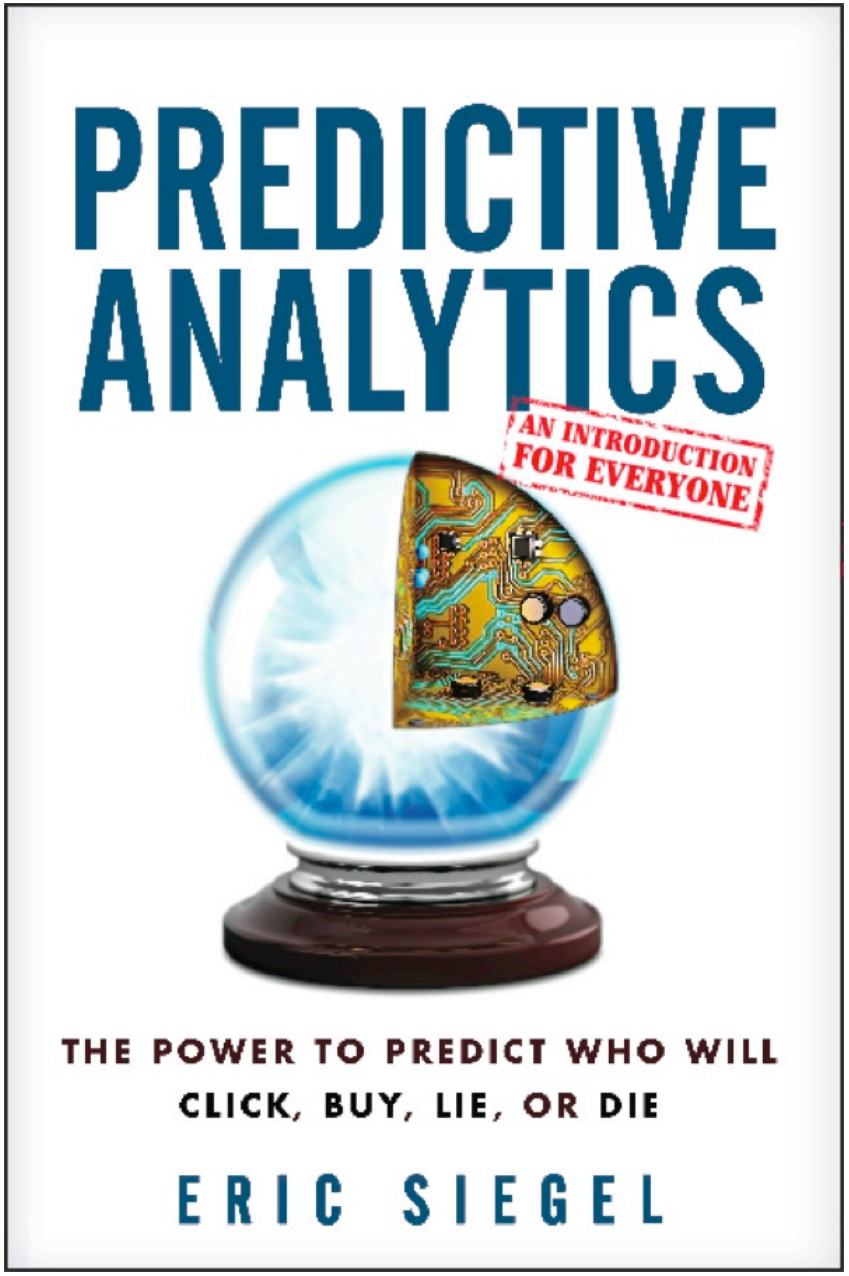
©2014 bruno.kerouanton.net



©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net



©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

©2014 bruno.kerouanton.net

Structured, analytical, repeatable

Creative, exploratory, intuitive

Security Intelligence Platform

Real-time Processing

- Real-time data correlation
- Anomaly detection
- Event and flow normalization
- Security context & enrichment
- Distributed architecture

Security Operations

- Pre-defined rules and reports
- Offense scoring & prioritization
- Activity and event graphing
- Compliance reporting
- Workflow management

