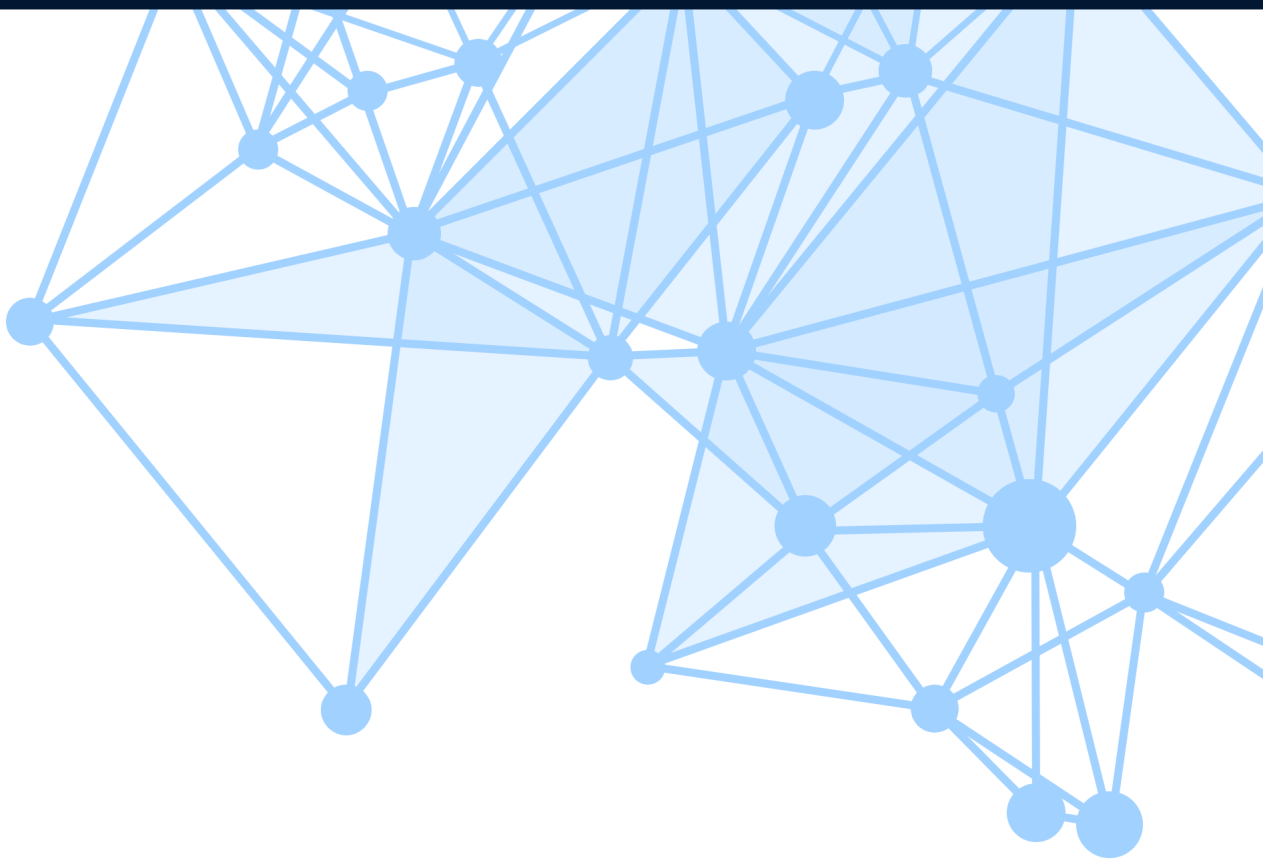
OPERATIONAL SUMMARY

OTTOBRE 2026

DATI ED INDICATORI DELLA MINACCIA CYBER IN ITALIA

Servizio Operazioni
e gestione delle crisi cyber

TLP:CLEAR



INTRODUZIONE

Il presente documento riporta su base mensile alcuni numeri e indicatori derivanti dalle attività operative dell'Agenzia per la Cybersicurezza Nazionale, utili per caratterizzare lo stato della minaccia cyber in Italia. In particolare, il CSIRT Italia, articolazione tecnico-operativa dell'Agenzia, è hub nazionale delle notifiche obbligatorie e volontarie di incidenti previste per legge (tra cui il Perimetro di Sicurezza Nazionale Cibernetica, la Legge 28 giugno 2024, n. 90 e il D.Lgs. 4 settembre 2024, n. 138 che recepisce la c.d. Direttiva NIS2) e riceve altresì informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali ed internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni dotano l'Agenzia di un ampio cono di visibilità sullo stato della minaccia cyber a danno del sistema Paese e forniscono, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali. Tutte le informazioni vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di triage le analizzano e classificano come eventi o incidenti cyber; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento, come:

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

Per le definizioni si rimanda al Glossario del CSIRT Italia e alla Tassonomia Cyber dell'ACN.

Le informazioni contenute in questo documento sono il risultato dell'analisi dei dati disponibili al momento della redazione; esse potrebbero essere aggiornate a seguito di nuove evidenze o di ulteriori approfondimenti.

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

Sommario

pag.

1. EXECUTIVE SUMMARY **5**
2. EVENTI ED INCIDENTI **10**
2.1. Settori impattati **11**
2.2. Tipologia di minacce negli eventi **12**
2.3. Distribuzione delle minacce per settore **13**
2.4. Distribuzione geografica delle vittime **14**
3. VULNERABILITÀ **15**
3.1. Vulnerabilità più gravi pubblicate sul sito del CSIRT Italia **15**
3.2. Distribuzione delle vulnerabilità sui vendor **17**
3.3. CWE nel mese **18**
3.4. Vulnerabilità con maggior probabilità di sfruttamento **19**
4. MINACCIA **21**
4.1. Ransomware: distribuzione delle vittime **21**
4.2. Rivendicazioni ransomware **22**
4.3. Rivendicazioni DDoS **23**
4.4. Indicatori di Compromissione (IoC) per famiglia di malware **24**
5. MONITORAGGIO **25**
5.1. Comunicazioni dirette **25**
6. ASPETTI DI INTERESSE DELLA MINACCIA CYBER GLOBALE **29**
6.1. Vulnerabilità e modalità operative **29**
6.2. Intelligenza artificiale **30**
6.3. Contesto geopolitico **31**

Indice delle figure

pag.

Figura 1 - indicatori delle attività operative ad ottobre 2026 e nei sei mesi precedenti 8
Figura 2 - andamento attività reattive e analisi previsionale 10
Figura 3 - numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente (top 15) 11
Figura 4 - tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente (top 15) 12
Figura 5 - numero di vittime per settore e tipologia di minacce 13
Figura 6 - distribuzione delle vittime degli eventi cyber 14
Figura 7 - top 25 produttori affetti da vulnerabilità nel mese 17
Figura 8 - top 25 prodotti affetti da vulnerabilità nel mese 18
Figura 9 - top 5 CWE nel mese 18
Figura 10 - distribuzione delle vittime di ransomware in base alla loro criticità 21
Figura 11 - andamento delle rivendicazioni ransomware per l'Italia 22
Figura 12 - distribuzione percentuale dei gruppi autori delle rivendicazioni 22
Figura 13 - andamento delle rivendicazioni DDoS riferite all'Italia 23
Figura 14 - distribuzione percentuale dei gruppi autori delle rivendicazioni 23
Figura 15 - numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware 24
Figura 16 - distribuzione delle segnalazioni per tipologia di soggetto 28

1 EXECUTIVE SUMMARY

- **Eventi e incidenti**

Nel mese di ottobre 2026, gli **attacchi DDoS** di matrice hacktivista e gli **attacchi web-based**, frequentemente associati allo sfruttamento di vulnerabilità nei servizi esposti su Internet, hanno rappresentato le principali minacce rilevate, contribuendo in misura significativa all'aumento del numero di eventi.

Parallelamente, è stato rilevato un numero significativo di **attacchi contro applicazioni e servizi web esposti su Internet**, prevalentemente ai danni di imprese dei settori tecnologico e manifatturiero, attività commerciali, imprese artigiane, strutture ricettive e di ristorazione, studi professionali, associazioni e amministrazioni locali. Una parte rilevante di tali attività è risultata riconducibile a campagne opportunistiche di *defacement*, ossia di alterazione dei contenuti dei siti web, condotte attraverso lo sfruttamento di vulnerabilità presenti nei plugin e in altri componenti dei CMS[1]. In alcuni casi, gli **attacchi web-based** hanno determinato conseguenze ulteriori rispetto all'alterazione dei contenuti, tra cui l'accesso non autorizzato a dati o l'indisponibilità dei servizi.

Sul tema, il **CSIRT Italia** ha continuato a pubblicare avvisi specifici sulle vulnerabilità dei CMS e dei servizi web, in continuità con le segnalazioni diffuse nei mesi precedenti per altri prodotti. Tra questi figurano gli avvisi relativi a Craft CMS e Drupal, nonché quello dedicato alle vulnerabilità critiche di PHP note come PHP2Shell, con indicazioni sugli aggiornamenti di sicurezza e sulle ulteriori misure di mitigazione da adottare.

Contromisure – Defacement

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

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

Anche per quanto sopra descritto, nel mese di ottobre 2026 sono stati registrati **691 eventi**, in **aumento** del 42% rispetto ai **487** di settembre. Anche gli **incidenti** sono risultati in **aumento**: **394** rispetto a **271** .

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

Complessivamente nel corso del mese di ottobre 2026, le minacce più frequenti negli eventi sono state **DDoS**, **Attacco web-based** e **Compromissione casella email**.

- **Settori interessati**

  I settori con il maggior numero di vittime di eventi cyber sono stati **Tecnologico**, **Pubblica amministrazione locale** e **Telecomunicazioni**. Nel settore Tecnologico sono prevalsi gli attacchi web-based e i DDoS; il settore Pubblica amministrazione locale è stato interessato principalmente da attacchi DDoS, mentre nel settore Telecomunicazioni sono prevalse le compromissioni delle caselle e-mail.

- **Ransomware**

  Nel mese di ottobre, gli attacchi ransomware, individuati da ACN tramite le attività di monitoraggio dei *data leak site* o segnalati dai soggetti impattati, hanno interessato prevalentemente i settori **Manifatturiero**, **Commercio all'ingrosso e al dettaglio** e **Tecnologico**. Tra le modalità di accesso iniziale individuate figurano l'impiego di **credenziali valide** precedentemente compromesse, il ricorso alla **posta elettronica** e lo sfruttamento di compromissioni di altri soggetti nella **supply chain**.

> **Contromisure – Ransomware**
>
> Le **principali** misure per evitare questo tipo di incidente sono:
> - aggiornamento tempestivo dei software, con priorità agli apparati perimetrali, per sanare vulnerabilità note;
> - utilizzo di politiche di autenticazione a più fattori e adozione del principio del privilegio minimo per gli account;
> - gestione separata e protetta degli ambienti di virtualizzazione e dei sistemi di archiviazione, mediante credenziali amministrative dedicate;
> - segmentazione della rete e soluzioni EDR/XDR;
> - mantenimento copie di backup separate, non alterabili e verificate periodicamente con prove di ripristino.
>
> Per approfondimenti, è disponibile sul sito web ACN il documento: "Caratteristiche, preparazione e risposta agli attacchi ransomware".

