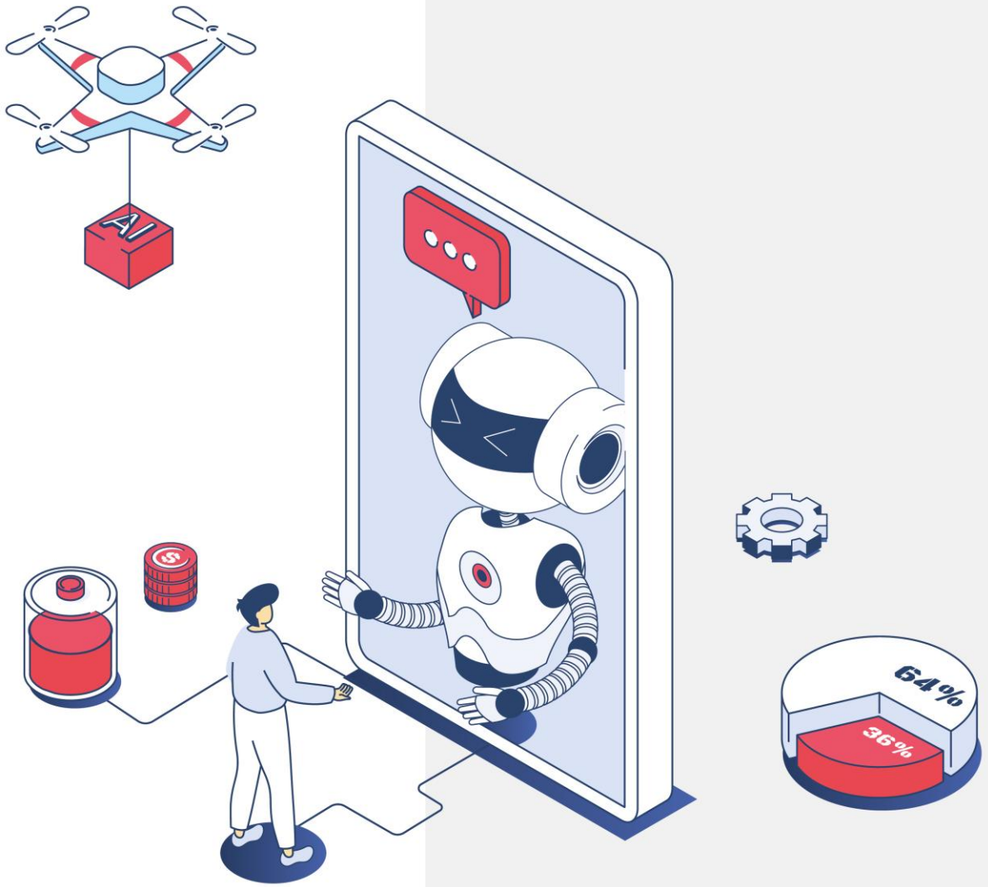
S3K

Cyber Threat

WEEKLY REPORT

\ week 26/01/2026 - 01/02/2026



www.s3kgroup.it

CTI WEEKLY

Sommario Settimanale (25/01/2026 – 01/02/2026)

Aumento degli Attacchi Ransomware

Diverse organizzazioni italiane, tra cui AUGUSTEA.COM, sono state colpite da attacchi ransomware, evidenziando la vulnerabilità del settore dei servizi online e della logistica

Vulnerabilità Zero-Day Critiche

Scoperte vulnerabilità zero-day in prodotti Ivanti e Fortinet, richiedendo aggiornamenti urgenti per mitigare i rischi di attacchi informatici

Data Leak Preoccupanti

Accessi non autorizzati a siti web italiani e vendita di database contenenti credenziali compromesse, aumentando il rischio di attacchi mirati

- **Attività di Phishing in Crescita**

  97 campagne di phishing registrate dal CERT-AGID, con 58 mirate ad obiettivi italiani, utilizzando tecniche di ingegneria sociale per rubare dati sensibili

- **Malware Avanzato in Circolazione**

  Nuove minacce come il malware fileless ShadowHS su Linux rappresentano un rischio crescente per le infrastrutture aziendali

NEWS CYBER

Attività Malevole della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo di attacchi ransomware, con diversi settori colpiti, tra cui logistica, comunicazioni e servizi pubblici. Le minacce emergenti, come quelle attribuite ai gruppi di attacco Clop e Qilin, hanno messo in evidenza la vulnerabilità di molte organizzazioni, in particolare in Europa e negli Stati Uniti.

