S3K

Cyber Threat

WEEKLY REPORT

\ week 09/02/2026 - 15/02/2026

www.s3kgroup.it

Aumento delle minacce alle infrastrutture critiche

Le autorità europee hanno avvertito riguardo alla vulnerabilità delle infrastrutture critiche, esortando ad investimenti maggiori per proteggere l'Europa da attacchi informatici sofisticati

Nuove vulnerabilità critiche

È stata identificata una vulnerabilità critica in BeyondTrust e in SharePoint, richiedendo patch urgenti per prevenire attacchi di esecuzione di codice remoto

Campagne ransomware in crescita

Gruppi come SpaceBears e Lynx Ransomware hanno intensificato gli attacchi, colpendo organizzazioni italiane e europee e sfruttando vulnerabilità note

- **Esposizione di dati sensibili**

  Diverse liste di email italiane sono state pubblicate sul dark web, aumentando il rischio di attacchi di phishing e frodi

- **Attività malevole di malware**

  Campagne di malware come Lumma Stealer e AMOS hanno preso di mira sistemi Windows e macOS, evidenziando l'evoluzione delle tecniche di attacco

NEWS CYBER

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un aumento significativo delle minacce e delle vulnerabilità, con particolare attenzione alle infrastrutture critiche e alle tecnologie operative. Le autorità europee hanno lanciato avvertimenti riguardo alla necessità di rafforzare le difese contro attacchi informatici sempre più sofisticati. Inoltre, sono emerse nuove vulnerabilità in software di uso comune, mentre le campagne di ransomware continuano a colpire aziende in tutto il mondo, inclusa l'Italia.

Infrastrutture Critiche e Vulnerabilità

- Infrastrutture critiche a rischio: l'UE non può più essere "naive"
- Vulnerabilità SolarWinds Web Help Desk attivamente sfruttate
- Vulnerabilità critica in BeyondTrust richiede patch urgenti
- CVE-2025-53770: vulnerabilità critica in SharePoint

Attacchi e Minacce Emergenti

- Campagna ClickFix tramite commenti Pastebin
- Attacchi di ransomware in aumento contro organizzazioni italiane
- Problemi con AWS WAF: tecniche di bypass in aumento
- CISA ordina patch urgenti per dieci vulnerabilità entro marzo

Focus San Valentino 2026: Sono stati registrati oltre 3.280 domini sospetti legati a truffe romantiche e frodi su criptovalute, evidenziando l'importanza di una vigilanza continua da parte degli utenti in vista di San Valentino.

DATA BREACH

Data Leak & Breach: Scenario Italiano

6.2M

Dati Odido Esposti

Il fornitore olandese Odido ha subito un attacco che ha esposto i dati personali di 6,2 milioni di clienti, inclusi nomi e numeri di conto bancario

5.5M

Clienti Marchi di Lusso

Louis Vuitton, Dior e Tiffany multati per 25 milioni di dollari per violazioni che hanno esposto dati di oltre 5,5 milioni di clienti

4M

Email Italiane sul Dark Web

Diverse liste di email italiane pubblicate sul dark web, con batch che contengono fino a 4 milioni di contatti

1

Database Smarterstore.it

Violazione confermata con database contenente informazioni sui clienti esposto, evidenziando rischi nel settore e-commerce

La settimana ha evidenziato un'intensa attività di violazioni e perdite di dati, con numerosi incidenti che hanno coinvolto sia aziende italiane che internazionali. Figure ha confermato una violazione dei dati con il gruppo ShinyHunters che ha rivendicato la responsabilità. La crescente disponibilità di dati sensibili sul dark web rappresenta una minaccia costante per le organizzazioni, richiedendo attenzione e misure di sicurezza adeguate.

Minacce per Settori Critici Globali

Settore Fintech

Figure ha subito una violazione dei dati dopo compromissione di un account dipendente. ShinyHunters ha rivendicato l'attacco, evidenziando vulnerabilità nel settore fintech

Telecomunicazioni

L'attacco a Odido ha esposto 6,2 milioni di clienti, dimostrando la vulnerabilità delle aziende di telecomunicazioni e la necessità di protezione dati rafforzata

Marchi di Lusso

Louis Vuitton, Dior e Tiffany multati per 25 milioni di dollari in Corea del Sud per inadeguate misure di sicurezza che hanno portato all'esposizione di dati di milioni di clienti

Sicurezza Nazionale

Un leak ha rivelato informazioni militari critiche, aumentando le preoccupazioni sulla sicurezza nazionale e sull'integrità delle informazioni sensibili

MALWARE

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un'intensificazione delle attività malevole, con attacchi mirati a diverse piattaforme e sistemi operativi. Le campagne di malware si sono evolute, sfruttando tecniche sempre più sofisticate, come l'abuso di servizi legittimi e l'ingegneria sociale. Le organizzazioni italiane ed europee devono rimanere vigili di fronte a queste minacce in continua evoluzione.

