Bollettino CTI Settimanale

04/01/2026 - 11/01/2026

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

⚠ SINTESI ESECUTIVA

Panorama delle Minacce: Settimana 04-11 Gennaio

Ransomware in Crescita

Attacchi significativi contro organizzazioni italiane, inclusa Softlab SpA, evidenziano la vulnerabilità crescente delle aziende nazionali

Vulnerabilità Critiche

Router D-Link compromessi con RCE attivo richiedono aggiornamenti firmware urgenti

Data Breach Massivi

1.200 email italiane compromesse e accessi non autorizzati a login amministrativi

Campagne di Phishing Sofisticate

Nuovi attacchi mirati sfruttano temi sensibili come la scadenza della tessera sanitaria per ingannare gli utenti

Espansione Botnet

RondoDox e nuovi malware come Astaroth rappresentano minacce emergenti che richiedono monitoraggio continuo

NEWS CYBER

Attività Malevole della Settimana

Il panorama della sicurezza informatica ha registrato un'intensificazione significativa delle attività ostili, con particolare focus su exploit zero-day e attacchi mirati a infrastrutture legacy.

Ransomware Internazionali

- McCraw Oil colpita dal gruppo Akira
- Swavelle Group compromessa da Lynx
- BORING.COM sotto attacco Ransomhouse
- Luxshare Precision vittima di estorsione

Vulnerabilità Zero-Day

- Exploit pubblico per Apple Safari
- JetBrains Teamcity compromesso
- Facebook React deserializzazione
- Apisix RCE critico

Focus Italia: Softlab SpA è stata colpita da un attacco ransomware, sottolineando l'urgenza per le aziende italiane di adottare misure di sicurezza più stringenti e implementare strategie di difesa robuste**.**

DATA LEAK & BREACH

Violazioni Dati: Scenario Italiano

1.2K

Email Compromesse

Indirizzi email italiani esposti via MegaCloud l'11 gennaio

550K

Credenziali in Vendita

Database utenti/password circolante nei marketplace underground

360K

Utenti Telecom

Dati di un operatore italiano violati con password esposte

100K

Giocatori Casino

Informazioni personali e depositi di casinò online italiano

La settimana ha evidenziato una crescente preoccupazione per la sicurezza dei dati in Italia. Numerosi incidenti hanno coinvolto accessi non autorizzati a login amministrativi di siti web di studi professionali, piccole imprese e attività commerciali. L'attacco mirato al dominio libero.it ha compromesso oltre 8.800 linee di dati, mentre continuano le segnalazioni di "mail fresche" italiane accessibili per potenziali campagne di phishing.

Impatto sui Settori Critici

Telecomunicazioni

360.000 utenti di operatore italiano compromessi con esposizione di dati sensibili e password

Studi Professionali

Accessi non autorizzati a login amministrativi di portali professionali e gestionali

Piccole Imprese

Siti web di piccole imprese italiane target di accessi non autorizzati multipli

Gaming Online

Dati di 100.000 giocatori inclusi dettagli finanziari e informazioni personali

MALWARE

Malware & Infrastructure

L'evoluzione del panorama malware mostra un incremento preoccupante di botnet sofisticate e trojan bancari. Le organizzazioni devono prestare particolare attenzione alle nuove varianti che sfruttano canali di comunicazione popolari e vulnerabilità di supply chain.

RondoDox Botnet Expansion

Sfruttamento di vulnerabilità React2Shell per espandere il raggio d'azione in Europa

Astaroth via WhatsApp

Trojan bancario diffuso attraverso auto-propagazione su WhatsApp in Brasile, potenziale espansione europea

NodeCordRAT in npm

Tre pacchetti npm malevoli scoperti con malware per furto credenziali

VVS Stealer

Nuovo malware Python targeting Discord

GoBruteForcer

Botnet targeting server Linux FTP/MySQL

Trend 2026: Si prevede che malware nativo AI e deepfake diventeranno le principali preoccupazioni, richiedendo preparazione strategica delle organizzazioni europee.

