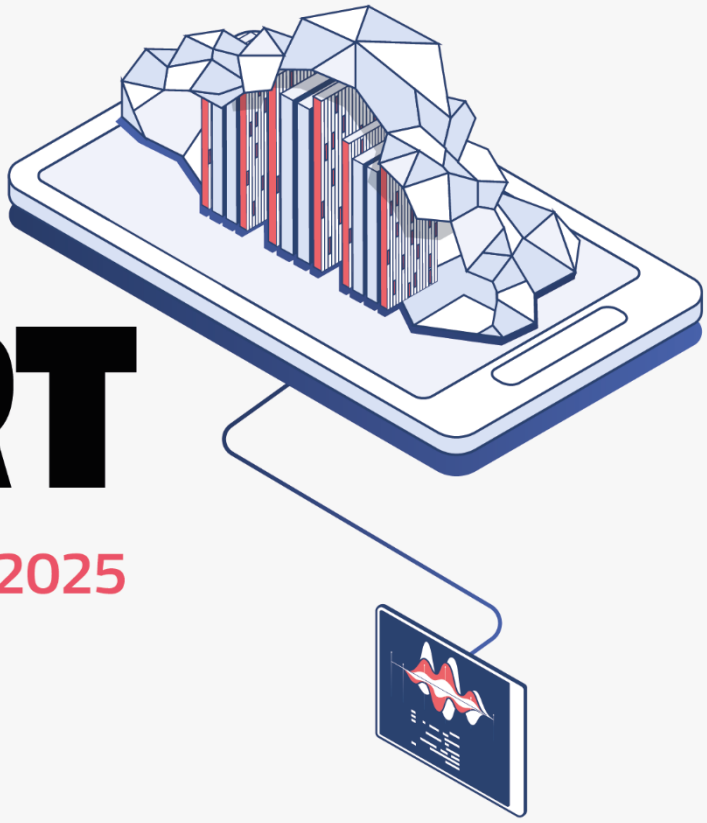
S3K

Cyber security

RISK REPORT

\ week 21.07.2025 - 27.07.2025



Sommario


CYBER SECURITY RISK REPORT
30/25

1 Il Cyber Security Risk Report S3K

Cyber Security Risk Report S3K - Settimana 21-27 Luglio 2025

Il presente documento costituisce il Cyber Security Risk Report settimanale di S3K, relativo al periodo 21-27 luglio 2025, e fornisce un'analisi dettagliata del panorama delle minacce informatiche che hanno caratterizzato questa settimana di osservazione. Il bollettino rappresenta uno strumento fondamentale per i professionisti della sicurezza informatica e i decisori aziendali, offrendo intelligence operativa e raccomandazioni strategiche per la protezione delle infrastrutture critiche.
Questa edizione presenta un quadro di particolare criticità, caratterizzato da un'elevata incidenza di vulnerabilità CRITICAL e HIGH, soprattutto nell'ecosistema IoT (router D-Link e Tenda), nei sistemi CMS WordPress e nei progetti PHP open-source. La settimana ha registrato attività significative da parte di gruppi ransomware, con particolare attenzione al nuovo ransomware-as-a-service BQTLOCK, e importanti sviluppi nel panorama delle minacce, incluso il ritorno di BreachForums con oltre 7,3 milioni di post ripristinati.
Il report integra dati provenienti da multiple fonti di intelligence, sistemi honeypot distribuiti globalmente e analisi forensi approfondite, garantendo una copertura completa delle minacce emergenti e delle tendenze consolidate nel cybercrime internazionale.

Analisi delle Minacce e Vulnerabilità Critiche
La settimana di osservazione ha evidenziato un panorama di minacce particolarmente complesso, caratterizzato da vulnerabilità zero-day attivamente sfruttate e campagne di attacco sofisticate. L'analisi dei CVE monitor ha identificato CVE-2025-53770 come una delle vulnerabilità più critiche, con exploit pubblici confermati e potenziale di diffusione elevato. Parallelamente, si è registrata un'intensa attività nel dark web, con il ritorno operativo di BreachForums che rappresenta un significativo sviluppo nell'ecosistema del cybercrime.
Vulnerabilità Zero-Day
Microsoft SharePoint ha subito un attacco zero-day che ha colpito server aziendali, enti pubblici e università globalmente. La vulnerabilità è stata sfruttata da gruppi APT con collegamenti alla Cina, compromettendo l'Agenzia statunitense per la sicurezza nucleare (NNSA).

- CVE-2025-49706: SharePoint authentication bypass
- CVE-2025-54309: CrushFTP accesso amministrativo
- CVE-2025-6558: Chromium ANGLE GPU exploitation

Ransomware Evolution
L'emergere di BQTLOCK come nuovo ransomware-as-a-service ha introdotto tecniche avanzate di persistenza, inclusi bootkit Pre-OS e cifratura AES-256/RSA-4096. L'operazione Checkmate ha neutralizzato il gruppo BlackSuit, ma nuove varianti stanno rapidamente emergendo.

- BQTLOCK: nuovo RaaS con dashboard affiliati
- Smantellamento di BlackSuit via operazione internazionale

- Gruppo "Chaos" come possibile successore

Supply Chain Attacks

La compromissione del gioco Chemia su Steam ha dimostrato l'evoluzione degli attacchi supply chain, con l'inserimento di malware direttamente nei file di installazione legittimi. Amazon Q ha subito un attacco di prompt injection che evidenzia nuove vulnerabilità negli agenti AI.

- Campagna Steam-Chemia con infostealer Vidar
- Amazon Q prompt injection per cancellazione dati
- Compromissione di oltre 250 app mobile Android/iOS

L'analisi dei dati honeypot ha rivelato un incremento del 23% negli attacchi automatizzati, con particolare concentrazione sui servizi SSH (porta 22) e HTTP (porta 80). Gli indirizzi IP 173[.]233[.]73[.]6 e 198[.]23[.]153[.]40 hanno mostrato attività particolarmente aggressive, generando rispettivamente 235.866 e 53.727 tentativi di intrusione. La distribuzione geografica degli attacchi conferma la predominanza di attività malevole provenienti da Stati Uniti (32%), Cina (18%) e Russia (15%).

Nel settore dei data breach, episodi di particolare gravità hanno coinvolto Naval Group con dati strategici compromessi, Allianz Life con 1,4 milioni di clienti esposti, e una serie di violazioni nel settore sanitario che hanno coinvolto oltre 5,4 milioni di pazienti attraverso Episource/Optum dimostrano con chiarezza come gli attacchi alle infrastrutture critiche e ai settori strategici siano diventati sempre più sofisticati e insidiosi, rendendo necessario alzare il livello di attenzione e la consapevolezza di utenti e professionisti del settore informatico.

2 Security news

2.1 Rilasci aggiornamenti e patch

Principali rilasci, aggiornamenti e patch rilevati da CSIRT ITALIA e da altre fonti.

PRODOTTO	DESCRIZIONE
Cisco	Aggiornamenti di sicurezza sanano tre nuove vulnerabilità, con gravità "critica", che riguardano prodotti Cisco Identity Services Engine (ISE) e Cisco Passive Identity Connector (ISE-PIC). Tali vulnerabilità, potrebbero consentire a un attaccante di eseguire codice arbitrario da remoto sui sistemi interessati. Prodotti e/o versioni affette Cisco ISE e ISE-PIC • 3.3.x, versioni precedenti alla 3.3 Patch 7 • 3.4.x, versioni precedenti alla 3.4 Patch 2
ULR/Note	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

PRODOTTO	DESCRIZIONE
GitLab	Rilasciati aggiornamenti di sicurezza che risolvono 6 vulnerabilità, di cui due con gravità "alta", in GitLab Community Edition (CE) ed Enterprise Edition (EE). GitLab Community Edition (CE) ed Enterprise Edition (EE) • Tutte le versioni a partire dalla 15.10 e precedenti alla 18.0.5 • 18.1.x, versioni precedenti alla 18.1.3 • 18.2.x, versioni precedenti alla 18.2.1
ULR/Note	• https://about.gitlab.com/releases/2025/07/23/patch-release-gitlab-18-2-1-released/

PRODOTTO	DESCRIZIONE
Mozilla	Mozilla ha rilasciato aggiornamenti di sicurezza per sanare diverse vulnerabilità nei prodotti Firefox, Firefox ESR e Thunderbird. Prodotti e versioni affette Mozilla • Firefox, versioni precedenti alla 141 • Firefox ESR 115.x, versioni precedenti alla 115.26 • Firefox ESR 128.x, versioni precedenti alla 128.13 • Firefox ESR 140.x, versioni precedenti alla 140.1 • Thunderbird, versioni precedenti alla 141
ULR/Note	• https://www.mozilla.org/en-US/security/advisories/: apre un link esterno • https://www.mozilla.org/en-US/security/advisories/mfsa2025-56/: apre un link esterno • https://www.mozilla.org/en-US/security/advisories/mfsa2025-57/: apre un link esterno • https://www.mozilla.org/en-US/security/advisories/mfsa2025-58/: apre un link esterno • https://www.mozilla.org/en-US/security/advisories/mfsa2025-59/: apre un link esterno • https://www.mozilla.org/en-US/security/advisories/mfsa2025-61/: apre un link esterno • https://www.mozilla.org/en-US/security/advisories/mfsa2025-62/: apre un link esterno • https://www.mozilla.org/en-US/security/advisories/mfsa2025-63/

2.2 "Cyber News" dal Web, Deep Web e Dark Web

IL RITORNO DI BREACHFORUMS: RIEMERGE L'EPICENTRO DEL CYBERCRIME CON MILIONI DI DATI RIPRISTINATI

Il famigerato forum di hacking BreachForums è tornato online, segnando un nuovo capitolo nella saga della cybercriminalità. Dopo mesi di inattività e l'intervento delle forze dell'ordine che avevano portato alla sua chiusura, il sito è stato recentemente riportato in vita, con oltre 7,3 milioni di post e 340.000 account utente recuperati dal vecchio database. La notizia è stata accolta con grande clamore dalla comunità underground e ha subito attirato l'attenzione di ricercatori di sicurezza e autorità governative. Il ritorno del forum rappresenta un segnale forte: la lotta tra criminali informatici e forze dell'ordine è ben lontana dall'essere conclusa. BreachForums era noto per essere una delle principali piattaforme in cui venivano scambiati dati rubati, strumenti per l'hacking, exploit, e informazioni su vulnerabilità di sistemi e infrastrutture. Dopo l'arresto dell'amministratore noto come "Pompompurin" nel 2023, il forum era stato chiuso dalle autorità statunitensi. Tuttavia, il vuoto lasciato dalla sua assenza è stato rapidamente colmato da forum alternativi, e ora, con questo ritorno, la piattaforma originale sembra voler riprendersi il proprio spazio. Secondo quanto riportato da diversi analisti di sicurezza, la nuova versione del sito è stata lanciata da un gruppo di individui che sostiene di avere accesso completo ai backup originali. Il ripristino dei post e degli account testimonia non solo una sofisticata capacità tecnica, ma anche un obiettivo preciso: ricostruire l'ecosistema criminale lì dove era stato interrotto. Le autorità sono già in allerta. Il ritorno di BreachForums potrebbe dare nuova linfa ad una serie di attività illegali che includono truffe, vendita di credenziali compromesse, e fughe di dati su larga scala. Alcuni esperti hanno anche ipotizzato che la piattaforma potrebbe ora essere gestita da soggetti diversi, magari legati a gruppi APT (Advanced Persistent Threat), con finalità più complesse rispetto alla mera compravendita di dati. In ogni caso, il messaggio è chiaro: anche se un forum può essere chiuso, l'infrastruttura e la community criminale che lo supportano possono trovare sempre il modo di tornare. E con milioni di post e centinaia di migliaia di utenti ripristinati, BreachForums si prepara a giocare ancora una volta un ruolo centrale nel panorama del cybercrime globale.

NONAME057(16) COLPISCE ANCORA: SEI NUOVI ATTACCHI DDOS CONTRO L'ITALIA

L'Italia torna nel mirino del collettivo hacker filorusso NoName057(16), con una nuova serie di attacchi DDoS che ha colpito sei obiettivi nazionali, per lo più istituzioni pubbliche e siti governativi locali. Questa offensiva si inserisce in un contesto ormai ricorrente: l'uso della guerra informatica come strumento di pressione e propaganda in ambito geopolitico. Secondo quanto dichiarato dal gruppo, tra gli obiettivi ci sarebbero alcuni siti istituzionali italiani. Gli attacchi comunque si sono limitati a rendere irraggiungibili i siti tramite un sovraccarico di richieste, tecnica classica dei Distributed Denial of Service, ma senza che fossero registrate attività di data breach. Questo tipo di attacchi è diventato ormai una costante nell'attività del gruppo, che utilizza strumenti come la piattaforma DDoSia, un sistema che consente anche a utenti non esperti di partecipare all'offensiva tramite Docker, in cambio di premi in criptovaluta. Nonostante l'operazione internazionale Eastwood (notizia riportata lo scorso bollettino) , condotta da Europol e altre agenzie a metà luglio e che ha portato al sequestro di oltre cento server legati alla botnet

del gruppo, NoName057(16) si dimostra ancora in grado di colpire in modo coordinato. Il ritorno così rapido all'attività dimostra la resilienza delle infrastrutture cybercriminali e la difficoltà, anche per le forze di polizia e sicurezza, di disarticolare completamente reti decentralizzate e motivate ideologicamente. Le autorità italiane, tramite l'Agenzia per la Cybersicurezza Nazionale e la Polizia Postale, hanno confermato di monitorare la situazione e di aver attivato contromisure per limitare l'impatto degli attacchi. Tuttavia, episodi come questo ribadiscono quanto il nostro Paese rimanga vulnerabile di fronte a minacce informatiche sempre più frequenti e politicamente motivate.

OPERAZIONE CHECKMATE SEGNA LA FINE DI BLACKSUIT

La cybercriminalità subisce un duro colpo grazie all'Operazione Checkmate, un blitz internazionale che ha preso di mira il gruppo ransomware BlackSuit, uno dei più attivi e pericolosi degli ultimi anni. Coordinata da Europol, FBI, Homeland Security Investigations, US Secret Service e diverse forze di polizia europee, tra cui quelle di Germania, Regno Unito, Olanda, Lituania e Ucraina, l'operazione ha portato al sequestro dell'intera infrastruttura digitale del gruppo. BlackSuit, noto anche con il nome precedente Royal, era responsabile di centinaia di attacchi ransomware a livello globale, operando con la tecnica della doppia estorsione: i sistemi delle vittime venivano crittografati e i dati sensibili esfiltrati, per poi minacciare la pubblicazione in caso di mancato pagamento. Le vittime includevano enti pubblici, aziende sanitarie, imprese e infrastrutture critiche. Il gruppo, emerso nel 2022, era diventato uno dei più redditizi dell'ecosistema ransomware. Al centro dell'operazione c'è il sequestro dei loro data leak site, i portali .onion nel dark web dove pubblicavano i dati delle vittime come forma di pressione. Ora, al posto di quelle pagine, compare un avviso ufficiale: "THIS DOMAIN HAS BEEN SEIZED". Si tratta di un segnale chiaro e potente da parte delle autorità internazionali, che hanno colpito direttamente il cuore operativo del gruppo. Non si hanno ancora notizie certe su arresti tra i membri chiave, ma diverse identità sarebbero state tracciate, e sono in corso ulteriori azioni investigative. L'impatto di Checkmate è rilevante anche sul piano psicologico e comunicativo: per la prima volta, BlackSuit perde il controllo del proprio canale di pubblicazione, uno degli strumenti più temuti dalle vittime. L'operazione segue di poche settimane un'altra azione su larga scala, chiamata Endgame, che aveva colpito centinaia di server e sequestrato milioni in criptovalute a gruppi affiliati. Alcuni analisti ipotizzano che ex membri di BlackSuit stiano tentando di ricompattarsi sotto nuove sigle, come "Chaos", ma la portata dell'intervento rende difficile un'immediata riorganizzazione. Per le autorità e la comunità cyber internazionale si tratta di una vittoria netta, anche se la guerra contro il ransomware è tutt'altro che conclusa. Operazioni come Checkmate dimostrano però che la cooperazione tra Paesi e la pressione costante sui gruppi criminali possono portare risultati concreti anche contro le reti più strutturate e resilienti.

