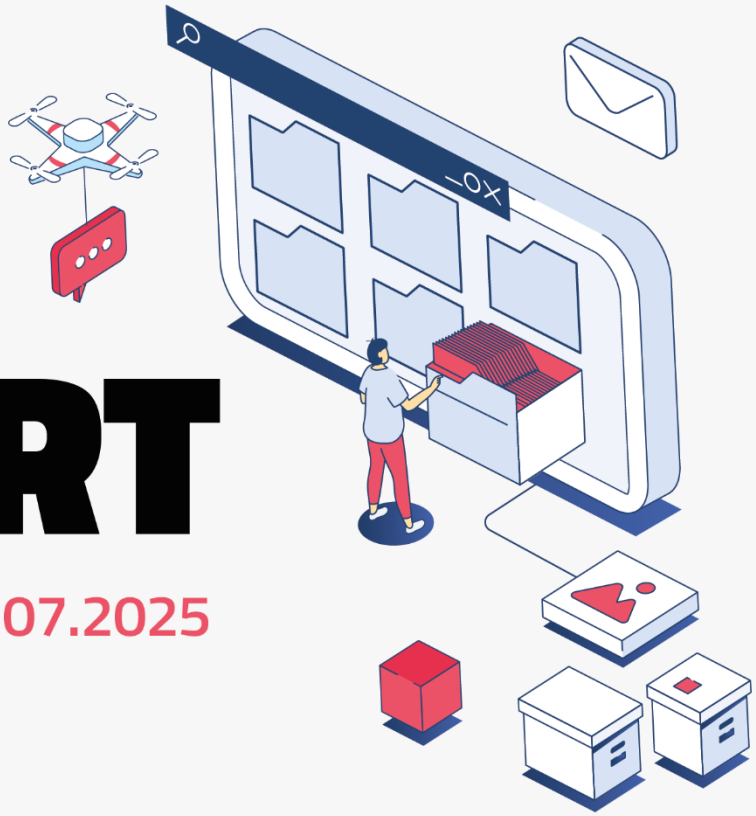
S3K

Cyber security

RISK REPORT

\ week 30.06.2025 - 06.07.2025



Sommario


CYBER SECURITY RISK REPORT
27/25

1 Il Cyber Security Risk Report S3K

Settimana 30.06.2025 - 06.07.2025

Il "Cyber Security Risk Report" è il risultato di uno specifico servizio erogato da S3K. Contiene un riepilogo settimanale delle notizie e degli avvenimenti dal mondo "cyber" e delle tendenze emergenti fornendo all'organizzazione le informazioni necessarie per stare al passo con il panorama in evoluzione delle minacce informatiche.
Per la sua elaborazione, gli analisti di S3K raccolgono ed esaminano dati provenienti da un alto numero di fonti, quali, ad esempio, produttori di hardware e software, ricercatori su tematiche di sicurezza, forum dedicati, canali di comunicazione dei gruppi di cyber criminali, black market, deep web, dark Web.
Alcune delle informazioni che vengono inserite nel bollettino sono:

- trend delle menzioni su social delle CVE
- nuove vulnerabilità, CVE, 0day pubblicati
- informazioni su nuovi attacchi e data breach
- campagne phishing
- attività dei gruppi di cyber criminali
- malware on the wild
- IP riportati come malevoli
- IoC
- pubblicazione di patch, aggiornamenti e workaround
- valutazione della situazione generale e possibili evoluzioni dello scenario cyber

1.1 Presentazione del Cyber Security Risk Report S3K

Il **Cyber Security Risk Report** è il risultato di un servizio specializzato erogato da S3K che offre un riepilogo settimanale completo delle minacce informatiche emergenti e degli eventi significativi nel panorama della cybersecurity. Questo bollettino di Cyber Threat Intelligence (CTI) rappresenta uno strumento essenziale per le organizzazioni che desiderano mantenersi aggiornate sulle ultime evoluzioni delle minacce digitali.

Per la sua elaborazione, gli analisti di S3K raccolgono ed esaminano dati provenienti da numerose fonti, tra cui produttori di hardware e software, ricercatori di sicurezza, forum specializzati, canali di comunicazione dei gruppi criminali, black market, deep web e dark web. Questa analisi approfondita permette di fornire un quadro completo e dettagliato delle minacce attuali e delle loro potenziali evoluzioni.

Il presente report copre la settimana dal 30 giugno al 6 luglio 2025, ed è classificato come **TLP:AMBER**, indicando che le informazioni contenute possono essere condivise solo all'interno dell'organizzazione e con i suoi clienti, limitatamente alle necessità di protezione.

1.2 Sommario degli argomenti trattati

Security News

Aggiornamenti critici rilasciati da Mozilla, Cisco e Apache per risolvere vulnerabilità di elevata gravità. Notizie su attacchi significativi, tra cui la campagna Houken contro settori strategici in Francia, lo smantellamento di una rete di riciclaggio crypto da 540 milioni di dollari e nuove tecniche di attacco che sfruttano funzionalità native di Windows.

Dettagli a questo link : "Cyber News" dal Web, Deep Web e Dark Web

CVE Monitor

Analisi dettagliata delle vulnerabilità più rilevanti della settimana, con focus su plugin WordPress, sistemi industriali e Samsung rLottie. Monitoraggio delle tendenze sui social media, nuove CVE emerse e quelle attivamente sfruttate dagli attaccanti, con particolare attenzione alle vulnerabilità critiche in Cisco ISE e IBM WebSphere.

Dettaglia questo link : CVE Monitor

Analisi Attacchi

Monitoraggio delle campagne di phishing con focus sulle tecniche di social engineering, analisi dei trend nei ransomware, diffusione di malware (NimDoor, DCRat, RondoDox), attacchi DDoS e casi significativi di data breach (Corte Penale Internazionale, Radix, Ingram Micro) e defacement rilevati nel periodo di osservazione.

Dettagli a questo link : Attacchi

Honeypot

Dati raccolti dall'infrastruttura di honeypot S3K dislocata a livello globale, con analisi dettagliata degli attacchi rilevati, servizi più colpiti, IP degli attaccanti e paesi di provenienza. Focus specifico sui due honeypot italiani, con statistiche e trend relativi al panorama nazionale delle minacce.

Dettagli a questo link : Honeypot

Questo report rappresenta uno strumento fondamentale per i professionisti della sicurezza informatica e i responsabili IT, fornendo informazioni tempestive e accurate per migliorare la postura di sicurezza dell'organizzazione e prevenire potenziali attacchi. Le informazioni contenute consentono di identificare rapidamente le minacce emergenti, comprendere le tattiche degli attaccanti e implementare le misure difensive più appropriate.

Questo report si propone come strumento essenziale per professionisti della sicurezza informatica e responsabili decisionali aziendali, fornendo informazioni aggiornate e rilevanti per comprendere il panorama delle minacce e adottare le necessarie contromisure. Le raccomandazioni specifiche incluse in ciascuna sezione offrono indicazioni pratiche per mitigare i rischi identificati e rafforzare la postura di sicurezza complessiva.

Raccomandazioni prioritarie

- Applicare le patch
  Implementare immediatamente gli aggiornamenti di sicurezza per i sistemi critici, specialmente per le vulnerabilità ad alto rischio identificate in questo bollettino, come quelle relative a Microsoft Windows, ClamAV, e plugin WordPress.
- Monitoraggio continuo
  Mantenere un controllo costante sulle attività sospette, specialmente per i servizi più bersagliati come SSH, Telnet, HTTP e RDP. Prestare particolare attenzione ai tentativi di accesso anomali provenienti da indirizzi IP segnalati come malevoli.
- Sensibilizzazione
  Formare il personale sulle più recenti tecniche di phishing, in particolare quelle che impersonano colleghi o contatti aziendali reali. Educare gli utenti Android sui rischi relativi al malware bancario e alle applicazioni sospette.

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Tenable	Tenable ha rilasciato aggiornamenti di sicurezza che risolvono una vulnerabilità con gravità "alta" nel noto vulnerability scanner Nessus. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di accedere in scrittura a file arbitrari sui sistemi interessati. Versioni affette: • Nessus, versione 10.8.4 e precedenti per Windows
ULR/Note	https://www.tenable.com/security/tns-2025-13

PRODOTTO	DESCRIZIONE
Google	Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere una vulnerabilità di sicurezza con gravità "alta". Versioni affette: • versioni precedenti alla 138.0.7204.96/.97 per Windows • versioni precedenti alla 138.0.7204.92/.93 per Mac • versioni precedenti alla 138.0.7204.96 per Linux
ULR/Note	https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_30.html

PRODOTTO	DESCRIZIONE
Trend Micro	Risolta una vulnerabilità di sicurezza con gravità "alta" relativa ai prodotti consumer di Trend Micro Security, suite di soluzioni per la cybersecurity sviluppata da Trend Micro. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di elevare i propri privilegi sul sistema target. Versioni affette: • Trend Micro Security (Consumer) 17.8.x, versioni precedenti alla 17.8.1476 per Windows
ULR/Note	https://helpcenter.trendmicro.com/en-us/article/TMKA-18876

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

CAMPAGNA HOUKEN CONTRO SETTORI STRATEGICI IN FRANCIA

L'Agenzia Nazionale francese per la sicurezza dei sistemi informativi (ANSSI) ha reso noto che, a partire da settembre 2024, una campagna cyber ha preso di mira i settori strategici della Francia, fra cui enti governativi, telecomunicazioni, media, banche e trasporti, sfruttando vulnerabilità zero-day nell'Ivanti Cloud Services Appliance (CSA). Le vulnerabilità identificate, CVE-2024-8190, CVE-2024-8963 e CVE-2024-9380, sono state usate a catena per ottenere l'accesso remoto, estrarre credenziali, installare web shell e persino impiantare un rootkit a livello kernel. Le intrusioni venivano poi raffinate con script PHP, shell pubbliche come Behinder e neo-reGeorg, e un modulo Linux denominato sysinitd.ko.
ANSSI ha denominato questo insieme di attività con il nome in codice Houken, evidenziando strette somiglianze con il cluster UNC5174 (alias Uteus), già monitorato da Mandiant e Google. Il modus operandi è tipico degli access broker: un gruppo individua le vulnerabilità, un altro le weaponizza su ampia scala, mentre un terzo gruppo compra l'accesso per condurre spionaggio o attività criminali, incluso il mining di criptovalute. In alcuni casi, dopo aver ottenuto accesso persistente, i criminali hanno patchato le stesse backdoor che avevano sfruttato, impedendo a concorrenti di entrare nei sistemi. Il traffico dannoso è stato instradato tramite server VPN commerciali e host dedicati, garantendo anonimato e resilienza operativa .
In aggiunta allo spionaggio digitale, ANSSI ha verificato casi di furto di email diplomatiche (da un ministero sudamericano) e di installazione di miner Monero su server compromessi, confermando il duplice scopo: intelligence e profitto. Le conseguenze per le vittime possono essere pesanti: ANSSI avverte che Houken e UNC5174 rimangono operativi e continueranno a sfruttare dispositivi esposti a livello mondiale, soprattutto gateway VPN e appliance cloud edge.

