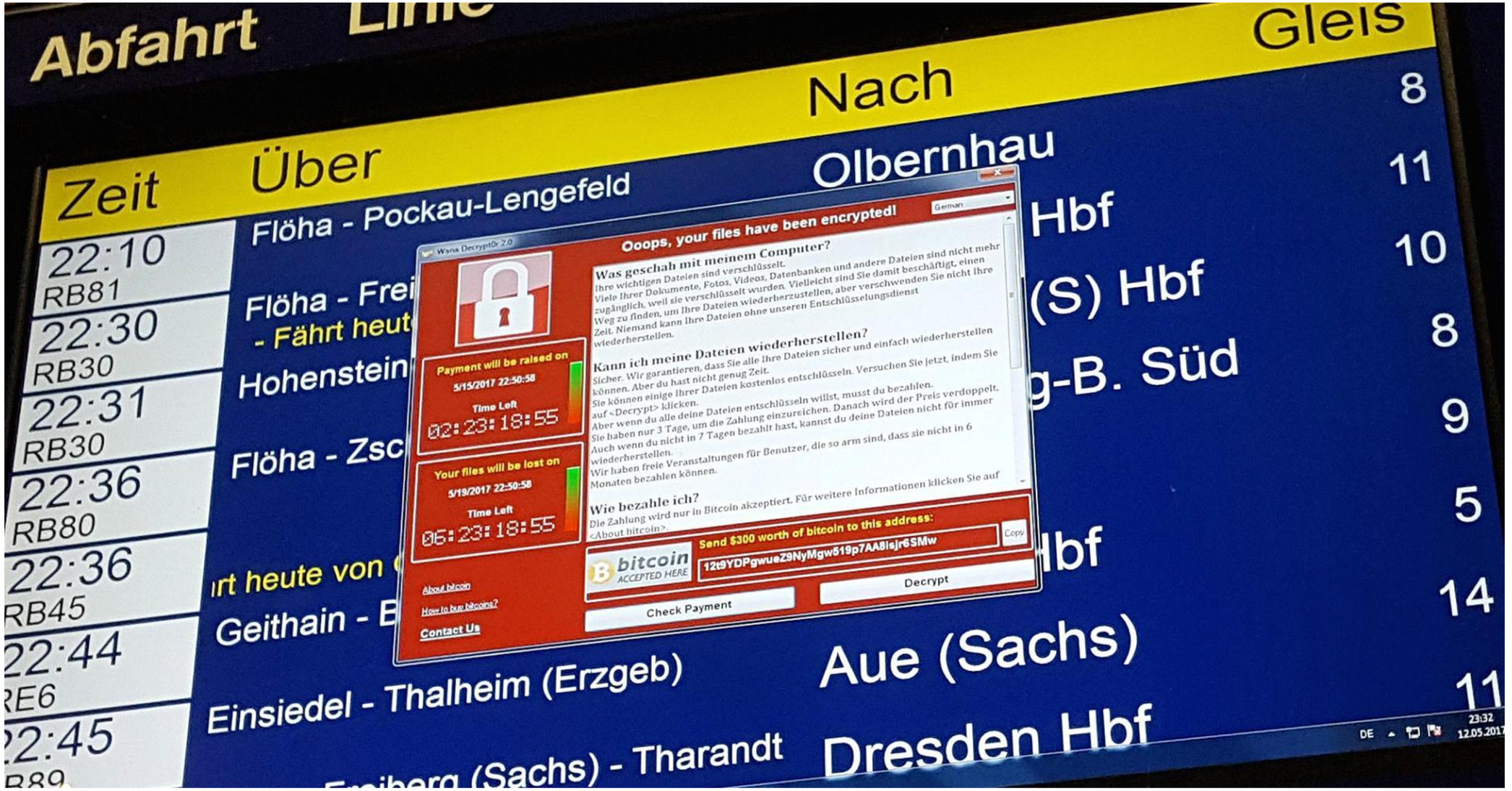
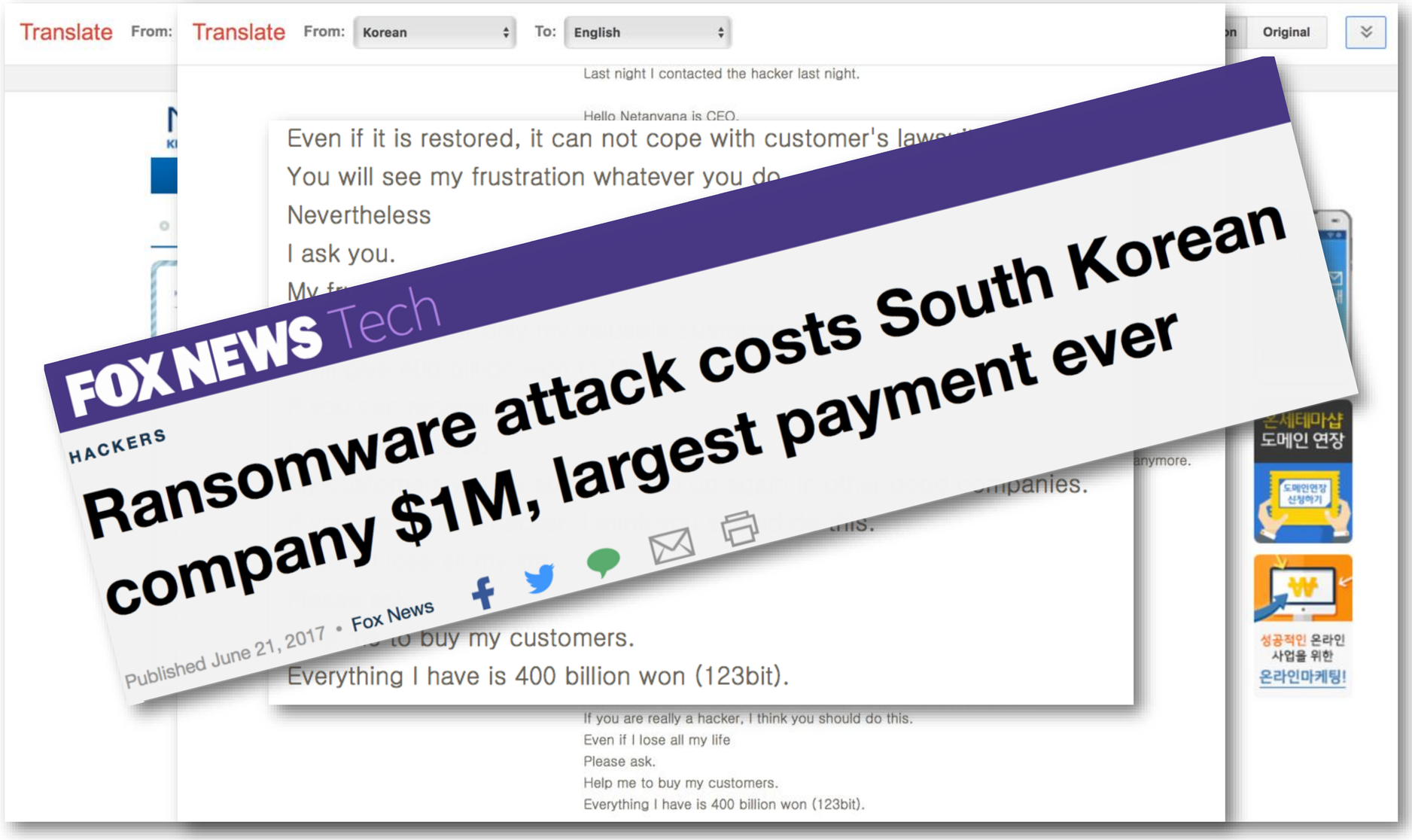
# O cenário atual de ameaças na América Latina e quais serão os desafios futuros.

Franzvitor Fiorim, Diretor Técnico, Trend Micro Brasil

# Ameaças digitais? Você se lembra?


Abfahrt
Linie
Nach
Gleis
Zeit
Über
22:10
RB81
Flöha - Pockau-Lengefeld
Olbernhau
8
22:30
RB30
Flöha - Frei
- Fährt heut
Hbf
11
22:31
RB30
Hohenstein
(S) Hbf
10
22:36
RB80
Flöha - Zsc
g-B. Süd
8
22:36
RB45
rt heute von
Geithain - E
lbf
9
22:44
RE6
Einsiedel - Thalheim (Erzgeb)
Aue (Sachs)
5
2:45
B89
Freiberg (Sachs) - Tharandt
Dresden Hbf
14
11
DE
23:32
12.05.2017
Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
German
Was geschah mit meinem Computer?
Ihre wichtigen Dateien sind verschlüsselt.
Viele Ihrer Dokumente, Fotos, Videos, Datenbanken und andere Dateien sind nicht mehr zugänglich, weil sie verschlüsselt wurden. Vielleicht sind Sie damit beschäftigt, einen Weg zu finden, um Ihre Dateien wiederherzustellen, aber verschwenden Sie nicht Ihre Zeit. Niemand kann Ihre Dateien ohne unseren Entschlüsselungsdienst wiederherstellen.
Kann ich meine Dateien wiederherstellen?
Sicher. Wir garantieren, dass Sie alle Ihre Dateien sicher und einfach wiederherstellen können. Aber du hast nicht genug Zeit.
Sie können einige Ihrer Dateien kostenlos entschlüsseln. Versuchen Sie jetzt, indem Sie auf <Decrypt> klicken.
Aber wenn du alle deine Dateien entschlüsseln willst, musst du bezahlen.
Sie haben nur 3 Tage, um die Zahlung einzureichen. Danach wird der Preis verdoppelt.
Auch wenn du nicht in 7 Tagen bezahlt hast, kannst du deine Dateien nicht für immer wiederherstellen.
Wir haben freie Veranstaltungen für Benutzer, die so arm sind, dass sie nicht in 6 Monaten bezahlen können.
Wie bezahle ich?
Die Zahlung wird nur in Bitcoin akzeptiert. Für weitere Informationen klicken Sie auf <About bitcoin>.
Payment will be raised on
5/15/2017 22:50:58
Time Left
02:23:18:55
Your files will be lost on
5/19/2017 22:50:58
Time Left
06:23:18:55
About bitcoin
How to buy bitcoins?
Contact Us
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
bitcoin ACCEPTED HERE
Check Payment
Decrypt


