S3K

Cyber security

RISK REPORT

\ week 25.08.2025 - 31.08.2025

Sommario


CYBER SECURITY RISK REPORT
35/25

1 Il Cyber Security Risk Report S3K

Il bollettino settimanale di S3K offre un'analisi completa della situazione della sicurezza informatica, riportando le principali minacce, vulnerabilità e attacchi rilevati nel periodo di riferimento. Il documento fornisce informazioni dettagliate su security news, CVE critiche, analisi di attacchi (phishing, ransomware, malware, DDoS), data breach significativi e attività di monitoraggio degli honeypot. Questo strumento essenziale permette ai professionisti della sicurezza informatica di rimanere aggiornati sulle minacce emergenti e sulle tendenze del panorama cyber, fornendo dati analitici e raccomandazioni operative per migliorare la postura di sicurezza delle organizzazioni.

1.1 Principali Security News e Tendenze

Aggiornamenti e Patch Critiche

ISC ha rilasciato patch per vulnerabilità ad alta gravità in Kea DHCP, che potrebbe compromettere la disponibilità dei sistemi. Cisco ha pubblicato aggiornamenti per molteplici vulnerabilità che interessano diversi prodotti, tra cui Switch Nexus e UCS Manager. Google Chrome ha corretto una vulnerabilità critica che potrebbe consentire l'esecuzione di codice arbitrario.

Nuove Minacce Identificate

Individuato "Sindoor Dropper", un malware Linux che sfrutta tensioni geopolitiche tra India e Pakistan. Una grave vulnerabilità nei sistemi Citrix viene attivamente sfruttata da hacker per infiltrarsi in organizzazioni globali. Rilevati falsi repository su GitHub e GitLab che ingannano gli sviluppatori. Scoperto "PromptLock", un ransomware potenziato dall'intelligenza artificiale.

CVE di Impatto Elevato

Identificate numerose CVE critiche e ad alto impatto questa settimana, con particolare attenzione a router e dispositivi IoT, plugin WordPress e software enterprise. Tra queste: CVE-2025-9012 (Tenda AC9 Router), CVE-2025-9077 (VMware vCenter), CVE-2025-9188 (Microsoft Exchange) e CVE-2025-9341 (D-Link DIR-878).

1.2 Analisi degli Attacchi Rilevati

Phishing e Ransomware

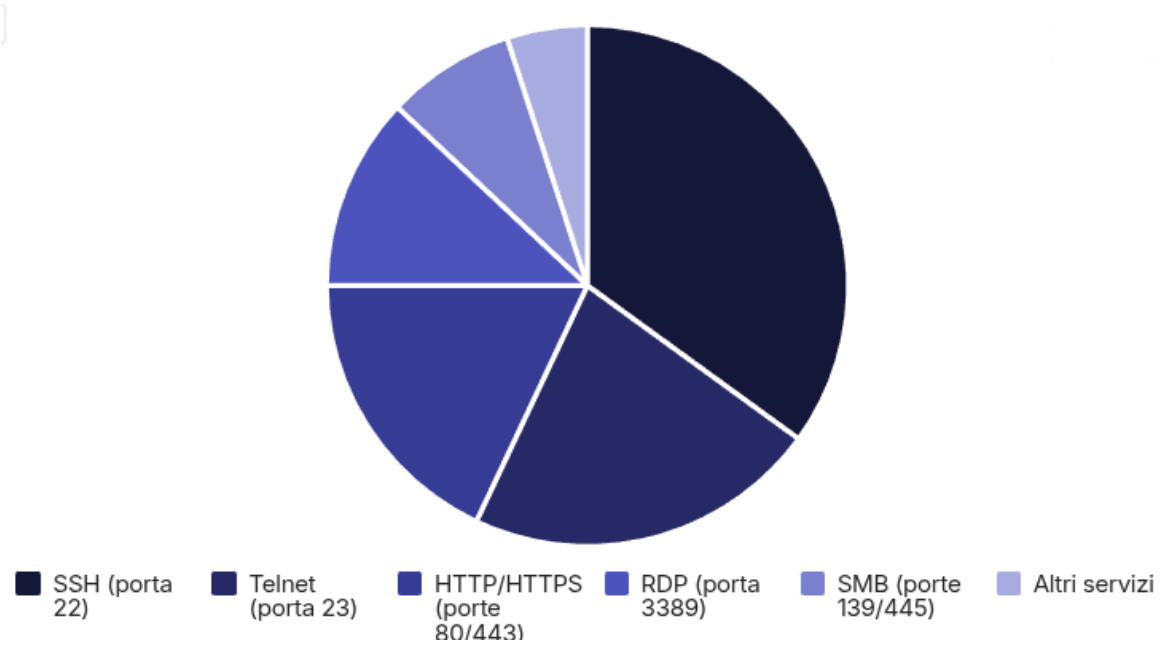
Campagne di phishing mirate a utenti italiani con email spoofate che impersonano notifiche di scadenza password. L'analisi dettagliata di un caso ha rivelato l'uso di bounce tracking attraverso domini legittimi per dirigere le vittime verso pagine di credential harvesting. Per quanto riguarda i ransomware, si osserva un'elevata attività dei gruppi Black Basta e LockBit, con aumenti significativi negli attacchi rispetto alla settimana precedente.

Malware e Data Breach

I cinque malware più attivi nell'ultima settimana includono Storm-0501, TamperedChef e APT36. Particolarmente preoccupante è Storm-0501, un gruppo RaaS che ha spostato il focus dagli ambienti on-premise ai servizi cloud. Segnalati importanti data breach, tra cui quello di TransUnion negli Stati Uniti, che ha compromesso dati personali di oltre 4,4 milioni di consumatori, e un possibile attacco a Eco Demolizioni S.r.l. in Italia.

1.3 Monitoraggio Honeypot e Rilevamenti

L'infrastruttura honeypot di S3K, distribuita strategicamente in Italia, Germania, Francia, Brasile, India e USA, ha registrato un significativo volume di attacchi nella settimana di riferimento. Questi sistemi, appositamente predisposti per la raccolta di dati sugli attacchi informatici, forniscono informazioni preziose sulle tecniche, le origini e gli obiettivi dei threat actor.



Gli honeypot italiani hanno registrato un'intensa attività di scanning e tentativi di accesso, con una predominanza di attacchi diretti verso servizi SSH e Telnet. L'analisi geografica rivela che Russia, Cina e Stati Uniti figurano tra i principali paesi di origine degli attacchi, seguiti da Germania e Brasile.

Tendenze DDoS

Gli attacchi DDoS hanno mostrato un incremento del 15% rispetto alla settimana precedente, con una particolare concentrazione verso gli Stati Uniti, Germania e Cina. Le tipologie di attacco più comuni sono state UDP Flood, SYN Flood e HTTP Flood, con un significativo aumento degli attacchi a livello applicativo rispetto a quelli a livello di rete.

Attività di Defacement

Rilevati numerosi attacchi di defacement contro siti web italiani, con una media di 12 attacchi giornalieri. I gruppi più attivi includono xNot_RespondinGx e altri collettivi hacktivisti. Questi attacchi, pur avendo un impatto limitato sulla disponibilità dei servizi, rappresentano un rischio significativo per la reputazione delle organizzazioni colpite.

IP Attaccanti Principali

L'analisi degli indirizzi IP più aggressivi ha evidenziato una concentrazione di attività malevole da parte di un numero limitato di sorgenti. In particolare, gli IP 178[.]162[.]136[.]160 e 103[.]159[.]133[.]164 hanno eseguito rispettivamente 199 e 149 tentativi di attacco contro l'honeypot italiano N.2, principalmente mirati a servizi SSH e web.

Raccomandazioni di Sicurezza

- Applicare immediatamente le patch di sicurezza rilasciate da ISC, Cisco e Google per mitigare le vulnerabilità critiche identificate.
- Rafforzare i controlli di autenticazione, implementando MFA dove possibile, in particolare per servizi esposti su internet.
- Aumentare la consapevolezza degli utenti sui rischi di phishing, con particolare attenzione alle false notifiche di scadenza password.
- Monitorare attentamente il traffico di rete per identificare comportamenti anomali, in particolare verso i servizi maggiormente presi di mira (SSH, Telnet, HTTP/HTTPS).
- Implementare segmentazione di rete e controlli di accesso granulari per limitare l'impatto potenziale di un'eventuale compromissione.

2 Security news

2.1 Rilasci aggiornamenti e patch

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

PRODOTTO	DESCRIZIONE

Kea DHCP	ISC ha rilasciato aggiornamenti di sicurezza per sanare una vulnerabilità con gravità "alta" in Kea DHCP. Tale vulnerabilità, qualora sfruttata, potrebbe consentire a utenti malintenzionati di compromettere la disponibilità dei sistemi target.
	Prodotti e/o versioni affette
	• ISC Kea DHCP
	  ○ 2.7, versioni dalla 2.7.1 alla 2.7.9
	  ○ 3.0, versioni precedenti alla 3.0.1
	  ○ 3.1, versioni precedenti alla 3.1.1

ULR/Note	• https://kb.isc.org/docs/cve-2025-40779

PRODOTTO	DESCRIZIONE

Cisco	Aggiornamenti di sicurezza sanano molteplici nuove vulnerabilità, di cui due con gravità "alta", che riguardano diversi prodotti Cisco.
	
	Prodotti e versioni affette
	• Cisco
	  ○ Switch Nexus Serie 3000
	  ○ Switch Nexus Serie 9000 in modalità NX-OS standalone
	  ○ Catalyst Serie 8300 Edge uCPE
	  ○ UCS Manager Software
	  ○ Blade Server UCS B-Series
	  ○ Rack Server UCS C-Series M6, M7, and M8
	  ○ UCS E-Series Servers M6
	  ○ UCS X-Series Modular System

ULR/Note	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n39k-isis-dos-JhJA8Rfx: apre un link esterno • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-vkvmorv-CnKrV7HK: apre un link esterno • https://sec.cloudapps.cisco.com/security/center/publicationListing.x

PRODOTTO	DESCRIZIONE

Google Chrome	Google ha rilasciato un aggiornamento per il browser Chrome al fine di correggere una vulnerabilità di sicurezza con gravità "critica". Tale vulnerabilità, qualora sfruttata, potrebbe consentire ad un utente malintenzionato remoto di eseguire codice arbitrario sui sistemi target.
	
	• Google Chrome
	  ○ versioni precedenti alla 139.0.7258.154/.155 per Windows e Mac
	  ○ versioni precedenti alla 139.0.7258.154 per Linux

ULR/Note	• https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_26.html

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

SINDOOR DROPPER: IL MALWARE LINUX CHE SFRUTTA LE TENSIONI GEOPOLITICHE

Nelle ultime settimane è stato individuato un nuovo malware progettato per colpire i sistemi Linux battezzato "Sindoor Dropper". La sua particolarità non sta soltanto nella tecnica di infezione, ma anche nel contesto geopolitico a cui si lega: il codice malevolo sfrutta infatti l'attuale clima di tensione tra India e Pakistan per attirare le vittime, utilizzando messaggi e documenti che richiamano al conflitto in corso. Il vettore di attacco principale è rappresentato da file Linux con estensione *.desktop*, normalmente utilizzati per lanciare applicazioni o script. In questo caso, però, dietro l'apparenza di file innocui si nasconde un meccanismo capace di avviare comandi Bash che scaricano e installano ulteriori componenti malevoli. Una volta attivato, il dropper apre la strada a un payload personalizzato che garantisce agli attaccanti l'accesso remoto al sistema compromesso.

Sindoor Dropper non si limita a penetrare nelle macchine bersaglio, ma implementa anche tecniche di persistenza: attraverso modifiche all'avvio automatico o l'utilizzo di cronjob, riesce a mantenersi attivo nel tempo e a sopravvivere ai riavvii del sistema. Questo consente agli aggressori di continuare a raccogliere informazioni, monitorare le attività della vittima ed eventualmente distribuire ulteriori moduli malevoli.

L'emergere di minacce di questo tipo conferma come Linux, un tempo percepito come un ambiente più sicuro rispetto a Windows, sia ormai entrato a pieno titolo nel mirino dei gruppi di cyber-spionaggio. L'obiettivo non è soltanto quello di sottrarre dati sensibili, ma anche di creare instabilità, colpendo le infrastrutture tecnologiche in momenti già caratterizzati da tensioni politiche e militari.

Per le organizzazioni che utilizzano Linux in ambienti strategici, questo caso rappresenta un campanello d'allarme. È fondamentale rafforzare le difese implementando controlli sugli script eseguiti, monitorando i processi sospetti e formando il personale sui rischi legati alle campagne di phishing. La vicenda dimostra come i conflitti del presente non si giochino soltanto sul piano militare o diplomatico, ma trovino nel cyberspazio un terreno di scontro altrettanto rilevante, dove la preparazione e la consapevolezza diventano armi decisive.

HACKER SFRUTTANO LA FALLA CITRIX: CRESCE LA MINACCIA A LIVELLO GLOBALE

Una grave vulnerabilità nei sistemi Citrix ha attirato l'attenzione della comunità di sicurezza informatica: gruppi di hacker stanno già sfruttando la falla per infiltrarsi nei sistemi di organizzazioni in tutto il mondo. Il difetto, individuato nei servizi di accesso remoto e nelle soluzioni per la virtualizzazione, consente a un attaccante di ottenere privilegi elevati e di muoversi liberamente all'interno delle reti aziendali.

Il rischio è particolarmente elevato perché Citrix è ampiamente utilizzato in ambienti critici, dal settore finanziario alla pubblica amministrazione, fino alle infrastrutture sanitarie. La possibilità per un cybercriminale di compromettere questi sistemi non riguarda solo la perdita di dati, ma può tradursi anche in interruzioni operative e gravi conseguenze per la continuità dei servizi.

Gli hacker hanno dimostrato estrema rapidità nell'adozione di questa vulnerabilità, integrandola nelle loro campagne di intrusione. Una volta ottenuto l'accesso iniziale, possono installare malware, creare backdoor per accessi futuri o utilizzare le macchine compromesse come punto di partenza per spostarsi lateralmente e compromettere ulteriori dispositivi all'interno della rete.

