S3K

Cyber security

RISK REPORT

\ week 22.09.2025 - 28.09.2025

Sommario


CYBER SECURITY RISK REPORT
39/25

1 Il Cyber Security Risk Report S3K

Report settimanale di intelligence sulle minacce informatiche per professionisti della sicurezza e responsabili IT. Analisi approfondita del panorama delle minacce dal 22 al 28 settembre 2025, con focus particolare sul mercato italiano e sulle tendenze globali emergenti.

1.1 Panorama delle Minacce: Settimana Critica per la Sicurezza Informatica

- Alert Critico CVE
  - 26 vulnerabilità critiche pubblicate il 22 settembre, con particolare focus su sistemi Cisco ASA e applicazioni web. Diverse CVE già attivamente sfruttate con exploit pubblici disponibili.
- Campagne Ransomware
  - Intensificazione degli attacchi Akira contro firewall SonicWall e ritorno del gruppo Hive0117 con trojan DarkWatchman. Perdite finanziarie significative nel settore gaming.
- Identità Digitali Compromesse
  - Scoperta la vendita di pacchetti completi di identità digitali italiane sul dark web a 300$ ciascuno, inclusi documenti KYC completi per aggirare i controlli bancari.
- Aggiornamenti di Sicurezza Prioritari
  - **GitLab:** 9 vulnerabilità risolte, 2 ad alta gravità
  - **Cisco IOS/XE:** Zero-day CVE-2025-20352 attivamente sfruttata
  - **Google Chrome:** 3 vulnerabilità ad alta gravità corrette
- Nuove Tecniche di Attacco
  - **File SVG camuffati:** PDF falsi con IA per phishing
  - **Container Docker:** Botnet ShadowV2 su AWS
  - **Gaming malware:** StimBlaster via aggiornamenti falsi
- Impatto Italia
  - Attacchi confermati al Comune di Forlì e SPERI S.p.A., con crescente presenza di identità digitali italiane nei mercati underground. Particolare attenzione richiesta per le infrastrutture critiche.

1.2 Analisi Dettagliata delle Minacce Emergenti

- Vulnerabilità Critiche e Exploit Attivi
  - 26 CVE Critiche

Vulnerabilità pubblicate il 22 settembre, principalmente su sistemi di gestione e applicazioni web

- 18 CVE Con Exploit Pubblici
- SQL injection su sistemi PHP open-source con proof-of-concept disponibili

- CVE Zero-Day Attive
  - Cisco ASA/FTD sotto attacco da gruppi APT cinesi con bootkit persistenti

- Campagne Malware Sofisticate

Malware	Tecnica Principale	Settore Target	Rischio
ShadowV2	Container Docker su AWS	Cloud Infrastructure	Alto
MiniJunk/MiniBrowse	DLL sideloading + firme valide	Europa Occidentale	Alto
StimBlaster/StealC	Aggiornamenti gaming falsi	Gaming/Crypto	Alto
RayInitiator/LINE VIPER	Bootkit firmware Cisco	Network Infrastructure	Critico

1.3 Trend di Attacco del Mercato Underground

L'analisi del dark web rivela una preoccupante commercializzazione delle identità digitali italiane, vendute in pacchetti completi contenenti carte d'identità, passaporti, tessere sanitarie e documenti di supporto per un valore medio di 300 dollari. Questi kit sono progettati specificamente per superare i controlli KYC (Know Your Customer) di banche e servizi finanziari.
"La professionalizzazione del cybercrime ha raggiunto livelli industriali. Non si tratta più di attacchi isolati, ma di un mercato organizzato che tratta i dati personali come merce di scambio." - Analisi S3K Threat Intelligence

1.4 Intelligence Operativa e Raccomandazioni Strategiche

- Priorità Immediate - Patch Management
  Aggiornamento urgente di sistemi Cisco ASA/FTD, applicazioni Campcodes/Fabian, e tutti i sistemi con CVE CVSS ≥ 9.8. Disabilitazione temporanea di plugin WordPress vulnerabili.

- Rafforzamento Controlli KYC

  Implementazione di verifiche biometriche multi-livello, analisi video in tempo reale, e controlli incrociati con database ufficiali per contrastare l'uso di identità digitali compromesse.

- Monitoraggio Avanzato

  Configurazione di regole SIEM per rilevare pattern di SQL injection, monitoring di connessioni verso domini .sbs e servizi cloud, e sorveglianza proattiva del dark web.

- Formazione e Awareness

  Training intensivo su riconoscimento phishing con IA, sensibilizzazione su allegati SVG camuffati, e procedure di verifica per aggiornamenti software non ufficiali.

- Indicatori di Compromissione Critici
  - Domini e URL Sospetti
    - *.azurewebsites.net (campagne Nimbus Manticore)
    - klant-bezoeknummer833893.sbs (phishing SumUp)
    - rcl.ink/* (shortener abusato)
    - shadow.aurozacloud.xyz (C2 ShadowV2)
  - IP sotto Monitoraggio
    - 46.203.233.114 (FREAKHOSTING abusato)
    - 23.97.62.139/136 (infrastruttura ShadowV2)
    - 203.188.171.156 (C2 StimBlaster)
    - 45.83.28.99 (botnet infrastructure)

1.5 Trend Crescenti negli Attacchi Informatici

- 68% Incremento attacchi Phishing
- Aumento degli attacchi di ingegneria sociale con tecniche IA per eludere i filtri tradizionali
- 42% Ransomware Evolution
- Crescita di attacchi mirati a infrastrutture critiche con tecniche di doppia estorsione
- 23% Zero-Day Exploitation
- Riduzione dei tempi tra disclosure e sfruttamento attivo delle vulnerabilità critiche

Azioni suggerite: Implementazione immediata delle contromisure raccomandate e attivazione di procedure di incident response per tutti i sistemi identificati come a rischio. Particolare attenzione agli ambienti cloud e ai servizi esposti pubblicamente.

1.6 Bollettino di Sicurezza Informatica

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

1.7 Aggiornamenti di Sicurezza e Vulnerabilità Critiche

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

  Correzione urgente per 4 vulnerabilità critiche, inclusa CVE-2025-10585 zero-day che consente attacchi tramite pagine web malevole. Aggiornamento alla versione 140.0.7339.185/.186.
- Greenshot
  Vulnerabilità ad alta gravità nell'applicativo di cattura schermo che permetterebbe l'esecuzione di codice arbitrario. Aggiornamento necessario alla versione 1.3.300 o superiore.

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

1.8 CVE Monitor - Tendenze Settimanali

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

1.9 Analisi degli Attacchi: Phishing, Ransomware e Malware

- Situazione Phishing in Italia

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

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

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

1.10 Attività Ransomware

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

1.11 Malware Emergenti

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

1.12 Raccomandazioni e Misure di Protezione

- Patch Management Prioritario

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

- Protezione dei Backup

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

- Formazione e Awareness

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

- Monitoring e Detection

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

- Segmentazione di Rete

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

- Threat Intelligence

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

1.13 Outlook delle Minacce

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

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

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE
GitLab	Rilasciati aggiornamenti di sicurezza che risolvono 9 vulnerabilità, di cui due con gravità "alta", in GitLab Community Edition (CE) ed Enterprise Edition (EE). Prodotti e/o versioni affette GitLab Community Edition (CE) ed Enterprise Edition (EE) • tutte le versioni precedenti alla 18.2.7 • 18.3.x, versioni precedenti alla 18.3.3 • 18.4.x, versioni precedenti alla 18.4.1
ULR/Note	https://about.gitlab.com/releases/2025/09/25/patch-release-gitlab-18-4-1-released/

PRODOTTO	DESCRIZIONE
Cisco	Aggiornamenti di sicurezza Cisco risolvono diverse vulnerabilità, di cui 8 con gravità "alta" e una zero-day attivamente sfruttata in rete. In particolare, è stato rilevato lo sfruttamento attivo della vulnerabilità zero-day, identificata come CVE-2025-20352 e con gravità "alta", presente nei software Cisco IOS e IOS XE. Tale vulnerabilità consentirebbe a un attaccante remoto autenticato di compromettere la disponibilità del servizio e/o di eseguire codice arbitrario sul sistema interessato. **Prodotti e/o versioni affette** • 1000 Series Integrated Services Routers • 1100 Terminal Services Gateways • 4000 Series Integrated Services Routers • 8100 Series Secure Routers • 8400 Series Secure Routers • ASR 1000 Series Aggregation Services Routers • C8375-E-G2 Platforms • Catalyst IE3300 Rugged Series Routers • Catalyst IR1100 Rugged Series Routers

	• Catalyst IR8100 Heavy Duty Series Routers • Catalyst IR8300 Rugged Series Routers • Catalyst 8200 Series Edge Platforms • Catalyst 8300 Series Edge Platforms • Catalyst 8500L Edge Platforms • Catalyst 9200 Series Switches • Embedded Services 3300 Series • VG410 Analog Voice Gateways • 1100 Integrated Services Routers • 4000 Series Integrated Services Routers • ASR 920 Series Aggregation Services Routers • ASR 1000 Series Aggregation Services Routers • Catalyst 1101 Rugged Routers • Catalyst 8000V Edge Software • Catalyst 8200 Series Edge Platforms • Catalyst 8300 Series Edge Platforms • Catalyst 8500 Edge Platforms • Catalyst 8500L Edge Platforms • Catalyst IR8300 Rugged Series Routers • Cisco IOS Software • Cisco IOS XE Software • Catalyst 9200 Series Switches • Catalyst 9300 Series Switches • Catalyst 9400 Series Switches • Catalyst 9500 Series Switches • Catalyst 9600 Series Switches • Cisco Industrial Ethernet (IE) Series Switches: • IE 2000 Series • IE 3010 Series • IE 4000 Series • IE 4010 Series • IE 5000 Series
ULR/Note	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmpwred-x3MJyf5M https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secboot-UqFD8AvC https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nbar-dos-LAvwTmeT https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-tacacs-hdB7thJw

	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-invalid-url-dos-Nvxszf6u https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cat9k-PtmD7bgy https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

PRODOTTO	DESCRIZIONE
Google Chrome	Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere 3 vulnerabilità di sicurezza con gravità "alta". Tali vulnerabilità, qualora sfruttate, potrebbero consentire a un utente malintenzionato remoto di accedere a informazioni sensibili e/o di eseguire codice arbitrario sui sistemi target. Prodotti e/o versioni affette • versioni precedenti alla 140.0.7339.207/.208 per Windows e Mac • versioni precedenti alla 140.0.7339.207 per Linux
ULR/Note	https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_23.html

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

RANSOMWARE AKIRA: CAMPAGNA MIRATA AI FIREWALL SONICWALL

Il ransomware Akira ha avuto una crescita significativa nelle ultime settimane, distinguendosi per una campagna che ha preso di mira in modo diretto i firewall SonicWall. Le indagini condotte dai ricercatori di Arctic Wolf Labs hanno mostrato un quadro particolarmente critico: gli aggressori sono riusciti a sfruttare le VPN SSL, compromettendo credenziali già utilizzate in precedenza, e in diversi casi hanno persino eluso i meccanismi di autenticazione multifattore. Questo aspetto rappresenta una delle variabili più preoccupanti, perché dimostra che anche sistemi considerati "a prova di intrusione" possono in realtà essere sfruttati attraverso vecchie credenziali non modificate.

Uno degli elementi tecnici centrali della campagna è la vulnerabilità CVE-2024-40766, legata a un difetto nei controlli di accesso. Questo problema, già noto alla comunità di sicurezza, è stato sfruttato in maniera mirata per aggirare barriere critiche di sicurezza e aprire la strada alle fasi successive dell'attacco. Una volta penetrati all'interno della rete, gli operatori di Akira hanno messo in atto procedure standardizzate ma estremamente rapide: mappatura della rete, creazione di nuovi account amministrativi, distribuzione di software di accesso remoto come AnyDesk, TeamViewer e RustDesk, e disattivazione mirata delle difese, comprese soluzioni EDR e Windows Defender.

Il processo culmina con la doppia estorsione: prima vengono esfiltrati i dati più sensibili, compressi e inviati all'esterno con strumenti come Rclone o WinRAR, poi i sistemi vengono crittografati, paralizzando le operazioni aziendali. Questo duplice approccio lascia le vittime di fronte a un ricatto particolarmente difficile da gestire, con il rischio concreto di subire danni sia operativi sia reputazionali.

Il messaggio è chiaro: non è sufficiente applicare le patch di sicurezza, perché se le credenziali già compromesse non vengono invalidate, il rischio rimane concreto. Per ridurre l'impatto di queste minacce è indispensabile reimpostare tutte le credenziali VPN e Active Directory, rafforzare le policy di autenticazione multifattore, introdurre sistemi di monitoraggio continuo delle connessioni in uscita e valutare l'adozione di soluzioni di intrusion detection che permettano di reagire in tempi rapidi a segnali di compromissione.

RITORNO DEL GRUPPO HIVE0117: EMAIL DANNOSE E TROJAN DARKWATCHMAN

Il gruppo criminale Hive0117 ha ripreso le proprie attività con una campagna di phishing su larga scala che ha destato particolare preoccupazione nella comunità di sicurezza. Dopo un periodo di silenzio, il collettivo ha infatti avviato una nuova operazione a partire dal 24 settembre, indirizzando email fraudolente verso un ampio spettro di obiettivi nei territori di Russia e Kazakistan. Tra i settori coinvolti figurano banche, telecomunicazioni, aziende manifatturiere, società IT, logistica, assicurazioni e istituti di ricerca scientifica, segno che l'obiettivo è colpire infrastrutture critiche e servizi fondamentali.

Le email impiegate nella campagna si presentano con un livello di sofisticazione elevato. I messaggi simulano comunicazioni ufficiali, provenienti da enti governativi o istituzioni legali, e utilizzano indirizzi di mittenti apparentemente legittimi. Gli attaccanti hanno fatto ricorso a una tecnica peculiare: inviare messaggi in cui il mittente e il destinatario coincidono, nascondendo in copia nascosta (CCN) gli indirizzi reali delle vittime. Inoltre, i domini creati ad hoc, come *4ad74aab.cfd* o *4ad74aab.xyz*, hanno rafforzato l'illusione di autenticità, offrendo alle vittime link a documenti e contenuti che in realtà contenevano codice malevolo.

