

La sicurezza informatica in navi intelligenti/IoT

Alberto Bartoli

21 Giugno 2019 - ore 15.00



REGIONE AUTONOMA
FRIULI VENEZIA GIULIA

UN INVESTIMENTO PER IL TUO FUTURO



Computer dappertutto...

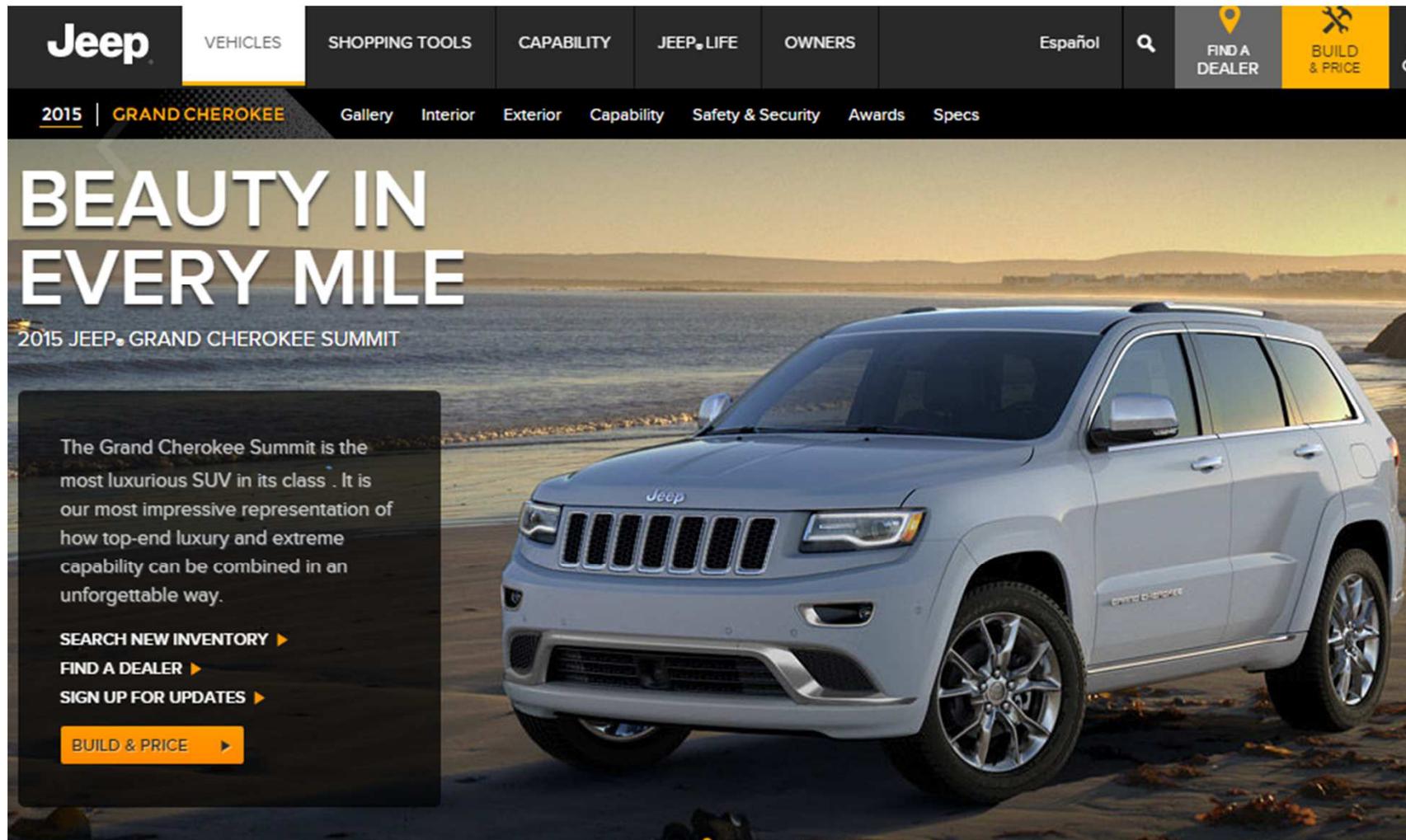
- ❑ Cyber-security
- ❑ Atteggiamento comune:
 1. *"Non è un problema"*
 2. *"Ok, ma questa è una possibilità solo teorica "*
 3. *"AIUTO!!!"*
- ❑ Speriamo che non accada anche per navi intelligenti / IoT
- ❑ La cyber-security non si può "inserire dopo"

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)