La criticità della situazione è accresciuta dal fatto che molti sistemi Citrix risultano ancora esposti perché non aggiornati. Le patch correttive sono state rilasciate, ma l'applicazione non è sempre immediata, soprattutto in realtà complesse dove l'interruzione dei servizi può avere un impatto significativo. Questo ritardo fornisce agli attaccanti una finestra temporale preziosa per sfruttare la falla e consolidare la loro presenza.

Il caso mette in evidenza, ancora una volta, come le vulnerabilità nei sistemi diffusi a livello globale possano trasformarsi in una corsa contro il tempo: da una parte i team di sicurezza che corrono per aggiornare e proteggere i sistemi, dall'altra i criminali che approfittano delle falle prima che vengano chiuse. In questo scenario, la velocità di reazione delle aziende diventa determinante per ridurre l'impatto degli attacchi e limitare i danni.

GITHUB E GITLAB NEL MIRINO: I FALSI REPOSITORY INSIDIANO GLI SVILUPPATORI

Il mondo dello sviluppo software è sempre più al centro delle attenzioni dei cybercriminali. Negli ultimi mesi si è registrato un aumento significativo di attacchi mirati contro piattaforme come GitHub e GitLab, due strumenti fondamentali per la collaborazione e la condivisione di codice. La tecnica utilizzata dagli attaccanti è tanto semplice quanto efficace: la creazione di repository falsi che imitano progetti legittimi e inducono gli sviluppatori a scaricare codice compromesso.

Questi repository, costruiti con grande cura per apparire autentici, possono contenere librerie malevole o script nascosti che, una volta integrati nei progetti degli sviluppatori, aprono la porta a backdoor, furti di credenziali e compromissione dell'intera catena di sviluppo. L'impatto di un singolo errore può essere devastante: un componente malevolo introdotto in fase di programmazione può diffondersi rapidamente, arrivando fino ai prodotti distribuiti agli utenti finali.

Gli attacchi contro gli ambienti DevOps non sono casuali. Colpire direttamente gli sviluppatori significa infiltrarsi nei processi di produzione software, un punto nevralgico che garantisce un accesso privilegiato alle infrastrutture aziendali e, in molti casi, a migliaia di utenti. Questo spiega perché la "supply chain software" sia ormai considerata una delle superfici di attacco più critiche e più redditizie per i criminali informatici.

La strategia degli aggressori si basa sulla fiducia implicita che gli sviluppatori ripongono nei repository pubblici. In ambienti caratterizzati da scadenze serrate e necessità di riutilizzare codice, è facile cadere nell'inganno di scaricare una libreria apparentemente utile senza controllarne a fondo l'origine. Una volta introdotto il codice infetto, individuare e rimuovere l'intrusione diventa estremamente complesso.

Questi episodi rappresentano un campanello d'allarme: serve maggiore attenzione alla sicurezza della supply chain, con controlli più rigorosi sui repository, strumenti di analisi automatizzata del codice e linee guida che incentivino le buone pratiche tra gli sviluppatori. Solo così sarà possibile ridurre i rischi di un settore che, per la sua centralità, resta uno degli obiettivi privilegiati della criminalità informatica.

PROMPTLOCK: IL RANSOMWARE POTENZIATO DALL'INTELLIGENZA ARTIFICIALE

Una nuova minaccia si affaccia nel panorama della cybersecurity: si chiama PromptLock ed è un ransomware che sfrutta l'intelligenza artificiale per aumentare la propria efficacia e ridurre i tempi di attacco. Diversamente dai ransomware tradizionali, che seguono procedure standard di cifratura e richiesta di riscatto, questo nuovo ceppo integra modelli di AI capaci di adattare il comportamento del malware in base al contesto in cui si trova.

PromptLock è in grado, ad esempio, di personalizzare i messaggi di riscatto per renderli più convincenti, modulando linguaggio e tono in funzione della vittima. Non solo: l'intelligenza artificiale può anche analizzare i sistemi colpiti, identificare i file più critici e prioritari da cifrare e scegliere la strategia di ricatto più efficace. Questo approccio aumenta la pressione sulle organizzazioni, costrette a valutare con urgenza se pagare o meno per recuperare i propri dati.

Un altro elemento preoccupante è la rapidità con cui il ransomware riesce a diffondersi e consolidarsi all'interno delle reti compromesse. Grazie all'automazione basata su AI, il malware può muoversi lateralmente, individuare nuove macchine vulnerabili e attivare meccanismi di difesa contro i sistemi di rilevamento. L'obiettivo è massimizzare i danni prima che le contromisure possano entrare in azione.

La comparsa di PromptLock segna un passo ulteriore nell'evoluzione delle minacce informatiche: la combinazione tra ransomware e intelligenza artificiale rappresenta infatti un salto qualitativo, che rende più complesso il lavoro dei difensori. Non si tratta più soltanto di malware che seguono schemi prevedibili, ma di strumenti capaci di apprendere e adattarsi, rendendo gli attacchi meno individuabili e più difficili da contenere.

Questo scenario sottolinea l'urgenza di un cambio di paradigma nelle difese: alle tecniche tradizionali vanno affiancati sistemi avanzati di rilevamento basati anch'essi sull'AI, insieme a strategie di resilienza che includano backup regolari, segmentazione delle reti e una solida formazione del personale. Solo così sarà possibile fronteggiare una minaccia che unisce tecnologia avanzata e logiche criminali, trasformando il ransomware in un'arma ancora più sofisticata.

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 25 Agosto – 1 Settembre 2025

Questa settimana si registra un numero medio di CVE CRITICAL & HIGH, con forte presenza di vulnerabilità nei router e dispositivi IoT, diversi casi su WordPress plugin e nuove segnalazioni su software enterprise (VMware, Microsoft).
Sono stati pubblicati exploit PoC per varie CVE, aumentando la priorità di patching.

CVE ad Alto Impatto (CRITICAL & HIGH)

CVE ID	Severità	Data Pubblicazione	Exploit Pubblico	Prodotto Coinvolto	Descrizione Sintetica
CVE-2025-9012	CRITICAL	26/08/2025	✅	Tenda AC9 Router	Stack overflow in formexeCommand (RCE)
CVE-2025-9077	CRITICAL	27/08/2025	❌	VMware vCenter	Privilege escalation tramite API
CVE-2025-9154	HIGH	27/08/2025	✅	WordPress WPBakery Plugin	Stored XSS su shortcode builder
CVE-2025-9188	CRITICAL	28/08/2025	❌	Microsoft Exchange	SSRF in servizio autodiscover
CVE-2025-9266	HIGH	29/08/2025	✅	WordPress LearnPress	SQLi in gestione corsi

CVE-2025-9320	HIGH	30/08/2025	❌	Oracle WebLogic	Deserialization RCE
CVE-2025-9341	CRITICAL	31/08/2025	✅	D-Link DIR-878	Command injection in gestione WAN

Distribuzione Giornaliera

- **26 agosto**: Router Tenda (overflow critico con PoC pubblico)
- **27 agosto**: VMware vCenter escalation + WordPress WPBakery (XSS)
- **28 agosto**: Microsoft Exchange (SSRF critico)
- **29 agosto**: SQLi su LearnPress (WordPress)
- **30 agosto**: Oracle WebLogic RCE via deserialization
- **31 agosto**: Command injection su router D-Link

Vendor e Tecnologie Coinvolti

- **Dispositivi IoT/Router**: Tenda e D-Link colpiti da RCE e command injection.
- **WordPress Plugin**: WPBakery e LearnPress vulnerabili a XSS e SQLi.
- **VMware vCenter**: Escalation privilegi tramite API.
- **Microsoft Exchange**: SSRF su autodiscover, rischio alto per esposizione su internet.
- **Oracle WebLogic**: RCE tramite oggetti serializzati.

Raccomandazioni Operative

Patch Prioritarie

- Router Tenda/D-Link → aggiornamento firmware immediato, WAN chiusa.
- WordPress plugin → aggiornare WPBakery e LearnPress; se non patchato, disabilitare.
- VMware vCenter → aggiornare e rafforzare autenticazioni API.
- Microsoft Exchange → applicare fix SSRF e monitorare autodiscover.
- Oracle WebLogic → mitigare RCE disabilitando deserialization non sicure.

Monitoraggio Consigliato

- Controllo log anomali su endpoint WordPress (/wp-admin/*, shortcode, course.php).
- SIEM: query su exploit noti per RCE/SSRF.
- IDS/IPS per signature PoC rilasciati su router Tenda/D-Link.

3.2 Tendenze

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

CVE	PRODOTTO	CVSS V3
CVE-2025-57819	FreePBX (centralino telefonico (PBX) open-source)	N/A
CVE-2025-43300	• macOS Sonoma 14.7.8 • macOS Ventura 13.7.8 • macOS Sequoia 15.6.1 • iPadOS 17.7.10 • iOS 18.6.2 • iPadOS 18.6.2	N/A
CVE-2025-29824	Driver Windows Common Log File System	N/A
CVE-2024-7206	eWeLink (dispositivi smart home)	N/A
CVE-2025-8067	UDisks daemon (dischi e dispositivi di archiviazione, sistemi Linux)	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-2025-48963	Acronis Cyber Protect Cloud Agent (per Linux, macOS e Windows)	N/A
VULNERABILITÀ	Escalation locale dei privilegi dovuta a una gestione impropria dei collegamenti simbolici (soft link).	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-54857	SkyBridge BASIC MB-A130 (Versione 1.5.8 e precedenti)	N/A
VULNERABILITÀ	Esiste una vulnerabilità di tipo "iniezione di comandi del sistema operativo" (OS Command Injection) a causa di una neutralizzazione impropria degli elementi speciali utilizzati in un comando di sistema operativo.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-6507	h2oai/h2o-3 — piattaforma open-source per machine learning e intelligenza artificiale sviluppata da H2O.ai.	N/A
VULNERABILITÀ	Una vulnerabilità nel repository h2oai/h2o-3 consente agli attaccanti di sfruttare la deserializzazione di dati non affidabili, con potenziale esecuzione arbitraria di codice e lettura di file di sistema.	

CVE	PRODOTTI	SCORE CVSS NIST
CVE-2025-9491	Microsoft Windows	N/A
VULNERABILITÀ	Vulnerabilità di esecuzione remota di codice (Remote Code Execution) tramite falsa rappresentazione dell'interfaccia utente nei file LNK di Microsoft Windows. Questa vulnerabilità consente ad attaccanti remoti di eseguire codice arbitrario sulle installazioni vulnerabili di Microsoft Windows. Per sfruttare la vulnerabilità è richiesta l'interazione dell'utente, che deve visitare una pagina web malevola o aprire un file malevolo. Il difetto specifico riguarda la gestione dei file con estensione .LNK. Dati appositamente creati all'interno di un file .LNK possono far sì che contenuti pericolosi nel file risultino invisibili all'utente che li esamina tramite l'interfaccia utente fornita da Windows.	

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-2025-48384
DESCRIZIONE	
Git aveva una vulnerabilità nella gestione dei ritorni a capo nei percorsi dei sottomoduli che poteva far estrarre i sottomoduli in posizioni sbagliate. Questo, in combinazione con symlink e script post-checkout eseguibili, poteva portare all'esecuzione involontaria di codice. La vulnerabilità è stata corretta a partire dalle versioni 2.43.7 fino alla 2.50.1.	

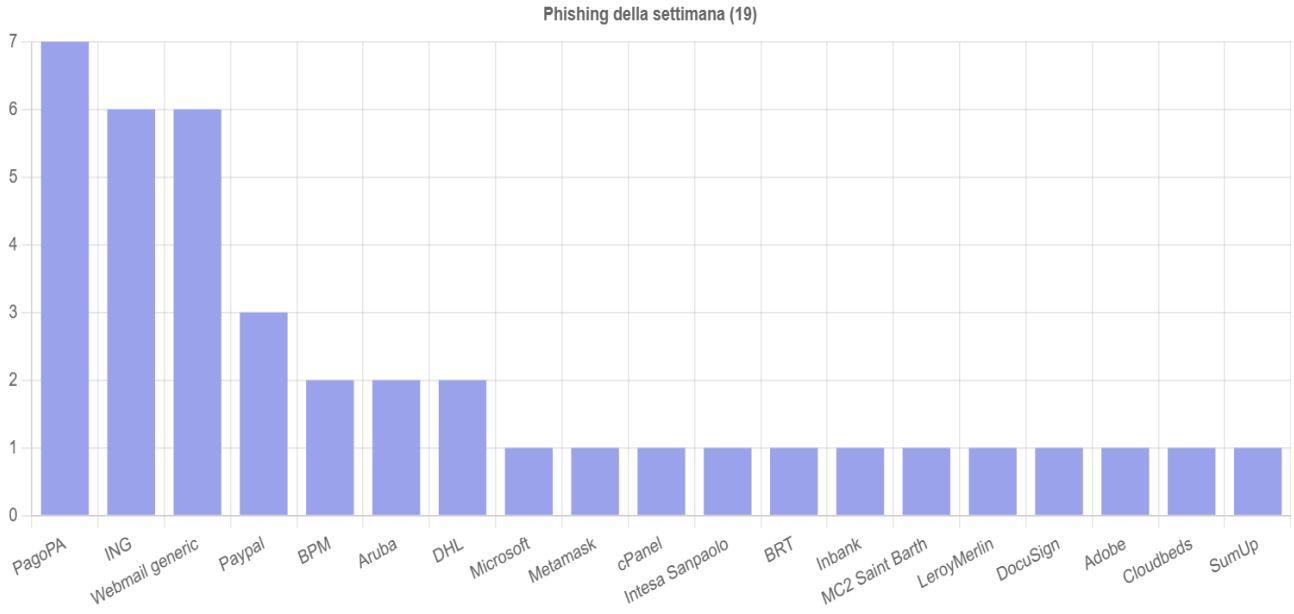
CVE	CVE-2025-57819
DESCRIZIONE	
FreePBX è un software per la gestione di centralini telefonici che offre un'interfaccia web per amministrare il sistema. In alcune versioni, non vengono controllati adeguatamente i dati inseriti dagli utenti, permettendo a un attaccante non autenticato (cioè, senza bisogno di login) di accedere all'amministrazione. Da lì, l'attaccante può modificare il database in modo arbitrario (es. cambiare configurazioni, inserire dati malevoli) e perfino eseguire codice a distanza sul server, compromettendo completamente il sistema.	

