S3K

Cyber Threat

WEEKLY REPORT

\ week 06/04/2026 - 12/04/2026

www.s3kgroup.it

Aumento delle minacce informatiche

Incremento significativo delle attività malevole, con attacchi mirati a infrastrutture critiche e vulnerabilità scoperte in dispositivi comuni.

Vulnerabilità nei router SOHO

Attacchi russi sfruttano vulnerabilità nei router SOHO per dirottamenti DNS, rappresentando un rischio diretto per le reti italiane.

Database di dati sensibili in vendita

Un database contenente informazioni personali italiane è stato messo in vendita sul dark web, evidenziando gravi rischi per la privacy degli individui.

Attacchi ransomware nel settore sanitario

Gruppi come Medusa e Anubis hanno colpito strutture sanitarie, sottolineando la vulnerabilità del settore e la necessità di misure rafforzate.

Campagne di phishing mirate

Campagne di phishing rivolte a Pubbliche Amministrazioni e dirigenti, con tecniche avanzate di ingegneria sociale per compromettere credenziali sensibili.

Vulnerabilità critiche attivamente sfruttate

Vulnerabilità in Adobe Acrobat e Marimo attivamente sfruttate, con aggiornamenti urgenti necessari per proteggere i sistemi delle organizzazioni.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della cybersecurity ha visto un aumento significativo delle minacce e delle vulnerabilità, con attacchi mirati a infrastrutture critiche e dispositivi di rete. Le attività di attori malevoli, in particolare quelli legati a stati come l'Iran e la Russia, hanno messo in evidenza la vulnerabilità delle reti e dei sistemi, mentre nuove scoperte su exploit e attacchi zero-day hanno sollevato preoccupazioni tra le organizzazioni europee.

- **Vulnerabilità nei router SOHO:** Gli hacker russi stanno sfruttando i router SOHO per campagne di dirottamento DNS, evidenziando una debolezza critica nella sicurezza delle reti globali. Ripercussioni anche per organizzazioni italiane che utilizzano dispositivi simili.
- **Attacchi iraniani ad infrastrutture USA:** Hacker legati all'Iran hanno preso di mira quasi 4.000 dispositivi industriali statunitensi, inclusi PLC esposti su Internet. Le organizzazioni europee devono prestare attenzione a simili vulnerabilità.
- **Rischi crescenti nel Golfo Persico:** La crisi in Iran ha messo in evidenza i rischi crescenti per la cybersecurity delle infrastrutture critiche nella regione, un'area strategicamente sensibile per l'Europa.
- **Vulnerabilità nelle telecamere smart Dahua:** Identificate vulnerabilità critiche nel firmware delle telecamere Dahua Hero C1. Le aziende italiane dovrebbero considerare l'aggiornamento dei loro dispositivi.
- **Attacco a Signature Healthcare:** Un attacco informatico ha causato interruzioni nei sistemi ospedalieri di Signature Healthcare, con impatti diretti sulla cura dei pazienti.
- **Criminalità informatica legata alle criptovalute:** Bitcoin Depot ha subito un furto di 3,6 milioni di dollari, evidenziando i rischi associati alle transazioni di criptovalute.
- **Attività di disinformazione su TikTok:** TikTok ha rimosso reti di account falsi che diffondevano contenuti politici in Ungheria, segnalando la crescente preoccupazione per la disinformazione online.
- **Attacco zero-day su Adobe Reader:** Scoperto un attacco zero-day che colpisce gli utenti di Adobe Reader, con exploit già in circolazione. Le aziende devono aggiornare le loro misure di sicurezza.

La settimana è stata caratterizzata da un aumento delle minacce informatiche, con attacchi mirati ad infrastrutture critiche e vulnerabilità scoperte in dispositivi comuni. Le organizzazioni italiane ed europee devono rimanere vigili e proattive.

Router SOHO nel mirino: hacker russi dirottano il DNS delle reti globali

CTI Weekly – 12 aprile 2026

Gli hacker russi stanno sfruttando attivamente le vulnerabilità dei router SOHO per condurre campagne di dirottamento DNS su scala globale. Questo vettore di attacco rappresenta una minaccia concreta per le reti aziendali italiane che fanno uso di questi dispositivi, spesso caratterizzati da configurazioni predefinite deboli e aggiornamenti firmware trascurati.

