Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

APRILE 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 (Perimetro di Sicurezza Nazionale Cibernetica, Legge 28 giugno 2024, n. 90, Direttiva NIS) e riceve altresì informazioni provenienti da fonti aperte e commerciali nonché da altre articolazioni omologhe nazionali ed internazionali, che le condividono di iniziativa o in base ad accordi di collaborazione. Queste informazioni dotano l'Agenzia di un ampio cono di visibilità sullo stato della minaccia cyber a danno del sistema Paese e forniscono, dal punto di vista qualitativo, un quadro strutturato delle minacce e del livello di esposizione dei soggetti nazionali. Tutte le informazioni vengono studiate e valorizzate dagli operatori del CSIRT Italia, i quali nella fase di triage le analizzano e classificano come eventi cyber; per ognuno di questi vengono esperite una serie di attività a seconda del soggetto impattato e del tipo di evento, come:

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

Per le definizioni si rimanda al Glossario del CSIRT Italia 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.

Indice

Elenco delle figure

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.

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 aprile 2026 sono stati registrati **265 eventi**, in **diminuzione** del 39% rispetto ai **435** di marzo, analoga contrazione ha riguardato il numero di **incidenti** (**174**), in **diminuzione** del 39% rispetto al mese precedente. Dopo l'incremento degli eventi e degli incidenti osservato nei primi mesi del 2026 - riconducibile alla progressiva entrata a regime degli obblighi di notifica introdotti dalla Direttiva NIS2 - nel mese di aprile 2026 si osserva una prima fase di assestamento. I valori registrati restano, tuttavia, superiori a quelli rilevati nel periodo precedente all'entrata a regime della nuova disciplina, a conferma di una più ampia emersione degli eventi e degli incidenti cyber. Nel corso del mese di aprile 2026, le principali minacce rilevate risultano l'**esposizione dati**, il **phishing** e le **compromissioni di caselle di posta elettronica**.

- **Settori interessati**
  I settori con il maggior numero di vittime di eventi cyber sono stati **Manifatturiero**, **Tecnologico** e **Pubblica amministrazione centrale**. Il manifatturiero è stato interessato prevalentemente da esposizione dati, mentre il settore tecnologico e delle telecomunicazioni da compromissione delle caselle e-mail.

- **Ransomware**
  Gli attacchi ransomware hanno interessato prevalentemente i settori manifatturiero, trasporti e altre società private. L'analisi degli eventi rilevati evidenzia come i principali vettori di compromissione

siano riconducibili all'**utilizzo di credenziali valide**, precedentemente compromesse, e allo **sfruttamento di servizi di accesso remoto** non adeguatamente configurati.

- **Attacchi DDoS**
  Nel mese in esame, **non sono state rilevate campagne di particolare rilevanza** rivolte a soggetti nazionali. Sono state tuttavia registrate 3 rivendicazioni, senza evidenze di impatti significativi.

- **Monitoraggio proattivo**
  Nell'ambito dell'attività proattiva di monitoraggio della superficie esposta dei soggetti nazionali, il CSIRT Italia ha inviato, ad aprile 2026, **1.500 comunicazioni di allertamento** a pubbliche amministrazioni e imprese appartenenti alla constituency, relative all'esposizione su Internet di **2.212 servizi a rischio**.
  L'analisi dei *log* provenienti da **malware di tipo infostealer** ha consentito, infine, di identificare **7 account** potenzialmente compromessi afferenti a soggetti istituzionali, prontamente allertati.

- **Vettori di attacco**
  Nel mese di aprile 2026 la posta elettronica si conferma il principale vettore di accesso iniziale. In stretta connessione, emerge lo sfruttamento di credenziali valide già compromesse, a conferma della centralità dell'abuso dell'identità digitale nelle dinamiche di attacco osservate. Permangono, seppure con minore incidenza, lo sfruttamento di vulnerabilità e l'abuso di servizi remoti esposti.

- **Vulnerabilità**
  Sono state pubblicate **5.885** nuove CVE, in **diminuzione** (**–307**) rispetto a marzo. Di queste, **1.251** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–30**), e per **10** CVE è stato rilevato lo sfruttamento attivo, **stabile** (**+3**) rispetto a marzo. Particolarmente critiche le vulnerabilità che interessano **Fortinet FortiClient EMS**, soluzione utilizzata per la gestione centralizzata di dispositivi e sistemi connessi alla rete aziendale (CVE-2026-21643 e CVE-2026-35616), che potrebbero consentire a un attaccante non autenticato l'esecuzione di codice da remoto; **Apache Tomcat**, server applicativo open source ampiamente impiegato per l'erogazione di applicazioni web basate su tecnologia Java (CVE-2026-29146), la cui compromissione potrebbe determinare l'accesso non autorizzato a informazioni sensibili; **Red Hat Enterprise Linux 10**, sistema operativo enterprise basato su Linux utilizzato in ambienti server, con specifico riferimento all'interfaccia web Cockpit per l'amministrazione remota dei sistemi (CVE-2026-4631). La vulnerabilità potrebbe permettere a un attaccante di eseguire comandi o codice da remoto sui sistemi affetti, anche in assenza di credenziali valide. Tali criticità sono state oggetto di specifiche attività di allertamento da parte del CSIRT Italia.

- **Allertamento**
  Le numerose vulnerabilità individuate ad aprile 2026 hanno determinato un **incremento del numero di sistemi e servizi potenzialmente esposti**, con conseguente **elevato numero di comunicazioni di allertamento** effettuate dall'Agenzia 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. Le **comunicazioni dirette**, effettuate dal CSIRT Italia sono state in totale **7.229**, **in aumento** (+13) rispetto a marzo.

I NUMERI DI APRILE 2026

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

- **265** eventi cyber, in **diminuzione** (**–170**);
- **344** vittime, in **diminuzione** (**–210**);
- **219** vittime della constituency[1], in **diminuzione** (**–70**);
- **174** incidenti con impatto confermato, in **diminuzione** (**–109**);
- **126** asset potenzialmente compromessi, in **aumento** (**+72**);
- **2.212** asset potenzialmente vulnerabili, in **diminuzione** (**–1.127**);
- **101** alert sul sito web del CSIRT Italia, **stabile** (**+ 3**);
- **7.229** comunicazioni inviate, in **aumento** (**+13**);
- **5.885** nuove CVE, in **diminuzione** (**–307**) .

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

PRODOTTI VULNERABILI

Di seguito **l'elenco dei prodotti** che ad aprile 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.

- **Citrix XenServer** (CVE-2026-23556, CVE-2026-23558, CVE-2026-23559, CVE-2026-23560, CVE-2026-23561) Link all'alert
- **Flowise** (CVE-2025-59528) Link all'alert
- **Notepad++** (CVE-2026-3008) Link all'alert
- **Langflow-ai** (CVE-2026-33309) Link all'alert
- **Cisco Identity Services Engine Software,Cisco ISE Passive Identity Connector** (CVE-2026-20147) Link all'alert
- **SaturdayDrive Ninja Forms - File Uploads** (CVE-2026-0740) Link all'alert
- **Progress ShareFile Storage Zones Controller** (CVE-2026-2699, CVE-2026-2701) Link all'alert
- **Cisco Enterprise NFV Infrastructure Software,Cisco Unified Computing System E-Series Software (UCSE),Cisco Unified Computing System (Standalone)** (CVE-2026-20093) Link all'alert
- **WebPros cPanel,WHM,WP Squared** (CVE-2026-41940) Link all'alert
- **Fortinet FortiClientEMS** (CVE-2026-21643, CVE-2026-35616) Link all'alert
- **Apache Kafka** (CVE-2026-33557) Link all'alert
- **Apache ActiveMQ,Apache ActiveMQ All,Apache ActiveMQ Broker** (CVE-2026-34197) Link all'alert
- **Zammad** (CVE-2026-34724) Link all'alert
- **GitHub Enterprise Server** (CVE-2026-3854) Link all'alert
- **ProFTPD** (CVE-2026-42167) Link all'alert
- **Apache Tomcat** (CVE-2026-29146) Link all'alert
- **Splunk Cloud Platform,Splunk Enterprise** (CVE-2026-20204) Link all'alert
- **Microsoft SharePoint Enterprise Server 2016,Microsoft SharePoint Server 2019,Microsoft SharePoint Server Subscription Edition,Windows Admin Center** (CVE-2026-32196, CVE-2026-32201) Link all'alert
- **OpenPrinting cups** (CVE-2026-34990) Link all'alert
- **Axios** (CVE-2026-40175) Link all'alert

Maggiori dettagli nelle sezioni 3 e 5.

2 EVENTI ED INCIDENTI

Ad aprile 2026 sono stati individuati **265** eventi cyber, in **diminuzione** del 39% rispetto al mese precedente. Questi ultimi hanno **interessato 271 soggetti nazionali**: 219 appartenenti alla constituency, i restanti hanno riguardato cittadini e società private operanti in settori non critici. Dei 265 eventi cyber, **174 sono stati classificati quali incidenti**, in **diminuzione** del 39% rispetto a marzo.

