S3K

Bollettino CTI Settimanale

12/01/2026 - 18/01/2026

Cyber Threat Intelligence Report prodotto da S3K Group S.p.A. - Security of the Third Millennium. Analisi delle principali minacce informatiche rilevate attraverso fonti OSINT, Deep e Dark Web.

www.s3kgroup.it

Introduzione al Report CTI

Il bollettino settimanale di Cyber Threat Intelligence di S3K Group S.p.A. fornisce una sintesi completa delle principali evidenze emerse nell'ultima settimana, concentrandosi su vulnerabilità critiche, campagne di attacco avanzate, violazioni di dati, ransomware e attività di phishing rilevanti per organizzazioni italiane ed europee.

01

Raccolta Dati

Correlazione di feed Telegram, fonti OSINT e canali specializzati

02

Analisi Automatizzata

Elaborazione attraverso sistemi proprietari di intelligence

03

Supervisione Esperta

Verifica e validazione da parte di analisti qualificati

04

Report Strutturato

Sintesi operativa con raccomandazioni strategiche

CTI WEEKLY

Sommario Settimanale (11/01/2026 – 18/01/2026)

Ransomware in Crescita

Fluorsid Spa colpita da attacco ransomware. Gruppi Sinobi e Qilin intensificano operazioni contro settori automotive, legale e sanitario

Vulnerabilità Critiche

Scoperte falle critiche in FortiSIEM e plugin Modular DS WordPress. Microsoft rilascia patch per 112 vulnerabilità di cui 2 zero-day

Data Breach Massivi

Oltre 30.000 email pubblica amministrazione compromesse. Database yachtshop.it e vincitu.it esposti con 376K contatti italiani

- **Campagne di Phishing Sofisticate**

  Nuove campagne AI-powered mirano a Banco BPM e utilizzano Google Ads per spear-phishing. APT28 intensifica attacchi contro enti europei

- **Espansione Botnet**

  GoBruteforcer attacca progetti crypto con credenziali deboli. Kimwolf raggiunge 2M di dispositivi infetti nonostante neutralizzazione di 550 server C2

NEWS CYBER

Attività Malevole della Settimana

Il panorama della sicurezza informatica ha visto un aumento significativo delle attività malevole, con attacchi mirati a infrastrutture critiche e vulnerabilità sfruttate in vari settori. Le organizzazioni italiane ed europee sono state particolarmente colpite.

Ransomware Internazionali

- Fluorsid Spa colpita da attacco ransomware
- Bergmanis Preyra compromessa (Canada)
- Central Roofing attaccata (UK)
- Dongguan HYX Industrial colpita (Cina)

Vulnerabilità Zero-Day

- Exploit pubblico per Apple Safari
- FortiSIEM attivamente sfruttata
- APT cinesi mirano Sitecore per infrastrutture critiche USA
- Facebook React documentazione compromessa

Focus Italia: Fluorsid SpA è stata colpita da ransomware, sottolineando l'urgenza per le aziende italiane di adottare misure di sicurezza rafforzate e implementare strategie di difesa proattive.

DATA BREACH

Violazioni Dati: Scenario Italiano

1.2K

Documenti Italiani

Video-selfie e documenti personali in vendita su forum di hacking

550K

Contatti Esposti

Database di 376K contatti italiani + 18.7K utenti vincitu.it compromessi

360K

Email PA

Oltre 30.000 indirizzi email funzionari pubblica amministrazione italiana

100K

Accessi Database

Accesso completo a database yachtshop.it, virgilio.it e Forex Italia

La settimana ha evidenziato una crescente disponibilità di dati sensibili italiani sui mercati neri. L'esposizione di oltre 30.000 email della pubblica amministrazione e migliaia di documenti personali rappresenta una minaccia seria per la sicurezza nazionale e la privacy dei cittadini. Gli attaccanti stanno inoltre sfruttando database di settori critici come nautica, gaming online e finanza, aumentando significativamente il rischio di frodi mirate.

