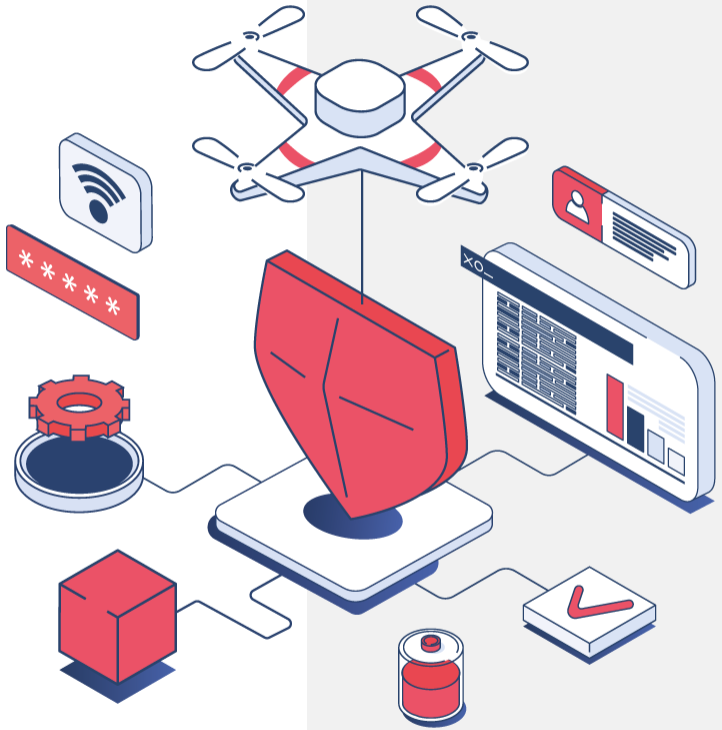
S3K

Cyber Threat

WEEKLY REPORT

\ week 04/05/2026 - 10/05/2026



www.s3kgroup.it

Sommario Settimanale CTI (03/05/2026 – 10/05/2026)

Aumento delle vulnerabilità critiche

Incremento significativo di vulnerabilità e exploit, con attacchi alla supply chain e zero-day che hanno impatti diretti su organizzazioni italiane ed europee.

Attacco Supply Chain JDownloader

Distribuita una versione malevola di JDownloader con installazione di RAT, evidenziando il rischio per utenti e aziende che utilizzano questo software.

Attacchi ransomware mirati

Gruppi come Safepay e TheGentlemen hanno rivendicato attacchi contro siti web e aziende italiane, sottolineando la vulnerabilità delle organizzazioni locali.

Campagne di phishing in aumento

116 campagne malevole rilevate dal CERT-AGID, di cui 78 mirate a obiettivi italiani, con smishing INPS e phishing a tema pedaggio autostradale.

Leak di dati sensibili

Numerosi database italiani in vendita sul dark web, con 1 milione di combinazioni di dati e 150.000 email italiane esposte, aumentando il rischio di furto d'identità.

Patch urgenti necessarie

Le organizzazioni sono esortate ad applicare tempestivamente patch per vulnerabilità critiche in PAN-OS, vm2, Ivanti EPMM, Exim e Sentry.

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 applicazioni e sistemi operativi. Le notizie più rilevanti riguardano attacchi alla supply chain, exploit zero-day e vulnerabilità critiche con impatti diretti su organizzazioni italiane ed europee.

