CRUISE USER GROUP, 21 JUNE 2017

Digital Services & Cybersecurity
Recent threats and response

Palemia Field, Digital Services Manager- HBU Finland
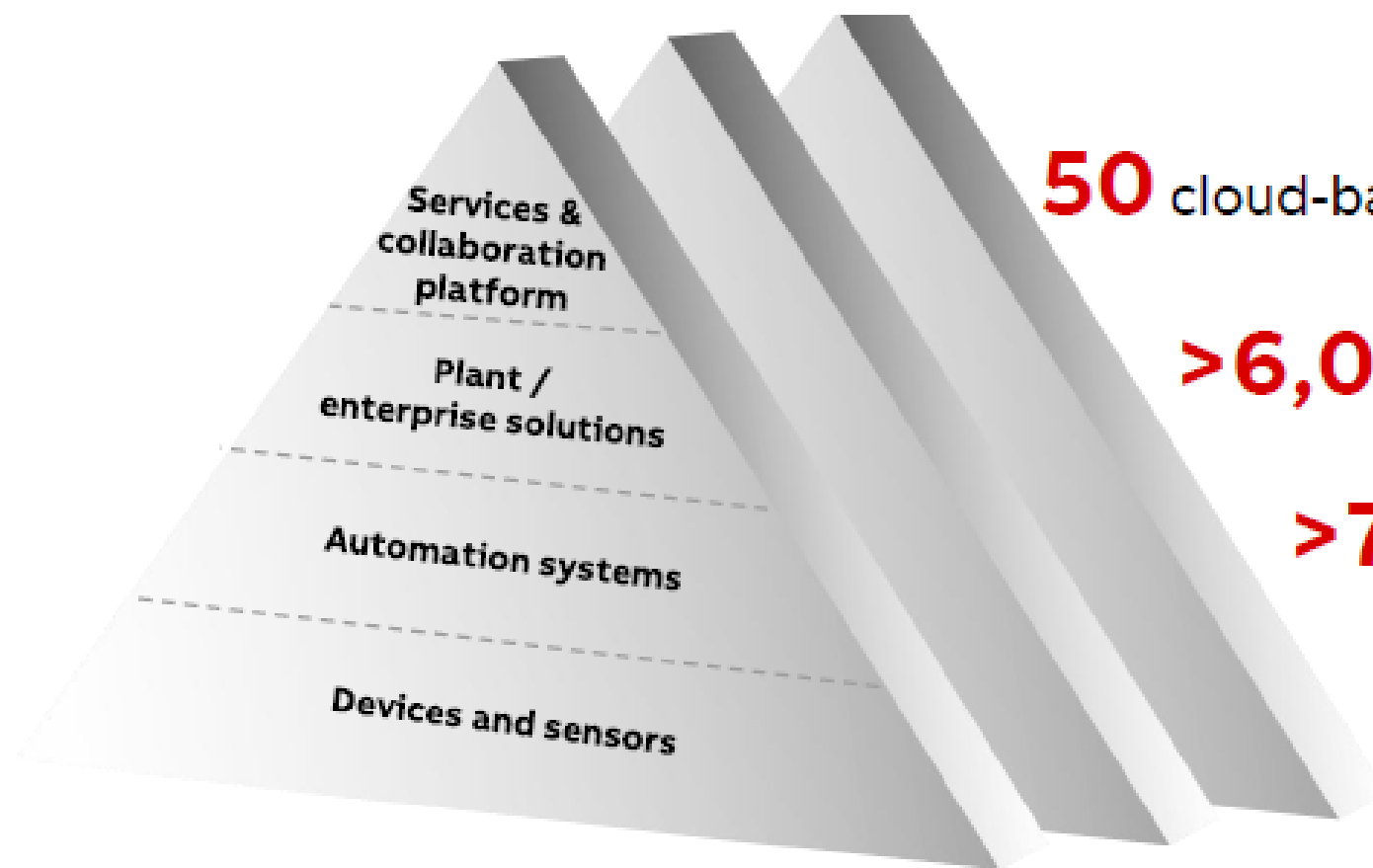
Agenda

