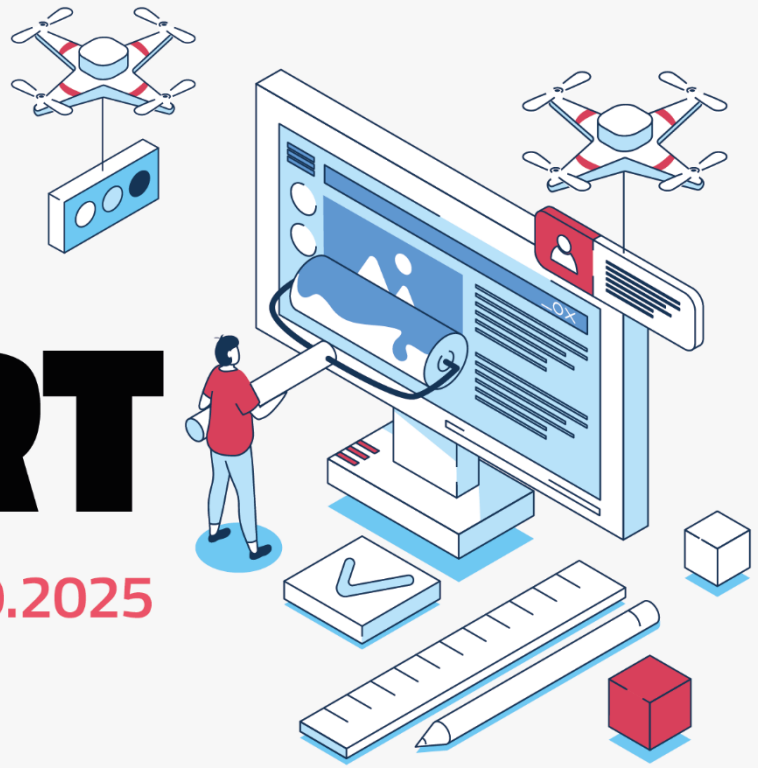
S3K

Cyber security

RISK REPORT

\ week 01.09.2025 - 07.09.2025



Sommario

1 Il Cyber Security Risk Report S3K 4

2 Security news 7

2.1 Rilasci aggiornamenti e patch 7

2.2 "Cyber News" dal Web, Deep Web e Dark Web 9

3 CVE Monitor 13

3.1 Sintesi Settimanale CVE 13

3.2 Tendenze 15

3.3 Nuove CVE 16

3.4 CVE attualmente utilizzate in attacchi 17

4 Attacchi 19

4.1 Phishing 19

4.2 Ransomware 26

4.3 Malware 28

4.4 DDoS rilevati 36

4.5 Data Breach 38

4.6 Defacement 40

5 Honeypot 41

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale 41

5.1.1 Attacchi ai servizi 42

5.1.2 IP Attaccanti 43

5.1.3 Paesi di provenienza degli attacchi 43

5.2 Italian Honeypot N.1 44

5.2.1 Attacchi ai servizi 44

5.2.2 IP Attaccanti 45

5.2.3 Paesi di provenienza degli attacchi 45

5.3 Italian Honeypot N.2 46

5.3.1 Attacchi ai servizi 46

5.3.2 IP attaccanti 47

5.3.3 Paesi di provenienza degli attacchi 48

6 Company Profile S3K 49

CYBER SECURITY RISK REPORT
36/25

1 Il Cyber Security Risk Report S3K

Report Settimanale CTI - Analisi delle Minacce Cyber 1-7 Settembre 2025

Questo bollettino di sicurezza informatica presenta un'analisi completa delle minacce cyber rilevate nella settimana dal 1 al 7 settembre 2025. Il documento fornisce intelligence operativa per operatori di sicurezza informatica, team IT e membri di CSIRT, offrendo una panoramica dettagliata delle vulnerabilità critiche, degli attacchi in corso e delle tendenze emergenti nel panorama delle minacce.

Il report copre diversi domini di sicurezza: vulnerabilità CVE ad alto impatto, campagne di phishing sofisticate, nuove varianti ransomware, attività di malware avanzati e violazioni di dati significative. Particolare attenzione viene dedicata all'analisi di 38 milioni di numeri telefonici italiani esposti nel dark web e alle nuove tecniche di attacco mobile che stanno compromettendo sia dispositivi Android che iOS.

Monitoraggio CVE e Vulnerabilità Attive

L'analisi CVE della settimana rivela un quadro critico con numerose vulnerabilità CRITICAL e HIGH che colpiscono principalmente router domestici, ambienti enterprise e plugin WordPress. Sono stati resi pubblici diversi exploit Proof-of-Concept per SQL injection e buffer overflow, aumentando significativamente il rischio di sfruttamento in ambiente reale.

CVE Critiche della Settimana

- CVE-2025-9401: Buffer overflow critico in Tenda AC18 Router
- CVE-2025-9530: Command injection in D-Link DIR-842
- CVE-2025-9620: RCE via deserialization in Oracle Fusion
- CVE-2025-9655: Stack overflow in Tenda F1202

Le tendenze mostrano un focus particolare sui dispositivi IoT, con router Tenda e D-Link che rappresentano target prioritari per gli attaccanti. Questi dispositivi, spesso mal configurati o non aggiornati, offrono punti di accesso privilegiati alle reti domestiche e aziendali. L'attività di intelligence di S3K si concentra su:

Particolarmente preoccupante è l'emergere di CVE-2025-53690 in Sitecore, attivamente sfruttata in attacchi reali per la deserializzazione di dati non affidabili, e CVE-2025-55177 in WhatsApp, che in combinazione con vulnerabilità del sistema operativo Apple potrebbe essere utilizzata in attacchi sofisticati mirati.

Minacce Attive: Phishing, Ransomware e Malware

L'analisi degli attacchi attivi rivela un panorama delle minacce in costante evoluzione, caratterizzato da campagne di phishing sempre più sofisticate e dall'emergere di nuove varianti ransomware. Il caso studio dell'email "You have [9] pending incoming emails" dimostra come i cybercriminali stiano perfezionando le tecniche di ingegneria sociale per aggirare le difese tradizionali.

Nuove Varianti Ransomware

SafePay rappresenta l'ultima evoluzione nel panorama ransomware, utilizzando tecniche di cifratura XChaCha20 estremamente rapide. Obscura si distingue per la sua capacità di infiltrarsi nei domain controller, mentre NEZHA combina keylogging con estorsione dati.

TinyLoader continua a evolversi come vettore per la distribuzione di payload multipli, inclusi RedLine Stealer e DCRat. La sua capacità di fungere da clipper per criptovalute lo rende particolarmente pericoloso per utenti e organizzazioni che gestiscono asset digitali.

Il gruppo APT GhostRedirector ha dimostrato sofisticate capacità di compromissione server attraverso l'uso di backdoor C++ personalizzati e moduli IIS nativi. Questi attacchi, principalmente finalizzati al SEO poisoning, indicano un'evoluzione delle tattiche APT verso obiettivi economici indiretti ma altamente redditizi.

Analisi delle Vulnerabilità e Attacchi Attivi - CVE Critiche della Settimana

Sono state identificate 8 vulnerabilità critiche e ad alto impatto, con exploit pubblici già disponibili per il 62% di esse. I router domestici rappresentano il target primario, seguiti da soluzioni enterprise come VMware ESXi e Microsoft SharePoint.

Le CVE attualmente sfruttate includono vulnerabilità in Sitecore (CVE-2025-53690), Chrome Android (CVE-2025-48543) e WhatsApp iOS (CVE-2025-55177), quest'ultima potenzialmente utilizzata in attacchi sofisticati mirati.

Intelligence Honeypot e Raccomandazioni Operative

L'infrastruttura honeypot S3K ha registrato attività significativa durante la settimana di osservazione, fornendo intelligence preziosa sui pattern di attacco e le tattiche degli avversari. I sensori distribuiti in Italia, Germania, Francia, Brasile, India e USA hanno intercettato tentativi di compromissione mirati a servizi SSH, SMTP e web server Apache.

Distribuzione Geografica Attacchi

Gli honeypot italiani hanno evidenziato una concentrazione di attacchi provenienti da IP di hosting commerciale, suggerendo l'uso di VPS compromessi o noleggiati per attività malevole. Particolare attenzione è stata riservata agli attacchi su servizi di posta elettronica, con numerosi tentativi di brute force su autenticazione SMTP.

Le raccomandazioni operative si concentrano sull'implementazione di controlli di sicurezza multicategoria: hardening dei sistemi esposti, deployment di soluzioni EDR avanzate, e sviluppo di programmi di awareness mirati alle nuove tecniche di ingegneria sociale. La correlazione tra intelligence honeypot e analisi delle minacce attive fornisce un quadro operativo completo per la protezione proattiva delle infrastrutture critiche.

Il presente bollettino sottolinea l'importanza di un approccio integrato alla sicurezza informatica, dove intelligence delle minacce, monitoraggio continuo e risposta rapida agli incidenti si combinano per creare una postura di sicurezza resiliente e adattiva alle sfide del panorama cyber contemporaneo.

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Android	Google ha rilasciato gli aggiornamenti di sicurezza di settembre per sanare diverse vulnerabilità che interessano il sistema operativo Android. Prodotti e/o versioni affette • Android 13, 14, 15, 16 con patch di sicurezza precedenti a settembre 2025.
ULR/Note	https://source.android.com/docs/security/bulletin/2025-09-01

PRODOTTO	DESCRIZIONE
udisks2	Risolta una vulnerabilità con gravità "alta" in UDisks, noto demone utilizzato nelle principali distribuzioni Linux per la gestione dei dispositivi di archiviazione. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a un utente malintenzionato di compromettere la disponibilità del servizio oppure di ottenere privilegi elevati sul sistema interessato. Prodotti e versioni affette • 2.10.x, versioni precedenti alla 2.10.91 • 2.10.x, versioni precedenti alla 2.10.2
ULR/Note	• https://www.openwall.com/lists/oss-security/2025/08/28/1: apre un link esterno • https://access.redhat.com/security/cve/cve-2025-8067: apre un link esterno • https://security-tracker.debian.org/tracker/CVE-2025-8067: apre un link esterno • https://ubuntu.com/security/CVE-2025-8067: apre un link esterno • https://github.com/storaged-project/udisks/security/advisories/GHSA-742q-gggc-473g

PRODOTTO	DESCRIZIONE
Log4cxx	Rilevate vulnerabilità di sicurezza, di cui una con gravità “alta”, in Log4cxx, framework progettato per fornire funzionalità di logging per applicazioni scritte in C++. Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato di alterare i dati sul sistema interessato. Prodotti e/o versioni affette • Log4cxx, versioni precedenti alla 1.5.0
ULR/Note	• https://logging.apache.org/security.html#CVE-2025-54813: apre un link esterno • https://logging.apache.org/security.html#CVE-2025-54812: apre un link esterno • https://seclists.org/oss-sec/2025/q3/135: apre un link esterno • https://seclists.org/oss-sec/2025/q3/134

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

38 MILIONI DI NUMERI DI TELEFONO ITALIANI NEL DARK WEB

Una nuova e massiccia fuga di dati sta scuotendo l'Italia: secondo le segnalazioni di analisti di sicurezza, sarebbero stati messi in vendita nel dark web circa 38 milioni di numeri di telefono appartenenti a cittadini italiani. Si tratta di un volume enorme, che rappresenta una parte significativa della popolazione e che, nelle mani dei cybercriminali, può diventare il carburante ideale per campagne di truffe digitali su larga scala.

Il rischio più concreto è quello legato allo smishing, ovvero l'invio di SMS fraudolenti con lo scopo di indurre le vittime a cliccare su link dannosi o a condividere dati riservati. Finora, questi messaggi si basavano spesso su numerazioni casuali o non aggiornate, risultando più facili da individuare come sospetti. Con una lista reale e recente di milioni di contatti, invece, i truffatori possono confezionare attacchi molto più credibili e mirati, facendo apparire il messaggio come un avviso autentico da parte della banca, di un corriere o di un servizio pubblico.

La vendita di questi archivi mette in evidenza un problema strutturale: i dati personali sono ormai una merce preziosa e ambita nei circuiti criminali. Non si tratta solo di una questione di privacy violata, ma di un rischio concreto per la sicurezza economica e digitale delle persone. In scenari simili, la prevenzione passa soprattutto dalla consapevolezza: diffidare di link ricevuti via SMS, controllare con attenzione il mittente e utilizzare canali ufficiali per qualsiasi comunicazione resta l'unica difesa realmente efficace contro questo tipo di frode.

