POLITECNICO DI MILANO

Cybersecurity in a changing world

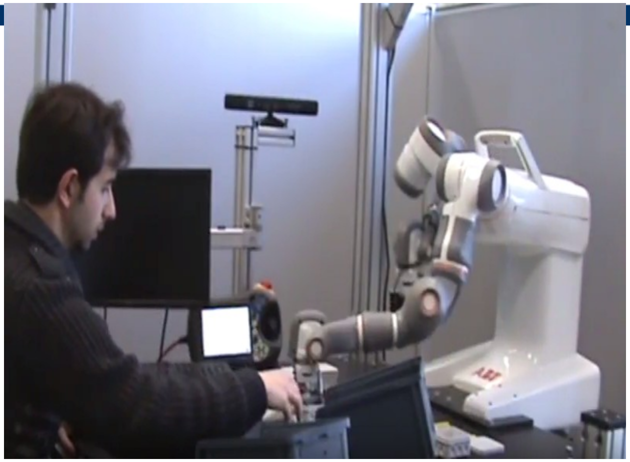
Stefano Zanero, PhD

Associate Professor, Politecnico di Milano

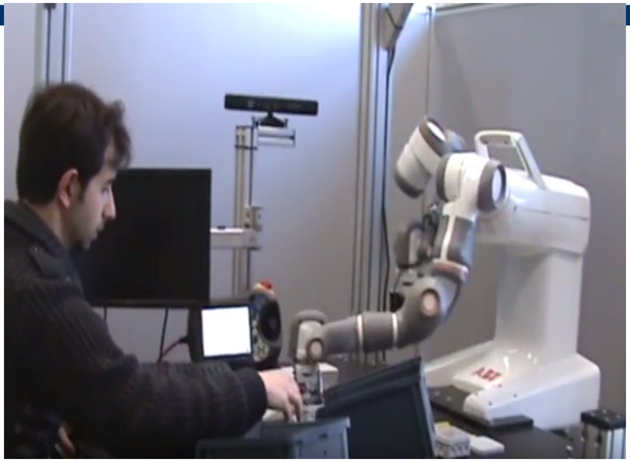
Founder, Secure Network Srl

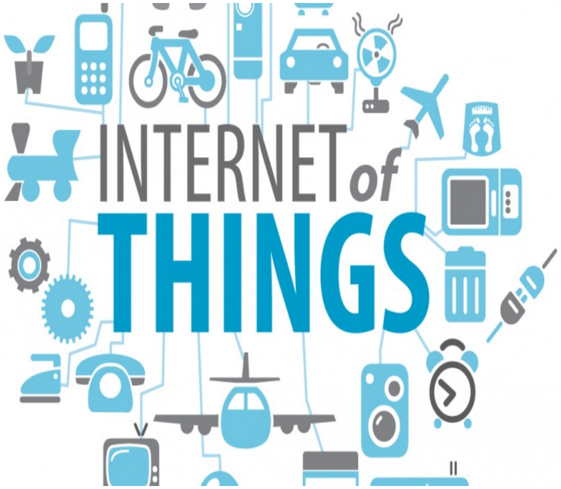
The iper-connected future

The iper-connected future

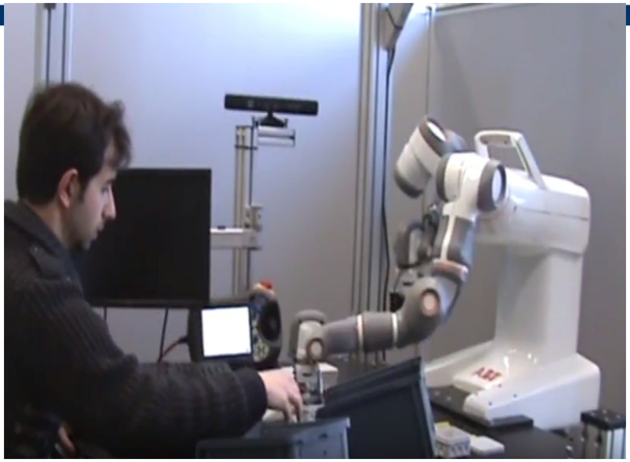


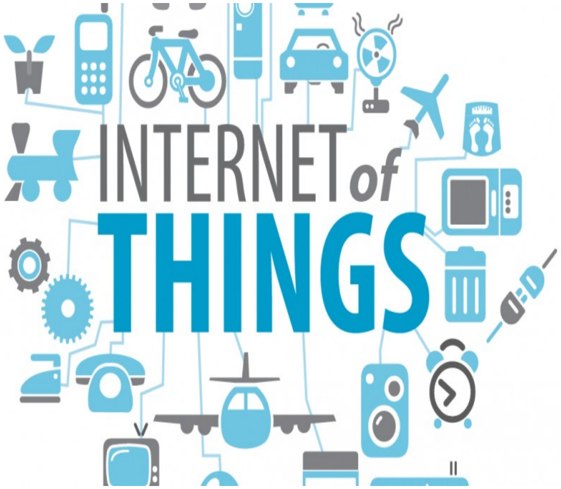
The iper-connected future



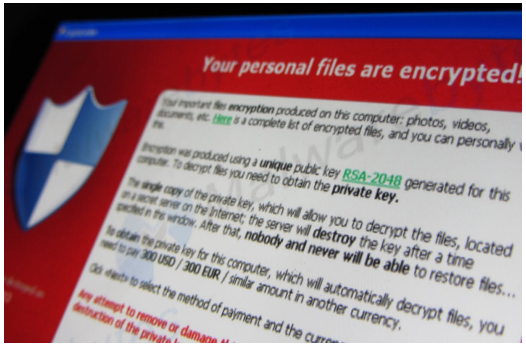


The iper-connected future





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.**

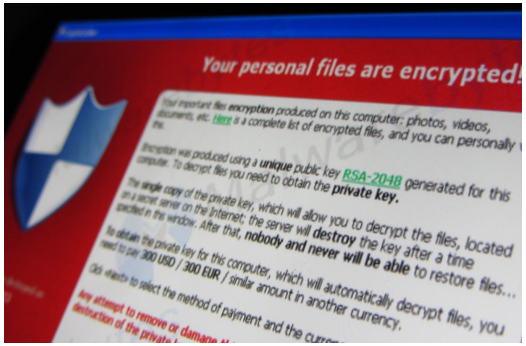
The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

