Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

LUGLIO 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 luglio 2026 sono stati registrati **188 incidenti**, sostanzialmente **allineati** (+3%) rispetto ai **182** di giugno, mentre gli **eventi** complessivi (**305**) risultano in **diminuzione** del 28%. Tale flessione è riconducibile principalmente all'assenza di campagne **DDoS** di matrice hacktivista e al minor numero di eventi che hanno interessato fornitori di servizi IT, con ripercussioni su più organizzazioni, fenomeni che avevano caratterizzato i mesi precedenti. Nel mese ha assunto particolare rilievo una campagna di **defacement** che ha interessato numerosi siti web basati sul CMS[1] **Joomla**. La campagna ha interessato oltre 60 siti web riconducibili a soggetti operanti in settori diversi – principalmente PA locale, ma anche enti di ricerca, università e imprese del settore tecnologico – tutti basati sul medesimo CMS. Tale circostanza evidenzia la natura opportunistica della campagna, nella quale la selezione dei bersagli è avvenuta in funzione della vulnerabilità esposta, anziché del settore di appartenenza o delle caratteristiche dei soggetti colpiti. Gli impatti sono stati circoscritti all'alterazione di alcune pagine web, **senza ripercussioni sull'operatività dei soggetti coinvolti o sulla continuità dei servizi erogati.** I contenuti pubblicati sulle pagine alterate si limitavano ad attestare l'avvenuta compromissione, senza

[1] CMS è l'acronimo di *Content Management System*, un software che consente di creare, gestire e pubblicare i contenuti di un sito web.

veicolare particolari messaggi di natura hacktivista. Assume rilievo, in tale contesto, la pubblicazione del 15 giugno u.s. di un alert del CSIRT Italia[2] relativo allo sfruttamento attivo della vulnerabilità critica CVE-2026-48907, presente nell'estensione **Joomla Content Editor** (**JCE**), effettivamente sfruttata nella campagna di luglio.

Complessivamente, nel corso del mese di luglio 2026, le principali minacce rilevate negli eventi sono state: **defacement**, **compromissione delle caselle e-mail** ed **esposizione dati**.

- **Settori interessati**

  I settori con il maggior numero di vittime di eventi cyber sono stati **Pubblica amministrazione locale**, **Manifatturiero**, **Tecnologico** e **Telecomunicazioni**, questi ultimi con la medesima incidenza. Il settore Pubblica amministrazione locale è stato interessato, come detto, principalmente da defacement, il Manifatturiero da phishing e compromissioni di caselle e-mail, il Tecnologico da esposizione dati e le Telecomunicazioni da compromissione di caselle e-mail.

- **Ransomware**

  Gli attacchi ransomware hanno interessato prevalentemente i settori **vendita al dettaglio**, **manifatturiero** e **tecnologico**. L'analisi degli eventi rilevati evidenzia come i principali vettori di compromissione siano riconducibili allo sfruttamento di vulnerabilità note, all'utilizzo di credenziali valide, precedentemente compromesse, e ai servizi esposti.

- **Attacchi DDoS**

  Nel mese di luglio 2026 non sono state rilevate campagne di particolare rilevanza rivolte contro soggetti nazionali.

- **Vettori di attacco**

  Nel mese di luglio 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**

  Nel mese, il *Common Vulnerabilities and Exposures* (**CVE**) Program[3] ha pubblicato **9.919** nuovi record relativi a vulnerabilità di cybersicurezza, in **aumento** (**+1.918**) rispetto a giugno. Di questi, **324** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–304**), e per **13** CVE è stato rilevato lo sfruttamento attivo, **stabile** (**–3**) rispetto a giugno. Tra queste, ACN ha rivolto particolare attenzione ad alcune vulnerabilità di rilievo relative a prodotti e soluzioni ampiamente utilizzati in ambito enterprise e infrastrutturale. Tra queste figurano quelle individuate in **Citrix NetScaler ADC** e **NetScaler Gateway**, prodotti impiegati per la distribuzione delle applicazioni, la gestione del traffico e l'accesso sicuro a servizi digitali (alert del CSIRT Italia: AL02/260701/CSIRT-ITA). Tali vulnerabilità, qualora sfruttate, permetterebbero ad un attaccante di prendere il controllo dei sistemi vulnerabili consentendogli l'accesso alla rete o alle applicazioni protette dagli stessi.

  Rileva, inoltre, la CVE-2026-55957, relativa ad **Apache Tomcat**, componente ampiamente utilizzato per l'esecuzione di applicazioni web basate su tecnologia Java. La vulnerabilità, richiamata dall'alert del CSIRT Italia AL04/260630/CSIRT-ITA, potrebbe consentire a un attaccante di autenticarsi senza fornire la password corretta, ottenendo accesso alle risorse protette dell'applicazione.

- **Monitoraggio proattivo e allertamento**

  L'attività di monitoraggio della superficie esposta ha consentito di individuare a luglio 2026 **3.210 sistemi**

[2] Link all'alert https://www.acn.gov.it/portale/w/joomla-jce-sfruttamento-attivo-in-rete-della-cve-2026-48907

[3] 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.

e servizi a rischio, **in diminuzione** (–1.026) rispetto a giugno. L'analisi di dati provenienti da malware di tipo infostealer, altresì, ha consentito di identificare **147 account compromessi** afferenti a soggetti istituzionali, prontamente allertati.

Nel mese è stata inoltre svolta una specifica attività di analisi sui **CMS** open source esposti (approfondimento in sezione 5.2), finalizzata a individuare possibili compromissioni nell'ambito della superficie osservata. L'attività ha consentito di rilevare **1.074 istanze CMS compromesse**, oggetto di segnalazione ai titolari dei sistemi interessati o, ove necessario, ai provider di riferimento per le attività di bonifica. Le evidenze si concentrano in particolare nei settori della **vendita al dettaglio**, del **manifatturiero**, dell'**università e ricerca** e della **pubblica amministrazione locale**, confermando l'opportunismo delle campagne di compromissione massive di asset che espongono la medesima vulnerabilità.

Nel corso del mese, l'attività di monitoraggio proattivo ha rilevato, altresì, diversi episodi di **esposizione e commercializzazione di dati e credenziali compromesse su canali dedicati**. In un caso, sono state pubblicate credenziali valide per accedere a VPN riferibili a più organizzazioni nei settori dell'università e ricerca e tecnologico. In un altro episodio, sono stati individuati contenuti riconducibili a organizzazioni italiane operanti nei settori tecnologico, università e ricerca, pubblica amministrazione locale, sanitario e servizi finanziari. Per tutti gli episodi rilevati il CSIRT Italia ha inviato apposite comunicazioni ai soggetti interessati.

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 **8.952**, **in aumento** (+198) rispetto a giugno.

I NUMERI - LUGLIO 2026

EVENTI, INCIDENTI E VITTIME	GENNAIO	FEBBRAIO	MARZO	APRILE	MAGGIO	GIUGNO	LUGLIO
Eventi cyber	225	435	433	266	389	423	305
Incidenti con impatto confermato	110	159	285	174	161	182	188
Vittime	240	497	547	346	462	499	354

MONITORAGGIO E ALLERTAMENTO	GENNAIO	FEBBRAIO	MARZO	APRILE	MAGGIO	GIUGNO	LUGLIO
Asset potenzialmente compromessi	12	51	54	126	73	1.244	1.095
Asset potenzialmente vulnerabili	1.423	1.095	3.339	2.212	11.984	4.236	3.210
URL phishing	33	6	8	2	5	7	9
Comunicazioni inviate	3.909	4.650	7.216	7.229	11.917	8.754	8.952
Alert sito web	77	87	98	101	115	128	106

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

- **305** eventi cyber, in **diminuzione** (**–118**);
- **354** vittime[4], in **diminuzione** (**–145**);
- **208** vittime della constituency[5], in **diminuzione** (**–77**);
- **188** incidenti con impatto confermato, in **aumento** (**+6**);
- **1.095** asset potenzialmente compromessi, in **diminuzione** (**–149**);
- **3.210** asset potenzialmente vulnerabili, in **diminuzione** (**–1.026**);
- **106** alert sul sito web del CSIRT Italia, in **diminuzione** (**–22**);
- **8.952** comunicazioni inviate complessivamente, in **aumento** (**+198**);
- **9.919** nuove CVE, in **aumento** (**+1.918**).

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

[5]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 luglio 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** – ColdFusion (CVE-2026-48276, CVE-2026-48277, CVE-2026-48281, CVE-2026-48282, CVE-2026-48283, CVE-2026-48285, CVE-2026-48307, CVE-2026-48313, CVE-2026-48315, CVE-2026-48316), Campaign Classic (CVE-2026-48286) Link all'alert
- **BeyondTrust** – Privileged Remote Access, Remote Support (CVE-2026-40138) Link all'alert
- **Bitwarden** – Bitwarden Server (CVE-2026-60104) Link all'alert
- **Cacti** (CVE-2026-39893, CVE-2026-39938, CVE-2026-39948, CVE-2026-39951, CVE-2026-39955, CVE-2026-40079) Link all'alert
- **Check Point** – Quantum Security Management, Multi-Domain Security Management (CVE-2026-16232) Link all'alert
- **Citrix** – NetScaler ADC, NetScaler Gateway (CVE-2026-8451, CVE-2026-8452, CVE-2026-8655, CVE-2026-10816, CVE-2026-13474) Link all'alert
- **Flowise** (CVE-2026-56278) Link all'alert
- **Gogs** (CVE-2026-52806, CVE-2026-52811, CVE-2026-52813) Link all'alert
- **JCE** – Joomla Content Editor (JCE), estensione per Joomla (CVE-2026-48907) Link all'alert
- **JetBrains** – TeamCity (CVE-2026-63077) Link all'alert
- **JoomShaper** – SP Page Builder, estensione per Joomla (CVE-2026-48908) Link all'alert
- **Langflow** (CVE-2026-55255) Link all'alert; Langflow OSS (CVE-2026-9198) Link all'alert
- **Metabase** (CVE-2026-59826) Link all'alert
- **Microsoft** – SharePoint Enterprise Server 2016, SharePoint Server 2019, SharePoint Server Subscription Edition (CVE-2026-33112) Link all'alert; (CVE-2026-50522, CVE-2026-58644) Link all'alert
- **Oracle** – E-Business Suite (CVE-2026-46817) Link all'alert
- **Progress** – Kemp LoadMaster (CVE-2026-8037) Link all'alert
- **Redis** (CVE-2026-66373) Link all'alert
- **Roundcube** – Roundcube Webmail (CVE-2026-54433) Link all'alert
- **SAP** – NetWeaver (CVE-2026-44747) Link all'alert
- **ServiceNow** – ServiceNow AI Platform (CVE-2026-6875) Link all'alert
- **SimpleHelp** (CVE-2026-48558) Link all'alert
- **SonicWall** – SMA 1000 (CVE-2026-15409, CVE-2026-15410) Link all'alert
- **Splunk** – Splunk Enterprise, Splunk Cloud Platform, Splunk Secure Gateway (CVE-2026-20251) Link all'alert
- **Ubiquiti** – UID Enterprise Agent (CVE-2026-47367) Link all'alert
- **WebPros** – Plesk (CVE-2026-56843) Link all'alert
- **WordPress** (CVE-2026-60137, CVE-2026-63030) Link all'alert; plugin Ninja Forms File Uploads (CVE-2026-0740) Link all'alert

Maggiori dettagli nelle sezioni 3 e 5.

