S3K

Cyber security

RISK REPORT

\ week 28.07.2025 - 03.08.2025

Sommario


CYBER SECURITY RISK REPORT
31/25

1 Il Cyber Security Risk Report S3K

Benvenuti al bollettino settimanale sulla sicurezza informatica, che copre il periodo dal 28 luglio al 3 agosto 2025. Questo rapporto, preparato dal team di analisti di S3K, offre una panoramica completa delle principali minacce cyber emerse nell'ultima settimana, fornendo approfondimenti su vulnerabilità, attacchi, tendenze e raccomandazioni per mitigare i rischi. Il documento è destinato a professionisti della sicurezza informatica e responsabili delle decisioni aziendali che necessitano di informazioni aggiornate e dettagliate per proteggere efficacemente le proprie infrastrutture digitali.

1.1 Come è strutturato il Cyber Security Risk Report

Il report è organizzato nelle seguenti sezioni principali:

Security News
Rilasci di aggiornamenti, patch e notizie dal mondo cyber, inclusi spionaggio informatico cinese in Africa, attacco ransomware Qilin e truffe tramite falsi SMS e social media.

CVE Monitor
Analisi delle vulnerabilità più impattanti, tendenze sui social media, nuove CVE emerse e quelle attivamente sfruttate dagli attaccanti.

Analisi Attacchi
Approfondimenti su phishing, ransomware, malware, DDoS, data breach e defacement, con analisi dettagliate e statistiche di distribuzione.

Honeypot
Dati raccolti dai sistemi honeypot di S3K, dislocati a livello globale, con focus particolare sugli attacchi diretti verso l'Italia.

1.2 Sommario delle principali notizie

Nuove CVE Critiche
Settimana segnata da exploit attivi su SharePoint Server, Cisco ISE e WebKit. Urgenza di applicare patch per vulnerabilità RCE non autenticate e privilege escalation root.

Campagne Malware
Rilevate nuove varianti: backdoor ApolloShadow per spionaggio diplomatico, DoubleTrouble per Android, JSCEAL per furto crypto e variante Linux del ransomware Gunra.

Attacchi Rilevanti
Qilin rivendica l'attacco al Consorzio Adige Po con conferma di esfiltrazione dati. Crescita degli attacchi di phishing bancario e truffe sui social network come il caso McDonald's.

1.3 Principali Vulnerabilità e Minacce della Settimana

Vulnerabilità Critiche in Evidenza

La settimana è stata caratterizzata da diverse vulnerabilità ad alto impatto che richiedono attenzione immediata. In particolare, le vulnerabilità su Microsoft SharePoint Server sono attivamente sfruttate dal ransomware ToolShell, mentre Cisco ISE presenta una grave falla che consente l'esecuzione di codice con privilegi root senza autenticazione. Anche Apple ha rilasciato aggiornamenti urgenti per tutti i suoi sistemi operativi per mitigare vulnerabilità di WebKit.

Top 5 CVE per Severità

CVE ID	Prodotto	CVSS v3
CVE-2025-53770	Microsoft SharePoint Server	9.8
CVE-2025-20281	Cisco Identity Services Engine	10.0
CVE-2025-3248	Langflow	9.8
CVE-2025-2776	SysAid On-Prem	9.8
CVE-2025-5777	Citrix NetScaler ADC	N/A

1.4 Principali Campagne Malware

ApolloShadow

Backdoor Windows utilizzata nella campagna "Secret Blizzard" attribuita a gruppi russi, che sfrutta una posizione man-in-the-middle nei provider russi per colpire sedi diplomatiche straniere a Mosca. Installa certificati root malevoli e permette spionaggio persistente.

DoubleTrouble

Trojan bancario per Android che si diffonde tramite canali Discord e siti fasulli di banche europee. Richiede permessi di Accessibilità per registrare l'interazione dell'utente e rubare credenziali da app bancarie e wallet crypto.

JSCEAL

Malware che si concentra su utenti di applicazioni di trading crypto, diffuso tramite malvertising su social e web. Utilizza un binario Node.js per eseguire codice JavaScript compilato che ruba credenziali e chiavi dei portafogli crypto.

Gunra (Linux)

Nuova variante Linux del ransomware Gunra che esegue fino a 100 thread di cifratura paralleli. Ha già colpito aziende in Brasile, Turchia, USA e altri paesi, prendendo di mira settori critici come sanità e manifatturiero.

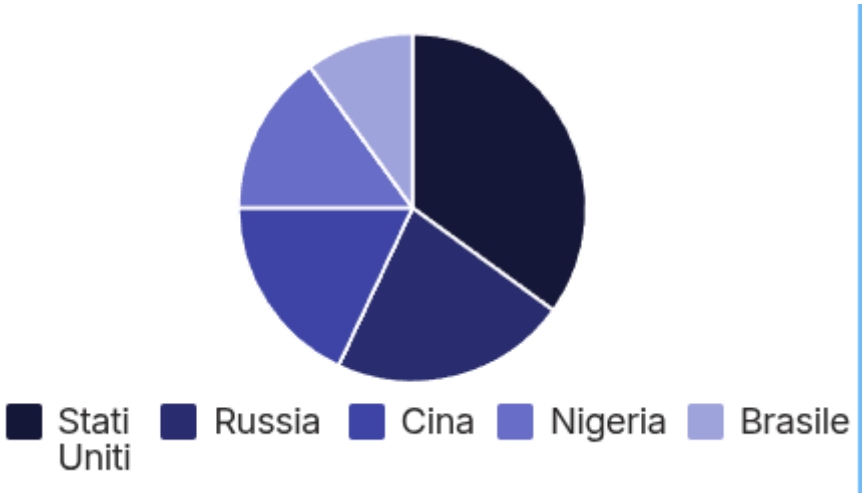
1.5 Cyber News in Evidenza

Il panorama delle minacce cyber continua a evolversi rapidamente, con gruppi di attaccanti che perfezionano le loro tecniche e ampliando i loro obiettivi. Il gruppo APT41, con presunti legami con la Cina, ha avviato una nuova campagna di spionaggio digitale rivolta ai sistemi informatici governativi di alcuni Paesi africani, area finora considerata poco rilevante per operazioni di questo tipo. Parallelamente, il gruppo ransomware Qilin ha rivendicato l'attacco al Consorzio di Bonifica Adige Po, confermando l'esfiltrazione di dati sensibili. Sul fronte delle truffe, sono emersi sia falsi SMS dai CAF che inducono le vittime a chiamare numeri a pagamento, sia una sofisticata frode su Instagram e Facebook che ha colpito oltre 10.000 persone con una falsa promozione di McDonald's.

1.6 Analisi degli Attacchi e Raccomandazioni Distribuzione Attacchi per Tipologia

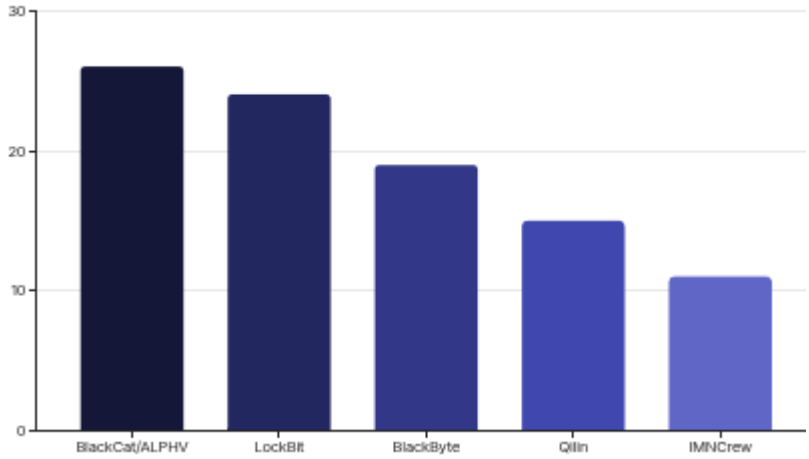
Phishing

L'analisi delle campagne di phishing della settimana evidenzia una sofisticazione crescente nelle tecniche di inganno. Un caso esemplare è la mail "Notifica di messaggi in quarantena sul tuo account Webmail", che utilizza una catena di reindirizzamenti attraverso domini compromessi per arrivare a una pagina di phishing che simula il portale webmail aziendale. Gli attacchi sfruttano sistematicamente l'assenza di protezioni SPF/DKIM/DMARC e utilizzano tecniche di social engineering per creare urgenza e indurre l'utente all'azione.



Ransomware

I gruppi ransomware più attivi nella settimana sono stati BlackCat/ALPHV, LockBit e BlackByte, con un significativo aumento delle attività rispetto alla settimana precedente. BlackCat ha mostrato un incremento particolarmente preoccupante, superando del 45% il numero di attacchi della settimana precedente, confermandosi come una delle minacce più persistenti nel panorama attuale.



Attività Honeypot

I sistemi honeypot di S3K hanno registrato un significativo aumento degli attacchi provenienti principalmente da Stati Uniti, Russia e Cina, con un totale di oltre 350.000 tentativi di intrusione nella settimana. In Italia, gli honeypot hanno evidenziato una concentrazione di attacchi verso i servizi SSH (22), HTTP/HTTPS (80/443) e Telnet (23), con un incremento del 28% rispetto alla settimana precedente. Gli IP più attivi sono stati identificati e tracciati, con una predominanza di attacchi provenienti da subnet note per attività malevole.

1.7 Raccomandazioni di Sicurezza

Aggiornamenti Prioritari

Applicare immediatamente le patch per SharePoint Server (protezione da ToolShell)
Aggiornare Cisco ISE alle versioni 3.3 patch 7 o 3.4 patch 2
Aggiornare tutti i dispositivi Apple (iOS, macOS, tvOS, visionOS, watchOS) alle ultime versioni
Installare gli aggiornamenti Autodesk Shared Components 2026.2 per tutti i prodotti interessati

Protezione Anti-Phishing

Abilitare SPF, DKIM e DMARC con politica reject sui domini aziendali
Bloccare ai gateway email i domini e gli IP identificati come malevoli nel report
Implementare autenticazione a più fattori (MFA) per tutti gli accessi critici
Formare gli utenti sul riconoscimento delle tecniche di phishing più recenti

Mitigazione Ransomware

Creare e testare regolarmente backup offline e non accessibili dalla rete principale
Segmentare la rete per limitare la propagazione laterale in caso di compromissione
Monitorare attivamente gli indicatori di compromissione (IoC) relativi a ToolShell e Gunra
Implementare soluzioni EDR con capacità di rilevamento comportamentale

Controlli Dispositivi Mobili

Vietare l'installazione di app da fonti non ufficiali
Implementare soluzioni Mobile Threat Defense (MTD) sui dispositivi aziendali
Sensibilizzare gli utenti sulle richieste sospette di permessi di Accessibilità
Monitorare anomalie nei pattern di traffico dati dei dispositivi mobili

1.8 Conclusioni

Il panorama delle minacce cyber continua a evolversi con rapidità e sofisticazione crescenti. La settimana ha evidenziato l'importanza di un approccio proattivo alla sicurezza, con particolare attenzione all'applicazione tempestiva delle patch di sicurezza, al monitoraggio continuo delle infrastrutture e alla formazione degli utenti. Le vulnerabilità in SharePoint Server e Cisco ISE rappresentano minacce particolarmente critiche che richiedono un'azione immediata, mentre l'emergere di nuove varianti malware come ApolloShadow e la versione Linux di Gunra sottolineano la necessità di strategie di difesa adattive e multiclivello. Le organizzazioni dovrebbero rivedere regolarmente le proprie posture di sicurezza alla luce di queste minacce emergenti e implementare le raccomandazioni fornite in questo report per migliorare la propria resilienza cyber.
Per ulteriori informazioni o assistenza sulle minacce descritte in questo report, contattare il team S3K all'indirizzo contattaci@s3kgroup.it o insidesales@s3kgroup.it.