- **Attacco alla Supply Chain di JDownloader:** Rilevata la distribuzione di una versione malevola di JDownloader attraverso un attacco alla supply chain, con installazione di un RAT sui sistemi compromessi. Rischio elevato per utenti e organizzazioni. Dettagli
- **Zero-Day in Palo Alto PAN-OS:** Segnalato un exploit critico per una vulnerabilità zero-day in PAN-OS, attivamente sfruttato in ambienti di produzione. Applicare patch urgenti. Dettagli
- **Vulnerabilità in MOVEit Automation:** Progress Software ha rilasciato aggiornamenti per correggere una vulnerabilità critica che consente bypass di autenticazione nella piattaforma di trasferimento file. Dettagli
- **Esplosione di exploit zero-day:** Rilasciati numerosi exploit zero-day, tra cui vulnerabilità in Apache Nifi e Google Android, con impatti su vasta gamma di applicazioni e dispositivi. Dettagli
- **Bug critico in vm2:** Identificata una vulnerabilità critica nel pacchetto vm2 che consente esecuzione di codice sui sistemi vulnerabili. Implementare misure di mitigazione. Dettagli
- **Vulnerabilità in Windows 11:** Scoperta una vulnerabilità di escalation dei privilegi che potrebbe consentire a un attaccante di ottenere accesso non autorizzato. Aggiornare i sistemi. Dettagli
- **Attacchi tramite CloudZ RAT:** Il malware CloudZ RAT sfrutta vulnerabilità nei dispositivi Windows Phone per rubare credenziali e OTP, evidenziando la necessità di proteggere i dispositivi mobili. Dettagli
- **Vulnerabilità nel kernel Linux:** Identificati exploit per diverse vulnerabilità nel kernel Linux, inclusi problemi di scrittura e condizioni di utilizzo di stringhe controllate esternamente. Dettagli

La settimana è stata caratterizzata da un aumento delle vulnerabilità critiche e degli exploit, con focus su attacchi alla supply chain e zero-day. È essenziale che le organizzazioni adottino misure proattive per proteggere sistemi e dati.

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama dei data leak ha mostrato un'attività preoccupante, con numerosi database e informazioni sensibili in vendita sul dark web. Diverse fonti hanno segnalato la disponibilità di kit di dati contenenti informazioni personali e credenziali di accesso italiane, con impatti potenzialmente significativi su individui e organizzazioni.

2.500

Kit documenti italiani

Database con ID e passaporti italiani messo in vendita su forum del dark web, con rischio elevato per l'identità degli individui coinvolti.

10.000

Combo email/password italiane

Pacchetto di combinazioni email e password italiane reso disponibile sul dark web, che evidenzia come molte credenziali di accesso siano vulnerabili.

1M

Combinazioni dati italiani

Leak di un milione di combinazioni di dati italiani segnalato, con ampia esposizione di informazioni sensibili.

150.000

Email italiane esposte (MailPass)

Emerso leak di 150.000 email italiane, che aumenta il rischio di attacchi di phishing e frode online.

In aggiunta, è stato segnalato un leak di accesso a **3.000 email italiane** con dati resi disponibili l'8 maggio; la compromissione del database di **RentalHomeBD.com** con informazioni personali e vulnerabilità critiche. Evidenziato un problema di sicurezza legato ad **Instagram**, e annunci su forum del dark web per l'acquisto di passaporti italiani. La settimana 03/05/2026 – 10/05/2026 ha evidenziato un aumento preoccupante delle violazioni, sottolineando l'importanza di rafforzare le misure di protezione dei dati.

Minacce per Settori Critici: Dettaglio Breach

Documenti d'identità italiani

Un database di 2.500 kit di documenti italiani (ID e passaporti) è in vendita su un forum del dark web, esponendo gli individui a gravi rischi di furto d'identità e frode documentale.

Credenziali e account email

Leak di 3.000 email italiane (8 maggio) e pacchetto di 10.000 combo email/password: le organizzazioni devono monitorare attività sospette e forzare il reset delle credenziali compromesse.

Piattaforme consumer e social

Problema di sicurezza su Instagram e database di RentalHomeBD.com compromesso: le aziende che utilizzano queste piattaforme dovrebbero rivedere le proprie politiche di sicurezza e protezione dei dati.

Dark Web & Monitoraggio

Un milione di combinazioni di dati italiani esposti, 150.000 email italiane in leak MailPass e passaporti italiani in vendita online. Necessario monitoraggio continuo del dark web per rilevare esposizioni aziendali.

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 software popolari e vulnerabilità critiche. Le campagne di compromissione delle supply chain continuano a rappresentare una minaccia rilevante, mentre nuovi malware emergono con tecniche sofisticate.

