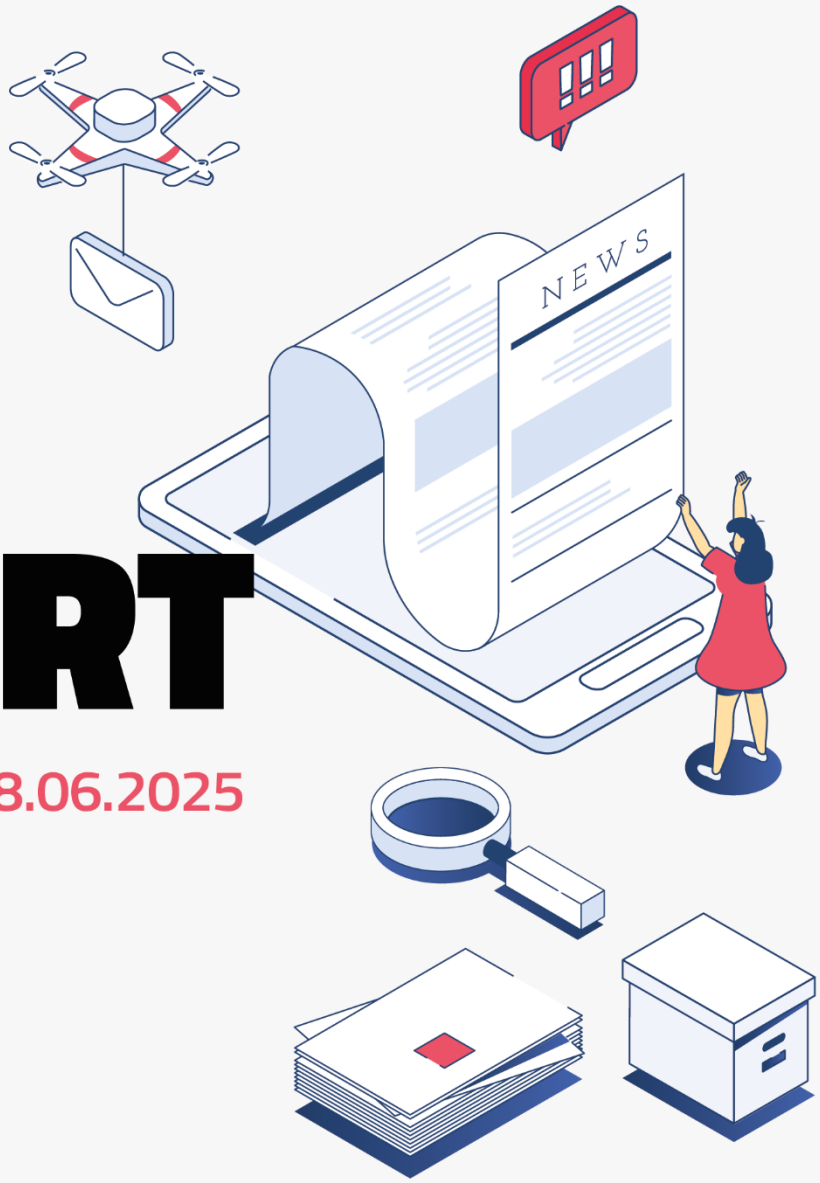
S3K

Cyber security

RISK REPORT

\ week 02.06.2025 - 08.06.2025



Sommario


CYBER SECURITY RISK REPORT
23/25

1 Il Cyber Security Risk Report S3K

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 Cosa leggerete in questo numero

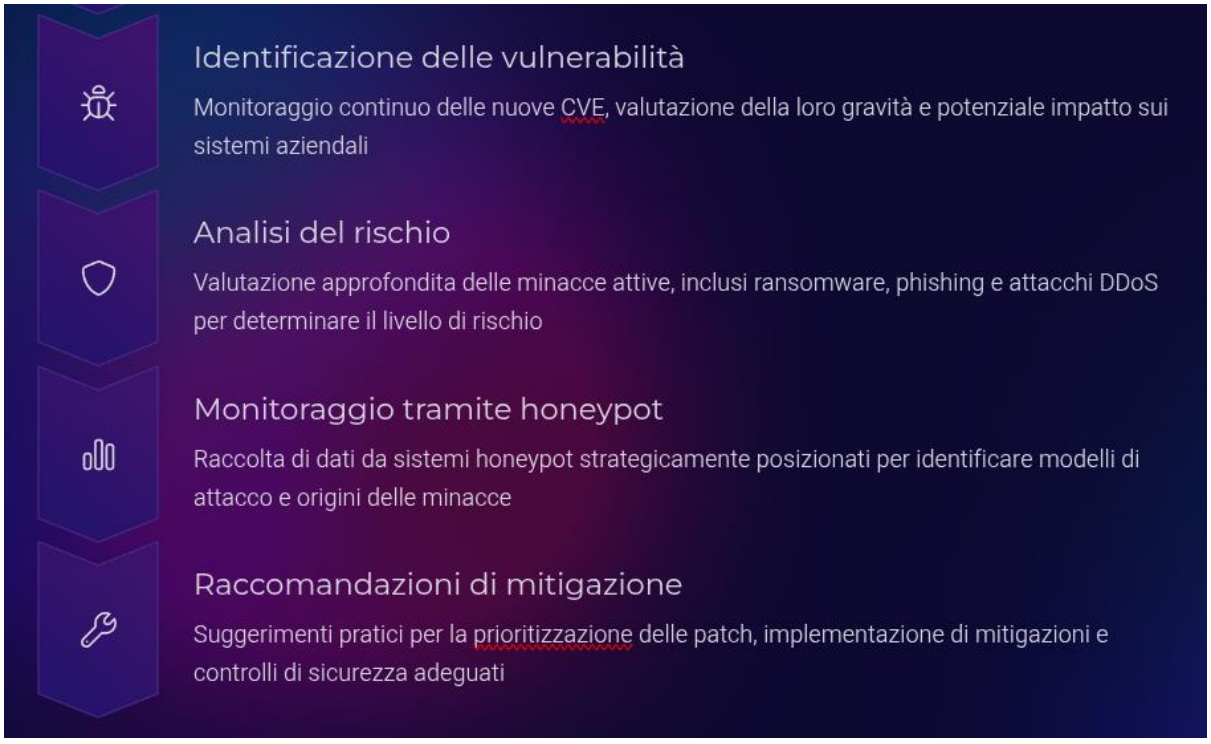
Il "Cyber Security Risk Report" di S3K rappresenta un'analisi approfondita settimanale del panorama delle minacce informatiche, offrendo alle organizzazioni informazioni essenziali per mantenersi aggiornate sulle tendenze emergenti e sulle vulnerabilità in corso. Il presente documento illustra i principali risultati del bollettino relativo alla settimana 02.06.2025 - 08.06.2025, con un'analisi dettagliata delle vulnerabilità, degli attacchi rilevati e delle tendenze significative nel panorama della sicurezza informatica globale.

1.2 Analisi delle Minacce e Vulnerabilità

Il bollettino settimanale di S3K si distingue per la sua approfondita analisi delle tendenze cyber attraverso un approccio metodico che integra dati provenienti da diverse fonti di intelligence. Gli analisti di S3K raccolgono ed esaminano informazioni da numerose fonti, tra cui produttori di hardware e software, ricercatori di sicurezza, forum specializzati, canali di comunicazione dei gruppi cybercriminali, black market, deep web e dark web.

1.3 Principali Vulnerabilità e CVE

Durante la settimana 02.06.2025 - 08.06.2025, sono state pubblicate numerose CVE ad alto impatto, con particolare attenzione ai dispositivi Cisco, Qualcomm e Splunk. Le vulnerabilità più critiche includono problemi nei sistemi Cisco UCS IMC (con possibilità di privilege escalation), problemi di validazione nelle connessioni SSH Cisco NDFC, e permessi errati nelle directory di installazione di Splunk Universal Forwarder. Inoltre, sono state identificate vulnerabilità significative nei componenti Qualcomm che possono portare a denial of service e memory corruption.
Tra le CVE di tendenza maggiormente citate sui social media troviamo vulnerabilità in prodotti FortiVoice, Grafana, Cisco Identity Services Engine e Microsoft Windows, evidenziando come le problematiche di sicurezza più discusse coinvolgano spesso sistemi ampiamente diffusi in ambito aziendale

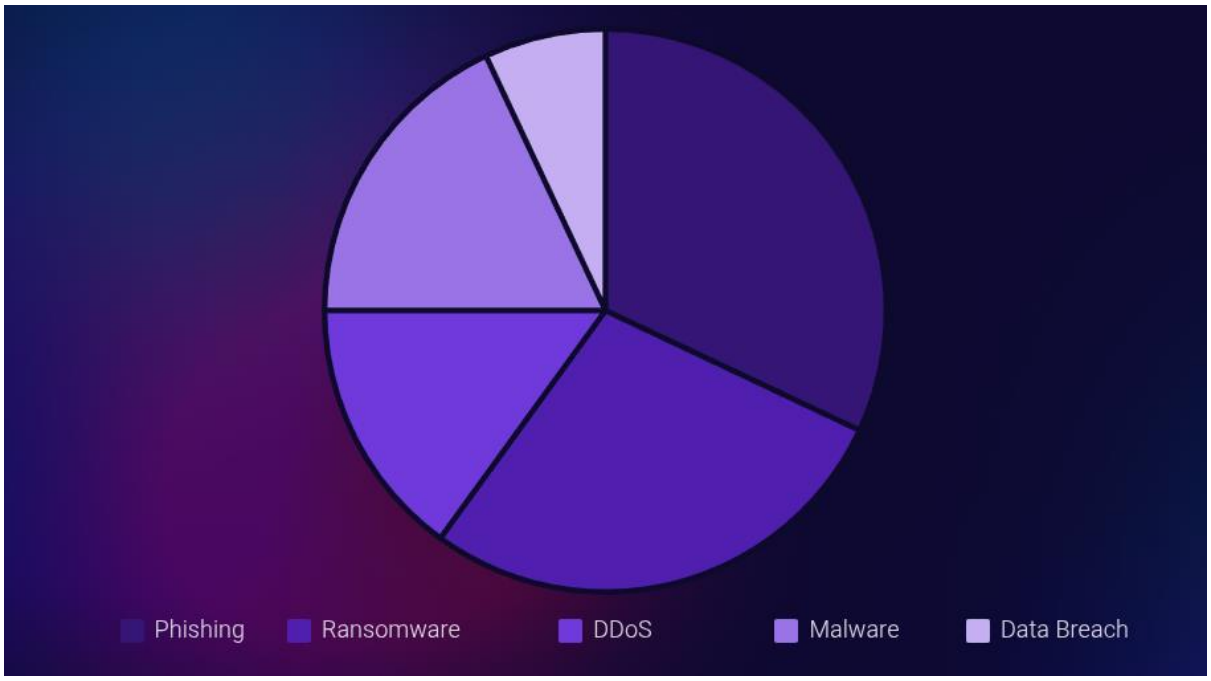


Approfondimenti al capitolo CVE Monitor

1.4 Analisi degli Attacchi

Il bollettino ha evidenziato diversi attacchi significativi durante la settimana di osservazione. Particolarmente rilevante è stata la scoperta della botnet BADBOX 2.0, che ha infettato oltre un milione di dispositivi domestici connessi a Internet, trasformandoli in proxy residenziali utilizzati per scopi illeciti. Questa botnet colpisce principalmente dispositivi Android economici prodotti in Cina e si diffonde attraverso firmware compromessi o applicazioni malevole.
Nel panorama italiano, sono stati registrati nuovi attacchi DDoS da parte del collettivo filorusso NoName057(16) contro diverse infrastrutture nazionali, tra cui trasporti, Ministero dello Sviluppo Economico, Arma dei Carabinieri e Intesa Sanpaolo. Parallelamente, è emerso un caso controverso

riguardante il collettivo GhostSec che ha accusato un'azienda italiana di aver commissionato operazioni hacker contro infrastrutture governative macedoni.
Approfondimenti nel paragrafo "Cyber News" dal Web, Deep Web e Dark Web
Le numeriche delle singole tipologie di attacco (la cui distribuzione è riassunta qui sotto) invece le trovate nel capitolo Attacchi



