Parte 1:

Sensibilizzazione

Problema reale
Problema pervasivo (nessuno è immune)

Evento significativo 1 (Marzo 2016)

L'assalto web alla sanità sferrato da un sedicenne

Minorenne friulano appartenente ad Anonymous indagato

IL PICCOLO

- 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...

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.

- 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 **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

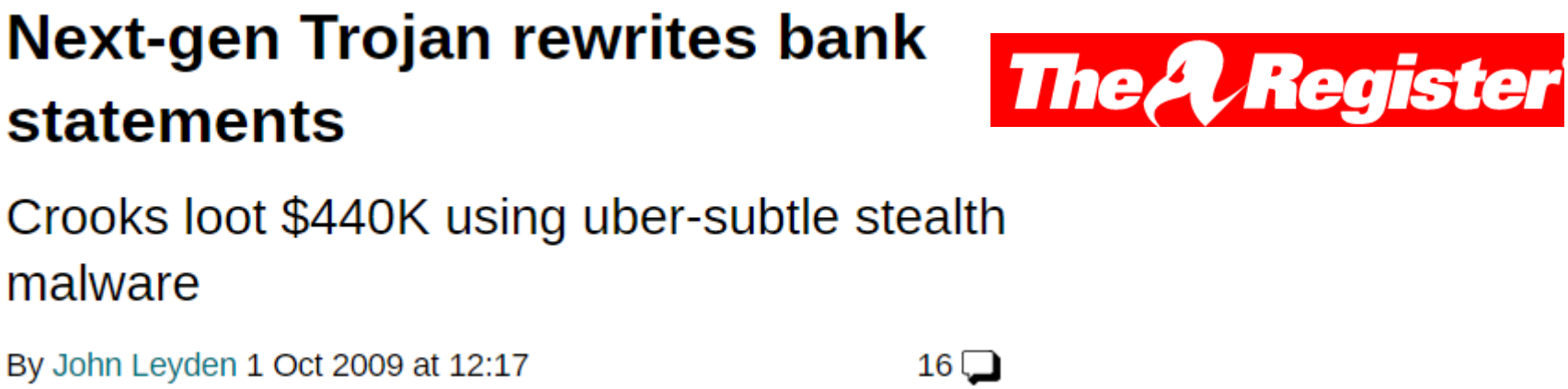
September, 2017

- 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 (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

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

- **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.

