POLITECNICO DI MILANO



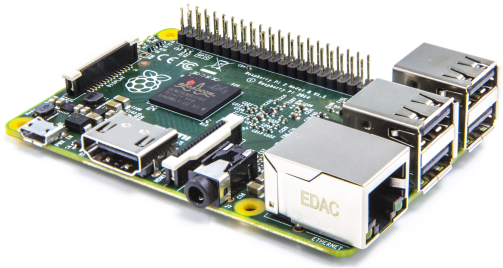


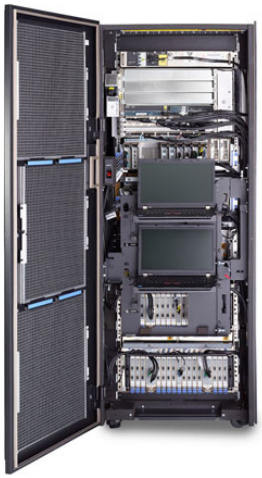
Security challenges in Industry 4.0

Stefano Zanero, PhD

Associate Professor, Politecnico di Milano

Industrial world of connected CPS



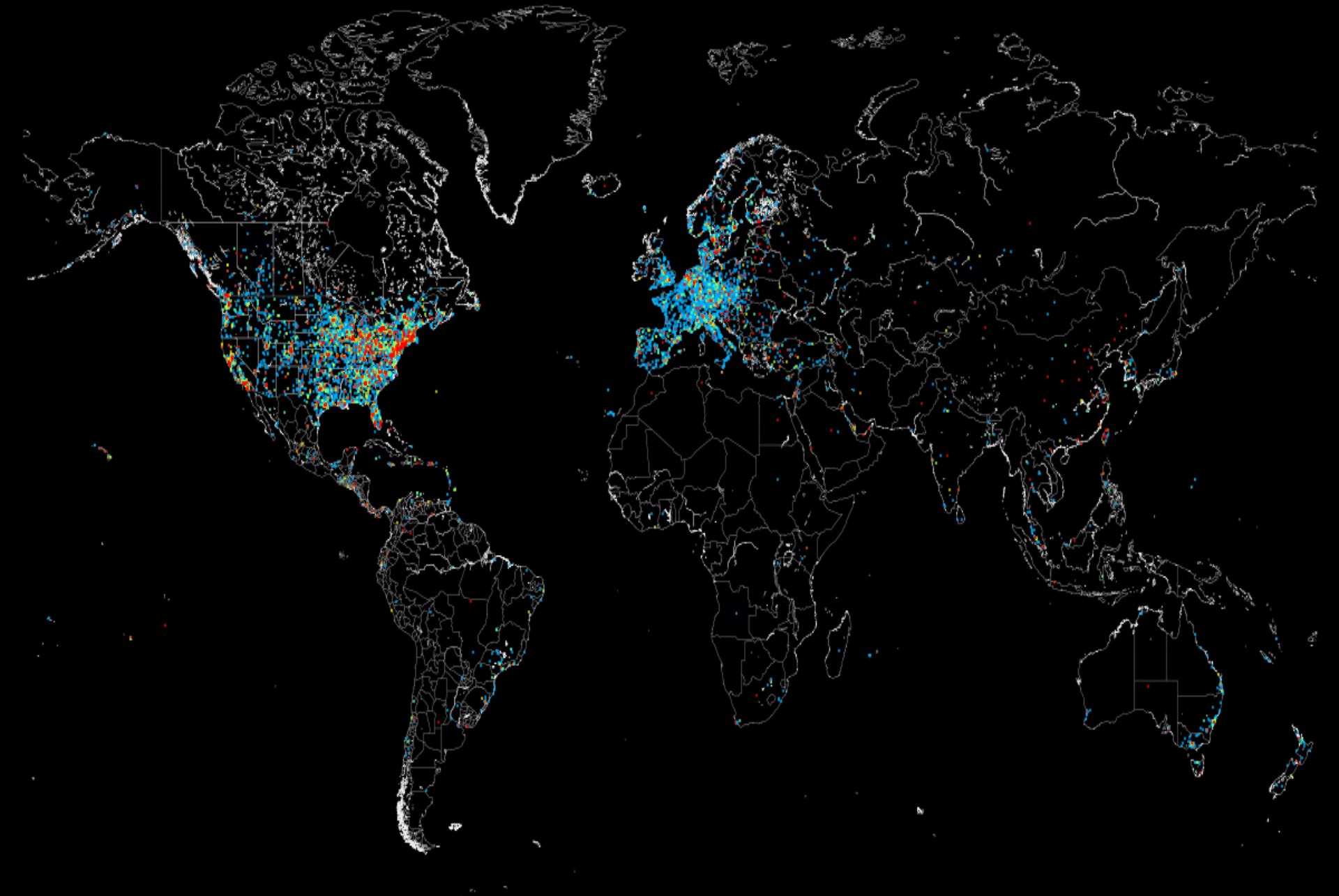


