ISC 2016

2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体

employee

Greater China Threat Landscape

Sergey Gordeychik | **SCADA StrangeLove Research Team**

The case of the
BLUE SCREEN

```
problem has been detected and Windows has been shut down to prevent damage
to your computer.

[illegible]_USB_DRIVER

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: [illegible] ([illegible])


Collecting data for crash dump ...
Initializing disk for crash dump ...
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

INVESTIGATION RESULTS: BANK

- Domain Controller in ATM network is compromised
- «USB-sniffers» installed on ATMs via Admin$ shares
- Sniffers collects information about credit cards
- Cash withdrawal via 3rd party banks and services
- Can’t find any evidence of compromise in core IT-network or perimeter

INVESTIGATION RESULTS: TELCO

TTP analysis: tools was uploaded to VirusTotal from several networks

One of the networks: large Telecom

Threat Intelligence analysis: unprotected routers on Bank’s perimeter

Joint incident investigation

Source of the attack – MPLS trunk of the Telecom

TECHNIQUES, TACTICS AND PROCEDURES

You don't have to be a target to be a victim

Supply chain attack

Attacks against infrastructure

To support attacks against client

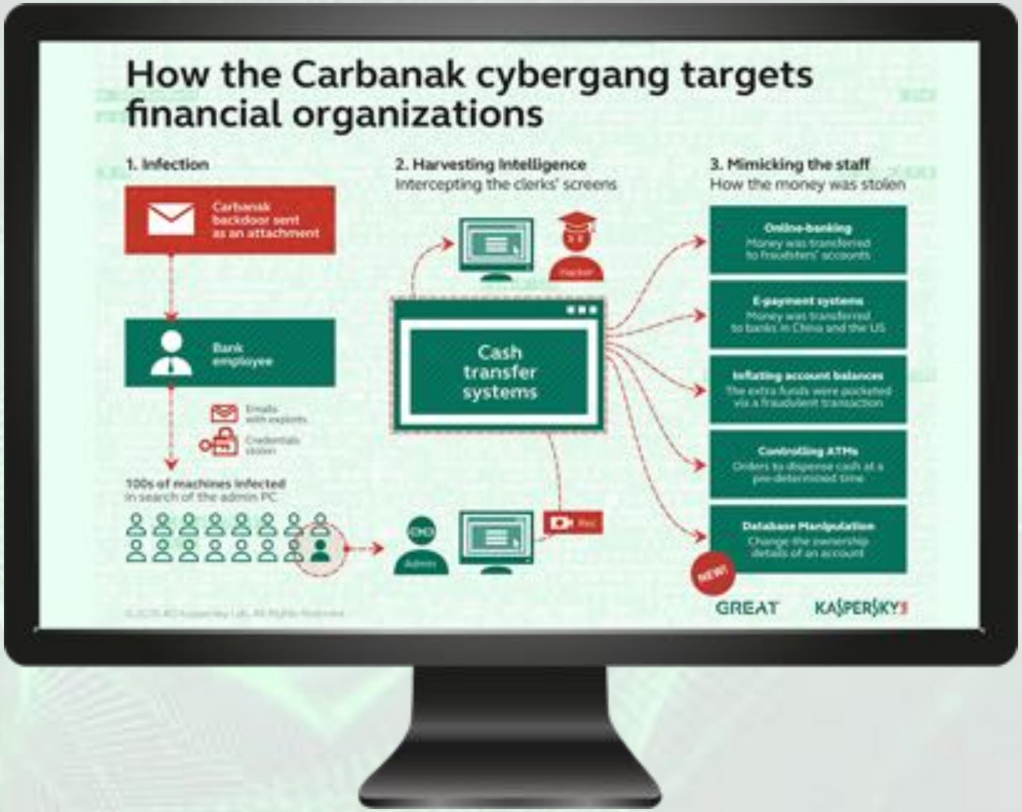
Sophisticated monetization scheme

Carbanak

Swift attacks

Taiwan ATM attack

other…


How the Carbanak cybergang targets financial organizations
1. Infection
Carbanak backdoor sent as an attachment
Bank employee
Emails with exploits
Credentials stolen
100s of machines infected
in search of the admin PC
Admin
2. Harvesting Intelligence
Intercepting the clerks' screens
Hacker
Cash transfer systems
Rec
3. Mimicking the staff
How the money was stolen
Online-banking
Money was transferred to fraudsters' accounts
E-payment systems
Money was transferred to banks in China and the US
Inflating account balances
The extra funds were pocketed via a fraudulent transaction
Controlling ATMs
Orders to dispense cash at a pre-determined time
Database Manipulation
Change the ownership details of an account
NEW!
GREAT
KASPERSKY

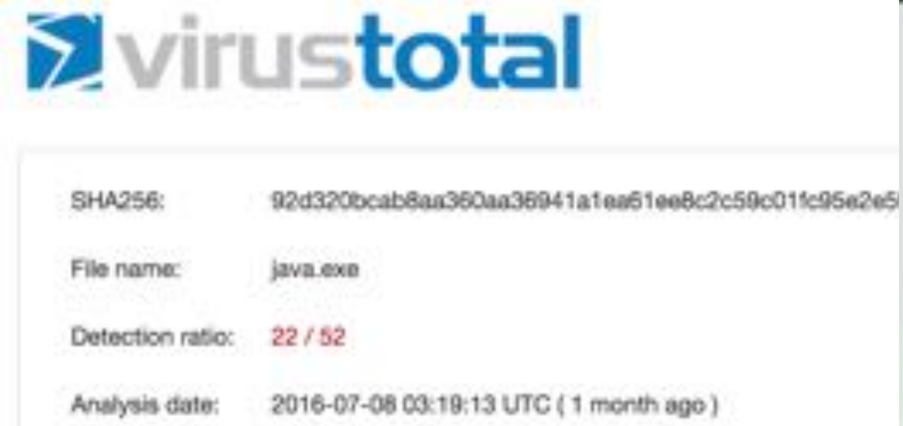
CYBER THREAT VELOCITY

https://www.youtube.com/watch?v=e50DpEvKJ-k

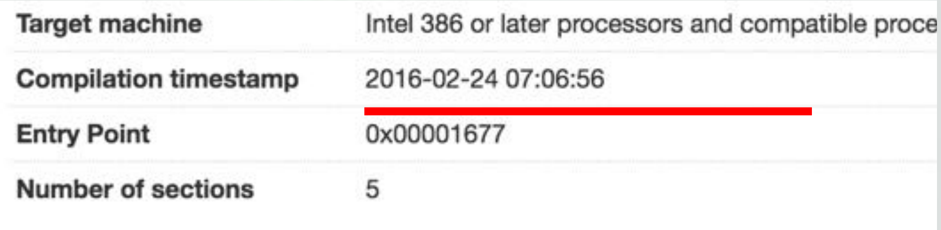
CYBER THREAT VELOCITY

https://www.youtube.com/watch?v=083s802WMw0

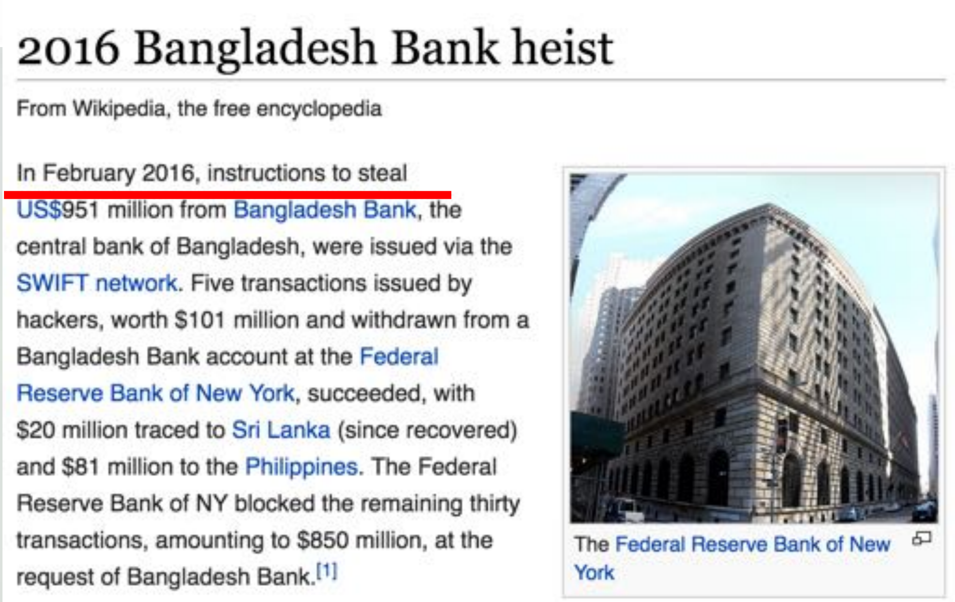
SWIFT ATTACK



SHA256:	92d320bcab8aa360aa36941a1ea61ee8c2c59c011c95e2e5
File name:	java.exe
Detection ratio:	22 / 52
Analysis date:	2016-07-08 03:19:13 UTC (1 month ago)



Target machine	Intel 386 or later processors and compatible proce