1.5 Monitoraggio tramite Honeypot

I dati raccolti dai sistemi honeypot di S3K, dislocati in Italia, Germania, Francia, Brasile, India e USA, hanno permesso di identificare i paesi di origine degli attacchi, i servizi più colpiti e gli indirizzi IP più attivi nelle operazioni malevole. L'analisi ha evidenziato come gli attacchi siano principalmente diretti verso i servizi SSH, HTTP e Database, con una significativa provenienza da Russia, Stati Uniti, Cina e altri paesi. I dati mostrano inoltre un aumento degli attacchi diretti verso l'Italia, con particolare attenzione ai servizi web e di connessione remota.
L'infrastruttura di monitoraggio di S3K ha rilevato numerosi tentativi di connessione malevola, con alcuni indirizzi IP responsabili di decine di migliaia di attacchi. Questa intelligence permette di identificare rapidamente le nuove minacce e di implementare contromisure efficaci per proteggere le infrastrutture critiche.
Il bollettino Cyber Security Risk Report rappresenta quindi uno strumento essenziale per i professionisti della sicurezza informatica e i responsabili IT, offrendo una panoramica completa e aggiornata delle minacce cyber più rilevanti e fornendo raccomandazioni pratiche per migliorare la postura di sicurezza delle organizzazioni in un panorama di minacce in continua evoluzione.
Approfondimenti nel capitolo Honeypot

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Acronis Cyber Protect Cloud	Acronis ha rilasciato aggiornamenti di sicurezza per sanare varie vulnerabilità, di cui una con gravità "alta", nel prodotto Acronis Cyber Protect Cloud, sistema di sicurezza e backup con funzionalità integrate anti-malware e antivirus. Versioni affette: • Acronis Cyber Protect Cloud Agent, versioni precedenti alla build 40077
ULR/Note	https://security-advisory.acronis.com/advisories/SEC-8646

PRODOTTO	DESCRIZIONE
Kea DHCP	ISC ha rilasciato aggiornamenti di sicurezza per sanare varie vulnerabilità, di cui 1 con gravità "alta", nel prodotto Kea DHCP. Versioni affette: • Kea DHCP 2.4.x, versioni precedenti alla 2.4.2 • Kea DHCP 2.6.x, versioni precedenti alla 2.6.3 • Kea DHCP 2.7.x, versioni precedenti alla 2.7.9
ULR/Note	https://kb.isc.org/docs/cve-2025-32801

PRODOTTO	DESCRIZIONE
Spring Cloud Gateway Server	Aggiornamenti di sicurezza risolvono una vulnerabilità in Spring Cloud Gateway Server, gateway API del progetto Spring Cloud. Tale vulnerabilità riguarda l'inoltro degli header "X-Forwarded-For" e "Forwarded" che potrebbero essere manipolati da utenti malintenzionati per evadere i meccanismi di protezione del sistema target. Versioni affette: • 3.1.x, versioni precedenti alla 3.1.10 • 4.0.x, versioni precedenti alla 4.0.12 • 4.1.x, versioni precedenti alla 4.1.8 • 4.2.x, versioni precedenti alla 4.2.3 • versioni 4.3.0-M1/M2/RC1 • tutte le versioni precedenti non più supportate • Spring Cloud Gateway Server MVC • 4.1.x, versione 4.1.7 • 4.2.x, versioni precedenti alla 4.2.3 • versioni 4.3.0-M1/M2/RC1 • tutte le versioni precedenti non più supportate
ULR/Note	https://spring.io/security/cve-2025-41235

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

BADBOX 2.0: LA BOTNET CHE HA INFETTATO OLTRE UN MILIONE DI DISPOSITIVI DOMESTICI CONNESSI A INTERNET

L'FBI ha segnalato che la botnet malware BADBOX 2.0 ha infettato oltre un milione di dispositivi domestici connessi ad Internet, trasformando comuni apparecchi elettronici in proxy residenziali utilizzati per scopi illeciti. Questo malware è diffuso principalmente su dispositivi Android economici prodotti in Cina, come smart TV, TV box, proiettori, tablet e altri apparecchi IoT. Secondo quanto riferito, i dispositivi arrivano spesso già compromessi oppure vengono infettati successivamente tramite aggiornamenti firmware manipolati o applicazioni Android malevole che riescono ad infiltrarsi sia su Google Play che su store di terze parti. Gli attori delle minacce possono accedere alle reti domestiche configurando i dispositivi con software dannoso prima che vengano acquistati dagli utenti oppure sfruttando applicazioni con backdoor installate durante la configurazione iniziale. Una volta che i dispositivi infetti si connettono ad Internet, entrano a far parte della botnet BADBOX 2.0 e dei relativi servizi proxy, spesso utilizzati per nascondere traffico malevolo e attività criminali. I dispositivi compromessi si collegano ai server di comando e controllo degli hacker, dai quali ricevono istruzioni da eseguire. Le attività più comuni includono il reindirizzamento del traffico di altri criminali informatici attraverso gli indirizzi IP domestici delle vittime, operazioni di frode pubblicitaria tramite il caricamento e clic automatici su annunci per generare profitti, e attacchi di credential stuffing utilizzando credenziali rubate. BADBOX 2.0 è un'evoluzione del malware BADBOX originale, scoperto nel 2023 su TV box Android a basso costo, ed ha continuato ad espandersi globalmente fino al 2024, quando le autorità tedesche sono riuscite a bloccare temporaneamente la comunicazione tra i dispositivi infetti e l'infrastruttura degli aggressori. Tuttavia, il malware è riapparso poco dopo su 192.000 dispositivi, inclusi modelli di marchi noti come Yandex e Hisense. HUMAN Satori Threat Intelligence ha confermato che a marzo 2025, oltre un milione di dispositivi risultavano infettati. La nuova variante BADBOX 2.0 colpisce soprattutto dispositivi basati su Android Open Source Project (AOSP), non certificati da Google Play Protect, prodotti in Cina e distribuiti in tutto il mondo. Il traffico legato alla botnet è stato rilevato in 222 paesi e territori, con le maggiori concentrazioni in Brasile, Stati Uniti, Messico e Argentina. In seguito ad un'operazione congiunta tra HUMAN, Google, Trend Micro, The Shadowserver Foundation e altri partner, è stata interrotta la comunicazione tra oltre 500.000 dispositivi e i server degli aggressori, ma la botnet continua comunque a crescere poiché nuovi dispositivi compromessi vengono continuamente messi in commercio. I segnali di un'infezione includono la presenza di marketplace di app sconosciuti, la disattivazione delle impostazioni di sicurezza di Google Play Protect, dispositivi promossi come sbloccati o in grado di accedere a contenuti gratuiti, marchi non ufficiali e traffico Internet sospetto. L'FBI raccomanda ai consumatori di controllare regolarmente i propri dispositivi IoT, evitare l'installazione di app da fonti non affidabili, monitorare il traffico di rete, installare tempestivamente gli aggiornamenti di sicurezza e, in caso di sospetta infezione, isolare immediatamente il dispositivo dalla rete per interrompere la comunicazione con il malware.

NONAME057(16), NUOVI ATTACCHI DDOS IN ITALIA MENTRE TELEGRAM OSTACOLA LA PROPAGANDA

Nuovi attacchi pochi giorni fa da parte del collettivo filorusso di hacktivisti NoName057(16) contro diversi obiettivi italiani. Parallelamente, Telegram ha intensificato le misure contro i gruppi hacker vicini alla Russia, tra cui proprio NoName057(16), rimuovendo sistematicamente i canali utilizzati da questi attori per coordinare le operazioni, diffondere propaganda e rivendicare gli attacchi. Questa strategia sta mettendo in seria difficoltà i gruppi colpiti, costretti a ricreare continuamente nuovi canali e a ricostruire da zero la propria base di follower, riducendo così la visibilità e la capacità di amplificazione dei loro messaggi. Sul loro nuovo canale Telegram, gli hacktivisti hanno rivendicato l'interruzione di servizi e siti italiani, accompagnando il messaggio "The resistance is almost zero. Minus a few more Italian sites" con i collegamenti a report di check-host che documenterebbero la temporanea indisponibilità di alcuni obiettivi, tra cui infrastrutture legate ai trasporti, al Ministero dello Sviluppo Economico, all'Arma dei Carabinieri e alla banca Intesa Sanpaolo. Sebbene i report riportino la dicitura "dead in ping", resta da verificare l'effettivo impatto operativo degli attacchi. NoName057(16), che ha dichiarato il proprio supporto alla Federazione Russa nel marzo 2022, è noto per aver colpito con attacchi informatici diversi Paesi europei, l'Ucraina e gli Stati Uniti, prendendo di mira principalmente siti governativi, media e aziende private. L'attività di contrasto di Telegram, che agisce come ostacolo alla continuità operativa e comunicativa di questi gruppi, si sta rivelando un elemento cruciale per ridurre la portata e l'impatto delle loro azioni nel panorama delle minacce cibernetiche.

GHOSTSEC ACCUSA AZIENDA ITALIANA: OPERAZIONI HACKER SU OBIETTIVI GOVERNATIVI E RIVALITÀ COMMERCIALI

Il collettivo di hacktivisti GhostSec ha recentemente rivelato dettagli su un'operazione delicata e controversa che coinvolgerebbe un'azienda italiana e obiettivi governativi in Macedonia del Nord. In un'intervista, il fondatore del gruppo, Sebastian Dante Alexander, ha raccontato che GhostSec sarebbe stato contattato da una società italiana ufficialmente privata ma, a detta del gruppo, presumibilmente collegata ai servizi di intelligence del nostro Paese. L'azienda avrebbe incaricato il collettivo di eseguire operazioni offensive contro infrastrutture governative macedoni. Dopo una prima fase operativa, la stessa società avrebbe poi chiesto a GhostSec di colpire anche un soggetto in Sardegna, descritto come una società concorrente. I contatti tra le parti si sarebbero svolti attraverso canali criptati, e l'ingaggio diretto dell'azienda verso il gruppo hacker ha suscitato particolare attenzione. Tuttavia, dopo l'esecuzione degli attacchi, l'azienda italiana avrebbe interrotto ogni comunicazione e non avrebbe corrisposto il compenso pattuito. In risposta, GhostSec ha minacciato di pubblicare le conversazioni e i dettagli delle operazioni come forma di pressione, affermando che tale divulgazione non solo creerebbe imbarazzo per l'azienda coinvolta, ma potrebbe anche causare problemi diplomatici con il governo della Macedonia del Nord. Nonostante le evidenti implicazioni legali, Alexander ha dichiarato che GhostSec è pronto a rendere pubbliche le prove, a meno che non si giunga ad un accordo con la controparte. Questo episodio apre interrogativi seri sull'etica dell'hacktivismo e sulla crescente commistione tra gruppi di hacker e soggetti privati che operano al confine con l'intelligence. Il fatto che una società possa, con relativa facilità, commissionare un attacco informatico contro un ente statale straniero evidenzia la complessità di regolamentare un cyberspazio dove anonimato, denaro e tecnologia si incontrano in assenza di controlli strutturati. Il caso, che resta al momento basato solo sulle dichiarazioni di GhostSec, solleva dubbi anche sulla veridicità del racconto, dato che non sono stati forniti elementi verificabili né prove concrete, e le parti coinvolte restano nell'ombra. Ciò nonostante, anche solo la minaccia di pubblicazione genera un impatto tangibile: aumenta la pressione su aziende ed istituzioni, accentua l'allerta dei governi e mostra come l'hacktivismo, una volta mosso da motivazioni idealistiche, possa oggi diventare strumento di contrattazione, pressione o addirittura vendetta.

