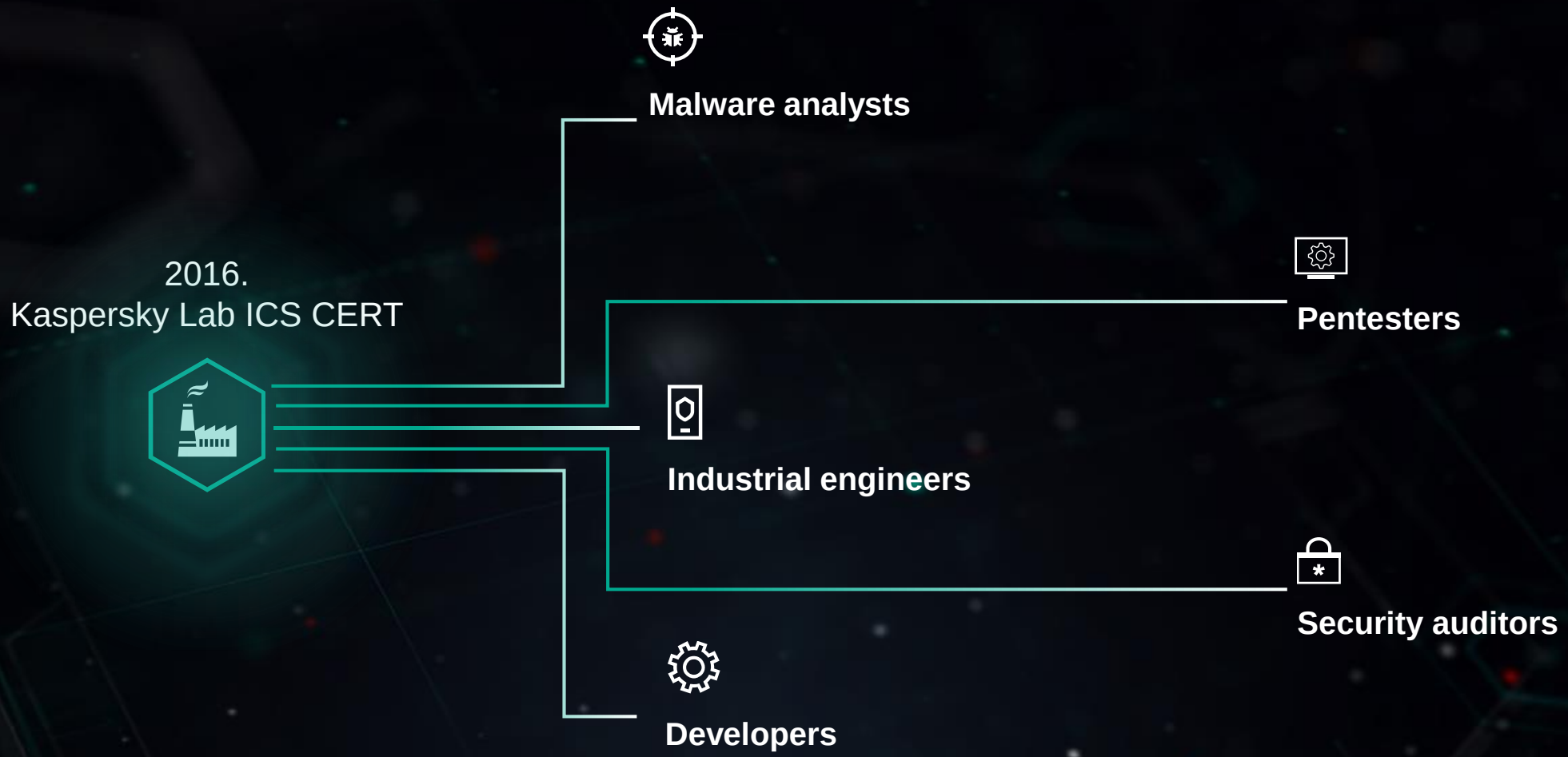
Industrial cyberthreats and mitigation measures

