I più significativi dati emersi da OAD 2018 sugli attacchi digitali intenzionali in Italia

Marco R. A. Bozzetti

Presidente AIPSI, Capitolo Italiano ISSA

Ideatore e realizzatore OAD

CEO Malabo Srl

m.bozzetti@aipsi.org

www.aipsi.org

www.oadweb.it

www.malaboadvisoring

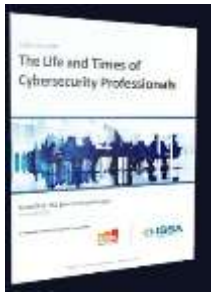
CWC 2018 CYBER WARFARE CONFERENCE

OAD Osservatorio Attacchi Digitali in Italia

MILANO - 12 DICEMBRE 2018
9^ EDIZIONE NAZIONALE
PALAZZO STELLINE - CORSO MAGENTA 61

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

- Associazione apolitica e senza fini di lucro
- Capitolo Italiano di ISSA, Information Systems Security Association, (www.issa.org) che conta >>12.000 Soci, la più grande associazione non-profit di professionisti della Sicurezza ICT nel mondo
- Obiettivo principale: aiutare i propri Soci nella crescita professionale → competenze →carriera e crescita business
  - Offrendo ai propri Soci servizi qualificati per tale crescita, che includono
    - Convegni, workshop, webinar sia a livello nazionale che internazionale via ISSA
    - ISSA Journal
    - Rapporti annuali e specifici; esempi:
      - Rapporto annuale OAD nel nuovo sito https://www.oadweb.it
      - ESG ISSA Survey "The Life and Times of Cyber Security Professionals"
    - Concreto supporto nell'intero ciclo di vita professionale, con formazione specializzata e supporto alle certificazioni, in particolare eCF Plus (EN 16234-1:2016)
    - Collaborazione con varie Associazioni ed Enti per eventi ed iniziative congiunte
    - Gruppo Specialistico di Interesse CSWI, Cyber Security Women Italy, aperto a tutte le donne che in Italia operano a qualsiasi livello nell'ambito della sicurezza digitale (anche non socie AIPSI)



OAD, Osservatorio Attacchi Digitali in Italia (ex OAI)

- *Che cosa è*
  - Indagine via web sugli attacchi digitali intenzionali ai sistemi informatici in Italia

- *Obiettivi iniziativa*
  - Fornire informazioni sulla reale situazione degli attacchi digitali in Italia
  - Contribuire alla creazione di una cultura della sicurezza informatica in Italia, sensibilizzando in particolare i vertici delle aziende/enti ed i decisori sulla sicurezza informatica

- *Che cosa fa*
  - Indagini annuali e specifiche su argomenti caldi, condotte attraverso un questionario on-line indirizzato a CIO, CISO, CSO, ai proprietari/CEO per le piccole aziende

- *Come*
  - Rigore, trasparenza, correttezza, assoluta indipendenza (anche dagli Sponsor)
  - Rigoroso anonimato per i rispondenti ai questionari
  - Collaborazione con numerose Associazioni (Patrocinatori) per ampliare il bacino dei rispondenti e dei lettori

2018
10 anni di indagini via web sugli attacchi ai sistemi informatici in Italia

CWC 2018 CYBER WARFARE CONFERENCE

OAD Osservatorio Attacchi Digitali in Italia

MILANO - 12 DICEMBRE 2018
9^ EDIZIONE NAZIONALE
PALAZZO STELLINE - CORSO MAGENTA 61

Rapporto 2018 OAD

- 160 pagine A4
- 140 grafici
- 11 Capitoli → 131 pagine A4
  - Cap. 11: Dati dalla Polizia Postale e delle Telecomunicazioni, commentati dall'autore
- 9 Allegati →29 pagine A4
- Prefazione dott. ssa Nunzia Ciardi, Direttore Polizia Postale e delle Telecomunicazioni
- Executive Summary in italiano e in inglese

Per scaricare il Rapporto 2018 OAD (gratuito):

- Registrarsi a https://www.oadweb.it
- Consenso esplicito privacy
- Scaricare il file in pdf

OAD 2018

SPONSOR

PAT

Con la collaborazione della Polizia Postale e delle Comunicazioni
e con la Prefazione al Rapporto 2018 del Direttore dott.sa Nunzia Ciardi

