S3K

Cyber Threat

WEEKLY REPORT

\ week 27/04/2026 - 03/05/2026

www.s3kgroup.it

Sommario CTI Settimanale (26/04/2026 – 03/05/2026)

Aumento delle vulnerabilità critiche

Sono emerse diverse vulnerabilità zero-day, tra cui un bug in cPanel e vulnerabilità nel Kernel di Linux, richiedendo aggiornamenti urgenti da parte degli utilizzatori.

Attacco alla supply chain di SAP

È stata rilevata la distribuzione di pacchetti malevoli di SAP, evidenziando l'importanza della sicurezza nelle supply chain per le aziende che utilizzano queste tecnologie.

Nuovo spyware Morpheus

Un nuovo spyware legato a un'azienda di sorveglianza italiana è stato scoperto, aumentando le preoccupazioni per la sicurezza dei dispositivi mobili.

Campagne di phishing mirate

Il CERT-AGID ha segnalato attacchi di phishing specifici contro il Consiglio Nazionale del Notariato e l'Università di Palermo, con un uso crescente di tecniche automatizzate supportate da intelligenza artificiale.

Ransomware in aumento

Gruppi di ransomware come Lockbit5 e M3rx hanno rivendicato attacchi a diverse aziende italiane, con nuove varianti come VECT 2.0 che mostrano capacità distruttive significative.

Offerte di dati rubati

Sono emerse pratiche illecite sui forum di hacking, con la vendita di dati sensibili e account social media, sottolineando la necessità di vigilanza continua per proteggere le informazioni sensibili.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo delle vulnerabilità e degli exploit, con particolare attenzione a diverse piattaforme e applicazioni. Sono emerse notizie di exploit zero-day critici, attacchi alla supply chain e nuove forme di malware, evidenziando la necessità di una vigilanza costante da parte delle organizzazioni italiane ed europee.

- **Attacco alla Supply Chain di SAP:** È stata rilevata la distribuzione di una versione malevola dei pacchetti SAP tramite canali ufficiali, con l'obiettivo di esfiltrare credenziali dai sistemi compromessi. Leggi di più
- **Vulnerabilità critica in cPanel:** Un bug di bypass dell'autenticazione in cPanel è stato sfruttato come zero-day, con una patch di emergenza rilasciata per mitigare il rischio. Le organizzazioni che utilizzano cPanel devono aggiornare immediatamente. Leggi di più
- **Nuovo spyware Android Morpheus:** È stato scoperto un nuovo spyware legato a un'azienda di sorveglianza italiana, evidenziando il crescente uso di malware per la sorveglianza dei dispositivi mobili. Leggi di più
- **Extradizione di hacker cinesi negli USA:** Un cittadino cinese è stato estradato dagli Stati Uniti dopo essere stato arrestato in Italia per presunti attacchi informatici contro organizzazioni americane, mettendo in luce la cooperazione internazionale. Leggi di più
- **Flaw in Windows confermato da Microsoft:** Microsoft ha confermato che una vulnerabilità zero-click in Windows, legata a una patch incompleta, è attivamente sfruttata, mettendo a rischio le credenziali degli utenti non aggiornati. Leggi di più
- **Nuovi exploit zero-day:** Sono stati segnalati diversi exploit zero-day, tra cui vulnerabilità in Linux e librerie di terze parti, che potrebbero avere un impatto significativo su molte applicazioni aziendali. Leggi di più
- **Attacco a LiteLLM:** È stata identificata una vulnerabilità critica in LiteLLM che consente attacchi SQLi pre-autenticazione, aumentando il rischio di compromissione per le applicazioni che utilizzano questo framework. Leggi di più
- **Rilascio di Wireshark 4.6.5:** È stata rilasciata una nuova versione di Wireshark, strumento fondamentale per l'analisi del traffico di rete, con aggiornamenti di sicurezza e nuove funzionalità. Leggi di più

La settimana ha evidenziato la continua evoluzione delle minacce informatiche, con un focus particolare su vulnerabilità critiche e attacchi alla supply chain. È fondamentale che le organizzazioni italiane ed europee rimangano vigili e adottino misure proattive per proteggere i propri sistemi e dati.