Impatto sui Settori Critici

Telecomunicazioni

Vulnerabilità in sistemi FortiSIEM utilizzati per monitoraggio di rete. Rischio di compromissione infrastrutture critiche nazionali

Studi Professionali

Attacchi ransomware a studi legali e di commercialisti. Dreher Law Firm e Bikkal & Associates tra le vittime

Piccole Imprese

Central Roofing (UK) e ITG-Electronics colpite da ransomware. Le PMI restano obiettivi vulnerabili con difese limitate

Gaming Online

Database vincitu.it compromesso con 18.7K utenti. Rischio elevato per dati finanziari e personali nel settore gaming

MALWARE

Malware & Infrastructure

L'intensificazione delle attività malevole ha coinvolto botnet sofisticate e malware mirati a infrastrutture critiche. I gruppi attaccanti stanno sfruttando credenziali deboli e tecniche evasive avanzate per compromettere ambienti cloud e progetti di criptovalute.

Botnet Dominanti

1. **GoBruteforcer:** Attacchi intensificati contro database crypto, sfruttando credenziali deboli su FTP/MySQL
2. **Kimwolf:** Oltre 2M dispositivi infetti, 550+ server C2 neutralizzati ma minaccia persiste
3. **Magecart:** Skimming su reti di pagamento online, furto dati carte di credito

Minacce Avanzate

VX Stealer

Nuovo malware targeting cloud

VoidLink

Minaccia avanzata per sistemi Linux

GootLoader

Evasione con 500-1000 archivi ZIP concatenati

Gli attacchi alle infrastrutture cloud sono in aumento. VoidLink utilizza tecniche avanzate per compromettere sistemi Linux, richiedendo monitoraggio costante e segmentazione di rete efficace.

PHISHING

Phishing & Social Engineering

01

Tresobank & Banco BPM

Campagne phishing mirate contro utenti bancari italiani. Furto credenziali tramite pagine login false

02

AI-Powered Phishing

Reti neurali generano testi sofisticati per bypassare filtri automatizzati

03

QR Code Malicious

Gli utenti si auto-phishing con QR code online malicious

04

APT28 Spear-Phishing

Fancy Bear utilizza Google Ads redirect e email contestualizzate contro enti europei/asiatici

05

LinkedIn IRS

Nuove configurazioni email routing per spelling inerno

Tecniche Emergenti

- Generazione testi AI/ML avanzata
- SMS spoofing per legittimità apparente
- Analisi psicologica per targeting mirato
- Spoofing interno e SEO poisoning

Settori Target

- Banche italiane (Banco BPM, Tresobank)
- Enti governativi europei
- Organizzazioni asiatiche (Microsoft 365)
- Utenti piattaforme banking private

RANSOMWARE

Operazioni Ransomware Active

La settimana ha registrato un'espansione significativa delle operazioni ransomware con Sinobi e Qilin che dominano il panorama. Settori colpiti includono automotive, legale, sanitario e tecnologico, con attacchi che si estendono globalmente.

Sinobi - Espansione Aggressiva

Nuove vittime rivendicate: ITG-Electronics, Galutti Automotive, Title Guaranty, Bikkal & Associates. Settori target: automotive, servizi legali, tecnologia

Qilin - Target Alto Profilo

Attacchi confermati: Università Volkswagen-Mazda, Dreher Law Firm, Vietnam Airlines, Balneario. Focus su istituzioni educative e trasporti

CrazyHunter - Settore Sanitario

Sei vittime confermate nel settore sanitario taiwanese. Tecniche di intrusione avanzate sfruttano vulnerabilità sistemi medicali

Tengu & Incransom

GSM Portal Teknoloji e MKC Customs Brokers colpite. Espansione verso logistica e commercio internazionale

Kyowon (Sud Corea) ha confermato furto dati massiccio, evidenziando l'impatto globale delle operazioni ransomware su organizzazioni di alto profilo.

