S3K

Cyber security

RISK REPORT

\ week 16.06.2025 - 22.06.2025

Sommario


CYBER SECURITY RISK REPORT
25/25

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 Contenuti di questo numero

Il presente **Cyber Security Risk Report S3K** rappresenta un'analisi dettagliata delle minacce informatiche rilevate nella settimana 16-22 giugno 2025. Questo bollettino settimanale è uno strumento indispensabile per i professionisti della sicurezza informatica, fornendo informazioni aggiornate sulle vulnerabilità emergenti, gli attacchi in corso e le raccomandazioni di sicurezza prioritarie.

1.2 Sommario dei contenuti del report

Questo report analizza le principali minacce cyber emerse nella settimana 16-22 giugno 2025. Tra gli elementi principali: aggiornamenti critici rilasciati da Microsoft per 68 vulnerabilità, attacchi a oltre 80.000 account Microsoft Entra ID, e importanti patch di sicurezza per ClamAV, Cisco Meraki e Google Chrome. Il report documenta l'attività dei gruppi ransomware BlackCat/ALPHV, Qilin e 8Base, oltre a dettagliare campagne di phishing sofisticate che impersonano persone reali. Analisi dei dati honeypot rivelano

attacchi prevalenti da Cina, Stati Uniti e Russia, con focus sui servizi SSH, Telnet e SMB. Particolare attenzione è data a una nuova versione del malware Godfather su Android e agli attacchi di defacement contro siti italiani da parte del gruppo xNot_RespondinGx.

1.3 Security News

Aggiornamenti critici da Microsoft, Tenable e Palo Alto Networks. Patch importanti per 68 vulnerabilità, incluse 2 zero-day. Campagna di attacchi che ha colpito oltre 80.000 account Microsoft Entra ID. Operazione coordinata tra FBI e forze europee per la chiusura di domini utilizzati per supportare ransomware.
Dettagli a questo link : "Cyber News" dal Web, Deep Web e Dark Web

1.4 Vulnerabilità critiche

Alta intensità di vulnerabilità in prodotti Microsoft Windows, Adobe, SAP, Dell, IBM, SolarWinds e plugin WordPress. CVE-2025-32711 (Microsoft M365 Copilot) che consente l'iniezione di comandi AI e diverse vulnerabilità nei sistemi Windows RRAS che permettono l'esecuzione di codice remoto attraverso heap overflow.
Dettaglia questo link : CVE Monitor

1.5 Attacchi

Incremento degli attacchi phishing che impersonano persone reali usando dati aziendali autentici. Gruppi ransomware più attivi: BlackCat/ALPHV, Qilin e 8Base. Malware di rilievo: MassJacker, Sosano, Gremlin Stealer, StilachiRAT e Interlock. Data breach significativi hanno colpito Zoomcar Holdings, WestJet e il Dipartimento della Cultura di Abu Dhabi.
Dettagli a questo link : Attacchi

1.6 Honeypot

Predominanza di attacchi da Cina, Stati Uniti e Russia. Servizi più colpiti: SSH (porta 22), Telnet (porta 23) e SMB (porta 445). In Italia, intensificazione degli attacchi verso HTTP (porta 80) e RDP (porta 3389), con significativa provenienza da Cina, Regno Unito e Stati Uniti.
Dettagli a questo link : Honeypot

1.7 Cyber News dal Web, Deep Web e Dark Web

1.7.1 Defacement di siti italiani

Il gruppo hacker xNot_RespondinGx ha condotto una serie di attacchi di defacement contro almeno quindici portali italiani, lasciando su ciascun sito un messaggio in indonesiano: "menikmati sisa hidup sebelum ajal menjemputku" (Assaporare ciò che resta della vita prima che la morte mi raggiunga). Tra i siti colpiti figurano aziende di servizi, piattaforme commerciali e siti tecnici, evidenziando la fragilità delle infrastrutture web italiane.

1.7.2 Nuova variante del malware Godfather

È stata individuata una nuova evoluzione del malware Android Godfather, capace di creare ambienti isolati all'interno dei dispositivi per eseguire applicazioni bancarie in modo nascosto. Questa versione aggiornata prende di mira oltre 500 applicazioni bancarie, di e-commerce e criptovalute a livello globale, utilizzando tecniche avanzate come un file system virtuale e componenti StubActivity per intercettare i dati sensibili degli utenti.

1.8 Raccomandazioni prioritarie

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

Il Cyber Security Risk Report S3K è elaborato dagli analisti di S3K che raccolgono ed esaminano dati da molteplici fonti, inclusi produttori di hardware e software, ricercatori di sicurezza, forum dedicati, canali di comunicazione dei gruppi cybercriminali, e monitoraggio del deep/dark web. La combinazione di dati analitici, tendenze emergenti e raccomandazioni pratiche fornisce ai professionisti della sicurezza informatica un quadro completo del panorama delle minacce, consentendo decisioni informate e interventi tempestivi.

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
ClamAV	Rilasciato un aggiornamento di sicurezza che mira a sanare due vulnerabilità, di cui una con gravità "critica", relativamente al prodotto ClamAV di Cisco. Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato di causare l'indisponibilità del servizio e/o l'esecuzione di codice arbitrario sui sistemi interessati. Versioni affette: • ClamAV, versioni precedenti alla 1.4.3 • ClamAV, versioni precedenti alla 1.0.9
ULR/Note	https://blog.clamav.net/2025/06/clamav-143-and-109-security-patch.html

PRODOTTO	DESCRIZIONE
Cisco Meraki MX, Cisco Meraki Z	Aggiornamento di sicurezza sana una nuova vulnerabilità, con gravità "alta", che riguarda la componente Cisco AnyConnect VPN server dei prodotti Cisco Meraki MX e Cisco Meraki Z. Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato di causare l'indisponibilità del servizio sui sistemi interessati. Versioni affette: • Meraki MX • Meraki Z
ULR/Note	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-sM5GCfm7

PRODOTTO	DESCRIZIONE
Chrome	Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere tre vulnerabilità di sicurezza, di cui due con gravità "alta". Versioni affette: • versioni precedenti alla 137.0.7151.119/.120 per Windows e Mac • versioni precedenti alla 137.0.7151.119 per Linux
ULR/Note	https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop_17.html

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

ONDATE DI DEFACEMENT COLPISCONO SITI ITALIANI: RIVENDICAZIONE DEL GRUPPO XNOT_RESPONDINGX

Negli ultimi giorni, una serie di attacchi informatici ha preso di mira numerosi portali italiani: sono almeno quindici i siti web coinvolti in un'azione coordinata di defacement. La responsabilità è stata rivendicata dal gruppo hacker conosciuto come xNot_RespondinGx, che ha lasciato un file denominato readme.txt su ciascuna piattaforma colpita, contenente un messaggio ben preciso. Tra le vittime si contano portali appartenenti a settori eterogenei: aziende di servizi, realtà commerciali online, strutture private e siti tecnici. Di seguito alcuni dei domini violati:

- https://www.languageteam.it
- https://www.ficusbarbistrot.it
- https://giuliettaallago.it
- https://www.servicewebsrl.it
- https://shoptechim.joyadv.it
- https://www.techimgroup.it
- https://prenotazioni.ristopollicino.it
- https://www.sape.it
- https://shop.speedyblock.it
- https://www.simasrl.it
- https://www.service3cleaning.it
- https://www.vistadarsena.it
- https://mymi.it/readme.txt
- https://www.strumentidiserraggio.it
- https://www.vinoungherese.it

Ogni sito presenta lo stesso identico messaggio: "menikmati sisa hidup sebelum ajal menjemputku", una frase in lingua indonesiana traducibile come "Assaporare ciò che resta della vita prima che la morte mi raggiunga". Questo tipo di messaggio potrebbe essere stato scelto non solo per trasmettere un senso esistenziale, ma anche per catturare l'attenzione con un tono cupo e profondo. Non è la prima volta che il collettivo si rende protagonista di episodi simili: in precedenza aveva inserito sui siti violati la frase "L'amore può dare forza alle persone, ma a volte le rende deboli", segno di uno stile comunicativo che unisce hacking e messaggi emotivamente forti. L'operazione portata avanti da xNot_RespondinGx evidenzia chiaramente la fragilità di molte infrastrutture web italiane. Sebbene queste incursioni non abbiano avuto come obiettivo il furto di dati o l'interruzione dei servizi, mettono in luce gravi carenze nella sicurezza informatica. È fondamentale che organizzazioni, aziende e gestori di portali online prendano coscienza del rischio e intervengano tempestivamente: mantenere aggiornate le tecnologie, rafforzare le protezioni e garantire un monitoraggio continuo sono misure indispensabili per tutelare i propri utenti e prevenire danni più gravi in futuro.

NUOVA VERSIONE DEL MALWARE GODFATHER SCOPERTA SU ANDROID

Una nuova evoluzione del malware Android Godfather è stata individuata pochi giorni fa; questa versione aggiornata è in grado di creare ambienti isolati all'interno dei dispositivi, dove esegue applicazioni bancarie in modo nascosto, permettendo ai cybercriminali di sottrarre dati sensibili e manipolare transazioni. Il malware Godfather è noto dal marzo 2021, quando fu analizzato per la prima volta da ThreatFabric. Nel tempo ha subito trasformazioni sostanziali, molto diverse rispetto alla variante esaminata da Group-IB a fine 2022, che allora aveva colpito circa 400 app di banche e servizi di criptovalute in 16 paesi attraverso schermate HTML falsificate. Secondo quanto riportato dagli esperti di sicurezza di Zimperium, l'ultima incarnazione del malware agisce creando un ambiente virtuale controllato sullo smartphone della vittima. Questo sistema permette di monitorare le attività dell'utente in tempo reale, accedere a credenziali bancarie e prendere il controllo di alcune funzionalità dell'app, il tutto mantenendo un livello elevato di furtività. Tattiche simili erano state osservate per la prima volta nel 2023 con FjordPhantom, un altro trojan Android che utilizzava container virtuali per evitare i controlli di sicurezza. A differenza di FjordPhantom però, Godfather ha un raggio d'azione più ampio e punta ad oltre 500 applicazioni, non solo bancarie ma anche di e-commerce e criptovalute, con una presenza significativa in diverse regioni del mondo. Tra le tecniche utilizzate vi sono l'impiego di un file system virtuale, un identificatore di processo simulato, l'Intent spoofing e una componente chiamata StubActivity. Quest'ultima è una sorta di "attività fantasma" integrata nel malware, che non ha un'interfaccia propria ma funge da tramite tra l'utente e l'app bersaglio, che viene eseguita all'interno di un contenitore virtuale. Questo stratagemma fa sì che Android creda di eseguire l'app legittima, mentre in realtà è il malware a gestirne l'avvio e l'interazione. Il pacchetto malevolo viene distribuito in formato APK e include un motore di virtualizzazione, spesso basato su progetti open source come VirtualApp e Xposed, utilizzati per intercettare le chiamate di sistema e monitorare l'attività dell'utente. Quando il malware si attiva su un dispositivo compromesso, cerca app specifiche già installate. Se ne trova, le integra nel suo ambiente virtuale e ne avvia l'esecuzione tramite StubActivity. L'utente continua a vedere l'interfaccia originale dell'app bancaria, ma in realtà tutto il traffico e i dati vengono intercettati da Godfather. Inoltre, il malware può utilizzare overlay ingannevoli per spingere l'utente a digitare PIN, password o altri dati sensibili nei momenti chiave. Una volta raccolti i dati, questi vengono inviati ai server remoti degli aggressori, che possono impartire ulteriori comandi: autorizzare trasferimenti di denaro, sbloccare il dispositivo o interagire con l'interfaccia utente per finalizzare operazioni finanziarie. Per mascherare le sue attività, Godfather visualizza schermate fittizie di aggiornamento o schermi neri, in modo da non destare sospetti nell'utente.