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

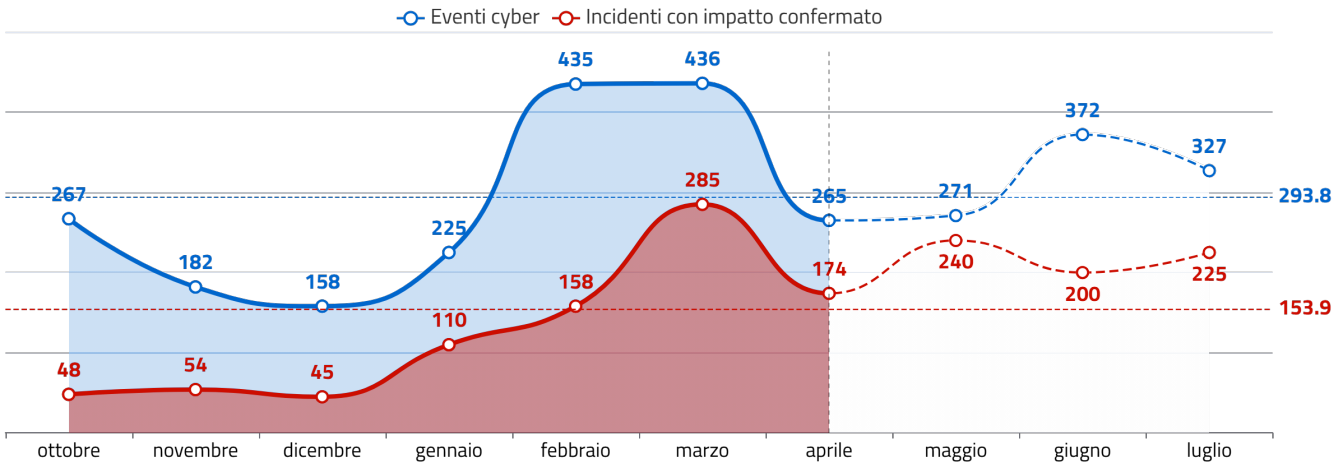

Figura 2 - *andamento attività reattive e analisi previsionale*

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

2.1 Settori impattati

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

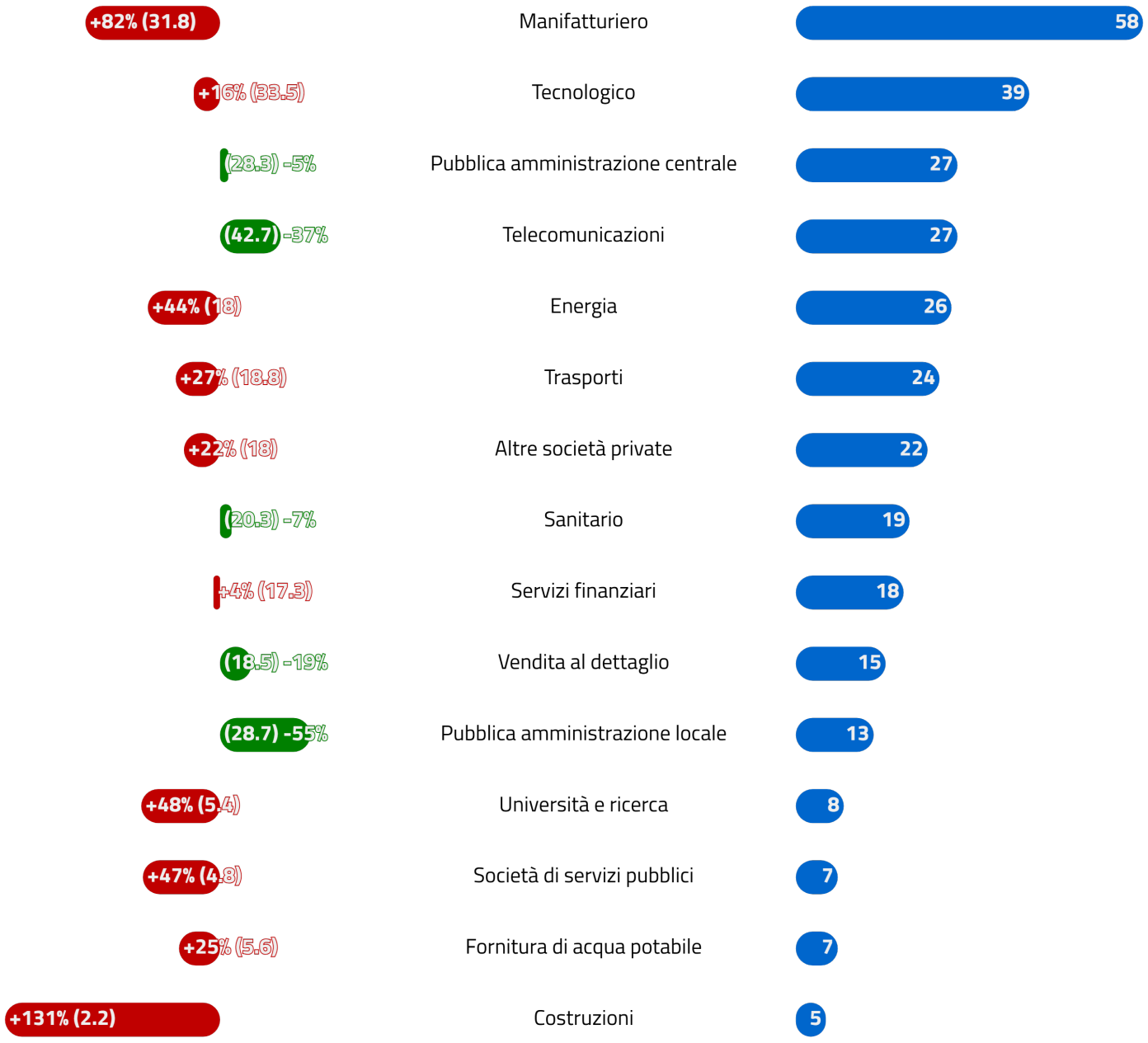

Figura 3 - *numero di vittime di eventi cyber per settore e variazione percentuale rispetto al semestre precedente (top 15)*

[3] Le notifiche NIS fanno riferimento a eventi con impatto su soggetti rientranti nell'ambito di applicazione della normativa. Tuttavia, gli effetti degli stessi eventi possono estendersi anche a soggetti non rientranti nella predetta disciplina.

2.2 Tipologia di minacce negli eventi

In Figura 4 si riporta la distribuzione delle principali tipologie di minacce rilevate negli eventi oggetto di notifica NIS[4] e la variazione percentuale rispetto alla media del semestre precedente (riportata tra parentesi nel grafico).
Per la definizione delle minacce far riferimento alla Tassonomia Cyber dell'ACN (https://www.acn.gov.it/portale/w/la-tassonomia-cyber-dellacn).

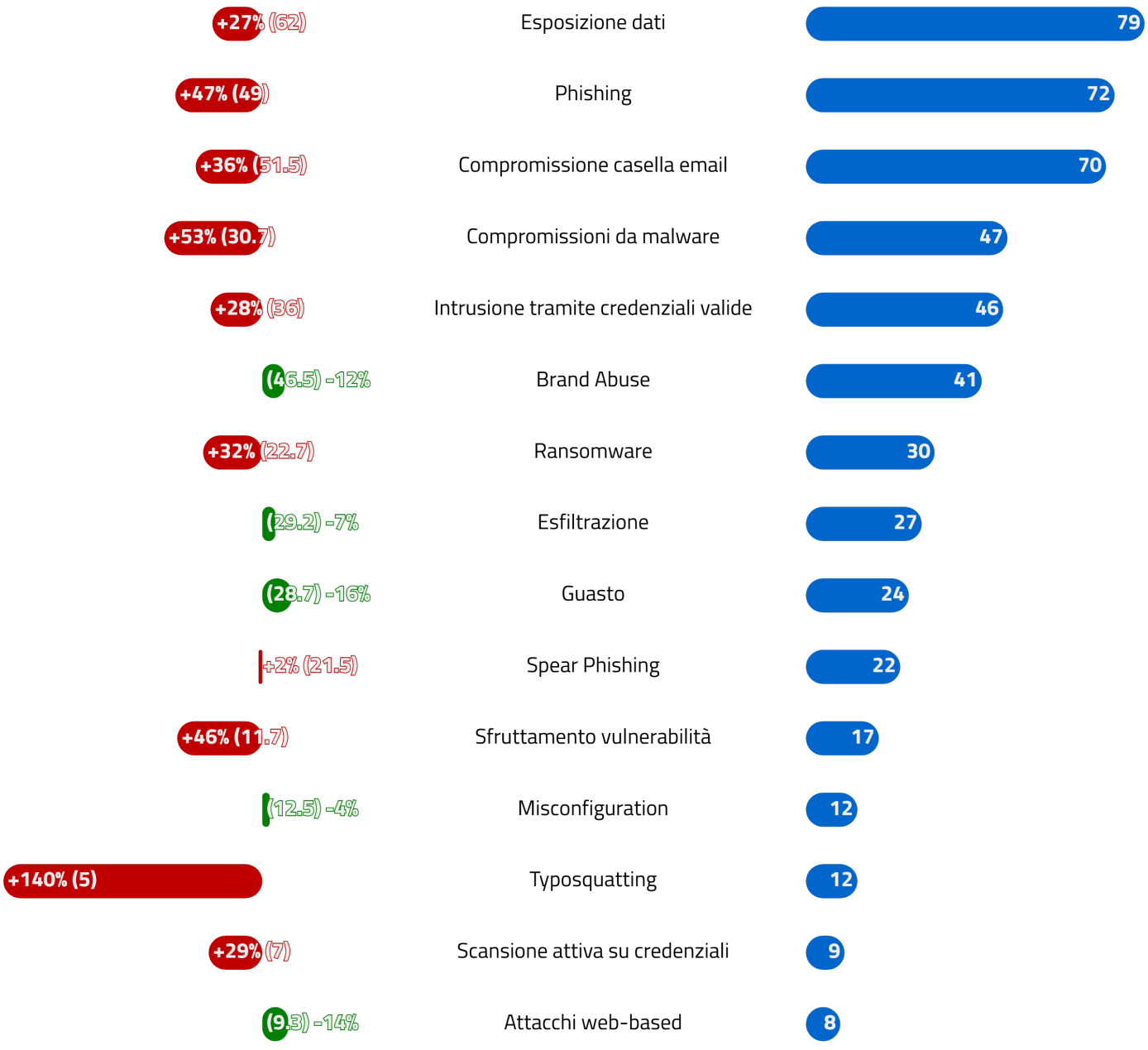

Figura 4 - *tipologie di minacce rilevate negli eventi e variazione percentuale rispetto al semestre precedente (top 15)*

[4] 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 aprile 2026. Si ricorda che ad un evento possono essere associate più minacce e più vittime. 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.

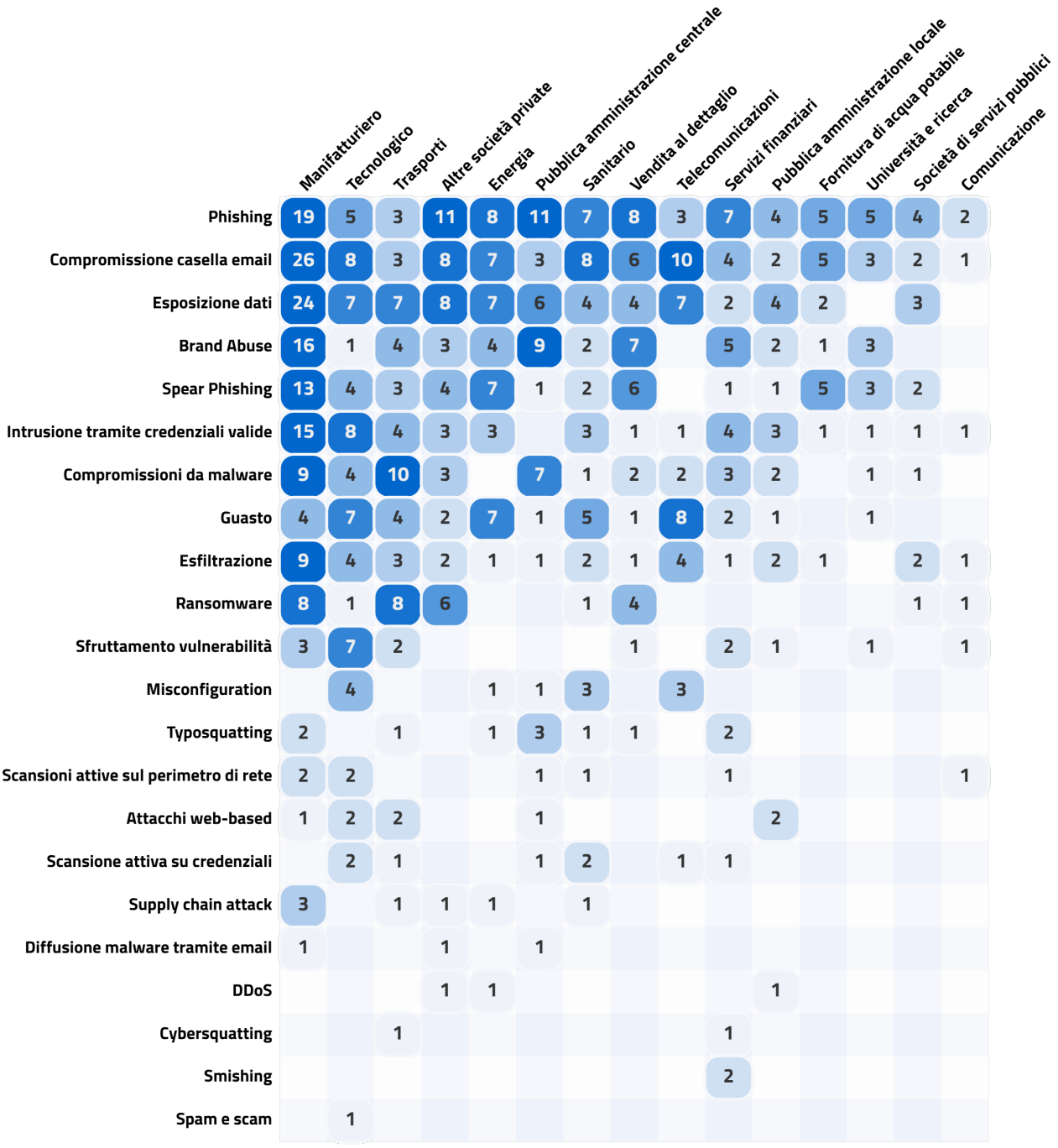

Figura 5 - *numero di vittime per settore e tipologia di minacce*

2.4 Distribuzione geografica delle vittime

I 265 eventi cyber hanno interessato **344** soggetti (in diversi casi più volte), distribuiti dal punto di vista geografico come riportato in Figura 6.