SMANTELLATA RETE DI RICICLAGGIO CRYPTO DA 540 MILIONI DI DOLLARI

Le autorità spagnole hanno smantellato una banda che avrebbe riciclato circa 540 milioni di dollari (poco meno di 460 milioni di euro), frutto di investimenti in criptovalute fraudolenti. Le forze dell'ordine hanno arrestato cinque persone, due a Madrid e tre nelle Isole Canarie, ritenute responsabili di truffe che avrebbero colpito oltre 5.000 vittime. L'operazione, guidata dalla Guardia Civil, è stata realizzata in stretta collaborazione con Europol e le autorità di Francia, Estonia e Stati Uniti (HSI). Le indagini, avviate nel 2023, hanno visto l'invio di un esperto di criptovalute in Spagna proprio nel giorno dei fermi, con l'obiettivo di intercettare e recuperare i capitali sottratti. Secondo le autorità, il gruppo criminale faceva confluire ingenti somme verso strutture aziendali e finanziarie con base a Hong Kong. Per nascondere la provenienza illecita dei fondi, venivano utilizzati circuiti di pagamento oscuri, conti intestati a più soggetti e più exchange, consolidando l'intera rete di riciclaggio. Europol, nel comunicato ufficiale, ha descritto le tattiche impiegate: un network globale di complici raccoglieva denaro tramite prelevamenti in contanti, trasferimenti bancari e transazioni in criptovalute. Il tutto, orchestrato con sofisticate infrastrutture digitali e aziendali distribuite a livello internazionale. Nel testo si sottolinea come la tecnologia stia avvantaggiando questa forma di criminalità finanziaria: "online fraud is expected to outpace other types" grazie all'uso dell'intelligenza artificiale, che potenzia l'ingegneria sociale. L'azione delle autorità spagnole si aggiunge ad un'altra operazione avvenuta ad aprile 2025, quando vennero fermate sei persone accusate

di impiegare deepfake (strumenti di IA) in truffe di investimento crypto, utilizzando volti noti per rendere più credibili gli annunci. Europol ha definito questo tipo di frodi "senza precedenti" per ampiezza e articolazione, avvertendo che nel prossimo futuro le truffe online potrebbero superare tutte le altre forme di criminalità organizzata. Nel frattempo, negli Stati Uniti la FTC ha rilevato che nel 2024 le perdite causate da frodi online hanno raggiunto i 12,5 miliardi di dollari, un record nazionale. Ad inizio giugno, il Dipartimento di Giustizia USA ha annunciato il sequestro di 225 milioni di dollari in criptovalute, legati a truffe d'investimento, cifra record per il Secret Service ma che resta comunque una piccola parte delle perdite totali.

NUOVA TECNICA DI ATTACCO SFRUTTA LE FUNZIONALITÀ DI WINDOWS PER INGANNARE GLI UTENTI

Un ricercatore noto con lo pseudonimo mr.d0x ha recentemente pubblicato una nuova modalità di attacco chiamata FileFix, che sfrutta funzionalità native di Windows per compromettere la sicurezza degli utenti in modo subdolo ma estremamente efficace. Il cuore di questa tecnica risiede nella manipolazione delle icone dei file, che possono essere facilmente alterate per far sembrare innocuo un file in realtà dannoso. Grazie all'uso del protocollo ms-appinstaller, un semplice clic sull'icona può indurre l'utente ad avviare l'installazione di un'applicazione malevola tramite il browser Edge, sfruttando App Installer di Windows.
Ciò che rende FileFix particolarmente insidioso è il suo impatto visivo: l'utente vede un file con un'icona rassicurante e familiare, come quella di un PDF o di un documento Word, ma in realtà è un collegamento dissimulato verso un payload ostile. Inoltre, dato che l'esecuzione avviene tramite funzioni apparentemente legittime del sistema operativo, molti strumenti di sicurezza potrebbero non rilevare l'attività come sospetta. Anche se questa tecnica è stata presentata a scopo dimostrativo e non è ancora stata rilevata in campagne attive, rappresenta un chiaro esempio di come le caratteristiche di usabilità dei sistemi operativi possano essere trasformate in vettori d'attacco. La raccomandazione è di prestare sempre attenzione all'estensione effettiva dei file e di evitare di aprire allegati provenienti da fonti non verificate, anche quando appaiono visivamente innocui.

ATTACCHI PHISHING TRAMITE PDF: CRESCE L'IMPERSONIFICAZIONE DI BRAND NOTI

Negli ultimi tempi si è registrato un aumento allarmante delle truffe informatiche che utilizzano file PDF per ingannare gli utenti. Questi documenti, che appaiono affidabili e professionali, vengono impiegati per imitare comunicazioni ufficiali di aziende note, con l'intento di carpire informazioni riservate o diffondere software dannoso. Un'indagine di Cisco Talos ha evidenziato che, tra il 5 maggio e il 5 giugno 2025, è cresciuto notevolmente l'uso di PDF allegati per impersonare aziende come Microsoft, PayPal, DocuSign, NortonLifeLock e Geek Squad. Questa tecnica, nota come TOAD (Telephone-Oriented Attack Delivery), utilizza numeri di assistenza contraffatti per indurre le vittime a contattare call center controllati dagli stessi criminali. Tra le tecniche più sofisticate figura l'invio di PDF che sembrano documenti interni aziendali – ad esempio, file intitolati "Aumento Retribuzione", contenenti codici QR. La scansione di questi codici QR conduce a pagine web fraudolente create per rubare le credenziali degli utenti. In molti casi, i documenti vengono condivisi tramite servizi noti come Dropbox, rendendo l'inganno più credibile agli occhi della vittima. Gli attaccanti fanno leva sull'apparente legittimità dei PDF, spesso realizzati con elementi grafici curati, collegamenti attivi e marchi riconoscibili, rendendo complesso distinguerli da documenti autentici. Per ridurre il rischio di cadere vittima di attacchi phishing veicolati tramite file PDF, è fondamentale adottare alcune buone pratiche di sicurezza digitale. Prima di tutto, è importante prestare particolare attenzione all'origine dei messaggi ricevuti, soprattutto quando contengono allegati inaspettati. Se un file PDF arriva senza preavviso o da un mittente sconosciuto, è bene trattarlo con sospetto. Inoltre, bisogna evitare di cliccare su link contenuti nel documento o di scansionare eventuali codici QR, poiché potrebbero reindirizzare a siti web fraudolenti progettati per sottrarre dati personali. In caso di dubbi sull'autenticità della comunicazione, è sempre consigliabile rivolgersi direttamente all'azienda o al servizio tramite i canali ufficiali, evitando di utilizzare i riferimenti presenti nel file stesso. Infine, mantenere aggiornati l'antivirus e gli altri strumenti di sicurezza presenti sul proprio dispositivo è un passo essenziale per intercettare tempestivamente eventuali minacce. La prevenzione e la consapevolezza restano le armi più efficaci contro un panorama di attacchi in costante evoluzione. Essere informati e mantenere un atteggiamento critico è fondamentale per evitare di cadere vittima di questi attacchi sempre più sofisticati.

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 30 Giugno – 6 Luglio 2025
Settimana caratterizzata da un'ondata di vulnerabilità critiche su numerosi plugin WordPress, sistemi industriali, Samsung rLottie, e Microsoft Edge. Molte vulnerabilità permettono esecuzione di codice remoto (RCE) o privilege escalation, alcune anche da attaccanti non autenticati.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Descrizione Sintetica
CVE-2025-41656	CRITICAL	01/07/2025	❌	IndustrialPI – RCE da remoto senza autenticazione (Node-RED non protetto).
CVE-2025-41648	CRITICAL	01/07/2025	❌	IndustrialPI – Bypass login webapp, accesso a tutte le impostazioni.
CVE-2025-53076	CRITICAL	30/06/2025	❌	Samsung rLottie v0.2 – RCE via overread buffer (improper input validation).
CVE-2025-4689	CRITICAL	02/07/2025	❌	WP Ads Pro – LFI combinato a SQLi per RCE remoto non autenticato.
CVE-2025-5746	CRITICAL	02/07/2025	❌	WP Drag&Drop Upload (WooCommerce) – Upload file arbitrari da non autenticati.
CVE-2025-3848	HIGH	02/07/2025	✅ Wordfence	WP SmartPay – Privilege escalation via account takeover (email reset).
CVE-2025-49713	HIGH	02/07/2025	❌	Microsoft Edge – RCE via type confusion (richiede interazione utente).
CVE-2025-5692	HIGH	02/07/2025	✅ Wordfence	WP Leads Builder – Privilege escalation da Subscriber a Admin.

CVE-2025-4380	HIGH	02/07/2025	❌	WP Ads Pro – LFI (file PHP eseguibili) via bsa_template.
CVE-2025-4381	HIGH	02/07/2025	❌	WP Ads Pro – SQL injection remota.
CVE-2025-5817	HIGH	02/07/2025	❌	WP Amazon Products – SSRF da remoto non autenticato.
CVE-2025-6463	HIGH	02/07/2025	❌	WP Forminator – Arbitrary file deletion via form auto-delete.
CVE-2025-6463	HIGH	04/07/2025	❌	WP HRM – Escalation privilegi da Employee a Admin via AJAX.
CVE-2025-5961	HIGH	03/07/2025	✅ GitHub	WPvivid – Arbitrary file upload (RCE possibile su NGINX).
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

- **WordPress Plugins:** escalation privilegi, SQLi, LFI, file upload in:
  - Ads Pro, SmartPay, Leads Builder, WPvivid, VikRentCar, Drag&Drop Upload, HRM, Forminator.
- **Sistemi Industriali:** IndustrialPI senza autenticazione adeguata → full RCE.
- **Samsung:** rLottie 0.2 con vulnerabilità critiche di overread/overflow.
- **Microsoft Edge:** RCE da tipo confuso (type confusion) in ambienti Chromium.

Distribuzione Giornaliera

- **1–2 luglio**: Wordfence disclosure multipli (WP), Samsung advisories.
- **3–4 luglio**: Exploit WPvivid pubblicato su GitHub, nuove CVE WP confermate.

Raccomandazioni

- **Patch Prioritarie:**
  - Aggiornare o disabilitare plugin WP vulnerabili.
  - Disabilitare o proteggere l'accesso a Node-RED (IndustrialPI).
  - Verificare rLottie in progetti embedded/IoT Samsung-based.
  - Monitorare Microsoft Edge → aggiornare browser.

- **Mitigazioni e Controlli:**
    - Bloccare .php upload su directory accessibili.
    - Verificare ruoli utenti WordPress (modifiche sospette).
    - Audit dei plugin installati → rimuovere Ads Pro o configurare WAF.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-1316	Edimax IC-7100 (IP camera)	N/A
CVE-2025-49826	Next.js	N/A
CVE-2025-32463	Sudo, componente Unix/Linux	N/A
CVE-2023-52927	kernel Linux, modulo Netfilter	N/A
CVE-2025-6554	Google Chrome	N/A

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-2025-41656	Node-RED	N/A
VULNERABILITÀ	Un attaccante remoto non autenticato può eseguire comandi arbitrari sui dispositivi interessati con privilegi elevati, poiché l'autenticazione del server Node-RED non è configurata per impostazione predefinita.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-6897	D-Link DI-7300G+ (router aziendale)	9.8
VULNERABILITÀ	È stata trovata una vulnerabilità classificata come critica nel dispositivo D-Link DI-7300G+, versione 19.12.25A1. La vulnerabilità riguarda una funzionalità non specificata del file httpd_debug.asp. La manipolazione del parametro Time consente un attacco di OS Command Injection, cioè permette a un attaccante di eseguire comandi arbitrari sul sistema operativo del dispositivo. L'exploit è stato reso pubblico, quindi potrebbe già essere utilizzato per attacchi reali.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-41648	IndustrialPI	N/A
VULNERABILITÀ	Un attaccante remoto non autenticato può bypassare il login dell'applicazione web dei dispositivi vulnerabili, rendendo possibile l'accesso e la modifica di tutte le impostazioni disponibili dell'IndustrialPI, un PLC basato su tecnologia RaspberryPI	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-5746	Plugin Drag and Drop Multiple File Upload (Pro) per WooCommerce su WordPress	N/A
VULNERABILITÀ	Il plugin Drag and Drop Multiple File Upload (Pro) per WooCommerce su WordPress è vulnerabile a caricamenti arbitrari di file a causa della mancanza di validazione del tipo di file nella funzione dnd_upload_cf7_upload_chunks() nelle versioni dalla 5.0 alla 5.0.5 (quando usato insieme al tema PrintSpace) e in tutte le versioni fino alla 1.7.1 inclusa (nella versione standalone). Questo permette ad attaccanti non autenticati di caricare file arbitrari sul server del sito vulnerabile, con possibile esecuzione remota di codice. L'esecuzione di PHP è disabilitata tramite un file .htaccess, ma in alcune configurazioni server è comunque possibile sfruttare la vulnerabilità.	

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-2025-48927
DESCRIZIONE	
La vulnerabilità CVE-2025-48927 riguarda il servizio TeleMessage, che fino al 5 maggio 2025 configura Spring Boot Actuator con un endpoint heap dump esposto all'URI /heapdump, consentendo potenzialmente a un attaccante di accedere a informazioni sensibili della memoria del sistema. Questa falla è stata già sfruttata attivamente in natura nel maggio 2025.	

