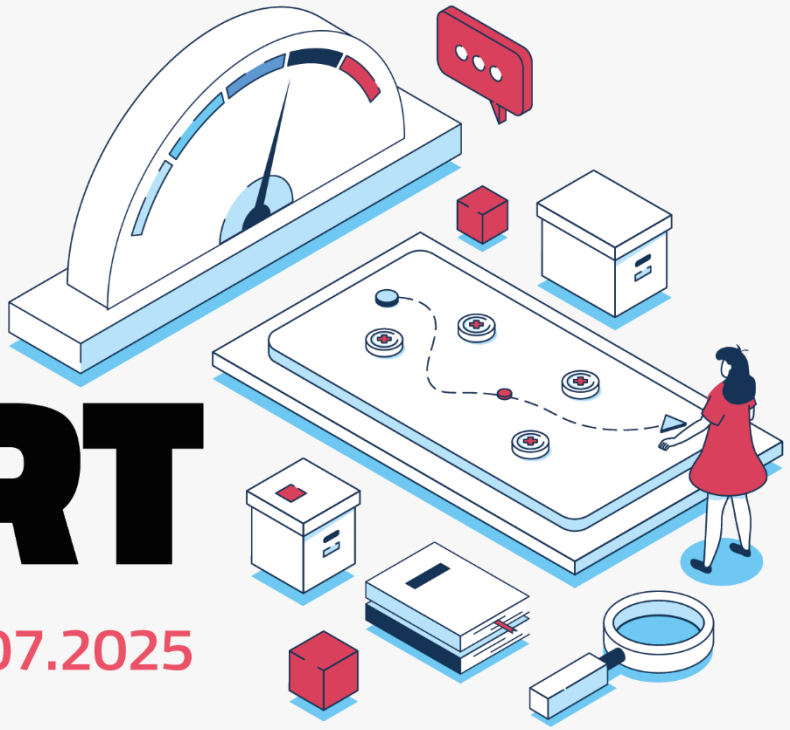
S3K

Cyber security

RISK REPORT

\ week 07.07.2025 - 13.07.2025



Sommario


CYBER SECURITY RISK REPORT
28/25

1 Il Cyber Security Risk Report S3K

Settimana 07.07.2025 – 13.07.2025

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

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

1.1 Presentazione del Cyber Security Risk Report S3K

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

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

1.2 Bollettino di Cybersicurezza 15 Luglio 2025

Questo bollettino presenta un'analisi approfondita delle principali minacce informatiche emerse nella settimana 7-13 luglio 2025. Il documento offre una panoramica completa delle vulnerabilità più critiche, degli attacchi in corso, delle tendenze nel panorama delle minacce e dei dati raccolti dai nostri sistemi honeypot. L'obiettivo è fornire ai professionisti della sicurezza informatica le informazioni necessarie per proteggere efficacemente le loro organizzazioni dalle minacce emergenti.

1.3 Executive Summary

Nel periodo 7-13 luglio 2025, il panorama delle minacce informatiche ha mostrato un'intensificazione significativa di attività malevole, con particolare impatto su settori critici e infrastrutture strategiche. La settimana è stata caratterizzata da oltre 10 vulnerabilità critiche con exploit già disponibili pubblicamente, principalmente legate a tecnologie Campcodes e sistemi di gestione industriale.

Sul fronte degli attacchi, è stato documentato un significativo caso di cyberspionaggio condotto dal gruppo DoNot APT contro il Ministero degli Affari Esteri italiano, utilizzando tecniche sofisticate di social engineering. Parallelamente, nel Regno Unito sono stati arrestati quattro sospettati per attacchi informatici a grandi marchi del retail come Marks & Spencer e Harrods, con impatti finanziari stimati in oltre 400 milioni di dollari.

I dati raccolti dai nostri honeypot evidenziano un aumento degli attacchi provenienti principalmente da Russia, Stati Uniti e Paesi Bassi, con particolare concentrazione su servizi SSH, HTTP e database. Il gruppo ransomware LockBit rimane il più attivo con un incremento del 28% rispetto alla settimana precedente, seguito da BlackCat e Play.

10+	28%	64M
CVE critiche	**Incremento LockBit**	**Record data breach**
Vulnerabilità con exploit pubblici già disponibili, principalmente legate a SQL Injection in prodotti Campcodes	Aumento degli attacchi ransomware LockBit rispetto alla settimana precedente	Dati di candidati esposti nel breach di McDonald's per credenziali banali (username/password: "123456")

Le principali vulnerabilità riguardano prodotti Adobe (35 con gravità "alta" e 3 "critiche"), sistemi Juniper Networks e soluzioni gestionali Campcodes, tutte sfruttabili remotamente e senza autenticazione. È stata inoltre documentata una nuova tecnica di tapjacking su Android chiamata TapTrap, che consente di aggirare il sistema di permessi utilizzando animazioni dell'interfaccia utente.

Si raccomanda di applicare tempestivamente le patch disponibili, monitorare attentamente i sistemi esposti e implementare difese a più livelli contro le minacce rilevate.

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	Adobe ha rilasciato aggiornamenti di sicurezza per risolvere molteplici vulnerabilità, di cui 35 con gravità "alta" e 3 con gravità "critica", nei prodotti Substance 3D Viewer, InCopy, InDesign, Connect, Dimension, Illustrator, FrameMaker, Experience Manager Forms e ColdFusion. Versioni affette: Adobe • Substance 3D Viewer, versione 0.22 e precedenti • InDesign, versione ID20.3 e precedenti (per Windows e macOS) • InDesign, versione ID19.5.3 e precedenti (per Windows e macOS) • Dimension, versione 4.1.2 e precedenti (per Windows e macOS) • Illustrator 2025, versione 29.5.1 e precedenti (per Windows e macOS) • Illustrator 2024, versione 28.7.6 e precedenti (per Windows e macOS) • FrameMaker 2020, Release Update 8 e precedenti (per Windows) • FrameMaker 2022, Release Update 6 e precedenti (per Windows) • ColdFusion 2025, Update 2 e precedenti • ColdFusion 2023, Update 14 e precedenti • ColdFusion 2021, Update 20 e precedenti • Experience Manager (AEM) Forms, versione 6.5.23.0 e precedenti • Connect, versione 24 e precedenti (per Windows) • InCopy, versione 20.3 e precedenti (per Windows e macOS) • InCopy, versione 19.5.3 e precedenti (per Windows e macOS)
ULR/Note	• https://helpx.adobe.com/security/Home.html • https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-54.html • https://helpx.adobe.com/security/products/incopy/apsb25-59.html • https://helpx.adobe.com/security/products/indesign/apsb25-60.html • https://helpx.adobe.com/security/products/connect/apsb25-61.html • https://helpx.adobe.com/security/products/dimension/apsb25-63.html • https://helpx.adobe.com/security/products/illustrator/apsb25-65.html • https://helpx.adobe.com/security/products/framemaker/apsb25-66.html • https://helpx.adobe.com/security/products/aem-forms/apsb25-67.html • https://helpx.adobe.com/security/products/coldfusion/apsb25-69.html

PRODOTTO	DESCRIZIONE
Tenable	Juniper Networks rilascia aggiornamenti di sicurezza per sanare diverse vulnerabilità, di cui una con gravità "critica" e 6 con gravita "alta", nei propri prodotti. versioni affette: Junos OS • tutte le versioni precedenti alla 22.2R3-S7 • 22.3, versioni precedenti alla 22.3R3-S3 • 22.4, versioni precedenti alla 22.4R3-S6 • 23.2, versioni precedenti alla 23.2R2-S4 • 23.4, versioni precedenti alla 23.4R2-S5 • 24.2, versioni precedenti alla 24.2R2-S1 • 24.4, versioni precedenti alla 24.4R1-S3 Junos OS Evolved • tutte le versioni precedenti alla 22.4R3-S7-EVO • 23.2-EVO, versioni precedenti alla 23.2R2-S4-EVO • 23.4-EVO, versioni precedenti alla 23.4R2-S5-EVO • 24.2-EVO, versioni precedenti alla 24.2R2-S1-EVO • 24.4-EVO, versioni precedenti alla 24.4R1-S2-EVO
ULR/Note	• https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Junos-OS-After-removing-ssh-public-key-authentication-root-can-still-log-in-CVE-2025-52983?language=en_US • https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Junos-OS-SRX-Series-Sequence-of-specific-PIM-packets-causes-a-flowd-crash-CVE-2025-52981?language=en_US • https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Junos-OS-SRX300-Series-Upon-receiving-a-specific-valid-BGP-UPDATE-message-rpd-will-crash-CVE-2025-52980?language=en_US • https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Junos-OS-Evolved-A-low-privileged-user-can-execute-CLI-commands-and-modify-the-configuration-compromise-the-system-CVE-2025-52954?language=en_US • https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Junos-OS-Low-privileged-user-can-cause-script-to-run-as-root-leading-to-privilege-escalation-CVE-2025-30661?language=en_US • https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Juniper-Security-Director-Insufficient-authorization-for-multiple-endpoints-in-web-interface-CVE-2025-52950?language=en_US • https://supportportal.juniper.net/s/article/2025-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-With-traceoptions-enabled-receipt-of-malformed-AS-PATH-causes-RPD-crash-CVE-2025-52946?language=en_US

PRODOTTO	DESCRIZIONE
Trend Micro	Rilevata vulnerabilità che interessa la libreria *resolv* di Ruby, che implementa la funzionalità per le risoluzioni DNS. Tale vulnerabilità, qualora sfruttata, potrebbe permettere la compromissione della disponibilità del servizio sulle istanze interessate. Versioni affette: Ruby 3.2 series • resolv gem 0.2.x, versione 0.2.2 e precedenti Ruby 3.3 series • resolv gem 0.3.x, versione 0.3.0 Ruby 3.4 series • resolv gem 0.6.x, versione 0.6.1 e precedenti
ULR/Note	https://www.ruby-lang.org/en/news/2025/07/08/dos-resolv-cve-2025-24294/

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

ATTACCO DI DONOT APT AL MINISTERO DEGLI ESTERI ITALIANO: NUOVA CAMPAGNA DI CYBERSPIONAGGIO

Secondo quanto riportato da Trellix il gruppo di cyberspionaggio DoNot APT ha recentemente portato avanti un'operazione articolata in più fasi, prendendo di mira il Ministero degli Affari Esteri italiano. Diverse aziende di cybersecurity attribuiscono questo gruppo, conosciuto anche come APT-C-35, Mint Tempest, Origami Elephant, SECTOR02 e Viceroy Tiger, all'India. In questa campagna, gli attaccanti si sono finti funzionari della difesa europei in visita in Bangladesh, convincendo le vittime a cliccare su un link malevolo ospitato su Google Drive. DoNot APT, attivo almeno dal 2016, è specializzato in attività di spionaggio informatico a scopo geopolitico, con un'attenzione particolare all'Asia meridionale. Le sue azioni si distinguono per una presenza prolungata all'interno dei sistemi bersaglio, sottrazione di dati sensibili e attività di sorveglianza continua. Il gruppo impiega spesso malware sviluppati ad hoc per Windows, come le backdoor YTY e GEdit, veicolati tramite e-mail di spear-phishing o documenti compromessi. L'obiettivo principale dell'attacco era ottenere accesso stabile all'infrastruttura della vittima e rubare informazioni riservate. L'analisi tecnica ha collegato il payload utilizzato al malware LoptikMod, uno strumento impiegato esclusivamente da DoNot APT sin dal 2018. Nonostante la loro attività sia stata storicamente rivolta all'Asia meridionale, l'attacco alle ambasciate dell'area presenti in Europa segnala un ampliamento dell'interesse del gruppo verso il monitoraggio delle comunicazioni diplomatiche e dell'intelligence europea, secondo quanto dichiarato dai ricercatori di Trellix in un report pubblicato l'8 luglio. L'attacco più recente osservato ha avuto origine da un'e-mail di spear-phishing inviata da un indirizzo Gmail camuffato come comunicazione diplomatica ufficiale (int[.]dte[.]afd[.]1@gmail[.]com). Il messaggio, indirizzato ad un organismo governativo italiano impegnato nel settore diplomatico, faceva riferimento ad una collaborazione tra Italia e Bangladesh nel contesto della difesa. Sebbene il contenuto esatto del messaggio non sia stato riportato, il suo oggetto – "Visita dell'addetto alla Difesa italiano a Dhaka, Bangladesh" – suggeriva un tentativo ben orchestrato di rendere l'e-mail credibile e compatibile con un contesto ufficiale. All'interno era presente un link a Google Drive che portava a un archivio RAR infetto denominato SyClrLtr[.]rar. Il rapporto Trellix conclude sottolineando come questo attacco ad un ministero europeo confermi la crescente ambizione del gruppo DoNot APT e la sua determinazione nel sottrarre informazioni riservate, ribadendo l'importanza di rafforzare la sicurezza informatica e l'attenzione contro minacce avanzate e persistenti.

UK, ARRESTATI QUATTRO SOSPETTATI PER ATTACCHI INFORMATICI A GRANDI MARCHI DEL RETAIL

La National Crime Agency (NCA) del Regno Unito ha arrestato quattro persone sospettate di essere coinvolte in una serie di cyberattacchi che hanno preso di mira alcuni dei principali rivenditori britannici, tra cui Marks & Spencer, Co-op e Harrods. I sospetti sono tre uomini tra i 17 e i 19 anni e una donna di 20 anni. Gli arresti sono avvenuti nelle loro abitazioni, a Londra e nelle West Midlands. Tre dei quattro sono cittadini britannici, mentre uno è di nazionalità lettone. Durante le perquisizioni, le autorità hanno sequestrato dispositivi elettronici che saranno analizzati alla ricerca di prove digitali o elementi che possano aiutare ad identificare altri eventuali complici. I quattro sono accusati di vari reati, tra cui violazione del Computer Misuse Act, estorsione, riciclaggio di denaro e partecipazione ad attività criminali organizzate. Secondo quanto ricostruito, gli attacchi sarebbero avvenuti tra la fine di aprile e l'inizio di maggio, provocando gravi disagi e danni economici alle aziende colpite. Marks & Spencer è stata costretta a sospendere temporaneamente gli ordini online e ha successivamente confermato una violazione dei dati dei clienti, obbligando tutti gli utenti a reimpostare le proprie password. Si stima che l'attacco abbia avuto un impatto finanziario pari a circa 402 milioni di dollari (300 milioni di sterline) sui profitti dell'azienda. Durante gli attacchi a Co-op e Marks & Spencer, i cybercriminali hanno cercato di installare il ransomware DragonForce. Tuttavia, solo l'attacco a M&S è andato a buon fine, mentre Co-op è riuscita a disattivare i propri sistemi prima che il malware fosse attivato. Secondo quanto riportato da BleepingComputer, gli attacchi sarebbero riconducibili al gruppo noto come Scattered Spider, una rete di hacker legata a numerose violazioni degli ultimi anni, che hanno coinvolto aziende come MGM, Twilio, Coinbase, DoorDash, Caesars, MailChimp, Riot Games e Reddit. "Da quando questi attacchi si sono verificati, i nostri investigatori specializzati in crimini informatici hanno lavorato intensamente. L'indagine rimane una delle priorità assolute per l'NCA," ha dichiarato Paul Foster, vicedirettore dell'Agenzia. "Gli arresti di oggi rappresentano un passo importante, ma il nostro lavoro continua, anche in collaborazione con partner nazionali e internazionali, per assicurare alla giustizia tutti i responsabili." Sebbene l'NCA non abbia menzionato direttamente il gruppo Scattered Spider nel comunicato ufficiale, le caratteristiche degli arrestati, tra cui età, tattiche di social engineering e background, corrispondono ai profili noti degli affiliati al gruppo, già oggetto di precedenti indagini e arresti nel Regno Unito, negli Stati Uniti e in Spagna. Gli arresti effettuati nel Regno Unito potrebbero rallentare le attività di Scattered Spider, spingendo gli altri membri a sospendere temporaneamente le operazioni. Tuttavia, poiché si ritiene che il gruppo faccia parte di una rete più ampia di hacker di lingua inglese che si coordinano attraverso piattaforme come Discord, Telegram e forum online, è improbabile che questi eventi mettano completamente fine alle loro attività.

