



# Panorama de la Cybercriminalité

Alain Thivillon – CTO

Hervé Schauer Consultants

<http://www.hsc.fr/>

Service généraux sur IP

# Migration IP

- Après la téléphonie , le reste des infrastructures générales migre sur les réseaux IP :
  - Migration complète (y compris le transport ou les équipements terminaux) ou partielle (supervision, commande, reporting, ...)
  - Surveillance et accès (portes, badgeuses, caméras, détecteurs présence, détecteurs incendie, humidité, ...)
  - Climatisation, chauffage, éléments de confort (volets)
  - Energie (onduleurs, électrogènes, ...)
  - Systèmes SCADA (pilotage, processus industriel, ...)

# Nouvelles offres/technologies

- Surveillance du domicile depuis Internet
  - Détection de fumée Orange : <http://mamaison.orange.fr/>
  - SFR HomeScope : <http://www.sfr.fr/vos-services/equipements/innovations/sfr-homescope/>
- Tous nouveaux services M2M : « Internet des objets »
- ZIGBEE
- IPv6, s'il arrive un jour ..
  - permettra d'adresser plus facilement les objets du bâtiment/domicile
  - Auto-configuration, intelligence du réseau, mobilité, ...

# Quels risques ?

- Changement radical de l'exposition :
  - Technologie plus facile à acquérir par les attaquants
  - Changements d'échelle des accès aux éléments sensibles
    - Exemple une centrale d'alarme connectée en IP accessible depuis une filiale étrangère
  - Complexité et intégration des systèmes
- Le risque informatique peut devenir un risque physique
  - Intrusion par le système d'accès
  - Déni de service sur les alarmes, l'incendie, ...
  - Vie privée, Chantage, ...

# Vulnérabilités liées à IP

- Equipements très souvent légers (mémoire, CPU, ...), système d'exploitation moins évolués (RT) et peu éprouvés
  - ⇒ Risque élevé de déni service sur la couche IP (par flood, déni de service, ...)
- Protocoles de communication « portés » et peu résistants
  - Déni de service, boucles, redémarrage, ...
  - Spoofing, 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 ...

# Vulnérabilités physiques/infra

- Comment résister à :
  - Coupure ou perturbations du réseau Ethernet
  - Brouillage Wifi
  - Coupure du Power On Ethernet ou alimentation
  - Perte de l'infrastructure IP (DHCP, DNS, Routage, ...)
  - Attaques par épuisement de ressources (batteries, ...)
- Rebonds IP
  - Exemple équipement connecté au GPRS pour la supervision externe \_et\_ au réseau de l'entreprise

# Vulnérabilité des serveurs

- Très souvent, les serveurs sont livrés par un intégrateur et échappent aux équipes IT : « Vous touchez à rien sinon ça ne marche plus ! »
- La sécurité est « abandonnée » :
  - Suivi des correctifs Windows (risque sur les vers, ...)
  - Mots de passe (système, bases de données)
  - Vulnérabilité des interfaces d'administration
  - Backups !
- Accès distants intégrateur ...
- Exemples récents HSC :
  - Gestion des Pointeuses avec SQL Server sans mot de passe
  - Serveur de gestion des écoutes d'un centre d'appel

# Caméras sur Internet ...

The screenshot shows the SHODAN search engine interface in a Mozilla Firefox browser. The search query is "port:80 'Camera' 'HTTP/1.0 200 OK'". The results page displays the following information:

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

» Top countries matching your search

<a href="#">United States</a>	320
<a href="#">Germany</a>	56
<a href="#">China</a>	48
<a href="#">Korea, Republic of</a>	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

