Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

Servizio Operazioni
e gestione delle crisi cyber

gennaio 2025

TLP:CLEAR

INTRODUZIONE

Il presente documento riporta su base mensile alcuni numeri e indicatori derivanti dalle attività operative dell'Agenzia per la Cybersicurezza Nazionale, utili per caratterizzare lo stato della minaccia cyber in Italia. In particolare, il CSIRT Italia, articolazione tecnico-operativa dell'Agenzia, è hub nazionale delle notifiche obbligatorie e volontarie di incidenti previste per legge (Perimetro di Sicurezza Nazionale Cibernetica, Legge 28 giugno 2024, n. 90, Direttiva NIS) e riceve altresì informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali ed internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni dotano l'Agenzia di un ampio cono di visibilità sullo stato della minaccia cyber a danno del sistema Paese e forniscono, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali. Tutte le informazioni vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di triage le analizzano e classificano come eventi cyber; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento, come:

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

Per le definizioni si rimanda al Glossario del CSIRT Italia.

Sommario

pag.

Indice delle figure

pag.

1 EXECUTIVE SUMMARY

- A gennaio 2025 si è registrata una **diminuzione** del numero di **eventi** mentre il numero di **incidenti** è rimasto sostanzialmente nella **media** del semestre.
- I settori con il maggior numero di vittime registrate sono stati: **Pubblica amministrazione centrale**, **Telecomunicazioni** e **Tecnologico**. L'aumento degli eventi nel settore della **Pubblica Amministrazione Centrale** è riconducibile agli attacchi DDoS.
- Nel mese di gennaio, le attività di hacktivism in Italia hanno registrato una continuità rispetto ai mesi precedenti, con **attacchi DDoS** rivendicati principalmente da gruppi **filorussi**. In questo contesto, si segnala, quale elemento di novità, l'azione diretta anche contro alcuni **siti web di strutture sanitarie**, motivata – secondo le rivendicazioni – dal sostegno militare fornito dall'Italia all'Ucraina. L'episodio si distingue rispetto alle tendenze finora osservate, in quanto le campagne di attacco di matrice hacktivista hanno tradizionalmente colpito settori istituzionali, finanziari e le infrastrutture, mentre le strutture sanitarie, pur non estranee alle minacce cyber, risultano meno frequentemente oggetto di azioni motivate da finalità ideologiche. Le operazioni hanno subito un'intensificazione il 10 gennaio, in concomitanza con la visita del **Presidente ucraino Zelensky** a Roma. Gli impatti sono rimasti contenuti, coerentemente con la strategia già adottata da questi gruppi, basata sul colpire siti secondari, spesso privi di protezioni adeguate, con l'obiettivo principale di amplificare la portata mediatica degli attacchi.
- Nel medesimo periodo, tra le attività riconducibili all'hacktivism si segnala altresì il **defacement** di diversi siti web rivendicato dal gruppo **DXPloit**. Le azioni hanno avuto il solo obiettivo di veicolare messaggi a supporto dell'Islam ed hanno avuto impatti limitati, avendo preso di mira principalmente siti web di piccole realtà aziendali, con livelli di protezione limitati.
- i gruppi più attivi per numero di rivendicazioni **ransomware** sono stati **Everest** e **Akira**.
- I **vettori di attacco** maggiormente rilevati a gennaio 2025 sono le campagne malevole veicolate tramite e-mail, lo sfruttamento di vulnerabilità note e l'utilizzo di credenziali valide precedentemente compromesse.
- Nel medesimo periodo, si è registrato un **aumento** dei casi di **esfiltrazione dei dati**, con la compromissione di informazioni appartenenti a organizzazioni operanti in ambiti differenti. In alcune circostanze, i dati sottratti sono stati successivamente diffusi su internet,

aumentando il potenziale impatto per le entità coinvolte in termini di sicurezza e reputazione.
- Contestualmente, è stato rilevato un **aumento** dei casi di accesso con **credenziali valide**, circostanza che lascia ipotizzare l'impiego di dati compromessi in precedenti violazioni o l'utilizzo di tecniche di **credential stuffing**.
- Il numero delle nuove CVE pubblicate è in sensibile **aumento** rispetto a dicembre.

I NUMERI DI GENNAIO 2025

- **205** eventi cyber, in **diminuzione** (**–31**);
- **201** vittime, in **diminuzione** (**–73**);
- **82** vittime della constituency[1] , in **diminuzione** (**–41**);
- **47** incidenti con impatto confermato, in **diminuzione** (**–32**);
- **15.000** asset potenzialmente vulnerabili, in **aumento** (**+14.315**);
- **47** alert sul sito web del CSIRT Italia, in **aumento** (**+6**);
- **4.417** nuove CVE, in **aumento** (**+973**).