Il payload principale distribuito è DarkWatchman, un trojan modulare già utilizzato in passato dal gruppo. Una volta eseguito, DarkWatchman permette movimenti laterali nella rete, esfiltrazione di dati e mantenimento della persistenza, diventando un trampolino di lancio per operazioni più gravi, come il ransomware o lo spionaggio industriale.

Questa campagna dimostra ancora una volta la centralità del phishing come vettore di attacco: nonostante l'evoluzione delle difese, l'ingegneria sociale resta la strategia più redditizia per i criminali, soprattutto quando viene accompagnata da tecniche avanzate di distribuzione e da domini apparentemente affidabili. Le aziende devono quindi investire in formazione continua del personale, rafforzare i sistemi di filtraggio della posta elettronica, verificare attentamente i domini di invio e implementare controlli comportamentali che consentano di individuare anomalie nelle connessioni e nelle attività interne.

FILE SVG CAMUFFATO DA PDF: PHISHING CON INTELLIGENZA ARTIFICIALE

Microsoft Threat Intelligence ha segnalato una campagna particolarmente insidiosa che sfrutta allegati mascherati e l'intelligenza artificiale per superare le difese tradizionali. Gli attaccanti hanno inviato email che contenevano documenti apparentemente in formato PDF, ma che in realtà erano file SVG con codice JavaScript malevolo nascosto al loro interno.

Il livello di sofisticazione dell'attacco è dato dall'uso di modelli di linguaggio AI per offuscare il codice e allo stesso tempo renderlo più plausibile. Nei file analizzati sono stati trovati riferimenti a dashboard aziendali, indicatori di performance e terminologia manageriale, tutti elementi inseriti con l'intento di convincere l'utente che si trattasse di documenti legittimi. L'allegato, una volta aperto, reindirizzava l'utente a una pagina CAPTCHA contraffatta e successivamente a un portale di login fasullo, progettato per sottrarre credenziali aziendali.

L'uso dell'intelligenza artificiale in questo contesto rappresenta un'evoluzione pericolosa, perché consente di creare contenuti personalizzati, realistici e meno sospetti, aumentando le probabilità di successo. Tuttavia, nonostante l'ingegno degli aggressori, Microsoft Defender è stato in grado di identificare la minaccia grazie all'analisi comportamentale: il formato SVG è insolito come allegato, i redirect a domini sospetti erano già stati osservati in precedenti campagne e il codice di scripting presentava pattern tipici di attività fraudolente.

Questo caso sottolinea come l'IA non renda invisibili gli attacchi, ma anzi possa lasciare tracce riconoscibili. Per mitigare i rischi, è necessario potenziare i sistemi antiphishing, limitare l'apertura di allegati non convenzionali, adottare metodi di autenticazione multifattore più robusti e sensibilizzare gli utenti a riconoscere segnali di allarme come formati inusuali o comportamenti sospetti degli allegati ricevuti.

IDENTITÀ DIGITALI ITALIANE IN VENDITA SUL DARK WEB

Negli ultimi mesi è emersa una tendenza estremamente allarmante che riguarda direttamente il panorama italiano della sicurezza digitale: la vendita di pacchetti completi di identità digitali italiane sui mercati neri del dark web. Questi pacchetti, commercializzati in forum underground frequentati da criminali informatici, vengono offerti a un prezzo medio di circa 300 dollari ciascuno. Una cifra apparentemente contenuta, che rende queste identità alla portata di chiunque voglia compiere frodi o attività illecite.

Il contenuto dei pacchetti è particolarmente ricco. Non si tratta di semplici scansioni di documenti, ma di veri e propri kit pensati per superare i controlli di verifica digitale (KYC – Know Your Customer). Tra i materiali offerti si trovano copie di carte d'identità, passaporti e tessere sanitarie, accompagnati da documenti aggiuntivi come bollette di utenze domestiche, certificati di residenza e in alcuni casi persino fotografie personali o prove biometriche. L'obiettivo è rendere il pacchetto credibile e completo, in modo da consentire ai criminali di bypassare i controlli più comuni applicati da banche, piattaforme di trading e servizi finanziari.

Le applicazioni di questi dati sono molteplici e potenzialmente devastanti. Con un'identità digitale acquisita illegalmente, i criminali possono aprire conti correnti o carte prepagate, registrarsi a servizi di e-commerce, condurre operazioni di riciclaggio di denaro, accedere a piattaforme di scambio di criptovalute o ottenere finanziamenti in modo fraudolento. Le conseguenze per le vittime sono gravissime: oltre al danno economico e reputazionale, rischiano di trovarsi coinvolte in indagini giudiziarie per attività a cui non hanno mai preso parte, con un impatto psicologico e legale difficile da gestire. Il fatto che queste identità vengano vendute in blocco indica anche che i criminali non si limitano a colpire singoli individui, ma cercano di costruire veri e propri archivi di identità pronte all'uso, da rivendere o riutilizzare in diverse operazioni illecite. Ciò riflette la crescente professionalizzazione del cybercrime: non più azioni isolate, ma un mercato organizzato che tratta i dati personali come una merce di scambio.

Per le aziende che gestiscono procedure KYC, questa minaccia rappresenta una sfida enorme. Limitarsi a verificare documenti digitalizzati non è più sufficiente, perché copie ben realizzate o pacchetti assemblati con cura possono facilmente superare i controlli tradizionali. È necessario adottare controlli multilivello, che comprendano verifiche biometriche, analisi video in tempo reale, sistemi di reverse image search per individuare immagini riciclate e controlli incrociati con database ufficiali. Inoltre, diventa fondamentale la sorveglianza costante del dark web, che consente di identificare in anticipo fughe di dati e di agire prima che vengano sfruttate per scopi criminali.

Questo fenomeno mette in evidenza come la protezione delle identità digitali non sia più solo una responsabilità individuale, ma un tema di sicurezza nazionale e aziendale. Ogni fuga di dati personali, ogni archivio compromesso o ogni sistema di autenticazione debole alimenta un mercato che sta diventando sempre più redditizio per la criminalità organizzata. La lezione che si può trarre è chiara: per contrastare la vendita di identità digitali è necessario un approccio globale, che combini tecnologie avanzate, strategie di prevenzione e una maggiore consapevolezza sia da parte delle istituzioni sia da parte dei cittadini. Solo così sarà possibile limitare i danni e ridurre l'attrattiva di questo mercato nero sempre più pericoloso.

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 22 – 28 Settembre 2025

Settimana caratterizzata da un picco molto alto di vulnerabilità critiche il 22 settembre (26 CVE) con advisories di Campcodes, Fabian, AngelJudeSuarez, Mayurik, che hanno impattato soprattutto applicazioni web, sistemi di management e e-learning.

Oltre a questi, continuano a emergere SQLi su applicativi open-source PHP (Campcodes, Fabian, AngelJudeSuarez) e vulnerabilità gravi su WordPress plugin e temi.

La presenza di PoC pubblici per varie SQL injection rende l'impatto immediato.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE	Data Pubblicazione	Severità	Exploit	Descrizione Sintetica	Prodotto Coinvolto
CVE-2025-9588	23/09/2025	CRITICAL (10.0)	❌	Neutralizzazione impropria elementi speciali	Generic Web Application
CVE-2025-9846	23/09/2025	CRITICAL (10.0)	❌	Unrestricted Upload File with Dangerous	Generic Web Application
CVE-2025-10779	22/09/2025	CRITICAL (9.8)	✅	Buffer overflow con esecuzione codice remoto	Dlink Dcs-935L Firmware
CVE-2025-10781	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Campcodes Online Learning Management System
CVE-2025-10782	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Campcodes Online Learning

					Management System
CVE-2025-10783	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Campcodes Online Learning Management System
CVE-2025-10784	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Campcodes Online Learning Management System
CVE-2025-10785	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su database applicazione	Campcodes Grocery Sales And Inventory System
CVE-2025-10786	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su database applicazione	Campcodes Grocery Sales And Inventory System
CVE-2025-10788	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su database applicazione	Fabian Online Hotel Reservation System
CVE-2025-10789	22/09/2025	CRITICAL (9.8)	❌	SQL Injection su database applicazione	Fabian Online Hotel Reservation System
CVE-2025-10791	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Fabian Online Bidding System
CVE-2025-10793	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Fabianros E-Commerce Website

CVE-2025-10795	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Fabian Online Bidding System
CVE-2025-10796	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Angeljudesu arez Hostel Managemen t System
CVE-2025-10797	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su database applicazione	Angeljudesu arez Hostel Managemen t System
CVE-2025-10798	22/09/2025	CRITICAL (9.8)	✅	SQL Injection su pannello amministrativo	Angeljudesu arez Hostel Managemen t System
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.					

Distribuzione Giornaliera

- **22 settembre 2025** → giornata con il maggior numero di advisory:
  - **Campcodes Systems** (deserialization, file upload, privilege escalation)
  - **AngelJudeSuarez Hostel Management** (buffer overflow, esposizione condivisioni)
  - **Fabian Hotel Systems** (path traversal → RCE critico)
  - **Web Applications e E-learning & HPC Pack** (SMB relay e deserialization RCE)
  - Diversi CMS open-source con SQLi già corredati di exploit pubblici
- **24 settembre 2025** → nuove disclosure per Management Systems Connector e Database Applications v1.2 (SQLi multiple).

Vendor e Tecnologie Coinvolti

- **SAP** → NetWeaver AS Java, IBM i-series → RCE e escalation di privilegi.
- **Siemens** → SIMATIC PCS neo, SIVaaS → vulnerabilità ICS ad alto rischio.
- **Microsoft** → HPC Pack, Windows 10/11/Server (SMB relay, deserialization).
- **Adobe** → ColdFusion (2021–2025), path traversal con exploit probabile.

- **WordPress** → BeyondCart Connector e Goza Charity Theme → escalation e file deletion.
- **PHPGurukul / Student Information Mgmt / CRM** → SQL injection diffuse con PoC pubblici.

Raccomandazioni Operative

Patch Prioritarie

- **Campcodes, Fabian, AngelJudeSuarez** → aggiornare immediatamente, soprattutto applicazioni con CVSS ≥ 9.8.
- **WordPress e temi vulnerabili** → disabilitare plugin/temi finché non disponibili patch.
- **Applicativi PHP open-source (Campcodes, Management Systems, E-learning platforms)** → alto rischio di exploit immediato, patch/rimozione consigliata.

Mitigazioni e Monitoraggio

- **Database** → monitorare query anomale verso tabelle users, login, profile.
- **Web server** → WAF con regole anti-SQLi e traversal.
- **ICS/ERP** → segmentazione rete, accessi minimi, audit di sicurezza post-patch.
- **SIEM** → correlazioni su login.php, wp-config.php, profile.php, richieste verso ColdFusion.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2024-36401	GeoServer	9.8
CVE-2025-20362	Cisco Secure Firewall Adaptive Security Appliance (ASA) Software and Cisco Secure Firewall Threat Defense (FTD) Software	6.5
CVE-2025-24085	Apple visionOS 2.3, iOS 18.3, iPadOS 18.3, macOS Sequoia 15.3, watchOS 11.3, and tvOS 18.3	7.9
CVE-2025-43300	Apple macOS Sonoma 14.7.8, macOS Ventura 13.7.8, iPadOS 17.7.10, macOS Sequoia 15.6.1, iOS 18.6.2, and iPadOS 18.6.2	8.8
CVE-2025-55177	WhatsApp for iOS before version 2.25.21.73, WhatsApp Business for iOS version 2.25.21.78, and WhatsApp for Mac version 2.25.21.78	5.4

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-2025-9846	Inka.Net (TalentSys Consulting)	N/A
VULNERABILITÀ	Caricamento non ristretto di file con vulnerabilità di tipo Dangerous Type in TalentSys Consulting Information Technology Industry Inc. Inka.Net consente un attacco di upload pericoloso, con possibilità di command injection. Il problema interessa Inka.Net prima della versione 6.7.1.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-8868	Progress Chef Automate	N/A
VULNERABILITÀ	In Progress Chef Automate, versioni precedenti alla 4.13.295 su Linux x86, un attaccante autenticato può accedere alle funzionalità del servizio compliance tramite input non neutralizzato in un comando SQL, usando un token noto.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-20333	Cisco Secure Firewall ASA/FTD	N/A
VULNERABILITÀ	Una vulnerabilità nel web server VPN di Cisco Secure Firewall Adaptive Security Appliance (ASA) e Threat Defense (FTD) consente a un utente remoto autenticato di eseguire codice arbitrario sul dispositivo, sfruttando una validazione impropria dell'input in richieste HTTP(S). Un exploit riuscito può portare al completo compromesso del dispositivo.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-11126	Apeman ID71	N/A
VULNERABILITÀ	Una falla di sicurezza è stata individuata in Apeman ID71. La manipolazione dei file di configurazione porta a credenziali codificate. L'attacco può essere sfruttato da remoto ed è stato divulgato pubblicamente.	

3.4 CVE attualmente utilizzate in attacchi

In questo paragrafo evidenziamo le principali CVE attivamente utilizzate e sfruttate dagli attaccanti con una breve descrizione.

CVE	CVE-2025-20333
DESCRIZIONE	
Si tratta di una vulnerabilità nel server web VPN di Cisco Secure Firewall ASA e FTD che, a causa di una mancata validazione degli input nelle richieste HTTP(S), può permettere a un attaccante remoto autenticato di eseguire codice arbitrario come root. Lo sfruttamento, possibile tramite credenziali VPN valide e richieste HTTP appositamente create, può portare alla compromissione completa del dispositivo.	