Sebbene l'attività individuata da Zimperium sembri focalizzarsi su alcune app bancarie turche, gli esperti mettono in guardia: è possibile che il malware venga adattato rapidamente per attaccare altri sottoinsiemi delle centinaia di applicazioni potenzialmente a rischio in tutto il mondo.

ATTACCO HACKER ALL'AZIENDA SANITARIA DI PALERMO, IN CORSO LE INDAGINI

L'Azienda Sanitaria Provinciale di Palermo, il 19 giugno, ha confermato di essere stata vittima di un attacco informatico, dopo che nei giorni scorsi si erano registrati rallentamenti e anomalie nei servizi. L'incidente si è verificato il 18 giugno e ha interessato circa 45 postazioni di lavoro interne. Al momento, non è ancora possibile stabilire con precisione quali sedi o reparti siano collegati alle postazioni compromesse. Dalle prime verifiche, risulta che tra i dati potenzialmente coinvolti potrebbero esserci informazioni personali come dati anagrafici, recapiti, elementi relativi a pratiche amministrative e altre tipologie di dati ancora in fase di accertamento. L'Azienda precisa che, non potendo identificare con certezza tutte le persone coinvolte, la comunicazione pubblica è stata diffusa anche come misura di notifica alternativa, così come previsto dal Regolamento Europeo sulla protezione dei dati personali. Per contenere l'impatto dell'attacco e limitare ulteriori conseguenze, l'ASP ha avviato tempestivamente una serie di interventi. Le postazioni compromesse sono state isolate, sono state attivate le procedure interne di sicurezza e avviate analisi tecniche approfondite. Inoltre, l'accaduto è stato segnalato al Garante per la Protezione dei Dati Personali, come richiesto dalla normativa, e sono in corso collaborazioni con le autorità competenti per portare avanti le indagini. Nel frattempo, l'ASP invita tutti gli utenti a mantenere alta l'attenzione. In particolare, si consiglia di non rispondere a messaggi sospetti, di verificare con cura mittenti e oggetti delle email ricevute e di monitorare eventuali attività insolite sui propri account personali. È inoltre importante non fornire informazioni sensibili via email o telefono, soprattutto se si ricevono richieste non attese.

MALFUNZIONAMENTI SU ONEDRIVE: BUG NELLA RICERCA E NEI LINK ALLE CARTELLE CONDIVISE

Microsoft ha recentemente segnalato un problema importante riguardo gli account personali di OneDrive, che causa un malfunzionamento nella funzione di ricerca. Molti utenti non riescono più a trovare i file all'interno del proprio spazio cloud, anche se sanno che sono presenti. Questo disservizio ne compromette fortemente l'utilizzo, rendendo difficile l'accesso rapido ai documenti tramite la ricerca. L'azienda ha aperto un'indagine per capire le cause di questo bug, che al momento sembra colpire solo una parte degli utenti. Sebbene i file restino raggiungibili esplorando manualmente le cartelle, la mancata restituzione dei risultati nelle ricerche sta creando problemi a chi si affida alla funzione per lavorare in modo efficiente. Oltre a questo, diversi utenti hanno riscontrato un altro problema legato ai collegamenti alle cartelle condivise di OneDrive, che appaiono come semplici file .url (collegamenti internet) invece che come cartelle vere e proprie. Ciò causa disagi ulteriori, soprattutto quando si tenta di aprire questi link, poiché gli utenti vengono spesso reindirizzati a pagine web che richiedono un nuovo login, anziché accedere direttamente ai contenuti condivisi. Microsoft ha confermato che non esistono soluzioni temporanee efficaci per il problema della ricerca e ha consigliato agli utenti di affidarsi alla navigazione manuale delle cartelle finché non verrà rilasciata una patch definitiva. Per il problema dei link alle cartelle condivise, invece, ha suggerito di collegarsi prima direttamente al sito onedrive.com per evitare errori di autenticazione quando si apre un collegamento. Questi malfunzionamenti stanno avendo un impatto significativo sia su utenti privati che su aziende che utilizzano OneDrive come strumento quotidiano per archiviare e accedere ai propri file. Microsoft ha dichiarato di essere al lavoro con priorità assoluta per risolvere queste criticità, riconoscendo in particolare il blocco della funzionalità di ricerca come un ostacolo grave per la produttività. Per fronteggiare temporaneamente il problema, l'azienda ha iniziato a distribuire una correzione e ha proposto alcune soluzioni alternative. Tra queste, suggerisce di uniformare le impostazioni della lingua del profilo Microsoft con quelle del computer o di rinominare la cartella Personal Vault per migliorare la sincronizzazione delle preferenze linguistiche, in attesa che la patch definitiva venga resa disponibile.

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 16- 22 Giugno 2025
Settimana molto attiva con disclosure critici riguardanti dispositivi di rete (D-Link, UTT, Cisco), sistemi libxml2, prodotti WordPress, e piattaforme enterprise come IBM QRadar e ClamAV. Sono presenti exploit pubblici per molte vulnerabilità, incluse quelle relative a router e plugin WP.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Descrizione Sintetica
CVE-2025-6098	CRITICAL	16/06/2025	✅ GitHub	UTT 750W: buffer overflow remoto su API setSysAdm.
CVE-2025-6121	CRITICAL	16/06/2025	✅ GitHub	D-Link DIR-632: stack overflow remoto via HTTP POST.
CVE-2025-6169	CRITICAL	16/06/2025	❌	HAMASTAR WIMP CMS: SQLi non autenticata su endpoint sconosciuto.
CVE-2025-49794	CRITICAL	16/06/2025	❌	libxml2: use-after-free parsing XPath con schematron sch:name.
CVE-2025-49796	CRITICAL	16/06/2025	❌	libxml2: memory corruption parsing sch:name → DoS o RCE.
CVE-2025-1562	CRITICAL	18/06/2025	✅ Wordfence	WP FunnelKit: installazione plugin arbitrari da remoto (non autenticato).
CVE-2025-20260	CRITICAL	18/06/2025	❌	ClamAV: buffer overflow parsing file PDF → DoS / potenziale RCE.
CVE-2025-4738	CRITICAL	19/06/2025	❌	MY ERP (Yirmibes): SQLi non autenticata su tutte le versioni < 1.170.
CVE-2025-33117	CRITICAL	19/06/2025	❌	IBM QRadar SIEM: utente privilegiato può caricare aggiornamenti malevoli (command injection).

Vendor e Tecnologie Coinvolti

- **Router e dispositivi di rete:** D-Link DIR-632, UTT 750W con overflow gravi e PoC pubblici.
- **CMS e gestionali:** SQLi su WIMP (Hamastar), MY ERP (Yirmibes) – accesso remoto senza login.
- **WordPress:** FunnelKit Plugin – rischio di compromissione completa via plugin upload arbitrari.
- **Enterprise:**
    - **IBM QRadar:** command injection con privilegi elevati.
    - **ClamAV:** overflow su file PDF → potenziale RCE.
    - **libxml2:** use-after-free e memory corruption da XML malevoli.

Distribuzione Giornaliera

- **16 giugno:** Disclosure massiccio (UTT, D-Link, libxml2, WIMP).
- **18 giugno:** Vulnerabilità critiche su WordPress (FunnelKit) e ClamAV.
- **19 giugno:** Advisory IBM QRadar e MY ERP.

Raccomandazioni

- **Patch Prioritarie:**
    - Router D-Link/UTT esposti su rete WAN.
    - WordPress + FunnelKit → rimozione immediata o aggiornamento.
    - Sistemi XML parsing (libxml2): attenzione a input esterni/XML da terze parti.
    - IBM QRadar → aggiornamento config file e controllo integrità.
- **Monitoraggio:**
    - CVE con PoC confermati (DIR-632, UTT, FunnelKit).
    - Query SQL sospette su gestionali WIMP e MY ERP.
    - Scan file PDF con ClamAV → possibile vettore di crash o exploit.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-31200	tvOS (versione 18.4.1), visionOS (versione 2.4.1), iOS e iPadOS (versione 18.4.1), macOS Sequoia (versione 15.4.1)	N/A
CVE-2025-30401	WhatsApp per Windows (versioni precedenti alla 2.2450.6)	N/A
CVE-2025-24201	visionOS (versione 2.3.2), iOS e iPadOS (versioni 18.3.2, 17.7.6, 16.7.11, 15.8.4), macOS Sequoia (versione 15.3.2), Safari (versione 18.3.1), watchOS (versione 11.4)	N/A
CVE-2025-3248	Langflow (Strumento visuale per collegare modelli linguistici AI)	N/A
CVE-2025-4275	InsydeH2O (UEFI/Bios)	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-2025-33117	IBM QRadar SIEM	N/A
VULNERABILITÀ	IBM QRadar SIEM dalla versione 7.5 fino alla 7.5.0 Update Package 12 potrebbe consentire a un utente con privilegi di modificare file di configurazione, permettendo così il caricamento di un file di aggiornamento automatico (autoupdate) malevolo, che può portare all'esecuzione di comandi arbitrari.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-4738	MY ERP di Yirmibes Software	N/A
VULNERABILITÀ	Vulnerabilità di SQL Injection dovuta a una non corretta neutralizzazione di elementi speciali usati in un comando SQL in Yirmibes Software MY ERP. Questo problema interessa MY ERP nelle versioni precedenti alla 1.170.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-6121	D-Link DIR-632 con firmware versione FW103B08	N/A
VULNERABILITÀ	È stata trovata una vulnerabilità classificata come critica nel D-Link DIR-632 FW103B08. Il problema riguarda la funzione get_pure_content del componente HTTP POST Request Handler. La manipolazione dell'argomento Content-Length può causare un overflow del buffer basato sullo stack. L'attacco può essere lanciato da remoto. L'exploit è stato reso pubblico e potrebbe essere utilizzato. Questa vulnerabilità interessa solo prodotti che non sono più supportati dal manutentore.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-4738	ClamAV (software antivirus open source)	N/A
VULNERABILITÀ	Una vulnerabilità nei processi di scansione PDF di ClamAV potrebbe consentire a un attaccante remoto non autenticato di causare una condizione di overflow del buffer, provocare un denial of service (DoS) o eseguire codice arbitrario sul dispositivo interessato. Questa vulnerabilità esiste perché i buffer di memoria vengono allocati in modo errato durante l'elaborazione dei file PDF. Un attaccante potrebbe sfruttare questa vulnerabilità inviando un file PDF appositamente creato da scansionare da ClamAV sul dispositivo vulnerabile. Un exploit riuscito potrebbe causare un overflow del buffer, portando probabilmente alla terminazione del processo di scansione ClamAV e a una condizione di DoS sul software interessato. Sebbene non confermato, esiste anche la possibilità che un attaccante possa sfruttare l'overflow per eseguire codice arbitrario con i privilegi del processo ClamAV.	