Maria Garnaeva

Senior Security Researcher, Kaspersky Lab ICS CERT

KL ICS CERT structure



Motives

Motive #1 – disruption/destruction

STUXNET

BLACKENERGY2

INDUSTROYER/CRASHOVERRIDE

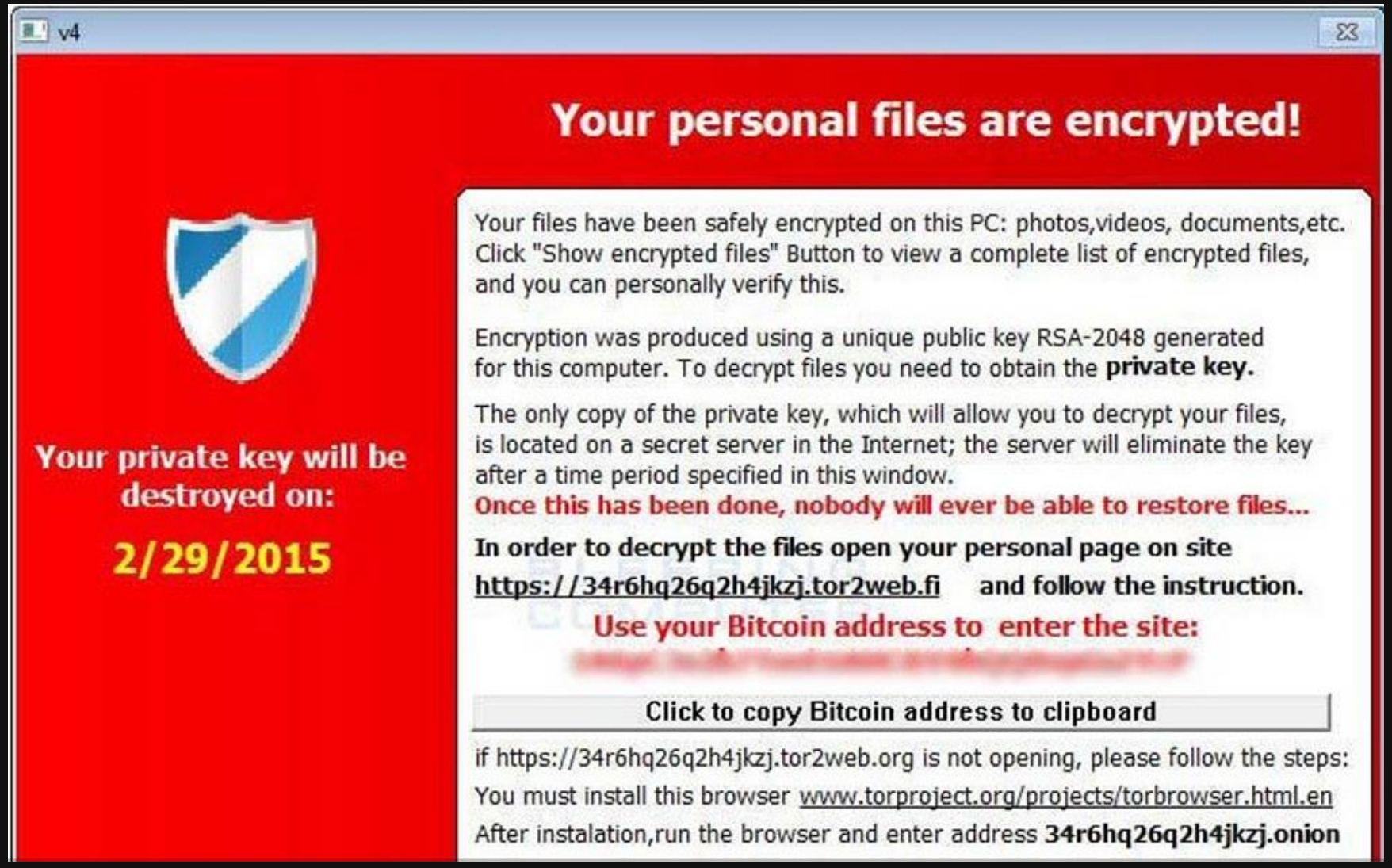
TRITON

Motive #2 – intelligence gathering

ENERGETIC BEAR

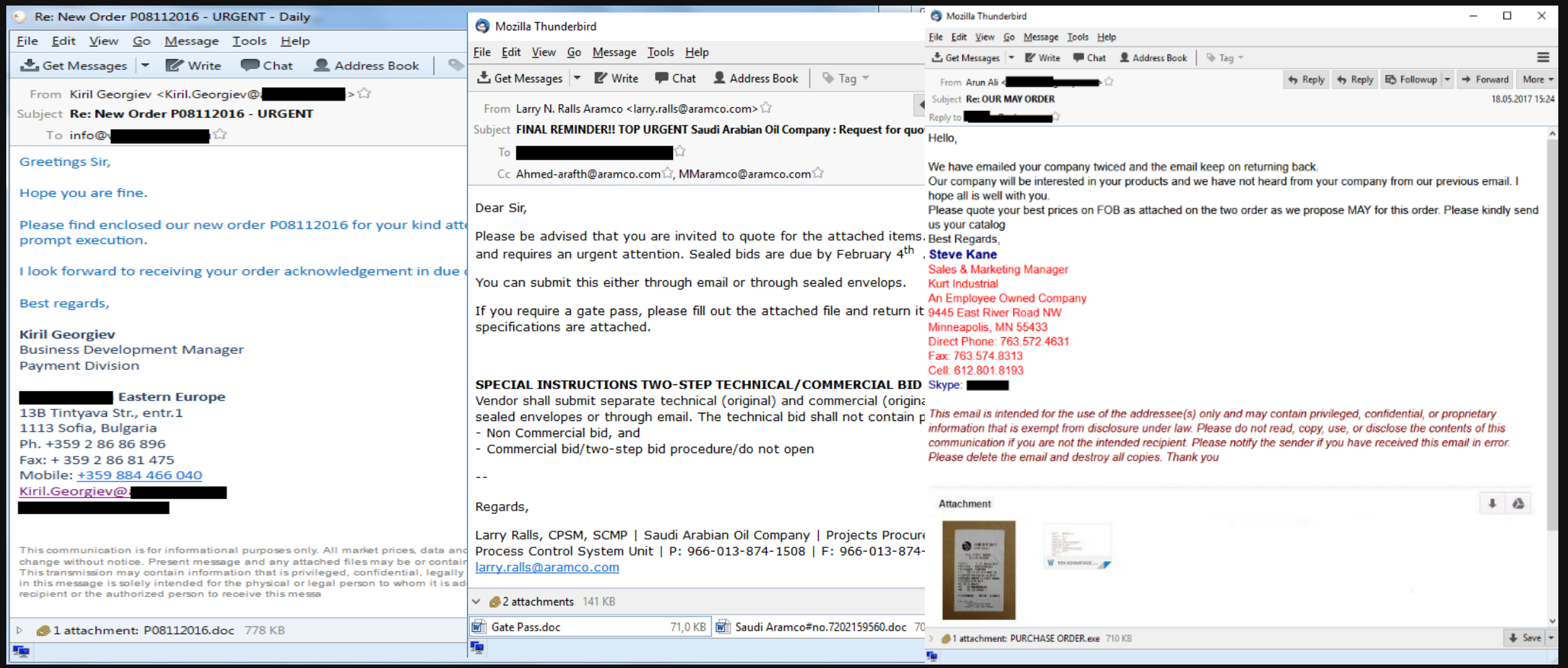
KASPERSKY lab

Motive #3 - Money



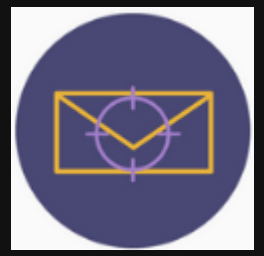
KASPERSKY lab

Motive #3 - Money



KASPERSKY lab

BUSINESS EMAIL COMPROMISE



Mozilla Thunderbird

File Edit View Go Message Tools Help

Get Messages | Write | Chat | Address Book | Tag

Reply | Reply | Followup | Forward | More

From Hardik Ray | [redacted] Steel <ray@[redacted]steel.com>

spoofed emails

Subject **Re: Banking information** [redacted]

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: HSBCHKHHHKH

Your quick reply is highly appreciated

Thanks and best regards!

