S3K

Cyber security

RISK REPORT

\ week 15.09.2025 - 21.09.2025

Sommario

1 Il Cyber Security Risk Report S3K 5

1.1 Bollettino di Sicurezza Informatica 5

1.2 Aggiornamenti di Sicurezza e Vulnerabilità Critiche 5

1.3 CVE Monitor - Tendenze Settimanali 5

1.4 Analisi degli Attacchi: Phishing, Ransomware e Malware 6

1.5 Attività Ransomware 6

1.6 Malware Emergenti 6

1.7 Raccomandazioni e Misure di Protezione 6

1.8 Outlook delle Minacce 8

2 Security news 9

2.1 Rilasci aggiornamenti e patch 9

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

3 CVE Monitor 15

3.1 Sintesi Settimanale CVE 15

3.2 Tendenze 17

3.3 Nuove CVE 18

3.4 CVE attualmente utilizzate in attacchi 19

4 Attacchi 21

4.1 Phishing 21

4.2 Ransomware 25

4.3 Malware 27

4.4 DDoS rilevati 37

4.5 Data Breach 39

4.6 Defacement 41

5 Honeypot 42

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale 42

5.1.1 Attacchi ai servizi 43

5.1.2 IP Attaccanti 43

5.1.3 Paesi di provenienza degli attacchi 44

5.2 Italian Honeypot N.1 45

5.2.1 Attacchi ai servizi 45

5.2.2 IP Attaccanti 46
5.2.3 Paesi di provenienza degli attacchi 46
5.3 Italian Honeypot N.2 48
5.3.1 Attacchi ai servizi 48
5.3.2 IP attaccanti 49
5.3.3 Paesi di provenienza degli attacchi 50
6 Company Profile S3K 51

CYBER SECURITY RISK REPORT
38/25

1 Il Cyber Security Risk Report S3K

1.1 Bollettino di Sicurezza Informatica

Analisi delle minacce e tendenze della sicurezza informatica per la settimana 15-21 Settembre 2025. Un rapporto completo sui rilasci di aggiornamenti, vulnerabilità critiche, attacchi ransomware e phishing, con un focus particolare sulle minacce che colpiscono il territorio italiano e le organizzazioni a livello globale.

1.2 Aggiornamenti di Sicurezza e Vulnerabilità Critiche

- Mozilla

Rilasciati aggiornamenti critici per Firefox, Firefox ESR, Thunderbird con 7 vulnerabilità ad alta gravità. Le versioni interessate includono Firefox precedenti alla 143 e Thunderbird precedenti alla 143.

- Google Chrome

Correzione urgente per 4 vulnerabilità critiche, inclusa CVE-2025-10585 zero-day che consente attacchi tramite pagine web malevole. Aggiornamento alla versione 140.0.7339.185/.186.

- Greenshot

Vulnerabilità ad alta gravità nell'applicativo di cattura schermo che permetterebbe l'esecuzione di codice arbitrario. Aggiornamento necessario alla versione 1.3.300 o superiore.

La settimana è stata caratterizzata da rilasci di patch critiche per software ampiamente utilizzati. I prodotti Mozilla hanno mostrato un numero significativo di vulnerabilità ad alta gravità, mentre Google ha dovuto affrontare un exploit zero-day attivamente sfruttato. Particolare attenzione merita la vulnerabilità di Greenshot, che dimostra come anche applicazioni apparentemente innocue possano nascondere falle di sicurezza significative.

1.3 CVE Monitor - Tendenze Settimanali

Le CVE più discusse sui social media includono CVE-2025-10035 (Fortra GoAnywhere MFT), CVE-2025-53770 (Microsoft SharePoint), e CVE-2025-52970 (Fortinet FortiWeb). Queste vulnerabilità rappresentano un rischio elevato per le infrastrutture aziendali e richiedono interventi immediati di patching e mitigazione.

1.4 Analisi degli Attacchi: Phishing, Ransomware e Malware

- Situazione Phishing in Italia

I dati CERT-AGID mostrano un'intensa attività di phishing con particolare concentrazione su tematiche fiscali e servizi finanziari. L'analisi di un caso specifico rivela una campagna sofisticata che abusa del brand QuickBooks/Intuit.

- Caso Studio: Campagna QuickBooks
    - Mittente spoofed: quickbooks@notification.intuit.com
    - Vettore: Link Dropbox con eseguibile camuffato (.pdf.exe)
    - Tattica: Remittance notification da $29.517,26
    - Infrastruttura: IP 193.233.113.23 (Partner Hosting LTD)

La campagna utilizza tecniche avanzate di social engineering, sfruttando servizi legittimi come Dropbox per migliorare la deliverability e aggirare i filtri antispam. L'uso di double extension (.pdf.exe) e l'importo elevato sono progettati per indurre urgenza e curiosità nelle vittime.

1.5 Attività Ransomware

Nell'ultima settimana l'attività ransomware ha mostrato un'intensificazione significativa, con ben 15 gruppi attivi individuati e il settore **healthcare** fra i più esposti: sono state infatti 25 le organizzazioni sanitarie colpite. Tra le principali famiglie di ransomware osservate, emergono varianti già note per aggressività e capacità di diffusione, confermando la tendenza a colpire infrastrutture critiche e realtà sensibili. Parallelamente, sul fronte della risposta internazionale, è da segnalare il sequestro di 340 domini nell'ambito di un'operazione congiunta che ha preso di mira il gruppo criminale **Raccoon0365**, a testimonianza di un impegno crescente delle forze dell'ordine nel contrasto a queste minacce

1.6 Malware Emergenti

La settimana ha visto l'emergere di nuove minacce significative, incluso Storm-0501 che ha spostato il focus verso ambienti cloud, TamperedChef nascosto in falsi editor PDF, e campagne APT36 mirate al settore governativo indiano utilizzando file .desktop su sistemi Linux BOSS.

1.7 Raccomandazioni e Misure di Protezione

- Patch Management Prioritario

Applicare immediatamente gli aggiornamenti per Microsoft SharePoint, Fortra GoAnywhere MFT, e Mozilla Firefox/Thunderbird. Implementare procedure di emergency patching per vulnerabilità zero-day.

- Protezione dei Backup

Implementare strategie air-gapped per le copie di sicurezza, utilizzare soluzioni di immutabilità dei dati, e testare regolarmente le procedure di ripristino per garantire l'efficacia in caso di compromissione.

- Formazione e Awareness

Intensificare la formazione su tecniche di phishing avanzate, in particolare campagne che abusano di servizi legittimi come Dropbox e utilizzano temi di pagamento/fatturazione per indurre azioni immediate.

- Monitoring e Detection

Implementare monitoraggio avanzato per comunicazioni anomale verso bot Telegram, attività di proxy residenziali, e comportamenti sospetti nei sistemi di backup e recovery.

- Segmentazione di Rete

Isolare sistemi critici come MFT e repository di backup. Implementare principi di Zero Trust e limitare i privilegi di accesso secondo il principio del least privilege.

- Threat Intelligence

Monitorare indicatori di compromissione specifici, inclusi domini malevoli, hash di malware, e pattern di comportamento associati ai gruppi APT attivi nel periodo osservato.

1.8 Outlook delle Minacce

Il panorama delle minacce continua a evolversi con attacchi sempre più sofisticati che combinano tecniche tradizionali e innovative. L'attenzione particolare verso i backup e le infrastrutture cloud rappresenta un cambio di paradigma che richiede un approccio olistico alla sicurezza informatica. Le organizzazioni devono adottare strategie difensive multi-livello che includano prevenzione, detection, response e recovery.

Prossimi Passi: Continuare il monitoraggio delle campagne APT36 e Storm-0501, implementare controlli specifici per domini .desktop su sistemi Linux, e mantenere alta l'attenzione sui vettori di phishing che sfruttano servizi cloud legittimi.

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Mozilla	Mozilla ha rilasciato aggiornamenti di sicurezza per sanare diverse vulnerabilità, di cui 7 con gravità "alta", nei prodotti Firefox, Firefox ESR, Thunderbird e Thunderbird ESR. Versioni affette: • Firefox, versioni precedenti alla 143 • Firefox ESR 140.x, versioni precedenti alla 140.3 • Firefox ESR 115.x, versioni precedenti alla 115.28 • Thunderbird, versioni precedenti alla 143 • Thunderbird ESR 140.x, versioni precedenti alla 140.3
ULR/Note	https://www.mozilla.org/en-US/security/advisories/mfsa2025-73/ https://www.mozilla.org/en-US/security/advisories/mfsa2025-74/ https://www.mozilla.org/en-US/security/advisories/mfsa2025-75/ https://www.mozilla.org/en-US/security/advisories/mfsa2025-77/ https://www.mozilla.org/en-US/security/advisories/mfsa2025-78/ https://www.mozilla.org/en-US/security/advisories/

PRODOTTO	DESCRIZIONE
Greenshot	Rilasciati aggiornamenti di sicurezza per risolvere una vulnerabilità, con gravità "alta", nell' applicativo open source Greenshot utilizzato per la cattura di istantanee dello schermo su Windows. La vulnerabilità, qualora sfruttata, consentirebbe a un utente malintenzionato di eseguire codice arbitrario. Versioni affette: • versioni precedenti alla 1.3.300
ULR/Note	https://getgreenshot.org/downloads/

PRODOTTO	DESCRIZIONE
Google Chrome	Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere quattro vulnerabilità di sicurezza con gravità "alta". Nel dettaglio la CVE-2025-10585, di tipo zero-day, consentirebbe a un utente malintenzionato remoto di indurre l'utente a visitare una pagina Web malevola opportunamente predisposta. Versioni affette: • versioni precedenti alla 140.0.7339.185/.186 per Windows • versioni precedenti alla 140.0.7339.185/.186 per Mac • versioni precedenti alla 140.0.7339.185 per Linux
ULR/Note	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html

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

MICROSOFT SMANTELLA 340 DOMINI COLLEGATI ALL'OPERAZIONE DI PHISHING RACCOON0365

Microsoft, in collaborazione con il provider Cloudflare ed i servizi segreti statunitensi, ha recentemente portato a termine un'operazione internazionale cui è seguito il sequestro di 340 siti web utilizzati per attività di phishing legate al servizio denominato *Raccoon0365*. Questo servizio, nato in Nigeria e diffuso soprattutto attraverso un canale Telegram con oltre 850 membri, forniva agli utenti gli strumenti per organizzare campagne di phishing mirate, capaci di imitare portali di login Microsoft e altri marchi conosciuti al fine di rubare credenziali e dati sensibili.

La portata dell'operazione è considerevole: dal suo lancio nel luglio 2024, Raccoon0365 ha permesso ai cybercriminali di guadagnare almeno 100.000 dollari in criptovalute, offrendo un "servizio chiavi in mano" a chiunque volesse lanciare campagne malevole. Tra i bersagli più colpiti figurano oltre 2.300 organizzazioni, molte delle quali prese di mira con email a tema fiscale diffuse tra il 12 e il 28 febbraio 2025.

Il settore sanitario risulta particolarmente danneggiato, con almeno cinque violazioni accertate e 25 organizzazioni complessivamente colpite da tentativi di phishing. Cloudflare, da parte sua, ha agito per limitare la possibilità di registrare nuovi account e bloccare l'infrastruttura sottostante.

L'azione legale che ha portato al sequestro è stata approvata dal tribunale di Manhattan, su richiesta della Digital Crimes Unit di Microsoft. L'azienda ha sottolineato come queste attività non siano circoscritte a un solo Paese, ma rappresentino un fenomeno globale, capace di sfruttare infrastrutture cloud e servizi legittimi per nascondere attività malevole. Questa operazione non elimina definitivamente il problema, ma costituisce un colpo importante a una rete criminale ben strutturata, riducendo la sua capacità di colpire nel breve termine.

DISAGI AGLI AEROPORTI EUROPEI DOPO L'ATTACCO INFORMATICO AI SISTEMI DI GESTIONE

Un attacco informatico mirato contro un importante fornitore di servizi IT che supporta le operazioni di check-in e imbarco passeggeri ha causato disagi senza precedenti in diversi aeroporti europei. I sistemi colpiti sono utilizzati da numerose compagnie aeree per la gestione di attività quotidiane fondamentali come la registrazione dei viaggiatori, l'assegnazione dei posti e la stampa delle carte d'imbarco.

Il malfunzionamento, che si è protratto per diversi giorni, ha avuto ripercussioni dirette sulla mobilità di migliaia di persone. In hub cruciali come Heathrow a Londra, Bruxelles e Berlino, molti voli sono stati cancellati o hanno subito ritardi significativi. In Irlanda, gli aeroporti di Dublino e Cork hanno vissuto situazioni simili, costringendo i passeggeri ad affrontare code interminabili e procedure manuali di accettazione.

