

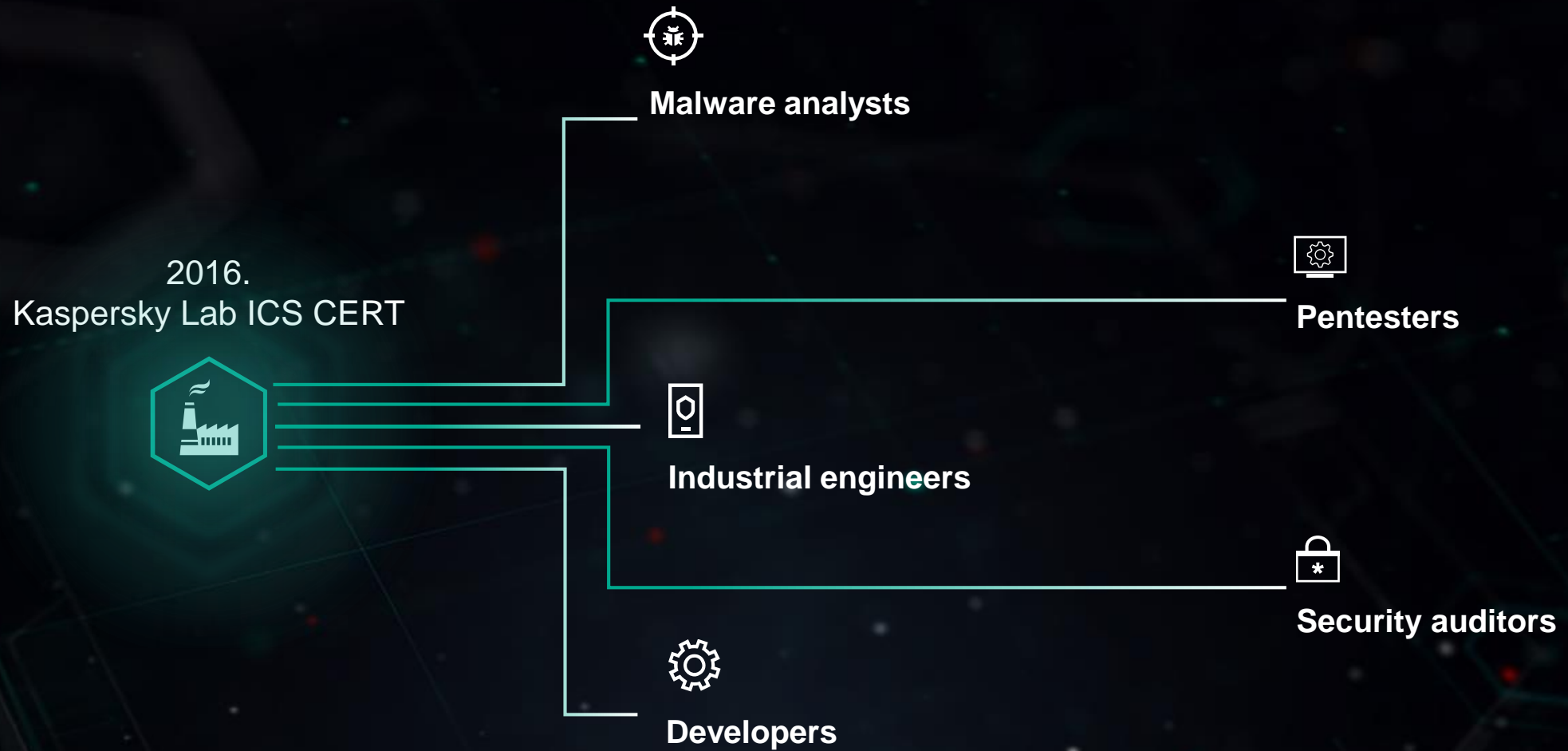
Industrial cyberthreats and mitigation measures



Maria Garnaeva

Senior Security Researcher, Kaspersky Lab ICS CERT

KL ICS CERT structure



Motives

Motive #1 – disruption/destruction

STUXNET



BLACKENERGY2



INDUSTROYER/CRASHOVERRIDE

TRITON

Motive #2 – intelligence gathering

ENERGETIC BEAR



Motive #3 - Money



Your personal files are encrypted!