Reuters


Translate From: Korean To: English
Original
Last night I contacted the hacker last night.
Hello Netanyana is CEO.
Even if it is restored, it can not cope with customer's lawsuits
You will see my frustration whatever you do
Nevertheless
I ask you.
My friends to buy my customers.
Everything I have is 400 billion won (123bit).
If you are really a hacker, I think you should do this.
Even if I lose all my life
Please ask.
Help me to buy my customers.
Everything I have is 400 billion won (123bit).
FOX NEWS Tech
HACKERS
Ransomware attack costs South Korean company $1M, largest payment ever
Published June 21, 2017 • Fox News
anymore.
companies.
this.
온세테마샵
도메인 연장
도메인연장 신청하기
성공적인 온라인 사업을 위한
온라인마케팅!


DEVELOPING THIS MORNING
GIANT DATA BREACH COULD HIT 143 MILLION PEOPLE
Credit reporting firm Equifax says hackers stole personal info
LIVE
CNN
12:24 AM PT
HURRICANE IRMA
CATEGORY 5
WIND SPEED
160 MPH
STORM MOVING
WNW 16 MPH
AT LEAST TWO DEAD AFTER POWERFUL EARTHQUAKE HIT
EARLY START

# Equifax Inc.

NYSE: EFX - 11 de set 19:59 GMT-4

**113,12** USD ↓10,11 (8,20%)

Após o horário comercial: 112,00 ↓0,99%

Um dia | Cinco dias | Um mês | Três meses | Um ano | Cinco anos | máx


| | | | |
|---|---|---|---|
| Abertura | 121,53 | Cap. merc. | 17,51 bi |
| Alta | 122,00 | Pr./lucro | 23,93 |
| Baixa | 111,17 | Rend. div. | 1,38% |

September 7, 2017 | Baird Equity Research
Information & Education Solutions

BAIRD

# Equifax Inc. (EFX)

## Announces Significant Data Breach; -13.4% in After-Hours

**Significant data breach obviously a material negative, but -13.4% after-hours seems like over-reaction** based on our understanding of events. Our understanding is data retained by EFX primarily generated through consumer interactions was breached via the Apache Struts flaw (i.e., core databases not believed to have been breached). We expect near-term operating headwinds plus material event-related expenses. However, we believe EFX's access to key data sources are unlikely to be affected, and client relationships and EFX's brand are unlikely to be meaningfully impaired intermediate to long term.

- **Data breach impacts ~143mn U.S. consumers, an event garnering widespread press/media attention.** Information accessed includes names, social security numbers, birth dates, addresses, and in some instances driver's license numbers. A smaller number of credit card numbers (209k), dispute documents (182k), and information on UK and Canadian residents also accessed.

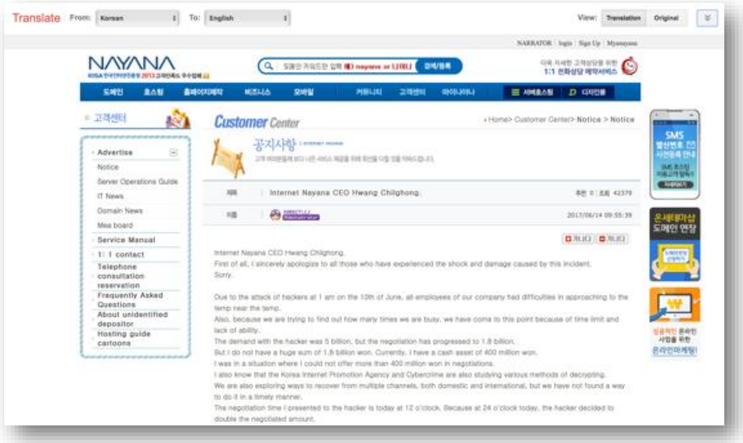
**LOWERING PRICE TARGET**

**1-Year Price Chart**


**Stock Data**

| | |
|---|---|
| Rating: | Outperform |
| Suitability: | Average Risk |
| Price Target/Previous: | ▼$141/$157 |


Abfahrt
Nach
Gleis
Zeit
Über
22:10 RB81 Flöha - Pockau-Lengefeld
Olbernhau
8
22:30 RB30
Hbf
11
22:31 RB30
(S) Hbf
10
22:36 RB80
g-B. Süd
8
9
22:36 RB45
5
22:44
14
Einsiedel - Thalheim (Erzgeb)
Aue (Sachs)
2:45
Dresden Hbf
11
Ooops, your files have been encrypted!
bitcoin

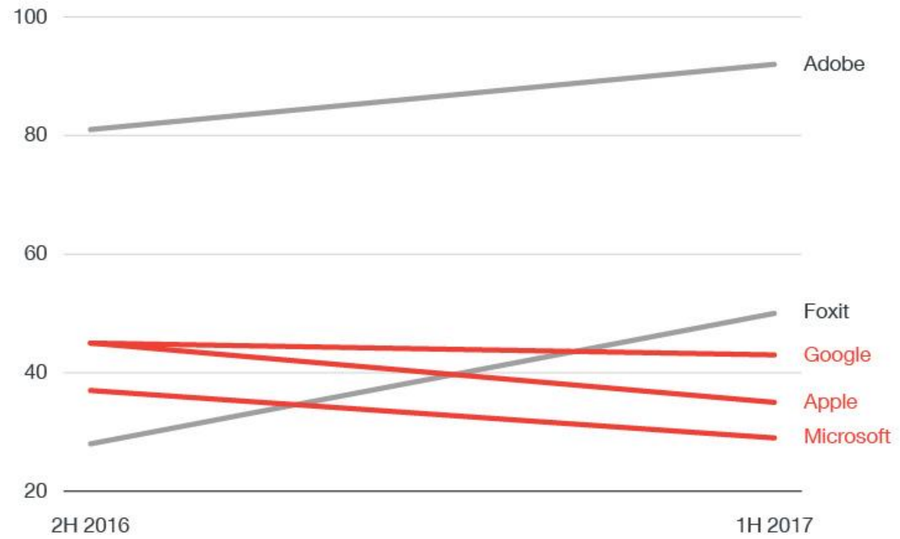

Translate
From: Korean
To: English
View: Translation Original
NAYANA
Customer Center
Home> Customer Center> Notice > Notice
Advertise
Notice
Server Operations Guide
IT News
Domain News
Mea board
Service Manual
1: 1 contact
Telephone consultation reservation
Frequently Asked Questions
About unidentified depositor
Hosting guide cartoons
공지사항
Internet Nayana CEO Hwang Chilghong.
2017/06/14 09:55:39
Internet Nayana CEO Hwang Chilghong.
First of all, I sincerely apologize to all those who have experienced the shock and damage caused by this incident.
Sorry.
Due to the attack of hackers at 1 am on the 10th of June, all employees of our company had difficulties in approaching to the temp near the temp.
Also, because we are trying to find out how many times we are busy, we have come to this point because of time limit and lack of ability.
The demand with the hacker was 5 billion, but the negotiation has progressed to 1.8 billion.
But I do not have a huge sum of 1.8 billion won. Currently, I have a cash asset of 400 million won.
I was in a situation where I could not offer more than 400 million won in negotiations.
I also know that the Korea Internet Promotion Agency and Cybercrime are also studying various methods of decrypting.
We are also exploring ways to recover from multiple channels, both domestic and international, but we have not found a way to do it in a timely manner.
The negotiation time I presented to the hacker is today at 12 o'clock. Because at 24 o'clock today, the hacker decided to double the negotiated amount.


