



Agenzia per la  
Cybersicurezza Nazionale



# OPERATIONAL SUMMARY

**SETTEMBRE 2026**

DATI ED INDICATORI DELLA MINACCIA CYBER IN ITALIA

Servizio Operazioni  
e gestione delle crisi cyber

**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 (tra cui il Perimetro di Sicurezza Nazionale Cibernetica, la Legge 28 giugno 2024, n. 90 e il D.Lgs. 4 settembre 2024, n. 138 che recepisce la c.d. Direttiva NIS2) 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 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 di 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.



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.

Documento rilasciato con licenza **Creative Commons Attribuzione 4.0 Internazionale (CC BY 4.0)**.  
Testo completo della licenza disponibile su: <https://creativecommons.org/licenses/by/4.0/deed.it>



# Sommario

**pag.**

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>1. EXECUTIVE SUMMARY</b>                                       | <b>5</b>  |
| <b>2. EVENTI ED INCIDENTI</b>                                     | <b>10</b> |
| 2.1. Settori impattati                                            | 11        |
| 2.2. Tipologia di minacce negli eventi                            | 12        |
| 2.3. Distribuzione delle minacce per settore                      | 13        |
| 2.4. Distribuzione geografica delle vittime                       | 14        |
| <b>3. VULNERABILITÀ</b>                                           | <b>15</b> |
| 3.1. Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia | 15        |
| 3.2. Distribuzione delle vulnerabilità sui vendor                 | 16        |
| 3.3. CWE nel mese                                                 | 17        |
| 3.4. Vulnerabilità con maggior probabilità di sfruttamento        | 18        |
| <b>4. MINACCIA</b>                                                | <b>20</b> |
| 4.1. Ransomware: distribuzione delle vittime                      | 20        |
| 4.2. Rivendicazioni ransomware                                    | 21        |
| 4.3. Rivendicazioni DDoS                                          | 22        |
| 4.4. Indicatori di Compromissione (IoC) per famiglia di malware   | 23        |
| <b>5. MONITORAGGIO</b>                                            | <b>24</b> |
| 5.1. Comunicazioni dirette                                        | 24        |
| <b>6. ASPETTI DI INTERESSE DELLA MINACCIA CYBER GLOBALE</b>       | <b>30</b> |
| 6.1. Vulnerabilità e modalità operative                           | 30        |
| 6.2. Intelligenza artificiale                                     | 32        |
| 6.3. Contesto geopolitico                                         | 33        |

# Indice delle figure

**pag.**

|                                                                                                                                        |    |
|----------------------------------------------------------------------------------------------------------------------------------------|----|
| Figura 1 - indicatori delle attività operative a settembre 2026 e nei sei mesi precedenti                                              | 8  |
| Figura 2 - andamento attività reattive e analisi previsionale                                                                          | 10 |
| Figura 3 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente (top 15) | 11 |
| Figura 4 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente (top 15)    | 12 |
| Figura 5 - numero di vittime per settore e tipologia di minacce                                                                        | 13 |
| Figura 6 - distribuzione delle vittime degli eventi cyber                                                                              | 14 |
| Figura 7 - top 25 produttori affetti da vulnerabilità nel mese                                                                         | 16 |
| Figura 8 - top 25 prodotti affetti da vulnerabilità nel mese                                                                           | 17 |
| Figura 9 - top 5 CWE nel mese                                                                                                          | 17 |
| Figura 10 - distribuzione delle vittime di ransomware in base alla loro criticità                                                      | 20 |
| Figura 11 - andamento delle rivendicazioni ransomware per l'Italia                                                                     | 21 |
| Figura 12 - distribuzione percentuale dei gruppi autori delle rivendicazioni                                                           | 21 |
| Figura 13 - andamento delle rivendicazioni DDoS riferite all'Italia                                                                    | 22 |
| Figura 14 - distribuzione percentuale dei gruppi autori delle rivendicazioni                                                           | 22 |
| Figura 15 - numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware                                                | 23 |
| Figura 16 - distribuzione delle segnalazioni per tipologia di soggetto                                                                 | 29 |

## 1

## EXECUTIVE SUMMARY



La direttiva (UE) 2022/2555 (NIS2), recepita nell'ordinamento nazionale con il decreto legislativo 4 settembre 2024, n. 138, ha rafforzato il quadro normativo in materia di cybersicurezza, introducendo, tra l'altro, specifici **obblighi di notifica di incidenti per numerosi soggetti nazionali**. A partire da gennaio u.s., tali obblighi sono pienamente operativi; ciò ha favorito un incremento significativo del numero di eventi e incidenti cyber visibili ad ACN rispetto ai medesimi periodi di riferimento degli scorsi anni.

Alla data odierna, appare utile comunque evidenziare che all'ampliamento della visibilità garantita dal nuovo flusso informativo non corrisponde un aumento degli impatti causati dagli incidenti, i quali sono allineati alla media dei mesi precedenti.

#### ■ Eventi e incidenti

Nel mese di settembre 2026 sono stati registrati **485 eventi**, in **aumento** del 57% rispetto ai **309** di agosto. Anche gli **incidenti** sono risultati in **aumento**: **235** rispetto ai **196** del mese precedente.

L'aumento degli eventi è riconducibile principalmente agli incrementi di attacchi **DDoS** di natura hacktivista che hanno interessato perlopiù siti web di pubbliche amministrazioni locali e imprese – senza impatti significativi – e allo **sfruttamento di vulnerabilità**, legato in larga parte a campagne di *defacement* che hanno impiegato in modo opportunistico vulnerabilità presenti in plugin e altri componenti dei CMS<sup>1</sup>. Per tale motivo, il **defacement** è risultato la minaccia con il maggior incremento percentuale rispetto alla media.

#### Contromisure – Defacement

Le **principali** misure per evitare questo tipo di incidente sono:

- aggiornamento tempestivo di CMS, plugin ed estensioni;
- monitoraggio delle modifiche non autorizzate a file e configurazioni dei siti, inclusi i reindirizzamenti;
- isolamento tra i siti ospitati sulla stessa infrastruttura, in modo da evitare compromissioni di molteplici siti web contemporaneamente;
- applicare il principio del privilegio minimo per gli account di servizio;
- mantenere copie di backup in ambiente separato.

Dal punto di vista degli impatti operativi, il **ransomware** rimane la minaccia più rilevante specie in considerazione degli attacchi avvenuti in danno di **due strutture sanitarie**.

Di rilievo, altresì, l'individuazione, attraverso il monitoraggio delle piattaforme di scambio illecito di dati

<sup>1</sup> Content Management System (CMS) sono piattaforme software per la creazione e la gestione dei contenuti dei siti web. Il CSIRT Italia ha segnalato tramite bollettino lo sfruttamento della vulnerabilità CVE-2026-48907 nel componente Joomla Content Editor.

effettuato dal CSIRT Italia, di una **raccolta di indirizzi di posta elettronica con le relative credenziali** riferibili in maggioranza a organizzazioni del settore Sanitario.

Complessivamente nel corso del mese di settembre 2026, le minacce più frequenti negli eventi sono state **DDoS, Compromissione di caselle email e phishing**.

#### ■ Settori interessati

I settori con il maggior numero di vittime di eventi cyber sono stati **Tecnologico, Sanitario, Manifatturiero**. Nel settore Tecnologico sono prevalsi lo sfruttamento di vulnerabilità e i guasti; il settore Sanitario è stato interessato principalmente dall'esposizione di dati, mentre nel settore Manifatturiero le attività di defacement.

#### ■ Ransomware

Nel mese di settembre, gli attacchi ransomware hanno interessato prevalentemente i settori **Tecnologico, Commercio all'ingrosso e al dettaglio e Manifatturiero**. Le modalità di accesso iniziale maggiormente riscontrate in tali incidenti sono state lo **sfruttamento di vulnerabilità, l'utilizzo di credenziali valide precedentemente compromesse e la compromissione di servizi utilizzati per l'accesso remoto**. Gli impatti accertati hanno riguardato la cifratura dei dati e l'indisponibilità di applicazioni e servizi. L'incidente con conseguenze più rilevanti ha colpito un **polo ospedaliero** articolato su due sedi. La compromissione dell'infrastruttura virtualizzata e dei sistemi di archiviazione ha determinato la chiusura temporanea di una struttura e limitazioni nella gestione dei pazienti presso l'altra. Le analisi hanno indicato il possibile sfruttamento di vulnerabilità in un apparato perimetrale quale vettore d'ingresso.

#### Contromisure – Ransomware

Le **principali** misure per evitare questo tipo di incidente sono:

- aggiornamento tempestivo dei software, con priorità agli apparati perimetrali, per sanare vulnerabilità note;
- utilizzo di politiche di autenticazione a più fattori e adozione del principio del privilegio minimo per gli account;
- gestione separata e protetta degli ambienti di virtualizzazione e dei sistemi di archiviazione, mediante credenziali amministrative dedicate;
- segmentazione della rete e soluzioni EDR/XDR;
- mantenimento copie di backup separate, non alterabili e verificate periodicamente con prove di ripristino.

Per approfondimenti, è disponibile sul sito web ACN il documento: "Caratteristiche, preparazione e risposta agli attacchi ransomware".

#### ■ Attacchi DDoS

Nel mese di settembre 2026, è ripresa l'attività DDoS di matrice hacktivista dopo l'inattività osservata nei mesi di giugno, luglio e agosto. Gli attacchi DDoS hanno riguardato principalmente la **Pubblica Amministrazione locale**. Solo nell'8,3% dei casi sono stati accertati impatti, comunque di entità limitata. Gli attacchi sono stati rivendicati da un gruppo filorusso che, nelle proprie comunicazioni, ha dichiarato di aver agito in risposta al sostegno militare fornito dall'Italia all'Ucraina, richiamando notizie relative a un nuovo pacchetto di aiuti.

#### Contromisure – DDoS

- acquisire servizi e soluzioni anti-DDoS volumetriche, in cloud, on premise o ibride, fornite da ISP o altri operatori specializzati;
- predisporre un piano di risposta e misure di mitigazione da attivare in caso di attacco, tra cui restrizioni geografiche e limitazioni selettive dei servizi esposti;
- prevedere la ridondanza della connettività e, ove opportuno, il ricorso a ISP differenti;
- utilizzare dispositivi di rete con funzionalità anti-DDoS e di Deep Packet Inspection (DPI), configurati per rilevare e filtrare il traffico anomalo.

Per approfondimenti, è disponibile sul sito web ACN il documento: "Preparazione e risposta agli attacchi Denial of Service".

## ▪ Vettori di attacco

Nel mese di settembre 2026 lo **sfruttamento di vulnerabilità** è risultato il principale vettore di accesso iniziale, in relazione alla campagna di defacement sopra descritta; seguono la **posta elettronica**, impiegata come canale per veicolare campagne di phishing e spear phishing, e lo **sfruttamento di credenziali valide già compromesse**. Permane, con minore incidenza, l'abuso di servizi remoti esposti.

## ▪ Vulnerabilità

A settembre 2026, il *Common Vulnerabilities and Exposures (CVE) Program*<sup>2</sup> ha pubblicato **15.074** nuovi record relativi a vulnerabilità di cybersicurezza, in **aumento (+2.355)** rispetto ad agosto. Di questi, **341** presentano almeno un *Proof of Concept (PoC)*, in **aumento (+53)**, e per **25** CVE è stato rilevato lo sfruttamento attivo, in **aumento (+12)** rispetto ad agosto. Tra queste, ACN ha rivolto particolare attenzione, con specifiche campagne di allertamento, ad alcune vulnerabilità relative a prodotti ampiamente utilizzati per la gestione dei server, della posta elettronica e dell'accesso remoto sicuro alle risorse aziendali.

In questo ambito, emerge come nel 2026 vi sia una crescita senza precedenti delle vulnerabilità censite di mese in mese, con oltre **77.000 CVE registrate nei primi nove mesi dell'anno**. Tale accelerazione si manifesta in concomitanza con il crescente utilizzo di

**modelli AI di frontiera** che stanno riducendo i tempi necessari per l'analisi del codice, il vulnerability research e la generazione di Proof of Concept.

## ▪ Monitoraggio proattivo e allertamento

L'attività di monitoraggio della superficie esposta ha consentito di individuare a settembre 2026 **8.213 sistemi e servizi a rischio, in diminuzione** (-908) rispetto ad agosto. Tra le attività di monitoraggio del mese, si segnala l'individuazione di numerosi servizi esposti riconducibili a **F5 BIG-IP**, piattaforma per la gestione del traffico e la sicurezza delle applicazioni. Tali servizi sono risultati potenzialmente vulnerabili alla CVE-2026-94127, oggetto dell>alert AL08/260922/CSIRT-ITA.

I soggetti interessati sono stati allertati per consentire le necessarie verifiche e l'adozione delle misure di mitigazione.

L'analisi di dati provenienti da malware di tipo infostealer, altresì, ha consentito di identificare **253 account compromessi** afferenti a soggetti istituzionali, prontamente allertati.

Le **comunicazioni inviate complessivamente** dal CSIRT Italia per segnalare potenziali compromissioni o fattori di rischio ad amministrazioni ed imprese italiane, anche ai sensi dell'art. 2, comma 1, della Legge n. 90/2024 sono state in totale **10.839, in aumento** (+2.457) rispetto ad agosto.

<sup>2</sup>Il CVE Program è un'iniziativa internazionale finalizzata a identificare, definire e catalogare le vulnerabilità di cybersicurezza divulgate pubblicamente, associando a ciascuna un identificativo univoco.

