CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Systèmes industriels (SCADA), pourquoi les RSSI ne s'emparent -ils pas de ce sujet critique ?

Assises de la Sécurité
Monte-Carlo (Principauté de Monaco), 6 octobre 2010

Pascal LOINTIER
Président du CLUSIF
CHARTIS Conseiller sécurité de l'information, CHARTIS

Situation sous contrôle ! (de supervision ;-))...

Country	Number of users
india	86258
indonesia	34138
iran, islamic republic of	14171
russian federation	7904
kazakhstan	6316
afghanistan	3081
syrian arab republic	2926
uzbekistan	2798
pakistan	2758
azerbaijan	2566
bangladesh	2489
malaysia	1691
iraq	1593
nepal	1453
belarus	1238
united arab emirates	1206
kyrgyzstan	1097
united states	805
turkmenistan	796
tajikistan	780

source : Aleks, Kaspersky Lab Expert

Publié le 03/10/2010 à 16:09 - Modifié le 03/10/2010 à 16:21 | Le Point.fr

VIRUS

L'Iran assure avoir nettoyé ses ordinateurs industriels de Stuxnet

Source AFP

Les ordinateurs industriels iraniens infectés par le virus Stuxnet ont été nettoyés, a déclaré un responsable iranien,

... Aucune revendication n'a, pour le moment, été formulée. Par ailleurs, le ver a touché d'autres ordinateurs en Chine, en Inde, au Pakistan ou encore en Indonésie. Les experts s'accordent pour considérer que les installations nucléaires iraniennes étaient les cibles prioritaires du ver, notamment celles de Natanz...
(Le Point 20101001)

Plusieurs millions d'ordinateurs infectés par Stuxnet en Chine

LEMONDE.FR avec AFP | 30.09.10 | 14h29

October 2, 2010

Iran Says It Arrested Computer Worm Suspects

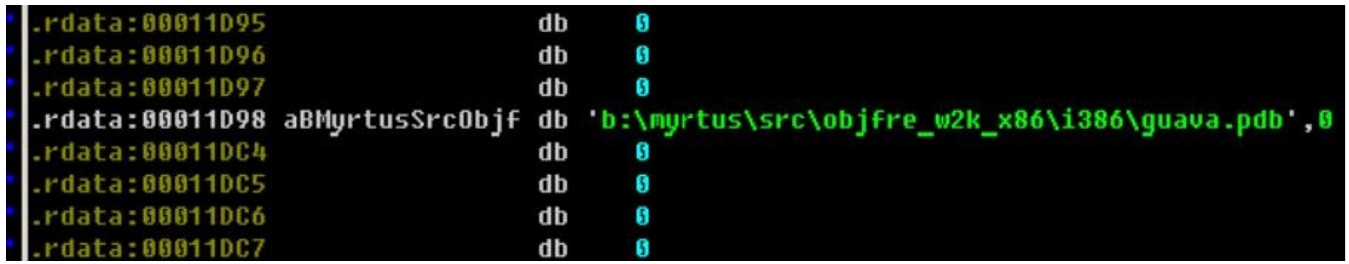
By WILLIAM YONG

TEHRAN — Iran has arrested an unspecified number of "nuclear spies" in connection with a damaging worm that has infected computers in its nuclear program, the intelligence minister, Heydar Moslehi, said Saturday.

Une certitude :
virus multiplateformes visant spécifiquement un environnement de production industrielle.
Pour le reste (auteur(s), mobile, cible(s)), à suivre...

Pour les adeptes de *Conspiracy Theory* ou de…

« …As Iran's nuclear assets would probably be isolated from outside computers, hackers would be unable to access them directly, Borg said. Israeli agents would have to conceal the malware software used by the Iranians or discreetly plant it on portable hardware brought in, unknowingly, by technicians. "A contaminated USB stick would be enough," Borg said… ». Scott Borg, director of the US Cyber Consequences Unit (YNetNews (IsraelNews), 20090707)



Deep inside the computer worm that some specialists suspect is aimed at slowing Iran's race for a nuclear weapon lies what could be a fleeting reference to the Book of Esther, the Old Testament tale in which the Jews pre-empt a Persian plot to destroy them.

That use of the word "Myrtus" — which can be read as an allusion to Esther — to name a file inside the code is one of several murky clues that have emerged… (New York Times, 20100929)

Toutes les théories, même les plus « originales » sont envisageables. 9/11 :

« …Al-Qaida could detonate a Chechen-type building-buster bomb at a federal building. Suicide bomber(s) belonging to al-Qaida's Martyrdom Battalion could crash-land an aircraft packed with high explosives (C-4 and semtex) into the Pentagon, the headquarters of the Central Intelligence Agency (CIA),… » (*Who Becomes a Terrorist and Why*, Library of Congress, 199909)

