Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

Servizio Operazioni
e gestione delle crisi cyber

febbraio 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

- A febbraio 2025 si è registrato un **aumento** del numero di **eventi** mentre il numero di **incidenti** è rimasto sostanzialmente nella **media** del semestre.
- I settori con il maggior numero di vittime registrate sono stati: **Pubblica amministrazione locale**, **Pubblica amministrazione centrale** e **Energia**. L'aumento degli eventi nel settore della **Pubblica Amministrazione Centrale** è riconducibile agli attacchi DDoS.
- Nel mese di febbraio, l'Italia ha registrato un'intensificazione delle attività di **hacktivismo**, caratterizzate da attacchi DDoS ed alcuni defacement contro soggetti pubblici e privati. Le operazioni, riconducibili a gruppi con finalità politico-ideologiche, hanno visto il coinvolgimento di diversi collettivi filorussi e di altri attori legati principalmente alla causa palestinese.
- Le campagne offensive sono state indirizzate contro siti web della pubblica amministrazione, nonché di aziende operanti nei settori dei trasporti e dei servizi finanziari. Tali azioni sono state impiegate come mezzo per ottenere visibilità mediatica e amplificare il messaggio propagandistico delle rivendicazioni. A conferma di ciò, **dei 181 attacchi DDoS rilevati nel periodo, solo il 3% ha determinato disservizi, che si sono rivelati comunque di carattere temporaneo** (tipicamente circa un'ora di irraggiungibilità della risorsa attaccata).
- Tra le attività riconducibili a gruppi hacktivisti, sono state osservate operazioni di **defacement** di alcuni siti web. Le azioni, finalizzate unicamente alla diffusione di messaggi propagandistici, hanno prodotto impatti limitati, colpendo prevalentemente siti web di piccole realtà aziendali, in maggioranza nel settore tecnologico, caratterizzate da livelli di protezione ridotti.
- L'aumento dei numeri relativi al **ransomware** è dovuto, invece, ad un solo attacco che ha compromesso la disponibilità dei sistemi informatici di un'azienda del settore energetico e la conseguente erogazione dei servizi ai suoi clienti, determinando così disservizi su altri operatori del settore.
- i gruppi più attivi per numero di rivendicazioni **ransomware** sono stati **FOG** e **Akira**.
- I **vettori di attacco** maggiormente rilevati a febbraio 2025 sono le campagne malevole veicolate tramite e-mail, lo sfruttamento di vulnerabilità note e l'utilizzo di credenziali valide precedentemente compromesse.
- Il numero delle nuove CVE pubblicate è in sensibile **diminuzione** rispetto a gennaio.

I NUMERI DI FEBBRAIO 2025

- **302** eventi cyber, in **aumento** (**+97**);
- **324** vittime, in **aumento** (**+123**);
- **172** vittime della constituency[1] , in **aumento** (**+90**);
- **48** incidenti con impatto confermato, **stabile** (**+1**);
- **1.207** asset potenzialmente vulnerabili, in **diminuzione** (**–13.793**);
- **51** alert sul sito web del CSIRT Italia, in **aumento** (**+4**);
- **3.386** nuove CVE, in **diminuzione** (**–1.031**).

PRODOTTI VULNERABILI

Di seguito **l'elenco dei prodotti** che a febbraio 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.

- **Parallels Inc.** (CVE-2024-34331) Link all'alert;
- **Mattermost** (CVE-2025-25279) Link all'alert;
- **Microsoft** (CVE-2025-24989) Link all'alert;
- **PostgreSQL** (CVE-2025-1094)Link all'alert;
- **Fortinet** (CVE-2025-24472, CVE-2025-24470, CVE-2024-40591, CVE-2024-35279) Link all'alert;
- **Ivanti Connect Secure e Policy Secure** (CVE-2024-10644, CVE-2025-22467, CVE-2024-38657 e CVE-2024-13813) Link all'alert;
- **GFI KerioControl** (CVE-2024-52875, CVE-2024-52875)
- **Zyxel DSL CPE** (CVE-2025-0890, CVE-2024-40890, CVE-2024-40891); Link all'alert;
- **Exim** (CVE-2025-26794) Link all'alert;
- **Palo Alto PAN-OS Management Interface** (CVE-2025-0108); Link all'alert;
- **Cacti** (CVE-2025-22604) Link all'alert;
- **SonicWall Firewall** (CVE-2024-53704) Link all'alert;
- **Craft CMS** (CVE-2025-23209);
- **Xwiki** (CVE-2025-24893) Link all'alert;
- **Paessler PRTG Network Monitor** (CVE-2018-19410);
- **NAKIVO Backup & Replication** (CVE-2024-48248) 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.

2 EVENTI ED INCIDENTI

A febbraio 2025 sono stati individuati **302** eventi cyber, in **aumento** del 47% rispetto al mese precedente. Questi ultimi hanno avuto un **impatto su 247 soggetti nazionali**: 172 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 302 eventi cyber, **48 sono stati classificati quali incidenti**, in **aumento** del 2% rispetto a gennaio.