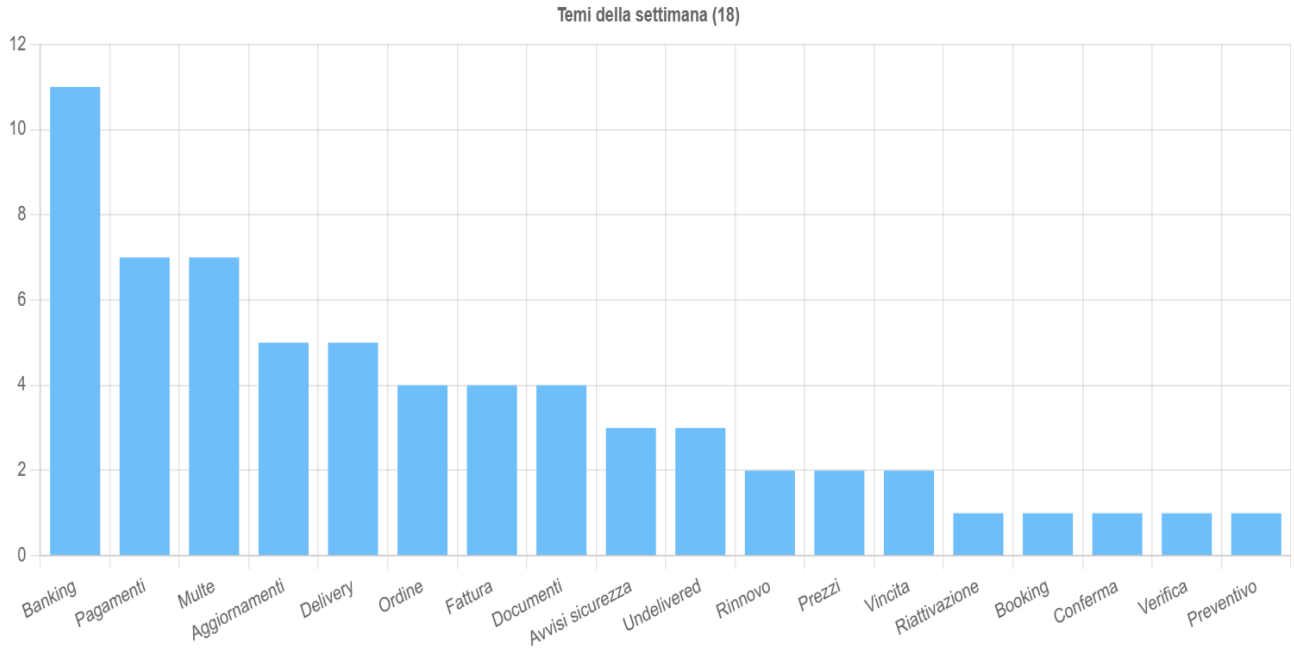
4 Attacchi

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.

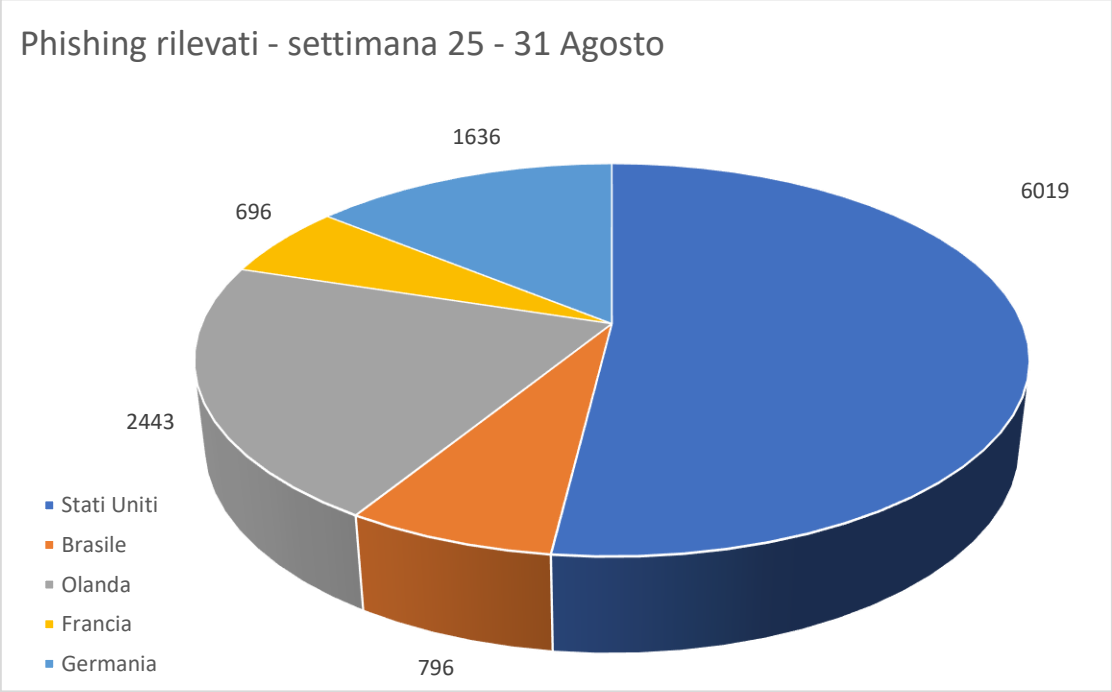




Fonte :CERT-AGID

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.

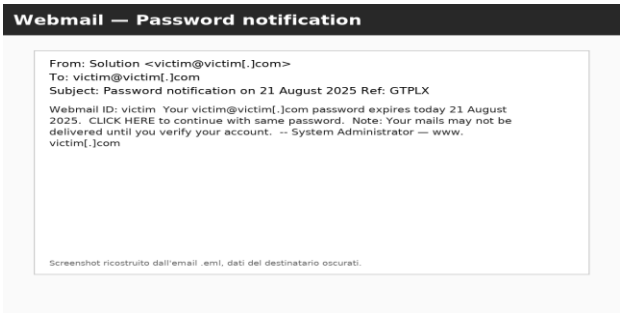


Report Analisi Email Spoofata

Analisi email di phishing "Password notification on 21 August 2025 Ref: GTPLX" (EML)

- Sintesi esecutiva.

L'email analizzata è una finta notifica "webmail password expiry" inviata al destinatario interno con mittente spoofato sullo stesso dominio del destinatario. Il messaggio spinge a cliccare un pulsante "CLICK HERE" che redirige verso un percorso sospetto su blog.authorpods[.]com attraverso un bounce di tracciamento da analytics.oemsecrets[.]com. Gli header non riportano risultati SPF/DKIM/DMARC, indizio di inoltro/inganno; il Return-Path coincide con l'indirizzo spoofato. L'host di invio nei Received risulta un VM Google Cloud (34[.]127[.]49[.]253). Lo schema è classico credential harvesting su finti portali webmail. Non risultano allegati.



- Contesto e fonti

L'analisi è stata condotta partendo dal file .eml fornito, integrando verifiche OSINT su dominio/IP/URL, reputazione e possibili compromissioni del sito di destinazione. Estratti chiave dell'email (header e corpo) che supportano i rilievi sono citati di seguito.

- Header, catena di consegna e autenticazioni
  Dalla traccia Received si osserva:
  - Consegna locale e inoltri interni, quindi ricezione sul dominio target [.]it (nel report sostituito con victim[.]com).
  - Origine applicativa da host localhost.localdomain → 253.49.127[.]34.bc.googleusercontent[.]com (IP 34[.]127[.]49[.]253), indicativo di istanza Google Cloud.
  - Assenza nei metadati visibili di risultati SPF/DKIM/DMARC (Authentication-Results non presente).
  - Return-Path e From coincidono con l'indirizzo dell'utente interno.
- Estratti rilevanti:
  - Received: from localhost.localdomain (253.49.127[.]34.bc.googleusercontent[.]com [34.127.49[.]253]) ...
  - From: Solution <victim@victim[.]com>
  - To: victim@victim[.]com>
  - Subject: Password notification ...
  - Content-Type: text/html (nessun allegato).
- Osservazione "mittente = destinatario" (dominio coincidente).
  Nel messaggio il dominio del mittente spoofato coincide con quello del destinatario. In questo report tali riferimenti sono pseudonimizzati in victim[.]com e l'utente come victim. Lo schema è tipico dei self-phish: l'attaccante falsifica il brand aziendale per accrescere fiducia e il tasso di clic.
- Geolocalizzazione/Hosting mittente.
  L'IP 34[.]127[.]49[.]253 risolve in *.bc.googleusercontent[.]com (Google Cloud). Vedi panoramica del blocco /24 che elenca gli hostname bc.googleusercontent[.]com su questa rete. (ipinfo.io)
- Contenuto e tecnica di ingegneria sociale
  Il corpo del messaggio è HTML minimale brandizzato come "Webmail", annuncia la scadenza odierna della password "today 21 August 2025" e minaccia mancata consegna email se non si verifica l'account. È presente una call-to-action "CLICK HERE" che rimanda a un URL complesso con parametro event_link= che a sua volta punta a un percorso sotto blog.authorpods[.]com. Il

frammento #*****...dXRpb24uaXQ= è Base64 che decodifica l'indirizzo del destinatario (qui pseudonimizzato in victim@victim[.]com), tipico per pre-popolare il form di phishing.

- Schema tecnico.
  - Pretesto: scadenza password webmail.
  - Urgenza/Minaccia: possibile mancata consegna finché non si "verifica l'account".
  - Brand impersonation interna: usa victim[.]com come mittente visuale.
  - Redirect chaining: uso di analytics.oemsecrets[.]com come bouncer verso la pagina malevola su blog.authorpods[.]com.
  - Email harvesting: Base64 nell'ancora # con l'email della vittima.
- Artefatti e reputazione (OSINT)
  - URL e domini coinvolti

    Dall'EML emerge un singolo bottone di azione:
    - Prima tappa (bouncer/tracking): https://analytics.oemsecrets[.]com/main.php?...&event_link=... (dominio noto dell'aggregatore OEMsecrets, legittimo; l'uso come redirect può essere abusato per far passare il click da un hostname "pulito"). Informazioni sulla piattaforma OEMsecrets: sito ufficiale, schede e articoli di settore che ne confermano la legittimità commerciale. (oemsecrets.com, EE Times, FineEngineering Magazine, exhibitors.electronica.de)
    - Destinazione finale (landing): https://blog.authorpods[.]com/divine/index.html#<base64 di victim@victim[.]com>: il sottodominio blog.authorpods[.]com appare essere un WordPress; risultano report pubblici urlquery che indicano percorso anomalo sotto wp-includes/widgets/z/mail/.../webma/index.html, tipico di webshell/drop o kit phishing posizionato in una directory non standard. Questo è fortemente suggeritivo di compromissione del sito/blog. (UQA, Urlquery, UrlQuery)

Nota: i report urlquery mostrano schermate e percorsi specifici sotto blog.authorpods[.]com/wp-includes/.../mail/webma/index.html, correlabili allo schema di "webmail login spoof". Anche se la CTI non è un giudizio forense definitivo, la presenza del path anomalo dentro wp-includes/ rafforza l'ipotesi compromise & host-as-a-service per kit di phishing. (UQA, UrlQuery)

  - IP di invio (Google Cloud)

    34[.]127[.]49[.]253 — reverse 253.49.127.34.bc.googleusercontent.com; blocco /24 in Google Cloud. Non sono emersi (con gli strumenti accessibili pubblicamente in questa sede) report specifici su questo IP, ma l'infrastruttura è comune nei campaign kits per invii massivi o app di invio. (ipinfo.io)
  - Reputazione su VT / OTX / PhishTank / AbuseIPDB
    - URL/Domain — blog.authorpods[.]com: evidenze urlquery su path d'interesse (vedi sopra).
    - URL/Domain — analytics.oemsecrets[.]com: dominio legittimo (aggregatore di componenti). L'uso come redirect va trattato come *potentially unwanted* nella

catena di attacco, non come origine malevola. (oemsecrets.com, FineEngineering Magazine)

- IP 34[.]127[.]49[.]253: rete Google Cloud; La consultazione diretta di AbuseIPDB e OTX mostra la presenza di alcune segnalazioni recenti su AbuseIPDB. Riferimenti: home di AbuseIPDB; vista IPinfo della subnet. (abuseipdb.com, ipinfo.io)

- Link operativi delle analisi (copiabili):
  - urlquery (report blog[.]authorpods): https://uqa.urlquery[.]net/report/4608b60f-eda5-4d3a-a86d-479befb8ec04
  - urlquery (indice report correlati): https://mobile.urlquery[.]net/report/e71dd483-a67b-4101-b3b6-daec20f59e98
  - OEMsecrets (sito ufficiale): https://www.oemsecrets[.]com/
  - OEMsecrets (intervista / profilo): https://easyengineering[.]eu/interview-with-oemsecrets-com/
  - IPinfo subnet 34[.]127[.]49[.]0/24: https://ipinfo[.]io/ips/34.127.49.0/24
  - AbuseIPDB (home per query IP): https://www.abuseipdb[.]com/
- WHOIS / Registrazione domini e TLS
  - victim[.]com (dominio target [.]it) — dominio interno/aziendale (dettagli omessi e pseudonimizzati). L'uso come mittente senza allineamento SPF/DKIM/DMARC osservabile nell'EML suggerisce spoofing o inoltro non autenticato.
  - authorpods[.]com — presenza di un sito "AuthorPods" legato al mondo libri/autori, con blog blog.authorpods[.]com. Le evidenze OSINT indicano possibile compromissione del blog WordPress (cfr. urlquery). (blog.authorpods .com, UQA)
  - oemsecrets[.]com — società UK di comparazione prezzi componenti, attiva da anni, con presenza a fiere e API pubbliche; dominio legittimo. (exhibitors.electronica.de, PR Newswire, EE Times)
- TLS/Certificati.
  Le pagine https://blog.authorpods[.]com/... risultano servite in HTTPS; non sono stati riscontrati dettagli di misconfigurazione del certificato. La combinazione "WordPress + path anomali sotto wp-includes + redirect da dominio terzo" resta l'indicatore tecnico più forte di kit installato. (Per un riscontro completo si consiglia scansione con SSL Labs e verifica CT logs). (UQA)
- Allegati
  Non presenti: Content-Type: text/html; charset=UTF-8 senza multipart né attachment. Nessuna analisi hash/VT/joesandbox è applicabile in assenza di file.
- Indicatori di Compromissione (IoC)
  (Tutti i puntini sono sostituiti con [.] su domini/IP/email)
  - Mittente visuale spoofato: victim@victim[.]com (corrisponde al destinatario).
  - Host di invio osservato nei Received: 34[.]127[.]49[.]253 — 253.49.127[.]34.bc.googleusercontent[.]com.
  - Bouncer/redirect: analytics.oemsecrets[.]com (legittimo, usato nella catena).

