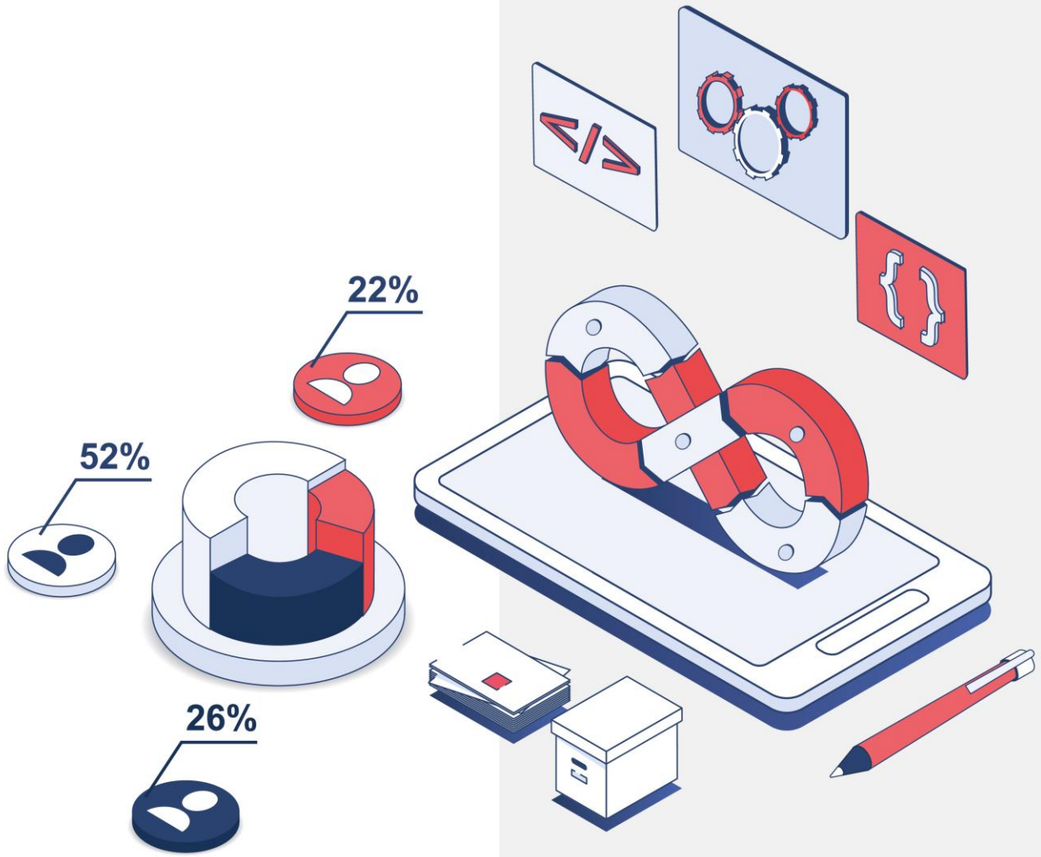
S3K

Cyber Threat

WEEKLY REPORT

\ week 23/02/2026 - 01/03/2026



www.s3kgroup.it

CTI WEEKLY

Aumento delle vulnerabilità critiche

Cisco e Trend Micro hanno rilasciato patch per vulnerabilità critiche che potrebbero compromettere sistemi ampiamente utilizzati, richiedendo aggiornamenti urgenti dalle organizzazioni italiane.

Attacchi ransomware mirati

Il gruppo Qilin ha rivendicato un attacco contro Traffic Tech in Italia, evidenziando la vulnerabilità delle aziende locali e la necessità di misure di sicurezza rafforzate.

Violazioni di dati significative

Le violazioni di dati di aziende come Odido e ManoMano hanno esposto milioni di informazioni personali, sottolineando l'importanza della protezione dei dati sensibili.

- **Nuove minacce malware**

  Emergenza di nuovi malware come Oblivion e PromptSpy, che colpiscono dispositivi Android con tecniche avanzate di evasione e AI generativa.

- **Campagne di phishing attive**

  Attacchi di phishing mirati a INPS ed Enel hanno messo a rischio le credenziali bancarie degli utenti, con 73 campagne malevole rilevate dal CERT-AGID.