La crisi si è estesa anche ad altri aeroporti di medie dimensioni, confermando la natura interconnessa e vulnerabile del settore. Alcuni scali hanno implementato procedure d'emergenza, tra cui la registrazione cartacea dei viaggiatori e l'imbarco manuale, ma queste soluzioni hanno inevitabilmente rallentato i processi, causando disagi prolungati. In particolare, la gestione dei bagagli è stata gravemente compromessa, con numerosi casi di valigie smarrite, voli in partenza senza i bagagli dei passeggeri e accumuli nelle aree di stoccaggio.

Secondo le autorità, non vi sono indicazioni che l'attacco abbia provocato danni permanenti all'infrastruttura informatica o messo a rischio la sicurezza dei voli. Tuttavia, la gravità delle conseguenze ha riacceso il dibattito sull'adeguatezza delle misure di sicurezza informatica nel settore del trasporto aereo, che si conferma un target privilegiato per i criminali informatici. L'attacco dimostra come un singolo punto di vulnerabilità in un fornitore esterno possa generare un effetto domino su scala continentale, colpendo migliaia di passeggeri e numerosi operatori contemporaneamente.

Le indagini sono in corso per identificare le modalità dell'attacco, la sua origine e i responsabili. Nel frattempo, le compagnie aeree stanno lavorando a stretto contatto con gli operatori IT per ripristinare pienamente i sistemi e garantire la continuità dei servizi. La vicenda rappresenta un monito: le infrastrutture critiche devono dotarsi non solo di barriere difensive più robuste, ma anche di piani di continuità operativa ben collaudati, in grado di ridurre al minimo l'impatto di futuri incidenti.

GLI HACKER PRENDONO DI MIRA I BACKUP: QUANDO LE COPIE DI SICUREZZA DIVENTANO UN BERSAGLIO

Un recente rapporto di Apricorn ha messo in luce un fenomeno in crescita che sta destando forte preoccupazione tra le organizzazioni: gli hacker non si limitano più a colpire i server di produzione o i sistemi centrali, ma rivolgono la loro attenzione direttamente ai backup, ovvero le copie di sicurezza che dovrebbero rappresentare l'ultima difesa contro attacchi distruttivi o ransomware.

In passato, il backup era considerato una sorta di "assicurazione" contro gli incidenti informatici: in caso di compromissione dei sistemi principali, le aziende potevano ripristinare rapidamente le attività grazie alle copie ridondanti dei dati. Oggi, invece, gli aggressori hanno compreso che eliminando o cifrando i backup possono annullare ogni possibilità di recupero, amplificando l'impatto degli attacchi e aumentando le possibilità di ottenere riscatti o altre forme di guadagno illecito.

I dati parlano chiaro: il 18% delle aziende intervistate ha segnalato che la compromissione dei backup è stata la causa diretta di incidenti significativi, mentre il 13% ha ammesso che le procedure di ripristino erano inadeguate o troppo lente per garantire una ripresa tempestiva. Questo significa che quasi un'azienda su tre non è in grado di fare affidamento in modo sicuro sulle proprie copie di sicurezza.

Le tecniche utilizzate dai cybercriminali sono sempre più raffinate. In alcuni casi, l'accesso alle copie di backup avviene dopo che l'attaccante ha già compromesso la rete principale, sfruttando credenziali rubate o vulnerabilità di sistema. In altri casi, vengono utilizzati malware progettati per identificare e distruggere automaticamente i backup, cancellando file o corrompendo gli archivi.

Un caso emblematico è quello di CloudNordic, dove un attacco mirato ha portato non solo alla cifratura dei server di produzione, ma anche alla compromissione completa delle copie di sicurezza, rendendo di fatto impossibile il ritorno alla normalità. L'azienda ha subito un danno irreversibile, perdendo dati e clienti.

Questo scenario evidenzia la necessità di ripensare radicalmente la protezione dei backup. Non è più sufficiente limitarsi a effettuare copie periodiche: è essenziale adottare soluzioni che prevedano backup isolati (air-gapped), sistemi distribuiti e procedure di test frequenti. Inoltre, cresce l'importanza di strategie di immutabilità dei dati, che impediscono modifiche o cancellazioni non autorizzate.

Nonostante il quadro preoccupante, ci sono segnali di miglioramento. Sempre più aziende stanno investendo in tecnologie di backup automatizzato e ridondante, e cresce la consapevolezza dell'importanza di effettuare test regolari di ripristino. Tuttavia, il messaggio rimane chiaro: senza una protezione adeguata, i backup possono trasformarsi da risorsa fondamentale a punto debole critico, esponendo le organizzazioni a conseguenze devastanti.

NUOVA VULNERABILITÀ NEL PROTOCOLLO WINDOWS RPC: RISCHI DI SPOOFING E IMPERSONIFICAZIONE

I ricercatori di SafeBreach hanno scoperto una vulnerabilità critica nel protocollo Windows Remote Procedure Call (RPC), segnalata come CVE-2025-49760 e corretta da Microsoft con la patch di luglio 2025.
Il problema risiede nella gestione del componente Endpoint Mapper (EPM), responsabile della registrazione delle interfacce RPC.
In condizioni normali, EPM permette ai servizi di registrare le proprie interfacce per rendersi disponibili agli utenti e ai processi di sistema. Tuttavia, è emerso che non viene verificata l'identità del processo che effettua la registrazione, aprendo la strada a potenziali attacchi di spoofing. Un attaccante può così registrare per primo un'interfaccia destinata a un servizio legittimo non ancora avviato, facendo credere al sistema di interagire con un server autentico.
Gli scenari di attacco possibili sono molteplici:

- impersonificazione di un server SMB per catturare le credenziali degli utenti;
- trasmissione e intercettazione di hash NTLM;
- escalation dei privilegi tramite l'ottenimento di certificati sfruttando credenziali rubate.

La vulnerabilità, se sfruttata con successo, avrebbe consentito a un utente non privilegiato di muoversi lateralmente nella rete e di compromettere ulteriormente l'infrastruttura.
Per mitigare i rischi, i ricercatori consigliano di monitorare con attenzione le chiamate RpcEpRegister e di utilizzare l'Event Tracing for Windows (ETW) per rilevare attività sospette. Naturalmente, l'applicazione tempestiva delle patch rilasciate da Microsoft rimane la misura più efficace per ridurre il livello di esposizione.
Questa scoperta sottolinea ancora una volta come anche protocolli consolidati e fondamentali per il funzionamento di Windows possano nascondere falle di sicurezza significative, capaci di esporre sistemi e reti aziendali a rischi considerevoli.

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 15 Settembre – 21 Settembre 2025
Settimana caratterizzata da vulnerabilità critiche su piattaforme MFT, SharePoint, appliance web e componenti client/OS. Patch e mitigazioni urgenti raccomandate per ambienti esposti.
CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Descrizione Sintetica
CVE-2025-8077	CRITICAL	17/09/2025	✅	NeuVector — default admin password hardcoded; se non cambiata permette ottenimento token admin via API e controllo della piattaforma container security.
CVE-2025-10035	CRITICAL	18/09/2025	✅	Fortra GoAnywhere MFT — deserializzazione in License Servlet: un attore con risposta di licenza contraffatta può deserializzare oggetti controllati dall'attaccante → possibile command injection / takeover. Aggiornare subito
CVE-2025-7744	HIGH	16/09/2025	❌	Dolusoft Omaspot — SQL Injection (CWE-89) che permette esfiltrazione/modifica DB; interessa versioni precedenti al 12.09.2025

CVE-2025-5948	HIGH	19/09/2025	❌	WordPress plugin Service Finder Bookings — account takeover / privilege escalation via azione claim_business (una richiesta AJAX non validata) che può consentire login come admin.
CVE-2025-53770	CRITICAL	19/07/2025	✅	Microsoft SharePoint on-prem — deserializzazione di dati non fidati → RCE remota; exploit osservati (ToolShell / campagne Warlock); urgente patching e mitigazioni (AMSI, rotazione MachineKey).

Vendor e Tecnologie Coinvolti

- **Microsoft / SharePoint:** CVE-53770/53771 (ToolShell) rimangono prioritarie per patch e azioni di containment.
- **Fortra (GoAnywhere):** CVE-10035 può portare a takeover completo di istanze MFT non aggiornate.
- **Fortinet / NeuVector / vari plugin web:** più CVE di appliance e plugin web richiedono patch mirate.

Distribuzione Giornaliera

- **15 settembre**: disclosure e attività exploit osservata per Microsoft SharePoint
- **16 settembre:** advisory vendor e rilascio patch per NeuVector
- **17 settembre:** segnalazioni di account takeover e possibili exploit per WordPress Service Finder Bookings
- **18 settembre:** divulgazione tecnica di Dolusoft Omaspot

Raccomandazioni

- **Patch Prioritarie:**
    - Aggiornare immediatamente le istanze Microsoft SharePoint on-premise alle release correttive e ruotare MachineKey dopo l'applicazione delle patch.
    - Applicare urgentemente gli aggiornamenti su Fortra GoAnywhere (MFT) forniti dal vendor.
    - Aggiornare appliance web/proxy/WAF (es. FortiWeb o equivalenti) alle versioni che correggono le vulnerabilità di gestione parametri.

- Aggiornare/patchare le piattaforme di sicurezza container (NeuVector): rimuovere password di default e installare le release correttrici.
- Eseguire aggiornamenti Windows per risolvere i problemi di gestione file/estrazione (Explorer / gestione .library-ms / decompressione automatica).

Mitigazioni e Controlli:

- Limitare l'esposizione pubblica dei servizi critici (SharePoint, appliance di gestione web); applicare accesso tramite VPN/Zero Trust quando possibile.
- Applicare regole WAF e filtri specifici per bloccare payload SQLi / richieste API anomale (rate limiting, blocking su pattern di exploit conosciuti).
- Segmentare reti e limitare privilegi: isolare sistemi MFT e repository critici, applicare least-privilege per account di servizio.
- Eseguire scansioni di asset con strumenti aggiornati (SCA / vulnerability scanner) e rispondere agli allarmi con playbook per containment e remediation.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-10035	Fortra's GoAnywhere MFT	N/A
CVE-2025-53770	Microsoft SharePoint Server	N/A
CVE-2025-53771	Microsoft Office SharePoint	N/A
CVE-2025-52970	Fortinet FortiWeb	N/A
CVE-2025-24071	Windows File Explorer	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-2025-8077	NeuVector	N/A
VULNERABILITÀ	Esiste una vulnerabilità in NeuVector nelle versioni fino alla 5.4.5 inclusa, in cui viene utilizzata una stringa fissa come password predefinita per l'account integrato admin. Se questa password non viene modificata immediatamente dopo il deployment, qualsiasi workload con accesso di rete all'interno del cluster potrebbe utilizzare le credenziali predefinite per ottenere un token di autenticazione. Questo token può poi essere usato per eseguire qualsiasi operazione tramite le API di NeuVector.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-7744	Dolusoft	N/A
VULNERABILITÀ	Una vulnerabilità di neutralizzazione impropria di elementi speciali utilizzati in un comando SQL ("SQL Injection") in Dolusoft Omaspot consente un attacco di SQL Injection.Questo problema riguarda Omaspot nelle versioni precedenti al 12.09.2025.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-57631	TDuckCloud v.5.1	N/A
VULNERABILITÀ	Una vulnerabilità di SQL Injection in TDuckCloud v.5.1 permette a un attaccante remoto di eseguire codice arbitrario nella sezione "Add a file upload module"	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-5948	WordPress	N/A
VULNERABILITÀ	Il plugin Service Finder Bookings per WordPress è vulnerabile a un'elevazione di privilegi tramite takeover di account in tutte le versioni fino (e incluso) alla 6.0. Questo è dovuto al fatto che il plugin non valida correttamente l'identità di un utente prima di effettuare la rivendicazione di un'attività tramite l'azione AJAX claim_business. Ciò rende possibile per attaccanti non autenticati effettuare il login come qualsiasi utente, inclusi gli amministratori. Si noti che per completare il takeover dell'attività sono necessari privilegi di subscriber o il brute-forcing. Il claim_id è necessario per prendere il controllo dell'account admin, ma il brute-forcing è un approccio pratico per ottenere ID validi.		

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	
Una vulnerabilità di deserializzazione di dati non attendibili che interessa DELMIA Apriso dalla Release 2020 fino alla Release 2025 potrebbe consentire l'esecuzione di codice da remoto (RCE).	

CVE	CVE-2025-48543
DESCRIZIONE	
Vulnerabilità Use-After-Free in Android Runtime: Android Runtime contiene una vulnerabilità di tipo use-after-free che potrebbe consentire un chrome sandbox escape, portando a una local privilege escalation.	