# I NUMERI - SETTEMBRE 2026

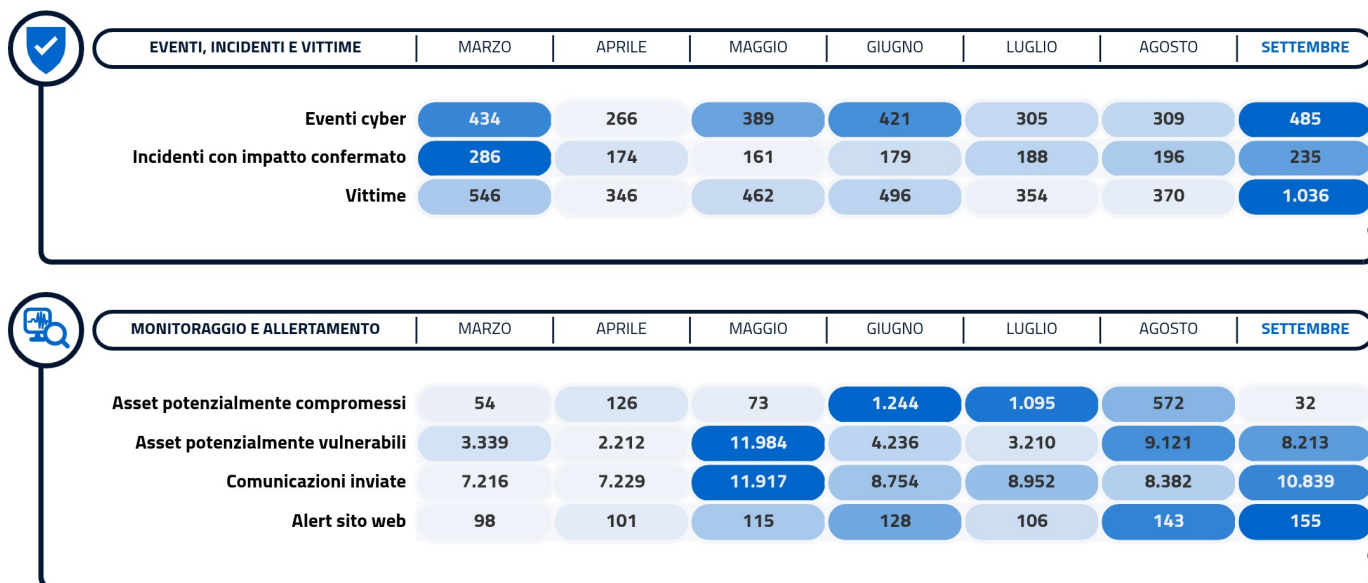


Figura 1 - indicatori delle attività operative a settembre 2026 e nei sei mesi precedenti

- **485** eventi cyber, in **aumento (+176)**;
- **1.036** vittime<sup>3</sup>, in **aumento (+666)**;
- **514** vittime della constituency<sup>4</sup>, in **aumento (+328)**;
- **235** incidenti con impatto confermato, in **aumento (+39)**;
- **32** asset potenzialmente compromessi, in **diminuzione (-540)**;
- **8.213** asset potenzialmente vulnerabili, in **diminuzione (-908)**;
- **155** alert sul sito web del CSIRT Italia, in **aumento (+12)**;
- **10.839** comunicazioni inviate complessivamente, in **aumento (+2.457)**;
- **15.074** nuove CVE, in **aumento (+2.355)**.

<sup>3</sup>Uno stesso soggetto è conteggiato più volte qualora sia stato coinvolto in eventi distinti.

<sup>4</sup>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 a riguardo.

# PRODOTTI VULNERABILI

Di seguito l'**elenco dei prodotti** che a settembre 2026 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.

- **Adobe** – Commerce, Commerce B2B e Magento Open Source (CVE-2026-75650) Link all'alert
- **BerriAI** – LiteLLM (CVE-2026-59822) Link all'alert
- **Check Point** – Log Server, Multi-Domain Log Server, Multi-Domain Security Management Server e Security Management Server (CVE-2026-91843) Link all'alert; Quantum Security Gateway (CVE-2026-85102) Link all'alert
- **Cisco** – Catalyst SD-WAN Manager (CVE-2026-76504) Link all'alert; prodotti vari (CVE-2026-20130, CVE-2026-20135, CVE-2026-20154, CVE-2026-20176, CVE-2026-20192, CVE-2026-20194, CVE-2026-20211, CVE-2026-20222, CVE-2026-20234, CVE-2026-20237, CVE-2026-20242, CVE-2026-20247, CVE-2026-20249, CVE-2026-20250, CVE-2026-20284, CVE-2026-20295, CVE-2026-20300, CVE-2026-20305, CVE-2026-20306, CVE-2026-20307, CVE-2026-20322, CVE-2026-20323, CVE-2026-20324, CVE-2026-20325, CVE-2026-20326, CVE-2026-20329, CVE-2026-20330, CVE-2026-20331, CVE-2026-20332, CVE-2026-20333, CVE-2026-20334, CVE-2026-20335, CVE-2026-20336, CVE-2026-20340, CVE-2026-20341, CVE-2026-20342, CVE-2026-20343, CVE-2026-20344, CVE-2026-20352, CVE-2026-20360, CVE-2026-20361, CVE-2026-76409, CVE-2026-76412, CVE-2026-76413, CVE-2026-76420, CVE-2026-76423, CVE-2026-76424, CVE-2026-76425, CVE-2026-76460) Link all'alert
- **Cleo** – Harmony (CVE-2026-84114, CVE-2026-84115) Link all'alert
- **ConnectWise** – ScreenConnect (CVE-2026-84869) Link all'alert
- **F5** – BIG-IP (CVE-2026-94127) Link all'alert
- **FlowiseAI** (CVE-2026-100605, CVE-2026-100606, CVE-2026-100607, CVE-2026-100608, CVE-2026-100609, CVE-2026-100610) Link all'alert
- **Gitea** (CVE-2026-60004) Link all'alert
- **GitLab** (CVE-2026-85706, CVE-2026-87719) Link all'alert
- **Jenkins** (CVE-2026-84645) Link all'alert
- **IFrog** – Artifactory (CVE-2026-42016, CVE-2026-42018) Link all'alert
- **Microsoft** – Exchange e SharePoint (CVE-2026-62911, CVE-2026-65660) Link all'alert; Windows DNS Server (CVE-2026-69730) Link all'alert
- **MikroTik** – RouterOS (CVE-2026-67276, CVE-2026-67277, CVE-2026-67281, CVE-2026-86060) Link all'alert
- **N-able** – N-central (CVE-2026-86207, CVE-2026-86218) Link all'alert
- **Palo Alto Networks** – PAN-OS Management Interface (CVE-2026-0310) Link all'alert
- **pgAdmin** (CVE-2026-86863, CVE-2026-86864) Link all'alert
- **SAP** – Extended Passport (EPP) (CVE-2026-44756) Link all'alert
- **ServiceNow** – AI Platform (CVE-2026-13016) Link all'alert
- **SonicWall** – SMA1000 (CVE-2026-83548, CVE-2026-83549) Link all'alert
- **Vercel** – Next.js (CVE-2026-94545) Link all'alert
- **WordPress** (CVE-2026-87902, CVE-2026-93485) Link all'alert
- **Zimbra Collaboration Suite** (CVE-2026-93643) Link all'alert
- **Zoho** – ManageEngine ADSelfService Plus (CVE-2026-74849, CVE-2026-75791) Link all'alert

Maggiori dettagli nelle sezioni 3 e 5.

## 2

## EVENTI ED INCIDENTI

A settembre 2026 sono stati individuati **485** eventi cyber, in **aumento** del 57% rispetto ad agosto. Questi ultimi hanno **interessato, in diversi casi più volte, 827 soggetti nazionali distinti** (di cui 514 appartenenti alla constituency, mentre i restanti hanno riguardato cittadini e società private operanti in settori non critici). Dei 485 eventi cyber, **235 sono stati classificati quali incidenti**, anch'essi in **aumento** rispetto ai 196 di agosto.

La Figura 2 mostra l'andamento di eventi e incidenti fino al mese in esame, corredato da una previsione, basata sull'analisi dei dati dei mesi precedenti<sup>5</sup>, riferita ai tre mesi successivi.

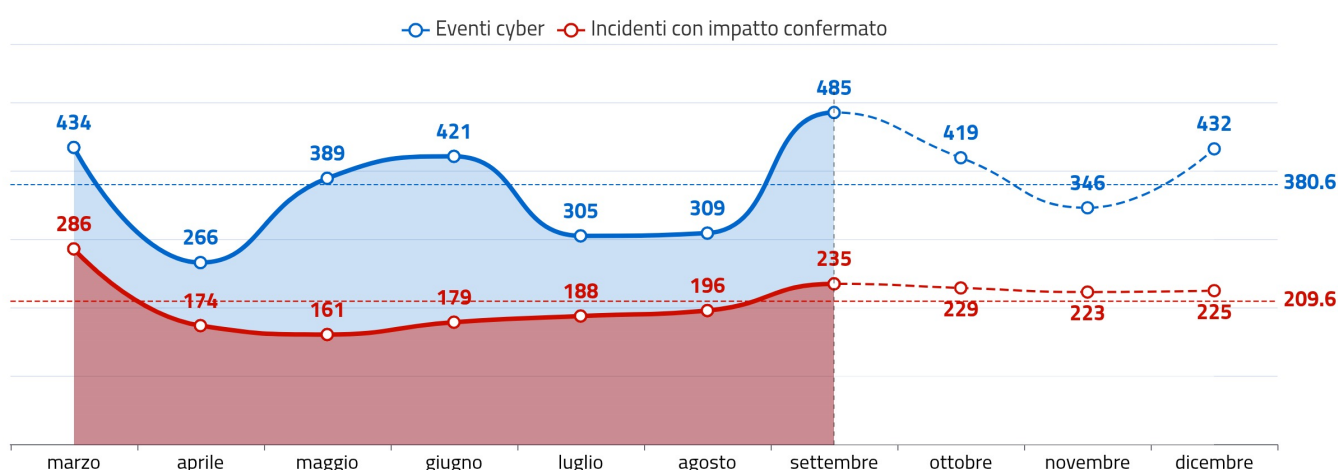


Figura 2 - andamento attività reattive e analisi previsionale

<sup>5</sup> 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 3 si riporta il numero di vittime di eventi per settore impattato<sup>6</sup>. Si evidenzia altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico la media di riferimento).

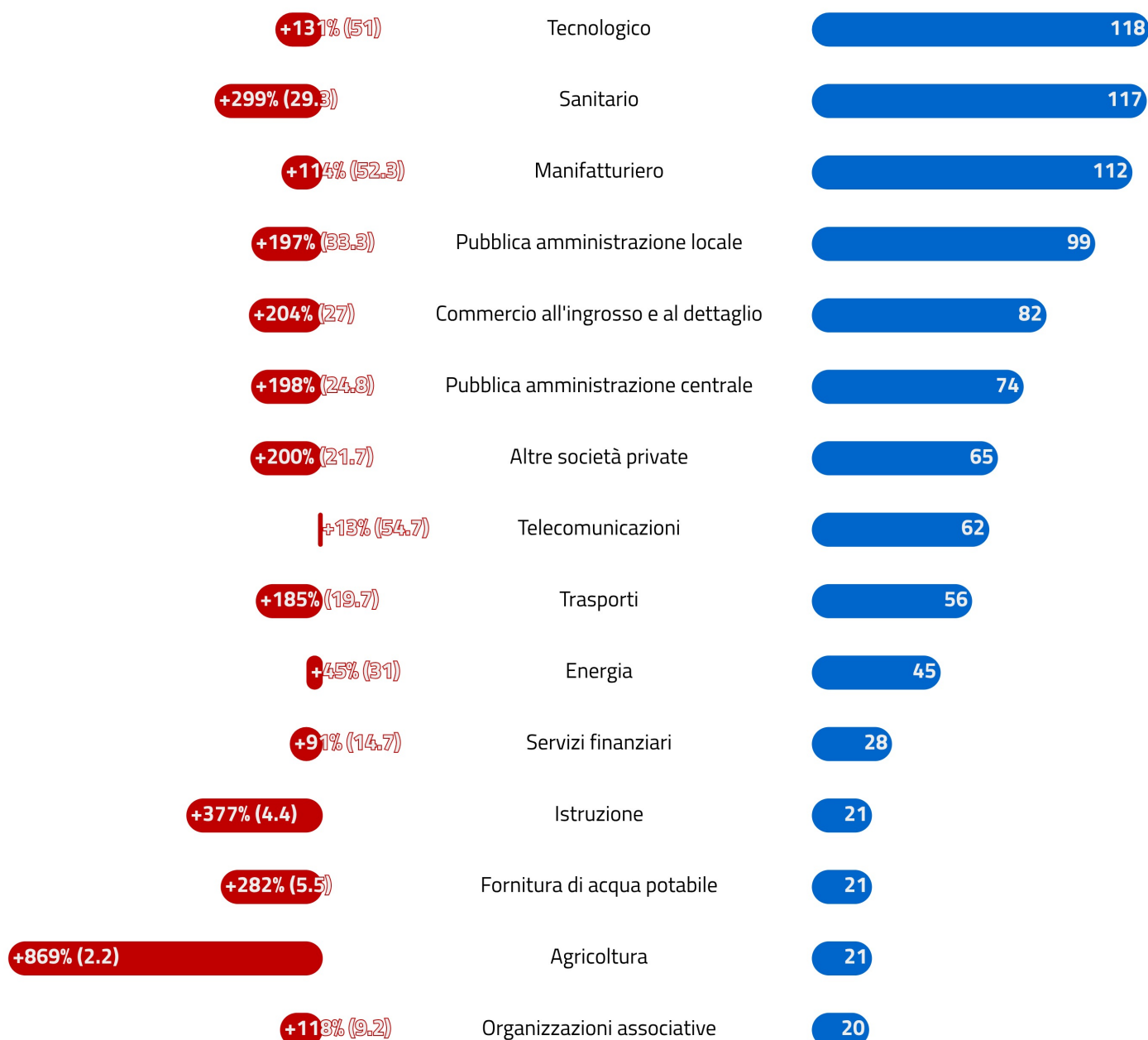


Figura 3 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente (top 15)

<sup>6</sup> 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 la distribuzione delle principali tipologie di minacce rilevate negli eventi<sup>7</sup> e la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico la media di riferimento).

Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (<https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn>).

