S3K

Cyber Threat

WEEKLY REPORT

\ week 20/04/2026 - 26/04/2026

www.s3kgroup.it

Aumento delle vulnerabilità critiche

Cisco ha rilasciato aggiornamenti urgenti per vulnerabilità che consentono attacchi di esecuzione di codice remoto, richiedendo un'immediata attenzione da parte delle organizzazioni italiane.

Attacchi alla supply chain

È stata identificata una versione malevola del pacchetto Bitwarden CLI, evidenziando il rischio crescente di compromissioni nella catena di approvvigionamento.

Campagne di phishing mirate

Sono state registrate 130 campagne di phishing, con un focus su utenti SPID e istituzioni italiane, sottolineando l'importanza della consapevolezza e della formazione degli utenti.

Incremento delle violazioni di dati

Un database contenente documenti italiani è stato messo in vendita sul dark web, sollevando preoccupazioni per la privacy e la sicurezza dei dati.

Attività ransomware in aumento

Gruppi come Qilin e Lockbit5 hanno rivendicato attacchi recenti, suggerendo un'evoluzione nelle tattiche di attacco verso approcci più mirati.

Sfruttamento attivo di vulnerabilità

Diverse vulnerabilità, tra cui quelle in Zimbra e protobufjs, sono attivamente sfruttate, evidenziando la necessità di aggiornamenti tempestivi per mitigare i rischi.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo delle vulnerabilità e degli attacchi, con un focus particolare su exploit critici e attacchi alla supply chain. Diverse aziende, tra cui Cisco e Microsoft, hanno dovuto affrontare gravi problemi di sicurezza, mentre attacchi attribuiti a gruppi di hacker, come quelli nordcoreani, continuano a rappresentare una minaccia per il settore delle criptovalute. Le organizzazioni italiane ed europee devono prestare particolare attenzione a queste dinamiche, poiché le implicazioni possono essere significative per la loro sicurezza e conformità.

- **Vulnerabilità critiche in Cisco:** Cisco ha rilasciato aggiornamenti di sicurezza per il suo Identity Services Engine e Webex Services, avvertendo che le vulnerabilità consentono attacchi di esecuzione di codice remoto. È fondamentale che le organizzazioni aggiornino i loro sistemi per mitigare i rischi. Leggi di più
- **Attacchi alla supply chain su Bitwarden:** È stata rilevata la distribuzione di una versione malevola del pacchetto Bitwarden CLI, con l'obiettivo di esfiltrare credenziali dai sistemi compromessi. Questo attacco si inserisce in una serie di compromissioni recenti delle supply chain. Leggi di più
- **Zero-day di Microsoft Defender:** Due exploit critici di Microsoft Defender sono ancora attivi e non patchati, rappresentando una minaccia significativa per le organizzazioni che utilizzano questo software. Leggi di più
- **Furto di criptovalute attribuito a hacker nordcoreani:** Un furto di circa 290 milioni di dollari in criptovalute è stato attribuito a hacker nordcoreani, evidenziando la vulnerabilità del settore e la necessità di misure di sicurezza più robuste. Leggi di più
- **Sanzioni a Poste Italiane per violazioni della privacy:** L'autorità italiana ha multato Poste Italiane e Postepay per aver trattato illegalmente i dati personali di milioni di utenti, sottolineando l'importanza della conformità alle normative sulla privacy. Leggi di più
- **Attacchi di impersonificazione su Microsoft Teams:** Microsoft ha avvertito che gli attori delle minacce stanno abusando di Microsoft Teams per attacchi di impersonificazione, utilizzando strumenti legittimi per accedere e muoversi lateralmente nelle reti aziendali. Leggi di più
- **Cyberattacco a un'agenzia governativa francese:** Un attacco informatico ha colpito un sito governativo francese, esponendo i dati personali degli utenti. Questo incidente mette in evidenza la vulnerabilità delle infrastrutture governative. Leggi di più

La settimana ha evidenziato la continua evoluzione delle minacce informatiche, con un aumento degli exploit critici e degli attacchi alla supply chain. Le organizzazioni italiane ed europee devono rimanere vigili e adottare misure proattive per proteggere i propri sistemi e dati.

