Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

OTTOBRE 2025

DATI ED INDICATORI DELLA MINACCIA CYBER IN ITALIA

Servizio Operazioni
e gestione delle crisi cyber

TLP:CLEAR

INTRODUZIONE

Il presente documento riporta su base mensile alcuni numeri e indicatori derivanti dalle attività operative dell'Agenzia per la Cybersicurezza Nazionale, utili per caratterizzare lo stato della minaccia cyber in Italia. In particolare, il CSIRT Italia, articolazione tecnico-operativa dell'Agenzia, è hub nazionale delle notifiche obbligatorie e volontarie di incidenti previste per legge (Perimetro di Sicurezza Nazionale Cibernetica, Legge 28 giugno 2024, n. 90, Direttiva NIS) e riceve altresì informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali ed internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni dotano l'Agenzia di un ampio cono di visibilità sullo stato della minaccia cyber a danno del sistema Paese e forniscono, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali. Tutte le informazioni vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di triage le analizzano e classificano come eventi cyber; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento, come:

- **approfondire le informazioni** a disposizione, analizzando i contenuti anche dal punto vista strettamente tecnico, quale lo studio dei malware, valutando il rischio d'impatto sistemico di vulnerabilità e incidenti;
- **se necessario inviare richieste di informazioni** ai soggetti;
- **fornire supporto da remoto o in loco** ai soggetti impattati;
- **inviare comunicazioni** ai soggetti impattati oppure a tutti i soggetti potenzialmente impattati;
- **pubblicare alert o bollettini**.

Per le definizioni si rimanda al Glossario del CSIRT Italia e alla Tassonomia Cyber dell'ACN.

Le informazioni contenute in questo documento sono il risultato dell'analisi dei dati disponibili al momento della redazione; esse potrebbero essere aggiornate a seguito di nuove evidenze o di ulteriori approfondimenti.

Indice

1 EXECUTIVE SUMMARY

- Nel mese di ottobre 2025 sono stati registrati **267 eventi**, in **equilibrio** rispetto ai **270** di settembre, mentre il numero di **incidenti** (**51**) è in **diminuzione** del 9% rispetto al mese precedente.
- I settori con il maggior numero di vittime di eventi cyber registrate nel mese sono stati: **Pubblica amministrazione locale**, **Pubblica amministrazione centrale** e **Telecomunicazioni**.
- Nel mese di ottobre, l'attività riconducibile a gruppi **hacktivisti** si conferma su livelli sostanzialmente analoghi a quelli del mese precedente, con la prosecuzione di attacchi DDoS legati al contesto del conflitto russo-ucraino. I settori maggiormente interessati sono risultati quelli della Pubblica amministrazione, sia centrale che locale, delle telecomunicazioni e dei trasporti. **L'impatto operativo di tali attacchi è, come di consueto, molto limitato: in questo mese solo il 4% degli eventi DDoS ha generato brevi indisponibilità dei servizi, senza conseguenze significative sull'operatività dei siti web interessati**. All'interno dello stesso quadro, sono state rilevate rivendicazioni, sempre da parte di hacktivisti filorussi, di compromissioni di interfacce di sistemi **SCADA**, riferibili a piccole imprese del comparto manifatturiero. I soggetti potenzialmente coinvolti sono stati tempestivamente informati, per consentire le necessarie verifiche tecniche e l'adozione delle eventuali misure di mitigazione.
- Nell'ambito dell'attività di monitoraggio della superficie esposta dei soggetti italiani sono state inviate **1.299 comunicazioni** di allertamento a pubbliche amministrazioni e imprese che esponevano su Internet **3.836 servizi a rischio**. Sempre nell'ambito delle attività di monitoraggio proattivo, rilevante quella svolta a seguito delle nuove vulnerabilità dei prodotti **F5**, soluzioni ampiamente utilizzate per la gestione, il bilanciamento e la sicurezza del traffico applicativo nelle infrastrutture di rete. Lo sfruttamento di tali vulnerabilità avrebbe consentito a un attore malevolo di causare **Denial of Service**, di **eseguire codice arbitrario sui sistemi interessati** e di fare **Priviledge Escalation**. Pertanto, CSIRT Italia ha avviato il rilevamento dei servizi potenzialmente vulnerabili esposti sullo spazio di indirizzamento italiano ed inviato comunicazioni dirette ai soggetti potenzialemente vulnerabili al fine di favorire la tempestiva adozione degli interventi risolutivi (ex Articolo 2, comma 1 della legge 28 giugno 2024, n. 90).
- A ottobre 2025 si conferma la tendenza, già osservata

nei mesi precedenti, relativa all'**esposizione online di dati**, che ha interessato in misura prevalente i settori della Pubblica Amministrazione, telecomunicazioni e servizi finanziari. Le attività di monitoraggio hanno permesso di individuare e segnalare quanto rinvenuto su diverse piattaforme di scambio e vendita di dati, dataset e credenziali compromesse, solitamente acquisite attraverso infezioni da malware di tipo *infostealer*.

- I **vettori di attacco** maggiormente rilevati ad ottobre 2025 sono stati le e-mail, l'utilizzo di account validi e l'abuso di funzionalità[1].
- Sono state pubblicate **4.384** nuove CVE, in **diminuzione** rispetto a settembre (**–131**).
- Le **comunicazioni dirette**, effettuate dal CSIRT Italia per segnalare potenziali compromissioni o fattori di rischio ad amministrazioni ed imprese italiane, nel mese di ottobre 2025 sono state **4.367**, in **diminuzione** rispetto a settembre.

[1] Utilizzo improprio o non previsto di funzioni legittime di un sistema, servizio o protocollo per eludere i controlli di sicurezza o ampliare i privilegi di accesso, senza sfruttare vulnerabilità note.

I NUMERI DI OTTOBRE 2025

Figura 1 - *indicatori delle attività operative ad ottobre 2025 e nei sei mesi precedenti*

- **267** eventi cyber, **stabile** (**–3**);
- **327** vittime, in **aumento** (**+71**);
- **169** vittime della constituency[2], in **aumento** (**+49**);
- **51** incidenti con impatto confermato, in **diminuzione** (**–5**);
- **0** asset potenzialmente compromessi, in **diminuzione** (**–1.183**);
- **3.836** asset potenzialmente vulnerabili, in **aumento** (**+2.313**);
- **80** alert sul sito web del CSIRT Italia, in **aumento** (**+9**);
- **4.367** comunicazioni inviate, in **diminuzione** (**–20**);
- **4.384** nuove CVE, in **diminuzione** (**–131**).

[2]La constituency è l'insieme dei soggetti che operano nei settori NIS, Perimetro, Telco o nella Pubblica amministrazione, nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli eventi cibernetici. Sul sito ACN è disponibile un documento di approfondimento sulla constituency del CSIRT Italia.

PRODOTTI VULNERABILI

Di seguito **l'elenco dei prodotti** che ad ottobre 2025 sono stati oggetto di specifici alert pubblicati sul sito web del CSIRT Italia a causa di vulnerabilità. Tali vulnerabilità, oggetto di alert o perché di recente scoperta oppure perché ne è stato rilevato lo sfruttamento, **richiedono l'adozione tempestiva di aggiornamenti di sicurezza** o delle misure di mitigazione disponibili nell'alert di seguito referenziato.

- **Microsoft Windows Server 2019** (CVE-2025-59287) Link all'alert;
- **ISC BIND 9** (CVE-2025-8677, CVE-2025-40780, CVE-2025-40778) Link all'alert;
- **Gladinet CentreStack and TrioFox** (CVE-2025-11371) Link all'alert;
- **WatchGuard Fireware OS** (CVE-2025-9242) Link all'alert;
- **Oracle Concurrent Processing** (CVE-2025-61882) Link all'alert;
- **F5 F5OS e BIG-IP** (CVE-2025-53521, CVE-2025-53474, CVE-2025-48008, CVE-2025-46706 e CVE-2025-41430) Link all'alert;
- **Apache Tomcat** (CVE-2025-55752 e CVE-2025-55574) Link all'alert;
- **Zimbra Collaboration Suite** (CVE-2025-62763) Link all'alert;
- **ISC BIND** (CVE-2025-40778) Link all'alert;
- **Libraesva Email Security Gateway** (CVE-2025-59689) Link all'alert;
- **Squid** (CVE-2025-62168) Link all'alert;
- **SAP Netweaver** (CVE-2025-42944) Link all'alert;
- **TP-Link Gateway Omada** (CVE-2025-7851, CVE-2025-7850, CVE-2025-6542 e CVE-2025-6541) Link all'alert;
- **Telerik UI** (CVE-2025-3600) Link all'alert;
- **Nagios Log Server** (CVE-2025-44824 e CVE-2025-44823) Link all'alert;
- **Microsoft ASP.NET Core 8.0** (CVE-2025-55315) Link all'alert;
- **Ivanti Connect Secure** (CVE-2025-22457) Link all'alert;
- **Microsoft Windows Server Update Service** (CVE-2025-59287) Link all'alert;
- **Atlassian Jira** (CVE-2025-22167) Link all'alert;
- **Mattermost** (CVE-2025-58075 e CVE-2025-58073) Link all'alert;
- **Veeam Backup & Replication** (CVE-2025-48984 e CVE-2025-48983) Link all'alert;
- **DNN** (CVE-2025-64095) Link all'alert;
- **Redis** (CVE-2025-49844) Link all'alert;
- **Adobe Commerce/Magento** (CVE-2025-54236) Link all'alert;
- **Netbird** (CVE-2025-10678) Link all'alert;
- **FlowiseAI** (CVE-2025-61913) Link all'alert;
- **Gladinet CentreStack e TrioFox** (CVE-2025-11371) Link all'alert;
- **Fortinet FortiSwitchManager** (CVE-2025-49201) Link all'alert;
- **Oracle E-Business Suite** (CVE-2025-61884, CVE-2025-62481 e CVE-2025-53072) Link all'alert; Link all'alert;
- **VMware Aria Operations** (CVE-2025-41244) Link all'alert;
- **Ivanti Endpoint Manager** (CVE-2025-9713 e CVE-2025-11622) Link all'alert;

Maggiori dettagli nelle sezioni 3 e 5.