VULNERABILITÀ

Vulnerabilità Critiche & Patch

1	**CVE-2025-61937** AVEVA: RCE non autenticato con privilegi sistema. Punteggio CVSS 10.0. Aggiornamento urgente richiesto
2	**CVE-2026-0491** SAP Landscape: Code Injection con privilegi admin. Punteggio 9.1. Rischio compromissione sistemi SAP
3	**CVE-2025-62581** Delta Electronics: Authentication Bypass, CVSS 9.8. Accesso funzioni critiche senza autenticazione
4	**CVE-2026-1022** Gotac Statistics DB: Arbitrary File Read remoto non autenticato. Punteggio 8.7
5	**CVE-2026-21223** Microsoft Edge: Escalation privilegi per utenti locali. Rischio esecuzione comandi privilegiati
6	**CVE-2025-3977** FortiSIEM: Vulnerabilità attivamente sfruttata. Patch immediata necessaria

Vulnerabilità Aggiuntive

CVE-2025-49373

Patch Tuesday Microsoft: 112 vulnerabilità risolte di cui 2 zero-day. Include RCE, DoS, EoP. Priorità massima

CVE-2025-7570

Coolify: 3 PoC pubblici per RCE e Information Disclosure. Aggiornamenti software urgenti

Trend Generale

Incremento vulnerabilità RCE con CVSS > 9.0. Sistemi industriali e cloud particolarmente esposti

Raccomandazione Immediata

Applicare Patch Tuesday Microsoft e aggiornare FortiSIEM, AVEVA, SAP entro 48 ore

Vulnerability Scanning

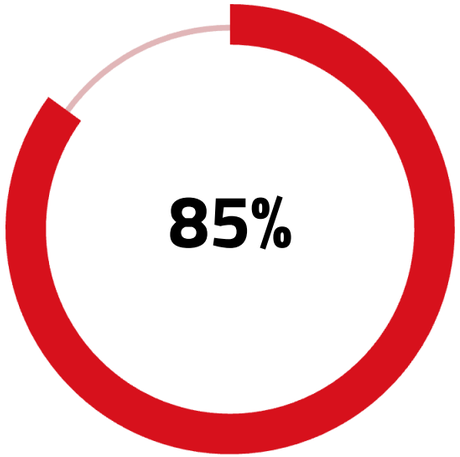
Intensificare scansioni per individuare esposizione a CVE critiche. Focus su perimetro esterno e cloud

La settimana ha evidenziato un incremento significativo di vulnerabilità ad alta gravità con exploit pubblici disponibili. Le organizzazioni devono prioritizzare il patch management e implementare controlli compensativi dove l'aggiornamento immediato non è possibile.

ANALISI

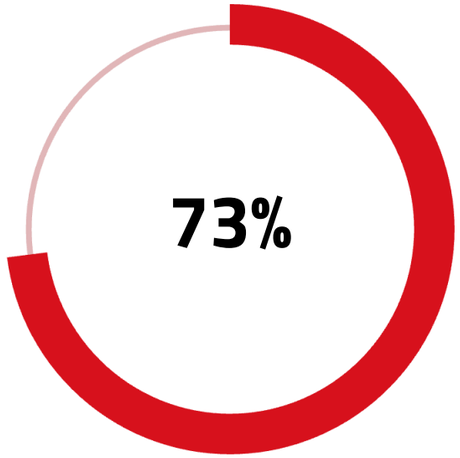
Analisi Trasversale e Tendenze

L'analisi della settimana rivela un incremento preoccupante delle attività malevole con sofisticazione crescente. Le organizzazioni italiane ed europee affrontano minacce sempre più complesse che richiedono vigilanza costante e approcci di sicurezza multilivello.



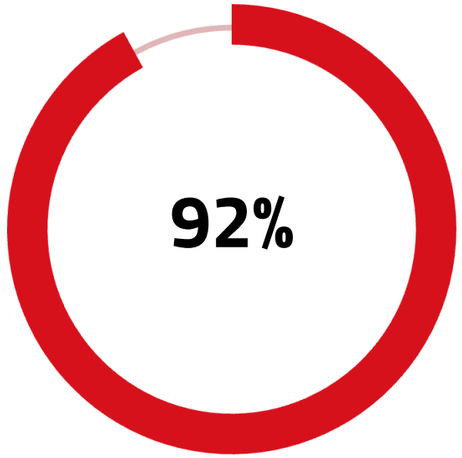
Aumento Ransomware

Crescita attacchi rispetto a settimana precedente



Vulnerabilità Critiche

Percentuale patch con CVSS >8.0



Phishing Efficace

Tasso successo campagne AI-powered

Tendenze Emergenti

- Ransomware mira a settori specifici con attacchi mirati
- Botnet sfruttano credenziali deboli su infrastrutture cloud
- Phishing AI-generated bypassa controlli tradizionali
- Targeting ransomware verso dipendenti con accessi critici