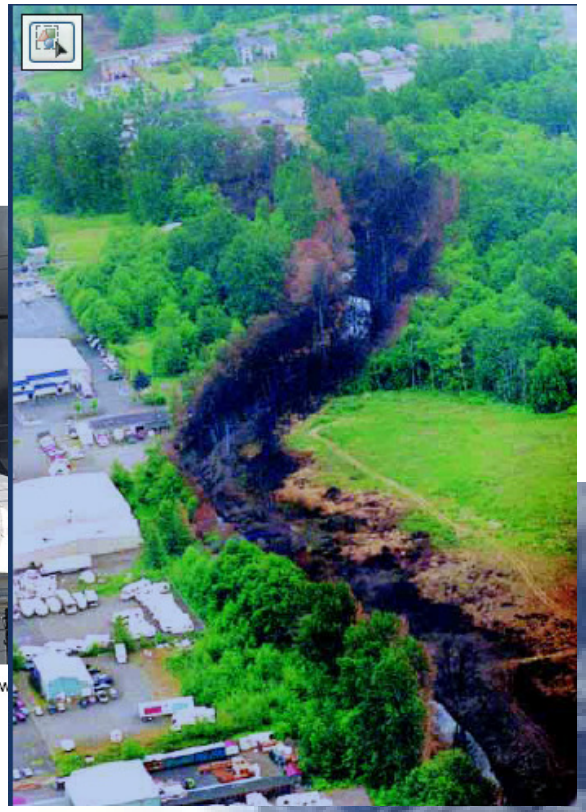
Et pourtant… accidents

Texas City Explosion 3/23/05

- Gauge-in-error assumed correct
- Accurate-gauge assumed wrong.
- 15 dead, 170 injured, economic losses in excess of $1.5 billion

(Chemical Safety Board)

Photo by Dwight C. Andrew



Bellingham (USA), 1999 : 3morts. 2007, le système informatique a été mis en cause également

Homeland Security

Jersey City (New Jersey, USA) 2009/07: erreur informatique du système de sécurité (mauvaise lecture de la pression)… inondations

Et pourtant… accidents (contamination non ciblée, paramétrage)

2003 : ver Slammer et site nucléaire (Ohio)

2003 : ver Nachi et réseau DAB (billeterie) Diebold *(et Panorama 2009 pour le réseau DAB Europe de l'Est… ciblé)*

2003 : virus SoBig et signalisation ferroviaire (Floride)

2005 : ver Zotob, arrêt de 13 usines d'assemblage de véhicules (E-U)

2007 : erreur de commande et contamination accidentelle (hydroxide de sodium pour le Ph) des eaux de ville, dizaines de victimes, blessures légères (Michigan)

Et pourtant… sabotage en interne (via le S.I.)

2007 : bombe logique d'un employé sur un système de contrôle d'irrigation des eaux de barrage (Californie)

2007 : prise de contrôle et perturbation des feux de signalisation (Californie)

2007 (et 2000 en Australie) : sabotage logique par un administrateur réseau du système d'approvisionnement en eau (Californie)

2007 destruction expérimentale d'un générateur électrique (Idaho pour CNN)

2008 : prise de contrôle et déraillement de 4 wagons, plusieurs blessés (Pologne)

« Exercice » de destruction d'une turbine à partir d'une faille de sécurité, depuis corrigée

Partage d'information… variable

Aggravation du risque (terme d'assurance) : préjudices économiques importants (Pertes d'Exploitation), dommages matériels et/ou corporels

Information Offreurs orientée sûreté de fonctionnement (fiabilité, maintenabilité, disponibilité) sur des environnements autrefois hétérogènes mais avec une tendance à la standardisation

- ☞Systèmes d'exploitation (Linux, Windows)
- ☞TCP/IP
- ☞Hypervision
- ☞Télémaintenance, M2M…

Littérature et colloques (sécurité, hacking) essentiellement anglo-saxons, volumétrie croissante depuis 2007

Création d'un Groupe de Travail CLUSIF ? ☺

Eléments d'organisation

Légitimité du RSSI

Historiquement, management de la sécurité logique : Connaissance des procédures et types de solution à mettre en œuvre

Répartition des taches

- La responsabilité fonctionnelle (administration) reste aux métiers (« prod », « process »)
- La responsabilité technique est, *a minima*, partagée avec le département SSI
  - A l'instar de la téléphonie (quoique souvent basculée vers la DSI)
  - ou du contrôle d'accès (*badging*)
  - ou des MFP (imprimantes multifonctions) gérées par les Services Généraux

Eléments d'organisation

Compétence du RSSI

Historiquement, management de la sécurité logique :
Définition des cahiers des charges

- Veille technologique et validation des specs produits
- Spécificité d'infrastructure (ouverture et interconnexion)

Analyse de risques, réaction sur incidents/scénarios

Webographie indicative

SCADA

http://www.clusif.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE (in Panorama 2007)
http://www.clusif.fr/fr/infos/event/archive2008.asp (in conférence du 17 avril)
http://www.fic2010.fr/pdf/2010/A4_informatique_industrielle.pdf

Services Généraux sur IP

http://www.fic2010.fr/pdf/2010/Les_actes.pdf
http://www.01net.com/fichiersAttaches/CLUSIF.pdf

Stuxnet (en cours…), « complots »

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
http://www.f-secure.com/weblog/archives/00002040.html
http://www.h-online.com/security/news/item/Stuxnet-brings-more-new-tricks-to-cyberwar-1098810.html?view=print
http://www.economist.com/node/17147818
http://www.nytimes.com/2010/10/03/world/middleeast/03iran.html?pagewanted=print
http://tammybruce.com/2010/09/allusion-to-bibles-esther-found-in-stuxnet-computer-worm.html
http://www.loc.gov/rr/frd/pdf-files/Soc_Psych_of_Terrorism.pdf