kaspersky

A insegurança cibernética fora das mãos de TI
O calcanhar de Aquiles da infraestrutura

Roberto Rebouças

Kaspersky Brasil Managing Director

25.07.2019

CYBERCRIME IS A HUGE GLOBAL PROBLEM

Cybercrime costs the world
$400*-500** billion per year

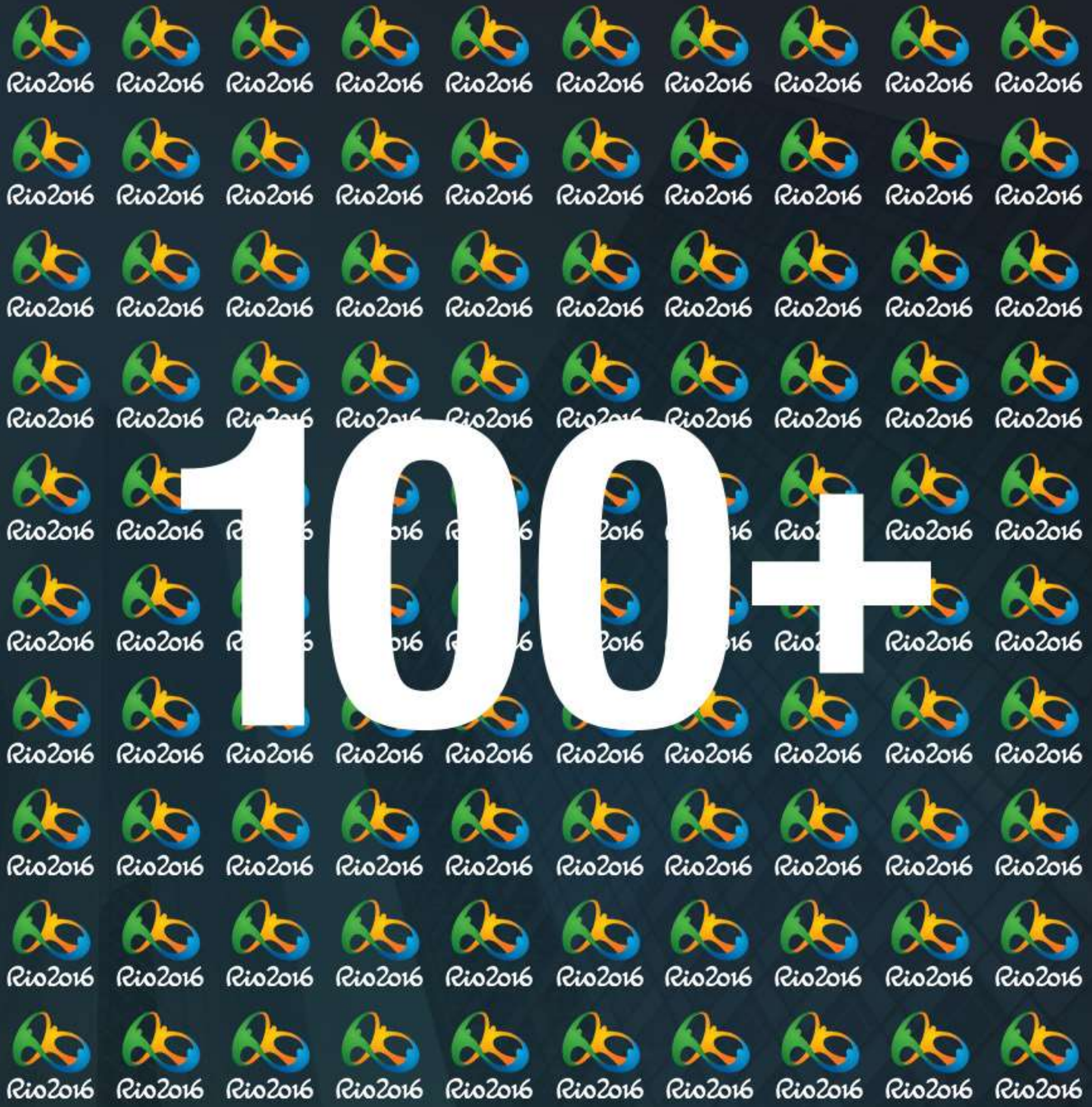
* Lloyds insurance – https://kas.pr/3vnZ
** Juniper Research – https://kas.pr/5SDw