Your private key will be destroyed on:
2/29/2015

Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key**.

The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...

In order to decrypt the files open your personal page on site <https://34r6hq26q2h4jkzj.tor2web.fi> and follow the instruction.

Use your Bitcoin address to enter the site:
~~34r6hq26q2h4jkzj.onion~~

Click to copy Bitcoin address to clipboard

if <https://34r6hq26q2h4jkzj.tor2web.org> is not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After installation, run the browser and enter address **34r6hq26q2h4jkzj.onion**

Motive #3 - Money

Re: New Order P08112016 - URGENT - Daily

From Kiril Georgiev <Kiril.Georgiev@...>
Subject **Re: New Order P08112016 - URGENT**
To info@...
Greetings Sir,
Hope you are fine.
Please find enclosed our new order P08112016 for your kind attention and prompt execution.
I look forward to receiving your order acknowledgement in due time.
Best regards,
Kiril Georgiev
Business Development Manager
Payment Division
... Eastern Europe
13B Tintyava Str., entr.1
1113 Sofia, Bulgaria
Ph. +359 2 86 86 896
Fax: + 359 2 86 81 475
Mobile: +359 884 466 040
Kiril.Georgiev@...
This communication is for informational purposes only. All market prices, data and change without notice. Present message and any attached files may be or contain information that is privileged, confidential, legally in this message is solely intended for the physical or legal person to whom it is addressed. If you are not the intended recipient, please notify the sender immediately. If you have received this message in error, please delete the message and destroy all copies. Thank you.

Mozilla Thunderbird

From Larry N. Ralls Aramco <larry.ralls@aramco.com>
Subject **FINAL REMINDER!! TOP URGENT Saudi Arabian Oil Company : Request for quotation**
To ...
Cc Ahmed-arafth@aramco.com, MMaramco@aramco.com
Dear Sir,
Please be advised that you are invited to quote for the attached items and requires an urgent attention. Sealed bids are due by February 4th. You can submit this either through email or through sealed envelopes.
If you require a gate pass, please fill out the attached file and return it. Specifications are attached.
SPECIAL INSTRUCTIONS TWO-STEP TECHNICAL/COMMERCIAL BID
Vendor shall submit separate technical (original) and commercial (original) sealed envelopes or through email. The technical bid shall not contain:
- Non Commercial bid, and
- Commercial bid/two-step bid procedure/do not open
--
Regards,
Larry Ralls, CPSM, SCMP | Saudi Arabian Oil Company | Projects Procurement
Process Control System Unit | P: 966-013-874-1508 | F: 966-013-874-1508
larry.ralls@aramco.com
2 attachments 141 KB
Gate Pass.doc 71,0 KB Saudi Aramco#no.7202159560.doc 70 KB

Mozilla Thunderbird

From Arun Ali <...>
Subject **Re: OUR MAY ORDER**
Reply to ...
18.05.2017 15:24
Hello,
We have emailed your company twice and the email keep on returning back. Our company will be interested in your products and we have not heard from your company from our previous email. I hope all is well with you.
Please quote your best prices on FOB as attached on the two order as we propose MAY for this order. Please kindly send us your catalog.
Best Regards,
Steve Kane
Sales & Marketing Manager
Kurt Industrial
An Employee Owned Company
9445 East River Road NW
Minneapolis, MN 55433
Direct Phone: 763.572.4631
Fax: 763.574.8313
Cell: 612.801.8193
Skype: ...
This email is intended for the use of the addressee(s) only and may contain privileged, confidential, or proprietary information that is exempt from disclosure under law. Please do not read, copy, use, or disclose the contents of this communication if you are not the intended recipient. Please notify the sender if you have received this email in error. Please delete the email and destroy all copies. Thank you
Attachment
PURCHASE ORDER.exe 710 KB