Compilation timestamp	2016-02-24 07:06:56
Entry Point	0x00001677
Number of sections	5

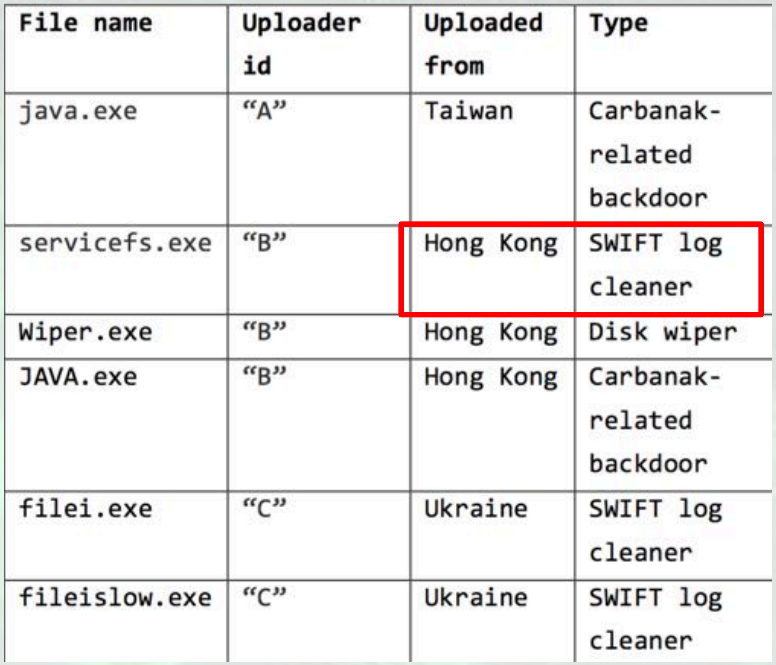


2016 Bangladesh Bank heist

From Wikipedia, the free encyclopedia

In February 2016, instructions to steal US$951 million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka (since recovered) and $81 million to the Philippines. The Federal Reserve Bank of NY blocked the remaining thirty transactions, amounting to $850 million, at the request of Bangladesh Bank.[1]

The Federal Reserve Bank of New York



File name	Uploader id	Uploaded from	Type
java.exe	"A"	Taiwan	Carbanak-related backdoor
servicefs.exe	"B"	Hong Kong	SWIFT log cleaner
Wiper.exe	"B"	Hong Kong	Disk wiper
JAVA.exe	"B"	Hong Kong	Carbanak-related backdoor
filei.exe	"C"	Ukraine	SWIFT log cleaner
fileislow.exe	"C"	Ukraine	SWIFT log cleaner

http://www.scmagazine.com/kaspersky-confirms-return-of-carbanak-and-two-more-banking-apt-groups/article/472224/
https://en.wikipedia.org/wiki/2016_Bangladesh_Bank_heist

THREAT VELOCITY

ATM attack

- 2014: Russia/East Europe
- 2015: Western Europe
- mid 2016: Taiwan

Swift attack

- Feb 2016: Bangladesh (Lazarus Group)
- Feb 2016: Tools by Carbanak Group
- Vietnam
- …

The case of the Encrypted disk

INVESTIGATION RESULTS: TELCO

500+ endpoints controlled by threat actors

The initial breach occurred 6 months before

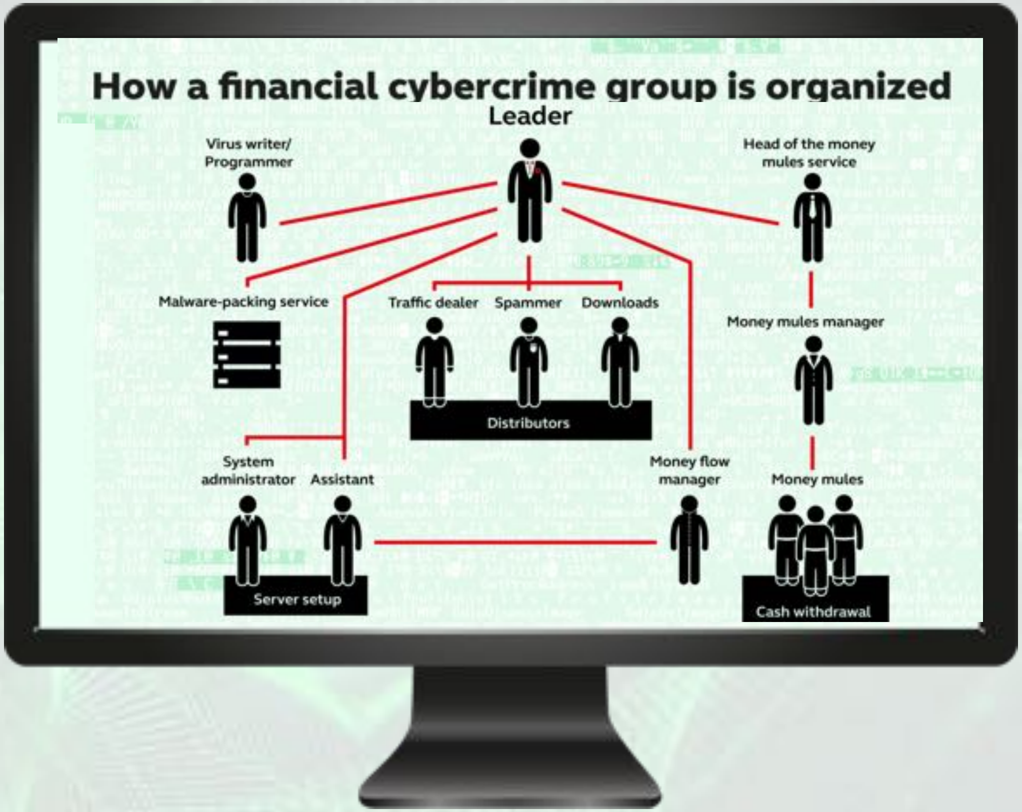
SQL Injection in eNodeB management interface

Remote access to the Enterprise was sold on the black market

Encryption was a mistake of botnet operator

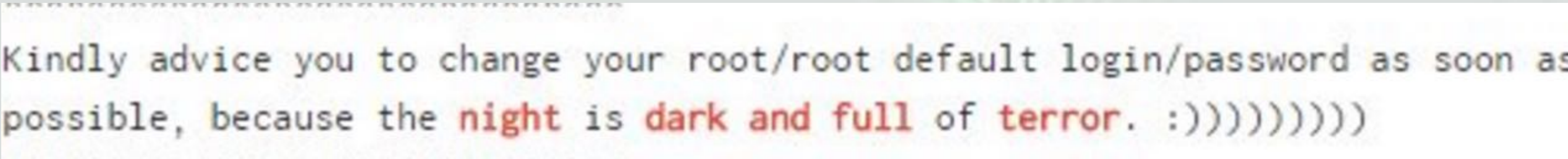
TECHNIQUES, TACTICS AND PROCEDURES

- Vulnerabilities in “hardware” devices
- Massive breach post processing
  - Targets selection and profiling
- Black market
  - Remote access
  - Insiders
  - Passwords
- Ransomware
  - Black Energy
  - Saudi Aramco
  - Locky
  - …

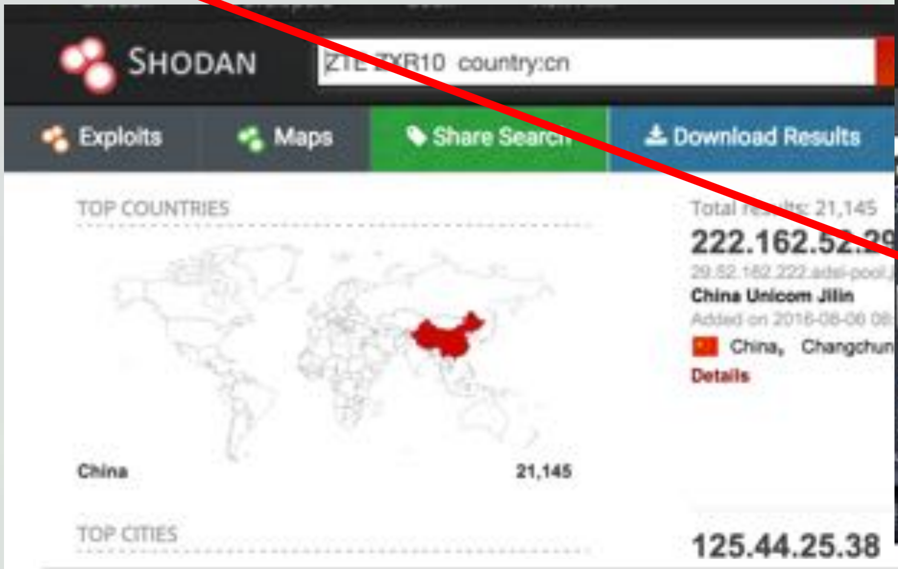


https://securelist.com/analysis/publications/72782/russian-financial-cybercrime-how-it-works/

TELECOMS IN THE INTERNET



```
*******************************
Kindly advice you to change your root/root default login/password as soon as
possible, because the night is dark and full of terror. :)))))))))
```

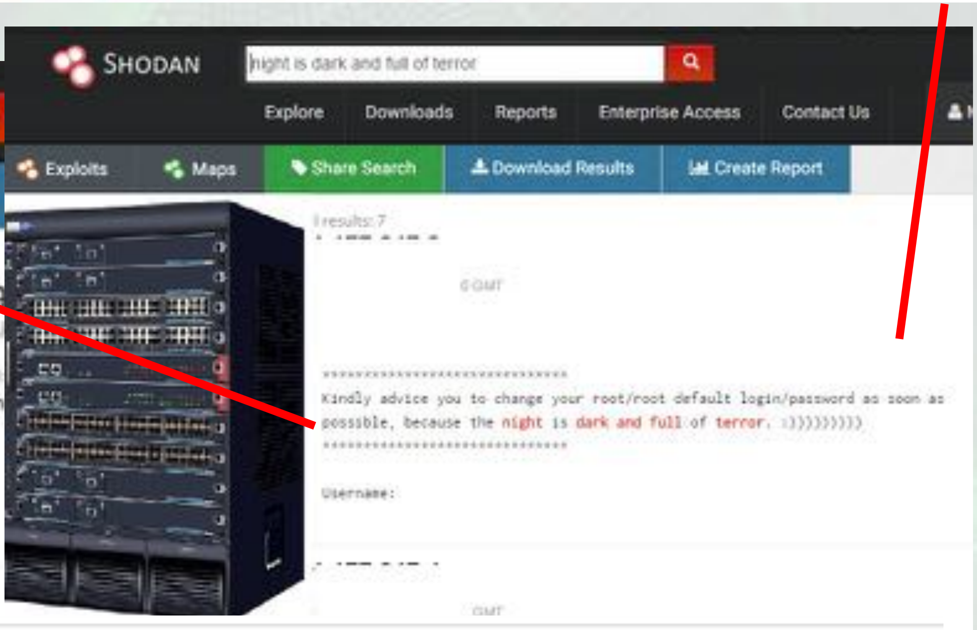


China	21,145

Total results: 21,145

222.162.52.29
29.52.162.222.adsl-pool...
China Unicom Jilin
Added on 2016-08-08 08:...
China, Changchun

125.44.25.38

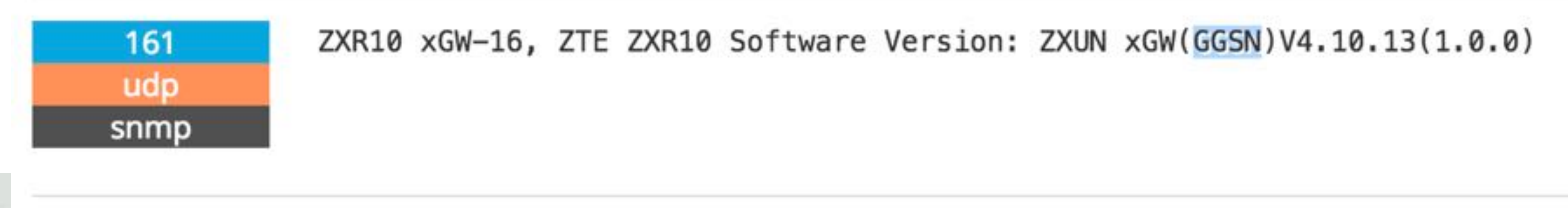


results: 7

```
GMT

*******************************
Kindly advice you to change your root/root default login/password as soon as
possible, because the night is dark and full of terror. :)))))))))