kaspersky

2016 OLYMPICS COST: $4.6 BILLION

kaspersky

THE COST OF CYBERCRIME IN RIO OLYMPICS:



100+

kaspersky

INDUSTRIAL CYBERSECURITY APPROACH

1. Availability
2. Integrity
3. Confidentiality

1. Confidentiality
2. Integrity
3. Availability

- Corporate IT Security is about Data protection
- Industrial Security is about Process protection
- Process should be continuous and only then secure

kaspersky

IT WORLD vs OT (OPERATIONAL TECHNOLOGY) WORLD

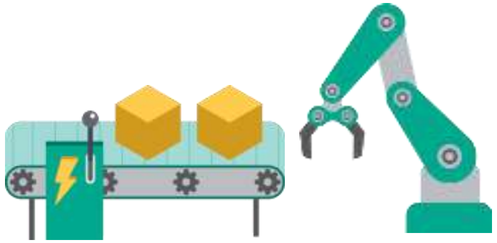
CIA - CONFIDENTIALITY

NEW PRIORITIES

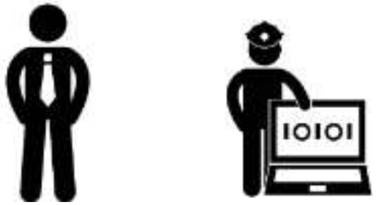
AIC - AVAILABILITY

PC, SERVER, MOBILE

NEW OBJECTS TO PROTECT

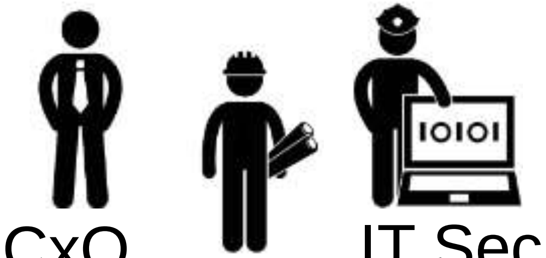


PLC, HMI, IND. PROTOCOLS, ETC



CxO IT Security

NEW STAKEHOLDERS



CxO Engineers IT Security

INDUSTRIAL CYBERSECURITY TODAY – LOW AWARENESS

C-level

Doesn’t see how
Cyber Security spending
relates to Revenues

IT Security

Is not allowed to go
into Industrial sites

Engineers

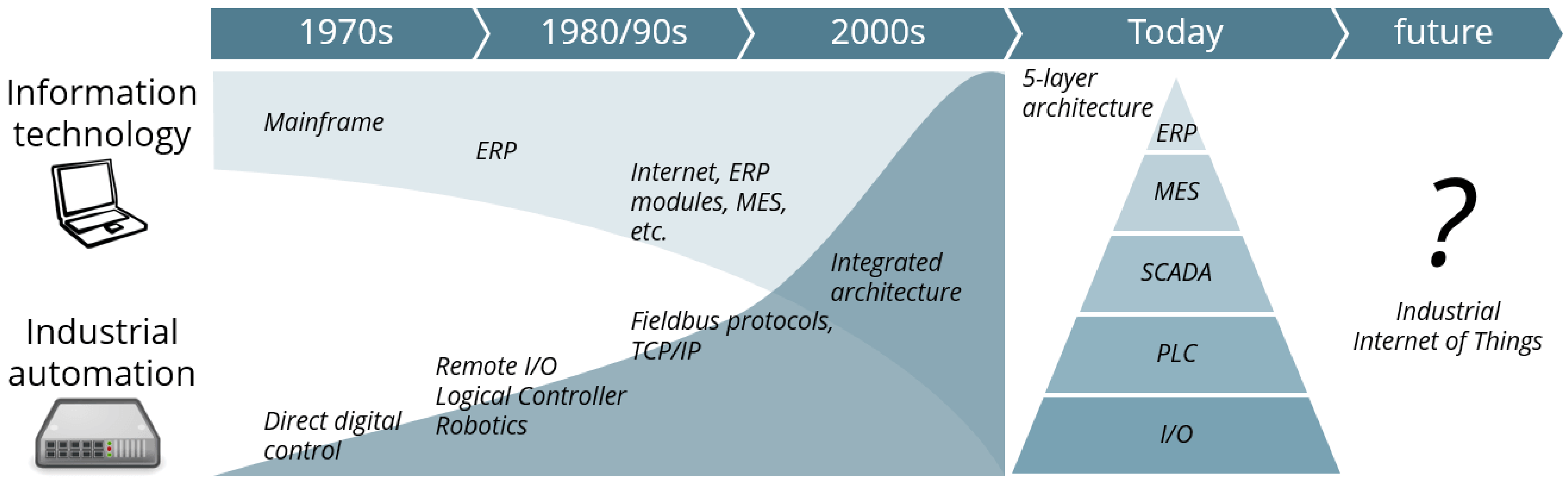
Are more concerned
about security measures
than malware

Mutual understanding and partnership between these 3 are crucial to successful cyber security and Critical Infrastructure Protection