2 EVENTI ED INCIDENTI

Ad ottobre 2025 sono stati individuati **267** eventi cyber, in **equilibrio** rispetto al mese precedente. Questi ultimi hanno **interessato 241 soggetti nazionali**: 169 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 267 eventi cyber, **51 sono stati classificati quali incidenti**, in **diminuzione** del 9% rispetto a settembre.

La Figura 2 mostra l'andamento di eventi e incidenti fino al mese in esame, corredato da una previsione, basata sull'analisi dei dati precedenti[3], riferita ai successivi 3 mesi.

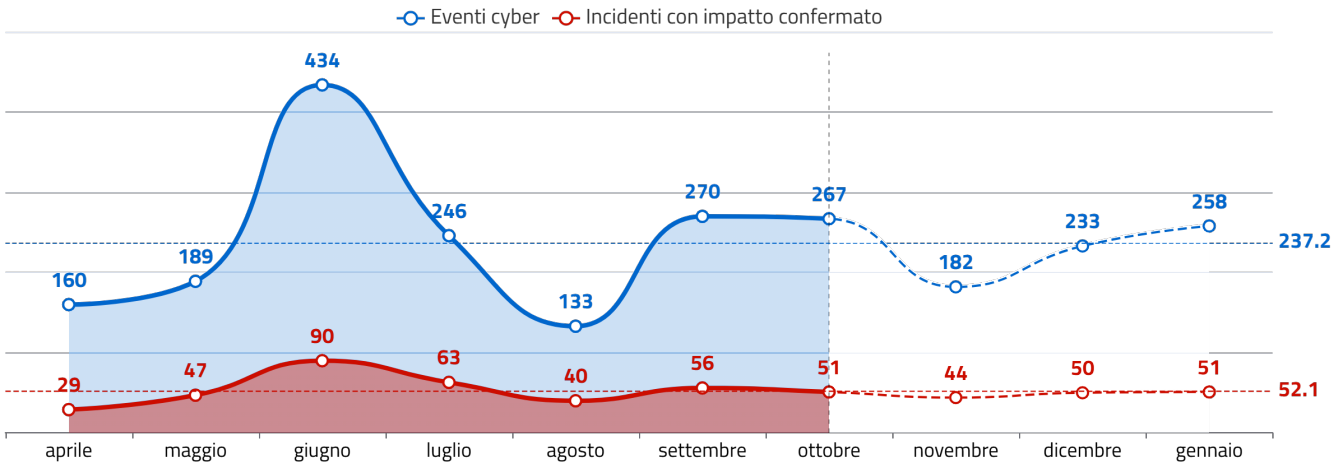

Figura 2 - *andamento attività reattive e analisi previsionale*

[3] La previsione dà un'idea generale degli andamenti futuri utilizzando un modello ARIMA (AutoRegressive Integrated Moving Average). È importante sottolineare che la previsione non può essere accurata in quanto il manifestarsi degli eventi dipende da molti fattori, tra i quali quelli di natura geopolitica, la scoperta di nuove vulnerabilità, la capacità degli attaccanti e così via.

2.1 Settori impattati

In figura 3 si riporta il numero di vittime di eventi per settore impattato[4]. Si evidenza altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico).

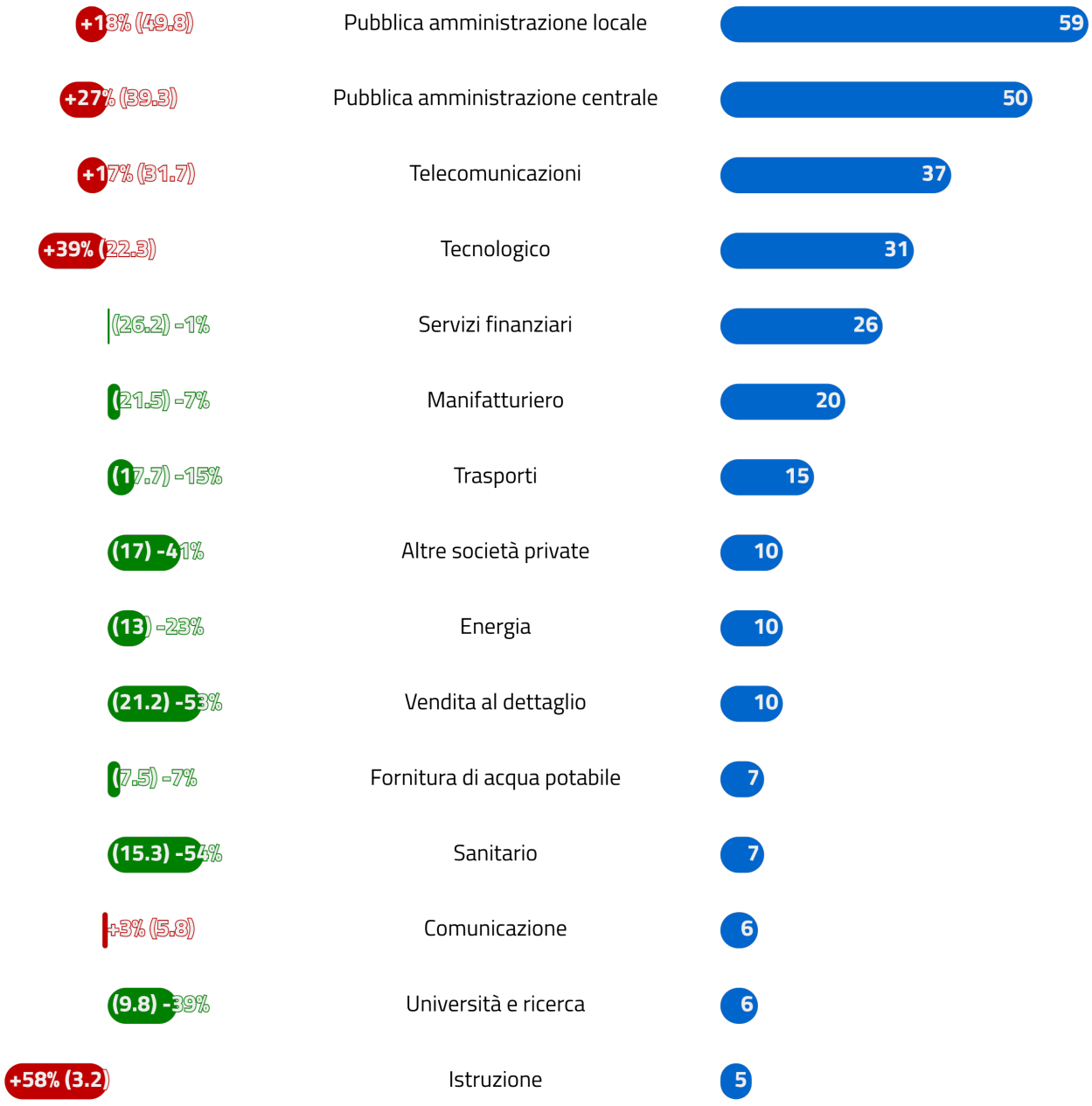

Figura 3 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente (top 15)*

[4] Si noti che ogni evento può avere più vittime afferenti ad uno o più settori di attività e che una vittima può operare in più settori. Talvolta non è possibile associare un evento ad una vittima e la vittima ad un settore.

2.2 Tipologia di minacce negli eventi

In Figura 4 si riporta il numero di minacce rilevate negli eventi[5] e la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico).
Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn).