*******************************

Username:
```



161	udp	snmp

```
ZXR10 xGW-16, ZTE ZXR10 Software Version: ZXUN xGW(GGSN)V4.10.13(1.0.0)
```

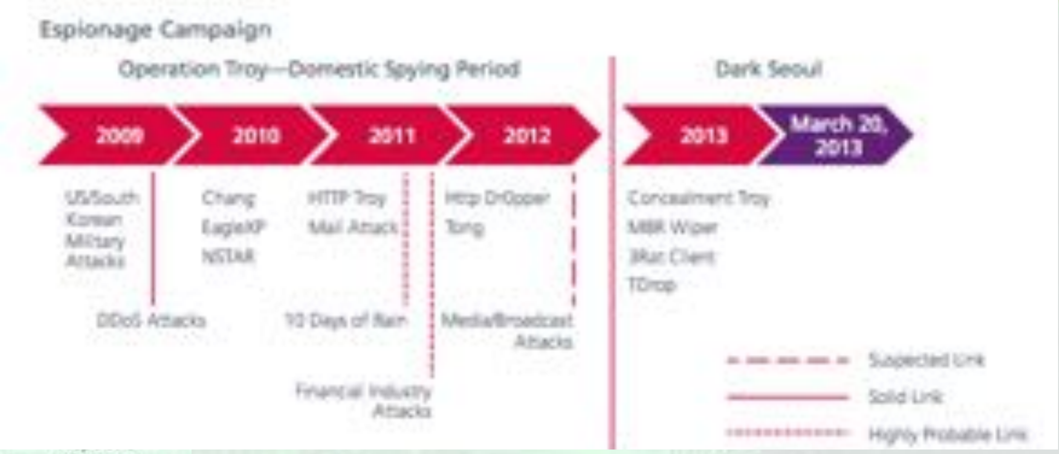
TELECOMS IN THE INTERNET

★OPERATION★

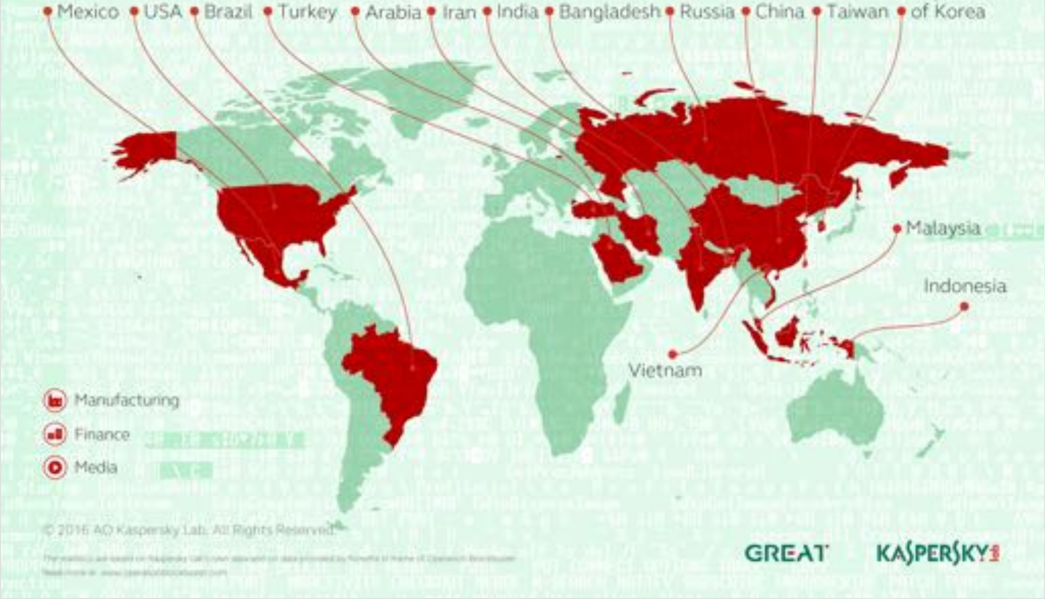
BLOCKBUSTER

Unraveling the Long Thread of the Sony Attack

NOVETTA



The targets of the Lazarus Group



The Analysis of SWIFT attacks revealed five additional pieces of malware containing portions of code shared by Lazarus Group

Pierluigi Paganini

http://securityaffairs.co/wordpress/47941/malware/lazarus-group-swift-attacks.html
http://www.theregister.co.uk/2013/07/11/mcafee_dark_seoul_analysis/
https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf
https://blog.kaspersky.com/operation-blockbuster/11407/

THE DROPPING ELEPHANT/UNVEILING PATCHWORK

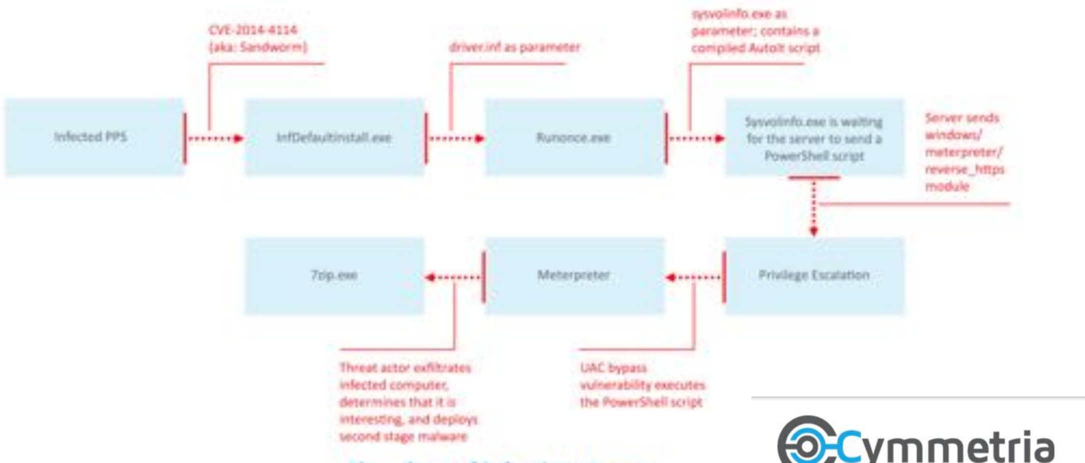
Focused on China and APAC

Reuse of Sandworm/BlackEnergy

Simple tools (AutoIT)

国务院关于同意设立哈尔滨新区的批复

三、黑龙江省人民政府要切实加强组织领导，明确工作分工，完善工作机制，加大支持力度，积极探索与现行体制协调、联动、高效的新区管理方式，扎实稳妥推进新区建设发展。要认真做好哈尔滨新区发展规划编制工作，规划建设必须符合土地利用总体规划、城市总体规划、镇总体规划、环境保护规划、水资源综合规划等相关专项规划的要求。要推动新区探索“多规合一”，着力优化空间布局。涉及的重要政策和重大建设项目要按规定程序报批。


CVE-2014-4114
(aka: Sandworm)
driver.inf as parameter
sysvolinfo.exe as parameter; contains a compiled AutoIt script
Infected PPS
InfDefaultInstall.exe
Runonce.exe
Sysvolinfo.exe is waiting for the server to send a PowerShell script
Server sends windows/meterpreter/reverse_https module
7zip.exe
Meterpreter
Privilege Escalation
Threat actor exfiltrates infected computer, determines that it is interesting, and deploys second stage malware
UAC bypass vulnerability executes the PowerShell script

Flowchart of infection stages

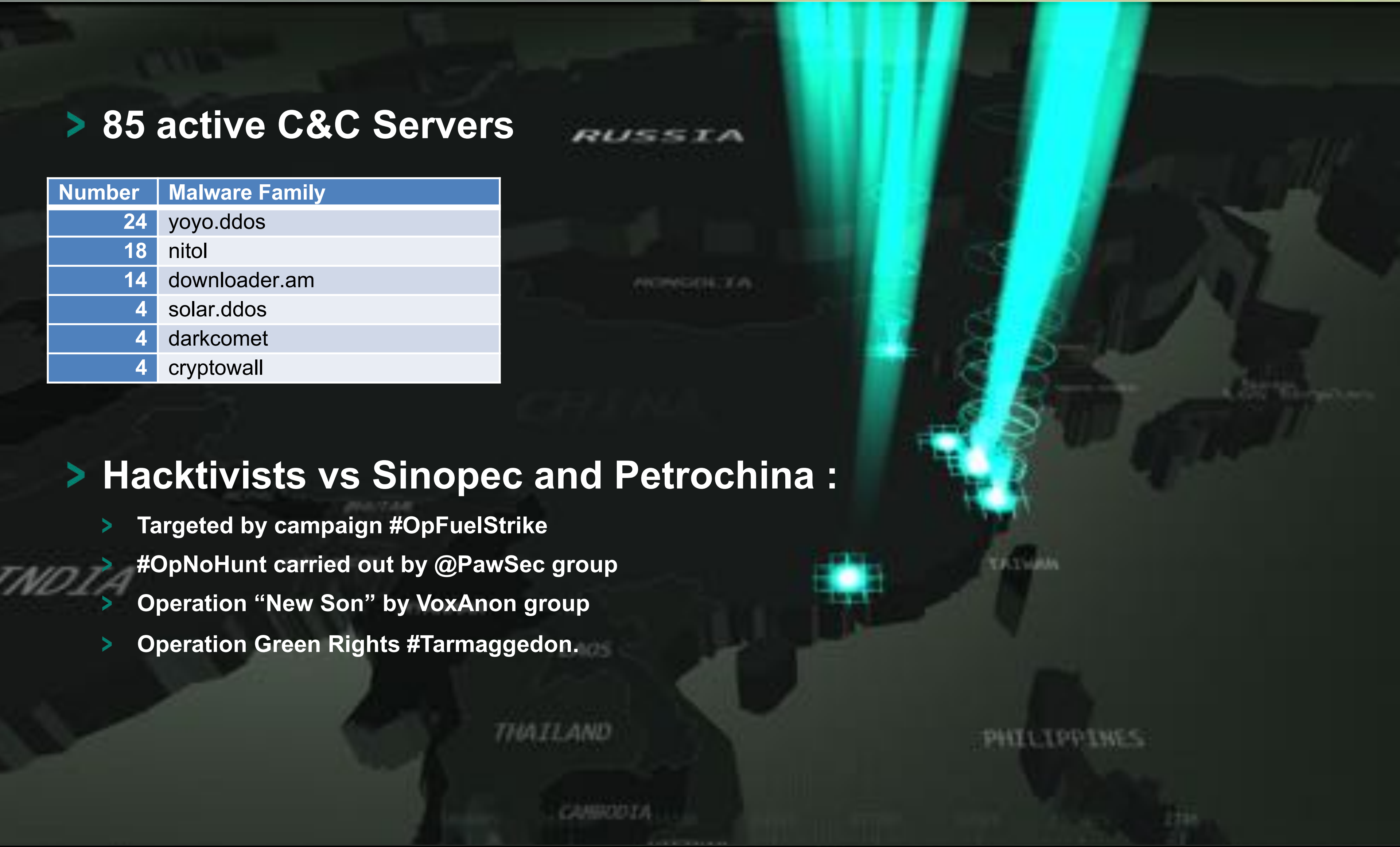
Cymmetria

https://securelist.com/blog/research/75328/the-dropping-elephant-actor/

https://www.cymmetria.com/patchwork-targeted-attack/

COVEOPS

DDOS ATTACKS



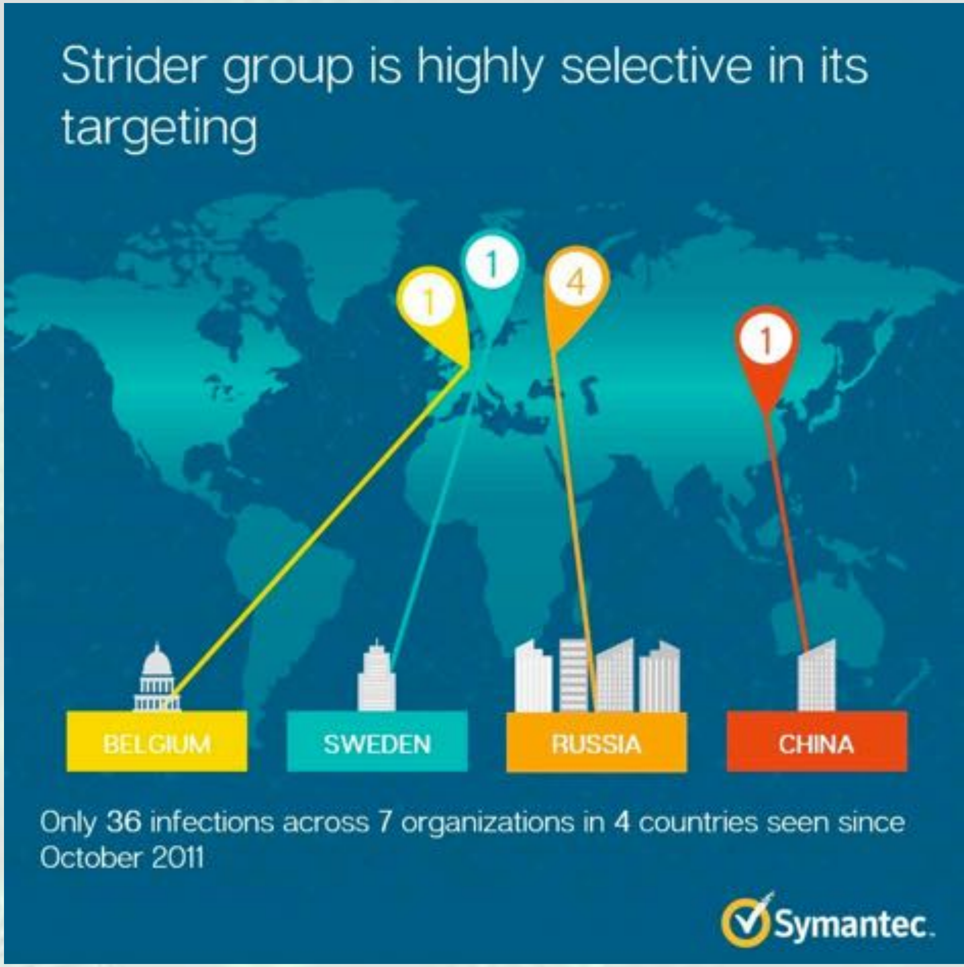
- 85 active C&C Servers

Number	Malware Family
24	yoyo.ddos
18	nitol
14	downloader.am
4	solar.ddos
4	darkcomet
4	cryptowall

- Hacktivists vs Sinopec and Petrochina :
  - Targeted by campaign #OpFuelStrike
  - #OpNoHunt carried out by @PawSec group
  - Operation “New Son” by VoxAnon group
  - Operation Green Rights #Tarmaggedon.

PROJECT SAURON/STRIDER

- Focus on gov and military
- Active since 2011
- Use of zero day exploits
- Never identified attack vectors
- Works in air gapped networks
- Exist only in memory
- Undocumented OS features



Strider group is highly selective in its targeting

Only 36 infections across 7 organizations in 4 countries seen since October 2011

Symantec.

