S3K

Cyber security

RISK REPORT

\ week 19/01/2026 - 25/01/2026

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 (18/01/2026 – 25/01/2026)

Aumento Attacchi Ransomware

Gruppi come Clop, Qilin e Sarcoma hanno intensificato gli attacchi, colpendo aziende italiane e internazionali, evidenziando la necessità di misure di sicurezza rafforzate

Vulnerabilità Critiche Sfruttate

Vulnerabilità critica nel servizio telnetd scoperta. Exploit attivi segnalati in prodotti Cisco e Oracle, richiedendo aggiornamenti immediati

Data Leak e Violazioni

Leak di credenziali e database contenenti dati sensibili di aziende italiane, aumentando il rischio di attacchi mirati e furti di identità

- **Campagne di Phishing Mirate**

  Campagne che sfruttano loghi ufficiali e piattaforme legittime, con particolare attenzione alle imminenti Olimpiadi di Milano-Cortina 2026

- **Malware Evoluto**

  Nuove tecniche di malware inclusi attacchi a infrastrutture critiche e utilizzo di intelligenza artificiale, evidenziando la crescente sofisticazione degli attaccanti

NEWS CYBER

Attività Malevole della Settimana

Il panorama della sicurezza informatica ha visto un aumento significativo delle attività malevole, con diversi attacchi ransomware e vulnerabilità critiche sfruttate da gruppi di hacker. Le minacce si sono concentrate su organizzazioni in vari settori, evidenziando la necessità di una vigilanza costante e di aggiornamenti tempestivi delle misure di sicurezza.

Attacchi Ransomware Dominanti

- Clop colpisce ITROBOTICS.COM e AERIFY.IO
- Qilin attacca HARTE-BAVENDAMM (Germania) e YCC Parts Mfg (UK)
- Dragonforce compromette Uinta Bank (USA) e HanseMerkur (Germania)
- Sarcoma colpisce MecMatica (Italia) con 74 GB esfiltrati

Vulnerabilità Critiche

- Bypass autenticazione telnetd per accesso root
- Broadcom rilascia aggiornamenti Web Security Services Agent
- Vulnerabilità Oracle con PoC disponibile (CVE-2026-21962)
- Exploit attivi su prodotti Cisco (CVE-2026-20045)

Focus Italia: La società italiana MecMatica è stata compromessa dal gruppo Sarcoma, con 74 GB di dati esfiltrati inclusi database SQL e registri clienti sensibili, sottolineando l'urgenza per le aziende italiane del settore software di adottare misure di sicurezza rafforzate.

DATA BREACH

Data Leak & Breach: Scenario Italiano

2.5K

Kit Documenti Italiani

Database con 2.500 kit di documenti italiani, inclusi documenti d'identità e selfie, in vendita su dark web

143K

Combolist Email/Password

Lista di 143.000 combinazioni email/password italiane pubblicata per attacchi di credential stuffing

1K

Email MegaCloud

Leak di accesso a 1.000 email italiane tramite MegaCloud per campagne di phishing

3

Pannelli Admin Compromessi

Credenziali di accesso per pannelli amministrativi di ylon.it, creditline.it, pmadvisors.it

La settimana ha evidenziato un aumento preoccupante delle violazioni di dati e dei leak, con un impatto diretto sulle organizzazioni italiane ed europee. Sono emersi leak di credenziali e database contenenti dati sensibili che potrebbero essere sfruttati per attacchi mirati e furti di identità. L'esposizione di documenti personali e accessi amministrativi rappresenta una minaccia seria per la sicurezza e la privacy.

