Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

Servizio Operazioni
e gestione delle crisi cyber

aprile 2025

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.

Sommario

pag.

Indice delle figure

pag.

1 EXECUTIVE SUMMARY

- Ad aprile 2025 si è registrata una **diminuzione** del numero di **eventi**, mentre il numero di **incidenti** è rimasto sostanzialmente nella **media** rispetto ai sei mesi precedenti.
- I settori con il maggior numero di vittime registrate sono stati: **Pubblica amministrazione centrale**, **Telecomunicazioni** e **Trasporti**.
  L'aumento degli eventi nel settore **Telecomunicazioni** è riconducibile ad un incremento dei tentativi di spearphishing segnalati dai soggetti coinvolti. È stata inoltre rilevata un'errata configurazione dei meccanismi di autenticazione della posta elettronica (DMARC, DKIM e SPF) sui server di numerosi soggetti istituzionali, prontamente allertati dal CSIRT Italia.
- Nel corso del mese, in continuità con quanto già osservato nel mese precedente, si è registrata una ulteriore sensibile attenuazione delle campagne di **hacktivism**, riconducibili al contesto del conflitto russo-ucraino, che hanno preso di mira l'Italia dal dicembre 2024 al febbraio 2025. In particolare, si rileva una **diminuzione** di circa il 90% degli attacchi DDoS e dell'80% degli attacchi di **defacement** rispetto ai livelli osservati nel mese precedente.
- Nel corso delle attività di monitoraggio svolte sulle principali piattaforme online di scambio e condivisione illecita di **data breach** è stata rilevata l'esposizione di dati riferibili al social network **X**, con particolare riferimento al mome utente ed e-mail utilizzati per l'accesso alla piattaforma. L'esposizione è stata comunicata ai soggetti istituzionali interessati.
- Nel mese di aprile 2025 sono stati rilevati **24 attacchi ransomware**, con un **aumento** del 30% rispetto al periodo precedente. Tra gli incidenti più significativi si segnala la compromissione di un fornitore di servizi digitali, con impatti diretti su diverse pubbliche amministrazioni locali. Un secondo episodio ha interessato un laboratorio diagnostico di una struttura ospedaliera, con ripercussioni sulla continuità operativa dei servizi sanitari.
- I **vettori di attacco** maggiormente rilevati ad aprile 2025 sono stati: campagne malevole veicolate tramite e-mail, utilizzo di credenziali valide precedentemente compromesse e sfruttamento di vulnerabilità note.
- È stata condotta dal CSIRT Italia un'attività di analisi finalizzata all'individuazione di prodotti **SAP** potenzialmente compromessi a seguito dello sfruttamento della vulnerabilità CVE-2024-31324, attraverso la quale attori malevoli avrebbero potuto

installare una **web shell**. Parallelamente, sono stati analizzati anche apparati **Fortinet** esposti su Internet e potenzialmente compromessi a seguito di una campagna di sfruttamento delle vulnerabilità CVE-2022-42475, CVE-2023-27997 e CVE-2024-21762, con una modalità non precedentemente nota, volta a ottenere accesso persistente in sola lettura ai sistemi esposti.

- Il numero delle nuove CVE pubblicate è in sensibile **aumento** rispetto a marzo.
- Nel mese di aprile 2025, il CSIRT Italia ha inviato **3.733** comunicazioni dirette, effettuate per segnalare potenziali compromissioni o fattori di rischio ad amministrazioni ed imprese italiane;

I NUMERI DI APRILE 2025

- **163** eventi cyber, in **diminuzione** (**–82**);
- **260** vittime, in **diminuzione** (**–531**);
- **116** vittime della constituency[1], in **diminuzione** (**–415**);
- **29** incidenti con impatto confermato, in **diminuzione** (**–52**);
- **426** asset potenzialmente compromessi, in **diminuzione** (**–819**);
- **289** asset potenzialmente vulnerabili, in **diminuzione** (**–172**);
- **67** alert sul sito web del CSIRT Italia, in **aumento** (**+13**);
- **3.733** comunicazioni inviate, in **diminuzione** (**–144**);
- **4.299** nuove CVE, in **aumento** (**+360**).

PRODOTTI VULNERABILI

Di seguito **l'elenco dei prodotti** che ad aprile 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.

- **pgAdmin** (CVE-2025-2945), (CVE-2025-2946) Link all'alert;
- **Ivanti** (CVE-2025-22457) Link all'alert;
- **Craft CMS** (CVE-2025-32432), (CVE-2025-58136) Link all'alert;
- **Broadcom** (CVE-2025-1976) Link all'alert;
- **Erlang** (CVE-2025-32433) Link all'alert;
- **CrushFTP** (CVE-2025-32102 e CVE-2025-32103) Link all'alert;
- **SAP NetWeaver** (CVE-2025-31324) Link all'alert;
- **Gladinet CentreStack e Triofox** (CVE-2025-30406) Link all'alert;
- **Erlang/OTP** (CVE-2025-32433) Link all'alert;
- **Fortinet FortiSwitch** (CVE-2024-48887) Link all'alert;
- **GLPI** (CVE-2025-24801);
- **Kentico Xperience** (CVE-2025-2748);
- **Infodraw Media Relay Service (MRS)** (CVE-2025-43928);
- **Adobe ColdFusion** (CVE-2025-30290, CVE-2025-30289, CVE-2025-30288, CVE-2025-30287, CVE-2025-30286, CVE-2025-30285, CVE-2025-30284, CVE-2025-30282, CVE-2025-30281, CVE-2025-24447 e CVE-2025-24446) Link all'alert.