Le novità di OAD 2018

Chiara separazione tra **che cosa** e **come** attacco

Che cosa è attaccato	Come (tecniche attaccco)						
	Attacco fisico	Raccolta informazioni (es. social engineering, phishing, pharming, hoax,scanning, indagini su Internet, ecc.)	Script e programmi maligni (ransomware, spyware, adware, ..)	Agenti autonomi: programmi maligni che si replicano e diffondono autonomamente, come virus e worm	Toolkit: programmi in grado di scoprire e sfruttare vulnerabilità (rootkit, metaexploit, ..)	Strumenti distribuiti controllati centralmente (Command Control) quali bootnet	utilizzzo di due o più delle precedenti tecniche (APT, Advanced Persistent Threat)
Distruzione fisica di dispositivi ICT o di loro parti							
Furto fisico di dispositivi ICT o di loro parti							
Furto informazioni da sistemi fissi (PC, server, storage system, ...)							
Furto informazioni da sistemi mobili (palmari, smartphone, tablet, ecc.)							
Attacchi all'identificazione, autenticazione e controllo accessi degli utenti e degli operatori							
Attacchi alle reti locali e geografiche, fisse e wireless, e ai DNS							
Uso non autorizzato risorse ICT (dal PC ai server-storage e ai servizi in cloud)							
Modifiche non autorizzate ai programmi applicativi e di sistema, alle configurazioni, ecc.							
Modifiche non autorizzate alle informazioni trattate dai sistemi ICT							
Saturazione risorse digitali (DoS, DDoS)							
Attacchi ai propri sistemi in cloud o in hosting presso Fornitori							
Attacchi a dispositivi IoT (Internet of Thinks) in uso							
Attacchi ai propri sistemi di automazione (DCS, PLC, ..) e di robotica							
Attacchi a sistemi e/o servizi basati su blockchain							

- per ogni tipo di attacco (che cosa), se l'attacco è stato rilevato appaiono delle sotto domande che includono:
  - la frequenza di attacchi
  - le "macro" tecniche di attacco (come)
  - i principali impatti subiti dall'attacco più grave
  - le possibili motivazioni dell'attacco più grave
  - il tempo massimo richiesto per il ripristino ex ante nel caso del più grave attacco di quel tipo subito nell'anno
- se no si salta al tipo di attacco successivo