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

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

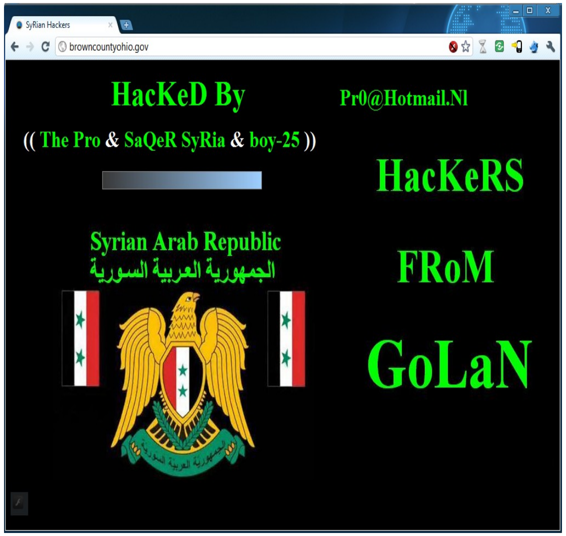
Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

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



HacKeD By

Pr0@Hotmail.Nl

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

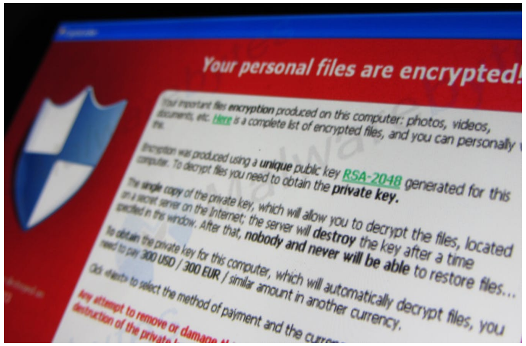
HacKeRS

FRoM

GoLaN

Syrian Arab Republic
الجمهورية العربية السورية

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

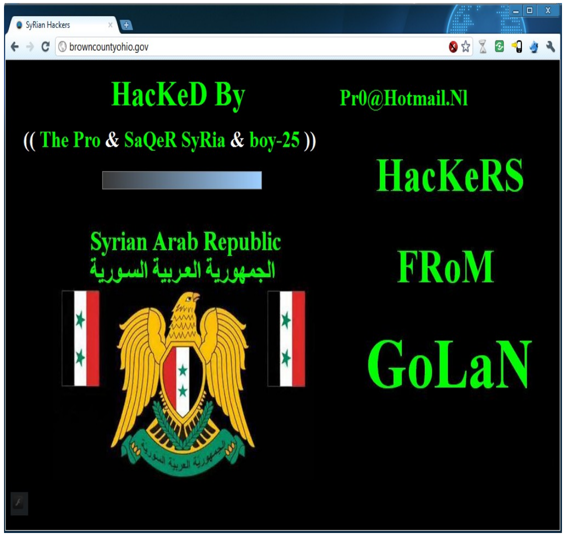
Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

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



HacKeD By

Pr0@Hotmail.Nl

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

HacKeRS

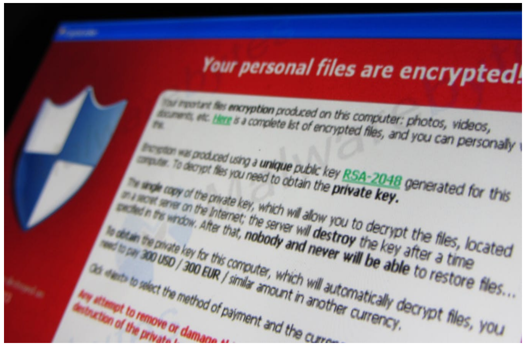
FRoM

GoLaN

Syrian Arab Republic
الجمهورية العربية السورية

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

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.

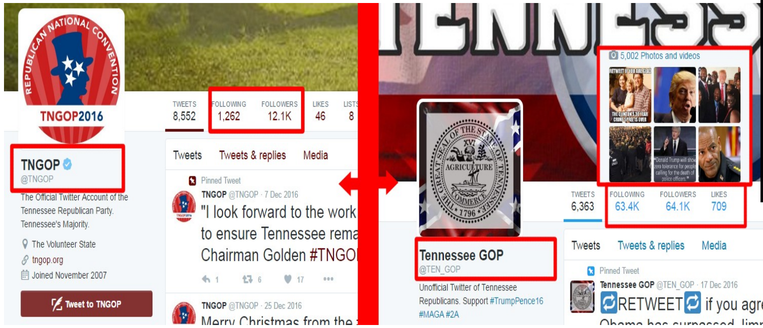
Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

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



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

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 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

5,002 Photos and videos

RETWEET IF YOU ARE GLAD
THE CLINTON'S 30 YEAR CRIME SPREE IS OVER
"Donald Trump will show zero tolerance for people calling for the death of police officers."

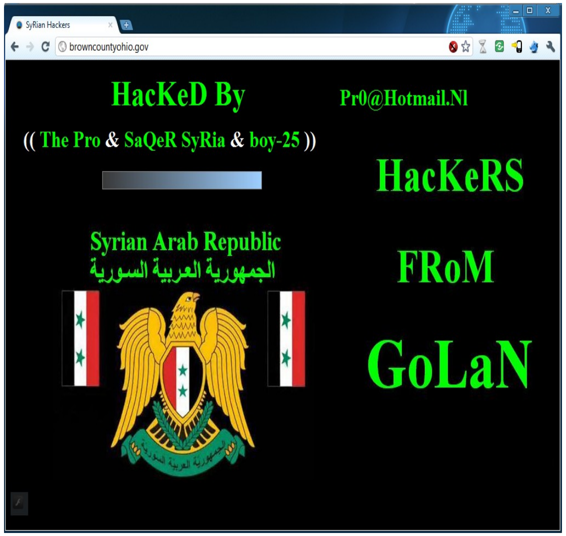
TWEETS 6,363 FOLLOWING 63.4K FOLLOWERS 64.1K LIKES 709

Tennessee GOP
@TEN_GOP

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

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))

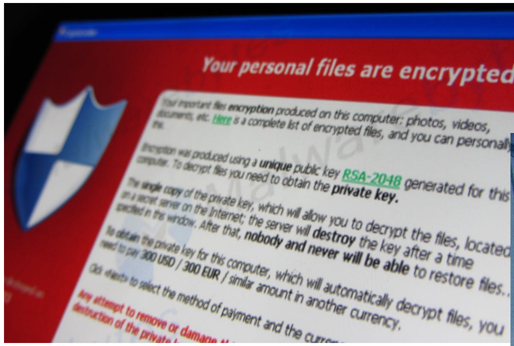
HacKeRS

Syrian Arab Republic
الجمهورية العربية السورية

FRoM

GoLaN

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 personal this.