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Apple	Apple ha rilasciato aggiornamenti di sicurezza per sanare molteplici vulnerabilità presenti nei propri prodotti. Versioni affette: • macOS Sequoia, versioni precedenti alla 15.6 • macOS Sonoma, versioni precedenti alla 14.7.7 • macOS Ventura, versioni precedenti alla 13.7.7 • Safari, versioni precedenti alla 18.6 • iOS, versioni precedenti alla 18.6 • iPadOS, versioni precedenti alla 18.6 • tvOS, versioni precedenti alla 18.6 • visionOS, versioni precedenti alla 2.6 • watchOS, versioni precedenti alla 11.6
ULR/Note	https://support.apple.com/en-sg/124147 https://support.apple.com/en-sg/124148 https://support.apple.com/en-sg/124149 https://support.apple.com/en-sg/124150 https://support.apple.com/en-sg/124151 https://support.apple.com/en-sg/124153 https://support.apple.com/en-sg/124154 https://support.apple.com/en-sg/124155 https://support.apple.com/en-us/100100 https://support.apple.com/en-us/124152

PRODOTTO	DESCRIZIONE
Autodesk	Autodesk risolve molteplici vulnerabilità di sicurezza con gravità "alta" in Autodesk Shared Components, componenti condivise utilizzate nei prodotti AutoCAD, Advance Steel, 3ds Max, Civil 3D, InfraWorks, Inventor, Revit e Vault. Tali vulnerabilità, qualora sfruttate, potrebbero consentire ad un utente malintenzionato di eseguire codice arbitrario, accedere ad informazioni sensibili, manomettere i dati e/o causare l'indisponibilità del servizio sui sistemi target. Versioni affette: • Revit 2026, Autodesk Shared Components 2026.2 • Revit LT 2026, Autodesk Shared Components 2026.2 • Vault 2026, Autodesk Shared Components 2026.2 • Advance Steel 2026, Autodesk Shared Components 2026.2 • 3ds Max 2026, Autodesk Shared Components 2026.2 • Civil 3D 2026, Autodesk Shared Components 2026.2 • InfraWorks 2026, Autodesk Shared Components 2026.2 • Inventor 2026, Autodesk Shared Components 2026.2 • AutoCAD 2026 toolset: ○ Achitecture 2026, Autodesk Shared Components 2026.2 ○ Electrical 2026, Autodesk Shared Components 2026.2 ○ Mechanical 2026, Autodesk Shared Components 2026.2 ○ MEP 2026, Autodesk Shared Components 2026.2 ○ Plant 3D 2026, Autodesk Shared Components 2026.2 ○ Map 3D 2026, Autodesk Shared Components 2026.2
ULR/Note	https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0015

PRODOTTO	DESCRIZIONE
IBM Db2	Aggiornamenti di sicurezza risolvono molteplici vulnerabilità, di cui una con gravità "alta", in Db2, noto relational database management system della IBM. Tale vulnerabilità, qualora sfruttata, potrebbe permettere a un utente malintenzionato di compromettere la disponibilità del servizio e di eseguire codice arbitrario sui sistemi interessati. Versioni affette: • 12.1.x, versioni precedenti alla 12.1.1 Special Build #62100 • 11.5.x, versioni precedenti alla 11.5.9 Special Build #62071
ULR/Note	https://www.ibm.com/support/pages/node/7240940 https://www.ibm.com/support/pages/published-security-vulnerabilities-db2-linux-unix-and-windows-including-special-build-information

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

SPIONAGGIO INFORMATICO CINESE IN AFRICA: SCOPERTA UN'OPERAZIONE DI APT41

Il gruppo APT41, un collettivo di cybercriminali con presunti legami con la Cina, ha avviato una nuova campagna di spionaggio digitale rivolta ai sistemi informatici governativi di alcuni Paesi africani, una mossa sorprendente dato che l'area era finora considerata poco rilevante per operazioni di questo tipo. L'attacco è stato individuato dagli esperti di sicurezza di Kaspersky, che hanno rilevato comportamenti anomali su alcuni terminali appartenenti ad un'organizzazione non specificata. Gli autori dell'intrusione hanno fatto uso di strumenti di accesso remoto e comandi personalizzati per mantenere attivi i propri server di comando all'interno della rete compromessa. L'accesso iniziale è avvenuto attraverso un host difficile da tracciare, sul quale è stato sfruttato il framework Impacket, in particolare i moduli Atexec e WmiExec, all'interno di un account di servizio. Dopo una fase iniziale di attività, gli attaccanti hanno interrotto temporaneamente le operazioni, per poi riprenderle sfruttando credenziali con privilegi elevati. Ciò ha permesso loro di muoversi lateralmente nella rete, impiegando anche Cobalt Strike, un noto tool di penetration testing, distribuito tramite la tecnica del DLL sideloading. Uno degli aspetti distintivi del malware impiegato è la sua capacità di riconoscere la lingua del sistema operativo: se viene rilevato l'uso del cinese (tradizionale o semplificato), del giapponese o del coreano, il codice malevolo si arresta. Questa misura sembra studiata per evitare infezioni accidentali nei paesi di origine degli sviluppatori. Gli aggressori hanno anche sfruttato SharePoint Server presente nell'ambiente target, trasformandolo in un nodo di comando e controllo. Le operazioni dannose venivano mascherate come traffico aziendale lecito. Da lì, comandi remoti venivano impartiti ad un trojan scritto in C#, installato nel sistema tramite i file "agents.exe" e "agentx.exe", distribuiti attraverso il protocollo SMB. Questi programmi interagivano con la web shell "CommandHandler.aspx" installata su SharePoint, fungendo da canale esecutivo per i comandi degli attaccanti. L'intera operazione ha combinato metodi classici di compromissione con strategie tipiche del modello "Living off the Land", che prevede l'uso di strumenti e servizi legittimi già presenti nel sistema per mimetizzare le attività malevole. Le tecniche impiegate rientrano nei profili MITRE ATT&CK T1071.001 e T1047, rendendo complesso il rilevamento tramite difese tradizionali. Successivamente, l'attività si è focalizzata su dispositivi e risorse di interesse strategico. In questa fase, attraverso script avviati da "cmd.exe", venivano scaricati file HTA da fonti esterne camuffate come repository ufficiali su GitHub. Anche se il funzionamento preciso di questi file rimane in parte sconosciuto, è stato verificato che uno di questi script era in grado di stabilire una reverse shell, offrendo accesso remoto completo al sistema. Per quanto riguarda la raccolta di dati, il gruppo ha utilizzato un'ampia varietà di strumenti. Una versione modificata di Pillager ha permesso di sottrarre password, documenti, messaggi e-mail, screenshot e altri dati sensibili. Il tool Checkout, invece, era impiegato per acquisire informazioni su file scaricati e dati di pagamento da browser come Chrome, Opera, Brave e altri. Con l'utility RawCopy venivano estratti i log di sistema non ancora processati, mentre Mimikatz veniva utilizzato per esfiltrare credenziali direttamente dalla memoria. APT41 ha evidenziato un'elevata capacità di adattamento, modificando il codice malevolo in funzione della configurazione della rete attaccata. Inoltre, il mix di strumenti legittimi e software personalizzato ha contribuito a rendere l'azione difficile da distinguere da normali attività interne. Questa incursione segna un cambiamento importante nel focus geografico del gruppo, che ora dimostra interesse per territori finora poco presi di mira. Secondo quanto rilevato da Trend Micro, i primi segnali di

un'espansione delle operazioni verso l'Africa erano già comparsi verso la fine del 2022. L'utilizzo di infrastrutture aziendali interne per gestire le comunicazioni e l'esfiltrazione dati riflette un'evoluzione nelle tecniche offensive, dove i confini tra attività simulate (pentest) e veri attacchi diventano sempre più sfumati.

QILIN RIVENDICA L'ATTACCO AL CONSORZIO ADIGE PO: CONFERMATA LA FUGA DI DATI

Il 31 luglio 2025 il Consorzio di Bonifica Adige Po ha diffuso un nuovo comunicato destinato ai cittadini ed agli utenti coinvolti, confermando ufficialmente che il cyberattacco subito a inizio mese è stato rivendicato dal gruppo ransomware Qilin. Oltre alla rivendicazione, il gruppo criminale ha pubblicato una selezione di documenti esfiltrati contenenti dati sensibili e informazioni riservate, a riprova della compromissione. Nel messaggio più recente, l'Ente fornisce alcuni dettagli sull'accaduto e invita alla prudenza, fornendo raccomandazioni concrete ai soggetti potenzialmente coinvolti. Pur riconoscendo la gravità della situazione, il Consorzio mantiene un tono responsabile e rassicurante, ribadendo l'impegno alla trasparenza e alla comunicazione continua. "Consideriamo questo episodio non solo un attacco ai nostri sistemi, ma un'aggressione alla comunità che serviamo. Continueremo ad informare tempestivamente sull'evoluzione della vicenda, attivando ogni misura utile per contenere i rischi e rafforzare le difese digitali." Questo approccio, improntato alla responsabilità e alla chiarezza, riflette una scelta comunicativa non sempre scontata da parte delle istituzioni pubbliche. Il Consorzio sottolinea inoltre che, se necessario, verrà predisposto un canale diretto per l'assistenza agli utenti. La catena di eventi ha avuto inizio a fine giugno con una prima comunicazione sul sito ufficiale dell'Ente, seguita, il 3 luglio, da un annuncio in cui veniva reso noto che i sistemi informativi gestionali e amministrativi erano stati colpiti da un attacco informatico. Il messaggio, già allora, aveva attirato l'attenzione per il tono diretto e privo di ambiguità: "L'operatività sul territorio non è mai stata compromessa. L'attacco è stato gestito prontamente secondo i protocolli, con il supporto di esperti in sicurezza." A distanza di pochi giorni, il 7 luglio, il Consorzio ha dichiarato di aver avviato un progressivo ripristino delle funzionalità digitali, rassicurando che i servizi essenziali non avevano subito interruzioni. Tuttavia, il 10 luglio è arrivata la rivendicazione ufficiale da parte del gruppo Qilin, tramite il loro data leak site, dove sono stati pubblicati i primi file a conferma dell'avvenuta esfiltrazione. Al momento, restano ignote sia la quantità complessiva di dati trafugati sia eventuali termini di un countdown per la pubblicazione integrale. Ma la gestione dell'incidente, almeno sul piano comunicativo, mostra un livello di maturità non comune nel panorama pubblico italiano, spesso restio a condividere apertamente incidenti informatici. Infine, rimane da valutare quale sarà la risposta delle autorità garanti in materia di protezione dei dati personali. Un eventuale provvedimento del Garante Privacy potrà tenere conto anche dell'approccio trasparente adottato, che ha contribuito ad informare tempestivamente gli interessati, mitigando almeno in parte il potenziale danno reputazionale.

FALSI SMS DAI CAF: TRUFFA AI DANNI DEI CONTRIBUENTI TRAMITE NUMERI A PAGAMENTO

Negli ultimi giorni diversi Centri di Assistenza Fiscale italiani, tra cui CAF CIA, CAF UIL e CAF CISL, hanno segnalato un'ondata di SMS sospetti ricevuti da propri clienti, in cui un presunto "CAF Centro Assistenza Formativa" invita a chiamare con urgenza un numero a pagamento con prefisso 893, noto per applicare tariffe maggiorate rispetto ad una chiamata standard. A riportare la vicenda è stato Massimo Tenaglia del CED Nazionale di Caf Cia srl, ma il fenomeno sembra estendersi rapidamente. Il messaggio punta chiaramente a sfruttare la fiducia che i cittadini ripongono nei CAF per indurre le vittime a contattare un servizio truffaldino, con lo scopo di generare guadagni illeciti. Ciò che rende la situazione particolarmente allarmante è il fatto che i numeri di telefono coinvolti risultano effettivamente appartenere a clienti reali, persone che hanno usufruito recentemente dei servizi fiscali offerti dai CAF, facendo ipotizzare un'esfiltrazione mirata di dati. Secondo alcune testimonianze interne al settore, è improbabile che la violazione sia avvenuta direttamente nei sistemi dei CAF, mentre appare più plausibile che a essere stati compromessi siano i sistemi dei fornitori informatici, come software house che gestiscono piattaforme per la compilazione dei modelli fiscali, portali di prenotazione o servizi cloud per l'archiviazione dei documenti. Un attacco di questo tipo si inserirebbe in uno schema già noto in altri settori, dove i cybercriminali colpiscono infrastrutture esterne per ottenere accesso a dati sensibili senza attaccare direttamente le organizzazioni principali. In alternativa, non si può escludere che i numeri siano stati ricavati da combinazioni di dati già trafugati in passato e poi rivenduti nel dark web o aggregati tramite malware infostealer, in grado di carpire informazioni direttamente dai dispositivi infetti degli utenti. Questo rende estremamente difficile risalire all'origine esatta della violazione, poiché i dati potrebbero essere transitati attraverso molteplici canali e compromissioni nel tempo. L'intera vicenda evidenzia quanto sia cruciale rafforzare la sicurezza non solo dei singoli CAF, ma anche dell'intero ecosistema digitale che ruota intorno alla gestione dei dati fiscali, richiedendo maggiore collaborazione tra centri di assistenza, fornitori tecnologici e autorità competenti per prevenire attacchi futuri e tutelare la privacy dei cittadini.

10.000 PERSONE TRUFFATE SU INSTAGRAM E FACEBOOK TRAMITE UNA FALSA PROMO MCDONALD'S

In un periodo in cui le truffe online si moltiplicano rapidamente, la Romania si è trovata al centro di una frode digitale su vasta scala camuffata da promozione di McDonald's. Più di 10.000 utenti sono caduti nella trappola di un'offerta apparentemente irresistibile: un pasto completo, hamburger, patatine e bibita, a soli 10 lei, l'equivalente di circa due dollari. Sui social, in particolare su Instagram e Facebook, sono apparsi annunci sponsorizzati pubblicati da un fantomatico marchio chiamato McDelight România, che simulava in modo credibile lo stile comunicativo di McDonald's. Gli utenti venivano invitati a partecipare ad un gioco a premi preceduto da un sondaggio, con la promessa che avrebbero potuto vincere una ricompensa. Naturalmente, tutti risultavano vincitori. Le pagine erano costruite per sembrare autentiche, arricchite da immagini accattivanti e false recensioni di presunti clienti soddisfatti. Dopo aver convinto le vittime della legittimità dell'offerta, la truffa entrava nella fase più insidiosa: un modulo da compilare con dati personali e della carta di credito, teoricamente per coprire una spesa simbolica. In realtà, nascosto tra le clausole scritte in caratteri quasi illeggibili, si celava un abbonamento da 63,42 euro ogni quattordici giorni, che cominciava ad addebitarsi regolarmente sulla carta inserita. Bitdefender, che ha scoperto e analizzato la campagna, ha confermato che l'operazione ha avuto inizio il 17 luglio e che gli annunci fraudolenti sono ancora attivi, con almeno sei varianti in circolazione e una diffusione già confermata anche in altri Paesi come l'Ungheria e i Paesi Bassi. Ciò che rende l'operazione particolarmente pericolosa è la sua capacità di sfruttare l'impatto visivo e psicologico del marketing online: urgenza, scarsità, estetica familiare e comunicazione studiata per colpire gli utenti più distratti o impulsivi. Gli esperti hanno ribadito che nessuna azienda reale chiederebbe oltre 60 euro ogni due settimane per un panino gratis, invitando gli utenti a diffidare da promozioni che richiedono pagamenti anticipati e a leggere sempre con attenzione le condizioni contrattuali. L'episodio dimostra quanto facilmente campagne pubblicitarie ingannevoli possano essere messe online anche a nome di brand famosi, eludendo i sistemi di sicurezza, anche quelli basati sull'intelligenza artificiale, delle piattaforme come Meta, e sottolinea l'importanza di un approccio più critico da parte degli utenti e di un controllo più severo da parte dei gestori.