Principali Incidenti e Minacce

- **Attacco supply chain JDownloader:** Distribuita una versione malevola di JDownloader che installa un RAT sui sistemi compromessi. Tra il 6 e il 7 maggio il sito ufficiale ha servito malware a utenti Windows e Linux, sostituendo gli installer legittimi. Dettagli
- **PCPJack credential stealer:** Il malware PCPJack sfrutta cinque CVE per diffondersi come un worm attraverso sistemi cloud, mettendo a rischio le credenziali degli utenti. Dettagli
- **Malware su Google Ads e Claude.ai:** Hacker abusano di Google Ads e chat di Claude.ai per diffondere malware su sistemi Mac tramite ingegneria sociale. Dettagli
- **Botnet Mirai xlabs_v1:** Nuova botnet basata su Mirai sfrutta ADB per dirottare dispositivi IoT e lanciare attacchi DDoS. Dettagli

Nuovi Malware Identificati

TCLBanker
Trojan bancario che si diffonde attraverso WhatsApp e Outlook, prendendo di mira piattaforme finanziarie con capacità di auto-diffusione. Dettagli

Vidar Stealer (ClickFix)
Attacchi ClickFix segnalati in Australia con utilizzo di Vidar Stealer per rubare informazioni sensibili. Dettagli

Malware stealth Linux P2P
Nuovo malware stealth trasforma i sistemi Linux in reti di attacco P2P, richiedendo maggiore attenzione alla sicurezza in ambienti aziendali. Dettagli

CloudZ RAT
Malware che sfrutta vulnerabilità nei dispositivi Windows Phone per rubare credenziali e OTP, con impatto su applicazioni aziendali mobili. Dettagli

- Le organizzazioni italiane ed europee devono adottare misure proattive per proteggere i propri sistemi, verificare l'integrità dei software scaricati da fonti ufficiali e monitorare costantemente i dispositivi IoT e i sistemi Linux aziendali. La compromissione del sito ufficiale di JDownloader evidenzia che nemmeno i canali ufficiali sono sempre affidabili.

Phishing & Social Engineering

Negli ultimi sette giorni, il CERT-AGID ha riportato 116 campagne malevole, di cui 78 mirate ad obiettivi italiani. Le tecniche utilizzate spaziano da messaggi SMS fraudolenti ad email ingannevoli, con l'obiettivo di rubare dati sensibili e credenziali. Si evidenzia un aumento significativo delle campagne di smishing che sfruttano nomi di enti pubblici.

01

Phishing N26

Campagna phishing che colpisce gli utenti della banca tedesca N26, mirata al furto di credenziali, informazioni personali e OTP per completare operazioni fraudolente. Dettagli

02

Smishing INPS

Campagna di smishing che utilizza il nome dell'INPS per raccogliere nome, codice fiscale e dati bancari attraverso false promesse di erogazioni statali. Il dominio malevolo è stato sospeso e gli IoC distribuiti. IoC

03

Phishing pedaggio autostradale

Campagna via WhatsApp che inganna le vittime con la falsa notizia di un mancato pagamento del pedaggio autostradale, chiedendo di inserire i dati della carta di pagamento. Dettagli

04

Campagna phishing globale Microsoft

Microsoft ha avvertito di una campagna di phishing su larga scala che ha colpito oltre 35.000 utenti in 26 paesi, utilizzando email di compliance false per rubare credenziali.

05

Phishing tramite Google Ads

Hacker abusano di Google Ads per lanciare attacchi di phishing mirati a utenti di servizi di gestione come GoDaddy, con tecniche di attacco in continua evoluzione.

06

Servizi di Social Engineering

Forum del dark web offrono servizi di social engineering e strumenti per bypassare i meccanismi di sicurezza, aumentando il rischio per le organizzazioni e amplificando la portata degli attacchi.

