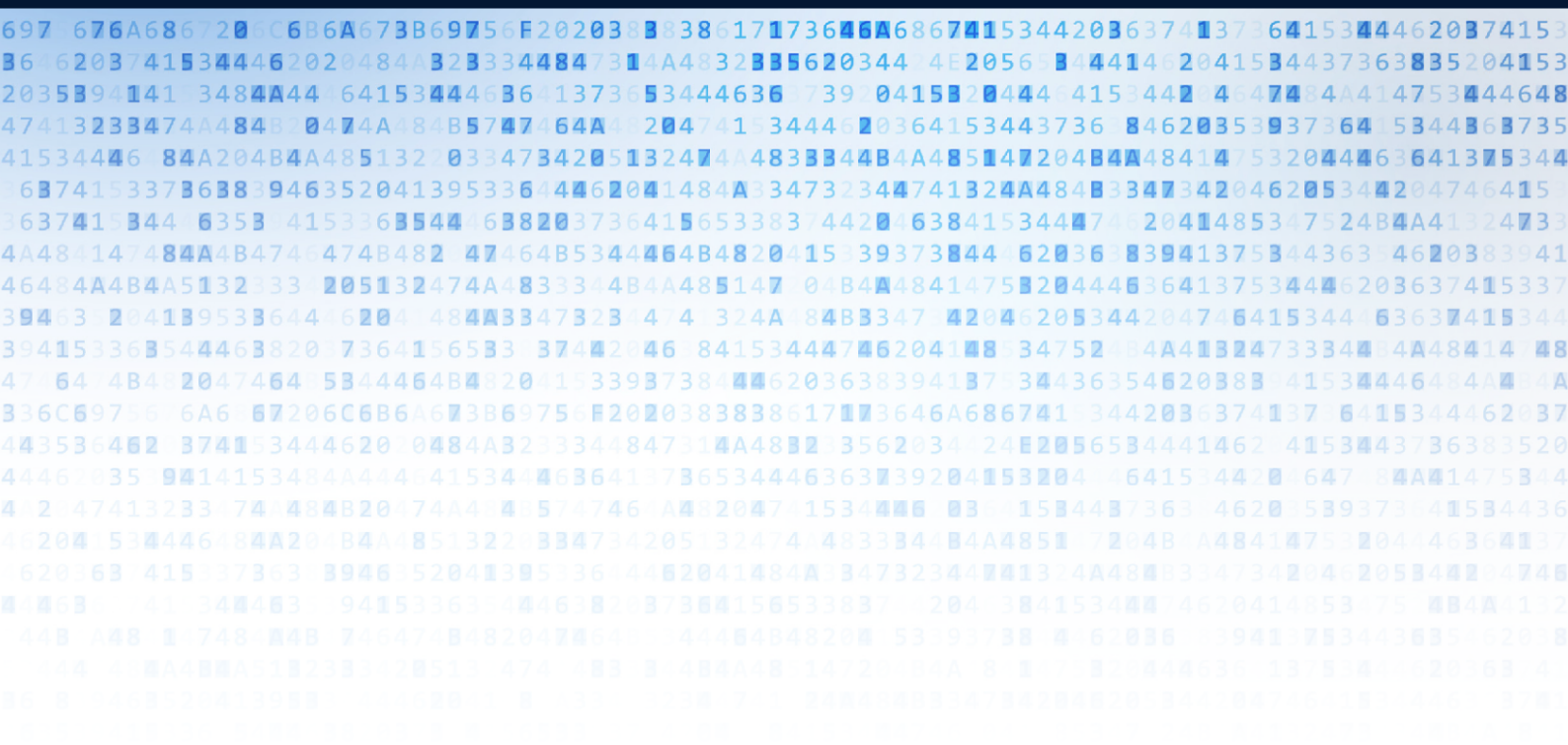
Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

Servizio Operazioni
e gestione delle crisi cyber

maggio 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.

Indice

1. EXECUTIVE SUMMARY **4**
2. EVENTI ED INCIDENTI **7**
2.1. Settori impattati **8**
2.2. Tipologia di minacce negli eventi **8**
2.3. Focus constituency **9**
3. VULNERABILITÀ **11**
3.1. Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia **11**
3.2. Distribuzione delle vulnerabilità sui vendor **12**
3.3. CWE nel mese **13**
3.4. Vulnerabilità con maggior probabilità di sfruttamento **13**
4. MINACCIA **15**
4.1. Indicatori di Compromissione (IoC) per famiglia di malware **15**
4.2. Rivendicazioni ransomware **16**
4.3. Rivendicazioni DDoS **16**
5. MONITORAGGIO **18**
5.1. Comunicazioni dirette **18**

