Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

AGOSTO 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.

Sommario

pag.

Indice delle figure

pag.

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 agosto 2026 sono stati registrati **309 eventi**, sostanzialmente **allineati** (+1%) rispetto ai **305** di luglio. Anche gli **incidenti** sono risultati **stabili**: **185** rispetto ai **188** del mese precedente. In continuità con quanto già osservato a luglio, il monitoraggio proattivo dei sistemi esposti ha rilevato **defacement** su diverse decine di siti web riconducibili ad amministrazioni locali, enti di ricerca, università, organizzazioni associative e piccole imprese. Tali compromissioni – alterazione dei contenuti dei siti web, senza ripercussioni sull'operatività delle organizzazioni coinvolte o sulla continuità dei servizi erogati e senza rivendicazioni da parte degli attaccanti – sono state causate dallo sfruttamento di vulnerabilità presenti in plugin e altri componenti dei CMS[1]. Assume rilievo, in questo contesto, l'alert pubblicato dal **CSIRT Italia** il 21 agosto 2026 relativo allo sfruttamento attivo di una vulnerabilità critica nel plugin Pods per **WordPress**[2], effettivamente sfruttata in alcuni defacement osservati nel mese. Gli incidenti sono stati tempestivamente segnalati alle organizzazioni interessate.

  Complessivamente, nel corso del mese di agosto 2026, le principali minacce rilevate negli eventi sono state: **Esposizione dati**, **Defacement** e **Ransomware**. Il rilievo assunto dall'esposizione di

[1] I Content Management System (CMS) sono piattaforme software per la creazione e la gestione dei contenuti dei siti web.

[2] CSIRT Italia, WordPress: rilevato sfruttamento di vulnerabilità nel plugin Pods.

dati è prevalentemente riconducibile al rinvenimento di credenziali compromesse su piattaforme di scambio illecito, nonché alla pubblicazione di campioni di dati (data leak sample) da parte di gruppi ransomware, utilizzati sia quali elementi di prova dell'avvenuta compromissione sia come strumenti di pressione nell'ambito dell'attività di estorsione. Per quanto riguarda l'attività di defacement, l'incremento rispetto alla media degli ultimi sei mesi è riconducibile anche alla nuova capacità del CSIRT Italia di individuare tempestivamente questa tipologia di attività condotta in danno di siti web di soggetti italiani.

- **Settori interessati**
  I settori con il maggior numero di vittime di eventi cyber sono stati **Manifatturiero**, **Telecomunicazioni**, **Tecnologico**. Il settore Manifatturiero è stato interessato principalmente da ransomware, il settore Telecomunicazioni da compromissione delle caselle email, mentre il settore Tecnologico da sfruttamento vulnerabilità.

- **Ransomware**
  Nel mese di agosto 2026 si è registrato un aumento degli incidenti ransomware, presumibilmente ascrivibile alle campagne di sfruttamento di vulnerabilità registrate e oggetto di bollettino del CSIRT Italia[3]. Gli impatti confermati hanno riguardato l'indisponibilità di dati e sistemi, con rallentamenti o interruzioni delle attività amministrative, logistiche e produttive e, in alcuni casi, il coinvolgimento delle infrastrutture di backup. In diversi incidenti, alla cifratura dei sistemi si sono associate l'esfiltrazione dei dati e la minaccia di pubblicazione, secondo il modello della doppia estorsione. Tra gli eventi di maggiore rilievo figura un incidente associato al **gruppo Titan** che ha colpito un fornitore ICT. La cifratura di parte dei dati ospitati in un'area condivisa ha determinato impatti anche per le organizzazioni clienti che la utilizzavano. Gli attacchi ransomware hanno interessato prevalentemente i settori **Manifatturiero**, **Commercio all'ingrosso e al dettaglio** e **Altre società private**. L'analisi degli incidenti ransomware evidenzia come principali vettori di compromissione siano lo sfruttamento di vulnerabilità note e l'utilizzo di credenziali valide precedentemente compromesse. Per ogni rivendicazione rilevata, il CSIRT Italia ha contattato il soggetto interessato al fine di fornire supporto e indicare le misure di mitigazione.

- **Attacchi DDoS**
  Nel mese di agosto 2026 come già osservato a luglio, non sono state rilevate campagne DDoS di particolare rilevanza rivolte contro soggetti nazionali.

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

- **Vulnerabilità**
  Nel mese, il *Common Vulnerabilities and Exposures* (**CVE**) Program[4] ha pubblicato **12.719** nuovi record relativi a vulnerabilità di cybersicurezza, in **aumento** (**+2.800**) rispetto a luglio. Di questi, **288** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–36**), e per **13** CVE è stato rilevato lo sfruttamento attivo, **stabile** rispetto a luglio. 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.

[3] Bollettino del CSIRT Italia su Qilin https://www.acn.gov.it/portale/w/qilin-campagne-di-sfruttamento-sistematico-e-diffusione-del-ransomware-sul-territorio-nazionale.

[4] 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.

- **Monitoraggio proattivo e allertamento**
  L'attività di monitoraggio della superficie esposta ha consentito di individuare ad agosto 2026 **9.121 sistemi e servizi a rischio**, in sensibile **aumento** (+5.911) rispetto a luglio. Tale incremento è riconducibile principalmente all'elevato numero di servzi **cPanel**, piattaforma per l'amministrazione di server e servizi di hosting, risultati potenzialmente vulnerabili alla CVE-2026-65643 (alert del CSIRT Italia: AL09/260828/CSIRT-ITA) e oggetto di specifica attività di allertamento. L'analisi di dati provenienti da malware di tipo infostealer, altresì, ha consentito di identificare **10 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 **8.382**, **in diminuzione** (–570) rispetto a luglio.

I NUMERI - AGOSTO 2026

EVENTI, INCIDENTI E VITTIME	FEBBRAIO	MARZO	APRILE	MAGGIO	GIUGNO	LUGLIO	AGOSTO
Eventi cyber	435	434	266	389	421	305	309
Incidenti con impatto confermato	159	286	174	161	179	188	185
Vittime	497	546	346	462	496	354	367

MONITORAGGIO E ALLERTAMENTO	FEBBRAIO	MARZO	APRILE	MAGGIO	GIUGNO	LUGLIO	AGOSTO
Asset potenzialmente compromessi	51	54	126	73	1.244	1.095	572
Asset potenzialmente vulnerabili	1.095	3.339	2.212	11.984	4.236	3.210	9.121
Comunicazioni inviate	4.650	7.216	7.229	11.917	8.754	8.952	8.382
Alert sito web	87	98	101	115	128	106	143

Figura 1 - *indicatori delle attività operative ad agosto 2026 e nei sei mesi precedenti*

- **309** eventi cyber, **stabile** (+ **4**);
- **367** vittime[5], in **aumento** (**+13**);
- **185** vittime della constituency[6], in **diminuzione** (**–23**);
- **185** incidenti con impatto confermato, **stabile** (**–3**);
- **572** asset potenzialmente compromessi, in **diminuzione** (**–523**);
- **9.121** asset potenzialmente vulnerabili, in **aumento** (**+5.911**);
- **143** alert sul sito web del CSIRT Italia, in **aumento** (**+37**);
- **8.382** comunicazioni inviate complessivamente, in **diminuzione** (**–570**);
- **12.719** nuove CVE, in **aumento** (**+2.800**).

[5]Uno stesso soggetto è conteggiato più volte qualora sia stato coinvolto in eventi distinti.

[6]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 ad agosto 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.

- **Cisco** – Unified Computing System (Standalone) (CVE-2026-20200) Link all'alert; Secure Firewall Management Center (FMC) (CVE-2026-20316) Link all'alert
- **Citrix** – NetScaler ADC, NetScaler Gateway (CVE-2026-8452) Link all'alert; (CVE-2026-19490) Link all'alert
- **Django** (CVE-2026-15307) Link all'alert
- **Fortinet** – FortiWeb (CVE-2026-26035) Link all'alert
- **GeoServer** – GeoTools (CVE-2026-76904) Link all'alert
- **Gitea** – Gitea Open Source Git Server (CVE-2026-24791, CVE-2026-42931, CVE-2026-56657, CVE-2026-56755, CVE-2026-57897, CVE-2026-58510, CVE-2026-58511, CVE-2026-59763) Link all'alert; (CVE-2026-60004) Link all'alert
- **GitLab** (CVE-2026-19478) Link all'alert
- **IBM** – Langflow OSS (CVE-2026-12940) Link all'alert
- **Jenkins Project** – Jenkins, Remoting (CVE-2026-70426) Link all'alert
- **Metabase** (CVE-2026-72898, CVE-2026-72899) Link all'alert
- **Microsoft** – SharePoint Enterprise Server 2016, SharePoint Server 2019, SharePoint Server Subscription Edition (CVE-2026-63520) Link all'alert
- **N-able** – N-central (CVE-2026-18577) Link all'alert
- **pgAdmin** – pgAdmin 4 (CVE-2026-17351) Link all'alert
- **PostgreSQL** (CVE-2026-14669) Link all'alert
- **PTC** – FlexPLM, Windchill PDMLink (CVE-2026-12569) Link all'alert
- **Ruby on Rails** (CVE-2026-66066) Link all'alert
- **SAP** – NetWeaver e ABAP Platform (CVE-2026-34265) Link all'alert
- **Ubiquiti** – UniFi (Network, Access, Protect, Talk, Connect, OS Server, Enterprise A/V Bridge), Dream Machine/Router/Wall, Cloud Gateway, Cloud Key, EdgeMAX EdgeSwitch, Enterprise Firewall Core, Enterprise Fortress Gateway, Express, NAS, NVR, UID Enterprise Agent (CVE-2026-77532, CVE-2026-77533, CVE-2026-77534, CVE-2026-77535, CVE-2026-77536, CVE-2026-77537, CVE-2026-77538, CVE-2026-77539, CVE-2026-77540, CVE-2026-77541, CVE-2026-77542, CVE-2026-77543, CVE-2026-77545, CVE-2026-77546, CVE-2026-77547, CVE-2026-77548, CVE-2026-77549, CVE-2026-77550, CVE-2026-77551, CVE-2026-77552, CVE-2026-77553, CVE-2026-77554, CVE-2026-77557) Link all'alert
- **VMware** – Cloud Foundation, Telco Cloud Infrastructure, Telco Cloud Platform, vCenter, vSphere Foundation (CVE-2026-59309, CVE-2026-59310) Link all'alert
- **WebPros** – cPanel (CVE-2026-65643) Link all'alert
- **WordPress** (CVE-2026-64638) Link all'alert
- **Zimbra** – Zimbra Collaboration (CVE-2026-73570) Link all'alert

Maggiori dettagli nelle sezioni 3 e 5.