The case of the

FIRE DETECTOR

SECURITY ASSESSMENT

Web-server backup on contractor’s open ftp

Passwords from Web-server can be used for VPN

Smart fire detectors in corporate network

Smart fire detectors in technology network

Full access to SCADA and PLC from the Internet in 3 days

THREATS?

Four Cyber Attacks On UK Railways In A Year

A security experts says the hackers could create "real disaster related to train safety".

Video: Sky News has learned that the UK railway network has suffered at least four major cyber attacks over the last year alone.

Ukrainian blackout caused by hackers that attacked media company, researchers say

Power company suffered a major attack that led to blackouts across western Ukraine, after an attack on a Ukrainian media company

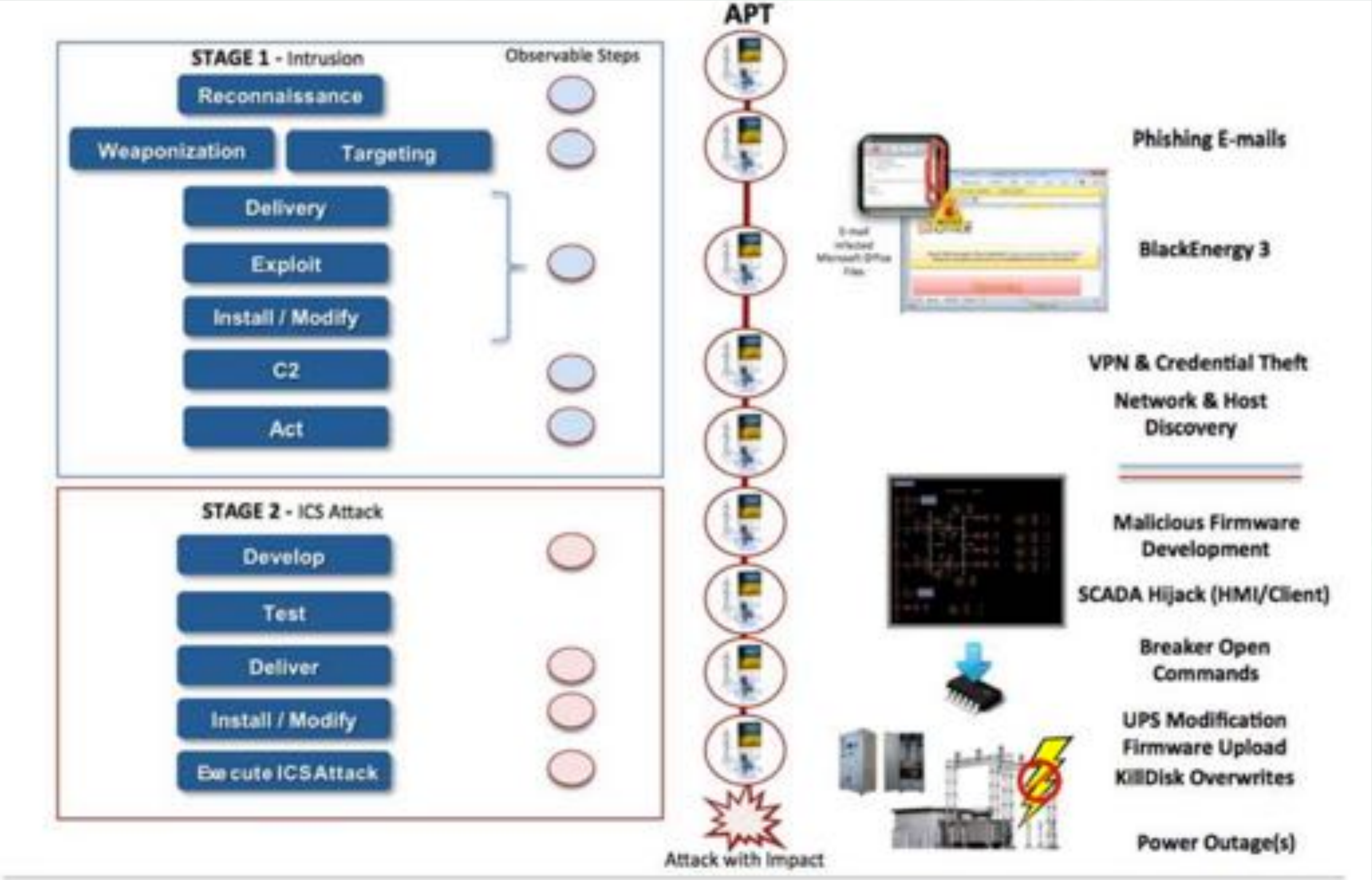
Smokestacks in Dniprodzershynsk, Ukraine. Photograph: John Mcconnico/AP

http://news.sky.com/story/four-cyber-attacks-on-uk-railways-in-a-year-10498558

https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company

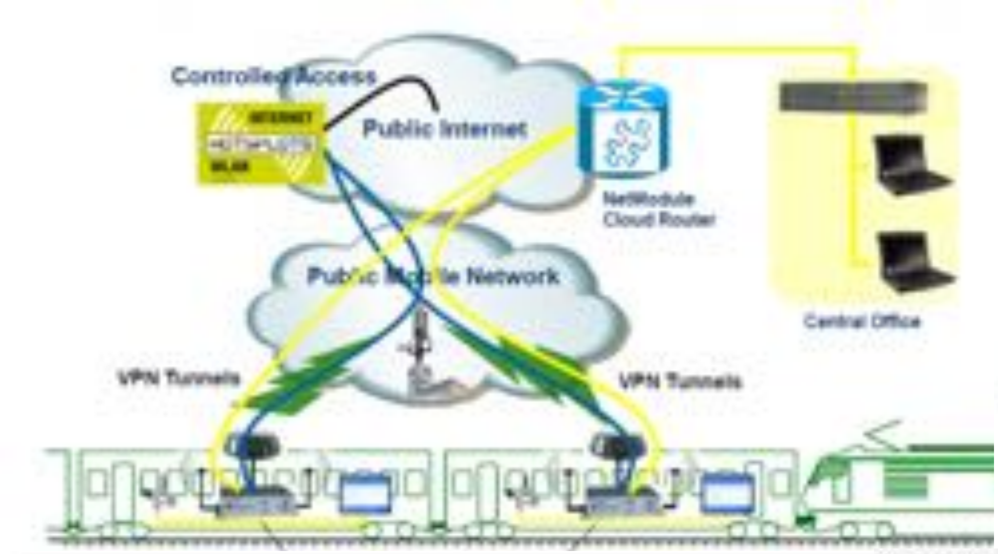
“REAL” ICS ATTACK?

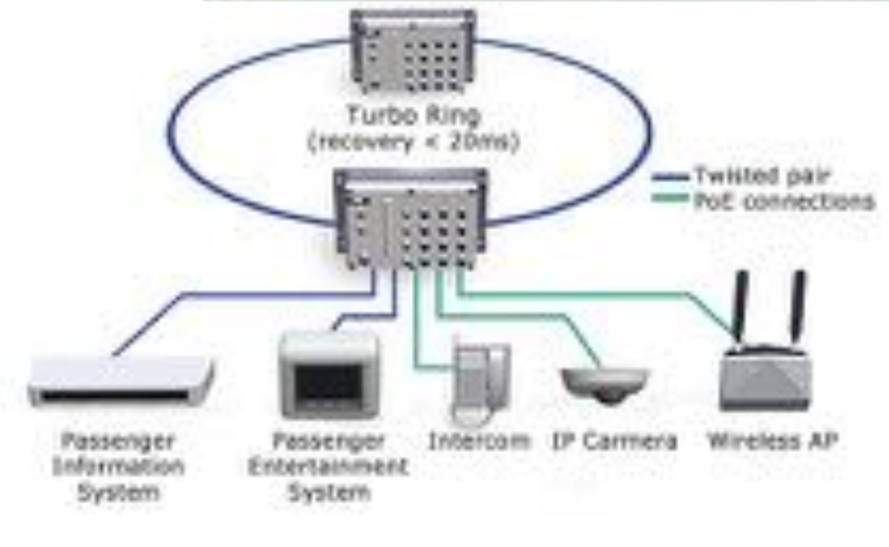
«It is extremely important to note that neither BlackEnergy 3, unreported backdoors, KillDisk, nor the malicious firmware uploads alone were responsible for the outage»

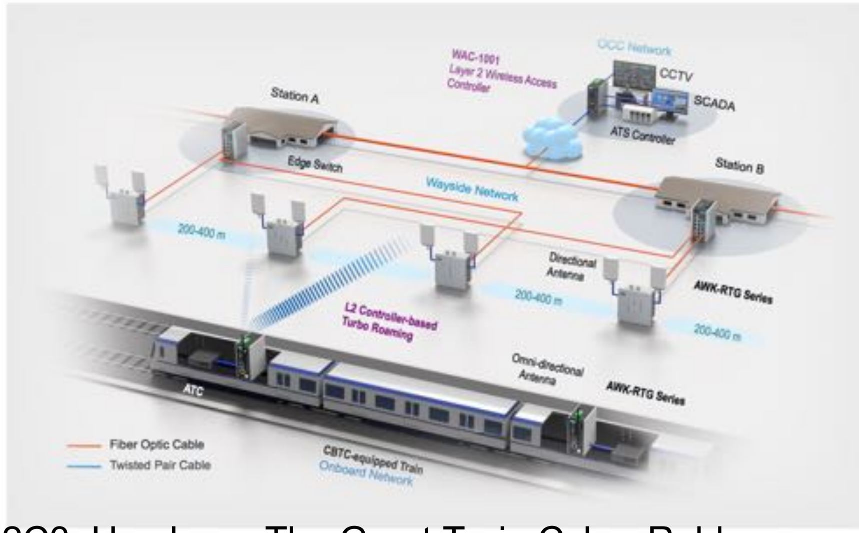


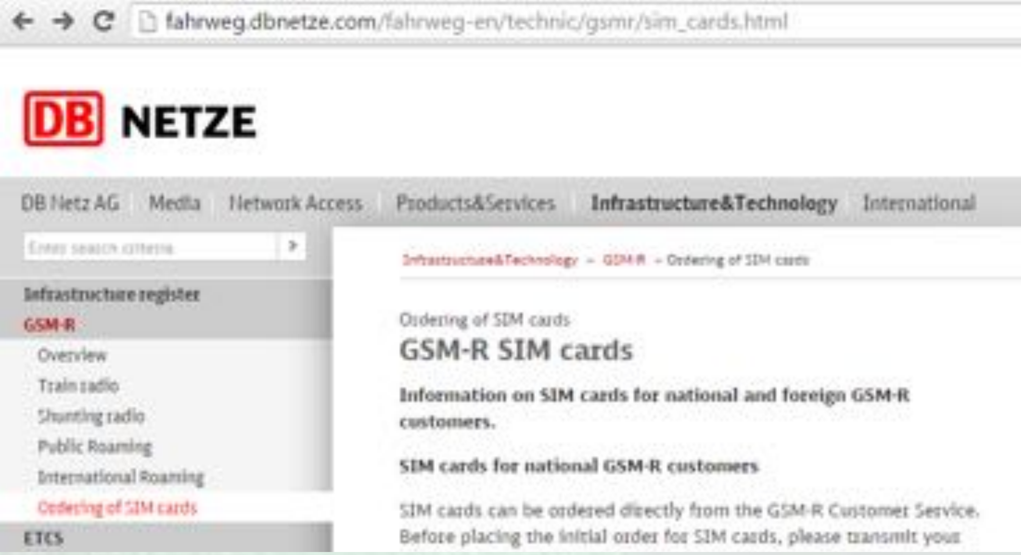
http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

INTERCONNECTED WORLD








fahrweg.dbnetze.com/fahrweg-en/technic/gsmr/sim_cards.html

DB NETZE

DB Netz AG | Media | Network Access | Products&Services | Infrastructure&Technology | International

Enter search criteria

Infrastructure register
GSM-R