TAPTRAP: NUOVA TECNICA DI TAPJACKING SFRUTTA LE ANIMAZIONI PER AGGIRARE LA SICUREZZA DI ANDROID

Un gruppo di ricercatori ha scoperto una nuova tecnica di tapjacking chiamata TapTrap, capace di sfruttare le animazioni dell'interfaccia utente per eludere il sistema di autorizzazioni di Android e ottenere l'accesso a dati sensibili o indurre gli utenti a compiere azioni potenzialmente pericolose, come la cancellazione completa del dispositivo. A differenza degli attacchi di tapjacking tradizionali basati su overlay, TapTrap non richiede permessi speciali e può essere eseguito anche da app apparentemente innocue. La tecnica consente infatti di lanciare un'attività trasparente e pericolosa sopra un'app legittima, sfruttando animazioni personalizzate. Questo comportamento, secondo i ricercatori, non è ancora mitigato nelle versioni Android 15 e 16. TapTrap è stato sviluppato da un team delle università TU Wien e Bayreuth (Philipp Beer, Marco Squarcina, Sebastian Roth e Martina Lindorfer) e verrà presentato ufficialmente il mese prossimo all'USENIX Security Symposium. La tecnica sfrutta il modo in cui Android gestisce le transizioni tra schermate con animazioni. Un'app malevola installata sul dispositivo target può utilizzare il comando startActivity() per lanciare una schermata di sistema sensibile, ad esempio, una richiesta di autorizzazione o le impostazioni, applicando un'animazione quasi completamente trasparente. "La chiave di TapTrap è l'uso di animazioni con opacità bassissima, che rendono la schermata bersaglio praticamente invisibile", spiegano i ricercatori. "È possibile definire un'animazione personalizzata impostando il valore alfa iniziale e finale su 0,01, rendendo così il contenuto critico praticamente trasparente." Inoltre, si può applicare un effetto di zoom per far sì che un singolo elemento (come un pulsante "Consenti") occupi l'intero schermo, aumentando la probabilità che l'utente lo tocchi inconsapevolmente. Anche se il prompt riceve effettivamente i tocchi, ciò che l'utente vede è solo l'interfaccia grafica dell'app visibile in background. Il risultato è che, credendo di interagire con un'app innocua, l'utente può in realtà toccare punti dello schermo che corrispondono a pulsanti per concedere autorizzazioni o eseguire azioni critiche. Un video dimostrativo pubblicato dai ricercatori mostra un'app di gioco che sfrutta TapTrap per attivare l'accesso alla fotocamera tramite il browser Chrome, ad insaputa dell'utente. Per verificare la portata della vulnerabilità, i ricercatori hanno analizzato quasi 100.000 app presenti su Google Play, scoprendo che il 76% di esse potrebbe essere vulnerabile a TapTrap. Le condizioni principali che rendono un'app esposta a questo tipo di attacco sono: la possibilità di essere avviata da un'altra app, l'uso della stessa attività principale dell'app che l'ha lanciata, la mancata personalizzazione delle animazioni di transizione, e il fatto che l'app non attende la fine dell'animazione prima di accettare input utente. Secondo gli autori, le animazioni sono attive di default su Android, a meno che non vengano disattivate manualmente tramite le opzioni sviluppatore o le impostazioni di accessibilità, rendendo la maggior parte dei dispositivi vulnerabile. TapTrap è stato inizialmente testato su Android 15, ma dopo l'uscita di Android 16, sono stati effettuati nuovi test che hanno confermato la persistenza del problema. Marco Squarcina ha dichiarato di aver testato TapTrap su un Google Pixel 8a con Android 16, confermando che la vulnerabilità è ancora presente. Anche GrapheneOS, il sistema operativo mobile orientato alla privacy, ha confermato che Android 16 resta esposto a TapTrap ed ha annunciato che introdurrà una patch nella prossima versione del proprio sistema operativo. Google ha risposto con una dichiarazione ufficiale: "Android continua a migliorare le proprie difese contro il tapjacking. Siamo a conoscenza di questa ricerca e il problema verrà

affrontato in un aggiornamento futuro. Google Play applica regole rigorose per la protezione degli utenti, e qualora un'app risultasse in violazione, prendiamo provvedimenti adeguati."

OLTRE 17.000 SITI COINVOLTI IN UNA TRUFFA SUGLI INVESTIMENTI ONLINE

Un nuovo rapporto pubblicato dalla società di cybersecurity CTM360 ha portato alla luce un'estesa operazione fraudolenta che si avvale di falsi siti di notizie, denominati Baiting News Sites (BNS), per orchestrare truffe legate agli investimenti in oltre 50 Paesi. Questi siti sono progettati per imitare in modo convincente portali giornalistici noti come CNN, BBC, CNBC o testate locali e pubblicano articoli fasulli che riportano dichiarazioni di personaggi famosi, banche centrali o brand finanziari. I contenuti suggeriscono falsamente il sostegno a nuovi strumenti per generare "reddito passivo". L'intento è quello di costruire rapidamente credibilità e indirizzare l'utente verso piattaforme fraudolente dall'aspetto professionale, come Trap10, Solara Vynex o Eclipse Earn. I truffatori promuovono questi siti attraverso annunci sponsorizzati su piattaforme come Google, Meta e network di blog, utilizzando titoli sensazionalistici del tipo "Scopri cosa ha appena rivelato questa celebrità", corredati da immagini ufficiali o simboli nazionali per aumentarne la legittimità percepita. Cliccando sull'annuncio, l'utente accede ad un falso articolo giornalistico che lo conduce successivamente a una piattaforma di investimento fasulla. Il raggiro si sviluppa solitamente in due fasi: nella prima, l'utente viene attirato da contenuti ingannevoli; nella seconda, dopo l'interazione iniziale, riceve una telefonata da un sedicente consulente finanziario, che richiede documenti personali, depositi in criptovalute e altre verifiche di sicurezza, tutti stratagemmi per ritardare i prelievi e mantenere la vittima nel sistema il più a lungo possibile. Questo approccio, a più livelli, aiuta i truffatori a costruire fiducia e a massimizzare il profitto prima che l'inganno venga scoperto. Sono stati individuati finora oltre 17.000 siti web coinvolti in questo schema. Molti di questi sono ospitati su domini economici (.xyz, .click, .shop), mentre in altri casi vengono compromessi siti legittimi, che ospitano i contenuti truffaldini in sottocartelle, rendendo più complesse le operazioni di rimozione. Le pagine sono spesso personalizzate per l'area geografica dell'utente, con lingue locali, loghi familiari e riferimenti a influencer o banche regionali per aumentare la fiducia. Le vittime tipiche si imbattono in queste truffe mentre cercano modi per investire online o generare reddito passivo, spesso attraverso ricerche specifiche. I contenuti sono ottimizzati per intercettare esattamente queste query, con esche come "criptotrading automatico" o "opportunità di investimento approvate da celebrità". Una volta atterrati sulla piattaforma truffaldina, agli utenti viene chiesto di registrarsi con nome, email e numero di telefono. Segue quasi subito una chiamata da un "agente di investimento", che con tono convincente e professionale, spinge la vittima a versare un primo deposito, spesso intorno ai 240 dollari. La piattaforma mostra poi finti rendimenti in tempo reale attraverso una dashboard simulata, inducendo l'utente ad investire ancora, sotto pressione costante. Oltre alla frode economica, questi schemi servono anche a raccogliere informazioni sensibili, che possono essere riutilizzate in campagne di phishing, furti di identità o altri tipi di truffe. Questo rende i siti BNS una minaccia ibrida, che combina inganno finanziario, furto di dati e impersonificazione di marchi. Il modello risulta sempre più diffuso all'interno di truffe complesse come la pig butchering, le false verifiche KYC e le frodi basate su programmi di affiliazione.

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 7 – 13 Luglio 2025
Settimana con un numero elevato di vulnerabilità critiche che colpiscono principalmente i prodotti Campcodes e alcune piattaforme di gestione industriale e gestionali. Oltre 10 CVE critiche con exploit pubblici già disponibili. Forte esposizione a SQL Injection non autenticata e a vulnerabilità in ambienti web non sicuri.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Prodotto Coinvolto	Descrizione Sintetica
CVE-2025-41672	CRITICAL	07/07/2025	❌	Sistema ICS industriale	JWT statico in ambienti ICS → accesso remoto completo non autenticato.
CVE-2025-7119	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su /users/index.php in Complaint Management System.
CVE-2025-7120	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi via parametro email in /check_availability.php.
CVE-2025-7120	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi in /admin/index.php di Complaint Mgmt System.

CVE-2025-7128	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi via parametro ID in Payroll Mgmt System (calculate_payroll).
CVE-2025-7128	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su delete_employee_attendance_single.
CVE-2025-7128	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su delete_payroll (remote, no auth).
CVE-2025-7131	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su save_employee_attendance..
CVE-2025-7132	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su save_payroll.
CVE-2025-7134	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su delete_application (Recruitment Mgmt System).
CVE-2025-7135	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su save_vacancy.
CVE-2025-7136	CRITICAL	07/07/2025	✅ GitHub	Complaint Management System (Campcodes)	SQLi su view_vacancy.php.
CVE-2025-53527	CRITICAL	07/07/2025	✅ GitHub	WeGIA (piattaforma donazioni)	Blind SQLi nel progetto WeGIA via parametro almox.

Nota: Le CVE che hanno un exploit pubblico confermato riportano un segno di spunta (verde), mentre la presenza della X sta ad indicare che l'exploit non è confermato.

Vendor e Tecnologie Coinvolti

- **Campcodes:** coinvolti tre progetti principali (Complaint, Payroll, Recruitment) con SQLi critiche in decine di endpoint.
- **Ambienti ICS:** JWT non sicuri permettono bypass completo e accesso ai dispositivi.
- **WeGIA:** piattaforma di gestione donazioni vulnerabile a SQL injection persistente.

Distribuzione Giornaliera

- Tutte le CVE pubblicate tra il **7 e l'8 luglio 2025**, con exploit già presenti su GitHub o VulDB.

Raccomandazioni

- **Azioni Immediate:**
  - Rimuovere o aggiornare tutti i software Campcodes vulnerabili.
  - Disabilitare o sostituire JWT statici in ambienti ICS.
  - Applicare la patch 3.4.1 di WeGIA.
- **Monitoraggio:**
  - Controllare traffico SQL sospetto verso endpoint ajax.php, admin/, users/, ecc.
  - Analizzare comportamenti anomali su portali HR, payroll o complaint.
- **Prevenzione:**
  - Implementare WAF con regole anti-SQLi.
  - Utilizzare parametri preparati nei backend PHP.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-1727	Sistemi di comunicazione EoT/HoT per treni (controllo remoto dei freni dei treni)	N/A
CVE-2022-38392	Seagate STDT4000100	N/A
CVE-2025-47812	Wing FTP Server	N/A
CVE-2023-45866	BlueZ (stack Bluetooth per Linux)	6.3
CVE-2025-49704	Microsoft Office SharePoint	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-2025-52950	Juniper Networks Security Director	N/A
VULNERABILITÀ	Una vulnerabilità di autorizzazione mancante in Juniper Networks Security Director consente ad un attaccante non autenticato, operante tramite la rete, di leggere o manomettere numerose risorse sensibili attraverso l'interfaccia web. Molti endpoint sull'appliance di Security Director non verificano correttamente i livelli di autorizzazione, fornendo risposta a chiamate che non dovrebbero avere accesso a tali informazioni. Un attaccante può quindi accedere a dati oltre a quelli accessibili con i propri privilegi, utilizzabili per ottenere ulteriori informazioni o eseguire altri attacchi, con impatti anche sui dispositivi gestiti a valle dell'endpoint attaccato.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-49533 CVE-2025-27203	Adobe Connect, Adobe Experience Manager (MS)	N/A
VULNERABILITÀ	Entrambe le vulnerabilità riguardano prodotti Adobe e permettono l'esecuzione di codice arbitrario tramite la deserializzazione di dati non sicuri. In Adobe Connect è necessario un intervento dell'utente, mentre in Adobe Experience Manager l'attacco può avvenire senza interazione, rendendolo potenzialmente più critico.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-7574	Dispositivi LB-LINK	N/A
VULNERABILITÀ	È stata individuata una vulnerabilità, classificata come critica, nei seguenti dispositivi LB-LINK: BL-AC1900, BL-AC2100_AZ3, BL-AC3600, BL-AX1800, BL-AX5400P e BL-WR9000, fino alla versione del firmware 20250702. La vulnerabilità riguarda la funzione reboot/restore nel file /cgi-bin/lighttpd.cgi dell'interfaccia web. La manipolazione di questa funzione porta a un'autenticazione impropria, permettendo un attacco da remoto. L'exploit è stato reso pubblico e potrebbe essere utilizzato attivamente. Il fornitore è stato contattato in anticipo, ma non ha fornito alcuna risposta.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-7217 CVE-2025-7218 CVE-2025-7219 CVE-2025-7220	Campcodes Payroll Management System	9.8
VULNERABILITÀ	Il Campcodes Payroll Management System 1.0 presenta quattro vulnerabilità critiche di SQL injection in differenti endpoint AJAX (save_position, delete_position, delete_allowances, save_deductions). Tutte sfruttano la manipolazione del parametro ID, sono sfruttabili da remoto e i relativi exploit sono pubblici, rendendo il rischio estremamente alto.	

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-2016-10033
DESCRIZIONE	
La funzione mailSend nel trasporto isMail di PHPMailer, nelle versioni precedenti alla 5.2.18, potrebbe consentire ad attaccanti remoti di inviare parametri aggiuntivi al comando mail e, di conseguenza, eseguire codice arbitrario, sfruttando un carattere \" (barra rovesciata + doppio apice) inserito in modo apposito nella proprietà Sender.	

