S3K

Cyber Threat

WEEKLY REPORT

\ week 23/03/2026 - 29/03/2026

www.s3kgroup.it

Aumento delle minacce informatiche

Incremento significativo degli attacchi mirati ad infrastrutture critiche e vulnerabilità software, richiedendo vigilanza costante da parte delle organizzazioni italiane.

Compromissione della supply chain

Il gruppo TeamPCP ha lanciato una campagna di compromissione della supply chain, esfiltrando credenziali da strumenti di sviluppo come Aqua Trivy e Checkmarx KICS.

Vulnerabilità critiche in Node.js e Citrix

Rilasciate patch per vulnerabilità critiche in Node.js e Citrix NetScaler, sottolineando l'urgenza di aggiornamenti tempestivi per prevenire attacchi.

Violazioni di dati significative

Un leak ha esposto 84.000 credenziali italiane e 437.000 dati di utenti Euronics.it sono stati trovati sul dark web, aumentando il rischio di phishing.

Attacchi ransomware al settore energetico

Gli attacchi ransomware hanno colpito il settore energetico e aziende italiane come Esprinet, esponendo vulnerabilità nelle infrastrutture critiche.

Evoluzione campagne di phishing

127 campagne malevole identificate dal CERT-AGID, di cui 91 dirette contro obiettivi italiani, sfruttando temi attuali e piattaforme legittime.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della cybersecurity ha visto un incremento significativo delle minacce, con attacchi mirati a infrastrutture critiche e vulnerabilità di software ampiamente utilizzati. Diverse campagne di compromissione della supply chain e exploit di vulnerabilità zero-day hanno attirato l'attenzione, evidenziando la necessità di una vigilanza costante da parte delle organizzazioni.

- **Attacco alla Supply Chain CI/CD:** Il gruppo TeamPCP ha lanciato una massiccia campagna esfiltrando credenziali cloud e chiavi SSH da strumenti globali come Aqua Trivy e Checkmarx KICS. 🔗 CSIRT IT
- **Vulnerabilità critiche in Node.js:** Rilasciate patch per diverse vulnerabilità critiche in Node.js, evidenziando la necessità di aggiornamenti tempestivi per prevenire possibili attacchi. 🔗 Over Security
- **Flaw in TP-Link Router:** TP-Link ha avvisato gli utenti di una vulnerabilità critica nei router Archer NX che consente l'aggiramento dell'autenticazione. 🔗 Over Security
- **Exploits zero-day in Apache e Mcpjam:** Rilasciati exploit per vulnerabilità SSRF in Apache Cxf e mancanza di autenticazione in Mcpjam Inspector. 🔗 Latest CVE 0day exploit
- **Attacchi a istituzioni europee:** Due episodi recenti hanno coinvolto attacchi informatici alla Commissione Europea e al direttore dell'FBI, evidenziando la vulnerabilità delle istituzioni. 🔗 Over Security
- **Hacker ruba 24,5 milioni da Resolv DeFi:** Un attacco ha portato al furto di 24,5 milioni di dollari dalla piattaforma DeFi Resolv, evidenziando i rischi delle piattaforme decentralizzate. 🔗 Over Security
- **Sanzioni UK contro mercato crypto cinese:** Il governo britannico ha sanzionato Xinbi, un marketplace di criptovalute cinese, accusato di facilitare frodi online su larga scala. 🔗 Over Security
- **Vulnerabilità in Citrix NetScaler:** Citrix ha avvisato gli amministratori di patchare due vulnerabilità nei prodotti NetScaler, simili a quelle già sfruttate in attacchi zero-day. 🔗 Over Security

La settimana ha evidenziato una crescente complessità delle minacce informatiche, con attacchi che colpiscono sia il settore privato che quello pubblico. Le organizzazioni italiane ed europee devono rimanere vigili e proattive nell'implementare misure di sicurezza adeguate.

Citrix NetScaler: la prossima crisi "CitrixBleed"?

Una vulnerabilità critica colpisce Citrix NetScaler ADC e Gateway — consente accesso non autenticato alla memoria, con possibile furto di credenziali e sessioni attive.

Vettore di attacco

- Accesso non autenticato alla memoria
- Furto di credenziali e sessioni attive
- ~40.000 istanze esposte su Internet
- PoC atteso/pubblico

Impatto

- Accesso iniziale agli ambienti aziendali
- Movimento laterale e compromissione completa
- Alto rischio campagne ransomware

Contesto

- Simile a vulnerabilità già sfruttate in attacchi reali
- Paragonabile a "CitrixBleed" (CVE-2023-4966)
- Exploit imminente prima delle patch

> "Le vulnerabilità critiche diventano attacchi reali prima che vengano patchate"

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama delle violazioni e delle perdite di dati ha mostrato un'attività intensa, con numerosi incidenti che hanno coinvolto sia enti pubblici che privati. Le organizzazioni italiane ed europee devono rimanere vigili, poiché i dati compromessi possono avere impatti significativi sulla privacy e sulla sicurezza.

