Quelli che…

…la sicurezza non è mai abbastanza!

Luca Bechelli

Information & Cyber Security Advisor P4I – Partner4Innovation

DIGITAL 360 | Group

Direttivo e Comitato Tecnico – Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

QUELLI CHE...

...TANTO IO HO SOLO QUALCHE SOFTWARE CHE MI SONO FATTO FARE DA UNA DITTA DI QUI CHE CONOSCO. SONO BRAVI!!

Ci sono cose che non cambiano mai…

OWASP Top ten vulnerabilities 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Tecniche di attacco (rispetto al II sem.2017)

+37%

Know Vulnerabilities

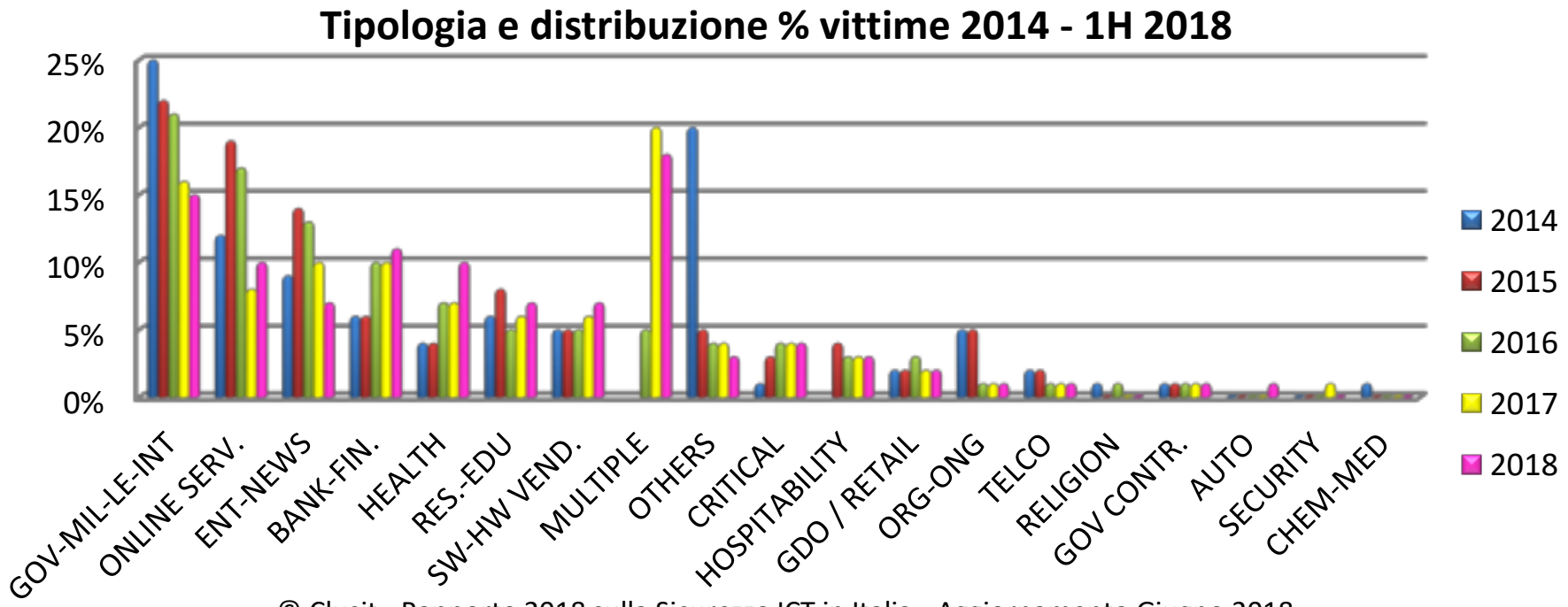
SQL Injection

QUELLI CHE...

CHI!!

MICA SONO UNA BANCA, IO!!

Le vittime



QUELLI CHE...

CHE POTRANNO MAI FARMI?

IO FACCIO BULLONI!