CVE	CVE-2025-20362
DESCRIZIONE	
Una vulnerabilità nel server web VPN di Cisco ASA e FTD consente a un attaccante remoto non autenticato di accedere a endpoint URL riservati della VPN. Il problema deriva da una validazione impropria degli input nelle richieste HTTP(S) e può essere sfruttato inviando richieste appositamente forgiate per bypassare l'autenticazione.	

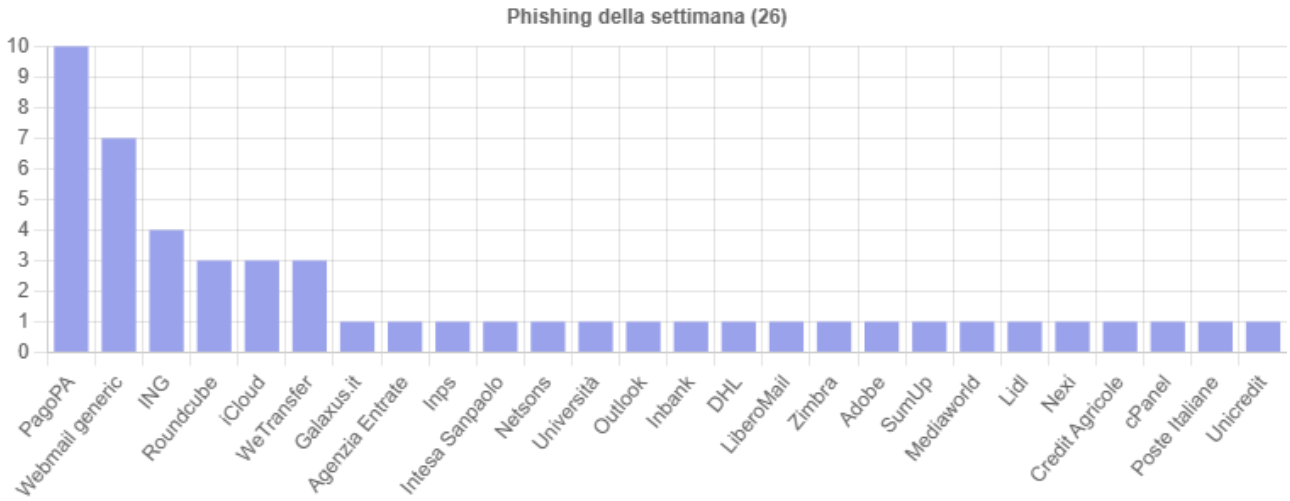
CVE	CVE-2025-10585
DESCRIZIONE	
Una vulnerabilità di type confusion nel motore V8 di Google Chrome, prima della versione 140.0.7339.185, poteva consentire a un attaccante remoto di sfruttare una corruzione della memoria heap tramite una pagina HTML appositamente creata. La gravità è classificata come alta.	

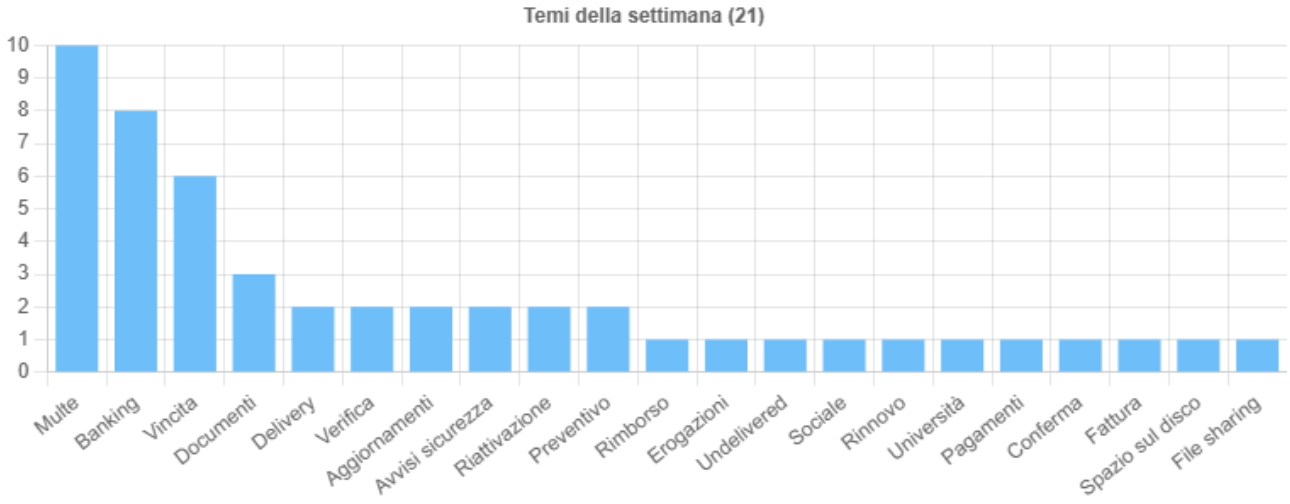
4 Attacchi

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.

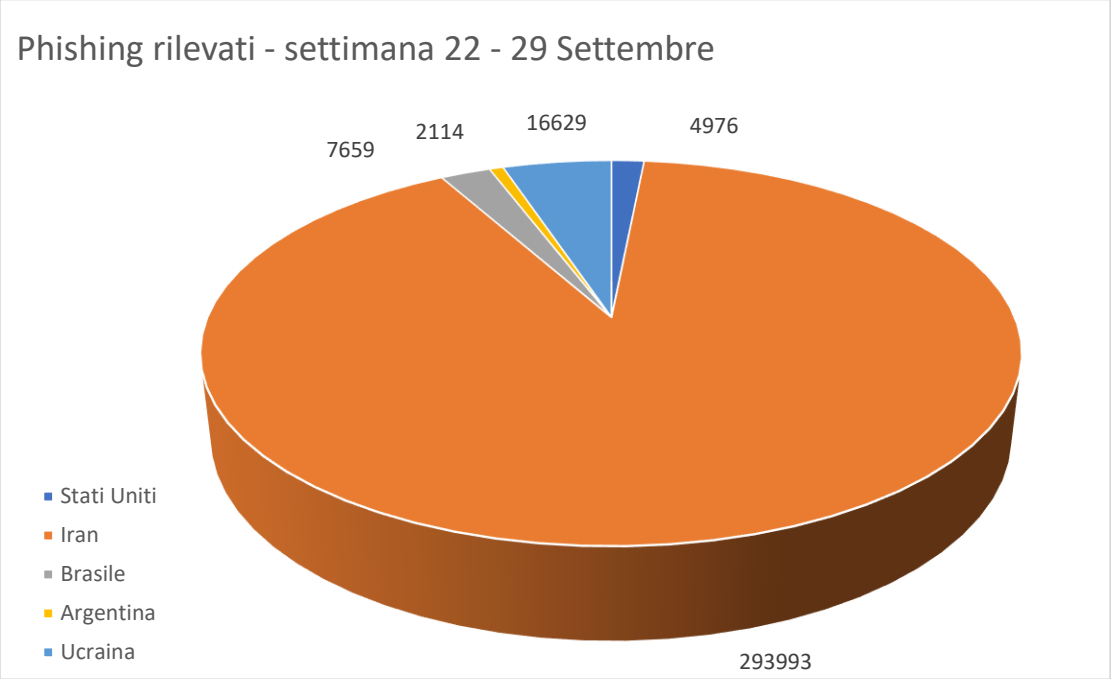




Fonte :CERT-AGID

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.



Riportiamo qui di seguito il consueto report di analisi CTI relativo ad una email di phishing

- Contesto e sintesi narrativa

  L'email oggetto di analisi riporta come mittente SumUp <noreply@sumup[.]it> e ha per oggetto "Tentativo di accesso sospetto rilevato". È stata recapitata a victim@victim[.]com il 17/09/2025 15:50 (Europe/Rome). Il contenuto comunica presunti "tentativi di accesso ripetuti" da un iPhone non registrato, localizzati a Den Haag (Paesi Bassi), con un "Indirizzo IP: 217[.]68[.]63[.]255". Il messaggio invita a "verificare" cliccando un pulsante "Clicca qui" che punta a un link accorciato rcl[.]ink/lQXPc e, nel corpo, suggerisce di "accedere a **www.sumup[.]com**" ma il link reale rimanda a un dominio .sbs: https://klant-bezoeknummer833893[.]sbs/account/.La struttura, la narrativa di safety warning, l'uso di URL shortener e di un dominio terzo non collegato a SumUp sono indicatori tipici di brand impersonation e di phishing per furto credenziali.

- Evidenze principali dall'header

  Dalle intestazioni disponibili:

  - Catena Received: l'host dichiara provenienza da sumup[.]it con sorgente 46[.]203[.]233[.]114. Il blocco IP 46[.]203[.]233[.]0/24 risulta assegnato ad

AS215703 – "FREAKHOSTING" (RIPE), con country indicata DE. Questo profilo è compatibile con hosting low-cost/VPS, frequentemente abusati per invii malevoli, e disallineato rispetto all'infrastruttura attesa per un mittente enterprise come SumUp.

- SPF/DKIM/DMARC: nel frammento di header disponibile non sono presenti linee Authentication-Results né record di allineamento SPF/DKIM/DMARC; non si possono quindi attestare firme o allineamenti. L'assenza nei metadati visionati, unita alla catena Received anomala, aumenta il sospetto di spoofing (o invio tramite infrastruttura compromessa/abuso VPS).

- Analisi contenuto e tecniche di social engineering

  Il messaggio applica la tecnica "security alert / account at risk" con urgenza implicita (ripetuti tentativi di accesso, device sconosciuto) e mismatch tra testo e hyperlink: testuale "www.sumup[.]com" ma click effettivo su klant-bezoeknummer833893[.]sbs e/o rcl[.]ink/lQXPc. È una classica catena di reindirizzamento (shortener → dominio esca → presunta area account) usata per offuscare la destinazione reale e aggirare filtri.SumUp stessa avverte che email non richieste con link a siti esterni che imitano pagine SumUp configurano tipicamente tentativi di phishing (sezione sicurezza / "Recognise phishing attacks").

- OSINT su domini, URL e IP
  - Shortener rcl[.]ink
    - WHOIS: dominio attivo dal 2018-06-03 (scadenza 2026-06-03). Servizio noto come URL shortener; in sé neutro, ma spesso abusato come ponte verso pagine di phishing.
    - Reputazione: fonti OSINT segnalano casi di abuso/"malware distributor" su rcl[.]ink (valutazioni algoritmiche; prendere con cautela, ma utile come segnale).
  - PhishTank: lo shortener rcl[.]ink risulta presente in storiche segnalazioni di URL (es. rcl[.]ink/RAvx8) — indicatore che il dominio accorciatore è stato usato in passate campagne di phishing (non implica che tutti i link siano malevoli).
  - Dominio di destinazione klant-bezoeknummer833893[.]sbs
    - Contesto: il TLD .sbs è gestito da ShortDot; non è di per sé malevolo, ma è economico/diffuso e spesso sfruttato in campagne di phishing per la facilità di registrazione.
    - Evidenza esterna specifica: è documentato pubblicamente un modello di email phishing SumUp che utilizza proprio un URL klant-bezoeknummer833893[.]sbs/account come destinazione "auth.sumup[.]com", a conferma del pattern osservato.
    - Tentativi su certificate transparency (crt.sh) non hanno prodotto evidenze utili pubbliche in tempo reale su quel FQDN: possibile assenza di certificati dedicati o uso di wildcard/MI certificato su host dinamico.
  - IP sorgente 46[.]203[.]233[.]114 (server che ha consegnato la mail)

- AS/Range: ricade nel 46[.]203[.]233[.]0/24 – AS215703 "FREAKHOSTING" (RIPE).
- AbuseIPDB: sono presenti segnalazioni recenti (Set 2025) per attività abusive su questo IP (incluso "SPF failure"): ulteriore indicatore di rischio dell'infrastruttura mittente.

- IP indicato nel corpo: 217[.]68[.]63[.]255
- L'IP viene presentato come "origine del login" (Den Haag, NL). Non è correlato alle infrastrutture SumUp note e, in assenza di ulteriori riscontri, va considerato **esca narrativa** per dare verosimiglianza all'allarme. (Si suggerisce comunque verifica ex-post su log applicativi locali o del fornitore, se esistenti.)

- Brand/tema "SumUp" nel threat landscape recente
  - SumUp pubblica avvisi/guide su riconoscimento phishing, smishing, vishing e best practice di difesa; più segnalazioni della community indicano campagne di spoofing/impersonation a tema SumUp. Queste fonti, pur non collegate 1:1 all'email in esame, corroborano il contesto di brand abuse.

- Tabella di sintesi OSINT (estratto)

Voce	Dato	Esito / Note
Short link	rcl[.]ink/lQXPc	WHOIS: attivo dal 2018; accorciatore talvolta abusato
Dominio destinazione	klant-bezoeknummer833893[.]sbs	Pattern confermato in campione pubblico di phishing SumUp - Il certificato HTTPS è valido fino al 14 dicembre 2025. - Registrato il 15 settembre 2025, con scadenza il 15 settembre 2026.
IP sorgente SMTP	46[.]203[.]233[.]114	Range AS215703 (FREAKHOSTING), segnalazioni AbuseIPDB recenti
IP "evento" nel testo	217[.]68[.]63[.]255	Dato narrativo nel body, non verificabile dai soli header
TLD info	.sbs	Registry ShortDot (facile/cheap → spesso abusato)
Best practice brand	SumUp Security/Phishing	Linee guida e avvisi ufficiali SumUp

- WHOIS e registrazione domini (mittente vs destinazione)

Il mittente dichiara sumup[.]it, ma i link reali puntano a dominio di destinazione differente (*.sbs). La verifica WHOIS su sumup[.]com conferma registrazione storica e governance coerente con l'azienda (u-domains), mentre *.sbs non è correlato. Questo mismatch mittente/destinazione è tipico del phishing: brand legittimo a schermo, ma destinazione esogena per la cattura delle credenziali.