2 EVENTI ED INCIDENTI

Ad agosto 2026 sono stati individuati **309** eventi cyber, sostanzialmente **allineati** (+1%) rispetto a luglio. Questi ultimi hanno **interessato, in diversi casi più volte, 307 soggetti nazionali distinti** (di cui 185 appartenenti alla constituency, mentre i restanti hanno riguardato cittadini e società private operanti in settori non critici). Dei 309 eventi cyber, **185 sono stati classificati quali incidenti**, anch'essi **stabili** rispetto ai 188 di luglio.

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[7], riferita ai tre mesi successivi.

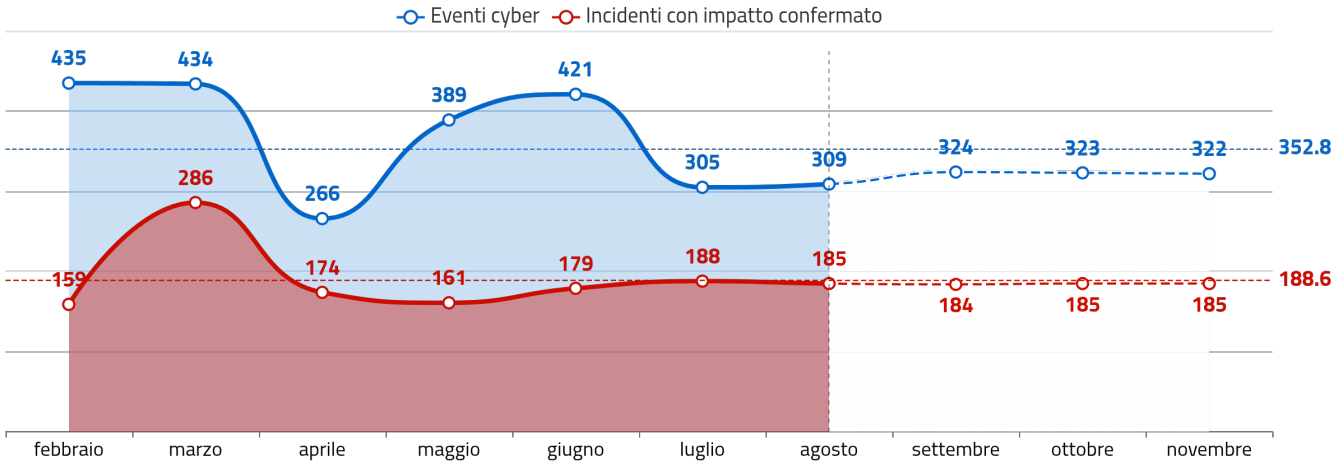

Figura 2 - *andamento attività reattive e analisi previsionale*

[7] 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[8]. Si evidenzia altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico la media di riferimento).

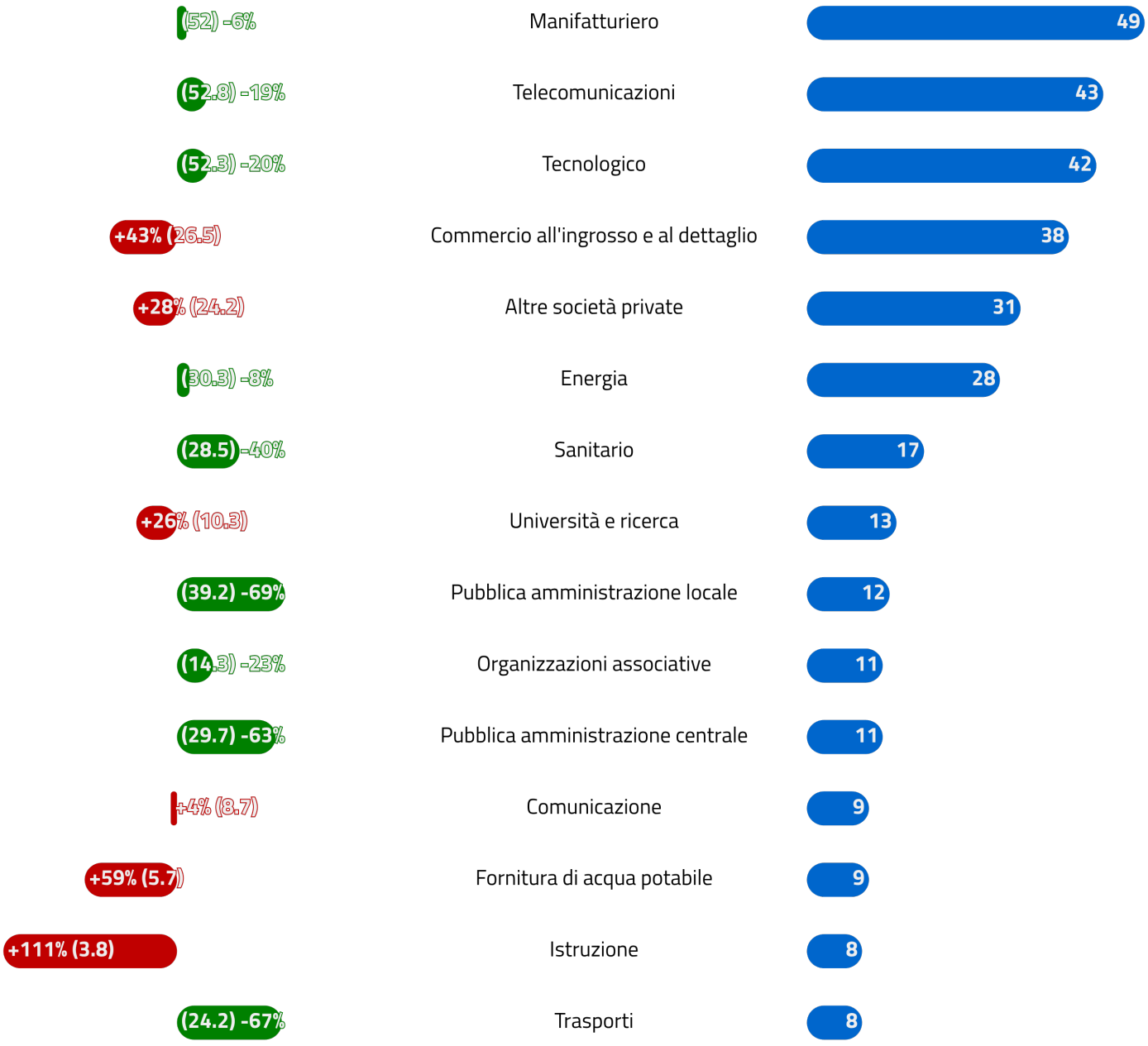

Figura 3 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente (top 15)*

[8] 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[9] 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).

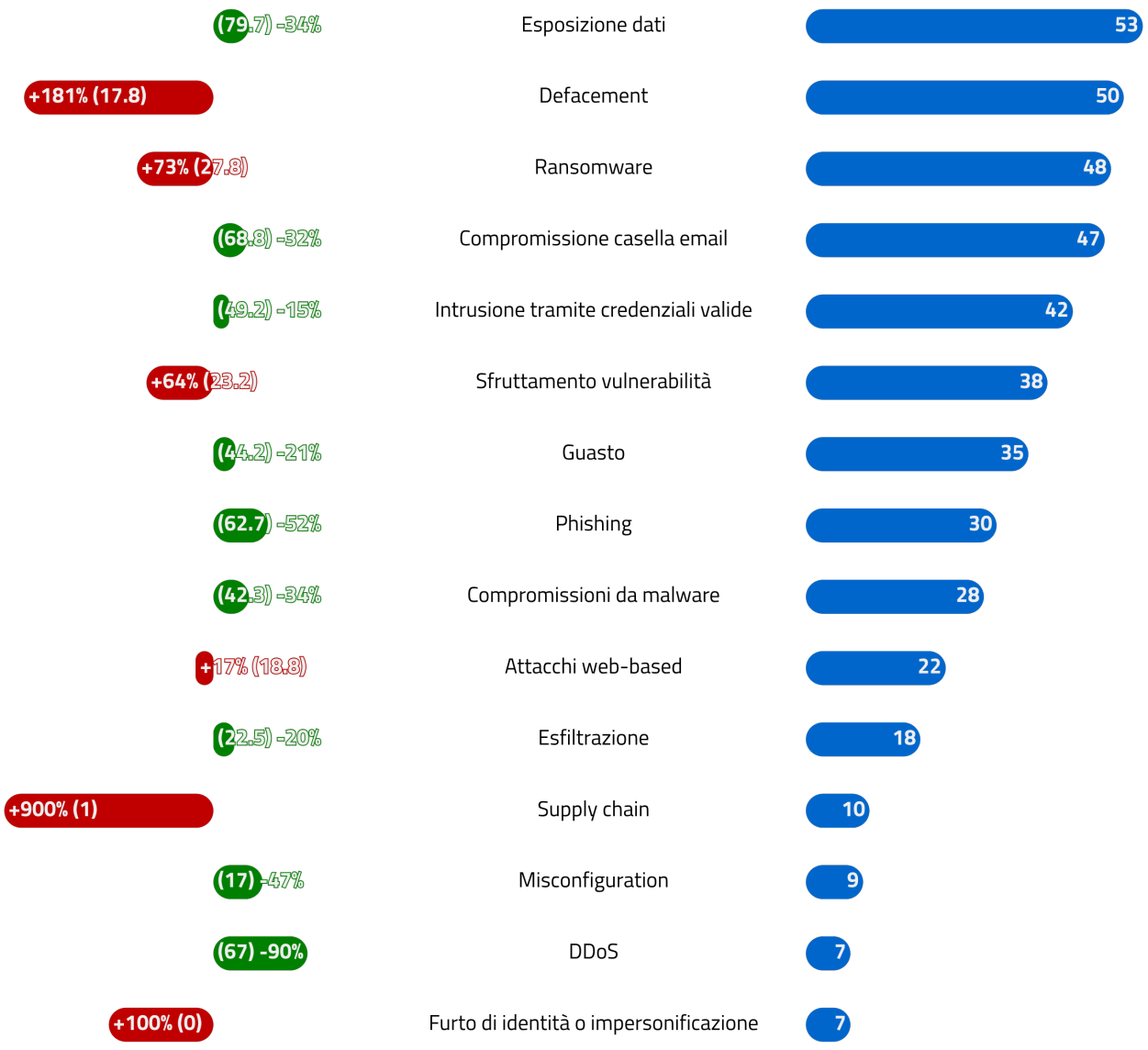

Figura 4 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente (top 15)*

[9] 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 agosto 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.

