S3K

Cyber security

RISK REPORT

\ week 26.05.2025 - 01.06.2025

Sommario

1 Il Cyber Security Risk Report S3K 4

2 Security news 5

2.1 Rilasci aggiornamenti e patch 5

2.2 "Cyber News" dal Web, Deep Web e Dark Web 7

3 CVE Monitor 11

3.1 Sintesi Settimanale CVE 11

3.2 Tendenze 14

3.3 Nuove CVE 15

3.4 CVE attualmente utilizzate in attacchi 16

4 Attacchi 18

4.1 Phishing 18

4.2 Ransomware 24

4.3 Malware 26

4.4 DDoS rilevati 27

4.5 Data Breach 29

4.6 Defacement 31

5 Honeypot 32

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale 32

5.1.1 Attacchi ai servizi 33

5.1.2 IP Attaccanti 34

5.1.3 Paesi di provenienza degli attacchi 34

5.2 Italian Honeypot N.1 36

5.2.1 Attacchi ai servizi 36

5.2.2 IP Attaccanti 36

5.2.3 Paesi di provenienza degli attacchi 37

5.3 Italian Honeypot N.2 37

5.3.1 Attacchi ai servizi 37

5.3.2 IP attaccanti 38

5.3.3 Paesi di provenienza degli attacchi 38

6 Company Profile S3K 39


CYBER SECURITY RISK REPORT
22/25

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, 0day 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

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
Acronis Cyber Protect Cloud	Acronis ha rilasciato aggiornamenti di sicurezza per sanare varie vulnerabilità, di cui una con gravità "alta", nel prodotto Acronis Cyber Protect Cloud, sistema di sicurezza e backup con funzionalità integrate anti-malware e antivirus. Versioni affette: • Acronis Cyber Protect Cloud Agent, versioni precedenti alla build 40077
ULR/Note	https://security-advisory.acronis.com/advisories/SEC-8646

PRODOTTO	DESCRIZIONE
Kea DHCP	ISC ha rilasciato aggiornamenti di sicurezza per sanare varie vulnerabilità, di cui 1 con gravità "alta", nel prodotto Kea DHCP. Versioni affette: • Kea DHCP 2.4.x, versioni precedenti alla 2.4.2 • Kea DHCP 2.6.x, versioni precedenti alla 2.6.3 • Kea DHCP 2.7.x, versioni precedenti alla 2.7.9
ULR/Note	https://kb.isc.org/docs/cve-2025-32801

PRODOTTO	DESCRIZIONE
Spring Cloud Gateway Server	Aggiornamenti di sicurezza risolvono una vulnerabilità in Spring Cloud Gateway Server, gateway API del progetto Spring Cloud. Tale vulnerabilità riguarda l'inoltro degli header "X-Forwarded-For" e "Forwarded" che potrebbero essere manipolati da utenti malintenzionati per evadere i meccanismi di protezione del sistema target. Versioni affette: • 3.1.x, versioni precedenti alla 3.1.10 • 4.0.x, versioni precedenti alla 4.0.12 • 4.1.x, versioni precedenti alla 4.1.8 • 4.2.x, versioni precedenti alla 4.2.3 • versioni 4.3.0-M1/M2/RC1 • tutte le versioni precedenti non più supportate • Spring Cloud Gateway Server MVC • 4.1.x, versione 4.1.7 • 4.2.x, versioni precedenti alla 4.2.3 • versioni 4.3.0-M1/M2/RC1 • tutte le versioni precedenti non più supportate
ULR/Note	https://spring.io/security/cve-2025-41235

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

INTERLOCK E IL TROJAN NODESNAKE: ATTACCHI MIRATI AL SETTORE UNIVERSITARIO

Il gruppo ransomware conosciuto come Interlock è stato recentemente associato alla diffusione di un nuovo trojan di accesso remoto (RAT), fino ad ora non documentato, denominato NodeSnake, utilizzato specificamente in attacchi mirati alle istituzioni accademiche con l'obiettivo di ottenere un accesso persistente alle infrastrutture di rete. Secondo quanto rilevato dagli esperti, questo malware è stato osservato in almeno due attacchi distinti rivolti ad università nel Regno Unito, avvenuti rispettivamente a gennaio e marzo del 2025. Le due varianti del trojan analizzate presentano differenze sostanziali tra loro, segno evidente di un processo di sviluppo attivo volto ad incrementare le funzionalità e le capacità operative di NodeSnake. Emerso nel settembre 2024, Interlock è un gruppo criminale relativamente recente, ma già noto per aver preso di mira bersagli di alto profilo, tra cui la Texas Tech University, la compagnia sanitaria statunitense DaVita e il sistema ospedaliero Kettering Health con sede in Ohio. Il gruppo è inoltre noto per aver sfruttato una particolare tecnica di compromissione iniziale nota come attacco ClickFix, che consiste nel camuffare strumenti di supporto IT per ingannare le vittime ed indurle a scaricare software dannoso. Le campagne più recenti rivolte al settore educativo sono basate su e-mail di phishing contenenti link o allegati malevoli, che portano all'esecuzione del RAT NodeSnake. NodeSnake è sviluppato in JavaScript e viene eseguito tramite Node.js, rendendolo particolarmente versatile. Una volta infettato il sistema, il malware assicura la persistenza installandosi come un falso aggiornamento di Google Chrome tramite una voce di registro ingannevole denominata "ChromeUpdater"; questo stratagemma gli consente di mimetizzarsi all'interno dell'ambiente di sistema. Per evitare il rilevamento, NodeSnake opera come processo secondario in background, utilizza nomi di file casuali per i propri componenti, varia gli indirizzi dei server C2 (Command and Control) ed introduce ritardi casuali nella comunicazione. Il codice è pesantemente offuscato, ricorre a crittografia XOR con chiavi e seed variabili ed impiega tecniche di sabotaggio della console per interrompere i normali messaggi di debug, rendendo più difficile l'analisi da parte degli analisti di sicurezza. Sebbene l'indirizzo IP del server C2 sia integrato nel codice, il traffico viene incanalato attraverso domini proxy Cloudflare, una tattica che serve a mascherare le reali destinazioni delle comunicazioni ed aumentare la resilienza del malware. Una volta attivo, NodeSnake raccoglie una vasta gamma di informazioni sensibili, tra cui metadati dell'utente, processi in esecuzione, servizi di sistema attivi e configurazioni di rete, che vengono poi trasmessi al server C2. Il trojan è anche in grado di interrompere l'esecuzione di processi specifici o caricare nuovi payload in formato EXE, DLL o JavaScript.

Le versioni più recenti del malware includono il supporto all'esecuzione diretta di comandi CMD, nonché l'uso di moduli dinamici per modificare il comportamento del polling verso il server C2, facilitando un'interazione in tempo reale simile ad una shell remota. I risultati dei comandi vengono confezionati all'interno dei pacchetti di dati esfiltrati, migliorando le capacità di controllo remoto. La continua evoluzione di NodeSnake rappresenta un chiaro segnale dell'impegno di Interlock nello sviluppo di strumenti sempre più sofisticati, orientati alla persistenza silente e di lungo termine all'interno delle reti compromesse. Il monitoraggio e la rilevazione tempestiva di questi indicatori possono giocare un ruolo cruciale nel bloccare gli attacchi nelle prime fasi, prima che si arrivi alla esfiltrazione e cifratura dei dati, tipiche delle operazioni ransomware.

GRAVE VULNERABILITÀ IN CURSOR PER MACOS: A RISCHIO LA SICUREZZA DEI DATI SENSIBILI

Una grave vulnerabilità è stata individuata in Cursor, un editor AI per macOS, che può permettere accessi non autorizzati ad informazioni sensibili. Il problema deriva da una configurazione errata di Electron, il framework su cui si basa l'app: l'opzione RunAsNode, attivata in modo inappropriato, consente l'esecuzione di codice arbitrario. Questo permette agli attaccanti di sfruttare i privilegi dell'app, bypassando i meccanismi di sicurezza del sistema operativo. La falla rappresenta una minaccia seria per il sistema di Trasparenza, Consenso e Controllo (TCC) di Apple, progettato per tutelare la privacy degli utenti su macOS. TCC agisce come un filtro centrale che regola l'accesso delle app a risorse sensibili, come le cartelle Documenti, Download, Desktop e hardware come webcam e microfoni. Normalmente, qualsiasi accesso a queste risorse richiede un'autorizzazione esplicita da parte dell'utente, gestita tramite finestre di consenso. La vulnerabilità è stata identificata mentre alcuni ricercatori studiavano le tecniche usate per eludere le protezioni TCC in applicazioni di terze parti per macOS. Nonostante la segnalazione agli sviluppatori di Cursor, la falla non è stata corretta, con la motivazione che la problematica "non rientra nel loro modello di minaccia". Questa risposta ha suscitato preoccupazione nella comunità, tanto che alcuni utenti hanno deciso di rendere pubblica la scoperta, così da informare gli altri e permettere decisioni consapevoli sull'uso dell'app. Il rischio non si limita all'accesso ai file: mina una delle difese principali di macOS, rendendo il sistema vulnerabile a compromissioni silenziose. Se un attore malevolo dovesse sfruttare questa falla, potrebbe ereditare le autorizzazioni TCC dell'app, ottenendo accesso a dati privati, eseguendo screenshot, registrazioni audio o video senza avvisi o richieste di consenso visibili all'utente.

Gli scenari di attacco variano da operazioni completamente invisibili per l'utente a strategie più elaborate di ingegneria sociale, che celano richieste dannose dietro funzionalità apparentemente lecite dell'app.

Ciò che accentua la gravità della situazione è la diffusione crescente di Cursor tra gli sviluppatori, data la sua integrazione con strumenti di sviluppo basati su intelligenza artificiale. Questo lo rende un bersaglio ideale per chi vuole infiltrarsi negli ambienti di sviluppo e iniettare codice dannoso nei progetti software.