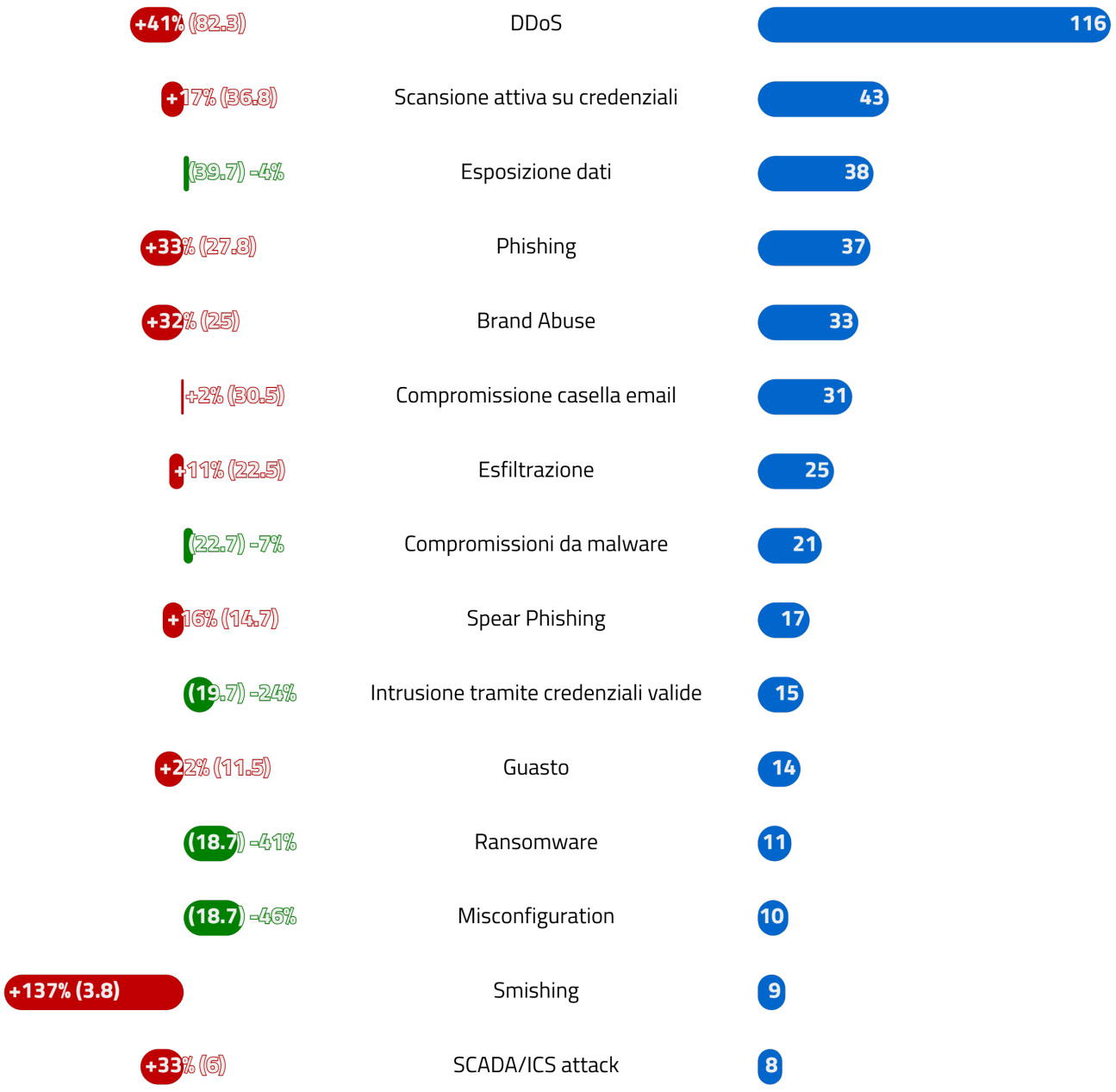

Figura 4 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al semestre precedente (top 15)*

[5] Si noti che ognuno degli eventi può essere stato associato ad una o più tipologia di minacce.

2.3 Distribuzione delle minacce per settore

In Figura 5 si riporta, per ogni settore, il numero di vittime che hanno subito la minaccia specificata, ottenuto analizzando gli eventi di ottobre 2025. Si ricorda che ad un evento possono essere associate più minacce e più vittime. Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn). In Figura sono mostrati solo i 15 settori più interessati dalle minacce.

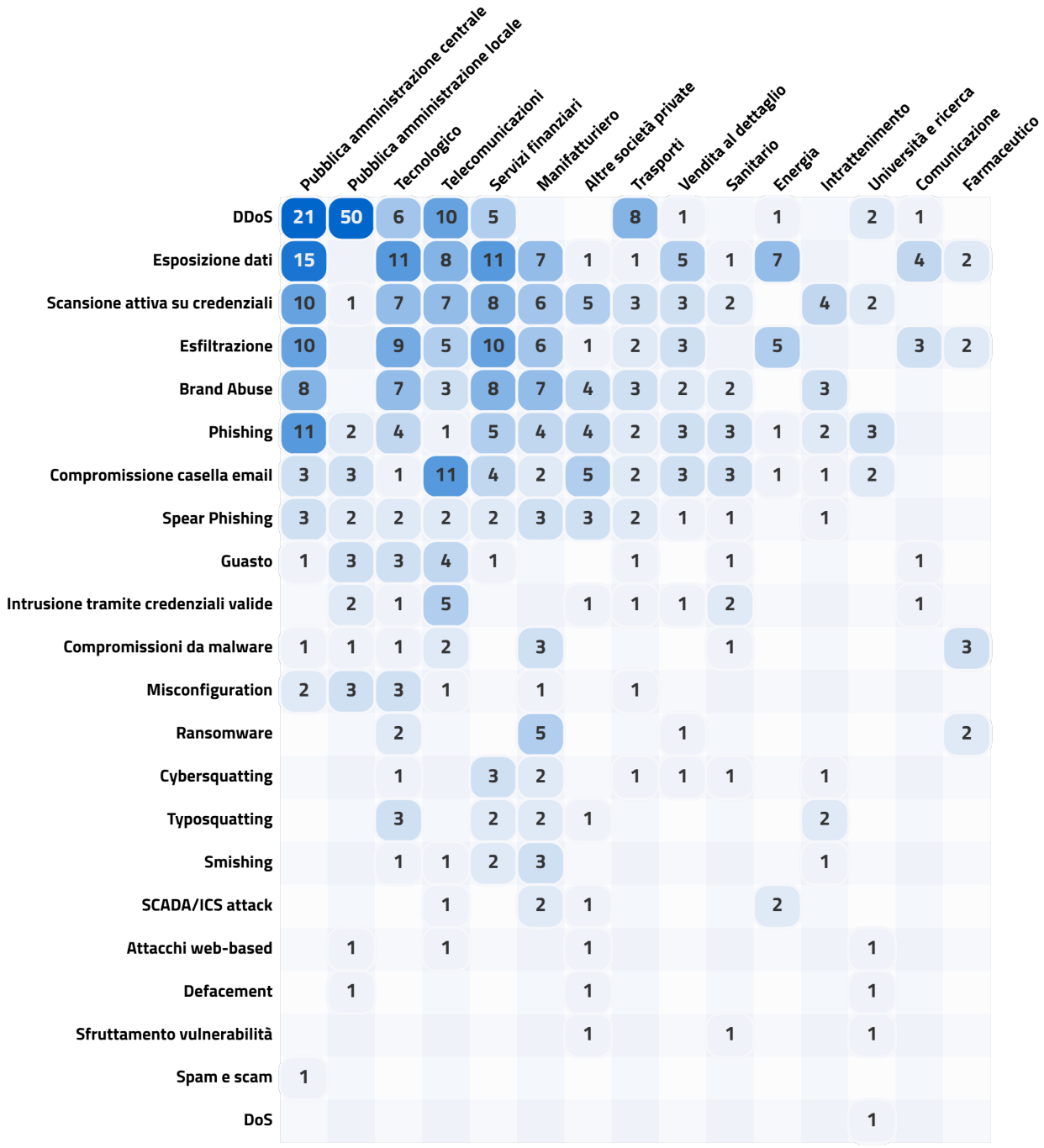

Figura 5 - *numero di vittime per settore e tipologia di minacce*

2.4 Distribuzione geografica delle vittime

I 267 eventi cyber hanno interessato **327** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