Attacchi Ransomware Principali

- Clop colpisce AUGUSTEA.COM (Italia)
- Qilin attacca Trace (Francia) e Cooperativa de Hostelería de Navarra (Spagna)
- 0apt prende di mira Urban Outfitters e National Rail Network (UK)
- Meridian Logistics sotto attacco ransomware

Organizzazioni Sanitarie e Infrastrutture

- Rocky Mountain Associated Physicians (USA)
- Atlantic National Trust (USA)
- Tulsa International Airport compromesso
- Studi legali brasiliani PK Pinhão e Diehl and Cella Advogados

Focus Italia: Il sito italiano AUGUSTEA.COM è stato colpito da un attacco ransomware attribuito al gruppo Clop, evidenziando la vulnerabilità delle aziende locali nel settore dei servizi online e sottolineando l'urgenza per le organizzazioni italiane di adottare misure di sicurezza rafforzate.

DATA BREACH

Data Leak & Breach: Scenario Italiano

150K

Database Email Italiane

Database contenente 150.000 email italiane disponibile, potenzialmente utilizzato per attacchi di phishing o spam

130K

Good Combolist

Lista di combinazioni di credenziali con 130.000 voci, sfruttabile per attacchi mirati a vari servizi online

3

Siti Italiani Compromessi

Accessi non autorizzati a dronezine.it, fisioterapialaquila.it con credenziali di amministrazione esposte

2

Database Freschi

Database di livecongress.it e italiamilitare.it resi disponibili, aumentando rischio attacchi mirati

La settimana ha mostrato un'attività intensa nei data leak e violazioni di dati, con numerosi incidenti che coinvolgono principalmente dati sensibili e accessi non autorizzati a piattaforme italiane. Diverse fonti hanno riportato la vendita di dati personali e credenziali di accesso, evidenziando un trend preoccupante per la sicurezza informatica in Italia e in Europa.

Rischi per Settori Critici

Settore dei Servizi Online

AUGUSTEA.COM colpita da Clop. Vulnerabilità delle aziende italiane nel settore dei servizi digitali e necessità di protezioni robuste

Settore Logistica e Trasporti

Meridian Logistics, Apex Logistics Solutions e Skyline Logistics Group sotto attacco. Rischi per aziende in settori critici di trasporto

Settore Sanitario

Organizzazioni sanitarie negli USA colpite. Importanza della sicurezza informatica per proteggere dati sensibili dei pazienti

Infrastrutture Critiche

Tulsa International Airport e National Rail Network sotto attacco, evidenziando vulnerabilità infrastrutture critiche europee e americane

MALWARE

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha mostrato un'attività intensa, con attori malevoli che continuano a sfruttare vulnerabilità e tecnologie emergenti per lanciare attacchi sempre più sofisticati. Le notizie evidenziano una crescente preoccupazione per le campagne di malware mirate, l'uso di tecniche avanzate come il fileless malware e l'emergere di nuove minacce legate all'intelligenza artificiale.

Minacce Fileless e Advanced

1. **ShadowHS su Linux:** Nuovo framework di post-exploitation con loader fileless che esegue payload in memoria senza lasciare tracce su disco
2. **Malware SEO UAT-8099:** Attacchi contro server IIS vulnerabili in Asia da attore legato alla Cina
3. **Attacco Supply Chain eScan:** eScan Antivirus come vettore per diffusione malware, evidenziando vulnerabilità delle catene di approvvigionamento

Minacce AI-Powered e Emerging

RedKitten AI Malware

Malware sviluppato tramite IA per colpire dissidenti politici in Iran

Android Malware su Hugging Face

Migliaia di varianti di malware per Android distribuite tramite piattaforma

Nordcoreano Hydra

Evoluzione in "Hydra a tre teste" con nuove varianti mirate

Google ha interrotto le reti proxy residenziali IPIDEA, alimentate da malware. È emersa inoltre una crisi degli infostealer con 149 milioni di credenziali compromesse, evidenziando la necessità di misure di sicurezza rafforzate per proteggere i dati sensibili.