Maggiori dettagli nelle sezioni 3 e 5.

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.

[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.

IL 2025 FINORA

Nei primi 4 mesi del 2025 (1 gennaio 2025 - 30 aprile 2025), rispetto allo stesso periodo del 2024 (1 gennaio - 30 aprile 2024) l'ACN ha registrato [2]:

- **915 eventi** cyber, in **aumento** del **36**% rispetto ai **674** dei primi 4 mesi del 2024;
- **205 incidenti** cyber, in **diminuizione** del **-24**% rispetto ai **270** dei primi 4 mesi del 2024;
- **1.579 vittime**, in **aumento** del **31**% rispetto alle **1.203** dei primi 4 mesi del 2024;
- **345 DDoS**, in **aumento** del **107**% rispetto ai **167** dei primi 4 mesi del 2024;
- **309 rivendicazioni di DDoS** da parte di gruppi di attivisti in danno di soggetti italiani, in **aumento** del **192**% rispetto alle **106** dei primi 4 mesi del 2024. NoName057(16) il gruppo più attivo con il **42,3**% degli attacchi, seguito da Dark Storm Team (6,5%);
- **118 ransomware**, in **aumento** del **64**% rispetto ai **72** dei primi 4 mesi del 2024;
- **73 rivendicazioni di ransomware** da parte di gruppi criminali in danno di soggetti italiani, in **aumento** rispetto alle **51** dei primi 4 mesi del 2024. Akira e Sarcoma Group gli attori ransomware più attivi;
- **16.957 asset potenzialmente vulnerabili**, in **aumento** del **443**% rispetto ai **3.120** dei primi 4 mesi del 2024.

I **settori** con più vittime registrati dal CSIRT Italia nei primi 4 mesi del 2025 sono stati:

- **Pubblica amministrazione centrale** (264 vittime);
- **Pubblica amministrazione locale** (225 vittime);
- **Telecomunicazioni** (152 vittime).

Nei primi 4 mesi del 2024 furono: Pubblica amministrazione centrale (191 vittime), Telecomunicazioni (125 vittime) e Pubblica amministrazione locale (114 vittime).

Le **tipologie di minacce** più frequentemente registrate nei primi 4 mesi del 2025 sono state:

- **DDoS** (345 attacchi);
- **Esposizione dati** (122 occorrenze);
- **Phishing** (118 occorrenze).

Nei primi 4 mesi del 2024 furono: DDoS (167 attacchi), Brand Abuse (119 eventi) e Phishing (109 occorrenze).

[2] Si noti che determinati incrementi sono ascrivibili anche all'aumentata capacità del CSIRT Italia di rilevare eventi, incidenti e vulnerabilità, nonché al modificato impianto normativo.

2 EVENTI ED INCIDENTI

Ad aprile 2025 sono stati individuati **163** eventi cyber, in **diminuzione** del 33% rispetto al mese precedente. Questi ultimi hanno avuto un **impatto su 202 soggetti nazionali**: 116 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 163 eventi cyber, **29 sono stati classificati quali incidenti**, in **diminuzione** del 64% rispetto a marzo.

La Figura 1 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.

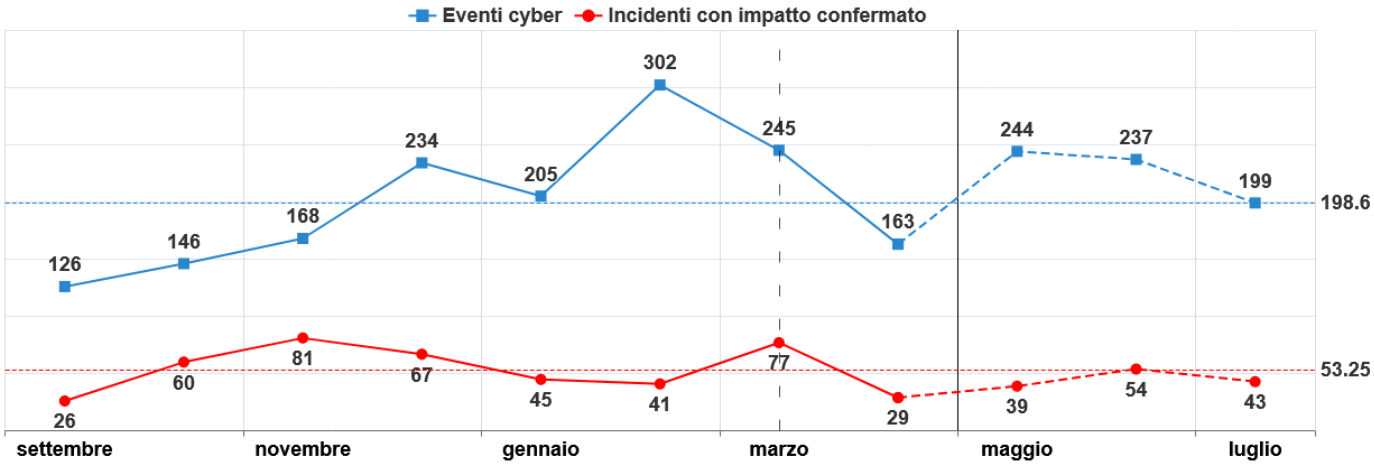

Figure 1 - *andamento attività reattive e analisi previsionale*

[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 2 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).