Bitwarden CLI compromesso: attacco alla supply chain in evidenza

È stata rilevata la distribuzione di una versione malevola del pacchetto Bitwarden CLI tramite attacco alla supply chain, con l'obiettivo di esfiltrare credenziali dai sistemi compromessi. Questo vettore di attacco rappresenta una minaccia concreta per le organizzazioni italiane, con possibili ripercussioni su credenziali aziendali e accessi privilegiati.

Supply chain Bitwarden CLI

Una versione malevola del pacchetto Bitwarden CLI è stata distribuita per esfiltrare credenziali dai sistemi compromessi, inserendosi in un trend crescente di compromissioni delle supply chain software.

Vulnerabilità critiche Cisco

Cisco ha rilasciato aggiornamenti urgenti per Identity Services Engine e Webex Services: le vulnerabilità consentono l'esecuzione di codice remoto e richiedono patching immediato.

Zero-day Microsoft Defender non patchati

Due exploit critici di Microsoft Defender rimangono attivi e senza patch, rappresentando una minaccia persistente per le organizzazioni che dipendono da questa soluzione di sicurezza.

Rischio per l'Italia

Le organizzazioni italiane sono esposte a rischi diretti tramite supply chain compromesse, furto di credenziali e violazioni della privacy, come dimostrato dalla sanzione a Poste Italiane e Postepay.

Obiettivi e superfici di attacco

- Pacchetti open source e gestori di credenziali (Bitwarden CLI)
- Prodotti Cisco Identity Services Engine e Webex
- Sistemi Microsoft Defender non aggiornati
- Piattaforme di collaborazione aziendale (Microsoft Teams)
- Settore criptovalute (furto da 290 milioni di dollari)
- Infrastrutture governative europee

Verificare immediatamente la versione del pacchetto Bitwarden CLI in uso e aggiornare i prodotti Cisco. Applicare le patch disponibili per Microsoft Defender e monitorare attività sospette su Microsoft Teams. Controllare la conformità privacy alla luce delle sanzioni a Poste Italiane.

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama dei data leak e delle violazioni di dati ha mostrato un aumento significativo di incidenti, con numerosi elenchi di dati sensibili e database in vendita sul dark web. Diverse fonti hanno segnalato la disponibilità di combolist e database contenenti informazioni personali, con un focus particolare sull'Italia. Questi eventi sollevano preoccupazioni per la sicurezza delle informazioni e la protezione dei dati, specialmente per le organizzazioni italiane ed europee.

1M	4+	3	2026

Record combolist italiana	Paesi europei coinvolti	Tipologie di documenti italiani	Zs Stealer – Nuova minaccia
Combolist contenente un milione di record italiani, utile per attacchi di credential stuffing e altre attività malevole.	Combolist multi-nazione con dati da Italia, Spagna, Portogallo e altri paesi, evidenziando la crescente interconnessione delle minacce informatiche europee.	Database contenente DL, ID e passaporti italiani messo in vendita su un noto sito di cracking, compromettendo gravemente la privacy degli individui coinvolti.	Nuovo malware progettato per estrarre credenziali memorizzate, aumentando il rischio di attacchi mirati contro utenti e organizzazioni italiane.

Ulteriori violazioni hanno coinvolto **Seiko USA** (database clienti Shopify rubato con rischio di divulgazione in assenza di riscatto), **ADT** (violazione dei dati confermata dopo minaccia di leak da parte di un gruppo hacker) e **Tshirtmakers.it** (dati italiani esposti con potenziali implicazioni per la reputazione del marchio). 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 documenti italiani, inclusi patenti, carte d'identità e passaporti, è stato messo in vendita su un noto sito di cracking. Questo leak potrebbe compromettere gravemente la privacy degli individui coinvolti, aumentando il rischio di furto d'identità.

