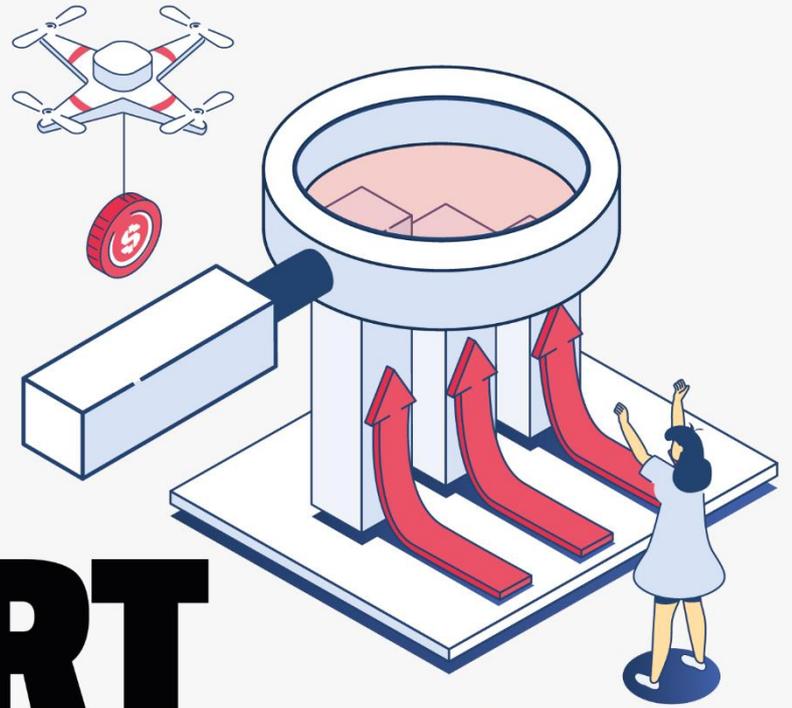




Cyber security

# RISK REPORT

\ week 09.06.2025 - 15.06.2025





# Sommario

1	Il Cyber Security Risk Report S3K.....	5
	Contenuti di questo numero del Bollettino.....	5
1.1	Security News .....	5
1.2	Vulnerabilità critiche.....	6
1.3	CVE Monitor.....	6
1.4	Attacchi .....	6
1.5	Honeypot.....	7
1.6	Raccomandazioni prioritarie .....	7
2	Security news.....	9
2.1	Rilasci aggiornamenti e patch .....	9
2.2	"Cyber News" dal Web, Deep Web e Dark Web.....	12
3	CVE Monitor.....	16
3.1	Sintesi Settimanale CVE.....	16
3.2	Tendenze .....	19
3.3	Nuove CVE.....	20
3.4	CVE attualmente utilizzate in attacchi .....	22
4	Attacchi .....	23
4.1	Phishing .....	23
4.2	Ransomware .....	28
4.3	Malware.....	30
4.4	DDoS rilevati.....	37
4.5	Data Breach .....	39
4.6	Defacement .....	41
5	Honeypot.....	42
5.1	Attacchi Settimanali Honeypot S3K – Analisi generale .....	42
5.1.1	Attacchi ai servizi.....	43
5.1.2	IP Attaccanti.....	44
5.1.3	Paesi di provenienza degli attacchi .....	44
5.2	Italian Honeypot N.1 .....	46
5.2.1	Attacchi ai servizi.....	46
5.2.2	IP Attaccanti.....	46



5.2.3 Paesi di provenienza degli attacchi .....	47
5.3 Italian Honeypot N.2 .....	47
5.3.1 Attacchi ai servizi .....	47
5.3.2 IP attaccanti.....	48
5.3.3 Paesi di provenienza degli attacchi.....	48
6 Company Profile S3K .....	49



**CYBER SECURITY RISK REPORT**

**24/25**



# 1 Il Cyber Security Risk Report S3K

Il "Cyber Security Risk Report" è il risultato di uno specifico servizio erogato da S3K. Contiene un riepilogo settimanale delle notizie e degli avvenimenti dal mondo "cyber" e delle tendenze emergenti fornendo all'organizzazione le informazioni necessarie per stare al passo con il panorama in evoluzione delle minacce informatiche.

Per la sua elaborazione, gli analisti di S3K raccolgono ed esaminano dati provenienti da un alto numero di fonti, quali, ad esempio, produttori di hardware e software, ricercatori su tematiche di sicurezza, forum dedicati, canali di comunicazione dei gruppi di cyber criminali, black market, deep web, dark Web.

Alcune delle informazioni che vengono inserite nel bollettino sono:

- trend delle menzioni su social delle CVE
- nuove vulnerabilità, CVE, Oday pubblicati
- informazioni su nuovi attacchi e data breach
- campagne phishing
- attività dei gruppi di cyber criminali
- malware on the wild
- IP riportati come malevoli
- IoC
- pubblicazione di patch, aggiornamenti e workaround
- valutazione della situazione generale e possibili evoluzioni dello scenario cyber

## Contenuti di questo numero del Bollettino

Il Cyber Security Risk Report S3K per la settimana 9-16 giugno 2025 ha evidenziato diverse minacce e tendenze significative che richiedono l'attenzione immediata dei professionisti della sicurezza informatica. Ecco una sintesi delle principali evidenze emerse dall'analisi.

### 1.1 Security News

Questa sezione fornisce aggiornamenti sui rilasci di patch e correzioni di sicurezza da parte dei principali vendor, oltre a notizie rilevanti dal mondo cyber, deep web e dark web. Nel bollettino attuale, vengono riportati aggiornamenti cruciali da Microsoft, Tenable e Palo Alto Networks, insieme a notizie su attacchi significativi come quelli contro Microsoft Entra ID e sui rischi legati alle VPN gratuite. Questa settimana Microsoft ha rilasciato aggiornamenti critici che risolvono 68 vulnerabilità, tra cui 2 di tipo zero-day.



Sono stati inoltre segnalati aggiornamenti importanti per Nessus e PAN-OS. Tra le notizie principali, una campagna di attacchi che ha colpito oltre 80.000 account Microsoft Entra ID, l'operazione coordinata tra FBI e forze europee che ha portato alla chiusura di domini utilizzati per supportare ransomware, e un report di Trend Micro sull'aumento del rischio cyber per le imprese italiane a causa di asset sconosciuti e IoT non gestiti.

## 1.2 Vulnerabilità critiche

La settimana è stata caratterizzata da un'alta intensità di vulnerabilità critiche, con particolare impatto su prodotti Microsoft Windows, Adobe, SAP, Dell, IBM, SolarWinds e plugin WordPress. Diverse CVE presentano potenziale di esecuzione di codice remoto (RCE), escalation di privilegi e denial of service, alcune già dotate di Proof of Concept noti.

Tra le più gravi troviamo la CVE-2025-32711 che interessa Microsoft M365 Copilot e che consente l'iniezione di comandi AI con possibile divulgazione di informazioni, e diverse vulnerabilità nei sistemi Windows RRAS che permettono l'esecuzione di codice remoto attraverso heap overflow.

## 1.3 CVE Monitor

Il bollettino include un'analisi dettagliata delle vulnerabilità più rilevanti della settimana, con particolare attenzione alle CVE (Common Vulnerabilities and Exposures) di tendenza sui social media, alle nuove vulnerabilità identificate e a quelle attivamente sfruttate dagli attaccanti con raccomandazioni specifiche per la prioritizzazione delle patch.

La settimana 9-15 giugno 2025 ha visto numerose vulnerabilità ad alto impatto che interessano Microsoft Windows, Adobe, SAP, Dell, IBM, SolarWinds e plugin WordPress. Particolarmente critiche le CVE-2025-32711 (Microsoft M365 Copilot), CVE-2025-33064 e CVE-2025-33066 (Windows RRAS), che potrebbero consentire l'esecuzione di codice remoto. Tra le vulnerabilità attivamente sfruttate troviamo CVE-2025-32433 (Erlang/OTP), CVE-2025-24016 (Wazuh) e CVE-2025-33053 (WebDAV).

## 1.4 Attacchi

Il bollettino dedica un'ampia sezione all'analisi degli attacchi informatici, suddivisi per tipologia: phishing, ransomware, malware, DDoS, data breach e defacement. Per ciascuna categoria vengono forniti dati statistici, trend e casi di studio specifici, con particolare attenzione alla situazione italiana e al contesto internazionale.

Gli attacchi DDoS mostrano una concentrazione particolare verso Stati Uniti, Germania, Francia, Gran Bretagna e Paesi Bassi, con tecniche principalmente rivolte ai servizi UDP, SYN e TCP. L'analisi delle



campagne di phishing ha evidenziato un aumento degli attacchi che impersonano persone reali, utilizzando dati aziendali autentici per aumentare la credibilità. Nel settore ransomware, i gruppi più attivi questa settimana sono stati BlackCat/ALPHV, Qilin e 8Base. Tra i malware più diffusi spiccano MassJacker (cryptojacker), Sosano (backdoor poliglotta), Gremlin Stealer (infostealer), StilachiRAT e Interlock (ransomware). Sono stati inoltre rilevati data breach significativi che hanno colpito Zoomcar Holdings (India), WestJet (Canada) e il Dipartimento della Cultura e del Turismo di Abu Dhabi.

## 1.5 Honeypot

Un'analisi dei dati raccolti attraverso una rete di sensori honeypot distribuiti globalmente (Italia, Germania, Francia, Brasile, India e USA). Questi sistemi, appositamente predisposti per attirare e registrare attività malevole, forniscono informazioni preziose sugli attacchi in corso, sui servizi più colpiti, sugli IP attaccanti e sui paesi di provenienza degli attacchi.

Ogni sezione è arricchita da grafici, tabelle e visualizzazioni che facilitano la comprensione dei dati e delle tendenze. Le informazioni sono presentate in modo chiaro e strutturato, consentendo ai professionisti della sicurezza di identificare rapidamente le minacce più rilevanti per la propria organizzazione e di implementare le appropriate misure di mitigazione.

I dati raccolti dall'infrastruttura di honeypot S3K mostrano una predominanza di attacchi provenienti da Cina, Stati Uniti e Russia. I servizi più colpiti sono stati SSH (porta 22), Telnet (porta 23) e SMB (porta 445). In Italia, gli honeypot hanno registrato un'intensificazione degli attacchi verso le porte HTTP (80) e RDP (3389), con una significativa porzione di attacchi provenienti da indirizzi IP localizzati in Cina, Regno Unito e Stati Uniti

## 1.6 Raccomandazioni prioritarie

- Applicare immediatamente le patch per i sistemi critici
- Monitoraggio continuo
- Verificare l'attività anomala sui sistemi esposti
- Protezione infrastrutturale
- Rafforzare sicurezza di endpoint, rete e applicazioni



- Sensibilizzazione
- Formare il personale sulle minacce attuali

Il Cyber Security Risk Report S3K rappresenta uno strumento indispensabile per i professionisti della sicurezza informatica e i responsabili IT che necessitano di informazioni aggiornate e affidabili per proteggere le proprie organizzazioni. La combinazione di dati analitici, tendenze emergenti e raccomandazioni pratiche fornisce un quadro completo del panorama delle minacce informatiche, consentendo decisioni informate e interventi tempestivi. L'approccio multidisciplinare di S3K, unito alla sua vasta esperienza nel campo della sicurezza, garantisce l'alta qualità e l'affidabilità delle informazioni fornite in questo bollettino settimanale.



