S3K

Cyber security

RISK REPORT

\ week 08.09.2025 - 14.09.2025

Sommario

1 Il Cyber Security Risk Report S3K 5

1.1 Vulnerabilità e Aggiornamenti di Sicurezza 5

1.2 Panorama delle Minacce e Attacchi 5

1.3 Ransomware: Attività della Settimana 6

1.4 Data Breach e Raccomandazioni 6

1.5 Intelligence da Honeypot 7

2 Security news 8

2.1 Rilasci aggiornamenti e patch 8

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

3 CVE Monitor 11

3.1 Sintesi Settimanale CVE 11

3.2 Tendenze 14

3.3 Nuove CVE 15

3.4 CVE attualmente utilizzate in attacchi 16

4 Attacchi 17

4.1 Phishing 17

4.2 Ransomware 22

4.3 Malware 24

4.4 DDoS rilevati 34

4.5 Data Breach 36

4.6 Defacement 37

5 Honeypot 38

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale 38

5.1.1 Attacchi ai servizi 39

5.1.2 IP Attaccanti 40

5.1.3 Paesi di provenienza degli attacchi 41

5.2 Italian Honeypot N.1 42

5.2.1 Attacchi ai servizi 42

5.2.2 IP Attaccanti 43

5.2.3 Paesi di provenienza degli attacchi 43

5.3 Italian Honeypot N.2 45

5.3.1 Attacchi ai servizi 45
5.3.2 IP attaccanti 45
5.3.3 Paesi di provenienza degli attacchi 46
6 Company Profile S3K 47

CYBER SECURITY RISK REPORT
37/25

1 Il Cyber Security Risk Report S3K

Rapporto di analisi della sicurezza informatica per la settimana 8-14 Settembre 2025, con focus su vulnerabilità critiche, attacchi ransomware e minacce emergenti nel panorama digitale italiano e mondiale.

1.1 Vulnerabilità e Aggiornamenti di Sicurezza

La settimana è stata caratterizzata da un picco straordinario di vulnerabilità critiche, con particolare concentrazione il 9 settembre quando SAP, Siemens, Microsoft e Adobe hanno rilasciato contemporaneamente advisory di sicurezza ad alto impatto. Questi aggiornamenti hanno interessato principalmente ambienti enterprise e sistemi di controllo industriale.

- Zabbix

Rilevate vulnerabilità di gravità "alta" nel noto prodotto open source per monitoraggio. Versioni interessate: 6.0.x (≤6.0.33), 6.4.x (≤6.4.18), 7.0.x (≤7.0.3).

- NVIDIA NVDebug

Identificate 3 vulnerabilità con gravità "alta" che riguardano NVIDIA NVDebug, versioni precedenti alla 1.7.0.

- Samsung Critical Patch

Bollettino settembre 2025 corregge 25 vulnerabilità, inclusa CVE-2025-21043 già sfruttata attivamente (Android 13-16).

Di particolare preoccupazione sono le numerose vulnerabilità SQL injection scoperte in applicativi PHP open-source (PHPGurukul, Student System, CRM) già corredate di proof-of-concept pubblici, che rendono l'impatto immediato e critico per le organizzazioni che utilizzano questi sistemi.

- CVE Critiche della Settimana
    - CVE-2025-42944 - SAP NetWeaver (CVSS 10.0)
    - CVE-2025-54261 - Adobe ColdFusion (CVSS 10.0)
    - CVE-2025-55232 - Microsoft HPC Pack (CVSS 9.8)
    - CVE-2025-55234 - Windows SMB Server (CVSS 9.8)

1.2 Panorama delle Minacce e Attacchi

L'analisi degli attacchi evidenzia un'evoluzione significativa delle tecniche di social engineering, con particolare focus sui deepfake e sui nuovi metodi di phishing. La manipolazione digitale sta diventando sempre più sofisticata, passando dal semplice furto di immagini alla creazione di contenuti completamente artificiali ma estremamente convincenti.

- Deepfake e Manipolazione Digitale

Crescente utilizzo di tecnologie AI per creare contenuti fraudolenti, dalle false sponsorizzazioni finanziarie ai contenuti pornografici non consensuali. Le persone comuni risultano più vulnerabili rispetto ai personaggi pubblici.

- Truffe Mirate agli Anziani

Nuova ondata di truffe informatiche USA con focus sulla popolazione anziana. Gli attaccanti sfruttano falsi allarmi di sicurezza per indurre al download di software malevoli e successivo prosciugamento dei conti bancari.

- Mercato Spyware

L'Italia si posiziona al terzo posto mondiale per investitori nel settore spyware, dopo Israele e USA, sollevando preoccupazioni per la sicurezza nazionale e i diritti umani.

1.3 Ransomware: Attività della Settimana

L'attività ransomware ha mostrato una distribuzione concentrata su pochi gruppi principali, con particolare attenzione ai settori finance e pubblica amministrazione. Il grafico evidenzia come alcuni gruppi abbiano intensificato le operazioni rispetto alla settimana precedente.

- Malware più Attivi

I kit di phishing Adversary-in-the-Middle dominano la scena delle minacce, con particolare pericolosità per gli ambienti Microsoft 365 e servizi cloud aziendali.

    - **Tycoon 2FA** - Kit PhaaS con bypass MFA
    - **Lumma Stealer** - Infostealer MaaS diffuso
    - **Sneaky 2FA** - Nuovo kit AiTM via Telegram
    - **Quasar RAT** - Remote access trojan persistente

1.4 Data Breach e Raccomandazioni

La settimana ha registrato diversi incidenti significativi che evidenziano la necessità di rafforzare le misure di protezione, particolare attenzione agli enti pubblici italiani che risultano sempre più nel mirino dei cybercriminali.

- Comune di Firenze

Presunta violazione con database contenenti informazioni anagrafiche sensibili (codice fiscale, dati personali) messi in vendita per 1.500$ su forum underground.

- MEF Panama

Attacco rivendicato da INC Ransom con sottrazione di oltre 1,5 TB di dati finanziari e documenti di bilancio.

- Comune di Canegrate

Database e credenziali di accesso in vendita per 500$ su forum cybercriminali, con sample di dati pubblicati.

1.5 Intelligence da Honeypot

I sistemi di monitoraggio S3K hanno rilevato oltre 15.000 attacchi questa settimana, con particolare concentrazione su servizi SSH (22), HTTP (80/443) e Telnet (23). La distribuzione geografica mostra Cina, Russia e Stati Uniti come principali fonti di attacco.

- Raccomandazioni Prioritarie
    - Applicare immediatamente patch SAP, Siemens, Adobe e Microsoft
    - Implementare MFA resistente al phishing (FIDO2)
    - Rafforzare controlli email anti-phishing
    - Monitorare login anomali con soluzioni UEBA
    - Segmentare reti ICS/ERP critiche

"La convergenza di vulnerabilità critiche enterprise e l'evoluzione delle tecniche di social engineering richiedono un approccio integrato alla cybersecurity, che combini aggiornamenti tempestivi, formazione del personale e tecnologie anti-phishing avanzate."

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Zabbix	Rilevate alcune nuove vulnerabilità, di cui una con gravità "alta", in Zabbix, noto prodotto open source per il monitoraggio di reti e sistemi informatici. Prodotti e/o versioni affette • 6.0.x, versione 6.0.33 e precedenti • 6.4.x, versione 6.4.18 e precedenti • 7.0.x, versione 7.0.3 e precedenti
ULR/Note	• https://support.zabbix.com/browse/ZBX-26986 • https://www.zabbix.com/security_advisories

PRODOTTO	DESCRIZIONE
Axios	Risolta una vulnerabilità con gravità "alta" in Axios. Tale vulnerabilità, qualora sfruttata, potrebbe permettere ad un utente malintenzionato remoto di compromettere la disponibilità del sistema target. **Prodotti e versioni affette** • Axios, versioni precedenti la 1.11.0
ULR/Note	• https://github.com/axios/axios/security/advisories/GHSA-4hjh-wcwx-xvwj

PRODOTTO	DESCRIZIONE
NVIDIA	Rilevate 3 nuove vulnerabilità, con gravità "alta", che riguardano il prodotto NVIDIA NVDebug. **Prodotti e/o versioni affette** • NVIDIA NVDebug, versioni precedenti alla 1.7.0
ULR/Note	• https://nvidia.custhelp.com/app/answers/detail/a_id/5696

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

DAL FURTO D'IMMAGINE AI DEEPFAKE: LA NUOVA FRONTIERA DELLA MANIPOLAZIONE DIGITALE

La manipolazione digitale sta evolvendo rapidamente e si sta trasformando in un fenomeno sempre più complesso e insidioso. Se in passato si parlava principalmente di furto e diffusione non autorizzata di immagini personali, oggi il rischio principale è rappresentato dai deepfake. Questa tecnologia consente di creare contenuti video e audio estremamente realistici, nei quali il volto o la voce di una persona vengono riprodotti artificialmente per inserirli in contesti falsi.

Le applicazioni criminali di questi strumenti spaziano da false sponsorizzazioni finanziarie a contenuti pornografici non consensuali, fino a sofisticate campagne di disinformazione. La criticità maggiore riguarda le persone comuni, che si trovano più esposte rispetto ai personaggi pubblici perché non hanno la stessa possibilità di difendersi o di far rimuovere rapidamente i contenuti manipolati.

Dal punto di vista normativo, gli strumenti attuali non risultano sufficienti a contrastare il fenomeno. È in discussione un aggiornamento legislativo che prevede nuove fattispecie di reato e aggravanti specifiche per l'uso improprio dell'intelligenza artificiale nella produzione di deepfake, ma il percorso è ancora agli inizi.

L'ITALIA TRA I GRANDI DEGLI SPYWARE: UN TERZO POSTO MONDIALE DIETRO ISRAELE E USA

Un recente report dell'Atlantic Council fotografa la crescita del mercato globale degli spyware, software capaci di monitorare e raccogliere informazioni sensibili da dispositivi compromessi. Secondo i dati, l'Italia si colloca al terzo posto a livello mondiale per numero di investitori coinvolti in questo settore, subito dopo Israele e Stati Uniti.

Questa posizione fa emergere un ruolo attivo del nostro Paese non solo come fruitore, ma anche come attore di rilievo in una filiera caratterizzata da intermediari, broker e rivenditori, spesso operanti in una zona grigia dal punto di vista etico e legale. Il rapporto evidenzia inoltre che la crescita del mercato non è legata esclusivamente alla scoperta autonoma di vulnerabilità da parte dei singoli attori, ma soprattutto alla capacità di acquistare exploit da altri soggetti e rivenderli o sfruttarli in modo strategico.
Si tratta di un quadro che solleva preoccupazioni in termini di sicurezza nazionale e di diritti umani, perché l'uso degli spyware, se non adeguatamente regolamentato, può facilmente degenerare in pratiche di sorveglianza abusiva o in attività di cyber spionaggio a danno di cittadini e istituzioni.

ANZIANI NEL MIRINO: LA NUOVA ONDATA DI TRUFFE INFORMATICHE

Le autorità statunitensi hanno lanciato un nuovo allarme riguardante le truffe informatiche mirate contro la popolazione anziana, un target sempre più sfruttato dai gruppi criminali. La dinamica della frode si basa su messaggi o avvisi che segnalano presunte minacce informatiche imminenti e invitano le vittime a contattare un numero di supporto tecnico. Da quel momento, gli aggressori inducono la persona a scaricare software malevoli che consentono l'accesso remoto al dispositivo.

In una seconda fase, i truffatori si spacciano per personale bancario e spingono la vittima a trasferire i propri risparmi su conti controllati dagli hacker o a convertirli in criptovalute. L'inganno sfrutta elementi psicologici come la paura, l'isolamento e la fiducia negli operatori di "assistenza", portando in breve tempo al prosciugamento dei risparmi di una vita.

Le raccomandazioni diffuse dalle autorità invitano a diffidare dei link sospetti, a non installare programmi su richiesta di sconosciuti e a verificare sempre tramite canali ufficiali l'autenticità di eventuali comunicazioni ricevute.