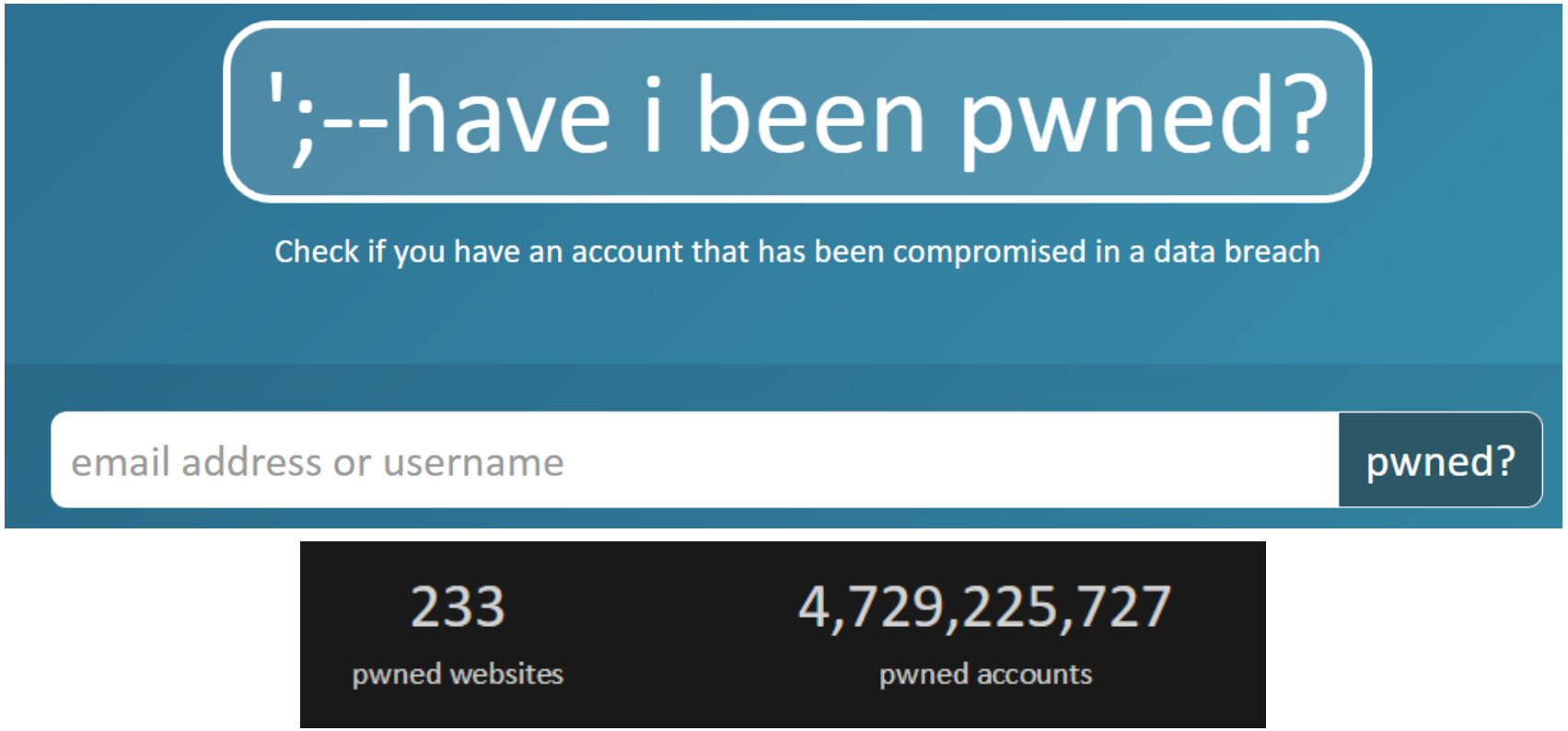
Impronte digitali (Settembre 2015)