- **Attacchi DDoS**

  Nel mese di ottobre 2026, si è registrata una significativa intensificazione delle attività di matrice hacktivista in ambito europeo. Le evidenze indicano una maggiore concentrazione delle azioni contro **Italia** e **Francia**, con ulteriori iniziative nei confronti di **Repubblica Ceca** e **Germania**.

  Per quanto riguarda il nostro Paese, la campagna di ottobre si colloca tra le più estese per numero di soggetti interessati e durata: avviata il 5 ottobre, ha interessato obiettivi italiani in 23 giornate del mese, con una sequenza massima di 13 giorni consecutivi, dal 18 al 30 ottobre, coinvolgendo anche domini web non emersi nelle precedenti campagne. Gli attacchi hanno interessato prevalentemente società di trasporti, amministrazioni locali e centrali, fornitori di servizi digitali e operatori della logistica. Anche grazie all'attività di allertamento svolta dal **CSIRT Italia** nei confronti dei soggetti individuati tra i possibili target, **a fronte di 249 eventi censiti, sono stati accertati impatti soltanto in circa l'8% dei casi**. Le conseguenze sono risultate generalmente limitate e prevalentemente circoscritte a rallentamenti o temporanee indisponibilità di siti e servizi web, senza evidenze generalizzate di compromissione dei sistemi o perdita di dati.

> **Contromisure – DDoS**
>
> - acquisire servizi e soluzioni anti-DDoS volumetriche, in cloud, on premise o ibride, fornite da ISP o altri operatori specializzati;
> - predisporre un piano di risposta e misure di mitigazione da attivare in caso di attacco, tra cui restrizioni geografiche e limitazioni selettive dei servizi esposti;
> - prevedere la ridondanza della connettività e, ove opportuno, il ricorso a ISP differenti;
> - utilizzare dispositivi di rete con funzionalità anti-DDoS e di Deep Packet Inspection (DPI), configurati per rilevare e filtrare il traffico anomalo.
>
> Per approfondimenti, è disponibile sul sito web ACN il documento: "Preparazione e risposta agli attacchi Denial of Service".

- **Vettori di attacco**

  Nel mese di ottobre 2026 lo **sfruttamento di vulnerabilità** è risultato il principale vettore di accesso iniziale, a conferma delle campagne di sfruttamento opportunistico, anche supportate da strumenti di AI; 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**
  Ad ottobre 2026, il *Common Vulnerabilities and Exposures* (**CVE**) Program[2] ha pubblicato **17.481** nuovi record relativi a vulnerabilità di cybersicurezza, in **aumento** (**+2.407**) rispetto a settembre. Di questi, **615** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (**+274**), e per **20** CVE è stato rilevato lo sfruttamento attivo, in **diminuzione** (**–5**) rispetto a settembre.
  Tra queste, ACN ha rivolto particolare attenzione, con specifiche campagne di allertamento, ad alcune vulnerabilità relative a prodotti ampiamente utilizzati per la gestione dei server, della posta elettronica e dell'accesso remoto sicuro alle risorse aziendali.
  In questo ambito, nel 2026 si osserva una crescita senza precedenti del numero di vulnerabilità censite, con oltre **92.000 CVE registrate nei primi dieci mesi dell'anno**. Tale accelerazione si colloca in un contesto caratterizzato dal crescente impiego di **modelli di AI di frontiera**, in grado di ridurre sensibilmente i tempi necessari per l'analisi del codice, la ricerca di vulnerabilità e la generazione di *proof of concept*.

- **Monitoraggio proattivo e allertamento**
  L'attività di monitoraggio della superficie esposta ha consentito di individuare ad ottobre 2026 **16.593 sistemi e servizi a rischio**, in sensibile **aumento** (+8.380) rispetto a settembre. All'incremento hanno contribuito in misura prevalente le attività preventive del CSIRT Italia sui sistemi di gestione della **catena del freddo** e sui servizi web potenzialmente vulnerabili a **PHP2Shell**.

> **Focus – Catena del freddo**
> Nella notte tra l'11 e il 12 ottobre una campagna di compromissione ha colpito in Francia i sistemi di controllo della refrigerazione di centinaia di supermercati: l'attivazione remota dei cicli di sbrinamento e la modifica dei parametri operativi degli impianti hanno interrotto la catena del freddo, causando ingenti danni economici. Al fine di prevenire analoghi episodi sul territorio nazionale, il CSIRT Italia ha avviato verifiche sui sistemi accessibili da Internet impiegati per monitorare e regolare gli **impianti di refrigerazione**, anche in raccordo con produttori e distributori, e ha pubblicato un bollettino con le misure urgenti di verifica e mitigazione. Pur in assenza di impatti rilevati in Italia, l'attività ha consentito di individuare i soggetti potenzialmente esposti e di inviare loro, **tra il 12 e il 16 ottobre, 4.057 comunicazioni contenenti le misure di mitigazione da adottare**. L'azione preventiva ha contribuito a ridurre il rischio di compromissione e a contenere i potenziali impatti sulla continuità operativa degli impianti.

Tra le ulteriori attività di monitoraggio, a seguito della pubblicazione delle vulnerabilità note come **PHP2Shell**, l'ACN ha avviato un'attività volta ad individuare i servizi web basati su versioni vulnerabili di **PHP**[3]. Su oltre **740.000 servizi PHP rilevati in Italia**, circa **285.000** utilizzavano versioni potenzialmente vulnerabili, pari all'**82% dei servizi per i quali è stato possibile identificare la versione in uso**. I gestori dei domini potenzialmente interessati sono stati conseguentemente allertati per consentire le necessarie verifiche e la tempestiva adozione delle misure di mitigazione. Ulteriori dettagli nell'alert AL07/261021/CSIRT-ITA sul sito web ACN.

L'analisi di dati provenienti da malware di tipo infostealer, altresì, ha consentito di identificare **473 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 **24.398**, in sensibile **aumento** (+13.559) rispetto a settembre.

[2] 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.

[3] Linguaggio di scripting impiegato per lo sviluppo di applicazioni web lato server.

I NUMERI - OTTOBRE 2026

EVENTI, INCIDENTI E VITTIME	APRILE	MAGGIO	GIUGNO	LUGLIO	AGOSTO	SETTEMBRE	OTTOBRE
Eventi cyber	266	389	421	305	304	487	691
Incidenti con impatto confermato	174	161	179	188	193	271	394
Vittime	346	462	496	354	365	1.041	884

MONITORAGGIO E ALLERTAMENTO	APRILE	MAGGIO	GIUGNO	LUGLIO	AGOSTO	SETTEMBRE	OTTOBRE
Asset potenzialmente compromessi	126	73	1.244	1.095	572	32	28
Asset potenzialmente vulnerabili	2.212	11.984	4.236	3.210	9.121	8.213	16.593
Comunicazioni inviate	7.229	11.917	8.754	8.952	8.382	10.839	24.398
Alert sito web	101	115	128	106	143	155	184

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

- **691** eventi cyber, in **aumento** (**+204**);
- **884** vittime[4], in **diminuzione** (**–157**);
- **367** vittime della constituency[5], in **diminuzione** (**–151**);
- **394** incidenti con impatto confermato, in **aumento** (**+123**);
- **28** asset potenzialmente compromessi, in **diminuzione** (**–4**);
- **16.593** asset potenzialmente vulnerabili, in **aumento** (**+8.380**);
- **184** alert sul sito web del CSIRT Italia, in **aumento** (**+29**);
- **24.398** comunicazioni inviate complessivamente, in **aumento** (**+13.559**);
- **17.481** nuove CVE, in **aumento** (**+2.407**).

[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 ad ottobre 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.

- **AnyDesk** (CVE-2026-109390) Link all'alert
- **Apache** – HTTP Server (CVE-2026-63292) Link all'alert
- **Arista Networks** (CVE-2026-114625) Link all'alert
- **Atlassian** – Bitbucket, Confluence, Jira e altri prodotti Data Center (CVE-2026-21589) Link all'alert
- **BeyondTrust** – Remote Support (CVE-2026-102764) Link all'alert
- **Check Point** – Log Server, Multi-Domain Log Server, Multi-Domain Security Management Server, Security Management Server e SmartEvent (CVE-2026-93616) Link all'alert
- **Cisco** – Secure Email Gateway (CVE-2026-76519) Link all'alert
- **Citrix** – NetScaler ADC, NetScaler Gateway (CVE-2026-88771, CVE-2026-88772) Link all'alert; (CVE-2026-88779) Link all'alert; NetScaler (CVE-2026-107406) Link all'alert
- **Drupal** (CVE-2026-108097) Link all'alert
- **Fortinet** – FortiMail (CVE-2026-104286) Link all'alert
- **GitLab** (CVE-2026-14814, CVE-2026-16301, CVE-2026-81839, CVE-2026-92883, CVE-2026-96893, CVE-2026-97229) Link all'alert e Link all'alert successivo; Community Edition e Enterprise Edition (CVE-2026-19478) Link all'alert
- **Google** – Brotli (CVE-2026-111497) Link all'alert
- **Ivanti** – Connect Secure (CVE-2026-104935) Link all'alert
- **JFrog** – Artifactory (CVE-2026-82329) Link all'alert
- **Langflow** (CVE-2026-105697, CVE-2026-105699, CVE-2026-105740, CVE-2026-105741) Link all'alert
- **Laravel** (CVE-2026-114509) Link all'alert
- **MariaDB** (CVE-2026-102523, CVE-2026-107814, CVE-2026-107815, CVE-2026-107818, CVE-2026-107821, CVE-2026-107823, CVE-2026-85746, CVE-2026-85748, CVE-2026-86047, CVE-2026-92262, CVE-2026-97380) Link all'alert
- **MikroTik** – RouterOS (CVE-2026-84411) Link all'alert
- **Nextcloud** (CVE-2026-110447) Link all'alert
- **Oracle** – E-Business Suite (CVE-2026-101767) Link all'alert
- **PaperCut** – MF e NG (CVE-2026-81578, CVE-2026-82077, CVE-2026-82078) Link all'alert
- **PHP** (CVE-2026-109618, CVE-2026-109619, CVE-2026-115560) Link all'alert
- **SonicWall** – SMA 1000 (CVE-2026-102255, CVE-2026-102256, CVE-2026-102257) Link all'alert
- **Splunk** – Splunk Enterprise (CVE-2026-76268) Link all'alert
- **Zammad** (CVE-2026-102489, CVE-2026-102490) Link all'alert
- **Zimbra Collaboration** (CVE-2026-50056, CVE-2026-50057, CVE-2026-93631, CVE-2026-93639) Link all'alert

Maggiori dettagli nelle sezioni 3 e 5.

