S3K

Cyber security

RISK REPORT

\ week 14.07.2025 - 20.07.2025

Sommario

1 Il Cyber Security Risk Report S3K 5

1.1 Sommario e Presentazione del Cyber Security Risk Report S3K 5

1.2 Principali Evidenze del Bollettino 6

1.3 Attacchi Attivi che Sfruttano CVE-2025-53770 6

1.4 Altri Elementi di Rilievo 7

1.5 Analisi degli Attacchi e Dati Honeypot 7

1.6 Analisi dei Dati Honeypot 8

1.7 Conclusioni e Raccomandazioni 8

2 Security news 10

2.1 Rilasci aggiornamenti e patch 10

2.2 "Cyber News" dal Web, Deep Web e Dark Web 13

3 CVE Monitor 17

3.1 Sintesi Settimanale CVE 17

3.2 Tendenze 21

3.3 Nuove CVE 22

3.4 CVE attualmente utilizzate in attacchi 24

4 Attacchi 25

4.1 Phishing 25

4.2 Ransomware 31

4.3 Malware 33

4.4 DDoS rilevati 39

4.5 Data Breach 41

4.6 Defacement 43

5 Honeypot 44

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale 44

5.1.1 Attacchi ai servizi 45

5.1.2 IP Attaccanti 45

5.1.3 Paesi di provenienza degli attacchi 46

5.2 Italian Honeypot N.1 47

5.2.1 Attacchi ai servizi 47

5.2.2 IP Attaccanti 47

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

CYBER SECURITY RISK REPORT
29/25

1 Il Cyber Security Risk Report S3K

Settimana 14.07.2025 – 20.07.2025

Il Cyber Security Risk Report S3K è un bollettino settimanale che fornisce un'analisi approfondita del panorama delle minacce informatiche, dedicato a professionisti della sicurezza e responsabili della protezione dei dati. Questo documento offre informazioni aggiornate sulle vulnerabilità emergenti, tendenze degli attacchi, malware in circolazione e dati raccolti dall'infrastruttura honeypot di S3K. L'edizione corrente copre il periodo dal 14 al 20 luglio 2025, con particolare attenzione alle nuove CVE critiche, agli aggiornamenti di sicurezza rilasciati dai principali vendor e alle attività malevole osservate a livello globale.

1.1 Sommario e Presentazione del Cyber Security Risk Report S3K

Presentazione del Report

Il Cyber Security Risk Report S3K rappresenta un'analisi settimanale completa del panorama delle minacce informatiche, elaborata dagli analisti di S3K per fornire informazioni tempestive e actionable ai professionisti della sicurezza.

Struttura del Bollettino

Il documento è strutturato in sezioni tematiche che coprono: aggiornamenti di sicurezza dei principali vendor, analisi delle CVE più critiche, monitoraggio delle tendenze di attacco, analisi dei malware più diffusi, statistiche su attacchi DDoS, data breach e defacement, e dati raccolti dall'infrastruttura honeypot di S3K dislocata a livello mondiale.

Periodo di Osservazione

Il bollettino si riferisce alla settimana dal 14 al 20 luglio 2025, fornendo un'istantanea delle minacce informatiche più rilevanti in questo intervallo temporale. Le analisi e le statistiche presentate consentono di identificare tendenze emergenti e pianificare adeguate strategie di mitigazione.

1.2 Principali Evidenze del Bollettino

Aggiornamenti di Sicurezza

La settimana ha visto il rilascio di importanti aggiornamenti di sicurezza da parte di Oracle, Microsoft e Node.js. In particolare, Microsoft ha rilasciato patch per 130 vulnerabilità, tra cui una di tipo 0-day, mentre Oracle ha corretto numerose vulnerabilità su vari prodotti, incluse 15 di gravità "alta" e una "critica".

CVE Monitor

Sono state identificate oltre 20 CVE di gravità critica e alta, molte delle quali con exploit pubblici disponibili. Le vulnerabilità più significative hanno riguardato software open-source PHP, dispositivi IoT/Router (D-Link, Tenda) e ambienti cloud Microsoft (Azure ML/DevOps).

1.3 Attacchi Attivi che Sfruttano CVE-2025-53770

Alert: CVE-2025-53770 Attivamente Sfruttata

È stata rilevata un'intensa attività di attacchi che sfruttano la vulnerabilità CVE-2025-53770 in Microsoft SharePoint Server on-premises. Questa vulnerabilità critica è causata dalla deserializzazione di dati non attendibili, un processo in cui il software ricostruisce oggetti a partire da dati esterni.

La vulnerabilità CVE-2025-53770 permette a un attaccante di inviare oggetti malevoli che, una volta deserializzati, consentono l'esecuzione di codice arbitrario da remoto, senza necessità di autenticazione. Microsoft ha confermato che la falla è già attivamente sfruttata ("exploit in the wild") e sta lavorando a una patch completa.

Gli analisti di S3K hanno osservato un incremento significativo di tentativi di sfruttamento di questa vulnerabilità nelle ultime 72 ore, con attacchi provenienti principalmente da indirizzi IP localizzati in Russia, Cina e paesi dell'Est Europa. Le organizzazioni che utilizzano Microsoft SharePoint Server on-premises sono fortemente invitate ad applicare immediatamente le mitigazioni indicate nella documentazione del CVE per ridurre il rischio di compromissione, in attesa della patch definitiva.

Raccomandazioni immediate per CVE-2025-53770:

- Applicare immediatamente le mitigazioni temporanee indicate da Microsoft
- Monitorare attentamente i log dei server SharePoint per identificare potenziali indicatori di compromissione
- Limitare l'accesso esterno ai server SharePoint quando possibile
- Implementare regole di firewall per bloccare traffico sospetto verso i server vulnerabili
- Prepararsi all'applicazione immediata della patch non appena rilasciata da Microsoft

1.4 Altri Elementi di Rilievo

Operazione Eastwood

Coordinata da Europol e Eurojust, con il contributo determinante delle forze dell'ordine italiane, l'operazione ha colpito il gruppo hacker filo-russo NoName057(16), responsabile di numerosi attacchi DDoS contro infrastrutture critiche, enti governativi e aziende strategiche europee.

LameHug: Malware AI-Powered

Scoperto un nuovo malware chiamato LameHug che utilizza modelli linguistici di grandi dimensioni (LLM) per generare in tempo reale comandi adattivi capaci di esfiltrare dati da sistemi Windows, modificando il proprio comportamento in base all'ambiente in cui viene eseguito.

Attacchi via Microsoft Teams

Rilevato un nuovo schema di attacco che sfrutta le chiamate vocali automatiche di Microsoft Teams per diffondere il malware Matanbuchus, un potente loader progettato per aggirare le difese tradizionali e installare ulteriori payload dannosi.

1.5 Analisi degli Attacchi e Dati Honeypot

Panoramica degli Attacchi

Durante la settimana di osservazione (14-20 luglio 2025), sono stati registrati numerosi attacchi di varia natura. I gruppi ransomware più attivi sono stati LockBit, BlackCat e Play, con un notevole incremento delle attività di RagnarLocker rispetto alla settimana precedente. Nel campo dei malware, LameHug, Diskstation, Konfety e Matanbuchus 3.0 hanno rappresentato le minacce più significative, con livelli di rischio da alto a critico.

Gli attacchi DDoS hanno colpito principalmente Stati Uniti, Cina e Germania, con l'Italia che si posiziona al quinto posto per numero di attacchi subiti. Le tecniche più diffuse sono state gli attacchi UDP Flood, TCP SYN Flood e HTTP Flood, con un incremento degli attacchi a livello applicativo verso obiettivi italiani nella seconda metà della settimana.

Data Breach Significativi

Tra i principali data breach della settimana, si segnalano quelli che hanno colpito Flutter Entertainment (con oltre 800.000 utenti coinvolti), Media Broadcast Satellite GmbH (con sottrazione di 870 GB di dati) e Morrison Companies (attacco attribuito al gruppo Play). Questi incidenti evidenziano la continua minaccia rappresentata dai gruppi ransomware e la necessità di implementare solide strategie di protezione dei dati.

1.6 Analisi dei Dati Honeypot

L'infrastruttura honeypot di S3K, composta da sensori dislocati in vari paesi (Italia, Germania, Francia, Brasile, India e USA), ha raccolto dati significativi sugli attacchi informatici durante la settimana. L'analisi di questi dati fornisce una panoramica dettagliata delle tendenze di attacco e delle tecniche utilizzate dagli attori malintenzionati.

Distribuzione Geografica

Gli honeypot italiani hanno registrato il 22% degli attacchi totali, con una predominanza di attacchi provenienti da Cina (28,6%), Stati Uniti (17,8%) e Russia (14,3%). L'Italia è risultata il quarto paese per numero di attacchi originati.

Servizi Attaccati

I servizi più colpiti sono stati SSH (31,8%), HTTP/HTTPS (27,4%), Telnet (12,6%) e SMB (9,8%). Rispetto alla settimana precedente, si è registrato un incremento significativo degli attacchi ai servizi RDP (+18%) e ai database SQL (+12%).

1.7 Conclusioni e Raccomandazioni

L'analisi del panorama delle minacce per la settimana 14-20 luglio 2025 evidenzia un ecosistema di attacchi in continua evoluzione, con l'emergere di tecniche avanzate che sfruttano l'intelligenza artificiale (come il malware LameHug) e nuovi vettori di distribuzione attraverso piattaforme di collaborazione (come Microsoft Teams).

La presenza di numerose vulnerabilità critiche, molte delle quali con exploit pubblicamente disponibili, sottolinea l'importanza di mantenere aggiornati i sistemi e applicare tempestivamente le patch di sicurezza. Particolare attenzione deve essere rivolta alla vulnerabilità CVE-2025-53770 in Microsoft SharePoint Server, già attivamente sfruttata in attacchi reali.

Raccomandazioni Generali

- Implementare un processo di patch management efficace per garantire l'applicazione tempestiva degli aggiornamenti di sicurezza
- Rafforzare le misure di autenticazione, preferibilmente adottando soluzioni multi-fattore
- Monitorare attivamente i sistemi per identificare comportamenti anomali
- Implementare soluzioni di sicurezza a più livelli per difendersi da attacchi sofisticati
- Formare regolarmente il personale sulle nuove minacce e sulle tecniche di social engineering

Il team di analisti S3K continuerà a monitorare l'evoluzione delle minacce e a fornire aggiornamenti tempestivi attraverso i futuri bollettini di sicurezza. Per ulteriori informazioni o assistenza, è possibile contattare S3K agli indirizzi email indicati nella sezione "Contatti" del Company Profile.

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Oracle	Oracle ha rilasciato il Critical Patch Update di luglio che mira a correggere numerose vulnerabilità su più prodotti, di cui 15 con gravità "alta" e una con gravità "critica". Tra queste, alcune potrebbero essere sfruttate per eseguire operazioni non autorizzate oppure compromettere la disponibilità del servizio sui sistemi target. Versioni affette: • Application Express • BI Publisher • Database Server • Java SE • Lease and Finance Management • Mobile Field Service • PeopleSoft Enterprise HCM Global Payroll Core • Universal Work Queue • VM VirtualBox • WebLogic Server
ULR/Note	https://www.oracle.com/security-alerts/cpujul2025.html: apre un link esterno

PRODOTTO	DESCRIZIONE
Node.js	Rilasciati aggiornamenti di sicurezza che risolvono due vulnerabilità, con gravità "alta", in Node.js, noto software open source per l'esecuzione di codice Javascript. Versioni affette: • 24.x, versioni precedenti alla 24.4.1 • 22.x, versioni precedenti alla 22.17.1 • 20.x, versioni precedenti alla 20.19.4
ULR/Note	https://nodejs.org/en/blog/vulnerability/july-2025-security-releases

PRODOTTO	DESCRIZIONE
Microsoft	Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 130 nuove vulnerabilità, 1 di tipo 0-day Versioni affette: • Azure Monitor Agent • Capability Access Management Service (camsvc) • HID class driver • Kernel Streaming WOW Thunk Service Driver • Microsoft Brokering File System • Microsoft Configuration Manager • Microsoft Edge (Chromium-based) • Microsoft Graphics Component • Microsoft Input Method Editor (IME) • Microsoft MPEG-2 Video Extension • Microsoft Office • Microsoft Office Excel • Microsoft Office PowerPoint • Microsoft Office SharePoint • Microsoft Office Word • Microsoft PC Manager • Microsoft Teams • Microsoft Windows QoS scheduler • Microsoft Windows Search Component • Office Developer Platform • Remote Desktop Client • Role: Windows Hyper-V • SQL Server • Service Fabric • Storage Port Driver • Universal Print Management Service • Virtual Hard Disk (VHDX) • Visual Studio • Visual Studio Code - Python extension • Windows Ancillary Function Driver for WinSock • Windows AppX Deployment Service • Windows BitLocker • Windows Connected Devices Platform Service • Windows Cred SSProvider Protocol • Windows Cryptographic Services • Windows Event Tracing

