La sicurezza informatica in navi intelligenti/IoT

Alberto Bartoli

21 Giugno 2019 - ore 15.00

Il Fondo Sociale Europeo in Friuli Venezia Giulia
Programma Operativo Regionale 2014-2020
REGIONE AUTONOMA FRIULI VENEZIA GIULIA
UN INVESTIMENTO PER IL TUO FUTURO
in rete fvg
seminari per l'innovazione in rete

Computer dappertutto...

- Cyber-security
- Atteggiamento comune:
  1. *"Non è un problema"*
  2. *"Ok, ma questa è una possibilità solo teorica "*
  3. *"AIUTO!!!"*

- Speriamo che non accada anche per navi intelligenti / IoT
- La cyber-security non si può "inserire dopo"

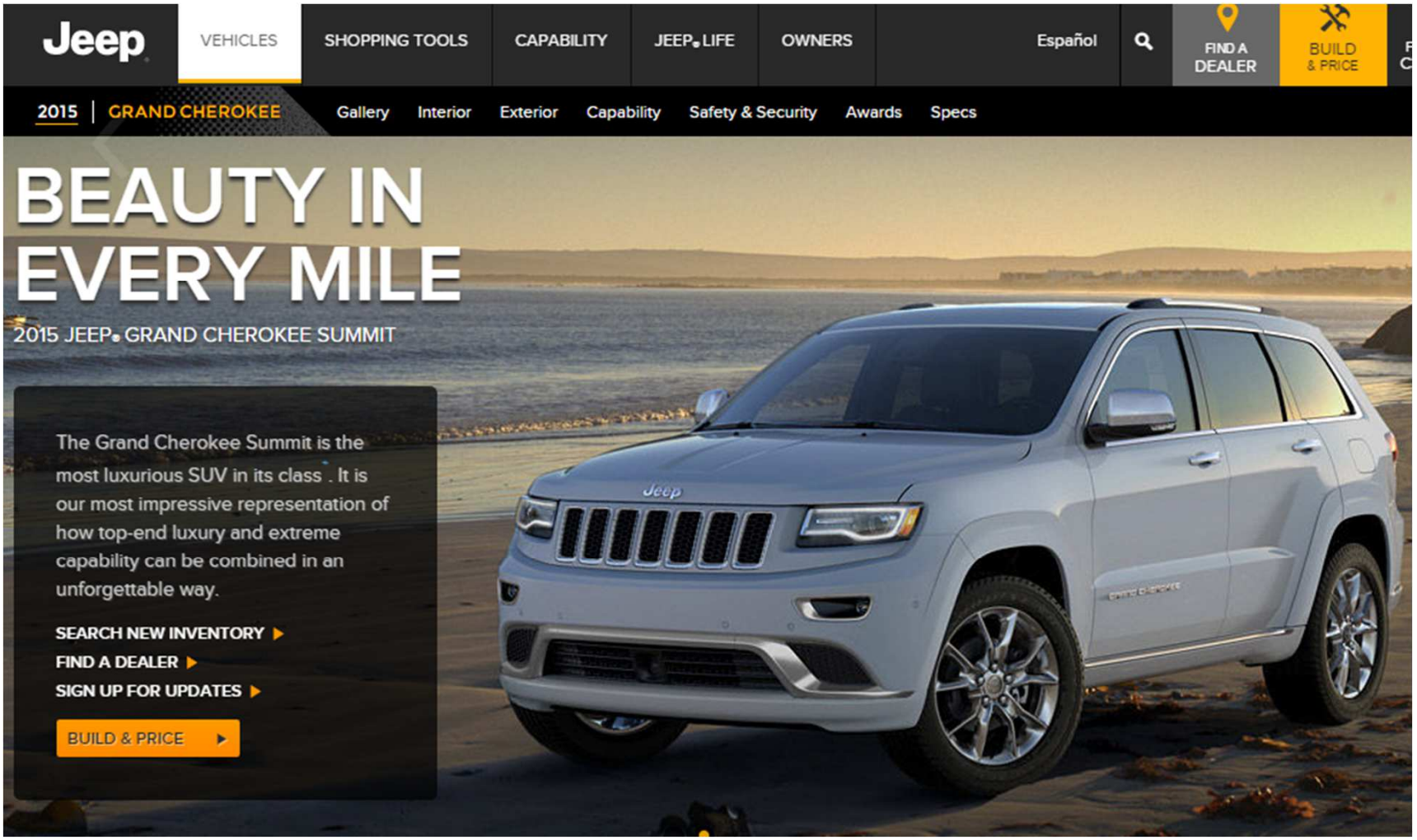
Fatto #1
I computer "sono differenti"