1 EXECUTIVE SUMMARY

- A maggio 2025 sono stati registrati **201 eventi**, in **aumento** del **23**% rispetto ad aprile, mentre il numero di **incidenti** (**51**) è **lievemente inferiore** alla media dei sei mesi precedenti.
- I settori con il maggior numero di vittime registrate sono stati: **Servizi finanziari**, **Telecomunicazioni** e **Vendita al dettaglio**.
- Nel mese di maggio sono stati rilevati **17 attacchi ransomware**, con un **aumento** del **20%** rispetto alla media dei sei mesi precedenti. Tra gli incidenti ransomware di maggiore rilievo si segnala quello rivendicato dal **gruppo INC**[1] ai danni dell'**Università di Roma Tre**[2].
- In continuità con quanto osservato a marzo e aprile, si è registrata una ulteriore attenuazione delle campagne di **hacktivism** legate al conflitto russo-ucraino. Ciò si è concretizzato in una netta riduzione sia degli attacchi **DDoS** sia dei **defacement** rispetto ai mesi precedenti.
- Nel corso delle attività di monitoraggio condotte dal CSIRT Italia, particolarmente significativo è stato il rilevamento di una campagna di **phishing** di oltre trecento messaggi di posta elettronica originati da una casella compromessa ad un operatore del settore energetico. I messaggi invitavano i destinatari a inserire le proprie credenziali in un sito web malevolo appositamente predisposto dall'attaccante.
- Di rilievo, altresì, è stato il rinvenimento di **credenziali compromesse in vendita** (username e password), in larga parte riconducibili a clienti di istituti bancari e potenzialmente associati all'accesso ai conti corrente, segnalata dal CSIRT ai soggetti istituzionali preposti.
- Nel mese di maggio è stata svolta un'importante attività di analisi mirata all'individuazione di dispositivi potenzialmente compromessi, utilizzati come infrastruttura per la distribuzione di ransomware. Ciò a seguito dell'**Operation Endgame**: una vasta operazione internazionale coordinata da Europol ed Eurojust, che ha portato all'arresto di quattro soggetti, oltre al sequestro di più di 100 server e 2.000 domini. L'operazione ha colpito botnet strategiche come **IcedID**, **Smokeloader** e **Bumblebee**, frequentemente impiegate nella fase iniziale della **kill chain** dei ransomware.

[1] Il CSIRT Italia ha pubblicato, ad aprile, un bollettino dedicato alla diffusione del ransomware INC: https://www.acn.gov.it/portale/w/inc-ransomware-rilevata-diffusione

[2] Comunicato dell'ateneo: https://www.uniroma3.it/articoli/attacco-informatico-allinfrastruttura-dellateneo-467162/

L'attività ha permesso di individuare e segnalare **1.977** dispositivi potenzialmente compromessi, esposti su Internet da soggetti italiani.

- I **vettori di attacco** maggiormente rilevati a maggio 2025 sono stati: campagne malevole veicolate tramite e-mail, sfruttamento di vulnerabilità note e l'utilizzo di credenziali valide precedentemente compromesse.
- **4.262** le nuove CVE pubblicate, in **diminuzione** rispetto ad aprile (**–37**).
- Nel mese di maggio 2025, il CSIRT Italia ha inviato **3.440** comunicazioni dirette, effettuate per segnalare potenziali compromissioni o fattori di rischio ad amministrazioni ed imprese italiane;

I NUMERI DI MAGGIO 2025

- **201** eventi cyber, in **aumento** (**+38**);
- **341** vittime, in **aumento** (**+80**);
- **108** vittime della constituency[3], in **diminuzione** (**–8**);
- **51** incidenti con impatto confermato, in **aumento** (**+22**);
- **2.171** asset potenzialmente compromessi, in **aumento** (**+1.745**);
- **532** asset potenzialmente vulnerabili, in **aumento** (**+243**);
- **51** alert sul sito web del CSIRT Italia, in **diminuzione** (**–16**);
- **3.440** comunicazioni inviate, in **diminuzione** (**–293**);
- **4.262** nuove CVE, in **diminuzione** (**–37**).

PRODOTTI VULNERABILI

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

- **Mozilla** (CVE-2025-4918), (CVE-2025-4919) Link all'alert;
- **Microsoft** Link all'alert;
- **Samsung** (CVE-2025-4632), Link all'alert;
- **Fortinet** (CVE-2025-22252), (CVE-2025-25251), (CVE-2025-39780)Link all'alert;
- **Asus** (CVE-2025-32433) Link all'alert;
- **CrushFTP** (CVE-2025-32102 e CVE-2025-32103) Link all'alert;
- **Prodotti Fortinet FortiCamera, FortiMail, FortiNDR, FortiRecorder e FortiVoice** (CVE-2025-32756) Link all'alert;
- **SysAid** (CVE-2025-2775) Link all'alert;
- **Ivanti Endpoint Manager Mobile** (CVE-2025-4427,CVE-2025-4428) Link all'alert;
- **ConnectWise ScreenConnect** (CVE-2025-3935) Link all'alert;
- **Commvault Command Center** (CVE-2025-34028) Link all'alert;
- **Craft CMS** (CVE-2024-58136) Link all'alert;
- **Srimax Output Messenger** (CVE-2025-27920);
- **OpenCTI** (CVE-2025-24977) Link all'alert;
- **Samsung MagicINFO** (CVE-2024-7399) 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.

[3]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 maggio 2025 sono stati individuati **201** eventi cyber, in **aumento** del 23% rispetto al mese precedente. Questi ultimi hanno **interessato 270 soggetti nazionali**: 108 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 201 eventi cyber, **51 sono stati classificati quali incidenti**, in **aumento** del 76% rispetto ad aprile.

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[4], riferita ai successivi 3 mesi.