Tecniche in Evidenza

- Smishing con impersonificazione INPS (erogazioni statali false)
- Phishing a tema pagamenti e pedaggi via WhatsApp
- Campagne di phishing su banche europee (N26)
- Abuso di Google Ads per distribuzione malware e phishing

Target Principali Italiani

- Utenti di servizi bancari europei (N26)
- Cittadini esposti a comunicazioni INPS false
- Automobilisti (pedaggio autostradale)
- Utenti di piattaforme di gestione dominio (GoDaddy)

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama dei ransomware ha visto un incremento significativo degli attacchi mirati ad organizzazioni italiane. Gruppi come Safepay, TheGentlemen, Bavacai, Medusalocker e LeakBazaar hanno rivendicato attacchi contro aziende italiane, evidenziando la continua vulnerabilità delle organizzazioni locali.

Attacchi Safepay in Italia

Safepay ha rivendicato attacchi contro studioubertazzi.it (6 maggio), soavegel.it (6 maggio) e zonaovest.to.it (5 maggio), con codici hash documentati per ciascun incidente.

Attacchi TheGentlemen

Il gruppo TheGentlemen ha colpito DATAMATIC e Media-Consulting il 6 maggio 2026, con codici hash specifici documentati per entrambe le vittime italiane.

Attacco a SIT-Group--Robusta

Due gruppi distinti, Bavacai e Medusalocker, hanno rivendicato separatamente attacchi contro SIT-Group--Robusta il 5 maggio 2026, evidenziando il rischio di attacchi multipli simultanei.

LeakBazaar: nuove vittime (10 maggio)

Il gruppo LeakBazaar ha pubblicato una serie di nuove vittime il 10 maggio 2026, tra cui Wayne-Brothers, Omax-Autos e Millennium-packages, con codici hash specifici per ciascun attacco.

MuddyWater e Chaos Ransomware

Il 9 maggio 2026 è emerso che i MuddyWater Hackers utilizzano il Chaos Ransomware come decoy nei loro attacchi, con una strategia di diversione per mascherare le loro vere intenzioni.

Vulnerabilità Critiche & Patch

Negli ultimi sette giorni, il panorama delle vulnerabilità ha visto un aumento significativo di attività, con diverse vulnerabilità critiche e zero-day scoperte e, in alcuni casi, già sfruttate attivamente. Le organizzazioni italiane ed europee sono esortate a prestare particolare attenzione agli aggiornamenti di sicurezza.

1	**Ivanti Endpoint Manager Mobile** Rilasciati aggiornamenti per cinque vulnerabilità di gravità alta, inclusa una zero-day, che potrebbero consentire esecuzione di codice remoto e elevazione dei privilegi. Aggiornamento fondamentale. Dettagli
2	**vm2 per Node.js** Disponibili PoC per vulnerabilità critiche nella libreria vm2, che potrebbero consentire l'esecuzione di comandi arbitrari sul sistema ospitante. Implementare misure di mitigazione urgenti. Dettagli
3	**CVE-2026-43284 – Linux Dirty Frag** Rilevata una PoC per la vulnerabilità Dirty Frag che consente l'elevazione dei privilegi nel kernel Linux, permettendo a un utente non privilegiato di ottenere diritti di root. Dettagli
4	**CVE-2026-0300 – Palo Alto PAN-OS** Rilevato sfruttamento attivo in rete della vulnerabilità che consente esecuzione di codice remoto. Le organizzazioni devono mantenere aggiornati i sistemi PAN-OS per prevenire attacchi. Dettagli
5	**Juniper Secure Analytics** Juniper ha rilasciato aggiornamenti per vulnerabilità di gravità alta che potrebbero consentire a un attaccante locale di ottenere il controllo completo dei sistemi. Dettagli
6	**CVE-2026-44331 – ProFTPD** Disponibile una PoC per la vulnerabilità che consente l'elusione dei meccanismi di sicurezza in ProFTPD. Aggiornare i sistemi per mitigare il rischio. Dettagli
7	**Exim – Vulnerabilità critiche** Rilevate vulnerabilità di gravità critica nel server di posta Exim che potrebbero portare a divulgazione di informazioni e attacchi Denial of Service. Dettagli
8	**Sentry – SAML SSO critico** Scoperta una vulnerabilità critica nel processo SAML SSO che consente l'associazione di identità utente non autorizzata. Corretta nella versione 26.4.1. Aggiornare immediatamente. Dettagli