- Ogni sistema software ha molte vulnerabilità
- Errore che ha impatto sulla sicurezza dei dati (progetto, realizzazione, configurazione)

- Impatto comune:
  Utilizzo arbitrario da parte di chiunque,
  spesso da remoto

- Nessun'altra tecnologia ha questa caratteristica
- Problema reale. Non è una possibilità teorica

Automobili (I)
(Luglio 2015)



Dimostrazione

- ...Quando hanno iniziato a giocare da remoto con aria condizionata e radio, dentro di me mi sono congratulato con loro...
- ...Quando l'acceleratore ha smesso di funzionare il divertimento è finito....
- ...Il peggio è stato quando mi hanno disattivato i freni, lasciandomi freneticamente a premere il pedale...

Automobili (II) (Settembre 2016)

Hackers take over Tesla Model S while car is moving

naked security

- Da 20 Km di distanza, mentre l'auto era in movimento...
- ...hanno premuto i freni, aperto il bagagliaio e ripiegato gli specchietti retrovisori...
- ...aperto il tetto, acceso le frecce...

Dispositivi medicali: Pompe insulina (Ottobre 2016)

J&J warns diabetic patients: Insulin pump vulnerable to hacking

- ...un attaccante remoto può attivare iniezioni non autorizzate di insulina...
- ...stando a uno o due Km di distanza...

Dispositivi medicali: Pacemaker (Agosto 2017)

465,000 Patients Need Software Updates for Their Hackable Pacemakers, FDA Says MOTHERBOARD

- ...un attaccante può prendere il controllo del pacemaker...

Rilevatori di Gas (Dicembre 2015)