NEWS CYBER

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo delle vulnerabilità critiche e degli attacchi ransomware, con un focus particolare su software ampiamente utilizzati. Diverse aziende, tra cui SolarWinds e Trend Micro, hanno rilasciato patch per vulnerabilità che potrebbero consentire l'esecuzione di codice remoto.

Vulnerabilità e Attacchi Mirati

- Vulnerabilità critiche in Apex One di Trend Micro: esecuzione codice remoto su Windows
- SolarWinds Serv-U: quattro vulnerabilità critiche con potenziale accesso root
- Hacker cinesi sfruttano vulnerabilità VPN Ivanti su decine di clienti
- Sanzioni USA contro broker russo di exploit zero-day

Incidenti e Misure Difensive

- Attacco ransomware Qilin a Traffic Tech in Italia
- Attacco ransomware a LISI Group in Francia
- Samsung raggiunge accordo con Texas per raccolta dati non autorizzata da smart TV
- Verificatruffa.it sotto attacco con temporanea sospensione del servizio

Trend Micro Alert: Sono state corrette due vulnerabilità critiche in Apex One che consentono l'esecuzione di codice remoto su sistemi Windows vulnerabili. Le organizzazioni devono aggiornare urgentemente i loro sistemi per mitigare il rischio. Approfondisci

DATA BREACH

Data Leak & Breach: Scenario Settimanale

316K

Account Odido

La compagnia olandese ha subito una violazione con 1 milione di record pubblicati, inclusi email, telefoni e dati bancari

38M

Clienti ManoMano

La catena fai-da-te ha notificato una violazione causata da un attacco a un fornitore terzo, esponendo dati personali di milioni di clienti

208GB

Dati Air Côte d'Ivoire

Il gruppo INC ha rivendicato il furto di 208 GB di dati dalla compagnia aerea, evidenziando la vulnerabilità del settore trasporti

90

Batch Niflheim

Pubblicate diverse liste di email italiane con batch dal 71 al 90, rappresentando un rischio significativo per la privacy degli utenti

La settimana ha evidenziato un aumento preoccupante delle violazioni di dati, con impatti significativi su utenti e aziende in Italia e in Europa. Oltre ai breach principali, sono state diffuse liste di email italiane e dati di Eurotours Italia, mentre Cisco ha avvertito dello sfruttamento attivo di una vulnerabilità critica per infiltrarsi nelle reti di grandi clienti.

Minacce per Settori Critici: Dettaglio Breach

Settore Telecomunicazioni

Odido ha subito una violazione con 316.912 account compromessi e 1 milione di record pubblicati, inclusi indirizzi email, numeri di telefono e dati bancari di clienti europei

Settore Retail / E-Commerce

ManoMano ha notificato una violazione causata da un attacco a un fornitore di servizi terzo, esponendo le informazioni personali di circa 38 milioni di clienti

Settore Sport e Intrattenimento

L'Olympique Marseille ha confermato un attacco informatico dopo che un attore malevolo ha rivendicato la compromissione dei sistemi del club, sottolineando la vulnerabilità anche delle organizzazioni sportive

Settore Hospitality & Gaming

Wynn Resorts ha confermato che un hacker ha rubato dati dei dipendenti dopo essere stata elencata su un sito di leak, evidenziando la necessità di proteggere le informazioni interne aziendali

MALWARE

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un incremento significativo delle minacce, con nuovi strumenti e tecniche emergenti che pongono sfide crescenti per le organizzazioni in Italia e in Europa. Campagne mirate colpiscono settori critici come l'istruzione e la sanità, mentre nuove varianti Android e attacchi a reti isolate attirano l'attenzione degli esperti.

Nuovi Malware Identificati

1. **Oblivion RAT:** Remote Access Trojan venduto a 300$/mese, capace di compromettere dispositivi Android dalla versione 8 alla 16. Approfondisci
2. **PromptSpy:** Primo malware Android a integrare AI generativa, con capacità di adattamento dinamico che rendono difficile la rilevazione. Approfondisci
3. **DarkCloud Infostealer:** Utilizza tecniche di evasione in Visual Basic 6 e metodi di crittografia avanzata per il furto di credenziali aziendali.