- Overview
- Train radio
- Shunting radio
- Public Roaming
- International Roaming
- Ordering of SIM cards

ETCS

Infrastructure&Technology → GSM-R → Ordering of SIM cards

Ordering of SIM cards

GSM-R SIM cards

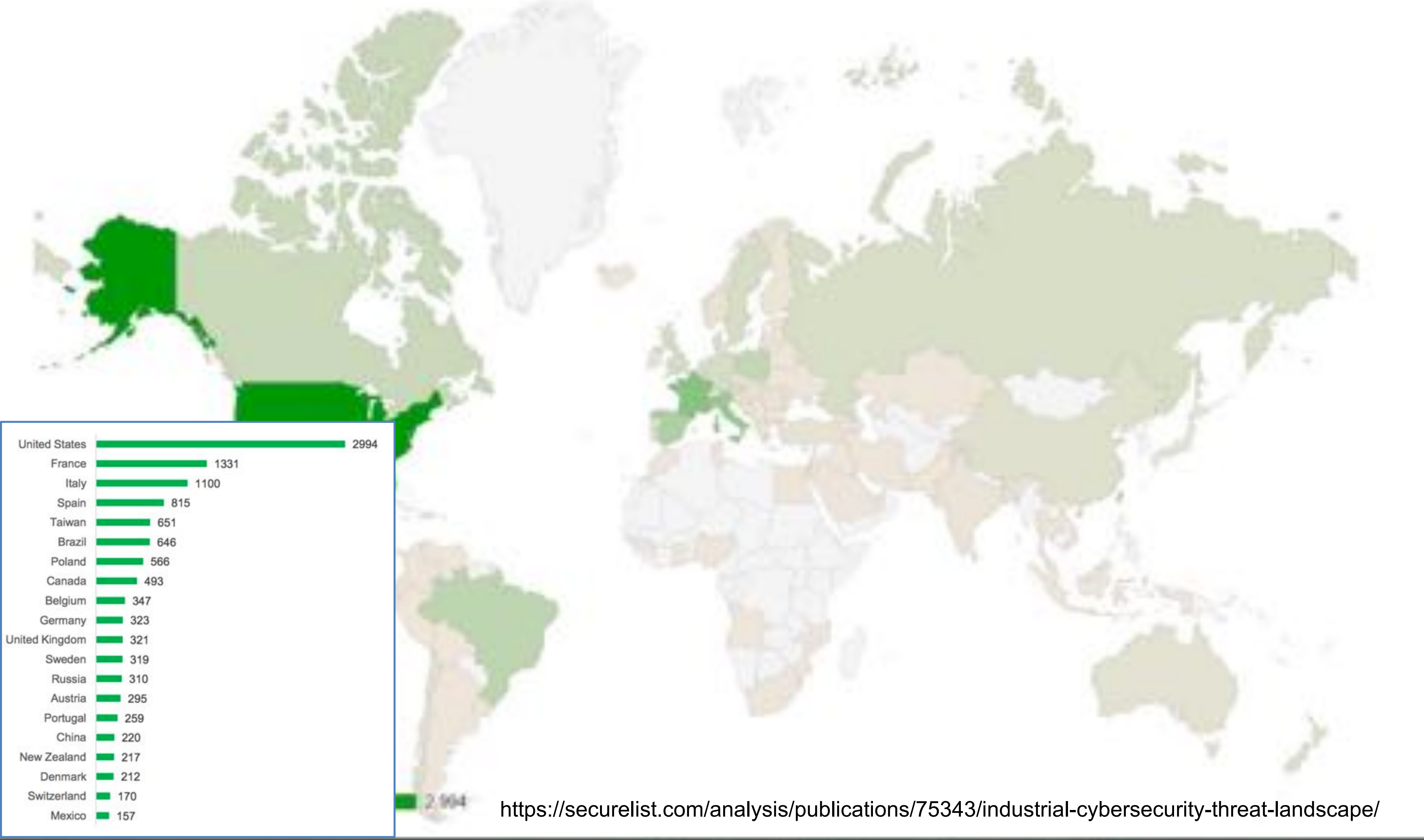
Information on SIM cards for national and foreign GSM-R customers.

SIM cards for national GSM-R customers

SIM cards can be ordered directly from the GSM-R Customer Service. Before placing the initial order for SIM cards, please transmit your

32C3, Hamburg, The Great Train Cyber Robbery

220,558 ONLINE, 17,042 IN ENTERPRISES

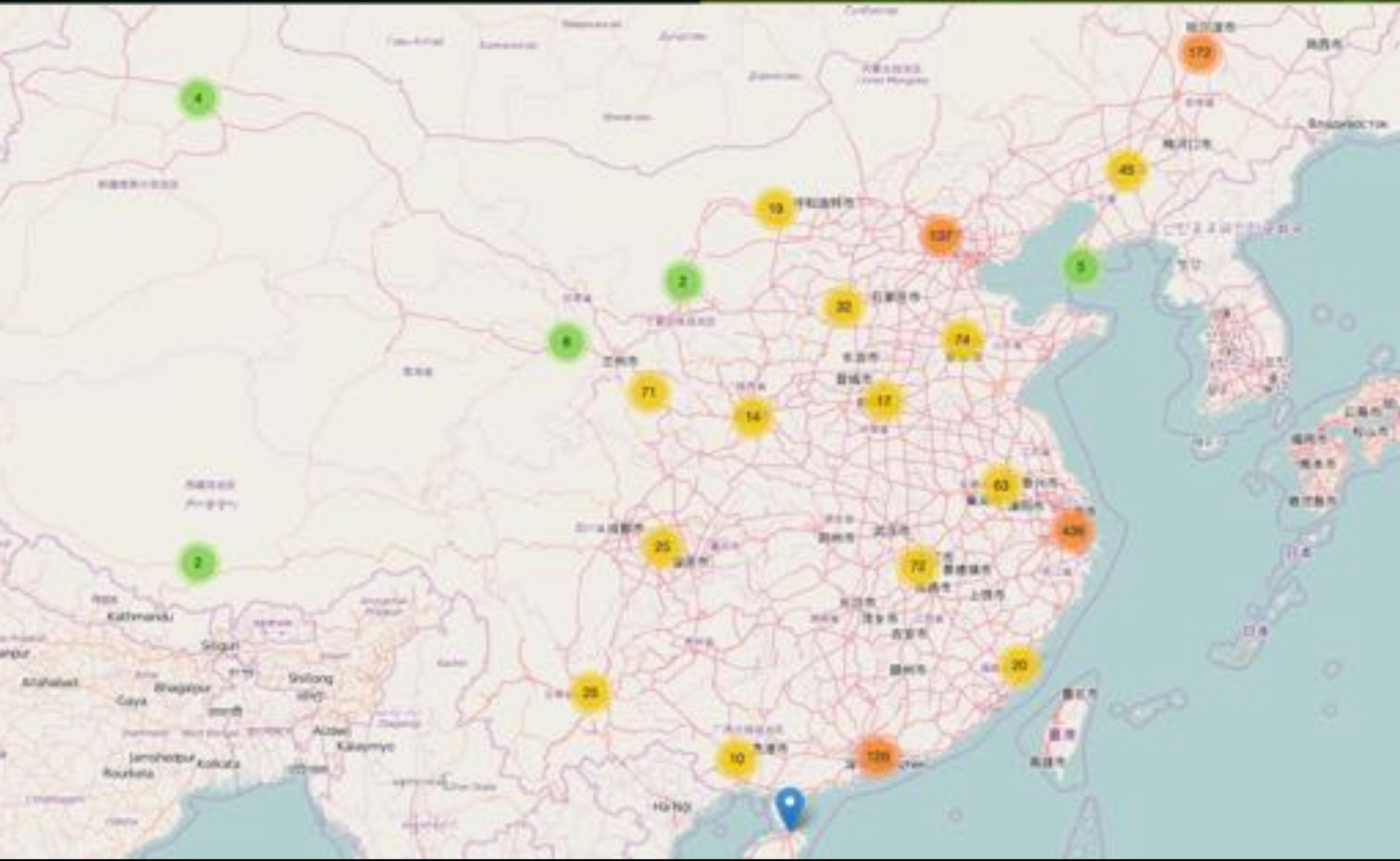


https://securelist.com/analysis/publications/75343/industrial-cybersecurity-threat-landscape/

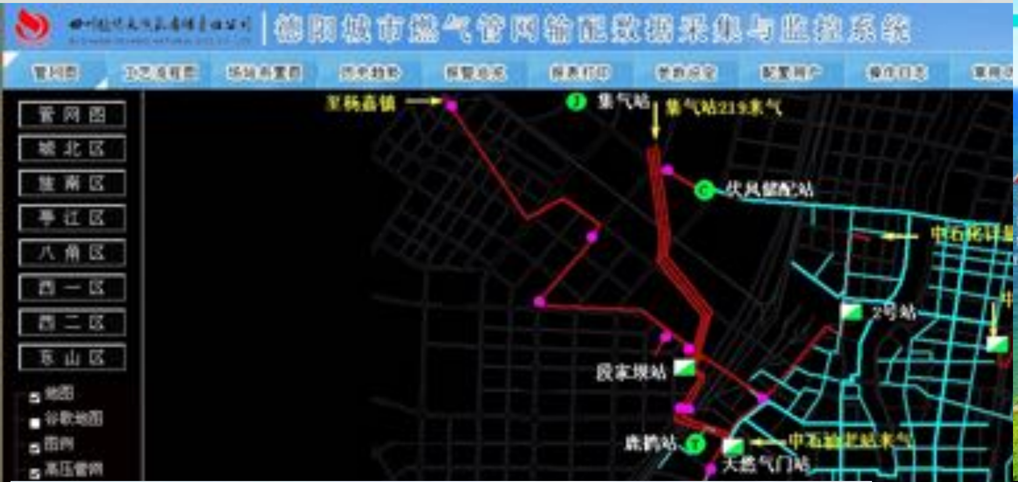
ICS ONLINE: CHINA

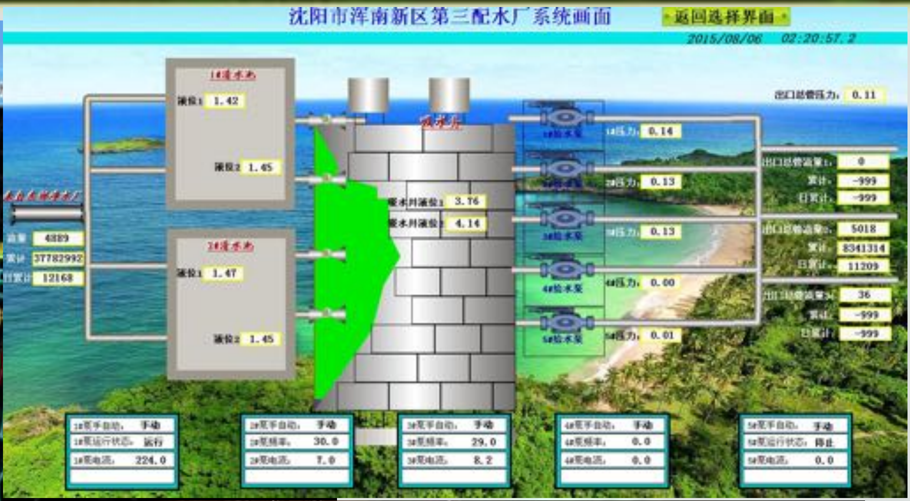
ISC 2016 中国互联网安全大会

360互联网安全中心



ICS ONLINE: CHINA





http://plcscan.org/blog/2016/03/census-scanning-from-siemens-s7-plc-cpustatus/

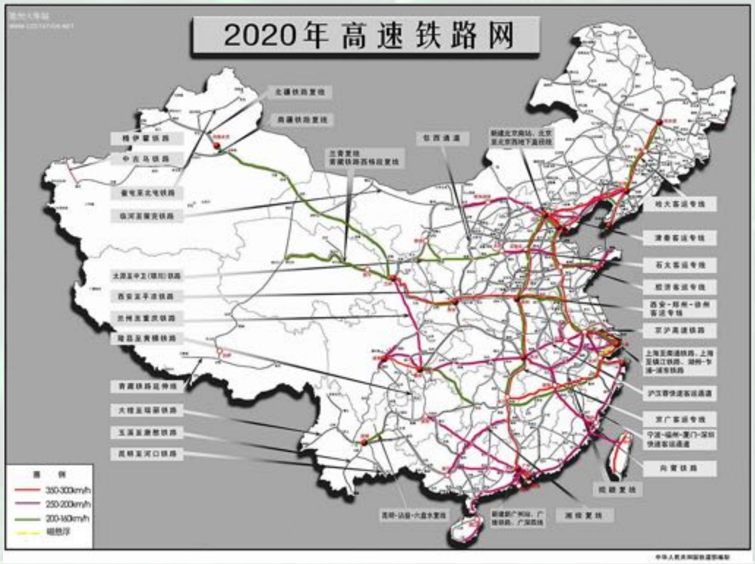
GREATER CHINA

~10,000 OF “SMART” POWER GRID OBJECTS

- GREEN ENERGY
- SMART GRID
- DIGITAL SUBSTATIONS

121,000 KM OF RAILWAYS

- NATIONAL HIGH-SPEED RAIL GRID (4+4)
- 19,000 KM OF HIGH-SPEED
- HIGHLY AUTOMATED



DIGITAL SUBSTATION TAKEOVER

- FIND VULNERABILITIES IN IEC-61850 SUBSTATIONS
- CREATE EXPLOIT
- TRIGGER CYBER-PHYSICAL ATTACK

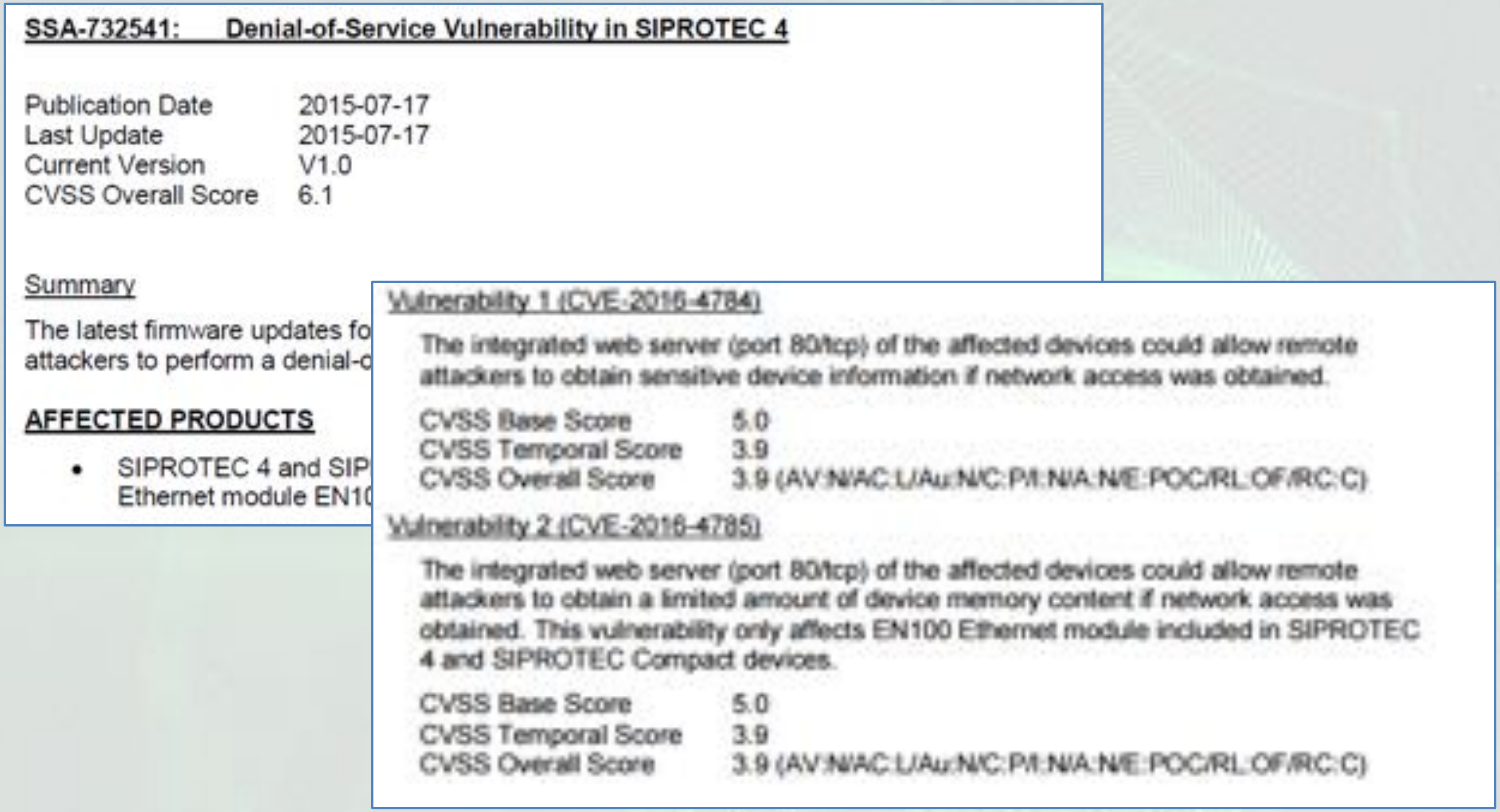
http://www.phdays.com/press/news/41213/

CYBER PHYSICAL ATTACK

- CYBER-PHISICAL ATTACK

https://www.youtube.com/watch?v=w8T-bbO3Qec

VULNERABILITIES IN RELAY PROTECTION



SSA-732541: Denial-of-Service Vulnerability in SIPROTEC 4

Publication Date	2015-07-17
Last Update	2015-07-17
Current Version	V1.0
CVSS Overall Score	6.1

Summary