Attacco hacker alla Maschio Gaspardo a casa per tre giorni 650 dipendenti

Padova, tre stabilimenti chiusi fino a lunedì: chiesta la cassa integrazione

IL CASO

Attacco hacker alla Maschio Gaspardo
a casa per tre giorni 650 dipendenti

Padova, tre stabilimenti chiusi fino a lunedì: chiesta la cassa integrazione

PADOVA La Maschio Gaspardo è finita sotto attacco hacker. Da martedì i sistemi operativi sono bloccati, tre stabilimenti sono stati chiusi e 650 tecnici e operai rimandati a casa. Caso più unico che raro in Italia, dove si è concentrato il 10% dei ricatti dei cyber-pirati ma le vittime non denunciano, è stata la stessa azienda a renderlo noto. La prima e unica in Veneto, di sicuro. «Sono stati disattivati precauzionalmente alcuni sistemi informativi, sospendendo la normale attività produttiva per valutare la situazione e programmare il pronto ripristino di tutte le funzionalità – spiegano dall'impresa - Rimangono operativi tutti i servizi commerciali, in particolare quelli di assistenza e ricambi. Ogni sforzo è mirato a superare questa situazione quanto prima». Player mondiale nella produzione di macchine per la lavorazione del terreno, semina, trattamento delle colture e manutenzione del verde, Maschio Gaspardo ha annunciato che chiederà la cassa integrazione ordinaria fino a domani per i 650 addetti degli stabilimenti di Campodarsego, Cadoneghe e Morsano al Tagliamento in modo da non costringere il personale ad attingere al monte ferie.

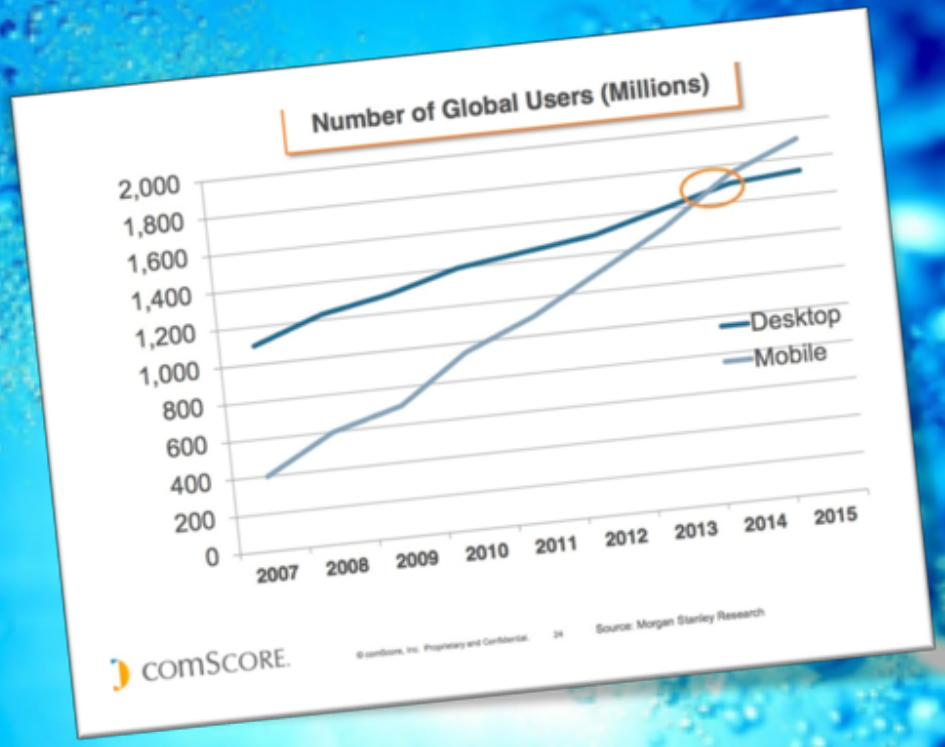
Dagli ultimi dati…

- un danno economico complessivo di circa 500 miliardi di dollari
- danni quintuplicati in 6 anni
- 730 attacchi gravi con danno economico, reputazionale e perdita di dati sensibili. **+31,77%** rispetto al **semestre** precedente
- La finalità cybercrime cresce del 35%, per raggiungere l'80% del totale degli attacchi

QUELLI CHE...