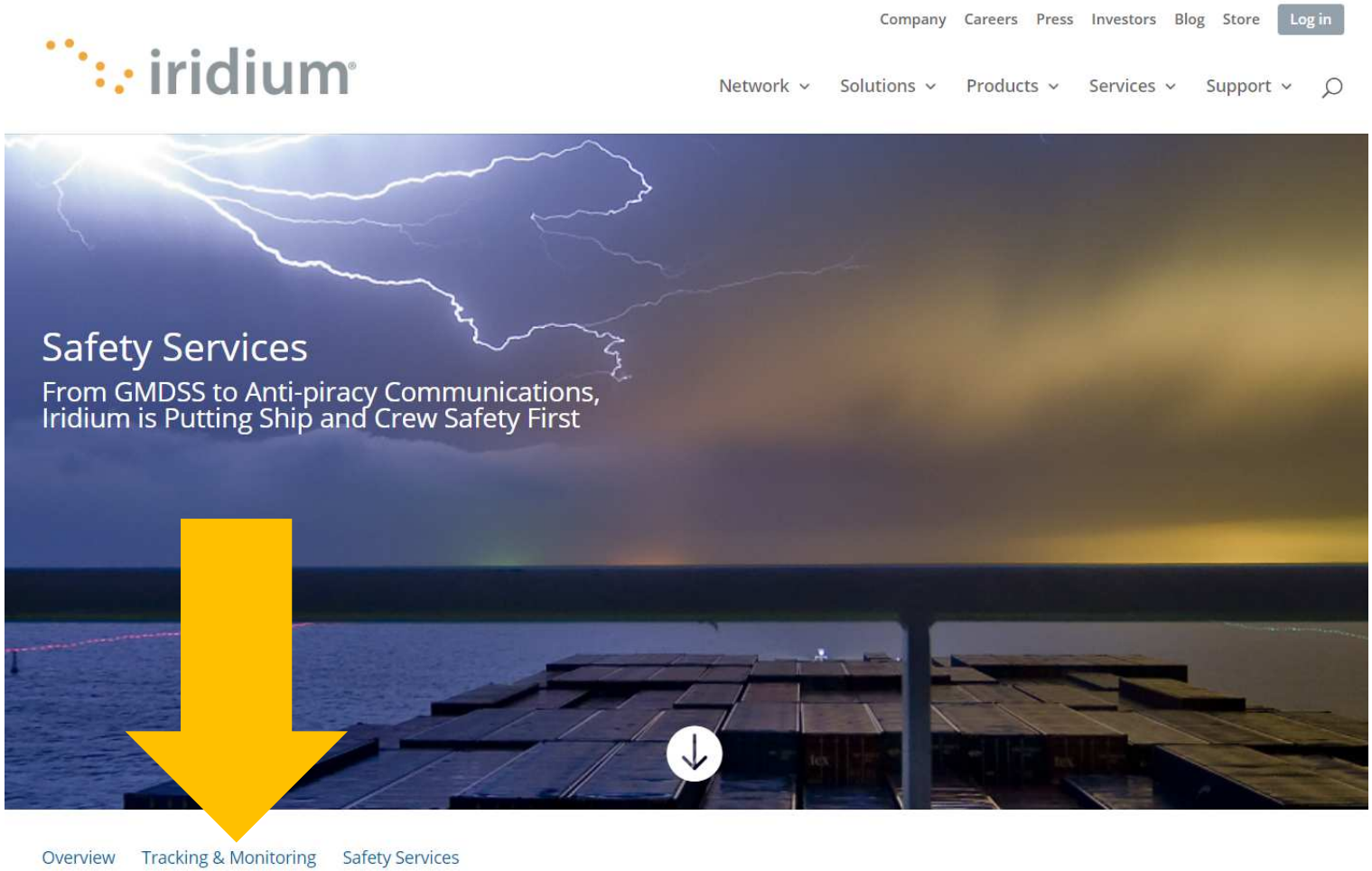
- ...rilevatori di gas usati in impianti di tutto il mondo...rilevano gas tossici e infiammabili ...
- un attaccante remoto senza particolari capacità tecniche può accedere facilmente al rilevatore e cambiare la configurazione

Navi: GPS (Luglio 2013)

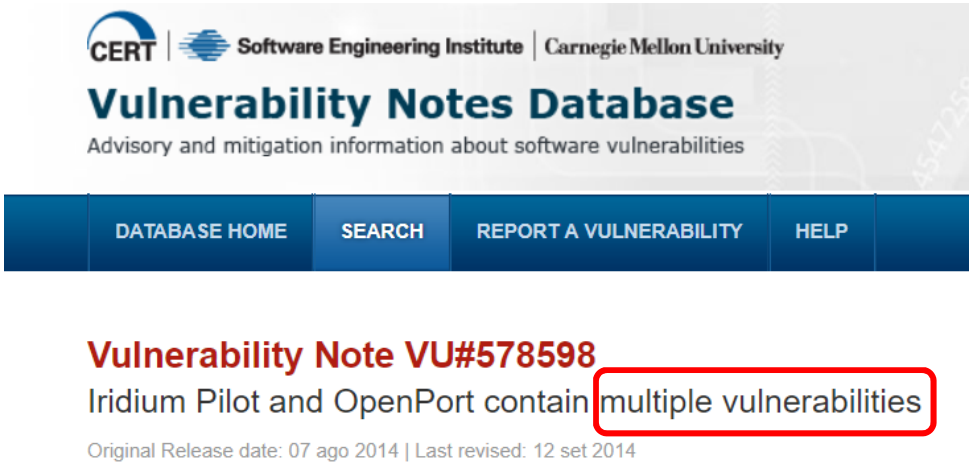
UT Austin Researchers Spoof Superyacht at Sea

- Per il GPS della nave i segnali falsi erano indistinguibili da quelli veri
- "La nave **ha girato** ma il segnale in plancia mostrava solo una **linea retta**"
- "...è stata spostata su una rotta **parallela distante centinaia di metri** da quella voluta"