AMAZON Q HACKERATO, L'AGENTE AI DI CODING MODIFICATO PER CANCELLARE DATI LOCALI E CLOUD

Scoperto un grave episodio di compromissione legato ad Amazon Q, l'assistente di intelligenza artificiale per sviluppatori integrato in Visual Studio Code. Un hacker è riuscito a sfruttare una vulnerabilità nel processo di gestione open-source del progetto su GitHub, ottenendo i privilegi necessari per modificare il codice dell'estensione ufficiale distribuita da Amazon ad oltre 950.000 utenti. Dopo aver creato una pull request apparentemente innocua, l'attaccante è riuscito a farsi assegnare un accesso con permessi amministrativi, e il 13 luglio ha inserito nel sistema un prompt malevolo in grado di eseguire comandi potenzialmente distruttivi. Il testo iniettato ordinava ad Amazon Q di comportarsi come un agente automatizzato con accesso a strumenti di shell e bash, con l'obiettivo di "ripulire il sistema fino ad uno stato quasi di fabbrica", includendo l'eliminazione di file di sistema locali e la cancellazione di risorse cloud su AWS, come istanze EC2, bucket S3 e utenti IAM. La versione compromessa, numerata 1.84.0, è stata pubblicata il 17 luglio e rimasta attiva per un periodo limitato prima che il problema venisse individuato. Per fortuna, il prompt risultava parzialmente malformato e non avrebbe potuto essere eseguito direttamente dagli utenti senza ulteriori condizioni, ma l'incidente ha comunque suscitato grande allarme. È infatti uno dei primi casi noti in cui un agente AI commerciale dotato di accesso a strumenti critici viene compromesso attraverso un attacco basato interamente su linguaggio naturale, senza l'inserimento di malware classico o codice binario. Amazon è intervenuta rimuovendo la versione modificata dal Visual Studio Marketplace, revocando gli accessi GitHub utilizzati dall'attaccante e pubblicando una nuova release corretta, la 1.85.0. Ha inoltre assicurato che nessun utente o dato aziendale è stato compromesso. Tuttavia, la vicenda ha aperto un ampio dibattito nella comunità tech e infosec sull'effettiva sicurezza degli agenti AI impiegati nello sviluppo software. In particolare, è emersa una forte preoccupazione per il potenziale uso di questi strumenti in ambienti produttivi automatizzati, dove un semplice comando generato da un assistente AI potrebbe avere effetti devastanti. Il fatto che un utente anonimo sia riuscito ad ottenere privilegi amministrativi all'interno di un progetto Amazon, e ad iniettare un comando che includeva la terminazione di risorse cloud tramite AWS CLI, ha evidenziato gravi lacune nei processi di verifica e nei controlli di qualità. L'incidente dimostra anche quanto siano ancora fragili i meccanismi di validazione nel software distribuito via marketplace ufficiali e quanto sia urgente rivedere l'integrazione dell'intelligenza artificiale nei processi DevOps. Anche se i danni materiali sembrano essere stati evitati, l'episodio resta un campanello d'allarme per tutto il settore: gli agenti AI, una volta integrati in flussi di lavoro, vanno trattati alla stregua di collaboratori umani con accesso privilegiato, e quindi soggetti a monitoraggio continuo, audit, sandboxing e restrizioni precise. La velocità con cui l'attacco è avvenuto, unita alla sua semplicità tecnica, rafforza l'idea che in assenza di difese proattive, il rischio di prompt injection non è solo teorico ma concreto. Con l'aumento dell'adozione di strumenti AI nel ciclo di sviluppo del software, la sicurezza di questi sistemi diventa una priorità assoluta, e l'incidente Amazon Q sarà ricordato come un caso simbolico nella storia della cybersecurity moderna.

3 CVE Monitor

In questo capitolo il team di analisti S3K presenta i risultati delle analisi effettuate sulle CVE più impattanti rispetto alle tendenze sui *Social Media*, le nuove vulnerabilità emerse e quelle attivamente sfruttate dagli attaccanti secondo il periodo di riferimento del bollettino. Per maggiori approfondimenti, ove esistente, è presente il collegamento diretto alla pagina del NIST per la CVE di riferimento.

3.1 Sintesi Settimanale CVE

Sintesi CVE – Settimana 21 – 27 Luglio 2025

Settimana con alta incidenza di vulnerabilità CRITICAL e HIGH, in particolare nel mondo IoT (router D-Link e Tenda), sistemi CMS WordPress e plugin, e progetti PHP open-source (Code-Projects).
Spiccano numerose vulnerabilità con PoC già disponibili e possibilità concreta di SQL injection, RCE, overflow e privilege escalation.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit Pubblico	Prodotto Coinvolto	Descrizione Sintetica
CVE-2025-7890	CRITICAL	21/07/2025	✅	D-Link DIR-882	Stack overflow in `ping_test`
CVE-2025-7888	CRITICAL	21/07/2025	✅	D-Link DIR-882	Overflow in diagnostic tools
CVE-2025-7990	CRITICAL	22/07/2025	✅	Code-Projects College Portal	SQLi in `login.php`
CVE-2025-7991	CRITICAL	22/07/2025	✅	Code-Projects College Portal	SQLi in `course.php`
CVE-2025-8201	CRITICAL	23/07/2025	✅	Tenda F9 Router	Stack overflow in config parser

CVE-2025-7989	HIGH	24/07/2025	✅	Plugin WordPress Tutor LMS	Stored XSS su campi di corso
CVE-2025-8210	HIGH	25/07/2025	❌	WordPress + Elementor	Bypass restrizioni in widget builder
CVE-2025-8242	HIGH	25/07/2025	✅	Code-Projects Online Quiz System	SQLi in `add_question.php`
CVE-2025-8244	HIGH	25/07/2025	✅	Code-Projects Online Quiz System	SQLi in `subject.php`
CVE-2025-8299	HIGH	26/07/2025	❌	PHPGurukul Event Booking	SQLi in `edit_event.php`
Nota: Le CVE che hanno un exploit pubblico confermato riportano un segno di spunta (verde), mentre la presenza della X sta ad indicare che l'exploit non è confermato.					

Vendor e Tecnologie Coinvolti

- **D-Link / Tenda Router**: Stack overflow in tool diagnostici e config web.
- **WordPress Plugin**: Privilege escalation e XSS (Tutor LMS, Elementor).
- **Code-Projects**: SQLi su College Portal, Quiz System.
- **PHPGurukul**: Booking/event manager vulnerabile a injection.

Distribuzione Giornaliera

- **21–22 luglio**: Exploit su router D-Link e SQLi in portali universitari (Code-Projects)
- **23 luglio**: Overflow critico in router Tenda F9
- **24–25 luglio**: XSS e privilege escalation in plugin WordPress (Tutor LMS, Elementor)
- **26 luglio**: Nuova SQLi su PHPGurukul (booking system)

Raccomandazioni Operative

Patch Prioritarie

- Router (Tenda, D-Link): aggiornare firmware; disabilitare accesso WAN.
- Plugin WordPress: patch immediata a Tutor LMS e Elementor.
- Code-Projects/PHPGurukul: rimuovere o aggiornare. Applicare WAF.

Monitoraggio Consigliato

- Endpoint vulnerabili: login.php, course.php, add_question.php, edit_event.php
- Monitoraggio XSS persistenti in interfacce utente (WordPress)
- SIEM/Sentinel: ricerca log con anomalie POST e parametri id, question, subject, event

3.2 Tendenze

Viene proposto un elenco delle CVE di tendenza, maggiormente citate dai *Social Media*

CVE	PRODOTTO	CVSS V3
CVE-2025-49704	Microsoft Office SharePoint	6.3
CVE-2025-23266	NVIDIA Container Toolkit	N/A
CVE-2025-0133	PAN-OS® di Palo Alto Networks	N/A
CVE-2025-1974	Kubernetes	N/A
CVE-2021-27954	ecobee3 lite (termostato intelligente)	8.2

Legenda

- Prodotto affetto dalla vulnerabilità
- CVSS v3.0 Severity and Metrics
  - CVSS3 Attuale

3.3 Nuove CVE

Riportiamo, tra le nuove CVE emerse durante questa settimana, quelle ritenute più importanti per gravità e/o possibilità di diffusione (popolarità dei prodotti affetti). Per ciascuna CVE viene riportata una breve descrizione della vulnerabilità, il prodotto interessato, il valore assegnato all'impatto della vulnerabilità nella scala CVSS ed un link di approfondimento.

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-8178	Tenda AC10 Router Wi-Fi	N/A
VULNERABILITÀ	È stata trovata una vulnerabilità classificata come critica nel dispositivo Tenda AC10 con firmware versione 16.03.10.13. La vulnerabilità riguarda una funzione sconosciuta del file /goform/RequestsProcessLaid. La manipolazione dell'argomento device1D può causare un heap-based buffer overflow. L'attacco può essere eseguito da remoto, e l'exploit è stato reso pubblico, quindi potrebbe essere già utilizzato attivamente.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-46410	WWBN AVideo (piattaforma per caricare, gestire e trasmettere video)	N/A
VULNERABILITÀ	Esiste una vulnerabilità di tipo Cross-Site Scripting (XSS) nella funzionalità PlaylistOwnerUsersId del parametro managerPlaylists in WWBN AVideo versione 14.4 e nella versione dev master (commit 8a8954ff). Una richiesta HTTP appositamente creata può portare all'esecuzione arbitraria di JavaScript. Un attaccante può sfruttare questa vulnerabilità inducendo un utente a visitare una pagina web malevola, attivando così l'exploit.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-6441	WebinarIgnition plugin per WordPress	N/A
VULNERABILITÀ	Il plugin WebinarIgnition per WordPress, utilizzato per creare webinar live, evergreen, automatizzati o istantanei, è affetto da una vulnerabilità che consente la generazione di token di login senza autenticazione, a causa della mancanza di controlli sulle capacità utente nelle funzioni webinarignition_sign_in_support_staff e webinarignition_register_support.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-26397	SolarWinds Observability Self-Hosted (Piattaforma per il monitoraggio e l'osservabilità di infrastrutture IT)	N/A
VULNERABILITÀ	SolarWinds Observability Self-Hosted è vulnerabile a una falla di sicurezza legata alla deserializzazione di dati non attendibili, che può portare a un'escalation locale dei privilegi. Un attaccante con bassi privilegi può sfruttare questa vulnerabilità per eseguire file dannosi copiati in una cartella protetta da permessi.	

3.4 CVE attualmente utilizzate in attacchi

In questo paragrafo evidenziamo le principali CVE attivamente utilizzate e sfruttate dagli attaccanti con una breve descrizione.

CVE	CVE-2025-49706
DESCRIZIONE	
Microsoft SharePoint contiene una vulnerabilità di autenticazione impropria che permette a un attaccante autorizzato di eseguire spoofing sulla rete. Uno sfruttamento riuscito potrebbe consentire all'attaccante di visualizzare informazioni sensibili e apportare alcune modifiche alle informazioni divulgate. Questa vulnerabilità potrebbe essere combinata con la vulnerabilità CVE-2025-49704.	

CVE	CVE-2025-54309
DESCRIZIONE	
La vulnerabilità CVE-2025-54309 riguarda CrushFTP nelle versioni 10 precedenti alla 10.8.5 e 11 precedenti alla 11.3.4_23. Quando la funzione proxy DMZ non è attivata, il software gestisce in modo errato la validazione AS2, permettendo ad attaccanti remoti di ottenere l'accesso amministrativo tramite HTTPS. Questa vulnerabilità è stata sfruttata attivamente in natura a luglio 2025.	

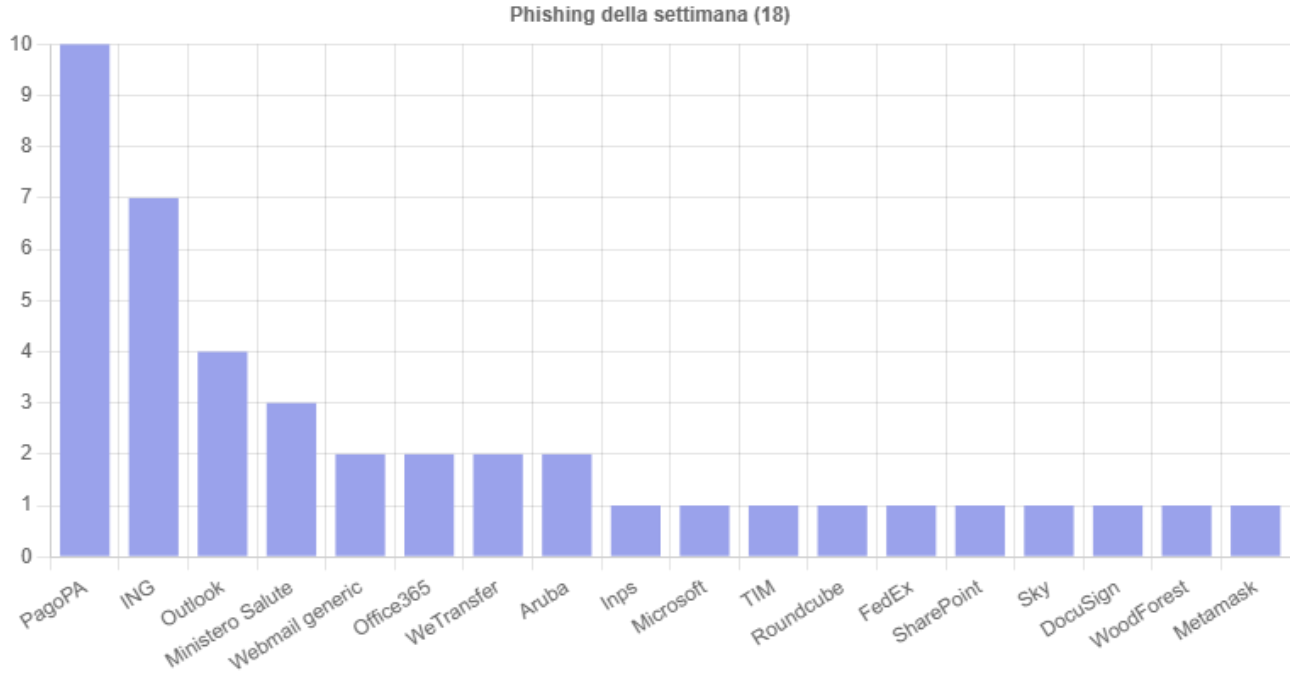
CVE	CVE-2025-6558
DESCRIZIONE	
Google Chromium contiene una vulnerabilità di validazione dell'input impropria in ANGLE e GPU. Questa vulnerabilità potrebbe consentire a un attaccante remoto di eseguire potenzialmente una fuga dalla sandbox tramite una pagina HTML appositamente creata. La vulnerabilità potrebbe interessare diversi browser web che utilizzano Chromium, inclusi, ma non solo, Google Chrome, Microsoft Edge e Opera.	