...E POI SE METTO IN SICUREZZA I PC SONO A POSTO, VERO?

Mobilis in mobile



212 BILLION

Total number of available sensor enabled objects by 2020

212B is **28x** the total population of the world

30 BILLION

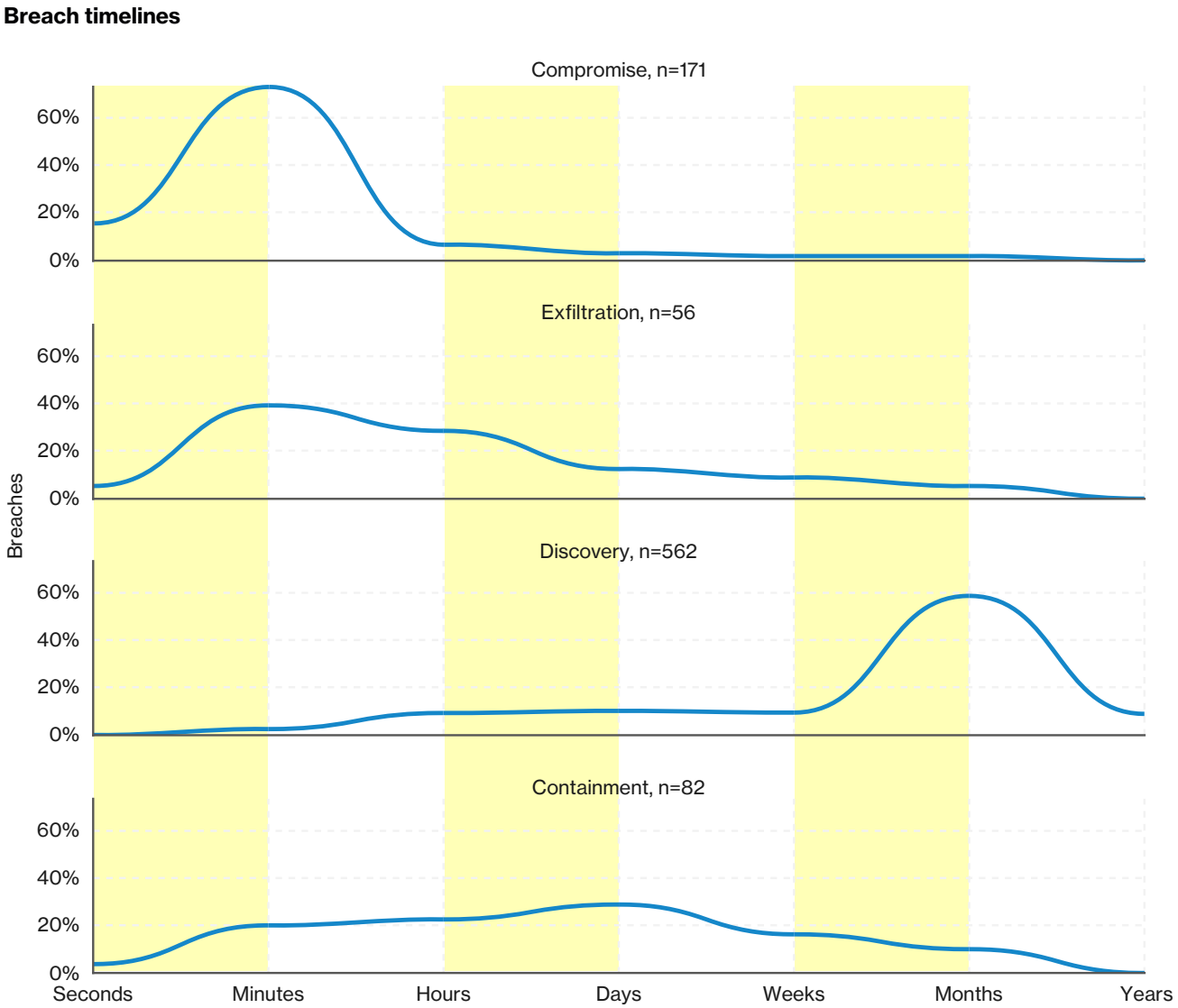
Sensor enabled objects **connected to networks** by 2020


Mirai botnet, a DDoS nightmare
turning Internet of Things
into Botnet of things

QUELLI CHE...