- Landing sospetta (kit webmail): blog.authorpods[.]com/wp-includes/widgets/z/mail/webma/index.html e blog.authorpods[.]com/divine/index.html#<base64(victim@victim[.]com)>. (UQA, UrlQuery)
- Tabelle di riepilogo

Tabella A — Header e catena SMTP (estratto)

Elemento	Valore (pseudonimizzato)	Evidenza
From	Target <victim@victim[.]com>	EML
To	victim@victim[.]com	EML
Return-Path	<victim@victim[.]com>	EML
Received (origine)	localhost.localdomain (253.49.127[.]34.bc.googleusercontent[.]com [34.127.49[.]253])	EML
Autenticazioni	Nessun risultato SPF/DKIM/DMARC visibile	EML

Fonte: EML originale.

Tabella B — Artefatti URL/Dominio/IP e reputazione

Artefatto	Ruolo	Esito/Note	Fonti
analytics.oemsecrets[.]com	Redirect/ bounce tracking	Dominio legittimo (aggregatore componenti); probabile abuso come trampolino	(oemsecrets.com, FineEngineering Magazine)
blog.authorpods[.]com (path anomalo)	Landing phishing	Report urlquery evidenziano percorso wp-includes/.../mail/webma/	(UQA, UrlQuery)
34[.]127[.]49[.]253	IP invio	Rete Google Cloud (*.bc.googleusercontent[.]com)	(ipinfo.io)

- Valutazione complessiva
  - TLP: GREEN
  - Classificazione: Phishing (credential harvesting) mirato a casella webmail con brand interno per aumentare credibilità.
  - Vettore: link HTML con redirect tramite dominio legittimo e landing su WordPress compromesso.
  - Rischio immediato: sottrazione di credenziali posta aziendale, successivi BEC, abuso di rubrica, laterale su altri servizi SSO.
  - Confidenza: Alta (catena, contenuto e tracce urlquery sono coerenti).
- Raccomandazioni operative (difesa e risposta)
  - Bloccare IoC a livello proxy/DNS/EDR: domini e path indicati, includendo pattern blog.authorpods[.]com/wp-includes/*/mail/*/webma/*.
  - MTA / SEG: rafforzare SPF/DKIM/DMARC alignment; applicare p=reject/quarantine con ARC per preservare inoltri legittimi.

- Awareness interna: campagna mirata su "webmail password expiry" e link da domini insospettabili (es. servizi analytics).
- Threat-hunting: cercare HTTP(S) verso i path indicati e submissions di form verso domini non aziendali nella stessa finestra temporale.
- Segnalazione: opzionale notifica responsabile del sito authorpods[.]com circa possibile compromissione del blog WordPress.

- Evidenze visive e link alle analisi
  Screenshot ricostruito:

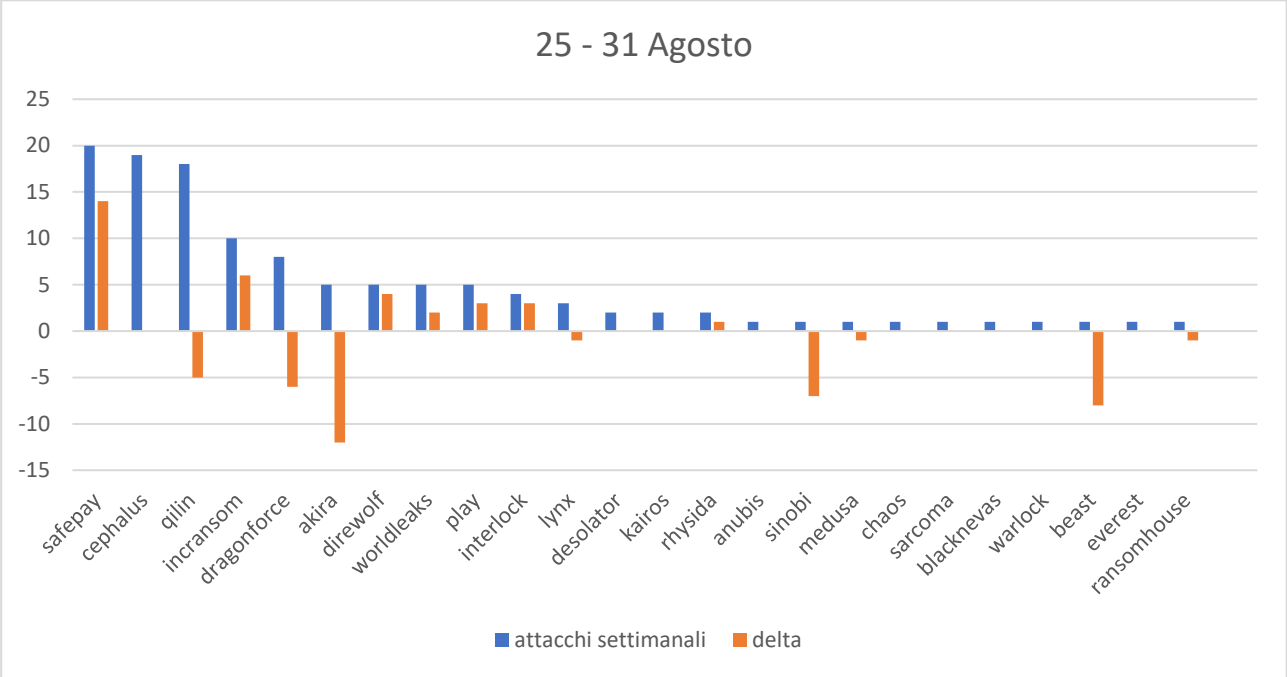
- Link (copiabili) alle analisi OSINT eseguite:
  - urlquery (report 1 - blog.authorpods): https://uqa.urlquery[.]net/report/4608b60f-eda5-4d3a-a86d-479befb8ec04
  - urlquery (indice/simili): https://mobile.urlquery[.]net/report/e71dd483-a67b-4101-b3b6-daec20f59e98
  - OEMsecrets (sito ufficiale): https://www.oemsecrets[.]com/
  - Intervista OEMsecrets: https://easyengineering[.]eu/interview-with-oemsecrets-com/
  - IPinfo — 34[.]127[.]49[.]0/24: https://ipinfo[.]io/ips/34.127.49.0/24
  - AbuseIPDB (home): https://www.abuseipdb[.]com/
  - Fonti di contesto su OEMsecrets/AuthorPods e settore (legittimità/uso): (oemsecrets.com, FineEngineering Magazine, blog.authorpods.com)
- Conclusioni
  L'email è indubbiamente malevola: simula una scadenza password per indurre la vittima a cliccare e inserire credenziali su una pagina fittizia ospitata su blog WordPress verosimilmente compromesso (blog.authorpods[.]com), raggiungibile dopo un redirect su host legittimo (analytics.oemsecrets[.]com). L'origine dell'invio risale a un host Google Cloud. La mancanza di evidenze SPF/DKIM/DMARC e il mittente = destinatario rafforzano la natura di spoofing interno. Nessun allegato è presente.

- Appendice — Estratti dall'EML (perizia minima)
    - Header chiave: From: Target <victim@victim[.]com>; To: victim@victim[.]com; Return-Path: <victim@victim[.]com>;
      Received: from localhost.localdomain (253.49.127[.]34.bc.googleusercontent[.]com [34.127.49[.]253]) ...
    - CTA/URL: ... CLICK HERE ... puntato a analytics.oemsecrets[.]com/...&event_link=https://blog.authorpods[.]com/divine/index.html#<base64>
    - Base64 nel frammento: decodifica all'email della vittima (qui victim@victim[.]com).

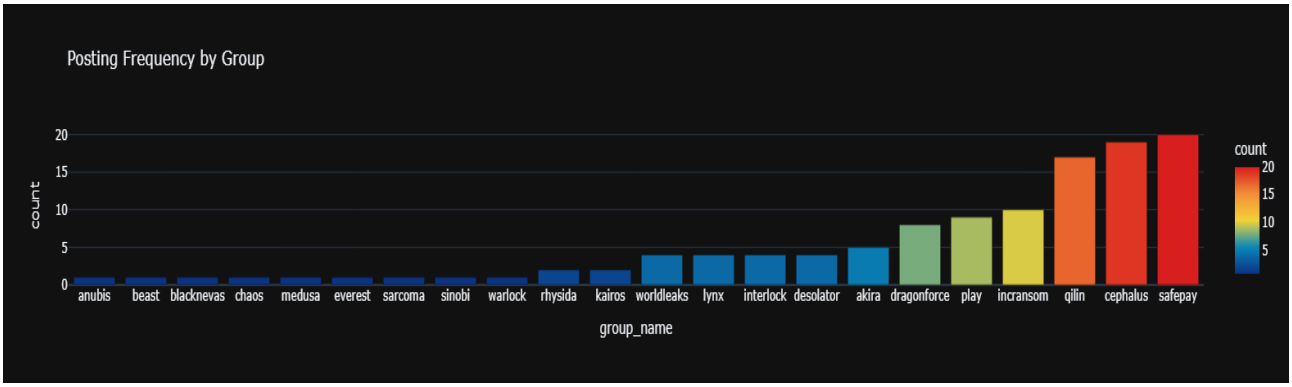
Nota sulla pseudonimizzazione: conformemente alle politiche di riservatezza, tutti i riferimenti al dominio e all'utente interni sono sostituiti rispettivamente con victim[.]com e victim. Il dominio mittente e quello di destinazione coincidono (spoofing interno); si è mantenuta la sostituzione per evitare esposizioni.

4.2 Ransomware

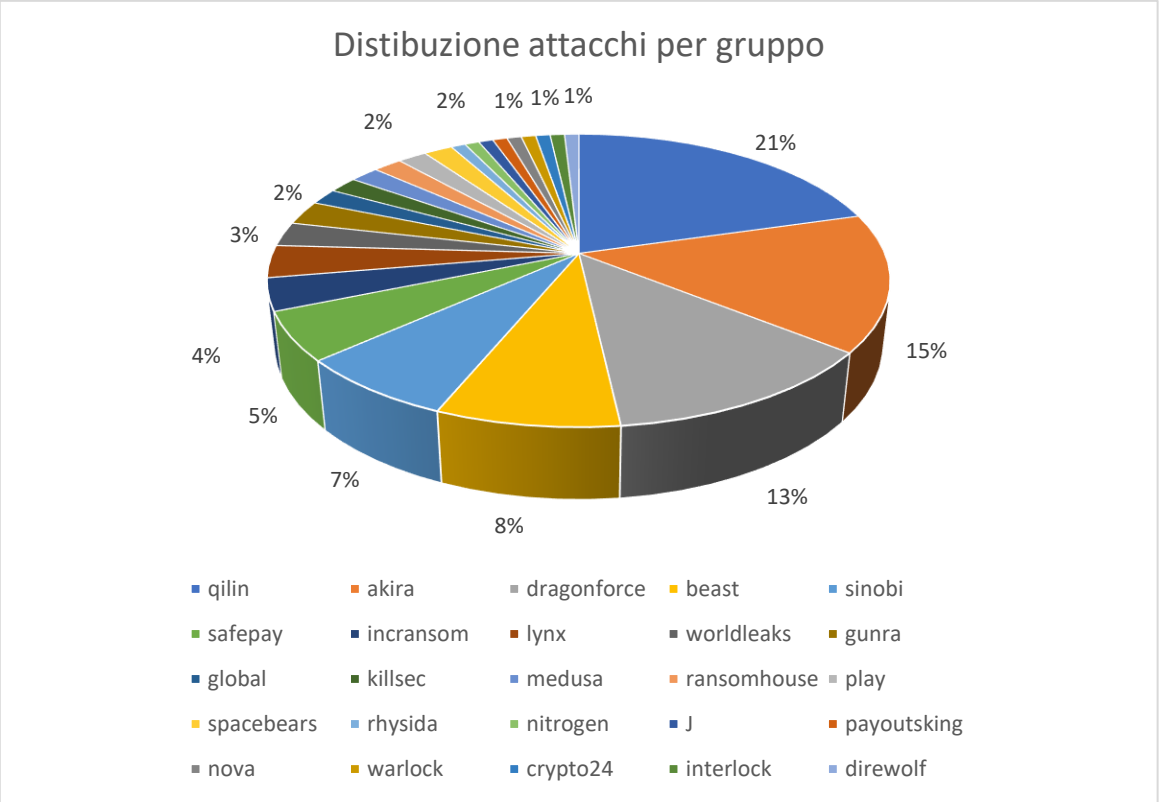
In questa sezione analizziamo il numero di attacchi di tipo ransomware emersi nella settimana di osservazione (25 – 31 Agosto). Il grafico sotto riportato evidenzia il numero di attacchi attribuiti ai gruppi hacker più attivi questa settimana (barra azzurra) e la variazione relativa alla settimana precedente (barra arancione).