Minacce Emergenti

APT37 – Reti Isolate

Hacker nordcoreani sviluppano strumenti per spostare dati tra sistemi connessi e reti isolate tramite drive rimovibili per sorveglianza clandestina.

Campagna Dohdoor

Cisco Talos ha scoperto una campagna che colpisce istruzione e sanità, utilizzando un backdoor "Dohdoor" per attacchi multi-fase.

QuickLens Compromessa

L'estensione Chrome è stata rimossa dopo essere stata compromessa per rubare criptovalute da migliaia di utenti tramite supply chain attack.

SURXRAT, un Trojan per Android, è emerso come operazione di malware strutturata commercialmente. Moonrise RAT è un Trojan basato su Go progettato per mantenere un C2 attivo senza essere rilevato, con potenziali conseguenze costose per le vittime. Le organizzazioni devono rimanere vigili sulle minacce mobile emergenti.

Phishing & Social Engineering

01

Phishing ai danni di INPS ed Enel

Il CERT-AGID ha segnalato campagne che sfruttano i nomi di INPS ed Enel per rubare credenziali bancarie tramite email che richiedono aggiornamenti per presunti rimborsi, portando a pagine di login fasulle.

02

Campagna "Diesel Vortex"

Gruppo finanziariamente motivato ha lanciato attacchi contro operatori logistici in Europa e USA, usando 52 domini per rubare oltre 1.600 credenziali e dirottare spedizioni. Leggi di più

03

Campagne CERT-AGID: 73 rilevate

Il CERT-AGID ha identificato 73 campagne malevole, di cui 45 mirate a obiettivi italiani. Forniti 968 indicatori di compromissione (IoC) alle organizzazioni accreditate.

04

Phishing a tema Google Docs / OAuth 2.0

Campagna rilevata che usa il protocollo OAuth 2.0 per ottenere Access Token permanenti, accedendo ai dati Microsoft 365 degli utenti e bypassando l'autenticazione a più fattori.

05

Attacco Vishing a Optimizely

L'azienda di tecnologia pubblicitaria ha confermato una violazione dei dati a seguito di un attacco di vishing che ha compromesso alcuni dei suoi sistemi. Ulteriori dettagli

Tecniche Avanzate Emergenti

- Email spoofing: 44% delle principali aziende italiane vulnerabile
- Smishing con finte consegne e servizi bancari in aumento
- Phishing OAuth 2.0 per aggirare MFA su Microsoft 365
- Vishing come vettore di violazione aziendale confermato

Target Principali Italiani

- Utenti INPS (credenziali bancarie e rimborsi fittizi)
- Clienti Enel (aggiornamenti presunti e pagine login fasulle)
- Operatori logistici europei (campagna Diesel Vortex)
- Account Microsoft 365 (bypass MFA via OAuth 2.0)

RANSOMWARE

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama degli attacchi ransomware ha mostrato un'attività intensa e preoccupante, con diverse organizzazioni colpite in vari settori. Le vulnerabilità note continuano a essere sfruttate rapidamente dai gruppi di cybercriminali, con un uso sempre più strategico delle cyber minacce a livello geopolitico.

Traffic Tech – Italia (Qilin)

Il gruppo ransomware Qilin ha rivendicato un attacco contro Traffic Tech in Italia, evidenziando la vulnerabilità delle aziende italiane del settore logistico a minacce informatiche mirate. 🔗 Ransomfeed

LISI Group – Francia

Un attacco ransomware ha colpito LISI Group in Francia, dimostrando come le aziende europee del settore manifatturiero siano nel mirino di attori malevoli. 🔗 Ransomfeed

Keliweb e Martecit – Italia (Vect & Tengu)

Due aziende italiane sono state recentemente colpite da attacchi ransomware, con i gruppi Vect e Tengu che hanno rivendicato le responsabilità, fornendo hash specifici per identificare le infezioni.

