Parte 1:

Sensibilizzazione

Problema reale
Problema pervasivo (nessuno è immune)

Evento significativo 1 (Marzo 2016)

- **Siti resi inagibili**
- **Dati sensibili prelevati e diffusi**

- Agenzia italiana del farmaco
- Croce rossa
- Ministero della Salute
- Numerose ASL

Evento significativo 2 (Dicembre 2017)

GAZZETTA DI REGGIO

Correggio, attacco hacker di Anonymus contro gli autovelox

- ... entrato in un computer della **polizia municipale** dell'Unione Pianura Reggiana ...accesso ai software degli **autovelox**
- ha **inviato una mail** ai giornali locali e nazionali **dall'account della polizia municipale**, con link e password per scaricare i database
- ...più foto di auto, reclami di automobilisti, **mail privati** sulla spartizione dei proventi tra i comuni...

Adolescente impersona il capo della CIA (Febbraio 2018)

The Telegraph

British 15-year-old gained access to intelligence operations in Afghanistan and Iran by pretending to be head of CIA, court hears

By **Hayley Dixon**

19 JANUARY 2018 • 5:44 PM

A 15-year-old gained access to plans for intelligence operations in Afghanistan and Iran by pretending to be the head of the CIA to gain access to his computers, a court has heard.

Evento MOLTO significativo (Febbraio 2016)

Clever bank hack allowed crooks to make unlimited ATM withdrawals

Banking malware is using techniques once reserved for state-sponsored hacking gangs.

ars technica

- Malware nei PC interni alla Banca
- Cancella evidenza prelievo al Bancomat
  - **Prelievi illimitati**
- Malware **sofisticatissimo** (30 moduli)

Perché MOLTO significativo?

- Attacchi hanno **forti motivazioni**
  - Tipicamente (ma non sempre) **economiche**

- Sono **attività professionali**
- **Non** estemporanee o dilettantesche

Il nostro problema

- Moltissime situazioni con **Costo Attacco < Guadagno**
- Non ce ne rendiamo conto

Credenziali Internet Banking

Underground Hacker Markets

ANNUAL REPORT—APRIL 2016

SecureWorks

Bank Account Credentials	Price based on account balance
Bank accounts — ANZ (Australia)	$18,000 cost $4,750
Bank accounts — ANZ (Australia)	$22,000 cost $2,250
Bank accounts — ANZ (Australia)	$62,567 cost $3,800
Bank accounts with no balance listed — Turkey, Sweden, Norway, Romania, Bulgaria, Croatia,	$400 (flat fee)
Bank accounts — (U.K.)	$27,003 cost $2,000
Bank account — (U.S.)	$1,000 cost $40
Bank account — (U.S.)	$2,000 cost $80
High Quality Bank Accounts with Verified, Large Balances of $70,000 – $150,000	6% of the balance of the account