SMARTPHONE SEMPRE PIÙ SOTTO ATTACCO

Gli smartphone sono diventati lo strumento attraverso cui gestiamo gran parte della vita personale e professionale: chat, social, foto, dati bancari, credenziali di lavoro. Non sorprende, quindi, che siano entrati nel mirino dei cybercriminali. Secondo le ultime analisi, sia utenti Android che iOS sono bersagli di nuove campagne malevole che sfruttano app compromesse, pubblicità ingannevoli e siti web trappola per distribuire malware.

Questi software dannosi non si limitano a rallentare il dispositivo, ma possono arrivare a rubare password, intercettare messaggi, clonare carte di credito o accedere ai conti correnti online. In alcuni casi, il malware ottiene privilegi elevati, consentendo agli attaccanti di controllare lo smartphone da remoto e trasformarlo in una vera e propria porta d'ingresso ai dati più sensibili.

Il fenomeno è particolarmente allarmante perché i dispositivi mobili sono stati a lungo percepiti come relativamente sicuri, grazie ai controlli sugli store ufficiali di Apple e Google. Eppure, i criminali hanno dimostrato di saper aggirare queste barriere, introducendo applicazioni apparentemente legittime che nascondono funzionalità malevole. In questo scenario, la responsabilità ricade anche sull'utente, che deve prestare attenzione alle autorizzazioni richieste dalle app e diffidare da link sospetti ricevuti via SMS o social.

La crescita del cybercrime mobile segna un punto di svolta: non esiste più distinzione netta tra sicurezza informatica "tradizionale" e "mobile". Il telefono, ormai, è un vero computer in miniatura e deve essere protetto con la stessa cura di un server aziendale.

SAFEPAY: LA NUOVA VARIANTE RANSOMWARE

Il fenomeno ransomware continua a dominare la scena delle minacce informatiche, e l'ultima novità si chiama SafePay. Questa nuova variante utilizza tecniche di cifratura estremamente rapide ed efficaci, rendendo i file delle vittime completamente inaccessibili in pochi istanti. Dopo l'attacco, compare il consueto messaggio che chiede il pagamento di un riscatto – solitamente in criptovaluta – come unica possibilità per recuperare i dati.

Ciò che rende SafePay particolarmente pericoloso è la sua capacità di adattarsi a diversi scenari: può colpire tanto utenti privati quanto aziende, senza distinzione di settore o dimensione. Per un singolo cittadino, la perdita di foto, documenti o credenziali può rappresentare un danno incalcolabile; per un'organizzazione, invece, può significare giorni di inattività, perdita di clienti e costi di ripristino elevatissimi.

Il ransomware non è più un fenomeno sporadico, ma un vero modello di business criminale, con gruppi che investono nello sviluppo di nuove versioni e persino offrono servizi "chiavi in mano" ad altri criminali. SafePay è la dimostrazione di quanto il fenomeno sia ancora in piena espansione e di come ogni nuova variante riesca a superare, almeno temporaneamente, le difese esistenti.

La lezione resta sempre la stessa: non esistono difese infallibili, ma solo strategie di mitigazione. Backup regolari, piani di risposta agli incidenti e una costante formazione del personale restano le armi più efficaci per non trovarsi in ginocchio di fronte a un attacco ransomware.

UN EXPLOIT CHE AGGIRA I CONTROLLI DI INTEGRITÀ DEL CODICE

Un'altra scoperta recente getta nuove ombre sulla sicurezza dei sistemi operativi: i ricercatori hanno individuato un exploit capace di eludere i controlli di integrità del codice, uno dei meccanismi più importanti progettati per impedire l'esecuzione di software non autorizzato. In sostanza, il sistema che dovrebbe bloccare programmi manipolati o potenzialmente pericolosi può essere aggirato, consentendo a codice malevolo di sembrare legittimo e di avviarsi senza ostacoli.

Questo tipo di vulnerabilità è particolarmente critico perché va a colpire il cuore delle difese di un sistema. Se un attaccante riesce a sfruttarlo, può installare malware che si nasconde sotto le sembianze di software sicuro, guadagnando privilegi elevati e mantenendo un livello di persistenza molto alto. In uno scenario reale, questo significa che un trojan, una backdoor o uno spyware potrebbero infiltrarsi e restare attivi a lungo senza essere rilevati dalle soluzioni di sicurezza.

Gli esperti sottolineano che l'impatto non riguarda solo gli utenti domestici, ma soprattutto aziende e infrastrutture critiche, che fanno affidamento proprio su queste barriere per mantenere un ambiente sicuro. Il fatto che un exploit sia in grado di indebolire un pilastro così centrale mette in evidenza quanto sia sottile il margine di protezione e quanto rapida debba essere la reazione dei produttori di software per correggere la falla.

La vicenda si inserisce in un quadro più ampio: la corsa tra chi sviluppa sistemi di difesa e chi cerca di abbatterli non conosce tregua. Ogni nuovo exploit è un passo avanti per i criminali, e ogni patch è un tentativo di riportare equilibrio. Ma finché il ciclo continuerà, resterà sempre un margine di rischio che non potrà mai essere azzerato del tutto.

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 1 – 7 Settembre 2025
Settimana con numerose CVE CRITICAL & HIGH che colpiscono principalmente router domestici (Tenda, D-Link), ambienti enterprise (VMware, Microsoft, Oracle) e plugin WordPress.
Sono stati resi pubblici diversi exploit PoC per SQLi e buffer overflow.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit Pubblico	Prodotto Coinvolto	Descrizione Sintetica
CVE-2025-9401	CRITICAL	01/09/2025	✅	Tenda AC18 Router	Buffer overflow in formexeCommand (RCE remoto)
CVE-2025-9412	CRITICAL	01/09/2025	❌	VMware ESXi	Privilege escalation locale
CVE-2025-9444	HIGH	02/09/2025	✅	WordPress Plugin WPForms	SQLi in gestione form
CVE-2025-9488	HIGH	03/09/2025	❌	Microsoft SharePoint	SSRF in gestione workflow
CVE-2025-9530	CRITICAL	04/09/2025	✅	D-Link DIR-842	Command injection in ping.ccp

CVE-2025-9591	HIGH	06/09/2025	✅	PHPGurukul Library Mgmt	SQLi in search_books.php
CVE-2025-9620	CRITICAL	07/09/2025	❌	Oracle Fusion Middleware	RCE via deserialization
CVE-2025-9655	CRITICAL	08/09/2025	✅	Tenda F1202 Router	Stack overflow in formWifiWpsStart

Distribuzione Giornaliera

- **1 settembre** → Router Tenda (overflow) e VMware ESXi escalation
- **2 settembre** → SQLi su plugin WPForms
- **3 settembre** → Microsoft SharePoint SSRF
- **4 settembre** → Command injection critico su router D-Link
- **6 settembre** → SQLi su PHPGurukul Library Management
- **7 settembre** → RCE su Oracle Fusion Middleware
- **8 settembre** → Nuovo stack overflow su router Tenda

Vendor e Tecnologie Coinvolti

- **Router IoT (Tenda, D-Link)** → exploit critici con PoC per RCE e command injection
- **VMware ESXi** → escalation privilegi locale
- **Microsoft SharePoint** → SSRF critico in workflow
- **Oracle Fusion Middleware** → deserialization RCE
- **WordPress Plugin (WPForms)** → SQLi su form builder
- **PHPGurukul** → SQLi in Library Mgmt System

Raccomandazioni Operative / Patch Prioritarie

- **Router Tenda/D-Link** → aggiornamento firmware immediato, disabilitare accesso WAN e servizi diagnostici esposti.
- **VMware ESXi** → applicare patch senza ritardi, rafforzare controlli sugli account locali ed eseguire audit delle VM in esecuzione.

- **Microsoft SharePoint** → aggiornare il workflow engine, limitare richieste SSRF e monitorare traffico anomalo verso servizi interni.
- **Oracle Fusion Middleware** → mitigare le deserialization RCE, disabilitare moduli legacy non utilizzati e abilitare logging esteso.
- **WordPress WPForms / PHPGurukul** → aggiornamento immediato; in assenza di patch, considerare la disattivazione dei plugin/applicativi vulnerabili.

Monitoraggio Consigliato

- **Endpoint vulnerabili da monitorare:**
  - Router → formexeCommand, ping.ccp, formWifiWpsStart
  - WebApp → search_books.php, form builder di WPForms
- **SIEM:** creare regole di detection per pattern SQLi e tentativi di overflow.
- **DS/IPS:** aggiornare signature per exploit PoC pubblicati (soprattutto Tenda/D-Link).
- **Cloud/Enterprise:** rafforzare controlli di accesso in VMware ESXi e Microsoft SharePoint.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-42957	SAP S/4HANA	N/A
CVE-2024-30088	Windows Kernel	N/A
CVE-2025-7388	OpenEdge AdminServer	N/A
CVE-2020-24363	TP-Link TL-WA855RE	8.8
CVE-2025-57052	cJSON (libreria C open-source)	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-2025-58628	Miraculous	N/A
VULNERABILITÀ	Una vulnerabilità di tipo SQL Injection cieca (Blind SQL Injection) è presente nell'applicazione Miraculous sviluppata da kamleshyadav, a causa di una neutralizzazione impropria degli elementi speciali usati in una query SQL.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-55241	Microsoft Azure Entra	N/A
VULNERABILITÀ	Un difetto di autenticazione impropria (CWE-287) in Azure Entra ID consente a un attaccante remoto non autenticato di inviare richieste malevole e ottenere privilegi elevati all'interno dell'ambiente Azure, potenzialmente fino al livello amministrativo	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-55037	TkEasyGUI (libreria Python)	N/A
VULNERABILITÀ	In TkEasyGUI, nelle versioni precedenti alla v1.0.22, esiste un problema di neutralizzazione impropria degli elementi speciali usati in un comando di sistema operativo (nota come OS Command Injection – CWE-78). Se questa vulnerabilità viene sfruttata, un attaccante remoto non autenticato può eseguire comandi arbitrari sul sistema operativo, a condizione che le impostazioni del software siano configurate per costruire messaggi da fonti esterne.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-9276	Cockroach Labs	N/A
VULNERABILITÀ	Vulnerabilità di bypass dell'autenticazione in cockroach-k8s-request-cert di Cockroach Labs, dovuta alla presenza di una password vuota per l'utente root nel file di configurazione del sistema (/etc/shadow). Questa configurazione errata può permettere a un attaccante remoto di bypassare completamente l'autenticazione su sistemi che utilizzano l'immagine container vulnerabile. Il difetto risiede nella gestione del file shadow, dove l'utente root risulta configurato senza password.	

3.4 CVE attualmente utilizzate in attacchi

In questo paragrafo evidenziamo le principali CVE attivamente utilizzate e sfruttate dagli attaccanti con una breve descrizione.

CVE	CVE-2025-53690
DESCRIZIONE	
I prodotti Sitecore Experience Manager (XM), Experience Platform (XP), Experience Commerce (XC) e Managed Cloud contengono una vulnerabilità legata alla deserializzazione di dati non affidabili, che coinvolge l'uso di machine keys predefinite in ASP.NET. Questa vulnerabilità consente a un attaccante di sfruttare chiavi ASP.NET (machine keys) esposte o predefinite per effettuare la deserializzazione malevola di oggetti, ottenendo così la possibilità di eseguire codice da remoto (Remote Code Execution) sul server vulnerabile.	

CVE	CVE-2025-48543
DESCRIZIONE	
In diversi punti del codice, esiste una possibile modalità per sfuggire alla sandbox di Chrome ed attaccare il processo android system_server a causa di un problema di use-after-free (uso di memoria già liberata). Questa vulnerabilità può portare a una escalation locale dei privilegi senza richiedere ulteriori privilegi di esecuzione. Non è necessaria alcuna interazione da parte dell'utente per sfruttare la vulnerabilità.	