BUSINESS EMAIL COMPROMISE



Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages Write Chat Address Book Tag

From Hardik Ray | [REDACTED] Steel <ray@[REDACTED]steel.com> ☆ ↻

Subject Re: Banking information

To t.lockhart@[REDACTED].com ☆

Cc Amrin Pathan | [REDACTED] Steel <amrin@[REDACTED]steel.com> ☆, 'Sanjay Pangam | [REDACTED] Steel' <sanjay@[REDACTED]steel.com> ☆, 1 more

Dear Tom

Good day.

Regarding my last email on banking dated 4/30/2015 henceforth disregards any payment to our previous bank account because All our payments should be made to our subsidiary Sister's account in Hong kong as stated below .we are waiting the evidence of the payment

BANK INSTRUCTION:

BANK NAME: HSBC HONG KONG

BANK ADDRESS:1 GARDEN ROAD CENTRAL,HONG KONG

BENEFICIARY NAME:WELL GRACE TRADING LIMITED

BENEFICIARY ADDRESS:22-23 WANCHAI ROAD 15/F CENTRAL HONG KONG

ACCOUNT NUMBER:112511092838

SWIFT CODE: HSBCHKHCHK

Your quick reply is highly appreciated

Thanks and best regards!

Hardik Ray
Marketing Officer
Tel. No.: + [REDACTED]

[REDACTED] Steel & Alloys Pvt. Ltd.
[REDACTED]

spoofed emails

Motive #4 – No motive, but big problems

Unpredictable collateral damage: DoS by Wannacry



+



=



Ransomware nightmare



WANNACRY

13.4% of all computers in industrial infrastructure attacked

The most affected organizations included healthcare institutions and government sector

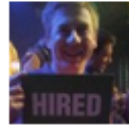


EXPETR

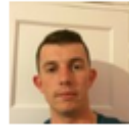
at least 50% of the companies from manufacturing, and Oil&Gas industries attacked

Attack vectors

- A human factor - targeted attack (spear phishing emails, waterhole sites, social engineering, etc)



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



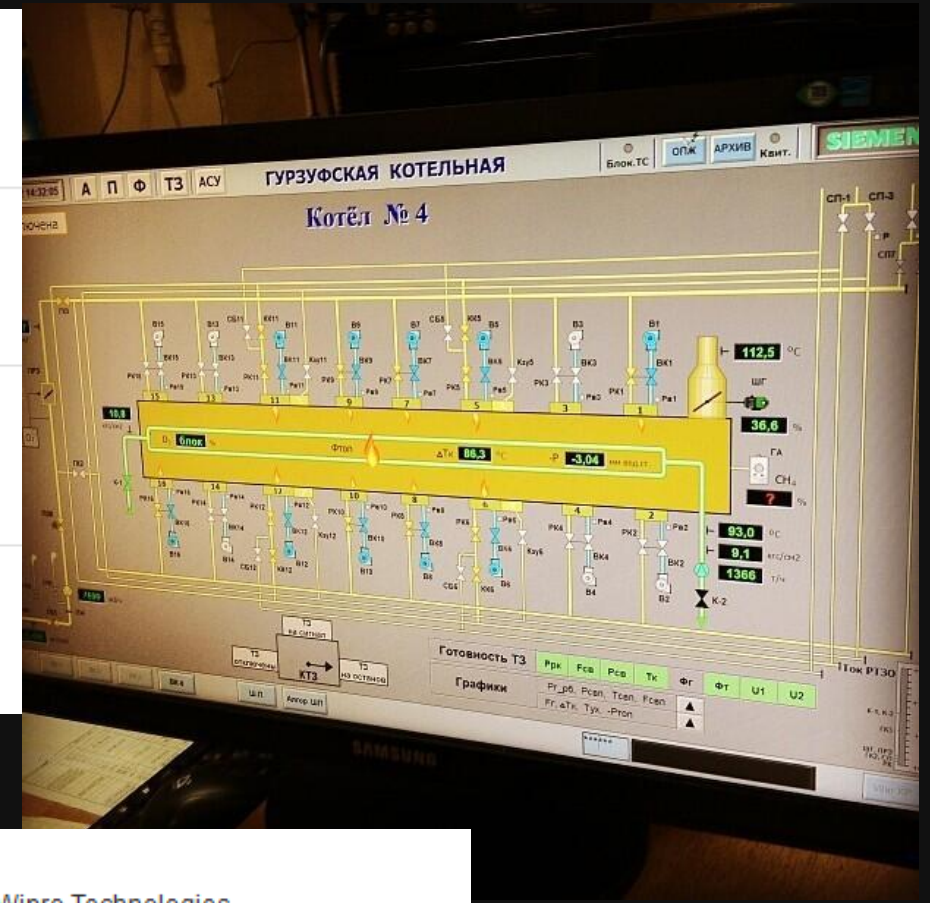
H. 3rd
 Project Engineer at Thames Water
 Rochester, United Kingdom • Utilities
[Similar](#)



