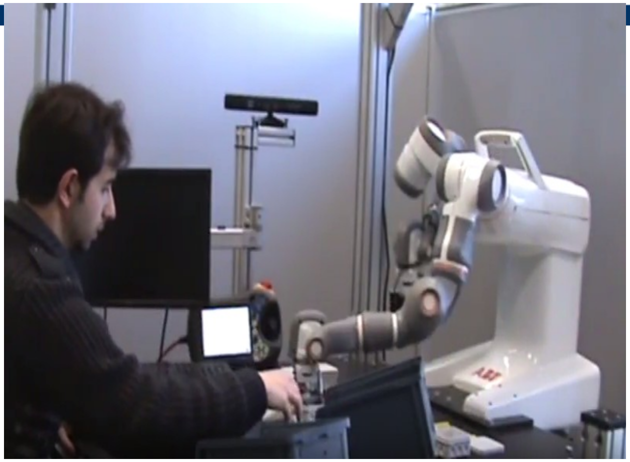
POLITECNICO DI MILANO

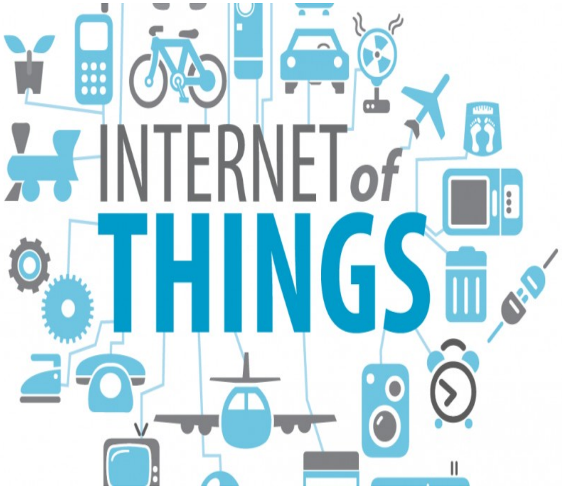
# Cybersecurity in a changing world

Stefano Zanero, PhD

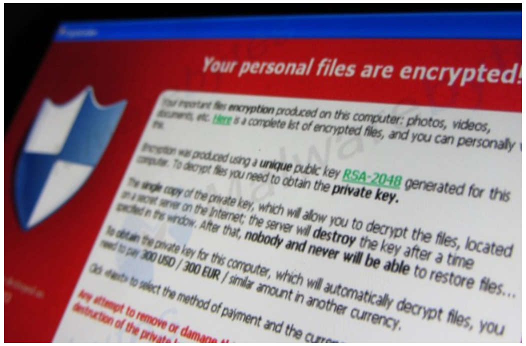
Associate Professor, Politecnico di Milano

# The iper-connected future





# Upcoming threats



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally ... this.

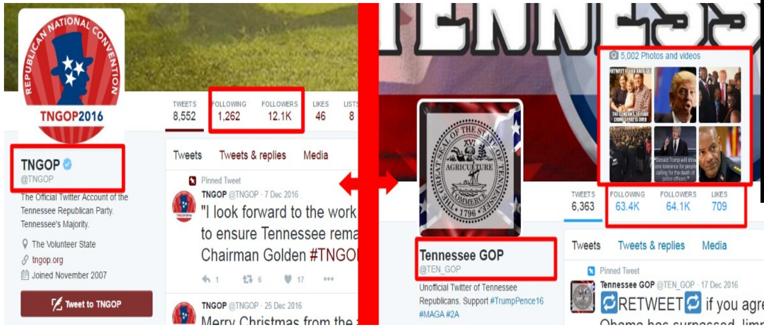
Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single** copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click «Next» to select the method of payment and the curren...

Any attempt to remove or damage th... destruction of the private k...



TNGOP2016

TNGOP @TNGOP

The Official Twitter Account of the Tennessee Republican Party. Tennessee's Majority.

The Volunteer State

tngop.org

Joined November 2007

Tweet to TNGOP

| TWEETS | FOLLOWING | FOLLOWERS | LIKES | LISTS |
|---|---|---|---|---|
| 8,552 | 1,262 | 12.1K | 46 | 8 |

Tweets Tweets & replies Media

Pinned Tweet

TNGOP @TNGOP · 7 Dec 2016

"I look forward to the work ... to ensure Tennessee rema... Chairman Golden #TNGO...

1 6 17

TNGOP @TNGOP · 25 Dec 2016

Merry Christmas from the ...

Tennessee GOP @TEN_GOP

Unofficial Twitter of Tennessee Republicans. Support #TrumpPence16 #MAGA #2A

5,002 Photos and videos

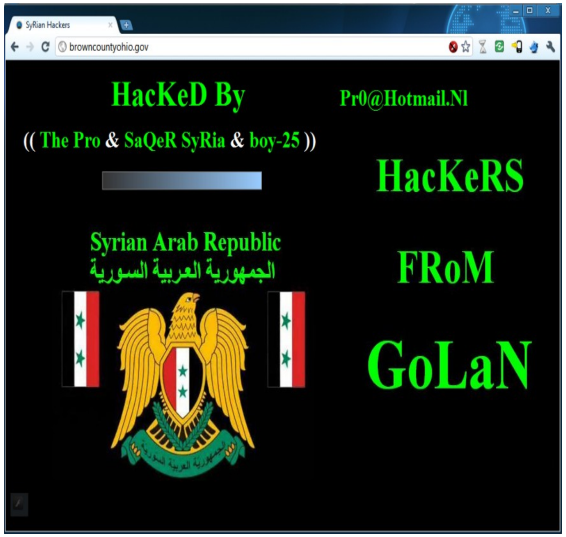
| TWEETS | FOLLOWING | FOLLOWERS | LIKES |
|---|---|---|---|
| 6,363 | 63.4K | 64.1K | 709 |

Tweets Tweets & replies Media

Pinned Tweet

Tennessee GOP @TEN_GOP · 17 Dec 2016

RETWEET if you agree Barack Obama has surpassed Jimmy Carter as ...



SyRian Hackers

browncountyohio.gov

HacKeD By Pr0@Hotmail.Nl

(( The Pro & SaQeR SyRia & boy-25 ))

HacKeRS

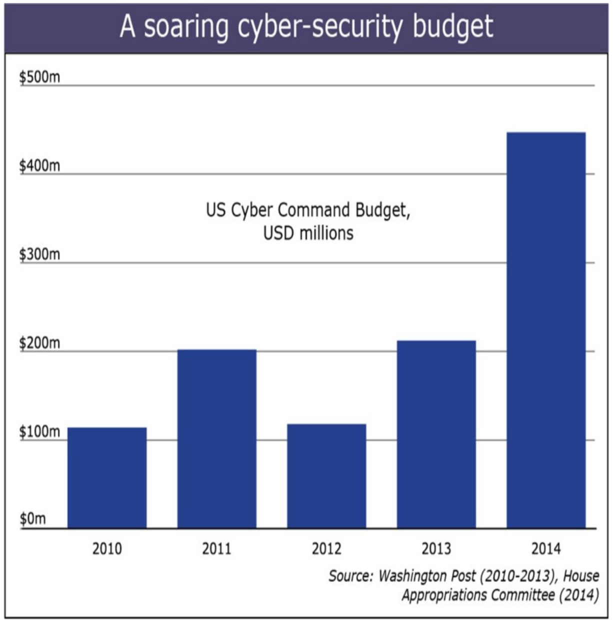
FRoM

GoLaN

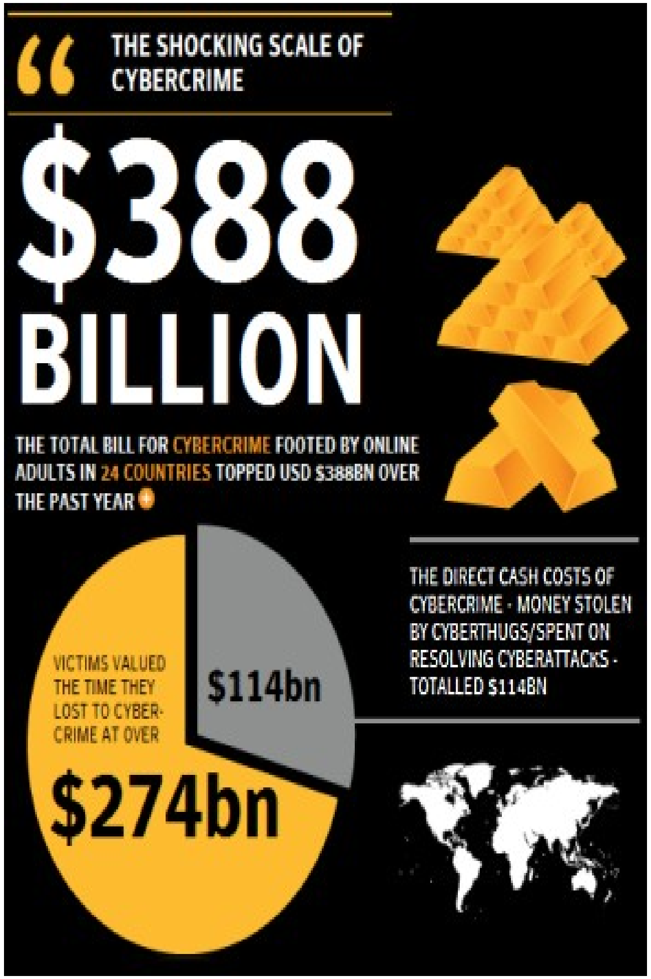
Syrian Arab Republic

الجمهورية العربية السورية

# Costs and damage


A soaring cyber-security budget

Source: Washington Post (2010-2013), House Appropriations Committee (2014)