IT AND OT (OPERATIONAL TECHNOLOGY) COLLIDE

IoT Analytics – *Quantifying the connected world*

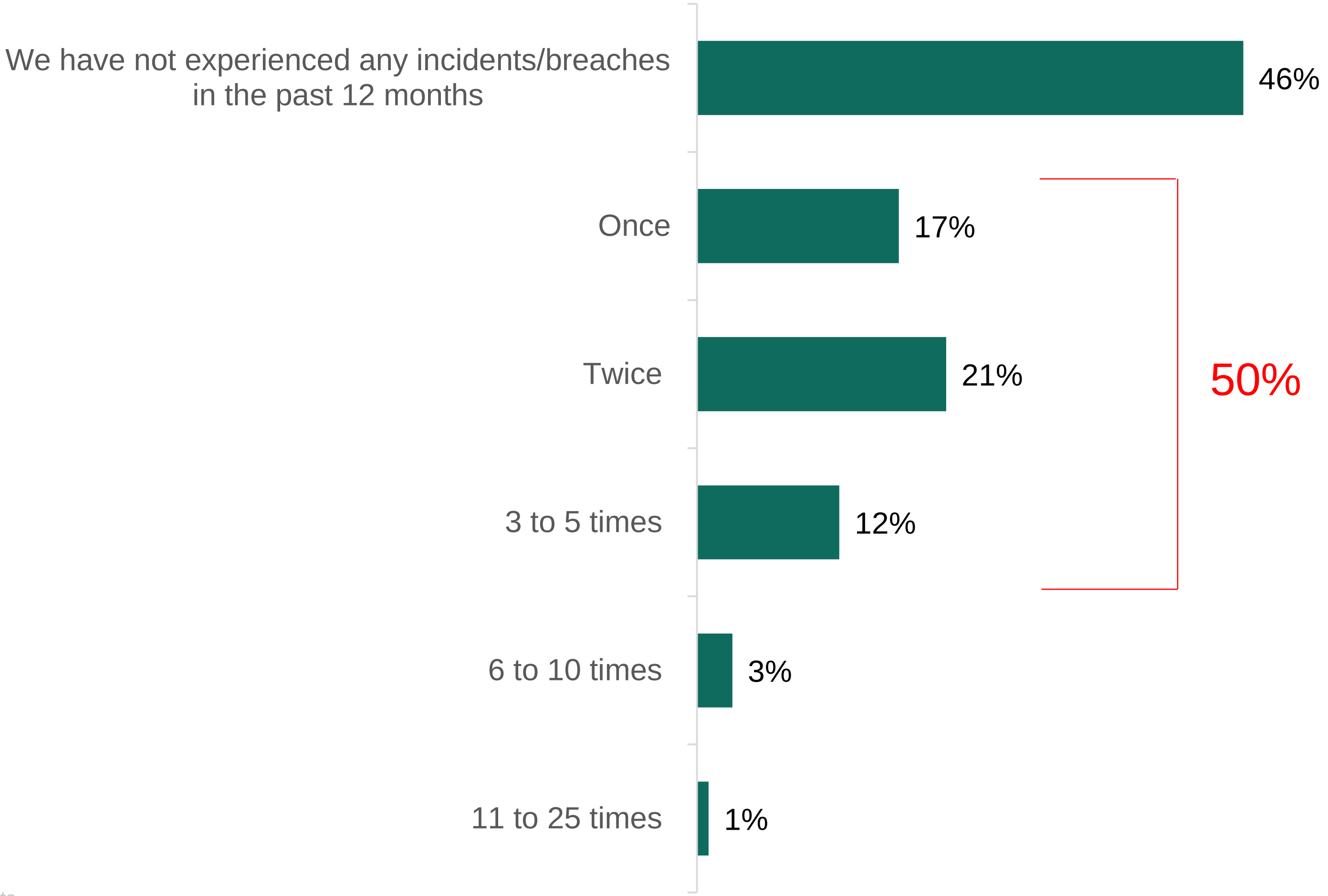
Convergence of IT and automation



ERP = Enterprise Resource Planning MES = Manufacturing Execution System SCADA = Supervisory Control and Data Acquisition PLC = Programmable Logic Controller I/O = Input/Output signals Source: IoT Analytics