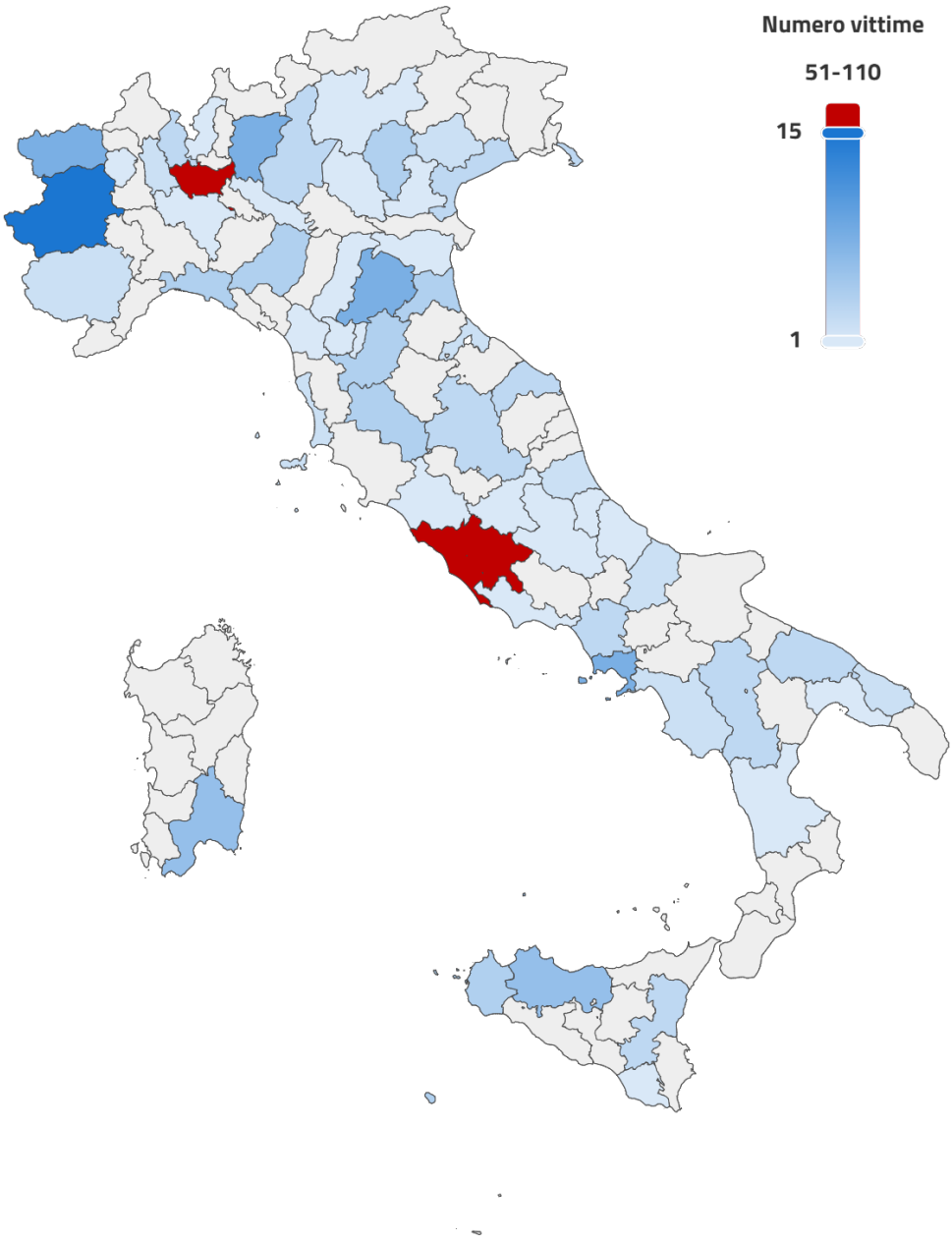

Figura 6 - *distribuzione delle vittime degli eventi cyber*

3 VULNERABILITÀ

Ad ottobre 2025 sono state pubblicate[6] **4.384** nuove CVE, in **diminuzione** (**–131**) rispetto a settembre. Di queste, **587** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (**+119**), e per **7** CVE è stato rilevato lo sfruttamento attivo, **stabile** (**–2**) rispetto a settembre.

3.1 Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia

Gli alert sulle vulnerabilità oggetto di pubblicazione sul sito del CSIRT Italia sono stati **80**. Oltre al consueto aggiornamento mensile di Microsoft (link) all'alert sul sito web, che ha risolto un totale di 175 nuove vulnerabilità (2 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Microsoft**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-59287 con gravità "critica" – già sanata dal vendor – relativa a Windows Server Update Service (WSUS), servizio di Microsoft che consente agli amministratori di sistema di gestire centralmente la distribuzione degli aggiornamenti software per i prodotti Microsoft all'interno di una rete aziendale. Tale vulnerabilità potrebbe consentire a un utente malevolo non autenticato di eseguire codice arbitrario remoto sui sistemi target (stima di impatto sistemico **79,23/100**). Link all'alert del 25/10/2025;
- **ISC**: aggiornamenti di sicurezza ISC sanano due vulnerabilità con gravità "alta", nel prodotto BIND. Tali vulnerabilità, qualora sfruttate, potrebbero causare la manomissione della cache DNS e/o la compromissione della disponibilità del servizio (stima di impatto sistemico **77,69/100**). Link all'alert del 22/10/2025;
- **Gladinet**: ricercatori di sicurezza hanno rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-11371 che interessa i prodotti Gladinet CentreStack e TrioFox, soluzioni di accesso remoto sicuro ai file server aziendali, progettate per modernizzare la gestione dei file senza richiedere la migrazione al cloud (stima di impatto sistemico **77,05/100**). Link all'alert del 10/10/2025;
- **WatchGuard**: ricercatori di sicurezza hanno recentemente pubblicato un Proof of Concept (PoC) per la CVE-2025-9242, che interessa i firewall WatchGuard Firebox. Qualora sfruttata, tale vulnerabilità potrebbe consentire a un

[6] Dati del National Vulnerability Database `https://nvd.nist.gov/vuln` del NIST. Il database completo delle CVE è pubblicamente accessibile `https://cve.mitre.org/`.

attaccante remoto non autenticato di eseguire codice arbitrario sui sistemi target (stima di impatto sistemico **75,38/100**). Link all'alert del 16/10/2025;

- **Oracle**: a seguito delle indagini avviate da Oracle in merito a presunte attività malevole mirate a istanze di E-Business Suite esposte su Internet, il vendor ha recentemente individuato una vulnerabilità, con gravità "critica", di tipo zero-day che, qualora sfruttata, potrebbe consentire l'esecuzione di codice arbitrario sui sistemi target (stima di impatto sistemico **75,12/100**). Link all'alert del 05/10/2025;

All'indirizzo https://www.acn.gov.it/portale/csirt-italia/alert-e-bollettini è possibile accedere a tutti gli altri alert pubblicati.

3.2 Distribuzione delle vulnerabilità sui vendor

In Figura 7 è riportato il numero delle vulnerabilità rilevate distribuite tra i principali vendor[7].

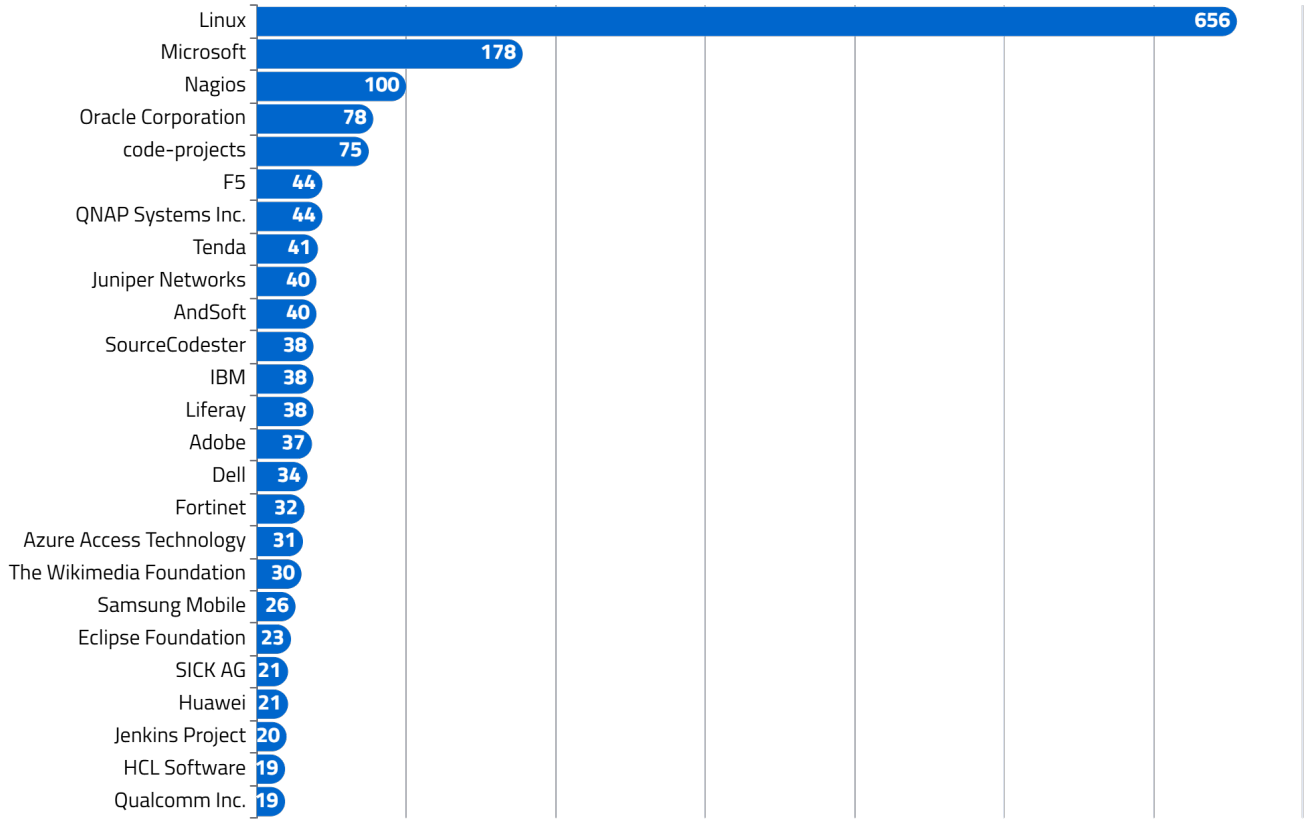

Figura 7 - *top 25 produttori affetti da vulnerabilità nel mese*

[7] I valori attribuiti alla voce *Linux* si riferiscono esclusivamente alle vulnerabilità registrate dalla CVE Numbering Authority (CNA) https://kernel.org/ e afferiscono dunque unicamente al kernel Linux. Maggiori informazioni a questo link: https://www.cve.org/PartnerInformation/ListofPartners/partner/Linux

In Figura 8 è riportato, invece, il numero delle vulnerabilità rilevate distribuite tra i principali prodotti.