NUOVA CAMPAGNA DI PHISHING CONTRO UTENTI LIBEROMAIL CON FINTE FATTURE PER RUBARE CREDENZIALI

Negli ultimi giorni si è diffusa una nuova campagna di phishing ai danni degli utenti di LiberoMail, che sfrutta il pretesto di una finta fattura da pagare per sottrarre credenziali d'accesso alla casella email. Il messaggio, ben scritto in italiano e con l'apparenza di una conversazione preesistente, invita a scaricare un file PDF protetto tramite un link che rimanda ad una pagina clone del sito di Libero. Qui la vittima, convinta della legittimità della comunicazione, inserisce i propri dati di accesso che finiscono così nelle mani dei truffatori. I cybercriminali, una volta ottenuto l'accesso, possono leggere e inviare email a nome dell'utente, intercettare dati sensibili e portare avanti ulteriori attacchi. Questo tipo di truffa è particolarmente subdolo perché fa leva sul senso di urgenza e sull'aspetto apparentemente autentico del messaggio, rendendo difficile distinguere la truffa da una comunicazione legittima. Per difendersi è fondamentale prestare attenzione ad alcuni dettagli: controllare sempre il vero indirizzo del mittente, evitare di cliccare su link sospetti, non aprire allegati se non si è certi della provenienza, e soprattutto non inserire le credenziali in pagine web raggiunte da link ricevuti via email. È anche raccomandato utilizzare password robuste, attivare l'autenticazione a due fattori se disponibile, e dotarsi di sistemi antiphishing aggiornati. In caso di dubbio, è bene segnalare il messaggio come spam e cancellarlo subito, oltre a cambiare immediatamente la password se si sospetta di essere stati tratti in inganno. La prudenza resta l'arma più efficace: prendersi qualche secondo per verificare può fare la differenza tra sicurezza e compromissione.

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 2 - 8 Giugno 2025

Durante questa settimana sono state pubblicate numerose CVE ad alto impatto, con particolare enfasi su dispositivi Cisco, Qualcomm e Splunk, spesso con accesso remoto o privilege escalation. Non risultano exploit pubblici confermati fino ad ora, ma la severità complessiva resta elevata.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Descrizione Sintetica
CVE-2025-20261	HIGH	4/06/2025	❌	Cisco UCS IMC – SSH crafted syntax → privilege escalation e creazione admin.
CVE-2025-20163	HIGH	4/06/2025	❌	Cisco NDFC – MITM SSH via validazione errata host key.
CVE-2025-20163	HIGH	2/06/2025	❌	Splunk Universal Forwarder – permessi errati su directory installazione.
CVE-2025-20163	HIGH	3/06/2025	❌	Qualcomm – Denial of Service tramite beacon EHT malformato.
CVE-2025-20163	HIGH	3/06/2025	❌	Qualcomm – memory corruption GPU micronode via comandi non autorizzati.

CVE-2025-20163	HIGH	3/06/2025	❌	Qualcomm – memory corruption da sequenze comandi GPU non valide.
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

- **Cisco UCS / NDFC:** vulnerabilità su connessioni SSH con possibilità di privilege escalation e MITM.
- **Splunk Universal Forwarder (Windows):** permessi di file system errati post-installazione.
- **Qualcomm (firmware):** multiple vulnerabilità su chip FastConnect, Snapdragon e GPU con potenziali impatti su device Android/IoT.

Distribuzione Giornaliera

- **2 giugno:** Advisory Splunk.
- **3 giugno:** Disclosure Qualcomm (DoS + memory corruption).
- **4 giugno: Cisco:** NDFC + UCS IMC advisory SSH privilege escalation.

Raccomandazioni

- **Patch Prioritarie:**
  - Sistemi di gestione Cisco UCS / NDFC in ambienti enterprise.
  - Aggiornamento Splunk UF su ambienti Windows → hardening ACL.
  - Aggiornamento firmware Qualcomm in dispositivi mobili, automotive, embedded.
- **Mitigazioni:**
  - Limitare l'accesso SSH alle interfacce di gestione.
  - Abilitare logging per accessi non autorizzati e controlli di integrità su file system post-installazione.
- **Monitoraggio:**
  - Verifica dispositivi Qualcomm vulnerabili (Snapdragon, GPU Micronode).
  - Nessun exploit pubblico noto al momento, ma alta attenzione lato firmware e gestione remota.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-32756	FortiVoice, FortiRecorder, FortiMail, FortiNDR, FortiCamera	N/A
CVE-2025-4123	Grafana	N/A
CVE-2025-20286	Cisco Identity Services Engine (ISE)	N/A
CVE-2025-49113	Roundcube Webmail	N/A
CVE-2025-29824	Microsoft Windows (Common Log File System Driver - CLFS)	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-2025-5893	Smart Parking Management System di Honding Technology	N/A
VULNERABILITÀ	Il Sistema di Gestione del Parcheggio Intelligente (Smart Parking Management System) di Honding Technology presenta una vulnerabilità di tipo esposizione di informazioni sensibili. Questa vulnerabilità consente a un attaccante remoto non autenticato di accedere a una pagina specifica e ottenere le credenziali dell'amministratore in chiaro (plaintext).	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-5620 CVE-2025-5621	D-Link DIR-816	9.8
VULNERABILITÀ	Due vulnerabilità critiche (CVE-2025-5620 e CVE-2025-5621) colpiscono il router D-Link DIR-816 nella versione firmware 1.10CNB05. Entrambe permettono a un attaccante remoto di eseguire comandi arbitrari sul dispositivo attraverso funzionalità esposte nel pannello di gestione web (/goform/qosClassifier e /goform/setipsec_config) sfruttando parametri non sanitizzati. Le vulnerabilità sono sfruttabili senza autenticazione e sono già noti exploit pubblici. Poiché il prodotto non è più supportato, si consiglia fortemente la rimozione o la sostituzione del dispositivo.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-5582	CodeAstro Real Estate Management System (sistema di gestione immobiliare)	9.8
VULNERABILITÀ	Il problema riguarda l'elaborazione non specificata del file: /profile.php La manipolazione del parametro content può portare a una SQL Injection, permettendo a un attaccante remoto di eseguire comandi SQL arbitrari sul database. L'exploit è già stato divulgato pubblicamente e potrebbe essere utilizzato attivamente.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-47966	Microsoft Power Automate	N/A
VULNERABILITÀ	Un attaccante non autorizzato può sfruttare un problema di esposizione di informazioni sensibili per ottenere un aumento dei privilegi sulla rete. In pratica, l'attaccante può accedere a dati riservati o informazioni di sistema non destinate a lui, e questo può consentirgli di ampliare il proprio livello di accesso, potenzialmente compromettendo ulteriori risorse o sistemi collegati.	

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-2025-5419
DESCRIZIONE	
La vulnerabilità CVE-2025-5419 è una lettura e scrittura fuori dai limiti (out-of-bounds read and write) nel motore JavaScript V8 di Google Chrome. Questa problematica consente a un attaccante remoto di potenzialmente sfruttare una corruzione dell'heap tramite una pagina HTML appositamente progettata. La corruzione dell'heap può portare a esecuzione di codice arbitrario, crash del browser o compromissione del sistema. La vulnerabilità è stata classificata con una severità alta dal team di sicurezza di Chromium.	

CVE	CVE-2025-27038
DESCRIZIONE	
La vulnerabilità CVE-2025-27038 riguarda una corruzione di memoria nel processo di rendering grafico utilizzando i driver Adreno GPU integrati in Google Chrome. Questo problema si verifica durante l'elaborazione dei contenuti grafici, e può essere sfruttato da un attaccante remoto tramite una pagina web appositamente manipolata. La corruzione di memoria causata da questa falla può portare a diversi esiti negativi, tra cui il crash del browser, la corruzione dei dati o, in scenari più gravi, l'esecuzione di codice arbitrario con i privilegi associati al processo di Chrome. Tali implicazioni rappresentano un rischio significativo per la sicurezza degli utenti, in particolare su dispositivi mobili e sistemi che utilizzano driver Adreno, tipicamente associati a chip Qualcomm.	

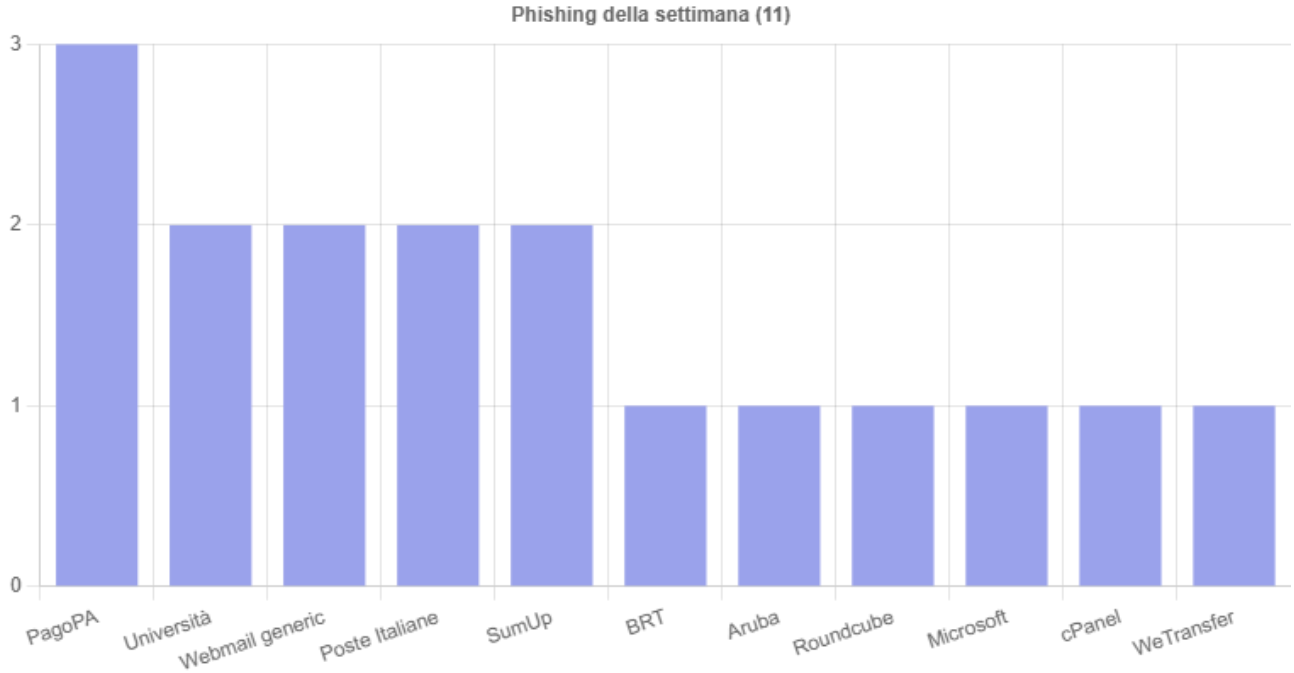
CVE	CVE-2025-21480
DESCRIZIONE	
La vulnerabilità CVE-2025-21480 riguarda una corruzione di memoria nel micronodo GPU di diversi chipset Qualcomm. Questa problematica si verifica durante l'esecuzione di una sequenza specifica di comandi non autorizzati, che può compromettere la stabilità del sistema e, in scenari avanzati, consentire l'esecuzione di codice arbitrario.	

