Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

Servizio Operazioni
e gestione delle crisi cyber

marzo 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 marzo 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 locale**, **Pubblica amministrazione centrale** e **Tecnologico**. L'aumento degli incidenti nel settore della **Pubblica Amministrazione locale** è il risultato di una violazione dei sistemi di un un fornitore di servizi web. L'incidente ha determinato la compromissione di ventisei siti istituzionali di piccoli comuni, con l'obiettivo, da parte degli attori malevoli, di utilizzarli per la creazione di pagine di phishing.
- Nel mese di marzo 2025 si è osservata una **diminuzione** degli attacchi DDoS, con una riduzione del 60% rispetto al mese precedente. Le attività continuano ad essere condotte da una pluralità gruppi, che operano attraverso forme di alleanza e coordinamento su piattaforme social. Tali dinamiche consentono di amplificare la visibilità delle offensive, rilanciando in maniera coordinata obiettivi e rivendicazioni. I **76 attacchi DDoS** registrati sono stati indirizzati prevalentemente contro i siti web della Pubblica Amministrazione locale e centrale.
- Nel mese di marzo 2025 sono stati rilevati **28 attacchi ransomware**, alcuni anche in danno di soggetti all'interno della Constituency. I gruppi più attivi per numero di rivendicazioni sono stati **RansomHub** e **Lockbit30**.
- Nel corso del mese sono state rilevate e segnalate esposizioni non autorizzate di dati relativi a piattaforme di streaming, servizi di e-commerce e amministrazioni pubbliche.
- I **vettori di attacco** maggiormente rilevati a marzo 2025 sono stati: campagne malevole veicolate tramite e-mail, utilizzo di credenziali valide precedentemente compromesse e sfruttamento di vulnerabilità note.
- Il numero delle nuove CVE pubblicate è in sensibile **aumento** rispetto a febbraio.
- Nel mese di marzo 2025, il CSIRT Italia ha inviato **3.877** comunicazioni dirette, effettuate per segnalare potenziali compromissioni o fattori di rischio ad amministrazioni ed imprese italiane;
- A marzo 2025 è stato rilevato un incremento del numero di **asset potenzialmente compromessi** a seguito di un'attività di analisi condotta dal CSIRT Italia, finalizzata all'individuazione di dispositivi di videosorveglianza compromessi e parte della **botnet DDoS** denominata **Eleven11bot**.

I NUMERI DI MARZO 2025

- **245** eventi cyber, in **diminuzione** (**–57**);
- **352** vittime, in **aumento** (**+28**);
- **179** vittime della constituency[1] , in **aumento** (**+6**);
- **81** incidenti con impatto confermato, in **aumento** (**+33**);
- **1.245** asset potenzialmente compromessi, in **aumento** (**+956**);
- **461** asset potenzialmente vulnerabili, in **diminuzione** (**–746**);
- **54** alert sul sito web del CSIRT Italia, **stabile** (**3**);
- **3.939** nuove CVE, in **aumento** (**+553**).

PRODOTTI VULNERABILI

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

- **Mautic** (CVE-2024-47051) Link all'alert;
- **Freetype** (CVE-2025-27363) Link all'alert;
- **Paragon** (CVE-2025-0289) Link all'alert;
- **Apache** (CVE-2025-24813)Link all'alert;
- **Wazuh** (CVE-2025-24016) Link all'alert;
- **Ivanti** (CVE-2025-0282) Link all'alert;
- **PostgreSQL** (CVE-2025-1094) Link all'alert;
- **F5 Networks** (CVE-2025-20029);
- **Apache Tomcat** (CVE-2025-24813) Link all'alert;
- **Tenda Router AC7** (CVE-2025-1851) Link all'alert;
- **Vercel Next.js** (CVE-2025-29927) Link all'alert;
- **CrushFTP** (CVE-2025-31161) Link all'alert;
- **Veeam Backup & Replication** (CVE-2025-23120) Link all'alert;
- **Elastic Kibana** (CVE-2025-25012) Link all'alert;
- **VMware ESXi, Workstation e Fusion** (CVE-2025-22226), (CVE-2025-22225), (CVE-2025-22224) Link all'alert;
- **Kubernetes Ingress NGINX Controller** (CVE-2025-24513), (CVE-2025-1974), (CVE-2025-1097), (CVE-2025-24514) 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 marzo 2025 sono stati individuati **245** eventi cyber, in **diminuzione** del 19% rispetto al mese precedente. Questi ultimi hanno avuto un **impatto su 263 soggetti nazionali**: 179 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 245 eventi cyber, **81 sono stati classificati quali incidenti**, in **aumento** del 69% rispetto a febbraio.