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

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

KASPERSKY lab

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

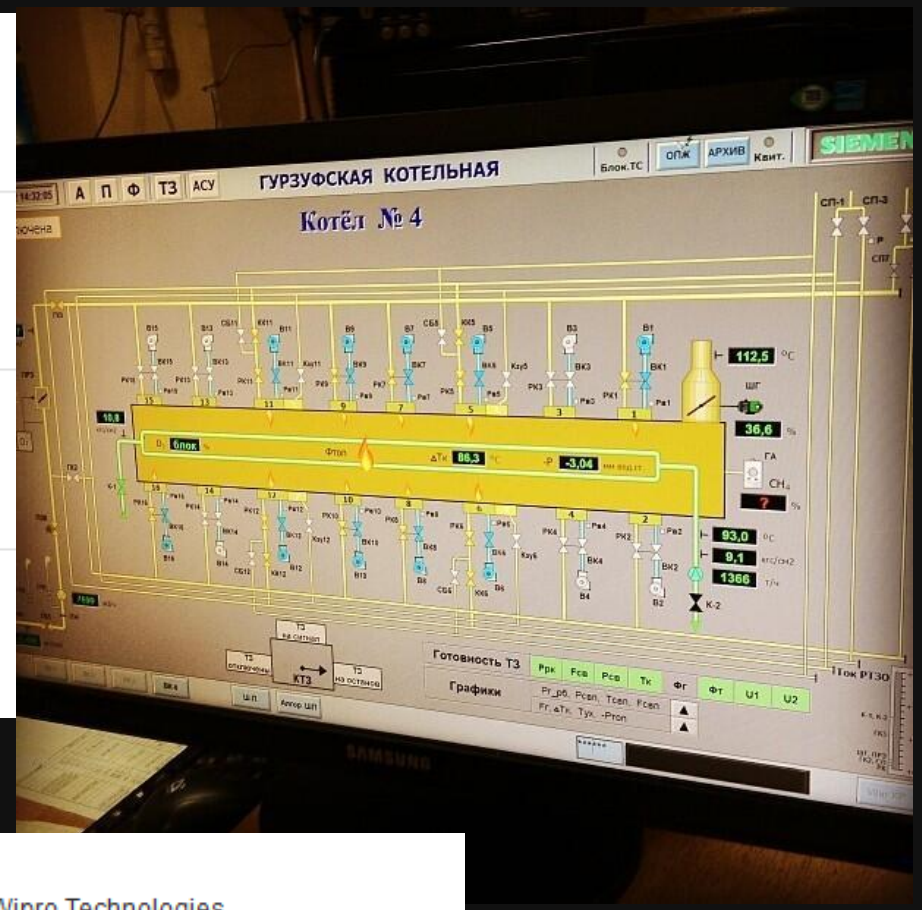
- A human factor - targeted attack (spear phishing emails, waterhole sites, social engineering, etc)

[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

KASPERSKY lab

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

me doc

Why do you want to defend yourself?