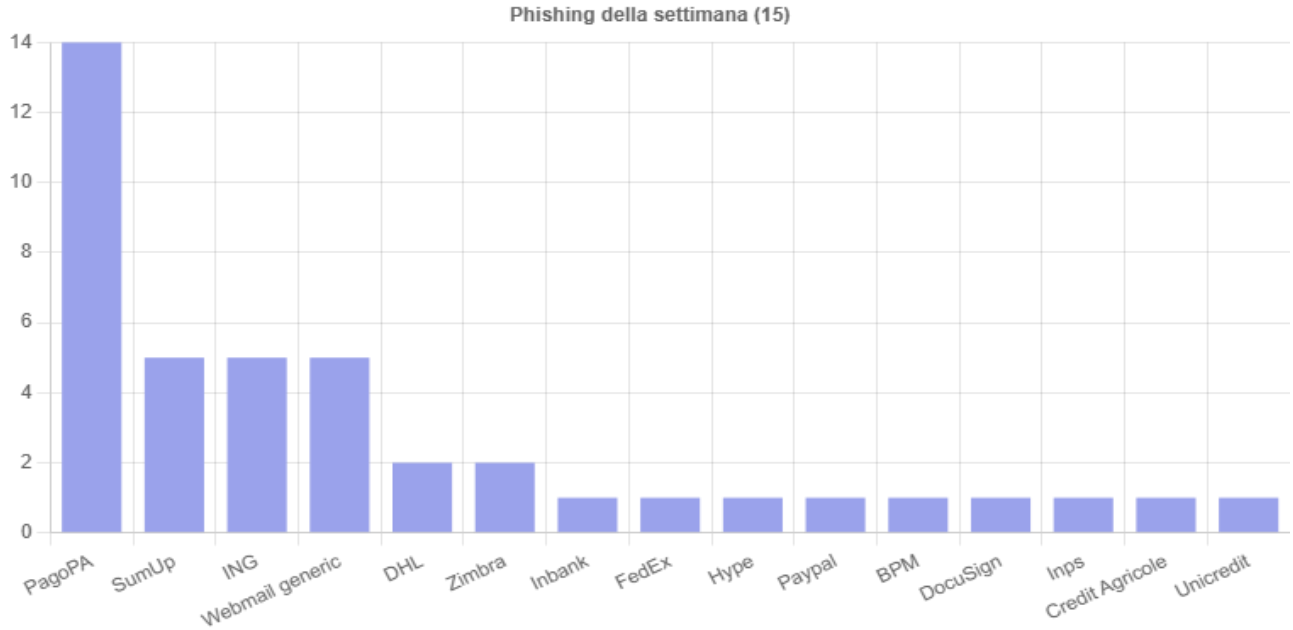
CVE	CVE-2025-9377
DESCRIZIONE	
Nei router TP-Link Archer C7(EU) V2 e TL-WR841N/ND(MS) V9 è stata riscontrata una vulnerabilità di remote command execution (RCE) autenticata nella pagina di Controllo Genitori. Il problema interessa Archer C7(EU) V2 nelle versioni precedenti alla 241108 e TL-WR841N/ND(MS) V9 nelle versioni precedenti alla 241108. Entrambi i prodotti sono EOL (end-of-life). Si consiglia di sostituirli con un modello più recente per migliorare sicurezza e prestazioni. Se la sostituzione non è possibile a breve, è disponibile una patch da scaricare e installare tramite il secondo link di riferimento.	

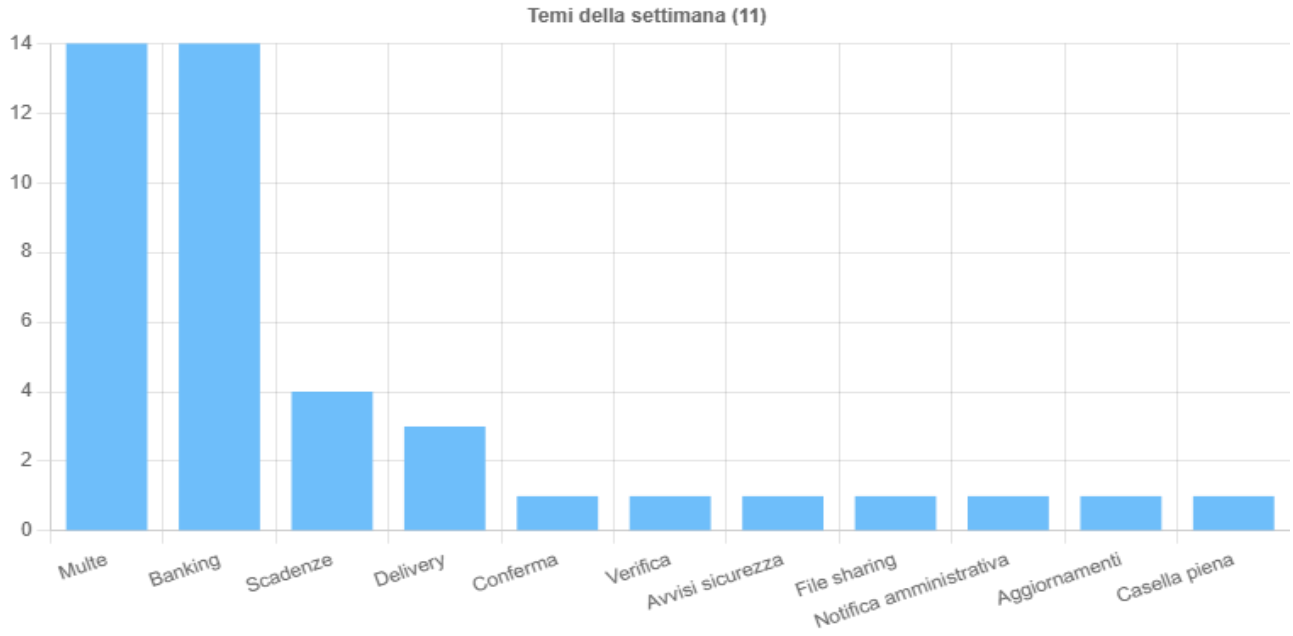
4 Attacchi

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.

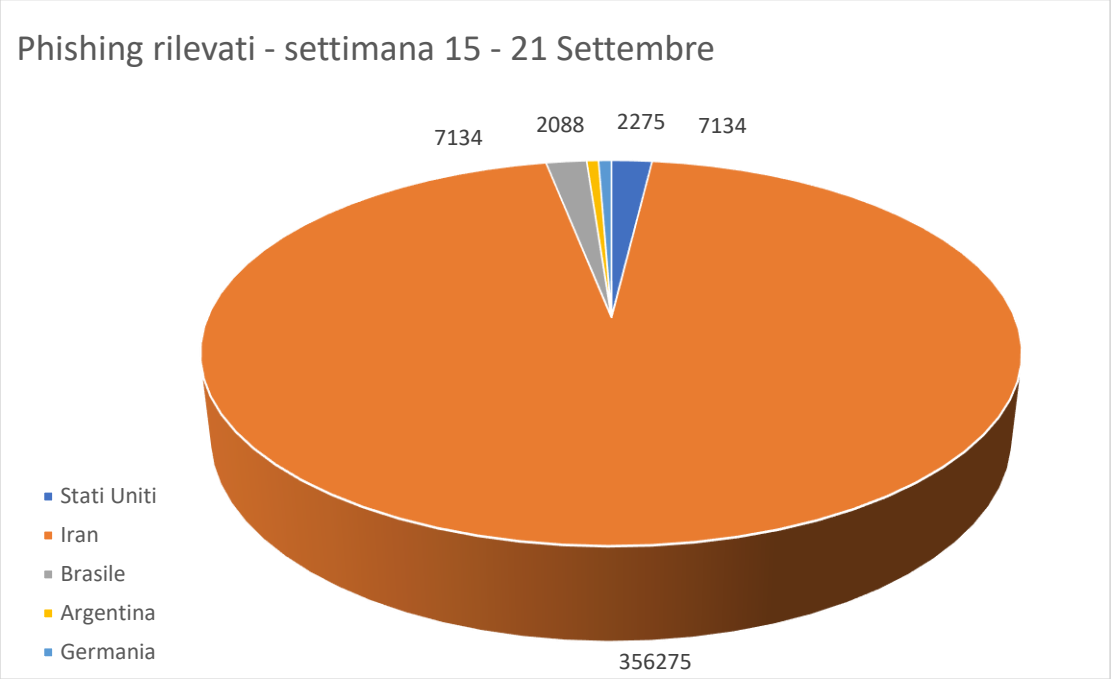




Fonte :CERT-AGID

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 (QuickBooks / ACH)
  Data del report: 2025-09-22 17:18:28
  Destinatario analizzato: victim <victim@victim[.]com> (nome sostituito e dominio normalizzato per policy)
  Avvertenza sul mascheramento: tutti gli IP, domini ed email sono mostrati con i punti sostituiti da "[.]".
- Anteprima email (dati del destinatario oscurati)

Payee Remittance Notification

From: Futurapay <quickbooks@notification[.]intuit[.]com>
To: victim <victim@victim[.]com>
Subject: Payment A0104692
Date: 20 Sep 2025 06:51:02 +0300

Hello: This email is to inform you that a payment in the amount of $29,517.26
via our ACH Corporate (CCD) Payments has been submitted to your account.
NOTE Deposit will occur approximately two working days after the payment date.

VIEW REMITTANCE ADVICE | DOWNLOAD REMITTANCE ADVICE

Link (masked):
https://www[.]dropbox[.]com/scl/fi/t02e9u14j4amtc73igugn
ACH_Payment-for-PO9838-on-20250919-pdf[.]exe?rlkey=bg1qiy7pg84l9iih1e4qpt18u&st=b8g5bihu&dl=1

- Executive summary

  Email tematica 'remittance / ACH payment' che abusa del brand Intuit/QuickBooks e contiene link Dropbox a un eseguibile Windows camuffato da PDF. Indicatori e tattiche coerenti con campagne di malware loader/stealer (es. catena .pdf.exe) e BEC lure. Il server mittente indicato nelle intestazioni non coincide con l'infrastruttura legittima di Intuit: IP sorgente 193[.]233[.]113[.]23 annuncia ASN Partner Hosting LTD (hosting di bassa reputazione). Rischio: ALTO. Azione immediata: blocco URL, IOC su EDR/Proxy, alert al personale, rimozione eventuali esecuzioni.
- Intestazioni email (sintesi)

From	Futurapay <quickbooks@notification[.]intuit[.]com>
To	victim <victim@victim[.]com>
Subject	Payment A0104692
Date	20 Sep 2025 06:51:02 +0300
Received da	notification[.]intuit[.]com (HELO) → IP 193[.]233[.]113[.]23 (Partner Hosting LTD)
SPF/DKIM/DMARC	Non presenti nel blocco header fornito. Incongruenza IP vs SPF di notification[.]intuit[.]com → probabile fail.

- Analisi contenuto & tecnica di social engineering

  Messaggio "**Payee Remittance Notification**" con importo **$29.517,26**, promessa di accredito entro 2 giorni (**urgenza**), tono professionale e **pulsanti** "VIEW / DOWNLOAD REMITTANCE ADVICE". Il **link** punta a **Dropbox** ma scarica ...-pdf.exe (doppia estensione), tipico stratagemma per indurre all'esecuzione di un **malware loader/stealer/RAT**. Pattern coerente con campagne osservate che abusano di **Dropbox** per delivery.

- OSINT su dominio/IP e certificati

  Il dominio legittimo di invio notifiche Intuit è tipicamente sotto il sotto-dominio notification[.]intuit[.]com (e vari host come links[.]notification[.]intuit[.]com) con DNS e certificati gestiti via Akamai/CloudFront/DigiCert. Tuttavia, il recapito di questa email proviene da IP 193[.]233[.]113[.]23 (ASN Partner Hosting LTD), non compatibile con i range pubblici/SendGrid autorizzati dall'SPF della catena di invio di Intuit.
- Verifiche esterne effettuate (link)

  Cloudflare Radar – links.notification.intuit[.]com: https://radar.cloudflare.com/domains/domain/links.notification.intuit[.]com
  SPF checker – notification.intuit[.]com: https://www.spf-record.com/spf-lookup/notification.intuit[.]com
  IPInfo – 193.233.113.0/24: https://ipinfo.io/ips/193.233.113.0/24
  BGP Tools – AS215826 Partner Hosting LTD: https://bgp.tools/as/215826
  AbuseIPDB – check 193.233.113[.]23: https://www.abuseipdb.com/check/193.233.113[.]23
  VirusTotal – IP 193.233.113.23 (GUI): https://www.virustotal.com/gui/ip-address/193.233.113[.]23
  urlscan – links.notification.intuit[.]com: https://api.urlscan.io/domain/links.notification.intuit[.]com
  Dropbox – segnalazione abusi: https://help.dropbox.com/security/phishing-virus-protection
  ANY.RUN – task (campione correlato, .pdf.exe): https://app.any.run/tasks/ff6ff5a3-d4a8-4a6c-b22a-7d4cb264f00f

- Analisi URL e allegati

  La call-to-action punta a un link Dropbox che scarica un eseguibile Windows con nome ingannevole '...-pdf.exe'. Tale naming è tipico di catene di infezione (loader/stealer/RAT). Il file osservato su sandbox è stato classificato 'Malicious activity' (ANY.RUN) e mostra tattiche di anti-analysis e persistenza.
- Indicatori di Compromissione (IoC)