CVE	CVE-2019-5418
DESCRIZIONE	
È presente una vulnerabilità di divulgazione del contenuto di file in Action View nelle versioni precedenti a 5.2.2.1, 5.1.6.2, 5.0.7.2, 4.2.11.1 e nella versione 3, dove intestazioni Accept appositamente manipolate possono causare l'esposizione del contenuto di file arbitrari presenti nel filesystem del sistema bersaglio.	

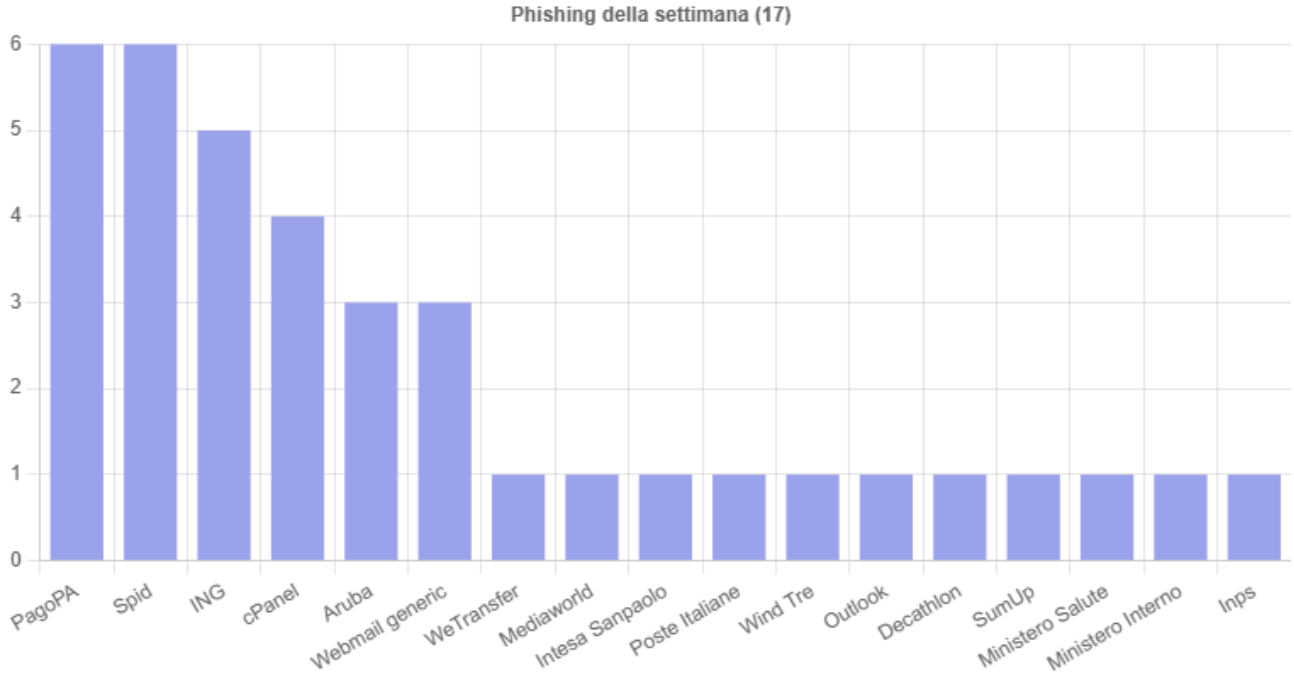
CVE	CVE-2019-9621
DESCRIZIONE	
Alcune versioni di Zimbra Collaboration Suite precedenti alle patch indicate (8.6 patch 13, 8.7.x patch 10, 8.8.x patch 7 e 8.8.x patch 3) presentano una vulnerabilità di tipo Server-Side Request Forgery (SSRF) nel componente ProxyServlet. Questa falla permette a un attaccante di far effettuare al server richieste HTTP arbitrarie verso destinazioni scelte, anche all'interno della rete interna, con possibili rischi di accesso non autorizzato e compromissione della sicurezza.	

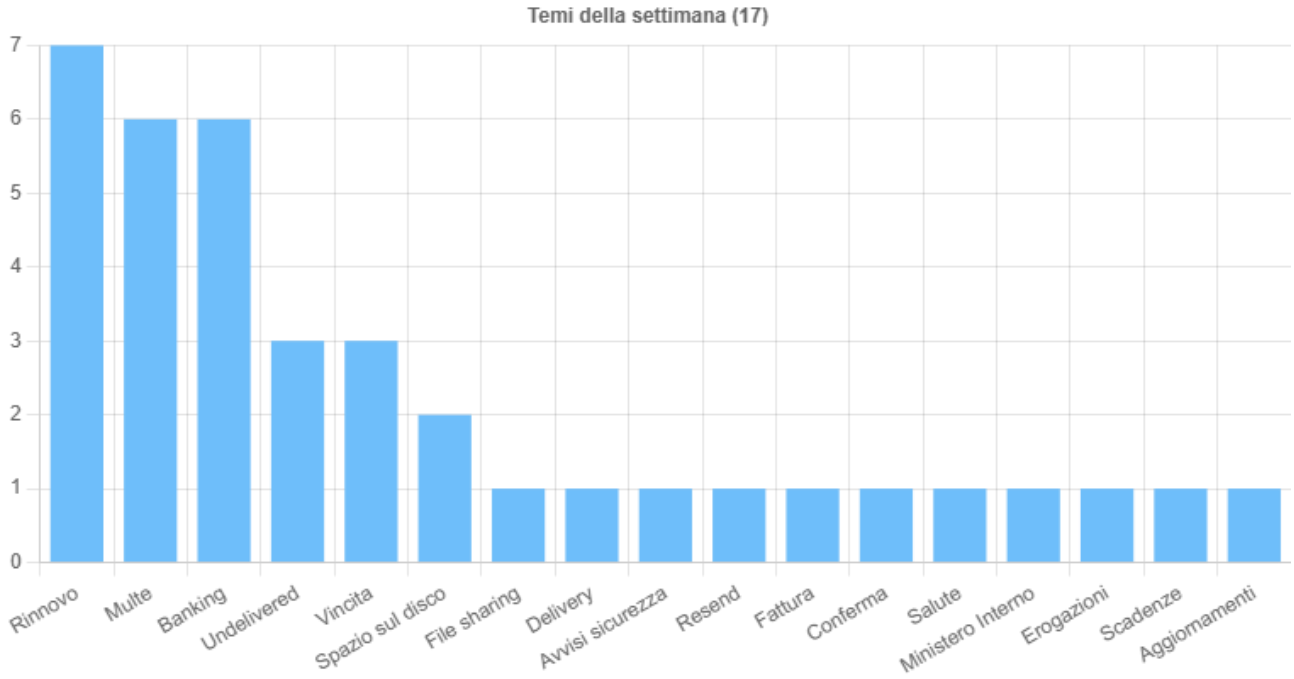
4 Attacchi

4.1 Phishing

Situazione italiana:

Nei grafici 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.

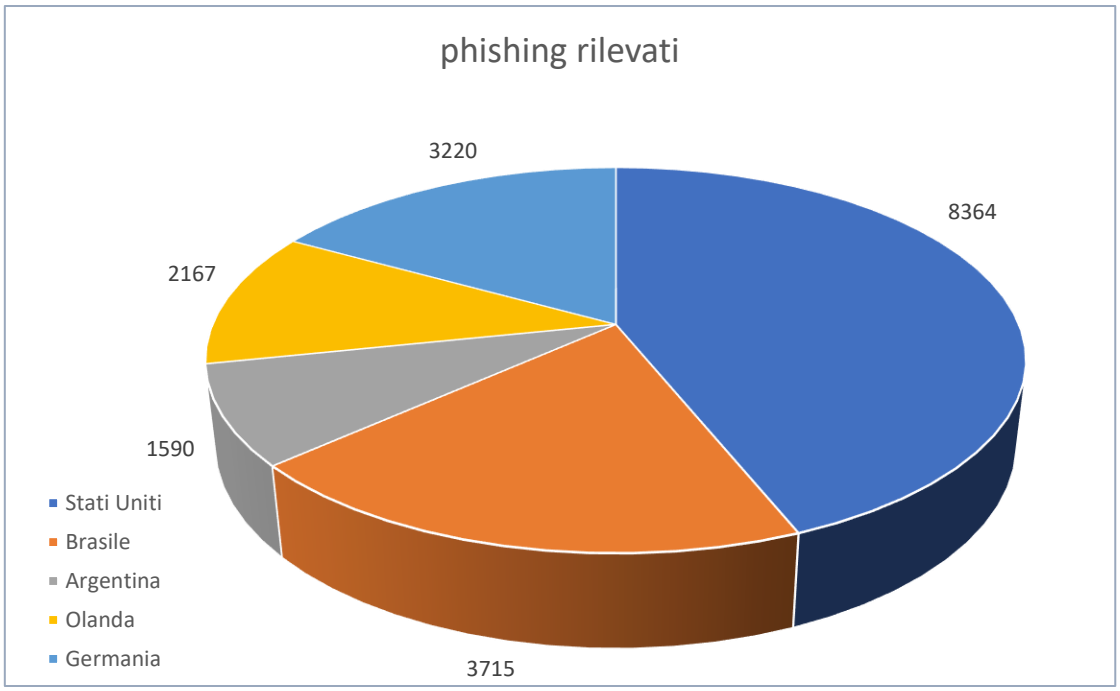




Fonte :CERT-AGID

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.

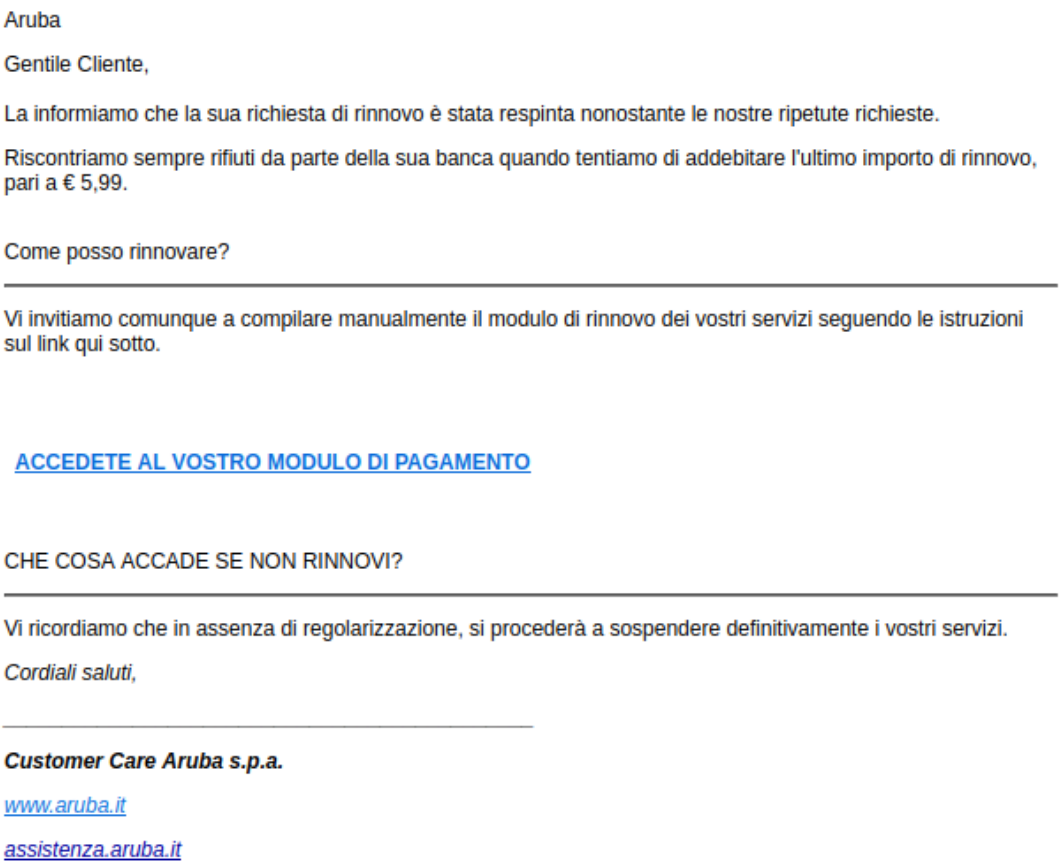


Come di consueto analizziamo una mail raccolta dalla redazione che può essere catalogata come "phishing":

Analisi Investigativa dell'Email di Phishing

- **Sintesi dell'Incidente:**

Un'email sospetta è stata ricevuta dall'indirizzo **pastor@iamsavednow[.]com** con oggetto "Fattura non pagata". Il messaggio, apparentemente proveniente da un'entità denominata "Aruba.it", contiene un link malevolo che indirizza l'utente a una pagina di pagamento fraudolenta. L'email utilizza tecniche di ingegneria sociale per indurre il destinatario a cliccare sul link, minacciando la sospensione dei servizi in caso di mancato pagamento.



Aruba

Gentile Cliente,

La informiamo che la sua richiesta di rinnovo è stata respinta nonostante le nostre ripetute richieste.

Riscontriamo sempre rifiuti da parte della sua banca quando tentiamo di addebitare l'ultimo importo di rinnovo, pari a € 5,99.

Come posso rinnovare?

Vi invitiamo comunque a compilare manualmente il modulo di rinnovo dei vostri servizi seguendo le istruzioni sul link qui sotto.

ACCEDETE AL VOSTRO MODULO DI PAGAMENTO

CHE COSA ACCADE SE NON RINNOVI?

Vi ricordiamo che in assenza di regolarizzazione, si procederà a sospendere definitivamente i vostri servizi.

Cordiali saluti,

Customer Care Aruba s.p.a.

www.aruba.it

assistenza.aruba.it

Analisi Tecnica:

- **Intestazioni dell'Email:**
  - **Mittente:** pastor@iamsavednow[.]com
  - **Destinatario:** victim@victim[.]com
  - **Server di Invio:** 195.238.122[.]169 (Kamatera Inc.)
  - **Protocollo di Trasporto:** OpenSMTPD tramite LMTP(ipinfo.io)

L'uso di un server IP associato a Kamatera Inc. è comune per attività di hosting, ma non garantisce l'affidabilità del mittente.(ipinfo.io)

- **Analisi del Dominio "iamsavednow[.]com":**

Il dominio "iamsavednow[.]com" non è registrato a nome di Aruba S.p.A.. In origine si trattava di un sito a sfondo religioso ma attualmente appare come un dominio generico utilizzato per scopi di phishing. La registrazione del dominio non è recente è il sito web è attualmente" parcheggiato" presso il provider Vix, indicando una possibile violazione subita dal dominio per utilizzarlo a scopi di phishing.

L’analisi della reputation effettuata tramite vari strumenti non rileva particolari segnalazioni a parte la presenza del dominio in una sola blacklist, segno questo di attività malevoli recenti non individuate in precedenza.