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 28 Luglio – 4 Agosto 2025
Settimana segnata da exploit attivi su SharePoint Server, Cisco ISE e WebKit (Apple/Chrome). Aumenta l'urgenza patch per vulnerabilità RCE non autenticate e privilege escalation root.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Descrizione Sintetica
CVE-2025-53770	CRITICAL	30/07/2025	✅	SharePoint Server – RCE non autenticata sfruttata in ToolShell (ransomware).
CVE-2025-20337	CRITICAL	29/07/2025	✅	Cisco ISE – RCE root via API senza autenticazione (patch urgenti).
CVE-2025-6558	CRITICAL	01/08/2025	✅	WebKit/Chrome – Sandbox escape RCE attiva, patch Apple e Google.
CVE-2025-49704	CRITICAL	30/07/2025	✅	SharePoint – RCE autenticata da spoofing, parte della chain ToolShell.

Vendor e Tecnologie Coinvolti

- **Microsoft SharePoint:** exploit ToolShell – attacchi attivi con esecuzione codice da remoto e privilege escalation.
- **Cisco ISE:** vulnerabilità critiche su API, RCE root senza credenziali.
- **WebKit/Chrome/iOS/macOS:** zero-day in-the-wild per bypass sandbox e RCE.
- **WordPress Plugins:** vedi sezione precedente (settimana 1–4 luglio).

Distribuzione Giornaliera

- **29–30 luglio:** disclosure Cisco ISE + SharePoint RCE (ToolShell).
- **1 agosto:** zero-day WebKit attivamente sfruttata, advisory Apple + CISA.

Raccomandazioni

- **Patch Prioritarie:**
  - SharePoint Server (ToolShell): aggiornare e mitigare con AMSI + rotazione MachineKey.
  - Cisco ISE: applicare patch 7 (v3.3) o patch 2 (v3.4) immediatamente.
  - Chrome / iOS / macOS: aggiornare browser e dispositivi.
- **Mitigazioni e Controlli:**
  - Monitoraggio indicatori compromissione (IoC ToolShell, Warlock).
  - Audit API exposed su appliance Cisco.
  - Censimento e aggiornamento urgente SharePoint on-premises.

3.2 Tendenze

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

CVE ID	Prodotto	CVSS v3
CVE-2025-53770	Microsoft SharePoint Server (on-prem)	9.8
CVE-2025-5777	Citrix NetScaler ADC / Gateway	N/A
CVE-2025-20281	Cisco Identity Services Engine (ISE)	10
CVE-2025-3248	Langflow (Flodrix Botnet Target)	9.8
CVE-2025-2776	SysAid On-Prem - Unauthenticated XXE	9.8

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-2025-8529	cloudfavorites favorites-web	N/A
VULNERABILITÀ	È stata scoperta una vulnerabilità classificata come "critica" in cloudfavorites favorites-web fino alla versione 1.3.0. La funzione interessata è getCollectLogoUrl, nel file • app/src/main/java/com/favorites/web/CollectController.java. La vulnerabilità permette la manipolazione dell'argomento url e porta a una falla di tipo Server-Side Request Forgery (SSRF). L'attacco può essere lanciato da remoto. L'exploit è stato divulgato pubblicamente e potrebbe essere utilizzato.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-20337	Cisco ISE / Cisco ISE-PIC	9.8
VULNERABILITÀ	Una vulnerabilità in una specifica API di Cisco ISE e Cisco ISE-PIC potrebbe consentire a un attaccante remoto e non autenticato di eseguire codice arbitrario sul sistema operativo sottostante come root. L'attaccante non ha bisogno di credenziali valide per sfruttare questa vulnerabilità. La causa risiede in una convalida insufficiente dell'input fornito dall'utente. Un attaccante potrebbe sfruttare questa debolezza inviando una richiesta API appositamente modificata. Un attacco riuscito potrebbe consentire all'aggressore di ottenere i privilegi di root sul dispositivo interessato.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-6558	Google Chrome	N/A
VULNERABILITÀ	Una convalida insufficiente dell'input non attendibile in ANGLE e GPU su Google Chrome (versioni precedenti alla 138.0.7204.157) permetteva a un attaccante remoto di eseguire potenzialmente una "sandbox escape" tramite una pagina HTML appositamente creata. (Gravità di sicurezza di Chromium: Alta)	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-8371	Exam Form Submission 1.0	N/A
VULNERABILITÀ	È stata scoperta una vulnerabilità classificata come "critica" in code-projects Exam Form Submission 1.0. La falla si trova nel file /admin/update_s5.php, in una funzione non specificata, e permette una SQL injection attraverso la manipolazione dell'argomento credits. L'attacco può essere eseguito da remoto. L'exploit è stato reso pubblico e potrebbe essere già in uso.	

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-2025-20281
DESCRIZIONE	
Una vulnerabilità in una specifica API di Cisco ISE e Cisco ISE-PIC potrebbe consentire a un attaccante remoto non autenticato di eseguire codice arbitrario sul sistema operativo sottostante con privilegi root. L'attaccante non necessita di credenziali valide per sfruttare questa vulnerabilità. Questa vulnerabilità è causata da una convalida insufficiente dell'input fornito dall'utente.Un attaccante potrebbe sfruttarla inviando una richiesta API appositamente creata. Un exploit riuscito potrebbe consentire all'attaccante di ottenere privilegi root su un dispositivo vulnerabile.	

CVE	CVE-2025-2775
DESCRIZIONE	
Le versioni di SysAid On-Prem pari o inferiori alla 23.3.40 sono vulnerabili a una falla di tipo XML External Entity (XXE) che non richiede autenticazione. Questa vulnerabilità, presente nella funzionalità di elaborazione del "Checkin", consente a un aggressore di leggere file arbitrari e di compromettere l'account di amministratore.	

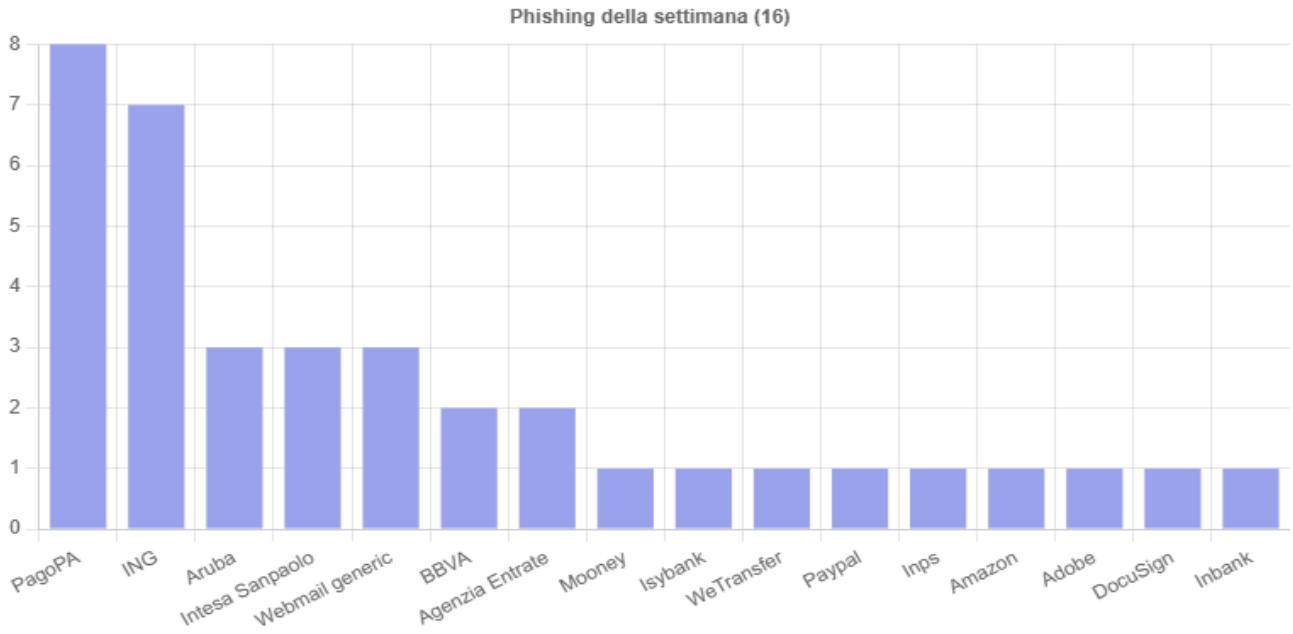
CVE	CVE-2023-2533
DESCRIZIONE	
È stata individuata una vulnerabilità di tipo Cross-Site Request Forgery (CSRF) in PaperCut NG/MF. In determinate condizioni, questa falla potrebbe permettere a un attaccante di modificare le impostazioni di sicurezza o di eseguire codice arbitrario. Lo sfruttamento della vulnerabilità richiederebbe che un amministratore con una sessione attiva venga ingannato e portato a cliccare su un link appositamente preparato, con conseguenti modifiche non autorizzate.	

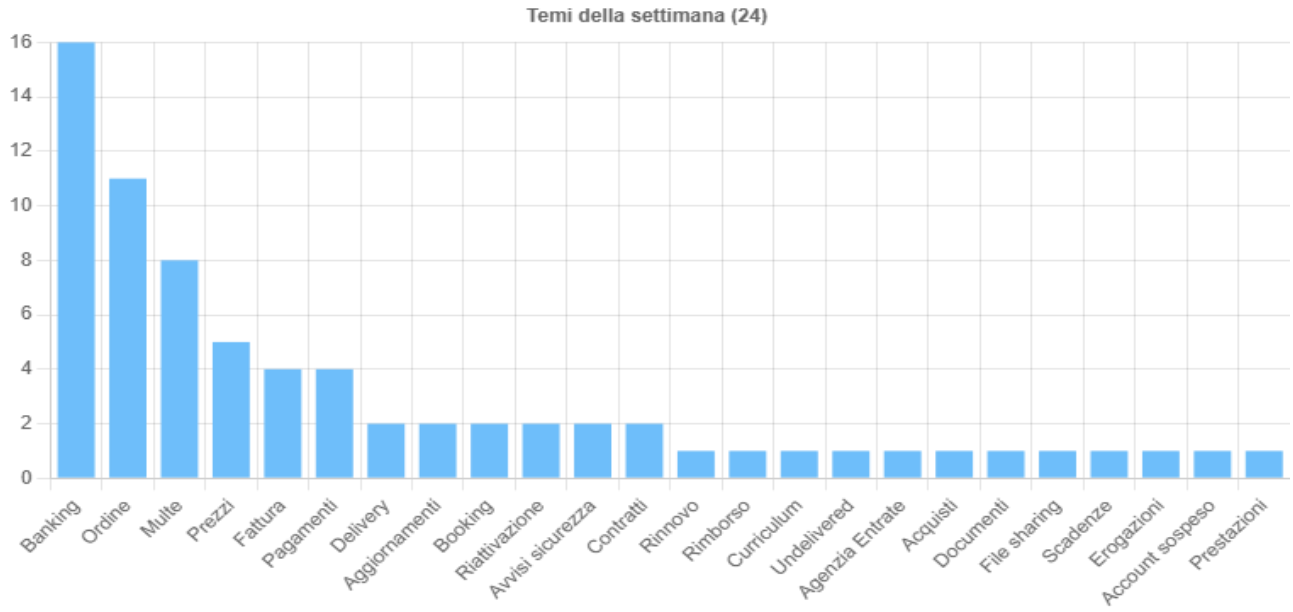
4 Attacchi

4.1 Phishing

Situazione italiana:

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

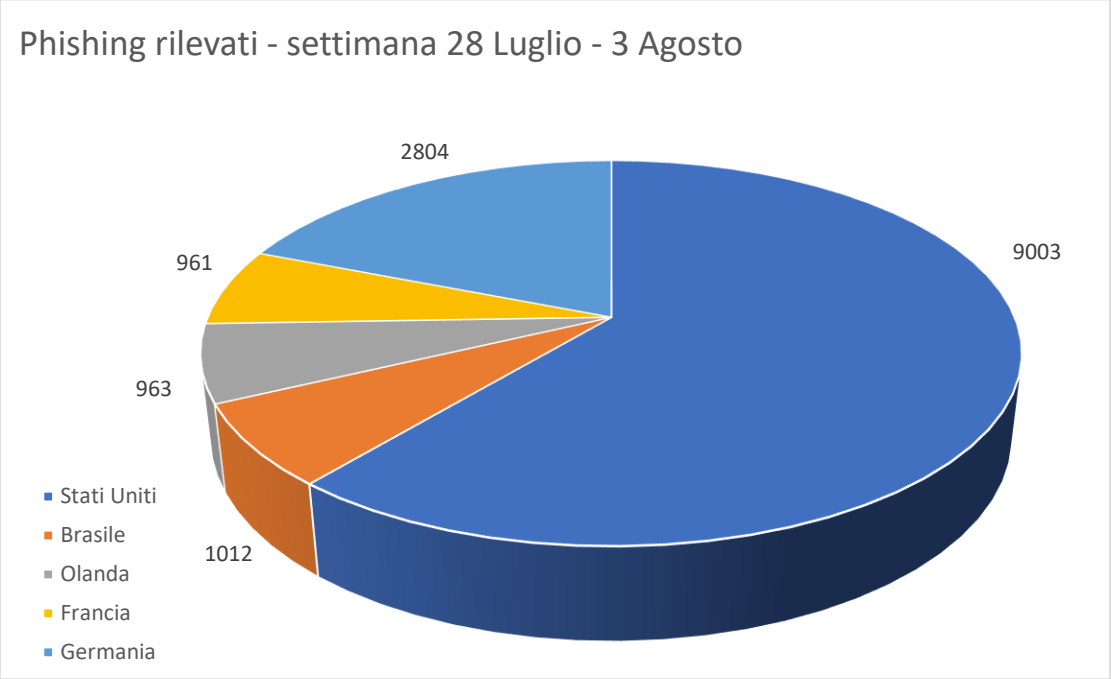




Fonte :CERT-AGID

Situazione Mondiale:

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



Analisi dettagliata di una mail di phishing:

Anche in questo m numero riportiamo un'analisi approfondita di una mail giunta all'attenzione della redazione di S3K.
L'email intitolata "Notifica di messaggi in quarantena sul tuo account Webmail" è un tentativo di phishing mirato alla raccolta credenziali: sfrutta un finto avviso di quarantena per spingere l'utente vittima@dominio_vittima[.]com a premere un pulsante che, attraverso un open-redirect sul dominio r.brandreward[.]com, atterra sulla pagina bandeirantesvistoria[.]com[.]br/lojaz che viene a sua volta reindirizzato su https://dieselecia[.]com[.]br/lojaz/wordpress/#account_vittima@dominio_vittima.com dove viene richiesto il login tramite una pagina che simula il sito reale della vittima – pagina classificata dai sandbox come malevola.
Gli header mostrano spoofing, assenza di SPF/DKIM/DMARC e catena SMTP che parte da 185[.]64[.]78[.]9 (AS396356 Latitude.sh) e transita per 161[.]132[.]109[.]138 (mail server peruviano di layconsa[.]com[.]pe). La combinazione di infrastruttura abusata, domini a bassa reputazione e tecniche di social-engineering (urgenza + brand interno "dominio_vittima Webmail") colloca il rischio su livello Alto per furto credenziali e successiva compromissione di caselle aziendali.