CVE	CVE-2025-48928
DESCRIZIONE	
Il servizio TeleMessage fino al 5 maggio 2025 si basa su un'applicazione JSP in cui il contenuto dell'heap è simile a un "core dump" che includeva password inviate precedentemente via HTTP; questa vulnerabilità è stata sfruttata attivamente nel maggio 2025.	

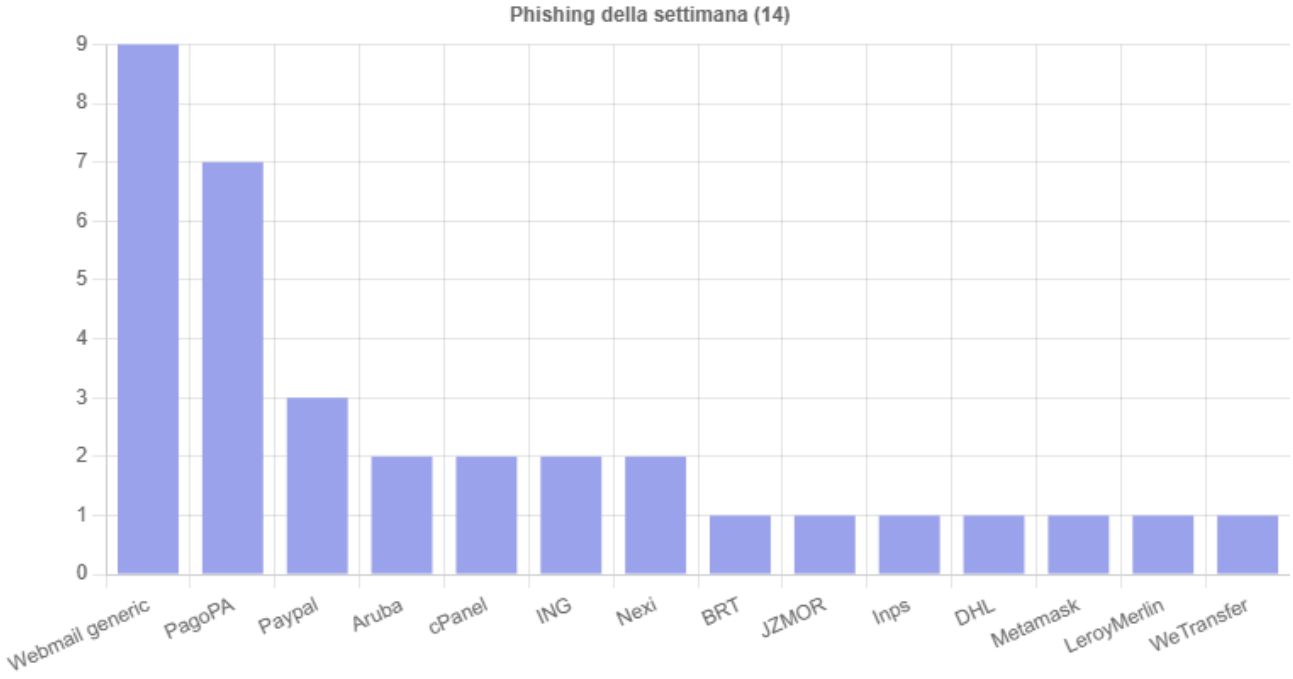
CVE	CVE-2025-6554
DESCRIZIONE	
Una vulnerabilità di tipo type confusion nel motore V8 di Google Chrome, presente nelle versioni precedenti alla 138.0.7204.96, permette a un attaccante remoto di eseguire operazioni di lettura e scrittura arbitrarie tramite una pagina HTML appositamente creata; la gravità segnalata per questa falla è alta.	

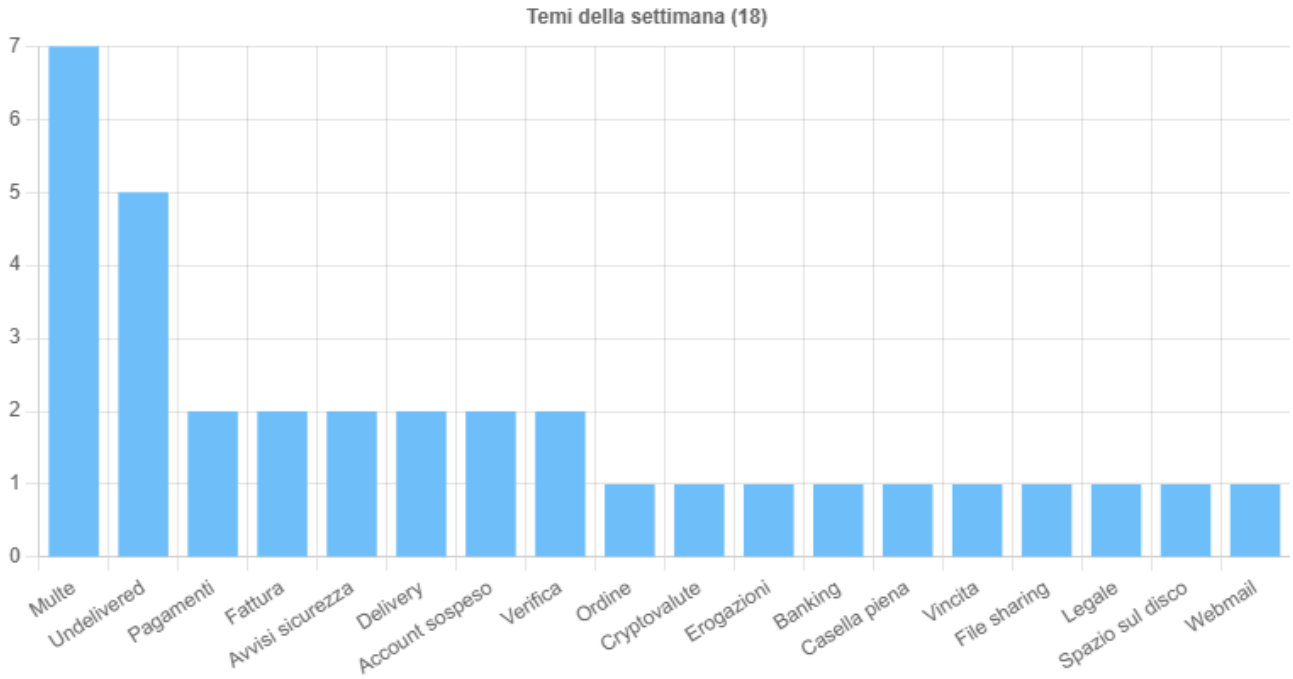
4 Attacchi

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.

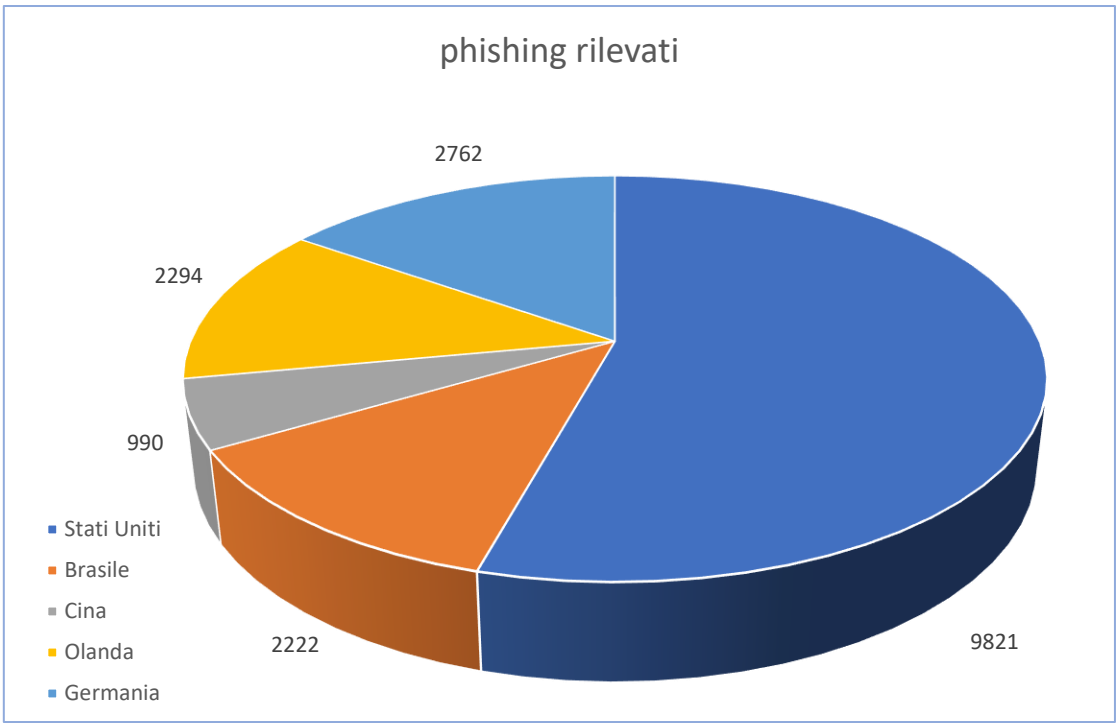




Fonte :CERT-AGID

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.



Nelle pagine seguenti l'analisi dettagliata di una mail raccolta dalla redazione che può essere catalogata come "phishing":

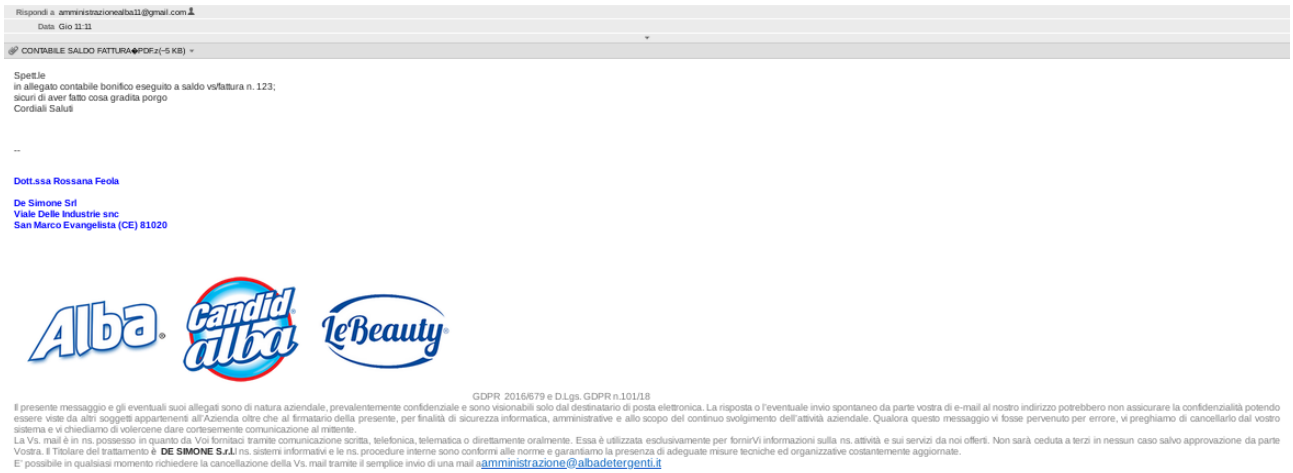
- Analisi email phishing

  L'e-mail analizzata è una campagna di malspam in lingua italiana che finge di provenire da "ALBA DETERGENTI" e invita la vittima ad aprire un falso documento contabile ("CONTABILE SALDO FATTURA.PDF.z"). L'header rivela invece l'origine da un server compromesso – dixonparker[.]proyectojuvenil[.]com [45[.]138[.]183[.]203] – privo di SPF, DKIM e DMARC e già coinvolto in numerosi invii di malware. L'allegato, un archivio LZH camuffato da PDF, contiene un executable .scr rilevato da 10 / 36 motori AV su MalwareBazaar, con correlazioni a campagne MassLogger/AgentTesla distribuite dallo stesso IP. Di seguito l'analisi completa (il dominio di destinazione è sostituito con victim.com, il destinatario con victim).