Piccola parentesi: Software per manipolare SMS

NEW ANDROID TROJAN TARGETING OVER 60 BANKS AND SOCIAL APPS

CSD BY SFYLABS

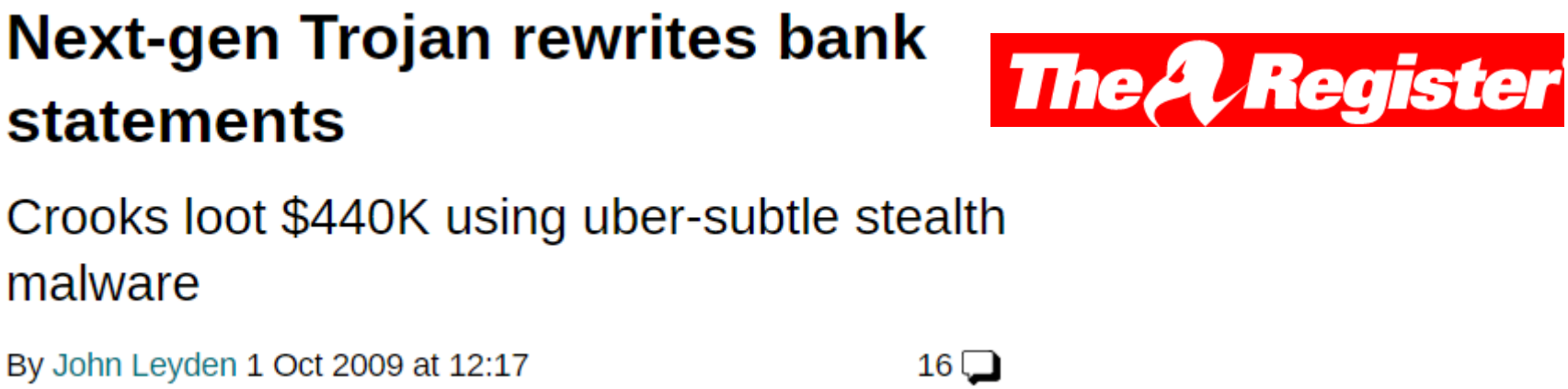
September, 2017

- Blocca chiamate provenienti da banche
- Manipola SMS di nascosto all'utente

```
a.a = new a("START_SMS_INTERCEPTION", 0, "startSmsInterception");
a.b = new a("STOP_SMS_INTERCEPTION", 1, "stopSmsInterception");
a.c = new a("SEND_SMS", 2, "sendSms");
```

- Affittabile per 500$/mese

Piccola parentesi: Modifica estratti conto a schermo



Next-gen Trojan rewrites bank statements

Crooks loot $440K using uber-subtle stealth malware

By John Leyden 1 Oct 2009 at 12:17 16

- Esegue bonifici mentre utente è collegato
- **Modifica** estratti conto **visualizzati** su schermo
- Utente **crede** di fare una cosa e in realtà ne fa una diversa...

Numeri di carta di credito

FireEye

- "Il venditore offriva **20 milioni di carte di credito**...costo medio 21$"

Aprile 2016

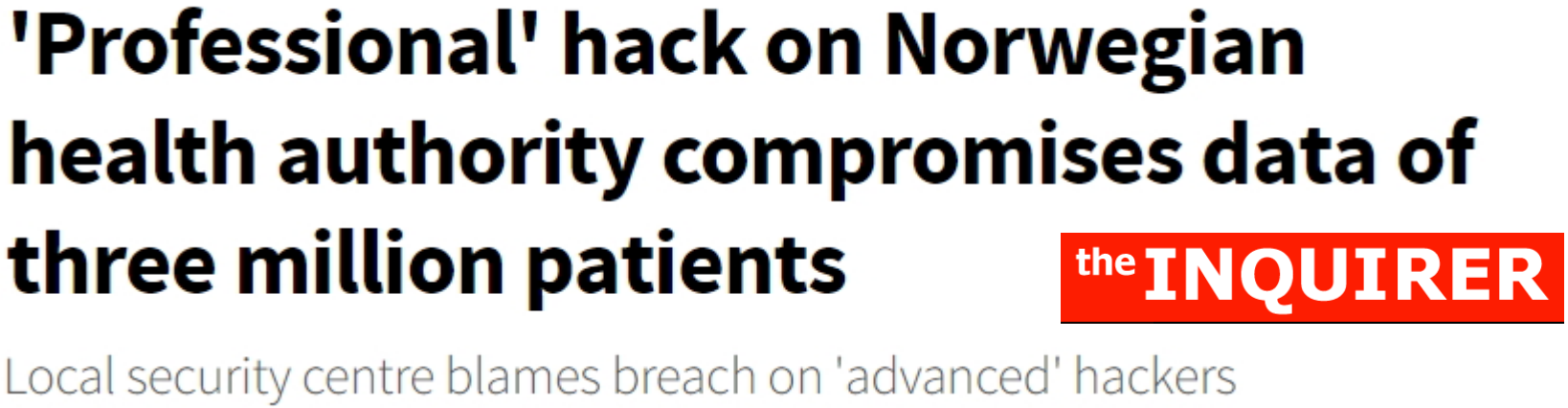
Cartelle sanitarie (Stati Uniti 2015)

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

Credit reporting (Settembre 2017)

Stand up who HASN'T been hit in the Equifax mega-hack – whoa, whoa, sit down everyone

The Register

143m in US, unknown number in UK, Canada – gulp!