- Analisi delle intestazioni

Campo	Valore normalizzato	Evidenza
Mittente visualizzato	"dominio_vittima Servizio Webmail" <venatz@layconsa[.]com[.]pe>	header originali
Reply-To	gerente.fogan@mail[.]com	segnalato in thread di phishing (X (formerly Twitter))
IP client STARTTLS	185[.]64[.]78[.]9	subnet hosting, 0 domini noti, risk ASN Latitude.sh (IPinfo)
Relay peruviano	161[.]132[.]109[.]138 (mail[.]holdingelsol[.]com[.]pe)	stessa /17 Red Científica Peruana con hit abuse recenti (IPinfo, abuseipdb.com)
Autenticazioni	SPF none · DKIM none · DMARC none	facilita spoofing (kb.mit.edu)

- Reputazione IP
  - La classe 185[.]64[.]78[.]0/24 è un blocco hosting senza domini legittimi e varie segnalazioni spam/port-scan (IPinfo, abuseipdb.com).
  - La rete 161[.]132[.]128/17 (RCP-Peru) conta > 30 report "Email Spam / Phishing" negli ultimi mesi (abuseipdb.com, abuseipdb.com).
- Catena di reindirizzamento malevola
  - https://r.brandreward[.]com/?key=<uuid>&url=https://bandeirantesvistoria[.]com[.]br/lo-jaz/?va=vittima@dominio_vittima[.]com

Hop	Funzione	Evidenze
r.brandreward[.]com	Open Redirect noto (CVE-style) sfruttato da affiliate abuse	bug bounty pubblici ID 320343 e 824257 (Open Bug Bounty, Open Bug Bounty)
bandeirantesvistoria[.]com[.]br	Redirect: classificata *Malicious* dal sandbox ANY.RUN	report 30 gen 2025 (ANY.RUN)
brandreward[.]com	Servizio affiliate con scarsa reputazione (TrustScore 2.5/5) — spesso usato in redirect fraud	(Trustpilot, Referral Rock)
dieselecia[.]com[.]br	Landing cred-harvest: classificata *Malicious* dal sandbox ANY.RUN	Vedi screenshot (ANY.RUN, VirusTotal)

La presenza di open-redirect monetizzato tramite reti affiliate è tipica delle campagne di phishing contemporanee (Reddit).

- Contenuto & Tecniche di ingegneria sociale
  - Fake quarantine: avvisa di "7 messaggi trattenuti" per creare urgenza.
  - Brand spoofing: logo e colore blu riportante il nome deominio vittima: "dominio_vittima Webmail", pur inviato da dominio esterno peruviano.
  - Pulsante "Verifica messaggi" unico, quindi click-ratio elevato.
  - HTML responsive con CSS moderno per bypassare filtri (font Segoe UI, media-queries).
  - Template ricalca modelli di phishing "quarantine release" documentati in guide O-365/MIT KB (kb.mit.edu).

- Indicatori di Compromissione (IoC)

Tipo	Valore (con "[.]")	Origine
IP origine	185[.]64[.]78[.]9	header
IP relay	161[.]132[.]109[.]138	header
Dominio mittente	layconsa[.]com[.]pe	header
Reply-To	gerente.fogan@mail[.]com	header
Redirect 1	r.brandreward[.]com	open-bug-bounty
Redirect 2	bandeirantesvistoria[.]com[.]br/lojaz	sandbox ANY.RUN
Oggetto	"Notifica di messaggi in quarantena sul tuo account Webmail"	header

- Mappatura MITRE ATT&CK

Fase	Tecnica	Evidenza
Initial Access	T1566.002 – Phishing via link	email + URL spoof
Credential Access	T1056.007 – Web forms	landing login fake
Command & Control	T1071.001 – Web protocols	HTTPS verso dominio .br
Defense Evasion	T1041 – Exfiltration over C2 channel	dati inviati tramite POST cliente

- Valutazione del rischio

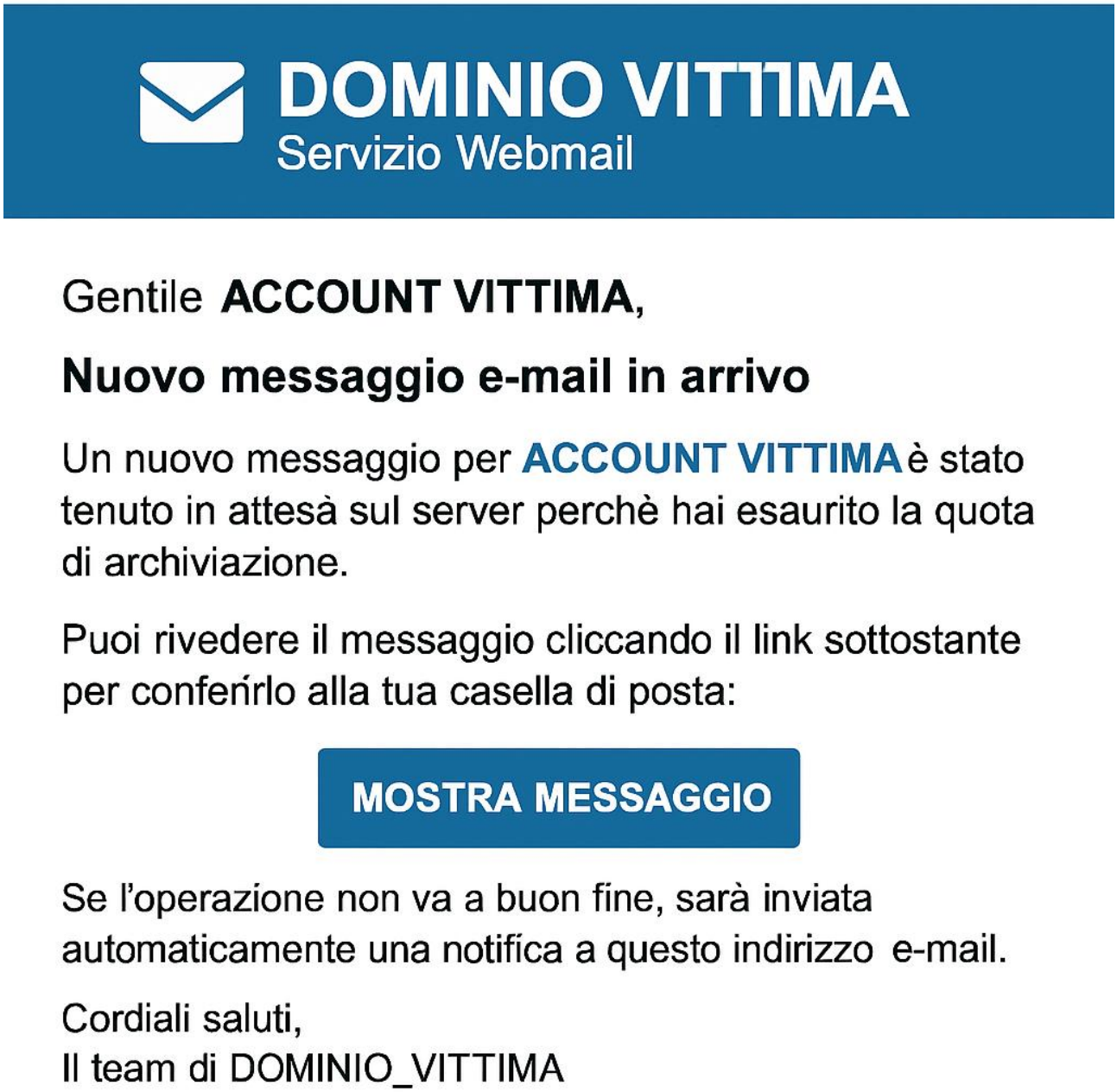
Vettore	Gravità	Commento
Furto credenziali casella	Alto	login webmail raccolto sulla landing
Propagazione interna	Medio	accesso casella → spear-phish laterale
Malware	Basso	nessun allegato rilevato; rischio successivo

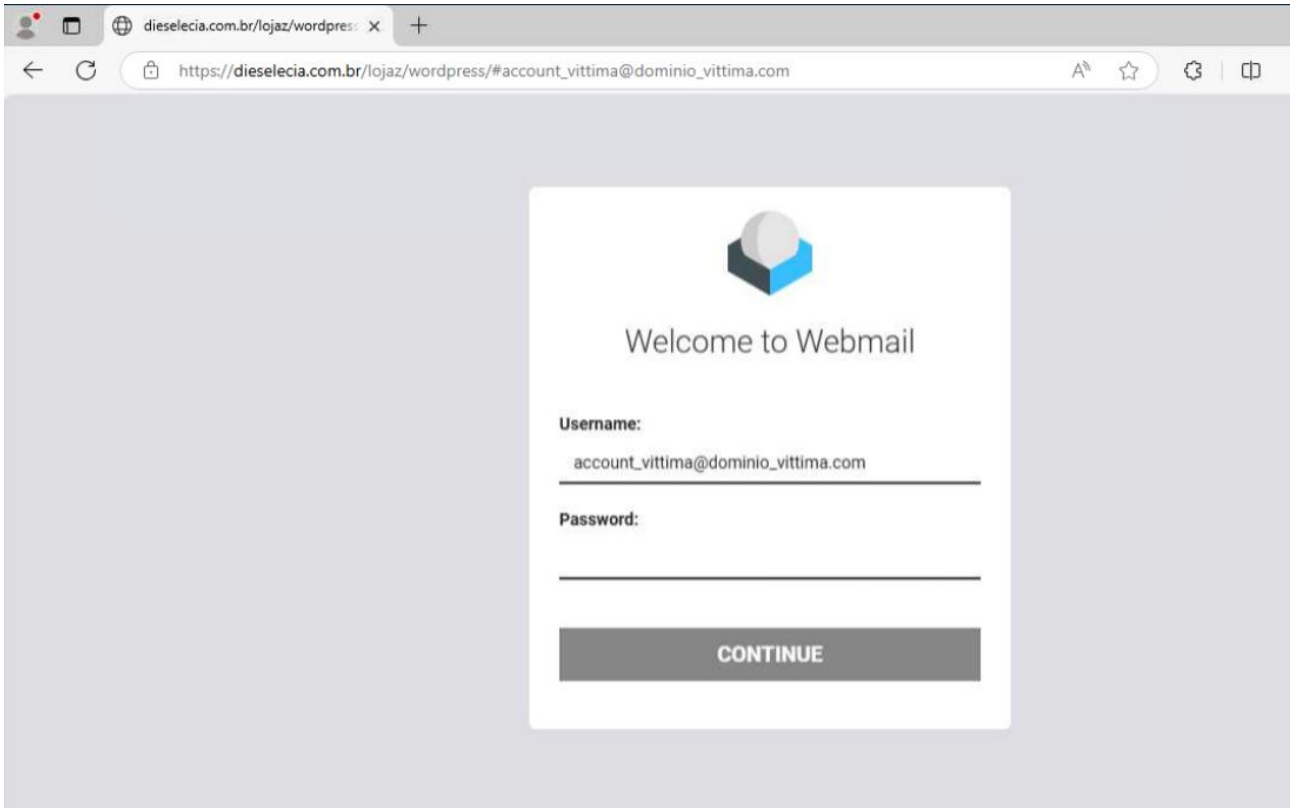
- Raccomandazioni
  - Bloccare ai gateway i domini r.brandreward[.]com e bandeirantesvistoria[.]com[.]br e gli IP 185[.]64[.]78[.]0/24 – 161[.]132[.]109[.]0/24.
  - Abilitare SPF, DKIM, DMARC con politica reject sul dominio dominio_vittima[.]com per prevenire spoof.
  - Segnalare l'open-redirect a BrandReward Security (vulnerability IDs citati).
  - Formazione utenti: diffondere linee guida anti-phishing e riconoscimento false "quarantine" (PRODEST).
  - Threat-hunt: cercare HTTP/HTTPS verso gli IoC negli ultimi 30 giorni; resettare password se click avvenuto.
  - Monitorare future campagne: pattern identico già osservato in America Latina (Perù) (AMPYX CYBER) e in environment O-365 (Reddit).