The latest firmware updates fo
attackers to perform a denial-o

AFFECTED PRODUCTS

- SIPROTEC 4 and SIP
  Ethernet module EN10

Vulnerability 1 (CVE-2016-4784)

The integrated web server (port 80/tcp) of the affected devices could allow remote attackers to obtain sensitive device information if network access was obtained.

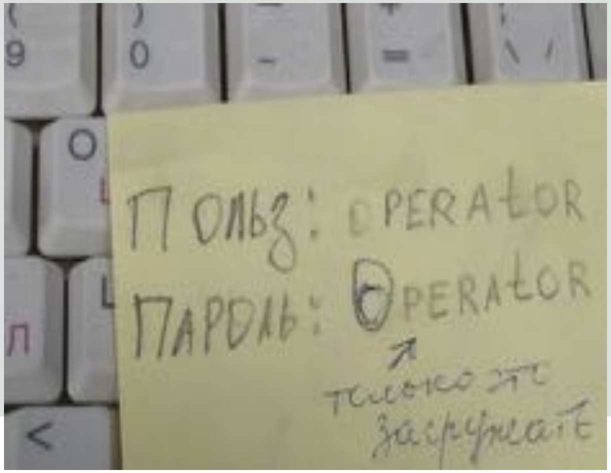
CVSS Base Score	5.0
CVSS Temporal Score	3.9
CVSS Overall Score	3.9 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

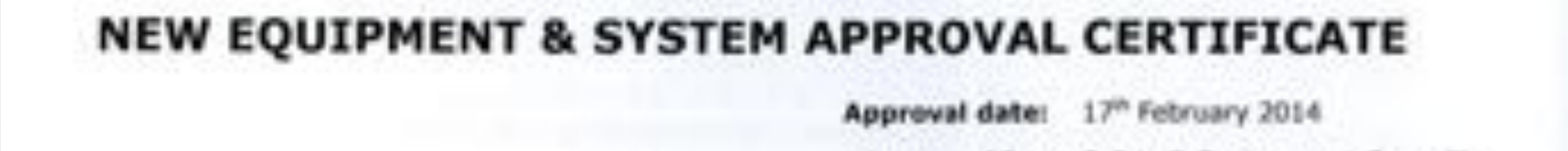
Vulnerability 2 (CVE-2016-4785)

The integrated web server (port 80/tcp) of the affected devices could allow remote attackers to obtain a limited amount of device memory content if network access was obtained. This vulnerability only affects EN100 Ethernet module included in SIPROTEC 4 and SIPROTEC Compact devices.

CVSS Base Score	5.0
CVSS Temporal Score	3.9
CVSS Overall Score	3.9 (AV:N/AC:L/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

RAILWAY ATC





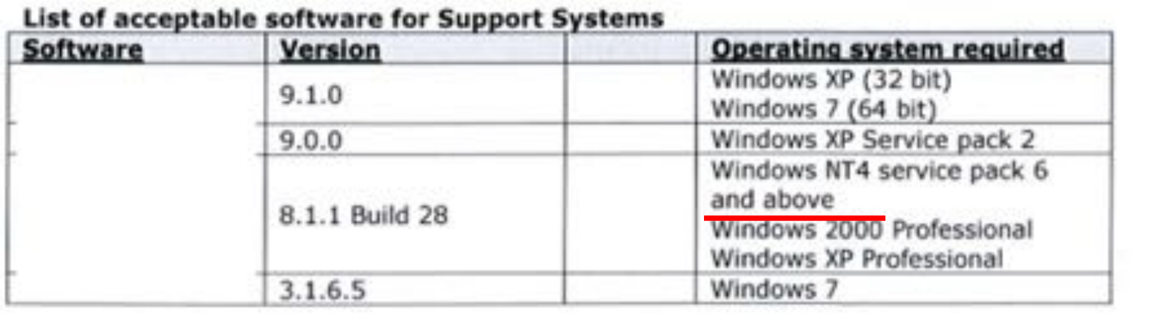
NEW EQUIPMENT & SYSTEM APPROVAL CERTIFICATE

Approval date: 17th February 2014

by: Safety & Environment Committee

no.: [redacted]

ate: 30th January 2014



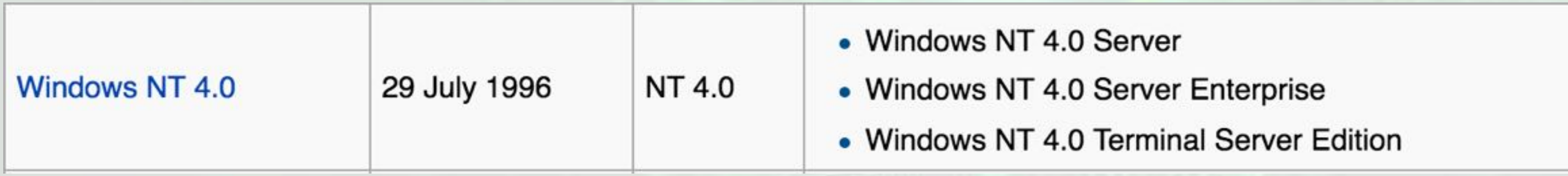
List of acceptable software for Support Systems

Software	Version		Operating system required
	9.1.0		Windows XP (32 bit) Windows 7 (64 bit)
	9.0.0		Windows XP Service pack 2
	8.1.1 Build 28		Windows NT4 service pack 6 and above Windows 2000 Professional Windows XP Professional
	3.1.6.5		Windows 7

http://scadastrangelove.blogspot.com/2015/12/32c3-slides.html

RAILWAY COMPUTER BASED INTERLOCKING

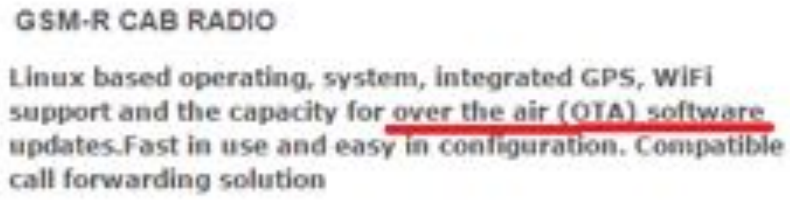
WINDOWS NT 4.0 SERVICE PACK 6!