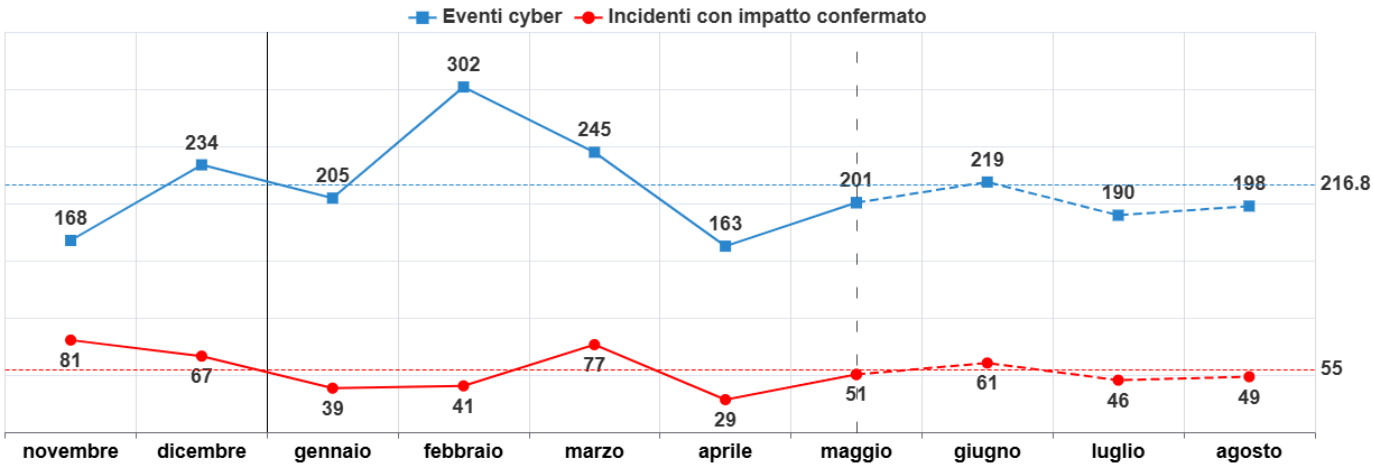


Figura 1 - *andamento attività reattive e analisi previsionale*

[4] 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[5]. Si evidenza altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico)[6].

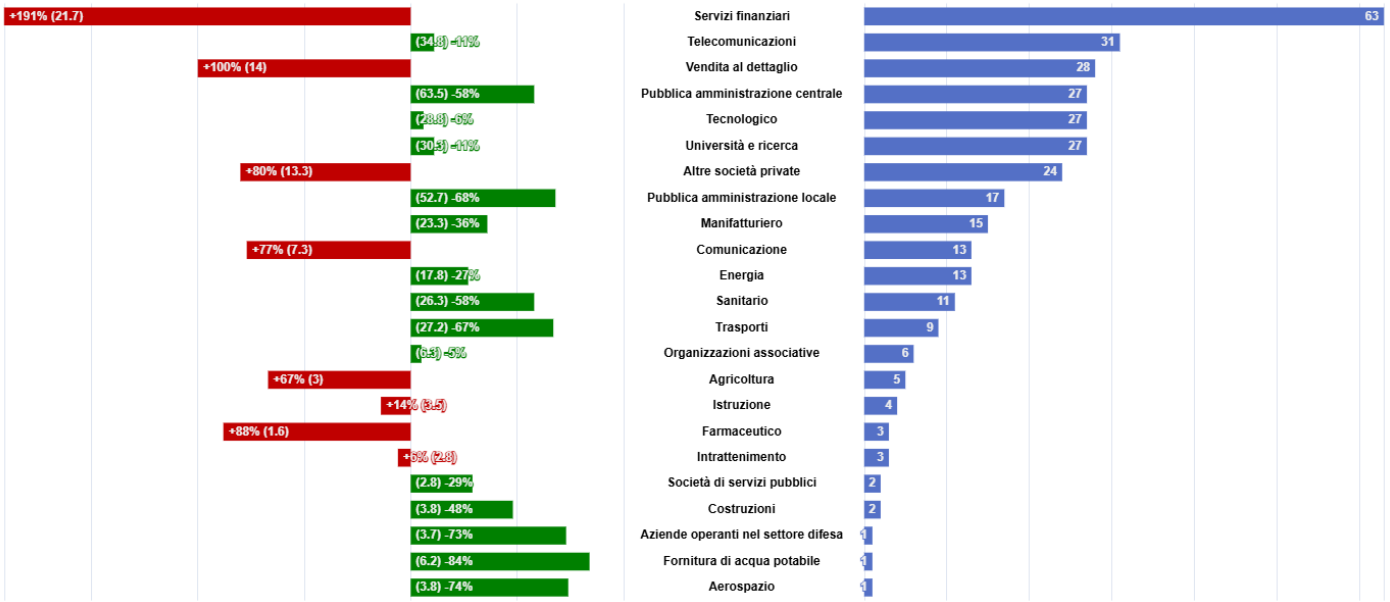


Figura 2 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente*

2.2 Tipologia di minacce negli eventi

In Figura 3 si riporta il numero di minacce rilevate negli eventi[7] e la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico) .

[5] 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.

[6] L'incremento degli eventi rilevati nel settore dei **Servizi finanziari** è dovuto a un solo evento ransomware in danno di un operatore con ripercussioni sulla confidenzialità delle informazioni anche dei suoi clienti

