

# Cybersecurity, è il momento!

E' un momento critico: da un lato si moltiplicano gli **attacchi informatici** (WannaCry, Petya, Bad Rabbit ...), dall'altro aumentano **responsabilità, normative e sanzioni**. Come fare?



**Primo Bonacina**  
Managing Partner  
PBS – Primo Bonacina Services

The poster features a light blue background with various icons like a lightbulb, a fingerprint, and a flame. At the top right is the SOIEL INTERNATIONAL logo with the tagline 'Eventi e riviste per l'organizzazione aziendale'. Below it, the text reads 'SOIEL Consulting HUB' in large white letters, followed by 'FIERA MILANO - RHO' and 'Dal 15 al 17 NOVEMBRE 2017'. A central dark blue banner contains the text 'Si parlerà di: CYBERSECURITY, È IL MOMENTO!'. On the right side, there is a portrait of Primo Bonacina with the text 'Con la partecipazione di: PBS Digital + Actionable + Measurable' above it and 'Primo Bonacina, Managing Partner PBS - Primo Bonacina Services' below it. At the bottom, it says 'Scopri gli altri contenuti e iscriviti su WWW.SOIEL.IT' and includes a Twitter icon with the handle '#SoielConsultingHub17 @soiel\_it'.



# Agenda

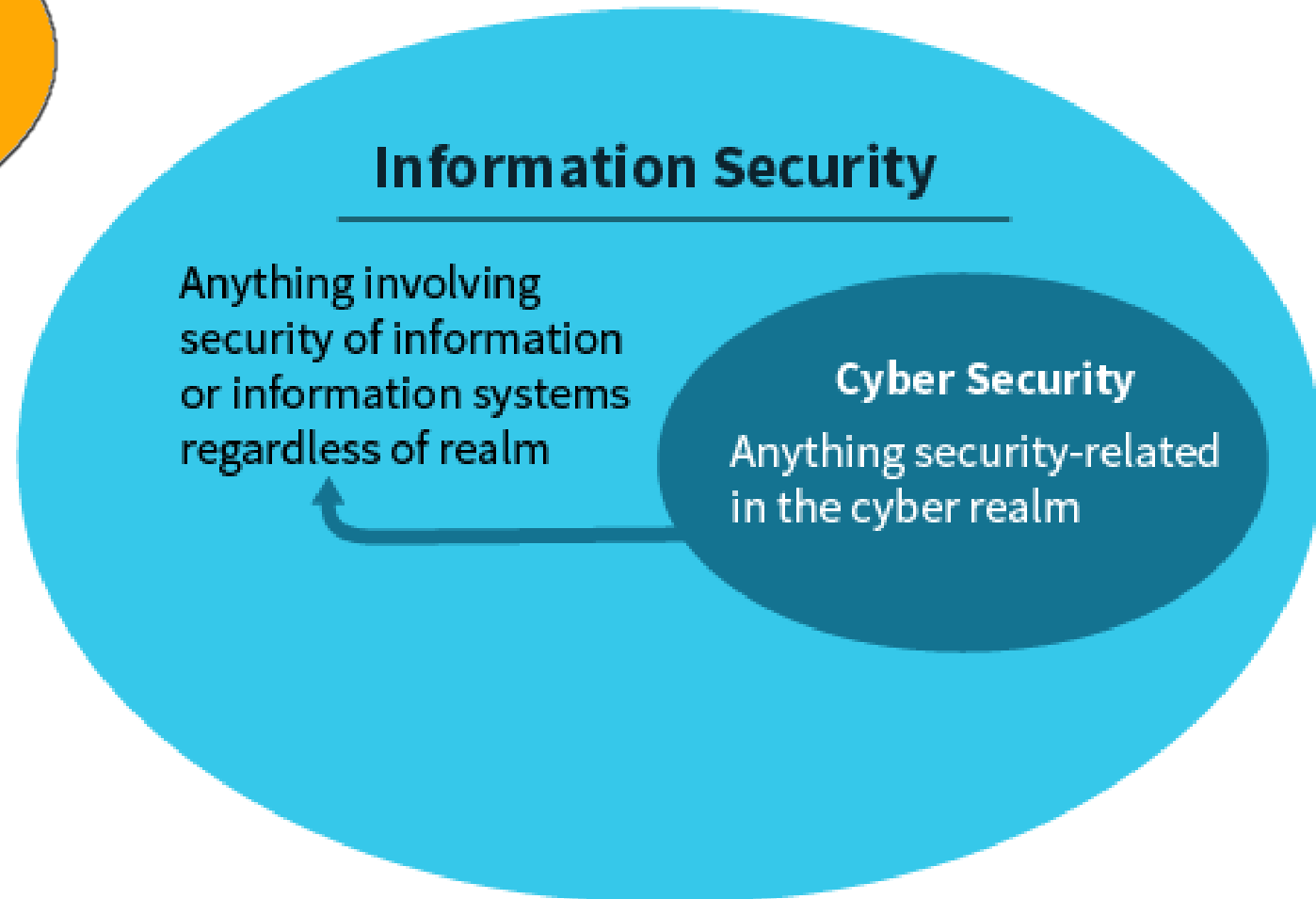
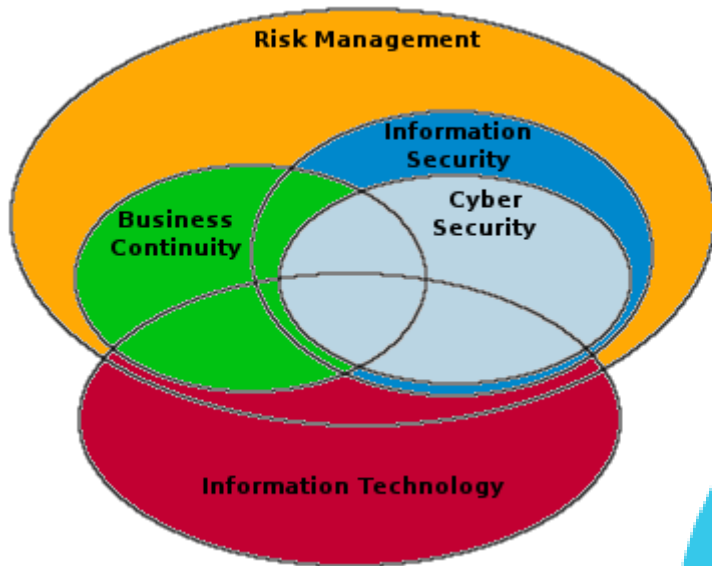
Cisco

Report annuale sulla cybersecurity 2017

- La situazione delle minacce
- L'impatto sul business
- Il ruolo del CISO e dell'organizzazione in azienda
- Il ruolo dei partner
- Restiamo in contatto!

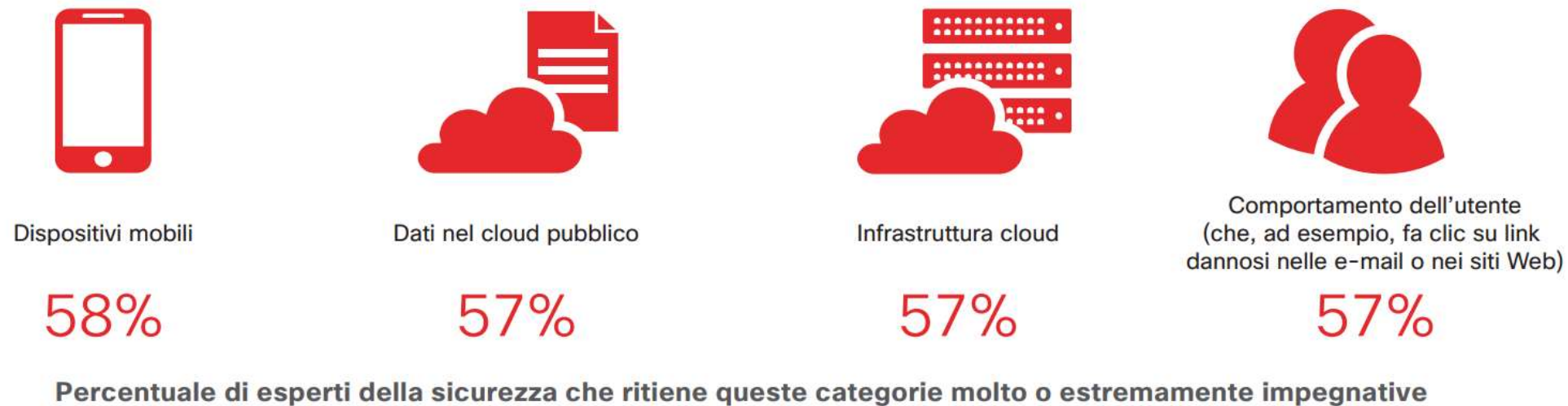


# Parliamo di Cybersecurity



# La principale preoccupazione: l'espansione della superficie di attacco

Figura 1 Le principali fonti di preoccupazione degli esperti della sicurezza in merito agli attacchi informatici



# Il comportamento degli hacker

Metodi di attacco tramite Web: le minacce con la "coda corta" consentono ai criminali informatici di gettare le basi per le campagne

La ricognizione è, ovviamente, una fase fondamentale del lancio di attacchi informatici, durante la quale gli autori vanno alla ricerca di infrastrutture Internet vulnerabili o di punti deboli delle reti che consentano loro di ottenere l'accesso ai computer degli utenti e, in ultima analisi, di infiltrarsi nelle aziende.

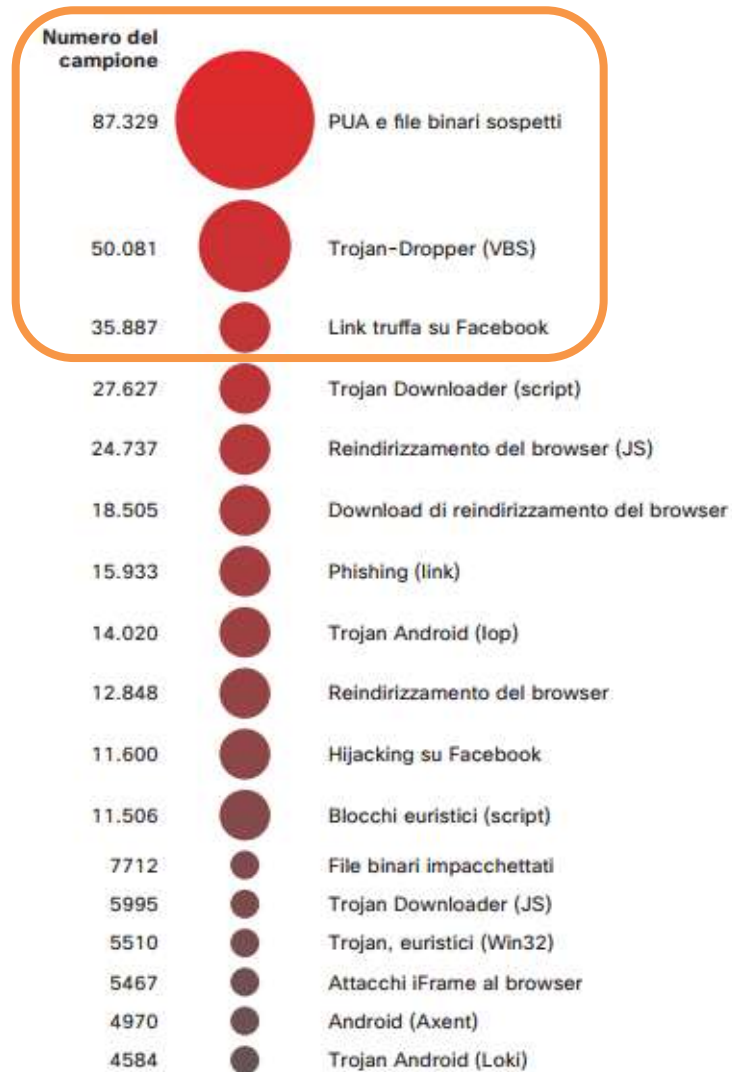
I file binari di Windows sospetti e le applicazioni potenzialmente indesiderate (PUA) si stagliano

inequivocabilmente in cima alla classifica dei metodi di attacco tramite Web per il 2016 (vedere la figura 2).