	• Windows Fast FAT Driver • Windows GDI • Windows Imaging Component • Windows KDC Proxy Service (KPSSVC) • Windows Kerberos • Windows Kernel • Windows MBT Transport driver • Windows Media • Windows NTFS • Windows Netlogon • Windows Notification • Windows Performance Recorder • Windows Print Spooler Components • Windows Remote Desktop Licensing Service • Windows Routing and Remote Access Service (RRAS) • Windows SMB • Windows SPNEGO Extended Negotiation • Windows SSDP Service • Windows Secure Kernel Mode • Windows Shell • Windows SmartScreen • Windows StateRepository API • Windows Storage • Windows Storage VSP Driver • Windows TCP/IP • Windows TDX.sys • Windows Universal Plug and Play (UPnP) Device Host • Windows Update Service • Windows User-Mode Driver Framework Host • Windows Virtualization-Based Security (VBS) Enclave • Windows Win32K - GRFX • Windows Win32K - ICOMP • Workspace Broker
ULR/Note	Aggiornamenti Mensili Microsoft - ACN

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

COLPITO IL CUORE DIGITALE DI NONAME057(16): BLITZ INTERNAZIONALE GUIDATO DALL'ITALIA

Nel corso della settimana tra il 14 e il 17 luglio 2025, le cronache internazionali hanno visto emergere una delle operazioni più significative degli ultimi anni in ambito di sicurezza informatica: l'"Operazione Eastwood". Coordinata da Europol e Eurojust, con il contributo determinante delle forze dell'ordine italiane, l'operazione ha mirato al cuore del gruppo hacker filo-russo NoName057(16), una formazione ben nota nel panorama della cyber-guerra europea per i suoi attacchi contro infrastrutture critiche, enti governativi e aziende strategiche, specialmente nei Paesi considerati "ostili" alla Russia. Tra questi, l'Italia ha avuto un ruolo centrale, sia come obiettivo prediletto che come promotrice delle indagini che hanno portato all'arresto di alcuni membri chiave del collettivo. NoName057(16) non è un nome nuovo: attivo sin dall'inizio dell'invasione russa dell'Ucraina nel 2022, il gruppo si è distinto per una campagna sistematica di attacchi DDoS volta a bloccare, rallentare o rendere inaccessibili i portali di istituzioni, ministeri, media, aeroporti e aziende occidentali. In particolare, l'Italia ha subito decine di attacchi, a partire da quelli al Ministero degli Esteri, a vari Comuni e al sistema giudiziario. La svolta è arrivata dopo mesi di indagini incrociate, nelle quali la Polizia Postale italiana, insieme al CNAIPIC (il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche), ha contribuito in modo determinante. È stata l'Italia infatti ad emettere cinque dei sette mandati di arresto internazionali che hanno poi dato il via ai blitz in più Paesi europei. Durante l'operazione sono stati sequestrati oltre 180 server utilizzati come centri di comando e controllo per gli attacchi, sono stati oscurati 17 canali Telegram che servivano da strumenti di coordinamento e propaganda, e sono state smantellate alcune botnet che coinvolgevano centinaia di dispositivi infetti. Secondo quanto riferito dalle autorità, l'intera struttura operativa del gruppo ha subito un colpo durissimo. Dal giorno successivo ai sequestri NoName057(16) ha interrotto la pubblicazione di nuovi target e gli attacchi DDoS da parte della rete di "volontari digitali" sono praticamente cessati. È difficile dire se si tratti della fine definitiva del collettivo o di una semplice pausa, ma il segnale lanciato è forte e chiaro: l'impunità non è più una garanzia. L'intervento congiunto ha dimostrato che la cooperazione internazionale, se ben strutturata, può avere un impatto reale e immediato anche contro minacce digitali distribuite e ideologicamente motivate. L'Italia esce da questa vicenda con un ruolo rafforzato nella scena della sicurezza informatica europea. La capacità di coordinamento, la competenza investigativa e la volontà politica di reagire in modo deciso agli attacchi hanno fatto la differenza. Tuttavia, come hanno sottolineato esperti e analisti, il rischio non è svanito. I gruppi hacker possono mutare rapidamente, riorganizzarsi sotto nuovi nomi o adottare strategie diverse. In questo senso, l'Operazione Eastwood rappresenta un successo operativo, ma anche un campanello d'allarme: è fondamentale continuare ad investire in formazione, tecnologie di difesa e cooperazione internazionale per contrastare una minaccia che non conosce confini né tregua.

MICROSOFT TEAMS SOTTO ATTACCO, CHIAMATE VOCALI USATE PER DIFFONDERE IL MALWARE MATANBUCHUS

Nel panorama in continua evoluzione delle minacce informatiche, anche gli strumenti di comunicazione quotidiana stanno diventando bersagli e, in certi casi, veri e propri veicoli di attacchi sofisticati. È il caso di Microsoft Teams, una delle piattaforme di collaborazione più utilizzate al mondo. Secondo quanto emerso da analisi condotte da ricercatori di sicurezza, le chiamate vocali automatiche di Teams sono state sfruttate per spingere gli utenti a scaricare e attivare Matanbuchus, un potente malware progettato per aggirare le difese tradizionali e installare ulteriori payload dannosi. Il meccanismo di attacco si basa su una combinazione di social engineering e abuso delle funzionalità legittime di Teams. Le vittime ricevono una notifica di chiamata vocale, apparentemente proveniente da un contatto o gruppo di lavoro credibile, che le indirizza a partecipare ad una riunione o ad ascoltare un messaggio. Tuttavia, una volta cliccato il link, si viene reindirizzati ad un sito web che simula l'interfaccia di Teams o presenta un documento di lavoro fittizio. Qui entra in scena Matanbuchus: viene proposta l'apertura di un file o l'attivazione di contenuti "protetti", dietro cui si nasconde il loader. Matanbuchus non è nuovo nel panorama del malware, in quanto è stato identificato per la prima volta nel 2021 come loader-as-a-service, ovvero un componente malevolo venduto sul dark web che consente a gruppi criminali di distribuire ransomware, spyware e altri malware ad alto impatto. Ciò che lo rende particolarmente pericoloso è la sua capacità di eseguire codice PowerShell da remoto, aggirare i controlli UAC (User Account Control) e sfruttare vulnerabilità di sistema per ottenere privilegi elevati. Una volta installato, può scaricare ulteriori minacce come Cobalt Strike o agenti ransomware come Conti e BlackCat. In questo nuovo schema, la novità sta tutta nell'uso di una piattaforma diffusa ed affidabile come Microsoft Teams per guadagnarsi la fiducia dell'utente. La combinazione di una chiamata in app ed un invito apparentemente legittimo abbassa le difese psicologiche e porta la vittima a cliccare con maggiore disinvoltura, soprattutto in contesti aziendali dove le videoconferenze sono frequenti e spesso urgenti. Microsoft non ha tardato a reagire; in un aggiornamento della propria documentazione sulla sicurezza, ha riconosciuto il potenziale abuso del sistema di notifiche ed ha avviato un'indagine interna per identificare eventuali falle o comportamenti anomali lato server. L'azienda ha inoltre ribadito l'importanza di abilitare protezioni avanzate come Defender for Office 365, bloccare l'apertura di macro da fonti esterne e formare il personale contro le tecniche più diffuse di social engineering. L'episodio rappresenta l'ennesima conferma di una tendenza ormai consolidata: gli attaccanti non si limitano più a cercare falle nei software, ma sfruttano le abitudini, i ritmi e la fiducia degli utenti nei confronti degli strumenti che utilizzano quotidianamente. Per utenti e aziende, la lezione è chiara: è necessario considerare ogni canale digitale come un potenziale vettore d'attacco, anche (e forse soprattutto) quelli che sembrano più sicuri perché legati a provider affidabili.

VIOLAZIONE A BIGONE CON PERDITA DI 27 MILIONI IN ASSET DIGITALI

L'ultima vittima di una lunga serie di attacchi rivolti al mondo delle criptovalute, è l'exchange BigONE, uno dei nomi più noti in Asia, colpito da una violazione che ha portato alla sottrazione di oltre 27 milioni di dollari in asset digitali. Secondo quanto riportato da diverse fonti di sicurezza blockchain, si tratterebbe di un attacco mirato condotto da un singolo attore altamente sofisticato, che ha sfruttato una vulnerabilità operativa per esfiltrare i fondi dai cosiddetti "hot wallet" della piattaforma. L'attacco è avvenuto in modo silenzioso e preciso, senza causare interruzioni visibili ai servizi dell'exchange. Gli investigatori ritengono che l'autore del furto sia riuscito ad accedere a chiavi private o token d'accesso API interni, compromettendo così il sistema di firma delle transazioni senza generare allarmi immediati. Solo dopo il trasferimento di grandi quantità di Ethereum (ETH), Bitcoin (BTC) e altre stablecoin come USDT verso indirizzi non etichettati, ossia non associati ad exchange ufficiali o wallet noti, il team di BigONE si è accorto dell'anomalia e ha confermato la violazione. Il valore stimato del furto si aggira attorno ai 27 milioni di dollari, una cifra che colloca questo incidente tra i più gravi del 2025. Dopo l'accaduto, BigONE ha sospeso temporaneamente i prelievi, rassicurando gli utenti sul fatto che le perdite saranno coperte dal fondo di garanzia dell'exchange. Tuttavia, come spesso accade in questi casi, la fiducia degli investitori è stata scossa. Le reazioni online non si sono fatte attendere: numerosi utenti hanno riportato ritardi nei rimborsi, mentre alcuni analisti mettono in dubbio la sostenibilità economica della compensazione promessa, almeno per gli asset meno liquidi. Il furto solleva questioni cruciali sulla gestione della sicurezza negli hot wallet che, per garantire velocità di transazione, sono per forza di cose esposti a rischi maggiori rispetto ai cold wallet, non connessi alla rete. Non è la prima volta che un exchange subisce un attacco di questo tipo, ma ciò che colpisce è la precisione con cui è stato condotto, senza lasciare tracce evidenti né indizi sul possibile autore. Le prime indagini condotte da società di analisi sembrano indicare che il flusso di fondi rubati è stato rapidamente offuscato attraverso mixer decentralizzati, rendendo complessa ogni operazione di tracciamento. Al momento, BigONE collabora con le autorità competenti e con altri exchange internazionali per bloccare eventuali movimenti successivi degli asset rubati, nella speranza che almeno una parte dei fondi possa essere congelata prima che venga definitivamente convertita o nascosta. Tuttavia, la natura stessa delle criptovalute, fondata sull'anonimato e sulla mancanza di intermediazione, rende molto difficile un recupero completo. Questo episodio non fa che rafforzare il dato sempre più evidente per cui la sicurezza in ambito crypto non è più solo una questione tecnica, ma anche strategica e culturale. Finché gli exchange continueranno a bilanciare la comodità operativa con la sicurezza infrastrutturale, ci sarà sempre un margine di rischio.

IL MALWARE LAMEHUG USA INTELLIGENZA ARTIFICIALE PER RUBARE DATI DA WINDOWS IN TEMPO REALE

Scoperto nuovo malware LameHug che utilizza modelli linguistici di grandi dimensioni (LLM, Large Language Model), simili a quelli che alimentano chatbot come ChatGPT, per generare in tempo reale comandi adattivi capaci di esfiltrare dati da sistemi operativi Windows, modificando il proprio comportamento in base all'ambiente in cui viene eseguito. Questa rapidità di "pensiero", seppur ancora grezza rispetto all'intelligenza umana, rende LameHug estremamente pericoloso. Il malware non ha bisogno di sapere in anticipo quali dati cercare o quali directory colpire: osserva il contesto, interroga l'ambiente di sistema e genera query, script o comandi personalizzati per massimizzare l'esfiltrazione. Ad esempio, su un computer che presenta cartelle contenenti dati contabili, LameHug potrebbe generare comandi PowerShell per cercare file con estensioni .xls o .csv, o addirittura leggere nomi dei documenti per filtrare quelli di interesse. Secondo i ricercatori di sicurezza che lo stanno monitorando, LameHug include al suo interno un componente LLM light-weight o si appoggia ad un'istanza remota criptata per generare i comandi. Ciò significa che il codice malevolo invia informazioni sull'ambiente infetto ad un server remoto che risponde con comandi creati al momento, rendendo la rilevazione comportamentale molto più complessa. È l'equivalente digitale di un ladro che entra in casa e, invece di seguire un piano preimpostato, decide dove cercare in base a ciò che vede. Uno dei punti più preoccupanti riguarda la flessibilità di LameHug nel linguaggio di scripting. Può generare codice batch, PowerShell, comandi WMI, o perfino script in Python o VBScript se trova che l'ambiente supporta interpreti alternativi. Il tutto con uno scopo ben preciso: rubare credenziali, archiviare screenshot, elencare file sensibili e inviarli silenziosamente a server C2 (Command and Control). Al momento, non è ancora chiaro chi ci sia dietro LameHug. Gli indicatori di compromissione (IoC) trovati nei primi campioni non permettono di collegare il malware con certezza ad attori noti, anche se alcune tecniche ricordano campagne APT matrice russa e cinese. La sofisticazione, in particolare l'uso dell'AI per creare comandi operativi in tempo reale, suggerisce un attacco mirato. Questa evoluzione rappresenta un cambio di paradigma: fino a poco tempo fa, l'uso dei LLM nel cybercrime era ipotizzato soprattutto per generare phishing o scrivere codice dannoso in modo più semplice. Con LameHug, invece, si entra in un territorio nuovo, quello in cui l'intelligenza artificiale non serve solo a creare malware, ma diventa parte attiva del malware stesso, contribuendo a renderlo più dinamico, imprevedibile e mirato. Per le aziende e i singoli utenti, ciò si traduce in una maggiore difficoltà nella prevenzione. Le soluzioni di sicurezza tradizionali, basate su firme o pattern statici, rischiano di non bastare. È sempre più importante affiancare strumenti di rilevamento comportamentale, analisi in tempo reale e segmentazione delle reti, così da limitare i danni anche in caso di infezione. E, naturalmente, serve una maggiore attenzione su come e dove vengono integrati modelli di AI nei sistemi operativi e nelle applicazioni.