Credenziali & Account finanziari

Un'offerta su un forum del dark web includeva account bancari e crypto dell'UE, suggerendo che i criminali informatici stanno mirando a dati finanziari sensibili e aumentando il rischio di frodi per cittadini e aziende europee.

Retail & E-commerce

Il sito web di Seiko USA è stato compromesso, con gli attaccanti che affermano di aver rubato il database dei clienti di Shopify. In assenza del pagamento di un riscatto, i dati potrebbero essere divulgati, mettendo a rischio anche i clienti europei.

Servizi di sicurezza & PMI

ADT ha confermato una violazione dei dati dopo una minaccia di leak da parte di un gruppo di hacker. Il caso Tshirtmakers.it evidenzia ulteriormente il rischio per le piccole imprese italiane che gestiscono dati sensibili dei clienti online.

Malware & Infrastructure

Negli ultimi sette giorni, il panorama delle minacce informatiche ha mostrato un'attività intensa nel settore del malware e delle infrastrutture. Diverse campagne malevole hanno preso di mira sviluppatori, istituzioni governative e settori critici. Le nuove famiglie di malware e le tecniche sofisticate adottate evidenziano l'evoluzione continua delle minacce per le organizzazioni italiane ed europee.

Principali Incidenti e Minacce

1. **Supply chain npm malevola:** Identificati pacchetti npm che si propagano in modo simile a un worm, rubando le credenziali degli sviluppatori. Rischio significativo per le aziende che utilizzano librerie open source.
2. **Tropic Trooper e SumatraPDF:** Un gruppo di attacco ha utilizzato una versione trojanizzata di SumatraPDF per distribuire il malware AdaptixC2, consentendo l'accesso remoto tramite tunnel di Microsoft Visual Studio Code.
3. **GopherWhisper – APT cinese:** Nuovo gruppo APT scoperto mentre attaccava istituzioni governative mongole con malware basato su Go, evidenziando l'interesse per infrastrutture in regioni geopoliticamente sensibili.
4. **FakeWallet su Apple Store:** Scoperte 26 app malevole sull'Apple App Store che imitano portafogli di criptovalute per rubare frasi di recupero e chiavi private degli utenti.

Nuovi Malware Identificati

FIRESTARTER – Cisco Firepower

Backdoor che ha compromesso un dispositivo Cisco Firepower di un'agenzia federale statunitense, resistendo agli aggiornamenti di sicurezza. Sottolinea la vulnerabilità delle infrastrutture critiche.

Lotus Wiper – Venezuela

Malware di tipo wiper utilizzato in attacchi contro il settore energetico venezuelano, evidenziando l'uso di malware distruttivi in contesti geopolitici.

UNC6692 – Microsoft Teams

Nuovo cluster di attività malevole che impersona il supporto IT tramite Microsoft Teams per distribuire malware personalizzato tramite ingegneria sociale.

Malware pre-Stuxnet 'fast16'

Scoperto malware datato 2005 progettato per sabotare software di ingegneria, potenzialmente legato alle tensioni cyber tra Stati Uniti e Iran.

Le organizzazioni italiane ed europee devono adottare misure proattive contro malware specializzati e aggiornare i sistemi di rilevamento per identificare nuove varianti come FIRESTARTER, Lotus Wiper e le app FakeWallet in circolazione. Prestare particolare attenzione ai pacchetti npm e alle app di criptovalute non verificate.

Phishing & Social Engineering

Negli ultimi sette giorni, il panorama del phishing e del social engineering ha mostrato un'attività intensa, con 130 campagne registrate dal CERT-AGID, di cui 96 specificamente rivolte a obiettivi italiani. Le tecniche utilizzate dai criminali informatici si sono evolute, sfruttando nomi e loghi di enti pubblici per ingannare gli utenti e raccogliere informazioni sensibili.