Settori più Colpiti

- Sanità: sistemi medicali vulnerabili
- Finanza: phishing bancario intensificato
- PMI: difese limitate vs ransomware
- PA: 30K+ email esposte aumentano superficie attacco

RACCOMANDAZIONI

Raccomandazioni Operative Prioritarie

Per affrontare efficacemente le minacce rilevate, le organizzazioni devono adottare un approccio proattivo e multilivello alla sicurezza informatica. Le seguenti azioni prioritarie sono raccomandate per la settimana.

01

Patch Management Rigoroso

Applicare entro 48-72 ore patch per CVE-2025-61937 (AVEVA), CVE-2026-0491 (SAP) e Patch Tuesday Microsoft. Priorità massima per sistemi esposti a Internet

02

Formazione Continua

Sensibilizzare dipendenti su phishing bancario (Banco BPM), Google Ads malicious e LinkedIn scam. Focus su riconoscimento email AI-generated

03

Difesa Multistrato

Implementare SIEM per correlazione eventi, segmentazione rete per contenimento laterale, e backup immutabili per difesa ransomware

04

Monitoraggio Proattivo

Intensificare monitoraggio per IOC correlati a Sinobi, Qilin, GoBruteforcer e Kimwolf. Hunting proattivo su accessi anomali e movimenti laterali

05

Collaborazione Settoriale

Condividere intelligence con CSIRT Italia coordinandosi tramite sistemi DDoP sulla sicurezza condivisa

Framework di Implementazione

1

Valutazione Rischio

Mappatura completa superfici di attacco e priorità asset critici

2

Prioritizzazione

Focus su vulnerabilità critica/organizzazione esposta

3

Implementazione

Roll-out patch, configurazioni di sicurezza, e formazione utenti

4

Verifica

Testing efficacia difese via security assessment

5

Miglioramento

Revisione continua in base a lesson learned

Coordinamento Nazionale: Per minacce che coinvolgono infrastrutture critiche nazionali o dati PA, coordinare risposta con CSIRT Italia e ACN per massimizzare efficacia delle contromisure.

13K

Post Analizzati Fonti OSINT monitorate settimanalmente

7

Giorni Copertura Monitoraggio continuativo minacce

24/7

MonitoraggioSorveglianza indicatori compromissione

S3K Group: Il Vostro Partner di Fiducia

S3K Group S.p.A. - Security of the Third Millennium si posiziona come Full Service Partner della Digital & Security Transformation, guidando i clienti nei processi di cambiamento e riducendo complessità e rischi attraverso competenze multidisciplinari integrate.

Cybersecurity Excellence

Managed Security Services, SOC, Threat Intelligence e consulenza specialistica per protezione completa

Data Analytics & Big Data

Soluzioni avanzate per elaborazione, analisi e valorizzazione dei dati aziendali

Cloud & Infrastructure

Gestione infrastrutture, migrazione cloud e Infrastructure Management professionale

550+

Professionisti

40

Partnership

500+

Clienti Attivi

I Nostri Valori: Affidabilità, Integrità, Rispetto, Valorizzazione delle Persone, Passione, Innovazione

Contatti:

- **Email:** contattaci@s3kgroup.it
- **Marketing:** marketing@s3kgroup.it

TLP:CLEAR DIVULGAZIONE ILLIMITATA

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).

Company Profile S3K

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:CLEAR = Divulgazione illimitata

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

Cyber security

RISK REPORT

S3K

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

ISO 14001 BUREAU VERITAS Certification

ISO 27001 BUREAU VERITAS Certification

ISO 9001 BUREAU VERITAS Certification

ISO 45001 BUREAU VERITAS Certification