Mittente (visualizzato)	quickbooks@notification[.]intuit[.]com
IP sorgente SMTP	193[.]233[.]113[.]23
URL (Dropbox)	https://www[.]dropbox[.]com/scl/fi/t02e9u14j4amtc73igugn/ACH_Payment-for-PO9838-on-20250919-pdf[.]exe?rlkey=bg1qiy7pg84l9iih1e4qpt18u&st=b8g5bihu&dl=1
Hash MD5 (campione)	FFBFEF17590BCD4A546E36A7A7DCF274
Hash SHA1 (campione)	AD3FDFD80B8F2E83B6EC2B56F753BC68CA8469F8
Hash SHA256 (campione)	EE502269DF06E79F540F1D6B4529109F73AD096228FE8A73D56B92F193850C3F

- Ingegneria sociale e struttura del contenuto

  Tema 'ACH payment / remittance' con importo elevato per indurre curiosità/urgenza. Brand impersonation (Intuit/QuickBooks), tonalità formale e pulsanti 'VIEW/DOWNLOAD'. Uso di servizio affidabile (Dropbox) per miglior deliverability e fiducia apparente.
- Certificati SSL/TLS

  Per i sottodomini legittimi di Intuit (es. links[.]notification[.]intuit[.]com) risultano certificati emessi da DigiCert (vedi Cloudflare Radar). La catena SMTP osservata nel recapito verso victim non transita da IP coerenti con tali infrastrutture.
- WHOIS, hosting e geolocalizzazione

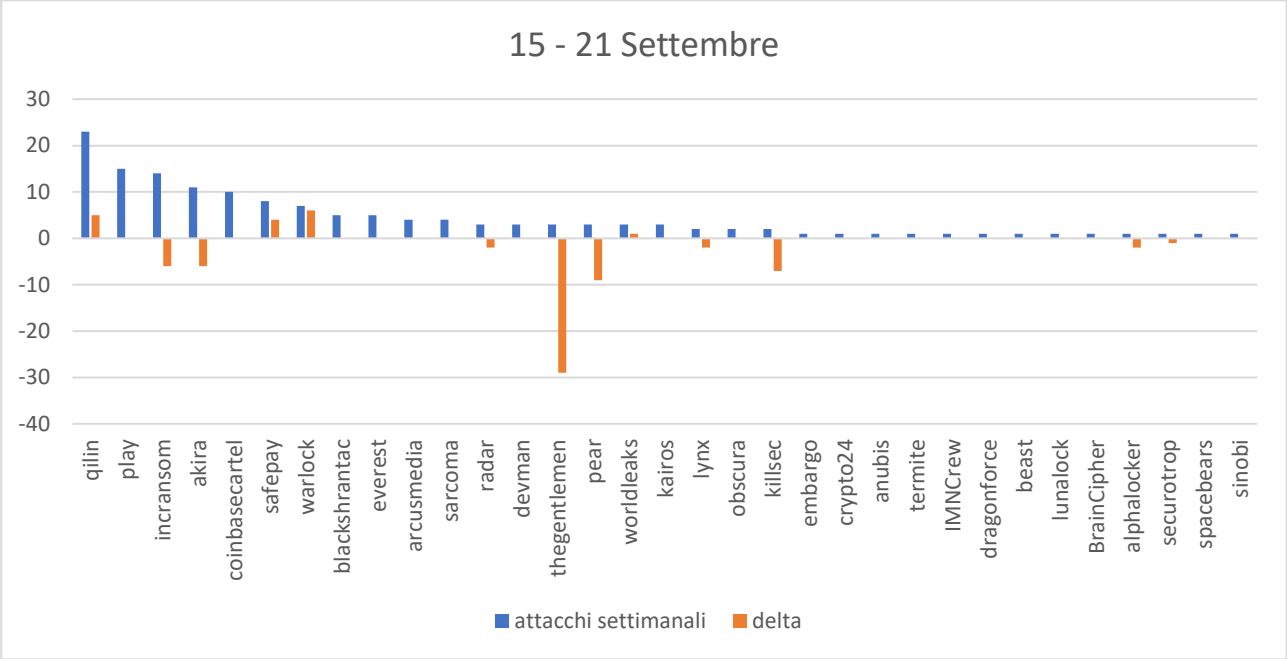
  IP 193[.]233[.]113[.]23 ricade nel blocco 193[.]233[.]112[.]0/23 annunciato da AS215826 (Partner Hosting LTD), provider multi-country con reputazione mista e impiego frequente in campagne abusive. Assenza di PTR/rDNS e assenza di domini hosted noti sul /24 analizzato suggeriscono uso come nodo spedizione.
- SPF/DKIM/DMARC

  Nel blocco header analizzato non sono presenti record 'Authentication-Results'. L'SPF pubblicato per notification[.]intuit[.]com elenca indirizzi SendGrid/Akamai e non include 193[.]233[.]113[.]23. Conclusione: forte indicazione di spoofing/frode del dominio visualizzato.
- Raccomandazioni operative

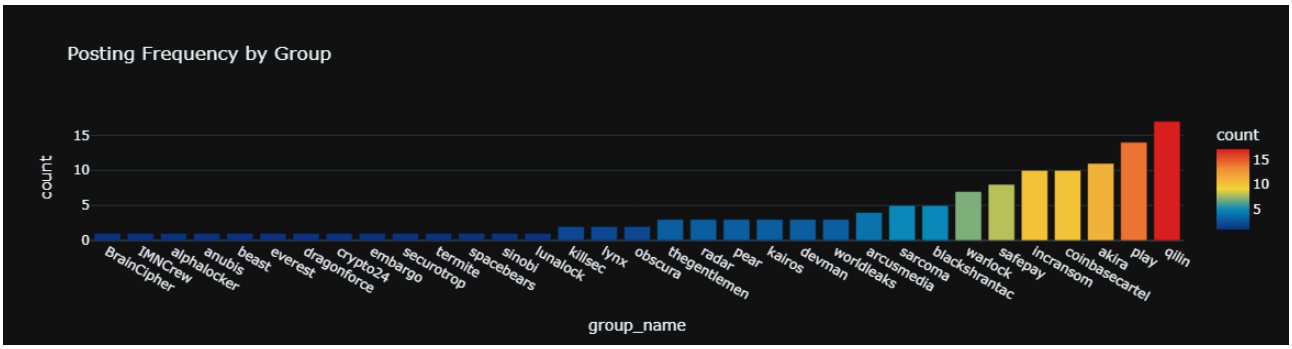
  Bloccare a livello di proxy/EDR l'URL Dropbox indicato e gli hash IoC. 2) Bonifica endpoint che hanno scaricato/eseguito il file. 3) Aggiornare regole antispam (SPF/DMARC enforcement) e banner esterni. 4) Segnalare l'URL a Dropbox (abuse@dropbox.com) per takedown. 5) Awareness al personale su 'ACH payment' lure.

4.2 Ransomware

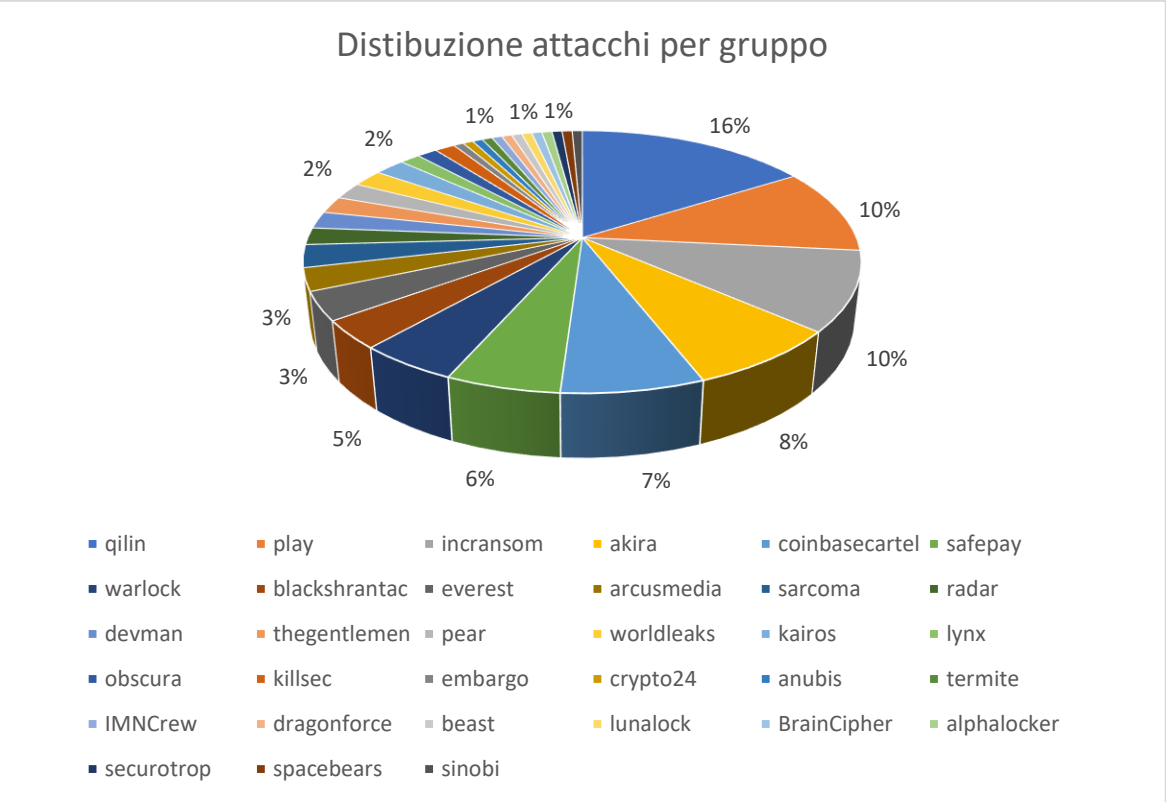
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (15 - 21 Settembre). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

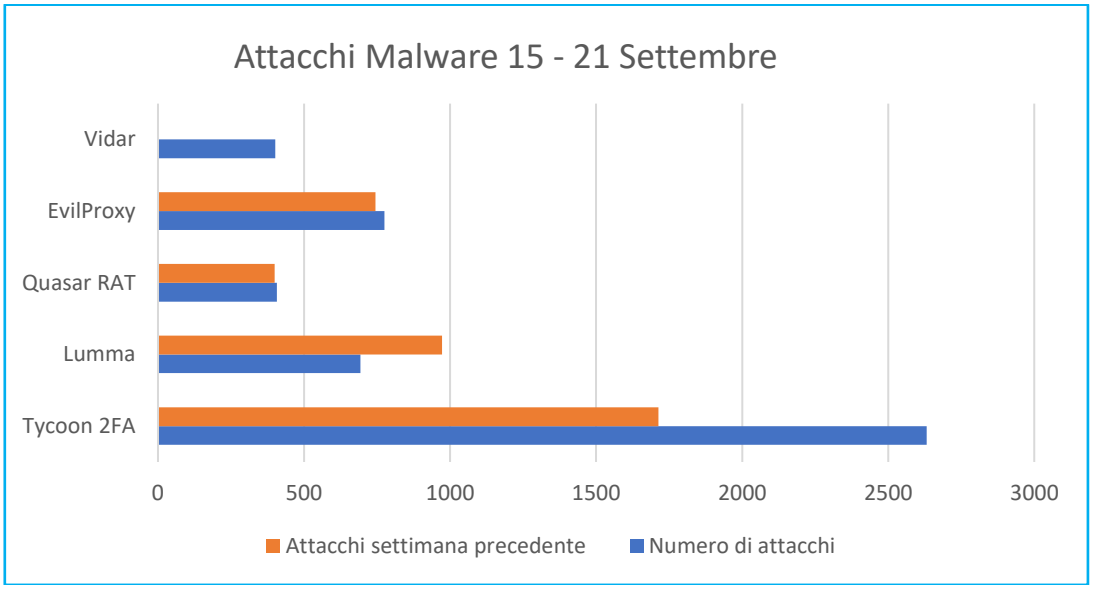


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:


Distibuzione attacchi per gruppo
16%
10%
10%
8%
7%
6%
5%
3%
3%
2%
2%
1%
1%
1%
qilin
play
incransom
akira
coinbasecartel
safepay
warlock
blackshrantac
everest
arcusmedia
sarcoma
radar
devman
thegentlemen
pear
worldleaks
kairos
lynx
obscura
killsec
embargo
crypto24
anubis
termite
IMNCrew
dragonforce
beast
lunalock
BrainCipher
alphalocker
securotrop
spacebears
sinobi

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

- **Storm-0501**

Storm-0501 è un gruppo criminale specializzato in ransomware (RaaS) che ha recentemente spostato il suo focus dagli ambienti on-premise ai servizi cloud. In un attacco recente gli autori hanno sfruttato credenziali valide ed escalation dei privilegi in ambienti Microsoft Entra/Azure, esfiltrando dati e cancellando backup prima di chiedere il riscatto. L'attacco tipo di Storm-0501 vede un compromesso iniziale di Active Directory, poi un pivot al cloud, seguiti da esfiltrazione massiva dei dati e criptaggio selettivo basato su tecniche native cloud (senza usare il classico eseguibile ransomware sui PC).