Intro: ABB Marine & Ports Digital

Wannacry attack analysis & explanation

Responses

Solutions

ABB as a supplier of devices, systems and enterprise solutions

Large, global software and digital offering

Services & collaboration platform

Plant / enterprise solutions

Automation systems

Devices and sensors

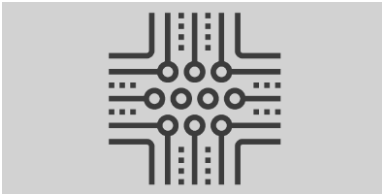**50** cloud-based services and advanced analytics

>6,000 solutions installed

>70,000 systems installed

>70,000,000 digitally enabled devices connected

ABB and Microsoft partner for world's largest industrial cloud platform
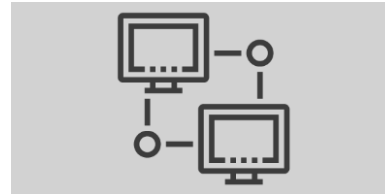
ABB Ability™

- End-to-end digital solution
- Closing the loop at every level

- Intelligent cloud platform

- Control room mastery
- Connected systems, devices

- Customer access and trust
- Domain and process expertise

Customer benefits

- Integrated digital platform, from device to system to cloud
- Combined strengths – each partner leading in its respective area

A quantum leap in digital solutions and offerings

ABB Ability™ : One common offering for end-to-end solutions

Open access, intelligent cloud

New end-to-end digital solutions

Closing the loop with connected devices
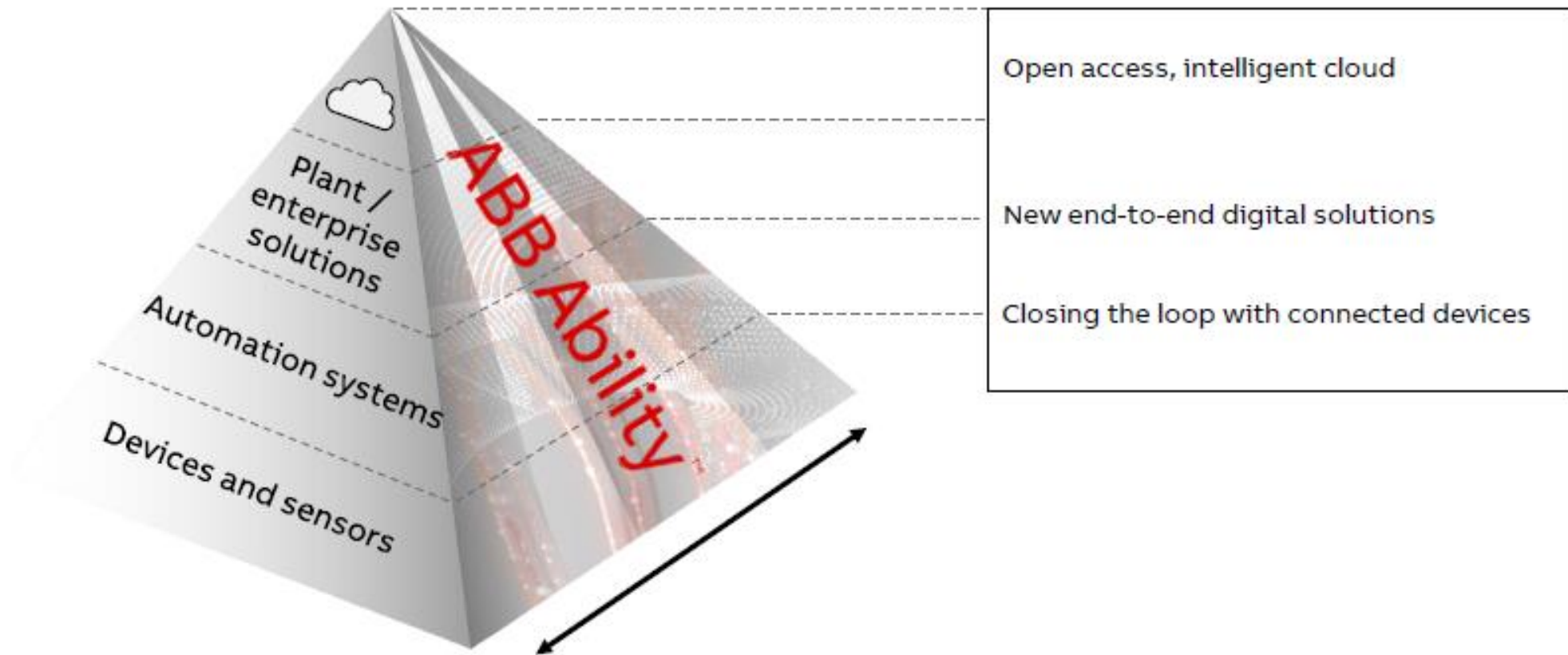
Analytics

What data we collect every day?

