Cloud Security, from an Hacker's Perspective

(从专业视角看云安全)

Raoul "Nobody" Chiesa

Founder, Partner, Security Brokers

Principal, Cyberdefcon Ltd.

Founder, Owner, @ Mediaservice.net

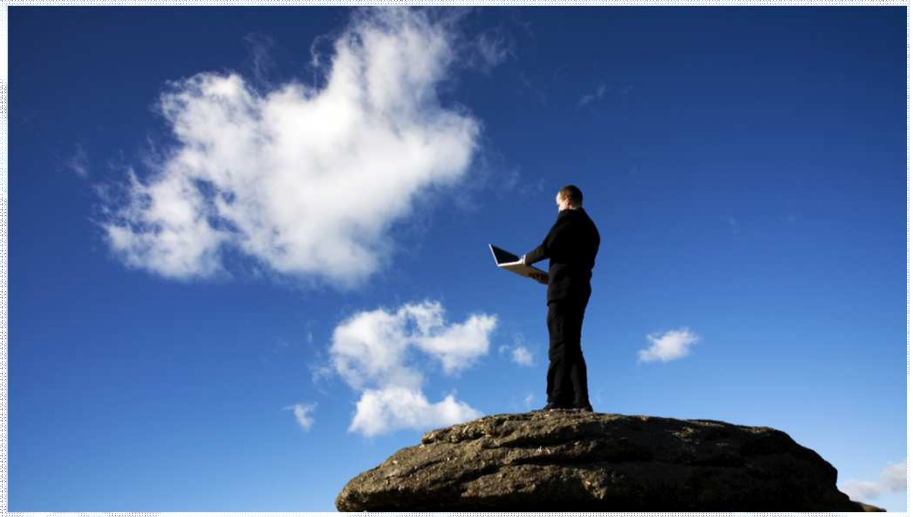
SecurityBrokers

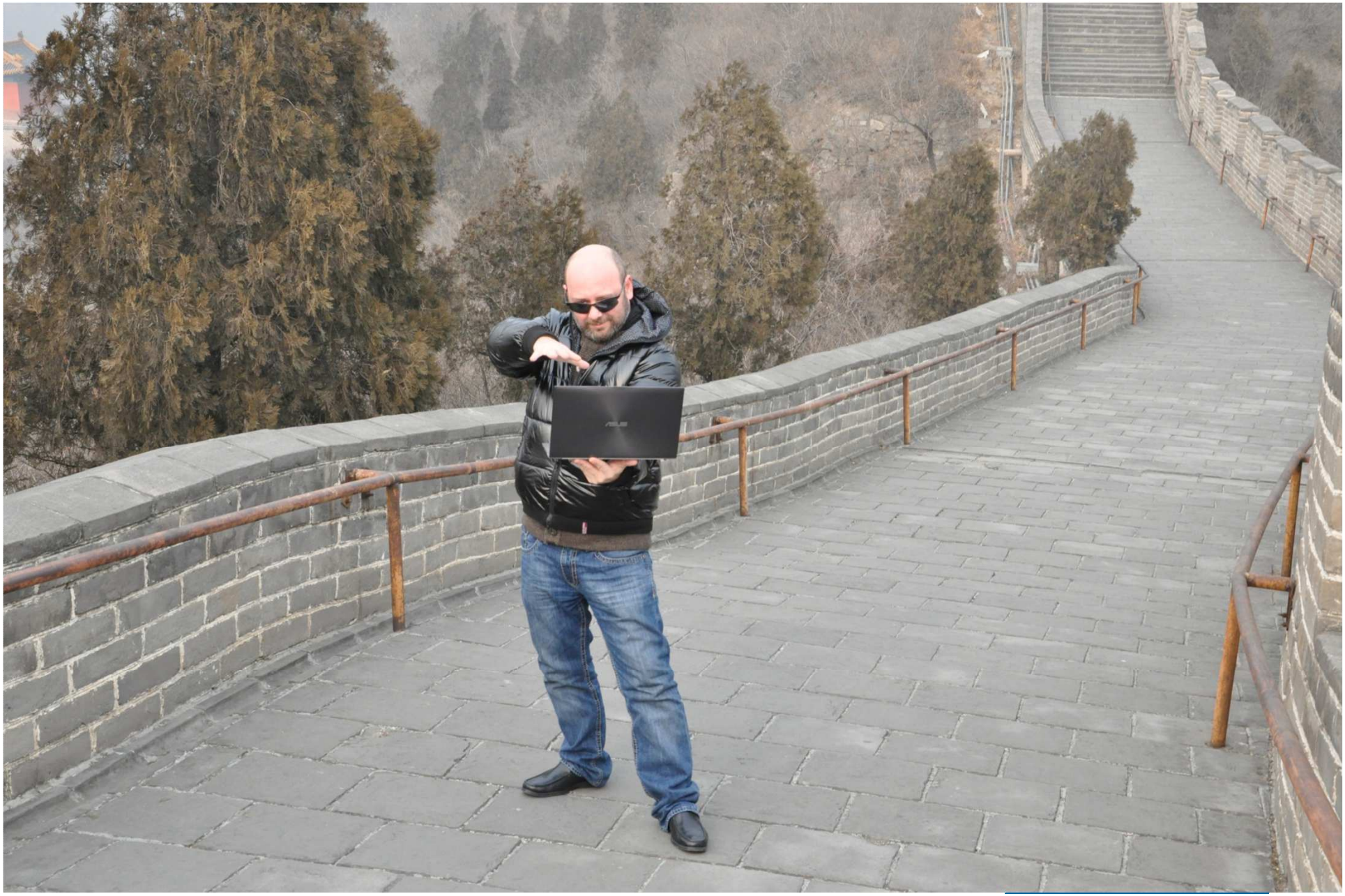
Global Cybersecurity Defense Services

Perugia, July 23, 2012

Agenda

- Introductions
- What's this "cloud"?
- History plays back…
- Known issues
- First "problems"
- Unknown issues?
- Conclusions
- Contacts, Q&A





Intro – The Speaker

Raoul Chiesa

- Founder, Partner, **Security Brokers**
- Principal, **CyberDefcon** UK
- Senior Advisor & Strategic Alliances on Cybercrime @ **UNICRI (United Nations Interregional Crime & Justice Research Institute)**
- **PSG Member**, **ENISA (Permanent Stakeholders Group, European Network & Information Security Agency)**
- Founder, Member of the Steering Committee and Technical Board, **CLUSIT, Italian Information Security Association)**
- Steering Committee, **AIP/OPSI**, Privacy & Security Observtory
- Board of Directors, **ISECOM**
- Board of Directors, **OWASP** Italian Chapter
- Founder, Owner, **@ Mediaservice.net**

SecurityBrokers
Global Cybersecurity Defense Services

CyberDefcon

unicri
advancing security, serving justice, building peace

enisa
European Network and Information Security Agency

opsi aip

Clusit
Associazione Italiana per la Sicurezza Informatica

APWG Committed to Wiping Out Internet Scams and Fraud