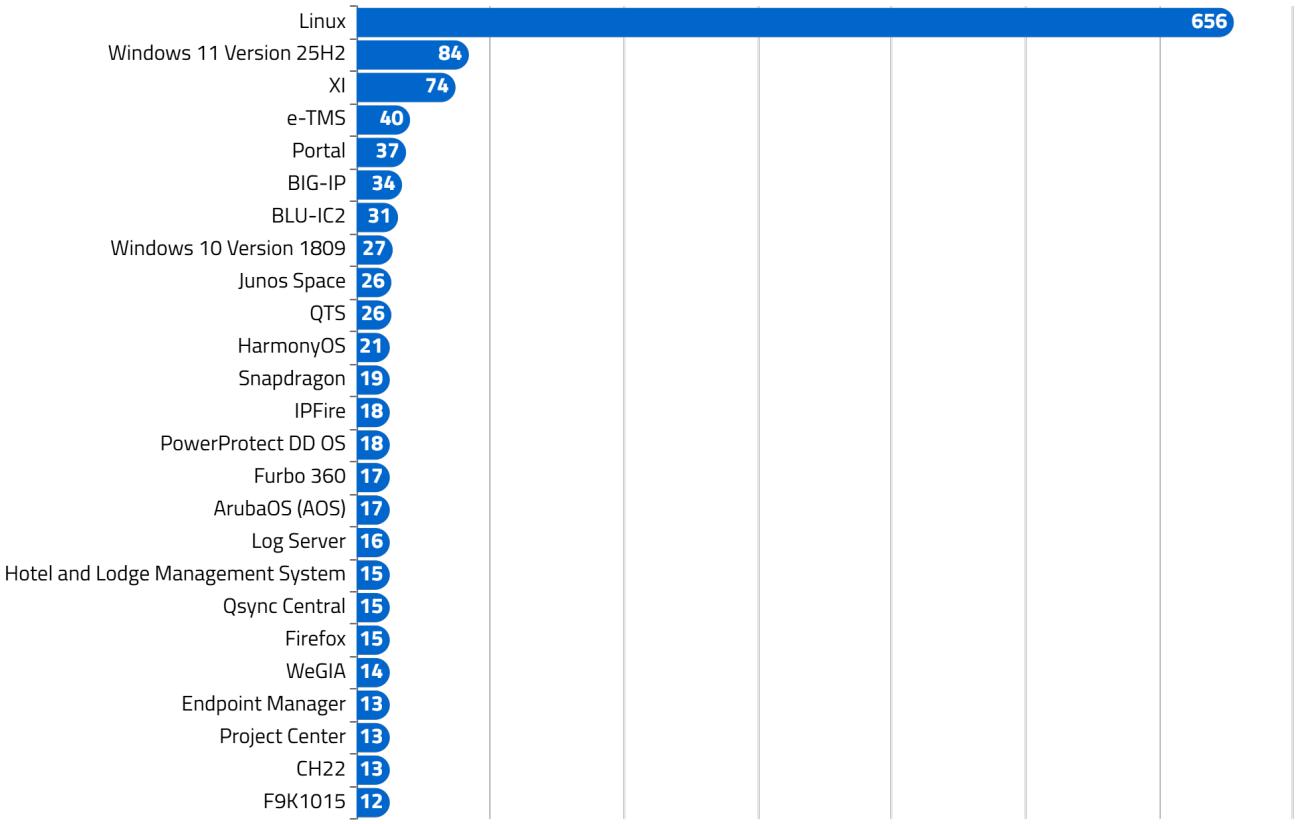

Figura 8 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

In Figura 9 sono riportate le 5 tipologie di weakness (Common Weakness Enumeration – CWE) più rilevate.

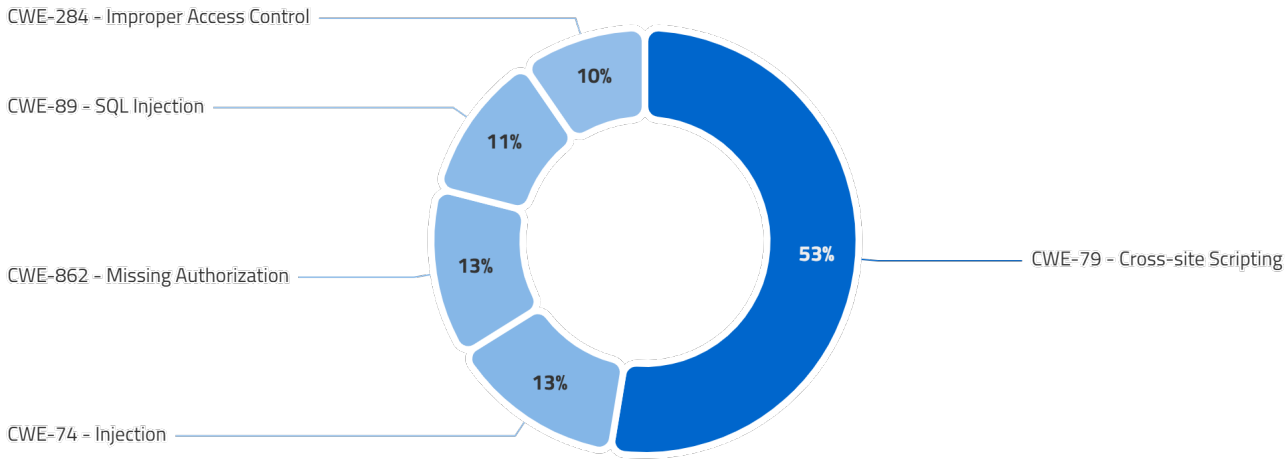

Figura 9 - *top 5 CWE nel mese*

3.4 Vulnerabilità con maggior probabilità di sfruttamento

Di seguito il dettaglio delle 3 vulnerabilità che potrebbero subire il maggior incremento nel trend di exploitation, ottenuto monitorando l'Exploit Prediction Scoring System (EPSS)[8] fornito dal FIRST nel mese in esame.

Vendor	**Kentico**
Prodotti e versioni vulnerabili	**Xperience tutte le versioni fino alla 13.0.178**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante di eludere i controlli d'accesso.**
Data di rilascio CVE	**17/03/2025 modificata il 27/10/2025**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.85**

Tabella 1 - *CVE-2025-2747*

Vendor	**Oracle**
Prodotti e versioni vulnerabili	**Oracle E-Business Suite (component: BI Publisher Integration) versioni dalla 12.2.3 alla 12.2.14**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo da remoto**
Data di rilascio CVE	**05/10/2025 modificata il 27/10/2025**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.85**

Tabella 2 - *CVE-2025-61882*

[8] `https://www.first.org/epss/` fornisce un'indicazione della probabilità che una vulnerabilità venga sfruttata, è un valore aggiornato quotidianamente dal FIRST.

Vendor	**Adobe**
Prodotti e versioni vulnerabili	**Adobe Commerce versioni:** ▪ **2.4.9-alpha2 e precedenti,** ▪ **2.4.8-p2 e precedenti,** ▪ **2.4.7-p7 e precedenti,** ▪ **2.4.6-p12 e precedenti,** ▪ **2.4.5-p14 e precedenti,** ▪ **2.4.4-p15 e precedenti.**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette da remoto ad un attaccante non autenticato di eseguire codice malevolo da remoto**
Data di rilascio CVE	**09/09/2025 modificata il 02/11/2025**
CVSS score 3.0	**9.1 Critical**
EPSS max score	**0.63**

Tabella 3 - *CVE-2025-54236*

4 MINACCIA

In questa sezione si riporta un dettaglio sulle minacce ransomware e DDoS, anche in termini di rivendicazioni effettuate dai gruppi hacker in Italia ed UE, mentre per il malware uno spaccato sul numero degli IoC[9] condivisi dal CSIRT Italia tramite piattaforma MISP[10], in modo da caratterizzarne le tipologie più frequenti.

4.1 Ransomware: distribuzione delle vittime

Ad ottobre 2025, nessun attacco ransomware ha colpito soggetti critici, mentre il 9% ha colpito soggetti a media criticità ed il restante 91% ha coinvolto altri soggetti a criticità minore. Questo conferma la preferenza di questa tipologia di attaccanti a colpire obiettivi meno strutturati e dotati di limitate capacità di cybersicurezza.

