S3K

Cyber security

# RISK REPORT

\ week 18.08.2025 - 24.08.2025

# Sommario


1 Il Cyber Security Risk Report S3K ..... 5

1.1 Sommario ..... 5

1.2 Rilasci di aggiornamenti e patch critiche ..... 5

1.3 Notizie dal cyberspazio ..... 5

1.4 CVE Monitor: Vulnerabilità critiche della settimana ..... 6

1.5 Analisi degli Attacchi e Dati Honeypot ..... 6

1.6 Distribuzione geografica degli attacchi ..... 7

1.7 Riepilogo delle minacce della settimana ..... 7

1.8 Conclusioni ..... 8

2 Security news ..... 9

2.1 Rilasci aggiornamenti e patch ..... 9

2.2 "Cyber News" dal Web, Deep Web e Dark Web ..... 11

3 CVE Monitor ..... 15

3.1 Sintesi Settimanale CVE ..... 15

3.2 Tendenze ..... 17

3.3 Nuove CVE ..... 18

3.4 CVE attualmente utilizzate in attacchi ..... 20

4 Attacchi ..... 21

4.1 Phishing ..... 21

4.2 Ransomware ..... 28

4.3 Malware ..... 30

4.4 DDoS rilevati ..... 39

4.5 Data Breach ..... 41

4.6 Defacement ..... 43

5 Honeypot ..... 44

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale ..... 44

5.1.1 Attacchi ai servizi ..... 45

5.1.2 IP Attaccanti ..... 45

5.1.3 Paesi di provenienza degli attacchi ..... 46

5.2 Italian Honeypot N.1 ..... 47

5.2.1 Attacchi ai servizi ..... 47

5.2.2 IP Attaccanti ..... 48
5.2.3 Paesi di provenienza degli attacchi ..... 48
5.3 Italian Honeypot N.2 ..... 50
5.3.1 Attacchi ai servizi ..... 50
5.3.2 IP attaccanti ..... 51
5.3.3 Paesi di provenienza degli attacchi ..... 52
6 Company Profile S3K ..... 53

CYBER SECURITY RISK REPORT
34/25

# 1 Il Cyber Security Risk Report S3K

Benvenuti al bollettino settimanale di cybersecurity, una raccolta completa delle principali minacce informatiche, vulnerabilità critiche e aggiornamenti di sicurezza rilevati nel periodo 18-24 agosto 2025. Questo documento è stato preparato per fornire a responsabili IT, analisti di sicurezza e stakeholder aziendali informazioni dettagliate sulle tendenze emergenti e sugli incidenti significativi nel panorama della sicurezza informatica.

## 1.1 Sommario

- Security News : Aggiornamenti e patch critiche rilasciate da produttori di software e notizie di attualità dal mondo della cybersecurity
- CVE Monitor : Analisi delle vulnerabilità più impattanti, nuove CVE emerse e quelle attivamente sfruttate dagli attaccanti
- Attacchi : Dettagli su phishing, ransomware, malware, DDoS, data breach e defacement rilevati nel periodo di osservazione
- Honeypot : Dati raccolti dall'infrastruttura di honeypot dislocata in vari paesi con analisi degli attacchi e delle loro origini

## 1.2 Rilasci di aggiornamenti e patch critiche

- Google Chrome : Rilasciato aggiornamento per correggere una vulnerabilità di sicurezza con gravità "alta" che potrebbe consentire l'esecuzione di codice arbitrario. Versioni vulnerabili: precedenti alla 139.0.7258.138/.139 per Windows e Mac, e precedenti alla 139.0.7258.138 per Linux.
- Apple : Rilasciati aggiornamenti di sicurezza per sanare una vulnerabilità con gravità "alta" che potrebbe consentire l'esecuzione di codice arbitrario o compromettere la disponibilità del servizio. Sistemi coinvolti: macOS Sequoia, Sonoma, Ventura, iOS e iPadOS.
- Mozilla : Rilasciati aggiornamenti per correggere diverse vulnerabilità, di cui 3 critiche e 7 con gravità "alta", nei prodotti Firefox, Firefox ESR, Focus, Thunderbird e Thunderbird ESR. Queste vulnerabilità potrebbero consentire il bypass dei meccanismi di sicurezza e l'esecuzione di codice remoto.

## 1.3 Notizie dal cyberspazio

- Dati personali di milioni di italiani esposti : Un attore malevolo noto come Chucky_BF avrebbe messo in commercio sul dark web un database contenente circa 35 milioni di profili Facebook di utenti italiani, con dati sensibili come nomi e numeri di telefono. Il file in formato CSV conterrebbe informazioni identificabili grazie al prefisso telefonico +39. Non è chiaro se si tratti di una nuova violazione o di un rimaneggiamento della raccolta "Fuck Facebook", già diffusa da anni.

- Vulnerabilità in app VPN del Play Store : Un'indagine di Citizen Lab ha rivelato importanti vulnerabilità in oltre 20 applicazioni VPN del Google Play Store, con quasi un miliardo di download totali. Le app, sviluppate da società apparentemente separate ma in realtà collegate tra loro, presentano falle che consentono di intercettare e leggere il traffico dell'utente, compromettendo la riservatezza delle comunicazioni.
- Campagna malevola contro enti pubblici italiani : Il CERT-AGID ha ricevuto segnalazioni riguardanti una nuova campagna malevola contro le Pubbliche Amministrazioni italiane. Gli attaccanti inviano email ingannevoli relative a un presunto aggiornamento del software di firma digitale, inducendo i destinatari a scaricare uno script VBS dannoso. L'obiettivo è l'installazione abusiva di Action1, un software legittimo per la gestione remota, per ottenere accesso non autorizzato ai dispositivi.
- Operazione internazionale contro il cybercrime : Un'operazione coordinata da INTERPOL, denominata Serengeti 2.0, ha portato all'arresto di oltre 1.200 sospetti in Africa, tutti coinvolti in attività criminali online. Sono stati sequestrati 97,4 milioni di dollari, smantellate più di 11.000 infrastrutture digitali ostili e individuate quasi 88.000 vittime in tutto il mondo.

## 1.4 CVE Monitor: Vulnerabilità critiche della settimana

- CVE-2025-43300 (Apple ImageIO)
  - **Severità:** CRITICA
  - **Exploit confermato:** ✅
  - Vulnerabilità di tipo out-of-bounds write che consente l'esecuzione remota di codice tramite immagini malevole. Zero-day attivamente sfruttato su iOS, iPadOS e macOS.
- CVE-2025-9074 (VMware vCenter)
  - **Severità:** CRITICA
  - **Exploit confermato:** ❌
  - Consente RCE non autenticata via gestione plugin. Patch urgente disponibile.
- CVE-2025-27214 (PostgreSQL)
  - **Severità:** ALTA
  - **Exploit confermato:** ⚠️ PoC pubblico
  - SQL injection remota che consente exfiltrazione dati ed eventuale RCE.
- CVE-2025-5352 (Linux Kernel)
  - **Severità:** CRITICA
  - **Exploit confermato:** ❌
  - Use-after-free in networking stack con possibilità di RCE locale e privilege escalation.

## 1.5 Analisi degli Attacchi e Dati Honeypot

- Ransomware e attacchi significativi : Durante la settimana 18-24 agosto 2025 si è osservata un'intensa attività di ransomware, con gruppi come LockBit, Black Basta e ALPHV (BlackCat) particolarmente attivi. L'analisi dei dati raccolti mostra un aumento significativo degli attacchi rispetto alla settimana precedente, specialmente nel settore manifatturiero e sanitario. Tra i

malware più diffusi emergono SHAMOS (infostealer per macOS), QuirkyLoader (loader multipayload), DarkCloud (variante fileless) e Lampion (infostealer bancario).

- Data breach significativi : Il caso più rilevante ha coinvolto Nissan Motor, con il laboratorio di design "Nissan Creative Box" colpito da un attacco ransomware attribuito al gruppo Qilin, che afferma di aver sottratto oltre 4 terabyte di dati sensibili, tra cui progetti 3D di veicoli, report, fotografie e documentazione interna.

## 1.6 Distribuzione geografica degli attacchi

I dati raccolti dai sistemi honeypot mostrano una significativa concentrazione di attacchi provenienti principalmente da Stati Uniti, Russia, Cina, Paesi Bassi e Germania. In particolare, la rete di honeypot distribuita globalmente ha rilevato un aumento degli attacchi diretti verso l'Italia, con particolare focus sui servizi SSH, RDP e HTTP.

## 1.7 Riepilogo delle minacce della settimana

- Aggiornamenti critici
- Patch urgenti rilasciate per Google Chrome, Apple e Mozilla per vulnerabilità che consentono esecuzione di codice remoto. Si raccomanda l'aggiornamento immediato dei sistemi interessati.
- Vulnerabilità ad alto impatto : CVE-2025-43300 (Apple ImageIO) attivamente sfruttata in attacchi mirati. Altre vulnerabilità critiche identificate in VMware vCenter, PostgreSQL e Linux Kernel richiedono attenzione immediata.
- Attacchi rilevanti : Significativo aumento di ransomware da parte di gruppi come LockBit, Black Basta e ALPHV. Data breach significativo a Nissan Motor con 4TB di dati rubati. Nuova campagna phishing contro PA italiane.
- Trend emergenti : Proliferazione di infostealer per macOS (SHAMOS), crescita di malware fileless come DarkCloud, e vulnerabilità in app VPN con oltre 1 miliardo di download. Aumento di attacchi DDoS contro obiettivi italiani.
- Raccomandazioni urgenti
    - Aggiornare immediatamente i sistemi operativi Apple, browser Chrome e Firefox, e installare tutte le patch di sicurezza disponibili.
    - Verificare la presenza di IoC relativi alle campagne phishing e malware descritte nel bollettino, in particolare lo script VBS segnalato dal CERT-AGID.
    - Rimuovere le app VPN vulnerabili dai dispositivi aziendali e controllare il traffico di rete per identificare possibili compromissioni.
    - Rafforzare le misure di sicurezza per i servizi più attaccati (SSH, RDP, HTTP) e limitare l'esposizione dei servizi critici.

## 1.8 Conclusioni

Il panorama delle minacce informatiche nel periodo 18-24 agosto 2025 mostra un'intensificazione degli attacchi ransomware e un aumento delle vulnerabilità critiche in software di ampia diffusione. L'attività di phishing contro enti pubblici italiani e l'esposizione di dati personali di milioni di utenti Facebook italiani rappresentano minacce significative per il panorama nazionale. Si raccomanda un'attenzione particolare all'implementazione tempestiva delle patch di sicurezza e al monitoraggio dei sistemi per rilevare indicatori di compromissione.

Per ulteriori informazioni o assistenza sulle minacce descritte in questo report, contattare il team S3K all'indirizzo contattaci@s3kgroup.it o insidesales@s3kgroup.it.

# 2 Security news

## 2.1 Rilasci aggiornamenti e patch

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

| PRODOTTO | DESCRIZIONE |
|---|---|
| Google Chrome | Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere una vulnerabilità di sicurezza con gravità "alta". Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato remoto di eseguire codice arbitrario sui sistemi target.<br>Versioni affette:<br>• versioni precedenti alla 139.0.7258.138/.139 per Windows e Mac<br>• versioni precedenti alla 139.0.7258.138 per Linux |
| **ULR/Note** | https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_19.html |

| PRODOTTO | DESCRIZIONE |
|---|---|
| Apple | Apple ha rilasciato aggiornamenti di sicurezza per sanare una vulnerabilità con gravità "alta" presente nei propri prodotti. Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato remoto di eseguire codice arbitrario e/o compromettere la disponibilità del servizio sui sistemi target.<br>Versioni affette:<br>• macOS Sequoia, versioni precedenti alla 15.6.1<br>• macOS Sonoma, versioni precedenti alla 14.7.8<br>• macOS Ventura, versioni precedenti alla 13.7.8<br>• iOS, versioni precedenti alla 18.6.2<br>• iPadOS, versioni precedenti alla 18.6.2 |
| **ULR/Note** | https://support.apple.com/en-us/124925<br>https://support.apple.com/en-us/124926<br>https://support.apple.com/en-us/124927<br>https://support.apple.com/en-us/124928<br>https://support.apple.com/en-us/124929<br>https://support.apple.com/en-us/100100 |

| PRODOTTO | DESCRIZIONE |
|---|---|
| Mozilla | Mozilla ha rilasciato aggiornamenti di sicurezza per sanare diverse vulnerabilità, di cui 3 con gravità "critica" e 7 con gravità "alta", nei prodotti Firefox, Firefox ESR, Focus, Thunderbird e Thunderbird ESR. Tali vulnerabilità, qualora sfruttate, potrebbero consentire il bypass dei meccanismi di sicurezza e l'esecuzione di codice remoto sui sistemi target.<br>Versioni affette:<br>• Firefox, versioni precedenti alla 142<br>• Firefox ESR 115.x, versioni precedenti alla 115.27<br>• Firefox ESR 128.x, versioni precedenti alla 128.14<br>• Firefox ESR 140.x, versioni precedenti alla 140.2<br>• Thunderbird, versioni precedenti alla 142<br>• Thunderbird ESR 140.x, versioni precedenti alla 140.2<br>• Thunderbird ESR 128.x, versioni precedenti alla 128.14<br>• Focus per iOS, versioni precedenti alla 142 |
| **ULR/Note** | https://www.mozilla.org/en-US/security/advisories/mfsa2025-64/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-65/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-66/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-67/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-68/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-69/https://www.mozilla.org/en-US/security/advisories/mfsa2025-69/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-70/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-71/<br>https://www.mozilla.org/en-US/security/advisories/mfsa2025-72/<br>https://www.mozilla.org/en-US/security/advisories/ |