- Analisi tecnica della e-mail

Voce	Evidenza	Commento investigativo
Mittente dichiarato	ALBA DETERGENTI <amministrazionealba11@gmail.com>	Gmail gratuito, non coerente con il brand; probabile spoofing/impersonation.
Return-Path	amministrazionealba11@gmail.com	Disallineato con dominio source.
Destinatario	victim@victim.com	Dato redatto su richiesta utente.
Subject	"CONTABILE SALDO FATTURA"	Social engineering a tema contabile/fattura.
Allegato	CONTABILE SALDO FATTURA.PDF.z (23 KB, LZH)	Archivio con estensione fuorviante.
Received-path	Origina da dixonparker[.]proyectojuvenil[.]com [45[.]138[.]183[.]203], poi inoltro su host interni	Fonte non correlata a Gmail; catena tipica di spam relay.
SPF / DKIM / DMARC	Assenti → SPF fail, DKIM missing, DMARC none	Facilita spoofing.

Lo screenshot di seguito riportato mostra la finta email (indirizzo del destinatario oscurato). La formulazione cortese, il riferimento a un presunto bonifico e l'estensione ".PDF.z" sono tipici trigger di fiducia sfruttati dalle campagne in oggetto.


Rispondi a amministrazionealba11@gmail.com
Data Gio 11:11
CONTABILE SALDO FATTURA◆PDF.z(~5 KB)

Spett.le
in allegato contabile bonifico eseguito a saldo vs/fattura n. 123;
sicuri di aver fatto cosa gradita porgo
Cordiali Saluti

--

Dott.ssa Rossana Feola

De Simone Srl
Viale Delle Industrie snc
San Marco Evangelista (CE) 81020

GDPR 2016/679 e D.Lgs. GDPR n.101/18
Il presente messaggio e gli eventuali suoi allegati sono di natura aziendale, prevalentemente confidenziale e sono visionabili solo dal destinatario di posta elettronica. La risposta o l'eventuale invio spontaneo da parte vostra di e-mail al nostro indirizzo potrebbero non assicurare la confidenzialità potendo essere viste da altri soggetti appartenenti all'Azienda oltre che al firmatario della presente, per finalità di sicurezza informatica, amministrative e allo scopo del continuo svolgimento dell'attività aziendale. Qualora questo messaggio vi fosse pervenuto per errore, vi preghiamo di cancellarlo dal vostro sistema e vi chiediamo di volercene dare cortesemente comunicazione al mittente.
La Vs. mail è in ns. possesso in quanto da Voi fornitaci tramite comunicazione scritta, telefonica, telematica o direttamente oralmente. Essa è utilizzata esclusivamente per fornirVi informazioni sulla ns. attività e sui servizi da noi offerti. Non sarà ceduta a terzi in nessun caso salvo approvazione da parte Vostra. Il Titolare del trattamento è **DE SIMONE S.r.l.** I ns. sistemi informativi e le ns. procedure interne sono conformi alle norme e garantiamo la presenza di adeguate misure tecniche ed organizzative costantemente aggiornate.
E' possibile in qualsiasi momento richiedere la cancellazione della Vs. mail tramite il semplice invio di una mail a amministrazione@albadetergenti.it

- Reputazione di dominio, IP e hosting

Indicatore	Risultato sintetico	Fonti
45[.]138[.]183[.]203	ASN AS215761 (HostingTurchia), nessun reverse legittimo, range usato per mail botnet.	ipinfo.ioipinfo.io
Stesso IP in altre mail malevole	Presente in invii “AWB9284730932” e “New Order 0104202501” collegate a campagne Agent Tesla.	bazaar.abuse.chbazaar.abuse.ch
Abuse/Spam listing	Range 45[.]138[.]183[.]0/24 segnalato su Spamhaus come “bullet-proof hosting”.	spamhaus.org
dixonparker[.]proyectojuvenil[.]com	Dominio 1 anno, registrar NameCheap, nessun MX valido; reputazione sospetta.	gridinsoft.com
Brand legittimo albadetergenti[.]it	Azienda italiana reale (prodotti detergenti) non coinvolta nello spam.	albadetergenti.it

- Analisi dell'allegato

Hash	Tipo / estratto	Detections
SHA-256 add17378…e3a (file .z)	Archivio LZH camuffato	5 vendor TI; 10 / 36 AV ("Win32.Trojan.Generic", "Mal/DrodLzh") bazaar.abuse.ch
Contenuto interno CONTABILE SALDO FATTURAúPDF.scr SHA-256 bc9d8717…48dd	PE executable (39 KB)	Indicatore primario di compromissione (downloader)

MalwareBazaar conferma la delivery via e-mail attachment e associa tag *malspam*; identica infrastruttura compare in lotti MassLogger/AgentTesla diffusi tra marzo e luglio 2025. bazaar.abuse.chbazaar.abuse.ch

- Consultazioni su database e sandbox
    - VirusTotal – hash presente, link pubblico fornito (richiede JS) virustotal.com analisi
    - Hybrid-Analysis – comportamenti sospetti (process hollowing, connessioni HTTP) collegati al sample (link in MalwareBazaar) bazaar.abuse.ch
    - PhishTank – nessuna entry per URL (non presenti link phishing), metodica centrata sull'allegato. phishtank.org
    - AbuseIPDB / OTX AlienVault – API non accessibili senza autenticazione; l'IP rientra comunque nei blocchi Spamhaus/XBL sopra citati.
- Indicatori di compromissione (IoC)

Categoria	Valore (con "[.]")
IP	45[.]138[.]183[.]203
Dominio mittente reale	dixonparker[.]proyectojuvenil[.]com
Dominio impersonato	albadetergenti[.]it
Hash archivio	add1737843baac4d8005469e2c5910fb0a806b093e07a3e0b975cd5064469e3a
Hash payload	bc9d8717914b732c4108091364065da314903213a64b26b7fd176db8a22148dd

Categoria	Valore (con "[.]")
Return-Path	amministrazionealba11[@]gmail[.]com
Subject	CONTABILE SALDO FATTURA

- Tecniche di ingegneria sociale

  L'attore sfrutta:

  - Urgenza finanziaria (saldo fattura, allegato "contabile") per obbligare l'apertura dell'archivio.
  - Brand spoofing di un marchio domestico italiano con buona reputazione – ALBA Detergenti – per aumentare la credibilità.
  - Estensione doppia (.PDF.z) che simula un documento ma contiene un archivio compresso con eseguibile .scr.
  - Campo Reply-To identico al From per mascherare eventuali incongruenze.

- Conclusioni e raccomandazioni

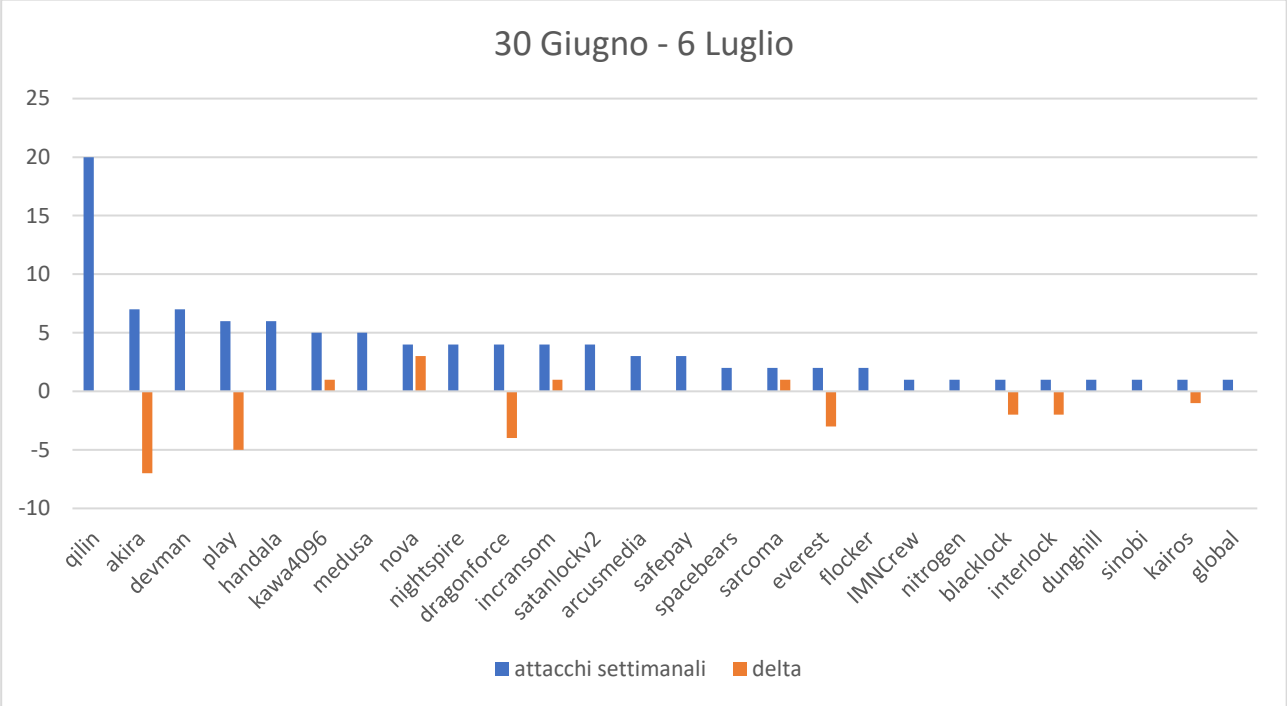
  L'e-mail rappresenta un tentativo di phishing/malware delivery mirato a reti aziendali italiane. L'infrastruttura è collegata a campagne note di stealer (MassLogger / AgentTesla) propagate dallo stesso IP bullet-proof.

- Raccomandazioni operative

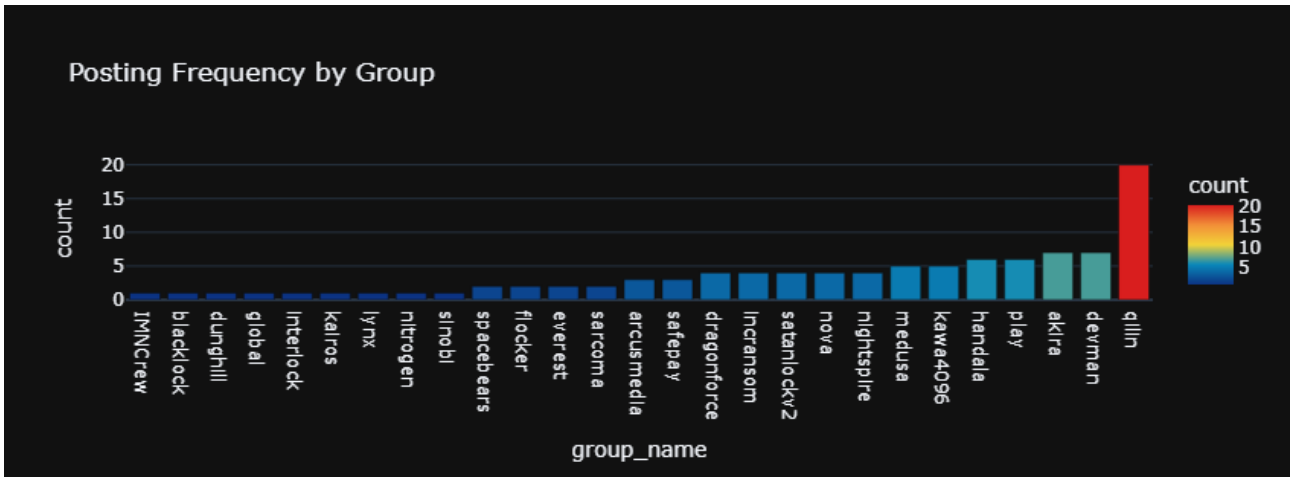
  - Bloccare a livello gateway l'IP 45[.]138[.]183[.]203 e il dominio dixonparker[.]proyectojuvenil[.]com.
  - Aggiornare le firme AV/EDR con gli hash sopra elencati; abilitare decompressione di archivi LZH.
  - Forzare controlli SPF-DKIM-DMARC in *reject* per messaggi che dichiarano Gmail ma provengono da IP terzi.
  - Sensibilizzare l'utente finale sull'estensione ingannevole e sul tema "contabile fattura".