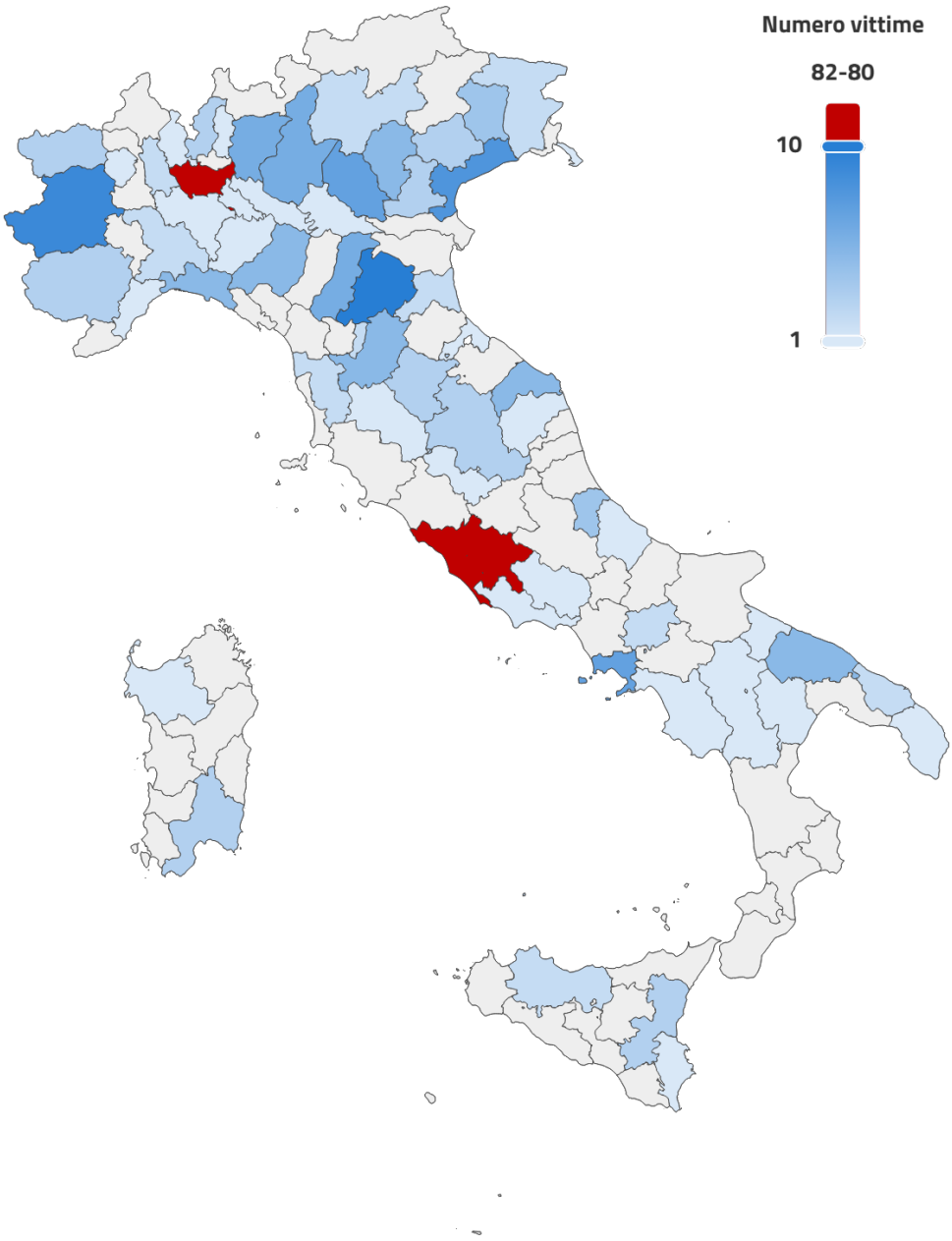

Figura 6 - *distribuzione delle vittime degli eventi cyber*

3 VULNERABILITÀ

Ad aprile 2026 sono state pubblicate[5] **5.885** nuove CVE, in **diminuzione** (**–307**) rispetto a marzo. Di queste, **1.251** presentano almeno un *Proof of Concept (PoC)*, in **diminuzione** (**–30**), e per **10** CVE è stato rilevato lo sfruttamento attivo, **stabile** (**+3**) rispetto a marzo.

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 **101**. Oltre al consueto aggiornamento mensile di Microsoft (link) all'alert sul sito web, che ha risolto un totale di 165 nuove vulnerabilità (2 di tipo 0-day), sono risultate particolarmente gravi quelle pubblicate nei seguenti alert, relative a prodotti di:

- **Axios**: disponibile un Proof of Concept (PoC) per lo sfruttamento della CVE-2026-40175 presente nella libreria Axios, client HTTP ampiamente utilizzato in applicazioni JavaScript per browser e ambienti Node.js, incluse architetture cloud e microservizi (stima di impatto sistemico **79,48/100**). Link all'alert del 13/04/2026;
- **Flowise**: rilevato lo sfruttamento attivo in rete della vulnerabilità CVE-2025-59528 – già sanata dal vendor – presente in Flowise, piattaforma open-source con interfaccia drag & drop per costruire flussi personalizzati basati su modelli linguistici di grandi dimensioni (LLM). Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un attore malevolo di eseguire codice arbitrario da remoto sui sistemi interessati, con possibile accesso al file system e compromissione completa dell'istanza applicativa (stima di impatto sistemico **79,48/100**). Link all'alert del 08/04/2026;
- **Langflow**: disponibile Proof of Concept (PoC) per la CVE-2026-33309 presente nel LocalStorageService di Langflow, software usato per sviluppare e distribuire workflow e agent gestiti dall'AI (stima di impatto sistemico **79,48/100**). Link all'alert del 03/04/2026;
- **Notepad++**: disponibile un Proof of Concept (PoC) per la CVE-2026-3008 – già sanata dal vendor – presente nel software "Notepad++", noto editor di testo avanzato per Windows. Tale vulnerabilità, qualora sfruttata, potrebbe

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

consentire a un utente malintenzionato di compromettere la disponibilità del servizio o accedere a informazioni sensibili presenti nei registri e nello stack del processo Notepad++ in esecuzione sul sistema locale (stima di impatto sistemico **79,48/100**). Link all'alert del 27/04/2026;

- **Progress**: disponibili Proof of Concept (PoC) per le CVE-2026-2699 e CVE-2026-2701 – già sanate dal vendor a marzo 2026 – presenti negli Storage Zone Controller di Progress ShareFile, software enterprise usato per condividere, archiviare e gestire file in modo sicuro nel cloud (stima di impatto sistemico **79,48/100**). Link all'alert del 02/04/2026;

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[6].

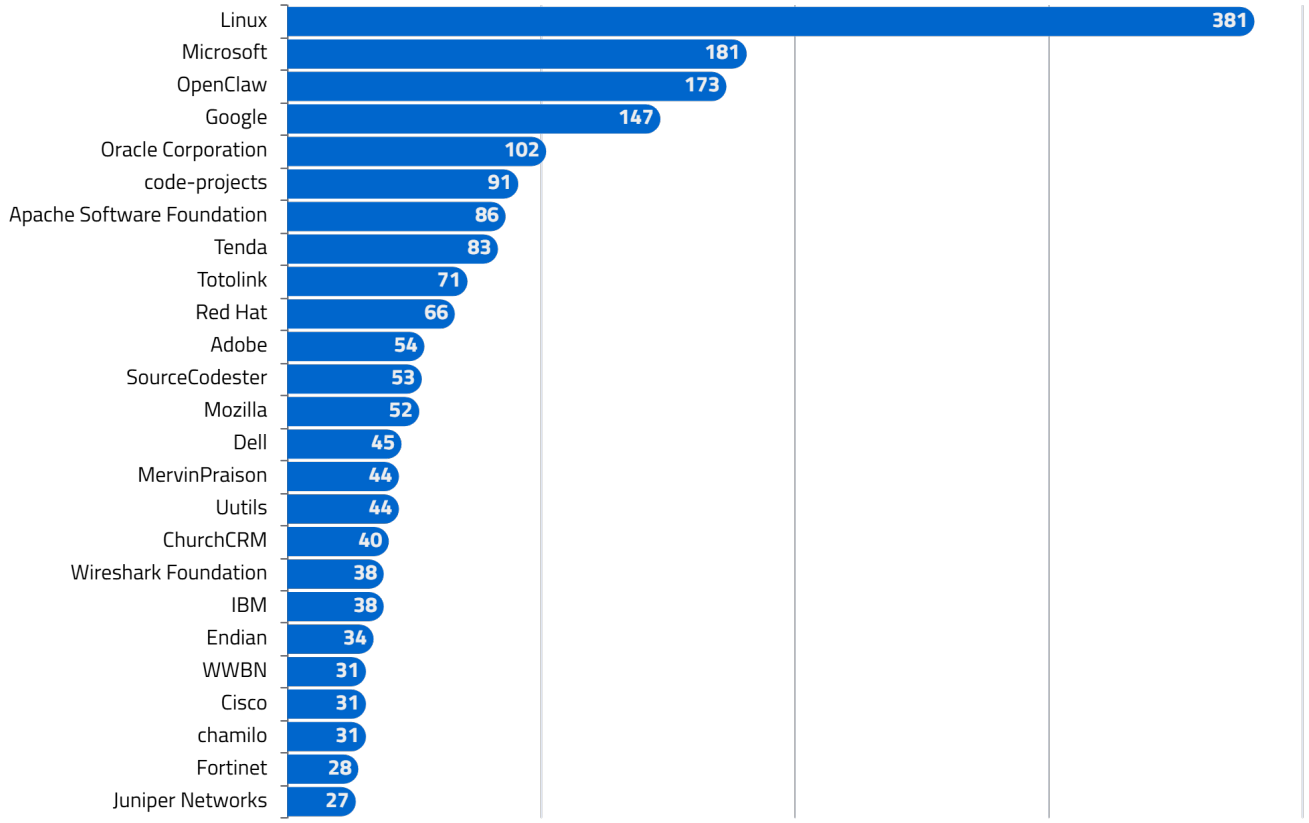

Figura 7 - *top 25 produttori affetti da vulnerabilità nel mese*

[6] 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.