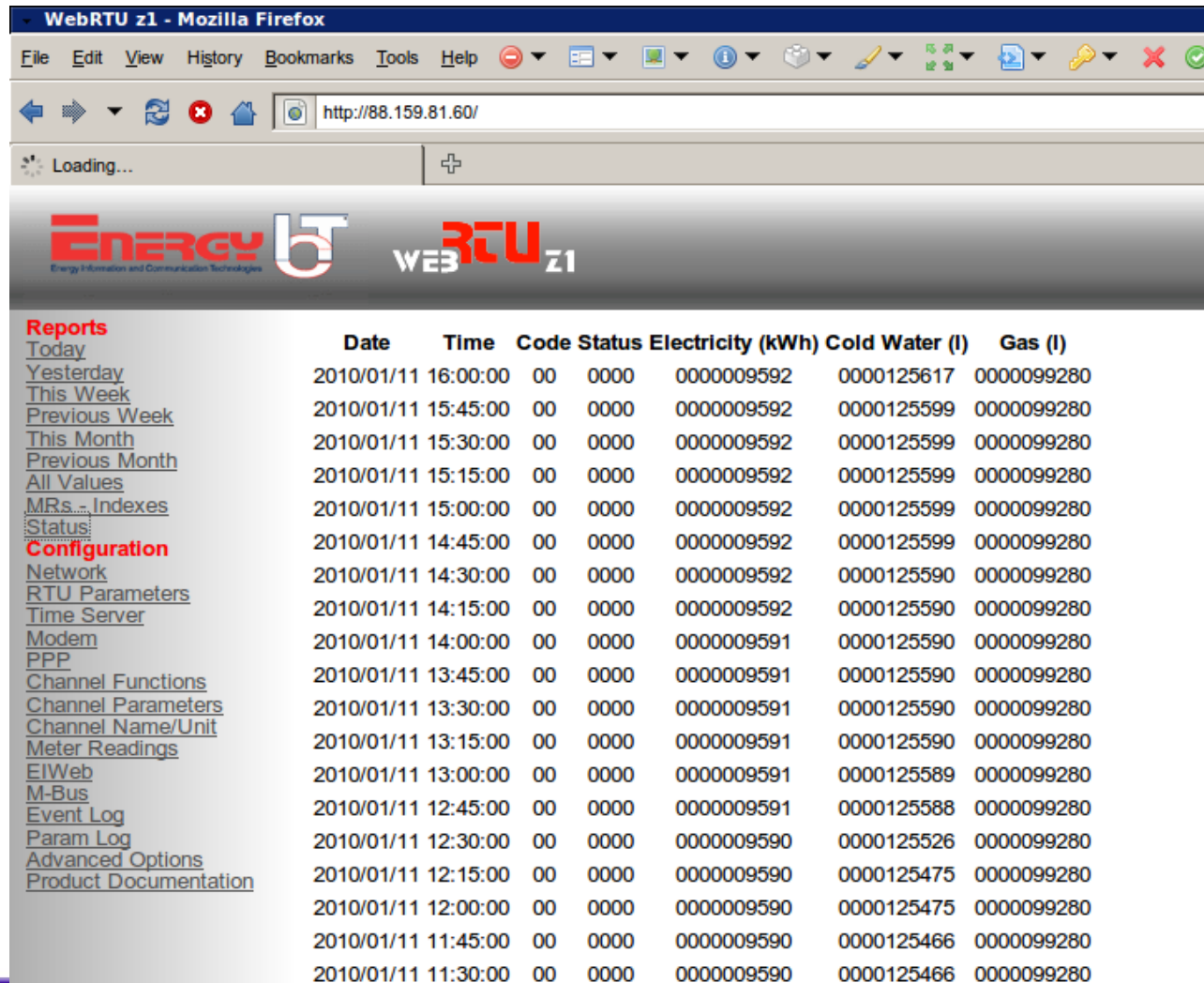
222.184.67.226  
Added on 01.12.2009

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

Ads by Google

Feedback

# RTU sur Internet ...



**WebRTU z1 - Mozilla Firefox**

File Edit View History Bookmarks Tools Help

http://88.159.81.60/

Loading...

**ENERGY BT** WEB RTU z1

**Reports**

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

## Que faire ?

- Reprendre la main ...
  - Se faire expliquer et comprendre les technologies utilisées, les flux de données, les interfaces, ...
  - Préférer ce qui est normé et ouvert
  - Envisager une segmentation réseau
  - Audits, Tests intrusifs
- Amener la PSSI à ces équipements
  - Mots de passe, Correctifs, Domaine, bonnes pratiques, ...
  - Intégration, Supervision, Masters, Sauvegardes, PCA
  - Contrats
  - Règles d'accès par des Tiers

# URLs

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://www.theregister.co.uk/2009/08/01/video_feed_hacking/) ,

[http://hackerpoetry.com/images/defcon-17/dc-17-presentations/defcon-17-ostrom-sambamoorthy-video\\_application\\_attacks.pdf](http://hackerpoetry.com/images/defcon-17/dc-17-presentations/defcon-17-ostrom-sambamoorthy-video_application_attacks.pdf)

RISKS Digest : <http://catless.ncl.ac.uk/Risks>