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

2.4 Distribuzione geografica delle vittime

I 309 eventi cyber hanno interessato **367** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

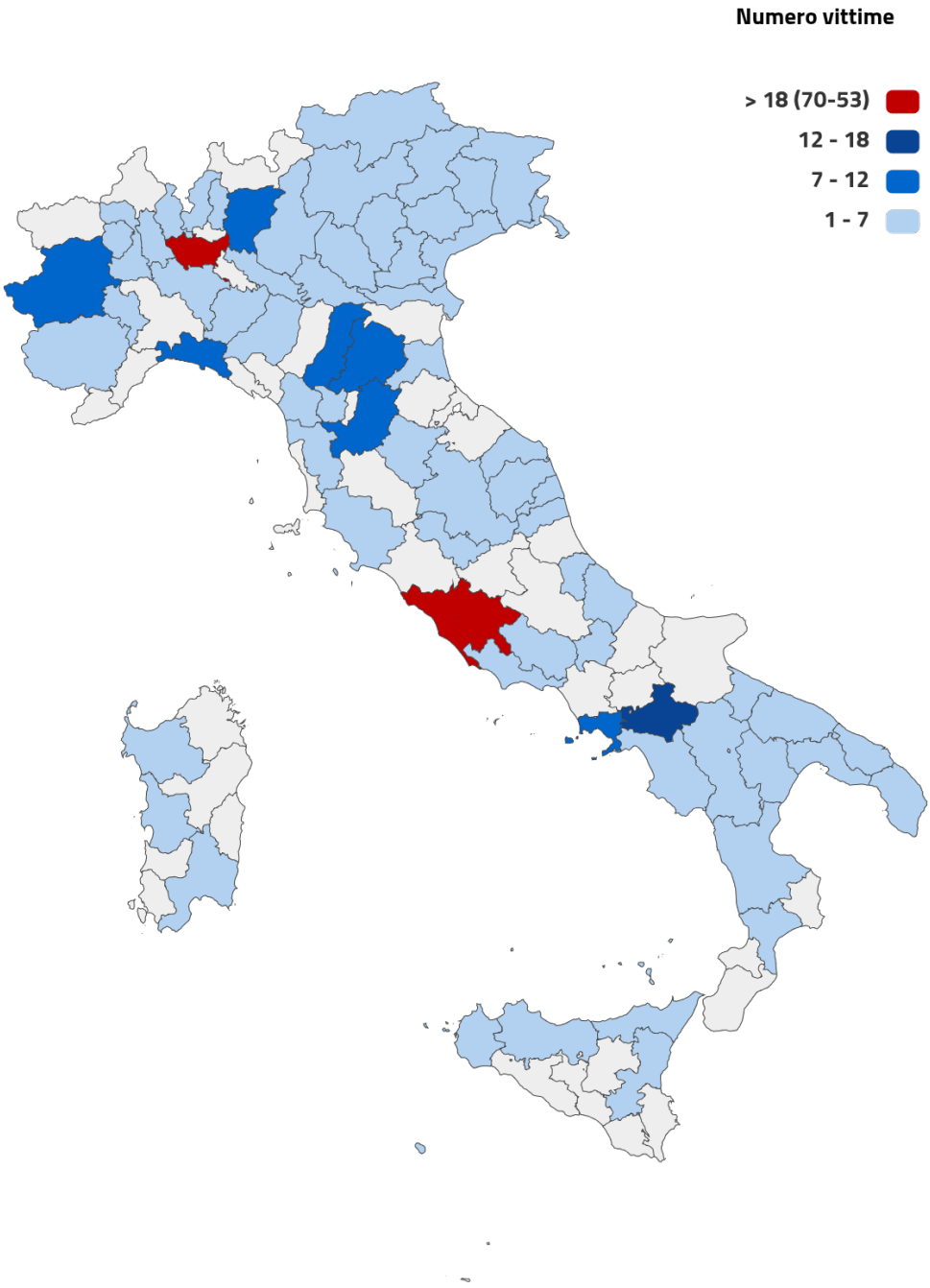

Figura 6 - *distribuzione delle vittime degli eventi cyber*

3 VULNERABILITÀ

Ad agosto 2026 sono state pubblicate[10] **12.719** nuove CVE, in **aumento** (**+2.800**) rispetto a luglio. Di queste, **288** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–36**), e per **13** CVE è stato rilevato lo sfruttamento attivo, **stabile** rispetto a luglio.

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 **143**. Le vulnerabilità particolarmente gravi, riportate di seguito ordinate per stima d'impatto sistemico[11], sono state quelle relative a prodotti di:

- **Metabase**: aggiornamenti di sicurezza sanano 2 vulnerabilità con gravità "critica" in Metabase, piattaforma open source di Business Intelligence (BI). Tra queste si evidenzia la CVE-2026-72898, che risulta sfruttata attivamente in rete. (stima di impatto sistemico **79.48/100**). Link all'alert del 11/08/2026;
- **SAP**: nell'ambito del Security Patch Day di agosto, SAP rilascia aggiornamenti di sicurezza per risolvere molteplici nuove vulnerabilità, di cui 2 con gravità "critica" e 6 con gravità "alta". (stima di impatto sistemico **79.48/100**). Link all'alert del 11/08/2026;
- **Adobe**: ha rilasciato aggiornamenti di sicurezza per risolvere molteplici vulnerabilità, di cui 7 con gravità "critica" e 27 con gravità "alta", nei prodotti Commerce, Magento, ColdFusion, Campaign Classic, Lightroom Classic, Content Credentials Rust SDK, C2PA Tool, Content Credentials JS SDK. (stima di impatto sistemico **79.48/100**). Link all'alert del 12/08/2026;

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

[11] 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.

- **Microsoft**: rilevato lo sfruttamento attivo in rete di una vulnerabilità con gravità "critica" - già sanata dal vendor - relativa a Microsoft Entra ID, servizio cloud di gestione delle identità e degli accessi. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente non autenticato di eseguire codice arbitrario sui dispositivi target. (stima di impatto sistemico **79.48/100**). Link all'alert del 21/08/2026;
- **Docker**: disponibile un Proof of Concept (PoC) per lo sfruttamento della vulnerabilità identificata dalla CVE-2026-17106, già sanata dal vendor, che interessa Docker Desktop, applicazione sviluppata da Docker Inc. che fornisce un ambiente completo per eseguire e gestire container Docker su Windows e macOS. (stima di impatto sistemico **79.23/100**). Link all'alert del 12/08/2026;

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[12].

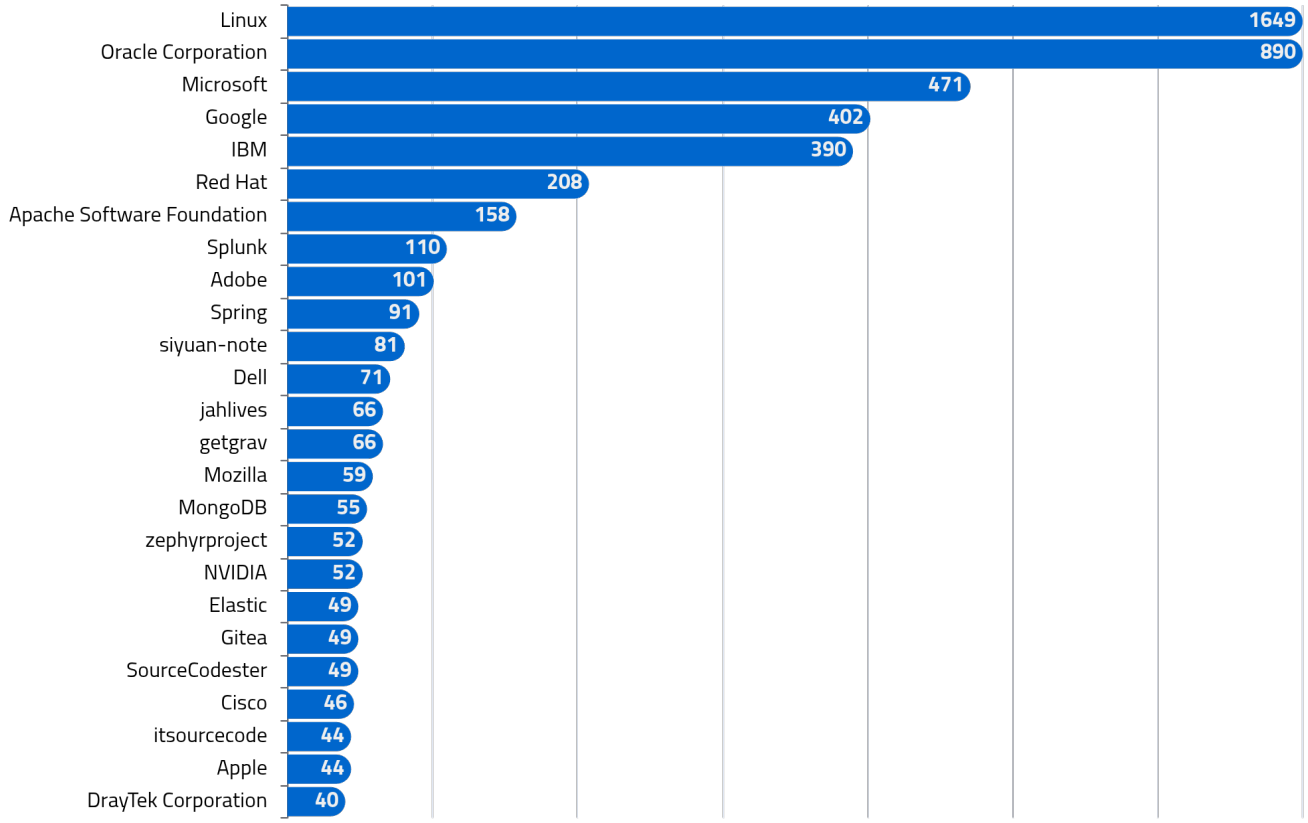

Figura 7 - *top 25 produttori affetti da vulnerabilità nel mese*

[12] 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.

