RSA Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-W09

ICS Threats. A Kaspersky Lab view, predictions and reality

Andrey Nikishin

Special Projects Director
Kaspersky Lab
@andreynikishin

#RSAC

Type of incidents

- Accidental infection by (traditional) malware
- Insiders' actions
- Targeted attacks (including APT)

Energetic Bear / Crouching Yeti

Energetic Bear / Crouching Yeti

- APT campaign since 2010, 2800+ victims world wide
- Energy sector, manufacturing, pharmaceutical
- Spreading via
  - Emails with exploit
  - Infected legitimate web sites (watering hole)
  - Infected (repacked) legitimate installation packages
- Compromised Legitimate web sites as Control centres
- Contains a number of different trojans, backdoors and exploit packs

Energetic Bear / Crouching Yeti

- Infected (repacked) legitimate installation packages hosted on vendors' web and FTP sites :
  - "eWon" – Belgium Developer of SCADA software and network equipment
  - "MB Connect Line GmbH" – PLC remote control software developer
  - "MESA Imaging AG" – super speed 3D cameras and sensors manufacturer (Switzerland)

Energetic Bear / Crouching Yeti

- Watering hole web recourses:
  - gse.com.ge - Georgian State Electrosystem
  - gamyba.le.lt - Lithuania's largest electricity generating company
  - chariotoilandgas.com - Chariot Oil and Gas Ltd
  - longreachoilandgas.com - Longreach Oil & Gas Ltd
  - vitogaz.com - French-based gas distributor, supplier and technical developer

Energetic Bear / Crouching Yeti

- List of ports used by Havex in order to discover OPC :
  - 502 - Modbus
  - 102 - Siemens PLC
  - 11234 - Measuresoft ScadaPro
  - 12401 - 7-Technologies IGSS SCADA
  - 44818 - Rockwell Rslinx / FactoryTalk

aluigi.altervista.org/adv.htm

Luigi Auriemma

me@aluigi.org

- News
- QuickBMS
- Research
- MyToolz
- Advisories
- Proof-of-concepts
- Fake_players_bug
- Patches
- Password_recovery
- MyMusic
- TestingToolz
- About...
- RSS_feeds
- Amiga_ADF
- Forum

ADVISORIES

The complete archive of my advisories about software security vulnerabilities found by me.
The (SCADA) tag covers anything of the HMI/SCADA, PLC, automation and industrial sector.
There are other tags like (enterprise), (game), (media), (streaming), (p2p) and (no tag) for other types of software.
All the advisories include the steps for replicating the problems or links to the relative proof-of-concept.

Heap overflow in Rockwell RSLogix 19 (FactoryTalk RnaUtility.dll) (SCADA)
13 Sep 2011: adv - rslogix_1

Multiple vulnerabilities in Measuresoft ScadaPro 4.0.0 (SCADA)
13 Sep 2011: adv - scadapro_1

Vulnerabilities in 7-Technologies IGSS 9.00.00.11059 (SCADA)
21 Mar 2011: adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - adv8 - igss_1/8

Vulnerabilities in DATAC RealWin 2.1 (Build 6.1.10.10) (SCADA)
21 Mar 2011: adv1 - adv2 - adv3 - adv4 - adv5 - adv6 - adv7 - realwin_2/8

US ICS-CERT report (ICSA-14-178-01) :

- In particular, the payload gathers server information that includes CLSID, server name, Program ID, OPC version, vendor information, running state, group count, and server bandwidth. In addition to more generic OPC server information, the Havex payload also has the capability of enumerating OPC tags.
- ICS-CERT testing has determined that the Havex payload has caused multiple common OPC platforms to intermittently crash. This could cause a denial of service effect on applications reliant on OPC communications.

== ping of death

Miancha

Miancha

- On 2nd January 2014 Monju Nuclear Power Plant sys admin discovered multiple connections to one of the 8 PCs in nuclear reactor control centre
- Reason – malicious update for GOM Media Player was installed 5 days before.
- There were 42,000+ emails and documents on the compromised PC. Some of them were stolen by criminals