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-2023-0386
DESCRIZIONE	
Nel kernel Linux è stato scoperto un difetto nel sottosistema OverlayFS che gestisce il montaggio di file system sovrapposti. Quando un utente copia un file con privilegi speciali (setuid e capacità) da un mount con l'opzione nosuid disabilitata a un altro mount, la mappatura degli UID è errata. Questo permette a un utente locale di eseguire il file con privilegi elevati, ottenendo un aumento dei privilegi sul sistema.	

CVE	CVE-2025-43200
DESCRIZIONE	
In alcuni sistemi Apple, c'era un problema nella gestione di foto o video creati appositamente in modo malevolo e condivisi tramite un link iCloud. Il sistema faceva un errore logico nel processare questi contenuti, permettendo potenzialmente a un attaccante sofisticato di sfruttare questa falla per colpire specifiche persone con un attacco mirato. Apple ha corretto questo problema con miglioramenti nei controlli di sicurezza nelle versioni indicate.	

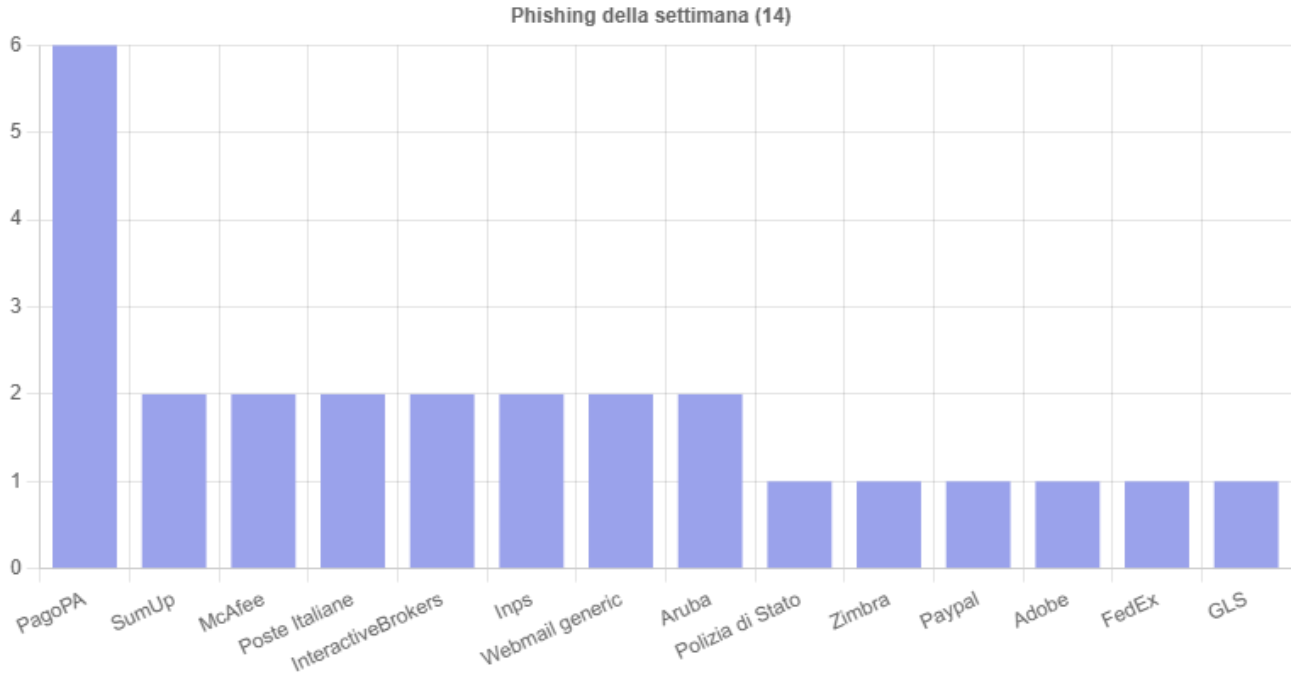
CVE	CVE-2023-33538
DESCRIZIONE	
La CVE-2023-33538 riguarda una vulnerabilità di command injection presente in alcuni modelli di router TP-Link: TL-WR940N (V2, V4), TL-WR841N (V8, V10) e TL-WR740N (V1, V2). Il problema si trova nel componente /userRpm/WlanNetworkRpm, che gestisce la configurazione della rete wireless. Un attaccante remoto può sfruttare questa falla per eseguire comandi arbitrari sul router, ottenendo così il controllo completo del dispositivo. Questo può portare a modifiche non autorizzate della rete, intercettazione del traffico o compromissione della sicurezza della rete domestica o aziendale collegata.	

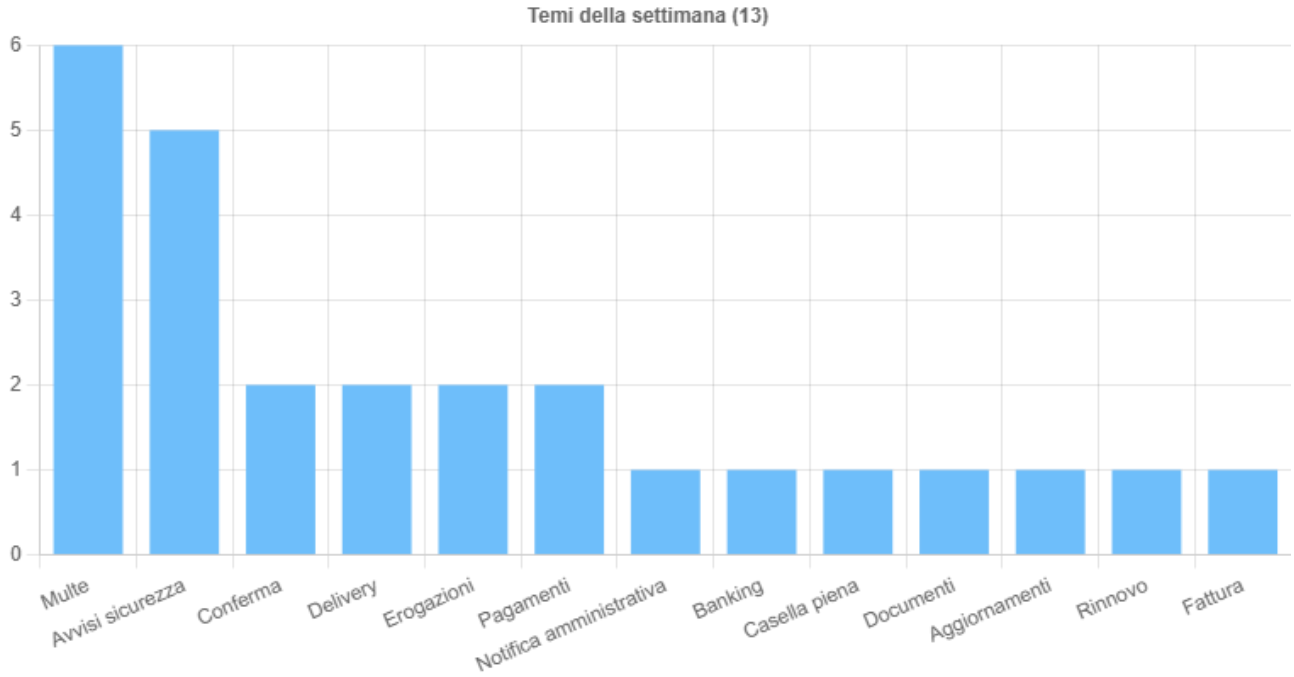
4 Attacchi

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.

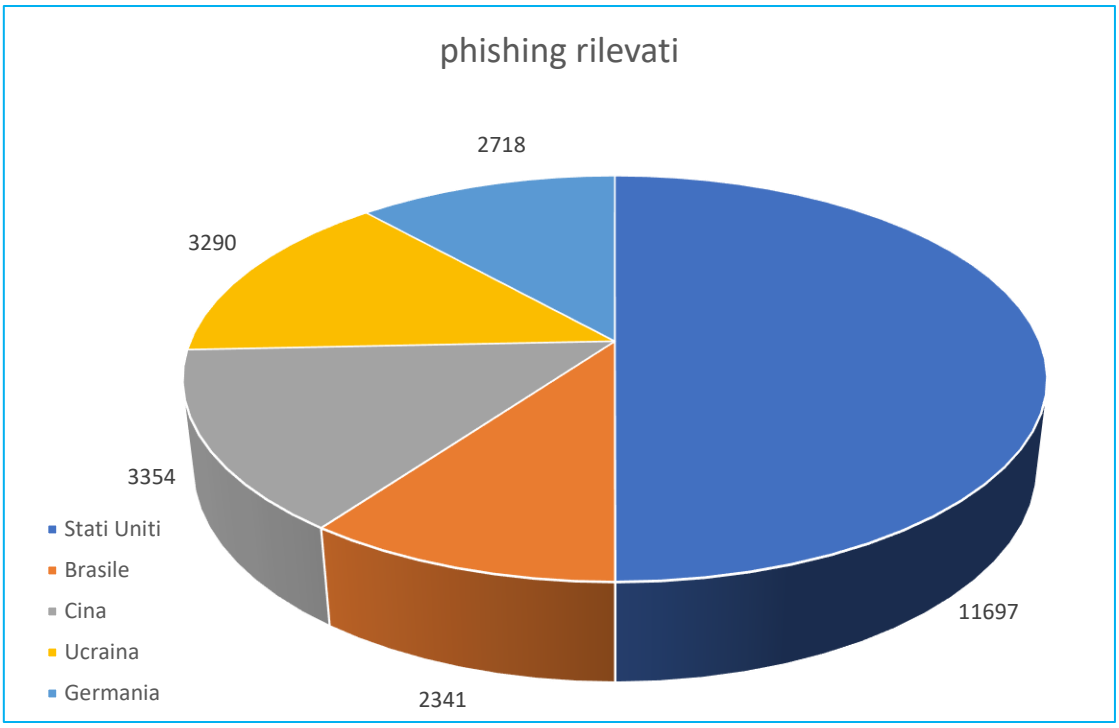




Fonte :CERT-AGID

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 di Analisi Investigativa Email Sospetta di Phishing

Oggetto: "Abbiamo riscontrato attività sospette sul Suo conto – La invitiamo a controllarlo"
Mittente: Paypal <postmaster@ecd9f07f6d[.]nxcli[.]io>
Data Ricezione: 20 Giugno 2025, 14:35
Destinatario: victim@victim[.]com (nome e dominio sostituiti per privacy e uniformità)

Introduzione

La presente analisi è stata condotta su una email sospetta segnalata come potenziale phishing, con intento fraudolento di indurre il destinatario a fornire dati personali sensibili simulando una comunicazione ufficiale PayPal. La metodologia impiegata ha previsto un'analisi approfondita degli header della mail, della reputazione del dominio mittente e dell'infrastruttura di rete, dell'URL presente nel corpo della mail, del certificato SSL/TLS, della struttura e contenuto del messaggio, e la verifica tramite strumenti OSINT e sandboxing per confermare la natura malevola della email.