3100 signals from remote diagnostics

40 technical questions

6 critical alarms

Up to 50 different signals on sea conditions (waves, wind, current, water depth etc.)

220k nautical miles added to voyage data

1500 signals on energy consumption, 3GB

ABB
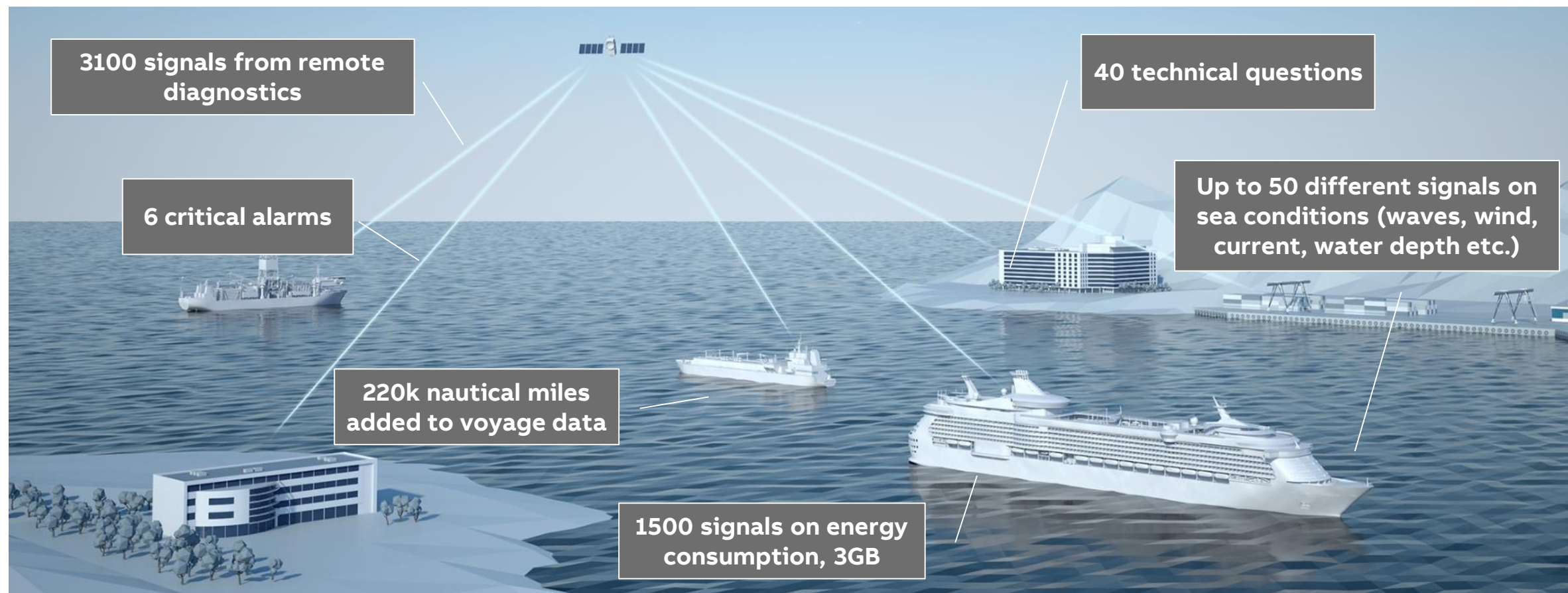
Collaborative Operations Centers

Global Support

Collaborative Operations

The Collaborative Operations Center (COC) is an integrated part of the Service, Warranty, Global Technical Support and Commissioning operations.

All COCs can track technical support cases and ABB Marine and Ports can manage technical support questions in a true 24/7 manner – there is always an engineer on duty.