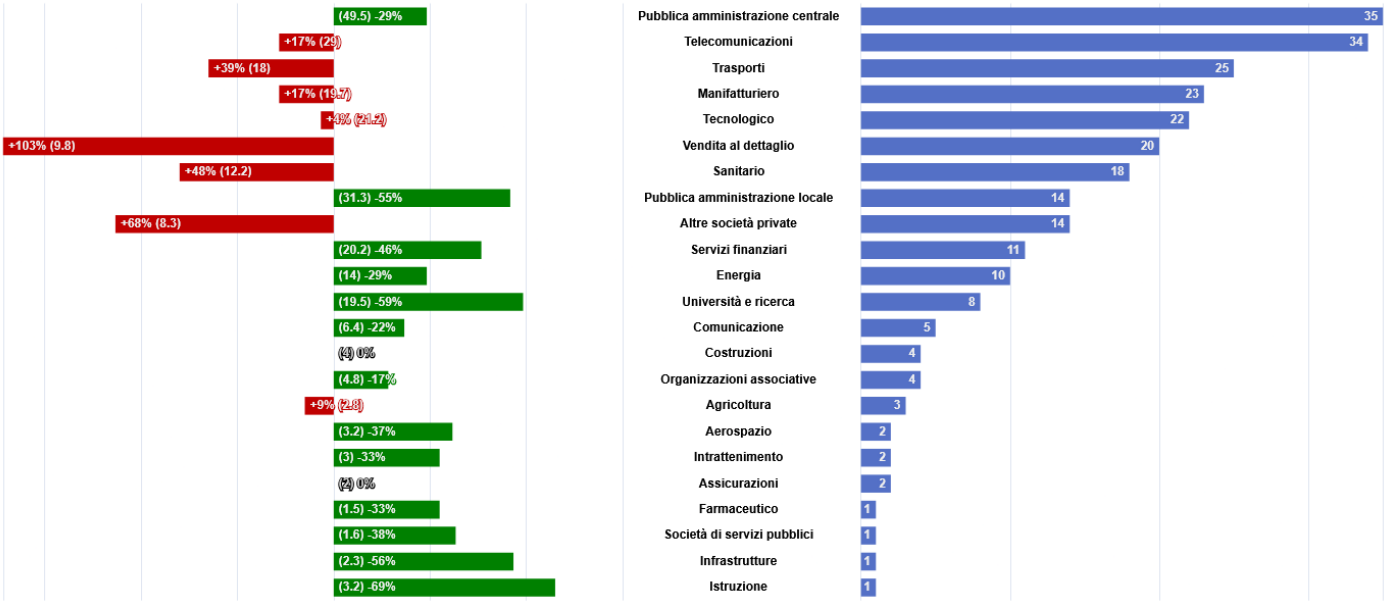

Figure 2 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente*

2.2 Tipologia di minacce negli eventi

In figura 3 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) .

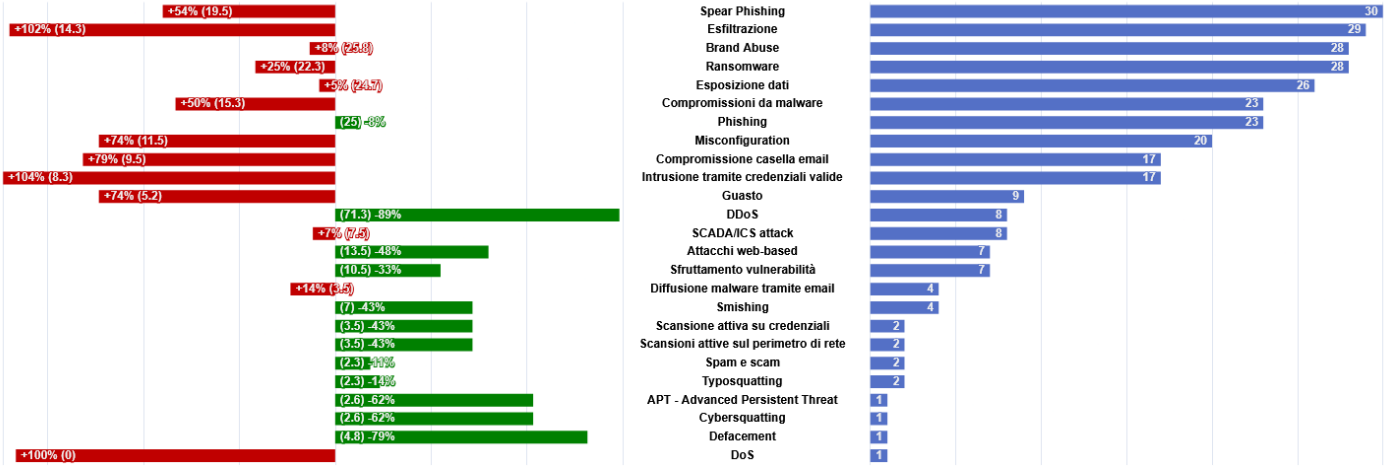

Figure 3 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente*

[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.