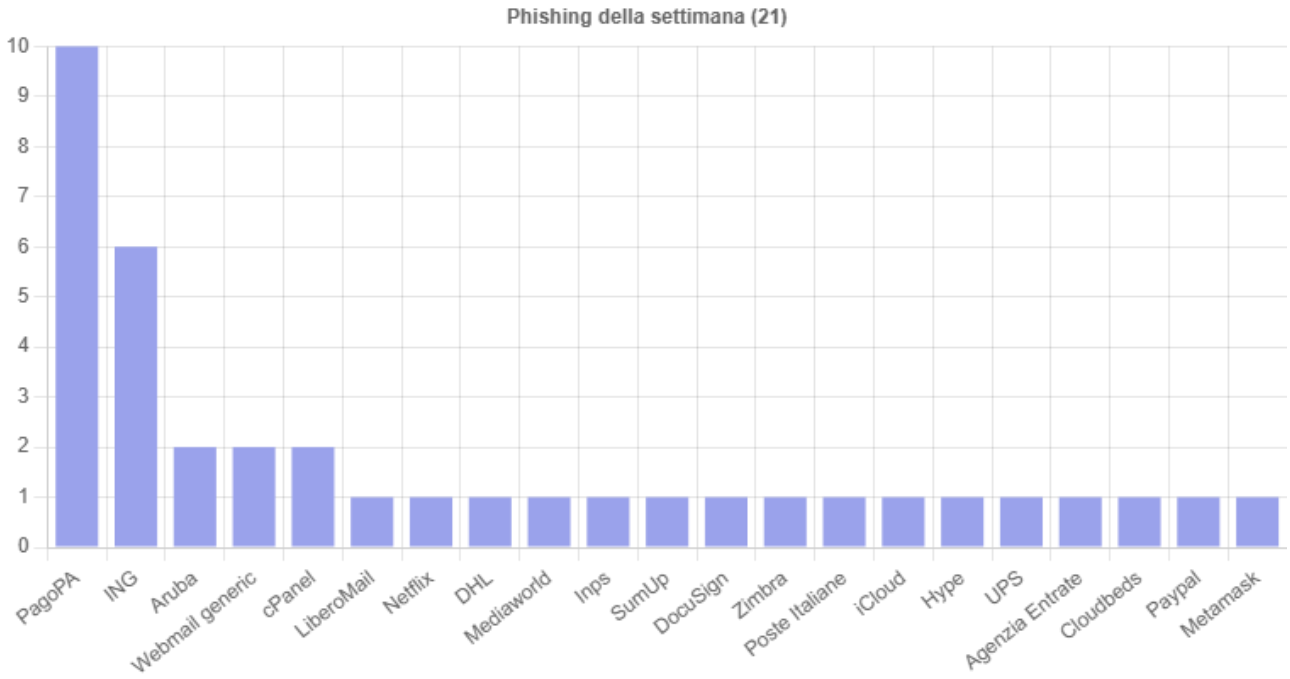
CVE	CVE-2025-55177
DESCRIZIONE	
Autorizzazione incompleta dei messaggi di sincronizzazione dei dispositivi collegati in WhatsApp per iOS (versioni precedenti alla v2.25.21.73), WhatsApp Business per iOS v2.25.21.78 e WhatsApp per Mac v2.25.21.78. Questa vulnerabilità avrebbe potuto permettere a un utente non autorizzato di far elaborare contenuti provenienti da un URL arbitrario sul dispositivo della vittima. Valutiamo che questa vulnerabilità, in combinazione con una vulnerabilità a livello di sistema operativo su piattaforme Apple (CVE-2025-43300), potrebbe essere stata sfruttata in un attacco sofisticato mirato a specifici utenti.	

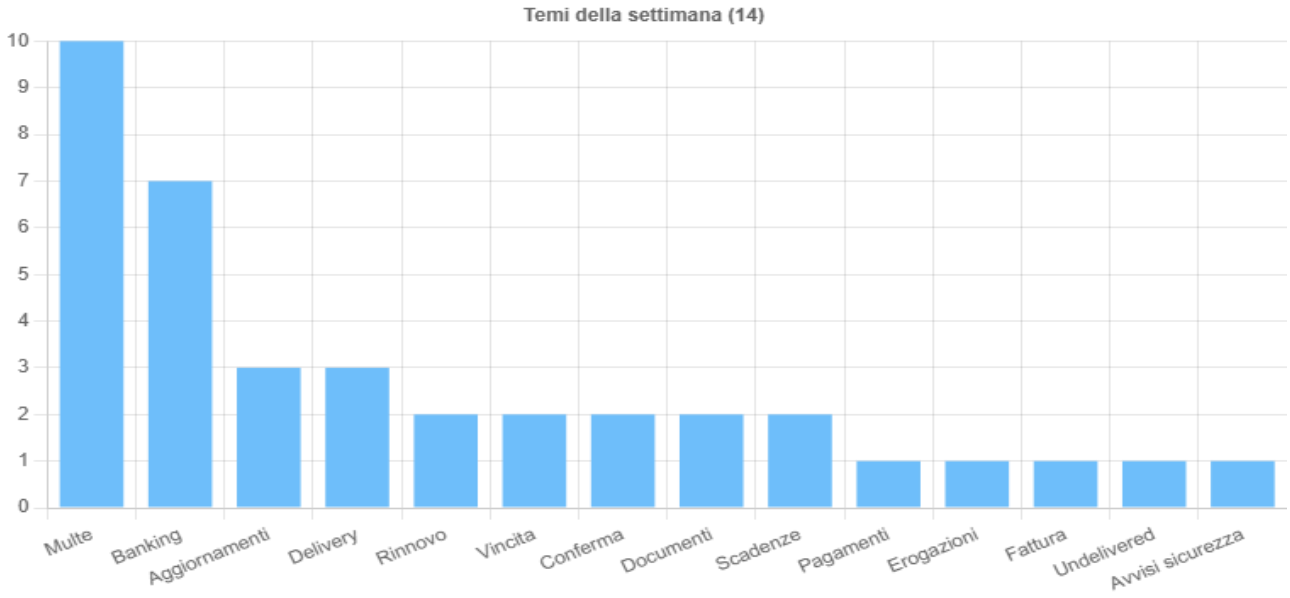
4 Attacchi

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.

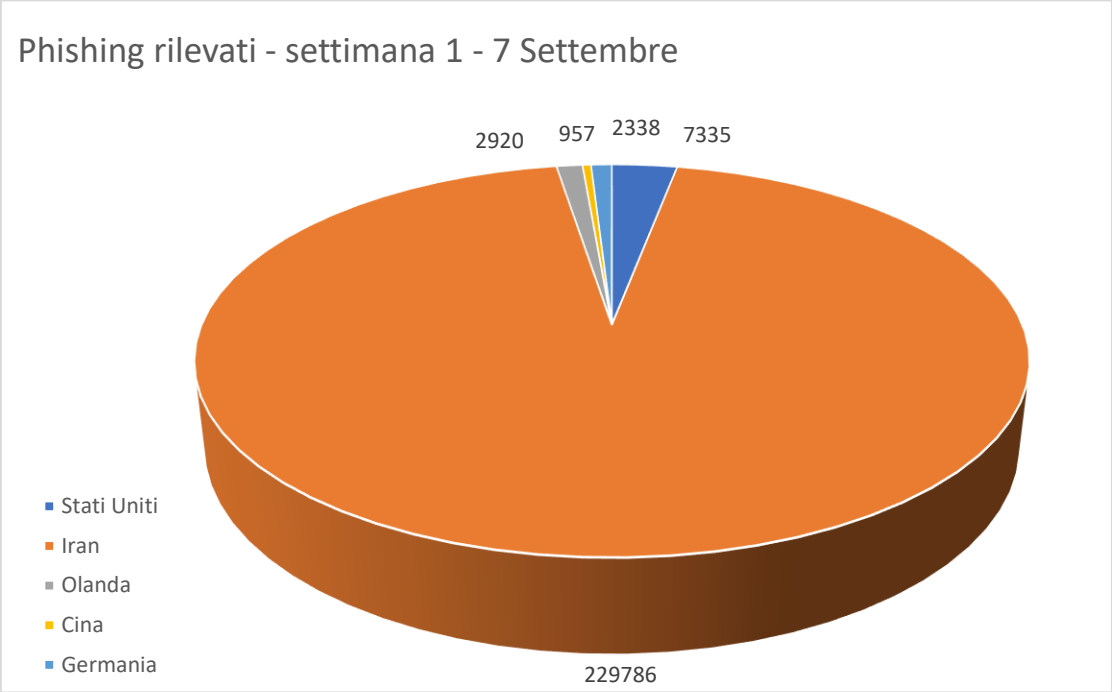




Fonte :CERT-AGID

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 CTI — Analisi email di phishing (caso "You have [9] pending incoming emails")

Di seguito presentiamo l'analisi investigativa completa di una email sospetta. É stato sostituito il dominio di destinazione con victim[.]com e il nome del destinatario con victim, per motivi di riservatezza. In questo caso mittente e destinatario coincidono nello stesso dominio (caso tipico di spoofing interno/BEC-like): per questo motivo tutte le occorrenze del dominio reale sono state sostituite con victim[.]com ai fini del report.

Phishing email (redatta) – 'You have [9] pending inco

From: Mail Delivery System <support@victim[.]com>
To: victim@victim[.]com
Subject: You have [9] pending incoming emails victim@victim[.]com
Date: 25 Aug 2025 20:54:03 +0200

Notification of pending messages.

Some messages are restrained from delivering to victim@victim[.]com
Due to low bandwidth we notify you to take prompt actions
Message should be moved to inbox. Goto Clutter.

Release Messages Review Here

Embedded link:

https://mailprivacy[.]world/login?email=victim@victim[.]com

Questo è un riassunto grafico con dati del destinatario oscurati.

- **Contesto e sintesi**

L'email asserisce un problema di consegna ("You have [9] pending incoming emails"), invita a "rilasciare i messaggi" e **contiene un link esterno** a https://mailprivacy[.]world/login?email=victim@victim[.]com. Lo schema ricalca campagne note di phishing "pending emails / bandwidth / delivery status" che imitano sistemi di posta per sottrarre credenziali dell'utente (webmail/Office-like). Esemplari simili sono stati documentati in passato da analisti anti-phishing e portali di awareness (es. Brendinghat e guide di rimozione) con linguaggio e struttura pressoché identici. (brendinghat.com, pcrisk.com)

- **Evidenze tecniche dalla .eml**

L'oggetto riporta "You have [9] pending incoming emails victim@victim[.]com". Il mittente visualizzato è "Mail Delivery System" con indirizzo support@victim[.]com (indicazione fuorviante: è comune l'abuso del nome "Mail Delivery System" per indurre fiducia). Nel corpo si legge: "Some messages are restrained from delivering … Due to low bandwidth … Release Messages / Review Here", con pulsanti che puntano all'URL esterno https://mailprivacy[.]world/login?email=victim@victim[.]com.
Dalle righe di trasporto presenti (estratto header Received) risulta un passaggio tramite un host identificato come victim.com (alliterationexamples[.]com [192[.]3[.]96[.]68]): questa discrepanza tra HELO/hostname e reverse suggerisce relay/alias non coerente con un'infrastruttura legittima dell'organizzazione. Il blocco header fornito non include record di autenticazione visibili (SPF/DKIM/DMARC) né un chiaro Authentication-Results:: l'assenza di tali campi nella porzione acquisita impedisce di convalidare una firma DKIM o un allineamento DMARC.

Tabelle riassuntive

- **Dati principali del messaggio**

Campo	Valore normalizzato
Mittente (visual)	"Mail Delivery System" <support@victim[.]com>
Destinatario	victim@victim[.]com
Oggetto	"You have [9] pending incoming emails victim@victim[.]com"
Data	02-09-2025 20:54 +0200
Link/CTA	https://mailprivacy[.]world/login?email=victim@victim[.]com
Testo-esca	"pending emails", "low bandwidth", "Release Messages" / "Review Here"

Commento: la leva di ingegneria sociale è l'urgenza operativa (perdita di email) combinata con il mimetismo del sistema di posta. Pattern ampiamente osservato in campagne di credential harvesting.

- **Verifica intestazioni (SPF, DKIM, DMARC, Received)**

Voce	Esito nell'estratto
SPF	Non visibile nell'estratto fornito (manca Authentication-Results: / Received-SPF:)
DKIM	Non visibile (nessuna DKIM-Signature: nell'estratto)
DMARC	Non visibile (nessun allineamento riscontrabile)
Catena Received	Presente un hop con victim.com (alliterationexamples[.]com [192[.]3[.]96[.]68]) → incoerenza nome/IP

Commento operativo: Gli Header non sono completi, senza l'header completo non è possibile attestare i risultati di SPF/DKIM/DMARC. La presenza di un dominio terzo nell'HELO/rdns suggerisce inoltro/relay non autorizzato o spoofing.

- **Analisi URL e domini coinvolti (WHOIS/DNS/reputazione)**

Indicatore	Osservazioni & reputazione	Fonti/Note
mailprivacy[.]world (dominio di atterraggio)	Dominio raggiungibile; OSINT su Pulsedive mostra un profilo TI per l'URL e per il path /login (indicativo d'uso per raccolta credenziali).	(pulsedive.com)
Tematica "Mail Privacy / pending mail"	Social-engineering ricorrente (falso portale "Mail Privacy Protection"/webmail): pattern ampiamente documentato nella letteratura marketing/email security (MPP citato spesso come buzzword).	
alliterationexamples[.]com 192[.]3[.]96[.]68	IP range 192[.]3[.]96[.]0/24 (US). Reverse mapping su IPinfo mostra associazione diretta all'host alliterationexamples[.]com e contiguità con nomi *.colocrossing.com ⇒ probabile hosting presso ColoCrossing/VPS.	https://ipinfo.io/ips/192.3.96.0/24
Geolocalizzazione/Hosting IP 192[.]3[.]96[.]68	Blocco 192[.]3[.]0[.]0/16 in area ARIN (USA).	whois.arin.net https://www.abuseipdb.com/check/192.3.96.68
rapirescate[.]com (citato in campagne simili)	Sito legittimo (plumbing, Costa Rica) abusato come riferimento/menzione in campagne "You have [9] pending…". Non correlato all'organizzazione vittima; indicativo di spoofing/frode.	