OWASP
The Open Web Application Security Project

ICANN

TEAM CYMRU

E.A.S.T

mediaservice.net
CORPORATE SECURITY & IMAGE

ISECOM

Intro – Security Brokers

The Security Brokers

- Security Brokers (SB) was established in order **to fill a gap**: the actual ICT Security just **doesn't work** ☹
- SB è un **marketplace globale dell'Information Security avanzata e non convenzionale**,
- Security Brokers (SB) was established after **three year-long phase** of «*human start-up*» and bootstrapping.
- SB's **concept** can be summarized as an agile **IT and InfoSec marketplace provider with 360° vision** and an **unconventional approach**, which uses a **business model similiar to traditional brokerages**: we locate the best «product» (expert, service, product), typically located in «niche» sectors to best serve our clients.
- The model itself is based chiefly upon **personal** relationships and networks cultivated over 20 years and tried & tested in the field over the past **10 years**.
- This said, SB has as «input» its own key **Suppliers** (Associates) and its **High-Level Independent Consulting Services** as «output».
- The **full listing** of SB's Associates **is not yet public** (ETA: SEPT 2012), though it encompass many respected Ethical Hackers, IT Security Researchers and top-class experts.
- **Some** names:
  - **Andrea Zapparoli Manzoni**, **Elena Bassoli**, **Gianna Detoni**, **Fabio Massa**, **Selene Giupponi**… and many, many more!