Rischi per Settori Critici

Settore Energia

Wiper malware contro la rete energetica polacca. Attacco mirato in coincidenza con il decimo anniversario dell'attacco russo alla rete ucraina

Settore Software

MecMatica (Italia) colpita da Sarcoma. Attacco Watering Hole su EmEditor. Evelyn Stealer prende di mira sviluppatori Microsoft Visual Studio Code

Settore Bancario

Phishing mirato contro SPID sfruttando logo AdE e Google Sites. Aumento campagne contro piattaforme bancarie legittime

Eventi Critici

Olimpiadi Milano-Cortina 2026: phishing e siti spoofed identificati come principali minacce informatiche per l'evento

MALWARE

Malware & Infrastructure

L'intensificazione delle attività malevole ha visto un aumento significativo degli attacchi mirati a settori critici e nuove tecniche di evasione. Diverse campagne hanno colpito utenti e organizzazioni, evidenziando la crescente sofisticazione degli attaccanti e l'uso di tecnologie avanzate come l'intelligenza artificiale.

Attacchi Mirati Infrastrutture

1. **Wiper Malware Polonia:** Malware distruttivo contro rete energetica polacca, attacco sventato ma evidenzia rischio per infrastrutture critiche europee
2. **Watering Hole EmEditor:** Attacco mirato agli utenti di EmEditor per furto di informazioni
3. **Malware Windows Security:** Nuovo attacco per disabilitare le protezioni di sicurezza di Windows

Minacce AI-Powered

Konni AI-Generated

Malware generato da IA per attaccare ingegneri blockchain

Evelyn Stealer

Furto credenziali sviluppatori e dati crittografici Visual Studio Code

Android AI Trojan

Trojan che usano IA per cliccare su annunci nascosti nei browser

Il gruppo Konni ha iniziato a utilizzare malware generato da intelligenza artificiale per attaccare ingegneri blockchain. Questo approccio innovativo rappresenta una nuova frontiera nelle tecniche di compromissione e richiede strategie di difesa adeguate.

Phishing & Social Engineering

01

Phishing con Logo AdE

Campagna che utilizza logo Agenzia delle Entrate per rubare credenziali SPID tramite siti fraudolenti

02

Scadenza Tessera Sanitaria

Campagna con messaggi su scadenza Tessera Sanitaria per indurre vittime a fornire dati personali

03

Google Sites SPID

Nuova campagna che sfrutta Google Sites per ingannare utenti SPID aumentando credibilità del sito

04

Olimpiadi Milano-Cortina 2026

Phishing e siti spoofed identificati come principali minacce per le imminenti Olimpiadi

05

LogMeIn RMM Attack

Attacco con credenziali rubate per installare LogMeIn RMM e accesso persistente ai sistemi

Tecniche Utilizzate

- Sfruttamento loghi ufficiali (AdE)
- Uso piattaforme legittime (Google Sites)
- Messaggi su servizi pubblici (Tessera Sanitaria)
- Abuso di Zendesk per email legittime ma malevole

Contromisure Adottate

- 1Password introduce avvisi pop-up per siti sospetti
- Maggiore sensibilizzazione su eventi critici (Olimpiadi)
- Monitoraggio campagne social engineering su LinkedIn
- Protezione credenziali e accessi persistenti

RANSOMWARE

Operazioni Ransomware Active

La settimana ha registrato un'espansione significativa delle operazioni ransomware con Clop, Qilin e Sarcoma che dominano il panorama. Settori colpiti includono software, manifatturiero, alimentare e trasporti, con attacchi che si estendono globalmente.

Sarcoma - Target Italia

MecMatica compromessa con 74 GB di dati esfiltrati, inclusi database SQL e registri clienti sensibili. Focus su settore software italiano

Clop - Attacchi Multipli

Serie di vittime rivendicate: RSTRT.IT, ITROBOTICS.COM (USA), AERIFY.IO. Aggressività elevata con più obiettivi in breve tempo

Qilin - Espansione Europea

Attacchi confermati: Casadei (Italia), HARTE-BAVENDAMM (Germania), YCC Parts Mfg (UK). Vulnerabilità aziende manifatturiere

Thegentlemen - Settore Alimentare

Sita-Sud e San Carlo Gruppo Alimentare colpiti. Potenziale impatto su operazioni di trasporto e produzione alimentare

Lockbit ha rivendicato un attacco contro frandent.it, mentre worldleaks ha colpito LTS Group. Ingram Micro è stata compromessa con impatto su circa 42.000 persone, evidenziando l'ampia portata degli attacchi ransomware.