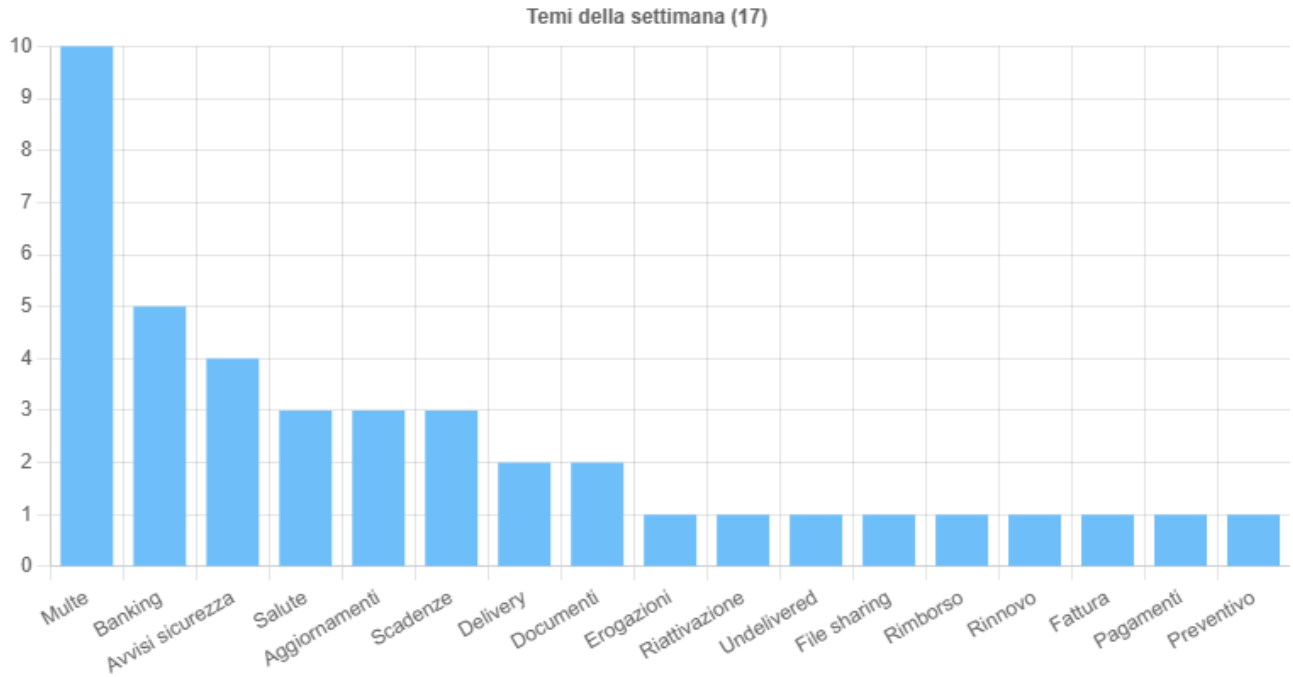
4 Attacchi

4.1 Phishing

Situazione italiana:

Nelle tabelle seguenti vengono riportate in sintesi le distribuzioni del numero di mail di phishing rilevate la settimana in oggetto suddivise per vari parametri quali mittente e area tematica.

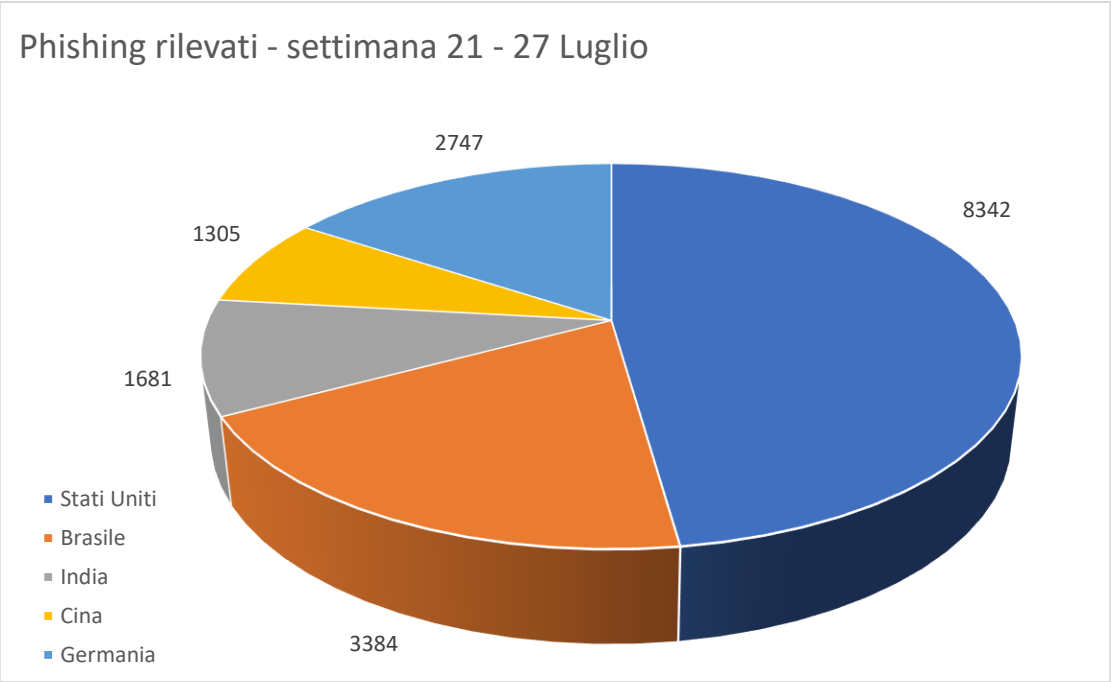




Fonte :CERT-AGID

Situazione Mondiale:

Nel seguente grafico troviamo la distribuzione dei primi cinque paesi di provenienza, per quanto riguarda il numero di email rilevate come attacchi di phishing sui sistemi honeypot.



Riportiamo l'analisi dettagliata relativa ad una mail di phishing recapitata questa settimana.

Report di Analisi CTI – Campagna Email di Sextortion su IP 223[.]185[.]22[.]4

Data di redazione: 28 luglio 2025

Executive Summary

È stata identificata una campagna di sextortion via email indirizzata a utenti individuali. I messaggi analizzati presentano caratteristiche tipiche di estorsione digitale: minaccia di diffusione di materiale compromettente, richiesta di pagamento in criptovaluta e utilizzo di tecniche di social engineering. Le email provengono da IP associati a infrastrutture in India (Bharti Airtel) e non contengono allegati o link dannosi. L'indirizzo Bitcoin utilizzato (12tFKBMezUXnrdDd3Ae3RT1ATFi7oiTaji) risulta statico e riutilizzato in campagne simili. L'impatto tecnico è basso, ma le implicazioni reputazionali e psicologiche possono essere significative.

- **2. Descrizione della Minaccia**

La campagna si basa su email di sextortion che affermano falsamente che l'attore malevolo abbia ottenuto accesso completo al dispositivo della vittima. Il messaggio include un ultimatum di 48 ore e la richiesta di un pagamento di 790 EUR in Bitcoin per evitare la divulgazione di un presunto video compromettente. Il

testo sfrutta una narrativa comune nella sextortion, spesso documentata da fonti come KrebsOnSecurity e Malwarebytes.

- **3. Indicatori di Compromissione (IoC)**

Tipo	Valore	Note
BTC Wallet	12tFKBMezUXnrdDd3Ae3RT1ATFi7oiTaji	Indirizzo statico, riutilizzato
Mittente spoof	vittima@victim[.]com	From & Envelope spoofing
IP origine	223[.]185[.]22[.]4	Bharti Airtel, segnalato su AbuseIPDB
Subject email	"Proposta di Collaborazione."	Oggetto generico tipico delle campagne
Tecniche dichiarate	RAT, webcam, keylogger	Non confermate da prove tecniche

- **Analisi Tecnica**
    - Linguaggio e Struttura
        - L'italiano utilizzato è corretto, suggerendo un certo livello di personalizzazione.
        - L'email è strutturata con HTML obfuscation minimale, compatibile con charset Windows-1250.
        - Self-spoofing: l'email simula provenienza dall'indirizzo della vittima.
    - Tattiche e Tecniche
        - Social engineering e minaccia reputazionale.
        - Mancanza di allegati o link; assenza di prove a supporto delle affermazioni.
        - Le tecniche dichiarate non trovano riscontro nei dispositivi analizzati.
    - Credibilità dell'attacco
        - Non risultano screenshot, registrazioni o altre evidenze reali.
        - L'uso di un indirizzo Bitcoin pubblico statico suggerisce una campagna generica.
        - La probabilità che l'attore sia realmente in possesso dei contenuti dichiarati è bassa.

- **Wallet Bitcoin Analizzato**

L'indirizzo 12tFKBMezUXnrdDd3Ae3RT1ATFi7oiTaji è stato utilizzato nella campagna per ricevere il riscatto.

- Tracciabilità e Rischi
    - Le transazioni possono essere monitorate pubblicamente su blockchain explorer.
    - Il wallet è pseudonimo: non collegabile direttamente a un'identità reale.
    - Dopo eventuali versamenti, è comune il trasferimento verso altri indirizzi ("tumbling").
- Stato delle Transazioni

- Nessuna transazione recente rilevata secondo DFPI/Chainabuse.
- Utilizzo in campagne di massa e bassa monetizzazione osservata.

- Raccomandazioni
  - Non effettuare alcun pagamento.
  - Segnalare il wallet a piattaforme specializzate (BitcoinAbuse, Chainabuse).

- **Analisi dell'Infrastruttura: IP 223[.]185[.]22[.]4**
  - Dati Tecnici

Campo	Valore
IP	223[.]185[.]22[.]4
ASN	AS45609 (Bharti Airtel Ltd.)
Localizzazione	Panchkula, Haryana, India
WHOIS	APNIC – PO Box 3646, South Brisbane, AU
AbuseIPDB Score	4/100, 1 segnalazione
OTX Reputation	0 (nessun dato rilevante)
VirusTotal	0 voti malevoli
Shodan/GreyNoise	Nessun dato disponibile

  - Valutazione
    - Nessuna prova concreta di attività malevole diretta.
    - IP situato in subnet con altri indirizzi segnalati per spam/brute force.

- **Mappatura MITRE ATT&CK**

Fase	Tecnica	Codice	Fonte
Initial Access	Phishing/Extortion	T1566.002	NYSP advisory
Impact	Denial of Reputation	T1499.004	KrebsOnSecurity

- **Valutazione del Rischio**

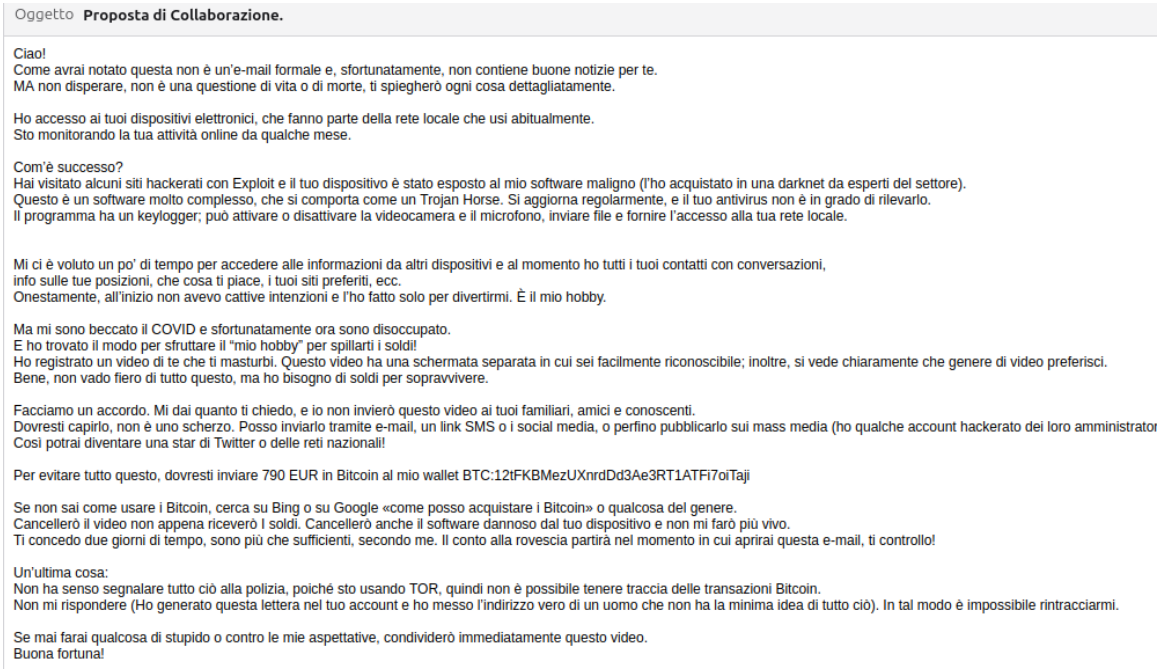
Asset	Gravità	Commento
Malware	Basso	Nessun allegato o link malevolo
Reputazione aziendale	Medio	Possibile allarme nei destinatari
Perdita finanziaria utente	Medio	Alcuni potrebbero versare il riscatto

- **Raccomandazioni Operative**
  - Sensibilizzazione interna: Inviare comunicazioni agli utenti spiegando la natura della minaccia.

- Misure tecniche anti-spoofing: Implementare SPF, DKIM e DMARC sul dominio destinatario.
- Blocchi IP: Valutare il blocco della subnet 223[.]185[.]22[.]0/24 sui gateway aziendali.
- Segnalazioni esterne: Inoltrare il wallet BTC e l'email alle autorità e piattaforme anti-abuso.
- Controlli dispositivi: Eseguire scansioni antivirus/malware aggiornate.
- Awareness costante: Fornire materiale formativo su phishing e ingegneria sociale.

- **Fonti di Riferimento**
  - AbuseIPDB – abuseipdb.com
  - KrebsOnSecurity – krebsonsecurity.com
  - Malwarebytes – malwarebytes.com
  - NY State Police – sextortion advisory
  - DFPI Crypto Scam Tracker – dfpi.ca.gov
  - Microsoft Learn – SPF/DKIM/DMARC
  - Reddit Phishing Community – reddit.com/r/phishing
  - Mass.gov – guidance crypto scam

Qui di seguito lo screenshot della mail:



Oggetto **Proposta di Collaborazione.**

Ciao!
Come avrai notato questa non è un'e-mail formale e, sfortunatamente, non contiene buone notizie per te.
MA non disperare, non è una questione di vita o di morte, ti spiegherò ogni cosa dettagliatamente.