KASPERSKY lab

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

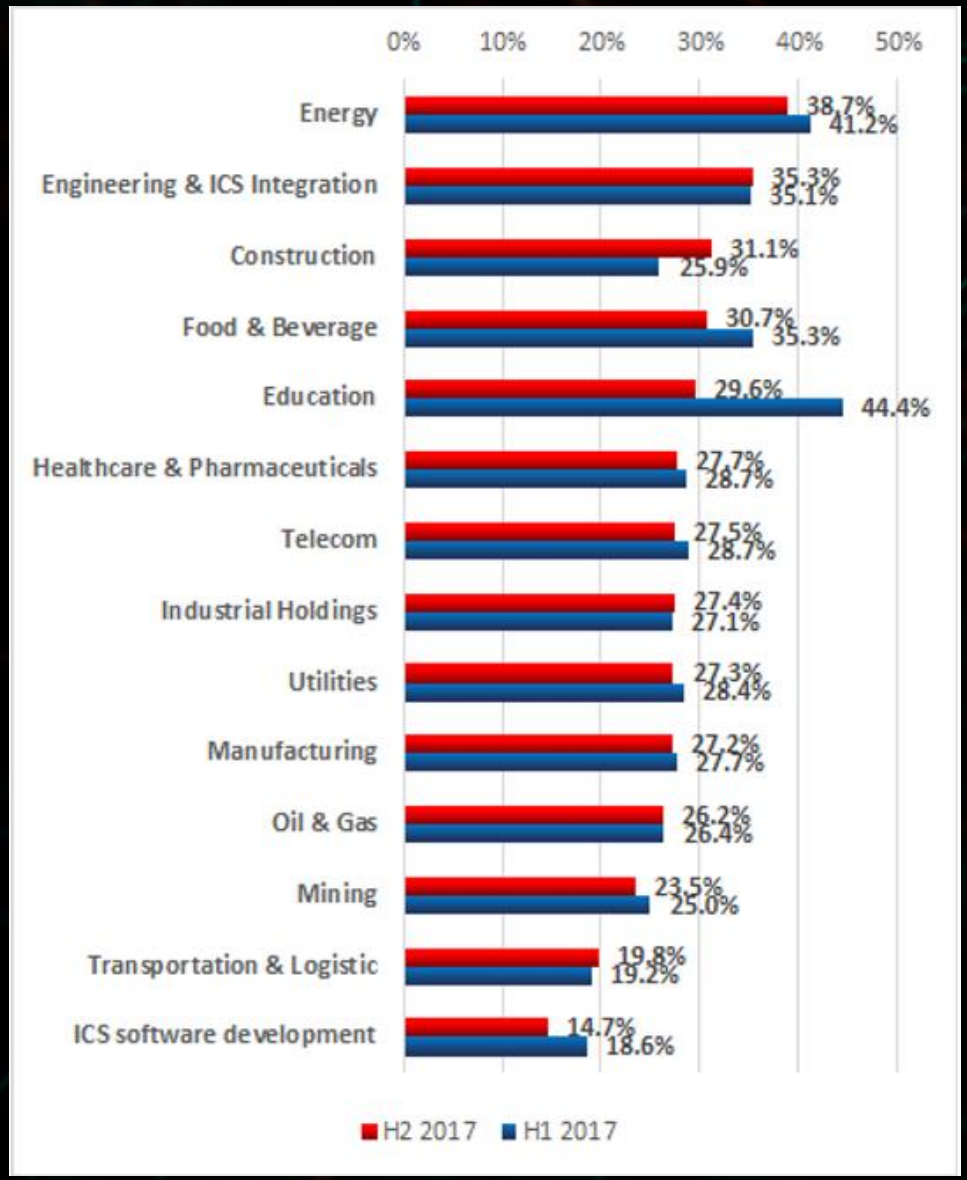
- Communication with the actor's server

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

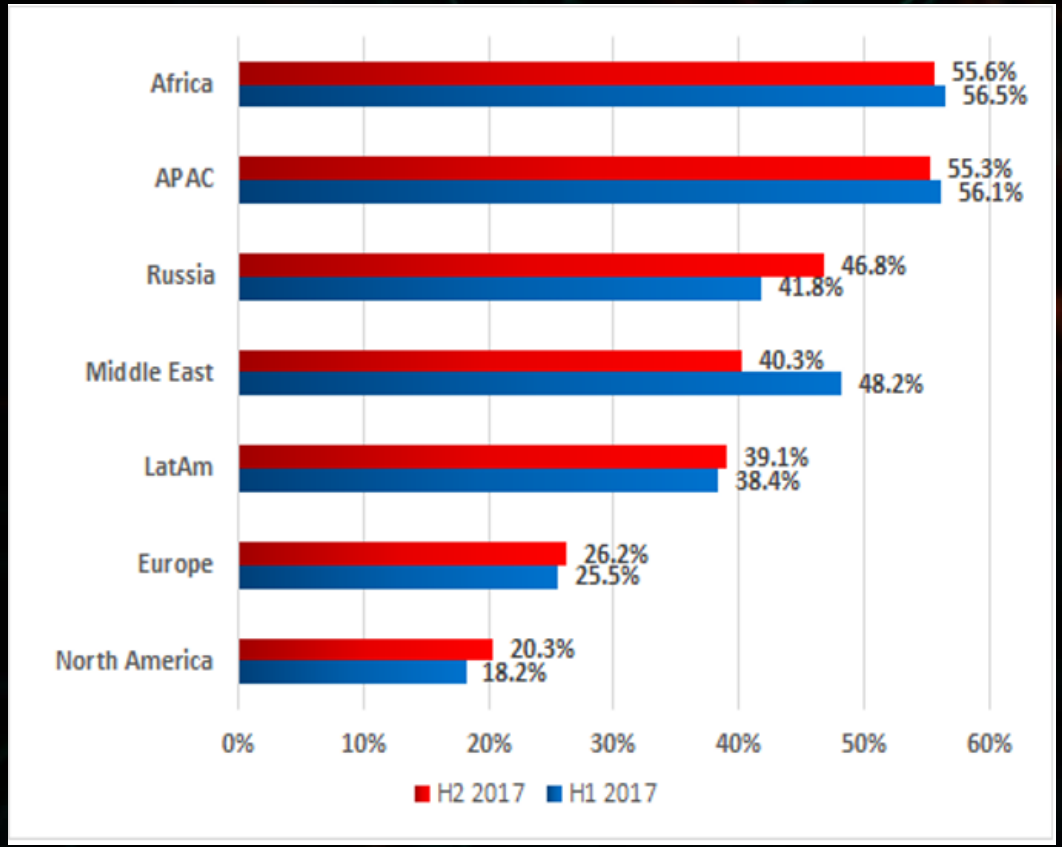


KASPERSKY lab

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)



KASPERSKY lab

Risks, Malware & Attacks

LEVEL 3

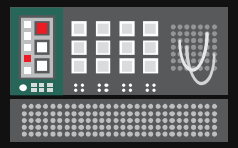
- Manufacturing Operations management

- 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

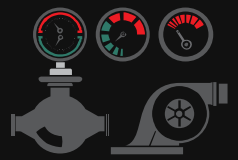
- Malware via USB, Network, Contractors
- Human actions (insiders, contractors)
- Internet attacks



- 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

KASPERSKY lab

Summary

- There are more cyber incidents than 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
- 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 lab