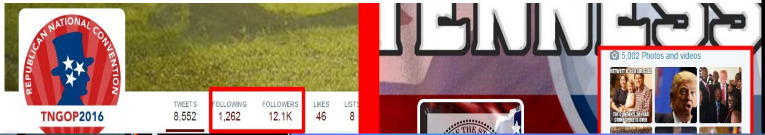
Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

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



TNGOP2016

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

5,002 Photos and videos

SyRian Hackers

browncountyohio.gov

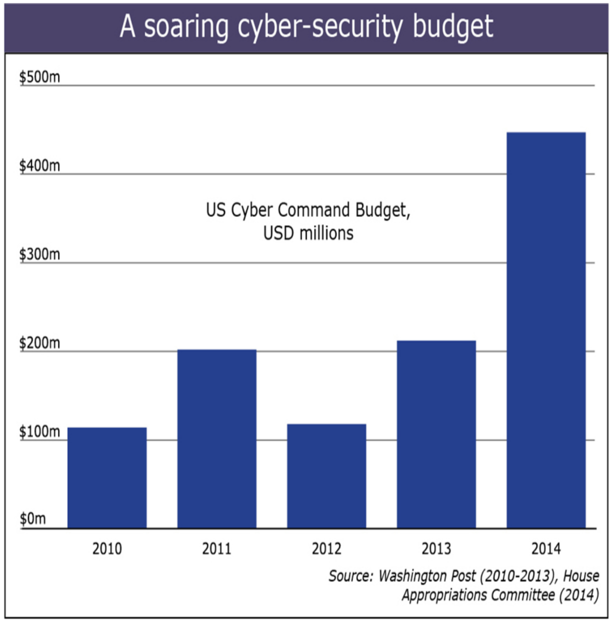
HacKeD By

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

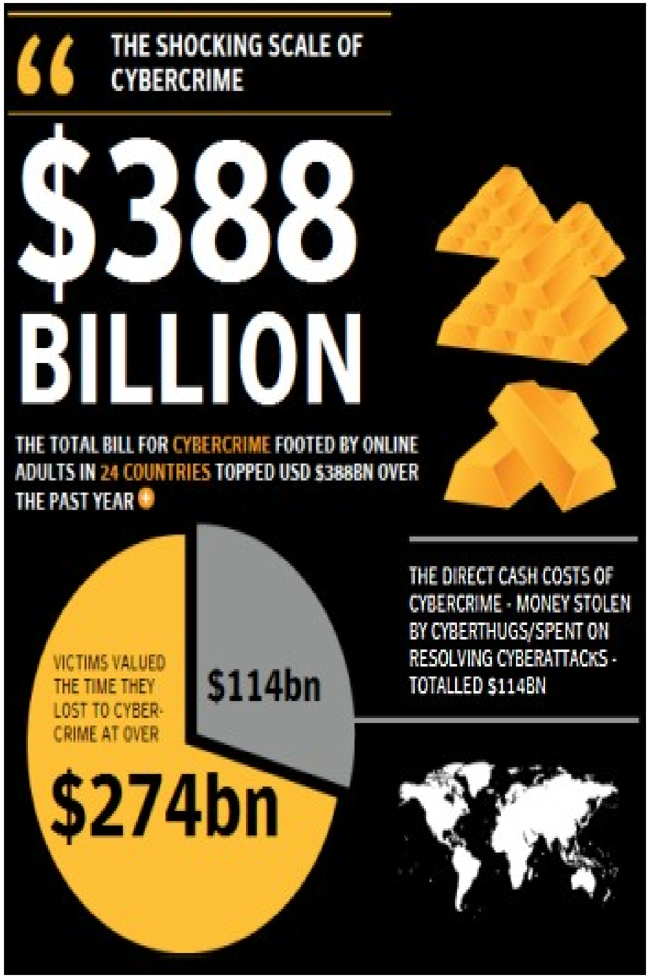
Syrian Arab Republic

الجمهورية العربية السورية

Costs and damage


A soaring cyber-security budget

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

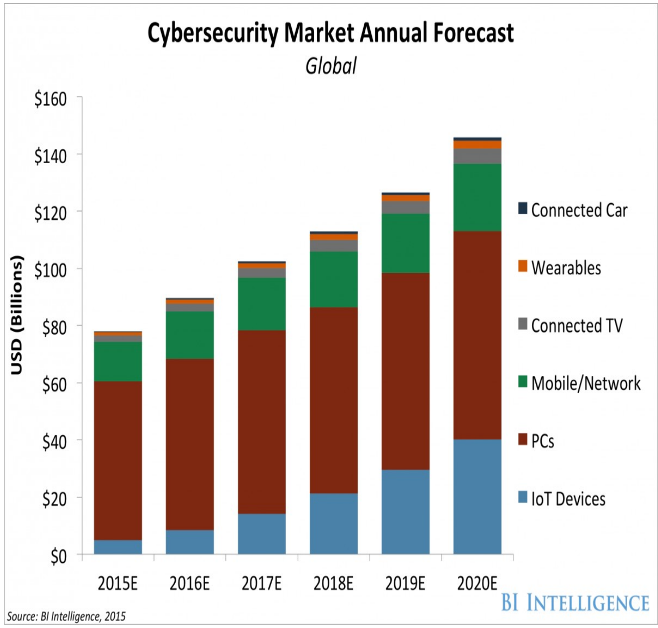

THE SHOCKING SCALE OF CYBERCRIME

$388 BILLION

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

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