Attacco alla Supply Chain di SAP

È stata rilevata la distribuzione di una versione malevola dei pacchetti SAP tramite canali ufficiali, con l'obiettivo di esfiltrare credenziali dai sistemi compromessi. Questo attacco sottolinea l'importanza della sicurezza nelle supply chain e rappresenta una minaccia concreta per tutte le organizzazioni italiane che utilizzano tecnologie SAP.

Supply Chain SAP compromessa

Una versione malevola dei pacchetti SAP è stata distribuita tramite canali ufficiali, con l'obiettivo primario di esfiltrare credenziali dai sistemi compromessi delle aziende target.

Vulnerabilità critica in cPanel

Un bug di bypass dell'autenticazione in cPanel è stato sfruttato come zero-day. È stata rilasciata una patch di emergenza: le organizzazioni devono aggiornare immediatamente per evitare compromissioni.

Spyware Morpheus su Android

Un nuovo spyware Android legato a un'azienda di sorveglianza italiana è stato scoperto, evidenziando il crescente uso di malware per la sorveglianza e i rischi per i dispositivi mobili aziendali.

Rischio per l'Italia

Le organizzazioni italiane che utilizzano SAP, cPanel e dispositivi Android sono esposte a rischi diretti. La cooperazione internazionale sull'estradizione di hacker cinesi segnala un panorama di minacce sempre più globale.

Obiettivi e superfici di attacco

- Sistemi aziendali SAP (supply chain compromessa tramite canali ufficiali)
- Server di hosting con cPanel (bypass autenticazione zero-day)
- Dispositivi Android aziendali (spyware Morpheus)
- Applicazioni che utilizzano il framework LiteLLM (SQLi pre-autenticazione)
- Sistemi Windows non aggiornati (vulnerabilità zero-click attivamente sfruttata)
- Infrastrutture Linux con librerie di terze parti vulnerabili

Verificare immediatamente l'integrità dei pacchetti SAP in uso e applicare la patch di emergenza per cPanel. Aggiornare i sistemi Windows per mitigare la vulnerabilità zero-click confermata da Microsoft. Monitorare i dispositivi mobili aziendali per rilevare tracce dello spyware Morpheus.

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama delle violazioni e delle perdite di dati ha registrato un aumento significativo di incidenti, con diverse organizzazioni e piattaforme coinvolte. Le notizie più rilevanti riguardano la fuga di dati sensibili da database di aziende, oltre a offerte di servizi illeciti che sfruttano informazioni rubate. Questo scenario evidenzia l'importanza di una vigilanza costante e di misure di sicurezza adeguate per le organizzazioni italiane ed europee.

100K	AXA	SSN	SMS
Utenti CRM esposti	**Colpatria Database violato**	**Dati personali USA in vendita**	**Verifica SMS low-cost sospetta**
Un post ha rivelato la disponibilità di dati di 100.000 utenti statunitensi da un CRM, evidenziando la vulnerabilità delle piattaforme di marketing.	È stata segnalata una violazione dei dati che ha coinvolto il database di AXA Colpatria, con informazioni potenzialmente sensibili esposte ai clienti.	Diversi post su forum di hacking offrono servizi di verifica e lead di utenti statunitensi, inclusi dati personali come SSN, nomi e numeri di telefono.	Offerte di servizi di verifica SMS a prezzi stracciati sono emerse, suggerendo un possibile uso di dati rubati per bypassare i controlli di sicurezza.

Ulteriori attività illecite hanno incluso la **vendita di account Twitter e Reddit** con profili reali e attivi, offerte di **servizi SEO e backlink** potenzialmente basati su dati rubati, nonché **tentativi di phishing** che sfruttano dati sottratti per ingannare gli utenti. La settimana ha evidenziato l'importanza di rafforzare le misure di protezione dei dati a tutti i livelli.

Minacce per Settori Critici: Dettaglio Breach

Finanziario & Assicurativo

AXA Colpatria ha subito una violazione del proprio database, con informazioni potenzialmente sensibili esposte. Le implicazioni per i clienti potrebbero essere gravi, richiedendo un monitoraggio attento delle attività sospette e una comunicazione trasparente agli utenti coinvolti.