- **Certificato SSL/TLS**

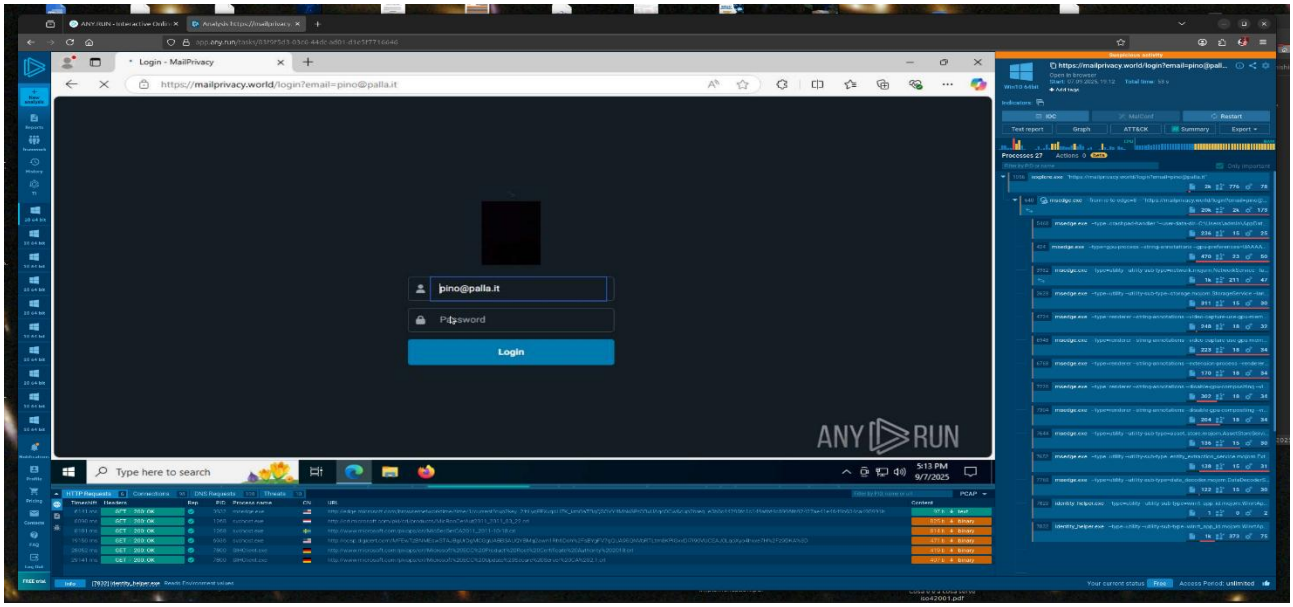
Destinazione	Dettagli reperiti
https://mailprivacy[.]world/login?...	crt.sh ID Logged At ⇧ Not Before Not After Common Name Matching Identities Issuer Name 20211081247 2025-08-08 2025-08-08 2025-11-06 mailprivacy.world *.mailprivacy.world mailprivacy.world C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV E36 20211081199 2025-08-08 2025-08-08 2025-11-06 mailprivacy.world *.mailprivacy.world mailprivacy.world C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV E36 20210965251 2025-08-08 2025-08-08 2025-11-06 mailprivacy.world *.mailprivacy.world mailprivacy.world C=US, O=Google Trust Services, CN=WE1 20210927560 2025-08-08 2025-08-08 2025-11-06 mailprivacy.world *.mailprivacy.world mailprivacy.world C=US, O=Google Trust Services, CN=WE1

- **Allegati**

Allegato	Esito
-	**Nessun allegato** presente nel messaggio analizzato. Di conseguenza non sono stati calcolati hash né avviate sandbox (Joe Sandbox / VT file).

- **Analisi contenuto e tecnica di ingegneria sociale**

Il messaggio sfrutta ansia da perdita ("hai [9] email bloccate"), urgenza ("low bandwidth", azione immediata), autorità simulata ("Mail Delivery System"), e coerenza visiva con servizi di webmail generici. Il bottone "Release Messages" indirizza a un dominio non correlato all'organizzazione (mailprivacy[.]world) con query pre-compilata dell'email: segno tipico di credential phishing (prefill del campo utente e richiesta password sul sito clone). I testi e la UX sono in linea con trend osservati da APWG (alto volume di phishing su posta/pagamenti) e articoli di awareness.



- **Whois/registrar e DNS (quanto ricavabile da OSINT pubblico)**

Oggetto	Dati chiave
mailprivacy[.]world	TLD .world gestito da registry di gruppo Identity Digital; i dettagli RDAP nominali sono consultabili via portali pubblici, ma spesso, come in questo caso, privacy-protected. La data di registrazione è : August 8, 2025. La data recente indica la probabile volontà di creare un dominio da utilizzare specificatamenteper attività malevole
Ip del dominio mailprivacy[.]world 188[.]114[.]96[.]7	L'IP è segnalato come malevolo dal ABUSEIPDB
alliterationexamples[.]com	Host associato all'IP 192[.]3[.]96[.]68 (US/ARIN). La classe /24 mostra vicinanza a host *.colocrossing.com, tipico hosting VPS/dedicato. (ipinfo.io, whois.arin.net)

- **Reputazione di IP/host (Abuse/Threat)**

LI'IP 192[.]3[.]96[.]68 è stato segnalato come malevolo su ABUSEIPDB.
Il range 192[.]3[.]96[.]0/24 risulta tipico di hosting commerciale statunitense e utilizzato spesso per file illeciti data la facilitòà di creazione di domini usa e getta.
Verifica "mittente = destinatario (stesso dominio)"
Il mittente visualizzato usa support@victim[.]com e il destinatario è victim@victim[.]com. Questo accoppiamento è un segnale frequente nelle frodi BEC-like o nello spoofing (From falsificato). Nel report, in ottemperanza alle istruzioni, tutte le occorrenze del dominio reale sono sostituite da victim[.]com e l'uso del medesimo dominio è stato evidenziato come parte della tattica.

- **IoC (Indicatori di Compromissione)**

Nota: tutti gli IoC sono defangati (punti sostituiti con [.]).

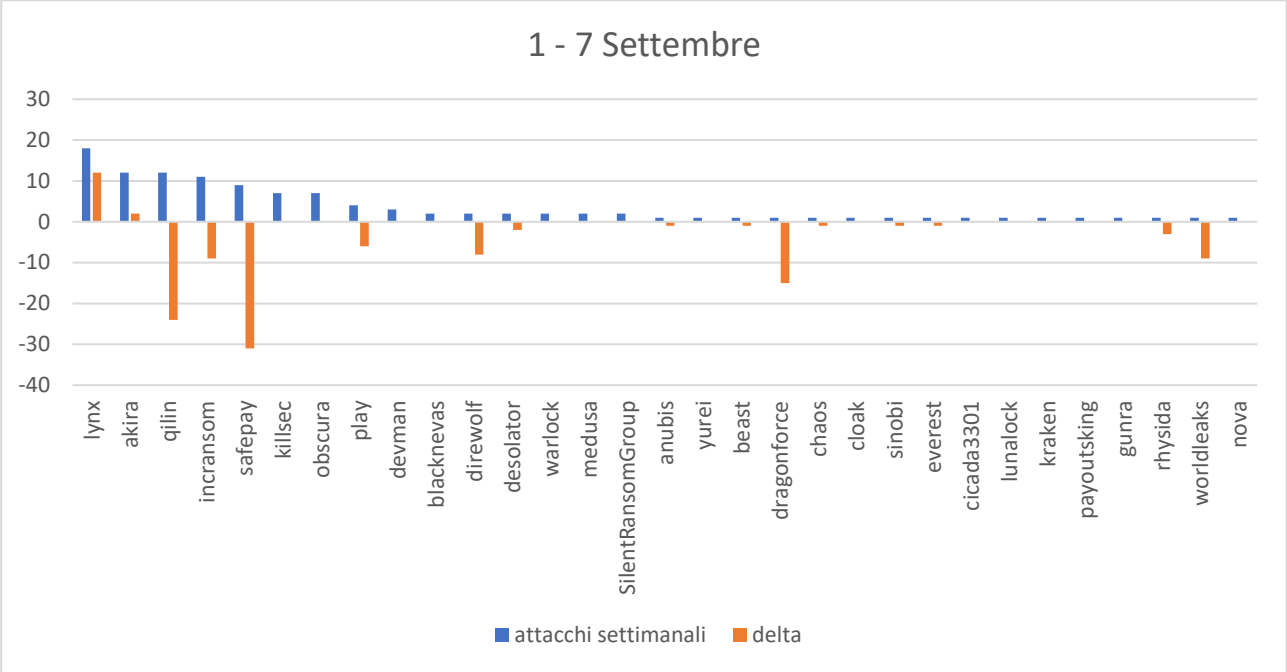
  - Dominio di atterraggio: mailprivacy[.]world
  - URL completo: https://mailprivacy[.]world/login?email=victim@victim[.]com
  - Host visto in header: alliterationexamples[.]com
  - Indirizzo IP associato: 192[.]3[.]96[.]68
  - Pattern testuale: "You have [9] pending incoming emails", "Due to low bandwidth", "Release Messages", "Review Here"
  - Tema campagna: fake mail delivery / mailbox pending / MPP buzzword

- **Valutazione e raccomandazioni**
  - Valutazione: Phishing mirato al furto credenziali (webmail/posta). Indicatori multipli (dominio esterno non affiliato, pre-compilazione email, tema "pending emails", host/IP su infrastruttura hosting generica) convergono su intento malevolo.
- **Azioni consigliate (immediate):**
  - Bloccare a livello gateway/proxy il dominio mailprivacy[.]world e l'URL indicato.
  - Harden DNS: assicurare pubblicazione/validità di SPF, DKIM, DMARC con policy DMARC almeno p=quarantine (idealmente reject dopo fase di tuning).
  - Retro-hunting: cercare hit di mailprivacy[.]world/alliterationexamples[.]com/192[.]3[.]96[.]68 nei proxy/log di rete negli ultimi 30 giorni.
  - User awareness: ribadire che nessun "Mail Delivery System" chiede di autenticarsi su domini esterni; aggiornare playbook di segnalazione.
  - Segnalazione: inviare l'URL a piattaforme comunitarie (PhishTank, OTX), e — se disponibile — al registrar/hosting (tramite contatti RDAP/ARIN) per takedown.
- **Riepilogo conclusivo**

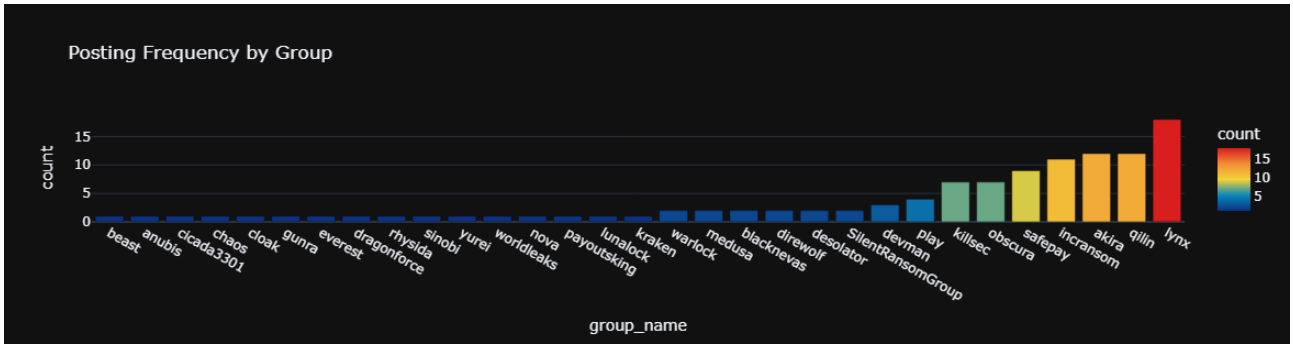
L'email analizzata adotta uno schema "pending messages / low bandwidth" per indurre l'utente ad autenticarsi su mailprivacy[.]world, verosimilmente un portale clone volto al furto di credenziali. Gli header non mostrano (nell'estratto) tracce di SPF/DKIM/DMARC; l'infrastruttura menzionata (alliterationexamples[.]com su 192[.]3[.]96[.]68) ricade in hosting commerciale USA e non appare correlata al dominio della vittima. Il caso è coerente con campagne documentate in open-source (Brendinghat/PCRisk). Si raccomanda blocco degli IoC, verifica dei log, hardening DMARC e sensibilizzazione utenti.