- Fonti principali
  - OpenBugBounty CVE-style report #320343 – open redirect r.brandreward[.]com (Open Bug Bounty)
  - OpenBugBounty report #824257 – stesso host, vulnerabilità non mitigata (Open Bug Bounty)
  - ANY.RUN sandbox – link classificato Malicious (ANY.RUN, ANY.RUN)
  - Trustpilot score BrandReward 2.5/5 (Trustpilot)
  - ReferralRock article on redirect fraud (Referral Rock)
  - MIT KB – riconoscere false quarantine O-365 (kb.mit.edu)
  - AmpyxCyber – boom di phishing in Perù (AMPYX CYBER)
  - IPinfo subnet 185[.]64[.]78[.]0/24 AS396356 (IPinfo)
  - AbuseIPDB multiple reports 185[.]64[.]189[.]112 similare (abuseipdb.com)
  - IPinfo rete 161[.]132[.]128/17 Red Científica Peruana (IPinfo)
  - AbuseIPDB 161[.]132[.]216[.]202 report phishing (abuseipdb.com)
  - Mail.com best-practices anti-phish (support.mail.com)
  - MIT Spamhaus guide reputazione IP (The Spamhaus Project)
  - Reddit discussion redirect abuse vigilance (Reddit)
  - Google form per segnalazione phishing/malware (Google for Developers)
  - VirusTotal, segnalazione domini malevoli (VirusTotal, VirusTotal)

Report CTI redatto il 2 agosto 2025. Tutti i riferimenti al dominio aziendale reale sono anonimizzati in dominio_vittima[.]com; i punti negli IoC sono sostituiti con "[.]" in conformità alle policy di riservatezza.

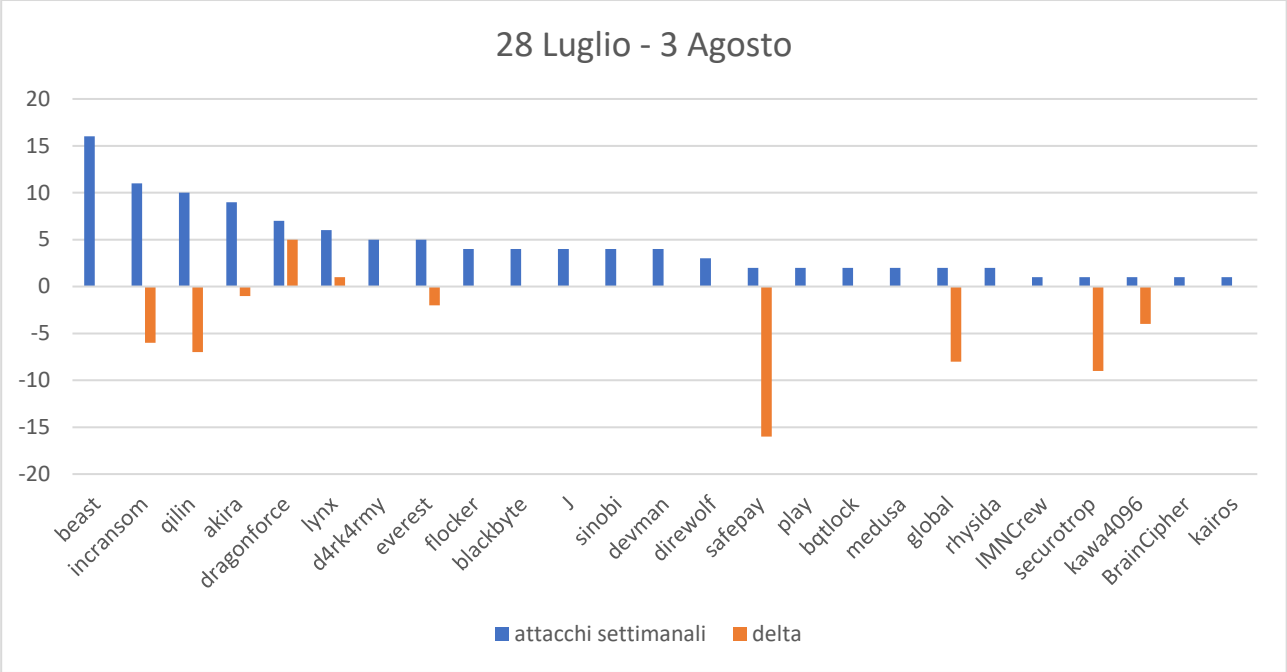
Qui di seguito alcuni screenshot della mail:



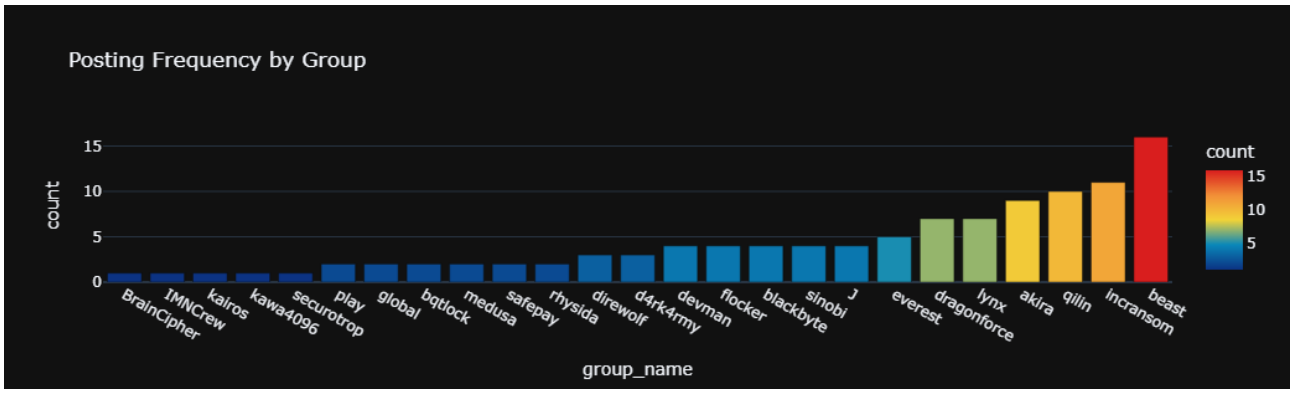

dieselecia.com.br/lojaz/wordpres
https://dieselecia.com.br/lojaz/wordpress/#account_vittima@dominio_vittima.com
Welcome to Webmail
Username:
account_vittima@dominio_vittima.com
Password:
CONTINUE

4.2 Ransomware

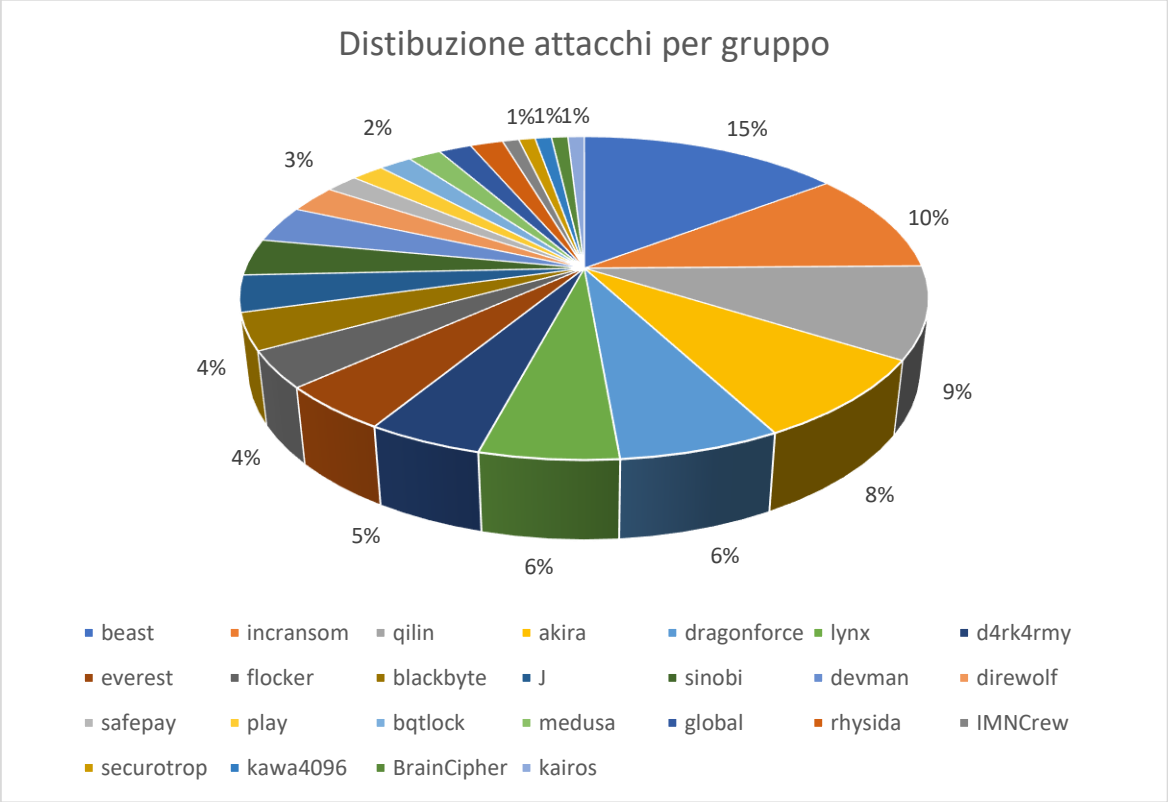
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (28 Luglio – 3 Agosto). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

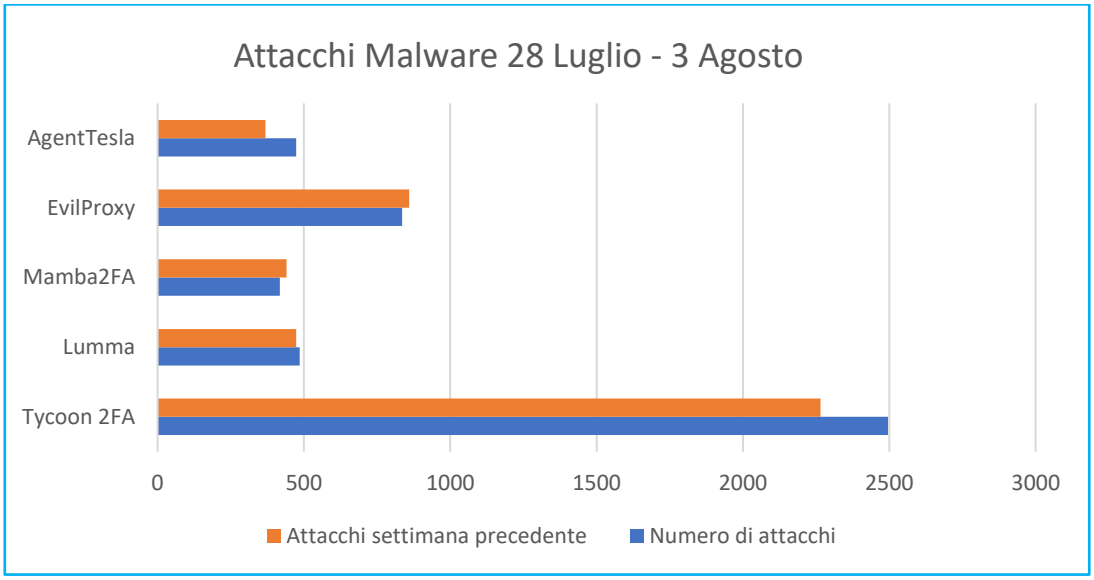


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



4.3 Malware

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



Anche questa settimana riportiamo un'analisi dettagliata dei malware risultati più attivi nella settimana di osservazione

- **Backdoor ApolloShadow (campagna Secret Blizzard)**

il 31 luglio, Microsoft ha scoperto la campagna di cyberspionaggio "Secret Blizzard" (probabilmente FSB russo, VENOMOUS BEAR) che sfrutta una posizione man-in-the-middle nei provider russi per colpire le sedi diplomatiche straniere a Mosca. Con questa tecnica, l'attaccante installa certificati di root malevoli e scarica il malware personalizzato ApolloShadow sui dispositivi delle vittime.

ApolloShadow è un backdoor Windows in grado di raccogliere informazioni e mantenere la persistenza silenziosa. Cert-UA ha attribuito questa campagna ad APT28 (Fancy Bear) con moderata confidenza.

Descrizione tecnica e contesto: attacco di tipo AiTM in cui gli aggressori, sfruttando infrastrutture ISP russe (SORM), inseriscono un certificato Kaspersky falso per bypassare SSL e iniettano su PC diplomatici l'implant ApolloShadow.

Il malware installa in memoria un rootkit legittimo modificato e consente lo spionaggio persistente. Rispetto storico, è la prima conferma di operazioni di cyberspionaggio attive dentro la Russia.

IoC:

Tipo	Indicatore
Dominio	kav-certificates[.]info
Indirizzo IP	45[.]61[.]149[.]109
Hash SHA256	13fafb1ae2d5de024e68f2e2fc820bc79ef0690c40dbfd70246bcc394c52ea20
File sospetto	CertificateDB.exe

MITRE ATT&CK:

- TA0001 (Initial Access)
- Man in the Middle (T1557) attraverso compromissione infrastrutturale;
- TA0004 (Privilege Escalation) – possibili modifiche del registro;
- TA0005 (Defense Evasion) – installer rootkit e certificati malevoli;
- TA0006 (Credential Access) – raccolta token e cookie;
- TA0007 (Discovery) con WMI e comandi di sistema,
- TA0009 (Collection) per raccolta dati sensibili.