Per le definizioni si rimanda al Glossario del CSIRT Italia.

PRODOTTI VULNERABILI

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

- **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).

Maggiori dettagli nelle sezioni 3 e 5.

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

2 EVENTI ED INCIDENTI

A gennaio 2025 sono stati individuati **205** eventi cyber, in **diminuzione** del 13% rispetto al mese precedente. Questi ultimi hanno avuto un **impatto su 150 soggetti nazionali**: 82 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 205 eventi cyber, **47 sono stati classificati quali incidenti**, in **diminuzione** del 41% rispetto a dicembre.

La Figura 1 mostra l'andamento di eventi e incidenti fino al mese in esame, corredato da una previsione, basata sull'analisi dei dati precedenti[2], riferita ai successivi 3 mesi.

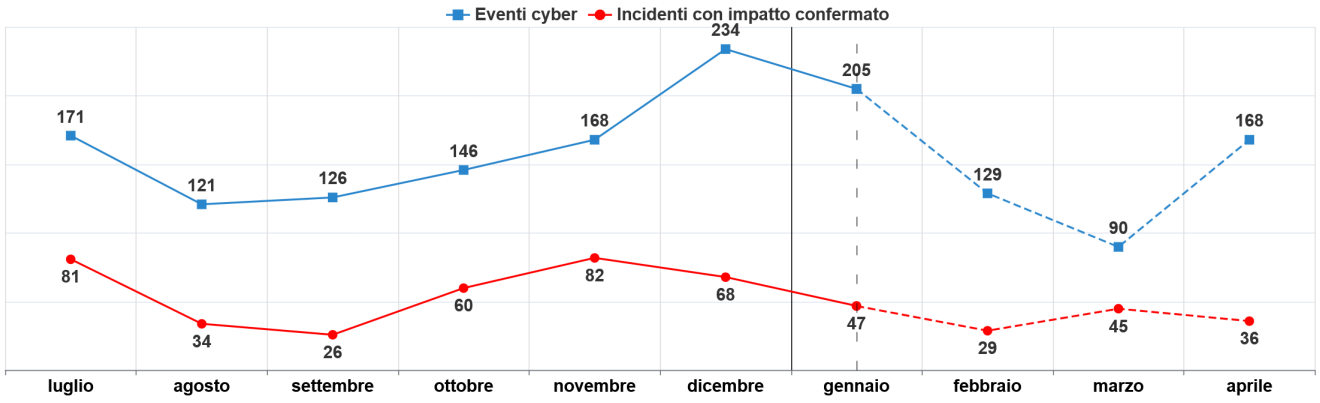

Figura 1 - andamento attività reattive e analisi previsionale

[2]La previsione dà un'idea generale degli andamenti futuri utilizzando un modello ARIMA (AutoRegressive Integrated Moving Average). È importante sottolineare che la previsione non può essere accurata in quanto il manifestarsi degli eventi dipende da molti fattori, tra i quali quelli di natura geopolitica, la scoperta di nuove vulnerabilità, la capacità degli attaccanti e così via.

2.1 Settori impattati

In Figura 2 si riporta il numero di vittime di eventi per settore impattato[3]. Si evidenza altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico).