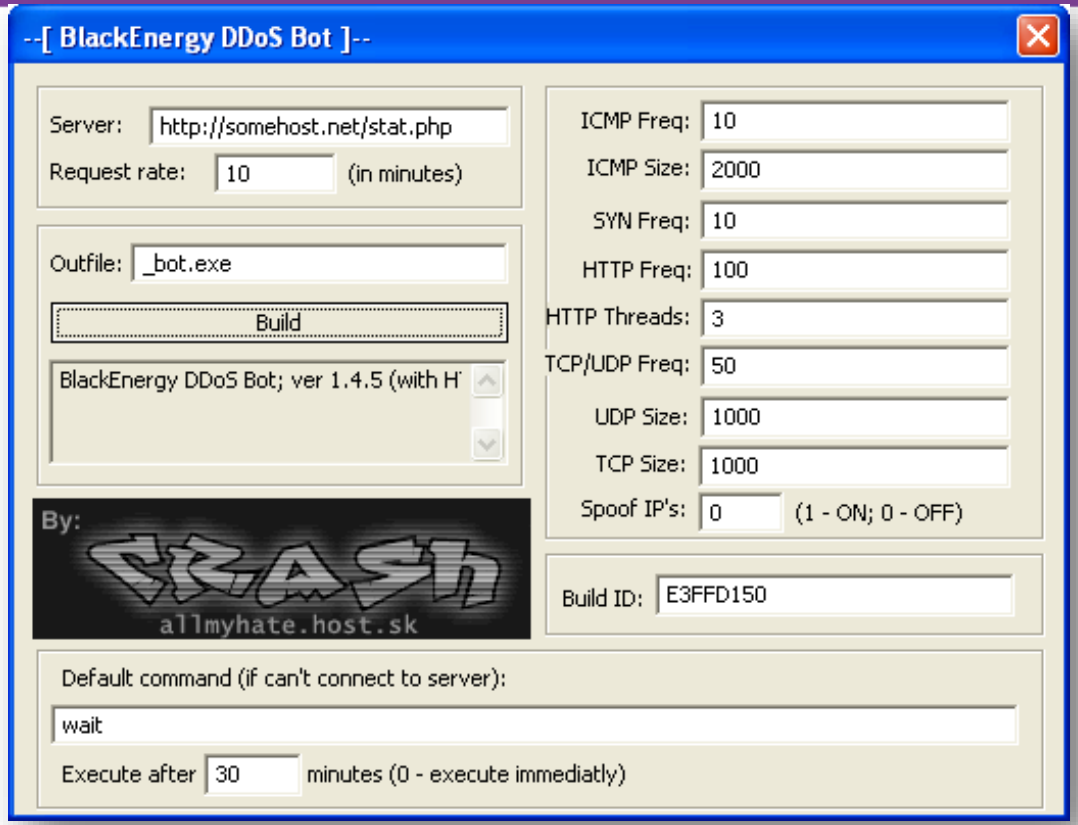
Problem of detection

Problem of detection

- Lack of or complete miss of network monitoring
- Lack of or complete miss of experience dealing with malware
  - “Computer virus” as ultimate reason for all issues or malfunction
  - It’s difficult to detect unknown malware without 3rd party experts
- It’s easier to reinstall then find out the reason of a problem
- SCADA Files don’t have digital signature

BlackEnergy 2

BlackEnergy 2



Evolution of BlackEnergy

- In 2013, BlackEnergy attackers began deploying SCADA-related plugins to victims in the ICS and energy sectors around the World
- In the past BlackEnergy, focusing on their destructive payloads, Siemens equipment exploitation and router attack plugins
- Since middle of 2014, one of the preferred attack vectors for BlackEnergy in Ukraine has been Excel documents with macros.
- Works on 32-bit and 64-bit systems without problems

Windows plugins

fs	File search, network and system
ps	Password collector (stealer)
ss	Screenshot maker
vsnet	Network spreading via RDP
rd	Remote desktop
scan	Port Scan
jn	File infector
cert	Digital certificate stealer
grc	Backup communication channel via plus.google.com
sn	Network traffic credential (login:password)extractor
usb	USB drives information collector
dstr	destroys hard disk by overwriting with random data

virustotal intelligence

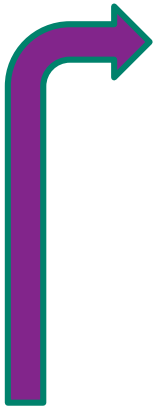
File information

Identification | Content | Analyses | Submissions | ITW | Additional | Comments

Date	File name	Source	Country
2013-11-24 20:57:38	vti-rescan	107b9a04 (community)	US
2013-11-21 18:09:20	Shale Gas.docx	5966c44c (community)	PL
2013-11-21 17:55:38	vti-rescan	107b9a04 (community)	US
2013-11-21 13:25:04	Shale Gas.docx	5966c44c (community)	PL
2013-11-20 15:56:26	vti-rescan	0fe95056 (community)	IN
2013-11-20 13:06:42	Shale_Gas.docx	89c9d99c (api)	PL
2013-11-20 13:01:42	Shale_Gas.docx	89c9d99c (api)	PL
2013-11-20 12:30:59	Shale Gas.docx	11fed007 (web)	PL

Download file | Re-scan file | Close

CnC Server



```
<plugins>
<plugin>
<name>plugin_win</name>
<version>3</version>
</plugin>
<plugin>
<name>plugin_mps</name>
<version>1</version>
</plugin>
</plugins>
```

routerpwn.com

2Wire	Comtrend	Netgear	TRENDnet
3Com	DD-Wrt	Pirelli	Ubee
Arris	D-Link	RuggedCom	Ubiquiti
Alcatel	EE	Sagem	UTStarcom
Lucent	EasyBox	Seagate	Xavi
Alpha	Fibrehome	Siemens	ZyXEL
Asmax	Freebox	Sitecom	ZTE
Asus	Huawei	SMC	Zoom
Belkin	MiFi	Thomson	
Cisco	Motorola	TP-Link	

How often do you update network routers' firmware?