I file binari di Windows sospetti veicolano minacce quali spyware e adware, mentre le estensioni dannose per i browser sono un esempio di PUA.

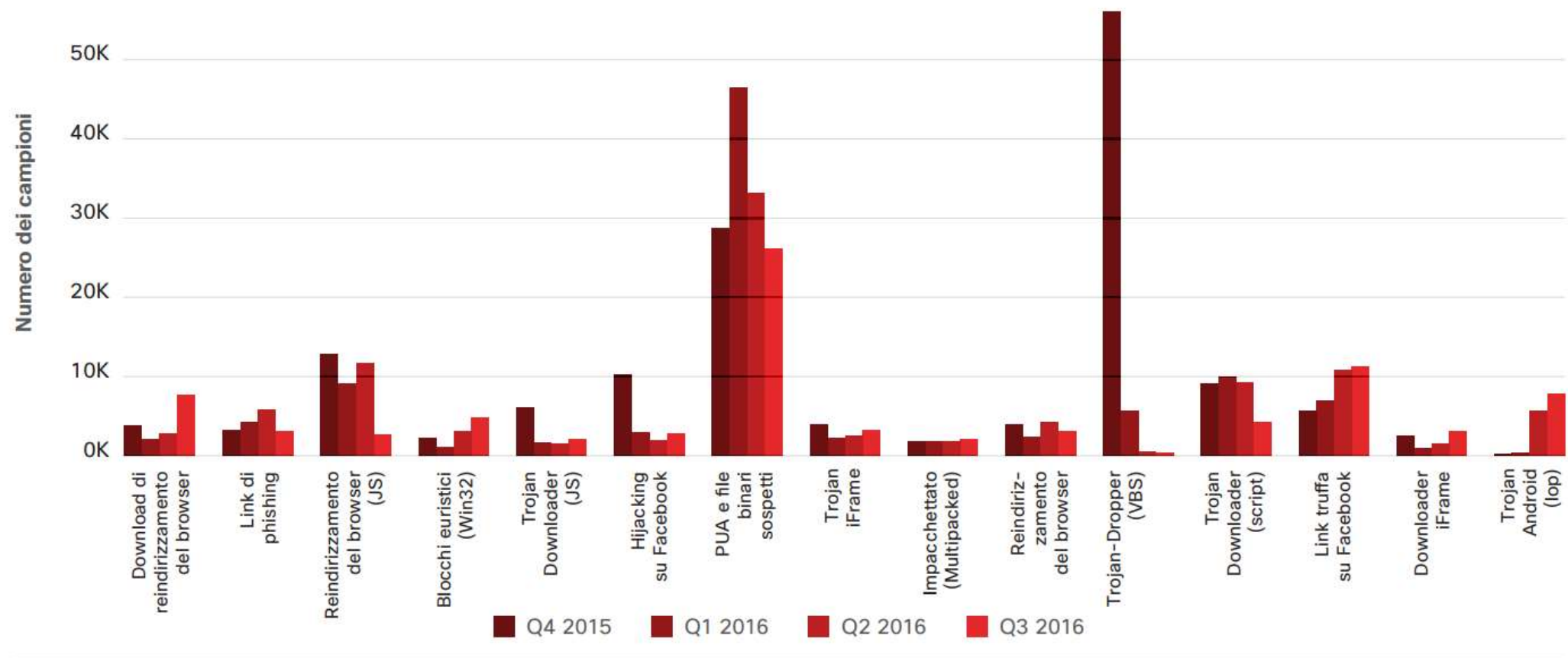
Le truffe su Facebook, costituite da false offerte e contenuti multimediali associati a finti sondaggi si sono classificati al terzo posto. La costante prevalenza delle truffe su Facebook nelle nostre classifiche annuali e semestrali relative ai casi di malware osservati più di frequente evidenzia il ruolo fondamentale del social engineering in molti attacchi informatici. Facebook dispone di circa 1,8 miliardi di utenti attivi al mese in tutto il mondo<sup>4</sup> ed è il terreno di caccia ideale per i criminali informatici e altri attori intenzionati a truffare gli utenti. Una notizia positiva è costituita dal recente annuncio dell'azienda di provvedimenti che verranno assunti per eliminare le notizie false e gli hoax. I critici ipotizzano che questi contenuti possano avere influito sul voto in occasione delle elezioni presidenziali del 2016 negli Stati Uniti.<sup>5</sup>

Figura 2 Malware più comuni



# Una svolta alla fase di ricognizione degli attacchi Web: più minacce hanno per obiettivo browser e plug-in vulnerabili

Figura 3 Il malware più comune, Q4 2015-Q3 2016



# Sicurezza delle applicazioni: come gestire il rischio delle connessioni in seguito al boom delle app e del cloud

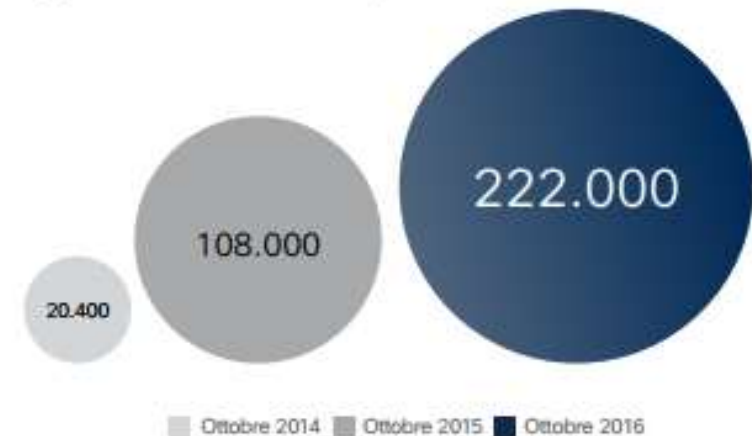


Figura 4 Crescita esponenziale delle applicazioni cloud connesse di terze parti nel 2016



Fonte: Cisco CloudLock

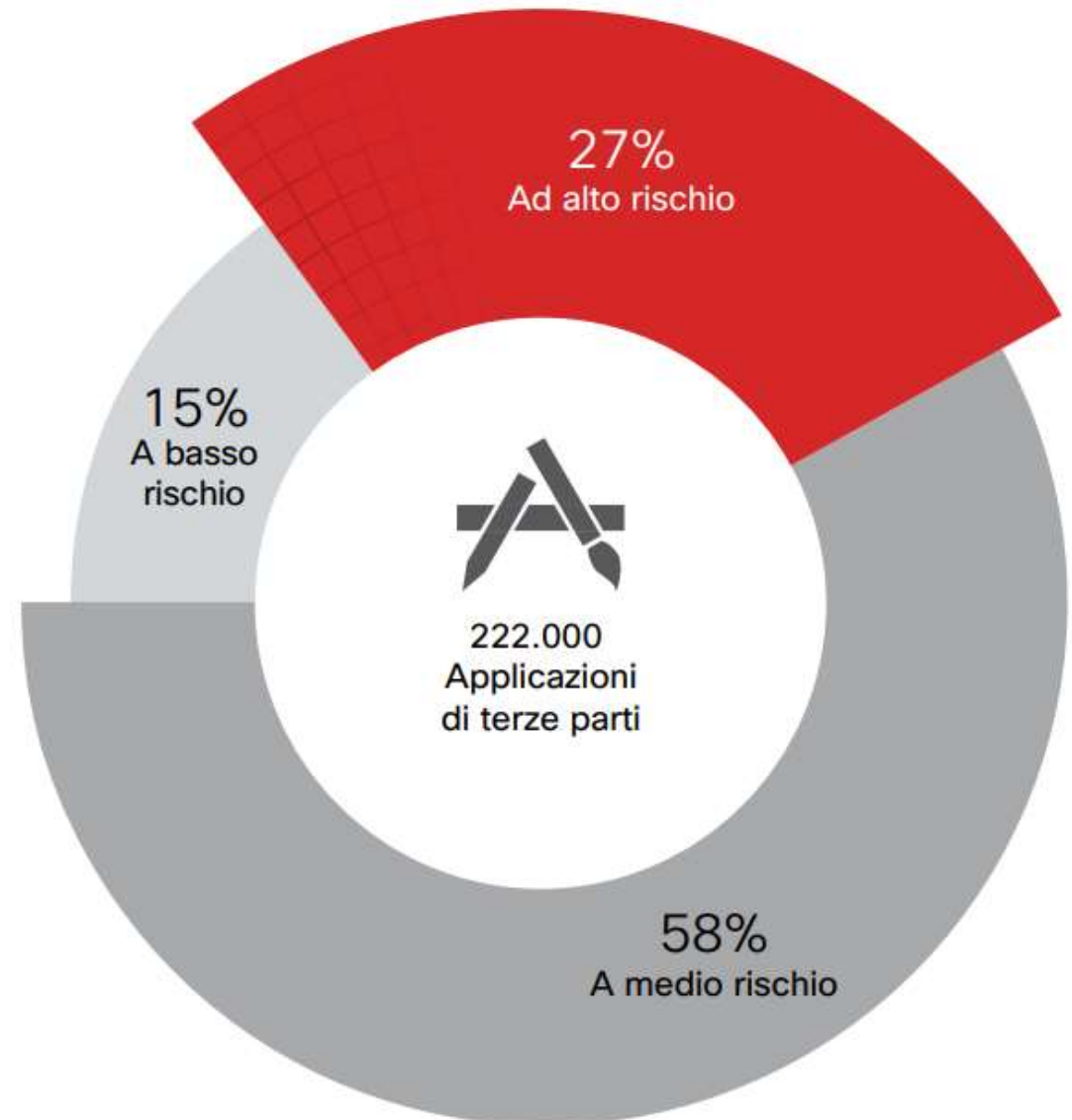
Figura 5 Confronto anno per anno della crescita delle applicazioni cloud di terze parti