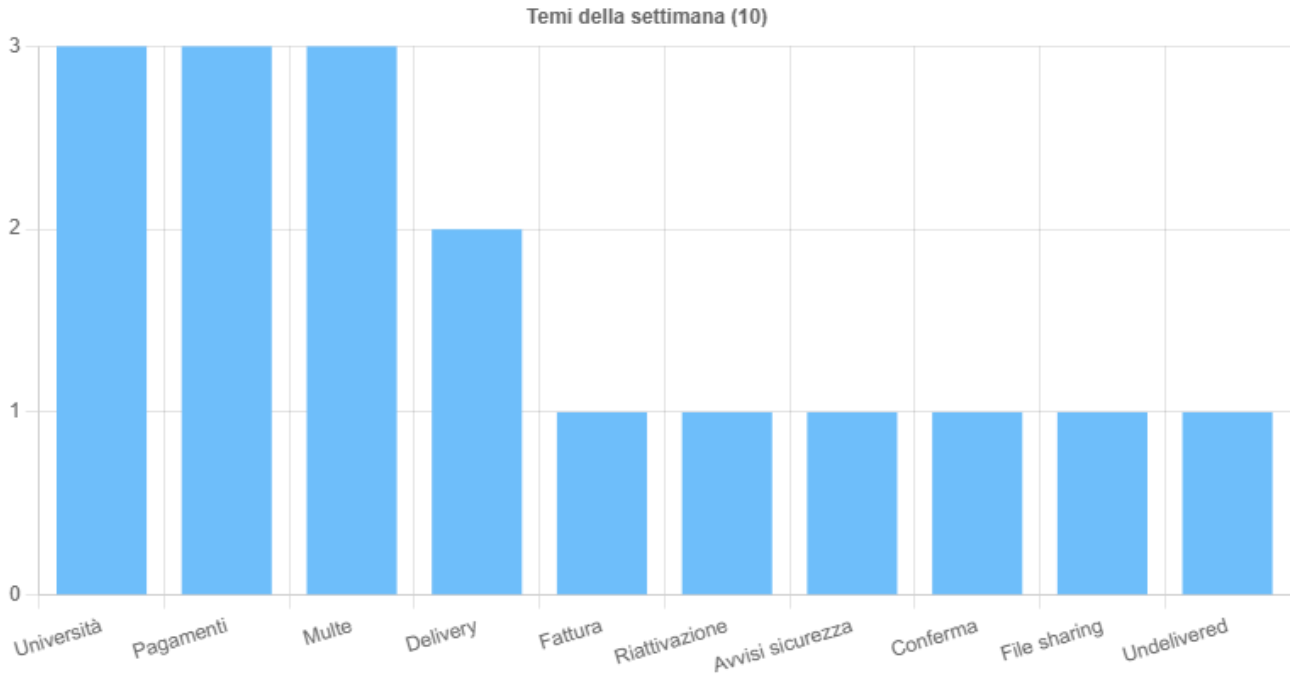
4 Attacchi

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.

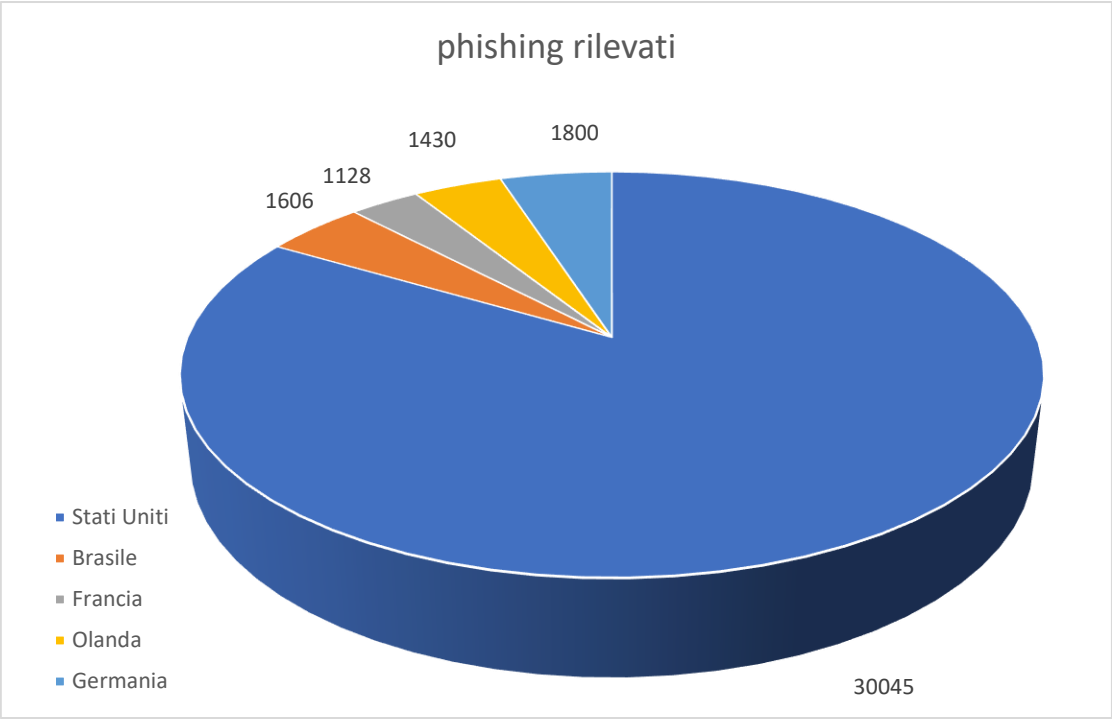




Fonte :CERT-AGID

Situazione Mondiale:

Nella seguente tabella troviamo una classifica dei primi cinque posti per Paese di provenienza, per quanto riguarda il numero di email rilevate come attacchi di phishing sui sistemi honeypot.



Come di consueto analizziamo una mail raccolta dalla redazione che può essere catalogata come "phishing":

Report di Analisi Email di Phishing

- Data: 7 Giugno 2025
- Destinatario: victim@victim[.]com
- Mittente dichiarato: kyc@binance[.]com
- Dominio mittente: ahflzjs[.]com
- Indirizzo IP mittente: 117[.]86[.]185[.]235

Premessa

Questo documento analizza un'email ricevuta con oggetto:

- '[Binance] Account Update Required: Link your external wallet and protect your assets'.

L'obiettivo è verificare la natura malevola del messaggio e identificare Indicatori di Compromissione (IoC) e tecniche di phishing.

Analisi Header Email

L'email risulta inviata da un dominio non associato ufficialmente a Binance. L'indirizzo IP di origine è 117[.]86[.]185[.]235, localizzato in Cina, ASN China Unicom. L'infrastruttura non presenta record SPF, DKIM o DMARC validi per garantire l'autenticità dell'invio.

- **Mittente dichiarato:** kyc@binance[.]com
- **IP mittente effettivo:** 117[.]86[.]185[.]235
- **Hostname dichiarato:** ahflzjs[.]com
- **Client di invio dichiarato:** Microsoft Outlook Express 6.00.2900.5512

Osservazioni:

- Non vi è alcun riferimento nei record SPF, DKIM o DMARC nei log forniti. Questo è **altamente sospetto** per una comunicazione ufficiale da parte di Binance.
- Il dominio *ahflzjs[.]com* non è collegato a *binance[.]com*.
- Received: from ahflzjs[.]com (<unknown> [117[.]86[.]185[.]235])

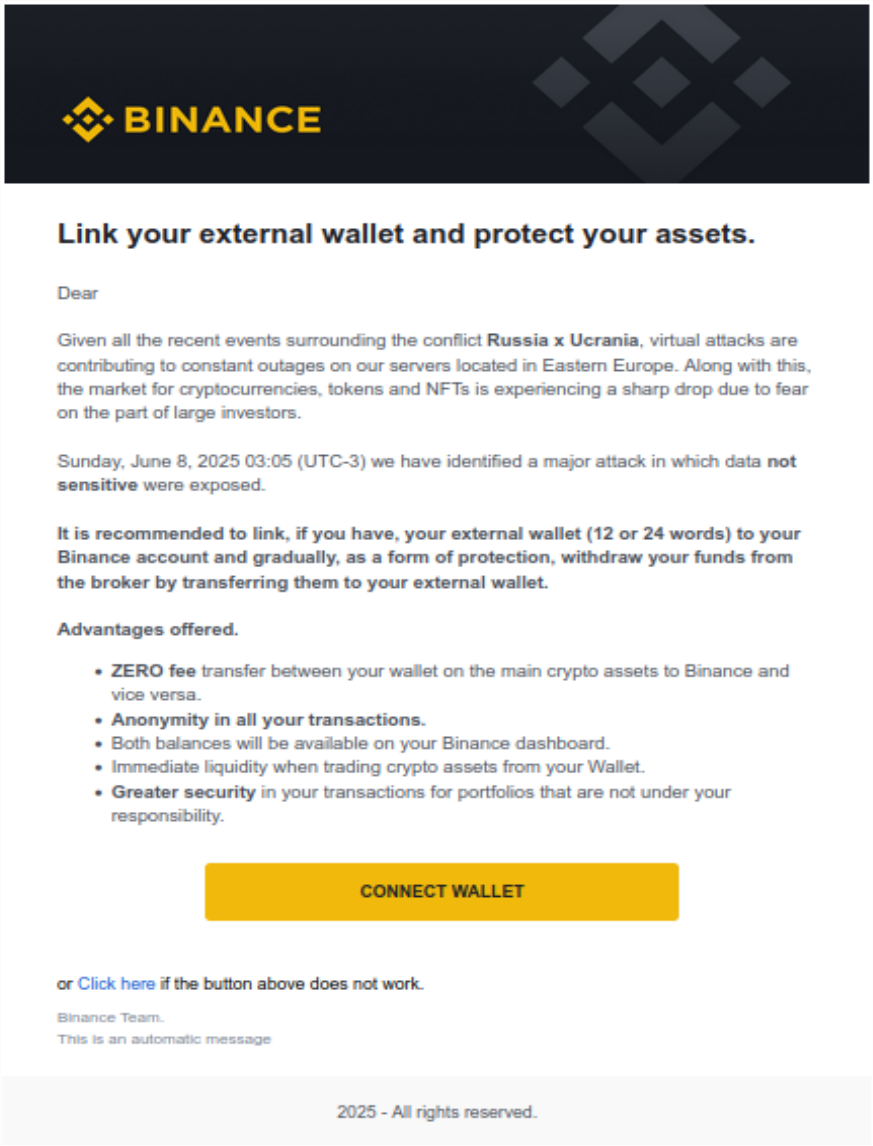
Analisi Infrastruttura

- Dominio mittente: ahflzjs[.]com
- IP mittente: 117[.]86[.]185[.]235

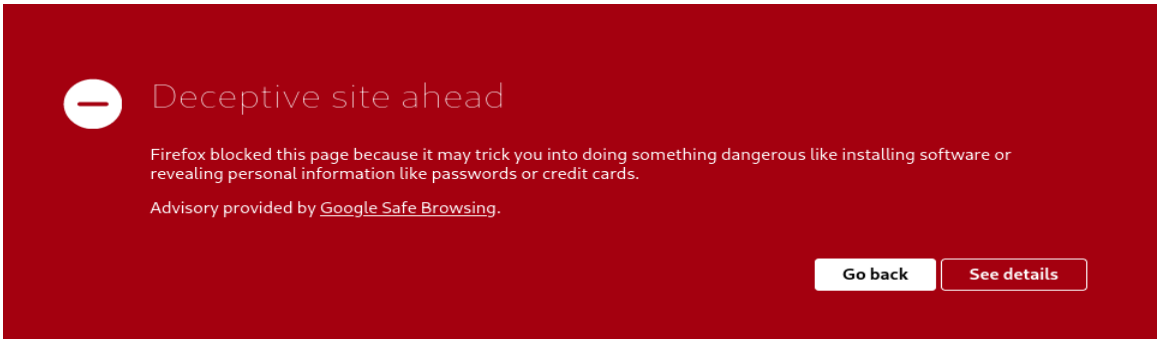
Il dominio ahflzjs[.]com non risulta essere stato registrato. L'indirizzo IP è presente su VirusTotal con diverse segnalazioni per attività di spam e phishing.