Analisi Tecnica Email

Header e Infrastruttura mittente
La mail è partita da:
Mittente: postmaster@ecd9f07f6d[.]nxcli[.]io

Dominio mittente: ecd9f07f6d[.]nxcli[.]io (sottodominio nxcli[.]io)
IP Server mittente: 209[.]87[.]149[.]204 (cloudhost-3261933.us-midwest-1.nxcli[.]net)
Tecnologia SMTP: OpenSMTPD con TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384

Verifica WHOIS dominio:

Campo	Valore
Dominio	nxcli[.]io
Registrar	Namecheap, Inc.
Data creazione	2019-10-12
Stato dominio	Attivo, senza segnalazioni EPP
Proprietario	Privacy Protected (registrazione anonima)

Verifica hosting e geolocalizzazione IP:

IP	209[.]87[.]149[.]204
Provider	nxcli[.]net (Cloud hosting provider)
Paese	Stati Uniti (Midwest - Illinois)
Abuse Contact Email	abuse@nxcli[.]net

Reputazione IP e dominio
VirusTotal: IP e dominio associati a hosting cloud pubblico, nessuna segnalazione diretta di phishing o malware attivo.
AbuseIPDB: Presenti record di abusi recenti relativi all'IP

Autenticazione Email (SPF, DKIM, DMARC)
SPF: Non presente record SPF pubblicato per ecd9f07f6d[.]nxcli[.]io, si evidenzia possibile falsificazione del mittente.
DKIM: Firma DKIM presente, associata al dominio ecd9f07f6d[.]nxcli[.]io, ma dominio non riconducibile ufficialmente a PayPal.
DMARC: Non riscontrato record DMARC valido per il dominio mittente.
Valutazione: L'assenza di record SPF e DMARC legittimi aumenta la probabilità che la mail sia spoofata.

Certificato SSL/TLS sito collegato
L'URL indicato nel pulsante "Verifica ora" è:
https://checkout[.]shopify[.]com/gift_cards/76302156033/93b000ed8ca09b4150515f8649a4b15f-
Hosting URL: Shopify (piattaforma di e-commerce legittima)
Certificato SSL: Valido, emesso da DigiCert con nome corrispondente a shopify[.]com
Analisi: Il link non punta a un dominio PayPal ma a un URL generato su Shopify, utilizzato da phisher per veicolare la vittima su pagina di raccolta dati o truffa.

Analisi contenuto email e tecnica di ingegneria sociale

La mail presenta un testo in italiano con tono urgente, utilizzando la leva della sicurezza ("attività insolite sul tuo conto PayPal") per spingere l'utente a cliccare sul pulsante e confermare i dati personali. Tecniche individuate:

Spear phishing: Riferimento personalizzato al conto PayPal (anche se generico).

Urgency and fear: Invito a verificare "ora" per evitare problemi.

Link mascherato: Pulsante con link non riconducibile al dominio PayPal ufficiale.

Assenza di saluti personalizzati: Nessun nome proprio o riferimento specifico, comune nelle mail phishing, anche se nel testo si specifica "*PayPal ti contatterà sempre utilizzando il tuo nome e cognome".*

Verifica Allegati

Nessun allegato presente nella mail.

Analisi URL e Sandbox

L'URL sospetto è stato analizzato con:

VirusTotal URL scan: hosting su Shopify. IP e dominio associati a hosting cloud pubblico, presenti segnalazioni dirette di phishing o malware attivo.

Joe Sandbox: non applicabile direttamente poiché URL non contiene payload eseguibile, ma hosting di pagina phishing.

Analisi di WHOIS per dominio Shopify conferma legittimità piattaforma, ma URL probabilmente creato da attaccante per campagne phishing.

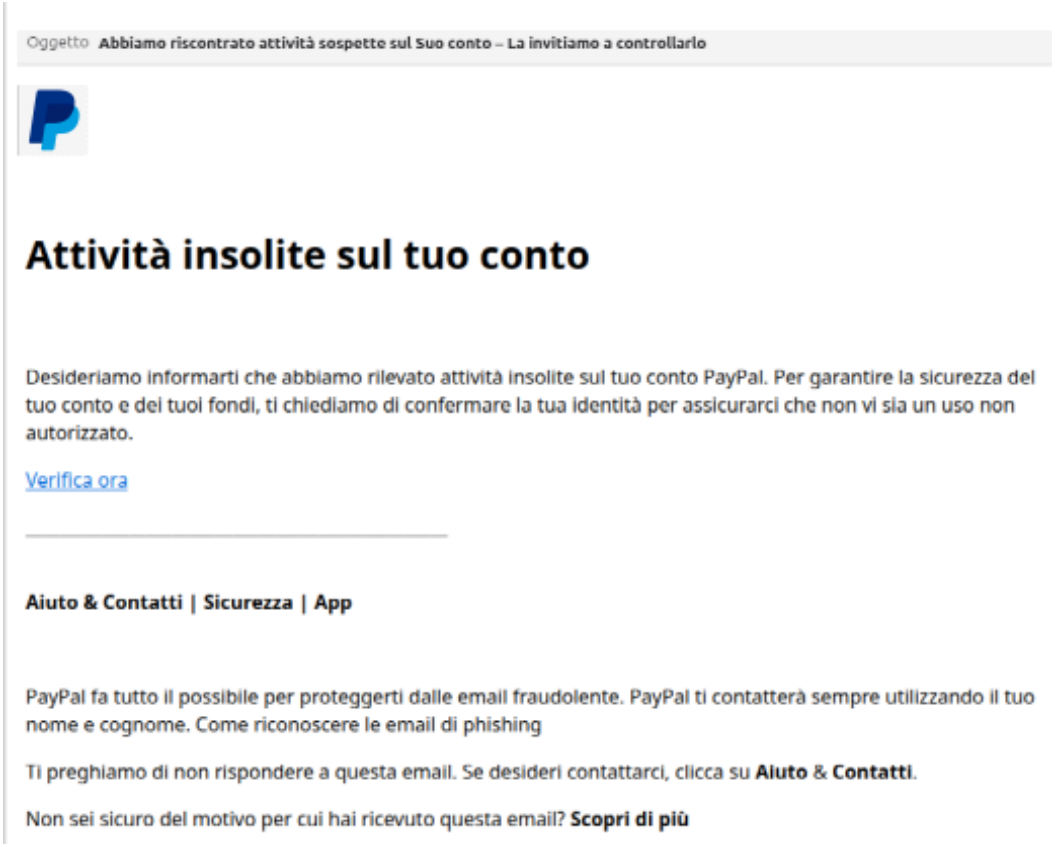
AbuseIPDB: Presenti record di abusi recenti relativi all'IP.

PhishTank: Presenti report diretto sul dominio o URL presenti nella mail.

Indicatori di Compromissione (IoC)

Tipo	Valore	Note
Mittente	postmaster@ecd9f07f6d[.]nxcli[.]io	Dominio sospetto non PayPal
Dominio	ecd9f07f6d[.]nxcli[.]io	Hosting cloud non associato PayPal
IP SMTP	209[.]87[.]149[.]204	Hosting USA, presenti segnalazioni note
URL	https://checkout[.]shopify[.]com/gift_cards/...	Link phishing mascherato su Shopify
DKIM	ecd9f07f6d[.]nxcli[.]io	Firma presente ma dominio non legittimo

Screenshot email (con dati sensibili oscurati)



Oggetto **Abbiamo riscontrato attività sospette sul Suo conto – La invitiamo a controllarlo**

Attività insolite sul tuo conto

Desideriamo informarti che abbiamo rilevato attività insolite sul tuo conto PayPal. Per garantire la sicurezza del tuo conto e dei tuoi fondi, ti chiediamo di confermare la tua identità per assicurarci che non vi sia un uso non autorizzato.

Verifica ora

Aiuto & Contatti | Sicurezza | App

PayPal fa tutto il possibile per proteggerti dalle email fraudolente. PayPal ti contatterà sempre utilizzando il tuo nome e cognome. Come riconoscere le email di phishing

Ti preghiamo di non rispondere a questa email. Se desideri contattarci, clicca su **Aiuto** & **Contatti**.

Non sei sicuro del motivo per cui hai ricevuto questa email? **Scopri di più**

Riepilogo e Conclusioni

L'email analizzata presenta tutte le caratteristiche tipiche di un attacco phishing mirato a utenti PayPal, sfruttando tecniche di social engineering basate sull'urgenza e l'imitazione grafica di comunicazioni ufficiali.

La verifica degli header email evidenzia un mittente con dominio non ufficiale, senza adeguate protezioni SPF e DMARC, ma con firma DKIM probabilmente generata da server compromesso o legittimo ma non PayPal. L'indirizzo IP del server mittente è associato a un provider di hosting cloud generico negli USA, senza reputazione sospetta nota, ma non appartenente all'infrastruttura PayPal.

Il link indicato nel messaggio porta a un dominio Shopify utilizzato per scopi fraudolenti. La pagina collegata non risulta avere certificati o segnalazioni malware ma rientra nella categoria di pagine usate da phisher per raccolta dati.

Consiglio operativo: non cliccare sul link, non fornire alcun dato personale o di accesso. Segnalare come phishing e bloccare mittente.

Collegamenti utili per verifica

VirusTotal IP 209[.]87[.]149[.]204:https://www[.]virustotal[.]com/gui/ip-address/209[.]87[.]149[.]204/detection

PhishTank (ricerca dominio): https://www[.]phishtank[.]com

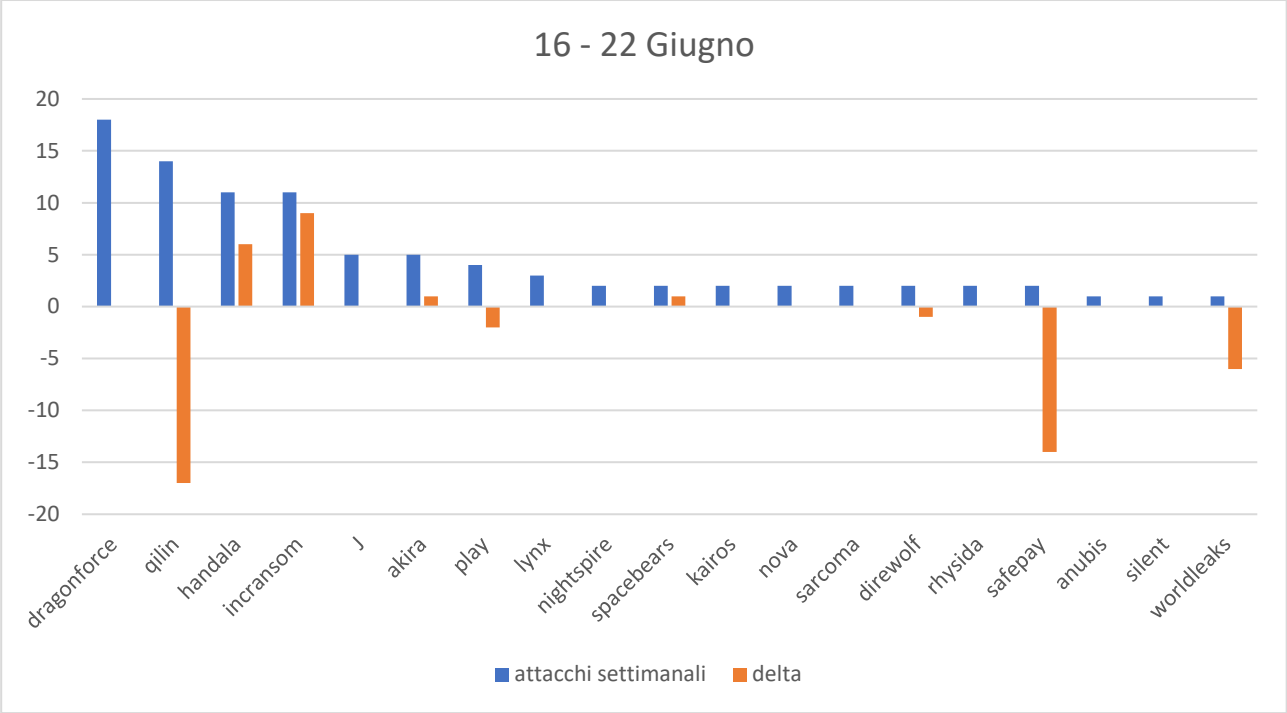
AbuseIPDB: https://www[.]abuseipdb[.]com/check/209[.]87[.]149[.]204

