Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

NOVEMBRE 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 novembre 2025 sono stati registrati **182 eventi**, in **diminuzione** del 32% rispetto ai **267** di ottobre, mentre il numero di **incidenti** (**54**) è in **aumento** del 13% rispetto al mese precedente.
- I settori con il maggior numero di vittime di eventi cyber registrate nel mese sono stati: **Pubblica amministrazione centrale**, **Pubblica amministrazione locale** e **Telecomunicazioni**.
- Nel corso del mese di novembre 2025, l'attività riconducibile alla matrice **hacktivista** si è attestata su livelli inferiori rispetto al mese precedente, rappresentando il 31% degli eventi complessivamente monitorati, a fronte del 49% registrato nel mese di ottobre. Tale andamento risulta associato alla **riduzione degli attacchi di tipo DDoS rilevati nel periodo**, che hanno interessato in via prevalente il settore dei Trasporti e la Pubblica Amministrazione, sia a livello locale sia centrale. In tale contesto, sono stati osservati attacchi DDoS ai danni dei siti web di alcune società di gestione aeroportuale, che operano su diversi scali del territorio nazionale, con temporanee indisponibilità dei servizi web, limitate a intervalli di alcuni minuti. All'interno dello stesso quadro, e in linea con quanto già osservato nei mesi precedenti, sono state rilevate rivendicazioni 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 **423 comunicazioni** di allertamento a pubbliche amministrazioni e imprese che esponevano su Internet **614 servizi a rischio**, in quanto presentavano prodotti potenzialmente vulnerabili, in particolar modo alle CVE di WatchGuard Firebox (CVE-2025-59396) e SolarWinds Web Help Desk (CVE-2025-40549, CVE-2025-40548 e CVE-2025-40547). Sempre nell'ambito delle attività di monitoraggio proattivo, è stata rilevata una nuova attività malevola finalizzata all'installazione di varianti aggiornate della **webshell** denominata **BadCandy**, associata a minacce di tipo avanzato e osservata per la prima volta nel mese di ottobre 2023, con possibile impatto su prodotti Cisco IOS XE esposti in rete. A seguito di tali evidenze, è stata condotta un'analisi mirata volta a valutare la diffusione sul territorio nazionale del suddetto impianto malevolo.

- L'analisi dei *log* provenienti da **malware di tipo infostealer** ha consentito, nel mese, di identificare **112 account** afferenti a soggetti istituzionali, tutti prontamente allertati.
- I **vettori di attacco** maggiormente rilevati a novembre 2025 sono stati le e-mail, l'utilizzo di account validi e lo sfruttamento di vulnerabilità di note.
- Sono state pubblicate **3.115** nuove CVE, in sensibile **diminuzione** rispetto ad ottobre (**–1.269**).
- Le **comunicazioni dirette**, effettuate dal CSIRT Italia per segnalare potenziali compromissioni o fattori di rischio ad amministrazioni ed imprese italiane, nel mese di novembre 2025 sono state **1.420**, in **diminuzione** rispetto ad ottobre.

I NUMERI DI NOVEMBRE 2025

Figura 1 - *indicatori delle attività operative a novembre 2025 e nei sei mesi precedenti*

- **182** eventi cyber, in **diminuzione** (**–85**);
- **196** vittime, in **diminuzione** (**–131**);
- **109** vittime della constituency[1], in **diminuzione** (**–61**);
- **54** incidenti con impatto confermato, in **aumento** (**+6**);
- **181** asset potenzialmente compromessi, in **aumento** (**+181**);
- **614** asset potenzialmente vulnerabili, in **diminuzione** (**–3.226**);
- **78** alert sul sito web del CSIRT Italia, **stabile** (**–2**);
- **1.420** comunicazioni inviate, in **diminuzione** (**–2.945**);
- **3.115** nuove CVE, in **diminuzione** (**–1.269**).

[1]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 a novembre 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.

- **Ollama** Link all'alert;
- **Grafana Labs** (CVE-2025-41115) Link all'alert;
- **React Native Community** (CVE-2025-11953) Link all'alert;
- **Gladinet Triofox** (CVE-2025-12480) Link all'alert;
- **D-Link DIR-878** (CVE-2025-60676, CVE-2025-60674, CVE-2025-60673, CVE-2025-60672) Link all'alert;
- **SolarWinds Web Help Desk** (CVE-2025-40549, CVE-2025-40548 e CVE-2025-40547) Link all'alert;
- **Django** (CVE-2025-64459) Link all'alert;
- **Open Source Geospatial Foundation GeoServer** (CVE-2025-58360) Link all'alert;
- **Fortinet FortiWeb** (CVE-2025-58034) Link all'alert;
- **PostgreSQL pgAdmin** (CVE-2025-12762) Link all'alert;
- **W3 Total Cache** (CVE-2025-9501) Link all'alert;
- **Open WebUI** (CVE-2025-64495) Link all'alert;
- **Symfony** (CVE-2025-64500) Link all'alert;
- **OpenWRT** (CVE-2025-62526 e CVE-2025-62525) Link all'alert;
- **Monsta FTP** (CVE-2025-34299) Link all'alert;
- **Twonky Server** (CVE-2025-13316 e CVE-2025-13315) Link all'alert;
- **Asus AiCloud** (CVE-2025-59366) Link all'alert;
- **R.V.R Elettronica TEX** (CVE-2025-63207) Link all'alert;
- **Apache OFBiz** (CVE-2025-61623 e CVE-2025-59118) Link all'alert;
- **N-Able N-Central** (CVE-2025-11700) Link all'alert;

Maggiori dettagli nelle sezioni 3 e 5.

2 EVENTI ED INCIDENTI

A novembre 2025 sono stati individuati **182** eventi cyber, in **diminuzione** del 32% rispetto al mese precedente. Questi ultimi hanno **interessato 158 soggetti nazionali**: 109 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 182 eventi cyber, **54 sono stati classificati quali incidenti**, in **aumento** del 13% rispetto ad ottobre.

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[2], riferita ai successivi 3 mesi.