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[2], riferita ai successivi 3 mesi.

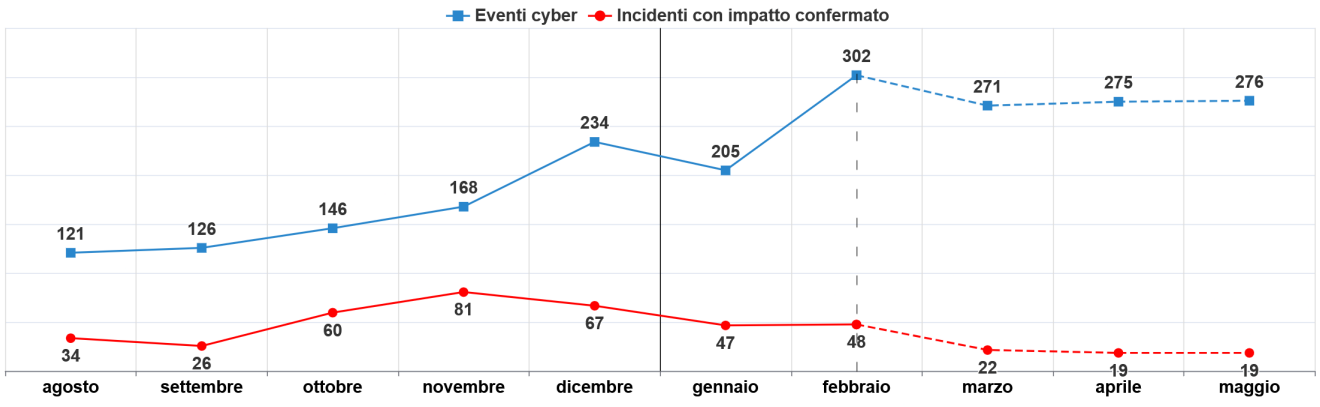

Figura 1 - *andamento attività reattive e analisi previsionale*

[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 2 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).

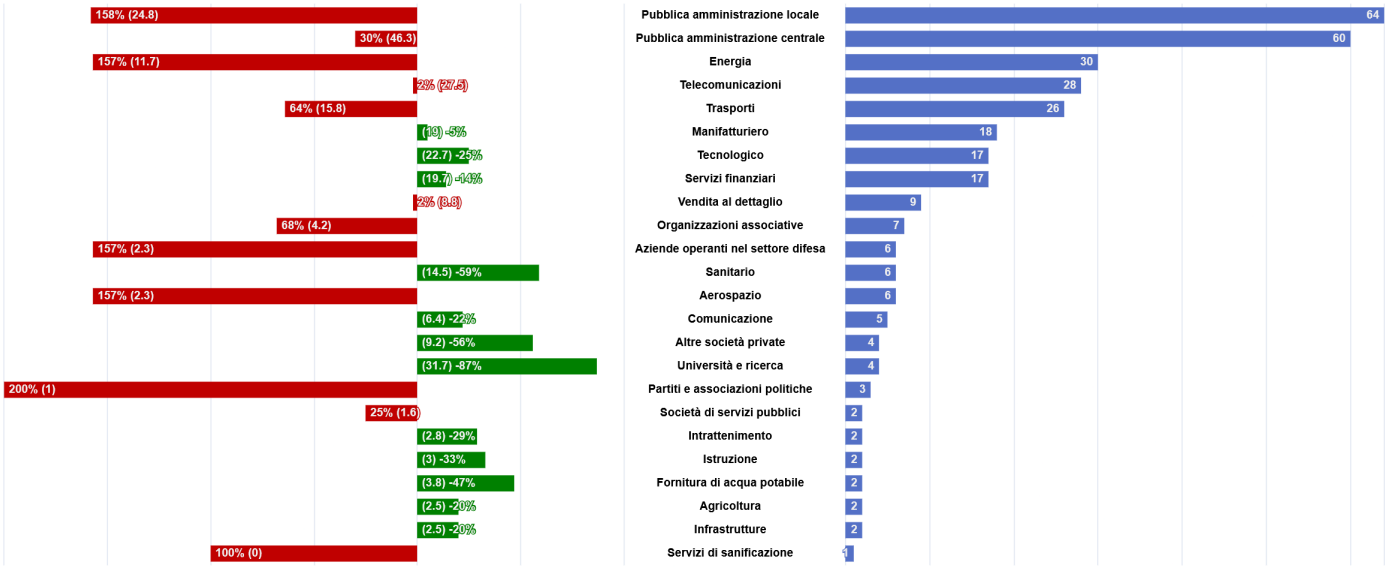

Figura 2 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente*

[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 3 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).