Screenshot Email

L'immagine seguente mostra l'email ricevuta. L'immagine con il logo di Binance è caricato da un link account su Google che prende l'immagine da imgur[.]com.



L'immagine seguente mostra l'avviso di Firefox relativa alla URL presente nella email:

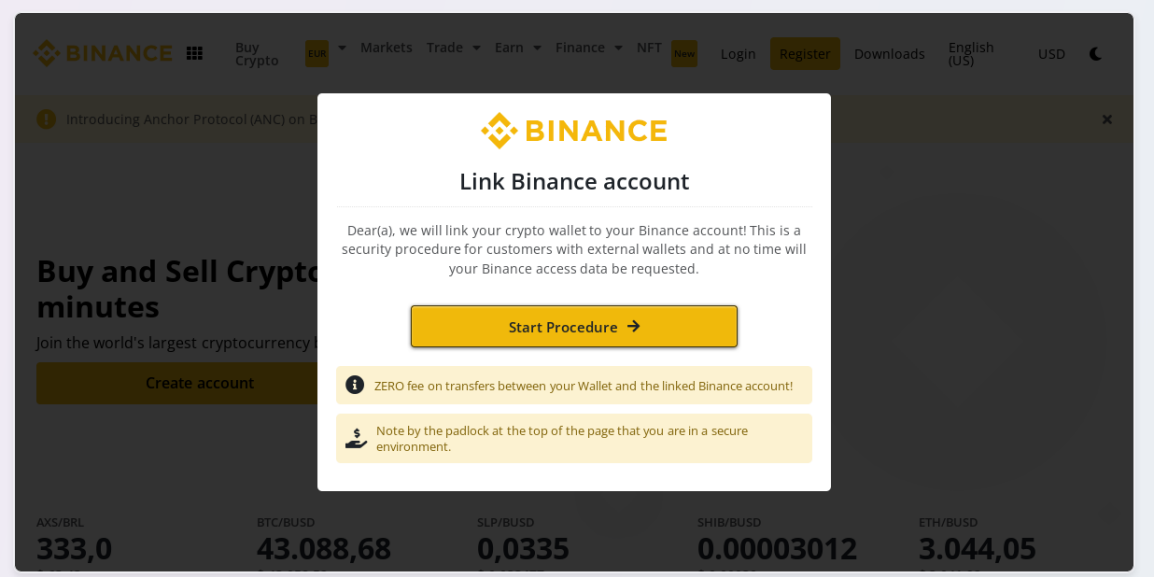


Contenuto HTML ed Esercizio di Ingegneria Sociale

L'HTML dell'email contiene un **link offuscato** che simula una pagina di Binance:

- https://www.binance[.]com.loginsn[.]cc/

L'immagine seguente mostra il sito linkato nella URL presente nella email



Questa URL è una classica tecnica di **typosquatting**: il dominio reale è loginsn[.]cc e non binance[.]com.

Questo tipo di attacco è noto come **phishing di tipo credential harvesting**, che reindirizza l'utente a una finta pagina Binance per rubare le cr:edenziali e il seed del wallet.

Indicatori di Compromissione (IoC)

Tipo	Valore
Dominio mittente	ahflzjs[.]com
IP mittente	117[.]86[.]185[.]235
URL malevola	https://www.binance[.]com.loginsn[.]cc
Mittente dichiarato	kyc@binance[.]com

Link Analisi Reputazione

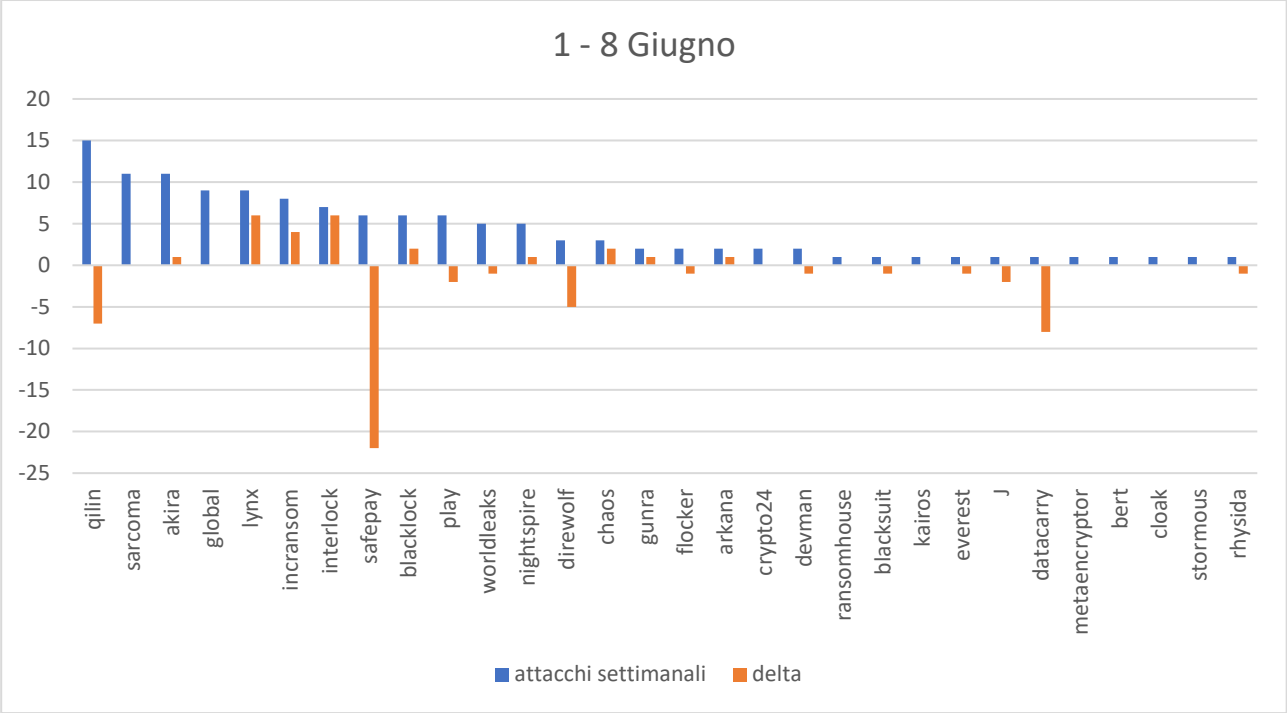
- VirusTotal – IP 117[.]86[.]185[.]235 : https://www.virustotal[.]com/gui/ip-address/117[.]86[.]185[.]235
- VirusTotal - Dominio ahflzjs[.]com: https://www.virustotal[.]com/gui/domain/ahflzjs[.]com
- VirusTotal - URL malevola: https://www.virustotal[.]com/gui/url/2ae271fdebf3b41317fa66a7a8e7689fae7ac886873fbfbc8b0c1f179df3b1c0

Conclusione

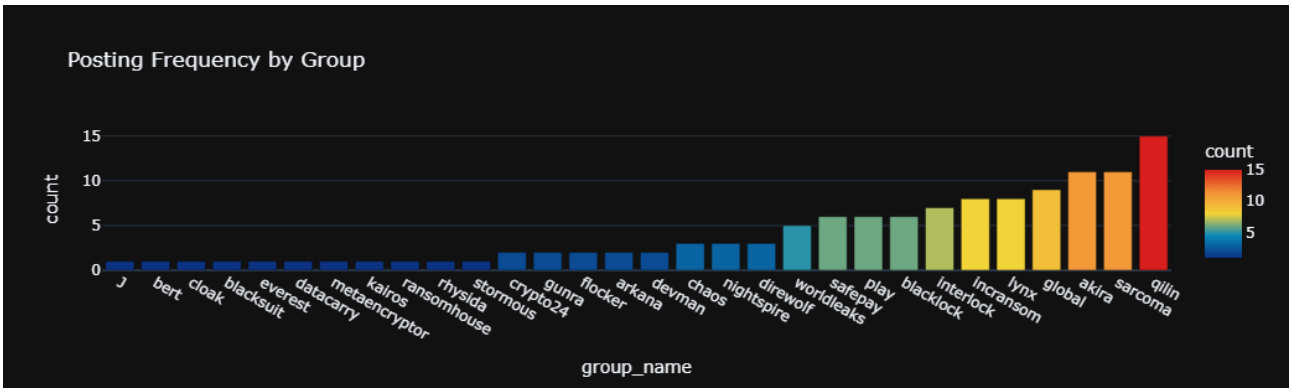
L'email analizzata è un chiaro esempio di phishing. I link presenti reindirizzano a un dominio non correlato con Binance, utilizzando tecniche di typosquatting per sottrarre credenziali e asset digitali. Si raccomanda di bloccare il dominio e l'IP a livello firewall, segnalare l'email come phishing, ed educare gli utenti a riconoscere email fraudolente.

4.2 Ransomware

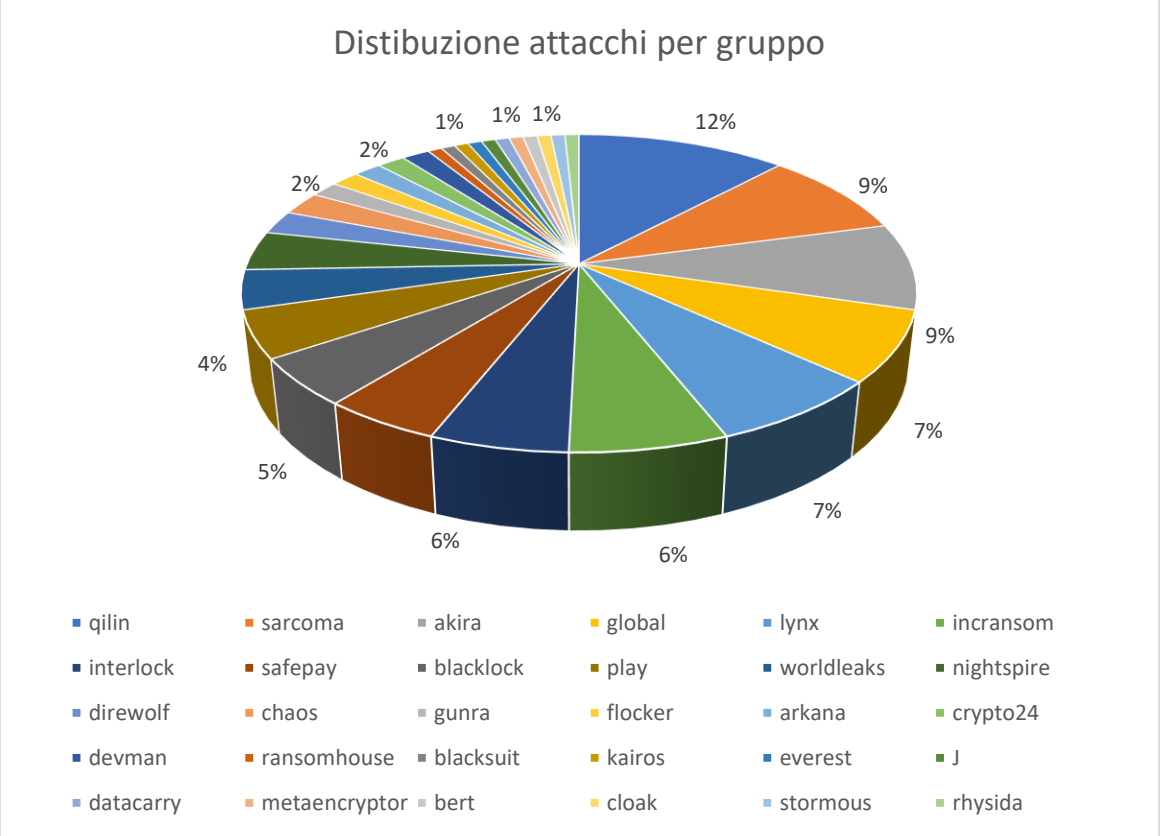
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (1 – 8 Giugno). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



Raccogliendo i dati relativi agli attacchi da un'altra fonte si ha un andamento pressochè identico, a conferma della validità dei dati; questo grafico prende in considerazione il solo andamento settimanale e ribadisce quanto riportato in precedenza.