01

Phishing utenti SPID

Rilevata una campagna di phishing che utilizza il nome e il logo di AgID per rubare le credenziali SPID. Gli utenti sono stati avvisati di non fornire dati personali tramite link sospetti e di accedere direttamente ai portali ufficiali.

02

Attacco all'Università Federico II

Un attacco di phishing ha preso di mira studenti e personale dell'Università di Napoli, con una pagina fraudolenta su Weebly che imitava il portale di accesso dell'ateneo. Il CERT-AGID ha informato l'università e richiesto la rimozione della pagina.

03

Furto dati – Ministero della Salute

Campagna di phishing che sfrutta il nome del Ministero della Salute per raccogliere dati personali e bancari, promettendo falsi rimborsi per prestazioni sanitarie. Gli utenti sono avvisati di non cliccare sui link nelle email ingannevoli.

04

Operazione TrustTrap

Analisi rivela una campagna di spoofing di domini governativi con oltre 16.800 domini malevoli attivi, mirati a ingannare gli utenti facendoli credere di interagire con servizi pubblici legittimi.

05

Phishing su app di criptovalute

Segnalate oltre venti app di phishing nell'Apple App Store, mascherate da portafogli di criptovalute popolari, con l'obiettivo di rubare informazioni sensibili degli utenti.

06

Social engineering su dipendenti NASA

Segnalati attacchi di phishing mirati a dipendenti della NASA, dove un attaccante si è spacciato per un ricercatore statunitense per ottenere informazioni sensibili, evidenziando l'evoluzione delle tecniche di social engineering.

07

Nuovi kit di phishing – Bluekit.cc

Identificati nuovi kit di phishing come Bluekit.cc, che offrono strumenti avanzati per attacchi su più piattaforme, aumentando significativamente il rischio per le organizzazioni.

Tecniche Avanzate Emergenti

- Spoofing di domini governativi (Operazione TrustTrap – 16.800 domini)
- Kit di phishing multi-piattaforma (Bluekit.cc)
- Spoofing SMS con mascheramento dell'identità del mittente
- Impersonificazione di enti pubblici (AgID, Ministero della Salute)

Target Principali Italiani

- Utenti SPID (credenziali AgID)
- Studenti e personale universitario (Federico II)
- Cittadini – falsi rimborsi sanitari (Ministero della Salute)
- Pubblica Amministrazione (130 campagne CERT-AGID)

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama degli attacchi ransomware ha mostrato un'attività intensa, con diversi gruppi di cybercriminali che hanno rivendicato attacchi contro organizzazioni in vari settori. Si nota un cambiamento nelle tattiche degli attaccanti, che sembrano preferire approcci più mirati rispetto a quelli di massa, con un'evoluzione verso tecniche di compromissione più sofisticate.

Gentlemen Ransomware – SystemBC Botnet

Indagine rivela che il ransomware Gentlemen ha integrato una botnet di proxy SystemBC, composta da oltre 1.570 host, presumibilmente vittime aziendali. Questo sviluppo suggerisce un'evoluzione nelle tecniche di attacco, aumentando il rischio per le organizzazioni europee.

Qilin colpisce Exclusive-Networks e Istarpal

Il gruppo ransomware Qilin ha rivendicato attacchi contro diverse aziende, tra cui Exclusive-Networks e Istarpal, evidenziando la continua e attiva operatività di questo gruppo nel panorama ransomware internazionale.

Lockbit5 pubblica nuove vittime

Lockbit5 ha pubblicato una lista di nuove vittime, tra cui studi professionali e aziende di logistica. Questi attacchi evidenziano la continua minaccia per le organizzazioni in vari settori, incluse le PMI italiane.

Vulnerabilità critiche Sky Co. – CVE-2026-39454 e CVE-2026-5967

Identificate vulnerabilità gravi nei prodotti SKYSEA Client View e SKYMEC IT Manager di Sky Co.,LTD., che potrebbero essere sfruttate per attacchi ransomware. Le aziende devono applicare le patch di sicurezza disponibili.