DEVELOPING THIS MORNING
GIANT DATA BREACH COULD HIT 143 MILLION PEOPLE
Credit reporting firm Equifax says hackers stole personal info
LIVE
CNN
12:24 AM PT
HURRICANE IRMA
CATEGORY 5
WIND SPEED
160 MPH
STORM MOVING
WNW 16 MPH
AT LEAST TWO DEAD AFTER POWERFUL EARTHQUAKE HIT
EARLY START

# Novos ataques, velhas vulnerabilidades

# Menos vulnerabilidades dos principais fabricantes

| 2H 2016 | | 1H 2017 | |
|---|---|---|---|
| **Adobe** | 81 | Adobe | 92 |
| **Google** | 45 | Google | 43 |
| **Apple** | 45 | Apple | 35 |
| **Microsoft** | 37 | Microsoft | 29 |
| **Foxit** | 28 | Foxit | 50 |



# A história por trás da maior vulnerabilidade de 2017

| | |
|---|---|
| MARÇO | Microsoft lança o patch para CVE-2017-0144 |
| ABRIL | EternalBlue lançado pelo Shadow Brokers |
| MAIO | Ataque do WannaCry usando EternalBlue |
| JUNHO | Ataque do Petya usando EternalBlue |

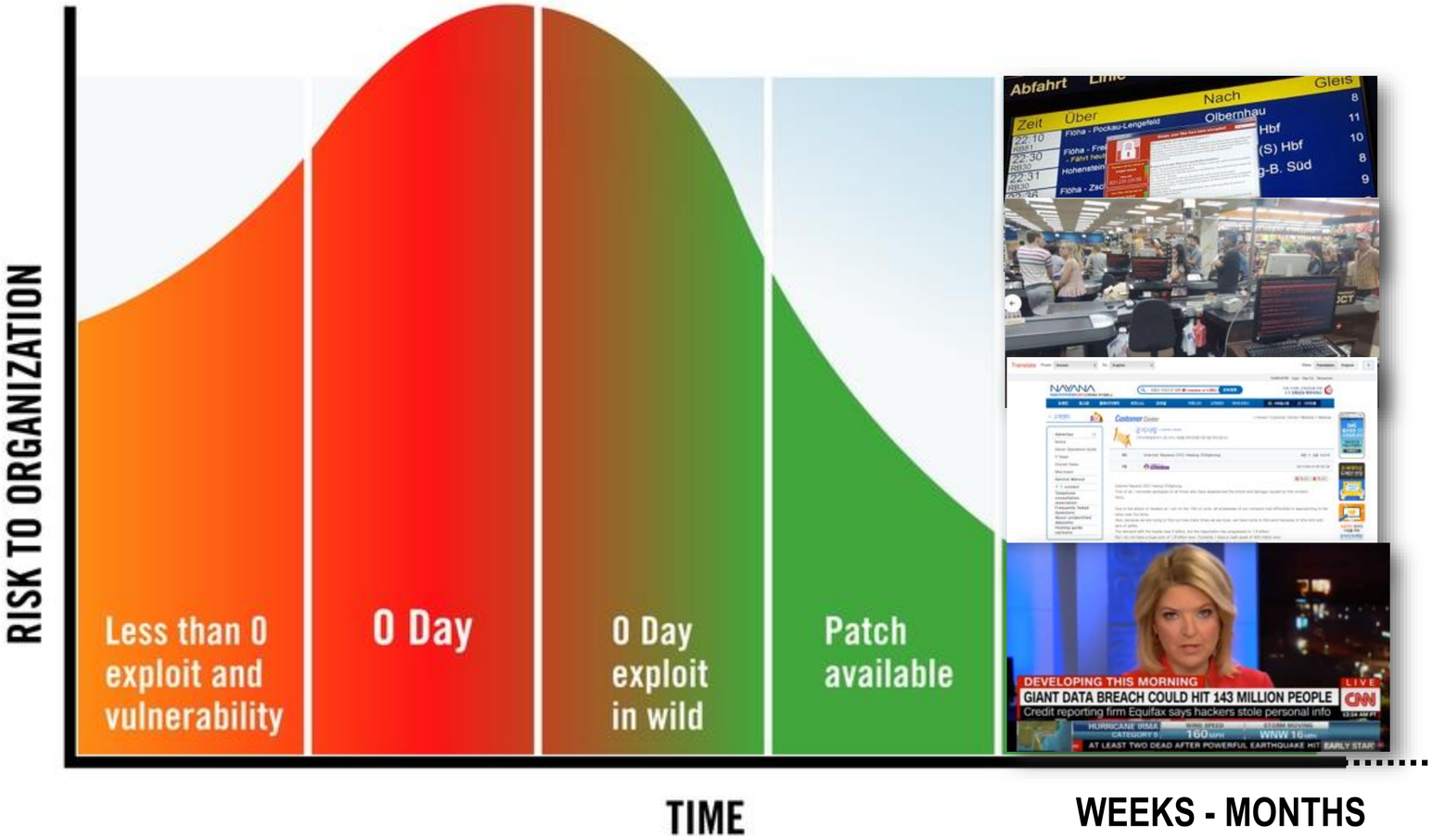
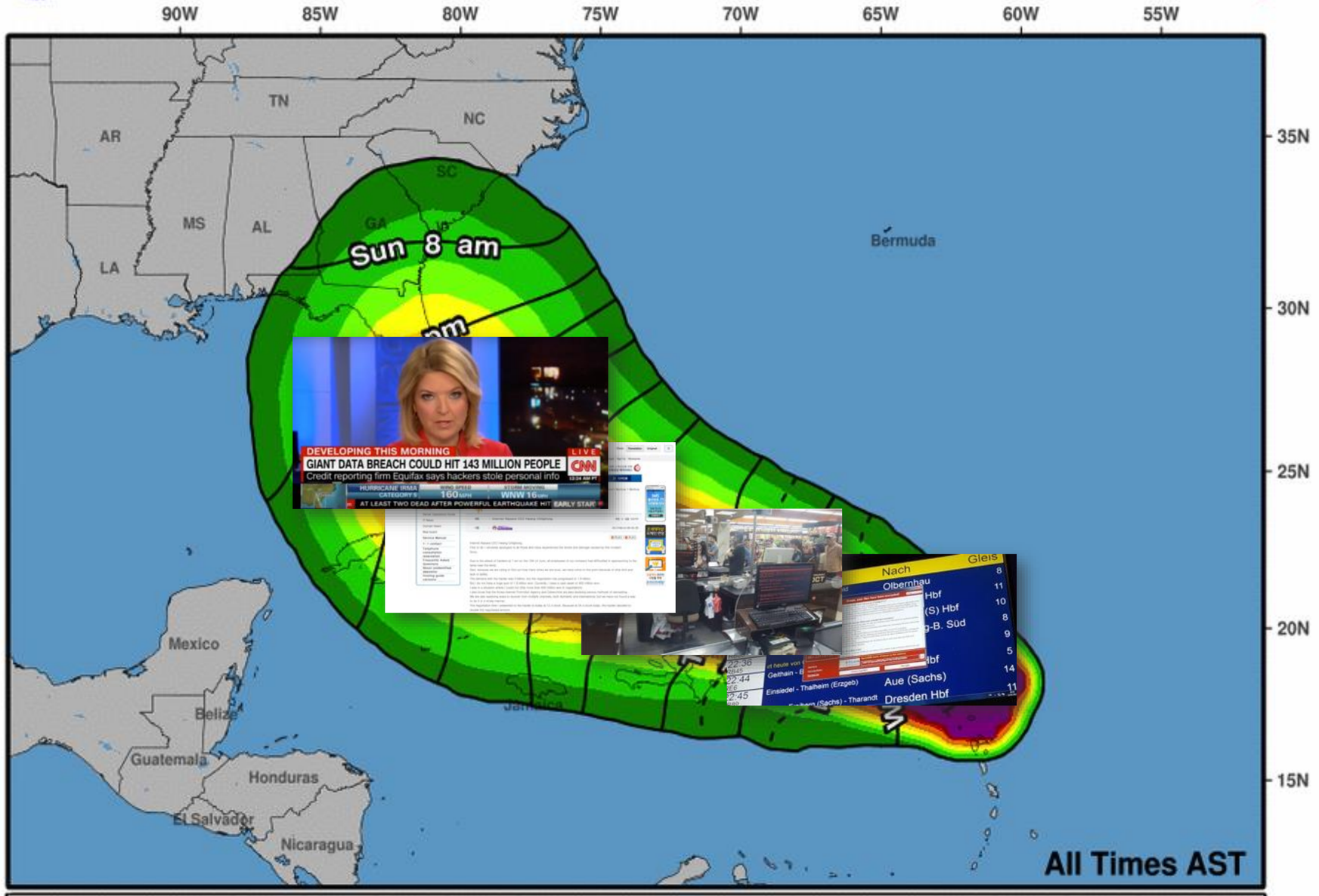



Chart source: http://www.ashimmy.com/less_than_zero/

# Earliest Reasonable Arrival Time of Tropical-Storm-Force Winds



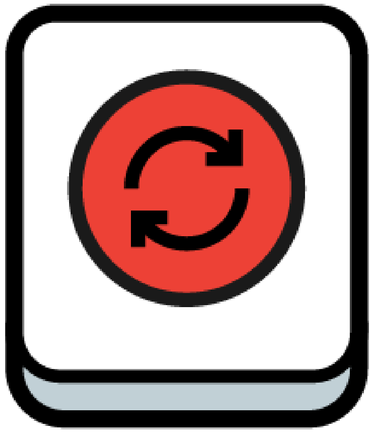

**Hurricane Irma**
**Wed. Sep. 6, 2017 5 am AST**
**Advisory 29**

**Storm Location & Wind Speed (knots)**
○ <34 ◔ 34-63 ● ≥64

**Five-day chance of receiving sustained 34+ knot (39+ mph) winds**

5 10 20 30 40 50 60 70 80 90 100 %

# Proteção contra vulnerabilidades



Mantenha software e apps atualizados

Medidas proativas como blindagem de vulnerabilidades

# Crescimento de ransomware para mas cibercriminosos diversificam


# Número médio de novas famílias de ransomware em 1H de 2017

# Maiores ataques de ransomware em 2017

## WannaCry

- Infects machines with an open port 445 and spreads through local networks and the internet