2 EVENTI ED INCIDENTI

Ad ottobre 2026 sono stati individuati **691** eventi cyber, in **aumento** del 42% rispetto a settembre. Questi ultimi hanno **interessato, in diversi casi più volte, 684 soggetti nazionali distinti** (di cui 367 appartenenti alla constituency, mentre i restanti hanno riguardato cittadini e società private operanti in settori non critici). Dei 691 eventi cyber, **394 sono stati classificati quali incidenti**, anch'essi in **aumento** rispetto ai 271 di settembre.

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.

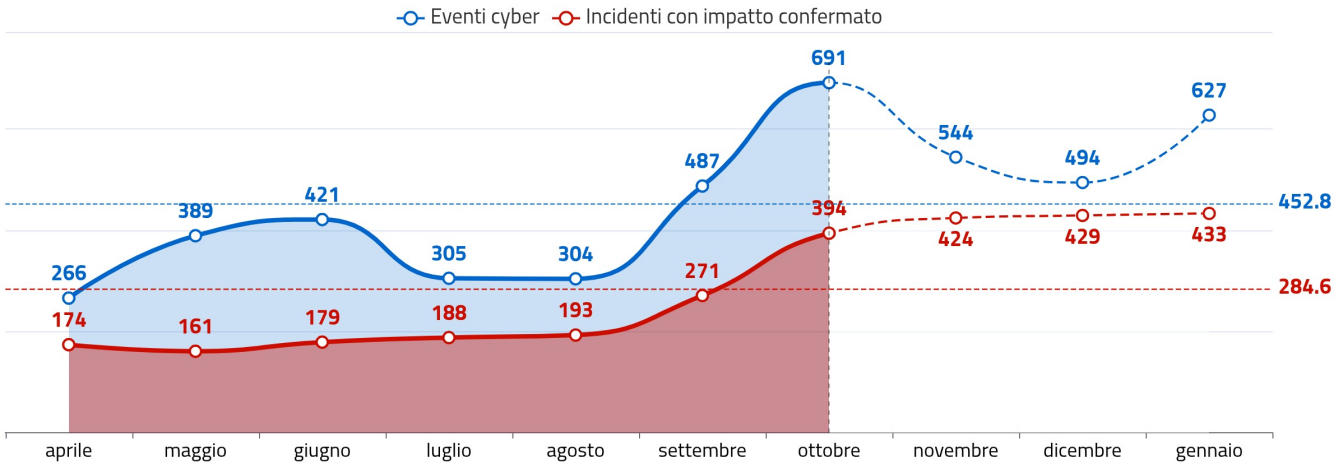


Figura 2 - *andamento attività reattive e analisi previsionale*

[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).

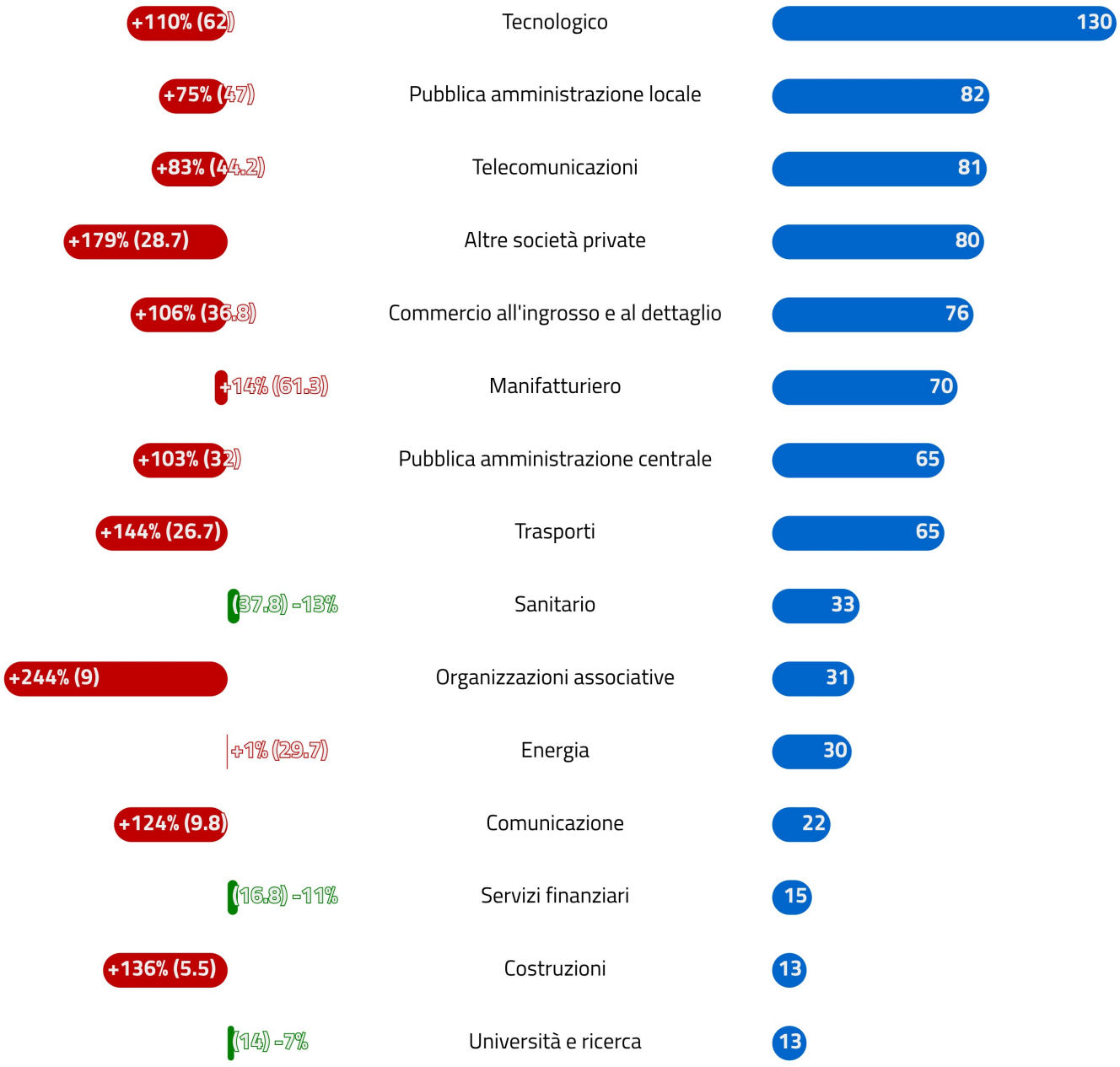


Figura 3 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto alla media del semestre precedente (top 15)*

[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).

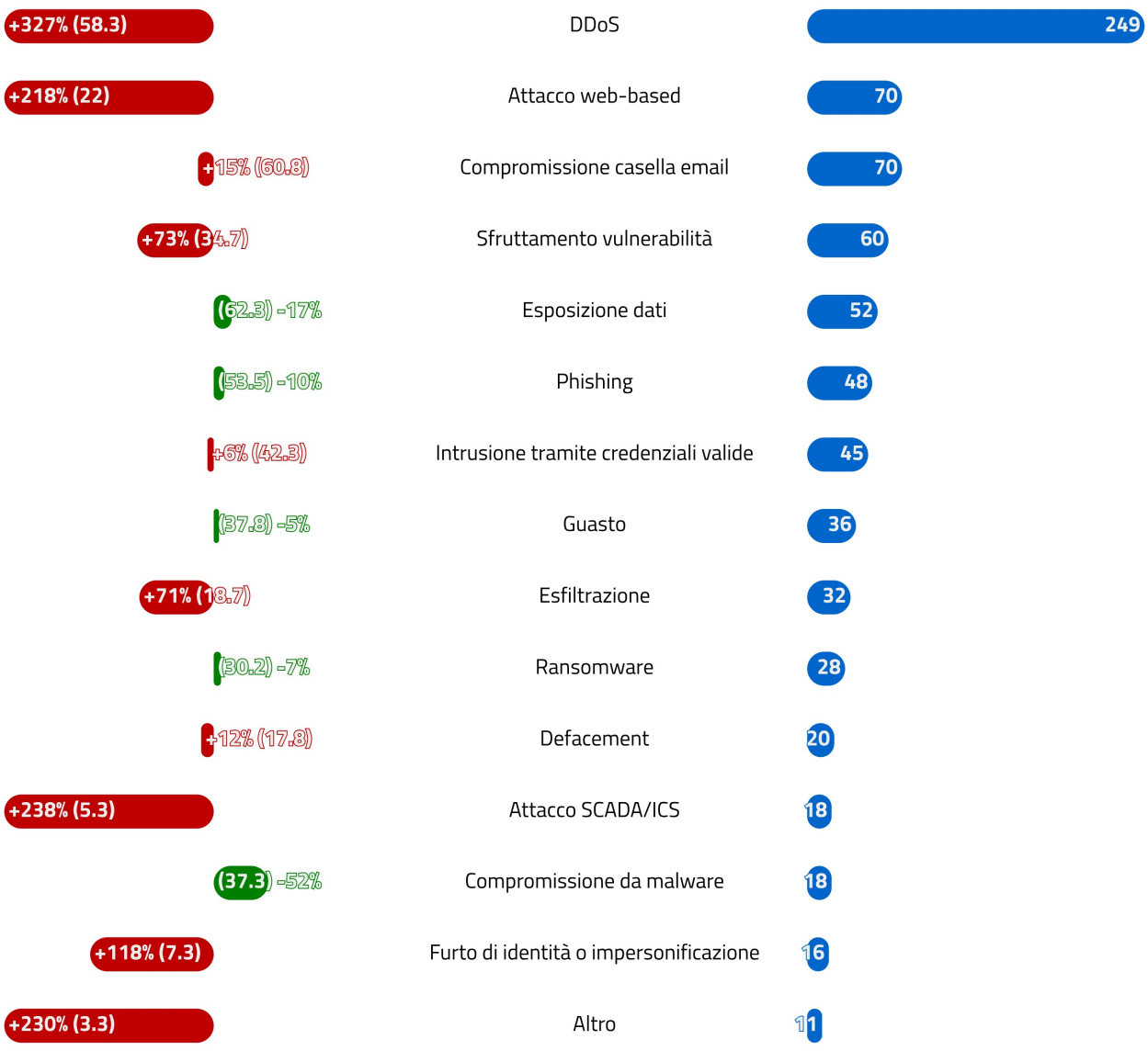


Figura 4 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto alla media del semestre precedente (top 15)*

[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 ottobre 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 691 eventi cyber hanno interessato **684** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