VULNERABILITÀ

Vulnerabilità Critiche & Patch

1

CVE-2026-1162

UTT HiPER 810: Buffer overflow nella funzione strcpy. CVSS 9.3. Attacchi remoti possibili, correzione immediata necessaria

2

CVE-2025-64293

Golemiq 0 Day Analytics: SQL Injection in plugin WordPress. CVSS 7.6. Compromissione dati possibile

3

Exploited - SmarterMail

Vulnerabilità 0-day con sfruttamento attivo: Authentication Bypass e Remote Code Execution. Monitoraggio sistemi urgente

4

CVE-2026-21962

Oracle: PoC pubblico disponibile. Rischio di gravi conseguenze. Aggiornamento immediato raccomandato

5

CVE-2026-20045

Cisco Products: Sfruttamento attivo confermato. RCE e escalation privilegi. Patch urgente per sistemi esposti

6

Telnetd Critical

Bypass autenticazione nel servizio telnetd per accesso root. Aggiornamenti regolari e patching critici

Vulnerabilità Aggiuntive

CVE-2025-12420

ServiceNow: PoC per escalation privilegi reso pubblico. Applicare patch disponibili per mitigare rischio

CVE-2025-62507

Redis: PoC per Remote Code Execution scoperto. Mantenere sistemi aggiornati per evitare sfruttamenti

CVE-2025-2913

HDF5: Vulnerabilità critica che consente attacchi locali. Prestare attenzione e applicare patch necessarie

Broadcom Updates

Aggiornamenti di sicurezza per Web Security Services Agent, affrontando escalation privilegi. Implementazione immediata invitata

Raccomandazione Immediata

Priorità assoluta per patch telnetd, Cisco CVE-2026-20045, e Oracle CVE-2026-21962 entro 48 ore

Vulnerability Scanning

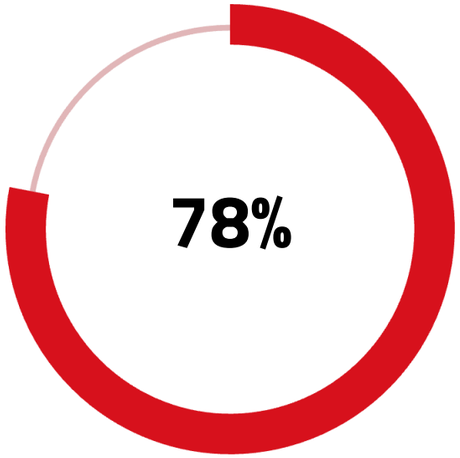
Intensificare scansioni per SmarterMail 0-day e prodotti con exploit attivi. Focus su perimetro esterno

La settimana ha evidenziato un incremento delle vulnerabilità critiche e degli exploit attivi che potrebbero avere un impatto significativo sulle organizzazioni. È essenziale che le aziende italiane ed europee rimangano vigili e aggiornino tempestivamente i loro sistemi per mitigare i rischi associati a queste minacce in continua evoluzione.

ANALISI

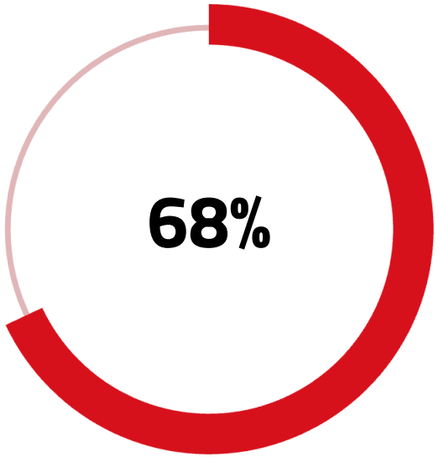
Analisi Trasversale e Tendenze

L'analisi della settimana rivela un incremento preoccupante delle attività malevole con sofisticazione crescente. I gruppi di ransomware hanno intensificato le loro operazioni, mentre vulnerabilità significative sono state sfruttate per ottenere accesso non autorizzato a sistemi sensibili. Le organizzazioni italiane ed europee affrontano minacce sempre più complesse.