## Petya

- Spreads to Windows XP machines
- Encrypts Master File Table and deletes key

# Cybercriminals Diversifying Into New Attack Methods

**Cerber**

Avoids detection from machine learning solutions

**SLocker**

Encrypts files rather than lockscreen

# Ransomware Overview

67% tied to email with malicious attachment/URLs

29% tied to malicious websites

4% are actual ransomware files

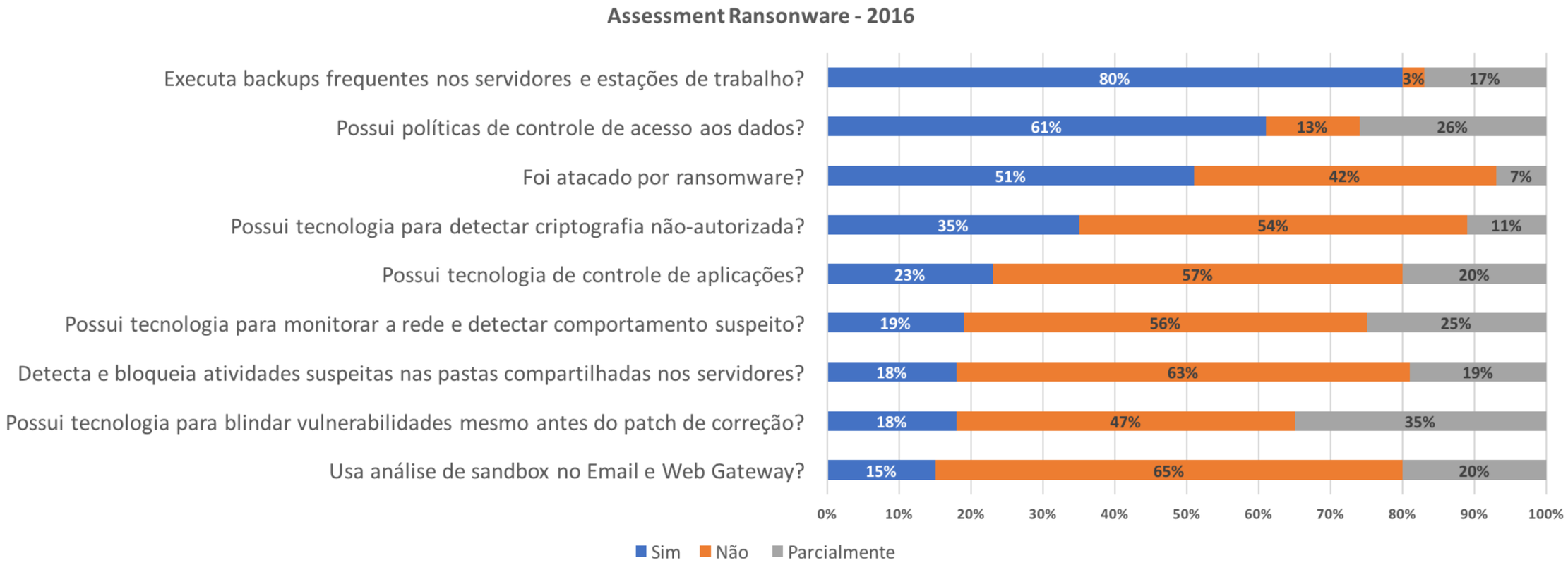
# Cenário América Latina…

# Latin America

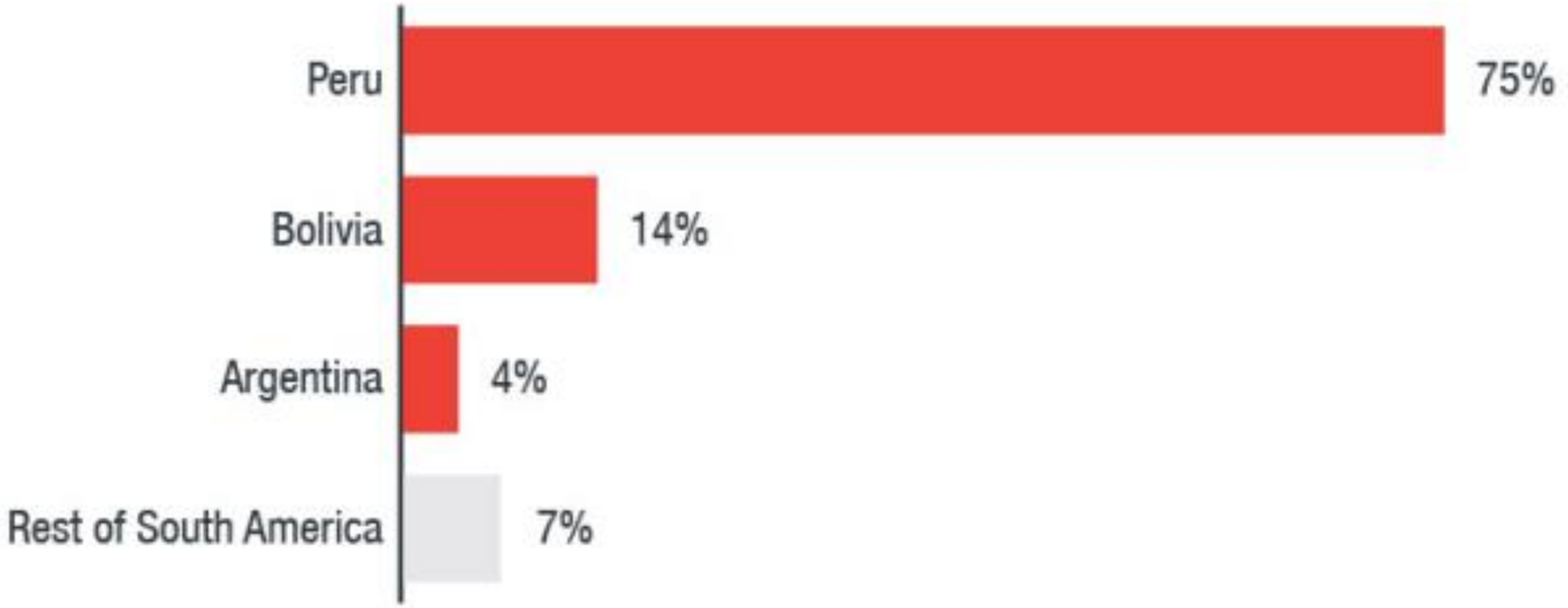
| Threats Detected | Presence |
|---|---|
| Known Malware? | 97% |
| Conficker/Downad? | 50% |
| Unknown Malware/Zero-Day? | 69% |
| Android Malware? | 34% |
| Malware for MAC OS? | 8% |
| Malicious Documents? | 85% |
| C&C Communications (Botnet)? | 90% |
| Data leak activity? | 25% |
| Unauthorized applications? | 80% |
| Targeted Malware/APT? | 23% |
| Cloud Storage services? | 51% |
| Network Attacks or Exploits? | 83% |