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

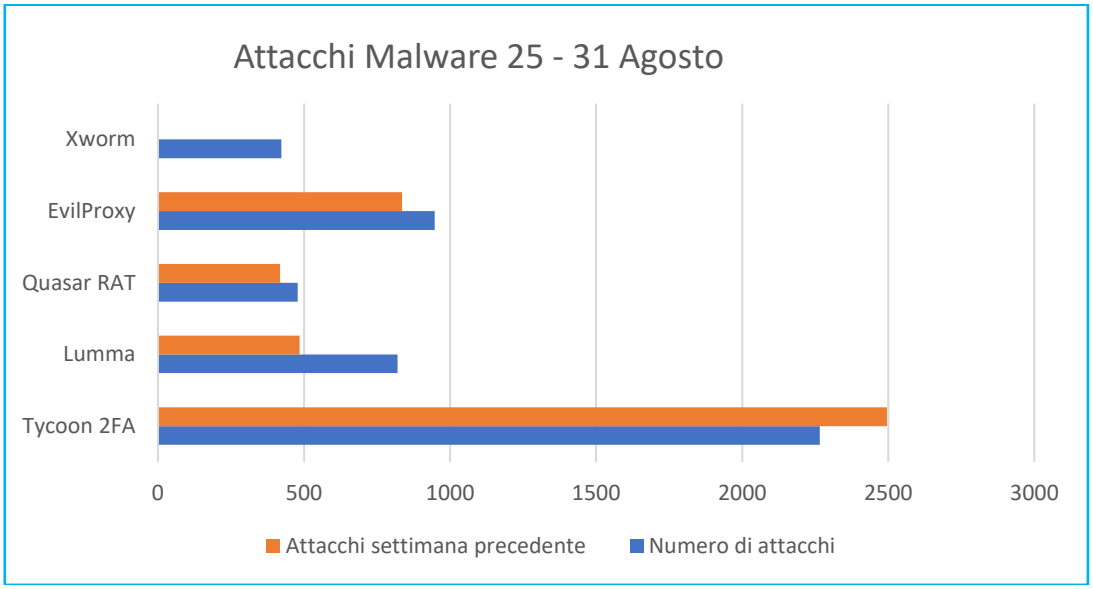


Nella pagina successiva un grafico che mostra la distribuzione percentuale degli attacchi attribuiti ai vari gruppi, sempre relativamente al periodo di osservazione sopra citato:


Distibuzione attacchi per gruppo
21%
15%
13%
8%
7%
5%
4%
3%
2%
2%
2%
1%
1%
1%
qilin
akira
dragonforce
beast
sinobi
safepay
incransom
lynx
worldleaks
gunra
global
killsec
medusa
ransomhouse
play
spacebears
rhysida
nitrogen
J
payoutsking
nova
warlock
crypto24
interlock
direwolf

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

- **Storm-0501**

Storm-0501 è un gruppo criminale specializzato in ransomware (RaaS) che ha recentemente spostato il suo focus dagli ambienti on-premise ai servizi cloud. In un attacco recente gli autori hanno sfruttato credenziali valide ed escalation dei privilegi in ambienti Microsoft Entra/Azure, esfiltrando dati e cancellando backup prima di chiedere il riscatto. L'attacco tipo di Storm-0501 vede un compromesso iniziale di Active Directory, poi un pivot al cloud, seguiti da esfiltrazione massiva dei dati e criptaggio selettivo basato su tecniche native cloud (senza usare il classico eseguibile ransomware sui PC).

Descrizione tecnica: Gruppo RaaS (ransomware-as-a-service) finanziario, che ora adotta tattiche basate su infrastrutture cloud native. Utilizza credenziali d'accesso rubate, exploit di servizi directory e piattaforme cloud per ottenere privilegi di amministratore globale, quindi esfiltra grandi volumi di dati e impedisce ripristini cancellando backup. Questo approccio si differenzia dal ransomware tradizionale perché non si limita a crittografare file locali, ma punta a rendere irrecuperabili anche i dati nel cloud.

IoC: attualmente non sono stati pubblicati indicatori specifici di file, hash o domini legati alle campagne cloud-based di Storm-0501. L'analisi si concentra sulle tecniche TTP utilizzate, piuttosto che su singoli artefatti maligni.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1490	Inhibit System Recovery	Eliminazione di snapshot e backup cloud per impedire il ripristino dei sistemi compromessi.
T1486	Data Encrypted for Impact	Cifratura dei dati per causare impatto operativo e richiedere un riscatto.
T1550	Use Alternate Authentication Material	Utilizzo di hash NTLM e token per movimenti laterali e accessi non autorizzati.
T1003.006	OS Credential Dumping: DCSync	Utilizzo della tecnica DCSync per replicare hash NTLM e credenziali da controller di dominio.
T1021.001	Remote Services: Evil-WinRM	Accesso remoto malevolo tramite Evil-WinRM per eseguire comandi e ottenere escalation.

Contromisure:

- adottare misure di difesa su cloud e identità.
- abilitare l'MFA, monitorare i log di accesso ai tenant cloud, usare EDR/UEBA per rilevare attività sospette, segmentare le risorse cloud e tenere aggiornati AD Connect.
- Effettuare backup sicuri (offline) e verificare sistematicamente le policy di accesso condizionato in Azure.
- I prodotti di sicurezza (es. Defender for Cloud/Endpoint) devono essere attivi su tutte le istanze per evitare blind spots.

Livello di rischio: Alto (attività finanziariamente motivate con forte impatto su infrastrutture critiche).

- **TamperedChef**

TamperedChef è un nuovo malware stealer individuato nell'ambito di una campagna malspam che utilizza falsi editor PDF per veicolare un trojan. I ricercatori Truesec e G DATA hanno scoperto siti ingannevoli che promuovono un presunto "PDF Editor" (es. AppSuite PDF Editor): dopo l'installazione il setup scarica un payload che si installa come applicazione legittima, crea attività programmate e funge da backdoor.

All'attivazione, TamperedChef sottrae credenziali e cookie dai browser (Chrome, OneLaunch, Wave), modificando chiavi di registro e intercettando il traffico web.

Descrizione tecnica: Malware informazionale nascosto in un installer di un fantomatico editor PDF. Il setup victimato effettua richieste a un C2 remoto per scaricare il file PDF editor e installa attività programmate (PDFEditorScheduledTask, PDFEditorUScheduledTask) per la persistenza.

La funzione "--install" dell'eseguibile scaricato crea un servizio dove, oltre all'applicazione, vengono inclusi moduli di info-stealing. All'aggiornamento (dopo circa 56 giorni) il malware attiva funzionalità clandestine, terminando i browser aperti e prelevando cookie e credenziali salvate.

I domini e il nome esatto del file variano per ogni campagna di malvertising (le versioni trojanizzate del PDF editor sono distribuite tramite annunci compromessi).

IoC:

Indicativi sono i nomi delle task schedulate ("PDFEditorScheduledTask" e "PDFEditorUScheduledTask") e il parametro di avvio --cm=... nell'eseguibile maligno. Poiché i siti malevoli e gli installer cambiano, non esistono IoC statici fissi noti al pubblico. Gli EDR possono cercare comportamenti come eseguibili con nome PDFEditor o le chiavi di registro usate.

Tipo	Indicatore
File	"AppSuite PDF Editor" (installer trojan)
Attività	Task schedulate PDFEditorScheduledTask, PDFEditorUScheduledTask

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing / Malvertising	Distribuzione tramite campagne malvertising (Google Ads) e link ingannevoli
T1204	User Execution	Inganno dell'utente a eseguire installer apparentemente legittimi di software popolari.
T1053	Scheduled Task / Job	Creazione di task pianificati per garantire persistenza sul sistema infetto.
T1555	Credentials from Password Stores	Raccolta di credenziali e informazioni sensibili dai browser o dai password manager.

Contromisure:

- Bloccare fonti pubblicitarie e siti sospetti di distribuzione di software PDF.
- Impostare policy di sicurezza per la navigazione (EDR, antivirus) che segnalino l'installazione di software non firmato o riconosciuto. Monitorare la presenza di task schedulate anomale (nomi PDFEditor…) e processi con parametri --cm.
- Disabilitare l'esecuzione automatica di applicazioni non autorizzate.

Livello di rischio: Medio (furto di credenziali e cookie con potenziale impatto su account web).

- **ManualFinder/PDF Editor Trojan**

Il CERT-NL/NCSC ha allertato su una campagna globale di malware diffusa tramite falsi software per cercare manuali o modificare PDF.

Le vittime scaricano innocue app come "ManualFinder" o "PDF-editor" da annunci online, ma tali applicazioni creano una task schedulata (sys_component_health_) che esegue quotidianamente uno script JS (nome casuale GUID) con Node.js. Questo malware trasforma il PC infetto in un "residential proxy" utilizzato dai criminali per mascherare attacchi informatici.

In altre parole, il computer compromesso diventa una sorta di server relay: gli attaccanti instradano il loro traffico attraverso questo proxy rendendo difficile risalire alla fonte del vero attacco. È stata osservata anche l'installazione di un tool di "ManualFinder" con funzionalità proxy durante la campagna.

Descrizione tecnica: Malware nascosto in finti software utilità. All'installazione viene creata una scheduled task (sys_component_health_) che ogni giorno avvia un file JavaScript nascosto in %TEMP% con un nome a GUID.

Lo script JS comunica con server di comando remoto (C2) e abilita la modalità proxy tramite un componente denominato ManualFinder (legittimo solo di nome). In pratica, l'attacco usa software firmati in modo ufficiale (con certificati compromessi) per diffondere il malware e utilizza risorse legittime per nascondere l'infezione.

IoC:

Tipo	Indicatore
File	File JS con nome GUID e suffisso "ro.js" o "or.js" eseguito da Node
Domini	y2iax5[.]com, 5b7crp[.]com, mka3e8[.]com (C2 della campagna)
Certificati	Certificati digitali compromessi: "GLINT SOFTWARE SDN BHD", "ECHO INFINI SDN BHD", "Summit Nexus Holdings LLC
Software	"ManualFinder" (utilità proxy)
Hashes	• PDFEditor.exe cb15e1ec1a472631c53378d54f2043ba57586e3a28329c9dbf40cb69d7c10d2c • PDFEditorSetup.exe da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0

	• AppSuite-PDF.msi fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b • ConvertMate.exe e0db7b5eaf92feff220c805b0e5f3d8916e18d51 • ConvertMate.exe d9f9584f4f071be9c5cf418cae91423c51d53ecf9924ed39b42028d1314a2edc • conmate_update.ps1 372d89d7dd45b2120f45705a4aa331dfff813a4be642971422e470eb725c4646 • Uninstaller.exe e95de8452d32b439e0286868ed16f63943af3bc059dca6bcb48d1cbe2431440e

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1053	Scheduled Task/Job	L'utente viene indotto a scaricare ed eseguire il finto editor PDF tramite ingegneria sociale.
T1204	User Execution	Creazione di task pianificati per mantenere la persistenza sul sistema compromesso.
T1090	Proxy / Tunneling	Utilizzo di proxy o tunneling per nascondere le comunicazioni C2 e l'esfiltrazione di dati.

Contromisure:

- Bloccare i domini elencati come malevoli (blacklist DNS/firewall) e rimuovere qualsiasi applicazione "ManualFinder" o PDF-editor sconosciuta.
- Controllare e cancellare task schedulate sospette in cui Node.js avvia script sconosciuti.

- Aggiornare le piattaforme di sicurezza (EDR, antivirus) per rilevare comportamenti di proxy inversi. Sensibilizzare gli utenti a non installare tool da annunci pubblicitari.

Livello di rischio: Medio (il sistema infetto viene abusato come proxy per altre attività malevole).

- **APT36 (Transparent Tribe)**

Il gruppo APT36, legato all'intelligence pachistana, ha lanciato una campagna mirata di spionaggio verso istituzioni indiane, utilizzando file .desktop su Linux BOSS (sistema governativo indiano).

In questa operazione di spear phishing, le vittime ricevono una e-mail con un allegato .zip che contiene un file .desktop camuffato da collegamento a un PDF.

All'apertura del file .desktop (che in realtà è uno script), vengono eseguiti comandi per scaricare un payload maligno e installare un malware. Contestualmente viene avviato Firefox in background su un documento benigno (ospitato su Google Drive) per sviare l'utente dall'attività illecita.

Una volta stabile il canale col server C2, il malware raccoglie dati sensibili dal sistema e li esfiltra ai malintenzionati.

Questa tattica dimostra come APT36 stia diversificando i vettori di attacco verso ambienti protetti (Linux) mantenendo attività tradizionali su Windows e mobile.

Descrizione tecnica: Attacco di tipo spear-phishing su infrastrutture Linux governative. Viene inviato un file .desktop (con estensione .desktop) nascosto in un archivio, presentato come scorciatoia PDF. Eseguendo questo file .desktop, il sistema scarica e lancia un malware che esfiltra informazioni.

Per ingannare l'utente viene contemporaneamente aperto un documento Google Drive innocuo in Firefox, simulando un'attività lecita

Indicatori di compromissione (IoC): la minaccia non ha nomi di dominio o hash pubblici noti. Segnali d'allarme includono la comparsa di file .desktop non autorizzati e attività anomale di Firefox in background. Le istruzioni maligni sono incorporate nello stesso file .desktop.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566.001	Phishing: Spearphishing Attachment	Invio di allegati malevoli (file .desktop) come vettore iniziale di infezione.
T1204	User Execution	Richiede che la vittima apra manualmente il file allegato per avviare l'esecuzione del malware.
T1560	Archive Collected Data	Esfiltrazione e compressione dei dati raccolti dal sistema compromesso.
T1036	Masquerading	Avvio di Firefox per mascherare l'attività malevola e ridurre la possibilità di rilevamento.

Contromisure:

- Formare gli utenti sul rischio di allegati e scorciatoie sospette. Bloccare allegati .desktop e archivi da mittenti non affidabili.
- Su Linux verificare integrità e provenienza dei file eseguibili e usare soluzioni di sicurezza endpoint su Linux BOSS.
- Monitorare traffico in uscita insolito verso server strani (anche su TLS).

Livello di rischio: Alto (spionaggio politico/settore militare con furto di dati sensibili).

- **ShadowSilk**

Un cluster di attività APT attivo in Asia centrale e Pacifico (denominato ShadowSilk) ha preso di mira enti governativi e settore energia nei paesi ex-sovietici e vicini.

Gli autori, caratterizzati da due team bilingue (russo e cinese), sfruttano campagne di spear-phishing con archivi protetti da password che contengono un loader personalizzato. Questo loader nasconde il canale C2 dietro bot di Telegram, rendendo difficile il tracciamento.

Nel corso degli attacchi sono stati sfruttati exploit pubblici su Drupal (CVE-2018-7600/7602) e un plugin WordPress (CVE-2024-27956).

Dopo la compromissione, ShadowSilk impiega web shell (es. ANTSWORD, Behinder) e strumenti di post-exploitation per muoversi lateralmente e creare tunnel crittografati (Resocks, Chisel). Infine utilizza RAT basati su Python che inviano screenshot e dati sottratti a bot Telegram, mimetizzando il traffico come chat legittima.

Descrizione tecnica: APT multiregionale (alleanza operativo YoroTrooper e Silent Lynx) che usa un misto di spear-phishing e vulnerabilità note per entrare nelle reti governative in Asia centrale.