THE SHOCKING SCALE OF CYBERCRIME

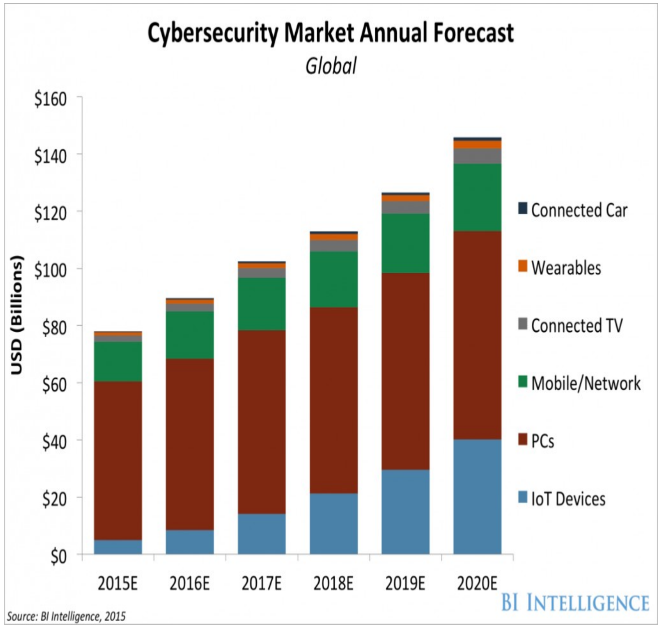
$388 BILLION

THE TOTAL BILL FOR CYBERCRIME FOOTED BY ONLINE ADULTS IN 24 COUNTRIES TOPPED USD $388BN OVER THE PAST YEAR

VICTIMS VALUED THE TIME THEY LOST TO CYBER-CRIME AT OVER $274bn

$114bn

THE DIRECT CASH COSTS OF CYBERCRIME - MONEY STOLEN BY CYBERTHUGS/SPENT ON RESOLVING CYBERATTACKS - TOTALLED $114BN


Cybersecurity Market Annual Forecast

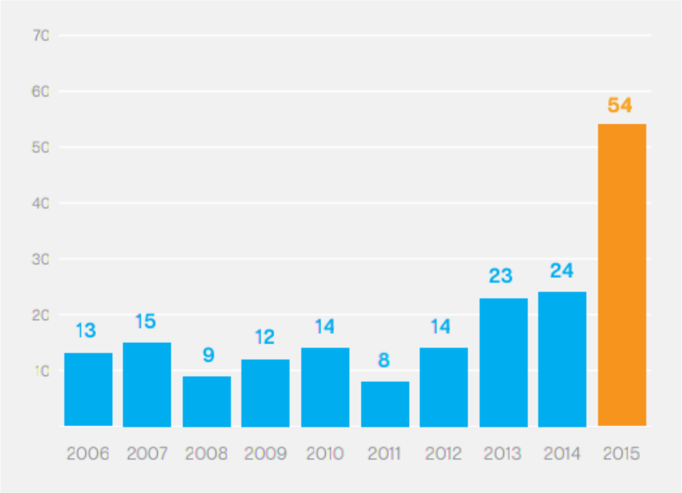
*Global*

Source: BI Intelligence, 2015

# Phishing, spear phishing, and the most important vulnerability...

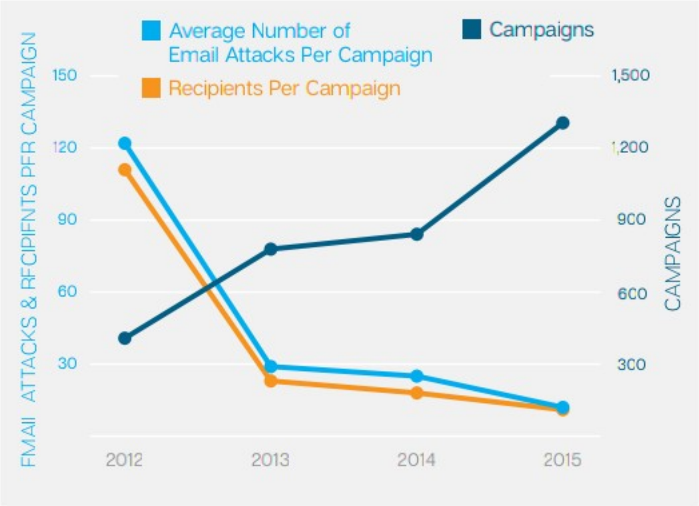
## Zero-Day Vulnerabilities, Annual Total

▶ *The highest number of zero-day vulnerabilities was disclosed in 2015, evidence of the maturing market for research in this area.*



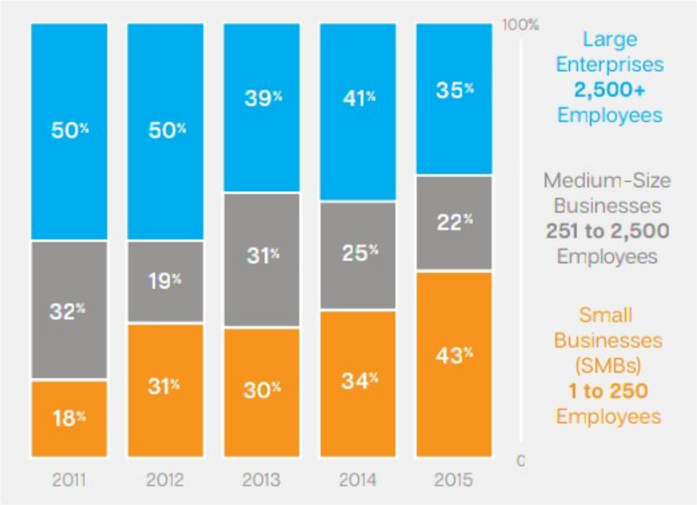
## Spear-Phishing Email Campaigns

▶ *In 2015, the number of campaigns increased, while the number of attacks and the number of recipients within each campaign continued to fall. With the length of time shortening, it's clear that these types of attacks are becoming stealthier.*



## Spear-Phishing Attacks by Size of Targeted Organization

▶ *Attacks against small businesses continued to grow in 2015, although many of these attacks were directed to fewer organizations, increasing by 9 percentage points.*



Source: Symantec Internet Security Threat Report 2016

# The underground economy

- The underground financial fraud community has become increasingly organized, facilitating an expanded reach
- Anyone, independently from their skill level, can buy a malware builder and create a customized sample
- The price depends on the features of the trojans, typically starting from 100$ for an old, leaked version, to about 3,000$ for a new complete version
- Cybercriminals also offer paid support and customization, or sell advanced configuration files that the end users can include in their custom builds
- Compromised banking accounts are traded for five to ten percent of their current balance

# Information Stealers: an overview

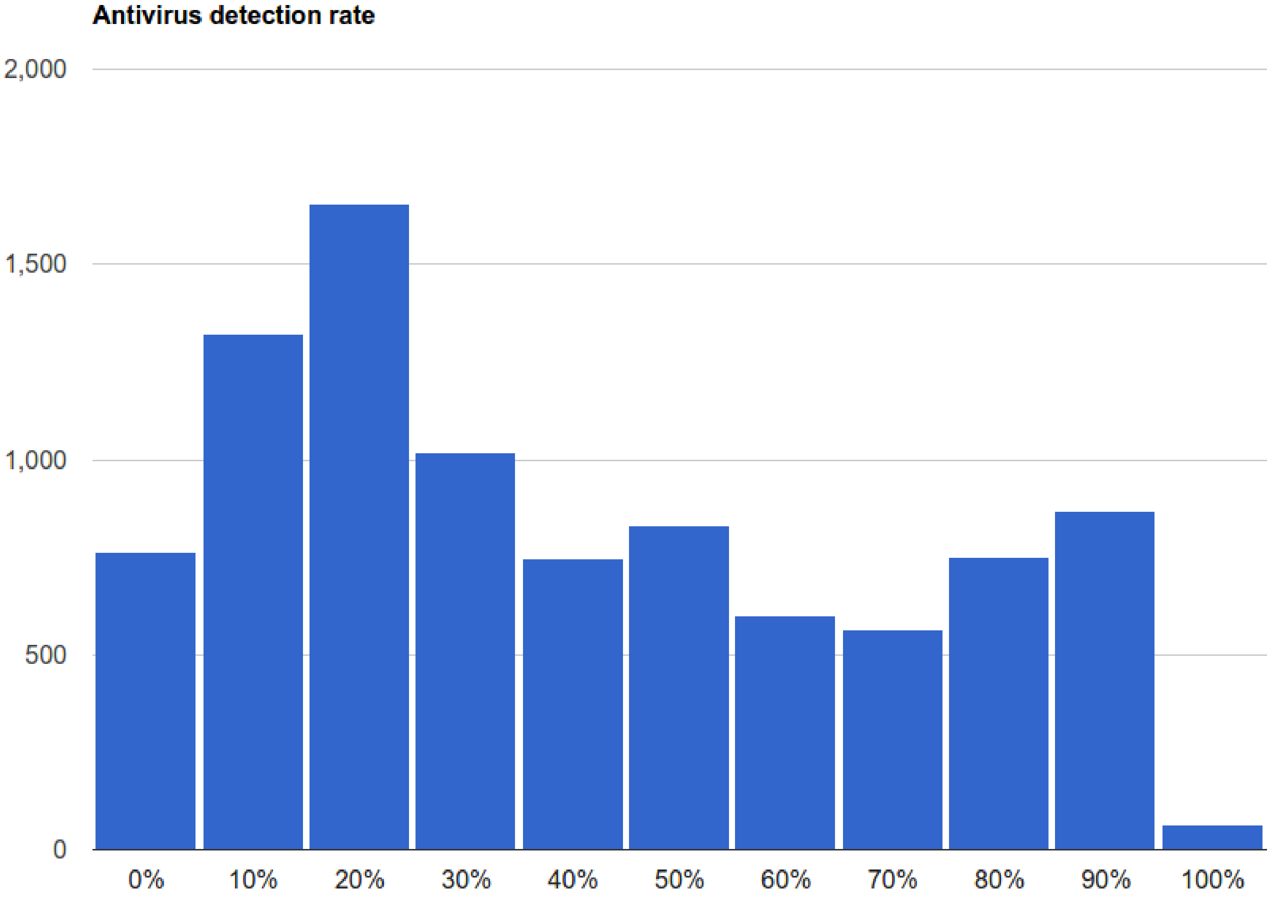
- What they are:
  - ✓Malware that steal credentials such as usernames, passwords, and second factors of authentication
  - ✓They are also named “banking trojans”, because they are often used to steal banking credentials and perform online financial frauds

- ZeuS (2007), SpyEye (2011), Citadel (2012), are the most notorious

- What they do:
  - ✓Steal private information submitted to web forms
  - ✓Harvest and steal files
  - ✓Hijack browser session
  - ✓Use the victim as a proxy

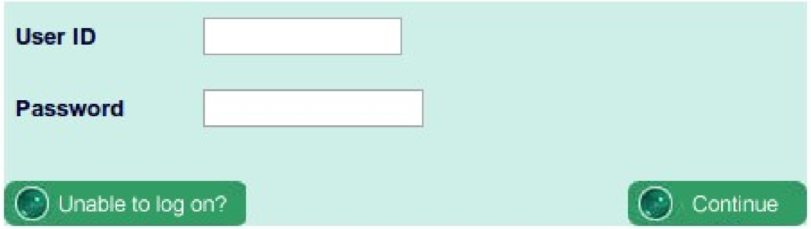
# AV Detection Rate

Low detection rate: as of yesterday, according to ZeuS Tracker the overall detection rate is 40.04%



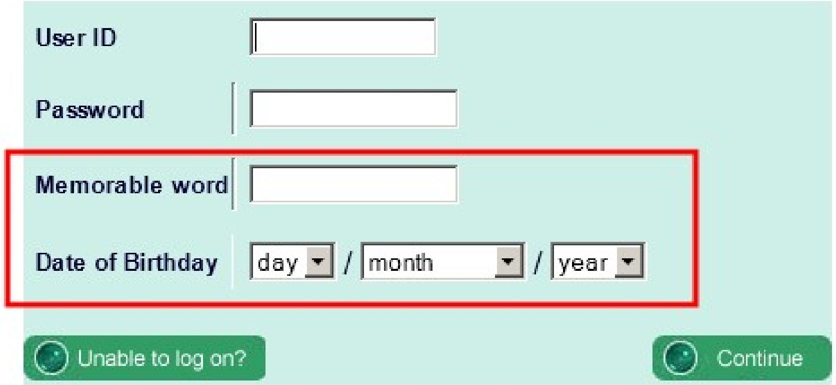
# Man in the Browser and WebInject

- Info-stealing trojans exploit API hooking techniques to be able to intercept all the data going through the browser even when the connection is encrypted (Man in the Browser attacks)
- They also contain a module called WebInject able to manipulate and modify web pages injecting new content
- The goal is to make the victim believe that the web page is legitimately asking for the second factor of authentication or any other private information