**Source:** 331 PoVs in Latin America, from 2013 to September of 2017.

# Ransomware - Latin America

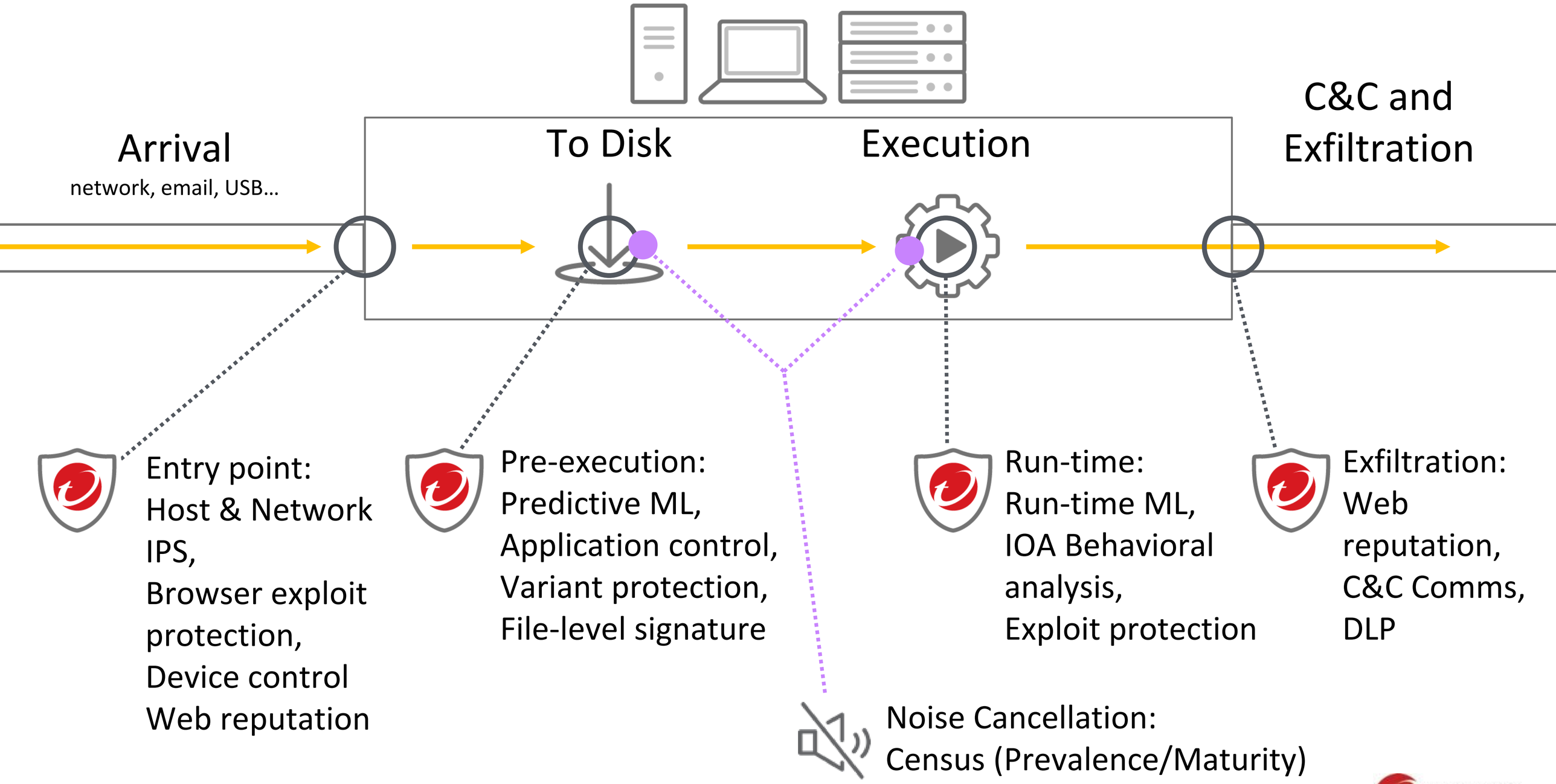


# New RETADUP Variants Hit South America, Turn To Cryptocurrency Mining

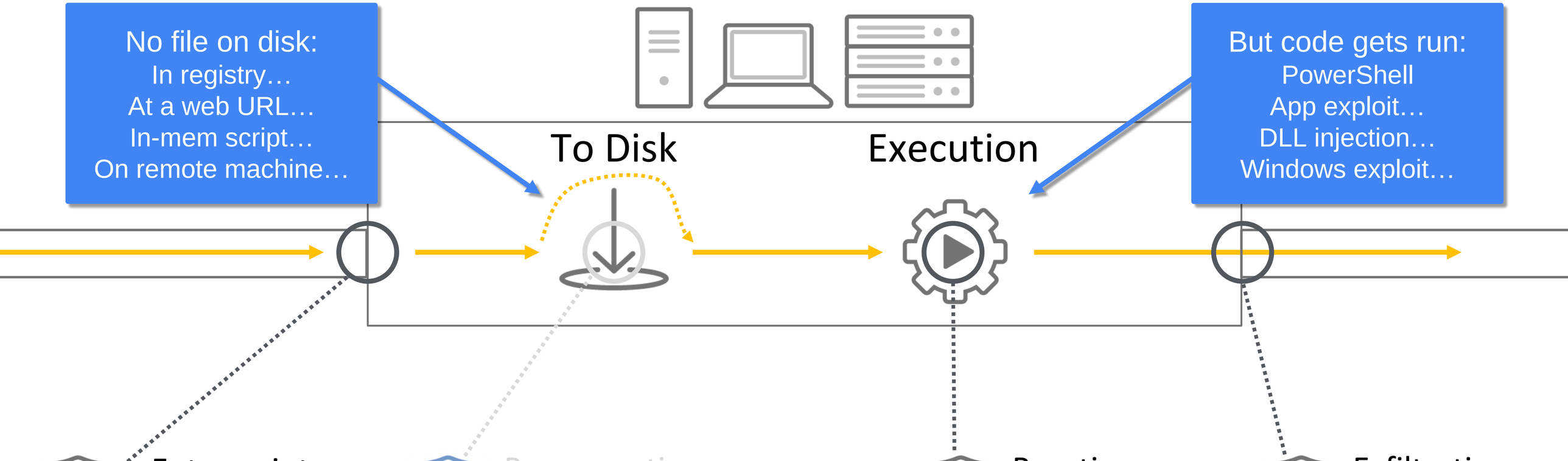



Source: *Distribution of victims in South America.*

# E os desafios de amanhã?



# Defending Against Fileless Malware



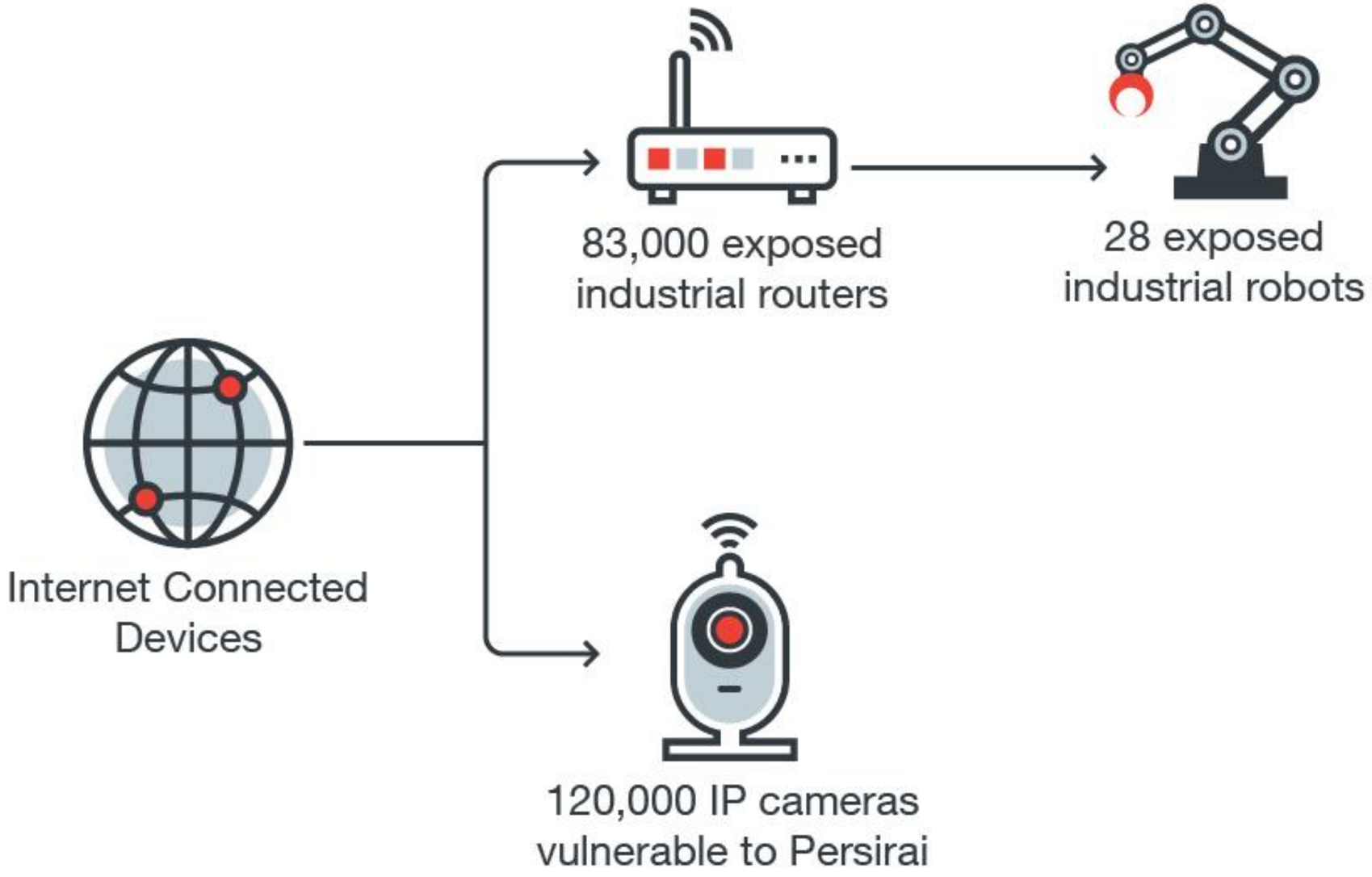

Entry point:
Host IPS,
Browser exploit protection,
Device control
Web reputation

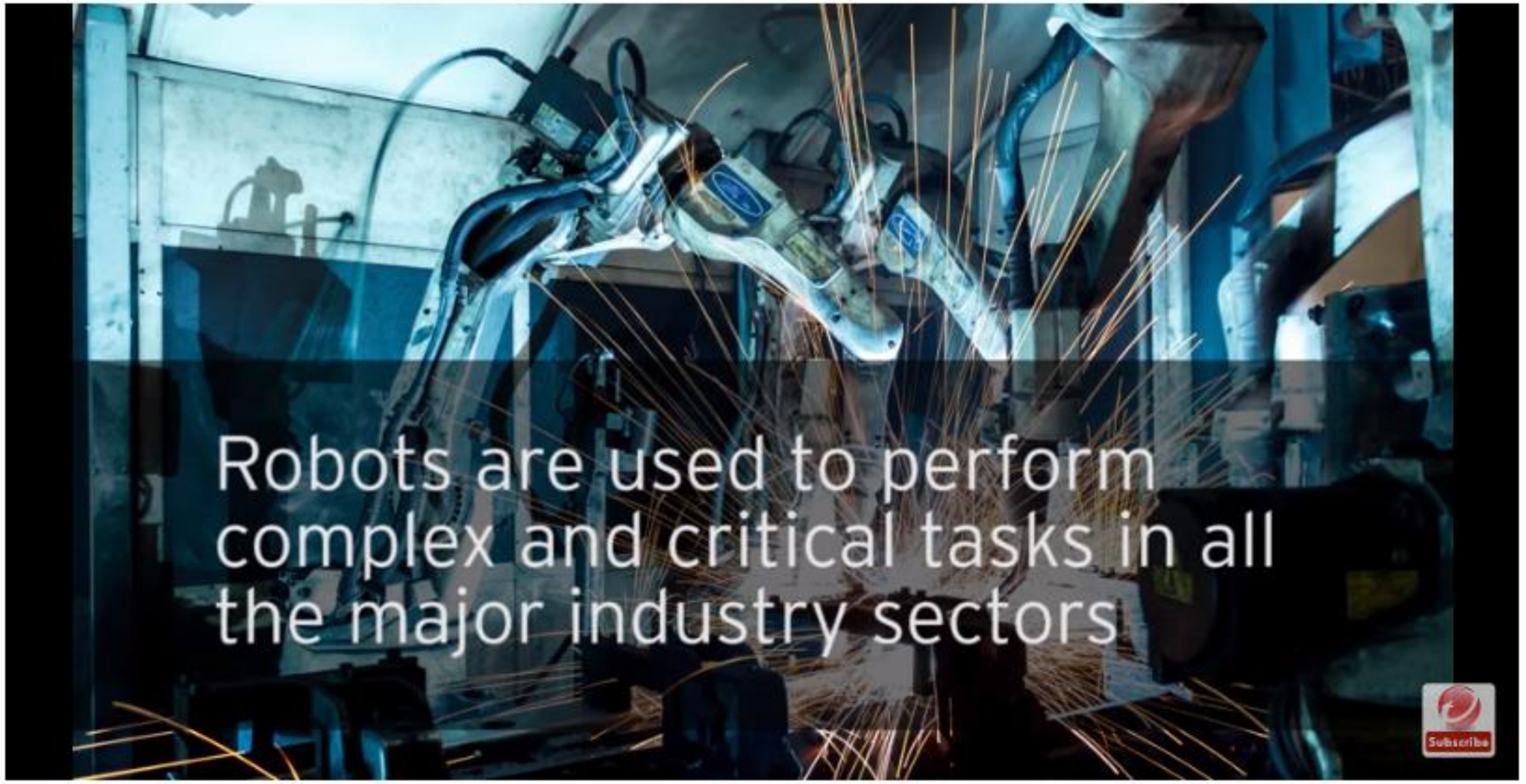
Pre-execution:
Predictive ML,
Application control,
Variant protection,
File-level signature

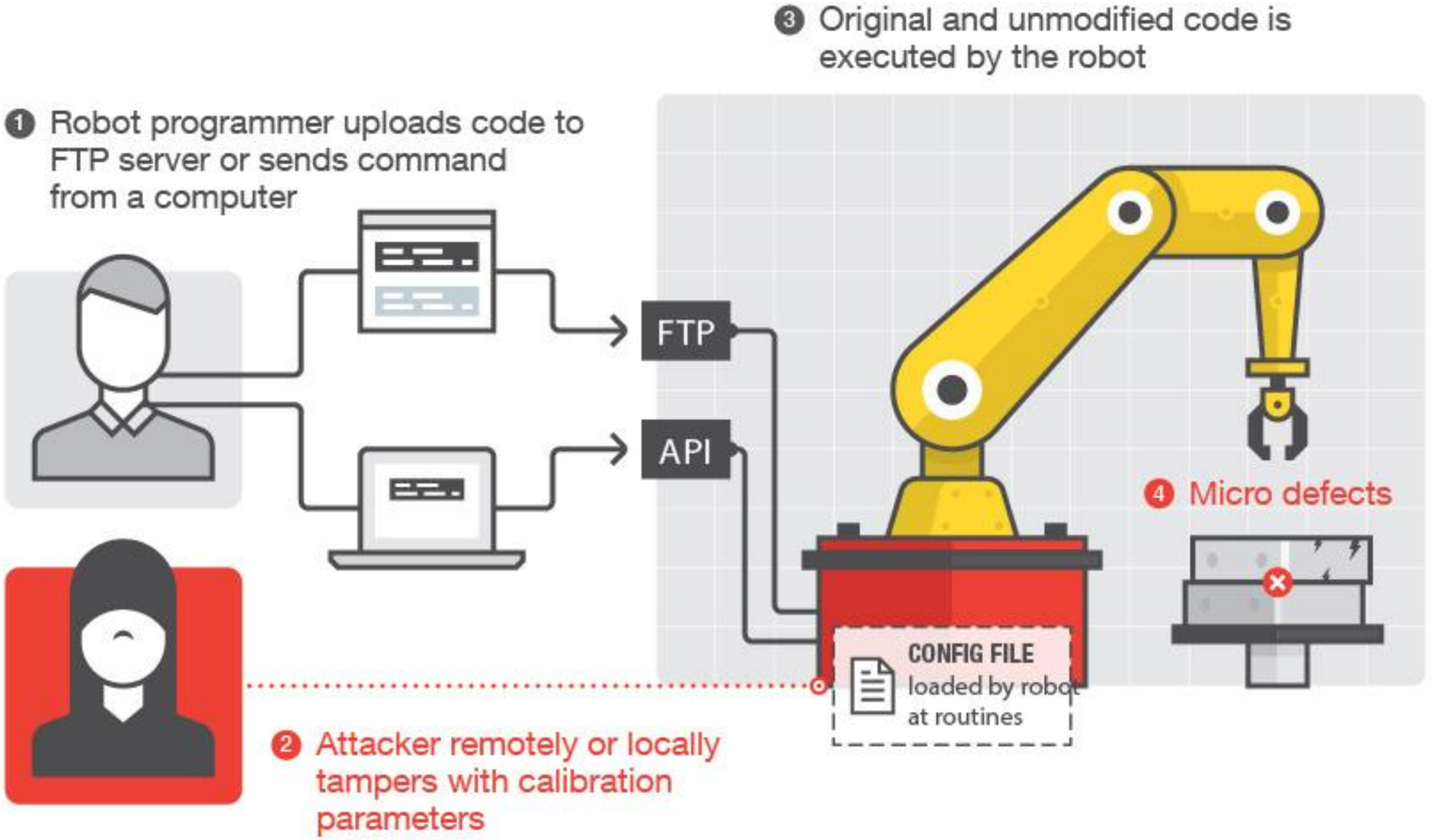
Run-time:
Run-time ML,
IOA Behavioral analysis,
Exploit protection

Exfiltration:
Web reputation,
C&C Comms,
DLP

# Connected Devices Put Smart Life at Risk


83,000 exposed
industrial routers
28 exposed
industrial robots
Internet Connected
Devices
120,000 IP cameras
vulnerable to Persirai


Robots are used to perform complex and critical tasks in all the major industry sectors
Subscribe


3 Original and unmodified code is executed by the robot
1 Robot programmer uploads code to FTP server or sends command from a computer
FTP
API
4 Micro defects
CONFIG FILE
loaded by robot at routines
2 Attacker remotely or locally tampers with calibration parameters