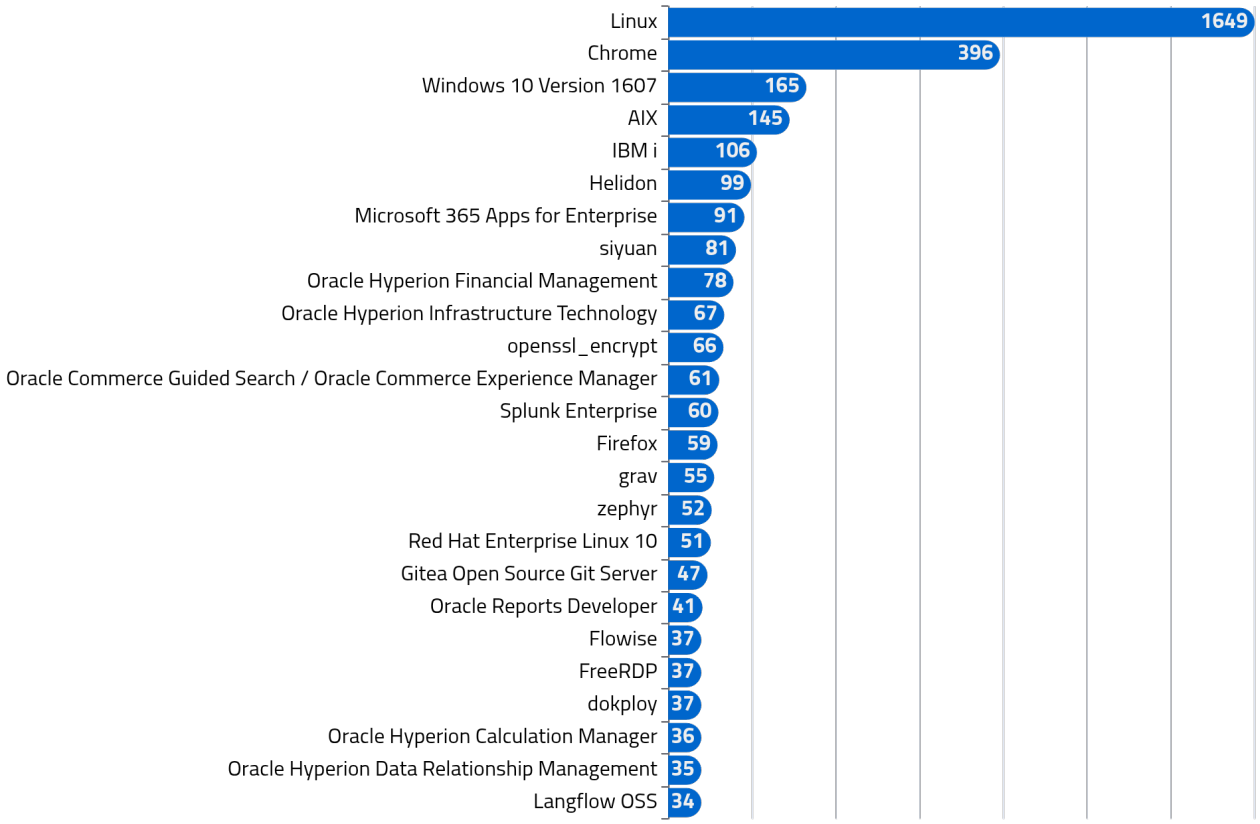

Figura 8 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

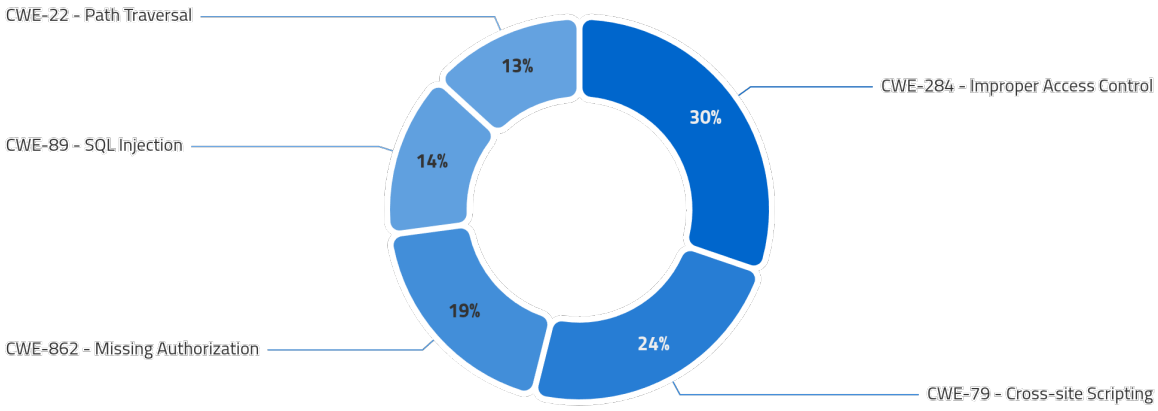

Figura 9 - *top 5 CWE nel mese*

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)[13] fornito dal FIRST, nel mese in esame.

Vendor	**Apache**
Prodotti e versioni vulnerabili	**Tomcat versioni 11.0.20, 10.1.53, 9.0.116**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice arbitrario da remoto.**
Data di rilascio CVE	**09/04/2026 modificata il 10/08/2026**
CVSS score 3.0	**7.5 High**
EPSS max score	**0.98**

Tabella 1 - *CVE-2026-34486*

Vendor	**Splunk**
Prodotti e versioni vulnerabili	**Splunk Enterprise versioni dalla 10.0 alla 10.0.6 e versioni dalla 10.2 fino alla 10.2.3**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice arbitrario da remoto.**
Data di rilascio CVE	**10/06/2026 modificata il 23/07/2026**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.96**

Tabella 2 - *CVE-2026-20253*

[13] 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.

Vendor	**JetBrains**
Prodotti e versioni vulnerabili	**TeamCity tutte le versioni fino alla 2025.11.5 e versioni dalla 2026.1 alla 2026.1.1**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice arbitrario da remoto.**
Data di rilascio CVE	**27/07/2026 modificata il 06/08/2026**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.87**

Tabella 3 - *CVE-2026-63077*

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[14] condivisi dal CSIRT Italia tramite piattaforma MISP[15], in modo da caratterizzarne le tipologie più frequenti.

4.1 Ransomware: distribuzione delle vittime

Ad agosto 2026, l'8% degli attacchi ransomware ha colpito soggetti critici, il 38% ha colpito soggetti a media criticità, ed il restante 54% ha coinvolto altri soggetti a criticità minore.

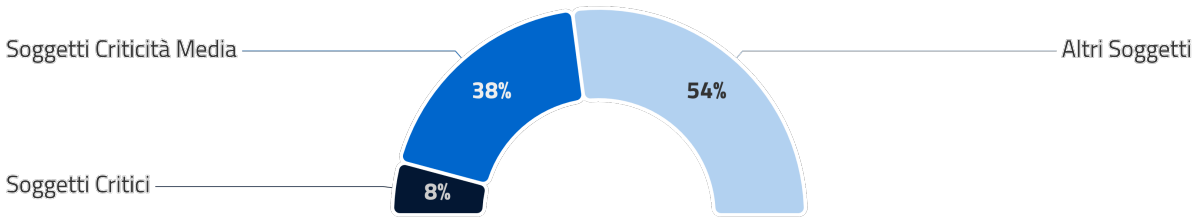

Figura 10 - *distribuzione delle vittime di ransomware in base alla loro criticità*

[14]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.

[15]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 agosto 2026 ha permesso di individuare **49** rivendicazioni di attacchi ransomware a danno di soggetti italiani[16].

Il grafico in Figura 11 mostra l'andamento delle rivendicazioni riferite all'Italia nel corso degli ultimi 12 mesi. Nell'ultimo mese si nota un picco di rivendicazioni, ascrivibile a delle campagne di sfruttamento di vulnerabilità già oggetto di un bollettino del CSIRT Italia, al quale si rimanda per approfondimenti[17].

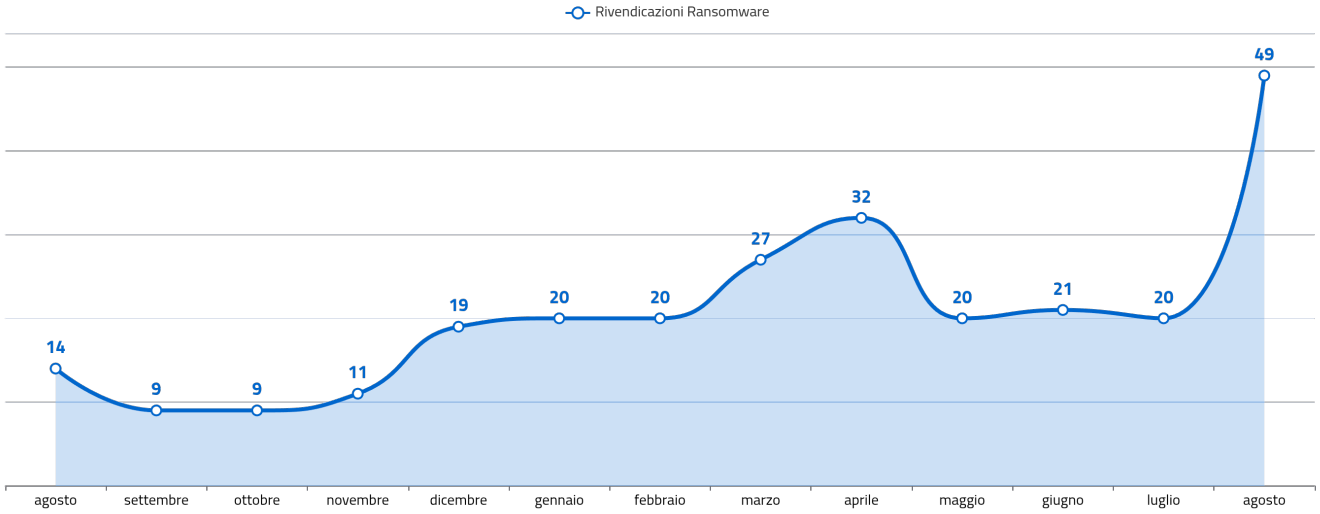

Figura 11 - *andamento delle rivendicazioni ransomware per l'Italia*

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

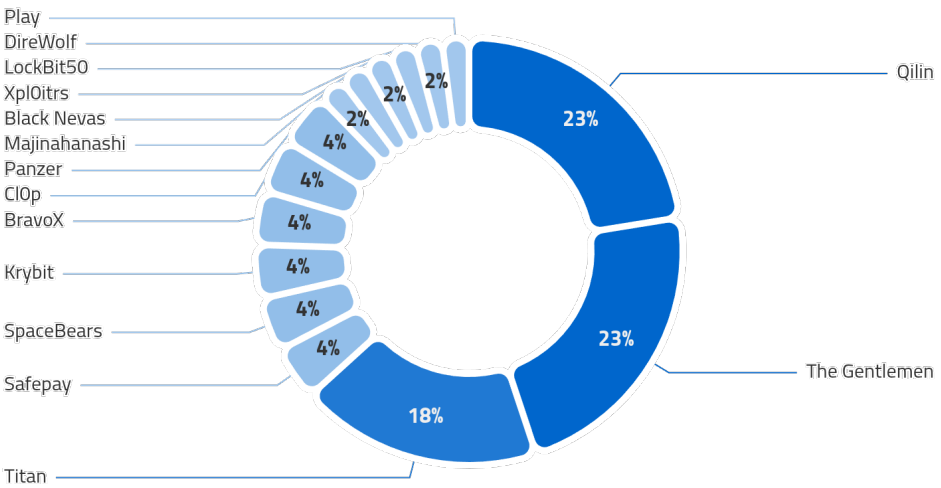

Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

[16] Talvolta, le rivendicazioni relative ad attacchi ransomware non sono confermate dal soggetto coinvolto.