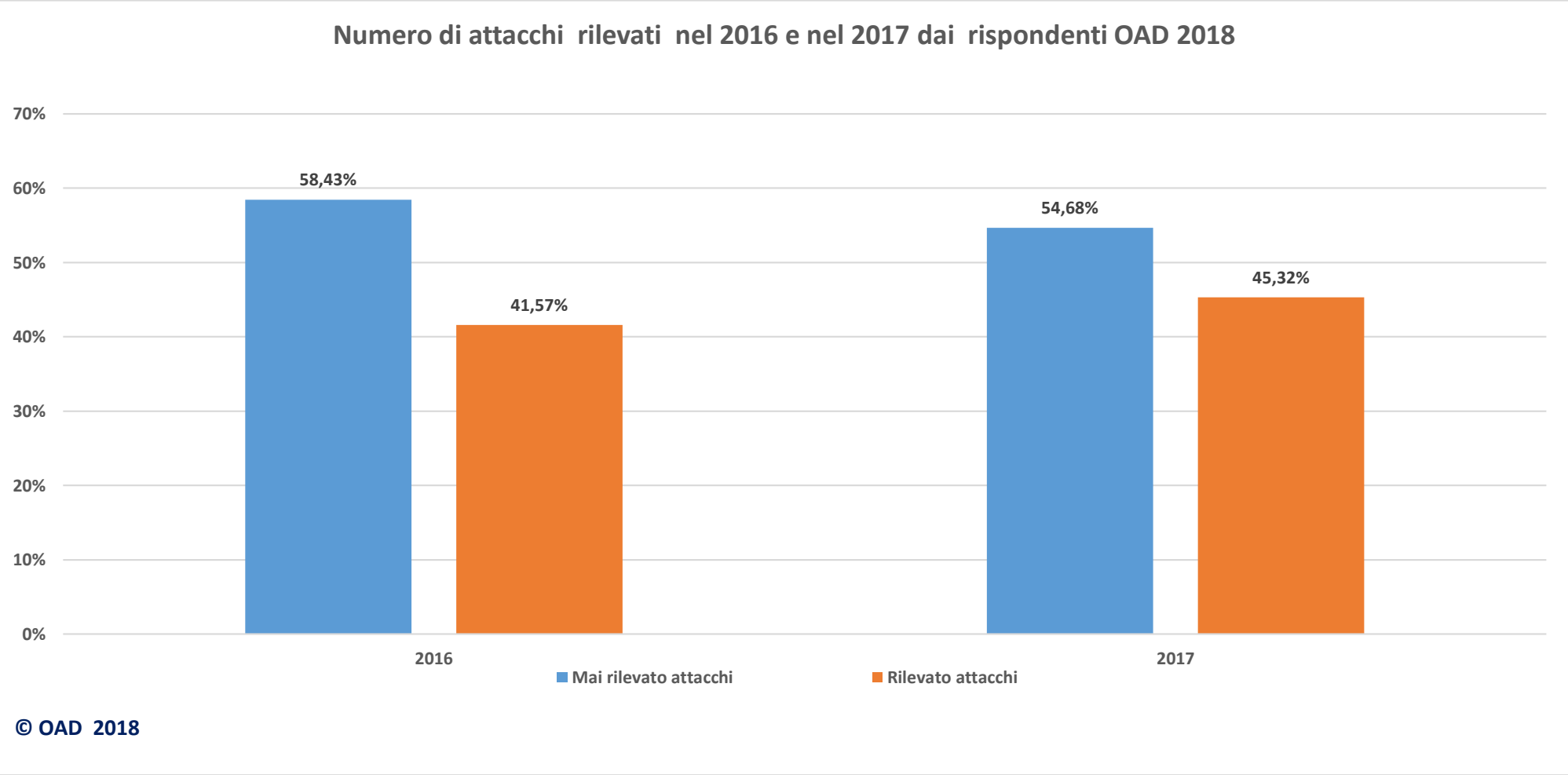
Attacchi ai servizi ICT terziarizzati

Attacchi a IoT

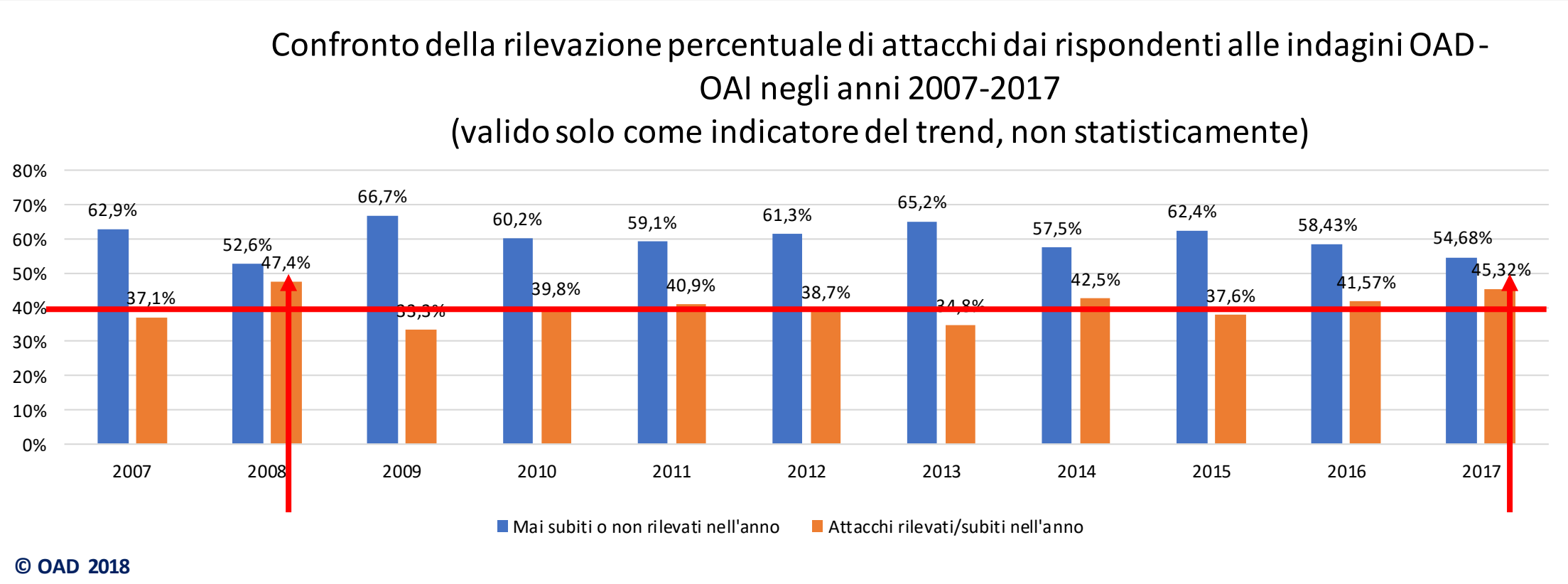
Attacchi sistemi aut. industriale e robotici