Descrizione tecnica: Gruppo RaaS (ransomware-as-a-service) finanziario, che ora adotta tattiche basate su infrastrutture cloud native. Utilizza credenziali d'accesso rubate, exploit di servizi directory e piattaforme cloud per ottenere privilegi di amministratore globale, quindi esfiltra grandi volumi di dati e impedisce ripristini cancellando backup. Questo approccio si differenzia dal ransomware tradizionale perché non si limita a crittografare file locali, ma punta a rendere irrecuperabili anche i dati nel cloud.

IoC: attualmente non sono stati pubblicati indicatori specifici di file, hash o domini legati alle campagne cloud-based di Storm-0501. L'analisi si concentra sulle tecniche TTP utilizzate, piuttosto che su singoli artefatti maligni.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1490	Inhibit System Recovery	Eliminazione di snapshot e backup cloud per impedire il ripristino dei sistemi compromessi.
T1486	Data Encrypted for Impact	Cifratura dei dati per causare impatto operativo e richiedere un riscatto.
T1550	Use Alternate Authentication Material	Utilizzo di hash NTLM e token per movimenti laterali e accessi non autorizzati.
T1003.006	OS Credential Dumping: DCSync	Utilizzo della tecnica DCSync per replicare hash NTLM e credenziali da controller di dominio.
T1021.001	Remote Services: Evil-WinRM	Accesso remoto malevolo tramite Evil-WinRM per eseguire comandi e ottenere escalation.

Contromisure:

- adottare misure di difesa su cloud e identità.
- abilitare l'MFA, monitorare i log di accesso ai tenant cloud, usare EDR/UEBA per rilevare attività sospette, segmentare le risorse cloud e tenere aggiornati AD Connect.
- Effettuare backup sicuri (offline) e verificare sistematicamente le policy di accesso condizionato in Azure.
- I prodotti di sicurezza (es. Defender for Cloud/Endpoint) devono essere attivi su tutte le istanze per evitare blind spots.

Livello di rischio: Alto (attività finanziariamente motivate con forte impatto su infrastrutture critiche).

- **TamperedChef**

TamperedChef è un nuovo malware stealer individuato nell'ambito di una campagna malspam che utilizza falsi editor PDF per veicolare un trojan. I ricercatori Truesec e G DATA hanno scoperto siti ingannevoli che promuovono un presunto "PDF Editor" (es. AppSuite PDF Editor): dopo l'installazione il setup scarica un payload che si installa come applicazione legittima, crea attività programmate e funge da backdoor.

All'attivazione, TamperedChef sottrae credenziali e cookie dai browser (Chrome, OneLaunch, Wave), modificando chiavi di registro e intercettando il traffico web.

Descrizione tecnica: Malware informazionale nascosto in un installer di un fantomatico editor PDF. Il setup victimato effettua richieste a un C2 remoto per scaricare il file PDF editor e installa attività programmate (PDFEditorScheduledTask, PDFEditorUScheduledTask) per la persistenza.

La funzione "--install" dell'eseguibile scaricato crea un servizio dove, oltre all'applicazione, vengono inclusi moduli di info-stealing. All'aggiornamento (dopo circa 56 giorni) il malware attiva funzionalità clandestine, terminando i browser aperti e prelevando cookie e credenziali salvate.

I domini e il nome esatto del file variano per ogni campagna di malvertising (le versioni trojanizzate del PDF editor sono distribuite tramite annunci compromessi).

IoC:

Indicativi sono i nomi delle task schedulate ("PDFEditorScheduledTask" e "PDFEditorUScheduledTask") e il parametro di avvio --cm=... nell'eseguibile maligno. Poiché i siti malevoli e gli installer cambiano, non esistono IoC statici fissi noti al pubblico. Gli EDR possono cercare comportamenti come eseguibili con nome PDFEditor o le chiavi di registro usate.

Tipo	Indicatore
File	"AppSuite PDF Editor" (installer trojan)
Attività	Task schedulate PDFEditorScheduledTask, PDFEditorUScheduledTask

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing / Malvertising	Distribuzione tramite campagne malvertising (Google Ads) e link ingannevoli
T1204	User Execution	Inganno dell'utente a eseguire installer apparentemente legittimi di software popolari.
T1053	Scheduled Task / Job	Creazione di task pianificati per garantire persistenza sul sistema infetto.
T1555	Credentials from Password Stores	Raccolta di credenziali e informazioni sensibili dai browser o dai password manager.

Contromisure:

- Bloccare fonti pubblicitarie e siti sospetti di distribuzione di software PDF.
- Impostare policy di sicurezza per la navigazione (EDR, antivirus) che segnalino l'installazione di software non firmato o riconosciuto. Monitorare la presenza di task schedulate anomale (nomi PDFEditor…) e processi con parametri --cm.
- Disabilitare l'esecuzione automatica di applicazioni non autorizzate.

Livello di rischio: Medio (furto di credenziali e cookie con potenziale impatto su account web).

- **ManualFinder/PDF Editor Trojan**

Il CERT-NL/NCSC ha allertato su una campagna globale di malware diffusa tramite falsi software per cercare manuali o modificare PDF.

Le vittime scaricano innocue app come "ManualFinder" o "PDF-editor" da annunci online, ma tali applicazioni creano una task schedulata (sys_component_health_) che esegue quotidianamente uno script JS (nome casuale GUID) con Node.js. Questo malware trasforma il PC infetto in un "residential proxy" utilizzato dai criminali per mascherare attacchi informatici.

In altre parole, il computer compromesso diventa una sorta di server relay: gli attaccanti instradano il loro traffico attraverso questo proxy rendendo difficile risalire alla fonte del vero attacco. È stata osservata anche l'installazione di un tool di "ManualFinder" con funzionalità proxy durante la campagna.

Descrizione tecnica: Malware nascosto in finti software utilità. All'installazione viene creata una scheduled task (sys_component_health_) che ogni giorno avvia un file JavaScript nascosto in %TEMP% con un nome a GUID.

Lo script JS comunica con server di comando remoto (C2) e abilita la modalità proxy tramite un componente denominato ManualFinder (legittimo solo di nome). In pratica, l'attacco usa software firmati in modo ufficiale (con certificati compromessi) per diffondere il malware e utilizza risorse legittime per nascondere l'infezione.

IoC:

Tipo	Indicatore
File	File JS con nome GUID e suffisso "ro.js" o "or.js" eseguito da Node
Domini	y2iax5[.]com, 5b7crp[.]com, mka3e8[.]com (C2 della campagna)
Certificati	Certificati digitali compromessi: "GLINT SOFTWARE SDN BHD", "ECHO INFINI SDN BHD", "Summit Nexus Holdings LLC
Software	"ManualFinder" (utilità proxy)
Hashes	• PDFEditor.exe cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c • PDFEditorSetup.exe da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0

	• AppSuite-PDF.msi fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b • ConvertMate.exe e0db7b5eaf92feff220c805b0e5f3d8916e18d51 • ConvertMate.exe d9f9584f4f071be9c5cf418cae91423c51d53ecf9924ed39b42028d1314a2edc • conmate_update.ps1 372d89d7dd45b2120f45705a4aa331dfff813a4be642971422e470eb725c4646 • Uninstaller.exe e95de8452d32b439e0286868ed16f63943af3bc059dca6bcb48d1cbe2431440e

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1053	Scheduled Task/Job	L'utente viene indotto a scaricare ed eseguire il finto editor PDF tramite ingegneria sociale.
T1204	User Execution	Creazione di task pianificati per mantenere la persistenza sul sistema compromesso.
T1090	Proxy / Tunneling	Utilizzo di proxy o tunneling per nascondere le comunicazioni C2 e l'esfiltrazione di dati.

Contromisure:

- Bloccare i domini elencati come malevoli (blacklist DNS/firewall) e rimuovere qualsiasi applicazione "ManualFinder" o PDF-editor sconosciuta.
- Controllare e cancellare task schedulate sospette in cui Node.js avvia script sconosciuti.

- Aggiornare le piattaforme di sicurezza (EDR, antivirus) per rilevare comportamenti di proxy inversi. Sensibilizzare gli utenti a non installare tool da annunci pubblicitari.

Livello di rischio: Medio (il sistema infetto viene abusato come proxy per altre attività malevole).

- **APT36 (Transparent Tribe)**

Il gruppo APT36, legato all'intelligence pachistana, ha lanciato una campagna mirata di spionaggio verso istituzioni indiane, utilizzando file .desktop su Linux BOSS (sistema governativo indiano).

In questa operazione di spear phishing, le vittime ricevono una e-mail con un allegato .zip che contiene un file .desktop camuffato da collegamento a un PDF.

All'apertura del file .desktop (che in realtà è uno script), vengono eseguiti comandi per scaricare un payload maligno e installare un malware. Contestualmente viene avviato Firefox in background su un documento benigno (ospitato su Google Drive) per sviare l'utente dall'attività illecita.

Una volta stabile il canale col server C2, il malware raccoglie dati sensibili dal sistema e li esfiltra ai malintenzionati.

Questa tattica dimostra come APT36 stia diversificando i vettori di attacco verso ambienti protetti (Linux) mantenendo attività tradizionali su Windows e mobile.

Descrizione tecnica: Attacco di tipo spear-phishing su infrastrutture Linux governative. Viene inviato un file .desktop (con estensione .desktop) nascosto in un archivio, presentato come scorciatoia PDF. Eseguendo questo file .desktop, il sistema scarica e lancia un malware che esfiltra informazioni.

Per ingannare l'utente viene contemporaneamente aperto un documento Google Drive innocuo in Firefox, simulando un'attività lecita

Indicatori di compromissione (IoC): la minaccia non ha nomi di dominio o hash pubblici noti. Segnali d'allarme includono la comparsa di file .desktop non autorizzati e attività anomale di Firefox in background. Le istruzioni maligni sono incorporate nello stesso file .desktop.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566.001	Phishing: Spearphishing Attachment	Invio di allegati malevoli (file .desktop) come vettore iniziale di infezione.
T1204	User Execution	Richiede che la vittima apra manualmente il file allegato per avviare l'esecuzione del malware.
T1560	Archive Collected Data	Esfiltrazione e compressione dei dati raccolti dal sistema compromesso.
T1036	Masquerading	Avvio di Firefox per mascherare l'attività malevola e ridurre la possibilità di rilevamento.

Contromisure:

- Formare gli utenti sul rischio di allegati e scorciatoie sospette. Bloccare allegati .desktop e archivi da mittenti non affidabili.
- Su Linux verificare integrità e provenienza dei file eseguibili e usare soluzioni di sicurezza endpoint su Linux BOSS.
- Monitorare traffico in uscita insolito verso server strani (anche su TLS).

Livello di rischio: Alto (spionaggio politico/settore militare con furto di dati sensibili).

- **ShadowSilk**

Un cluster di attività APT attivo in Asia centrale e Pacifico (denominato ShadowSilk) ha preso di mira enti governativi e settore energia nei paesi ex-sovietici e vicini.

Gli autori, caratterizzati da due team bilingue (russo e cinese), sfruttano campagne di spear-phishing con archivi protetti da password che contengono un loader personalizzato. Questo loader nasconde il canale C2 dietro bot di Telegram, rendendo difficile il tracciamento.

Nel corso degli attacchi sono stati sfruttati exploit pubblici su Drupal (CVE-2018-7600/7602) e un plugin WordPress (CVE-2024-27956).

Dopo il compromesso, ShadowSilk impiega web shell (es. ANTSWORD, Behinder) e strumenti di post-exploitation per muoversi lateralmente e creare tunnel crittografati (Resocks, Chisel). Infine utilizza RAT basati su Python che inviano screenshot e dati sottratti a bot Telegram, mimetizzando il traffico come chat legittima.

Descrizione tecnica: APT multiregionale (alleanza operativo YoroTrooper e Silent Lynx) che usa un misto di spear-phishing e vulnerabilità note per entrare nelle reti governative in Asia centrale.

La post-compromissione include la modifica del registro per persistenza, uso di web shell e tool penetration (Metasploit, Cobalt Strike) e esfiltrazione dati occultata come traffico Telegram.

Indicatori di compromissione (IoC): nessun IoC statico pubblicato; tra gli indicatori osservati vi sono payload serviti da siti compromessi, nomi di script (es. jramosh come esempio di web panel) e pattern di traffico a bot Telegram.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing (Spearphishing Email)	Diffusione iniziale tramite email di phishing mirate agli utenti.
T1190	Exploit Public-Facing Application	Sfruttamento di vulnerabilità note in Drupal/WordPress per l'accesso iniziale.
T1059.006	Command and Scripting Interpreter: PowerShell	Utilizzo di PowerShell/jRAT come loader per eseguire codice maligno.
T1105	Ingress Tool Transfer	Download di payload aggiuntivi dai server C2 mascherati dietro Telegram.