The screenshot shows the Jeep website's product page for the 2015 Grand Cherokee Summit. The top navigation bar includes the Jeep logo, a 'VEHICLES' menu, and various utility links like 'SHOPPING TOOLS', 'CAPABILITY', 'JEEP LIFE', and 'OWNERS'. A search bar and 'FIND A DEALER' button are also present. Below the navigation, a secondary menu lists '2015 | GRAND CHEROKEE' and sub-categories like 'Gallery', 'Interior', 'Exterior', 'Capability', 'Safety & Security', 'Awards', and 'Specs'. The main content area features a large image of a silver Jeep Grand Cherokee Summit parked on a beach at sunset. The headline reads 'BEAUTY IN EVERY MILE' and the sub-headline is '2015 JEEP GRAND CHEROKEE SUMMIT'. A text box on the left describes the vehicle as the most luxurious SUV in its class, combining top-end luxury with extreme capability. Below this text are four call-to-action buttons: 'SEARCH NEW INVENTORY', 'FIND A DEALER', 'SIGN UP FOR UPDATES', and 'BUILD & PRICE'.

Jeep VEHICLES SHOPPING TOOLS CAPABILITY JEEP LIFE OWNERS Español   FIND A DEALER  BUILD & PRICE

2015 | GRAND CHEROKEE Gallery Interior Exterior Capability Safety & Security Awards Specs

BEAUTY IN EVERY MILE

2015 JEEP GRAND CHEROKEE SUMMIT

The Grand Cherokee Summit is the most luxurious SUV in its class . It is our most impressive representation of how top-end luxury and extreme capability can be combined in an unforgettable way.

[SEARCH NEW INVENTORY](#) ▶

[FIND A DEALER](#) ▶

[SIGN UP FOR UPDATES](#) ▶

[BUILD & PRICE](#) ▶

Dimostrazione

- ❑ ...Quando hanno iniziato a giocare da remoto con **aria condizionata** e **radio**, dentro di me mi sono congratolato 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...

WIRED

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)

safety equipment vulnerable to a remote 'attacker with low skill'

naked **security**

- ❑ ...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**

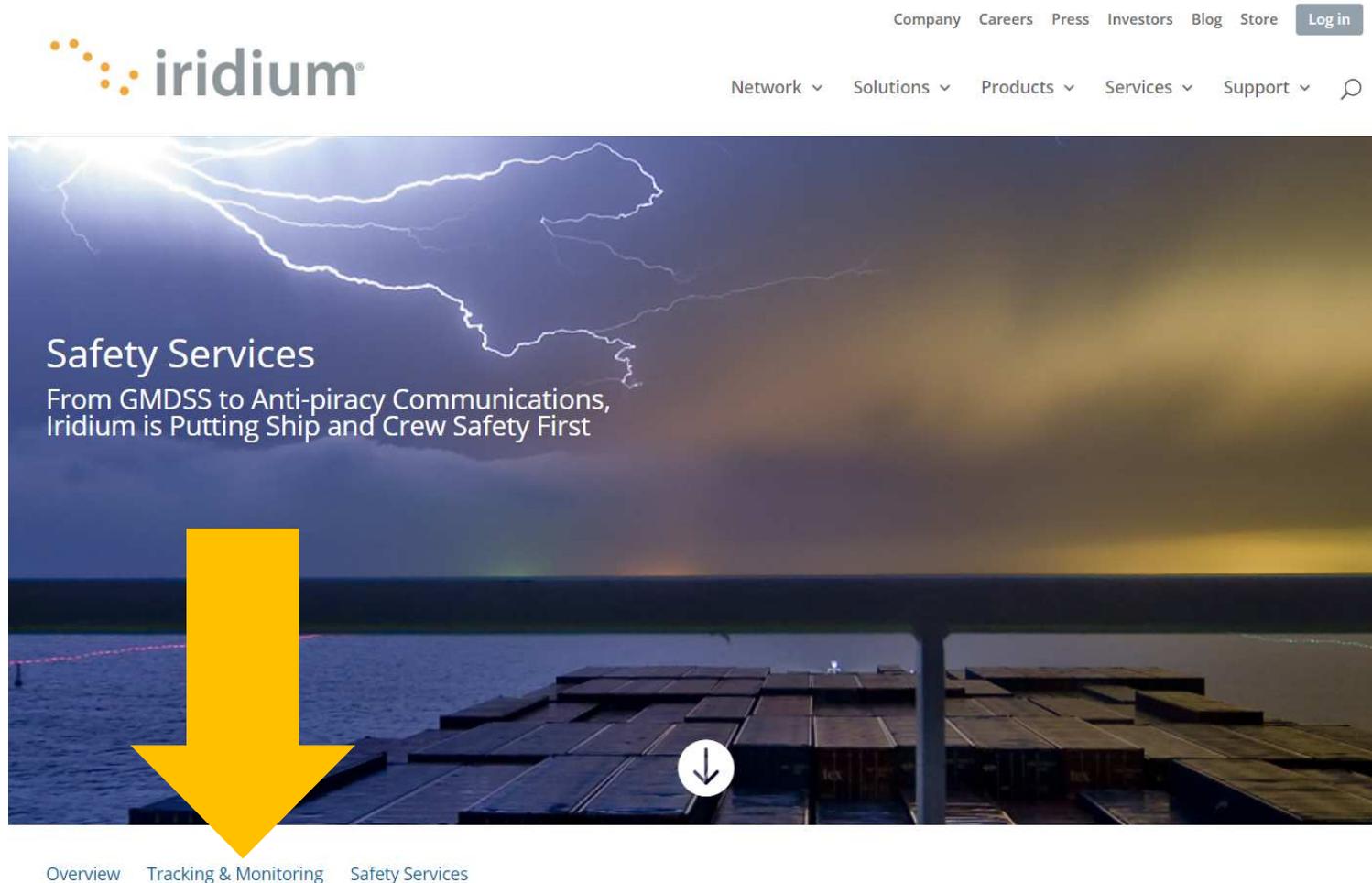
Navi: GPS (Luglio 2013)