Navi: Monitoraggio e Tracciamento (2014)

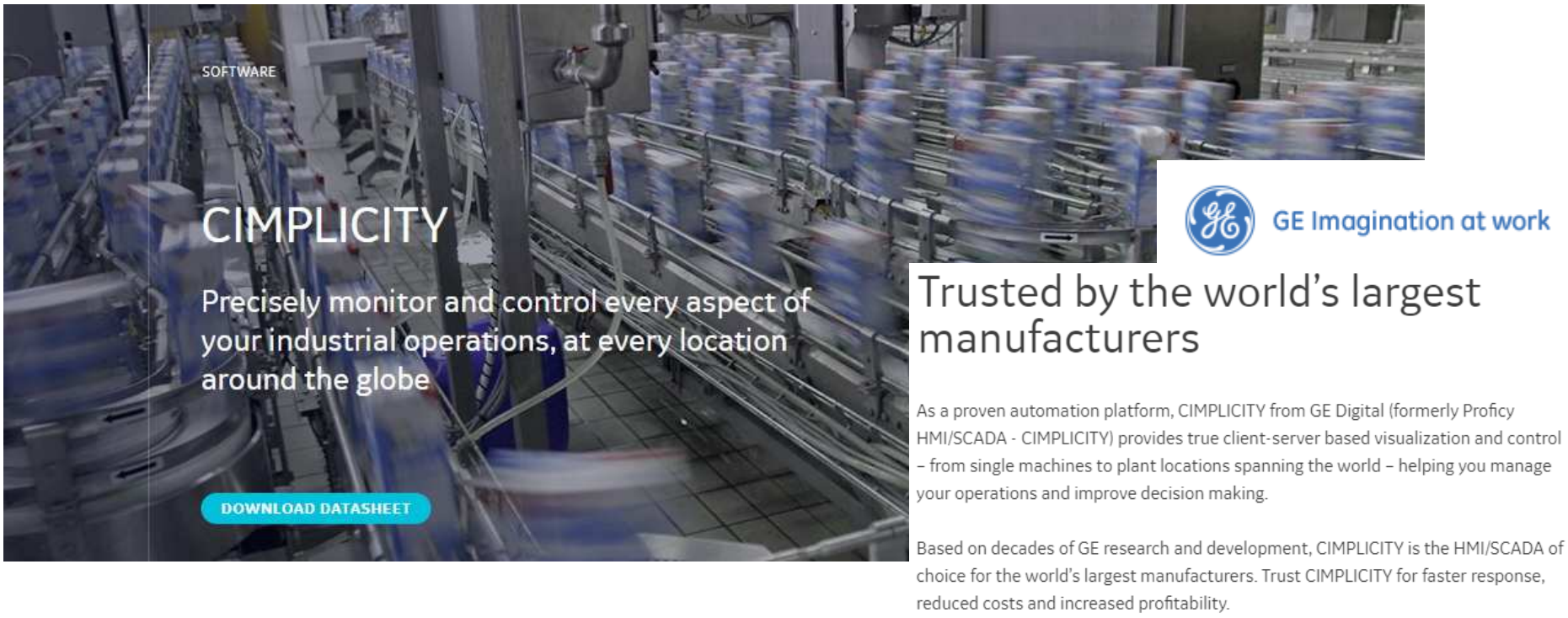


Ahia...



- Un attaccante remoto non autenticato può avere accesso di sistema ed eseguire codice arbitrario
- "Non siamo a conoscenza di nessuna soluzione praticabile"

Sistemi di controllo: (2017)



- Dighe, impianti chimici, acquedotti, energia, agricoltura, trasporti, energia elettrica...

Ahia...