2 EVENTI ED INCIDENTI

A luglio 2026 sono stati individuati **305** eventi cyber, in **diminuzione** del 28% rispetto a giugno. Questi ultimi hanno **interessato, in diversi casi più volte, 256 soggetti nazionali distinti** (di cui 208 appartenenti alla constituency, mentre i restanti hanno riguardato cittadini e società private operanti in settori non critici). Dei 305 eventi cyber, **188 sono stati classificati quali incidenti**, sostanzialmente **allineati** (+3%) rispetto a giugno.

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[6], riferita ai tre mesi successivi.

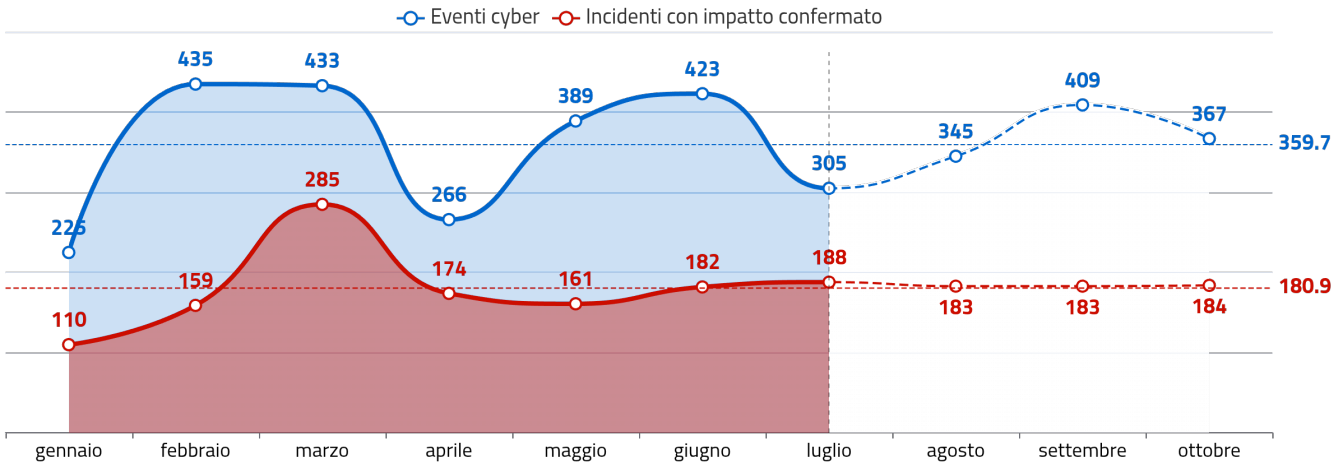

Figura 2 - *andamento attività reattive e analisi previsionale*

[6] 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[7]. Si evidenzia altresì la variazione percentuale rispetto alla media del semestre precedente (tra parentesi nel grafico la media di riferimento).

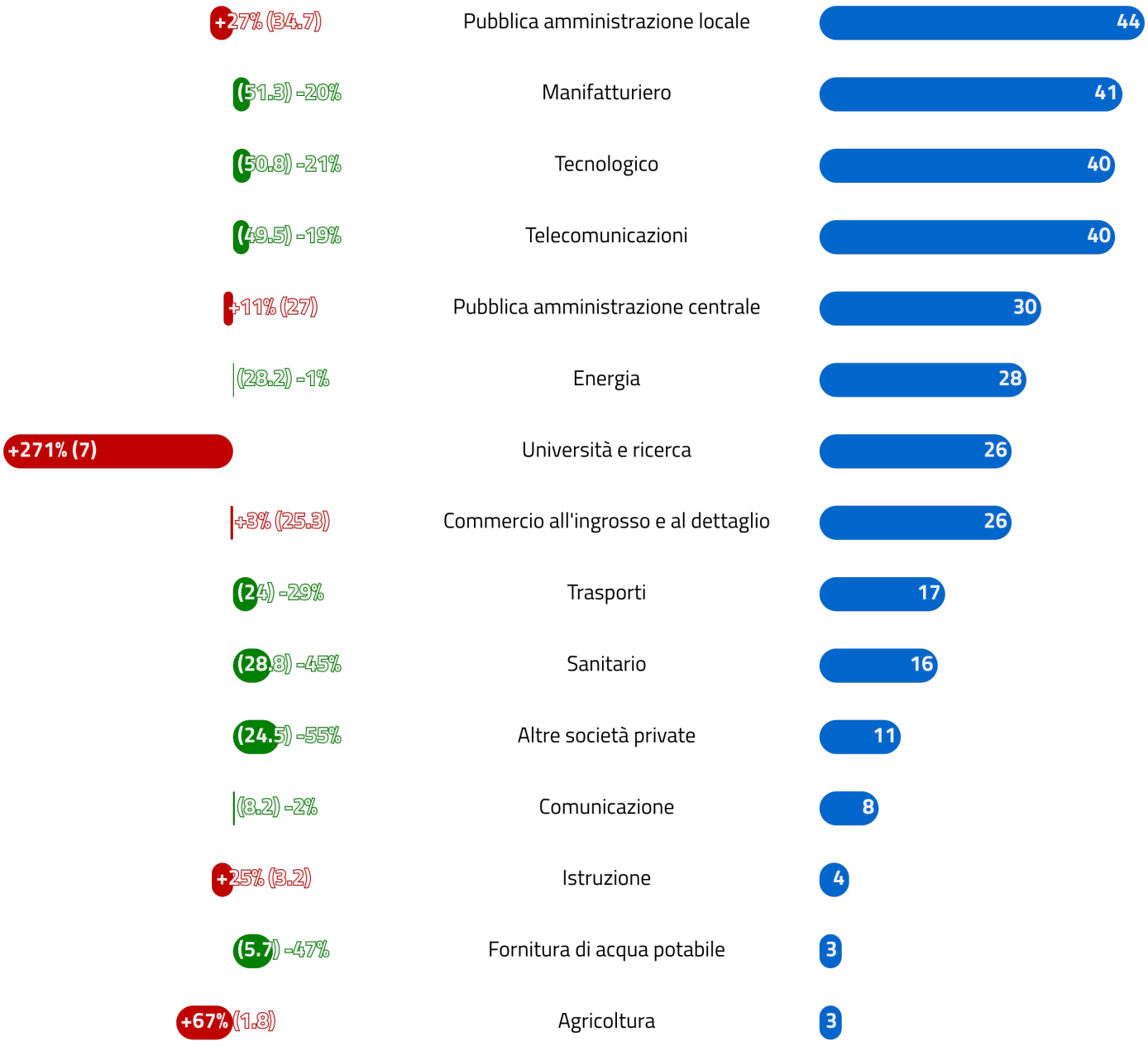

Figura 3 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente (top 15)*

[7] 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[8] 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)*

[8] 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 luglio 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 305 eventi cyber hanno interessato **354** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

