Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

1° SEMESTRE 2025

DATI ED INDICATORI DELLA MINACCIA CYBER IN ITALIA

Servizio Operazioni
e gestione delle crisi cyber

TLP:CLEAR

INTRODUZIONE

Il presente documento presenta numeri e indicatori relativi alle attività operative svolte dall'Agenzia per la Cybersicurezza Nazionale (ACN) nel primo semestre del 2025, mettendoli a confronto con quelli del primo semestre del 2024. I dati analizzati provengono dal CSIRT Italia, articolazione tecnico-operativa dell'Agenzia e punto di riferimento nazionale per le notifiche obbligatorie e volontarie di incidenti previste dalla normativa (tra cui, Perimetro di Sicurezza Nazionale Cibernetica, Legge n. 90 del 2024, D.lgs n.138 del 2024, che recepisce la c.d. Direttiva NIS2). Il CSIRT riceve inoltre informazioni da fonti aperte e commerciali, nonché da enti omologhi nazionali e internazionali, che le condividono spontaneamente o nell'ambito di accordi di collaborazione. Queste informazioni dotano l'ACN 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 o incidenti cyber; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento, come:

- **approfondire le informazioni** a disposizione, analizzando i contenuti anche dal punto vista strettamente tecnico, quale lo studio dei malware, valutando il rischio d'impatto sistemico di vulnerabilità e incidenti;
- **se necessario inviare richieste di informazioni** ai soggetti;
- **fornire supporto da remoto o in loco** ai soggetti impattati;
- **inviare comunicazioni** ai soggetti impattati oppure a tutti i soggetti potenzialmente impattati;
- **pubblicare alert o bollettini**.

Per le definizioni si rimanda al Glossario del CSIRT Italia e alla Tassonomia Cyber dell'ACN mentre per maggiori dettagli sui singoli mesi si può far riferimento agli *Operational Summary* mensili, disponibili pagina dedicata del sito web ACN.

Indice

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 EXECUTIVE SUMMARY

- **Eventi e Incidenti**
  Nel primo semestre 2025 ACN ha censito **1.549 eventi cyber**, in **aumento** del **53**% rispetto allo stesso periodo dell'anno precedente (1° semestre 2024). Il numero di **incidenti con impatto confermato** è stato pari a **346**, in **aumento** del **98**%. Sebbene una parte di tali incrementi siano ascrivibili alle capacità del CSIRT Italia di rinvenire minacce, fattori di rischio e compromissioni in continua evoluzione, e al mutato assetto normativo, specie con l'entrata in vigore della Legge n.90 e del D.lgs n.138 del 2024, i restanti aumenti sono dovuti principalmente a: campagne **DDoS**, **esposizione dati** e **phishing**.
- **Settori interessati**
  Il maggior numero di vittime di eventi sono state registrate nei settori della **Pubblica amministrazione locale**, **Pubblica amministrazione centrale** e **Telecomunicazioni**. Nel settore delle **Telecomunicazioni** il numero significativo è dovuto principalmente ai tentativi di spearphishing avvenuti nel mese di aprile, mentre per quanto riguarda la **Pubblica Amministrazione Locale**, una violazione dei sistemi di un un fornitore di servizi web avvenuta a marzo, con impatti su molteplici amministrazioni, ha causato un insolito numero di vittime. Nella PA Centrale, invece, sono i DDoS, le esposizioni di dati e il phishing a motivare l'ingente numero di casi.
- **Ransomware**
  I ransomware si confermano quale una delle minacce più impattanti, con **91 attacchi** complessivi (nel 1° semestre 2024 furono 92). Gli episodi più significativi del semestre hanno interessato una università, un laboratorio diagnostico ospedaliero e alcuni fornitori di servizi digitali per la PA. Di rilievo anche un attacco avvenuto a febbraio a un'azienda del settore energetico, che ha compromesso la sua capacità di erogare servizi ai clienti, determinando così effetti su diversi operatori del settore.
- **Attacchi DDoS**
  Per quanto riguarda i **DDoS**, si è osservato un **aumento** del 77% nel 1° semestre 2025 con **598** attacchi rispetto ai **336** del 1° semestre 2024. Tali campagne di **hacktivism**, molto intense tra dicembre 2024 e febbraio 2025, hanno subito una progressiva attenuazione nei mesi successivi, per poi ripresentarsi alla fine del semestre. In particolare, la campagna avvenuta a giugno ad opera di attori filorussi è durata **13** giorni di seguito, interessando con **275 attacchi DDoS** un totale di **124** soggetti appartenenti a diversi settori. Gli impatti sono stati – come di consueto per questo tipo di attività – mitigati efficacemente dai soggetti italiani, anche grazie all'attività di allertamento del CSIRT Italia, che comunica tempestivamente contromisure ai soggetti

interessati. In questo semestre, alla stregua del 2024, solo il **13%** degli attacchi ha causato impatti misurabili (ovvero disservizi transienti per gli utenti dei portali attaccati tipicamente della durata di qualche ora).

- **Phishing**
  Nel 1° semestre 2025 sono state rilevate diverse campagne di **phishing**, tra cui una particolarmente intensa nel settore energetico avvenuta nel mese di maggio. Il CSIRT Italia effettua un'attività di rilevamento di pagine web artefatte, specificatamente ai fini di phishing, le quali imitano quelle originali, tipicamente di soggetti istituzionali e imprese parte della propria constituency, per indurre gli utenti ad inserire le credenziali. Nel 1° semestre 2025 tale attività ha permesso di individuare e segnalare **1.530 URL di phishing**.
- **Esposizione dati**
  Nel corso delle attività di monitoraggio delle principali piattaforme di scambio illecito di dati, nel 1° semestre 2025 si è osservato un incremento significativo rispetto al 1° semestre 2024 degli episodi di **esposizione di dati**, che hanno coinvolto organizzazioni appartenenti a settori diversi. Nel complesso, gli eventi di tale tipo sono stati **186**, mentre nel 1° semestre 2024 furono 91. Nel periodo considerato, hanno suscitato particolare attenzione le esposizioni di dati relativi a piattaforme di streaming e servizi di e-commerce (a marzo), quelle afferenti a pubbliche amministrazioni rinvenute ad aprile, i nomi utente ed email associati ad account del social network X rinvenuti e segnalati nello stesso mese. Importanti, in tale contesto, anche i molteplici casi di **vendita di credenziali compromesse** rinvenute dal CSIRT Italia, in particolare riferite a clienti di istituti bancari, nel mese di maggio.
- **Monitoraggio proattivo**
  Tra le attività proattive, effettuate per rilevare vulnerabiltà, compromissioni, e altri fattori di rischio esposti dai soggetti italiani su internet, la più importante è stata quella effettuata a giugno e volta all'individuazione dei soggetti nazionali che esponevano versioni vulnerabili degli applicativi **Citrix NetScaler ADC** e **Gateway**, soluzioni comunemente utilizzate per abilitare l'accesso remoto a reti e servizi e servizi aziendali (VPN, proxy applicativi, autenticazione federata). Ciò a seguito della scoperta di vulnerabilità critiche: la CVE-2025-5777 (*Out-of-Bounds Read*), nota anche come **CitrixBleed 2**, che avrebbe potuto consentire a un attore non autenticato di accedere a dati sensibili in memoria, laddove il sistema fosse configurato come Gateway; la CVE-2025-5349 (*Improper Access Control*), che avrebbe potuto consentire a un attore con accesso alla rete di gestione di ottenere privilegi non autorizzati; e la CVE-2025-6543 (*Buffer Overflow*), potenzialmente sfruttabile per indurre il sistema in uno stato di Denial of Service. In tale attività sono stati **individuati 638 indirizzi IP** appartenenti a soggetti critici, prontamente allertati. Di rilievo anche le attività condotte a maggio per il discovery di dispositivi compromessi utilizzati per la distribuzione di ransomware, anche in seguito all'operazione internazionale **Endgame**, che ha colpito botnet come **IcedID**, **Smokeloader** e **Bumblebee** e consentito l'individuazione di oltre **1.977 dispositivi**. Anche quella di marzo, finalizzata all'individuazione di dispositivi di videosorveglianza compromessi e parte della botnet DDoS denominata Eleven11bot, ha consentito di individuare **1.245 indirizzi IP italiani potenzialmente compromessi** e allertare i soggetti interessati.
- **Vettori di attacco**
  I punti d'ingresso più frequenti delle attività malevole censite sono stati: **campagne malevole via e-mail**, **sfruttamento di vulnerabilità** e l'impiego di **credenziali valide** precedentemente compromesse, in linea con quanto registrato nel 2024.
- **Vulnerabilità**
  Il numero di **nuove vulnerabilità (CVE)** pubblicate nell'ambito del CVE program (`www.cve.org`) è stato pari a **24.098**, sostanzialmente allineato rispetto al 1° semestre 2024.
- **Allertamento**
  Nel 1° semestre 2025 il CSIRT Italia ha inviato **23.144 comunicazioni dirette** ai fini di allertamento preventivo, a seguito dell'individuazione di asset compromessi,

vulnerabili o esposti in maniera inopportuna, o per altri fattori di rischio, nei confronti dei soggetti della constituency nazionale. Nel 1° semestre 2024 le comunicazioni inviate a tal scopo furono **21.224**. Oltre alle comunicazioni dirette, nel 1° semestre 2025 sono stati pubblicati **329 alert** sul sito web del CSIRT Italia (`https://www.acn.gov.it/portale/csirt-italia`), relativi a vulnerabilità e fattori di rischio, corredati dalle necessarie contromisure, mentre, nel corso del 1° semestre 2024 gli alert pubblicati sono stati **289**.

Il prosieguo del documento presenta, in **questo Capitolo**, i principali numeri e le vulnerabilità del 1° semestre 2025; nel **Capitolo 2** un focus sugli eventi e incidenti, con settori impattati, tipologia di minacce rilevate e loro distribuzione sui settori nonché distribuzione geografica delle vittime; nel **Capitolo 3** un approfondimento sulle **vulnerabilità** più gravi del semestre con la loro distribuzione sui vendor e le CWE più comuni; i dettagli sulle **minacce ransomware, DDoS e malware** sono riportati nel **Capitolo 4** mentre il **Capitolo 5** mostra i risultati del **monitoraggio proattivo**, con i numeri e le tipologie di dispositivi e servizi a rischio individuati dal CSIRT Italia.
Per maggiori dettagli sui singoli mesi del 1° semestre 2025 si può far riferimento agli *Operational Summary* mensili, disponibili pagina dedicata del sito web ACN.