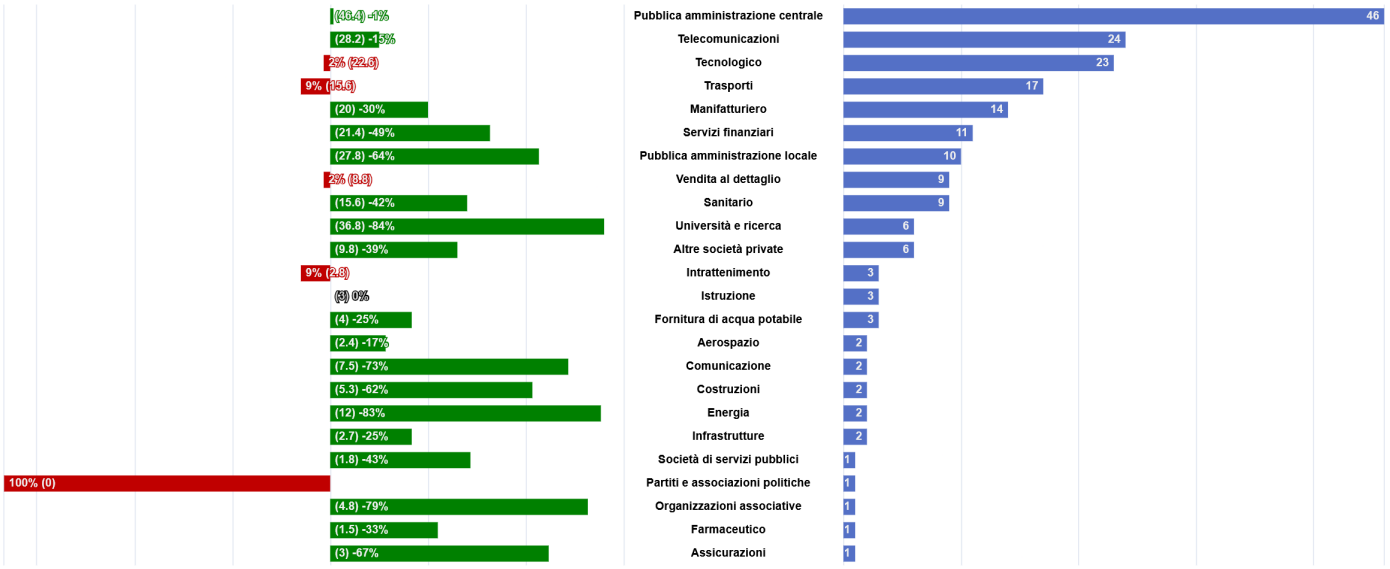

Figura 2 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente

2.2 Tipologia di minacce negli eventi

In Figura 3 si riporta il numero di minacce rilevate negli eventi[4] e la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico).

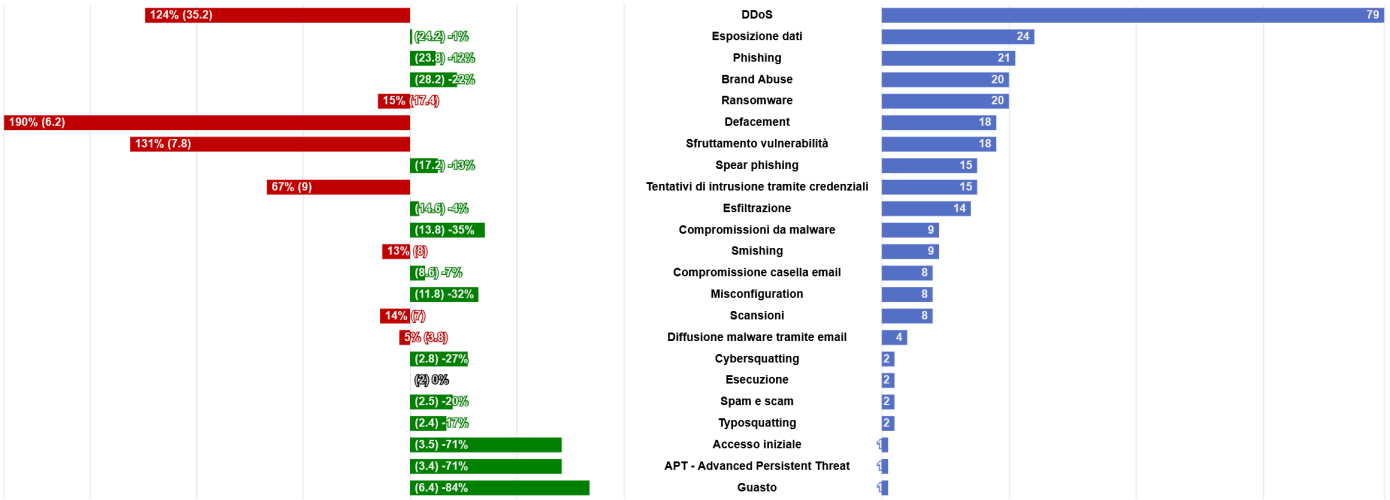

Figura 3 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente

[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.

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

2.3 Focus constituency

I 205 eventi cyber hanno interessato **82** soggetti appartenenti alla constituency, distribuiti dal punto di vista geografico come riportato in Figura 4.