PATCH DI SICUREZZA SAMSUNG SETTEMBRE 2025: CORRETTA UNA VULNERABILITÀ CRITICA

Samsung ha reso disponibile il bollettino di sicurezza di settembre 2025, che introduce correzioni a 25 vulnerabilità ed esposizioni (SVE) individuate nei propri dispositivi. Tra queste spicca una vulnerabilità classificata come critica, già oggetto di sfruttamento attivo da parte degli attaccanti. Si tratta della CVE-2025-21043, un bug di scrittura fuori dai limiti presente nella libreria libimagecodec, che potrebbe consentire l'esecuzione di codice remoto.

Il problema interessa in particolare i dispositivi con sistema operativo Android nelle versioni comprese tra la 13 e la 16, e viene considerato ad alto rischio per la diffusione e la possibilità di sfruttamento in attacchi reali.

Il rilascio della patch sottolinea l'importanza di mantenere costantemente aggiornati i propri dispositivi, poiché le vulnerabilità critiche possono rappresentare un vettore privilegiato per attività malevole. Samsung raccomanda a tutti gli utenti di procedere senza ritardi all'installazione dell'aggiornamento.

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 8 – 14 Settembre 2025

Settimana caratterizzata da un picco molto alto di vulnerabilità critiche il 9 settembre con advisories di SAP, Siemens, Microsoft e Adobe, che hanno impattato soprattutto ambienti enterprise ed ICS.
Oltre a questi, continuano a emergere SQLi su applicativi open-source PHP (PHPGurukul, Student System, CRM) e vulnerabilità gravi su WordPress plugin e temi.
La presenza di PoC pubblici per varie SQL injection rende l'impatto immediato.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE	Data Pubblicazione	Severità	Exploit	Descrizione Sintetica	Prodotto Coinvolto
CVE-2025-10112	09/09/2025	CRITICAL (9.8)	✅	SQL Injection via department/index.php	Student Information Management System 1.0
CVE-2025-10113	09/09/2025	CRITICAL (9.8)	✅	SQL Injection via room/index.php	Student Information Management System 1.0
CVE-2025-10114	09/09/2025	CRITICAL (9.8)	✅	SQL Injection su profile.php	Small CRM 4.0 (PHPGurukul)
CVE-2025-10118	09/09/2025	CRITICAL (9.8)	✅	SQL Injection su login.php	E-Logbook Health Monitoring 1.0

CVE-2025-42922	09/09/2025	CRITICAL (9.9)	❌	File upload arbitrario → RCE	SAP NetWeaver AS Java
CVE-2025-42944	09/09/2025	CRITICAL (10.0)	❌	Deserialization via RMI-P4 → RCE	SAP NetWeaver
CVE-2025-42958	09/09/2025	CRITICAL (9.1)	❌	Missing auth check → data access & privilege abuse	SAP NetWeaver IBM i-series
CVE-2025-10134	09/09/2025	CRITICAL (9.1)	❌	Arbitrary file deletion (wp-config.php rischio RCE)	Goza Charity WP Theme
CVE-2025-40795	09/09/2025	CRITICAL (9.8)	❌	Buffer overflow in UMC	Siemens SIMATIC PCS neo & UMC
CVE-2025-40804	09/09/2025	CRITICAL (9.1)	❌	Network share exposed senza auth	Siemens SIMATIC SIVaaS
CVE-2025-54261	09/09/2025	CRITICAL (10.0)	❌	Path Traversal → RCE	Adobe ColdFusion (2021–2025)
CVE-2025-55232	09/09/2025	CRITICAL (9.8)	❌	Deserialization → RCE	Microsoft HPC Pack
CVE-2025-55234	09/09/2025	CRITICAL (9.8)	❌	SMB Relay → Privilege escalation	Microsoft Windows (10, 11, Server)
CVE-2025-8570	11/09/2025	CRITICAL (9.8)	❌	JWT secret exposure → Privilege Escalation	WordPress BeyondCart Connector

CVE-2025-40687	11/09/2025	CRITICAL (9.8)	❌	SQLi su add-team.php	PHPGurukul Online Fire Reporting v1.2
CVE-2025-40689	11/09/2025	CRITICAL (9.8)	❌	SQLi su request-details.php	PHPGurukul Online Fire Reporting v1.2
CVE-2025-40690	11/09/2025	CRITICAL (9.8)	❌	SQLi su edit-team.php	PHPGurukul Online Fire Reporting v1.2

Distribuzione Giornaliera

- **9 settembre 2025** → giornata con il maggior numero di advisory:
  - **SAP NetWeaver** (deserialization, file upload, privilege escalation)
  - **Siemens SIMATIC** (buffer overflow, esposizione condivisioni)
  - **Adobe ColdFusion** (path traversal → RCE critico)
  - **Microsoft Windows & HPC Pack** (SMB relay e deserialization RCE)
  - Diversi CMS open-source con SQLi già corredati di exploit pubblici
- **11 settembre 2025** → nuove disclosure per WordPress BeyondCart Connector e PHPGurukul Fire Reporting v1.2 (SQLi multiple).

Vendor e Tecnologie Coinvolti

- **SAP** → NetWeaver AS Java, IBM i-series → RCE e escalation di privilegi.
- **Siemens** → SIMATIC PCS neo, SIVaaS → vulnerabilità ICS ad alto rischio.
- **Microsoft** → HPC Pack, Windows 10/11/Server (SMB relay, deserialization).
- **Adobe** → ColdFusion (2021–2025), path traversal con exploit probabile.
- **WordPress** → BeyondCart Connector e Goza Charity Theme → escalation e file deletion.
- **PHPGurukul / Student Information Mgmt / CRM** → SQL injection diffuse con PoC pubblici.

Raccomandazioni Operative

Patch Prioritarie

- **SAP, Siemens, Adobe, Microsoft** → aggiornare immediatamente, soprattutto ColdFusion e Windows SMB relay.
- **WordPress e temi vulnerabili** → disabilitare plugin/temi finché non disponibili patch.
- **Applicativi PHP open-source (PHPGurukul, CRM, Student System)** → alto rischio di exploit immediato, patch/rimozione consigliata.

Mitigazioni e Monitoraggio

- **Database** → monitorare query anomale verso tabelle users, login, profile.
- **Web server** → WAF con regole anti-SQLi e traversal.
- **ICS/ERP** → segmentazione rete, accessi minimi, audit di sicurezza post-patch.
- **SIEM** → correlazioni su login.php, wp-config.php, profile.php, richieste verso ColdFusion.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-21692	Linux Kernel	7.8
CVE-2025-32756	FortiVoice, FortiRecorder, FortiMail, FortiNDR, FortiCamera	N/A
CVE-2025-1055	K7 Security Anti-Malware	N/A
CVE-2024-7344	Howyar UEFI Application "Reloader"	8.2
CVE-2025-54906	Microsoft Office	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-2025-9994	Amp'ed RF BT-AP 111 (Access point Bluetooth)	N/A
VULNERABILITÀ	L'interfaccia di amministrazione HTTP del Bluetooth access point BT-AP 111 prodotto da Amp'ed RF non dispone di un sistema di autenticazione, consentendo l'accesso non autorizzato a chiunque abbia accesso alla rete.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-9943	Shibboleth Service Provider	N/A
VULNERABILITÀ	È stata identificata una vulnerabilità di SQL injection nell'attributo "ID" della risposta SAML quando la replay cache del Shibboleth Service Provider (SP) è configurata per utilizzare un database SQL come servizio di storage. Un attaccante non autenticato può sfruttare la vulnerabilità tramite una blind SQL injection, consentendo l'estrazione di dati arbitrari dal database, se la connessione al database è configurata usando il plugin ODBC. La vulnerabilità deriva dalla mancanza di un'adeguata gestione degli apici singoli (') nella classe SQLString nel file odbc-store.cpp (righe 253-271).	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-58462	OPEXUS FOIAXpress Public Access Link (PAL)	N/A
VULNERABILITÀ	OPEXUS FOIAXpress Public Access Link (PAL), nelle versioni precedenti alla 11.13.1.0, è vulnerabile a una SQL injection attraverso la pagina SearchPopularDocs.aspx. Un attaccante remoto e non autenticato potrebbe leggere, scrivere o cancellare qualsiasi contenuto nel database sottostante.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-55234	Microsoft SMB Server	9.8
VULNERABILITÀ	CVE-2025-55234 riguarda una vulnerabilità del Microsoft SMB Server, che può essere soggetto ad attacchi di tipo relay, a seconda della configurazione. Un attaccante non autenticato potrebbe sfruttare questa debolezza per eseguire attacchi di elevazione dei privilegi. Anche se il server SMB supporta già meccanismi di protezione come la firma SMB e l'Extended Protection for Authentication (EPA), Microsoft ha pubblicato questo CVE per permettere ai clienti di valutare i propri ambienti tramite funzionalità di audit introdotte con gli aggiornamenti di sicurezza di settembre 2025, prima di applicare misure di hardening. È consigliato attivare queste protezioni per mitigare il rischio.	

3.4 CVE attualmente utilizzate in attacchi

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

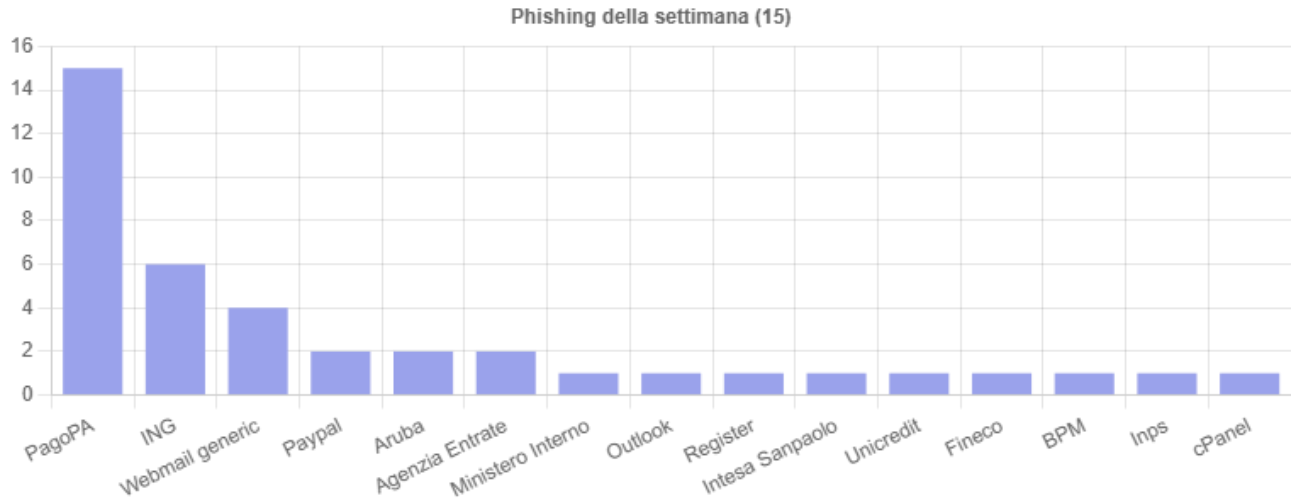
CVE	CVE-2025-5086
DESCRIZIONE	
CVE-2025-58462 riguarda una vulnerabilità di tipo SQL injection nel componente Public Access Link (PAL) del software OPEXUS FOIAXpress, presente nelle versioni precedenti alla 11.13.1.0. La falla si trova nella pagina SearchPopularDocs.aspx e consente a un attaccante remoto non autenticato di inviare comandi SQL malevoli al database sottostante. Questo può permettere di leggere, modificare o cancellare dati sensibili, compromettendo completamente il sistema. FOIAXpress PAL è il portale web utilizzato da enti pubblici per la gestione delle richieste FOIA e l'accesso pubblico ai documenti. La vulnerabilità espone a gravi rischi per la sicurezza dei dati e può essere mitigata aggiornando alla versione 11.13.1.0 o superiore.	