By Iain Thomson in San Francisco 7 Sep 2017 at 22:11 157 SHARE ▼

- ...massive breach of security that could affect almost **half of the US population**.
- ... hackers managed to get access to some of its internal data in mid-May... They remained on the system until they were discovered on July 29.

Consulting data (Settembre 2017)

Source: Deloitte Breach Affected All Company Email, Admin Accounts

KrebsonSecurity
In-depth security news and investigation

- **Deloitte**, one of the world's "big four" accounting firms, has acknowledged a breach of its internal email systems
- ...according to a source close to the investigation, the breach dates back to **at least the fall of 2016**, and involves the compromise of all administrator accounts at the company as well as Deloitte's entire internal email system

Vigilanza Borsa (Settembre 2017)

S.E.C. Says It Was a Victim of Computer Hacking Last Year

The New York Times

- The top securities regulator in the United States said Wednesday night that its computer system had been hacked **last year**, giving the attackers private information that could have been exploited for trading.

Impronte digitali (Settembre 2015)

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

The New York Times

- The hackers got the **fingerprints** of **5.6 million federal employees**

- Biometric authentication? Una password può essere revocata...un fingerprint no
- Anche potenziale per **ricatti** enorme

PEC e Ordine Avvocati Roma (poche settimane fa...)

Un attacco hacker ha violato 500mila caselle pec in Italia

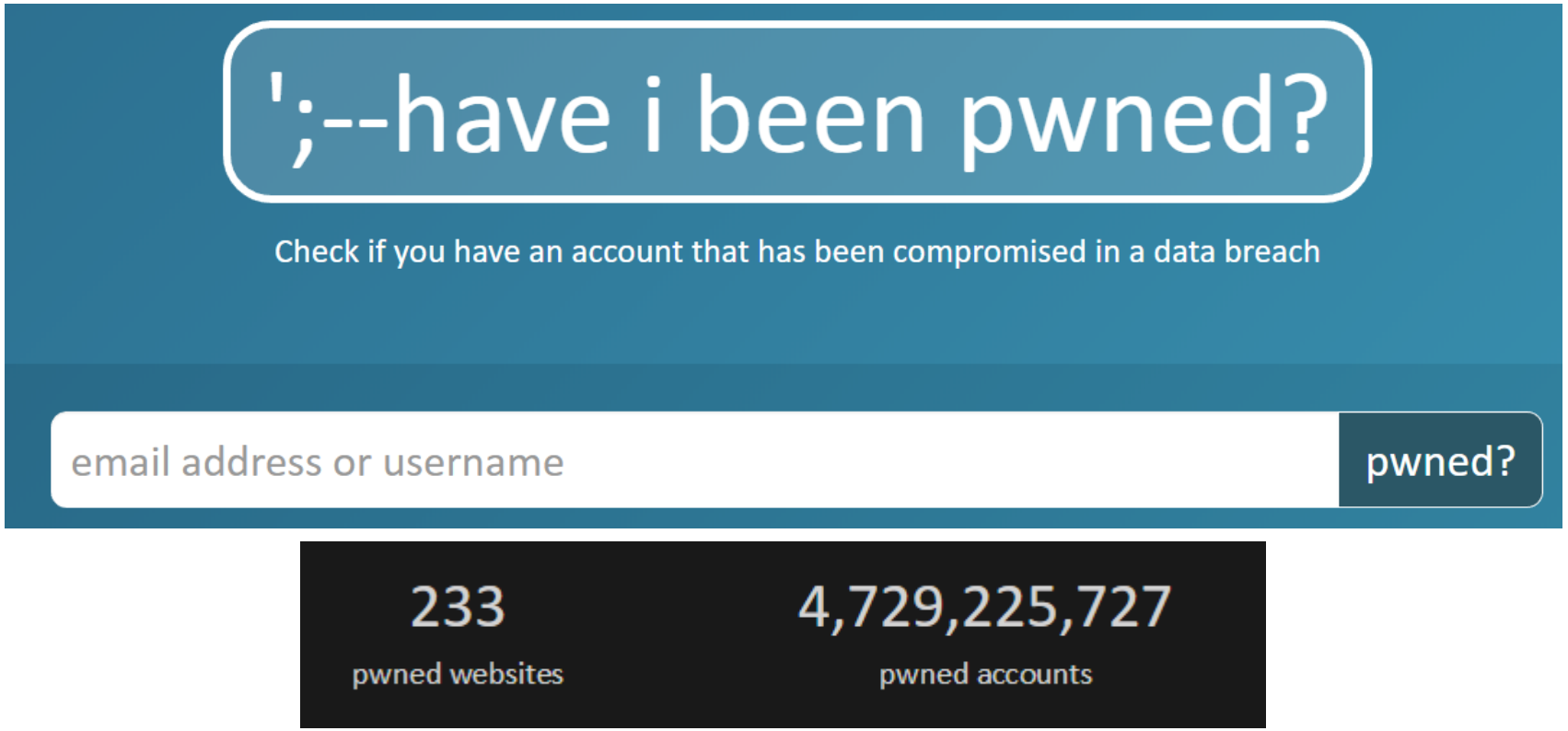
Una violazione delle caselle mail di posta elettronica certificata di tremila soggetti pubblici e privati, tra cui ministeri e uffici governativi, ha causato un blocco ai tribunali