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

### DARK WEB: ESPOSTI I DATI PERSONALI DI MILIONI DI ITALIANI SU FACEBOOK

Un nuovo episodio legato alla cybersicurezza scuote la rete: è emersa online una raccolta massiva di dati personali appartenenti ad utenti italiani di Facebook. Secondo alcune fonti, un attore malevolo noto con il nickname Chucky_BF avrebbe messo in commercio, su un popolare forum nel dark web, un database contenente circa 35 milioni di profili, contenente tra gli altri dati sensibili come nomi e numeri di telefono degli utenti. Il file, in formato CSV, conterrebbe informazioni riferite esclusivamente ad utenti italiani, facilmente identificabili grazie al prefisso telefonico +39. Non è stato chiarito se questi dati siano frutto di una nuova violazione o se si tratti di un rimaneggiamento della ben nota raccolta "Fuck Facebook", già diffusa da anni in ambienti sotterranei ed accessibile anche tramite motori di ricerca specifici del dark web. Il post originale al momento risulta rimosso. Tuttavia, DarkWeb Informer ha documentato l'esistenza dell'annuncio prima della sua sparizione, fornendo anche alcune prove visive. A quanto pare, si tratterebbe di una riorganizzazione di materiale già sottratto in passato e ora riproposto per finalità illecite. L'associazione tra nomi reali e numeri di cellulare rappresenta un grave pericolo: può essere sfruttata per operazioni di phishing, smishing e altre forme di truffa online. Per dare credibilità all'offerta, l'autore avrebbe condiviso immagini di anteprima dei dati, oltre ad indicare canali Telegram per essere contattato. Nonostante si tratti di pratiche comuni nel mondo della criminalità informatica, questi elementi non garantiscono l'autenticità del materiale proposto e lasciano spazio al dubbio che si tratti anche di un possibile inganno tra criminali. Questo nuovo caso riporta al centro dell'attenzione la fragilità delle protezioni adottate dai social network e la scarsa resilienza nella gestione delle informazioni degli utenti. In Italia, la potenziale esposizione di milioni di dati rappresenta un rischio concreto non solo per i singoli cittadini, ma anche per aziende e pubbliche amministrazioni, che potrebbero diventare bersagli di attacchi basati su tecniche di social engineering. Esperti di sicurezza e autorità competenti consigliano agli utenti di mantenere alta l'attenzione, diffidare da messaggi sospetti e rafforzare la sicurezza dei propri account attraverso l'autenticazione a due fattori e altre misure preventive. In attesa di un'eventuale presa di posizione da parte di Meta, il caso evidenzia ancora una volta quanto sia esposto e vulnerabile il patrimonio digitale personale. La compravendita di dati personali, anche quando non del tutto verificata, continua ad essere uno dei mercati più redditizi nel dark web, a conferma del valore sempre più elevato che le informazioni sensibili hanno nel panorama della criminalità informatica.

## MILIONI DI UTENTI A RISCHIO PER VULNERABILITÀ NELLE APP VPN DEL PLAY STORE

Un'indagine condotta dagli esperti di Citizen Lab ha fatto emergere importanti vulnerabilità all'interno di oltre 20 applicazioni VPN disponibili sul Google Play Store. Queste app, che hanno totalizzato quasi un miliardo di download, mettono a rischio la privacy degli utenti e permettono, in alcuni casi, la decodifica del traffico dati, compromettendo l'affidabilità dei servizi offerti. Dallo studio emerge come numerosi fornitori di VPN, pur presentandosi come entità indipendenti, in realtà condividano strutture comuni e adottino tecniche per mascherare i legami tra loro. L'analisi approfondita ha rivelato che tre società Innovative Connecting, Autumn Breeze e Lemon Clove, tutte apparentemente con sede a Singapore, risultano legate tra loro da elementi condivisi a livello di codice, dipendenze software e persino password integrate staticamente nei file delle applicazioni. Le app sviluppate da questi tre soggetti, che da sole superano i 330 milioni di installazioni, presentano falle che possono permettere ad attori malevoli di intercettare e leggere il traffico dell'utente. Le connessioni VPN si basano sul protocollo Shadowsocks, originariamente sviluppato per bypassare la censura cinese, ma giudicato ora non sicuro per via dell'utilizzo di algoritmi di cifratura obsoleti e meccanismi di autenticazione deboli. In alcuni casi, il traffico potrebbe essere deviato o manipolato sfruttando falle legate al sistema operativo stesso. Tra le app coinvolte si segnalano: Turbo VPN, Turbo VPN Lite, VPN Monster, VPN Proxy Master (e la sua versione Lite), Snap VPN, Robot VPN e SuperNet VPN. Queste applicazioni condividono importanti porzioni di codice, adottano protocolli vulnerabili come IPsec e Shadowsocks, e impiegano tecniche per eludere i controlli di sicurezza e impedire l'analisi da parte di ricercatori e sistemi automatizzati. I test hanno evidenziato che tutte le app in questione sono esposte a manomissioni delle connessioni, iniezione di pacchetti malevoli e raccolgono in modo non trasparente dati sulla posizione degli utenti. La presenza della stessa password hard-coded tra più app ha permesso di confermare che le tre aziende VPN utilizzano un'infrastruttura condivisa, ulteriore segno della loro interconnessione. Lo studio evidenzia anche la possibile partecipazione di un secondo gruppo di sviluppatori, tra cui Matrix Mobile PTE LTD, ForeRaya Technology Limited, Wildlook Tech PTE LTD, Hong Kong Silence Technology Limited e Yolo Mobile Technology Limited, che potrebbe essere associato al primo trio. Le app di questi soggetti, con oltre 380 milioni di installazioni complessive, presentano caratteristiche molto simili: codice sovrapponibile, uso di password nascoste e connessioni agli stessi indirizzi IP. Infine, altri due provider, Fast Potato Pte. Ltd e Free Connected Limited, offrono client VPN che sfruttano la stessa implementazione di un protocollo proprietario potenzialmente insicuro. Secondo i ricercatori, le implicazioni per gli utenti sono gravi: oltre alla violazione della riservatezza, gli utenti rischiano di essere esposti a sistemi di sorveglianza, intercettazioni e attacchi informatici. Molte di queste app, infatti, raccolgono dati personali senza trasparenza, sfruttano protocolli vulnerabili e non offrono un reale livello di protezione.

## NUOVA CAMPAGNA MALEVOLA VIA EMAIL PRENDE DI MIRA ENTI PUBBLICI ITALIANI

Il CERT-AGID ha ricevuto pochi giorni fa, diverse segnalazioni da parte di enti pubblici riguardo ad una nuova campagna malevola in corso, progettata per colpire i sistemi delle Pubbliche Amministrazioni. Gli aggressori hanno inviato email ingannevoli che fingono di comunicare un presunto aggiornamento urgente del software di firma digitale, allo scopo di convincere i destinatari a cliccare su un link incluso nel testo del messaggio. Cliccando, l'utente viene indirizzato al download di un archivio compresso in formato ZIP che contiene uno script VBS dannoso. Questo script è privo di tecniche di offuscamento e contiene commenti scritti in lingua italiana, il che potrebbe indicare il coinvolgimento di cybercriminali locali o, alternativamente, un tentativo deliberato di depistare gli analisti. L'obiettivo finale dell'attacco sembra essere l'installazione abusiva di Action1, un software solitamente utilizzato da professionisti IT per la gestione remota di aggiornamenti e patch di sicurezza. Tuttavia, in questo caso lo strumento viene impiegato per ottenere accesso remoto non autorizzato ai dispositivi delle vittime. È la prima volta che si registra in Italia un uso malevolo di Action1, anche se a livello internazionale il tool è già noto per essere stato sfruttato in campagne di distribuzione di malware, compresi attacchi attribuiti al gruppo ransomware Conti. Come già accaduto con altri strumenti legittimi di gestione remota, tra cui ScreenConnect, anche in questo caso i criminali informatici si avvalgono di software autentici per eludere i controlli dei sistemi di sicurezza, riducendo la probabilità di essere rilevati da antivirus e soluzioni EDR. Al momento non è stato identificato alcun payload finale o malware specifico rilasciato dal VBS, il che fa supporre che gli attaccanti stiano aspettando il momento ideale per attivare la fase successiva dell'operazione. Il CERT-AGID ha già avviato le attività di contenimento della minaccia, distribuendo agli enti competenti gli Indicatori di Compromissione (IoC) rilevati finora, e ha informato il gestore del software di firma digitale coinvolto nella campagna. L'ente raccomanda a tutti gli utenti, ed in particolare alle Pubbliche Amministrazioni, di non interagire con i link presenti nell'email sospetta, utilizzare gli IoC pubblicati dal CERT-AGID per effettuare controlli nei propri ambienti IT, eseguire scansioni dei file sospetti con strumenti come hashr per individuare eventuali minacce ed in caso di sospetta compromissione mettere subito in isolamento il dispositivo e segnalare l'incidente al CSIRT Italia. Gli indicatori relativi a questa campagna sono già stati condivisi attraverso i canali ufficiali di distribuzione IoC alle organizzazioni accreditate.

## MAXI OPERAZIONE IN AFRICA: OLTRE 1.200 ARRESTI E MILIONI DI DOLLARI SEQUESTRATI

Una vasta azione coordinata a livello internazionale ha portato all'arresto di oltre 1.200 sospetti in Africa, tutti coinvolti in attività criminali online su scala globale. L'operazione, denominata Serengeti 2.0, è stata guidata da INTERPOL con la collaborazione delle autorità di 18 Paesi africani e del Regno Unito, e si è conclusa proprio nel mese di agosto. Nel corso dell'operazione sono stati sequestrati 97,4 milioni di dollari, smantellate più di 11.000 infrastrutture digitali ostili e individuate quasi 88.000 vittime in tutto il mondo. Le attività illecite scoperte comprendono ransomware, frodi online e compromissione di sistemi aziendali di posta elettronica. INTERPOL ha sottolineato come questa azione congiunta miri a colpire organizzazioni criminali transfrontaliere con metodi sempre più evoluti, facendo leva su tecnologie legittime sfruttate in modo fraudolento. La campagna fa parte di un più ampio progetto di contrasto alla criminalità informatica in Africa, finanziato dal Foreign, Commonwealth and Development Office del Regno Unito. A supporto dell'operazione, anche numerosi partner del settore privato, come Cybercrime Atlas, Kaspersky, Group-IB, Fortinet, Trend Micro, e altri, che hanno fornito intelligence e dati tecnici fondamentali per le indagini. Questa non è la prima offensiva internazionale contro il cybercrime sul continente africano. In passato, altre azioni simili hanno portato a centinaia di arresti e alla neutralizzazione di vaste reti criminali. Ad esempio, tra novembre 2024 e febbraio 2025, la cosiddetta Operazione Cartellino Rosso ha condotto all'arresto di oltre 300 soggetti, collegati ad attacchi che hanno colpito più di 5.000 vittime a livello globale. Anche la prima edizione di Serengeti, attiva tra settembre e ottobre 2024, aveva visto la cattura di 1.006 persone, coinvolte in attività di estorsione digitale, attacchi ransomware, BEC e truffe online. Risale invece all'aprile 2023 l'operazione Africa Cyber Surge II, che ha interessato 25 nazioni africane e portato all'arresto di 14 sospetti, collegati a frodi informatiche che hanno causato oltre 40 milioni di dollari di danni. Secondo Valdecy Urquiza, segretario generale dell'INTERPOL, ogni operazione rafforza la collaborazione tra le forze dell'ordine internazionali, migliorando la capacità dei Paesi membri di affrontare minacce cyber sempre più sofisticate. "Lavorando insieme, i risultati diventano sempre più incisivi. Il nostro network globale è oggi più forte che mai e continua a proteggere le persone reali da crimini digitali reali", ha dichiarato.

# 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 18 Agosto – 24 Agosto 2025

Settimana segnata da vulnerabilità critiche che toccano Apple, VMware, PostgreSQL, Linux Kernel e componenti Microsoft. Alcuni bug presentano exploit attivi o proof-of-concept pubblici e richiedono interventi immediati.

CVE ad Alto Impatto (CRITICAL & HIGH)

| CVE ID | Severità | Data Pubblicazione | Exploit confermato | Descrizione Sintetica |
|---|---|---|---|---|
| CVE-2025-43300 | CRITICAL | 19/08/2025 | ✅ | Apple ImageIO – RCE tramite immagini malevole (out-of-bounds write); zero-day attivamente sfruttato su iOS, iPadOS, macOS. |
| CVE-2025-9074 | CRITICAL | 20/08/2025 | ❌ | VMware vCenter Server – RCE non autenticata via gestione plugin; patch urgente. |
| CVE-2025-27214 | HIGH | 21/08/2025 | ⚠️ PoC pubblico | PostgreSQL – SQL injection remota che consente exfiltrazione dati ed eventuale RCE. |

| | | | | |
|---|---|---|---|---|
| CVE-2025-5352 | CRITICAL | 22/08/2025 | ❌ | Linux Kernel – Use-after-free in networking stack con possibilità di RCE locale e privilege escalation. |
| CVE-2025-54988 | HIGH | 23/08/2025 | ❌ | Linux Kernel – Use-after-free in networking stack con possibilità di RCE locale e privilege escalation. |

**Vendor e Tecnologie Coinvolti**

- **Apple:** ImageIO framework vulnerabile a RCE, sfruttato attivamente.
- **VMware:** vCenter Server esposto a RCE non autenticata.
- **PostgreSQL:** vulnerabilità SQL injection con PoC disponibile.
- **Linux Kernel:** bug critico in networking stack.
- **Microsoft Office/Excel**: RCE tramite documenti malevoli.

**Distribuzione Giornaliera**

- **19 agosto:** disclosure Apple ImageIO zero-day (exploit attivo).
- **20 agosto:** advisory VMware vCenter Server (RCE).
- **21 agosto:** pubblicazione PoC PostgreSQL SQLi.
- **22 agosto:** Linux Kernel networking bug (UAF).
- **23 agosto:** disclosure Microsoft Office/Excel RCE.