User ID

Password



User ID

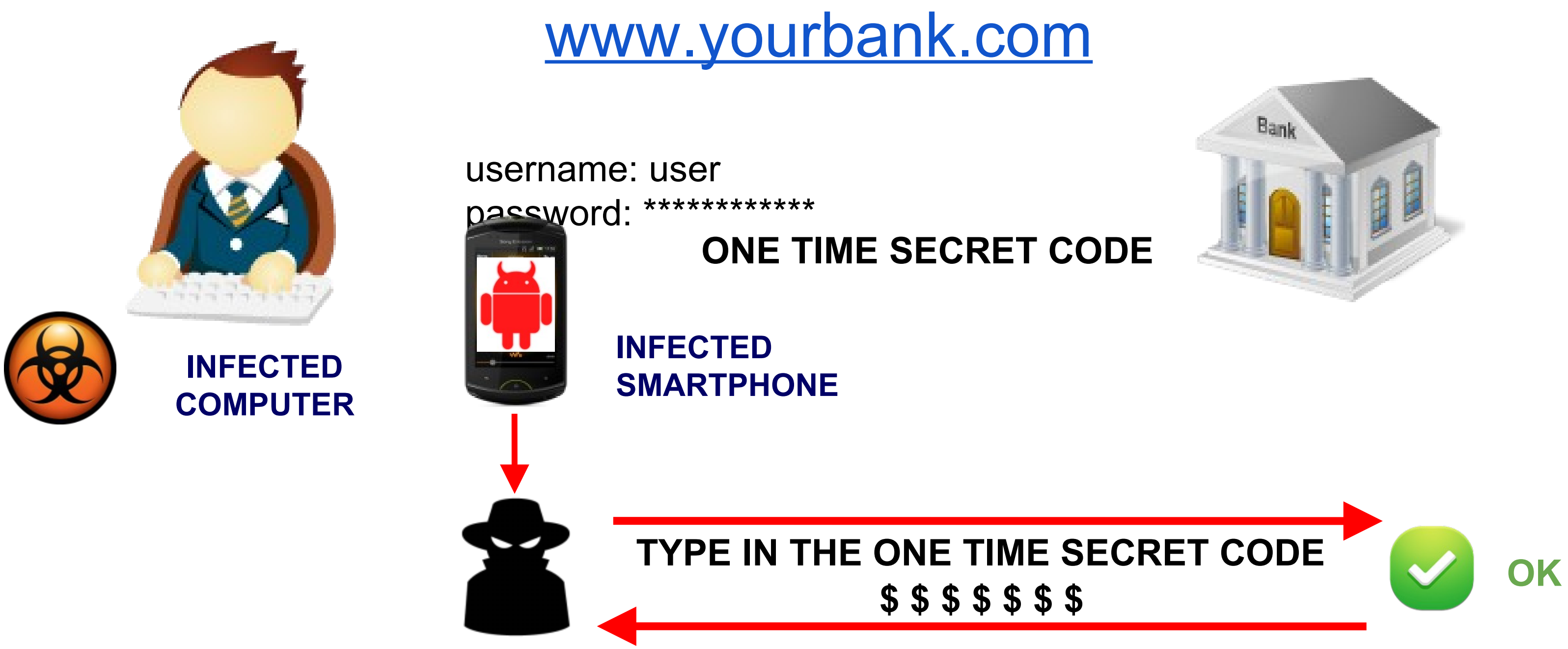
Password

Memorable word

Date of Birthday day / month / year

# Mobile trojans

- Most banking trojan toolkits include nowadays a mobile component
- This mobile component works in pairs with the PC versions and can access all the information in the user's phone, including SMS sent by banks containing One Time Passwords (OTP)



www.yourbank.com

username: user
password: ************

ONE TIME SECRET CODE

INFECTED COMPUTER

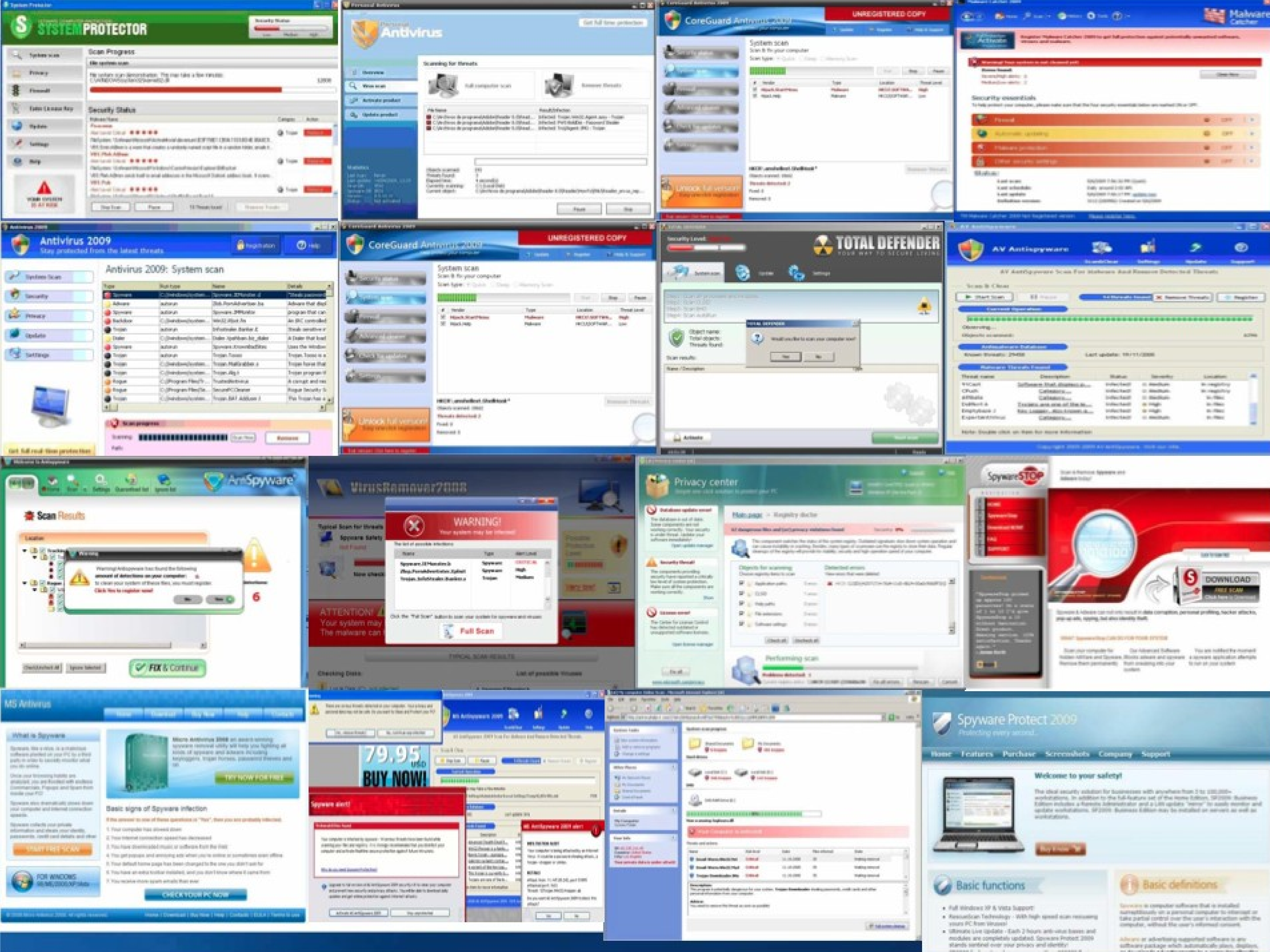
INFECTED SMARTPHONE

TYPE IN THE ONE TIME SECRET CODE

$ $ $ $ $ $ $

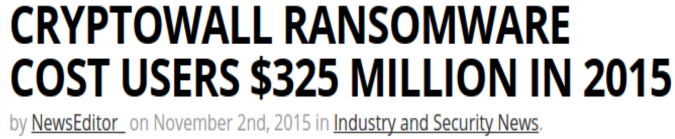
# Another example: rogue AV

- Suppose a “rogue AV” well designed costs $1500
- At the peak of the phenomenion, 3.5% of clients worldwide was exposed once per month to a rogue AV (PandaLabs)
- There’s surely in excess of a billion computers in the world (Forrester)
- So let’s guess 35 million “exposures” per month
- Thinking that a couple of users, on average, use a computer, and using a Gartner estimate of 3.3% of failures in handling phishing emails...
- ~500.000 Rogue AV are successful every month. With an average “price” of $59.95… it means > $415M a year...


SYSTEM PROTECTOR
Personal Antivirus
CoreGuard Antivirus 2009
UNREGISTERED COPY
Malware Catcher
Antivirus 2009
Stay protected from the latest threats
Antivirus 2009: System scan
CoreGuard Antivirus 2009
UNREGISTERED COPY
TOTAL DEFENDER
AV Antispyware
AntiSpyware
Scan Results
FIX & Continue
VirusRemover2008
WARNING!
ATTENTION!
Full Scan
Privacy center
SpywareSTOP
DOWNLOAD
FREE SCAN
MS Antivirus
What is Spyware
Basic signs of Spyware infection
79.95 USD
BUY NOW!
Spyware alert!
MS Antispyware 2009
Spyware Protect 2009
Welcome to your safety!
Basic functions
Basic definitions

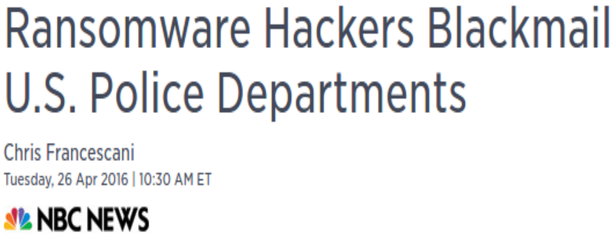
http://gizmodo.com/385113/this-is-how-cyber-criminals-party-mimes-and-blow+up-dolls

# Yet another example: ransomware



CRYPTOWALL RANSOMWARE
COST USERS $325 MILLION IN 2015

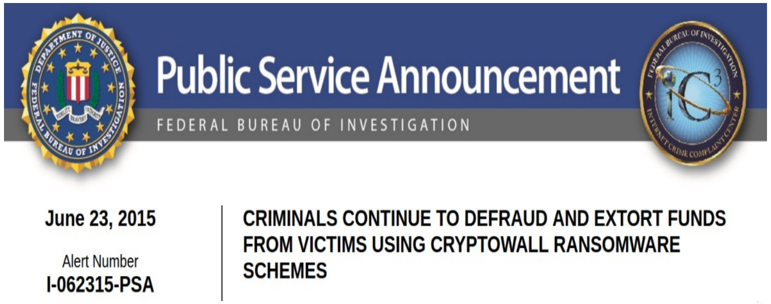
by NewsEditor on November 2nd, 2015 in Industry and Security News.