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.

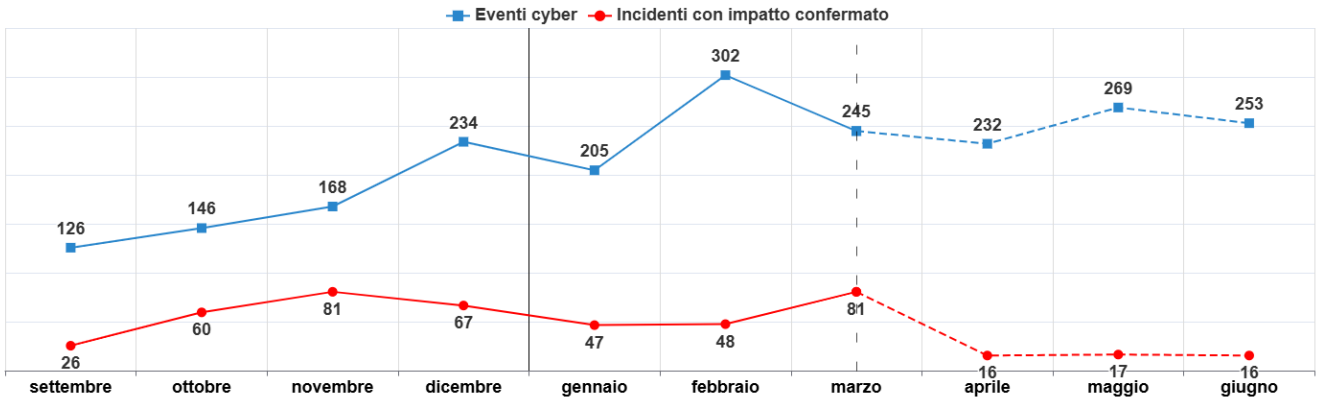

Figura 1 - *andamento attività reattive e analisi previsionale*

[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).

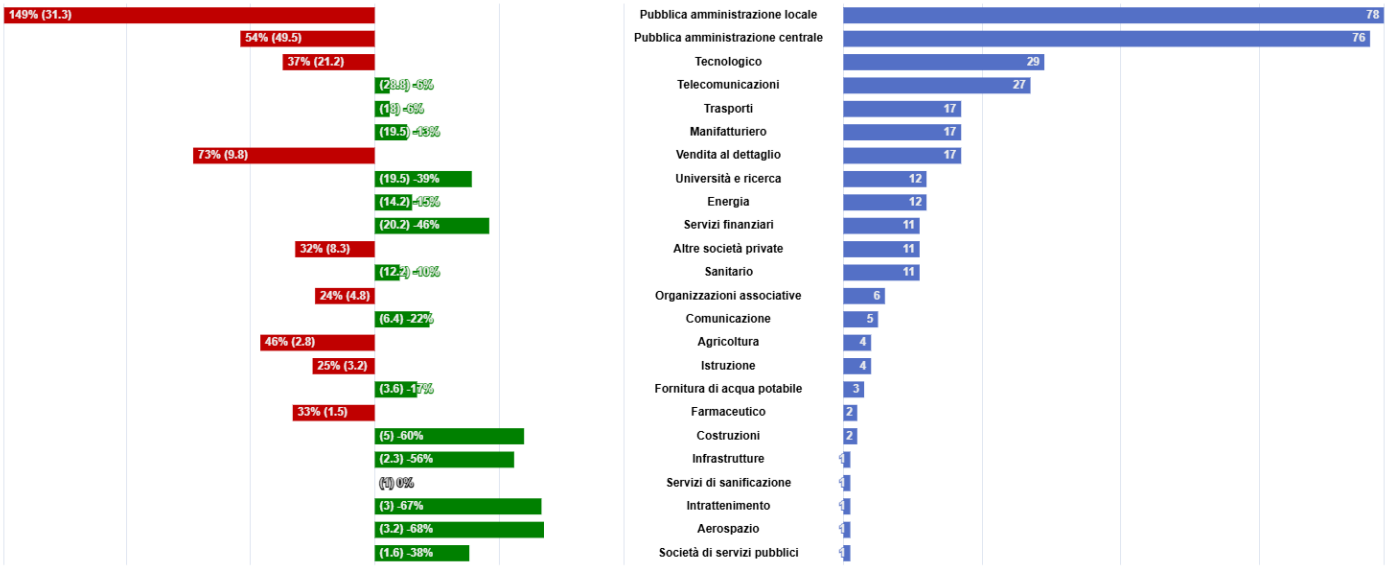

Figura 2 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente*

[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).