Fonte: Cisco CloudLock

# Classificazione delle applicazioni più rischiose

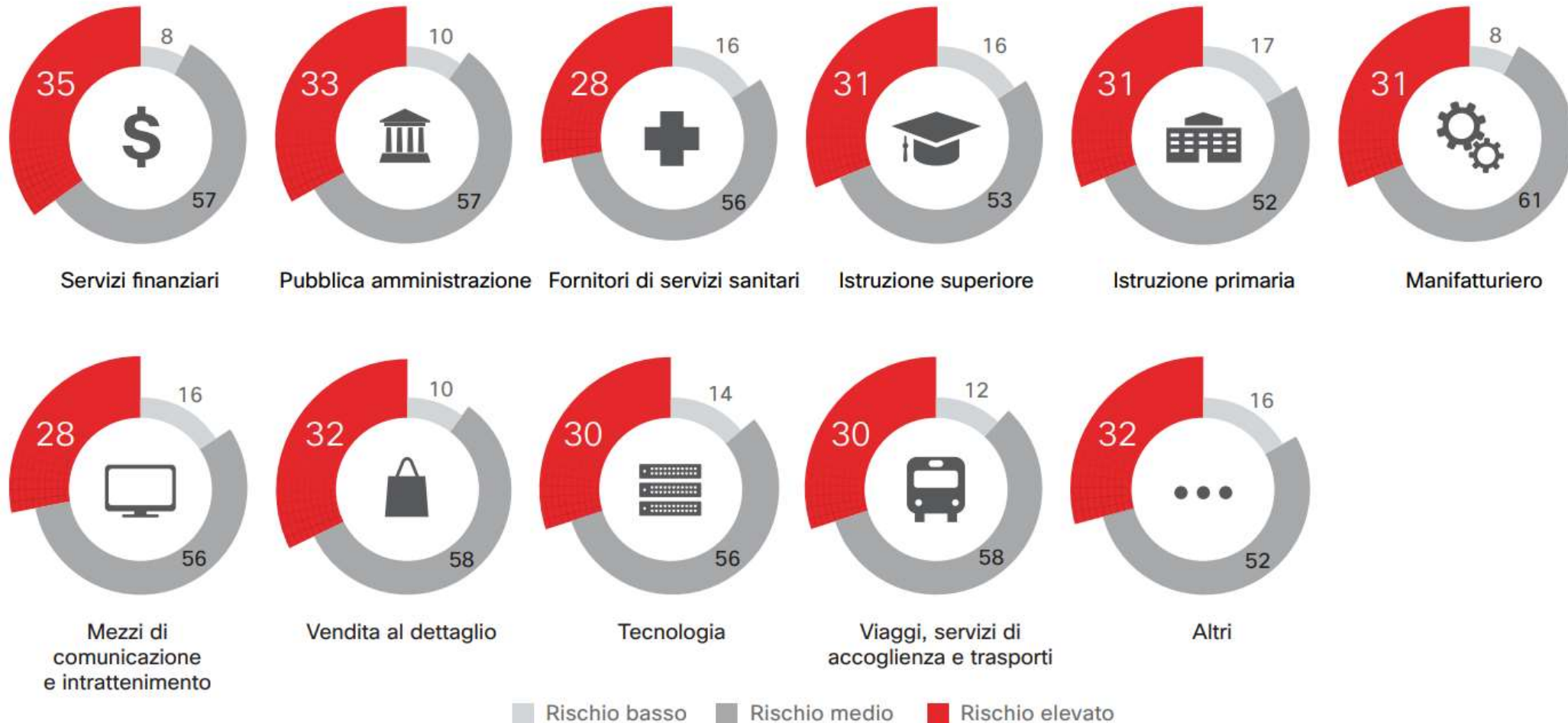
Figura 6 Applicazioni di terze parti classificate ad alto rischio





# Tutte le aziende, indipendentemente da dimensioni/settore/area geografica, presentano una quantità simile di applicazioni a rischio

Figura 8 Distribuzione di applicazioni a basso, medio e alto rischio per settore



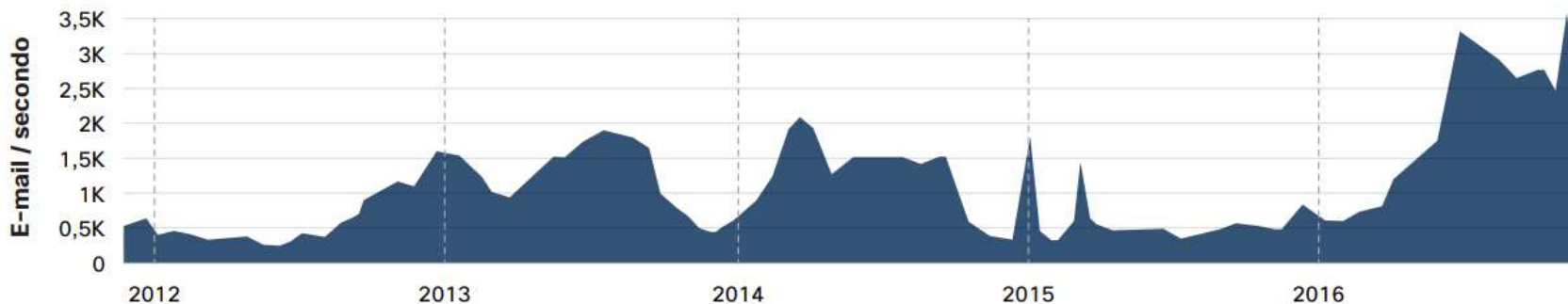
# Il 75% delle aziende è interessata da infezioni Adware

Figura 12 Percentuale di aziende colpite da infezioni da adware



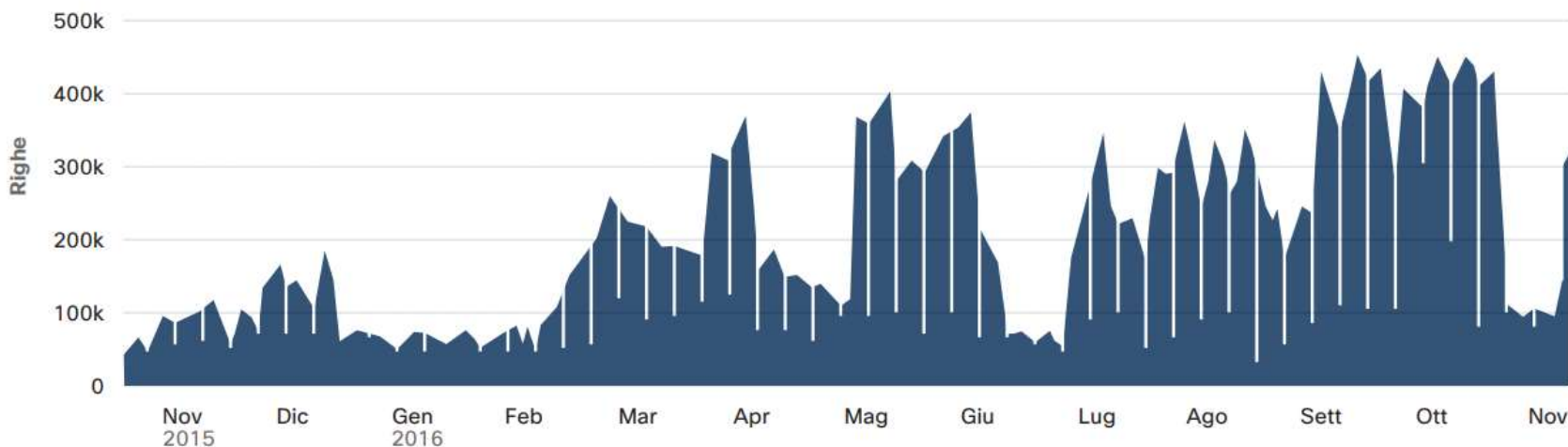
# La quantità complessiva di spam è in aumento, così come la percentuale degli allegati dannosi, #1