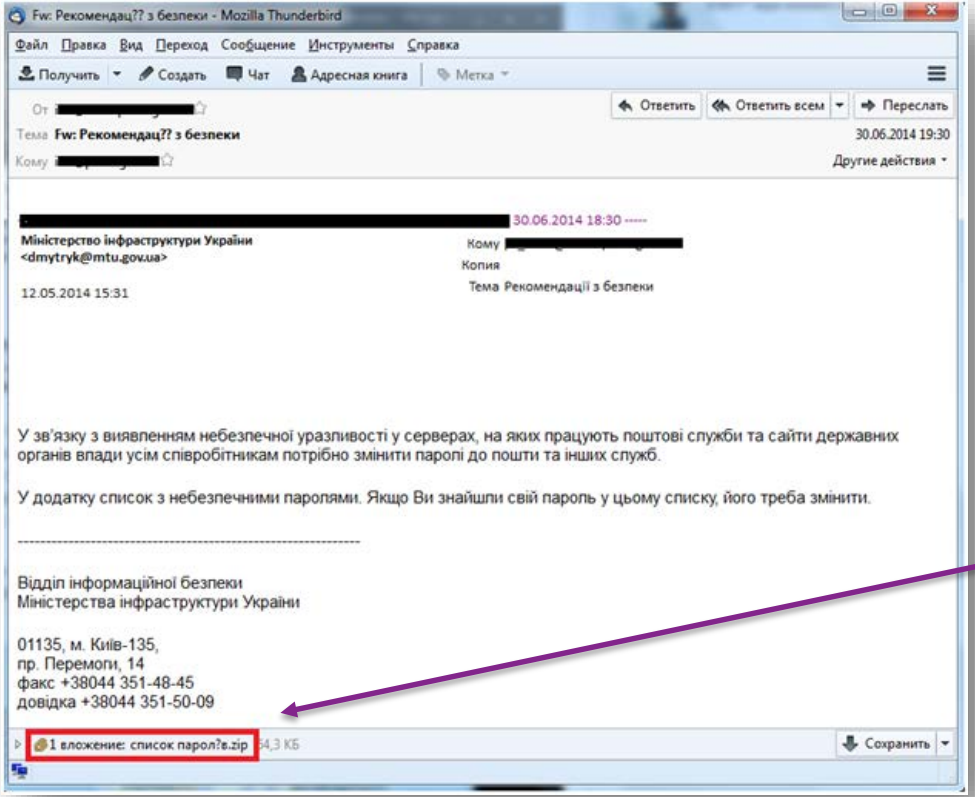
End point protection is not enough!

Attack on Ukrainian State Railway

- **May 2014:** massive spear-phishing attack hit Ukrainian State Railway
- Phishing email contained EXE file with MS Office Word icon
- Malware was detected in some organizations, but not everywhere
- This stage was intended to collect information about the infected orgs

Source: cys-centrum.com

2014 Spear-phishing email



Infected attachment contained zip archive with exe file inside

BlackEnergy on Ukraine in 2015

- **March 2015** – attack against Power Grid
  - BE attack Ukrainian Library system, some Power grid on West of the country
- **Oct 2015** – attack against UKR Election systems, TV and Media companies
  - Likely, the infection persisted on that systems from March 2015
  - Malware destroyed video project files, OS system files
- **23 Dec 2015** – massive attack against Ukrainian Power Grid
  - Thousands of power substations were shutdown for up to 8 hours on West and Central Ukraine. No SCADA until January 09 2016
  - TV and Media companies were also under heavy attacks

Source: cys-centrum.com

Dec 2015 attack to Ukrainian Power Grid

- BE2 used as penetration method to network using Sphere phishing via PE and PowerPoint exploit
- Hackers disabled operation remote control and switched power off
- Substation control was switched to manual for weeks.
- 80,000 consumers were w/o energy for at least 6 hours
- No SCADA control until January 9 2016 or even later

Source: cys-centrum.com

BlackEnergy on Ukraine in 2016

- **Jan 2016** – attack against Kiev airport (Borispol)
  - Few computers were infected. No further destructive actions were reported

- **19-20 Jan 2016** – new Spear-phishing attack against ~100 Energy sector organizations
  - email attachment contained infected Ocenka.XLS macros with root.exe
  - Gcat instead of BE, that is backdoor written on Python.