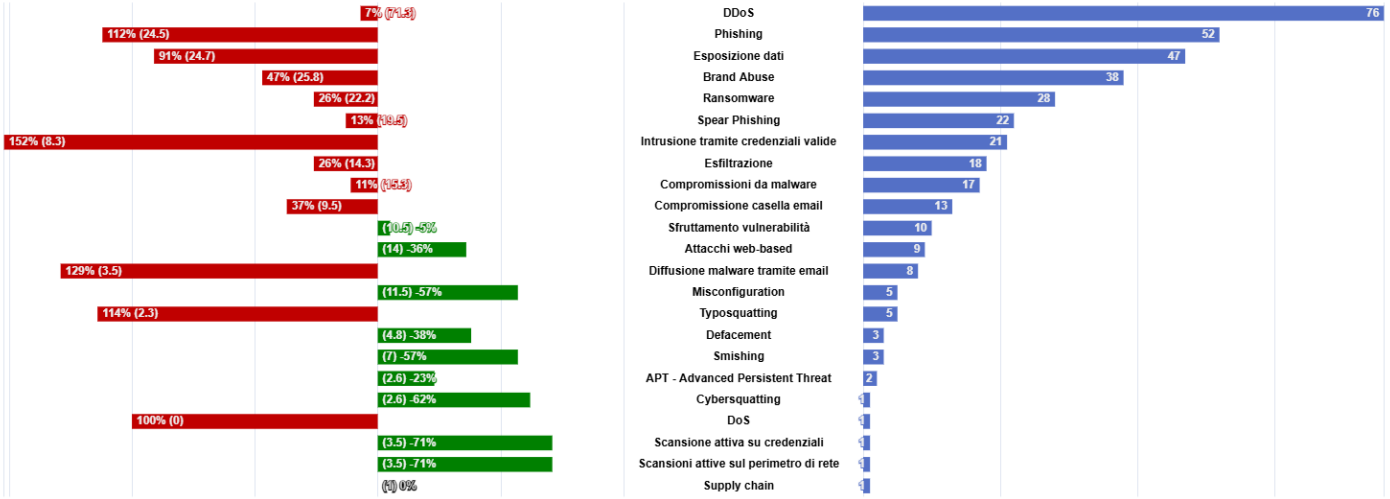

Figura 3 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente*

2.3 Focus constituency

I 245 eventi cyber hanno interessato **179** soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

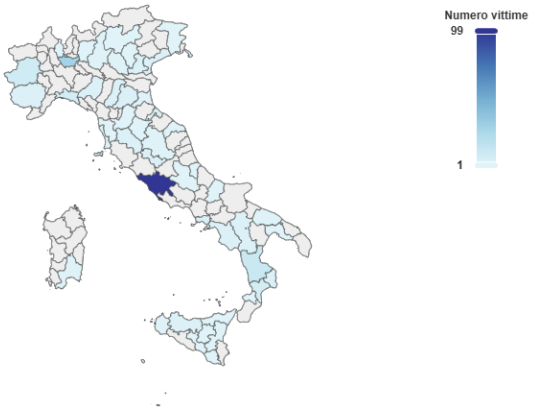

Figura 4 - *distribuzione geografica delle vittime appartenenti alla constituency*

[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.