Dirottamento DNS

I router SOHO compromessi vengono utilizzati per reindirizzare il traffico DNS verso server controllati dagli attaccanti, consentendo intercettazione di credenziali e dati sensibili.

Attacchi iraniani a ICS/PLC

Quasi 4.000 dispositivi industriali statunitensi, inclusi PLC esposti su Internet, sono stati presi di mira. Il rischio si estende alle infrastrutture europee con esposizione simile.

Telecamere Dahua vulnerabili

Vulnerabilità critiche nel firmware delle telecamere smart Dahua Hero C1 potrebbero essere sfruttate per attacchi mirati a reti aziendali e di sorveglianza.

Rischio per l'Italia

Le organizzazioni italiane che utilizzano router SOHO e dispositivi IoT non aggiornati sono esposte a rischi diretti di compromissione della rete e furto di dati.

Obiettivi e superfici di attacco

- Router SOHO con firmware non aggiornato
- Dispositivi industriali PLC esposti su Internet
- Telecamere di sorveglianza con vulnerabilità firmware
- Infrastrutture critiche con scarsa igiene informatica
- Reti aziendali con configurazioni predefinite deboli
- Sistemi di controllo industriale (ICS) accessibili da remoto

Aggiornare immediatamente il firmware dei router SOHO, cambiare le credenziali predefinite e verificare la configurazione DNS. Isolare i dispositivi IoT in segmenti di rete dedicati per ridurre la superficie di attacco.

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama dei leak e delle violazioni di dati ha mostrato un'attività preoccupante, con numerosi incidenti che hanno coinvolto dati sensibili di utenti e organizzazioni in Europa, inclusa l'Italia. Le informazioni trapelate includono dati personali, credenziali di accesso e documenti ufficiali.

2.5K+

Kit documenti italiani

Patenti, documenti d'identità e passaporti italiani in vendita sul dark web.

280K+

Record Kupi-Chasovnik

Dati clienti esposti dalla violazione del rivenditore online di orologi, inclusi utenti italiani e rumeni.

300K+

Individui colpiti Eurail

Eurail ha confermato la compromissione di dati personali inclusi numeri di passaporto e informazioni di viaggio.

91 GB

Leak Commissione Europea

Dati della Commissione Europea compromessi a causa di uso improprio di strumenti compromessi.

Ulteriori violazioni hanno coinvolto **My Lovely AI** (oltre 106.000 account esposti con prompt e immagini generate), la piattaforma **Glovo** (credenziali con dati di pagamento in vendita sul dark web) e un'infrastruttura **cloud europea** compromessa a causa di configurazioni errate. La settimana ha evidenziato l'importanza di rafforzare le misure di protezione dei dati a tutti i livelli.

Minacce per Settori Critici: Dettaglio Breach

Documenti d'identità italiani

Un database contenente patenti, documenti d'identità e passaporti italiani è stato messo in vendita su piattaforme del dark web, con oltre 2.500 kit disponibili. Grave rischio per la privacy degli individui coinvolti.

Settore E-commerce & Retail

Kupi-Chasovnik ha subito una violazione con oltre 280.000 record di clienti esposti, inclusi dati personali di utenti in vari paesi europei, tra cui Italia e Romania.

Settore Trasporti & Turismo

Eurail ha confermato che un attacco informatico avvenuto a dicembre ha compromesso informazioni personali di oltre 300.000 individui, inclusi numeri di passaporto e informazioni di viaggio.

Istituzioni Europee & Cloud

Un leak di 91 GB ha coinvolto dati della Commissione Europea. Un'infrastruttura cloud europea è stata compromessa per configurazioni errate e credenziali deboli. Exploit zero-day Windows rilasciato pubblicamente.

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 diverse piattaforme e tecnologie. Le campagne di malvertising continuano a proliferare, sfruttando la reputazione di marchi noti, mentre nuove varianti di malware, come RAT e infostealer, stanno emergendo.

Principali Incidenti e Minacce

- **Google Chrome DBSC:** Google ha introdotto la protezione Device Bound Session Credentials (DBSC) in Chrome 146 per Windows, per bloccare il malware infostealer dal raccogliere cookie di sessione.
- **Malvertising su Facebook:** Una campagna persistente sfrutta la reputazione di noti exchange di criptovalute per ingannare le vittime e diffondere malware, con rischio significativo per gli utenti europei.
- **Attacco a 100 negozi Magento:** Codice nascosto in un'immagine SVG ha colpito quasi 100 negozi online, rubando dati di carte di credito e evidenziando vulnerabilità nell'e-commerce.
- **Compromissione CPUID:** Il progetto CPUID è stato usato per distribuire versioni compromesse di CPU-Z e HWMonitor, strumenti di monitoraggio hardware molto diffusi.