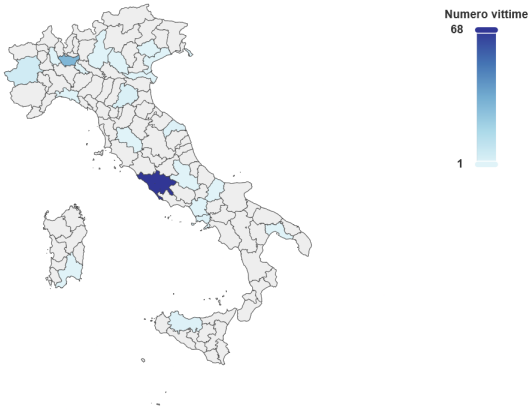

Figura 4 - distribuzione geografica delle vittime appartenenti alla constituency

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.

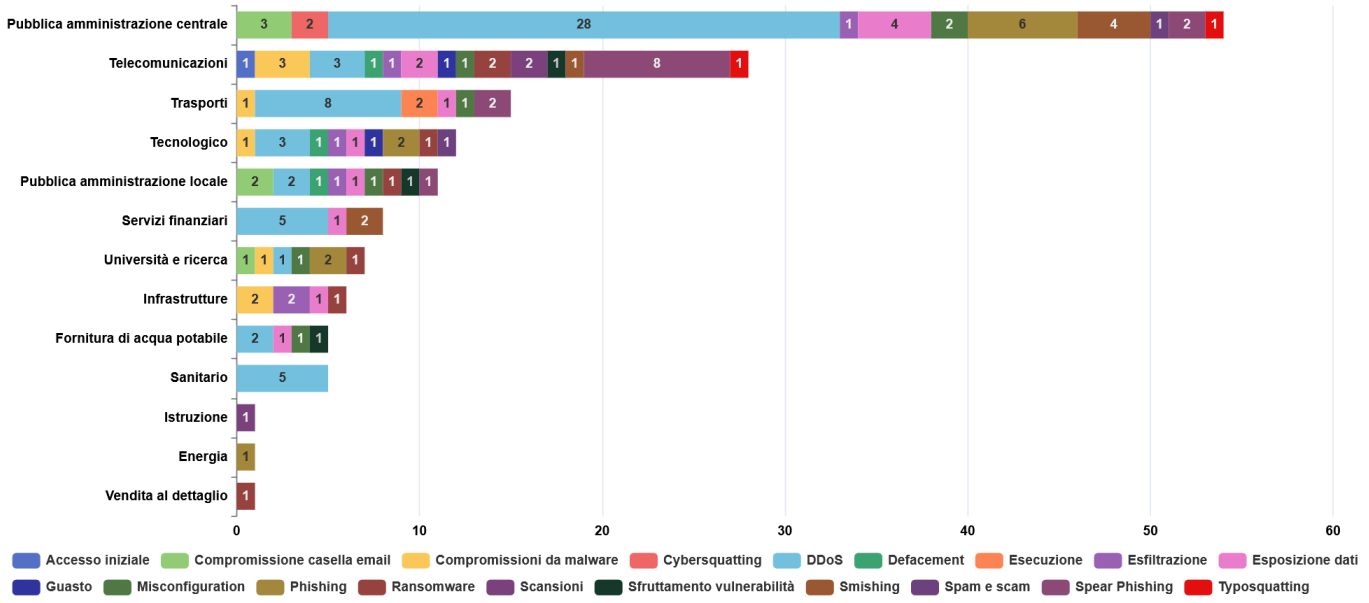

Figura 5 - tipologia di minacce con impatto sui settori della constituency

3 VULNERABILITÀ

A gennaio 2025 sono state pubblicate[5] **4.417** nuove CVE, in **aumento** (**+973**) rispetto a dicembre. Di queste, **173** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–28**), e per **8** CVE è stato rilevato lo sfruttamento attivo, in **aumento** (**+2**) rispetto a dicembre.

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 **47**. Oltre al consueto aggiornamento mensile di Microsoft (link all'alert sul sito web), che ha risolto un totale di 159 nuove vulnerabilità (8 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **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;
- **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;
- **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**: rilasciati 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

[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/`.

sistemico **78,20/100**). Link all'alert del 09/01/2025;

- **Howyar**: ricercatori di sicurezza di ESET hanno recentemente rilevato la vulnerabilità CVE-2024-7344 relativa al bootloader UEFI "Howyar Reloader" (versione 32-bit e 64-bit), distribuito come parte di SysReturn di Howyar e di diverse altre suite di software, sviluppate da altri produttori, per il recupero del sistema in tempo reale (stima di impatto sistemico **75/100**). Link all'alert del 21/01/2025.