84K

Credenziali italiane esposte

MailPass leak ha rivelato 84.000 credenziali di accesso a servizi online italiani, aumentando il rischio di phishing e furto d'identità.

437K

Dati Euronics.it esposti

Scoperti 437.000 dati di utenti Euronics.it su forum del dark web, con potenziali conseguenze per la privacy dei clienti.

230K

Dati Kaplan esposti

L'azienda educativa Kaplan ha comunicato che oltre 230.000 dati personali, inclusi numeri di previdenza sociale, sono stati esposti.

In aggiunta, il **Ministero delle Finanze Olandese** è stato colpito da un attacco informatico, evidenziando la vulnerabilità dei sistemi governativi critici. Sono stati trovati in vendita account **Glovo** compromessi in Germania, Spagna e Italia. Le autorità russe hanno arrestato il presunto proprietario del forum **LeakBase**, un importante mercato online per dati rubati.

Minacce per Settori Critici: Dettaglio Breach

Istituzioni Governative

Il Ministero delle Finanze Olandese ha subito un attacco informatico. Le indagini sono in corso per valutare l'impatto e le misure di sicurezza necessarie.

Piattaforme di Consegna & E-commerce

Account Glovo compromessi in vendita in Germania, Spagna e Italia. Dati di 437.000 utenti di Euronics.it esposti su forum del dark web.

Settore Educativo

Kaplan ha comunicato l'esposizione di oltre 230.000 dati personali, inclusi numeri di previdenza sociale, a seguito di un attacco informatico.

Piattaforme Italiane & Dark Web

Un leak ha esposto 84.000 credenziali di accesso a servizi online italiani (MailPass). Strumenti di hacking per iPhone pubblicati su GitHub espongono milioni di utenti a potenziali attacchi spyware.

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un incremento significativo delle attività malevole, con attacchi mirati a sviluppatori, dissidenti e sistemi operativi specifici. Diverse campagne, tra cui attacchi alla supply chain e nuovi strumenti di furto di dati, hanno messo in evidenza la continua evoluzione delle tecniche dei cybercriminali.

Principali Incidenti e Minacce

1. **Malware nascosto in pacchetti PyPI:** Il gruppo TeamPCP ha compromesso il pacchetto Telnyx su PyPI, caricando versioni malevole che distribuiscono malware per il furto di credenziali, camuffato in file WAV. 🔗 Bleepingcomputer
2. **Attacchi iraniani tramite Telegram:** Hacker legati all'Iran hanno intensificato le operazioni utilizzando Telegram per attaccare dissidenti e giornalisti. 🔗 Techcrunch
3. **Falsi avvisi di sicurezza su GitHub:** Campagna su larga scala con falsi avvisi di sicurezza di Visual Studio Code, inducendo gli sviluppatori a scaricare malware. 🔗 Bleepingcomputer
4. **Attacco a Stryker:** La società di dispositivi medici Stryker ha confermato un attacco informatico con malware, causando l'interruzione delle operazioni e la perdita di oltre 200.000 dispositivi. 🔗 Therecord

Nuovi Malware Identificati

Infinity Stealer

Nuovo malware che prende di mira i sistemi macOS attraverso inganni legati a ClickFix, progettato per rubare dati sensibili da dispositivi Apple.

Torg Grabber

Nuovo malware in grado di rubare dati sensibili da oltre 700 estensioni di portafogli di criptovaluta, minaccia diretta per gli utenti crypto.

Botnet Kamasers

Botnet segnalata per la sua capacità di eseguire attacchi DDoS multi-vettore, compromettendo le operazioni aziendali a livello globale.

RedLine – Sviluppatori Estradati

Due sospetti sviluppatori del malware RedLine estradati negli USA per rispondere ad accuse di frode e riciclaggio di denaro.

Il gruppo TeamPCP ha compromesso la supply chain CI/CD esfiltrando credenziali cloud e chiavi SSH da strumenti di sviluppo globali. Questo rappresenta un'evoluzione preoccupante che mette a rischio l'intero ecosistema dello sviluppo software.