- Norway and Dalfsen, open since 2015
- Finland, Singapore and Genoa opened 2016
- Miami and Shanghai to be opened in 2017

COC Dalfsen
Operations Monitoring

COC Oslo
Europe, Oil & Gas

COC Västerås
Ports

COC Helsinki
Pax, Cargo, Ice & Azipod

COC Genoa
Marine Automation

COC San Digeo
Ports 4/17

COC Shanghai
CN Customers Within 2017

COC Miami
Americas

COC Singapore
Asia Pacific

Operating

Planned/ under construction

ABB
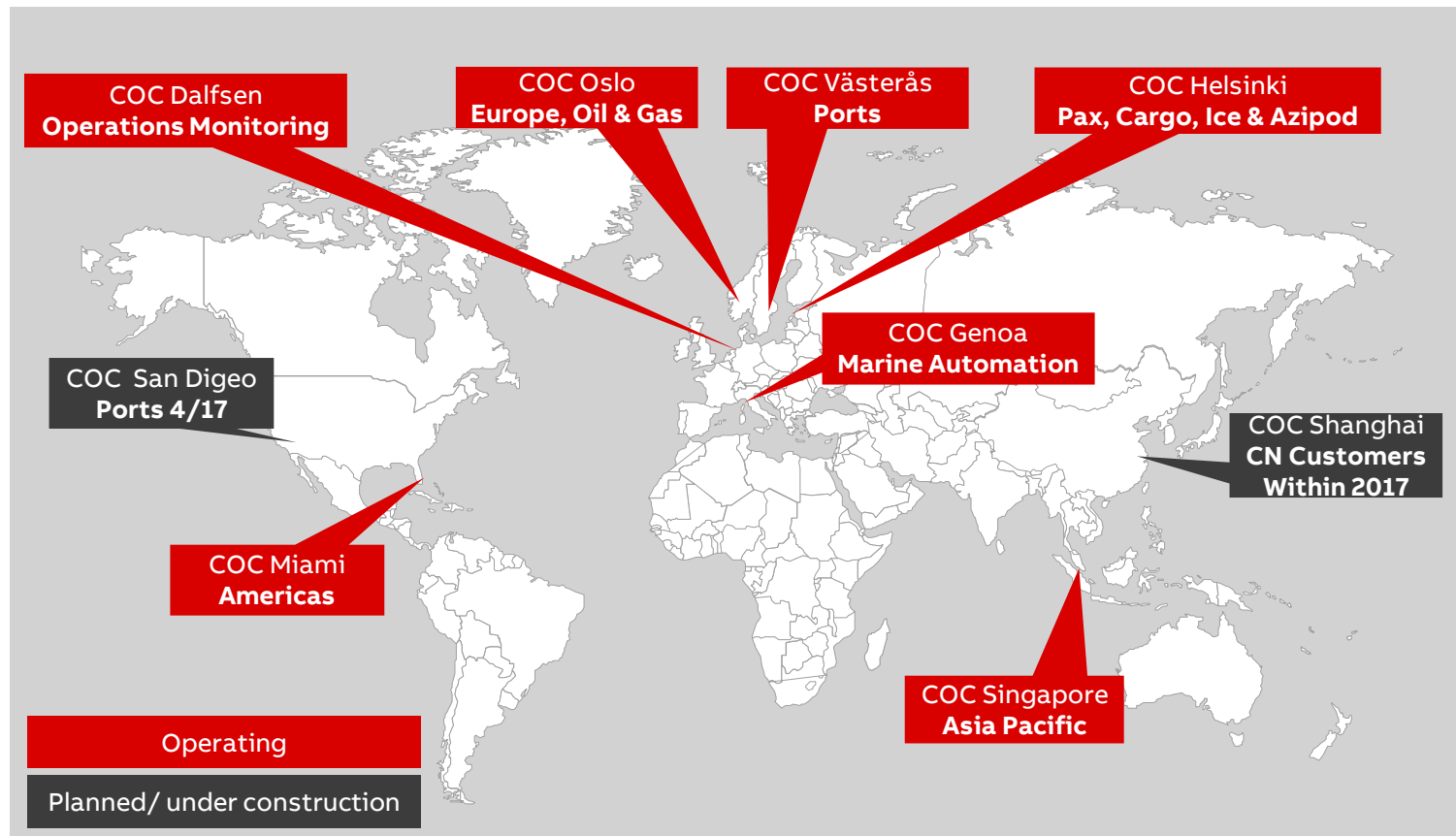
Wannacry Ransomware

Wannacry/ Wannacrypt

Overview

What is it?