# Advisory (ICSMA-17-241-01)

More Advisories

## Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities

Original release date: August 29, 2017



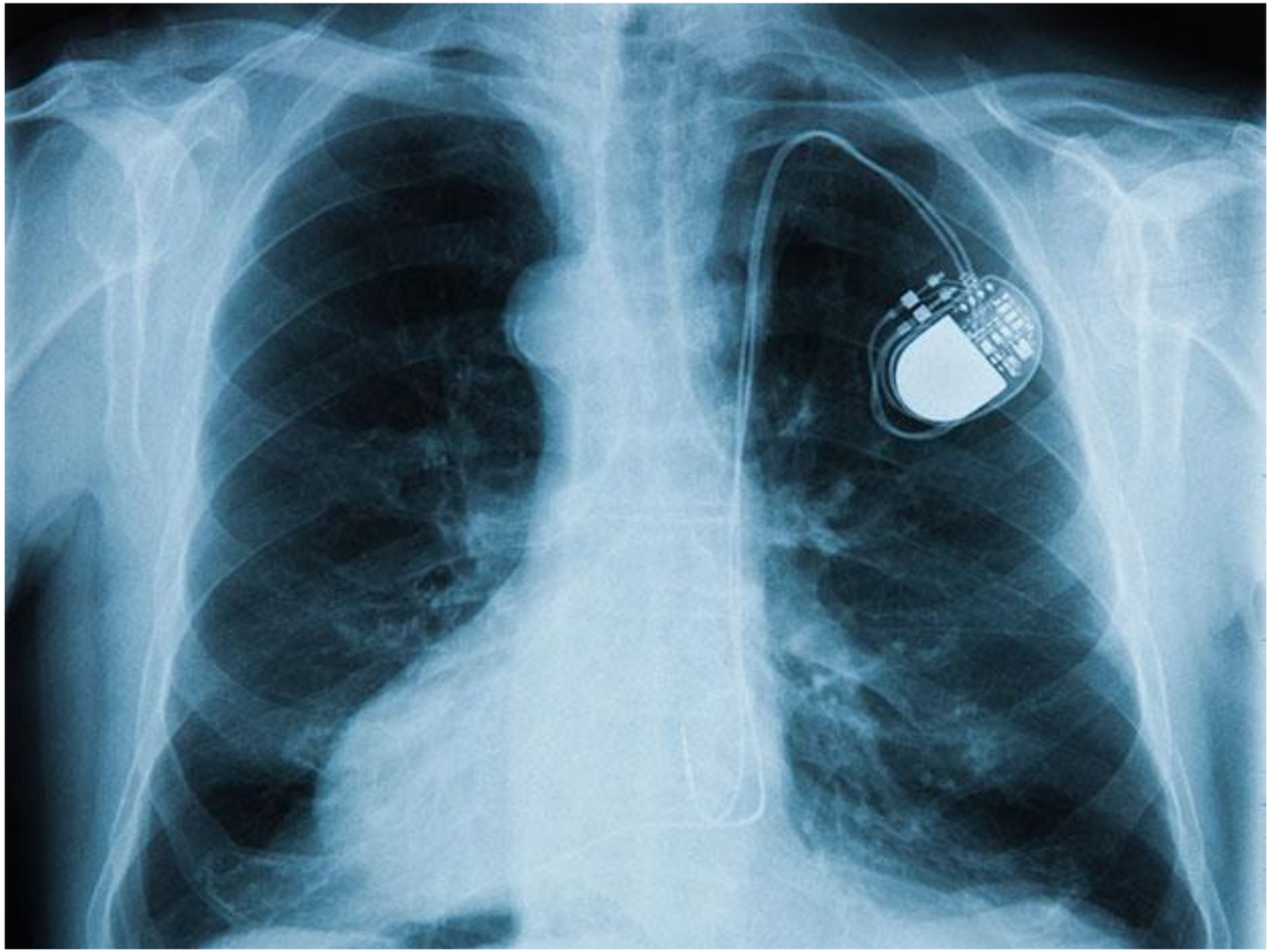
### Legal Notice



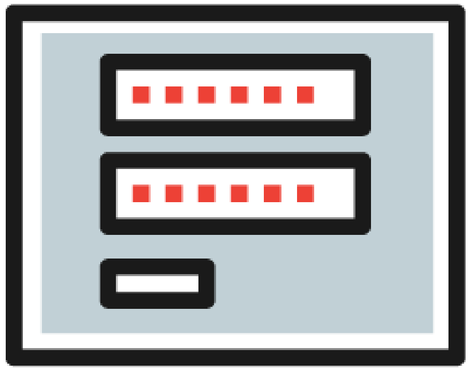
## OVERVIEW

MedSec Holdings Ltd has identified vulnerabilities in Abbott Laboratories' (formerly St. Jude Medical) pacemakers. Abbott has produced a firmware patch to help mitigate the identified vulnerabilities in their pacemakers that utilize radio frequency (RF) communications. A third-party security research firm has verified that the new firmware version mitigates the identified vulnerabilities.


IS-1
ST. JUDE MEDICAL
Sylmar, CA USA
VICTORY™ SR
5610 SSIR
S/N 1723182

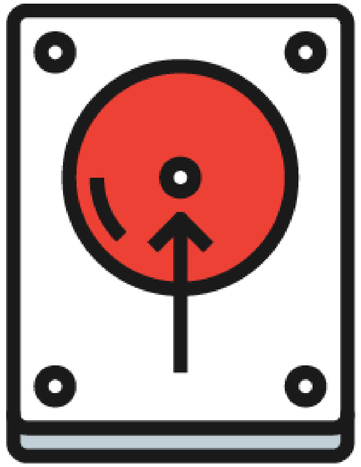


# Protection Against IoT Threats



For users: Change the default passwords of IoT devices

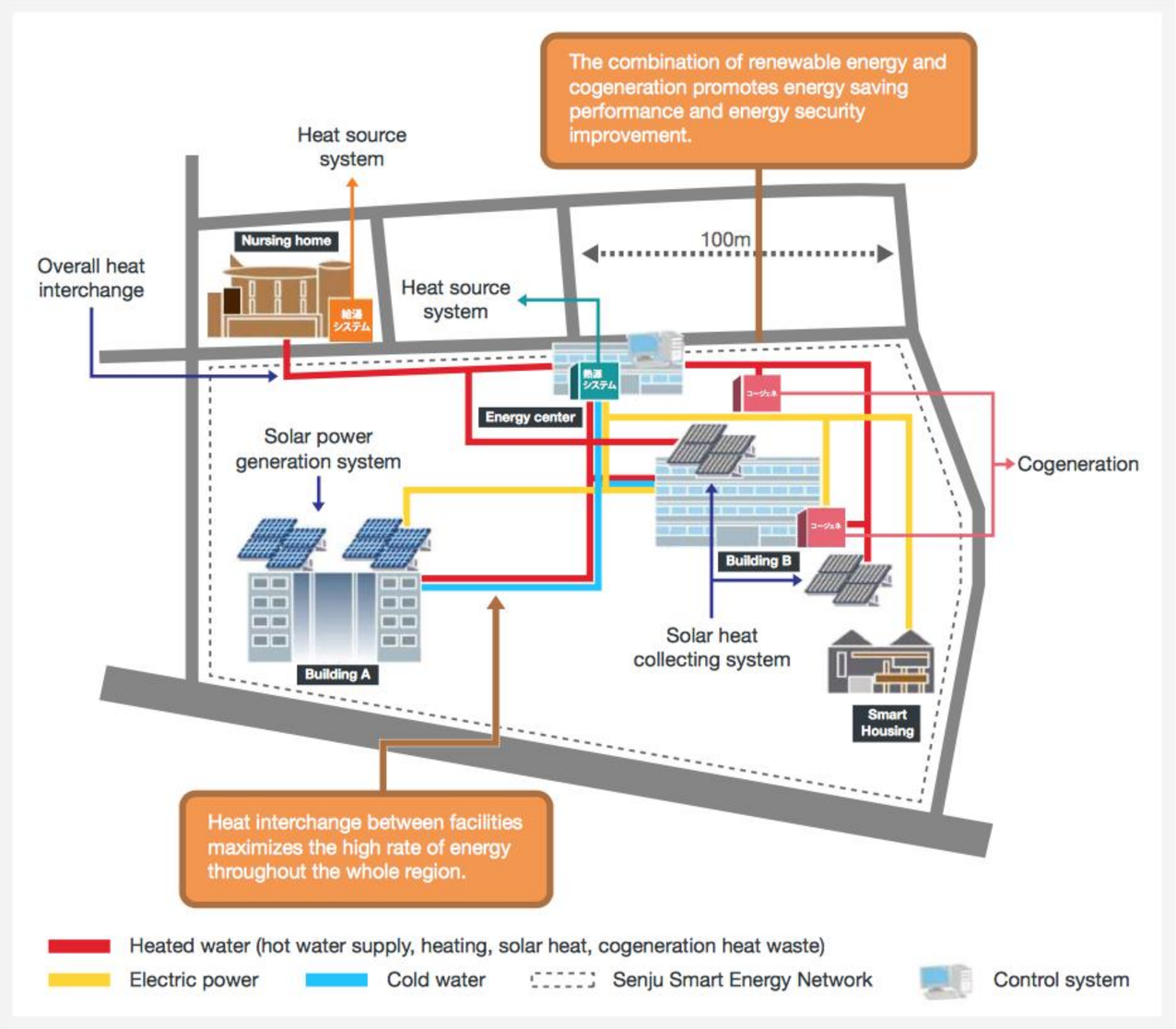
For the manufacturers: Fix vulnerabilities at SDK level