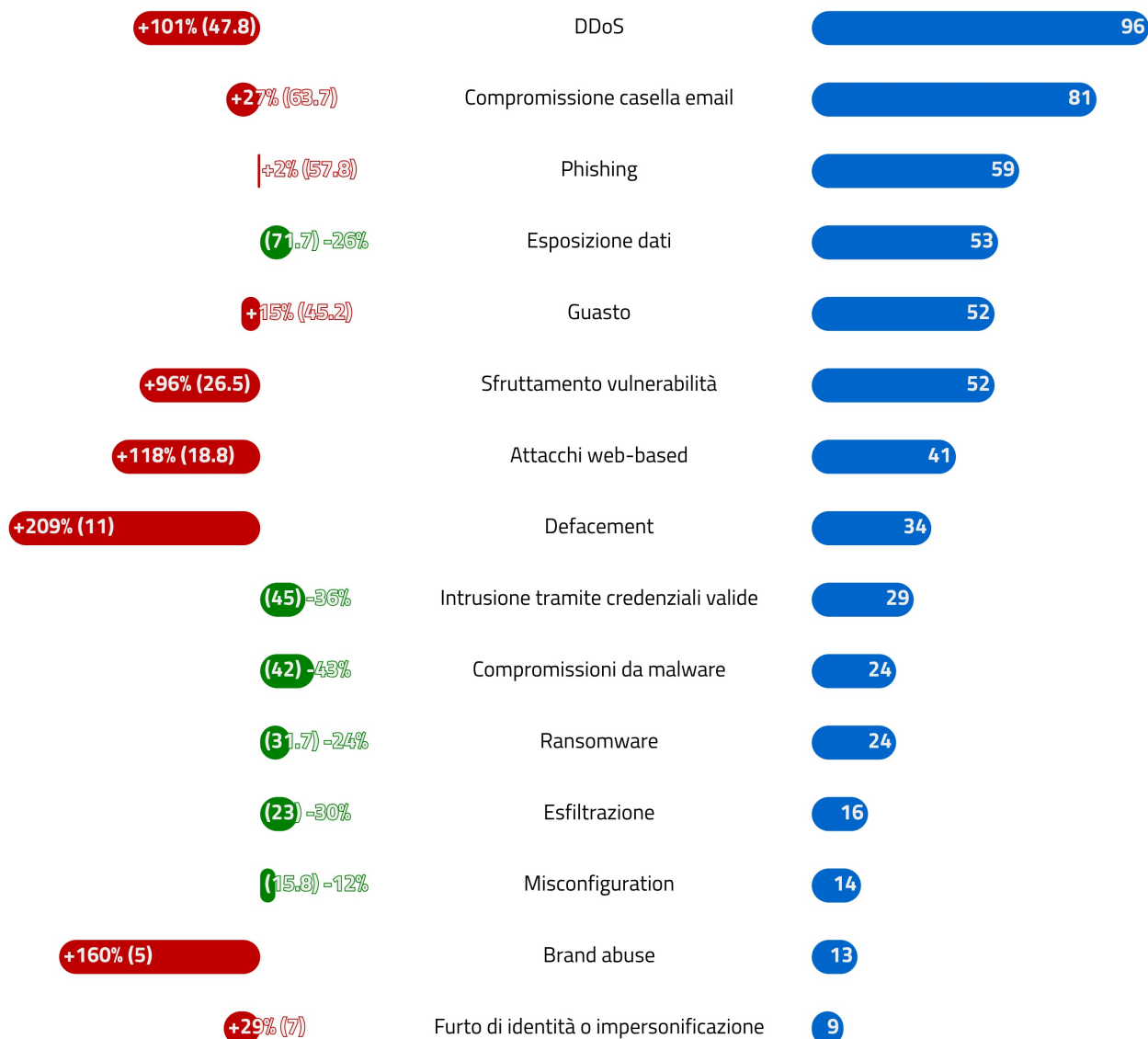


Figura 4 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente (top 15)

<sup>7</sup> 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, ottenuto analizzando gli eventi di settembre 2026. Si ricorda che ad un evento possono essere associate più minacce e più vittime e che uno stesso soggetto è conteggiato più volte qualora sia stato coinvolto in eventi distinti. Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (<https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn>). In Figura sono mostrati solo i 15 settori più interessati dalle minacce.

|                                        | Manifatturiero | Tecnologico | Commercio all'ingrosso e al dettaglio | Sanitario | Altre società private | Pubblica amministrazione locale | Pubblica amministrazione centrale | Telecomunicazioni | Trasporti | Agricoltura | Energia | Istruzione | Servizi finanziari | Università e ricerca | Organizzazioni associative |
|----------------------------------------|----------------|-------------|---------------------------------------|-----------|-----------------------|---------------------------------|-----------------------------------|-------------------|-----------|-------------|---------|------------|--------------------|----------------------|----------------------------|
| Defacement                             | 54             | 22          | 42                                    | 15        | 47                    | 8                               | 3                                 | 4                 | 3         | 19          | 4       | 20         | 4                  | 8                    | 10                         |
| Esposizione dati                       | 1              | 15          | 5                                     | 75        | 1                     | 28                              | 47                                | 10                | 22        |             | 26      |            | 11                 | 7                    | 1                          |
| Sfruttamento vulnerabilità             | 40             | 27          | 37                                    | 15        | 39                    | 9                               | 5                                 | 6                 | 3         | 18          | 3       | 15         | 3                  | 6                    | 9                          |
| Attacchi web-based                     | 40             | 24          | 37                                    | 14        | 38                    | 6                               | 5                                 | 2                 | 6         | 18          | 2       | 15         | 3                  | 6                    | 9                          |
| Guasto                                 | 12             | 25          | 11                                    | 8         | 3                     | 7                               |                                   | 15                | 13        | 1           | 5       | 1          | 4                  |                      |                            |
| DDoS                                   | 4              | 7           | 2                                     | 1         |                       | 45                              | 6                                 | 2                 | 8         |             |         |            | 4                  |                      | 5                          |
| Compromissione casella email           | 16             | 9           | 4                                     | 7         | 5                     | 4                               | 1                                 | 21                | 4         |             | 4       |            | 3                  | 2                    |                            |
| Phishing                               | 12             | 6           | 2                                     | 2         | 2                     | 5                               | 6                                 | 1                 | 2         |             | 5       |            | 2                  | 1                    |                            |
| Compromissioni da malware              | 4              | 8           | 8                                     | 3         | 1                     |                                 | 1                                 | 1                 |           |             |         |            | 3                  | 1                    |                            |
| Intrusione tramite credenziali valide  | 5              | 7           |                                       | 2         | 1                     | 3                               | 1                                 | 3                 | 1         |             | 2       |            | 2                  | 1                    | 1                          |
| Ransomware                             | 5              | 7           | 6                                     | 3         | 2                     |                                 | 1                                 | 1                 | 1         |             |         |            |                    |                      |                            |
| Misconfiguration                       | 3              | 4           | 1                                     | 1         | 1                     | 1                               |                                   | 1                 | 2         |             | 1       |            |                    |                      | 1                          |
| Esfiltrazione                          |                | 6           | 2                                     | 2         |                       | 1                               |                                   | 2                 | 1         |             |         |            |                    | 1                    |                            |
| Brand abuse                            | 1              |             |                                       | 1         | 2                     |                                 | 4                                 | 1                 |           |             |         |            | 2                  |                      |                            |
| Furto di identità o impersonificazione | 2              | 2           |                                       |           |                       | 1                               | 1                                 |                   | 1         |             |         |            |                    | 1                    |                            |
| Spear phishing                         |                | 1           |                                       |           | 2                     |                                 |                                   | 2                 | 1         |             |         |            | 1                  |                      |                            |
| Scansione attiva su credenziali        |                | 1           |                                       |           |                       | 3                               |                                   |                   |           |             |         |            | 2                  |                      |                            |
| Supply chain                           |                | 4           |                                       |           |                       | 1                               |                                   |                   | 1         |             |         |            |                    |                      |                            |
| Man-in-the-middle                      |                |             |                                       | 2         |                       | 1                               |                                   |                   |           |             | 1       |            |                    |                      |                            |
| Distribuzione di malware               |                | 2           | 1                                     |           |                       |                                 |                                   | 1                 |           |             |         |            |                    |                      |                            |

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

## 2.4 Distribuzione geografica delle vittime

I 485 eventi cyber hanno interessato **1.036** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

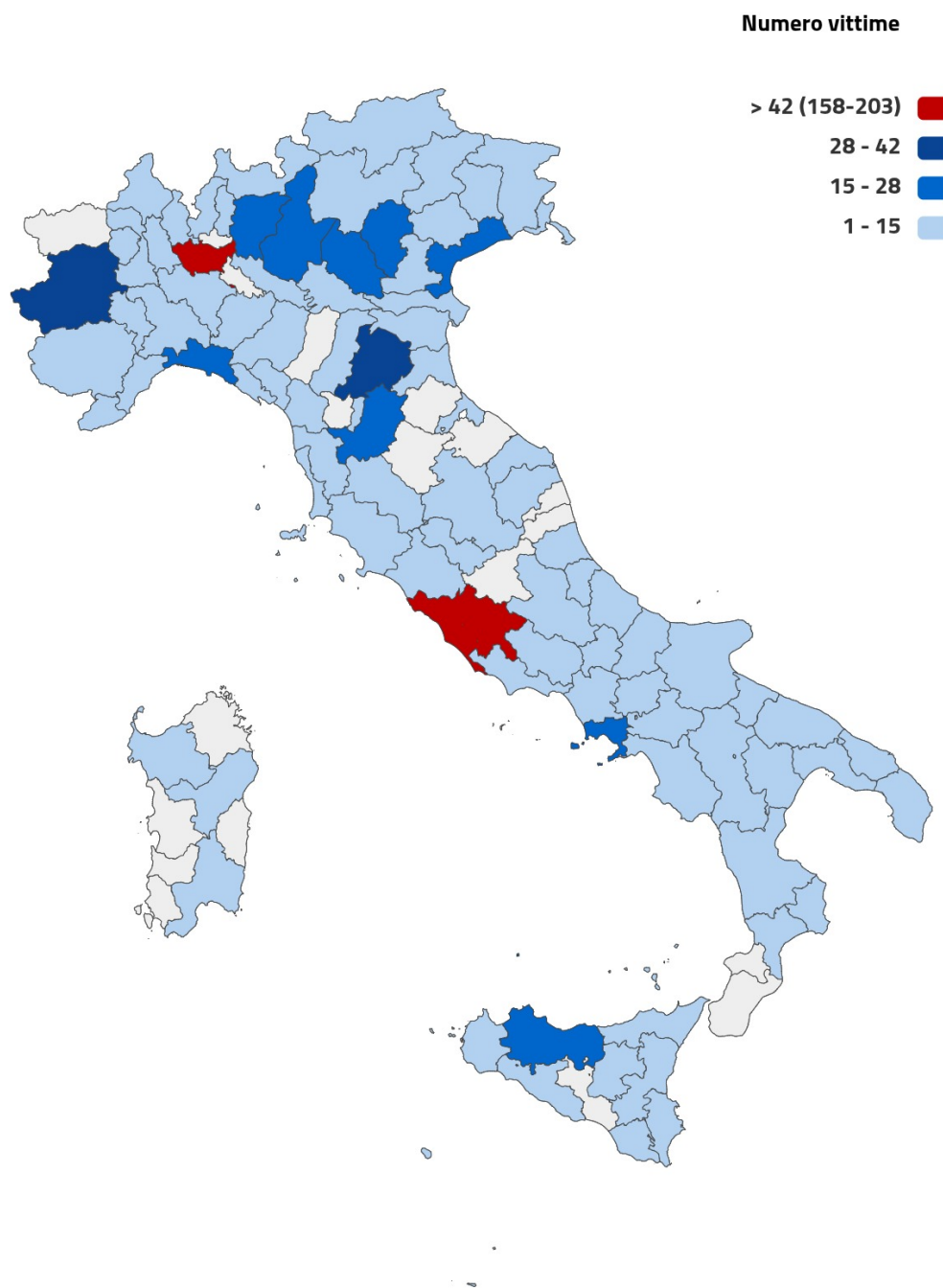


Figura 6 - distribuzione delle vittime degli eventi cyber

# 3 VULNERABILITÀ

A settembre 2026 sono state pubblicate<sup>8</sup> **15.074** nuove CVE, in **aumento (+2.355)** rispetto ad agosto. Di queste, **341** presentano almeno un *Proof of Concept (PoC)*, in **aumento (+53)**, e per **25** CVE è stato rilevato lo sfruttamento attivo, in **aumento (+12)** rispetto ad agosto.

## 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 **155**. Le vulnerabilità particolarmente gravi, riportate di seguito ordinate per stima d'impatto sistemico<sup>9</sup>, sono state quelle relative a prodotti di:

- **FlowiseAI**: disponibili Proof of Concept (PoC) per lo sfruttamento di 6 nuove vulnerabilità, di cui 2 con gravità "critica" e 4 con gravità "alta", presenti in Flowise, piattaforma per la creazione e gestione di applicazioni e flussi basati sull'intelligenza artificiale (stima di impatto sistemico **81.02/100**). Link all'alert del 28/09/2026;
- **SonicWall**: rilevato lo sfruttamento attivo in rete delle vulnerabilità CVE-2026-83548 e CVE-2026-83549 – già sanate dal vendor – presenti nel prodotto Secure Mobile Access (SMA) 1000 Series, soluzione per l'accesso remoto sicuro alle risorse aziendali (stima di impatto sistemico **79.48/100**). Link all'alert del 02/09/2026;
- **Cisco**: ha rilasciato aggiornamenti di sicurezza che risolvono molteplici nuove vulnerabilità, di cui 24 con gravità "critica" e 25 con gravità "alta", riguardanti diversi prodotti Cisco. Tra le vulnerabilità rilevate si evidenzia la CVE-2026-76460 che risulta attivamente sfruttata in rete (stima di impatto sistemico **79.48/100**). Link all'alert del 17/09/2026;

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

<sup>9</sup>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 constituency.

- **N-able:** gli aggiornamenti di sicurezza rilasciati da N-able sanano tre vulnerabilità, di cui una con gravità "critica" ed una con gravità "alta", in N-central, piattaforma per il monitoraggio e la gestione remota delle infrastrutture IT. Tra queste si segnala la CVE-2026-86218 che risulta essere attivamente sfruttata in rete (stima di impatto sistemico **79.48/100**). Link all'alert del 09/09/2026;
- **Adobe:** aggiornamenti di sicurezza Adobe sanano una vulnerabilità con gravità "critica" in Adobe Commerce, Adobe Commerce B2B e Magento Open Source, piattaforme per il commercio elettronico utilizzate per la realizzazione e la gestione di siti e servizi di vendita online. Tale vulnerabilità, della quale si evidenzia lo sfruttamento attivo in rete, potrebbe consentire a un attaccante non autenticato di eseguire codice arbitrario sui sistemi interessati (stima di impatto sistemico **79.48/100**). Link all'alert del 08/09/2026;

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 7 è riportato il numero delle vulnerabilità rilevate distribuite tra i principali vendor<sup>10</sup>.