## 2 Security news

### 2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Microsoft	<p>Microsoft ha rilasciato gli aggiornamenti di sicurezza mensili che risolvono un totale di 68 nuove vulnerabilità, 2 di tipo 0-day.</p> <p>Versioni affette:</p> <ul style="list-style-type: none"><li>• .NET and Visual Studio</li><li>• App Control for Business (WDAC)</li><li>• Microsoft 365 Copilot</li><li>• Microsoft AutoUpdate (MAU)</li><li>• Microsoft Local Security Authority Server (Isasrv)</li><li>• Microsoft Office</li><li>• Microsoft Office Excel</li><li>• Microsoft Office Outlook</li><li>• Microsoft Office PowerPoint</li><li>• Microsoft Office SharePoint</li><li>• Microsoft Office Word</li><li>• Nuance Digital Engagement Platform</li><li>• Power Automate</li><li>• Remote Desktop Client</li><li>• Visual Studio</li><li>• WebDAV</li><li>• Windows Common Log File System Driver</li><li>• Windows Cryptographic Services</li><li>• Windows DHCP Server</li><li>• Windows DWM Core Library</li><li>• Windows Hello</li><li>• Windows Installer</li><li>• Windows KDC Proxy Service (KPSSVC)</li><li>• Windows Kernel</li><li>• Windows Local Security Authority (LSA)</li><li>• Windows Local Security Authority Subsystem Service (LSASS)</li><li>• Windows Media</li><li>• Windows Netlogon</li></ul>



	<ul style="list-style-type: none"><li>• Windows Recovery Driver</li><li>• Windows Remote Access Connection Manager</li><li>• Windows Remote Desktop Services</li><li>• Windows Routing and Remote Access Service (RRAS)</li><li>• Windows SDK</li><li>• Windows Security App</li><li>• Windows Shell</li><li>• Windows SMB</li><li>• Windows Standards-Based Storage Management Service</li><li>• Windows Storage Management Provider</li><li>• Windows Storage Port Driver</li><li>• Windows Win32K - GRFX</li></ul>
<b>ULR/Note</b>	<p><a href="https://msrc.microsoft.com/update-guide/releaseNote/2025-Jun">https://msrc.microsoft.com/update-guide/releaseNote/2025-Jun</a></p> <p><a href="https://msrc.microsoft.com/update-guide">https://msrc.microsoft.com/update-guide</a></p> <p><a href="https://blog.redteam-pentesting.de/2025/reflective-kerberos-relay-attack/">https://blog.redteam-pentesting.de/2025/reflective-kerberos-relay-attack/</a></p>

<b>PRODOTTO</b>	<b>DESCRIZIONE</b>
Nessus	<p>Tenable ha rilasciato aggiornamenti di sicurezza che risolvono 3 vulnerabilità con gravità "alta" nel noto vulnerability scanner <i>Nessus</i>.</p> <p>Versioni affette:</p> <ul style="list-style-type: none"><li>• Nessus Agent, versione 10.8.4 e precedenti per Windows</li></ul>
<b>ULR/Note</b>	<p><a href="https://www.tenable.com/security/tns-2025-11">https://www.tenable.com/security/tns-2025-11</a></p>

<b>PRODOTTO</b>	<b>DESCRIZIONE</b>
PAN-OS, GlobalProtect	<p>Aggiornamenti di sicurezza sanano alcune vulnerabilità, di cui 2 con gravità "alta" in PAN-OS e GlobalProtect. Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato di elevare i propri privilegi o di eseguire codice arbitrario sui sistemi target.</p> <p>Versioni affette:</p> <ul style="list-style-type: none"><li>• PAN-OS 11.0.x, versioni precedenti alla 11.0.3</li><li>• PAN-OS 10.2.x, versioni precedenti alla 10.2.8</li><li>• PAN-OS 10.1.x, tutte le versioni</li><li>• GlobalProtect App 6.3.x, versioni precedenti alla 6.3.3 per macOS</li><li>• GlobalProtect App 6.2.x, versioni precedenti alla 6.2.8-h2 per macOS</li><li>• GlobalProtect App 6.1.x, tutte le versioni per macOS</li></ul>



	<ul style="list-style-type: none"><li>• GlobalProtect App 6.0.x, tutte le versioni per macOS</li></ul>
<b>ULR/Note</b>	<a href="https://security.paloaltonetworks.com/CVE-2025-4232">https://security.paloaltonetworks.com/CVE-2025-4232</a> <a href="https://security.paloaltonetworks.com/CVE-2025-4231">https://security.paloaltonetworks.com/CVE-2025-4231</a>



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

### **ATTACCHI SU LARGA SCALA A MICROSOFT ENTRA ID: SCOPERTA UNA CAMPAGNA GLOBALE CON OLTRE 80.000 ACCOUNT NEL MIRINO**

È di recente scoperta ed analisi un'ondata di attacchi informatici che ha preso di mira oltre 80.000 account Microsoft Entra ID appartenenti a centinaia di organizzazioni a livello globale, sfruttando il framework di penetration testing TeamFiltration. Secondo quanto riportato da alcuni ricercatori di sicurezza, la campagna, iniziata a dicembre 2024, è stata attribuita ad un gruppo di cybercriminali identificato come UNK\_SneakyStrike. Il picco dell'attività è stato registrato l'8 gennaio 2025, quando ben 16.500 account sono stati presi di mira in un solo giorno. Nei mesi successivi dopo queste fasi intense, si sono osservati brevi periodi di pausa, caratterizzati da un'assenza quasi totale di attività. TeamFiltration, rilasciato nel 2022 dal ricercatore red team di TrustedSec, Melvin Langvik, è un framework multiplatforma progettato per svolgere operazioni come enumerazione di account, password spraying, esfiltrazione di dati e inserimento di backdoor nei sistemi O365/Entra ID. Durante la campagna condotta da UNK\_SneakyStrike, il framework ha svolto un ruolo cruciale nei tentativi di accesso non autorizzato su

larga scala. Secondo Proofpoint, l'attore della minaccia tende ad attaccare tutti gli utenti in tenant di piccole dimensioni, mentre nei tenant più grandi seleziona solo un sottoinsieme di utenti da colpire. "A partire da dicembre 2024, l'attività di UNK\_SneakyStrike ha coinvolto oltre 80.000 account in centinaia di organizzazioni, causando diversi casi di compromissione," si legge nel report di Proofpoint. I ricercatori sono riusciti a collegare gli attacchi a TeamFiltration grazie all'individuazione di un user-agent insolito, proprio dello strumento, e alla corrispondenza di client ID OAuth codificati presenti nel suo codice. Ulteriori indizi che hanno confermato il legame includono pattern di accesso a servizi incompatibili e il rilevamento, all'interno di TeamFiltration, di una vecchia versione del progetto FOCI di Secureworks. Gli attacchi sono stati condotti tramite server AWS dislocati in diverse regioni, utilizzando un account Office 365 con licenza Business Basic, sfruttato per l'enumerazione degli account attraverso l'API di Microsoft Teams. Le fonti IP principali degli attacchi provengono da Stati Uniti (42%), Irlanda (11%), Regno Unito (8%).



## FBI E FORZE EUROPEE CHIUDONO QUATTRO DOMINI USATI PER SUPPORTARE RANSOMWARE

Un'azione coordinata tra Stati Uniti, Paesi Bassi, Finlandia ed altri Stati europei ha portato alla chiusura di quattro siti web e alla confisca di server utilizzati per offrire servizi di offuscamento e strumenti pensati per aggirare i software antivirus. Tali risorse erano fondamentali per consentire ai gruppi ransomware di diffondere codice malevolo eludendo i sistemi di difesa informatici. Le autorità inquirenti hanno rivelato che queste piattaforme erano direttamente collegate a gruppi ransomware operanti sia sul territorio statunitense che all'estero. Le operazioni investigative, condotte dalla sede FBI di Houston con il supporto dell'iniziativa internazionale Operation Endgame, hanno inferto un colpo significativo all'infrastruttura tecnologica che alimenta le attività di molti cybercriminali. L'uso del crypting, tecnica che consente di mascherare software dannoso attraverso algoritmi di offuscamento, è da tempo considerato uno degli strumenti più insidiosi nelle mani degli attori malevoli. I domini sequestrati offrivano vere e proprie *suite* di servizi Counter-Antivirus (CAV), utilizzate per verificare e ottimizzare i malware prima della loro distribuzione. Durante l'inchiesta, le forze dell'ordine hanno effettuato operazioni sotto copertura acquistando direttamente dai portali in

questione. Tali transazioni hanno confermato che i servizi erano espressamente progettati per finalità illecite. Le analisi condotte durante l'operazione hanno inoltre messo in luce legami concreti con noti gruppi ransomware responsabili di attacchi su scala globale, inclusi episodi che hanno interessato l'area di Houston. "Contro una criminalità informatica sempre più sofisticata, servono risposte altrettanto avanzate", ha dichiarato il Procuratore Nicholas J. Ganjei. "Non basta colpire i singoli operatori: è fondamentale disarticolare tutta la rete che li sostiene." L'intervento giunge in un contesto in cui gli attacchi ransomware sono in costante crescita. I servizi di crypting rappresentano un passaggio cruciale nell'intera catena operativa di questi gruppi, permettendo loro di sfuggire ai meccanismi di rilevamento delle aziende, rimanere nascosti all'interno delle reti compromesse, massimizzare i danni prima che l'attacco venga scoperto, ostacolare le indagini post-attacco. "Oggi i criminali informatici non si limitano a scrivere codice malevolo: lo rendono più efficace, più furtivo e più devastante," ha aggiunto Douglas Williams, agente speciale dell'FBI di Houston. "Con l'aiuto di servizi CAV, riescono a perfezionare le loro minacce per sfidare anche i sistemi di sicurezza più evoluti al mondo."



## ASSET SCONOSCIUTI E IOT FUORI CONTROLLO: CRESCE IL RISCHIO CYBER PER LE IMPRESE ITALIANE

Secondo quanto emerge dal report “AI is accelerating Cyber Risk Exposure” pubblicato da Trend Micro, leader globale nella sicurezza informatica, oltre la metà delle aziende italiane ha subito almeno un incidente cyber riconducibile ad asset sconosciuti o gestiti in modo inadeguato. Con la rapida diffusione dell’intelligenza artificiale generativa, molte organizzazioni si trovano oggi a fronteggiare un aumento incontrollato di dispositivi e risorse non monitorati, come gli IoT impiegati sia negli uffici che nelle abitazioni dei dipendenti in smart working. Questa evoluzione ha ampliato e complicato la cosiddetta superficie d’attacco, rendendo ancora più difficile il controllo del perimetro digitale. Nonostante una crescente consapevolezza del rischio, molte imprese italiane non hanno ancora adottato misure e strumenti adeguati per una gestione preventiva e strutturata dell’esposizione agli attacchi informatici. Lo confermano i dati della ricerca: l’87% dei professionisti intervistati riconosce un legame diretto tra la gestione della superficie d’attacco e il rischio d’impresa, sottolineando che una mancata supervisione può generare conseguenze pesanti. Tra gli ambiti più colpiti in caso di incidente, le aziende indicano: continuità operativa (34%), capacità competitiva sul mercato (34%), produttività del personale (32%), fiducia dei clienti e reputazione del brand (29%), rapporti con partner e fornitori (25%), stabilità finanziaria (21%).

Tuttavia, solo il 40% delle organizzazioni italiane dichiara di aver adottato strumenti pensati per una gestione proattiva e continuativa della superficie esposta. Un ulteriore 29% agisce solo a posteriori, ossia dopo che l’incidente è già avvenuto, aumentando così il rischio di danni estesi e imprevedibili. Anche sul fronte degli investimenti la situazione risulta problematica: in media, solo un quarto del budget cybersecurity viene destinato alla gestione del rischio connesso alla superficie d’attacco. Nonostante ciò, ben il 75% dei responsabili IT italiani afferma di ritenere adeguate le risorse attualmente a disposizione, segno di una percezione non sempre allineata alla realtà dei rischi. “Già nel 2022 molte aziende temevano di aver perso il controllo della propria superficie d’attacco. Oggi questa minaccia è diventata ancora più pressante. Sebbene sia aumentata la consapevolezza dei rischi per il business, sono ancora poche le realtà che scelgono un approccio realmente proattivo. È fondamentale che la gestione dell’esposizione ai rischi informatici diventi una priorità strategica per ogni organizzazione”, ha dichiarato Salvatore Marcis, Country Manager di Trend Micro Italia. Lo studio è stato commissionato da Trend Micro e realizzato da Sapio Research, con la partecipazione di 2.250 professionisti IT e cybersecurity provenienti da aziende di vari settori e dimensioni, distribuite in 21 paesi tra Europa, Nord America e Asia-Pacifico. Il campione italiano ha incluso 100 partecipanti.



## LA TRAPPOLA DELLE VPN GRATUITE E LA SICUREZZA SVENDUTA ALLA CINA

Almeno 17 applicazioni VPN gratuite con possibili collegamenti ad entità cinesi restano disponibili negli store digitali statunitensi di Apple e Google, nonostante gli avvertimenti lanciati da esperti di sicurezza. Già ad aprile 2025, TTP aveva pubblicato un primo report segnalando che i dati di milioni di utenti potevano essere trasferiti in Cina all'insaputa degli interessati. Alcune app coinvolte risultano associate a Qihoo 360, società precedentemente sanzionata dagli Stati Uniti per sospetti legami con le forze armate cinesi.

Nel nuovo aggiornamento pubblicato sei settimane dopo, i ricercatori hanno confermato che la maggior parte di queste VPN è ancora accessibile negli store americani, con la possibilità che Apple e Google continuino a trarne profitto tramite acquisti in-app e contenuti pubblicitari. Tra i nomi evidenziati figurano Turbo VPN, VPN Proxy Master, Thunder VPN, Snap VPN e Signal Secure VPN. Altre app, come X-VPN e VPNIFY, fanno parte di un elenco esteso di servizi che potrebbero agire come veicoli per la raccolta e l'esportazione di dati sensibili. I

ricercatori sottolineano che queste applicazioni spesso mascherano la loro vera origine, adottando strategie di brandizzazione che oscurano i reali sviluppatori o registrando le società in Paesi terzi. Alcune di esse presentano persino messaggi rassicuranti sulla sicurezza, pur non rispettando gli standard minimi di protezione dei dati. Apple ha dichiarato di applicare criteri rigorosi per lo sviluppo di app VPN, negando qualsiasi trasferimento illecito di informazioni verso terzi. Tuttavia, il luogo di provenienza dello sviluppatore non costituisce, di per sé, un motivo di esclusione dagli store. Google, al momento, non ha rilasciato dichiarazioni ufficiali. L'indagine ha anche rilevato che le stesse app sono scaricabili da altri store regionali, incluso quello britannico, indicando una diffusione del problema ben oltre i confini statunitensi. Gli esperti temono che milioni di utenti in tutto il mondo stiano inconsapevolmente condividendo informazioni con entità che potrebbero utilizzarle per finalità di sorveglianza o manipolazione.