Intro – Security Brokers: what, how

SecurityBrokers
Global Cybersecurity Defense Services

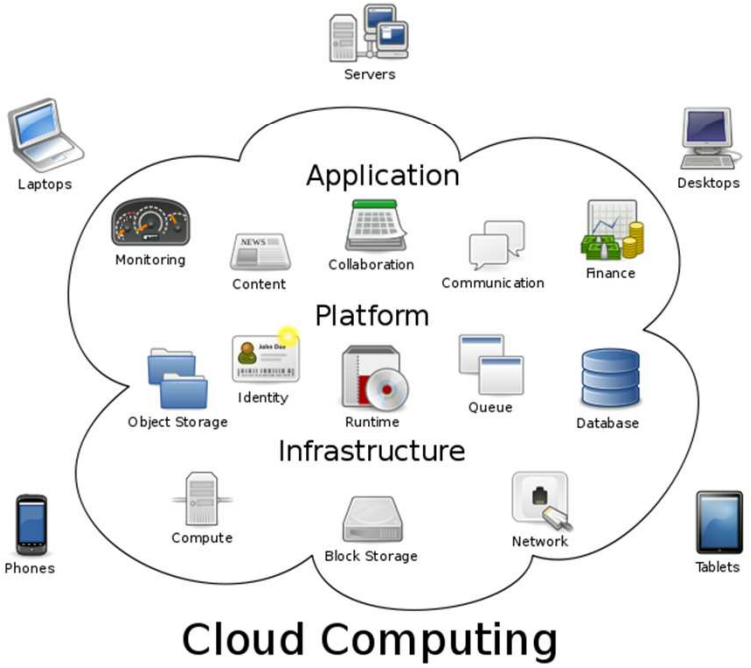
- We focus on critical and interesting topics. Thanks to the know-how and specialization our **30+ global experts** have gathered over **20 years of demonstrable field experience** in the **Information Security** and **Cyber Intelligence** communities (and a few others!), we can claim **over 600 combined references per year.**
- Our **main service areas** can be summarized here:
  - **Proactive Security**
    - With a focus on mobile networks and devices, modern telco networks, SCADA/NCI security, **Cloud**, IA in the Transport, Space & Air sectors, Social Networks, proactive identification and mitigation of security issues.
  - **Post-Incident & Incident Response**
    - Attacker profiling (MO, Behaviour, Motivations), Digital Forensics (Host, Network, Mobile, GPS, **Cloud**, etc..), Trainings
  - **Cyber Security Strategic Consulting** (Technical, Legal, Compliance, PR, Strategy)
    - On-demand «Ninja Teams»
    - Security Incident PR Handling & Management
  - **Psychological, Behavioural and Social aspects of hacking and infosec**
  - **Cybercrime**
    - Botnet takeovers and takedowns, Cybercriminal profiling and bounties, Cyber Intelligence reports, facilitator towards external CERTs and LEAs/LEOs,[…]
  - **Information Warfare, Information Superiority & Cyber War** (intended exclusively for MoD clients)
    - 0-day vulnerabilites and “digital munitions”; OSINT Trainings & Services; CNA/CND/CNE.

What's this "cloud"?

