ICS Threats.
A Kaspersky Lab view, predictions and reality
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 worldwide
- 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
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
Luigi Auriemma
me@aluigi.org

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
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

- [ BlackEnergy DDoS Bot ]-

Server: `http://somehost.net/stat.php`
Request rate: 10 (in minutes)

Outfile: `_bot.exe`

ICMP Freq: 10
ICMP Size: 2000
SYN Freq: 10
HTTP Freq: 100
HTTP Threads: 3
TCP/UDP Freq: 50
UDP Size: 1000
TCP Size: 1000
Spoof IP's: 0 (1 - ON; 0 - OFF)

Build ID: E3FFD150

Default command (if can't connect to server):
`wait`
Execute after 30 minutes (0 - execute immediately)
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

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs</td>
<td>File search, network and system</td>
</tr>
<tr>
<td>ps</td>
<td>Password collector (stealer)</td>
</tr>
<tr>
<td>ss</td>
<td>Screenshot maker</td>
</tr>
<tr>
<td>vsnet</td>
<td>Network spreading via RDP</td>
</tr>
<tr>
<td>rd</td>
<td>Remote desktop</td>
</tr>
<tr>
<td>scan</td>
<td>Port Scan</td>
</tr>
<tr>
<td>jn</td>
<td>File infector</td>
</tr>
<tr>
<td>cert</td>
<td>Digital certificate stealer</td>
</tr>
<tr>
<td>grc</td>
<td>Backup communication channel via plus.google.com</td>
</tr>
<tr>
<td>sn</td>
<td>Network traffic credential (login:password) extractor</td>
</tr>
<tr>
<td>usb</td>
<td>USB drives information collector</td>
</tr>
<tr>
<td>dstr</td>
<td>Destroys hard disk by overwriting with random data</td>
</tr>
<tr>
<td>Date</td>
<td>File name</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------</td>
</tr>
<tr>
<td>2013-11-24 20:57:38</td>
<td>vti-rescan</td>
</tr>
<tr>
<td>2013-11-21 18:09:20</td>
<td>Shale Gas.docx</td>
</tr>
<tr>
<td>2013-11-21 17:55:38</td>
<td>vti-rescan</td>
</tr>
<tr>
<td>2013-11-21 13:25:04</td>
<td>Shale Gas.docx</td>
</tr>
<tr>
<td>2013-11-20 15:56:26</td>
<td>vti-rescan</td>
</tr>
<tr>
<td>2013-11-20 13:06:42</td>
<td>Shale_Gas.docx</td>
</tr>
<tr>
<td>2013-11-20 13:01:42</td>
<td>Shale_Gas.docx</td>
</tr>
<tr>
<td>2013-11-20 12:30:59</td>
<td>Shale Gas.docx</td>
</tr>
</tbody>
</table>
<plugins>
<plugin>
<name>plugin_win</name>
<version>3</version>
</plugin>
<plugin>
<name>plugin_mps</name>
<version>1</version>
</plugin>
</plugins>
How often do you update network routers' firmware?
End point protection is not enough!
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

- **Jan 19:** Continues attacks to Power Grid
- 100 of energy sector organizations received spear-phishing email. Email text says UKRENERGO requires new process
- Infected attachment included backdoor written on Python. The 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

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
Do you recognize these filenames and paths targeted by one of the cryptic #Duqu2 modules? Let us know.
US public utility company case
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.
Windows XP
Social Networks
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

- 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 downloaded SAM database and got a password from engineering PC
- Operator clicked it and got infected
- Hacker sent a URL directed to a malware (using social engineering)
- 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 than we are aware of (or even think)
- Almost all APTs know and are 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)
SESSION ID: SBX1-W09

ICS Threats.
A Kaspersky Lab view, predictions and reality

Andrey Nikishin
Special Projects Director
Kaspersky Lab
@andreynikishin