Source: cys-centrum.com

BlackEnergy on Ukraine in 2016

- Ja
- 10 phishing
  er rocess
- In Python. The
  re

УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025 - Mozilla Thunderbird

Get Messages | Write | Chat | Address Book | Tag

From Ukrenergo <info@ukrenergo.energy.gov.ua> | Reply | Reply All | Forward | More

Subject **УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025** 19.01.16 16:51

To [redacted]

Відповідно до положень Закону України «Про засади функціонування ринку електричної енергії України» та «Порядку підготовки Системним оператором плану розвитку Об'єднаної енергетичної системи України на наступні десять років», затвердженого наказом Міністерства енергетики та вугільної промисловості України від 29.09.2014 № 680, системним оператором було розроблено та розміщено на офіційному сайті компанії проект «Плану розвитку ОЕС України на 2016 – 2025 роки».

Проект Плану розвитку знаходиться в додатку до листа.

На виконання пункту 5 положення Порядку підготовки 20 січня 2016 року о 14-00 в адміністративному приміщенні ПС 750 кВ «Київська» (Київська область, Макарівський район, с. Наливайківка, вул. Жовтнева, 112-Б) будуть проводитись громадські обговорення та консультації щодо проекту Плану розвитку.

Державне підприємство
Національна енергетична компанія
УКРЕНЕРГО

1 attachment: Ocenka.xls 816 KB | Save

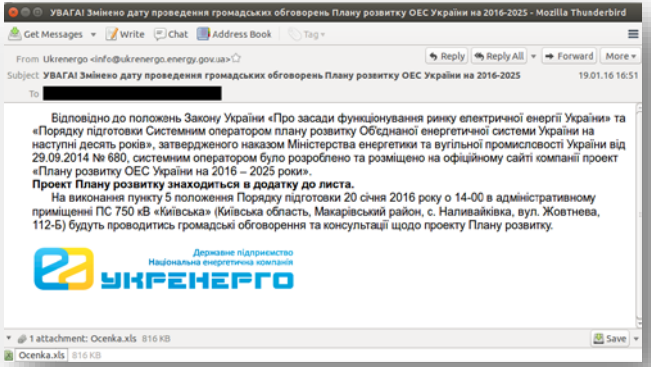
Ocenka.xls 816 KB

Infected attachment Ocenka.xls – infected XLS macros which downloads root.exe from CC server

Source: cys-centrum.com

BlackEnergy on Ukraine in 2016

- Jan 20: Infection getting deeper
- About 9 workers from 4 Energy organizations downloaded backdoor components to their infected systems


УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025 - Mozilla Thunderbird

Get Messages | Write | Chat | Address Book | Tag

From Ukrenergo <info@ukrenergo.energy.gov.ua>

Reply | Reply All | Forward | More

Subject УВАГА! Змінено дату проведення громадських обговорень Плану розвитку ОЕС України на 2016-2025 19.01.16 16:51

To [redacted]

Відповідно до положень Закону України «Про засади функціонування ринку електричної енергії України» та «Порядку підготовки Системним оператором плану розвитку Об'єднаної енергетичної системи України на наступні десять років», затвердженого наказом Міністерства енергетики та вугільної промисловості України від 29.09.2014 № 680, системним оператором було розроблено та розміщено на офіційному сайті компанії проект «Плану розвитку ОЕС України на 2016 – 2025 роки».

Проект Плану розвитку знаходиться в додатку до листа.

На виконання пункту 5 положення Порядку підготовки 20 січня 2016 року о 14-00 в адміністративному приміщенні ПС 750 кВ «Київська» (Київська область, Макарівський район, с. Наливайківка, вул. Жовтнева, 112-Б) будуть проводитись громадські обговорення та консультації щодо проекту Плану розвитку.

Державне підприємство
Національна енергетична компанія
УКРЕНЕРГО

1 attachment: Ocenka.xls 816 KB | Save

Ocenka.xls 816 KB

Source: cys-centrum.com

Other APT's victims

Equation (targeted world-wide)

- National nuclear centre
- Railways / metro development company
- Aerospace and automotive supplier
- National airport(s)
- Plasma research organisation
- National oil company
- National engineering & scientific commission
- National space agencies & centres
- Power Generation Transmission & Distribution Management Company

Other APT's victims

Desert Falcons (targeted middle east region)

- National smart grid provider

FlowerShop (targeted middle east region) (public report hasn't published yet)

- Power distribution company
- Power plant Company
- National Disaster Mitigation Management Org

Duqu 2.0

Costin Raiu @craiu · Jun 11

Do you recognize these filenames and paths targeted by one of the cryptic #Duqu2 modules? Let us know.