Welcome to the IoIT (Industrial Things)

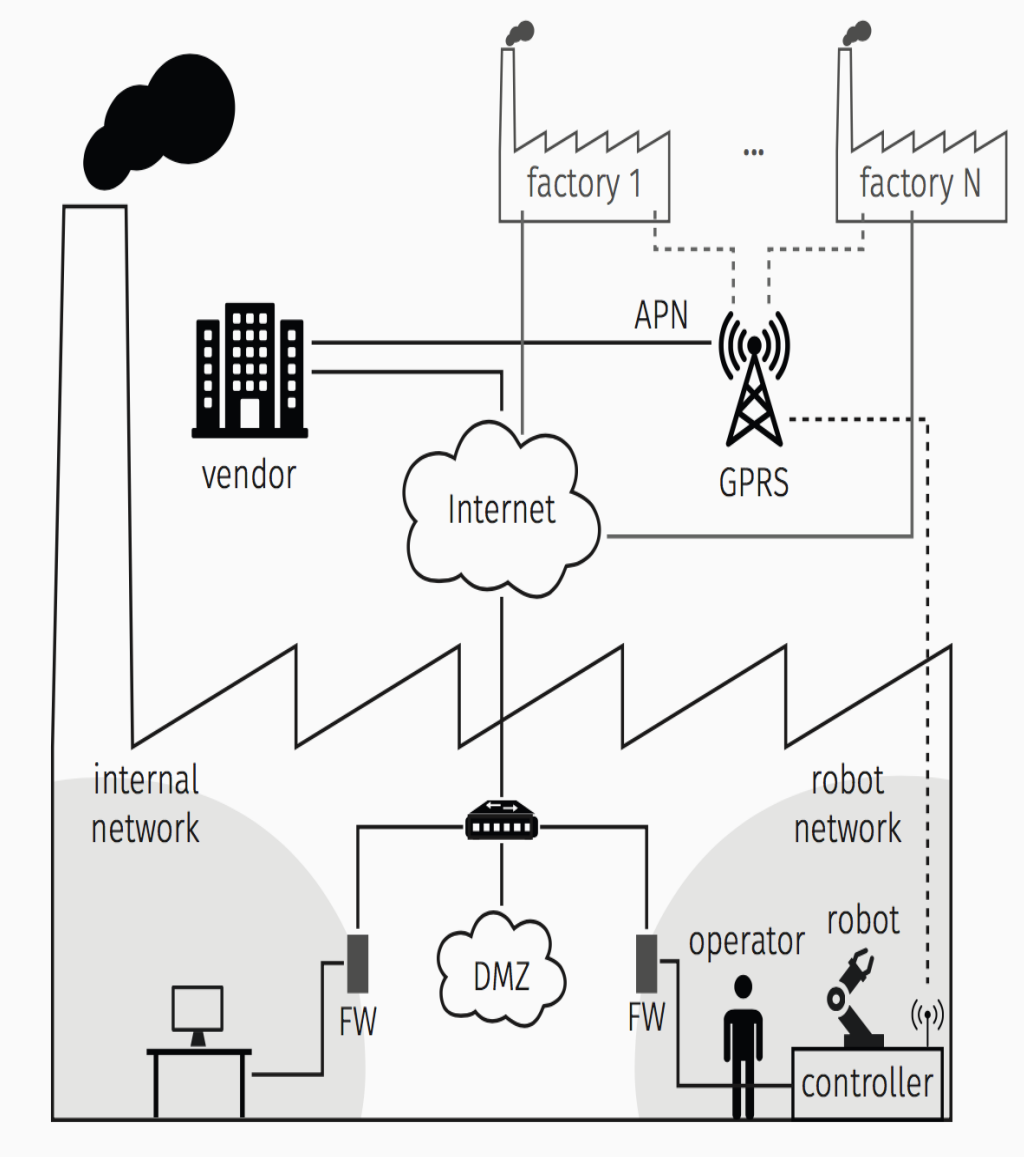
- **Originally-disconnected systems now "opening" to the Internet**
- Critical infrastructure and safety-critical systems
- (sometimes) no humans in the middle
- → Influence environment and humans (≠ data security!)