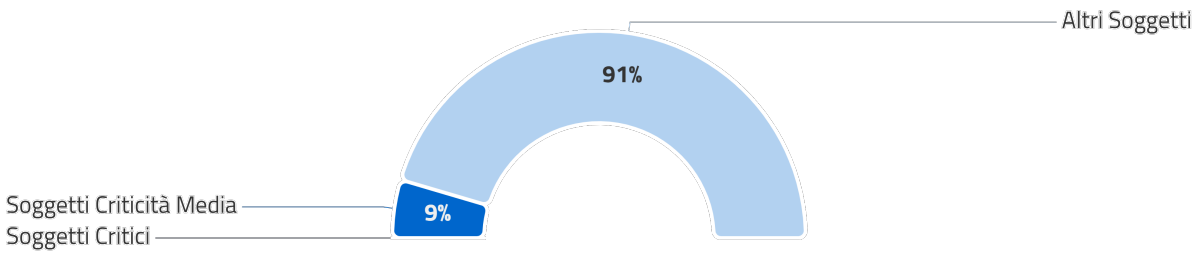

Figura 10 - *distribuzione delle vittime di ransomware in base alla loro criticità*

[9] IoC (Indicatore di Compromissione), indica la possibile presenza di un'attività malevola o un'intrusione nel sistema informatico. Gli IoC sono prove che gli analisti di sicurezza informatica utilizzano per identificare, rilevare e rispondere a una compromissione.

[10] MISP (Malware Information Sharing Platform) è una soluzione software open source per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di sicurezza informatica e minacce cyber.

4.2 Rivendicazioni ransomware

Il monitoraggio di fonti aperte nel mese di ottobre 2025 ha permesso di individuare **8** rivendicazioni di attacchi ransomware a danno di soggetti italiani[11].

Il grafico in Figura 11 mostra l'andamento delle rivendicazioni nel corso degli ultimi 12 mesi.

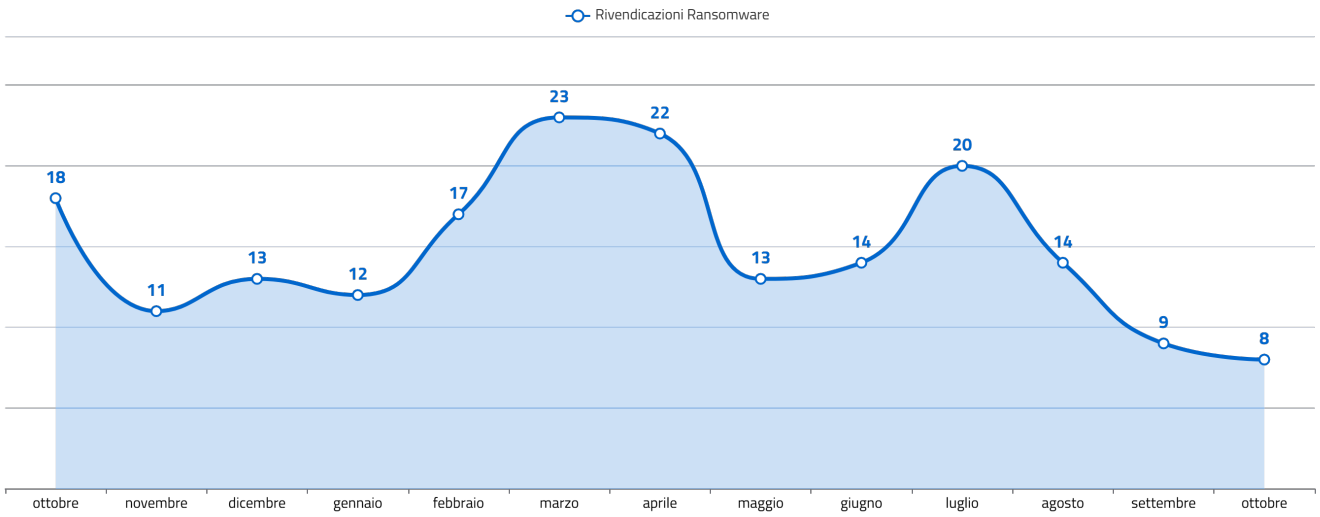

Figura 11 - *andamento delle rivendicazioni Ransomware*

Il grafico in Figura 12 mostra i gruppi più attivi in termini di rivendicazioni in Italia.

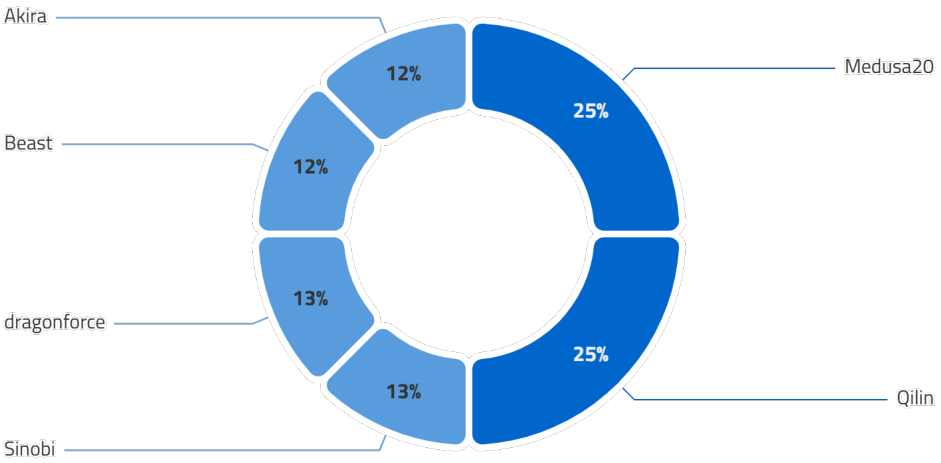

Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

[11] Talvolta, le rivendicazioni relative ad attacchi ransomware non sono confermate dal soggetto coinvolto.

4.3 Rivendicazioni DDoS

A ottobre 2025 sono state individuate[12] **79** rivendicazioni di attacchi DDoS in danno di soggetti italiani.

Il grafico in Figura 13 mostra l'andamento delle rivendicazioni DDoS nel corso degli ultimi 12 mesi.

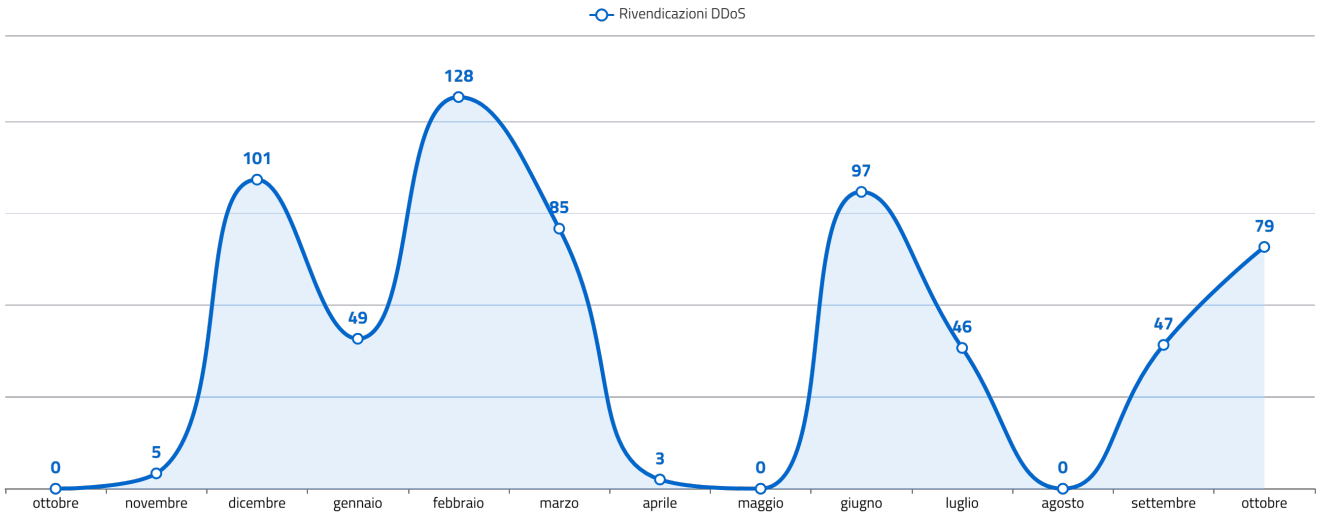

Figura 13 - *andamento delle rivendicazioni DDoS*

Il grafico in Figura 14 mostra i gruppi più attivi in termini di rivendicazioni.