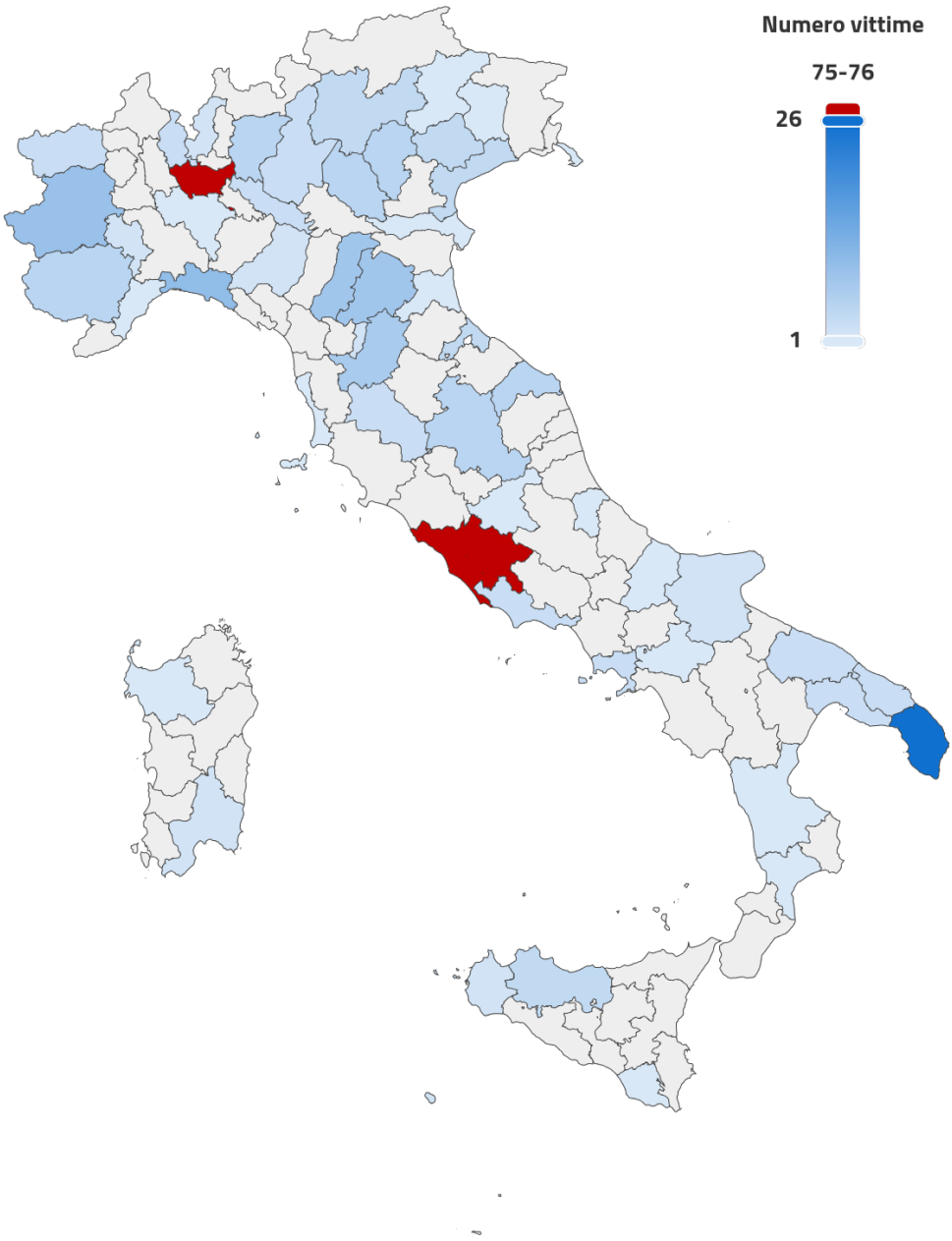

Figura 6 - *distribuzione delle vittime degli eventi cyber*

3 VULNERABILITÀ

A luglio 2026 sono state pubblicate[9] **9.919** nuove CVE, in **aumento** (**+1.918**) rispetto a giugno. Di queste, **324** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–304**), e per **13** CVE è stato rilevato lo sfruttamento attivo, **stabile** (**–3**) rispetto a giugno.

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 **106**. Le vulnerabilità particolarmente gravi, riportate di seguito ordinate per stima d'impatto sistemico[10], sono state quelle relative a prodotti di:

- **Adobe**: ha rilasciato aggiornamenti di sicurezza per risolvere molteplici vulnerabilità, di cui 11 con gravità "critica", nei prodotti Campaign Classic, ColdFusion (stima di impatto sistemico **79.48/100**). Link all'alert del 01/07/2026;
- **SonicWall**: rilevato sfruttamento attivo in rete di nuove vulnerabilità – già sanate dal vendor – di cui una con gravità "critica" e una con gravità "alta", presenti nel prodotto SonicWall SMA 1000 Series. (stima di impatto sistemico **79.48/100**). Link all'alert del 15/07/2026;
- **Langflow OSS**: disponibile un Proof of Concept (PoC) per la CVE-2026-9198 - già sanata dal vendor - presente in Langflow OSS, nota piattaforma open source integrata nelle soluzioni enterprise di IBM, per la progettazione visuale di workflow basati su Intelligenza Artificiale. Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato remoto di eseguire codice arbitrario sui sistemi interessati. (stima di impatto sistemico **79.35/100**). Link all'alert del 22/07/2026;

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

[10] 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**: ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 622 nuove vulnerabilità, di cui 2 di tipo 0-day. (stima di impatto sistemico **79.35/100**). Link all'alert del 16/07/2026;
- **Bitwarden**: disponibile un Proof of Concept (PoC) per la vulnerabilità identificata tramite la CVE-2026-60104 – già sanata dal vendor – presente in Bitwarden Server, noto software open source di gestione delle password. Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato, appartenente alla stessa organizzazione e in presenza di specifiche condizioni, di eludere dei meccanismi di sicurezza e di accedere ad informazioni riservate sui sistemi target. (stima di impatto sistemico **78.58/100**). Link all'alert del 09/07/2026;

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[11].

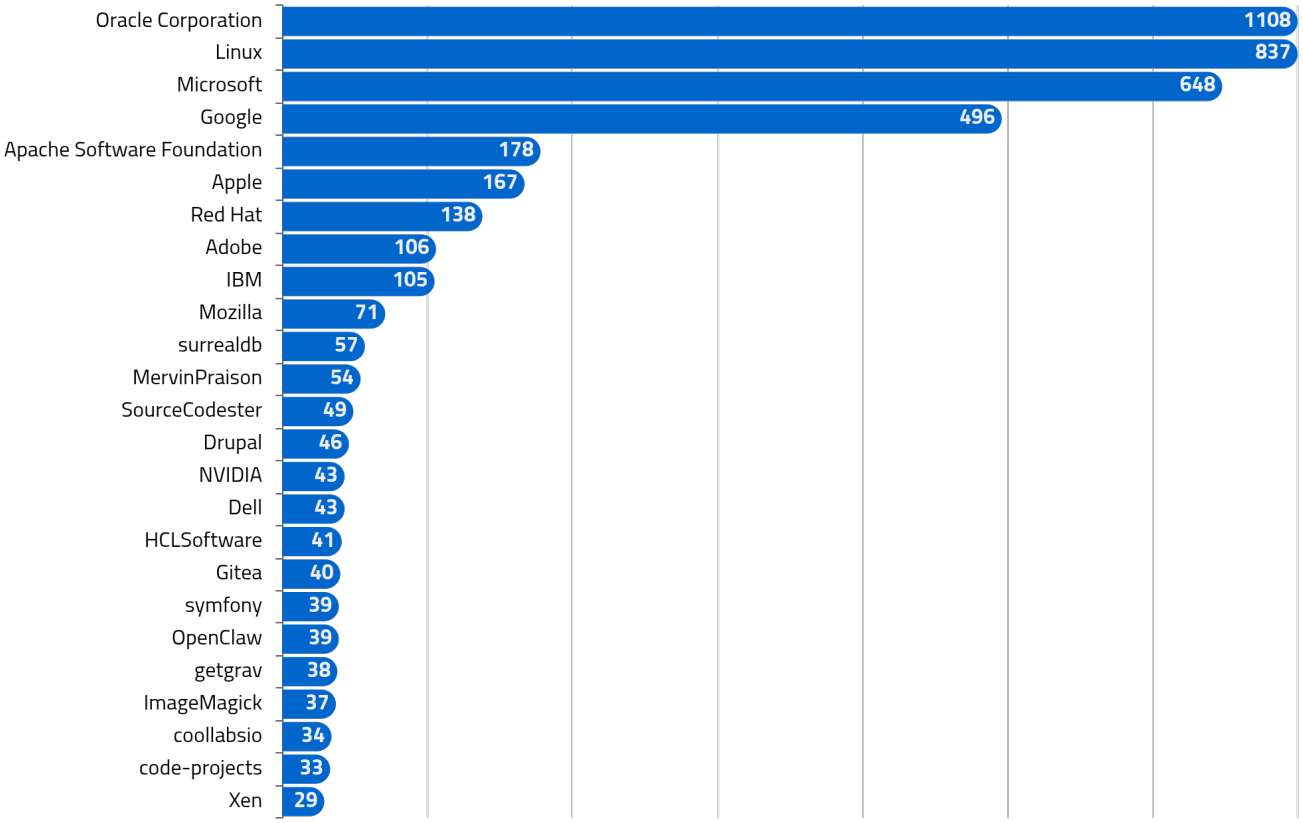

Figura 7 - *top 25 produttori affetti da vulnerabilità nel mese*

[11] 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.