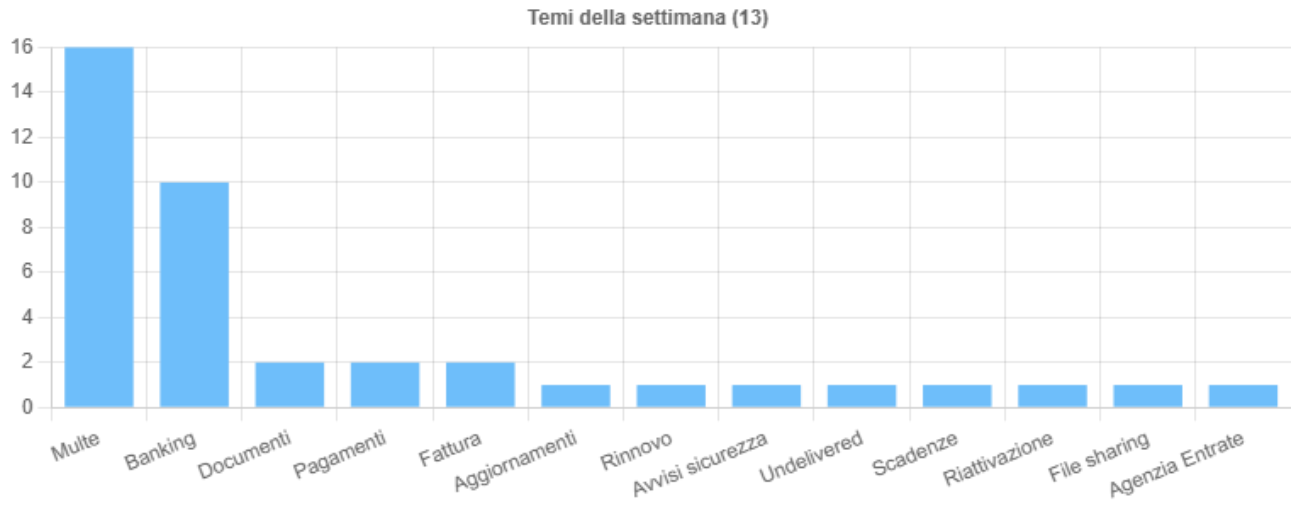
4 Attacchi

4.1 Phishing

Situazione italiana:

Nelle tabelle seguenti vengono riportate in sintesi le distribuzioni del numero di mail di phishing rilevate la settimana in oggetto suddivise per vari parametri quali mittente e area tematica.

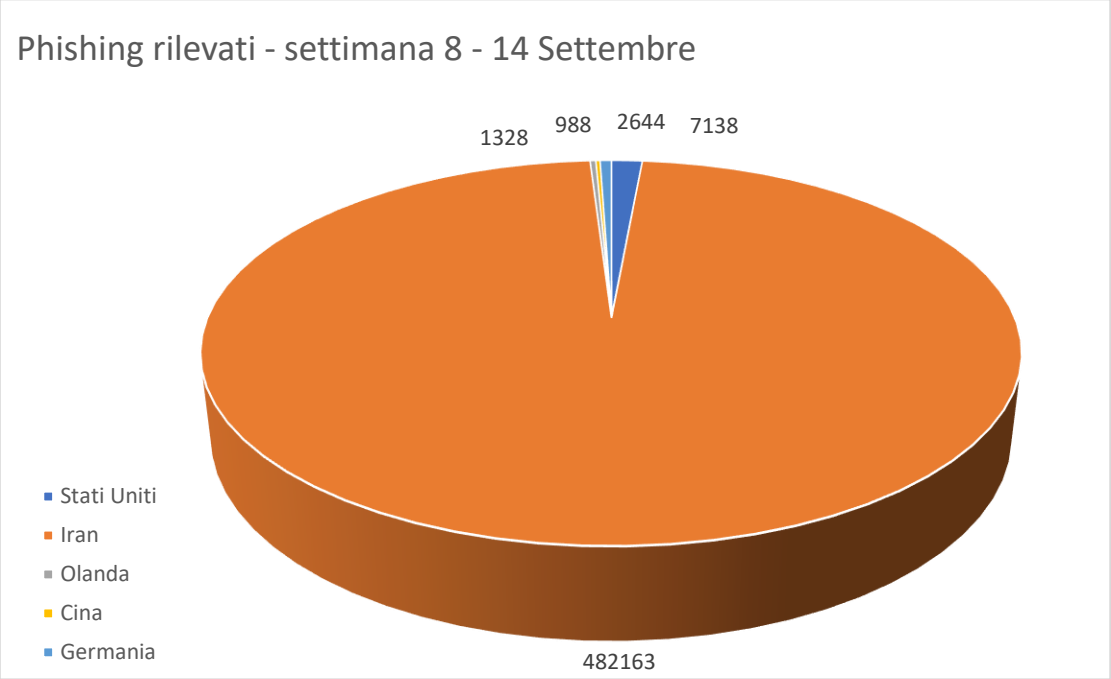




Fonte :CERT-AGID

Situazione Mondiale:

Nel seguente grafico troviamo la distribuzione dei primi cinque paesi di provenienza, per quanto riguarda il numero di email rilevate come attacchi di phishing sui sistemi honeypot.



Report di Analisi CTI – Email di Phishing

- Premessa

L'analisi è stata condotta sulla email sospetta ricevuta dall'indirizzo <postmaster@dbe75ae91a.nxcli[.]io > con oggetto "Notifica di accesso al tuo account – dispositivo riconosciuto". La mail si presenta come proveniente da PayPal, ma contiene indicatori tipici di un tentativo di phishing.
Il messaggio mira a indurre la vittima a cliccare un link esterno (https[:]//dove.tamatos[.]com/xxx.php) per "gestire la sicurezza". La struttura HTML replica elementi grafici di PayPal, ma mittente, domini e link di atterraggio non sono PayPal. Le intestazioni mostrano generazione via PHP su host nxcli/Nexcess e DKIM rsa-sha1 (obsoleto) firmato dal sottodominio mittente, non dal brand impersonato.

- Analisi Header

  Dall'analisi delle intestazioni emerge:

  - Return-Path / From: postmaster@dbe75ae91a.nxcli[.]io → dominio nxcli[.]io non riconducibile a PayPal.
  - Received: instradamento attraverso host cloudhost-1457566.us-midwest-1.nxcli[.]net [8[.]29[.]157[.]227].
  - SPF/DKIM/DMARC:

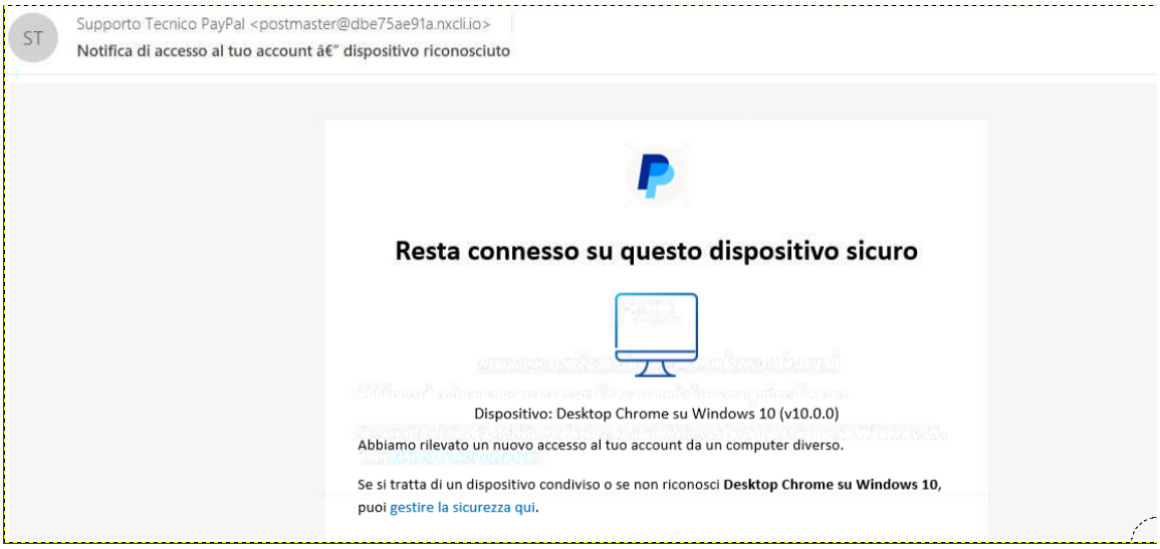
DKIM presente ma firmato con dominio dbe75ae91a.nxcli[.]io , non PayPal.
SPF/DMARC non allineati con il dominio PayPal.
X-PHP-Originating-Script: indica che il messaggio è stato generato da script PHP (xpx.php) su server compromesso/abusato.

- Analisi del Dominio Mittente
  - Dominio: dbe75ae91a.nxcli[.]io
  - WHOIS: sottodominio legato a nxcli[.]io , provider di hosting (likely Nexcess / Liquid Web).
  - Data di creazione: recente, pattern randomico (dbe75ae91a) tipico di domini malevoli o sottodomini dinamici.
  - Hosting e geolocalizzazione: server su rete USA (IP 8[.]29[.]157[.]227).
  - Reputazione: query su VirusTotal, PhishTank e AbuseIPDB riportano attività sospette legate a domini simili *.nxcli[.]io .
- Analisi URL malevolo

  Nel corpo della mail è presente un link fraudolento:
  https://dove.tamatos[.]com/xxx.php
  - Dominio: tamatos[.]com (non legato a PayPal).
  - Hosting/GeoIP: dominio registrato di recente, non associato a brand noti.
  - VirusTotal: segnalazioni di phishing.
  - PhishTank: indicatori presenti per sottodomini correlati.
- Analisi del Certificato SSL/TLS

  Il link porta a tamatos[.]com → certificato SSL valido ma emesso per dominio generico, non PayPal.
  Uso tipico dei phisher: certificati Let's Encrypt per dare parvenza di legittimità.
- Struttura e Contenuto della Email
  - Tecnica di ingegneria sociale: impersonificazione di PayPal.
  - Elementi grafici: logo e immagini ufficiali di PayPal caricati da paypalobjects.com per aumentare la credibilità.
  - Richiesta d'azione: cliccare su link per "gestire la sicurezza", con forte leva psicologica ("nuovo accesso rilevato").
  - Incongruenza: PayPal non invia notifiche senza riportare nome e cognome dell'utente → in questa mail è assente.

- Evidenze Visive



Screenshot (con dati vittima oscurati):

- Indicatori di Compromissione (IoC)

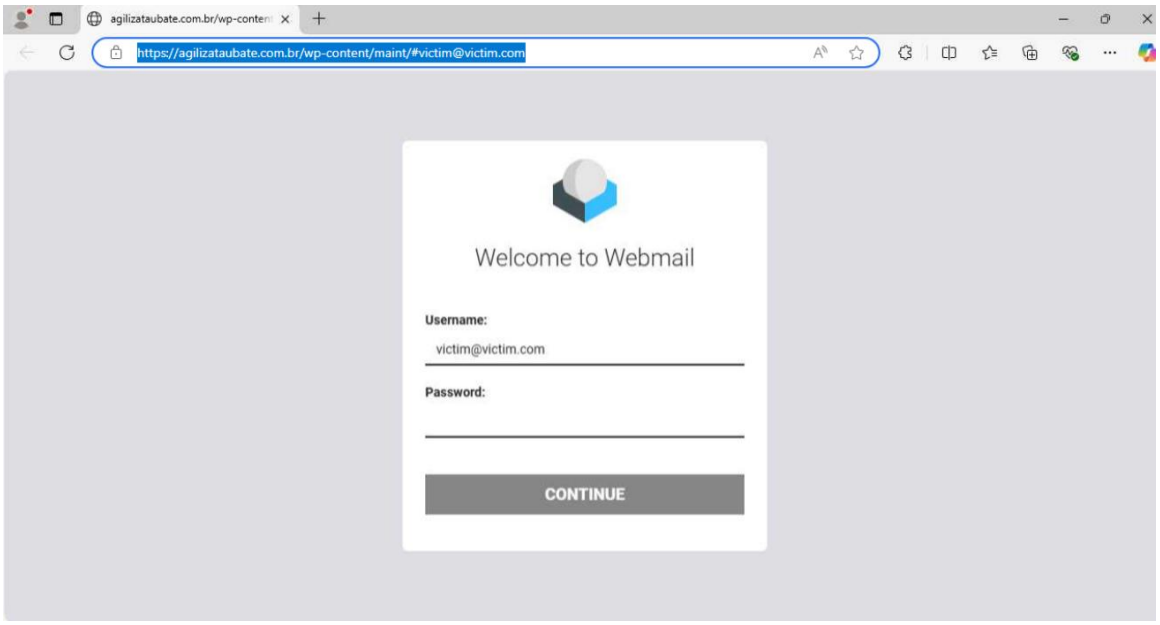
Tipo	Valore
Mittente	postmaster@dbe75ae91a.nxcli[.]io
Dominio fraudolento	dbe75ae91a.nxcli[.]io
IP sorgente	8[.]29[.]157[.]227
URL phishing	https://dove.tamatos[.]com/xxx.php
Dominio phishing	tamatos[.]com
Script generante	xpx.php su nxcli.net

- Riepilogo Risultanze

  L'email è un chiaro esempio di phishing mirato a carpire credenziali PayPal.
  Utilizza server compromessi/hosting abusati (nxcli[.]io) per l'invio.
  Inserisce link esterni (tamatos[.]com) per reindirizzare l'utente a un sito di raccolta credenziali.
  Firma DKIM e intestazioni non corrispondono a PayPal.
  Uso di ingegneria sociale con allarme sicurezza ("accesso sconosciuto") per indurre al click.

