« Sécurité » des objets connectés

Exemple de vulnérabilité

« Sécurité » des objets connectés
Découverte

```
nmap -T4 -F 134.206.NNN.MMM
 Nmap scan report for xxxxx-clim.univ-lille1.fr
 […]
 PORT      STATE     SERVICE
 21/tcp    open      ftp
 23/tcp    open      telnet
 25/tcp    filtered  smtp
 80/tcp    open      http

telnet xxxxx-clim.univ-lille1.fr
 Trying 134.206.NNN.MMM...
 Connected to xxxxx-clim.univ-lille1.fr.
 Escape character is '^]'.
 Linux 2.4.21-rmk1 (pCOWeb) (ttya0)
```

« Sécurité » des objets connectés
Apprentissage

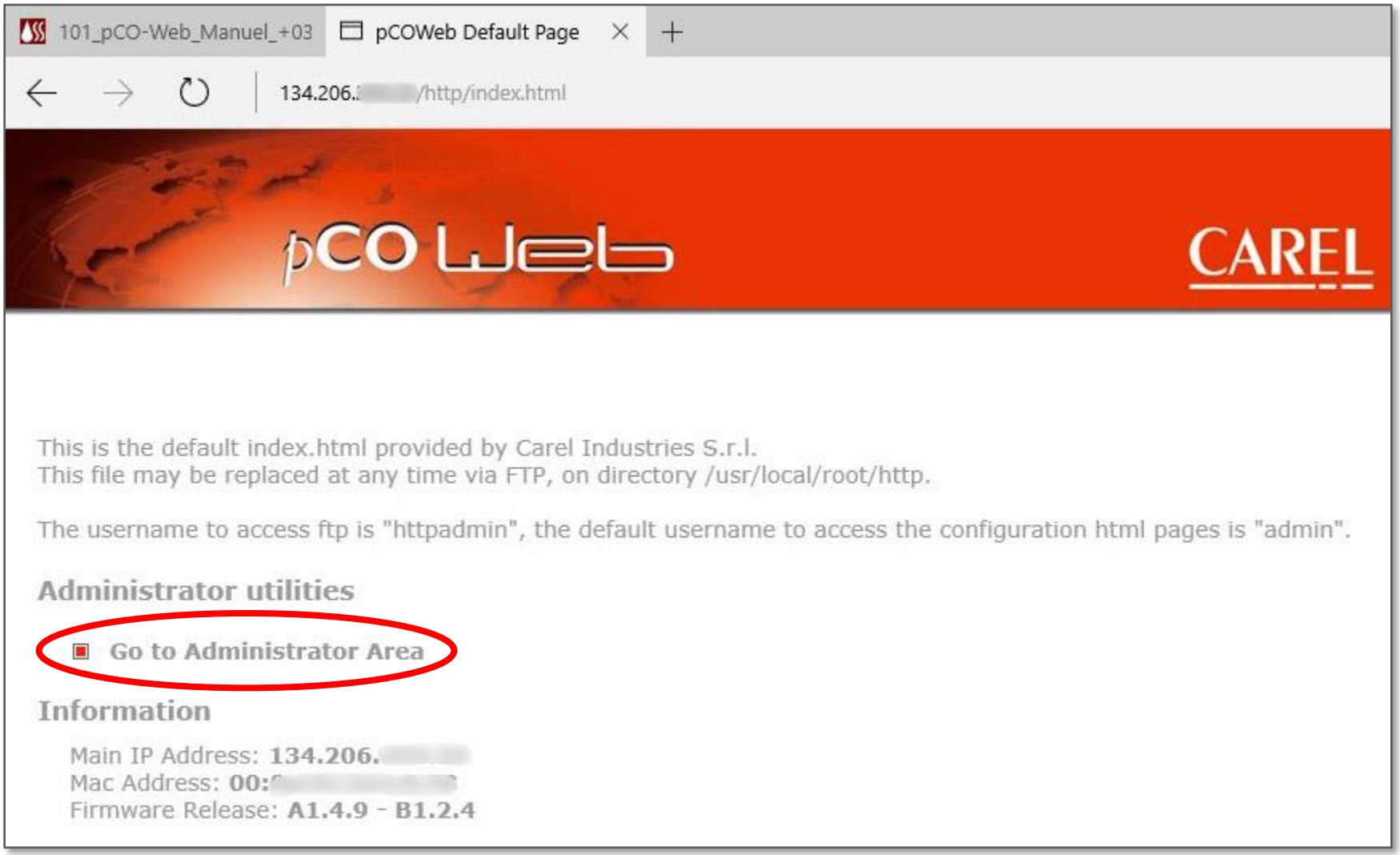
Google « pcoweb » :