Attacchi alla blockchain

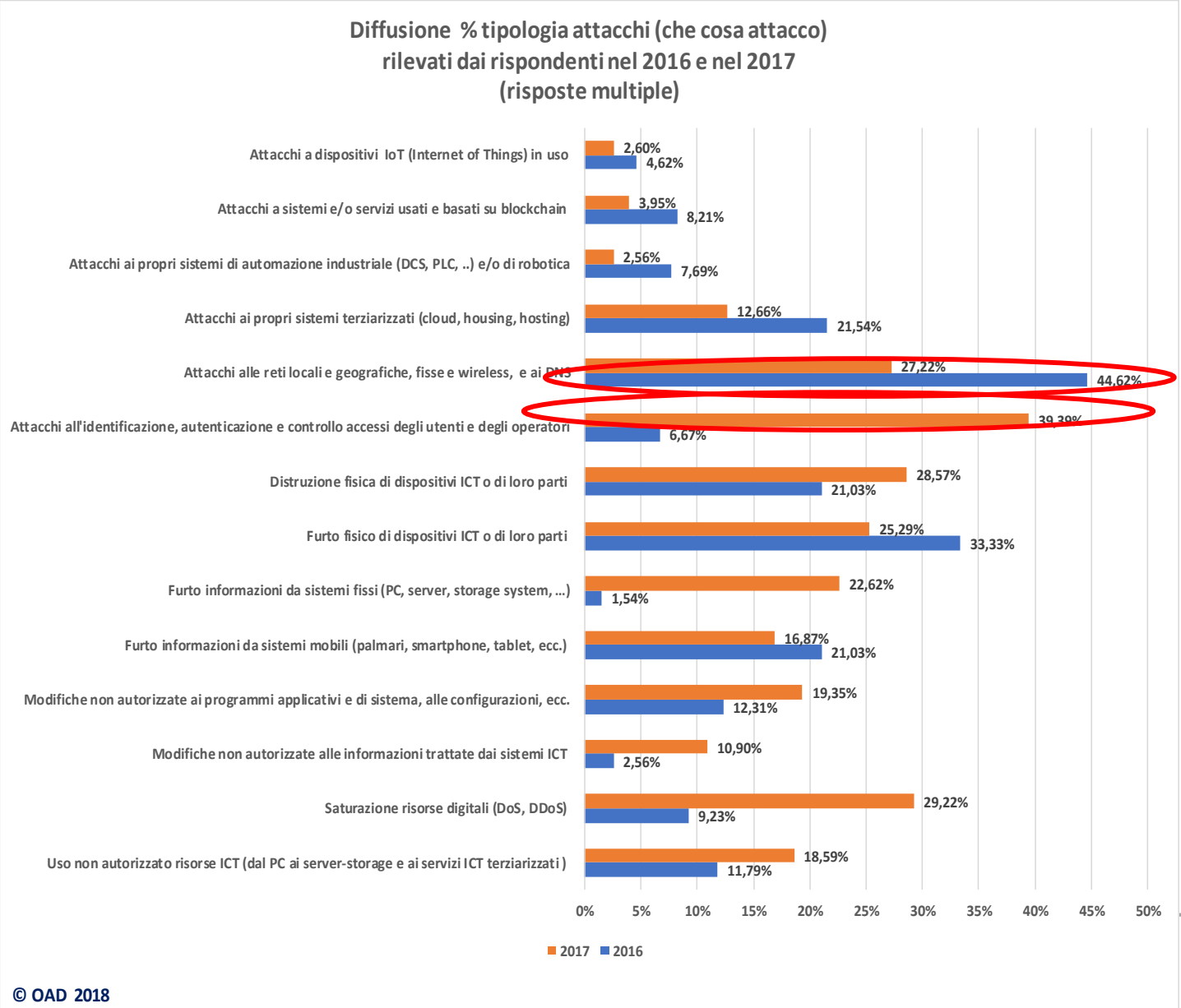
OAD 2018: attacchi rilevati 2016-17