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

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$

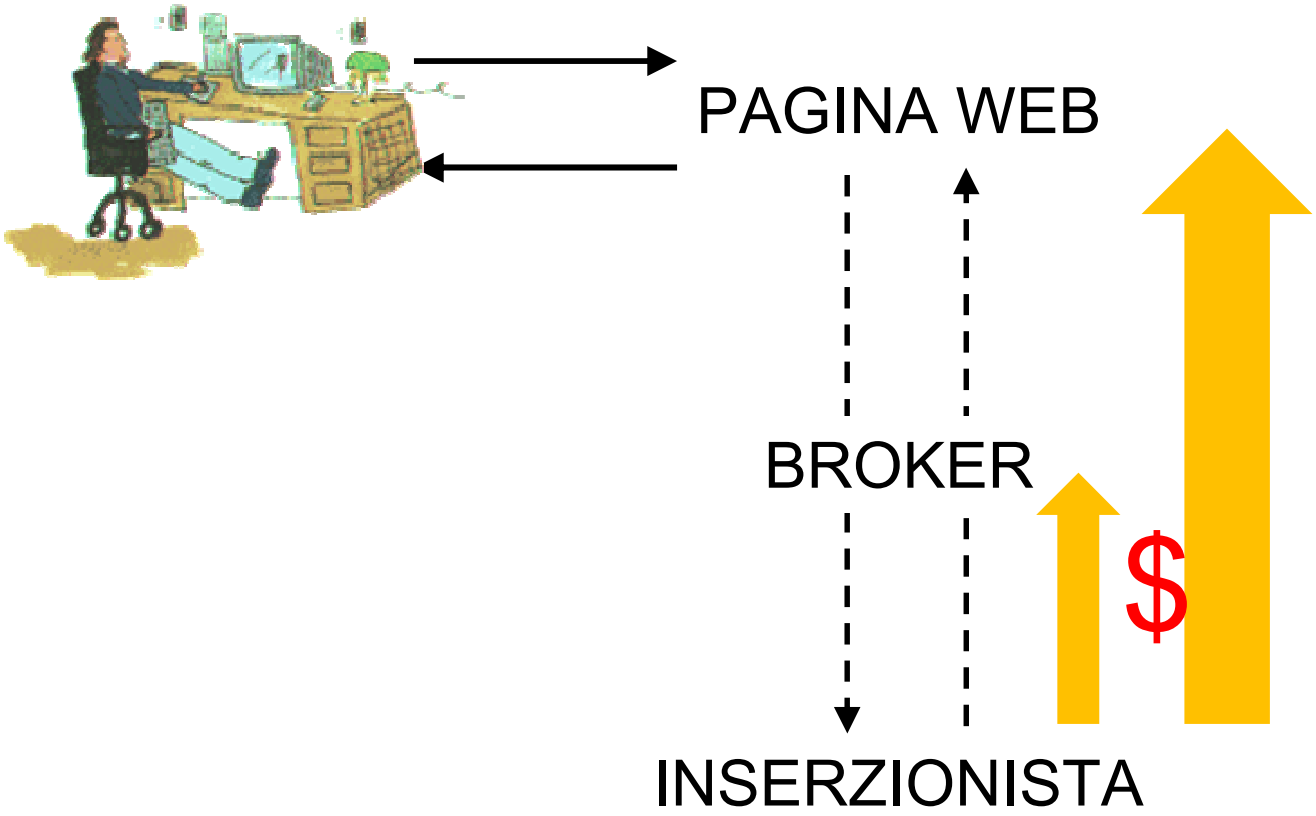
Riuso Credenziali

How Hackers Become You With Credential Stuffing

Forbes

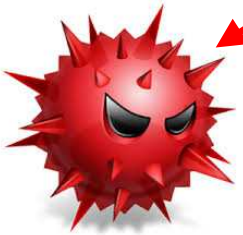
1. Furto migliaia username-password sito S1
2. Bot master le ottiene e distribuisce ai bot
3. Ogni bot prova ad usarle su **molti altri siti**
   - Automaticamente e lentamente...

Premessa: Pubblicità sul web

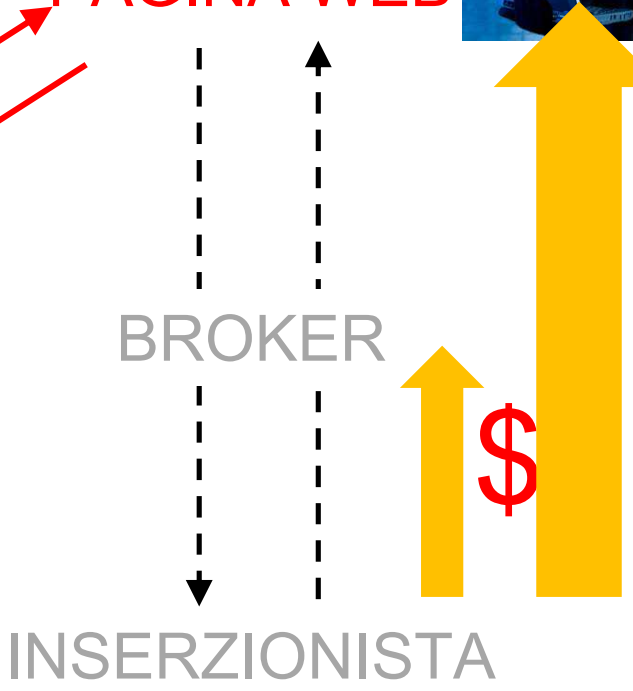


Per ogni
Visualizzazione
o ***Click***
su una pubblicità

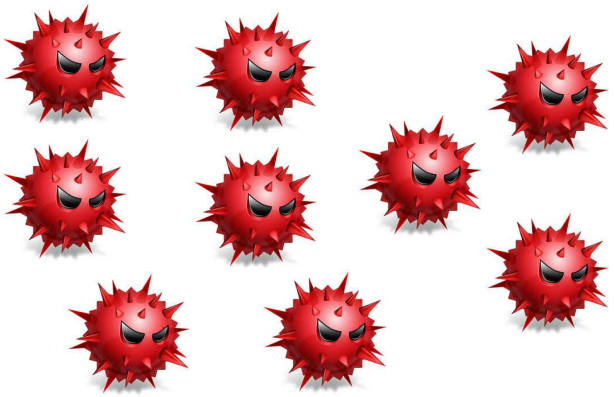
Clickfraud (I)