## 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 9 - 5 Giugno 2025

Settimana ad altissima intensità, con molte vulnerabilità ad alto impatto su Microsoft Windows, Adobe, SAP, Dell, IBM, SolarWinds e plugin WordPress. Diverse CVE presentano potenziale di esecuzione di codice remoto (RCE), escalation di privilegi e denial of service, alcune già dotate di PoC noti (es. Wordfence).

#### CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Descrizione Sintetica
<a href="#">CVE-2025-32711</a>	CRITICAL	11/06/2025	✗	Microsoft M365 Copilot – AI command injection → information disclosure (network).
<a href="#">CVE-2025-33064</a>	HIGH	10/06/2025	✗	Windows RRAS – RCE da heap overflow remoto autenticato.
<a href="#">CVE-2025-33066</a>	HIGH	10/06/2025	✗	Windows RRAS – RCE da heap overflow remoto non autenticato.
<a href="#">CVE-2025-32710</a>	HIGH	10/06/2025	✗	Windows RDP – Use-after-free → RCE da remoto.
<a href="#">CVE-2025-32713</a>	HIGH	10/06/2025	✗	Windows CLFS – heap overflow → privilege escalation.



<a href="#">CVE-2025-30317</a>	HIGH	10/06/2025	✘	Adobe InDesign – heap overflow via file malevolo.
<a href="#">CVE-2025-30327</a>	HIGH	10/06/2025	✘	Adobe InCopy – integer overflow → RCE locale.
<a href="#">CVE-2025-25050</a>	HIGH	13/06/2025	✘	Dell ControlVault3 – OOB write → RCE via API locale.
<a href="#">CVE-2025-24922</a>	HIGH	13/06/2025	✘	Dell ControlVault3 – stack overflow → RCE.
<a href="#">CVE-2025-24311</a>	HIGH	13/06/2025	✘	Dell ControlVault3 – OOB read → leak memoria.
<a href="#">CVE-2025-26395</a>	HIGH	10/06/2025	✘	SolarWinds Observability – XSS autenticato.
<a href="#">CVE-2025-23192</a>	HIGH	10/06/2025	✘	SAP BI Workspace – XSS persistente da utente non autenticato.
<a href="#">CVE-2025-33050</a>	HIGH	10/06/2025	✘	Windows DHCP – DoS remoto (protezione fallita).
<a href="#">CVE-2025-32717</a>	HIGH	11/06/2025	✘	Microsoft Word – heap overflow → RCE locale.



<a href="#">CVE-2025-32721</a>	HIGH	10/06/2025	✗	Windows Recovery Driver – EoP via link traversal.
<a href="#">CVE-2025-3234</a>	HIGH	14/06/2025	✔ Wordfence	WP Plugin File Manager Pro – Upload file arbitrario → possibile RCE.
<a href="#">CVE-2025-3302</a>	HIGH	11/06/2025	✔ Wordfence	WP Plugin Xagio SEO – XSS persistente non autenticato via HTTP_REFERER.
<b>Nota:</b> 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:** Massiccio patch Tuesday su RDP, RRAS, CLFS, SMB, DHCP, LSASS, Word, Copilot, etc.
- **Adobe:** InDesign e InCopy vulnerabili a heap overflow con RCE da file malevoli.
- **Dell ControlVault3:** Diverse vulnerabilità critiche su firmware (OOB read/write, stack overflow).
- **SAP:** XSS persistente da remoto senza autenticazione su BI Workspace.
- **WordPress Plugin:** Nuove vulnerabilità gravi con PoC pubblici (File Manager, Xagio SEO).
- **SolarWinds:** XSS in ambienti self-hosted con impatto su admin autenticati.

### Distribuzione Giornaliera

- **10–11 giugno:** Disclosure massiccia Microsoft e SAP.
- **13–14 giugno:** Advisory Dell e WordPress Plugin (Wordfence).

### Raccomandazioni

- **Patch Prioritarie:**
  - Sistemi Microsoft (in particolare RDP, RRAS, Copilot, CLFS).
  - Adobe InDesign / InCopy: attenzione file ricevuti da terzi.
  - WordPress plugin vulnerabili (File Manager, Xagio SEO).
  - Infrastrutture Dell ControlVault3 (PC, server protetti da autenticazione hardware).



- **Monitoraggio:**
  - Exploit pubblici disponibili per plugin WordPress (verificare installazioni attive).
  - Attività anomala su Copilot, Word, RDP, e interfacce RRAS/LSASS.

### 3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
<a href="#">CVE-2025-33073</a>	Windows Server Message Block (SMB)	N/A
<a href="#">CVE-2025-4275</a>	BIOS/firmware UEFI di Insyde	N/A
<a href="#">CVE-2025-49113</a>	Roundcube Webmail	N/A
<a href="#">CVE-2025-24201</a>	WebKit, motore di rendering utilizzato da Safari	8.8
<a href="#">CVE-2025-21420</a>	Windows Disk Cleanup Tool (cleanmgr.exe)	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
<a href="#">CVE-2025-6169</a>	WIMP (Web Intergrated Management Platform)	N/A
<b>VULNERABILITÀ</b>	La vulnerabilità CVE-2025-6169 riguarda la piattaforma di gestione della co-costruzione di siti web WIMP sviluppata da HAMASTAR Technology. Questa vulnerabilità è di tipo SQL Injection, che consente a un attaccante remoto non autenticato di iniettare comandi SQL arbitrari. Ciò potrebbe permettere la lettura, modifica o cancellazione dei contenuti del database, compromettendo gravemente la sicurezza del sistema.	

CVE	PRODOTTI	SCORE CVSS NIST
<a href="#">CVE-2025-32711</a>	Microsoft 365 Copilot	N/A
<b>VULNERABILITÀ</b>	La vulnerabilità CVE-2025-32711 riguarda Microsoft 365 Copilot, l'assistente basato su intelligenza artificiale integrato in applicazioni come Word, Excel, Outlook e Teams. Questa vulnerabilità consente a un attaccante non autenticato di sfruttare un'iniezione di comandi AI, potenzialmente esponendo informazioni sensibili attraverso la rete.	

CVE	PRODOTTI	SCORE CVSS NIST
<a href="#">CVE-2025-6098</a>	UTT 进取 750W (dispositivo di rete)	N/A
<b>VULNERABILITÀ</b>	È stata scoperta una vulnerabilità critica nel dispositivo UTT 进取 750W fino alla versione 5.0. La falla si trova nella funzione strcpy all'interno del file /goform/setSysAdm, che fa parte del componente API del dispositivo. In particolare, la vulnerabilità nasce dalla manipolazione del parametro passwd1, che causa un buffer overflow. Questo permette a un attaccante remoto di eseguire un attacco senza bisogno di autenticazione, potenzialmente compromettendo il dispositivo.	



CVE	PRODOTTI	SCORE CVSS NIST
<a href="#">CVE-2025-40585</a>	G5DFR (Digital Fault Recorder)	N/A
<b>VULNERABILITÀ</b>	<p>La vulnerabilità CVE-2025-40585 riguarda il componente G5DFR di Energy Services, una piattaforma utilizzata per la gestione e il monitoraggio di sistemi energetici. La vulnerabilità è dovuta alla presenza di credenziali predefinite nel sistema, che non vengono modificate durante l'installazione o la configurazione iniziale.</p> <p>Questa situazione consente a un attaccante di ottenere accesso non autorizzato al componente G5DFR, con la possibilità di manipolare i dati in uscita dal dispositivo. Tale accesso potrebbe compromettere l'integrità e l'affidabilità dei dati gestiti dal sistema energetico, con potenziali impatti sulla sicurezza e sull'efficienza operativa.</p>	



### 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	<a href="#">CVE-2025-32433</a>
DESCRIZIONE	
<p>Questa vulnerabilità riguarda Erlang/OTP, un insieme di librerie e runtime per il linguaggio di programmazione Erlang. Erlang/OTP è ampiamente utilizzato in sistemi distribuiti, telecomunicazioni e applicazioni che richiedono alta affidabilità.</p> <p>La CVE-2025-32433 è una vulnerabilità nel server SSH integrato in Erlang/OTP che consente a un attaccante remoto non autenticato di eseguire codice arbitrario senza necessità di credenziali.</p> <p>Il problema interessa le versioni precedenti a OTP-27.3.3, OTP-26.2.5.11 e OTP-25.3.2.20, a causa di una gestione difettosa dei messaggi del protocollo SSH.</p>	

CVE	<a href="#">CVE-2025-24016</a>
DESCRIZIONE	
<p>Wazuh è una piattaforma open source per la prevenzione, il rilevamento e la risposta alle minacce.</p> <p>La vulnerabilità interessa le versioni dalla 4.4.0 fino alla 4.9.0 (esclusa la 4.9.1) ed è causata da una deserializzazione insicura dei parametri JSON nell'API DistributedAPI tramite la funzione <code>as_wazuh_object</code>.</p> <p>Un attaccante che riesce a iniettare dati non sanitizzati può far scattare un'eccezione non gestita (<code>__unhandled_exc__</code>) che permette di eseguire codice Python arbitrario.</p> <p>L'attacco può essere effettuato da chiunque abbia accesso all'API, come una dashboard o server compromesso, o in alcune situazioni da un agente compromesso.</p>	

CVE	<a href="#">CVE-2025-33053</a>
DESCRIZIONE	
<p>La vulnerabilità riguarda il protocollo WebDAV (Web Distributed Authoring and Versioning), che consente la gestione e modifica di file su server web da remoto, spesso usato in ambienti aziendali per la collaborazione. Il problema nasce quando un attaccante può manipolare il nome o il percorso di un file senza un adeguato controllo, permettendo al sistema di usare dati non affidabili per accedere o modificare file in modo pericoloso.</p>	

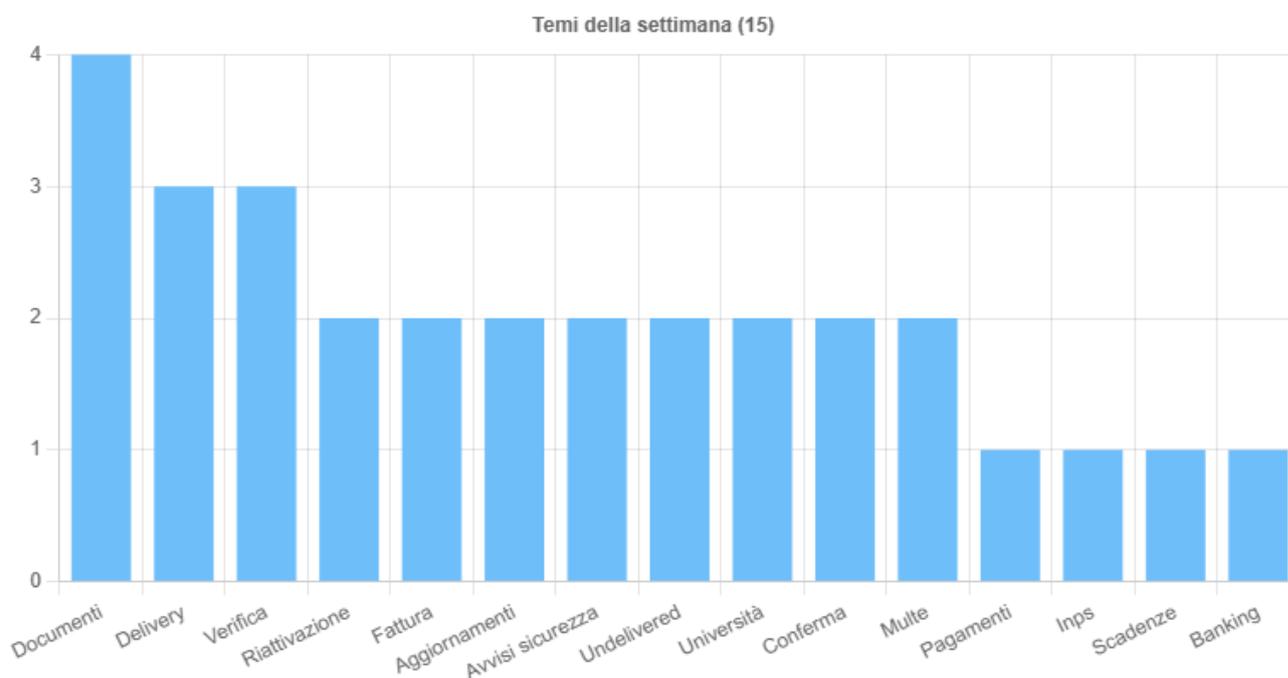
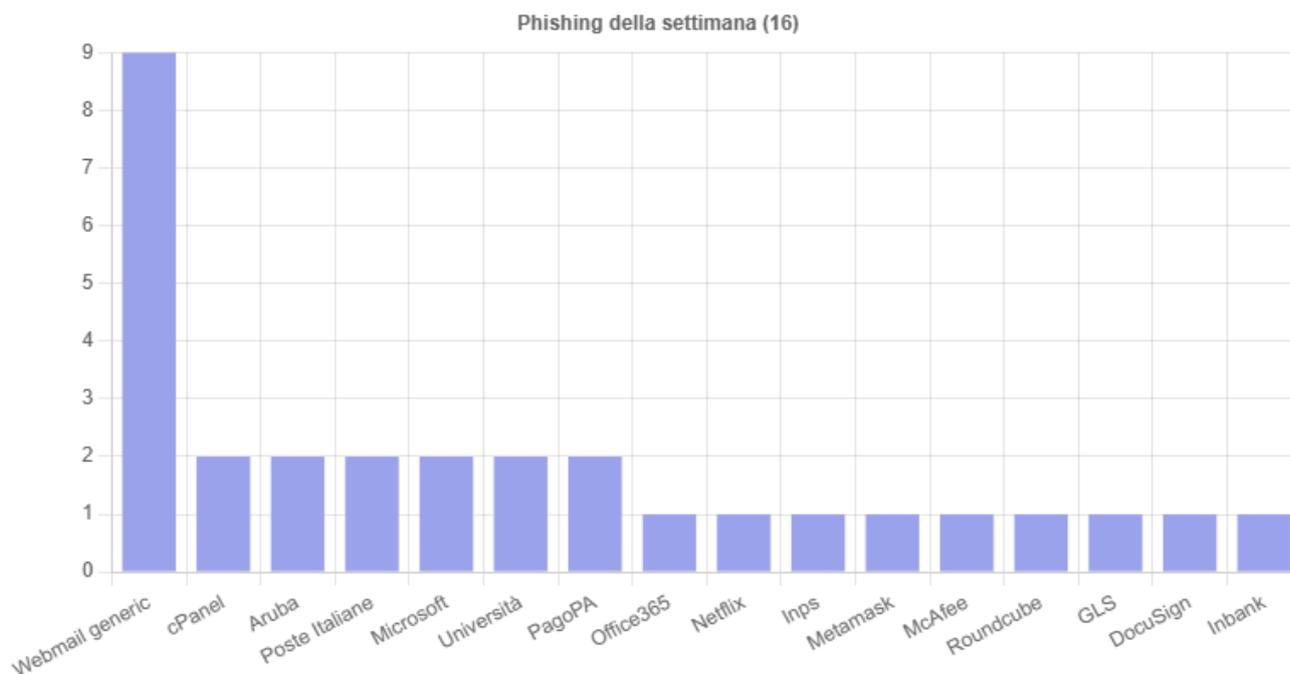