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



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



K. 3rd
 Senior Software Engineer at Wipro Technologies
 Leicester, United Kingdom • Information Technology and Services
[Similar](#)

Current: Domain Consultant-SCADA at National Grid



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



Attack vectors

- A human factor - targeted attack (spear phishing emails, waterhole sites, social engineering, etc)
- Vulnerable software (SCADA, OS, 3rd-party)



BlackEnergy Attack on SCADA

- Specially prepared scripts for SCADA
- Example for General Electric **CIMPLICITY**

- Exploitation of CVE-2014-0751 vuln

(Directory traversal vulnerability in CimWebServer.exe allows remote attackers to execute arbitrary code via a crafted message to TCP port 10212)

- Scripts were launched automatically
- Downloaded “CimCMSafegs.exe” installer from a remote server
- Copied it to “Cimplicity” directory and executed it
- Installer self-deleted after installation complete

Attack vectors

- A human factor - targeted attack (spear phishing emails, waterhole sites, social engineering, etc)
- Vulnerable software (SCADA, OS, 3rd-party)
- ERP/MES & Internet connections

Direct connection fail

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**.

Attack vectors

- A human factor – targeted attack (spear phishing emails, waterhole sites, social engineering, etc)
- Vulnerable software (SCADA, OS, 3rd-party)
- ERP/MES & Internet connections
- Uncontrolled software usage
- Uncontrolled external devices (USB, SATA, etc.)
- 3rd parties and contractors
- Supply chain

Scenario – SUPPLY CHAIN

Energetic Bear actor:

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

Scenario – SUPPLY CHAIN



EXPETR

At least 50% of the companies attacked were from manufacturing, and Oil & Gas industries attacked



Why do you want to defend yourself?