Contromisure:

- adottare reti VPN cifrate ed utilizzare provider sicuri (idealmente con tunneling esterni) per evitare l'ispirazione del traffico locale.
- Disabilitare servizi non necessari (es. SMB remoto) e verificare i certificati di sistema (rimuovere certificati Kaspersky sospetti).
- I sistemi Endpoint Detection & Response (EDR) possono rilevare la presenza del file CertificateDB.exe o connessioni al dominio di C2. Piani di formazione per il personale diplomatico (gestione connessioni pubbliche).

Livello di rischio: Critico/Alto. Coinvolge organizzazioni diplomatiche sensibili con rischio di spionaggio pesante, difficilmente mitigabile con solo patch (interessa infrastruttura di rete).

➢ Trojan bancario Android DoubleTrouble

DoubleTrouble è un trojan bancario Android precedentemente diffuso tramite siti fasulli di banche europee. La sua ultima evoluzione, scoperta a fine luglio 2025, estende la distribuzione tramite canali Discord. Gli aggressori pubblicano falsi APK in chat Discord; le app si mascherano da app legittime (spesso con icona Google Play) per indurre l'installazione.

Il malware richiede i permessi di Accessibilità Android, registrando l'interazione dell'utente (overlay per PIN/schermo di blocco, registrazione schermo, keylogger avanzati) e ruba credenziali da app bancarie e wallet crypto.

Descrizione tecnica e contesto: bersaglia utenti in Europa fingendosi app bancarie; viene distribuito tramite Discord (malvertising o link diretti).

I payload contengono il trojan principale nascosto in un installer a sessione, che convince l'utente ad abilitare i servizi di Accessibilità. Il malware dispone di overlay fraudolente per PIN/lockscreen, registrazione segreta dello schermo e invio di dati raccolti al C2 remoto.

IoC:

Tipo	Indicatore
Dominio	hxxp[://]begans[.]cfd/ hxxp[://]unicredit[.]appaggiornamento[.]com/ hxxp[://]volksbank[.]applogininfo[.]com/
Indirizzo IP	• 104[.]238[.]34[.]15 • 77[.]105[.]164[.]255 • 41[.]216[.]183[.]248 • 82[.]115[.]223[.]2
APKs Hash SHA256	▪ 7a924c7bdb1fd32cfc838f3cdd624abc10da19713c123b84a0f2325fef3d2bbc ▪2f9d70c75330b49a1a97479587d5e0b6016cf8004e454badf2b021e8bbb28469

	▪ 890601564414 34da8f016bd872aeaa542d32820d49b3c00bce4426120110282e ▪ d181f30e0404c3ff85af22833600c3666c54cf904cc6387b926c9ad321c1206e 7eb4305dbc23c5acc2c35e0d4ccd417e9448be27facca1a1d42408464e156825

MITRE ATT&CK:

- TA0005 (Defense Evasion) – abuso dei Mobile Accessibility
- (T1359) per ottenere permessi;
- TA0004 (Privilege Escalation) – richieste di permessi elevati;
- TA0009 (Collection) – Screenshots (T1632), Keylogging (T1056.001 Android);
- TA0006 (Credential Access) – Credential API Access (T1555.004).

Contromisure:

- vietare l'installazione di app da sorgenti non ufficiali. I
- implementare soluzioni Mobile Threat Defense (MTD) su dispositivi aziendali per identificare app bancarie malevole.
- Fornire campagne di sensibilizzazione agli utenti sulle richieste di Accessibilità sospette.
- Utilizzare software di protezione mobile (Play Protect, EDR mobile) per bloccare comportamenti di spyware.
- In sede, controllare i log delle applicazioni Android per individuare attività di overlay o registrazione schermo.

Livello di rischio: Alto. Malware mobile in grado di sfuggire alla maggior parte delle difese tradizionali, in grado di sottrarre credenziali finanziarie sensibili.

- **Malware JSCEAL (campagna di cryptomalvertising)**

Il gruppo di ricerca Check Point ha riportato il malware JSCEAL, attivo dall'inizio del 2024, che si concentra su utenti di applicazioni di trading crypto. La tecnica sfrutta pubblicità malevole (malvertising) su social e web, presentando false app di trading/popular crypto apps.

Gli utenti che cliccano sono reindirizzati a siti fasulli che li spingono a installare un file MSI. L'MSI esegue script PowerShell di profilazione del sistema, poi scarica il payload JSCEAL (un binario Node.js che esegue codice JavaScript compilato).

Grazie a V8 JavaScript compilato in .JSC, il malware nasconde il suo codice finché non viene eseguito da Node.js. Alla fine, ruba credenziali e chiavi dei portafogli crypto

Tra gennaio e giugno 2025 sono state stimate ~35.000 pubblicità malevole servite in UE.

Descrizione tecnica e contesto: si basa su annunci ingannevoli che fingono istituzioni finanziarie o piattaforme crypto per indurre download di MSI malevoli.

L'installazione avvia uno script di profiling (raccolta dati di sistema via PowerShell) e infine un payload Node.js contenente codice JS compilato V8.

Il binario finale JSCEAL sottrae informazioni sensibili (wallet e credenziali crypto) grazie a code injection nelle app crypto o tramite UI overlay, sfruttando la struttura modulare del malware.

La portata geografica è globale (estesa nell'Unione Europea).

IoC:

Tipo	Indicatore
Dominio	vertical-scaling[.]com ggr-lach[.]com llm-0014[.]com resolve-ns[.]pages[.]dev hasv[.]pages[.]dev
Hash SHA256	**build[.]zip** • b90e3aaae14e7787e5ea4a6d4beee672049bd5eb05427f2c80b64f605860d2b8 • f6c670e65765d10a5ca0205a6ece3a3e6c7c730b0a8534c5adef4a3cbf06eb9c

	MSI Installers • a696d03aeb1bde633b674bdd640a1a313cae7da711d99cfba3fd06f02d3864de • e881682b59640c05cd540696955a849610260415e576f79b62383108c1aa3354 **JSCEAL Payload** • 62ba626bce09db5f8750938edced3768b401084a7d6584cd6ff9d53d2517781d • 95b39a0bad021f33e08df042b02d3267faee7bbc3e3080dda295c35b464dd607

MITRE ATT&CK:

- TA0001 (Initial Access) – tramite Drive-by Compromise e Spearphishing via Service (T1566.002) con malvertising;
- TA0004 (Privilege Escalation) – abuso di Windows Powershell (T1059.001) per profiling;
- TA0005 (Defense Evasion) – uso di codice JavaScript compilato (T1059.006) e nascondimento;
- TA0006 (Credential Access) – rubare credenziali crypto (T1555.004, Credential API Hooking);
- TA0007 (Discovery) – raccolta info di sistema (T1082).

Contromisure:

- bloccare l'esecuzione di script PowerShell non autorizzati.
- Implementare soluzioni di URL filtering e scanner anti-malvertising sui browser aziendali.
- Configurare le soluzioni anti-malware avanzate per analisi emulativa (sandboxes) che individuino payload JavaScript/Node.js malevoli. Monitorare la libreria annunci (Facebook ad library) per identificare annunci maligni sospetti e rimuoverli.

Livello di rischio: Medio/Alto. Rappresenta una minaccia significativa per i singoli utenti crypto, sfruttando piattaforme legittime (social media) come vettore, ma colpisce pesantemente in UE.

➢ Ransomware Gunra (nuova variante Linux)

Il gruppo "Gunra" (emergente da aprile 2025) ha introdotto una variante Linux del proprio ransomware. I ricercatori di Trend Micro hanno evidenziato che questa versione nativa Linux esegue fino a 100 thread di cifratura paralleli e consente la cifratura parziale dei file.

I file cifrati vengono rinominati con l'estensione .ENCRT (senza lasciare nota di riscatto). Gunra è ispirato a Conti e ha già colpito aziende in vari Paesi (Brasile, Turchia, USA, ecc.) e settori critici (sanità, manifatturiero, IT), evidenziando che il gruppo sta diventando cross-platform.

Descrizione tecnica e contesto: originariamente rivolto a Windows con tecniche da Conti, il nuovo payload Linux implementa cifratura multithread avanzata.

I file compromessi vengono rinominati con estensione .ENCRT

Gli operatori hanno pubblicato leak di dati ("40 TB" da un ospedale) e preso di mira organizzazioni di governo e imprese in settori diversificati.

Non lascia tracce sui file cifrati oltre alla nuova estensione.

IoC:

Tipo	Indicatore
URLs	Data Leak Site: ▪ gunrabxbig445sjqa535uaymzerj6fp4nwc6ngc2xughf2pedjdhk4ad[.]onion Chat Server: ▪ hxxp[://]2bw7r32r5eshwk2h7uekj3lwzorxds2jyhyzqyil-phid3r27x5hsf4yd[.]onion Chat Server hxxp[://]jzbhtsuwysslrzi2n5is3gmzsyh6ayhm7jt3xowldhk7rej4dqqub-xqd[.]onion/
Hash SHA256	**Linux Variant** • Ransom.Linux.GUNRA.AA 8404521cf2a53de3459a75ff946873c43211afb6

	Windows Variant • Ransom.Win64.GUNRA.AA 0c3c878b678c7254446e84cca6f0d63caeb51880 • Ransom.Win64.GUNRA.AA 79e19d3d8405425735e4b3cd36a8507d99dfee20 Ransom.Win32.GUNRA.AA 912217b09b13e1e53f7f26335f7f84b3c3918491
Estensione file	*.ENCRT* (file cifrati)

MITRE ATT&CK:

- TA0040 (Impact) – Data Encrypted for Impact (T1486) esteso a Linux;
- TA0006 (Credential Access) – se usato per spostarsi orizzontalmente;
- TA0009 (Collection) – raccolta preliminare e movimento laterale;
- TA0042 (Resource Development) – possibili nuove infrastrutture di C2 Linux.

Contromisure:

- isolare immediatamente i sistemi Linux sospetti.
- Mantenere backup offline aggiornati e testati.
- Applicare principi di least privilege per account SSH e servizi remoti.
- Utilizzare soluzioni di EDR/IDS per Linux in grado di rilevare attività di cifratura di massa e le firme del ransomware (ad es. eventuali binari sospetti in esecuzione).
- Segmentare la rete e limitare i protocolli di amministrazione remota.

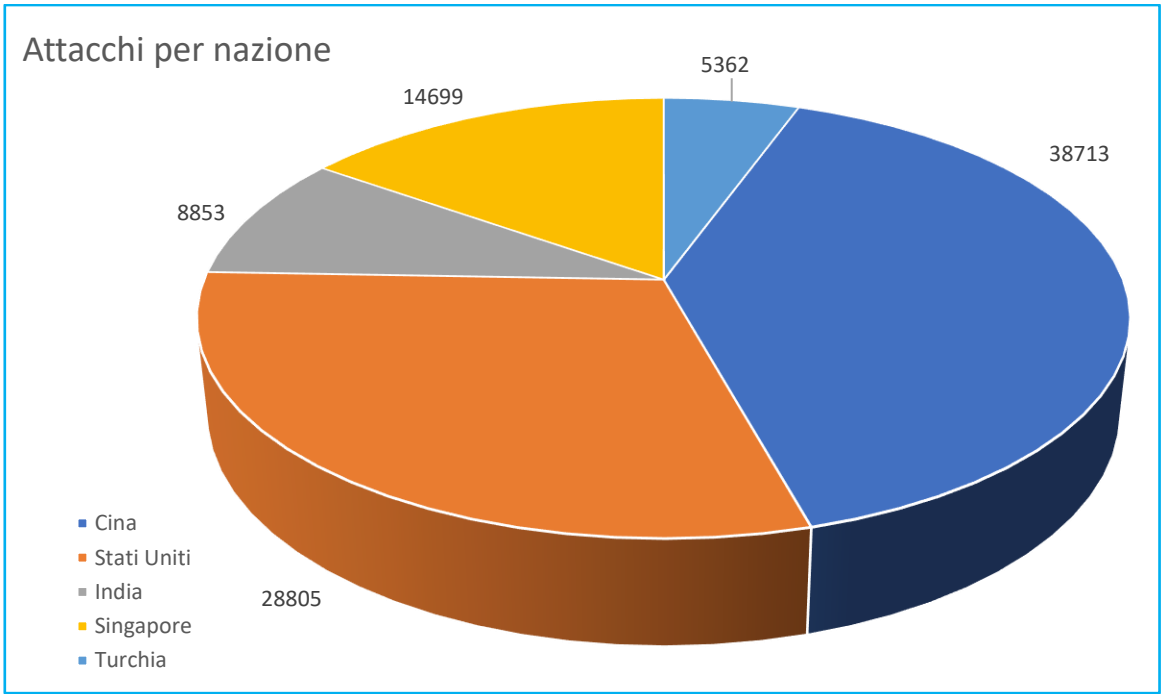
Livello di rischio: Alto. Ransomware maturo che ora colpisce anche sistemi Linux critici, ampliando notevolmente la superficie di attacco.