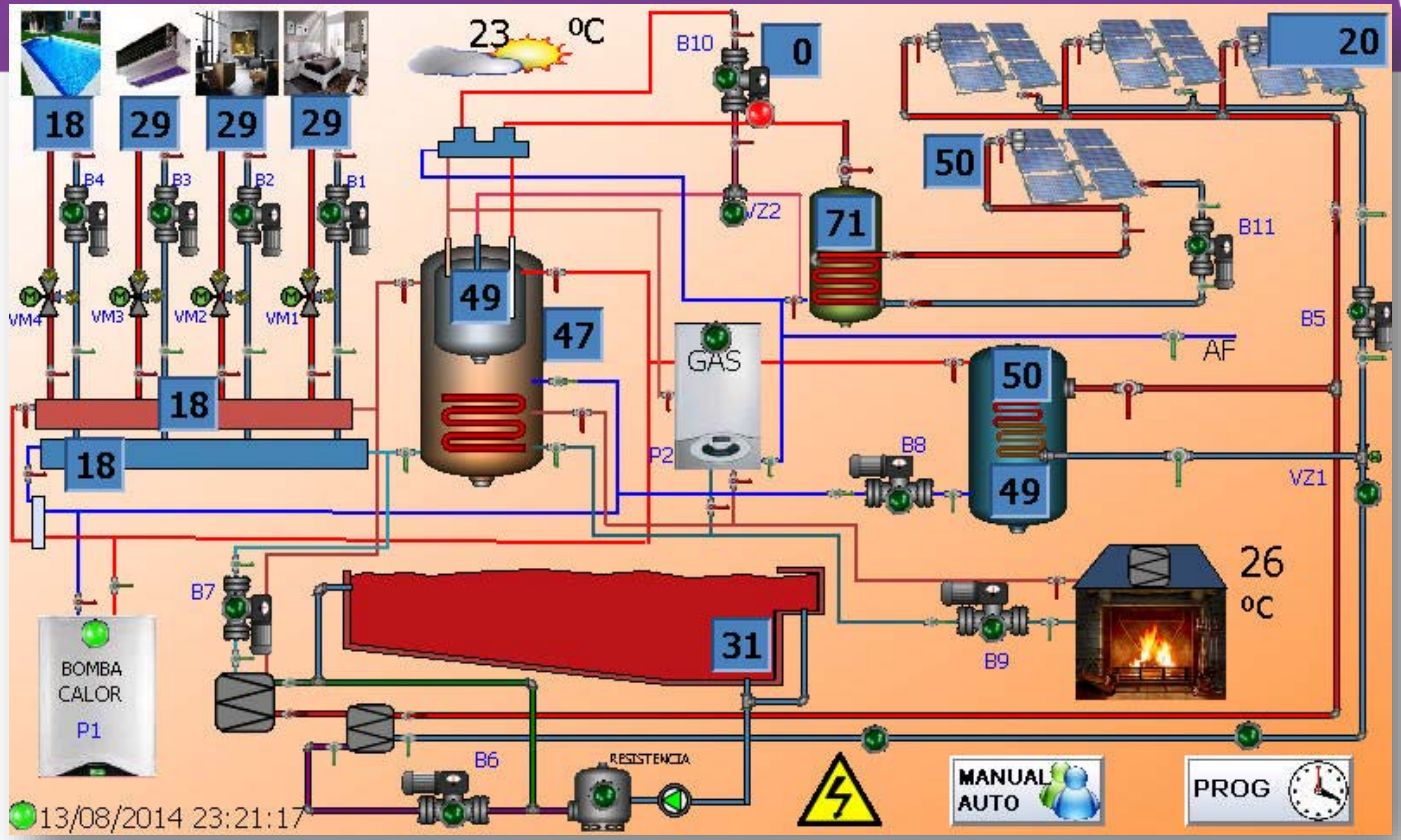
```
3E908: 4C A9 01 80 01 00 00 00  B0 69 00 80 01 00 00 00  L-ØÇØ   ▒i ÇØ
3E918: C0 A9 01 80 01 00 00 00  74 AA 01 80 01 00 00 00  └-ØÇØ   t¬ØÇØ
3E928: 00 00 00 00 00 00 00 00  68 00 6D 00 6C 00 00 00          h m l
3E938: 64 00 61 00 74 00 61 00  2E 00 68 00 6D 00 69 00  d a t a . h m i
3E948: 00 00 00 00 00 00 00 00  76 00 61 00 6C 00 2E 00          v a l .
3E958: 64 00 61 00 74 00 00 00  2F 00 49 00 6E 00 74 00  d a t   / I n t
3E968: 2F 00 48 00 4D 00 49 00  2F 00 00 00 C0 27 09 00  / H M I /   └'○
3E978: 2F 00 4C 00 47 00 2F 00  48 00 4D 00 2F 00 00 00  / L G / H M /
3E988: 00 80 3E D5 DE B1 9D 01  01 00 00 00 00 00 00 00  Ç>╒▐▒¥ØØ
3E998: C0 2F 04 80 01 00 00 00  00 00 00 00 00 00 00 00  └/♦ÇØ
3E9A8: 18 9E 02 80 01 00 00 00  04 00 04 00 08 00 04 00  ↑₧☻ÇØ   ♦ ♦ ◘ ♦
```