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


Cybersecurity Market Annual Forecast

Global

Source: BI Intelligence, 2015

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

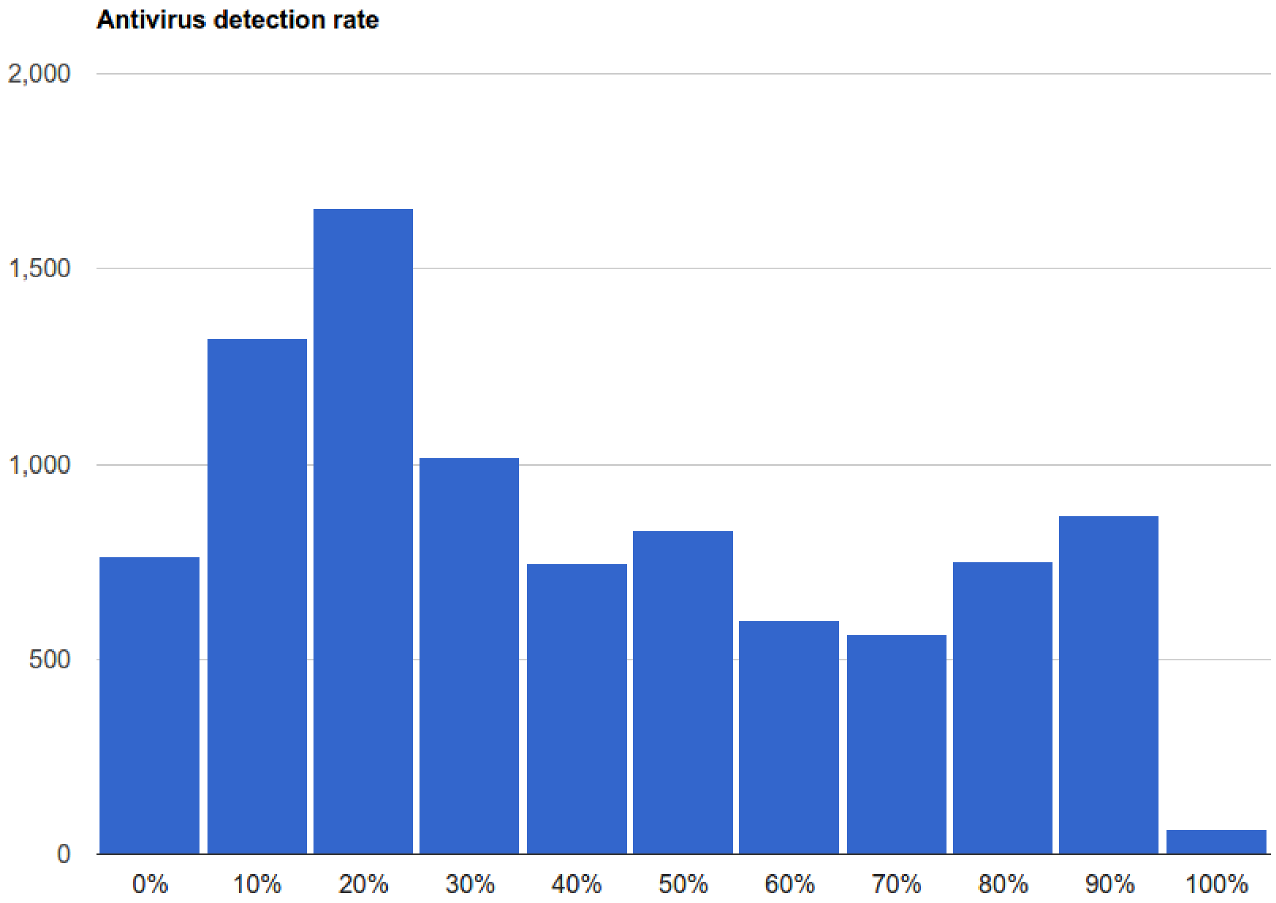
- What they are:
  - ✓ Malware that steal credentials such as usernames, passwords, and second factors of authentication
  - ✓ They are also named “banking trojans”, because they are often used to steal banking credentials and perform online financial frauds

- 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

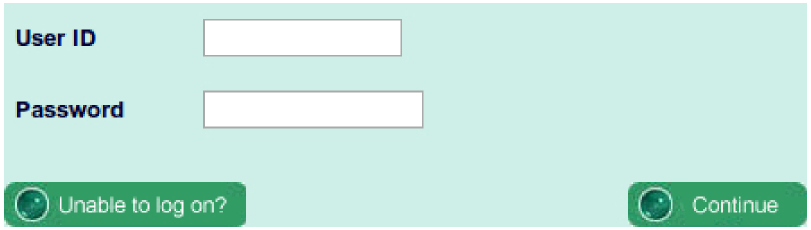
AV Detection Rate

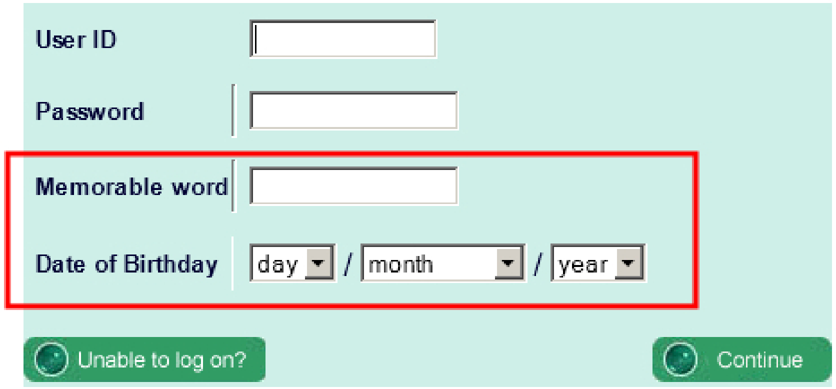
Low detection rate: as of yesterday, according to ZeuS Tracker the overall detection rate is 40.04%