Air Côte d'Ivoire – Gruppo INC

La compagnia aerea ha confermato un attacco informatico con il gruppo INC che ha rivendicato il furto di 208 GB di dati, sottolineando la vulnerabilità del settore dei trasporti. 🔗 Dettagli

Sviluppi strategici e statistiche: Il capo della cybersecurity romeno ha avvertito che recenti attacchi ransomware contro infrastrutture critiche potrebbero essere parte di un'operazione ibrida russa. Nonostante l'aumento degli attacchi, il tasso di vittime che pagano riscatti è sceso al **28%**, il livello più basso mai registrato. Il gruppo Lazarus nordcoreano è stato collegato ad attacchi con Medusa contro organizzazioni sanitarie.

VULNERABILITÀ

Vulnerabilità Critiche & Patch

1

CVE-2026-20127 – Cisco SD-WAN

Bypass di autenticazione attivamente sfruttato in attacchi zero-day, consentendo a malintenzionati di compromettere i controller e inserire peer malevoli nelle reti. Aggiornamenti di sicurezza rilasciati.

2

CVE-2026-1442 – Unitree UPK

Vulnerabilità di alta gravità che espone il firmware a potenziali attacchi: la chiave di crittografia utilizzata è accessibile a chiunque, compromettendo la sicurezza dei dispositivi Unitree.

3

CVE-2025-29629 – Gardyn Home Kit

Vulnerabilità critica nel firmware che consente accesso non autorizzato a causa di credenziali predefinite deboli. Aggiornamento del firmware essenziale per evitare exploit.

4

CVE-2026-28562 – wpForo (WordPress)

Vulnerabilità di SQL injection che potrebbe consentire attacchi per estrarre credenziali dal database di WordPress. Gli utenti sono invitati ad aggiornare il plugin immediatamente.

5

CVE-2026-27767 – SWITCH EV

Grave vulnerabilità che consente attacchi di impersonificazione non autorizzata a causa di endpoint WebSocket privi di meccanismi di autenticazione, compromettendo la sicurezza delle stazioni di ricarica.

6

CVE-2026-28515 – openDCIM

Vulnerabilità critica che consente a utenti non autorizzati di modificare la configurazione dell'applicazione, esponendo i sistemi di gestione data center a potenziali attacchi.

Vulnerabilità Aggiuntive e Patch

CVE-2026-22379 – WordPress Netmix

Vulnerabilità di inclusione di file remoti che potrebbe compromettere la sicurezza dei siti web che utilizzano il tema Netmix. Aggiornamento urgente consigliato.

CVE-2026-2980 – UTT HiPER 810G

Vulnerabilità di buffer overflow che potrebbe consentire l'esecuzione di codice arbitrario su dispositivi vulnerabili, rappresentando un rischio significativo per la sicurezza delle reti.

Trend Micro Apex One

Due vulnerabilità critiche corrette che consentivano l'esecuzione di codice remoto su sistemi Windows. Aggiornamento urgente obbligatorio per le organizzazioni che utilizzano Apex One.

SolarWinds Serv-U

Quattro vulnerabilità critiche che potrebbero concedere accesso root a server non aggiornati. Rischio significativo per le infrastrutture IT aziendali.

Ivanti VPN – Sfruttamento Attivo

Hacker cinesi hanno compromesso decine di clienti Ivanti sfruttando vulnerabilità nei sistemi VPN. Patch urgenti disponibili e raccomandate.

Azione Immediata

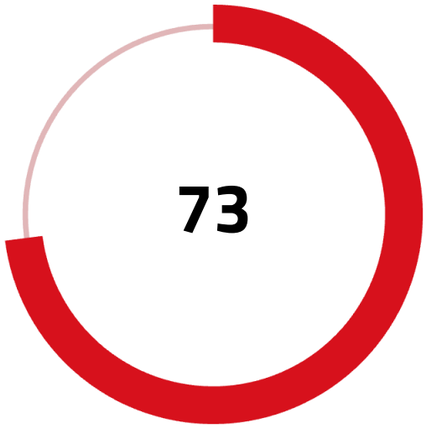
Priorità assoluta: Cisco SD-WAN, Trend Micro Apex One, SolarWinds Serv-U. Monitorare attivamente wpForo e openDCIM per versioni non aggiornate.