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)



The screenshot shows the Iridium website's navigation bar with links for Company, Careers, Press, Investors, Blog, Store, and a Log in button. Below the navigation bar are dropdown menus for Network, Solutions, Products, Services, and Support, along with a search icon. The main content area features a large image of a ship's deck at night with lightning in the sky. The text 'Safety Services' is prominently displayed, followed by the subtext 'From GMDSS to Anti-piracy Communications, Iridium is Putting Ship and Crew Safety First'. A large yellow arrow points down from the 'Safety Services' text to a navigation menu at the bottom of the page, which includes 'Overview', 'Tracking & Monitoring', and 'Safety Services'. A small white arrow icon is also visible on the image.

Company Careers Press Investors Blog Store [Log in](#)

Network Solutions Products Services Support

Safety Services

From GMDSS to Anti-piracy Communications,
Iridium is Putting Ship and Crew Safety First

Overview Tracking & Monitoring Safety Services

Ahia...



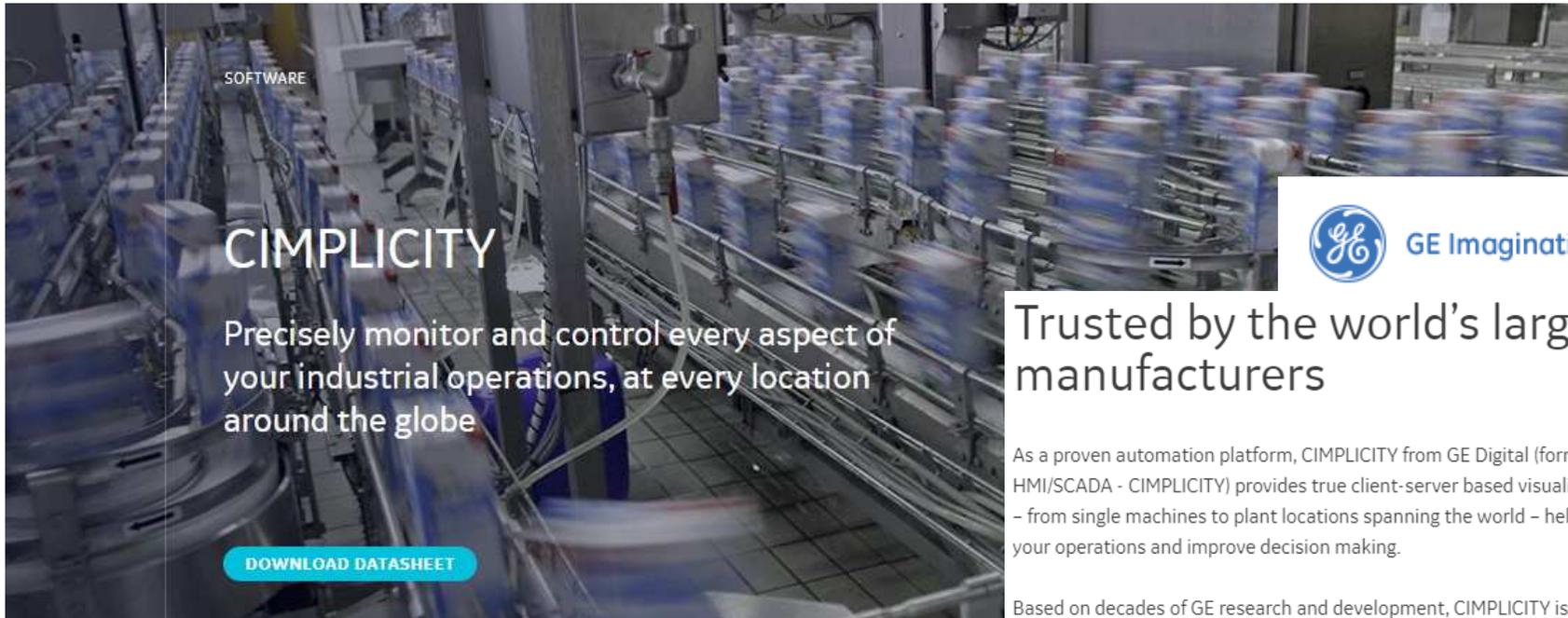
Vulnerability Note VU#578598

Iridium Pilot and OpenPort contain **multiple vulnerabilities**

Original Release date: 07 ago 2014 | Last revised: 12 set 2014

- ❑ 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)



SOFTWARE

CIMPPLICITY

Precisely monitor and control every aspect of your industrial operations, at every location around the globe

[DOWNLOAD DATASHEET](#)



GE Imagination at work

Trusted by the world's largest manufacturers

As a proven automation platform, CIMPPLICITY from GE Digital (formerly Proficy HMI/SCADA - CIMPPLICITY) provides true client-server based visualization and control - from single machines to plant locations spanning the world - helping you manage your operations and improve decision making.