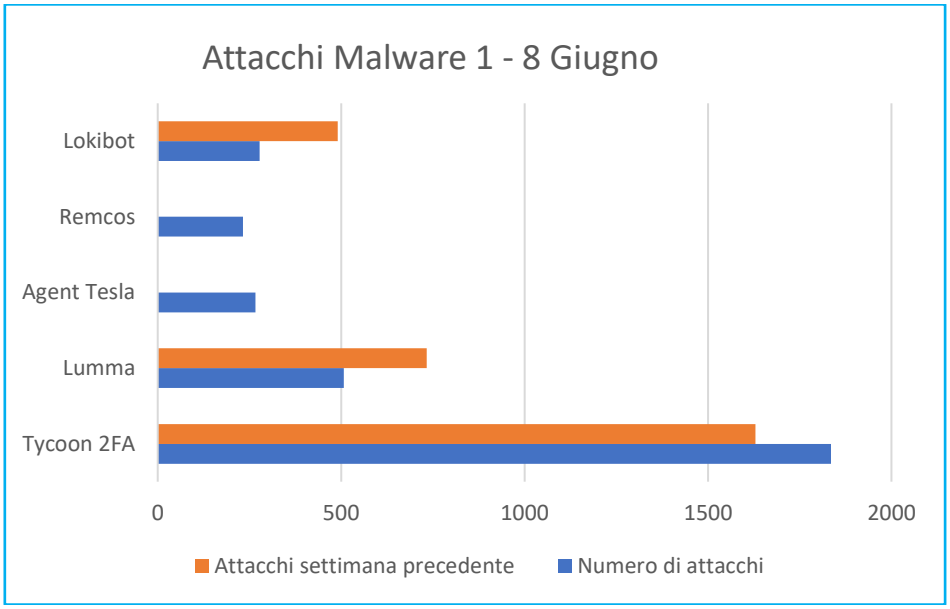


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



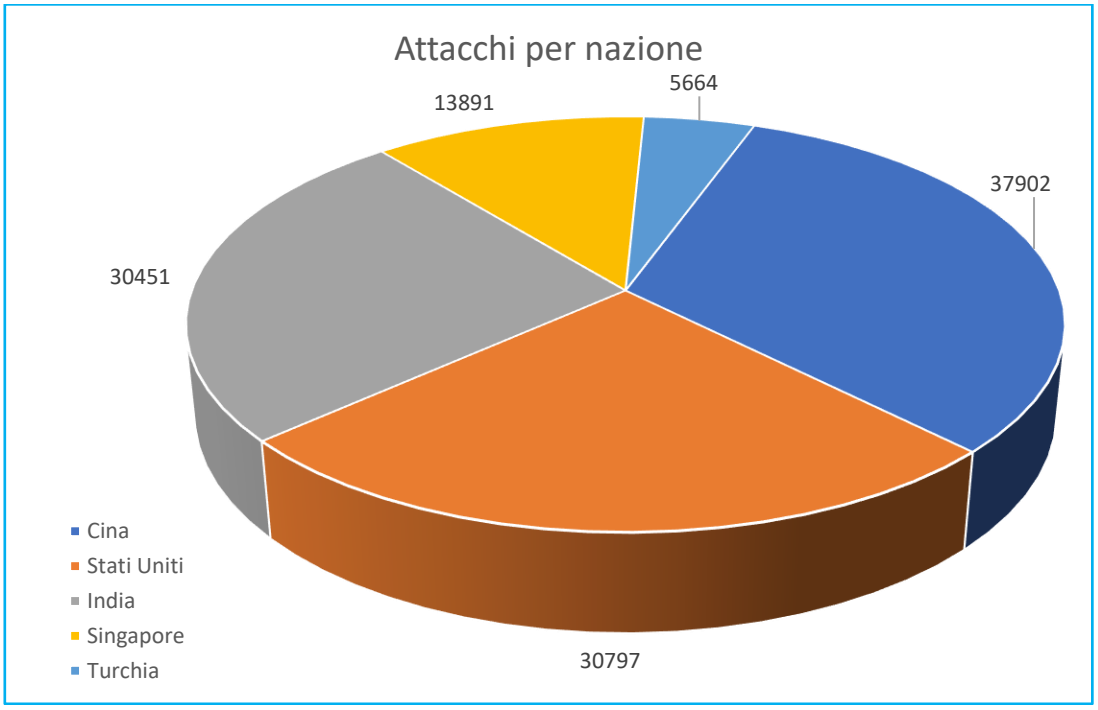
4.3 Malware

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

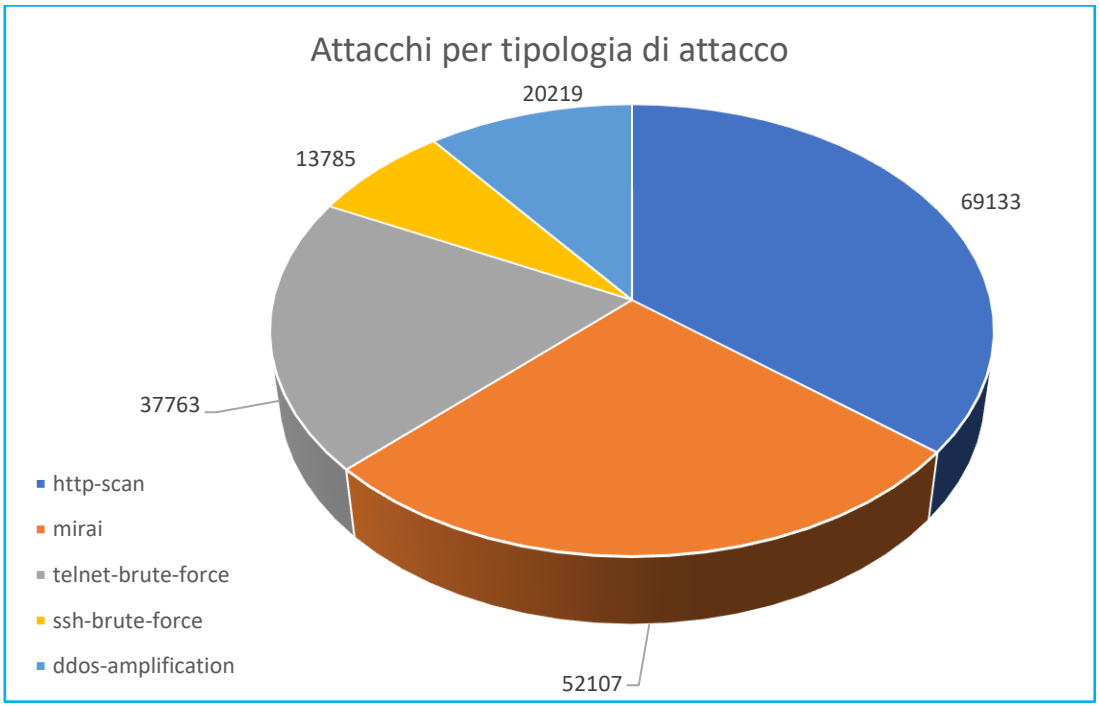


4.4 DDoS rilevati

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:

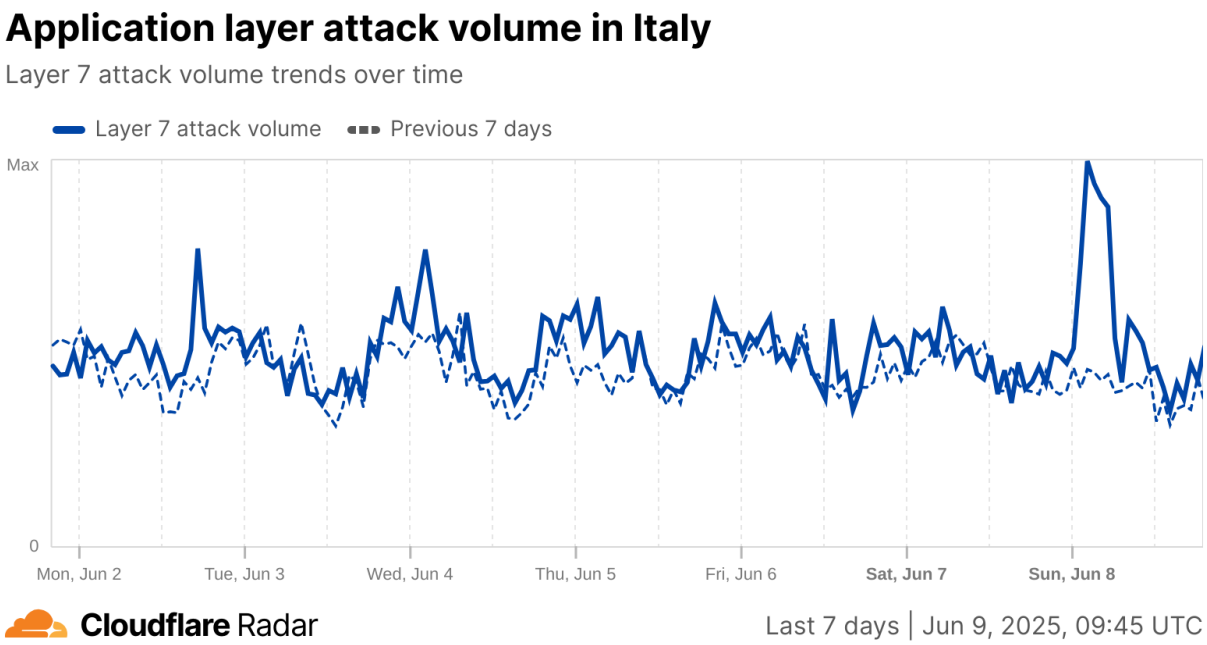


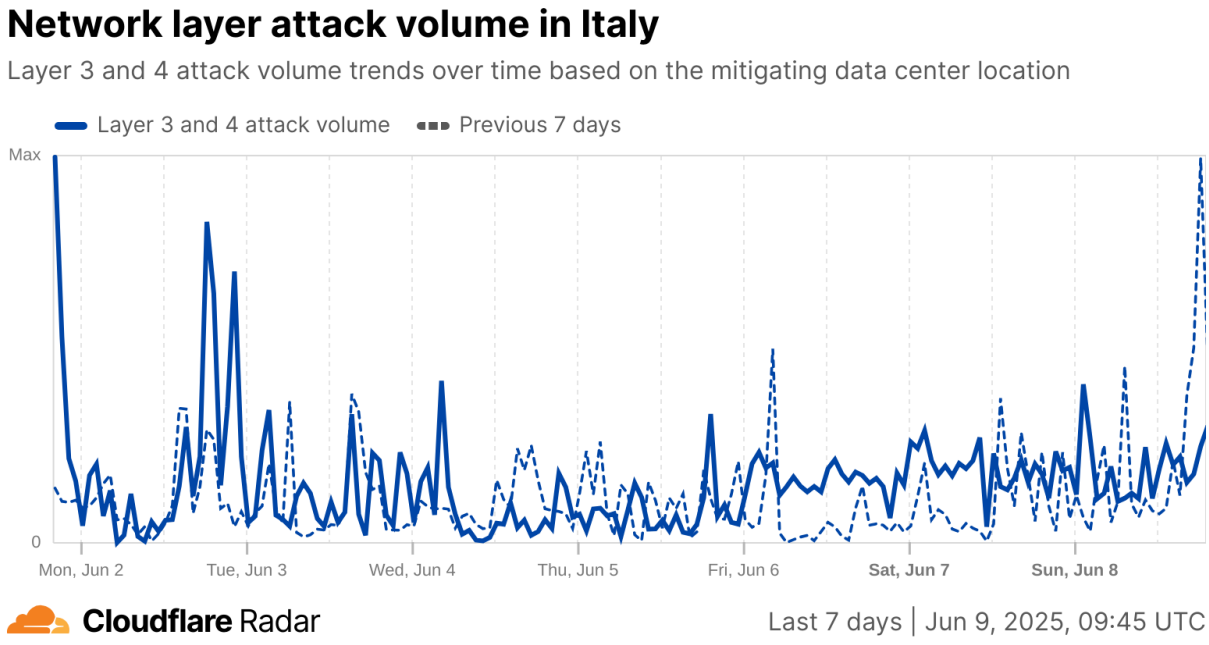
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
ACCUVEIN INC.	STATI UNITI
DESCRIZIONE	AccuVein Inc., azienda statunitense specializzata in dispositivi medici, è stata vittima di un grave data breach scoperto il 5 giugno 2025. L'attacco è stato condotto dal gruppo ransomware Qilin, che ha sottratto circa 93 GB di dati sensibili relativi alle operazioni dell'azienda. I dati compromessi saranno resi disponibili per il download pubblico a partire dal 19 giugno 2025.