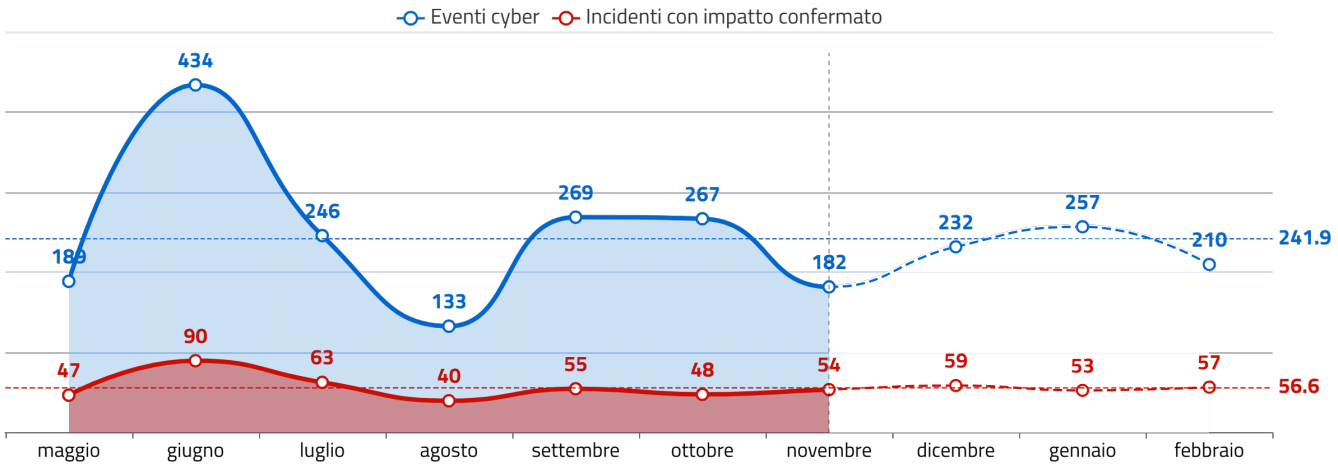

Figura 2 - *andamento attività reattive e analisi previsionale*

[2] 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[3]. Si evidenza altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico).

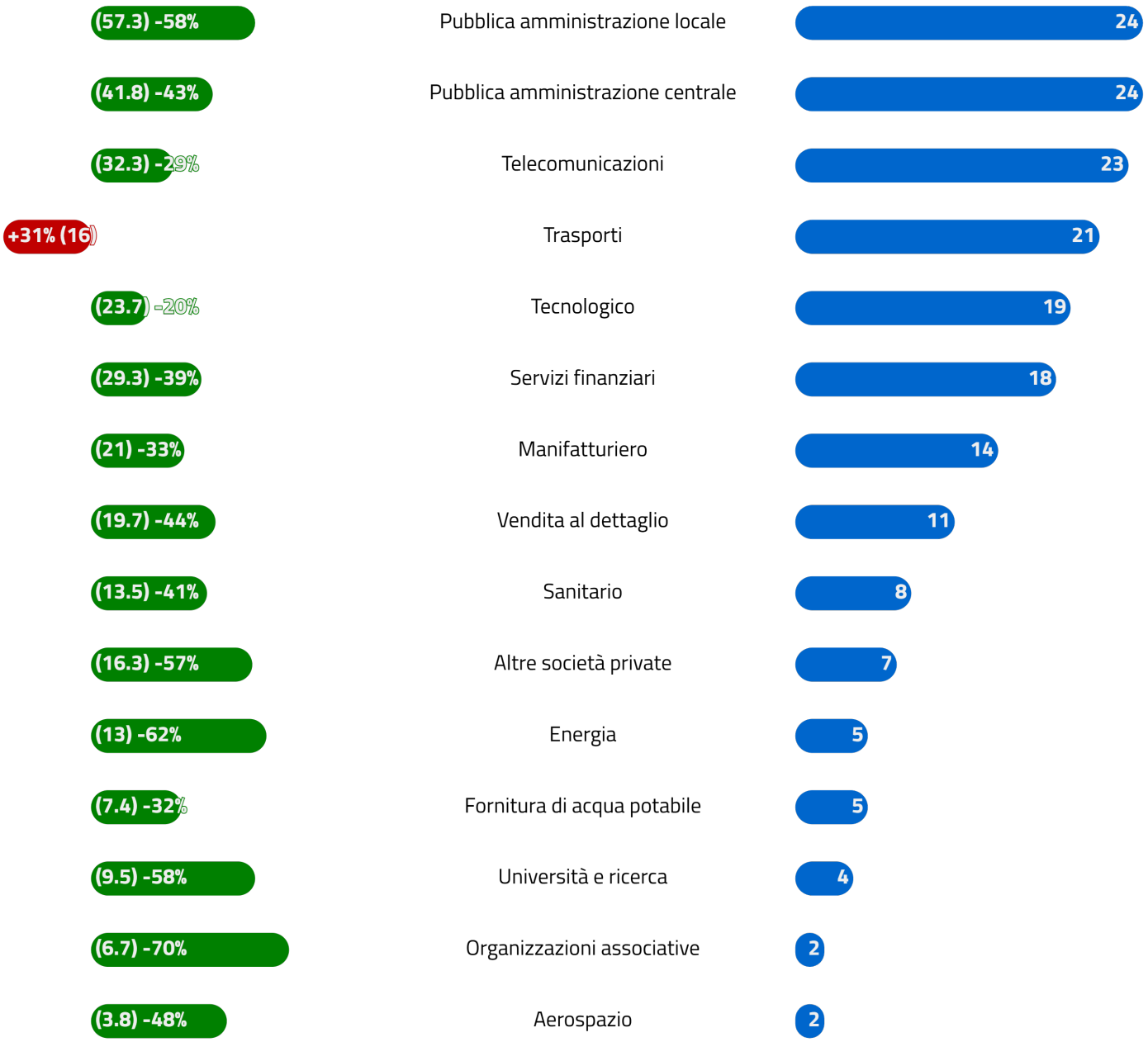

Figura 3 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente (top 15)*

[3] 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[4] 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)*

[4] 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 novembre 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.