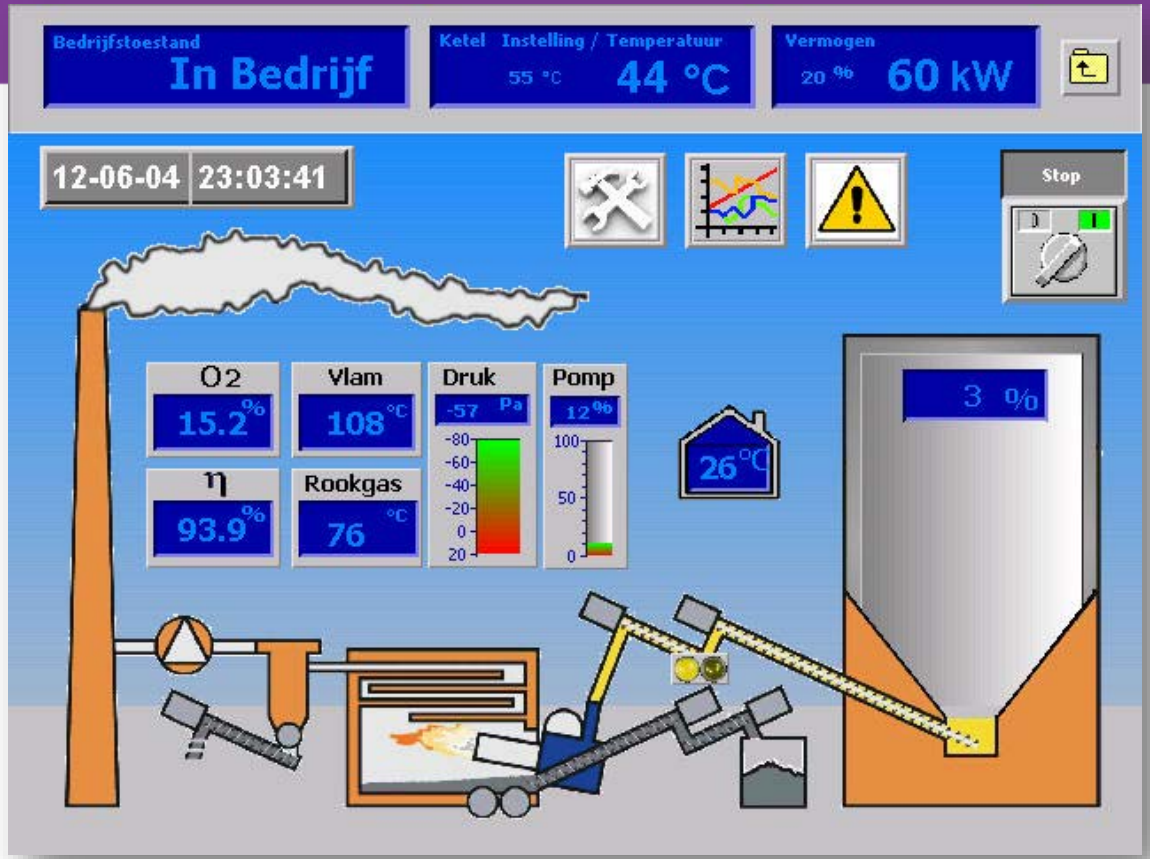
US public utility company case

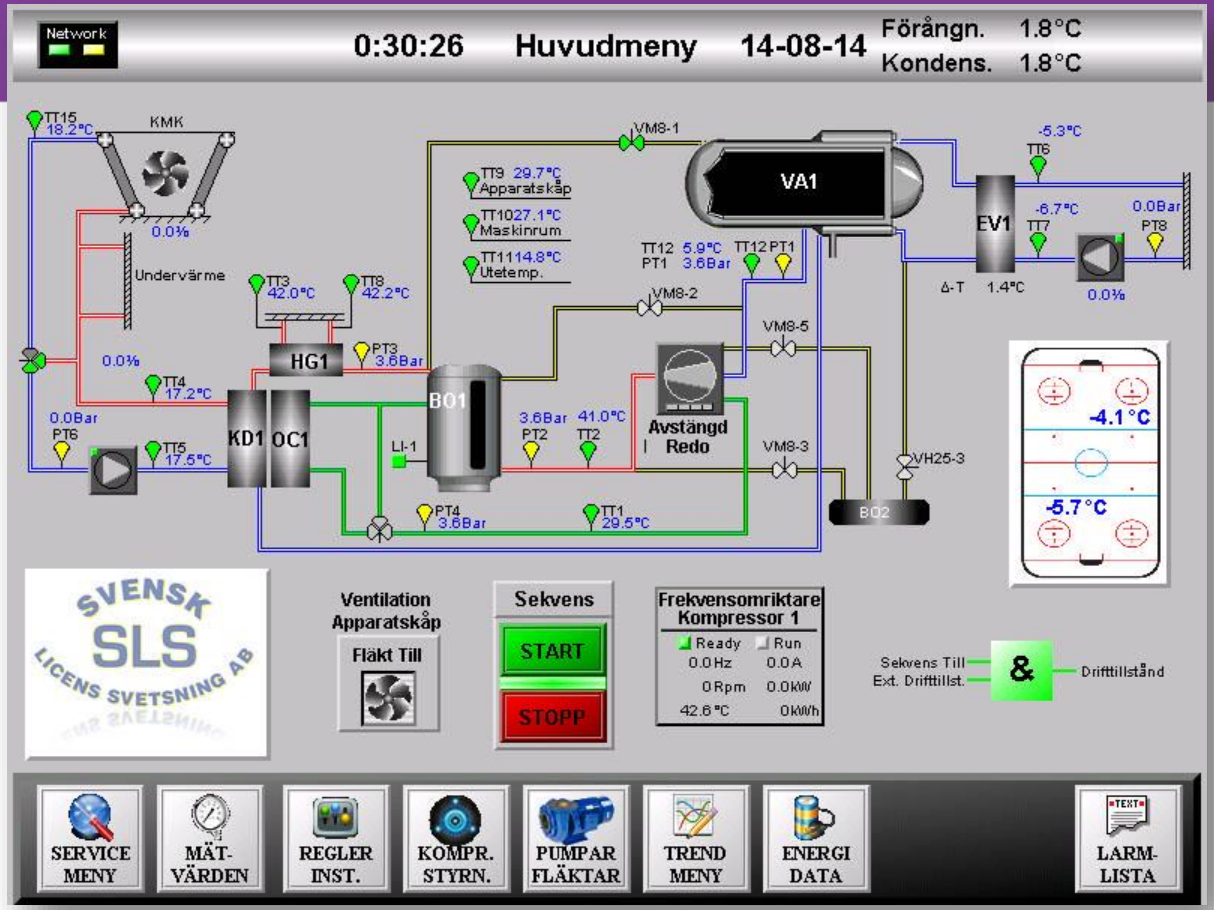
US public utility company case

US ICS-CERT Monitor Q1 2014:

- A major US public utility was compromised by a brute-force attack that managed to bypass security settings and infiltrate systems.
- software used to administer the control system assets was accessible via internet-facing hosts.
- The systems were configured with a remote access capability, utilising a simple password mechanism; however, the authentication method was susceptible to compromise via standard brute-force techniques.

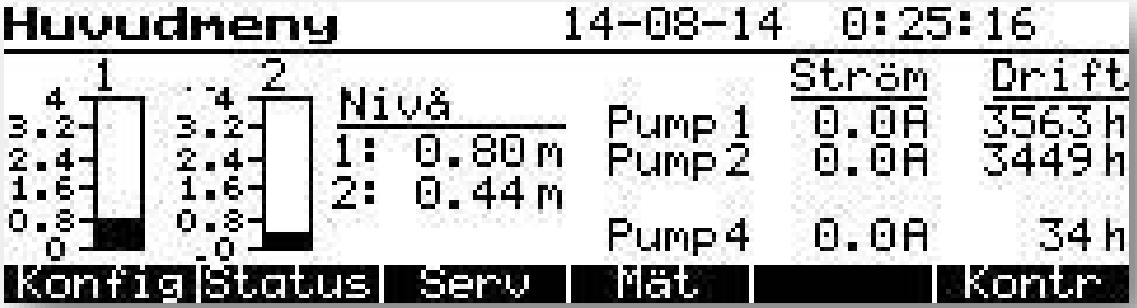

23 ºC
B10
0
20
18
29
29
29
B4
B3
B2
B1
VZ2
71
50
B11
VM4
VM3
VM2
VM1
49
47
GAS
B5
AF
50
18
18
P2
B8
49
VZ1
26
ºC
B7
31
B9
BOMBA
CALOR
P1
B6
RESISTENCIA
MANUAL
AUTO
PROG
13/08/2014 23:21:17


Bedrijfstoestand
In Bedrijf
Ketel Instelling / Temperatuur
55 °C
44 °C