4.2 Ransomware

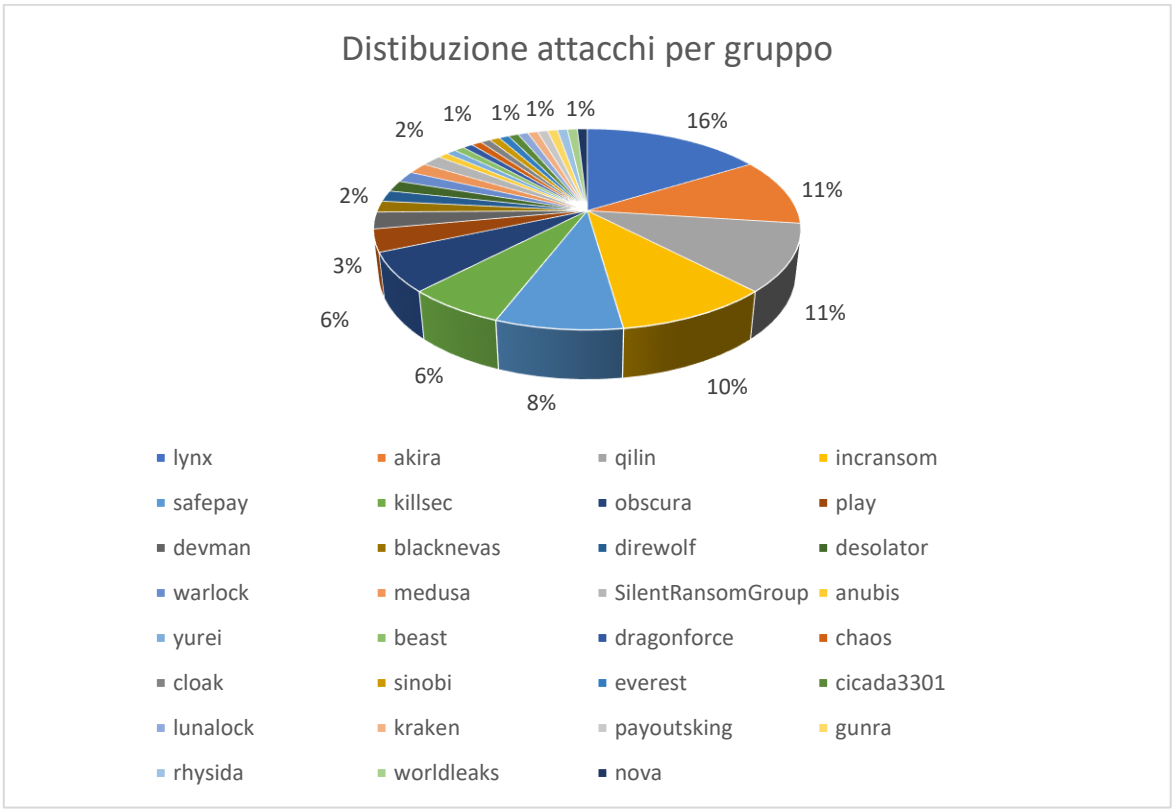
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (1 – 7 Settembre). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

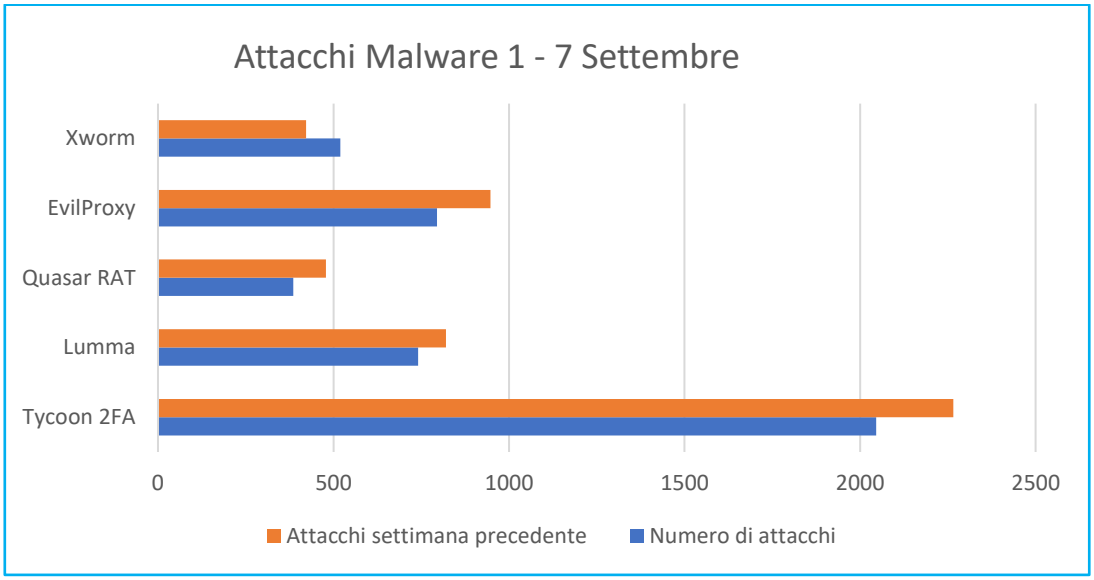


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:


Distibuzione attacchi per gruppo
16%
11%
11%
10%
8%
6%
6%
3%
2%
2%
1%
1%
1%
1%
lynx
akira
qilin
incransom
safepay
killsec
obscura
play
devman
blacknevas
direwolf
desolator
warlock
medusa
SilentRansomGroup
anubis
yurei
beast
dragonforce
chaos
cloak
sinobi
everest
cicada3301
lunalock
kraken
payoutsking
gunra
rhysida
worldleaks
nova

4.3 Malware

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



Come sempre riportiamo un'analisi dettagliata dei malware risultati più attivi nella settimana di osservazione

- **Obscura (ransomware)**

Il ransomware Obscura è emerso il 29 agosto 2025 come nuova minaccia. Il payload si installa sui domain controller, sfrutta i servizi NETLOGON e avvia attività di sistema nascoste (attività pianificate e script) per diffondersi e criptare i dati. Dopo la cifratura – effettuata con algoritmi avanzati (XChaCha20) – Obscura rimuove i backup (Shadow Copy) per impedire il ripristino dei file. Il malware include inoltre un ransom note ("README_Obscura.txt") in cui esorta le vittime a contattare gli aggressori via email (accordi privati senza terze parti).

IoC:

Tipo	Indicatore
SHA256	c00a2d757349bfff4d7e0665446101d2ab46a1734308cb3704f93d20dc7aac23
File	README_Obscura.txt (ransom note)
Script Path	C:\WINDOWS\sysvol\sysvol\[domain].local\scripts\

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1053.005	Scheduled Task	Persistenza tramite attività pianificate
T1486	Data Encrypted for Impact	Criptografia dei file
T1490	Inhibit System Recovery	Eliminazione di Shadow Copy per impedire il ripristino
T1027	Obfuscated Files or Information	Offuscamento del payload

Contromisure:

- Applicare EDR con regole che intercettino la creazione di attività pianificate sospette, l'uso di strumenti di backup manipolati e script di policy di dominio non autorizzati.
- Mantenere backup offline; aggiornare costantemente i sistemi operativi e disabilitare account non utilizzati.
- Anche la segmentazione di rete e il principio del minor privilegio riducono l'impatto.

Livello di rischio: Critico (ransomware in rapida evoluzione).

- **NEZHA**

Il ransomware NEZHA è stato individuato da Cyfirma all'inizio di settembre 2025. Viene distribuito presumibilmente via email dannose o exploit, quindi esegue operazioni di discovery (raccolta informazioni di sistema), keylogging (per eventuali credenziali) e stealth grazie a tecniche di offuscamento. Al termine dell'infezione, NEZHA cifra i file con estensione ".NEZHA" e rilascia la nota di riscatto "README.TXT". Gli aggressori avvertono le vittime di non consultare terze parti e minacciano la pubblicazione dei dati esfiltrati.

IoC:

non ancora pubblicati dettagli completi; si segnala l'estensione ".NEZHA" e l'uso del file README.TXT come ransom note

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1047	Windows Management Instrumentation	Esecuzione di comandi via WMI
T1059.001	Command and Scripting Interpreter: PowerShell	Uso di PowerShell per installazione malware
T1056.001	Input Capture: Keylogging	Raccolta di credenziali tramite keylogger
T1486	Data Encrypted for Impact	Cifratura dei dati

Contromisure:

- Implementare EDR con visibilità su WMI/Powershell anomali.
- Applicare policy di restrizione macros e script; disabilitare account locali non necessari.
- Mantenere patch aggiornate (soprattutto componenti remoting); predisporre back-up isolati.

Livello di rischio: Alto (ransomware emergente con estorsione dati).

- **TinyLoader**

TinyLoader è un malware loader riportato il 2 settembre 2025. Viene diffuso via condivisioni di rete, unità USB infette e collegamenti ingannevoli. Una volta eseguito, TinyLoader installa malware secondari – ad esempio il trojan ladro di credenziali RedLine Stealer e il RAT DCRat – e agisce da clipper criptovalute (sostituisce indirizzi wallet copiati in memoria).

Mantiene persistenza copiandosi in cartelle nascoste e creando modifiche al registro di sistema, e comunica con server C2 in diversi paesi europei.

il loader sfrutta risorse locali (USB, file .lnk) e vulnerabilità per infiltrarsi; la sua infrastruttura (IP 176[.]46[.]152[.]47 LV) gestisce pannelli Web di comando. TinyLoader mira prevalentemente a sistemi Windows aziendali di vari settori per sottrarre credenziali e criptovalute

IoC:

Tipo	Indicatore
IPs	• 107[.]150[.]0[.]155 • 176[.]46[.]152[.]47 • 77[.]90[.]153[.]62 • 176[.]46[.]152[.]46
Files	• injector.exe.DcRat (Main payload injector component) • c.exe.DcRat (Configuration or communication module) • index.php.DcRat (Web-based C2 communication script) • svchost.exe.DcRat (Masquerades as legitimate Windows service)

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1059.001	Command and Scripting Interpreter: PowerShell	Automazione con PowerShell
T1112	Modify Registry	Persistenza modificando il registro
T1562.001	Impair Defenses: Disable or Modify Tools	Disabilitazione antivirus o firewall

Contromisure:

- Bloccare gli IP C2 noti (firewall).
- Disabilitare l'esecuzione automatica da unità rimovibili (policy). Monitorare accessi a file nascosti e modifiche sospette al registro.
- Utilizzare antivirus/EDR con signature contro TinyLoader/DCRat.

Livello di rischio: Medio-Alto (facile diffusione tramite clipper + installazione di stealers).

- **GhostRedirector (backdoor C++ e moduli IIS)**

Il gruppo GhostRedirector (nuovo attore APT presumibilmente collegato alla Cina) ha compromesso decine di server Windows in Brasile, Thailandia, Vietnam e altri Paesi. Utilizza due strumenti artigianali: Rungan, un backdoor C++ passivo che esegue comandi sul server, e Gamshen, un modulo nativo IIS che manipola il traffico Web per campagne di "SEO poisoning" a favore di siti criminali.

Gli attaccanti sfruttano exploit noti (EfsPotato, BadPotato) per elevare privilegi e creare account amministrativi "fantoccio" che installano i payload. Questo malware è finalizzato non a estrarre dati, ma a controllare server web e alterarne i risultati di ricerca.

GhostRedirector non pare concentrato su un settore specifico; ha agito inizialmente con SQL injection su app Web pubbliche, ottenendo accesso tramite exploit su SSDP (es. T1190) e scaricando i moduli Dannosi via PowerShell

IoC:

Tipo	Indicatore
IPs	• 103.251.112[.]11 • 43.228.126[.]4 • 104.233.192[.]1 • 104.233.210[.]229
Domini	• xzs.868id[.]com • q.822th[.]com • gobr.868id[.]com • brproxy.868id[.]com • www.cs01[.]shop
Files	• miniscreen.dll (Rungan, a passive C++ backdoor) • auto_sign.exe (Uno strumento per creare un nuovo utente o distribuire webshell sul server compromesso) • auto.exe (Uno strumento per creare un nuovo utente sul server compromesso) • SitePut.exe • EfsNetAutoUser.exe • NetAutoUser.exe

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1190	Exploit Public-Facing Application	Sfruttamento di vulnerabilità web (SQLi)
T1059.001	Command and Scripting Interpreter: PowerShell	Esecuzione di script PowerShell per drop di payload
T1106	Native API	Uso di API di basso livello (ad es. HTTP in C++)
T1608.001	Stage Capabilities: Upload Malware	GhostRedirector ha installato Rungan e Gamshen su server controllati dagli aggressori..
T1583.001	Acquire Infrastructure: Domains	GhostRedirector utilizza domini dannosi per ospitare payload e per i suoi server C&C
T1587.001	Develop Capabilities: Malware	GhostRedirector sviluppa il proprio malware

Contromisure:

- correggere la vulnerabilità note di SQL injection o configurazione errata del server Web.
- Isolare immediatamente i server compromessi.
- Usare WAF (Web Application Firewall); adottare soluzioni EDR per rilevare i vari tool Rungan/Gamshen (ad es. flag per DLL nativi IIS sospetti).
- Rimuovere gli utenti creati arbitrariamente. Bloccare i domini maligni (es. *.868id[.]com) e monitorare l'anomalia del traffico DNS verso i server Cloudflare usati dai C2.