Ransomware Hackers Blackmail U.S. Police Departments

Chris Francescani
Tuesday, 26 Apr 2016 | 10:30 AM ET

NBC NEWS



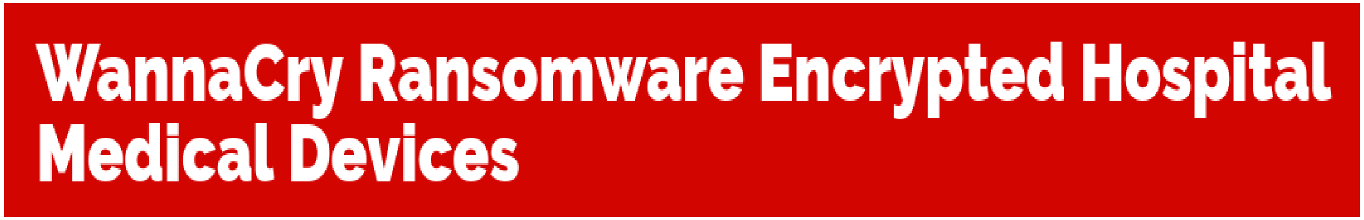
Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

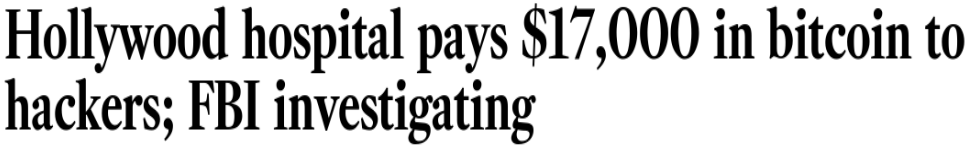
June 23, 2015

Alert Number
I-062315-PSA

CRIMINALS CONTINUE TO DEFRAUD AND EXTORT FUNDS FROM VICTIMS USING CRYPTOWALL RANSOMWARE SCHEMES

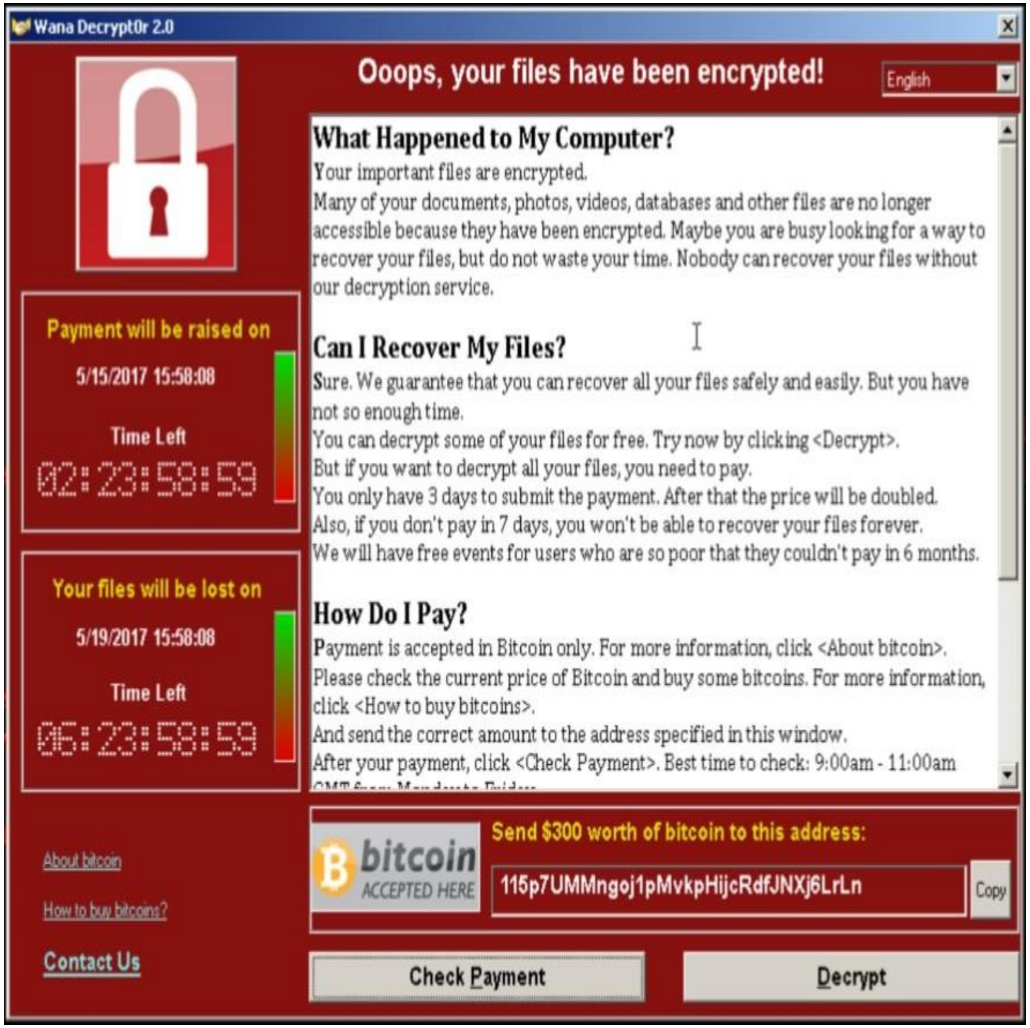


WannaCry Ransomware Encrypted Hospital Medical Devices



Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

# Do you wannacry?



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 15:58:08

Time Left

02:23:58:59

Your files will be lost on

5/19/2017 15:58:08

Time Left

06:23:58:59

## What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

## Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

## How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

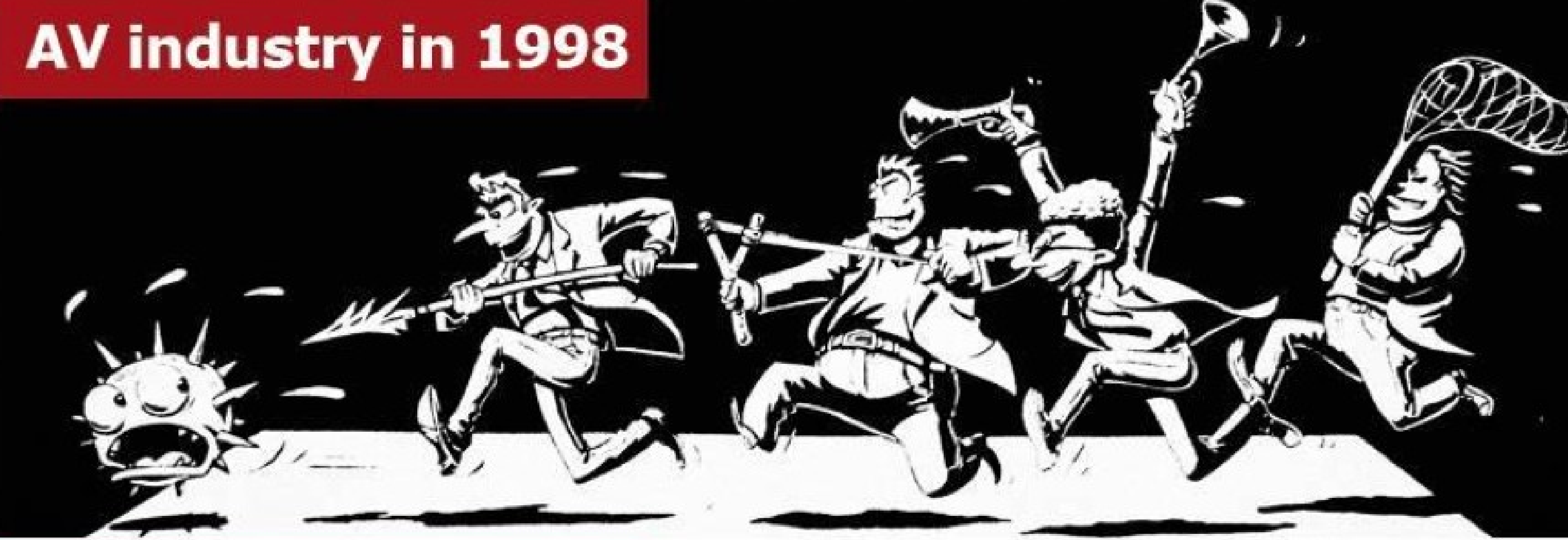
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

## AV industry in 1998



## AV industry in 2008

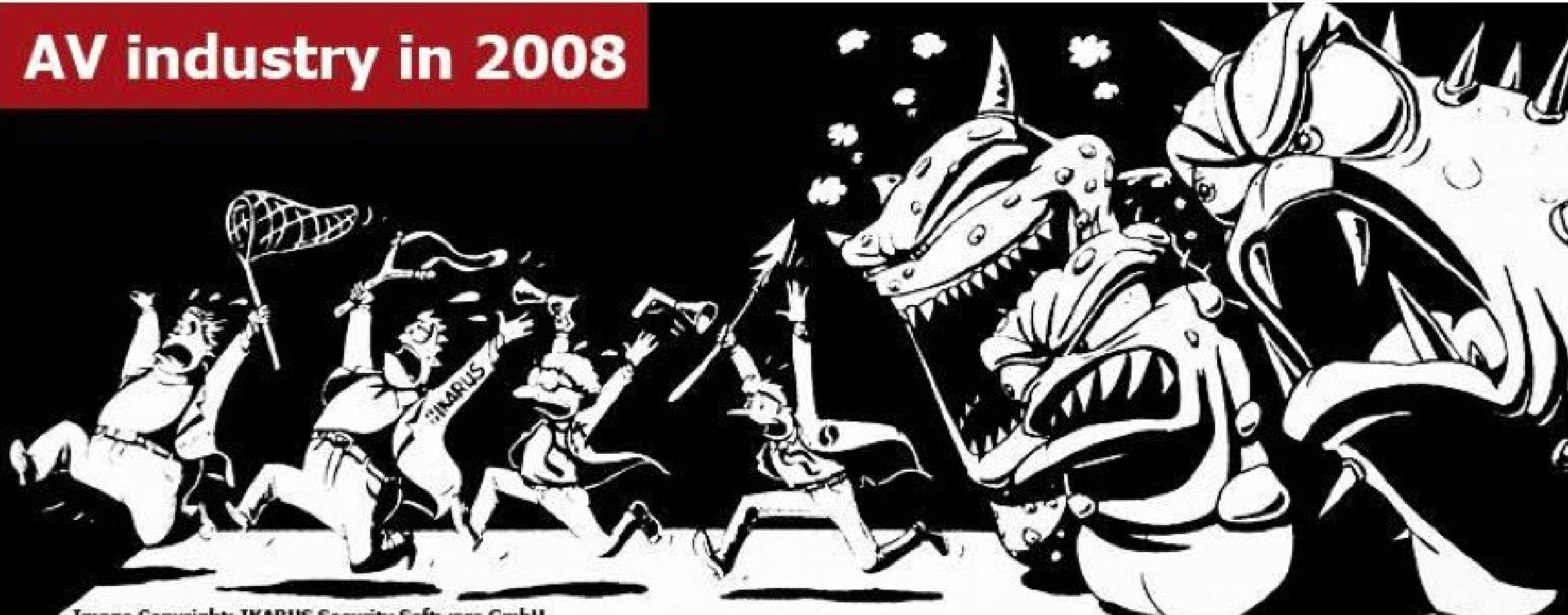


Image Copyright: IKARUS Security Software GmbH

# Enter the Internet of Things

*The IoT is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enables these objects to collect and exchange data*