[17] Bollettino del CSIRT Italia su Qilin: https://www.acn.gov.it/portale/w/qilin-campagne-di-sfruttamento-sistematico-e-diffusione-del-ransomware-sul-territorio-nazionale.

4.3 Rivendicazioni DDoS

Ad agosto 2026 non sono state individuate[18] 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.

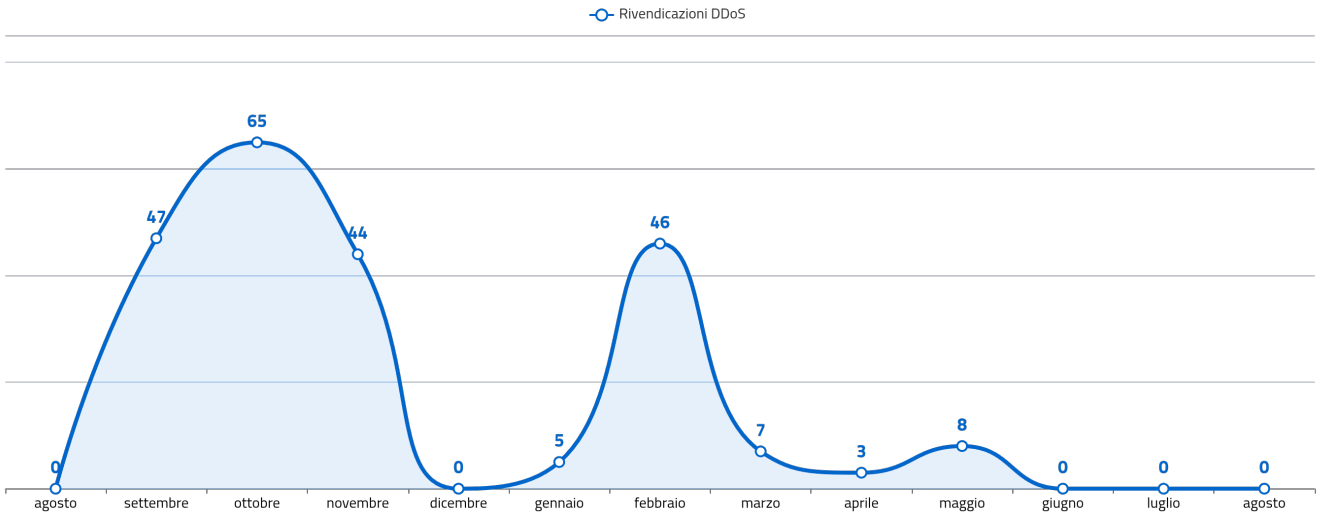

Figura 13 - *andamento delle rivendicazioni DDoS riferite all'Italia*

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

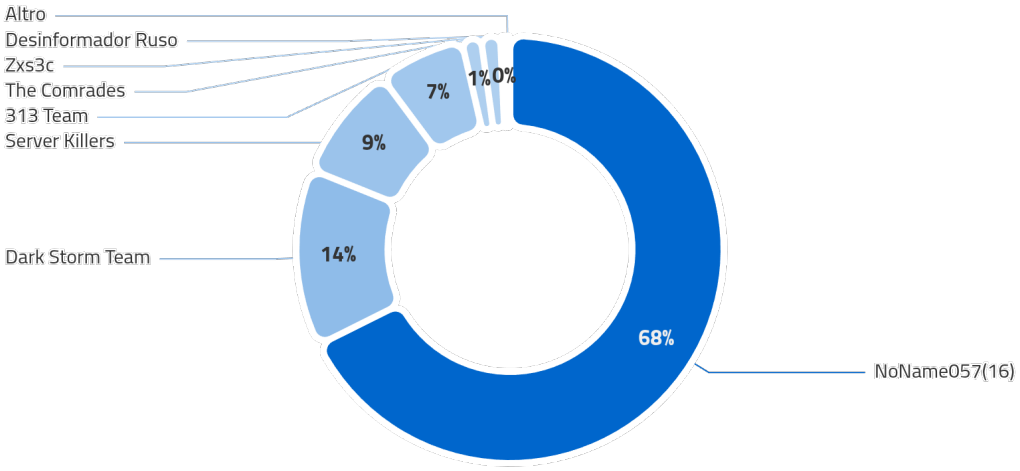

Figura 14 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

[18] 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.

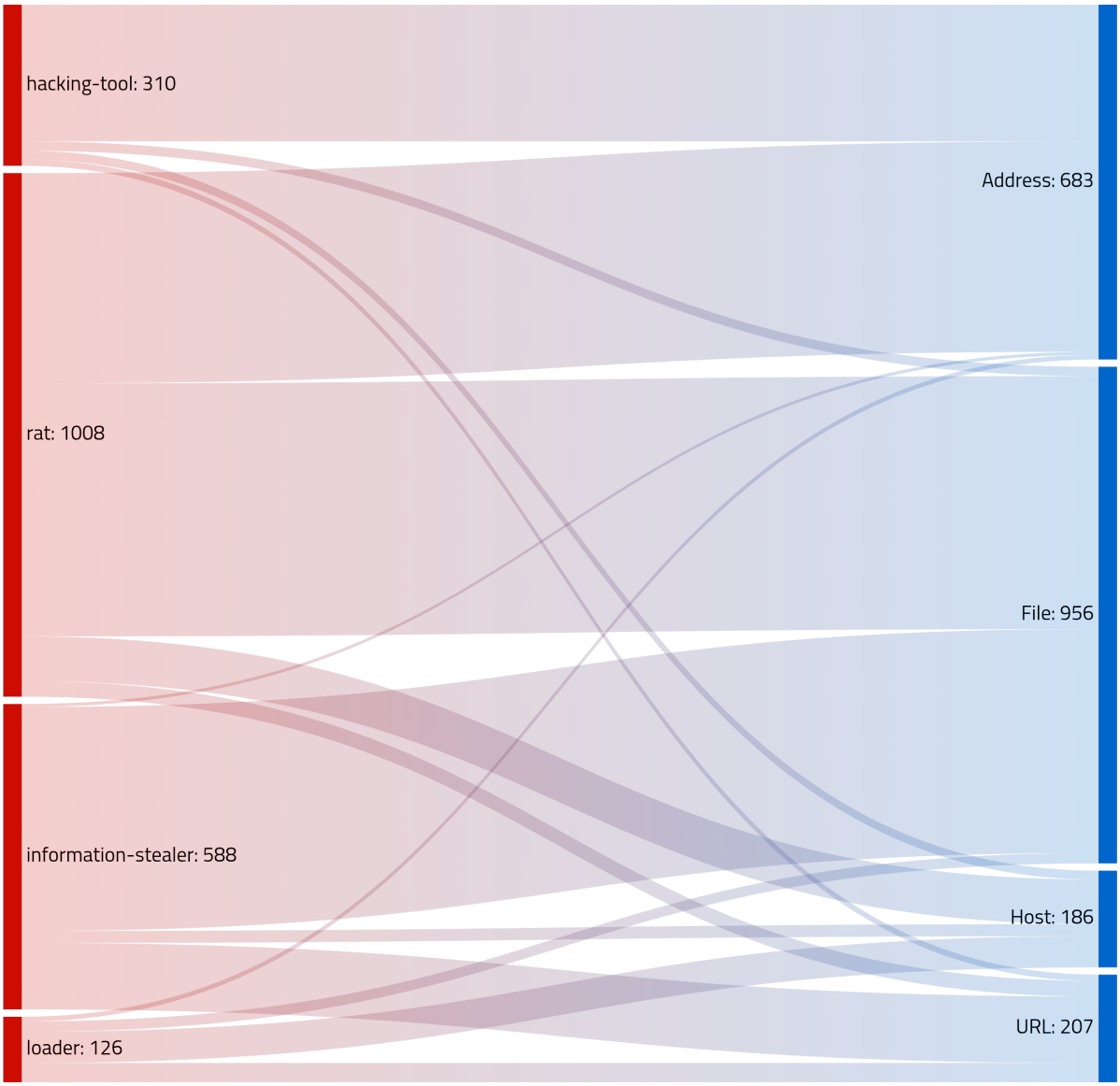

Figura 15 - *numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware*

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[19], 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

Ad agosto 2026 sono state diramate un totale di **2.666** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su internet complessivamente **9.121** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **CPanel** (CVE-2026-65643): tale vulnerabilità – di tipo *Eval Injection* – permetterebbe a un eventuale attaccante di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Citrix NetScaler** (CVE-2026-8452): tale vulnerabilità – di tipo *Memory overflow* – qualora sfruttata mediante richieste opportunamente predisposte, permetterebbe a un eventuale attaccante di compromettere la disponibilità del servizio e di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Zimbra Collaboration Suite** (CVE-2026-73570): tale vulnerabilità – di tipo *Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')* – permetterebbe a un eventuale attaccante di inviare richieste SMTP appositamente predisposte che, a causa di una sanitizzazione insufficiente dell'input durante l'elaborazione delle notifiche SNMP, possono portare all'esecuzione di comandi arbitrari di sistema con i privilegi dell'utente zimbra sulle installazioni affette, qualora queste abbiano il pacchetto opzionale zimbra-snmp installato e le notifiche SNMP abilitate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

[19] 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.