Nuovi Malware Identificati

Mirax RAT Android

Nuovo RAT per Android che prende di mira i paesi di lingua spagnola tramite Meta Ads, trasformando i dispositivi infetti in nodi proxy residenziali.

Atomic Stealer macOS

Nuova campagna sfrutta Script Editor per distribuire l'Atomic Stealer su macOS, bypassando le misure di sicurezza di Apple.

ClipBanker

Trojan mascherato da software legittimo che sostituisce gli indirizzi dei portafogli di criptovaluta negli appunti, minacciando gli utenti crypto.

LummaStealer & CastleLoader

LummaStealer mostra un aumento dell'attività, dimostrando resilienza delle operazioni malware nonostante gli sforzi delle forze dell'ordine.

Le organizzazioni italiane ed europee devono adottare misure proattive contro le campagne di malvertising e aggiornare i sistemi di rilevamento per identificare le nuove varianti di infostealer e RAT in circolazione.

Phishing & Social Engineering

Negli ultimi sette giorni, il panorama del phishing e del social engineering ha mostrato un aumento significativo delle attività malevole, con un focus particolare su campagne mirate che colpiscono le Pubbliche Amministrazioni italiane e i dirigenti di alto livello. Le tecniche si sono evolute sfruttando strumenti automatizzati e intelligenza artificiale.

01

Phishing Agenzia delle Entrate

Il CERT-AGID ha segnalato una campagna di phishing rivolta alle Pubbliche Amministrazioni per rubare credenziali. La pagina fraudolenta simula il login all'area riservata usando loghi ufficiali.

02

Piattaforma VENOM su C-suite

Nuova piattaforma phishing-as-a-service "VENOM" prende di mira le credenziali dei dirigenti di alto livello, rappresentando una minaccia significativa per le aziende.

03

Campagna a tema Klarna

Il CSIRT Italia ha identificato una campagna di phishing che simula comunicazioni di Klarna, mirata a rubare le credenziali degli utenti tramite email ingannevoli.

04

Device Code Flow Microsoft

Microsoft ha avvisato di una campagna sofisticata che sfrutta il "device code flow" per compromettere account aziendali, supportata da automazione e AI.

05

Campagna token OAuth

Rilevata una campagna che mira a ottenere token OAuth tramite social engineering, inducendo le vittime a seguire procedure di verifica dell'account.

06

Phishing su piattaforme di collaborazione

Cisco Talos ha osservato un aumento del phishing che sfrutta le pipeline di notifica delle piattaforme di collaborazione per inviare email di spam e phishing.

07

Spear-phishing ONG e università

Scoperto un attacco di spear-phishing mirato a organizzazioni non governative e università per rubare credenziali e dati sensibili, con il malware LucidRook rilevato i

Tecniche Avanzate Emergenti

- Phishing-as-a-Service (piattaforma VENOM)
- Sfruttamento del device code flow OAuth
- Automazione e AI per attacchi mirati
- Abuso di pipeline di notifica di collaboration tools

Target Principali Italiani

- Pubbliche Amministrazioni (Agenzia delle Entrate)
- Dirigenti C-suite (VENOM)
- Utenti di servizi finanziari (Klarna)
- ONG, università e settore sanitario

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama dei ransomware ha visto un'intensificazione delle attività, con attacchi mirati a settori critici come la sanità e l'istruzione. Gruppi come Medusa e Anubis continuano a sfruttare vulnerabilità zero-day con tecniche di attacco sempre più rapide.