Phishing & Social Engineering

01

Smishing a tema INPS

Campagna che richiede caricamento di documenti sensibili come CUD e informazioni lavorative sfruttando il nome dell'INPS

02

Phishing Polizia di Stato

Campagna che utilizza logo della Polizia di Stato per rubare credenziali email tramite pagina malevola creata con Webflow

03

Phishing tramite Caselle PA

Attaccanti sfruttano email di Pubbliche Amministrazioni compromesse per inviare messaggi mascherati da fatture

04

Campagna Tessera Sanitaria

Email ingannevoli su "scadenza imminente" della Tessera Sanitaria per raccogliere dati personali e informazioni di pagamento

05

Phishing a tema SPID

Campagna che abusa del nome di AgID e Dipartimento per la Trasformazione Digitale per verifica profilo SPID

Tecniche Utilizzate

- Sfruttamento loghi ufficiali (Polizia, INPS, AgID)
- Uso caselle email PA compromesse
- Messaggi su servizi pubblici (Tessera Sanitaria, SPID)
- Campagne WhatsApp con account compromessi

Settori Bancari Sotto Attacco

- Phishing Intesa Sanpaolo per credenziali bancarie
- Campagne WhatsApp per richieste pagamento
- ClickFix sfrutta vulnerabilità WordPress
- 97 campagne totali, 58 mirate a obiettivi italiani

RANSOMWARE

Operazioni Ransomware Active

Negli ultimi sette giorni, il panorama delle minacce ransomware ha visto un incremento significativo di attacchi mirati, con diversi gruppi che hanno rivendicato attacchi contro aziende di logistica, tecnologia e servizi. Le operazioni si sono concentrate su organizzazioni vulnerabili, evidenziando la continua evoluzione delle tecniche utilizzate dai criminali informatici.

Clop - Target Italia

AUGUSTEA.COM compromessa, evidenziando vulnerabilità aziende italiane nel settore servizi online. Focus su settore digitale nazionale

Qilin - Espansione Europea

Attacchi multipli: Trace (Francia), Cooperativa de Hostelería de Navarra (Spagna). Operazione coordinata su scala internazionale

0apt - Settore Logistica

Meridian Logistics, Apex Logistics Solutions, Skyline Logistics Group colpiti. Vulnerabilità settore logistico evidenziata

Everest - Attività Giapponese

Hosowaka Micron Group e Shinwa Co Ltd compromesse. Aumento attività del gruppo con focus su aziende tecnologiche

Altri gruppi attivi includono thegentlemen (Hydrometrics), incransom (Foamtec International), Play (Deatak) e Worldleaks (FluidOne). Gli attacchi hanno interessato anche infrastrutture critiche come il Tulsa International Airport e organizzazioni sanitarie negli Stati Uniti.

VULNERABILITÀ

Vulnerabilità Critiche & Patch

1

Ivanti Zero-Day

Due vulnerabilità critiche in Endpoint Manager Mobile (EPMM), inclusa una zero-day. Esecuzione codice arbitrario remoto possibile. Aggiornamenti essenziali

2

CVE-2026-24858

Fortinet: Sfruttamento attivo della zero-day in FortiOS che consente bypass dell'autenticazione. Mitigazioni disponibili per ridurre rischio

3

CVE-2026-21509

Microsoft Office: Sfruttamento attivo di vulnerabilità zero-day che interessa varie versioni. Aggiornamenti di sicurezza disponibili

4

CVE-2026-23988

Rufus: PoC pubblico per vulnerabilità che consente esecuzione codice arbitrario con privilegi elevati. Aggiornamento raccomandato

5

CVE-2026-24061

GNU Inetutils: Sfruttamento attivo di vulnerabilità nel demone telnetd che consente bypass dell'autenticazione. Patch disponibili

6

CVE-2026-25069

SunFounder: Traversamento di percorso in Pironman Dashboard v1.3.13. CVSS 9.3. Lettura e cancellazione file arbitrari possibile

Vulnerabilità Aggiuntive

CVE-2020-37043

10-Strike Bandwidth Monitor v3.9: Buffer overflow che consente esecuzione codice remoto. CVSS 9.8. Aggiornamento urgente