Man in the Browser and WebInject

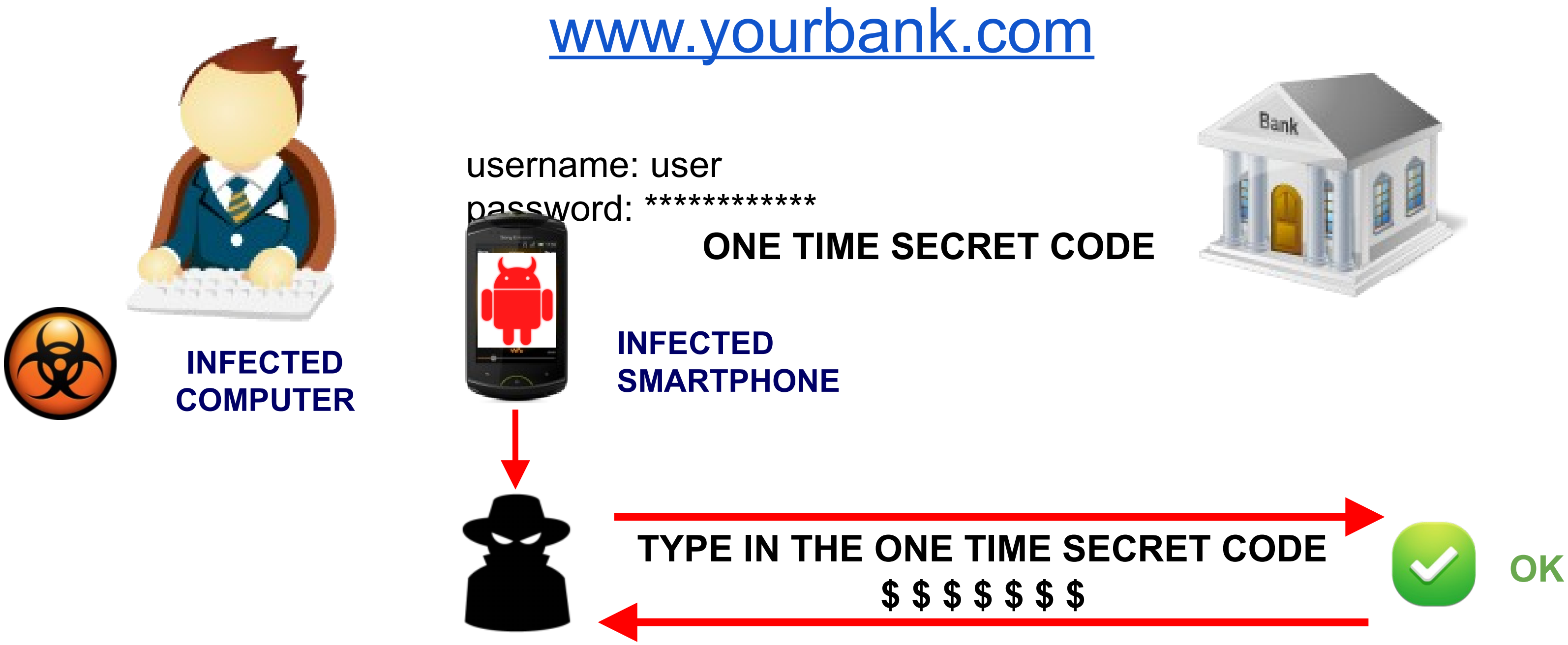
- Info-stealing trojans exploit API hooking techniques to be able to intercept all the data going through the browser even when the connection is encrypted (Man in the Browser attacks)
- They also contain a module called WebInject able to manipulate and modify web pages injecting new content
- The goal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