WIRED.IT

Gli hacker di Anonymous hanno pubblicato i dati sensibili di 30.000 avvocati romani (Raggi compresa)

TGCOM24

Password


';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address or username
pwned?
233
pwned websites
4,729,225,727
pwned accounts
164,611,595 LinkedIn accounts
152,445,165 Adobe accounts

Rubare informazioni

- **Relativamente semplice**
  - Anche su larga scala
  - Anche a entità molto protette

- La vera difficoltà è nell'estrarre valore

E i "nostri dispositivi"?

- **Idem**
- Prenderne possesso è **semplicissimo**
- **Hanno valore** per gli attaccanti

Botnet

- **Bot**
  - Malware che può essere **controllato da remoto**
  - **Invisibile**

- **Botnet**
  - Insieme di bot controllati da un **bot master**
  - Ne esistono molte
  - Spesso con **centinaia di migliaia** di bot

https://reti2.blogspot.it/search?q=botnet
https://news-bartolialberto.blogspot.it/search?q=botnet

Furto informazioni bancarie

- **Torpig** 10 giorni:
  - **182.000** bot hanno contattato il bot master
  - **8,310** credenziali di **410** istituti finanziari
  - **1,660** numeri di carta di credito U.S. (49%), **Italy (12%)**, Spain (8%), e 40 altri paesi

  - It scans the infected system for credentials, as well as allowing attackers **full access** to the computer and **man-in-the-browser attacks**

Denial of Service

World's Biggest Mirai Botnet Is Being Rented Out For DDoS Attacks

Forbes

- Servizio per bombardare (**bloccare**) un sito
  - 50.000 bot 4600$
    (2 settimane, attacchi 1 ora, riposo di 10 minuti)
  - 100.000 bot 7500$