SHODAN

ICS on the Internet



Modern factory



Modern robots are *meant* to be connected

17.4 Sending PDL2 commands via e-mail

The user is allowed to send PDL2 commands to the C4G Controller Unit, via e-mail. To do that, the required command is to be inserted in the e-mail title with the prefix 'CL' and the same syntax of the strings specified in SYS_CALL built-in. Example: if the required

.fm

l Functionality

command is ConfigureControllerRestartCold, the user m
the e-mail title: 'CL CCRC'.

The authentication is performed by inserting a text whicl
c4gmp program (on a PC), in the message body. Such
system identifier ($BOARD_DATA[1].SYS_ID), the send
the required command, the user login and password; i
inserted into the message body, and it will work as an a
time and the Controller time (as well as the corrs
synchronized, because the message returned by *c4gm*
interval of half an hour, more or less, since the generatic

17.3 Sending/receiving e-mails on C4G Controller

A PDL2 program called "email" is shown below ("email" program): it allows to send and receive e-mails on C4G Controller.

DV4_CNTRL Built-In Procedure is to be used to handle such functionalities.

See DV4_CNTRL Built-In Procedure in Chap. BUILT-IN Routines List section for further information about the e-mail functionality parameters.

17.3.1 "email" program

```
PROGRAM email NOHOLD, STACK = 10000
CONST ki_email_cnfg = 20
  ki_email_send = 21
  ki_email_num = 22
  ki_email_recv = 23
  ki_email_del = 24
  ki_email_hdr = 25
```

Home Store Developers Knowledge Base Ras Blog Robopedia My Account About [Log In]

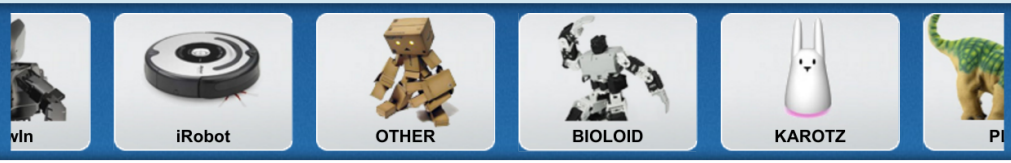
Robot App Store

BETA

OK, now that you've developed the coolest app for your robot, why not making some money out of it? RobotAppStore is the home for every Robot-App™ whether it's for a vacuum cleaner, or the latest humanoid.

Upload Robot App

* We're open only for developers for now.