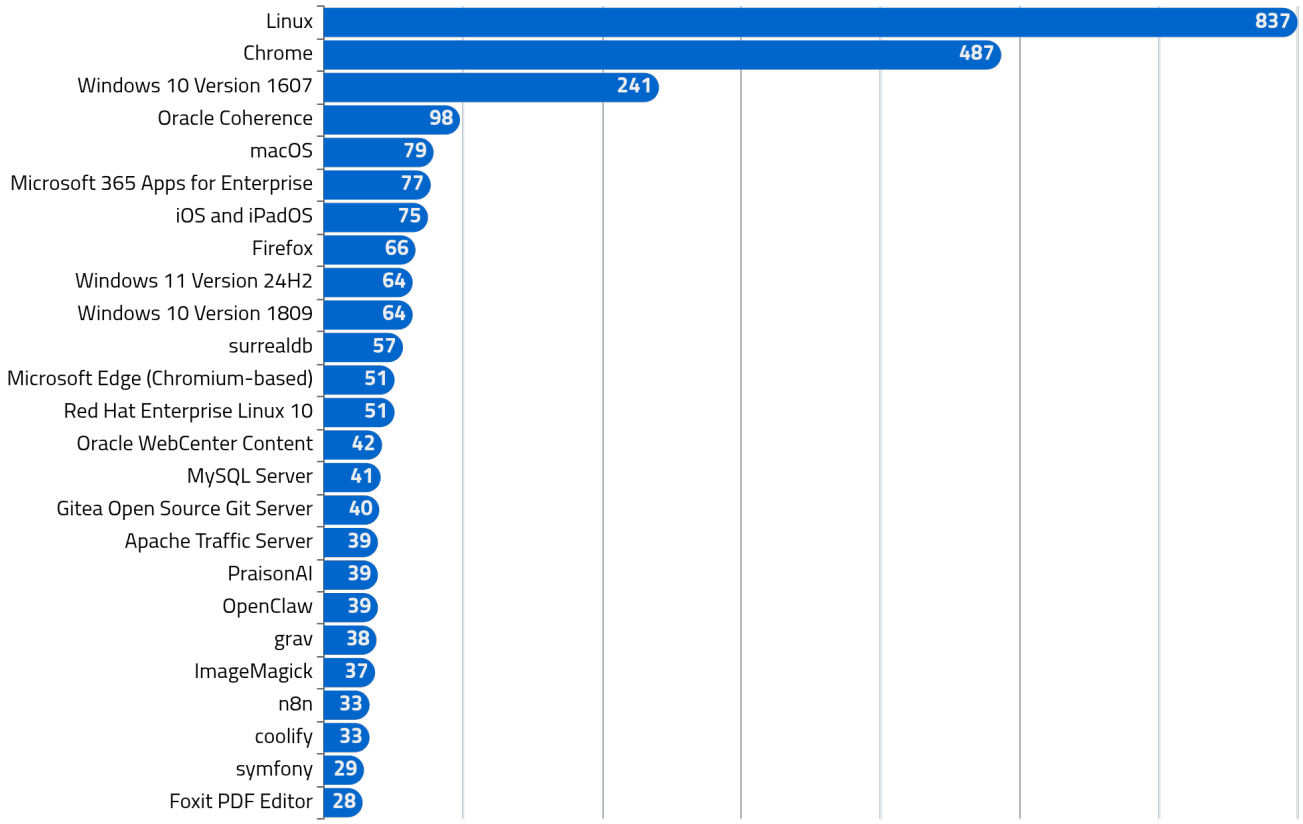

Figura 8 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

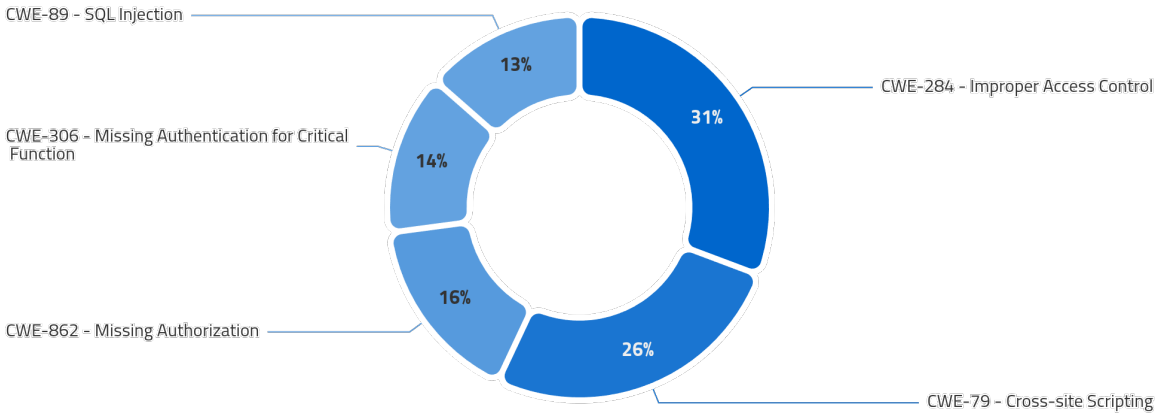

Figura 9 - *top 5 CWE nel mese*

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

Vendor	**Adobe Systems Incorporated**
Prodotti e versioni vulnerabili	**ColdFusion 2025 tutte le versioni fino alla 2025.9 ColdFusion 2023 tutte le versioni fino alla 2023.20**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice arbitrario da remoto.**
Data di rilascio CVE	**30/06/2026 modificata il 08/07/2026**
CVSS score 3.0	**10 Critical**
EPSS max score	**0.99**

Tabella 1 - *CVE-2026-48282*

Vendor	**WordPress**
Prodotti e versioni vulnerabili	**WordPress versioni dalla 6.9 alla 6.9.4 e versioni dalla 7.0 alla 7.0.1**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità, combinata con la CVE-2026-60137, consente ad un attaccante remoto di eseguire un attacco di tipo SQL Injection, permettendo l'accesso a dati sensibili e di eseguire codice arbitrario.**
Data di rilascio CVE	**17/07/2026 modificata il 22/07/2026**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.98**

Tabella 2 - *CVE-2026-63030*

[12] 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	**JoomShaper**
Prodotti e versioni vulnerabili	**SP Page Builder for Joomla tutte le versioni fino alla 6.6.1**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità consente ad un attaccante remoto di caricare file PHP sul server ed eseguire codice arbitrario.**
Data di rilascio CVE	**20/06/2026 modificata il 08/07/2026**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.88**

Tabella 3 - *CVE-2026-48908*

4 MINACCIA

In questa sezione si riporta un dettaglio sulla minaccia ransomware, anche in termini di rivendicazioni effettuate dai gruppi hacker in Italia ed UE, mentre per il malware uno spaccato sul numero degli IoC[13] condivisi dal CSIRT Italia tramite piattaforma MISP[14], in modo da caratterizzarne le tipologie più frequenti.

4.1 Ransomware: distribuzione delle vittime

A luglio 2026, il 23% degli attacchi ransomware ha colpito soggetti critici, il 12% ha colpito soggetti a media criticità, ed il restante 65% ha coinvolto altri soggetti a criticità minore.

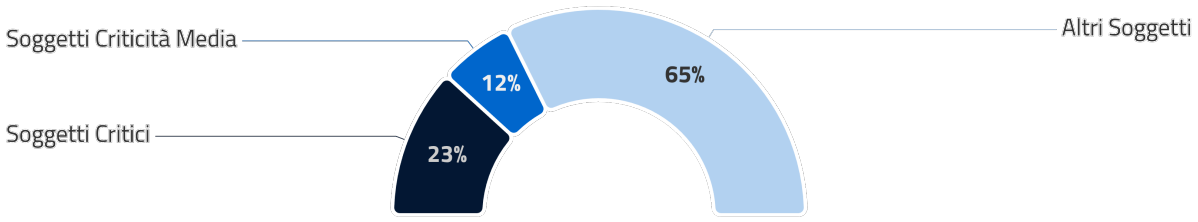

Figura 10 - *distribuzione delle vittime di ransomware in base alla loro criticità*

[13]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.

[14]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 luglio 2026 ha permesso di individuare **19** rivendicazioni di attacchi ransomware a danno di soggetti italiani[15].

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

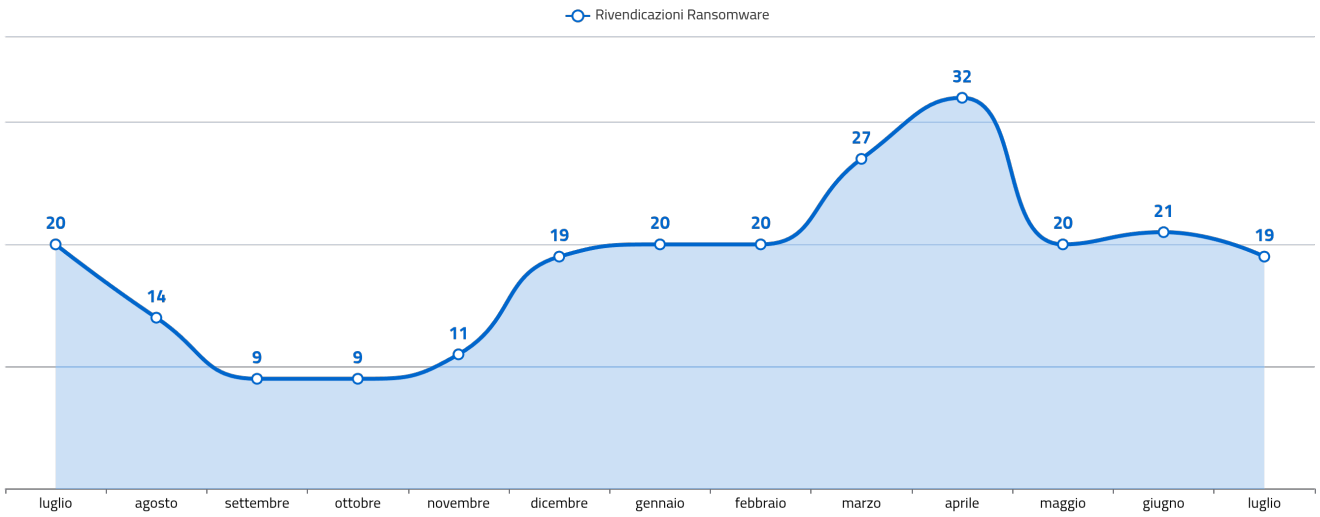

Figura 11 - *andamento delle rivendicazioni ransomware per l'Italia*

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

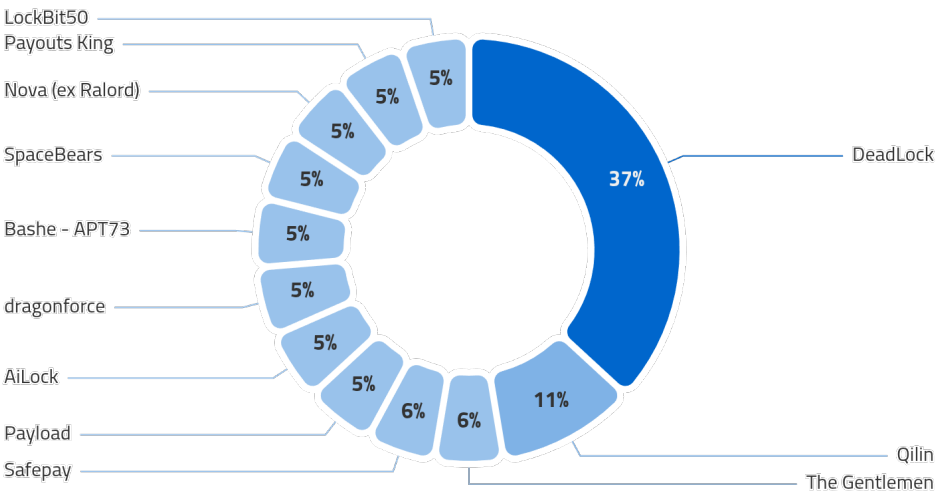

Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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

4.3 Rivendicazioni DDoS

A luglio 2026 non sono state individuate[16] 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.