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



Clickfraud (II)



PAGINA WEB 

- 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

Motivazioni NON economiche (rischi per la democrazia)

Twitter says it exposed nearly 700,000 people to Russian propaganda during US election

From more than 50,000 automated accounts

By Nick Statt | @nickstatt | Jan 19, 2018, 6:26pm EST

- Enorme potenziale per **fake news**, **discredito mirato** e molto altro

Un nuovo business model: Ransomware

- **Dati 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 The Register®

Infection forces patients onto phones and medicos onto *faxes*

22 MAR 16 **Hospital Declares 'Internal State of Emergency' After Ransomware Infection** KrebsonSecurity In-depth security news and investigation

University (!) of 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

Un nuovissimo business model

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

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

Trasporti pubblici (Novembre 2016)

- Bloccate **tutte le biglietterie** nel week end del Thanksgiving

Webcam pubbliche (Gennaio 2017)

Ransomware killed 70% of Washington DC CCTV ahead of inauguration

- 123 video registratori, ognuno con 4 webcam
- 4 giorni **senza sorveglianza**
- 8 giorni prima dell'insediamento di Trump

Piccola selezione dalla ultima settimana....

Notare le date

Un "classico"

Sembra una cartella esattoriale ma è un virus: già colpiti la Camera, gli Interni e Trenitalia

Lo hanno creato su misura per le aziende italiane e viene distribuito come una mail che sembra provenire dal ministero delle Finanze. TaxOlolo ha colpito più di 80 compagnie ed enti. Tra loro Aci, Fineco, Autostrade e i comuni di Brescia e Bologna. L'attacco è partito da un server inglese pagato probabilmente in bitcoin

R.it | 22 gennaio 2018

Dati Sanitari di (letteralmente) mezza Norvegia

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

Local security centre blames breach on 'advanced' hackers

the INQUIRER

18 January 2018

Furto di cryptocurrency (simili a bitocin)

Blackwallet hacked, hackers stole $400,000 from users' accounts through DNS hijacking

January 15, 2018 By Pierluigi Paganini

Spionaggio organizzato da governo

EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World

PRESS RELEASE | JANUARY 18, 2018

Mobile Devices Compromised by Fake Secure Messaging Clients – Hundreds of Gigabytes of Data Stolen

San Francisco – The Electronic Frontier Foundation (EFF) and mobile security company Lookout have uncovered a new malware espionage campaign infecting thousands of people in more than 20 countries. Hundreds of gigabytes of data has been stolen, primarily through mobile devices compromised by fake secure messaging clients.

ELECTRONIC FRONTIER FOUNDATION

Adolescente impersona il capo della CIA

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.

PA Brasile ospita siti di phishing

NETCRAFT

Brazilian government providing warm waters for shoals of phish

Security holes in Brazilian government websites are still rife, with no fewer than eight different *gov.br* sites being compromised within the past week to host phishing attacks and hacking scripts. The situation does not seem to have improved much since two years ago, when we noticed a similar spate of phishing sites and malware hosted on *gov.br* domains, with evidence of some sites suffering repeated security compromises.

In one of this week's attacks, a *gov.br* domain was compromised to such an extent that the fraudsters were able to set up their own custom hostname, which was also configured to use HTTPS. The website, at account-verification-redirect-center.[redacted].gov.br, was then used to host a PayPal phishing site, which is still present at the time of writing.

Posted by Paul Mutton on 18th January, 2018 in Security

Spegnimento impianti industriali

REUTERS

THU JAN 18, 2018 / 4:52 PM EST

Schneider Electric says bug in its technology exploited in hack

Schneider Electric SE (SCHN.PA) said on Thursday that hackers had exploited a flaw in its technology in a watershed incident discovered last month that halted operations at an undisclosed industrial facility

The system is used in **nuclear** facilities, **oil and gas plants**, mining, **water treatment facilities** and other plants to safely shut down industrial processes when hazardous conditions are detected. It is the first reported cyber attack on this type of system.

Clickfraud

Op EvilTraffic CSE CybSec ZLAB Malware Analysis Report – Exclusive, tens of thousands of compromised sites involved in a new massive malvertising campaign

January 22, 2018 By Pierluigi Paganini