Two part ransomware:

– Exploit: Infect & Propagate (SMB Worm)

– Encryptor: Downloaded after infection → Ransom Demand

Primary infection vector unclear

Cryptoworm exploits SMB* on Windows machines.

On activation, encrypts files rendering them inaccessible.

Spreads through a network without user interaction

Ransom to decrypt via Bitcoin

SMB Worm Component

Malware stops

Connection Success

Connection Fail

mssecsvc.exe
lhdfrgui.exe

Connect to
www.iuqerfsodp9ifjaposdfjhg
osurijfaewrwergwea.com

tasksche.exe

Ransomware Component

Data encrypted

Ransom demanded

SMB
enumeration

ETERNALBLUE
exploit against
unpatched systems

ABB
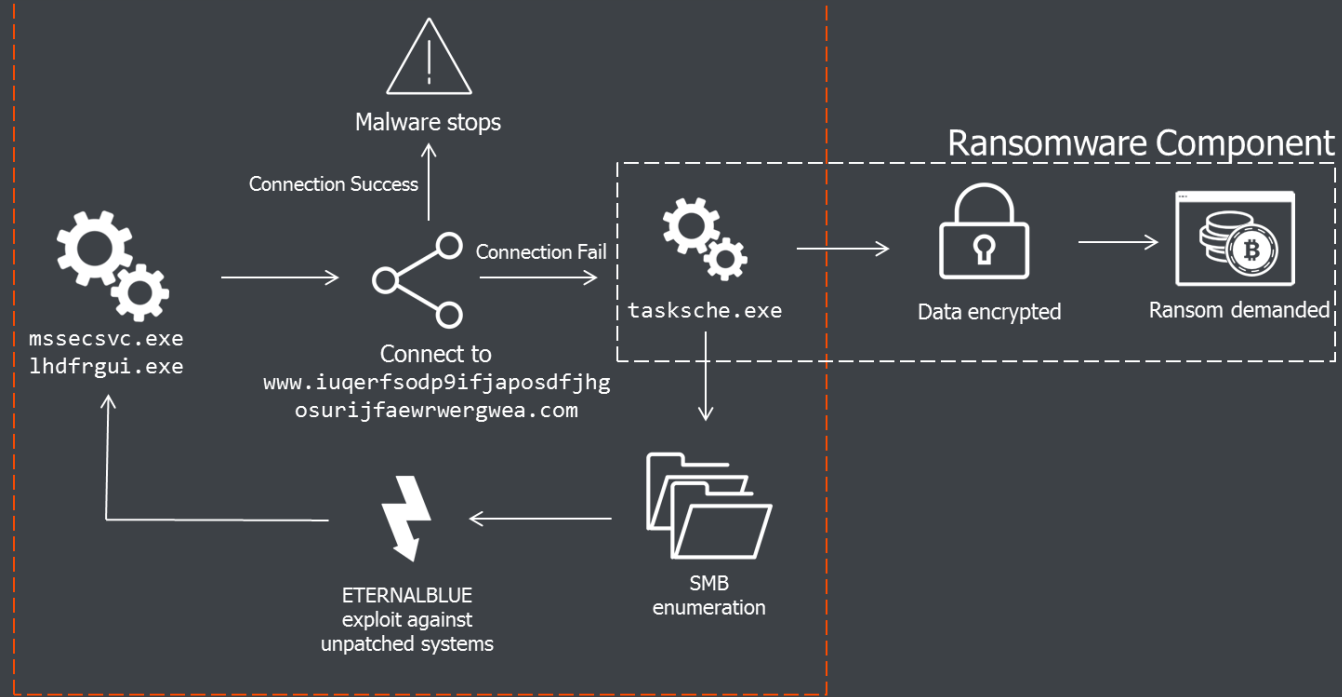
Wannacry/ Wannacrypt

The Impact

Thought to affect between 200,000 to 3 million affected systems, however confirmed number two weeks after release was 727,000

Kaspersky reports "*WannaCry reached over 9,500 unique ISP and/or organization IP WHOIS registrations, 8,900 cities, 90 countries with a measurable (1000+ uniques) impact, and some infection traces reaching virtually all countries worldwide*."