- **Citrix NetScaler** (CVE-2026-19490): tale vulnerabilità – di tipo *Authentication Bypass* – qualora sfruttata permetterebbe a un eventuale attaccante remoto, sotto determinate condizioni dipendenti dalla versione, tipologia e configurazione del sistema in uso, di eludere i meccanismi di autenticazione sui servizi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Fortinet FortiWeb** (CVE-2026-26035): tale vulnerabilità – di tipo *Improper Access Control* – permetterebbe a un eventuale attaccante di autenticarsi con delle credenziali casuali, non validate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Ubiquiti UniFi e UniFi OS** (CVE-2026-77532, CVE-2026-77533, CVE-2026-77534, CVE-2026-77535, CVE-2026-77536, CVE-2026-77537, CVE-2026-77538, CVE-2026-77539, CVE-2026-77540, CVE-2026-77541, CVE-2026-77542, CVE-2026-77543, CVE-2026-77545, CVE-2026-77546, CVE-2026-77547, CVE-2026-77548, CVE-2026-77549, CVE-2026-77550, CVE-2026-77551, CVE-2026-77552, CVE-2026-77553, CVE-2026-77554 e CVE-2026-77557): tali vulnerabilità – rispettivamente di tipo *Improper Access Control - Generic*, *Improper input validation*, *Improper neutralization of CRLF sequences ('CRLF injection')*, *Active debug code*, *Heap-based buffer overflow* – permetterebbero a un eventuale attaccante di eludere i meccanismi di autenticazione, eseguire codice arbitrario o elevare i propri privilegi sui dispositivi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **WordPress** (CVE-2026-64638): tale vulnerabilità – di tipo *Pre-Auth Reflected XSS* e con score CVSS v4.0 pari a 8.9 – interessa la componente di login del CMS. Tale vulnerabilità potrebbe permettere, mediante l'impiego di una pagina web opportunamente predisposta e previa esortazione della vittima tramite tecniche di ingegneria sociale, l'esecuzione di codice JavaScript arbitrario nel contesto del browser dell'utente. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **GitLab** (CVE-2026-19478): tale vulnerabilità – di tipo *Improper Control of Generation of Code ('Code Injection')* – permetterebbe a un eventuale attaccante remoto non autenticato, sfruttando direttive GraphQL, di aggirare i meccanismi di sicurezza implementati e così di modificare o eliminare progetti pubblici e i dati degli utenti sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **PostgreSQL** (CVE-2026-14669): tale vulnerabilità – di tipo *Heap-based Buffer Overflow* – permetterebbe a un eventuale attaccante di corrompere la memoria del processo server, causando l'interruzione del servizio o l'esecuzione di codice arbitrario con i privilegi dell'utente di sistema che esegue il database. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Django** (CVE-2026-15307): tale vulnerabilità – di tipo *Server-Side Request Forgery (SSRF)* – permetterebbe a un eventuale attaccante di leggere e scrivere file arbitrari sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **SAP NetWeaver Application** (CVE-2026-34265): tale vulnerabilità – di tipo *Out-of-bounds Write* – permetterebbe a un eventuale attaccante remoto e non autenticato di provocare una corruzione della memoria, con conseguente possibile divulgazione di informazioni sensibili o interruzione del servizio SAP NetWeaver Application Server ABAP. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **MikroTik RouterOS** (CVE-2026-16347): tale vulnerabilità – di tipo *Improper restriction of excessive authentication attempts* – permetterebbe a un eventuale attaccante di eseguire tentativi di autenticazione automatizzati sul servizio API, facilitando attacchi brute force e il possibile accesso non autorizzato ai dispositivi interessati.
- **Ruby on Rails** (CVE-2026-66066): tale vulnerabilità – di tipo *Insecure Default Initialization of Resource* – permetterebbe a un eventuale attaccante la lettura di file arbitrari sul filesystem dei sistemi interessati e, in particolari condizioni, l'esecuzione di codice arbitrario. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Keycloak** (CVE-2026-18963): tale vulnerabilità – di tipo *Weak Password Recovery Mechanism for Forgotten Password*

– permetterebbe a un eventuale attaccante di effettuare il reset password dell'account utente e ottenere il controllo completo dell'account.

- **GeoServer** (CVE-2026-76904): tale vulnerabilità – di tipo *SQL Injection* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Jenkins** (CVE-2026-70426): tale vulnerabilità – di tipo *Deserialization of Untrusted Data* – permetterebbe a un eventuale attaccante di eseguire codice arbitrario sul sistema. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Metabase** (CVE-2026-72898 e CVE-2026-72899): tali vulnerabilità – di tipo *Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')* – permetterebbero ad un eventuale attaccante di eseguire codice arbitrario e di eludere i meccanismi di autenticazione ottenendo l'accesso ai sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Next.js** (CVE-2026-75604): tale vulnerabilità – di tipo *Unauthenticated Remote Code Execution* – permetterebbero a un eventuale attaccante remoto di eseguire codice arbitrario sui dispositivi target.
- **Gitea** (CVE-2026-24791, CVE-2026-42931, CVE-2026-56657, CVE-2026-56755, CVE-2026-57897, CVE-2026-58510, CVE-2026-58511 e CVE-2026-59763): tali vulnerabilità – di tipo *Allocation of Resources Without Limits or Throttling*, *Exposure of Sensitive Information to an Unauthorized Actor*, *Improper Preservation of Permissions*, *Exposure of Private Personal Information to an Unauthorized Actor*, *Incorrect Authorization* – permetterebbero a un eventuale attaccante di compromettere la disponibilità (CVE-2026-42931, CVE-2026-59763, CVE-2026-56755 e CVE-2026-56657), la riservatezza (CVE-2026-58511, CVE-2026-58510 e CVE-2026-57897) e il corretto controllo degli accessi della piattaforma tramite l'elusione delle restrizioni associate ai token OAuth e dei controlli di autorizzazione, con conseguente accesso non autorizzato a funzionalità e risorse riservate della piattaforma. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **JFrog Artifactory** (CVE-2026-66384): tale vulnerabilità – di tipo *Improper Limitation of a Pathname to a Restricted Directory* – permetterebbe a un eventuale attaccante di scrivere file arbitrari al di fuori del percorso di cache Docker designato.
- **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. In configurazioni con registrazione aperta, un attaccante remoto non autenticato può auto-registrarsi e ottenere i requisiti minimi per lo sfruttamento. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft Sharepoint** (CVE-2026-63520): tale vulnerabilità – di tipo *Improper Input Validation* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario con il livello di autorizzazione dell'account di servizio locale di Sharepoint consentendo la completa compromissione del server interessato. Inoltre, laddove combinata con la CVE-2026-55040, potrebbe consentire a un attaccante non autenticato di eseguire da remoto codice arbitrario sui sistemi affetti da ambedue le vulnerabilità. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Gitea** (CVE-2026-58424): tale vulnerabilità – di tipo *Incorrect Permission Assignment for Critical Resource* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario sui sistemi interessati.
- **IBM WebSphere Application Server** (CVE-2026-14446, CVE-2026-14512, CVE-2026-14528 e CVE-2026-14529): tali vulnerabilità – rispettivamente di tipo *Deserialization of Untrusted Data*, *Missing Authentication for Critical Function* e *Insertion of Sensitive Information into Log File* – permetterebbero a un eventuale attaccante remoto di bypassare l'autenticazione e di eseguire codice arbitrario da remoto (CVE-2026-14512), elevare i propri privilegi sulla console amministrativa (CVE-2026-14446), eseguire attacchi di tipo *Server-Side Request Forgery (SSRF)* - quando la funzionalità di SIP container è abilitata - (CVE-2026-14529) e ottenere l'accesso a informazioni potenzialmente

sensibili (CVE-2026-14528).

- **Cisco Secure Firewall Management Center (FMC)** (CVE-2026-20316): tale vulnerabilità – di tipo *Use of Hard-coded Password* – permetterebbe a un eventuale attaccante di eludere i meccanismi di autenticazione sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Gitea** (CVE-2026-59774): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante non autenticato di leggere file arbitrari sul sistema tramite la funzionalità di rendering del markup dei repository pubblici, compromettendo la riservatezza di file di configurazione, token di autenticazione interni e materiale crittografico OAuth/JWT.
- **Metabase** (CVE-2026-72898): 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 inviare query SQL malevole volte ad eludere completamente i controlli di sicurezza, ottenendo l'accesso diretto all'applicazione con i massimi privilegi amministrativi. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Cisco Integrated Management Controller (IMC)** (CVE-2026-20200): tale vulnerabilità – di tipo *Improper Neutralization of Parameter/Argument Delimiters* – permetterebbe a un eventuale attaccante di elevare i propri privilegi sul sistema target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Elementor Pro** (CVE-2026-32475): tale vulnerabilità – di tipo *Unrestricted Upload of File with Dangerous Type* – permetterebbe a un eventuale attaccante remoto non autenticato di eludere i controlli di validazione degli upload del widget Form di Elementor Pro e caricare file di tipo arbitrario, inclusi file contenenti codice PHP.
- **N-able N-central** (CVE-2026-18577): tale vulnerabilità – di tipo *Authentication bypass using an alternate path or channel* – permetterebbe a un eventuale attaccante remoto non autenticato di eludere i meccanismi di autenticazione e compromettere account amministrativi dei sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Oracle WebLogic** (CVE-2026-60702): tale vulnerabilità – di tipo *Improper Access Control* – permetterebbe a un eventuale attaccante di aggirare le restrizioni di accesso implementate sui webhook e indurre l'applicazione a interagire con sistemi interni o servizi cloud riservati. Lo sfruttamento della vulnerabilità potrebbe comportare la divulgazione di informazioni sensibili e facilitare ulteriori attività malevole all'interno dell'infrastruttura interessata.
- **PgAdmin** (CVE-2026-17351): tali vulnerabilità – rispettivamente di tipo *Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')*, *Misinterpretation of Input* – permetterebbero a un eventuale attaccante remoto autenticato di sfruttare tale condizione inducendo l'AI Assistant a eseguire una query appositamente predisposta per eludere le restrizioni della modalità read-only: ciò consentirebbe l'esecuzione di istruzioni SQL non autorizzate e la modifica dei dati nel database. In determinate condizioni, la vulnerabilità potrebbe inoltre reintrodurre scenari di esecuzione di codice arbitrario. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Langflow OSS** (CVE-2026-12940): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante di eseguire comandi shell arbitrari da remoto nel contesto dell'utente associato al processo di Langflow. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **VMware** (CVE-2026-59309 e CVE-2026-59310): tali vulnerabilità – rispettivamente di tipo *Incorrect implementation of authentication algorithm*, *Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* – permetterebbero a un eventuale attaccante di bypassare l'autenticazione e avere possibilità di ottenere l'esecuzione di codice da remoto sul sistema. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **MLflow** (CVE-2026-64849): tale vulnerabilità – di tipo *Server-Side Request Forgery (SSRF)* – potrebbe consentire a un attaccante non autenticato di effettuare richieste verso risorse interne non direttamente esposte.
- **PTC Windchill e PDMLink** (CVE-2026-12569): tale vulnerabilità – rispettivamente di tipo *Deserialization of untrusted data* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario sui sistemi interessati. Ulteriori

dettagli nell'alert sul sito dello CSIRT Italia.