- Hosting, geolocalizzazione e reputazione
    - Sorgente invio (46[.]203[.]233[.]114): hosting/ASN AS215703 FREAKHOSTING, country DE, con segnalazioni di abuso su AbuseIPDB (ultima nel periodo della ricezione). Ciò suggerisce infrastruttura non enterprise e compatibile con campagne malevole.
    - Destinazione .sbs: infrastruttura non riconducibile a SumUp, registrabile rapidamente e idonea a campagne "usa e getta".

- Certificato SSL/TLS (server destinazione)

  Per il FQDN klant-bezoeknummer833893[.]sbs non sono emerse evidenze pubbliche su CT log nel momento della consultazione; ciò può significare assenza di certificato dedicato, uso di wildcard non immediatamente visibile o scadenza/rotazione rapida. In ogni caso, la disallineata ownership del dominio resta l'IoC determinante.

- Analisi header di autenticazione (SPF, DKIM, DMARC)

  Sulle porzioni d'header disponibili non risultano voci Authentication-Results né DKIM-Signature. Non è quindi possibile attestare allineamento o firme valide per sumup[.]it. La combinazione assenza segnali di autenticazione + invio da IP VPS sostiene l'ipotesi di spoofing/abuso infrastrutturale.

- Allegati

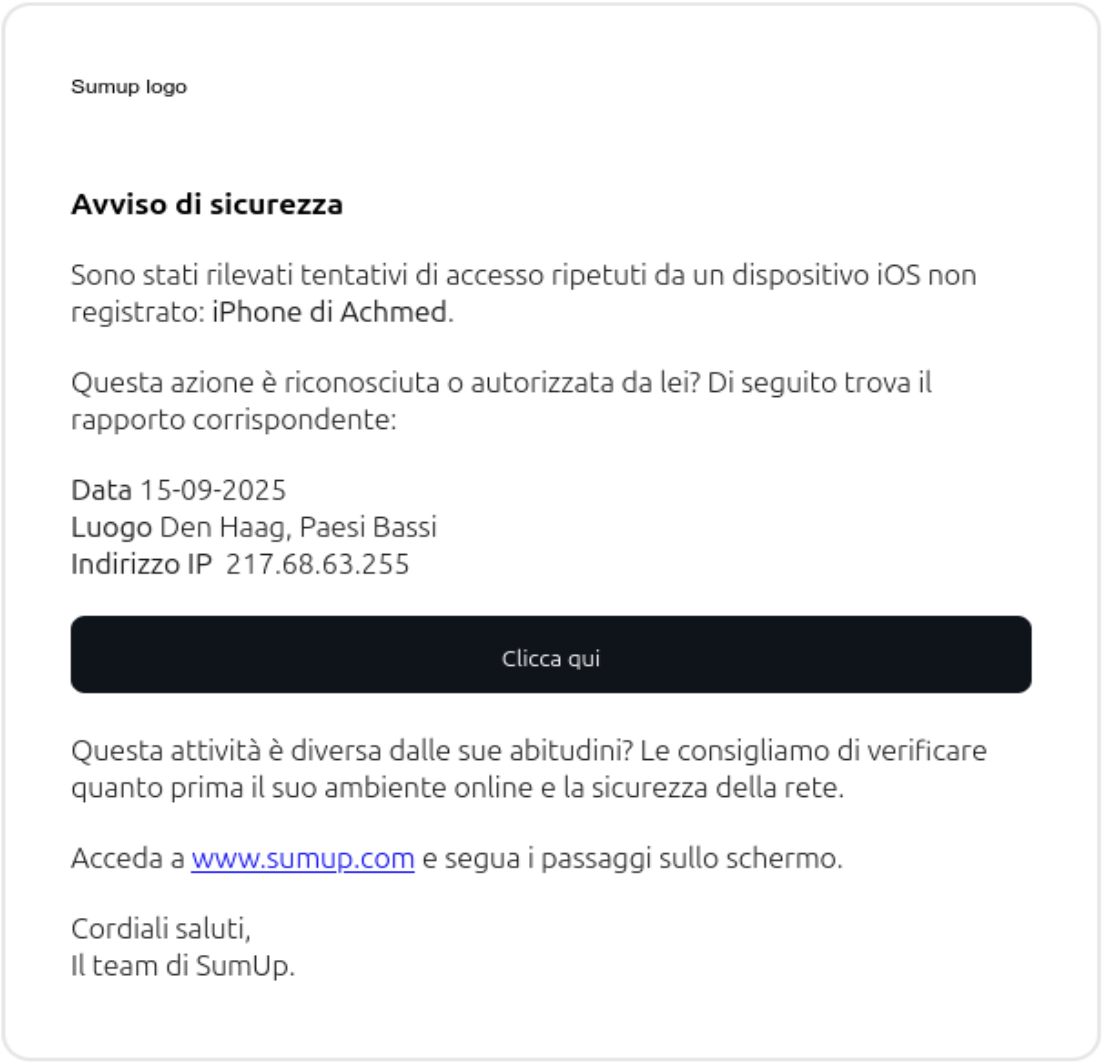
  Nessun allegato nel campione analizzato (quindi nessuna analisi hash/VT/JoeSandbox applicabile)

- OTX & VT (ricerche IoC)
    - OTX (AlienVault): utile per correlazioni su pattern SumUp e TLD .sbs; nessun pulse specifico recuperato nell'immediato per klant-bezoeknummer833893[.]sbs, ma sono presenti pulses tematici su brand impersonation/payment services (ricerca consigliata continuativa su tenant OTX).
    - VirusTotal: ricerche on the fly via GUI sui singoli IoC (shortlink/domino .sbs/IP) non hanno restituito un verdict univoco pubblicamente visualizzabile nel momento della consultazione; ciò è frequente per domini "usa e getta" e short link. Il dominio presenta comunque segnalazioni come "Suspicious" e "Malicious". L'insieme degli indizi (mismatch dominio, hosting VPS, pattern noto) rimane dunque probante.

- Indicatori di Compromissione (IoC)
    - Mittente dichiarato: noreply@sumup[.]it

- IP sorgente consegna (SMTP): 46[.]203[.]233[.]114
- Shortlink nel pulsante: rcl[.]ink/IQXPc
- Dominio di atterraggio (fake “auth.sumup”): klant-bezoeknummer833893[.]sbs
- IP “evento” nel corpo: 217[.]68[.]63[.]255
- Message-ID domain: sumup[.]it (non probante da solo)

- Immagine della email



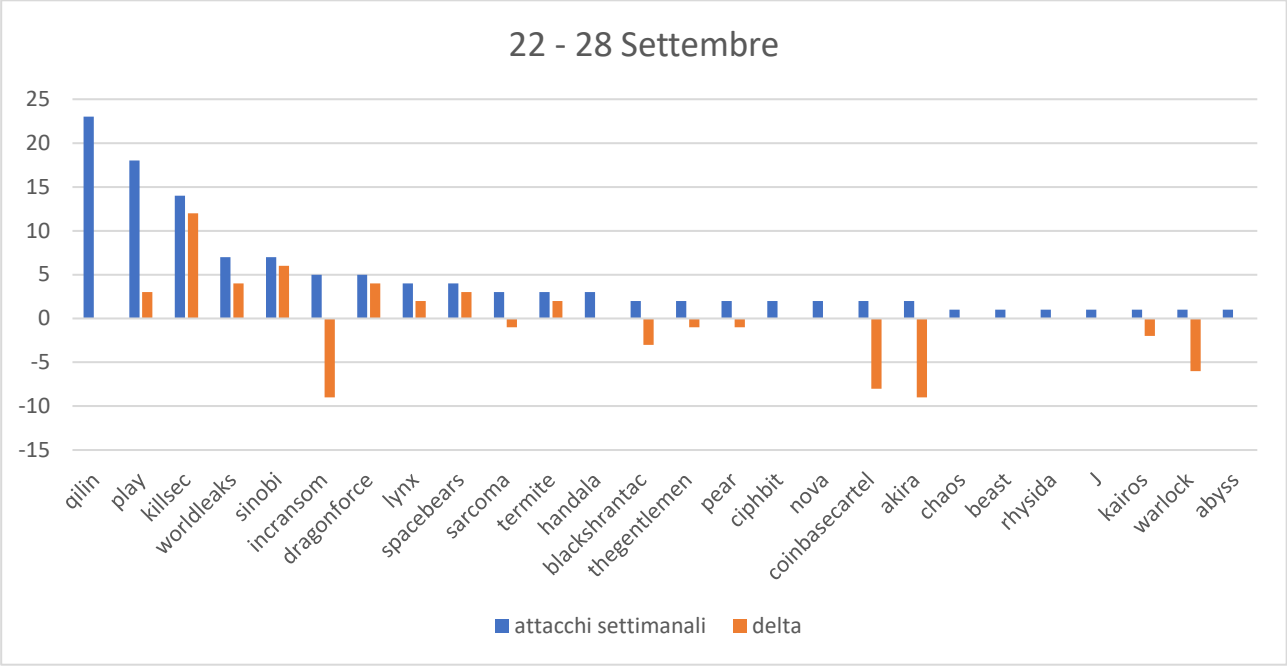
- Valutazione finale
  - Verdetto: PHISHING – Brand impersonation (SumUp) con esfiltrazione credenziali.
  - Motivi: mismatch mittente vs destinazione, shortener per offuscare la catena, TLD non correlato al brand, infrastruttura mittente VPS con segnalazioni di abuso, pattern già osservato pubblicamente con FQDN .sbs identico alla variante in analisi.

- Conclusioni

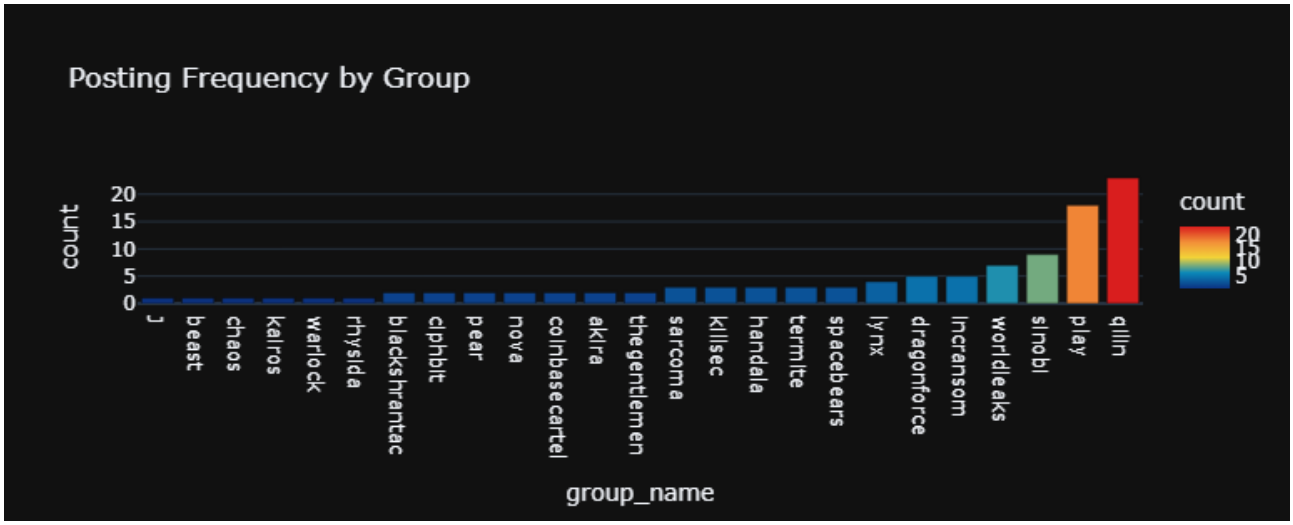
  L'email analizzata rientra a pieno titolo in una campagna di phishing diretta ad utenti Italiani che impersona SumUp: la combinazione di URL shortener, dominio .sbs non correlato, infrastruttura mittente in hosting non enterprise e pattern pubblico identico porta a un giudizio tecnico "Malicious/Phishing" con obiettivo furto credenziali.