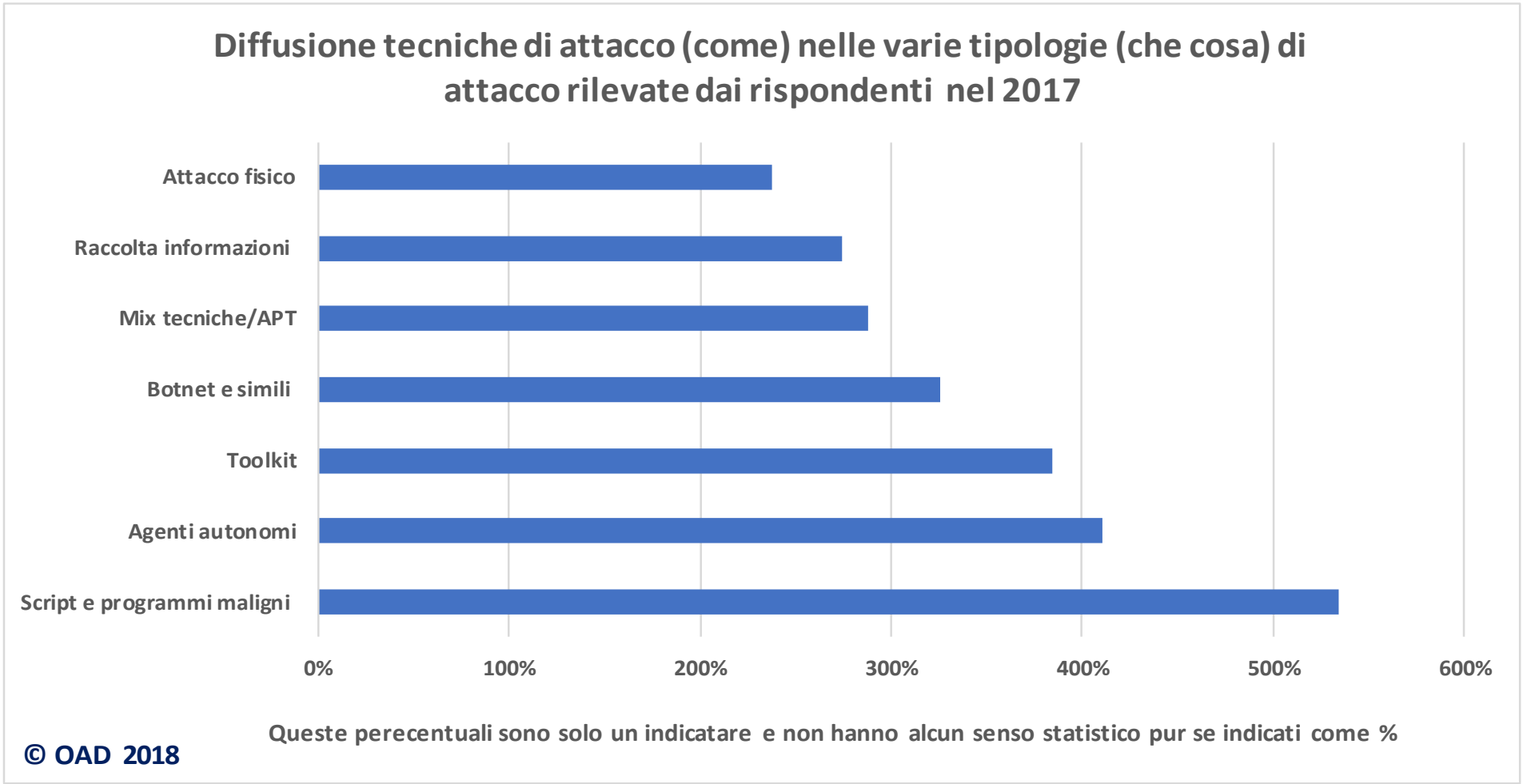
Un indicatore di confronto 2007-2017