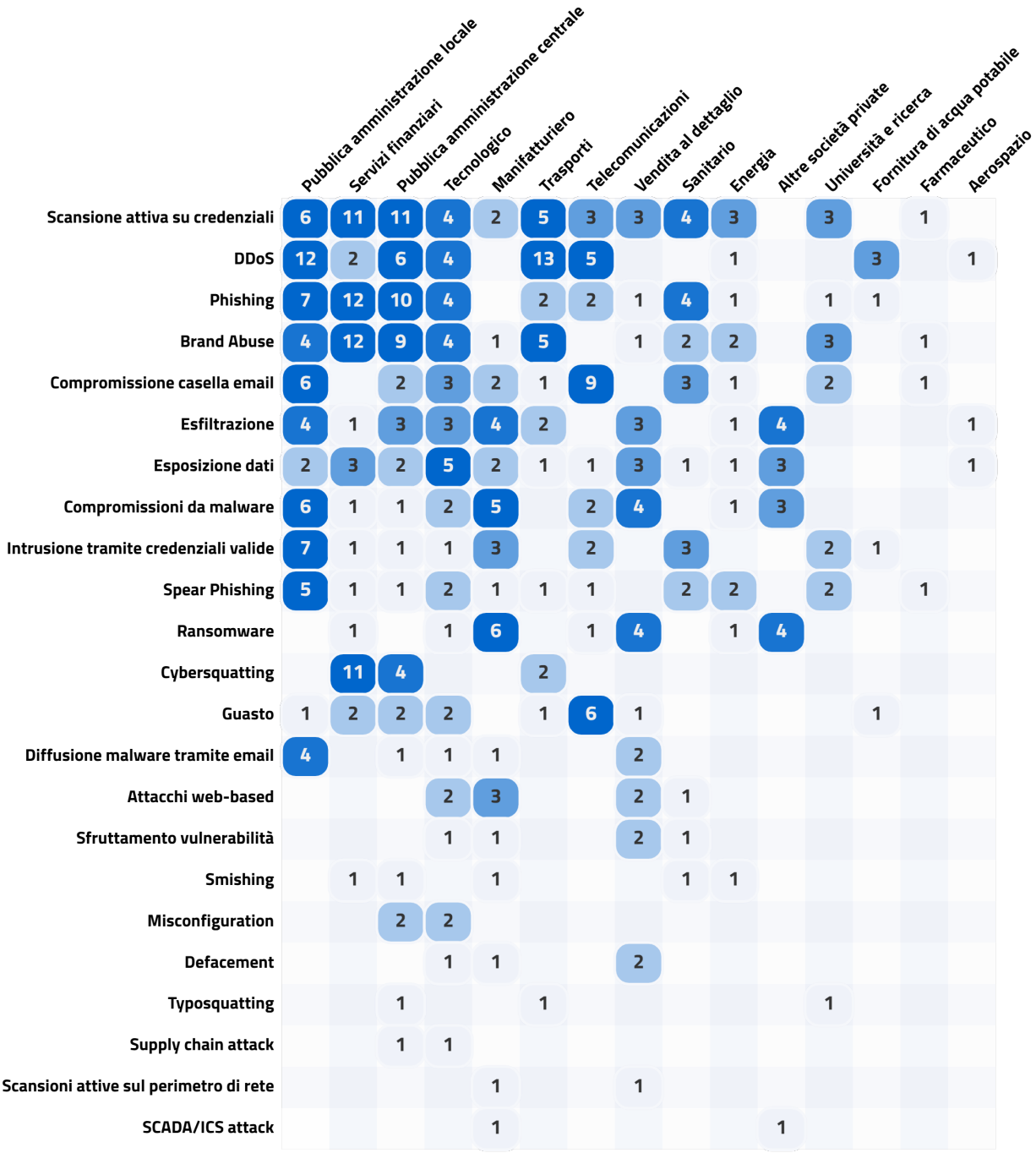

Figura 5 - *numero di vittime per settore e tipologia di minacce*

2.4 Distribuzione geografica delle vittime

I 182 eventi cyber hanno interessato **196** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