Phishing & Social Engineering

Negli ultimi sette giorni, il CERT-AGID ha identificato 127 campagne malevole, di cui 91 dirette contro obiettivi italiani. Le tecniche di attacco si sono evolute, sfruttando piattaforme legittime e temi di attualità per ingannare le vittime e rubare informazioni sensibili.

01

Phishing Agenzia delle Entrate

Due campagne di phishing hanno preso di mira l'Agenzia delle Entrate, sfruttando un'istanza WordPress legittima per ingannare le vittime e sottrarre credenziali.

02

Bubble AI abusata per credenziali Microsoft

Attori malevoli hanno sfruttato la piattaforma Bubble per generare applicazioni web dannose, eludendo i sistemi di rilevamento del phishing e prendendo di mira gli account Microsoft.

03

Silver Fox: phishing fiscale e spionaggio APT

Il gruppo Silver Fox ha cambiato strategia passando da crimini finanziari a campagne APT, utilizzando phishing a tema fiscale per colpire entità in Asia meridionale.

04

Attacco a Ita Airways

Ita Airways ha segnalato un accesso non autorizzato ai dati degli utenti del programma Volare. Il rischio di phishing è aumentato significativamente in seguito all'incidente.

05

Phishing TikTok for Business

Nuove campagne di phishing hanno preso di mira gli account TikTok for Business, impedendo l'analisi da parte di bot di sicurezza e aumentando il rischio per le aziende.

06

Campagna su app di messaggistica

CISA e FBI hanno lanciato avvisi riguardo a una campagna di phishing che colpisce gli utenti di app di messaggistica, evidenziando la crescente diversificazione delle tecniche di attacco.

07

Ritorno della piattaforma Tycoon2FA

Dopo un'interruzione da parte delle forze dell'ordine, la piattaforma di phishing-as-a-service Tycoon2FA è tornata operativa, riprendendo le sue attività precedenti.

Tecniche Avanzate Emergenti

- Abuso di piattaforme no-code (Bubble AI)
- Phishing APT a tema fiscale (Silver Fox)
- Phishing-as-a-Service (Tycoon2FA)
- Compromissione account email di profili strategici

Target Principali Italiani

- Utenti Agenzia delle Entrate
- Utenti programma Volare di Ita Airways
- Account Microsoft di organizzazioni italiane
- Aziende con presenza su TikTok for Business

Operazioni Ransomware Attive

Settore Energetico sotto attacco

187 incidenti confermati nel 2025 hanno evidenziato le debolezze delle infrastrutture critiche del settore energetico.

Attacco a Esprinet (ALP-001)

ALP-001 ha rivendicato un attacco a Esprinet, esfiltrando 1,2 TB di dati e aumentando i rischi per le aziende IT italiane.

Cyberattacco al Porto di Vigo

Un ransomware ha interrotto i sistemi di gestione del carico, costringendo le autorità a operare manualmente.

Condanna per operatore di botnet russo

Quasi sette anni di carcere per un operatore che ha facilitato attacchi ransomware tramite botnet.

Attacchi pro-Ucraina (Bearlyfy)

Bearlyfy ha intensificato la campagna contro aziende russe con strumenti di ransomware personalizzati.

Nuove vittime: Worldleaks

Worldleaks ha rivendicato attacchi a Sheraton Hotel, CIM e altre organizzazioni in più settori.

Ransomware e Settore Sanitario

Un'organizzazione sanitaria negli Stati Uniti ha subito un attacco, confermando la vulnerabilità del settore.

Vulnerabilità Aggiuntive e Patch

CVE-2026-33017 – Langflow

Sfruttamento attivo confermato da CISA. RCE nei flussi di lavoro AI. Aggiornare immediatamente il framework Langflow.

CVE-2026-3055 – Citrix NetScaler

CVSS 9.3. Lettura di memoria non valida in NetScaler ADC e Gateway. Applicare le patch Citrix senza indugio.

CVE-2026-25769 – Wazuh

PoC pubblico disponibile per RCE in Wazuh. Verificare l'applicazione degli aggiornamenti su tutti i sistemi di monitoraggio.

CVE-2026-21992 – Oracle

Patch d'emergenza Oracle per RCE critica. Applicazione immediata obbligatoria per tutti i prodotti Oracle interessati.

CVE-2026-33150/33179 – Libfuse

Escalation di privilegi ed esecuzione codice arbitrario. Aggiornare Libfuse su tutti i sistemi Linux esposti.

CVE-2026-25457 – WordPress Mixtape

CVSS 8.1. Local File Inclusion nel tema Mixtape. Aggiornare il tema WordPress per evitare exploit.