GOOGLE APPS SCRIPT NEL MIRINO DEL PHISHING PER BYPASSARE I CONTROLLI

Ricercatori di sicurezza hanno individuato una nuova tecnica di phishing che sfrutta in modo improprio Google Apps Script, la piattaforma di scripting basata su JavaScript integrata nei servizi cloud di Google Workspace, per ospitare pagine di accesso contraffatte progettate per rubare credenziali sensibili. L'analisi mette in luce come gli attori delle minacce stiano approfittando della reputazione e dell'affidabilità dei domini Google per creare pagine di phishing altamente credibili, in grado di ingannare anche utenti attenti. Secondo i ricercatori, la schermata di login fraudolenta è stata costruita con estrema cura per imitare perfettamente una finestra di accesso legittima, inducendo la vittima ad inserire i propri dati senza sospetti. La truffa comincia generalmente con l'invio di email ingannevoli mascherate da notifiche fiscali o fatture, che contengono link diretti ad una pagina web creata utilizzando Google Apps Script. Questa piattaforma consente a chiunque possegga un account Google di pubblicare un'applicazione web accessibile tramite un URL su dominio "script.google.com", spesso considerato sicuro da browser e strumenti di sicurezza. Gli attaccanti sfruttano questa possibilità per distribuire uno script che carica un modulo di login fasullo. Una volta che la vittima inserisce le proprie credenziali, i dati vengono inviati silenziosamente ad un server controllato dai cybercriminali. Per non destare sospetti, l'utente viene poi reindirizzato ad un vero servizio Google o ad una pagina coerente con il contenuto dell'email, rendendo meno evidente l'avvenuto furto di informazioni. Oltre all'efficacia ingannevole, questa tecnica offre agli attori malevoli flessibilità operativa: possono modificare il contenuto dello script in tempo reale senza dover aggiornare o inviare un nuovo link. Questo permette loro di adattare rapidamente l'attacco, cambiare l'esca o persino riciclare la stessa infrastruttura per nuove campagne, tutto senza interrompere la distribuzione dell'attacco. L'abuso di servizi cloud affidabili per ospitare contenuti dannosi è una tattica in crescita tra i gruppi criminali che operano campagne di phishing sempre più sofisticate. In particolare, Google Apps Script diventa un vettore particolarmente utile proprio per la fiducia implicita associata ai domini Google, che spesso non vengono bloccati dai gateway di sicurezza aziendali. Per ridurre il rischio di compromissione, le organizzazioni dovrebbero rafforzare i filtri di sicurezza per la posta elettronica, prestando particolare attenzione ai link che rimandano a servizi cloud come Google Apps Script. Una misura preventiva efficace potrebbe consistere nel monitorare o limitare l'accesso a questi URL, oppure segnalarli come sospetti anche se tecnicamente appartengono a domini legittimi. Al momento, Google non ha rilasciato dichiarazioni ufficiali in merito alla possibilità di introdurre meccanismi di protezione specifici contro questo tipo di abuso.

PUMABOT: NUOVA BOTNET LINUX MIRATA CONTRO DISPOSITIVI IOT

È stato recentemente individuato un nuovo malware botnet per sistemi Linux, denominato PumaBot, sviluppato in linguaggio Go. Questo codice malevolo prende di mira dispositivi IoT embedded, tentando di comprometterli attraverso attacchi brute force alle credenziali SSH, con l'obiettivo di distribuire payload dannosi. A differenza di molte altre botnet che operano tramite scansioni massicce di IP su Internet, PumaBot adotta un approccio mirato, selezionando bersagli specifici da una lista di indirizzi IP fornita da un server di comando e controllo (C2) — identificato come ssh.ddos-cc.org. Questo comportamento indica una strategia più sofisticata e selettiva, finalizzata probabilmente ad obiettivi di maggiore valore.

Durante la fase iniziale di compromissione, il malware tenta l'accesso SSH sulla porta 22, utilizzando credenziali fornite dal server C2. In questo processo, verifica anche la presenza della stringa "Pumatronix", il che lascia ipotizzare che il botnet sia stato progettato per prendere di mira in particolare sistemi di sorveglianza o telecamere per il traffico, potenzialmente prodotti da fornitori legati a quel nome.

Se l'accesso al dispositivo bersaglio ha successo, PumaBot esegue il comando uname-a per raccogliere informazioni sull'ambiente operativo e accertarsi che non si tratti di un honeypot (un sistema trappola usato per l'analisi del malware). Dopodiché, scrive il suo payload, chiamato jierui, nella directory /lib/redis e imposta un servizio systemd (redis.service) per garantirsi la persistenza anche dopo un riavvio del dispositivo. Per assicurarsi un accesso permanente, PumaBot aggiunge la propria chiave pubblica SSH al file authorized_keys, consentendo all'attaccante di connettersi in futuro anche se il malware principale venisse rimosso. Una volta stabilita la compromissione, il bot può ricevere ulteriori comandi dal C2 per eseguire attività come il furto di dati, il lateral movement all'interno della rete o l'installazione di payload aggiuntivi. Darktrace ha osservato diversi esempi di payload malevoli associati a PumaBot, tra cui:

- Script di auto-aggiornamento, utilizzati per mantenere il malware aggiornato.
- Un rootkit PAM che sostituisce il file legittimo pam_unix.so, intercettando le credenziali di accesso locali e remote.
- Un file binario denominato "1", che funge da "osservatore"

Il modulo PAM alterato raccoglie i dati di accesso SSH e li memorizza in un file chiamato con.txt; il file "1" lo monitora costantemente e, una volta rilevati nuovi dati, li invia al server C2. Subito dopo l'esfiltrazione, il file viene eliminato per cancellare le tracce dell'attività malevola. Al momento, non sono disponibili informazioni certe sull'entità dell'infezione o sull'estensione degli elenchi di IP presi di mira da PumaBot.

Ciò che rende questa botnet particolarmente pericolosa è il suo approccio mirato: piuttosto che limitarsi a usare dispositivi IoT compromessi per attacchi DDoS o come nodi proxy, PumaBot sembra progettato per infiltrarsi più in profondità nelle reti aziendali, potenzialmente per attività di spionaggio o sabotaggio.

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 26 Maggio – 1 Giugno 2025

Questa settimana è stata segnata da un'elevata concentrazione di vulnerabilità CRITICAL e HIGH, con particolare attenzione al mondo WordPress, sistemi ICS/IoT, e prodotti di Red Hat, Lenovo, Esri e IBM. Sono stati pubblicati diversi exploit pubblici, con impatti che spaziano dal privilege escalation all'esecuzione di codice remoto (RCE).

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit confermato	Descrizione Sintetica
CVE-2025-3357	CRITICAL	28/05/2025	❌	IBM Tivoli Monitoring: RCE remoto via accesso array senza validazione.
CVE-2025-41651	CRITICAL	27/05/2025	❌	ICS VDE: Nessuna autenticazione su comando remoto → RCE e file access.
CVE-2025-41652	CRITICAL	27/05/2025	❌	ICS VDE: Auth bypass via MD5 collision e brute-force.
CVE-2025-4607	CRITICAL	31/05/2025	✅ (Wordfence)	WP Plugin PSW Login: reset password admin via OTP debole.
CVE-2025-4631	CRITICAL	31/05/2025	✅ (Wordfence)	WP Plugin Profitori: privilege escalation da utente a admin.

CVE-2025-4967	CRITICAL	29/05/2025	❌	Esri ArcGIS Portal: SSRF bypass da remoto, non autenticato.
CVE-2025-5176	CRITICAL	26/05/2025	✅ GitHub	Realce Kiosk: SQLi remota in login admin.
CVE-2025-5190	CRITICAL	31/05/2025	✅ (Wordfence)	WP Plugin Browse As: bypass autenticazione via cookie hash.
CVE-2025-2501 CVE-2025-2502 CVE-2025-2503	HIGH	30/05/2025	❌	Lenovo PC Manager: 3 privilege escalation locali (permessi, path, file delete).
CVE-2025-32801	HIGH	28/05/2025	❌	Kea DHCP: load librerie malevoli via configurazione non sicura.
CVE-2025-4103	HIGH	31/05/2025	✅ (Wordfence)	WP Plugin GeoMeta: escalation privilegi via funzione senza controllo.
CVE-2025-4800	HIGH	28/05/2025	✅ (Wordfence)	MasterStudy LMS WP: upload arbitrario file → possibile RCE.
CVE-2025-48796 CVE-2025-48797 CVE-2025-48798	HIGH	27/05/2025	❌	GIMP: buffer overflow e use-after-free via ANI/TGA/XCF.
CVE-2025-5117	HIGH	27/05/2025	✅ (Wordfence)	WP Plugin Property: escalation privilegi via meta user role.

CVE-2025-5117 - 55	HIGH	26–27/05/2025	❌	ICS VDE – DoS, reboot remoto, SNMP leak e attacchi non autenticati.
CVE-2025-5172	HIGH	26/05/2025	✅ GitHub	Econtrata – SQLi su endpoint /valida?usuario=.
CVE-2025-4857	HIGH	31/05/2025	✅ Wordfence	WP Plugin Newsletters – LFI via parametro file, possibile 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

- **WordPress Plugin Ecosystem**: 8 vulnerabilità critiche → escalation privilegi, reset password, LFI, upload file.
- **ICS / IoT (VDE)**: vulnerabilità non autenticate (DoS, RCE, reboot remoto, SNMP).
- **Red Hat (GIMP)**: vulnerabilità locali via file grafici craftati.
- **Esri**: SSRF critico da remoto su Portal for ArcGIS.
- **Lenovo**: escalation di privilegi su PC Manager.
- **Econtrata & Realce**: SQLi pubbliche con PoC noti.
- **Kea DHCP**: Insecure default e config injection.

Distribuzione Giornaliera

- **27 maggio**: Disclosure ICS VDE, Red Hat (GIMP), Esri.
- **28–30 maggio**: Advisory IBM, Kea, Lenovo, MasterStudy.
- **31 maggio – 2 giugno**: Wordfence disclosure (Profitori, PSW, Browse As, Newsletters).

Raccomandazioni

- **Patch Prioritarie**:
    - Plugin WordPress con possibilità di escalation (PSW, Profitori, Browse As, Property, GeoMeta).
    - Dispositivi ICS/IoT esposti (VDE): isolare rete, disabilitare SNMP, aggiornare firmware.

- Sistemi aziendali: IBM Tivoli, Esri ArcGIS, Kea DHCP.

- **Monitoraggio**:
  - Exploit attivi GitHub / Wordfence.
  - Endpoint critici: /valida, paypal-submit.php, wp-ajax, wp-mailinglist.php.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2024-29269	Telesquare TLR-2005Ksh (dispositivo di rete)	N/A
CVE-2025-30397	Microsoft Scripting Engine	N/A
CVE-2025-5054	Canonical Apport (strumento di gestione dei crash usato nei sistemi Ubuntu)	N/A
CVE-2025-4598	systemd-coredump (componente del sistema systemd utilizzato nelle distribuzioni Linux per gestire e registrare i core dump, cioè i file che contengono lo stato della memoria di un processo al momento del crash)	N/A
CVE-2025-20188	software Cisco IOS XE, utilizzato nei Wireless LAN Controllers (WLC)	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-2025-5408	WAVLINK (QUANTUM D2G, QUANTUM D3G, WL-WN530G3A, WL-WN530HG3, WL-WN532A3, WL-WN576K1)	N/A
VULNERABILITÀ	Una grave vulnerabilità di tipo buffer overflow è stata scoperta nei dispositivi WAVLINK; questa falla si trova nella funzione di login (sys_login) del file /cgi-bin/login.cgi, che gestisce le richieste HTTP POST. La manipolazione del parametro login_page permette a un attaccante remoto di causare un buffer overflow, potenzialmente eseguendo codice arbitrario.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-4967	Esri Portal for ArcGIS (piattaforma software che consente alle organizzazioni di creare, gestire e condividere mappe, dati geografici e applicazioni GIS (Geographic Information System))	N/A
VULNERABILITÀ	La CVE-2025-4967 riguarda una vulnerabilità nel componente Server-Side Request Forgery (SSRF) di Esri Portal for ArcGIS, versione 11.4 e precedenti. Questa falla consente a un attaccante remoto non autenticato di aggirare le protezioni SSRF del portale. Sfruttando questa vulnerabilità, l'attaccante potrebbe inviare richieste HTTP malformate al sistema, potenzialmente accedendo a risorse interne non esposte all'esterno, compromettendo la sicurezza e la riservatezza dei dati.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-3357	IBM Tivoli Monitoring (software progettato per monitorare e gestire le prestazioni, la disponibilità e la salute di sistemi IT)	N/A
VULNERABILITÀ	Una vulnerabilità in IBM Tivoli Monitoring versioni da 6.3.0.7 fino al Service Pack 19 consente ad un attaccante remoto di eseguire codice arbitrario sfruttando una validazione errata di un indice in un array dinamico, che può portare a manipolazioni della memoria.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2024-51360	Hospital Management System in PHP	9.8
VULNERABILITÀ	La CVE-2024-51360 riguarda una vulnerabilità nel sistema Hospital Management System in PHP v4.0 sviluppato da PHPGurukul. Questa falla consente a un attaccante remoto non autenticato di eseguire codice arbitrario sfruttando un difetto nel file hms/doctor/edit-profile.php.	