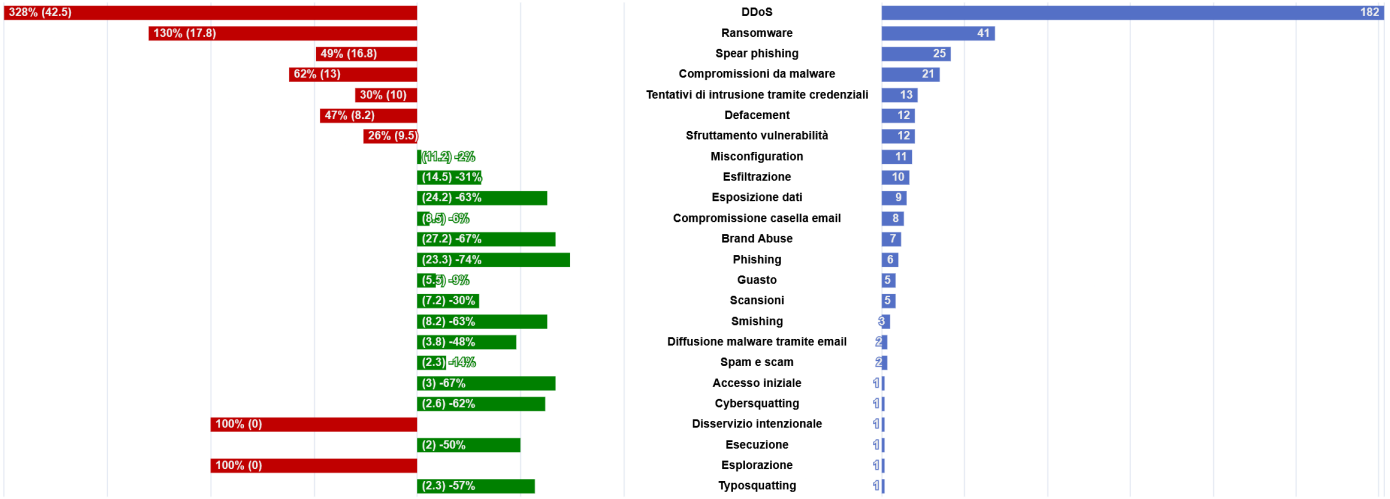

Figura 3 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente*

2.3 Focus constituency

I 302 eventi cyber hanno interessato **172** soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

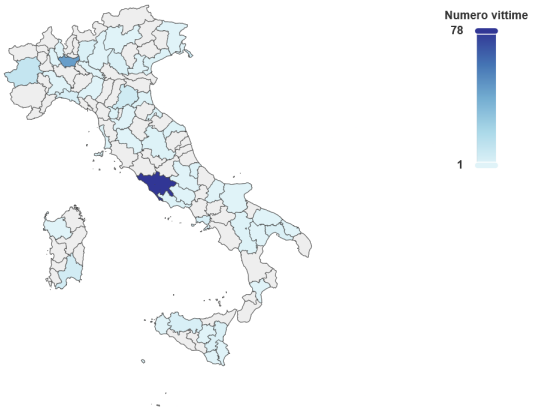

Figura 4 - *distribuzione geografica delle vittime appartenenti alla constituency*

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

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.