La post-compromissione include la modifica del registro per persistenza, uso di web shell e tool penetration (Metasploit, Cobalt Strike) e esfiltrazione dati occultata come traffico Telegram.

Indicatori di compromissione (IoC): nessun IoC statico pubblicato; tra gli indicatori osservati vi sono payload serviti da siti compromessi, nomi di script (es. jramosh come esempio di web panel) e pattern di traffico a bot Telegram.

MITRE ATT&CK:

ID	Tecnica	Descrizione
T1566	Phishing (Spearphishing Email)	Diffusione iniziale tramite email di phishing mirate agli utenti.
T1190	Exploit Public-Facing Application	Sfruttamento di vulnerabilità note in Drupal/WordPress per l'accesso iniziale.
T1059.006	Command and Scripting Interpreter: PowerShell	Utilizzo di PowerShell/jRAT come loader per eseguire codice maligno.
T1105	Ingress Tool Transfer	Download di payload aggiuntivi dai server C2 mascherati dietro Telegram.

Contromisure:

- Applicare patch di sicurezza (in particolare a CMS come Drupal e WordPress).
- Bloccare comunicazioni con server noti di Telegram bot sospetti. Utilizzare EDR con analisi comportamentale per individuare attivazioni insolite di web shell o script di rete.

- Segmentare la rete per limitare movimenti laterali e raccogliere intelligence su infrastrutture note dell'APT.

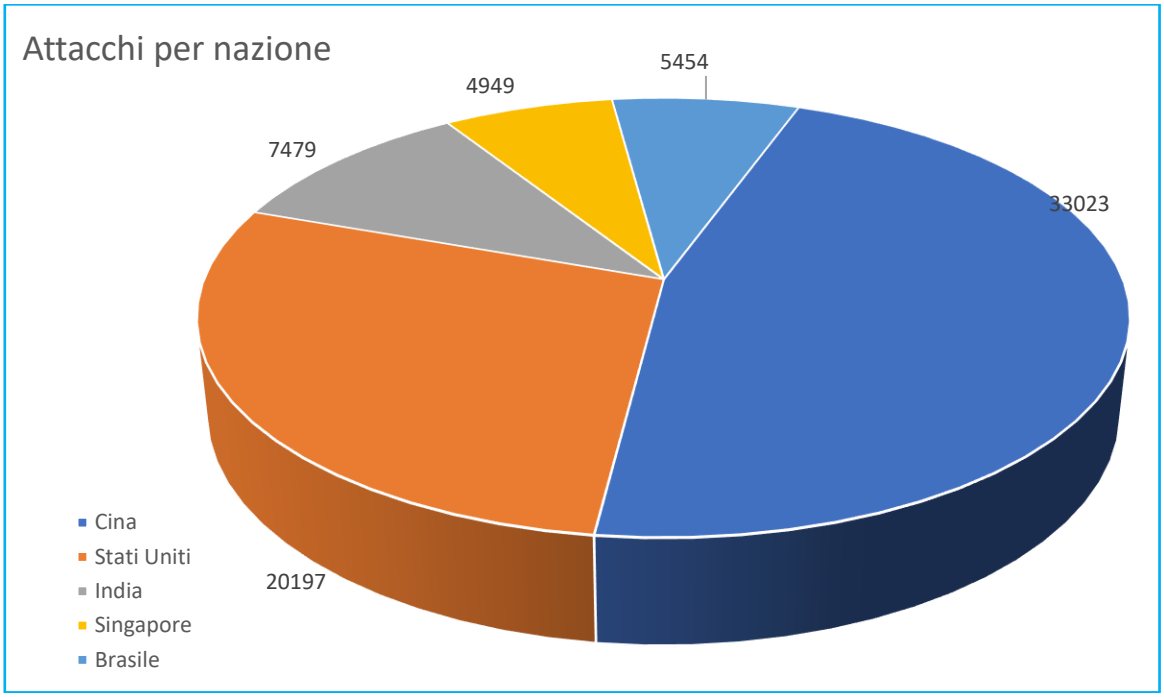
Livello di rischio: Alto (mirato a governi/industrie, con sofisticazione e raccolta dati su larga scala).

Riepilogo:

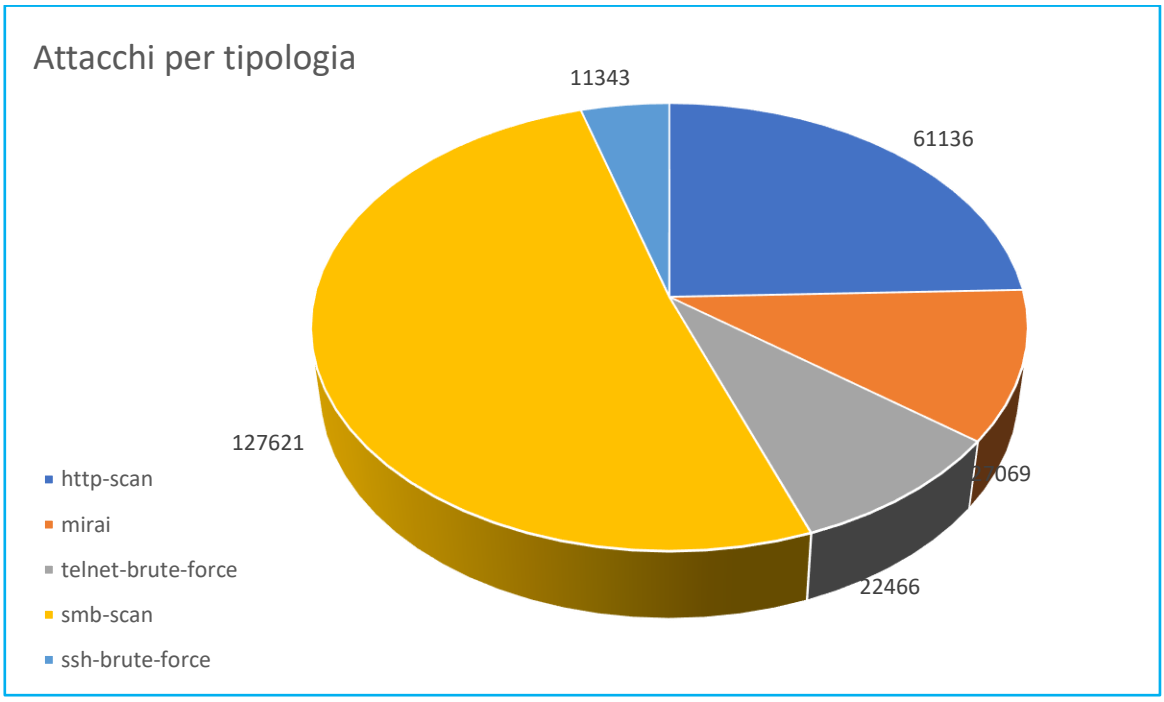
Malware	Categoria	Livello di rischio
Storm-0501	Ransomware (RaaS)	Alto
TamperedChef	Infostealer (Stealer credenziali)	Medio
ManualFinder Trojan	Trojan (proxy residenziale)	Medio
APT36 (Transparent Tribe)	APT/Spionaggio	Alto
ShadowSilk	APT/Spionaggio	Alto

4.4 DDoS rilevati

Nel grafico seguente riportiamo la media giornaliera degli attacchi DDoS rilevati a livello mondiale nel periodo 25 - 31 Agosto, suddivisa per nazione e limitata alle prime cinque posizioni:

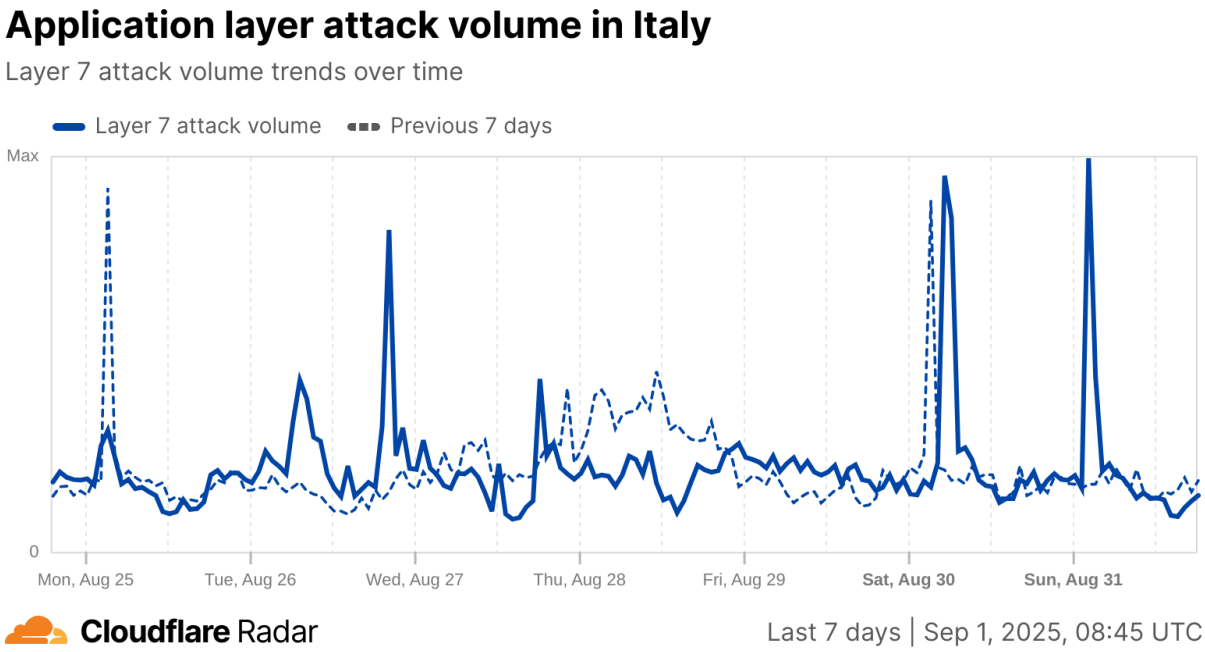


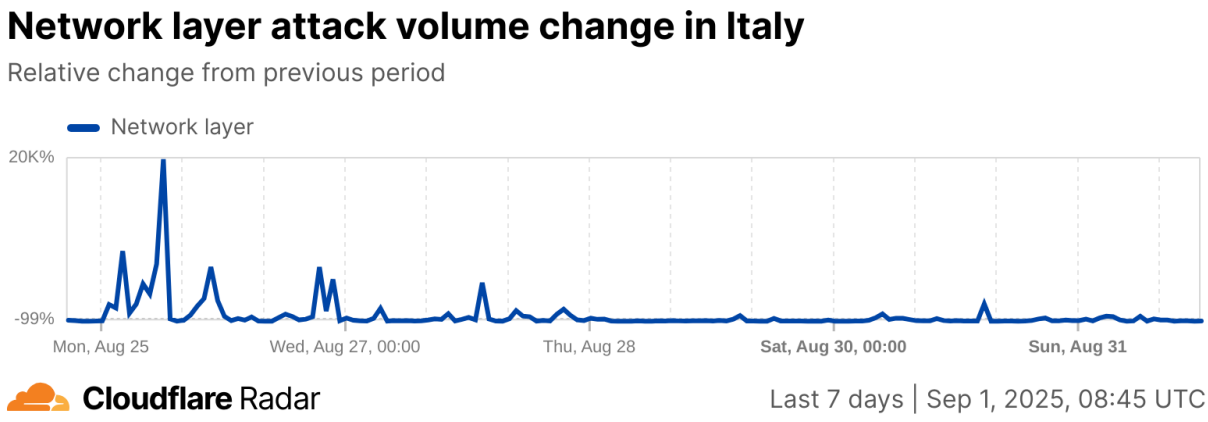
Nel grafico seguente invece la suddivisione degli attacchi per tipologia di attacco:



SITUAZIONE ITALIANA

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





Fonte: Cloudflare Radar

4.5 Data Breach

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

TARGET	LOCALIZZAZIONE
ECO DEMOLIZIONI S.R.L.	ITALIA
DESCRIZIONE	Ad inizio settimana, il sito ufficiale di Eco Demolizioni S.r.l. sarebbe stato colpito da un data breach. L'attacco viene attribuito al gruppo ransomware Qilin, noto per la compromissione di dati aziendali a scopo di estorsione. Al momento l'azienda non si è pronunciata in merito all'incidente e non sono state rese note informazioni su quali dati sarebbero stati sottratti.

TARGET	LOCALIZZAZIONE
TRANSUNION	STATI UNITI
DESCRIZIONE	Il 28 agosto è stato reso noto un importante data breach che ha coinvolto TransUnion, una delle principali agenzie di credito statunitensi. L'incidente ha compromesso i dati personali di oltre 4,4 milioni di consumatori USA, tra cui nomi, numeri di previdenza sociale e date di nascita. L'attacco ha preso di mira un'applicazione di terze parti usata da TransUnion per il supporto ai clienti, ma fortunatamente non sono stati esposti dati finanziari. Il gruppo hacker ShinyHunters è stato indicato come responsabile dell'intrusione. TransUnion ha reagito offrendo 24 mesi di monitoraggio del credito e protezione contro il furto d'identità tramite servizi dedicati.

4.6 Defacement

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

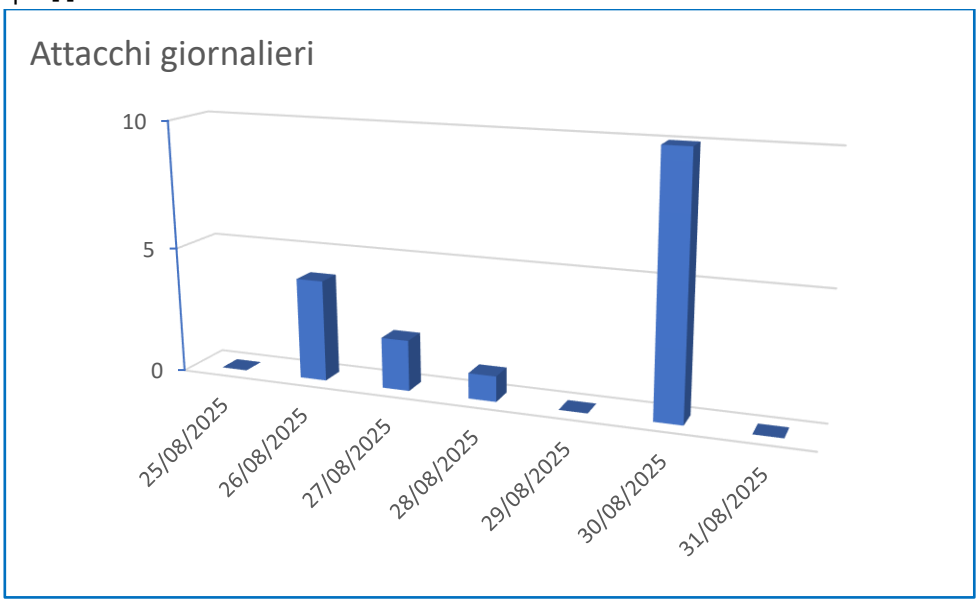


Figura 1: Defacement – Andamento giornaliero del numero di domini [.]it che hanno subito un defacement.