Livello di rischio: Alto (backdoor finalizzata a campagne furtive e mantenimento di accesso a lungo termine).

- **NotDoor**

NotDoor è un nuovo backdoor VBA scoperto da Lab52 e attribuito al gruppo APT28 ("Fancy Bear"). Si insinua nelle installazioni di Outlook tramite un DLL legittimo vulnerabile (Microsoft OneDrive.exe) che carica SSPICLI.dll: questo installer VBA carica un macro backdoor in Outlook e disabilita le protezioni macro. Il malware monitora le email in arrivo cercando trigger ("Daily Report" nell'esempio) e, quando il testo corrisponde, esegue comandi (invia/esfiltra file, esegue payload) sul PC della vittima.

È stato riscontrato in attacchi contro compagnie in paesi NATO. Veicolato via phishing con exploit DLL sideload: usa OneDrive.exe (firmato) come vettore (T1218.011).

Una volta attivato, il backdoor VBA persiste modificando chiavi di registro di Outlook per abilitare macro e cancellare gli alert. Scambia dati via HTTP e invia report attraverso email (es. a indirizzo proton.me)

Indicatori di compromissione (IoC):

Tipo	Indicatore
Hashs	Malicious DLL "SSPICLI.dll" (loader VBA): • 5a88a15a1d764e635462f78a0cd958b17e6d22c716740febc114a408eef66705 File di configurazione "testtemp.ini" (payload): • 8f4bca3c62268fff0458322d111a511e0bcfba255d5ab78c45973bd293379901

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1218.011	Signed Binary Proxy Execution: Mshta/OneDrive	DLL sideloading tramite OneDrive.exe
T1566.001	Phishing: Spearphishing Attachment	Veicolazione via email malevole
T1059.001	Command and Scripting Interpreter: PowerShell	Esecuzione di comandi offuscati via PowerShell
T1562.001	Impair Defenses: Disable or Modify Tools	Disabilitazione protezioni macro di Outlook

Contromisure:

- Applicare restrizioni su esecuzione di codice da percorsi non standard.
- Abilitare sempre la protezione macro in Office (non permettere macro non firmate).
- Bloccare o monitorare il caricamento di DLL in OneDrive.exe.
- Usare EDR per intercettare processi di Outlook che eseguono script sospetti.
- Educare gli utenti a non aprire allegati inattesi e a verificare la firma digitale dei file.

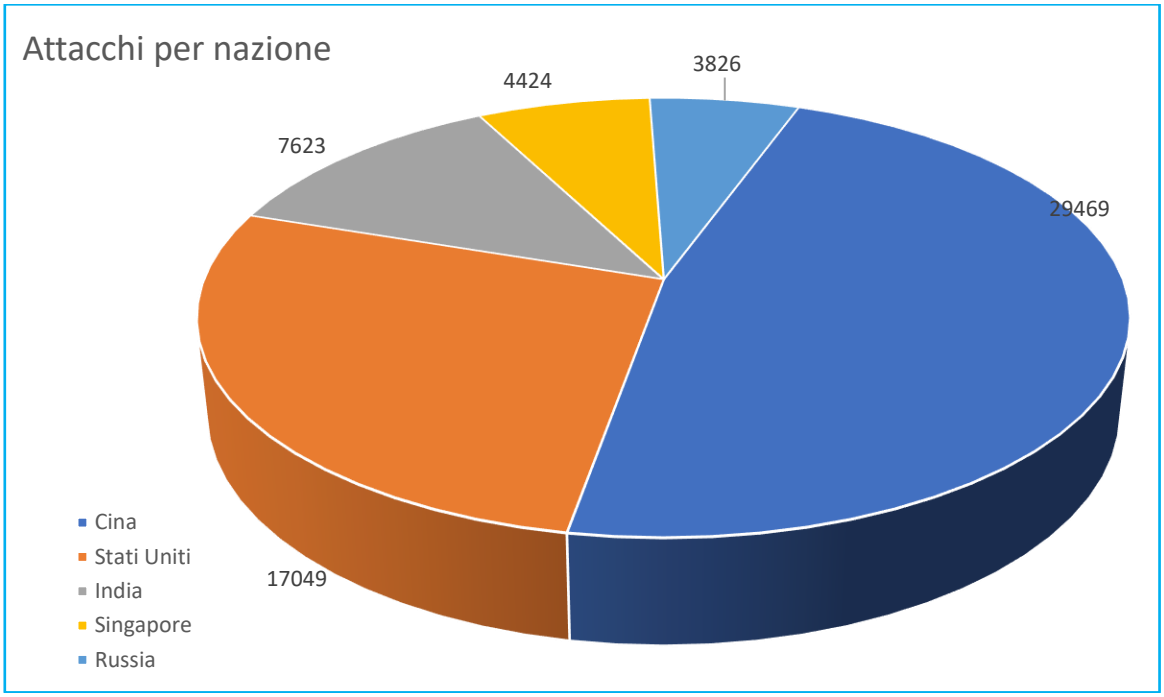
Livello di rischio: Alto.

Riepilogo:

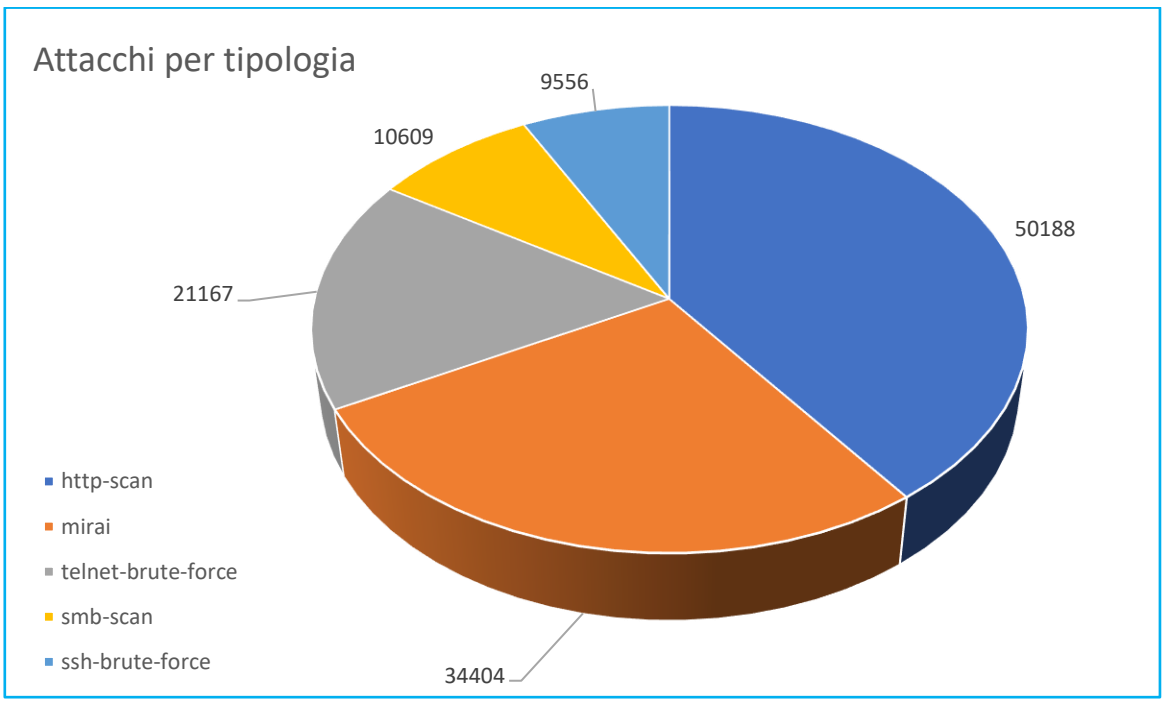
Malware	Categoria	Livello di rischio
Obscura	Ransomware	Critico
NEZHA	Ransomware	Alto
TinyLoader	Loader (Stealer)	Medio-Alto
GhostRedirector	Backdoor C++ e IIS	Alto
NotDoor	Backdoor (Outlook)	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 1 – 7 Settembre, suddivisa per nazione e limitata alle prime cinque
ùù posizioni:

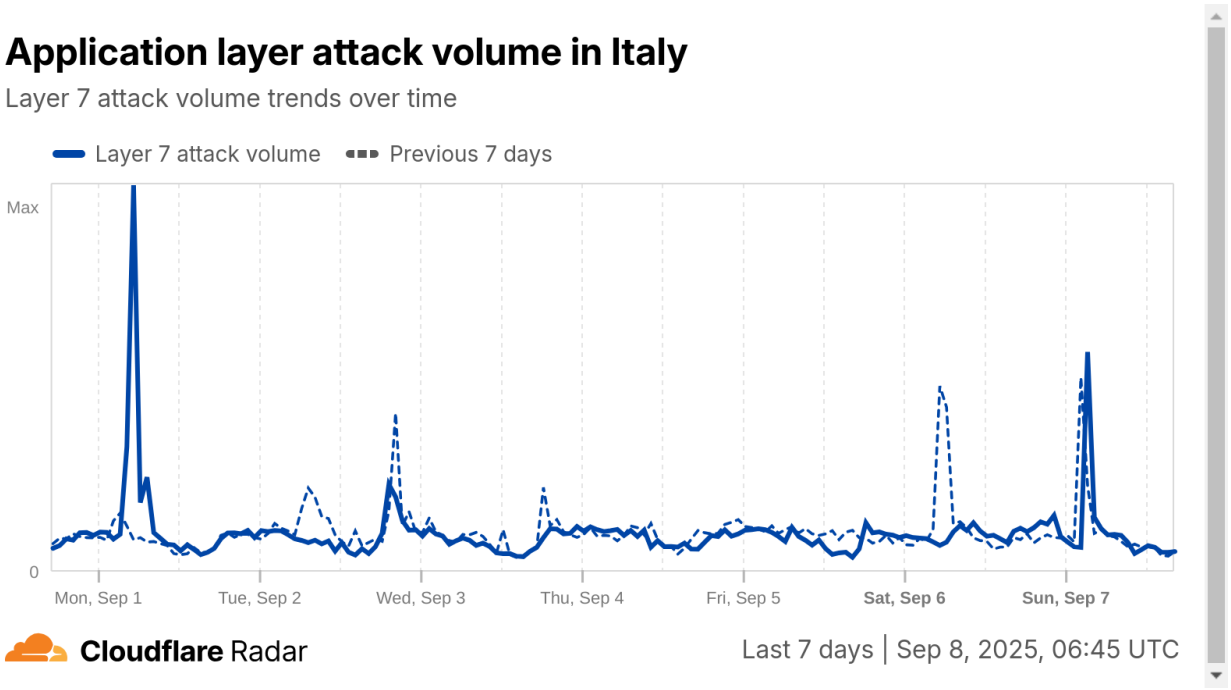


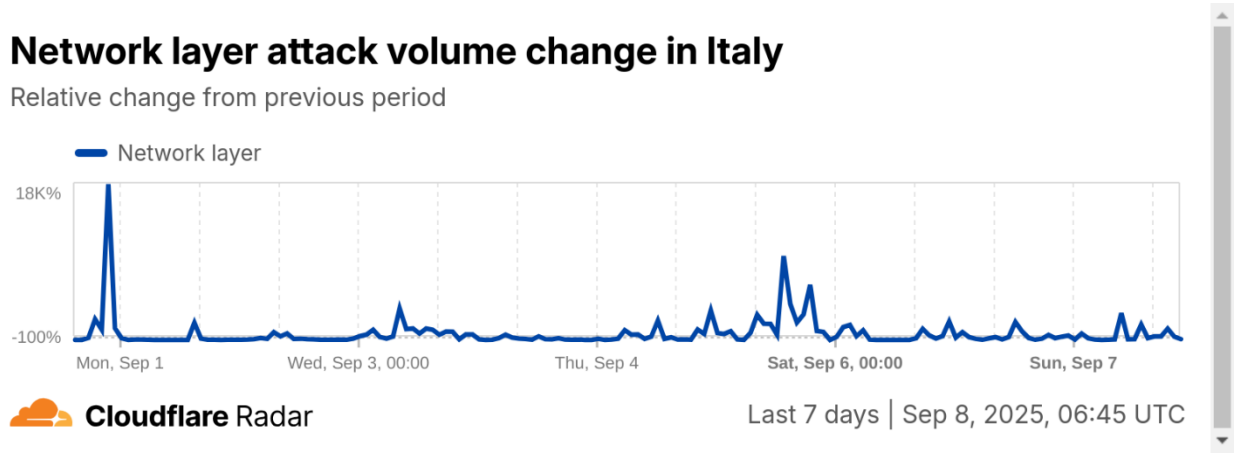
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
UNIVERSITY OF ST. THOMAS	STATI UNITI
DESCRIZIONE	La University of St. Thomas (Houston, Texas) ha subito un attacco informatico che ha causato un blackout dei sistemi online per nove giorni, bloccando servizi fondamentali come la registrazione dei corsi, l'accesso alle borse di studio e l'acquisto di libri. Il 4 settembre, il gruppo ransomware INC_RANSOM ha rivendicato l'attacco, affermando di aver sottratto 1,8 TB di dati e pubblicando alcuni documenti rubati come prova. Tuttavia, l'università non ha confermato ufficialmente né la rivendicazione né la reale entità del furto. I sistemi sono stati ripristinati gradualmente attraverso un sito temporaneo predisposto per garantire i servizi essenziali.