**Raccomandazioni**

- **Patch Prioritarie:**
  - Aggiornare dispositivi Apple (iOS, iPadOS, macOS) alle ultime release.
  - Applicare urgentemente patch VMware vCenter.
  - Aggiornare PostgreSQL all'ultima versione stabile.
  - Applicare fix kernel Linux distribuiti dai vendor.
  - Aggiornare Office/Excel e bloccare macro da fonti non affidabili.

- **Mitigazioni e Controlli:**
    - Monitorare traffico e log per indicatori di compromissione.
    - Limitare esposizione pubblica di vCenter Server.
    - Utilizzare WAF per ridurre rischio SQLi su PostgreSQL.
    - Abilitare antivirus e AMSI su endpoint Office.

## 3.2 Tendenze

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

| CVE | PRODOTTO | CVSS V3 |
|---|---|---|
| CVE-2025-43300 | Apple | N/A |
| CVE-2025-9074 | Docker Desktop | N/A |
| CVE-2025-1316 | Edimax | 9.8 |
| CVE-2025-54253 | Adobe Experience Manager | 10.0 |
| CVE-2025-38236 | Linux kernel | 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-2025-5352 | Lunary-ai | N/A |
| **VULNERABILITÀ** | Una vulnerabilità critica di tipo Cross-Site Scripting (XSS) è presente nel componente Analytics di lunary-ai/lunary fino alla versione 1.9.23. La variabile d'ambiente NEXT_PUBLIC_CUSTOM_SCRIPT viene iniettata direttamente nel DOM tramite dangerouslySetInnerHTML senza alcuna sanificazione o convalida. Ciò permette l'esecuzione di codice JavaScript arbitrario nei browser di tutti gli utenti se un aggressore riesce a controllare la variabile d'ambiente durante la distribuzione o tramite la compromissione del server. La vulnerabilità può portare al controllo completo dell'account, all'esfiltrazione di dati, alla distribuzione di malware e a attacchi persistenti che colpiscono tutti gli utenti finché la variabile d'ambiente non viene ripulita. Il problema è stato risolto nella versione 1.9.25. | |

| CVE | PRODOTTI | SCORE CVSS NIST |
|---|---|---|
| CVE-2025-54988 | Apache Tika | N/A |
| **VULNERABILITÀ** | Una vulnerabilità critica di tipo XXE (XML External Entity) è presente in Apache Tika (modulo tika-parser-pdf-module) nelle versioni da 1.13 a 3.2.1 su tutte le piattaforme. Un aggressore può eseguire un'iniezione di entità esterne XML tramite un file XFA appositamente creato all'interno di un PDF. Ciò potrebbe consentire a un malintenzionato di leggere dati sensibili o di attivare richieste dannose verso risorse interne o server di terze parti. Il modulo tika-parser-pdf-module è una dipendenza utilizzata in diversi pacchetti Tika, inclusi tika-parsers-standard-modules, tika-parsers-standard-package, tika-app, tika-grpc e tika-server-standard. Si raccomanda agli utenti di aggiornare alla versione 3.2.2, che risolve il problema. | |

| CVE | PRODOTTI | SCORE CVSS NIST |
|---|---|---|
| CVE-2025-43300 | Apple | N/A |
| **VULNERABILITÀ** | Un problema di scrittura al di fuori dei limiti (out-of-bounds write) è stato risolto con un miglioramento del controllo dei limiti. Questo problema è stato corretto in macOS Sonoma 14.7.8, macOS Ventura 13.7.8, iPadOS 17.7.10, macOS Sequoia 15.6.1, iOS 18.6.2 e iPadOS 18.6.2. L'elaborazione di un file immagine dannoso potrebbe causare un danneggiamento della memoria. Apple è a conoscenza di un rapporto secondo cui questo problema potrebbe essere stato sfruttato in un attacco estremamente sofisticato contro individui specifici e mirati. | |

| CVE | PRODOTTI | SCORE CVSS NIST |
|---|---|---|
| CVE-2025-27214 | UniFi Connect EV Station Pro | N/A |
| **VULNERABILITÀ** | Vulnerabilità "Autenticazione mancante per una funzione critica" in UniFi Connect EV Station Pro potrebbe consentire a un malintenzionato con accesso fisico o adiacente di eseguire un ripristino di fabbrica non autorizzato. | |

## 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-2025-43300 |
|---|---|
| **DESCRIZIONE** | |
| Un problema di scrittura al di fuori dei limiti (out-of-bounds write) è stato risolto con un miglioramento del controllo dei limiti. Questo problema è stato corretto in macOS Sonoma 14.7.8, macOS Ventura 13.7.8, iPadOS 17.7.10, macOS Sequoia 15.6.1, iOS 18.6.2 e iPadOS 18.6.2. L'elaborazione di un file immagine dannoso potrebbe causare un danneggiamento della memoria. Apple è a conoscenza di un rapporto secondo cui questo problema potrebbe essere stato sfruttato in un attacco estremamente sofisticato contro individui specifici e mirati. | |

| CVE | CVE-2020-25078 |
|---|---|
| **DESCRIZIONE** | |
| Una vulnerabilità è stata scoperta sui dispositivi D-Link DCS-2530L (versioni precedenti alla 1.06.01 Hotfix) e DCS-2670L (fino alla 2.02). L'endpoint non autenticato /config/getuser permette la divulgazione da remoto della password dell'amministratore. | |

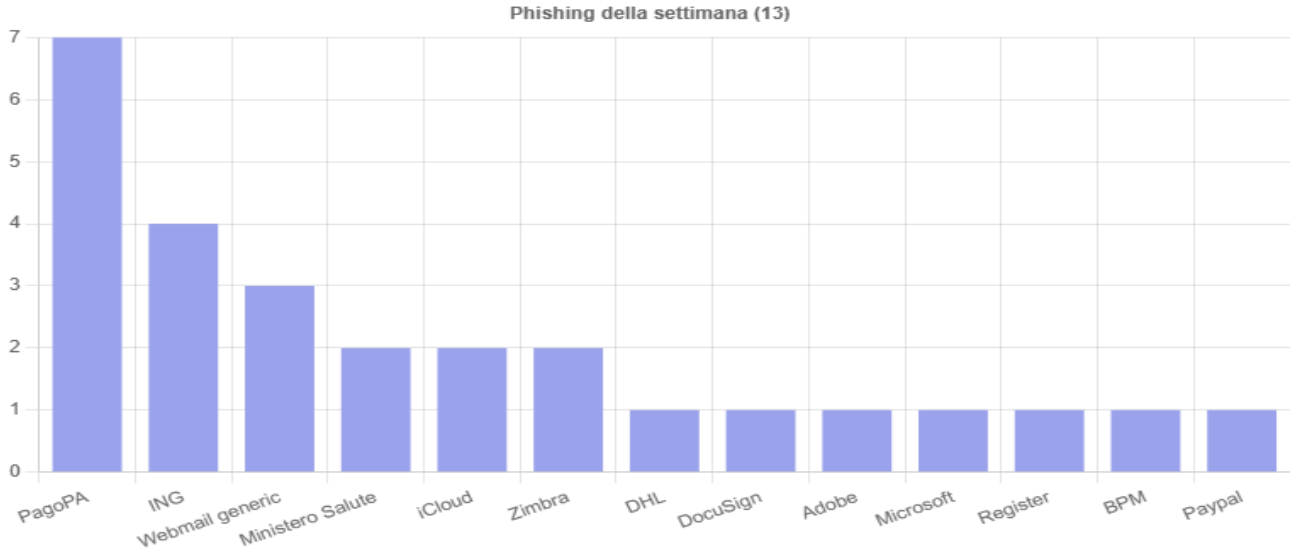
| CVE | CVE-2023-3893 |
|---|---|
| **DESCRIZIONE** | |
| Una vulnerabilità di tipo use-after-free nell'implementazione di SetMouseCapture in mshtml.dll (Microsoft Internet Explorer 6 fino all'11) consente ad aggressori remoti di eseguire codice arbitrario tramite stringhe JavaScript appositamente create. Un esempio di attacco sfrutta un URL del tipo ms-help: che innesca il caricamento di hxds.dll. | |

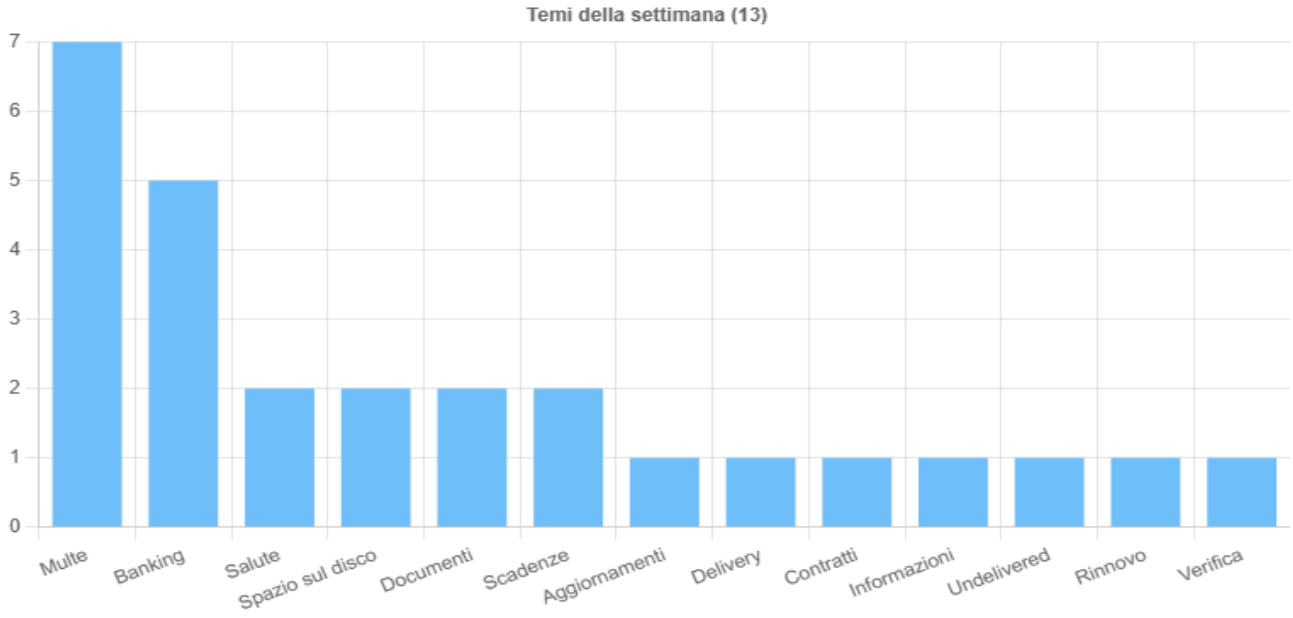
# 4 Attacchi

## 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.

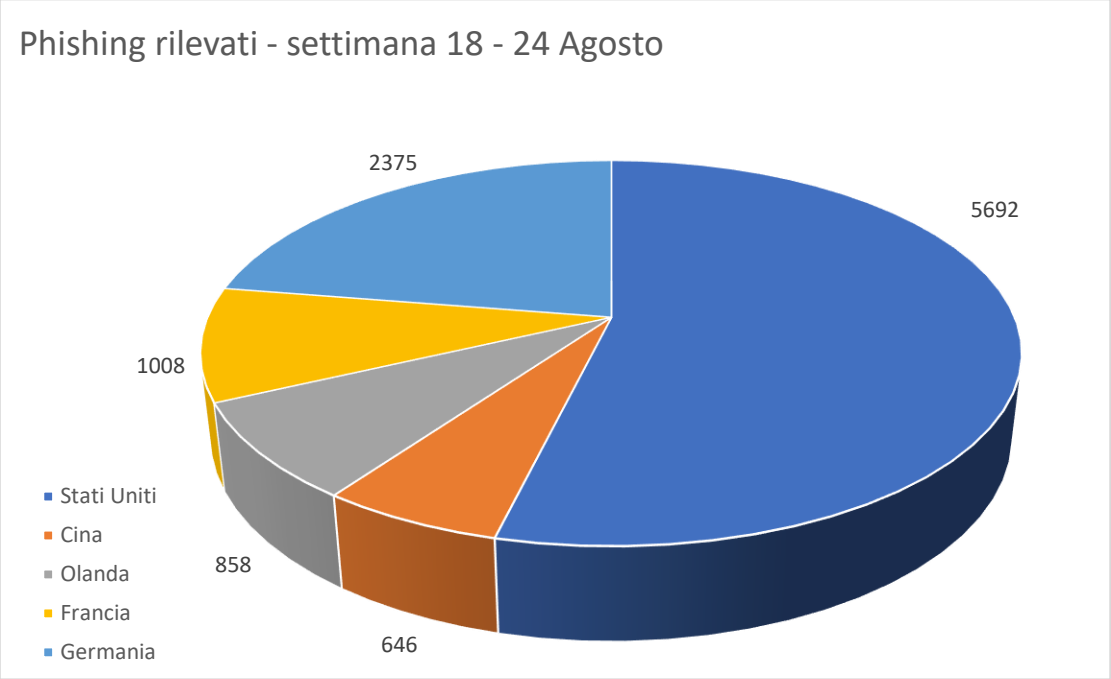



Fonte :CERT-AGID

**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.



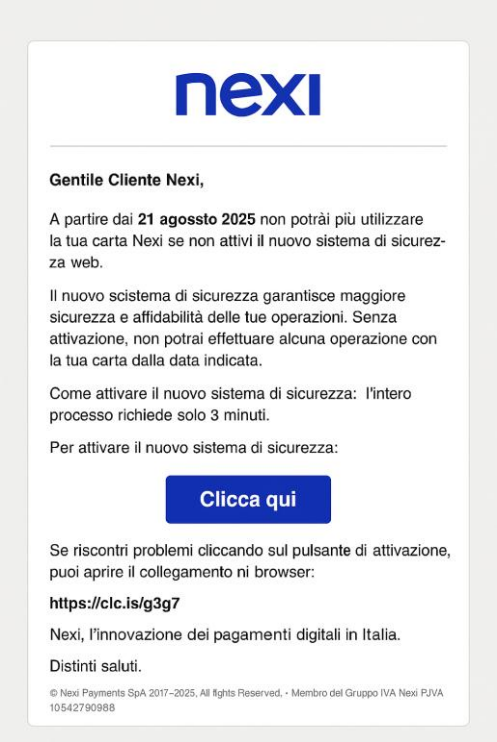

**Report Analisi Email Spoofata**

**Introduzione**

- Il presente report analizza un'email sospettata di essere spoofata, proveniente dal dominio "pagamento-noreply[.]it".
- L'analisi si concentra su vari aspetti tecnici, inclusi header, informazioni OSINT, stato TLS e allegati.
- Inoltre, verranno forniti Indicatori di Compromissione (IoC) e una mappatura secondo il framework MITRE ATT&CK.