- **pCOWeb est une carte série Ethernet pour système pCO CAREL. Complètement personnalisable, elle permet d'accéder à toutes les variables R/W de l'automate et de facilement modifier certains paramètres utilisateurs comme par exemple un point de consigne**

- **Mode admin, the default settings are:**
  Username : `admin`
  Password : `fadmin`

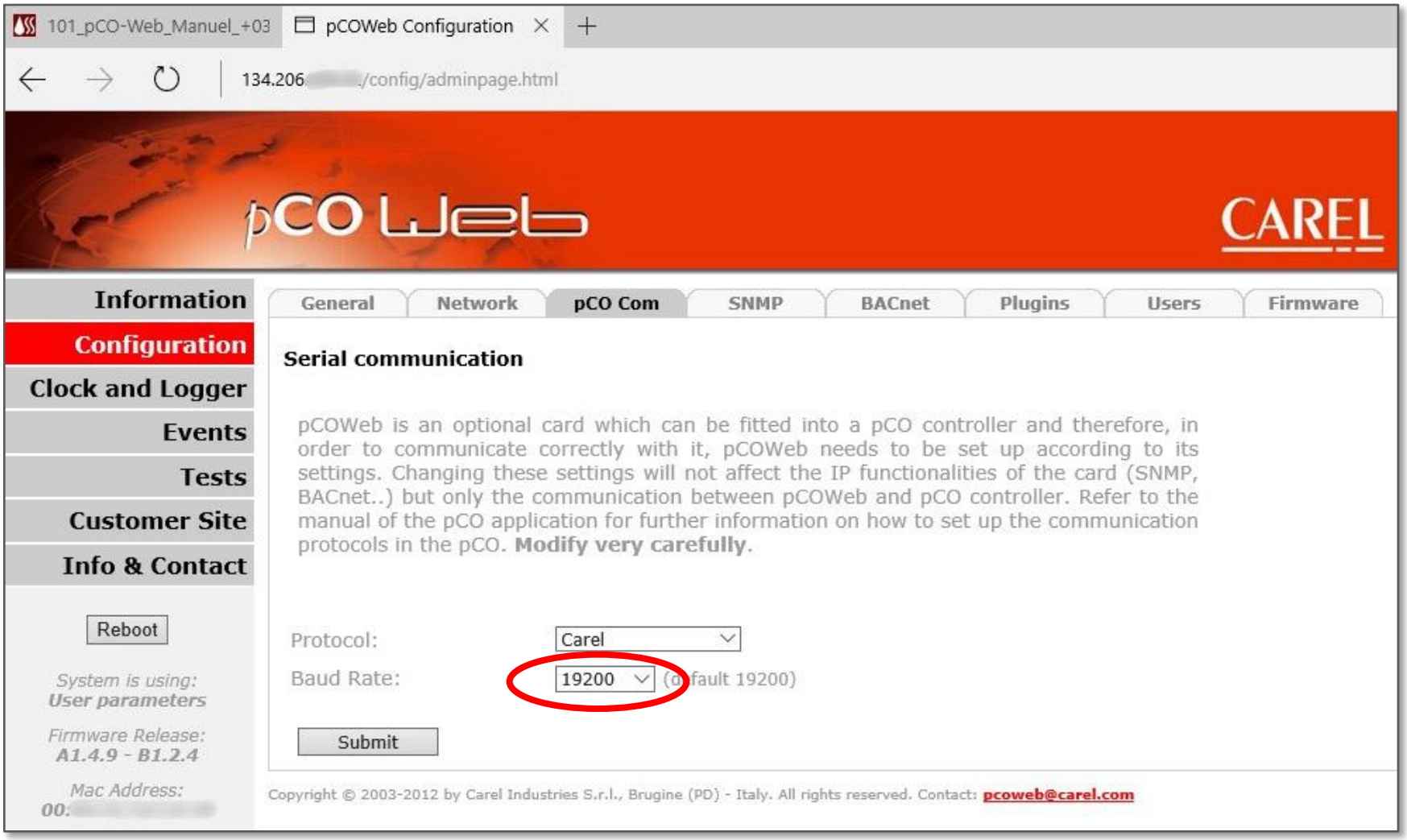
« Sécurité » des objets connectés

Exploration



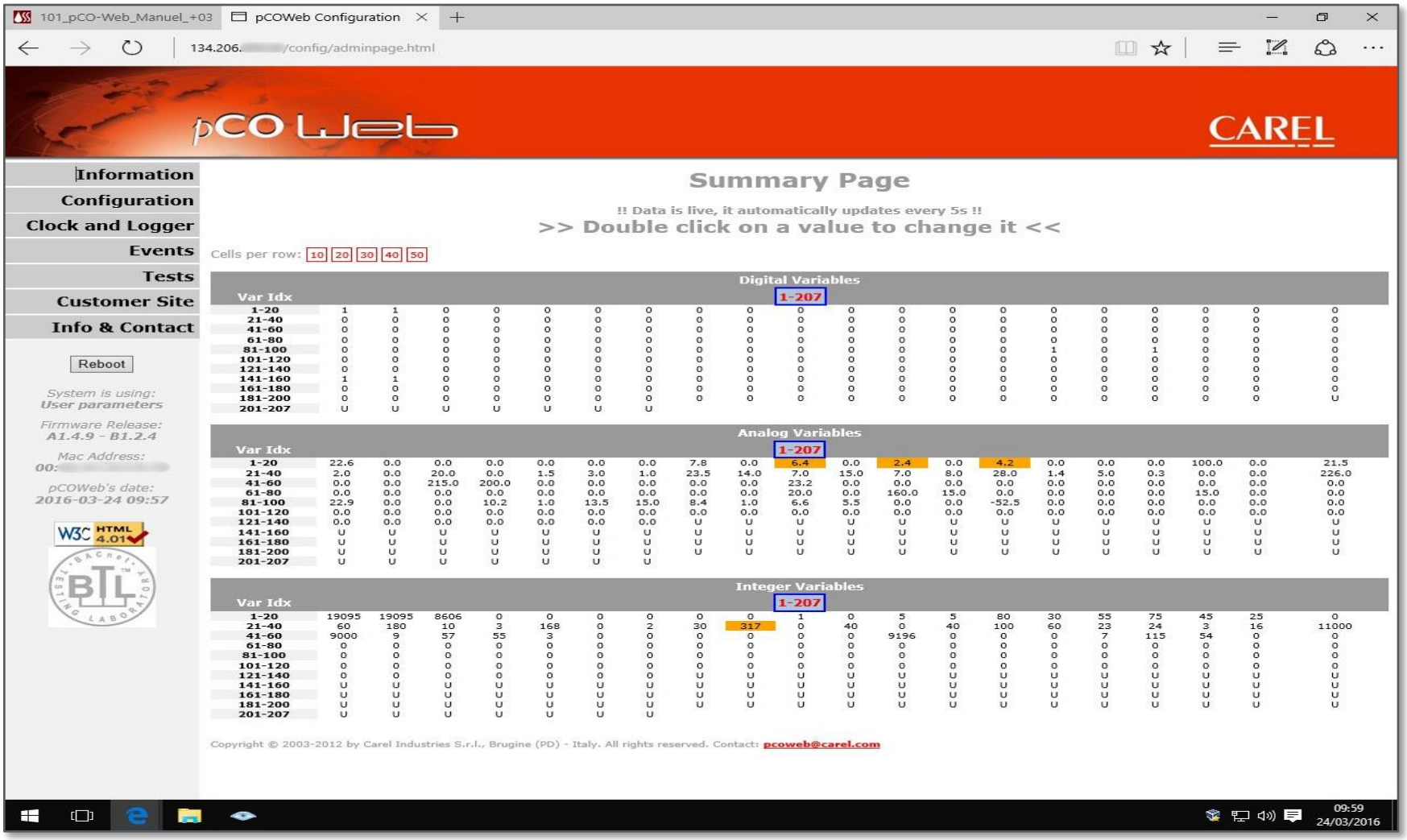
« Sécurité » des objets connectés

Exploration



« Sécurité » des objets connectés

Exploration



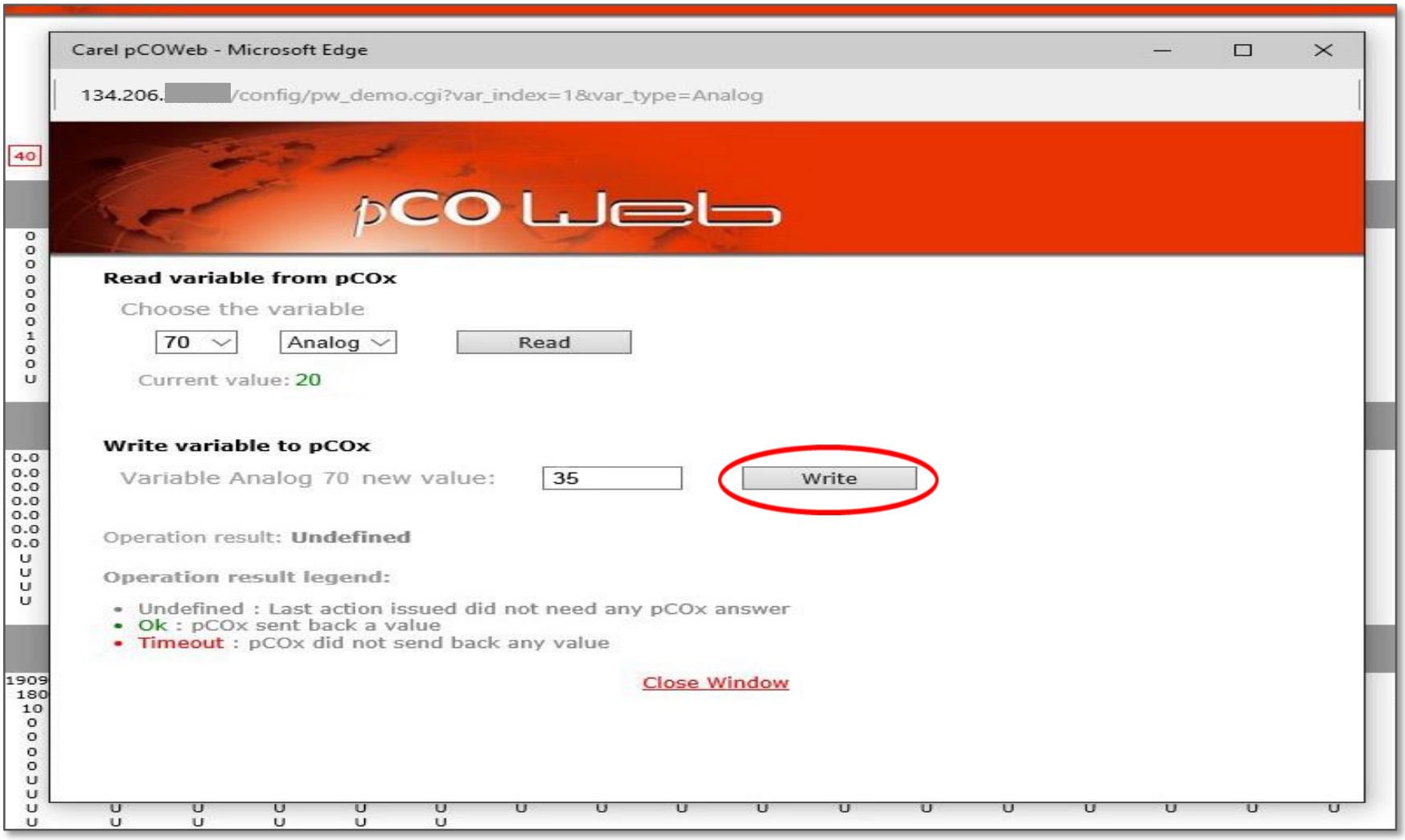
« Sécurité » des objets connectés

Exploration

Analog Variables						
			1-207			
0.0	7.8	0.0	6.4	0.0	2.4	0.0
1.0	23.5	14.0	7.0	15.0	7.0	8.0
0.0	0.0	0.0	23.2	0.0	0.0	0.0
0.0	0.0	0.0	20.0	0.0	160.0	15.0
15.0	8.4	1.0	6.6	5.5	0.0	0.0
0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.0	U	U	U	U	U	U
U	U	U	U	U	U	U
U	U	U	U	U	U	U
U	U	U	U	U	U	U
U						