Figura 15 Volume totale di spam



Fonte: CBL

Figura 16 Volume complessivo di SCBL



SCBL = Spam Cop Block List

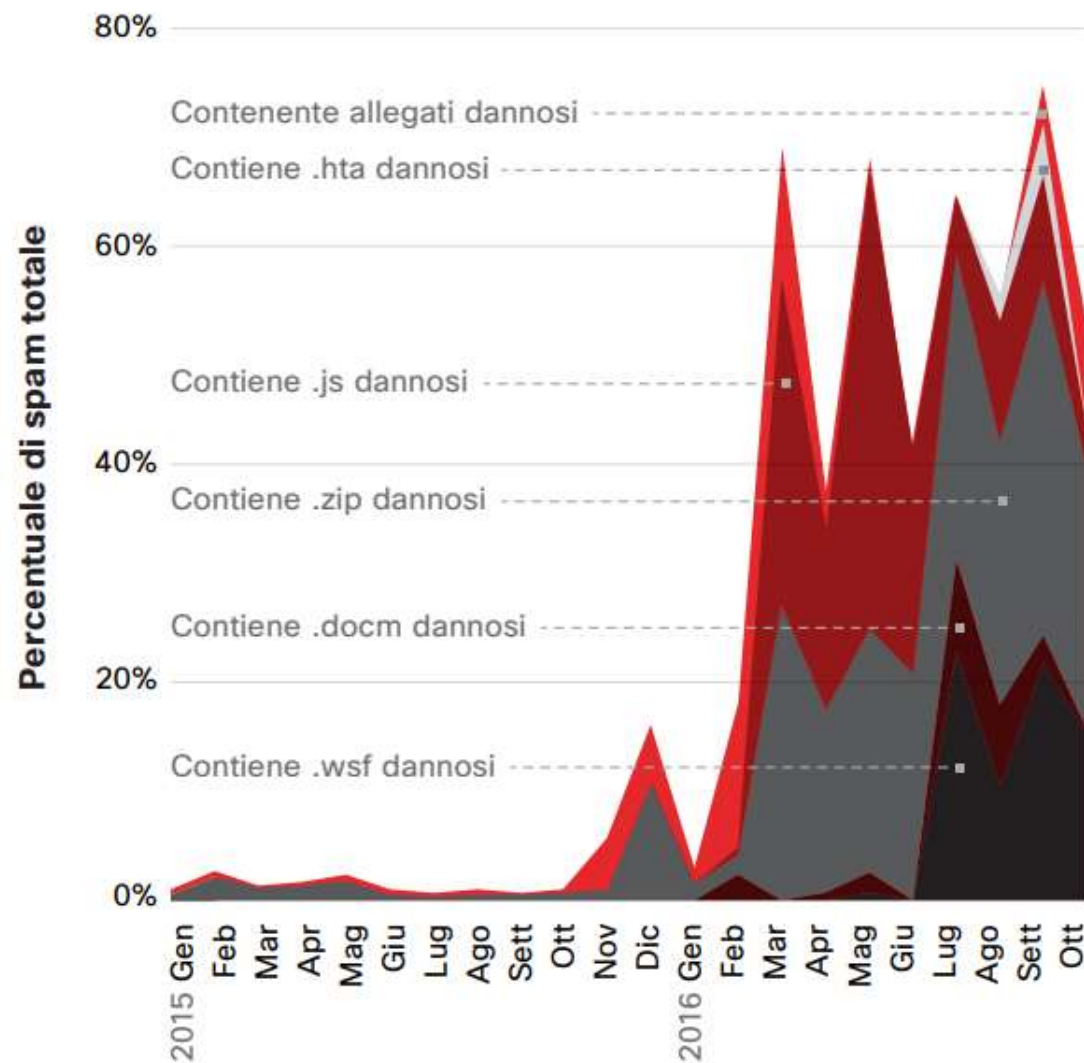
Fonte: SpamCop



# La quantità complessiva di **spam** è in aumento, così come la percentuale degli allegati dannosi, #2

70%

Figura 17 Percentuale di spam totale contenente allegati dannosi



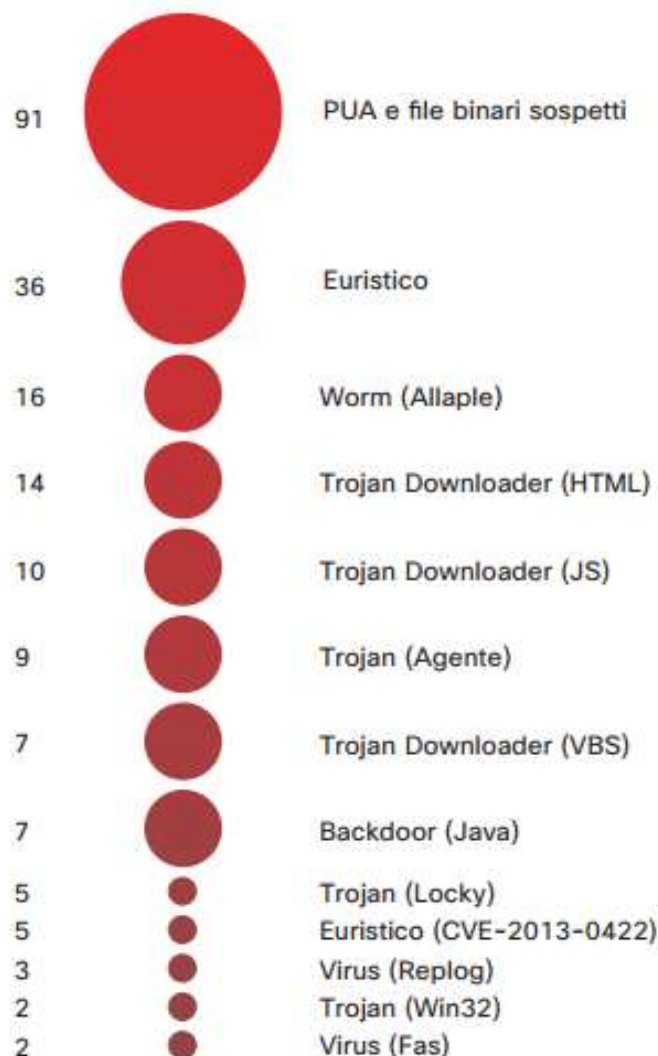
# Una volta posizionatasi, la minaccia installa una backdoor sul sistema dell'obiettivo, fornendo agli hacker un accesso costante

## Metodi di attacco Web: una panoramica sulla "coda lunga" svela le minacce che gli utenti possono evitare con facilità

La cosiddetta coda lunga del panorama dei metodi di attacco Web (figura 20) presenta una raccolta di malware che generano volumi inferiori impiegati in una fase successiva della catena di attacco: l'installazione. In questa fase, la minaccia che è giunta a destinazione (un trojan bancario, un virus, un downloader o un exploit di altro tipo) installa una backdoor nel sistema oggetto di attacco, garantendo agli hacker un accesso permanente e, insieme, l'opportunità di esfiltrare dati, lanciare attacchi ransomware e compiere altri misfatti.

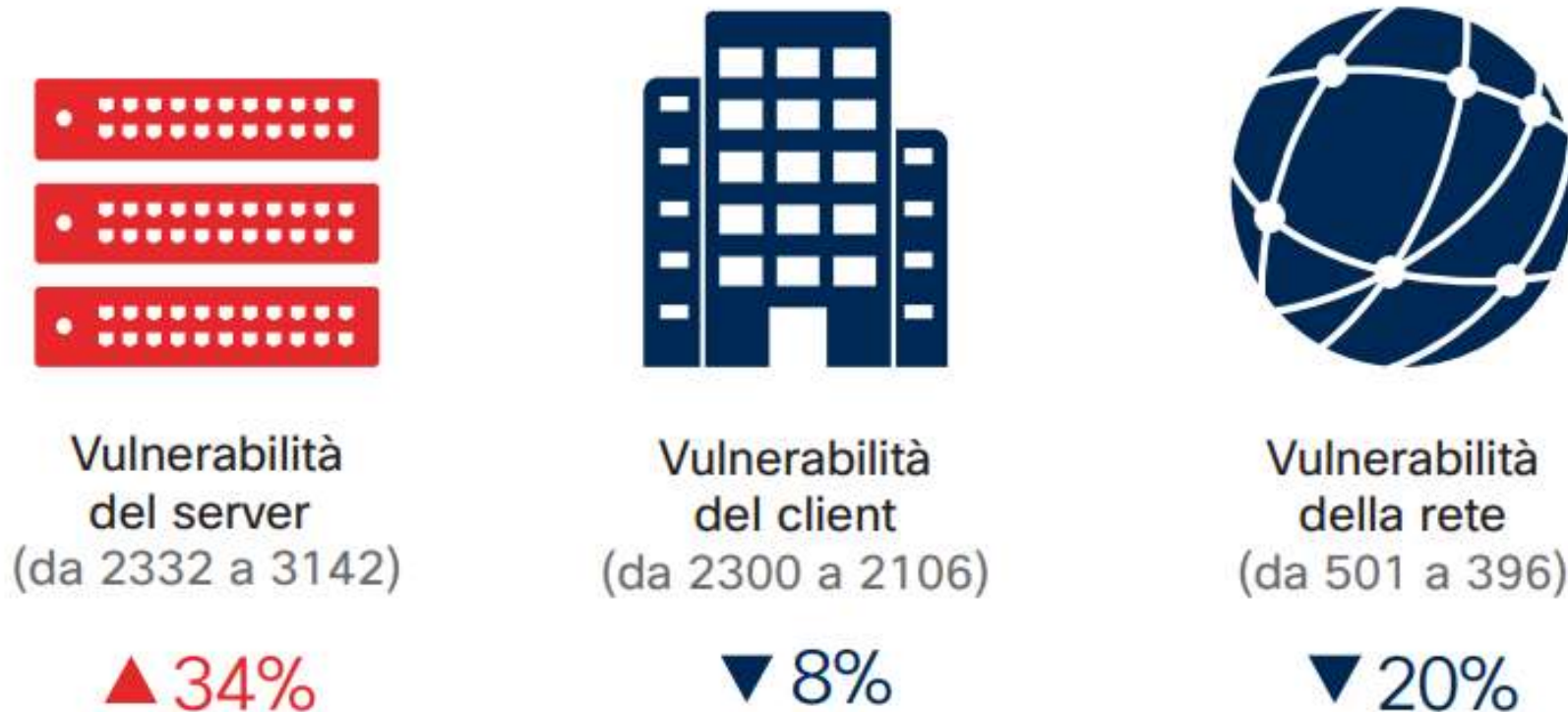
Le minacce elencate nella figura 20 sono esempi di firme individuate nei 50 tipi di malware osservati più di frequente. La coda lunga dei metodi di attacco Web è, sostanzialmente, un'istantanea delle minacce che lavorano silenziosamente all'interno dei computer e dei sistemi in seguito a un attacco condotto con successo. Molte di queste infezioni sono state diffuse inizialmente dall'incontro con adware dannoso o dall'esposizione a una truffa basata sul phishing ben architettata: queste sono situazioni che gli utenti spesso possono evitare facilmente o correggere rapidamente.

Figura 20 Campione di malware a più basso volume osservato



Lanciando attacchi ai software dei server, si può acquisire il controllo di più risorse o spostarsi su risorse fondamentali per le aziende, #1

## Figura 40 Analisi dettagliata delle vulnerabilità client-server, 2015-2016



Fonte: National Vulnerability Database

# Lanciando attacchi ai software dei server, si può acquisire il controllo di più risorse o spostarsi su risorse fondamentali per le aziende, #2



The screenshot shows the website of CERT nazionale Italia, the Computer Emergency Response Team. The header includes the CERT logo and the text 'COMPUTER EMERGENCY RESPONSE TEAM'. In the top right corner, there is a box for 'MINISTERO DELLO SVILUPPO ECONOMICO'. Below the header, there are navigation links: 'Home', 'Chi siamo', 'News', 'Bollettini', 'Documenti', and 'Contatti'. A search bar is located on the right side. The main content area features a breadcrumb trail: 'Home > News > Avviso relativo a vulnerabilità critiche in prodotti Microsoft sfruttabili in attacchi reali'. The title of the article is 'INFORMAZIONI - VULNERABILITÀ AVVISO RELATIVO A VULNERABILITÀ CRITICHE IN PRODOTTI MICROSOFT SFRUTTABILI IN ATTACCHI REALI'.

microsoft remote code execution mercoledì, 14 giugno 2017

Nella giornata del 13 giugno 2017 **Microsoft** ha emesso un avviso relativo ad aggiornamenti di sicurezza critici, alcuni nuovi ed altri pubblicati nell'arco dell'ultimo decennio, che riguardano vulnerabilità ad alto rischio che si ritiene possano essere sfruttabili in attacchi reali. Se sfruttate con successo, le più gravi tra queste vulnerabilità possono causare l'esecuzione di codice arbitrario da remoto.

Si raccomanda ai gestori e agli utenti di sistemi e prodotti Microsoft di prendere visione del [Microsoft Security Advisory 4025685](#).

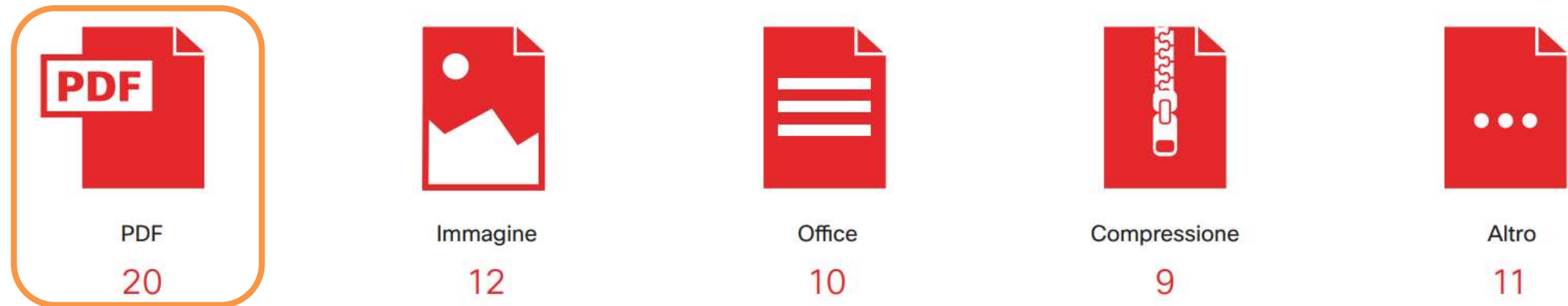
Gli utenti che hanno abilitato per le proprie piattaforme gli aggiornamenti automatici dovrebbero risultare già protetti. I gestori di sistemi più vecchi o per i quali gli aggiornamenti vengono installati manualmente debbono applicare al più presto gli aggiornamenti necessari, previa opportuna verifica.

Dettagli degli aggiornamenti contenuti nell'avviso di Microsoft:

- [Critico] **Vulnerability in Server Service Could Allow Remote Code Execution** ([MS08-067](#)): questo aggiornamento di sicurezza risolve una vulnerabilità nel servizio Server sui sistemi Windows. Questa vulnerabilità può consentire l'esecuzione di codice in modalità remota se il sistema affetto riceve una richiesta [HTTP](#) appositamente predisposta. Un attaccante potrebbe sfruttare questa vulnerabilità sui sistemi **Microsoft Windows XP** e **Windows Server 2003** per eseguire codice arbitrario senza autenticazione. Si ritiene che questa vulnerabilità possa essere utilizzata per realizzare un [exploit](#) con caratteristiche di [worm](#).