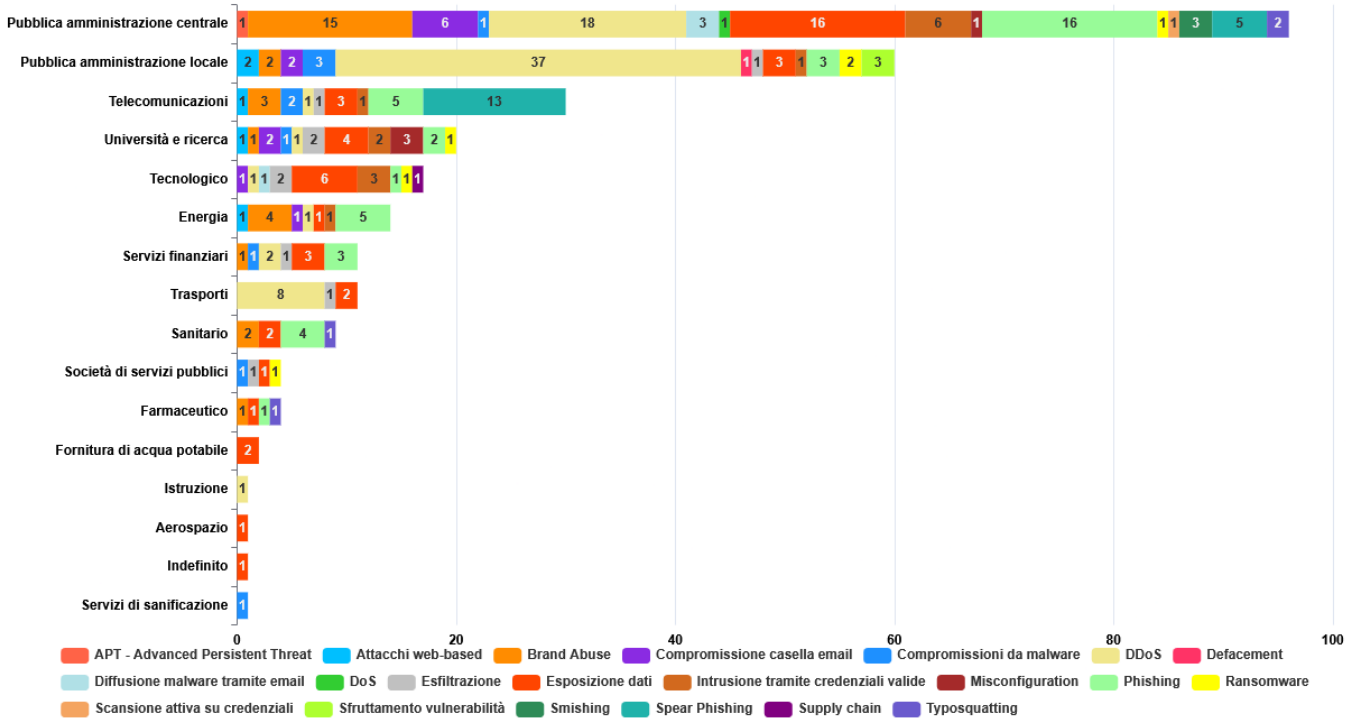

Figura 5 - *tipologia di minacce con impatto sui settori della constituency*

3 VULNERABILITÀ

A marzo 2025 sono state pubblicate[5] **3.939** nuove CVE, in **aumento** (**+553**) rispetto a febbraio. Di queste, **234** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (**+76**), e per **18** CVE è stato rilevato lo sfruttamento attivo, in **aumento** (**+6**) rispetto a febbraio.

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 **54**. Oltre al consueto aggiornamento mensile di Microsoft (link all'alert sul sito web), che ha risolto un totale di 57 nuove vulnerabilità (7 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Mautic**: disponibile un Proof of Concept (PoC) per la CVE-2024-47051 – già sanata dal vendor – presente in Mautic, nota piattaforma open-source di automazione del marketing che consente alle aziende di gestire campagne, tracciare il comportamento degli utenti e automatizzare varie attività di marketing (stima di impatto sistemico **78,33/100**). Link all'alert del 03/03/2025;
- **Freetype**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-27363 – già sanata nella versione 2.13.1 – che interessa la libreria di rendering dei font FreeType. Tale vulnerabilità, qualora sfruttata, consentirebbe l'esecuzione di codice remoto su una moltitudine di dispositivi (stima di impatto sistemico **77,05/100**). Link all'alert del 13/03/2025;
- **Paragon**: ricercatori di sicurezza hanno recentemente rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-0289 presente su molteplici prodotti basati su Paragon Hard Disk Manager (stima di impatto sistemico **76,66/100**). Link all'alert del 03/03/2025;
- **Apache**: rilevata una vulnerabilità di sicurezza, con gravità "alta", nel noto server web open source sviluppato da Apache Software Foundation. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato

[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/`.

remoto di eseguire codice arbitrario sul sistema interessato (stima di impatto sistemico **76,28/100**). Link all'alert del 11/03/2025;

- **Wazuh**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-24016 – già sanata – che interessa il software Wazuh, noto strumento open-source per la prevenzione, il rilevamento e la risposta alle minacce (stima di impatto sistemico **75,51/100**). Link all'alert del 10/03/2025.

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.