...SE CAPITERA', IO C'HO UN SISTEMISTA CHE E' BRAVO A RISOLVERE...

Una questione di velocità



verizon

QUELLI CHE...

...IO HO GIA' DATO!

Tecniche di attacco (rispetto al II sem.2017)

+140% 0-day

+48% APT

…e malware, malware, MALWARE!

Vabbè, ma ho l'antivirus

Il cloud Azure, a livello mondiale, incontra lo stesso malware

sola volta in più del 97% dei casi

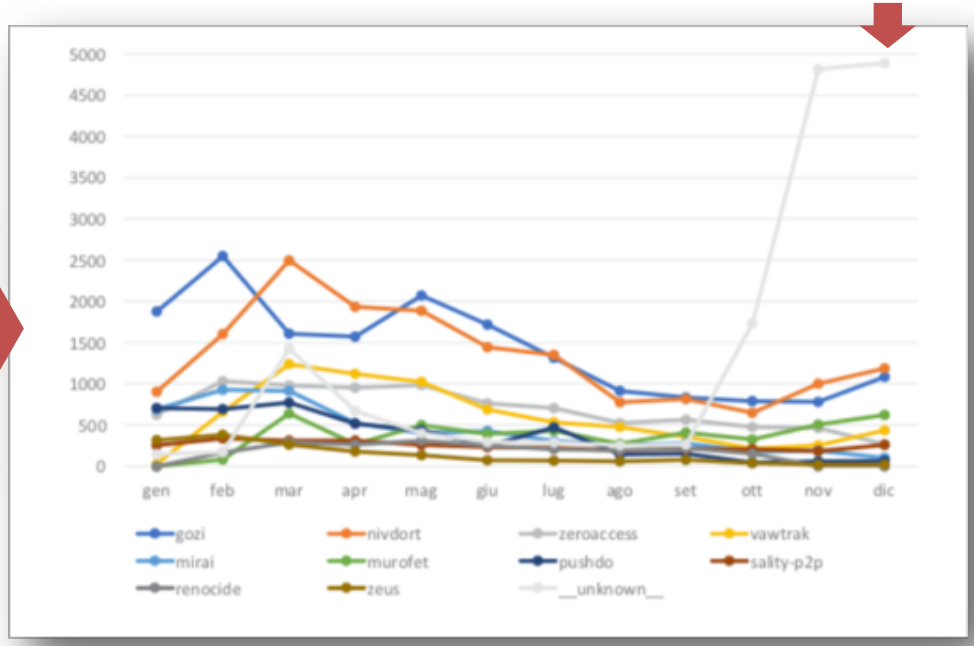
Niente di nuovo sotto il sole?

Rapporto Clusit

Principali famiglie di malware e botnet

Analizzando i trend temporali delle varie tipologie di malware si nota una decisa flessione di gozi e nivdort mentre per gli altri il trend è pressoché costante.

È importante però evidenziare come, a partire da settembre, siano cresciuti in maniera significativa gli eventi (quasi 5000 nei mesi di novembre e dicembre) relativi a minacce non ancora conosciute e catalogate. Tale tipologia di attacchi è più pericolosa della media perché queste ultime non sono rilevabili da sistemi tradizionali poiché non ancora riconosciute dai principali sistemi di protezione (ad esempio gli antivirus). Per questo motivo sul mercato stanno nascendo diverse soluzioni che utilizzando tecniche di analisi comportamentale e machine-learning in grado di rilevare queste tipologie di infezioni. Purtroppo la diffusione



Quanto siamo capaci di evolvere?