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-2023-39780
DESCRIZIONE	
Sui dispositivi ASUS RT-AX55 con firmware versione 3.0.0.4.386.51598, un attaccante autenticato può sfruttare una vulnerabilità di iniezione di comandi OS attraverso il parametro qos_bw_rulelist presente nella pagina /start_apply.htm. Questo significa che l'attaccante, inserendo comandi malevoli in questo parametro, può eseguire comandi arbitrari sul sistema operativo del dispositivo, compromettendo la sicurezza del router.	

CVE	CVE-2025-35939
DESCRIZIONE	
Craft CMS memorizza contenuti arbitrari forniti da utenti non autenticati nei file di sessione. Questi contenuti potrebbero essere accessibili ed eseguiti, eventualmente sfruttando una vulnerabilità indipendente. Craft CMS reindirizza le richieste che richiedono autenticazione alla pagina di login e genera un file di sessione sul server nella cartella /var/lib/php/sessions. Tali file di sessione sono denominati sess_[valore_sessione], dove [valore_sessione] viene fornito al client nell'intestazione di risposta Set-Cookie. Craft CMS memorizza l'URL di ritorno richiesto dal client senza sanificare i parametri. Di conseguenza, un client non autenticato può inserire valori arbitrari, come codice PHP, in una posizione di file locale nota sul server.	

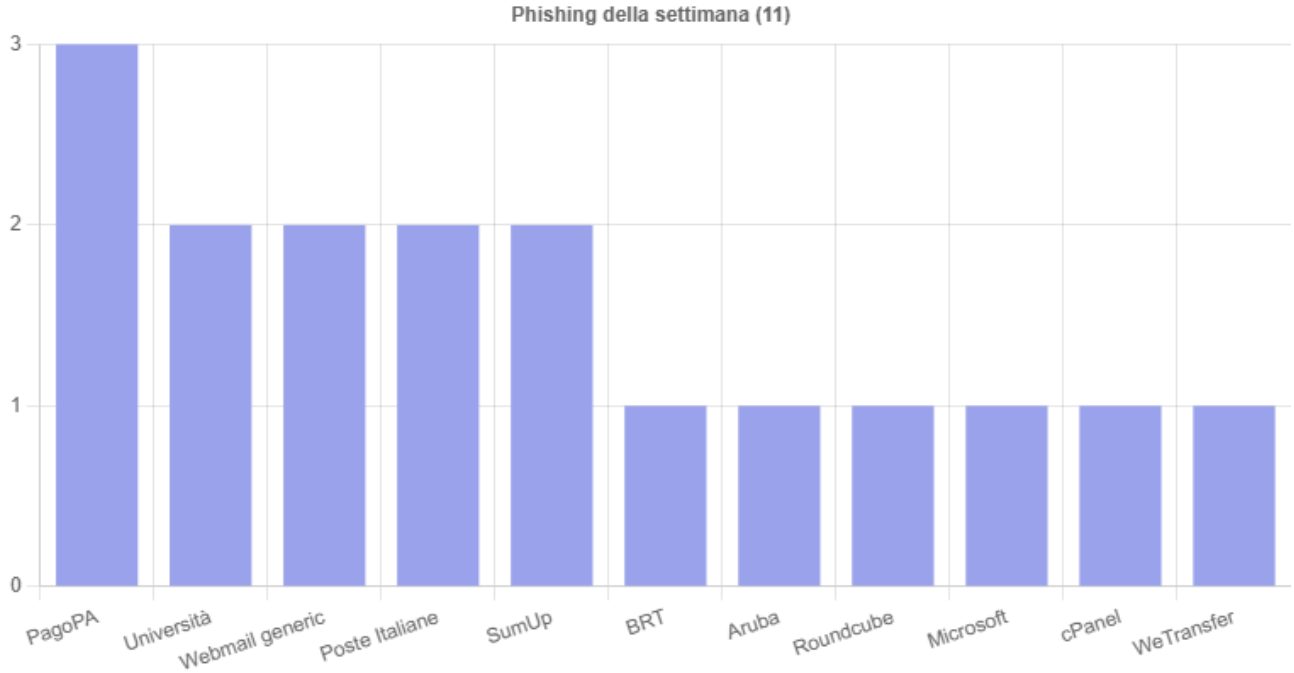
CVE	CVE-2025-3935
DESCRIZIONE	
Le versioni di ScreenConnect 25.2.3 e precedenti potrebbero essere vulnerabili a un attacco di iniezione di codice tramite ViewState. ASP.NET Web Forms utilizza ViewState per preservare lo stato della pagina e dei controlli, con i dati codificati in Base64 e protetti da chiavi macchina (machine keys). È importante notare che per ottenere queste chiavi macchina è necessario avere accesso privilegiato a livello di sistema. Se queste chiavi venissero compromesse, un attaccante potrebbe creare e inviare un ViewState malevolo al sito web, potenzialmente causando l'esecuzione di codice remoto sul server. Il rischio non deriva da una vulnerabilità introdotta da ScreenConnect, ma dal comportamento a livello di piattaforma.	

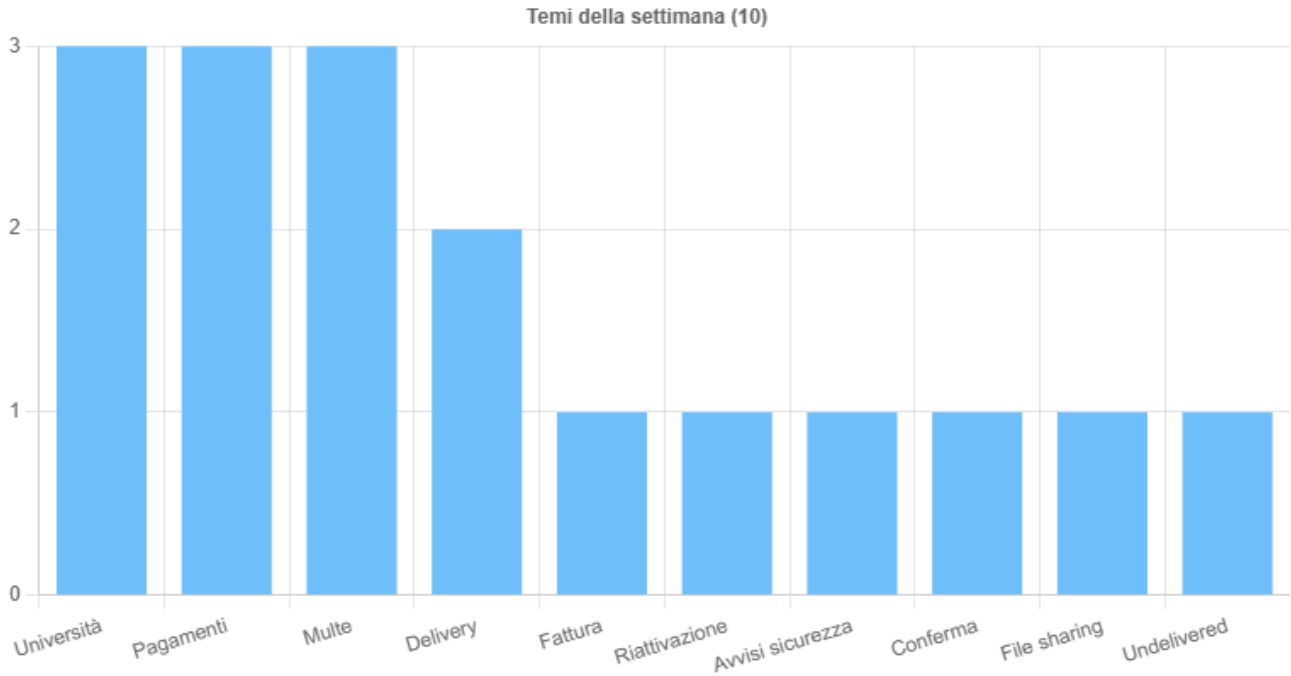
4 Attacchi

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.

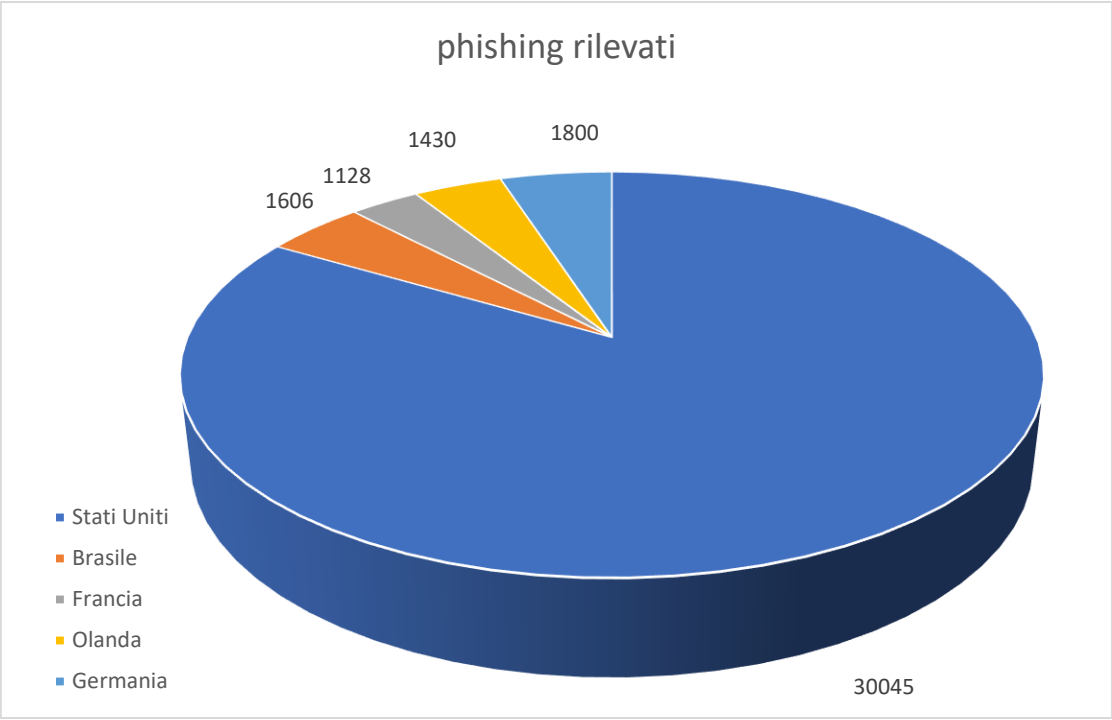




Fonte :CERT-AGID

Situazione Mondiale:

Nel seguente grafico troviamo una classifica dei primi cinque posti per Paese 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":

Rapporto di Analisi:

Email Phishing "Servizio di spedizione"

- Riepilogo Email

Campo	Valore
Mittente	Servizio di spedizione <6@buffetolives[.]com>
Return-Path	<6@buffetolives[.]com>
Relay	mailchannels[.]net (autenticato da webafrica)
Oggetto	Messaggio importante: il tuo pacco è in attesa di conferma
Destinatari	Oltre 500 (invio di massa)
URL incorporato	https://depositopedernal[.]com[.]uy/zeb
Lingua	Italiano
Brand imitato	DHL

- **Descrizione sintetica:**

  È stata inviata un'email di massa, apparentemente firmata come "Servizio di spedizione", che cerca di imitare comunicazioni ufficiali di DHL, richiedendo un pagamento di € 7,99 per la conoscenza di un presunto pacco in attesa di conferma. Il messaggio contiene un link sospetto a un dominio ".com.uy" non affiliato a DHL.