# Middleware: gli hacker individuano opportunità nel software privo di patch

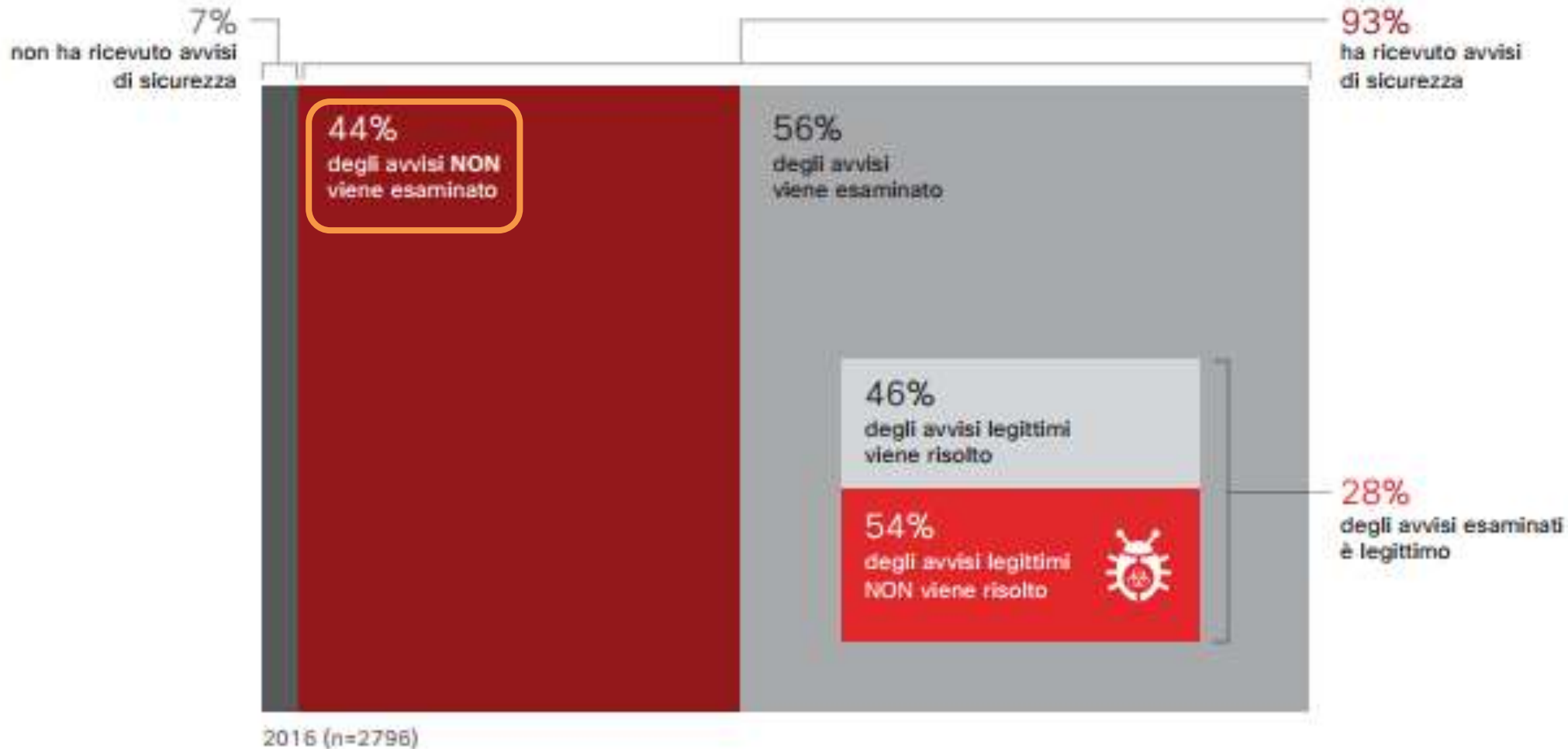
Figura 41 Vulnerabilità riscontrate nelle librerie del middleware





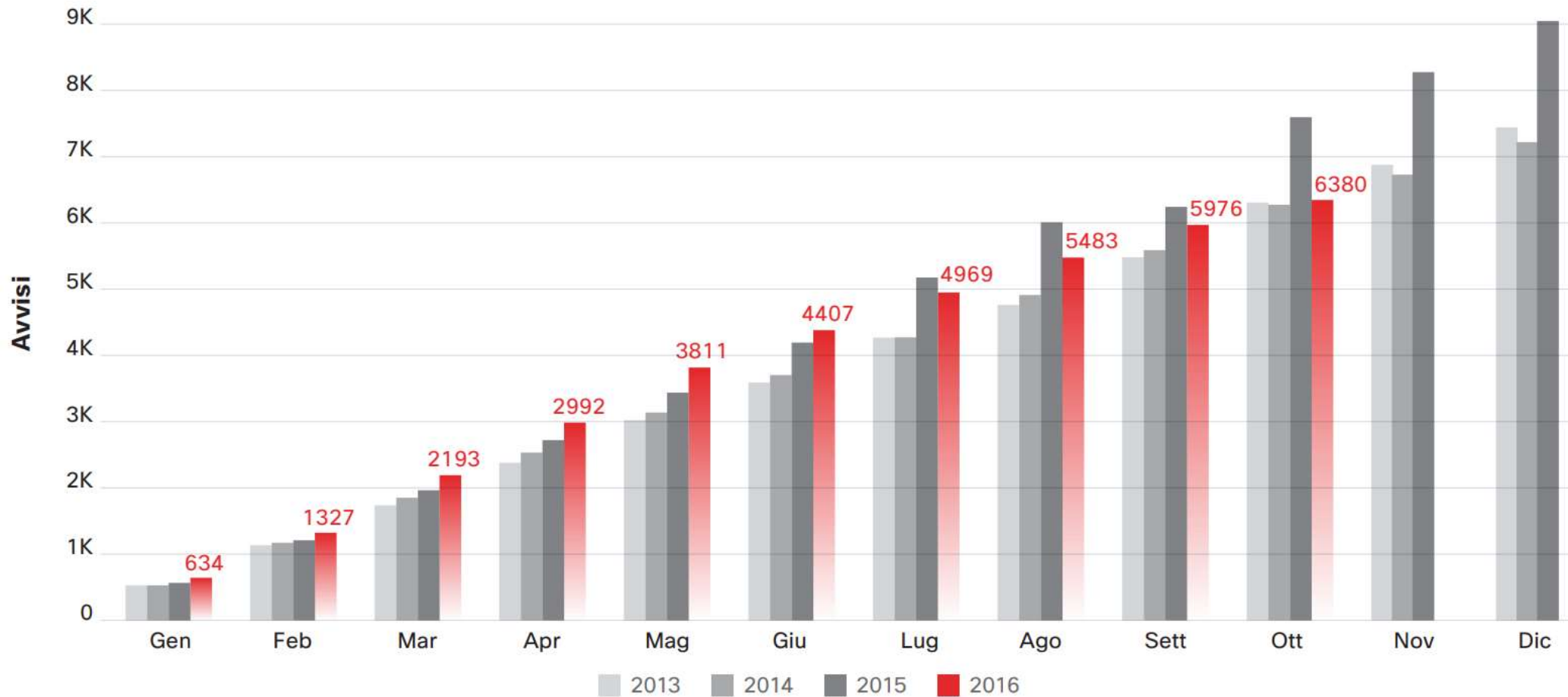
# Quante volte siamo efficaci?

Figura 52 Percentuali di avvisi di sicurezza che non vengono analizzati o corretti



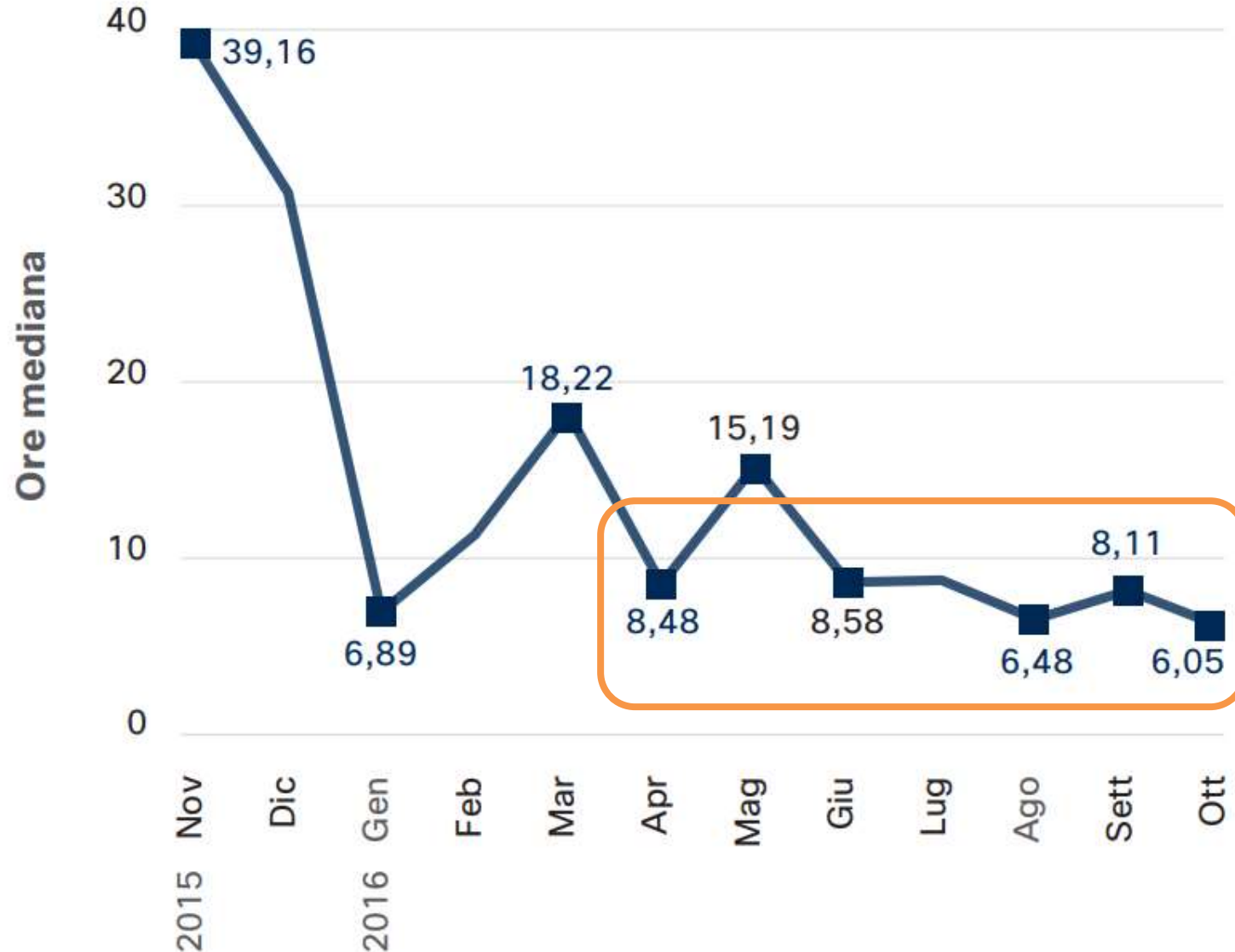
# Qualche progresso: Vulnerabilità in declino nel 2016