ICS CYBERSECURITY INCIDENTS

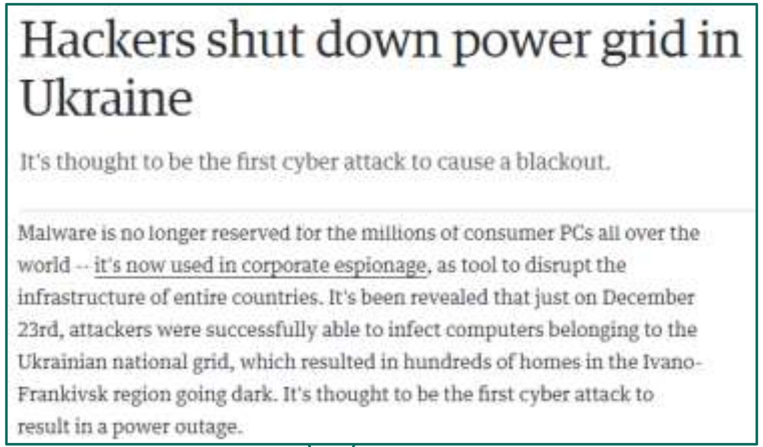
50% of companies have **experienced** between **1 and 5 cybersecurity incidents** with OT/ICS environment in the past 12 months



Q18.How many times did your organisation experience any cybersecurity incidents with OT/ICS and/or control system network in the past 12 months?
Base: Total sample=359

THE BIGGEST GAME OF TETRIS EVER!