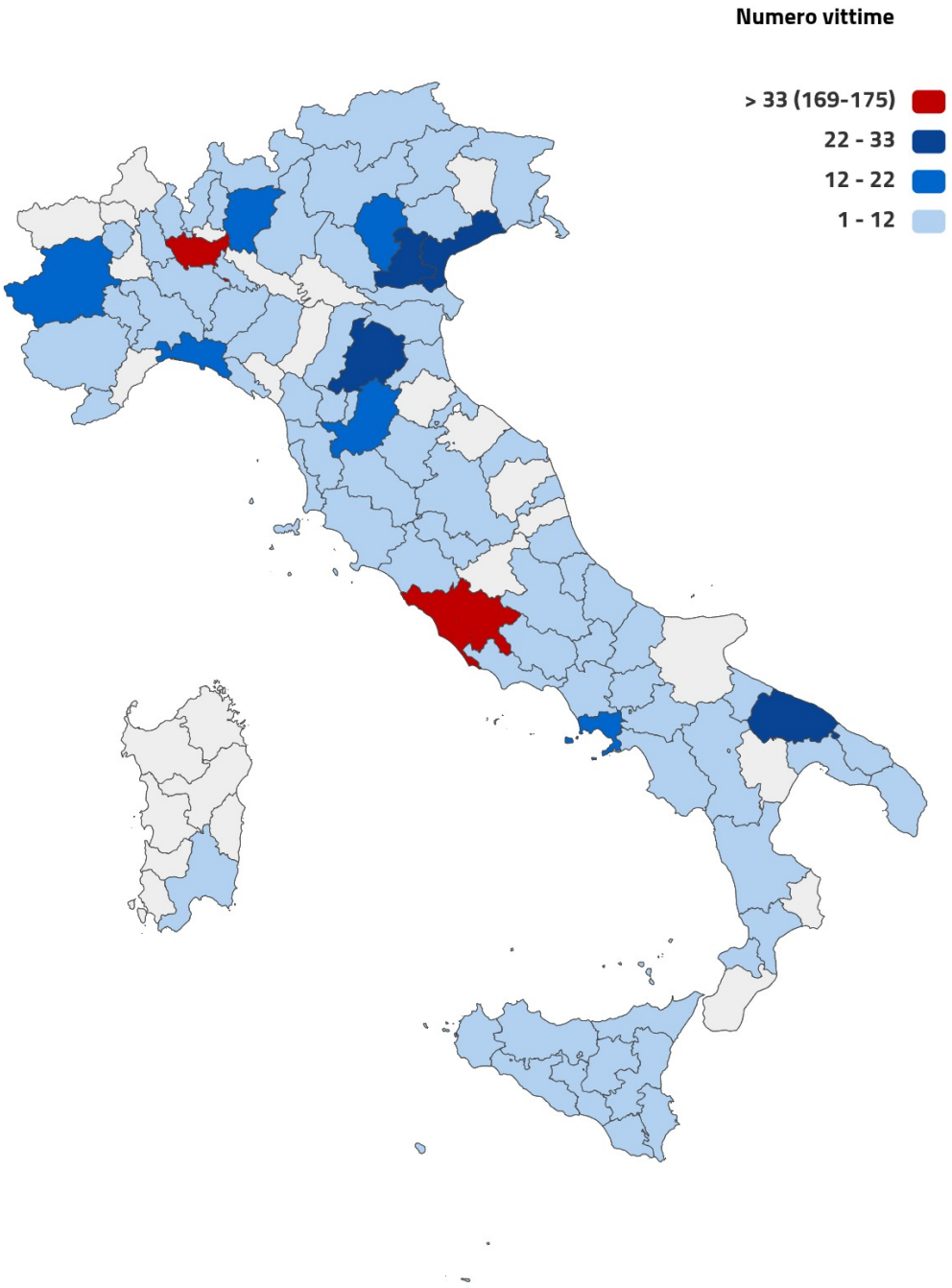


Figura 6 - *distribuzione delle vittime degli eventi cyber*

3 VULNERABILITÀ

Ad ottobre 2026 sono state pubblicate[9] **17.481** nuove CVE, in **aumento** (**+2.407**) rispetto a settembre. Di queste, **615** presentano almeno un *Proof of Concept (PoC)*, in **aumento** (**+274**), e per **20** CVE è stato rilevato lo sfruttamento attivo, in **diminuzione** (**–5**) rispetto a settembre.

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

- **GitLab**: rilasciati aggiornamenti di sicurezza che risolvono 24 vulnerabilità, di cui 1 con gravità "critica" e 5 con gravità "alta", in GitLab Community Edition (CE) ed Enterprise Edition (EE). Tra queste si evidenzia la CVE-2026-97229 per la quale risulta disponibile un Proof of Concept (PoC) in rete (stima di impatto sistemico **79.48/100**). Link all'alert del 12/10/2026;
- **SonicWall**: ha rilasciato aggiornamenti di sicurezza per sanare 4 vulnerabilità, di cui 1 con gravità "critica" e 2 con gravità "alta", che interessano i modelli 6210, 7210 e 8200v appartenenti alla serie SMA1000. Tali vulnerabilità, qualora sfruttate, potrebbero consentire ad un utente malintenzionato di eludere dei meccanismi di sicurezza e di eseguire codice arbitrario sui sistemi interessati (stima di impatto sistemico **79.48/100**). Link all'alert del 07/10/2026;
- **Langflow**: disponibili Proof of Concept (PoC) per lo sfruttamento di 4 nuove vulnerabilità di sicurezza, di cui 2

[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.

con gravità "critica" e 2 con gravità "alta", che interessano il software Langflow, nota piattaforma open-source che permette di costruire, testare e distribuire applicazioni e agenti basati su intelligenza artificiale. Tra queste si evidenzia la CVE-2026-105740 che risulta sfruttata attivamente in rete (stima di impatto sistemico **79.35/100**). Link all'alert del 06/10/2026;

- **Arista Networks**: Arista Networks ha rilevato lo sfruttamento in rete di una vulnerabilità con gravità "critica", identificata tramite la CVE-2026-114625, in VeloCloud Orchestrator (VCO) On-Prem, piattaforma di gestione e orchestrazione centralizzata per infrastrutture SD-WAN, utilizzata per la configurazione, il monitoraggio e l'amministrazione delle reti VeloCloud (stima di impatto sistemico **79.35/100**). Link all'alert del 23/10/2026;
- **MariaDB**: risolte molteplici vulnerabilità, di cui 3 con gravità "critica" e 8 con gravità "alta", in MariaDB Server, noto database relazionale open source compatibile con MySQL, ampiamente impiegato per la gestione di dati strutturati in applicazioni web e ambienti enterprise (stima di impatto sistemico **79.35/100**). Link all'alert del 12/10/2026;

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].

Il numero particolarmente elevato di vulnerabilità attribuite ai primi vendor è riconducibile al *Patch Tuesday* di ottobre di **Microsoft**, che ha corretto oltre 1.400 vulnerabilità, valore per la prima volta oltre quota 1.000 in un solo mese, mentre per **Oracle**, a cui sono attribuite 1.078 vulnerabilità, il dato riflette anche il *Critical Patch Update* trimestrale pubblicato il 20 ottobre. Per il **kernel Linux** la crescita riflette l'aumento delle vulnerabilità individuate grazie all'impiego di strumenti di AI[12].

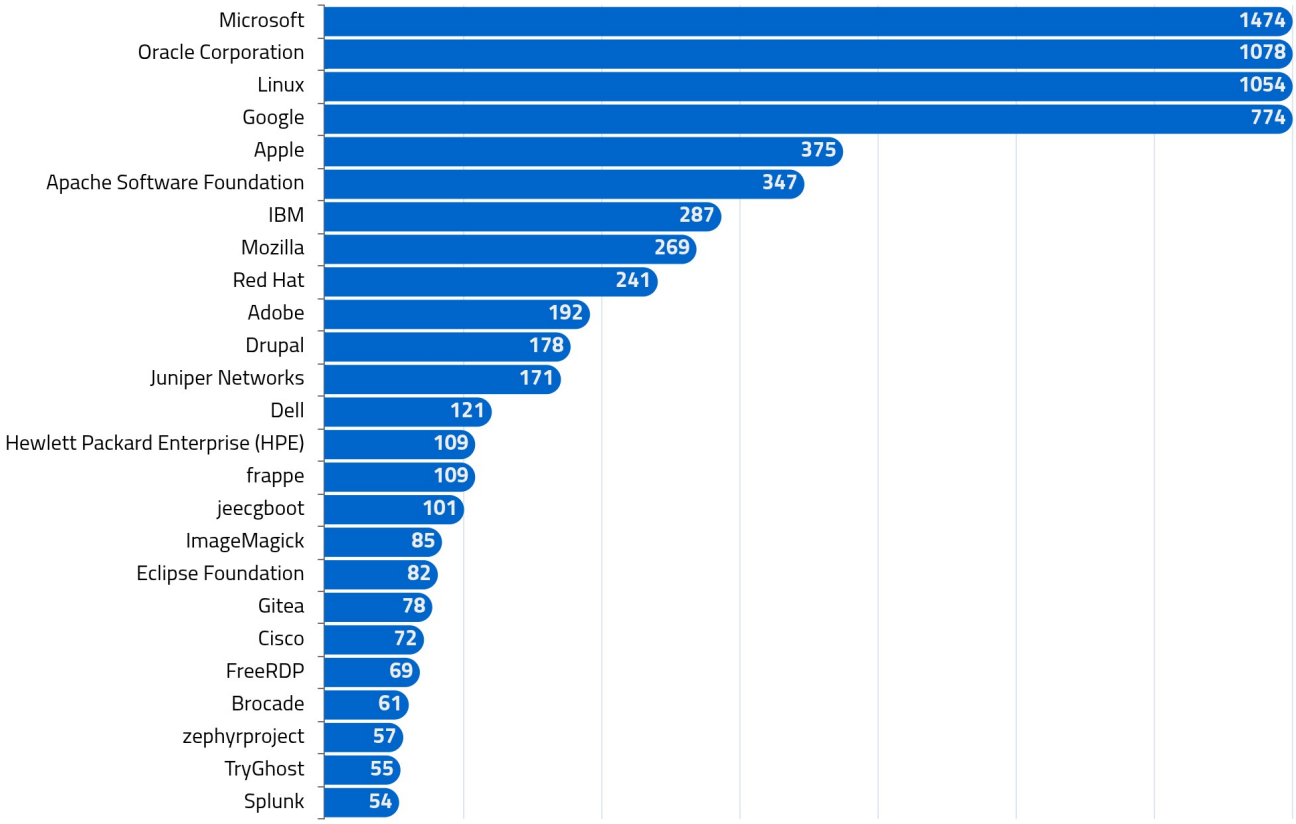


Figura 7 - *top 25 produttori affetti da vulnerabilità nel mese*

[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

[12] A titolo di esempio, OpenAI ha riportato che un proprio prototipo basato su agenti AI, eseguito sul kernel a metà ottobre, ha riprodotto 1.724 vulnerabilità e generato 948 exploit funzionanti per l'acquisizione di privilegi di root *Mille vie in meno per ottenere l'accesso root*, 4 novembre 2026.