- The very official, "serious" term: ***Cloud Computing***

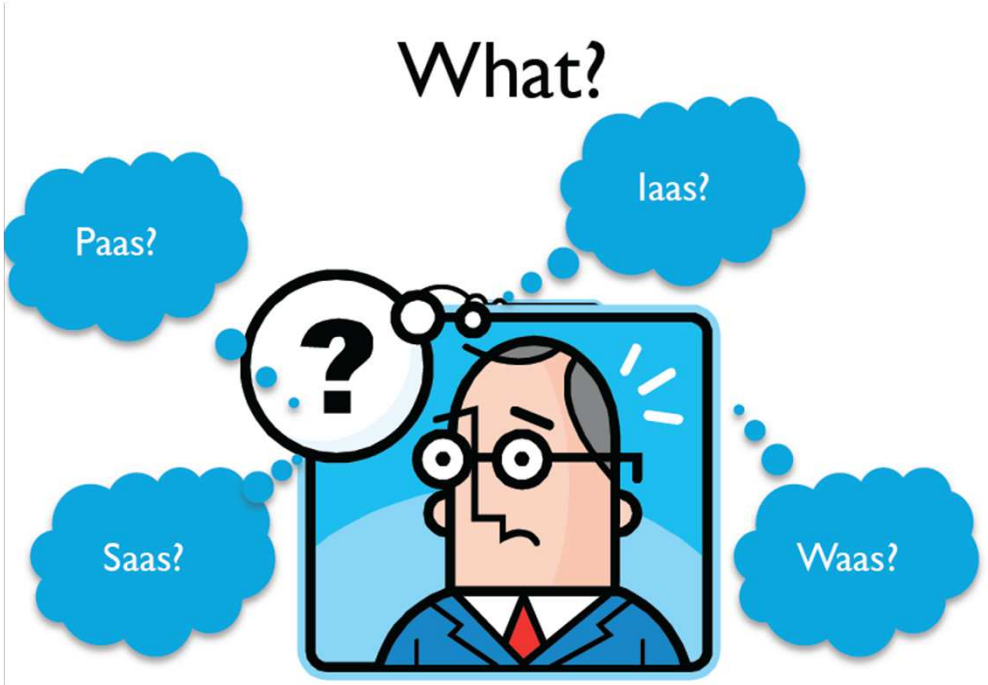
- **Wikipedia:**
  - ***Cloud computing*** *is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).*

- **Henry J. Sienkiewicz – DISA (Defense Information Systems Agency)**
  - *A style of computing where* ***massively scalable*** *(and elastic)* ***IT-related capabilities*** *are provided "as a service" to* ***external customers*** *using* ***Internet technologies****.*



“Cloud” /2

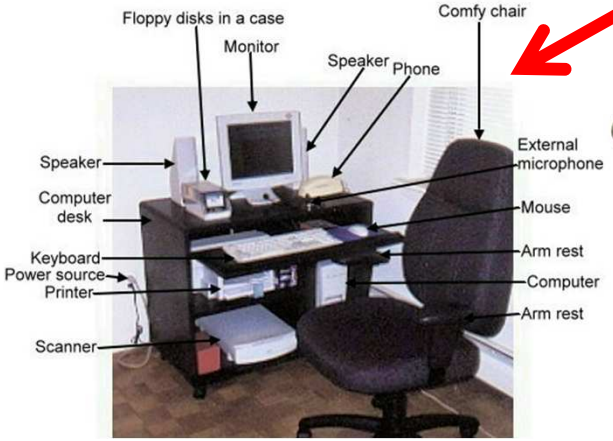
- **IaaS**: Infrastructure As-a-Service
  - **Processing, networking, storage, virtualization**
- **PaaS**: Platform-As-a-Service
  - **Applications development, platforms to develop and test and study SaaS applications. Intended for sw developers communities.**
- **SaaS**: Software-As-a-Service
  - **Pay-per-Use your application through the Web**
- **XaaS**: Whatever-As-a-Service:
  - Data-As-a-Service (on-line storage or DaaS)
  - Cracking-As-a-Service?
  - DDoS-aaS?
  - Crime-As-a-Service (already existing!)



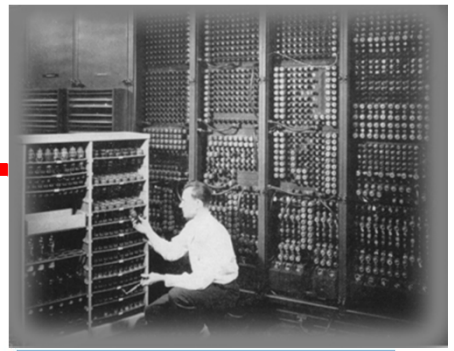
History plays back…

Traditional Data Center

VIRTUAL
Server
Consolidation



CLOUD
COMPUTING



Author: Raoul Chiesa, Security Brokers

Cloud's fans and opponents (PROs/CONs)

☹

Cloud sucks because...

- ✓ It doesn't has security
- ✓ I want to manage my stuff on my own
- ✓ I don't go for cloud 'cause I don't have any stuff on cloud and I never will
- ✓ I don't cloud 'cause I already have my cloud: it's my datacenter, close to my town
- ✓ If it's gonna rain, I'll lose my data
- ✓ On cloud they would steal my data and the USA would read my emails
- ✓ They already screwed up MegaUpload!