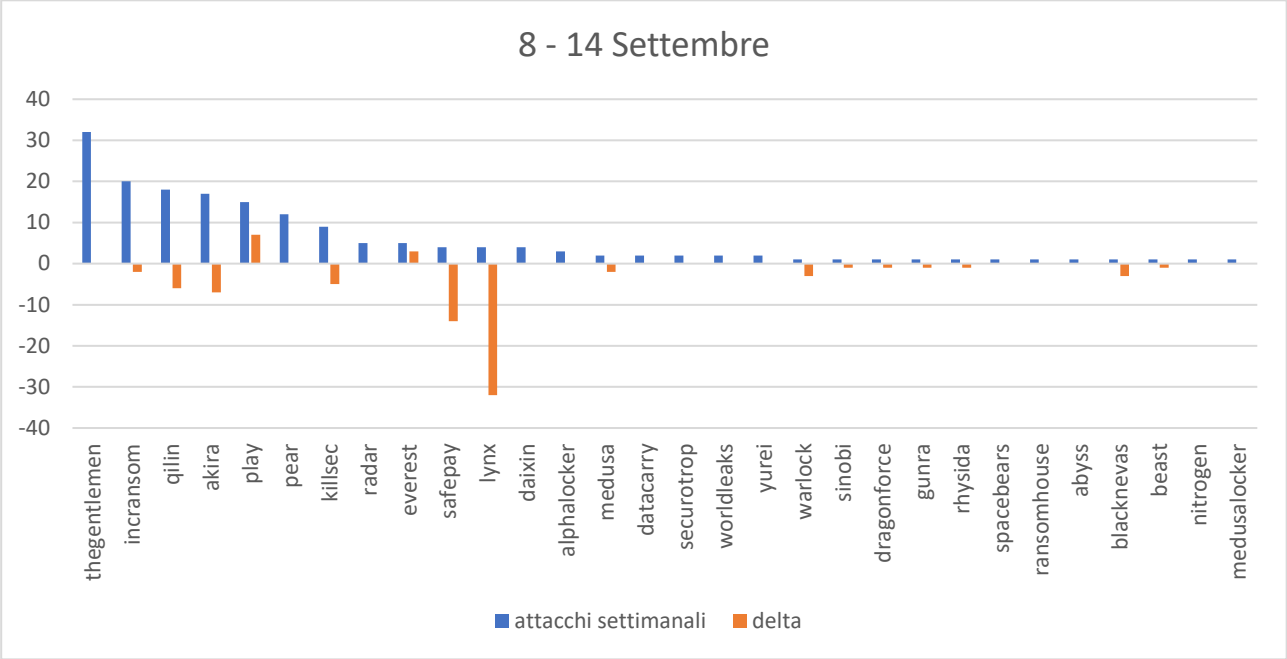
- Conclusione: Email fraudolenta. Si raccomanda il blocco immediato dei domini/IP segnalati e la segnalazione a PayPal Security e PhishTank.

Di seguito lo screenshot della pagina fake richiamata dalla url nella email.

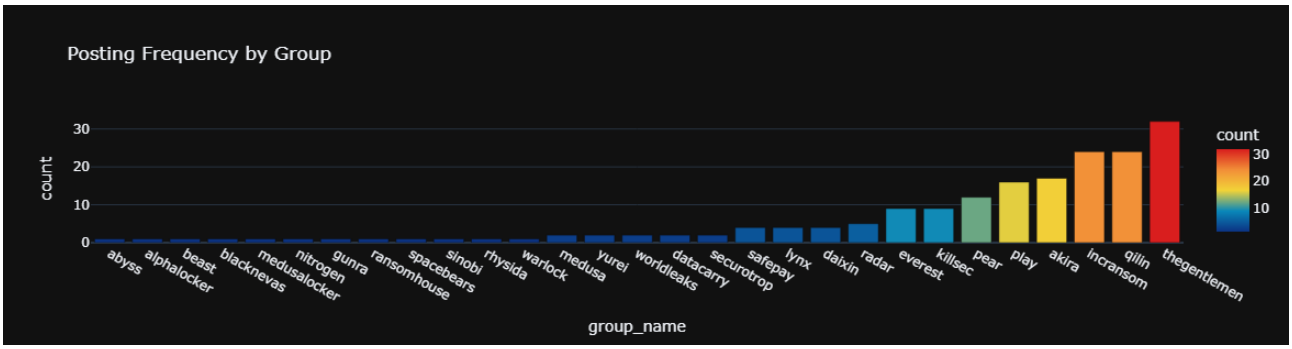

agilizataubate.com.br/wp-conten
https://agilizataubate.com.br/wp-content/maint/#victim@victim.com
Welcome to Webmail
Username:
victim@victim.com
Password:
CONTINUE

4.2 Ransomware

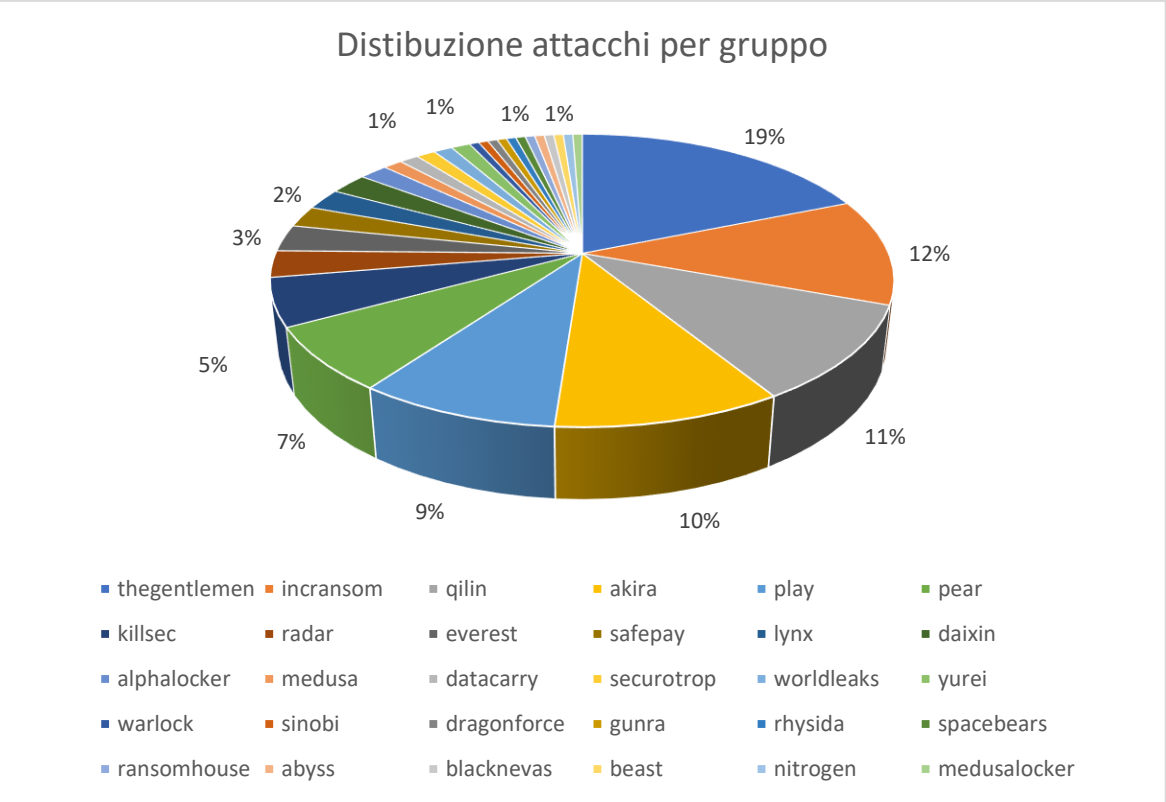
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (8 - 14 Settembre). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

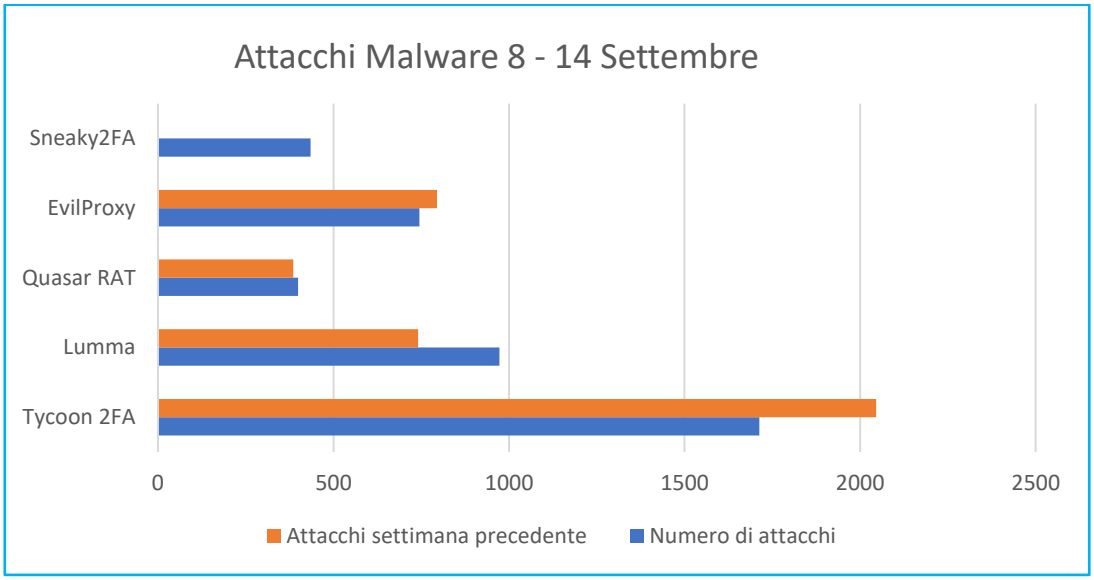


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:


Distibuzione attacchi per gruppo
19%
12%
11%
10%
9%
7%
5%
3%
2%
1%
1%
1%
1%
thegentlemen
incransom
qilin
akira
play
pear
killsec
radar
everest
safepay
lynx
daixin
alphalocker
medusa
datacarry
securotrop
worldleaks
yurei
warlock
sinobi
dragonforce
gunra
rhysida
spacebears
ransomhouse
abyss
blacknevas
beast
nitrogen
medusalocker

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

- **Tycoon 2FA**

Tycoon 2FA è un kit di phishing Adversary-in-the-Middle (AiTM) offerto come Phishing-as-a-Service (PhaaS) dal 2023 e aggiornato fino al 2025. Vettori tipici sono email mirate e QR code che reindirizzano le vittime; talvolta tramite servizi legittimi compromessi (es. Milanote);verso pagine di login contraffatte molto simili a Microsoft 365 o Gmail.

Le pagine usano CAPTCHA evoluti (da Cloudflare Turnstile a soluzioni HTML5 canvas custom), controlli ambientali (IP, user-agent, fingerprinting) e offuscamento JavaScript/HTML per filtrare bot e analisi automatizzate; questo permette al kit di rimanere attivo più a lungo e di eludere molte difese basate su firme.