Ho accesso ai tuoi dispositivi elettronici, che fanno parte della rete locale che usi abitualmente.
Sto monitorando la tua attività online da qualche mese.

Com'è successo?
Hai visitato alcuni siti hackerati con Exploit e il tuo dispositivo è stato esposto al mio software maligno (l'ho acquistato in una darknet da esperti del settore).
Questo è un software molto complesso, che si comporta come un Trojan Horse. Si aggiorna regolarmente, e il tuo antivirus non è in grado di rilevarlo.
Il programma ha un keylogger; può attivare o disattivare la videocamera e il microfono, inviare file e fornire l'accesso alla tua rete locale.

Mi ci è voluto un po' di tempo per accedere alle informazioni da altri dispositivi e al momento ho tutti i tuoi contatti con conversazioni,
info sulle tue posizioni, che cosa ti piace, i tuoi siti preferiti, ecc.
Onestamente, all'inizio non avevo cattive intenzioni e l'ho fatto solo per divertirmi. È il mio hobby.

Ma mi sono beccato il COVID e sfortunatamente ora sono disoccupato.
E ho trovato il modo per sfruttare il "mio hobby" per spillarti i soldi!
Ho registrato un video di te che ti masturbi. Questo video ha una schermata separata in cui sei facilmente riconoscibile; inoltre, si vede chiaramente che genere di video preferisci.
Bene, non vado fiero di tutto questo, ma ho bisogno di soldi per sopravvivere.

Facciamo un accordo. Mi dai quanto ti chiedo, e io non invierò questo video ai tuoi familiari, amici e conoscenti.
Dovresti capirlo, non è uno scherzo. Posso inviarlo tramite e-mail, un link SMS o i social media, o perfino pubblicarlo sui mass media (ho qualche account hackerato dei loro amministrator
Così potrai diventare una star di Twitter o delle reti nazionali!

Per evitare tutto questo, dovresti inviare 790 EUR in Bitcoin al mio wallet BTC:12tFKBMezUXnrdDd3Ae3RT1ATFi7oiTaji

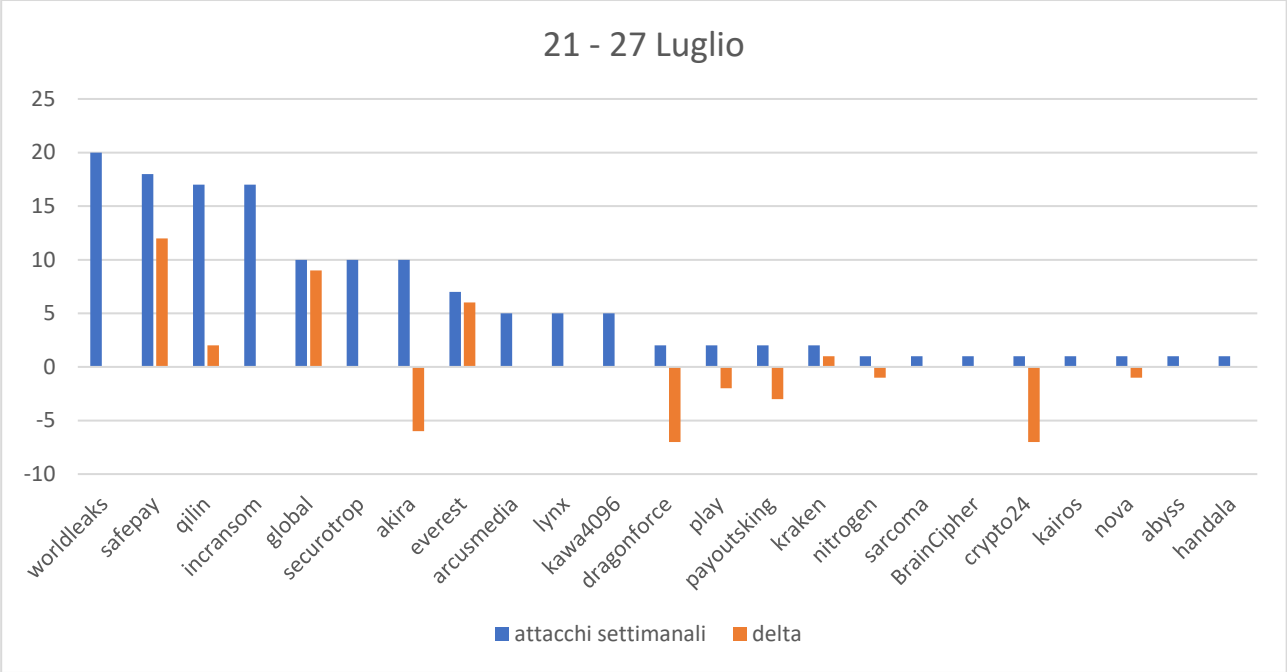
Se non sai come usare i Bitcoin, cerca su Bing o su Google «come posso acquistare i Bitcoin» o qualcosa del genere.
Cancellerò il video non appena riceverò I soldi. Cancellerò anche il software dannoso dal tuo dispositivo e non mi farò più vivo.
Ti concedo due giorni di tempo, sono più che sufficienti, secondo me. Il conto alla rovescia partirà nel momento in cui aprirai questa e-mail, ti controllo!

Un'ultima cosa:
Non ha senso segnalare tutto ciò alla polizia, poiché sto usando TOR, quindi non è possibile tenere traccia delle transazioni Bitcoin.
Non mi rispondere (Ho generato questa lettera nel tuo account e ho messo l'indirizzo vero di un uomo che non ha la minima idea di tutto ciò). In tal modo è impossibile rintracciarmi.

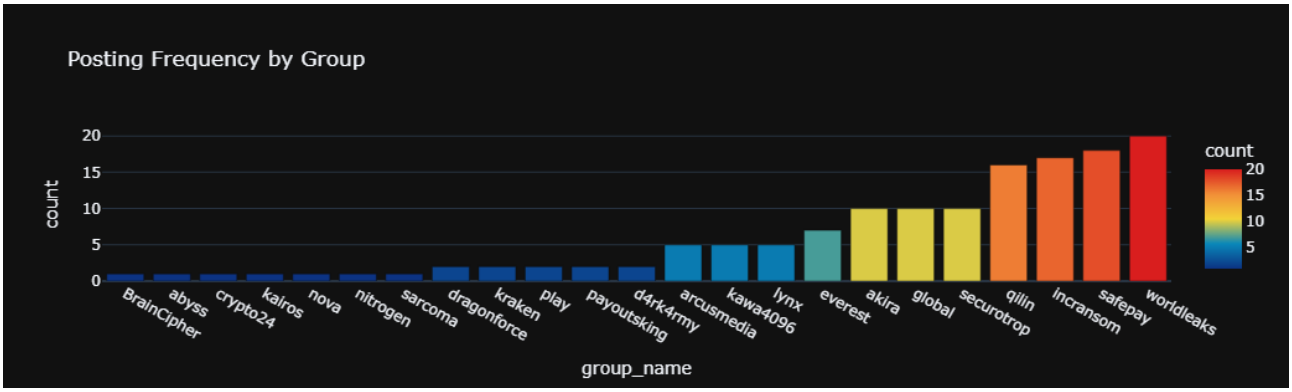
Se mai farai qualcosa di stupido o contro le mie aspettative, condividerò immediatamente questo video.
Buona fortuna!

4.2 Ransomware

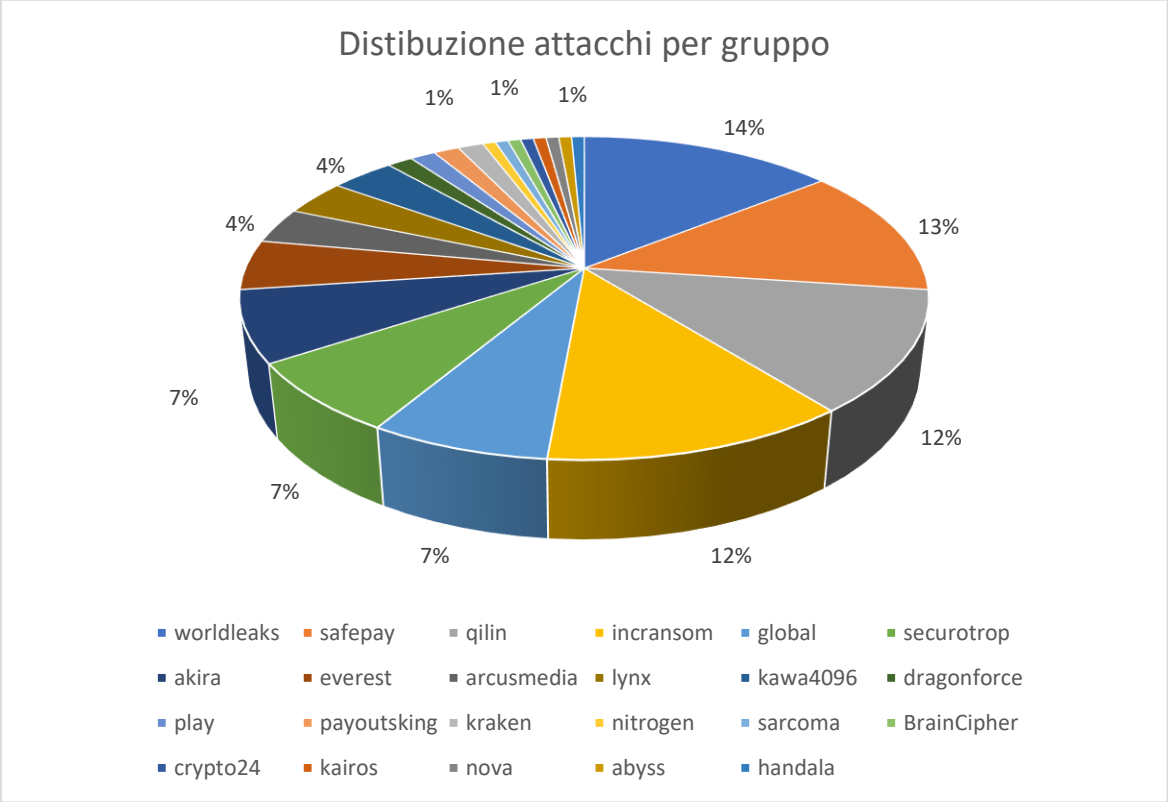
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (21 - 27 Luglio). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



Raccogliendo i dati da un'altra fonte si ha la conferma di quanto sopra riportato riguardo l'andamento degli attacchi settimanali:

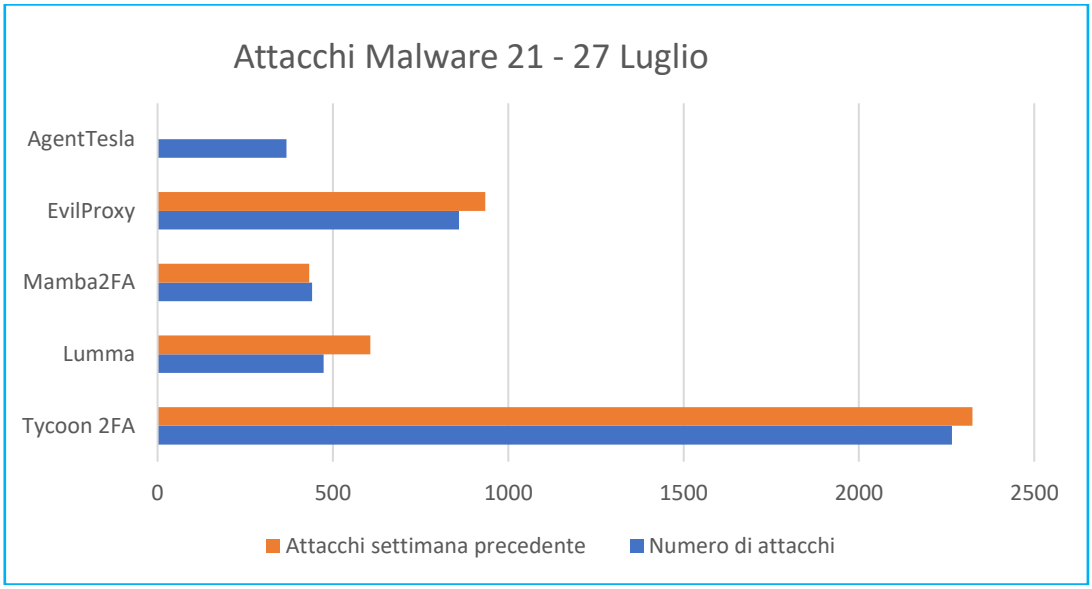


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



4.3 Malware

Il grafico sottostante riporta i 5 malware più attivi nell'ultima settimana, secondo quanto emerso dai sistemi di rilevamento.



Anche questa settimana riportiamo un'analisi dettagliata dei malware risultati più attivi nella settimana di osservazione

- **BQTLOCK (Ransomware)**

BQTLOCK è un nuovo ransomware-as-a-service emerso a metà luglio 2025. Questa famiglia cripta i file delle vittime, rinominandoli con l'estensione .BQTLOCK e lascia un file di riscatto (tipicamente del nome READ_ME-NOW_*.txt) in cui si richiede il pagamento in Monero.

L'attore alla guida è noto come ZeroDayX (Karim Fayad) ed è affiliato a LulzSec. I sistemi colpiti vedono l'intera rete compromessa, con dati cifrati mediante AES-256 e RSA-4096.

Il sito tor di BQTLOCK offre un portale RaaS con dashboard per affiliati, generazione automatica di decryptor e comunicazioni via Telegram,

Descrizione tecnica e contesto: Crypto-ransomware RaaS scoperto a luglio 2025.

Aggredisce Windows usando tecniche di persistenza (Scheduled Task), modifica del registro e persino bootkit (Pre-OS).

Cifra i dati utente e di sistema, impedisce il ripristino dei file e punta soprattutto a reti enterprise nei settori finanziario, manifatturiero, healthcare, ecc.

IoC:

Tipo	Indicatore
Hash (SHA-256)	324eabc27a25f524c94bb62573986b3335ab5181ddc6825d959d16aaaccdc7aa
File cifrato	*.<file>.BQTLOCK (estensione .BQTLOCK)
Ransom note	READ_ME-NOW_<numero>.txt
Canale Telegram	t.me/BQTlock (chat operativa)

MITRE ATT&CK:

- T1486 (Data Encrypted for Impact).
- T1490 (Inhibit System Recovery).
- T1053 (Scheduled Task) e T1542.003 (Bootkit) sono i più rilevanti.
- Ulteriori tecniche: credential dumping T1003, mascheramento T1036, cancellazione log T1070.004.

Contromisure (detection/mitigazione): mantenere copie di backup offline aggiornate; utilizzare EDR/antivirus con firme per BQTLOCK; monitorare l'attività insolita di cifratura file; configurare l'EDR per rilevare operazioni remote (Scheduled Task, registry, bootkit). segmentare la rete e limitare accessi RDP. Evitare il pagamento del riscatto quando possibile.