4.2 Ransomware

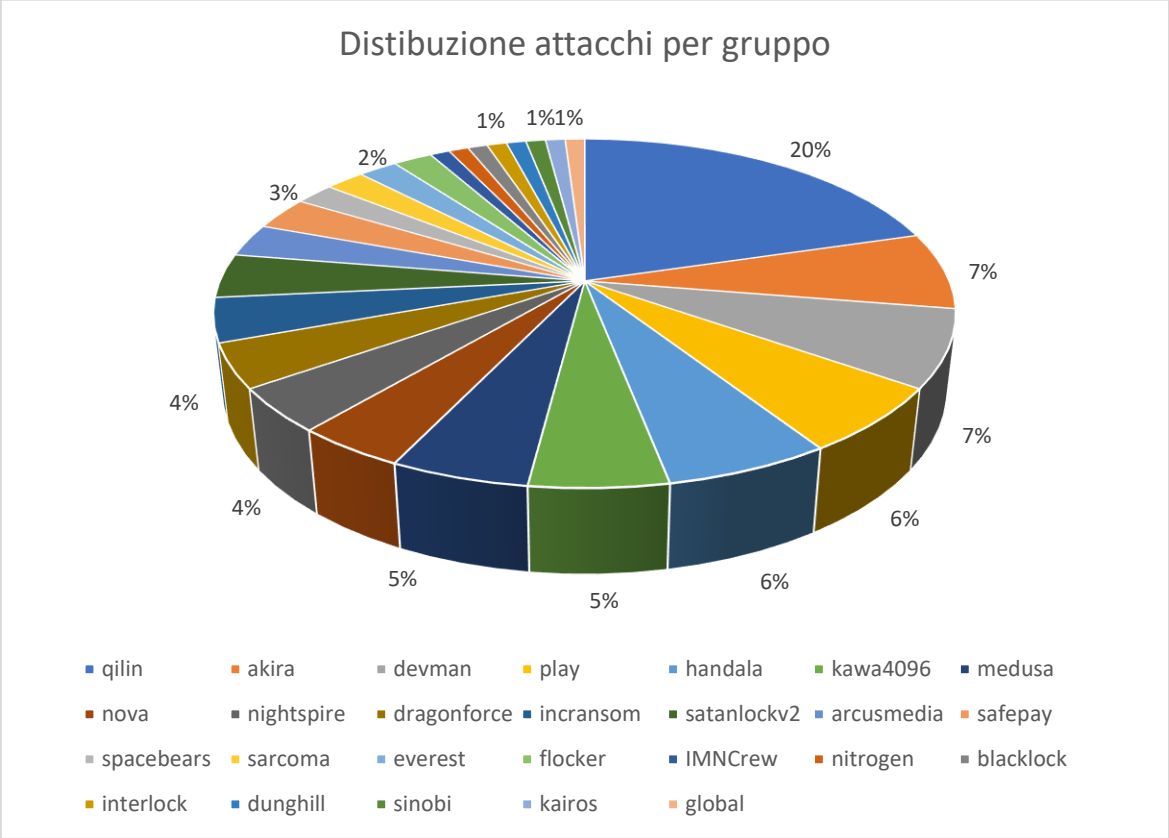
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (30 Giugno – 6 Luglio). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

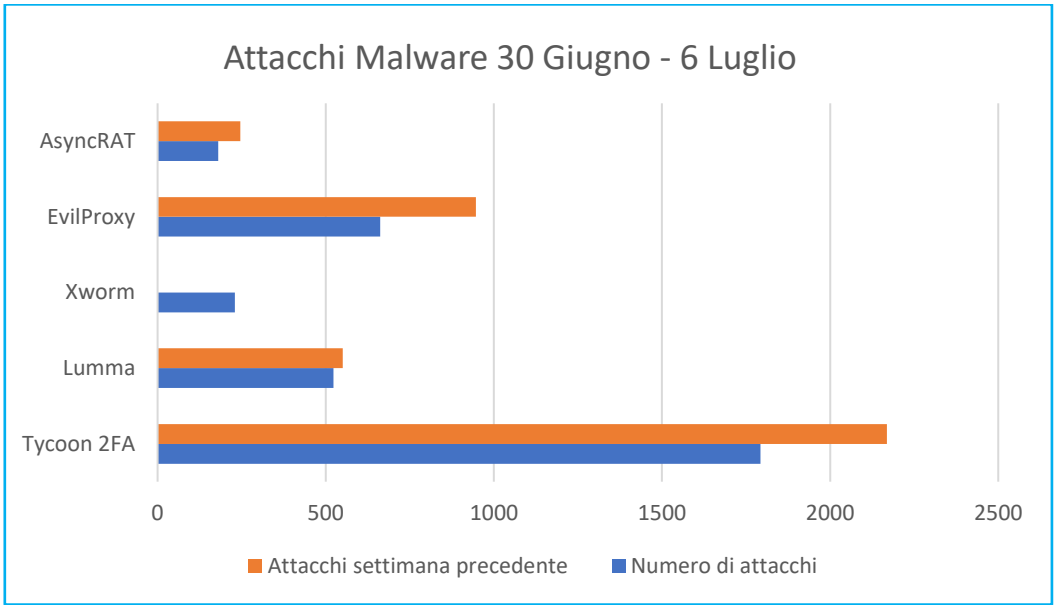


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



4.3 Malware

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



Report settimanale sui malware più attivi

NimDoor (macOS)

Descrizione tecnica: NimDoor è un malware per macOS scoperto da SentinelLabs (SentinelOne) in una campagna attribuita ad attori DPRK che prende di mira aziende Web3/crypto. L'attacco inizia con ingegneria sociale avanzata (messaggi su Telegram e link finti per aggiornamenti Zoom) che induce la vittima a eseguire uno script AppleScript (zoom_sdk_support.scpt) travestito da aggiornamento legittimo. Lo script recupera uno script aggiuntivo da un C2 (es. support.us05web-zoom[.]forum). Vengono quindi installati più payload binari (scritti in Nim e C++) in cartelle nascoste (~/Library/.../Google LLC, ~/Library/CoreKit, ecc.). Il malware utilizza process injection per iniettare codice in altri processi e implementa un meccanismo di persistenza insolito basato su segnali Unix (SIGINT/SIGTERM) che assicura la reinstallazione dei payload al riavvio. Infine stabilisce comunicazione cifrata TLS/WebSocket con il C2 per l'esfiltrazione dati (credenziali, chat Telegram, cronologia browser) e per ricevere nuovi comandi (cronologia attacchi, distribuzione di ulteriori malware)

IoC:

Tipo	Valore
Domain	ataupload[.]store (upl/tlgrm C2) firstfromsep[.]online (netchk C2) safeup[.]store (CoreKit C2) support[.]us05web-zoom[.]pro (zoom_sdk_support.scpt C2)

	writeup[.]live	(CoreKit C2)
FilePaths	~/Library/Application Support/Google LLC/Google LLC ~/Library/LaunchAgents/com.google.update.plist ~/.ses ~/Library/CoreKit/CoreKitAgent ~/Library/DnsService/a ~/Library/DnsService/netchk /private/tmp/.config /private/tmp/cfg /private/var/tmp/uplex_//	
SHA-1	027d4020f2dd1eb473636bc112a84f0a90b6651c 0602a5b8f089f957eeda51f81ac0f9ad4e336b87 06566eabf54caafe36ebe94430d392b9cf3426ba 08af4c21cd0a165695c756b6fda37016197b01e7 16a6b0023ba3fde15bd0bba1b17a18bfa00a8f59 1a5392102d57e9ea4dd33d3b7181d66b4d08d01d	trojan1_arm64 (x86_64) Google LLC (universal) installer (universal) installer (universal) Google LLC (arm64) CoreKitAgent (x86_64)
Scripts	023a15ac687e2d2e187d03e9976a89ef5f6c1617 bb72ca0e19a95c48a9ee4fd658958a0ae2af44b6 4743d5202dbe565721d75f7fb1eca43266a652d4	zoom_sdk_support.scpt tlgm upl

MITRE ATT&CK:

- Spearphishing via email/Telegram (T1566) usata per veicolare lo script maligno.
- Command and Scripting Interpreter – AppleScript (T1059.002) e Bash (T1059.004) per esecuzione dei payload.
- Process Injection (T1055) per iniettare codice nei processi di sistema.
- Persistence attraverso Launch Agent/Daemons (T1547.001) e il meccanismo basato sui segnali.

Contromisure (rilevazione e mitigazione):

- L'attività di NimDoor può essere mitigata con soluzioni EDR/NGAV aggiornate in grado di riconoscere gli script AppleScript sospetti e i pattern delle connessioni WebSocket a domini maligni.
- Si consiglia di bloccare i domini C2 noti (es. dataupload.store, firstfromsep.online ecc.) e di monitorare anomalie nei processi di sistema (ad es. modifiche non autorizzate ai file in ~/Library).
- Per la difesa, è cruciale applicare restrizioni alle esecuzioni di script non firmati su macOS, istruire gli utenti a non eseguire aggiornamenti provenienti da link non verificati e mantenere abilitata la sicurezza del Keychain.

Livello di rischio: Alto. NimDoor rappresenta una minaccia avanzata (APT) con capacità di elusione sofisticate e impatta direttamente obiettivi strategici (Web3/Crypto).

DCRat Malware

Descrizione tecnica: DCRat è un Remote Access Trojan (RAT) modulare per Windows recentemente identificato da Fortinet in una campagna phishing mirata alle organizzazioni colombiane. L'attacco inizia con un'email camuffata da comunicazione ufficiale del governo colombiano, contenente un archivio ZIP protetto da password (meccanismo di evasion). All'apertura, uno script batch installa un VBS fortemente offuscato prelevato da un servizio di paste esterno. Questo script VBS estrae e lancia un payload nascosto dentro un file immagine via steganografia. Infine DCRat scarica e decritta un eseguibile RAT dalla rete malevola usando una chiave AES256 prefabbricata.

DCRat offre controllo remoto completo (keylogging, esfiltrazione file/credenziali, manipolazione processi), crea un compito pianificato o modifica il registro per persistere, e disabilita l'AMSI di Windows per sfuggire a scansioni antivirus.

IoC:

Tipo	Valore
URLs	• hxxps[:]//ia601205[.]us[.]archive[.]org/26/items/new_image_20250430/new_image[.]jpg • hxxps[:]//paste[.]ee/d/oAqRiS3g • hxxp[:]//paste[.]ee/d/jYHEqBJ3/0
IP Address	176[.]65[.]144[.]19
Hash Values(SHA-256)	• 77a22e30e4cc900379fd4b04c707d2dfd174858c8e1ee3f1cbecd4ece1fab3fe

MITRE ATT&CK:

- Spearphishing email (T1566) con allegati ZIP protetti.
- Esecuzione via Batch script (T1059.005) e VBScript (T1059.006) offuscato.
- Obfuscated Files or Information (T1027) usando archivi password e steganografia.
- Scheduled Task o registro modificato per persistenza (T1547.001).
- Defense Evasion disabilitando l'AMSI (T1562.001).
- Credential Access e Exfiltration di dati tramite backdoor (T1555, T1560).

Contromisure (rilevazione e mitigazione):

- Per DCRat è essenziale bloccare l'indirizzo C2 noto (176.65.144.19) e aggiornare signature IPS/IDS che rilevino il traffico VBS/PowerShell sospetto.
- Gli avvisi di Fortinet suggeriscono l'uso di soluzioni FortiMail/EDR che identificano il malware come "MSIL/Agent.CFQ!tr".
- L'uso di antivirus aggiornati e la protezione dell'interfaccia AMSI possono mitigare questo RAT.

Livello di rischio: Alto. DCRat è altamente pericoloso per via della sua complessità (più stadi di evasione) e capacità di pieno controllo remoto del sistema.

RondoDox (Linux IoT)

Descrizione tecnica: RondoDox è un botnet Linux discovery da FortiGuard che sfrutta exploit pubblici per compromissioni di dispositivi IoT (videoregistratori TBK DVR e router Four-Faith).

Colpendo i CVE-2024-3721 (TBK DVR) e CVE-2024-12856 (Four-Faith), RondoDox ottiene RCE e scarica uno script di shell malevolo. Lo script verifica diritti in directory comuni e installa payload multipiattaforma (ARM, MIPS, x86). Per nascondersi, cancella log e crea persistenza modificando file di avvio di sistema (/etc/rcS, crontab) e creando symlink di avvio ("S99rondo").