I NUMERI DEL 1° SEMESTRE 2025

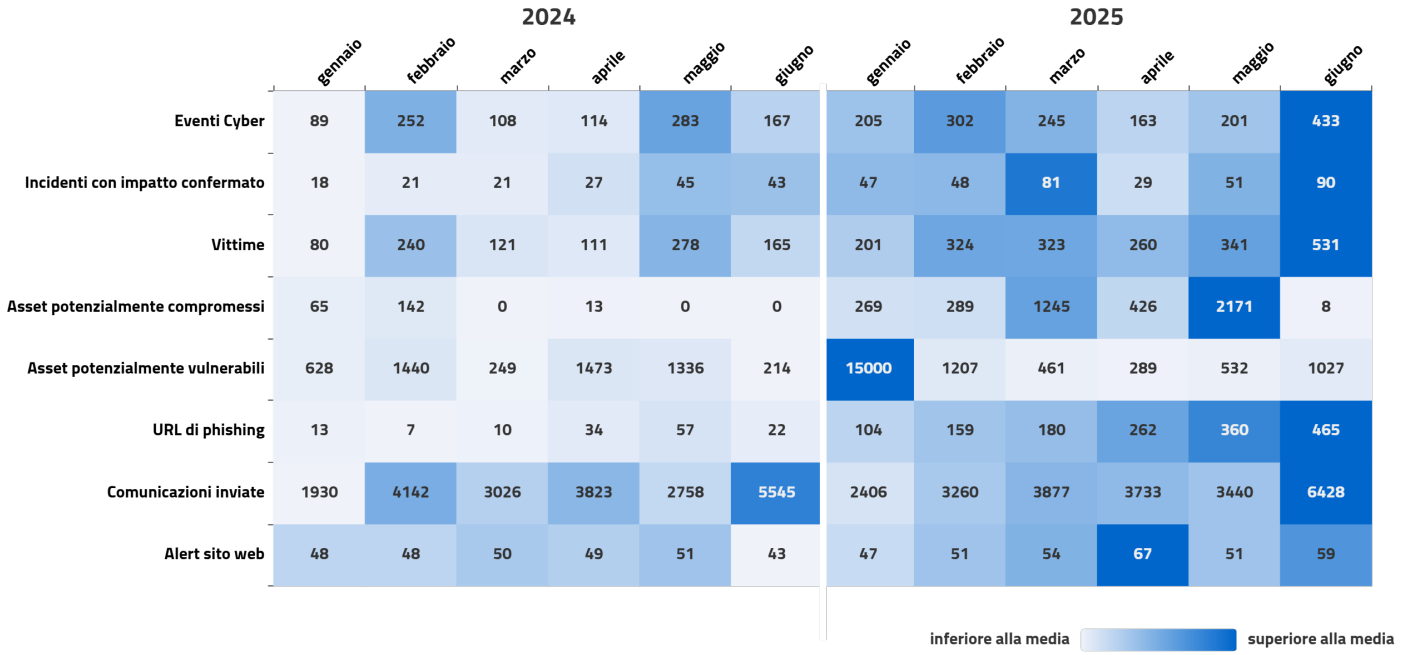

Figura 1 - *indicatori delle attività operative nel 1° semestre 2025 e nel 1° semestre 2024*

- **1.549** eventi cyber, in **aumento** (**+536**);
- **2.367** vittime, in **aumento** (**+1.374**);
- **829** vittime della constituency[1], in **aumento** (**+562**);
- **346** incidenti con impatto confermato, in **aumento** (**+171**);
- **4.408** asset potenzialmente compromessi, in **aumento** (**+4.188**);
- **18.516** asset potenzialmente vulnerabili, in **aumento** (**+13.176**);
- **329** alert sul sito web del CSIRT Italia, in **aumento** (**+40**);
- **23.144** comunicazioni inviate, in **aumento** (**+1.920**);
- **24.098** nuove CVE, in **aumento** (**+4.067**).

[1]La constituency è l'insieme dei soggetti che operano nei settori NIS, Perimetro, Telco o nella Pubblica amministrazione, nei confronti dei quali il CSIRT Italia offre servizi e supporto in termini di prevenzione, monitoraggio, rilevamento, analisi e risposta al fine di prevenire e gestire gli eventi cibernetici. Sul sito ACN è disponibile un documento di approfondimento sulla constituency del CSIRT Italia.

PRODOTTI VULNERABILI

Di seguito una selezione delle vulnerabilità particolarmente importanti, organizzate per prodotto o produttore che nel 1° semestre 2025 sono stati oggetto di specifici alert pubblicati sul sito web del CSIRT Italia o di allertamento tramite comunicazioni dirette. I soggetti utilizzatori di tali prodotti sono invitati a verificare l'avvenuta adozione delle azioni di mitigazioni rilasciate dal vendor o riportate negli alert referenziati di seguito.

Gennaio:

- **Zyxel** (CVE-2024-40891) Link all'alert;
- **Fortinet** (CVE-2024-55591) Link all'alert;
- **Cacti** (CVE-2024-45598, CVE-2024-54145, CVE-2024-54146, CVE-2025-22604, CVE-2025-24367). Link all'alert;
- **Ivanti** (CVE-2025-0282, CVE-2025-0283) Link all'alert;
- **Howyar** (CVE-2024-7344) Link all'alert;
- **Zabbix** (CVE-2024-42327) Link all'alert;
- **Mitel** (CVE-2024-41713, CVE-2024-35286) Link all'alert;
- **Ivanti Cloud Service Application** (CVE-2024-11773, CVE-2024-11772, CVE-2024-11639) Link all'alert;
- **Veeam Service Provider Console** (CVE-2024-42449, CVE-2024-42448) Link all'alert;
- **Cleo Harmony** (CVE-2024-50623) Link all'alert;
- **Pandora FMS** (CVE-2024-11320).

Febbraio:

- **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.

Marzo:

- **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;

Aprile:

- **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.

Maggio:

- **Mozilla** (CVE-2025-4918), (CVE-2025-4919) Link all'alert;
- **Microsoft Active Directory** 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;

Giugno:

- **Microsoft** Link all'alert;
- **Roundcube** (CVE-2025-49113) Link all'alert;
- **CraftCMS** (CVE-2024-56145, CVE-2025-35939) Link all'alert;
- **Citrix** (CVE-2025-6543) Link all'alert;
- **Notepad++** (CVE-2025-49144) Link all'alert;
- **Citrix Netscaler ADC e Gateway** (CVE-2025-5777, CVE-2025-5349) Link all'alert;
- **Grafana** (CVE-2025-4123) Link all'alert;
- **Veeam Backup & Replication** (CVE-2025-23121) Link all'alert;
- **PostgreSQL pgAdmin** (CVE-2025-2945) Link all'alert;
- **BeyondTrust Remote Support (RS) e Privileged Remote Access (PRA)** (CVE-2025-5309) Link all'alert;
- **Mattermost** (CVE-2025-4981) Link all'alert;
- **Cisco Identity Services Engine (ISE) e ISE Passive Identity Connector (ISE-PIC)** (CVE-2025-20282, CVE-2025-20281) Link all'alert.

2 EVENTI ED INCIDENTI

Nel 1° semestre 2025 sono stati individuati **1.549** eventi cyber, in **aumento** del 53% rispetto al 1° semestre 2024. Questi ultimi hanno **interessato 1.357 soggetti nazionali**[2]: 829 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 1.549 eventi cyber, **346 sono stati classificati quali incidenti**, in **aumento** del 98% rispetto a quelli registrati nel 1° semestre 2024. I picchi di febbraio e giugno sono dovuti alle campagne di DDoS da parte di hacktivisti.

La Figura 2 mostra l'andamento del numero di eventi e incidenti del semestre, evidenziandone la media del periodo.

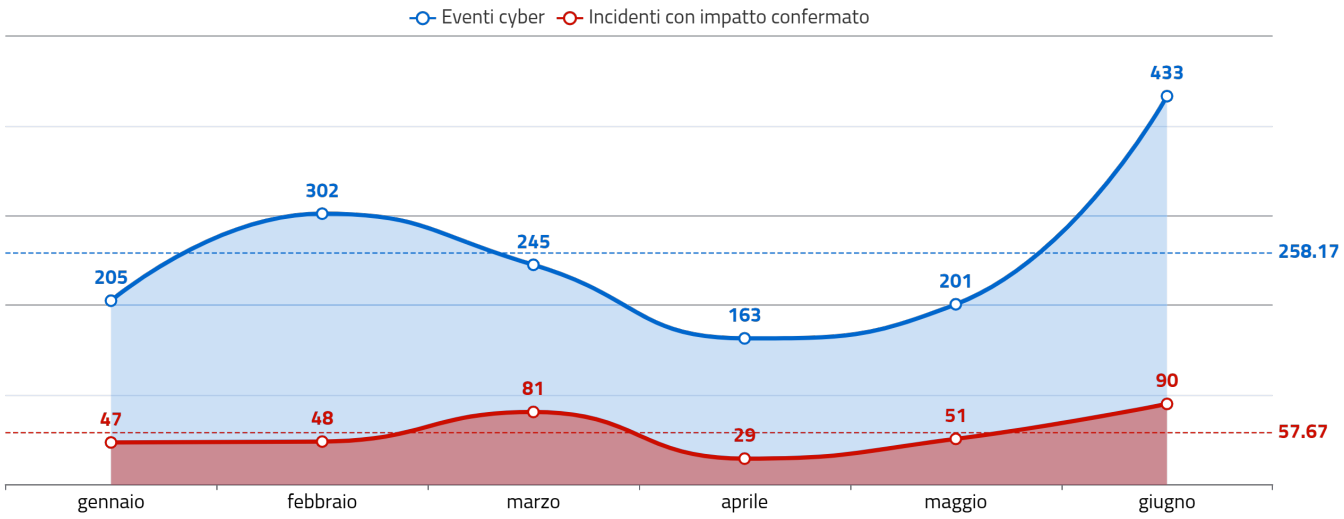

Figura 2 - *andamento del numero di eventi e incidenti del 1° semestre 2025*

[2]Alcuni soggetti sono stati interessati più volte. Il numero di vittime non univoche è stato 2.367.

2.1 Settori impattati

In Figura 3 si riporta il numero di vittime di eventi per settore impattato[3] nel 1° semestre 2025 e nel 1° semestre 2024. Si evidenza altresì la variazione percentuale tra i due valori. Emerge come gli aumenti siano distribuiti su tutti i settori. L'aumento nella Pubblica amministrazione locale è principalmente dovuto agli attacchi DDoS, che nel periodo recente, hanno iniziato ad interessare questo settore in maniera particolare.