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

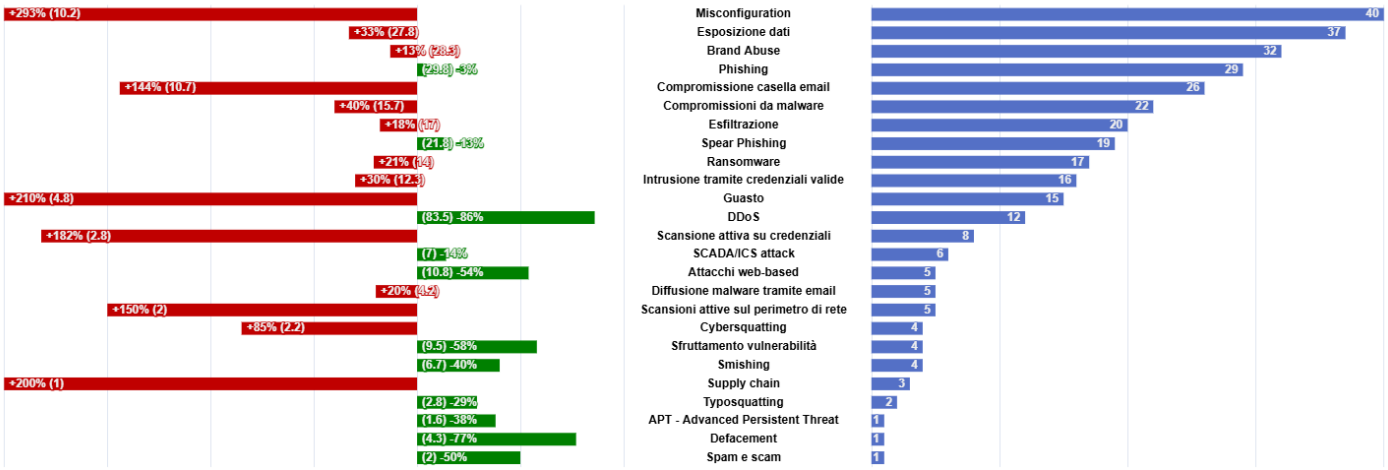


Figura 3 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente*

2.3 Focus constituency

I 201 eventi cyber hanno interessato **108** soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

Figura 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.

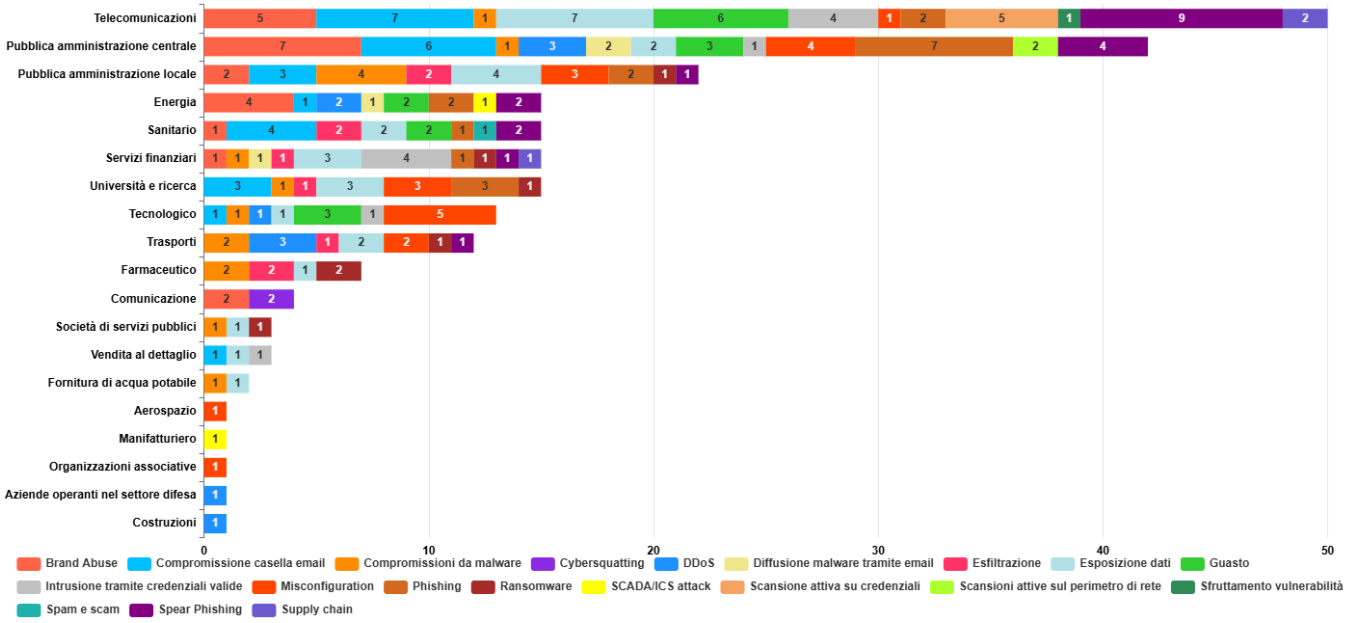


Figura 5 - *tipologia di minacce con impatto sui settori della constituency*

3 VULNERABILITÀ

A maggio 2025 sono state pubblicate[8] **4.262** nuove CVE, in **diminuzione** (**–37**) rispetto ad aprile. Di queste, **566** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (**+182**), e per **14** CVE è stato rilevato lo sfruttamento attivo, in **aumento** (**+14**) rispetto ad aprile.