All'indirizzo https://www.acn.gov.it/portale/csirt-italia/alert-e-bollettini è possibile accedere a tutti gli altri alert pubblicati.

3.2 Distribuzione delle vulnerabilità sui vendor

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

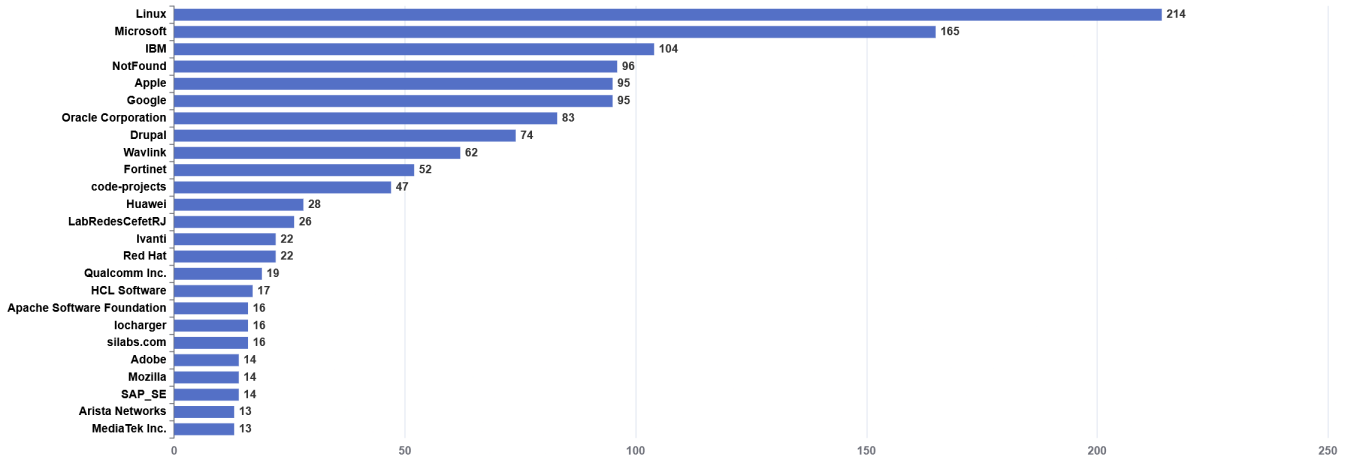

Figura 6 - top 25 produttori affetti da vulnerabilità nel mese

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

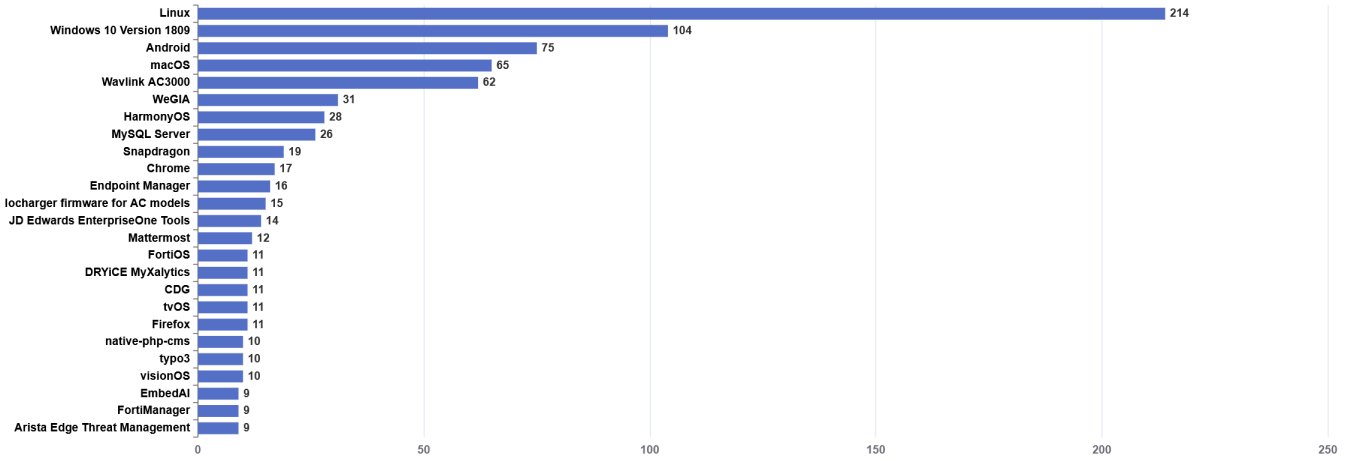

Figura 7 - top 25 prodotti affetti da vulnerabilità nel mese

3.3 CWE nel mese

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

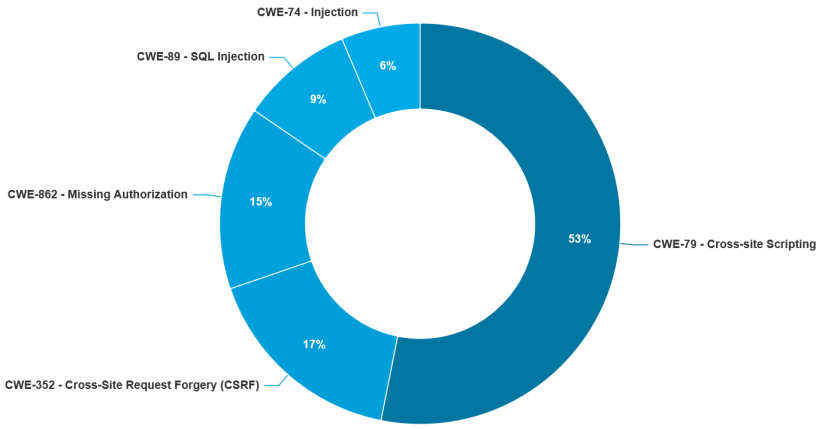

Figura 8 - top 5 CWE nel mese

3.4 Vulnerabilità con maggior probabilità di sfruttamento

Di seguito il dettaglio delle 3 vulnerabilità che potrebbero subire il maggior incremento nel trend di exploitation, ottenuto monitorando l'Exploit Prediction Scoring System (EPSS)[6] fornito dal FIRST nel mese in esame.

Vendor	**Ivanti**
Prodotti e versioni vulnerabili	**Ivanti Connect Secure tutte le versioni precedenti la 22.7R2.5** **Policy Secure tutte le versioni precedenti la 22.7R1.2** **ZTA Gateways tutte le versioni precedenti la 22.7R2.3**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice malevolo**
Data di rilascio CVE	**08/01/2025 modificata il 28/01/2025**