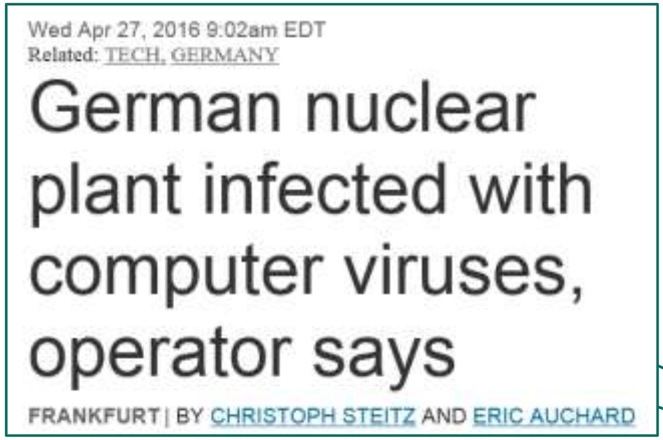
SOME (PUBLIC) ICS INCIDENTS



Hackers shut down power grid in Ukraine

It's thought to be the first cyber attack to cause a blackout.

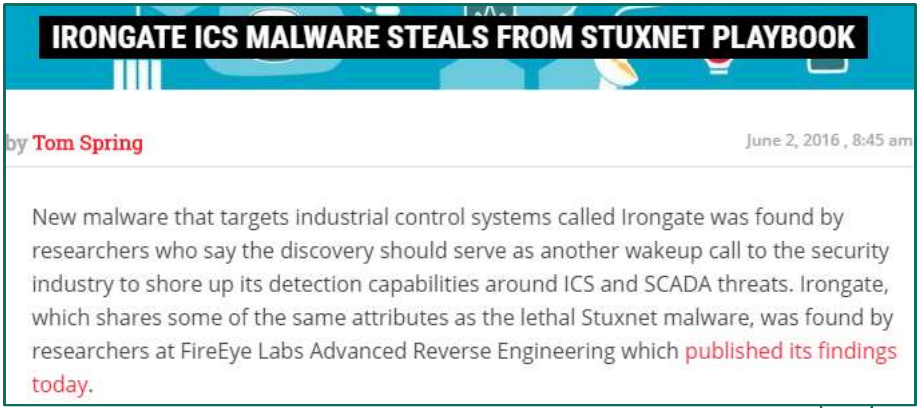
Malware is no longer reserved for the millions of consumer PCs all over the world -- it's now used in corporate espionage, as tool to disrupt the infrastructure of entire countries. It's been revealed that just on December 23rd, attackers were successfully able to infect computers belonging to the Ukrainian national grid, which resulted in hundreds of homes in the Ivano-Frankivsk region going dark. It's thought to be the first cyber attack to result in a power outage.