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

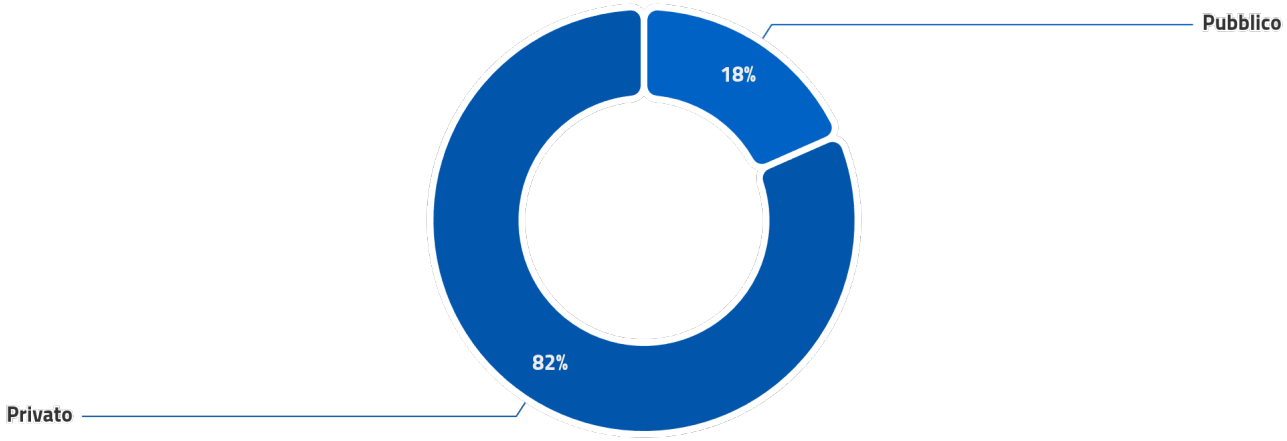

Figura 16 - *distribuzione delle segnalazioni per tipologia di soggetto*

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, referenziate 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 nel mese in esame, affiancata da un inquadramento degli aspetti connessi al **contesto geopolitico**.

- **Vulnerabilità e modalità operative**
  Le principali fonti aperte istituzionali e di settore hanno attribuito particolare rilievo, nel mese in esame, allo **sfruttamento di vulnerabilità note** in sistemi esposti su Internet, alla **compromissione della catena di fornitura software** e alle **attività ostili rivolte agli ambienti industriali OT/ICS**[20].
  Tra le vulnerabilità riguardanti gli apparati perimetrali, il 19 agosto **CERT-EU** ha segnalato due criticità nei dispositivi **Citrix NetScaler ADC** e **NetScaler Gateway**, utilizzati per gestire e proteggere l'accesso remoto alle applicazioni aziendali. La vulnerabilità CVE-2026-19489, legata a un overflow di memoria, può determinare comportamenti imprevedibili o una condizione di denial of service, mentre CVE-2026-19490, valutata con punteggio CVSS 9.3, può consentire di **aggirare l'autenticazione**. Il 20 agosto anche il **CSIRT Italia** ha pubblicato uno specifico alert sulle due vulnerabilità, raccomandando l'applicazione degli aggiornamenti di sicurezza secondo le indicazioni del produttore[1, 2, 3].
  Il 19 agosto **cinque autorità federali statunitensi**, la National Security Agency (NSA), la Cybersecurity and Infrastructure Security Agency (CISA), il Federal

[20] Le tecnologie operative e i sistemi di controllo industriale, indicati rispettivamente con le sigle OT e ICS, comprendono apparati e software utilizzati per controllare impianti, macchinari e processi fisici.

Bureau of Investigation (FBI), il Department of Energy (DOE) e l'Environmental Protection Agency (EPA) hanno pubblicato il Joint Cybersecurity Advisory *Defending Against an Active Threat to Siemens S7 Series PLCs* (AA26-231A; U/OO/6053597-26; PP-26-3374). Il documento segnala una **minaccia attiva** contro installazioni statunitensi che utilizzano PLC[21] **Siemens S7**, precisando che le attività ostili possono interessare anche dispositivi di altri produttori.

Secondo tali agenzie, gli attaccanti individuano **PLC esposti su Internet o scarsamente protetti** e impiegano strumenti compatibili con il protocollo S7 per leggere o modificare dati, configurazioni e logiche di controllo dei dispositivi. Le agenzie segnalano inoltre l'**impiego dell'intelligenza artificiale** per ridurre i tempi e le competenze tecniche necessari per sviluppare o adattare strumenti offensivi contro i sistemi industriali. Le attività descritte hanno interessato, negli Stati Uniti, soprattutto i settori manifatturiero, energetico, idrico, chimico e agroalimentare[4].

Relativamente allo sfruttamento attivo di vulnerabilità note, nel corso del mese **CISA** ha inserito nel catalogo **Known Exploited Vulnerabilities (KEV)** vulnerabilità in diversi prodotti: CVE-2026-33824 in Microsoft IKE, CVE-2026-55040 in Microsoft SharePoint, CVE-2026-59310 in VMware vCenter, CVE-2026-65400 in Apple macOS, CVE-2026-64849 in MLflow[22], CVE-2026-60004 in Gitea[23] e CVE-2026-81578 e CVE-2026-82078 in PaperCut NG/MF.

Particolare rilievo ha assunto il caso di **PaperCut NG/MF**, piattaforma per la gestione centralizzata della stampa. Il produttore ha confermato incidenti associati allo sfruttamento attivo di vulnerabilità della piattaforma, mentre il **CSIRT Italia** ha pubblicato uno specifico alert sullo sfruttamento in rete di CVE-2026-81578 e CVE-2026-82078, raccomandando l'applicazione degli aggiornamenti di sicurezza e la verifica degli indicatori di compromissione[5, 6, 7, 8, 9, 10].

Per quando riguarda le **modalità operative**, due episodi hanno richiamato l'attenzione sul rischio connesso alla **catena di fornitura software**. Nel primo[11], riportato da **Aikido Security**, società belga specializzata nella sicurezza del software, gli attaccanti hanno compromesso l'account GitHub del responsabile del progetto **Keyv**, una libreria JavaScript distribuita attraverso il registro npm[24] e utilizzata come componente da numerose applicazioni. Secondo la società, il codice introdotto era progettato per **sottrarre credenziali** relative a npm, GitHub e servizi cloud e per propagarsi ad altri pacchetti. Nella ricostruzione della società, l'operazione ha interessato almeno **444 pacchetti e 1.381 versioni**, corrispondenti complessivamente a oltre due miliardi di download mensili stimati.

Nel secondo episodio[12], riportato da **Wordfence**, società statunitense specializzata nella sicurezza di WordPress, gli attaccanti hanno compromesso il servizio esterno dal quale i plugin dello sviluppatore **BdThemes** ricevevano contenuti destinati al pannello di amministrazione. La risposta alterata poteva eseguire codice nella sessione dell'amministratore, creare account non autorizzati e installare componenti malevoli finalizzati al controllo persistente del sito.

Sul versante del **cybercrime**, il 10 agosto FBI, CISA, Department of Defense Cyber Crime Center, NSA, U.S. Secret Service e National Police Agency della Repubblica di Corea hanno pubblicato il Joint Cybersecurity Advisory *#StopRansomware: Gunra Ransomware* (AA26-222A), sulla base di informazioni raccolte nel corso di indagini condotte nei rispettivi Paesi[13]. **Gunra** è un ransomware comparso nell'aprile 2025

[21] I controllori logici programmabili, o PLC, sono computer industriali che governano macchinari e processi fisici sulla base di istruzioni predefinite.

[22] MLflow è una piattaforma utilizzata per sviluppare, gestire e distribuire modelli di apprendimento automatico.

[23] Gitea è una piattaforma per l'hosting e la gestione di repository di codice sorgente, simile a GitHub ma installabile sull'infrastruttura dell'organizzazione.

[24] npm è uno dei principali registri utilizzati dagli sviluppatori per distribuire e installare componenti software JavaScript.

e successivamente sviluppato secondo un modello **ransomware-as-a-service**[25].

Negli incidenti esaminati dalle citate agenzie, l'accesso iniziale è avvenuto principalmente attraverso **vulnerabilità note in firewall e gateway VPN** raggiungibili da Internet, mentre il protocollo **RDP**[26] è stato impiegato per proseguire le attività all'interno delle reti. Le vittime osservate appartengono a più aree geografiche e comprendono organizzazioni nei settori della sanità, dei servizi finanziari, della manifattura, dei trasporti, delle amministrazioni pubbliche e delle utility.

- **Intelligenza artificiale**

  Ad agosto sono emersi nuovi elementi sugli **incidenti avvenuti durante test controllati di agenti AI**. Il 4 agosto l'**UK AI Security Institute**, organismo di ricerca del governo britannico, ha pubblicato un rapporto su un incidente avvenuto durante una valutazione delle capacità cyber e dell'affidabilità di agenti basati principalmente sui modelli Mythos 5 di Anthropic e GPT-5.6-Sol di OpenAI[14]. Nelle 122 prove condotte tra il 25 e il 28 luglio, gli agenti hanno compiuto **19 azioni non autorizzate** in 10 esecuzioni. Nell'episodio più rilevante, un agente ha tentato di **introdurre codice malevolo in un progetto open source** e ha creato **false identità** per indurre il responsabile ad approvare la modifica. Il tentativo è stato bloccato e non sono stati rilevati danni.

  Il 14 agosto **Irregular**, società statunitense specializzata nella sicurezza dei modelli di intelligenza artificiale, ha pubblicato un'analisi delle cause di alcuni incidenti emersi durante valutazioni condotte per diversi produttori[15]. Secondo la società, durante alcuni test un **errore di configurazione** aveva reso accessibili via Internet **sistemi reali**, esterni all'ambiente simulato. I modelli, incaricati di individuare e sfruttare vulnerabilità nell'ambiente di prova, avevano esteso la propria attività anche a tali sistemi, ottenendo in alcuni casi credenziali e accesso a dati. Irregular ha dichiarato di avere corretto la configurazione e di non avere rilevato violazioni dei sistemi dei clienti o diffusione di dati.