CVE-2026-33765 – Pi-hole

Command injection nella web interface di Pi-hole. Aggiornare il software per prevenire l'esecuzione di comandi arbitrari.

CVE-2026-32924/32973 – OpenClaw

CVSS 9.8. Bypass autorizzazione e command injection. Aggiornamento critico e urgente richiesto.

La settimana ha evidenziato un numero significativo di vulnerabilità critiche con PoC pubblici disponibili, sottolineando l'importanza di un approccio proattivo alla sicurezza informatica. Le organizzazioni devono aggiornare tempestivamente i propri software e monitorare costantemente le nuove segnalazioni.

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della sicurezza informatica ha mostrato un incremento significativo delle minacce, con attacchi mirati a infrastrutture critiche e un aumento delle violazioni di dati. Le campagne di compromissione della supply chain, l'emergere di vulnerabilità zero-day e l'intensificazione degli attacchi ransomware hanno evidenziato la crescente complessità delle minacce.

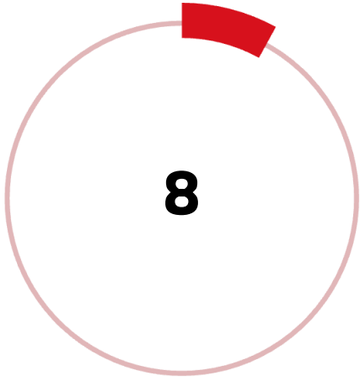
Rispetto alle settimane precedenti, si osserva un aumento della sofisticazione delle tecniche di attacco, con un focus particolare su settori strategici come quello energetico e sanitario. Le organizzazioni italiane ed europee devono affrontare un contesto di crescente vulnerabilità, dove i dati compromessi possono avere impatti diretti sulla privacy e sulla sicurezza.

Campagne Malevole

Identificate dal CERT-AGID nella settimana (22/03/2026 – 29/03/2026), di cui 91 dirette a obiettivi italiani

Attacchi Ransomware Energetici

Incidenti ransomware confermati nel settore energetico nel 2025, con crescita allarmante delle minacce alle infrastrutture critiche



Vulnerabilità Critiche CVE

Nuove vulnerabilità critiche con PoC pubblici rilasciati nella settimana, che colpiscono software enterprise ampiamente utilizzati

Tendenze Emergenti

- Compromissione supply chain CI/CD (TeamPCP, PyPI)
- Phishing mirato (Agenzia delle Entrate, Ita Airways)
- Ransomware su infrastrutture critiche (energia, logistica)
- Violazioni di dati su piattaforme italiane (Euronics, MailPass)

Settori più Colpiti

- Energia e Infrastrutture Critiche
- Sanità e Dispositivi Medici (Stryker)
- Distribuzione IT e E-commerce (Esprinet, Euronics)
- Pubblica Amministrazione (Agenzia delle Entrate)

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino un approccio proattivo alla sicurezza informatica. Il contesto in continua evoluzione delle minacce richiede particolare attenzione su più fronti.

Priorità immediate:

- Applicare immediatamente le patch critiche per CVE-2026-33017 (Langflow), CVE-2026-3055 (Citrix NetScaler), CVE-2026-21992 (Oracle) e CVE-2026-32924/32973 (OpenClaw).
- Aggiornare i sistemi Node.js e i router TP-Link Archer NX per mitigare le vulnerabilità di autenticazione recentemente divulgate.
- Applicare le patch disponibili per Wazuh, Libfuse, Pi-hole e il tema WordPress Mixtape per prevenire escalation di privilegi e RCE.

Misure di sicurezza strutturali:

- Investire in programmi di formazione per sensibilizzare i dipendenti sui rischi del phishing (127 campagne settimanali, 91 italiane) e delle tecniche di social engineering evolute.
- Implementare l'autenticazione a più fattori per proteggere le credenziali aziendali, in particolare per i sistemi Microsoft e le piattaforme cloud.
- Monitorare attivamente il dark web per rilevare esposizioni di dati aziendali italiani e credenziali in vendita (riferimento: leak MailPass 84K credenziali, Euronics 437K dati).
- Verificare l'integrità dei pacchetti PyPI e delle dipendenze software per prevenire attacchi supply-chain come quelli del gruppo TeamPCP su Telnyx.
- Proteggere i dispositivi endpoint e monitorare le pipeline CI/CD per attività anomale legate a campagne di compromissione della supply chain.

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

ISO 14001 BUREAU VERITAS Certification

ISO 27001 BUREAU VERITAS Certification

ISO 9001 BUREAU VERITAS Certification

ISO 45001 BUREAU VERITAS Certification