Windows NT 4.0	29 July 1996	NT 4.0	• Windows NT 4.0 Server • Windows NT 4.0 Server Enterprise • Windows NT 4.0 Terminal Server Edition

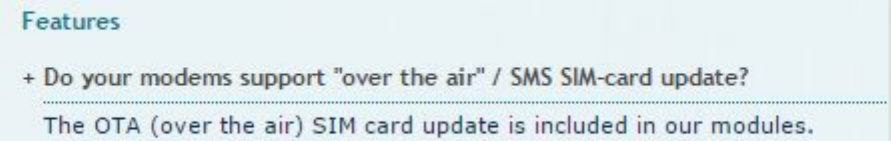
http://scadastrangelove.blogspot.com/2015/12/32c3-slides.html

RAILWAY GSM-R ISSUES



GSM-R CAB RADIO

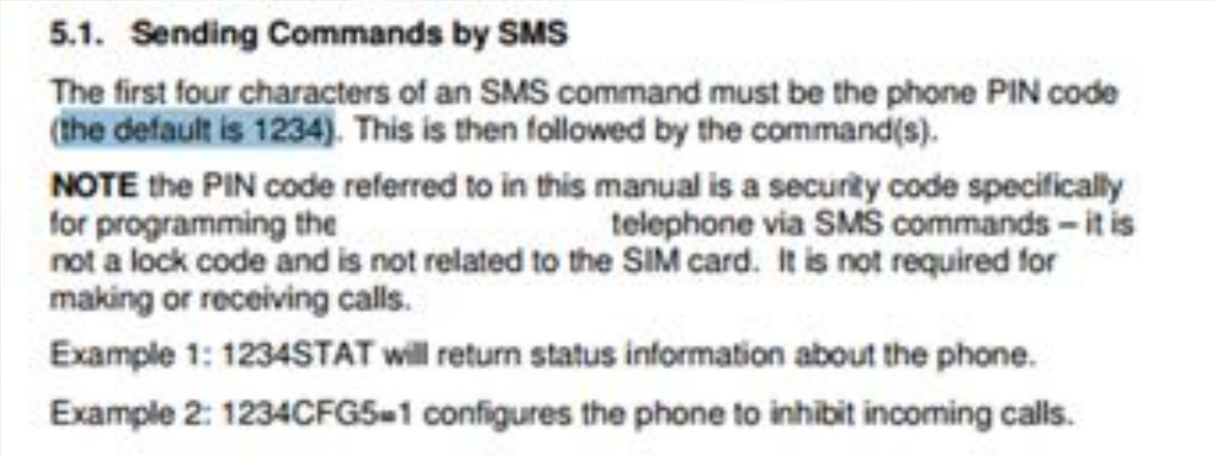
Linux based operating, system, integrated GPS, WiFi support and the capacity for over the air (OTA) software updates.Fast in use and easy in configuration. Compatible call forwarding solution



Features

+ Do your modems support "over the air" / SMS SIM-card update?

The OTA (over the air) SIM card update is included in our modules.



5.1. Sending Commands by SMS

The first four characters of an SMS command must be the phone PIN code (the default is 1234). This is then followed by the command(s).

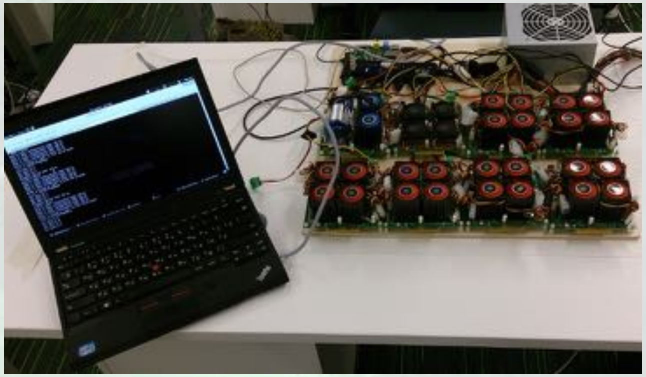
NOTE the PIN code referred to in this manual is a security code specifically for programming the telephone via SMS commands – it is not a lock code and is not related to the SIM card. It is not required for making or receiving calls.

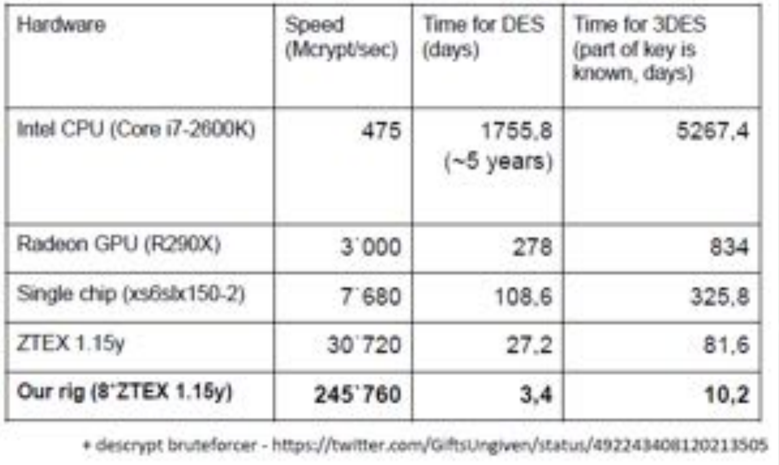
Example 1: 1234STAT will return status information about the phone.

Example 2: 1234CFG5=1 configures the phone to inhibit incoming calls.

VULNERABILITIES OF (U)SIM

- Remote data recovery (Kc, TIMSI)
  - Chanel decryption (including A5/3)
  - «Clone» the SIM and mobile station
- SIM “malware”
- Block SIM via PIN/PUK brute
- Extended OTA features (FOTA)



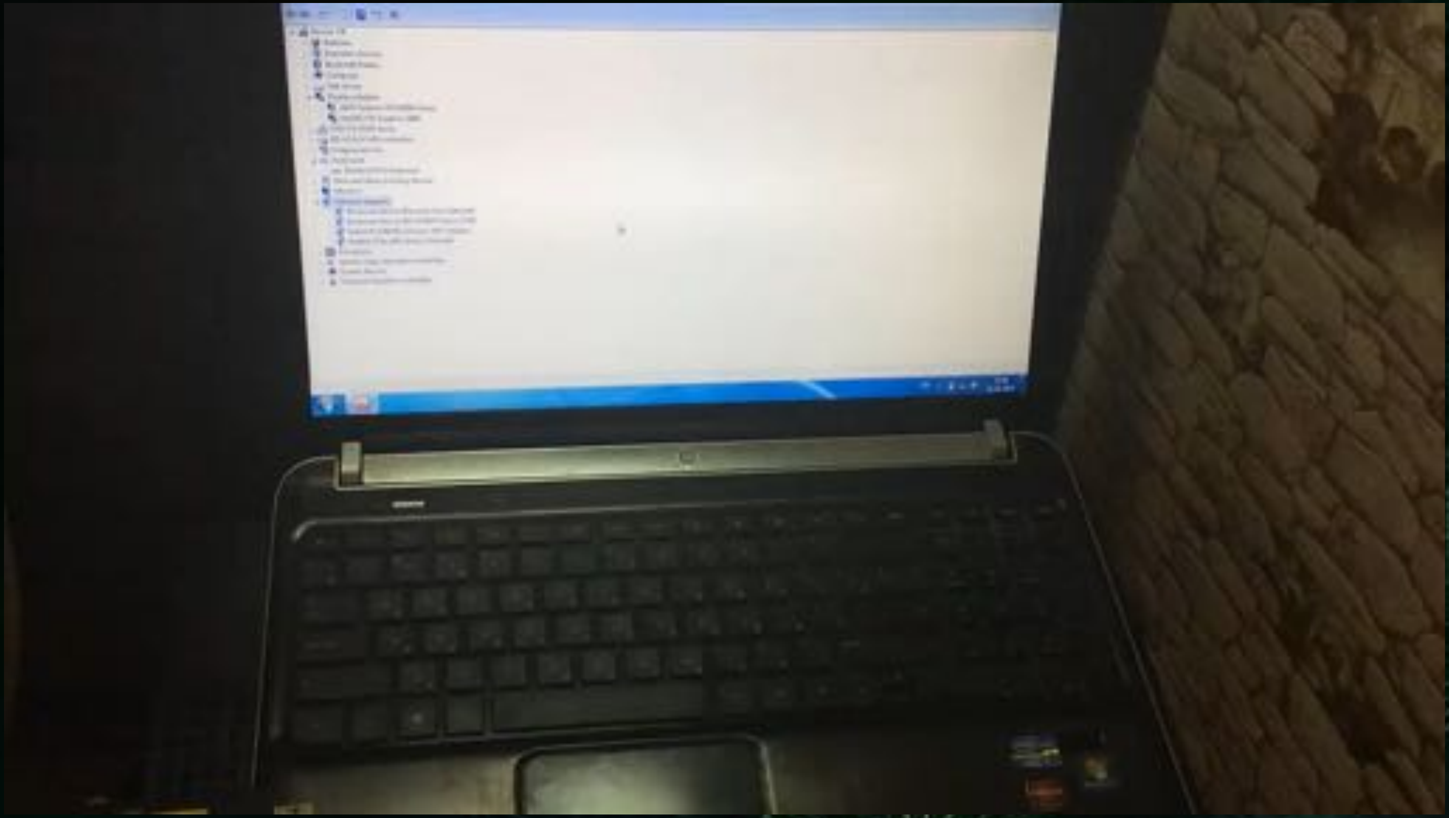


Hardware	Speed (Mcrypt/sec)	Time for DES (days)	Time for 3DES (part of key is known, days)
Intel CPU (Core i7-2600K)	475	1755,8 (~5 years)	5267,4
Radeon GPU (R290X)	3`000	278	834
Single chip (xs6slx150-2)	7`680	108,6	325,8
ZTEX 1.15y	30`720	27,2	81,6
Our rig (8*ZTEX 1.15y)	**245`760**	**3,4**	**10,2**

+ descrypt bruteforcer - https://twitter.com/GiftsUngiven/status/492243408120213505

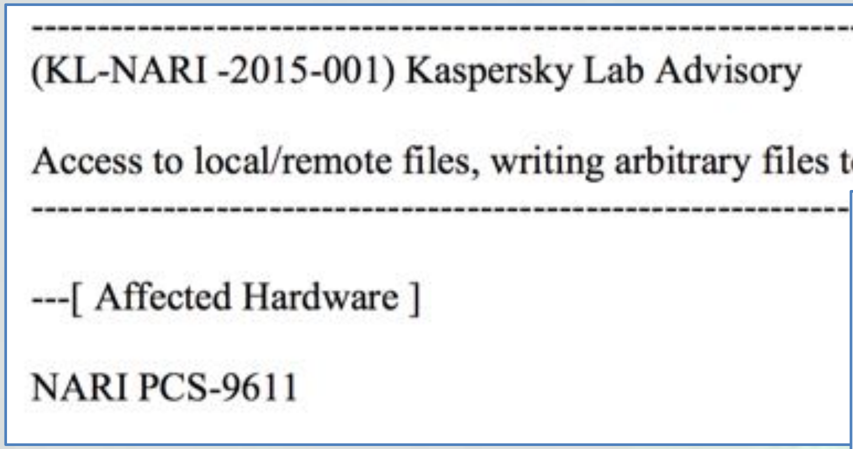
Karsten Nohl, https://srlabs.de/rooting-sim-cards/
Alexander Zaitsev, Sergey Gordeychik , Alexey Osipov, PacSec, Tokyo, Japan, 2014

BOOTKIT VIA SMS



https://www.youtube.com/watch?v=jmY9VRq5e1Y&t=5420

LOCAL VENDORS

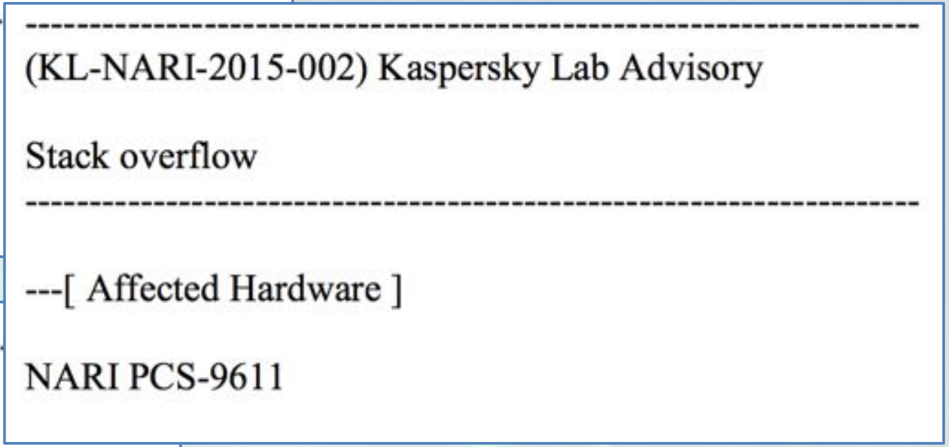


(KL-NARI -2015-001) Kaspersky Lab Advisory

Access to local/remote files, writing arbitrary files to file system.