Riuso Credenziali

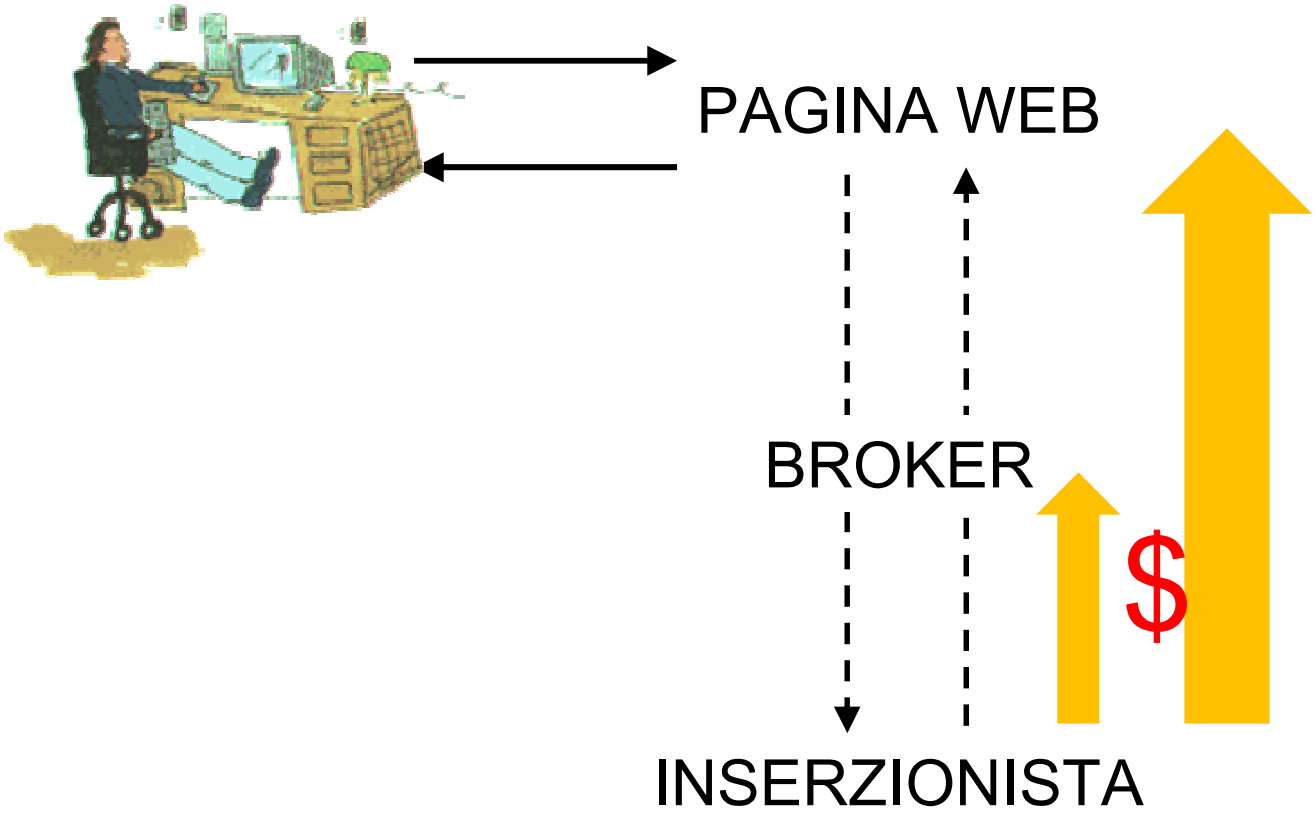
How Hackers Become You With Credential Stuffing

Forbes

1. Furto migliaia username-password da un sito
2. Bot master le ottiene e distribuisce ai bot
3. Ogni bot prova ad usarle su **molti altri siti**

   Automaticamente e lentamente...