- **Analisi del Link Malevolo:**

Il link contenuto nell'email indirizza a:

https://jobiz[.]life/newar.php

Il certificato del dominio è scaduto nel 2023 e risulta parcheggiato presso Epik platform.

Questo URL non è associato a nessun servizio ufficiale di Aruba e sembra essere stato creato per imitare una pagina di pagamento legittima.

Il dominio jobiz[.]life con IP 209[.]196[.]146[.]115 è segnalato come malevolo.

- **Analisi dell'IP di Invio (195[.]238[.]122[.]169):**

Secondo le informazioni disponibili, l'IP 195[.]238[.]122[.]169 è associato a Kamatera Inc., un provider di servizi cloud. Tuttavia, l'assenza di un dominio associato e la presenza di numerosi domini sospetti nella stessa rete indicano un potenziale uso improprio dell'infrastruttura.

- **Verifica della Reputazione del Dominio e dell'IP:**

Utilizzando strumenti di verifica della reputazione, è emerso che l'IP 195.238.122[.]169 non è attualmente presente in blacklist note. Tuttavia, la presenza di domini sospetti nella stessa rete potrebbe indicare un rischio elevato associato a questo IP.

- **Certificato SSL/TLS del Dominio "iamsavednow[.]com":**

Essendo “parcheggiato”, il dominio "iamsavednow[.]com" non dispone di un certificato SSL/TLS valido.

- **Analisi del Contenuto dell'Email:**

L'email presenta i seguenti elementi tipici di phishing:

  - **Mittente Fittizio:** "Aruba.it" con indirizzo email "pastor@iamsavednow[.]com".
  - **Minaccia Urgente:** "La informiamo che la sua richiesta di rinnovo è stata respinta".
  - **Richiesta di Azione Immediata:** Invito a cliccare su un link per completare il pagamento.
  - **Link Malevolo:** https://jobiz[.]life/newar.php.
  - **Firma Fittizia:** "Customer Care Aruba S.p.A." con link al sito ufficiale di Aruba.

- **Allegati e Link:**

Non sono stati rilevati allegati nell'email. Tuttavia, il link presente è stato identificato come malevolo e potenzialmente pericoloso.

- **Indicatori di Compromissione (IoC):**
  - **Indirizzo Email del Mittente:** pastor@iamsavednow[.]com
  - **Indirizzo IP di Invio:** 195[.]238[.]122[.]169
  - **Dominio del Link Malevolo:** jobiz[.]life
  - **IP del dominio malevolo:** 209[.]196[.]146[.]115
  - **URL del Link Malevolo:** https://jobiz[.]life/newar.php

Conclusioni:

L'email analizzata presenta caratteristiche tipiche di un attacco di phishing, tra cui l'uso di un mittente falso, minacce urgenti, link malevoli e la mancanza di autenticazione del dominio. Nonostante l'IP di invio non sia attualmente presente in blacklist, la presenza di domini sospetti nella stessa rete e l'assenza di un certificato SSL/TLS valido per il dominio "iamsavednow[.]com" indicano un alto rischio associato a questa comunicazione.

Si raccomanda di:

- **Non cliccare sul link** presente nell'email.
- **Segnalare l'email** come phishing al proprio provider di servizi email.
- **Verificare l'autenticità** di qualsiasi comunicazione ricevuta da Aruba S.p.A. attraverso i canali ufficiali.

Riportiamo ora un'analisi dettagliata delle campagne di phishing più attive nel corso dell'ultimo trimestre.

- **Phishing via Google/Gmail (attacco DKIM Replay)**

Il 23 aprile 2025 è emersa una campagna di phishing particolarmente insidiosa che impersona avvisi ufficiali di Google. Gli aggressori hanno sfruttato una combinazione di vulnerabilità nei servizi Google per inviare email di phishing autentiche da account "no-reply@google.com" firmate correttamente con DKIM. Le email segnalavano falsi "sovraccarichi" o richieste legali sull'account dell'utente e contenevano link a pagine di login contraffatte, ospitate su sottodomini di Google Sites (ad es. sites.google.com/...). Grazie a questa tecnica di DKIM replay, i messaggi bypassavano i filtri anti-phishing standard, apparendo perfettamente legittimi nelle caselle di posta delle vittime.

Nome/Attore: campagna non attribuita; attori sconosciuti (potenzialmente un "click fraud" o organizzazione criminale) dietro il DKIM replay.
Strategia di phishing: spear-phishing via email con mittente contraffatto di Google. Le email fingevano di essere avvisi di sicurezza legittimi (ad es. "notifica di indagine legale sul tuo account") e contenevano link a pagine compromesse su sites.google.com. Queste pagine imitavano perfettamente l'interfaccia di accesso Google o portali di supporto, inducendo la vittima a inserire le proprie credenziali.
Indicatori di compromissione (IoC): pagine di phishing ospitate su domini legittimi di Google (e.g. sites.google.com), link con parametri anomali. Non sono noti IP o domini malevoli distinti, poiché il caricamento avviene via Google Sites. Ad esempio, gli URL visualizzati cominciavano con sites.google.com o support.google.com, anche se il dominio signed-by risultava legittimo.
MITRE ATT&CK: Spearphishing Link (T1566.002); Esecuzione Utente (T1204.002) su pagine web; uso di Autenticazione Alternativa (T1550.004) e Furto cookie di sessione (T1539) sfruttando credenziali rubate.
Contromisure: abilitare sempre l'autenticazione a due fattori (es. via passkey o token) sugli account Google; informare gli utenti sulla minaccia e insegnare a riconoscere avvisi falsi da siti.google.com. Implementare filtri anti-phishing che flagghino email firmate (DKIM) con comportamenti sospetti; applicare soluzioni EDR in grado di rilevare tentativi di furto di sessione. Google ha affermato di aver già introdotto contromisure tecniche e raccomanda 2FA/passkeys.
Rischio: Alto. Questo attacco ha sfruttato debolezze interne a Google e ha ingannato anche utenti tecnici, mostrando l'efficacia di un'email perfettamente firmata.

- **Kit Tycoon 2FA (Phishing MFA-Bypass)**

Il kit Tycoon 2FA è un servizio di phishing-as-a-service emerso nel 2023 e in rapida evoluzione nel 2024-2025. Tycoon 2FA crea pagine di login fasulle (tipicamente Microsoft 365/Gmail) e sfrutta tecniche "man-in-the-middle" per intercettare credenziali e cookie di sessione, permettendo agli attaccanti di bypassare l'autenticazione a due fattori. A partire da novembre 2024 sono stati osservati aggiornamenti che rendono le pagine più realistiche (loghi personalizzati), la catena di redirect più lunga e il codice fortemente offuscato. Le email di phishing vengono spesso inviate da account legittimi o compromessi (es. servizi SMTP affidabili) per sfuggire ai controlli.

Nome/Attore: Tycoon 2FA (noto kit PhaaS). Non si tratta di un gruppo specifico riconosciuto, ma di un toolkit usato da varie gang di phishing. Il kit è associato a un gruppo denominato "Saad Tycoon" e viene pubblicizzato su forum sotterranei.
Strategia di phishing: invio di email di phishing mirate (spesso da account compromessi) con link ad una catena di redirezioni che terminano in pagine di login fasulle di servizi cloud (Microsoft 365, Gmail, etc.). Il kit inserisce un proxy malevolo tra il browser della vittima e il servizio reale, rubando cookie di sessione all'atto del login. Alcune varianti includono anche codici QR malevoli o finti aggiornamenti (es. avvisi di update WordPress). Le pagine di phishing dispongono di sofisticate misure anti-analisi (disabilitano click destro, blocco di strumenti di debug, CAPTCHA dinamici) per sfuggire ai rilevamenti automatici.
IoC:

Tipo	Valore / Esempio	Descrizione
Dominio d'appoggio	tycoongroup[.]ws	Dominio usato per ospitare il kit di phishing Tycoon
URL sospetti	login[.]microsoft-update[.]xyz, secure-mail-auth[.]info	Domini ingannevoli che simulano portali di login aziendali o servizi cloud

Tecniche MITRE: Spearphishing Link (T1566.002) e Allegato (T1566.001) – utilizzo di email di phishing. Evasione sandbox/virtualizzazione (T1497.001) tramite rilevamento strumenti di debugging. Offuscamento (T1027) e modifica della clipboard. Uso di session cookie (T1550.004, T1539) e Adversary-in-the-Middle (T1557) per rubare credenziali e autenticazioni.
Contromisure: usare EDR/XDR con analisi comportamentale per captare furto di cookie e login sospetti. Filtri email avanzati (spam/XDR) per individuare URL anonime, regole anti-URL offuscate e servizi di URL scanning intelligenti. Formare gli utenti a non cliccare link imprevisti e in generale a diffidare di richieste di login inattese. Monitorare i log di autenticazione (sessioni multiple o da IP sconosciuti). Tenere aggiornati i sistemi antifrode basati su UEBA (es. rilevamento di login anomali).
Rischio: Alto. Tycoon 2FA è un kit economico ma potente, capace di ingannare 2FA e MFA tradizionali. Gli utenti possono cadere nella trappola anche con un livello di attenzione discreto, e la compromissione di account aziendali ha impatti gravi. Le contromisure standard (autenticazione a più fattori) possono risultare inefficaci senza specifiche soluzioni di rilevamento cookie

- **Campagna PoisonSeed (falsa seed phrase Coinbase)**

PoisonSeed è una campagna di phishing ribattezzata così da esperti Silent Push (aprile 2025). L'attacco è in due fasi: prima compromette account di servizi email di massa (MailChimp, SendGrid, HubSpot, Zoho, ecc.) tramite phishing mirato ai loro gestori. Da quegli account furono esportate liste di indirizzi. Nella seconda fase, gli ignari iscritti ricevono email apparentemente da exchange crypto (es. Coinbase) che segnalano una transizione a "portafogli self-custodial". Il messaggio invita a incollare una falsa seed phrase di 12 parole nel proprio wallet – in realtà il seed consegna agli attaccanti pieno accesso al wallet della vittima. Fra le vittime confermate c'è anche un noto esperto di sicurezza (Troy Hunt).
Nome/Attore: campagna "PoisonSeed" (la designazione proviene da Silent Push). Gli autori non sono confermati, ma il loro modus operandi ha analogie con gruppi noti (CryptoChameleon/Scattered Spider) sebbene classificato separatamente.
Strategia di phishing: supply-chain di campagne di mailing. Inizialmente i cybercriminali inviarono email di phishing ai gestori di servizi CRM/bulk mail (usando domini e-mail provider falsi o compromessi come cloudflare-sendgrid.com, mail-chimpservices.com), per rubare le credenziali di quegli account. Successivamente, dalla piattaforma compromessa sono state inviate email massive ai clienti/lista del provider col prefisso del brand (es. presunte email da "Coinbase Support") con un invito a importare una seed phrase. Le email erano confezionate in modo molto convincente (pixel-perfect).
IoC:

Tipo	Indicatore
Domini	connect1-coinbase[.]com, sso-account[.]com, mailchimp-ssologin[.]com
URL	https://connect1-coinbase[.]com/sso (esempio)
Allegati	*Nessuno* (phishing tramite form web)
IP	212[.]224[.]88[.]188; 86[.]54[.]42[.]92

Tecniche MITRE: Spearphishing Link (T1566.002) – utilizzo di email mimetiche con link a siti falsi. In questo caso non si tratta di malware allegati, ma di furto di credenziali e social engineering. Potrebbe rientrare in Watering Hole o supply-chain (se considerati sotto T1195/T1608), ma principalmente è phishing.
Contromisure: bloccare a livello di gateway i domini sospetti (configurare liste di blocco per domini come quelli indicati). Monitorare eventuali accessi insoliti a provider di posta (autenticazione multi-fattore, riconoscimento anomalo di IP). Addestrare il personale e gli utenti finali a diffidare di email che invitano a incollare seed phrase o modificare wallet crypto. Utilizzare filtri antispam/antiphishing con reputazione dei domini e phishing detection specifica per crypto. In caso di compromissione di un account bulk, revocare immediatamente le sue API e credenziali.

Rischio: Alto. Il metodo è sofisticato e mira a trasferire direttamente i fondi delle vittime. Gli obiettivi includono utenti al di fuori del settore crypto tradizionale, con campagne mirate su aziende grandi (es.

Coinbase) e utenti privati. Gli effetti possono essere finanziari gravi (furto dei wallet) in quanto le vittime consegnano direttamente il controllo del proprio denaro.

- **Campagna Lazarus – "ClickFake Interview"**

Il Lazarus Group (gruppo APT legato alla Corea del Nord) ha lanciato una campagna mirata contro sviluppatori attivi nel settore delle criptovalute, nota come "ClickFake Interview". Gli obiettivi ricevevano messaggi su LinkedIn o altri social network, contenenti finti inviti a colloqui di lavoro presso presunte aziende del settore crypto.
I link contenuti nei messaggi reindirizzavano a decine di falsi portali di interviste che impersonavano società legittime come Coinbase, Kraken, Ripple, ecc. Questi siti simulavano vere e proprie interviste online, includendo moduli da compilare e richieste di registrare un video tramite webcam.
Durante il tentativo di attivare la webcam, veniva mostrato un messaggio di errore, con l'invito a installare un presunto "driver di sicurezza". A quel punto, la vittima era indotta a scaricare ed eseguire un comando PowerShell (tecnica nota come ClickFix), che installava un malware backdoor chiamato GolangGhost.
Questo malware permetteva agli attaccanti di esfiltrare file locali, credenziali salvate nel browser, e informazioni relative a wallet di criptovalute.
Nome/Attore: Lazarus Group (APT nordcoreana).
Contesto: Campagna in continuità con precedenti operazioni come Dream Job e Contagious Interview, anch'esse mirate a sviluppatori nel settore crypto.
Strategia di phishing:
Spear-phishing tramite social network professionali (es. LinkedIn) ed email. L'esca consiste in falsi portali per colloqui di lavoro dall'aspetto credibile. La tecnica principale sfrutta un meccanismo di ingegneria sociale tipo ClickFix: al momento della richiesta di attivazione webcam, l'utente è indotto a eseguire comandi PowerShell o tramite prompt di sistema per installare un falso driver.
Questo innesca una catena di compromissione basata su script e payload scritti in Python o PowerShell, che portano all'installazione del malware.
IoC:

Tipo	Valore / Esempio	Descrizione
Dominio sospetto	krkcoinbase[.]com, coinba-seapi[.]com	Domini simili a brand legittimi (es. Coin-base, Kraken)
Pattern dominio	Simulazione di brand crypto + API/client UI (coinbase, kraken, rip-ple)	Utilizzati per ingannare gli utenti con in-terfacce "familiari"
Numero domini	Oltre 180 URL unici	Secondo Sekoia, domini frequentemente variati e difficilmente tracciabili
File allegati	references[.]pdf[.]lnk, altri .lnk	File shortcut Windows che eseguono co-mandi maligni

Tecniche MITRE: Spearphishing Link (T1566.002) via messaggi LinkedIn/email. Esecuzione Utente (T1204.002) – comando PowerShell eseguito su richiesta dell'utente (ClickFix). Persistenza attraverso backdoor GolangGhost (T1053, T1574). Raccolta di credenziali (T1539 Furto cookie) e dati (stealing browser info).
Contromisure: verificare sempre la veridicità di offerte di lavoro inaspettate, specialmente quelle legate a crypto. Addestrare gli utenti a rifiutare comandi "installa driver" o download non richiesti durante call di intervista. Bloccare l'esecuzione di script PowerShell non firmati tramite policy di gruppo (GPO) e software whitelisting. Utilizzare EDR per monitorare processi sospetti (es. qualsiasi Python o shell script avviato involontariamente). Abilitare scan di rete e endpoint per rilevare download anomali da URL stranieri.
Rischio: Alto – Critico. Lazarus è noto per furti di massa di cryptocurrency (oltre $2B nel 2023-24). Compromettere uno sviluppatore crypto può portare a perdite immediate. Inoltre la tecnica convince l'utente di agire "manualmente", rendendo difficile il rilevamento.