Livello di rischio: Alto–Critico (gli esperti prevedono che il gruppo evolverà verso la doppia estorsione)

- **Campagna Chemia/EncryptHub (Vidar & Fickle Stealer)**

Nome malware/campagna: Campagna Steam-Chemia di EncryptHub (infostealer Vidar/Fickle).

Nel luglio 2025 il gruppo cybercriminale EncryptHub (alias Larva-208) ha compromesso il gioco Chemia disponibile in Early Access su Steam, inserendo malware direttamente nei suoi file di installazione.

I ricercatori Prodaft hanno scoperto che il 22 luglio i criminali hanno aggiunto il downloader HijackLoader (file CVKRUTNP.exe) all'installazione del gioco. Questo loader garantisce persistenza e scarica in background l'info-stealer Vidar (v9d9d.exe).

In seguito è stato incorporato un malware aggiuntivo, Fickle Stealer, tramite una libreria cclib.dll; questo utilizza uno script PowerShell (worker.ps1) per ottenere il payload principale da un server remoto (soft-gets[.]com).

Il risultato è che gli utenti scaricando Chemia si trovano involontariamente un infostealer in esecuzione in background, che ruba credenziali di browser e portafogli crypto senza influire sulle prestazioni del gioco. Il payload è dissimulato per apparire legittimo, rendendo la campagna insidiosa.

Descrizione tecnica e contesto: Attacco supply-chain via piattaforma Steam (luglio 2025).

Uso di installer compromesso per diffondere malware: HijackLoader scarica l'infostealer Vidar, che ruba dati; successivamente Fickle Stealer (via cclib.dll e worker.ps1) ottiene payload da soft-gets[.]com. Tecnica di ingegneria sociale efficace (gioco apparentemente legittimo su Steam).

IoC:

Tipo	Indicatore
File	CVKRUTNP.exe (HijackLoader), v9d9d.exe (Vidar), cclib.dll, worker.ps1
Dominio	soft-gets[.]com

MITRE ATT&CK:

- Command and Scripting Interpreter (T1059.001, PowerShell per loader).
- Process Injection (T1055 se presente).
- Data from Local System (T1005, raccolta dati browsers).
- Application Layer Protocol (T1071.001, C2 su HTTP) e Exfiltration Over C2 Channel (T1646) tramite HTTP.

Contromisure (detection/mitigazione): scan antivirus/EDR in grado di rilevare HijackLoader, Vidar e Fickle Stealer; bloccare il dominio soft-gets.com; verificare l'integrità dei file di installazione e disinstallare versioni sospette; educare il personale a non fidarsi ciecamente di software in Early Access o scaricato via link non ufficiali. Mantenere aggiornate le soluzioni di sicurezza e attivare la verifica in lettura per software remoti.

Livello di rischio: Alto (campagna mirata ad ampia diffusione, con potenziale furto massivo di credenziali aziendali).

- **Coyote (Trojan bancario UIA)**

Nome malware: Coyote (variante UIA).

Akamai ha segnalato il 22 luglio 2025 una variante del trojan bancario Coyote che sfrutta il framework UI Automation di Windows. Questa versione colpisce principalmente utenti in Brasile, prendendo di mira credenziali di 75 siti di banche e exchange crypto. Coyote installa un keylogger/overlay (per phishing bancario) e in più usa API Windows UIA per leggere il contenuto delle finestre del browser (tab e barre degli indirizzi) e identificare indirizzi appartenenti alle banche bersaglio. Durante l'attacco il malware invia al server C2 informazioni sul sistema (nome computer, username, servizi finanziari usati). L'uso del framework UIA (mai visto prima in Coyote) permette di aggirare controlli di sicurezza e ottenere dati anche senza strumenti standard di scraping.

Descrizione: Trojan bancario Windows, noto sin dal 2024, aggiornato con una nuova tecnica di raccolta automatizzata delle finestre del browser tramite UIA.

Funzionalità chiave: cattura input (keylogging e overlay), utilizza GetForegroundWindow e UIA per esfiltrare dati finanziari specifici. Mira al settore finanziario (target test regionale in Brasile).

IoC: per questa variante non sono stati rilasciati pubblicamente domini o hash specifici. Una possibile IoC è la presenza di processi sospetti che sfruttano UIA.

MITRE ATT&CK:

- Input Capture (UI Accessibility) (T1056.003, raccolta credenziali via UI Automation);
- Data Encrypted for Impact (T1486, se coinvolge cifratura);
- Persistence (T1053, attività pianificate).
- Anche l'analisi di processi attivi (T1082) può rilevare Coyote.

Contromisure (detection/mitigazione): aggiornare gli EDR e i sistemi anti-malware per rilevare nuovi comportamenti associati a Coyote. impedire l'esecuzione di software sconosciuti su macchine finanziarie; segregare i sistemi bancari dalla navigazione web generale; abilitare l'autenticazione forte per login

bancari; attivare contromisure sul framework UIA (ad esempio disabilitare l'accessibilità per applicazioni non attendibili).

Livello di rischio: Alto (trojan specializzato e in evoluzione, potenzialmente estendibile al di fuori del Brasile).

- **SarangTrap (Campagna Mobile)**

Nome campagna: SarangTrap (malware mobile extorsivo).

SarangTrap è una vasta campagna di malware mobile scoperta a fine luglio 2025 da Zimperium e altri ricercatori. Gli aggressori hanno creato oltre 250 app Android malevole (e relative app iOS), tutte camuffate da popolari servizi social/dating (Tinder, Bumble, cloud storage, ecc.). Queste app fittizie venivano pubblicizzate tramite più di 80 domini phishing ben realizzati (e perfino indicizzati da Google) che promettevano inviti esclusivi a servizi di incontri.

Dopo l'installazione, l'app richiede un codice "invito" (che invia al C2) e quindi insolitamente ampi permessi (accesso a SMS, contatti, foto).

Solo dopo l'interazione dell'utente parte la sottrazione dei dati: l'app mostra una UI ingannevole che finge funzioni di chat/SMS, mentre nel frattempo esfiltra silenziosamente numeri di telefono, lista contatti, immagini private e messaggi SMS al server degli attaccanti. Alcune vittime sono poi ricattate con minacce di diffusione di foto personali rubate.

Descrizione: Campagna mobile "romance scam" globale (emergenza luglio 2025).

Utilizza social engineering avanzato: app Android/iOS camuffate da dating app con UI attraente, invite codes falsi e domini phishing studiati su Google.

Tecniche mobile: l'app richiede password e permessi critici solo dopo l'interazione per sfuggire ai sandbox. Ruba contatti, SMS, immagini usando API di sistema (UI Automation) e invia i dati via HTTP al C2. Esegue esfiltrazione e (sulla variante Android) persino lettura SMS (T1582).

IoC: la campagna non ha IoC semplici noti, data la varietà di app e domini. Indicativamente: oltre 80 domini di phishing tematici (dating, cloud storage, servizio taxi) ed oltre 250 APK Android sospetti segnalati.

MITRE ATT&CK:

- Masquerading (T1655.001, app truffaldine con nomi legittimi).
- System Network Configuration Discovery e System Info Discovery (T1422, T1426).
- Protected User Data: Contact List (T1636.003) ed Data from Local System (T1533) per esportare contatti e file.

- Application Layer Protocol (T1437.001, comunicazione HTTP con C2) e Exfiltration Over C2 Channel (T1646).
- SMS Control (T1582) per leggere messaggi in Android.

Contromisure (detection/mitigazione): rafforzare le policy BYOD e le soluzioni MTD/EDR mobile; bloccare a livello di rete/DNS i domini noti legati alla campagna e aggiornare i filtri anti-phishing. Formare gli utenti sul rischio di app di dating fasulle e verificare sempre le recensioni sulle app; controllare le autorizzazioni delle app e rimuovere quelle sospette; monitorare attività anomale sui dispositivi (esfiltrazioni di contatti/foto) con sistemi di rilevamento comportamentale.

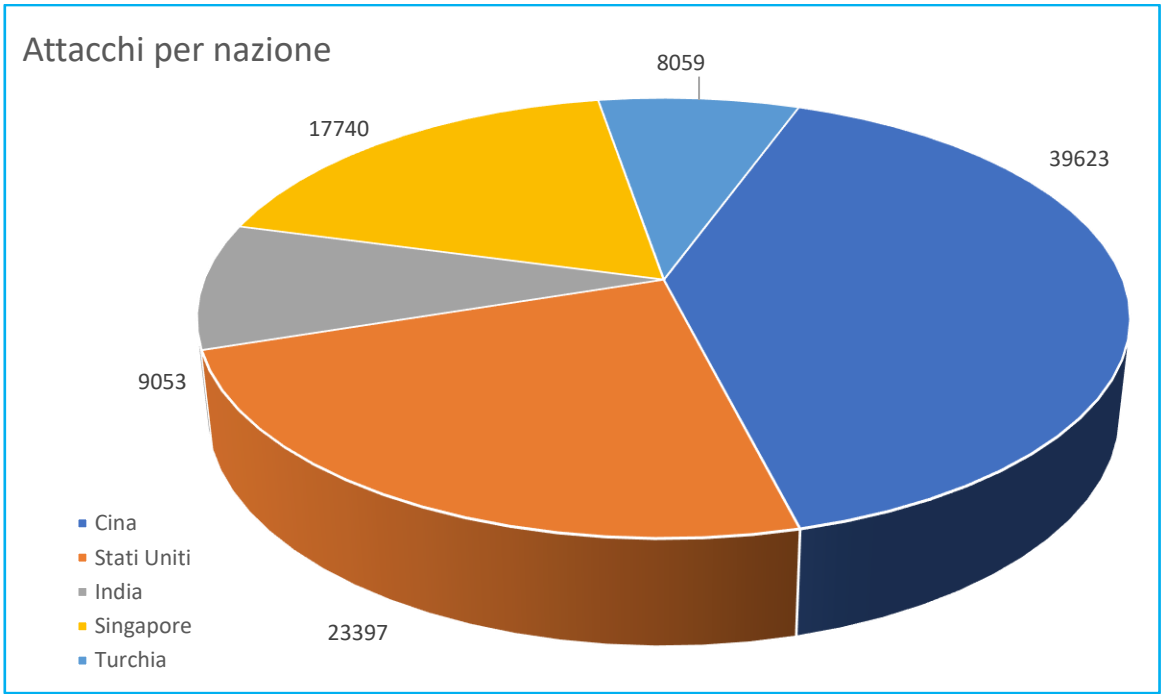
Livello di rischio: Alto (campagna sofisticata, mirata a dati sensibili personali e potenzialmente scalabile).

Riepilogo

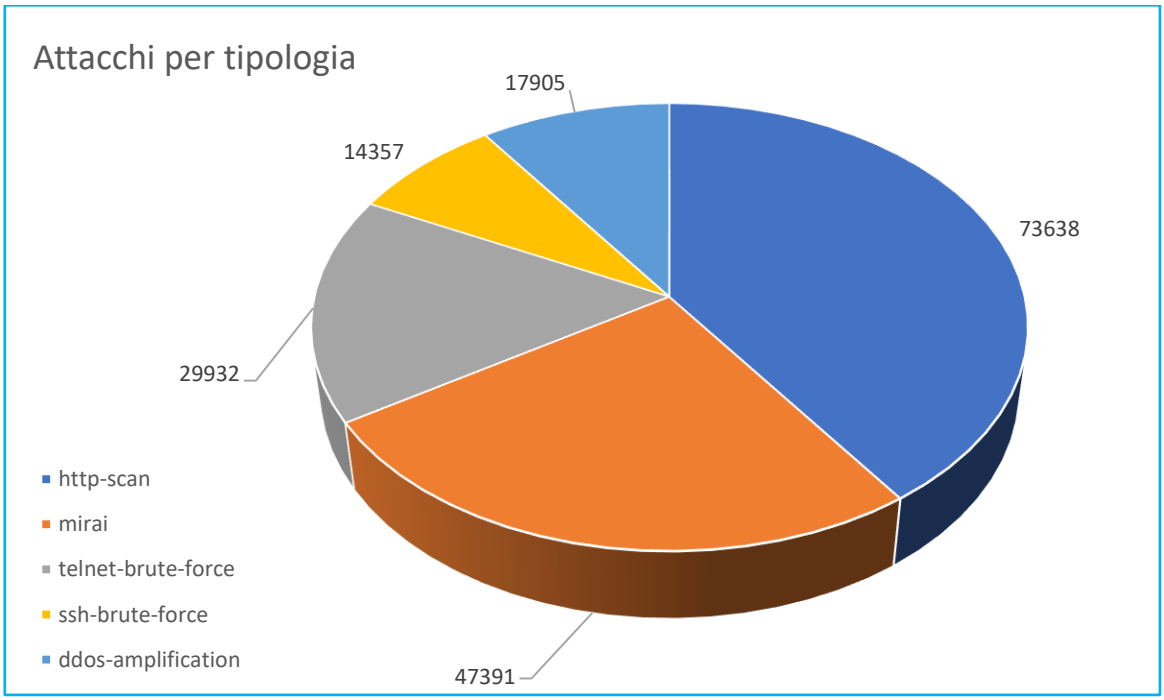
Malware	Categoria	Livello di rischio
BQTLOCK	Ransomware	Alto/Critico
Chemia/EncryptHub	Infostealer (supply-chain)	Alto
Coyote	Trojan bancario (Windows)	Alto
SarangTrap	Malware mobile (spyware/ext.)	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 21 – 27 Luglio, suddivisa per nazione e limitata alle prime cinque posizioni:

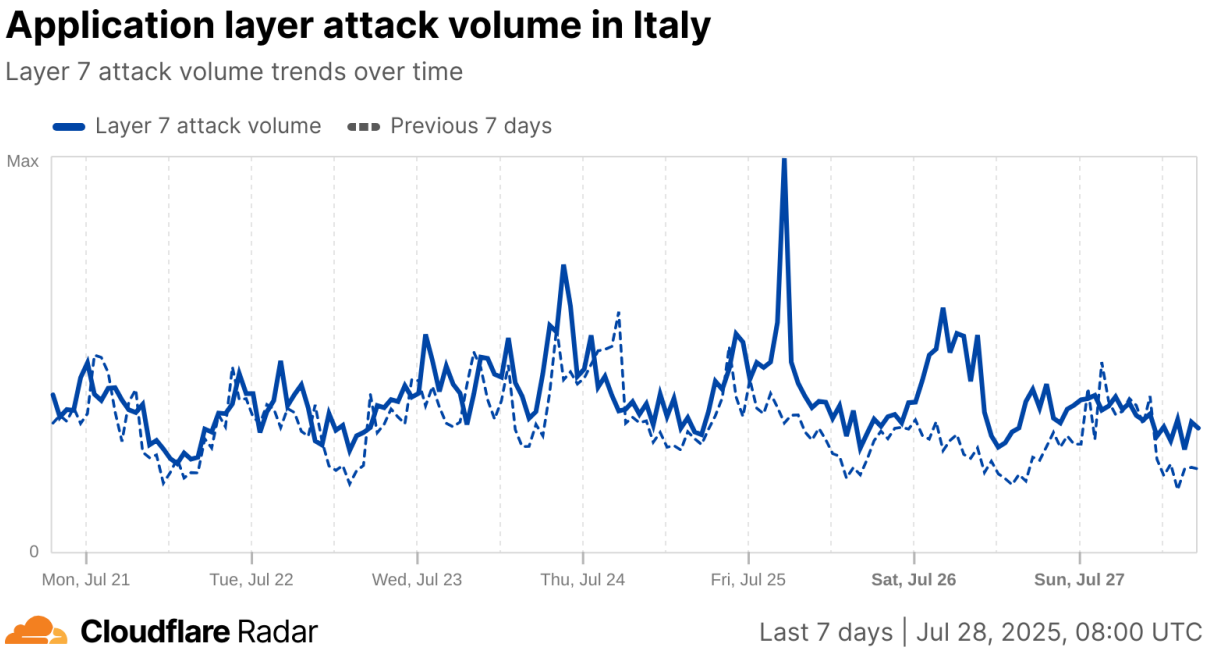


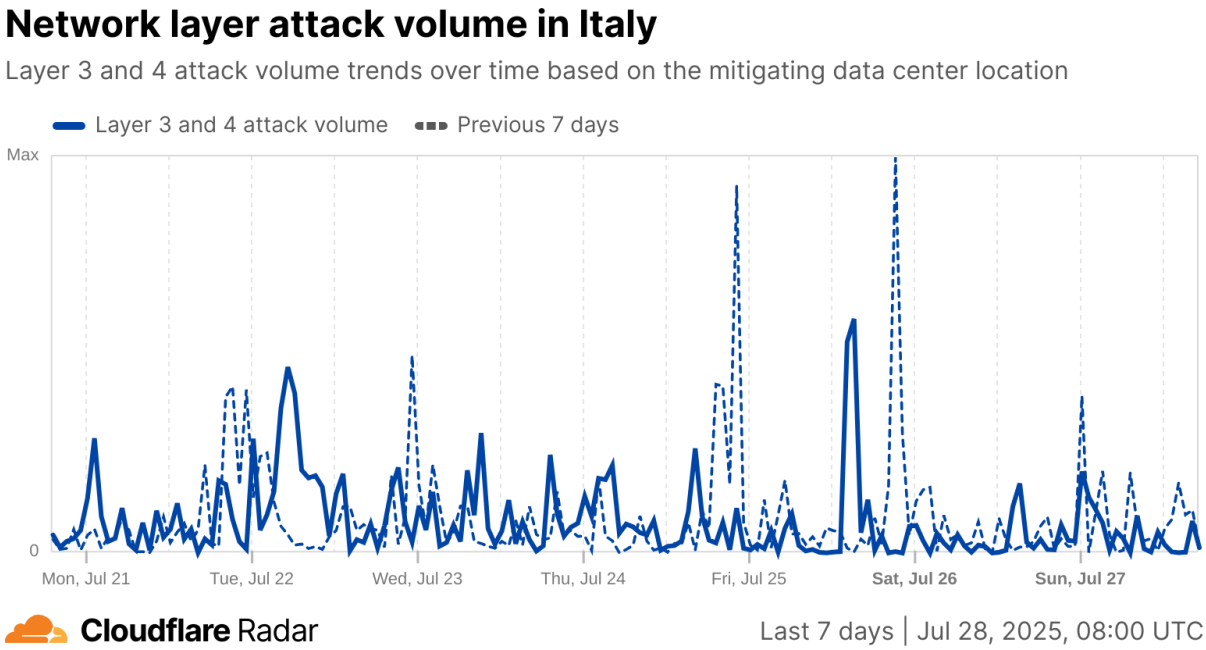
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



SITUAZIONE ITALIANA

Nei due grafici seguenti viene riportato l'andamento settimanale degli attacchi DDoS condotti a livello applicativo e a livello network rispettivamente:





Fonte: Cloudflare Radar

4.5 Data Breach

In questa sezione sono riportati alcuni tra i principali Data Breach individuati nella settimana di osservazione.

TARGET	LOCALIZZAZIONE
NAVAL GROUP	MONDO
DESCRIZIONE	Il 25 luglio 2025 un gruppo di hacker ha rivendicato un attacco informatico di rilevante portata contro Naval Group, azienda leader nel settore della difesa navale e della costruzione di sottomarini. Secondo quanto comunicato dagli aggressori, sono stati sottratti dati riservati e sensibili, tra cui informazioni strategiche e tecniche di grande valore. I criminali hanno imposto un ultimatum di 72 ore per il pagamento di un riscatto, minacciando di pubblicare o vendere i dati sottratti qualora la richiesta non venga soddisfatta entro il termine stabilito. Naval Group ha prontamente avviato un'indagine interna e sta collaborando con le autorità nazionali ed internazionali per contenere la minaccia e valutare l'entità del danno.

TARGET	LOCALIZZAZIONE
ALLIANZ LIFE I.C. OF N.A.	STATI UNITI
DESCRIZIONE	Qualche giorno fa, Allianz Life Insurance Company of North America ha subito una violazione dei dati che ha compromesso le informazioni personali della maggior parte dei suoi 1,4 milioni di clienti statunitensi. L'attacco è stato attribuito ad un attore malintenzionato che ha sfruttato una tecnica di social engineering per accedere ad un sistema CRM basato su cloud fornito da un fornitore terzo. Secondo l'azienda, i propri sistemi interni non sono stati compromessi, ma solo la piattaforma del fornitore esterno. I dati esfiltrati includono informazioni personali identificabili (PII) di clienti, professionisti finanziari e alcuni dipendenti. Allianz Life ha preso misure immediate per contenere l'incidente, ha notificato l'FBI e ha avviato un'indagine interna. L'azienda ha inoltre offerto ai clienti colpiti 24 mesi di protezione contro il furto d'identità e monitoraggio del credito. Le notifiche ufficiali agli interessati sono previste per l'1 agosto 2025

TARGET	LOCALIZZAZIONE
NNSA	STATI UNITI
DESCRIZIONE	L'Agenzia statunitense per la sicurezza nucleare (NNSA) è stata vittima di un attacco informatico che ha sfruttato una vulnerabilità zero-day nel software Microsoft SharePoint. L'attacco, attribuito a gruppi di hacker sponsorizzati dallo Stato cinese, ha consentito l'accesso non autorizzato a sistemi interni della NNSA. Fortunatamente, non risultano compromessi dati sensibili o classificati, grazie anche all'uso di infrastrutture cloud sicure. Tuttavia, l'agenzia ha dovuto isolare e ripristinare alcune parti dei sistemi compromessi per contenere i danni. Microsoft ha rilasciato patch di sicurezza urgenti per chiudere la falla, invitando tutti gli utenti a installarle rapidamente.

Statistiche e Impatto di Mercato dei Data Breach (Maggio–Luglio 2025)

Tra maggio e luglio 2025 sono stati documentati decine di incidenti di data breach in diversi settori. Ad esempio, IT Governance ha segnalato per giugno 2025 ben 33 eventi confermati, con l'esposizione di oltre 16 miliardi di credenziali (anche da vecchi archivi) e 23 milioni di nuovi record personali, causati soprattutto da campagne di ransomware, phishing e compromissione di fornitori terzi. Complessivamente, gli attacchi noti in questo periodo hanno coinvolto decine di milioni di persone: i casi di punta includono circa 8,4 milioni di utenti Zoomcar, 5,7 milioni di clienti Qantas, 5,4 milioni di pazienti Episource, oltre a centinaia di migliaia in altri incidenti. I settori più colpiti sono stati: trasporti/viaggi (es. compagnie aeree e sharing mobility), retail e lusso (catene di negozi e moda), sanità/assicurazioni e tech/software. Ad esempio, l'attacco a Qantas e Zoomcar ha interessato viaggi aerei e car sharing; violazioni a Episource e Aflac hanno investito il settore sanitario/assicurativo; mentre Belk e Louis Vuitton UK hanno colpito il retail/lusso. Anche il settore tecnologico è stata coinvolto: a luglio è emersa una compromissione su larga scala tramite una vulnerabilità zero-day in Microsoft SharePoint, che ha permesso a gruppi criminali di colpire aziende e agenzie governative in tutto il mondo. I tipi di dati più comunemente esposti sono le informazioni personali identificative (PII) – nomi, indirizzi, email, dati di contatto – unitamente a dati sensibili quali codici fiscali e numeri di previdenza sociale (SSN).

In vari casi sono emersi anche dati sanitari (referti medici in Episource) o bancari (IBAN in Promosfera). A differenza degli anni passati, casi di esposizione massiva di carte di credito sono stati rari: i criminali hanno invece preferito rubare dati di account e credenziali. Gli attacchi hanno utilizzato principalmente ransomware e phishing: molti incidenti recenti – come quelli contro Belk e M&S – sono riconducibili a ransomware-as-a-service (gruppi come DragonForce), che infestano le reti aziendali e poi diffondono i dati. Anche l'ingegneria sociale (phishing mirato) resta un vettore comune: per esempio Aflac ha confermato un accesso interno tramite social engineering. Infine gli exploit di vulnerabilità note (es. SharePoint) e le compromissioni di fornitori esterni (es. piattaforme CRM o call center di Qantas) sono emersi come motivi ricorrenti. In sintesi, i metodi dominanti nel Q2/2025 sono stati il phishing/ingegneria sociale, i malware di tipo ransomware e lo sfruttamento di falle software.

Analizziamo ora gli attacchi perpetrati ai danni delle maggiori compagnie in ambito mondiale verificatisi nel periodo di osservaione:

- **Microsoft**

Cap. di mercato (luglio 2025): ~3,82 trilioni USD (NASDAQ: MSFT), seconda per valore al mondo.

Settore: tecnologia/informatica (software, cloud); Sede: Redmond (Washington, USA).

Attacco: il 19 luglio 2025 è stata sfruttata una grave vulnerabilità zero-day su Microsoft SharePoint, colpendo server aziendali, enti pubblici e università in tutto il mondo.

Microsoft ha pubblicato patch di emergenza e istruito clienti a isolare i server a rischio.

Mercato azionario: il titolo MSFT rimane stabile intorno ai valori pre-attacco, senza variazioni significative legate al problema di sicurezza. Microsoft ha fornito aggiornamenti tecnici ma nessuna dichiarazione rivolta specificamente agli investitori.

- **Promosfera**

Cap. di mercato: società privata.

Settore: marketing/promozioni (gestione concorsi e cashback); Sede: Casorate Sempione (VA, Italia).

Attacco: dal 2 al 4 maggio 2025 i server di Promosfera sono stati violati da criminali informatici.

Sono stati esfiltrati dati personali di migliaia di consumatori italiani che avevano partecipato a promozioni tra il 2018 e il 2024, incluse nome, cognome, contatti e, per chi ha richiesto premi in denaro, anche gli IBAN.

I sistemi hanno eseguito backup regolari, ma l'attacco è riuscito a bypassare parte delle misure di sicurezza.

Mercato azionario: non applicabile (azienda non quotata). Di conseguenza non si registra impatto diretto sul mercato azionario né comunicazioni ufficiali a investitori esterni. Promosfera ha emesso un'informativa alla clientela e denunciato l'accaduto alle autorità competenti.

- **Qantas**

Cap. di mercato (Luglio 2025): ~10,2 miliardi USD (ASX: QAN)

Settore: trasporti aerei; Sede: Sydney, Australia.

Attacco: il 30 giugno 2025 Qantas ha annunciato una violazione informatica di un suo database gestito da terzi, che ha esposto dati di clienti. Inizialmente si parlava di "oltre 1 milione" di utenti colpiti; più tardi la compagnia ha indicato fino a 5,7 milioni di clienti unici interessati, con informazioni come nome, email, numero di telefono, indirizzo e data di nascita.

Nessun dato finanziario sensibile (es. carte di credito) risulta compromesso.

Effetti sul titolo: il titolo QAN su ASX ha mostrato oscillazioni fisiologiche legate al mercato, ma senza un crollo evidente imputabile all'incidente. Qantas non ha segnalato dichiarazioni ai mercati sulla violazione, limitandosi a comunicare i fatti e a instaurare un centro di assistenza clienti. In seguito è stata disposta un'inchiesta legale ed un ordine restrittivo per bloccare la diffusione delle informazioni rubate, ma finora senza impatti rilevanti sulla quotazione.

- **Belk**

Cap. di mercato: catena privata.

Settore: grande distribuzione/abbigliamento; Sede: Charlotte, North Carolina (USA).

Attacco: gruppi RaaS (ransomware-as-a-service) collegati a DragonForce hanno rivendicato un'intrusione a maggio 2025 nella rete del retailer Belk, sottraendo circa 150 GB di dati aziendali.

Secondo gli analisti, i criminali hanno agito sfruttando credenziali sottratte e installando malware, ma Belk non ha finora confermato i dettagli.

Effetti aziendali: essendo un'azienda privata, non si dispone di quotazioni di borsa. La notizia, però, ha generato preoccupazione nel settore retail: alcune fonti indicano che le azioni di Belk siano scese di circa il 20% in pochi giorni a causa dell'allarme (anche per via delle rivendicazioni di DragonForce), sebbene la società non abbia comunicato pubblicamente l'impatto sull'attività.

Non ci sono comunicazioni ufficiali agli investitori, ma Belk ha probabilmente avviato un'indagine interna e un'azione legale contro i responsabili.

- **Zoomcar**

Cap. di mercato (luglio 2025): ~$3,3 milioni USD (OTC: ZCAR).

Settore: car sharing / mobilità (P2P rental); Sede: Bengaluru (India).

Attacco: il 9 giugno 2025 Zoomcar ha rivelato che un hacker ha avuto accesso ai dati di almeno 8,4 milioni di clienti.

Sono stati esposti nomi, numeri di telefono e numeri di targa dei veicoli prenotati. L'incidente, segnalato tramite documento SEC, è stato risolto rapidamente e Zoomcar ha ripreso le normali operazioni entro due giorni senza interruzioni ai servizi.

Mercato azionario: Zoomcar è quotata come ZCAR nei mercati USA. Al momento della violazione aveva una capitalizzazione molto modesta (~$9–10 M USD), ridottasi a ~3,3 M USD entro fine luglio 2025. Nell'anno precedente la capitalizzazione era già crollata di oltre il 90%, riflettendo problemi finanziari dell'azienda (sterne al breach). Dopo l'annuncio del giugno 2025 il titolo ha avuto un lieve calo iniziale, ma si aggira tuttora intorno a $0,60–0,70. Non risultano dichiarazioni formali agli azionisti oltre al documento SEC divulgato.

- **Aflac**

Cap. di mercato (giugno 2025): ~$55,5 miliardi USD (NYSE: AFL)

Settore: assicurazioni (sanitaria e vita); Sede: Columbus, Georgia (USA).

Attacco: il 12 giugno 2025 Aflac ha confermato di aver individuato attività sospetta nella propria rete USA. L'accesso non autorizzato – ottenuto tramite social engineering – ha portato all'esposizione potenziale di dati relativi a clienti e dipendenti: informazioni sui sinistri, dati sanitari, numeri di previdenza sociale (SSN) e altri dati personali. Aflac ha assicurato che non si tratta di ransomware e che le operazioni aziendali non sono state interrotte. Ha attivato esperti esterni e sta offrendo servizi di protezione identità (credit monitoring) per i soggetti coinvolti.