Share: Tweet 549 Email 21 Share 2 Like 1.3K G+1 70

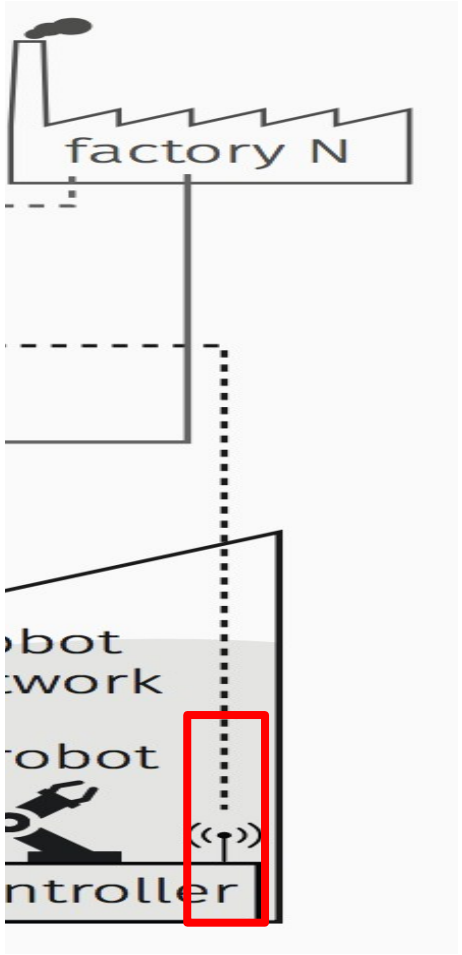
Developer Stories

Everyone can develop applications for robots. Even the robot NAO!. We encourage developers from all around the world to join us now. Opening an account is free and easy. So join us now, and start generating revenues from your Apps!

Twitter Updates

Follow @RobotAppStore 1,753 followers

Factories (and robots) ARE connected



Brand	Overall	Auth. Disabled
eWON	2,800	1,160
Welotec	1	0
Moxa	12,300	2,300
Virtual Access	260	0
Belden	500	0
Westermo	4,000	1,200
NetModule	530	135
Eurotech	0	-
InHand	608	0
Digi	1,200	0
Robustel	2,900	0
Sierra Wireless	0	0

Threat scenarios

1) Production Plant Halting (“up to 20,000$/min”)
2) Production Outcome Alteration
3) Physical Damage
4) Unauthorized Access

- And, of course, there is the ransomware scheme, but that’s not too interesting in the era of “oh, I could ransom that, too!”

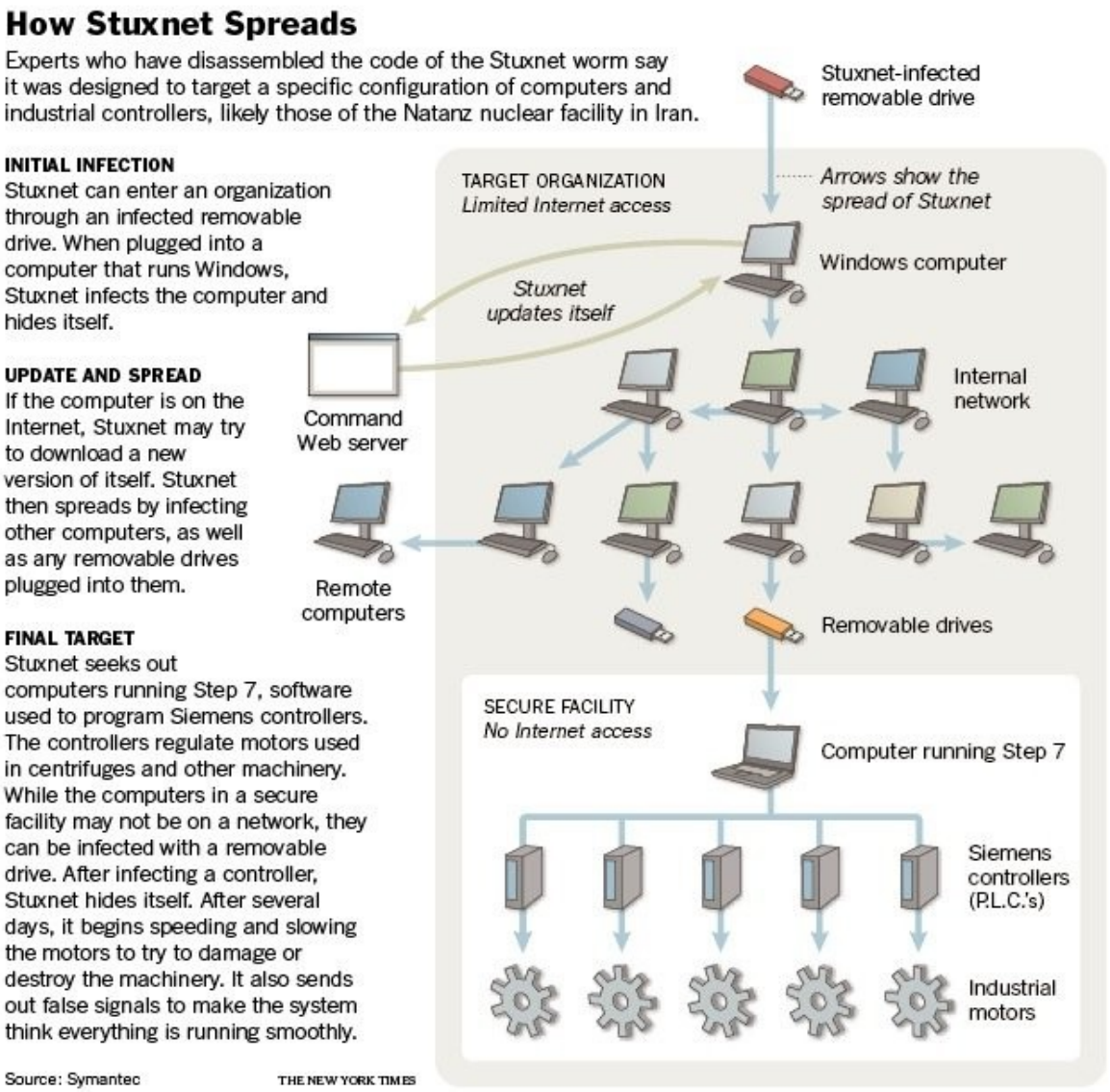
- Find detailed scenarios on http://robosec.org