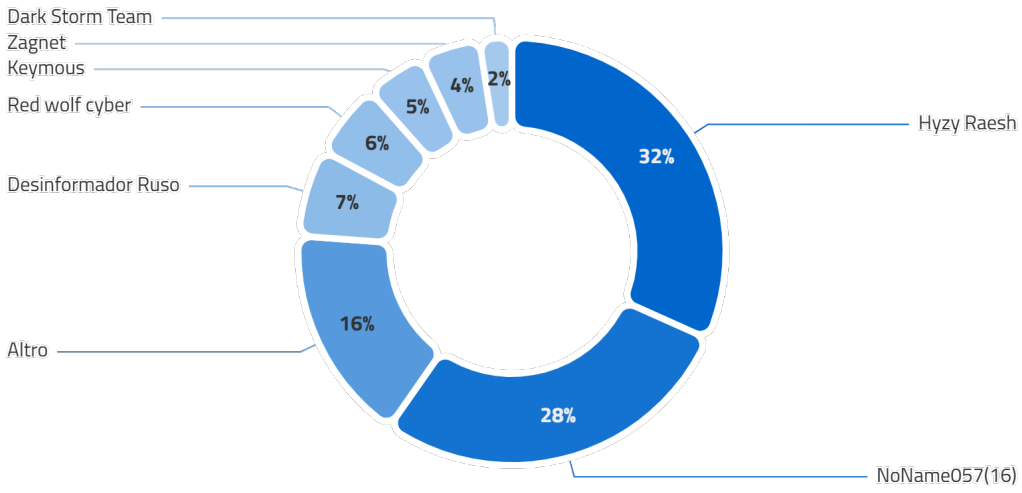

Figura 14 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

[12] I dati rappresentano solo gli eventi pubblicamente rivendicati.

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[13], condotte al fine di individuare e segnalare tempestivamente ai soggetti della constituency l'esposizione a specifiche minacce, rischi, vulnerabilità e criticità, che possono essere sfruttati, o che sono già in corso di sfruttamento, da parte degli attaccanti.

5.1 Comunicazioni dirette

Ad ottobre 2025 sono state diramate un totale di **1.299** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **3.836** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **F5** (CVE-2025-53521, CVE-2025-53474, CVE-2025-48008, CVE-2025-46706 e CVE-2025-41430): tali vulnerabilità – di tipo *Denial of Service* e *Arbitrary Code Execution* – potrebbero consentire a un attaccante non autenticato il blocco del traffico di rete da remoto dei sistemi affetti – tramite l'invio pacchetti opportunamente predisposti – e la potenziale esecuzione di codice arbitrario, laddove l'attaccante disponga invece di un accesso in locale ai sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Apache Tomcat** (CVE-2025-55752 e CVE-2025-55574): tali vulnerabilità – rispettivamente di tipo *Improper Neutralization of Escape, Meta, or Control Sequences* e *Path Traversal* – permetterebbe a un eventuale attaccante di manipolare la visualizzazione dei log nella console, di eludere i meccanismi di sicurezza e/o di eseguire codice arbitrario da remoto sui sistemi impattati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Zimbra Collaboration Suite** (CVE-2025-62763): tale vulnerabilità - di tipo *Server-Side Request Forgery (SSRF)* - potrebbe consentire a un'attaccante, tramite l'invio di richieste HTTP opportunamente predisposte e non correttamente validate dal modulo chat proxy di Zimbra, di accedere a risorse interne e dati sensibili. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

[13] Il monitoraggio individua dispositivi, servizi, asset ed errate configurazioni che incrementano la superficie di attacco sfruttabile da attori malevoli per penetrare all'interno della rete delle vittime.

- **ISC BIND** (CVE-2025-40778): tale vulnerabilità - di tipo *Acceptance of Extraneous Untrasted Data With Trusted Data* - consentirebbe a un attaccante di iniettare dati nella cache tramite l'invio di *Resource Record* non richiesti, compromettendo potenzialmente la cache con un attacco di tipo *DNS Cache Poisoning*, capace di alterare la risoluzione dei nomi e reindirizzare gli utenti verso domini malevoli. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Libraesva Email Security Gateway** (CVE-2025-59689): tale vulnerabilità - di tipo *Command Injection* - potrebbe consentire a un attaccante, non autenticato, l'esecuzione di codice arbitrario da remoto sfruttando una non corretta sanitizzazione dei comandi durante la fase di analisi automatica, in ricezione della posta elettronica, degli allegati compressi. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Squid** (CVE-2025-62168): tale vulnerabilità – di tipo *Information Disclosure* – consentirebbe a un eventuale attaccante remoto di accedere a informazioni sensibili – come token di sicurezza e credenziali – utilizzate internamente dalle applicazioni web relative alle istanze affette. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **SAP Netweaver** (CVE-2025-42944): tali vulnerabilità – di tipo *Insecure Deserialization* – potrebbero consentire a un attaccante non autenticato l'esecuzione arbitraria da remoto di comandi sul sistema operativo, tramite l'invio di richieste appositamente predisposte verso il modulo RMI-P4. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Cisco Adaptive Security Appliance (ASA), Firewall Threat Defense (FTD), IOS, IOS-XE, IOS-XR** (CVE-2025-20363, CVE-2025-20362 e CVE-2025-20333): le vulnerabilità identificate tramite le CVE-2025-20333 e CVE-2025-20363 - di tipo *Buffer Overflow* - consentirebbero a un attaccante autenticato l'esecuzione di codice arbitrario da remoto con privilegi elevati, tramite l'invio di richieste HTTP(s) opportunamente predisposte. La terza vulnerabilità identificata tramite la CVE-2025-20362 - di tipo *Missing Authorization* - consentirebbe invece l'accesso a URL riservate eludendo i meccanismi di autenticazione, sfruttando una non corretta validazione dei parametri di input.
- **TP-Link Gateway Omada** (CVE-2025-7851, CVE-2025-7850, CVE-2025-6542 e CVE-2025-6541): tali vulnerabilità – di tipo *OS Command Injection* (CVE-2025-6541, CVE-2025-6542, CVE-2025-7850) e *Improper Privilege Management* (CVE-2025-7851) – qualora sfruttate, potrebbero consentire a un eventuale attaccante, anche non in possesso di credenziali valide, di eseguire comandi arbitrario da remoto sui sistemi operativi dei prodotti interessati e - in casi particolari - ottenere una shell come utente root. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Telerik UI** (CVE-2025-3600): tale vulnerabilità - di tipo *Unsafe Reflection* - potrebbe consentire a un attaccante, tramite l'invio di richieste HTTP opportunamente predisposte, di compromettere la disponibilità del servizio e/o di eseguire codice arbitrario da remoto sul sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Nagios Log Server** (CVE-2025-44824 e CVE-2025-44823): tali vulnerabilità – rispettivamente di tipo *Information Disclosure* e *Improper Authorization* – potrebbero consentire a un utente autenticato (anche non con privilegi di amministratore) di ottenere accesso alle chiavi API in chiaro di altri utenti (amministratori inclusi) sfruttando l'endpoint /api/system/get_users (CVE-2025-44823) e a un utente autenticato con permessi "read-only" di causare l'interruzione temporanea della disponibilità del servizio di logging, invocando l'endpoint "/api/system/stop?subsystem=elasticsearch" al fine di arrestare l'istanza Elasticsearch utilizzata dal prodotto (CVE-2025-44824). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft ASP.NET Core 8.0** (CVE-2025-55315): tale vulnerabilità – di tipo *HTTP Request/Response Smuggling* – e relativa a ASP.NET Core permetterebbe a un eventuale attaccante remoto di effettuare il bypass di meccanismi di sicurezza. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Ivanti Connect Secure** (CVE-2025-22457): tale vulnerabilità - di tipo *Stack-based Buffer Overflow* - potrebbe consentire a un eventuale attaccante non autenticato l'esecuzione di codice arbitrario da remoto sui dispositivi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Milesight** (CVE-2023-43261): tale vulnerabilità - di tipo *Insertion of Sensitive Information into Log File* - consentirebbe

ad un eventuale attaccante di visualizzare file di log contenenti credenziali sensibili che potrebbero poi essere sfruttate per accedere all'interfaccia web, configurare VPN, disattivare firewall ed inviare SMS.