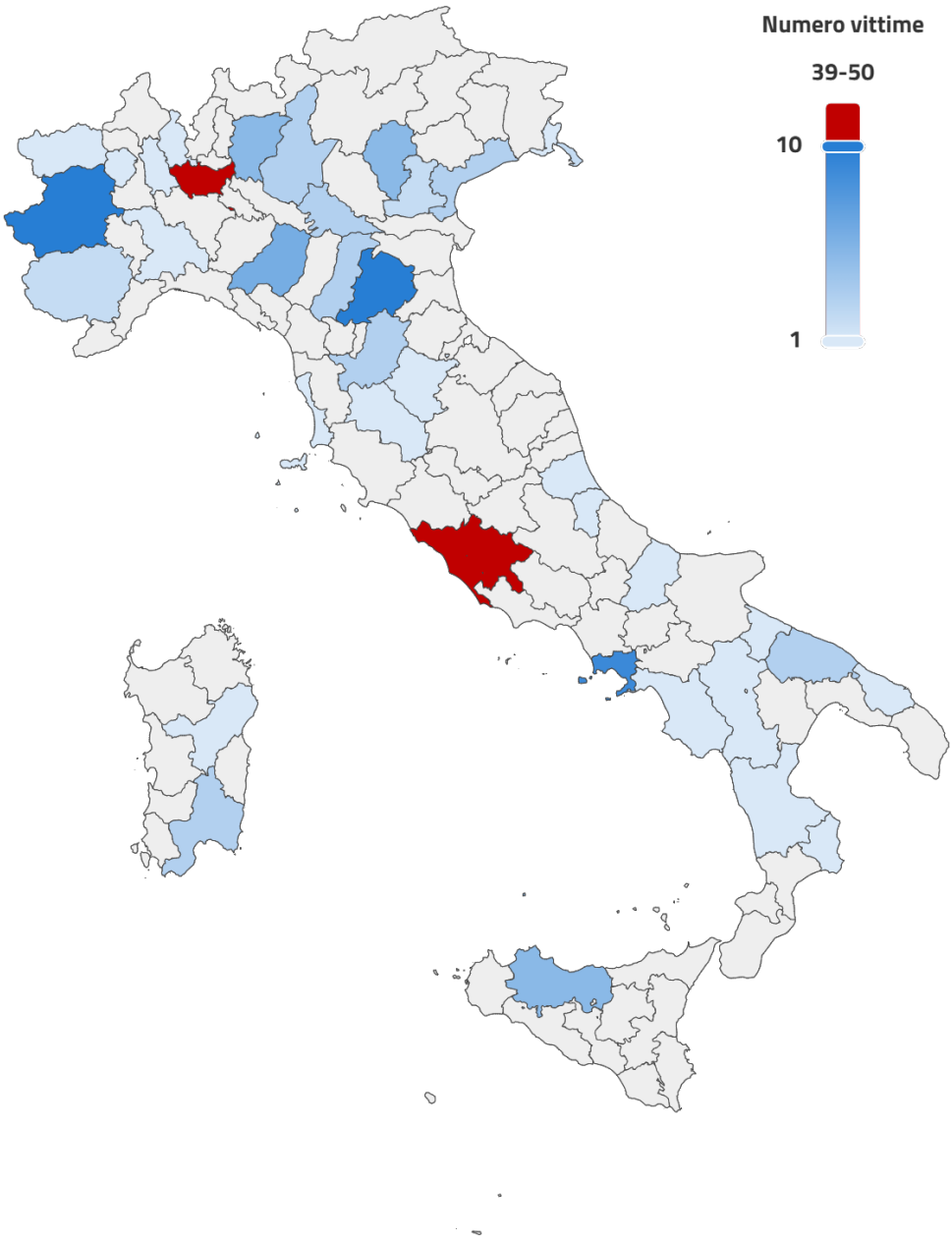

Figura 6 - *distribuzione delle vittime degli eventi cyber*

3 VULNERABILITÀ

A novembre 2025 sono state pubblicate[5] **3.115** nuove CVE, in **diminuzione** (**–1.269**) rispetto ad ottobre. Di queste, **485** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–102**), e per **5** CVE è stato rilevato lo sfruttamento attivo, **stabile** (**–2**) rispetto ad ottobre.

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 **78**. Oltre al consueto aggiornamento mensile di Microsoft (link) all'alert sul sito web, che ha risolto un totale di 63 nuove vulnerabilità (1 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Ollama**: rilevata una nuova vulnerabilità in Ollama, noto progetto open source, utilizzato per eseguire LLM localmente sulla propria infrastruttura, supportando vari modelli come gpt-oss, DeepSeek-R1, Meta Llama4, Google Gemma3. Tale vulnerabilità, qualora sfruttata, permetterebbe ad un utente malintenzionato, con accesso all'API di Ollama, di caricare un model malevolo ed eseguire codice arbitrario remoto (stima di impatto sistemico **84,35/100**). Link all'alert del 05/11/2025;
- **Grafana Labs**: sanata una vulnerabilità con gravità "critica" in Grafana, nota applicazione web per la visualizzazione e l'analisi interattiva di dati. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di elevare i propri privilegi o di impersonificare altri utenti sui sistemi interessati, qualora configurati come indicato nel bollettino di sicurezza del vendor (stima di impatto sistemico **79,48/100**). Link all'alert del 20/11/2025;
- **React Native Community**: disponibile un Proof of Concept (PoC) per la CVE-2025-11953, relativa al pacchetto NPM Cli, distribuito nell'ambito del progetto "React Native Community". Tale software gestisce la command-line interface di React Native, framework di sviluppo mobile JavaScript multipiattaforma. La vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto l'esecuzione di comandi arbitrari sul sistema interessato (stima di impatto sistemico **79,23/100**). Link all'alert del 05/11/2025;

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

- **Gladinet**: ricercatori di sicurezza hanno rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-12480 che interessa il prodotto Gladinet TrioFox, soluzione 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 **78,33/100**). Link all'alert del 13/11/2025;
- **D-Link**: disponibili Proof of Concept (PoC) per lo sfruttamento di varie vulnerabilità presenti nel modello D-Link DIR-878. Specificamente riguardo alle CVE-2025-60672, CVE-2025-60673, CVE-2025-60674 e CVE-2025-60676 (stima di impatto sistemico **77,94/100**). Link all'alert del 19/11/2025;

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[6].

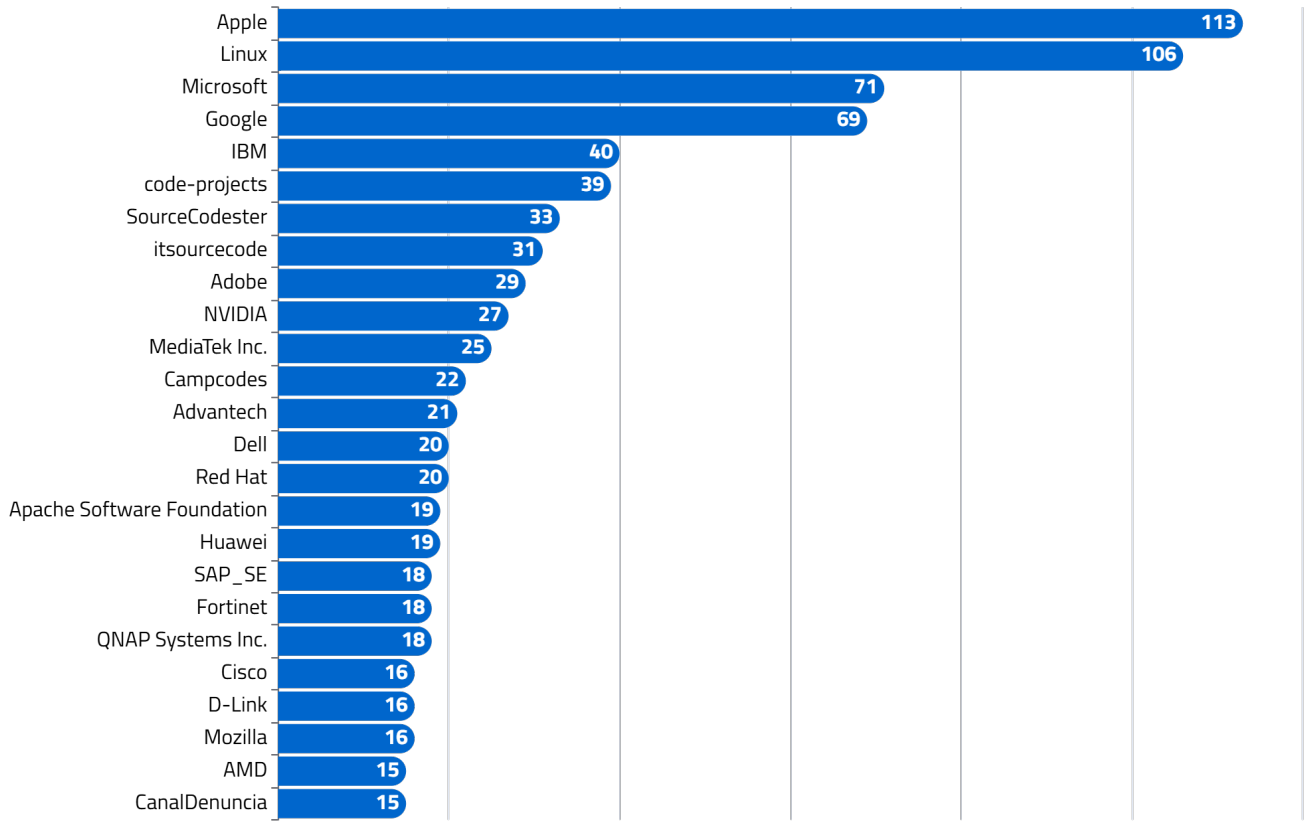

Figura 7 - *top 25 produttori affetti da vulnerabilità nel mese*

[6] 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.