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 14 – 20 Luglio 2025
Settimana con un volume elevato di vulnerabilità CRITICAL e HIGH, concentrate in particolare su software open-source PHP (PHPGurukul, Code-Projects), dispositivi IoT/Router (D-Link, Tenda) e ambienti cloud Microsoft (Azure ML/DevOps).
Sono state pubblicate oltre 20 CVE gravi, molte delle quali con exploit pubblici disponibili su GitHub.
I principali rischi includono: SQL injection non autenticata, privilege escalation, RCE, accesso remoto non autorizzato.
CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit Pubblico	Prodotto Coinvolto	Descrizione Sintetica
CVE-2025-49746	CRITICAL	18/07/2025	❌	Microsoft Azure ML	Privilege escalation via authorization flaw
CVE-2025-49747	CRITICAL	18/07/2025	❌	Microsoft Azure ML	Privilege escalation via missing authorization
CVE-2025-47158	CRITICAL	18/07/2025	❌	Azure DevOps	Authentication bypass via immutable data
CVE-2025-7599	CRITICAL	14/07/2025	✅	PHPGurukul Dairy Farm	SQLi in `/invoice.php` via param `del`
CVE-2025-7558	CRITICAL	14/07/2025	✅	Code-Projects Voting System	SQLi in `positions_add.php`

CVE-2025-7612	CRITICAL	18/07/2025	✅	Code-Projects Mobile Shop	SQLi in `login.php`
CVE-2025-7754	CRITICAL	14/07/2025	✅	Patient Record Mgmt (Code-Projects)	SQLi in `xray_form.php`
CVE-2025-7790	CRITICAL	14/07/2025	✅	D-Link DI-8100	Stack buffer overflow in `menu_nat.asp`
CVE-2025-7555	CRITICAL	14/07/2025	✅	Voting System (Code-Projects)	SQLi in `voters_add.php`
CVE-2025-7556	CRITICAL	14/07/2025	✅	Voting System (Code-Projects)	SQLi in `voters_edit.php`
CVE-2025-7561	CRITICAL	14/07/2025	✅	PHPGurukul Fire Reporting	SQLi in `team-ontheway-requests.php`
CVE-2025-7605	CRITICAL	14/07/2025	✅	AVL Rooms (Code-Projects)	SQLi in `profile.php`
CVE-2025-30749	CRITICAL	14/07/2025	❌	Oracle Java SE / GraalVM	RCE in 2D graphics component
CVE-2025-50106	CRITICAL	14/07/2025	❌	Oracle Java SE / GraalVM	RCE in 2D rendering pipeline

CVE-2025-53024	HIGH	16/07/2025	❌	Oracle VirtualBox	Local privilege escalation
CVE-2025-7610	HIGH	18/07/2025	✅	Electricity Billing System	SQLi in `change_password.php`
CVE-2025-7855	CRITICAL	19/07/2025	✅	Tenda FH451	Stack overflow in `fromqossetting`
CVE-2025-7553	CRITICAL	14/07/2025	✅	D-Link DIR-818LW	OS Command Injection via NTP
CVE-2025-7793	CRITICAL	18/07/2025	✅	Tenda FH451	Stack overflow in `formWebTypeLibrary`
CVE-2025-7611	CRITICAL	18/07/2025	✅	Wedding Reservation (Code-Projects)	SQLi in `global.php`
CVE-2025-7757	CRITICAL	14/07/2025	✅	Hospital Mgmt System (PHPGurukul)	SQLi in admin dashboard
CVE-2025-53770	CRITICAL	20/07/2025	✅	Microsoft Sharepoint	RCE

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

Vendor e Tecnologie Coinvolti

- **Microsoft Azure ML e DevOps**
    - Diverse CVE di escalation e bypass su sistemi cloud Microsoft, in particolare su ambienti DevOps e Machine Learning.
- **PHPGurukul & Code-Projects**
    - Oltre 10 vulnerabilità SQLi critiche con exploit pubblici disponibili. Coinvolti moduli come Complaint, Payroll, Patient, Fire Reporting, AVL Rooms, Voting System, Wedding Reservation, ecc.
- **Oracle Java SE & GraalVM**
    - RCE su componenti 2D. Critico per applicazioni Java desktop o server-side con rendering attivo.
- **D-Link & Tenda Router**
    - Stack overflow e OS command injection su modelli DI-8100, DIR-818LW, e FH451. Esposti da remoto se non protetti.
- **Electricity Billing System**
    - SQLi semplice su cambio password → escalation immediata.

Distribuzione Giornaliera delle CVE

- **14 luglio 2025**
    - Rilasciate la maggior parte delle CVE relative a sistemi PHP open-source.
    - Disclosure D-Link, Oracle Java, Voting System, Hospital Mgmt, Fire Reporting.
- **16 luglio 2025**
    - CVE Oracle VirtualBox (escalation locale).
- **18 luglio 2025**
    - Advisory Microsoft Azure ML / DevOps e vulnerabilità Tenda (RCE via overflow).
    - Nuove SQLi in Code-Projects Wedding Reservation e Electricity Billing.
- **19 luglio 2025**
    - Overflow critico in interfaccia web di Tenda FH451 (formWebTypeLibrary).

Raccomandazioni Operative

- **Patch Prioritarie**
  - **Azure ML/DevOps** → aggiornare servizi cloud + revisione RBAC
  - **Oracle Java SE / VirtualBox** → RCE critiche su pipeline grafica e escalation locali
  - **D-Link / Tenda router** → firmware aggiornato, WAN disabilitata
  - **PHPGurukul & Code-Projects** → SQLi multiple con PoC pubblici → rimuovere o aggiornare
- **Monitoraggio e Mitigazioni**
  - Audit endpoint: login.php, profile.php, invoice.php, save_*, delete_*
  - WAF + query parametriche per bloccare SQLi
  - Controllo accessi e logging sui router e sulle API cloud

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-49706	Microsoft Office SharePoint	6.3
CVE-2025-6965	SQLite	N/A
CVE-2025-20337	Cisco Identity Services Engine	N/A
CVE-2025-54309	CrushFTP	N/A
CVE-2025-6558	Google Chrome	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-2025-49747 CVE-2025-49746	Microsoft Azure Machine Learning	N/A
VULNERABILITÀ	Queste vulnerabilità riguardano un problema di autorizzazione all'interno del servizio Azure Machine Learning (una piattaforma cloud di Microsoft per lo sviluppo e la gestione di modelli di intelligenza artificiale). In pratica, un utente già autenticato (quindi con qualche livello di accesso) può ottenere più privilegi del dovuto, ad esempio diventare amministratore o accedere a risorse a cui non dovrebbe avere accesso, attraverso la rete.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-7921	Modem/router sviluppati da Askey (marchio OEM che produce dispositivi spesso venduti con altri nomi da provider Internet – come TIM, Spectrum, o altri)	N/A
VULNERABILITÀ	Alcuni modem Askey hanno una vulnerabilità di buffer overflow nello stack. Questa falla permette a un attaccante remoto, senza bisogno di credenziali, di inviare dati malevoli per prendere il controllo del dispositivo ed eseguire codice arbitrario.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-7697	Plugin WordPress: Integration for Google Sheets and Contact Form 7 / WPForms / Elementor / Ninja Forms (fino alla v1.1.1)	N/A
VULNERABILITÀ	Il plugin Integration for Google Sheets and Contact Form 7, WPForms, Elementor, Ninja Forms per WordPress è vulnerabile a una PHP Object Injection (fino alla versione 1.1.1), a causa della deserializzazione di input non affidabile nella funzione verify_field_val(). Se combinato con il plugin Contact Form 7, un attaccante non autenticato può cancellare file arbitrari (incluso wp-config.php), causando interruzione del sito o addirittura esecuzione di codice remoto (RCE).	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-7343	Digiwin SFT	N/A
VULNERABILITÀ	Il software SFT sviluppato da Digiwin presenta una vulnerabilità di tipo SQL Injection, che consente ad attaccanti remoti non autenticati di iniettare comandi SQL arbitrari per leggere, modificare o eliminare i contenuti del database.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-53770	Microsoft Sharepoint	N/A
VULNERABILITÀ	La vulnerabilità CVE-2025-53770 in Microsoft SharePoint Server on-premises è causata dalla deserializzazione di dati non attendibili, un processo in cui il software ricostruisce oggetti a partire da dati esterni. Se questi dati non vengono adeguatamente verificati, un attaccante può inviare oggetti malevoli che, una volta deserializzati, permettono l'esecuzione di codice arbitrario da remoto, senza autenticazione. Microsoft ha confermato che la falla è già attivamente sfruttata ("exploit in the wild") e sta lavorando a una patch completa. Nel frattempo, è fondamentale applicare le mitigazioni indicate nella documentazione del CVE per ridurre il rischio di compromissione.	

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-2025-25257
DESCRIZIONE	
Fortinet FortiWeb nelle versioni dalla 7.0.10 fino alla 7.6.3 presenta una vulnerabilità di SQL Injection causata da una gestione inadeguata di elementi speciali nei comandi SQL, che permette a un attaccante remoto non autenticato di eseguire comandi SQL non autorizzati inviando richieste HTTP o HTTPS appositamente costruite. Questa falla consente potenzialmente di manipolare o accedere il database del dispositivo compromettendo la sicurezza.	

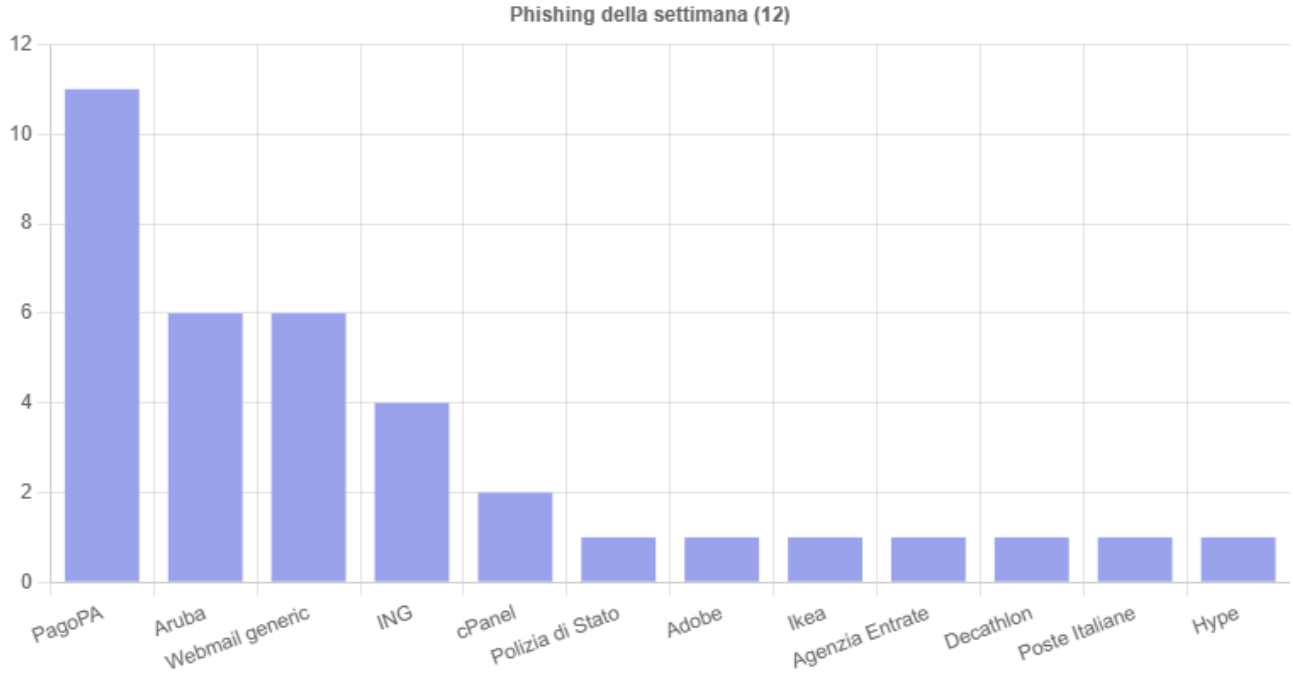
CVE	CVE-2025-47812
DESCRIZIONE	
Wing FTP Server prima della versione 7.4.4 gestisce in modo errato i byte '\0' nelle interfacce web utente e amministratore, permettendo l'iniezione di codice Lua arbitrario nei file di sessione degli utenti; ciò consente l'esecuzione remota di comandi di sistema con i privilegi del servizio FTP (di solito root o SYSTEM), rappresentando una vulnerabilità critica che può portare al completo compromesso del server, sfruttabile anche tramite account FTP anonimi.	