Wed Apr 27, 2016 9:02am EDT
Related: TECH, GERMANY

German nuclear plant infected with computer viruses, operator says

FRANKFURT | BY CHRISTOPH STEITZ AND ERIC AUCHARD

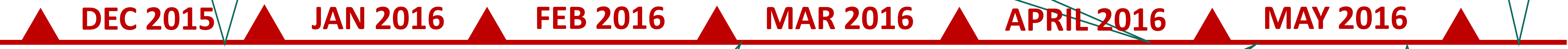


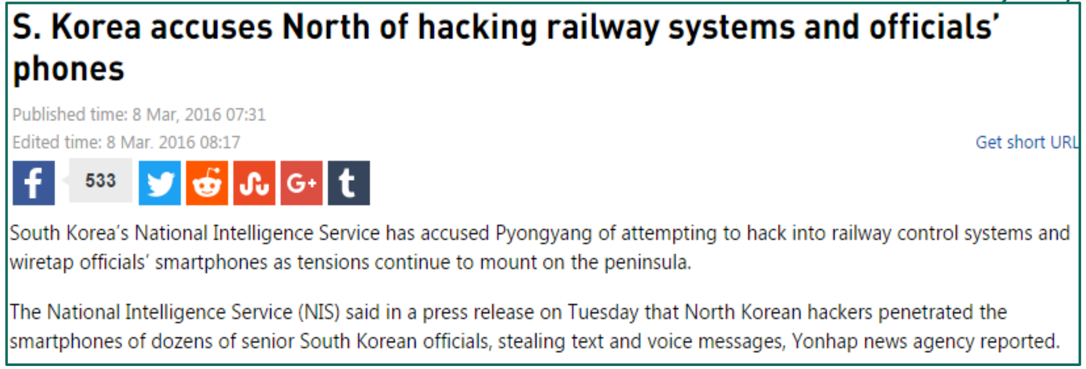
IRONGATE ICS MALWARE STEALS FROM STUXNET PLAYBOOK

by Tom Spring

June 2, 2016 , 8:45 am

New malware that targets industrial control systems called Irongate was found by researchers who say the discovery should serve as another wakeup call to the security industry to shore up its detection capabilities around ICS and SCADA threats. Irongate, which shares some of the same attributes as the lethal Stuxnet malware, was found by researchers at FireEye Labs Advanced Reverse Engineering which published its findings today.





S. Korea accuses North of hacking railway systems and officials' phones

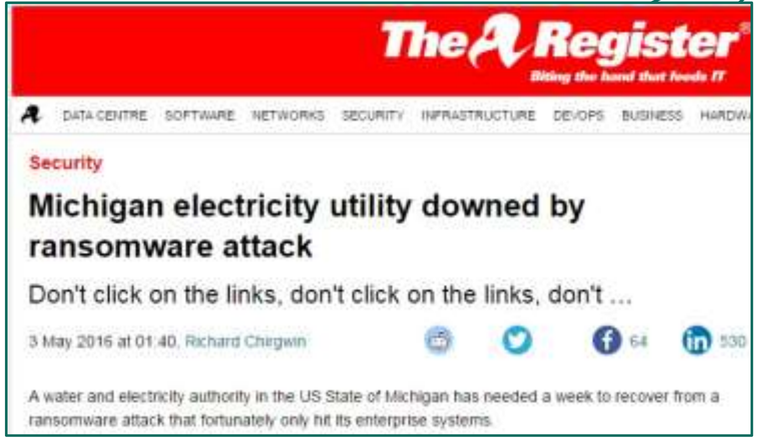
Published time: 8 Mar, 2016 07:31
Edited time: 8 Mar. 2016 08:17

Get short URL

533

South Korea's National Intelligence Service has accused Pyongyang of attempting to hack into railway control systems and wiretap officials' smartphones as tensions continue to mount on the peninsula.

The National Intelligence Service (NIS) said in a press release on Tuesday that North Korean hackers penetrated the smartphones of dozens of senior South Korean officials, stealing text and voice messages, Yonhap news agency reported.



Security

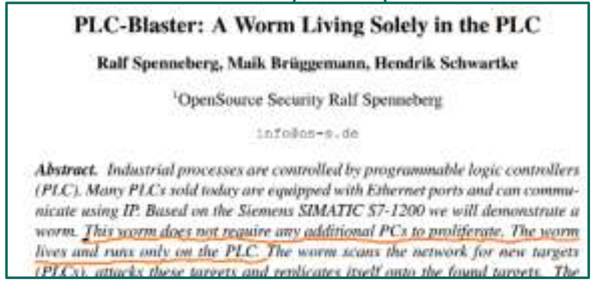
Michigan electricity utility downed by ransomware attack

Don't click on the links, don't click on the links, don't ...

3 May 2016 at 01:40, Richard Chirgwin

64 530

A water and electricity authority in the US State of Michigan has needed a week to recover from a ransomware attack that fortunately only hit its enterprise systems.



PLC-Blaster: A Worm Living Solely in the PLC

Ralf Spenneberg, Maik Brüggemann, Hendrik Schwartke

[1]OpenSource Security Ralf Spenneberg

info@os-s.de

Abstract. *Industrial processes are controlled by programmable logic controllers (PLC). Many PLCs sold today are equipped with Ethernet ports and can communicate using IP. Based on the Siemens SIMATIC S7-1200 we will demonstrate a worm. This worm does not require any additional PCs to proliferate. The worm lives and runs only on the PLC. The worm scans the network for new targets (PLCs), attacks these targets and replicates itself onto the found targets. The*

