

This website uses cookies to improve your experience. By using our services, you agree to our use of cookies.

[Accept](#)[Learn more](#)

Can't sleep, hackers will eat me!



Search

[About Me](#)[Disclaimer](#)[Tools](#)

# The Mobile Network Iceberg

November 5, 2015 08:28 | 9 Comments | Xavier



This is not a breaking news: The “*Internet of Things*” or connected objects is growing at the speed of the light. To convince the skeptics, just have a look at [shodan.io](#) to easily find plenty of devices that are (or should not be!) online.

A few days ago, I was discussing with a customer about an incident he faced: A corporate laptop was compromised via its 3G connectivity. Today, the IPv4 address space being full, mobile operators implement [CGN](#) (“Carrier Grade NAT”) for most of their mobile customers. Even if [NAT is not a firewall](#), it prevents incoming connections to reach the mobile device.

But, for some professional or high level services, public IP addresses can be assigned to mobile devices through their SIM card. This is particularly useful in M2M (“Machine to Machine”) communications where devices must be sometimes reachable! While discussing about the incident with my customer, I got the IP address assigned to the 3G dongle. The IP address being part of a /16 network, it was too tempting to see what could be reached from the Internet. I searched for interesting open port and took some screenshots of discovered websites.

The pictures below are just a short resume of the findings: industrial systems, routers, exotic devices, etc. So many devices are publicly available... just being a mobile network connection. I also found MySQL, Remote Desktop and many other juicy services!

Note: no device was harmed during the scan 😊

**Welcome to the main menu of Solar-Log<sup>1000</sup>**

The further functions can be chosen under the menu items above and on the left side.

Solar-Log Recording data.

**More information**

Inverters	13
Sensors	1
Plant size	239.2 kWp
Firmware	2.8.3 Build 53 - 08.07.2013
Serialnumber	1882062857

© 2011 Solare Datensysteme GmbH | [info@solar-log.com](mailto:info@solar-log.com)

Powered by



Follow Me



Upcoming Events

Here is a list of events that I will attend and cover via Twitter and wrap-ups. Ping me if you want to meet! The list is regularly updated.



Recent Posts

[The Truth is in Your Logs!](#)

[Physical Access == Pwn3d!](#)

[\[SANS ISC Diary\] Unity Makes Strength](#)

[Managing Palo Alto Firewalls Custom URL Categories](#)

[\[SANS ISC Diary\] Enforcing USB Storage Policy with PowerShell](#)

Popular Posts

[The Truth is in Your Logs!](#)

2,049 views

[Physical Access == Pwn3d!](#)

361 views

[Managing Palo Alto Firewalls Custom URL Categories](#)

206 views

Show me your SSID's, I'll Tell Who You Are!

**Windows CE Remote Management Tool**

**Remote Admin**

**Device Log On:**  
To access the device, type your password and then click **Log On**. Your base station password is case sensitive.

Password:   
Verification:

Apply Cancel

---

**TransPort WR21 (SN: 235834) Configuration and Management**

User authentication required. Login please.  
Username :   
Password :   
Please enter your login Username and Password  
Login

Copyright © Digi International, Inc. All rights reserved.

Connected

**Builtins**

- version** Console version
- lang** Set the console language
- reboot** Reboot

**Basics**

- 1wire** Display 1wire information
- iostate** Display input/output state
- modem** Display modem state
- gpspos** Retrieve last GPS position
- list** List available modules.  
[all] List all available modules parameters.  
[module] List available module parameters.  
[dl] Download result.
- g** Get module parameter value
- s** Set module parameter value
- listdb** List available DB parameters
- gdb** Get a DB parameter
- sdb** Set a DB parameter
- logdump** Display all logs
- configure** Upload a new conf file

**Advanced**

- ip** Display all ip addresses. If str, display only str address.
- stats** Display stats.
- skey** Update|Delete server key
- ukey** Update|Delete user key
- logs** Retrieve or Delete logs of software
- stopsoft** Stop the software
- usercpn** List user components
- update** Upload an update package
- sysupdate** Update the system
- restore** Restore parameters of write, db or pdm
- restorefull** Restore device to the initial configuration state
- version** Display software/hardware version

**Commands**

- cplist** List available commands
- chelp** Display command help
- cxelp** Find and display command help
- crun** Run the command
- cexe** Find and run the command (example : cexe .\* \_EnergyReferee.cmd ...)