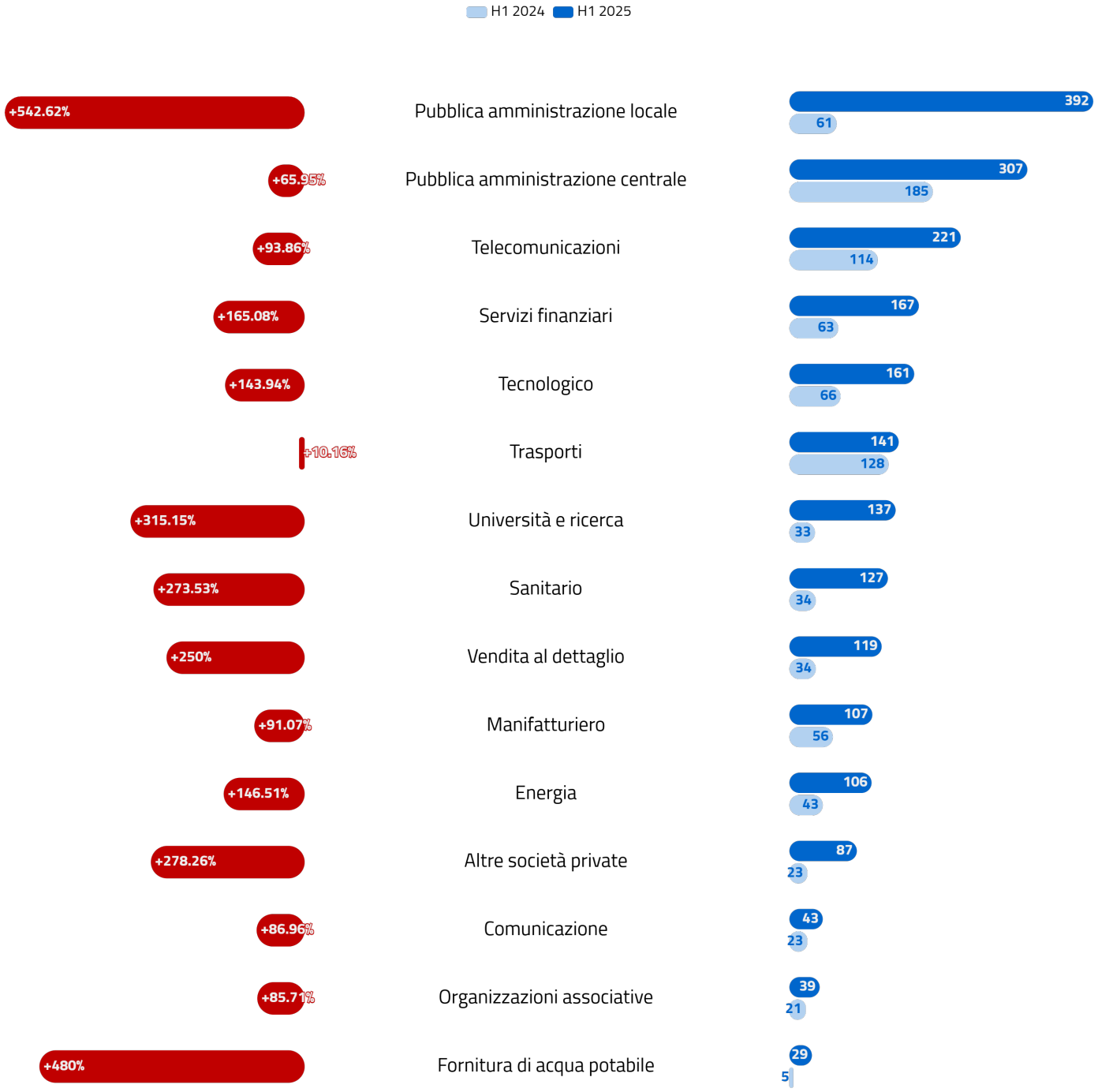

Figura 3 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto al 1° semestre 2024 (top 15)*

[3] Si noti che ogni evento può avere più vittime afferenti ad uno o più settori di attività e che una vittima può operare in più settori. Talvolta non è possibile associare un evento ad una vittima e la vittima ad un settore.

2.2 Tipologia di minacce negli eventi

In Figura 4 si riporta il numero di minacce rilevate negli eventi[4] nel 1° semestre 2025 e nel 1° semestre 2024. Si evidenza altresì la variazione percentuale tra i due valori.

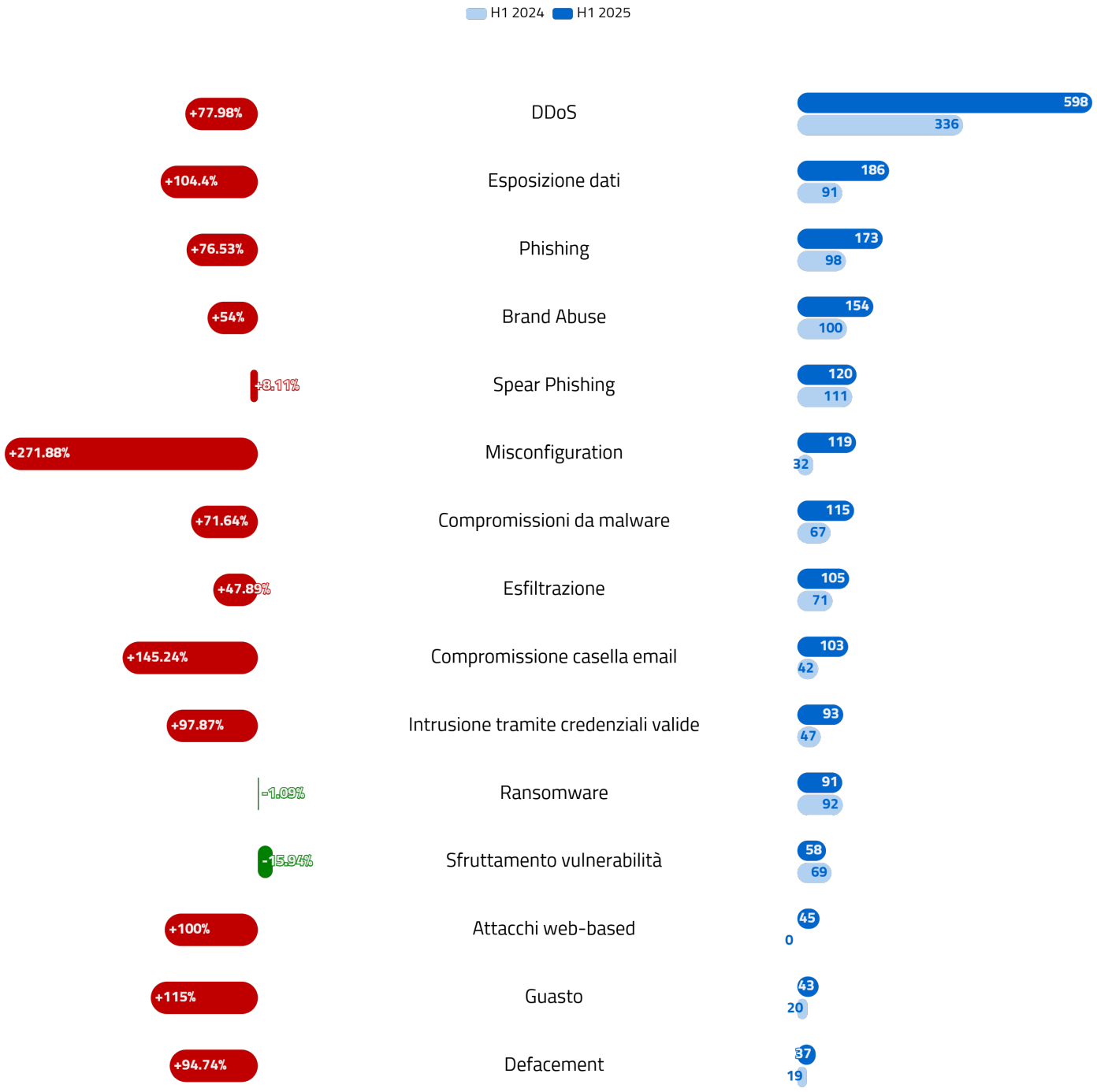

Figura 4 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al 1° semestre 2024*

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

2.3 Distribuzione delle minacce per settore

In Figura 5 si riporta, per ogni settore, il numero di vittime che hanno subito la minaccia specificata, analizzando gli eventi del 1° semestre 2025. Si ricorda che ad un evento possono essere associate più minacce e più vittime. Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn). Emerge come il DDoS abbia interessato principalmente la Pubblica Amministrazione, i trasporti e i servizi finanziari; il ransomware il manifatturiero; le esposizioni di dati abbiano interessato soggetti in una molteplicità di settori critici; lo spear phishing il settore delle telecomunicazioni e così via. In Figura sono mostrati solo i 15 settori più interessati dalle minacce.

	Pubblica amministrazione centrale	Pubblica amministrazione locale	Servizi finanziari	Telecomunicazioni	Tecnologico	Energia	Trasporti	Vendita al dettaglio	Manifatturiero	Sanitario	Università e ricerca	Altre società private	Comunicazione	Organizzazioni associative	Fornitura di acqua potabile
Esposizione dati	92	80	86	70	56	43	54	33	24	82	99	22	12	6	17
DDoS	102	238	37	29	19	9	61	11	12	2	2		6	10	11
Misconfiguration	30	11	3	4	28	2	5	48	15	4	23	30	14	16	1
Esfiltrazione	4	5	57	11	15	23	20	20	28	6	3	18	2	1	1
Phishing	51	10	10	20	15	16	9	15	20	20	11	9	1	4	1
Compromissioni da malware	8	19	55	20	15	22	14	10	15	6	4	9	1	1	1
Compromissione casella email	29	11	2	22	13	9	7	18	9	18	27	7		2	
Intrusione tramite credenziali valide	17	5	85	12	15	2	5	10	7	8	2	4		1	
Brand Abuse	53	7	6	23	14	18	3	3	11	9	2	6	7	2	1
Spear Phishing	20	4	2	65	9	29	3	4	3	9	1	5		2	
Attacchi web-based	2	29		4	11	20	1	6	8	3	2	10	1	2	
Ransomware	1	6	4	1	13	8	2	7	23	3	2	8	1	1	
Supply chain attack			52	2	2	2	3								
Sfruttamento vulnerabilità	3	7		4	12	2	5	5	7	5	2	6		2	1
Guasto	3	1	3	15	10	6	6			3					
SCADA/ICS attack		3		1	1	9		4	12			2			1
Defacement	1	1			5	1		6	6	2		7	1	1	
DoS	3	10	1		1	5	7	2				1			
Scansione attiva su credenziali	2	3	1	9	2	1	5		1			1	1		1
Diffusione malware tramite email	6		2	5	1	2		2	1		1	2			
Smishing	8		5	1	1	1									
Typosquatting	5			1	1	3				1			5		
Cybersquatting	5				1					1			7		
Scansioni attive sul perimetro di rete	4		1	1	3	2		1	1						
Spam e scam	3				1	1			1	1					

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

nDistribuzione geografica delle vittime

I 1.549 eventi cyber hanno interessato **2.367** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