- **Campagna Cloudflare (DMCA Phishing + Telegram C2)**

All'inizio di aprile 2025 è stata scoperta una campagna di phishing che sfruttava i servizi Cloudflare (Pages.dev, Workers.dev) in modo insolito. I criminali inviavano email di tipo lure su presunte violazioni del DMCA, inducendo le vittime ad "accedere a documenti" tramite un link che reindirizzava a siti ospitati su Cloudflare Pages (es. devgrid-72kx.pages.dev). La pagina mostrava un finto pulsante "Get Document" e, tramite il protocollo search-ms:, scaricava un file Windows .LNK camuffato da PDF (ad es. references[.]pdf[.]lnk). Aprendo tale collegamento, veniva eseguito uno script PowerShell che scaricava un archivio ZIP contenente il malware.
Inoltre, il malware iniziale contattava un bot Telegram controllato dagli attaccanti per trasmettere l'indirizzo IP della vittima, prima di connettersi a un server C2 (Pyramid C2) per ricevere ulteriori comandi..

Strategia di phishing: spear-phishing via email con link malevolo. Le email sfruttavano pagine ospitate su Cloudflare (*.pages.dev e *.workers.dev), che impersonavano un servizio di condivisione sicura di documenti. Veniva utilizzata la tecnica search-ms per lanciare un collegamento .LNK tramite Esplora Risorse. Il file .LNK conteneva uno script che scaricava e decriptava un archivio contenente il malware (KursorResources.zip). In sintesi, l'esca basata su Cloud scaricava un .LNK malevolo, che a sua volta eseguiva un trojan scritto in Python. Il bot Telegram raccoglieva l'IP infetto e lo inviava agli attaccanti.

IoC:

Tipo	Indicatore
Domini	devgrid-72kx[.]pages[.]dev; idufgljr[.]procansopa1987[.]workers[.]dev
IP	213[.]209[.]150[.]191:80
Allegati	references[.]pdf[.]lnk (shortcut malevolo)
Hash file	SHA256(references[.]pdf[.]lnk): bf3b19c30085a9611650aa283856bf3defec894aae0b303ccf90244746127206

Tecniche MITRE: Spearphishing Attachment (T1566.001) tramite file .lnk. Esecuzione Utente (T1204.002) – utente avvia manualmente lo script dal collegamento. Comando PowerShell (T1059.001) eseguito. Persistenza/avvio di servizio (T1543). Comunicazione C2 su Telegram (T1573.002 con Telegram).
Contromisure: bloccare sul proxy/EDR i domini Cloudflare sospetti e il protocollo search-ms: nei browser. Segnalare a Google e Cloudflare i sottodomini abusati per rapida rimozione. A livello endpoint, impedire l'esecuzione di shortcut .LNK non firmati e abilitare il monitoraggio di PowerShell attivo. Monitorare traffico verso domini Telegram e Cloudflare sospetti. Formare gli utenti a non aprire file scaricati via link ingannevoli. Impostare restrizioni GPO su .LNK e script.
Rischio: Medio-Alto. Pur non essendo un attacco di grande scala, sfrutta innovativamente l'infrastruttura Cloudflare e mette in luce come siti legittimi possano veicolare malware. L'infezione richiede azione dell'utente (aprire il .LNK), ma i ricercatori avvertono che anche utenti attenti potrebbero cadere nell'inganno. Le conseguenze includono furto di dati e ransomware, pertanto è un rischio significativo.

- **Phishing PagoPA (false fatture)**

Nel mese di maggio 2025, si è intensificata in Italia una campagna di phishing a tema PagoPA. Le email fraudolente simulavano richieste di pagamento per somme non dovute (es. presunte multe o quote da saldare), generalmente intorno ai 75 euro. I messaggi contenevano link a siti web fasulli che imitavano fedelmente l'interfaccia del portale PagoPA, inducendo le vittime a inserire dati personali e informazioni della carta di credito, con il pretesto di regolarizzare una presunta sanzione amministrativa.
Secondo quanto segnalato dal CERT-AGID, queste campagne hanno registrato una crescita significativa, con 45 episodi censiti tra marzo e giugno 2025.
Strategia di phishing: Email di massa scritte in italiano (talvolta anche tramite smishing/SMS) con oggetti relativi a multe o pagamenti PagoPA. I messaggi invitano la vittima a "regolarizzare la sanzione" cliccando su un link o scaricando un documento. I collegamenti conducono a siti truffaldini non indicizzati, progettati per imitare layout, loghi e contenuti riconducibili a PagoPA o alla Polizia Locale.
Vengono richiesti dati identificativi come nome, codice fiscale e dati della carta di credito. In alcuni casi, per conferire maggiore credibilità, vengono utilizzati brand fittizi come Ufficio Verbali o riferimenti al Comune di residenza..

IoC:

Tipo	Valore / Esempio	Descrizione
Email mittente	@pago-pa[.]it	Dominio simile a quello ufficiale, ma non legittimo
Email mittente	@amministrazionelocale[.]xyz	Dominio fraudolento mascherato come istituzionale
URL sospetti	http://pagopa-verifica[.]com, https://pago-fattura[.]top	Esempi tipici di URL fraudolenti che imitano portali di pagamento
Parole chiave	"PagoPA", "multa", "sanzione"	Termini comuni nei subject e contenuti delle email phishing
Pattern dominio	Contiene "pago" o "pa"	Utilizzati per creare domini simili a quelli reali

Tecniche MITRE: Spearphishing Link (T1566.002) – invio di link malevoli. L'uso di SMS (smishing) ricade in phishing via SMS (T1537). Utilizzo di pagine fasulle (Web Kit Phishing).
Contromisure: soluzioni EDR/UEBA possono intercettare login da siti esterni sospetti. Filtri email basati su HTML randomizzato (soprattutto se la pagina difende da analisi automatizzate) possono essere efficaci. Potenziare l'awareness degli utenti con training dedicati sulle frodi PagoPA e diffidare di richieste urgenti di pagamento non comunicate su canali ufficiali. Collaborazione CERT-AGID e PagoPA per inviare alert ai cittadini e rimuovere rapidamente domini di phishing segnalati.
Rischio: Medio. Coinvolge le vittime individuali con perdite economiche dirette (dati carta rubati). L'uso del marchio istituzionale rende l'attacco credibile, ma non si tratta di un malware sofisticato: è social engineering puro. Tuttavia, l'alto volume di email aumenta l'impatto complessivo.

- **Phishing Ministero della Salute**

Nello stesso periodo è emersa una campagna parallela che impersonava il Ministero della Salute. Le email, strutturate con linguaggio istituzionale e corredate da loghi ufficiali, promettevano un rimborso fiscale o un contributo economico a favore del cittadino, invitando l'utente a cliccare su un link.
In alcuni casi, il dominio utilizzato era ministerosalute[.]io.
Una volta cliccato il link, la vittima veniva indirizzata a una pagina fraudolenta, progettata per imitare un modulo online (simile a un Google Form o a un sito web creato ad hoc), dove veniva richiesto l'inserimento di dati anagrafici e informazioni bancarie (es. carta di credito o IBAN), con la scusa di "verificare" l'erogazione del rimborso.
Strategia di phishing: Campagna via email a tema sanitario/finanziario, spacciata per comunicazione ufficiale del Ministero della Salute. I messaggi facevano riferimento a presunti rimborsi fiscali o contributi per spese mediche, al fine di indurre l'utente a fornire dati personali e bancari. Il link conduceva a pagine fake dall'aspetto credibile, spesso realizzate con strumenti gratuiti o servizi di hosting temporaneo.

IoC:

Tipo	Valore / Esempio	Descrizione
Dominio sospetto	ministerosalute[.]io	Dominio fraudolento che simula il sito ufficiale del Ministero (quello reale è .gov.it)
Dominio sospetto	ministerosalute[.]xyz, altri simili	Possibili varianti future con TLD diversi ma nome simile
Parole chiave	"scaricare modulo rimborsi", "SPID", "rimborso"	Frasi usate nei messaggi email per spingere l'utente ad aprire link o allegati

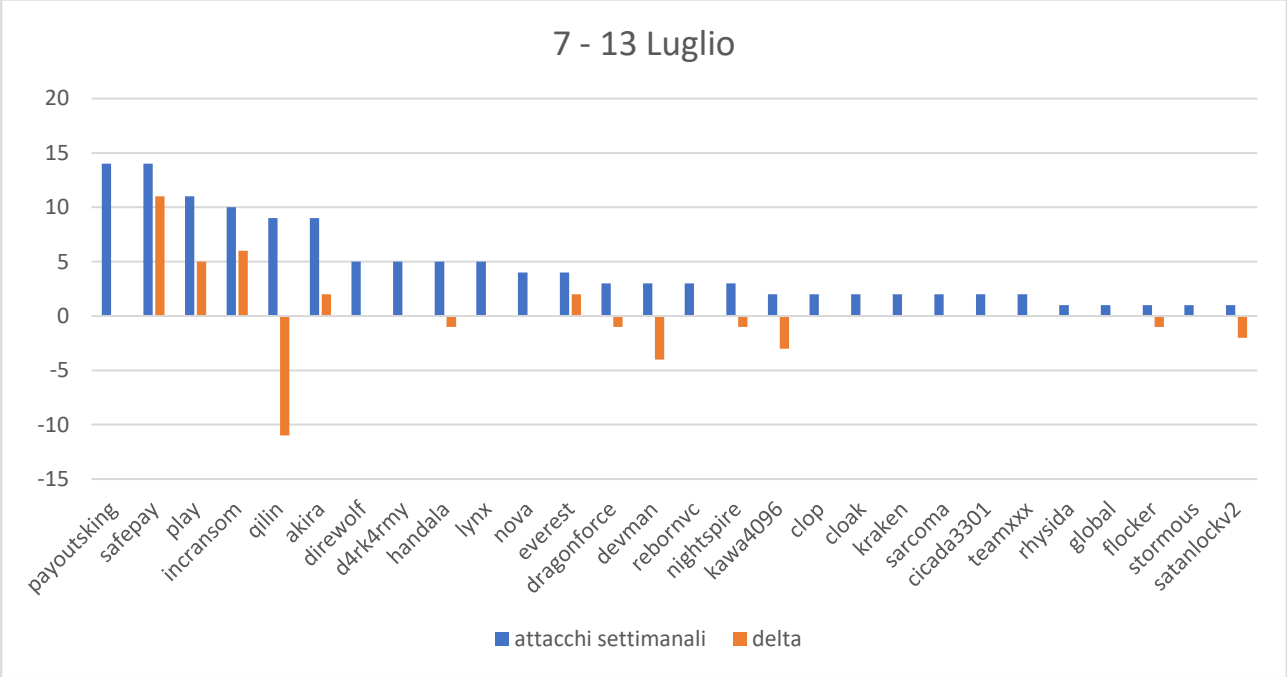
Tecniche MITRE: Spearphishing Link (T1566.002) via email.
Contromisure: blocco immediato di domini contraffatti che contengono "ministerosalute". Aggiungere filtri anti-phishing per pagine che replicano siti del Governo. Informare pubblico e personale sanitario di non fidarsi di email di rimborso non richieste. Anche qui EDR/ATP che controllano il caricamento di pagine inaspettate.
Rischio: Medio. L'attacco tenta di estorcere informazioni finanziarie direttamente agli utenti finali. Non comporta iniezione di malware, ma la divulgazione di dati personali e bancari. La fiducia nel brand Ministero lo rende insidioso.

Tabella Riepilogativa — Tendenze Attacchi di Phishing (Ultimi 3 Mesi)

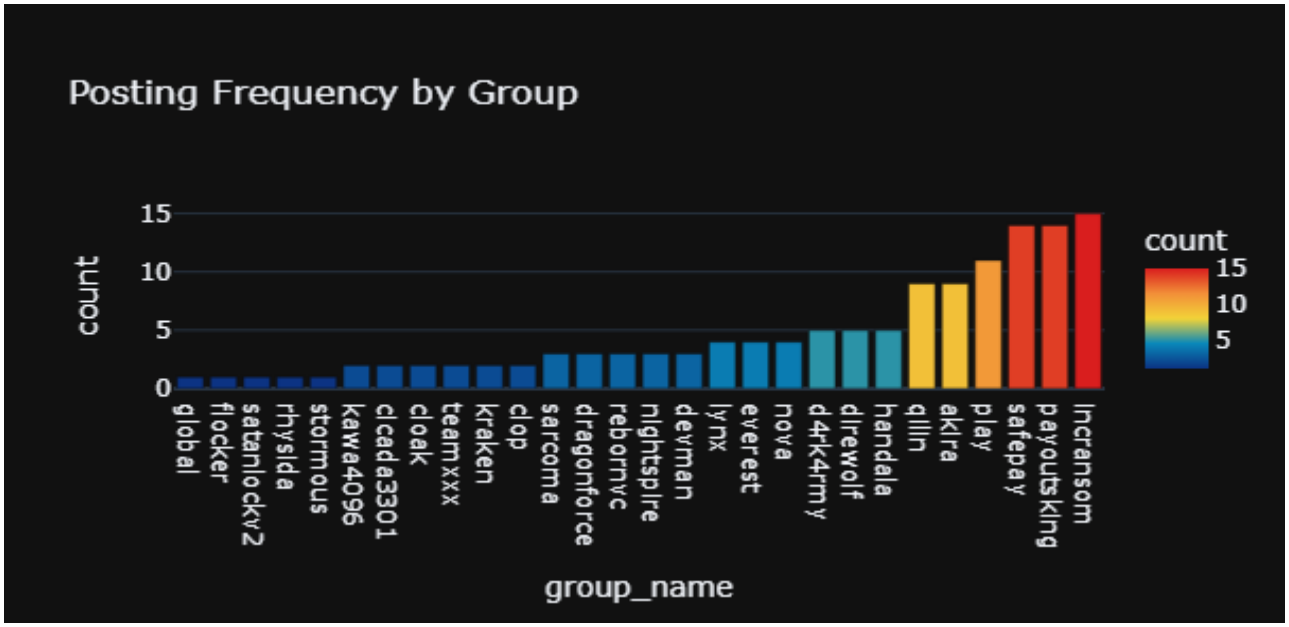
Campagna / Nome	Strategia / Tecnica	Rischio	Data
DKIM Replay / Gmail Abuse	Email fittizie "da Google" + pagine hostate su Google Sites	Alto	23 aprile 2025
Tycoon 2FA Phishing Kit	Email da account legittimi + pagine login fake + furto cookie MFA	Alto	Aprile – Giugno 2025
PoisonSeed (Crypto Scam)	Bulk email con link per rubare seed phrase crypto	Alto	4–7 aprile 2025
Lazarus – ClickFake Interview	Finto recruiter LinkedIn + link maligno (ClickFix)	Alto / Critico	Marzo – Giugno 2025
Cloudflare DMCA Phishing	Email DMCA falsa + hosting file su Cloudflare Pages / Workers	Medio-Alto	1 aprile 2025
PagoPA – Fatture False	Email massive su multe/fatture fasulle da "PagoPA"	Medio	22 aprile 2025
PagoPA – False Multe	Email mirate con avvisi di multe fasulle	Medio	Maggio 2025
Ministero Salute – Falsi Rimborsi	Email da finto "Ministero della Salute" per rimborsi Covid	Medio	14–15 aprile 2025