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

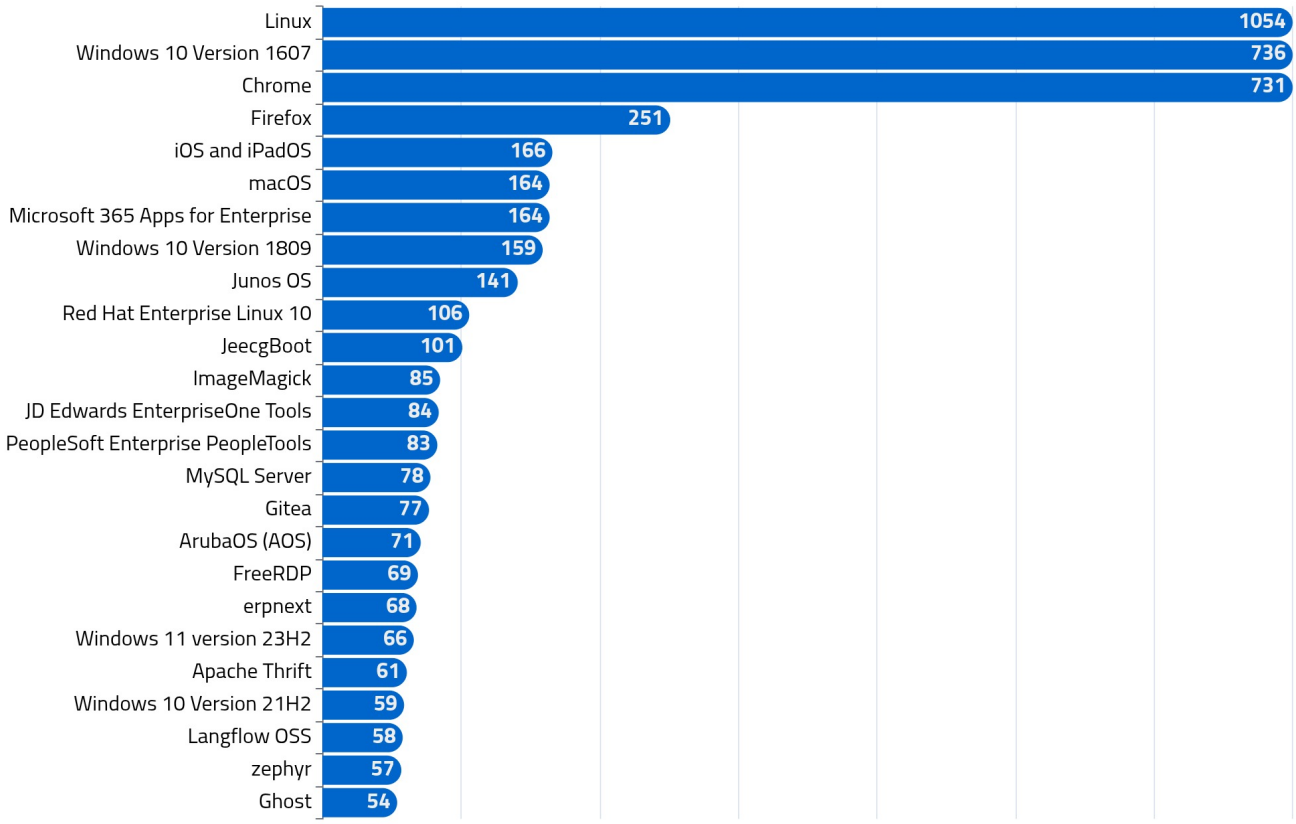


Figura 8 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

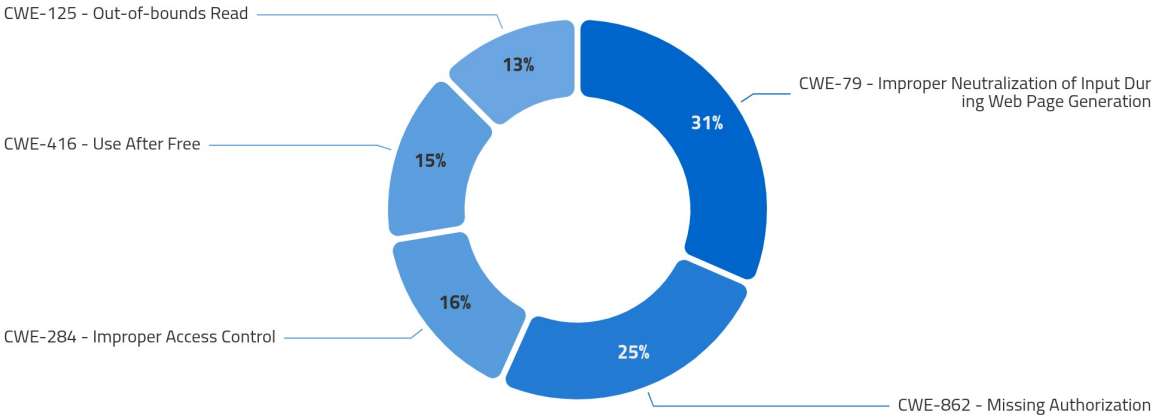


Figura 9 - *top 5 CWE nel mese*

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	**PHP Group**
Prodotti e versioni vulnerabili	**PHP versioni da 8.2.* a versioni antecedenti la 8.2.35; da 8.3.* a versioni antecedenti la 8.3.36; da 8.4.* a versioni antecedenti la 8.4.27; da 8.5.* a versioni antecedenti la 8.5.12**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante non autenticato di eseguire codice arbitrario da remoto.**
Data di rilascio CVE	**21/10/2026 modificata il 04/11/2026**
CVSS score 4.0	**9.2 Critical**
EPSS max score	**0.99**

Tabella 1 - *CVE-2026-109618*

Vendor	**Ivanti**
Prodotti e versioni vulnerabili	**Ivanti Connect Secure versioni fino alla 25.1.1.1; versioni fino alla 25.1.2.2; versioni fino alla 2.8R2.4**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante remoto di eludere i controlli di accesso ed eseguire comandi arbitrari sul sistema.**
Data di rilascio CVE	**13/10/2026 modificata il 13/10/2026**
CVSS score 3.0	**8.6 High**
EPSS max score	**0.86**

Tabella 2 - *CVE-2026-104935*

[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	**Citrix NetScaler**
Prodotti e versioni vulnerabili	**Citrix NetScaler ADC e Citrix NetScaler Gateway versione 14.1 e precedenti la 14.1-73.37 Citrix NetScaler ADC e Citrix NetScaler Gateway versione 13.1 e precedenti la 13.1-64.23 Citrix NetScaler ADC FIPS versioni precedenti la 14.1-73.37 FIPS Citrix NetScaler ADC FIPS e NDcPP versioni precedenti la 13.1-37.279**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette ad un attaccante remoto di eludere i controlli di accesso ed eseguire comandi arbitrari sul sistema.**
Data di rilascio CVE	**27/09/2026 modificata il 29/09/2026**
CVSS score 4.0	**9.5 Critical**
EPSS max score	**0.82**

Tabella 3 - *CVE-2026-88771*

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 ottobre 2026, l'11% degli attacchi ransomware ha colpito soggetti critici, il 36% ha colpito soggetti a media criticità, ed il restante 53% ha coinvolto altri soggetti a criticità minore.

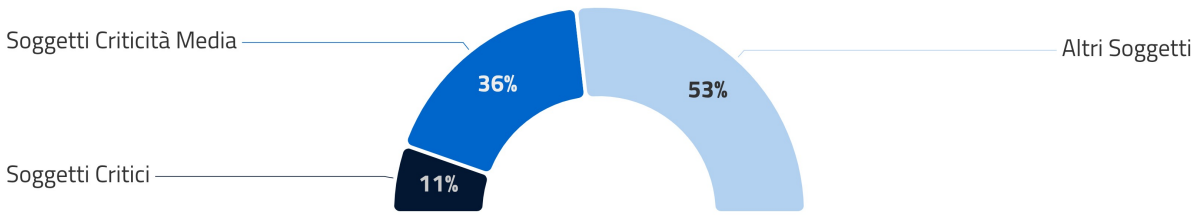


Figura 10 - *distribuzione delle vittime di ransomware in base alla loro criticità*

[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 ottobre 2026 ha permesso di individuare **22** 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.

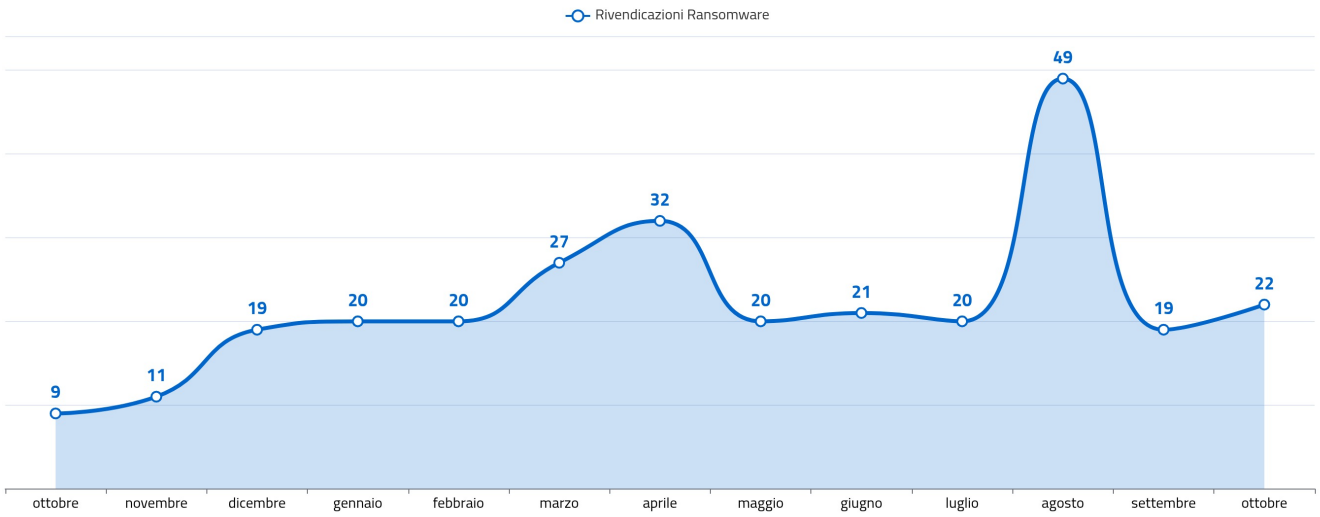


Figura 11 - *andamento delle rivendicazioni ransomware per l'Italia*

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

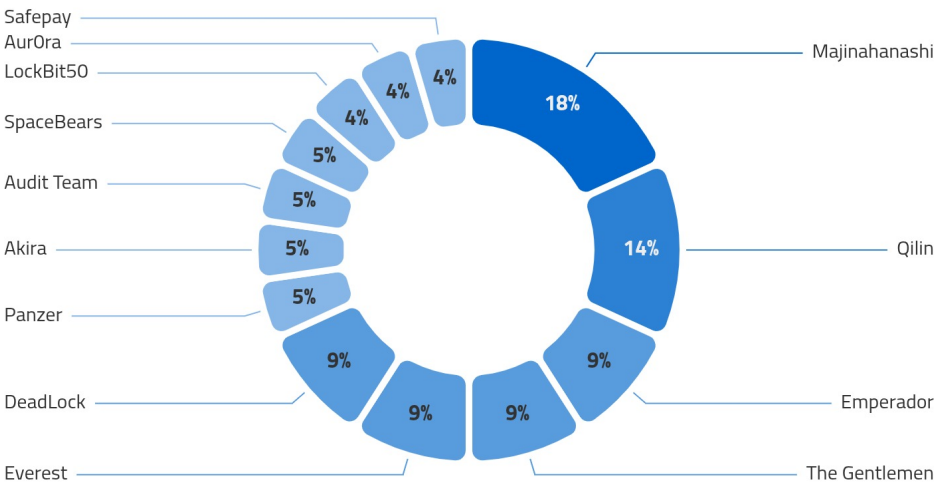


Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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

4.3 Rivendicazioni DDoS

Ad ottobre 2026 sono state individuate[17] **146** 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.