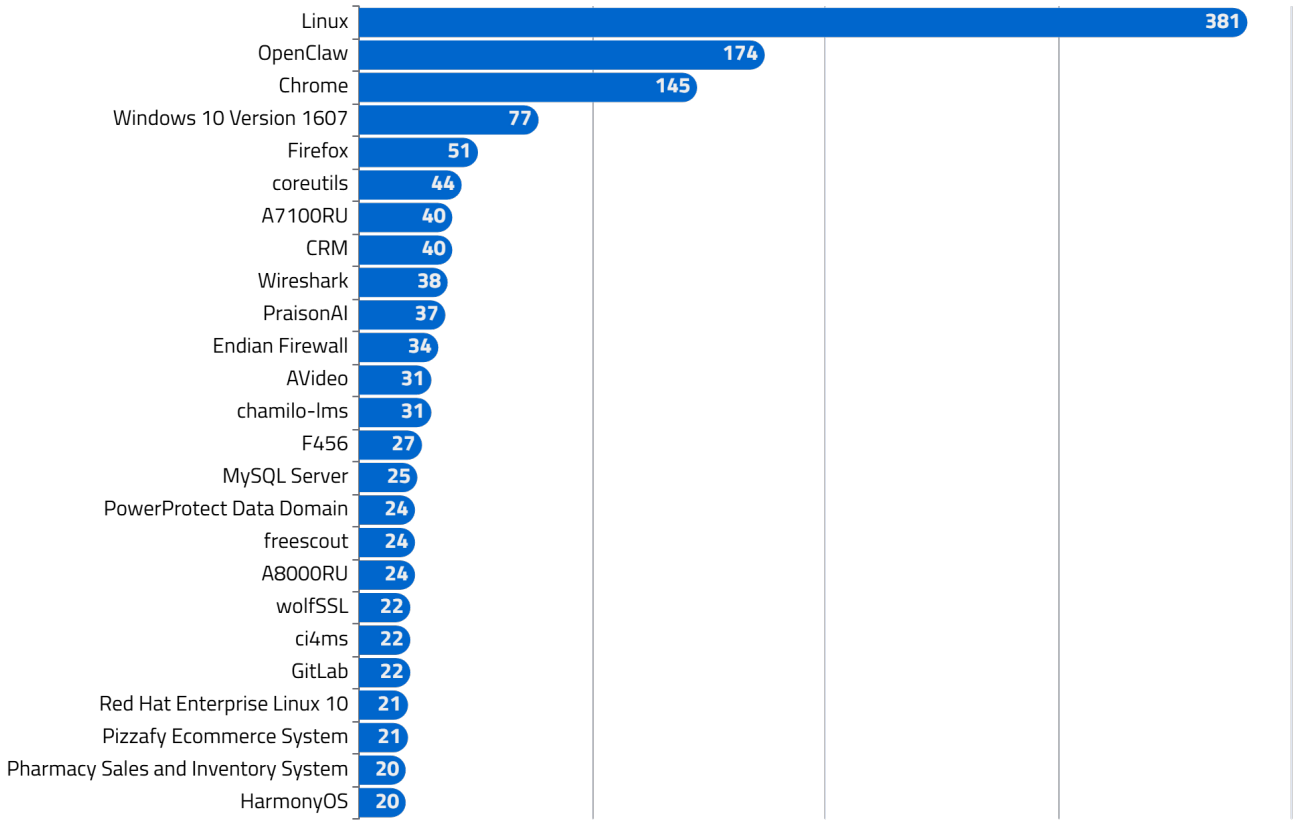

Figura 8 - *top 25 prodotti affetti da vulnerabilità nel mese*

3.3 CWE nel mese

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

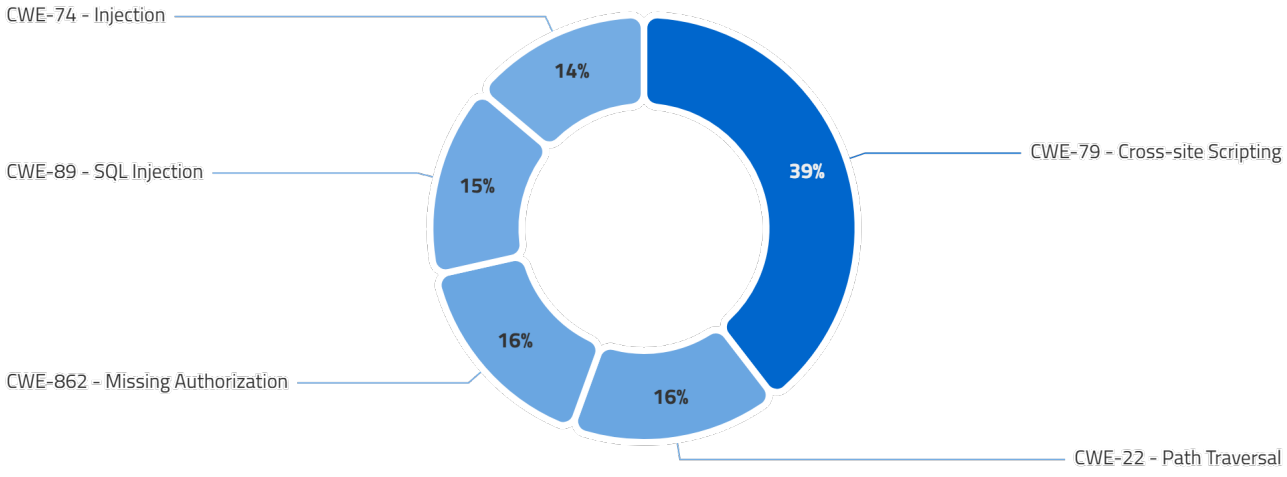

Figura 9 - *top 5 CWE nel mese*

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

Vendor	**Ivanti**
Prodotti e versioni vulnerabili	**Ivanti Endpoint Manager Mobile tutte le versioni fino alla 12.7.0.0**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette a un attaccante non autenticato di eseguire codice malevolo da remoto**
Data di rilascio CVE	**29/01/2026 modificata il 09/04/2026**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.75**

Tabella 1 - *CVE-2026-1340*

Vendor	**Apache Software Foundation**
Prodotti e versioni vulnerabili	**Apache ActiveMQ Broker e Apache ActiveMQ versioni fino alla 5.19.3 e versioni dalla 6.0.0 alla 6.2.2**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette a un attaccante non autenticato di eseguire codice arbitrario da remoto sul server**
Data di rilascio CVE	**07/04/2026 modificata il 16/04/2026**
CVSS score 3.0	**8.8 High**
EPSS max score	**0.65**

Tabella 2 - *CVE-2026-34197*

[7] 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	**Fortinet**
Prodotti e versioni vulnerabili	**Fortinet FortiClientEMS versione 7.4.4**
Descrizione vulnerabilità	**Lo sfruttamento di questa vulnerabilità permette a un attaccante non autenticato di eseguire codice arbitrario da remoto.**
Data di rilascio CVE	**06/02/2026 modificata il 16/04/2026**
CVSS score 3.0	**9.8 Critical**
EPSS max score	**0.43**

Tabella 3 - *CVE-2026-21643*

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[8] condivisi dal CSIRT Italia tramite piattaforma MISP[9], in modo da caratterizzarne le tipologie più frequenti.

4.1 Ransomware: distribuzione delle vittime

Ad aprile 2026, il 13% degli attacchi ransomware ha colpito soggetti critici, il 30% ha colpito soggetti a media criticità, ed il restante 57% ha coinvolto altri soggetti a criticità minore.

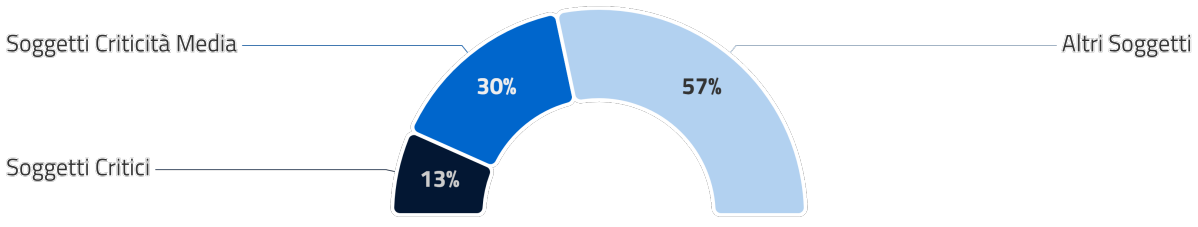

Figura 10 - *distribuzione delle vittime di ransomware in base alla loro criticità*

[8]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.

[9]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 aprile 2026 ha permesso di individuare **28** rivendicazioni di attacchi ransomware a danno di soggetti italiani[10].