**Analisi della email**

- **Aspetto grafico**: l'HTML è strutturato come tipica email commerciale o di notifica bancaria (tabella centrata, font Verdana, colori blu/bianco, pulsante call-to-action).
- **Branding**: viene usato il nome e il logo testuale di **Nexi**, società reale che gestisce carte e pagamenti digitali in Italia.
- **Contenuto**: il testo avvisa che dal *21 agosto 2025* la carta Nexi non sarà più utilizzabile se non si attiva un "nuovo sistema di sicurezza web".
- **Call to action**: invita a cliccare su un link per l'attivazione.




**Indicatori di Phishing**

- **Link sospetti**
  - **Pulsante: https://noisy-fog-4346-afo4.857e3f5179[.]workers[.]dev**

    Questo dominio **non appartiene a Nexi** (che usa nexi.it o sottodomini correlati).È un dominio *workers.dev* → infrastruttura gratuita di **Cloudflare Workers**, spesso usata in campagne di phishing.

  - Link alternativo: https://clc[.]is/g3g7

    Si tratta di un **URL shortener** (clc.is), utilizzato per mascherare la destinazione reale. Anche questo è un indicatore di phishing.

- **Urgenza artificiale**
    - La mail impone una scadenza ("dal 21 agosto 2025 la carta sarà bloccata"), tipico espediente per spingere la vittima a cliccare senza riflettere.
- **Stile e struttura**
    - Anche se l'italiano è corretto, la comunicazione è generica ("Gentile Cliente Nexi"), non personalizzata → altro segnale tipico di campagne massive di phishing.
- **Base64 non valido**
    - Probabilmente il messaggio era originariamente parte di un MIME email con contenuti codificati (es. logo Nexi o tracking pixel).
    - L'indicazione "base64: input non valido" mostra che il contenuto non era un allegato valido → ulteriore indizio che non si tratta di email ufficiale.

**Conclusioni**

- **La mail è un tentativo di phishing**: cerca di far inserire credenziali o dati della carta su un sito non ufficiale.
- **Indicatori principali**:
    - Dominio esterno workers[.]dev (non correlato a Nexi).
    - URL shortener clc[.]is.
    - Messaggio generico e minaccioso ("non potrai più utilizzare la tua carta").
    - Mancanza di contatti ufficiali o riferimenti a canali clienti Nexi.

**Analisi Tecnica**

- **Header**
    - **IP di origine**: 213[.]165[.]249[.]235
    - **Informazioni di autenticazione**: Mancanza di DKIM e DMARC, suggerendo una potenziale falsificazione dell'email.

**OSINT**

- **Dominio:** pagamento-noreply[[.]]it
- **Età:** Registrato in data 18/08/2025
- **Registrar:** non disponibile
- **Flag malware/phishing:** Nessuna evidenza negativa
- **Stato TLS:** impossibile connettersi
- **Hosting IP/ASN:** non disponibile

**TLS**

- Stato TLS per pagamento-noreply[.]it: impossibile connettersi.

**Allegati**

- Non presenti

**Indicatori di Compromissione (IoC)**

| Tipo | Valore |
|---|---|
| Dominio | pagamento-noreply[.]it |
| IP | 213[.]165[.]249[.]235 |
| URL | https://clc[.]is/g3g7 |
| IP | 104[.]21[.]96[.]1 |
| URL | https://noisy-fog-4346-afo4.857e3f5179[.]workers[.]dev/ |
| IP | 172[.]67[.]128[.]146 |

**Mappatura MITRE ATT&CK**

| Tattica | Tecnica | Evidenze |
|---|---|---|
| Impersonation | Email Spoofing | DKIM-Signature Body Hash Not Verified |
| Command and Control | Use of External Remote | IP di origine 213[.]165[.]249[.]235 |

**Analisi Link**

Il link https://clc[.]is/g3g7  mascherato con shortner punta all'indirizzo IP  104[.]21[.]96[.]1

**Analisi IP:  104[.]21[.]96[.]1**

L'analisi dell'indirizzo IP ** 104[.]21[.]96[.]1 ** ha rivelato una serie di informazioni significative attraverso diverse fonti di intelligence sulle minacce.

- **OTX** segnala una reputazione neutra con 25 pulsazioni, e presenta collegamenti a contenuti potenzialmente dannosi.
- **AbuseIPDB** indica un punteggio di fiducia pari a 0 e un totale di 628 rapporti di abuso, suggerendo una certa preoccupazione per l'uso di questo IP.
- **GreyNoise** classifica l'IP come benigno, associandolo a **Cloudflare CDN** e confermando che non è stato ancora segnalato come malevolo.
- I motori di **VirusTotal** mostrano 4 segnalazioni di attività malevola, con un punteggio di reputazione negativo di -135.

In sintesi, sebbene l'IP sia utilizzato da un provider CDN noto e abbia una classificazione benigno da GreyNoise, le segnalazioni di VirusTotal e AbuseIPDB suggeriscono un attento monitoraggio.

**Analisi link https://noisy-fog-4346-afo4.857e3f5179[.]workers[.]dev/|**

La URL è indicata come malevola da vari motori e punta all'indirizzo IP  172[.]67[.]128[.]146

**Risultati dell'Analisi dei  Motori di Sicurezza**

- Google Safebrowsing: Malicious (phishing)
- Lionic: Malicious (phishing)
- Sophos: Suspicious (spam)
- Trustwave: Suspicious

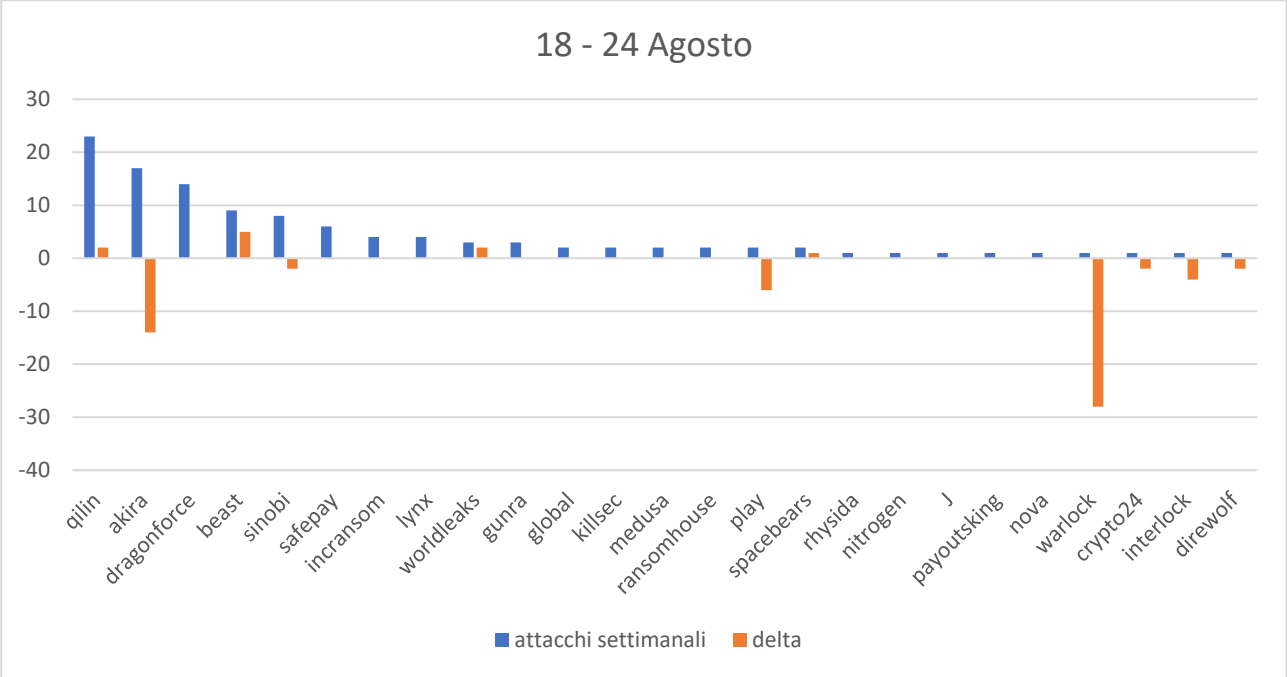
**Riepilogo Rischio**

L'email analizzata presenta un alto rischio di spoofing a causa della mancanza di meccanismi di autenticazione corretti (DKIM, DMARC). L'IP di origine della email ha una reputazione neutra, e non ci sono segnalazioni di abuso ma i link contenenuti nel testo della email sono risultati presenti nei database e indicati come malevoli.

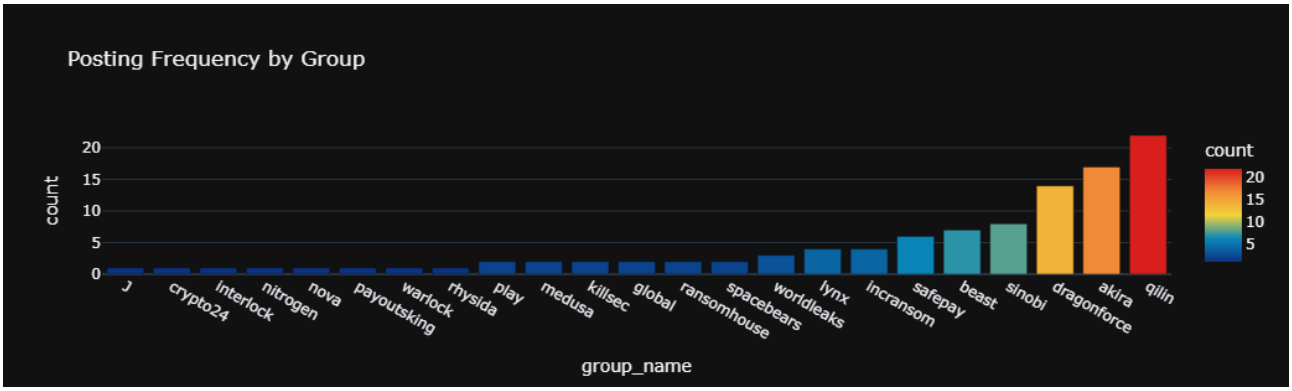
Il fatto che il dominio sia stato registrato il giorno precedente l'invio della email, il contenuto del testo ed i link presenti sono indicatori di attività malevole.

## 4.2 Ransomware

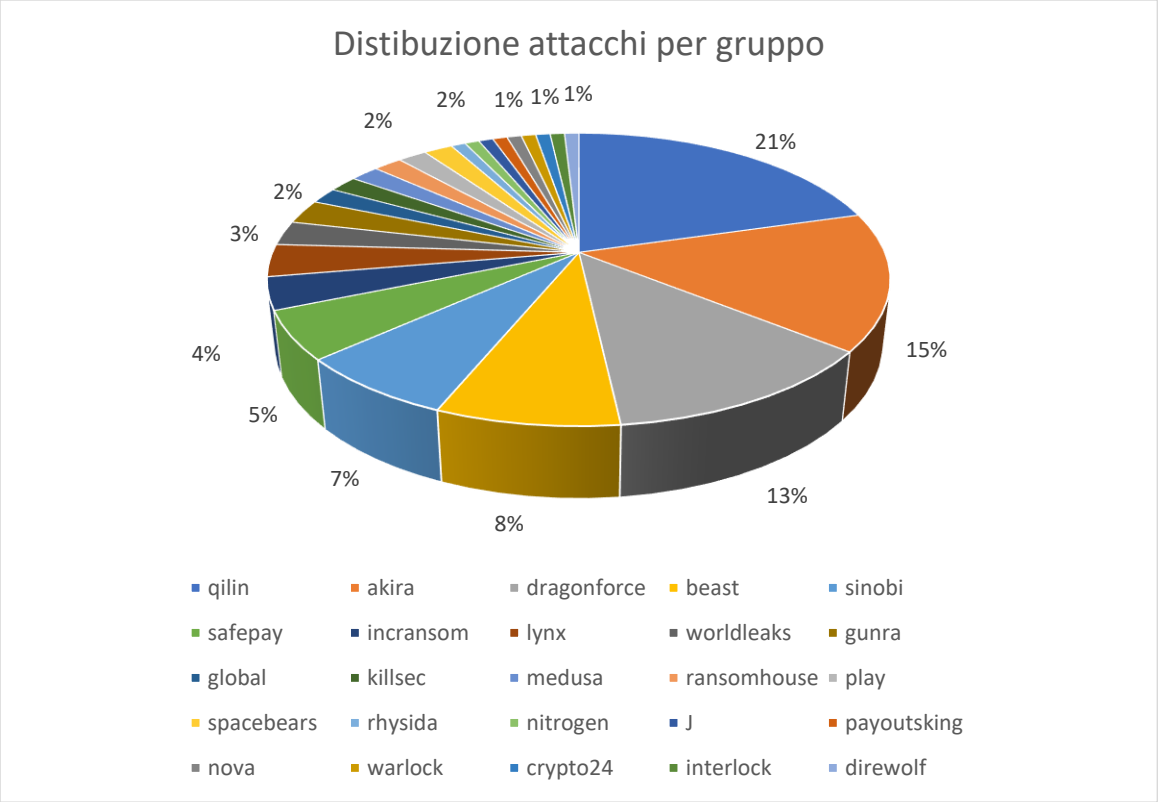
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (18 - 24 Agosto). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).