Rapporto Clusit

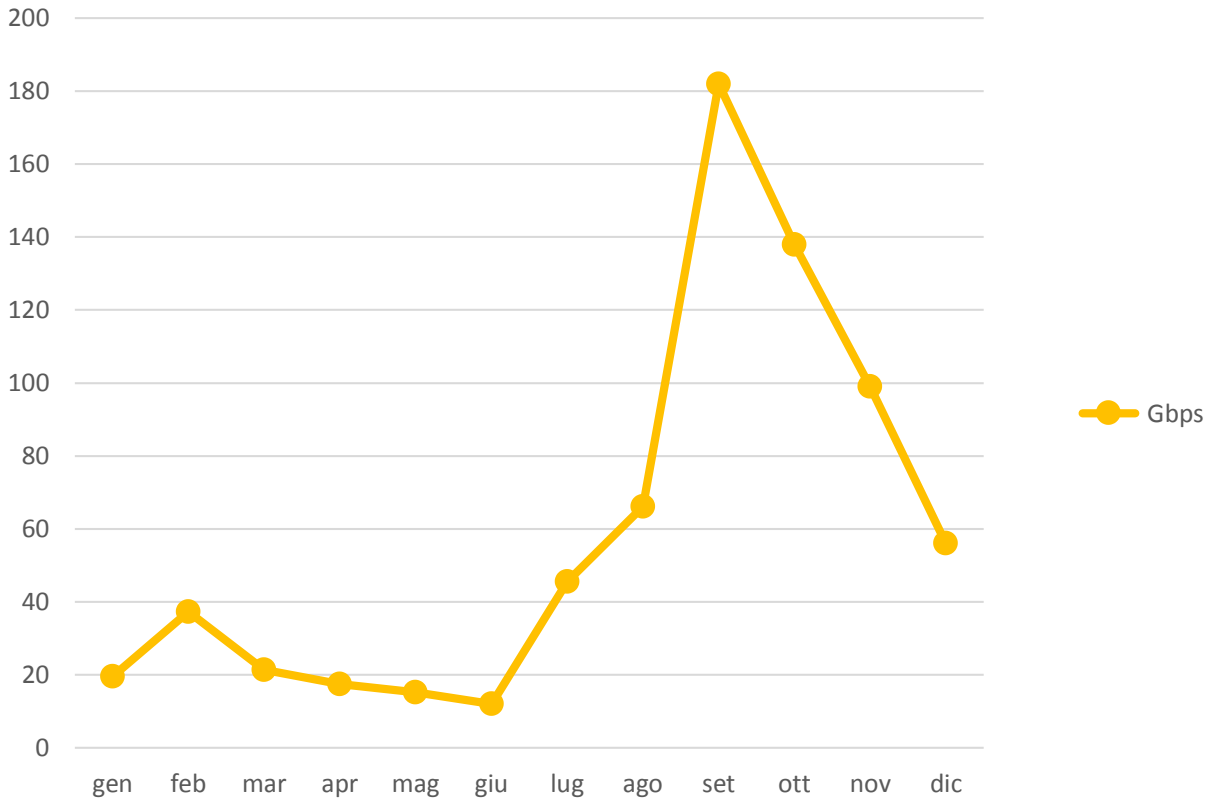


Figura 7 - *Banda totale mensile impegnata negli attacchi DDoS*
(Dati Fastweb relativi all'anno 2017)

QUELLI CHE...

...VABBE', MA GLI ALTRI CHE

FANNO?

…anche in Italia

Campione: 1107 organizzazioni italiane

OSSERVATORI.NET digital innovation

Principali motivi di spesa

Dati ottenuti tramite un'elaborazione statistica di un campione di 947 micro, piccole e medie imprese (addetti compresi tra 2 e 249)