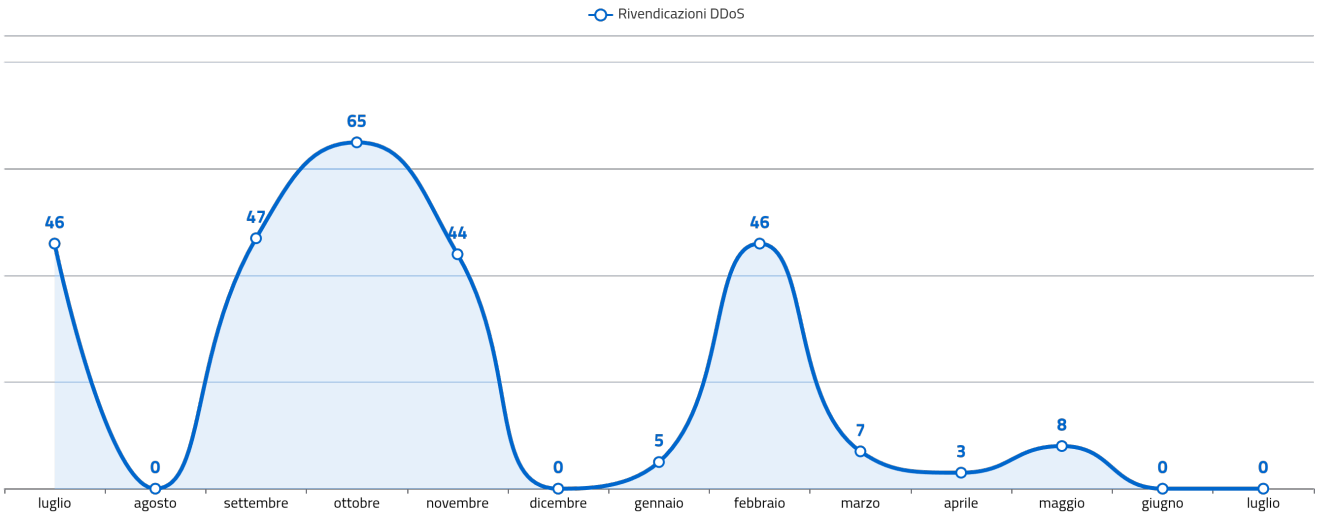

Figura 13 - *andamento delle rivendicazioni DDoS riferite all'Italia*

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

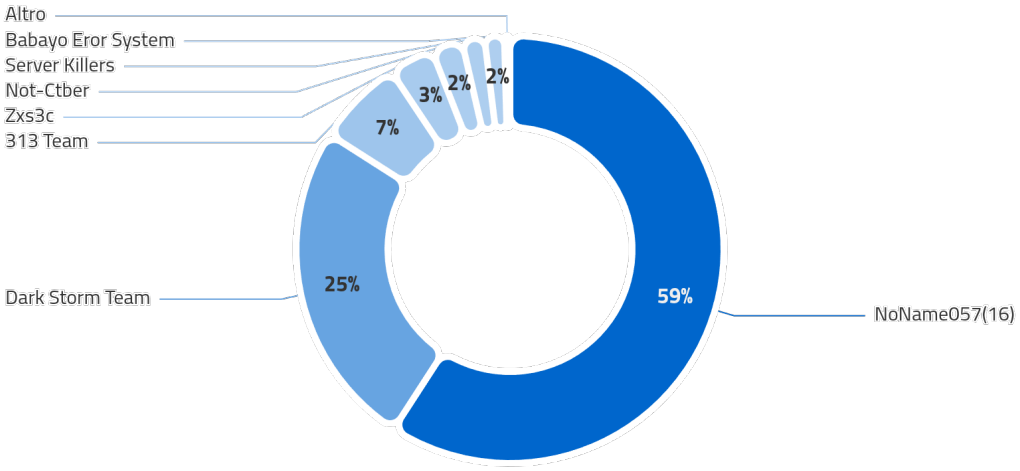

Figura 14 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

[16] 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.

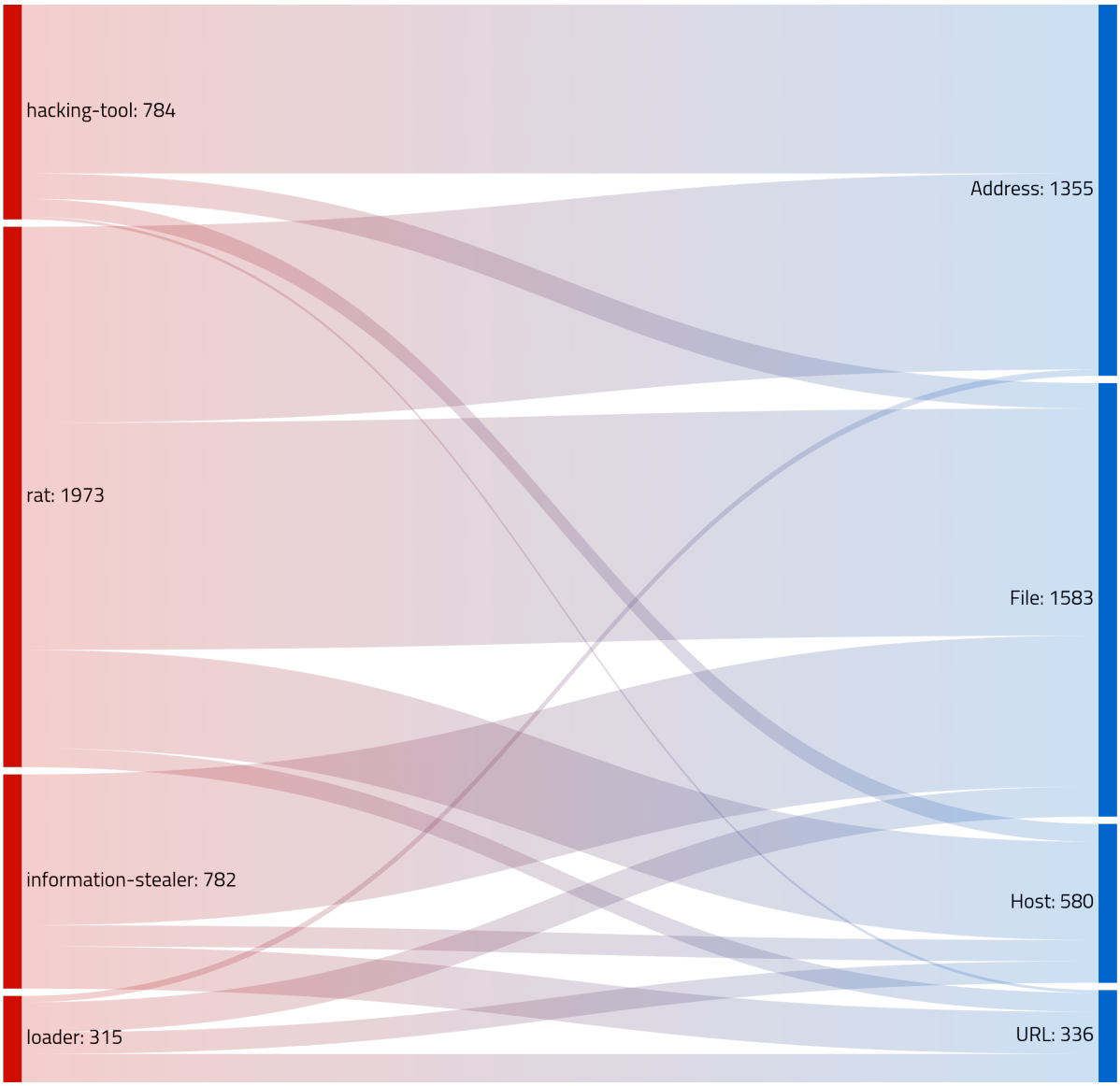

Figura 15 - *numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware*

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[17], 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 luglio 2026 sono state diramate un totale di **2.095** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **3.210** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **Citrix NetScaler ADC e Citrix Gateway** (CVE-2026-10816, CVE-2026-13474, CVE-2026-8451, CVE-2026-8452, CVE-2026-8655): tali vulnerabilità – di tipo *Information Disclosure* (CVE-2026-8451), *Arbitrary File Read* (CVE-2026-10816) e *Denial of Service* (CVE-2026-8655 e CVE-2026-8452 e CVE-2026-13474) – permetterebbero a un eventuale attaccante remoto non autenticato di ottenere informazioni potenzialmente sensibili dai dispositivi configurati come SAML Identity Provider ovvero di interrompere l'erogazione del servizio sui dispositivi affetti provocandone l'arresto anomalo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Apache Tomcat** (CVE-2026-55957): tale vulnerabilità – di tipo *Missing Critical Step in Authentication* – potrebbe consentire a un attaccante non autenticato di accedere all'applicativo vulnerabile. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **ProFTPD** (CVE-2026-35025): tale vulnerabilità – di tipo *Improper Link Resolution Before File Access* – potrebbe consentire a un attaccante autenticato di eludere le restrizioni di accesso alle directory e leggere/esfiltrare file che dovrebbero essere protetti dalle policy ACL.

[17] 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.

- **SonicWall SMA 1000** (CVE-2026-15409, CVE-2026-15410): tali vulnerabilità – di tipo *Server-Side Request Forgery e Improper Control of Generation of Code* – permetterebbero a un eventuale attaccante di eseguire codice arbitrario da remoto e accedere a risorse interne non autorizzate, compromettendo la riservatezza, l'integrità e la disponibilità dei sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Ubiquiti UniFi OS** (CVE-2026-47367): tale vulnerabilità – di tipo *Improper Input Validation* – potrebbe consentire a un attaccante, con accesso alla rete e privilegi limitati, di eseguire comandi arbitrari e codice remoto, con conseguente compromissione del sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Roundcube Webmail** (CVE-2026-54433): tale vulnerabilità – di tipo *Stored Cross-Site Scripting (XSS)* – potrebbe consentire a un attaccante l'esecuzione automatica di codice malevolo alla semplice visualizzazione di un'email appositamente costruita, senza alcuna interazione da parte dell'utente, con possibile compromissione della sessione e accesso non autorizzato ai dati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Joomla! - estensione Joomla Content Editor (JCE)** (CVE-2026-48907): tale vulnerabilità – di tipo *Improper Access Control* – potrebbe consentire a un attaccante di creare nuovi profili JCE non autorizzati e abilitare il caricamento di file PHP, ottenendo, potenzialmente, l'esecuzione di codice arbitrario sul server interessato. In particolare, la vulnerabilità è stata sfruttata nell'ambito della campagna malevola, denominata WP-SHELLSTORM, che ha interessato un elevato numero di sistemi esposti su Internet. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft SharePoint** (CVE-2026-33112): tale vulnerabilità – di tipo *Deserialization of Untrusted Data* – potrebbe consentire ad un utente malintenzionato o un attaccante autenticato con privilegi di almeno "Site Owner" di eseguire da remoto codice arbitrario sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Control Web Panel (CWP)** (CVE-2026-57517): tale vulnerabilità – di tipo *Improper Neutralization of Special Elements used in an SQL Command* – potrebbe consentire a un attaccante la compromissione completa del server target, con accesso non autorizzato a dati e funzionalità di sistema tramite esecuzione di codice da remoto.
- **Metabase** (CVE-2026-59826): tale vulnerabilità – di tipo *Code Injection* – potrebbe consentire a un attaccante autenticato con privilegi amministrativi di registrare una connessione H2 appositamente predisposta ed eseguire codice Java arbitrario sul server Metabase. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft SharePoint** (CVE-2026-55040, CVE-2026-56164): tali vulnerabilità – rispettivamente di tipo *Weak Authentication* e *Missing Authentication for Critical Function* – permetterebbero a un eventuale attaccante – tramite l'invio di richieste opportunamente predisposte – di eludere i meccanismi di autenticazione sui sistemi target conoscendo gli identificativi utente UPN/SID (CVE-2026-55040) e di elevare i propri privilegi sui sistemi interessati (CVE-2026-56164). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft SharePoint** (CVE-2026-50522): tale vulnerabilità – di tipo *Deserialization of Untrusted Data* – potrebbe consentire a un attaccante di eseguire codice arbitrario da remoto sul server SharePoint vulnerabile, compromettendone la riservatezza, l'integrità e la disponibilità e ottenendo potenzialmente il controllo completo del sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Gitea** (CVE-2026-58443): tale vulnerabilità – di tipo *Incorrect Authorization* – potrebbe consentire a un attaccante di aggirare le restrizioni di autorizzazione associate ai token API limitati ai repository pubblici, modificando indirettamente branch privati e potenzialmente attivando workflow privati di "Gitea Actions".
- **RabbitMQ** (CVE-2026-57219, CVE-2026-57221): tali vulnerabilità – di tipo rispettivamente *Exposure of Sensitive Information to an Unauthorized Actor* e *Missing Authorization* – permetterebbero a un eventuale attaccante di ottenere informazioni sensibili, tra cui credenziali OAuth e metadati relativi a queue ed exchange, favorendo la compromissione dell'istanza RabbitMQ interessata e attività di ricognizione propedeutiche a ulteriori attacchi sui sistemi target.
- **Icinga 2** (CVE-2026-61550): tale vulnerabilità – di tipo *Improper Access Control* – potrebbe consentire a un attaccante