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

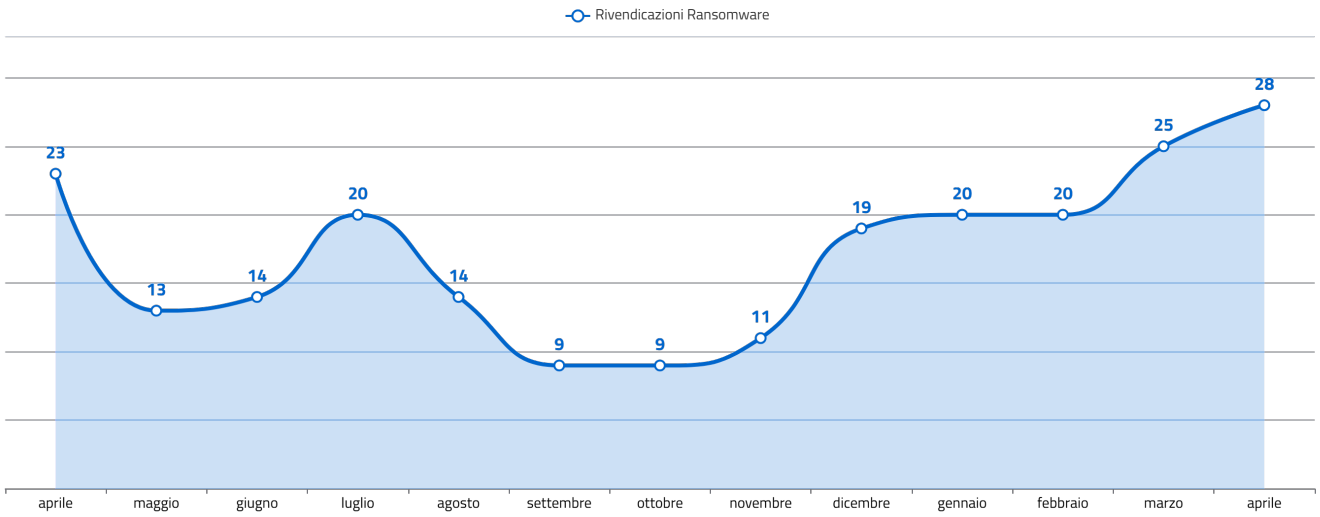

Figura 11 - *andamento delle rivendicazioni Ransomware per l'Italia*

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

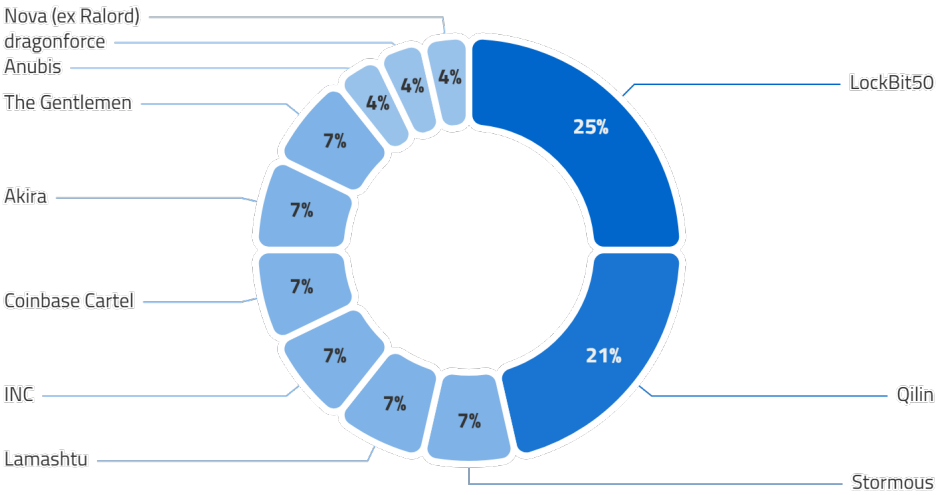

Figura 12 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

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

4.3 Rivendicazioni DDoS

A aprile 2026 sono state individuate[11] **3** 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.

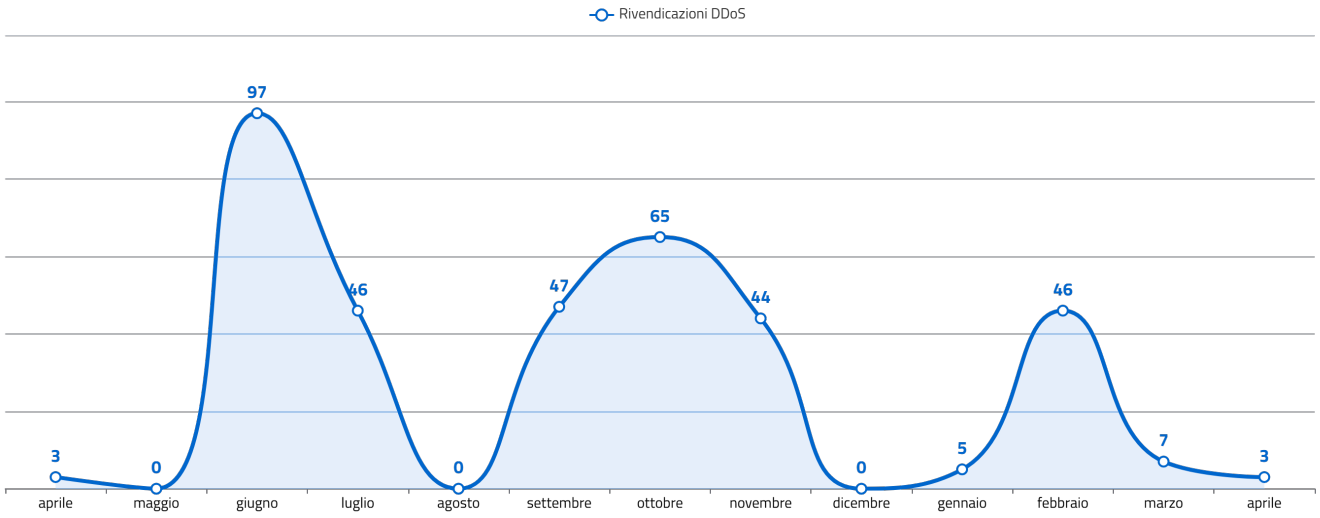

Figura 13 - *andamento delle rivendicazioni DDoS riferite all'Italia*

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

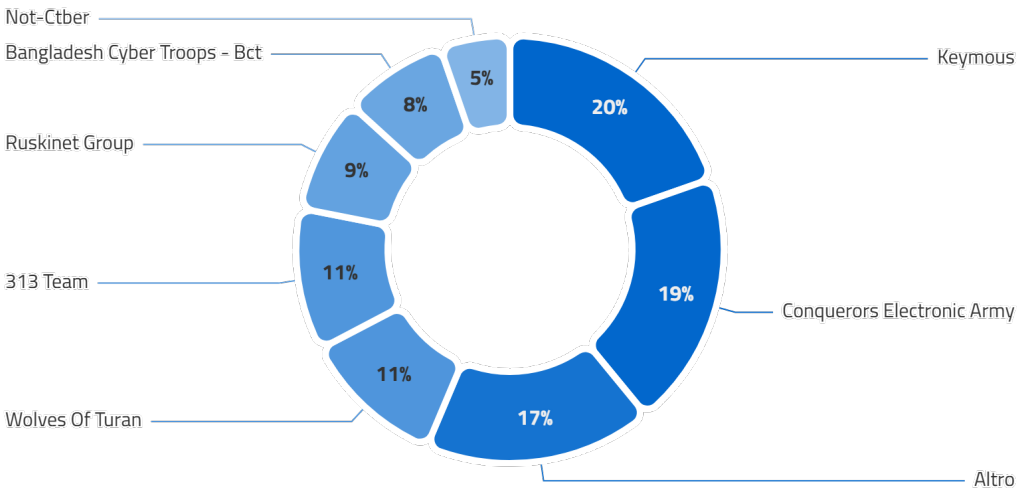

Figura 14 - *distribuzione percentuale dei gruppi autori delle rivendicazioni*

[11] 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.

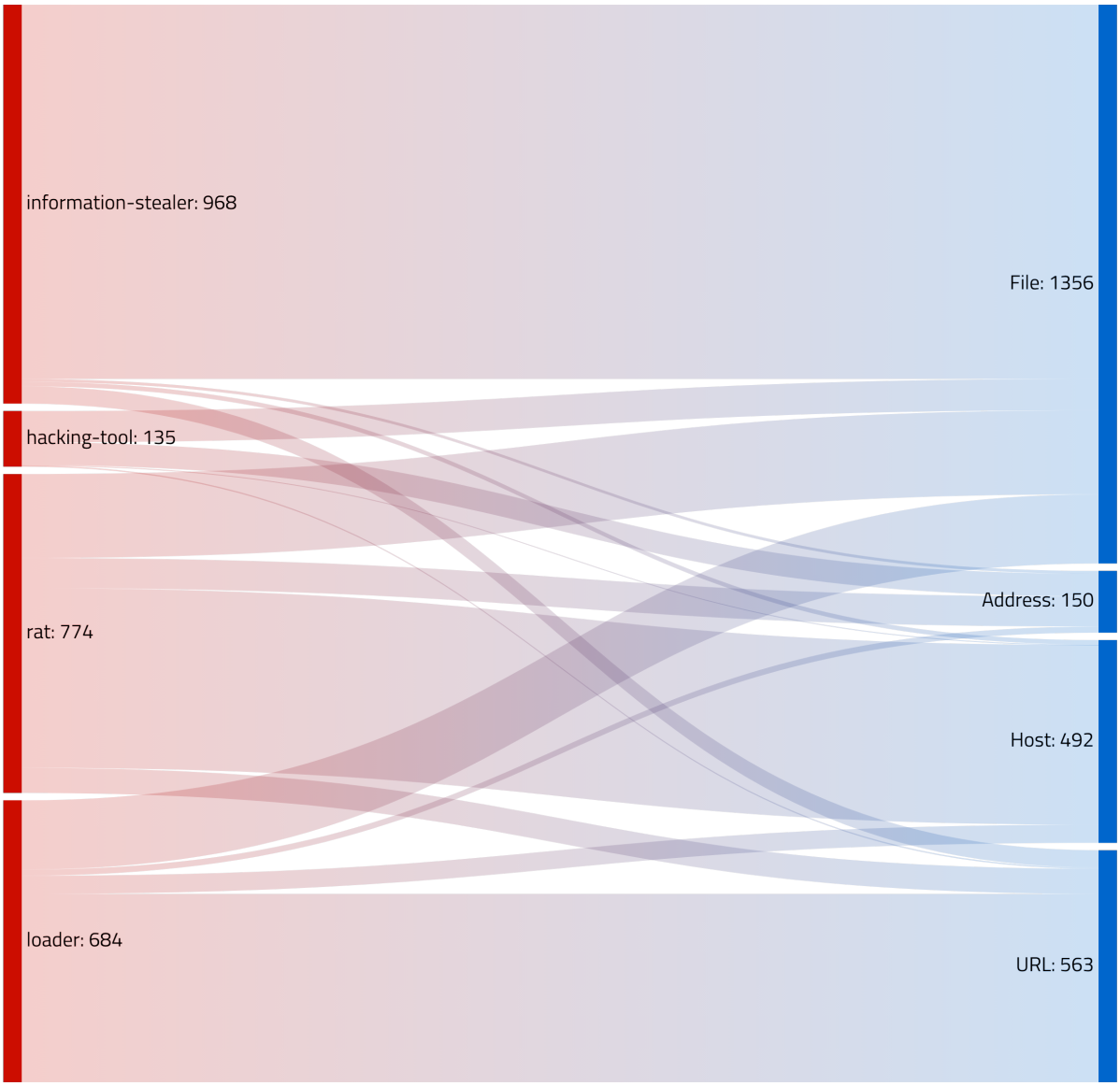

Figura 15 - *numero di IoC condivisi dal CSIRT Italia suddivisi per tipologie di malware*

5 MONITORAGGIO

In questa sezione sono riportate le attività di monitoraggio proattivo[12], 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 aprile 2026 sono state diramate un totale di **1.500** comunicazioni verso i soggetti della constituency che esponevano pubblicamente su Internet complessivamente **2.212** servizi a rischio. Le comunicazioni sono state inviate in relazione ai prodotti:

- **Fortinet FortiClientEMS** (CVE-2026-21643 e CVE-2026-35616): tali vulnerabilità – rispettivamente di tipo *Improper Access Control* e *SQL Injection* – permetterebbero a un eventuale attaccante non autenticato, tramite l'invio di richieste HTTP opportunamente predisposte, di eseguire codice arbitrario da remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Apache Software Foundation Tomcat** (CVE-2026-29146, CVE-2026-34486 e CVE-2026-34500): tali vulnerabilità – di tipo rispettivamente *External Control of Critical State Data*, *Missing Encryption of Sensitive Data* e *Improper Authentication* – permetterebbero ad un eventuale attaccante l'accesso ad informazioni sensibili. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Cockpit** (CVE-2026-4631): tale vulnerabilità – di tipo *Command Injection* – permetterebbe, tramite richieste HTTP opportunamente predisposte, a un eventuale attaccante con accesso all'interfaccia web di Cockpit di specificare opzioni SSH malevole all'interno del client OpenSSH dell'host ed eseguire così comandi shell o codice da remoto sui sistemi affetti senza la necessità di specificare credenziali valide.