4.2 Ransomware

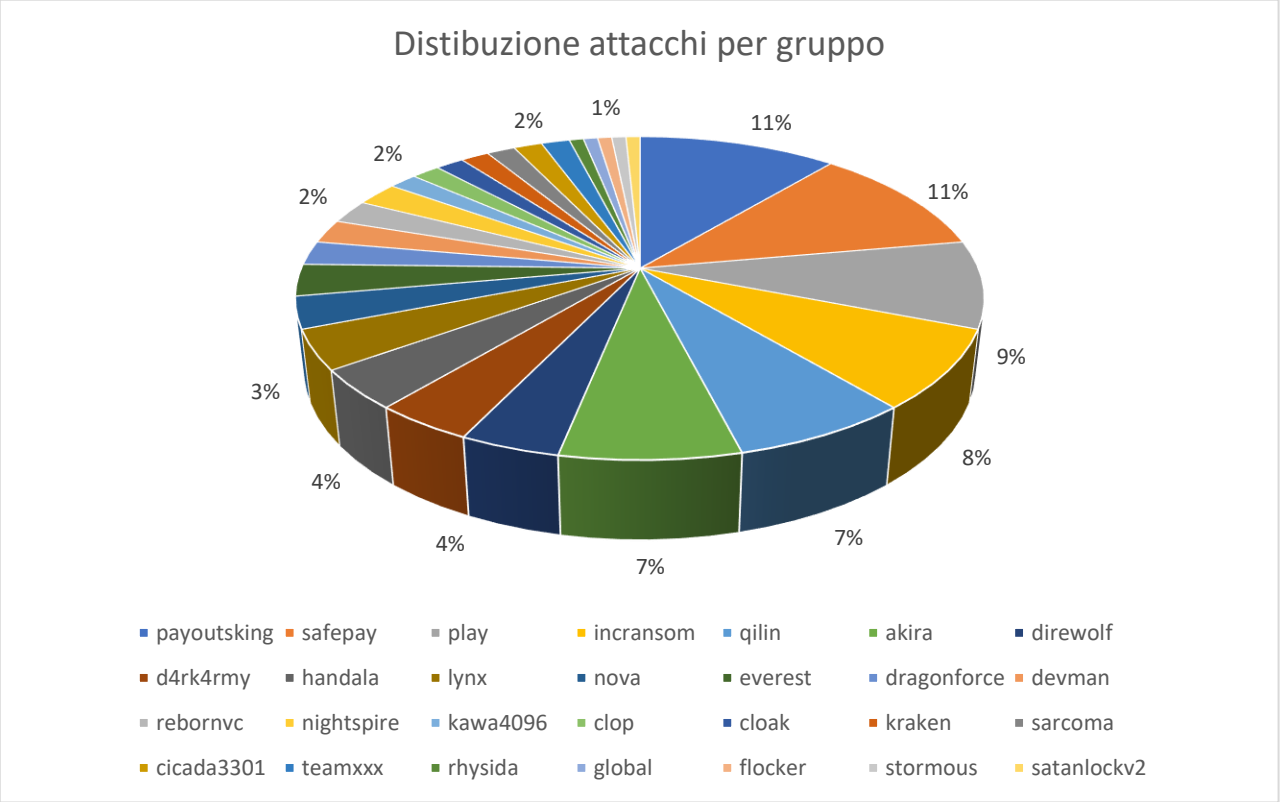
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (7 - 13 Luglio). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

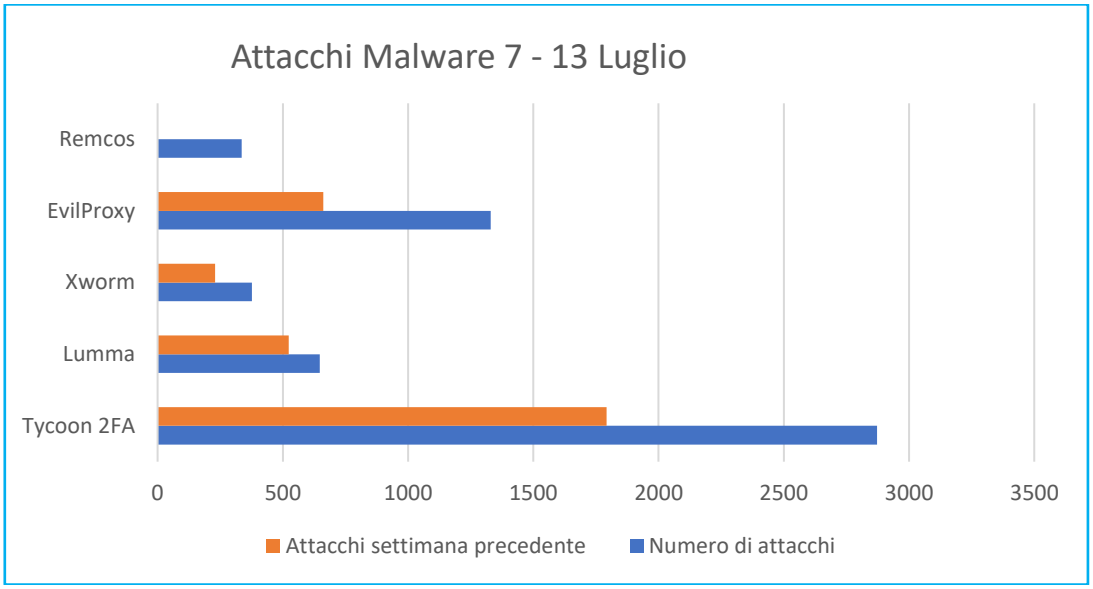


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



4.3 Malware

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



Riportiamo un'analisi dettagliata dei malware risultati più attivi nella settimana di osservazione

- **macOS.ZuRu**

Una nuova variante del malware macOS noto come ZuRu è stata scoperta a fine maggio 2025 e resa pubblica su 10 luglio 2025. Questa variante utilizza l'applicazione legittima Termius (SSH client) modificata: al suo interno i criminali hanno inserito due eseguibili malevoli (.localized loader e ".Termius Helper1") che scaricano il backdoor Khepri da un server C2 (il dominio download[.]termius[.]info). In particolare, il loader richiama il C2 via HTTP (es. http://download[.]termius[.]info/bn[.]log[.]enc) e verifica la versione via hash MD5, gestendo un meccanismo di aggiornamento. Anche il server di comando e controllo (C2) principale è un dominio fittizio: ctl01[.]termius[.]fun, che risolve all'IP Alibaba 47[.]238[.]28[.]21.

IoC:

Tipo IoC	Valore	Descrizione
Hash SHA-1	a7a9b0f8cc1c89f5c195af74ce3add74733b15c0	Payload .fseventsd (beacon Khepri)
Hash SHA-1	ace81626924c34dfbcd9a485437cbb604e184426	Termius Helper1 (Mach-O trojan)
Hash SHA-1	de8aca685871ade8a75e4614ada219025e2d6fd7	Termius9.5.0.dmg (immagine disco trojan)
Hash SHA-1	fa9b89d4eb4d47d34f0f366750d55603813097c1	Loader .localized (Termius Malware Loader)
Dominio	download[.]termius[.]info	C2 di primo livello (ricarica payload)
Dominio	ctl01[.]termius[.]fun	C2 utilizzato per beaconing (dominio fittizio)
IP	47[.]238[.]28[.]21	IP Alibaba associato a ctl01[.]termius[.]fun
File	Termius9.5.0.dmg	Nome dell'immagine disco infetta
File	/Library/LaunchDaemons/com[.]apple[.]xssooxx-agent[.]plist	Plist di persistenza creato da ZuRu

MITRE ATT&CK:

- **T1574.007 – Entrypoint Obfuscation**: caricamento di librerie in esecuzione.
- **T1547.001 – Launch Agent**: persistenza tramite file LaunchDaemon.
- **T1059 – Command and Scripting Interpreter**: esecuzione di comandi sul sistema compromesso.
- **T1071.001 – Web Protocols**: comunicazione mascherata con il server di comando e controllo (C2), spesso tramite domini apparentemente legittimi (es. baidu.com usato come decoy).

Contromisure (rilevazione e mitigazione):

- Applicare **policy restrittive** sui dispositivi macOS (es. bloccare applicazioni non firmate da sviluppatori affidabili).
- **Monitorare percorsi sensibili** come /tmp e i file di persistenza creati nei LaunchDaemon.
- Utilizzare soluzioni **EDR o antimalware avanzati** capaci di rilevare il malware Khepri/Zuru.

Livello di rischio: Medio (bersaglio specifico di professionisti, ma aggira protezioni standard).

- **BERT (nuovo gruppo ransomware multipiattaforma)**

BERT è un nuovo gruppo ransomware (detto anche "Water Pombero" da Trend Micro) attivo dal 2025. Ha colpito organizzazioni in Asia, Europa e USA (sanità, tech, eventi) con varianti Windows e Linux. Il campionamento indica modalità semplici ma efficaci: i payload terminano processi specifici (per velocizzare la cifratura parallela fino a 50 thread su Linux), e usano script PowerShell per lanciare il ransomware sui sistemi Windows. Anche la variante Linux può spegnere macchine virtuali ESXi per incrementare l'impatto (processo "maximalista").

IoC:

Tipo IoC	Valore	Descrizione
Hash SHA-256	75fa5b506d095015046248cf6d2ec1c48111931b4584a040ceca57447e9b9d71	BERT Windows (ransomware MSIL)
Hash SHA-256	c7efe9b84b8f48b71248d40143e759e6fc9c6b7177224eb69e0816cc2db393db	BERT Linux (ransomware Linux)
Hash SHA-256	bd2c2cf0631d881ed382817afcce2b093f4e412ffb170a719e2762f250abfea4	PowerShell downloader ("THEBIBE")
IP	185[.]100[.]157[.]74	Server che ospita payload[.]exe
File	payload[.]exe	Nome del file ransomware scaricato via HTTP

MITRE ATT&CK:

- **T1059.001 – PowerShell**: utilizzo di script PowerShell per eseguire comandi dannosi.
- **T1059.004 – JScript**: uso di scripting JScript per automatizzare l'infezione.
- **T1489 – Service Stop**: terminazione di processi e servizi prima della cifratura.
- **T1486 – Data Encrypted for Impact**: cifratura massiva dei dati per estorsione.

Contromisure (rilevazione e mitigazione):

- Applicare **patch critiche** ai sistemi, in particolare su **VPN** e software di **accesso remoto** vulnerabili.
- Utilizzare **antimalware con rilevamento comportamentale**.
- Impiegare **regole di threat hunting** fornite da Trend Micro per identificare i payload di BERT.

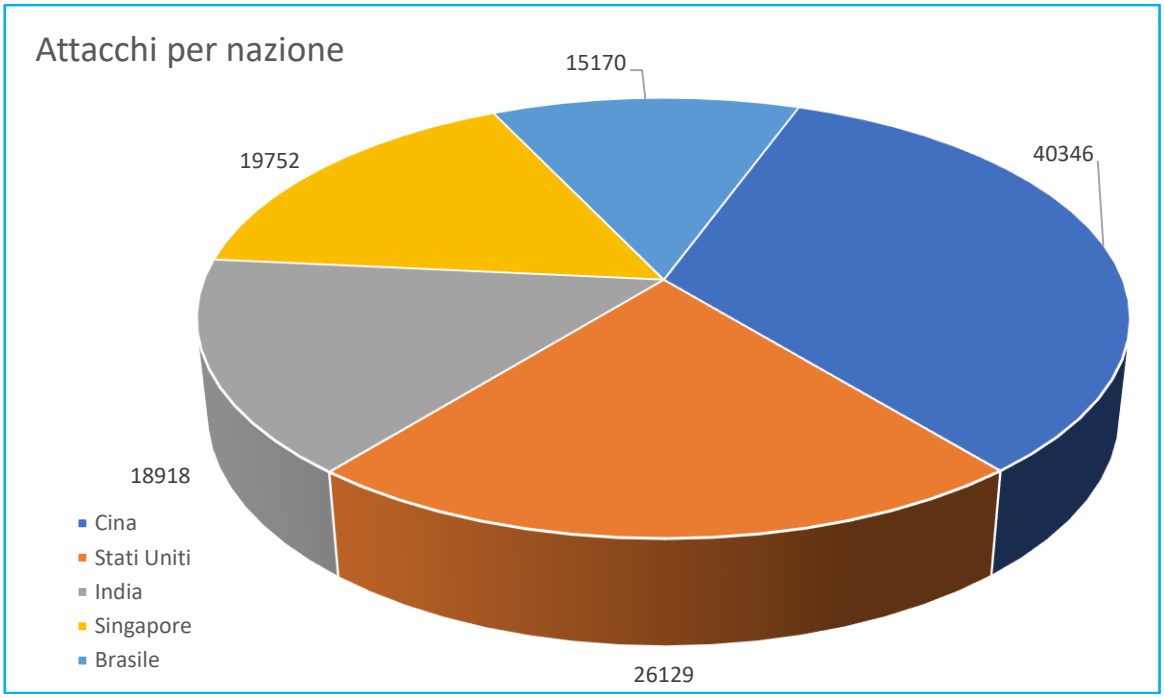
Livello di rischio: Alto (ransomware completo multi-sistema, già vittime confermate)