- 179 views  
Sending Windows Event Logs to Logstash
- 126 views  
dns2tcp: How to bypass firewalls or captive portals?
- 125 views  
Forensics: Reconstructing Data from Pcap Files
- 87 views  
Vulnerability Scanner within Nmap
- 77 views  
Keep an Eye on SSH Forwarding!
- 75 views  
Email Tracking for Dummies

## Recent Tweets

- #CCC is alive! src\_ip="151.217.0.0/16" -> 245 hits in my logs since 26th Dec...  
11 hours ago
- Usually, we're looking for a password...  
Here, I found one and I'm looking to who it belongs ;-) 13 hours ago
- Any idea why all cmd's return "Rex::TimeoutError Operation timed out" in a valid #Meterpreter session!?  
#LazyTweet 16 hours ago
- xortool.py: a tool to guess the key length and key of a XOR'd file  
(kitploit.com/2013/02/xortoo...) 19 hours ago
- Anybody has access to a #Barracuda spam firewall? I've a question... (Please RT) 2 days ago

Follow Me on Twitter

## Time Machine

### Time Machine

Select Month ▾

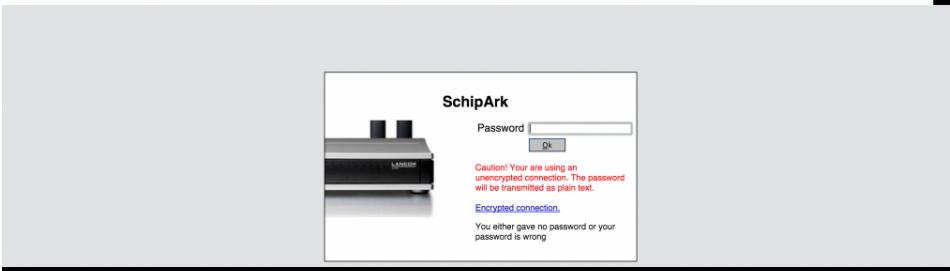
"SecurityFocus Vulnerabilities"

- Vuln: Google Chrome Prior to 47.0.2526.106 Multiple Remote Code Execution Vulnerabilities
- Vuln: libxml2 CVE-2015-7500 Denial of Service Vulnerability
- Vuln: Mozilla Firefox Multiple Security Vulnerabilities

LANCOM 1780EW-4G

LANCOM  
Systems

... CONNECTING YOUR BUSINESS



Vuln: Libxml2

'xmlParseConditionalSections()' Function Denial of Service Vulnerability

Bugtraq: [oCERT 2015-012] Ganeti multiple issues

Bugtraq: WebKitGTK+ Security Advisory WSA-2015-0002

Bugtraq: libtiff bmp file Heap Overflow (CVE-2015-8668)

Bugtraq: libtiff: invalid write (CVE-2015-7554)

More rss feeds from SecurityFocus

**Device Information**

- Device Serial Number: 5338517425
- Firmware Version: 3e15b1a9\_PROD-7.3.0
- Ignition Switch: On
- Master Disconnect: Closed
- R-Term: Inactive
- System Voltage: 23.6 V
- Service Meter Hours: Unavailable
- CAN Bus Recipe: default
- Back Office Link: CONNECTED

**GPS Status**

- Satellites Tracked: 0
- Estimated GPS Accuracy: 23 m

**Enabled Options**

- Telematics
- WiFi Access Point
- Cellular Parameter Modification
- Connected Machine

**RTK Rebroadcast Status**

- RTK Rebroadcast Status: On
- NTRIP Status: Connected

**Device Input Status**

- Switch 1: OFF (ground for ON)
- Switch 2: OFF (ground for ON)
- Switch 3: OFF (battery for ON)
- Analog: 0.1 V
- TPMS: Not Connected
- CAN A: 2 packets received
- CAN B: 0 packets received

**Cellular Status**

- Cell Modem Type: GSM
- Cell Band Mode: Automatic
- Signal Strength: -63 dBm
- Internet Access: On

**WiFi Status**

- Strength: -97 dBm
- Mode: Ad-Hoc
- SSID: Trimble Service (5338517425)

**Access Point Status**

- Access Point Status: Off

**SunnyWebBox**

Startpagina

SMA Afmelden

Vermogen:	0 W
Dagopbrengst:	331,5 kWh
Totale opbrengst:	509,26 MWh

Taal: Nederlands

Wachtwoord:

Aanmelden

User name:

Password:

Language: 简体中文

Stream: MainFlow

Player: Download

Auto Login

Login



NB1600 WEB MANAGER

Welcome to NB1600  
Please provide username and password to log in:

Username:

Password:

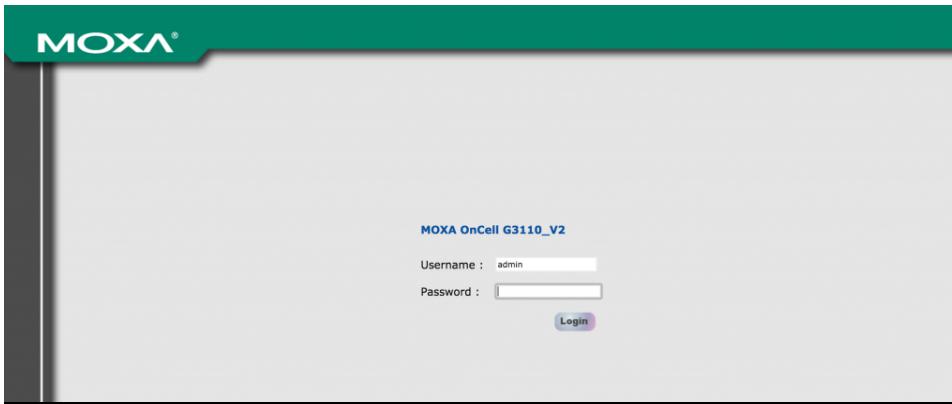
NB1600 NetModule Router  
Software Version 3.7.0.104  
© 2004-2015, Netmodule AG



**PSI-MODEM-GSM/ETH**

- 📁 Device information
- 📁 Local network
- 📁 Wireless network
- 📁 Network security
- 📁 VPN
- 📁 I/O
- 📁 System

<%@ Language=VBScript %>  
**Welcome to BECKHOFF CE device**



MOXA OnCell G3110\_V2

Username : admin

Password :

Login



**Login**

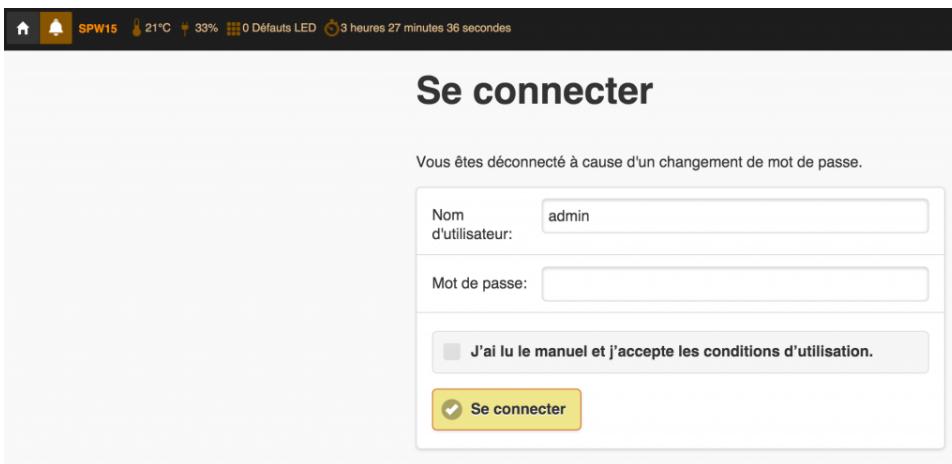
Account

Password

Language English

Login

**D-Link**



SPW15 21°C 33% 0 Défaux LED 3 heures 27 minutes 36 secondes

## Se connecter

Vous êtes déconnecté à cause d'un changement de mot de passe.

Nom d'utilisateur: admin

Mot de passe:

J'ai lu le manuel et j'accepte les conditions d'utilisation.

Se connecter



#### TransPort WR21 (SN: 402515) Configuration and Management

This screenshot shows the main configuration interface for the TransPort WR21. It is a three-panel layout:

- Login Panel:** Contains fields for 'Username' and 'Password', and a 'Log in' button.
- System Panel:** Displays system information including Model (TransPort WR21), Part Number (WR21-U92A-DB1-TA), Serial Number (402515), Uptime (95 days 11 hours 42 minutes 33 seconds), System Time (27 Oct 2015 20:15:26), CPU Utilization (1% Min: 1%, Max: 51%, Avg: 2%), Description (publ01), Contact, and Location.
- Interface Status Panel:** Shows the status of three interfaces: Ethernet 0 (green), Ethernet 1 (grey), and Cellular (green).