- **Microsoft Windows Server Update Service** (CVE-2025-59287): tale vulnerabilità di tipo *Deserialization of Untrusted Data* - consentirebbe a un attaccante non autenticato, tramite l'invio di una richiesta opportunamente predisposta sulle porte TCP 8530/8531, una non corretta deserializzazione degli oggetti, permettendo l'esecuzione di codice arbitrario da remoto sui sistemi impattati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Atlassian Jira** (CVE-2025-22167): tale vulnerabilità - di tipo *Path Traversal* - consentirebbe a un attaccante, tramite l'invio di richieste HTTP opportunamente predisposte e sfruttando una non corretta validazione da parte del sistema affetto, di accedere a al contenuto di file sensibili, sovrascrivere configurazioni e/o inserire codice malevolo che può portare all'esecuzione di codice arbitrario da remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Mattermost** (CVE-2025-58075 e CVE-2025-58073): tali vulnerabilità – entrambe di tipo *Missing Authorization* – potrebbero consentire a un utente malintenzionato il bypass dei meccanismi di sicurezza nella gestione degli utenti dei team, manipolando l'*OAuth State* o il *RelayState* sulle istanze target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Veeam Backup & Replication** (CVE-2025-48984 e CVE-2025-48983): tali vulnerabilità - entrambe di tipo *Remote Code Execution* - permetterebbero a un attaccante - autenticato come un utente di dominio - di eseguire codice arbitrario da remoto tramite l'invio di richieste opportunamente predisposte al servizio di *Mount* (che effettua una corretta validazione dei comandi), compromettendo potenzialmente l'intera infrastruttura di backup qualora questa sia *domain-joined*. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **DNN** (CVE-2025-64095): tale vulnerabilità - di tipo *Unrestricted File Upload* – permetterebbe a un attaccante remoto non autenticato di caricare file arbitrari e sovrascrivere file esistenti sul server a causa della mancanza di controlli di autenticazione e validazione nella funzionalità di upload dell'editor HTML. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **IBM Maximo** (CVE-2025-36386): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe a un eventuale attaccante remoto di bypassare i meccanismi di autenticazione e ottenere accesso non autorizzato all'applicazione.
- **DNN** (CVE-2025-59545): tale vulnerabilità – di tipo *Cross-site Scripting (XSS)* – permetterebbe, tramite il modulo *Prompt*, l'esecuzione di comandi che possono restituire HTML grezzo. In tal modo, un input malevolo, anche se sanificato per la visualizzazione in altri contesti, potrebbe essere eseguito quando viene elaborato tramite determinati comandi, portand o a una potenziale esecuzione di script (XSS).
- **Redis** (CVE-2025-49844): tale vulnerabilità – di tipo *Use-After-Free* – e riguardante la componente di scripting Lua, potrebbe consentire a utenti malintenzionati di eseguire da remoto codice arbitrario tramite uno script Lua appositamente predisposto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Adobe Commerce/Magento** (CVE-2025-54236): tale vulnerabilità — di tipo *Improper Input Validation* — potrebbe permettere a un attaccante non autenticato di manipolare sessioni e oggetti applicativi, con possibili conseguenze quali l'impersonificazione di account utente, takeover di sessione e, su sistemi che preservano la sessione all'interno di file, possibile esecuzione remota di codice. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Netbird** (CVE-2025-10678): durante l'installazione del prodotto tramite lo script fornito dal vendor, viene creato automaticamente un account amministrativo per la componente ZITADEL (identity provider integrato). Tuttavia, lo script non rimuove né modifica la password di default utilizzata per l'account. Un attaccante potrebbe sfruttare tali credenziali predefinite per ottenere accesso non autorizzato all'applicazione. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **FlowiseAI** (CVE-2025-61913): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante

autenticato di leggere e scrivere file arbitrari in qualsiasi percorso del file system ed eseguire potenzialmente da remoto codice arbitrario sui sistemi affetti, sfruttando i componenti *WriteFileTool* e *ReadFileTool* di Flowise, i quali non limitano correttamente l'accesso ai percorsi dei file. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **Veeder-Root TLS4B** (CVE-2025-58428): tale vulnerabilità – *Command Injection* – consentirebbe a un eventuale attaccante di ottenere accesso completo alla shell, eseguire comandi da remoto, muoversi lateralmente all'interno della rete, provocare condizioni di *Denial of Service*, causare il blocco dell'accesso amministrativo e compromettere le funzionalità principali del sistema.
- **Gladinet CentreStack e TrioFox** (CVE-2025-11371): tale vulnerabilità – di tipo *Local File Inclusion* – se sfruttata in combinazione con la CVE-2025-30406 potrebbe consentire a un attaccante non autenticato di accedere a file di sistema ed eseguire codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Fortinet FortiSwitchManager** (CVE-2025-49201): tale vulnerabilità – di tipo *Weak Authentication* – relativa alla componente WAD/GUI, consentirebbe ad un attaccante di bypassare l'autenticazione attraverso attacchi di tipo brute-force. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Oracle E-Business Suite** (CVE-2025-61884): tale vulnerabilità – di tipo *Unauthorized Access* – consentirebbe a un eventuale attaccante non autenticato, tramite l'invio di richieste HTTP opportunamente predisposte e la non corretta validazione delle stesse, di accedere a dati sensibili e compromettere parzialmente i sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Oracle E-Business Suite** (CVE-2025-62481 e CVE-2025-53072): tali vulnerabilità – entrambe di tipo *Missing Authentication for Critical Function* – consentirebbero a un eventuale attaccante non autenticato, tramite l'invio di richieste HTTP opportunamente predisposte e la non corretta validazione delle stesse da parte del componente "Marketing", di eseguire codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **VMware Aria Operations** (CVE-2025-41244): tale vulnerabilità – di tipo zero-day e *Local Privilege Escalation* – qualora sfruttata, potrebbe consentire ad un attaccante con accesso non amministrativo a una macchina virtuale gestita da Aria Operations – con il *Software Development Management Pack (SDMP)* abilitato e VMware tools installati – di elevare i propri privilegi sul sistema impattato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Ivanti Endpoint Manager** (CVE-2025-9713 e CVE-2025-11622): tali vulnerabilità – di tipo rispettivamente *Path Traversal* e *Deserialization of Untrusted Data* - consentirebbero, senza necessità di autenticazione e tramite interazione utente, l'esecuzione di codice da remoto (relativo alla CVE-2025-9713, presente nel metodo "OnSaveToDB") e a un attaccante autenticato localmente di evelare i propri privilegi (relativo alla CVE-2025-11622, presente nel servizio "AgentPortal"). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

In Figura 15 viene riportata la distribuzione delle segnalazioni per tipologia di soggetto e prodotto.

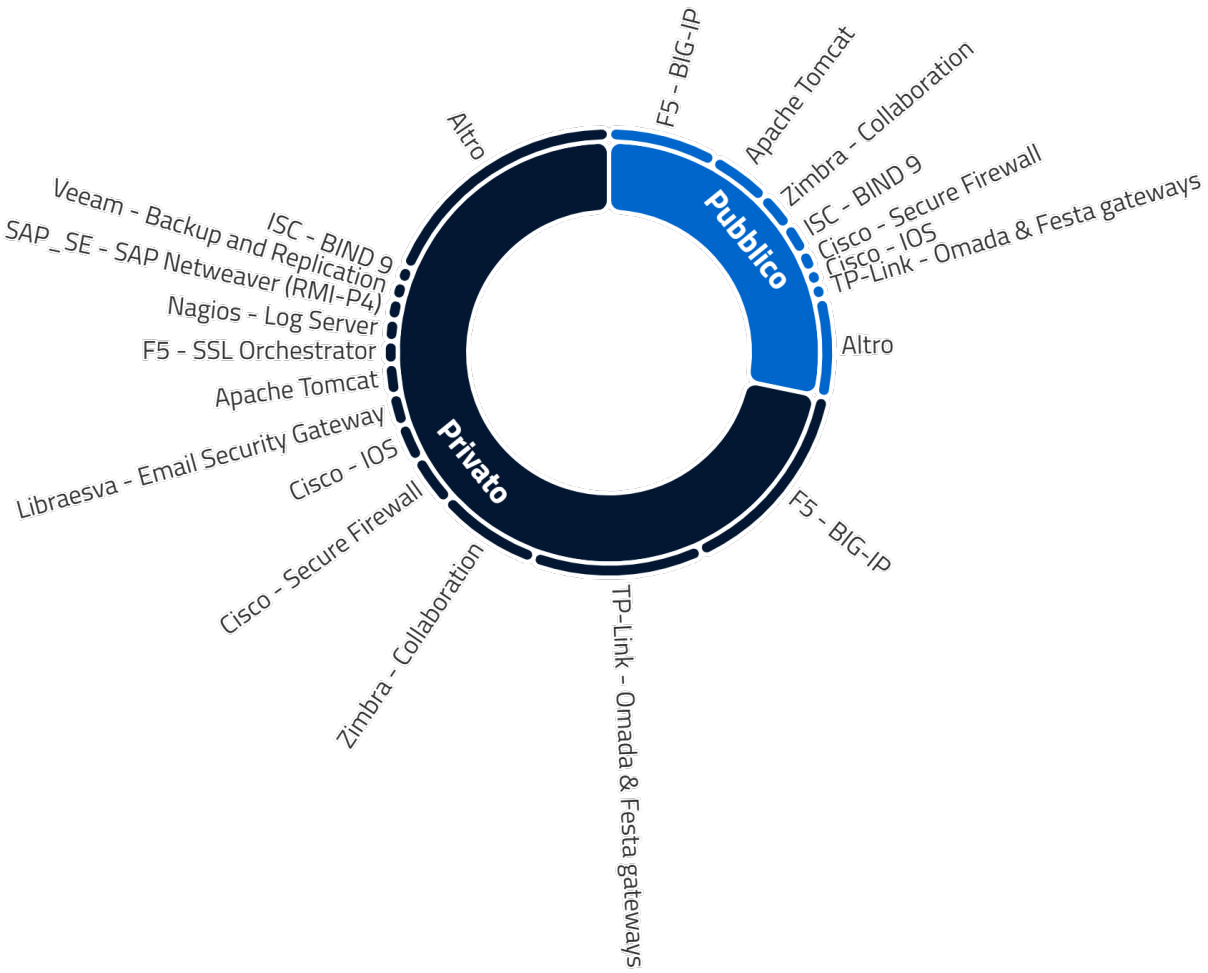

Figura 15 - *distribuzione delle segnalazioni per tipologia di soggetto e prodotto*

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

ottobre 2025