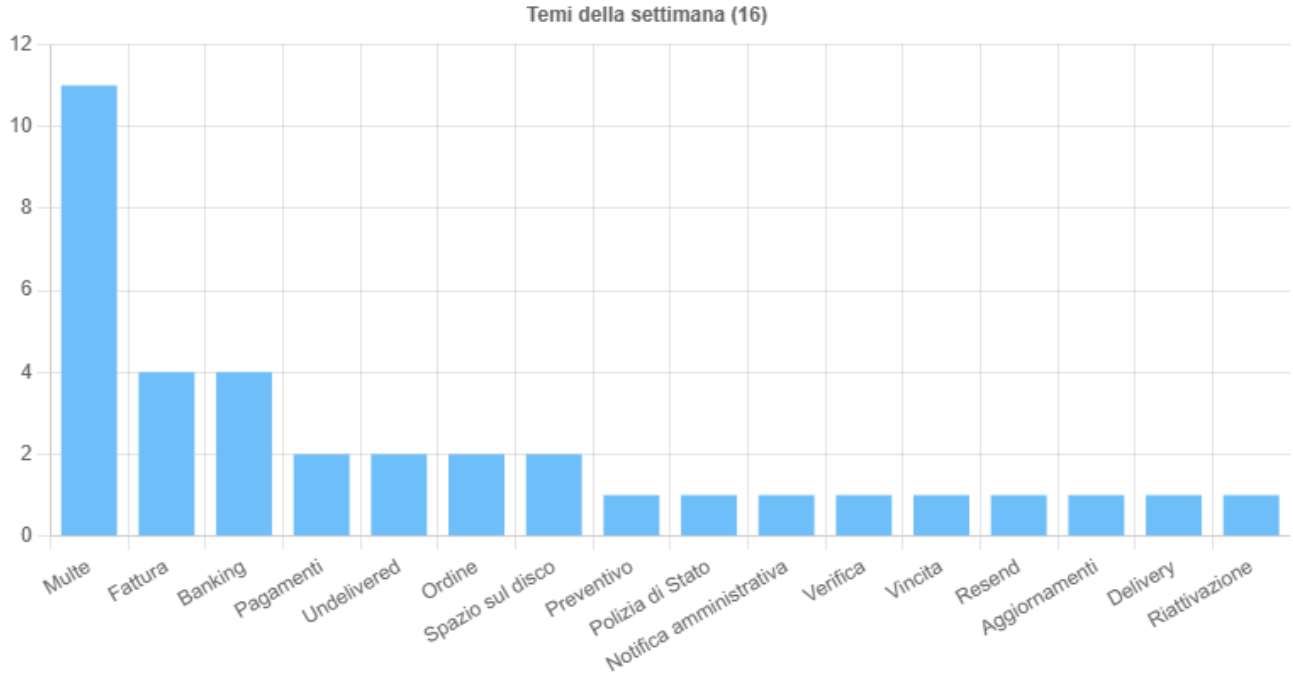
4 Attacchi

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.

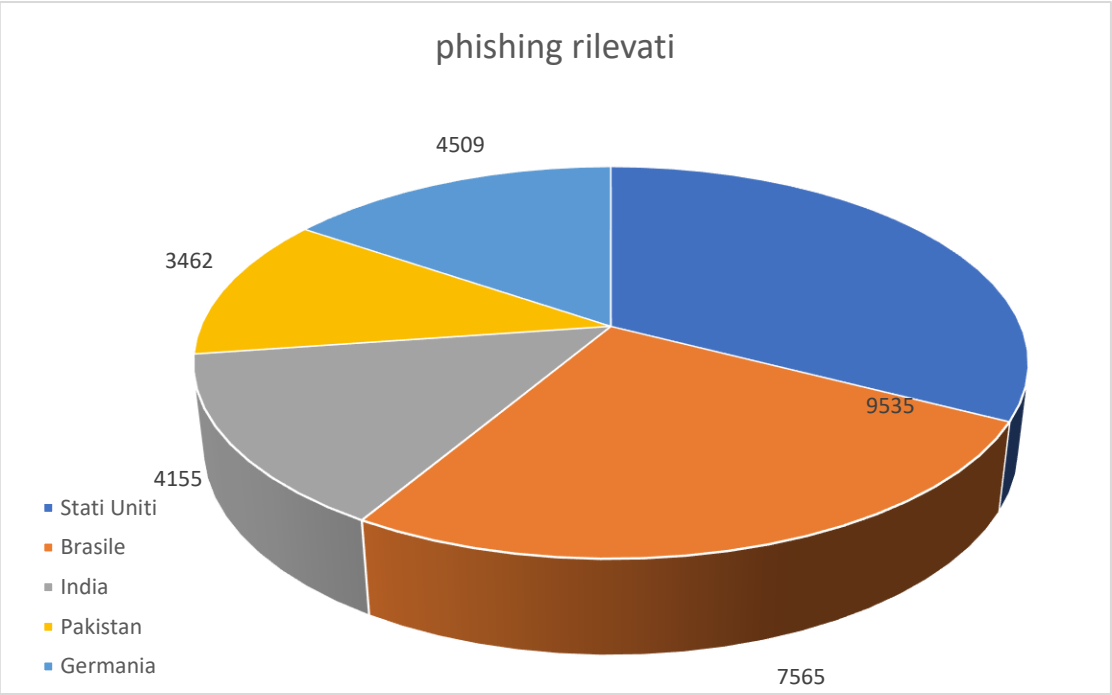




Fonte :CERT-AGID

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.



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

Executive Summary

L'email con oggetto **"E-mail Account Verification For mailvittima@victim[.]com !!!"** è un tentativo di **phishing credential-harvesting** che sfrutta il brand "Roundcube Webmail" per indurre l'utente a "verificare" il proprio account entro 24 ore. Il messaggio proviene dall'IP 167[.]160[.]161[.]96 – un blocco di hosting (AS214943 Railnet / Virtualine Technologies) più volte segnalato per spam e attività malevole – e contiene un pulsante **VERIFY** che reindirizza a https://gig[.]com[.]sg/001/Roundcubenvi.html, dominio classificato da diversi motori OSINT come **malicious**. La combinazione di mittente internamente spoofato, assenza di meccanismi SPF/DKIM/DMARC, hosting IP compromesso e URL di recente registrazione rende l'email ad alto rischio.

- Header & Infrastructure Analysis

Campo	Valore normalizzato	Evidenza
Mittente visibile	Noreply@victim[.]com	trace nei raw header
IP origine	167[.]160[.]161[.]96	Presenza su abuseip db nella settimana in esame. Segnalazioni su virustotal come “Suspicious”, “Malicius”, e “Malware”.
Ricezione	mail.victim[.]com via OpenSMTPD	spoof interno
SPF / DKIM / DMARC	non pubblicati o non allineati	facilita spoofing

- **Reputazione IP**

AbuseIPDB mostra circa 10 segnalazioni recenti di “Phishing Email Spam” per questo IP.

- Malicious URL Analysis

https://gig[.]com[.]sg/001/Roundcubenvi.html#mailvittima@victim[.]com

  - **Maltiverse** classifica l’URL come *malicious* attivo.
  - **Hybrid-Analysis** evidenzia indicatori MITRE T1566 (Phishing) e dominio registrato da 75 giorni.
  - Il dominio gig[.]com[.]sg compare in diverse liste di ad-blocking / phishing (KADhosts).
  - Il tema “Roundcube” è coerente con campagne note di phishing che imitano il webmail open-source.

- Content & Social-Engineering Techniques

Il corpo HTML personalizza il saluto con l'alias locale ("mailvittima"), minaccia la **sospensione della casella entro 24 ore** e propone un solo call-to-action ("VERIFY") colorato (rgb 53, 88, 168) che porta al link malevolo. Gli elementi riflettono:

- **Tattica Urgency/Scarcity** – finestra di 24 h.
- **Brand Spoofing** – uso di Roundcube e del dominio interno victim[.]com.
- **Single-Click Trap** – pulsante centrale con ancoraggio all'indirizzo email per pre-riempire form di phishing.

- MITRE ATT&CK Mapping

Fase	Tecnica	Evidenza
Initial Access	**T1566.002 (Phishing via link)**	email con URL gig[.]com[.]sg
Credential Access	**T1056.007 (Web Credential Phishing)**	form ospitato su pagina Roundcube fake
Command & Control	**T1071.001 (Web Protocols)**	URL HTTPS verso dominio esfiltrazione
Defense Evasion	**T1204 (User Execution)**	richiesta click utente

- Indicators of Compromise (IoC)

Tipo	Valore (punteggiato → [.])	Fonte
IP SMTP	167[.]160[.]161[.]96	Abuse segnalato (abuseipdb[.]com)
ASN	AS214943 Railnet / Virtualine	(ipregistry[.]co)
Dominio URL	gig[.]com[.]sg	(maltiverse[.]com)
Path	[/]001[/]Roundcubenvi[.]html	HTML link
Email spoof	Noreply@victim[.]com	Header

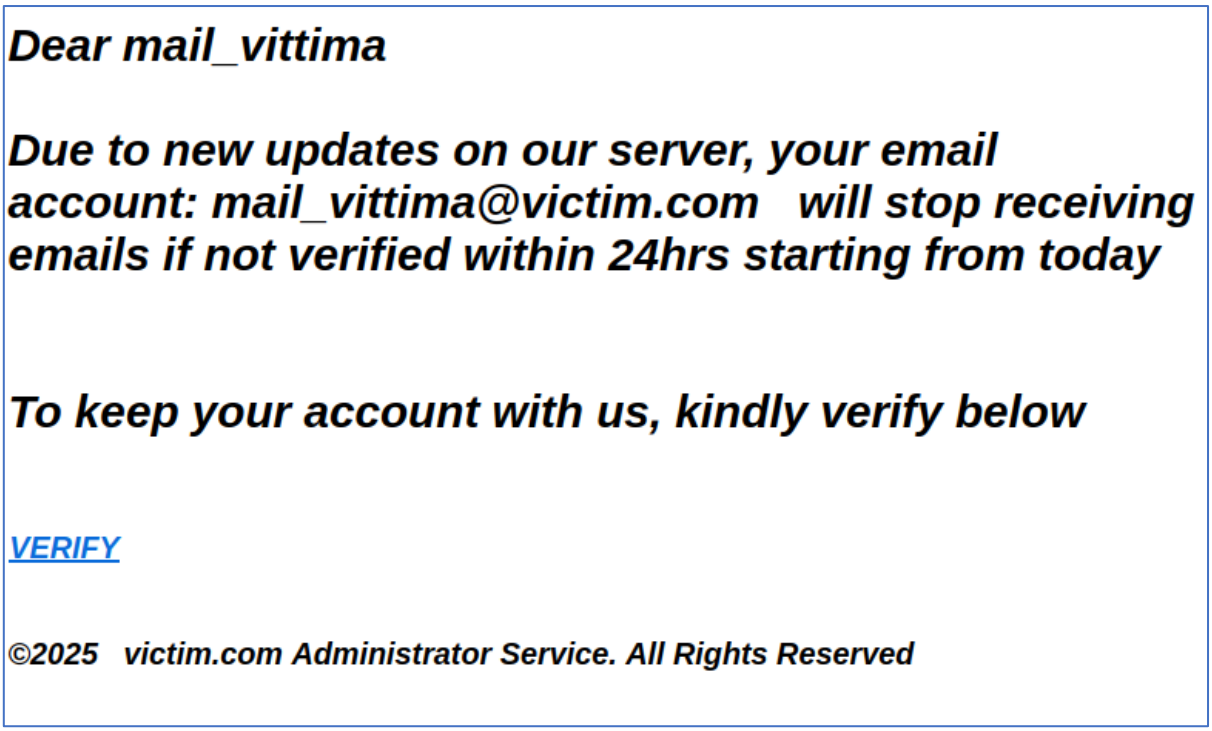
- Risk Assessment

Vettore	Gravità	Commento sintetico
Compromissione credenziali	Alta	URL di phishing mirato a rubare password webmail
Compromissione dominio mittente	Media	Mancanza SPF/DKIM/DMARC facilita spoof
Impatto reputazione	Media	Possibili campagne in uscita da IP/ASN spam
Malware secondario	Bassa*	Non rilevati allegati; rischio successivo di dropper

* il dominio ospita spesso kit credential-grabber, non malware binario; rischio escalation se credenziali vengono riutilizzate.