Microsoft forced to issue emergency patches for obsolete systems (xP, 8 & Server 2003) in addition to March 14 patch (MS17-0101)

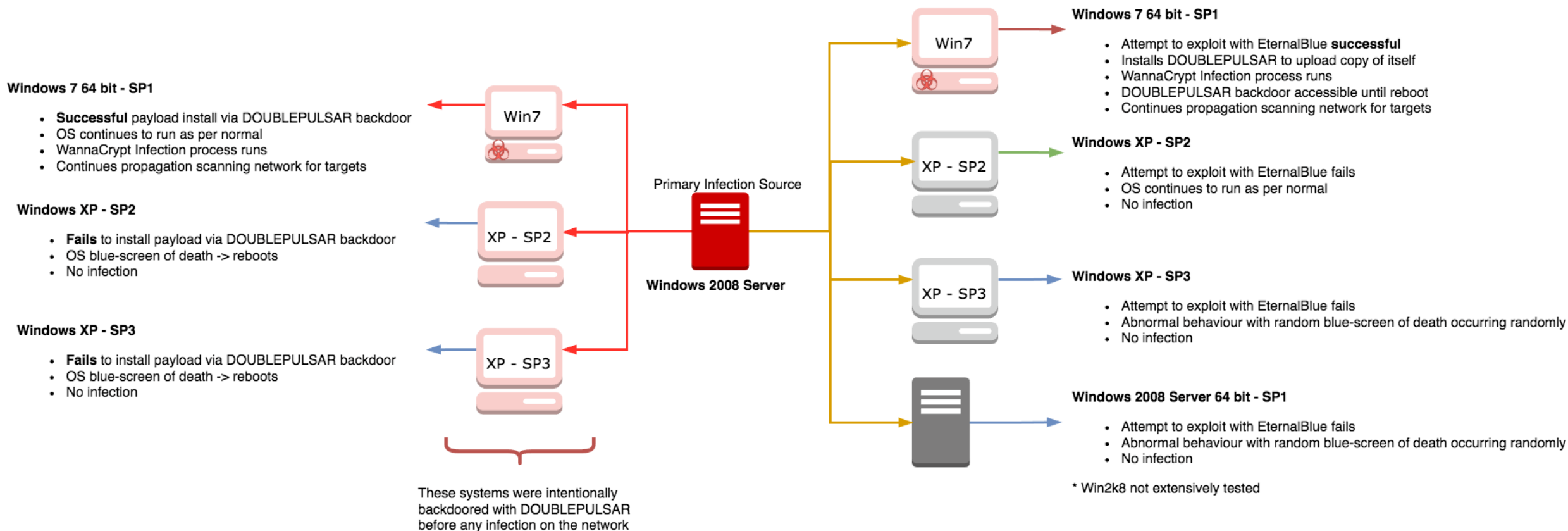Traces back to EternalBlue & DoublePulsar exploit tools suspected to be developed by NSA and leaked publically in April

Impact on PCs depend on Windows Version.

ABB

Which Windows version

Wannacry infection tests

Windows 7 64 bit - SP1

- **Successful** payload install via DOUBLEPULSAR backdoor
- OS continues to run as per normal
- WannaCrypt Infection process runs
- Continues propagation scanning network for targets

Windows XP - SP2

- **Fails** to install payload via DOUBLEPULSAR backdoor
- OS blue-screen of death -> reboots
- No infection

Windows XP - SP3

- **Fails** to install payload via DOUBLEPULSAR backdoor
- OS blue-screen of death -> reboots
- No infection

These systems were intentionally backdoored with DOUBLEPULSAR before any infection on the network

Primary Infection Source

Windows 2008 Server

Windows 7 64 bit - SP1

- Attempt to exploit with EternalBlue **successful**
- Installs DOUBLEPULSAR to upload copy of itself
- WannaCrypt Infection process runs
- DOUBLEPULSAR backdoor accessible until reboot
- Continues propagation scanning network for targets