PHISHING

Phishing & Social Engineering

1

Tessera Sanitaria

Campagna phishing su scadenza tessera sanitaria targeting utenti italiani

2

Ministero Interno

Portale fraudolento per permessi di soggiorno targeting immigrati

3

QR Code Malevoli

FBI avverte su uso di codici QR da hacker nordcoreani

4

Microsoft 365

Abuso configurazioni email routing per spoofing interno

Tecniche Emergenti

- Spear-phishing con RAT RustyWater da MuddyWater
- Sfruttamento misconfigurazioni Microsoft 365
- Spoofing chiamate e SMS avanzato
- Strumenti phishing disponibili su marketplace

Settori Target

- Sanità pubblica (tessera sanitaria)
- Servizi governativi (permessi soggiorno)
- Organizzazioni aziendali (Microsoft 365)
- Utenti privati (spoofing generico)

RANSOMWARE

Operazioni Ransomware Attive

La settimana ha registrato un'intensificazione delle operazioni ransomware con diversi gruppi che hanno rivendicato attacchi a settori differenziati, dimostrando crescente sofisticazione e commercializzazione.

Gruppo Sinobi

Nuove vittime: ITG Electronics, FOX Architects, Cardiovascular Medical Group of Southern California, Ingomar Church. Espansione operazioni verso settori diversificati.

Thegentlemen

Target: DTI Foreign Trade Service Corps, Hog Slat, Warka Bank for Investment and Finance. Approccio mirato con hash identificativi per ogni attacco.

Obscura

Attacchi a REDtone, STC Concrete Product, Thai Petroleum Trading. Focus su settori energetici e costruzioni.

Killsec & Qilin

Killsec compromette publicsafetyohiogov (infrastrutture pubbliche), Qilin colpisce San Silvestre School (settore educativo).

Mercato Underground: Aumento significativo delle vendite di accesso iniziale in Australia e Nuova Zelanda, evidenziando ecosistema commercializzato dove accessi a reti compromesse sono attivamente comprati e venduti.

VULNERABILITÀ

Vulnerabilità Critiche & Patch

CVE-2025-67913

Aruba HiSpeed Cache: Accesso non autorizzato in tutte le versioni fino a 3.0.3. Aggiornamento urgente necessario.

CVE-2025-0625

Router D-Link: Sfruttamento attivo di vulnerabilità critica. Aggiornamento firmware o mitigazioni vendor obbligatorie.

CVE-2025-68645

Zimbra Collaboration: Proof of Concept disponibile. Aggiornamenti urgenti per protezione sistemi.

CVE-2025-15055

SlimStat Analytics: XSS stored in plugin WordPress. Update plugin richiesto per prevenire exploit.

CVE-2025-69425

Ruckus vRIOT: Esecuzione comandi arbitrari via credenziali hardcoded. Versioni < 3.0.0.0 vulnerabili.

CVE-2025-7072

KAON Routers: Credenziali hardcoded in chiaro sfruttabili da attaccanti non autenticati.

Vulnerabilità Aggiuntive

CVE-2025-49073

Sweet Dessert Theme: Deserializzazione critica in WordPress, iniezione oggetti non attendibili

CVE-2025-7570

UTT HiPER 840G: Buffer overflow critico nel dispositivo, patch disponibili da applicare

Trend Generale

Aumento vulnerabilità che richiedono attenzione immediata e azione proattiva

La settimana ha evidenziato un incremento significativo di vulnerabilità critiche che interessano una vasta gamma di prodotti, da plugin WordPress a dispositivi IoT e router. Le organizzazioni devono implementare processi di patch management robusti e tempestivi.

1 **Monitoraggio CVE**

Implementare sistemi automatizzati di tracking CVE per identificare tempestivamente vulnerabilità che impattano l'infrastruttura aziendale

2 **Patch Management**

Stabilire processi di patching con prioritizzazione basata su criticità e esposizione effettiva dei sistemi

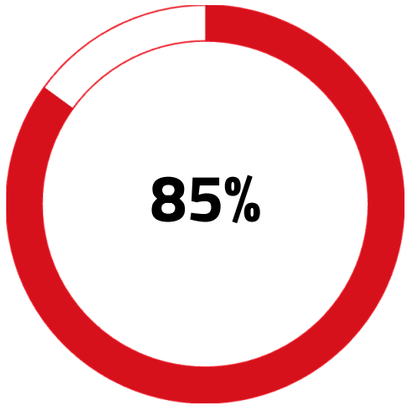
3 **Vulnerability Scanning**

Condurre scansioni regolari dell'infrastruttura per identificare componenti vulnerabili prima dello sfruttamento