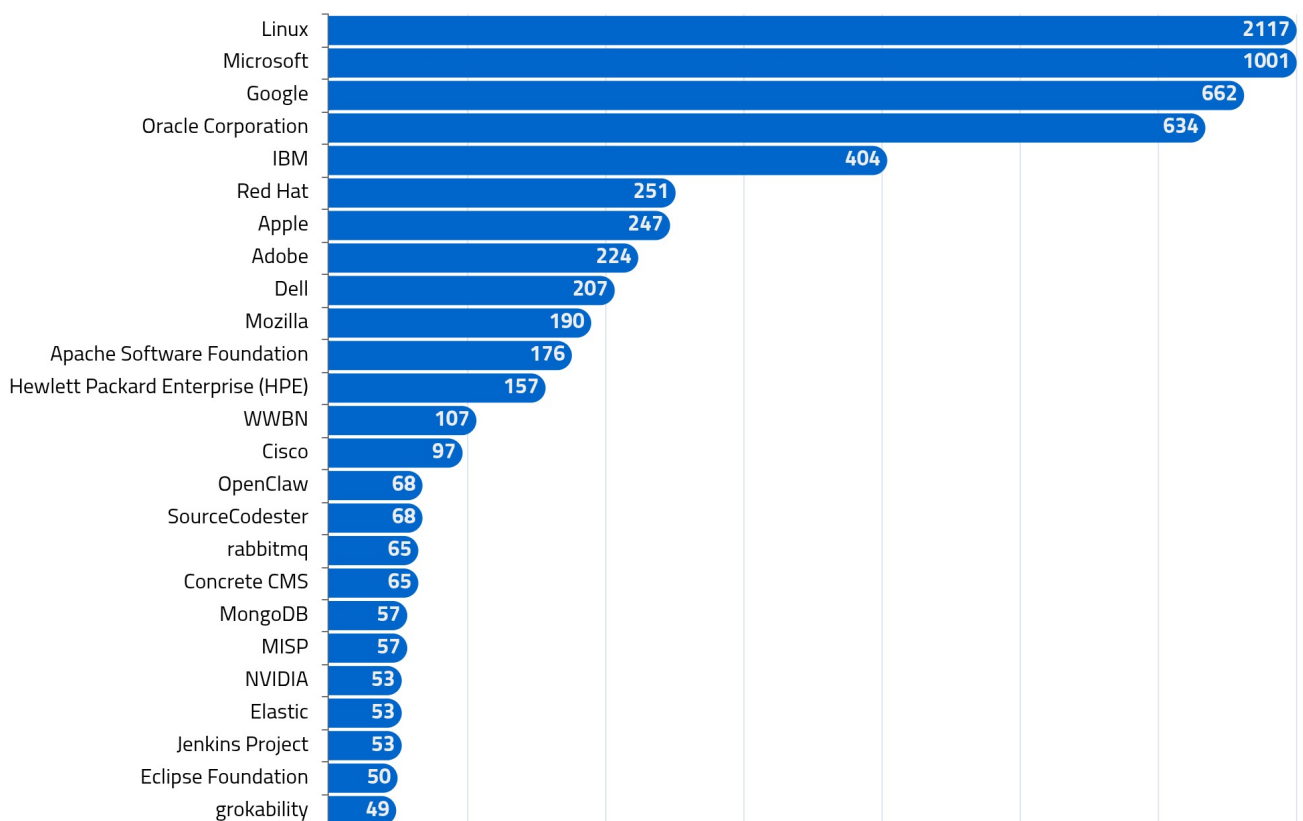


Figura 7 - top 25 produttori affetti da vulnerabilità nel mese

<sup>10</sup>I valori attribuiti alla voce *Linux* si riferiscono esclusivamente alle vulnerabilità registrate dalla CVE Numbering Authority (CNA) <https://kernel.org/> e afferiscono dunque unicamente al kernel Linux. Maggiori informazioni a questo link: <https://www.cve.org/PartnerInformation/ListofPartners/partner/Linux>

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

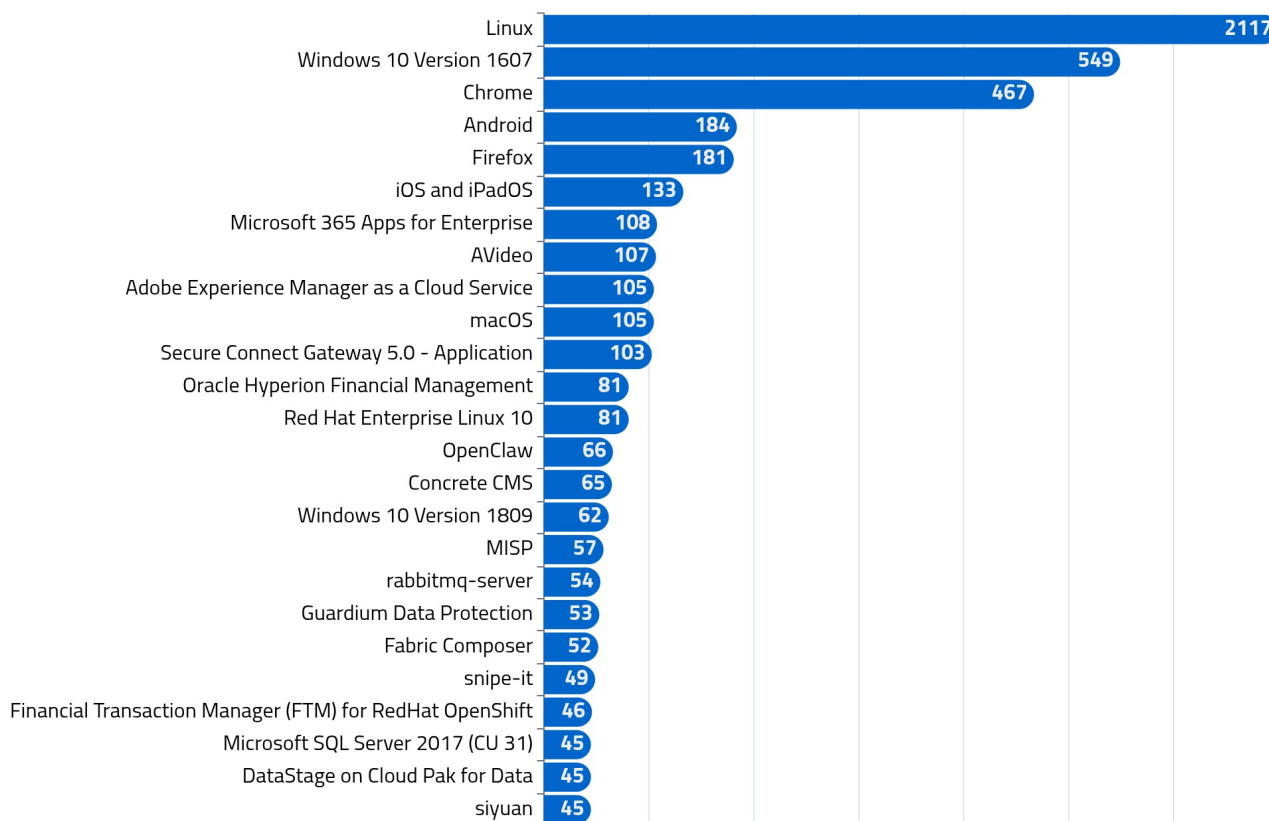


Figura 8 - top 25 prodotti affetti da vulnerabilità nel mese

### 3.3 CWE nel mese

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

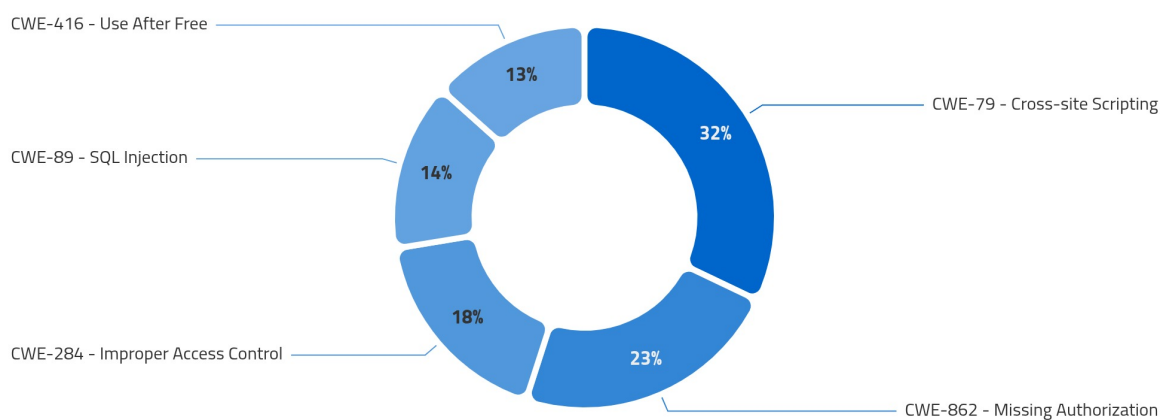


Figura 9 - top 5 CWE nel mese

### 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)<sup>11</sup> fornito dal FIRST, nel mese in esame.

|                                        |                                                                                                                                                                                                                                                                                             |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor</b>                          | <b>GitLab</b>                                                                                                                                                                                                                                                                               |
| <b>Prodotti e versioni vulnerabili</b> | <b>GitLab Community Edition (CE) e Enterprise Edition (EE) tutte le versioni dalla 18.7 a prima della 18.11.12, versioni dalla 19.0 a prima della 19.0.9, versioni dalla 19.1 a prima della 19.1.8, versioni dalla 19.2 a prima della 19.2.6 e versioni dalla 19.3 a prima della 19.3.2</b> |
| <b>Descrizione vulnerabilità</b>       | <b>Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di leggere file arbitrari sul server da remoto.</b>                                                                                                                                                    |
| <b>Data di rilascio CVE</b>            | <b>12/09/2026 modificata il 24/09/2026</b>                                                                                                                                                                                                                                                  |
| <b>CVSS score 3.0</b>                  | <b>10 Critical</b>                                                                                                                                                                                                                                                                          |
| <b>EPSS max score</b>                  | <b>0.91</b>                                                                                                                                                                                                                                                                                 |

Tabella 1 - CVE-2026-85706

|                                        |                                                                                                                                                              |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor</b>                          | <b>PaperCut</b>                                                                                                                                              |
| <b>Prodotti e versioni vulnerabili</b> | <b>PaperCut MF/NG tutte le versioni fino alla 24.1.9; versioni dalla 25.0.0 alla 25.0.11 e versioni dalla 26.0.0 alla 26.0.3</b>                             |
| <b>Descrizione vulnerabilità</b>       | <b>Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di modificare da remoto parametri nella configurazione del sistema.</b> |
| <b>Data di rilascio CVE</b>            | <b>28/08/2026 modificata il 14/09/2026</b>                                                                                                                   |
| <b>CVSS score 3.0</b>                  | <b>8.8 High</b>                                                                                                                                              |
| <b>EPSS max score</b>                  | <b>0.85</b>                                                                                                                                                  |

Tabella 2 - CVE-2026-81578

<sup>11</sup>Il sito web <https://www.first.org/epss/> fornisce un'indicazione della probabilità che una vulnerabilità venga sfruttata. Il valore è aggiornato quotidianamente dal FIRST.

|                                        |                                                                                                                                                                        |
|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor</b>                          | Cisco                                                                                                                                                                  |
| <b>Prodotti e versioni vulnerabili</b> | Cisco AsyncOS for Cisco Secure Email Gateway tutte le versioni fino alla 15.5.4-012; versioni dalla 16.0 alla 16.0.4-209 e versioni dalla 16.5 alla 16.5.0-748         |
| <b>Descrizione vulnerabilità</b>       | Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice arbitrario da remoto con privilegi di root sul sistema operativo. |
| <b>Data di rilascio CVE</b>            | 14/09/2026 modificata il 15/09/2026                                                                                                                                    |
| <b>CVSS score 3.0</b>                  | 9.8 Critical                                                                                                                                                           |
| <b>EPSS max score</b>                  | 0.28                                                                                                                                                                   |

Tabella 3 - CVE-2026-76461

# 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<sup>12</sup> condivisi dal CSIRT Italia tramite piattaforma MISP<sup>13</sup>, in modo da caratterizzarne le tipologie più frequenti.

## 4.1 Ransomware: distribuzione delle vittime

A settembre 2026, il 17% degli attacchi ransomware ha colpito soggetti critici, il 25% ha colpito soggetti a media criticità, ed il restante 58% ha coinvolto altri soggetti a criticità minore.

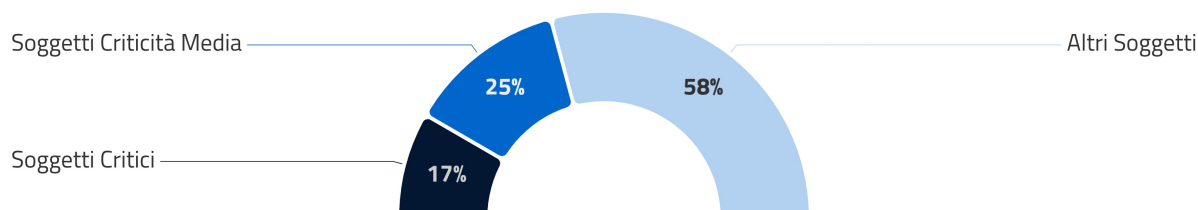


Figura 10 - distribuzione delle vittime di ransomware in base alla loro criticità

<sup>12</sup>IoC (Indicatore di Compromissione), 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.

<sup>13</sup>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 mese di settembre 2026 ha permesso di individuare **19** rivendicazioni di attacchi ransomware a danno di soggetti italiani<sup>14</sup>.

Il grafico in Figura 11 mostra l'andamento delle rivendicazioni riferite all'Italia nel corso degli ultimi 12 mesi.

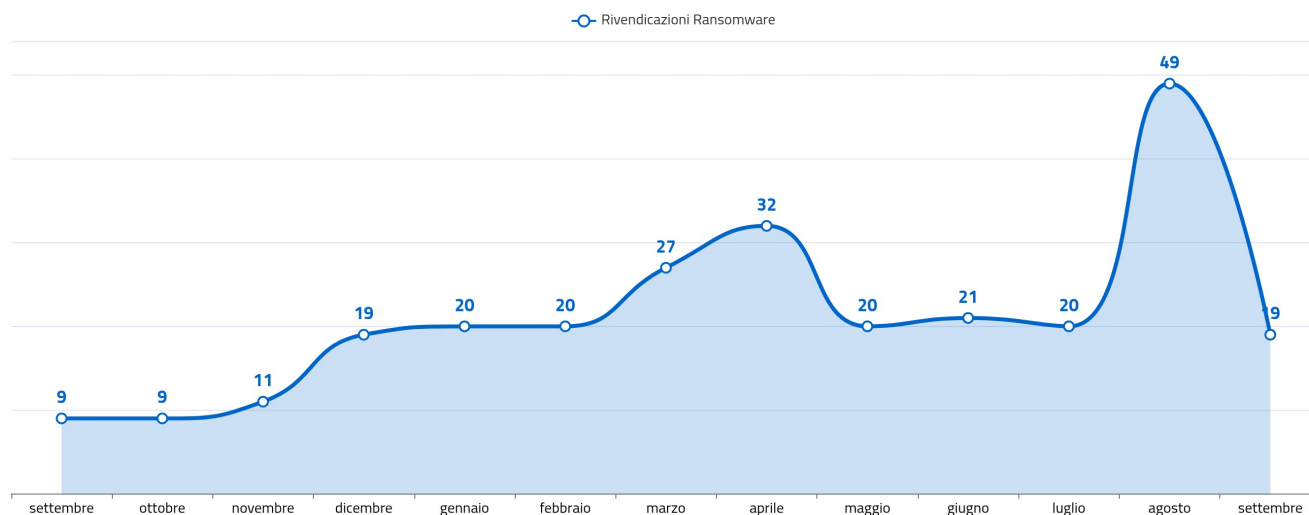


Figura 11 - andamento delle rivendicazioni ransomware per l'Italia

Il grafico in Figura 12 mostra i gruppi più attivi in termini di rivendicazioni in Italia.