CVSS score 3.x	**9.0 CRITICAL**
EPSS max score	**0.15**

Tabella 1 - CVE-2025-0282

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

Vendor	**Mitel**
Prodotti e versioni vulnerabili	**NuPoint Unified Messaging (NPM) componente di Mitel MiCollab versioni fino alla 9.8 SP1 FP2 (9.8.1.201)**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di modificare files utenti e configurazioni del sistema**
Data di rilascio CVE	**21/10/2024 modificata il 08/01/2025**
CVSS score 3.x	**9.8 CRITICAL**
EPSS max score	**0.95**

Tabella 2 - CVE-2024-41713

Vendor	**Aviatrix**
Prodotti e versioni vulnerabili	**NAviatrix Controller before 7.1.4191 and 7.2.x before 7.2.4996 FortiManager Cloud 6.4.x., tutte le versioni**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante di eseguire comandi e codice malevolo**
Data di rilascio CVE	**07/01/2025 modificata il 23/01/2025**
CVSS score 3.x	**9.8 CRITICAL**
EPSS max score	**0.88**

Tabella 3 - CVE-2024-50603

4 MINACCIA

In questa sezione si riportano, per quanto riguarda il malware, il numero degli Indicatori di Compromissione (IoC)[7] condivisi dal CSIRT Italia tramite piattaforma MISP (Malware Information Sharing Platform)[8], per il ransomware e il DDoS un'analisi sulle rivendicazioni in Italia ed UE.