In modo distruttivo, il malware cerca e termina processi di analisi (wireshark, tcpdump) o rivali (xmrig, Redtail) e rinomina file di sistema critici (iptables, passwd, shutdown) con stringhe casuali, compromettendo la stabilità. Il malware decodifica quindi l'indirizzo del server C2 (83.150.218.93) e stabilisce una connessione continua.

Da lì può lanciare attacchi DDoS (HTTP/UDP/TCP) mascherando il traffico come servizi legittimi (p.es. pacchetti di Minecraft, Discord, OpenVPN)

IoC:

IP	File/Folder
83[.]150[.]218[.]93	iptables, passwd, shutdown (rinominati)/etc/rcS, crontab, /etc/rc3.d/S99rondo (persistenza)

MITRE ATT&CK:

- Exploitation di vulnerabilità note (T1203) per esecuzione remota di comandi Linux; esecuzione via shell script (T1059.004).
- System Binary Proxy Execution (T1569.002) rinominando eseguibili di sistema; Persistence tramite script di avvio (T1547.001).
- pulizia log (T1070.004); Impact con attacchi DDoS (T1499).
- Inoltre utilizza evasione (T1565) mascherando i propri pacchetti come traffico legittimo di giochi o VPN.

Contromisure (rilevazione e mitigazione):

- Per RondoDox si raccomanda di applicare immediatamente le patch CVE-2024-3721 e CVE-2024-12856 sui dispositivi affetti.
- Bloccare l'IP 83.150.218.93 e monitorare traffico insolito di rete (pacchetti HTTP/UDP con pattern di gaming/VPN). I
- log di sistema dovrebbero segnalare la rinomina anomala di binari critici.

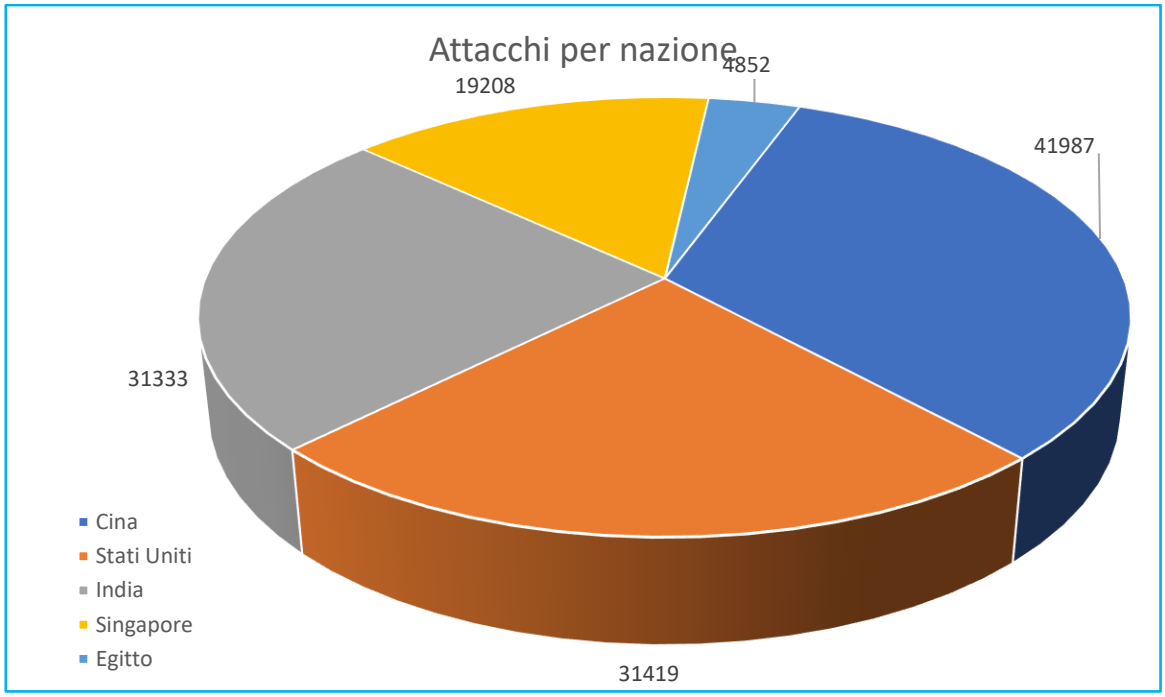
Livello di rischio: Alto. RondoDox mette a rischio l'integrità di sistemi IoT critici, combina evasione avanzata con capacità di attacco massivo (DDoS).

Tabella riepilogativa

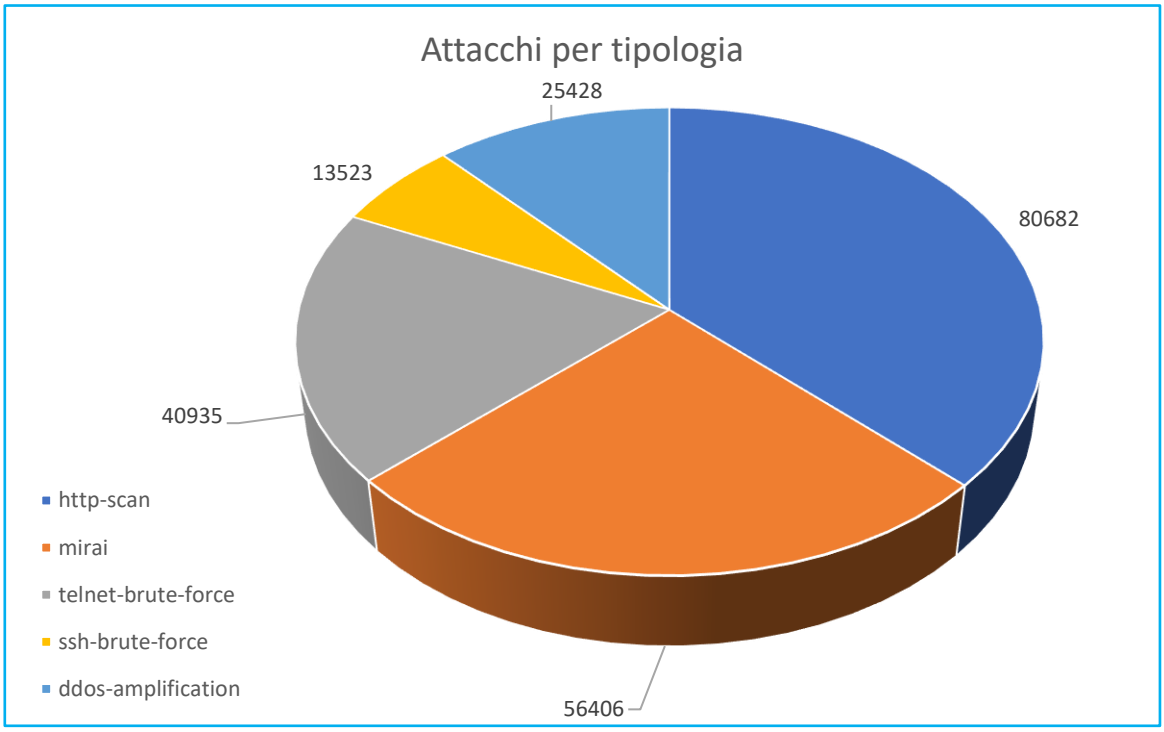
Nome Malware	Descrizione Breve	Piatta-forma	Data Scoperta Pubblica
NimDoor	Trojan per macOS distribuito via AppleScript e Web3 targeting da APT DPRK	macOS	2 luglio 2025
DCRat (nuova campagna)	RAT modulare distribuito tramite ZIP con script VBS offuscato in Colombia	Windows	5 luglio 2025
RondoDox	Botnet Linux per dispositivi IoT, usa exploit CVE e tecniche DDoS mascherate	Linux / IoT	3 luglio 2025

4.4 DDoS rilevati

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

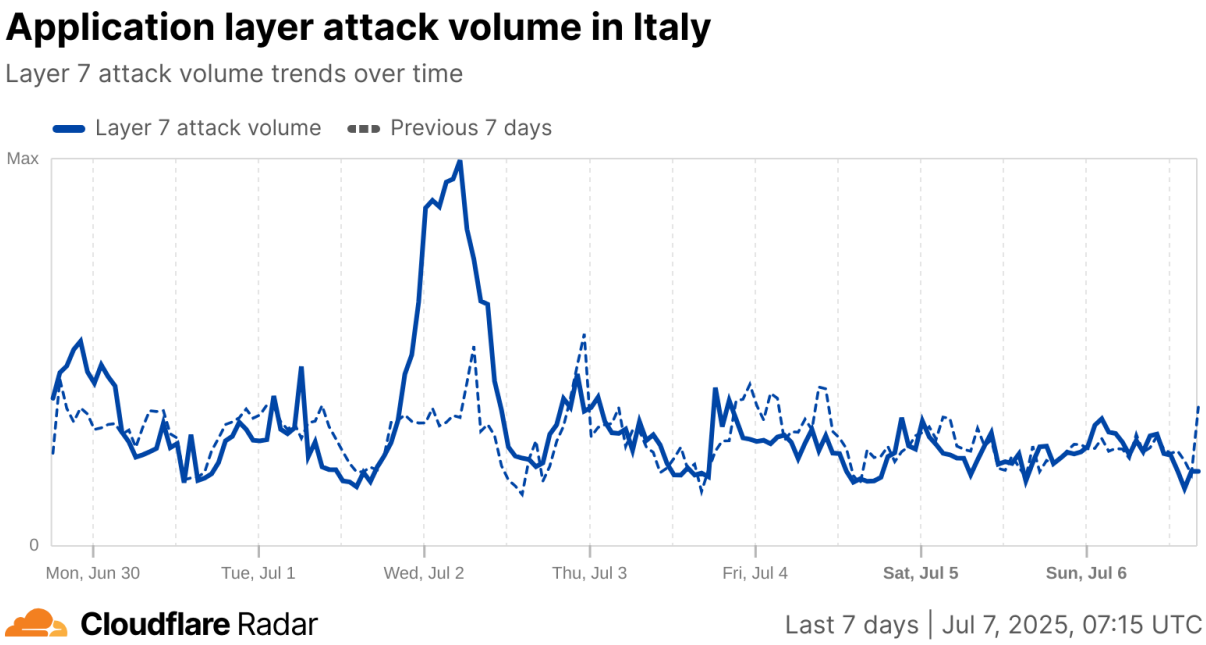


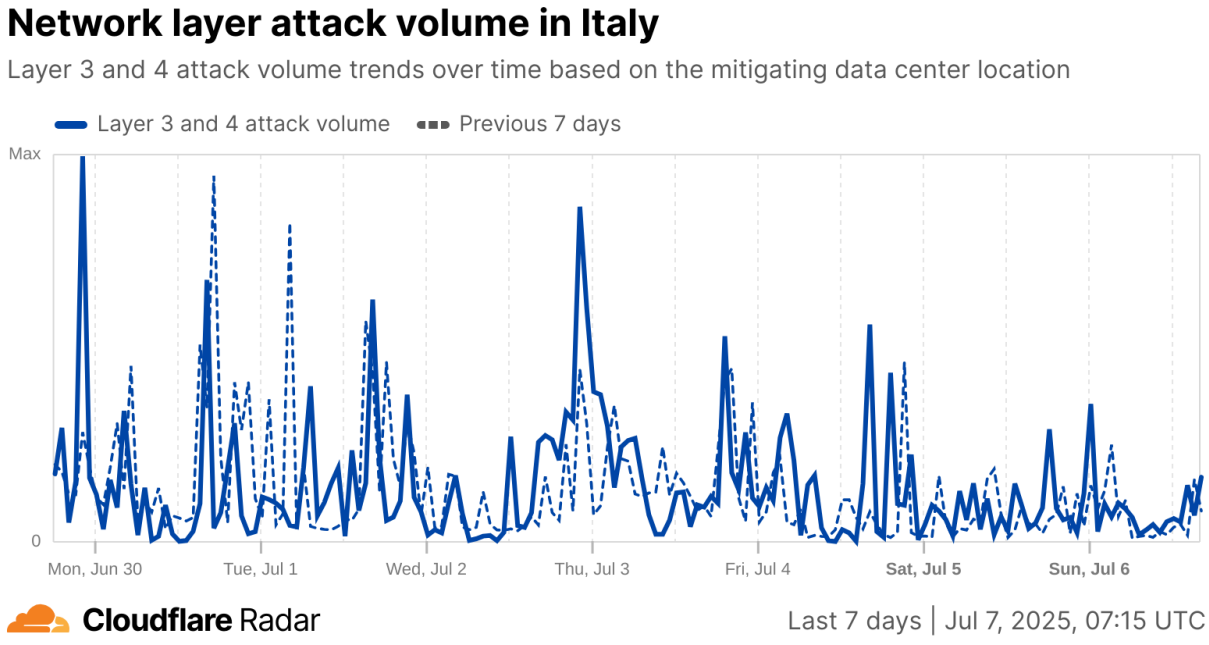
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
CORTE PENALE INTERNAZIONALE	PAESI BASSI
DESCRIZIONE	Scoperto il 30 giugno attacco alla Corte Penale Internazionale (CPI), con sede all'Aia, avvenuto tra il 23 e il 25 giugno 2025, proprio durante il vertice dei leader NATO ospitato nel vicino World Forum. Non si tratta di un episodio isolato: è il secondo attacco di simili proporzioni in pochi anni, dopo quello del 2023. Secondo le autorità della Corte, l'intrusione è stata scoperta grazie ad un sistema avanzato di allerta interna, che ha permesso di isolare l'attacco in tempi relativamente brevi. È stata avviata un'indagine forense completa per valutare eventuali danni alle infrastrutture o ai dati, ma al momento non è stata confermata la sottrazione di documenti riservati. Malgrado l'incidente non abbia interrotto le attività della Corte, permangono problemi tecnici.