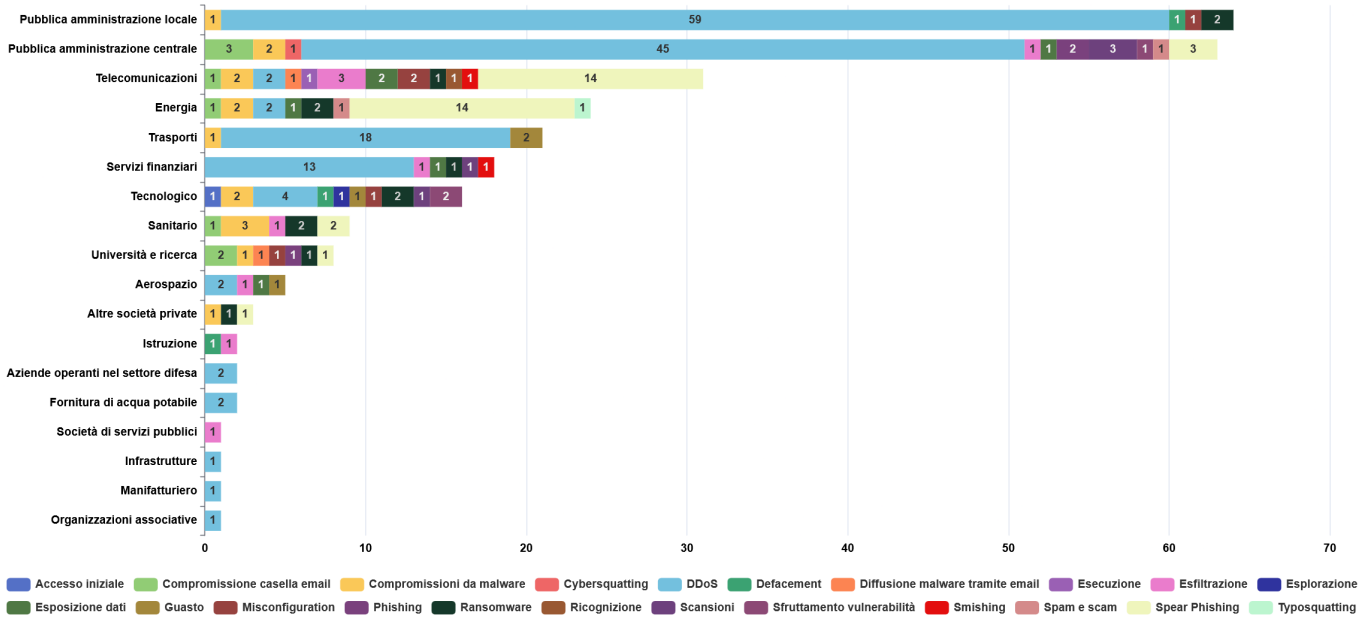

Figura 5 - *tipologia di minacce con impatto sui settori della constituency*

3 VULNERABILITÀ

A febbraio 2025 sono state pubblicate[5] **3.386** nuove CVE, in **diminuzione** (**–1.031**) rispetto a gennaio. Di queste, **158** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–15**), e per **12** CVE è stato rilevato lo sfruttamento attivo, in **aumento** (**+4**) rispetto a gennaio.

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 **51**. Oltre al consueto aggiornamento mensile di Microsoft (link all'alert sul sito web), che ha risolto un totale di 66 nuove vulnerabilità (4 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Parallels Inc.**: ricercatori di sicurezza hanno recentemente rilevato 2 vulnerabilità 0-day in Parallels Desktop, software di virtualizzazione per sistemi macOS. Tali vulnerabilità - di tipo "Privilege Escalation" – sono correlate alla CVE-2024-34331, non correttamente sanata dal vendor (stima di impatto sistemico **84,74/100**). Link all'alert del 26/02/2025;
- **Mattermost**: rilevate 5 vulnerabilità, di cui 3 con gravità "critica", in Mattermost, piattaforma di collaborazione open-source progettata per la comunicazione interna di organizzazioni e aziende. Tali vulnerabilità, qualora sfruttate, potrebbero permettere ad un utente malintenzionato di accedere ad informazioni sensibili e/o ottenere l'accesso arbitrario a file sui dispositivi target (stima di impatto sistemico **79,35/100**). Link all'alert del 25/02/2025;
- **Microsoft**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-24989 – già sanata dal vendor – relativa al prodotto Microsoft Power Pages, piattaforma per la creazione, l'hosting e la gestione di siti web. Tale vulnerabilità potrebbe consentire a un utente malintenzionato di elevare i propri privilegi sui sistemi interessati (stima di impatto sistemico **77,17/100**). Link all'alert del 20/02/2025;
- **PostgreSQL**: PostgreSQL Global Development Group ha rilasciato aggiornamenti di sicurezza per risolvere 1 vulnerabilità con gravità "alta" in PostgreSQL (stima di impatto sistemico **77,05/100**). Link all'alert del 14/02/2025;

[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/`.

- **Fortinet**: rilevate nuove vulnerabilità in vari prodotti, di cui quattro con gravità "alta" . Tali vulnerabilità potrebbero permettere l'accesso a informazioni sensibili, l'esecuzione di comandi arbitrari e la possibilità di elevare i privilegi utente sui sistemi interessati (stima di impatto sistemico **77,05/100**). Link all'alert del 12/02/2025.