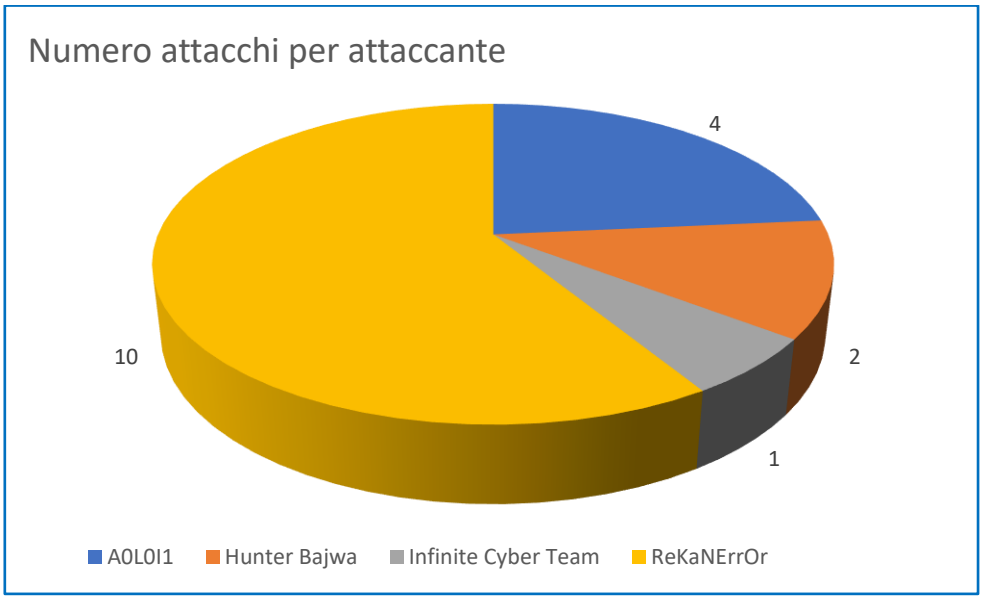


Figura 2: Defacement - Attaccanti più attivi nel periodo 25 - 31 Agosto

Oltre al consueto report settimanale, così come fatto per le altre tipologie di attacco riportiamo una analisi più approfondita relativa ai più importanti attacchi di tipo defacement che hanno avuto come target siti italiani e non, e come intervallo temporale gli ultimi tre mesi (Giugno – Agosto 2025).

Defacement di siti web aziendali italiani (giugno 2025)

Nel giugno 2025 il CSIRT italiano ha rilevato una campagna di hacktivismo filo-russo che ha colpito siti web di piccole aziende del settore manifatturiero. Gli aggressori hanno modificato la home page dei portali

con messaggi pro-Russia (defacement) ma senza causare interruzioni gravi dei servizi – solo il 13% degli attacchi ha provocato brevi disservizi.
MITRE ATT&CK: Il defacement è classificato sotto T1491.002 (External Defacement) della matrice ATT&CK, nell'ambito della tattica Impact. Gli hacker hanno compromesso sistemi web (ad es. CMS obsoleti) per sostituirne i contenuti, senza installare malware persistente.
Misure di rilevamento:Monitorare i log delle applicazioni web e le modifiche ai file delle pagine (ad es. tramite SIEM o strumenti di integrità). In particolare, verificare la creazione di nuovi contenuti e ogni modifica anomala ai file delle pagine internet (file changes).
Misure di mitigazione:

- Applicare regolari backup dei siti, aggiornare tempestivamente CMS, plugin e server web, e filtrare il traffico con WAF o IDS/IPS.
- Limitare l'accesso all'area di amministrazione (es. tramite VPN o restrizioni geografiche), disabilitare componenti inutilizzati e monitorare eventuali credenziali rubate in dark web.

Livello di rischio: Basso. L'attacco è principalmente dimostrativo/politico (imbottito di propaganda) e, come riportato, ha avuto impatto tecnico contenuto. Il rischio operativo rimane modesto per le aziende bersaglio, sebbene simili defacement possano nuocere all'immagine e richiedere intervento di ripristino.

Defacement di siti italiani (xNot_RespondinGx, 20 giugno 2025)

Indicatori di compromissione: una serie di siti web italiani (agenzie, e-commerce, portali tecnici) sono stati compromessi con un file readme.txt malevolo lasciato dal gruppo xNot_RespondinGx.
Tra i domini colpiti si segnalano:

- Languageteam[.]it,
- ficusbarbistrot[.]it,
- giuliettaallago[.]it,
- servicewebsrl[.]it,
- techimgroup[.]it,
- ristopollicino[.]it,
- simasrl[.]it

MITRE ATT&CK:

- il defacement rientra nella tecnica T1491.002 (External Defacement).
- L'attacco presuppone l'accesso ai sistemi web target, probabilmente ottenuto tramite vulnerabilità di applicazioni pubbliche (es. exploit di CMS, T1190) o credenziali rubate (FTP/SSH compromessi, T1078).

- Una volta avuto accesso, gli aggressori hanno modificato la homepage sostituendo i contenuti originali.

Rilevamento e mitigazione:

- è essenziale il monitoraggio continuo dei siti web (es. usando WAF/IDS e confronti di integrità), oltre a backup regolari del contenuto pubblico.
- Dopo l'attacco, si consiglia di ripristinare i file da backup puliti, reimpostare tutte le credenziali di amministratore e applicare patch di sicurezza note.

Livello di rischio: medio-basso. I defacement non hanno coinvolto furto di dati sensibili o interruzione critica di servizi, ma danneggiano la reputazione e mostrano gravi lacune nella sicurezza (i siti sono stati "sfregiati" con messaggi provocatori).

Defacement di siti sportivi israeliani (1–2 agosto 2025)

La stampa israeliana ha riferito che tra il 1° e il 2 agosto 2025 un gruppo di hacker pro-Palestina ha coordinato una campagna di defacement su siti sportivi nazionali.

Tra i bersagli confermati figurano il sito web del club di basket Maccabi Tel Aviv e il portale ufficiale della Premier League calcistica israeliana. Le pagine colpite sono state rimpiazzate con un messaggio "Time is Running Out" in più lingue, a sostegno della resistenza palestinese.

IOC: Domini bersaglio noti: maccabi.co.il (Maccabi Tel Aviv B.C.) e football.co.il (Lega calcistica israeliana). Non sono disponibili indirizzi IP o hash dai report open-source.

MITRE ATT&CK: Ancora una volta si tratta di T1491.002 External Defacement (tattica Impact), poiché gli hacker hanno modificato i contenuti web esposti al pubblico.

Non è stato introdotto malware persistente; l'azione è limitata a change nei file statici (homepage).

Misure di rilevamento: Implementare controlli di integrità del sito web e log dell'applicazione web. In particolare, monitorare cambiamenti nei file delle pagine e traffico insolito diretto agli endpoint di amministrazione. Una scansione periodica del contenuto web (ad es. confrontando hash del file) può rilevare istantaneamente eventuali defacement.

Misure di mitigazione:

- backup regolari del sito prima di ogni modifica, sistemi di aggiornamento continuo dei CMS e patch dei server.
- Configurare un Web Application Firewall (WAF) per bloccare richieste malevole o tentativi di sfruttare vulnerabilità note.
- Disabilitare componenti web inutilizzati e usare meccanismi di autenticazione forte per l'accesso al pannello di controllo.
- La geolocalizzazione (geofencing) può limitare l'accesso dall'estero durante fasi critiche.

Livello di rischio: Medio. L'attacco è di natura politica/protesta: non ha compromesso dati sensibili né causato interruzioni di servizio significative, ma ha impatto mediatico elevato. Per le entità coinvolte (club sportivi e piattaforme media) il defacement è un evento grave in termini di reputazione, anche se il danno tecnico è contenuto.

Attacco al Ministero del Lavoro thailandese (Devman/DragonForce, luglio 2025)
Indicatori di compromissione: il sito ufficiale del Ministry of Labour thailandese è stato defacciato dagli hacker del gruppo Devman (associato alla famiglia DragonForce). Il gruppo ha rivendicato di aver esfiltrato ~300 GB di dati sensibili e di aver cifrato circa 2.000 laptop aziendali.

MITRE ATT&CK:

- l'attacco combina T1491.002 (Defacement esterno) con tecniche di ransomware.
- Gli aggressori hanno probabilmente usato un accesso da remoto (es. credenziali RDP compromesse, T1078, o exploit di applicazioni web, T1190) per penetrare nella rete.
- Hanno poi propagato ransomware (DragonForce) cifrando dati (T1486) e hanno esfiltrato grandi quantità di informazioni (probabilmente via canale C2, T1041).

Rilevamento e mitigazione:

- secondo fonti giornalistiche, il sito è stato temporaneamente messo offline, i file defacciati sono stati sostituiti con backup puliti e tutte le password di accesso sono state cambiate.
- Come contromisure generali, sono utili l'isolamento dei segmenti di rete critici, la scansione anti-malware completa dei server, la segmentazione dei privilegi, aggiornamenti tempestivi (patch) e soluzioni di backup off-site.
- In incidente simili è raccomandato il coinvolgimento immediato di forze dell'ordine/cert nazionale e l'analisi forense della compromissione.

Livello di rischio: alto. L'attacco di ransomware ha causato cifratura di dati e furto di informazioni governative critiche (identità dei lavoratori, dati di cittadini, ecc.), oltre al defacement visibile. Il riscatto richiesto è stato di 15 milioni di dollari. Questo tipo di incidente minaccia gravemente disponibilità e riservatezza, richiedendo misure di sicurezza avanzate (es. MFA, segmentazione severa, disaster recovery testati).

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

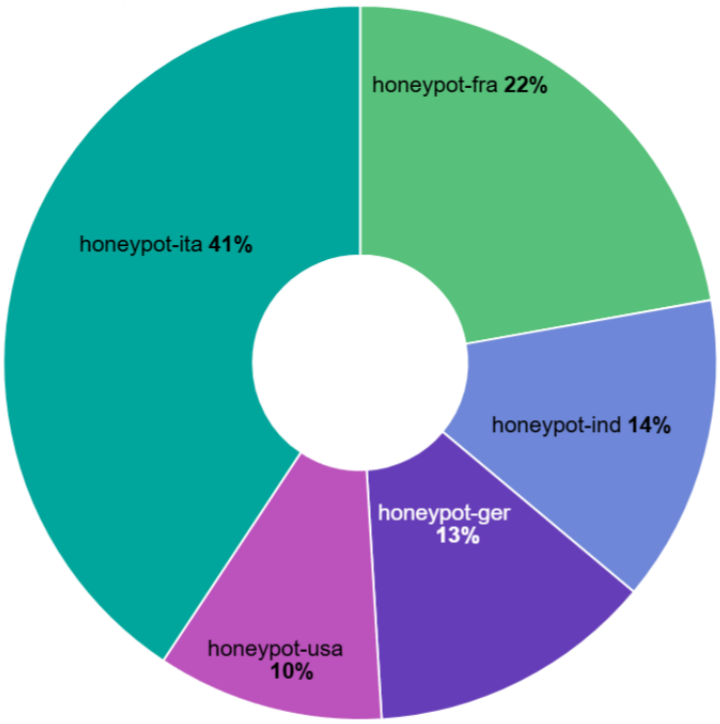
Riportiamo qui sotto i dati relativi agli attacchi rilevati questa settimana.