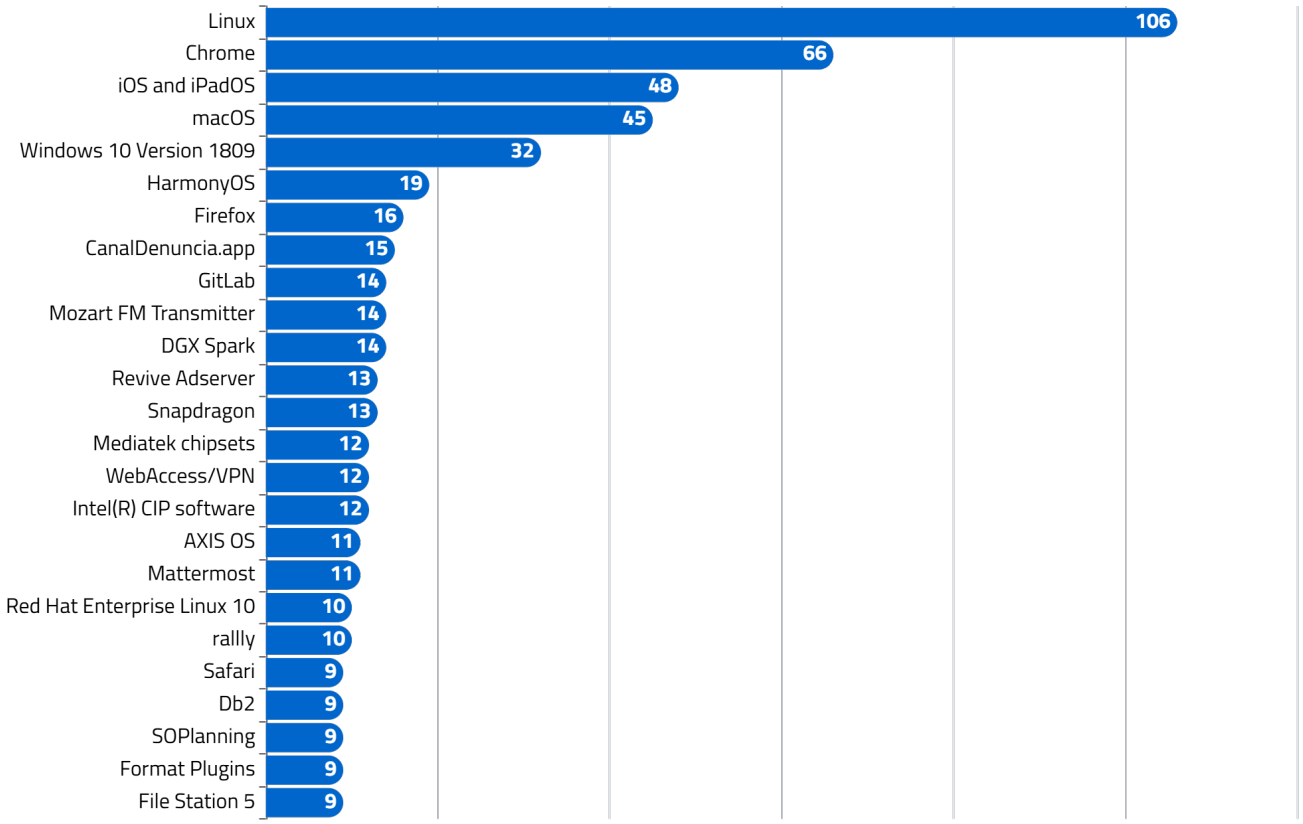

Figura 8 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

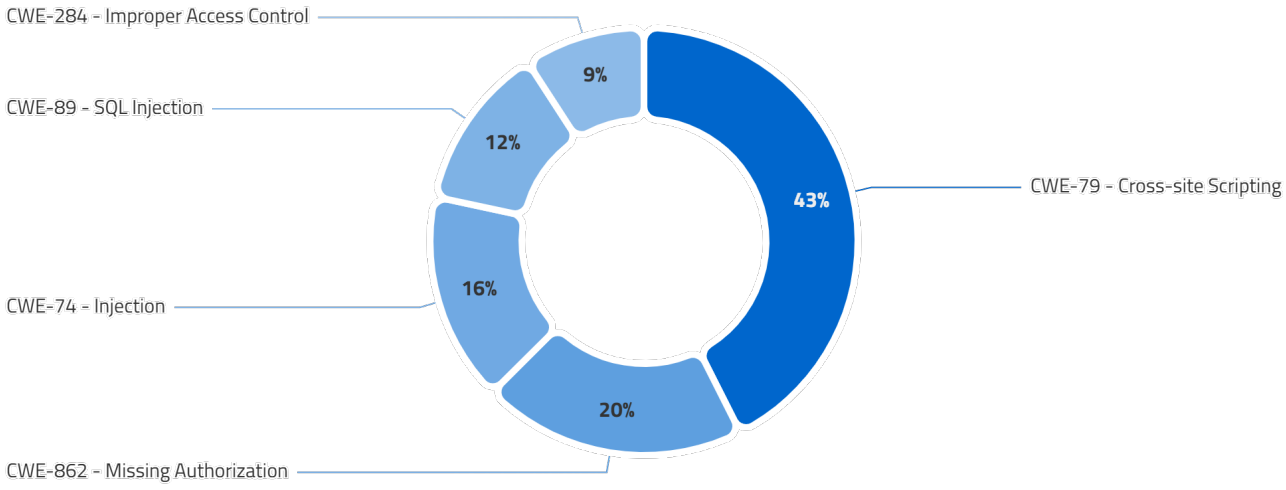

Figura 9 - *top 5 CWE nel mese*

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)[7] fornito dal FIRST nel mese in esame.