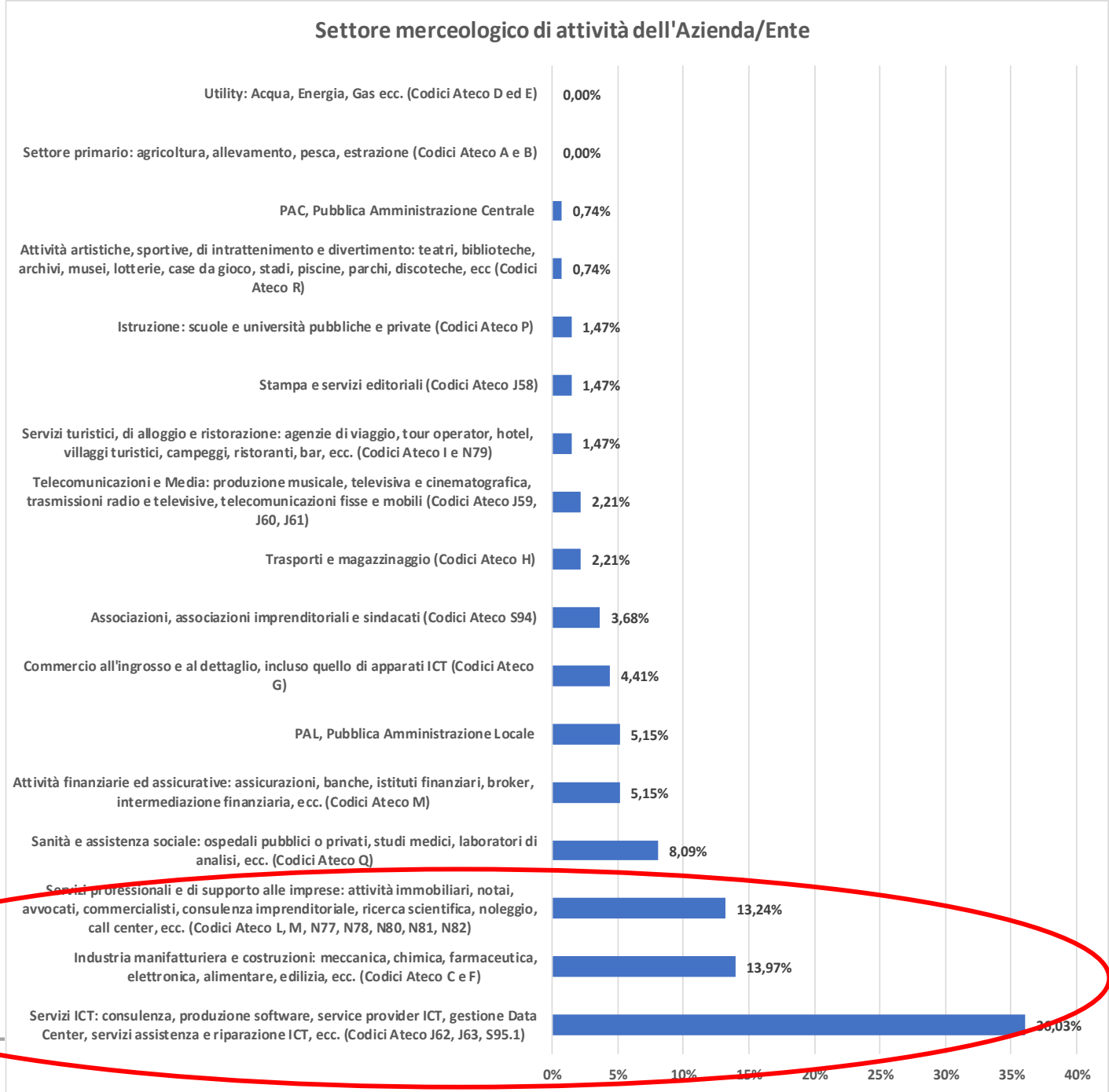
OAD 2018: diffusione tipologia attacchi rilevati 2016-17