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

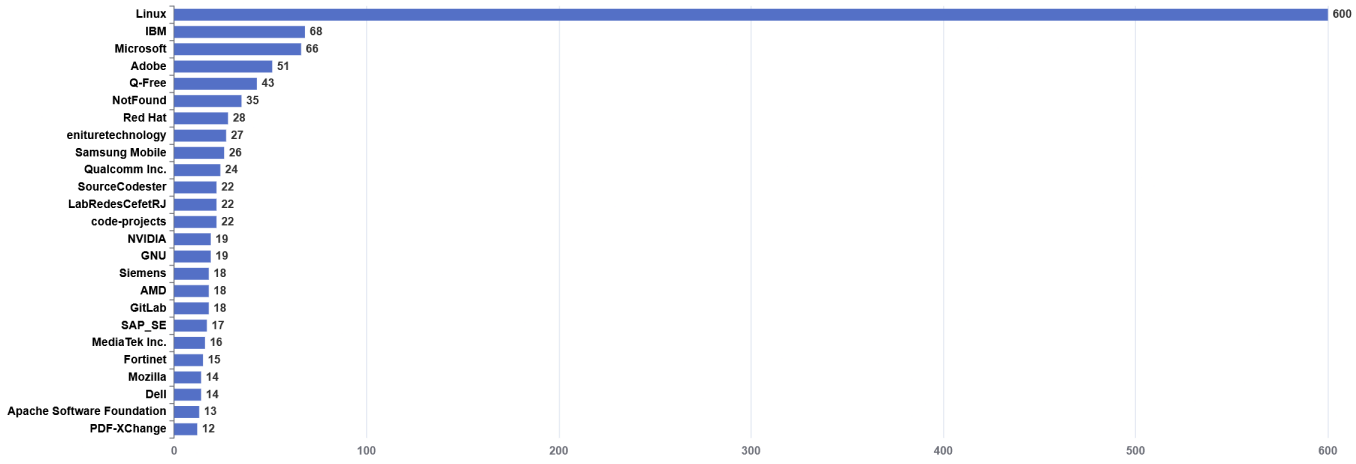

Figura 6 - *top 25 produttori affetti da vulnerabilità nel mese*

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

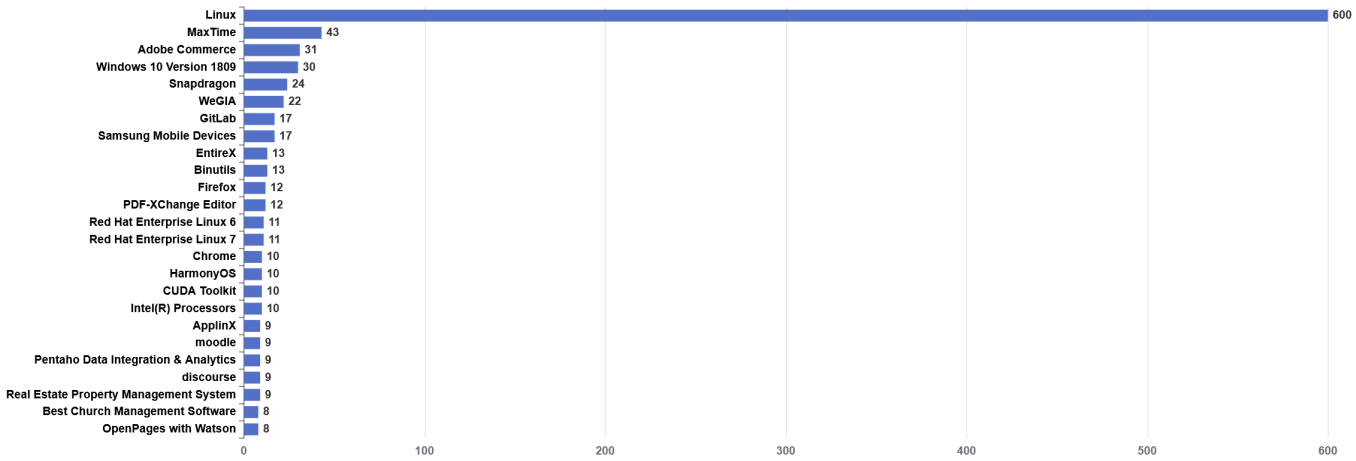

Figura 7 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

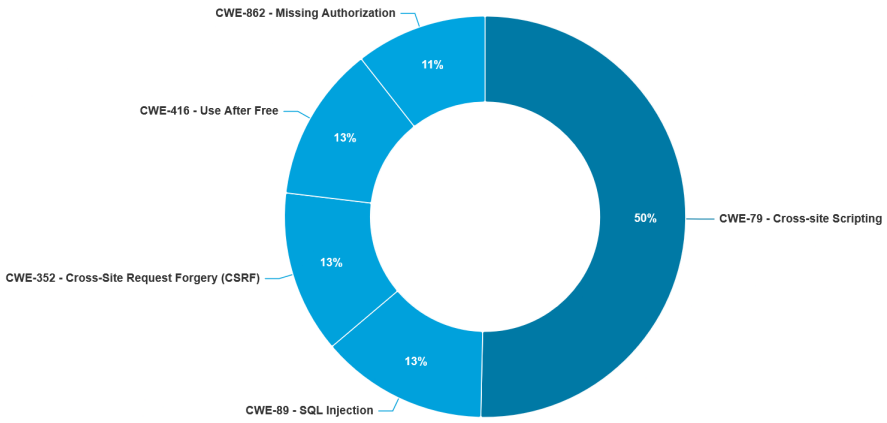

Figura 8 - *top 5 CWE nel mese*

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

Vendor	**Palo Alto Networks**
Prodotti e versioni vulnerabili	**PAN-OS 10.1:** ▪ **Tutte le versioni precedenti la 10.1.14-h9** **PAN-OS 10.2:** ▪ **Tutte le versioni precedenti la 10.2.7-h24** ▪ **Tutte le versioni precedenti la 10.2.8-h21** ▪ **Tutte le versioni precedenti la 10.2.9-h21** ▪ **Tutte le versioni precedenti la 10.2.10-h14** ▪ **Tutte le versioni precedenti la 10.2.11-h12** ▪ **Tutte le versioni precedenti la 10.2.12-h6** ▪ **Tutte le versioni precedenti la 10.2.13-h3** **PAN-OS 11.1:** ▪ **Tutte le versioni precedenti la 11.1.2-h18** ▪ **Tutte le versioni precedenti la 11.1.4-h13** ▪ **Tutte le versioni precedenti la 11.1.6-h1** **PAN-OS 11.2:** ▪ **Tutte le versioni precedenti la 11.2.4-h4** ▪ **Tutte le versioni precedenti la 11.2.5**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante di eludere l'autenticazione all'interfaccia web di gestione ed eseguire script PHP che potrebbero compromettere l'integrità e la confidenzialità del sistema.**
Data di rilascio CVE	**12/02/2025 modificata il 19/02/2025**
CVSS score 3.x	**9.1 CRITICAL**
EPSS max score	**0.95**