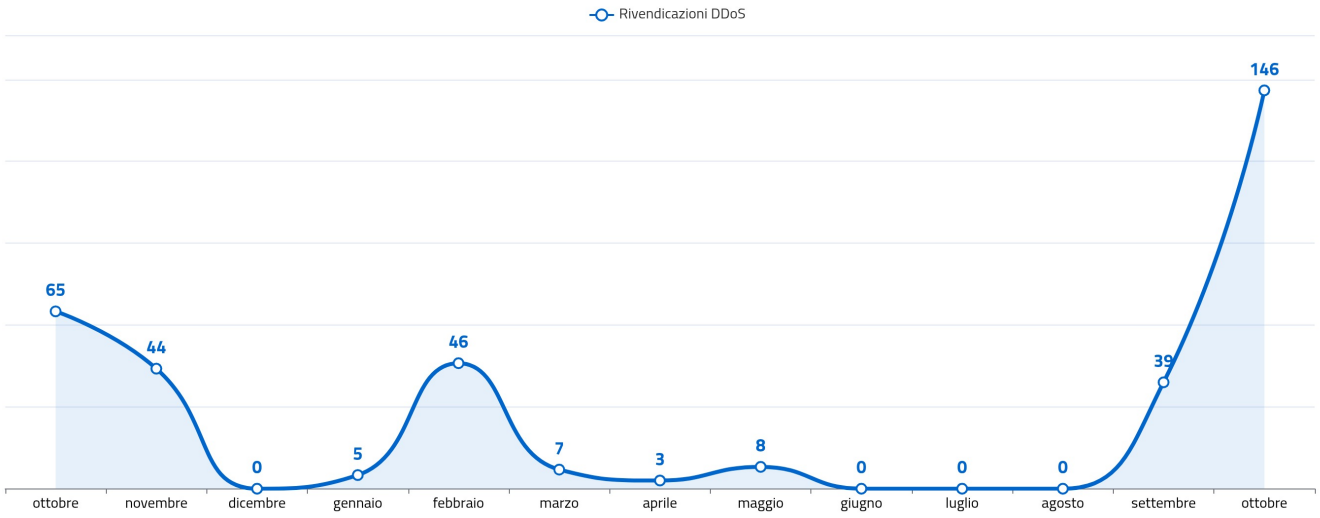


Figura 13 - *andamento delle rivendicazioni DDoS riferite all'Italia*

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

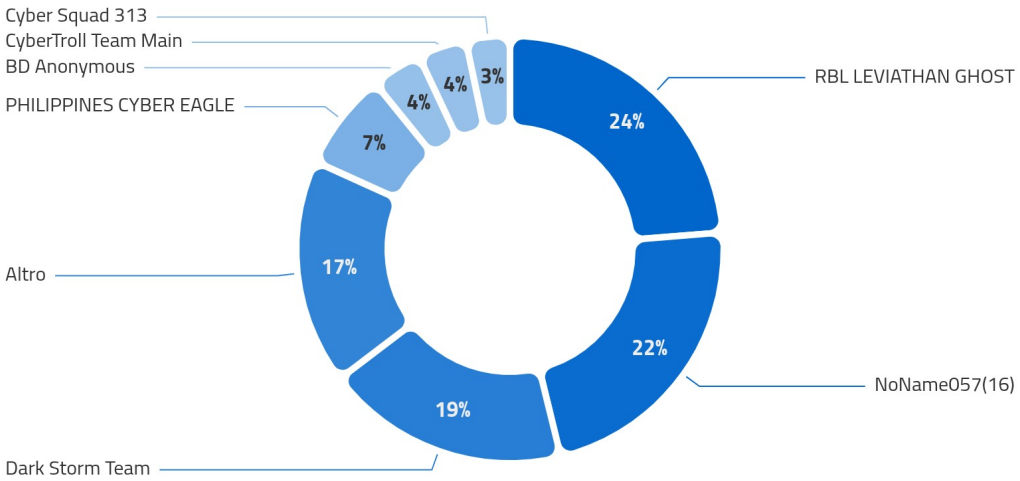


Figura 14 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

[17] 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.

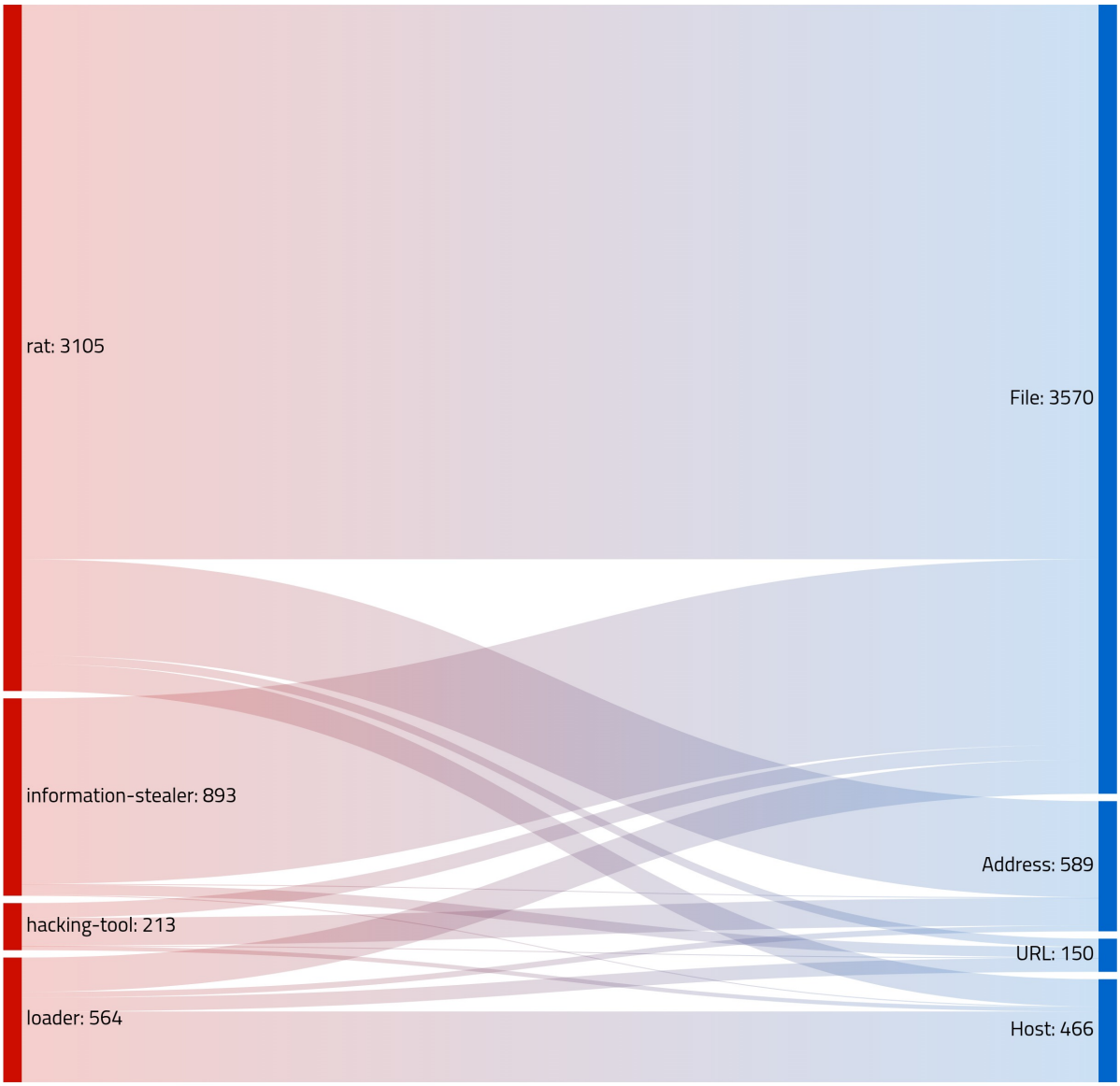


Figura 15 - *numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware*

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[18], 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 ottobre 2026 sono state diramate un totale di **6.894** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su internet complessivamente **16.593** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **PHP CORE** (CVE-2026-109618, CVE-2026-109619, CVE-2026-115560): tali vulnerabilità – di tipo *Use after free* – permetterebbero a un eventuale attaccante remoto non autenticato di eseguire codice remoto sulla macchina. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Moxa MGate** (CVE-2026-86325, CVE-2026-86326): tali vulnerabilità – rispettivamente di tipo *Stack-based Buffer Overflow* e *Improper Verification of Cryptographic Signature* – permetterebbero a un eventuale attaccante remoto di compromettere i dispositivi interessati permettendo l'accesso a informazioni sensibili negli apparati, la modifica arbitraria della memoria e, nei casi più gravi, l'esecuzione di codice non autorizzato mediante l'installazione di firmware appositamente manipolato.
- **Citrix NetScaler Gateway e NetScaler ADC** (CVE-2026-88779): tale vulnerabilità – di tipo *Memory Overflow* e con CVSS 4.0 8.7. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Zimbra Collaboration** (CVE-2026-50056, CVE-2026-50057, CVE-2026-93631, CVE-2026-93639): tali vulnerabilità - di tipo rispettivamente *Argument Injection*, *Incorrect Permission Assignment for Critical Resource*, *Cross-Site Request Forgery (CSRF)* e *Missing Authorization* - potrebbero consentire la compromissione di account e sessioni utente, con

[18] 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.