Advisory (ICSA-17-278-01A)

GE CIMPLICITY (Update A)

Original release date: October 05, 2017 | Last revised: October 10, 2017

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

- Un attaccante remoto può eseguire codice arbitrario
- Non richiede capacità tecniche elevate

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT Advisories

Avvisi sui problemi di sicurezza nei dispositivi per controllo industriale

- ICSA-17-087-01 : Siemens RUGGEDCOM ROX I
- ICSA-17-087-02 : 3S-Smart Software Solutions GmbH CODESYS Web Server
- ICSA-17-082-01 : LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA
- ICSMA-17-082-01 : BD Kiestra PerformA and KLA Journal Service Applications Ha
- ICSA-17-047-01 : Rockwell Automation Connected Components Workbench
- ICSA-17-047-02 : Rockwell Automation FactoryTalk Activation
- ICSA-17-075-01 : LCDS - Leão Consultoria e Desenvolvimento de Sistemas LTDA
- ICSA-17-073-01 : Fatek Automation PLC Ethernet Module
- ICSA-17-068-01 : Schneider Electric ClearSCADA
- ICSA-17-066-01 : Schneider Electric Wonderware Intelligence
- ICSA-17-061-01 : Eaton xComfort Ethernet Communication Interface
- ICSA-17-061-02 : Schneider Electric Conext ComBox
- ICSA-17-061-03 : Siemens SINUMERIK Integrate and SINUMERIK Operate
- ICSA-17-059-01 : Siemens RUGGEDCOM NMS
- ICSA-17-054-02 : Red Lion Controls Sixnet-Managed Industrial Switches, Automat Ethernet Switches Vulnerability

Atteggiamento comune (sbagliato)

- Atteggiamento comune verso la cyber-security
  1. *"Non è un problema"*
  2. *"Ok, ma questa è una possibilità solo teorica "*

- *"D'accordo, ho capito che si può fare...*

  ma io non gestisco ***denaro****: a chi vuoi che interessino i miei dispositivi?"*

Fatto #2
Dipende solo dalla convenienza

- Innumerevoli esempi per:
  - Ottenere Guadagno
  - Con Costo Attacco < Guadagno
- Difficili da prevedere (anche per gli esperti)

- Molto diffuso:

  Rendere sistema inutilizzabile fino al pagamento di un riscatto (ransom)

Hotel (Gennaio 2016)

Hotel ransomed by hackers as guests locked out of rooms

THE LOCAL at

- Impossibile riprogrammare chiavi per i nuovi clienti
- Quarta volta

Smart TV (Dicembre 2016)

Japan Reports over 300 Ransomware Attacks on Smart TVs This Year

- TVs completamente bloccata
- Mostra solo istruzioni per il pagamento del riscatto

Ospedali (Febbraio 2016)

Hospital paid 17K ransom to hackers of its computer network

AP

Medical superbugs: Two German hospitals hit with ransomware

Infection forces patients onto phones and medicos onto *faxes*

The Register®

22 MAR 16 **Hospital Declares 'Internal State of Emergency' After Ransomware Infection**

KrebsonSecurity
In-depth security news and investigation

L'amministrazione di una città intera! (Maggio 2019)

Hackers have been holding the city of Baltimore's computers hostage for 2 weeks

recode

- Tutte le operazioni informatiche bloccate (ad eccezione di polizia e pompieri)
- Più di due settimane

Fabbricante di alluminio - NORSK HYDRO (Marzo 2019)

MOTHERBOARD | By Lorenzo Franceschi-Bicchierai | Mar 19 2019, 5:33pm
TECH BY VICE

Ransomware Forces Aluminum Manufacturing Giant to Shut Down Network Worldwide

- Uno dei più grandi al mondo: 35.000 dipendenti in 40 paesi
- Attacco propagato in 160 impianti
- Ha dovuto spegnere la rete in tutto il mondo: produzione e uffici
- Danni stimati 50$ milioni

Guadagno:
Anche non "monetizzabile" direttamente

- SE Costo Attacco < Guadagno Sperato
- ALLORA Ahia...