4.2 Ransomware

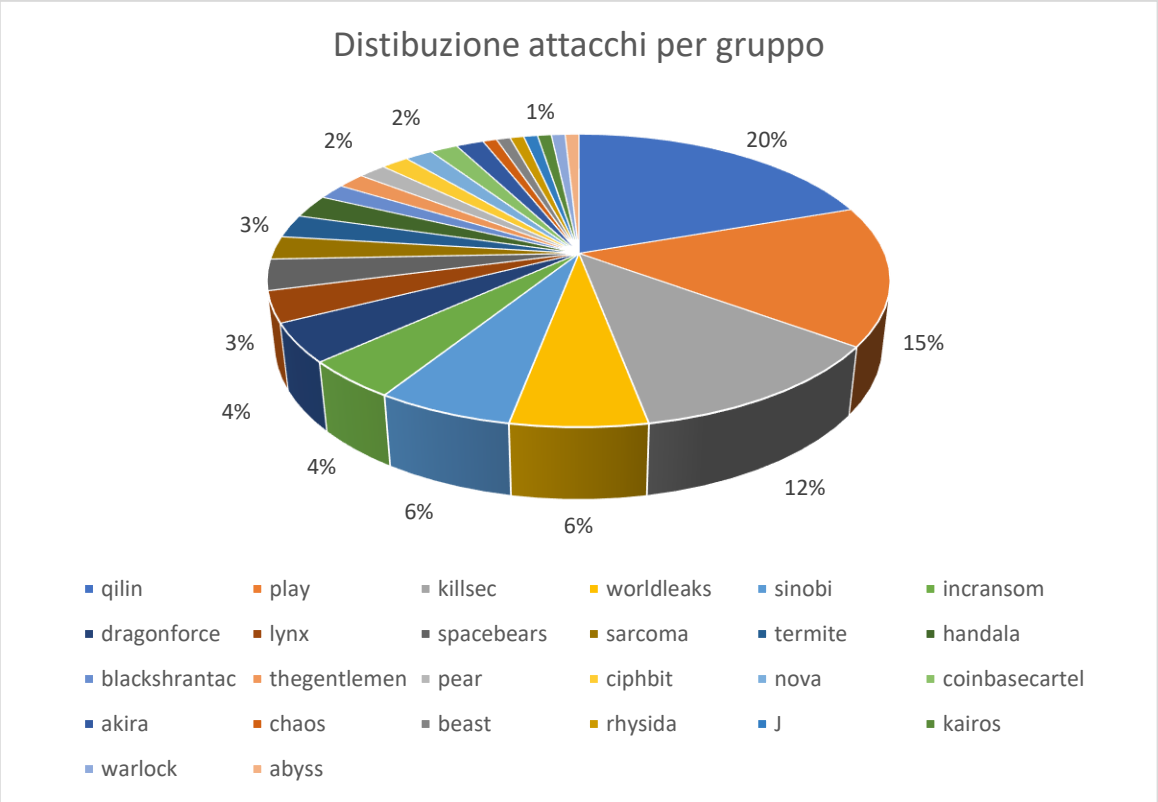
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (22 - 28 Settembre). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

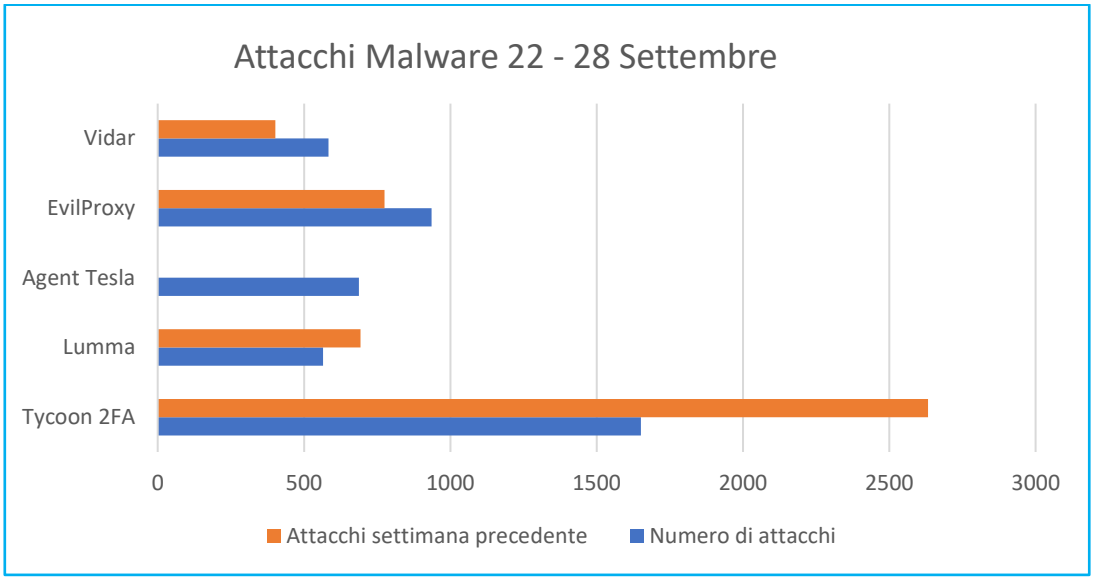


Questa invece la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:


Distibuzione attacchi per gruppo
20%
15%
12%
6%
6%
4%
4%
3%
3%
2%
2%
1%
qilin
play
killsec
worldleaks
sinobi
incransom
dragonforce
lynx
spacebears
sarcoma
termite
handala
blackshrantac
thegentlemen
pear
ciphbit
nova
coinbasecartel
akira
chaos
beast
rhysida
J
kairos
warlock
abyss

4.3 Malware

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



Come sempre riportiamo un'analisi dettagliata dei malware risultati più attivi nella settimana di osservazione

- **ShadowV2**

Gli analisti di Darktrace hanno individuato ShadowV2, un nuovo botnet DDoS-as-a-Service che sfrutta container Docker mal configurati su AWS. L'infezione parte da uno script Python su GitHub CodeSpaces che crea container contenenti un malware Go che trasforma le macchine compromesse in nodi DDoS. Il C2 utilizza richieste HTTP periodiche e persino tecniche avanzate di attacco (HTTP/2 Rapid Reset, bypass di Cloudflare Under Attack Mode).

Il malware è particolarmente insidioso: impiega un'interfaccia API completa con login e controlli di operatori, rendendolo un vero servizio DDoS modulare che:

- usa cluster container (Docker) su istanze cloud (AWS) mal configurate come vettore di infezione e come ambiente di esecuzione per nodi bot;
- componente operator-side in Python (API/GUI/operazioni) e agent in Go come payload runtime nei container;
- persistence legata alla gestione dei container (cron + orchestrator scripts) invece che a un tradizionale servizio Windows — ciò lo rende resistente al semplice reboot della macchina se i container ricreano il payload;

- supporta numerose modalità DDoS (HTTP/1.1, HTTP/2 Rapid Reset, UDP flood, layer7 con by-pass a protezioni tipo Cloudflare "Under Attack Mode").

IoC:

Tipo	Indicatore
Domini C2	• shadow.aurozacloud[.]xyz
Hashes	• 2462467c89b4a62619d0b2957b21876dc4871db41b5d5fe230aa7ad107504c99 • 1b552d19a3083572bc433714dfbc2b75eb6930a644696dedd600f9bd755042f6 • 1f70c78c018175a3e4fa2b3822f1a3bd48a3b923d1fbdeaa5446960ca8133e9c
IP	• 23.97.62[.]139 • 23.97.62[.]136

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1595	Ricognizione	Scansione e raccolta di immagini/container esposti e API Docker pubbliche per identificare host vulnerabili
T1190	Sfruttamento di servizi esposti	Sfruttamento di Docker API o servizi cloud mal configurati per eseguire codice o creare container.
T1071.001	Comando e controllo: HTTP(S)	Comunicazione C2 tramite richieste HTTP/HTTPS (heartbeat, comandi, download payload).
T1498.001	Denial of Service: Volumetric	Condotta di attacchi DDoS layer 3/4/7 (UDP flood, HTTP flood, HTTP/2 Rapid Reset).

T1562.001	Elusione: Disabilitazione/log tampering	Tecniche per ridurre la visibilità (offuscamento dei heartbeat, uso di CDN, possibile soppressione log).

Rilevamento:

- monitorare traffico insolito verso domini AWS/Docker, analizzare log di container e processi Docker.
- Applicare regole YARA dedicate nei sistemi di rilevamento endpoint.
- Utilizzare intrusion detection per intercettare attività di rete sospette (es. heartbeat su domini noti).

Livello di rischio: alto. ShadowV2 consente attacchi DDoS potenti e difficili da rilevare.

- **Nimbus Manticore**

Il report di Check Point evidenzia una campagna dello Stato iraniano Nimbus Manticore (a volte legata a UNC1549/Smoke Sandstorm) focalizzata su Europa occidentale (Danimarca, Svezia, Portogallo).

L'attacco inizia con spear-phishing mirato via falsi portali di lavoro; payload in ZIP contenente Setup.exe e DLL collaterali per DLL sideloading (catena multi-stage).

E infine all'installazione di due malware custom: il backdoor MiniJunk (evoluzione di Minibike/SlugResin) e lo stealer MiniBrowse. Questi payload usano firme digitali valide, grandi dimensioni artificiali ed estrema obfusazione per sfuggire alle difese.

Dettagli tecnici:

- DLL sideloading chain: un processo legittimo carica una DLL malevola posta nello stesso folder; il malware sfrutta API Windows non documentate per cambiare la search order dinamicamente.
- Persistenza: scheduled task che lancia il loader all'avvio e copia eseguibili in %APPDATA%\Local\Microsoft\MigAutoPlay\ o %APPDATA%\Roaming\<app>

IoC:

Tipo	Indicatore
Domini C2	• asylimed[.]azurewebsites[.]net • clinichaven[.]azurewebsites[.]net • healsanctum[.]azurewebsites[.]net • healthdataanalyticsrecord[.]azurewebsites[.]net • medical-deepresearch[.]azurewebsites[.]net • oletask-tracker.azurewebsites[.]net
Hashes	• 23c0b4f1733284934c071df2bf953a1a894bb77c84cff71d9bfcf80ce3dc4c16- malicious zip • 0b2c137ef9087cb4635e110f8e12bb0ed43b6d6e30c62d1f880db20778b73c9a - malicious zip • 6780116ec3eb7d26cf721607e14f352957a495d97d74234aade67adbdc3ed339 - malicious zip • 9b186530f291f0e6ebc981399c956e1de3ba26b0315b945a263250c06831f281 - Minibrowse

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566.002	Phishing mirato (spearphishing link)	Consegna iniziale mediante email/portali di lavoro falsi che inducono a scaricare payload.
T1574.002	DLL Side-Loading	Caricamento di DLL malevole sfruttando eseguibili legittimi vulnerabili (DLL search order hijack).
T1041 / T1071.001	Esfiltrazione / C2 via Web	Esfiltrazione dati e comando/controllo usando HTTPS verso sottodomini cloud

T1027	Offuscamento	Cifratura/obfuscazione delle stringhe e controllo di flusso per evitare il rilevamento statico.

Rilevamento:

- Controllare esecuzione anomala di processi firmati (es. carichi DLL sospetti in processi di sistema).
- Analizzare file XLS/DOCX in arrivo e usare sandbox per rilevare comportamenti di sideloading e obfuscazione.
- Monitorare connessioni ai domini Azure identificati.
- Utilizzare strumenti EDR/IDS con regole per individuare manipolazioni di processi (ad es. regola per DLL sideloading).

Livello di rischio: Alto. MiniJunk e MiniBrowse sono usati da un APT avanzato con tradecraft sofisticato (firme valide, payload mutati) e mirano ad infrastrutture critiche.

NOTA: Il termine "tradecraft" si riferisce all'insieme di abilità, metodi, tecniche e tecnologie usate in attività di spionaggio e raccolta di informazioni segrete

- **Campagna BlockBlasters – StimBlaster e StealC**

Un incidente diffuso a fine settembre: una patch malevola per il gioco Steam BlockBlasters (pubblicato a luglio) ha installato un trojan «StimBlaster» e uno stealer StealC, rubando soprattutto criptovalute. Il malware si diffonde tramite file batch e script VBS camuffati all'interno dell'aggiornamento fraudolento.

Componenti:

- StimBlaster (client-built2.exe) è un backdoor Python compilato che comunica con un C2 .
- StealC (Block1.exe) è uno stealer C++ che cerca e cifra le chiavi di wallet in Chrome/Brave/Edge.

Il risultato è stato il furto di oltre 150.000 USD in crypto dai giocatori, anche tra streamer (un caso notevole: un giocatore ha perso 30.000 USD raccolti per beneficenza)

IoC:

Tipo	Indicatore
IP C2	• 203[.]188[.]171[.]156 • 45[.]83[.]28[.]99
Hashes	Block1.exe • 59f80ca5386ed29eda3efb01a92fa31fb7b73168e84456ac06f88fdb4cd82e9e Client-built2.exe • 17c3d4c216b2cde74b143bfc2f0c73279f2a007f627e3a764036baf272b4971a

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1059.003	Esecuzione: script batch	Uso di file .bat come dropper per avviare payload e scaricare componenti malevoli.
T1059.005	Esecuzione: VBScript	Uso di script VBS per persistenza o esecuzione offuscata di componenti secondari.
T1056.002	Raccolta: intercettazione clipboard	Monitoraggio e sostituzione degli indirizzi copiati negli appunti (wallet hijacking).
T1005	Raccolta: accesso a file locali	Accesso e copia di file di wallet (es. wallet.dat), credenziali e dati sensibili.

T1041	Esfiltrazione	Invio di dati raccolti verso C2 via HTTP/HTTPS a IP/host controllati dagli operatori.

Rilevamento:

- Usare antivirus/EDR per segnalare i payload StimBlaster/StealC (es. firme Win32.Trojan-Stealer.StealC su Block1.exe.
- Monitorare connessioni verso gli IP di C2 noti.
- Analizzare i log del processo Steam e di file batch anomali (es. cartella SteamLibrary con script non ufficiali).

Livello di rischio: Alto. I malware StimBlaster e StealC hanno permesso furti diretti di criptovalute su vasta scala

- **Lone None**

Il gruppo vietnamita "Lone None" ha veicolato malware via email fittizi di copyright takedown. Le vittime ricevono false notifiche legali contenenti link a archivi malevoli (spesso ospitati su Dropbox/Mediafire). Il malware si diffonde tramite un installer che utilizza un PDF reader legittimo (Haihaisoft) come loader DLL per installare Python in cartella pubblica e lanciare script offuscati. Il payload finale sono due stealer:

- PureLogs Stealer (rubacredenziali, cookie, file locali e dati di wallet)
- Il nuovo LoneNone Stealer (anche chiamato PXA Stealer), specializzato nel furto di criptovalute tramite intercettazione/alterazione degli indirizzi copiati negli appunti.

La comunicazione C2 usa canali non convenzionali come account Telegram e servizi pastebin.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566.002	Phishing mirato (spearphishing link)	Email di notifica legale/falsi avvisi con link ad archivi o dropper ospitati su cloud

T1574.003	DLL sideloading	Sfruttamento di reader legittimi per caricare DLL malevole come loader.
T1059.006	Esecuzione: script Python offuscati	Esecuzione di payload Python (PyInstaller/embedded) altamente offuscati come primo stage.
T1041	Esfiltrazione: canali non convenzionali	Uso di Telegram bot, paste services (es. 0x0.st) e upload verso servizi cloud per esfiltrare dati
T1547.001	Persistenza: Run keys	Creazione di chiavi di registro HKCU\...\Run con script Python per persistenza su login

Rilevamento:

- Monitorare creazione di eseguibili Python in percorsi non standard, uso anomalo di certutil.exe, powershell -enc e chiamate a Telegram API da workstation.

Livello di rischio: Alto.