Aumento attacchi ransomware in Australia

Recenti rapporti indicano un raddoppio degli attacchi ransomware in Australia nel primo semestre del 2025, suggerendo una tendenza preoccupante che potrebbe riflettersi anche in Europa, dove le aziende devono prepararsi a un aumento simile.

Cambiamento nelle tattiche – Approccio mirato

Un'analisi ha mostrato un calo nel volume degli attacchi ransomware, suggerendo un passaggio verso un approccio più mirato e strategico da parte degli attaccanti, che ora si concentrano su vulnerabilità specifiche piuttosto che su attacchi indiscriminati. I backup da soli non garantiscono la continuità operativa: sono necessarie strategie BCDR robuste.

Vulnerabilità Critiche & Patch

Negli ultimi sette giorni, il panorama delle vulnerabilità ha visto un'intensa attività, con numerosi aggiornamenti critici e exploit attivi segnalati. Diverse piattaforme e software, tra cui Cisco, Oracle e librerie JavaScript, hanno rilasciato patch per vulnerabilità significative, alcune delle quali sono già oggetto di sfruttamento attivo. Le organizzazioni italiane ed europee sono esortate a mantenere i propri sistemi aggiornati.

1. **CVE-2026-20127 – Cisco Authentication Bypass**
   Cisco ha rilasciato aggiornamenti di sicurezza per questa vulnerabilità che consente l'Authentication Bypass. È già stata sfruttata attivamente in rete, rendendo urgente l'implementazione delle patch. CSIRT Italia
2. **Oracle Critical Patch Update – Aprile**
   Oracle ha pubblicato il Critical Patch Update di aprile, che affronta 29 vulnerabilità, di cui 6 classificate come critiche, includendo vulnerabilità di tipo Denial of Service e Remote Code Execution. CSIRT Italia
3. **CVE-2026-34415 – Xerte Online Toolkits RCE**
   Vulnerabilità di Remote Code Execution nella versione 3.15 e precedenti di Xerte Online Toolkits, a causa di una validazione incompleta degli input. Punteggio CVSS di 9.3, indicante un rischio critico. VulnCheck
4. **CVE-2025-48700 – Zimbra Collaboration Suite**
   Segnalato lo sfruttamento attivo di questa vulnerabilità in Zimbra, che consente la divulgazione di informazioni. Le organizzazioni sono esortate a mantenere aggiornati i loro sistemi per prevenire attacchi. CSIRT Italia
5. **CVE-2026-41242 – protobufjs PoC disponibile**
   Reso disponibile un Proof of Concept per la vulnerabilità nella libreria JavaScript protobufjs, che consente l'esecuzione remota di codice. Le organizzazioni devono aggiornare questa libreria per mitigare i rischi. CSIRT Italia
6. **CVE-2026-41328 – Dgraph accesso non autenticato**
   Questa vulnerabilità consente a un attaccante non autenticato di accedere a tutti i dati in un database Dgraph, se non sono attivate le ACL. Punteggio CVSS di 9.8, evidenziando la sua gravità critica. CVE Monitor
7. **CVE-2026-39920 – BridgeHead FileStore RCE**
   Consente l'esecuzione di comandi arbitrari da parte di attaccanti non autenticati a causa di credenziali predefinite esposte. Classificata come critica con punteggio CVSS di 9.3. CVE Monitor

Vulnerabilità Aggiuntive e Patch

Cisco – Authentication Bypass

CVE-2026-20127 già sfruttata attivamente in rete. Aggiornamento immediato necessario per i prodotti Cisco Identity Services Engine e Webex Services.

Oracle – 29 vulnerabilità patched

6 vulnerabilità critiche tra le 29 del Critical Patch Update di aprile. Aggiornare immediatamente tutti i prodotti Oracle per prevenire attacchi di tipo DoS e RCE.