Contromisure:

- Applicare patch di sicurezza (in particolare a CMS come Drupal e WordPress).
- Bloccare comunicazioni con server noti di Telegram bot sospetti. Utilizzare EDR con analisi comportamentale per individuare attivazioni insolite di web shell o script di rete.

- Segmentare la rete per limitare movimenti laterali e raccogliere intelligence su infrastrutture note dell'APT.

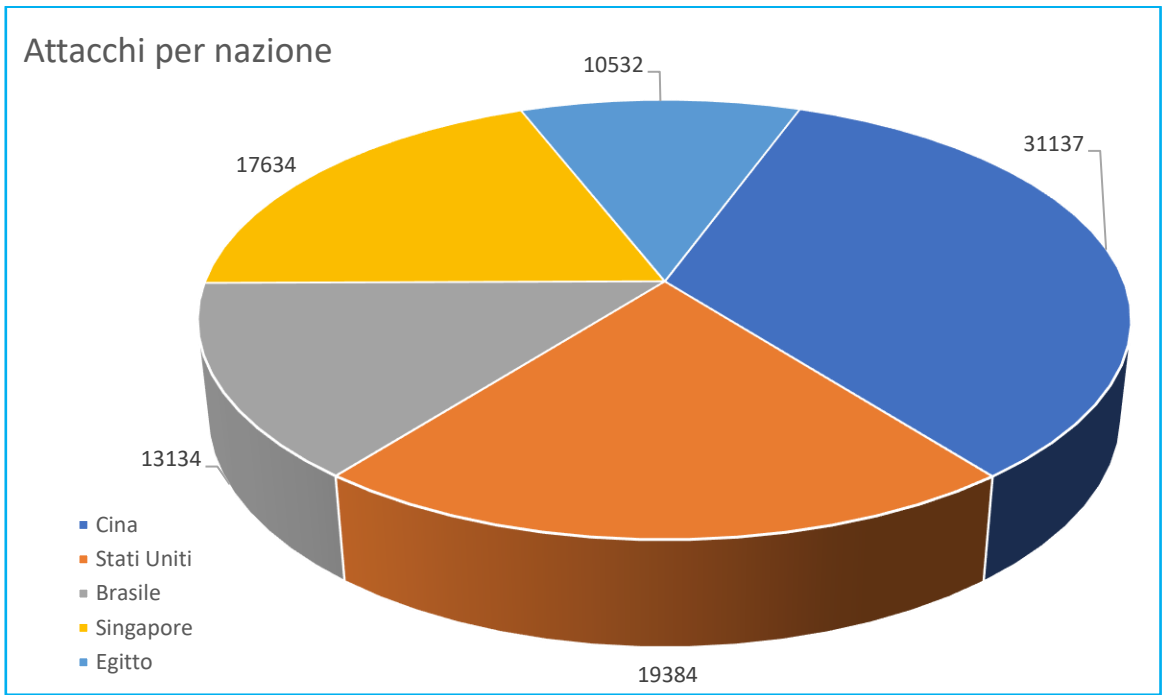
Livello di rischio: Alto (mirato a governi/industrie, con sofisticazione e raccolta dati su larga scala).

Riepilogo:

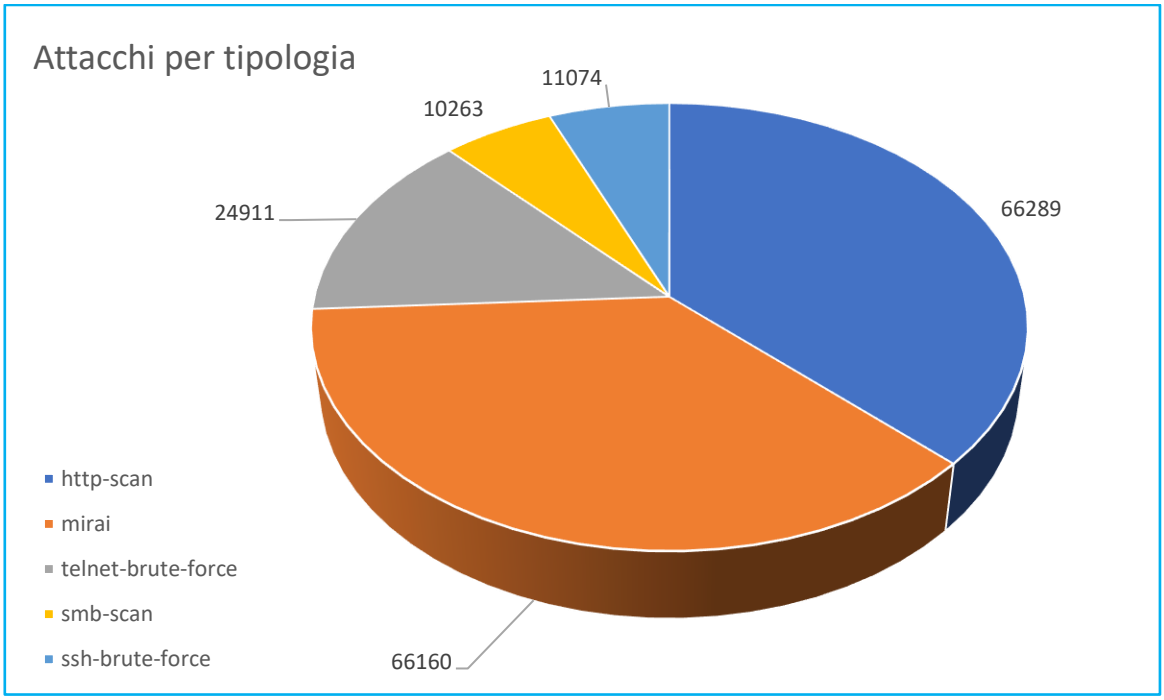
Malware	Categoria	Livello di rischio
Storm-0501	Ransomware (RaaS)	Alto
TamperedChef	Infostealer (Stealer credenziali)	Medio
ManualFinder Trojan	Trojan (proxy residenziale)	Medio
APT36 (Transparent Tribe)	APT/Spionaggio	Alto
ShadowSilk	APT/Spionaggio	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 15 – 21 Settembre, suddivisa per nazione e limitata alle prime cinque posizioni:

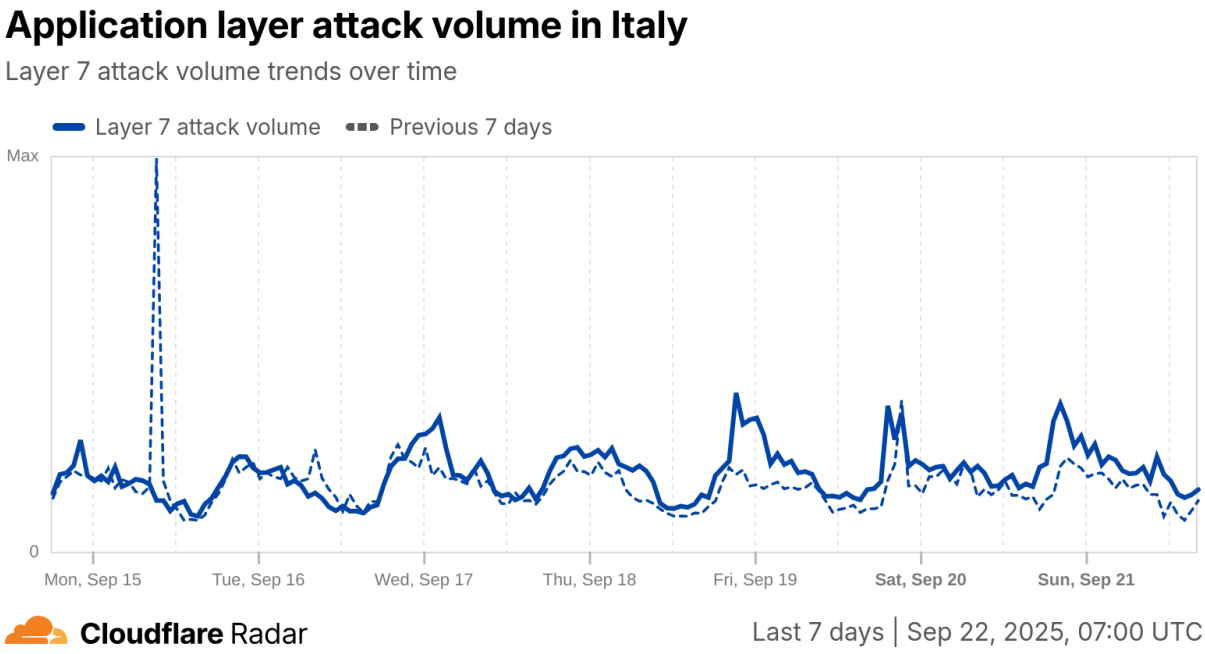


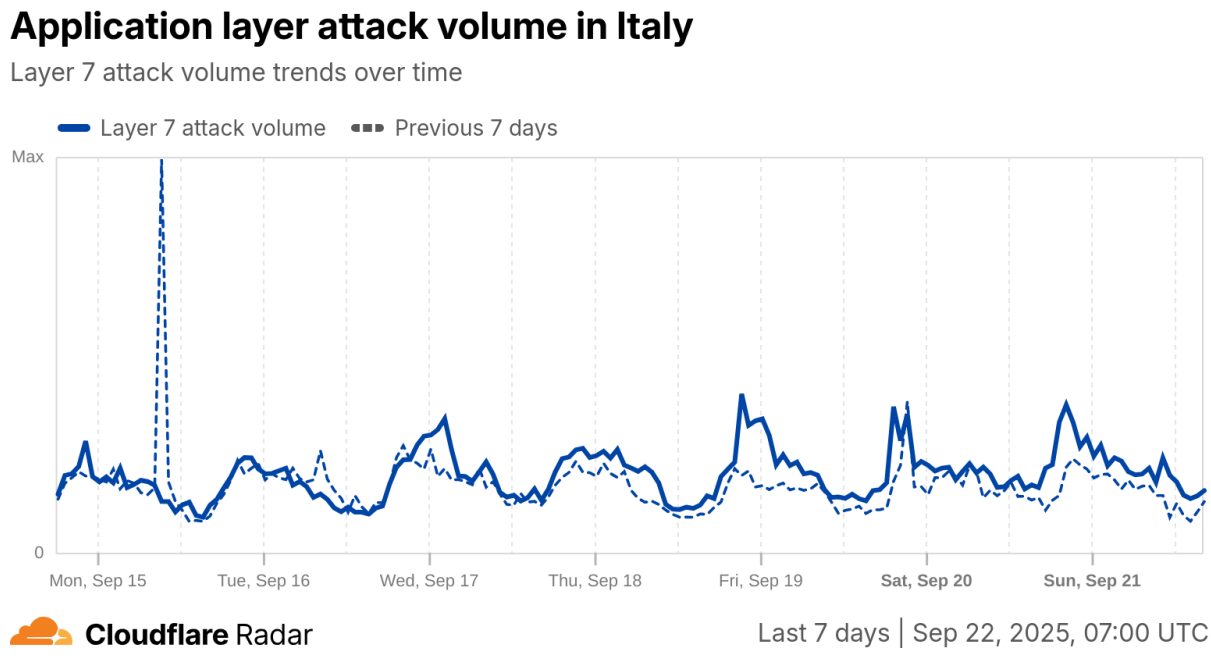
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
BMW GROUP	MONDO
DESCRIZIONE	Nei giorni scorsi, il gruppo Everest Ransomware ha rivendicato un attacco ai danni di BMW, affermando di aver sottratto circa 600.000 record di dati, tra cui documenti di audit interni. BMW ha confermato un incidente informatico, ma ha chiarito che ad essere stato colpito è un fornitore esterno (change2target) e non i propri sistemi centrali. Everest ha pubblicato alcuni documenti contenenti nomi, email e report relativi al periodo tra il 2021 e il 2025, ma resta incerta l'entità completa del leak. Il countdown pubblicato dagli hacker è scaduto e parte dei dati è stata effettivamente divulgata online. BMW ha bloccato gli accessi compromessi e sta indagando, ma non risultano al momento coinvolti dati sensibili di clienti.

TARGET	LOCALIZZAZIONE
PIEFFE AUTO GROUP	ITALIA
DESCRIZIONE	Il gruppo automobilistico italiano Pieffe Auto Group è stato vittima di un data breach rilevato il 18 settembre 2025, che ha interessato il dominio pieffeautogroup.it. Al momento, non sono stati resi noti dettagli precisi sull'entità della violazione né sul tipo di dati compromessi, ma l'incidente è stato confermato da diverse fonti affidabili. Non risultano ancora comunicazioni ufficiali da parte di Pieffe Auto Group o dalle autorità competenti, né conferme sulla natura dei dati sottratti. L'azienda ha probabilmente avviato indagini interne per valutare l'impatto e mettere in sicurezza i sistemi.