accesso non autorizzato a dati e funzionalità di Zimbra Collaboration Suite. Il loro sfruttamento combinato potrebbe inoltre portare all'elevazione dei privilegi fino a root, determinando il controllo completo del sistema interessato. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **Microsoft Exchange** (CVE-2026-96940): tale vulnerabilità – di tipo *Weak Authentication* – permetterebbe a un eventuale attaccante di elevare i propri privilegi a seguito dell'autenticazione al sistema, ottenendo accesso non autorizzato alle caselle di posta di altri utenti appartenenti alla medesima organizzazione e consentendo la consultazione di messaggi di posta elettronica e relativi allegati.
- **Apache HTTP Server** (CVE-2026-63292): tale vulnerabilità – di tipo *Stack-based Buffer Overflow* – permetterebbe a un eventuale attaccante di eseguire codice arbitrario da remoto mediante richieste HTTP appositamente predisposte. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Check Point Security Management Server, Multi-Domain Security Management Server, Log Server, SmartEvent e Multi-Domain Log Server** (CVE-2026-93616): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe, tramite l'invio di richieste opportunamente predisposte, a un eventuale attaccante remoto non autenticato di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **GitLab** (CVE-2026-97229): tale vulnerabilità – di tipo *Integer Overflow or Wraparound* – permetterebbe a un eventuale attaccante, sotto determinate condizioni, di eseguire codice arbitrario, eludere dei meccanismi di sicurezza e accedere ad informazioni sensibili sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **NextCloud** (CVE-2026-110447): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante non autenticato – e senza interazione utente, laddove il servizio "CODE" integrato non sia in esecuzione – di eseguire comandi arbitrari sul sistema sottostante mediante l'invio di richieste appositamente predisposte all'endpoint proxy.php dell'applicazione vulnerabile. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Citrix NetScaler** (CVE-2026-107406): tale vulnerabilità – di tipo *Improper Restriction of Operations within the Bounds of a Memory Buffer* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario sul dispositivo NetScaler. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Laravel** (CVE-2026-114509): tale vulnerabilità – di tipo *Improper Authentication* – permetterebbe a un eventuale attaccante di eludere i meccanismi di autenticazione sui sistemi interessati, consentendo di impersonare un altro utente. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Drupal** (CVE-2026-108097): tale vulnerabilità – di tipo *Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')* – permetterebbe a un eventuale attaccante remoto non autenticato di eseguire codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Mikrotik RouterOS** (CVE-2026-84411): tale vulnerabilità – di tipo *Integer Underflow (Wrap or Wraparound)* – permetterebbe a un eventuale attaccante remoto non autenticato di eseguire codice arbitrario con privilegi di root o di compromettere la disponibilità del servizio sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Ivanti Connect Secure** (CVE-2026-104935): tale vulnerabilità – di tipo *Authentication Bypass by Spoofing* – permetterebbe a un eventuale attaccante remoto non autenticato di eseguire codice arbitrario nei sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **FortiNet FortiMail** (CVE-2026-104286): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante remoto non autenticato di sfruttare tale criticità inviando richieste HTTP/HTTPS opportunamente predisposte volte ad alterare l'interpretazione dell'input da parte dell'applicazione, ottenendo la scrittura arbitraria di file e la successiva esecuzione di codice o comandi non autorizzati sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **GitLab Enterprise Edition e Community Edition** (CVE-2026-19478): tale vulnerabilità – di tipo *Improper Control of Generation of Code ('Code Injection')* – qualora sfruttata, potrebbe consentire ad un eventuale attaccante non autenticato di alterare i dati e di aggirare i meccanismi di sicurezza implementati sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Mautic** (CVE-2026-115188): tali vulnerabilità – rispettivamente di tipo *Unrestricted Upload of File with Dangerous Type e Improper Control of Generation of Code ("Code Injection")* – permetterebbero a un eventuale attaccante autenticato di caricare ed eseguire codice arbitrario sul server vulnerabile, ottenendo il controllo del sistema e l'accesso non autorizzato a dati, credenziali, configurazioni e funzionalità dell'applicativo compromesso.
- **Google Brotli** (CVE-2026-111497): tale vulnerabilità – di tipo *Out-of-bounds Write* – permetterebbe a un attaccante di causare la corruzione della memoria di un'applicazione Node.js mediante l'invio di dati Brotli malevoli, determinando potenzialmente condizioni di Denial of Service (DoS), la divulgazione di informazioni sensibili e l'esecuzione di codice arbitrario, con conseguenti impatti sulla riservatezza, integrità e disponibilità del sistema. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Zammad** (CVE-2026-102489, CVE-2026-102490): tali vulnerabilità – rispettivamente di tipo *Session Hijacking* e *Local Privilege Escalation* – permetterebbero a un eventuale attaccante remoto di eseguire codice arbitrario da remoto sul sistema target tramite l'utenza "zammad" (CVE-2026-102489) e di elevare i propri privilegi a quelli di root (CVE-2026-102490). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **SonicWall SMA 1000** (CVE-2026-102255): tale vulnerabilità – di tipo *Server-Side request forgery (SSRF)* – permetterebbe a un eventuale attaccante non autenticato di lanciare comandi interni ed eseguire operazioni non autorizzate. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Atlassian** – Bitbucket, Confluence, Jira e altri prodotti Data Center (CVE-2026-21589): tale vulnerabilità – di tipo *Files or Directories Accessible to External Parties* – permetterebbe a un eventuale attaccante di accedere a specifici file – anche di natura potenzialmente sensibile – all'interno della cartella root del relativo web server dei prodotti affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **AnyDesk** (CVE-2026-109390): tale vulnerabilità – di tipo *Heap-Based Buffer Overflow* – permetterebbe a un eventuale attaccante remoto non autenticato di sfruttare un'inadeguata validazione del parametro payload length del protocollo di sessione provocando una corruzione della memoria heap ed ottenere l'esecuzione di codice arbitrario con privilegi elevati sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **PaperCut MF e NG** (CVE-2026-81578, CVE-2026-82077, CVE-2026-82078): tali vulnerabilità – rispettivamente di tipo *Path Traversal*, *Unsafe Reflection* e *Authentication Bypass* – permetterebbero, laddove utilizzate in maniera congiunta, a un eventuale attaccante non autenticato di eseguire da remoto codice arbitrario sui sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **BeyondTrust Remote Support** (CVE-2026-102764): tale vulnerabilità – di tipo *Authentication bypass by Spoofing* – permetterebbe a un eventuale attaccante di effettuare operazioni non autorizzate sui file dell'appliance interessata. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Citrix Netscaler ADC e Gateway** (CVE-2026-88771, CVE-2026-88772): tali vulnerabilità – rispettivamente di tipo *Improper input validation* e *Improper Restriction of Operations within the Bounds of a Memory Buffer* – permetterebbero a un eventuale attaccante remoto di eseguire comandi arbitrari, eseguire codice da remoto o compromettere la disponibilità del servizio sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Splunk Enterprise** (CVE-2026-76268): tale vulnerabilità – di tipo *Missing Authentication for Critical Function* – permetterebbe a un eventuale attaccante non autenticato con accesso di rete alla Patroni API REST di un Search Head Cluster di eseguire comandi arbitrari sul sistema operativo dei sistemi affetti. Ulteriori dettagli nell'alert sul

sito dello CSIRT Italia.

- **JFrog Artifactory** (CVE-2026-82329): tale vulnerabilità – di tipo *Authentication Bypass* – permetterebbe a un eventuale attaccante remoto non autenticato di ottenere privilegi amministrativi completi su istanze vulnerabili. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Cisco Secure Email Gateway** (CVE-2026-76519): tale vulnerabilità – di tipo *Relative Path Traversal* – permetterebbe a un eventuale attaccante non autenticato, laddove il modulo di Advanced Malware Protection (AMP) sia presente e attiva la funzionalità di analisi della reputazione dei file allegati, di scrivere file arbitrari e di eseguire con i privilegi di root comandi arbitrari sul sistema operativo dei sistemi affetti mediante l'invio di e-mail contenenti allegati appositamente predisposti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Oracle E-Business Suite** (CVE-2026-101767): tale vulnerabilità – di tipo Missing Authentication for Critical Function – permetterebbe a un eventuale attaccante non autenticato di eseguire comandi arbitrari sul sistema operativo per tramite del Concurrent Manager dell'applicativo, sfruttando una vulnerabilità di tipo SQL Injection per mezzo di richieste POST appositamente predisposte verso i sistemi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

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

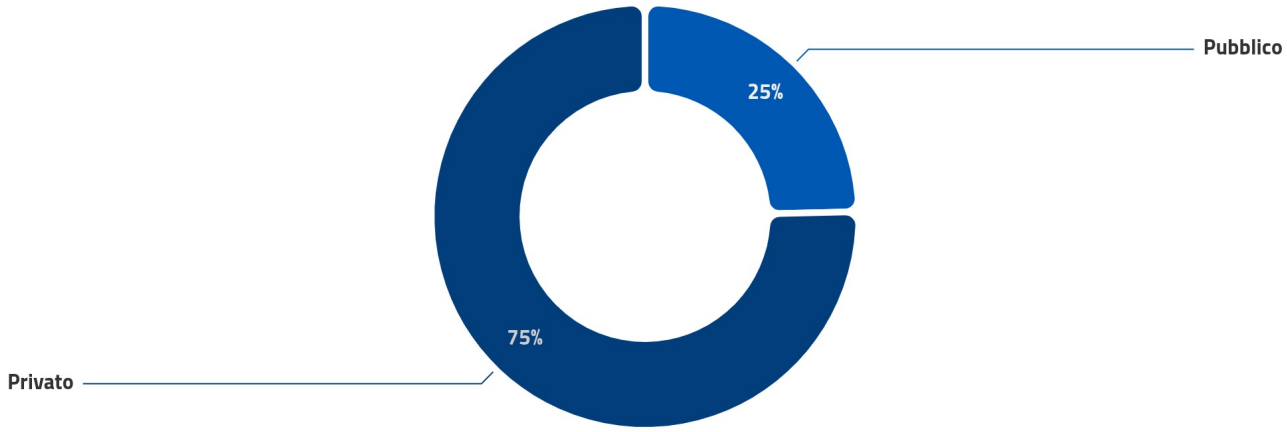


Figura 16 - *distribuzione delle segnalazioni per tipologia di soggetto*

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 dalle fonti aperte nel mese in esame. Approfondisce inoltre alcuni casi di impiego dell'**intelligenza artificiale** nelle attività cyber e alcuni sviluppi della minaccia connessi al **contesto geopolitico**.

6.1 Vulnerabilità e modalità operative

Oltre alle già discusse vulnerabilità PHP2Shell e alla campagna di compromissione degli impianti frigoriferi, di rilievo quanto pubblicato il 15 ottobre da **Google Threat Intelligence Group (Mandiant)** relativo a un'analisi della CVE-2026-102764, vulnerabilità di **BeyondTrust Remote Support** [1]. Nel corso di un'attività di risposta a un incidente, Mandiant ha rilevato evidenze del suo sfruttamento come *zero-day* risalenti alla fine di agosto e ha ricondotto l'attività ad **Armory Castle**, gruppo di spionaggio informatico precedentemente identificato come UNC5221 e ritenuto dalla società collegato alla Repubblica Popolare Cinese. Secondo la ricostruzione tecnica, dopo lo sfruttamento della vulnerabilità gli attaccanti avevano utilizzato funzionalità proprie dell'appliance e configurazioni del *reverse proxy* per elevare i privilegi e mantenere l'accesso. Mandiant ha inoltre rilevato la *webshell* **SAWFLY**, il *tunneler* **BARECLAW** e attività di cancellazione degli artefatti.