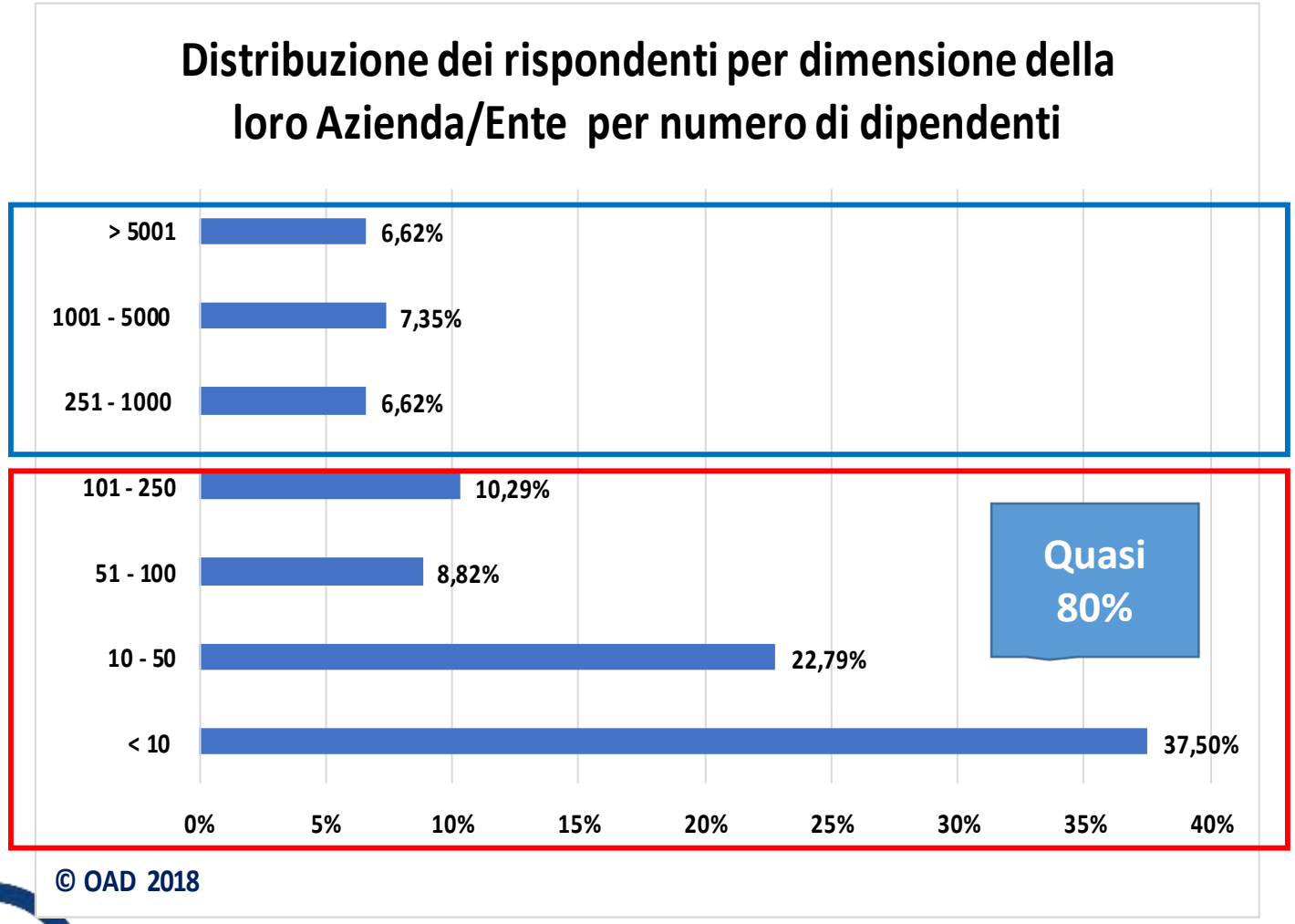
OAD 2018: diffusione tecniche di attacco 2017