Marketing & CRM

Un post ha rivelato la disponibilità di dati di 100.000 utenti statunitensi estratti da un CRM, evidenziando la vulnerabilità delle piattaforme di marketing e la necessità di proteggere i dati dei clienti con misure di controllo accessi più rigorose.

Social Media & Identità digitale

Sono stati segnalati annunci per la vendita di account Twitter e Reddit con profili reali e attivi. Questa attività non solo infrange le politiche delle piattaforme, ma può esporre ulteriormente i dati degli utenti e facilitare campagne di disinformazione.

Servizi online & Phishing

Sono stati identificati nuovi metodi per sfruttare vulnerabilità nei servizi online, con offerte di exploit e malware su forum di hacking. I tentativi di phishing che sfruttano dati rubati richiedono una formazione continua dei dipendenti per il riconoscimento delle minacce.

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un incremento significativo di attività malevole, con attacchi mirati a diverse piattaforme e tecnologie. Le campagne di malware si sono evolute, sfruttando vulnerabilità in pacchetti software e servizi cloud, mentre i gruppi di hacker continuano a perfezionare le loro tecniche di ingegneria sociale. Le organizzazioni italiane ed europee devono rimanere vigili di fronte a queste minacce in continua evoluzione.

Principali Incidenti e Minacce

1. **Falsi allarmi di Microsoft Defender:** Microsoft Defender ha erroneamente identificato i certificati DigiCert come Trojan, creando confusione e potenziali problemi di fiducia per le aziende che utilizzano questi certificati per la sicurezza delle loro comunicazioni.
2. **Abuso delle Mini App di Telegram:** Sono emerse segnalazioni di abusi delle Mini App di Telegram per la distribuzione di malware su Android e per truffe legate alle criptovalute, evidenziando la necessità di maggiore vigilanza sulle piattaforme di messaggistica.
3. **Nuovo malware DDoS su Jenkins:** Un nuovo malware DDoS è stato scoperto, sfruttando Jenkins per attaccare i server di gioco Valve Source Engine, con possibili ripercussioni per le aziende che utilizzano queste tecnologie.
4. **Attacchi della Corea del Nord:** I gruppi di hacker nordcoreani stanno utilizzando interviste false per ingannare sviluppatori freelance, distribuendo malware e rubando criptovalute con un approccio innovativo di ingegneria sociale.

Nuovi Malware Identificati

Supply chain SAP – npm

Una campagna di attacco alla supply chain ha compromesso pacchetti npm legati a SAP, utilizzando malware per il furto di credenziali. Le aziende che utilizzano SAP devono prestare attenzione a queste vulnerabilità.

PyTorch Lightning – Infostealer

È stato identificato un attacco di supply chain in PyTorch Lightning, dove il malware si attiva all'importazione rubando credenziali cloud, evidenziando i rischi associati all'uso di librerie di terze parti.

GlassWorm – OpenVSX

Il malware GlassWorm è riemerso, attaccando tramite 73 estensioni "sleeper" di OpenVSX. Le organizzazioni devono essere pronte a identificare e mitigare queste minacce nei loro ambienti di sviluppo.

Botnet DDoS brasiliana

Una società brasiliana specializzata in protezione DDoS è stata accusata di aver abilitato un botnet per attaccare altri operatori di rete, evidenziando la complessità delle minacce interne.

Le organizzazioni italiane ed europee devono adottare misure proattive contro malware di supply chain e aggiornare i sistemi di rilevamento per identificare nuove varianti. Prestare particolare attenzione ai pacchetti npm SAP, alle librerie PyTorch Lightning e alle estensioni OpenVSX non verificate.

Phishing & Social Engineering

Negli ultimi sette giorni, il panorama del phishing e del social engineering ha mostrato un'attività intensa, con un aumento significativo delle campagne malevole mirate ad enti e organizzazioni italiane. Il CERT-AGID ha registrato 138 campagne malevole, di cui 97 specificamente mirate ad obiettivi italiani. Le tecniche si sono evolute, con un preoccupante trend di attacchi automatizzati supportati da intelligenza artificiale.