[12] 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.

- **ProFTPD** (CVE-2026-42167): tale vulnerabilità – di tipo *SQL Injection* – permetterebbe a un eventuale attaccante di eseguire codice arbitrario da remoto sfruttando il parametro "username", laddove la funzionalità di logging sfrutti espansioni per il suddetto parametro (come %U) e il back-end SQL permetta l'esecuzione di comandi. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Microsoft SharePoint** (CVE-2026-32201): tale vulnerabilità – di tipo *Spoofing* – permetterebbe a un eventuale attaccante remoto di visualizzare e di modificare informazioni sensibili all'interno dei server affetti senza bisogno di autenticazione consentendo diversi tipi di impatti tra cui: manipolazione dei dati, amplificazione di phishing, ovvero insediamento in ambienti enterprise. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Keycloak** (CVE-2026-3429 e CVE-2026-4636): tali vulnerabilità – di tipo *Improper Access Control* e *Incorrect Behavior Order* – consentirebbero a un attaccante autenticato di eludere meccanismi di sicurezza, inclusi i controlli MFA e la validazione delle policy UMA (*User-Managed Access*).
- **OpenPrinting CUPS** (CVE-2026-34980 e CVE-2026-34990): tali vulnerabilità – rispettivamente di tipo *Improper Input Validation* e *Improper Authentication*– permetterebbero, laddove utilizzate in maniera combinata, a un eventuale attaccante di eseguire codice arbitrario sul sistema impattato con privilegi elevati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Zammad** (CVE-2026-34724): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante, autenticato e con privilegi tali da poter modificare la configurazione *type_enrichment_data*, di eseguire codice remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Citrix XenServer** (CVE-2026-23556, CVE-2026-23558, CVE-2026-23559, CVE-2026-23560 e CVE-2026-23561): tali vulnerabilità – di tipo rispettivamente *Denial of Service* e *Privilege Escalation* – sono relative alla XAPI permetterebbero a un eventuale attaccante di provocare il crash della macchina host (CVE-2026-23556) ed elevare i propri privilegi al livello dell'hypervisor (CVE-2026-23558) o ottenere comunque privilegi più elevati di quelli specificati all'interno delle relative RBAC (CVE-2026-23559, CVE-2026-23560 e CVE-2026-23561). Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Apache Software Foundation ActiveMQ** (CVE-2026-34197): tale vulnerabilità – di tipo *Code Injection* – permetterebbe a un eventuale attaccante remoto non autenticato di eseguire codice arbitrario sui sistemi interessati, mediante il caricamento di file di configurazioni malevoli caricati da remoto sfruttando la "Jolokia API". Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **WebPros cPanel, WP Squared e WHM** (CVE-2026-41940): tale vulnerabilità – di tipo *Missing Authentication for Critical Function* – permetterebbe a un eventuale attaccante non autenticato di bypassare l'autenticazione e di ottenere una sessione autenticata per ogni utente, incluso root. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Progress ShareFile** (CVE-2026-2699 e CVE-2026-2701): tali vulnerabilità – rispettivamente di tipo *Improper Access Control* e *Unrestricted File Upload* – permetterebbero a un eventuale attaccante l'elusione dei meccanismi di autenticazione e l'esecuzione di codice arbitrario sui sistemi interessati. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Fortinet FortiClientEMS** (CVE-2026-35616): tale vulnerabilità – di tipo *Improper Access Control* – permetterebbe a un eventuale attaccante non autenticato, tramite l'invio di richieste HTTP opportunamente predisposte, di eseguire codice arbitrario da remoto. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Vitejs vite e vite-plus** (CVE-2026-39363 e CVE-2026-39364): tali vulnerabilità – rispettivamente di tipo *Exposure of Sensitive Information*, *Improper Access Control* e *Missing Authentication* – permetterebbero a un eventuale attaccante remoto non autenticato, di leggere file sensibili e codice sorgente dai sistemi affetti, eludendo i controlli di accesso.

- **Cisco Integrated Management Controller (IMC)** (CVE-2026-20093): tale vulnerabilità – di tipo *Improper Input Validation* – permetterebbe a un eventuale attaccante di eludere i meccanismi di autenticazione sui sistemi interessati e di ottenere un accesso amministrativo. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Axios** (CVE-2026-40175): tale vulnerabilità – di tipo *Server-Side Request Forgery* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario nel contesto del processo Node. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Plugin WordPress "SaturdayDrive Ninja Forms"** (CVE-2026-0740): tale vulnerabilità di tipo *Arbitrary File Upload* permetterebbe a un eventuale attaccante di caricare file arbitrari al fine di poter eseguire codice arbitrario. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Apache Software Foundation ActiveMQ** (CVE-2026-40466 e CVE-2026-41044): tali vulnerabilità – di tipo *Code Injection* – permetterebbero a un eventuale attaccante remoto autenticato di caricare uno Spring XML attraverso la Admin Web Console (CVE-2026-41044) e di eludere la mitigazione introdotta per la CVE 2026 34197 bypassando i controlli di validazione (CVE-2026-40466) ed eseguire, sfruttando o l'una o l'altra vulnerabilità, codice arbitrario da remoto sui sistemi affetti.
- **Apache Software Foundation Kafka** (CVE-2026-33557): tale vulnerabilità – di tipo *Improper Validation* – permetterebbe, attraverso la creazione un JWT arbitrario non verificato dai sistemi affetti, a un eventuale attaccante di autenticarsi al broker Kafka senza credenziali valide impersonificando qualsiasi utente e ottenendo, così, accesso non autorizzato al sistema. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **GitHub Enterprise Server** (CVE-2026-3854): tale vulnerabilità – di tipo *Command Injection* – permetterebbe a un eventuale attaccante remoto di eseguire codice arbitrario sui sistemi affetti, sfruttando l'errata sanitizzazione delle opzioni specificate dall'utente all'interno del parametro "option" (-o) del comando "push" tramite protocollo SSH. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Splunk Enterprise e Cloud Platform** (CVE-2026-20204): tale vulnerabilità – di tipo *Insecure Temporary File* – permetterebbe a un eventuale attaccante con privilegi bassi di eseguire codice da remoto (RCE) caricando un file malevolo nella directory "$SPLUNK_HOME/var/run/splunk/apptemp a causa di una gestione impropria e di un insufficiente isolamento dei file temporanei all'interno della directory "apptemp_". Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **OxJacky Nginx UI** (CVE-2026-33032): tale vulnerabilità – di tipo *Missing Authentication for Critical Function* – permetterebbe a un eventuale attaccante di controllare completamente il servizio NGINX da remoto senza autenticazione, eseguendo operazioni amministrative come modificare configurazioni e riavviare il server.
- **BerriAI LiteLLM** (CVE-2026-42208): tale vulnerabilità – di tipo *SQL Injection* – permetterebbe a un eventuale attaccante non autenticato di accedere ed eventualmente manipolare tutti i dati contenuti nel database.
- **Langflow-ai Langflow** (CVE-2026-33309): tale vulnerabilità – di tipo *Path Traversal* – permetterebbe a un eventuale attaccante autenticato di scrivere file arbitrari nel filesystem del sistema e, verosimilmente, permettere l'esecuzione di codice arbitrario. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Etcd-io etcd** (CVE-2026-33413): tale vulnerabilità – di tipo *Missing Authorization* – permetterebbe a un eventuale attaccante di bypassare i controlli di autenticazione o autorizzazione e chiamare determinate funzioni nei cluster che espongono l'API gRPC a client non attendibili o parzialmente affidabili.
- **Microsoft Windows Admin Center** (CVE-2026-32196): tale vulnerabilità – di tipo *Cross-site Scripting (XSS)* – permetterebbe a un eventuale attaccante non autenticato di indurre, tramite un URL valido ma manipolato o un redirect da un sito compromesso, un amministratore WAC a visitare una risorsa apparentemente legittima controllata dall'attaccante la quale risponde alla richiesta del browser della vittima con contenuto malevolo che

viene interpretato ed eseguito. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.

- **Cisco Identity Services Engine Software e ISE Passive Identity Connector** (CVE-2026-20147): tale vulnerabilità – di tipo *Command injection* – permetterebbe a un eventuale attaccante remoto con diritti amministrativi di eseguire comandi arbitrari verso il sistema operativo dei dispositivi affetti. Ulteriori dettagli nell'alert sul sito dello CSIRT Italia.
- **Plugin WordPress "Cloudways Breeze Cache"** (CVE-2026-3844): tale vulnerabilità – di tipo *Unrestricted File Upload* – permetterebbe a un eventuale attaccante remoto non autenticato di eludere le funzionalità di sicurezza sui sistemi interessati per caricare file arbitrari nel sistema target.
- **Marimo-team Marimo** (CVE-2026-39987): tale vulnerabilità – di tipo *Missing Authentication for Critical Function* – permetterebbe, a causa di un errore nel sistema di controllo degli accessi per l'endpoint "/terminal/ws", a un attaccante non autenticato di ottenere una shell completa e di eseguire comandi arbitrari sul sistema operativo dei sistemi affetti.
- **Dolibarr** (CVE-2026-23500): tale vulnerabilità – di tipo *OS Command Injection* – permetterebbe a un eventuale attaccante in grado di autenticarsi come amministratore dell'applicativo di eseguire codice arbitrario sul sistema operativo del sistema impattato.
- **Windmill Labs Windmill** (CVE-2026-22683, CVE-2026-23696 e CVE-2026-29059): tali vulnerabilità – rispettivamente di tipo *Path Traversal*, *SQL Injection* e *Authorization Bypass* – permetterebbero a un eventuale attaccante di leggere file sensibili, manipolare il database, aggirare i meccanismi di controllo delle autorizzazioni e di eseguire codice arbitrario sul sistema interessato.