OAD 2018: settore merceologico aziende/enti dei rispondenti



OAD 2018: rispondenti per dimensioni azienda/ente



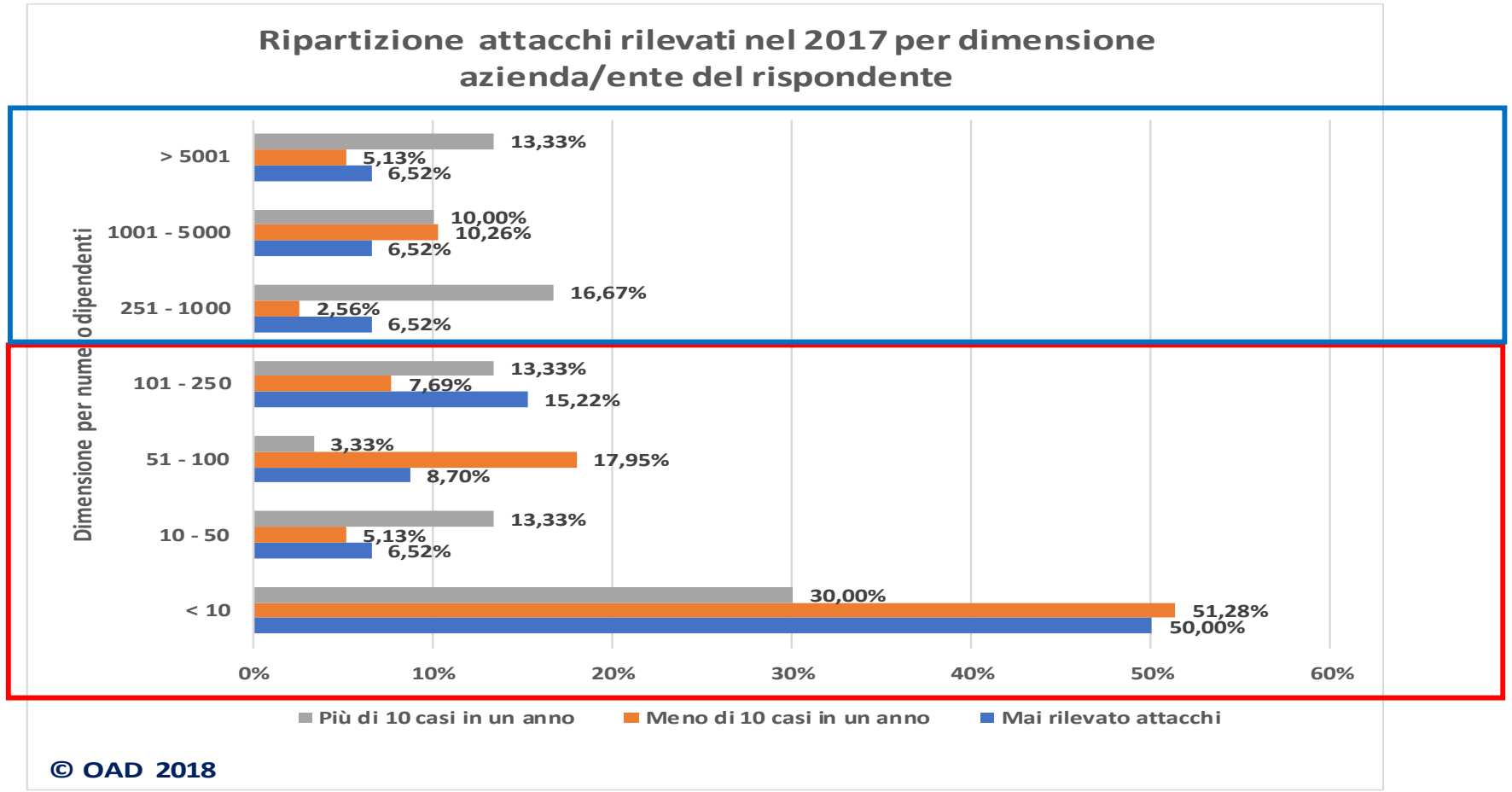
I più recenti dati ISTAT per le aziende:

- Fino a 9 dipendenti: **4.180.870**
- Da 10 a 49: 184.098
- Da 50 a 249: 22.156
- 250 e più: 3.787.

Pubbliche Amministrazioni:

- Circa **55.000**

OAD 2018: ripartizione attacchi 2017 per dimensioni azienda/ente



OAD 2018: dati Polizia Postale - 1

C.N.A.I.P.I.C. Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

Protezione strutture critic	gen – 31 dic 201	gen – 31 dic 2016	Differenza %
Attacchi rilevati	1032	844	**22,27%**
Alert diramati	31524	6721	**369,04%**
Indagini avviate	72	70	**2,86%**
Persone arrestate	3	3	**0,00%**
Persone denunciate	1316	1226	**7,34%**
Perquisizioni	73	58	**25,86%**
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	83	85	**-2,35%**

Indagini/ attacchi 6,89%

Indagini/ attacchi 8,29%

Arresti/ denunce 0,23%

Arresti/ denunce 0,24%

OAD 2018: dati Polizia Postale - 2

Financial Cyber Crime

Financial Cyber Crime	1 gen – 31 dic 2017	1 gen – 31 dic 2016	Differenza %
Transazioni Fraudolente Bloccate in €	€ 20.839.576,00	€ 16.050.812,50	**29,84%**
Somme Recuperate	€ 862.000,00	=	
Arrestati	25	25	**0,00%**
Denunciati	2851	3772	**-24,42%**

Arresti/ denunce 0,88%

Arresti/ denunce 0,66%

Cyber Terrorismo

Cyber Terrorismo	1 gen – 31 dic 2017	gen – 31 dic 2016	Differenza %
Arrestati	4	2	**100,00%**
Denunciati	18	9	**100,00%**

Arresti/ denunce 22%

Arresti/ denunce 22%

aipsi
ASSOCIAZIONE ITALIANA PROFESSIONISTI SICUREZZA INFORMATICA

GRAZIE DELL'ATTENZIONE