Tabella 1 - *CVE-2025-0108*

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

Vendor	**Beyondtrust**
Prodotti e versioni vulnerabili	**Privileged remote access(PRA) tutte le versioni fino alla 24.3.1 Remote support(RS) tutte le versioni fino alla 24.3.1**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire comandi.**
Data di rilascio CVE	**17/12/2024 modificata il 17/02/2025**
CVSS score 3.x	**9.8 CRITICAL**
EPSS max score	**0.87**

Tabella 2 - *CVE-2024-12356*

Vendor	**Sonicwall**
Prodotti e versioni vulnerabili	**▪ Gen7 Firewalls - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W,TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 Con versione di Sonicos: 7.1.1-7058 e precedenti versioni e versione 7.1.2-7019 ▪ Gen7 NSv - NSv 270, NSv 470, NSv 870 Con versione di Sonicos: 7.1.1-7058 e precedenti versioni e versione 7.1.2-7019 ▪ TZ80 Con versione di Sonicos: 8.0.0-8035**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire comandi.**
Data di rilascio CVE	**17/12/2024 modificata il 17/02/2025**
CVSS score 3.x	**9.8 CRITICAL**
EPSS max score	**0.87**

Tabella 3 - *CVE-2024-53704*

4 MINACCIA

In questa sezione si riportano, per quanto riguarda il malware, il numero degli Indicatori di Compromissione (IoC)[7] condivisi dal CSIRT Italia tramite piattaforma MISP (Malware Information Sharing Platform)[8], 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 famiglie 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.

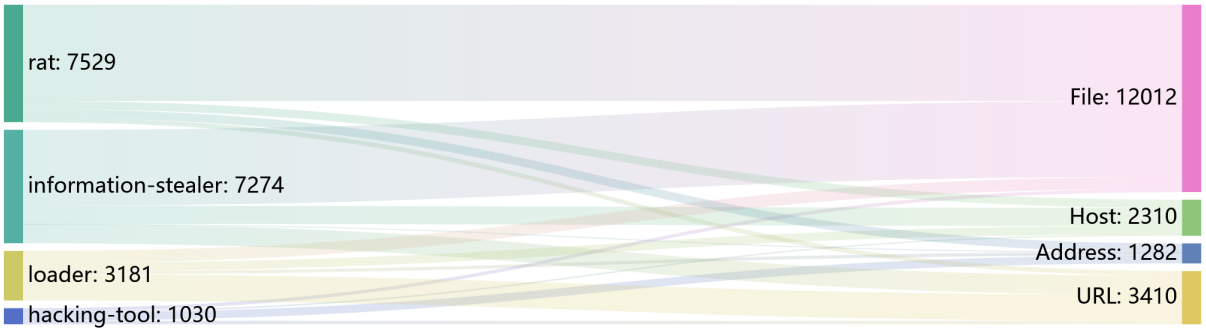

Figura 9 - *Numero di IoC condivisi dal CSIRT Italia suddivisi per famiglie di malware*

[7]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.

[8]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 febbraio 2025 ha permesso di individuare **16** rivendicazioni di attacchi ransomware a danno di soggetti italiani. I gruppi più attivi sono stati **FOG** e **Akira**.

Il grafico in Figura 10 mostra l'andamento delle rivendicazioni nell'anno in corso.