Effetti sul titolo: il titolo AFL ha reagito con un calo di entità contenuta nella giornata immediatamente successiva alla diffusione della notizia, ma rapidamente ha recuperato terreno. L'impatto sul valore di mercato è stato minimo (date le solide fondamenta aziendali), e l'azienda ha continuato a comunicare regolarmente con gli investitori tramite i suoi canali consueti. Aflac ha rassicurato gli azionisti sul fatto che l'attacco non ha compromesso la capacità di sottoscrivere polizze o pagare sinistri, pur riconoscendo il problema al proprio top management.

- **Episource (Optum/UnitedHealth)**

Cap. di mercato del gruppo (luglio 2025): UnitedHealth Group (NYSE: UNH) – società madre di Episource via la controllata Optum – ~255 miliardi USD (prima nell'assicurazione sanitaria USA).

Settore: servizi sanitari/fatturazione medica; Sede: Episource ha sede negli USA (parte di Optum, Minnesota).

Attacco: Episource ha notificato a luglio 2025 che un cybercriminale ha visto e copiato dati di pazienti e clienti durante un'intrusione durata circa una settimana (terminata il 6 febbraio 2025).

Sono stati esfiltrati dati personali (nomi, indirizzi, email, numeri di telefono) e dati sanitari completi (referti medici, diagnosi, cure, dati assicurativi) di oltre 5,4 milioni di persone. Nonostante Episource non abbia specificato il vettore d'attacco, fonti interne (Sharp Healthcare) indicano che si è trattato di ransomware.

Effetti sul gruppo: non essendo quotata separatamente, Episource non ha una propria capitalizzazione. Tuttavia, UnitedHealth Group ha visto un forte calo del titolo in Q2 2025 (~-40% nel trimestre, a causa di fattori vari tra cui l'esposizione del gruppo agli attacchi cyber).

Episource ha inviato avvisi a enti regolatori e clienti colpiti; UnitedHealth/Optum non ha ancora rilasciato commenti pubblici specifici su questo incidente, sebbene abbia ribadito in conference call trimestrali l'impegno a rafforzare la sicurezza informatica.

- **Louis Vuitton UK**

Cap. di mercato (LVMH): ~560 miliardi USD (gruppo quotato).

Settore: lusso/moda; Sede: Parigi, Francia (Louis Vuitton UK opera come filiale).

Il 2 luglio 2025 il marchio di lusso Louis Vuitton (gruppo LVMH) ha subito un data breach mirato ai clienti nel Regno Unito (parte di un'ondata più ampia di violazioni in Europa e Asia). I criminali hanno ottenuto accesso a informazioni come nominativo, contatti e storico degli acquisti di numerosi clienti UK, senza però carpire dati bancari o password.

L'attacco, scoperto il 2 luglio, avrebbe sfruttato un account di un fornitore terzo ed era stato preparato circa un mese prima.

In totale, in Turchia sono stati compromessi quasi 143.000 residenti, mentre LV UK non ha ancora quantificato il numero esatto di clienti coinvolti.

Reazioni ufficiali: LVMH ha rilasciato una dichiarazione in cui conferma la violazione, sottolineando che nessun dato di pagamento era coinvolto e che sta notificando clienti e autorità competenti.

L'azienda ha affermato di avere rafforzato le proprie misure di sicurezza per prevenire futuri attacchi.

Nonostante l'elevato profilo dell'incidente, il titolo LVMUY (LVMH) ha risentito solo marginalmente della notizia, in linea con la resilienza storica del titolo a problemi di sicurezza minori.

- **Riepilogo**

Azienda (titolo / gruppo)	Settore	Gravità	Note principali
Microsoft (MSFT)	Tecnologia / software	Medio–alto	Stock resiliente, attenzione su gestione patch
Qantas (QAN.AX)	Trasporti / aerei	Alto	breach piattaforma terza parte, impatto privacy
Zoomcar (ZCAR OTC)	Mobilità / car sharing	Alto	esposizione dati 8,4 M utenti, impatto reputazione
Aflac (AFL)	Assicurazioni / sanità	Critico	esposizione di dati sanitari e SSN
UnitedHealth Group (UNH)	Servizi sanitari (via Optum / Episource)	Critico	breach su 5,4 M pazienti, dati sanitari sensibili
LVMH (es. LV UK)	Lusso e moda	Medio–alto	esfiltrazione dati clienti UK, nessun dato pagamento
Belk (privata)	Retail / abbigliamento	Critico	150 GB di dati interni rubati, SSN coinvolti
Promosfera (privata)	Marketing promozionale	Alto	dati anagrafici e IBAN di migliaia di clienti

4.6 Defacement

Questo è l'andamento settimanale rilevato dai nostri sistemi riguardo attività di tipo "defacement" ai danni di domini di tipo [.]it :

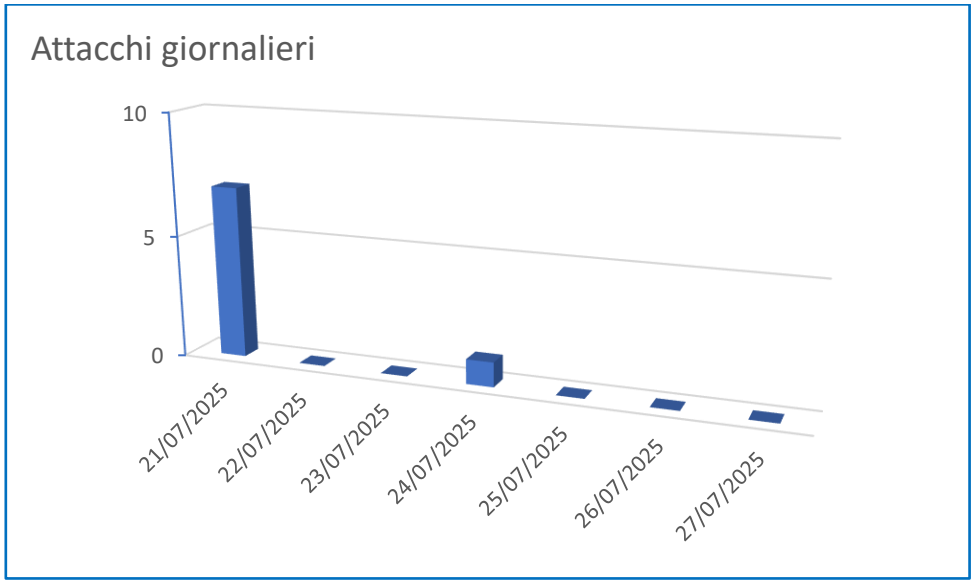


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

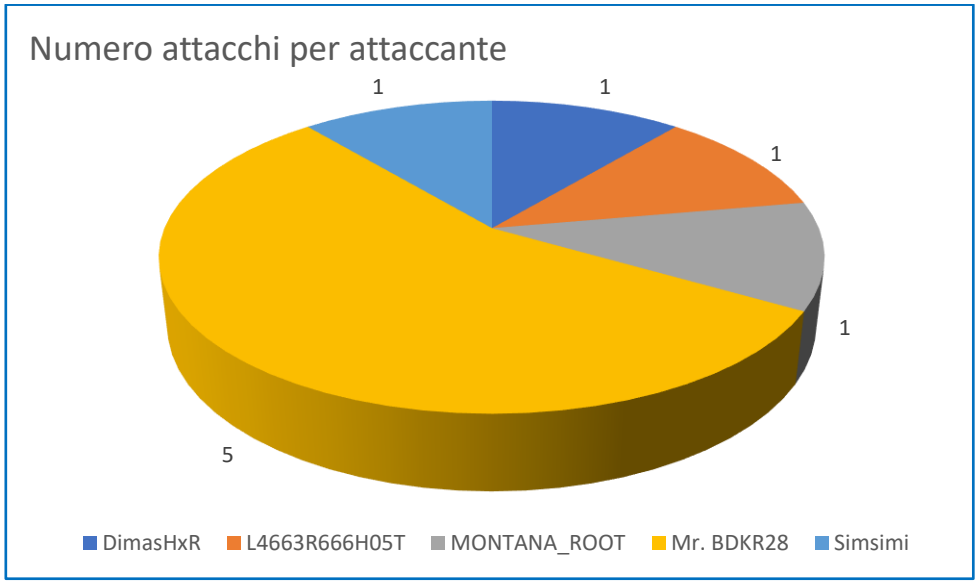


Figura 2: Defacement - Attaccanti più attivi nel periodo 21 - 27 Luglio

5 Honeypot

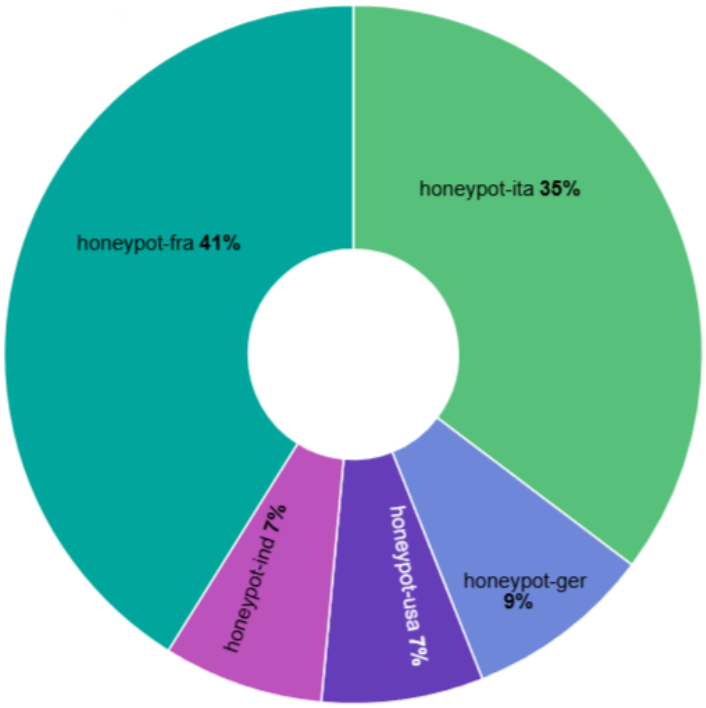
I seguenti dati sono raccolti da sistemi appositamente predisposti per la raccolta dei log sugli attacchi informatici (Honeypot). L'infrastruttura è composta da sensori honeypot dislocati nei principali paesi di interesse mondiale. Ad oggi, i sensori sono stati installati nei seguenti paesi: Italia, Germania, Francia, Brasile, India e USA. Le informazioni raccolte vengono poi aggregate ed elaborate dal team di analisti di S3K.

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale

Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

877.524 Attacks **6.962** Unique Src IPs **58** Unique HASSHs

Il grafico seguente rappresenta la distribuzione degli attacchi in valori percentuali sui vari honeypot.

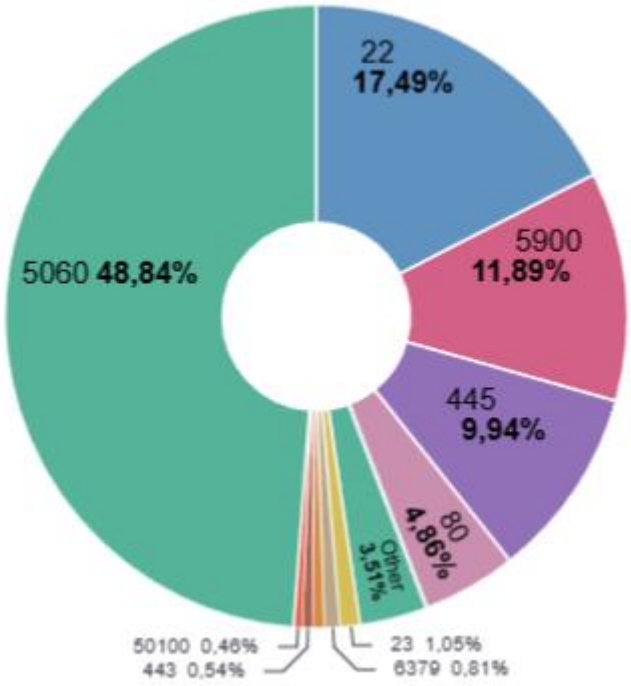


Questa invece la situazione a livello italiano:

309.693 Attacks **2.742** Unique Src IPs **40** Unique HASSHs

5.1.1 Attacchi ai servizi

Nel grafico sottostante viene rappresentata la distribuzione degli attacchi per tipo di servizio:



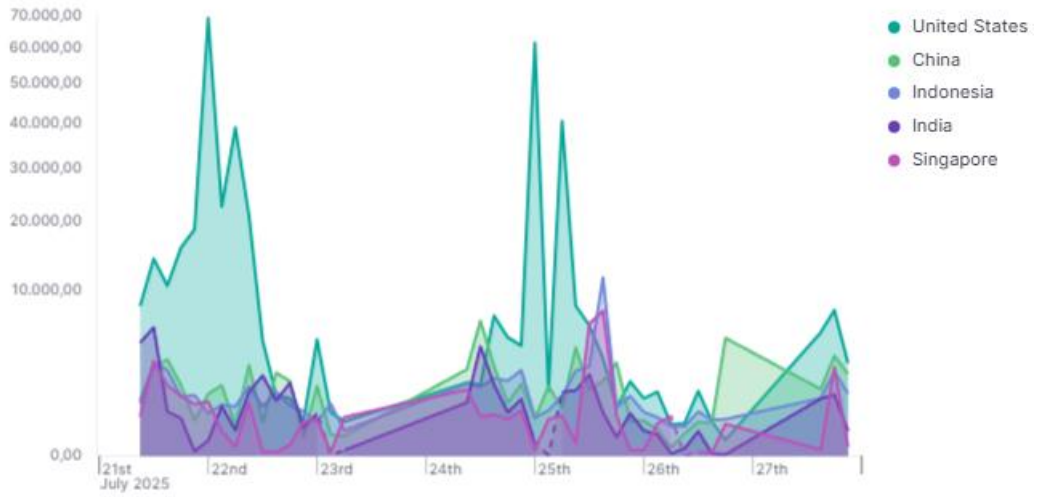
5.1.2 IP Attaccanti

Sotto riportiamo la Top 10 degli indirizzi IP che hanno effettuato il maggior numero di movimenti sospetti sulla rete sottoposta a monitoraggio.