01

Phishing – Consiglio del Notariato

Il CERT-AGID ha identificato una pagina di phishing che simula il portale di accesso al servizio di posta del Consiglio Nazionale del Notariato, mirata alla raccolta di credenziali. Il sito è parte di una rete più ampia di attacchi.

02

Phishing – Università di Palermo

È stata scoperta una pagina di phishing che si finge il portale di accesso dell'Università di Palermo, utilizzando un template già visto in attacchi precedenti per sottrarre credenziali tramite un modulo di login fraudolento.

03

Phishing automatizzato con AI

Ricerche recenti hanno mostrato che l'86% degli attacchi di phishing è ora guidato da intelligenza artificiale, con attori malevoli che utilizzano agenti autonomi per mappare reti e ottenere credenziali in tempi record.

04

Bluekit – Nuovo kit di phishing AI

È emerso un nuovo kit di phishing chiamato Bluekit, che include un assistente AI e 40 modelli, rendendo più facile per i criminali informatici lanciare attacchi personalizzati e convincenti su larga scala.

05

Robinhood – Phishing via registrazione

Un difetto nel processo di registrazione di Robinhood è stato abusato per inviare email di phishing convincenti agli utenti della piattaforma, aumentando significativamente il rischio di compromissione degli account.

06

Campagna contro funzionari tedeschi

È stata identificata una campagna di phishing che prende di mira funzionari governativi in Germania, sospettata di essere orchestrata da attori russi, evidenziando l'uso di tecniche di social engineering sofisticate.

07

Campagne CERT-AGID – 138 totali

Il CERT-AGID ha registrato 138 campagne malevole nella settimana, di cui 97 mirate ad obiettivi italiani, tra cui email malevole che abusano del nome di SPID, evidenziando la pressione costante sul tessuto digitale del Paese.

Tecniche Avanzate Emergenti

- Phishing guidato da AI (86% degli attacchi)
- Kit Bluekit con assistente AI e 40 modelli preconfigurati
- Abuso di falle di registrazione per email phishing convincenti
- Campagne statali con social engineering sofisticato

Target Principali Italiani

- Consiglio Nazionale del Notariato (portale email clonato)
- Università degli Studi di Palermo (portale di accesso clonato)
- Utenti SPID (97 campagne CERT-AGID su 138 mirate a italiani)
- Pubblica Amministrazione e istituzioni italiane

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama degli attacchi ransomware ha visto un'intensificazione degli attacchi, con diverse organizzazioni europee e italiane nel mirino di gruppi di cybercriminali. Le nuove varianti di ransomware, come VECT 2.0 e M3rx, hanno mostrato capacità distruttive significative, mentre diversi gruppi hanno rivendicato attacchi ad importanti aziende. Questo scenario mette in evidenza la necessità di un monitoraggio costante e di misure di sicurezza rafforzate.

Payoutsking – Sofinter S.p.a.

Il gruppo ransomware payoutsking ha rivendicato un attacco contro Sofinter S.p.a. (sofinter.it). Hash identificativo: bfdbb37aad5b9027fdb40b7a522abd566e539d65dc18be380f546b52b5cce3c5.

M3rx – Rotak S.r.l.

Il gruppo m3rx ha attaccato rotak.it. Hash identificativo: b412664f6b126388d45055f434451c655b2f8082de938f19fbc4fd2aa32483fe. M3rx ha inoltre rivendicato attacchi a emtco.com, it-freitag.de e manateeair.com.

Lockbit5 colpisce Defcon5 Italy

Lockbit5 ha pubblicato defcon5italy.com come nuova vittima, evidenziando l'attività continua di questo noto gruppo di ransomware nel panorama italiano ed europeo.

VECT 2.0 – Ransomware distruttivo

La variante VECT 2.0 è stata segnalata come capace di distruggere file anziché semplicemente criptarli, rendendo impossibile il recupero anche per gli stessi attaccanti. Questo rappresenta un cambiamento significativo nel modus operandi dei ransomware.