- Indicatori Principali di Phishing

Indicatore	Descrizione
Dominio mittente falso	buffetolives[.]com non appartiene a DHL; il mittente non è riconducibile al brand ufficiale.
Autenticazione email fallita	SPF risulta "passa" ma non è allineato (il dominio mittente non corrisponde al record SPF), DKIM assente, DMARC assente → elevato rischio di spoofing.
Link sospetto	URL punta a depositopedernal[.]com[.]uy, dominio geograficamente e logisticamente non correlato a DHL.
Email inviata in massa	Oltre 500 destinatari (campo "To:" usato per invio di massa), tipico schema di campagne phishing.
Saluto generico	"Gentile cliente" invece di utilizzare il nome personale del destinatario, segnale di invio massivo e non targettizzato.
Truffa economica	Viene richiesto un pagamento fittizio di € 7,99 per "sbloccare" il presunto pacco, stratagemma per estorcere dati di pagamento.
Grafica DHL falsificata	Layout, loghi e immagini riproducono in modo approssimativo l'aspetto ufficiale di DHL, per indurre in errore l'utente.
Errori di codifica	Appaiono caratteri malformati (es. "Gentile cliente, Ã¨ importante…"), dovuti a errata conversione UTF-8/ISO, altro indizio di creazione affrettata del messaggio.
Relay usato da spammer	Utilizzo di mailchannels[.]net e host sudafricano ("webafrica") per aggirare filtri antispam, frequente in campagne malevole.

- Analisi dell'Autenticazione Email

Protocollo	Risultato	Allineamento	Note
SPF	✅ Passa	❌ Non allineato	Il record SPF di mailchannels[.]net è valido, ma non corrisponde al dominio mittente (buffetolives[.]com).
DKIM	❌ Assente	—	Non è presente alcuna firma DKIM, quindi l'integrità del messaggio non è verificata.
DMARC	❌ Assente	—	Nessuna policy DMARC dichiarata, nessun vincolo di allineamento tra SPF/DKIM e dominio mittente.

- **Valutazione complessiva:**

  Il passaggio SPF non allineato, unito alla completa assenza di DKIM e DMARC, aumenta la probabilità di spoofing e phishing.

- Analisi del Link Incorporato
  - URL identificato: Errore. Riferimento a collegamento ipertestuale non valido.
  - Valutazione di sicurezza:
    - HTTPS presente, ma senza certificato EV (Extended Validation): questo dà un'impressione di sicurezza, ma non garantisce che il sito sia legittimo.
    - Dominio non affiliato a DHL: "depositopedernal.com.uy" non ha alcuna relazione con il brand DHL, né con alcuna società di spedizioni nota.
    - Geolocalizzazione in Uruguay (.uy): anomalia rispetto a una compagnia di logistica globale come DHL, che solitamente utilizza domini ufficiali (es. "dhl.com", "dhl.it").
    - Comportamento atteso: pagina clone progettata per carpire credenziali o dati di carta di credito sotto la falsa promessa di un servizio di consegna.
- Probabilità di Contenuto Generato da AI
  - Livello di sofisticazione linguistica:
    - Frasi persuasivi, urgenti e ottimizzati per massimizzare l'engagement ("Messaggio importante", "in attesa di conferma").
    - Assenza di errori grammaticali significativi, nonostante siano presenti caratteri malformati a causa di errata codifica.
    - Uso strategico di termini psicologici per creare senso di urgenza e responsabilità: "conferma", "pacco", "servizio", "importante", "attività finale".
  - Probabile origine AI (black-hat):

        - Il tono professionale, l'uniformità stilistica e la qualità "pulita" del testo, uniti alla mancanza di dettagli contestuali (es. numero di tracciamento reale), suggeriscono l'utilizzo di un modello generativo avanzato (es. "Xanthorox" o analoghi).
- Analisi dell'Header
    - Relay e route di consegna:
        - Passage attraverso mailchannels[.]net come server SMTP intermediario, autenticato tramite servizi "webafrica" (South Africa).
        - Questa configurazione è nota per essere usata da spammer e gruppi phishing per eludere i filtri basati su IP.
    - Assenza di firme e autenticazioni aggiuntive:
        - Nessuna firma DKIM → il messaggio non è "proveniente da un mittente verificato" secondo gli standard di posta certificata.
        - Nessuna intestazione Proofpoint (o similari), il che implica che non sono stati applicati meccanismi avanzati di sicurezza/filtraggio a monte.
- Verdetto tecnico sull'header:
    - Elevata probabilità di routing malevolo, mancata autenticazione certificata e utilizzo di relay "no-reputation" per sfuggire ai controlli antispam.

- Verdetto Finale

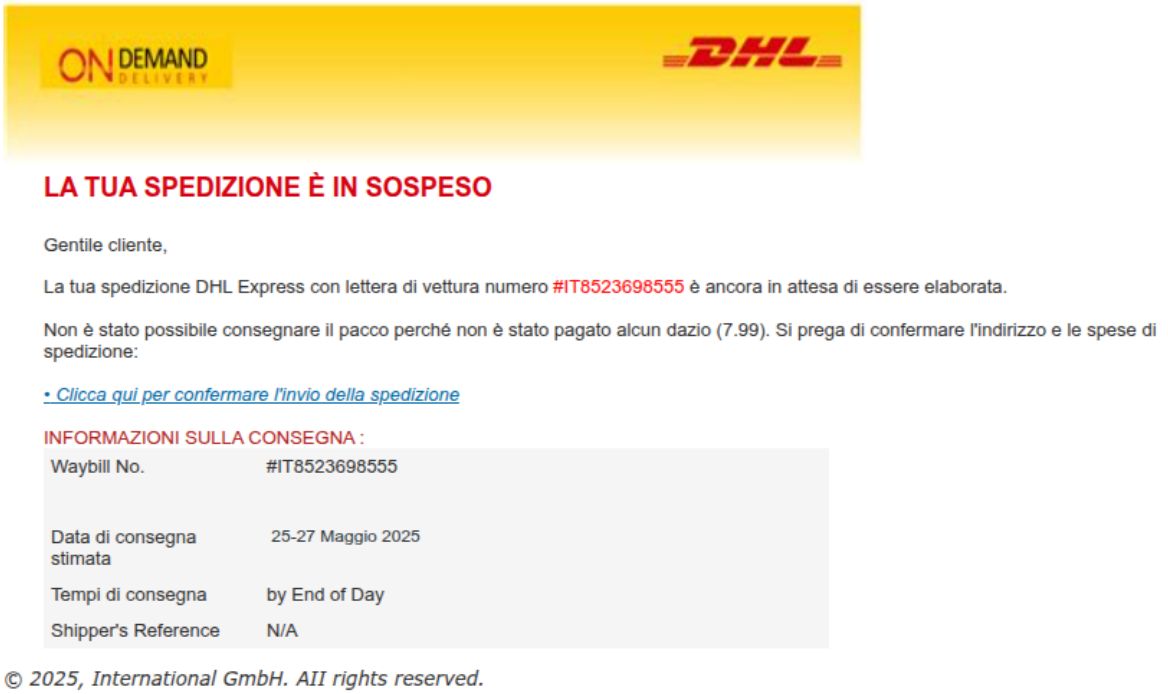
La combinazione di dominio mittente e di destinazione sospetti, l'assenza di adeguate firme di autenticazione (DKIM/DMARC), i contenuti generati con intento fraudolento (richiesta di € 7,99 per sbloccare un presunto pacco) e la presenza di un link verso un dominio ".uy" non riconosciuto rendono questa email un tentativo di phishing estremamente credibile e pericoloso.

- Catena dell'Attacco
    - Invio Email di Massa
        a. Mittente: 6@buffetolives[.]com tramite relay mailchannels[.]net (autenticato da webafrica).
        b. Oltre 500 destinatari ricevono contemporaneamente il messaggio, aumentando il potenziale di diffusione.
    - Imitazione del Brand DHL
        a. Il soggetto e il layout grafico simulano comunicazioni ufficiali di DHL.
        b. Invito a cliccare sul link per "confermare il proprio pacco".
    - Reindirizzamento al Sito Malevolo
        a. Link: https://depositopedernal[.]com[.]uy/zeb

b. Dominio geolocalizzato in Uruguay, con certificato HTTPS non EV, progettato per mascherarsi da pagina di pagamento/dati sensibili.

- Clonazione della Pagina di Login/Pagamento
  a. La vittima viene indotta a inserire dati personali e informazioni di pagamento su una pagina che riproduce il layout DHL, con l'obiettivo di rubare credenziali o denaro.

Qui di seguito uno screenshot della mail



ON DEMAND DELIVERY

DHL

LA TUA SPEDIZIONE È IN SOSPESO

Gentile cliente,

La tua spedizione DHL Express con lettera di vettura numero #IT8523698555 è ancora in attesa di essere elaborata.