## 4 Attacchi

### 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.

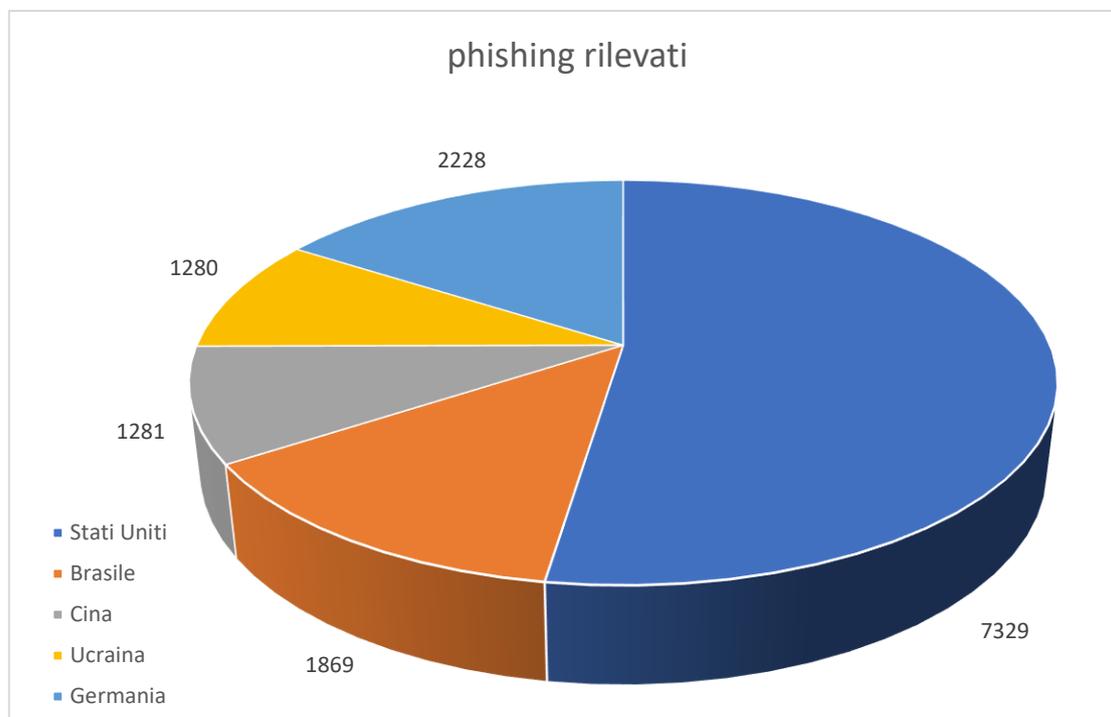


Fonte :CERT-AGID



## 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.



Qui di seguito viene il report dell'analisi di intelligence effettuata su una e-mail sospetta, con dominio mittente spoof[.]dom e server rivelatosi come 185[.]59[.]44[.]224. I risultati includono evidenze WHOIS, geolocalizzazione, reputazione IP, header, tecniche social engineering; IoC. Il dominio di destinazione sarà indicato come *victim[.]com* e destinatario come *victim* mentre il dominio mittente sarà indicato come *spoof[.]dom*.

Pur essendo una email "datata" viene analizzata in quanto presenta l'interessante caratteristica di impersonare una persona reale, dipendente di una azienda italiana realmente esistente e di utilizzare nel corpo della email i dati reali (indirizzo, telefono, ragione sociale) effettivi dell'azienda spoofata, al fine di raggirare il destinatario sembrando provenire da un mittente legittimo.

Anche il testo della email è studiato per sembrare parte di una conversazione in corso e fa leva sui soliti sensi di urgenza e necessità di eseguire una azione, che nel caso in esame è aprire un allegato contenente un ordine urgente.

- Verifica WHOIS dominio mittente ( spoof[.]dom )

L'email proviene da nome.cognome@spoof[.]dom. Dalla verifica dei record WHOIS il dominio spoof[.]dom risulta regolarmente registrato da una azienda italiana, e l'indirizzo della sede coincide con quello indicato nel corpo della email.



L'analisi degli header rivela che il server utilizzato per l'invio della mail non è il server MX legittimo del dominio impersonato ma `webmail[.]marlev[.]org`.

➤ Received: from `server[.]marlev[.]org` (static. 185[.]59[.]44[.]224 .netiyi.com [ 185[.]59[.]44[.]224 ])

- Hosting & geolocalizzazione server mittente

Il dominio `marlev.org` risponde all'IP `185[.]59[.]44[.]224`, assegnato ad ASN AS201928, provider Netiyi Telekomunikasyon Ltd. Sti (Turchia), città İzmir (`ipinfo.io`). Dunque il server si trova in Turchia, non in Italia come suggerito.

Un servizio interno (Forcepoint per SD-WAN) ha tracciato traffico e-mail significativo in luglio-novembre 2023 da quell'IP (`api.app.rwth-aachen.de`), ma non distingue tra buono e malevolo.

- Reputazione IP server mittente
  - Blacklist/DNSBL: le blacklist interrogate dallo strumento `WhatIsMyIPAddress` (`whatismyipaddress.com`) riportano segnalazioni di utilizzo malevolo dell'IP.
  - AbuseIPDB & APIVoid: Il rapporto sul dominio `marlev.org` riporta una segnalazione di abuso per quell'IP (`abuseipdb.com`).
  - Synoptica (Forcepoint): l'IP risulta in top IP mittenti di e-mail, ma senza valutazione negativa esplicita .
  - Conclusione reputazionale: IP già noto per utilizzi malevoli con segnalazione pubblica di phishing/spam, proveniente da infrastruttura incongruente (server in Turchia, mittente italiano).

- 
- Header email

L'header mostra:

- SPF: pass (il server mail maschera SPF passando come `webmail.marlev.org`, IPv6 ::1 sull'host) (`whois.com`).
  - DKIM: non presente; nessuna firma DKIM nel header.
  - DMARC: assenza totale di record e policy.
  - Il Return-Path è congruente con mittente, ma via infrastructure mascherata (server `marlev.org`, `marlev=provider`).
  - Il server mittente non risiede in Italia, generando sospetto di incongruenza.
- Analisi contenuto + tecniche social

Il messaggio usa tono urgente e professionale, autenticità apparente (firma, logo, contatti). Il mittente riprende contatti precedenti, tecniche di follow-up ("nessuna risposta"), allegato richiesto fattura proforma: classico pretesto phishing B2B per indurre la vittima ed eseguire una azione. Nessun link malevolo esplicito, ma allegato sospetto.



- Allegati ("logo.png", "Nuova LISTA ORDINI .zip)

Nella mail è allegato il logo ufficiale della azienda spoofata.

Il file zip invece contiene un allegato eseguibile. L'analisi tramite sandbox ha confermato trattarsi di un eseguibile malevolo, nella fattispecie si tratta del trojan downloader MODILOADER.

- Evidenze visive

Da nome cognome <nome.cognome@spoof.com>  Rispo  
A undisclosed-recipients;  
Oggetto **RE: RE: RE: Conferma dell'ordine**

Ciao,

Ti abbiamo inviato mail molte volte ma nessuna risposta da parte tua, non so se ricevi la nostra posta o no, allegato è il nostro nuovo ordine, si prega di inviare una fattura proforma per effettuare il pagamento.

Distinti saluti.  
Responsabile acquisti,  
nome cognome  
[azienda spoofed] S.p.A

Address: [indirizzo azienda spoofed] - Italy  
Phone: +39 [telefono azienda spoofed] Email: [nome.cognome@spoof.com](mailto:nome.cognome@spoof.com)

Il giorno sab 10 giu 2023 alle ore 18:22 nome cognome <[nome.cognome@spoof.com](mailto:nome.cognome@spoof.com)> ha scritto:

Ciao,

in allegato il nostro nuovo ordine,  
si prega di inviare una fattura proforma.

Distinti saluti.  
Responsabile acquisti,  
nome cognome  
[azienda spoofed] S.p.A

Address: [indirizzo azienda spoofed] - Italy  
Phone: +39 [telefono azienda spoofed] Email: [nome.cognome@spoof.com](mailto:nome.cognome@spoof.com)

2 allegati almeno 371 kB  
logo.png NUOVA LISTA ORDINI.zip 371 kB

Dallo screenshot della mail si nota la presenza del logo aziendale (non visualizzato per garantire riservatezza) e allegato .zip

- IoC individuati

IoC Type	Value
IP Mittente	185[.]59[.]44[.]224
Dominio mittente	spoof[.]dom
Email mittente	Nome.cognome@ spoof[.]dom



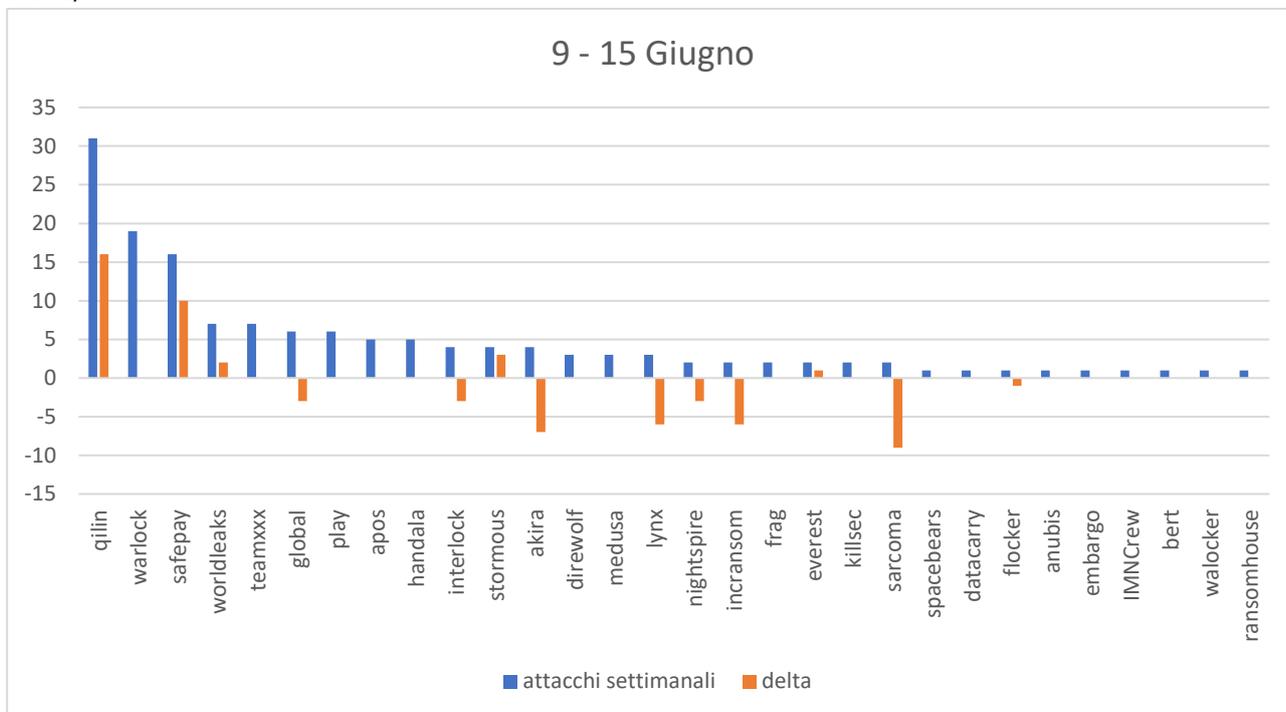
- Riepilogo

L'analisi mostra un'incongruenza strutturale: l'email sembra inviata da un'azienda italiana ma è instradata da un mail server in Turchia (Netiyi Telekom). L'IP è noto come malevolo. L'assenza di DKIM/DMARC e server basati fuori Italia per account aziendali legittimi è altamente sospetta. L'allegato è un .zip, cosa insolita nelle comunicazioni aziendali e una volta analizzato ha rivelato contenere un malware.