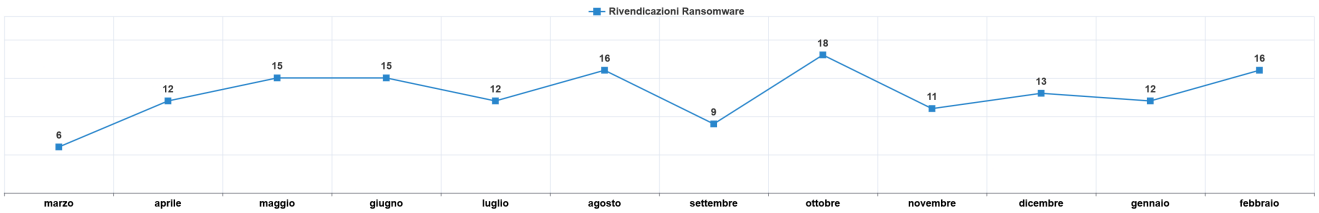

Figura 10 - *andamento delle rivendicazioni Ransomware*

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

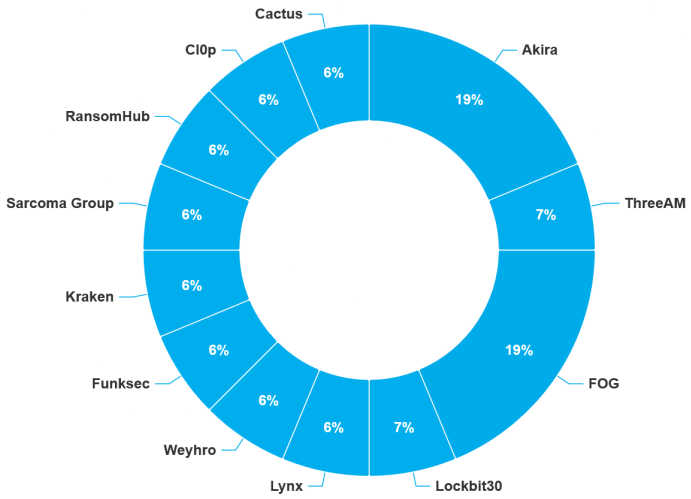

Figura 11 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

*

4.3 Rivendicazioni DDoS

A febbraio 2025 sono state individuate[9] **128** rivendicazioni di attacchi DDoS in danno di soggetti italiani. I gruppi più attivi su scala globale sono stati **nnm057_16** e **noname05716_reborn2**

Il grafico in Figura 12 mostra l'andamento delle rivendicazioni DDoS dell'anno in corso.

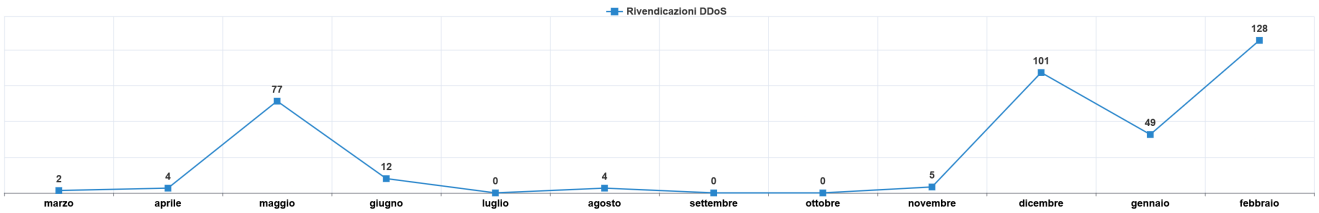

Figura 12 - *andamento delle rivendicazioni DDoS*

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

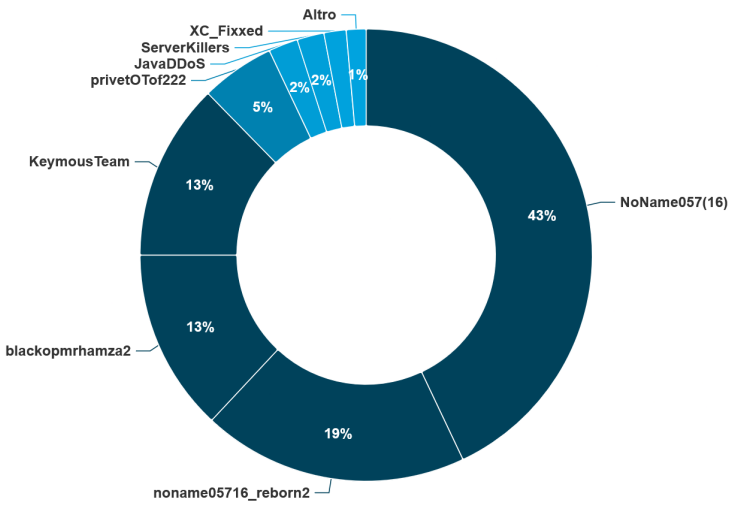

Figura 13 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[10], 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 febbraio 2025 sono state diramate un totale di **469** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **1005** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **PostgreSQL** (CVE-2025-1094): tale vulnerabilità - di tipo *SQL Injection* - potrebbe essere sfruttata da un utente malevolo per eseguire statement SQL arbitrari e codice arbitrario sui sistemi affetti attraverso la funzionalità dei Meta-command. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art. 2 comma 1 della Legge n. 90/2024 in considerazione dello sfruttamento attivo in rete della vulnerabilità.
- **Ivanti Connect Secure e Policy Secure** (CVE-2024-10644, CVE-2025-22467, CVE-2024-38657 e CVE-2024-13813): tali vulnerabilità consentirebbero ad un utente autenticato con privilegi amministrativi l'esecuzione di codice remoto arbitrario e la scrittura illecita di file. Ulteriori dettagli nell'alert rilevati sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione della tipologia del dispositivo impattato (*Accesso Remoto*) e della vulnerabilità (*Remote Code Execution*).
- **Fortinet FortiOS e FortiProxy** (CVE-2025-24472): tale vulnerabilità - di tipo *Authentication Bypass* - potrebbe consentire agli attori malevoli di ottenere i privilegi di super-admin, attraverso delle richieste CSF proxy appositamente predisposte. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale

[10] 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.

comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione della tipologia del dispositivo impattato (*Accesso Remoto*) e della vulnerabilità (*Authentication Bypass*).