1.198.609 Attacks

7.827 Unique Src IPs

69 Unique HASSHs

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



Questa invece la situazione a livello italiano:

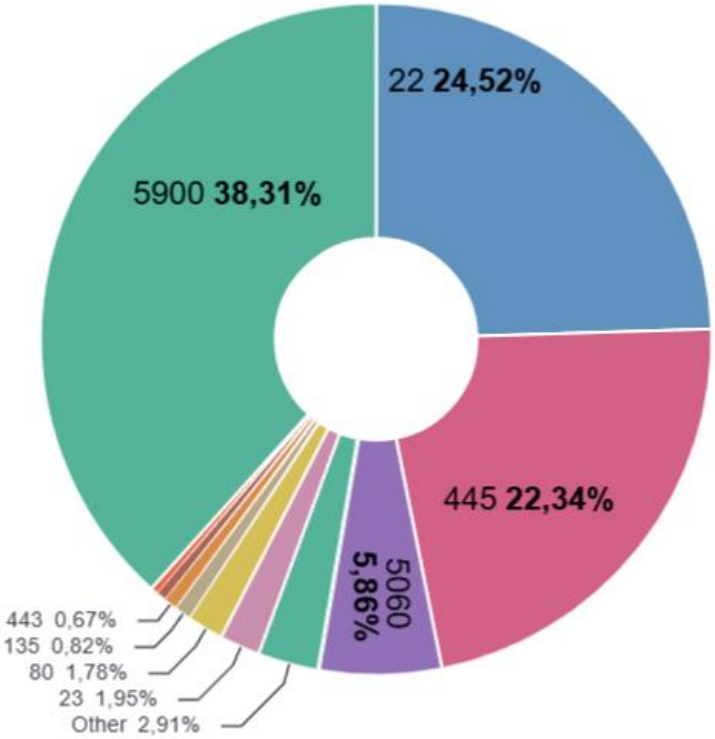
487.721 Attacks

2.941 Unique Src IPs

50 Unique HASSHs

5.1.1 Attacchi ai servizi

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



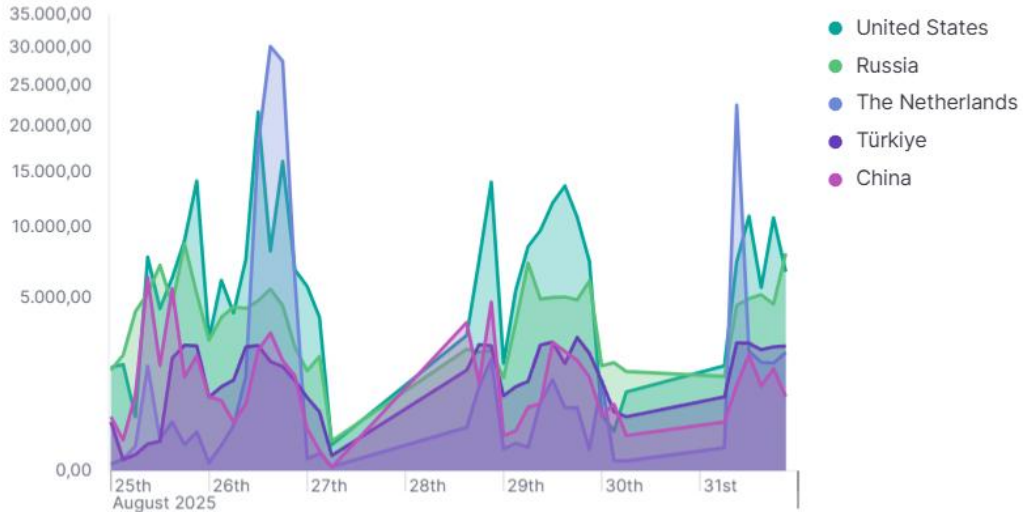
5.1.2 IP Attaccanti

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

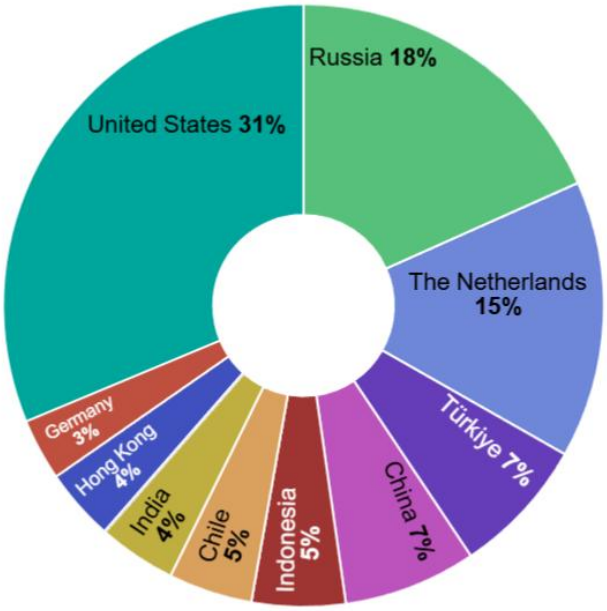
Source IP	Count
185.233.247.245	58.910
186.67.186.10	37.386
142.202.189.5	35.091
79.124.56.162	23.207
171.22.117.82	21.797
172.81.61.121	20.913
193.37.69.157	20.276
45.134.26.33	20.218
172.81.60.34	19.415
142.202.191.234	17.832

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:

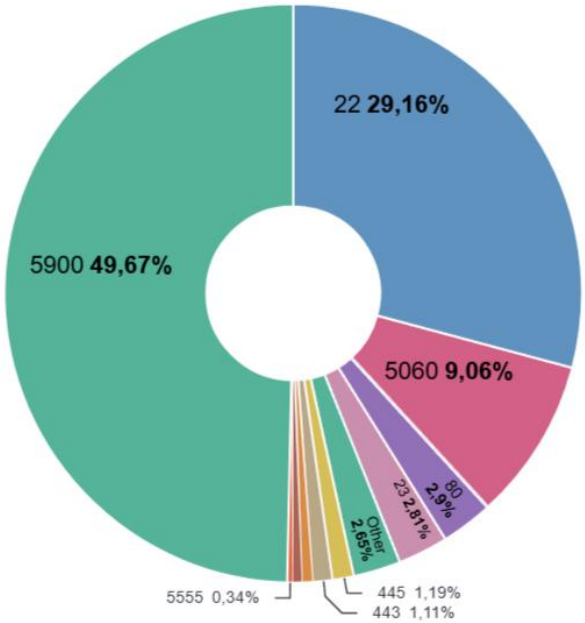


5.2 Italian Honeypot N.1

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
5900	53.344
22	31.313
5060	9.726
80	3.110
23	3.022
445	1.283
443	1.191
6379	648
3306	553
5555	362

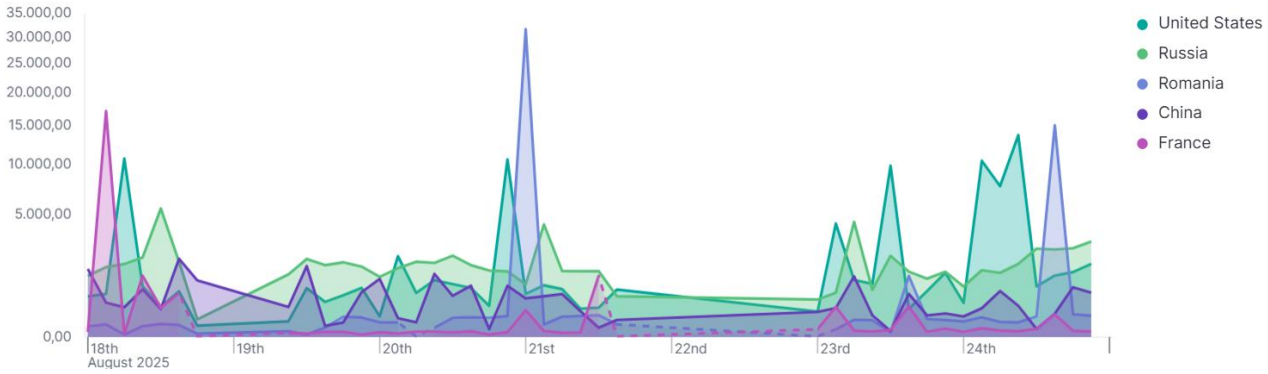
5.2.2 IP Attaccanti

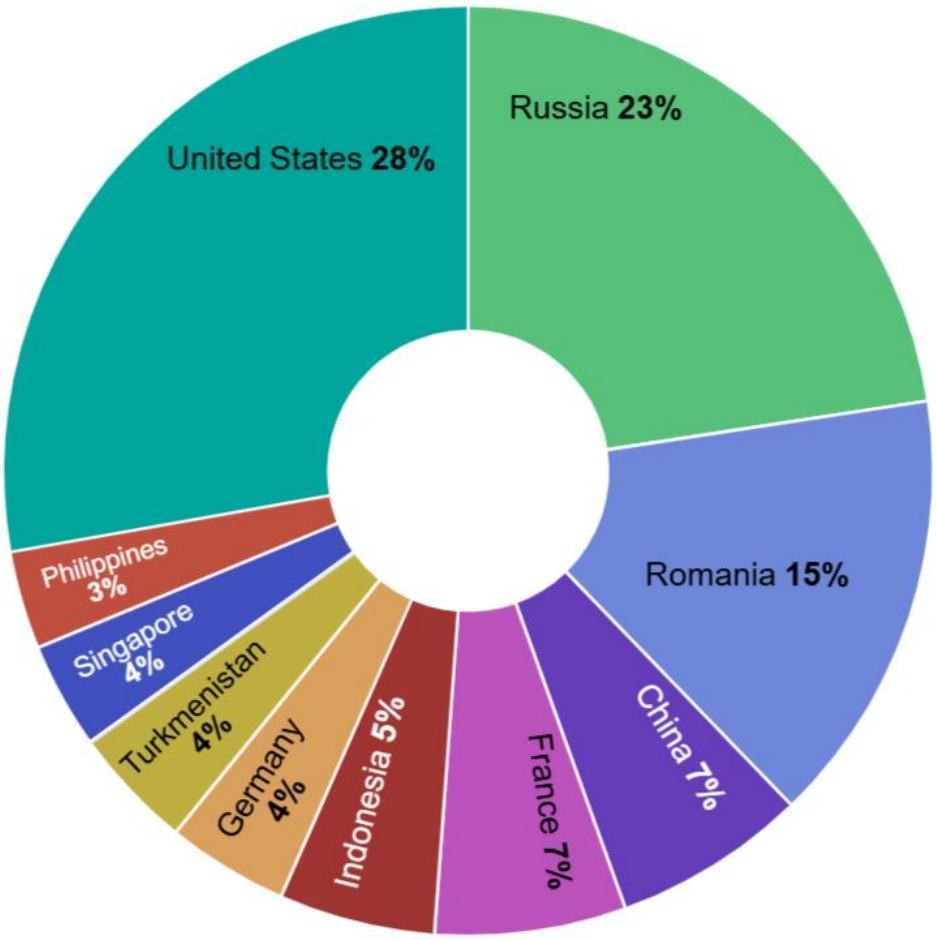
Questa invece la classifica relativa ai 10 IP che hanno effettuato il maggior numero di attacchi:

Source IP	Count
171.22.117.82	21.797
185.233.247.245	17.532
45.134.26.33	11.037
142.202.189.5	10.604
196.251.66.39	10.121
196.251.66.40	10.113
196.251.84.35	10.113
196.251.115.130	10.110
196.251.115.97	10.108
196.251.81.119	10.108

5.2.3 Paesi di provenienza degli attacchi

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



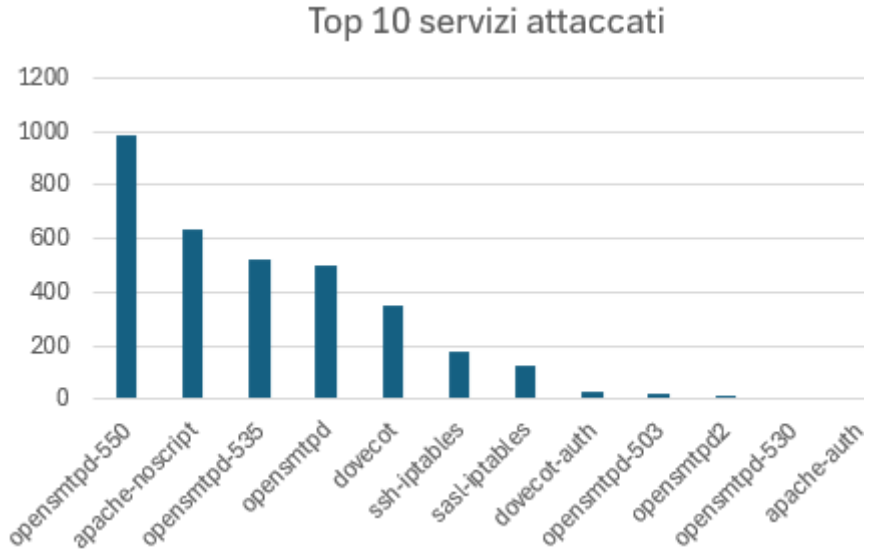

Russia 23%
Romania 15%
China 7%
France 7%
Indonesia 5%
Germany 4%
Turkmenistan 4%
Singapore 4%
Philippines 3%
United States 28%

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

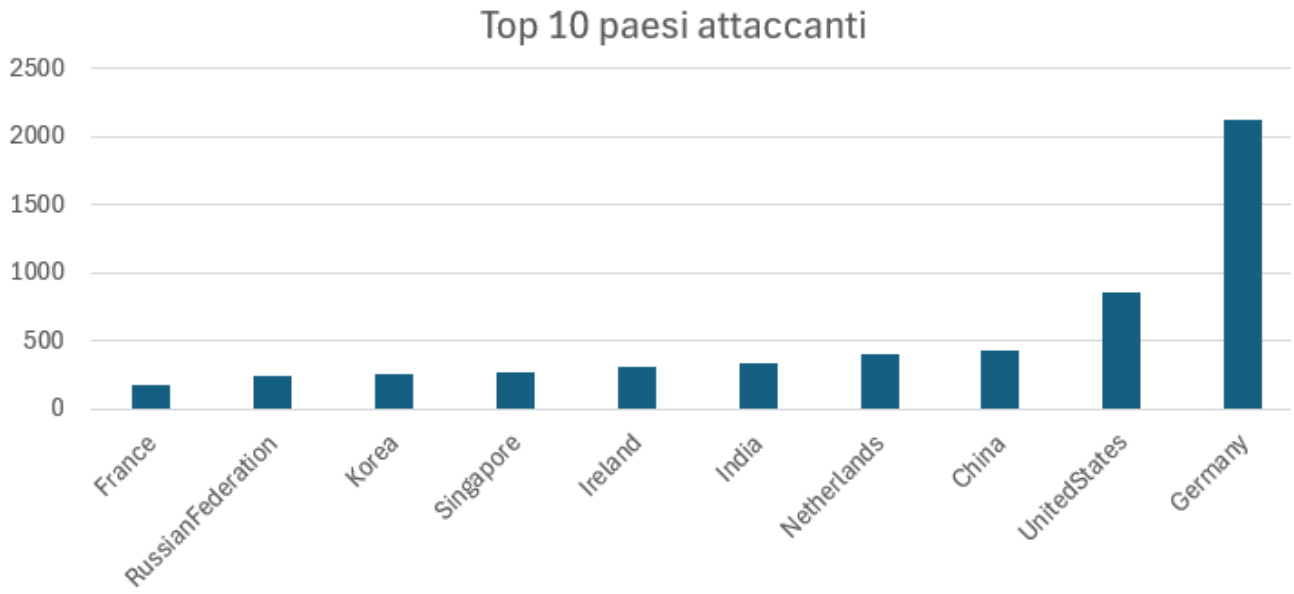
5.3.2 IP attaccanti

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
178[.]162[.]136[.]160	199
103[.]159[.]133[.]164	149
5[.]253[.]59[.]162	111
77[.]87[.]213[.]12	46
62[.]173[.]141[.]88	46
62[.]152[.]59[.]17	39
175[.]123[.]253[.]38	23
179[.]24[.]55[.]101	21
41[.]90[.]172[.]248	21
147[.]235[.]210[.]50	21

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