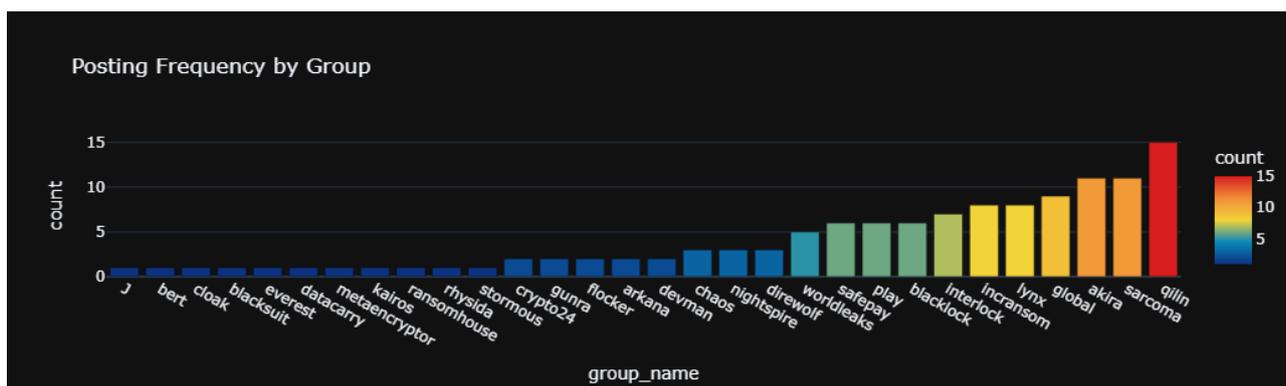


## 4.2 Ransomware

In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (9 - 16 Giugno). 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).

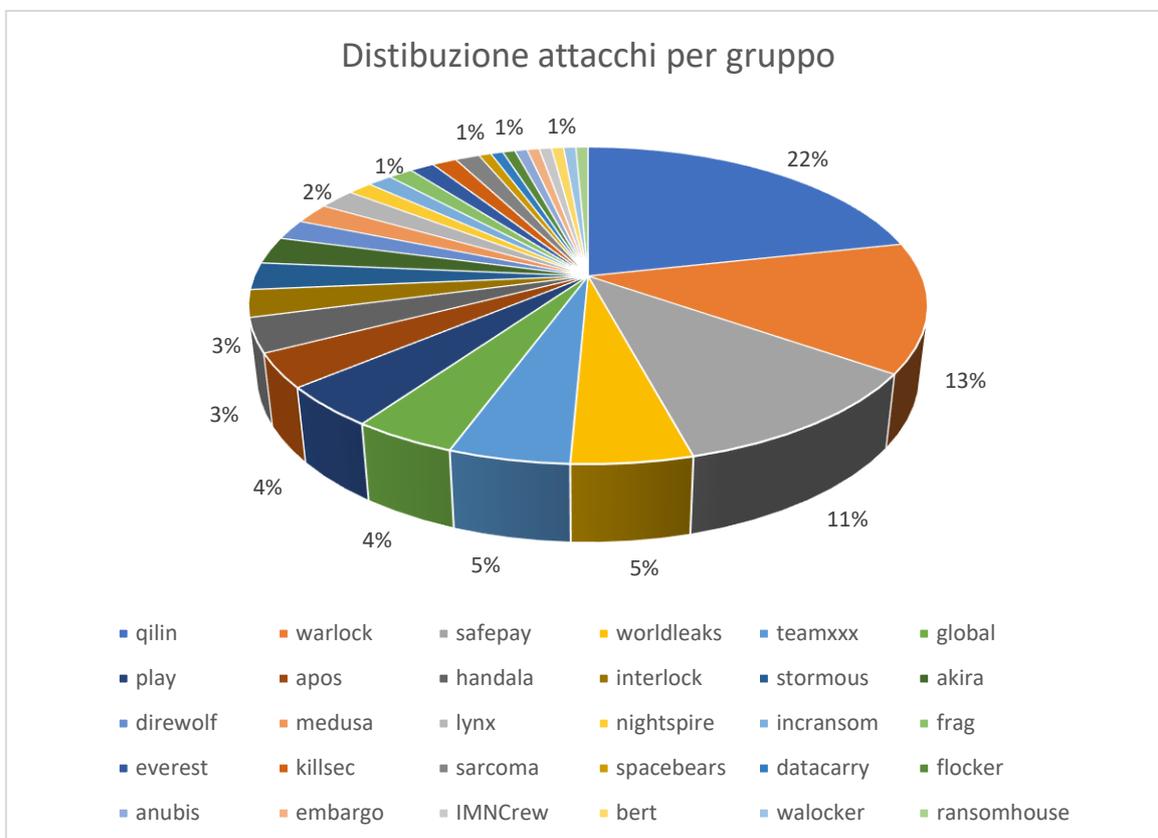


Raccogliendo i dati da un'altra fonte si ha la conferma di quanto sopra riportato riguardo l'andamento degli attacchi settimanali:





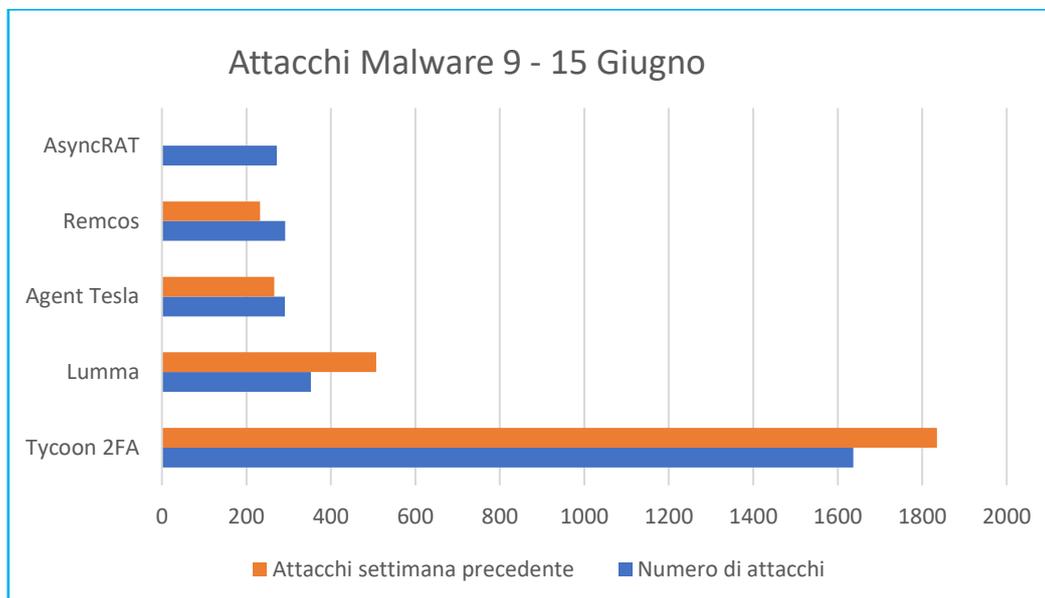
Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:





### 4.3 Malware

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



### Analisi Approfondita delle Minacce Malware Avanzate Rilevate (Marzo – Maggio) 2025

- MassJacker
  - Descrizione

MassJacker è un nuovo clipper per cryptojacking scoperto nel primo trimestre del 2025. Infetta le vittime attraverso un sito di software pirata (pesktop.com) ed esegue uno script PowerShell che scarica più payload: una botnet (Amadey) e due loader .NET (chiamati PackerE e PackerD). Questi loader decrittano e iniettano il payload finale di MassJacker nel processo InstalUtil.exe, usando un'ampia offuscazione (hooking JIT, nascondimento dei metadati, VM personalizzata, loop anti-debug) per eludere l'analisi. Una volta in esecuzione, MassJacker *monitora gli appunti di Windows* alla ricerca di indirizzi di portafogli di criptovalute (tramite regex) e sostituisce ogni indirizzo copiato con uno controllato dall'attaccante. In pratica, intercetta transazioni legittime per dirottare i fondi. I ricercatori hanno identificato oltre 778.000 portafogli controllati dagli attaccanti (423 contenenti ~95.000 USD al momento dell'analisi) collegati a questa operazione. In sintesi, MassJacker è un clipper furtivo che si inietta in un processo fidato e dirotta criptovalute attraverso la manipolazione degli appunti.



- Indicatori di Compromissione

Indicatore	Tipo
pesktop[.]com	Dominio

- Tecniche MITRE:

Il comportamento di MassJacker include esecuzione, iniezione e accesso alle credenziali. Il delivery avviene via PowerShell (T1059.001: Command and Scripting Interpreter – PowerShell) . Utilizza T1055.001 (Process Injection) per iniettarsi in InstalUtil.exe . La sua funzione principale è il dirottamento degli appunti (T1056.001 – Input Capture: Clipboard) .

Rilevamento e Mitigazione: I difensori dovrebbero bloccare l'infrastruttura del malware e la sua catena di esecuzione. In particolare, bloccare o filtrare il dominio pesktop.com su firewall/DNS, e rilevare script PowerShell non autorizzati o esecuzioni anomale da installer piratati . Le soluzioni EDR possono rilevare i loader .NET avanzati e l'iniezione in memoria su InstalUtil.exe. Monitorare processi che modificano ripetutamente gli appunti.

- Livello di Rischio:

*Medio.* MassJacker è altamente evasivo, ma al momento si diffonde solo tramite canali di nicchia (siti di pirateria), limitandone la diffusione . L'impatto per vittima è contenuto (~95K USD finora), ma la sua capacità di operare in modo silente lo rende rilevante.

- Fonti:

- Tanium CTI June 2025: "MassJacker" malware analysis
- Tanium CTI internal telemetry – Wallet enumeration results
- Cisco Talos: "New MassJacker Clipper Delivered via Pirated Software Sites" (April 2025)

- Malware Poliglotta (Sosano)

- Descrizione

All'inizio del 2025, i ricercatori hanno scoperto una campagna mirata che distribuisce un nuovo backdoor multistadio denominato Sosano. Gli attaccanti hanno utilizzato *file poliglotta* (payload che appaiono come più tipi di file) per eludere i controlli . Proofpoint ha collegato questa tecnica a una campagna di spear-phishing (marzo 2025) rivolta a meno di cinque organizzazioni nei settori aviazione/satelliti e trasporti critici degli Emirati Arabi Uniti . Le email contenevano allegati come "OrderList.zip", "electronica-2024.pdf", ecc. Questi file, una volta eseguiti dall'utente, distribuivano DLL o eseguibili dannosi. Il payload finale (Sosano) era fortemente offuscato, polimorfico e costruito per sfuggire agli scanner statici .



- Indicatori di Compromissione

- Tecniche MITRE:

La campagna impiega *spearphishing con allegati malevoli* (T1566.001) e *esecuzione tramite LNK/macro* (T1204.002) . Sosano comunica via HTTP (T1071.001 – Exfiltration via Web Service).

- Rilevamento e Mitigazione:

Implementare filtri email e formazione utenti per evitare l’apertura di allegati sospetti. Analizzare archivi e PDF in sandbox. Bloccare i domini indicelectronics[.]net e bokhoreshonline[.]com. Usare EDR comportamentali per rilevare i file polimorfi. Segmentare le reti critiche.

- Livello di Rischio: *Alto*. La campagna è estremamente mirata e usa tecniche sofisticate. I settori colpiti sono infrastrutture critiche, e un successo avrebbe un impatto grave .