La settimana ha evidenziato un numero significativo di vulnerabilità critiche, con sfruttamento attivo confermato su Cisco SD-WAN e vulnerabilità nelle VPN Ivanti. Le organizzazioni devono aggiornare tempestivamente i propri software e prestare particolare attenzione ai dispositivi IoT e ai plugin WordPress esposti a SQL injection e inclusione di file remoti.

ANALISI

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della sicurezza informatica ha mostrato un incremento preoccupante delle vulnerabilità critiche e degli attacchi ransomware, con un focus su software e infrastrutture ampiamente utilizzati. Le aziende italiane ed europee sono state colpite da attacchi mirati su settori chiave come la logistica, il retail e i servizi online. Si osserva un aumento della sofisticazione delle tecniche di attacco, con l'emergere di nuove varianti di malware Android dotate di AI e campagne di phishing sempre più elaborate.

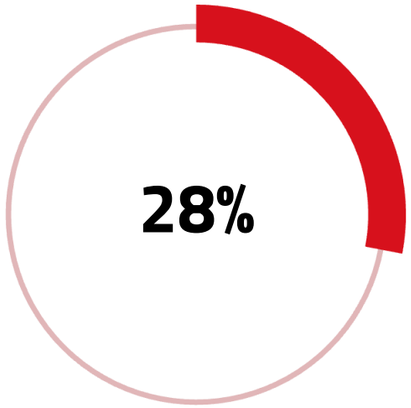


Campagne Malevole

Identificate dal CERT-AGID nella settimana, di cui 45 dirette a obiettivi italiani

IoC Condivisi

Indicatori di compromissione forniti dal CERT-AGID alle organizzazioni accreditate



Tasso Pagamento Ransom

Livello più basso mai registrato: le vittime di ransomware pagano sempre meno i riscatti

Tendenze Emergenti

- Malware Android con AI generativa (Oblivion, PromptSpy)
- Phishing mirato a utenti italiani (INPS, Enel)
- Ransomware come strumento geopolitico (Romania, operazioni ibride)
- Violazioni massive via fornitori terzi (ManoMano, 38M clienti)

Settori più Colpiti

- Logistica: Traffic Tech Italia (Qilin), operatori europei (Diesel Vortex)
- Telecomunicazioni: Odido (316K account, 1M record)
- Retail / E-commerce: ManoMano (38 milioni di clienti)
- Infrastrutture critiche: Romania, Emirati Arabi, settore energetico

RACCOMANDAZIONI

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino misure proattive. Il contesto in continua evoluzione delle minacce informatiche richiede particolare attenzione. Solo attraverso un approccio integrato e collaborativo sarà possibile affrontare efficacemente il panorama delle minacce informatiche in rapida evoluzione.

01

Patch Management Urgente

Implementare aggiornamenti immediati per Cisco SD-WAN, Trend Micro Apex One e SolarWinds Serv-U. Monitorare attivamente wpForo, openDCIM e dispositivi IoT per versioni vulnerabili.

02

Formazione Anti-Phishing

Sensibilizzare il personale sulle campagne attive a tema INPS ed Enel. Formare sulle tecniche OAuth 2.0 per bypass MFA, smishing e campagne di vishing come quella subita da Optimizely.

03

Monitoraggio Infrastrutture e Supply Chain

Valutare il rischio associato ai fornitori terzi (caso ManoMano). Implementare scansione continua di Active Directory e monitorare canali underground per IoC legati a Oblivion e DarkCloud.

04

Piano Risposta Ransomware

Rafforzare piani di risposta con focus su aziende italiane di logistica e servizi IT. Applicare patch urgenti per Cisco SD-WAN e Ivanti VPN per prevenire vettori di attacco attivi come quelli usati da Qilin e Tengu.

05

Collaborazione con CSIRT e CERT-AGID

Coordinare con CSIRT Italia e CERT-AGID per ricevere i 968 IoC settimanali e le segnalazioni di campagne attive contro obiettivi italiani come INPS, Enel e Verificatruffa.it.

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).

CONTATTI:
contattaci@s3kgroup.it
insidesales@s3kgroup.it
marketing@s3kgroup.it

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