WHOIS dominio nxcli[.]io: https://whois[.]domaintools[.]com/nxcli[.]io

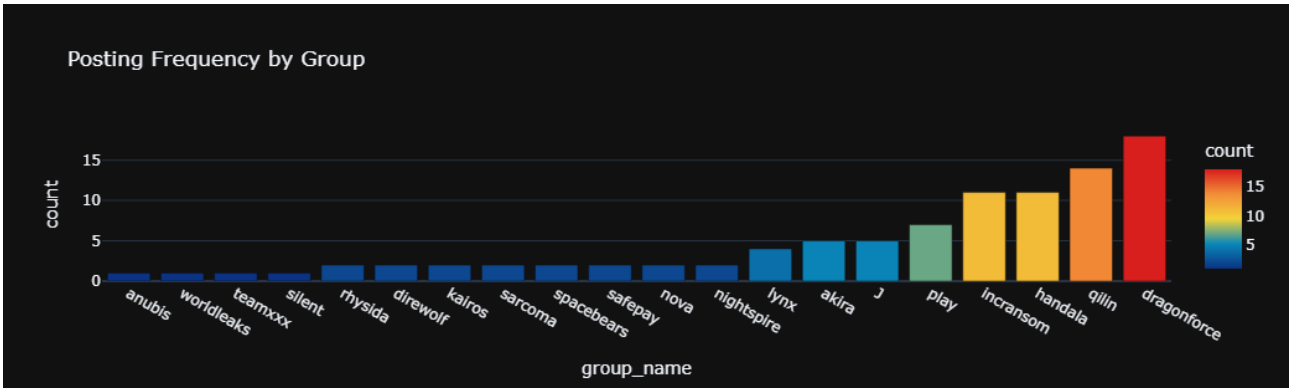
VirusTotal URL :https://www.virustotal[.]com/gui/url/28f1a6d65fe5032e9292e42735c5e8259b324f79d792fb9d20489aebc4a47114

4.2 Ransomware

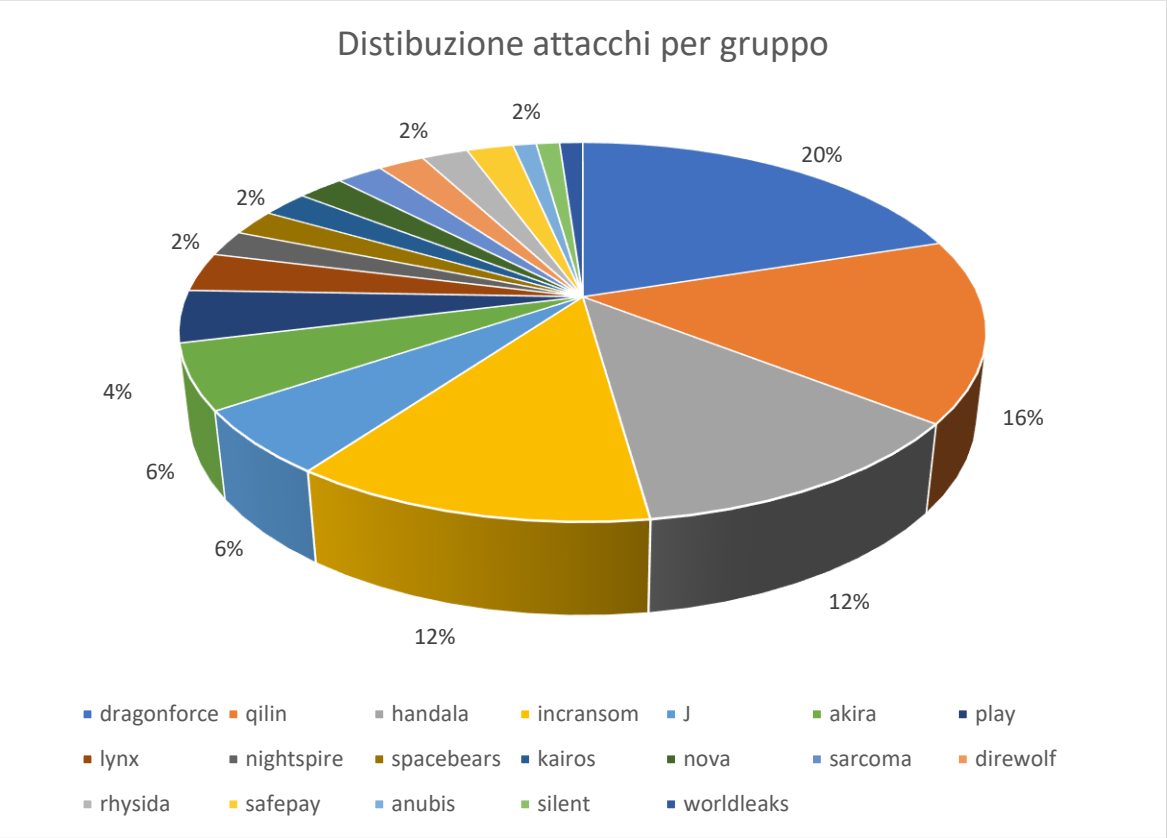
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (16 - 22 Giugno). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

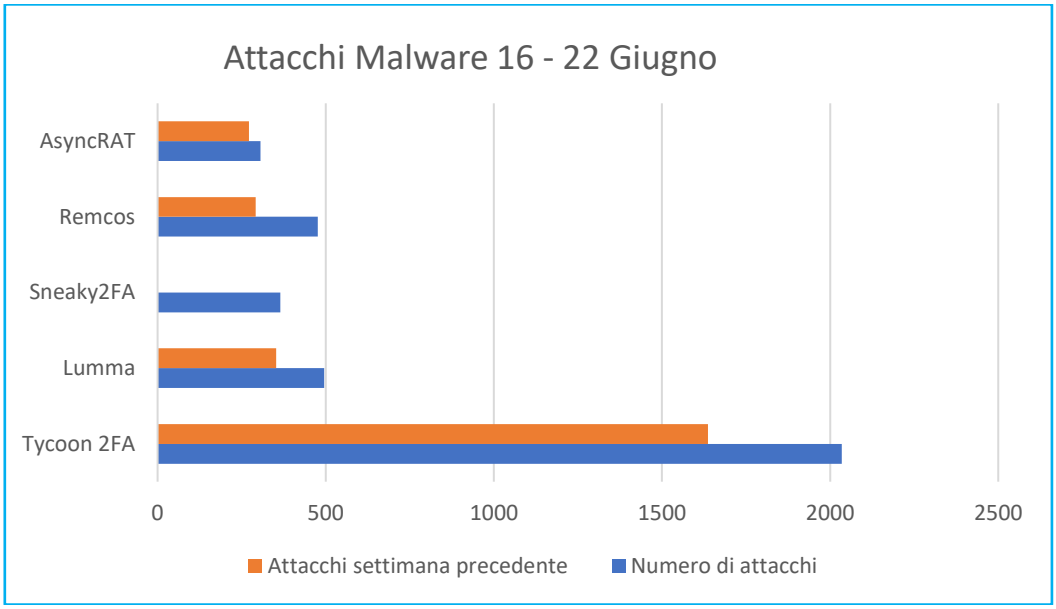


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



4.3 Malware

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



Report settimanale sui malware più attivi

Stargazers Ghost Network (mod Minecraft infetto)

Una campagna malware a più fasi è stata scoperta su GitHub, in cui mod di Minecraft infette (es. Oringo, Taunahi) venivano usate per diffondere un infostealer scritto in .NET. Il downloader iniziale è scritto in Java e funge da dropper.

- Indicatori di compromissione (IoC):

Tipo	Valore
SHA256	05b143fd7061bdd317bd42c373c5352bec351a44fa849ded5823601312 6d2963
Dominio	негры[.]рф
URL	http://147.45.79.104/download hxxp://негры[.]рф/MixinLoader-v2.4[.]jar hxxp[://]185[.]95[.]159[.]125/upload
GitHub Repo	hxxps://github[.]com/A1phaD3v/Oringo-Client hxxps://github[.]com/AlphaPigeonDev/Polar-Client hxxps://github[.]com/AlphaPigeonDev/Skyblock-Extras hxxps://github[.]com/P1geonD3v/Funny-Map-Extras hxxps://github[.]com/P1geonD3v/Taunahi-V3

- MITRE ATT&CK:
  - T1204 – Esecuzione da parte dell'utente
  - T1036 – Mascheramento (mod legittimi)
  - T1059 – Scripting
  - T1560 – Esfiltrazione dati
- Contromisure (Rilevamento e Mitigazione):
  - Impiego di sandbox e tecniche di emulazione
  - Blocco di hash/domìni/URL noti
  - Limitare l'uso di mod da fonti ufficiali
  - Protezione endpoint aggiornata
- Livello di rischio: Alto.

PylangGhost RAT (APT nordcoreano)

Nuova variante Python (successore di GolangGhost) usata dal gruppo APT nordcoreano *Famous Chollima* contro professionisti crypto. Utilizza un attacco di tipo "ClickFix" per indurre le vittime a incollare comandi malevoli nel terminale.

- IoC:

Tipo	Valore
Payload name	clickfix.py

- MITRE ATT&CK:
  - T1566.002 – Phishing via link malevoli
  - T1204.002 – Esecuzione comandi da terminale
  - T1059 – Scripting
  - T1555 – Accesso a credenziali
- Contromisure:
  - Sensibilizzazione contro il "copy-paste" da fonti non attendibili
  - Blocco comportamenti sospetti in PowerShell/terminali
  - Uso di EDR/AV con rilevamento comportamentale
- Livello di rischio: Alto

Water Curse (campagna su GitHub)

Campagna malevola che sfrutta 76 repository GitHub con progetti Visual Studio trojanizzati. Include fasi in VBScript e PowerShell che scaricano payload cifrati. Il malware finale consente esfiltrazione di credenziali e persistenza tramite attività pianificate.

- IoC:

Tipo	Valore
GitHub Repo	github.com/.../Email-Bomber-SMTP, github.com/.../Sakura-Rat
URL malevoli	http://rlim[.]com https://pastejustit[.]com

- MITRE ATT&CK:
  - T1195 – Compromissione della catena di distribuzione
  - T1059 – Esecuzione script (MSBuild/VBS)
  - T1547 – Persistenza (Scheduled Task)
  - T1555 – Accesso a credenziali
- Contromisure:
  - Analisi manuale dei progetti open source
  - Monitoraggio delle attività GitHub
  - Soluzioni XDR
  - Rilevamento di esfiltrazione su Telegram/go-file
- Livello di rischio: Alto

AsyncRAT fileless – Germania

Campagna di phishing che induce utenti tedeschi a eseguire manualmente un comando PowerShell offuscato da una finestra "I'm not a robot". Il malware viene eseguito interamente in memoria (fileless), fornendo accesso remoto e furto di credenziali.