- Ransomware fornisce guadagno:
  - "monetario"
  - diretto
- Innumerevoli esempi con guadagno:
  - "di altra natura"
  - indiretto

Cartelle sanitarie (Stati Uniti 2015)

Data Breaches In Healthcare Totaled Over 112 Million Records In 2015

Forbes

- 112 milioni di file (35% popolazione US)
- 6 furti > 1.000.000
- 253 furti > 500

Cartelle sanitarie (Norvegia 2018)

'Professional' hack on Norwegian health authority compromises data of three million patients

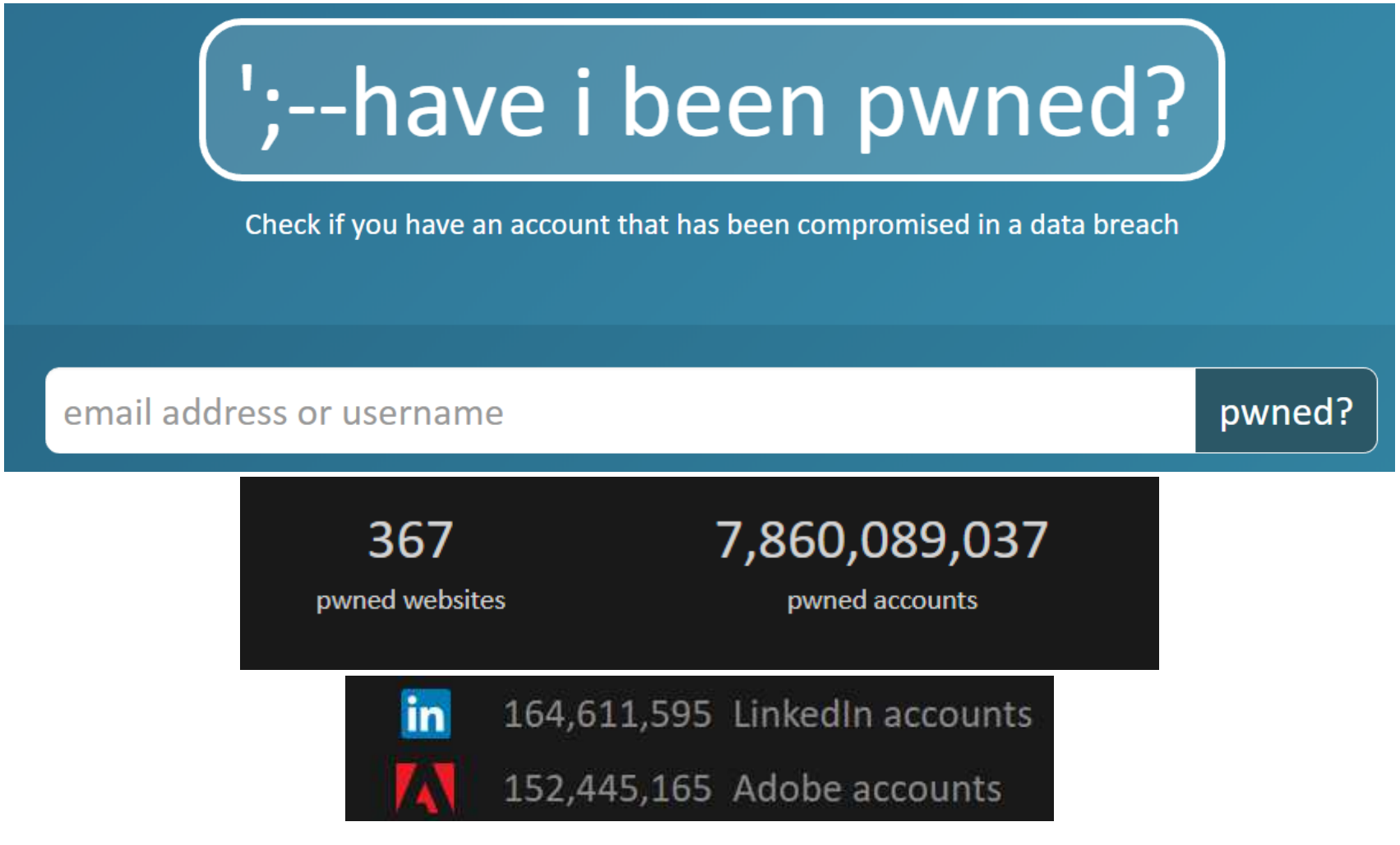
the INQUIRER

Local security centre blames breach on 'advanced' hackers

- Letteralmente mezza Norvegia...