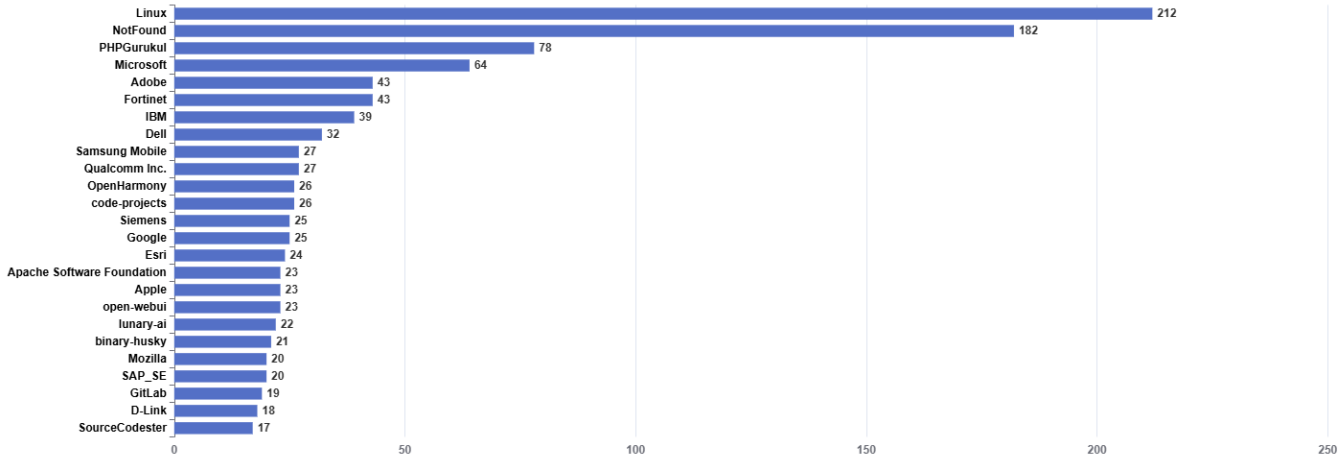

Figura 6 - *top 25 produttori affetti da vulnerabilità nel mese*

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

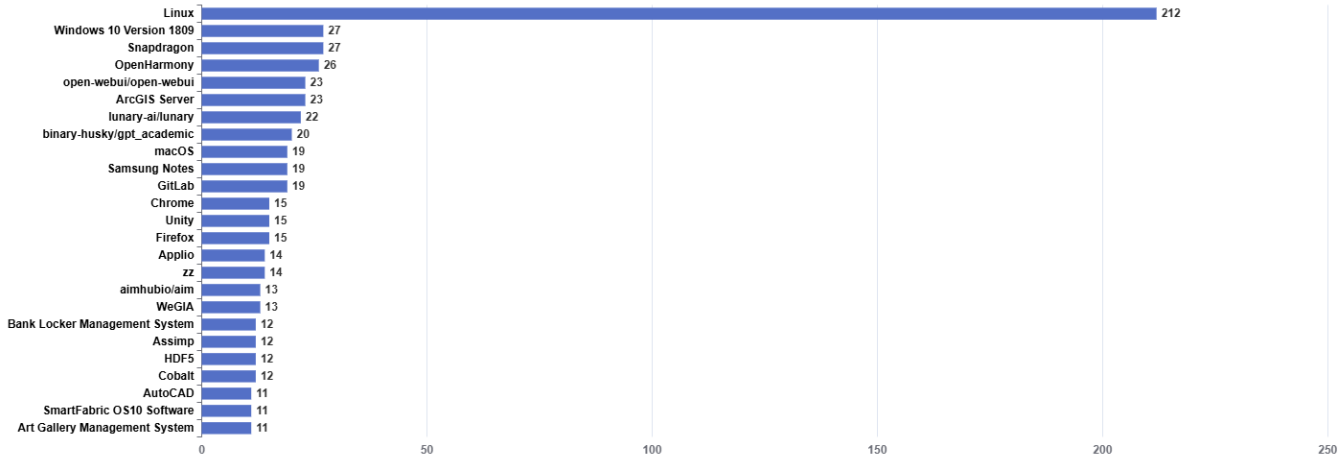

Figura 7 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

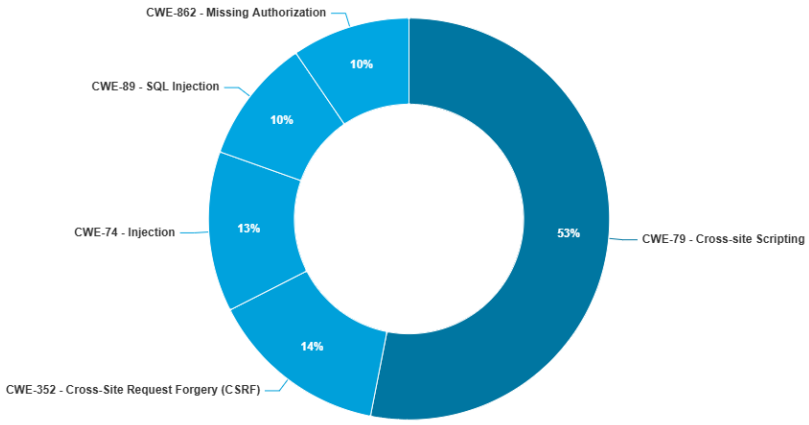

Figura 8 - *top 5 CWE nel mese*

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	**Ivanti**
Prodotti e versioni vulnerabili	**Ivanti Connect Secure versioni prrecedenti la 22.7R2.5** **Ivanti Policy Secure versioni precedenti la 22.7R1.2** **Ivanti Neurons for ZTA gateways versioni precedenti la 22.7R2.3**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo da remoto.**
Data di rilascio CVE	**08/01/2025 modificata il 19/02/2025**
CVSS score 3.x	**9.0 CRITICAL**
EPSS max score	**0.92**

