



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

Introduction sur les risques avec l'informatique « industrielle »



Sécurité du Cloud & Attaques Scada :

Paris, 23 novembre 2010

Hervé Schauer

<Herve.Schauer@hsc.fr>

- Introduction
- Services concernés
- Vulnérabilités
 - IP
 - Infrastructure
 - Serveurs
 - IT
- Solutions
- Conclusion
- Ressources

- Migration vers le tout IP
 - Téléphonie classique → Téléphonie sur IP
 - Machines industrielles → IP
 - Avions, trains, voitures → IP
 - Services généraux → IP
 - Migration complète ou partielle
 - Transport & équipements terminaux
 - Supervision, commande, télémaintenance
- Parfois difficile de sensibiliser les responsables concernés
 - Merci conficker & stuxnet

- Sécurité physique
 - Portes, badgeuses, caméras, détecteurs de présence, détecteurs incendie, détecteurs de fumée, hydromètres, thermomètres, etc
- Services généraux
 - Ventilation, climatisation, chauffage, éléments de confort (volets), etc
 - Energie : onduleurs, groupes électrogènes, etc
 - Ascenseurs
- Pilotage de systèmes industriels
 - Souvent regroupé sous le terme SCADA (*Supervisory Control And Data Acquisition*) : machines-outils, appareils biomédicaux, etc
- Services grand public
 - Surveillance du domicile, objets intelligents, véhicules (voitures, camions, avions, etc)

- Changement radical de l'exposition aux risques :
 - Tout interconnecté, tout sur internet
 - Changements d'échelle des accès aux éléments sensibles
 - Exemple : centrale d'alarme connectée en IP accessible depuis une filiale étrangère
 - Technologie plus facile à acquérir par les attaquants
 - Alors que les systèmes sont plus complexes
- Risque physique et risque sur la vie des individus à partir d'un risque informatique
 - Intrusion physique par le système de contrôle d'accès
 - Déni de service sur les alarmes ou les détecteurs incendie, ...
 - Atteinte à la vie privée, chantage, ...
 - Appareils médicaux dont dépend la vie du patient
 - Véhicules

- Légèreté des appareils
 - Peu de mémoire, peu de CPU
 - Systèmes d'exploitation moins évolués et peu éprouvés
 - ⇒ Risque élevé d'intrusion ou de déni de service via le réseau (inondation, etc)
- Protocoles de communication « portés » et peu résistants
 - Déni de service, boucles, redémarrage, ...
 - Usurpations, interceptions, rejeu, ...
- Exemples :
 - Defcon 17 : Déni de service sur la vraie caméra, puis injection de flux vidéo (« Ocean's Eleven Attack »)
 - HSC 2009 : plantage capteur à distance à travers la box, puis génération de fausses alarmes ...