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

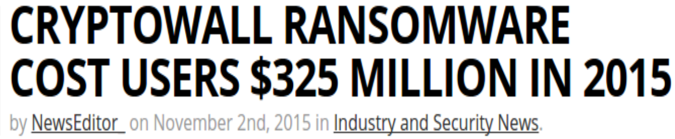
INFECTED SMARTPHONE

TYPE IN THE ONE TIME SECRET CODE

$ $ $ $ $ $ $

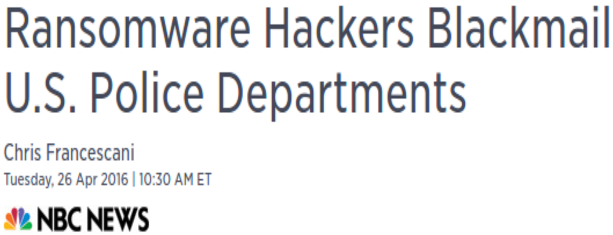
OK

Yet another example: ransomware



CRYPTOWALL RANSOMWARE COST USERS $325 MILLION IN 2015

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

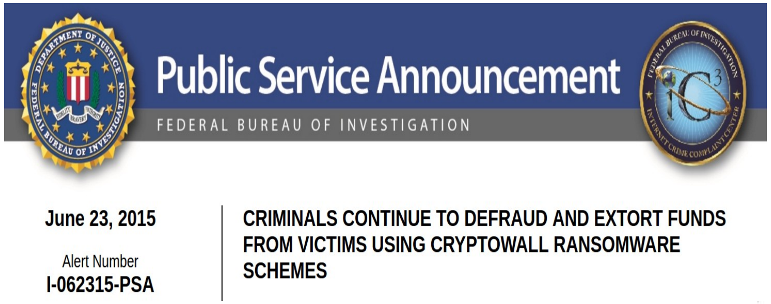


Ransomware Hackers Blackmail U.S. Police Departments

Chris Francescani

Tuesday, 26 Apr 2016 | 10:30 AM ET

NBC NEWS



Public Service Announcement

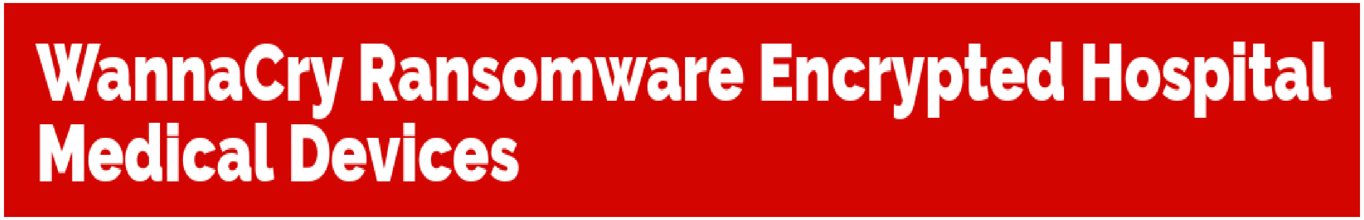
FEDERAL BUREAU OF INVESTIGATION

June 23, 2015

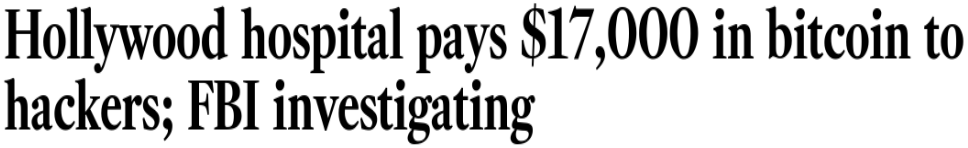
Alert Number

I-062315-PSA

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

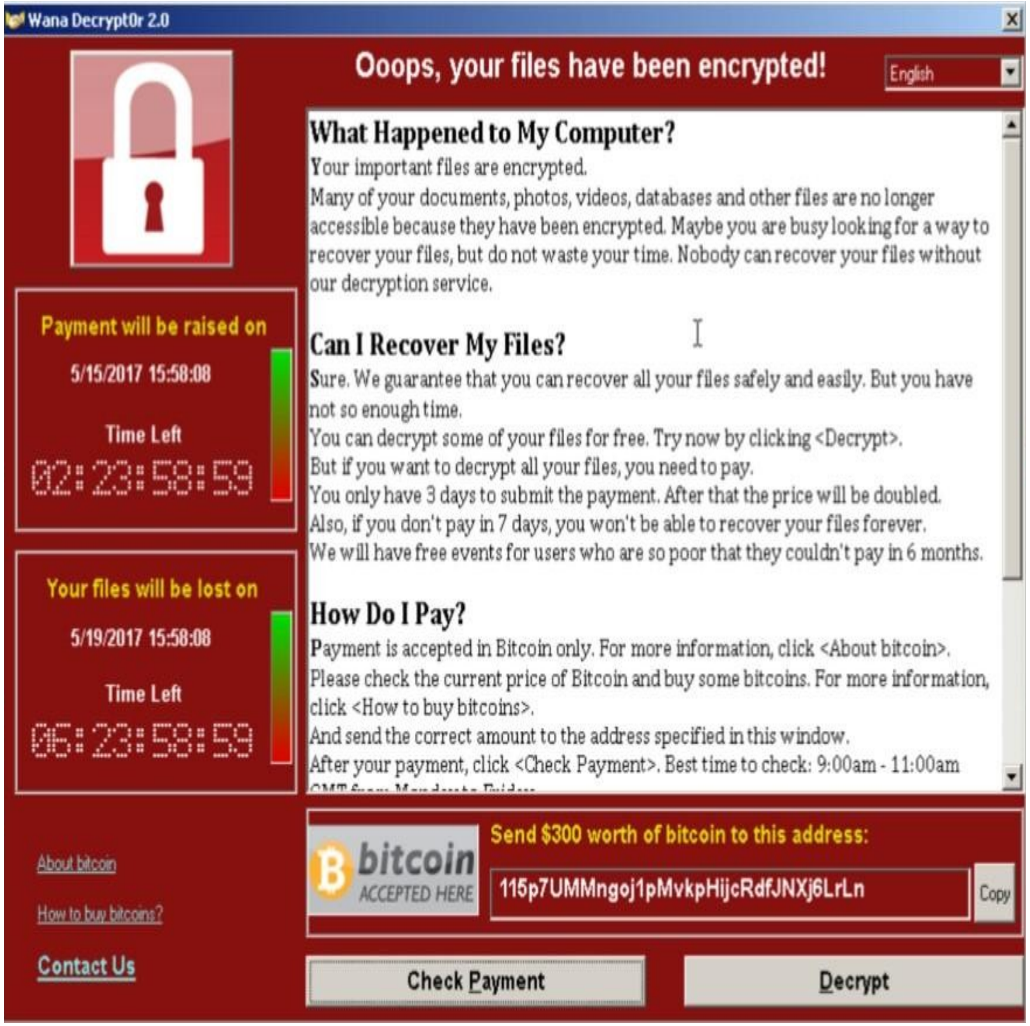


WannaCry Ransomware Encrypted Hospital Medical Devices



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

Do you wannacry?



Ooops, your files have been encrypted!