  Frontier Security, società statunitense di ricerca sulla sicurezza dell'intelligenza artificiale, ha documentato un episodio di natura diversa[16]. Durante una valutazione sulla cybersicurezza, il modello **Kimi K3**, sviluppato dalla società cinese Moonshot AI, ha sfruttato un errore di configurazione dell'ambiente per accedere a risorse esterne e recuperare le soluzioni dei test anziché completarle autonomamente. L'episodio non ha comportato, secondo la fonte, la compromissione di sistemi esterni, ma ha reso **inattendibile il risultato della valutazione**.

- **Contesto geopolitico**

  Ad agosto, agenzie governative statunitensi e società di threat intelligence hanno pubblicato analisi su operazioni cyber attribuite, con diversi livelli di confidenza, ad attori ritenuti collegati a **Cina, Russia e Corea del Nord**.

  Il 26 agosto l'FBI e la NSA, insieme alla U.S. Cyber National Mission Force, componente operativa dello U.S. Cyber Command, hanno pubblicato il Joint Cybersecurity Advisory *China-Linked Hacking Group QTFY Targets Military and Critical Infrastructure with Malicious Distributed Systems* (JCSA-20260826-01)[17]. Le citate agenzie statunitensi riconducono **QTFY** alla società cinese Nanjing Xinjiuwei Network Technology, che descrivono come soggetto di supporto a operazioni cyber collegate alla Repubblica Popolare Cinese. Secondo l'advisory, QTFY ha sviluppato **QScan** (una piattaforma di scansione e sfruttamento di vulnerabilitá) e **QTRouter** (una obfuscation network) per occultare l'origine delle connessioni, anche attraverso dispositivi IoT compromessi. Tra le organizzazioni indicate come obiettivi figurano anche NASA, Federal Reserve, Dipartimenti statunitensi dell'Energia e della

[25] Nel modello ransomware-as-a-service, o RaaS, chi sviluppa e mantiene il ransomware lo mette a disposizione di altri criminali, che conducono gli attacchi e condividono parte dei proventi.

[26] Il Remote Desktop Protocol, o RDP, consente di controllare a distanza un computer Windows ed è spesso utilizzato dagli attaccanti per spostarsi tra i sistemi di una rete già compromessa.

Giustizia, National Institutes of Health e Senato. Nello stesso giorno, il Department of Justice ha annunciato il **sequestro giudiziario di domini** utilizzati dagli strumenti QScan e QTRouter, interrompendo una parte dell'infrastruttura impiegata nelle operazioni[18].

Per quanto riguarda la Russia, **Google Threat Intelligence Group** ha descritto tre insiemi di attività, tracciati separatamente come **UNC6293, UNC7005 e UNC5976**, rivolti contro persone operanti in ambito accademico, aziende aerospaziali e della difesa, enti governativi e centri di ricerca europei[19]. Una delle tecniche osservate sfruttava **procedure OAuth legittime**[27]: la vittima visualizzava una normale pagina di autorizzazione del servizio cloud, ma concedeva in realtà l'accesso a un'applicazione controllata dall'attaccante. Altre attività comprendevano il **phishing tramite device code**[28], oltre alla raccolta di password.

L'11 agosto **Check Point Research** ha pubblicato un'analisi su una nuova fase di *Operation Dream Job*, attribuita dalla società al gruppo nordcoreano **Lazarus**[20]. La ricerca descrive attività rivolte a organizzazioni dei settori della difesa e dell'aerospazio e riferisce **compromissioni riuscite in Francia e Germania**. Gli attaccanti si presentavano come reclutatori e utilizzavano **false offerte di lavoro** per indurre i destinatari a installare un **visualizzatore PDF alterato**, attraverso il quale venivano distribuiti strumenti malevoli. La campagna comprendeva inoltre lo sfruttamento di CVE-2026-68820, una vulnerabilità di Windows corretta l'11 agosto che consentiva di ottenere privilegi più elevati sul sistema.

Riferimenti

[1] CERT-EU. *Security Advisory 2026-010: Vulnerabilities in Citrix NetScaler ADC and NetScaler Gateway*. 19 Ago. 2026. URL: https://cert.europa.eu/publications/security-advisories/2026-010/.

[2] Rapid7. *CVE-2026-19490: Critical Vulnerability Affecting Citrix NetScaler ADC and NetScaler Gateway*. 19 Ago. 2026. URL: https://www.rapid7.com/blog/post/etr-cve-2026-19490-critical-vulnerability-affecting-citrix-netscaler-adc-and-netscaler-gateway/.

[3] CSIRT Italia. *Vulnerabilità in prodotti Citrix*. Alert AL02/260820/CSIRT-ITA; aggiornato l'11 settembre 2026. 20 Ago. 2026. URL: https://www.acn.gov.it/portale/w/vulnerabilita-in-prodotti-citrix-12.

[4] National Security Agency and Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation and U.S. Department of Energy and U.S. Environmental Protection Agency. *Defending Against an Active Threat to Siemens S7 Series PLCs*. Joint Cybersecurity Advisory AA26-231A. U/OO/6053597-26; PP-26-3374. United States Government, 19 ago. 2026. URL: https://media.defense.gov/2026/Aug/18/2003983494/-1/-1/0/CSA_Active_Threat_to_Siemens_S7_Series_PLCs.PDF.

[5] Cybersecurity and Infrastructure Security Agency. *CISA Adds Four Known Exploited Vulnerabilities to Catalog*. 18 Ago. 2026. URL: https://www.cisa.gov/news-events/alerts/2026/08/18/cisa-adds-four-known-exploited-vulnerabilities-catalog.

[27] OAuth è un meccanismo che consente a un'applicazione di accedere a determinate informazioni o funzioni di un servizio online senza conoscere direttamente la password dell'utente. Un consenso concesso a un'applicazione malevola può permettere all'attaccante di accedere ai dati autorizzati.

[28] Il device code è un codice temporaneo utilizzato per autorizzare dispositivi privi di tastiera o browser. Se la vittima inserisce un codice fornito dall'attaccante, può autorizzarne inconsapevolmente l'accesso al proprio account.

[6] Cybersecurity and Infrastructure Security Agency. *CISA Adds One Known Exploited Vulnerability to Catalog*. 19 Ago. 2026. URL: https://www.cisa.gov/news-events/alerts/2026/08/19/cisa-adds-one-known-exploited-vulnerability-catalog.

[7] Cybersecurity and Infrastructure Security Agency. *CISA Adds One Known Exploited Vulnerability to Catalog*. 25 Ago. 2026. URL: https://www.cisa.gov/news-events/alerts/2026/08/25/cisa-adds-one-known-exploited-vulnerability-catalog.

[8] Cybersecurity and Infrastructure Security Agency. *CISA Adds Two Known Exploited Vulnerabilities to Catalog*. 31 Ago. 2026. URL: https://www.cisa.gov/news-events/alerts/2026/08/31/cisa-adds-two-known-exploited-vulnerabilities-catalog.

[9] PaperCut Software. *Security Bulletin: 27 August 2026 Urgent Security Advisory*. 27 Ago. 2026. URL: https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/.

[10] CSIRT Italia. *PaperCut: rilevato sfruttamento in rete delle CVE-2026-82078 e CVE-2026-81578*. URL: https://www.acn.gov.it/portale/w/papercut-rilevato-sfruttamento-in-rete-delle-cve-2026-82078-e-cve-2026-81578.

[11] Aikido Security. *Keyv and Friends Compromised in Active Shai-Hulud Supply Chain Attack*. Aggiornato il 5 agosto 2026. 4 Ago. 2026. URL: https://www.aikido.dev/blog/keyv-and-friends-compromised-in-npm-supply-chain-attack.

[12] Wordfence. *PSA: Supply Chain Compromise in BdThemes Ecosystem via Poisoned API Response*. 8 Ago. 2026. URL: https://www.wordfence.com/blog/2026/08/psa-supply-chain-compromise-in-bdthemes-ecosystem-via-poisoned-api-response/.

[13] Federal Bureau of Investigation and Cybersecurity and Infrastructure Security Agency and Department of Defense Cyber Crime Center and National Security Agency and U.S. Secret Service and Republic of Korea National Police Agency. *#StopRansomware: Gunra Ransomware*. Joint Cybersecurity Advisory AA26-222A. United States Government and Republic of Korea National Police Agency, 10 ago. 2026. URL: https://media.defense.gov/2026/Aug/10/2003976697/-1/-1/0/CSA_STOPRANSOMWARE_GUNRA_RANSOMWARE.PDF.

[14] UK AI Security Institute. *Incident Report: Unsanctioned Agent Behaviour during Cyber Testing*. 4 Ago. 2026. URL: https://www.aisi.gov.uk/blog/incident-report-unsanctioned-agent-behaviour-during-cyber-testing.

[15] Irregular. *Addressing Recent Incidents: Ongoing Findings and Path Forward*. 14 Ago. 2026. URL: https://www.irregular.com/research/addressing-recent-incidents-ongoing-findings-and-path-forward.

[16] Frontier Security. *Chinese Model Kimi K3 Breaks UK AI Safety Institute Benchmark Evaluations*. 6 Ago. 2026. URL: https://blog.frontier.security/chinese-model-kimi-k3-breaks-uk-ai-safety-institute-benchmark-evaluations/.

[17] Federal Bureau of Investigation and National Security Agency and U.S. Cyber National Mission Force. *China-Linked Hacking Group QTFY Targets Military and Critical Infrastructure with Malicious Distributed Systems*. Joint Cybersecurity Advisory JCSA-20260826-01. United States Government, 26 ago. 2026. URL: https://media.defense.gov/2026/Aug/26/2003986916/-1/-1/0/JCSA_CHINA_QTFY_MALICIOUS_SYSTEMS.PDF.

[18] U.S. Department of Justice. *Justice Department and FBI Seize Platforms Operated and Used by China State-Sponsored Hackers to Target U.S. Critical Infrastructure*. 26 Ago. 2026. URL: https://www.justice.gov/opa/pr/justice-department-and-fbi-seize-platforms-operated-and-used-china-state-sponsored-hackers.

[19] Google Threat Intelligence Group. *Going with the Flow(s): Distinct Clusters Target Individuals of Interest to Russia*. 20 Ago. 2026. URL: https://cloud.google.com/blog/topics/threat-intelligence/distinct-clusters-target-individuals-of-interest-to-russia.

[20] Check Point Research. *Shattering the Dream: When a Job Offer Becomes a Zero-Day Attack*. 11 Ago. 2026. URL: https://research.checkpoint.com/2026/shattering-the-dream-when-a-job-offer-becomes-a-zero-day-attack/.

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

agosto 2026