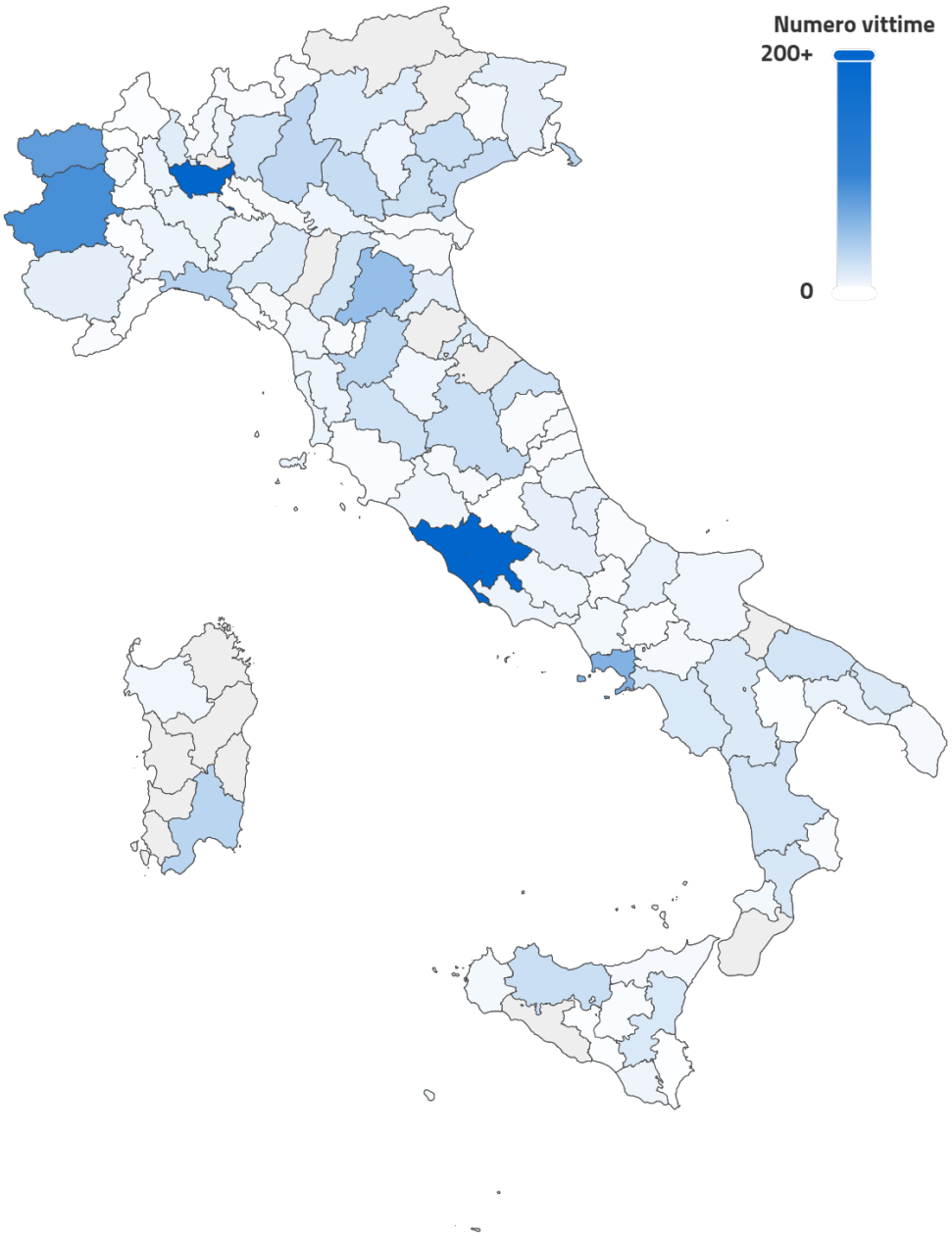

Figura 6 - *distribuzione delle vittime degli eventi cyber*

3 VULNERABILITÀ

Nel 1° semestre 2025 sono state pubblicate[5] **24.098** nuove CVE, in **aumento** (**+4.067**) rispetto al 1° semestre 2024. Le più gravi di queste divengono oggetto di comunicazioni dirette da parte del CSIRT Italia ai soggetti della constituency e di specifico alert sul sito web, corredati dalle contromisure da adottare. In questa sezione si riportano quelle più gravi oggetto di alert, evidenziando il prodotto affetto e il link all'alert sul sito web. Le vulnerabilità vengono altresì analizzate e organizzate per vendor, per prodotto e per tipologia, come mostrato più avanti.
All'indirizzo https://www.acn.gov.it/portale/csirt-italia/alert-e-bollettini è possibile accedere a tutti gli altri alert pubblicati.

3.1 Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia

Nel 1° semestre 2025 gli alert sulle vulnerabilità oggetto di pubblicazione sul sito del CSIRT Italia sono stati **329**. Le vulnerabilità particolarmente gravi, riportate di seguito ordinate per stima d'impatto sistemico[6], sono state quelle 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;
- **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

[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/`.

[6]La stima d'impatto sistemico è un valore da 0 a 100, associato a ogni vulnerabilità esaminata dal CSIRT Italia tenendo conto di diversi parametri, tra i quali il CVSS, la disponibilità di patch/workaround e Proof of Concept (POC), la diffusione dei software/dispositivi interessati nella costituency.

"Moderate Severity" e non ha ancora rilasciato una patch (stima di impatto sistemico **82,05/100**). Link all'alert del 27/05/2025;

- **Microsoft**: il CSIRT fornisce la seguente guida per prevenire e mitigare potenziali effetti indesiderati derivanti dallo sfruttamento di una vulnerabilità recentemente individuata nella funzionalità dMSA (delegated Managed Service Account), trattata nell'ambito del BL01/250527/CSIRT-ITA. Tale funzionalità, introdotta in Windows Server 2025 all'interno di Active Directory, potrebbe consentire l'elevazione dei privilegi utente (stima di impatto sistemico **82,05/100**). Link all'alert del 04/06/2025;
- **Zyxel**: ricercatori di sicurezza hanno recentemente rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2024-40891 – sfruttata come 0-day – presente su dispositivi DSL CPE non più supportati da Zyxel (stima di impatto sistemico **81,79/100**). Link all'alert del 30/01/2025;
- **Roundcube**: aggiornamenti di sicurezza sanano una vulnerabilità con gravità "critica" in Roundcube Webmail, noto gestore di posta elettronica open source. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato remoto autenticato di eseguire codice arbitrario sui sistemi target (stima di impatto sistemico **79,35/100**). Link all'alert del 03/06/2025;
- **pgAdmin**: rilasciato aggiornamento che risolve 2 vulnerabilità di sicurezza, con gravità "critica", in pgAdmin, 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;
- **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;
- **Citrix**: rilevate 2 nuove vulnerabilità di sicurezza, di cui una con gravità "critica" e una con gravità "alta", nei prodotti NetScaler ADC e NetScaler Gateway". Tali vulnerabilità potrebbero permettere, ad un utente malevolo, l'accesso non autorizzato all'interfaccia di gestione dei dispositivi e la potenziale divulgazione di informazioni sensibili (stima di impatto sistemico **79,23/100**). Link all'alert del 17/06/2025;
- **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;
- **CraftCMS**: rilevato lo sfruttamento attivo delle vulnerabilità CVE-2024-56145 e CVE-2025-35939 relative a Craft CMS (stima di impatto sistemico **79,23/100**). Link all'alert del 03/06/2025;
- **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;
- **Fortinet**: ricercatori di sicurezza hanno recentemente rilevato una campagna di sfruttamento della vulnerabilità CVE-2024-55591, con gravita "critica", relativa a firewall Fortinet, che prende di mira le interfacce di gestione esposte pubblicamente su internet di FortiOS e FortiProxy (stima di impatto sistemico **78,97/100**). Link all'alert del 14/01/2025;
- **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;

- **Cacti**: rilasciati aggiornamenti che risolvono 6 vulnerabilità, di cui una con gravità "critica" e una con gravità "alta", in Cacti, noto web tool open-source che consente la visualizzazione di grafici per il monitoraggio delle reti. Tali vulnerabilità, qualora sfruttate, potrebbero permettere ad un utente malintenzionato remoto, il bypass dei meccanismi di sicurezza, l'esecuzione di codice arbitrario e l'accesso arbitrario in lettura/scrittura a file sui sistemi target (stima di impatto sistemico **78,33/100**). Link all'alert del 27/01/2025;
- **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;
- **Ivanti**: Ivanti rilascia aggiornamenti di sicurezza che risolvono 2 vulnerabilità, di cui una con gravità "critica" e una con gravità "alta", nei prodotti ICS (Ivanti Connect Secure), IPS (Ivanti Policy Secure) e Ivanti Neurons (stima di impatto sistemico **78,20/100**). Link all'alert del 09/01/2025;
- **Asus**: e' stata 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;
- **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;
- **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;
- **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;
- **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;
- **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 remoto di eseguire codice arbitrario sul sistema interessato (stima di impatto sistemico **76,28/100**). Link all'alert del 11/03/2025;
- **Citrix**: rilevata una nuova vulnerabilità di sicurezza, con gravità "critica", nei prodotti "NetScaler ADC" e "NetScaler Gateway". Tale vulnerabilità potrebbe consentire a un utente malintenzionato di causare l'indisponibilità del servizio sui sistemi interessati (stima di impatto sistemico **75,89/100**). Link all'alert del 25/06/2025;

3.2 Distribuzione delle vulnerabilità sui vendor

In Figura 7 è riportato il numero delle vulnerabilità rilevate distribuite tra i principali vendor.

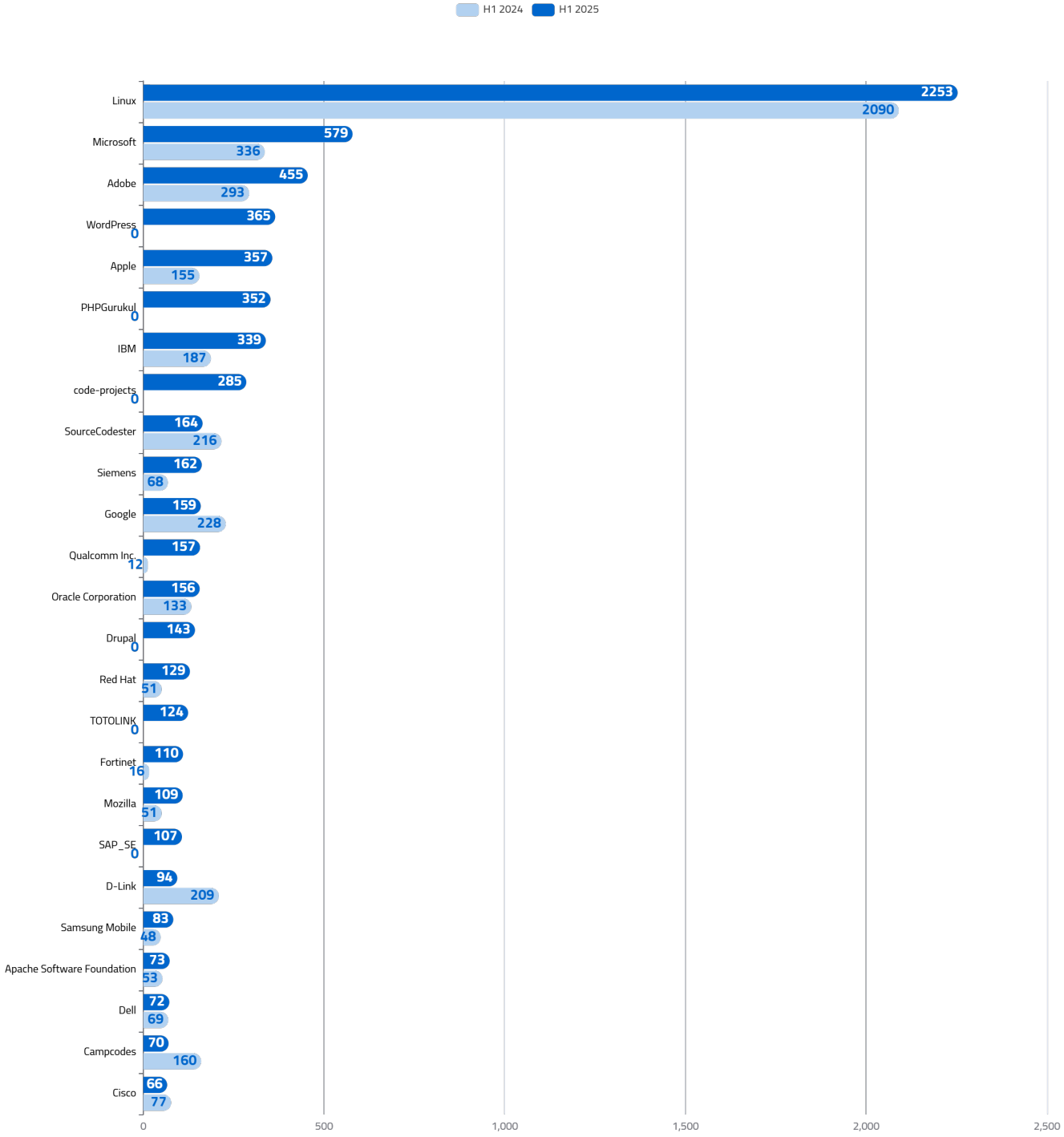

Figura 7 - *top 25 produttori affetti da vulnerabilità nel 1° semestre 2025 e 1° semestre 2024*

In Figura 8 è riportato, invece, il numero delle vulnerabilità rilevate distribuite tra i principali prodotti.