# Personal things...

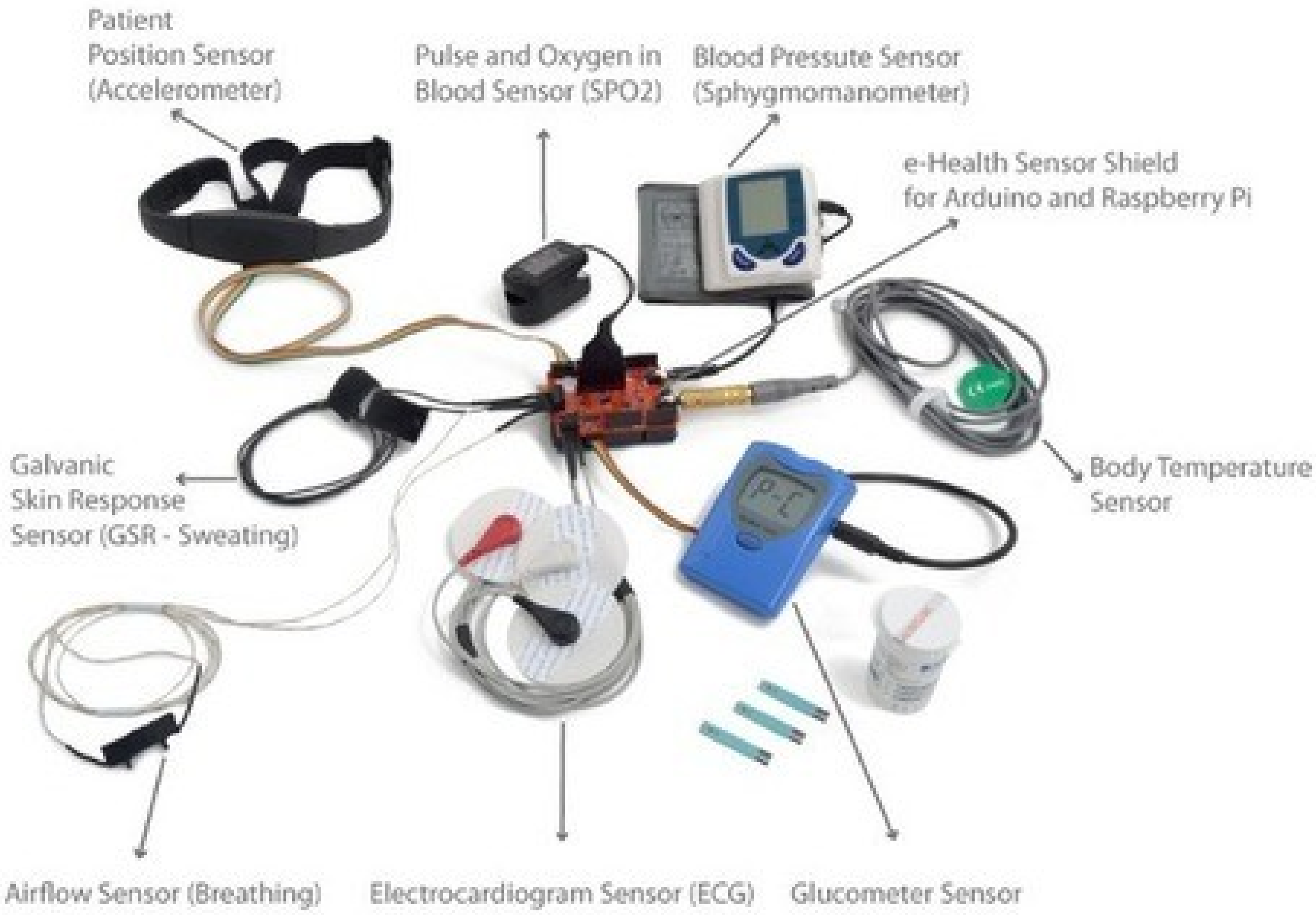
# Home things...

iSmartAlarm™

wemo
LINK
belkin
wemo
belkin
wemo

31
P
WeatherBug

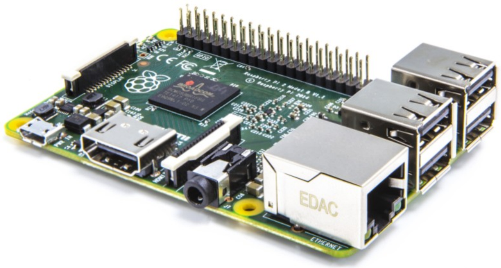
# Medical things (ouch!)



# Specific challenges in medical IoT

- Designed to interact intimately with the human body (→ value at risk very high)
- Small in scale, and constrained in power consumption
- Increasing connectivity → need to be insulated from the public Internet
- Firmware updates might be unfeasible, or risky
- Designers focus on *safety* rather than *security*, tested according to *standards* and regulatory specifications: this approach does not work with security engineering, where most testing is negative
- Security assessment and design needs a systemic approach, whereas most medical IoT devices are designed and certified separately

# But also industrial things…!

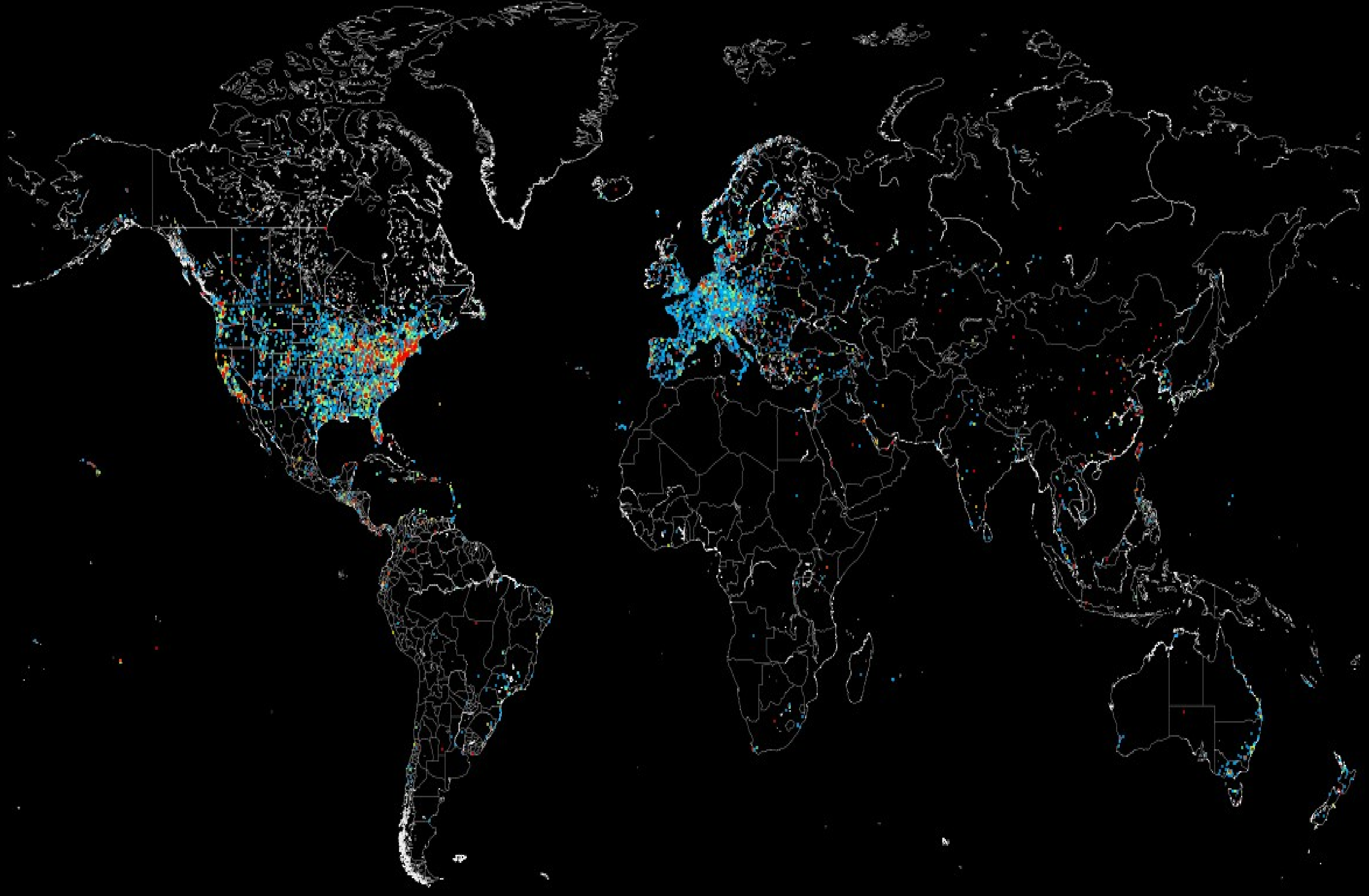


# Welcome to the IoIT (Industrial Things)

- **Originally-disconnected systems now “opening” to the Internet**
- Critical infrastructure and safety-critical systems
- (sometimes) no humans in the middle
- → Influence environment and humans (≠ data security!)

SHODAN

# ICS on the Internet



# Attacks against ICS share some characteristics

- 2014: Steel mill incident
  - Spear phishing leads to compromise of corporate network
  - Pivot into plant network
  - Exploitation phase (compromise network controllers)
- 23rd December 2015: Ukraine power outage
  - Black energy malware
  - Spear phishing leads to compromise of corporate network
  - BlackEnergy malware steals VPN credentials
  - Pivot into plant networks
  - Exploitation phase (modification of UPS controller firmware)

# Industrial robot research results

- The usual vulnerabilities (buffer overflows, command injection)
- "Outdated" coding practices
- Hardcoded credentials (and no real account lockout in place)
- No encryption (or, worse, placebo cryptography)
- Software and updates not signed
- No hardening: no privilege separation, nothing
- No physical security (physical access == full compromise)

- Read the full research report at http://robosec.org

# Industrial routers research results

- Information disclosure (way too verbose banners, detailed technical material)
- Outdated everything (kernel, compilers, libraries, …)
- Weak \ known \ static credentials
- Poor or misconfigured transport encryption (e.g., VPN with static auth keys, pre-generated certs, …)
- Insecure web interface (no input sanitization… and even security critical code copied straight from blog posts!)
- **No better than consumer IoT devices!**