- IoC:

Tipo	Valore
URL PS	http://namoet[.]de/x
LOLBin	conhost.exe
RAT	AsyncRAT (caricato in memoria)

- MITRE ATT&CK:
  - T1059.001 – PowerShell
  - T1127.001 – Compile After Delivery
  - T1547 – Persistenza tramite registro
  - T1056.001 – Input Capture: Keylogging / Terminal I/O

    - T1055.001 – Process Injection
- Contromisure:
    - Logging di invocazioni anomale conhost e PowerShell
    - Rilevamento di AsyncRAT in memoria
    - Formazione anti-phishing mirata
- Livello di rischio: Alto

Riepilogo generale

Malware / Campagna	Rischio	Tecniche MITRE Principali	Area Geografica
Stargazers Ghost Network	Alto	T1204, T1036, T1059, T1560	Globale
PylangGhost RAT	Alto	T1566.002, T1204.002, T1059, T1555	Globale (India)
Water Curse (GitHub)	Alto	T1195, T1059, T1547, T1555	Globale
AsyncRAT fileless	Alto	T1059.001, T1218, T1547	UE (Germania)

Fonti:

Stargazers Ghost Network

- **Fonte:** Check Point Research
- **Link:** https://research.checkpoint.com/2025/minecraft-mod-malware-stargazers/

PylangGhost RAT (APT Nordcoreano)

- **Fonte:** Cisco Talos
- **Link:** https://therecord.media/north-korea-india-crypto-applicants

Water Curse (Progetti GitHub trojanizzati)

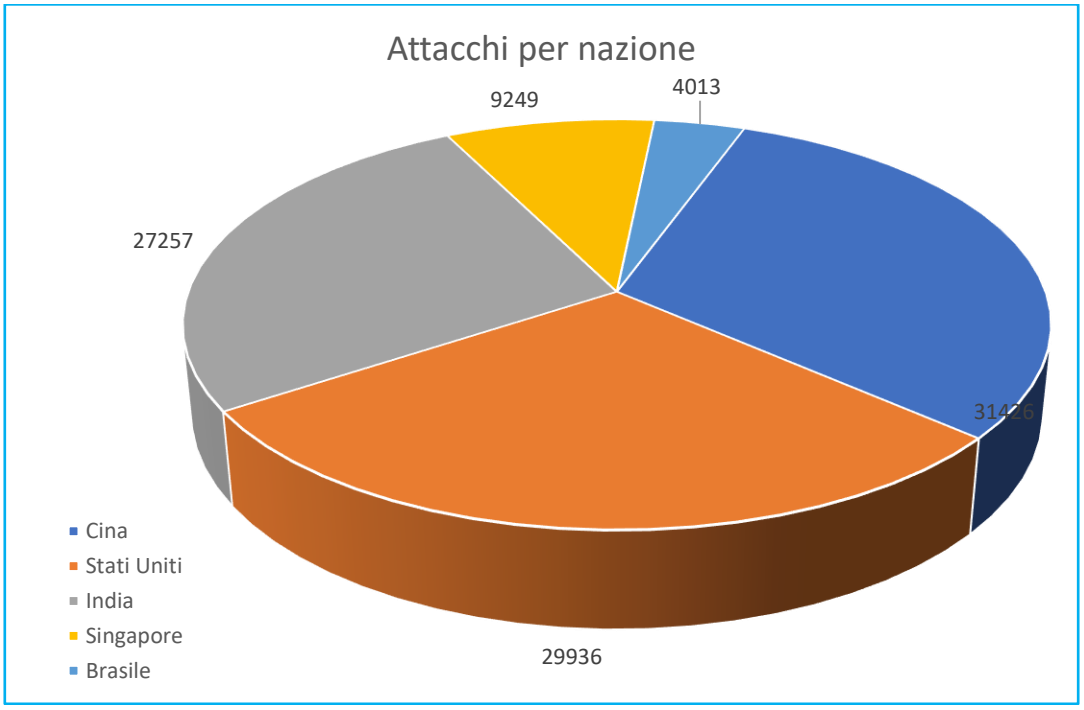
- **Fonte:** Trend Micro
- **Link:** https://www.trendmicro.com/en_us/research/25/f/water-curse.html

AsyncRAT Fileless – Germania (UE)

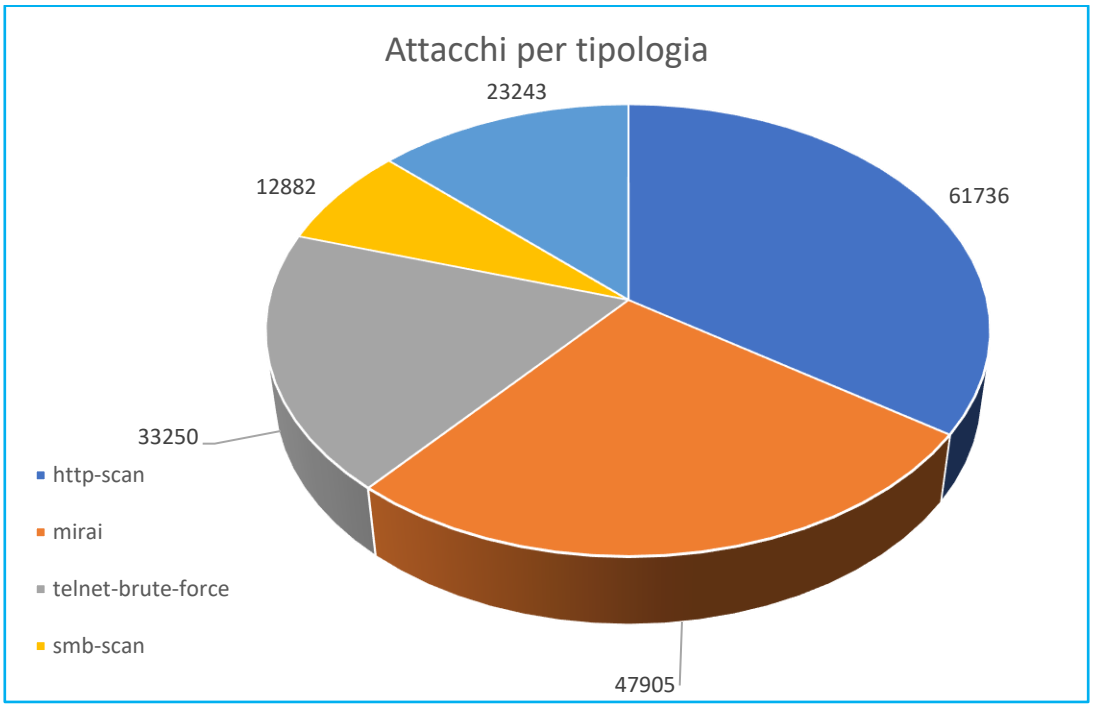
- **Fonte:** CloudSEK
- **Link:** https://www.cloudsek.com/blog/fileless-asyncrat-distributed-via-clickfix-technique-targeting-german-speaking-users

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:

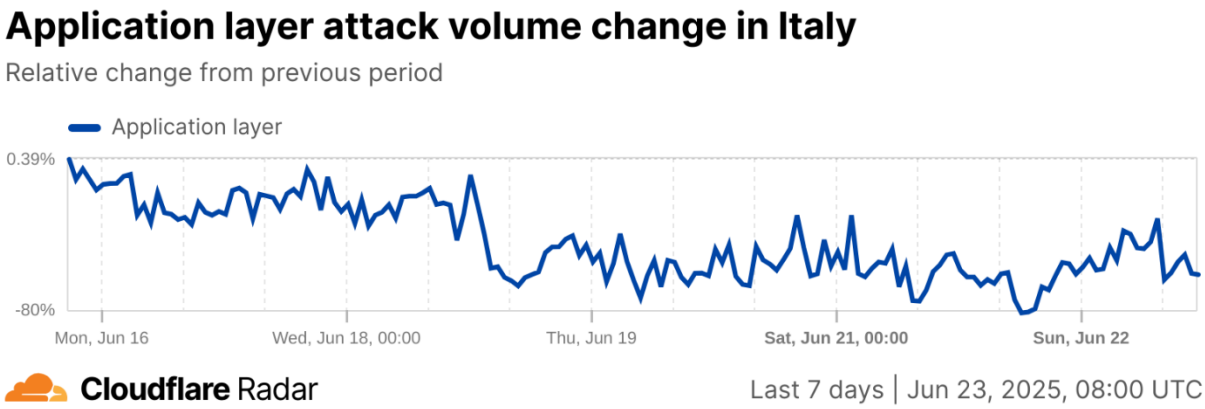


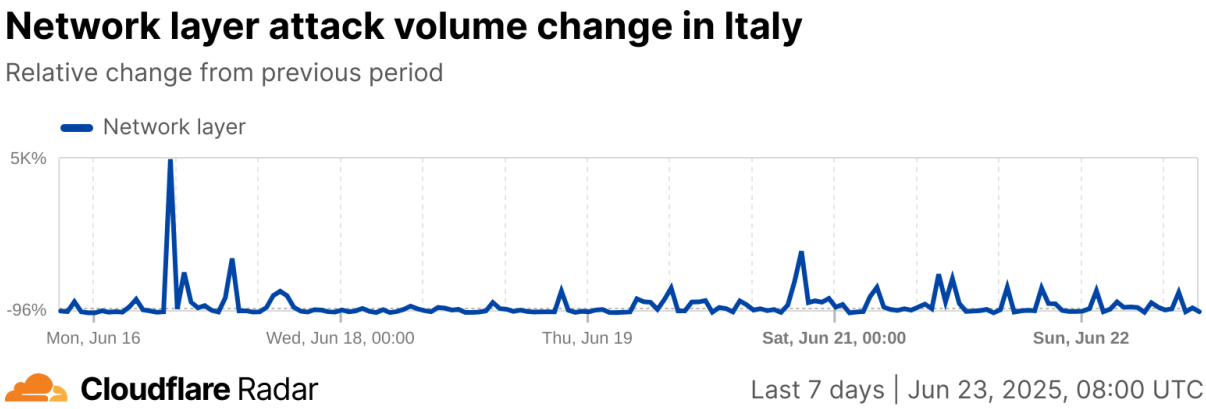
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
AFLAC	STATI UNITI
DESCRIZIONE	Aflac ha subito un attacco informatico da parte del gruppo di cybercriminali Scattered Spider, che ha compromesso dati sensibili di clienti, tra cui numeri di previdenza sociale e informazioni sanitarie. L'intrusione, basata su tecniche di social engineering senza l'uso di ransomware, è stata fermata in poche ore, ma ha comunque causato gravi rischi per la privacy degli utenti. Aflac ha attivato esperti di cybersecurity, notificato le autorità competenti e offerto servizi di monitoraggio del credito per le persone coinvolte.

TARGET	LOCALIZZAZIONE
TGC INC.	STATI UNITI
DESCRIZIONE	Il 18 giugno 2025, Technology Consultants Group (TCG Inc.), un fornitore statunitense di soluzioni IT enterprise, è stato vittima di un attacco ransomware condotto dal gruppo DragonForce. L'incidente ha portato ad una violazione dei dati con una perdita stimata di circa 624 MB di informazioni sensibili. Il breach è stato scoperto lo stesso giorno e ha colpito il dominio tcgrpinc.com, compromettendo la sicurezza e l'operatività dell'azienda.