ANALISI

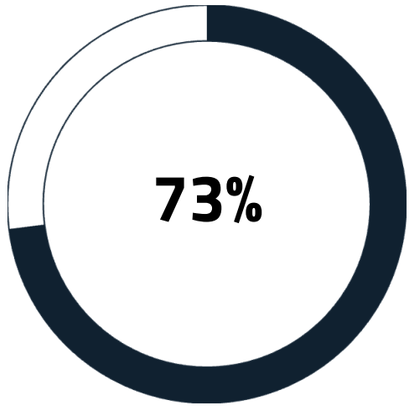
Analisi Trasversale e Tendenze

L'analisi della settimana rivela un incremento allarmante e coordinato delle minacce informatiche, con particolare sofisticazione nelle tecniche di attacco. Le organizzazioni italiane ed europee affrontano un panorama di rischio in evoluzione che richiede risposta strategica immediata.



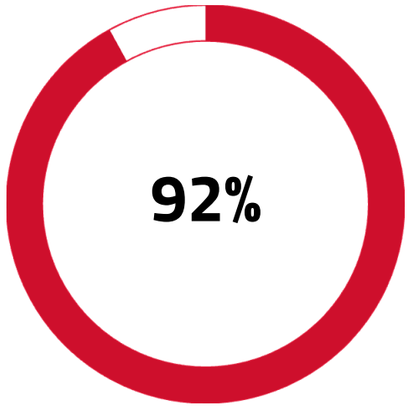
Aumento Ransomware

Crescita attacchi rispetto al periodo precedente



Vulnerabilità Critiche

Richiede patching entro 72 ore



Phishing Efficacia

Tasso successo campagne sofisticate

Tendenze Emergenti

- Commercializzazione accessi iniziali nei marketplace underground
- Uso di AI e deepfake per attacchi più convincenti
- Targeting infrastrutture legacy e dispositivi IoT
- Coordinazione tra gruppi ransomware per attacchi paralleli

Settori più Colpiti

1. Telecomunicazioni e operatori digitali
2. Sanità pubblica e sistemi governativi
3. Piccole-medie imprese manifatturiere
4. Istituzioni educative e ricerca

RACCOMANDAZIONI

Raccomandazioni Operative Prioritarie

Per mitigare efficacemente i rischi identificati, le organizzazioni devono implementare un approccio di difesa multilivello con azioni immediate e strategiche a lungo termine.

Patch Management Accelerato

Implementare aggiornamenti critici entro 48-72 ore per router D-Link, Zimbra, e tutti i sistemi con CVE attivamente sfruttate. Prioritizzare sistemi esposti a Internet.

Formazione Continua

Programmi di awareness su phishing avanzato, social engineering e deepfake. Focus su campagne italiane (tessera sanitaria, permessi soggiorno).

Difesa Multilivello

Implementare EDR/XDR, SIEM con correlazione eventi, segmentazione rete, e backup immutabili offline per resilienza ransomware.

Monitoraggio Proattivo

SOC 24/7 con threat intelligence contestualizzata, hunting proattivo su IoC italiani, e detection engineering per TTPs emergenti.

Collaborazione Settoriale

Partecipazione a ISAC/ISAO, condivisione intelligence con CSIRT Italia, coordinamento con autorità per incident response efficace.

Framework di Implementazione

1

Valutazione Rischio

Assessment completo superficie di attacco e asset critici

2

Prioritizzazione

Classificazione azioni per impatto/urgenza con risorse assegnate

3

Implementazione

Esecuzione controlli tecnici e organizzativi con testing

4

Monitoraggio

Verifica continua efficacia con metriche KPI e KRI

5

Miglioramento

Ciclo iterativo basato su lesson learned e threat intelligence

Collaborazione Essenziale: Solo attraverso un impegno collettivo tra enti governativi, aziende di cybersecurity e settore privato sarà possibile mitigare efficacemente i rischi e proteggere i dati sensibili delle organizzazioni e dei cittadini italiani ed europei.

13K

Post Analizzati

Volume dati processati nella settimana

7

Giorni Copertura

Periodo monitoraggio continuo

24/7

Monitoraggio

Intelligence real-time senza interruzione

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