- **Cisco ASA — RayInitiator e LINE VIPER**

A fine settembre CISA e NCSC hanno allertato per un attacco massivo alle firewall Cisco ASA (serie 5500-X). Uno zero-day nella VPN web di ASA (CVE-2025-20362/20333) è stato sfruttato da un gruppo di cyber-spionaggio cinese (Storm-1849/UAT4356) soprannominato ArcaneDoor. Il malware introdotto è un bootkit avanzato (RayInitiator, un GRUB persistente) che carica in memoria un loader utente (LINE VIPER).

LINE VIPER fornisce shell OTA avanzate, intercetta comandi CLI, abusa di AAA VPN, spegne il logging e sopprime analisi diagnostica.

Anche se non esiste un IOC tradizionale facilmente citabile (l'attacco si fonda su firmware/ROM modificati), l'evento è di massima gravità.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1190	Sfruttamento di servizi public-facing	Sfruttamento di vulnerabilità in servizi VPN/Web-facing (CVE-2025-20333 / CVE-2025-20362) per accesso iniziale.
T1547.003	Persistenza: Firmware/Bootkits	Installazione di un bootkit (modifica GRUB/bootloader/firmware) per ottenere persistenza a livello flash/ROM.
T1562.006	Elusione: Tampering dei log	Soppressione o manipolazione dei log di sistema per ostacolare rilevamento e risposta.
T1486	Impatto: Disponibilità compromessa	Possibile degradazione o controllo della disponibilità del dispositivo (impatto operativo, blocco servizi).

Rilevamento:

- Analizzare i dispositivi ASA sospetti (modelli EoS specifici) per segni di compromissione firmware (ad es. versioni di ROMMON non originali).
- Implementare sistemi di protezione di rete che rilevino configurazioni errate o crash frequenti delle appliance (gli attaccanti provocavano crash ad arte per impedire analisi).
- Abilitare registrazione centralizzata e analisi dei log a valle (anche se LINE VIPER tenta di sopprimerli).

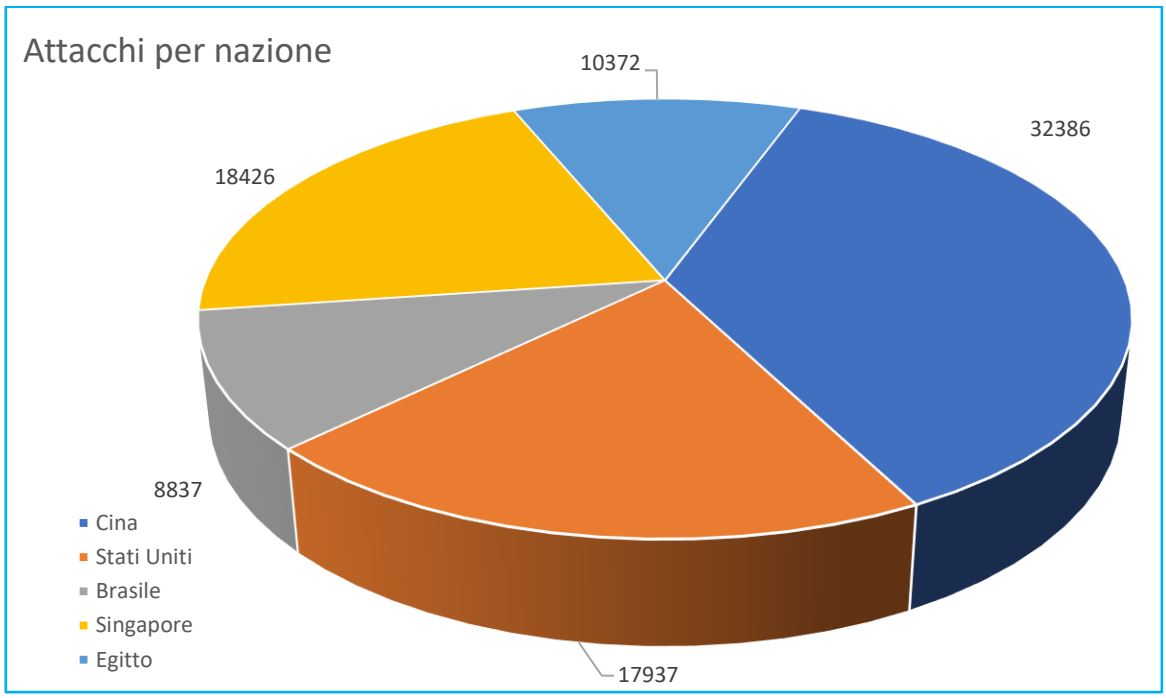
Livello di rischio: Alto.

Riepilogo:

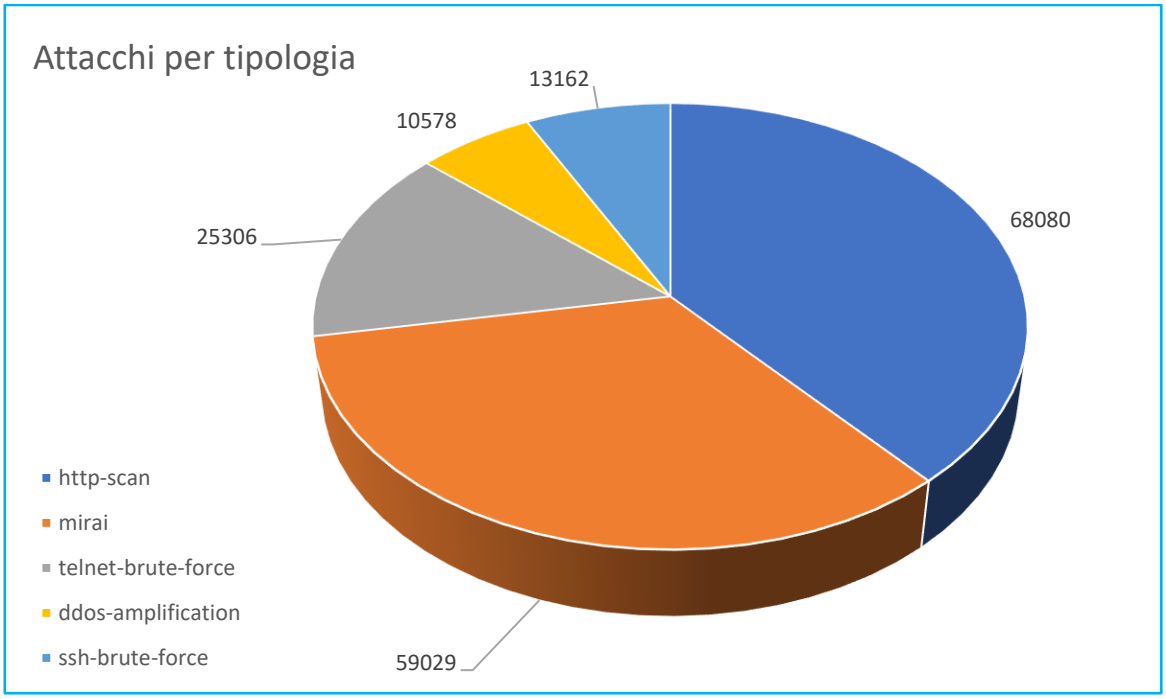
Malware	Categoria	Livello di rischio
ShadowV2	Botnet DDoS basata su container	Alto
Nimbus Manticore	Stealer / Backdoor (MiniJunk, MiniBrowse)	Alto
BlockBlasters	InfoStealer + Clipper (StimBlaster/StealC)	Alto
Lone None	Stealer avanzato con loader multipli	Alto
RayInitiator / LINE VIPER	Bootkit & Exploit VPN (Cisco ASA)	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 22– 28 Settembre, suddivisa per nazione e limitata alle prime cinque posizioni:

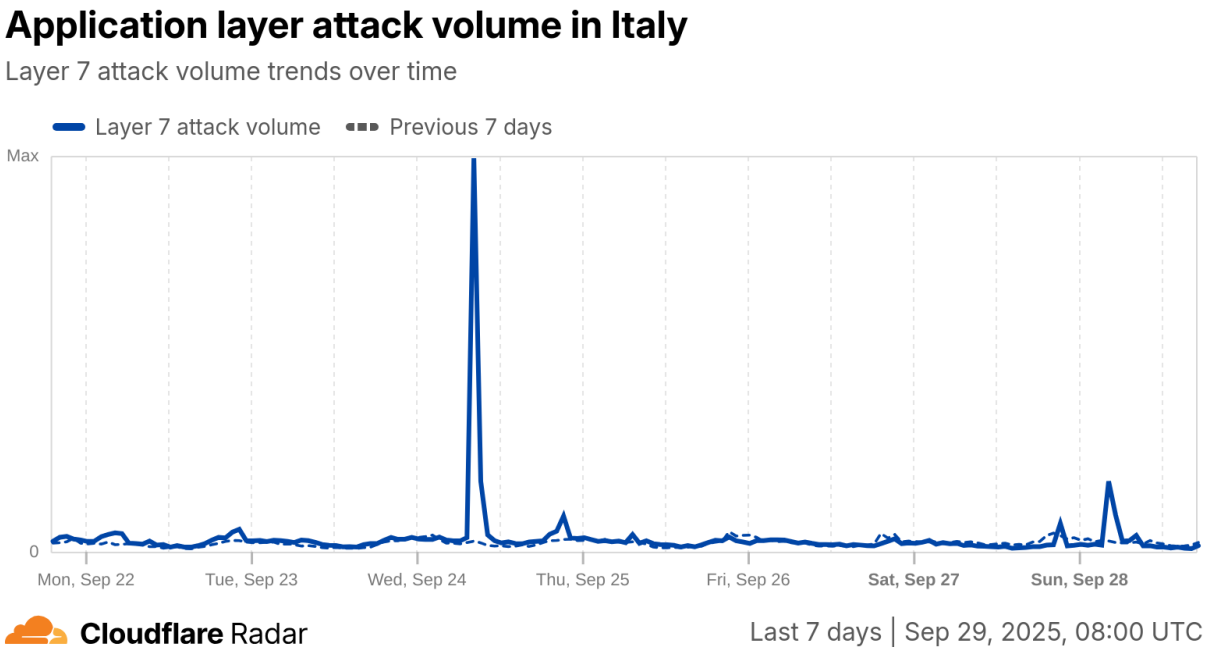


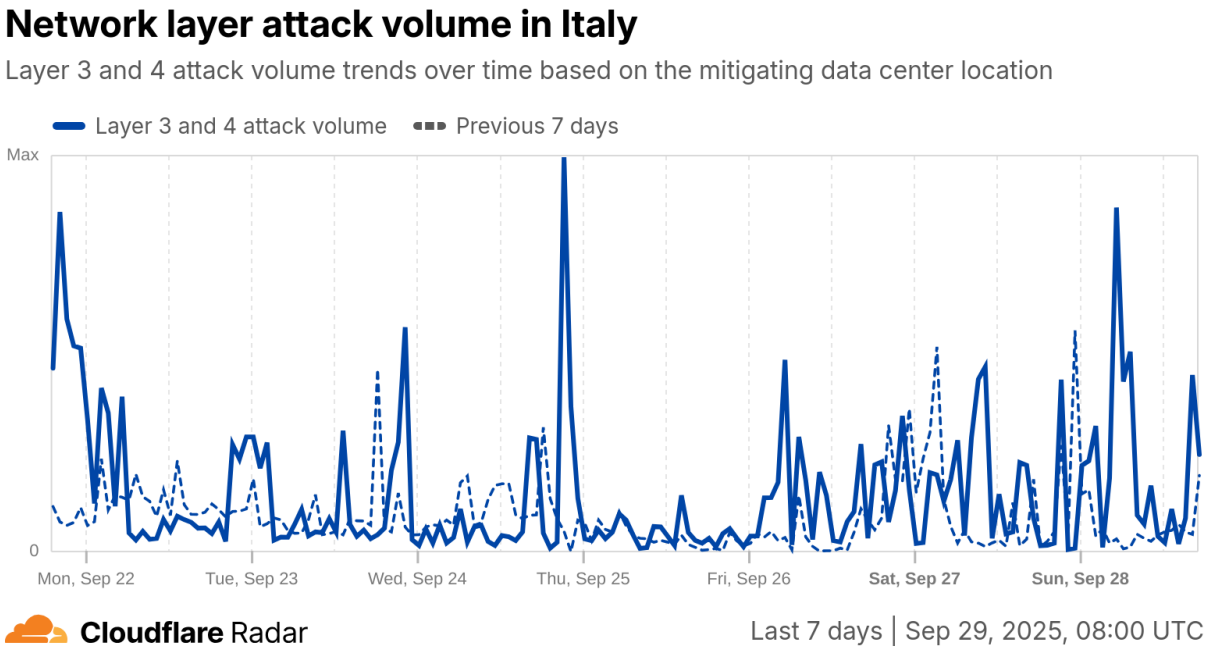
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



SITUAZIONE ITALIANA

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





Fonte: Cloudflare Radar

4.5 Data Breach

In questa sezione sono riportati alcuni tra i principali Data Breach individuati nella settimana di osservazione.

TARGET	LOCALIZZAZIONE
COMUNE DI FORLÌ	ITALIA
DESCRIZIONE	Pochi giorni fa il Comune di Forlì ha subito un attacco informatico che ha causato l'interruzione temporanea di alcuni servizi digitali. Le autorità comunali hanno attivato immediatamente le procedure di sicurezza e avviato verifiche con l'aiuto dell'Agenzia per la Cybersicurezza Nazionale. Al momento non risultano furti di dati sensibili e non è stato ancora identificato il responsabile dell'attacco ma le indagini sono ancora in corso.

TARGET	LOCALIZZAZIONE
BOYD GAMING	STATI UNITI
DESCRIZIONE	Boyd Gaming, società statunitense attiva nei casinò e nell'ospitalità, ha confermato di essere stata vittima di un attacco informatico recentemente, come indicato in un documento depositato alla SEC. Un soggetto non autorizzato ha ottenuto accesso ai sistemi interni, sottraendo dati relativi a dipendenti e ad altre persone esterne all'organizzazione. L'azienda ha spiegato che le operazioni dei casinò, hotel e altri servizi non sono state interrotte. Subito dopo la scoperta, sono stati coinvolti esperti esterni in cybersicurezza e le autorità federali per avviare le indagini e contenere i danni. Al momento non è chiaro chi sia l'autore dell'attacco né l'estensione esatta del danno, e l'azienda non ha reso noto se sia stato pagato un riscatto.