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

2.3 Focus constituency

I 163 eventi cyber hanno interessato **116** soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

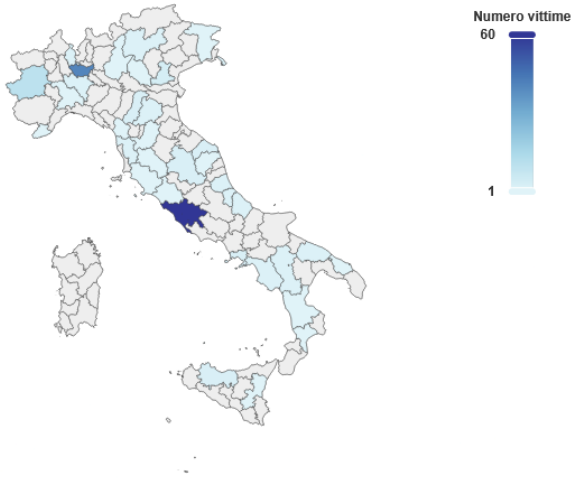

Figure 4 - *distribuzione delle vittime appartenenti alla constituency*

In figura 5 si riportano i settori di afferenza delle vittime, evidenziando, altresì, la tipologia di minaccia rilevata. Si ricorda che ad un evento possono essere associate più tipologie di minaccia.

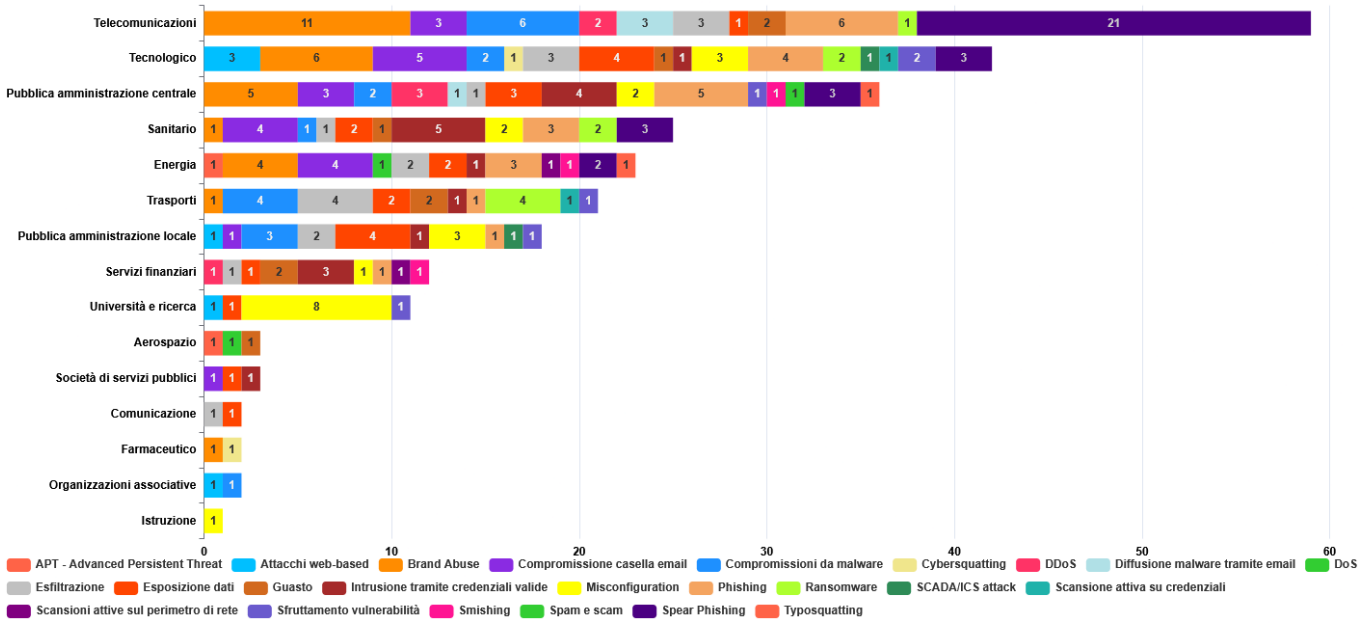

Figure 5 - *tipologia di minacce con impatto sui settori della constituency*

3 VULNERABILITÀ

Ad aprile 2025 sono state pubblicate[6] **4.299** nuove CVE, in **aumento** (**+360**) rispetto a marzo. Di queste, **384** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (**+150**), e per **0** CVE è stato rilevato lo sfruttamento attivo, in **diminuzione** (**–18**) rispetto a marzo.

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 **67**. Oltre al consueto aggiornamento mensile di Microsoft (link) all'alert sul sito web), che ha risolto un totale di 127 nuove vulnerabilità (1 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **pgAdmin**: aggiornamento che risolve 2 vulnerabilità di sicurezza, con gravità "critica" nella nota piattaforma di amministrazione e sviluppo open source per PostgreSQL. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato remoto di eseguire codice arbitrario sul sistema interessato (stima di impatto sistemico **79,35/100**). Link all'alert del 07/04/2025;
- **Ivanti**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-22457 – già sanata dal vendor a febbraio 2025 – per i prodotti Ivanti Connect Secure (ICS) e Pulse Connect Secure (PCS) (stima di impatto sistemico **78,20/100**). Link all'alert del 03/04/2025;
- **Craft CMS**: rilevato lo sfruttamento attivo in rete delle CVE-2025-32432 e CVE-2024-58136 relative ai prodotti Craft CMS e Yii framework (stima di impatto sistemico **73,07/100**). Link all'alert del 29/04/2025;
- **Broadcom**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-1976 – già sanata dal vendor ad aprile 2025 – per il prodotto Brocade Fabric OS (stima di impatto sistemico **72,69/100**). Link all'alert del 29/04/2025;
- **Erlang**: rilevata una vulnerabilità critica nella componente server SSH di Erlang/OTP, una tecnologia utilizzata nell'ambito delle telecomunicazioni, nei dispositivi IoT e nelle piattaforme di messaggistica in tempo reale. (stima di impatto sistemico **67,37/100**). Link all'alert del 17/04/2025;

[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/`.