TARGET	LOCALIZZAZIONE
THE FIXING COMPANY	IRLANDA
DESCRIZIONE	Il 5 settembre 2025, The Fixing Company, azienda irlandese attiva nella vendita di materiali edili e abbigliamento da lavoro, è stata vittima di un attacco informatico. Il gruppo Obscura ha rivendicato il breach, ma al momento non è chiaro quali dati siano stati rubati né l'entità del danno. L'azienda non ha ancora rilasciato dichiarazioni ufficiali, e non sono stati diffusi dettagli su eventuali conseguenze per clienti o partner. La situazione è ancora in fase di valutazione.

TARGET	LOCALIZZAZIONE
CAMERA DI COMMERCIO DI ALMERÍA	SPAGNA
DESCRIZIONE	Il 4 settembre 2025, la Camera di Commercio di Almería è stata vittima di un grave attacco informatico. Il breach è stato rivendicato dal gruppo hacker Qilin. Secondo le informazioni disponibili, gli attaccanti sono riusciti a sottrarre circa 771 GB di dati, anche se non è ancora stato chiarito nel dettaglio quali tipi di informazioni siano stati compromessi. L'attacco ha preso di mira il sito ufficiale dell'ente (camaradealmeria.com) e potrebbe aver coinvolto documenti amministrativi, dati aziendali sensibili, informazioni su corsi di formazione e pratiche relative ai servizi per le imprese locali.

4.6 Defacement

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

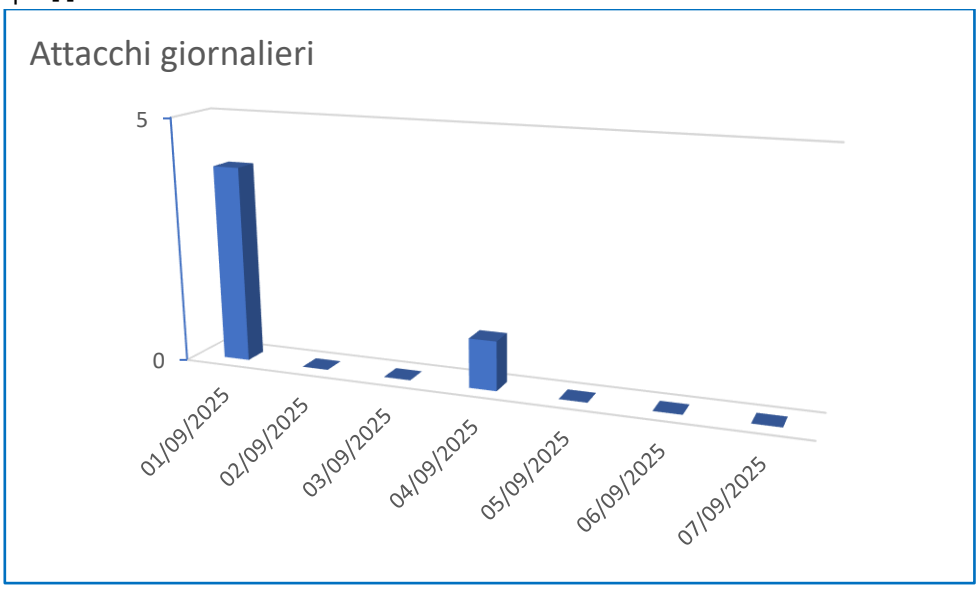


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

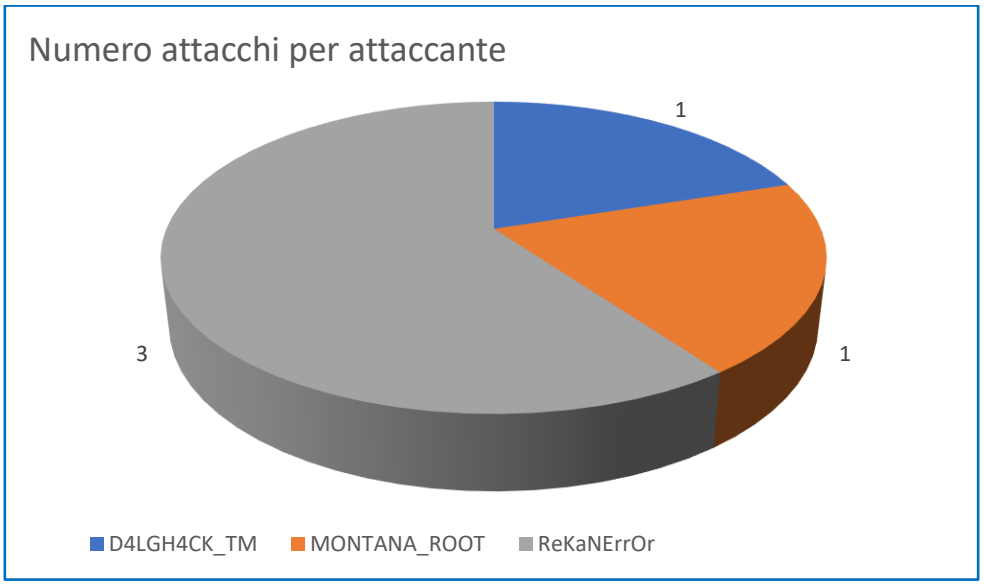


Figura 2: Defacement - Attaccanti più attivi nel periodo 1 – 7 Settembre

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

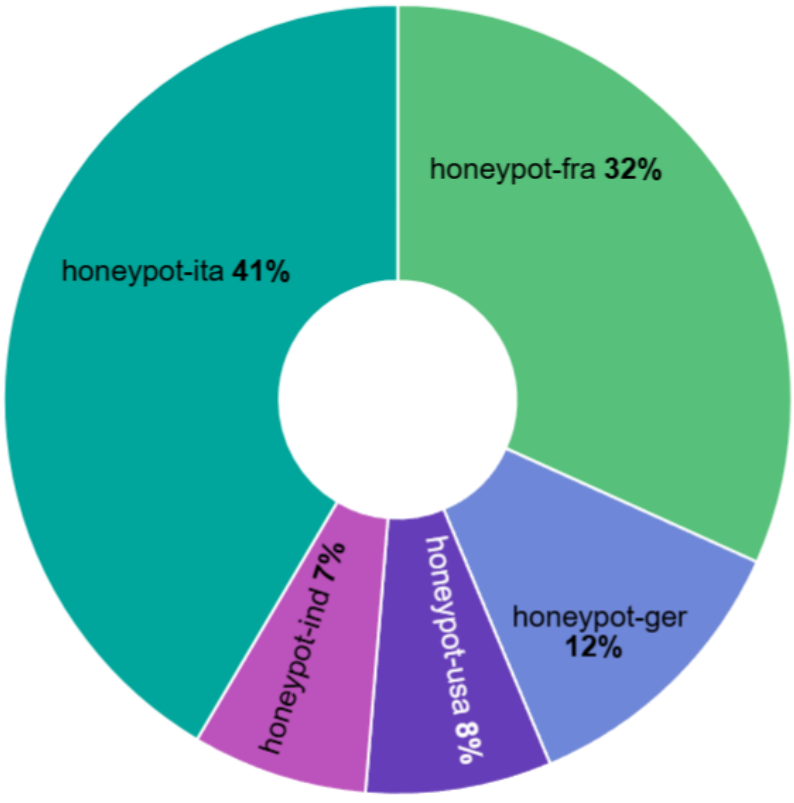
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

1.639.678 Attacks

12.763 Unique Src IPs

70 Unique HASSHs

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



Questa invece la situazione a livello italiano:

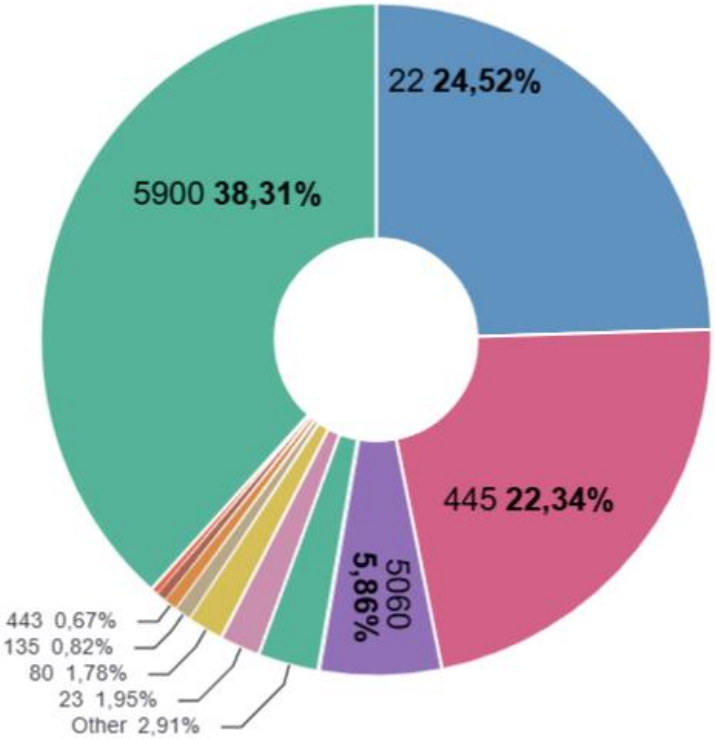
605.706
Attacks

5.125
Unique Src IPs

56
Unique HASSHs

5.1.1 Attacchi ai servizi

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



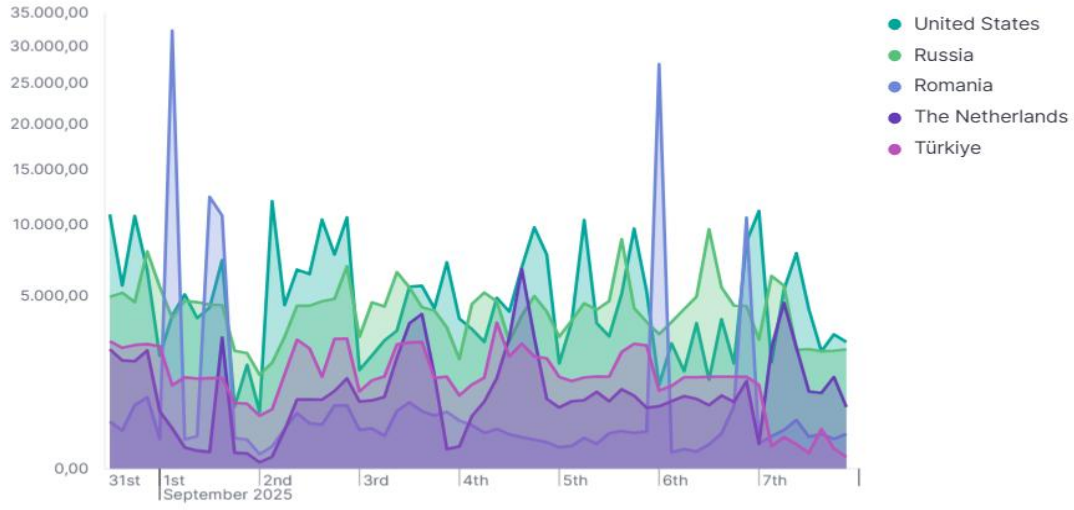
5.1.2 IP Attaccanti

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

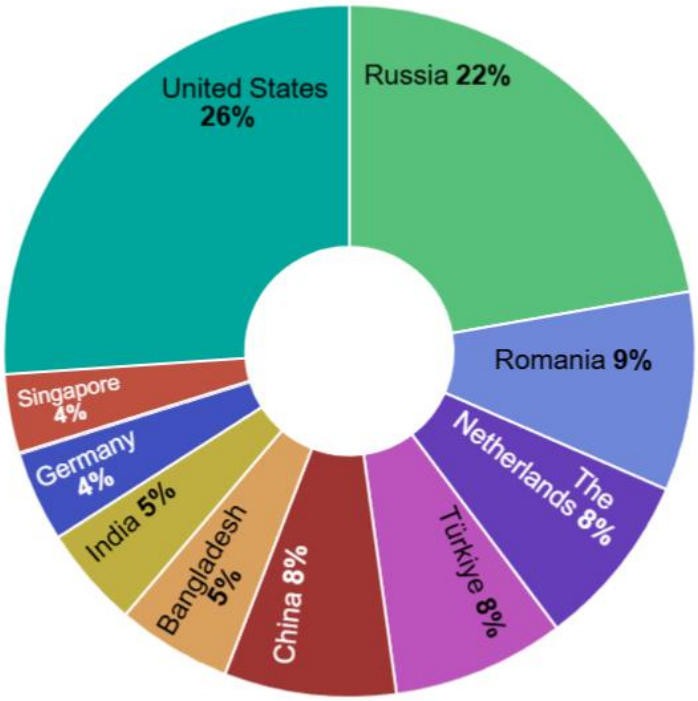
Source IP	Count
2.57.121.148	93.577
185.233.247.245	86.484
103.121.194.23	58.550
142.202.189.5	37.463
142.202.191.234	36.893
45.134.26.33	36.125
186.67.186.10	27.474
178.22.24.32	26.328
79.124.56.162	25.592
193.37.69.157	25.357