Vulnerabilità Aggiuntive e Patch

Ivanti EPMM – Zero-Day

Cinque vulnerabilità di gravità alta, inclusa una zero-day con possibilità di RCE ed elevazione dei privilegi. Aggiornamento urgente richiesto per tutti i sistemi Ivanti interessati.

Juniper Secure Analytics

Vulnerabilità di gravità alta con possibilità di controllo completo dei sistemi da parte di attaccanti locali. Applicare gli aggiornamenti rilasciati da Juniper.

vm2 Node.js – PoC pubblico

PoC disponibili per vulnerabilità critiche nella libreria vm2. Le aziende che utilizzano questo pacchetto devono implementare immediatamente misure di mitigazione.

ProFTPD – CVE-2026-44331

PoC pubblica per elusione dei meccanismi di sicurezza in ProFTPD. Aggiornamento dei sistemi necessario per mitigare il rischio di exploit.

CVE-2026-0300 – PAN-OS (Palo Alto)

Sfruttamento attivo confermato in ambienti di produzione. Applicare patch urgenti per prevenire esecuzione di codice remoto nei sistemi Palo Alto Networks.

Exim – Vulnerabilità critiche

Vulnerabilità critiche nel server di posta Exim con rischio di divulgazione di informazioni e Denial of Service. Applicare aggiornamenti immediatamente.

Linux Dirty Frag – CVE-2026-43284

PoC pubblica per elevazione dei privilegi nel kernel Linux. Un utente non privilegiato può ottenere diritti di root. Patch immediata necessaria.

Sentry – SAML SSO v26.4.1

Vulnerabilità critica nel processo SAML SSO corretta nella versione 26.4.1. Aggiornamento urgente per tutte le istanze Sentry in produzione.

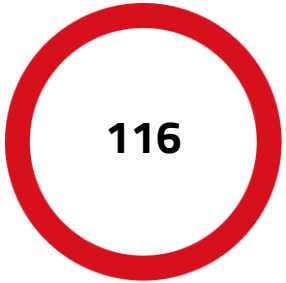
La settimana ha evidenziato un numero significativo di vulnerabilità critiche e PoC pubblici, sottolineando l'importanza di un approccio proattivo alla sicurezza informatica. Le organizzazioni devono aggiornare tempestivamente i propri software e monitorare costantemente le nuove segnalazioni di vulnerabilità.

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della sicurezza informatica ha evidenziato un incremento preoccupante delle vulnerabilità e degli exploit, con un focus particolare su attacchi alla supply chain e vulnerabilità zero-day. Le organizzazioni italiane ed europee si trovano ad affrontare una crescente varietà di minacce, tra cui attacchi mirati a software di uso comune e la diffusione di malware attraverso tecniche sofisticate. Si osserva un'intensificazione delle campagne di phishing e social engineering, con particolare attenzione alle campagne INPS e N26, che sfruttano l'ingegneria sociale per rubare dati sensibili.

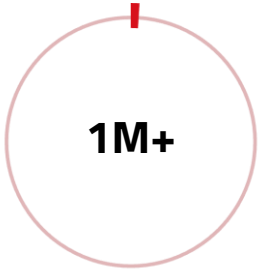
Il numero di leak di dati e violazioni ha raggiunto livelli allarmanti, con un milione di combinazioni di dati italiani esposte e 150.000 email italiane in leak, esponendo ulteriormente le aziende a rischi di furto d'identità e attacchi mirati. Gli attacchi ransomware da gruppi come Safepay e TheGentlemen si confermano persistenti contro le aziende italiane, mentre la scoperta dell'uso del Chaos Ransomware come decoy da parte di MuddyWater suggerisce una crescente sofisticazione tattica. La compromissione del sito ufficiale di JDownloader rappresenta un segnale d'allarme sulla fiducia negli aggiornamenti software anche da fonti apparentemente legittime.