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 6 è riportato il numero delle vulnerabilità rilevate distribuite tra i principali vendor.

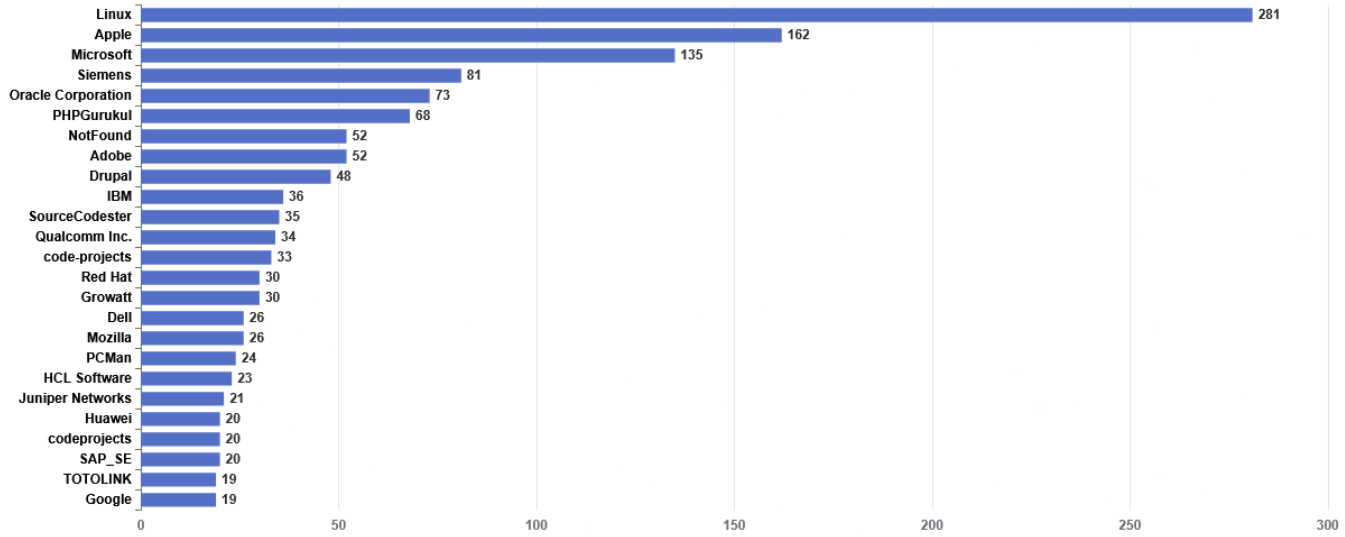

Figure 6 - *top 25 produttori affetti da vulnerabilità nel mese*

In Figura 7 è riportato, invece, il numero delle vulnerabilità rilevate distribuite tra i principali prodotti.

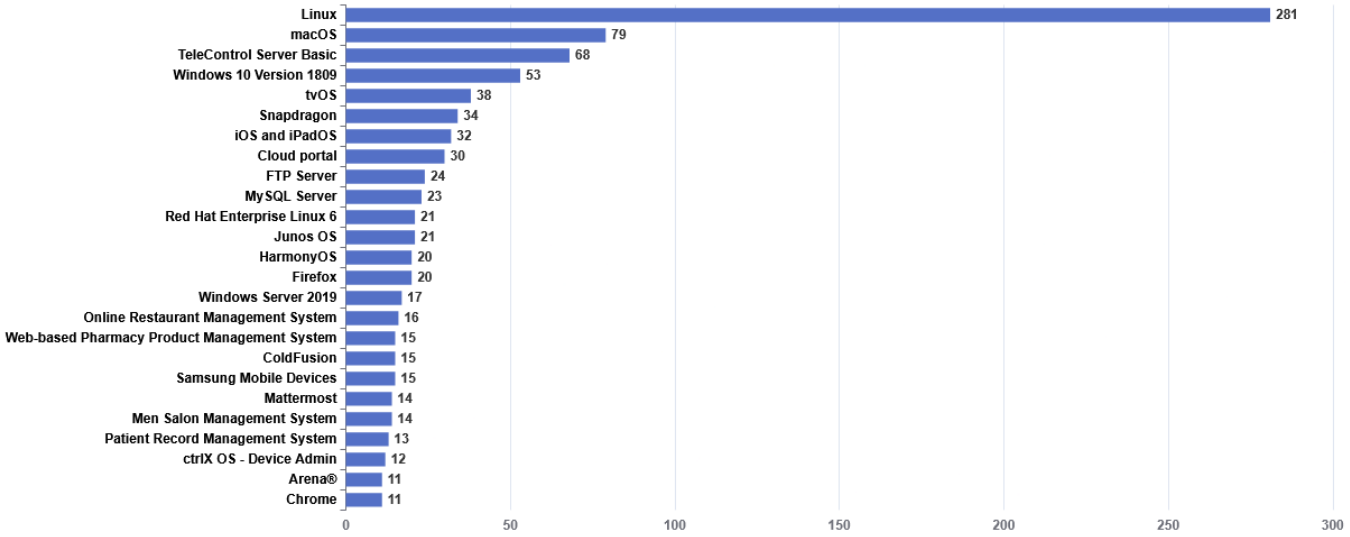

Figure 7 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

In Figura 8 sono riportate le 5 tipologie di weakness (Common Weakness Enumeration – CWE) più rilevate.