TARGET	LOCALIZZAZIONE
SPERI S.P.A.	ITALIA
DESCRIZIONE	Il 25 settembre 2025, SPERI S.p.A., azienda milanese attiva nei settori dell'architettura e ingegneria, è stata vittima di un attacco ransomware condotto dal gruppo Qilin. Il gruppo ha rivendicato l'attacco e minaccia di pubblicare dati sensibili se le sue richieste non verranno soddisfatte. Al momento non è chiaro l'ammontare né la natura precisa dei dati sottratti, ma potrebbero includere informazioni su clienti, progetti e documenti interni. Le indagini sono ancora in corso e l'azienda non ha rilasciato dichiarazioni ufficiali su eventuali negoziazioni o misure adottate.

4.6 Defacement

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

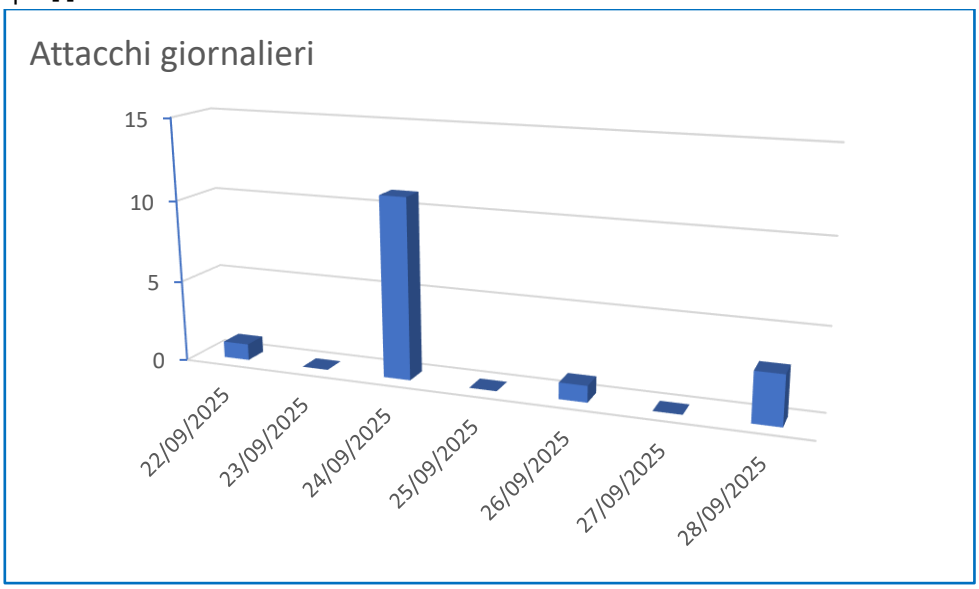


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

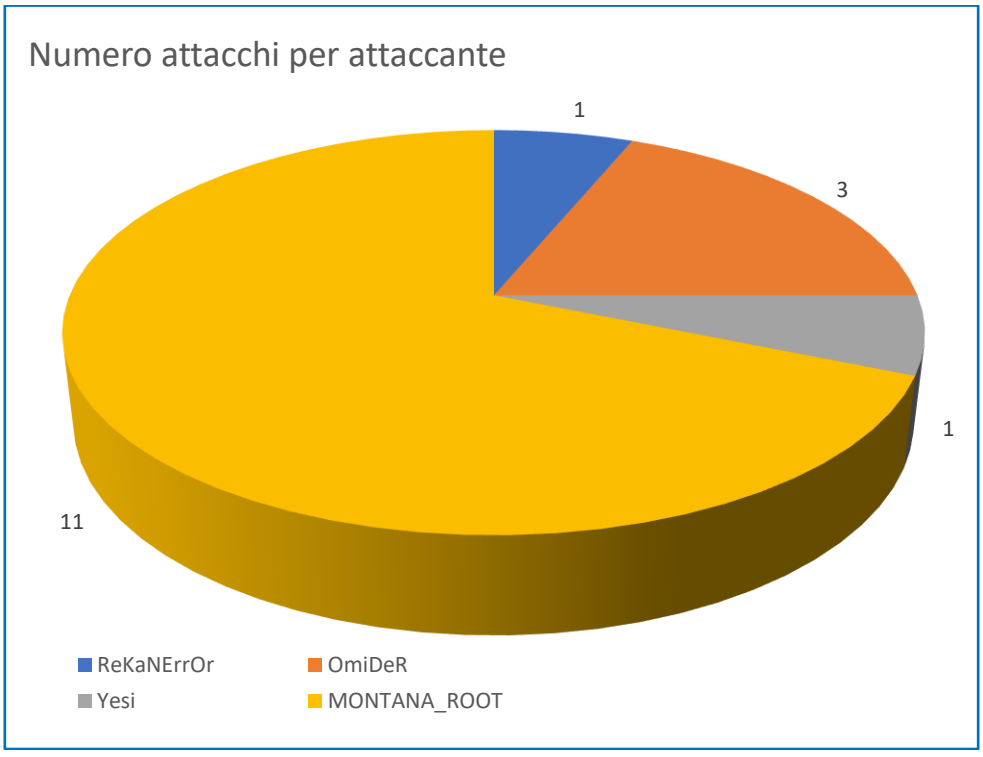


Figura 2: Defacement - Attaccanti più attivi nel periodo 22 – 28 Settembre

5 Honeypot

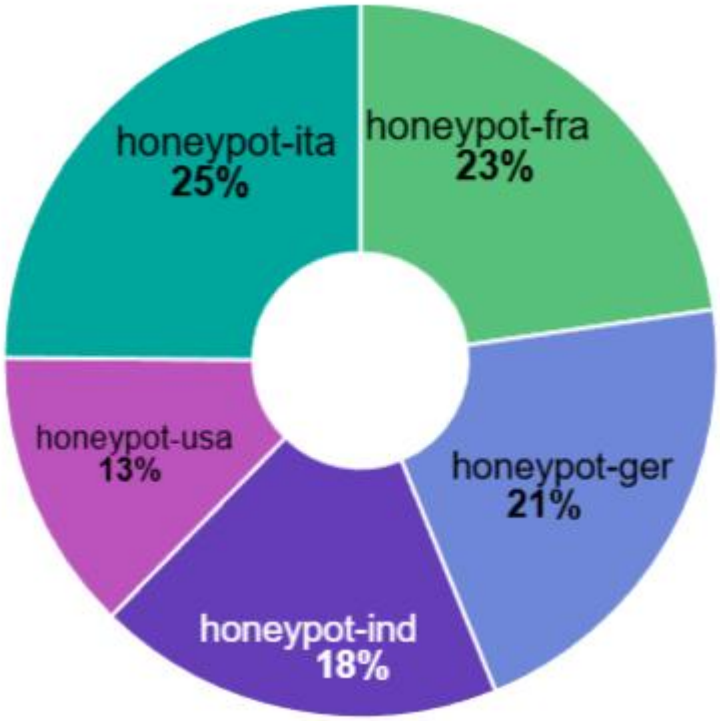
I seguenti dati sono raccolti da sistemi appositamente predisposti per la raccolta dei log sugli attacchi informatici (Honeypot). L'infrastruttura è composta da sensori honeypot dislocati nei principali paesi di interesse mondiale. Ad oggi, i sensori sono stati installati nei seguenti paesi: Italia,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

5.1 Attacchi Settimanali Honeypot S3K – Analisi generale

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

2.080.478 Attacks **9.609** Unique Src IPs **74** Unique HASSHs

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

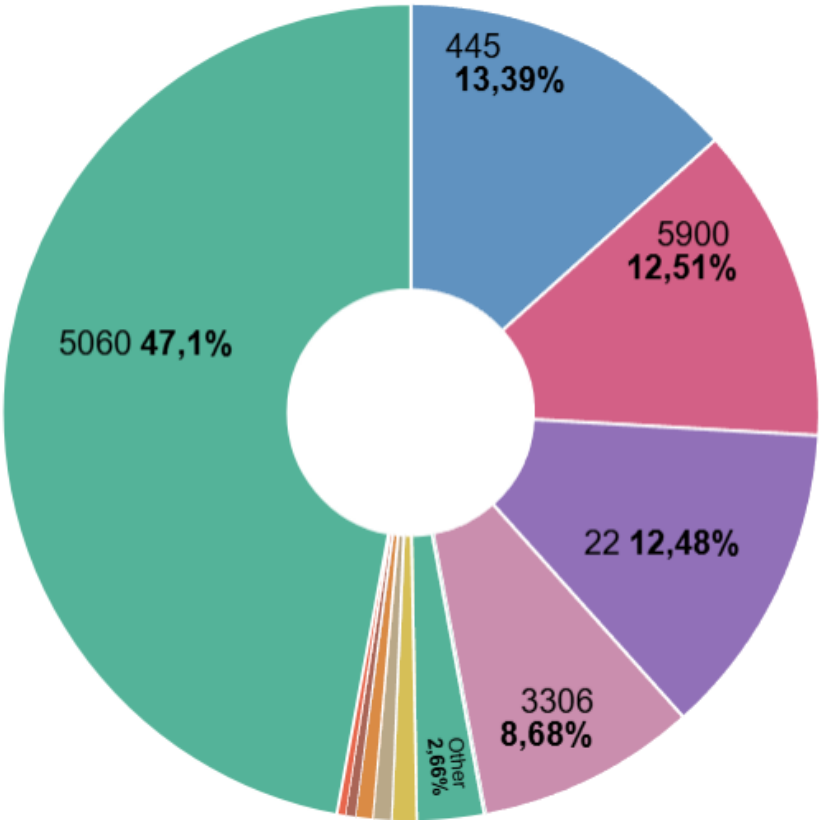


Questa invece la situazione a livello italiano:

517.497 Attacks **3.293** Unique Src IPs **49** Unique HASSHs

5.1.1 Attacchi ai servizi

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



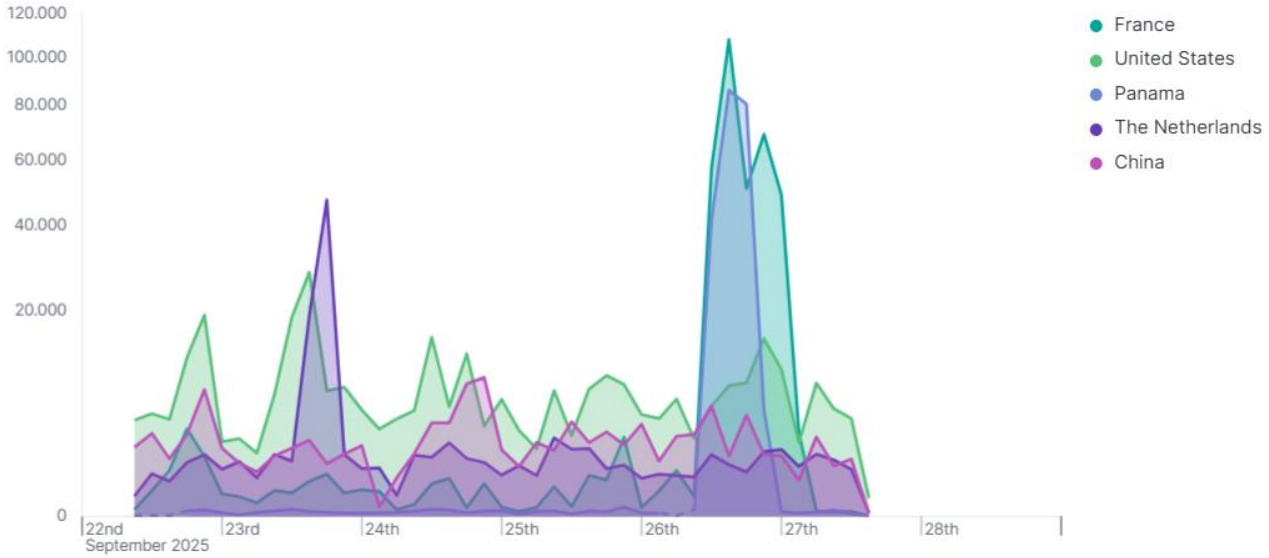
5.1.2 IP Attaccanti

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

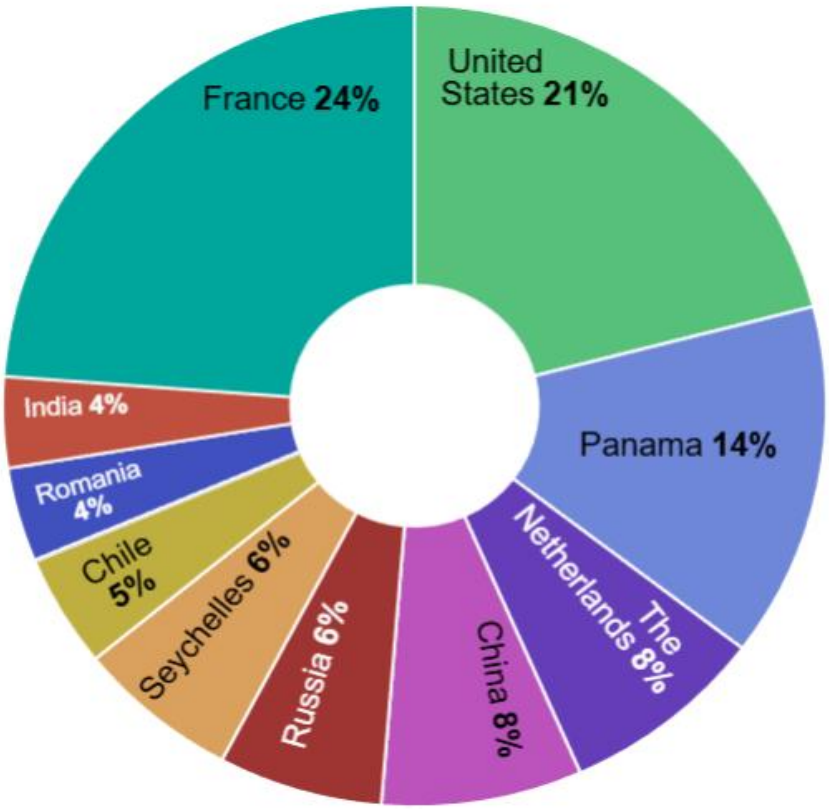
Source IP	Count
46.105.87.113	195.993
141.98.80.144	159.528
92.204.255.106	132.460
93.88.74.182	61.531
186.10.24.214	61.188
2.57.121.148	50.912
141.98.80.146	34.713
142.202.189.5	32.493
142.202.191.234	28.779
144.217.113.57	27.977