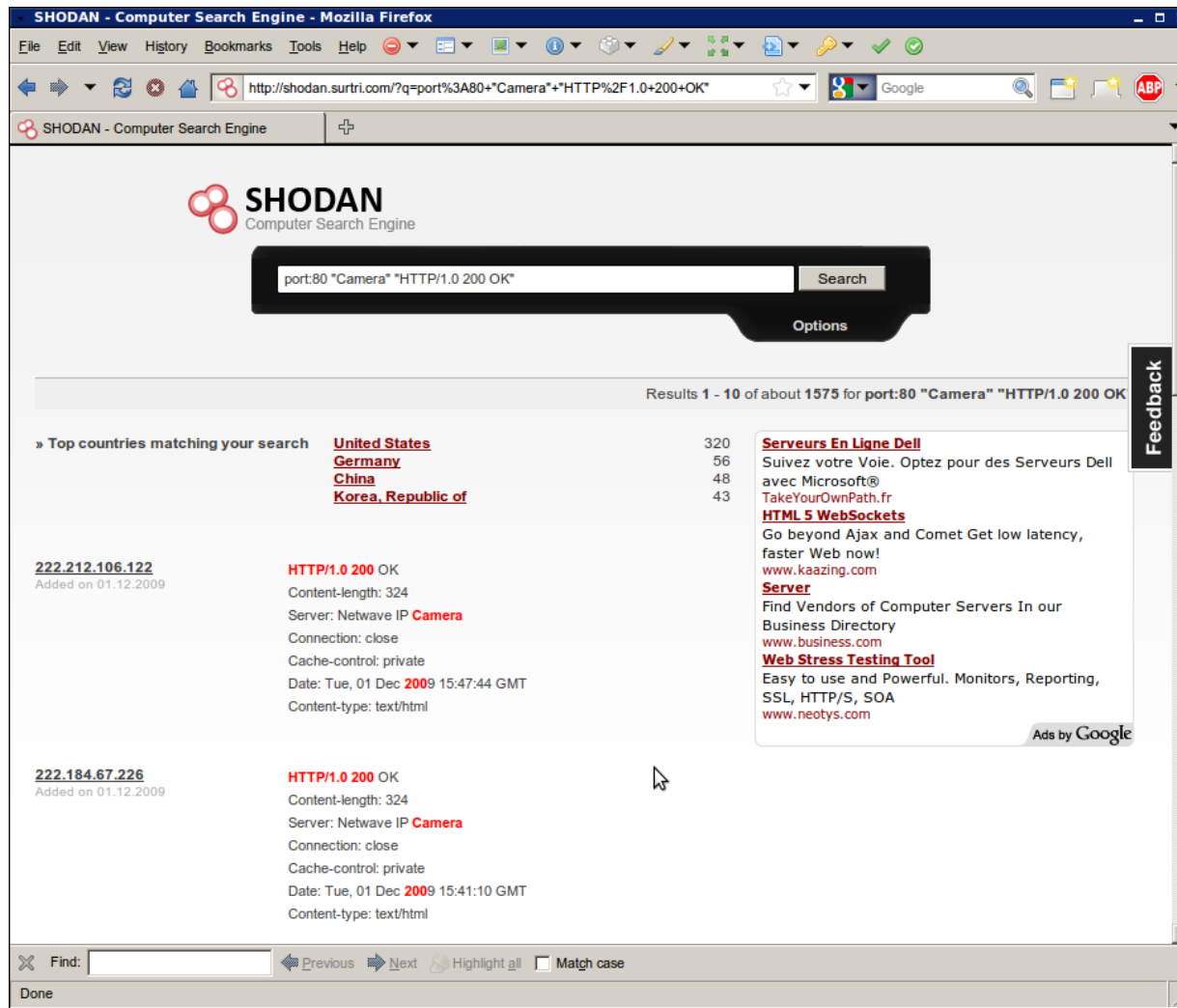
- Coupure ou perturbations du réseau Ethernet
- Brouillage Wifi & réseaux sans fil
- Coupure du *Power On Ethernet* ou de l'alimentation
- Perte de l'infrastructure IP
 - DHCP, DNS, routage, commutateurs, routeurs, etc
- Attaques par épuisement de ressources
 - Batteries
- Télémaintenance et rebonds IP
 - Exemple : équipement connecté au GPRS pour la supervision externe **et** au réseau de l'entreprise

- Serveurs (PC) livrés par un intégrateur qui échappent aux équipes IT : « Vous touchez à rien sinon ça ne marche plus ! »
- La sécurité est « abandonnée » :
 - Pas de suivi des correctifs Windows, Oracle, etc
 - Mots de passe (système, bases de données)
 - Jamais changés, partagés
 - Nombreuses vulnérabilités des interfaces d'administration
 - Programmation par des stagiaires sur un coin de table
 - Directement en production
 - Oubli de mise en oeuvre des sauvegardes
 - Accès distants intégrateur ...