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

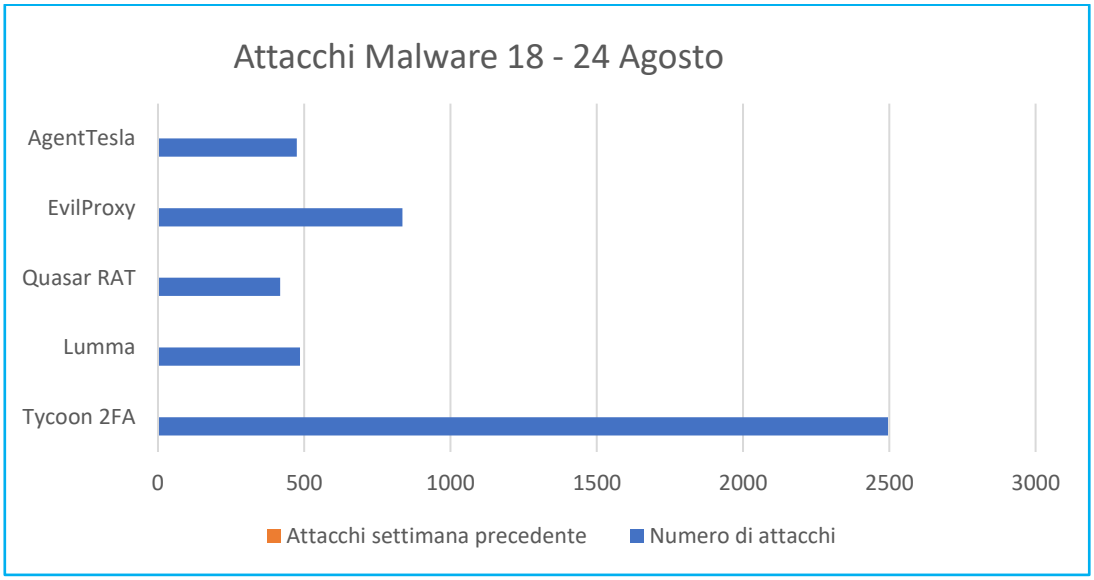


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



## 4.3 Malware

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




(n.b.: attacchi settimana precedente non riportati)

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

- **COOKIE SPIDER – SHAMOS (infostealer macOS)**

SHAMOS è un infostealer per macOS, variante di Atomic MacOS Stealer (AMOS) sviluppata dal gruppo criminale COOKIE SPIDER. Tra giugno e agosto 2025 una campagna malvertising ha convinto le vittime a visitare siti di "supporto macOS" falsi e a eseguire un unico comando da terminale che installava SHAMOS bypassando Gatekeeper. Il malware raccoglie credenziali e dati sensibili (Keychain, browser, portafogli crypto) e li esfiltra via Internet; è stato osservato in Nord America, Europa (inclusa l'Italia) e altri paesi.

**Descrizione tecnica:** infostealer per macOS diffuso come servizio ("malware-as-a-service"). Distribuito via annunci Google sponsorizzati malevoli; invita l'utente a copiare/incollare un comando nel Terminale che scarica ed esegue un file Bash. Questo installa il Mach-O stealer (rimuovendo attributi estesi per sfuggire al Gatekeeper) che quindi esegue AppleScript per raccogliere dati da Apple Notes, Keychain, browser e wallet. Il comando one-line spesso scarica lo script da icloudservers[.]com o mirror simili.

**IoC:**

| Tipo | Indicatore |
|---|---|
| Siti web di malvertising contenenti istruzioni per scaricare SHAMOS | • mac-safer[.]com<br>• rescue-mac[.]com<br>• https[:]//github[.]com/jeryrymoore/Iterm2 |
| URL | Bash script host URLs:<br>• hxxp://macostutorial[.]com/iterm2/install.sh<br>• hxxp://icloudservers[.]com/gm/install.sh<br>*SHAMOS* host URLs<br>• https[:]//icloudservers[.]com/gm/update<br>• https[:]//macostutorial[.]com/iterm2/update |
| Hash SHA256 | • 231c4bf14c374464a2921b0e370e5f512739e803ae47df05f44783afc131d204 (script Bash)<br>• 4549e2599dca14d0c48a783f7f6521d8a3b3be0dd4fbc6764b9c6f138e8cb7ca (SHAMOS Mach-O) |

**MITRE ATT&CK:**

| **ID** | Tecnica | Descrizione |
|---|---|---|
| **T1583.001** | Acquire Infrastructure: Domains | L'attore di eCrime ha registrato falsi siti web di assistenza per macOS |
| **T1189** | Drive-by Compromise | Il malvertising distribuisce siti web contenenti istruzioni di installazione di SHAMOS |
| **T1204** | User Execution | SHAMOS richiede all'utente di eseguire il comando di installazione dannoso |

| | | |
|---|---|---|
| **T1027.010** | Obfuscated Files or Information: Command Obfuscation | Il comando dannoso utilizza la codifica Base64 per offuscare l'URL di download dello script Bash |
| **T1105** | Ingress Tool Transfer | Uno script Bash dannoso scarica SHAMOS da un URL esterno |

**Contromisure:**

- attivare EDR/antivirus con firma comportamentale per rilevare gli script di installazione e i processi sospetti;
- bloccare i domini maliziosi (es. mac-safer[.]com, rescue-mac[.]com) e URL noti.

**Livello di rischio:** Alto (furto di credenziali e dati finanziari su vasta scala).

- **QuirkyLoader (loader multipayload)**

QuirkyLoader è un malware loader multi-stadio scoperto da IBM X-Force (agosto 2025). Viene veicolato via email phishing con allegati compressi che contengono un programma legittimo (.exe), un payload cifrato (.dll malevola) e librerie valide. L'esecuzione dell'EXE legittimo causa il caricamento (side-loading) della DLL malevola, la quale decritta e inietta (hollowing) il payload finale in un processo di sistema (es. AddInProcess32.exe, InstallUtil.exe o aspnet_wp.exe).

I payload consegnati includono comuni stealer e RAT (AgentTesla, AsyncRAT, FormBook, MassLogger, Remcos, Snake Keylogger, ecc.).

**Descrizione tecnica**: Loader .NET compilato con AOT (simula binario nativo). Riceve via email zip cifrati: un eseguibile legittimo (es. vbc.exe) con accanto un .DLL malevolo cifrato. L'EXE carica la DLL, che usa il cifrario Speck-128 in CTR mode per decifrare il payload; quindi esegue il payload attraverso process hollowing. In pratica QuirkyLoader nasconde il caricamento di stealer/RAT di vario genere, rendendo complessa l'analisi statica.

**IoC:**

| Tipo | Indicatore |
|---|---|
| Dominio | • catherinereynolds[.]info<br>• mail[.]catherinereynolds[.]info |
| Indirizzo IP | Indirizzo IP che si risolve in catherinereynolds[.]info:<br>• 157[.]66[.]22[.]11<br>Indirizzo IP correlato a QuirkyLoader:<br>• 161[.]248[.]178[.]212<br>• 103[.]75[.]77[.]90 |

**MITRE ATT&CK:**

| **ID** | Tecnica | Descrizione |
|---|---|---|
| **T1566** | Phishing | Invio di email malevole con allegati per iniziare l'infezione. |
| **T1574.006** | DLL Side-Loading | Caricamento di una DLL malevola al posto di una legittima per eseguire codice non autorizzato. |
| **T1055.012** | Process Hollowing | Iniezione del payload all'interno di un processo legittimo per mascherarne l'esecuzione. |
| **T1027** | Obfuscation | Utilizzo di tecniche di offuscamento per eludere i controlli di sicurezza e rendere difficile l'analisi del codice. |

**Contromisure:**

- Bloccare i messaggi con allegati eseguibili
- Evitare di aprire email inaspettate
- Evitare di aprire file provenienti da fonti non attendibili
- Mantenere i prodotti di sicurezza aggiornati e configurati correttamente
- Poiché i payload finali sono in genere infostealer e strumenti di accesso remoto, monitorare e ispezionare attivamente il traffico di rete in uscita
- Monitorare attentamente il comportamento dei seguenti processi legittimi, poiché sono obiettivi comuni per il process hollowing da parte di QuirkyLoader:
    - AddInProcess32.exe
    - InstallUtil.exe
    - aspnet_wp.exe

**Livello di rischio:** Alto (consegna vari malware informatici ai sistemi compromessi).

- **DarkCloud (nuova variante fileless)**

DarkCloud è uno stealth infostealer per Windows scoperto nel 2022. Fortinet ha identificato a inizio luglio 2025 una nuova variante fileless.

L'infezione inizia con un'email di phishing contenente un archivio RAR/JS fittizio. Il codice JavaScript allegato è offuscato e, una volta eseguito, decodifica al volo un payload PowerShell.

Questo scarica un'immagine JPEG da archive[.]org che contiene nascosta una libreria .NET cifrata. La DLL caricata tramite Powershell effettua process hollowing: scontorna un processo MSBuild sospeso, carica il payload DarkCloud (in memoria) e vi esegue un module infostealer. Il malware esfiltra credenziali, cookie, dati finanziari e informazioni sensibili raccolte nel sistema.

**Descrizione tecnica:** payload multi-fase: l'allegato .js decodifica e avvia uno script PowerShell (es. powershell -w hidden -noprofile -ep bypass -c …) che scarica e decodifica un'immagine JPG da archive[.]org; dalla JPG viene estratta una DLL .NET (named Microsoft.Win32.TaskScheduler per confondere). La DLL implementa persistence via chiave di registro e lancia il payload DarkCloud crittografato in memoria usando process hollowing. Da qui DarkCloud opera come infostealer, raccogliendo dati (password, cookie, crypto wallet, contatti) e inviandoli ai C2.

**IoC:**

| Tipo | Indicatore |
|---|---|
| URL | • hxxps://archive[.]org/download/universe-1733359315202-8750/universe-1733359315202-8750.jpg<br>• hxxp://paste[.]ee/d/0WhDakVP/0 |
| Hash SHA256 | Quote #$_260627.js<br>• 381AA445E173341F39E464E4F79B89C9ED058631BCBBB2792D9ECBDF9FFE027D<br>DarkCloud payload<br>• 82BA4340BE2E07BB74347ADE0B7B43F12CF8503A8FA535F154D2E228EFBEF69C |

**MITRE ATT&CK:**

| ID | Tecnica | Descrizione |
|---|---|---|
| **T1566** | Phishing | Invio di email con allegati malevoli per indurre l'utente ad aprirli. |
| **T1059.003** | Execution via JavaScript | Utilizzo di script JavaScript per eseguire codice malevolo. |
| **T1059.001** | Execution via PowerShell | Comandi PowerShell offuscati per scaricare/eseguire payload. |
| **T1027** | Obfuscation | Utilizzo di tecniche di offuscamento per eludere i controlli di sicurezza e rendere difficile l'analisi del codice. |
| **T1055.012** | Process Hollowing | Tecnica di iniezione per sostituire il codice di un processo legittimo. |

**Contromisure:**

- scansionare le email in entrata per allegati JS sospetti; bloccare domini come archive[.]org (nel contesto malevolo) e servizi paste;
- utilizzare EDR/antivirus per rilevare comportamenti fileless e process hollowing.
- Applicare politiche di restrizione all'uso di script (PowerShell, WScript) da fonti non attendibili;
- fare attenzione ad eseguire o aprire file da email sconosciute.

**Livello di rischio:** Alto (infostealer furtivo con capacità di esfiltrare dati aziendali).

- **Lampion (infostealer bancario via ClickFix)**

Lampion è un nuovo infostealer specializzato in dati bancari, scoperto in una campagna phishing "ClickFix" nel maggio 2025. La campagna ha preso di mira inizialmente organizzazioni portoghesi (ente governo, finanza, trasporti) e poi si è estesa in altri paesi europei.

Il malware si diffonde tramite email di phishing con allegati ZIP/HTML: le vittime sono indotte a seguire un "codice di verifica" che coinvolge eseguire comandi PowerShell sul proprio sistema.

Il risultato sarebbe (ipoteticamente) l'installazione di Lampion, ma in molti casi il payload finale era commentato e non attivato, rivelando l'attenzione degli attaccanti a non farsi scoprire rapidamente. Lampion, se installato, ruberebbe credenziali online e informazioni bancarie.

**Descrizione tecnica:** malware diffuso via tecnica ClickFix (una forma di social engineering): l'utente riceve phishing e viene ingannato a copiare/incollare un comando nel prompt dei comandi/PowerShell. Nella catena di infezione, dopo comandi in PS vengono scaricate più fasi di script (.vbs) che eseguono reconnaissance e infine un comando rundll32 per lanciare Lampion. Lampion è progettato per rubare dati d'accesso (credentiari di online banking, cookie, ecc.) dal sistema della vittima. La campagna Lampion rimane attiva almeno fino a giugno 2025.