Figura 37 Totale cumulativo annuo degli avvisi



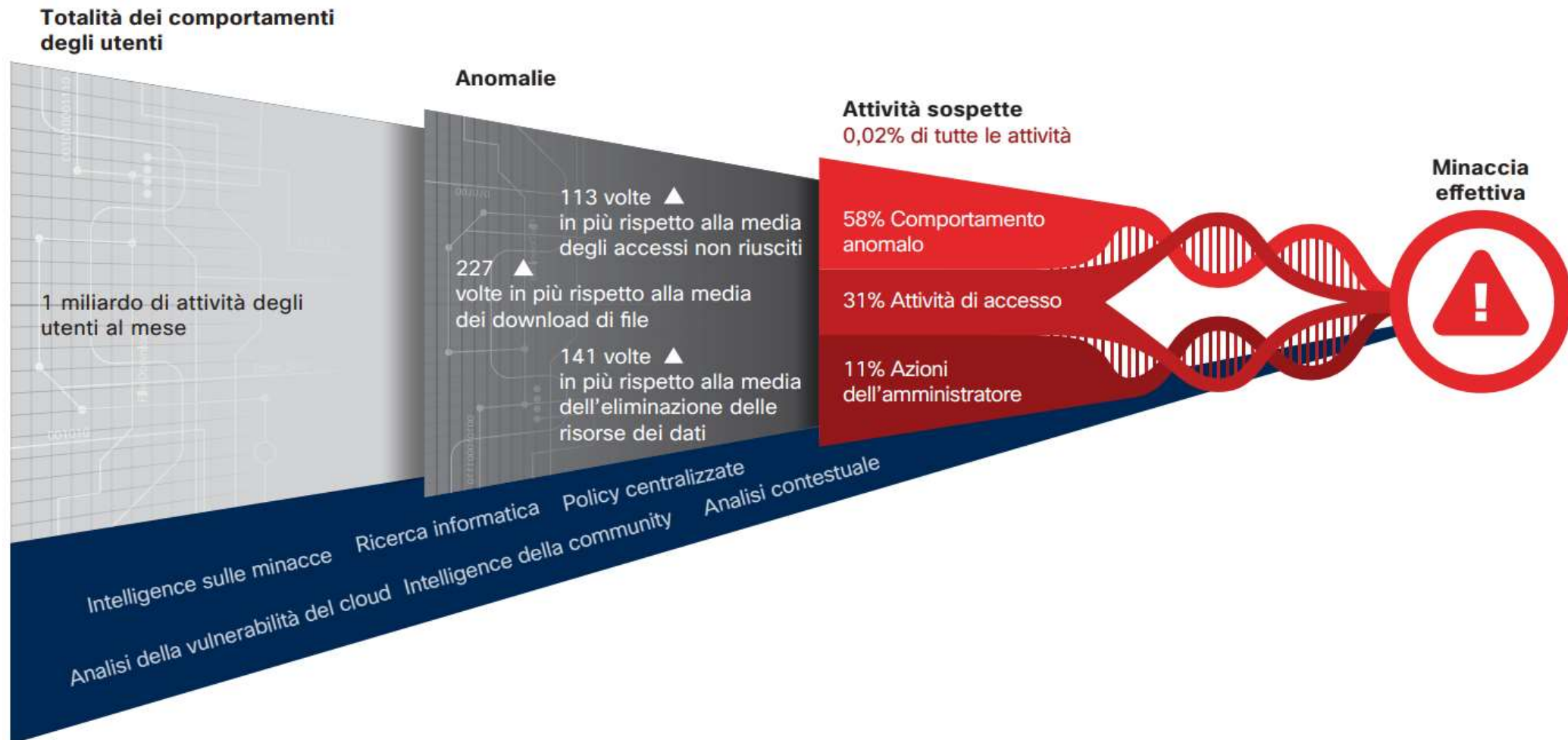
# Tempi di rilevamento («Time To Detect»): metrica essenziale per misurare i nostri progressi sulla sicurezza

Figura 23 Mediana mensile del TTD



# Solo l'automazione può aiutare a orientarsi nel "rumore" degli avvisi di sicurezza e a concentrarsi sull'analisi delle minacce reali

Figura 9 Identificazione dei modelli di comportamento degli utenti attraverso l'automazione (processo)



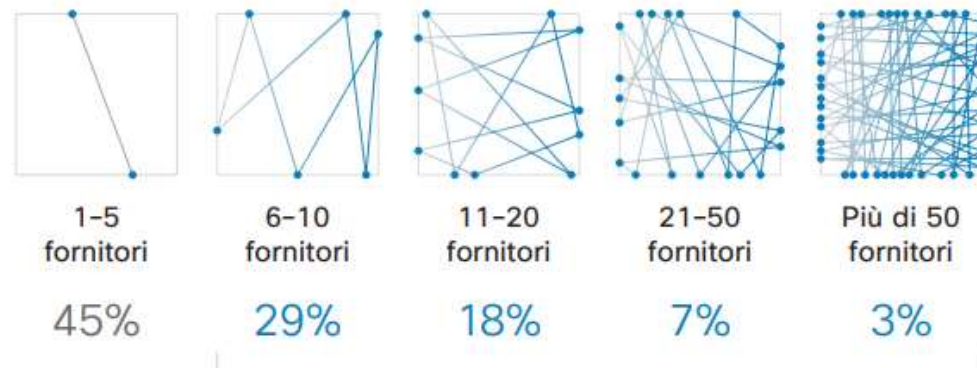
# Gli strumenti devono fornire una **visione olistica**: la mancata integrazione può aprire falle che i criminali utilizzano per lanciare attacchi

5 +

**Figura 51** Numero di fornitori e prodotti di sicurezza utilizzati dalle aziende

## Numero di fornitori di sicurezza nell'ambiente di sicurezza

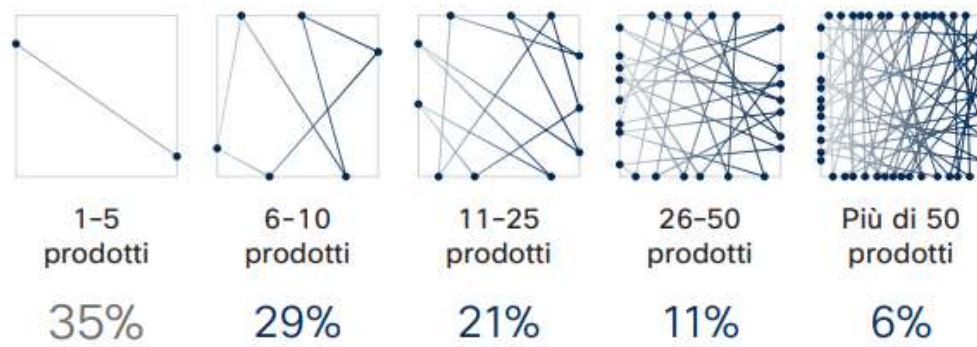
2016 (n=2850), grafico arrotondato al numero intero più vicino



**Il 55% utilizza più di 5 fornitori**

## Numero di prodotti per la sicurezza nell'ambiente di sicurezza

2016 (n=2860), grafico arrotondato al numero intero più vicino



**Il 65% utilizza più di 5 prodotti**

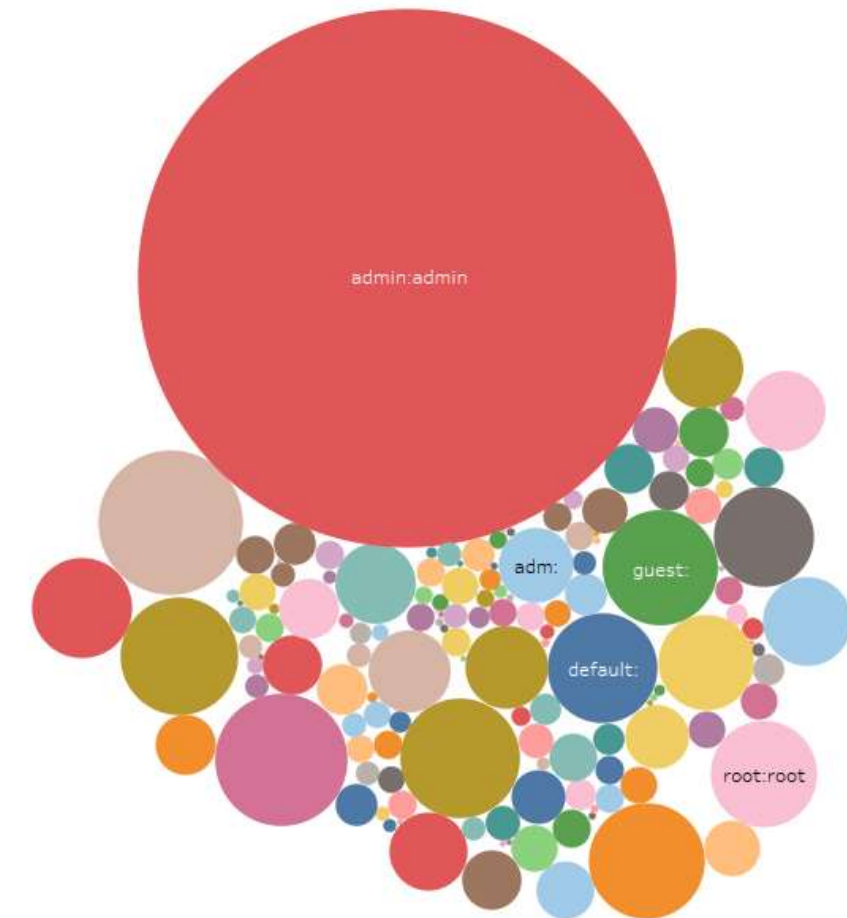
# A volte basterebbe poco

## Username Passwords Used in IOT Devices Visualisation

Recently about 33.000 Username/Password combinations from IOT devices have been released on Pastebin. Read more at: <https://arstechnica.com/information-technology/2017/08/leak-of-1700-valid-passwords-could-make-the-iot-mess-much-worse/>  
Created by @unbehandelt <https://twitter.com/unbehandelt>

Different Username/P..	142
Different Passwords	105
Different Users	19
Different IP	8.233
Number of Records	33.138

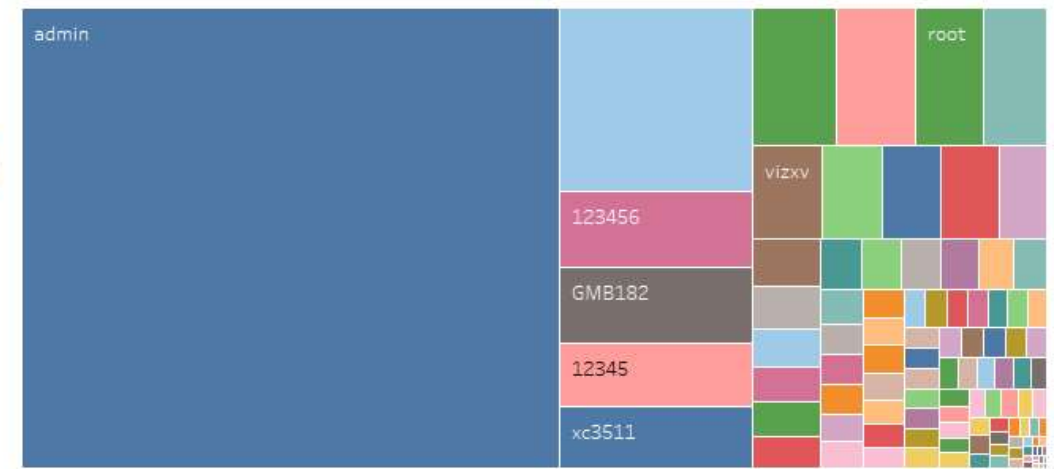
## Different Username/Passwort Combinations Used