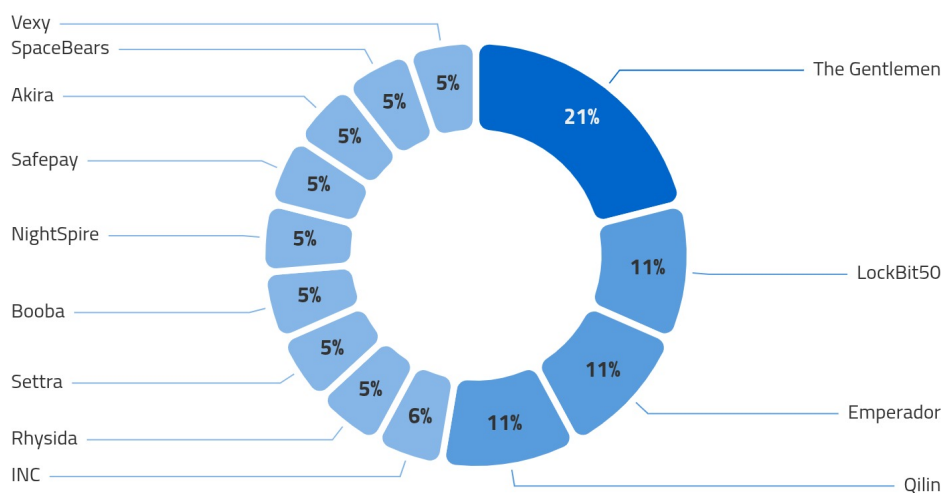


Figura 12 - distribuzione percentuale dei gruppi autori delle rivendicazioni

<sup>14</sup>Talvolta, le rivendicazioni relative ad attacchi ransomware non sono confermate dal soggetto coinvolto.

### 4.3 Rivendicazioni DDoS

A settembre 2026 sono state individuate<sup>15</sup> **39** rivendicazioni di attacchi DDoS in danno di soggetti italiani.

Il grafico in Figura 13 mostra l'andamento delle rivendicazioni DDoS riferite all'Italia nel corso degli ultimi 12 mesi.

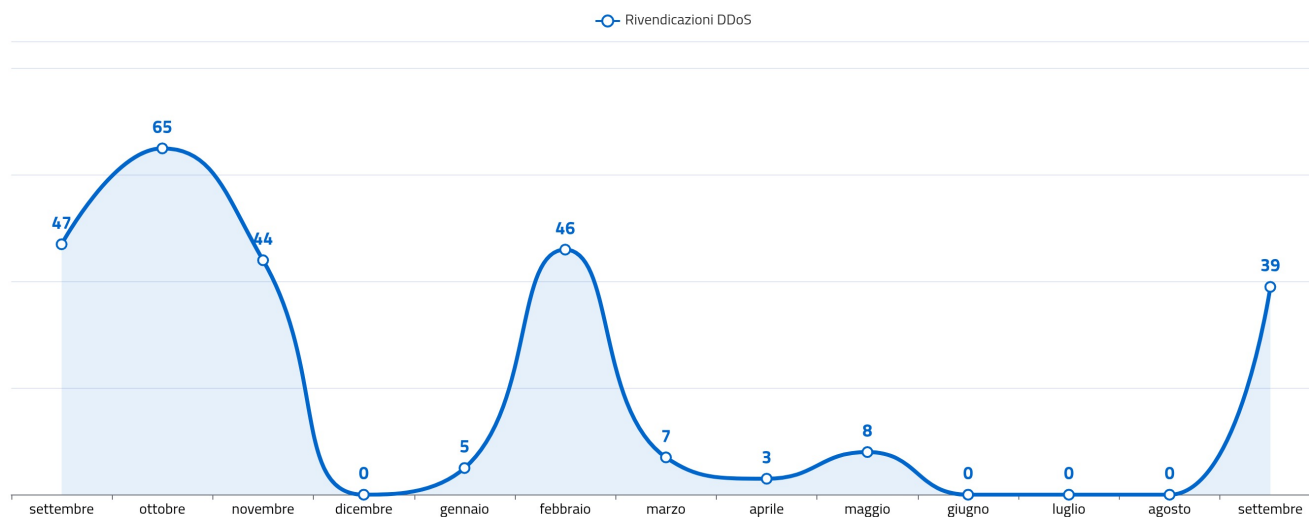


Figura 13 - andamento delle rivendicazioni DDoS riferite all'Italia

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

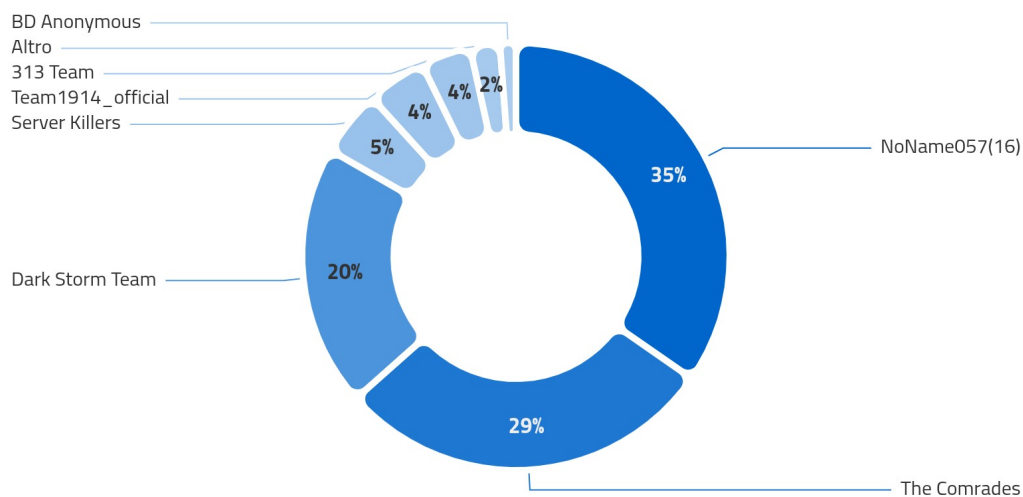


Figura 14 - distribuzione percentuale dei gruppi autori delle rivendicazioni

<sup>15</sup>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.

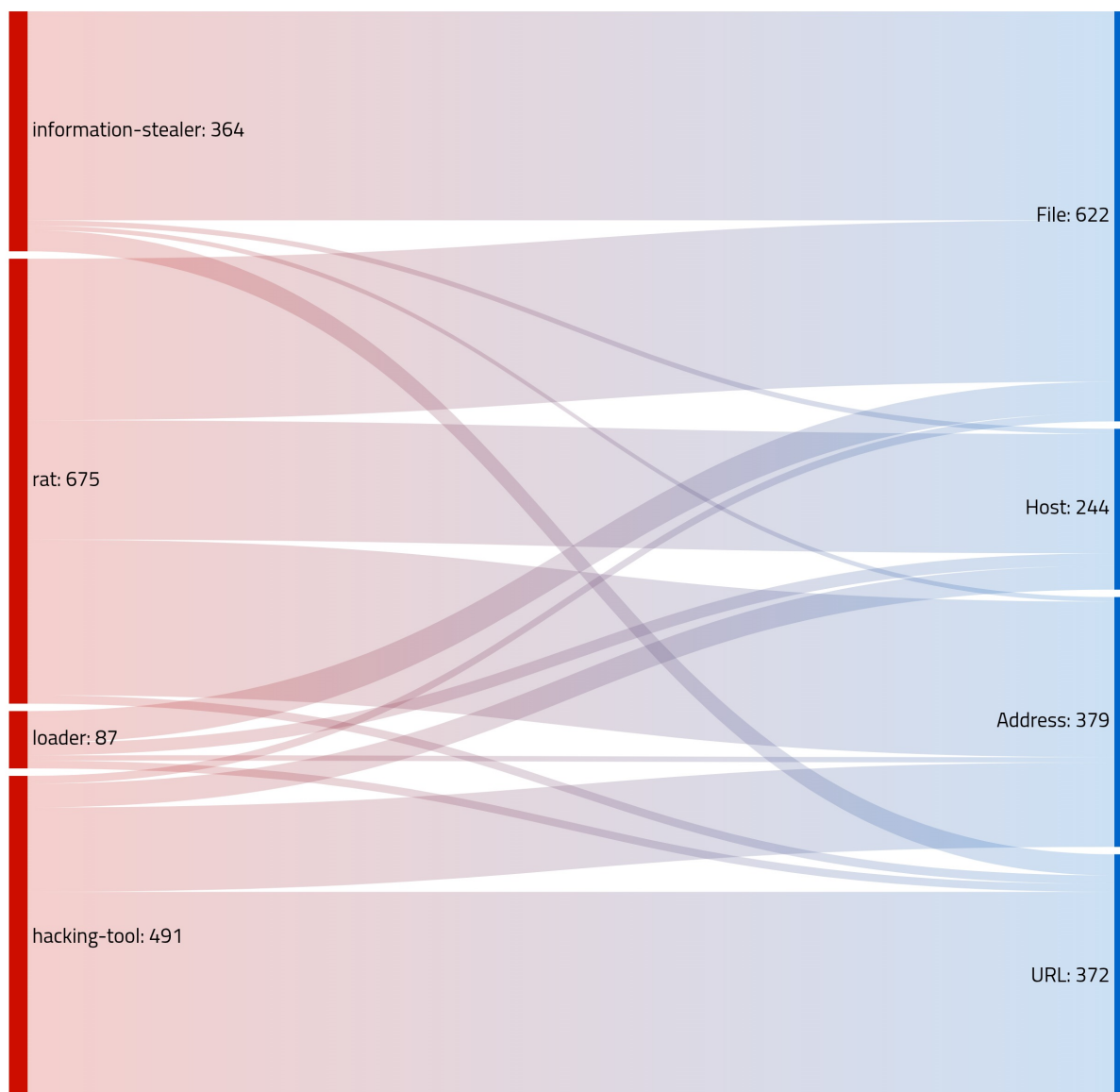


Figura 15 - numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware

# 5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo<sup>16</sup>, 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 settembre 2026 sono state diramate un totale di **4.460** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su internet complessivamente **8.213** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **F5 BIG-IP** (CVE-2026-94127): tale vulnerabilità – di tipo *Heap-based Buffer Overflow* – permetterebbe a un eventuale attaccante di sfruttare traffico malevolo appositamente predisposto per ottenere Remote Code Execution (RCE) sul dispositivo. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Checkpoint Quantum Security Gateway** (CVE-2026-85102): tale vulnerabilità – di tipo *Improper Certificate Validation* – permetterebbe a un eventuale attaccante da remoto non autenticato di eseguire codice arbitrario sul Security Gateway durante la negoziazione VPN, compromettendo sistemi, dati e servizi aziendali. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **WordPress** (CVE-2026-87902, CVE-2026-93485): tali vulnerabilità – rispettivamente di tipo *Remote File Inclusion* e *Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')* – permetterebbero a un eventuale attaccante, in presenza di specifiche condizioni, di eseguire codice da remoto. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.

<sup>16</sup>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.

- **Microsoft Exchange** (CVE-2026-62911): tale vulnerabilità – di tipo *Authentication Bypass by Capture-Replay* – potrebbe permettere a un eventuale attaccante non autenticato, soddisfatte alcune precondizioni, di eseguire da remoto codice arbitrario sui sistemi affetti. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Zimbra Collaboration Suite** (CVE-2026-93643): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante remoto non autenticato, purché in possesso dell’accesso a un documento pubblico supportato presente nel servizio “Briefcase”, di manipolare specifici parametri non firmati delle richieste “/downloads” per effettuare scritture arbitrarie di file in percorsi al di fuori delle directory previste. Mediante tale capacità, l’attaccante potrebbe caricare o sovrascrivere file controllati e successivamente ottenere l’esecuzione di comandi arbitrari sul sistema con i privilegi dell’utente zimbra. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **SonicWall SMA1000** (CVE-2026-83548, CVE-2026-83549): tali vulnerabilità – rispettivamente di tipo *Server-Side request forgery (SSRF)*, *Unintended Proxy or Intermediary (‘Confused Deputy’)*, *Improper neutralization of special elements used in an OS command (‘OS command injection’)* – permetterebbero a un eventuale attaccante remoto di eludere i meccanismi di sicurezza ed eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Cisco ASA** (CVE-2026-20329, CVE-2026-20332): tali vulnerabilità – rispettivamente di tipo *Improper handling of exceptional conditions*, *Improper Neutralization*, *Protection Mechanism Failure* e *Improper Access Control* – potrebbero permettere a un eventuale attaccante di aggirare i normali meccanismi di autenticazione ed eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Apache MyFaces** (CVE-2026-68536): tale vulnerabilità – di tipo *Server-Side Request Forgery (SSRF)* – permetterebbe a un eventuale attaccante remoto non autenticato di indurre l’applicazione a effettuare richieste verso risorse interne o accedere a file locali sensibili, con potenziale compromissione della riservatezza, integrità e disponibilità del sistema interessato.
- **Proxmox** (CVE-2023-54391): tale vulnerabilità – di tipo *Missing Critical Step in Authentication* – permetterebbe a un eventuale attaccante non autenticato, per mezzo dell’invio di apposite richieste API, di autenticarsi come ogni utente esistente, il quale non ha configurato un secondo fattore di autenticazione, sui sistemi interessati.
- **Vercel Next.js** (CVE-2026-75604): tale vulnerabilità – di tipo *Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’)* – permetterebbe a un eventuale attaccante non autenticato di eseguire codice da remoto.
- **GitLab** (CVE-2026-85706, CVE-2026-87719): tali vulnerabilità – rispettivamente di tipo *Arbitrary File Read* e *Information Disclosure* – permetterebbero a un eventuale attaccante di leggere file arbitrari sul filesystem e di accedere a informazioni sensibili sui sistemi interessati. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **Check Point Multi-Domain Security Management Server, Log Server, Security Management Server e Multi-Domain Log Server** (CVE-2026-91843): tale vulnerabilità – di tipo *Stack-based Buffer Overflow* – permetterebbe a un eventuale attaccante di eseguire codice arbitrario da remoto con privilegi di amministratore. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **SAP Extended Passport (EPP)** (CVE-2026-44756): la CVE-2026-44756 (OVERPASS), con punteggio CVSS 10.0, è una vulnerabilità critica di tipo *memory corruption* che interessa il componente Extended Passport Processing (EPP) del kernel SAP. Lo sfruttamento della falla consente a un attaccante remoto non autenticato di eseguire codice arbitrario con privilegi elevati e compromettere completamente il sistema SAP. Ulteriori dettagli nell’alert sul sito dello CSIRT Italia.
- **NLnet Labs Unbound** (CVE-2026-81642, CVE-2026-82717): tali vulnerabilità, di tipo *Heap-based Buffer Overflow*, permetterebbero a un eventuale attaccante di causare condizioni di Denial of Service (DoS) mediante arresto del servizio e, nei casi più gravi, ottenere l’esecuzione remota di codice arbitrario (RCE) sul sistema vulnerabile, con

conseguente compromissione della disponibilità, dell'integrità e della sicurezza dell'infrastruttura interessata.