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

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

AV industry in 1998

AV industry in 2008

Image Copyright: IKARUS Security Software GmbH

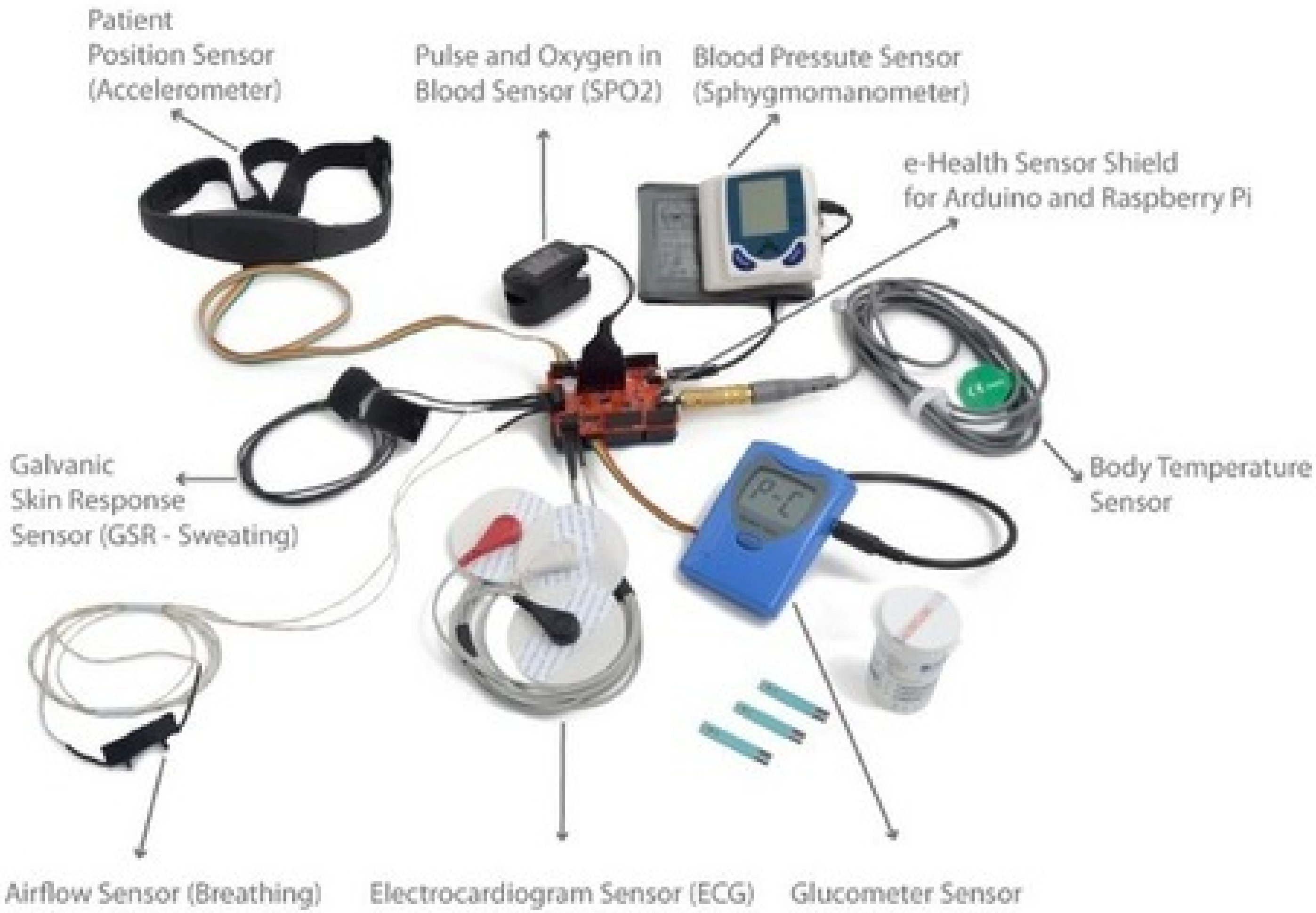
Enter the Internet of Things

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

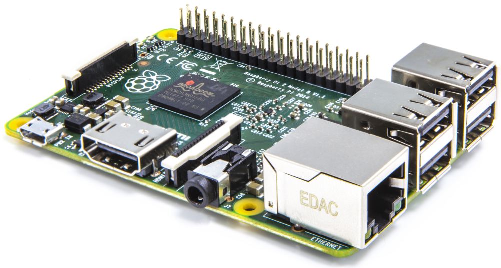
Personal things...

Home things...

Medical things (ouch!)



But also industrial things…!

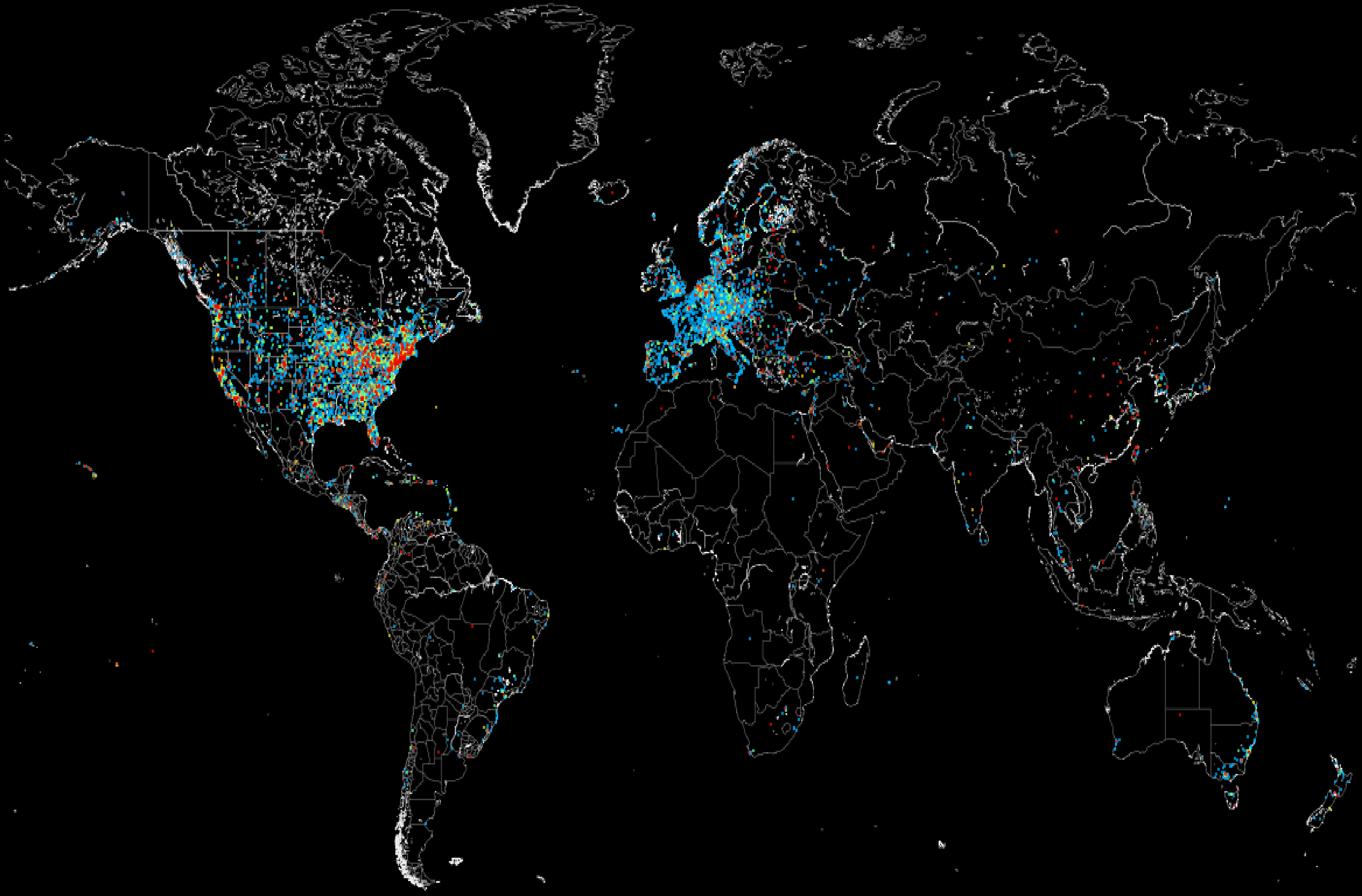


Welcome to the IoIT (Industrial Things)