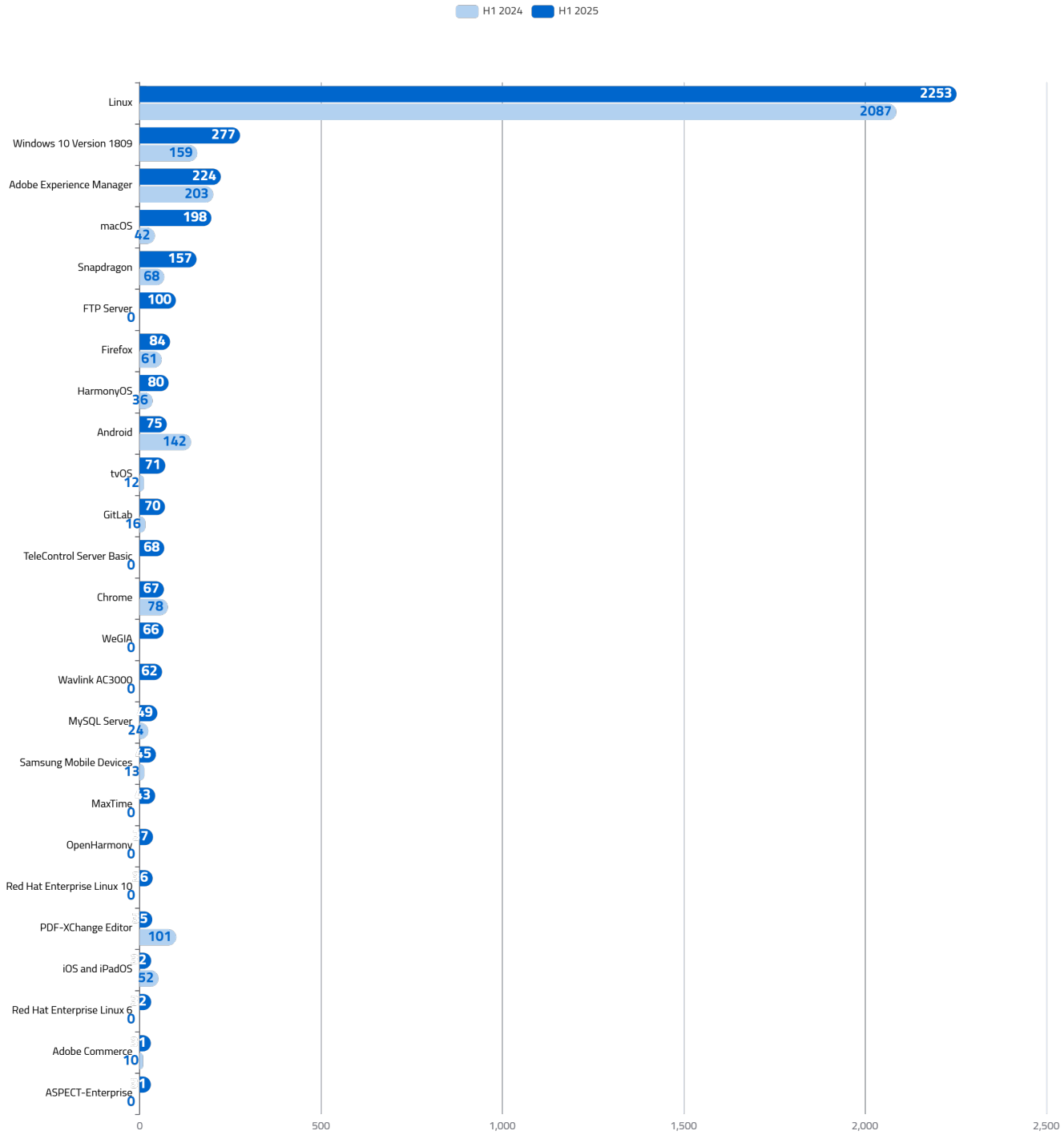

Figura 8 - *top 25 prodotti affetti da vulnerabilità nel 1° semestre 2025 e 1° semestre 2024*

3.3 CWE nel 1° semestre 2025

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

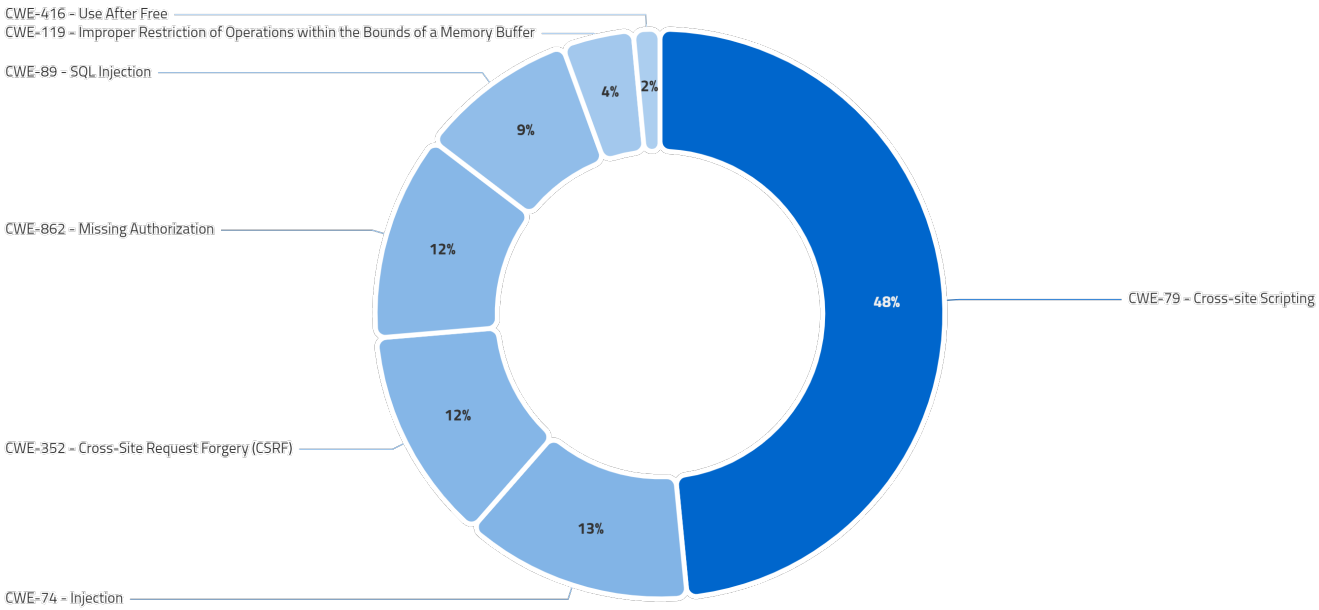

Figura 9 - *top 5 CWE nel 1° semestre 2025*

4 MINACCIA

In questa sezione si riporta un dettaglio sulle minacce ransomware e DDoS, anche in termini di rivendicazioni effettuate dai gruppi hacker in Italia ed UE, mentre per il malware uno spaccato sul numero degli IoC[7] condivisi dal CSIRT Italia tramite piattaforma MISP[8], in modo da caratterizzarne le tipologie più frequenti.

4.1 Ransomware: distribuzione delle vittime

Nel 1° semestre 2025, il 95% degli attacchi ransomware ha colpito soggetti a minor criticità, mentre il 5% ha coinvolto soggetti con obbligo di notifica. Questo conferma la tendenza, già emersa nel 1° semestre 2024, di questa tipologia di attaccanti a colpire maggiormente obiettivi meno strutturati in termini di capacità di cybersicurezza.

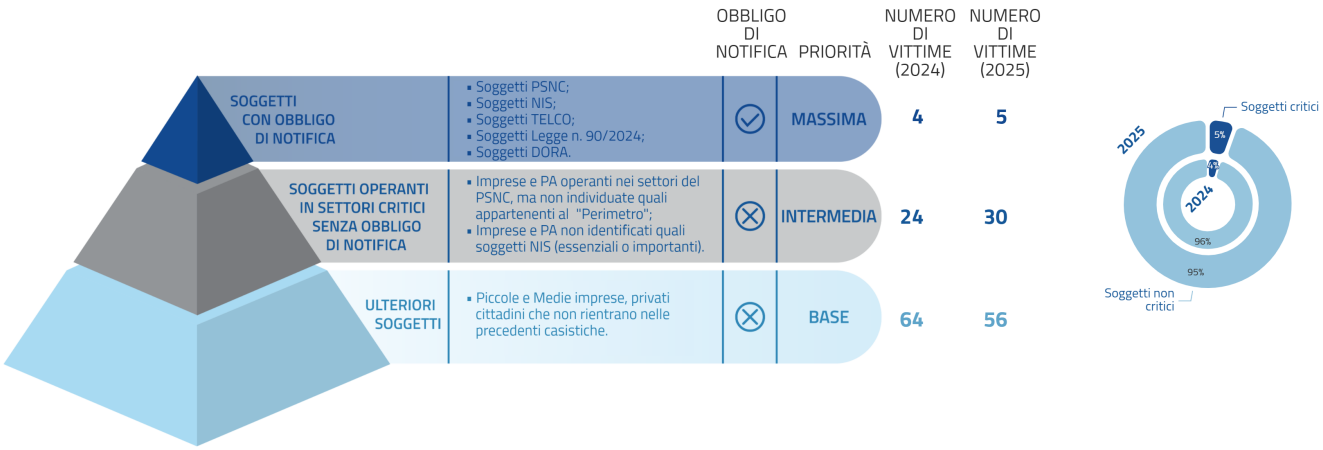

Figura 10 - *distribuzione delle vittime di ransomware in base alla loro criticità*

[7] IoC (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 (Malware Information Sharing Platform) è una soluzione software open source per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di sicurezza informatica e minacce cyber.

4.2 Rivendicazioni ransomware

Il monitoraggio di fonti aperte nel 1° semestre 2025 ha permesso di individuare **99** rivendicazioni di attacchi ransomware a danno di soggetti italiani.