5.1.3 Paesi di provenienza degli attacchi

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



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

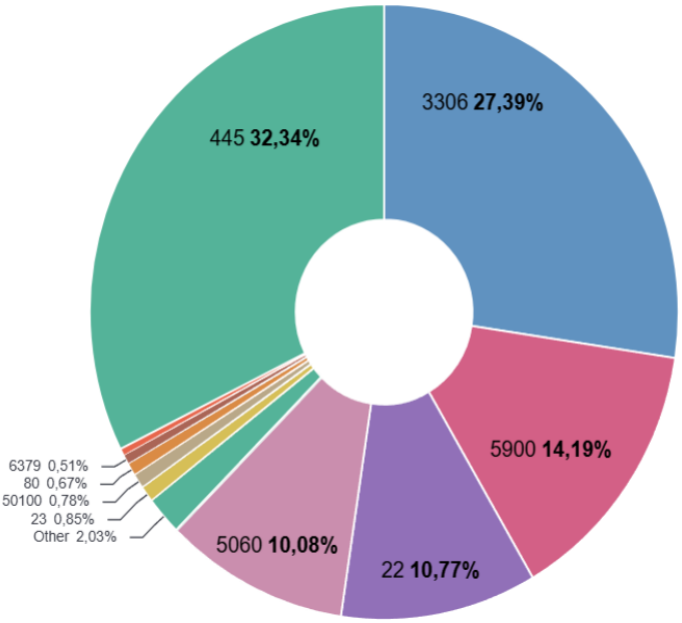


5.2 Italian Honeypot N.1

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

5.2.1 Attacchi ai servizi

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



Port	Count
445	68.791
3306	58.298
5900	30.178
22	22.921
5060	21.451
23	1.804
50100	1.683
80	1.428
6379	1.087
443	836

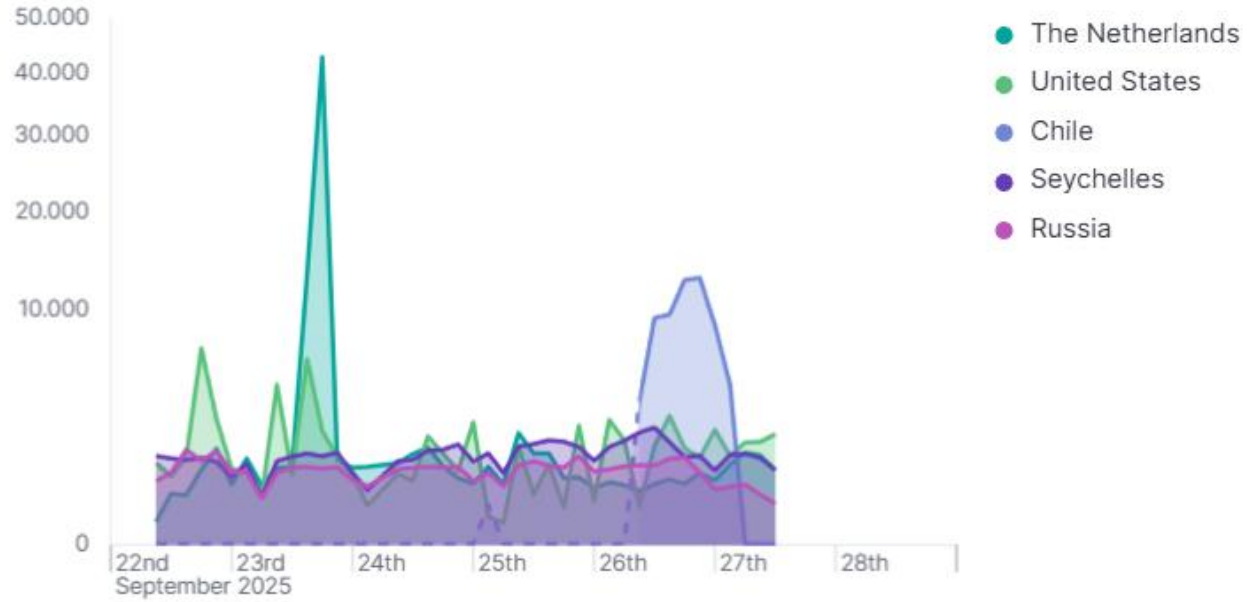
5.2.2 IP Attaccanti

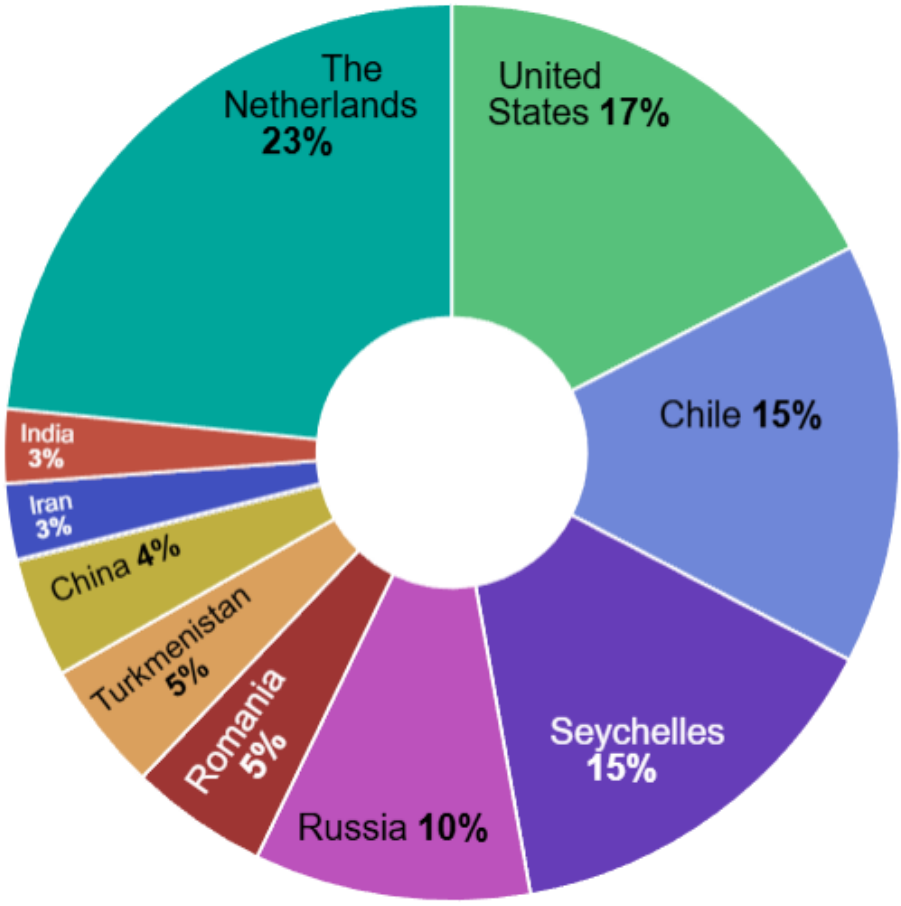
Questa invece la classifica relativa ai 10 IP che hanno effettuato il maggior numero di attacchi:

Source IP	Count
186.10.24.214	61.188
93.88.74.182	53.475
2.57.121.148	18.365
45.134.26.33	12.615
91.202.233.65	12.548
193.24.123.28	11.571
178.22.24.32	10.483
196.251.66.137	10.298
196.251.81.129	9.424
142.202.189.5	9.375

5.2.3 Paesi di provenienza degli attacchi

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



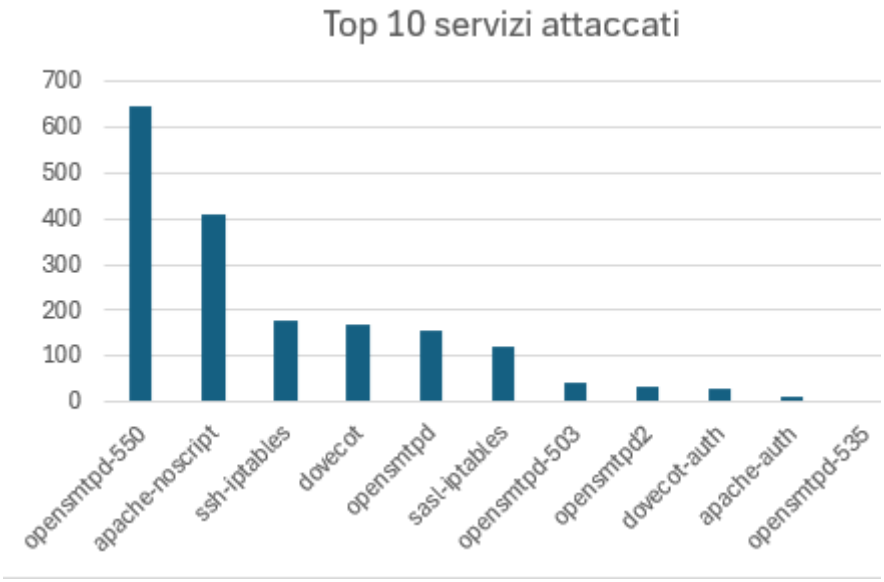


5.3 Italian Honeypot N.2

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.



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

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

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

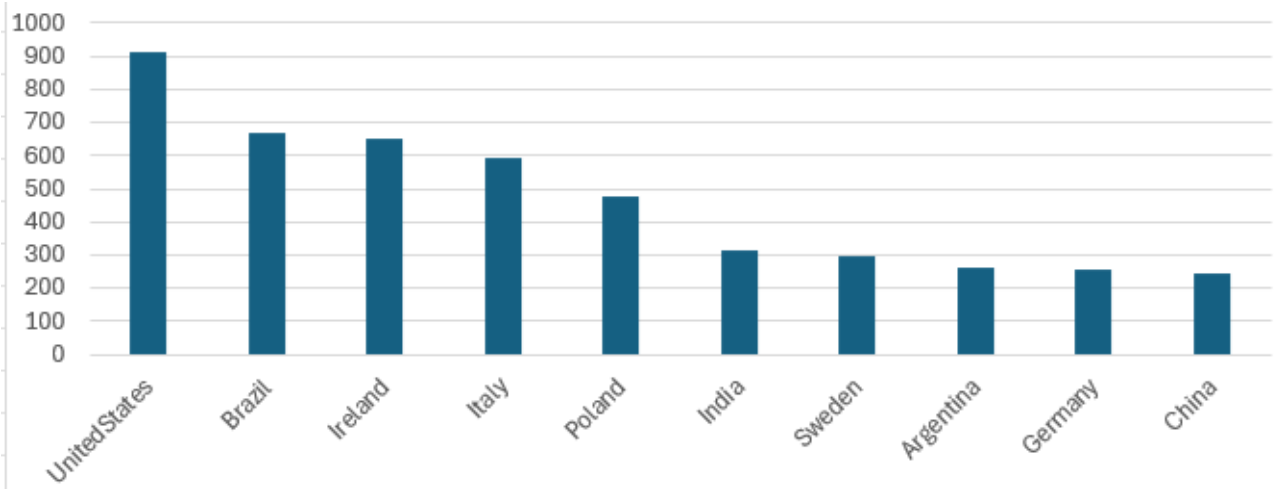
5.3.2 IP attaccanti

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

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

5.3.3 Paesi di provenienza degli attacchi

Questa invece la distribuzione dei paesi attaccanti:



6 Company Profile S3K

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

COME LO FACCIAMO:

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

Abbiamo un presidio esteso sul territorio con circa 550 dipendenti distribuiti tra le sedi di Roma, Milano, Torino, Padova, Firenze, Palermo e Catania.

L'ambizione e la prospettiva vedono un ulteriore e progressivo rafforzamento sia sul territorio nazionale che internazionale dove già operiamo con successo e con Clienti di primaria rilevanza.

CON QUALI LEVE OPERIAMO:

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

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

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

CHI SIAMO:

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

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

LA NOSTRA MISSION:

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

I NOSTRI VALORI:

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

CONTATTI:

contattaci@s3kgroup.it
insidesales@s3kgroup.it
marketing@s3kgroup.it

DISCLAIMER

Tutte le informazioni fornite in questo documento sono fornite "così come sono" solo a scopo informativo e, se non diversamente specificato, non costituiscono un contratto legale tra S3K e qualsiasi persona o entità.

Le informazioni fornite sono soggette a modifiche senza preavviso. Sebbene venga fatto ogni ragionevole sforzo per presentare informazioni aggiornate e accurate, non forniamo alcuna garanzia della loro validità e usabilità in relazione agli intendimenti e necessità dell'Organizzazione.

Questo documento contiene informazioni create e mantenute sia internamente che esternamente, provenienti da diverse fonti. In nessun caso S3K sarà responsabile, direttamente o indirettamente, per qualsiasi danno o perdita causati o

presumibilmente causati da o in connessione con l'uso o l'affidamento su qualsiasi contenuto presentato. Eventuali collegamenti a siti Web esterni non devono essere interpretati come un'approvazione del contenuto o invito alla visualizzazione dei materiali collegati.

CLASSIFICAZIONE DOCUMENTO

2.0 TLP: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