- **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



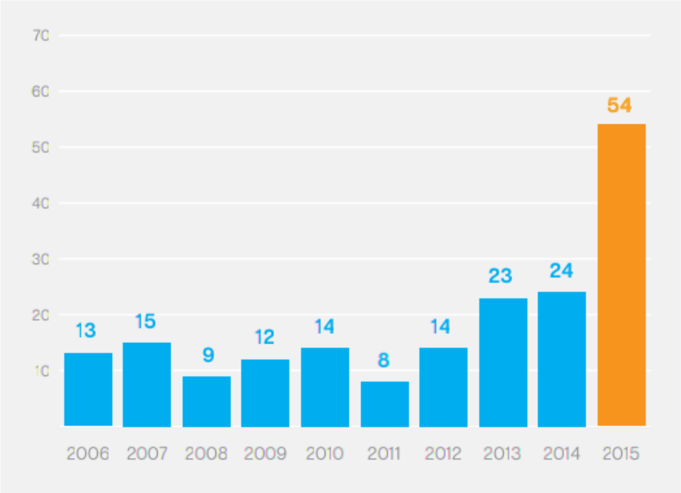
Attacks against ICS share some characteristics

- 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)

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

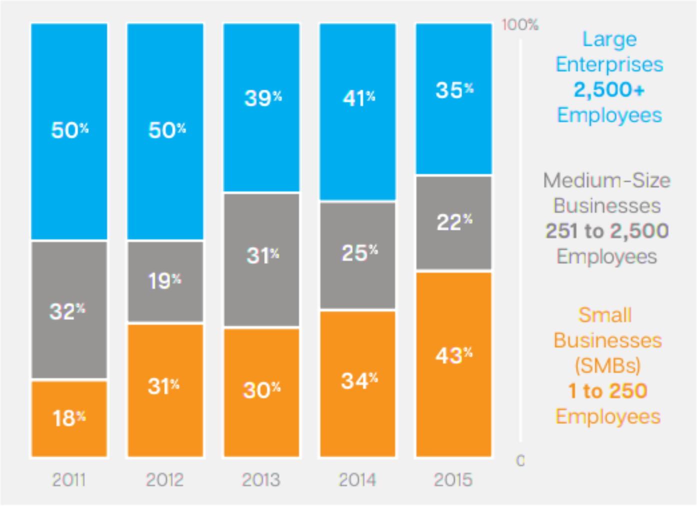
Zero-Day Vulnerabilities, Annual Total

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



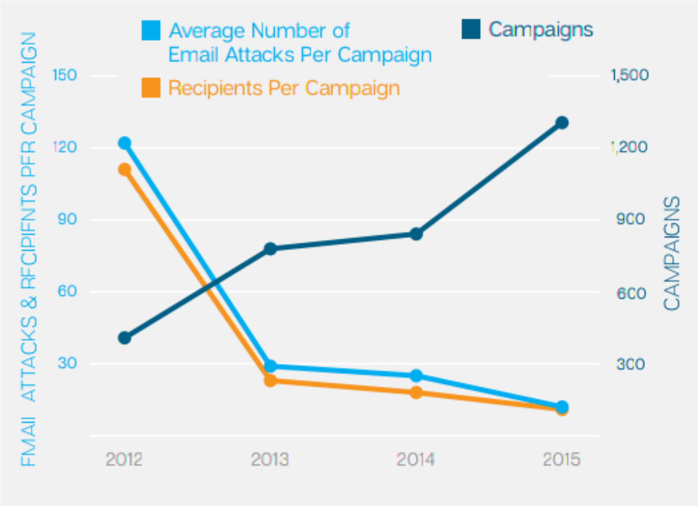
Spear-Phishing Attacks by Size of Targeted Organization

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



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.*



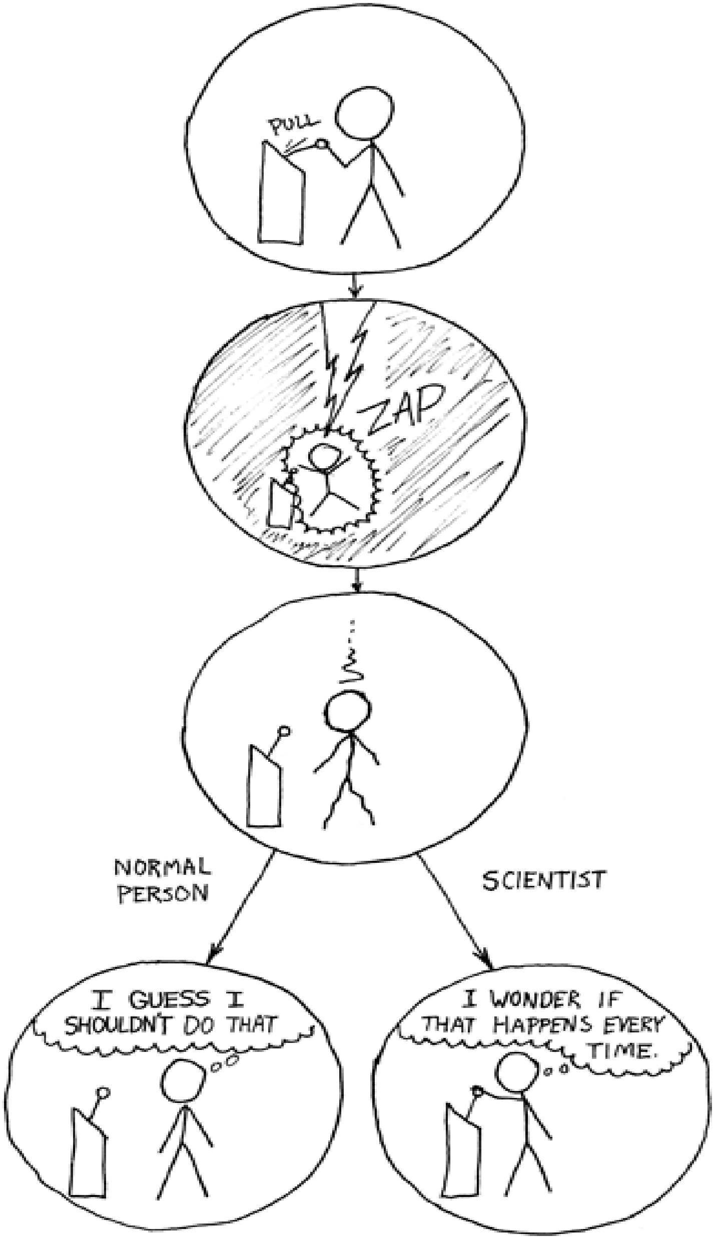
Source: Symantec Internet Security Threat Report 2016

Industrial robot research results

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

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.