Vendor	**Fortinet**
Prodotti e versioni vulnerabili	**FortiWeb versioni:** ▪ **dalla 8.0.0 fino alla 8.0.1,** ▪ **dalla 7.6.0 fino alla 7.6.4,** ▪ **dalla 7.4.0 fino alla 7.4.9,** ▪ **dalla 7.2.0 fino alla 7.2.11,** ▪ **dalla 7.0.0 fino alla 7.0.11.**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante di eseguire da remoto comandi con privilegi amministrativi**
Data di rilascio CVE	**14/11/2025 modificata il 18/11/2025**
CVSS score 3.0	**9.4 Critical**
EPSS max score	**0.82**

Tabella 1 - *CVE-2025-64446*

Vendor	**WatchGuard**
Prodotti e versioni vulnerabili	**Fireware OS versioni:** ▪ **dalla 11.10.2 fino alla 11.12.4_Update1,** ▪ **dalla 12.0 fino alla 12.11.3,** ▪ **dalla 2025.0 fino alla 2025.1.**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire da remoto codice malevolo**
Data di rilascio CVE	**17/09/2025 modificata il 14/11/2025**
CVSS score 4.0	**9.3 Critical**
EPSS max score	**0.77**

Tabella 2 - *CVE-2025-9242*

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

Vendor	**Oracle**
Prodotti e versioni vulnerabili	**Identity Manager, versione 12.2.1.4.0 e versione 14.1.2.1.0**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire da remoto codice malevolo**
Data di rilascio CVE	**21/10/2025 modificata il 24/11/2025**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.71**

Tabella 3 - *CVE-2025-61757*

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[8] condivisi dal CSIRT Italia tramite piattaforma MISP[9], in modo da caratterizzarne le tipologie più frequenti.

4.1 Ransomware: distribuzione delle vittime

A novembre 2025, nessun attacco ransomware ha colpito soggetti critici o soggetti a media criticità, confermando la preferenza di questa tipologia di attaccanti a colpire obiettivi meno strutturati e dotati di limitate capacità di cybersicurezza.

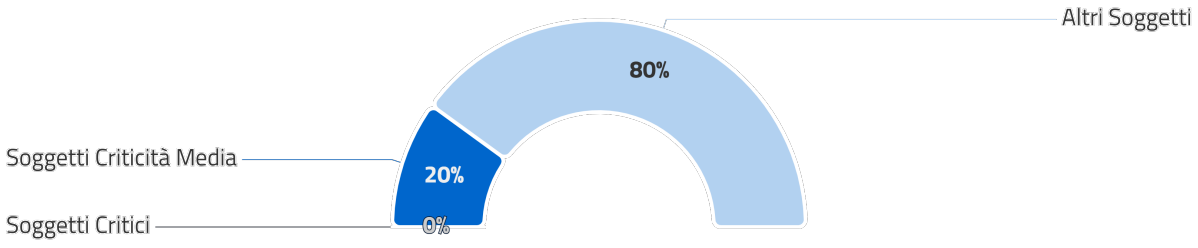

Figura 10 - *distribuzione delle vittime di ransomware in base alla loro criticità*

[8]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.

[9]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 novembre 2025 ha permesso di individuare **11** rivendicazioni di attacchi ransomware a danno di soggetti italiani[10].

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

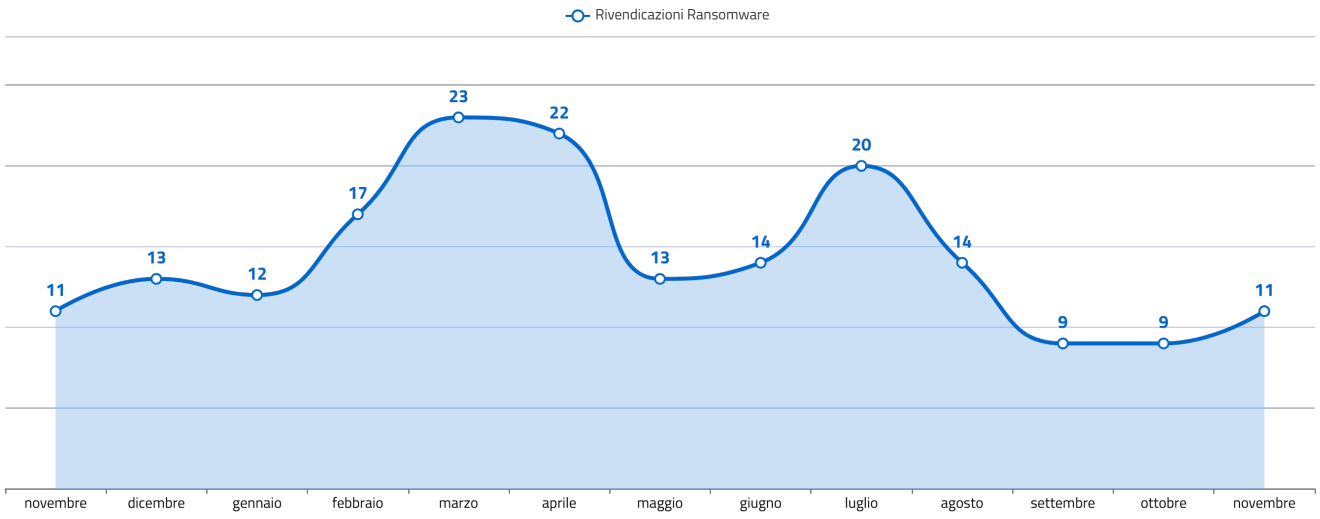

Figura 11 - *andamento delle rivendicazioni Ransomware*

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

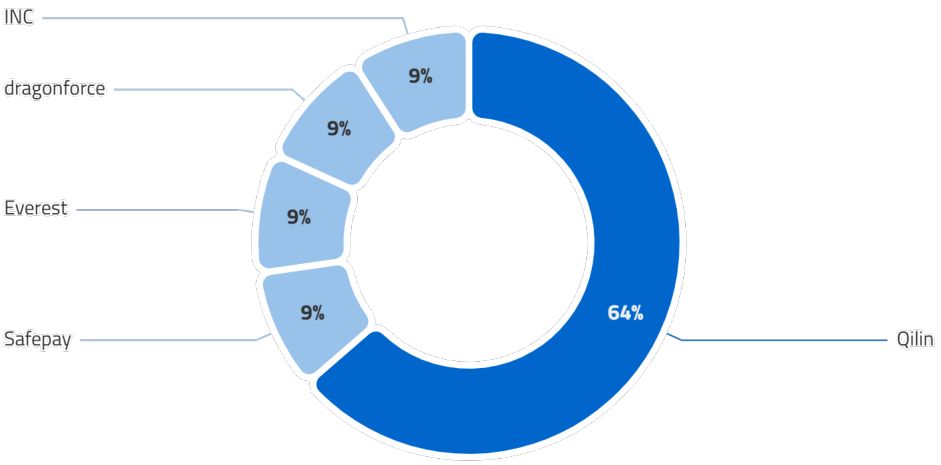

Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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

4.3 Rivendicazioni DDoS

A novembre 2025 sono state individuate[11] **44** 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.