kaspersky

MALWARE AT GERMAN NUCLEAR PLANT, APRIL 2016

- Malware were discovered at plant's B unit in a computer system upgraded in 2008 with data visualization software associated with equipment for handling nuclear fuel rods
- RWE, utility operator, said that the malware was found during “preparatory testing work”
- RWE did not consider it a threat as the infected computer is not connected to the internet and malware affected only the computer IT systems and not the ICS/SCADA equipment that interacts with the nuclear fuel
- Tobias Schmidt, spokesman for the Gundremmingen nuclear plant, said, “Systems that control the nuclear process are analog thus isolated from cyber threats. These systems are designed with security features that protect them against manipulation.”
- Still whole nuclear plant was shut down for several days

Gundremmingen nuclear plant, located about 120 km northwest of Munich, is run by the German utility RWE

19 YEARS AGO.. MAROOCHY SHIRE SEWAGE SPILL

- In 2000, Maroochy Shire (Queensland, Australia) sewage system had 46 unexpected faults causing extensive sewage spillage

- This was done by Vitek Boden – insider who was never an employee of attacked utility, but was an employee of contractor that supplied SCADA sewage controls

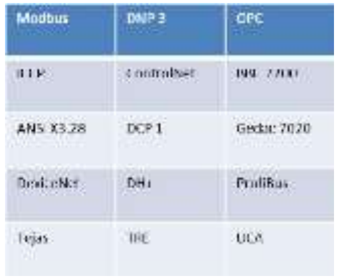
- Caused 800,000 liters of raw sewage to spill out into local parks and rivers

WANNACRY – ONE MORE EASY-TO-FORGET BLACK SWAN

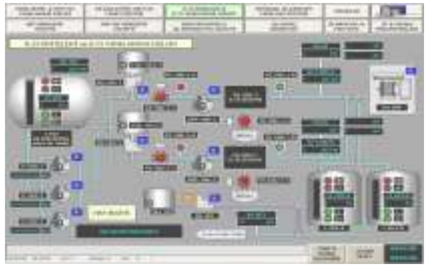
Industrial cases:

- Romanian carmaker Dacia halts production after global cyber attack http://www.reuters.com/article/us-cyber-attack-dacia-idUSKBN1890IG?il=0
- Renault stops production at some sites after cyber attack http://www.reuters.com/article/us-renault-cybercrime-idUSKBN1890AK
- Nissan's Sunderland plant hit by cyber-attack http://www.bbc.co.uk/news/uk-england-39906534
- In Spain, a number of large firms - including power firm Iberdrola and utility provider Gas Natural were also hit - http://www.bbc.com/news/technology-39901382

WHAT IS INDUSTRIAL CONTROL SYSTEM (AND WHAT ICS/AUTOMATION VENDORS PRODUCE)



Modbus	DNP 3	OPC
ICCP	ControlNet	IEC 61850
ANSI X3.28	DCP 1	Gedac 7020
DeviceNet	DH+	ProfiBus
Tejas	TRE	UCA