☺

Cloud is cool because...

- ✓ IDC/Gartner/whoever said it's the future
- ✓ It's SO trendy
- ✓ I save money on electricity
- ✓ I got a lot of CPU power
- ✓ The son of a friend of mine runs a Facebook page with +1000 friends and told me that cloud is a "must-have"
- ✓ Because "everything is on the Internet"

Known issues/1

- **Recording**
  - **Log**ging?
  - Which **type** of logs?
  - And what about the **data-retention** laws?
  - Where's **my data**, in **which country**?? -> EU vs rest-of-the-world **Privacy Laws**

- **Access**
  - **Who** can access my data?
  - **What if** I CAN'T access my **own** data??

- **Backups and safeties**
  - **What** is backuped?
  - **When**?
  - **How long** (data retention, again)

- **Compliance**
  - Which kind of **Security Audits** are allowed to be run? Despite the «compliances»
  - What about **Penetration Tests**? Who will **legally authorise** the pentesters?

Known issues/2

- **Lawful Interception**
  - TLC Service providers **must be compliance with LIS/LIG laws**
  - In this case **laws are pretty similar,** both into **UE** and **extra-EU** countries
- **Legal**
  - **Where** is the **datacenter physically** located?
  - **Local** laws (i.e. Privacy)
  - **Cloud Provider** VS **data management** (privacy, once again)
  - Transferring this data **abroad**….?
- **DLP (Data Loss Prevention)**
  - **How** can I **monitor what is happening** to my **boxes/applications/services?**
  - …what about **Digital Forensics ?!? Insurance's aspect** (break-ins)**??**
    - **We'll check this out later thanks to Eng. Selene Giupponi**
- **Hidden costs**
  - Is there anything **billed** in an "**hidden" way**?
  - **CPU**?
  - Data **Traffic**?
  - Disk **space** & Backups quotas?

First “problems”

- September 8°, **2001**
- **Google Docs** stopped working….
- **30 minutes** “black-out”
- Those data people was working on, just **got lost**
- And, people wasn’t able to work btw!!

Be secure? A good start from the folks at NIST, ENISA & CSA

- **NIST** Releases **Secure Cloud Computing Guidelines** (September 15, 2011)
  - Read the articles on **Infosec Island!**
  - NIST **Cloud Computing Standards Roadmap**

  (NIST SP-500-291): http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909024
  - The full document: http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

- **ENISA**, Cloud Computing - Benefits, risks and recommendations for information security, November 2009
  - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
  - ENISA, Cloud Computing - SME Survey, November 2009
  - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-sme-survey
  - ENISA, Cloud Computing Information Assurance Framework, November 2009
  - http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assuranceframework

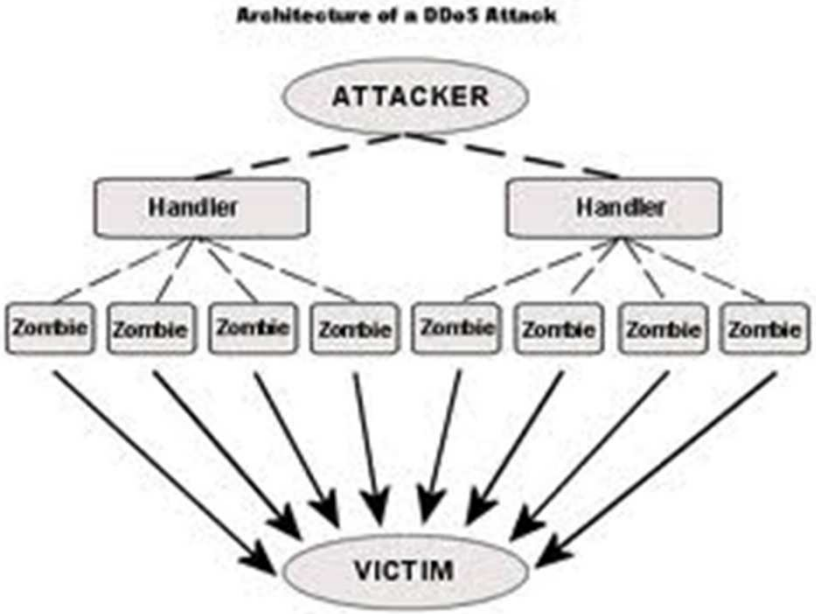
enisa
European Network and Information Security Agency