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 71 nuove vulnerabilità (7 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Mozilla**: rilevato lo sfruttamento attivo delle vulnerabilità 0day CVE-2025-4918 e CVE-2025-4919 che interessano i prodotti Firefox e Firefox ESR (stima di impatto sistemico **83,55/100**). Link all'alert del 20/05/2025;
- **Microsoft**: è stata rilevata una vulnerabilità in dMSA (delegated Managed Service Account), nuova funzionalità introdotta in Windows Server 2025 all'interno di Active Directory che consente di delegare la creazione e la gestione di account di servizio a utenti non privilegiati. Microsoft ha riconosciuto il problema, ma lo ha classificato come "Moderate Severity" e non ha ancora rilasciato una patch (stima di impatto sistemico **82,05/100**). Link all'alert del 27/05/2025;
- **Samsung**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-4632 – già sanata dal vendor – che interessa la componente server di MagicINFO 9 di Samsung, soluzione all-in-one per la gestione di contenuti, dati e dispositivi (stima di impatto sistemico **79,23/100**). Link all'alert del 16/05/2025;
- **Fortinet**: rilevate nuove vulnerabilità in alcuni prodotti Fortinet, di cui una con gravità "critica". Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto che conosca un account amministrativo esistente di accedere come amministratore al sistema target, bypassando l'autenticazione (stima di impatto sistemico **78,97/100**). Link all'alert del 14/05/2025;

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

- **Asus**: è stato rilevato lo sfruttamento di una vulnerabilità nei router Asus che consente l'apertura di una backdoor, persistente anche dopo il riavvio del dispositivo o gli aggiornamenti del firmware. (stima di impatto sistemico **77,94/100**). Link all'alert del 29/05/2025;

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.