Ivanti EPMM Critical

Due vulnerabilità critiche scoperte, inclusa zero-day attivamente sfruttata. Implementazione patch immediata necessaria

Fortinet FortiOS

CVE-2026-24858 sfruttata attivamente in rete. Bypass autenticazione possibile. Mitigazioni urgenti richieste

Microsoft Office Updates

Aggiornamenti per CVE-2026-21509 rilasciati. Sfruttamento attivo confermato. Applicazione patch prioritaria

Raccomandazione Immediata

Priorità assoluta per patch Ivanti, Fortinet CVE-2026-24858, Microsoft CVE-2026-21509 e GNU telnetd entro 48 ore

Vulnerability Scanning

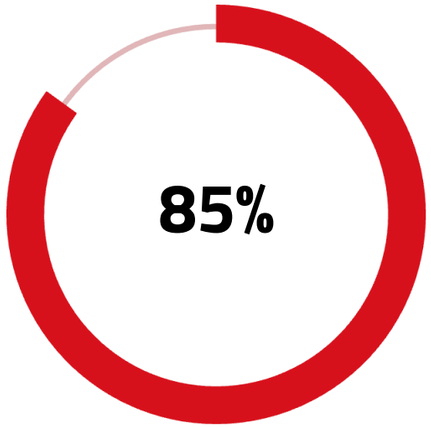
Intensificare scansioni per zero-day Ivanti e Fortinet. Focus su perimetro esterno e sistemi esposti pubblicamente

Il recente aumento delle vulnerabilità critiche e degli exploit attivi, in particolare le zero-day in Ivanti, Fortinet e Microsoft Office, richiede un'attenzione immediata da parte delle organizzazioni. È fondamentale che le aziende italiane ed europee aggiornino tempestivamente i loro sistemi per proteggersi da potenziali attacchi informatici.

ANALISI

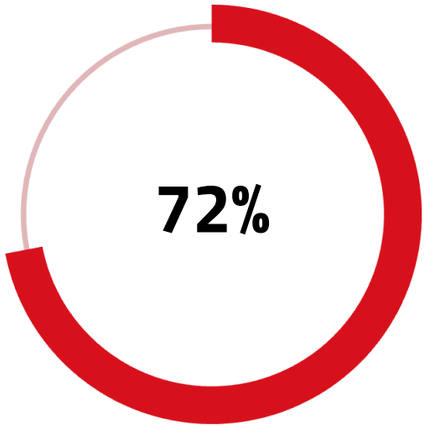
Analisi Trasversale e Tendenze

L'analisi della settimana rivela un incremento preoccupante delle attività malevole con sofisticazione crescente. I gruppi di ransomware hanno intensificato le loro operazioni contro il settore logistico e dei servizi online, mentre vulnerabilità zero-day significative in prodotti Ivanti, Fortinet e Microsoft Office sono state sfruttate attivamente. Le organizzazioni italiane ed europee affrontano minacce sempre più complesse e coordinate.



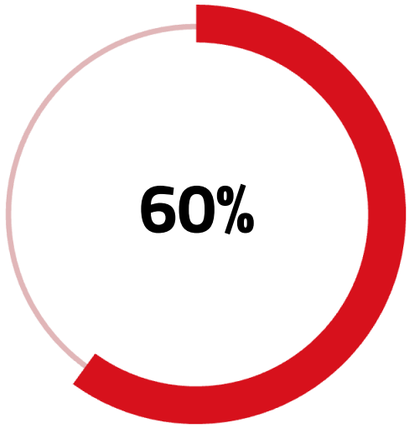
Attacchi Ransomware

Aumento intensità operazioni Clop, Qilin, 0apt con focus logistica



Zero-Day Exploit

Percentuale vulnerabilità zero-day con sfruttamento attivo confermato



Phishing Target Italia

58 su 97 campagne CERT-AGID mirate a obiettivi italiani

Tendenze Emergenti

- Ransomware mira settore logistico (Meridian, Apex, Skyline)
- Malware fileless aumenta difficoltà di rilevamento (ShadowHS)
- Phishing sfrutta enti pubblici (INPS, Polizia, AgID)
- AI-powered malware per campagne mirate (RedKitten)

Settori più Colpiti

- Logistica e trasporti: attacchi multipli coordinati
- Servizi online: AUGUSTEA.COM compromessa in Italia
- Sanità: organizzazioni USA sotto attacco ransomware
- Infrastrutture critiche: aeroporti e reti ferroviarie

RACCOMANDAZIONI

Raccomandazioni Operative Prioritarie

Per affrontare efficacemente le minacce rilevate, le organizzazioni devono adottare un approccio proattivo e multilivello alla sicurezza informatica. L'aumento degli attacchi ransomware contro il settore logistico e le vulnerabilità zero-day attivamente sfruttate richiedono particolare attenzione. Le seguenti azioni prioritarie sono raccomandate.