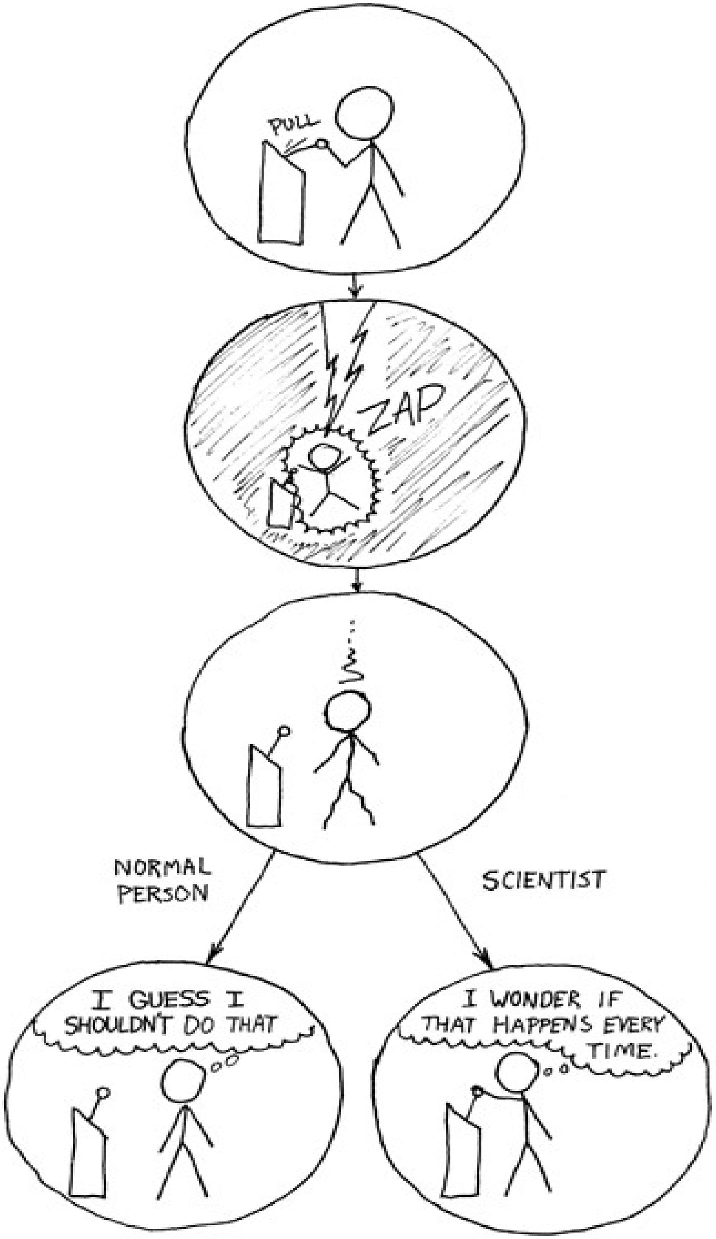
- Read the full research report at http://robosec.org

# OWASP top 13 IoT vulnerabilities...

1. Username Enumeration (really?)
2. Weak Passwords (you can't be serious)
3. Account Lockout (didn't we figure out this in 1970?)
4. Unencrypted Services (Snowden, anyone?!)
5. Two-factor Authentication (even my bank can do this)
6. Poorly Implemented Encryption (so, if it's not in clear, it's weak…)
7. Update Sent Without Encryption (…)
8. Update Location Writable (yup, why not executing random code?)
9. Denial of Service (on your oven, to burn your cake)
10. Removal of Storage Media (you can't make this stuff up)
11. No Manual Update Mechanism (fine, it's probably autom...)
12. Missing Update Mechanism (… or maybe not)
13. Firmware Version Display and/or Last Update Date (but in any case you don't even know)

# Questions?

- Thank you for your attention!
- You can reach me at stefano.zanero@polimi.it
- Or just tweet @raistolo


PULL
ZAP
NORMAL PERSON
SCIENTIST
I GUESS I SHOULDN'T DO THAT
I WONDER IF THAT HAPPENS EVERY TIME.

Videndum Media Solutions

# Cybersecurity:

## «i principali rischi le aziende e i più comuni tipi di attacco informatico»

16/06/2022

Flavio Fiorio – SVP IT&YWEB

# Videndum Company Profile

Videndum plc is a
leading global provider of

**premium branded hardware products and software solutions**

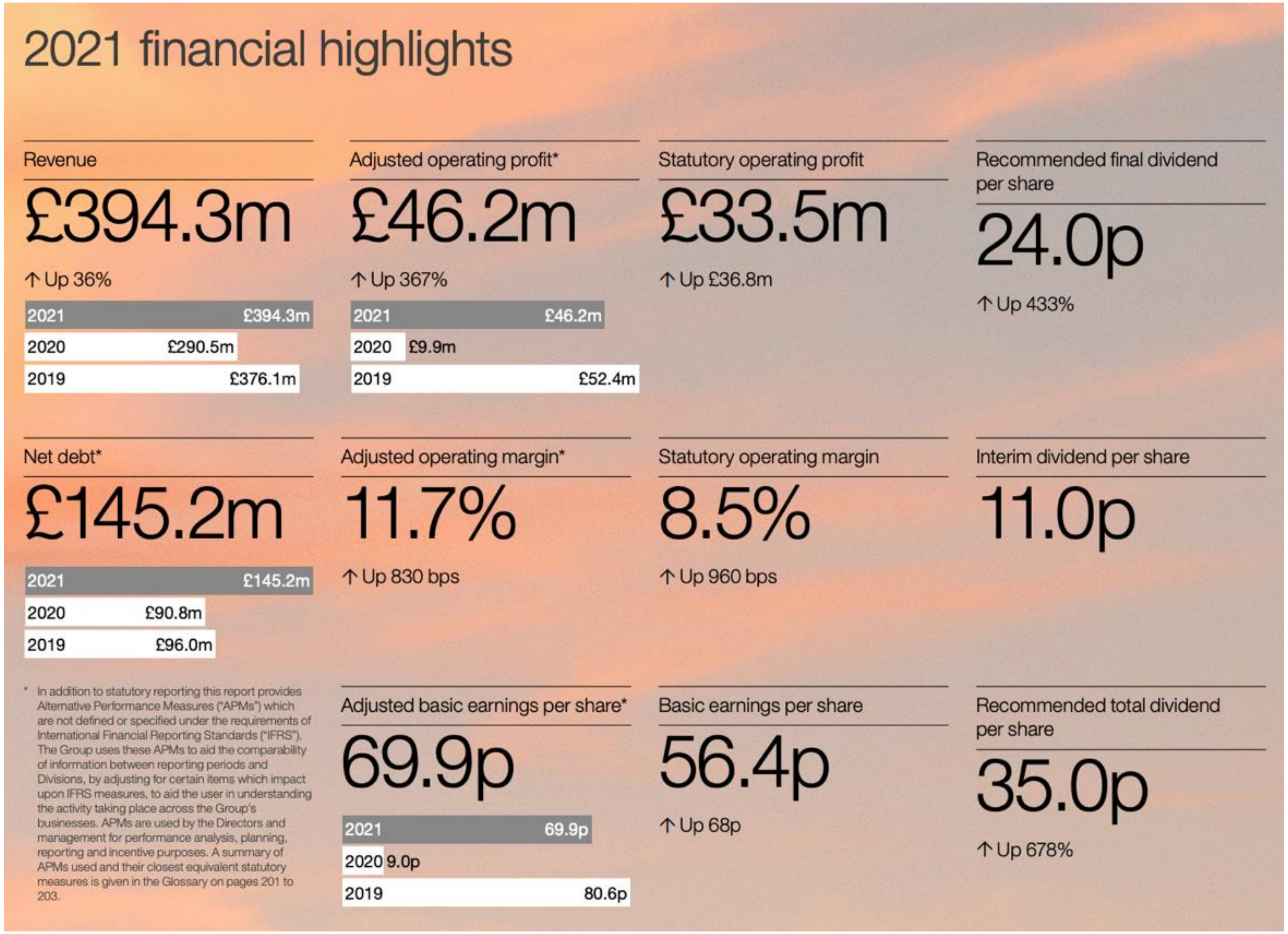
to the growing

**content creation market.**

Customers include broadcasters, film studios, production and rental companies, photographers independent content creators, gamers and enterprises.

**We design, manufacture and distribute** high performance products and solutions including camera supports, video transmission systems and monitors, live streaming solutions, smartphone accessories, robotic camera systems, prompters, LED lighting, mobile power, bags and motion control, audio capture and noise reduction equipment.

We are organised in three Divisions: **Media** Solutions, **Production** Solutions and **Creative** Solutions.



## 2021 financial highlights

Revenue

£394.3m

↑ Up 36%

| | |
|---|---|
| 2021 | £394.3m |
| 2020 | £290.5m |
| 2019 | £376.1m |

Adjusted operating profit*

£46.2m

↑ Up 367%

| | |
|---|---|
| 2021 | £46.2m |
| 2020 | £9.9m |
| 2019 | £52.4m |

Statutory operating profit

£33.5m

↑ Up £36.8m

Recommended final dividend per share

24.0p

↑ Up 433%

Net debt*

£145.2m

| | |
|---|---|
| 2021 | £145.2m |
| 2020 | £90.8m |
| 2019 | £96.0m |

Adjusted operating margin*

11.7%

↑ Up 830 bps

Statutory operating margin

8.5%

↑ Up 960 bps

Interim dividend per share

11.0p

Adjusted basic earnings per share*

69.9p

| | |
|---|---|
| 2021 | 69.9p |
| 2020 | 9.0p |
| 2019 | 80.6p |

Basic earnings per share

56.4p

↑ Up 68p

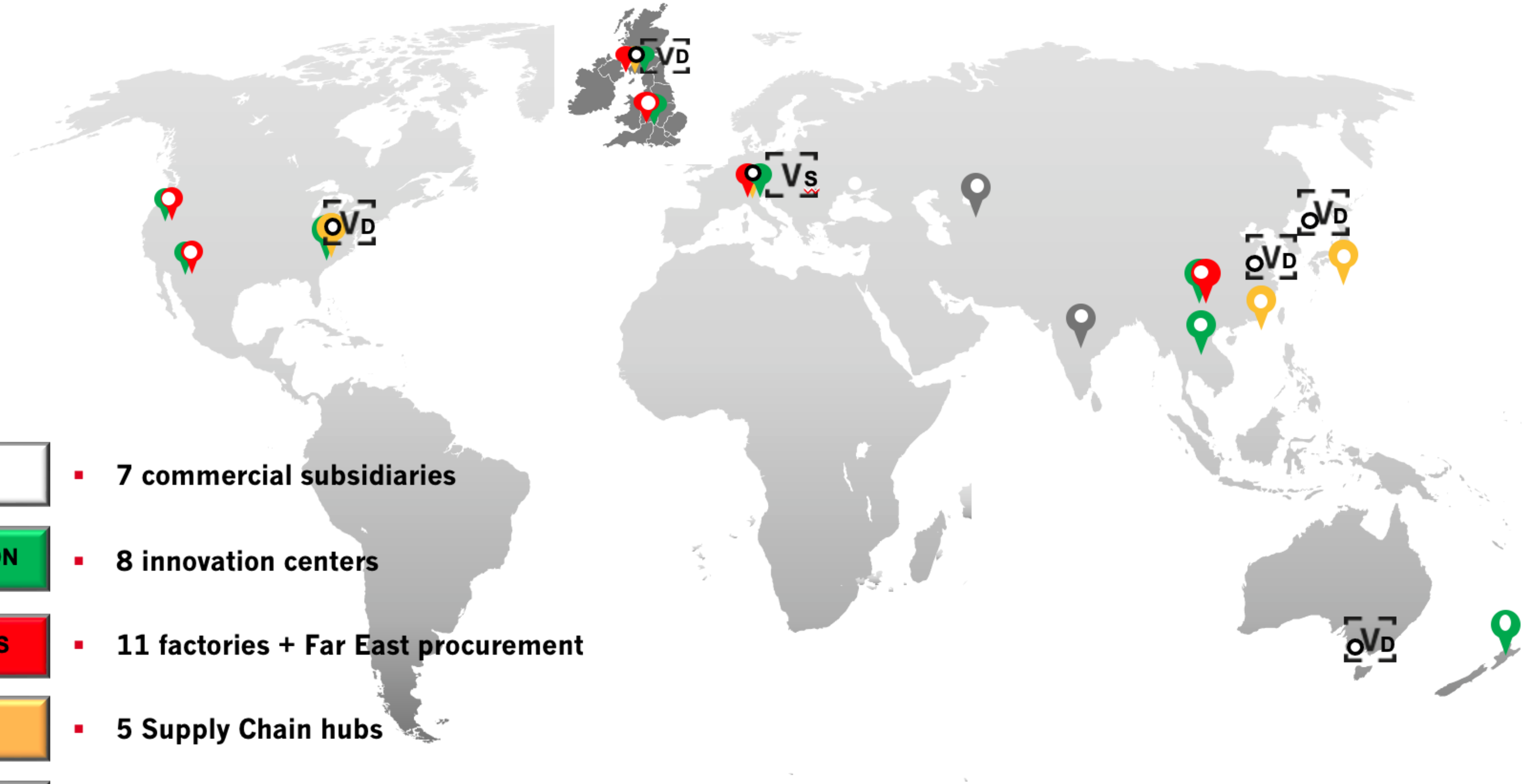
Recommended total dividend per share

35.0p

↑ Up 678%

* In addition to statutory reporting this report provides Alternative Performance Measures ("APMs") which are not defined or specified under the requirements of International Financial Reporting Standards ("IFRS"). The Group uses these APMs to aid the comparability of information between reporting periods and Divisions, by adjusting for certain items which impact upon IFRS measures, to aid the user in understanding the activity taking place across the Group's businesses. APMs are used by the Directors and management for performance analysis, planning, reporting and incentive purposes. A summary of APMs used and their closest equivalent statutory measures is given in the Glossary on pages 201 to 203.