Tendenze chiave: attacchi alla supply chain su software legittimi (JDownloader), sfruttamento attivo e accelerato di zero-day (PAN-OS, EPMM), intensificazione delle campagne smishing con impersonificazione INPS, escalation dei leak di dati italiani sul dark web, e utilizzo di ransomware come decoy per mascherare operazioni di spionaggio.



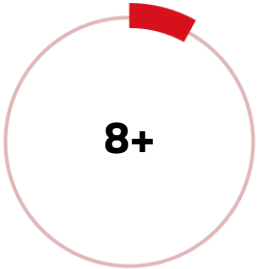
Campagne Malevole

Identificate dal CERT-AGID nella settimana (03/05/2026 – 10/05/2026), di cui 78 dirette ad obiettivi italiani



Dati Italiani Esposti

Combinazioni di dati italiani in leak sul dark web, tra cui email, password, documenti d'identità e passaporti



CVE Critiche Attive

Vulnerabilità critiche con PoC o sfruttamento attivo confermato nella settimana, tra cui PAN-OS, Linux, Exim e Sentry

Tendenze Emergenti

- Attacchi supply chain a software legittimi (JDownloader)
- Phishing mirato su servizi pubblici italiani (INPS, pedaggio)
- Sfruttamento accelerato di zero-day (PAN-OS, EPMM)
- Utilizzo di ransomware come decoy (MuddyWater + Chaos)

Settori più Colpiti

- Settore bancario e finanziario (TCLBanker, N26)
- Infrastrutture IT (supply chain, cloud, IoT)
- Pubblica Amministrazione (smishing INPS)
- PMI italiane (Safepay, TheGentlemen ransomware)

Framework di Implementazione

1

Valutazione Rischio

Mappatura superfici di attacco con focus su PAN-OS (CVE-2026-0300), Ivanti EPMM (zero-day), Linux kernel (Dirty Frag CVE-2026-43284), Exim e Sentry. Prioritizzare i sistemi esposti a internet e verificare installazioni JDownloader.

2

Patch Management Urgente

Applicare immediatamente le patch per Palo Alto PAN-OS, Ivanti EPMM, ProFTPD (CVE-2026-44331), Exim, Sentry (v26.4.1) e vm2 per Node.js. Verificare i sistemi Juniper Secure Analytics e aggiornare i prodotti MOVEit Automation.

3

Difesa Anti-Phishing

Implementare filtri avanzati per campagne smishing INPS, phishing N26 e pedaggio autostradale. Distribuire gli IoC pubblicati dal CERT-AGID (smishing INPS, 8 maggio). Formare i dipendenti su tecniche di social engineering e Google Ads phishing.

4

Protezione Anti-Malware

Bloccare gli indicatori di compromissione per TCLBanker, CloudZ RAT, PCPJack, Vidar Stealer e malware stealth Linux P2P. Verificare l'integrità di tutti i download JDownloader e monitorare i dispositivi IoT per attività Mirai.

5

Monitoraggio Continuo

Attivare alert per attività Safepay, TheGentlemen, LeakBazaar e MuddyWater. Monitorare il dark web per leak di dati italiani (1M combinazioni, 150K email, kit documenti). Verificare i log di accesso su piattaforme con autenticazione SAML SSO.

Coordinamento Nazionale: Per minacce che coinvolgono infrastrutture italiane critiche o dati di cittadini (campagne smishing INPS, database documenti italiani in vendita, attacchi ransomware a PMI italiane), coordinare la risposta con CSIRT Italia e ACN per massimizzare l'efficacia delle contromisure e la condivisione di intelligence.

116

Campagne Malevole
Identificate dal CERT-AGID nella settimana

7

Giorni Copertura
Monitoraggio continuativo minacce

24/7

Sorveglianza
Monitoraggio indicatori di compromissione

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