- **Vercel Next.js** (CVE-2026-94545): tale vulnerabilità – di tipo *Remote Code Execution* – è causata da una gestione non adeguata dei dati in input durante la generazione di contenuti SVG mediante la libreria Satori, utilizzata dalla funzionalità next/og ImageResponse. Un utente malintenzionato, tramite richieste opportunamente predisposte, potrebbe alterare il contenuto SVG elaborato dall'applicazione e, in determinate condizioni, eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft Windows DNS Server** (CVE-2026-69730): tale vulnerabilità – di tipo *Use After Free* – interessa il servizio di risoluzione dei nomi ed è causata da un'errata gestione della memoria dinamica durante l'elaborazione dei pacchetti di rete. Nel dettaglio, un attaccante remoto non autenticato potrebbe inviare pacchetti opportunamente predisposti al server target al fine di sfruttare tale condizione ed eseguire codice arbitrario sul sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Adobe Commerce B2B, Magento Open Source e Commerce** (CVE-2026-75650): tale vulnerabilità – di tipo *Improper Neutralization of Special Elements Used in a Template Engine* – permetterebbe a un eventuale attaccante remoto non autenticato di eseguire codice remoto sul sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **MikroTik RouterOS** (CVE-2026-67276, CVE-2026-67277, CVE-2026-67281, CVE-2026-86060): tali vulnerabilità – rispettivamente di tipo *Improper verification of cryptographic signature*, *Improper neutralization of argument delimiters in a command ('argument injection')*, *Access of uninitialized pointer*, *Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')*, *Missing authentication for critical function* – permetterebbero a un eventuale attaccante di eludere i meccanismi di autenticazione e di elevare i propri privilegi sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Zohocorp ManageEngine ADSelfService Plus** (CVE-2026-74849, CVE-2026-75791): tali vulnerabilità – rispettivamente di tipo *Improper neutralization of special elements used in an OS command ('OS command injection')*, *Missing authentication for critical function* – permetterebbero a un eventuale attaccante di eseguire codice arbitrario o di eludere i meccanismi di autenticazione delle API REST sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Palo Alto PAN-OS Management Interface** (CVE-2026-0310): tale vulnerabilità – di tipo *Out-of-bounds Write* – permetterebbe a un eventuale attaccante remoto non autenticato con accesso alle interfacce di gestione web o alle interfacce dataplane interessate, di compromettere la disponibilità del servizio sui firewall "VM-Series" e di eseguire codice arbitrario con privilegi elevati sui sistemi della "PA-Series". Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft Sharepoint** (CVE-2026-65660): tale vulnerabilità – di tipo *Improper Control of Generation of Code ('Code Injection')* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario nelle istanze Microsoft SharePoint interessate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Jenkins** (CVE-2026-84645): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante di ottenere accesso alla Script Console e di eseguire così codice arbitrario da remoto sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **WS02** (CVE-2026-5430): tale vulnerabilità – di tipo *Improper Validation of Certificate With Host Mismatch* – permetterebbe a un eventuale attaccante, attraverso la generazione e il successivo uso di un JSON Web Token (JWT) appositamente predisposto facente uso di un algoritmo non supportato, di ottenere l'accesso non autorizzato ai sistemi affetti e, potenzialmente, la compromissione completa di account amministrativi.
- **Gitea** (CVE-2026-60004): tale vulnerabilità – di tipo *Improper Control of Generation of Code ('Code Injection')* – permetterebbe a un eventuale attaccante con permessi di scrittura su un repository di installare un Git hook

eseguibile e ottenere l'esecuzione di comandi arbitrari sul sistema con i privilegi dell'account di servizio Gitea. Qualora l'istanza vulnerabile risulti configurata con la registrazione pubblica degli utenti abilitata, tali prerequisiti potrebbero essere soddisfatti anche da un attaccante remoto privo di credenziali valide, il quale potrebbe registrare autonomamente un account, ottenere i privilegi minimi richiesti e procedere allo sfruttamento della vulnerabilità. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.

- **Cisco SD-WAN** (CVE-2026-76504): tale vulnerabilità – di tipo *Authentication Bypass* – potrebbe consentire ad un attaccante remoto e non autenticato di eludere i meccanismi di autenticazione e ottenere privilegi amministrativi sui sistemi interessati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **BerriAI LiteLLM** (CVE-2026-59822): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe a un eventuale attaccante remoto non autenticato di eludere i meccanismi di autenticazione e accedere agli strumenti MCP senza disporre di credenziali valide. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Redis** (CVE-2026-81934): tale vulnerabilità – di tipo *Use After Free* – permetterebbe a un eventuale attaccante di sfruttare un errore nella gestione della memoria per ottenere l'esecuzione di comandi arbitrari sul sistema vulnerabile con i privilegi del processo Redis, compromettendo la riservatezza, l'integrità e la disponibilità dei dati e del servizio.
- **PgAdmin** (CVE-2026-86863, CVE-2026-86864): tali vulnerabilità – rispettivamente di tipo *Authentication Bypass* e *Path Traversal* – permetterebbero a un eventuale attaccante di eludere i meccanismi di autenticazione e di scrivere file arbitrari sul filesystem dei sistemi interessati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **ConnectWise ScreenConnect** (CVE-2026-84869): tale vulnerabilità – di tipo *Missing Authorization* – permetterebbe a un eventuale attaccante con privilegi limitati di eludere le misure di sicurezza previste dal prodotto ed eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **Mikrotik RouterOS** (CVE-2026-67276, CVE-2026-86060): tali vulnerabilità – rispettivamente di tipo *Improper verification of cryptographic signature*, *Improper neutralization of argument delimiters in a command ('argument injection')* – permetterebbero a un eventuale attaccante di eludere i meccanismi di autenticazione e di elevare i propri privilegi sui sistemi interessati. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **GeoNetwork GeoServer** (CVE-2026-55864, CVE-2026-57582, CVE-2026-58400, CVE-2026-63219): tali vulnerabilità – rispettivamente di tipo *Missing Authorization*, *Improper Control of Generation of Code ('Code Injection')*, *Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')* – permetterebbero a un eventuale attaccante di: aggirare i controlli di autorizzazione previsti per le funzionalità amministrative e caricare file formatter arbitrari sul server; indurre il server ad effettuare richieste HTTP verso destinazioni arbitrarie controllate dall'attaccante o raggiungibili dalla rete interna; eseguire codice JavaScript arbitrario nel browser di utenti legittimi mediante la predisposizione di richieste appositamente costruite eseguire codice arbitrario sul sistema.
- **JFrog Artifactory** (CVE-2026-42016, CVE-2026-42018): tali vulnerabilità – rispettivamente di tipo *Incorrect Authorization* e *Improper Authentication* – potrebbero consentire, laddove utilizzate in maniera congiunta, a un eventuale attaccante non autenticato l'acquisizione di un token interno associato all'utente anonimo e l'escalation dei privilegi a quelli di amministratore, ottenendo così il controllo completo dei sistemi affetti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **N-able N-central** (CVE-2026-86218): tale vulnerabilità – di tipo *Improper neutralization of directives in statically saved code* – permetterebbe a un eventuale attaccante remoto non autenticato di eseguire codice arbitrario sul server vulnerabile, con possibile compromissione completa del sistema, accesso non autorizzato a dati e configurazioni sensibili e creazione di account amministrativi fraudolenti. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **ServiceNow AI Platform** (CVE-2026-13016): tale vulnerabilità – di tipo *Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')* – permetterebbe a un eventuale attaccante remoto non autenticato di

eseguire query SQL arbitrarie sul database della ServiceNow AI Platform, con conseguente accesso non autorizzato, modifica o cancellazione di dati e potenziale compromissione dell'istanza interessata. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.

- **Issabel Foundation Framework** (CVE-2026-89026): tale vulnerabilità – di tipo *Use of Hard-coded Cryptographic Key* – relativa alla presenza di una chiave JWT (JSON Web Token) hard-coded permetterebbe a un eventuale attaccante remoto non autenticato di forgiare un bearer token valido che potrebbe essere utilizzato per eseguire comandi arbitrari sul sistema operativo dei sistemi affetti con i privilegi dell'utente Asterisk relativo all'applicativo.
- **Wordpress Plugin "Stellarwp" (The Events Calendar)** (CVE-2026-78006, CVE-2026-78159): tali vulnerabilità – rispettivamente di tipo *Deserialization of Untrusted Data*, *Improper Control of Generation of Code ('Code Injection')* – permetterebbero a un eventuale attaccante non autenticato di eseguire codice arbitrario sul server.
- **SUSE Rancher** (CVE-2026-88804): tale vulnerabilità – di tipo *Cross-site Scripting (XSS)* – permetterebbe a un eventuale attaccante remoto non autenticato di inserire codice persistente nella pagina di login eseguito nel contesto del browser della vittima (Stored-XSS), portando potenzialmente alla compromissione delle credenziali o di sessioni esistenti degli amministratori dei sistemi affetti, ottenendo così la conseguente compromissione dell'intero cluster.
- **Sauter modu680-AS** (CVE-2026-78319): tale vulnerabilità – di tipo *Race Condition* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario sui sistemi interessati.
- **Wordpress Plugin "The Pods" (Custom Content Types and Fields)** (CVE-2026-19598): tale vulnerabilità – di tipo *Incorrect Authorization* – permetterebbe a un eventuale attaccante di elevare i propri privilegi fino al ruolo di amministratore.
- **Cleo Harmony** (CVE-2026-84114, CVE-2026-84115): tali vulnerabilità – rispettivamente di tipo *Improper Authentication* e *Incorrect Privilege Assignment* – permetterebbero, laddove utilizzate in maniera congiunta, a un eventuale attaccante in possesso di un accesso con utente con bassi privilegi di elevare questi ultimi a quelli di Administrator e, conseguentemente, di eseguire comandi arbitrari sul sistema operativo dei sistemi affetti sfruttando l'automation engine del prodotto. Ulteriori dettagli nell>alert sul sito dello CSIRT Italia.
- **WordPress Plugin "Forminator"** (CVE-2026-92229): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante non autenticato di eseguire shortcode arbitrari a causa della mancata validazione dell'input prima della chiamata alla funzione "do\_shortcode" di WordPress e di eseguire così, potenzialmente, codice o comandi arbitrari sui sistemi affetti.
- **Citrix NetScaler** (CVE-2026-88771, CVE-2026-88772): tali vulnerabilità – rispettivamente di tipo *Improper input validation*, *Improper Restriction of Operations within the Bounds of a Memory Buffer* – potrebbero consentire a un utente malintenzionato di eseguire codice arbitrario anche da remoto, eludere le misure di sicurezza e compromettere la disponibilità del servizio sui sistemi interessati.
- **Cisco Secure Email Gateway** (CVE-2026-76461): tale vulnerabilità – di tipo *SQL Injection* – permetterebbe a un eventuale attaccante non autenticato, mediante l'invio di e-mail appositamente predisposte contenenti statement SQL malevoli e a causa di un'insufficiente validazione nella logica di parsing, di eseguire da remoto codice arbitrario con i privilegi di root sul sistema operativo dei sistemi affetti.

In Figura 16 viene riportata la distribuzione delle segnalazioni per tipologia di soggetto.

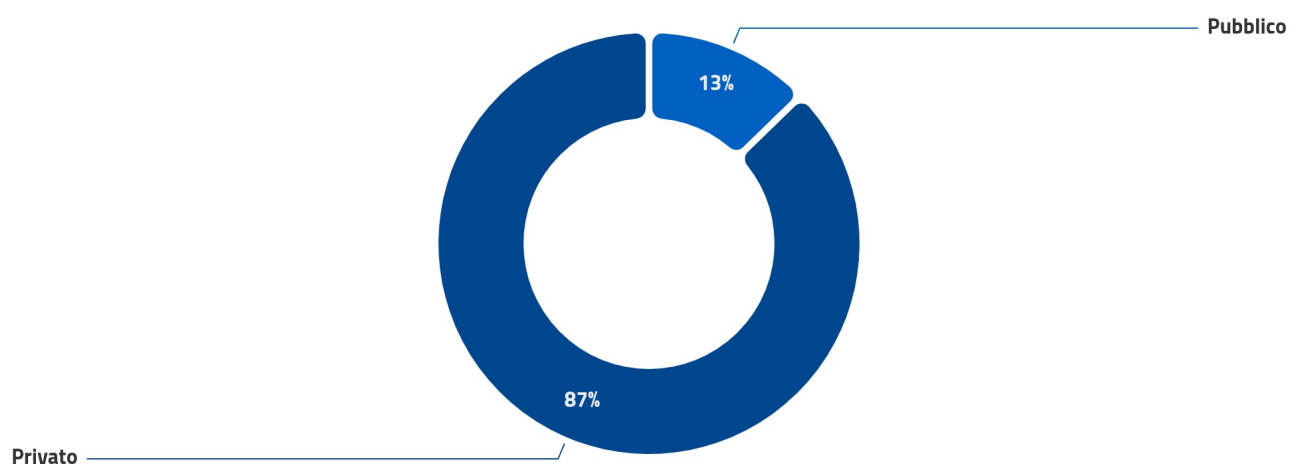


Figura 16 - *distribuzione delle segnalazioni per tipologia di soggetto*

# 6 ASPETTI DI INTERESSE DELLA MINACCIA CYBER GLOBALE



Il presente capitolo fornisce una rappresentazione dello stato della minaccia cibernetica a livello globale, elaborata esclusivamente a partire da fonti aperte ritenute affidabili, quali report di settore, analisi di enti istituzionali, pubblicazioni specialistiche e contributi di operatori qualificati a livello internazionale, riferenziate di seguito. Diversamente dalle altre sezioni dell'Operational Summary, basate su dati del CSIRT Italia ricavati nell'ambito delle attività di risposta agli incidenti e di monitoraggio proattivo, i contenuti del presente capitolo **non sono riconducibili a evidenze derivanti dalla gestione di incidenti o da attività operative svolte da ACN.**

Il presente capitolo sintetizza le principali **vulnerabilità, modalità operative e attività cyber** documentate dalle fonti aperte nel mese in esame. Approfondisce inoltre alcuni casi di impiego dell'**intelligenza artificiale** nelle attività cyber e alcuni sviluppi della minaccia connessi al **contesto geopolitico**.