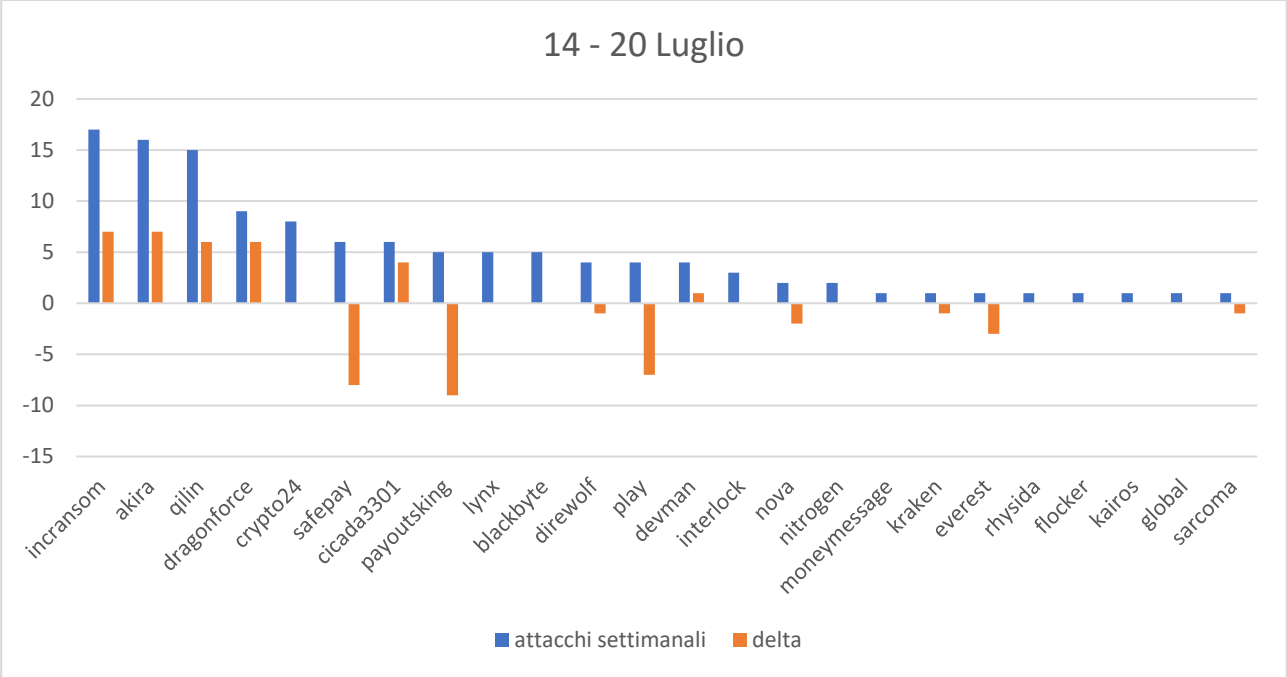
- Raccomandazioni
  - **Bloccare** l'IP 167[.]160[.]161[.]96 e il dominio gig[.]com[.]sg a livello di gateway e EDR.
  - **Abilitare SPF, DKIM e DMARC** su victim[.]com per impedire spoof futuro.
  - **Imporre MFA** agli account di posta; invalidare credenziali esposte.
  - **Formare gli utenti** sui finti avvisi Roundcube/"verifica account" e sulle finestre temporali urgenti.
  - **Monitorare i log** per connessioni in uscita verso gig[.]com[.]sg e sottodomini correlati.

Qui di seguito un screenshot della mail:

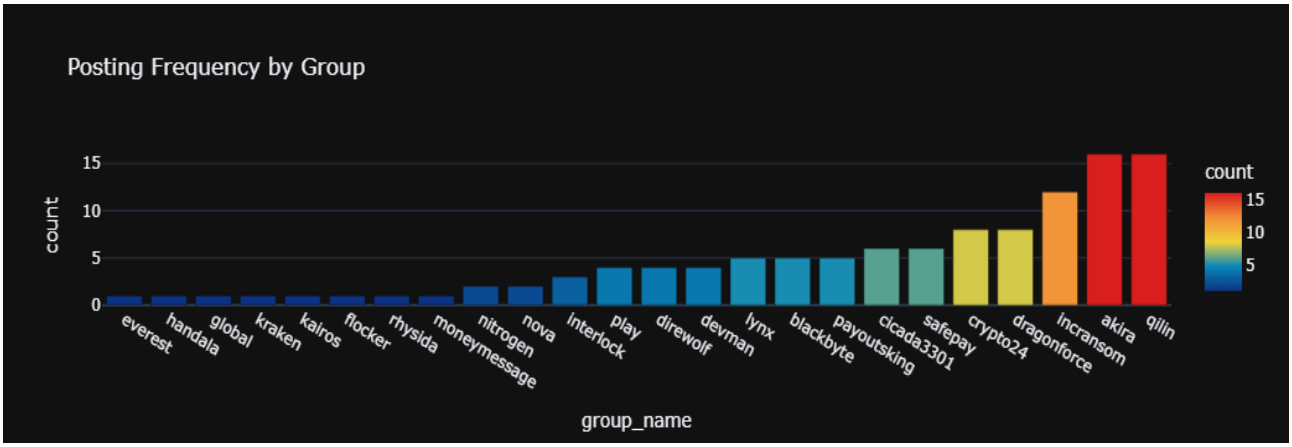


4.2 Ransomware

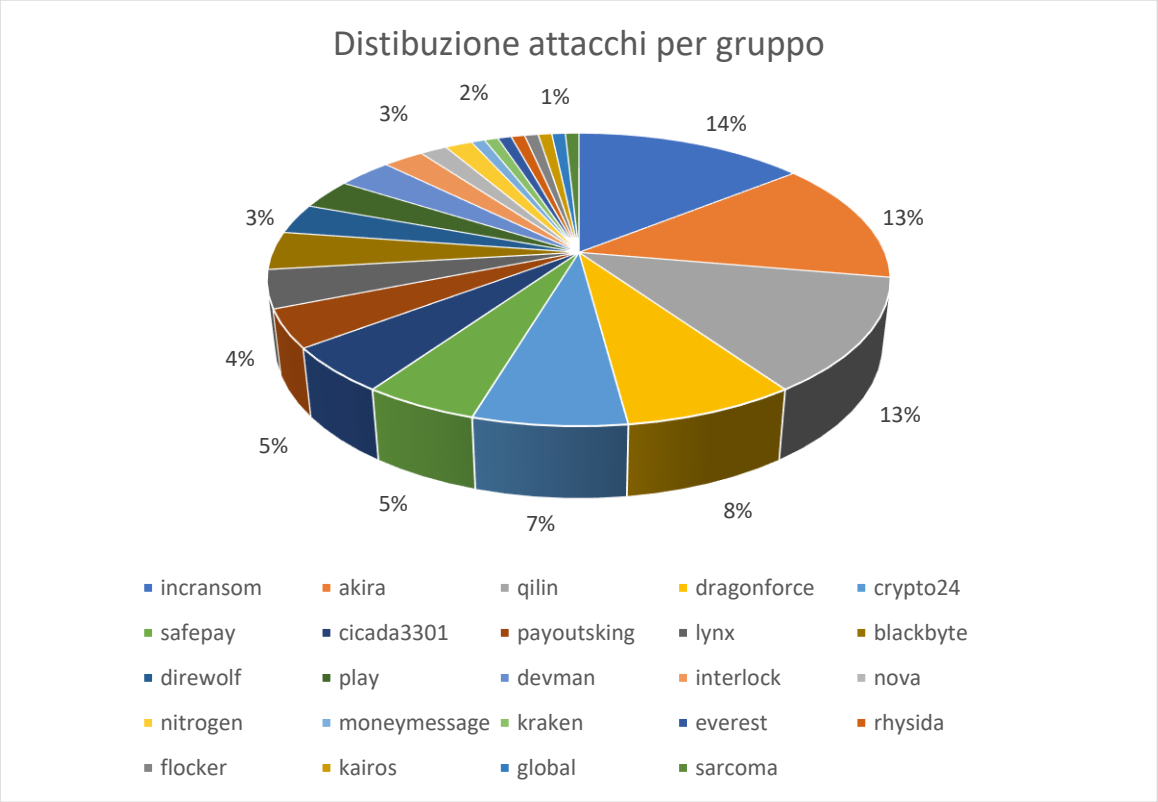
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (14 - 20 Luglio). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

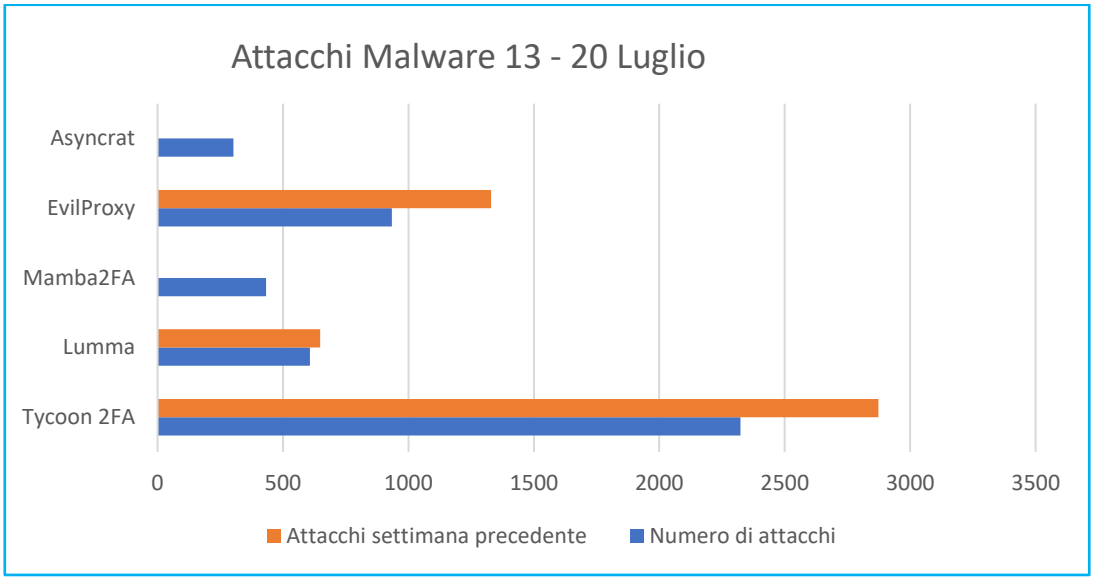


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



4.3 Malware

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



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

- **LameHug (malware AI di APT28)**

LameHug è un nuovo malware scoperto dal CERT-UA il 10 luglio 2025, attribuito all'APT russo Sofacy/Strontium (APT28). Si tratta del primo malware "AI-powered" che sfrutta un modello di linguaggio (LLM) per generare dinamicamente codice malevolo eseguibile. LameHug viene veicolato tramite email di spear-phishing, scarica ed esegue in automatico payload Python che comunicano con un servizio Hugging Face (modello Qwen) per trasformare input testuali in azioni malevole. Il malware effettua quindi uno scan in locale della macchina su cui è installato in modo da ottenere importanti informazioni quali enumerazione di processi, servizi, connessioni di rete e file sensibili, raccoglie documenti e dati nel %PROGRAMDATA%\info, e li esfiltra verso server controllati dagli attaccanti.

Descrizione: malware per Windows che utilizza l'intelligenza artificiale ed un modello LLM per generare in tempo reale comandi e payload, viene diffuso via email "mirate" con allegati ZIP malevoli. Colpisce principalmente enti governativi e organizzazioni ucraine.

IoC:

Tipo	Indicatore
Email (ZIP)	Додаток.pdf.zip (allegato malevolo)
File eseguibili	Attachment.pif, AI_generator_uncensored_Canvas_PRO_v0.9.exe, AI_image_generator_v0.95.exe

MITRE ATT&CK:

- T1566.001 – Spearphishing con allegati
- T1059.006 – Esecuzione di script Python
- T1027 – Offuscamento dei file
- T1057 – Discovery dei processi
- T1083 – Discovery dei file e directory
- T1041 – Esfiltrazione attraverso canali di comando e controllo

Rilevazione/Mitigazione:

- Utilizzare soluzioni EDR/Antivirus con capacità di analisi comportamentale per individuare attività sospette, specialmente relative a script Python.
- Filtrare allegati ZIP ed eseguirli in sandbox per analisi approfondita.
- Limitare l'esecuzione di script non firmati su sistemi aziendali.
- Monitorare connessioni verso servizi LLM (Large Language Model) non usuali.
- Fornire formazione agli utenti per riconoscere email di phishing sofisticate.

Livello di rischio: Critico – malware molto avanzato e difficile da individuare, con capacità di evasione AI e targeting statale.