TARGET	LOCALIZZAZIONE
RADIX	SVIZZERA
DESCRIZIONE	Il16 giugno 2025 la fondazione svizzera Radix, attiva nella promozione della salute e partner di vari uffici federali, è stata vittima di un attacco ransomware rivendicato dal gruppo Sarcoma. I criminali hanno esfiltrato e cifrato circa 1,3 TB di dati, includendo documenti, contratti e comunicazioni interne. Al rifiuto di pagare il riscatto, i dati sono stati pubblicati sul dark web pochi giorni fa. È emerso che tra i dati compromessi vi erano anche informazioni relative ad unità della Confederazione, anche se gli aggressori non hanno avuto accesso diretto ai sistemi governativi. È in corso un'indagine per valutare l'estensione dell'impatto.

TARGET	LOCALIZZAZIONE
INGRAM MICRO	MONDO
DESCRIZIONE	Ingram Micro, distributore globale di tecnologie IT, ha subito il 3 luglio, un attacco ransomware da parte del gruppo SafePay, che ha portato al blocco temporaneo di sistemi interni critici come Xvantage e Impulse. L'intrusione è stata facilitata con tutta probabilità da credenziali VPN compromesse (GlobalProtect), sfruttando tecniche come password spraying. In risposta, l'azienda ha immediatamente disattivato i sistemi interessati, attivato forze dell'ordine e convocato esperti di cyber-security per un'indagine forense. Il blocco delle piattaforme ha avuto un impatto globale, interrompendo ordini, consegne e operazioni per reseller, specialmente nei paesi del Medio Oriente e del Nord Africa. Nonostante non siano state segnalate violazioni di dati clienti, il danno economico potrebbe essere rilevante: fino a 136 milioni di dollari al giorno di mancati ricavi, in base ai volumi pre-attacco.

4.6 Defacement

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

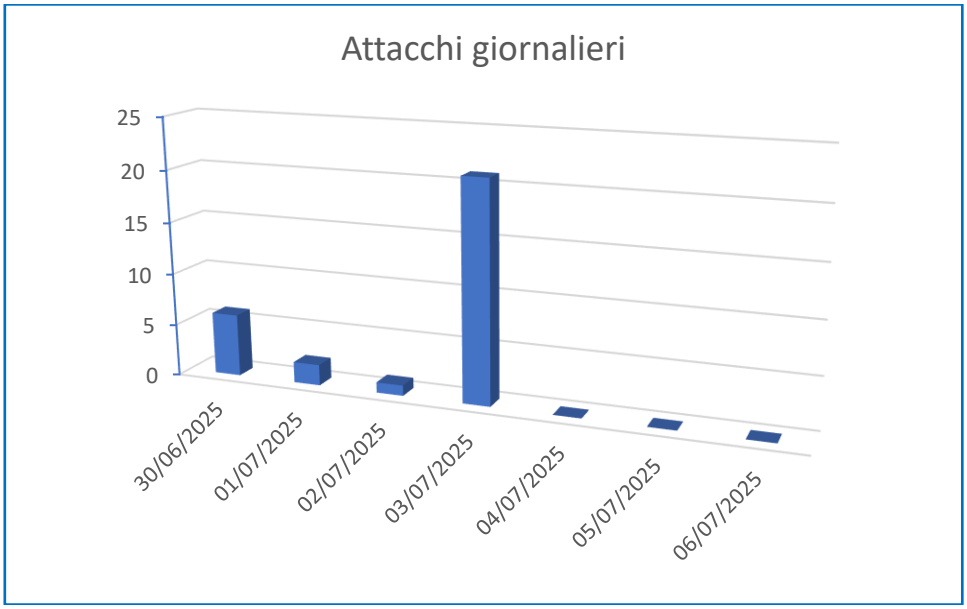


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

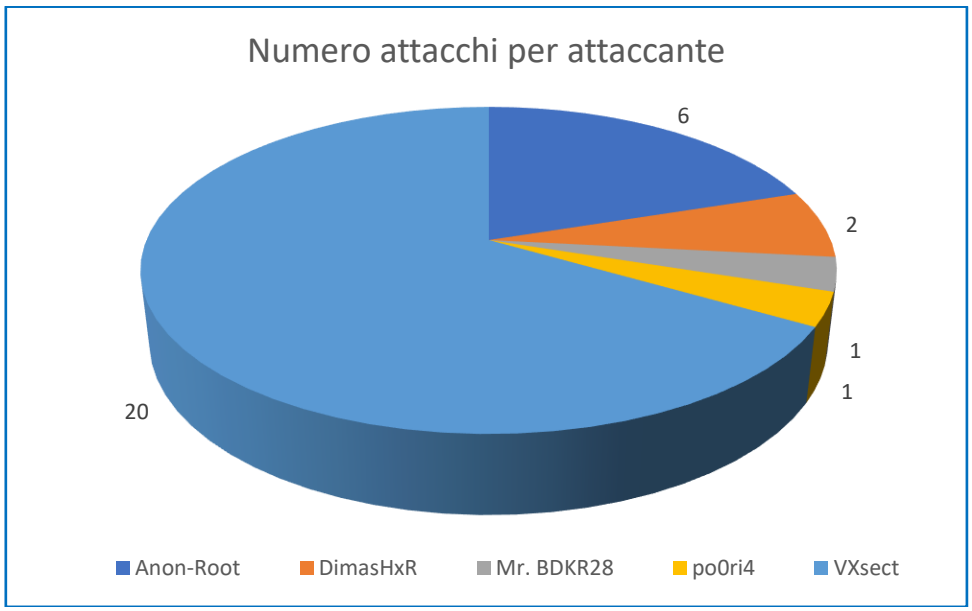


Figura 2: Defacement - Attaccanti più attivi nel periodo 30 Giugno – 6 Luglio

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

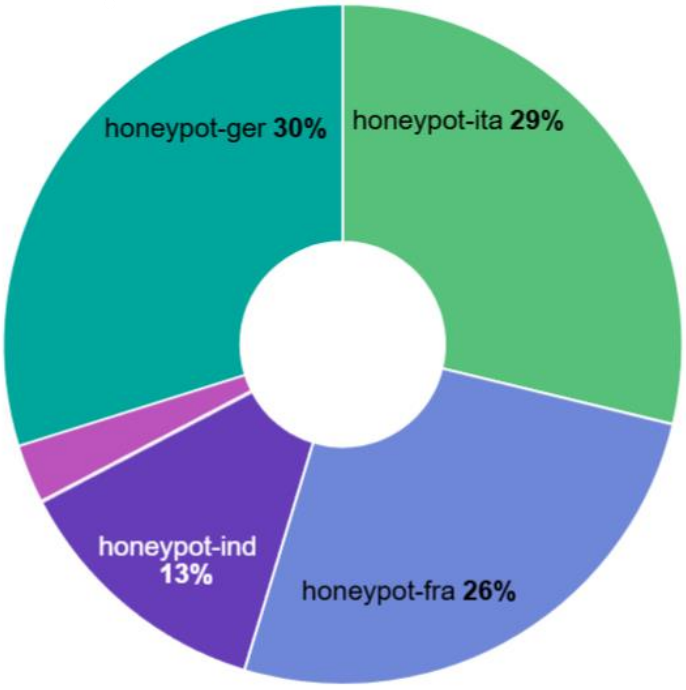
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

728.184 Attacks

8.014 Unique Src IPs

55 Unique HASSHs

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



Questa invece la situazione a livello italiano:

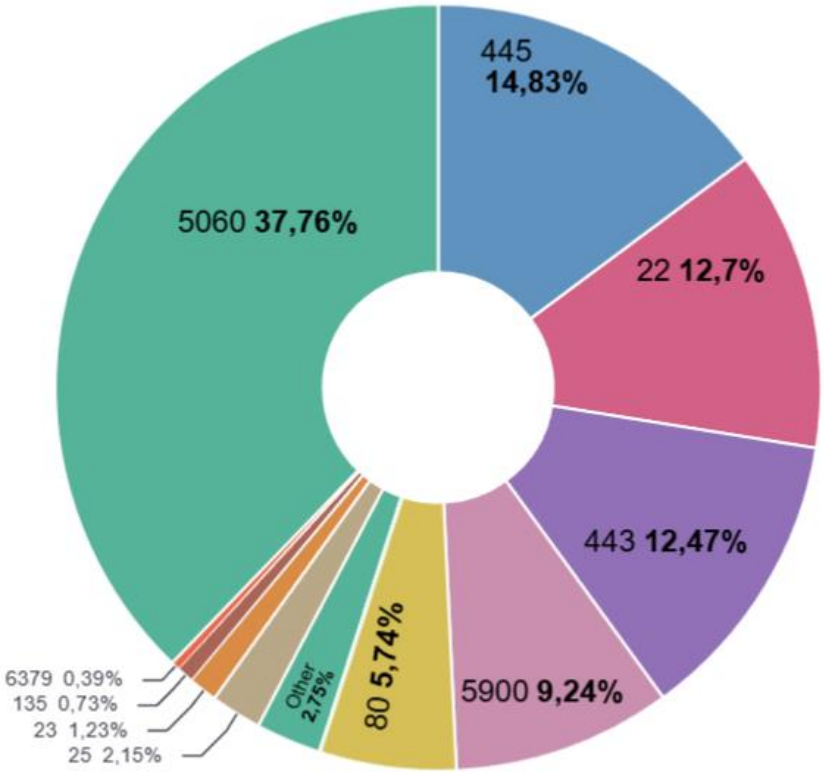
209.532 Attacks

2.712 Unique Src IPs

41 Unique HASSHs

5.1.1 Attacchi ai servizi

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



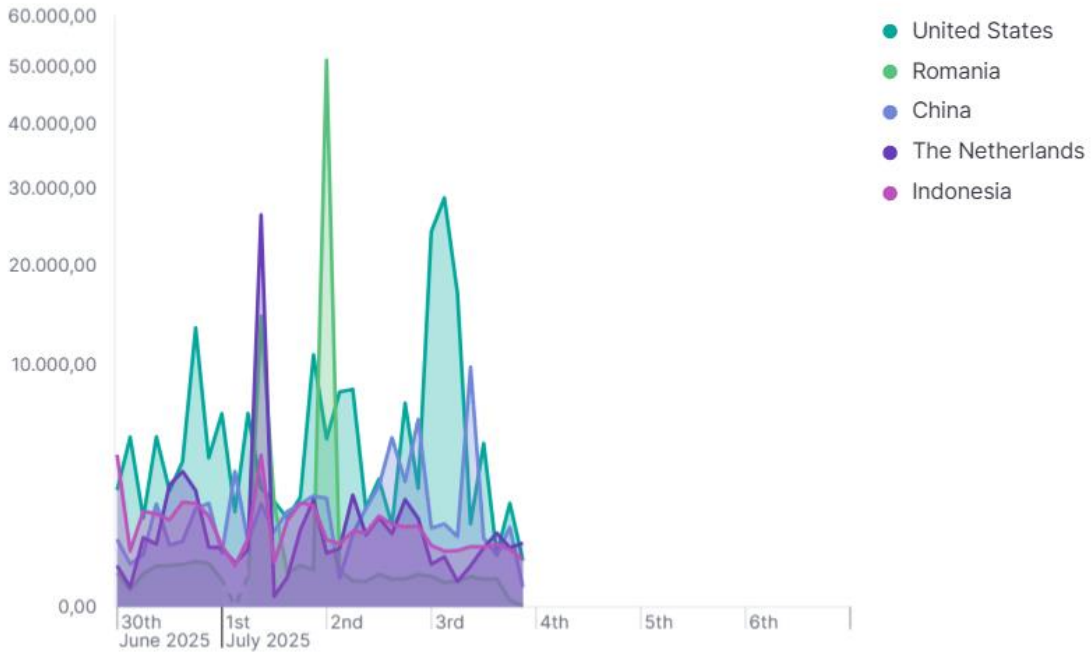
5.1.2 IP Attaccanti

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

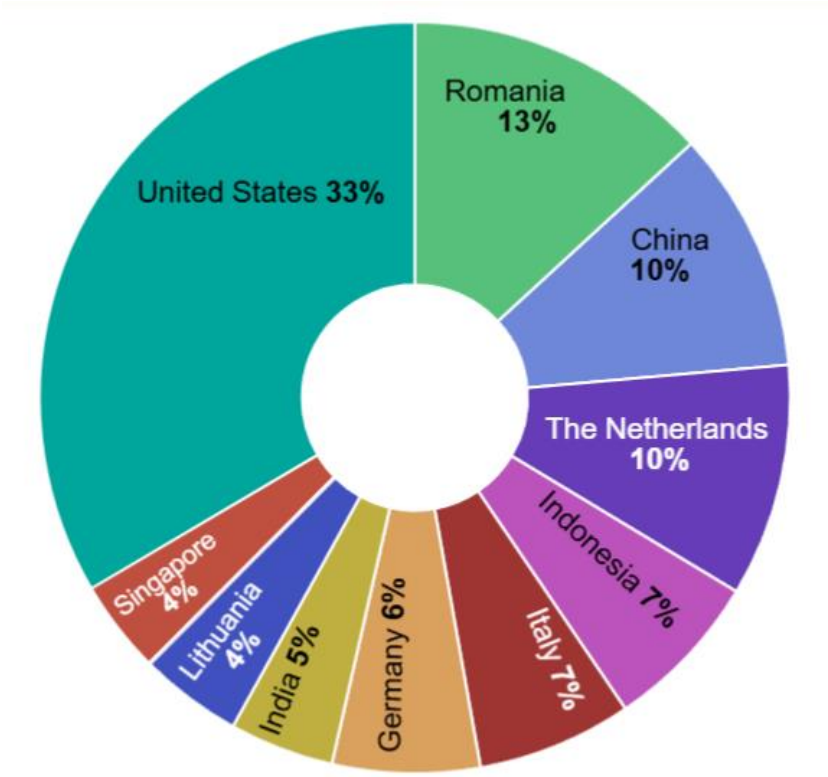
Source IP	Count
80.94.93.158	67.782
173.233.73.5	62.092
45.14.245.67	26.479
103.156.74.23	26.381
31.57.102.242	18.865
142.202.191.234	18.335
142.202.189.5	16.214
45.144.29.201	14.569
102.177.192.176	11.055
173.231.185.164	10.158

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:

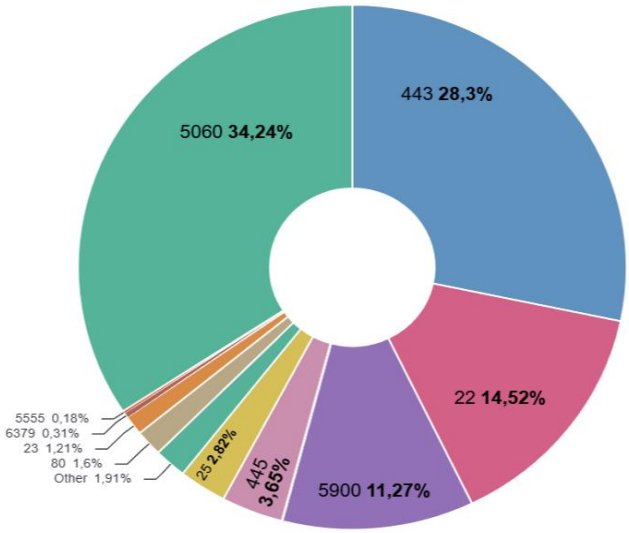


5.2 Italian Honeypot N.1

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	44.504
443	36.782
22	18.877
5900	14.649
445	4.738
25	3.671
80	2.078
23	1.569
6379	400
5555	237

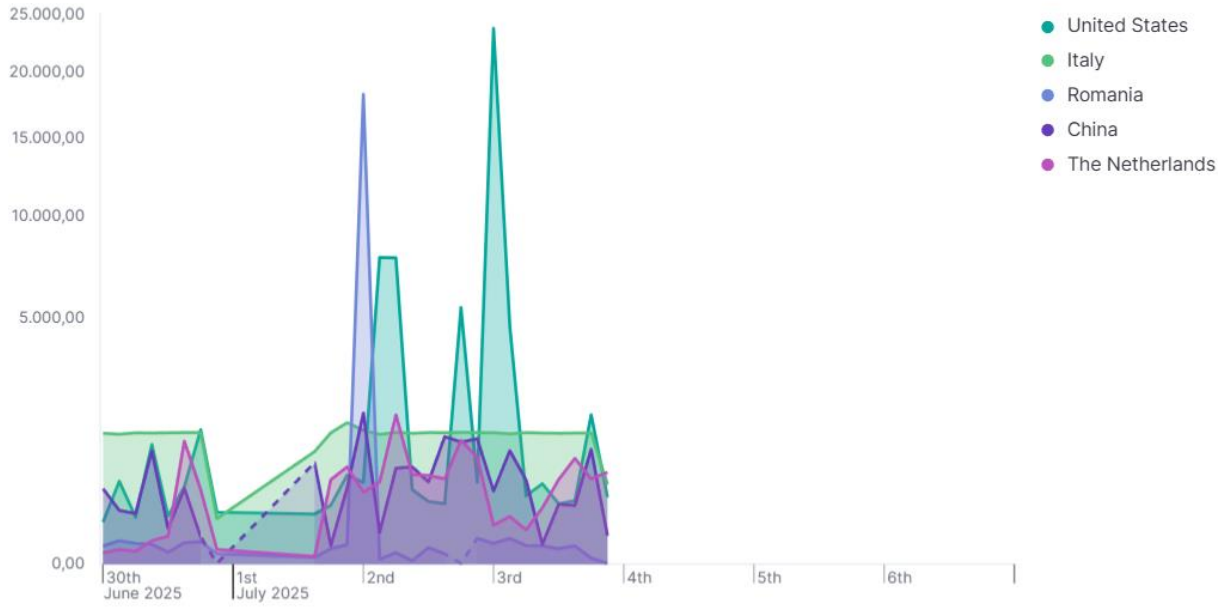
5.2.2 IP Attaccanti

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

Source IP	Count
173.233.73.5	23.436
80.94.93.158	18.295
142.202.191.234	9.098
176.65.151.53	7.797
103.156.74.23	7.556
142.202.189.5	4.813
108.174.50.72	3.880
77.90.185.6	3.464
173.231.185.164	2.822
58.57.63.214	2.216

5.2.3 Paesi di provenienza degli attacchi

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

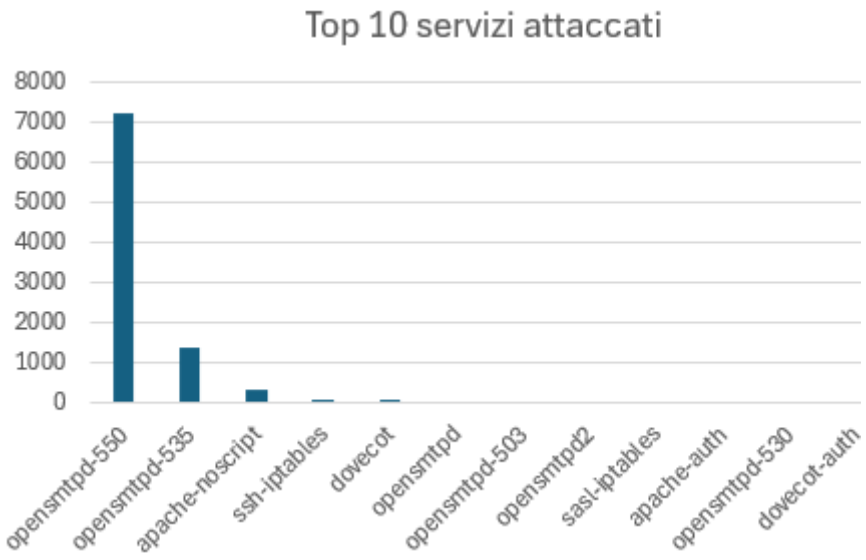


5.3 Italian Honeypot N.2

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.



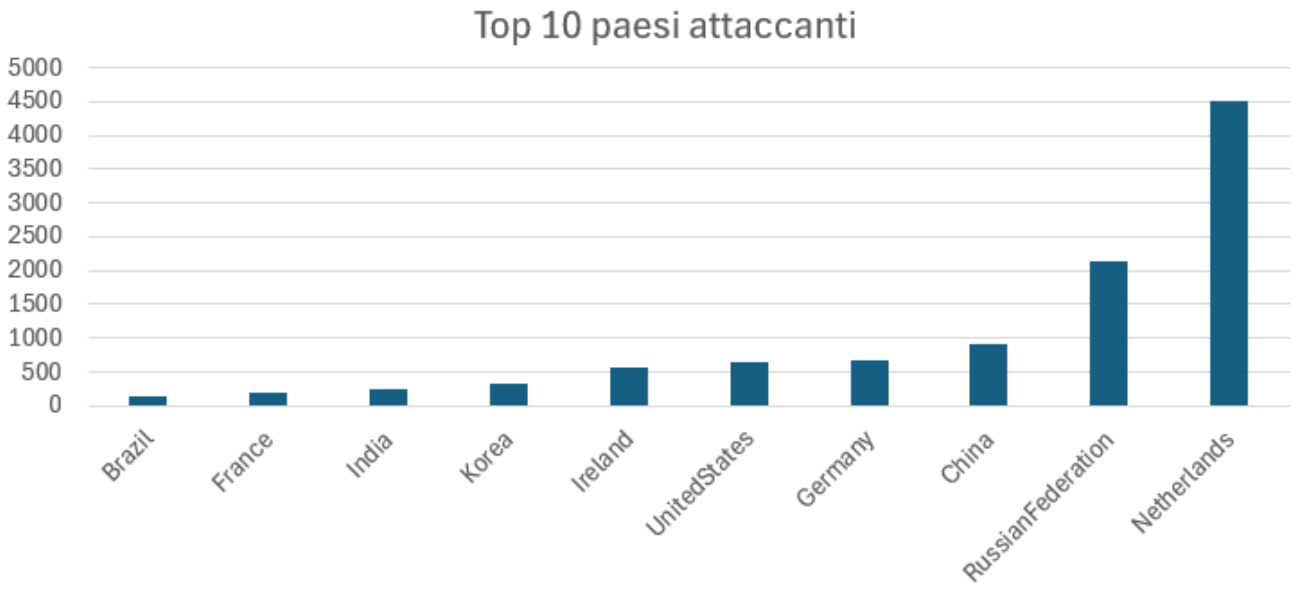
5.3.2 IP attaccanti

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
213[.]108[.]199[.]159	1910
37[.]48[.]90[.]236	1383
95[.]181[.]151[.]26	1115
37[.]48[.]120[.]235	821
62[.]173[.]145[.]115	720
195[.]54[.]33[.]154	573
62[.]212[.]95[.]133	68
5[.]79[.]97[.]121	65
62[.]173[.]141[.]189	58
37[.]48[.]90[.]229	55

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@s3k.it
insidesales@s3k.it
marketing@s3k.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:AMBER[1] = 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