Worldleaks – Studi legali

Worldleaks ha colpito diversi studi legali, tra cui Peyton Law Firm e Ceywater Consultants, con hash specifici forniti per ciascun attacco, confermando la crescente pressione sul settore legale.

Everest – Fiserv

Il gruppo Everest ha rivendicato un attacco a Fiserv. Hash identificativo: a9024fc0b33710ad12a091197972a6a1c4767388960c57872a4cd509d2b9f74f. Blackwater ha colpito Shenzhen Gongjin Electronics.

Vulnerabilità Critiche & Patch

Negli ultimi sette giorni, il panorama delle vulnerabilità ha visto un aumento significativo delle segnalazioni, con diverse vulnerabilità critiche che hanno attirato l'attenzione della comunità di sicurezza informatica. Sono stati resi disponibili Proof of Concept (PoC) per diverse vulnerabilità riguardanti software ampiamente utilizzati come ProFTPD, cPanel e Linux. Le organizzazioni italiane ed europee sono invitate a implementare tempestivamente le patch disponibili.

1	**CVE-2026-42167 – ProFTPD** È stato rilasciato un PoC per questa vulnerabilità critica che consente l'esecuzione di codice remoto e l'aggiramento dell'autenticazione. Gli attaccanti possono sfruttare questa vulnerabilità per compromettere i server FTP. Dettagli qui
2	**CVE-2026-41940 – cPanel & WHM** Un PoC è stato reso disponibile per questa vulnerabilità che consente a un attaccante non autenticato di ottenere accesso amministrativo ai servizi di hosting. È fondamentale applicare le patch fornite dal vendor. Dettagli qui
3	**CVE-2026-31431 – Kernel Linux** È stato pubblicato un PoC per questa vulnerabilità che consente l'elevazione dei privilegi nel Kernel di Linux. Gli amministratori di sistema sono esortati a mantenere aggiornati i loro sistemi per mitigare i rischi. Dettagli qui
4	**CVE-2026-3854 – GitHub** È stata identificata una vulnerabilità critica che consente l'esecuzione di comandi non autorizzati. Gli utenti di GitHub e GitHub Enterprise Server devono aggiornare immediatamente il software per evitare potenziali exploit. Dettagli qui
5	**CVE-2026-41176 & CVE-2026-41179 – Rclone** Sono stati resi disponibili PoC per due vulnerabilità che consentono l'aggiramento dell'autenticazione e l'esecuzione di codice remoto in Rclone. Le patch sono già disponibili. Dettagli qui
6	**CVE-2026-3008 – Notepad++** Un PoC è stato pubblicato per una vulnerabilità che potrebbe compromettere la disponibilità del servizio e rivelare informazioni sensibili. È consigliato aggiornare Notepad++ tempestivamente. Dettagli qui
7	**CVE-2026-4882 – WordPress** Questa vulnerabilità consente l'upload arbitrario di file, potenzialmente portando a un'esecuzione di codice remoto. Gli amministratori di siti WordPress devono prestare attenzione e applicare le patch disponibili. Dettagli qui

Vulnerabilità Aggiuntive e Patch

ProFTPD – CVE-2026-42167
PoC disponibile per RCE e bypass autenticazione su server FTP. Aggiornamento immediato necessario per tutti i sistemi che espongono servizi ProFTPD sulla rete.

cPanel & WHM – CVE-2026-41940
Accesso amministrativo non autenticato ai servizi di hosting. Patch urgente richiesta per proteggere i server esposti da compromissioni totali dell'infrastruttura di hosting.

Linux Kernel – CVE-2026-31431
Elevazione dei privilegi con PoC pubblico. Aggiornare immediatamente il kernel Linux in tutti i sistemi per mitigare il rischio di escalation di privilegi da parte di attaccanti locali.

GitHub – CVE-2026-3854
RCE critica su GitHub e GitHub Enterprise Server. Aggiornare immediatamente tutte le istanze per prevenire l'esecuzione di comandi non autorizzati sulle piattaforme di sviluppo.

Rclone – CVE-2026-41176/41179
PoC pubblici per bypass autenticazione e RCE su Rclone. Aggiornare immediatamente per chiudere le vulnerabilità prima che vengano sfruttate attivamente negli ambienti di produzione.