Non è stato possibile consegnare il pacco perché non è stato pagato alcun dazio (7.99). Si prega di confermare l'indirizzo e le spese di spedizione:

• *Clicca qui per confermare l'invio della spedizione*

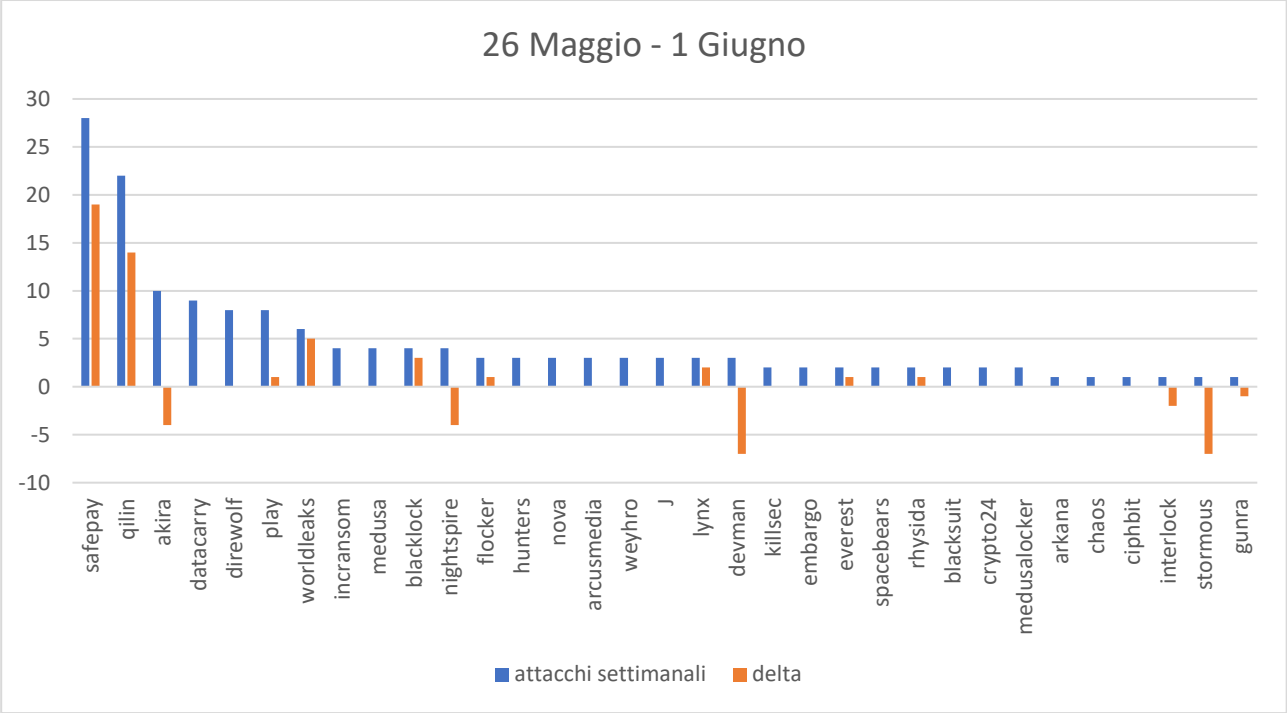
INFORMAZIONI SULLA CONSEGNA :

Waybill No.	#IT8523698555
Data di consegna stimata	25-27 Maggio 2025
Tempi di consegna	by End of Day
Shipper's Reference	N/A

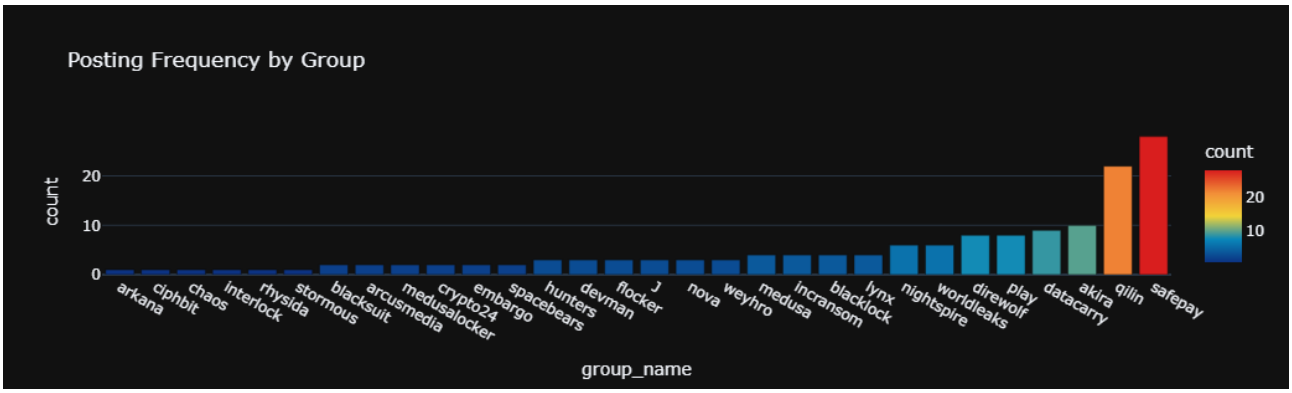
© 2025, International GmbH. AII rights reserved.

4.2 Ransomware

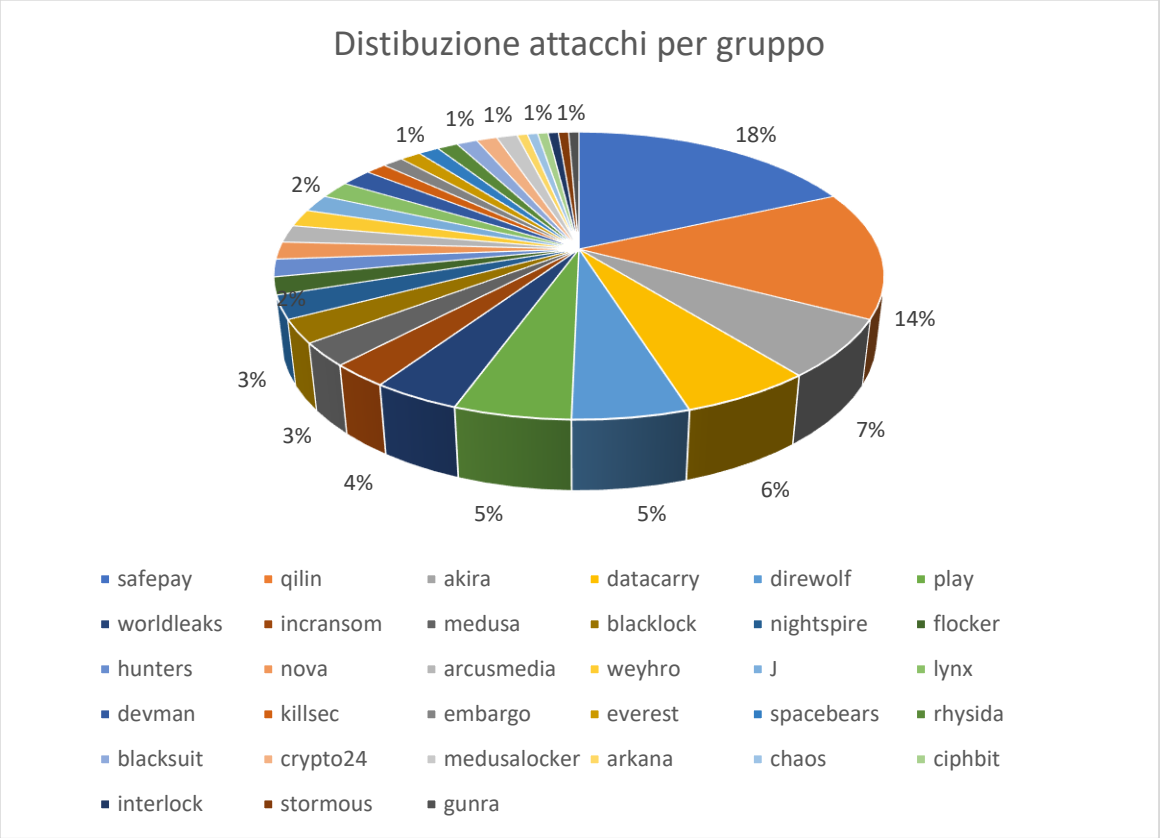
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (26 Maggio – 1 Giugno). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



Raccogliendo i dati relativi agli attacchi da un'altra fonte si ha un andamento pressochè identico, a conferma della validità dei dati; questo grafico prende in considerazione il solo andamento settimanale e ribadisce quanto riportato in precedenza.

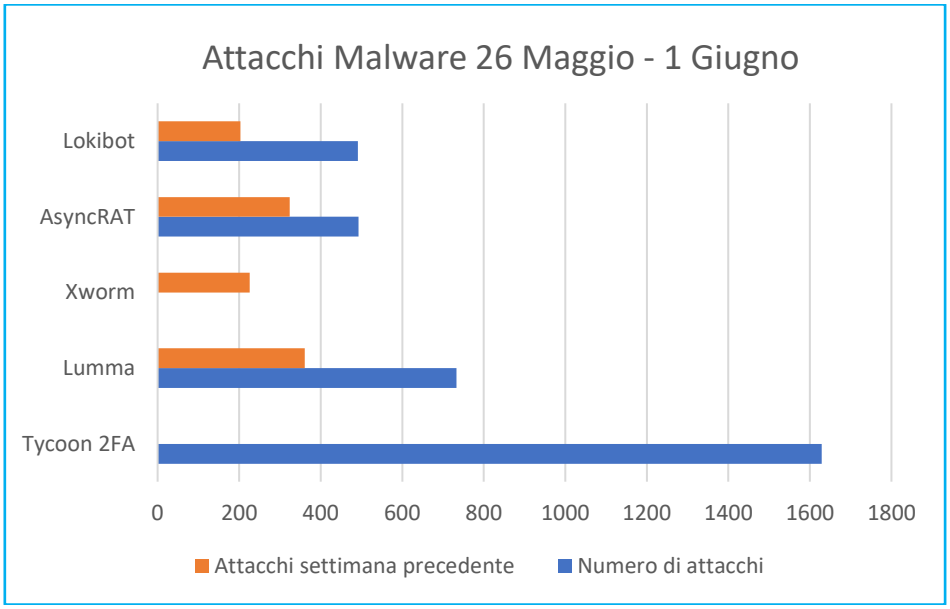


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:



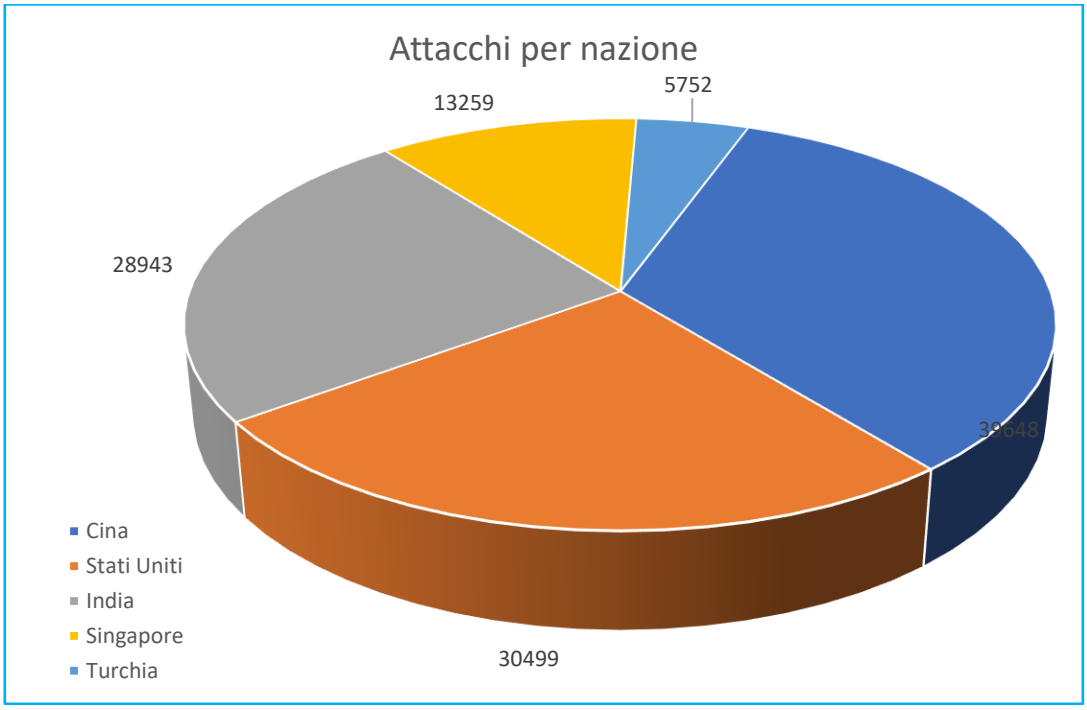
4.3 Malware

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

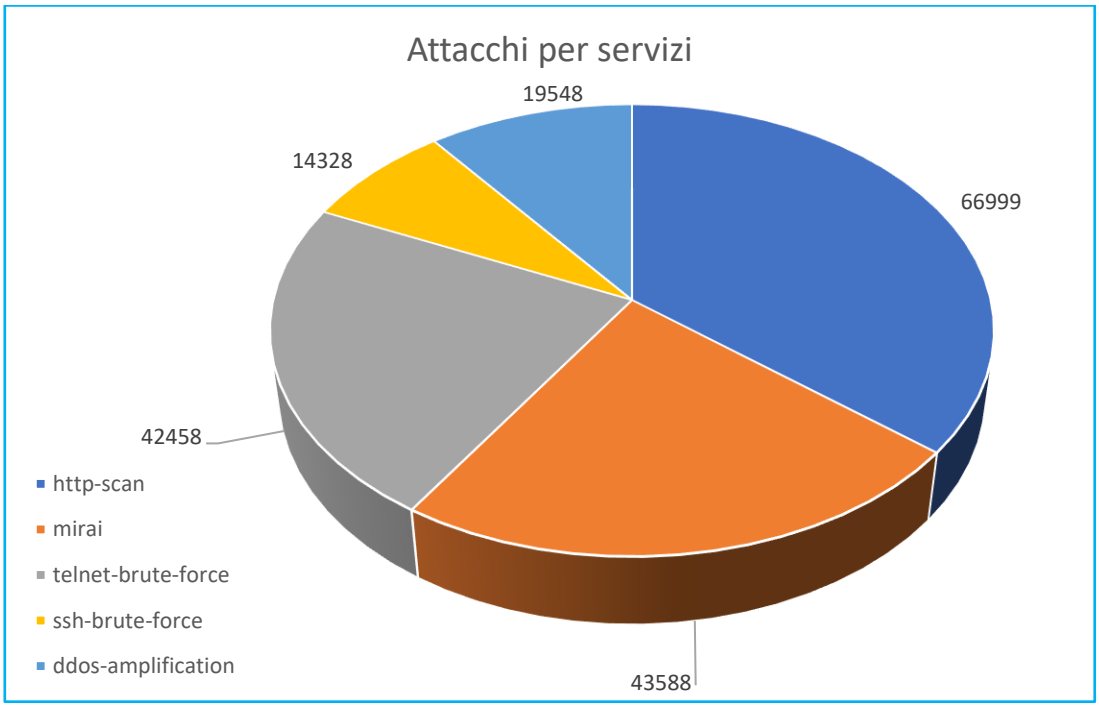


4.4 DDoS rilevati

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:

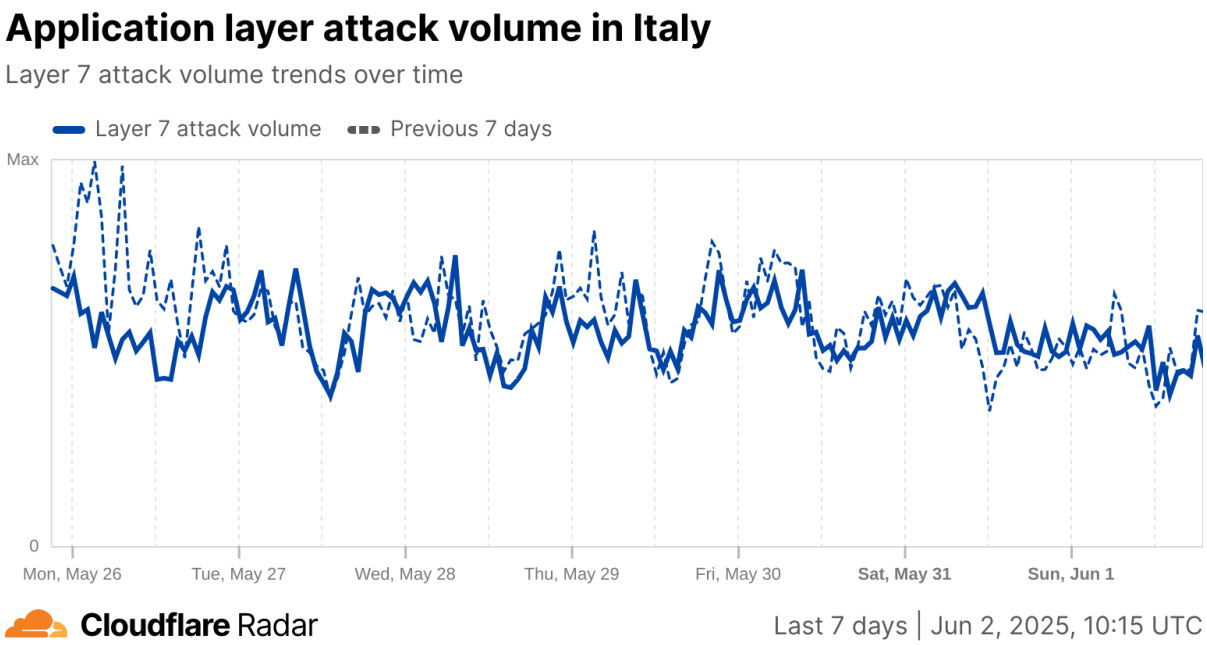


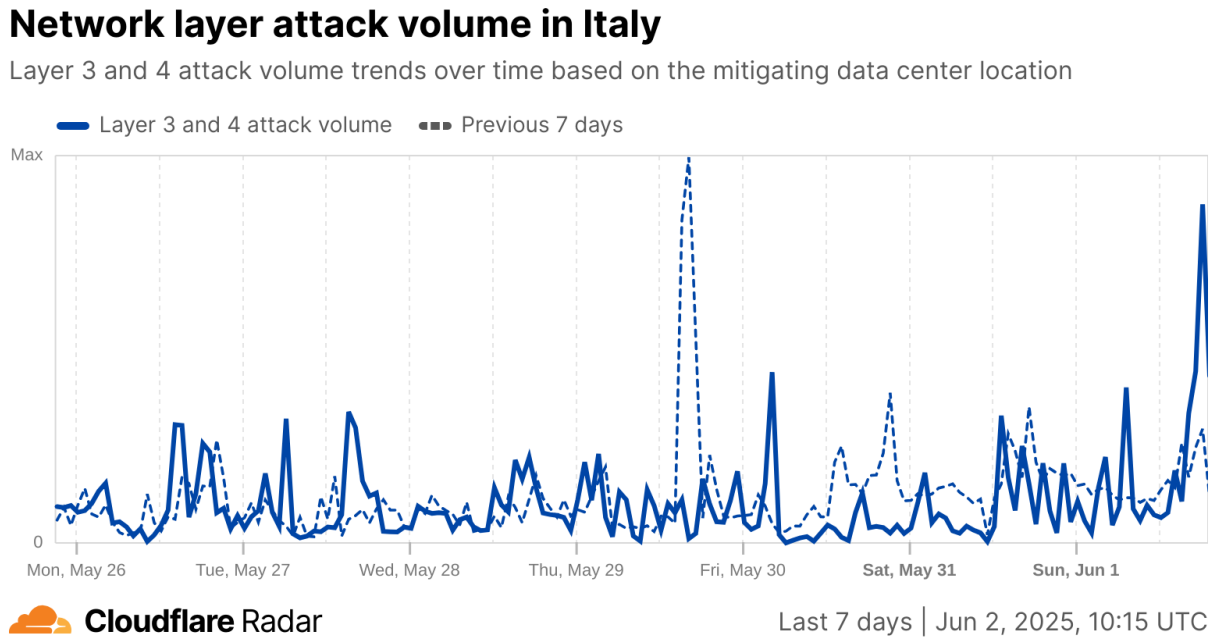
Nel grafico seguente invece la suddivisione degli attacchi per servizi:



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
ADIDAS	STATI UNITI
DESCRIZIONE	Adidas è stata recentemente vittima di un attacco che ha coinvolto i suoi clienti statunitensi. L'incidente è stato scoperto il 26 Maggio 2025, quando un'entità non autorizzata ha dichiarato di aver acquisito informazioni personali da alcuni consumatori che avevano effettuato acquisti sul sito web statunitense dell'azienda. I dati compromessi includono informazioni di contatto, nomi utente e password crittografate. Tuttavia, Adidas ha escluso che siano stati coinvolti dati sensibili come informazioni finanziarie o relative alla salute. L'azienda ha avviato immediatamente un'indagine approfondita in collaborazione con esperti di sicurezza informatica e autorità competenti, e sta notificando direttamente i consumatori potenzialmente interessati. Al momento, non è chiaro quante persone siano state effettivamente colpite dalla violazione .

TARGET	LOCALIZZAZIONE
VICTORIA'S SECRET	STATI UNITI
DESCRIZIONE	Victoria's Secret ha recentemente subito un incidente di sicurezza informatica che ha causato la sospensione temporanea del suo sito web negli Stati Uniti. L'azienda al momento non ha confermato se dati dei clienti o dei dipendenti siano stati compromessi ma alcuni dipendenti hanno segnalato problemi di accesso alla posta elettronica e ritardi nei pagamenti. I negozi fisici sono rimasti operativi, anche se con servizi limitati. L'attacco ha avuto ripercussioni anche a livello finanziario, con un calo del 7% del titolo in borsa.

TARGET	LOCALIZZAZIONE
IP TELECOM GMBH	AUSTRIA
DESCRIZIONE	Il 28 maggio 2025 è stato scoperto un data breach ai danni di IP Telecom GmbH, un'azienda che offre soluzioni personalizzate di comunicazioni prevalentemente in ambito sanitario. L'attacco è stato attribuito al gruppo hacker CiphBit, ma la dimensione esatta della fuga di dati non è stata resa nota. Al momento non risultano dichiarazioni ufficiali o comunicati pubblici da parte di IP Telecom a riguardo.