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

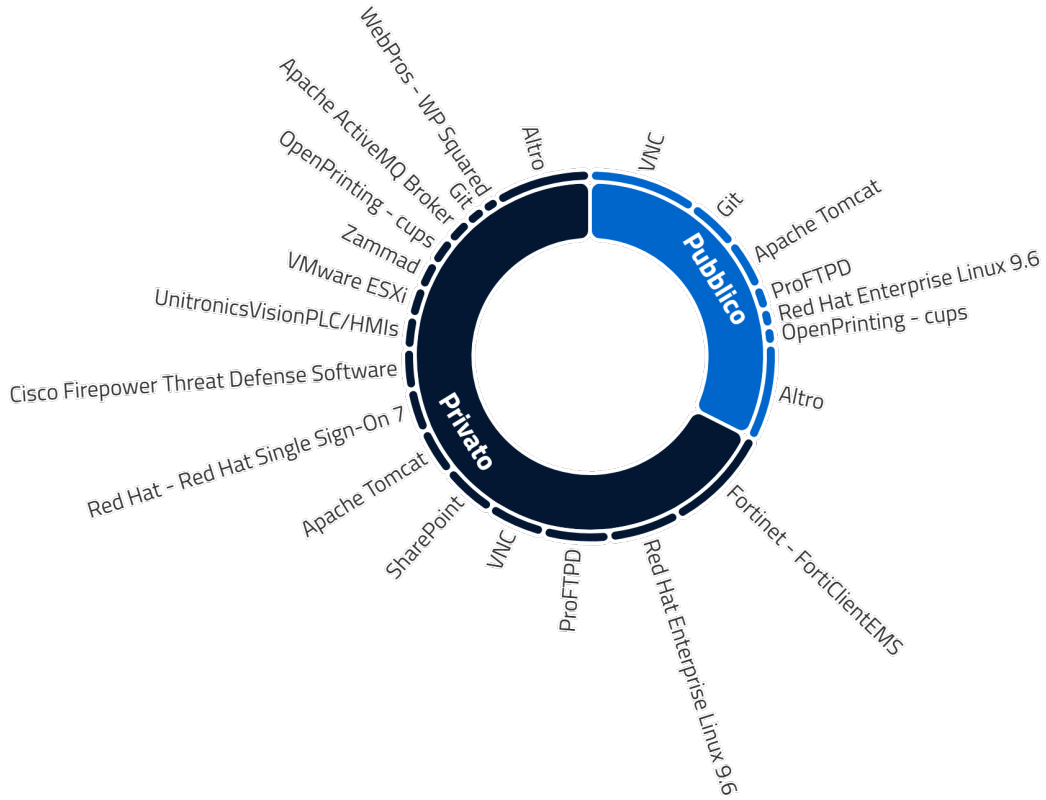

Figura 16 - *distribuzione delle segnalazioni per tipologia di soggetto*

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 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**.

- **Introduzione**

  Nel mese di aprile 2026, le fonti aperte analizzate confermano alcune direttrici di rischio consolidate, in particolare la **compromissione e l'abuso delle identità digitali**, l'**esposizione di vulnerabilità in prodotti e servizi ampiamente diffusi** e l'**impiego di strumenti e servizi legittimi a fini malevoli**. Si conferma altresì la persistenza di **attività cybercriminali con finalità estorsive**. Il contesto geopolitico, specie relativo al Medio Oriente continua a produrre effetti sul dominio cibernetico, con evidenze di targeting di infrastrutture critiche e asset informativi nell'area interessata dalla crisi oltre ad attività di carattere hacktivista.

  In tale contesto, l'**AI generativa** si conferma quale fattore abilitante per l'automazione e la scalabilità di tecniche già note, assumendo un ruolo di crescente rilievo anche alla luce delle nuove capacità offerte dai modelli frontier, che potrebbero essere specializzati o adattati a compiti tecnici specifici, inclusi quelli in ambito cybersecurity.

  Il presente capitolo fornisce una sintesi delle principali **vulnerabilità**, **modalità operative** e **superfici di compromissione** documentate nel mese in esame, affiancata da un inquadramento degli aspetti cyber legati al **contesto geopolitico**, basati su evidenze e analisi pubblicate da fonti internazionali nel corso di aprile 2026.

- **Vulnerabilità, modalità operative e superfici di compromissione**

  Nel periodo in esame, la **compromissione e l'abuso delle identità digitali** si conferma tra i vettori ricorrenti, sia nelle fasi di accesso iniziale, sia per le attività di persistenza e movimento laterale

all'interno degli ambienti compromessi, a seguito di phishing sempre più complesso, abilitato da AI e supportato da infrastrutture criminali dedicate. A testimonianza di ciò, nel mese di aprile 2026 Microsoft ha documentato una campagna di **AI-enabled device code phishing**, descritta come diffusa e finalizzata alla compromissione estesa di account organizzativi[1]. Secondo l'analisi, gli attaccanti avviano una procedura di autenticazione e ottengono un codice dispositivo valido, che viene poi trasmesso alla vittima attraverso contenuti di phishing. La vittima viene indotta a inserire tale codice su una pagina di autenticazione Microsoft legittima e a completare il processo di autenticazione; l'autorizzazione così rilasciata consente quindi all'attaccante di ottenere token validi associati all'account della vittima, senza necessità di sottrarre direttamente la password. La campagna è qualificata come **AI-enabled** in quanto l'AI risulta impiegata a supporto sia della funzionalità dell'infrastruttura di attacco (generazione dinamica dei codici dispositivo al momento dell'interazione della vittima con il link di phishing, così da preservare la validità del codice entro la finestra temporale prevista dal flusso di autenticazione), sia della personalizzazione dei contenuti per le vittime. Sempre Microsoft, nel suo report dedicato alle minacce via e-mail nel primo trimestre 2026 [2], evidenzia la centralità del **phishing** finalizzato al **furto di credenziali**, anche attraverso piattaforme di **phishing-as-a-service (PhaaS)**, come **Tycoon2FA** . In particolare,viene evidenziato il ricorso a **tecniche link-based**, nelle quali l'e-mail indirizza l'utente verso pagine esterne predisposte per la raccolta delle credenziali; a **QR code phishing**, in cui il collegamento malevolo è veicolato tramite codici QR; a **pagine di phishing precedute da CAPTCHA**, utilizzate per ostacolare l'analisi automatizzata e aumentare l'interazione dell'utente prima dell'accesso al contenuto malevolo; a **catene di reindirizzamento**, impiegate per articolare il percorso verso le pagine finali di phishing; e a schemi **adversary-in-the-middle (AiTM)** finalizzati a intercettare il flusso di autenticazione e tentare di superare difese MFA.

Anche il National Cyber Security Centre del Regno Unito ha evidenziato, il 23 aprile, come password, codici monouso, notifiche push e, più in generale, meccanismi di MFA non resistenti al phishing continuino a essere esposti a tecniche quali riutilizzo delle credenziali, session hijacking e intercettazione dei flussi di autenticazione. In tale prospettiva, il NCSC ha raccomandato l'adozione di soluzioni di autenticazione più robuste, quali passkey e credenziali basate sullo standard FIDO2 [3].

Sul piano delle **vulnerabilità**, oltre al Patch Tuesday di aprile (oggetto anche di alert del CSIRT Italia), tramite il quale **Microsoft** ha corretto 165 vulnerabilità, incluse otto classificate come critiche [4, 5], si evidenzia l'advisory relativo alla CVE-2026-35616 di **FortiClient EMS**, pubblicato da **Fortinet**. Tale vulnerabilità di improper access control può consentire a un attaccante non autenticato di eseguire codice o comandi non autorizzati tramite richieste appositamente costruite. Lo sfruttamento attivo di tale vulnerabilità è stato segnalato anche dal CSIRT Italia [6, 7]. Vale evidenziare anche la CVE-2026-31431, attenzionata dal CERT-EU e dal CSIRT Italia [8, 9], denominata Copy Fail: una vulnerabilità di local privilege escalation nel **Linux Kernel** con proof-of-concept pubblico e impatto su distribuzioni equipaggiate con kernel compilati a partire dal 2017.

Dal punto di vista delle **modalità operative**, due casi confermano la persistenza dell'**utilizzo di strumenti e servizi legittimi a fini malevoli**, con l'obiettivo di rendere più difficoltosa l'individuazione e il blocco delle attività ostili. Nella prima evidenza, pubblicata da Microsoft il 18 aprile, si descrive un'attività basata sull'**impersonificazione del personale helpdesk** tramite comunicazioni cross-tenant[13] in **Microsoft Teams** [10]. Secondo l'analisi, gli attori ostili hanno contattato gli utenti fingendosi personale di supporto IT e li hanno indotti ad avviare sessioni di assistenza

[13]Per comunicazioni cross-tenant si intendono interazioni avviate tra utenti appartenenti a tenant distinti, ossia ambienti organizzativi separati all'interno di servizi cloud come Microsoft 365 o Microsoft Teams.

remota tramite strumenti legittimi, come **Quick Assist** o soluzioni analoghe. Una volta ottenuto l'accesso interattivo al sistema, gli attaccanti hanno utilizzato applicazioni firmate, protocolli amministrativi nativi come **WinRM**, strumenti commerciali di **remote management** e utility di trasferimento dati come **Rclone**. Tali strumenti sono stati impiegati per muoversi all'interno dell'ambiente compromesso, raggiungere asset di maggiore valore e predisporre l'esfiltrazione di dati verso risorse esterne. Un ulteriore caso, documentato da **Sophos** il 16 aprile, riguarda l'**abuso di QEMU**, software open source di emulazione e virtualizzazione normalmente utilizzato per eseguire sistemi operativi o ambienti applicativi isolati [11]. In tale occasione **QEMU** è stato impiegato per creare un ambiente virtualizzato funzionale all'evasione dei controlli di sicurezza e alla distribuzione di ransomware, riducendo la visibilità degli strumenti di sicurezza installati sul sistema host. Tale modalità consente agli attori ostili di eseguire attività malevole in un ambiente meno visibile, rendendo più complessa la distinzione tra uso legittimo di strumenti di virtualizzazione e comportamento malevolo.

Per quanto riguarda l'**attività cybercriminale**, ad aprile **Europol** ha pubblicato l'**Internet Organised Crime Threat Assessment (IOCTA) 2026**, rapporto riferito all'evoluzione dell'ecosistema cybercriminale nell'arco degli ultimi dodici mesi. Il rapporto evidenzia il ruolo delle **infrastrutture criminali riusabili**, intese come servizi, piattaforme e risorse tecniche impiegabili trasversalmente da più attori o campagne; degli **accessi compromessi**, che alimentano mercati e servizi criminali orientati all'intrusione iniziale; e dei **servizi criminali specializzati**, riconducibili alla più ampia economia crime-as-a-service. Il rapporto richiama inoltre l'impiego di **proxy**, servizi di anonimizzazione, piattaforme cifrate e infrastrutture di hosting controllate o abusate dagli attori criminali, che rendono più difficili attribuzione, tracciamento e interruzione delle attività. Un ulteriore elemento di rilievo è rappresentato dall'**automazione** e dall'**AI**, descritte da Europol come fattori in grado di accelerare alcune fasi delle attività criminali, ridurre le barriere di ingresso per attori meno qualificati e aumentare la capacità di personalizzazione e scala di frodi, social engineering e altre condotte malevole. Nel dominio dei cyber-attacks, il rapporto evidenzia anche la persistenza dell'ecosistema **ransomware**, il ruolo degli **infostealer** nel rifornire il mercato criminale di credenziali e dati, e il ricorso a forme di pressione sulle vittime basate su **furto di dati**, minaccia di pubblicazione, indisponibilità dei servizi e altre leve estorsive [12].

In tale contesto si colloca il caso **VECT 2.0**, un **ransomware-as-a-service** emerso tra la fine del 2025 e l'inizio del 2026 e analizzato ad aprile da **Check Point Research**. Secondo l'analisi pubblicata, il malware è progettato per cifrare i dati delle vittime a fini estorsivi; tuttavia, a causa di errori nell'implementazione della cifratura, nei file di dimensioni superiori a 128 KB vengono perse informazioni necessarie alla successiva decifratura. Di conseguenza, in tali condizioni, il pagamento del riscatto non consentirebbe comunque il recupero completo dei dati, rendendo gli effetti dell'attacco assimilabili a quelli di un **wiper** [13].