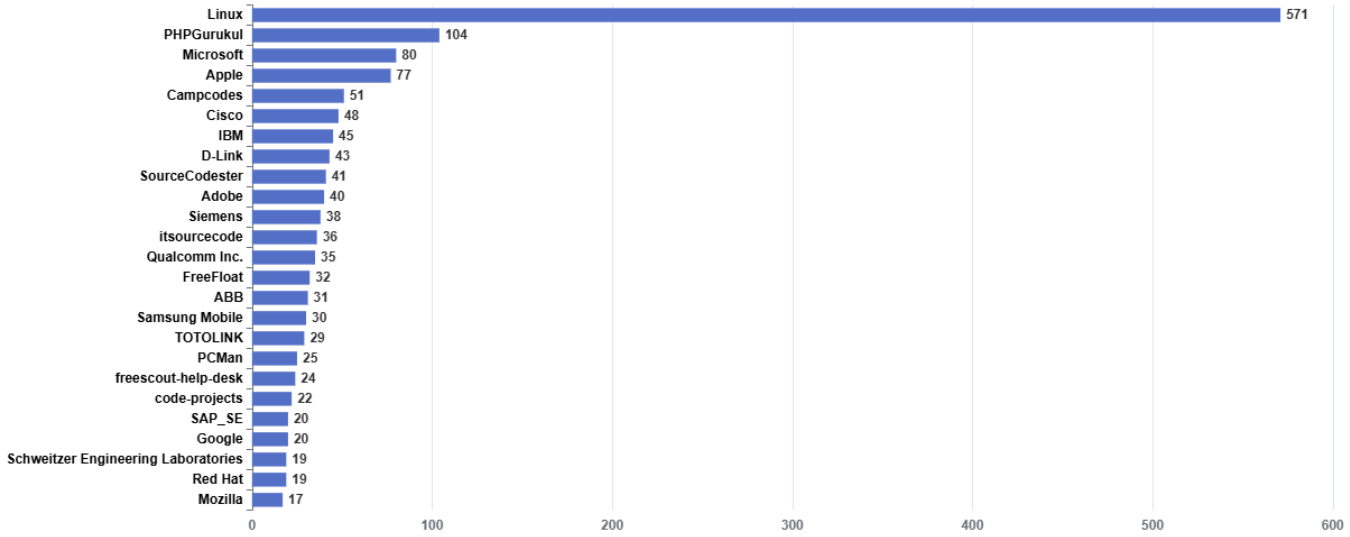


Figura 6 - *top 25 produttori affetti da vulnerabilità nel mese*

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

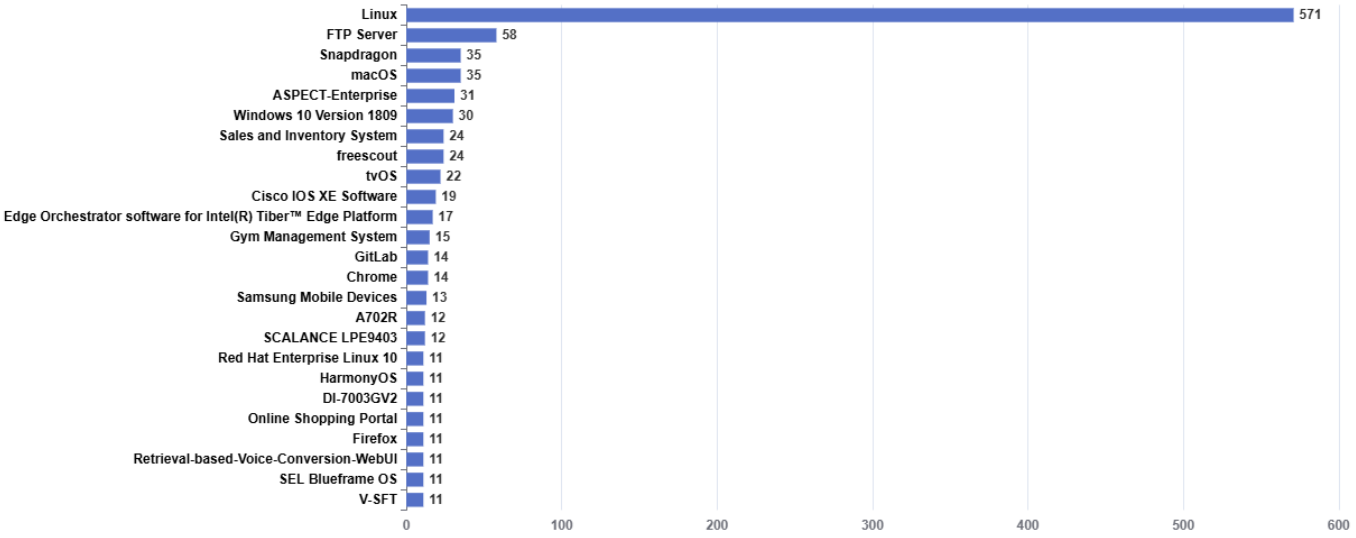


Figura 7 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

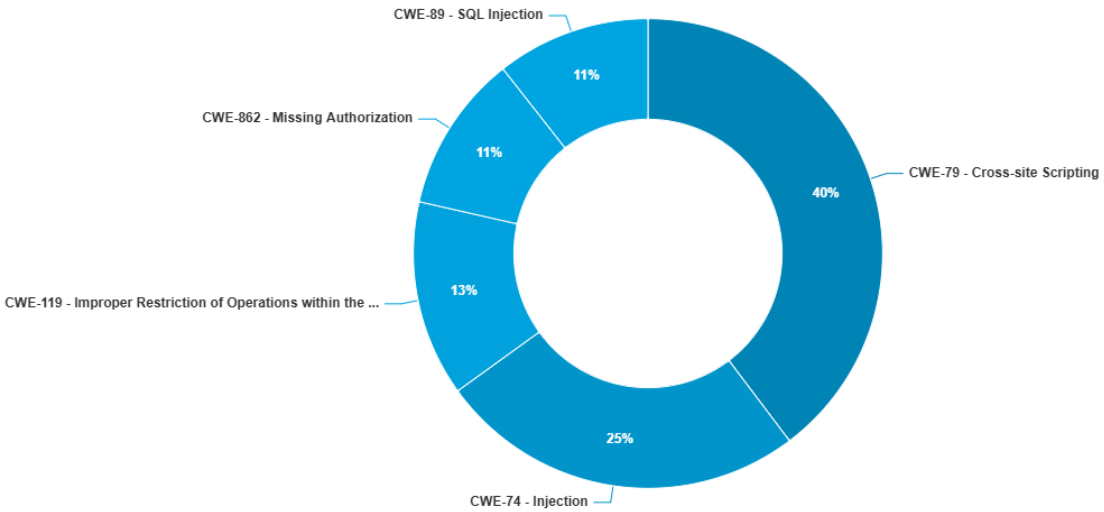


Figura 8 - *top 5 CWE nel mese*

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

Vendor	**Apache Software Foundation**
Prodotti e versioni vulnerabili	**Apache Tomcat seguenti versioni:** ▪ **da 11.0.0-M1 a 11.0.2** ▪ **da 10.1.0-M1 a 10.1.34** ▪ **da 9.0.0.M1 a 9.0.98**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo..**
Data di rilascio CVE	**10/03/2025 modificata il 18/03/2025**
CVSS score 3.x	**9.8 CRITICAL**
EPSS max score	**0.93**

Tabella 1 - *CVE-2025-24813*

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

Vendor	**Langflow**
Prodotti e versioni vulnerabili	**Langflow tutte le versioni fino alla 1.2.0**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo.**
Data di rilascio CVE	**07/04/2025 modificata il 07/05/2025**
CVSS score 3.x	**9.8 CRITICAL**
EPSS max score	**0.96**

Tabella 2 - *CVE-2025-3248*

Vendor	**Cloud Native Computing Foundation**
Prodotti e versioni vulnerabili	**Kubernetes Ingress-NGINX Controller tutte le versioni fino alla 1.11.4 e la versione 1.12.0**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante autenticato di eseguire codice malevolo.**
Data di rilascio CVE	**24/03/2025 modificata il 27/03/2025**
CVSS score 3.x	**9.8 CRITICAL**
EPSS max score	**0.87**

Tabella 3 - *CVE-2025-1974*

4 MINACCIA

In questa sezione si riportano, per quanto riguarda il malware, il numero degli Indicatori di Compromissione (IoC)[10]condivisi dal CSIRT Italia tramite piattaforma MISP (Malware Information Sharing Platform)[11], 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.

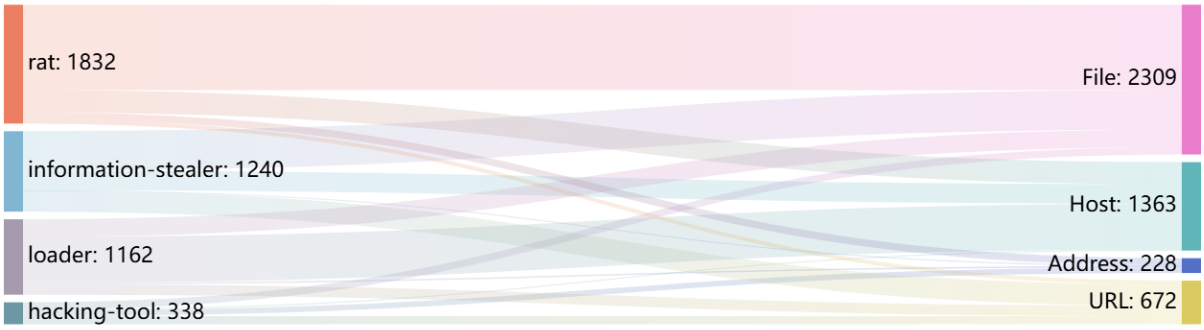


Figura 9 - *numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware*

[10]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.