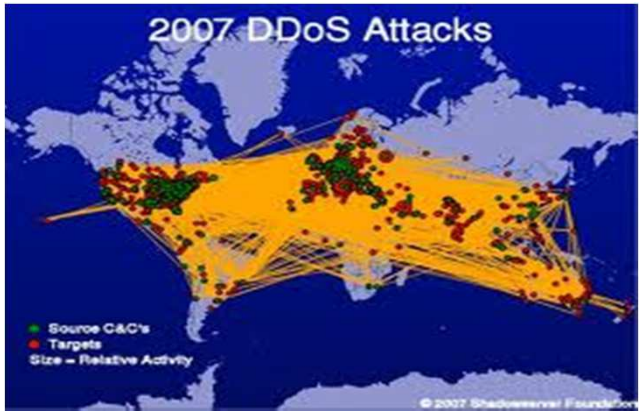
- **CSA – Cloud Security Alliance - https://cloudsecurityalliance.org/**

CSA cloud security alliance℠

Unknown issues?/1

- **DDoS attacks**
  - Running on cloud can be **extremely helpful** when mitigating DDoS attacks
  - These attacks **would not be** “as much easy” to mitigate within your standard infrastructure
  - On the other hand, from an attacker’s point of view, the cloud infrastructure itself **would represent a very powerful “shotgun”**





Unknown issues?/2

- **Password cracking**
  - Attackers **already have abused** Cloud's ISPs resources in order to run password cracking software:
    - https://www.infosecisland.com/blogview/11018-Cracking-WPA-Protected-WiFi-in-Six-Minutes.html
  - "Roth was able to ***crack* 400.000 *passwords per* second**"
    - http://www.darkreading.com/authentication/167901072/security/client-security/229301362/researcher-overcomes-legal-setback-over-cloud-cracking-suite.html
  - "Apparent mis-translation by a German newspaper of English-speaking reports on researcher's Amazon EC2-based password-cracking tool **led to raid, frozen bank account**"
  - 11 Jan **2011** – Researcher *cracks* Wi-Fi *passwords* with Amazon *cloud* **...** computers available for **28 cents *per* minute**, the **cost of the *crack* came to just $1.68**.
    - http://www.theregister.co.uk/2011/01/11/amazon_cloud_wifi_cracking/

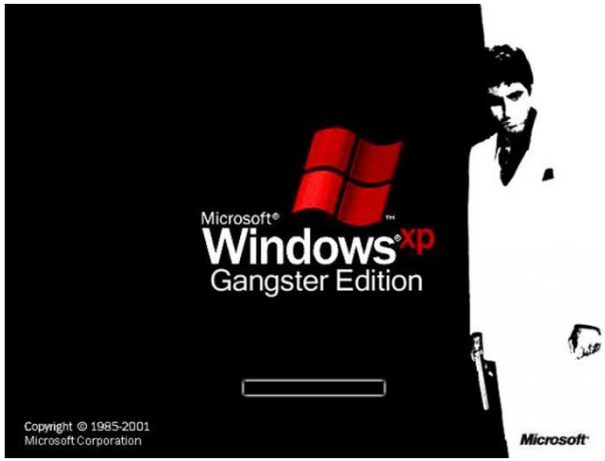
Unknown issues?/3

https://www.wpacracker.com/

Unknown issues?/4

- **Hosting mass-template configurations**
  - Just like those mass-hacks at ISPs: **1 hole**, **1.000.000 data breaches** in **one shot**!

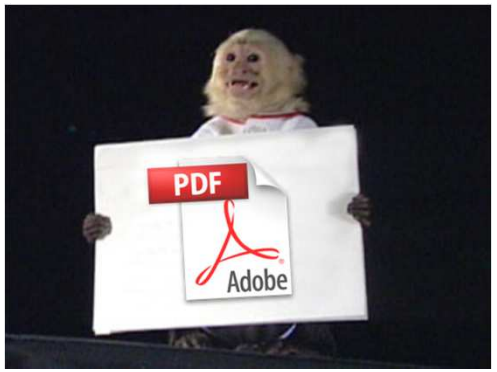
- **Cheap Cloud Providers**
  - [choose_your_cheap_service-provider]-like: **no grant of security** if you pay them 5 EUR/month ☹



- **«Not CSA» (OSSTMM, OWASP, ISO/IEC, NIST, …..) compliance Providers**
  - Compliance **means** something!