Tabella 1 - *CVE-2025-0282*

Vendor	**PostgreSQL Global Development Group**
Prodotti e versioni vulnerabili	**PostgreSQL** **▪ 17.x, versioni precedenti alla 17.3** **▪ 16.x, versioni precedenti alla 16.7** **▪ 15.x, versioni precedenti alla 15.11** **▪ 14.x, versioni precedenti alla 14.16** **▪ 13.x, versioni precedenti alla 13.19**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire comandi.**
Data di rilascio CVE	**13/02/2025 modificata il 21/02/2025**
CVSS score 3.x	**8.1 HIGH (valore rilasciato dal vendor)**
EPSS max score	**0.84**

Tabella 2 - *CVE-2025-1094*

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

Vendor	**F5 Networks**
Prodotti e versioni vulnerabili	**- iControl REST** **- BIG-IP TMOS Shell** **Versioni di BIG-IP e BIG-IQ vulnerabili:** **▪ 7.x, versioni da 17.1.0 a 17.1.2** **▪ 16.x, versioni da 16.1.0 a 16.1.5 e versione 16.1.5.2** **▪ 15.x, versioni da 15.1.0 a 15.1.10** **Il vendor non ha preso in considerazione le versioni che hanno raggiunto la End of Technical Support(EoTS)**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice arbitrario, creare o cancellare file.**
Data di rilascio CVE	**05/02/2025**
CVSS score 3.x	**8.8 HIGH (valore rilasciato dal vendor)**
EPSS max score	**0.83**

Tabella 3 - *CVE-2025-20029*

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.

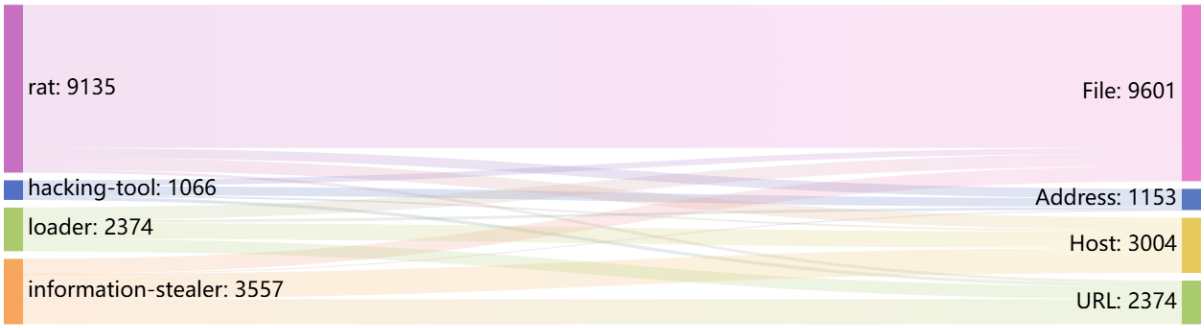

Figura 9 - *numero di IoC condivisi dal CSIRT Italia suddivisi per famiglie di malware*

[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 marzo 2025 ha permesso di individuare **23** rivendicazioni di attacchi ransomware a danno di soggetti italiani. I gruppi più attivi sono stati **RansomHub** e **Lockbit30**.