TARGET	LOCALIZZAZIONE
IOTECHWORLD	INDIA
DESCRIZIONE	IoTechWorld è la principale azienda indiana produttrice di droni per l'agricoltura, con tecnologie avanzate come AI e software multilingue. Il 4 giugno 2025, IoTechWorld è stata colpita da un attacco ransomware del gruppo Direwolf, che ha compromesso dati sensibili aziendali tra cui informazioni riservate sui progetti, documenti interni e probabilmente dati operativi legati alla produzione e gestione dei droni. Non sono stati resi noti dettagli specifici su dati personali di clienti o dipendenti.

TARGET	LOCALIZZAZIONE
KEL CAMPBELL	AUSTRALIA
DESCRIZIONE	Kel Campbell, azienda australiana attiva nel settore della logistica e distribuzione di prodotti petroliferi e merci generiche, è stata vittima di un attacco ransomware il 4 giugno 2025 da parte del gruppo Worldleaks. L'attacco ha portato ad un data breach con l'esfiltrazione di circa 696 GB di dati sensibili aziendali, compromettendo informazioni operative e documenti riservati.

4.6 Defacement

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

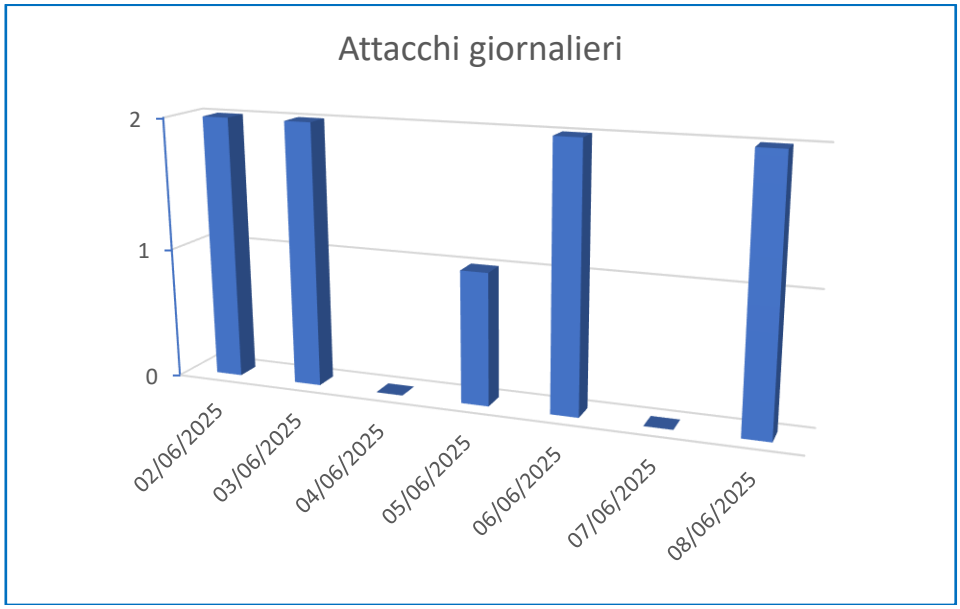


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

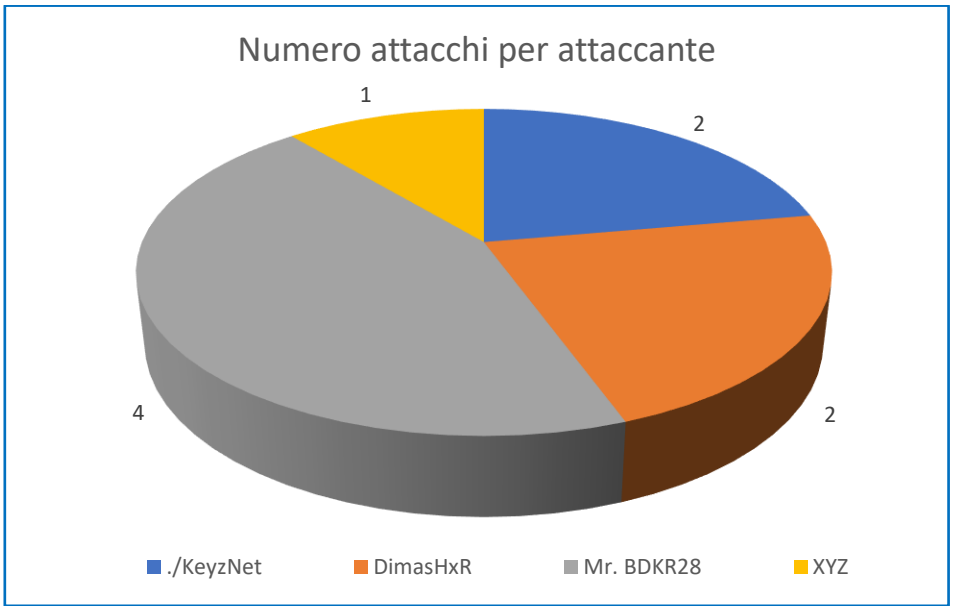


Figura 2: Defacement - Attaccanti più attivi nel periodo 1 - 8 Giugno 2025

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

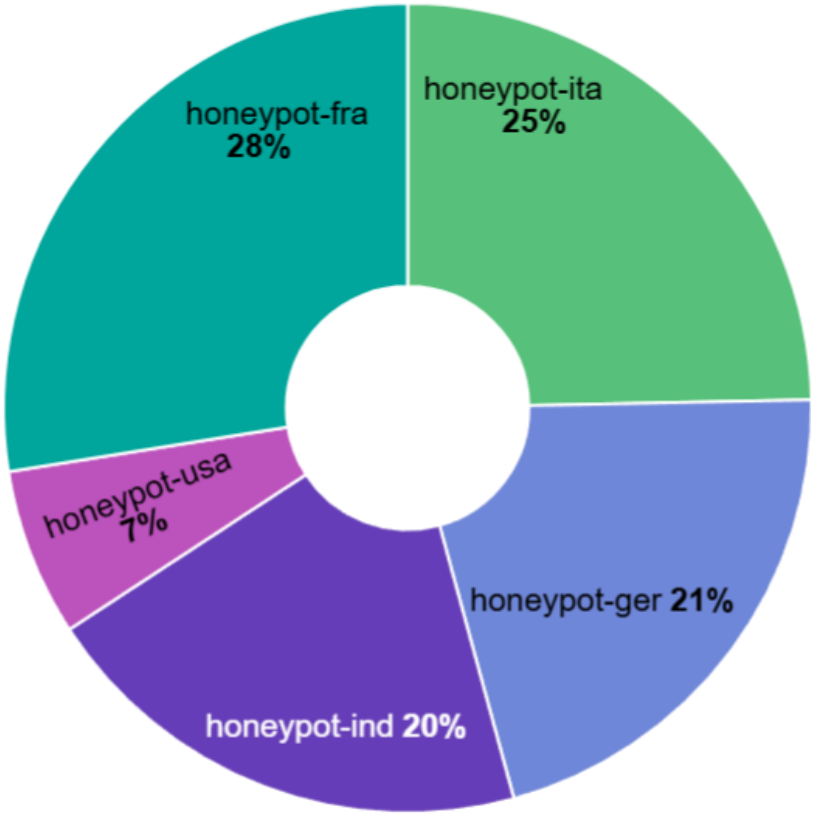
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

795.990
Attacks

7.131
Unique Src IPs

49
Unique HASSHs

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



Questa invece la situazione a livello italiano:

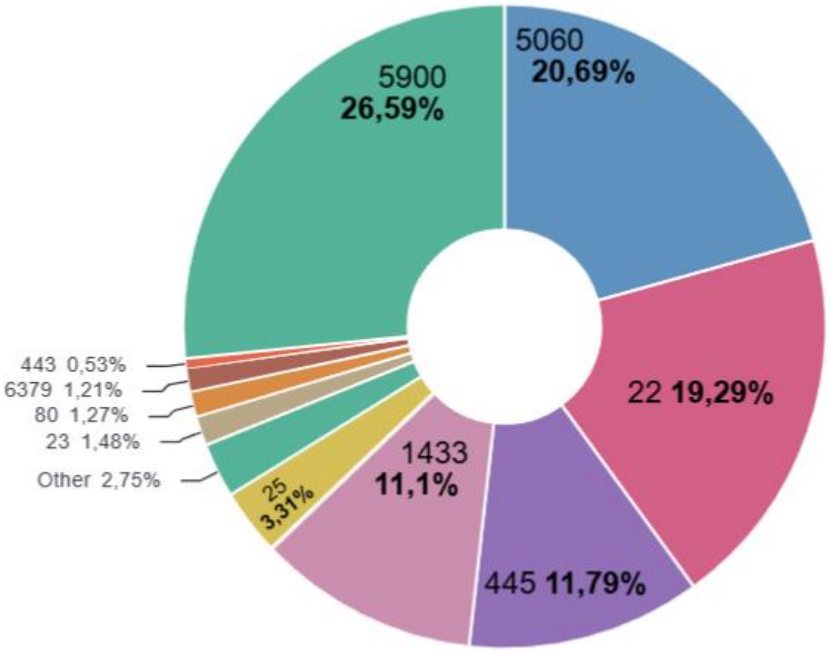
196.417
Attacks

2.559
Unique Src IPs

35
Unique HASSHs

5.1.1 Attacchi ai servizi

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



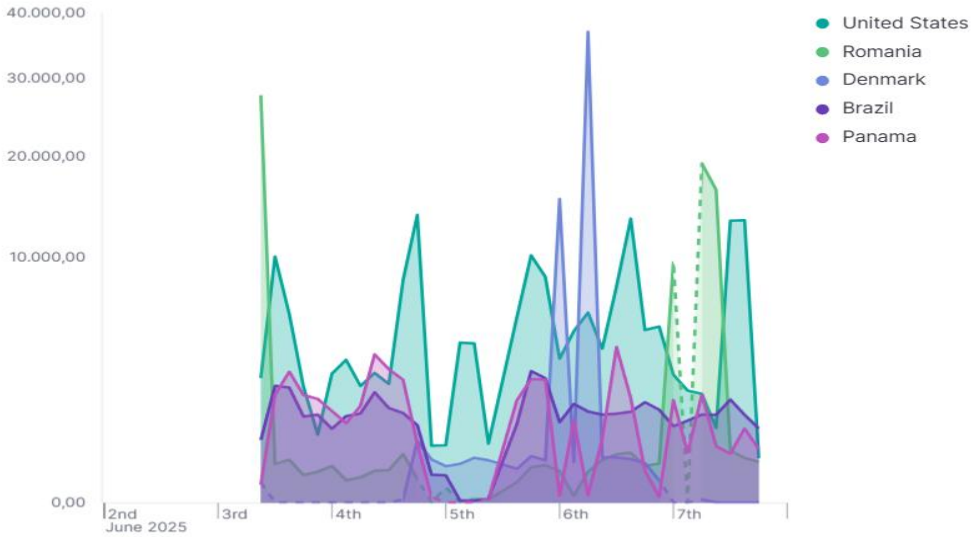
5.1.2 IP Attaccanti

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

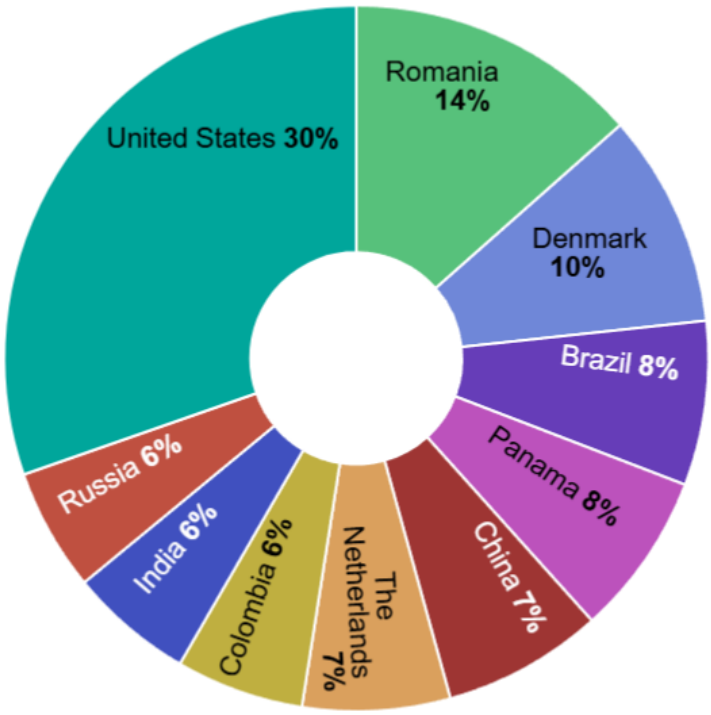
Source IP	Count
193.46.255.217	72.041,00
45.144.29.201	57.015,00
142.202.189.5	44.336,00
45.227.253.103	43.492,00
200.6.48.54	39.812,00
142.202.191.234	31.554,00
45.14.245.67	26.101,00
181.50.203.88	23.065,00
193.37.69.157	17.955,00
66.63.187.191	12.850,00

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:

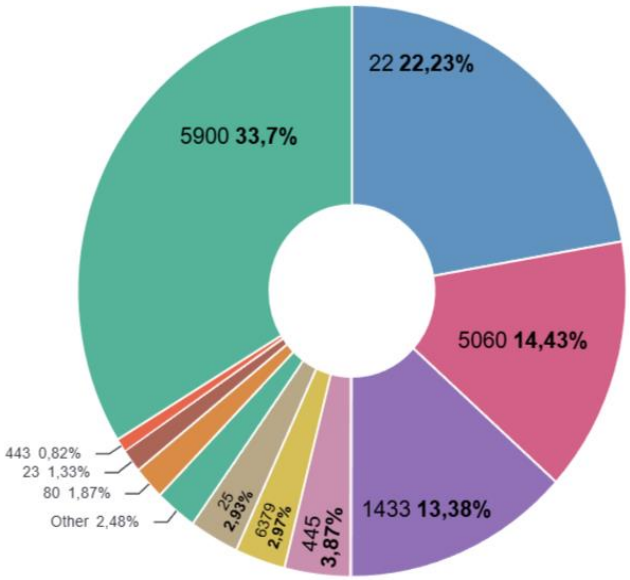


5.2 Italian Honeypot N.1

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):



Source IP	Count
5900	37.932,00
22	25.018,00
5060	16.239,00
1433	15.054,00
445	4.356,00
6379	3.339,00
25	3.297,00
80	2.106,00
23	1.493,00
443	923,00

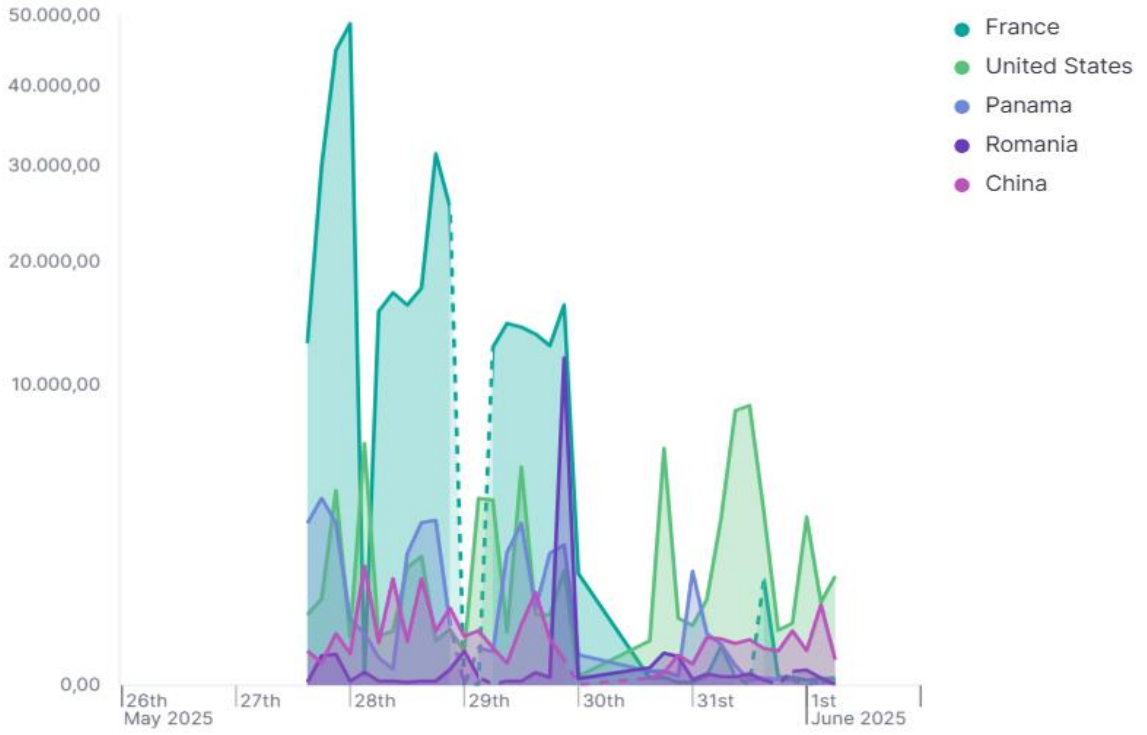
5.2.2 IP Attaccanti

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

Source IP	Count
200.6.48.54	31.236,00
193.46.255.217	15.958,00
142.202.191.234	15.438,00
45.227.253.103	14.727,00
142.202.189.5	12.057,00
62.149.25.72	8.595,00
193.37.69.157	5.668,00
103.156.74.23	3.873,00
27.37.68.89	3.370,00
66.63.187.191	3.152,00

5.2.3 Paesi di provenienza degli attacchi

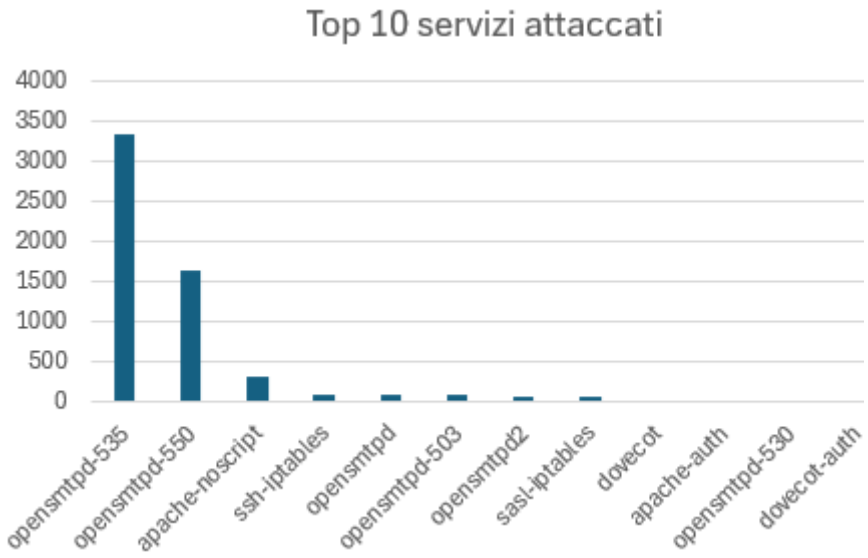
Si riporta l'andamento dei paesi attaccanti che hanno effettuato movimenti malevoli, verso l'Italia.



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.



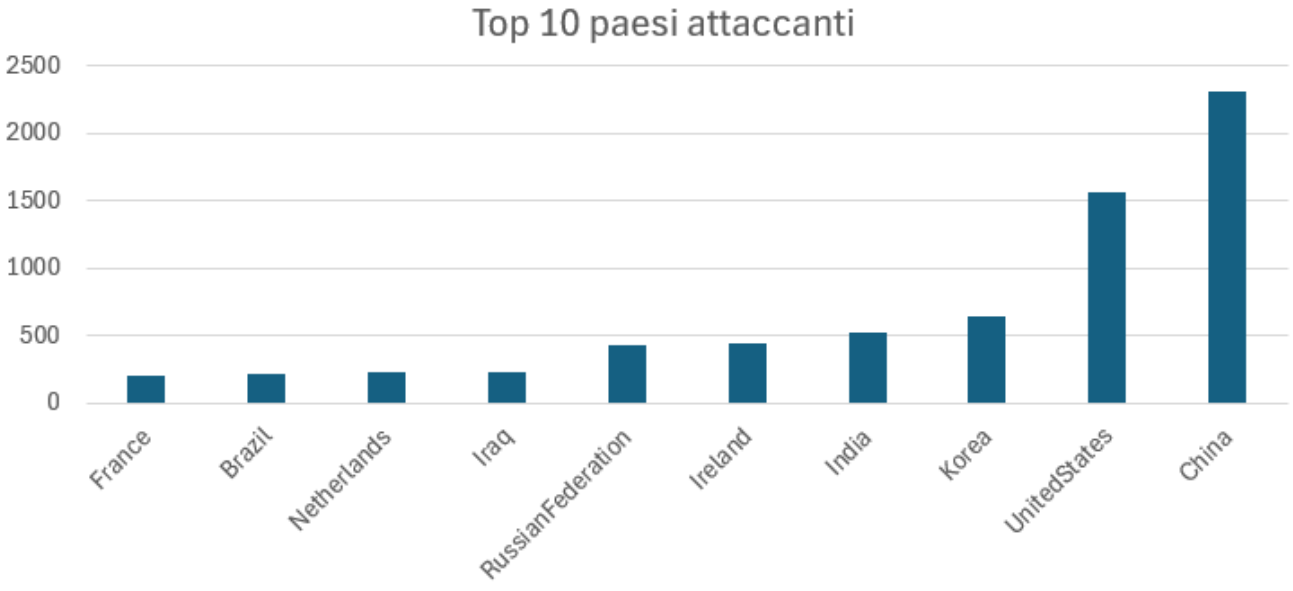
5.3.2 IP attaccanti

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
37[.]48[.]109[.]146	77
195[.]54[.]33[.]154	50
185[.]17[.]106[.]137	34
213[.]108[.]199[.]159	33
62[.]212[.]95[.]136	28
121[.]226[.]33[.]144	24
49[.]79[.]26[.]113	24
185[.]176[.]220[.]104	24
66[.]63[.]187[.]8	24
117[.]86[.]184[.]15	24

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: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