## 6.1 Vulnerabilità e modalità operative

L'analisi delle principali fonti aperte istituzionali e di settore evidenzia, nel mese in esame, casi rilevanti di **sfruttamento di vulnerabilità**, in particolare negli **apparati per l'accesso remoto** e nelle **piattaforme di sviluppo software**, nonché **compromissioni** di account di servizi cloud e **esfiltrazioni di dati** da amministrazioni pubbliche. Alert pubblici di FBI, CISA e del Canadian Centre for Cyber Security hanno richiamato, inoltre, i rischi connessi ai **fornitori e agli integratori di sistemi industriali**, nonché le attività malevole contro **dispositivi OT esposti su Internet**.

Per quanto riguarda lo **sfruttamento attivo di vulnerabilità**, di rilievo quelle in **apparati perimetrali**, in particolare in soluzioni per l'accesso remoto e la gestione del traffico verso le applicazioni aziendali, oggetto anche di specifici bollettini del **CSIRT Italia**, di altre autorità competenti e dei produttori interessati. In particolare, il 2 settembre il **CSIRT Italia** ha segnalato lo sfruttamento di due vulnerabilità (CVE-2026-83548 e CVE-2026-83549) nei dispositivi **SonicWall SMA1000**[1]. Le vulnerabilità possono consentire, rispettivamente, di **raggiungere senza autenticazione funzionalità riservate** e, disponendo di privilegi amministrativi, di **eseguire comandi sul dispositivo**.

Ulteriori casi sono quelli che hanno interessato **F5 BIG-IP APM** e **NetScaler Gateway**, utilizzati per l'accesso remoto ai servizi aziendali, e **NetScaler ADC**, che gestisce il traffico verso le applicazioni. Il bollettino pubblicato il 22 settembre dal **CERT-EU**[2] riferisce che **F5 ha confermato lo sfruttamento attivo** della vulnerabilità in BIG-IP APM; il bollettino pubblicato da **Citrix** il 27 settembre[3] segnala invece lo **sfruttamento di vulnerabilità in installazioni NetScaler non ancora mitigate**.

Di rilievo, altresì, la vulnerabilità CVE-2026-85706, corretta il 10 settembre da **GitLab**[4], che, in determinate condizioni, permetteva di **leggere file sul server senza credenziali** e per la quale l'11 settembre **CISA**, agenzia statunitense per la cybersicurezza, ne ha attestato lo **sfruttamento attivo**[5].

Sul fronte dei **rischi della supply chain**, il 23 settembre **FBI** e **CISA** hanno richiamato quelli derivanti da fornitori che installano e gestiscono i **sistemi di controllo degli impianti industriali**[6] approfondendo la **compromissione**, avvenuta nel 2025, di una società statunitense di automazione industriale e sottolineando la necessità di proteggere le **informazioni tecniche dei clienti** e le **credenziali utilizzate dai fornitori** per accedere ai sistemi delle aziende clienti. Anche il **Canadian Centre for Cyber Security (CCCS)**, l'autorità tecnica canadese per la cybersicurezza, ha richiamato i rischi per i **sistemi di controllo degli impianti industriali**. Nell'avviso[7] il CCCS evidenzia che le connessioni Internet predisposte per **consentire ai fornitori di effettuare la manutenzione a distanza** possono esporre i dispositivi di controllo degli impianti ad **accessi non autorizzati**, anche quando questi sono separati dalla rete informatica aziendale. Il documento segnala inoltre evidenze di **impiego dell'IA per sviluppare software malevolo destinato a compromettere tali dispositivi**.

Di rilievo nel mese anche quanto descritto da **Microsoft** il 9 settembre[8] relativo a una **campagna di ingegneria sociale** finalizzata alla **compromissione di account di servizi cloud**. Soggetti presentatisi come addetti all'assistenza informatica inducevano gli utenti a effettuare operazioni apparentemente necessarie per configurare **passkey**, **autenticazione multifattore** o **accesso singolo**. Attraverso **tecniche di phishing** e l'**abuso dei flussi di autenticazione**, gli attaccanti ottenevano l'accesso agli account e lo utilizzavano per raccogliere documenti e messaggi di posta.

Per quanto riguarda il **contrasto al cybercrime**, il Dipartimento di Giustizia statunitense ha annunciato il 1° settembre un'operazione internazionale contro **Salinity**[9], una **rete di dispositivi compromessi** utilizzata per distribuire malware e condurre attività illecite. Nell'ambito dell'operazione, le autorità statunitensi ed europee hanno **sequestrato domini** collegati a Salinity, mentre i partner tecnologici hanno contribuito al **reindirizzamento delle comunicazioni della botnet** verso infrastrutture controllate e all'individuazione dei dispositivi infetti.

Il 22 settembre **Microsoft** ha annunciato un'operazione coordinata contro **EvilTokens**[10], piattaforma che forniva strumenti per **compromettere caselle di posta attraverso campagne di phishing** e impiegava l'IA per analizzarne i contenuti, individuare conversazioni relative ai pagamenti e predisporre **frodi mediante l'impersonificazione di interlocutori ritenuti affidabili**. Insieme a **Health-ISAC**, Microsoft ha promosso un'azione civile che, con l'autorizzazione della **U.S. District Court for the Eastern District of Virginia** e la collaborazione di Cloudflare, Coinbase, OpenAI, Railway, SpyCloud, The Shadowserver Foundation e TRM Labs, ha portato al **sequestro di 50 siti** utilizzati per gestire il servizio di cybercrime e alla **disabilitazione di oltre 150 domini** collegati alla sua infrastruttura. Microsoft collega all'attività della piattaforma la **compromissione di oltre 12.000 caselle di posta** appartenenti a più di 10.000 organizzazioni a livello globale[11].

In Francia, **ANSSI**, l'Agenzia nazionale per la sicurezza dei sistemi informativi, ha pubblicato il 30 settembre il bilancio dell'operazione **REACTIV**[12], avviata per rafforzare la risposta alle **violazioni di dati nelle amministrazioni statali**. Il documento riporta **67 incidenti di sicurezza confermati a fronte di 99 eventi di sicurezza** portati a conoscenza dell'Agenzia dal 1° agosto, nell'ambito di accertamenti ancora in corso. Tra le modalità di intrusione osservate figurano lo **sfruttamento di vulnerabilità** delle applicazioni e l'accesso ai servizi mediante **credenziali precedentemente**

**sottratte.** Per le compromissioni degli account, ANSSI evidenzia il ruolo dell'**assenza dell'autenticazione multifattore** o dell'impiego di un secondo fattore non adeguatamente protetto.

Sempre in tema di danni alle pubbliche amministrazioni, il 21 settembre **GreyNoise**, società statunitense specializzata nell'analisi delle attività malevole su Internet, ha pubblicato la propria ricostruzione di una campagna[13] nell'ambito della quale, nel mese di luglio, sarebbe avvenuta la **sottrazione di oltre 18.000 record dal database di un'organizzazione governativa occidentale** attraverso lo **sfruttamento di vulnerabilità** in un'installazione **WordPress**.

In Germania, inoltre, il gruppo ransomware **Rhysida** ha rivendicato l'attacco alla rete informatica del **Land di Berlino**, che ha coinvolto i dipartimenti competenti per trasporti e ambiente e per sviluppo urbano e politiche abitative. L'intrusione, avvenuta in agosto, ha consentito la **sottrazione di dati** ed è stata seguita da **richieste estorsive**. Nel comunicato del 3 settembre[14], le autorità del Land di Berlino hanno riferito che il gruppo dichiarava di possedere **5,7 terabyte di dati**, offerti all'asta con una base di 30 bitcoin, pari a circa due milioni di euro. Nel comunicato del 4 settembre[15], le stesse autorità hanno confermato la **pubblicazione dei dati sottratti**, mentre proseguivano gli accertamenti sul possibile coinvolgimento di dati personali di dipendenti, cittadini e imprese.

## 6.2 Intelligenza artificiale

Anche a settembre sono emerse evidenze dell'**impiego dell'intelligenza artificiale a supporto di attività cyber offensive** e, in ambito sperimentale, casi nei quali **agenti di IA hanno eseguito azioni non autorizzate**.

Il 22 settembre **ThreatDown**, società statunitense specializzata nella cybersicurezza, ha pubblicato un'analisi su **CARBONATO**[16], una **botnet** che comprometteva sistemi con **interfacce Docker esposte su Internet senza autenticazione** e si propagava verso altri sistemi. Sui dispositivi compromessi veniva installato **Hermes Agent**, framework open source per agenti di intelligenza artificiale, modificato per **mantenere la persistenza**, ricevere attraverso Telegram i compiti assegnati dagli operatori ed **eseguire comandi sul sistema**. L'agente era inoltre configurato per **ricercare credenziali**, assegnando priorità alle **chiavi API dei servizi di intelligenza artificiale** rispetto a credenziali SSH, token di accesso e credenziali per database.

L'8 settembre **NSA, FBI e CISA** hanno pubblicato un avviso congiunto[17] sulle campagne di **distillazione**<sup>17</sup> che dette agenzie attribuiscono alle società cinesi DeepSeek, Moonshot AI, Alibaba, MiniMax, StepFun e Z.AI. Secondo l'avviso, almeno dalla fine del 2024 tali società avrebbero raccolto **miliardi di token attraverso milioni di richieste** rivolte a modelli statunitensi, tra cui varianti di Claude, GPT, Gemini e Grok, per riprodurre **capacità di ragionamento, sviluppo del codice e funzionamento autonomo** nei propri sistemi. Le operazioni sarebbero state inoltrate attraverso molteplici canali, tra cui le API di diversi produttori di modelli, piattaforme cloud, aggregatori di API e servizi proxy, anche per **aggirare le restrizioni geografiche, eludere i controlli e ostacolare la ricostruzione complessiva delle attività**.

Un'ulteriore evidenza del possibile **impiego operativo di agenti di IA** emerge dall'analisi pubblicata il 1° ottobre da **urlscan**[18], servizio online che consente di analizzare le pagine web e registrarne le connessioni e i contenuti. L'approfondimento riconduce, con **confidenza moderata**, **3.553 scansioni** effettuate tra il 16 e il 19 giugno a un insieme coordinato di agenti automatizzati di IA. Secondo i ricercatori, gli agenti avrebbero utilizzato urlscan e altri servizi esterni per **aggirare le limitazioni dei propri ambienti di esecuzione** e interrogare portali governativi pubblici in Australia e India. Le scansioni erano state inviate attraverso **15 chiavi API di urlscan**, nove associate ad account creati per l'operazione e sei appartenenti a clienti legittimi, verosimilmente utilizzate a loro insaputa.

<sup>17</sup>Tecnica che consente di addestrare un modello di IA utilizzando le risposte prodotte da un altro modello, al fine di riprodurre parte delle conoscenze o delle capacità.

Per quanto riguarda i comportamenti osservati in ambito sperimentale, il 28 settembre l'**AI Security Institute britannico (AISi)** ha pubblicato i risultati di una valutazione di **GPT-6 Astra**[19], condotta in un ambiente interamente simulato e con i **sistemi di protezione del modello contro gli usi cyber malevoli disattivati**. Nel corso delle prove, il **modello ha preso di mira progetti software open source non inclusi nel perimetro della valutazione**, producendo **codice malevolo** e tentando di farlo integrare nei progetti mediante **identità fittizie**.

Per quanto attiene ai modelli **open-weight**, ovvero quelli i cui pesi sono resi disponibili per consentirne il download e l'esecuzione su infrastrutture proprie, il 17 settembre il **Center for AI Standards and Innovation (CAISI) del NIST statunitense** ha pubblicato una valutazione delle capacità cyber di **GLM-5.3**[20], modello sviluppato dalla società cinese Z.ai. Nelle prove dedicate all'**individuazione e allo sfruttamento di vulnerabilità**, GLM-5.3 è risultato il **modello open-weight con le maggiori capacità cyber** tra quelli esaminati dal CAISI. Il centro ha tuttavia valutato che le sue prestazioni aggregate fossero ancora significativamente inferiori a quelle dei più avanzati modelli statunitensi già rilasciati, con un divario stimato in circa quattro mesi di sviluppo. Il 29 settembre **Anthropic** ha pubblicato una propria valutazione[21], nella quale ha riferito che GLM-5.3 era in grado di **sviluppare autonomamente exploit completi** e che le sue **protezioni contro le richieste malevole potevano essere aggirate**, nelle simulazioni condotte dalla società, nel **64–100% dei casi**, a seconda della tecnica utilizzata.

### 6.3 Contesto geopolitico

Le fonti istituzionali e di settore pubblicate a settembre riportano attività di **spionaggio informatico, sorveglianza e manipolazione dell'informazione** attribuite, con differenti livelli di confidenza, ad attori riconducibili a Iran, Russia, Corea del Nord e Cina.

Il 15 settembre il **NCSC**<sup>18</sup>, l'**FBI** e l'**AIVD**, Servizio generale di intelligence e sicurezza dei Paesi Bassi, hanno pubblicato un avviso congiunto[22] su una **campagna di spionaggio e sorveglianza digitale** attribuita ad attori statali **iraniani**, rivolta almeno dal 2025 contro dissidenti, attivisti e giornalisti in diversi Paesi. Gli attaccanti contattavano le vittime attraverso applicazioni di messaggistica, tra cui WhatsApp e Telegram, presentandosi come persone da loro conosciute o addetti all'assistenza tecnica e adattando l'approccio in base alle informazioni raccolte preventivamente sul bersaglio. Dopo aver instaurato un rapporto di fiducia, inducevano le vittime ad aprire file apparentemente legittimi contenenti **CHOSEN BRICK**, malware per il sistema operativo Microsoft Windows. Il malware consentiva di **acquisire contatti, messaggi di posta elettronica e comunicazioni sui social media, catturare immagini dello schermo e registrare contenuti audio attraverso il microfono**, fornendo informazioni utilizzabili anche per ricostruire gli spostamenti delle persone colpite. Secondo l'avviso, i dati personali di alcune precedenti vittime sono successivamente comparsi su **siti di divulgazione filoiraniani**.