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

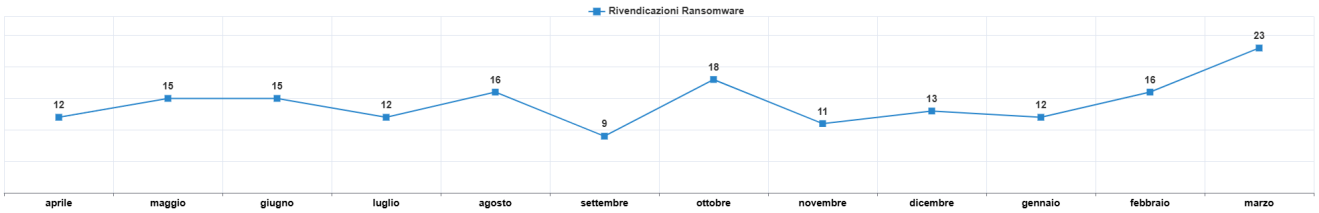

Figura 10 - *andamento delle rivendicazioni Ransomware*

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

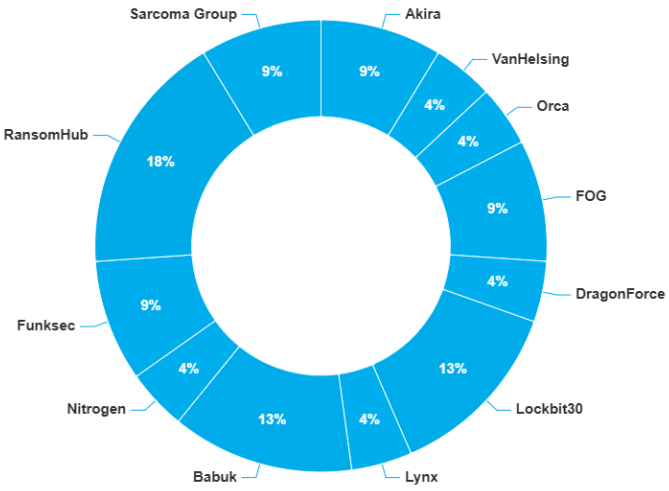

Figura 11 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

4.3 Rivendicazioni DDoS

A marzo 2025 sono state individuate[9] **124** rivendicazioni di attacchi DDoS in danno di soggetti italiani. I gruppi più attivi su scala globale sono stati **NoName05716** e **keymous**

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

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

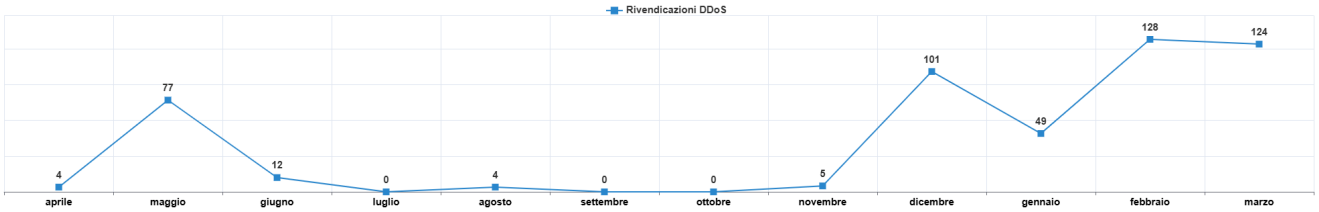

Figura 12 - *andamento delle rivendicazioni DDoS*

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

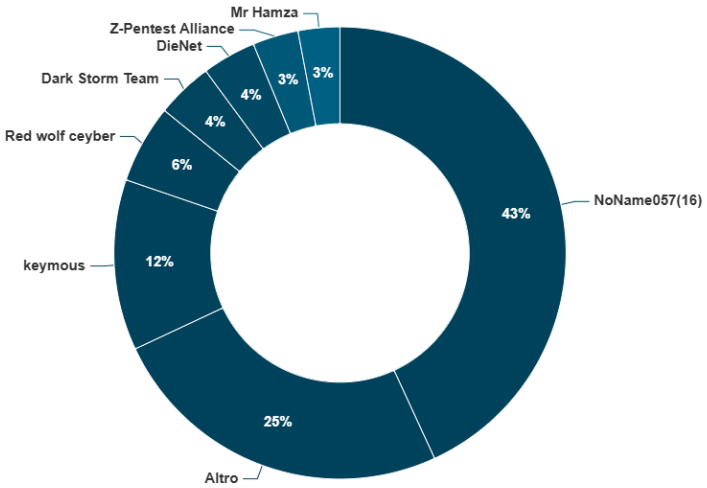

Figura 13 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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 marzo 2025 sono state diramate un totale di **277** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **461** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **Apache Tomcat** (CVE-2025-24813): tale vulnerabilità potrebbe consentire a un eventuale attaccante di eseguire codice arbitrario da remoto sul sistema interessato, l'accesso a file e/o informazioni sensibili e l'aggiunta di contenuti malevoli. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **VMware ESXi, Workstation e Fusion** (CVE-2025-22226, CVE-2025-22225, CVE-2025-22224): tali vulnerabilità – laddove sfruttate in maniera combinata – permetterebbero a un eventuale attaccante con privilegi amministrativi locali all'interno di una macchina virtuale di evadere dall'ambiente virtualizzato della stessa e di eseguire codice sull'host *hypervisor*. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Tenda Router AC7** (CVE-2025-1851): tale vulnerabilità - di tipo *Stack-Based Buffer Overflow* - potrebbe permettere a un eventuale attaccante autenticato di ottenere da remoto l'accesso ad una shell con privilegi di "root", tramite l'invio di richieste specificatamente predisposte verso l'interfaccia web del router. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Vercel Next.js** (CVE-2025-29927): tale vulnerabilità – di tipo *Authentication Bypass* – potrebbe consentire a un eventuale attaccante il bypass dei controlli di sicurezza del middleware di Next.js sfruttando un'intestazione HTTP

[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.