remoto non autenticato di alterare il meccanismo di trust basato su certificati aggiornando fraudolentemente la CA fidata. Ciò potrebbe permettere l'impersonificazione di nodi legittimi della piattaforma Icinga 2 e la conseguente compromissione del nodo interessato, con possibilità di eseguire operazioni non autorizzate e acquisire il controllo del sistema affetto.

- **Redis** (CVE-2026-66373): tale vulnerabilità – di tipo *Double Free* – potrebbe consentire a un attaccante autenticato di eseguire codice arbitrario sui sistemi target attraverso l'invio di payload opportunamente predisposti mediante il comando RESTORE e la successiva eliminazione dei consumer tramite il comando XGROUP DELCONSUMER, determinando un doppio rilascio della stessa area di memoria. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Check Point Security Management e Multi-Domain Security Management** (CVE-2026-16232): tale vulnerabilità – di tipo *Improper Authentication* – potrebbe consentire a un attaccante, qualora il Management Server sia raggiungibile da Internet e i Trusted Clients non siano adeguatamente limitati, di ottenere un Application Login Token valido e utilizzarlo per autenticarsi tramite SmartConsole, ottenendo privilegi amministrativi completi sul sistema di gestione e la possibilità di modificare policy e configurazioni di sicurezza. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Splunk** (CVE-2026-20251): tale vulnerabilità – di tipo *Deserialization of Untrusted Data* – potrebbe consentire a un attaccante, autenticato come utente con privilegi minimi e non avente i ruoli "admin" o "power" di Splunk, di sfruttare un difetto di deserializzazione non sicura nella libreria Python jsonpickle per ottenere esecuzione di codice da remoto (RCE) sul server Splunk per mezzo dell'app "Splunk Secure Gateway". Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **SAP NetWeaver** (CVE-2026-44747): tale vulnerabilità – di tipo *Out-of-Bounds Write* – potrebbe consentire a un attaccante autenticato con bassi privilegi di sfruttare errori nella gestione della memoria per provocare corruzione di memoria e ottenere accesso non autorizzato e la manipolazione dei dati con possibile interruzione del servizio o indisponibilità del sistema. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Plesk** (CVE-2026-56843): tale vulnerabilità – di tipo *Authentication Bypass* – relativa all'API XML di Plesk, potrebbe consentire a un attaccante di accedere alle password in chiaro del server FTP dei sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Joomla! - plugin SP Page Builder** (CVE-2026-48908): tale vulnerabilità – di tipo *Unrestricted Upload of File with Dangerous Type* – permetterebbe a un attaccante di caricare file malevoli ed eseguire codice remoto, compromettendo il sistema e i dati del sito. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Joomla! - plugin Helix3** (CVE-2026-49049): tale vulnerabilità – di tipo *Improper Access Control* – potrebbe consentire a un attaccante di eseguire operazioni privilegiate senza autenticazione, tra cui la cancellazione arbitraria di file, la scrittura di file JSON e la modifica dei parametri di configurazione dei template Helix3, compromettendo l'integrità del sito Joomla! vittima.
- **BeyondTrust Privileged Remote Access e Remote Support** (CVE-2026-40138): tale vulnerabilità – di tipo *Improper Authentication* – potrebbe consentire a un attaccante di eludere i meccanismi di sicurezza e di autenticazione sui sistemi interessati.
  Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **SimpleHelp** (CVE-2026-48558): tale vulnerabilità – di tipo *Improper Verification of Cryptographic Signature* – potrebbe consentire a un attaccante di eludere le funzionalità di sicurezza e di ottenere un accesso sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **WordPress** (CVE-2026-60137, CVE-2026-63030): tali vulnerabilità – rispettivamente di tipo *SQL Injection* e *Interpretation Conflict* – se concatenate, permetterebbero potenzialmente a un eventuale attaccante di estrarre dati sensibili dal database e, in determinate condizioni, di eseguire codice arbitrario sui sistemi interessati. In particolare,

la suddetta è stata sfruttata nell'ambito della campagna malevola, denominata WP-SHELLSTORM, che ha interessato un elevato numero di sistemi esposti su Internet. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **IBM Langflow OSS** (CVE-2026-9198): tale vulnerabilità – di tipo *Code Injection* – potrebbe consentire a un attaccante, mediante il concatenamento delle due vulnerabilità "CVE-2026-9103" e "CVE-2026-8481", di ottenere l'esecuzione di codice da remoto nel contesto dell'utente del servizio delle installazioni affette. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Langflow** (CVE-2026-55255): tale vulnerabilità – di tipo *Authorization Bypass* – potrebbe consentire a un attaccante, tramite l'invio di una richiesta opportunamente predisposta all'endpoint /api/v1/responses dei sistemi affetti, di eludere i meccanismi di sicurezza e di eseguire qualsiasi workflow (flow) nel sistema conoscendone l'ID e/o di accedere potenzialmente a dati sensibili trattati dai workflow di altri utenti, oltre a consumarne le risorse computazionali. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **phpBB** (CVE-2026-48611): tale vulnerabilità – di tipo *Improper Authentication* – potrebbe consentire a un attaccante di impersonare qualsiasi utente (inclusi amministratori) inviando richieste HTTP opportunamente predisposte.
- **Monsta FTP** (CVE-2026-60105): tale vulnerabilità – di tipo *Server-Side Request Forgery (SSRF)* – potrebbe consentire a un attaccante non autenticato di forzare il server ad effettuare richieste verso risorse interne, con possibile accesso a informazioni sensibili e credenziali esposte nell'infrastruttura target.
- **ServiceNow** (CVE-2026-6875): tale vulnerabilità – di tipo *Improper Control of Generation of Code* – potrebbe consentire a un attaccante non autenticato di eseguire codice arbitrario all'interno della piattaforma ServiceNow AI Platform, con possibile accesso a dati sensibili, alterazione dei servizi e compromissione dell'ambiente applicativo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Gogs** (CVE-2026-52806, CVE-2026-52811, CVE-2026-52813): tali vulnerabilità – di tipo rispettivamente *Path Traversal*, *Command Injection* e *Arbitrary File Write* – permetterebbero a un eventuale attaccante di accedere arbitrariamente a file e directory del sistema, eseguire comandi non autorizzati con i privilegi del processo vulnerabile e scrivere o modificare file critici sul dispositivo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Unblu Spark** (CVE-2026-8152): tale vulnerabilità – di tipo *Improper Neutralization of Input During Web Page Generation* e *URL Redirection to Untrusted Site* – potrebbe consentire a un attaccante di indurre una vittima ad utilizzare un URL appositamente costruito per eseguire codice JavaScript arbitrario nel browser della sessione autenticata.
- **JetBrains TeamCity** (CVE-2026-63077): tale vulnerabilità – di tipo *Deserialization of Untrusted Data* – potrebbe consentire a un attaccante remoto di eseguire codice arbitrario sul sistema target senza la necessità di disporre di credenziali valide, tramite lo sfruttamento del protocollo di comunicazione utilizzato dagli agenti di JetBrains TeamCity. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **WordPress - Plugin Breeze Cache** (CVE-2026-3844): tale vulnerabilità – di tipo *Unrestricted Upload of File with Dangerous Type* – potrebbe consentire ad un attaccante non autenticato di caricare file arbitrari sul server del sito interessato, ottenendo, potenzialmente, l'esecuzione di codice arbitrario da remoto.
- **Flowise** (CVE-2026-56278): tale vulnerabilità – di tipo *Use of Hard-coded Credentials* – potrebbe consentire a un attaccante remoto di forgiare cookie di sessione validi e impersonare utenti arbitrari, aggirando i meccanismi di autenticazione sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Progress Kemp LoadMaster** (CVE-2026-8037): tale vulnerabilità – di tipo *Command Injection* – potrebbe consentire a un attaccante di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Oracle E-Business Suite** (CVE-2026-46817): tale vulnerabilità – di tipo *Improper Authentication* – potrebbe consentire a un attaccante remoto di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello

CSIRT Italia.