# “Videndum Media Solutions” Organization



| | |
|---|---|
| V OFFICES | 7 commercial subsidiaries |
| V INNOVATION | 8 innovation centers |
| V OPERATIONS | 11 factories + Far East procurement |
| V HUBS | 5 Supply Chain hubs |
| V LIAISON | 2 Liaison offices |

**We are the largest manufacturer of branded supports in the world and 4 x larger than the No.2**

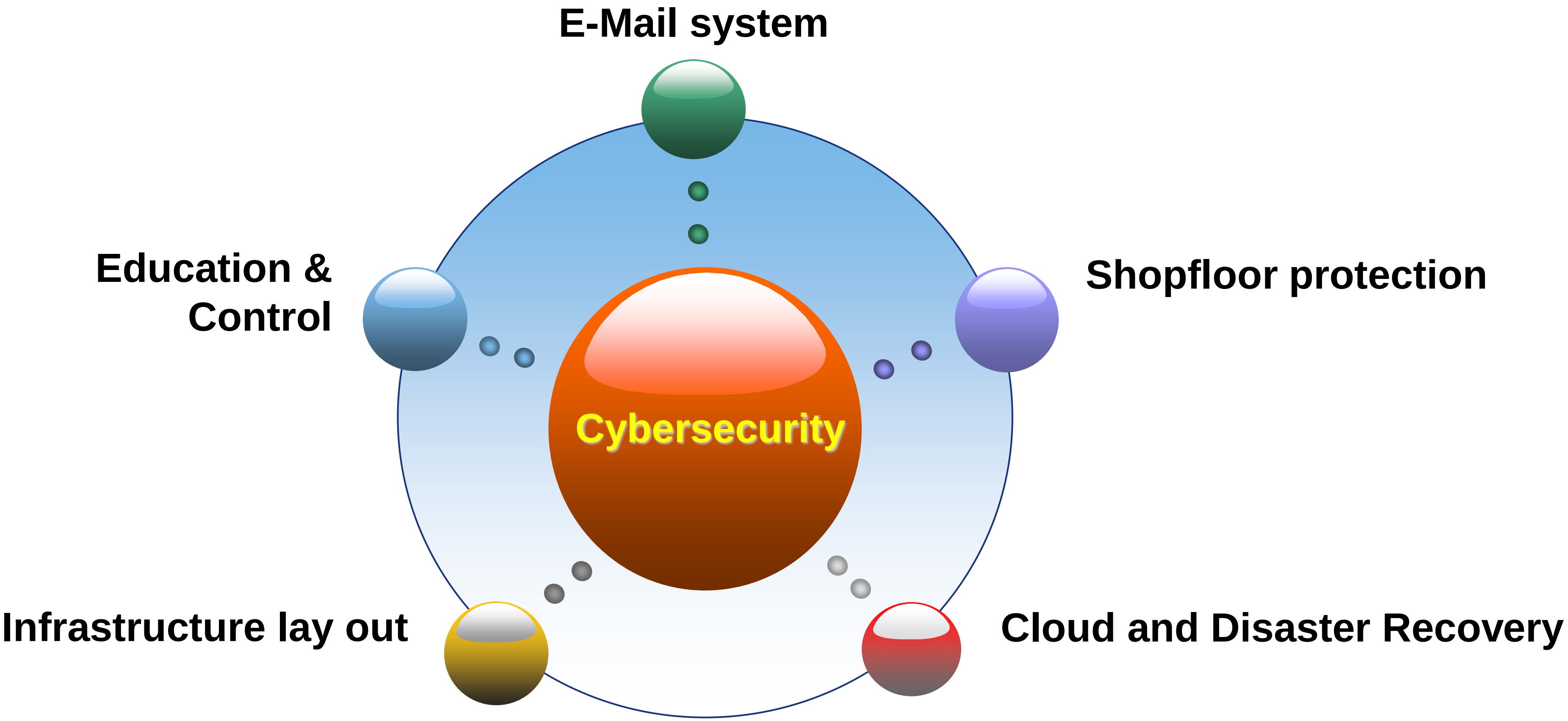
Germany

# Videndum manifest - Cyber Security Strategy

Cyber Strategy Plan

- *Align our strategy to a risk-based framework.*
- *Embed security and security culture into the business and our business processes.*
  - *Hold regular training and testing for all employees around security and data governance.*
  - *Work with functions such as engineering to ensure the same framework is applied to our development and products.*
- *External verification, assurance and certification*
  - *Bi-annual review of cyber strategy, plan and readiness.*
  - *IASME (Cyber Essential) + Certification*
  - *Increased levels of Pen testing*
- *Ensure our data is safe, secure and compliant.*
- *Have a Zero-Trust and layered approach to Security.*
- *Assess and secure our internal and external supply chain.*
- *Dedicated security resources.*

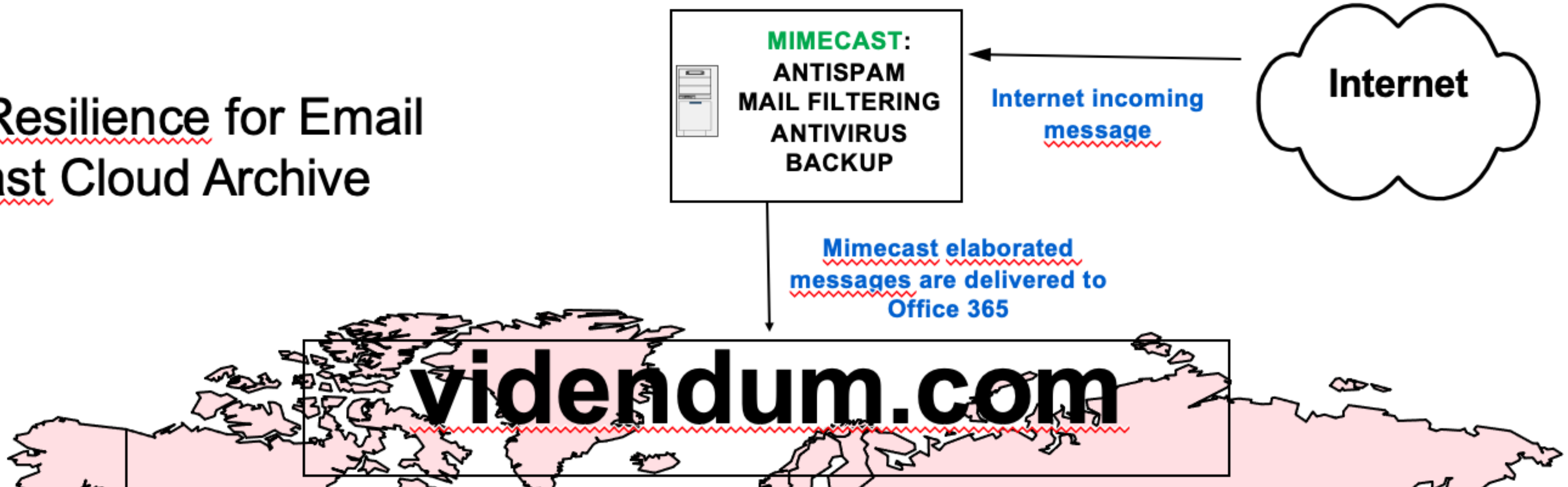
# Cybersecurity touch points

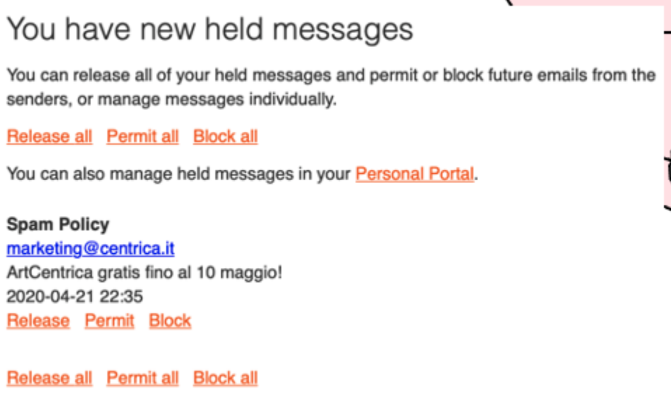


**We have to consider multiple touch points**

# eMail system protection

- Cyber Resilience for Email
- Mimecast Cloud Archive


MIMECAST:
ANTISPAM
MAIL FILTERING
ANTIVIRUS
BACKUP
Internet incoming message
Internet
Mimecast elaborated messages are delivered to Office 365
videndum.com



You have new held messages

You can release all of your held messages and permit or block future emails from the senders, or manage messages individually.