1. Reconnaissance

- OSINT
- Public available sources

2. Weaponization

- Spear-phishing emails
- Waterhole sites
- Credentials theft
-

3. Installation/Lateral movement

- Various malicious or even legal tools
- Phishing emails from inside

4. Command and Control

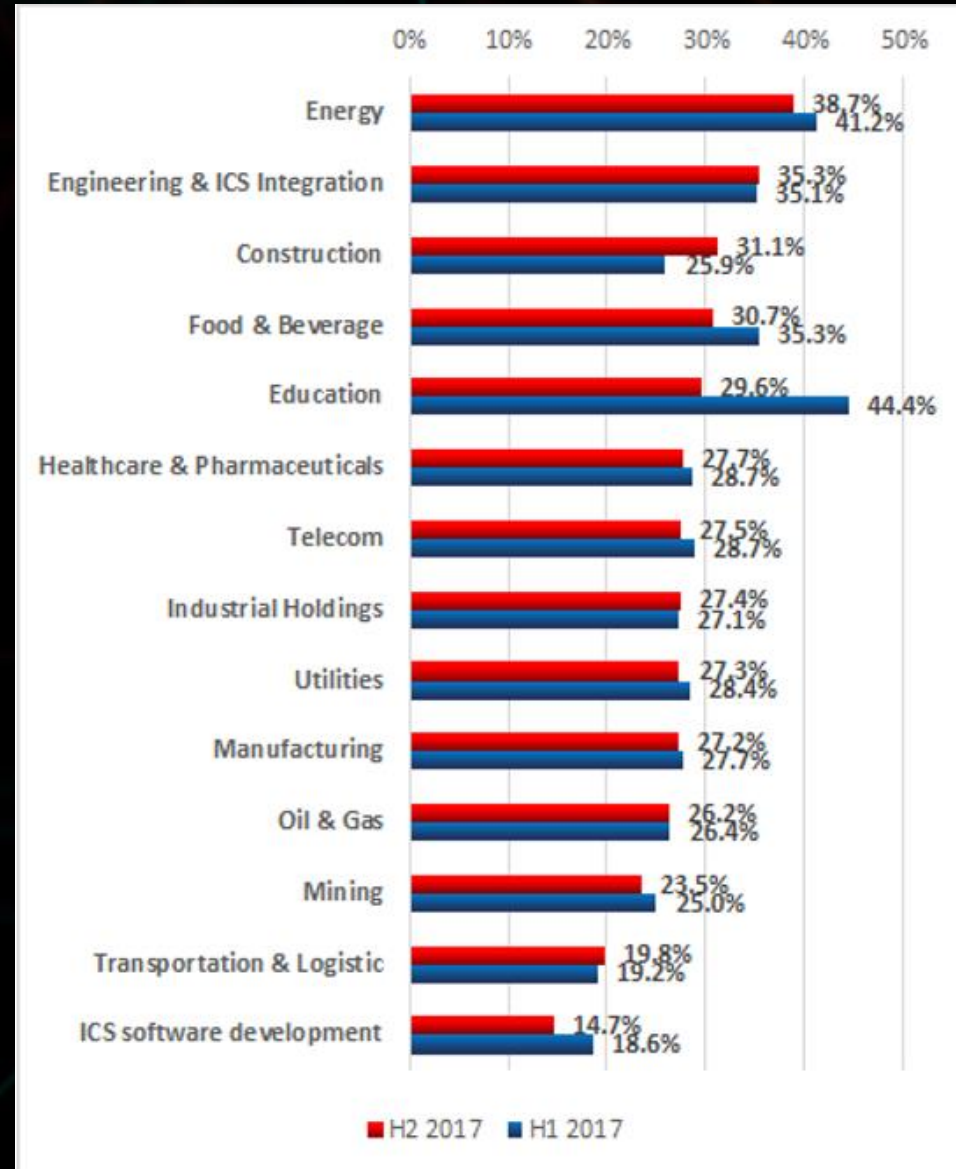
- Communication with the actor's server

5. Action

- Stealing docs
- Making changes In the configuration
- Uploading a Program to the controller