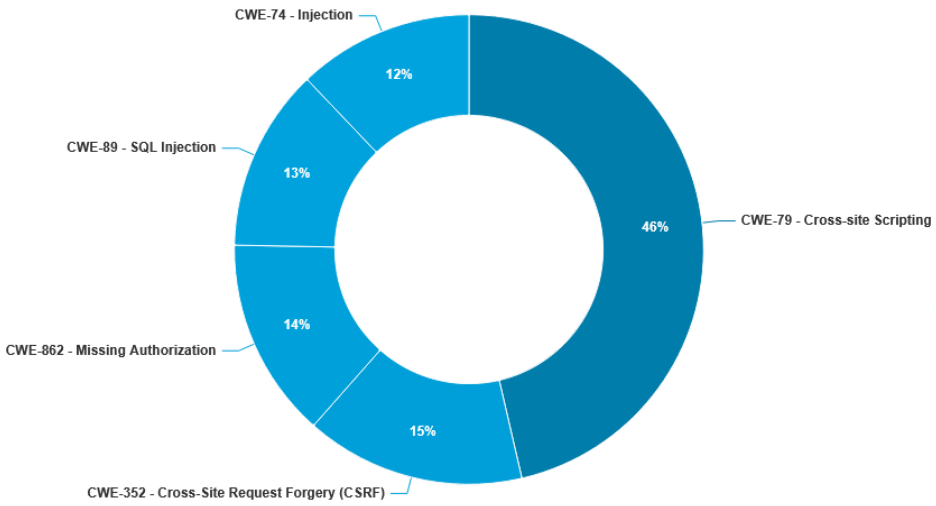

Figure 8 - *top 5 CWE nel mese*

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	**SAP SE**
Prodotti e versioni vulnerabili	**SAP NetWeaver (Visual Composer development server) versione VCFRAMEWORK 7.50**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di inviare file eseguibili malevoli al server.**
Data di rilascio CVE	**24/04/2025 modificata il 01/05/2025**
CVSS score 3.x	**10.0 CRITICAL**
EPSS max score	**0.58**

Table 1 - *CVE-2025-31324*

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

Vendor	**BentoML**
Prodotti e versioni vulnerabili	**BentoML versioni dalla 1.3.4 fino alla 1.4.2**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo.**
Data di rilascio CVE	**04/04/2025 modificata il 07/04/2025**
CVSS score 3.x	**9.8 CRITICAL (valore assegnato da GitHub, Inc.)**
EPSS max score	**0.49**

Table 2 - *CVE-2025-27520*

Vendor	**pgadmin-org**
Prodotti e versioni vulnerabili	**pgadmin4 tutte le versioni fino alla 9.1**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante autenticato di eseguire codice malevolo.**
Data di rilascio CVE	**03/04/2025 modificata il 07/04/2025**
CVSS score 3.x	**9.9 CRITICAL**
EPSS max score	**0.52**

Table 3 - *CVE-2025-2945*

4 MINACCIA

In questa sezione si riportano, per quanto riguarda il malware, il numero degli Indicatori di Compromissione (IoC)[8]condivisi dal CSIRT Italia tramite piattaforma MISP (Malware Information Sharing Platform)[9], per il ransomware e il DDoS un'analisi sulle rivendicazioni in Italia ed UE.

4.1 Indicatori di Compromissione (IoC) per famiglia di malware

In Figura 9 vengono raggruppati gli IoC condivisi dal CSIRT Italia su MISP, suddivisi per tipologie di malware. La suddivisione per famiglia di malware consente di evidenziare le varianti più diffuse a supporto delle attività di threat intelligence e di rilevamento delle minacce.

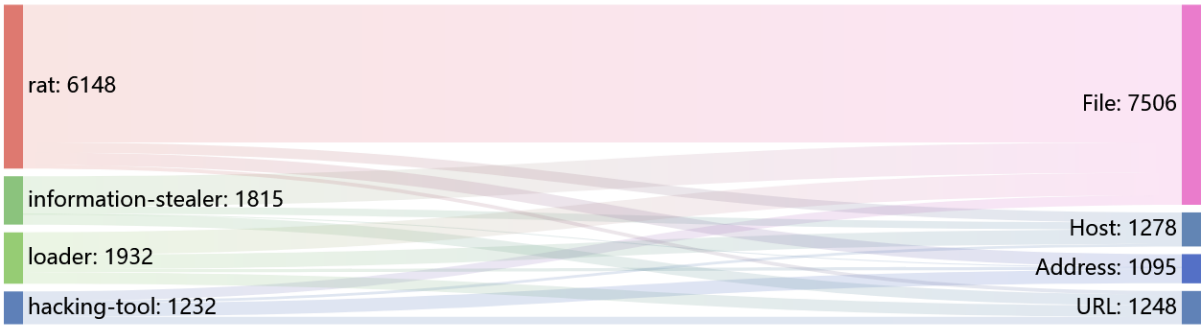

Figure 9 - *numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware*

[8]Indicatore di Compromissione, è un marcatore digitale che 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 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 aprile 2025 ha permesso di individuare **22** rivendicazioni di attacchi ransomware a danno di soggetti italiani. I gruppi più attivi sono stati **Akira** e **Qilin**.

Il grafico in Figura 10 mostra l'andamento delle rivendicazioni nel corso degli ultimi 12 mesi.