Tecnicamente Tycoon 2FA opera come reverse-proxy: quando la vittima inserisce credenziali e codice MFA, il proxy rilaya le richieste al servizio autentico e cattura in tempo reale i cookie di sessione validi, che gli attaccanti riutilizzano per ottenere accesso persistente senza bisogno del secondo fattore. L'effetto pratico è il takeover di account cloud aziendali, furto di email/documenti, impostazione di regole di forwarding e potenziale pivot verso frodi finanziarie o ransomware, per questo motivo rappresenta una minaccia critica per organizzazioni cloud-centric.

IoC:

Tipo	Indicatore
Dominio	httpx://dkrl[.]idrvlqvkov[.]es/dGeau/
Dominio	lrn[.]ialeahed[.]com

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing	Invio di email di phishing (spesso da account legittimi compromessi) per indirizzare le vittime a pagine di login fasulle.
T1204	User Execution	Inserimento credenziali/MFA
T1539	Steal Web Session Cookie	Il kit cattura il cookie di sessione post-MFA della vittima e permette replay dell'accesso.

Contromisure:

- Email security: rafforzare i controlli sulle email in uscita interne (Monitoraggio anomalie su invio massivo o nuovi mittenti), usare SPF/DKIM/DMARC per ridurre compromessi.
- Rilevamento: utilizzare sistemi UEBA per individuare logins anomali (es. login da IP non previsti, device diversi, attività successive sospette). Integrare alert su creazione di regole di inbox o inoltri email non autorizzati.
- Autenticazione: adottare MFA resistenti al phishing (security key FIDO2, certificati hardware) e verificare via canale out-of-band (OOB) eventuali richieste di MFA sospette.

Livello di rischio: Alto.

- **Lumma**

Lumma Stealer è un infostealer (MaaS) scritto in C, emerso nel 2022 e divenuto uno dei più diffusi tool di data exfiltration. Viene venduto con abbonamenti su forum criminali. Secondo Europol, era il "più grande infostealer al mondo" con oltre 394.000 host Windows compromessi.

Il kit si propaga principalmente tramite malvertising (es. banner ingannevoli) e campagne email con allegati HTA o ZIP contenenti script PowerShell. Una recente operazione internazionale (Endgame 2) ha colpito pesantemente la sua infrastruttura. Nel 2025, HP Security Lab riporta che, nonostante il takedown di maggio, Lumma ha ripreso attività in Q2 2025, veicolato anche tramite allegati IMG (immagini) sofisticate.

Campagne recenti intercettate (per esempio da CIS negli USA) hanno mostrato falsi CAPTCHA che inducono l'utente a eseguire script PowerShell che scaricano e installano Lumma Stealer.

Lumma ruba credenziali di browser, portafogli crypto, dati finanziari, ecc., e viene spesso utilizzato in attacchi massivi "spray-and-pray" a reti aziendali e governative globalmente.

IoC:

Tipo	Indicatore
IPs	82[.]117[.]255[.]127 195[.]123[.]226[.]91 94[.]158[.]244[.]69 185[.]99[.]133[.]246
Domini	evoliutwoqm[.]shop millyscroqwp[.]shop caffegclasiqwp[.]shop locatedblsoqp[.]shop stamppreewntnq[.]shop empiredzmwnx[.]shop creepydxzoxmj[.]shop

URLs	httpx://topographky[.]top/xlak httpx://tropiscbs[.]live/iuwxx httpx://cartograhphy[.]top/ixau httpx://clarmodq[.]top/qoxo httpx://biosphxere[.]digital/tqoa httpx://geographys[.]run/eirq httpx//vigorbridgoe[.]top/banb

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing / Malvertising	Distribuzione tramite email-malvertising: vittime ingannate da CAPTCHAs falsi che eseguono script
T1059	Command-Line Interface	Esecuzione di script PowerShell malevoli (download e avvio di payload Lumma)

Contromisure:

- Prevenzione: bloccare l'esecuzione di script PowerShell esterni (Policy di AppLocker/Constrained-Language), disabilitare Mshta ove possibile. Filtrare email e navigatori contro pagine CAPTCHA sospette.
- Rilevamento: usare EDR/AV con firme per le routine MSHTA e Powershell sospette; basarsi su heuristics (es. script PS da URL sospette). Monitorare il traffico verso domini registrati recentemente che presentano comportamenti di redirect (come quelli fake CAPTCHA).
- Hardening: applicare aggiornamenti, utilizzare anti-exploit, isolare i browser e negare l'uso di macro non firmate.
- Ripristino: isolare host infetti, cancellare o congelare servizi legati (traffic distribution), forzare password/domain reset.

Livello di rischio: Alto. Lumma Stealer consente il furto massivo di dati (password, carte di credito, chiavi) e rimane attivamente diffuso in Europa e USA.

- **EvilProxy**

EvilProxy è un toolkit phishing di tipo AiTM (man-in-the-middle) venduto come servizio, che agisce da reverse-proxy fra l'utente vittima e il sito legittimo. Originariamente scoperto nel 2022, nelle campagne del 2023-2025 si è specializzato nell'inganno di login Microsoft/Google: genera pagine maligne identiche a quelle vere, inoltrando le richieste reali ma raccogliendo le credenziali e il cookie di sessione del bersaglio. Menlo Security descrive una campagna 2023 in cui EvilProxy sfruttava un open redirect (su indeed.com) per colpire executive del settore finance. EvilProxy "si mimetizza" perfettamente: ad esempio, la sorgente HTML della pagina di login clonata è quasi identica all'originale. L'attacco consente agli aggressori di superare la MFA semplicemente "rubando" la sessione dell'utente. EvilProxy è stato osservato in attacchi globali contro account aziendali dal 2023, spesso con obiettivi finanziari/aziendali.

IoC:

Tipo	Indicatore
Domini	evilginx2.phish-domain.example

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing / Malvertising	Invio di email di phishing (spesso da account legittimi compromessi) per indirizzare le vittime a pagine di login fasulle.
T1539	Steal Web Session Cookie	Il kit cattura il cookie di sessione post-MFA della vittima e permette replay dell'accesso.
T1078	Account validi	Uso di account email compromessi (autore legittimo) per spedire il phishing

Contromisure:

- Rilevamento: utilizzare soluzioni avanzate anti-phishing che ispezionano i URL in tempo reale; prestare attenzione a redirect sospetti (in particolare domini di terze parti inseriti all'interno di link legittimi). Monitorare pattern di login insoliti (per es. MFA richieste ripetute senza login effettivo).
- Blocchi proattivi: disabilitare o rendere non sfruttabili note vulnerabilità di open redirect (come quella di Indeed), e stringere filtri anti-redirect. Utilizzare policy DNS/firewall per bloccare interazioni note con server EvilProxy (es. IP/range associati a infrastrutture di phishing).
- MFA avanzata: adottare MFA phishing-resistant (FIDO2 security key, certificati) che non si basino su token inviati via browser.
- Educazione: avvisare gli utenti di verificare l'URL (anche se apparentemente legittimo, v. la presenza di caratteri sospetti o trigger di MFA insolitamente frequenti).

Livello di rischio: Alto.

- **Sneaky 2FA**

Sneaky 2FA è un kit phishing Adversary-in-The-Middle (AiTM) distribuito come PhaaS (Phishing-as-a-Service) da una gang denominata "Sneaky Log". Scoperto da TDR Sekoia a fine 2024, il kit mima perfettamente le pagine di login Microsoft 365, riempendo automaticamente il campo utente con l'email della vittima (funzionalità autograb), e include CAPTCHA anti-bot per evitare analisi automatizzate.

In pratica, la vittima clicca un link email, viene reindirizzata a una pagina malevola (es. secure.toitoiiusa[.]com) che replica la login di Microsoft; durante il login 2FA, il kit "EvilProxy-style" intercetta il token e cattura il cookie di sessione al posto dell'utente. L'intera infrastruttura è venduta via Telegram (bot SneakyLog) e adotta domini compromessi o registrati ad hoc. Campagne di Sneaky 2FA hanno colpito globalmente dagli ultimi mesi 2024; tecnicamente indistinguibile dal login legittimo

IoC:

Tipo	Indicatore
IPs	101.99.92[.]124 *(Server operator SneakyLog (C2, hosting kit))*
Domini	sneakylog[.]store mysilverfox[.]com.my secure[.]toitoiiusa[.]com

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566.001	Phishing: Spearphishing Attachment	Distribuzione tramite email mirate: link malevoli che rimandano a pagine fasulle di login Office365.
T1539	Steal Web Session Cookie	Il kit intercetta il cookie di sessione post-MFA della vittima, consentendo all'attaccante di accedere al suo account senza la password second factor
T1114	Email Collection	Eventuale scansione della casella email della vittima dopo compromesso, esfiltrando altre credenziali.

Contromisure:

- Rilevamento: implementare soluzioni anti-phishing avanzate con detezione di pattern AiTM (ad es. URL anomali di lunghezza >150 caratteri contenenti /verify, /index o /validate). Monitora i log di autenticazione: accessi da MACAddress/ip nuovi, attività sospetta dopo MFA (basarsi su UEBA).

- Filtro domain/IP: bloccare preventivamente i domini noti (vedi tabella IoC) e le IP associate al servizio. Aggiornare liste di reputazione (e.g. Sekoia Threat Intel feeds).
- MFA avanzata: passare a MFA resistenti al phishing (FIDO2, token hardware) che non possono essere aggirati dal furto di sessione.

Livello di rischio: Molto Alto (Sneaky 2FA permette agli attaccanti di superare la protezione 2FA standard e ottenere accesso completo a caselle di posta Office365)

- **Quasar RAT**

Quasar RAT è un noto remote access trojan open-source scritto in C#, usato sia per scopi legittimi (supporto remoto) che abusato da gruppi criminali e APT. La sua architettura prevede un client (droppato via allegati ingannevoli in email spear-phishing o false pagine di download) e un pannello di controllo server con interfaccia grafica. I criminali lo usano per esfiltrare dati e mantenere accessi persistenti. Secondo Darktrace, già alla fine del 2023 si osservavano campagne di Quasar che sfruttavano tecniche avanzate come il DLL sideloading per aggirare le difese

In una recente indagine, Cyberint evidenzia che Quasar RAT viene veicolato tramite campagne di phishing e drive-by download (infezioni via pagine web compromesse)

Quasar è stato riscontrato in campagne globali, incluse varianti in Europa, e resta un rischio per data breach e attacchi di furto credenziali.

IoC:

Tipo	Indicatore
IPs	*108[.]213[.]32[.]144* *146[.]190[.]110[.]91* *146[.]190[.]29[.]250* *217[.]195[.]197[.]132*
Domini	7[.]tcp[.]eu[.]ngrok[.]io 0[.]tcp[.]eu[.]ngrok[.]io 27[.]ip[.]gl[.]ply[.]gg

	games-travel[.]gl[.]at[.]ply[.]gg
URLs	tcp://6[.]tcp[.]eu[.]ngrok[.]io:10324/ https://gofile[.]io/d/v2kHnq:8080 http://18[.]134[.]234[.]207/update/ping http://18[.]134[.]234[.]207/update/error

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing (Spearphishing Email)	Invio di email di spear-phishing con allegati malevoli (PDF/Word che scaricano Quasar)
T1590	Raccolta info di rete	Analisi della rete interna, scan porte e DNS (usato da Quasar per profilare reti target)
T1078	Account validi	Uso di credenziali legittime rubate o account compromessi per mantenere accesso persistente

Contromisure:

- Prevenzione: bloccare alle email ingressanti macro e script sospetti; applicare policy di execution control su PowerShell o Mshta.
- Monitoring: deploy di soluzioni EDR/NDR per rilevare attività anomale (es. nuovi processi Quasar, collegamenti C2 su domini DDNS come quelli citati); controllare traffico SSL sospetto e DNS (es. portmap[.]io, gl.at.ply[.]gg).
- Signature: aggiornare antivirus/EDR con le ultime firme/IOC (hash e domini noti) per Quasar.