Riepilogo:

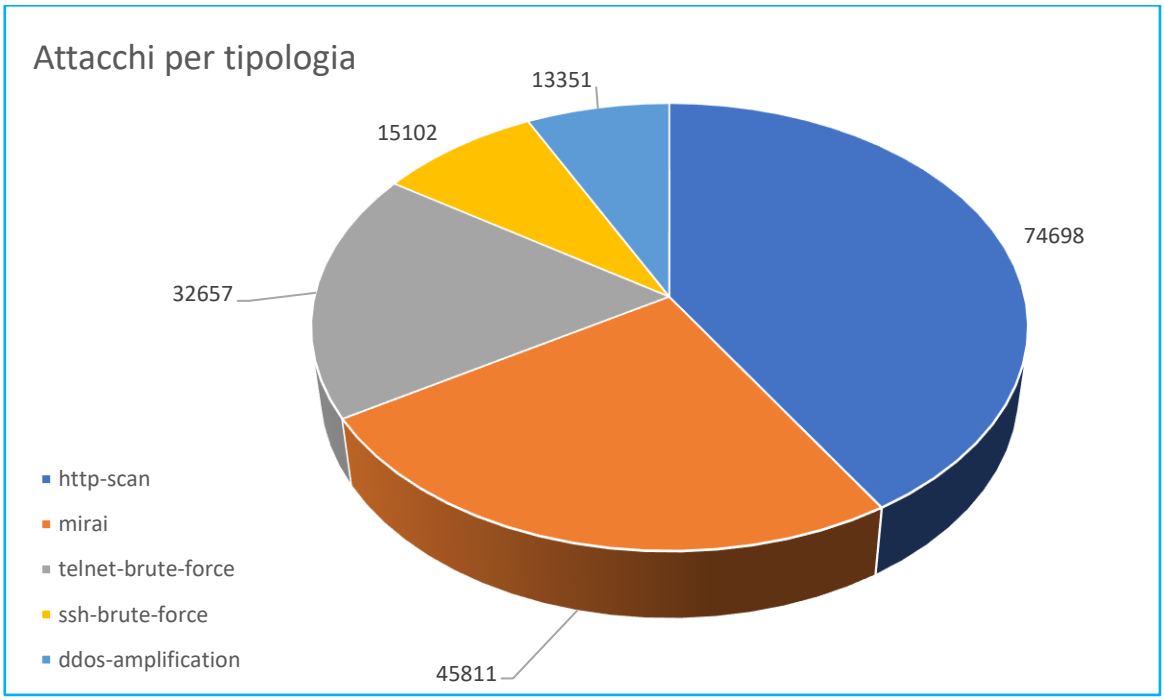
Malware	Categoria	Livello di rischio
ApolloShadow	Backdoor/Spionaggio	Critico
DoubleTrouble	Trojan bancario (Android)	Alto
JSCEAL	Malware crypto	Medio-Alto
Gunra (Linux var.)	Ransomware	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 28 Luglio – 3 Agosto, suddivisa per nazione e limitata alle prime cinque posizioni:

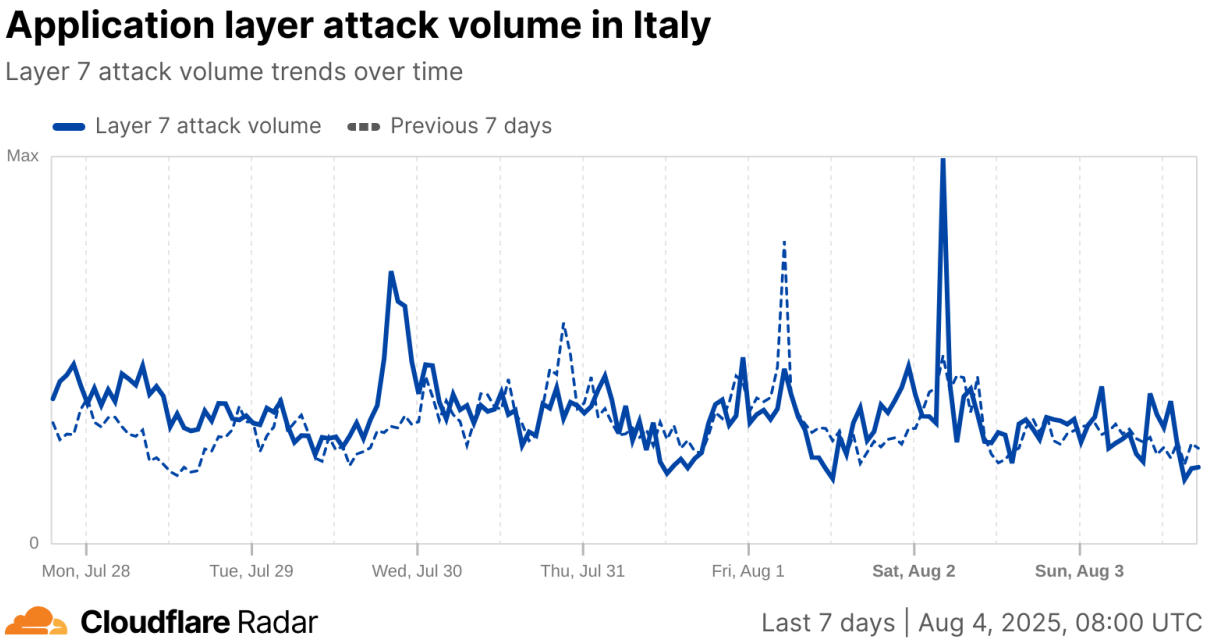


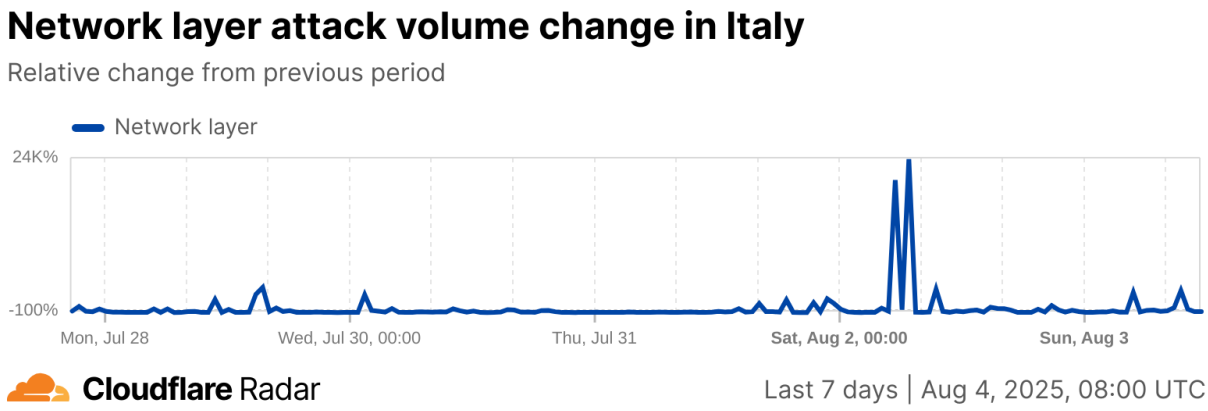
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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

4.6 Defacement

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

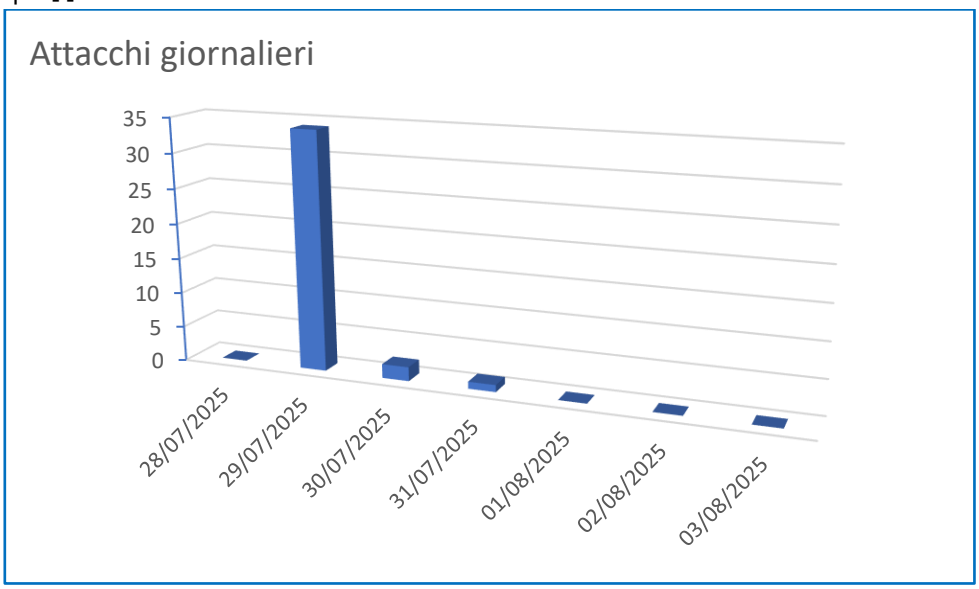


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

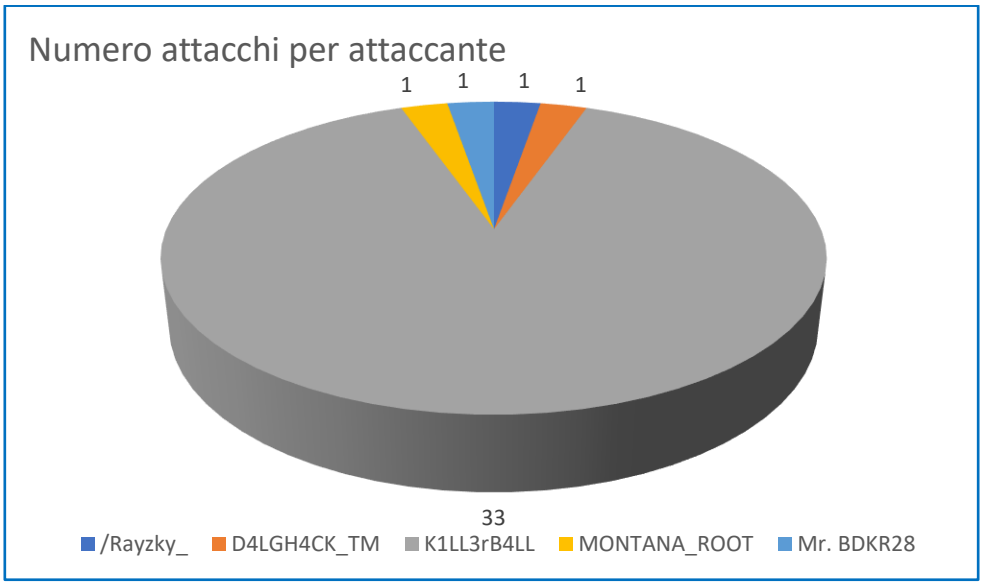


Figura 2: Defacement - Attaccanti più attivi nel periodo 28 Luglio – 3 Agosto

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

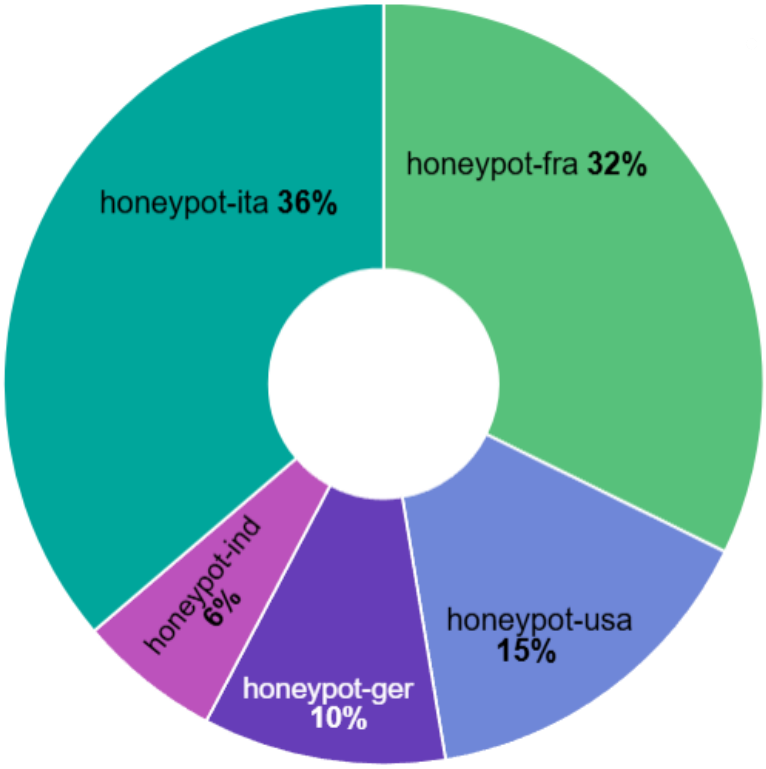
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

1.213.620 Attacks

9.597 Unique Src IPs

67 Unique HASSHs

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



Questa invece la situazione a livello italiano:

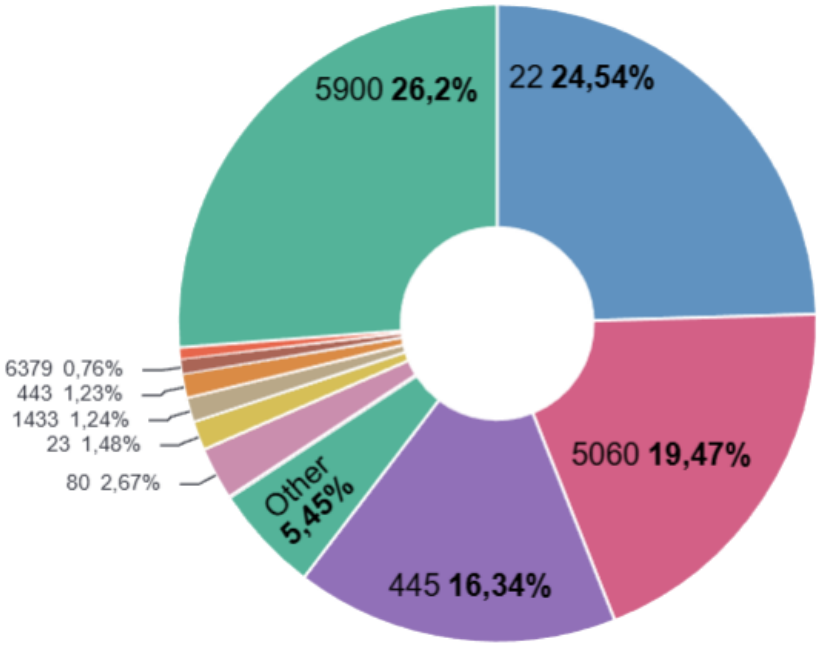
439.636 Attacks

4.869 Unique Src IPs

50 Unique HASSHs

5.1.1 Attacchi ai servizi

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



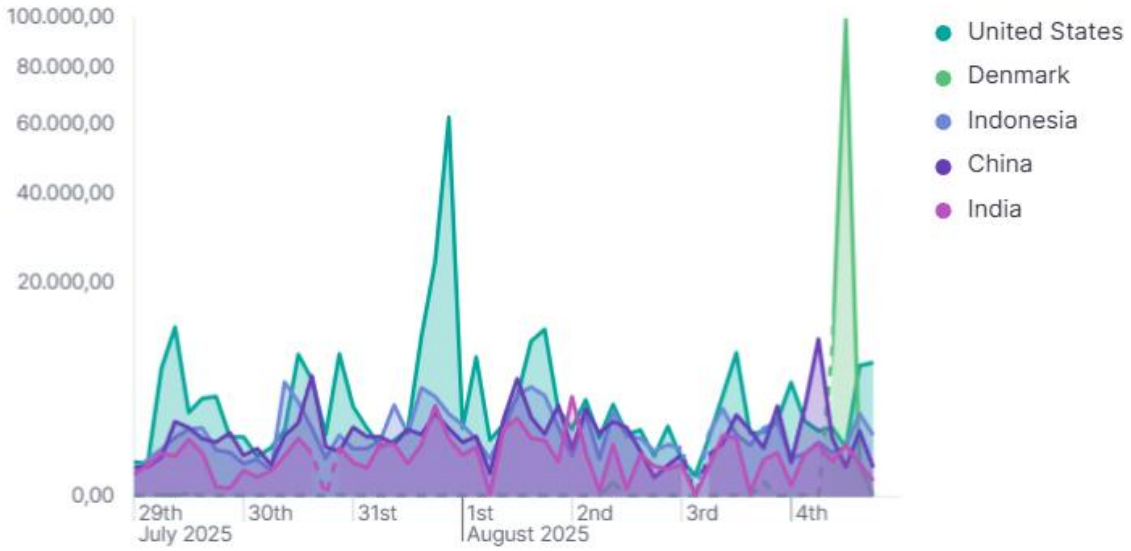
5.1.2 IP Attaccanti

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

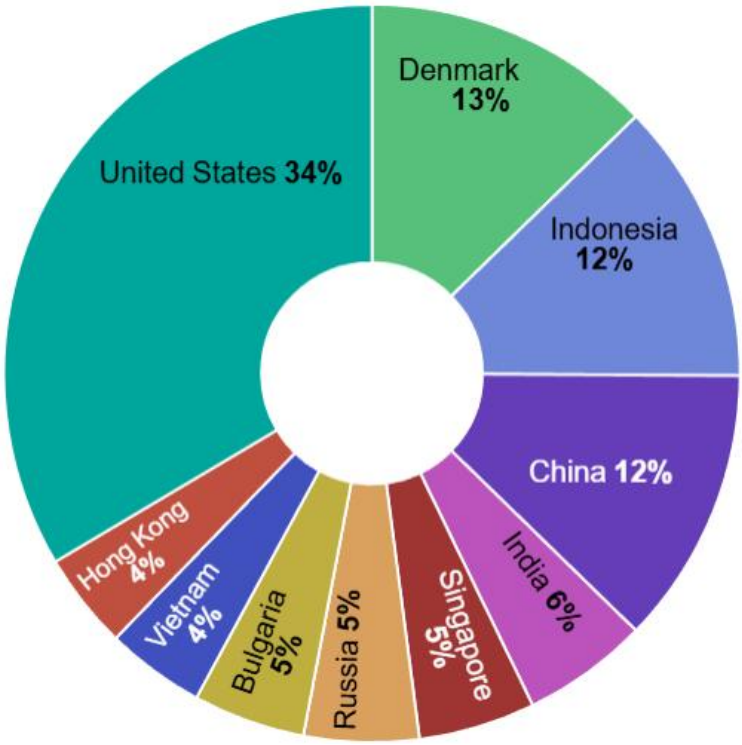
Source IP	Count
45.144.29.201	108.593
173.233.73.6	75.981
103.156.74.23	38.606
142.202.189.5	33.709
142.202.191.234	32.529
79.124.56.162	18.211
193.37.69.157	12.957
181.10.132.138	11.068
180.171.235.84	10.403
142.202.188.211	9.996

5.1.3 Paesi di provenienza degli attacchi

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



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

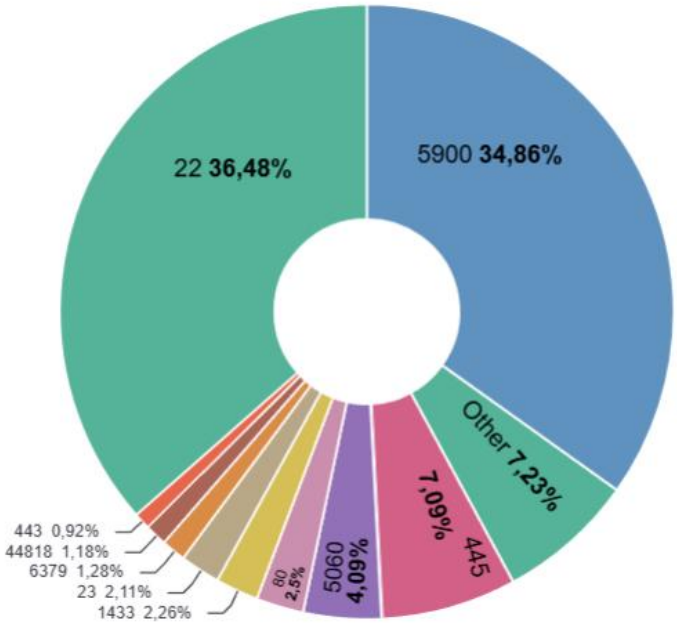


5.2 Italian Honeypot N.1

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

5.2.1 Attacchi ai servizi

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



Service Port	Count
22	44.343,00
5900	42.367,00
445	8.618,00
5060	4.966,00
80	3.036,00
1433	2.766,00
23	2.563,00
6379	1.557,00
44818	1.448,00
443	1.117,00

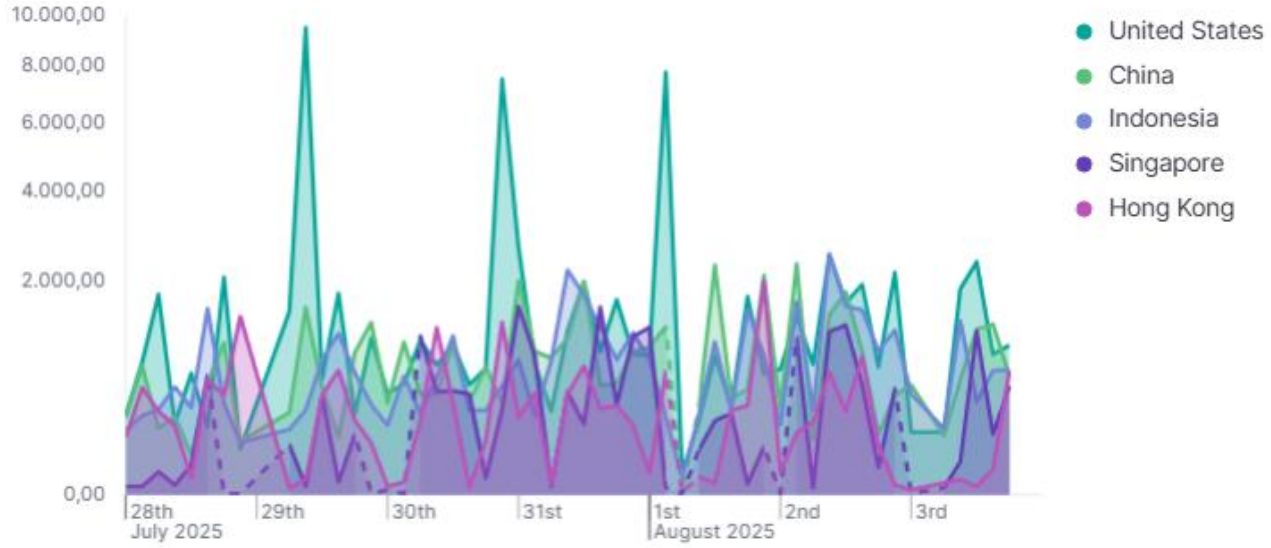
5.2.2 IP Attaccanti

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

Source IP	Count
103.156.74.23	14.649
142.202.191.234	12.252
142.202.189.5	11.484
212.34.230.50	6.982
79.124.56.162	6.025
193.37.69.157	4.950
43.153.174.38	3.826
112.223.42.162	3.779
173.231.185.164	3.696
179.43.189.98	2.844

5.2.3 Paesi di provenienza degli attacchi

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

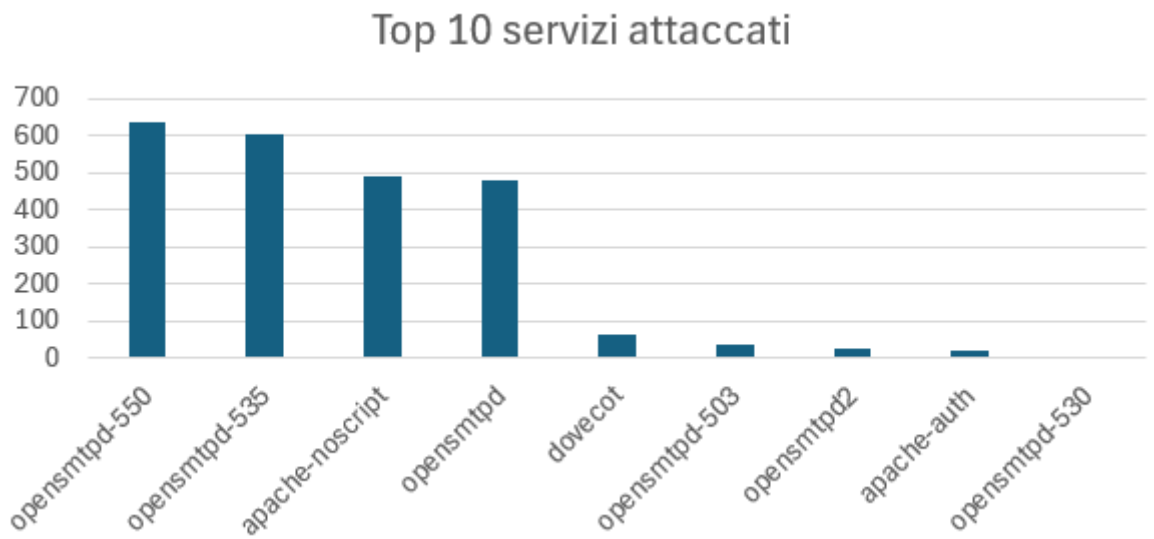


5.3 Italian Honeypot N.2

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

5.3.1 Attacchi ai servizi

Questa la distribuzione degli attacchi per servizio attaccato.



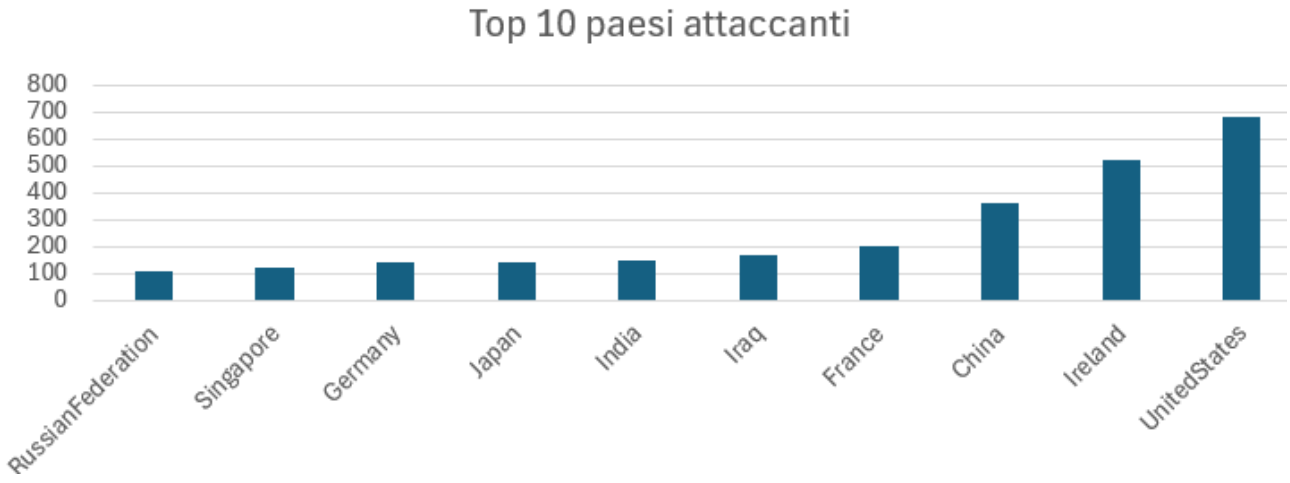
5.3.2 IP attaccanti

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

Source IP	Numero di attacchi
209[.]85[.]160[.]200	30
190[.]6[.]49[.]215	23
177[.]86[.]85[.]130	23
197[.]240[.]139[.]27	21
105[.]156[.]235[.]34	21
170[.]83[.]172[.]133	21
105[.]232[.]128[.]25	20
149[.]78[.]58[.]44	20
138[.]94[.]254[.]23	19
85[.]58[.]6[.]130	19

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

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

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

Cyber security

RISK REPORT

S3K

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