Il grafico in Figura 11 mostra l'andamento delle rivendicazioni nel corso del 1° semestre 2025 e del 1° semestre 2024.

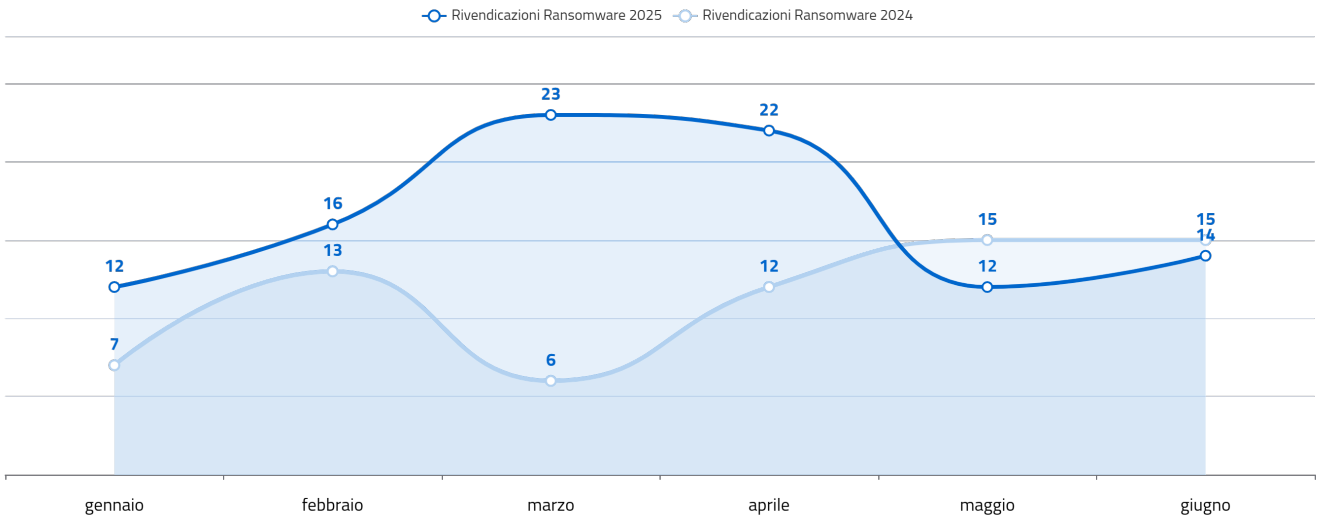

Figura 11 - *andamento delle rivendicazioni Ransomware*

Il grafico in Figura 12 mostra i gruppi più attivi in termini di rivendicazioni in Italia. I gruppi con meno dell'1% di rivendicazioni ricandono nella categoria "altro".

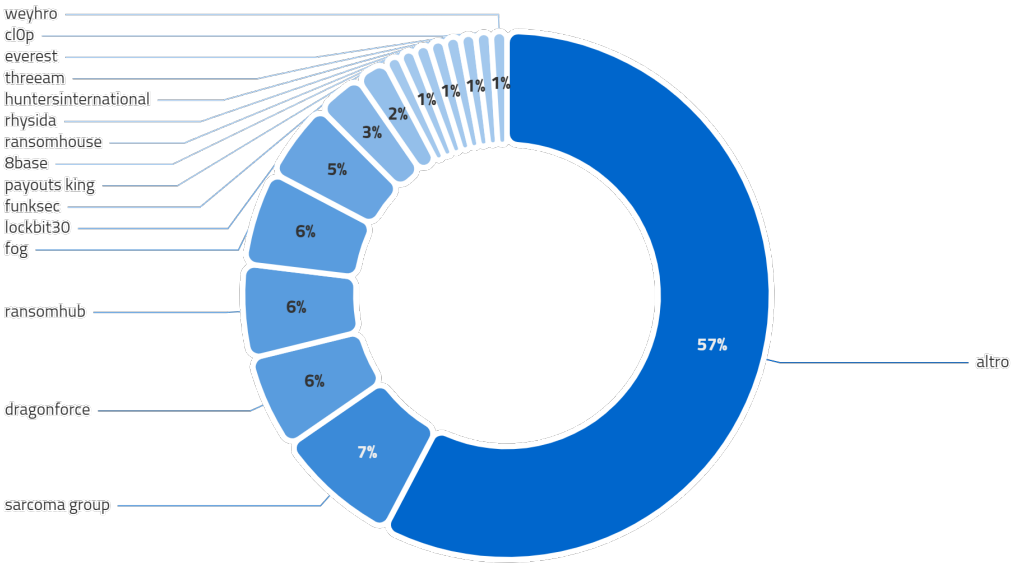

Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

4.3 Rivendicazioni DDoS

Nel 1° semestre 2025 sono state individuate[9] **492** rivendicazioni di attacchi DDoS in danno di soggetti italiani.

Il grafico in Figura 13 mostra l'andamento delle rivendicazioni DDoS nel corso del 1° semestre 2025 e del 1° semestre 2024.

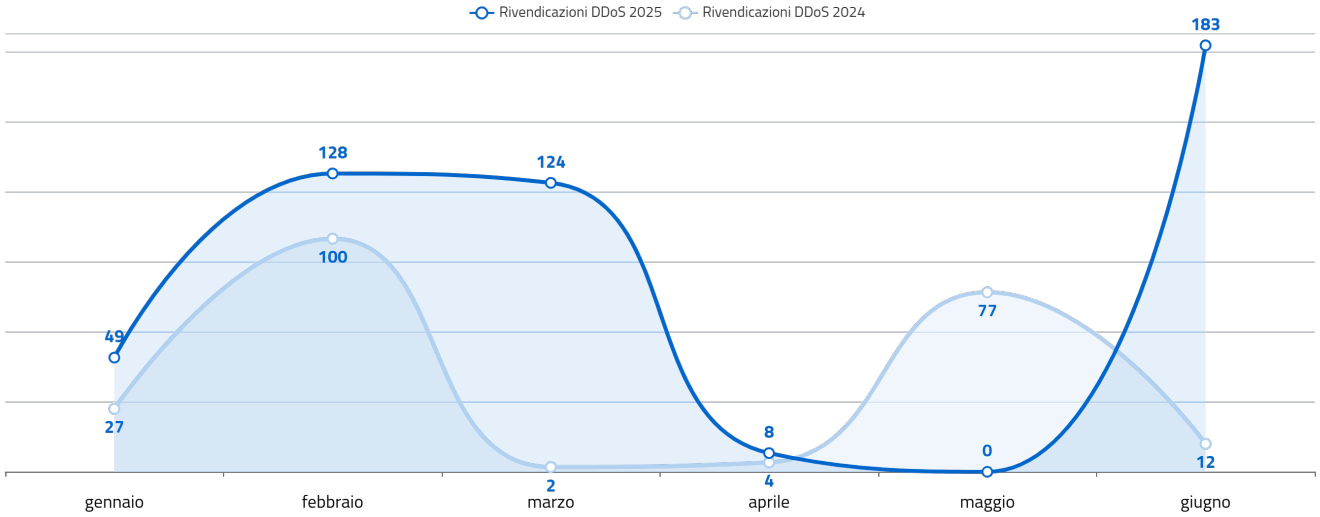

Figura 13 - *andamento delle rivendicazioni DDoS*

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

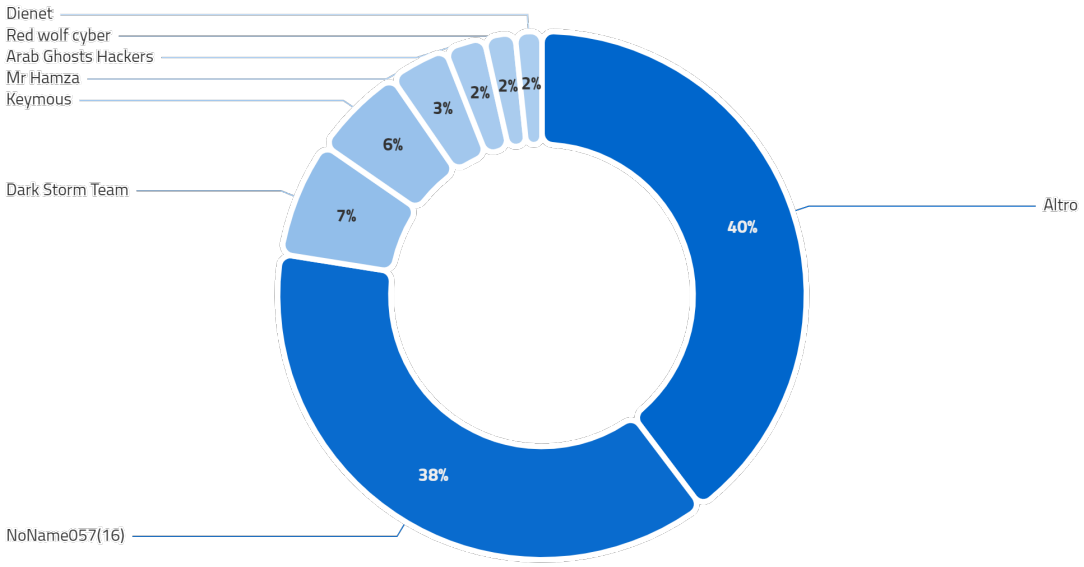

Figura 14 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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

4.4 Indicatori di Compromissione (IoC) per famiglia di malware

In Figura 15 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 .