Attacco a ChipSoft

Un attacco ransomware ha colpito il fornitore di software sanitario olandese ChipSoft, causando interruzioni nei servizi digitali utilizzati da ospedali e pazienti nei Paesi Bassi. 🔗 Fonte

Medusa e exploit zero-day

Microsoft ha collegato il gruppo Medusa a exploit zero-day: questi attori passano dall'accesso iniziale all'esfiltrazione dei dati in meno di 24 ore, rappresentando un rischio elevato. 🔗 Fonte

Anubis colpisce Brockton Hospital

Il Brockton Hospital, parte della rete Signature Healthcare, è stato colpito da un attacco ransomware rivendicato da Anubis, che ha minacciato di pubblicare i dati rubati. 🔗 Fonte

Iran integra criminali russi

Un report ha rivelato che l'Iran sta integrando attori criminali russi nelle sue operazioni offensive, aumentando il rischio di attacchi mirati contro obiettivi occidentali ed europei. 🔗 Fonte

Identificati leader di REvil e GandCrab

Le autorità tedesche hanno identificato due nazionali russi come i leader delle bande di ransomware REvil e GandCrab, attive tra il 2019 e il 2021. 🔗 Fonte

Nuove vittime: Dencom e Mytheresa

I gruppi Krybit e ShinyHunters hanno rivendicato attacchi ransomware contro Dencom e Mytheresa, evidenziando la continua espansione delle operazioni globali. 🔗 Fonte

Vulnerabilità Critiche & Patch

Negli ultimi sette giorni, il panorama delle vulnerabilità ha visto un aumento significativo delle minacce, con diverse vulnerabilità critiche attivamente sfruttate. Cyble ha tracciato 1.960 vulnerabilità, incluse 10 relative a sistemi di controllo industriale (ICS). Le organizzazioni devono aggiornare tempestivamente i sistemi.

1	**RCE in Marimo (pre-auth)** Identificata una vulnerabilità RCE pre-autenticazione in Marimo, attualmente sfruttata per furto di credenziali. Implementare misure di sicurezza immediate. Link
2	**CVE-2026-34621 – Adobe Acrobat** Rilevato un exploit attivo che consente l'esecuzione di codice arbitrario aprendo documenti PDF malevoli. Aggiornare Adobe Acrobat e Reader immediatamente. Link
3	**CVE-2025-59528 – Flowise RCE** Vulnerabilità RCE attivamente sfruttata, che mette a rischio migliaia di sistemi. Applicare patch tempestive per proteggere gli ambienti. Link
4	**CVE-2026-34980/34990 – CUPS** Disponibili PoC per vulnerabilità che potrebbero consentire esecuzione di codice arbitrario ed elevazione dei privilegi. Aggiornare i sistemi interessati. Link
5	**Ninja Forms – WordPress RCE** Difetto critico nel plugin Ninja Forms consente l'upload di file arbitrari, portando potenzialmente a esecuzione remota di codice. Agire rapidamente. Link
6	**CVE-2026-33703 – Chamilo LMS IDOR** Vulnerabilità critica che consente a utenti autenticati di accedere a dati personali di altri utenti. Aggiornare alla versione corretta. Link
7	**CVE-2025-62718 – Axios PoC** Rilasciato un PoC per vulnerabilità nella libreria Axios, utilizzata per l'interoperabilità tra browser e Node.js. Aggiornare i sistemi per prevenire attacchi. Link
8	**Report settimanale Cyble** Tracciati 1.960 vulnerabilità totali, incluse 10 relative a sistemi di controllo industriale (ICS), evidenziando la necessità di attenzione per le infrastrutture critiche. Link

Vulnerabilità Aggiuntive e Patch

RCE Marimo – Pre-Auth

Esecuzione remota di codice senza autenticazione, attivamente sfruttata per furto di credenziali. Misure immediate necessarie.

CVE-2026-34621 – Adobe Acrobat

Esecuzione di codice arbitrario tramite PDF malevoli. Exploit attivo in circolazione. Aggiornare immediatamente Adobe Acrobat e Reader.

CVE-2025-59528 – Flowise

Vulnerabilità RCE attivamente sfruttata su migliaia di sistemi. Patch urgente richiesta per proteggere gli ambienti Flowise.

CUPS – PoC Disponibili

PoC pubblici per CVE-2026-34980 e CVE-2026-34990: RCE ed elevazione dei privilegi. Aggiornare i sistemi CUPS immediatamente.

Ninja Forms – WordPress

Upload di file arbitrari con potenziale RCE. I siti WordPress con questo plugin devono applicare la patch con urgenza.

CVE-2026-33703 – Chamilo LMS

IDOR critico che espone dati personali degli utenti. Aggiornare Chamilo LMS alla versione corretta.

CVE-2025-62718 – Axios

PoC disponibile per vulnerabilità nella libreria Axios. Aggiornare le dipendenze nei progetti Node.js e browser.

Report Cyble Settimanale

1.960 vulnerabilità tracciate, 10 su ICS. Monitoraggio continuo essenziale per infrastrutture critiche.