Una modalità peculiare di **compromissione della supply chain software** è stata descritta sempre dal **Google Threat Intelligence Group (Mandiant)** in relazione all'infrastruttura di aggiornamento di **AOMEI Technology**, interessata da attività malevole osservate tra aprile e luglio 2026 [2]. Secondo la ricostruzione, l'attore malevolo modificava per

periodi compresi tra cinque e dieci minuti le configurazioni dei server utilizzati per la distribuzione degli aggiornamenti, ripristinandone successivamente la versione legittima. I sistemi che si collegavano all'infrastruttura compromessa per scaricare aggiornamenti legittimi del software ricevevano, in luogo dei componenti attesi, il downloader **CROSSROAD**, componente malevolo utilizzato per scaricare ulteriori file sul sistema, e la backdoor **SHINYROAD**, che consentiva agli attaccanti di mantenere l'accesso al dispositivo compromesso e di eseguire comandi da remoto. La campagna ha interessato organizzazioni dei settori tecnologico, delle telecomunicazioni e dell'istruzione in diversi Paesi, tra cui Portogallo, Spagna e Svizzera. Secondo Mandiant, la distribuzione del malware non era limitata a obiettivi preventivamente selezionati, ma poteva interessare qualsiasi sistema che richiedesse un aggiornamento durante le finestre di compromissione; per tale ragione, il numero delle organizzazioni coinvolte potrebbe essere superiore.

Il 1° ottobre **EUROPOL** ha reso noti i risultati dell'operazione **KillSwitch**, indagine internazionale guidata dalle autorità tedesche nei confronti di **KillSec**, gruppo cybercriminale attivo dal 2024. Il gruppo si introduceva nei sistemi delle organizzazioni sfruttando vulnerabilità e accessi non adeguatamente protetti, in particolare verso servizi di archiviazione cloud, per sottrarre dati. Le vittime venivano successivamente minacciate della pubblicazione dei dati su un apposito sito nel dark web qualora non avessero corrisposto il riscatto richiesto. Nel corso dell'indagine, le autorità hanno sequestrato cinque server, utilizzati anche per gestire le attività del gruppo e conservare i dati sottratti alle vittime, e i domini impiegati da KillSec. Il sito utilizzato per pubblicare i dati è stato reso inaccessibile al gruppo e reindirizzato verso un avviso delle autorità. L'operazione ha portato anche all'arresto provvisorio di tre persone e a otto perquisizioni in Grecia, Romania, Spagna e Regno Unito. Secondo gli investigatori, KillSec sarebbe stato collegato a circa mille attacchi sospetti a livello mondiale[3].

6.2 Intelligenza artificiale

Nel mese di ottobre sono state riportate due nuove evidenze dell'impiego di **framework agentici** in operazioni cyber. Tali strumenti combinano modelli linguistici e strumenti di *penetration testing*, coordinando più agenti software nello svolgimento di attività quali la **ricognizione**, l'**individuazione e lo sfruttamento di vulnerabilità**, l'esecuzione di comandi e il **movimento laterale**. Tali framework automatizzano e conducono in parallelo più fasi dell'intrusione, aumentando la velocità e la scala delle attività offensive.

Il 21 ottobre **Microsoft Threat Intelligence** ha riportato l'impiego di **ARTEX**, framework open source per attività offensive, da parte di **STORM-0940**, attore ritenuto da Microsoft allineato agli interessi statali della Repubblica Popolare Cinese [4]. Secondo la fonte il gruppo avrebbe utilizzato ARTEX in attività rivolte contro centinaia di organizzazioni appartenenti a diversi settori, a livello globale. In più casi, il tempo intercorso tra l'avvio delle attività e l'acquisizione di privilegi elevati nelle infrastrutture cloud delle vittime sarebbe stato **inferiore a tre ore**. Microsoft ha inoltre attribuito a **STORM-0940** la compromissione della supply chain di un'applicazione multi-tenant di **ConnectWise**. L'attore avrebbe successivamente impiegato **ARTEX** per accelerare i tentativi di accesso agli ambienti dei clienti a valle, sfruttando le autorizzazioni già concesse alle applicazioni compromesse. Le attività osservate comprendevano tentativi di autenticazione verso oltre 2.250 tenant, ricognizione attraverso Microsoft Graph, modifica delle credenziali applicative e tentativi di ampliare o mantenere i privilegi acquisiti.

Il 29 ottobre **CrowdStrike** ha descritto un'ulteriore campagna di spionaggio informatico, condotta da **VAPOR PANDA**, attore attivo almeno dal 2021 e ritenuto dalla società collegato alla Repubblica Popolare Cinese. Secondo la fonte, a partire dal 17 ottobre il gruppo avrebbe utilizzato ARTEX contro oltre 200 organizzazioni in almeno 14 Paesi, tra cui amministrazioni pubbliche, rappresentanze governative, centri di ricerca e imprese dei settori farmaceutico, dei semiconduttori, della difesa, nucleare, finanziario e delle telecomunicazioni [5]. Nella campagna osservata, ARTEX utilizzava un agente principale per coordinare agenti specializzati nella pianificazione e nell'esecuzione delle attività.

Questi condividevano informazioni sugli obiettivi, sui sistemi individuati e sui risultati ottenuti, coordinando le attività dall'accesso iniziale alla ricognizione interna e al movimento laterale. Il framework impiegava principalmente il modello linguistico **DeepSeek**, affiancato da un secondo modello non identificato. Gli agenti esploravano contemporaneamente diversi percorsi di compromissione, interessando applicazioni web, servizi cloud, infrastrutture container, Active Directory, sistemi di posta elettronica e servizi VPN. In caso di insuccesso, il framework poteva modificare il percorso seguito e tentare tecniche alternative. Le evidenze raccolte indicano, tuttavia, che ARTEX non operava in completa autonomia. Le trascrizioni analizzate da CrowdStrike mostrano un operatore che impartiva istruzioni in lingua cinese e interveniva nelle principali decisioni operative. In un caso, l'operatore aveva richiesto al framework di individuare i sistemi Windows privi del sensore **CrowdStrike Falcon**: la scelta dell'obiettivo rimaneva quindi affidata all'operatore, mentre agli agenti era demandata la verifica dei singoli sistemi [5].

6.3 Contesto geopolitico

Nel mese di ottobre, oltre alle attività connesse all'impiego del framework **ARTEX**, già descritte nella sezione precedente, è stata documentata un'operazione delle autorità statunitensi contro infrastrutture utilizzate da attori ritenuti sponsorizzati dalla Repubblica Popolare Cinese. È stata inoltre documentata una tecnica per la distribuzione mirata di spyware commerciale attraverso annunci pubblicitari online, per la quale non è stata formulata un'attribuzione statale.

L'8 ottobre il **Dipartimento di Giustizia** e il **Federal Bureau of Investigation (FBI)** degli Stati Uniti hanno annunciato il sequestro di sette domini associati a **Microscan** e **FishHub**, due strumenti gestiti dalla società cinese **Integrity Technology Group**[6]. Secondo le autorità statunitensi, la società avrebbe messo tali strumenti a disposizione di operatori associati a **Flax Typhoon**, gruppo di spionaggio informatico ritenuto dal **Dipartimento di Giustizia** e dall'**FBI** degli Stati Uniti sponsorizzato dallo Stato cinese. Microscan veniva utilizzato per individuare vulnerabilità nelle reti delle potenziali vittime, anche attraverso una rete di dispositivi compromessi mediante una variante del malware Mirai. FishHub supportava, invece, attività di *spear phishing*, consentendo la predisposizione di pagine contraffatte destinate alla sottrazione delle credenziali. Gli strumenti sarebbero stati impiegati per prendere di mira infrastrutture critiche e altre reti negli Stati Uniti e in ulteriori Paesi.

Il 15 ottobre **Citizen Lab** ha documentato **AdFection**, tecnica impiegata per distribuire spyware commerciale attraverso annunci pubblicitari mirati. L'attività sfruttava il meccanismo automatizzato con cui gli spazi pubblicitari online vengono assegnati in tempo reale agli inserzionisti (real-time bidding - RTB) per individuare specifici dispositivi e mostrare annunci contenenti codice malevolo; la sola visualizzazione dell'annuncio poteva avviare la catena di compromissione, senza richiedere ulteriori interazioni da parte dell'utente. La tecnica è stata riscontrata in attacchi condotti nel 2024 e nel 2025 contro almeno 45 dispositivi riconducibili ad **Al Jazeera**. I dispositivi sarebbero stati compromessi mediante spyware sviluppato da **Candiru**, società israeliana successivamente ridenominata Integrity Labs. Secondo Citizen Lab, gli annunci erano acquistati dalla società israeliana **Discover-Tech**, la cui piattaforma consentiva agli operatori di identificare, profilare e infettare automaticamente i dispositivi selezionati. L'analisi di circa quattro miliardi di registrazioni relative alle aste pubblicitarie ha inoltre rilevato la distribuzione degli annunci di Discover-Tech attraverso quasi 200.000 siti web e applicazioni mobili in numerosi Paesi. A seguito della pubblicazione dei risultati dell'indagine, diversi operatori del settore pubblicitario hanno interrotto o sospeso i rapporti con Discover-Tech [7].

Riferimenti

[1] Google Threat Intelligence Group (Mandiant). *ARMORY CASTLE Exploits BeyondTrust*. 15 Ott. 2026. URL: https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-beyondtrust.

[2] Google Threat Intelligence Group (Mandiant). *Investigating Ephemeral Supply Chain Tampering*. 15 Ott. 2026. URL: https://cloud.google.com/blog/topics/threat-intelligence/investigating-ephemeral-supply-chain-tampering.

[3] EUROPOL. *Teenager suspected of leading KillSec ransomware group as law enforcement seizes servers and leak site*. 1 Ott. 2026. URL: https://www.europol.europa.eu/media-press/newsroom/news/teenager-suspected-of-leading-killsec-ransomware-group-law-enforcement-seizes-servers-and-leak-site.

[4] Microsoft Threat Intelligence. *AI-driven, large-scale nation-state campaign using ARTEX enables supply chain compromise*. 21 Ott. 2026. URL: https://www.microsoft.com/en-us/security/blog/2026/10/21/storm-0940-uses-artex-agentic-ai-connectwise-supply-chain-compromise/.

[5] Crowdstrike. *VAPOR PANDA Uses AI-Driven ARTEX to Scale a Global Espionage Campaign*. 29 Ott. 2026. URL: https://www.crowdstrike.com/en-us/blog/vapor-panda-uses-artex-to-scale-global-campaign/.

[6] U.S. Department of Justice. *Justice Department and FBI Seize Vulnerability Scanning and Spear-Phishing Tools Operated and Used by China-State Sponsored Hackers*. 8 Ott. 2026. URL: https://www.justice.gov/opa/pr/justice-department-and-fbi-seize-vulnerability-scanning-and-spear-phishing-tools-operated.

[7] Citizenlab. *Exposing AdFection - How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware*. 15 Ott. 2026. URL: https://citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/.

LaTeX



OPERATIONAL SUMMARY

ottobre 2026