[11]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 maggio 2025 ha permesso di individuare **12** rivendicazioni di attacchi ransomware a danno di soggetti italiani. I gruppi più attivi sono stati **Nova (ex Ralord)** e **KillSec3.0**.

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

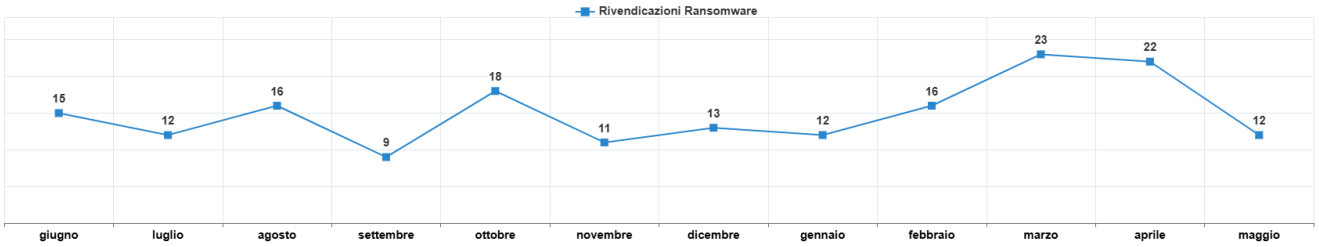


Figura 10 - *andamento delle rivendicazioni Ransomware*

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

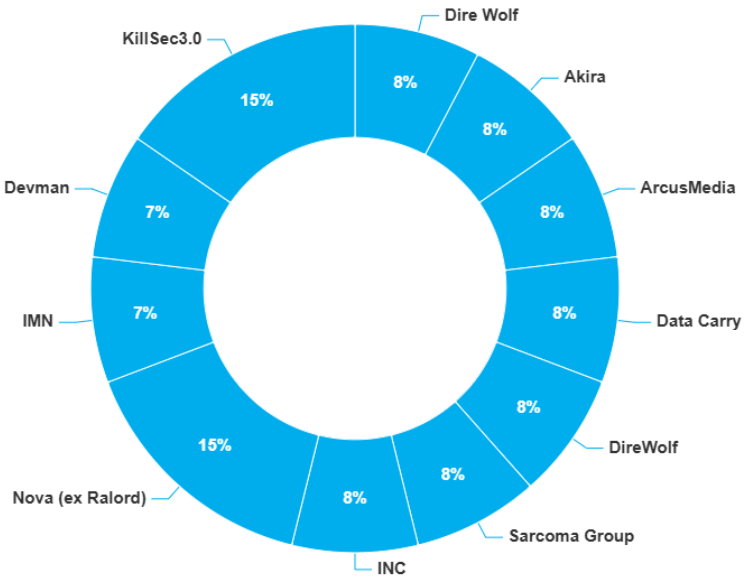


Figura 11 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

4.3 Rivendicazioni DDoS

A maggio 2025 non sono state individuate[12] rivendicazioni di attacchi DDoS in danno di soggetti italiani.
I gruppi più attivi su scala globale sono stati **NNM05716 En version** e **NNM05716**

[12] 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.