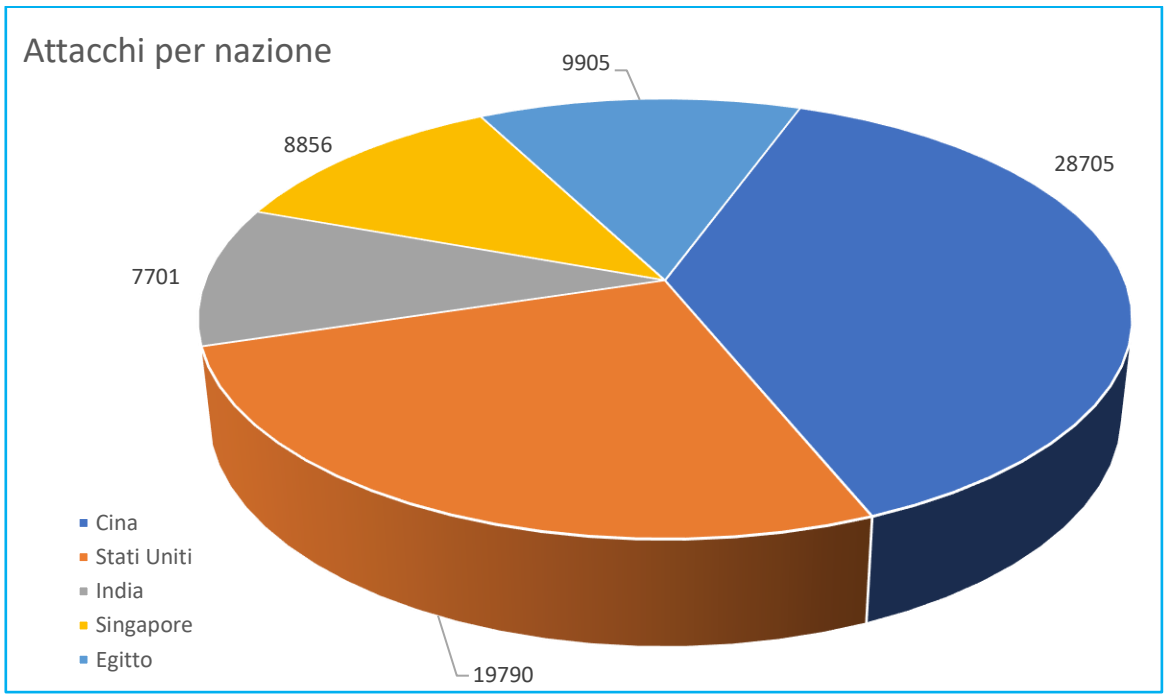
Livello di rischio: Alto (Quasar RAT consente controllo remoto totale delle macchine compromesse, facilitando spionaggio, furto di dati e movimenti laterali nella rete.).

Riepilogo:

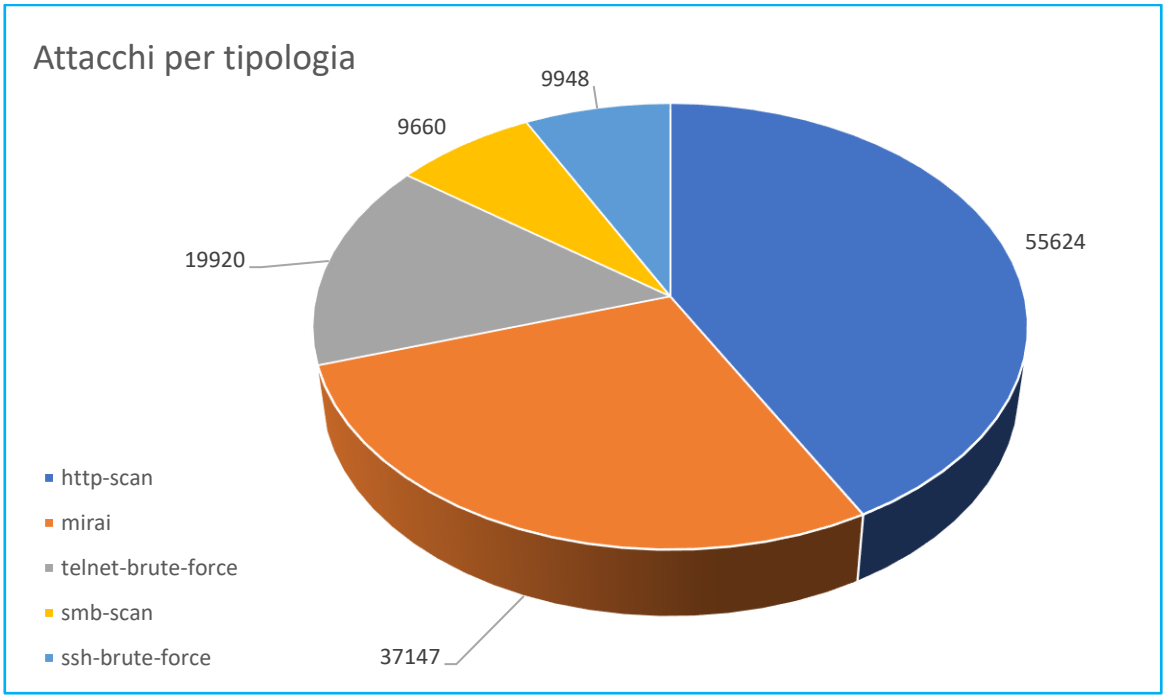
Malware	Categoria	Livello di rischio
Tycoon 2FA	Phishing AiTM Kit	Molto Alto
Lumma Stealer	Infostealer	Alto
EvilProxy	Phishing AiTM Kit	Alto
Sneaky 2FA	Phishing AiTM Kit	Molto Alto
Quasar RAT	Remote Access Trojan	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 8 – 14 Settembre, suddivisa per nazione e limitata alle prime cinque posizioni:

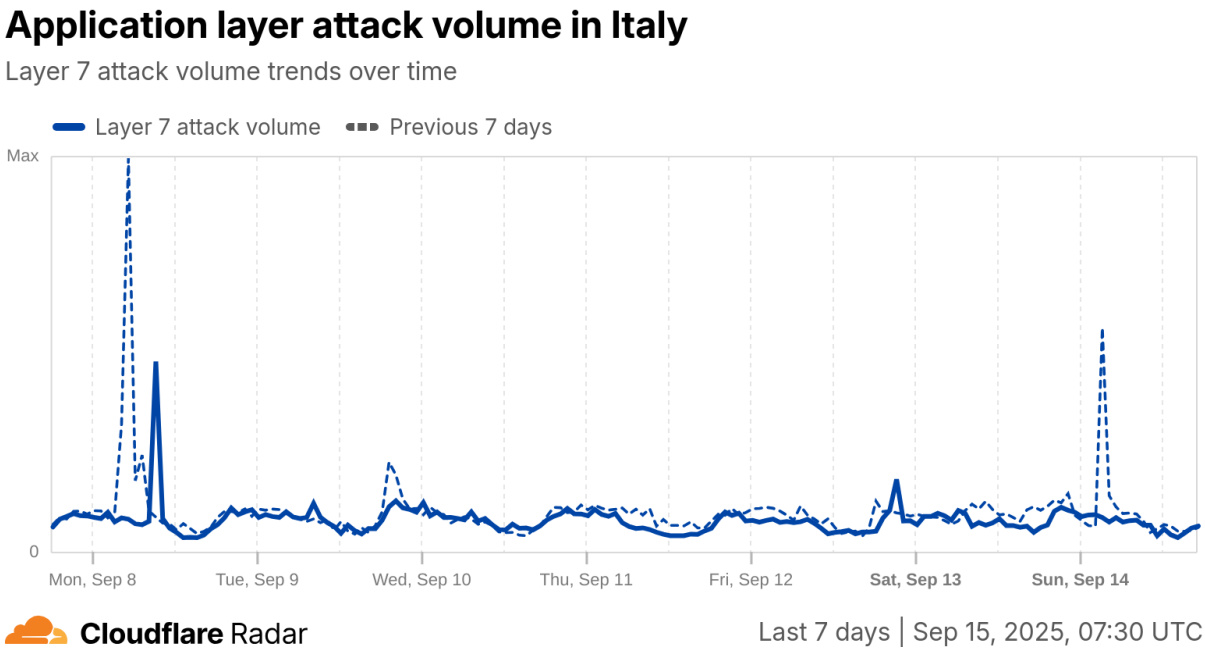


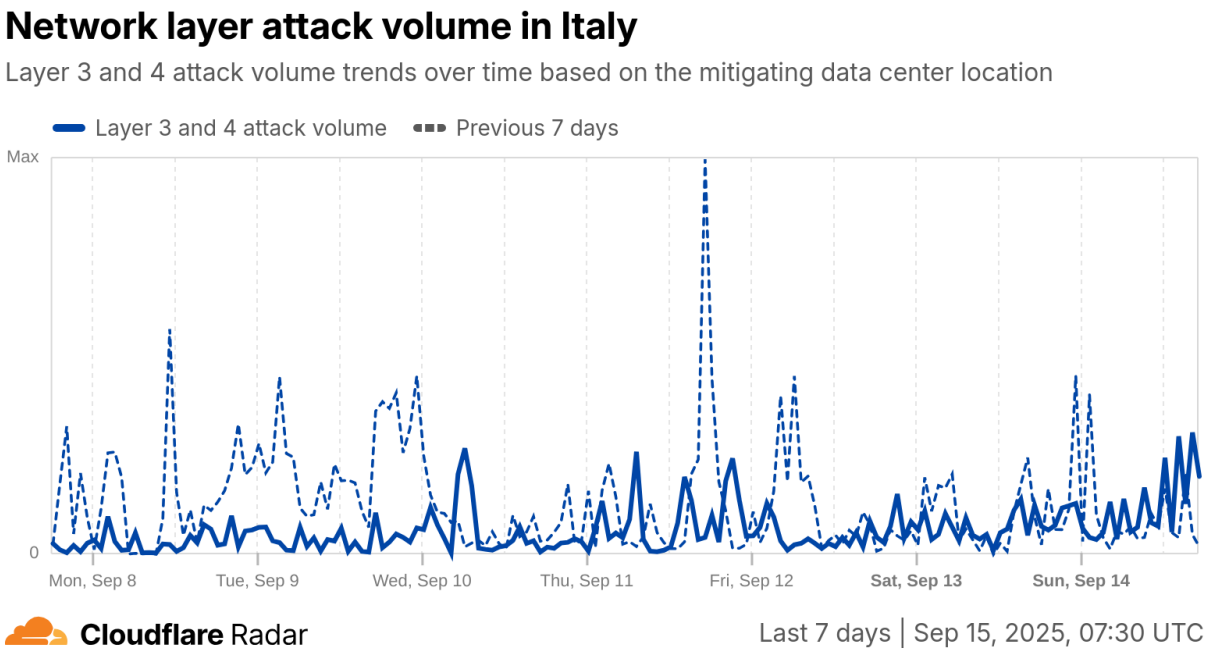
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
COMUNE DI FIRENZE	ITALIA
DESCRIZIONE	Un annuncio apparso su un forum underground ha destato allarme sulla possibile violazione dei dati del Comune di Firenze. Un utente con il nickname "krektti" ha messo in vendita, per 1.500 dollari, presunti accessi e database contenenti informazioni anagrafiche sensibili come codice fiscale, nome, cognome, data di nascita e indirizzi. L'annuncio, pubblicato pochi giorni fa, include campioni di dati strutturati che sembrano riferirsi ad un archivio anagrafico. Non ci sono ancora conferme ufficiali né smentite da parte del Comune o delle autorità.

TARGET	LOCALIZZAZIONE
MEF DI PANAMA	PANAMA (AMERICA CENTRALE)
DESCRIZIONE	Il Ministero dell'Economia e delle Finanze (MEF) di Panama ha segnalato un possibile attacco informatico che avrebbe coinvolto una singola postazione di lavoro, subito isolata secondo le procedure di sicurezza. Secondo il comunicato ufficiale, i sistemi principali e i dati sensibili sarebbero al sicuro. Tuttavia, la banda ransomware INC Ransom ha rivendicato l'attacco, dichiarando di aver sottratto oltre 1,5 TB di dati, tra cui email, documenti finanziari e di bilancio. Il gruppo ha pubblicato qualche giorno fa campioni dei presunti dati rubati sul dark web, inserendo il MEF nella lista delle sue vittime.