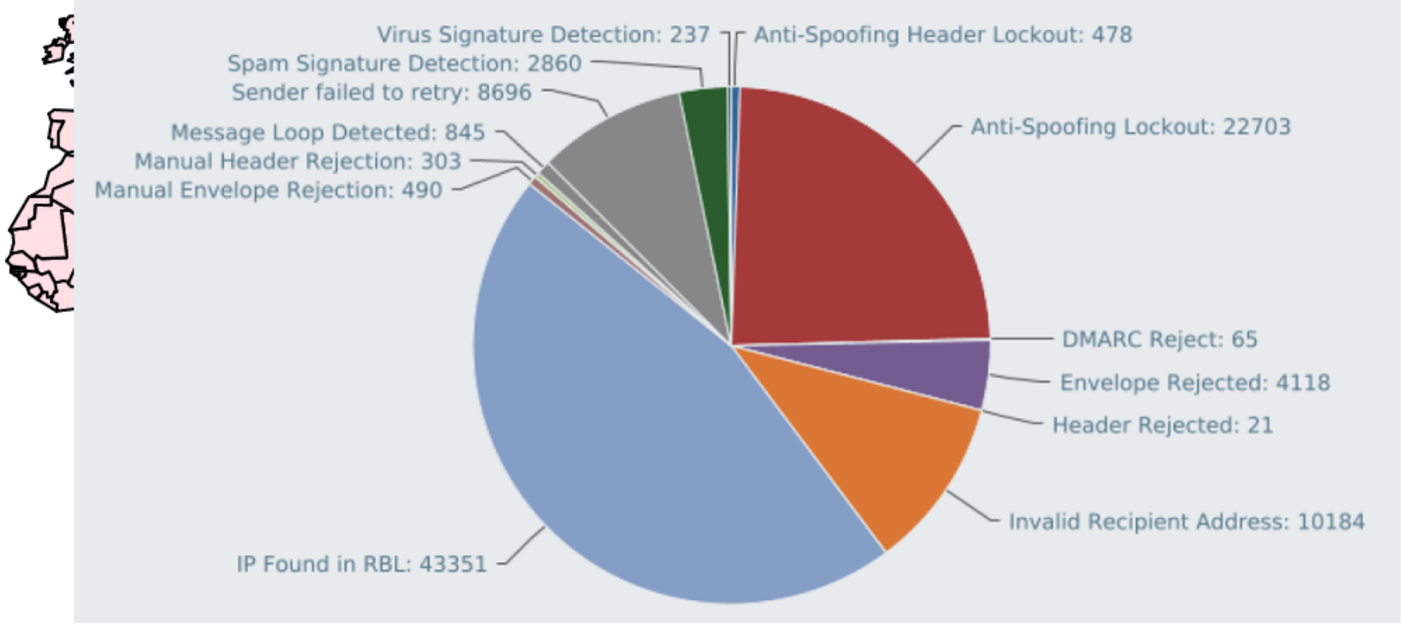
Release all Permit all Block all

You can also manage held messages in your Personal Portal.

**Spam Policy**
marketing@centrica.it
ArtCentrica gratis fino al 10 maggio!
2020-04-21 22:35
Release Permit Block

Release all Permit all Block all

mimecast®



# Shopfloor/Office protection

- L’industry 4.0 ha portato molta tecnologia nelle fabbriche, ed un fermo derivante da attacco informatico ha per noi una dimensione giornaliera di perdita del valore prodotto (non del fatturato che sarebbe ovviamente molto più alto) che va da 250K€ a 300K€)
  - *Aggiornare l’hardware di fabbrica alle ultime release di sistema operativo Microsoft*
  - *Controllo in tempo reale degli accessi al network mediante console*
  - *Gestione dei diversi profili che accedono*
  - *Documentare i login, e utilizzare un sistema semplice per l’accesso anche delle terze parti*
  - *Multiple network access (ad esempio abbiamo sdoppiato le linee di accesso per gli operatori di produzione e per gli impiegati)*
  - *Management console (MDM) for worldwide hardware control*

Extreme

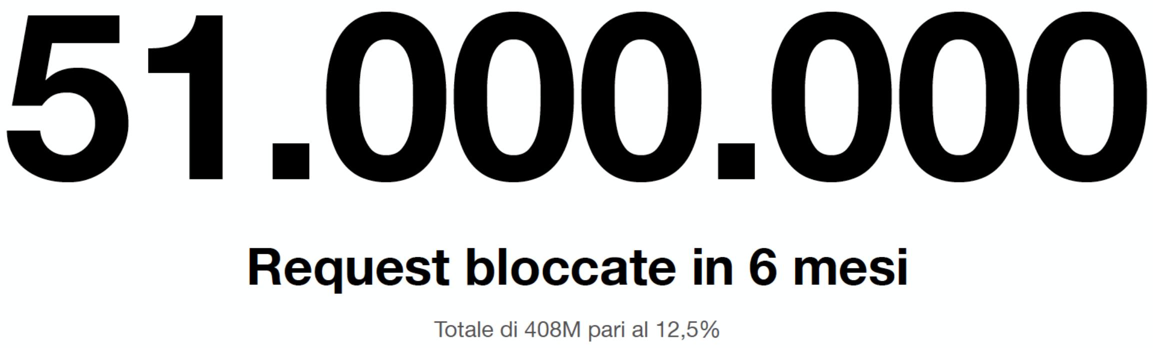
# Cloud and Disaster Recovery & infrastructure lay out

- Utilizziamo un cloud privato ed uno pubblico

  - *Cloud privato: la server farm TIM da servizio per processi standard come ERP e Business Intelligence alle filiali mediante una rete protetta da firewall Checkpoint*

  - *Cloud Pubblico: per servizi prettamente cloud come l'eCommerce che hanno un alta possibilità di essere attaccati, ci avvaliamo della protezione di WAF (web application firewall) rinforzati da servizi specifici di firewalling di secondo livello messi nel nostro caso a disposizione da AWS . Abbiamo un controllo 24x7 con un fornitore italiano di base a Padova che ci eroga il servizio.*

  - Disaster Recovery in seconda server farm locata a più di 50 km dalla prima ed in caso di AWS in due continenti diversi



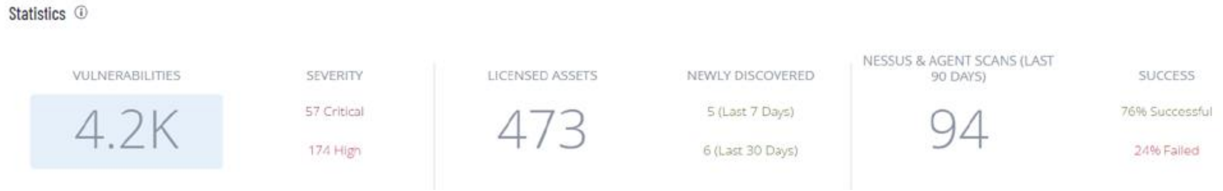
51.000.000

Request bloccate in 6 mesi

Totale di 408M pari al 12,5%

# Education

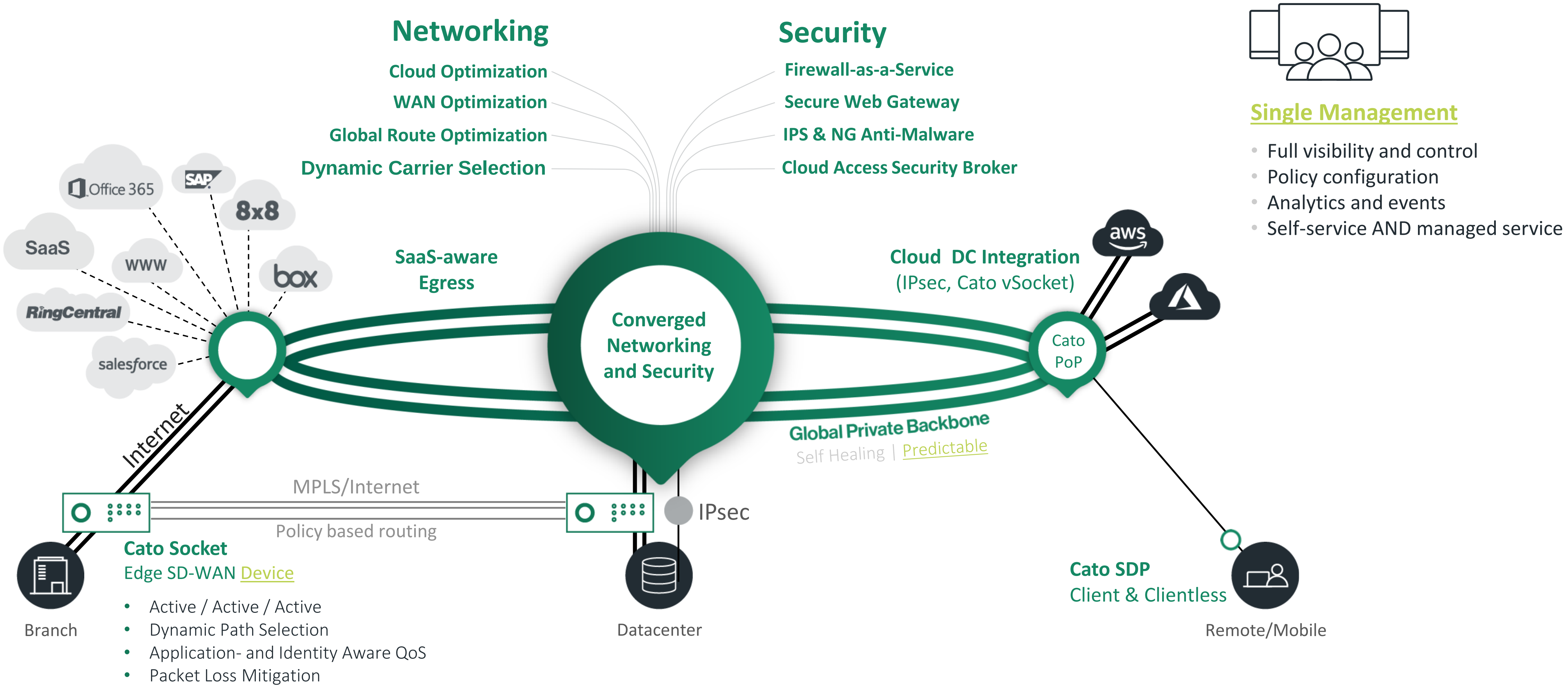
- Education
  - Sollecitare l’utenza con frequenti messaggi che chiariscano cos’è un cyber attacco, anche con esempi pratici
  - Con la collaborazione di HR, mettere in pista uno strumento di e-learning (nel nostro caso è Knowbe4) per chiarire ed educare i colleghi che potrebbero sottovalutare … un click
- Usare strumenti messi a disposizione da Microsoft per aumentare la sicurezza e quindi di conseguenza limitare i cyber attacchi
  - 2FA - Multifactor Authentication
  - MS One Drive
- Dotarsi di piattaforme di vulnerability management, che regolarmente facciano un check dell’infrastruttura (www.tenable.com)



Statistics ⓘ

| VULNERABILITIES | SEVERITY | LICENSED ASSETS | NEWLY DISCOVERED | NESSUS & AGENT SCANS (LAST 90 DAYS) | SUCCESS |
|---|---|---|---|---|---|
| 4.2K | 57 Critical<br>174 High | 473 | 5 (Last 7 Days)<br>6 (Last 30 Days) | 94 | 76% Successful<br>24% Failed |

# Opportunità tecnologica di rinforzo della protezione: SASE



## Networking

- Cloud Optimization
- WAN Optimization
- Global Route Optimization
- Dynamic Carrier Selection

## Security

- Firewall-as-a-Service
- Secure Web Gateway
- IPS & NG Anti-Malware
- Cloud Access Security Broker

## Single Management

- Full visibility and control
- Policy configuration
- Analytics and events
- Self-service AND managed service

Converged Networking and Security

SaaS-aware Egress

Cloud DC Integration (IPsec, Cato vSocket)

Cato PoP

Global Private Backbone

Self Healing | Predictable

Internet

MPLS/Internet

Policy based routing

IPsec

**Cato Socket**

Edge SD-WAN Device

- Active / Active / Active
- Dynamic Path Selection
- Application- and Identity Aware QoS
- Packet Loss Mitigation

**Cato SDP**

Client & Clientless

**Secure Access Service Edge: Semplificazione dell’infrastruttura e riduzione del rischio di cyber attack**

V