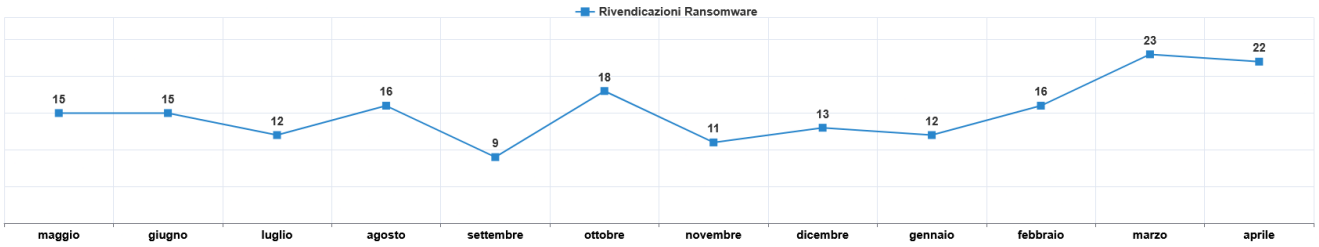

Figure 10 - *andamento delle rivendicazioni Ransomware*

Il grafico in Figura 11 mostra i gruppi più attivi in termini di rivendicazioni in Italia.

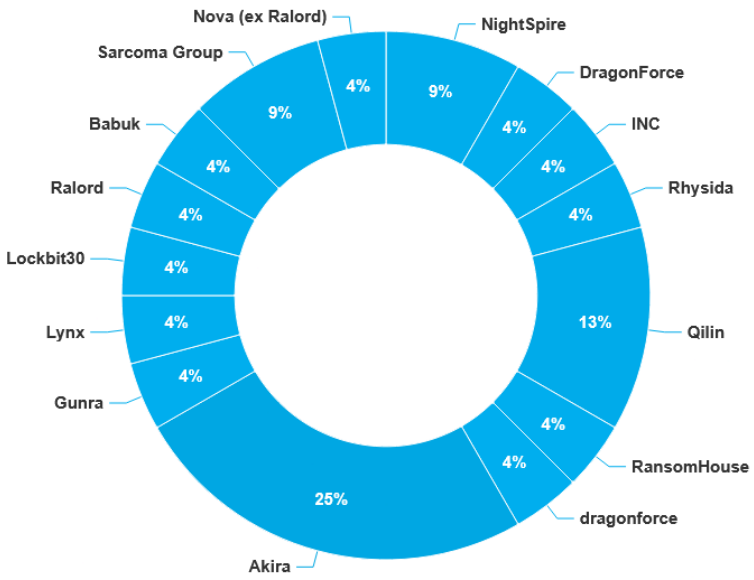

Figure 11 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

4.3 Rivendicazioni DDoS

A aprile 2025 sono state individuate[10] **8** rivendicazioni di attacchi DDoS in danno di soggetti italiani.
I gruppi più attivi su scala globale sono stati **NoName057(16)** e **Dark Storm Team**

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

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

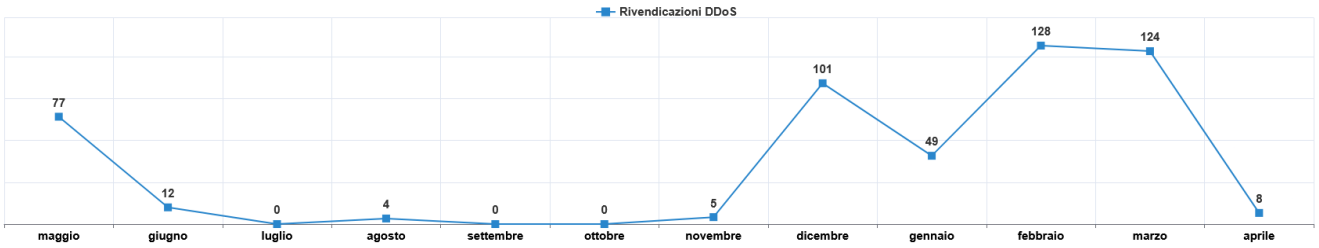

Figure 12 - *andamento delle rivendicazioni DDoS*

Il grafico in Figura 13 mostra i gruppi più attivi in termini di rivendicazioni.