- **BGP attacks**
  - Remember **China VS USA?**

- **Mass-attacks**
  - i.e. **recent Linkedin break-in** followed by **mass spear-phishing attacks (Yahoo! and others will follow!)**

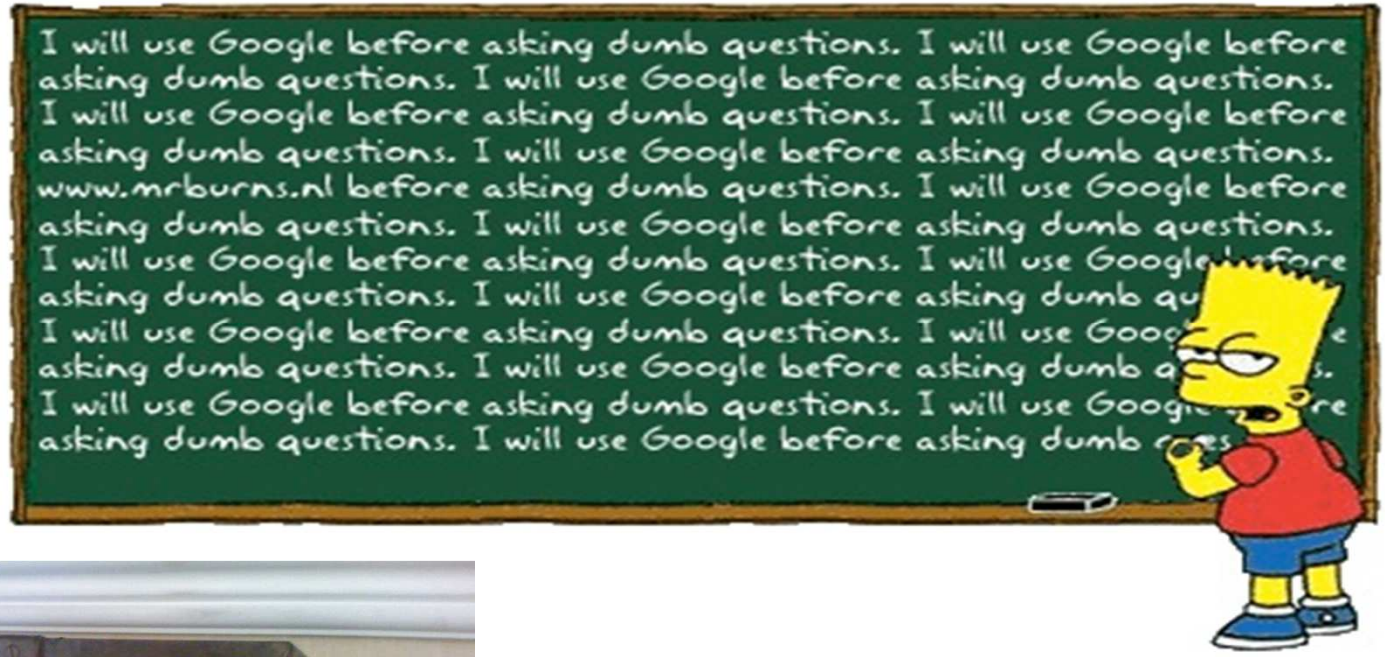


Conclusions

- Cloud is a **tool now available** to us.
- **It's not** the "final panacea" aka "the very one solution to everything".
- It can **help us**, tough.
- **Ahead** to "going cloud", please run:
  - **Cost** analysis
  - **IT infrastructure** analysis
  - Network and OS **Security Testing** (don't bring your holes into the cloud!)
  - **Web Applications** penetration testing!!!
  - **Legal** advisoring
- **When gone** "into the cloud", please run:
  - Web Applications penetration testing (at least!)
  - Social Engineering tests towards the physical access?

Questions?

Thanks for your attention! ☺



Raoul «nobody» Chiesa

raoul@cyberdefcon.com

GPG Key:
http://raoul.EU.org/RaoulChiesa.asc