TARGET	LOCALIZZAZIONE
COMUNE DI CANEGRATE	ITALIA
DESCRIZIONE	Un annuncio comparso ieri su un forum underground segnala una possibile violazione ai danni del Comune di Canegrate (Milano). L'utente "krek1i", con buona reputazione nella community cybercriminale, afferma di possedere accessi e un database del Comune, messi in vendita per 500 dollari. A supporto, ha pubblicato sample di dati che includerebbero informazioni personali, credenziali di accesso e strutture di database con molte tabelle. Non ci sono ancora comunicazioni ufficiali da parte del Comune, quindi l'effettiva compromissione non è confermata.

4.6 Defacement

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

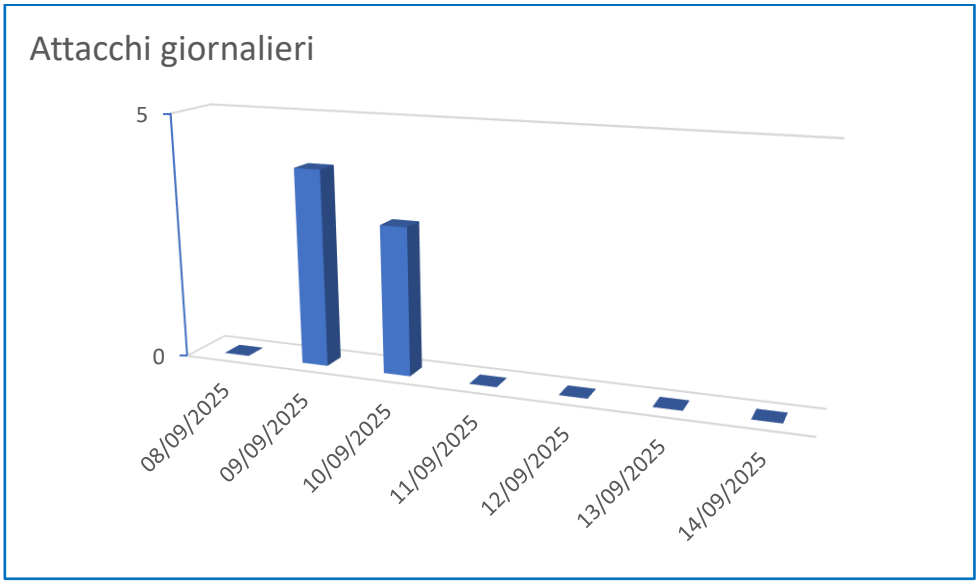


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

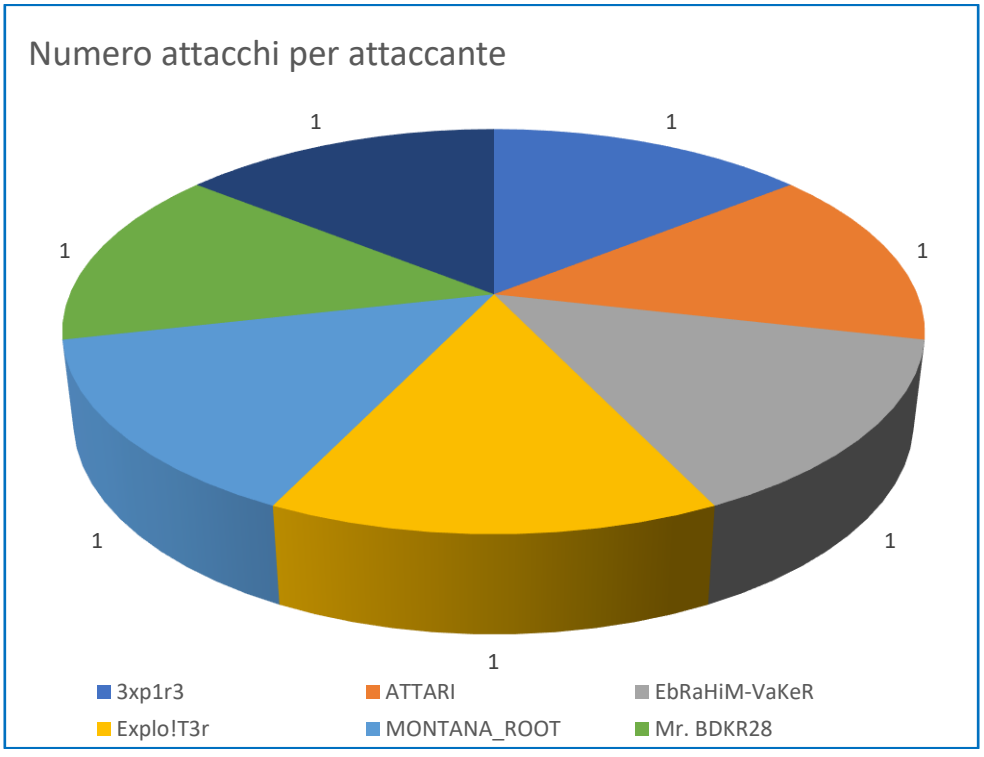


Figura 2: Defacement - Attaccanti più attivi nel periodo 8 – 14 Settembre

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.

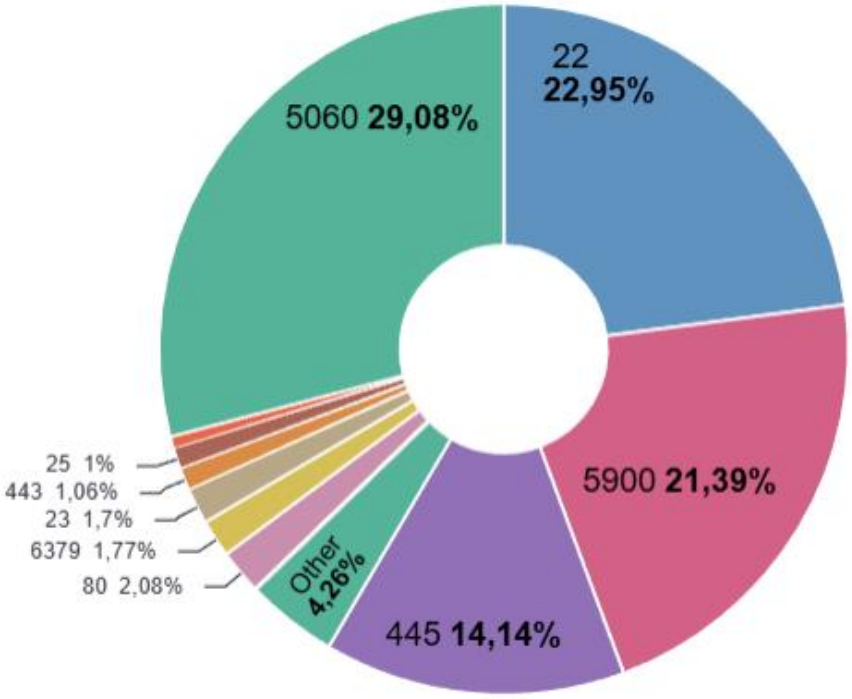
5.1 Attacchi Settimanali Honeypot S3K – Analisi generale

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

Questa invece la situazione a livello italiano, cioè considerando i soli honeypot presenti sul territorio italiano

5.1.1 Attacchi ai servizi

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



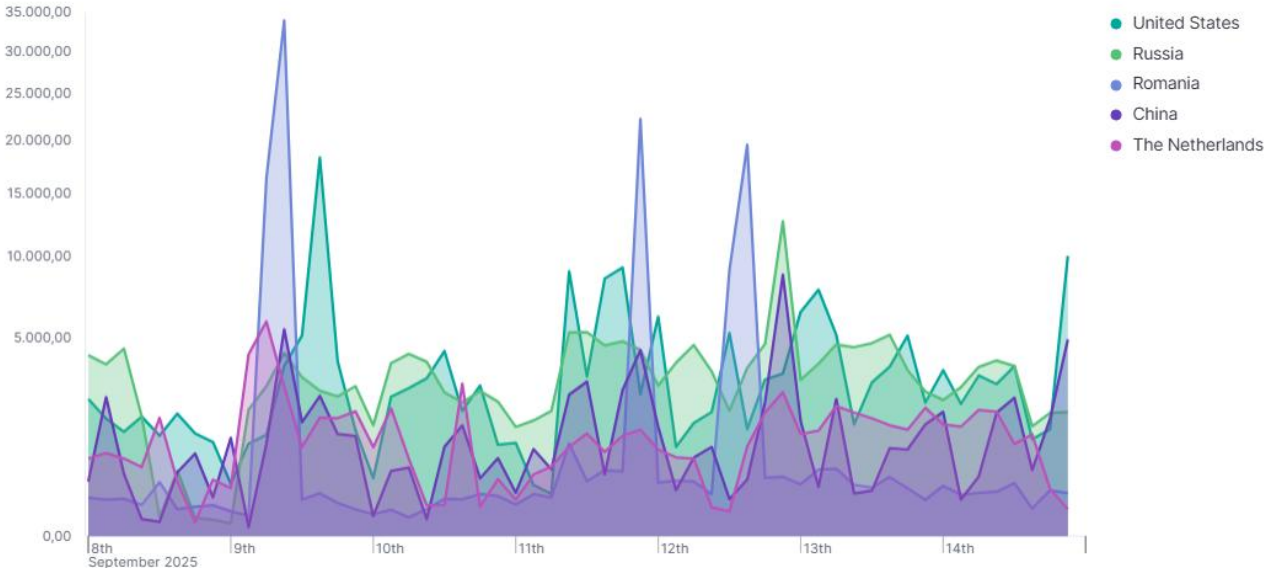
5.1.2 IP Attaccanti

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

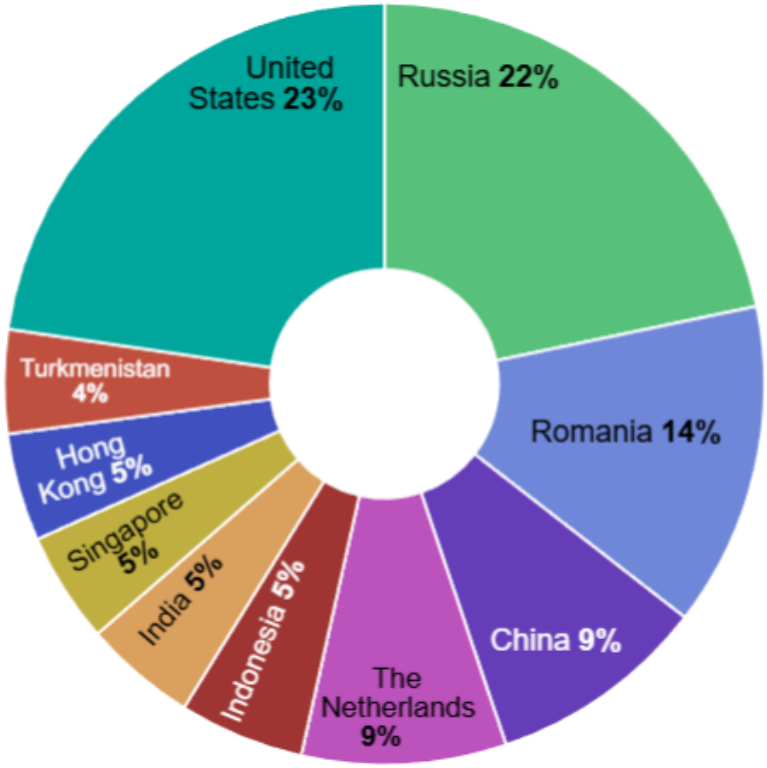
Source IP	Count
2.57.121.148	100.908
142.202.189.5	27.684
45.134.26.33	26.322
91.202.233.65	25.057
142.202.191.234	24.591
193.24.123.28	24.281
178.22.24.32	17.641
217.119.139.47	15.874
217.119.139.45	15.307
217.119.139.44	15.271

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:

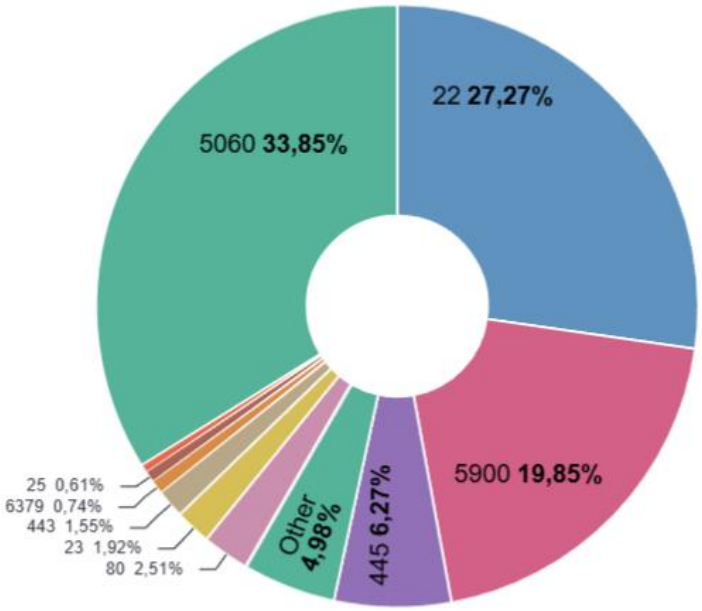


5.2 Italian Honeypot N.1

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
5060	37.041
22	29.838
5900	21.717
445	6.857
80	2.749
23	2.103
443	1.698
6379	808
25	672
3306	503

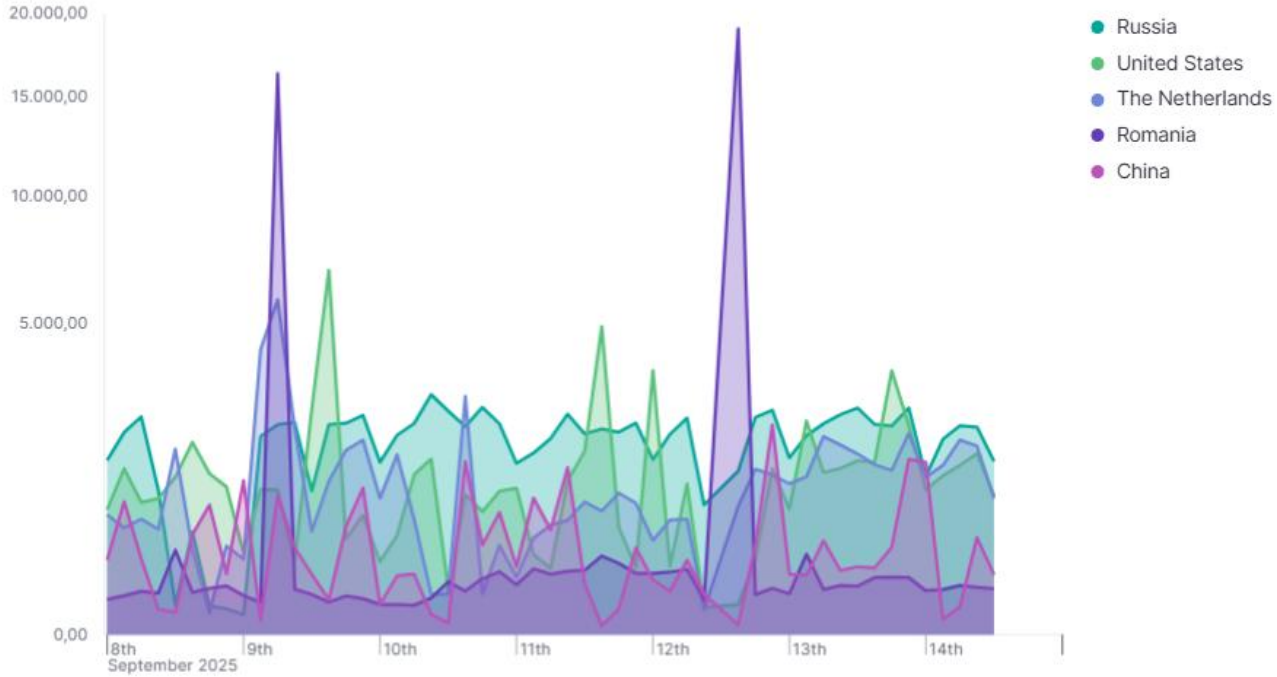
5.2.2 IP Attaccanti

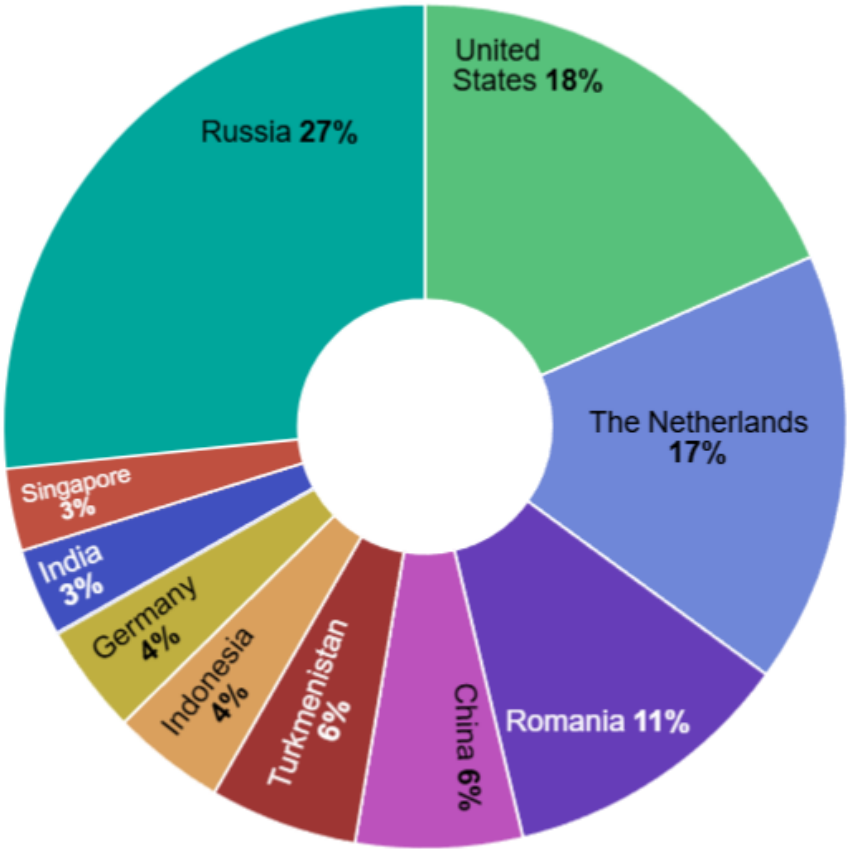
Questa invece la classifica relativa ai 10 IP che hanno effettuato il maggior numero di attacchi:

Source IP	Count
2.57.121.148	35.592
45.134.26.33	15.495
91.202.233.65	14.733
193.24.123.28	14.032
196.251.66.40	11.211
196.251.66.161	10.908
178.22.24.32	10.849
196.251.66.137	10.110
217.119.139.47	9.759
217.119.139.45	9.185

5.2.3 Paesi di provenienza degli attacchi

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



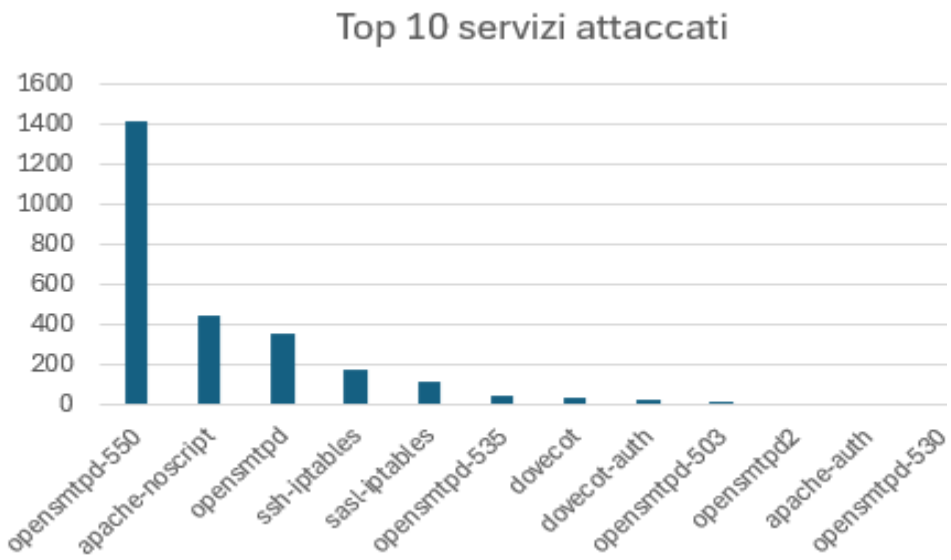

United States 18%
The Netherlands 17%
Romania 11%
China 6%
Turkmenistan 6%
Indonesia 4%
Germany 4%
India 3%
Singapore 3%
Russia 27%

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.



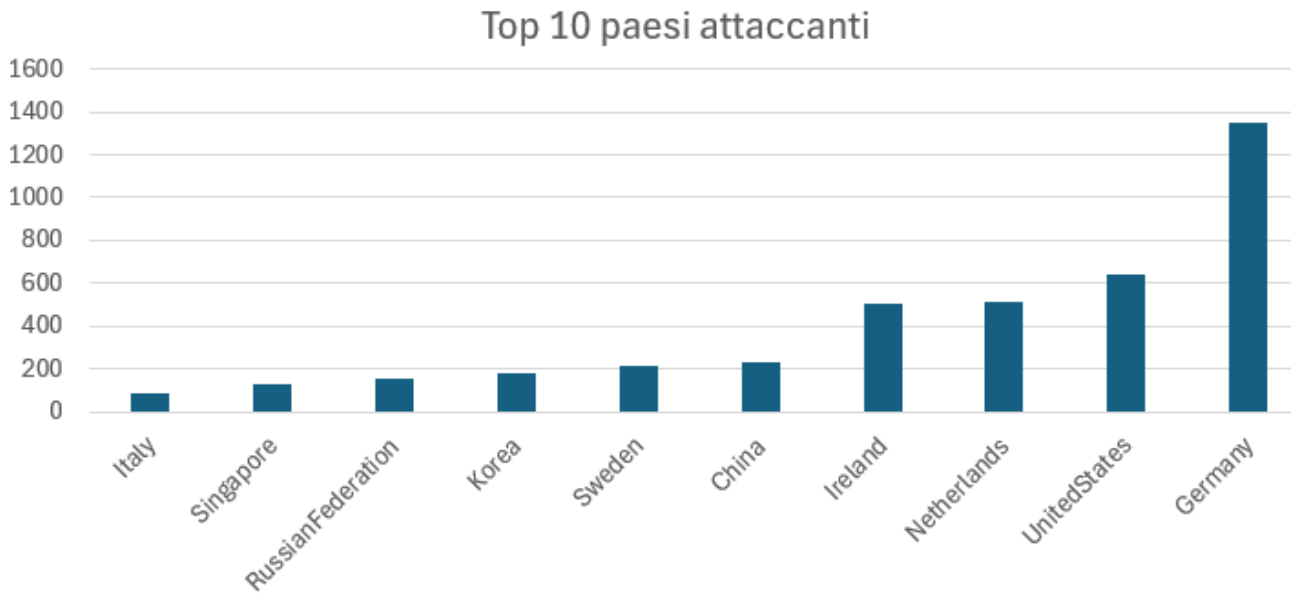
5.3.2 IP attaccanti

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
213[.]202[.]247[.]53	444
37[.]48[.]109[.]146	322
212[.]32[.]242[.]60	94
77[.]87[.]213[.]13	47
81[.]28[.]9[.]66	32
192[.]227[.]246[.]121	32
62[.]173[.]140[.]179	29
176[.]46[.]138[.]150	27
185[.]17[.]106[.]62	27
195[.]211[.]188[.]185	24

5.3.3 Paesi di provenienza degli attacchi

Questa invece la distribuzione dei paesi attaccanti:



6 Company Profile S3K

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

COME LO FACCIAMO:

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

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

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

CON QUALI LEVE OPERIAMO:

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

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

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

CHI SIAMO:

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

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

LA NOSTRA MISSION:

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

I NOSTRI VALORI:

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

CONTATTI:

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

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

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

Cyber security

RISK REPORT

S3K

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

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