**IoC:**

| Tipo | Indicatore |
|---|---|
| URL | • access-ssa-gov[.]es/ClientSetup.exe<br>• applemacios[.]com/vv/install.sh<br>• applemacios[.]com/vv/update<br>• guildmerger[.]co/verify/eminem |
| Dominio | • access-ssa-gov[.]es<br>• binancepizza[.]info<br>• panel-spectrum[.]net<br>• cqsf[.]live<br>• tesra[.]shop |
| Indirizzo IP | • 5.8.9[.]77<br>• 83.242.96[.]159<br>• 3.23.103[.]13<br>• 16.171.23[.]221 |

**MITRE ATT&CK:**

| **ID** | Tecnica | Descrizione |
|---|---|---|
| **T1566** | Phishing | Distribuzione tramite campagne e-mail con allegati malevoli o link ingannevoli. |
| **T1059.001** | Command-Line Interface: PowerShell/CMD | Uso di comandi PowerShell e CMD per scaricare ed eseguire script dannosi. |
| **T1059.001** | Modify registry | Modifica di chiavi di registro per garantire persistenza o configurazioni malevole. |
| **T1027** | Obfuscation | Utilizzo di tecniche di offuscamento per eludere i controlli di sicurezza e rendere difficile l'analisi del codice. |

| | | |
|---|---|---|
| **T1497** | Virtualization/Sandbox Evasion | Tecniche di verifica ambientale per rilevare sandbox o macchine virtuali ed evitare l'analisi. |

**Contromisure:**

- rafforzare filtraggio email e training anti-phishing; disabilitare l'uso del comando Esegui/Power-Shell dai profili non amministrativi come consigliato da Microsoft.
- Implementare XDR/EDR per monitorare attività di script e richieste di rete insolite.
- Aggiornare regolarmente OS/applicativi e utilizzare l'autenticazione a più fattori per gli accessi bancari.
- Gli amministratori di sistema dovrebbero creare regole di "software restrizione" e bloccare gli script obfuscati.

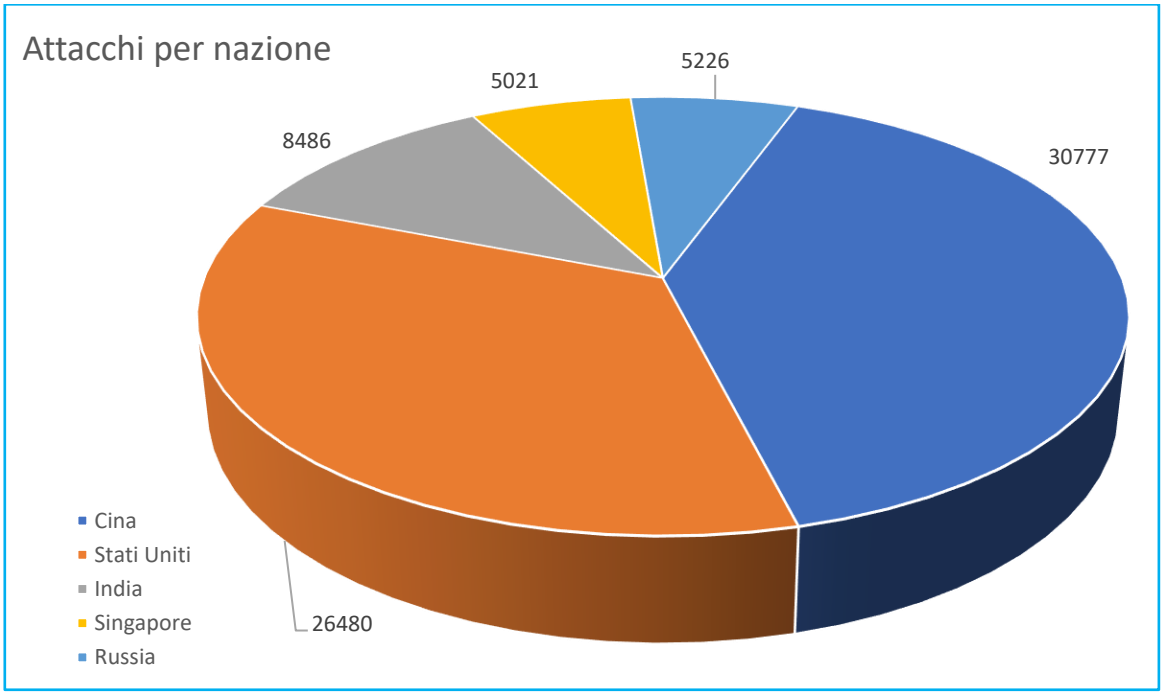
**Livello di rischio**: Alto (potenziale furto di credenziali bancarie anche se nella campagna osservata il payload finale era disattivato).

**Riepilogo:**

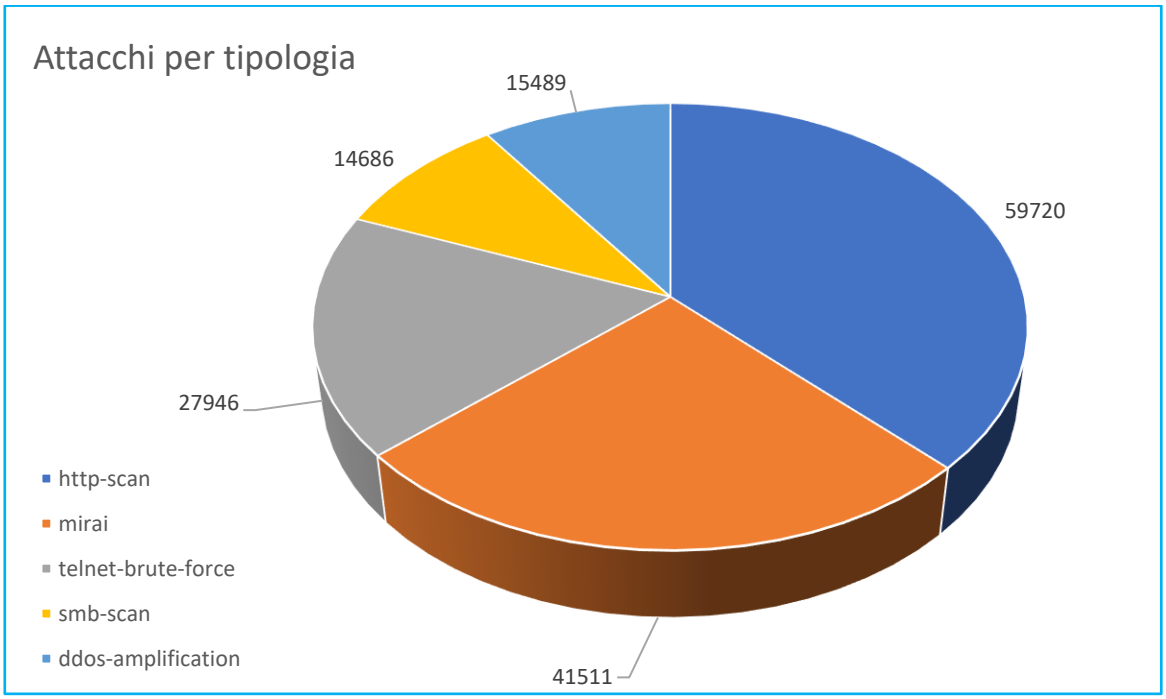
| Malware | Categoria | Livello di rischio |
|---|---|---|
| SHAMOS | Infostealer macOS | Alto |
| QuirkyLoader | Loader multipayload | Alto |
| DarkCloud | Infostealer Windows | Alto |
| Lampion | Infostealer bancario | Alto |

## 4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 18 - 24 Agosto, suddivisa per nazione e limitata alle prime cinque posizioni:

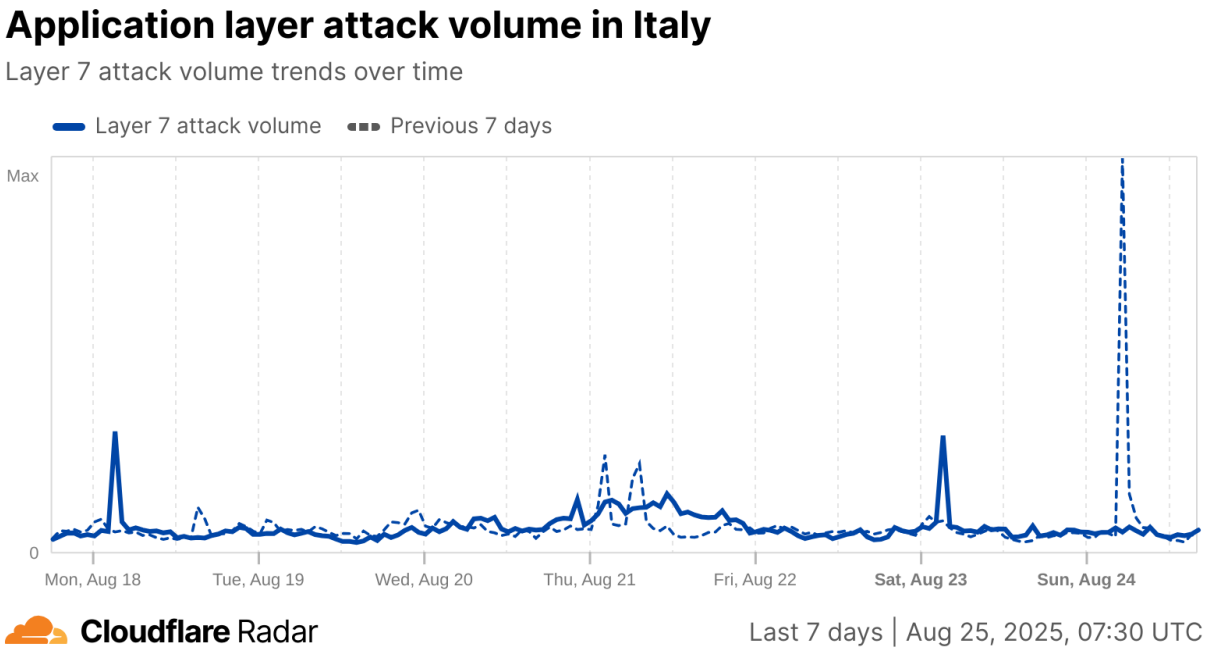


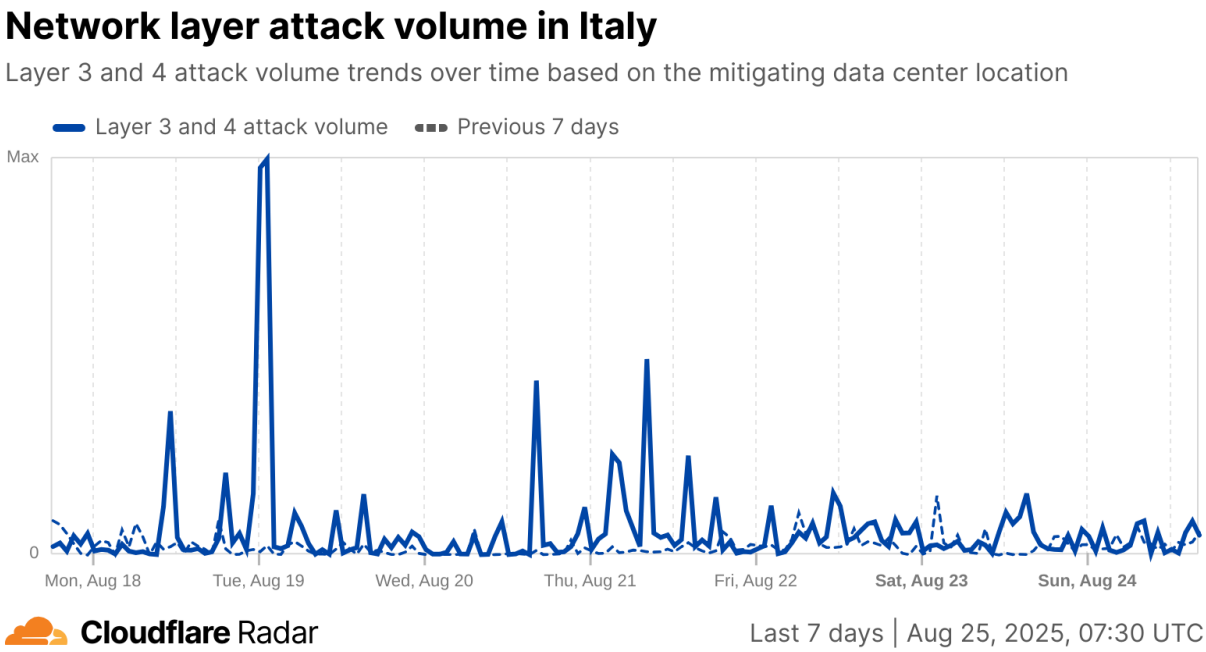

Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



**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 |
|---|---|
| NISSAN MOTOR | GIAPPONE |
| **DESCRIZIONE** | Il laboratorio di design creativo "Nissan Creative Box", di proprietà di Nissan Motor, è stato colpito da un attacco ransomware attribuito al gruppo Qilin, che afferma di aver sottratto oltre 4 terabyte di dati sensibili. Tra i file rubati figurerebbero più di 400.000 documenti, inclusi progetti 3D di veicoli, report, fotografie, video e documentazione interna, potenzialmente legati alla proprietà intellettuale dell'azienda. I criminali hanno anche inserito Nissan nel proprio sito di leak, minacciando di rendere pubblici i dati se l'azienda non dovesse riconoscere l'attacco. |

| TARGET | LOCALIZZAZIONE |
|---|---|
| ADVANCED BLENDING SOLUTIONS | STATI UNITI |
| DESCRIZIONE | Advanced Blending Solutions ha subito una violazione dei dati il 21 agosto 2025, l'attacco è stato attribuito al gruppo di hacker Akira. Tuttavia, i dettagli specifici sull'entità della violazione, come la quantità di dati compromessi o le informazioni esatte coinvolte, non sono stati divulgati pubblicamente. |

| TARGET | LOCALIZZAZIONE |
|---|---|
| EUROFILM MANTZARIS S.A. | GRECIA |
| DESCRIZIONE | Eurofilm Mantzaris S.A., azienda greca specializzata nella produzione di film in polietilene per imballaggi industriali e agricoli, è stata vittima di un attacco informatico significativo il 21 agosto 2025. L'incidente è stato rivendicato dal gruppo di ransomware INC_RANSOM, che ha esfiltrato dati sensibili dall'azienda. Al momento, non sono disponibili dettagli specifici sulla quantità o sul tipo di dati compromessi. Nonostante l'attacco, Eurofilm Mantzaris ha dichiarato di non aver riscontrato prove di accesso non autorizzato ai dati dei clienti. L'azienda ha scelto di non negoziare con gli aggressori, che hanno successivamente pubblicato i dati online. |