#### Connect WAN 3G Configuration and Management

This screenshot shows the login page for the Connect WAN 3G configuration interface. It includes a 'Login' header, a welcome message, and a login form with fields for 'Username' and 'Password' and a 'Login' button. A 'Help' link is located in the top right corner.

Welcome to the Configuration and Management interface of the Connect WAN 3G.  
Please specify the username and password to login to the web interface.  
See the User Guide and documentation for more information on logging in or retrieving a lost password.

Copyright © 1996-2011 Digi International Inc. All rights reserved.  
[www.digi.com](http://www.digi.com)

**NB1600 WEB MANAGER**

**net Module**

Welcome to NB1600  
Please provide username and password to log in:

Username:   
Password:

NB1600 NetModule Router  
Software Version 3.7.0.104  
© 2004-2015, NetModule AG

**Fronius Datalogger Web**

**Realtime total view**

**Fronius**

Realtime total view

en

Realtime total view

Realtime comparison view

Settings

11 °C

0 IG

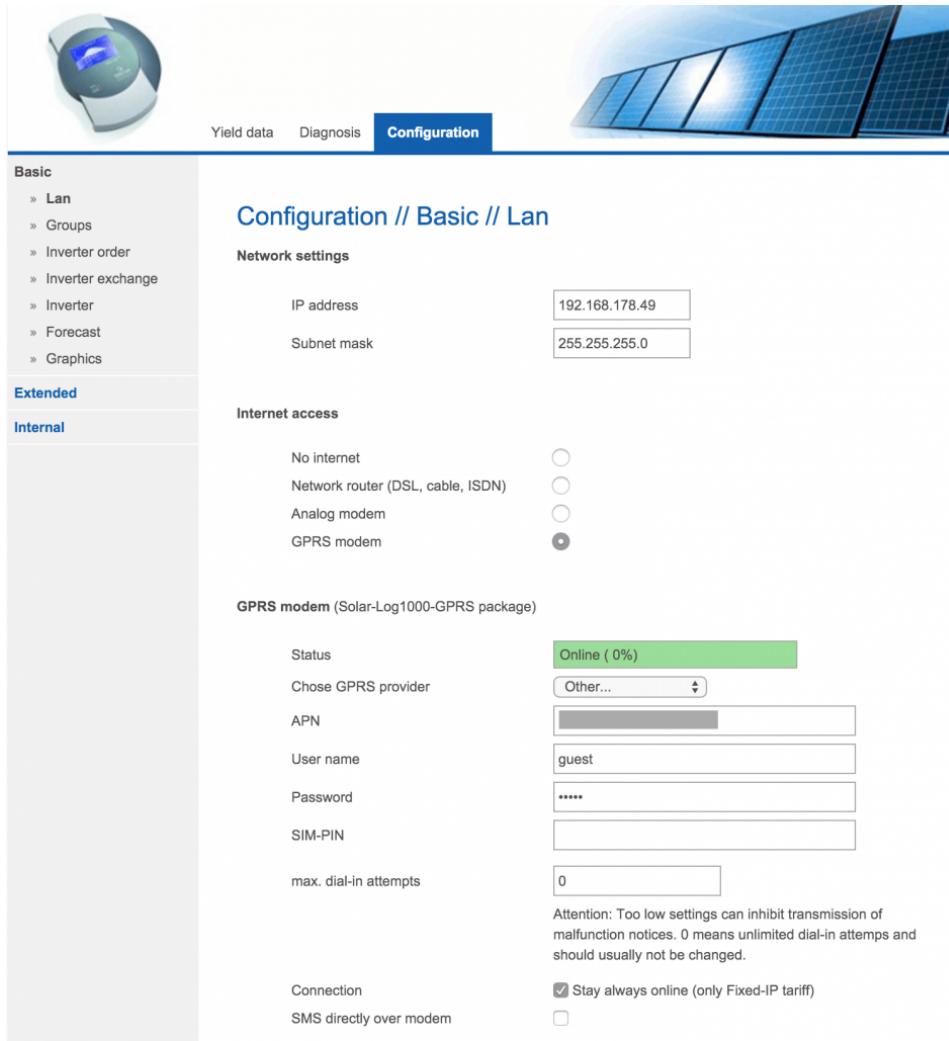
Digital 1

12 °C

0 km/h

CO<sub>2</sub> savings today  
CO<sub>2</sub> savings total  
Earnings Today  
Earnings Total

v2.0.1-1 / 1.4A      Update of version 2.0.1-1 to 2.0.5-4 available. :: Display changelog      Fronius International GmbH