Tabella riassuntiva

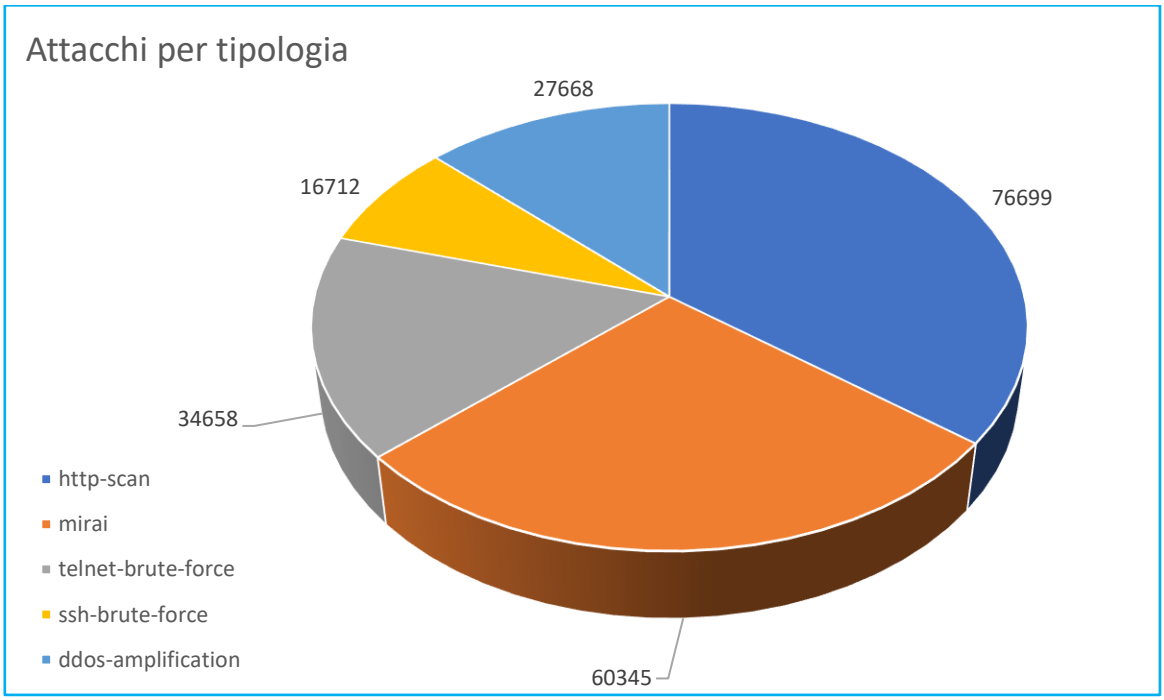
Malware	Descrizione	Data Scoperta	Tecniche MITRE Principali	Livello di Rischio
Bert	Ransomware modulare che usa PowerShell e JScript per propagarsi; cifra i dati e disattiva i servizi. Sfrutta vulnerabilità RDP/VPN	7 luglio 2025	T1059.001, T1059.004, T1486, T1489, T1070	**Critico**
Khepri (Zuru)	Infostealer per macOS, si installa come LaunchAgent, si nasconde in /tmp e comunica con C2 camuffato tramite domini fasulli (es. baidu.com)	10 luglio 2025	T1574.007, T1547.001, T1059, T1071.001	**Medio-Alto**

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:

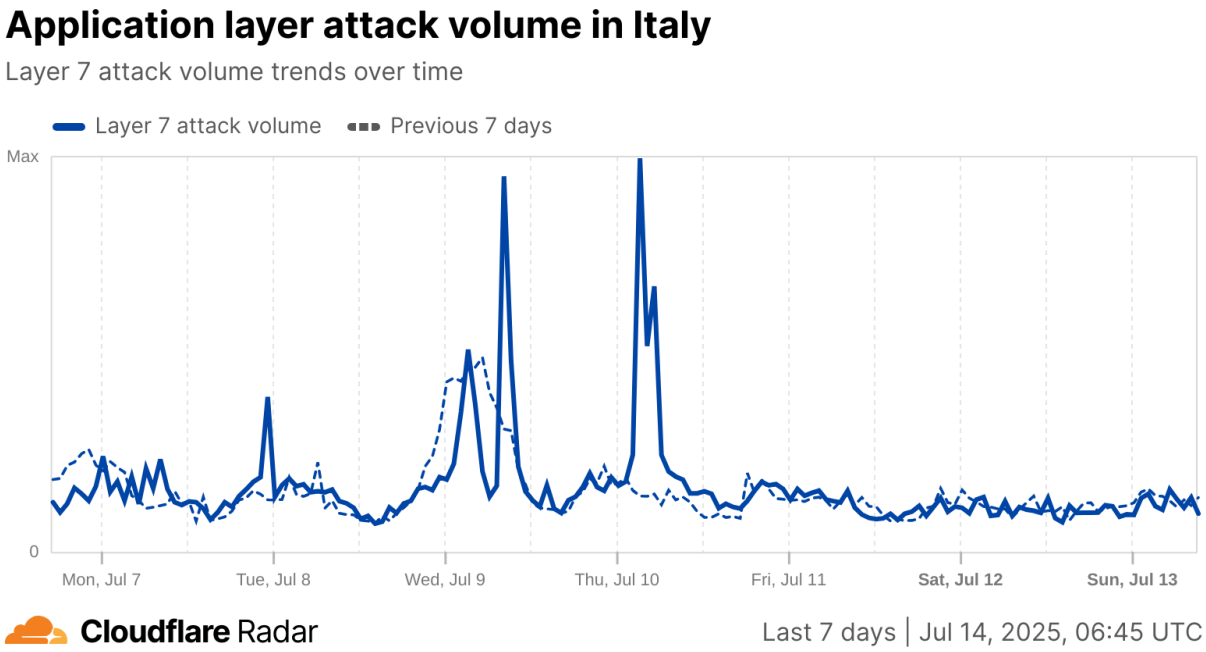


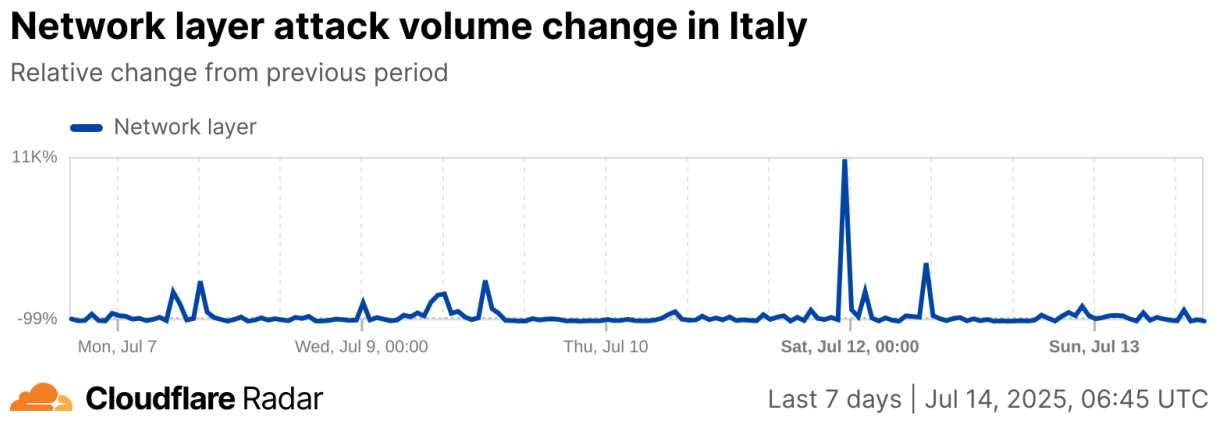
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
MCDONALD'S	MONDO
DESCRIZIONE	Un'importante falla di sicurezza è stata scoperta nella piattaforma di recruiting McHire, sviluppata da Paradox.ai per McDonald's. Alcuni ricercatori hanno trovato l'interfaccia di amministrazione accessibile pubblicamente e protetta da credenziali banali: username e password erano entrambe "123456". Questo errore ha permesso l'accesso a dati personali di oltre 64 milioni di candidati, tra cui email, IP e recapiti. L'esposizione ha colpito principalmente utenti in Australia, ma non si esclude un impatto a livello globale. La vulnerabilità è stata chiusa solo dopo la segnalazione, sollevando forti critiche sulla gestione della sicurezza da parte del fornitore tecnologico. McDonald's ha avviato un'indagine interna e notificato l'accaduto alle autorità australiane per la protezione dei dati.

TARGET	LOCALIZZAZIONE
LOUIS VUITTON	REGNO UNITO
DESCRIZIONE	Il brand di lusso Louis Vuitton ha notificato una violazione dei dati personali dei suoi clienti nel Regno Unito, avvenuta ad inizio luglio. I dati compromessi comprendono nomi, contatti email, indirizzi fisici e cronologia degli acquisti. Anche se l'azienda ha precisato che non sono stati trafugati dati finanziari o password, l'incidente solleva preoccupazioni poiché è il terzo breach subito da LVMH in meno di tre mesi. Le autorità britanniche sono state informate e i clienti coinvolti hanno ricevuto comunicazioni ufficiali. Non sono stati diffusi dettagli sull'origine tecnica dell'attacco, ma analisti sospettano un'esfiltrazione mirata legata a vulnerabilità interne o compromissioni tramite supply chain. Il gruppo LVMH ha dichiarato di aver rafforzato le misure di sicurezza.

TARGET	LOCALIZZAZIONE
TALENTHOOK	STATI UNITI
DESCRIZIONE	TalentHook, società statunitense specializzata in software per il reclutamento, ha accidentalmente lasciato esposto un container di archiviazione Blob in Azure contenente circa 26 milioni di curriculum vitae. I file includevano nomi, email, numeri di telefono, indirizzi, esperienze lavorative e qualifiche scolastiche. L'errore è stato attribuito ad una configurazione errata dei permessi di accesso pubblici, una vulnerabilità sempre più comune tra le aziende che utilizzano servizi cloud. Secondo esperti di sicurezza, non c'erano meccanismi di autenticazione o cifratura attiva sul container, rendendo i dati facilmente accessibili a chiunque ne conoscesse l'URL. La società non ha ancora confermato se i dati siano stati effettivamente scaricati da attori malevoli.

4.6 Defacement

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

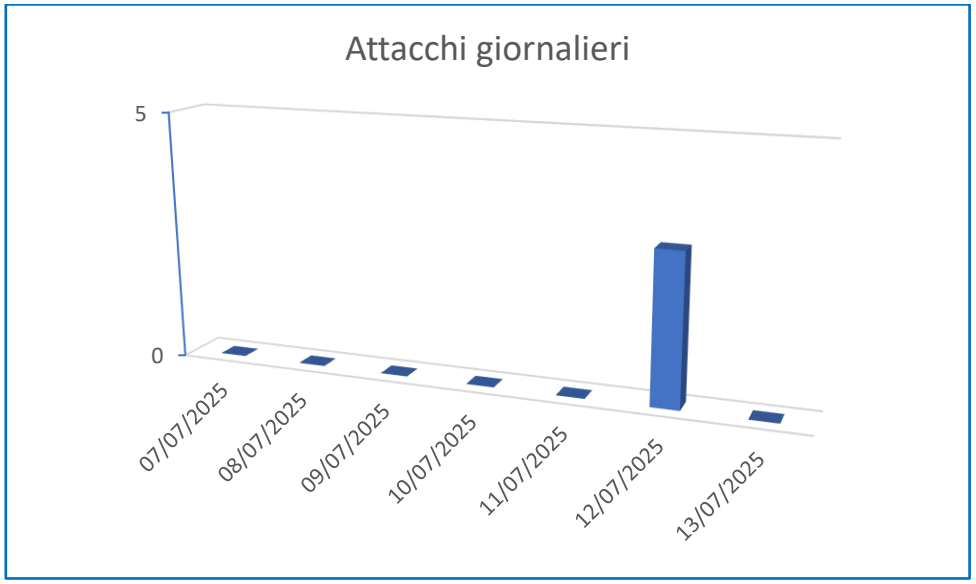


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

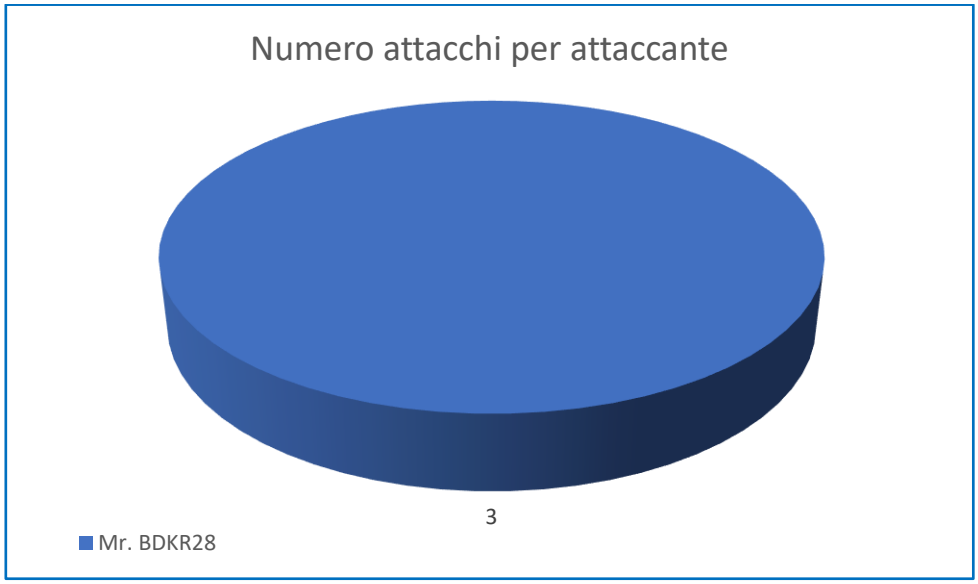


Figura 2: Defacement - Attaccanti più attivi nel periodo 7 - 13 Luglio

5 Honeypot

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

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale

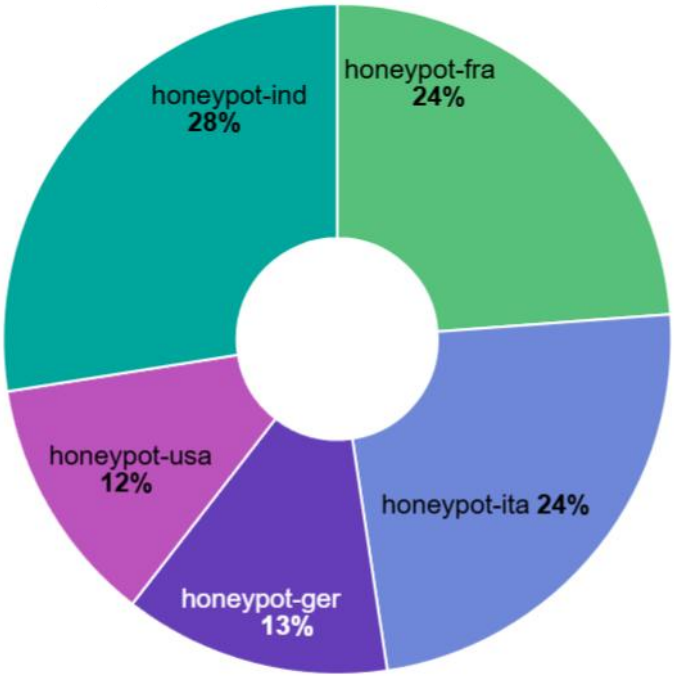
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