IBM Security Intelligence with Big Data

Big Data Platform

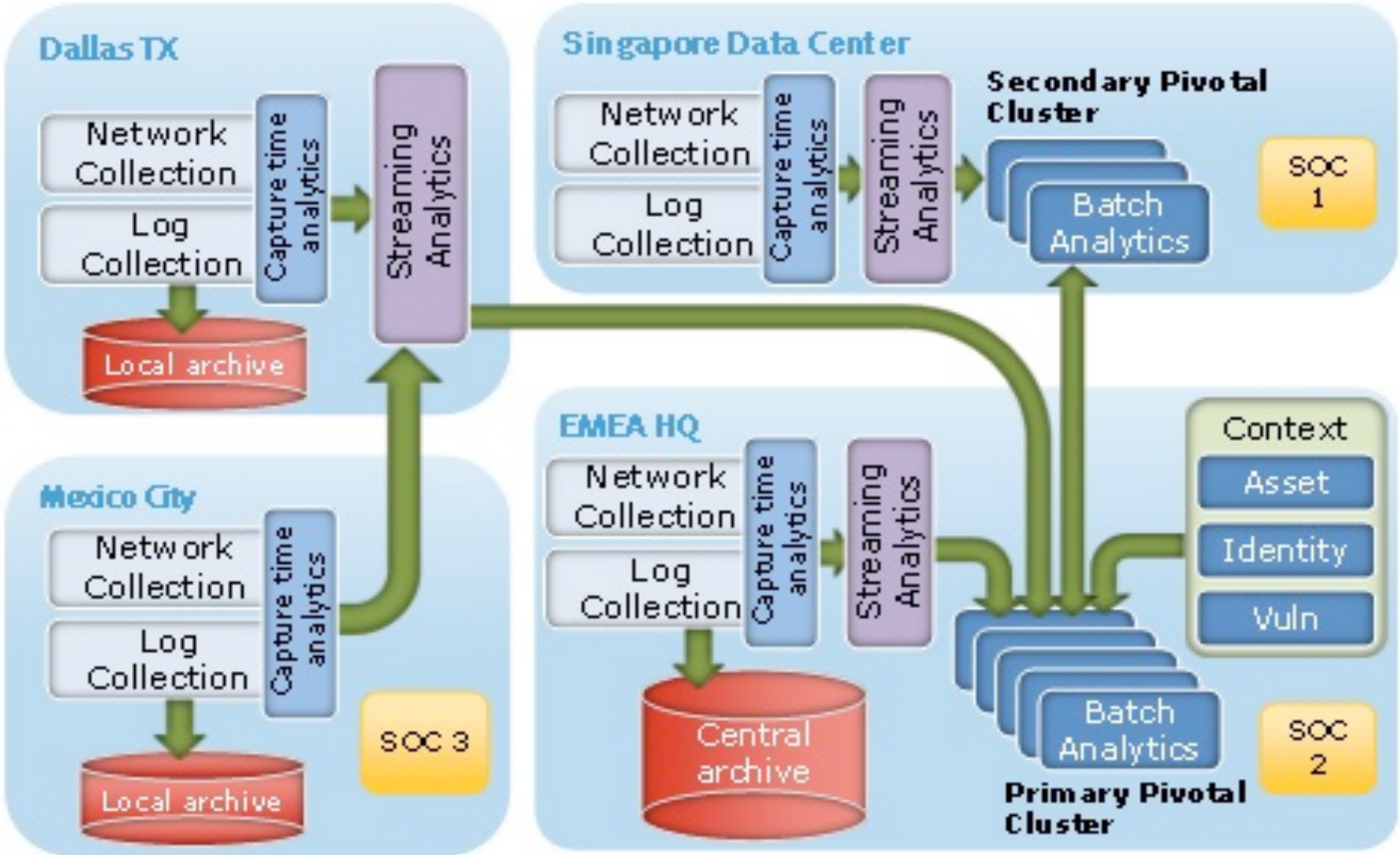
Big Data Processing

- Long-term, multi-PB storage
- Unstructured and structured
- Distributed Hadoop infrastructure
- Preservation of raw data
- Enterprise Integration

Analytics and Forensics

- Advanced visuals and interaction
- Predictive & decision modeling
- Ad hoc queries
- Interactive visualizations
- Collaborative sharing tools
- Pluggable, intuitive UI

©2014 bruno.kerouanton.net



©2014 bruno.kerouanton.net

En résumé

- Militarisation des cyber-conflits
- Sophistication croissante des attaques
- Mutation des enjeux IT

L'informatique de grand-papa, c'est ter-mi-né !

Cloud
Big-Data
IoT

➔ ***Big Data & Analyse Prédictive***

« Who owns the Internet ? » Jaron Lanier

« @War: The rise of Cyber-Warfare » Shane Harris

©2014 bruno.kerouanton.net

Merci

Restons en contact !

http:// éé.net / LinkedIn
http:// éé.net / twitter

Bruno KEROUANTON

© 2014 Bruno Kerouanton.net