Acquisition

- Field Devices
- Sensors
- Meters

Conversion

- PLC
- IED
- RTU

Communication

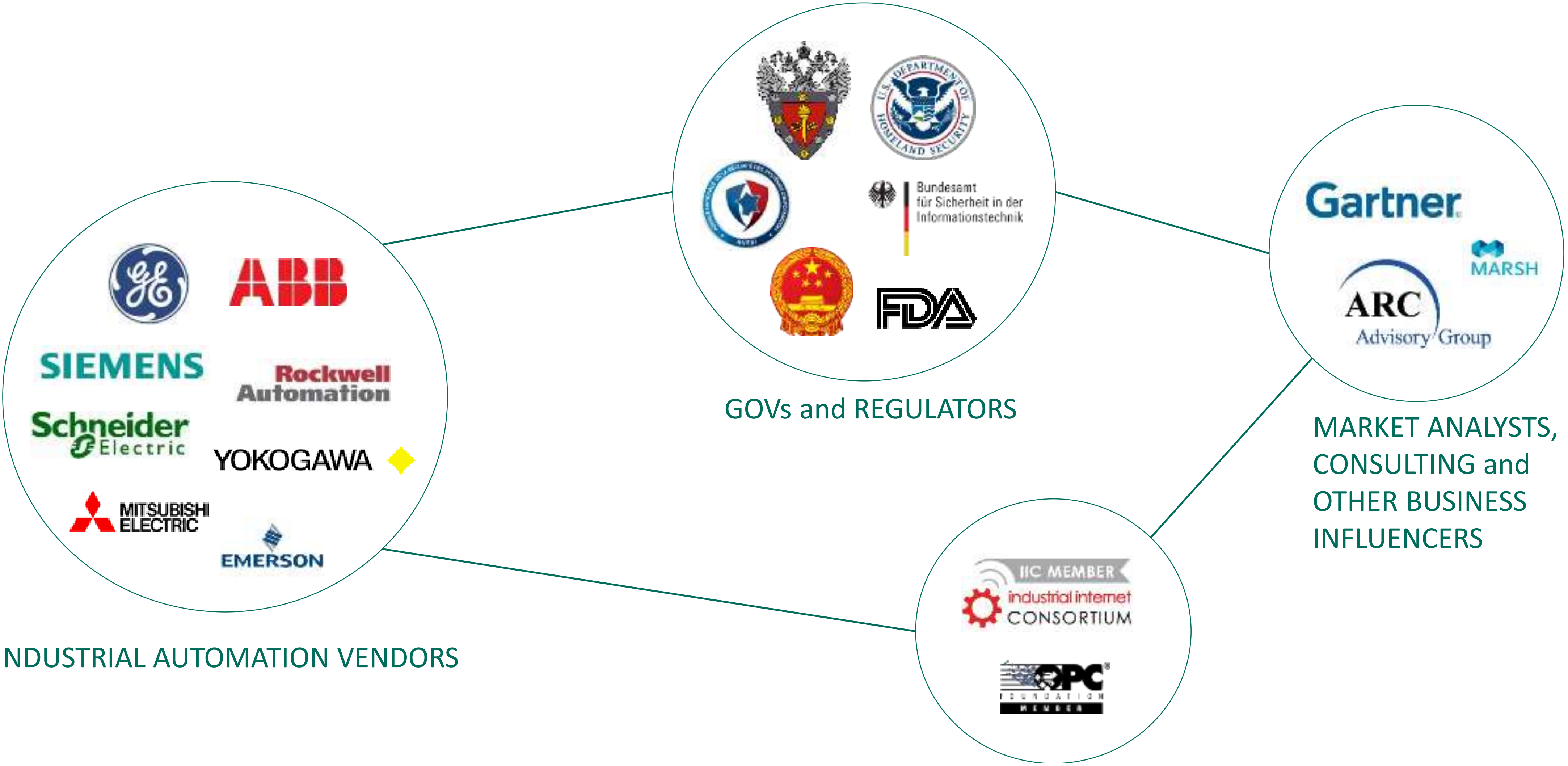
- Protocols
- Network equipment

Control

- SCADA
- HMI

NIST Guide to ICS Security
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

INDUSTRIAL CYBERSECURITY ECOSYSTEM MAP



GOVs and REGULATORS

MARKET ANALYSTS,
CONSULTING and
OTHER BUSINESS
INFLUENCERS

INDUSTRIAL AUTOMATION VENDORS

INDUSTRIAL PROFESIONAL ALLIANCES

EXPERTISE

1/3 of our employees are R&D specialists

325,000 new malicious files detected by Kaspersky Lab every day

40 world-leading security experts: our elite group

Our Global Research and Analysis Team of security experts constantly explores and fights the most advanced cyberthreats

kaspersky

THANK YOU

- kaspersky.com/ics
- ics-cert.kaspersky.com