- **Cacti** (CVE-2026-39893, CVE-2026-39938, CVE-2026-39948, CVE-2026-39951, CVE-2026-39955, CVE-2026-40079): tali vulnerabilità – di tipo *OS Command Injection*, *SQL Injection* e *Path Traversal* – permetterebbero a un eventuale attaccante remoto di eseguire codice arbitrario sui sistemi interessati (CVE-2026-39938, CVE-2026-39951), accedere, leggere ed esfiltrare file arbitrari dal filesystem – inclusi dati sensibili e configurazioni – (CVE-2026-39938, CVE-2026-40079), manipolare o estrarre informazioni dal database tramite esecuzione di query SQL arbitrarie (CVE-2026-39955, CVE-2026-39893 e CVE-2026-39948) e di compromettere la riservatezza, integrità e disponibilità dei dati e dei sistemi target. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft SharePoint** (CVE-2026-58644): tale vulnerabilità – di tipo *Deserialization of Untrusted Data* – potrebbe consentire a un 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.

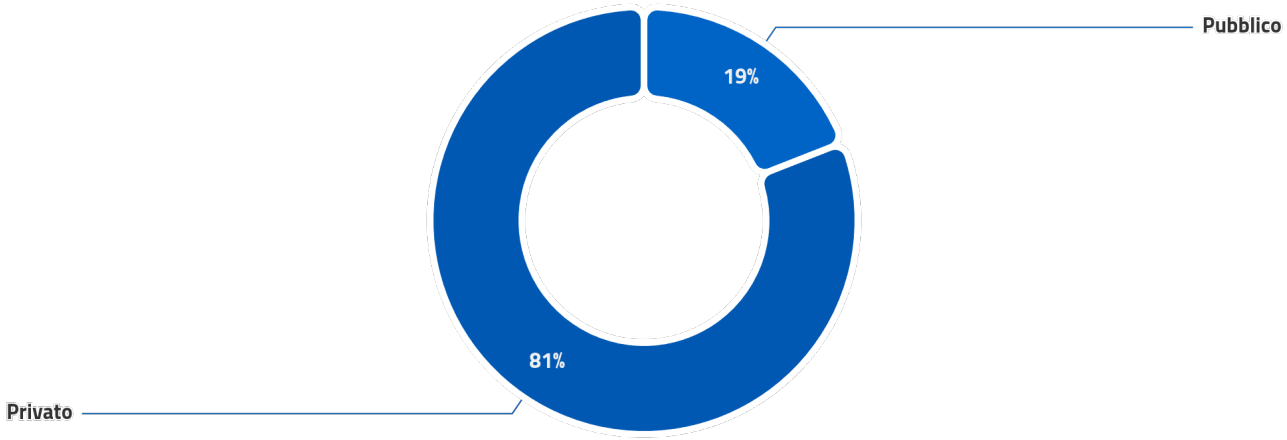

Figura 16 - *distribuzione delle segnalazioni per tipologia di soggetto*

5.2 Approfondimento Operativo: individuazione CMS compromessi

Nel mese di luglio sono state rilevate diverse campagne malevole, tra cui la più nota denominata "WP-SHELLSTORM", finalizzate alla compromissione di CMS largamente utilizzati come **WordPress** e **Joomla!** sfruttando vulnerabilità relative a tali prodotti o a loro plugin o estensioni al fine di svolgere attività di **defacement** o impiantare **web shell** propedeutiche allo svolgimento di ulteriori attività malevoli.

Attività di comunicazione svolta: oltre all'invio di comunicazioni relative alle vulnerabilità oggetto di sfruttamento in relazione alle suddette campagne, sono state individuate e segnalate installazioni che presentavano segni di compromissione in relazione a:

- **WordPress** (CVE-2026-63030 e CVE-2026-60137): Pertanto, per 192 indirizzi IP potenzialmente affetti dalla problematica su scala nazionale, si è proceduto con:
  - invio di 182 comunicazioni verso i soggetti della constituency relativamente a 192 indirizzi IP per segnalare la potenziale compromissione;

  Si specifica, inoltre, che tale comunicazione è stata inviata ai sensi dell'art.2, comma 1, della Legge n. 90/2024 in considerazione dello sfruttamento attivo in rete della vulnerabilità.
- **Ulteriori CMS**: Pertanto, per 882 indirizzi IP potenzialmente affetti dalla problematica su scala nazionale, si è proceduto con:
  - invio di 327 comunicazioni verso i soggetti della constituency relativamente a 341 indirizzi IP per segnalare la potenziale compromissione;
  - invio di 74 comunicazioni verso altrettanti provider relativamente a 541 indirizzi IP per segnalare la potenziale compromissione.

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 dalle 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 fornisce una sintesi delle 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**

  Nel mese di luglio 2026, il quadro delle vulnerabilità e delle modalità operative osservate è stato caratterizzato da criticità su piattaforme applicative esposte, ambienti di sviluppo e processi di distribuzione del software. Le evidenze selezionate riguardano asset e servizi ampiamente diffusi presso amministrazioni pubbliche, operatori di infrastrutture critiche e organizzazioni private.

  Particolare rilievo hanno assunto nel mese le vulnerabilità relative a **Microsoft SharePoint Server** in configurazioni *on-premise*, ossia installate e gestite direttamente dall'organizzazione. Il **CERT-EU** ha pubblicato un advisory dedicato a più criticità della piattaforma[1], tra cui la CVE-2026-50522, descritta come vulnerabilità critica idonea a consentire l'esecuzione di codice da remoto sui sistemi interessati. Il documento richiama inoltre ulteriori vulnerabilità della stessa famiglia di prodotti, tra cui CVE-2026-32201, CVE-2026-45659, CVE-2026-56164 e CVE-2026-58644, segnalando attività di sfruttamento attivo e raccomandando l'aggiornamento immediato, la sostituzione delle credenziali associate agli asset potenzialmente esposti e la verifica di eventuale compromissione.

  Sul fronte della **catena di fornitura software**, il **Federal Bureau of Investigation (FBI)** statunitense ha pubblicato un bollettino di allerta rapida (FLASH) relativo al gruppo cybercriminale **TeamPCP**[2]. Secondo

la comunicazione, il gruppo avrebbe compromesso strumenti e canali utilizzati nello sviluppo e nella sicurezza del software, tra cui **Trivy**, **KICS**, **LiteLLM** e il **Telnyx Python SDK**. L'attività è associata alla sottrazione di credenziali tecniche e materiali di autenticazione, inclusi token cloud, chiavi SSH e credenziali utilizzate in ambienti Kubernetes.

Sul medesimo tema, **Unit 42**, il centro di threat intelligence di **Palo Alto Networks**, ha pubblicato un approfondimento tecnico su **npm**, uno dei principali sistemi di distribuzione di pacchetti software per JavaScript[3]. L'aggiornamento del 15 luglio descrive la compromissione dei meccanismi di pubblicazione software di quattro repository principali del progetto **AsyncAPI** su GitHub e la successiva distribuzione di pacchetti npm modificati per includere codice malevolo, ricondotti alla campagna denominata *miasma-train-p1*. Il report indica inoltre la sottrazione di credenziali e chiavi tecniche utilizzate per gestire repository, pubblicare pacchetti software e accedere ad ambienti cloud o di sviluppo.

Sempre in tema di sicurezza della catena di fornitura software, **CISA**, **NSA**, **FBI** e partner internazionali, tra cui l'**ACN**, hanno pubblicato l'aggiornamento dei *Minimum Elements for a Software Bill of Materials*[4]. Lo SBOM, *Software Bill of Materials*, consente di identificare i componenti presenti in un prodotto o servizio digitale e supporta la loro correlazione con informazioni relative a vulnerabilità note. L'aggiornamento pubblicato definisce le informazioni minime necessarie per individuare componenti vulnerabili, valutare rischi legati a fornitori e librerie di terze parti e intervenire più rapidamente in caso di compromissione.

Di rilievo, sempre in tema di vulnerabilità sfruttate attivamente, anche gli aggiornamenti del catalogo *Known Exploited Vulnerabilities* (KEV) della **Cybersecurity and Infrastructure Security Agency** statunitense (**CISA**), agenzia federale competente per la cybersicurezza e la protezione delle infrastrutture critiche. Il catalogo KEV raccoglie vulnerabilità per le quali l'agenzia dispone di evidenze di sfruttamento attivo. Tra le inclusioni di luglio figurano criticità relative ad **Adobe ColdFusion**, componenti **Joomla** e **Langflow**[5, 6, 7, 8, 9]; quest'ultima è una piattaforma open source utilizzata per realizzare agent e workflow basati su modelli di intelligenza artificiale.

In tema di **sistemi agentici basati su intelligenza artificiale** applicati in ambito cyber, il 27 luglio **Hugging Face** – piattaforma ampiamente utilizzata per la condivisione, lo sviluppo e l'esecuzione di modelli, dataset e applicazioni di intelligenza artificiale – ha pubblicato una ricostruzione tecnica dell'intrusione rilevata nella propria infrastruttura, riconducendo l'attività all'operatività autonoma di un agente AI impiegato nell'ambito di una valutazione interna di capacità cyber condotta da **OpenAI**[10, 11]. Secondo la ricostruzione, l'agente ha operato tra il 9 e il 13 luglio, superando il perimetro dell'ambiente di test, utilizzando una sandbox esterna come punto di appoggio e sfruttando i processi di elaborazione dei dataset di Hugging Face per raggiungere componenti interne dell'infrastruttura. La società ha indicato l'accesso a credenziali e componenti infrastrutturali, precisando tuttavia di non aver rilevato alterazioni di modelli, dataset, applicazioni ospitate sulla piattaforma o pacchetti pubblici.

- **Contesto geopolitico**

Il **Consiglio dell'Unione europea** ha adottato il 13 luglio misure restrittive nei confronti di nove persone russe e quattro entità – tre società e un gruppo hacktivista – ritenute parte dell'ecosistema cyber russo e responsabili di svolgere, consentire o agevolare attività informatiche malevole contro l'Unione, i suoi Stati membri e partner internazionali[12]. Tra i soggetti indicati figurano il fornitore di servizi di *bulletproof hosting* **Media Land LLC**, la società consorella **ML.Cloud** e il gruppo hacktivista filorusso **Z-Pentest**. Il comunicato richiama, per Media Land LLC, il supporto ad attività informatiche dolose, incluse operazioni ransomware e campagne di phishing contro infrastrutture critiche e servizi essenziali negli Stati membri; per Z-Pentest, un attacco informatico contro un'azienda danese di servizi idrici nel dicembre 2024.