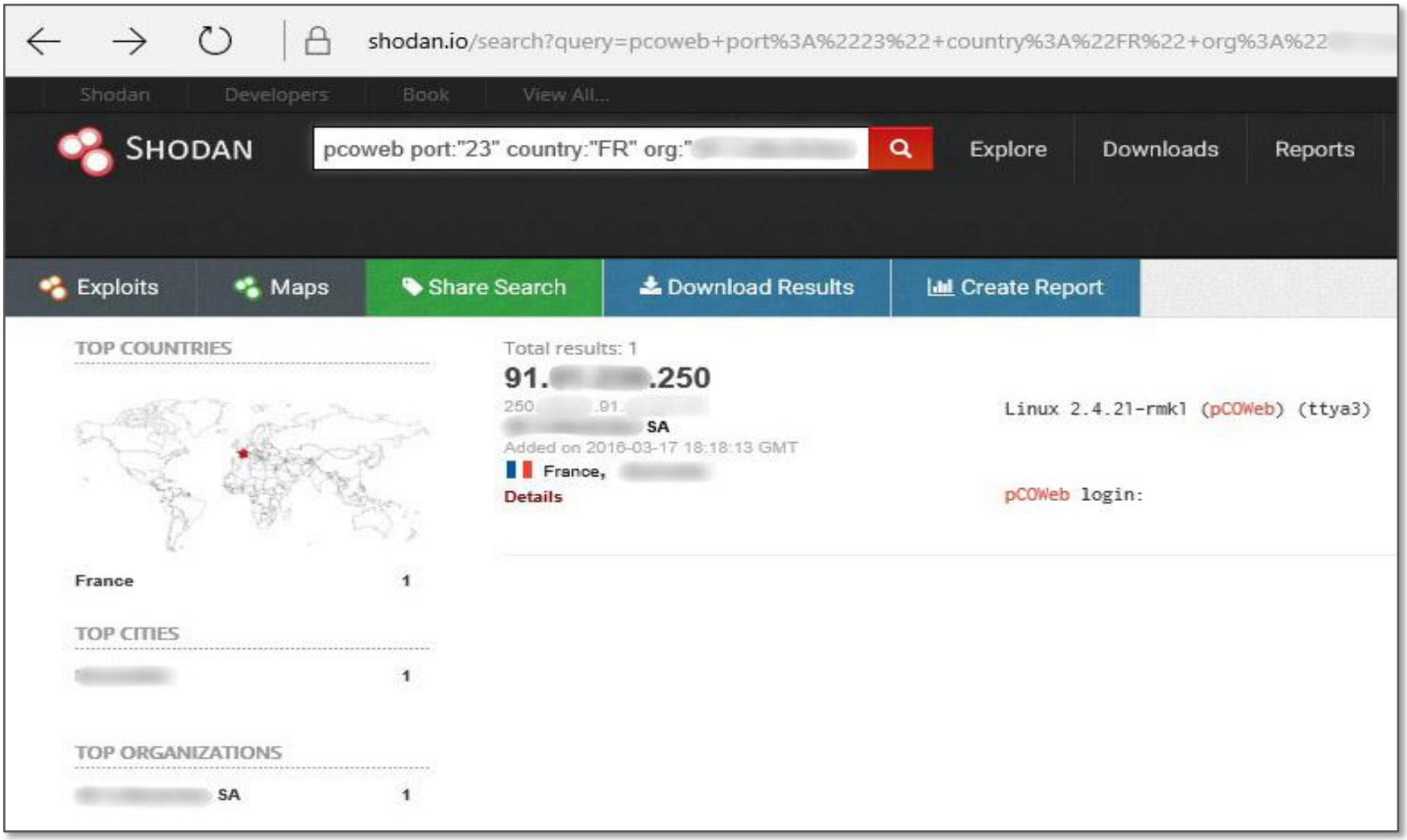
« Sécurité » des objets connectés

Piratage



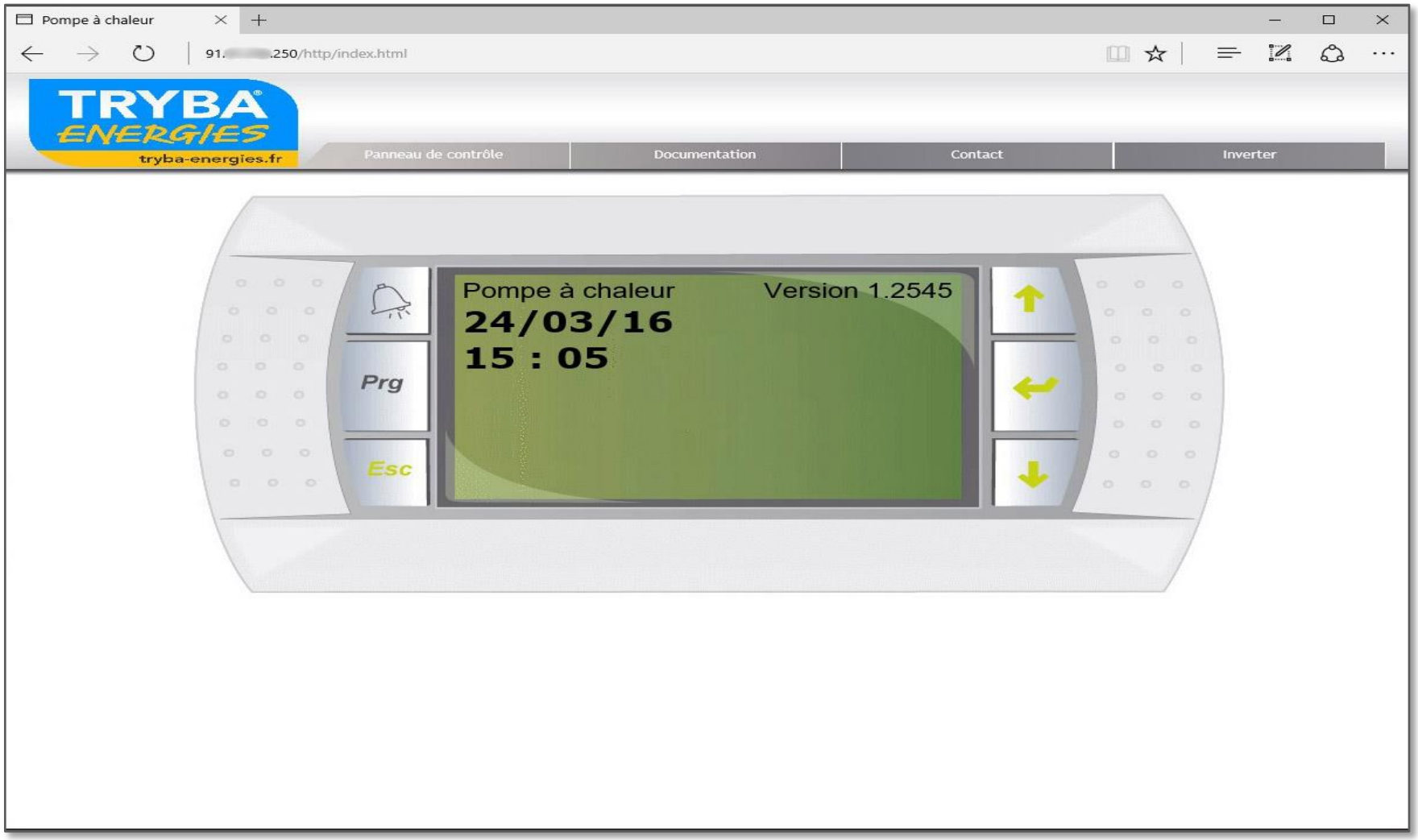
« Sécurité » des objets connectés

Nous ne sommes pas seul



« Sécurité » des objets connectés

Nous ne sommes pas seul



« Sécurité » des objets connectés
Conclusion

Protéger un objet connecté autant qu'un serveur :

- faire une recette de l'installation,
- réduire la visibilité (network IP séparé, filtres réseau, …),
- limiter les accès (adresses IP des clients),
- invalider tous les protocoles et fonctions inutiles,
- gérer les comptes de connexions (invalider les comptes inutiles, changer les mots de passe),
- Mettre à jour les composants logiciels (firmwares, sites WEB, …),
- …