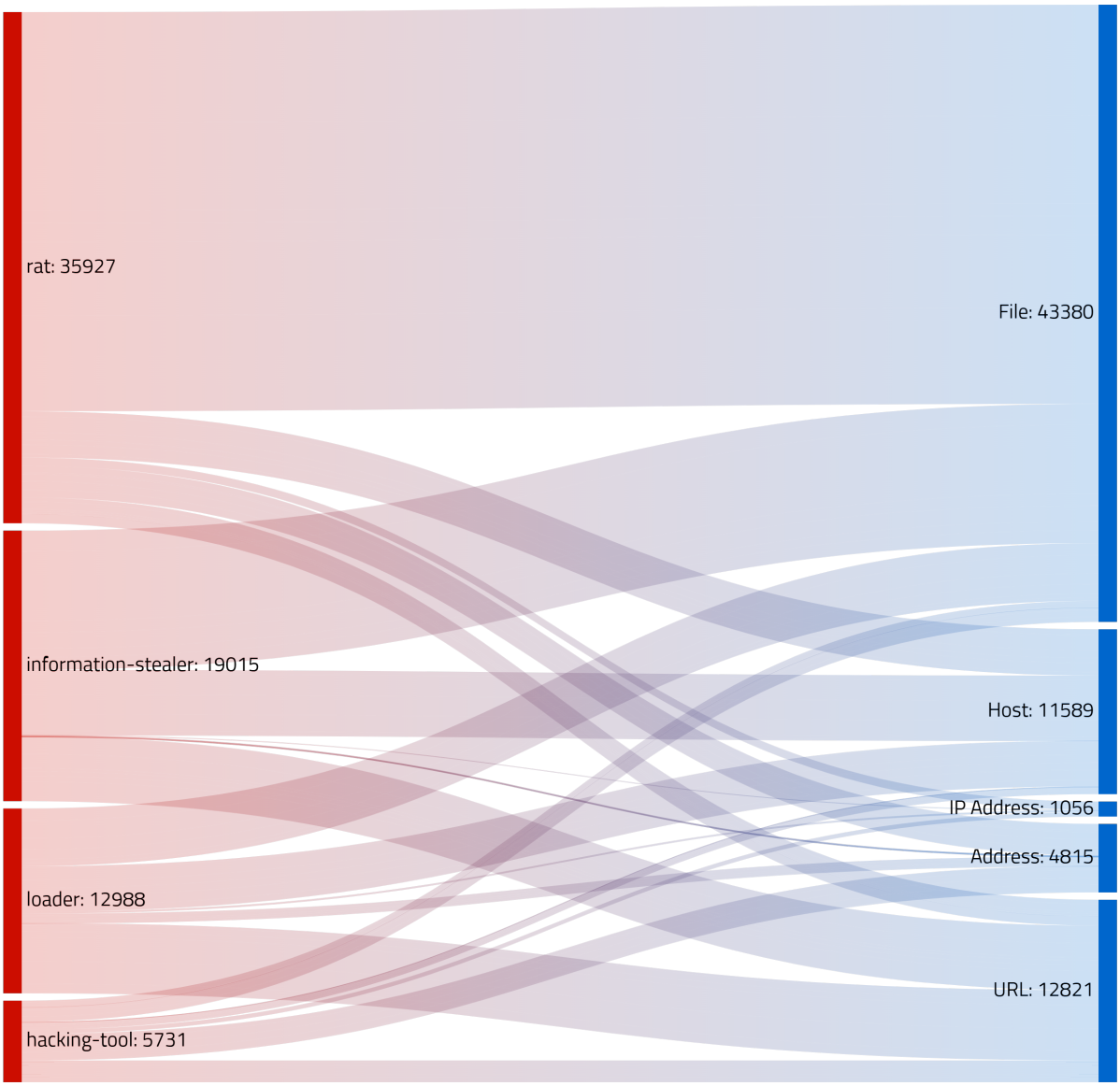

Figura 15 - *numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware*

5 MONITORAGGIO

L'ACN porta avanti attività di monitoraggio proattivo al fine di individuare e segnalare tempestivamente ai soggetti della constituency l'esposizione a specifiche criticità, che possono essere sfruttate, o che sono già in corso di sfruttamento. A valle dell'individuazione di tali criticità, il CSIRT Italia contatta i soggetti a rischio e, qualora risultino particolarmente diffuse, svolge opera di condivisione degli alert, sia tramite portale pubblico che attraverso i canali social dedicati (X, Telegram).
Durante il 1° semestre 2025 sono stati segnalati:

- **1.530 indirizzi web di phishing**, ovvero pagine web artefatte, contenenti riferimenti espliciti o simili a pagine web di circa **201** soggetti pubblici o privati della constituency, presumibilmente utilizzate per ingannare gli utenti e carpire credenziali;
- **4.408 dispositivi o servizi IT potenzialmente compromessi**, ovvero per i quali è stato rilevato un comportamento associabile a un'attività malevola in corso. Relativamente a tali dispositivi o servizi sono state inviate **384** comunicazioni, di cui il **12,5%** verso soggetti pubblici e **87,5%** verso soggetti privati;
- **18.516 dispositivi o servizi IT che esponevano potenziali rischi**, come ad esempio versioni di software vulnerabili, per i quali sono state inviate **2.239** comunicazioni. Di queste il **23%** verso soggetti pubblici e **77%** verso soggetti privati.

Con particolare riguardo a quest'ultima fattispecie, risulta di interesse soffermarsi sia sulle categorie di dispositivi e servizi maggiormente esposti al pericolo di sfruttamento delle vulnerabilità, sia sulle tipologie di vulnerabilità da cui origina tale rischio. Raggruppando i dispositivi e servizi a rischio segnalati per categorie (Figura 16), si evince come tra le categorie più esposte al pericolo vi sia quella delle tecnologie per il lavoro remoto (principalmente *Virtual Private Network* e *Virtual Desktop*). Ciò è dovuto non solo al numero di vulnerabilità gravi emerse nell'ultimo anno su tali dispositivi, ma anche alla loro maggiore intrinseca esposizione ai rischi, in quanto devono essere raggiungibili direttamente tramite Internet per consentire l'accesso da remoto degli utenti.

Il grafico in figura 16 riporta il numero di asset a rischio segnalati suddivisi per categoria (top 10).

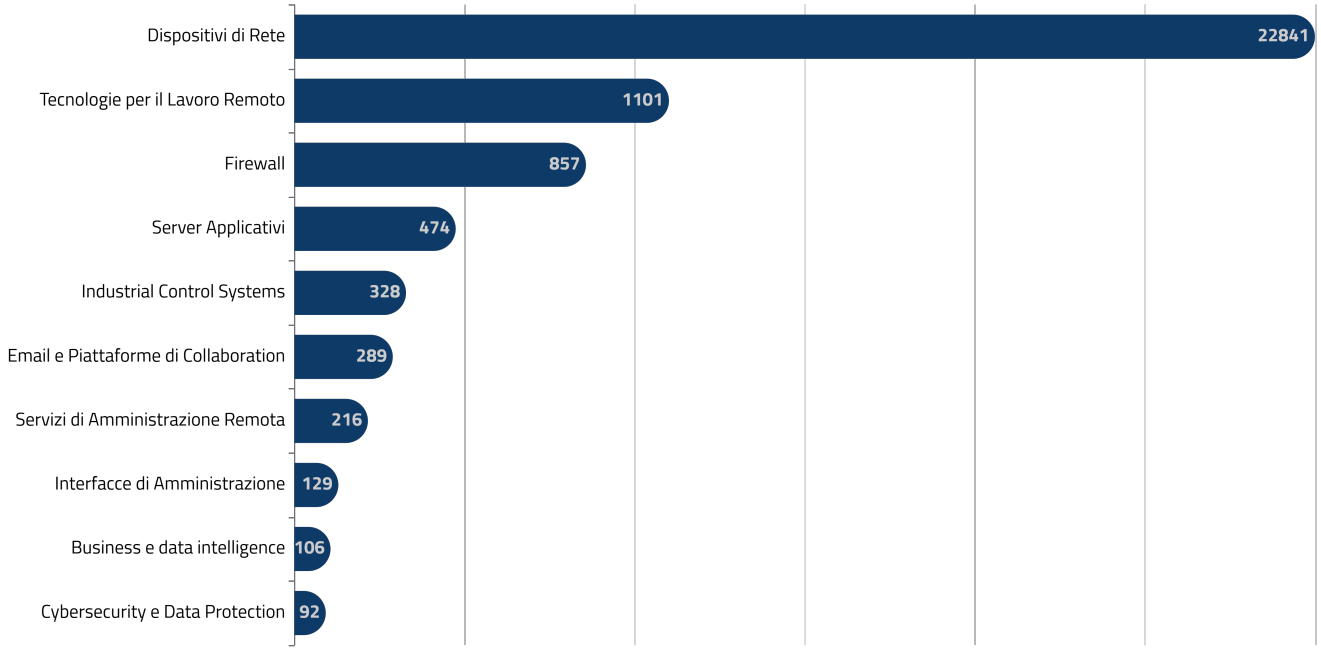

Figura 16 - *Numero di asset a rischio segnalati suddivisi per categoria*

Nella figura 17, invece, gli *asset* a rischio sono divisi a seconda delle tipologie di vulnerabilità, rinvenute e segnalate ai soggetti, con la relativa specifica del livello di gravità.

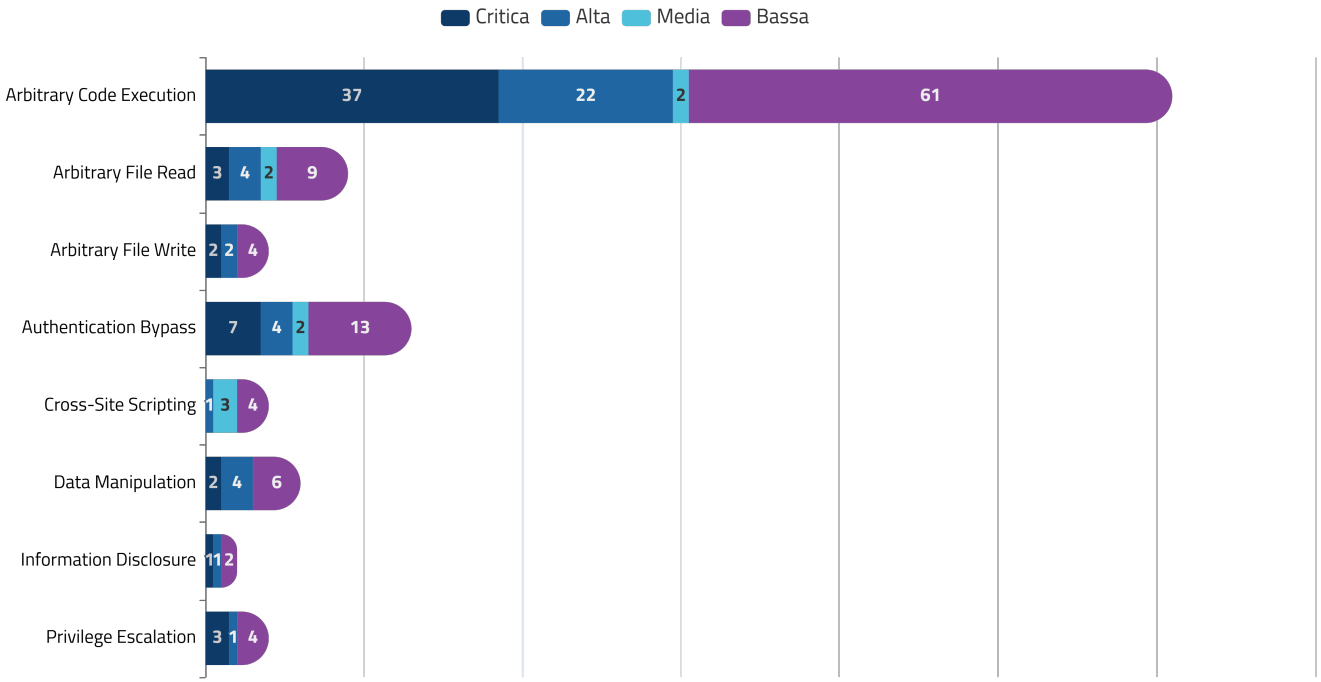

Figura 17 - *Tipologia e gravità delle vulnerabilità rinvenute e segnalate negli asset a rischio*

5.1 Comunicazioni dirette

Nel 1° semestre 2025 sono state diramate un totale di **2.238** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **3.985** servizi a rischio. In Figura 18 viene riportata la distribuzione delle segnalazioni per tipologia di soggetto e prodotto e di seguito si riportano i dettagli e i link agli alert (ove presenti) delle campagne di comunicazione di allertamento svolte dal CSIRT Italia nei vari mesi, evidenziando il prodotto interessato.