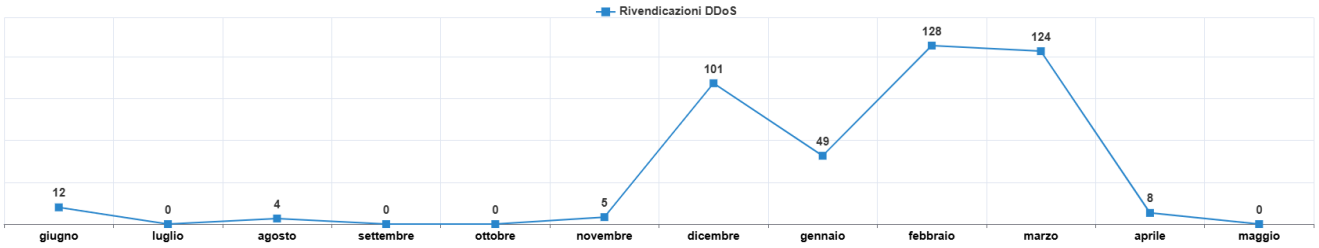


Figura 12 - *andamento delle rivendicazioni DDoS*

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

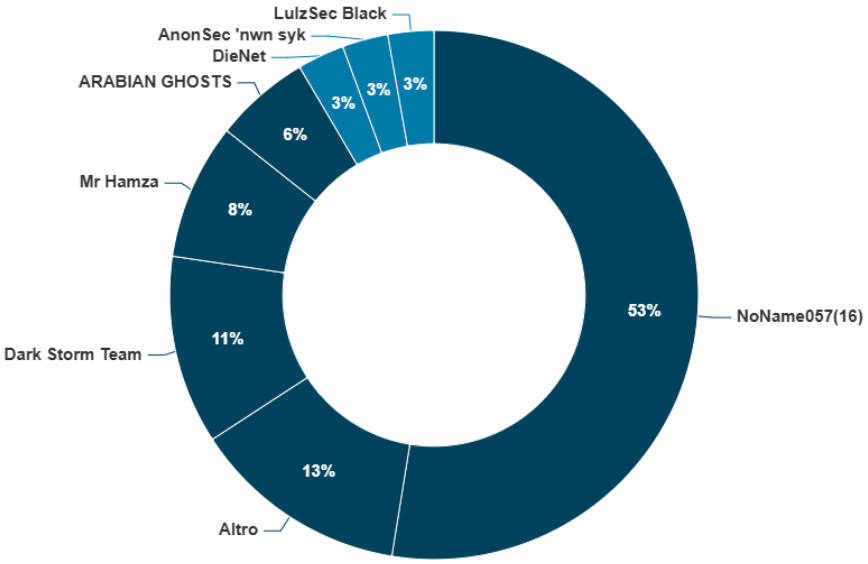


Figura 13 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

5 MONITORAGGIO

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

5.1 Comunicazioni dirette

A maggio 2025 sono state diramate un totale di **236** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **532** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **Prodotti Fortinet FortiCamera, FortiMail, FortiNDR, FortiRecorder e FortiVoice** (CVE-2025-32756): tale vulnerabilità - di tipo *Stack-Based Buffer Overflow* - potrebbe permettere a un eventuale attaccante di eseguire da remoto codice o comandi arbitrari sui sistemi affetti mediante l'invio di richieste HTTP opportunamente predisposte. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **SysAid** (CVE-2025-2775, CVE-2025-2776 e CVE-2025-2777): tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malevolo di bypassare i meccanismi di sicurezza, di eseguire codice da remoto e accedere a file sensibili sul sistema target.
- **Ivanti Endpoint Manager Mobile** (CVE-2025-4427 e CVE-2025-4428): tali vulnerabilità - di tipo *Authentication Bypass* e *Remote Code Execution* - qualora sfruttate in maniera combinata, potrebbero consentire ad un utente malintenzionato remoto non autenticato il bypass dei meccanismi di autenticazione e l'esecuzione di codice arbitrario sui dispositivi target. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **ConnectWise ScreenConnect** (CVE-2025-3935): tale vulnerabilità - di tipo *Code Injection* - permetterebbe a un eventuale attaccante che abbia acquisito privilegi di sistema di compromettere chiavi di sistema tali da consentire

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

l'esecuzione di codice arbitrario. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;

- **Commvault Command Center** (CVE-2025-34028): tale vulnerabilità - di tipo *Path Traversal* - e con score CVSS v3.1 pari a 10 - potrebbe consentire, a un utente malintenzionato remoto, l'esecuzione di codice arbitrario sul sistema interessato. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Craft CMS** (CVE-2024-58136 e CVE-2025-32432): In particolare, partendo dallo sfruttamento della vulnerabilità CVE-2025-32432, è possibile caricare un file PHP malevolo e di eseguirlo remotamente attraverso la seconda vulnerabilità sfruttando una anomalia presente nella deserializzazione del framework Yii.
  Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Srimax Output Messenger** (CVE-2025-27920): tale vulnerabilità – di tipo *Path Traversal* – consentirebbe a un eventuale attaccante di accedere a file arbitrari – anche sensibili – o di eseguire quest'ultimi attraverso la manipolazione dei percorsi dei file, sfruttando sequenze di caratteri "../" per eludere la struttura della directory prevista. Inoltre, laddove sia abilitata una output drive, è possibile per un attaccante autenticato procedere anche all'upload di file potenzialmente malevoli sui sistemi affetti.
- **OpenCTI** (CVE-2025-24977): tale vulnerabilità - di tipo *Remote Code Execution* e con score CVSS v3.1 pari a 9.1 - potrebbe consentire, a un utente malintenzionato remoto, l'esecuzione di codice arbitrario sul sistema interessato. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Samsung MagicINFO** (CVE-2024-7399): tale vulnerabilità - di tipo *Arbitrary File Upload* - permetterebbe a un attaccante non autenticato di caricare file arbitrari sui server affetti, permettendo così l'esecuzione di codice da remoto nel contesto di esecuzione di Apache Tomcat per mezzo di web shell JavaServer Pages (JSP) appositamente predisposte.
  Ulteriori dettagli nell'alert sul sito del CSIRT Italia;

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

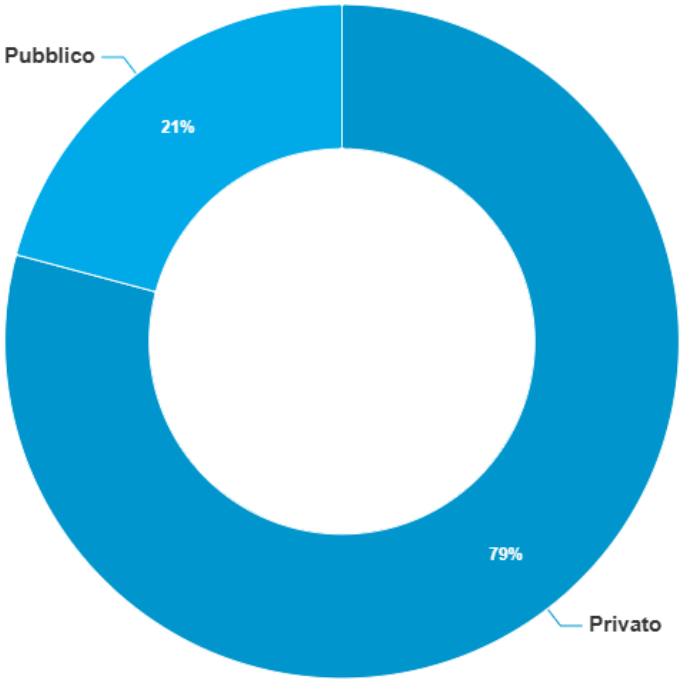


Figura 14 - *distribuzione delle segnalazioni per tipologia di soggetto*

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

maggio 2025