18 January 2018

Password
https://haveibeenpwned.com/



Impronte digitali (Settembre 2015)

Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says

The New York Times

- Sono state trafugate le impronte digitali di 5.6 milioni di dipendenti pubblici
- Biometric authentication? Una password può essere revocata...una impronta digitale no
- Potenziale per ricatti enorme

Altro atteggiamento comune (sbagliato)

- Atteggiamento comune verso la cyber-security
  1. *"Non è un problema"*
  2. *“Ok, questo è una possibilità teorica"”*

- *"D'accordo, ho capito che si può fare...*

  ma chi vuoi che sia interessato ad attaccare ***proprio me****, la mia casa, la mia nave....?"*

Tipologie di attacco: Mirato

1. Attaccante ti prende di mira
2. Raccoglie informazioni
3. Cerca di capire come fare

- ❑ Poco automatizzabile
- ❑ Costoso

- ❑ Poco Frequente

Tipologie di attacco: NON Mirato

- Attaccante "spara nel mucchio"
  (prova da usare la **stessa** vulnerabilità **ovunque**)

- Molto automatizzabile
- Economico

- Molto Frequente

MAERSK (Estate 2017): Bloccata da attacco NON mirato

Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack

BLEEPINGCOMPUTER January 25, 2018

- Il più grande armatore di navi mercantili del mondo
- Ha dovuto reinstallare 4,000 servers, 45,000 PCs, e 2500 applicativi
- "Immaginate un'azienda dove una nave con 20.000 container entra in un porto ogni 15 minuti, e non avete i computer"

Estate 2017:
Bloccate da attacco NON mirato

Last month's malware outbreak cost this household company

£100 million

Reckitt Benckiser

tripwire

NotPetya cyber-attack cost TNT at least $300m

BBC

"Chi vuoi che attacchi proprio me?"

- Atteggiamento SBAGLIATISSIMO
- Gli attacchi **più comuni** sono quelli **non mirati**
- Ogni dispositivo connesso in rete è un bersaglio potenziale

Colleghiamo tutto!!!

- Sistemi di controllo industriale
- ...
- Sistemi di tracking/monitoraggio navi
- ...
- Termostati
- Webcam
- Lavatrici / Lavastoviglie / Sex toys / Materassi
- ...

- Qual'è il rischio?

Ragionamento comune (sbagliatissimo)

- *"Ho capito che potrei essere attaccato, ma tanto c'è la **password**!"*

- *"Basta che la scelga in maniera adeguata"*

Esempio:
Access, Monitor and Control

Remotely Monitor, Manage and Control Industrial Equipment Over the Net

The UDS1100-IAP is a rugged and powerful tool which enables users to connect, manage and control just about any piece of industrial equipment from virtually anywhere over Ethernet or the Internet.

- Vulnerabilità:
  - Richiesta di formato errato
  - Risponde con le proprie informazioni di configurazione compresa la password
- Con sforzo minimo se ne trovano 6400 collegati a Internet

Ragionamento corretto

- SE il dispositivo **non ha vulnerabilità**
- ALLORA sono protetto dalla password
- ALTRIMENTI la password potrebbe essere inutile

- **Dispositivo vulnerabile** può essere attaccato (con successo) da chiunque:
  1. Conosce la vulnerabilità e sa come sfruttarla
  2. Riesce a rendere
     Costo Attacco < Guadagno Atteso

Ricordare sempre

- Ogni software raggiungibile da una rete
  può essere attaccato da quella rete

- Ogni software raggiungibile da Internet
  può essere attaccato da ogni parte del mondo

- Una **vulnerabilità** può rendere le password **inutili**

Come mi difendo?

Sintesi poco consolante...

Stanford Congressional Cyber Boot Camp
August 2015

Stanford | CISAC Center for International Security and Cooperation

"Quale che sia il vostro livello di preoccupazione sulla cybersecurity,
dovreste essere ancora più preoccupati"

Reid Hoffman - Co-fondatore LinkedIn

Grazie per l'attenzione

Google

"alberto bartoli trieste"