4.6 Defacement

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

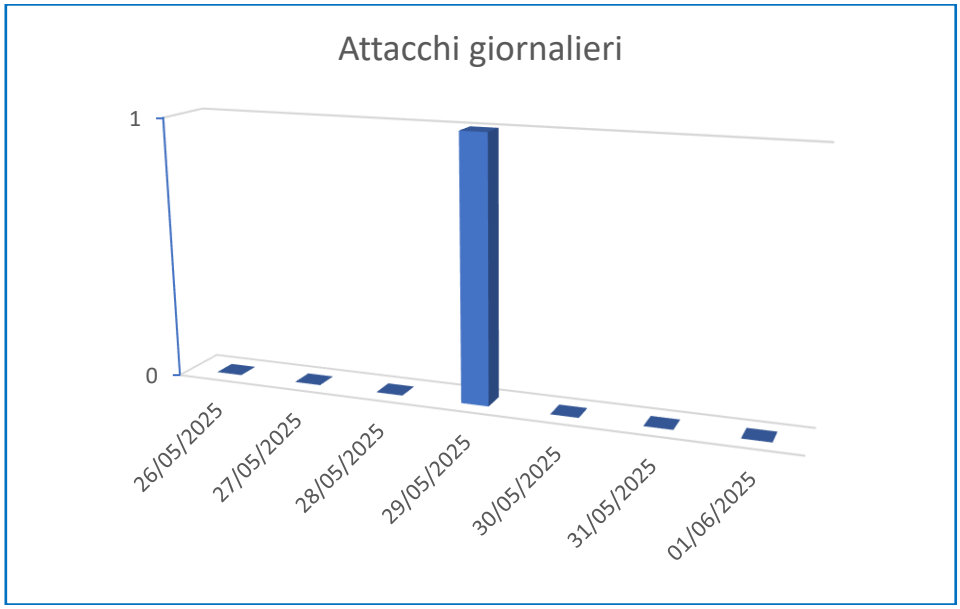


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

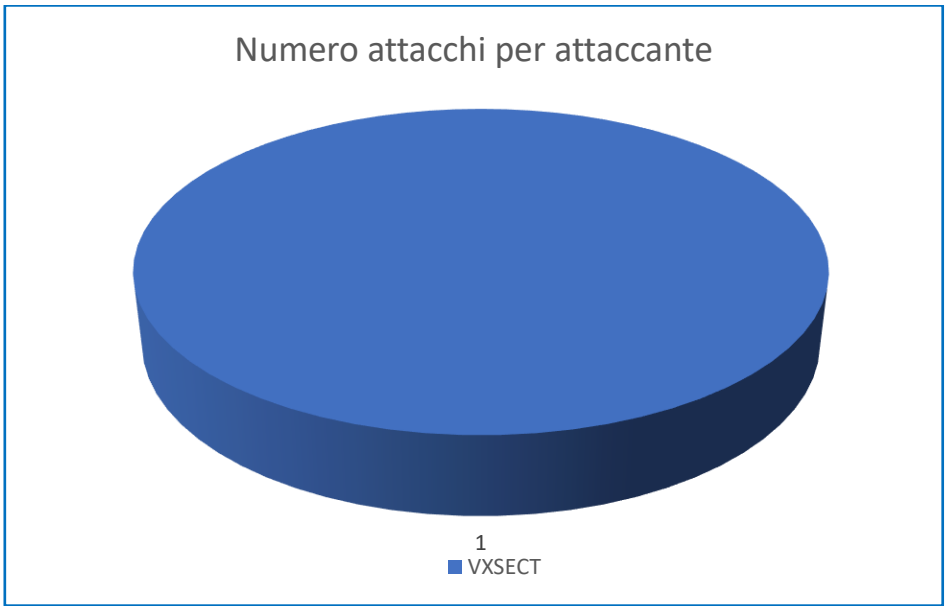


Figura 2: Defacement - Attaccanti più attivi nel periodo 26 Maggio - 1 Giugno 2025

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

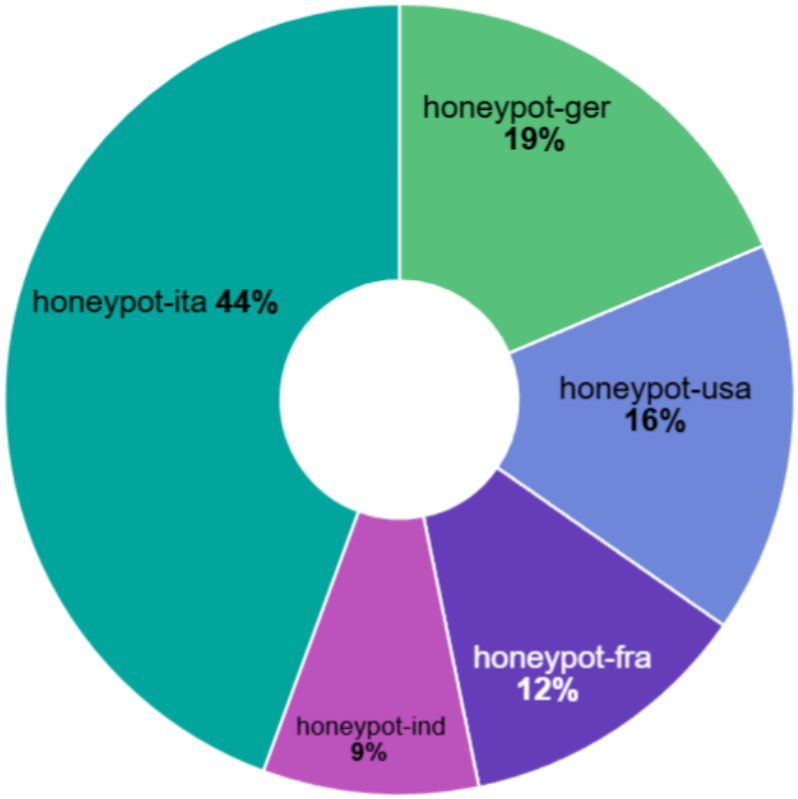
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

1.219.737
Attacks

9.176
Unique Src IPs

61
Unique HASSHs

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



Questa invece la situazione a livello italiano:

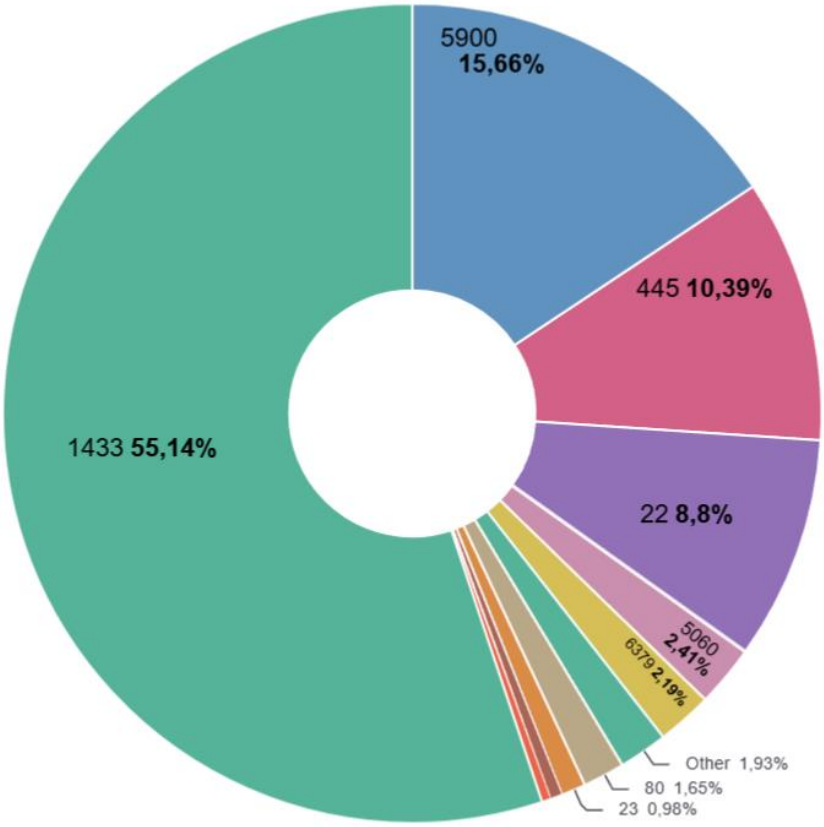
541.498 Attacks

2.771 Unique Src IPs

38 Unique HASSHs

5.1.1 Attacchi ai servizi

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



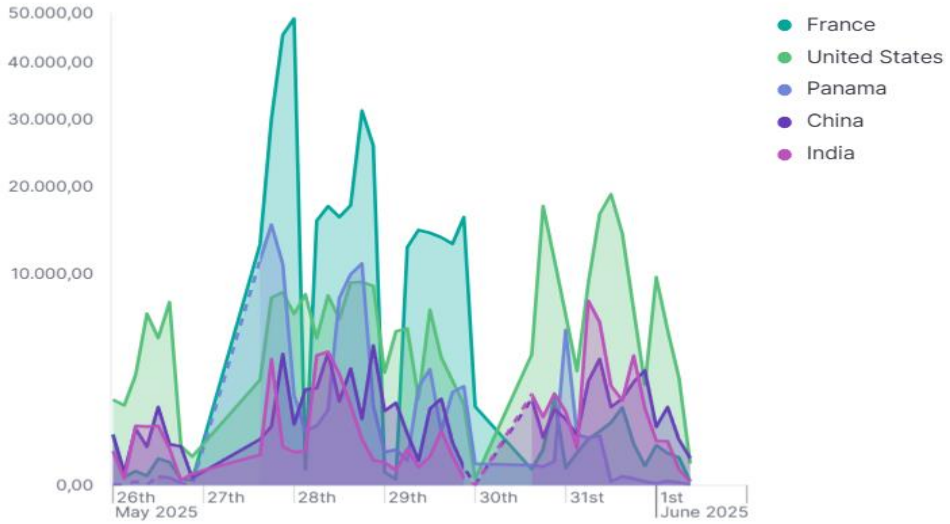
5.1.2 IP Attaccanti

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

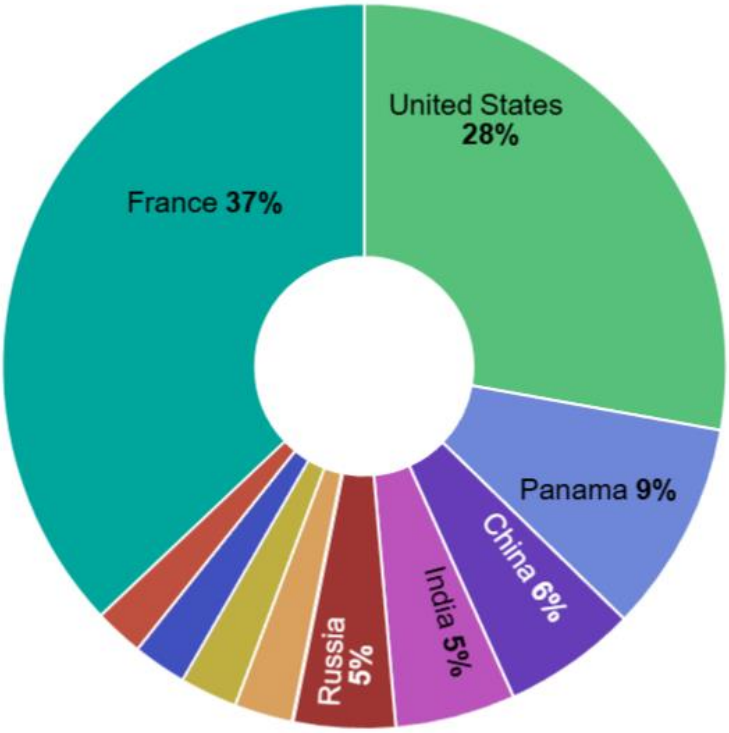
Source IP	Count
62.210.131.174	220.594,00
62.210.125.78	103.854,00
142.202.191.234	50.117,00
142.202.189.5	32.205,00
45.227.253.103	31.301,00
45.227.253.104	31.178,00
45.227.253.102	27.659,00
193.37.69.157	26.446,00
62.210.205.138	21.105,00
47.251.164.177	19.437,00