"x-middleware-subrequest" opportunamente predisposta. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;

- **Mautic** (CVE-2024-47051): tale vulnerabilità - di tipo *Code Injection* e *Path Traversal* - potrebbe consentire a un attaccante in possesso di credenziali valide l'esecuzione di codice arbitrario remoto tramite il caricamento di file eseguibili come script PHP e l'eliminazione arbitraria di file sulle installazioni affette. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **CrushFTP** (CVE-2025-31161): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe ad un eventuale attaccante l'accesso non autenticato ai server non aggiornati esposti su Internet in ascolto sulle porte HTTP e HTTPS, laddove non siano in essere eventuali mitigazioni poste in essere dalla funzionalità DMZ del prodotto. Ulteriori dettagli nell'alert rilevati sul sito del CSIRT Italia;
- **Veeam Backup & Replication** (CVE-2025-23120): tale vulnerabilità - di tipo *Deserialization of Untrusted Data* - consentirebbe, sfruttando un'errata implementazione dei meccanismi di deserializzazione basati su blacklist per il controllo degli accessi, di eseguire da remoto codice arbitrario sulle installazioni affette qualora queste siano domain-joined, utilizzando utenze locali o di dominio. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Elastic Kibana** (CVE-2025-25012): tale vulnerabilità - di tipo *Prototype Pollution* - permetterebbe ad un eventuale attaccante, con specifici privilegi utente, di eseguire codice arbitrario sui sistemi interessati tramite il caricamento di opportuni file o l'invio di richieste HTTP specificatamente predisposte. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **F5 BIG-IP** (CVE-2025-20029): tale vulnerabilità consentirebbe, tramite l'invio di richieste appositamente predisposte verso le componenti BIG-IP iControl REST e TMOS Shell (tmsh), a un utente autenticato con privilegi minimi l'esecuzione di codice arbitrario da remoto come l'utente "root" del sistema.
- **Kubernetes Ingress NGINX Controller** (CVE-2025-24513 E CVE-2025-1974, CVE-2025-1098, CVE-2025-1097, CVE-2025-24514): tali vulnerabilità - laddove sfruttate in maniera combinata - permetterebbero a un eventuale attaccante di eseguire da remoto codice arbitrario e di accedere a tutti i secrets del cluster dell'installazione Kubernetes, portando alla compromissione completa di quest'ultimo. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Wazuh** (CVE-2025-24016): tale vulnerabilità - di tipo *Deserialization of Untrusted Data* - potrebbe consentire, a un eventuale attaccante in possesso di credenziali API valide o di un accesso a un agent compromesso, l'esecuzione di codice arbitrario da remoto e/o la possibilità di effettuare *Denial of Service* sul sistema interessato sfruttando payload JSON appositamente predisposti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;

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

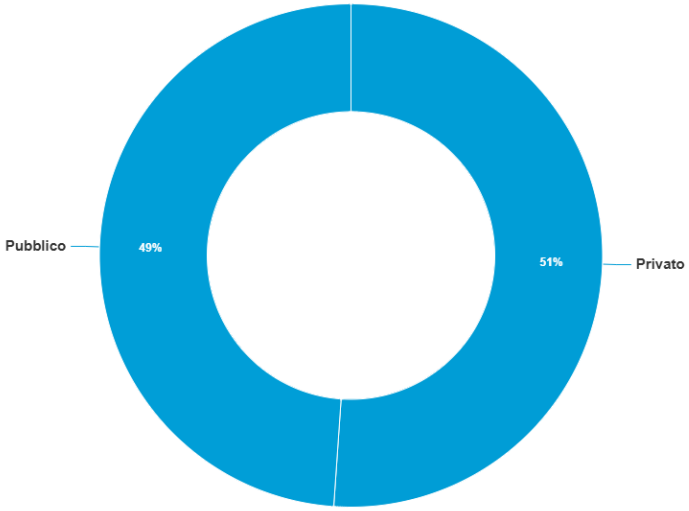

Figura 14 - *distribuzione delle segnalazioni per tipologia di soggetto*

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

marzo 2025