Vermogen
20 %
60 kW
12-06-04
23:03:41
Stop
O2
15.2 %
Vlam
108 °C
Druk
-57 Pa
-80
-60
-40
-20
0
20
Pomp
12 %
100
50
0
η
93.9 %
Rookgas
76 °C
26 °C
3 %


Network
0:30:26
Huvudmeny
14-08-14
Förångn. 1.8°C
Kondens. 1.8°C
TT15 18.2°C
KMK
0.0%
Undervärme
TT3 42.0°C
TT8 42.2°C
HG1
PT3 3.6Bar
0.0%
TT4 17.2°C
0.0Bar PT6
TT5 17.5°C
KD1
OC1
LI-1
BO1
PT4 3.6Bar
TT1 29.5°C
TT9 29.7°C Apparatskåp
TT10 27.1°C Maskinrum
TT11 14.8°C Utetemp.
VM8-1
VA1
TT12 5.9°C
PT1 3.6Bar
TT12 PT1
VM8-2
VM8-5
3.6Bar PT2
41.0°C TT2
Avstängd Redo
VM8-3
VH25-3
BO2
-5.3°C TT6
EV1
-6.7°C TT7
0.0Bar PT8
Δ-T 1.4°C
0.0%
-4.1°C
-5.7°C
SVENSK SLS LICENS SVETSNING AB
Ventilation Apparatskåp
Fläkt Till
Sekvens
START
STOPP
Frekvensomriktare Kompressor 1
Ready
Run
0.0Hz 0.0A
0Rpm 0.0kW
42.6°C 0kW/h
Sekvens Till
Ext. Drifttillst.
&
Drifttillstånd
SERVICE MENY
MÄT-VÄRDEN
REGLER INST.
KOMPR. STYRN.
PUMPAR FLÄKTAR
TREND MENY
ENERGI DATA
LARM-LISTA