Industry statistics

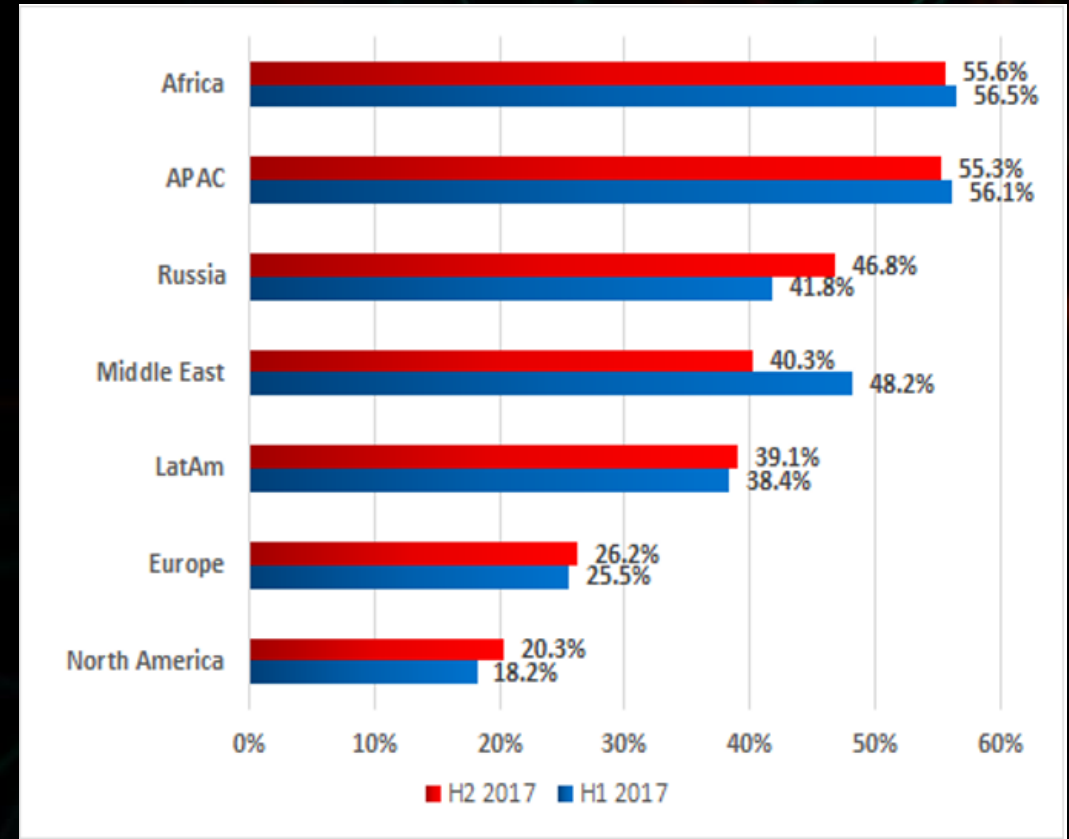
- At least every 3rd ICS computer in Energy sector was attacked in 2017



Europe Stats

Portugal	47,89%
Ukraine	45,47%
Belarus	44,25%
Poland	41,17%
Hungary	37,35%
Italy	35,16%
Spain	34,07%
Romania	30,51%
Slovakia	30,31%
France	26,85%
Germany	25,66%
United Kingdom	22,49%
Austria	22,40%
Belgium	21,51%
Czechia	20,94%
Ireland	20,93%
Switzerland	19,81%
Denmark	17,68%
Netherlands	17,59%
Sweden	17,20%

% attacked ICS (2017)



Risks, Malware & Attacks

LEVEL 3

- > Manufacturing Operations management



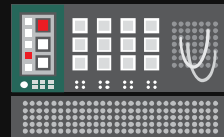
- > Malware via USB, Network, Corporate network, email, Web
- > Human actions (intention or not) (insiders, contractors)
- > Internet attacks (hackers, radicals, hacktivists, etc)

LEVEL 2, 1

- > SCADA
- > HMI
- > Engineering Wks
- > PLC, TRU
- > etc



- > Malware via USB, Network, Contractors
- > Human actions (insiders, contractors)
- > Internet attacks



- > Malware via Industrial network
- > Human actions

LEVEL 0

- > Physical



- > Human

Mandatory measures

- Endpoint Security
- Email Security
- Firewall/IDS
- Awareness & Education
- Privilege & Account Management
- Patches
- Proper configuration
- Whitelisting

Going extra mile

- Network Segmentation & Remote Access management
- ICS Network Monitoring
- Incident Response Team
- Security Testing and Audit

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
- End point protection is not enough!
- Industrial Cyber Security is not like Office Cyber Security
- It requires specific approach, products and services
- Cyber security is not a project, it is a process



Let's talk!

Maria Garnaeva

Maria.Garnaeva@Kaspersky.com

ics-cert.kaspersky.ru
www.kaspersky.com

KASPERSKY 