- **GFI KerioControl** (CVE-2024-52875, CVE-2024-52875): tale vulnerabilità, consentirebbero di eseguire codice arbitrario da remoto mediante la predisposizione di appositi payload di tipo Reflected XSS (Reflected Cross-Site Scripting). Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione dello sfruttamento attivo in rete della vulnerabilità.
- **Zyxel DSL CPE** (CVE-2025-0890, CVE-2024-40890, CVE-2024-40891): tali vulnerabilità consentirebbero ad utenti malintenzionati, l'esecuzione di codice arbitrario da remoto e/o l'accesso all'interfaccia di gestione del dispositivo utilizzando credenziali di default Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione dello sfruttamento attivo in rete della vulnerabilità.
- **Exim** (CVE-2025-26794): tale vulnerabilità – di tipo *SQL Injection* – potrebbe consentire ad un utente malevolo l'accesso non autorizzato ai dati e la loro manipolazione sulle installazioni affette. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione della disponibilità in rete del relativo Proof-of-Concept (PoC).
- **Palo Alto PAN-OS Management Interface** (CVE-2025-0108): tale vulnerabilità - di tipo *Authentication Bypass* - potrebbe consentire a un utente malintenzionato di bypassare l'autenticazione dell'interfaccia di management e di permettere l'esecuzione di codice PHP specifico. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione dello sfruttamento attivo in rete della vulnerabilità.
- **Cacti** (CVE-2025-22604): tale vulnerabilità - di tipo *OS Command Injection* - consentirebbe a un utente autenticato di eseguire codice arbitrario da remoto e l'accesso abusivo in lettura/scrittura di file - anche sensibili - sui sistemi affetti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione della disponibilità in rete del relativo Proof-of-Concept (PoC).
- **SonicWall Firewall** (CVE-2024-53704): tale vulnerabilità - di tipo *Authentication Bypass* - potrebbe permettere a un utente malintenzionato remoto di eludere i meccanismi di autenticazione sui dispositivi target. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione dello sfruttamento attivo in rete della vulnerabilità.
- **Mattermost** (CVE-2025-25279): tale vulnerabilità – di tipo *Arbitrary File Read* – permetterebbe ad un eventuale attaccante di ottenere l'accesso arbitrario a file sui sistemi affetti dalla vulnerabilità. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione della disponibilità in rete del relativo Proof-of-Concept (PoC).
- **Craft CMS** (CVE-2025-23209): tale vulnerabilità - di tipo *Code Injection* - permetterebbe ad un utente malevolo di eseguire da remoto codice arbitrario, qualora la chiave di sicurezza sia stata precedentemente compromessa.
- **Xwiki** (CVE-2025-24893): tale vulnerabilità - di tipo *Code Injection* - potrebbe permettere ad un utente malevolo l'esecuzione di codice da remoto, tramite l'invio di richieste opportunamente predisposte verso il motore di ricerca predefinito SolrSearch. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione della disponibilità in rete del relativo Proof-of-Concept (PoC).
- **Ivanti Cloud Services Application (CSA)** (CVE-2024-47908): tale vulnerabilità – di tipo *Remote Code Execution* – consentirebbe a un utente malintenzionato, con privilegi di amministratore, l'esecuzione di codice arbitrario da

remota. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;

- **Paessler PRTG Network Monitor** (CVE-2018-19410): tale vulnerabilità - di tipo *Local File Inclusion* - consentirebbe ad un utente non autenticato, tramite la predisposizione di apposite richieste HTTP, la creazione di utenti con privilegi amministrativi. Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione dello sfruttamento attivo in rete della vulnerabilità.
- **NAKIVO Backup & Replication** (CVE-2024-48248): tale vulnerabilità – di tipo *Arbitrary File Read* – potrebbe consentire ad un utente malevolo di accedere a file arbitrari, anche sensibili come credenziali memorizzate, sui sistemi affetti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia; Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2 comma 1 della Legge n. 90/2024 in considerazione della disponibilità in rete del relativo Proof-of-Concept (PoC).

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

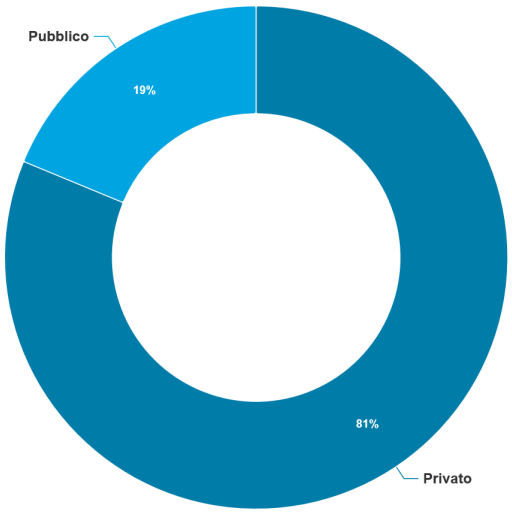

Figura 14 - *Distribuzione delle segnalazioni per tipologia di soggetto*

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

febbraio 2025