4.1 Indicatori di Compromissione (IoC) per famiglia di malware

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

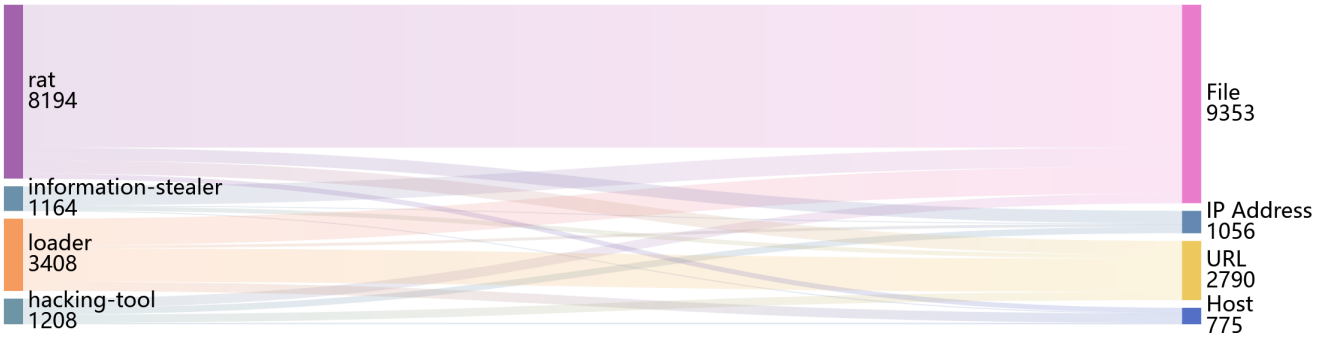

Figura 9 - Numero di IoC condivisi dal CSIRT Italia suddivisi per famiglie di malware

[7] Indicatore di Compromissione, è un marcatore digitale che indica la possibile presenza di un'attività malevola o un'intrusione nel sistema informatico. Gli IoC sono prove che gli analisti di sicurezza informatica utilizzano per identificare, rilevare e rispondere a una compromissione.

[8] MISP è una soluzione software open source per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di sicurezza informatica e minacce cyber.

4.2 Rivendicazioni ransomware

Il monitoraggio di fonti aperte nel mese di gennaio 2025 ha permesso di individuare **12** rivendicazioni di attacchi ransomware a danno di soggetti italiani. I gruppi più attivi sono stati **Everest** e **Akira**. Il grafico in Figura 10 mostra l'andamento delle rivendicazioni nell'anno in corso.

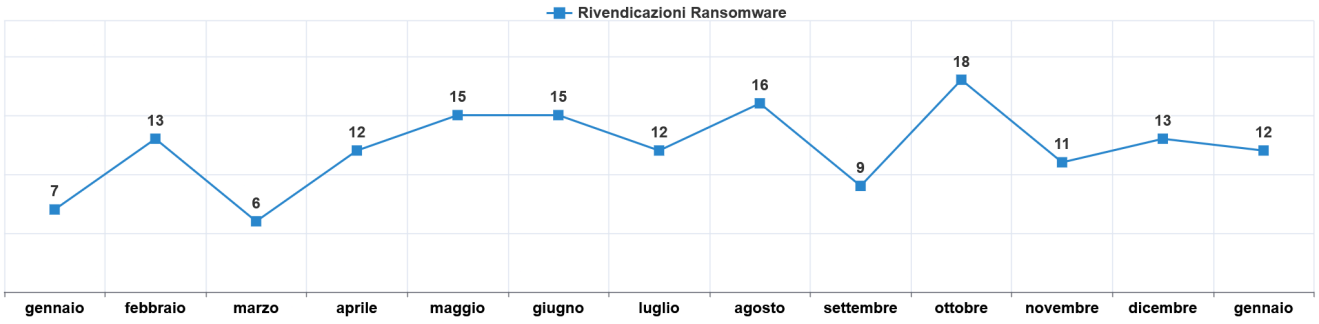

Figura 10 - andamento delle rivendicazioni Ransomware

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

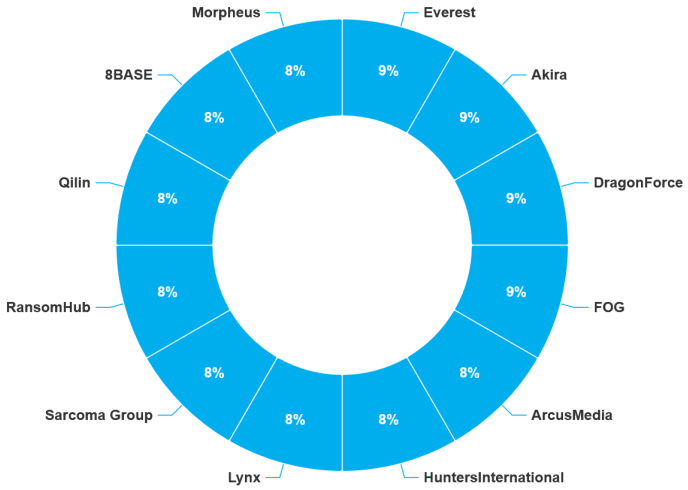

Figura 11 - distribuzione percentuale dei gruppi autori delle rivendicazioni

4.3 Rivendicazioni DDoS

A gennaio 2025 sono state individuate[9] **49** rivendicazioni di attacchi DDoS in danno di soggetti italiani. I gruppi più attivi su scala globale sono stati **nnm057_16** e **alixsecenglish**. Il grafico in Figura 12 mostra l'andamento delle rivendicazioni DDoS dell'anno in corso.