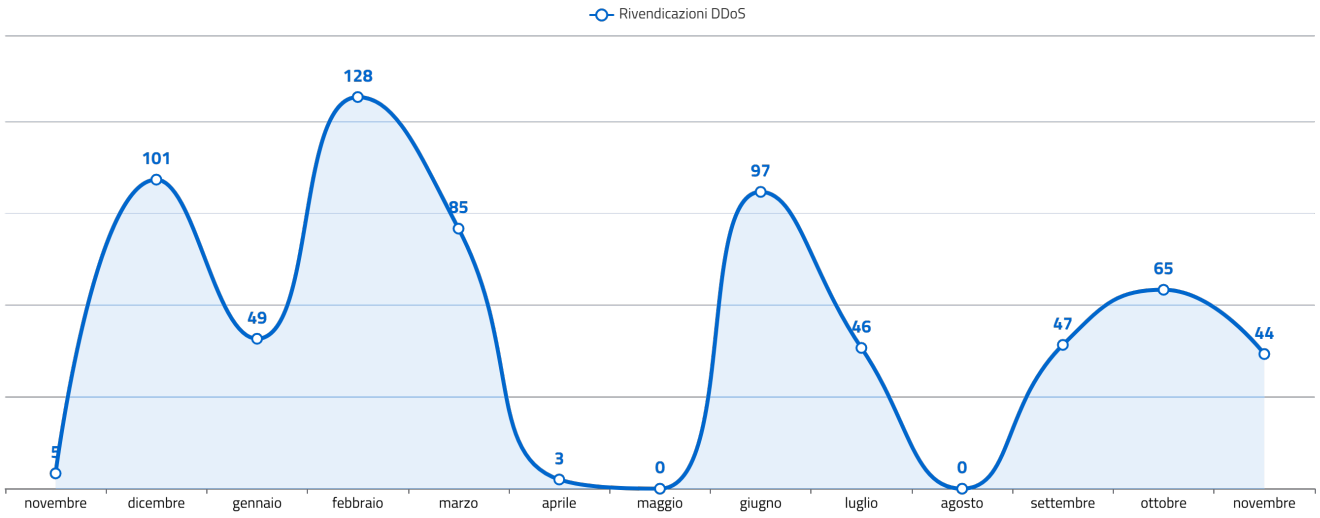

Figura 13 - *andamento delle rivendicazioni DDoS*

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

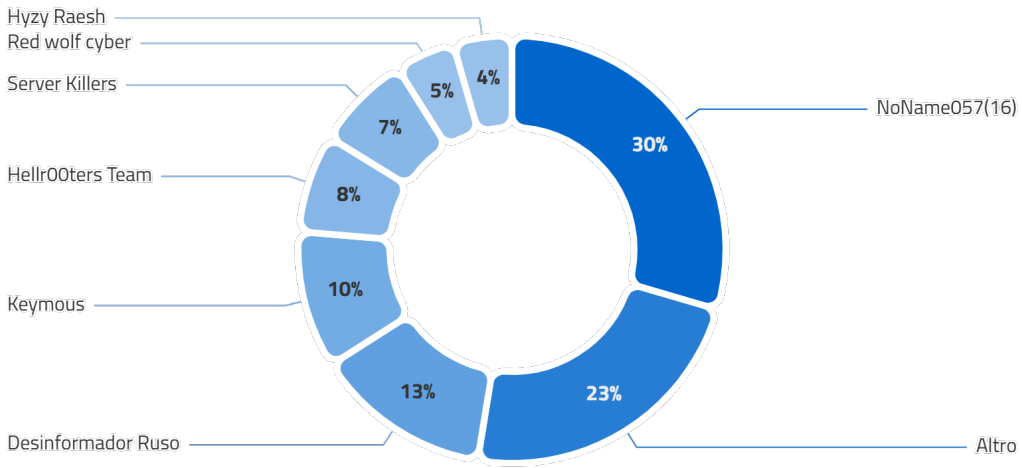

Figura 14 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[12], 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

A novembre 2025 sono state diramate un totale di **423** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **613** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **WatchGuard Firebox** (CVE-2025-59396): tale misconfigurazione - associata originariamente alla vulnerabilità CVE-2025-59396 rifiutata dal vendor - permetterebbe a un eventuale attaccante di ottenere un accesso amministrativo tramite un'interfaccia amministrativa esposta tramite protocollo SSH sulla porta 4118 utilizzando le credenziali predefinite, laddove esse non siano state esplicitamente sostituite in fase di installazione dei dispositivi.
- **SolarWinds Web Help Desk** (CVE-2025-40549, CVE-2025-40548 e CVE-2025-40547): tali vulnerabilità – rispettivamente di tipo *Code Injection*, *Improper Privilege Management* e *Path Traversal* – potrebbero consentire a un utente malintenzionato con privilegi di amministratore di eseguire codice arbitrario sul sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Django** (CVE-2025-64459): tale vulnerabilità - di tipo *SQL Injection* - potrebbe consentire a un attaccante remoto non autenticato di inviare un input malevolo, interpretato direttamente dal motore SQL, portando potenzialmente all'accesso non autorizzato ai dati, alla modifica e/o cancellazione di informazioni e all'esecuzione di comandi arbitrari sul database relativo al backend dell'applicazione web. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

[12] 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.