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!**

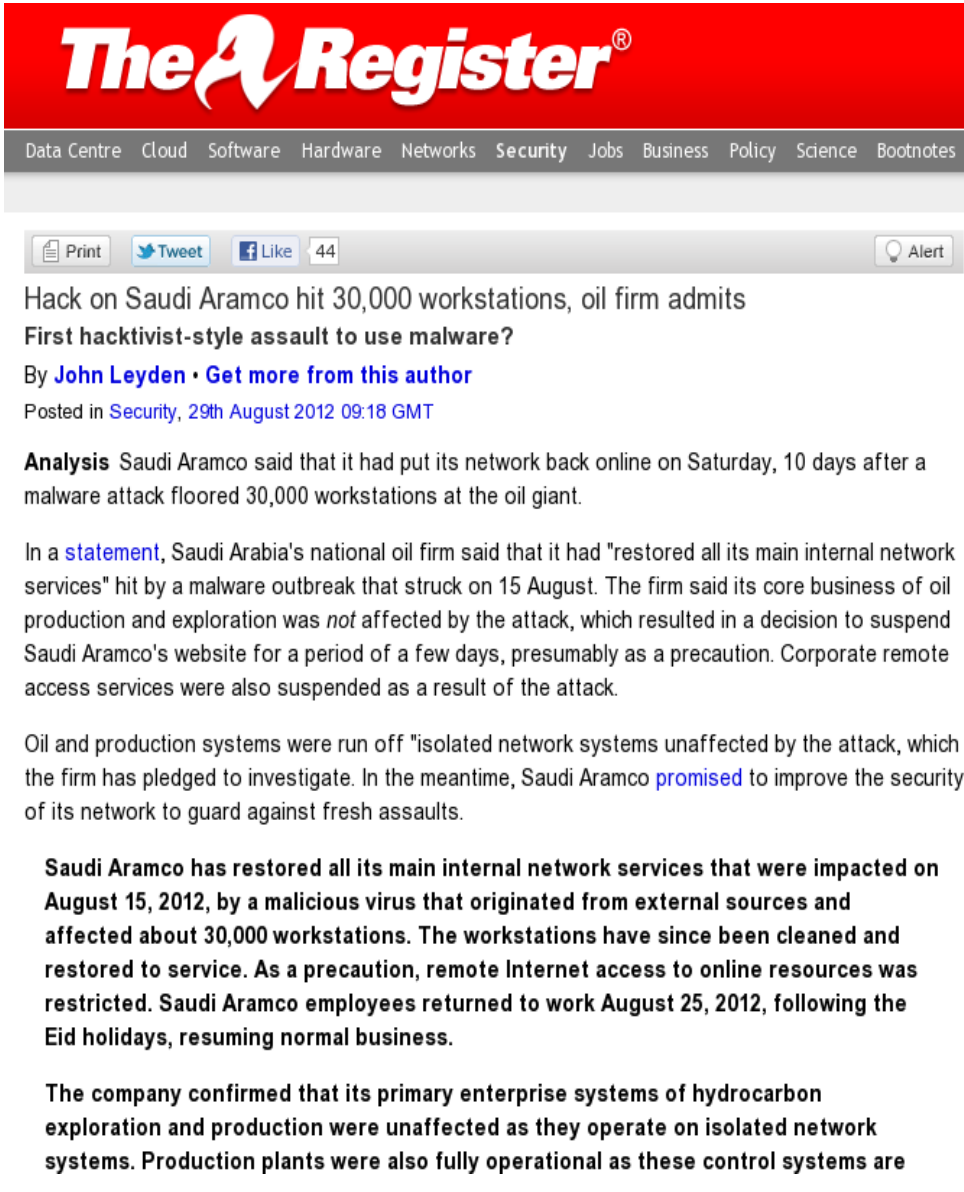
- Read the full research report at http://robosec.org