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:

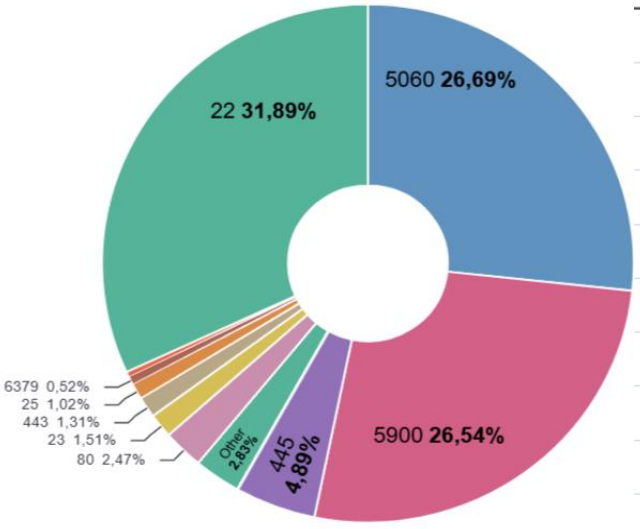


5.2 Italian Honeypot N.1

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):



Port	Count
22	54.804
5060	45.869
5900	45.619
445	8.400
80	4.239
23	2.591
443	2.251
25	1.751
6379	896
1025	582

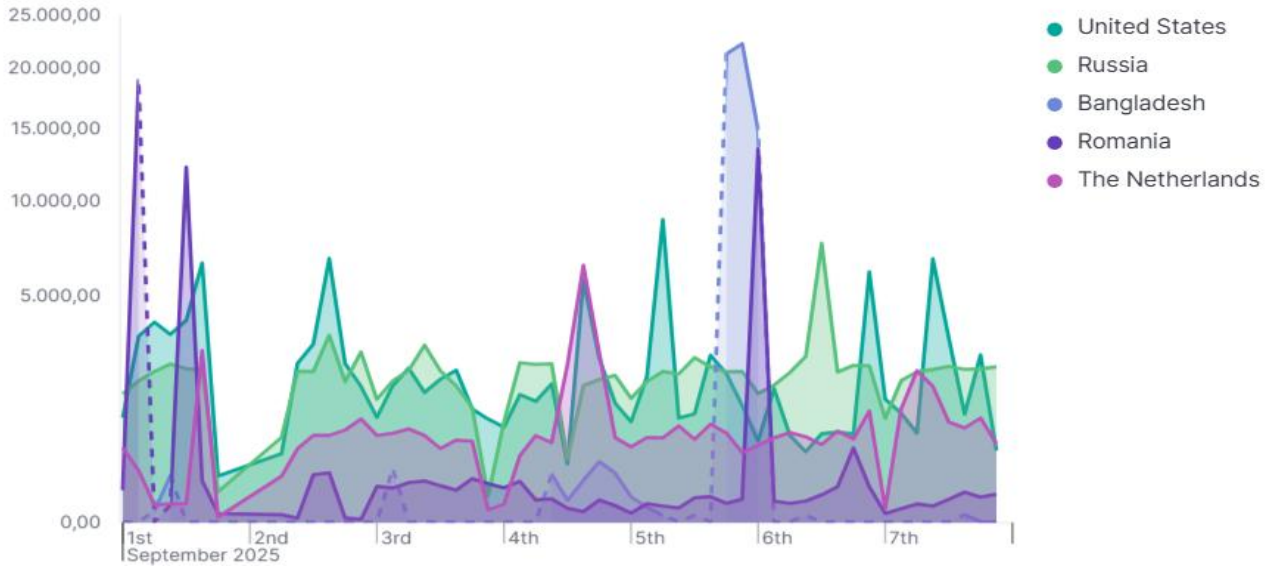
5.2.2 IP Attaccanti

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

Source IP	Count
103.121.194.23	58.550
2.57.121.148	44.733
185.233.247.245	27.209
45.134.26.33	16.484
142.202.191.234	16.321
148.72.158.192	15.872
178.22.24.32	12.460
142.202.189.5	10.685
217.119.139.47	10.170
196.251.66.132	10.103

5.2.3 Paesi di provenienza degli attacchi

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

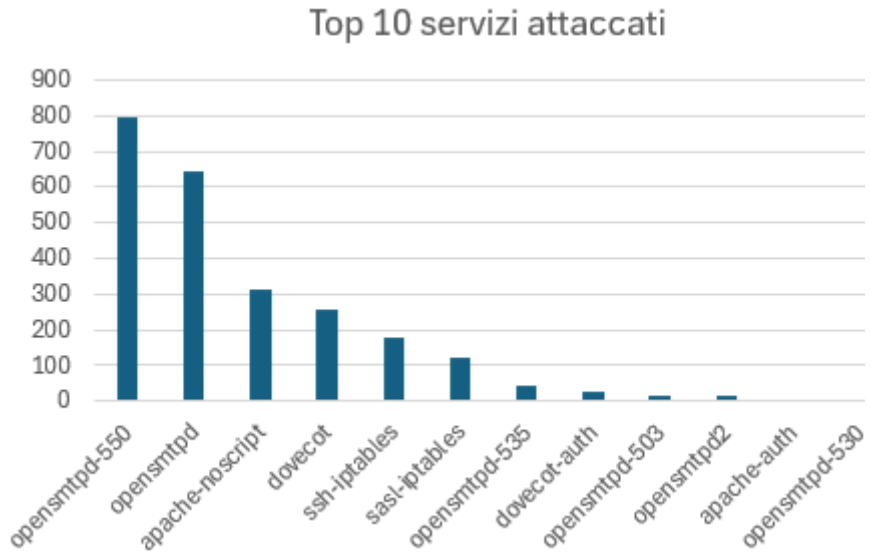


5.3 Italian Honeypot N.2

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.



Servizio / Codice	Significato tecnico	Tipologia di attacco tipica	Rischio associato
apache-noscript	Attacchi ad Apache su pagine/script non protetti	Exploit di script, RCE, SQL injection, upload malevoli	Compromissione del web server, distribuzione malware
opensmtpd	Connessioni SMTP generiche	Tentativi di relay abusivo, exploit di vulnerabilità note	Uso come server di spam, RCE
opensmtpd-535	535 = Authentication failed	Brute force su credenziali SMTP AUTH	Compromissione account email
opensmtpd-550	550 = Mailbox unavailable / Relay denied	Tentativi di relay aperto	Server usato per spam e phishing
dovecot	Server IMAP/POP3	Brute force per accesso a caselle email	Furto account, esfiltrazione mail
ssh-iptables	Attacchi SSH bloccati da fail2ban/iptables	Brute force su account SSH	Accesso non autorizzato al server
sasl-iptables	Autenticazioni SASL fallite bloccate	Brute force su autenticazione email (SMTP AUTH)	Compromissione account email

Servizio / Codice	Significato tecnico	Tipologia di attacco tipica	Rischio associato
dovecot-auth	Autenticazione Dovecot specifica	Brute force su POP3/IMAP	Compromissione account di posta
opensmtpd-503	503 = Bad sequence of commands	Scanner SMTP mal configurati	Ricognizione, tentativi di exploit
opensmtpd-502	502 = Command not implemented	Comandi SMTP non validi → test di relay	Identificazione di configurazioni vulnerabili
apache-auth	Autenticazione su aree protette Apache	Brute force su HTTP Basic/Digest	Accesso a directory riservate
opensmtpd-530	530 = Authentication required	Tentativi di invio mail senza login	Abuso relay per spam

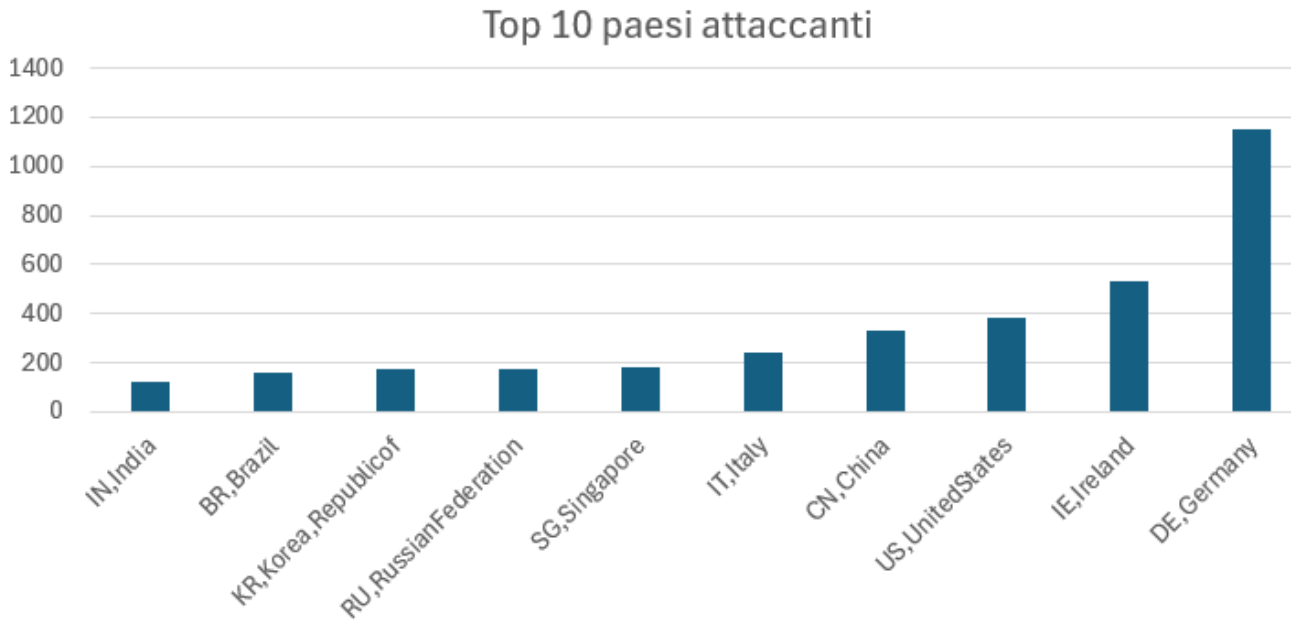
5.3.2 IP attaccanti

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
185[.]17[.]106[.]137	56
144[.]64[.]57[.]246	39
62[.]173[.]140[.]179	29
81[.]28[.]9[.]66	24
185[.]176[.]220[.]108	23
62[.]152[.]59[.]17	22
78[.]153[.]140[.]25	21
181[.]85[.]5[.]75	20
181[.]122[.]149[.]183	20
179[.]14[.]191[.]36	20

5.3.3 Paesi di provenienza degli attacchi

Questa invece la distribuzione dei paesi attaccanti:



6 Company Profile S3K

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

COME LO FACCIAMO:

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

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

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

CON QUALI LEVE OPERIAMO:

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

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

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

CHI SIAMO:

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

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

LA NOSTRA MISSION:

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

I NOSTRI VALORI:

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

CONTATTI:

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

DISCLAIMER

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

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

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

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

CLASSIFICAZIONE DOCUMENTO

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

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

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

Cyber security

RISK REPORT

S3K

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

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