TARGET	LOCALIZZAZIONE
PLAZA DENTAL GROUP	STATI UNITI
DESCRIZIONE	Il 19 settembre 2025, il gruppo dentistico statunitense Plaza Dental Group ha subito un attacco informatico attribuito al gruppo Obscura. L'incidente è stato rilevato lo stesso giorno, ma al momento non sono disponibili dettagli precisi sull'entità o il tipo di dati compromessi e non è chiaro se siano stati coinvolti dati sensibili dei pazienti o solo informazioni aziendali. Plaza Dental Group non ha ancora rilasciato comunicazioni ufficiali né sono intervenute autorità competenti sulla vicenda.

4.6 Defacement

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

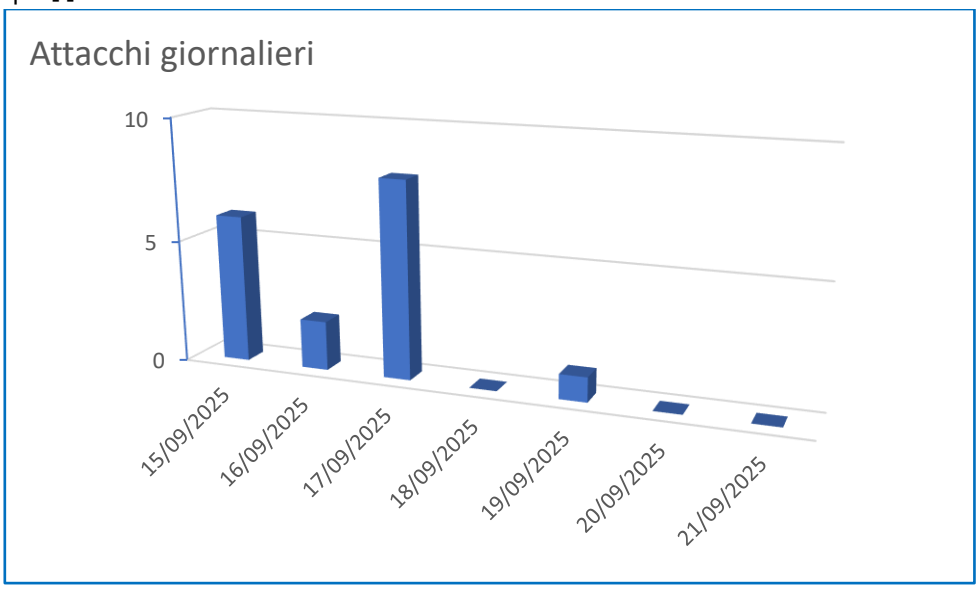


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

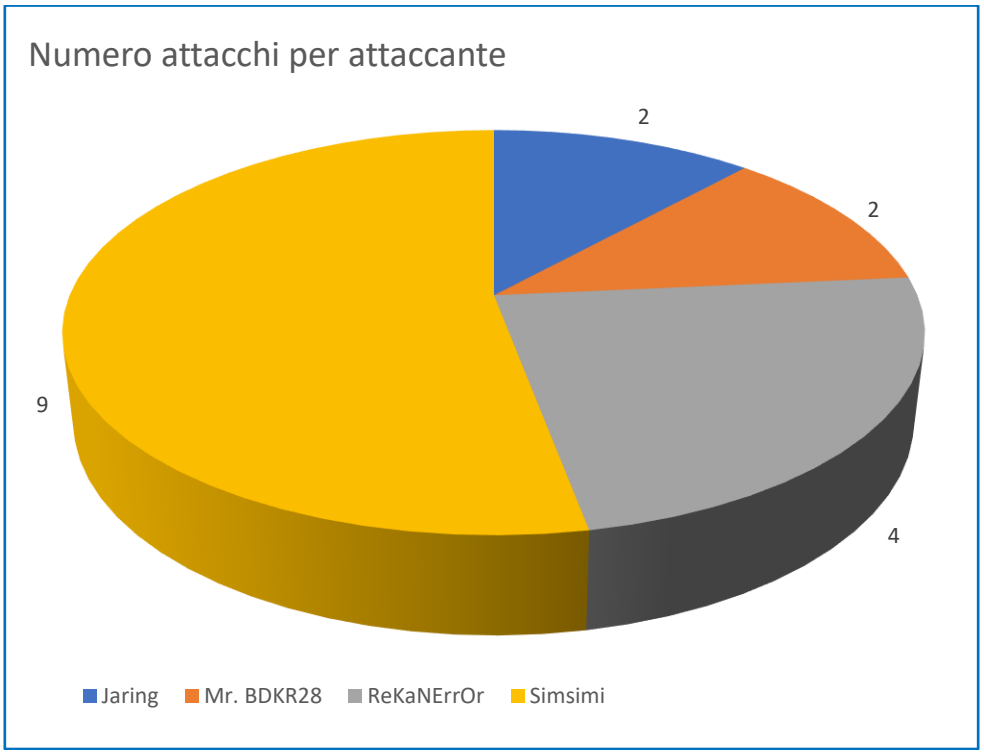


Figura 2: Defacement - Attaccanti più attivi nel periodo 15 – 21 Settembre

5 Honeypot

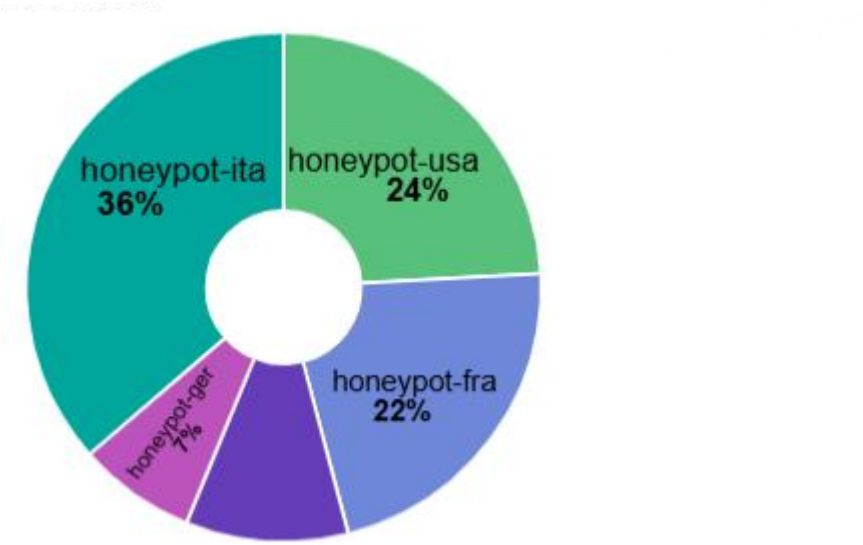
I seguenti dati sono raccolti da sistemi appositamente predisposti per la raccolta dei log sugli attacchi informatici (Honeypot). L'infrastruttura è composta da sensori honeypot dislocati nei principali paesi di interesse mondiale. Ad oggi, i sensori sono stati installati nei seguenti paesi: Italia, 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.

1.233.982 Attacks **7.293** Unique Src IPs **64** Unique HASSHs

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

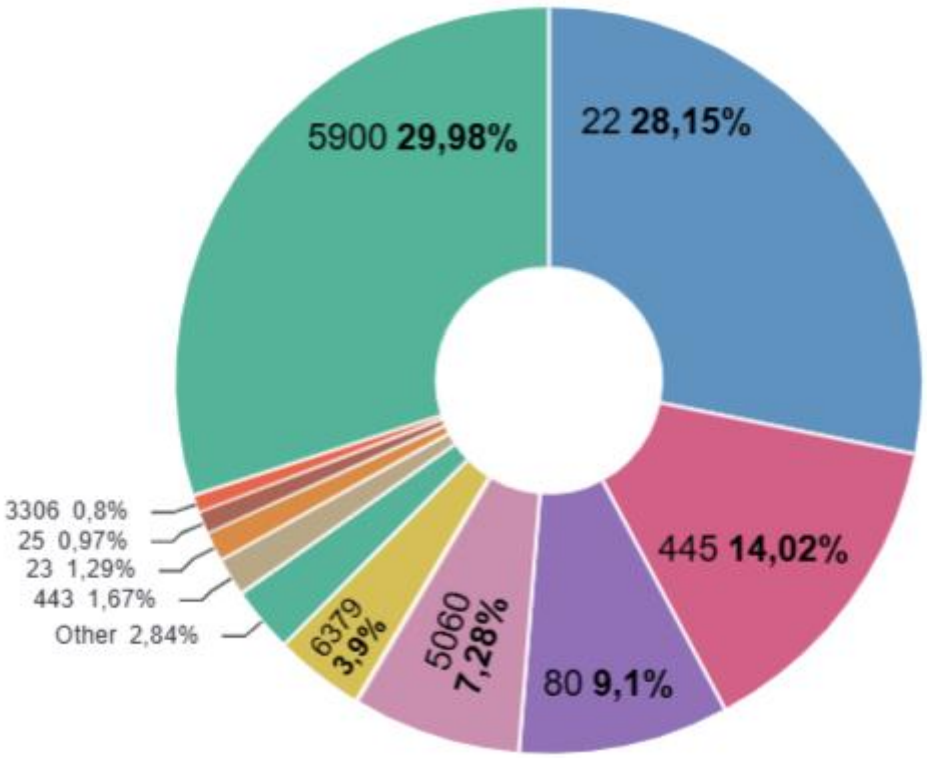


Questa invece la situazione a livello italiano:

449.029 Attacks **2.717** Unique Src IPs **48** Unique HASSHs

5.1.1 Attacchi ai servizi

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



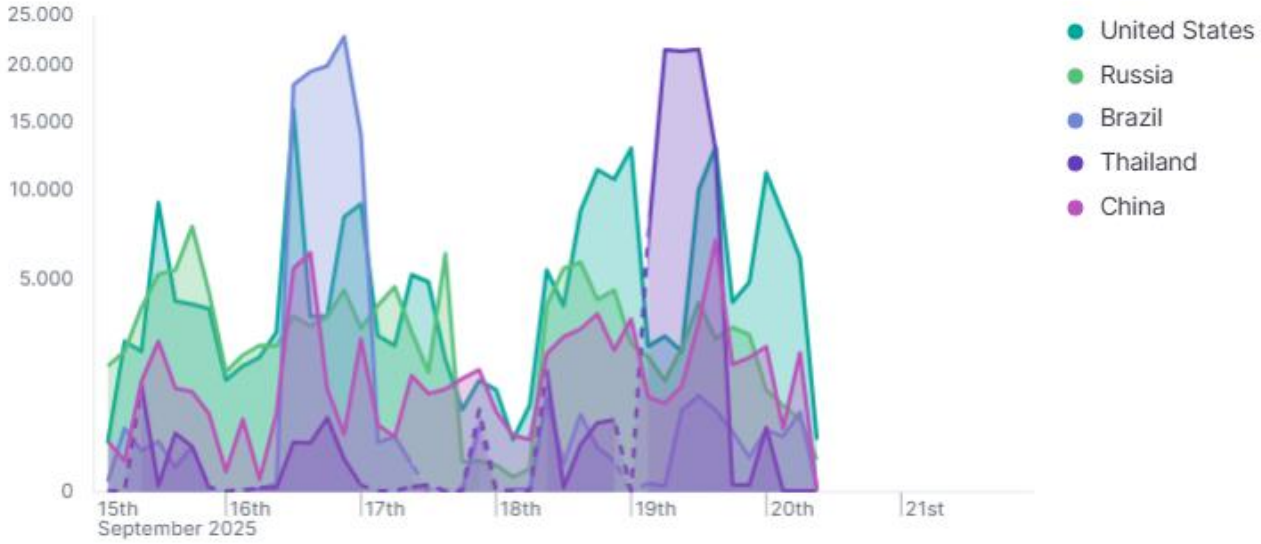
5.1.2 IP Attaccanti

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

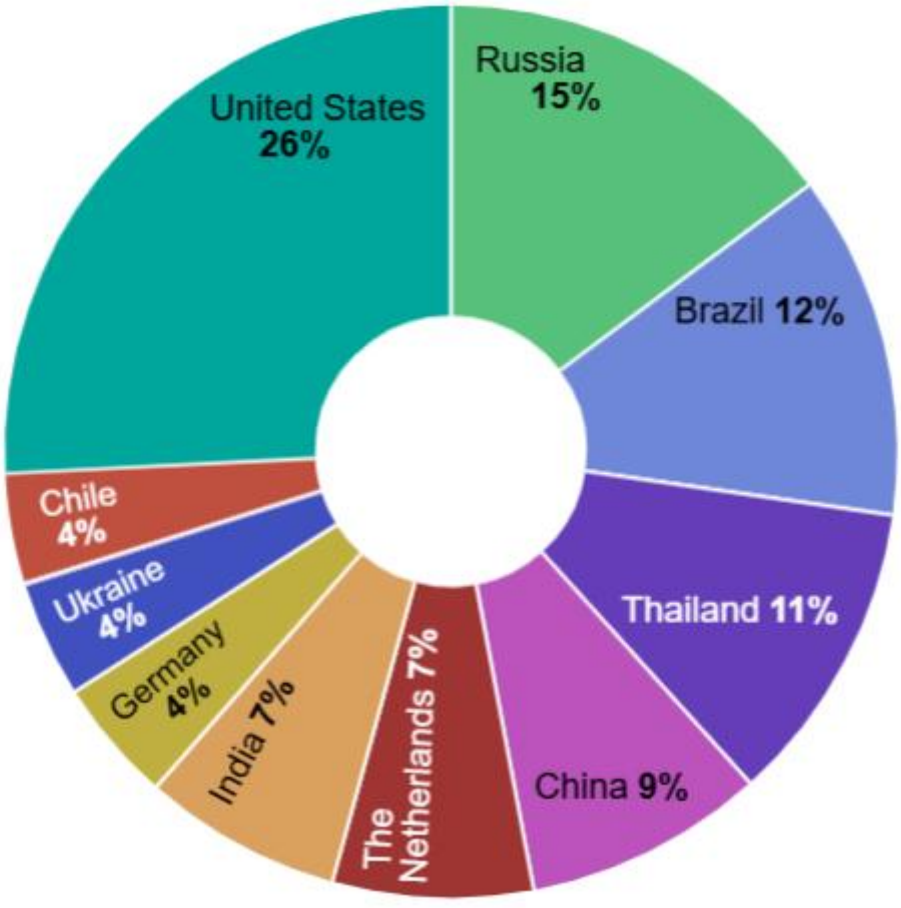
Source IP	Count
189.113.8.254	93.224
110.77.221.149	84.105
142.202.189.5	35.316
142.202.191.234	32.017
186.67.186.10	30.852
185.243.96.105	30.123
146.103.38.57	29.134
79.124.56.162	21.776
144.217.113.57	18.456
196.11.177.98	18.227

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:

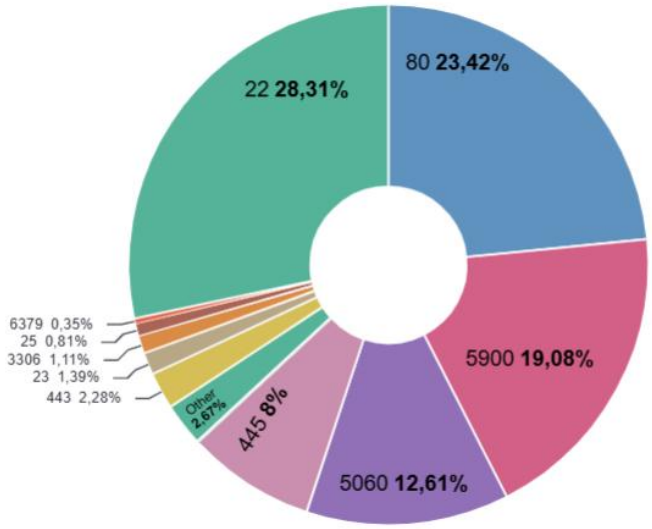


5.2 Italian Honeypot N.1

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	38.945
80	32.218
5900	26.245
5060	17.343
445	11.004
443	3.137
23	1.908
3306	1.521
25	1.108
6379	475

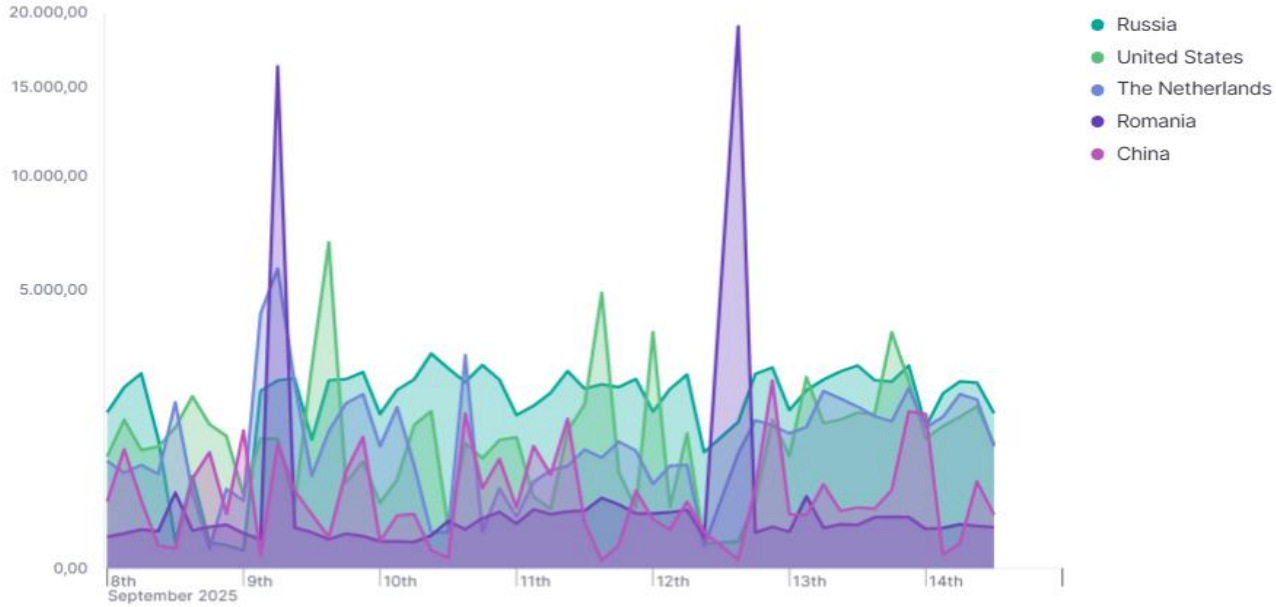
5.2.2 IP Attaccanti

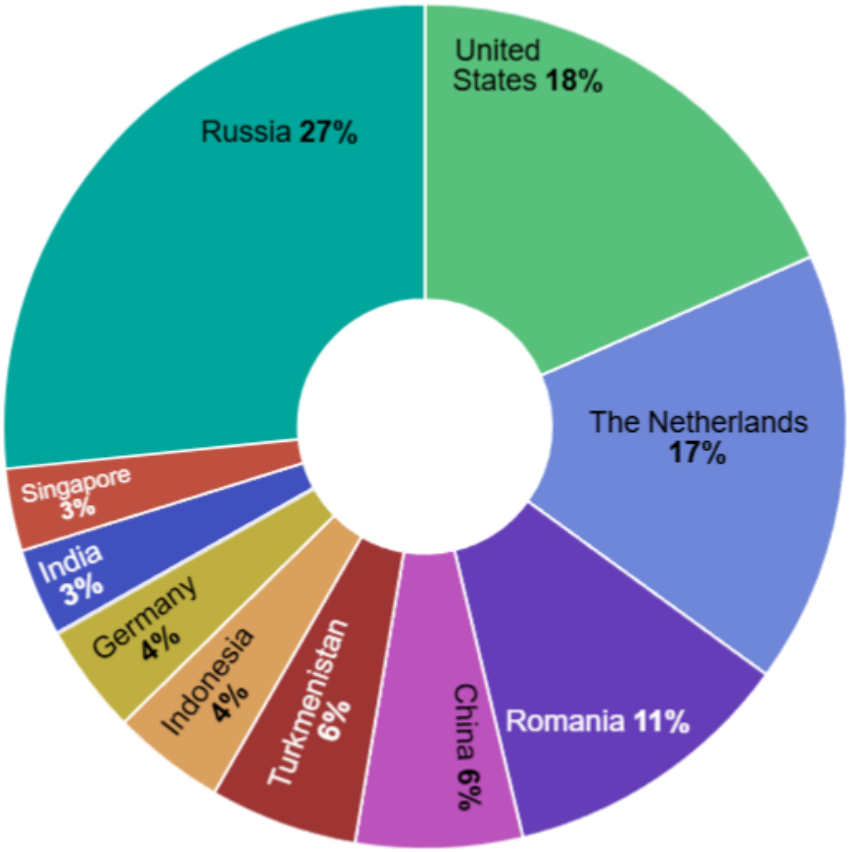
Questa invece la classifica relativa ai 10 IP che hanno effettuato il maggior numero di attacchi:

Source IP	Count
189.113.8.254	93.224
146.103.38.57	29.134
2.57.121.148	16.157
142.202.189.5	10.828
196.251.66.132	8.888
91.202.233.65	8.859
142.202.191.234	8.004
193.24.123.28	7.831
217.119.139.47	7.428
45.134.26.33	6.582

5.2.3 Paesi di provenienza degli attacchi

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



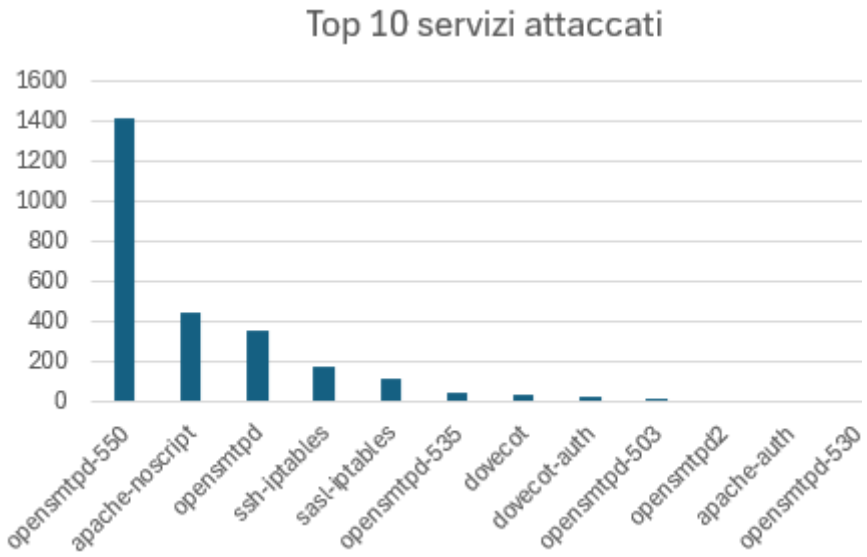

United States 18%
The Netherlands 17%
Romania 11%
China 6%
Turkmenistan 6%
Indonesia 4%
Germany 4%
India 3%
Singapore 3%
Russia 27%

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.



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

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

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

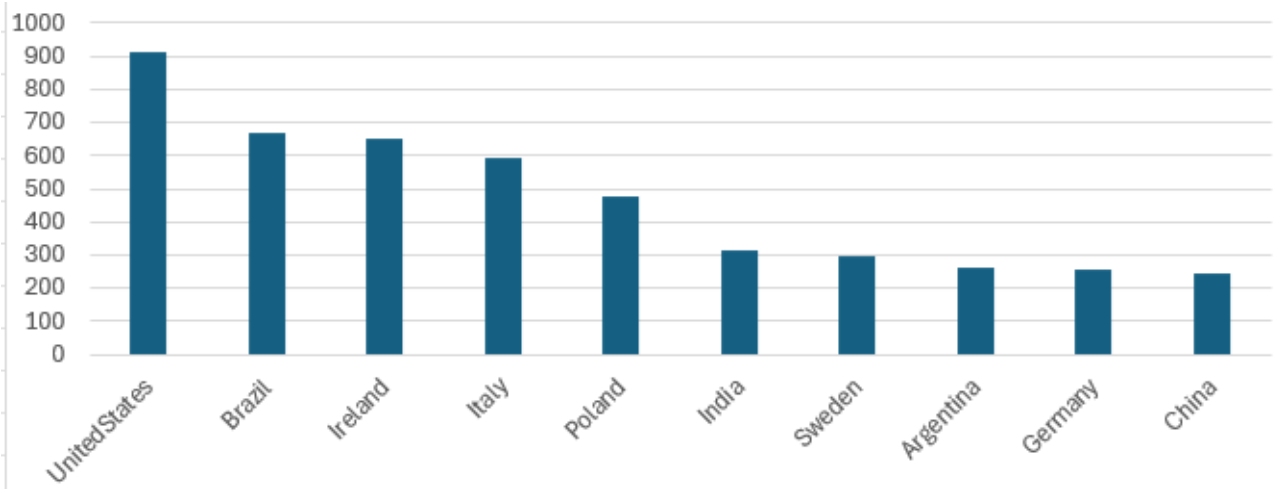
5.3.2 IP attaccanti

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

Source IP	Numero di attacchi
88[.]151[.]138[.]19	47
78[.]153[.]140[.]25	27
185[.]93[.]89[.]97	24
105[.]22[.]34[.]198	24
62[.]212[.]95[.]133	23
37[.]48[.]120[.]235	23
190[.]153[.]91[.]189	23
223[.]204[.]88[.]45	23
31[.]170[.]58[.]16	23
201[.]159[.]153[.]123	22

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