Il recente aumento delle vulnerabilità critiche e dei PoC pubblici richiede un'attenzione costante da parte delle organizzazioni italiane ed europee. È fondamentale mantenere i sistemi aggiornati e monitorare attivamente le segnalazioni di exploit per proteggere le infrastrutture e i dati sensibili.

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della cybersecurity ha evidenziato un incremento allarmante delle minacce, con attacchi mirati a infrastrutture critiche e vulnerabilità scoperte in dispositivi e software ampiamente utilizzati. Le attività attribuibili a gruppi legati a stati come l'Iran e la Russia hanno messo in luce la vulnerabilità delle reti, con un focus su attacchi ransomware e phishing che colpiscono settori sensibili come la sanità e le pubbliche amministrazioni.
Rispetto alle settimane precedenti, si osserva un'evoluzione nelle tecniche di attacco, con l'uso crescente di intelligenza artificiale e automazione, rendendo gli attacchi più sofisticati e difficili da rilevare. L'emergere di piattaforme phishing-as-a-service come VENOM e la capacità di gruppi come Medusa di passare dall'accesso iniziale all'esfiltrazione in meno di 24 ore rappresentano tendenze allarmanti per le organizzazioni europee.

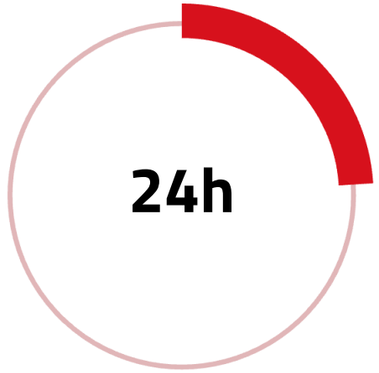
Tendenze chiave: sfruttamento di router SOHO e dispositivi IoT, attacchi ransomware ultra-rapidi al settore sanitario, campagne phishing su PA e C-suite, e numerosi leak di dati italiani ed europei sul dark web.

Vulnerabilità Tracciate

Identificate da Cyble nella settimana (05/04/2026 – 12/04/2026), incluse 10 relative a sistemi ICS

Dati Personali Esposti

Individui coinvolti nella violazione Eurail, con numeri di passaporto e dati di viaggio compromessi



Tempo di Attacco Medusa

Dalla compromissione iniziale all'esfiltrazione dei dati secondo l'analisi Microsoft sul gruppo ransomware

Tendenze Emergenti

- Sfruttamento di router SOHO per dirottamento DNS
- Ransomware ultra-rapidi (accesso → esfiltrazione in <24h)
- Phishing-as-a-Service su dirigenti (VENOM)
- Vendita massiva di documenti italiani sul dark web

Settori più Colpiti

- Sanità (ChipSoft, Brockton Hospital, Signature Healthcare)
- Pubblica Amministrazione e istituzioni europee
- E-commerce e piattaforme digitali
- Infrastrutture critiche (ICS/PLC, router SOHO)

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-2026-34621 (Adobe Acrobat), CVE-2025-59528 (Flowise), CVE-2026-34980/34990 (CUPS) e la vulnerabilità RCE pre-auth in Marimo.
- Aggiornare il firmware dei router SOHO, modificare le credenziali predefinite e verificare la configurazione DNS per prevenire dirottamenti.
- Applicare patch urgenti al plugin Ninja Forms per WordPress e alla libreria Axios in tutti i progetti Node.js.
- Aggiornare Adobe Acrobat e Reader su tutti i sistemi aziendali per mitigare il rischio di exploit via PDF malevoli.

Misure di sicurezza strutturali:

- Investire in programmi di formazione per sensibilizzare i dipendenti sui rischi del phishing, con focus su campagne a tema PA, VENOM e device code flow Microsoft.
- Implementare l'autenticazione a più fattori per proteggere le credenziali aziendali, in particolare per Microsoft 365, OAuth e piattaforme cloud.
- Monitorare attivamente il dark web per rilevare la vendita di documenti italiani, credenziali aziendali e dati sensibili.
- Isolare i dispositivi IoT (telecamere Dahua, router SOHO) in segmenti di rete dedicati per ridurre la superficie di attacco.
- Implementare soluzioni di rilevamento delle intrusioni per identificare comportamenti anomali legati a infostealer come LummaStealer e campagne di malvertising.

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