- PC : coût négligeable par rapport à l'appareil géré
 - Serveur parfois offert par le fournisseur de l'appareil
- Oubli du contrôle des ports USB
 - Conficker est généralement arrivé sur les SI industriels par clé USB
- Prise de contrôle à distance par l'assistance aux utilisateurs (*helpdesk*) du serveur
- Remplacement des serveurs dédiés par des machines virtuelles dans les nuages (*cloud*)
- SAP connecté directement sur les serveurs des appareils industriels
 - Et au réseau informatique, à Internet et à Walldorf

- Gestion des pointeuses avec SQL Server sans mot de passe
- Serveur de gestion des écoutes d'un centre d'appel ...
- Automates bancaires (en Afrique) ...
-

Exemple : caméras sur internet



SHODAN - Computer Search Engine - Mozilla Firefox

http://shodan.surtri.com/?q=port%3A80+*Camera*+*HTTP%2F1.0+200+OK*

SHODAN - Computer Search Engine

SHODAN
Computer Search Engine

port:80 *Camera* *HTTP/1.0 200 OK* Search

Options

Results 1 - 10 of about 1575 for port:80 "Camera" "HTTP/1.0 200 OK"

» Top countries matching your search

United States	320
Germany	56
China	48
Korea, Republic of	43

[222.212.106.122](#)
Added on 01.12.2009

HTTP/1.0 200 OK
Content-length: 324
Server: Netwave IP **Camera**
Connection: close
Cache-control: private
Date: Tue, 01 Dec 2009 15:47:44 GMT
Content-type: text/html

[222.184.67.226](#)
Added on 01.12.2009

HTTP/1.0 200 OK
Content-length: 324
Server: Netwave IP **Camera**
Connection: close
Cache-control: private
Date: Tue, 01 Dec 2009 15:41:10 GMT
Content-type: text/html

[Serveurs En Ligne Dell](#)
Suivez votre Voie. Optez pour des Serveurs Dell avec Microsoft®
[TakeYourOwnPath.fr](#)
HTML 5 WebSockets
Go beyond Ajax and Comet Get low latency, faster Web now!
[www.kaazing.com](#)
Server
Find Vendors of Computer Servers In our Business Directory
[www.business.com](#)
Web Stress Testing Tool
Easy to use and Powerful. Monitors, Reporting, SSL, HTTP/S, SOA
[www.neotys.com](#)

Ads by Google

Feedback

Find: Previous Next Highlight all Match case

Done

Exemple : Siemens Simatic

SHODAN - Computer Search Engine - Iceweasel

File Edit View History Bookmarks Tools Help

http://www.shodanhq.com/?q=port:161+simatic


Getting Started

SHODAN port:161 simatic Register Search login


Results 1 - 10 of about 35 for port:161 simatic

» Top countries matching your search


United States	25
Netherlands	2
Germany	2
Greece	1
Czech Republic	1

216.14.191.234
 Added on 04.07.2010



Siemens, **SIMATIC** HMI, XP277, 6AV6 643-0CD01-1AX0, HW: 0, SW: V 1 1 1

195.251.116.146
 Added on 04.07.2010


Siemens, **SIMATIC** HMI, TP177B, 6AV6 642-0BD01-3AX0, HW: 0, SW: V 1 0 0

148.223.53.200
 Added on 02.07.2010


Siemens, **SIMATIC** S7, CPU315-2 PN/DP, 6ES7 315-2EH13-0AB0 , HW: 4, FW: V2.6.7, S C-X8U12589200

134.221.203.72
 Added on 02.07.2010


Transferring data from ajax.googleapis.com...



Exemple : RTU sur internet

WebRTU z1 - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://88.159.81.60/

Loading...