**Configuration // Basic // Lan**

**Network settings**

IP address	192.168.178.49
Subnet mask	255.255.255.0

**Internet access**

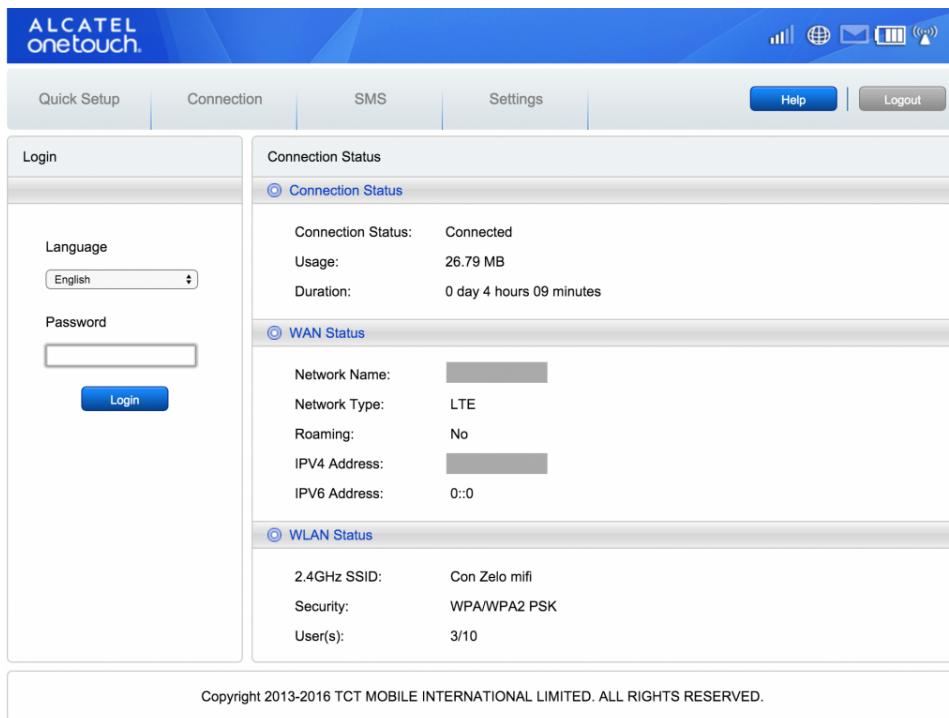
No internet   
 Network router (DSL, cable, ISDN)   
 Analog modem   
**GPRS modem**

**GPRS modem (Solar-Log1000-GPRS package)**

Status	Online ( 0% )
Chose GPRS provider	Other... <input type="button" value="▼"/>
APN	
User name	guest
Password	*****
SIM-PIN	
max. dial-in attempts	0

Attention: Too low settings can inhibit transmission of malfunction notices. 0 means unlimited dial-in attempts and should usually not be changed.

Connection  Stay always online (only Fixed-IP tariff)  
 SMS directly over modem

**Connection Status**

Connection Status: Connected  
 Usage: 26.79 MB  
 Duration: 0 day 4 hours 09 minutes

**WAN Status**

Network Name: [redacted]  
 Network Type: LTE  
 Roaming: No  
 IPV4 Address: [redacted]  
 IPV6 Address: 0::0

**WLAN Status**

2.4GHz SSID: Con Zelo mifi  
 Security: WPA/WPA2 PSK  
 User(s): 3/10

Copyright 2013-2016 TCT MOBILE INTERNATIONAL LIMITED. ALL RIGHTS RESERVED.

# GlobeSurfer III

OPTION

 Login

<b>Internet Connection</b>	
Operator:	Very good (-71 dBm)
Signal strength:	Connected
Connection status:	UMTS
Connection Type:	18:32:09 [hh:mm:ss]
Current connection time:	
Language:	EN English
User Name:	<input type="text"/>
Password (case sensitive):	<input type="password"/>
<input type="button" value="OK"/>	

[Like](#) [Share](#) [4](#) [Tweet](#)

• [Stui](#) [Pin It](#)

Posted in: [Uncategorized](#)

## Profile

[Sign in with Twitter](#) [Sign in with Facebook](#)

or

**Comment**

Name

Email

Not published

Website

[Post It](#)

- 9 Replies
- 0 Comments
- 9 Tweets
- 0 Facebook
- 0 Pingbacks

Last reply was 1 month ago



1.  @imifos

[View 1 month ago](#)

@xme Please do not scan the internet. You can go to jail for doing this!! Scanning is allowed only to criminals!!

[← Previous Post](#)

[Next Post →](#)