Windows XP - SP2

- Attempt to exploit with EternalBlue fails
- OS continues to run as per normal
- No infection

Windows XP - SP3

- Attempt to exploit with EternalBlue fails
- Abnormal behaviour with random blue-screen of death occurring randomly
- No infection

Windows 2008 Server 64 bit - SP1

- Attempt to exploit with EternalBlue fails
- Abnormal behaviour with random blue-screen of death occurring randomly
- No infection

* Win2k8 not extensively tested

https://blog.kryptoslogic.com/assets/two-weeks-later/propagation_testing_v.06.png

ABB

RDS4Marine

Remote Connection

Based on ABB Remote Access Platform (RAP)

Collaborative Operations Center
ABB Service organization for remote support

- <u>Layer 0</u>: Users launching the service center user interface in a web browser
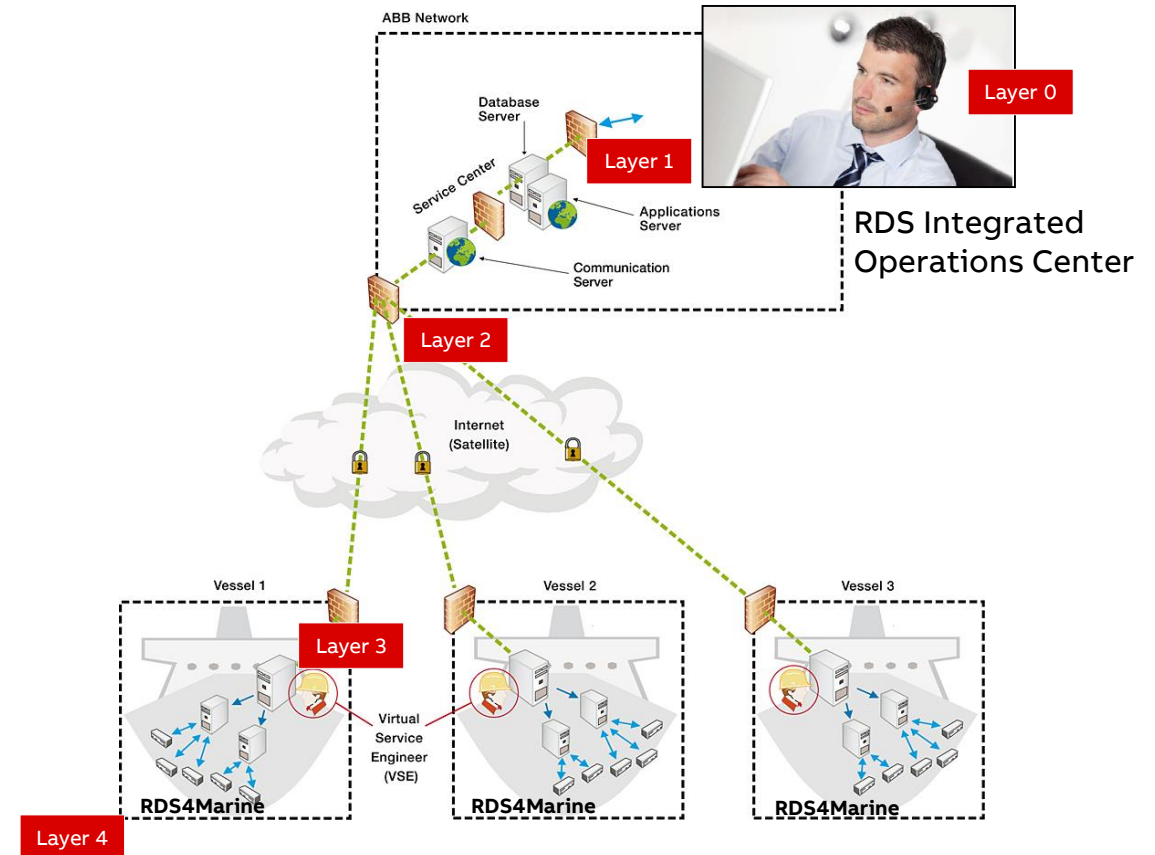
Service center
Web application server – the system core, control center and communication hub