## Different Usernames Used



## Different Passwords Used



# L'impatto sul business!

Figura 53 Durata e dimensioni delle interruzioni causate da violazioni della sicurezza

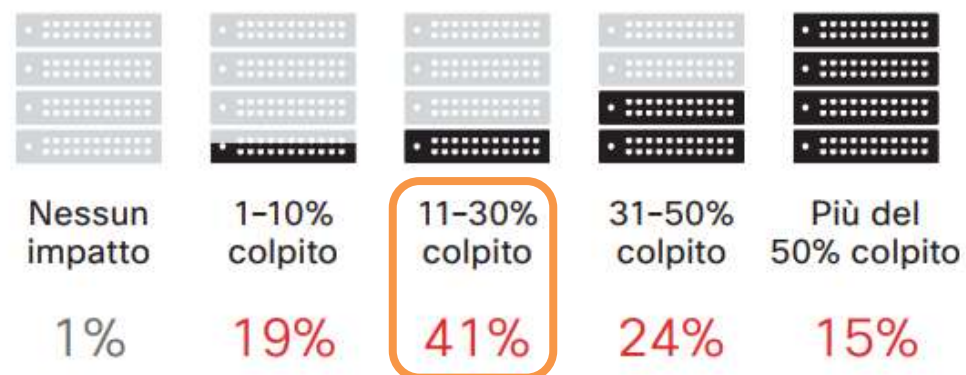
## Durata delle interruzioni dei sistemi aziendali a causa di una violazione

2016 (n=2665)



## Percentuale dei sistemi colpiti a causa di una violazione

2016 (n=2463)



# L'impatto sul business!

Figura 56 Percentuale di opportunità di business perse a causa di un attacco



Figura 58 Percentuale di clienti persi dalle aziende a causa degli attacchi



**42%**  
Ha riscontrato un numero notevole di opportunità perse  
(n=625)

**39%**  
Ha riscontrato una notevole perdita di clienti  
(n=641)



# Le violazioni della sicurezza possono generare dei miglioramenti ...



90%



Afferma che le violazioni della sicurezza hanno favorito il miglioramento delle tecnologie, delle policy o delle procedure di difesa dalle minacce

Esperti della sicurezza (n=1388)

## I 5 miglioramenti principali apportati per proteggere l'azienda dalle violazioni della sicurezza

2016 (n=1375)

38%



Separazione del team di sicurezza dal reparto IT

38%



Maggiore informazione e formazione sulla sicurezza per i dipendenti

37%



Maggiore attenzione all'analisi e alla mitigazione del rischio

37%



Aumento degli investimenti nelle tecnologie o soluzioni di difesa

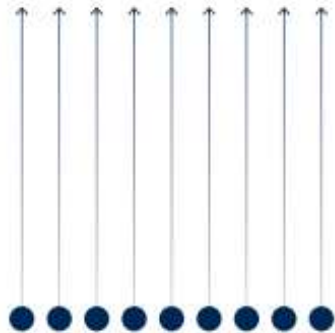
37%



Aumento degli investimenti per la formazione del personale di sicurezza

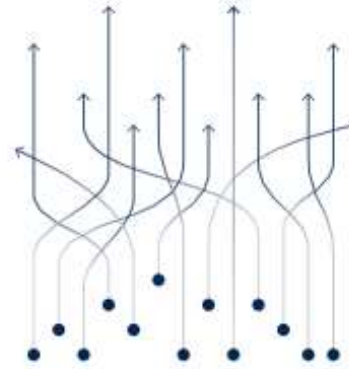
# Cosa ne pensano i CISO

**Figura 45** Percentuali di esperti della sicurezza che giudicano diversi strumenti di sicurezza estremamente efficaci



74%

Ritiene di disporre di strumenti molto o estremamente efficaci contro minacce alla sicurezza note



71%

Ritiene di disporre di strumenti molto o estremamente efficaci nel rilevare le anomalie di rete e nel difendere dinamicamente dalle variazioni delle minacce adattive

2016 (n=2912)

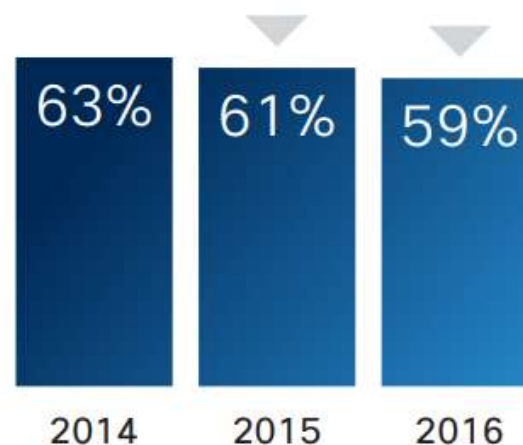


# La sfida sta nell'ottenere il sostegno del management per adottare risposte efficaci

Figura 46 Percentuali di esperti della sicurezza che ritengono che la sicurezza sia di massima priorità a livello dirigenziale, 2014-2016



Ampio accordo sul fatto che la sicurezza costituisca una priorità importante per i dirigenti dell'azienda

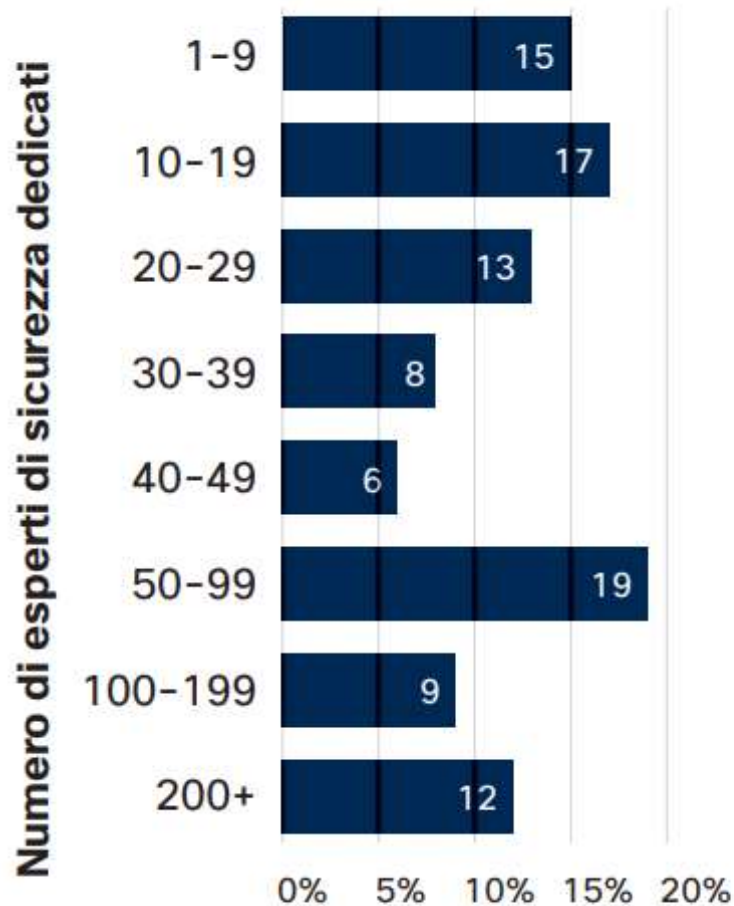


Ampio accordo sul fatto che i ruoli e le responsabilità di sicurezza siano chiaramente definiti all'interno del team di dirigenti dell'azienda



# Le grandi aziende si sono strutturate, #1

Figura 48 Numero di esperti della sicurezza assunti dalle aziende



Percentuale di aziende nel 2016



Numero medio di esperti dedicati alla sicurezza

# Le grandi aziende si sono strutturate, #2

LinkedIn search results for 'security' in Italy. The search bar shows 'security' and the location filter is set to 'Italy'. The results list three profiles:

- Renzo Mosca** • 2nd Information Technology & Security, Italy. Current: Head of IT Security at AgustaWestland. 48 shared connections.
- Nazzareno Guerra** • 2nd Cyber Security Engineer, Italy. Current: Cyber Security Engineer at Finmeccanica. 40 shared connections.
- Graziano Sommariva** • 2nd Network & Security Engineer, Genoa Area, Italy. Current: Networking & Security Expert at Leonardo. 33 shared connections.

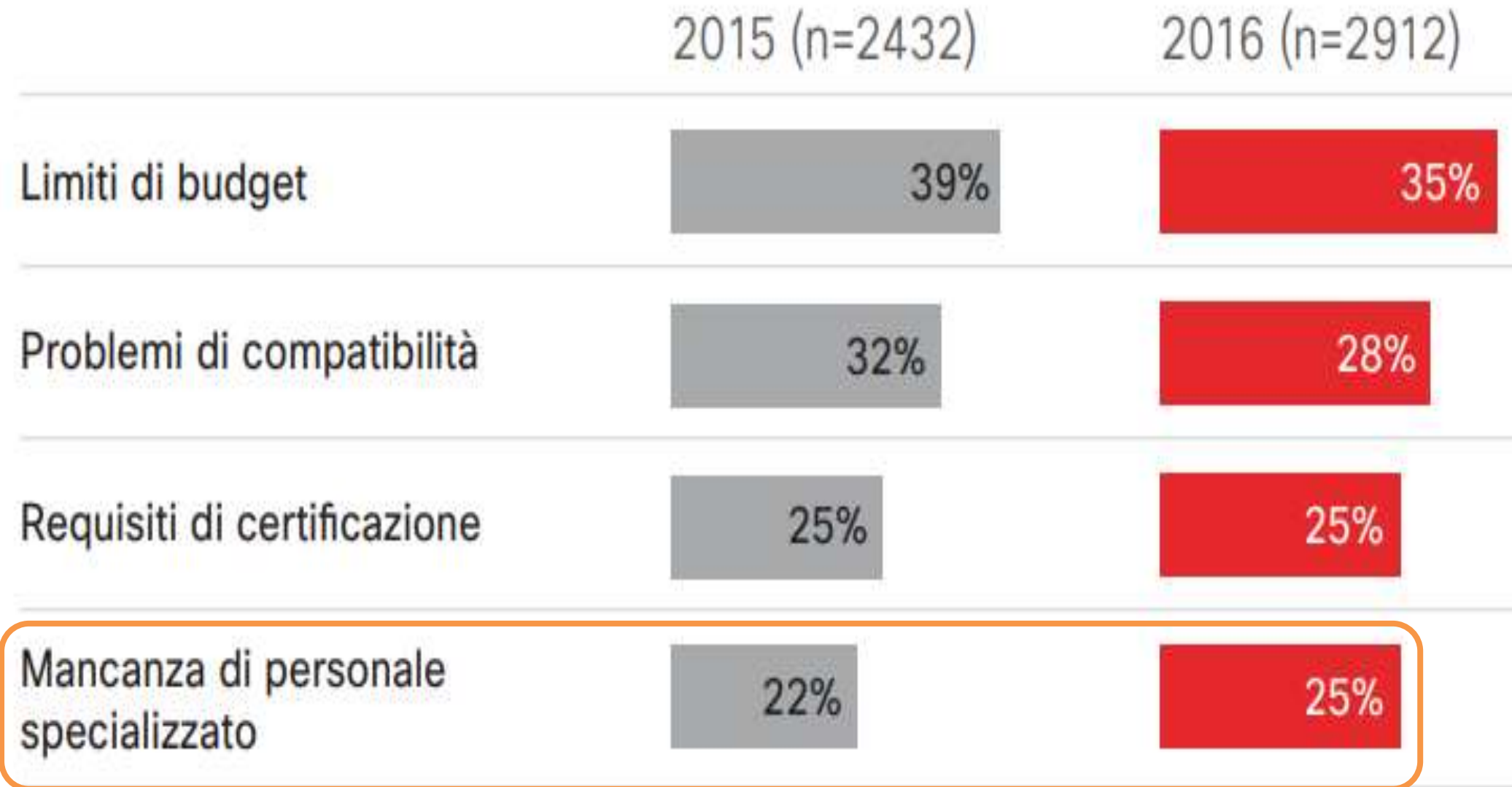
Each profile has a 'Connect' button. A red box highlights 'Showing 1,237 results'.