- Fonti

- Proofpoint Threat Insight: “Polyglot Malware Targets UAE Transportation Sector” (March 2025)

Indicatore	Tipo
indicelectronics[.]net	Domain
46.30.190[.]96	IP Address
SHA-256: 336d9501129129b917b23c60b01b56608a444b0fbe1f2fdea5d5beb4070f1f14	Malicious archive (OrderList.zip)
SHA-256: 394d76104dc34c9b453b5adaf06c58de8f648343659c0e0512dd6e88def04de3	Malicious LNK (OrderList.xlsx.lnk)
SHA-256: e692ff3b23bec757f967e3a612f8d26e45a87509a74f55de90833a0d04226626	Malicious PDF (electronica-2024.pdf)
SHA-256: 0c2ba2d13d1c0f3995fc5f6c59962cee2eb41eb7bdbba4f6b45cba315fd56327	Polyglot EXE ("Hyper-Info.exe")
bokhoreshonline[.]com	Domain (C2)
104.238.57[.]61	IP Address (C2)
SHA-256: 0ad1251be48e25b7bc6f61b408e42838bf5336c1a68b0d60786b8610b82bd94c	Sosano DLL payload



- Elastic Security: Polyglot attachment evasion techniques (April 2025)

- Gremlin Stealer

- Descrizione

Gremlin Stealer è un nuovo infostealer attivo su Telegram da metà marzo 2025 . È scritto in C#, simile ad Hannibal Stealer . L'operatore lo promuove in forum underground e ha già pubblicato archivi di dati rubati. Raccoglie cookie, password, dati di wallet crypto, credenziali FTP/VPN, info di sistema e screenshot . Riesce a bypassare le protezioni Chrome "cookie v20"

- Indicatori di Compromissione

Indicatore	Tipo
d1ea7576611623c6a4ad1990ffed562e8981a3aa209717065eddc5be37a76132	SHA-256 (Gremlin sample)
http://207.244.199[.]46/index.php	URL malevolo (C2)

- 3.3 Tecniche MITRE:

Usa T1071.001 per esfiltrare dati via HTTP . Legge dati locali (T1005) e monitora gli appunti (T1056.001).

- Rilevamento e Mitigazione:

Monitorare processi che accedono a browser o clipboard. Bloccare IP C2. Usare EDR per rilevare accessi anomali a Chrome. Limitare l'uso di Telegram in ambienti sensibili.

- Livello di Rischio:

*Medio.* Nuovo ma potente. Se dovesse diffondersi, l'impatto potrebbe aumentare significativamente .

- Fonti

- Palo Alto Networks: "New Gremlin Stealer Marketed on Telegram"
- Stamus Networks: Detection guidance for Gremlin traffic (May 2025)

- StilachiRAT

- Descrizione

StilachiRAT è un nuovo Remote Access Trojan (RAT) mirato al furto di criptovalute e dati di sistema . Scoperto da Microsoft IR (marzo 2025), opera come servizio Windows o standalone. Il payload principale, WWStartupCtrl64.dll, raccoglie info di sistema, estrae password da Chrome



e cerca estensioni di wallet crypto (20+) . Può copiare dati dagli appunti e impersonare utenti clonando token RDP .

- Indicatori di Compromissione

Indicatore	Tipo
394743dd67eb018b02e069e915f64417bc1cd8b33e139b92240a8cf45ce10fcb	SHA-256 (WWStartupCtrl64.dll)
app.95560[.]cc	Dominio (C2)
194.195.89[.]47	IP Address (C2)

- Tecniche MITRE:

Usa T1082 (System Info), T1555.003 (Chrome Credentials), T1056.001 (Clipboard), T1134.003 (Token Hijack).

- Rilevamento e Mitigazione:

Evitare software non verificato. Abilitare SmartScreen e link sicuri. Bloccare dominio/IP. Usare EDR in modalità blocco per prevenire DLL sospette

- Livello di Rischio:

*Medio.* Sofisticato e silenzioso, ma con diffusione limitata al momento.

- Fonti

- Microsoft Threat Intelligence Blog: “New C# RAT Targets Wallets with DLL Injection” (March 2025)
- Tanium CTI: Internal StilachiRAT tracking report
- Microsoft IOC Summary: StilachiRAT hash and C2 domains
- Microsoft Defender Guidance: Detection tuning and best practices for StilachiRAT (2025)
- SentinelLabs: “StilachiRAT – Chrome Wallet Hijacking”



- Interlock (Ransomware)

- Descrizione

Interlock è un nuovo gruppo di ransomware a doppia estorsione attivo dalla fine del 2024. Colpisce organizzazioni grandi (difesa, sanità, industria), criptando file e minacciando la pubblicazione dei dati esfiltrati. A maggio 2025 ha colpito la National Defense Corporation USA e le sue sussidiarie (es. AMTEC) . Dati sottratti sono stati pubblicati su un sito Tor (ebhmkooh...onion) . Interlock è attivo su Windows e FreeBSD e usa tecniche avanzate (ESXi targeting, rundll32.exe per persistenza).

- Indicatori di Compromissione

Indicatore	Tipo
ebhmkoohccl45qesdbvrjqtyro2hmkhkmh6vkyfyjzflm3ix72aqaid.onion	Sito leak Tor
23.95.182[.]59	IP Address
195.201.21[.]34	IP Address
159.223.46[.]184	IP Address
212.237.217[.]182	IP Address
216.245.184[.]170	IP Address

- Tecniche MITRE:

Cripta dati (T1486), esfiltra file (T1005), esegue via rundll32 (T1218.011), e potrebbe cancellare backup (T1490).

- Rilevamento e Mitigazione:

Usare backup offline. Monitorare vssadmin, cipher.exe, traffico Tor, e attività anomale di cifratura. Segmentare e aggiornare host virtualizzati. MFA e blocco RDP consigliati.

- Livello di Rischio:

*Alto.* Ha già colpito entità critiche. L'uso della doppia estorsione e la capacità cross-platform lo rendono una minaccia seria .

- Fonti

- Fortinet Threat Intelligence Brief: "Interlock Ransomware Hits US Defense Contractor" (May 2025)
    - Tanium CTI: Interlock server infrastructure



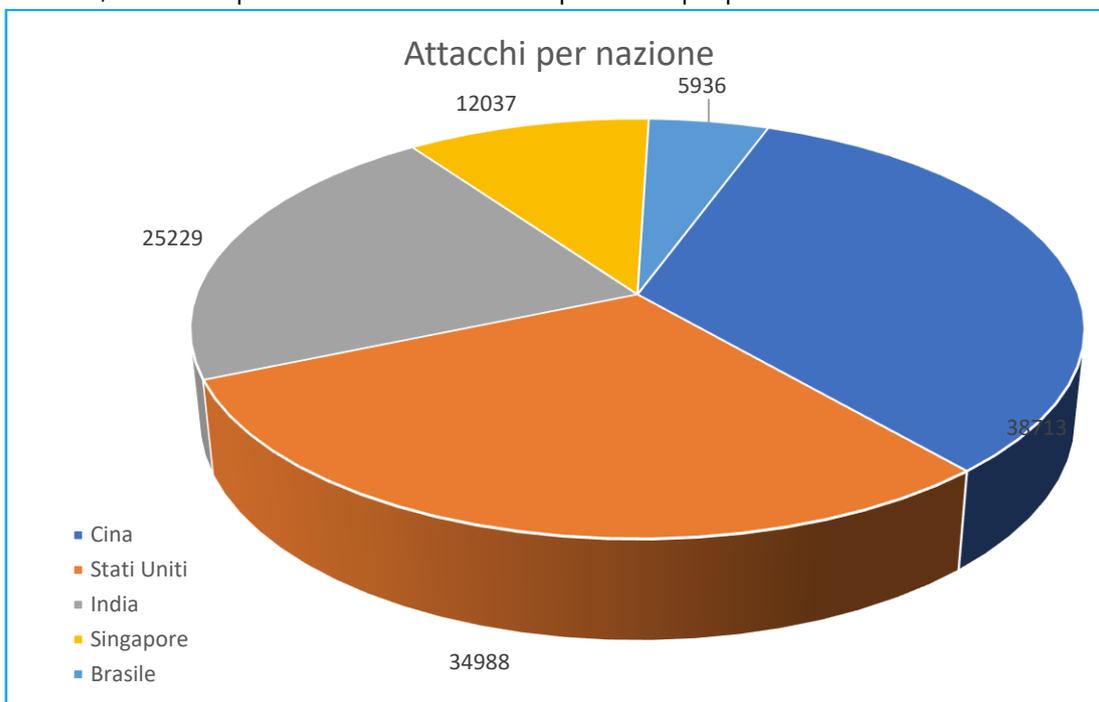
Riportiamo qui di seguito una tabella riassuntiva di quanto esposto in precedenza:

Malware	Tipo	Funzionalità Principale	Vettore di Infezione	Livello di Rischio
MassJacker	Clipper / Cryptojacker	Furto indirizzi wallet tramite clipboard	Software piratato (pesktop)	Medio
Sosano	Backdoor (Polyglot)	Controllo remoto e furto dati in ambienti aziendali	File allegati polimorfici (polyglot)	Alto
Gremlin Stealer	Infostealer	Estrazione credenziali, cookie e wallet	Diffusione su Telegram, mercati underground	Medio
StilachiRAT	RAT	Accesso remoto, furto di credenziali e wallet	Side-loading di DLL o aggiornamenti falsi	Medio
Interlock	Ransomware- as-a-Service	Crittografia e furto dati prima della richiesta	Phishing, script "ClickFix", RDP	Alto

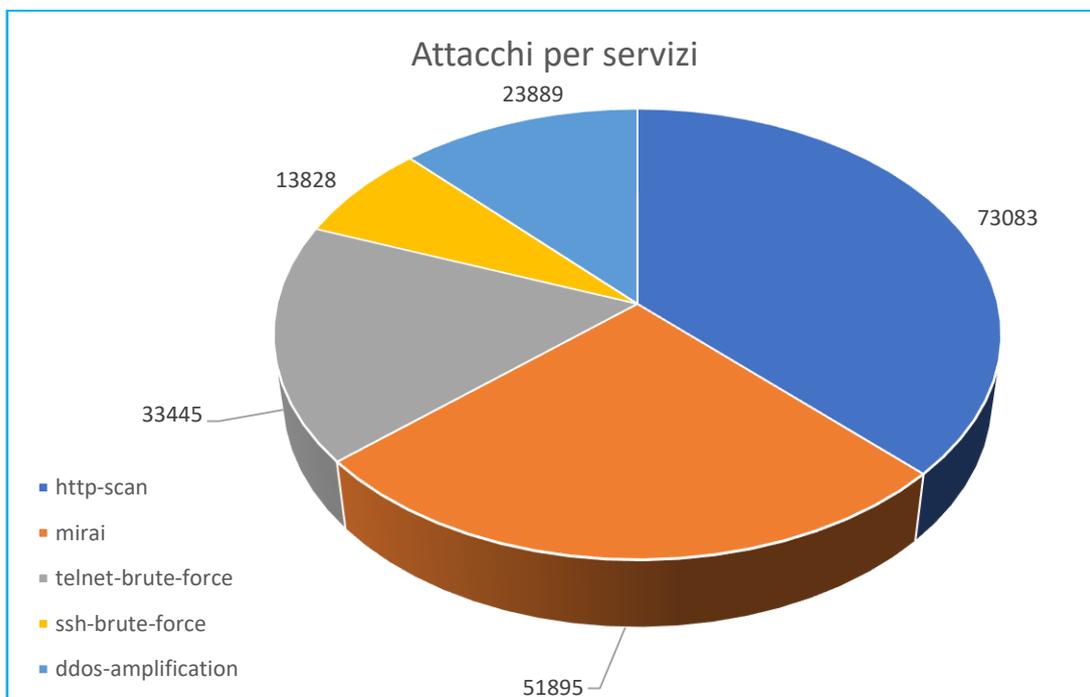


#### 4.4 DDoS rilevati

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



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



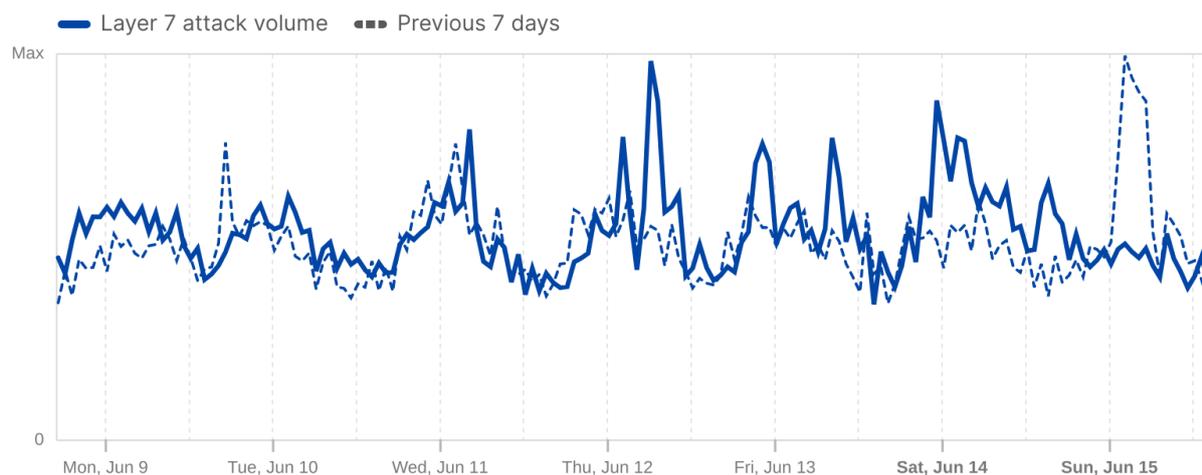


## SITUAZIONE ITALIANA

Nei due grafici seguenti viene riportato l'andamento settimanale degli attacchi DDoS condotti a livello applicativo e a livello network rispettivamente:

### Application layer attack volume in Italy

Layer 7 attack volume trends over time

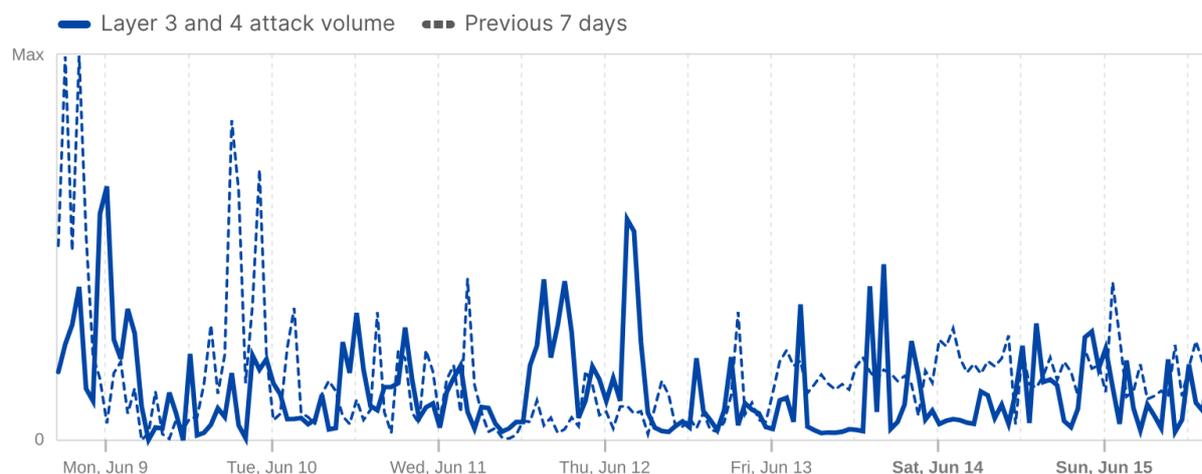


 Cloudflare Radar

Last 7 days | Jun 16, 2025, 06:30 UTC

### Network layer attack volume in Italy

Layer 3 and 4 attack volume trends over time based on the mitigating data center location



 Cloudflare Radar

Last 7 days | Jun 16, 2025, 06:45 UTC

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
ZOOMCAR HOLDINGS	INDIA
DESCRIZIONE	Il 9 giugno 2025, Zoomcar Holdings ha rilevato una violazione dei dati dopo che un attore di minaccia ha avvisato via email i dipendenti dell'azienda di un attacco informatico. La compromissione ha esposto i dati personali di 8,4 milioni di utenti, inclusi nome, numero di telefono, indirizzo email, targa e indirizzo di casa. Non risultano esposti dati finanziari o password in chiaro. Al momento nessun gruppo ha rivendicato l'attacco, la natura tecnica della violazione resta sconosciuta e l'azienda sta ancora indagando sull'impatto effettivo.

TARGET	LOCALIZZAZIONE
WESTJET	CANADA
DESCRIZIONE	Il 9 giugno 2025, la compagnia aerea canadese WestJet ha subito un incidente informatico che ha compromesso l'accesso alla sua app mobile e ad alcuni sistemi interni. L'azienda ha confermato che la sicurezza operativa e i voli non sono stati impattati, ma ha avviato un'indagine insieme alle autorità competenti per valutare l'estensione dell'attacco. Al momento non sono stati comunicati dettagli sui dati eventualmente sottratti, né alcun gruppo ha rivendicato la responsabilità della violazione. L'indagine è ancora in corso.



TARGET	LOCALIZZAZIONE
DIPARTIMENTO DELLA CULTURA E DEL TURISMO - ABU DHABI	EMIRATI ARABI UNITI
DESCRIZIONE	Il Dipartimento della Cultura e del Turismo di Abu Dhabi è stato vittima di un attacco ransomware da parte del gruppo Everest con un data breach scoperto e reso pubblico il 10 giugno 2025, anche se l'attacco è stato presumibilmente effettuato intorno al 26 maggio 2025. Il 10 giugno 2025 è stata pubblicata una fuga completa dei dati compromessi, evidenziando la gravità dell'incidente. L'attacco ha esposto dati interni e operativi, anche se non sono stati dettagliati dati personali sensibili specifici.



## 4.6 Defacement

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

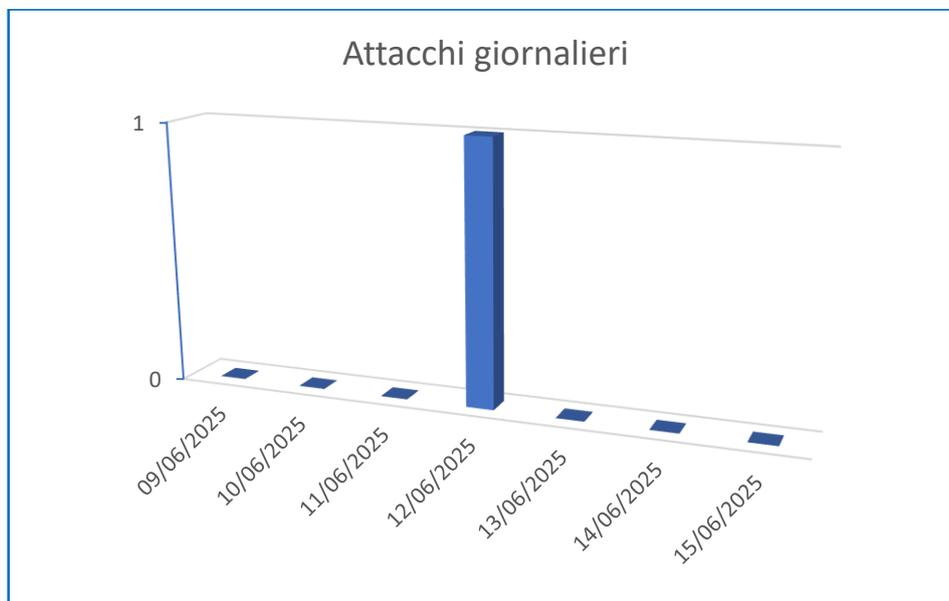


Figura 1: Defacement – Andamento giornaliero del numero di domini [.].it che hanno subito un defacement.



Figura 2: Defacement - Attaccanti più attivi nel periodo 1 - 8 Giugno 2025



## 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

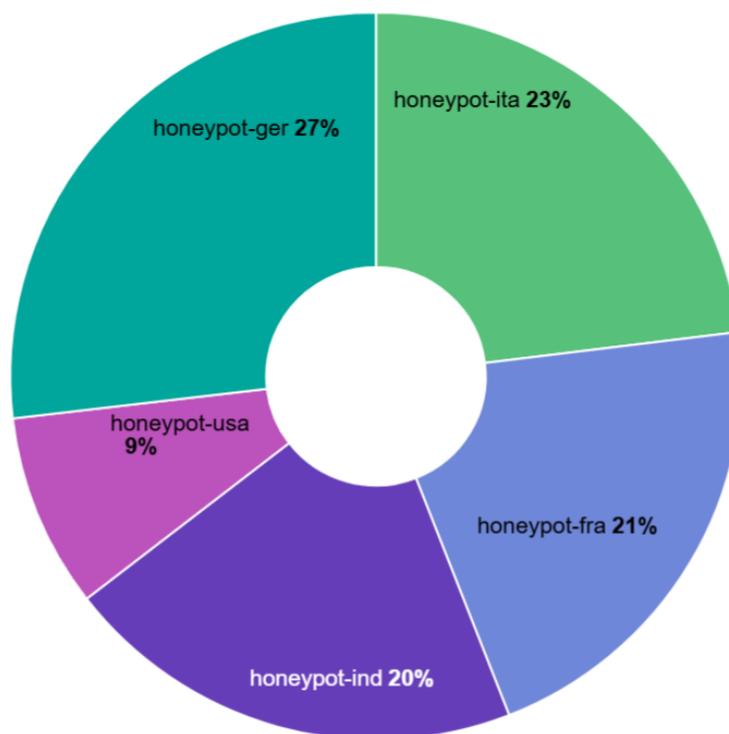
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

**840.622**  
Attacks

**10.141**  
Unique Src IPs

**59**  
Unique HASSHs

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



Questa invece la situazione a livello italiano:

**193.779**  
Attacks

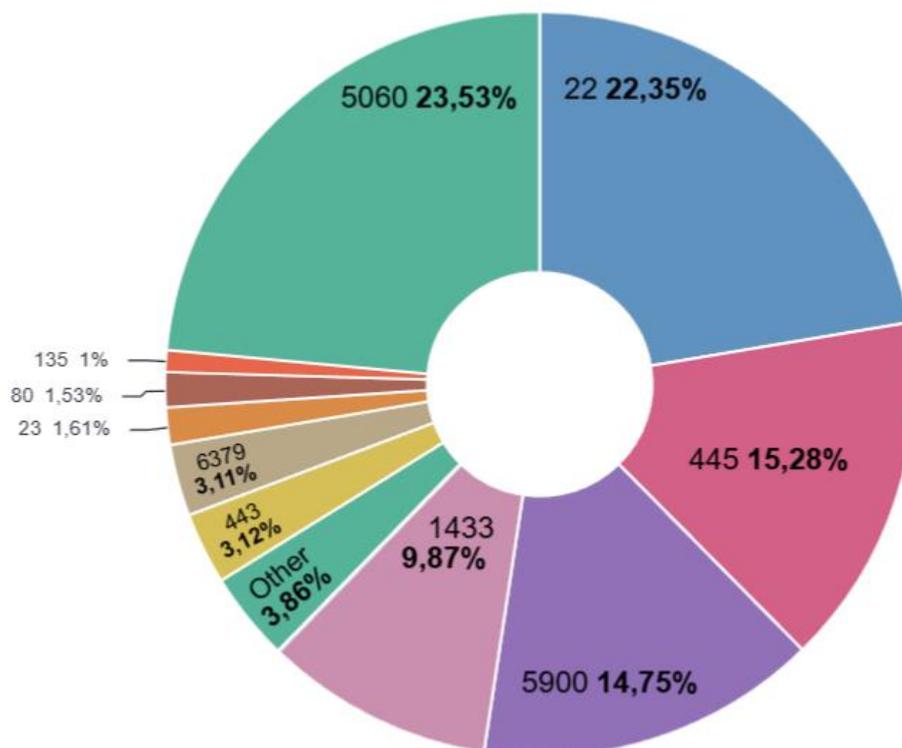
**3.257**  
Unique Src IPs

**41**  
Unique HASSHs



### 5.1.1 Attacchi ai servizi

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





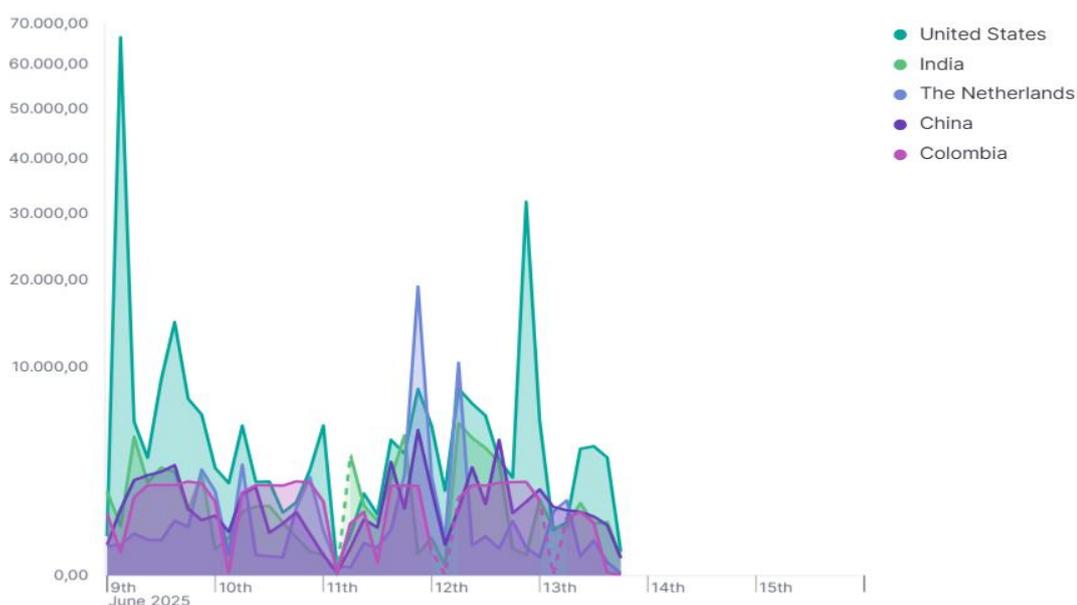
### 5.1.2 IP Attaccanti

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

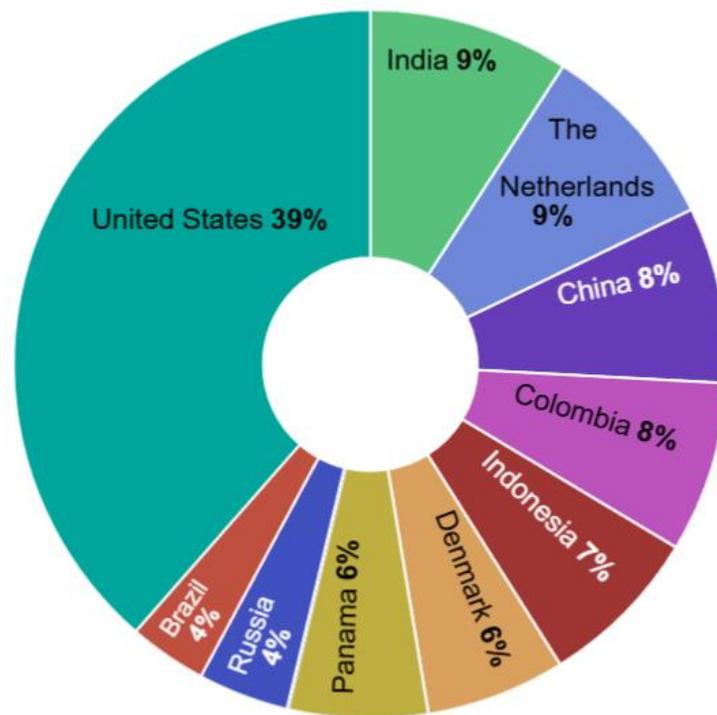
Source IP	Count
173.233.73.4	93.018
45.144.29.201	38.680
45.227.253.103	38.426
103.156.74.23	32.601
181.50.203.88	31.924
45.14.245.67	29.107
142.202.191.234	19.223
142.202.189.5	18.750
157.230.51.19	16.713
200.6.48.54	16.068

### 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:



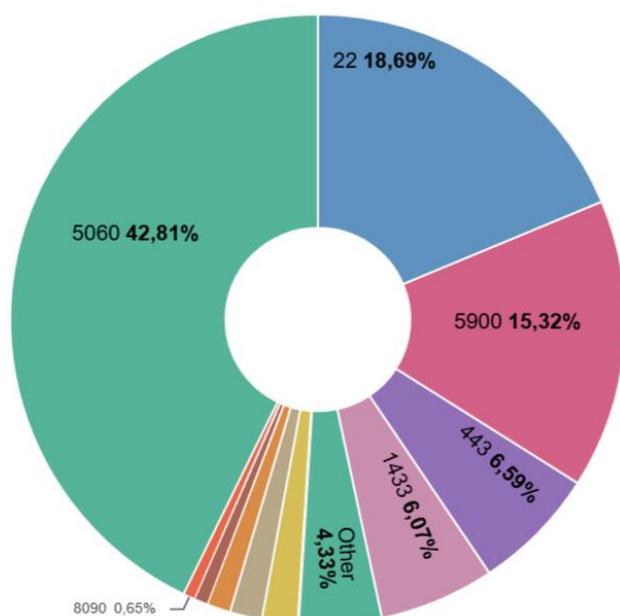


## 5.2 Italian Honeypot N.1

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):



Source IP	Count
5060	47.292
22	20.646
5900	16.921
443	7.280
1433	6.700
6379	2.071
23	1.865
80	1.382
8081	803
8090	722

### 5.2.2 IP Attaccanti

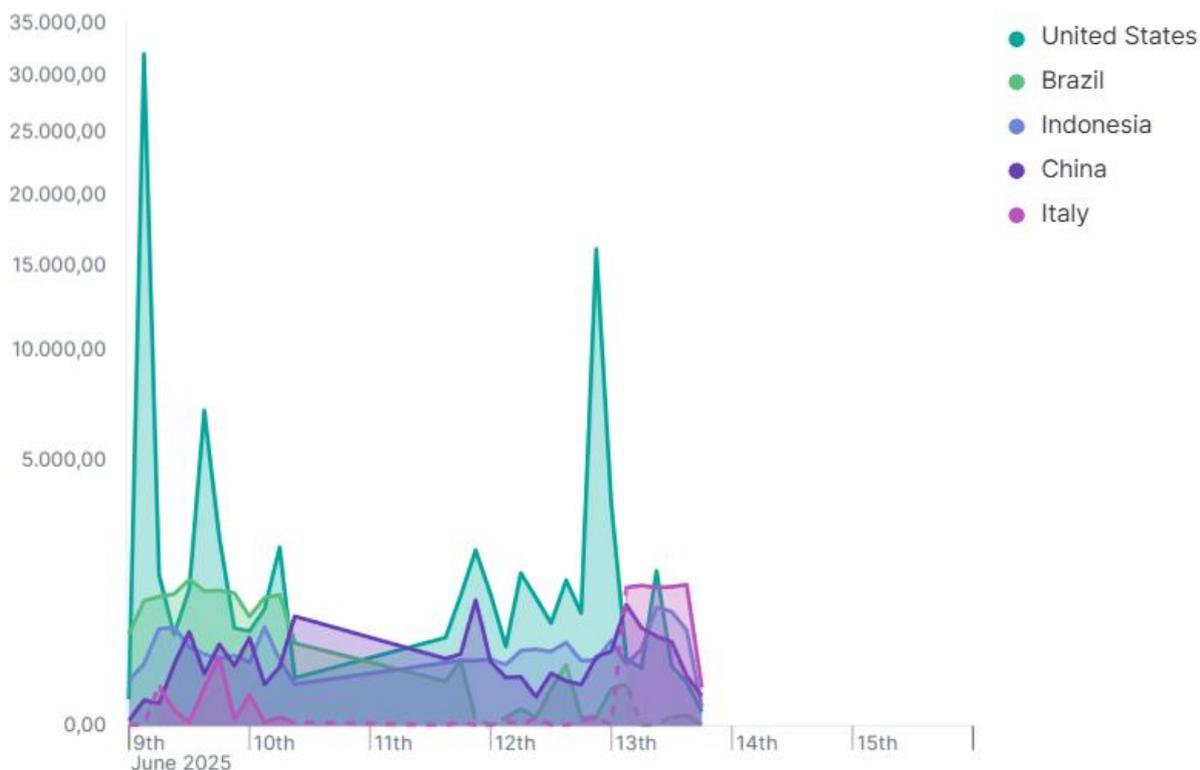
Questa invece la classifica relativa ai 10 IP che hanno effettuato il maggior numero di attacchi:

Source IP	Count
173.233.73.4	47.062
200.6.48.54	12.779
103.156.74.23	7.996
142.202.189.5	5.947
45.227.253.103	5.514
43.163.232.152	3.742
157.230.51.19	3.535
142.202.191.234	2.979
173.231.185.164	2.359
193.37.69.157	2.355



### 5.2.3 Paesi di provenienza degli attacchi

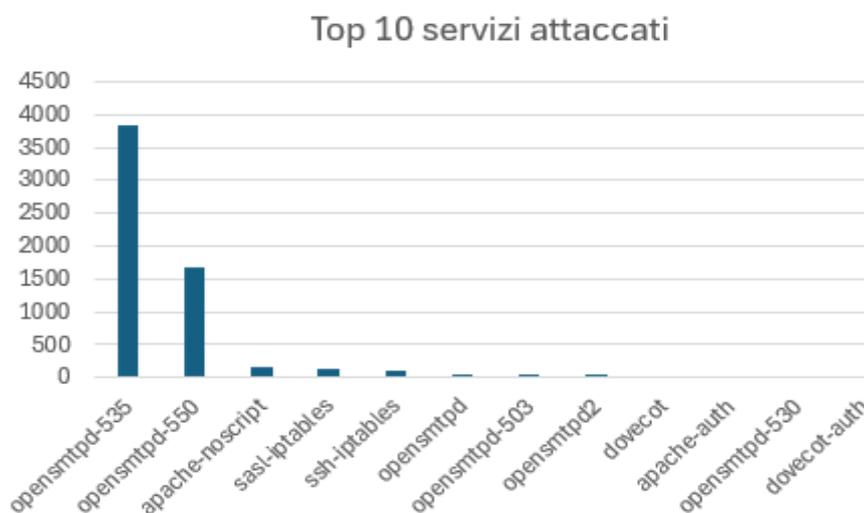
Si riporta l'andamento dei paesi attaccanti che hanno effettuato movimenti malevoli, verso l'Italia.



**5.3 Italian Honeypot N.2** Nel presente paragrafo vengono riportate le analisi relative all'honey-pot N.2 presente sul territorio italiano.

#### 5.3.1 Attacchi ai servizi

Questa la distribuzione degli attacchi per servizio attaccato.





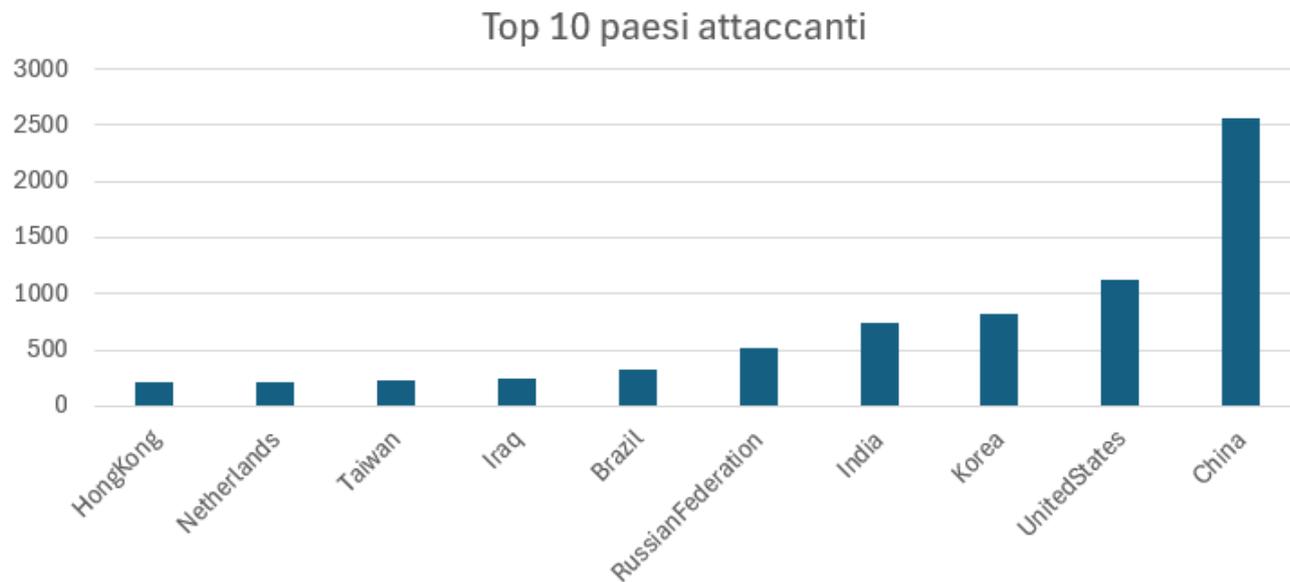
### 5.3.2 IP attaccanti

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
185[.]176[.]220[.]72	48
185[.]17[.]106[.]137	47
37[.]48[.]109[.]146	44
213[.]108[.]199[.]159	33
195[.]54[.]33[.]154	30
213[.]108[.]199[.]160	28
62[.]212[.]95[.]136	25
185[.]176[.]220[.]228	24
117[.]86[.]184[.]15	24
49[.]79[.]26[.]113	24

### 5.3.3 Paesi di provenienza degli attacchi

Questa invece la distribuzione dei paesi attaccanti:





## 6 Company Profile S3K

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

### **COME LO FACCIAMO:**

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

Abbiamo un presidio esteso sul territorio con circa 550 dipendenti distribuiti tra le sedi di Roma, Milano, Torino, Padova, Firenze, Palermo e Catania. L'ambizione e la prospettiva vedono un ulteriore e progressivo rafforzamento sia sul territorio nazionale che internazionale dove già operiamo con successo e con Clienti di primaria rilevanza.

### **CON QUALI LEVE OPERIAMO:**

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

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

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

### **CHI SIAMO:**

Un FULL SERVICE PARTNER DELLA DIGITAL & SECURITY TRANSFORMATION. Ci posizioniamo in modo unico nel mercato in cui operiamo, sia grazie

ad una precisa offerta multidisciplinare integrata, che al nostro approccio volutamente orientato alla semplificazione di tutto ciò che riguarda i processi di Digital e Security Transformation.

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

### **LA NOSTRA MISSION:**

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

### **I NOSTRI VALORI:**

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

### **CONTATTI:**

contattaci@s3k.it

insidesales@s3k.it

marketing@s3k.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.

---

<sup>1</sup> *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



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