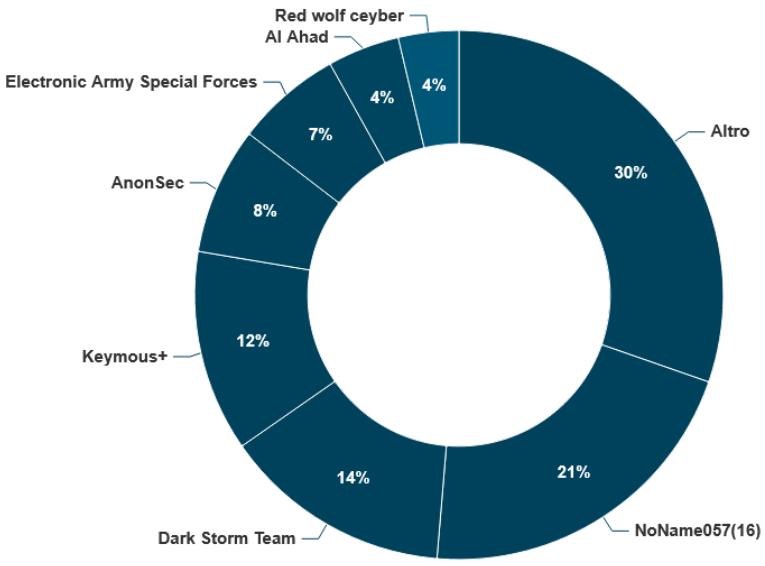

Figure 13 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[11], 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 aprile 2025 sono state diramate un totale di **177** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **275** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **Ivanti Connect Secure e Policy 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 sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **CrushFTP** (CVE-2025-32102 e CVE-2025-32103): tali vulnerabilità – rispettivamente di tipo *Side Request Forgery* e *Path Traversal* – permetterebbero a un eventuale attaccante remoto, per mezzo della manipolazione di specifici parametri nella URL, di testare la disponibilità di porte in ascolto su host remoti arbitrari raggiungibili dal server affetto (CVE-2025-32102) e scaricare e/o accedere a file/percorsi arbitrari su host remoti all'interno della stessa rete del sistema affetto o su Internet (CVE-2025-32103). Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **SAP NetWeaver** (CVE-2025-31324): tale vulnerabilità – di tipo *Unrestricted File Upload* – consentirebbe a un eventuale attaccante non autenticato di caricare file arbitrari all'interno delle installazioni aventi il componente *Visual Composer* installato e il modulo *Metadata Uploader* attivo. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Erlang/OTP** (CVE-2025-32433): tale vulnerabilità – di tipo *Improper Authentication* – permetterebbe a un attaccante con accesso al relativo servizio SSH affetto l'esecuzione da remoto di codice e comandi arbitrari sfruttando una falla

[11] 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.

nella gestione dei messaggi presente nel protocollo SSH. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;

- **GLPI** (CVE-2025-24801): tale vulnerabilità - di tipo *Unrestricted File Upload* - potrebbe consentire a un eventuale attaccante autenticato di eseguire codice arbitrario da remoto sul sistema interessato tramite opportuni file PHP previamente caricati o, alternativamente, sfruttando l'esistenza di specifici plugins disponibili nel Marketplace.
- **Adobe ColdFusion** (CVE-2025-30290, CVE-2025-30289, CVE-2025-30288, CVE-2025-30287, CVE-2025-30286, CVE-2025-30285, CVE-2025-30284, CVE-2025-30282, CVE-2025-30281, CVE-2025-24447 e CVE-2025-24446): tali vulnerabilità, permetterebbero a un eventuale attaccante di ottenere l'accesso non autorizzato a file, di eludere i sistemi di sicurezza del prodotto e di eseguire codice arbitrario nelle installazioni affette. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Kentico Xperience** (CVE-2025-2748): tale vulnerabilità – di tipo *Cross Site Scripting (XSS)* – permetterebbe il caricamento di script malevoli (*Stored XSS*) all'interno delle installazioni affette, consentendo a un eventuale attaccante di eseguire codice arbitrario nel contesto degli utenti che accedono a tali risorse, ad esempio, sfruttando tecniche di *Social Engineering*.
- **Gladinet CentreStack e Triofox** (CVE-2025-30406): tale vulnerabilità - di tipo *Insecure Deserialization* - permetterebbe a un eventuale attaccante di eseguire codice arbitrario da remoto tramite l'invio di un richieste opportunamente predisposte. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Fortinet FortiSwitch** (CVE-2024-48887): tale vulnerabilità - di tipo *Weak Authentication* - consentirebbe ad un eventuale attaccante non autenticato di modificare la password di amministrazione per mezzo di una richiesta HTTP appositamente predisposta. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Infodraw Media Relay Service (MRS)** (CVE-2025-43928): tale vulnerabilità – di tipo *Path Traversal* – potrebbe permettere a un eventuale attaccante non autenticato di cancellare o accedere a file arbitrari sui sistemi affetti, anche contenenti informazioni sensibili come credenziali di amministratore (conservate in formato MD5).

In Figura 14 viene riportata la distribuzione delle segnalazioni per tipologia di soggetto.

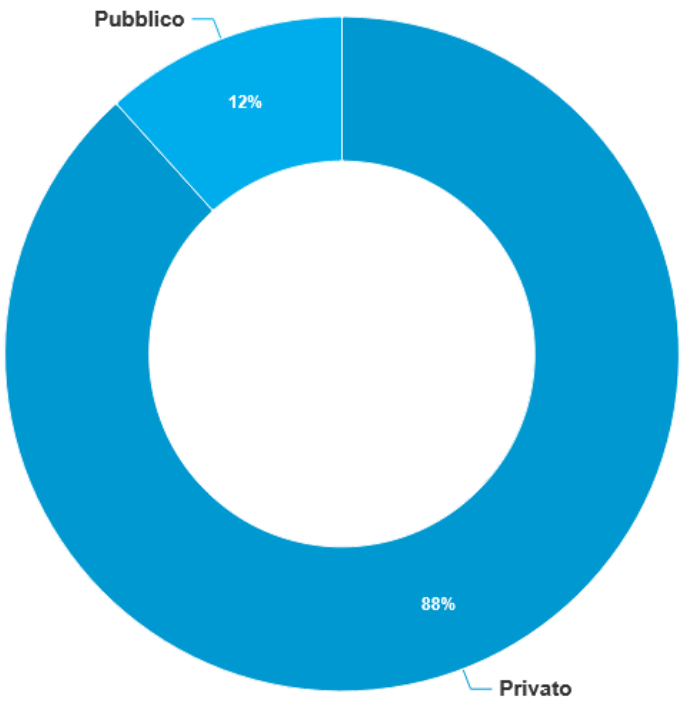

Figure 14 - *distribuzione delle segnalazioni per tipologia di soggetto*

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

aprile 2025