LinkedIn search results for 'security' in Italy, filtered by company 'Leonardo'. The search bar shows 'security' and the location filter is set to 'Italy'. The results list three profiles:

- Federico Ferro** • 2nd Information Security at Generali, Milan Area, Italy. 43 shared connections.
- Giuliano Merlo** • 2nd Security Advisor, Milan Area, Italy. Current: Head of IT Risk and Security at Generali. 203 shared connections.
- Paolo Guaschi** • 2nd Head of Information Security presso Generali, Milan Area, Italy. Current: Head of Information Security at Generali. 61 shared connections.

Each profile has a 'Connect' button. A red box highlights 'Showing 51 results'.

# Limiti di tempo, risorse qualificate e fondi incidono sulla capacità di rispondere alle minacce



# La «brutta bestia»: lo skill gap

## Growing skill gap



**Only 1 in 10**  
organizations has all the skills  
it needs to be successful



**Roughly 3 out of 4**  
students and educators report  
a moderate to major gap in their  
ability to meet the skill needs  
of the IT workforce

# La «brutta bestia» #2: il cybersecurity skill gap

## [WeLiveSecurity] Cybersecurity skills gap: It's big and it's bad for security

January 25, 2017 / Cybersecurity, Management, Recruiting, Technology, Top News

✓ Like 26
Share 26
in Share
Tweet

**We have great expertise in supporting companies and candidates in their social recruiting and talent hunting journey, alleviating the "skill gap" issue. Our capabilities and problem-solving approach are proven by the appreciation of our many customers. Let's have a talk!**

On this subject, here is an **article about the cybersecurity skill gap**: The cybersecurity skills gap, defined as a shortage of qualified people needed to fill open positions in IT security, is a phenomenon that I have researched quite extensively this year, and with good reason. You may have seen this recent headline:

"Donald Trump Advised to Train 100,000 Hackers to Protect the US"

I don't like the way that headline was worded, but I'm in agreement with the underlying point: the US President's Commission on Enhancing National Cybersecurity has strongly recommended that the country "should increase ... efforts on training security experts that would work for the country and not leave for the private sector, which has become a dramatic problem in the last few years" (Softpedia). And you may have seen other headlines, like this one from Forbes at the start of this year: "One Million Cybersecurity Job Openings In 2016". This is a problem that is negatively impacting governments, companies, non-profits, and even consumers (inadequate IT security staffing can lead to data breaches that expose your information).

**Describe your organization's experience when it comes to hiring people for the cybersecurity roles it needs to fill?**




- Very difficult
- Moderately difficult
- Moderately easy

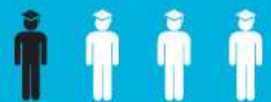
### Yes, the cybersecurity skills gap is *that* big

Having studied the numbers from multiple perspectives, I agree that the world is probably in need of one million more people with cybersecurity skills than are currently available to hire. The US alone needs something like 200,000 more people skilled in cybersecurity, and it's not talking about the people that IT security managers want to

#### Growing skill gap



**Only 1 in 10** organizations has all the skills it needs to be successful



**Roughly 3 out of 4** students and educators report a moderate to major gap in their ability to meet the skill needs of the IT workforce



# La Cybersecurity è un'opportunità di business?



# Sicuramente lo è per i criminali!



# Le aziende cercano risorse qualificate in **outsourcing**, per sfruttare competenze non reperibili internamente, #1

Figura 60 Le aziende si affidano all'esternalizzazione



## Servizi di sicurezza esternalizzati

2016 (n=2912)



Consulenza

51%



Reazione agli incidenti

45%

## Motivo per cui i servizi vengono esternalizzati

2016 (n=2631)



Avere una maggiore efficienza dei costi

52%

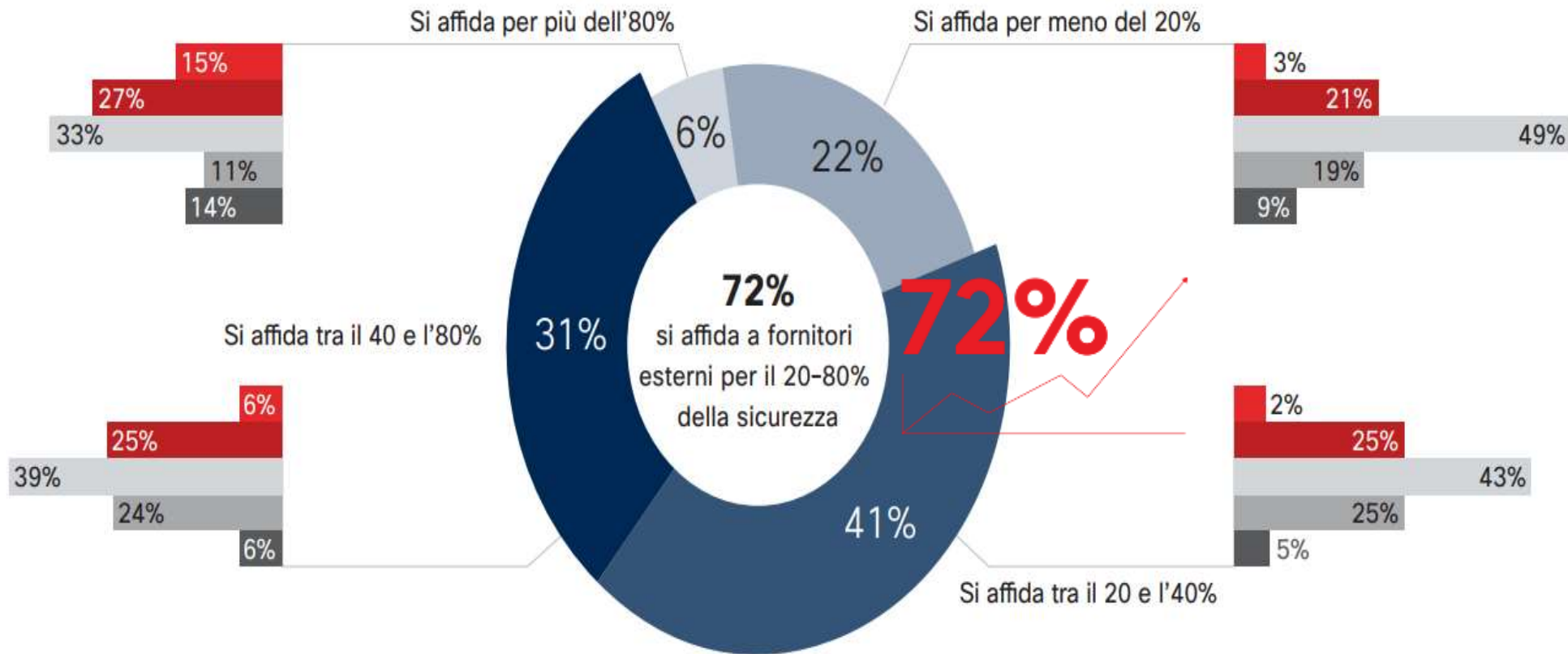


Ottenere analisi imparziali

48%

# Le aziende cercano risorse qualificate in **outsourcing**, per sfruttare competenze non reperibili internamente, #2

Personale addetto alla sicurezza IT (n=2595)



## Cambiamento nell'utilizzo dell'esternalizzazione nel corso del prossimo anno

Personale addetto alla sicurezza IT che si affida a fornitori terzi (n=2504)

■ Riduzione significativa
■ Riduzione lieve
■ Nessuna modifica
■ Aumento lieve
■ Aumento significativo

# CONCLUSIONS

---

A .

B .

C .



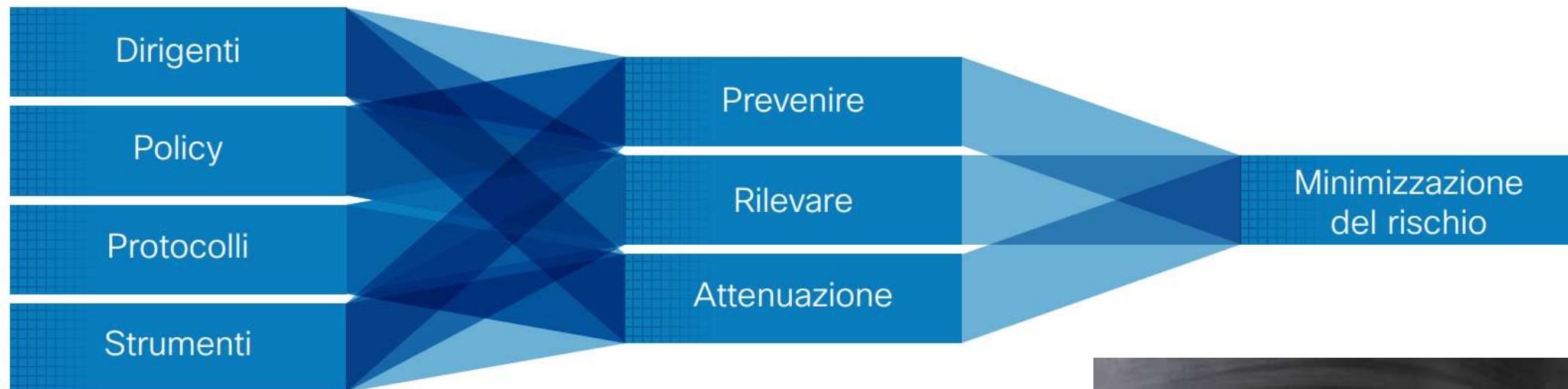
# Fattori determinanti e misure di sicurezza per ridurre i rischi

## Fattori

Misurano l'influenza di policy, dirigenti, protocolli e strumenti in relazione alla capacità dell'azienda di prevenire, rilevare e mitigare gli effetti di una violazione

## Misure di sicurezza

Misurano l'influenza della capacità dell'azienda di prevenire, rilevare e mitigare gli effetti di una violazione a rischio



# CONCLUSIONS

---

A

B

C

- Le minacce sono reali e potenzialmente dirompenti
- Gli strumenti ci sono
- Le competenze ci sono (poche, quindi da cercare e formare)
- La cybersecurity sarà sempre un tema di attualità (e di business)

**Grazie e restiamo in contatto**  
**([www.primobonacina.com/](http://www.primobonacina.com/))**



## **Primo Bonacina**

*Managing Partner, PBS - Primo Bonacina Services*

Phone: +39 334 6381071

[primo.bonacina@primobonacina.com](mailto:primo.bonacina@primobonacina.com)

Skype: primo.bonacina

[www.primobonacina.com](http://www.primobonacina.com)

**Primo Bonacina Services di Primo Ernesto Bonacina**

**Via Canneto, 10 - 25049 Iseo (BS) Italy - VAT id: IT04001550161**