Le evidenze mensili relative all'**impiego dell'AI in ambito cyber** confermano un utilizzo prevalentemente abilitante della tecnologia, più che l'emergere di capacità offensive pienamente autonome e generalizzate. In questo quadro rientra anche la già citata campagna di **AI-enabled device code phishing** documentata da **Microsoft**, nella quale l'AI risulta impiegata a supporto dell'automazione, della personalizzazione dei contenuti e della scalabilità di tecniche di accesso iniziale già note [1]. Ciò in coerenza con il quadro di scenario delineato nel già citato report **Internet Organised Crime Threat Assessment (IOCTA) 2026** di **Europol**, che descrive l'AI come un fattore di accelerazione, automazione e scalabilità delle attività cybercriminali, in particolare a supporto di **social engineering**, frodi, automazione dei processi e riduzione delle barriere di accesso a capacità tecniche specialistiche [12].

Di interesse sul tema, inoltre, quanto pubblicato

il 13 aprile 2026 dall'**UK AI Security Institute** relativamente alla valutazione delle capacità cyber di **Claude Mythos Preview**, modello frontier[14] sviluppato da **Anthropic** e collegato al **Project Glasswing**, iniziativa volta a impiegare tali capacità in chiave difensiva per la sicurezza del software critico [**Anthropic2026Glasswing**, 14]. In ambienti controllati e con accesso esplicitamente autorizzato, la valutazione indica che il modello avrebbe mostrato capacità rilevanti nella risoluzione di task cyber e nella conduzione di simulazioni multi-step [14]. Il 21 aprile, inoltre, **Mozilla** ha pubblicato un post in cui riferisce che l'impiego di una versione preliminare del medesimo modello su **Firefox** avrebbe contribuito all'identificazione di **271 vulnerabilità**, corrette nel rilascio di **Firefox 150** [15].

- **Contesto geopolitico**

  Nel mese di aprile 2026, il conflitto tra **Stati Uniti**, **Israele** e **Iran** ha continuato a produrre effetti anche nel **dominio cibernetico**, con particolare riferimento a **infrastrutture critiche**, **servizi essenziali**, sistemi **OT** e asset informativi riconducibili agli attori coinvolti o a soggetti collocati nell'area interessata dalla crisi. In tale quadro si colloca l'advisory pubblicato il 7 aprile da diverse agenzie statunitensi, tra cui **CISA**, **FBI** e **NSA**, che riporta attività di **attori affiliati all'Iran** contro **PLC Rockwell Automation/Allen-Bradley**[15] esposti su Internet, utilizzati nei settori dei **servizi governativi**, del **settore idrico e trattamento delle acque reflue** e dell'**energia** [16].

  Nel medesimo contesto si colloca l'analisi pubblicata il 16 aprile da **Darktrace**, società britannica specializzata in **cybersecurity**, su **ZionSiphon**, malware descritto come apparentemente progettato per il targeting di **infrastrutture idriche** e di **desalinizzazione israeliane**. L'azienda evidenzia tuttavia elementi di incompletezza o imperfezione implementativa nel campione analizzato, suggerendo cautela nel derivare conclusioni su eventuali **impatti operativi effettivi** [17, 18].

  D'interesse anche il ricorso a forme di **doxing**, **intimidazione** e **pressione informativa** nei confronti di personale militare, riportate da diverse fonti giornalistiche e rivendicate dal gruppo filo-iraniano **Handala**. Secondo tali fonti, sarebbero stati pubblicati dati personali di **2.379 Marines statunitensi** dispiegati nell'area del **Golfo Persico** e del **Medio Oriente**; contestualmente, sarebbe stato segnalato l'invio di messaggi intimidatori via **WhatsApp** a personale statunitense nella regione [19, 20, 21]. Le fonti disponibili precisano che la qualità delle informazioni e la portata effettiva della compromissione non risultano verificabili in maniera indipendente.

  Sul piano interno iraniano, si protraggono le forti restrizioni alla **connettività Internet** nel Paese [22]. Il 28 aprile, **Reuters** ha riferito una parziale riapertura dell'accesso a Internet, limitata ad alcune attività economiche attraverso il servizio denominato **Internet Pro**; nello stesso periodo, **NetBlocks** ha continuato a segnalare la persistenza di restrizioni alla connettività per la popolazione [23].

[14] Con l'espressione modelli frontier si fa riferimento a sistemi di AI di ultima generazione dotati di capacità avanzate e generaliste, suscettibili di essere specializzati o adattati a domini tecnici specifici, incluso quello cyber.

[15] I PLC sono dispositivi di controllo industriale utilizzati per gestire processi fisici, come valvole, pompe, sensori e sistemi di automazione; la loro esposizione in rete può quindi tradursi in rischi diretti per la continuità operativa dei servizi erogati. **Rockwell Automation** è un fornitore statunitense di soluzioni di **automazione industriale**, mentre **Allen-Bradley** identifica una linea di prodotti e controllori industriali utilizzati in ambienti **OT**.

Riferimenti

[1] Microsoft Defender Security Research. *Inside an AI-enabled device code phishing campaign*. Accessed 2026-05-05. Apr. 2026. URL: https://www.microsoft.com/en-us/security/blog/2026/04/06/ai-enabled-device-code-phishing-campaign-april-2026/.

[2] Microsoft Threat Intelligence. *Email threat landscape: Q1 2026 trends and insights*. Accessed 2026-05-05. Apr. 2026. URL: https://www.microsoft.com/en-us/security/blog/2026/04/30/email-threat-landscape-q1-2026-trends-and-insights/.

[3] National Cyber Security Centre (NCSC). *Passkeys are more secure than traditional ways to log in*. Accessed 2026-05-05. Apr. 2026. URL: https://www.ncsc.gov.uk/blogs/passkeys-are-more-secure-than-traditional-ways-to-log-in.

[4] Cisco Talos. *Microsoft Patch Tuesday for April 2026 – Snort Rule and Prominent Vulnerabilities*. Accessed 2026-05-05. Apr. 2026. URL: https://blog.talosintelligence.com/microsoft-patch-tuesday-april-2026/.

[5] CSIRT Italia. *Aggiornamenti Mensili Microsoft*. Alert AL02/260415/CSIRT-ITA; accessed 2026-05-06. Apr. 2026. URL: https://www.acn.gov.it/portale/w/aggiornamenti-mensili-microsoft-19.

[6] Fortinet FortiGuard Labs. *CVE-2026-35616 – FortiClient EMS Improper Access Control Vulnerability*. Accessed 2026-05-05. Apr. 2026. URL: https://fortiguard.fortinet.com/psirt/FG-IR-26-099.

[7] CSIRT Italia. *FortiClient EMS: rilevato sfruttamento in rete della CVE-2026-35616*. Alert AL01/260405/CSIRT-ITA; accessed 2026-05-06. Apr. 2026. URL: https://www.acn.gov.it/portale/w/forticlient-ems-rilevato-sfruttamento-in-rete-della-cve-2026-35616.

[8] CERT-EU. *2026-005: High Vulnerability in the Linux Kernel ("Copy Fail")*. Accessed 2026-05-05. Apr. 2026. URL: https://cert.europa.eu/publications/security-advisories/2026-005/.

[9] CSIRT Italia. *Linux: disponibile PoC per lo sfruttamento della CVE-2026-31431*. Alert AL02/260430/CSIRT-ITA; updated 2026-05-04; accessed 2026-05-06. Apr. 2026. URL: https://www.acn.gov.it/portale/w/linux-disponibile-poc-per-lo-sfruttamento-della-cve-2026-31431.

[10] Microsoft Threat Intelligence. *Cross-tenant helpdesk impersonation to data exfiltration: A human-operated intrusion playbook*. Accessed 2026-05-05. Apr. 2026. URL: https://www.microsoft.com/en-us/security/blog/2026/04/18/crosstenant-helpdesk-impersonation-data-exfiltration-human-operated-intrusion-playbook/.

[11] Sophos X-Ops. *QEMU abused to evade detection and enable ransomware delivery*. Accessed 2026-05-05. Apr. 2026. URL: https://www.sophos.com/en-us/blog/qemu-abused-to-evade-detection-and-enable-ransomware-delivery.

[12] Europol. *The evolving threat landscape: How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026*. Accessed 2026-05-05. Apr. 2026. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA-2026.pdf.

[13] Check Point Research. *VECT: Ransomware by design, Wiper by accident*. Accessed 2026-05-05. Apr. 2026. URL: https://research.checkpoint.com/2026/vect-ransomware-by-design-wiper-by-accident/.

[14] UK AI Security Institute. *Our evaluation of Claude Mythos Preview's cyber capabilities*. Accessed 2026-05-05. Apr. 2026. URL: https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities.

[15] Bobby Holley. *The zero-days are numbered*. Mozilla Blog. Apr. 2026. URL: https://blog.mozilla.org/en/privacy-security/ai-security-zero-day-vulnerabilities/ (visitato il giorno 07/05/2026).

[16] Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI) e National Security Agency (NSA). *Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers*. Joint advisory AA26-097A; accessed 2026-05-05. Apr. 2026. URL: https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a.

[17] Darktrace. *Inside ZionSiphon: Darktrace's Analysis of OT Malware Targeting Israeli Water Systems*. Accessed 2026-05-05. Apr. 2026. URL: https://www.darktrace.com/blog/inside-zionsiphon-darktraces-analysis-of-ot-malware-targeting-israeli-water-systems.

[18] Ravie Lakshmanan. *Researchers Detect ZionSiphon Malware Targeting Israeli Water, Desalination OT Systems*. Accessed 2026-05-06. Apr. 2026. URL: https://thehackernews.com/2026/04/researchers-detect-zionsiphon-malware.html.

[19] Shafaq News. *Iran-linked hackers leak data of 2K US soldiers*. Apr. 2026. URL: https://shafaq.com/en/Middle-East/Iran-linked-hackers-leak-data-of-2K-US-soldiers (visitato il giorno 07/05/2026).

[20] Stars and Stripes. *Handala hack: Iran-linked hackers claim leak of US personnel data*. Apr. 2026. URL: https://www.stripes.com/theaters/middle_east/2026-04-28/handala-hack-iran-bahrain-navy-21510827.html (visitato il giorno 07/05/2026).

[21] The Wall Street Journal. *Iran-linked hackers target U.S. troops in Middle East*. Apr. 2026. URL: https://www.wsj.com/livecoverage/iran-war-strait-of-hormuz-2026/card/iran-linked-hackers-target-u-s-troops-in-middle-east-34xGWbjMmtEv8djtTQLr (visitato il giorno 07/05/2026).

[22] NetBlocks. *Internet connectivity restrictions in Iran*. Apr. 2026. URL: https://mastodon.social/@netblocks/116498193803980435 (visitato il giorno 07/05/2026).

[23] Reuters. *Iran eases internet curbs for businesses as blackout enters third month*. Apr. 2026. URL: https://www.reuters.com/sustainability/society-equity/iran-eases-internet-curbs-businesses-blackout-enters-third-month-2026-04-28/ (visitato il giorno 07/05/2026).

LaTeX

Agenzia per la
Cybersicurezza Nazionale

OPERATIONAL SUMMARY

aprile 2026