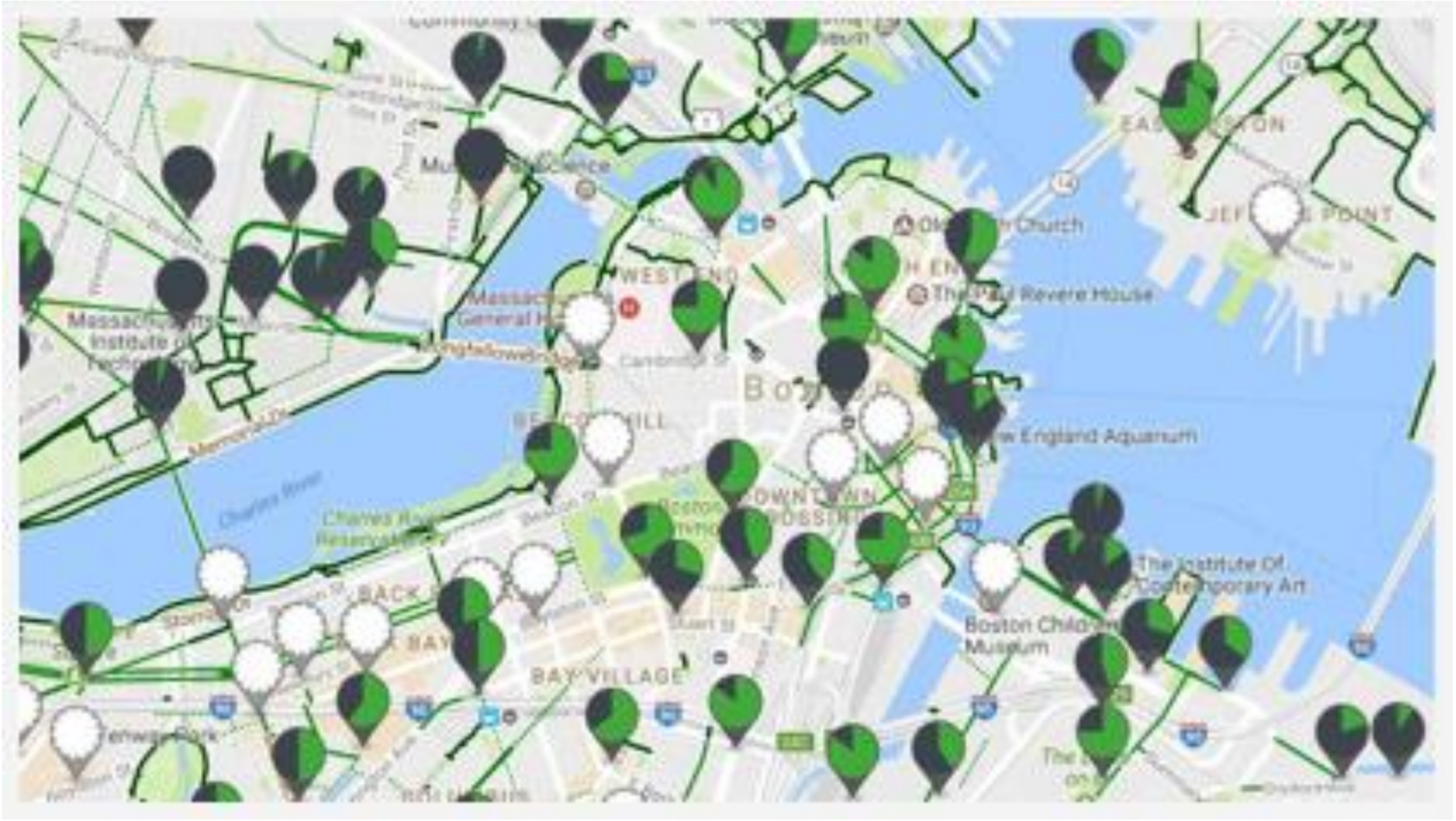
For enterprises: Create backup/restore policies in case of DDoS attacks

# Smart Cities and cybersecurity

# Smart energy



# Smart transportation



# Smart environment

# Smart connectivity

# Smart governance

# BEC Losses Reach $5 Billion Mark

# FBI Statistics

| | 2H 2016 | 1H 2017 |
|---|---|---|
| Running total | $ 3B | $5.3B |

# BEC Overview

**Most targeted countries:**

U.S.
Australia
U.K.

**Most spoofed/targeted position:**

CEO/CFO

**BEC attempts globally in 1H 2017**

3,175

# BEC Overview

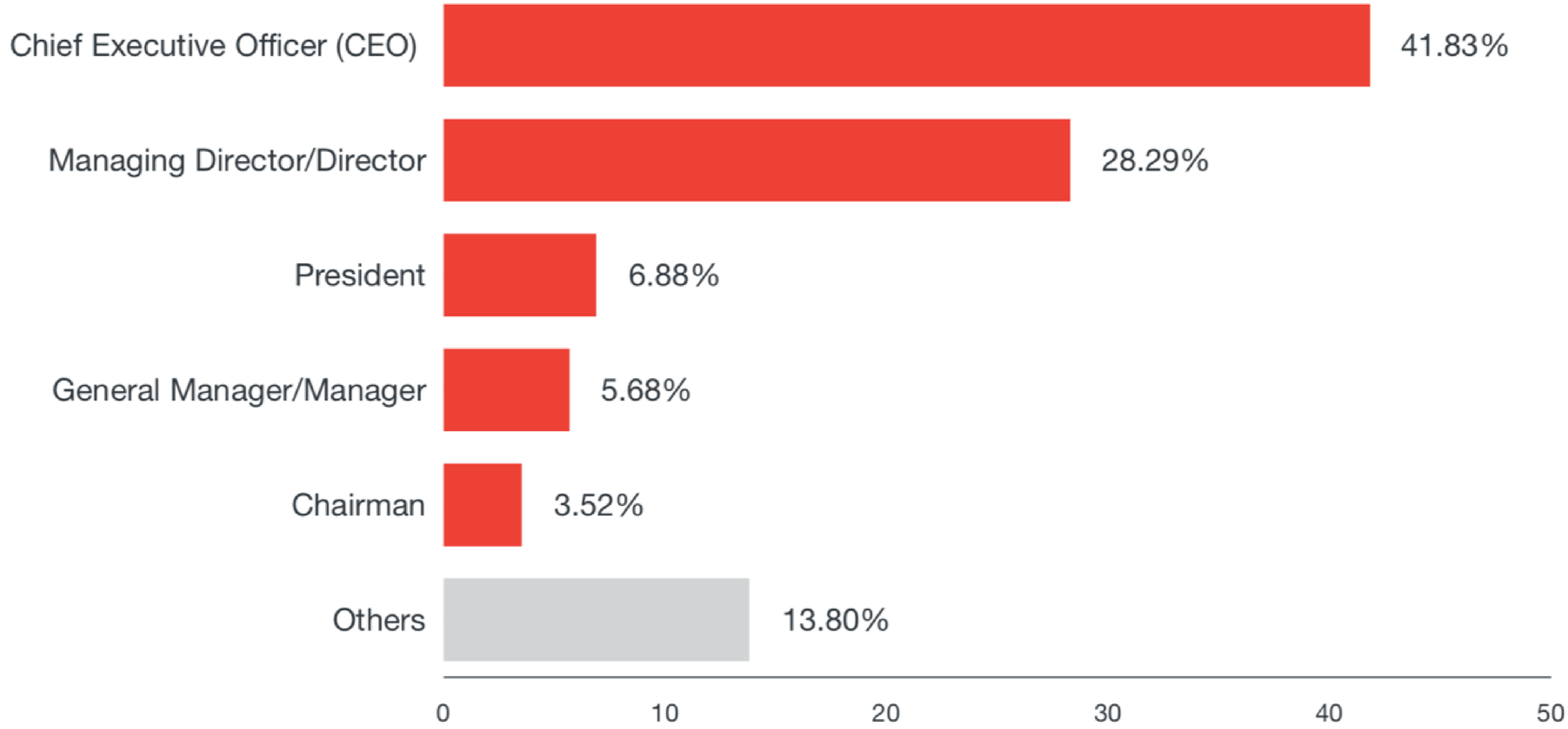
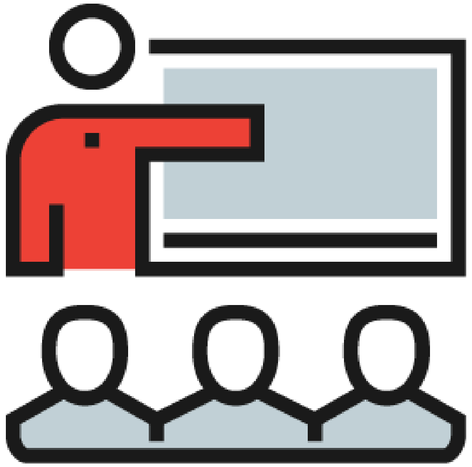



Figure 6. Percentage of BEC attack attempts that spoof specific positions, 1H 2017

# Protection Against BEC Scams



Raise employee awareness on how the scam works

Prevent social engineering attacks

# …but Email is not the only Business Compromise

# Hacking Is Now the Main Cause of Data Breach

# Protection Against Data Breaches

Classify high-value assets or core data (crown jewels)

Know the indicators of compromise (IoCs) of known attacks


Cybersecurity is becoming
more and more relevant


WORLD
ECONOMIC
FORUM

# The Global Risks Report 2017

General Data
Protection Regulation

# Perguntas?

# Obrigado!

Perguntas ou acompanhamento?

**Franzvitor_Fiorim@trendmicro.com** | Franzvitor Fiorim, Diretor Técnico Brasil