## 4.6 Defacement

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

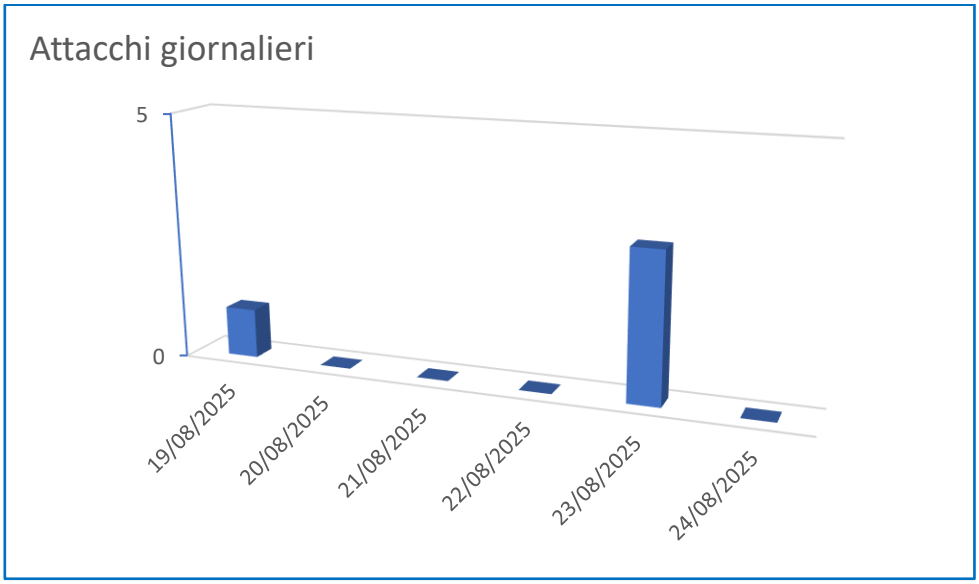



Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

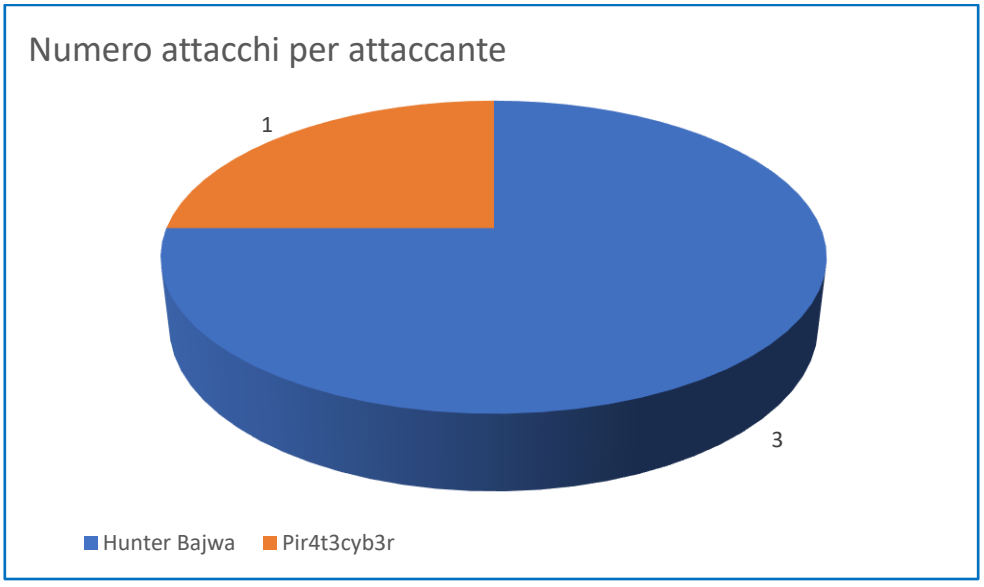



Figura 2: Defacement - Attaccanti più attivi nel periodo 18 - 24 Agosto

# 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

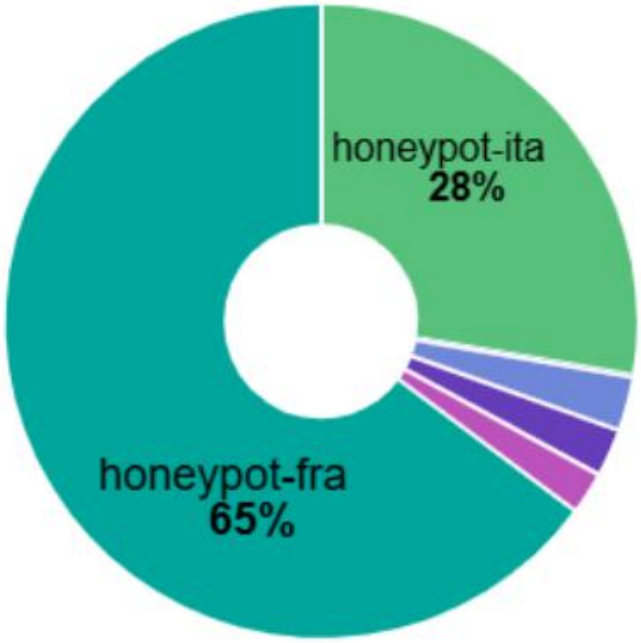
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

**1.575.127** Attacks

**7.559** Unique Src IPs

**67** Unique HASSHs

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




Questa invece la situazione a livello italiano:

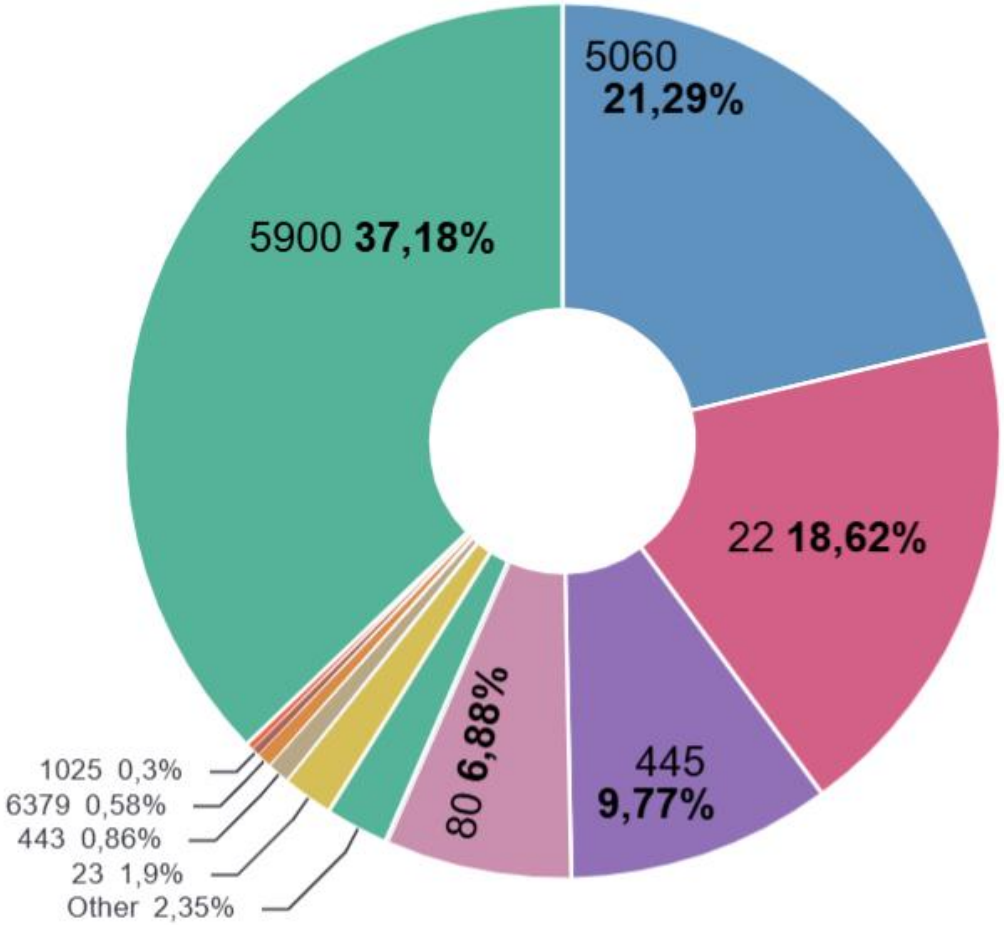
**436.572** Attacks

**4.030** Unique Src IPs

**52** Unique HASSHs

### 5.1.1 Attacchi ai servizi

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



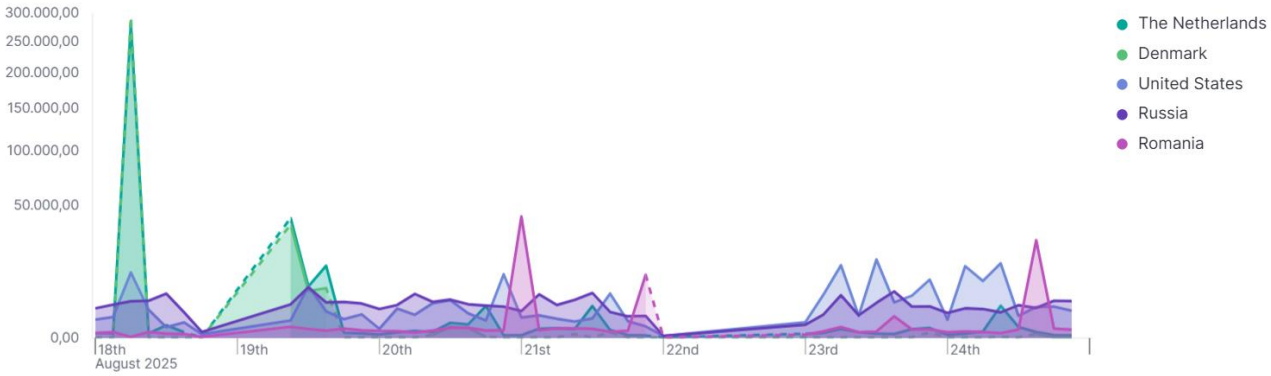

### 5.1.2 IP Attaccanti

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

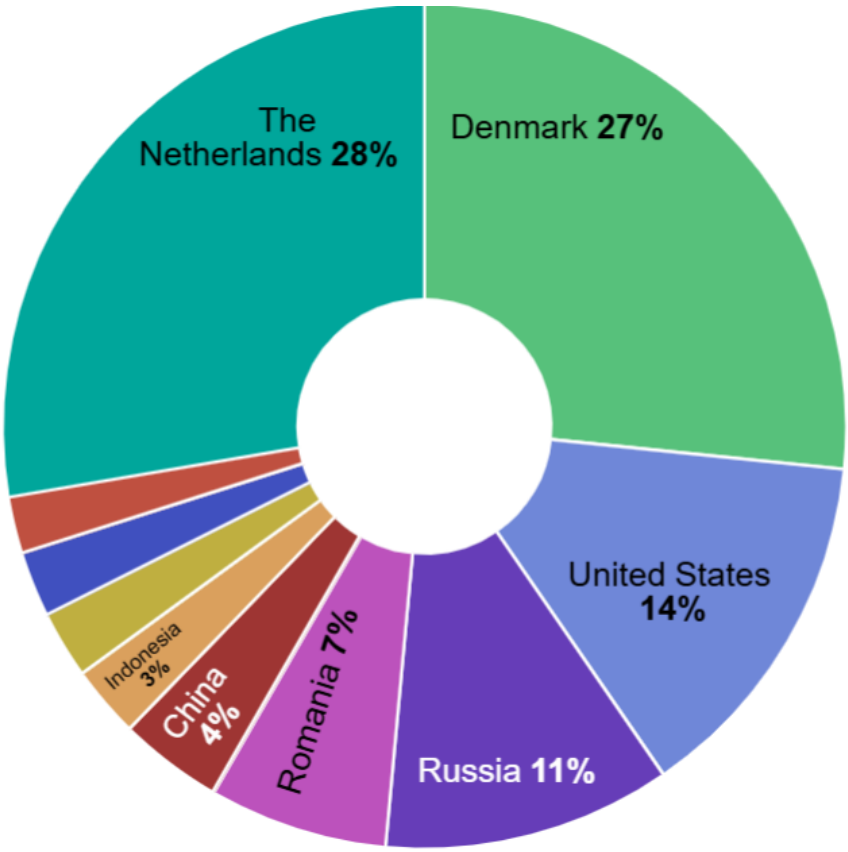
| Source IP | Count |
|---|---|
| 45.144.29.201 | 344.612 |
| 45.14.245.67 | 343.948 |
| 2.57.121.148 | 80.774 |
| 142.202.189.5 | 27.353 |
| 142.202.191.234 | 26.781 |
| 103.91.140.28 | 22.870 |
| 178.22.24.32 | 22.476 |
| 45.134.26.33 | 21.876 |
| 172.81.61.121 | 21.318 |
| 172.81.60.34 | 20.660 |

### 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:

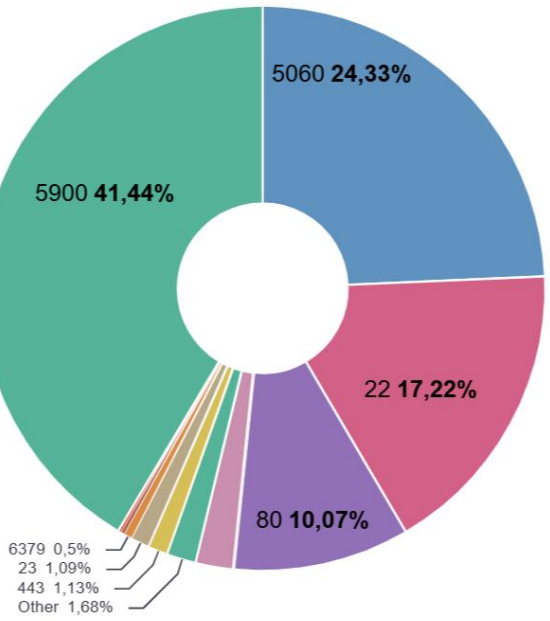


## 5.2 Italian Honeypot N.1

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):




| | |
|---|---|
| 5900 | 81.531 |
| 5060 | 47.867 |
| 22 | 33.876 |
| 80 | 19.804 |
| 445 | 4.214 |
| 443 | 2.229 |
| 23 | 2.146 |
| 6379 | 977 |
| 25 | 408 |
| 1025 | 384 |