670.296 Attacks

7.037 Unique Src IPs

63 Unique HASSHs

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



Questa invece la situazione a livello italiano:

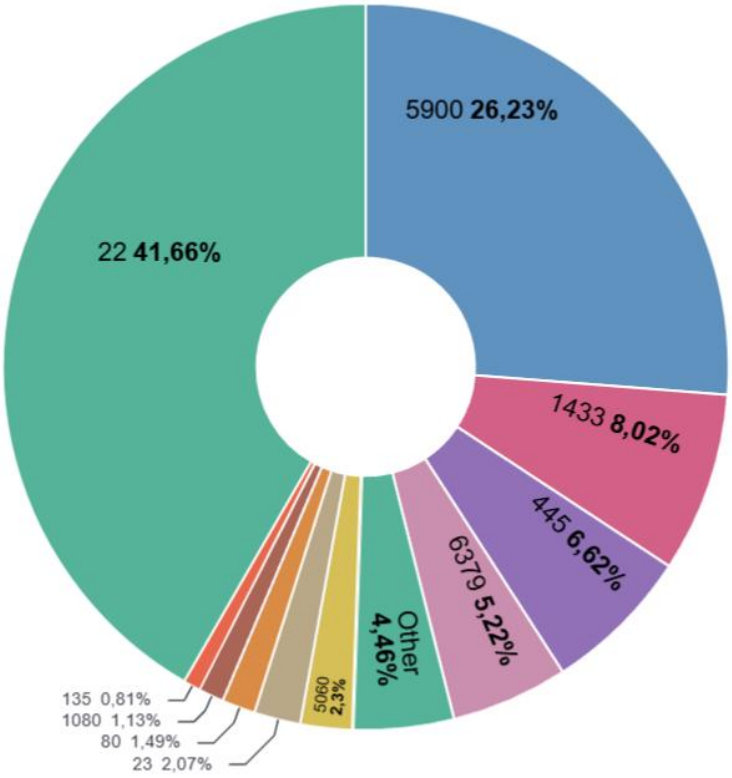
159.394 Attacks

2.529 Unique Src IPs

42 Unique HASSHs

5.1.1 Attacchi ai servizi

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



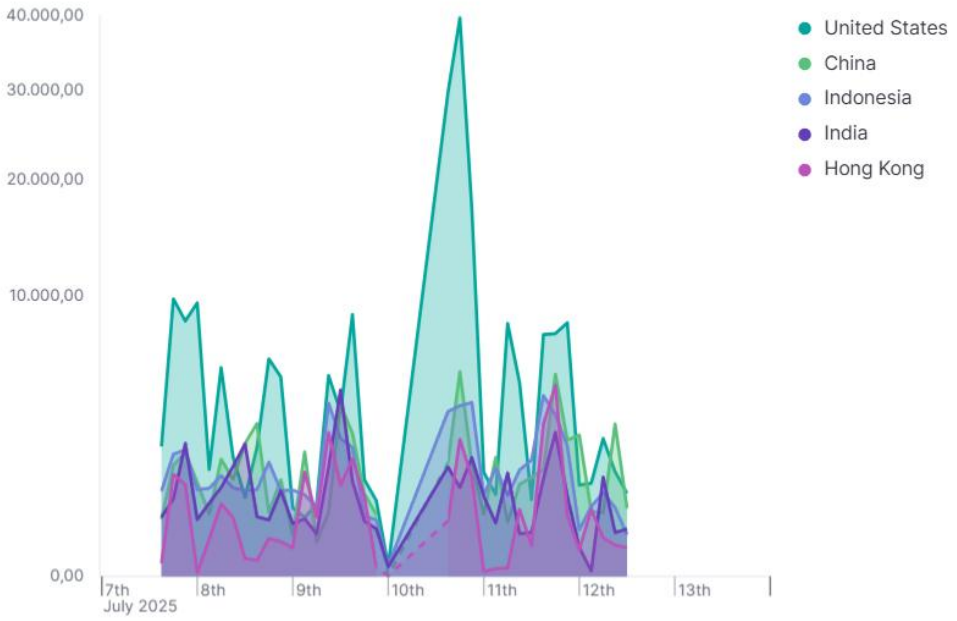
5.1.2 IP Attaccanti

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

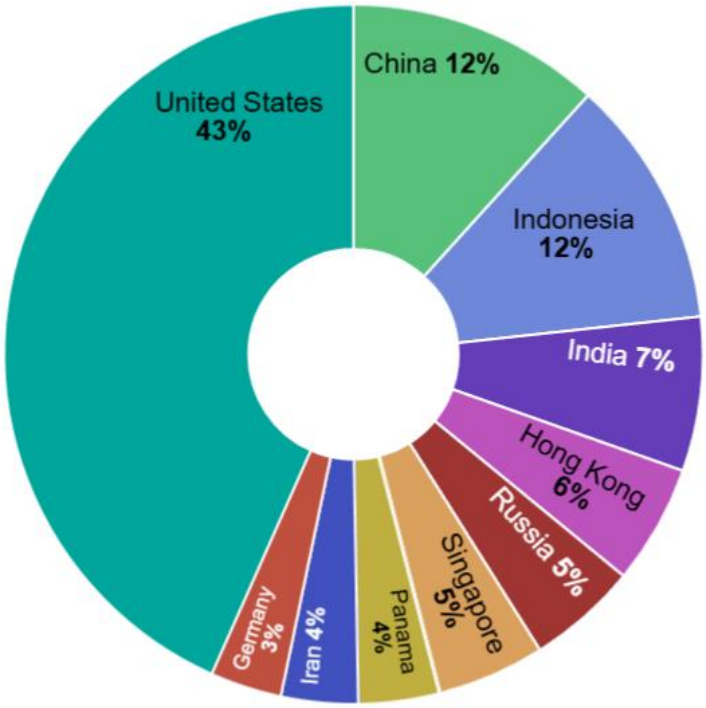
Source IP	Count
198.23.153.40	77.411
103.156.74.23	28.763
142.202.191.234	26.977
142.202.189.5	26.848
45.227.253.103	17.316
47.180.61.210	8.216
173.231.185.164	6.573
194.0.234.124	5.834
103.99.206.83	5.291
141.98.10.162	5.272

5.1.3 Paesi di provenienza degli attacchi

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



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

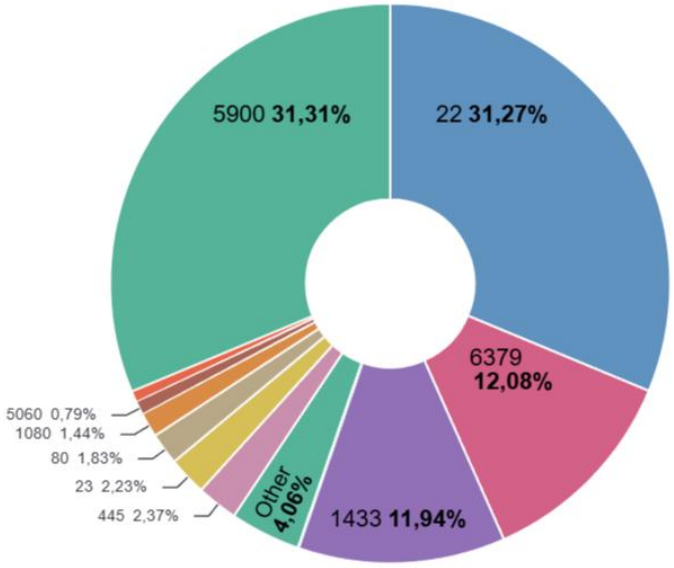


5.2 Italian Honeypot N.1

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

5.2.1 Attacchi ai servizi

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



Service Port	Count
5900	19.611
22	19.585
6379	7.567
1433	7.480
445	1.485
23	1.398
80	1.149
1080	900
5060	497
443	418

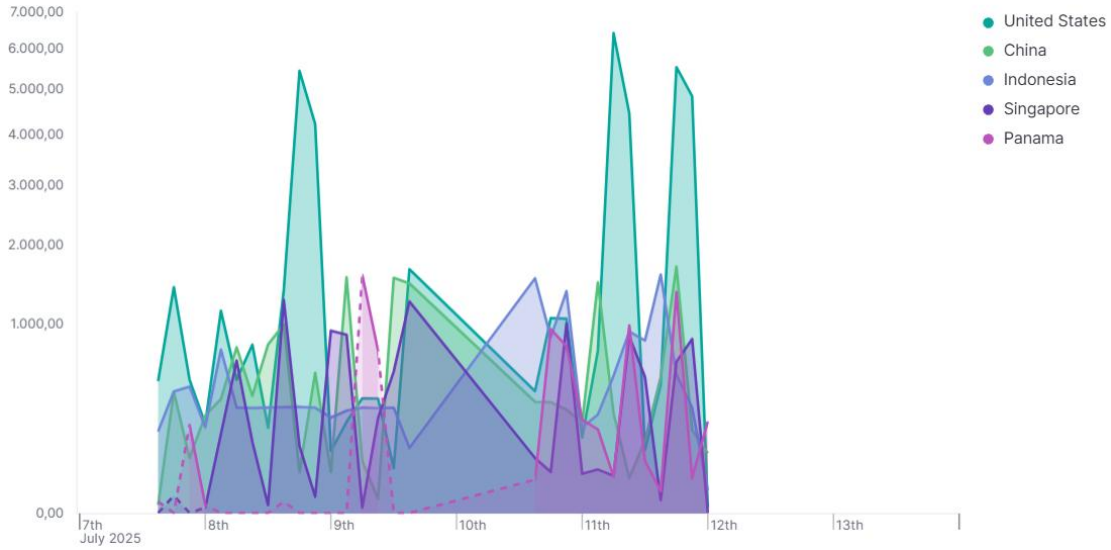
5.2.2 IP Attaccanti

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

Source IP	Count
142.202.191.234	8.924
142.202.189.5	8.914
47.180.61.210	8.216
103.156.74.23	7.921
45.227.253.103	7.138
194.0.234.124	5.834
173.231.185.164	2.070
141.98.10.162	1.712
209.97.182.13	1.259
167.160.188.112	1.257

5.2.3 Paesi di provenienza degli attacchi

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

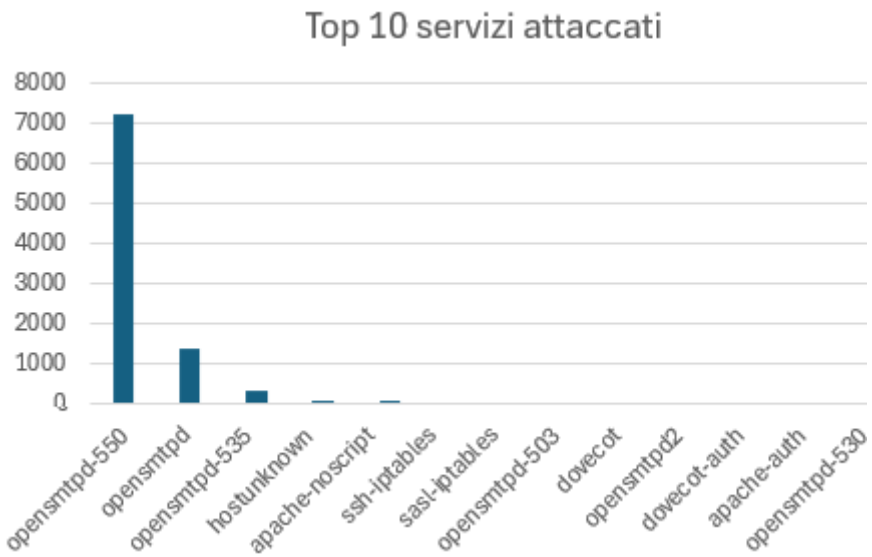


5.3 Italian Honeypot N.2

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

5.3.1 Attacchi ai servizi

Questa la distribuzione degli attacchi per servizio attaccato.



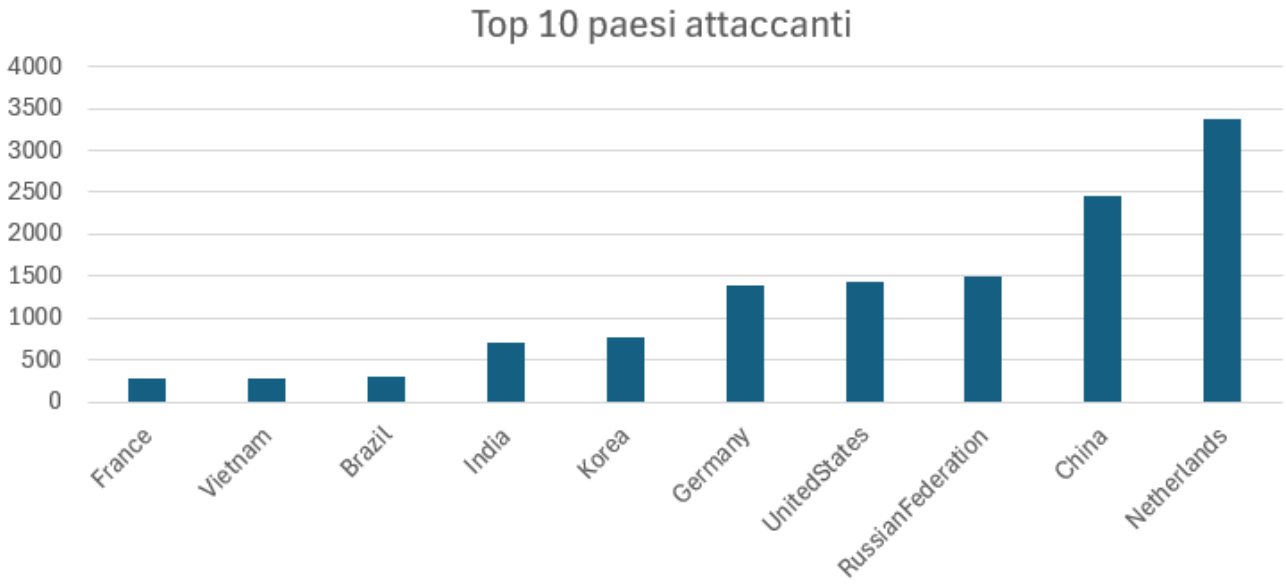
5.3.2 IP attaccanti

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

Source IP	Numero di attacchi
37[.]48[.]90[.]236	1388
195[.]54[.]33[.]154	1171
213[.]108[.]199[.]159	965
37[.]48[.]120[.]235	784
62[.]173[.]145[.]115	584
95[.]181[.]151[.]26	228
89[.]185[.]84[.]17	106
85[.]17[.]15[.]158	60
190[.]80[.]193[.]48	46
62[.]173[.]141[.]189	41

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 = 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