- **Gruppo Diskstation (ransomware NAS Synology)**

Il gruppo "Diskstation" è l'autore del ransomware specializzato in attacchi a dispositivi NAS Synology esposti su Internet. Attivo almeno dal 2021, il gruppo ha cambiato nome (DiskStation Security, Quick Security, LegendaryDisk, ecc.) ma continua a cifrare i file negli apparati NAS, richiedendo riscatti da 10.000 a 100.000 dollari. A metà luglio 2025 è stata portata a termine l'operazione "Elicius" della Polizia Postale italiana, che ha individuato ed arrestato alcuni membri del gang, attiva a livello internazionale ma con molte vittime in Lombardia (aziende di produzione video, ONG, studi di design).
Descrizione: ransomware mirato a dispositivi NAS Synology; cifra i dati e cancella backup (shadow copy), lasciando nota di riscatto. Le campagne del gruppo utilizzano motori di brute-force su credenziali deboli delle interfacce NAS, combinati a malware di cifratura avanzati. Recentemente sono stati colpiti anche enti italiani (eg. Regno Unito–Italia) con una serie di attacchi in Lombardia.

MITRE ATT&CK:

- T1486 – Data Encrypted for Impact (cifratura dei file)
- T1485 – Data Destruction (eliminazione dei backup)
- T1547 – Boot or Logon Autostart Execution (es. modifica di account amministratori)

Rilevazione e mitigazione:

- Disabilitare l'accesso NAT diretto alla porta DSM del NAS

- Applicare patch di sicurezza Synology in modo tempestivo
- Implementare autenticazione forte e accesso tramite VPN per la gestione remota
- Eseguire backup regolari e offline dei dati
- Adottare soluzioni EDR/AV che monitorino l'attività sospetta sui dispositivi NAS
- Fornire formazione al personale IT per identificare tentativi di login anomali sui sistemi NAS

Livello di rischio: Alto – ransomware mirato che può bloccare sistemi di produzione e causare perdite di dati ingenti.

➢ **Konfety (trojan Android con evasion avanzata)**

Konfety è un trojan bancario/stealer per Android tornato alla ribalta con una nuova variante altamente evasiva. Il 18 luglio 2025 Zimperium ha annunciato la scoperta di una versione aggiornata di Konfety. Gli aggressori utilizzano una doppia app "specchio": un'app legittima sul Google Play Store ed una versione malevola distribuita su store terzi con stesso nome di pacchetto e permessi nascosti. La nuova variante vanta sofisticate tecniche di offuscamento: modifica arbitraria della struttura ZIP dell'APK (compressione fittizia, flag falsi) per far collassare gli strumenti di analisi, caricamento di codice crittografato a runtime e comportamento ad-fraud (utilizzo del SDK CaramelAds per veicolare payload e spam). L'app infetta può dirottare utenti verso siti malevoli, installare app non autorizzate e mostrare notifiche indesiderate.
Descrizione: trojan Android/rustock-style riemerso con nuove tecniche di evasione. La variante 2025 si camuffa da app ordinaria (stesso package ID della versione legit su Play), ignora scanner statici tramite manipolazione ZIP e limita la sua visibilità (nasconde icona, attiva comportamenti fraudolenti solo in certe regioni). Obiettivo primario: frodi pubblicitarie e furto dati su dispositivi mobili.

IoC: non pubblicati indicatori concreti; è noto che viene usato un nome di pacchetto identico per la falsa app (sperimentale, non divulgato pubblicamente) e sfrutta domini di annunci.

Tipo	Indicatore
APK Android	App "legittima" vs malevola con stesso package name (doppio APK)

MITRE ATT&CK :
- T1475.001 – APK Obfuscation (offuscamento del pacchetto per eludere la rilevazione)
- T1497 (Mobile) – Sandbox Evasion (evasione degli ambienti di analisi automatica)

Rilevazione/Mitigazione:
- Utilizzare soluzioni di sicurezza mobile (MDM/EMM) con funzionalità di analisi comportamentale delle app
- Vietare l'installazione di app da store non ufficiali

- Abilitare Google Play Protect su tutti i dispositivi
- Monitorare anomalie di rete, ad esempio traffico verso domini sospetti
- Limitare i permessi delle app, soprattutto quelli relativi a dati sensibili
- Educare gli utenti ad installare esclusivamente app da fonti attendibili

Livello di rischio: Alto – malware sofisticato per dispositivi mobili con capacità di eludere i controlli standard.

➢ **Matanbuchus 3.0 (malware loader via Microsoft Teams)**

Matanbuchus è un loader malware-as-a-service noto dal 2021, usato per scaricare payload secondari (es. Cobalt Strike, ransomware). A luglio 2025 è emersa la versione 3.0 con funzionalità avanzate. In un attacco recente ricostruito da Morphisec, gli aggressori hanno sfruttato chiamate esterne via Microsoft Teams (finti operatori help-desk) per indurre gli utenti ad avviare lo strumento Microsoft Quick Assist, che a sua volta ha eseguito uno script PowerShell auto-avviante il loader Matanbuchus 3.0. Le novità di Matanbuchus 3.0 includono protocolli di comunicazione criptati migliorati, esecuzione in-memory, file di configurazione XML codificati, supporto remoto via WMI/CMD/PowerShell e capacità di eseguire payload MSI, DLL o shellcode. Il loader si persiste creando un'attività pianificata (scheduler) "EventLogBackupTask" e verifica la presenza di strumenti di sicurezza sul sistema.

Descrizione: malware di tipo loader (MaaS) che agisce da veicolo per altri payload (ransomware, RAT, beacon). La variante 3.0 è altamente evasiva: distribuita via Teams/phishing ingannevole, implementa offuscazione spinta, esecuzione stealth in memoria e supporto shell posteriore (WQL, CMD, PowerShell). È stato osservato in attacchi reali contro aziende cui è stato richiesto un riscatto.

IoC:

Tipo	Indicatore
URLs	• 94.159.113[.]33 – fixuplink[.]com [RU] • bretux[.]com • nicewk[.]com • emorista[.]org • notepad-plus-plu[.]org
Hashs	• libcurl.dll da9585d578f367cd6cd4b0e6821e67ff02eab731ae78593ab69674f649514872 • libcurl.dll 2ee3a202233625cdcdec9f687d74271ac0f9cb5877c96cf08cf1ae88087bec2e • libcurl.dll 19fb41244558f3a7d469b79b9d91cd7d321b6c82d1660738256ecf39fe3c8421 • libcurl.dll 211cea7a5fe12205fee4e72837279409ace663567c5b8c36828a3818aabef456 • libcurl.dll 0f41536cd9982a5c1d6993fac8cd5eb4e7f8304627f2019a17e1aa283ac3f47c

MITRE ATT&CK :

- T1059 – Command and Scripting Interpreter (es. PowerShell)
- T1053.005 – Scheduled Task/Job: Scheduled Task (attività pianificate)
- T1055 – Process Injection (es. shellcode tramite COM/DCOM)
- T1218 – Signed Binary Proxy Execution (uso di binari legittimi come regsvr32, rundll32)
- T1082 – System Information Discovery
- T1016 – System Network Configuration Discovery
- T1204 – Execution via User Interaction (es. phishing su Microsoft Teams)

Rilevazione e mitigazione:

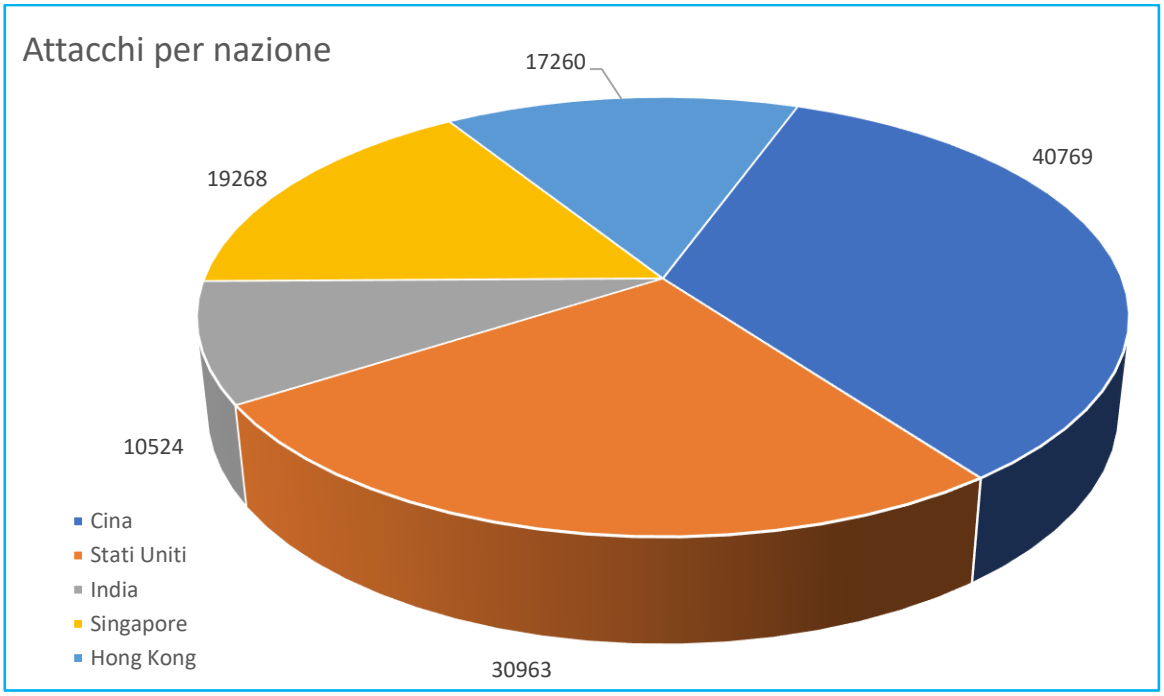
- Applicare policy di sicurezza su Microsoft Teams
- Abilitare autenticazione MFA
- Formare i dipendenti a non avviare tool come Quick Assist su richiesta di sconosciuti
- Utilizzare soluzioni EDR/AV con monitoraggio dei processi e degli script
- Bloccare l'esecuzione di aggiornamenti non ufficiali (es. Notepad++)
- Filtrare domini sospetti (es. fixuplink.com, emorista.org)
- Monitorare task pianificati sospetti (es. EventLogBackupTask)

Riepilogo generale

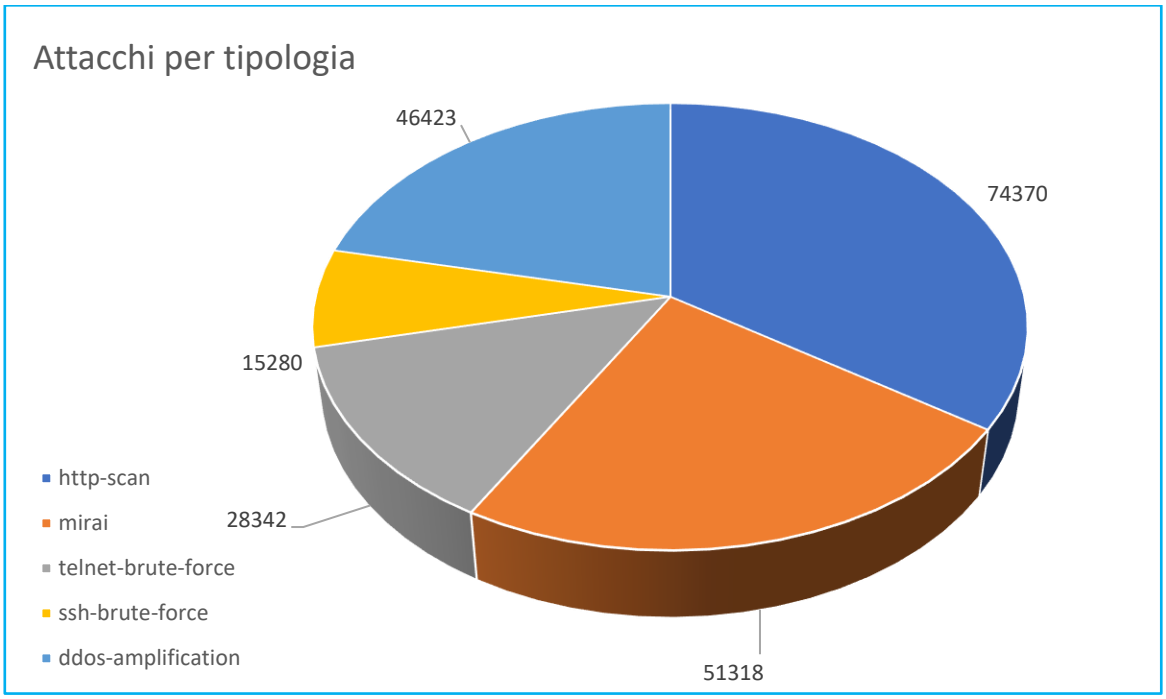
Malware	Categoria	Livello di rischio
LameHug (APT28)	Malware AI-powered (target mirati)	Critico
Diskstation	Ransomware (NAS Synology)	Alto
Konfety	Trojan Android (infostealer)	Alto
Matanbuchus 3.0	Loader malware (Windows)	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 14 – 20 Luglio, suddivisa per nazione e limitata alle prime cinque posizioni:

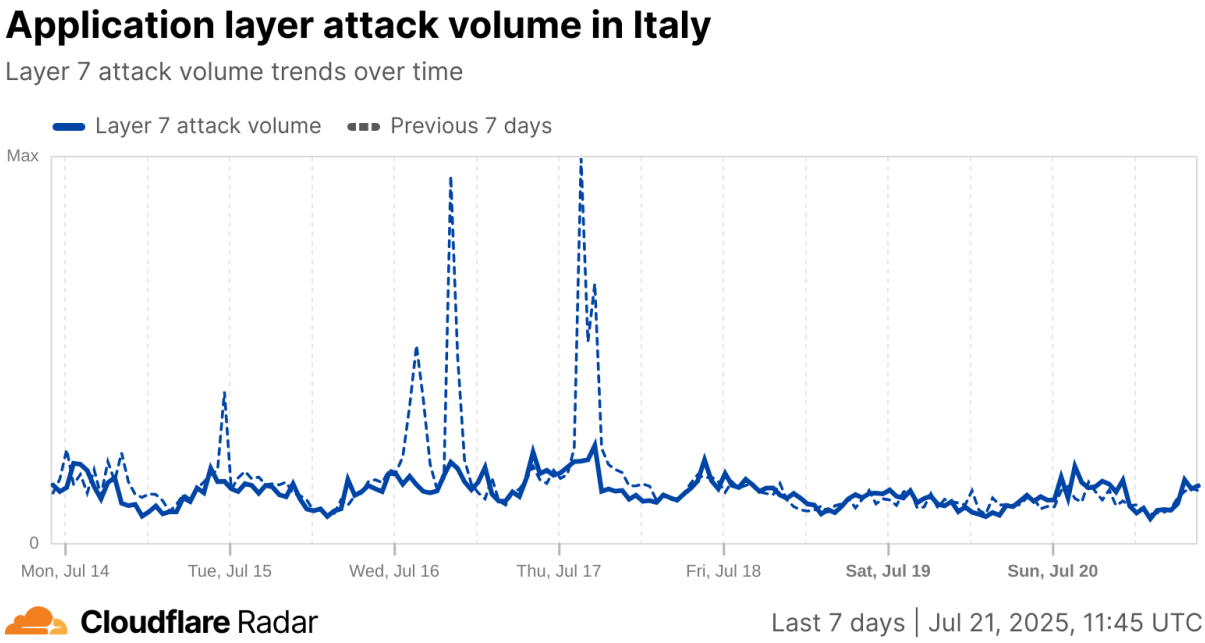


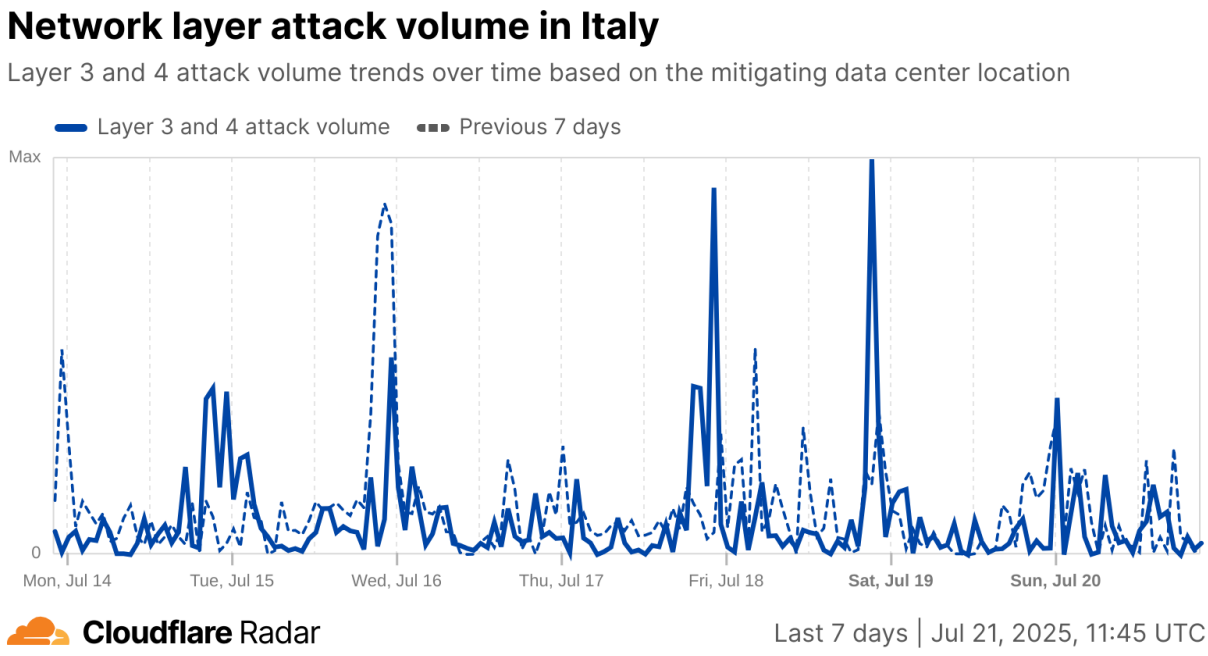
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



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
FLUTTER ENTERTAINMENT	REGNO UNITO e IRLANDA
DESCRIZIONE	Flutter Entertainment ha confermato una violazione di dati che ha coinvolto fino a 800.000 utenti dei servizi Paddy Power e Betfair in Regno Unito e Irlanda. La fuga ha riguardato informazioni personali come username, indirizzi email, IP, ID dispositivo e attività recenti sugli account, ed in alcuni casi isolati anche di indirizzi parziali. Non sono state compromesse password, documenti d'identità o dati di pagamento. Flutter ha immediatamente contenuto l'incidente, avviato un'indagine interna e informato le autorità inglesi e irlandesi. Flutter ha rassicurato i clienti che non è necessaria alcuna azione da parte degli utenti, invitandoli però a restare vigili nelle comunicazioni sospette.

TARGET	LOCALIZZAZIONE
MEDIA BROADCAST SATELLITE GMBH	GERMANIA
DESCRIZIONE	Media Broadcast Satellite GmbH, operatore tedesco di servizi di comunicazione via satellite, è stata vittima di un data breach rilevato il 17 luglio 2025 e attribuito al gruppo hacker Qilin. Durante l'attacco sono stati sottratti circa 870 GB di dati, anche se non sono stati ancora resi noti i dettagli specifici sulle informazioni compromesse. Vista la natura sensibile dei suoi servizi, l'incidente potrebbe avere implicazioni rilevanti. L'azienda sta attualmente gestendo la situazione e invita clienti e partner a restare aggiornati tramite i canali ufficiali.

TARGET	LOCALIZZAZIONE
MORRISON COMPANIES	STATI UNITI
DESCRIZIONE	Il 17 luglio 2025, Morrison Companies, gruppo statunitense attivo in sviluppo immobiliare e servizi, è stato vittima di un data breach attribuito al gruppo hacker Play. Sebbene non siano ancora stati resi noti i dettagli specifici sui dati compromessi, si teme che possano riguardare informazioni sensibili legate a transazioni finanziarie, proprietà e dati dei dipendenti. Play è noto per attacchi ransomware mirati a grandi aziende e per aver pubblicato dati sottratti sul dark web. Morrison Companies non ha ancora rilasciato dichiarazioni ufficiali.

4.6 Defacement

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

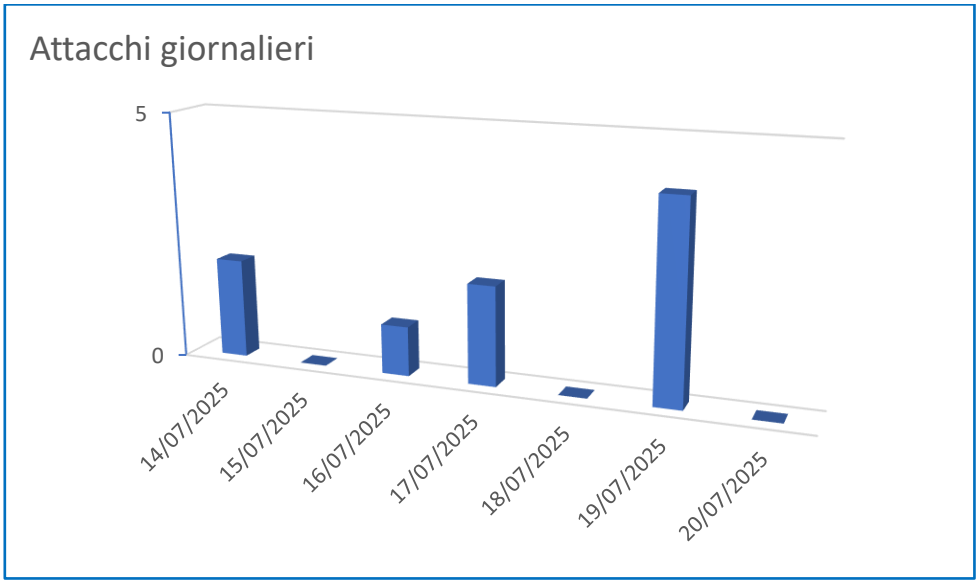


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

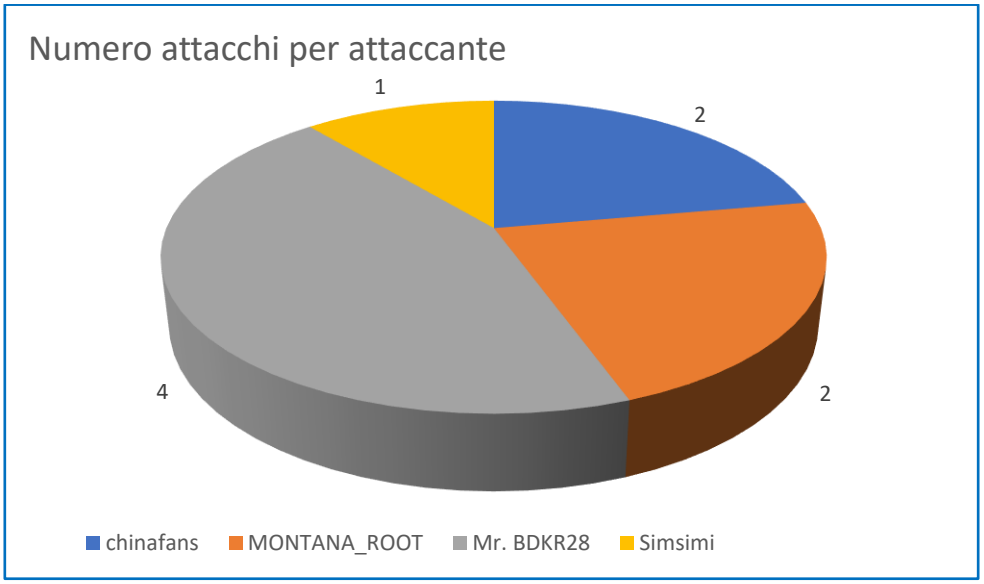


Figura 2: Defacement - Attaccanti più attivi nel periodo 14 - 20 Luglio

5 Honeypot

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

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale

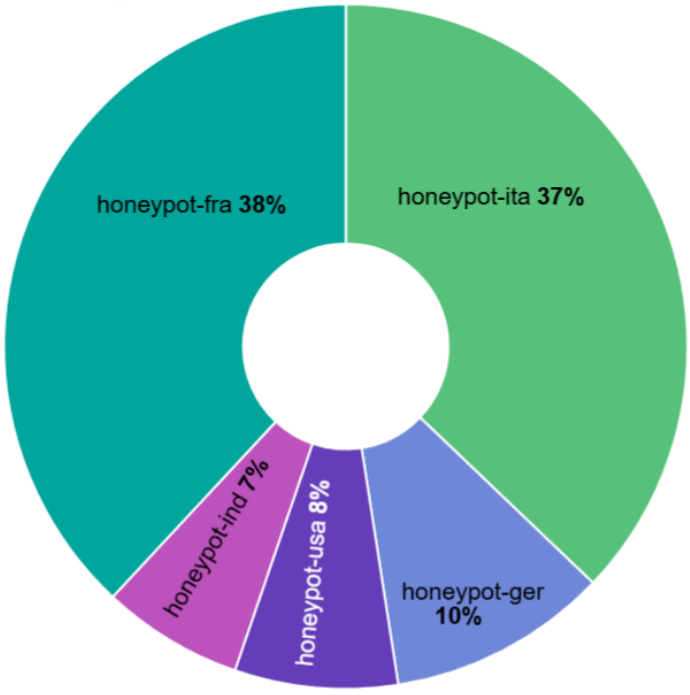
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

519.642 Attacks

5.874 Unique Src IPs

52 Unique HASSHs

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



Questa invece la situazione a livello italiano:

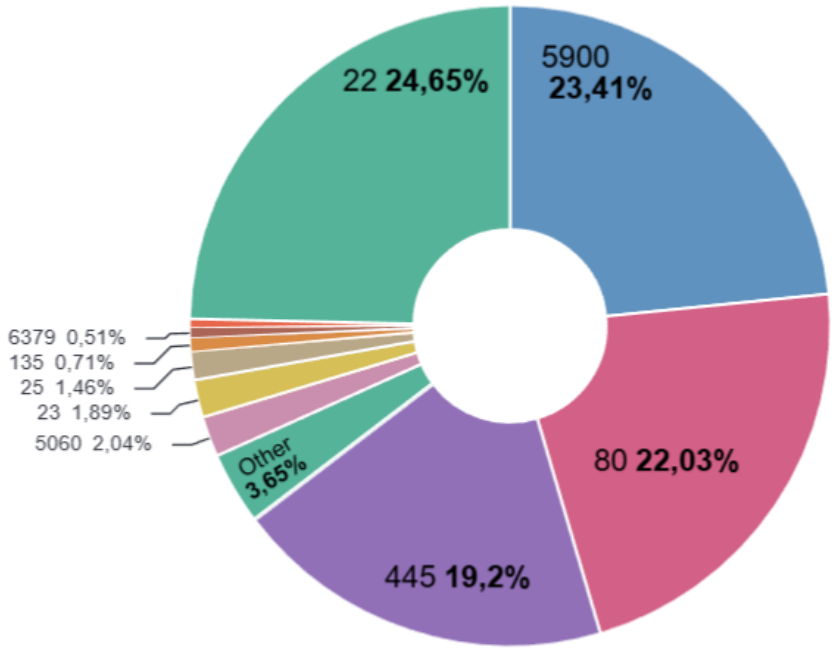
192.944 Attacks

2.876 Unique Src IPs

41 Unique HASSHs

5.1.1 Attacchi ai servizi

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



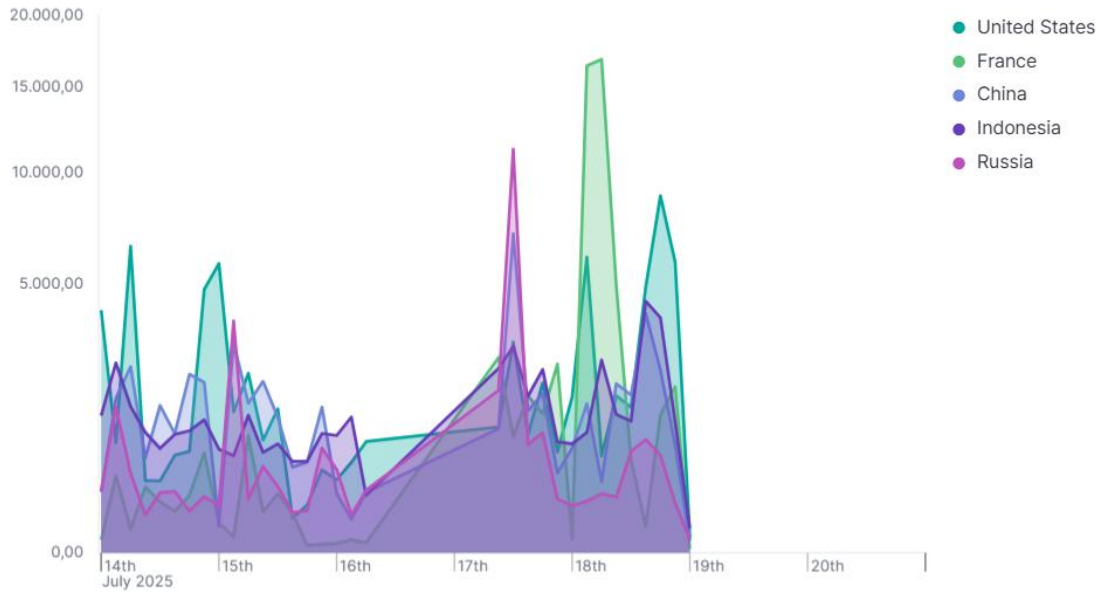
5.1.2 IP Attaccanti

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
185.177.72.111	37.454
103.156.74.23	21.406
142.202.189.5	15.943
142.202.191.234	12.583
79.124.56.162	11.893
80.255.136.209	11.058
45.144.29.201	10.991
212.34.230.50	5.421
193.37.69.157	3.516
185.177.72.205	3.402

5.1.3 Paesi di provenienza degli attacchi

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



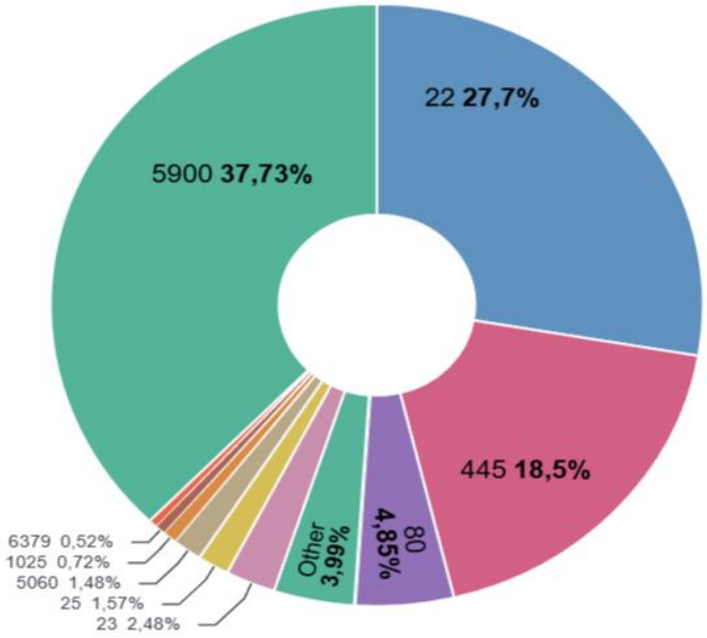
In quest'altro grafico viene rappresentata la distribuzione degli attacchi per paese di provenienza:

5.2 Italian Honeypot N.1

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

5.2.1 Attacchi ai servizi

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



Service Port	Count
5900	28.080
22	20.613
445	13.774
80	3.608
23	1.844
25	1.169
5060	1.104
1025	538
6379	390
443	336

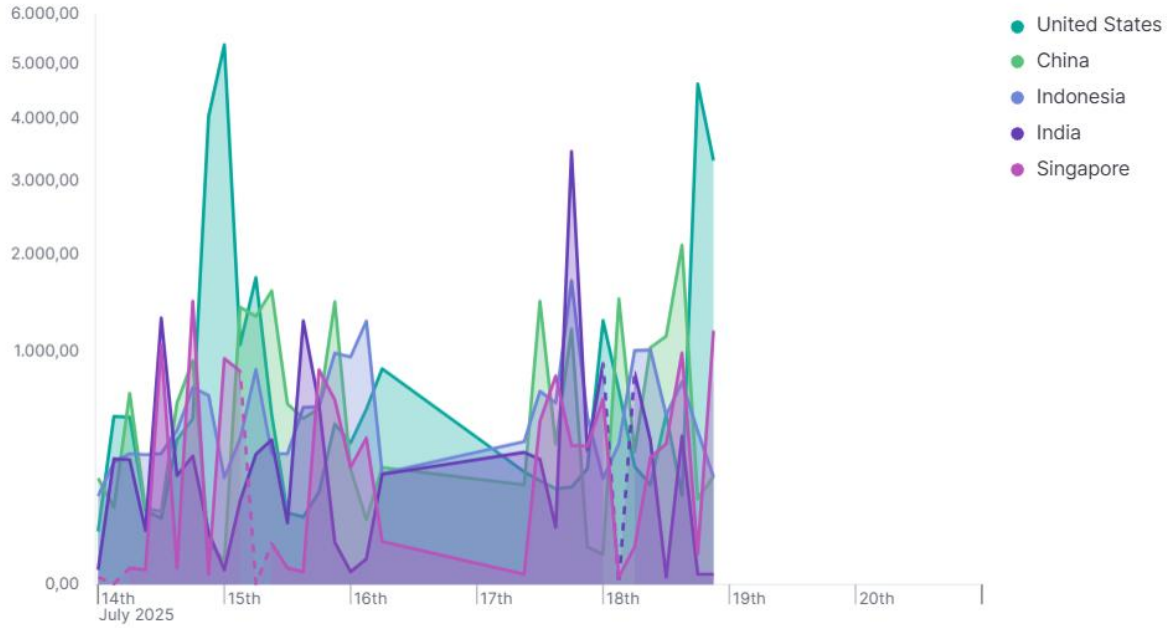
5.2.2 IP Attaccanti

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

Source IP	Count
103.156.74.23	8.949
142.202.189.5	8.710
142.202.191.234	7.396
79.124.56.162	6.891
212.34.230.50	5.421
193.37.69.157	3.516
223.139.63.226	3.157
117.192.45.225	3.150
45.78.192.81	1.618
31.56.204.247	1.555

5.2.3 Paesi di provenienza degli attacchi

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

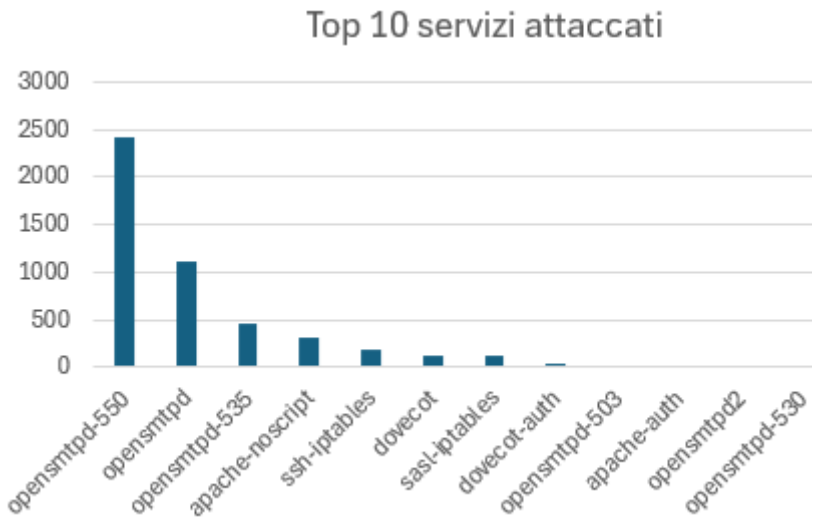


5.3 Italian Honeypot N.2

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.



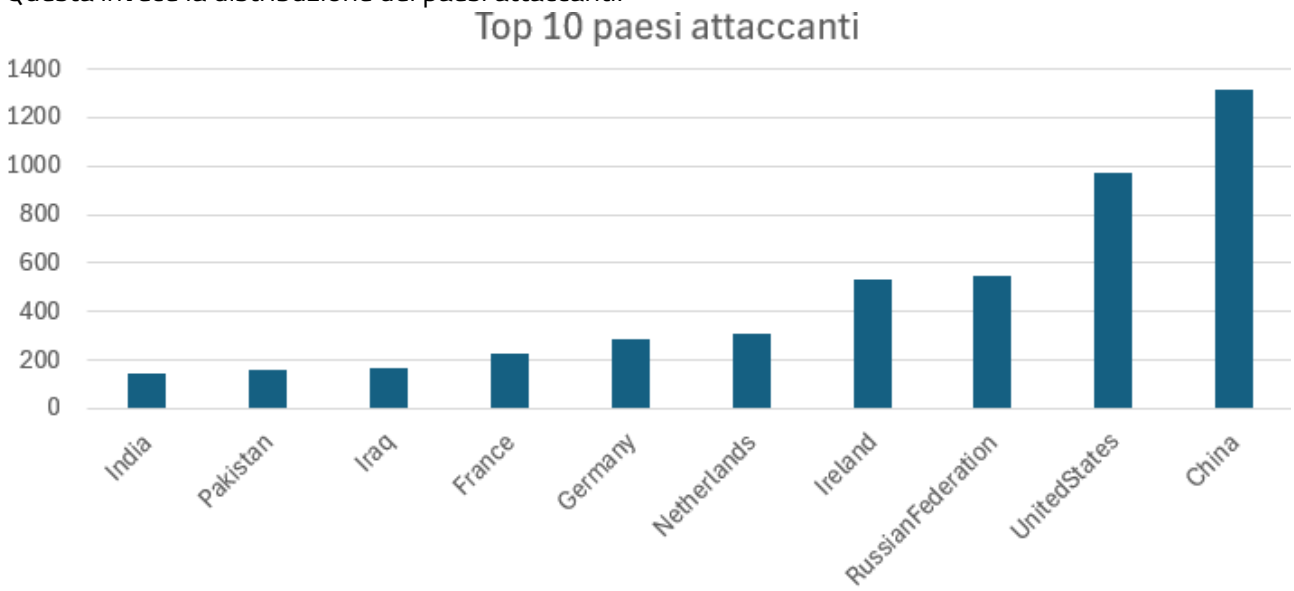
5.3.2 IP attaccanti

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
147[.]45[.]178[.]119	190
62[.]173[.]141[.]189	167
62[.]173[.]141[.]205	140
85[.]17[.]15[.]158	124
213[.]108[.]199[.]159	79
121[.]226[.]33[.]241	38
119[.]154[.]193[.]61	37
143[.]244[.]145[.]241	23
41[.]139[.]216[.]5	23
190[.]80[.]193[.]48	23

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