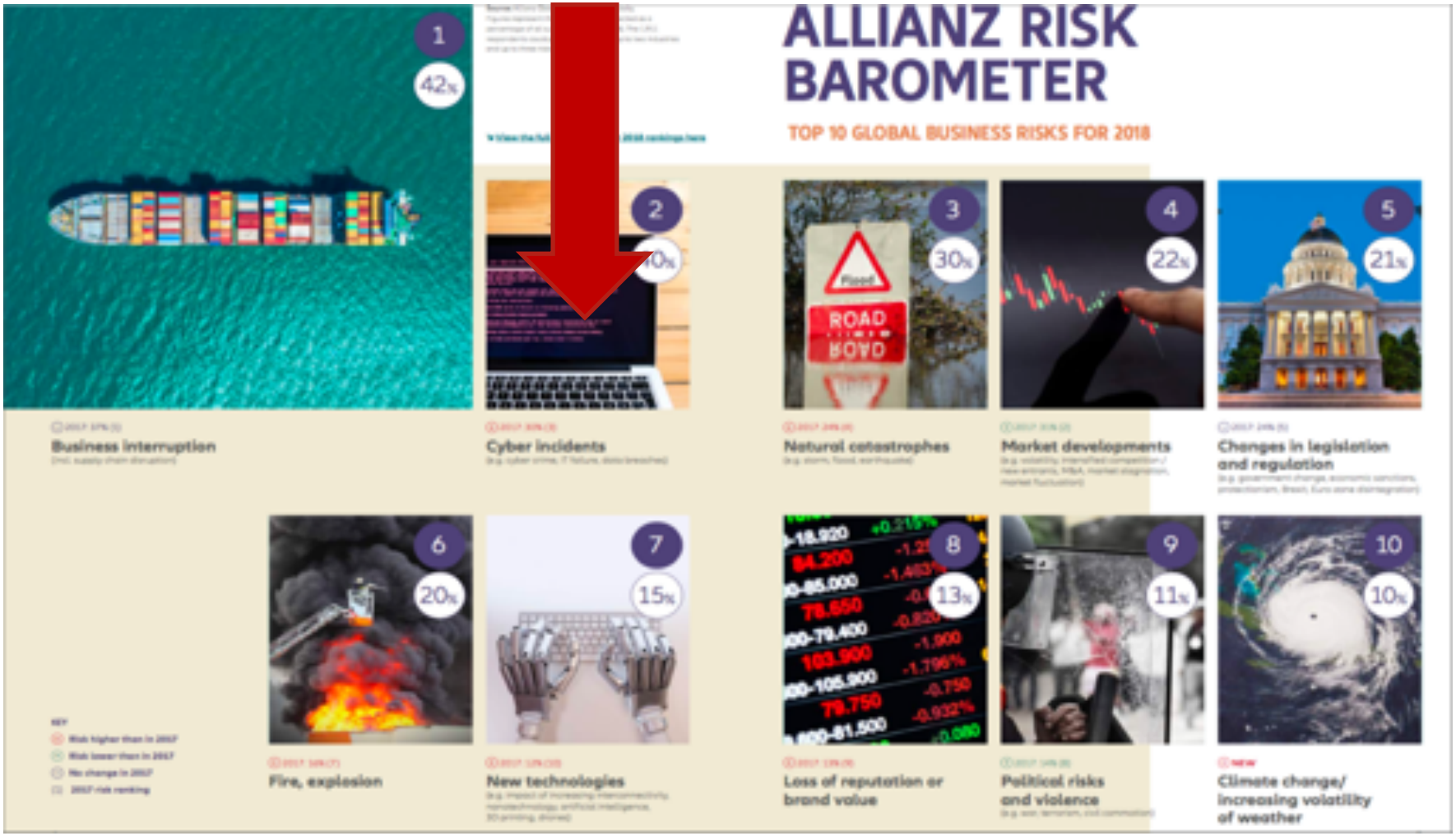
OSSERVATORI.NET digital innovation

QUELLI CHE...

...IO VORREI TANTO... IL PROBLEMA SONO I MIEI CAPI...

NON CAPISCONO...

La consapevolezza cresce…



QUELLI CHE...

...E IL GDPR?

GRAZIE

Domande?

Luca Bechelli
Direttivo e Comitato Tecnico Scientifico Clusit
luca@bechelli.net
www.bechelli.net
https://twitter.com/luca_bechelli
https://www.facebook.com/bechelli.luca
http://www.linkedin.com/in/lucabechelli