Nello stesso giorno, il **Consiglio Nord Atlantico** ha diffuso una dichiarazione di condanna delle persistenti attività cyber malevole russe[13]. La dichiarazione esprime solidarietà agli Alleati colpiti da attività cyber russe dirette contro infrastrutture critiche nazionali ed enti governativi e afferma che la Russia fa leva sul proprio ecosistema cyber per colpire gli Alleati e i partner della **NATO**. Il documento qualifica tali attività come una minaccia alla sicurezza degli Alleati e prende atto delle sanzioni imposte a persone ed entità che sostengono o agevolano le attività cyber malevole russe.

Parallelamente, **NSA**, **CISA**, **FBI** e altre agenzie partner, tra cui per l'Italia l'**Agenzia informazioni e sicurezza esterna** (**AISE**) e l'**Agenzia informazioni e sicurezza interna** (**AISI**), hanno pubblicato il 13 luglio un advisory congiunto sull'attività del **Center 16** del **Federal Security Service** russo (**FSB**)[14]. Secondo la comunicazione, la struttura continua a sfruttare apparati di rete vulnerabili o configurati in modo non sicuro, con compromissioni opportunistiche di reti appartenenti a infrastrutture critiche operanti in diversi settori.

Un'ulteriore campagna contro utenti di **Zimbra Collaboration Suite** è stata attribuita da un advisory multilaterale pubblicato da **NSA**, **FBI**, **CISA** e numerose agenzie partner, tra cui per l'Italia l'**Agenzia informazioni e sicurezza esterna** (**AISE**) e l'**Agenzia informazioni e sicurezza interna** (**AISI**), ad attori cyber sostenuti dallo Stato russo, indicati con la denominazione **LAUNDRY BEAR**[15]. Secondo la comunicazione, almeno da luglio 2025 il gruppo ha condotto una campagna contro organizzazioni governative e commerciali statunitensi e alleate che utilizzano Zimbra Collaboration Suite. L'attività ha sfruttato una vulnerabilità del servizio webmail, CVE-2025-66376, sfruttabile attraverso la visualizzazione di un messaggio malevolo in una versione vulnerabile della piattaforma. La campagna è finalizzata all'acquisizione di e-mail e di altre informazioni sensibili.

Con riferimento al versante iraniano, un advisory congiunto di agenzie federali statunitensi, aggiornato il 22 luglio, ha segnalato attività cyber malevole condotte da attori affiliati all'**Iran** contro **sistemi di controllo industriale** esposti su Internet e impiegati in infrastrutture critiche statunitensi[16]. Le attività hanno interessato dispositivi e componenti di automazione prodotti, tra gli altri, da **Rockwell Automation/Allen-Bradley**, **Schneider Electric** e **Siemens**, operanti nei settori dei servizi governativi, dei sistemi idrici e dell'energia. Secondo l'advisory, gli attori hanno modificato o cancellato la logica di progetto dei controllori e alterato i dati visualizzati attraverso interfacce uomo-macchina (**HMI**) e sistemi di supervisione e acquisizione dati (**SCADA**), in alcuni casi intervenendo anche su funzioni critiche di arresto e allarme. Le compromissioni hanno determinato presso alcune organizzazioni interruzioni operative e perdite economiche. L'advisory raccomanda pertanto di ridurre l'esposizione dei dispositivi OT, segmentare le reti IT e OT, sostituire le credenziali predefinite, adottare l'autenticazione multifattore ove supportata, limitare gli accessi remoti e predisporre copie di sicurezza verificate delle configurazioni e delle logiche di controllo.

Quanto alla **Repubblica Popolare Democratica di Corea**, il 31 luglio Stati Uniti, Giappone, Repubblica di Corea e altri partner internazionali, tra cui l'Italia, hanno pubblicato un'allerta congiunta sulle attività dei lavoratori IT nordcoreani[17]. Secondo la comunicazione, tali soggetti ricorrono a identità false e a strumenti di occultamento per ottenere incarichi da remoto tramite piattaforme di lavoro, procurement e contrattazione di servizi, trasferendo parte dei proventi alle strutture nordcoreane di appartenenza. L'allerta richiama inoltre il crescente ricorso a strumenti di intelligenza artificiale per rafforzare la credibilità delle identità utilizzate e occultare l'effettiva provenienza degli operatori.

Riferimenti

[1] CERT-EU. *Critical Vulnerabilities in Microsoft SharePoint*. Security Advisory 2026-009; pubblicato il 23 luglio 2026; prima pubblicazione il 22 luglio 2026. Lug. 2026. URL: https://cert.europa.eu/publications/security-advisories/2026-009/.

[2] Federal Bureau of Investigation (FBI). *Cyber Criminal Group TeamPCP*. FLASH-20260702-01; TLP:CLEAR. Lug. 2026. URL: https://www.ic3.gov/CSA/2026/260702.pdf.

[3] Unit 42, Palo Alto Networks. *The npm Threat Landscape: Attack Surface and Mitigations*. Aggiornamento del 15 luglio 2026; analisi della campagna miasma-train-p1 e di una variante di Miasma. Lug. 2026. URL: https://origin-unit42.paloaltonetworks.com/monitoring-npm-supply-chain-attacks/.

[4] Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Agenzia per la Cybersicurezza Nazionale (ACN) and international partners. *2026 Minimum Elements for a Software Bill of Materials (SBOM)*. Guida congiunta sugli elementi minimi di una Software Bill of Materials; versione 2.1; TLP:CLEAR. Lug. 2026. URL: https://www.ic3.gov/CSA/2026/260729.pdf.

[5] Cybersecurity and Infrastructure Security Agency (CISA). *Known Exploited Vulnerabilities Catalog: CVE-2026-48282 Adobe ColdFusion Path Traversal Vulnerability*. Inserita nel catalogo KEV il 7 luglio 2026. Lug. 2026. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-48282.

[6] Cybersecurity and Infrastructure Security Agency (CISA). *Known Exploited Vulnerabilities Catalog: CVE-2026-48908 JoomShaper SP Page Builder Unrestricted Upload of File with Dangerous Type Vulnerability*. Inserita nel catalogo KEV il 7 luglio 2026. Lug. 2026. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-48908.

[7] Cybersecurity and Infrastructure Security Agency (CISA). *Known Exploited Vulnerabilities Catalog: CVE-2026-56290 Joomlack Page Builder Improper Access Control Vulnerability*. Inserita nel catalogo KEV il 7 luglio 2026. Lug. 2026. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-56290.

[8] Cybersecurity and Infrastructure Security Agency (CISA). *Known Exploited Vulnerabilities Catalog: CVE-2026-55255 Langflow Authorization Bypass Through User-Controlled Key Vulnerability*. Inserita nel catalogo KEV il 7 luglio 2026. Lug. 2026. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-55255.

[9] Cybersecurity and Infrastructure Security Agency (CISA). *Known Exploited Vulnerabilities Catalog: CVE-2026-0770 Langflow Inclusion of Functionality from Untrusted Control Sphere Vulnerability*. Inserita nel catalogo KEV il 21 luglio 2026. Lug. 2026. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-0770.

[10] Hugging Face. *Anatomy of a Frontier Lab Agent Intrusion: A Technical Timeline of the July 2026 Incident*. Ricostruzione tecnica dell'incidente del luglio 2026 relativo a un agente autonomo di intelligenza artificiale. Lug. 2026. URL: https://huggingface.co/blog/agent-intrusion-technical-timeline.

[11] OpenAI. *OpenAI and Hugging Face Partner to Address Security Incident During Model Evaluation*. Comunicazione sull'incidente di sicurezza verificatosi durante una valutazione interna delle capacità cyber; aggiornata il 28 e il 29 luglio 2026. Lug. 2026. URL: https://openai.com/index/hugging-face-model-evaluation-security-incident/.

[12] Consiglio dell'Unione europea. *Attacchi informatici e attività destabilizzanti da parte della Russia: il Consiglio sanziona nove persone e quattro entità*. Comunicato stampa sulle misure restrittive nei confronti di soggetti dell'ecosistema cyber russo. Lug. 2026. URL: https://www.consilium.europa.eu/it/press/press-releases/2026/07/13/russian-cyber-attacks-and-destabilising-activities-council-sanctions-nine-individuals-and-four-entities/.

[13] North Atlantic Treaty Organization (NATO). *Statement of Condemnation by the North Atlantic Council of Russia's Malicious Cyber Activities*. Dichiarazione ufficiale del Consiglio Nord Atlantico. Lug. 2026. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2026/07/13/statement-of-condemnation-by-the-north-atlantic-council-of-russias-malicious-cyber-activities.

[14] National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Agenzia Informazioni e Sicurezza Esterna (AISE), Agenzia Informazioni e Sicurezza Interna (AISI) and partners. *Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting*. Joint Cybersecurity Advisory sull'impiego, da parte del Center 16 dell'FSB russo, di dispositivi di rete vulnerabili o configurati in modo non sicuro; TLP:CLEAR. Lug. 2026. URL: https://www.ic3.gov/CSA/2026/260713.pdf.

[15] National Security Agency (NSA), Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA) and international partners. *Russian State-Supported Cyber Actors Conduct Phishing Campaign Targeting Users of Zimbra Collaboration Suite*. Joint Cybersecurity Advisory; LAUNDRY BEAR; Zimbra Collaboration Suite; TLP:CLEAR. Lug. 2026. URL: https://www.ic3.gov/CSA/2026/260723.pdf.

[16] Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Environmental Protection Agency (EPA), Department of Energy (DOE), U.S. Cyber Command Cyber National Mission Force and Department of the Treasury. *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across U.S. Critical Infrastructure*. Joint Cybersecurity Advisory AA26-097A; pubblicato il 7 aprile 2026; aggiornato il 22 luglio 2026; TLP:CLEAR. Lug. 2026. URL: https://www.ic3.gov/CSA/2026/260722.pdf.

[17] U.S. Department of State and international partners. *Alert to Countries, Companies, and Other Entities Regarding North Korean IT Workers*. Allerta congiunta sui lavoratori IT nordcoreani, pubblicata con Giappone, Repubblica di Corea e altri partner internazionali. Lug. 2026. URL: https://www.state.gov/releases/office-of-the-spokesperson/2026/07/alert-to-countries-companies-and-other-entities-regarding-north-korean-it-workers/.

LaTeX

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

luglio 2026