Non-financial and state-sponsored threats



Businesses on the front line

- Shamoon targeted critical files from a specific company (Saudi Aramco)
- Targeted attack using signed driver component
- Overwrote critical files on 30.000 machines (¾) on the corporate network with a burning American flag
- Claimed by unknown “Cutting Sword of Justice” group on Pastebin



The Register®

Data Centre Cloud Software Hardware Networks **Security** Jobs Business Policy Science Bootnotes

Print Tweet Like 44 Alert

Hack on Saudi Aramco hit 30,000 workstations, oil firm admits

First hacktivist-style assault to use malware?

By John Leyden • Get more from this author

Posted in Security, 29th August 2012 09:18 GMT

Analysis Saudi Aramco said that it had put its network back online on Saturday, 10 days after a malware attack floored 30,000 workstations at the oil giant.

In a statement, Saudi Arabia's national oil firm said that it had "restored all its main internal network services" hit by a malware outbreak that struck on 15 August. The firm said its core business of oil production and exploration was *not* affected by the attack, which resulted in a decision to suspend Saudi Aramco's website for a period of a few days, presumably as a precaution. Corporate remote access services were also suspended as a result of the attack.

Oil and production systems were run off "isolated network systems unaffected by the attack, which the firm has pledged to investigate. In the meantime, Saudi Aramco promised to improve the security of its network to guard against fresh assaults.

Saudi Aramco has restored all its main internal network services that were impacted on August 15, 2012, by a malicious virus that originated from external sources and affected about 30,000 workstations. The workstations have since been cleaned and restored to service. As a precaution, remote Internet access to online resources was restricted. Saudi Aramco employees returned to work August 25, 2012, following the Eid holidays, resuming normal business.

The company confirmed that its primary enterprise systems of hydrocarbon exploration and production were unaffected as they operate on isolated network systems. Production plants were also fully operational as these control systems are

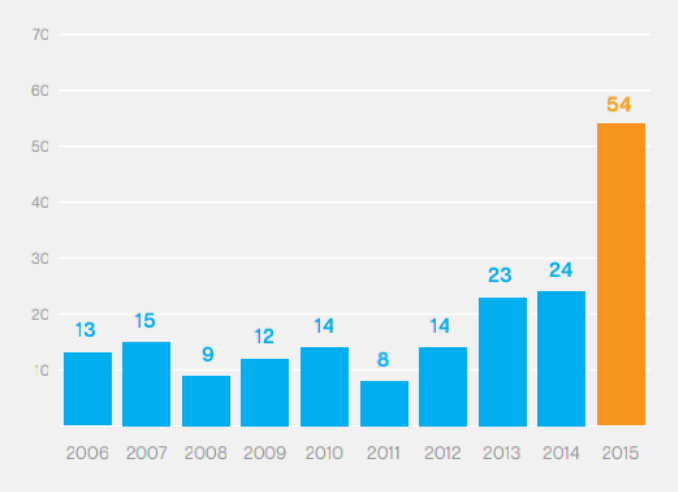
Attacks against ICS share some characteristics

- 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)