Notepad++ – CVE-2026-3008
PoC reso pubblico per DoS e divulgazione di informazioni sensibili. Aggiornare Notepad++ tempestivamente per prevenire interruzioni del servizio e accessi non autorizzati.

WordPress – CVE-2026-4882
Upload arbitrario di file con possibile RCE su WordPress. Aggiornare urgentemente tutte le installazioni vulnerabili per proteggere i siti web da compromissioni e defacement.

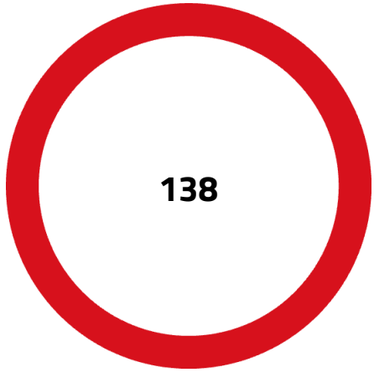
La presenza di PoC pubblici per ProFTPD, cPanel, Linux Kernel, GitHub e Rclone, unitamente alle vulnerabilità in Notepad++ e WordPress, richiede un'attenzione costante da parte delle organizzazioni italiane ed europee. È fondamentale mantenere i sistemi aggiornati e monitorare attivamente le segnalazioni 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 di vulnerabilità, attacchi e incidenti di data breach, con un focus particolare su exploit zero-day e attacchi alla supply chain. Le organizzazioni italiane ed europee devono affrontare una crescente varietà di minacce, che spaziano da malware sofisticati a campagne di phishing mirate con intelligenza artificiale.

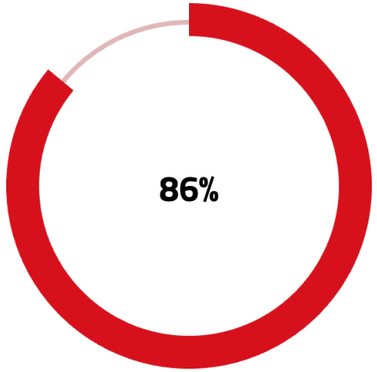
Rispetto alle settimane precedenti, si nota un aumento della complessità e della coordinazione degli attacchi, con l'uso di intelligenza artificiale per automatizzare le campagne di phishing (86% degli attacchi) e un numero crescente di attacchi ransomware che mirano a settori critici. Nuove varianti come VECT 2.0, capace di distruggere i file anziché criptarli, segnano un'evoluzione preoccupante nel modus operandi dei gruppi criminali. Questo scenario richiede una vigilanza costante e l'adozione di misure di sicurezza proattive.

Tendenze chiave: attacco alla supply chain SAP tramite canali ufficiali, spyware Morpheus legato a sorveglianza italiana, 138 campagne malevole CERT-AGID di cui 97 su obiettivi italiani, e PoC pubblici per vulnerabilità critiche in ProFTPD, cPanel e Linux Kernel.



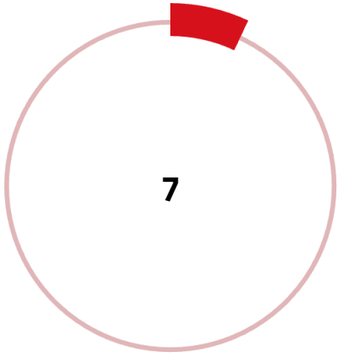
Campagne CERT-AGID

Campagne malevole registrate nella settimana, di cui 97 specificamente mirate ad obiettivi italiani, evidenziando la pressione costante sul tessuto digitale nazionale (26/04/2026 – 03/05/2026)



Phishing guidato da AI

Percentuale degli attacchi di phishing ora guidati da intelligenza artificiale, con agenti autonomi capaci di mappare reti e sottrarre credenziali in tempi record



CVE critiche con PoC

Vulnerabilità critiche con Proof of Concept pubblicamente disponibile nella settimana, tra cui ProFTPD, cPanel, Linux Kernel, GitHub, Rclone, Notepad++ e WordPress