Zimbra CVE-2025-48700

Sfruttamento attivo confermato in rete. Patch urgente richiesta per proteggere i sistemi Zimbra Collaboration Suite dalla divulgazione di informazioni sensibili.

protobufjs CVE-2026-41242

PoC disponibile pubblicamente per RCE. Aggiornare immediatamente la libreria protobufjs in tutti i progetti che la utilizzano per mitigare il rischio di exploit.

Xerte CVE-2026-34415 – CVSS 9.3

RCE critica su Xerte Online Toolkits 3.15 e precedenti. Aggiornare alla versione corretta per chiudere la vulnerabilità da validazione incompleta degli input.

Dgraph CVE-2026-41328 – CVSS 9.8

Accesso non autenticato all'intero database in assenza di ACL. Attivare immediatamente le ACL e aggiornare Dgraph per prevenire compromissioni dei dati.

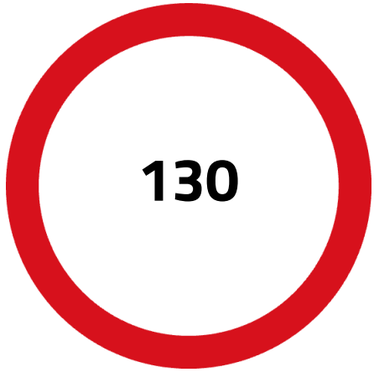
BridgeHead FileStore CVE-2026-39920

RCE senza autenticazione per credenziali predefinite esposte. Aggiornare urgentemente e modificare le credenziali predefinite per proteggere i sistemi.

Il rilascio di aggiornamenti critici da parte di Cisco e Oracle, unitamente alla presenza di PoC pubblici per protobufjs e Xerte, 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.

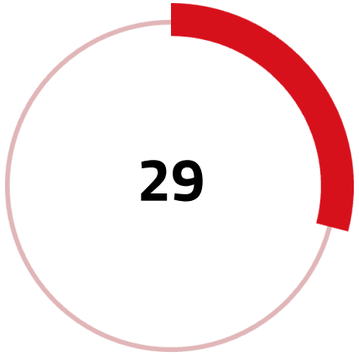
Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della sicurezza informatica ha mostrato un incremento preoccupante delle vulnerabilità e degli attacchi, con un focus particolare su exploit critici e attacchi alla supply chain. Le organizzazioni italiane ed europee devono affrontare una crescente varietà di minacce, tra cui attacchi di phishing mirati, ransomware e violazioni di dati, che evidenziano la necessità di una vigilanza costante e di misure di sicurezza adeguate.
Rispetto alle settimane precedenti, si nota un'evoluzione nelle tecniche di attacco, con un passaggio verso approcci più mirati e sofisticati, come dimostrano le recenti campagne di social engineering e l'uso di malware avanzati. Le vulnerabilità critiche, come quelle scoperte in prodotti Cisco e Oracle, sono già oggetto di sfruttamento attivo. L'impatto di queste minacce è significativo, poiché le violazioni possono compromettere la privacy degli utenti e la reputazione delle aziende, rendendo essenziale un approccio proattivo alla sicurezza informatica.
Tendenze chiave: attacchi alla supply chain npm e Bitwarden CLI, campagne di phishing su utenti SPID e istituzioni italiane, ransomware Qilin e Lockbit5 con approcci sempre più mirati, e sfruttamento attivo di vulnerabilità critiche in Zimbra e protobufjs.