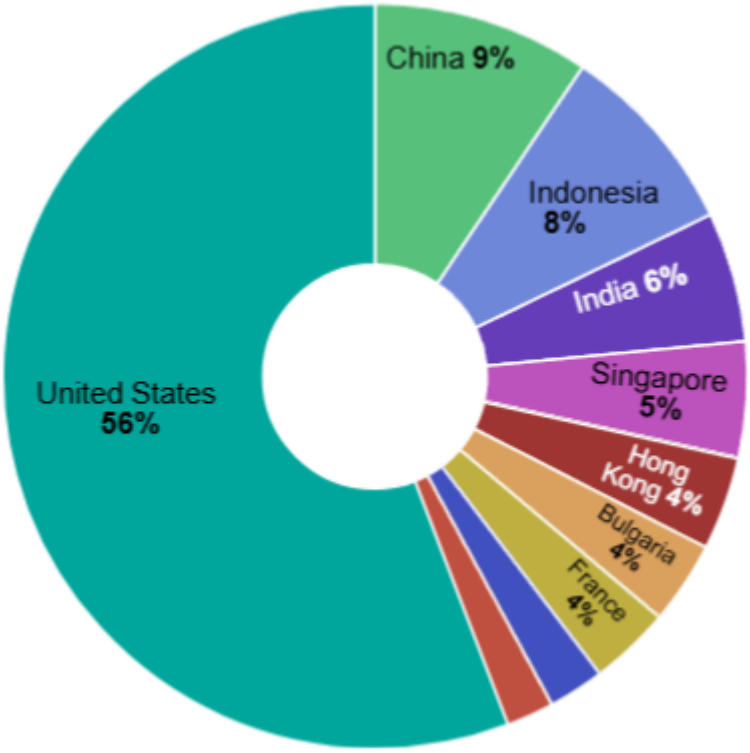
Source IP	Count
173.233.73.6	235.866
198.23.153.40	53.727
103.156.74.23	29.212
142.202.189.5	20.761
185.177.72.8	17.331
142.202.191.234	15.933
203.118.58.163	11.054
180.243.254.203	9.770
79.124.56.162	7.147
103.99.206.83	5.391

5.1.3 Paesi di provenienza degli attacchi

Il grafico seguente mostra l'andamento degli attacchi rilevato da ciascun singolo honeypot.



In quest'altro grafico viene rappresentata la distribuzione degli attacchi per paese di provenienza:

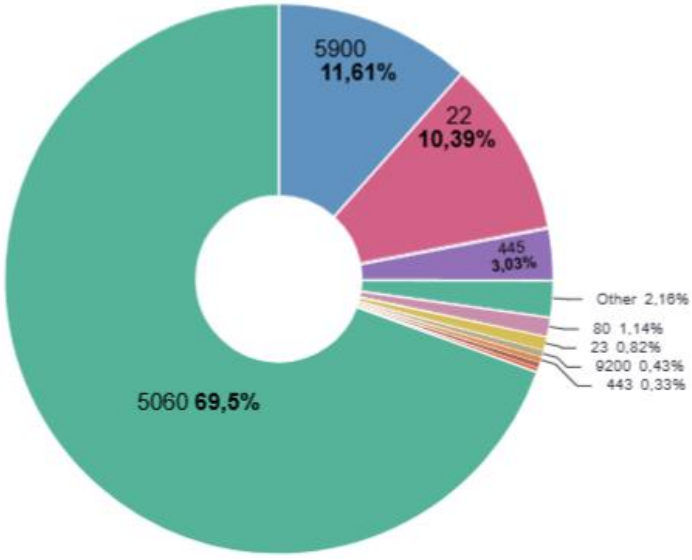


5.2 Italian Honeypot N.1

Nel presente paragrafo vengono riportate le analisi relative all'honeypot N.1 presente sul territorio italiano.

5.2.1 Attacchi ai servizi

Vengono riportate le numeriche sia in termini assoluti che percentuali relativamente agli attacchi ai vari servizi (porte):



Service Port	Count
5060	138.039
5900	23.059
22	20.637
445	6.019
80	2.270
23	1.632
9200	846
443	650
50100	631
10001	548

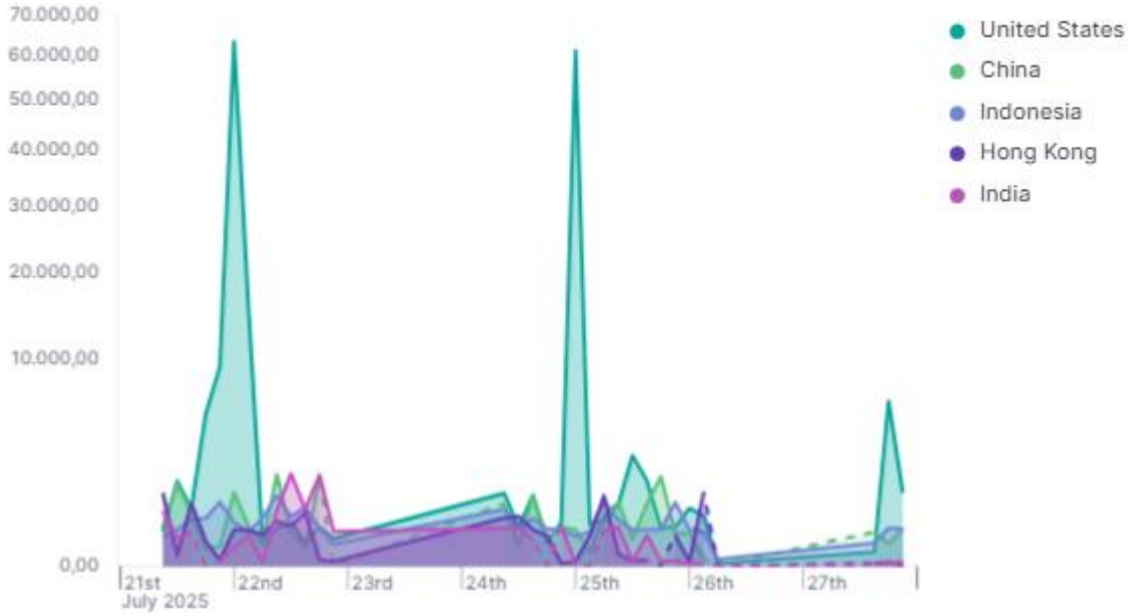
5.2.2 IP Attaccanti

Questa invece la classifica relativa ai 10 IP che hanno effettuato il maggior numero di attacchi:

Source IP	Count
173.233.73.6	137.590
103.156.74.23	8.522
142.202.189.5	7.658
142.202.191.234	7.470
193.37.69.157	5.133
212.34.230.50	2.927
134.209.171.128	2.616
103.114.246.37	2.548
156.231.11.80	2.490
94.26.90.41	1.844

5.2.3 Paesi di provenienza degli attacchi

Si riporta l'andamento dei paesi attaccanti che hanno effettuato movimenti malevoli, verso l'Italia.

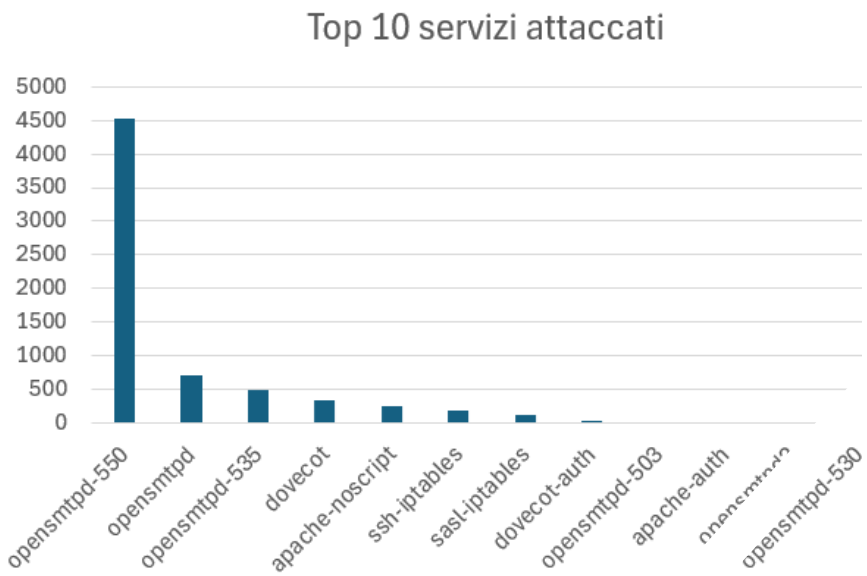


5.3 Italian Honeypot N.2

Nel presente paragrafo vengono riportate le analisi relative all'honeypot N.2 presente sul territorio italiano.

5.3.1 Attacchi ai servizi

Questa la distribuzione degli attacchi per servizio attaccato.



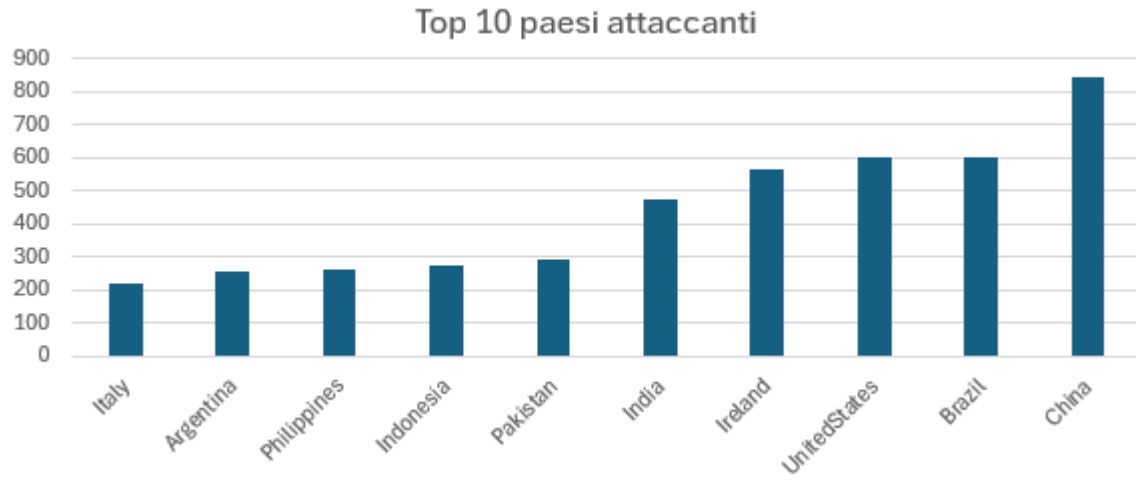
5.3.2 IP attaccanti

Di seguito vengono riportati i TOP 10 degli IP attaccanti per l'insieme degli attacchi effettuati all'Honeypot Italia N2.

Source IP	Numero di attacchi
31[.]28[.]27[.]77	56
5[.]8136[.]209[.]169	29
83[.]69[.]248[.]16	24
200[.]87[.]92[.]60	23
204[.]157[.]219[.]35	23
187[.]254[.]109[.]151	23
59[.]40[.]118[.]200	23
181[.]59[.]2[.]59	23
124[.]107[.]173[.]199	23
5[.]176[.]107[.]242	23

5.3.3 Paesi di provenienza degli attacchi

Questa invece la distribuzione dei paesi attaccanti:



6 Company Profile S3K

Tutto il nostro essere è racchiuso nella nostra VISION: "Rendere il mondo digitale un luogo accessibile, sicuro e sostenibile, al servizio della conoscenza"

COME LO FACCIAMO:

Ci posizioniamo in modo unico nel mercato in cui operiamo, sia grazie ad una precisa offerta multidisciplinare integrata, che al nostro approccio volutamente orientato alla semplificazione di tutto ciò che riguarda i processi di Digital e Security Transformation.

Abbiamo un presidio esteso sul territorio con circa 550 dipendenti distribuiti tra le sedi di Roma, Milano, Torino, Padova, Firenze, Palermo e Catania.

L'ambizione e la prospettiva vedono un ulteriore e progressivo rafforzamento sia sul territorio nazionale che internazionale dove già operiamo con successo e con Clienti di primaria rilevanza.

CON QUALI LEVE OPERIAMO:

Le nostre competenze principali: Data Analytics & Big Data, CyberSecurity, Application Development, Infrastructure Management, Cloud & Managed Security Services.

Più caratteristiche sono poi le nostre competenze verticali, nel novero delle quali particolare attenzione va al PLM, Modelling & Simulation (la società di S3K, Fabaris, è l'unica azienda italiana che sa utilizzare il sistema di modellazione e simulazione jtls (joint theatre level simulation) utilizzato dalla Nato)) e Digital Transaction Management, Business Operation Systems.

40 partnership strategiche, 215 certificazioni professionali, un'esperienza complessiva che sfiora i 150 anni uomo, ed oltre 500 clienti attivi.

CHI SIAMO:

Un FULL SERVICE PARTNER DELLA DIGITAL & SECURITY TRANSFORMATION. Ci posizioniamo in modo unico nel mercato in cui operiamo, sia grazie ad una precisa offerta multidisciplinare integrata, che al nostro approccio volutamente orientato alla semplificazione di tutto ciò che riguarda i processi di Digital e Security Transformation.

S3K nasce nel dicembre 2021 come fusione di importanti realtà già operanti su questi mercati in seguito all'ingresso di un importante Private Equity internazionale (HLD).

LA NOSTRA MISSION:

"Guidiamo i Clienti nei loro processi di cambiamento, riducendo complessità e rischi attraverso competenze multidisciplinari, nel pieno rispetto dei nostri valori fondamentali e delle nostre persone".

I NOSTRI VALORI:

Affidabilità; Integrità; Rispetto; Valorizzazione delle Persone; Passione; Innovazione.

CONTATTI:

contattaci@s3kgroup.it
insidesales@s3kgroup.it
marketing@s3kgroup.it

DISCLAIMER

Tutte le informazioni fornite in questo documento sono fornite "così come sono" solo a scopo informativo e, se non diversamente specificato, non costituiscono un contratto legale tra S3K e qualsiasi persona o entità.

Le informazioni fornite sono soggette a modifiche senza preavviso. Sebbene venga fatto ogni ragionevole sforzo per presentare informazioni aggiornate e accurate, non forniamo alcuna garanzia della loro validità e usabilità in relazione agli intendimenti e necessità dell'Organizzazione.

Questo documento contiene informazioni create e mantenute sia internamente che esternamente, provenienti da diverse fonti. In nessun caso S3K sarà responsabile, direttamente o indirettamente, per qualsiasi danno o perdita causati o

presumibilmente causati da o in connessione con l'uso o l'affidamento su qualsiasi contenuto presentato. Eventuali collegamenti a siti Web esterni non devono essere interpretati come un'approvazione del contenuto o invito alla visualizzazione dei materiali collegati.

CLASSIFICAZIONE DOCUMENTO

2.0 TLP:AM[1]BER = Divulgazione limitata, i destinatari possono diffonderla solo in caso di necessità all'interno della loro organizzazione e dei suoi clienti.

I destinatari possono condividere le informazioni TLP:AMBER con i membri della propria organizzazione e dei suoi clienti, ma solo in caso di necessità per proteggere la loro organizzazione e i suoi clienti e prevenire ulteriori danni.

[1] *Classificazione Traffic Light Protocol (TLP)*: sistema di contrassegni che definisce la misura in cui i destinatari possono condividere informazioni potenzialmente sensibili pubblicato formalmente da Forum of Incident Response and Security Teams (FIRST) nella versione TLP 1.0 nell'agosto 2016 e successivamente aggiornato alla versione TLP 2.0 nell'agosto 2022. Secondo FIRST, lo scopo di TLP è "facilitare una maggiore condivisione di informazioni potenzialmente sensibili e collaborazione più efficace". La versione 2.0 migliora TLP chiarendo ulteriormente le restrizioni di condivisione.

Cyber security

RISK REPORT

S3K

Via del Serafico, 200 - 00142 | Roma (RM)
C.S.iv. € 10.050.000,00 - C.F. e P.IVA: 15379561002