Based on decades of GE research and development, CIMPPLICITY is the HMI/SCADA of choice for the world's largest manufacturers. Trust CIMPPLICITY for faster response, reduced costs and increased profitability.

- ❑ 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



- 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
- IC SMA-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)

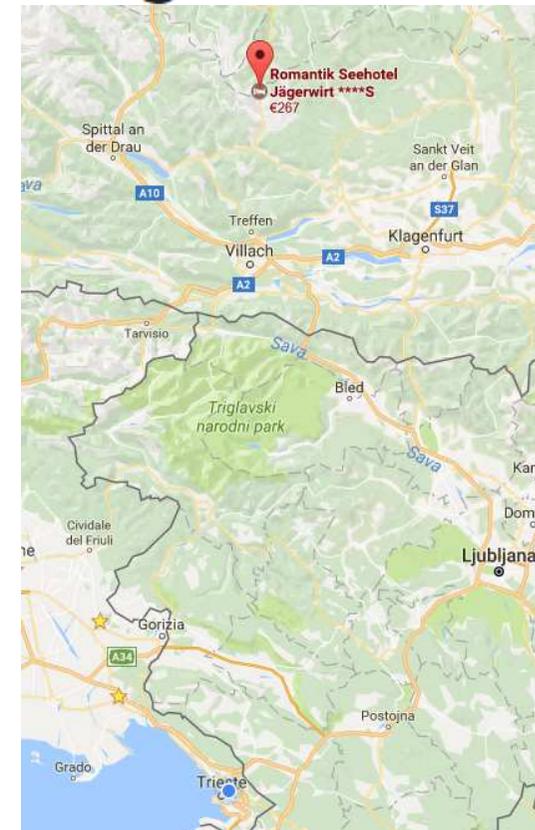
- ❑ Molto diffuso:
 - Rendere sistema inutilizzabile** fino al pagamento di un **riscatto (ransom)**

Hotel (Gennaio 2016)

Hotel ransomed by hackers as guests
locked out of rooms

THE LOCAL 

- 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 **AP**
network

Medical superbugs: Two German hospitals hit
with ransomware

The Register

Infection forces patients onto phones and medicos onto *faxes*

22 Hospital Declares 'Internal State of Emergency'
MAR 16 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-Bicchieri | Mar 19 2019, 5:33pm
TECHBY 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/>

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username

pwned?

367

pwned websites

7,860,089,037

pwned accounts



164,611,595 LinkedIn accounts



152,445,165 Adobe accounts

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



NotPetya cyber-attack cost TNT at least

\$300m



"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?

SECURITY <u>NONEXPERTS'</u> TOP ONLINE SAFETY PRACTICES	VS	SECURITY <u>EXPERTS'</u> TOP ONLINE SAFETY PRACTICES
1. USE ANTIVIRUS SOFTWARE		1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS		2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY		3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW		4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION		5. USE A PASSWORD MANAGER

Sintesi poco consolante...

Stanford Congressional Cyber Boot Camp

August 2015



“Quale che sia il vostro livello di preoccupazione sulla cybersecurity, dovrete essere ancora più preoccupati”

Reid Hoffman - Co-fondatore LinkedIn

Grazie per l'attenzione

Google

"alberto bartoli
trieste"