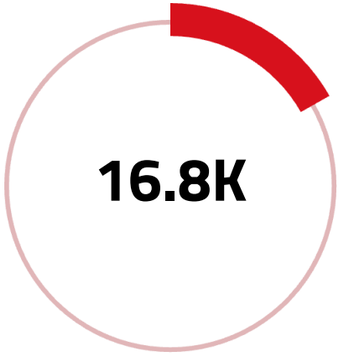
Campagne CERT-AGID

Campagne malevole registrate nella settimana, di cui 96 specificamente mirate ad obiettivi italiani (19/04/2026 – 26/04/2026)



Patch Oracle Aprile

Vulnerabilità affrontate nell'Oracle Critical Patch Update, di cui 6 classificate come critiche con potenziale di RCE e DoS



Domini TrustTrap

Domini malevoli attivi nell'Operazione TrustTrap, progettati per impersonare servizi governativi italiani ed europei

Tendenze Emergenti

- Attacchi alla supply chain su pacchetti npm e Bitwarden CLI
- Ransomware Qilin e Lockbit5 con approcci mirati
- Phishing su utenti SPID con impersonificazione AgID
- Sfruttamento attivo di Zimbra e protobufjs

Settori più Colpiti

- Pubblica Amministrazione e servizi governativi (TrustTrap, SPID)
- Sviluppatori e filiera software (npm, Bitwarden CLI)
- Settore energetico e infrastrutture critiche (Lotus Wiper)
- Utenti criptovalute e settore finanziario

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, con priorità agli aggiornamenti critici, alla protezione della supply chain e alla formazione del personale.

Priorità immediate:

- Applicare immediatamente le patch Cisco per le vulnerabilità nel Identity Services Engine e Webex Services (CVE-2026-20127), già sfruttate attivamente in rete.
- Aggiornare l'Oracle Critical Patch Update di aprile, con priorità per le 6 vulnerabilità classificate come critiche che includono RCE e DoS.
- Verificare e aggiornare la libreria protobufjs (CVE-2026-41242) e i sistemi Zimbra Collaboration Suite (CVE-2025-48700), entrambi oggetto di sfruttamento attivo.
- Aggiornare Xerte Online Toolkits (CVE-2026-34415, CVSS 9.3), Dgraph (CVE-2026-41328, CVSS 9.8) e BridgeHead FileStore (CVE-2026-39920, CVSS 9.3) con urgenza.

Misure di sicurezza strutturali:

- Investire in programmi di formazione per sensibilizzare i dipendenti sui rischi del phishing, con focus su campagne SPID, impersonificazione AgID e Ministero della Salute, e tecniche di spoofing SMS.
- Implementare controlli di sicurezza sulla supply chain software: verificare l'integrità dei pacchetti npm e delle dipendenze open source, con attenzione specifica al pacchetto Bitwarden CLI.
- Monitorare attivamente il dark web per rilevare la vendita di documenti italiani (DL, ID, passaporti) e combolist con credenziali italiane per prevenire attacchi di credential stuffing.
- Implementare strategie di Business Continuity e Disaster Recovery (BCDR) robuste, poiché i soli backup non garantiscono la continuità operativa durante attacchi ransomware come quelli di Qilin e Lockbit5.
- Attivare le ACL su tutti i database Dgraph esposti e modificare le credenziali predefinite nei sistemi BridgeHead FileStore per prevenire accessi non autenticati.

Focus Extra – Sicurezza delle Identità e delle Credenziali

Negli ultimi mesi si osserva un aumento significativo degli attacchi basati sul furto e abuso di credenziali, spesso come punto di ingresso iniziale per campagne ransomware, phishing e compromissioni della supply chain.

Principali rischi:

- Credential stuffing tramite combolist e leak recenti
- Furto credenziali tramite phishing mirato (SPID, PA, servizi sanitari)
- Compromissione di account aziendali e accessi privilegiati
- Abuso di strumenti legittimi (es. Microsoft Teams) per movimento laterale

Implicazioni per l'organizzazione:

- Accesso non autorizzato a sistemi critici
- Esfiltrazione di dati sensibili
- Escalation verso attacchi ransomware

Raccomandazioni:

- Abilitare MFA su tutti gli accessi critici
- Monitorare accessi anomali e tentativi di login sospetti
- Verificare eventuale esposizione di credenziali aziendali nel dark web
- Rafforzare la formazione utenti su phishing e social engineering

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