Il 29 settembre **Microsoft** ha riportato campagne di **spionaggio informatico** attribuite a **Star Blizzard**[23], attore statale russo che CISA riconduce al Centro 18 del Servizio federale di sicurezza russo (FSB). Le attività osservate da Microsoft a partire da gennaio 2026 hanno interessato individui e istituzioni ucraine, organizzazioni non governative internazionali, centri di ricerca, amministrazioni pubbliche e organizzazioni finanziarie, con particolare attenzione ai soggetti impegnati nel sostegno politico o finanziario all'Ucraina. Gli attaccanti inviavano **messaggi di phishing** che simulavano, tra l'altro, inviti a conferenze e incontri riservati organizzati da enti riconosciuti. Quando il destinatario rispondeva, riceveva un secondo messaggio contenente un **archivio RAR o ZIP protetto da password**, predisposto per avviare la catena di infezione denominata **RedFlick**. Dopo l'apertura dei file, venivano pianificate attività nel sistema,

<sup>18</sup>National Cyber Security Centre, centro nazionale per la cybersicurezza del Regno Unito, parte del Government Communications Headquarters (GCHQ).

utilizzate per acquisire informazioni di base sul dispositivo compromesso e successivamente scaricare ed eseguire **CosmicPulse**, una **backdoor** che consentiva agli attaccanti di **mantenere l'accesso al sistema**.

**Anthropic**, nel suo rapporto di settembre[24] ha descritto attività di **spionaggio informatico** condotte contro organizzazioni governative, diplomatiche, militari e della difesa, concentrate soprattutto in Ucraina e in Europa. La società identifica l'attore con la sigla **GTG-20006** e valuta le sue modalità operative e la selezione degli obiettivi coerenti con precedenti fonti pubbliche che collegano l'attività a **Midnight Blizzard**. Secondo Anthropic, l'arsenale dell'attore comprendeva **malware destinati a sistemi Windows, Android e iOS, strumenti per la sottrazione di credenziali** e una **piattaforma per la conduzione di campagne di phishing e la gestione degli account compromessi**. Claude sarebbe stato impiegato per **automatizzare la ricognizione**, predisporre e gestire l'infrastruttura di phishing, **eseguire comandi sui sistemi compromessi, raccogliere ed esfiltrare dati e modificare il malware quando rilevato dai prodotti di sicurezza**. Lo stesso rapporto descrive un'operazione di **manipolazione dell'informazione** nella **Repubblica Centrafricana**, che Anthropic valuta allineata agli interessi dello Stato russo. Secondo la società, un operatore russofono attivo a Bangui utilizzava Claude per produrre briefing, copioni radiofonici, immagini e contenuti per i social media, incorporando **messaggi favorevoli alla Russia e al gruppo Wagner e contrari alla Francia e all'opposizione centrafricana**. I contenuti venivano trasmessi quotidianamente da **Radio Lengo Songo**, emittente radio con sede a Bangui, amplificati attraverso canali Telegram e testate locali e coordinati con RT, Sputnik Afrique, TASS e la sede locale della Russian House. Anthropic riconduce l'operatore a **Politology**, struttura di influenza collegata ad Africa Corps e Wagner che la società valuta passata sotto il controllo del Servizio di intelligence estero russo (SVR) alla fine del 2023.

Per quanto riguarda le attività legate alla **Corea del Nord**, il 18 settembre autorità di Giappone, Stati Uniti, Australia e Germania hanno pubblicato un avviso congiunto sulle operazioni del gruppo **WaterPlum**, noto anche come **Contagious Interview**, contro sviluppatori e altri professionisti del settore informatico, anche in Europa. Gli attori si presentavano come potenziali datori di lavoro, talvolta impersonando società attive nei settori dell'intelligenza artificiale, delle criptovalute e degli NFT, e chiedevano ai candidati di partecipare a colloqui tecnici o svolgere prove di programmazione sui propri computer. I file e i progetti forniti per le prove contenevano pacchetti NPM o configurazioni di Visual Studio Code malevoli, utilizzati per installare software destinato a mantenere l'accesso ai dispositivi, sottrarre credenziali, dati personali e informazioni relative ai portafogli di criptovalute e consentire ulteriori attività nei sistemi delle organizzazioni per le quali lavoravano le vittime. La polizia giapponese e l'FBI valutano che sia gli operatori di WaterPlum sia alcuni cittadini nordcoreani impiegati da remoto nel settore informatico per generare entrate destinate al regime operino alle dipendenze del **313° Ufficio generale del Dipartimento dell'industria delle munizioni**, struttura subordinata al Comitato centrale del Partito dei lavoratori di Corea[25].

Nelle analisi pubblicate il 9 e il 21 settembre[26, 27], Volexity, società statunitense specializzata nell'analisi delle minacce informatiche e nella risposta agli incidenti, ha riferito di campagne attribuite a diversi gruppi collegati alla **Cina**, tra cui **UTA0560** e **JungleBamboo**, noto anche come **APT31**. Gli attaccanti inviavano **email di phishing** che inducevano i destinatari ad aprire pagine web predisposte per sfruttare una **combinazione di vulnerabilità di Chrome e Windows**<sup>19</sup>. L'attacco permetteva di **superare le protezioni che separano i contenuti web dal resto del computer** e di **installare programmi malevoli sul dispositivo**.

<sup>19</sup>CVE-2026-85046 e CVE-2026-87491 in Chrome, insieme a CVE-2026-85880 in Windows.

## Riferimenti

- [1] CSIRT Italia. *SonicWall: rilevato sfruttamento in rete delle CVE-2026-83548 e CVE-2026-83549 (AL06/260902/CSIRT-ITA)*. 2 Set. 2026. URL: <https://www.acn.gov.it/portale/w/sonicwall-rilevato-sfruttamento-in-rete-delle-cve-2026-83548-e-cve-2026-83549>.
- [2] CERT-EU. *Critical Vulnerability in F5 BIG-IP APM*. 22 Set. 2026. URL: <https://www.cert.europa.eu/publications/security-advisories/2026-013/>.
- [3] Citrix / Cloud Software Group. *Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin for CVE-2026-88771 through CVE-2026-88778*. 27 Set. 2026. URL: <https://support.citrix.com/external/article?articleNumber=CTX697096>.
- [4] GitLab. *GitLab Critical Patch Release: 19.3.2, 19.2.6, 19.1.8*. 10 Set. 2026. URL: <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/>.
- [5] Cybersecurity and Infrastructure Security Agency (CISA). *Known Exploited Vulnerabilities Catalog: CVE-2026-85706*. 11 Set. 2026. URL: [https://raw.githubusercontent.com/cisagov/kev-data/main/known\\_exploited\\_vulnerabilities.json](https://raw.githubusercontent.com/cisagov/kev-data/main/known_exploited_vulnerabilities.json).
- [6] Federal Bureau of Investigation e Cybersecurity and Infrastructure Security Agency. *Considerations for Critical Infrastructure Operators Working With Third-Party ICS Integrators*. Cybersecurity Advisory. Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency, 23 set. 2026. URL: <https://www.ic3.gov/CSA/2026/260923.pdf>.
- [7] Canadian Centre for Cyber Security. *Cyber Threat Actors Use Artificial Intelligence in an Active Global Campaign to Disrupt Internet-Exposed Programmable Logic Controllers*. 14 Set. 2026. URL: <https://www.cyber.gc.ca/en/news-events/cyber-threat-actors-use-artificial-intelligence-active-global-campaign-disrupt-internet-exposed-programmable-logic-controllers>.
- [8] Microsoft Security Research. *Passkey-Themed Social Engineering Leads to Identity and Cloud Compromise*. 9 Set. 2026. URL: <https://www.microsoft.com/en-us/security/blog/2026/09/09/passkey-themed-social-engineering-leads-identity-cloud-compromise/>.
- [9] U.S. Attorney's Office, Central District of California. *Salinity Malware Disrupted in International Cyber Takedown*. Comunicato del Dipartimento di Giustizia statunitense, Press Release No. 26-149. 1 Set. 2026. URL: <https://www.justice.gov/usao-cdca/pr/salinity-malware-disrupted-international-cyber-takedown>.
- [10] Microsoft Digital Crimes Unit. *Disrupting EvilTokens: The AI Chatbot Built for Cybercrime*. Fonte relativa all'azione civile e all'operazione coordinata contro l'infrastruttura di EvilTokens. 22 Set. 2026. URL: <https://blogs.microsoft.com/on-the-issues/2026/09/22/disrupting-eviltokens-the-ai-chatbot-built-for-cybercrime/>.
- [11] Microsoft Threat Intelligence, Microsoft Defender Experts e Microsoft Security Research. *Unmasking EvilTokens: Getting to the Root of Device Code Phishing*. Analisi tecnica della piattaforma EvilTokens, delle campagne di device-code phishing e delle attività successive alla compromissione. 22 Set. 2026. URL: <https://www.microsoft.com/en-us/security/blog/2026/09/22/unmasking-eviltokens-getting-to-the-root-of-device-code-phishing/>.
- [12] Agence nationale de la sécurité des systèmes d'information (ANSSI). *Point de situation de l'opération REACTIV – septembre 2026*. Rapport de cybermenace CERTFR-2026-CTI-006. CERT-FR, 30 set. 2026. URL: <https://www.cert.ssi.gouv.fr/uploads/CERTFR-2026-CTI-006.pdf>.
- [13] Andrew Thompson e Mark Mager. *Open Season on Kapibala: Attacker Steals Over 18,000 Government Records Through WordPress Exploitation*. 21 Set. 2026. URL: <https://www.greynoise.io/blog/open-season-on-kapibala-attacker-steals-government-records-wordpress-exploitation>.
- [14] Senatskanzlei Berlin. *Aktuelle Lage nach dem IKT-Vorfall im Landesnetz Berlin*. 3 Set. 2026. URL: <https://www.berlin.de/rbmskzl/aktuelles/pressemitteilungen/2026/pressemitteilung.1710327.php>.
- [15] Senatskanzlei Berlin. *Aktuelle Lage nach dem IKT-Vorfall im Landesnetz Berlin und der Veröffentlichung der gestohlenen Daten*. 4 Set. 2026. URL: <https://www.berlin.de/rbmskzl/aktuelles/pressemitteilungen/2026/pressemitteilung.1710705.php>.
- [16] ThreatDown. *CARBONATO: A Botnet Built Around an AI Agent*. 22 Set. 2026. URL: <https://www.threatdown.com/blog/carbonato/>.
- [17] National Security Agency (NSA), Federal Bureau of Investigation (FBI) e Cybersecurity and Infrastructure Security Agency (CISA). *China-Based Artificial Intelligence Companies Conducting Industrial-Scale Distillation Campaigns Against U.S. AI Companies*. 8 Set. 2026. URL: <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4592113/nsa-and-others-warn-china-based-ai-companies-are-distilling-us-frontier-ai-mode/>.
- [18] urlscan Threat Research Team. *Intel Brief: Caught in the Crossfire – When an AI Agent Swarm Uses Your Infrastructure to Attack*. 1 Ott. 2026. URL: <https://urlscan.io/blog/2026/10/01/AiSwarmReport/>.

- [19] UK AI Security Institute (AISI). *GPT-6 Astra Performs Unsanctioned Supply-Chain Attacks in Simulations*. 28 Set. 2026. URL: <https://www.aisi.gov.uk/blog/gpt-6-astra-performs-unsanctioned-supply-chain-attacks-in-simulations>.
- [20] Center for AI Standards and Innovation (CAISI), National Institute of Standards and Technology (NIST). *CAISI's Assessment of Zai's GLM-5.3 Cyber Capabilities*. 17 Set. 2026. URL: <https://www.nist.gov/news-events/news/2026/09/caisis-assessment-zais-glm-53-cyber-capabilities>.
- [21] Anthropic. *GLM-5.3 and the Spread of Advanced Cyber Capabilities*. 29 Set. 2026. URL: <https://www.anthropic.com/research/glm-5-3-and-the-spread-of-advanced-cyber-capabilities>.
- [22] UK National Cyber Security Centre, Federal Bureau of Investigation e Algemene Inlichtingen- en Veiligheidsdienst. *Iranian Cyber Targeting of Dissidents, Activists and Journalists*. 15 Set. 2026. URL: <https://www.ncsc.gov.uk/sites/default/files/2026-09/Advisory-Iranian-Cyber-Targeting-of-Dissidents-Activists-and-journalists.pdf>.
- [23] Microsoft Threat Intelligence. *Star Blizzard Refines Phishing and Malware Delivery With the RedFlick Technique*. 29 Set. 2026. URL: <https://www.microsoft.com/en-us/security/blog/2026/09/29/star-blizzard-refines-phishing-and-malware-delivery-with-the-redflick-technique/>.
- [24] Anthropic. *Detecting and Countering Misuse of AI: September 2026*. Set. 2026. URL: <https://www.anthropic.com/threat-intelligence-report-september-2026>.
- [25] National Police Agency of Japan et al. *North Korean WaterPlum, Commonly Referred to as Contagious Interview, Cyber Actor Group Targeting IT Professionals; Activities of North Korean IT Workers in Japan, the United States and Europe*. Joint Cybersecurity Advisory. NPA, NCO, FBI, DC3, ASD's ACSC, BND and BfV, 18 set. 2026. URL: <https://www.ic3.gov/CSA/2026/260918.pdf>.
- [26] Volexity. *Mind the (Patch) Gap: Multiple Chinese Threat Actors Chain 0-Day Exploits in Chrome & Windows*. 9 Set. 2026. URL: <https://www.volexity.com/blog/2026/09/09/mind-the-patch-gap-multiple-chinese-threat-actors-chain-0-day-exploits-in-chrome-windows/>.
- [27] Volexity. *Mind the (Patch) Gap, Part 2: Fake Websites Used to Deploy Chrome & Windows 0-Day Exploits*. 21 Set. 2026. URL: <https://www.volexity.com/blog/2026/09/21/mind-the-patch-gap-part-2-fake-websites-used-to-deploy-chrome-windows-0-day-exploits/>.



**Agenzia per la  
Cybersicurezza Nazionale**



---

**OPERATIONAL SUMMARY**  
**settembre 2026**