- <u>Layer 1</u>: application and database servers residing in DB DMZ,
- <u>Layer 2</u>: communication server residing in web DMZ (accessible from the Internet)

Onboard monitoring
Monitoring and diagnostic solution, customer HMI and control center for remote activity

- <u>Layer 3</u>: virtual support engineer (VSE) residing at a customer facility (behind firewalls) and installed on RDS4Marine onboard infrastructure
- <u>Layer 4</u>: RDS4Marine diagnostic solutions that monitor ABB equipment used in the vessel's power plant chain

RDS Integrated Operations Center

RDS4Marine

Remote Connection

Virtual Support Engineer (VSE)

Software package installed on board

- Acts as a software-site-manager

- Its main purpose is to set up a secure communication with the Service Center and signal its availability for a remote maintenance section.

- VSE will automatically contact the Service Center from anywhere in the world to make remote connection possible

- Allows Downstream (Remote) Patch Repository (installed in the Customer's network) to retrieve updates from the Upstream (Source) Patch Repository (installed in ABB).

- Windows Server Update Service (WSUS)

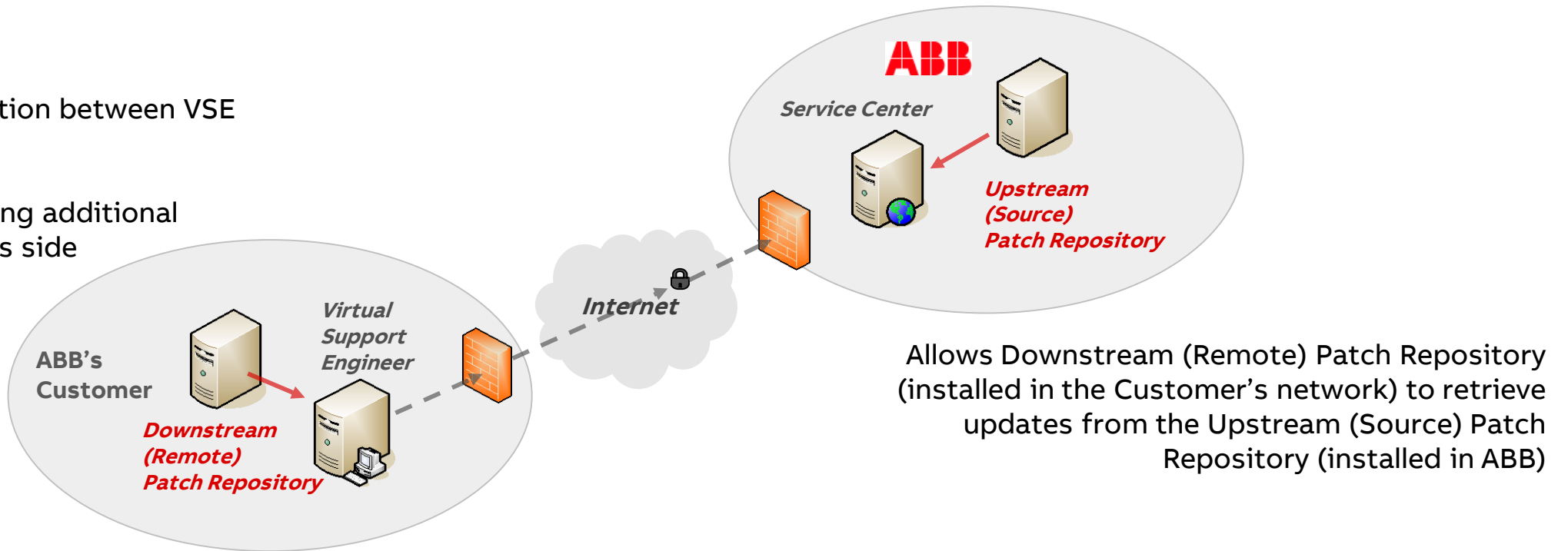- ePO – McAfee ePolicy and updates

ABB

RDS4Marine

Remote Connection

Security Update Service in RAP - Overview

Utilizes Secure Connection between VSE and Service Center.

Does not require opening additional ports at the Customer's side

Allows Downstream (Remote) Patch Repository (installed in the Customer's network) to retrieve updates from the Upstream (Source) Patch Repository (installed in ABB)