01

Patch Management Critico

Applicare immediatamente patch per Ivanti EPMM, Fortinet CVE-2026-24858, Microsoft Office CVE-2026-21509 e GNU telnetd CVE-2026-24061. Priorità massima per sistemi esposti

02

Formazione Anti-Phishing

Sensibilizzare dipendenti su campagne INPS, Polizia di Stato, SPID e Tessera Sanitaria. Focus su riconoscimento loghi falsificati e email PA compromesse

03

Protezione Credenziali

Monitorare leak di database email italiane (150K) e combolist (130K). Implementare autenticazione multi-fattore e rotazione password

04

Monitoraggio Settore Logistica

Intensificare hunting per IOC correlati a 0apt, Clop, Qilin. Protezione particolare per aziende logistica dopo attacchi multipli coordinati

05

Difesa da Malware Fileless

Implementare soluzioni EDR avanzate per rilevamento ShadowHS e malware fileless. Monitoraggio comportamentale in memoria critico

Framework di Implementazione

1

Valutazione Rischio

Mappatura superfici di attacco e identificazione asset critici esposti a vulnerabilità zero-day Ivanti, Fortinet, Microsoft

2

Prioritizzazione

Focus su zero-day attive, protezione settore logistica, difesa da phishing PA e monitoring leak credenziali italiane

3

Implementazione

Roll-out patch urgenti Ivanti/Fortinet/Microsoft, configurazioni MFA, formazione su phishing INPS/Polizia/SPID

4

Verifica

Testing efficacia difese anti-ransomware per logistica e risposta a campagne phishing enti pubblici

5

Miglioramento

Revisione continua basata su intelligence Clop/Qilin/0apt, monitoring zero-day e lesson learned da incidenti

Coordinamento Nazionale: Per minacce che coinvolgono aziende italiane (AUGUSTEA.COM), accessi non autorizzati a siti italiani o campagne phishing contro enti pubblici (INPS, Polizia, AgID), coordinare risposta con CSIRT Italia e ACN per massimizzare efficacia delle contromisure.

97

Campagne Phishing Registrate da CERT-AGID nella settimana

7

Giorni Copertura Monitoraggio continuativo minacce

24/7

MonitoraggioSorveglianza indicatori compromissione

Company Profile S3K

S3K Group (Security of the Third Millennium) è un **Trusted & Secure Digital Transformation Partner,** che supporta le organizzazioni nel **ridurre i rischi**, **proteggere il valore digitale** e **guidare il cambiamento**.

- ❑ **Core Capabilities**
- ❑ **Cyber Security**
- ❑ **Data Science & Big Data**
- ❑ **Cloud & Application Dev**
- ❑ **Telco & Security Infrastructure**
- ❑ **PLM (Product Lifecycle Management)**
- ❑ **Modelling & Simulation**
- ❑ **Consulting & ERP**
- ❑ **Intellectual Properties e R&D**

CLASSIFICAZIONE DOCUMENTO : 2.0 TLP:CLEAR = Divulgazione illimitata

Classificazione Traffic Light Protocol (TLP): sistema di contrassegni che definisce la misura in cui i destinatari possono condividere informazioni potenzialmente sensibili pubblicato formalmente da Forum of Incident Response and Security Teams (FIRST) nella versione TLP 1.0 nell'agosto 2016 e successivamente aggiornato alla versione TLP 2.0 nell'agosto 2022. Secondo FIRST, lo scopo di TLP è "facilitare una maggiore condivisione di informazioni potenzialmente sensibili e collaborazione più efficace". La versione 2.0 migliora TLP chiarendo ulteriormente le restrizioni di condivisione.

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