TARGET	LOCALIZZAZIONE
FENG CHIA UNIVERSITY	TAIWAN
DESCRIZIONE	Tra il 18 e il 20 giugno 2025, Feng Chia University, una nota università privata di Taichung, Taiwan, è stata colpita da un attacco ransomware da parte del gruppo emergente NOVA. L'università ha confermato l'incidente e ha subito adottato misure per contenere i danni, coinvolgendo esperti esterni per l'indagine. NOVA ha rivendicato il furto di circa 10 GB di dati sensibili, tra cui codice sorgente, informazioni sui dipendenti e dati sui pagamenti degli studenti, minacciando di pubblicarli entro 10 giorni se non veniva pagato un riscatto. Feng Chia ha però smentito la diffusione di dati personali e ha chiesto di evitare speculazioni durante l'indagine in corso.

4.6 Defacement

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

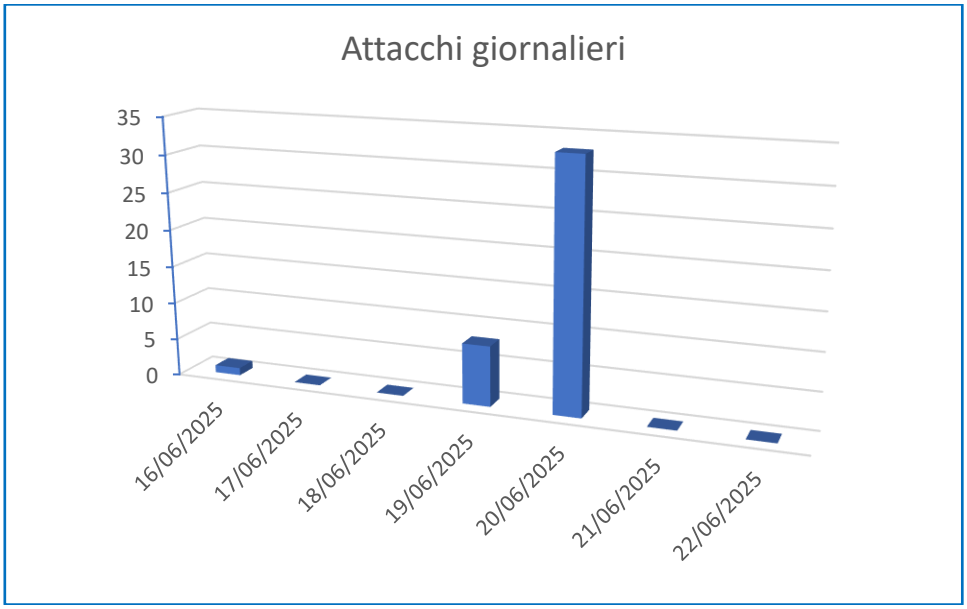


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

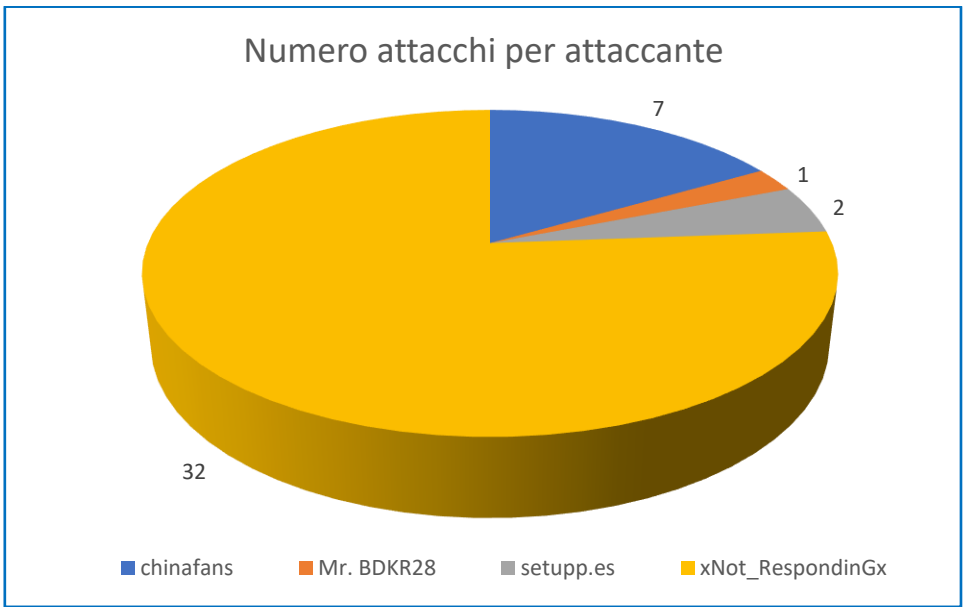


Figura 2: Defacement - Attaccanti più attivi nel periodo 16 – 22 Giugno

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

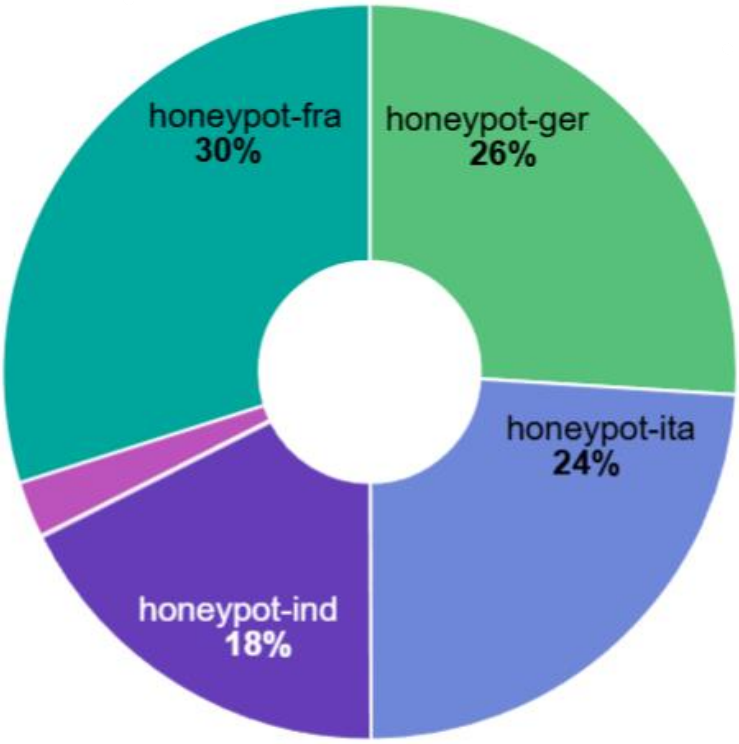
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

1.577.297 Attacks

10.198 Unique Src IPs

65 Unique HASSHs

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



Questa invece la situazione a livello italiano:

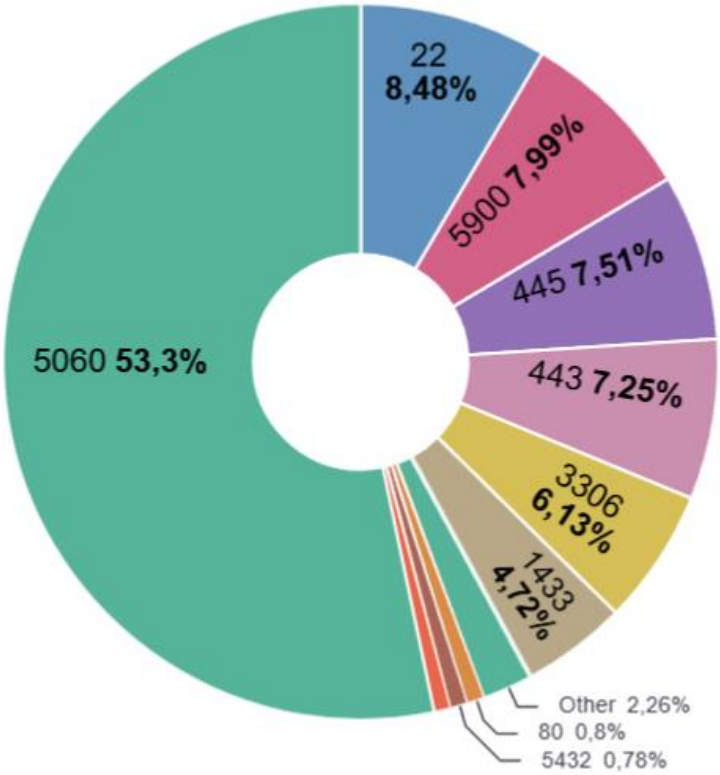
377.770 Attacks

3.465 Unique Src IPs

47 Unique HASSHs

5.1.1 Attacchi ai servizi

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



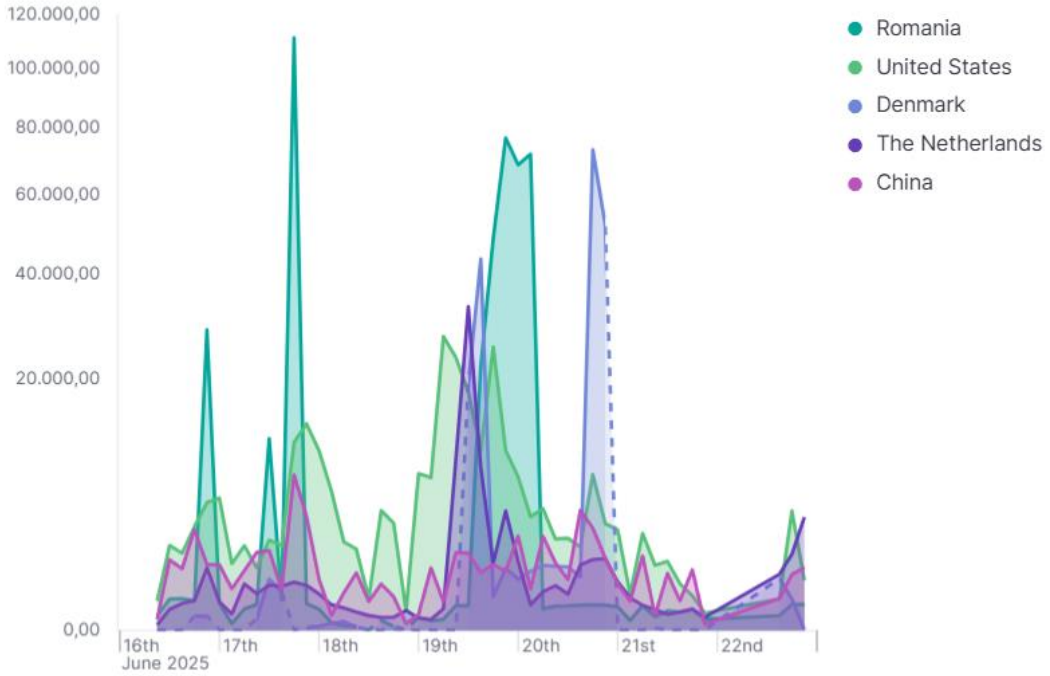
5.1.2 IP Attaccanti

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

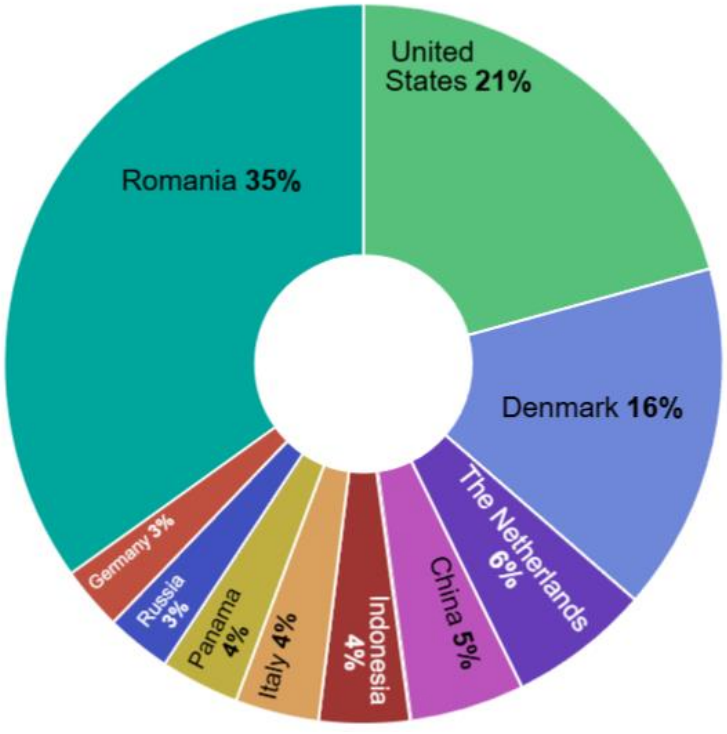
Source IP	Count
80.94.93.158	437.500
45.144.29.201	198.862
173.233.73.4	71.163
45.227.253.103	44.706
136.144.35.230	43.077
103.156.74.23	39.106
45.14.245.67	34.543
142.202.189.5	25.261
142.202.191.234	22.200
193.37.69.157	18.772

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:

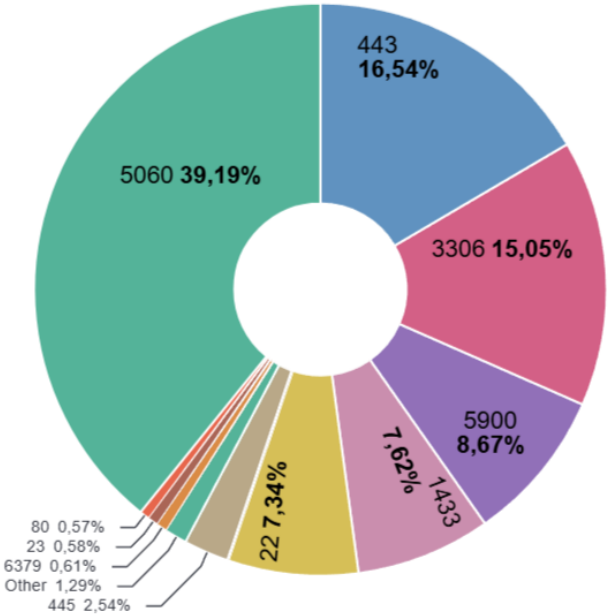


5.2 Italian Honeypot N.1

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
5060	112.138
443	47.327
3306	43.058
5900	24.798
1433	21.794
22	20.990
445	7.262
6379	1.750
23	1.672
80	1.640

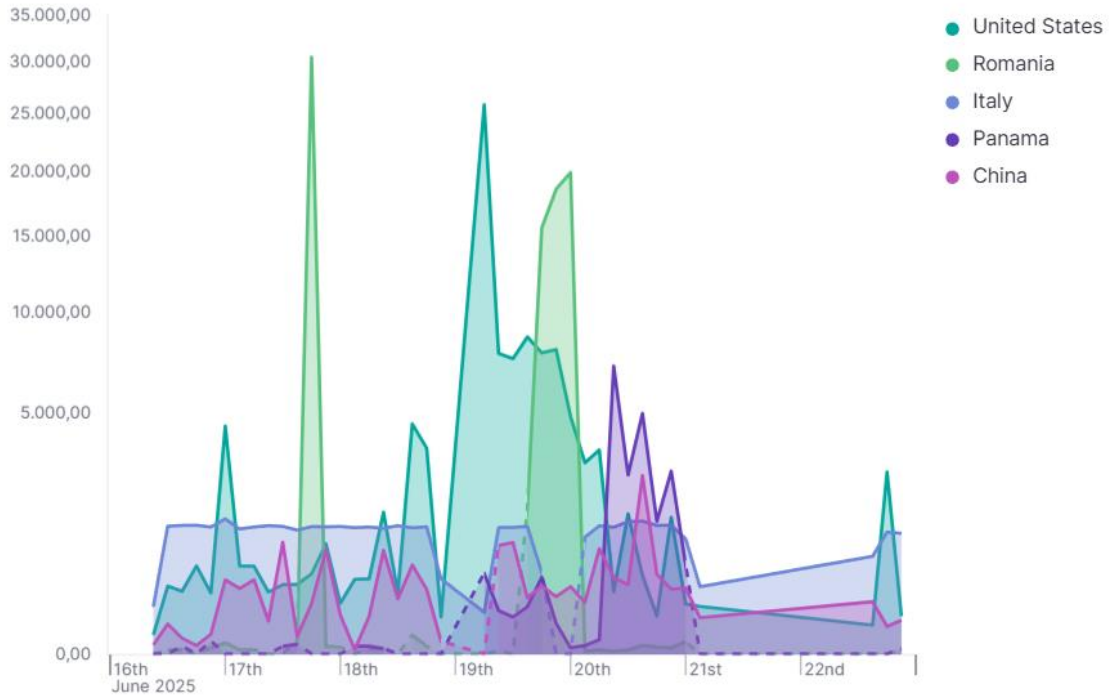
5.2.2 IP Attaccanti

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

Source IP	Count
80.94.93.158	86.403
136.144.35.230	42.834
173.233.73.4	25.066
45.227.253.103	21.610
103.156.74.23	10.543
142.202.189.5	9.215
176.65.151.53	7.388
193.37.69.157	6.657
142.202.191.234	5.858
173.231.185.164	3.387

5.2.3 Paesi di provenienza degli attacchi

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

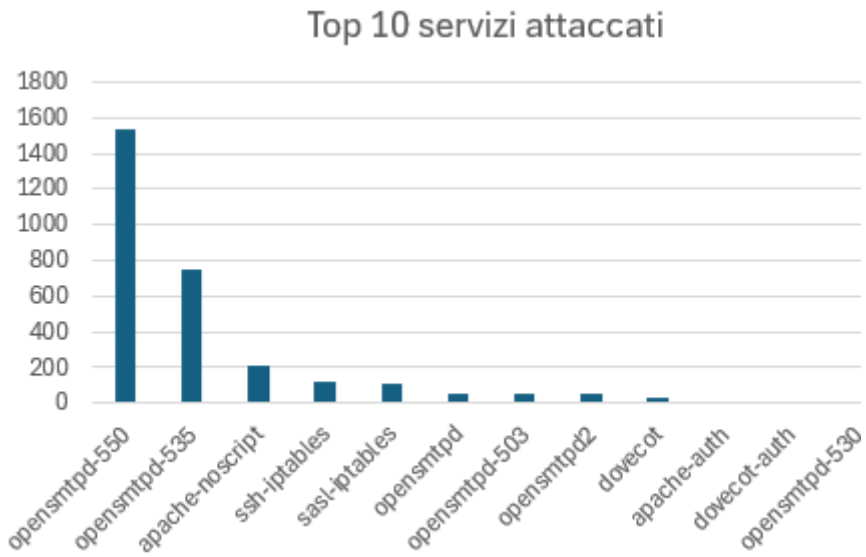


5.3 Italian Honeypot N.2

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.



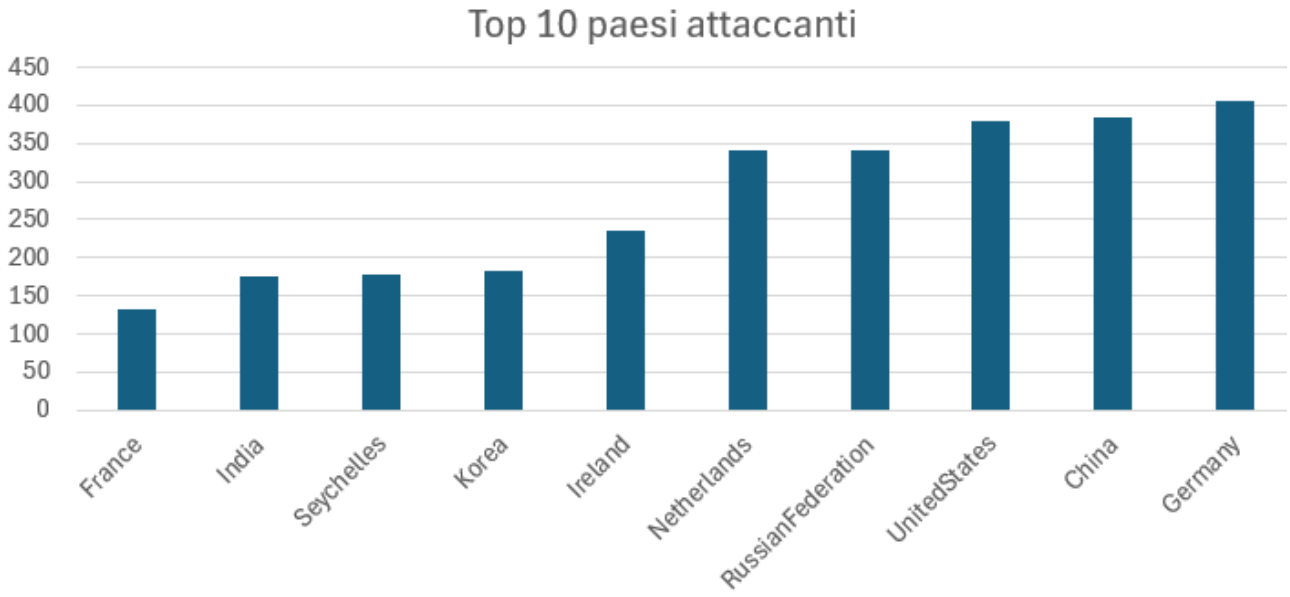
5.3.2 IP attaccanti

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
195[.]54[.]33[.]154	229
37[.]48[.]90[.]236	180
213[.]108[.]199[.]160	151
62[.]173[.]145[.]115	130
62[.]212[.]95[.]136	45
95[.]181[.]151[.]26	37
185[.]176[.]220[.]64	35
82[.]165[.]21[.]237	34
217[.]154[.]218[.]80	27
62[.]173[.]140[.]179	25

5.3.3 Paesi di provenienza degli attacchi

Questa invece la distribuzione dei paesi attaccanti:



6 Company Profile S3K

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

COME LO FACCIAMO:

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

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

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

CON QUALI LEVE OPERIAMO:

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

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

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

CHI SIAMO:

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

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

LA NOSTRA MISSION:

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

I NOSTRI VALORI:

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

CONTATTI:

contattaci@s3k.it
insidesales@s3k.it
marketing@s3k.it

DISCLAIMER

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

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

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

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

CLASSIFICAZIONE DOCUMENTO

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

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

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

Cyber security

RISK REPORT

S3K

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