- **Open Source Geospatial Foundation GeoServer** (CVE-2025-58360): tale vulnerabilità – di tipo *XML External Entity Reference (XXE)* – permetterebbe a un eventuale attaccante di generare entità esterne arbitrarie sui sistemi target e di accedere potenzialmente a file o servizi interni, comportando così l'accesso a informazioni sensibili o provocare altro genere di impatti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Grafana Enterprise** (CVE-2025-41115): tale vulnerabilità – di tipo *Incorrect Privilege Assignment* – permetterebbe a un eventuale attaccante di elevare i propri privilegi o di impersonificare altri utenti sui sistemi interessati, qualora il prodotto sia configurato con la funzionalità di "SCIM provisioning" attiva e sia abilitata la sincronizzazione automatica degli utenti sulla base delle richieste inviate tramite tale protocollo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **SuiteCRM** (CVE-2025-64493 e CVE-2025-64492): tali vulnerabilità – di tipo *SQL Injection* – permetterebbero a un eventuale attaccante autenticato di sfruttare una SQL injection di tipo "blind" e "time-based" per estrarre dati arbitrari - anche potenzialmente sensibili, nel caso della CVE-2025-64492 - dal database senza alcun privilegio amministrativo e compromettendone così la confidenzialità.
- **Fortinet FortiWeb** (CVE-2025-58034): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante autenticato di eseguire comandi arbitrari sul sistema operativo sottostante tramite richieste HTTP appositamente predisposte veicolate tramite API o specifici comandi CLI. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **PostgreSQL pgAdmin** (CVE-2025-12762): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante di iniettare ed eseguire comandi arbitrari da remoto sul server che ospita pgAdmin. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **W3 Total Cache** (CVE-2025-9501): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante di eseguire codice PHP arbitrario mediante l'inserimento di payload malevoli in commenti o input elaborati dal plugin. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Open WebUI** (CVE-2025-64495): tale vulnerabilità – di tipo *Cross-site Scripting (XSS)* – permetterebbe a un eventuale attaccante autenticato e con i permessi per creare prompt, di inserire un payload malevolo che potrebbe essere eseguito da altri utenti se questi utilizzano il comando con l'opzione "Insert Prompt as Rich Text" attiva. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Symfony** (CVE-2025-64500): tale vulnerabilità – di tipo *Incorrect Authorization* – permetterebbe a un eventuale attaccante di accedere a risorse protette bypassando i controlli di accesso tramite manipolazione del percorso dell'URL. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **OpenWRT** (CVE-2025-62526 e CVE-2025-62525): tali vulnerabilità – rispettivamente di tipo *Out-of-bounds Read/Write* e *Buffer Overflow* – permetterebbero a un eventuale attaccante nella rete locale dei sistemi affetti rispettivamente di leggere/scrivere aree di memoria riservate al Kernel con la possibilità di effettuare *sandbox escape* (CVE-2025-62525) ed eseguire codice arbitrario, sfruttando una falla nel codice utilizzato per il parsing degli eventi di registrazione alla rete (CVE-2025-62526). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Monsta FTP** (CVE-2025-34299): tale vulnerabilità – di tipo *Unrestricted File Upload* – permetterebbe a un eventuale attaccante, tramite un file opportunamente predisposto su un server FTP da lui controllato, di scaricare tale file in un percorso arbitrario sui sistemi affetti e portando potenzialmente all'esecuzione di codice arbitrario. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Twonky Server** (CVE-2025-13316 e CVE-2025-13315): tali vulnerabilità – di tipo *Authentication Bypass* – permetterebbero a un eventuale attaccante di ottenere le credenziali dell'utente amministratore, eludendo i meccanismi di autenticazione sui sistemi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **Asus AiCloud** (CVE-2025-59366): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante di eseguire alcuni comandi senza autorizzazione sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **R.V.R Elettronica TEX** (CVE-2025-63207): tale vulnerabilità – di tipo *Improper Authentication* – permetterebbe a un eventuale attaccante di modificare le credenziali degli account "Admin", "Operator" e "User" attraverso richieste POST non autenticate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Apache OFBiz** (CVE-2025-61623, CVE-2025-59118): tali vulnerabilità – di tipo *Unrestricted File Upload* e *Cross-site Scripting (XSS)* – permetterebbero, rispettivamente, a un eventuale attaccante remoto di caricare file malevoli sul target e di eseguire codice arbitrario lato client. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **N-Able N-Central** (CVE-2025-11700): tale vulnerabilità – di tipo *XML External Entity Reference (XXE)* – permetterebbe a un eventuale attaccante, sfruttando entità XML esterne, di leggere file sensibili dal file system del server ed esfiltrare informazioni riservate, inducendo l'applicazione a restituire come output il contenuto dei file. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **MLflow** (CVE-2025-11200): 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 e i suoi modelli, nonché di creare credenziali estremamente deboli o vuote.

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

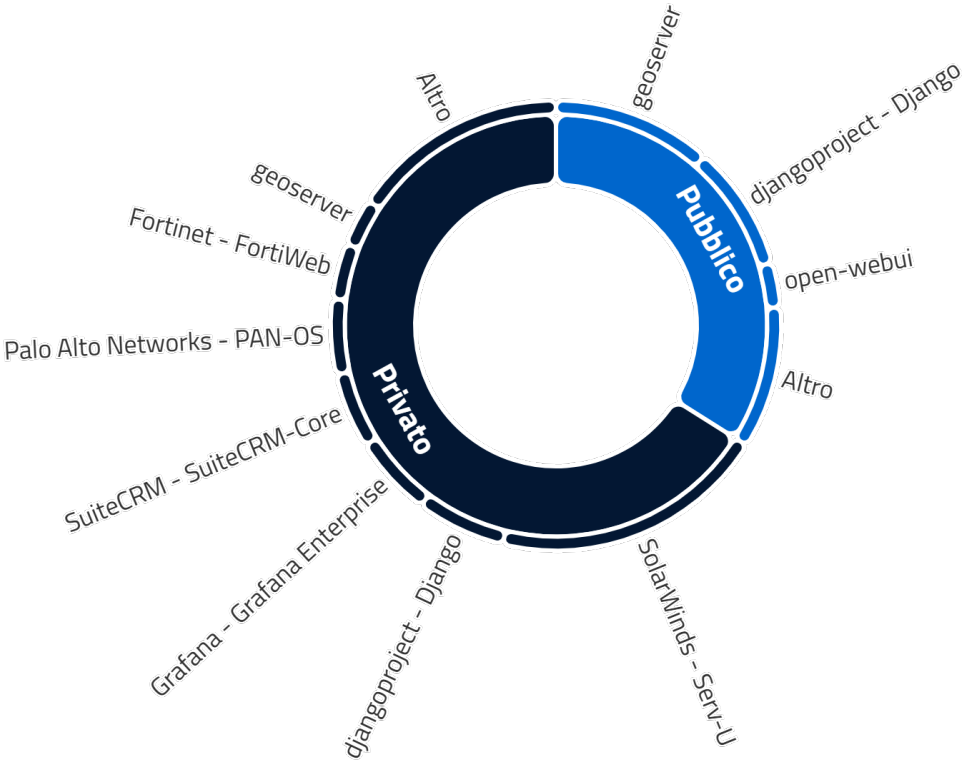

Figura 15 - *distribuzione delle segnalazioni per tipologia di soggetto*

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

novembre 2025