---[Affected Hardware]

NARI PCS-9611

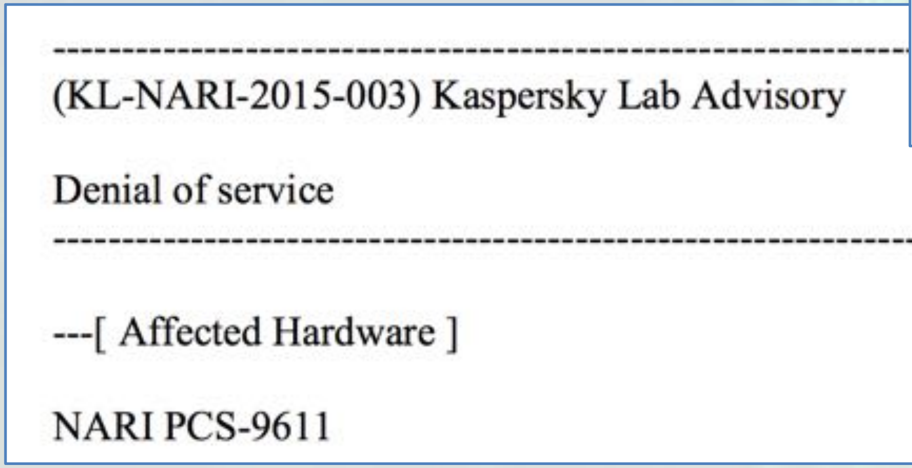


(KL-NARI-2015-002) Kaspersky Lab Advisory

Stack overflow

---[Affected Hardware]

NARI PCS-9611



(KL-NARI-2015-003) Kaspersky Lab Advisory

Denial of service

---[Affected Hardware]

NARI PCS-9611

LET DO IT TOGETHER!

- GOVERNMENT
  REGULATORY AUTHORITIES
  LAW ENFORCEMENTS
  CERTS

- RESEARCHERS

- ICS VENDORS

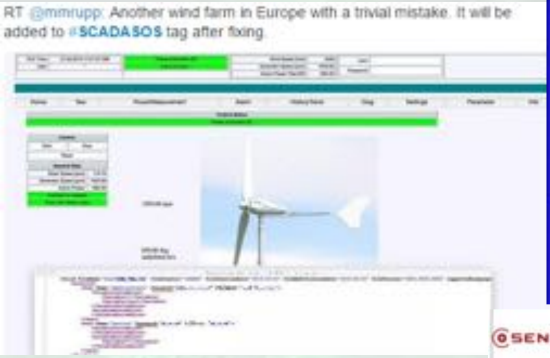
- SECURITY VENDORS

- OPERATORS OF CRITICAL INFRASTRUCTURE

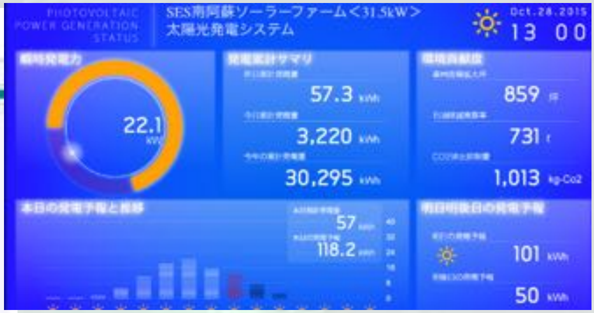
#SCADASOS

Q: WTF SACADSOS?
A: SCADASOS - (un)Secure Open SmartGrids is open initiative to rise awareness on insecurities of SmartGrid, Photovoltaic Power Stations and Wind Farms.

Q: How to participate
A: Find Internet-connected PV and Wind power stations and notify vendors/CERTs/community.



RT @mmrupp: Another wind farm in Europe with a trivial mistake. It will be added to #SCADASOS tag after fixing

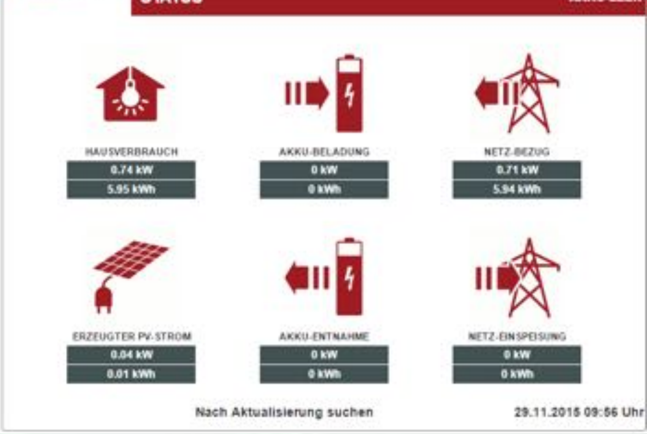


PHOTOVOLTAIC POWER GENERATION STATUS

SES南阿蘇ソーラーファーム<31.5kW>
太陽光発電システム

Oct.28.2015
13 00

Kagoshima – Nishinoomote
Fukuhira ES
鹿児島市立福平小
Goino
Kagoshimashi Hirakawadobutsu Park
鹿児島市平川動物公園
Kinkowan Park
錦江湾公園
226
Kagoshima Red Cross Hospital
鹿児島赤十字病院
Hama Hirakawa Post Office



SENEC.IES

STATUS | AUTARKIE | AKKUMULATOR | EINSTELLUNGEN

STATUS — AKKU-LEER

HAUSVERBRAUCH	AKKU-BELADUNG	NETZ-BEZUG
0.74 kW	0 kW	0.71 kW
5.95 kWh	0 kWh	5.94 kWh

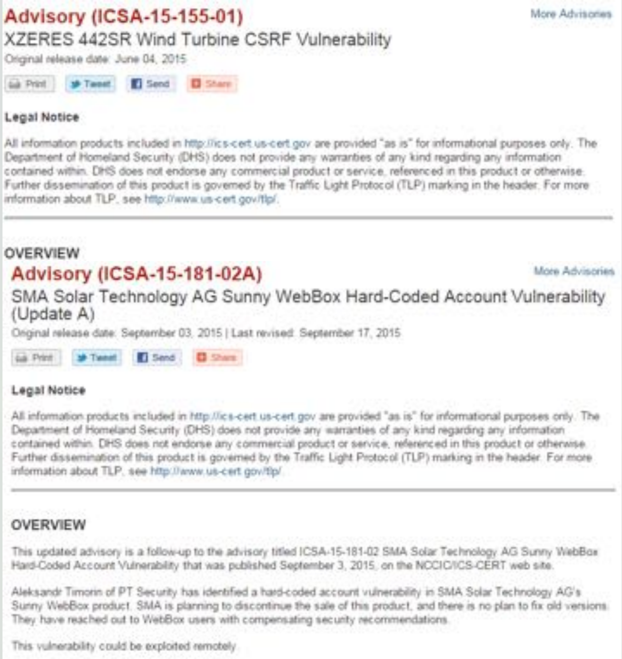
ERZEUGTER PV-STROM	AKKU-ENTNAHME	NETZ-EINSPEISUNG
0.04 kW	0 kW	0 kW
0.01 kWh	0 kWh	0 kWh

Nach Aktualisierung suchen

29.11.2015 09:56 Uhr

#SCADASOS RESULTS

- 60 000+ SmartGrid devices disconnected from the Internet
- Advisories/patches



Advisory (ICSA-15-155-01) More Advisories

XZERES 442SR Wind Turbine CSRF Vulnerability

Original release date: June 04, 2015

Print Tweet Send Share

Legal Notice

All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

Advisory (ICSA-15-181-02A) More Advisories

SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability (Update A)

Original release date: September 03, 2015 | Last revised: September 17, 2015

Print Tweet Send Share

Legal Notice

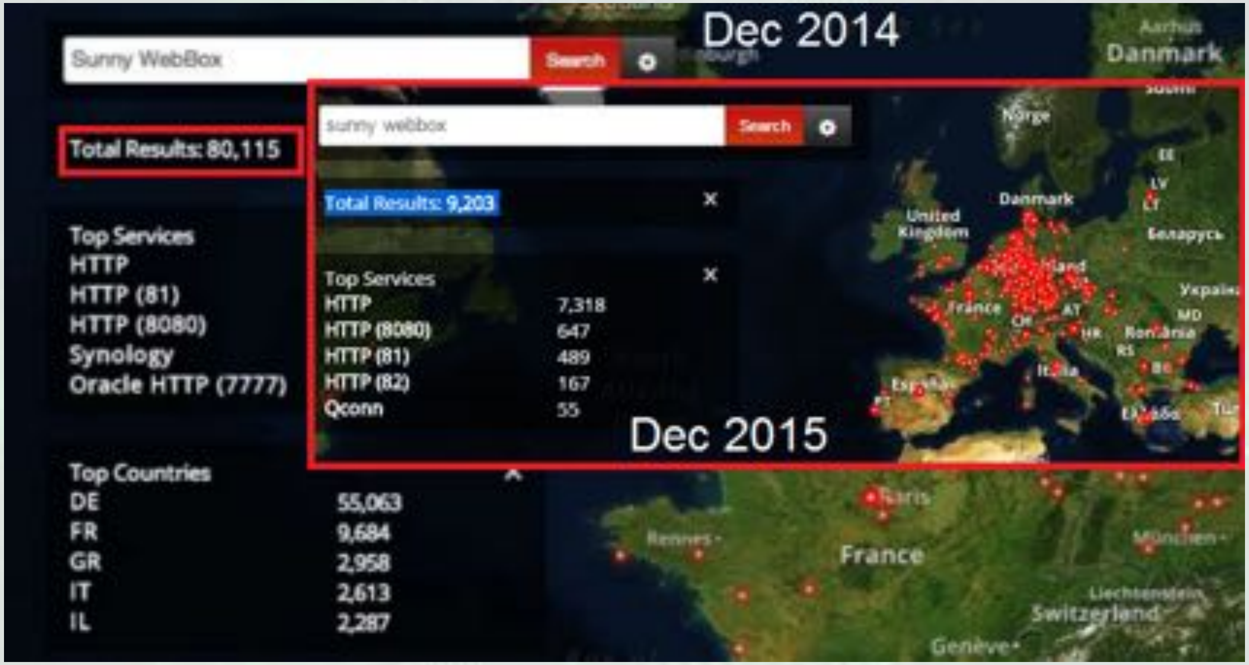
All information products included in http://ics-cert.us-cert.gov are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see http://www.us-cert.gov/tlp/.

OVERVIEW

This updated advisory is a follow-up to the advisory titled ICSA-15-181-02 SMA Solar Technology AG Sunny WebBox Hard-Coded Account Vulnerability that was published September 3, 2015, on the NCCIC/ICS-CERT web site.

Aleksandr Timorin of PT Security has identified a hard-coded account vulnerability in SMA Solar Technology AG's Sunny WebBox product. SMA is planning to discontinue the sale of this product, and there is no plan to fix old versions. They have reached out to WebBox users with compensating security recommendations.

This vulnerability could be exploited remotely.



Dec 2014

Sunny WebBox Search

Total Results: 80,115

Top Services
HTTP
HTTP (81)
HTTP (8080)
Synology
Oracle HTTP (7777)

Top Countries	
DE	55,063
FR	9,684
GR	2,958
IT	2,613
IL	2,287

Dec 2015

sunny webbox Search

Total Results: 9,203

Top Services	
HTTP	7,318
HTTP (8080)	647
HTTP (81)	489
HTTP (82)	167
Qconn	55

THANK YOU!

KISA Korea Internet & Security Agency

enisa

NISC

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

GovCERT.HK

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Governmental Computer Emergency Response Team

ICS Security Workspace
专注于工控安全攻防技术研究

Russian GOV CERT

THANKS

WWW.SCADA.SL
@SCADASL
SCADASTRANGELOVE@GMAIL.COM
1337@KASPERSKY.COM