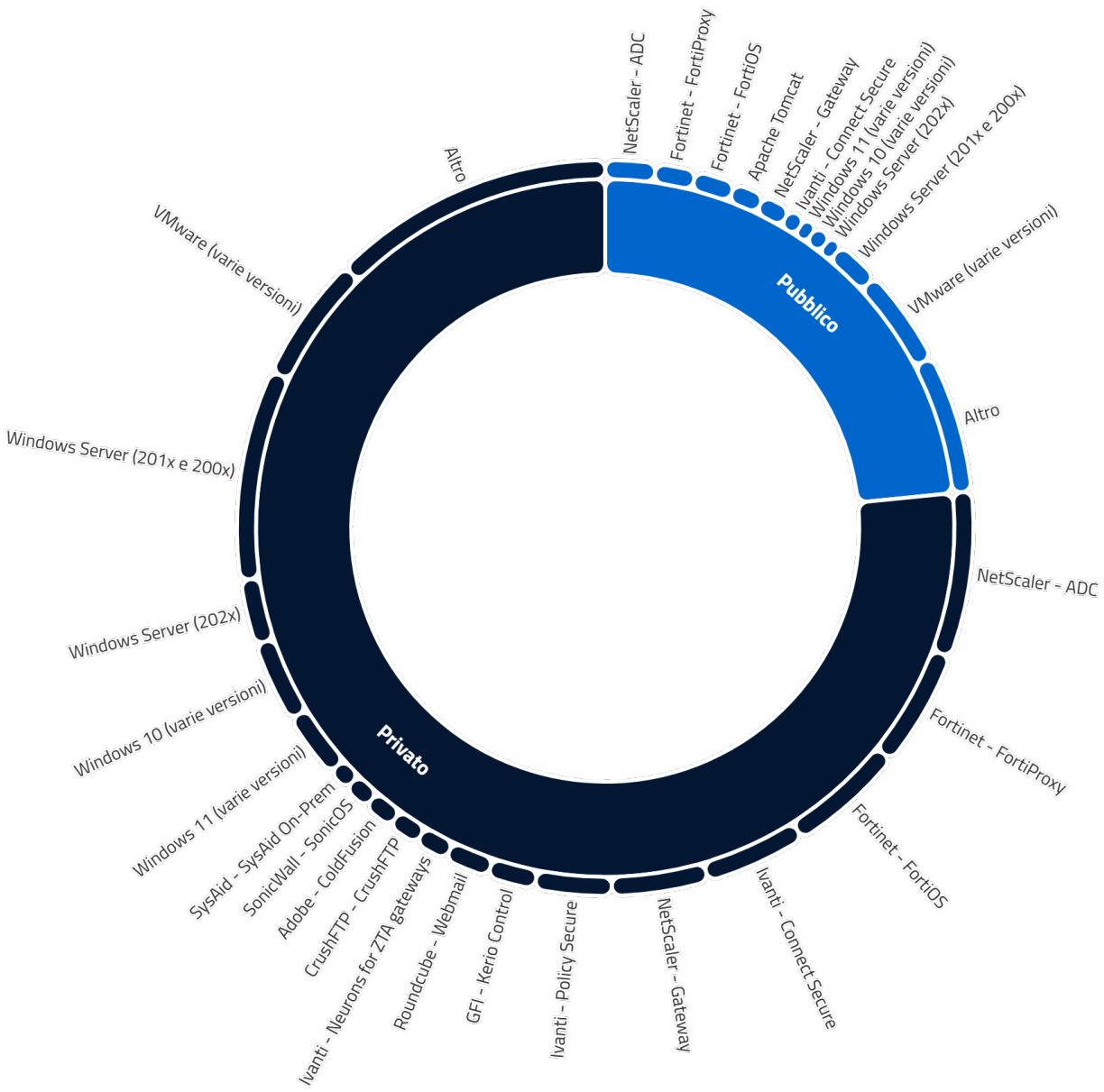

Figura 18 - *distribuzione delle segnalazioni per tipologia di soggetto e prodotto*

Gennaio

- **Qlik Sense** (CVE-2024-55580, CVE-2024-55579): tali vulnerabilità qualora sfruttate, potrebbero consentire a un utente malintenzionato l'esecuzione da remoto di codice malevolo o di eseguibili arbitrari presenti all'interno dei sistemi affetti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Ivanti Connect Secure** (CVE-2024-11634, CVE-2024-11633, CVE-2024-37401, CVE-2024-9844, CVE-2024-37377): tali vulnerabilità, sotto determinate condizioni consentirebbero a un utente malintenzionato di eludere le restrizioni di sicurezza, eseguire codice remoto malevolo ed effettuare Denial of Service sui sistemi affetti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Zabbix** (CVE-2024-42327): tale vulnerabilità – di tipo SQL Injection – permetterebbe a un eventuale attaccante, in possesso di un'utenza con accesso API valido, di elevare i propri privilegi ottenendo potenzialmente il controllo dei sistemi affetti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Servizi di remotizzazione desktop VNC senza autenticazione**: questa tipologia di servizio, configurato per la fruizione senza autenticazione, consente l'accesso diretto alla console dei sistemi esposti e permette, quindi, l'eventuale interazione da parte di malintenzionati, fino all'acquisizione del controllo completo.
- **Mitel** (CVE-2024-41713, CVE-2024-35286): tali vulnerabilità – rispettivamente di tipo SQL Injection, Authentication Bypass e Path Traversal – permetterebbero ad un eventuale attaccante, qualora sfruttate in combinazione, di bypassare i meccanismi di autenticazione, ottenendo così l'accesso arbitrario a file – anche sensibili – presenti sui dispositivi interessati e di eseguire potenzialmente su questi ultimi comandi e codice arbitrario. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Ivanti Cloud Service Application** (CVE-2024-11773, CVE-2024-11772, CVE-2024-11639): tali vulnerabilità, opportunamente sfruttate consentirebbero a un utente remoto non autenticato di ottenere privilegi amministrativi ed eseguire codice arbitrario sui sistemi affetti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Veeam Service Provider Console** (CVE-2024-42449, CVE-2024-42448): tali vulnerabilità - sotto condizioni specifiche - permetterebbero a un eventuale attaccante di eseguire codice arbitrario da remoto, di ottenere l'NTLM hash dell'account di servizio in uso al prodotto e di effettuare la cancellazione di file. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Cleo Harmony** (CVE-2024-50623): tali vulnerabilità permetterebbero a un eventuale attaccante remoto non autenticato di procedere al caricamento e alla successiva esecuzione di codice arbitrario sulle installazioni affette, anche con l'intento di creare una persistenza sui sistemi vittima tramite l'avvio di una reverse shell verso sistemi controllati dagli attaccanti. Ulteriori dettagli nell'alert sul sito del CSIRT Italia;
- **Pandora FMS** (CVE-2024-11320): in particolare, tale vulnerabilità consente l'esecuzione arbitraria di comandi remoti tramite command injection durante la fase di autenticazione LDAP.

Febbraio

- **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 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 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).

Marzo

- **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 "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 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;

Aprile

- **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 del 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 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).

Maggio

- **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 del 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 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;

Giugno

- **Citrix Netscaler ADC e Gateway** (CVE-2025-5777, CVE-2025-5349 e CVE-2025-6543): in particolare:
  - la CVE-2025-5777 (denominata *CitrixBleed 2*) – di tipo *Out-of-bounds Read* – consentirebbe a un eventuale attaccante non autenticato di accedere a dati potenzialmente sensibili presenti nella memoria dei sistemi affetti, sfruttando un'errata validazione dell'input (*Memory Overread*), laddove essi siano configurati come Gateway (ad esempio VPN virtual server, ICA Proxy, CVPN, RDP Proxy) oppure come AAA virtual server.
  - La CVE-2025-5349 – di tipo *Improper Access Control* – potrebbe, invece, consentire a un eventuale attaccante con accesso di rete all'interfacce di management dell'apparato (NSIP, Cluster Mangement o GSLB Site IP) di ottenere l'accesso non autorizzato a risorse protette e, potenzialmente, di accedere all'interfaccia di amministrazione ed effettuare movimenti laterali.
  - La CVE-2025-6543 – di tipo *Buffer Overflow* – infine, potrebbe consentire a un eventuale attaccante eludere il normale di esecuzione e di indurre il dispositivo in uno una condizione di Denial of Service.

  Ulteriori dettagli negli alert relativi alle CVE-2025-5777 e CVE-2025-5349 (alert) e alla CVE-2025-6543 (alert) sul sito dello 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 (*Information Disclosure*, che potrebbe consentire il bypass dei meccanismi di autenticazione in essere).
- **Roundcube Webmail** (CVE-2025-49113): tale vulnerabilità – di tipo *Deserialization of Untrusted Data* – potrebbe consentire a un utente malintenzionato autenticato di eseguire codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello 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).

- **Grafana** (CVE-2025-4123): tale vulnerabilità – di tipo Cross Site Scripting (XSS) – permetterebbe, laddove sia abilitato l'accesso anonimo e non sia configurata la direttiva "connect-src" all'interno della Content Security Policy del prodotto, a un utente malintenzionato il reindirizzamento degli utenti verso siti esterni e l'esecuzione di codice JavaScript malevolo compromettendo, potenzialmente, la relativa utenza della vittima. Inoltre, qualora sia installato il plugin "Image Renderer", tale vulnerabilità permetterebbe di ottenere una "Full-Read SSRF" sulle installazioni affette e di estrarre potenzialmente informazioni sensibili dall'ambiente delle installazioni affette. Ulteriori dettagli nell'alert sul sito dello 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.
- **Veeam Backup & Replication** (CVE-2025-23121): tale vulnerabilità - di tipo *Code Injection* - consentirebbe, laddove il prodotto in parola sia associato a un dominio (*domain-joined*), a un attaccante autenticato di eseguire codice arbitrario da remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **PostgreSQL pgAdmin** (CVE-2025-2945): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante autenticato di eseguire codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello 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).
- **BeyondTrust Remote Support (RS) e Privileged Remote Access (PRA)** (CVE-2025-5309): tale vulnerabilità – di tipo *Server-Side Template Injection* – potrebbe permettere a un eventuale attaccante di eseguire codice arbitrario da remoto sui sistemi affetti sfruttando un'errata sanitizzazione dell'input da parte del template engine; laddove il prodotto in uso sia BeyondTrust RS, non risulta necessario essere in possesso di credenziali valide ai fini dello sfruttamento della vulnerabilità. Ulteriori dettagli nell'alert sul sito dello 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*).
- **Mattermost** (CVE-2025-4981): tale vulnerabilità – di tipo *Path Traversal* – consentirebbe a un utente autenticato di scrivere file in posizioni arbitrarie del file system – oltre a permettere potenzialmente l'esecuzione di codice arbitrario da remoto – compromettendo così i sistemi affetti dalla vulnerabilità. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Cisco Identity Services Engine (ISE) e ISE Passive Identity Connector (ISE-PIC)** (CVE-2025-20282, CVE-2025-20281): tali vulnerabilità – rispettivamente di tipo *Code Injection* e *Improper Privilege Management* – consentirebbero a un eventuale attaccante di inviare una richiesta API opportunamente predisposta - ottenendo così l'accesso al dispositivo vulnerabile con privilegi massimi (CVE-2025-20281) - e il caricamento e la successiva esecuzione da remoto di file arbitrari da parte di un utente non autenticato (CVE-2025-20282). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

1° semestre 2025