The rise of targeted attacks against SME

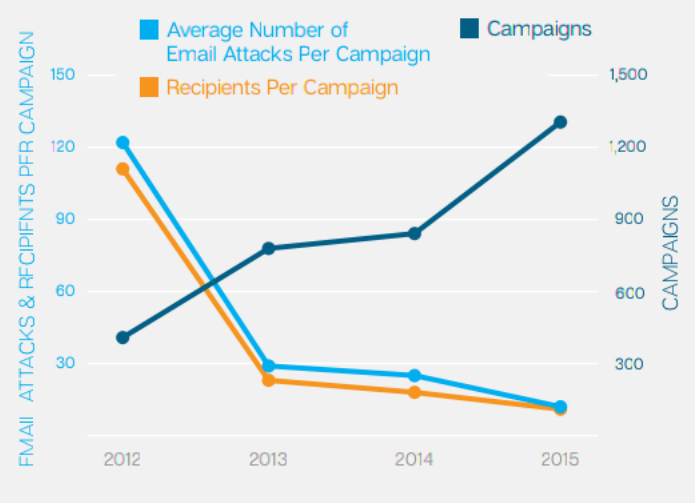
Zero-Day Vulnerabilities, Annual Total

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



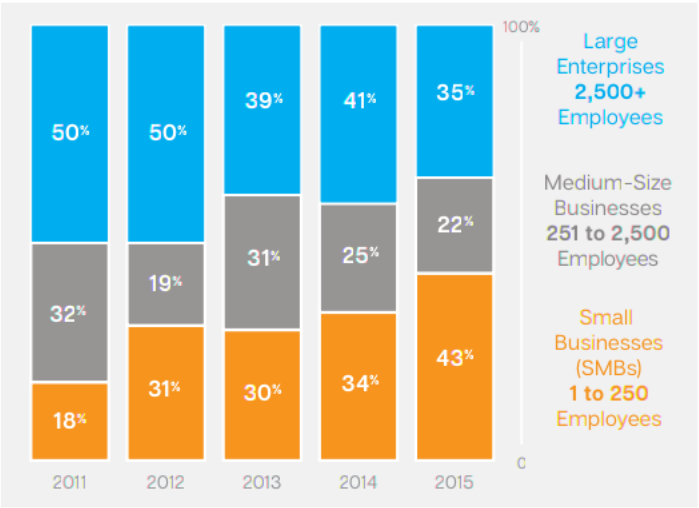
Spear-Phishing Email Campaigns

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

Sometimes, even untargeted attacks...

Articolo »

Cronaca 10 maggio 2019 Casale Monferrato

Nella notte tra martedì e mercoledì

Attacco informatico alla EPTA (IARP)

L'azienda: "Dopo gli opportuni test le normali attività riprenderanno gradualmente a partire da lunedì mattina."

di Massimiliano Francia

Aggiornamento sabato 11 maggio ore 19,30 - Sono stati ripristinati nel corso del pomeriggio di oggi, venerdì alcuni servizi aziendali, tra cui l'accesso al sito aziendale che nel primo pomeriggio risultava oscurato ed è tornato accessibile. Dall'ufficio stampa dell'azienda, verso le 18,30, hanno fatto sapere che alcune attività sono state riprese e che comunque non tutto il gruppo - è stato bloccato dall'attacco haker. Il ritorno alla normalità, insomma sembra essere iniziato e l'auspicio è che la produzione possa riprendere a pieno ritmo al più presto.

Sometimes, even untargeted attacks...

Renault sta riprendendo la produzione dopo un attacco informatico globale

Renault annuncia, dopo la sospensione della produzione da 5 suoi stabilimenti per gli attacchi informatici di venerdì, che tutto sta tornando alla normalità

di *Andrea Senatore*, pubblicato il **15 Maggio 2017** alle ore **19:47**

Il gruppo transalpino Renault e la partner nipponica Nissan hanno dichiarato questo lunedì che le cose stanno tornando alla normalità in quasi tutti i propri impianti, dopo un attacco informatico globale che ha causato danni estesi e la sospensione della produzione in diversi stabilimenti. Renault e il suo partner giapponese sono le uniche case automobilistiche più importanti che finora hanno segnalato problemi di produzione derivanti da **WannaCry ransomware,** l'attacco sul web senza fine che da venerdì si è diffuso in più **di 150 paesi.**