Windows XP


Microsoft
Windows NT
Server 4.0
Terminal Server Edition
© 1981 - 1998 Microsoft Corp. All rights reserved.
This product is protected by US and
international copyright laws as appropriate.
Press Ctrl + Alt + Delete to begin.
Microsoft
Windows NT
Server 4.0
Terminal Server Edition


Huvudmeny
14-08-14 0:25:16
1
2
4
3.2
2.4
1.6
0.8
0
Nivå
1: 0.80 m
2: 0.44 m
Ström
Drift
Pump 1 0.0A 3563 h
Pump 2 0.0A 3449 h
Pump 4 0.0A 34 h
Konfig
Status
Serv
Mät
Kontr

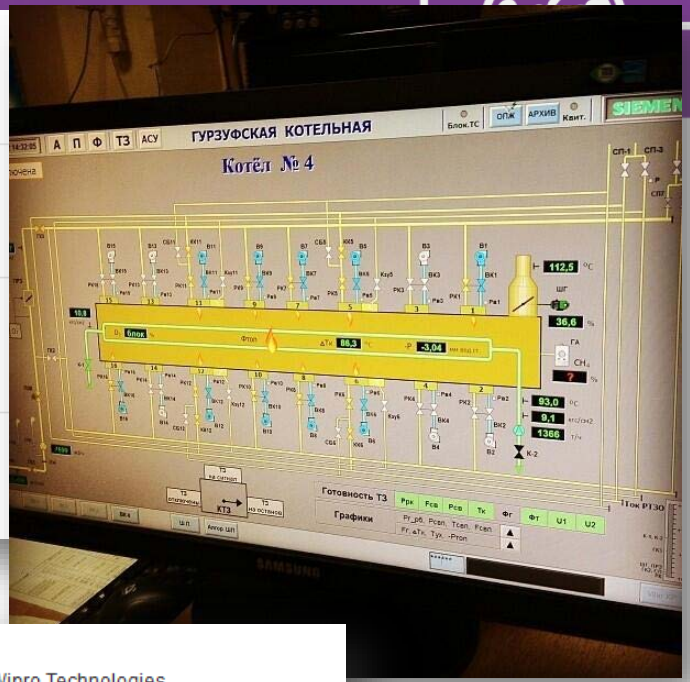
Social Networks

[redacted] C. 3rd
Asset Integration Engineer at Thames Water
London, United Kingdom • Utilities
Similar

[redacted] H. 3rd
Project Engineer at Thames Water
Rochester, United Kingdom • Utilities
Similar

[redacted] G. 3rd
SCADA Systems Support Engineer at Thames Water
London, United Kingdom • Utilities
Similar

[redacted] W. 3rd
ICA Systems Engineer at Thames Water
Twickenham, United Kingdom • Utilities
Similar



[redacted] K. 3rd
Senior Software Engineer at Wipro Technologies
Leicester, United Kingdom • Information Technology and Services
Similar
Current: Domain Consultant-SCADA at **National Grid**

[redacted] Bull 2nd
Smart **Grid** Program Director at **National Grid**
Greater Boston Area • Utilities
1 shared connection • Similar

Case. Hack of an Oil company in middle east

- Fact:
  - Industrial network Infiltration
- How:
  - Social Engineering, malware and compromise of Night shift engineer's PC
- Consequences:
  - 3 days of delay

Case. Hack of an Oil company in middle east

- A

Night shift operator was found in Facebook by hacker

Hacker has created a friendship with the operator

Hacker was finding operators' personal data and facts from his life

Hacker sent a URL directed to a malware (using social engineering)

Operator clicked it and got infected

Hacker downloaded SAM database and got a password from engineering PC

Hacker modified SCADA project

Remotely located plant/rig lost its ability to be controlled remotely

Delay in production for 3 days

Summary

- There are more cyber incidents then we aware of (or even think)
- Almost all APTs know and able to work on industrial objects
- Most developed APTs are able to jump over air gap (Turla, MiniDuke, RedOctober, Fanny…)
- End point protection is not enough! (but it has to be in place)

RSA Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-W09

ICS Threats. A Kaspersky Lab view, predictions and reality

Andrey Nikishin

Special Projects Director
Kaspersky Lab
@andreynikishin

#RSAC