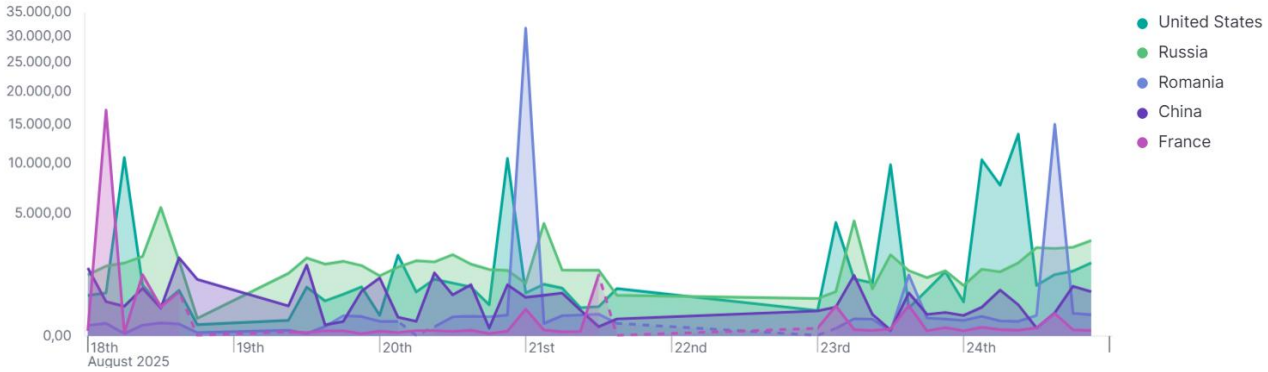
### 5.2.2 IP Attaccanti

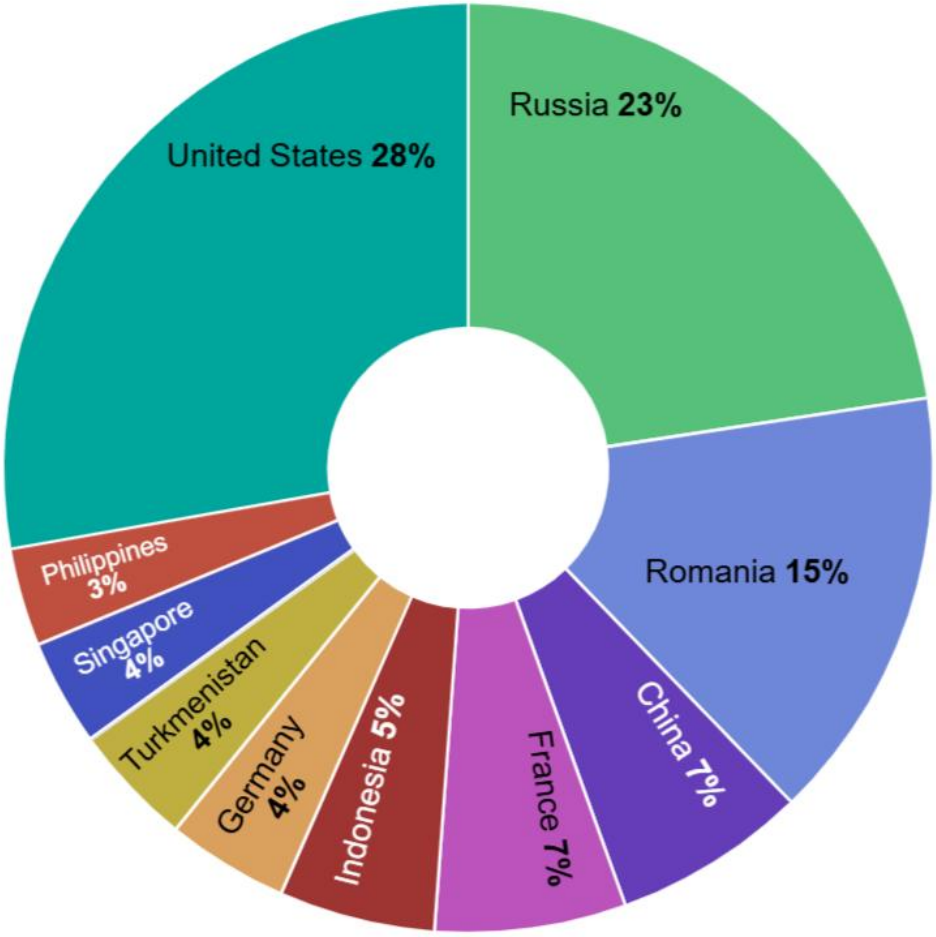
Questa invece la classifica relativa ai 10 IP che hanno effettuato il maggior numero di attacchi:

| Source IP | Count |
|---|---|
| 2.57.121.148 | 46.672 |
| 185.177.72.3 | 17.063 |
| 142.202.189.5 | 16.984 |
| 142.202.191.234 | 15.699 |
| 178.22.24.32 | 12.187 |
| 45.134.26.33 | 11.779 |
| 103.91.140.28 | 11.316 |
| 172.81.61.121 | 11.314 |
| 193.24.123.27 | 10.815 |
| 193.37.69.157 | 10.355 |

### 5.2.3 Paesi di provenienza degli attacchi

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



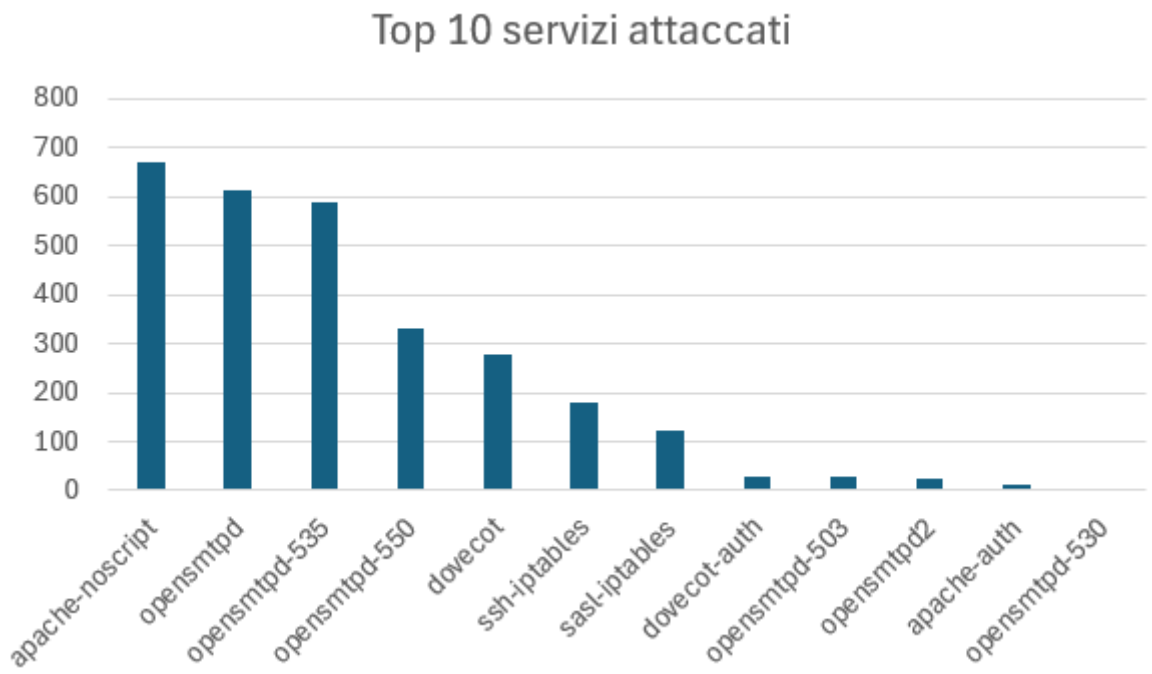

United States 28%
Russia 23%
Romania 15%
China 7%
France 7%
Indonesia 5%
Germany 4%
Turkmenistan 4%
Singapore 4%
Philippines 3%

## 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.




Nella tabella seguente riportiamo una analisi descrittiva della tipologia di attacchi:

| Servizio / Codice | Significato tecnico | Tipologia di attacco tipica | Rischio associato |
|---|---|---|---|
| **apache-noscript** | Attacchi ad Apache su pagine/script non protetti | Exploit di script, RCE, SQL injection, upload malevoli | Compromissione del web server, distribuzione malware |
| **opensmtpd** | Connessioni SMTP generiche | Tentativi di relay abusivo, exploit di vulnerabilità note | Uso come server di spam, RCE |
| **opensmtpd-535** | 535 = Authentication failed | Brute force su credenziali SMTP AUTH | Compromissione account email |
| **opensmtpd-550** | 550 = Mailbox unavailable / Relay denied | Tentativi di relay aperto | Server usato per spam e phishing |
| **dovecot** | Server IMAP/POP3 | Brute force per accesso a caselle email | Furto account, esfiltrazione mail |

| | | | |
|---|---|---|---|
| **ssh-iptables** | Attacchi SSH bloccati da fail2ban/iptables | Brute force su account SSH | Accesso non autorizzato al server |
| **sasl-iptables** | Autenticazioni SASL fallite bloccate | Brute force su autenticazione email (SMTP AUTH) | Compromissione account email |
| **dovecot-auth** | Autenticazione Dovecot specifica | Brute force su POP3/IMAP | Compromissione account di posta |
| **opensmtpd-503** | 503 = Bad sequence of commands | Scanner SMTP mal configurati | Ricognizione, tentativi di exploit |
| **opensmtpd-502** | 502 = Command not implemented | Comandi SMTP non validi → test di relay | Identificazione di configurazioni vulnerabili |

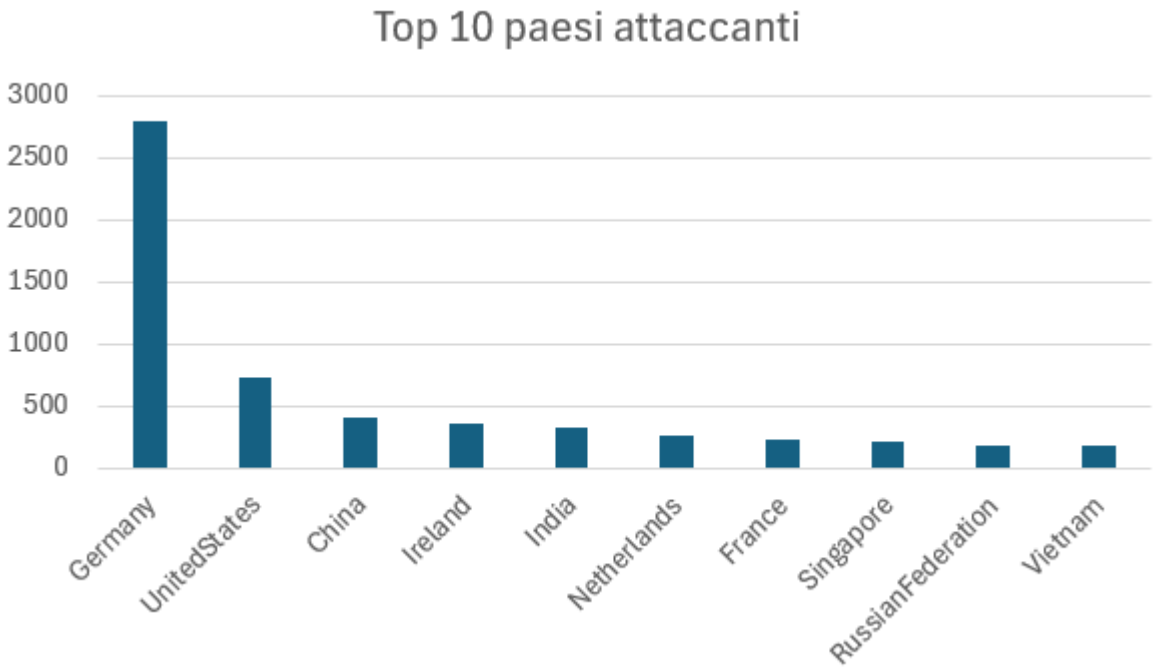
### 5.3.2 IP attaccanti

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 |
|---|---|
| 178[.]162[.]136[.]160 | 157 |
| 185[.]176[.]220[.]50 | 32 |
| 185[.]93[.]89[.]60 | 26 |
| 198[.]55[.]98[.]176 | 24 |
| 62[.]173[.]141[.]210 | 23 |
| 196[.]251[.]92[.]124 | 18 |
| 37[.]142[.]91[.]15 | 16 |
| 62[.]149[.]158[.]101 | 15 |
| 165[.]154[.]118[.]28 | 15 |
| 14[.]191[.]36[.]157 | 14 |

### 5.3.3 Paesi di provenienza degli attacchi

Questa invece la distribuzione dei paesi attaccanti:



# 6 Company Profile S3K

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

**COME LO FACCIAMO:**

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

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

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

**CON QUALI LEVE OPERIAMO:**

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

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

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

**CHI SIAMO:**

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

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

**LA NOSTRA MISSION:**

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

**I NOSTRI VALORI:**

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

**CONTATTI:**

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

**DISCLAIMER**

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

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

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

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

**CLASSIFICAZIONE DOCUMENTO**

**2.0 TLP:AMBER** = 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

ISO 14001 BUREAU VERITAS Certification
ISO 27001 BUREAU VERITAS Certification
ISO 9001 BUREAU VERITAS Certification
ISO 45001 BUREAU VERITAS Certification