GUIDA: **Renault**

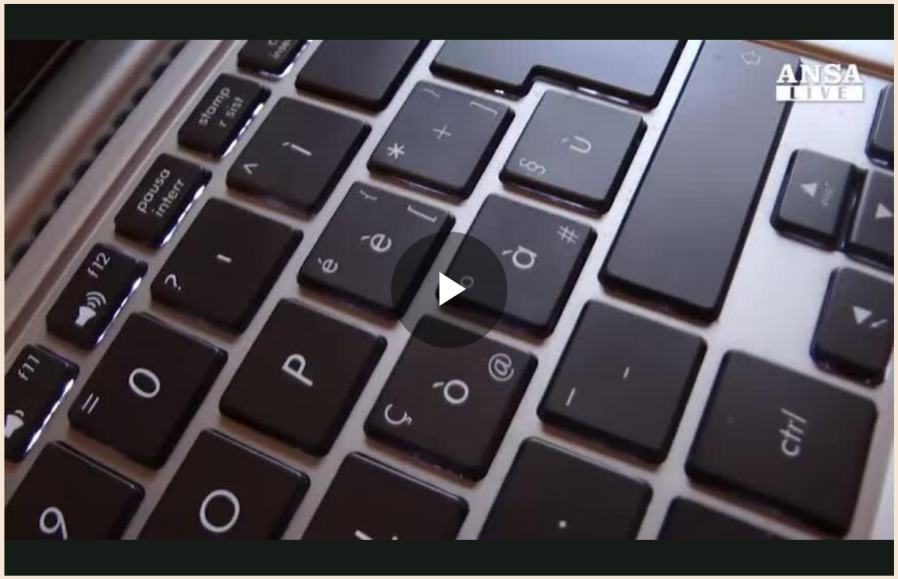
01. Audi, Renault e Volvo: novità importanti dal mondo dei motori
02. Skoda Vision E Concept: ecco come sarà interno ed esterno del veicolo
03. Volkswagen mantiene lontane PSA e Renault, risultati stupefacenti nel primo trimestre 2017
04. Renault e Nissan: collaborazione importante per il futuro dell'auto
05. Renault sta riprendendo la produzione dopo un attacco informatico globale
06. Renault Nissan prevede di superare Volkswagen e Toyota entro fine 2017

Sometimes, even untargeted attacks...

Cyberattacco contro Norsk Hydro, alluminio ai massimi da 3 mesi

–di **Sissi Bellomo** | 20 marzo 2019

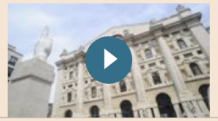
The Trust Project



Nuovo scossone sul mercato dell'alluminio, questa volta a causa del cybercrime. La norvegese **Norsk Hydro**, gigante mondiale attivo in tutta la filiera del metallo, ha rivelato di aver subito un «grave» attacco informatico che l'ha costretta a sospendere la produzione in diversi impianti e a farne funzionare altri in modalità manuale.

Gli hacker sono riusciti a violare i sistemi di sicurezza lunedì sera, presumibilmente negli Stati Uniti, per poi infettare quasi tutta la rete di

VIDEO



15 maggio 2019
Nelle sale operative di Mts, dove si forma lo spread

I PIÙ LETTI DI FINANZA & MERCATI

1. **SERVONO 64 MILIARDI IN DUE MESI** | 19 maggio 2019
   Titoli di Stato, le tre ragioni che possono fare salire la tensione
2. **IL MERCATO** | 19 maggio 2019
   Il mito del debito giapponese: perché non regge il confronto con Tokyo
3. **TRADING DALLO SPAZIO PROFONDO** | 18 maggio 2019
   Profitti stellari: in Borsa con le foto dal satellite guadagni fino al 5% in più
4. **FINANZA** | 19 maggio 2019
   Benetton, cambia l'ad della holding: via Patuano
5. **LA GIORNATA DEI MERCATI** | 17 maggio 2019
   Settimana positiva per Piazza Affari nonostante caro-spread, corre la Juve

ULTIME NOVITÀ
Dal catalogo del Sole 24 Ore

Questions?

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