Tendenze Emergenti

- Attacco supply chain SAP tramite canali ufficiali di distribuzione
- Spyware Morpheus legato ad azienda di sorveglianza italiana
- Phishing automatizzato AI con kit Bluekit (40 modelli)
- VECT 2.0: ransomware distruttivo che elimina i file definitivamente

Settori più Colpiti

- Aziende che utilizzano SAP (supply chain compromessa)
- Servizi legali e notarili italiani (phishing mirato)
- Istruzione universitaria italiana (Università di Palermo)
- Finanziario e assicurativo (AXA Colpatria, Fiserv)

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni implementino una serie di raccomandazioni operative. Il contesto in continua evoluzione delle minacce richiede particolare attenzione su più fronti, con priorità agli aggiornamenti critici, alla protezione contro il ransomware e alla formazione del personale.

Priorità immediate:

- Applicare immediatamente la patch di emergenza per cPanel (CVE-2026-41940) e aggiornare ProFTPD (CVE-2026-42167) per i quali sono disponibili PoC pubblici attivamente sfruttati.
- Aggiornare il Kernel di Linux (CVE-2026-31431) e tutti i sistemi GitHub e GitHub Enterprise Server (CVE-2026-3854) per prevenire escalation di privilegi e RCE non autenticata.
- Applicare le patch per Rclone (CVE-2026-41176 e CVE-2026-41179), Notepad++ (CVE-2026-3008) e WordPress (CVE-2026-4882) con urgenza.
- Verificare l'integrità di tutti i pacchetti SAP in uso, in particolare i pacchetti npm, per rilevare eventuali componenti malevoli distribuiti tramite la supply chain compromessa.

Misure di sicurezza strutturali:

- Investire in programmi di formazione per sensibilizzare i dipendenti sui rischi del phishing, con focus specifico sulle tecniche automatizzate AI (86% degli attacchi) e sul kit Bluekit con 40 modelli preconfigurati.
- Rafforzare la protezione dei dispositivi mobili aziendali Android per contrastare lo spyware Morpheus, adottando soluzioni di Mobile Device Management (MDM) e analisi comportamentale.
- Implementare strategie di Business Continuity e Disaster Recovery (BCDR) robuste, poiché la variante VECT 2.0 distrugge i file rendendone impossibile il recupero anche con i backup tradizionali.
- Monitorare attivamente le infrastrutture per rilevare attività sospette legate a malware di supply chain come quelli distribuiti tramite pacchetti npm SAP e librerie PyTorch Lightning.
- Adottare soluzioni di cybersecurity avanzate, come sistemi di rilevamento delle intrusioni e strumenti di analisi comportamentale, per migliorare la capacità di difesa contro le minacce in continua evoluzione.

Azioni Prioritarie

01 | Interventi Immediati

Applicare con urgenza le patch critiche per mitigare vulnerabilità attivamente sfruttate:

- cPanel (bypass autenticazione zero-day)
- Kernel Linux (elevazione privilegi)
- GitHub / Rclone / WordPress (RCE e bypass)

Verificare l'integrità dei pacchetti SAP utilizzati, in particolare quelli distribuiti tramite canali ufficiali potenzialmente compromessi.

02 | Azioni Prioritarie (entro 7 giorni)

Effettuare controlli mirati sulle superfici più esposte:

- Dispositivi Android aziendali → rilevamento spyware Morpheus
- Sistemi Windows → verifica aggiornamenti contro vulnerabilità zero-click
- Librerie e dipendenze → audit su componenti terze parti (npm, PyTorch, OpenVSX)

03 | Rafforzamento della Sicurezza

Adottare misure strutturali per ridurre il rischio nel medio periodo:

- Programmi di formazione sul phishing avanzato (AI-driven)
- Monitoraggio continuo delle infrastrutture e degli accessi
- Implementazione soluzioni MDM per dispositivi mobili

04 | Continuità Operativa & Ransomware

Adeguare le strategie di resilienza alla nuova evoluzione delle minacce:

- Revisione e test dei backup (rischio ransomware distruttivo)
- Aggiornamento dei piani di Business Continuity e Disaster Recovery
- Monitoraggio attivo delle attività anomale legate a gruppi ransomware

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