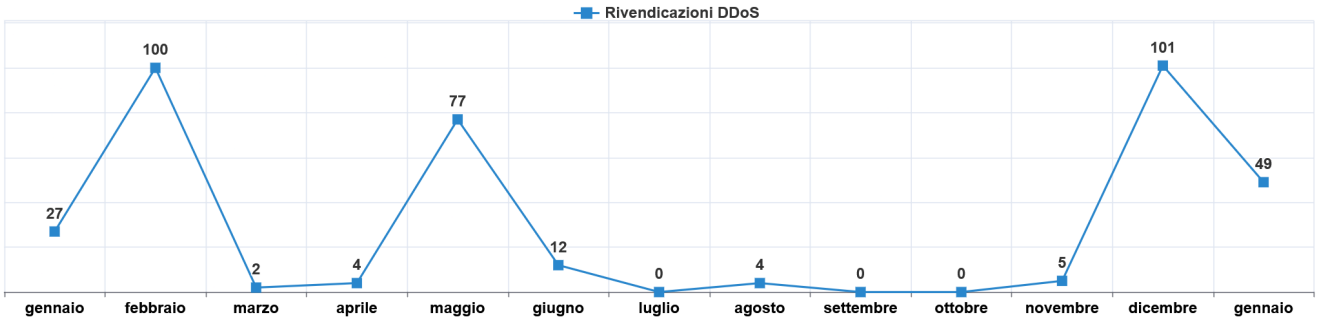

Figura 12 - andamento delle rivendicazioni DDoS

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

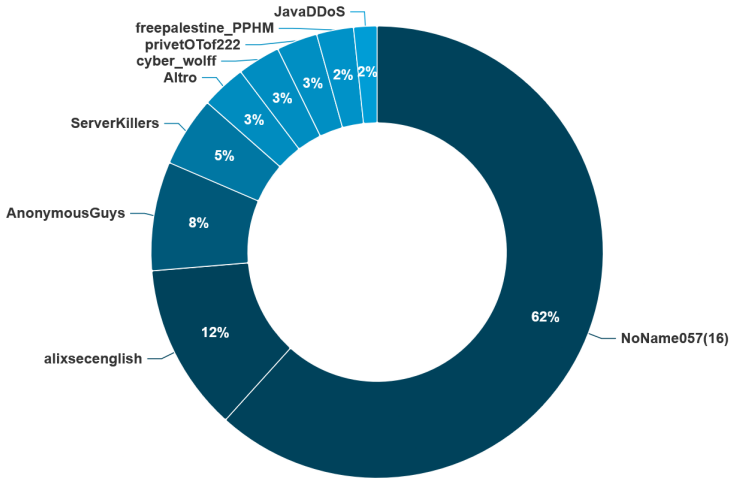

Figura 13 - distribuzione percentuale dei gruppi autori delle rivendicazioni

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

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[10], condotte al fine di individuare e segnalare tempestivamente ai soggetti della constituency l'esposizione a specifiche minacce, rischi, vulnerabilità e criticità, che possono essere sfruttati, o che sono già in corso di sfruttamento, da parte degli attaccanti.

5.1 Comunicazioni dirette

A gennaio 2025 sono state diramate un totale di **490** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **685** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **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 dello 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 e effettuare Denial of Service sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello 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 dello 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.

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

- **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 dello 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 dello 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 dello 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 dello 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.

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

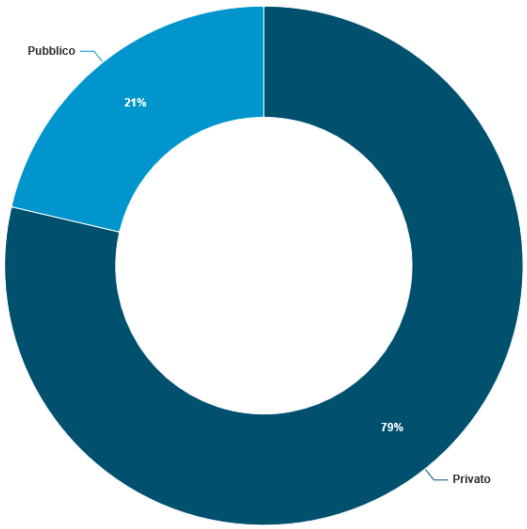

Figura 14 - Distribuzione delle segnalazioni per tipologia di soggetto