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:

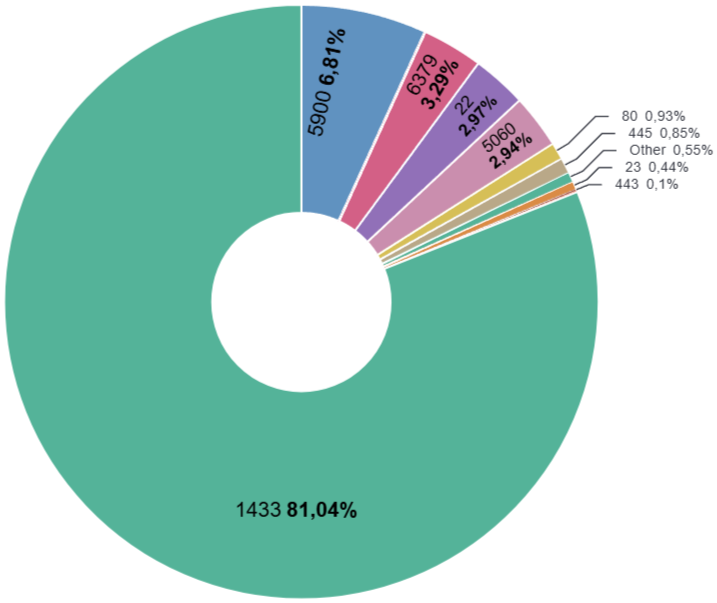


5.2 Italian Honeypot N.1

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
1433	376.945,00
5900	31.657,00
6379	15.322,00
22	13.836,00
5060	13.664,00
80	4.312,00
445	3.970,00
23	2.040,00
443	453,00
5555	370,00

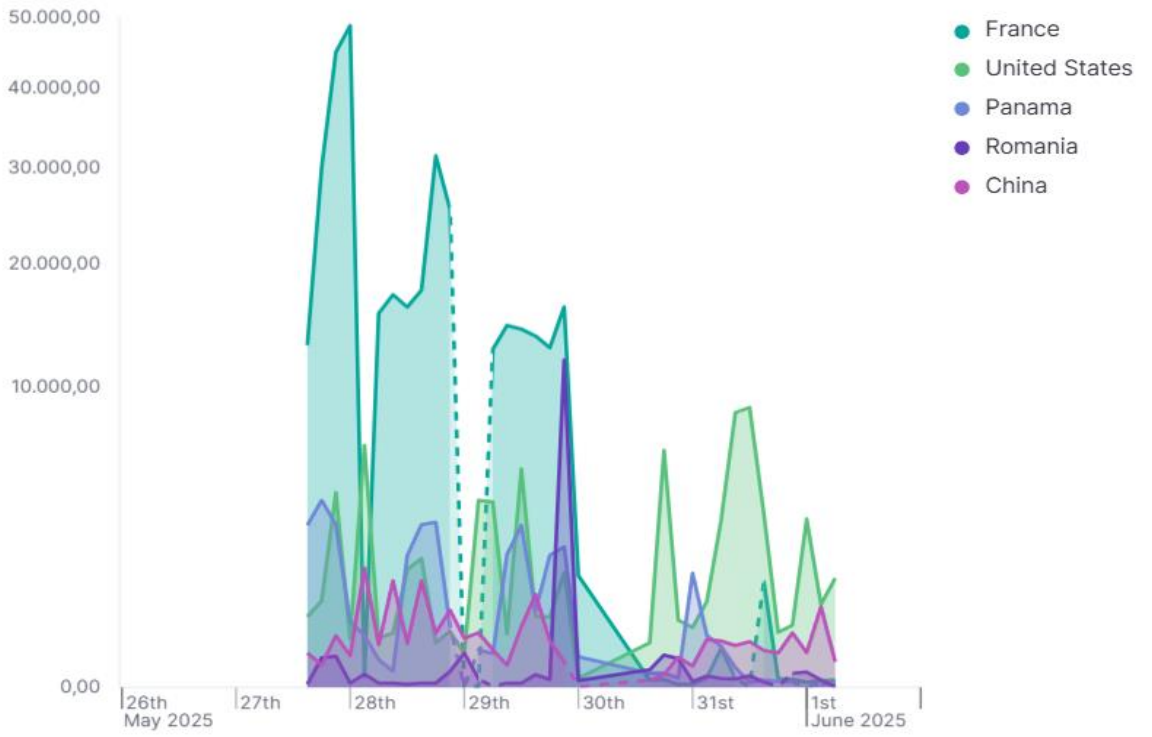
5.2.2 IP Attaccanti

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

Source IP	Count
62.210.131.174	220.594,00
62.210.125.78	103.854,00
62.210.205.138	21.105,00
47.251.164.177	19.437,00
142.202.191.234	15.441,00
193.46.255.217	11.897,00
45.227.253.103	10.933,00
45.227.253.104	10.189,00
45.227.253.102	9.960,00
142.202.189.5	9.340,00

5.2.3 Paesi di provenienza degli attacchi

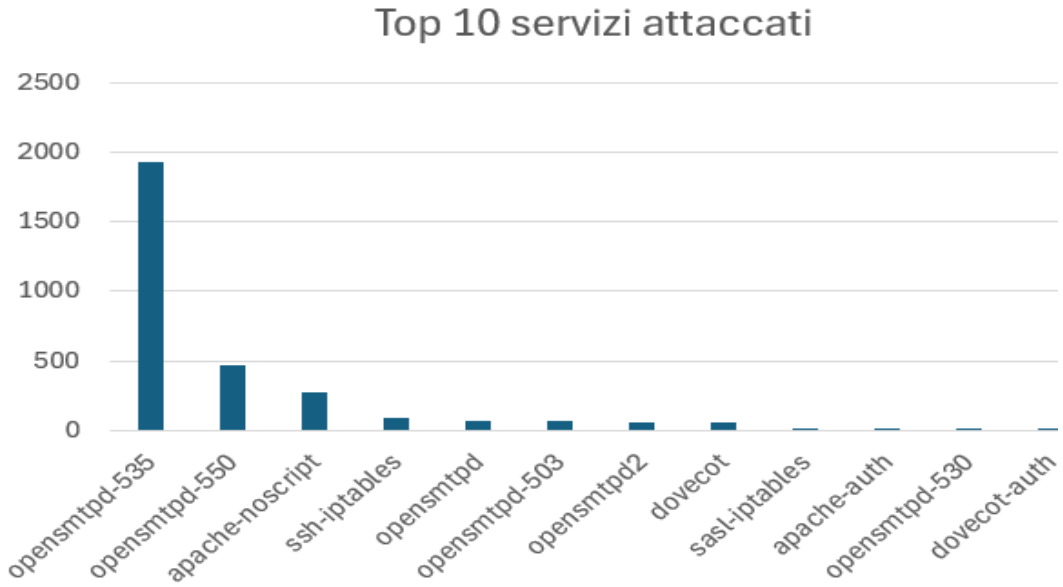
Si riporta l'andamento dei paesi attaccanti che hanno effettuato movimenti malevoli, verso l'Italia.



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.



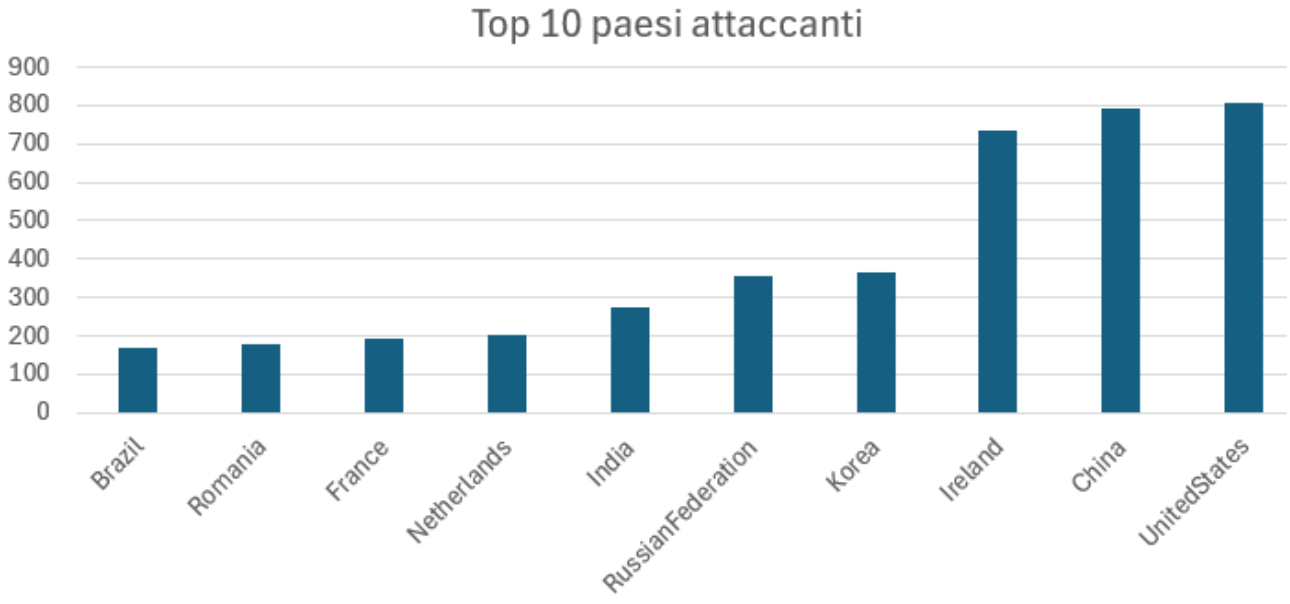
5.3.2 IP attaccanti

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
95[.]111[.]227[.]253	52
5[.]79[.]109[.]115	32
185[.]176[.]220[.]173	22
37[.]48[.]109[.]145	21
176[.]65[.]140[.]163	21
37[.]48[.]73[.]232	19
37[.]48[.]120[.]235	19
62[.]152[.]59[.]17	15
185[.]176[.]220[.]70	15
74[.]48[.]222[.]79	15

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

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

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

Cyber security

RISK REPORT

S3K

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