Reports	Date	Time	Code	Status	Electricity (kWh)	Cold Water (l)	Gas (l)
Today							
Yesterday	2010/01/11	16:00:00	00	0000	0000009592	0000125617	0000099280
This Week							
Previous Week	2010/01/11	15:45:00	00	0000	0000009592	0000125599	0000099280
This Month	2010/01/11	15:30:00	00	0000	0000009592	0000125599	0000099280
Previous Month							
All Values	2010/01/11	15:15:00	00	0000	0000009592	0000125599	0000099280
MRs... Indexes	2010/01/11	15:00:00	00	0000	0000009592	0000125599	0000099280
Status	2010/01/11	14:45:00	00	0000	0000009592	0000125599	0000099280
Configuration							
Network	2010/01/11	14:30:00	00	0000	0000009592	0000125590	0000099280
RTU Parameters							
Time Server	2010/01/11	14:15:00	00	0000	0000009592	0000125590	0000099280
Modem	2010/01/11	14:00:00	00	0000	0000009591	0000125590	0000099280
PPP							
Channel Functions	2010/01/11	13:45:00	00	0000	0000009591	0000125590	0000099280
Channel Parameters	2010/01/11	13:30:00	00	0000	0000009591	0000125590	0000099280
Channel Name/Unit							
Meter Readings	2010/01/11	13:15:00	00	0000	0000009591	0000125590	0000099280
EIWeb	2010/01/11	13:00:00	00	0000	0000009591	0000125589	0000099280
M-Bus							
Event Log	2010/01/11	12:45:00	00	0000	0000009591	0000125588	0000099280
Param Log	2010/01/11	12:30:00	00	0000	0000009590	0000125526	0000099280
Advanced Options	2010/01/11	12:15:00	00	0000	0000009590	0000125475	0000099280
Product Documentation	2010/01/11	12:00:00	00	0000	0000009590	0000125475	0000099280
	2010/01/11	11:45:00	00	0000	0000009590	0000125466	0000099280
	2010/01/11	11:30:00	00	0000	0000009590	0000125466	0000099280

- Stuxnet
 - Déni de service sur un système de contrôle industriel, mais le vol de données aurait pu être possible
 - Attaque ciblée sur certains automates Siemens Simatic et sur un processus particulier
 - Utilisation de plusieurs 0-days Windows, pilote signé
 - Mot de passe par défaut Siemens pour l'accès à MS-SQL
 - Modification de la fréquence des moteurs des centrales
 - A priori sans le but de détruire les centrifugeuses de gaz qui produisent de l'uranium enrichi dans les centrales iraniennes
 - Vibrations ainsi provoquées pourraient détruire le rotor de la centrifugeuse

- Comprendre soit-même les technologies utilisées
 - Comprendre les flux de données
 - Comprendre les interfaces
- Se faire expliquer par les fournisseurs
 - Préférer ce qui est normé et ouvert
- Intégrer l'informatique industrielle et l'informatique des services généraux à la DSI
 - Tout en intégrant les éventuels spécialistes du domaine
 - Comme pour la ToIP
 - Appliquer les procédures d'une DSI :
 - Intégration, supervision, masters, sauvegardes, PCA, etc
 - En respectant les contraintes de l'équipement et de l'utilisateur

- Déployer la PSSI à ces équipements
 - Appliquer ses mesures de sécurité en matière de mots de passe, correctifs de sécurité, mise à jour d'anti-virus, bonnes pratiques, ...
 - Intégrer la SSI dans les contrats
 - Imposer des règles d'accès par des tiers
 - Former les informaticiens à l'informatique industrielle les spécialistes des appareils à l'informatique
 - Cloisonner par une segmentation réseau
 - Pas toujours possible : certains protocoles propriétaires utilisant tous les ports
 - Procéder à des audits de sécurité et des tests d'intrusions
 - Si possible avant la mise en production

- Achat d'informatique → implication de la DSI et du RSSI
 - Intégration d'exigences de maintenance et de sécurité
- Matériel connecté au réseau → engagement contractuel
 - Acceptation d'intégration à la DSI, de l'auditabilité, etc
- Cloisonnement au niveau réseau

Questions ?

Herve.Schauer@hsc.fr www.hsc.fr

- Présentation d'Alain Thivillon au panorama de la Cybercriminalité :
http://www.hsc.fr/ressources/presentations/panocrim_athivillon_toutip/
- Shodan (Computer Search Engine) : <http://shodan.surtri.com/>
- Hacking Hospital :
<http://pcworld.about.com/od/securit1/Security-Guard-Charged-With-Ha.htm>
- Defcon 17 : Video Hacking :
http://www.theregister.co.uk/2009/08/01/video_feed_hacking/ ,
<http://hackerpoetry.com/images/defcon-17/dc-17-presentations/defcon>
- RISKS Digest : <http://catless.ncl.ac.uk/Risks>