Premessa: Pubblicità sul web

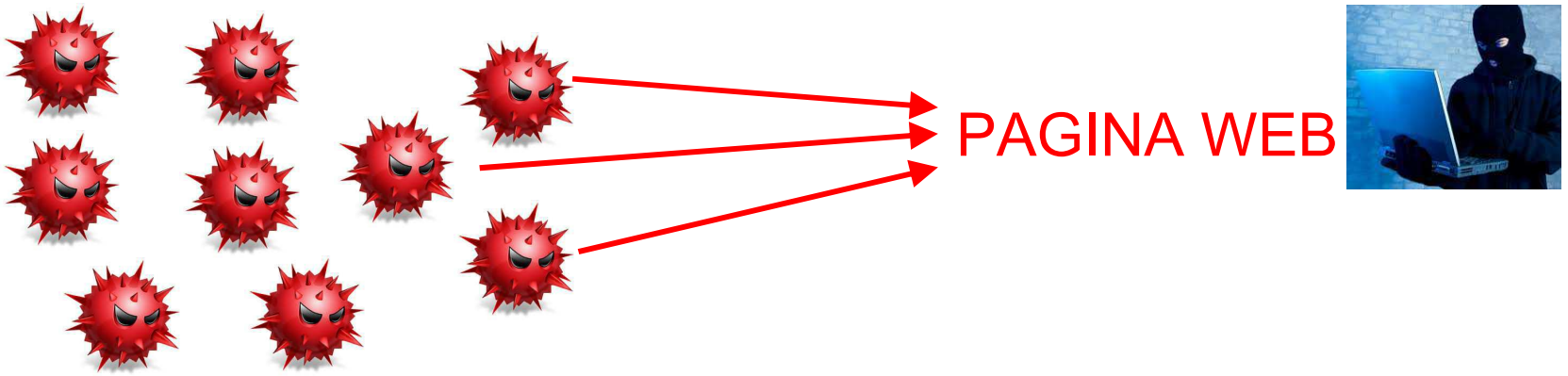


Per ogni
Visualizzazione
o ***Click***
su una pubblicità

Clickfraud (I)

prelievo e click
su di una pubblicità
(all'insaputa dell'utente)

Clickfraud (II)



- Botnet **ZeroAccess** ha generato circa **un milione di click fraudolenti al giorno**
- …equivalgono a circa **$100,000 al giorno**

https://reti2.blogspot.it/search?q=clickfraud

Si possono comprare i bot (!)

- Il Bot Master può decidere di **vendere** i bot
  - Acquirente ci installa il malware che vuole
- Costo unitario **decine di centesimi** (!)

- **1000** loads (2011 prices):
  - Asia $13
  - Europe $35
  - US $125

https://reti2.blogspot.it/2016/05/crime-report-2016.html

...e anche il malware per i bot (!)

Adwind: Malware-as-a-Service Platform that Hit more than 400,000 Users and Organizations Globally

KASPERSKY lab

- **Preleva** tutto: Tasti, Schermate, File...
- **Licenza** (ovviamente illegale): 2-300$ / anno

Febbraio 2016

Un nuovo business model: Ransomware

- **Dati e Sistemi resi inutilizzabili** fino al pagamento di un **riscatto**

- Estremamente attrattivo
  - Scompare problema **monetizzazione**
  - **Semplicissimo** da tentare su **larga scala**
    - Sufficiente inviare lo stesso email a tanti bersagli

Istituto di ricerca a Trieste (Aprile 2016)

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

Università di Calgary (Giugno 2016)

University of Calgary paid $20,000 in ransomware attack

- Crittati **600 computer** di **amministrazione** e **docenti**
- Compromessi **9000 caselle email**

- Hanno scelto di pagare **€13,900** all'attaccante

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

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

A ransomware attack means Baltimore citizens can't pay their water bills or parking tickets.

By Emily Stewart | May 21, 2019, 5:50pm EDT

recode

- **Tutte** le operazioni informatiche **bloccate** (ad eccezione di polizia e pompieri)
- Niente email, niente accessi Internet,...

Hotel (Gennaio 2016)

Hotel ransomed by hackers as guests locked out of rooms

THE LOCAL at

- Impossibilità di programmare **nuove chiavi** per le porte
- **Quarta** volta

Smart TV (Dicembre 2016)

Forget *Game of Thrones* as Android ransomware infects TVs

The Register®

Japan Reports over 300 Ransomware Attacks on Smart TVs This Year

By **Charles Whitlow** - November 2, 2016 418

Tech News Hunter

- Televisione completamente **bloccata**
- Mostrava solo istruzioni per il pagamento