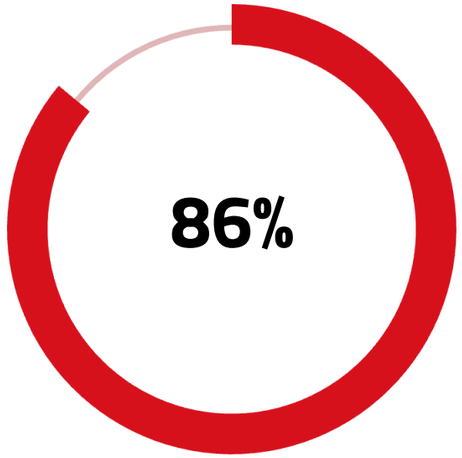
Attacchi Ransomware

Aumento intensità operazioni Clop, Qilin, Sarcoma



Exploit Attivi

Percentuale vulnerabilità con sfruttamento confermato



Phishing Efficace

Tasso successo campagne che sfruttano loghi ufficiali

Tendenze Emergenti

- Ransomware mira aziende italiane (MecMatica, Casadei, San Carlo)
- Malware AI-generated aumenta efficacia attacchi (Konni)
- Phishing sfrutta eventi critici (Olimpiadi Milano-Cortina 2026)
- Attacchi a infrastrutture energetiche critiche europee

Settori più Colpiti

- Software: MecMatica, sviluppatori Visual Studio Code
- Energia: rete energetica polacca sotto attacco
- Manifatturiero: Casadei e aziende europee
- Servizi pubblici: SPID e Tessera Sanitaria target phishing

RACCOMANDAZIONI

Raccomandazioni Operative Prioritarie

Per affrontare efficacemente le minacce rilevate, le organizzazioni devono adottare un approccio proattivo e multilivello alla sicurezza informatica. Il contesto delle imminenti Olimpiadi di Milano-Cortina 2026 richiede particolare attenzione. Le seguenti azioni prioritarie sono raccomandate.

01

Patch Management Critico

Applicare immediatamente patch per telnetd bypass, Cisco CVE-2026-20045, Oracle CVE-2026-21962 e SmarterMail 0-day. Priorità massima per sistemi esposti

02

Formazione Continua

Sensibilizzare dipendenti su phishing SPID (AdE, Google Sites), campagne Tessera Sanitaria e minacce Olimpiadi 2026. Focus su riconoscimento loghi falsificati

03

Protezione Credenziali

Monitorare leak di pannelli admin (ylon.it, creditline.it, pmadvisors.it) e combolist 143K email/password. Implementare autenticazione multi-fattore

04

Monitoraggio Proattivo

Intensificare hunting per IOC correlati a Clop, Qilin, Sarcoma e malware AI-generated. Monitorare accessi anomali e esfiltrazione dati

05

Preparazione Eventi Critici

Rafforzare sicurezza per Olimpiadi Milano-Cortina 2026. Coordinamento con CSIRT Italia per protezione da phishing e siti spoofed

Framework di Implementazione

1

Valutazione Rischio

Mappatura superfici di attacco e identificazione asset critici esposti a vulnerabilità attive

2

Prioritizzazione

Focus su telnetd, Cisco, Oracle, SmarterMail e protezione contro ransomware italiani

3

Implementazione

Roll-out patch urgenti, configurazioni MFA, formazione su phishing Olimpiadi 2026

4

Verifica

Testing efficacia difese anti-ransomware e risposta a campagne phishing SPID

5

Miglioramento

Revisione continua basata su intelligence Clop/Qilin/Sarcoma e lesson learned

Coordinamento Nazionale: Per minacce che coinvolgono aziende italiane (MecMatica, Casadei, San Carlo) o eventi nazionali (Olimpiadi 2026), 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.

S3K

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