Campagne Principali

1. **Lumma Stealer e Ninja Browser:** Oltre 4.000 Google Groups e 3.500 URL Google utilizzati per diffondere malware su Windows e Linux
2. **AMOS su macOS:** Nuovo infostealer che prende di mira utenti macOS attraverso app di intelligenza artificiale popolari
3. **Falsi reclutatori nordcoreani:** Campagne di phishing mirate a sviluppatori JavaScript e Python con malware nascosto in sfide di codifica

Minacce Emergenti

Claude LLM Abuse

Sfruttamento artefatti Claude e Google Ads per distribuire infostealer su macOS

SSHStalker Botnet

Nuova botnet Linux che utilizza IRC per comando e controllo

ZeroDayRAT Mobile

Spyware commerciale per controllo remoto completo su Android e iOS

La polizia olandese ha arrestato un giovane accusato di distribuire JokerOTP, un bot utilizzato per intercettare codici di autenticazione a due fattori. Si è registrato un aumento delle infezioni da LummaStealer dopo le campagne CastleLoader, evidenziando la resilienza del cybercrime.

Phishing & Social Engineering

01

Phishing adattivo tramite Telegram

Uso di spoofing del dominio mittente e allegati HTML attivi per sottrarre credenziali, con dati inviati a canali Telegram controllati dagli attaccanti

02

Furto di credenziali da Outlook

Add-in di Microsoft Outlook compromesso e trasformato in kit di phishing che ha rubato oltre 4.000 credenziali di account Microsoft

03

Campagne di phishing INPS

Nuove campagne mirate agli utenti INPS veicolate tramite email e SMS per ottenere dati personali e bancari di cittadini italiani

04

Truffe telefoniche evolute

Aumento delle truffe che sfruttano piattaforme SaaS legittime, eludendo i controlli di sicurezza tradizionali

05

Campagne mirate in Germania

Campagna di phishing collegata a stati, mirata a giornalisti e funzionari governativi tedeschi

Tecniche Avanzate Emergenti

- Uso di codici QR per phishing
- Attacchi basati su ClickFix
- Spoofing del dominio mittente
- Esfiltrazione tramite Telegram

Problemi di Sicurezza

- Exchange Online segnala erroneamente email legittime come phishing
- Vulnerabilità delle applicazioni SaaS
- Phishing adattivo in crescita
- Aumento uso di piattaforme di messaggistica

RANSOMWARE

Operazioni Ransomware Active

Negli ultimi sette giorni, il panorama dei ransomware ha visto un'intensificazione delle attività, con diversi attacchi mirati a organizzazioni in Europa, inclusa l'Italia. Le vulnerabilità critiche, in particolare quelle legate a software ampiamente utilizzati, continuano a rappresentare un rischio significativo per le aziende. Inoltre, nuovi gruppi di ransomware emergono, sfruttando tecniche sofisticate per infiltrarsi nei sistemi e rubare dati sensibili.

SpaceBears - Attacco a Siem Srl

Compromissione di Siem Srl con minaccia di divulgare disegni sensibili di aeroporti e fabbriche, oltre a dati finanziari e informazioni personali dei dipendenti

Lynx Ransomware in Espansione

Rapida espansione in Nord America ed Europa, utilizzando tecniche di doppia estorsione supportato da rete crescente di affiliati esperti

BridgePay Network Solutions

Attacco ransomware causando interruzioni sistemiche nei servizi di pagamento, con collaborazione con autorità per risolvere la situazione

Qilin - Pipeline Petrolifera Romania

Furto dati dalla Conpet S.A., gestore della pipeline petrolifera nazionale della Romania, colpendo infrastrutture critiche europee

Nuovi gruppi ransomware emergenti: Bashe (ex APT73) è emerso nel panorama RaaS, mentre il gruppo Crazy ha iniziato a sfruttare strumenti di monitoraggio dei dipendenti per mantenere la persistenza nelle reti aziendali. Il gruppo Warlock ha compromesso SmarterTools sfruttando una vulnerabilità interna.

VULNERABILITÀ

Vulnerabilità Critiche & Patch

1

CVE-2025-53770

SharePoint: Vulnerabilità critica di esecuzione di codice remoto emersa come potenziale vettore per attacchi ransomware. CVSS critico

2

BeyondTrust Critical

Vulnerabilità critica nel software di supporto remoto che potrebbe consentire a attaccanti non autenticati di eseguire codice arbitrario da remoto

3

SolarWinds Web Help Desk

Attori malevoli sfruttano vulnerabilità per ottenere diritti di esecuzione del codice su sistemi esposti, utilizzando strumenti come Velociraptor

4

Patch Tuesday Microsoft

Rilasciati 58 aggiornamenti di sicurezza, di cui 6 zero-day. Vulnerabilità includono Denial of Service e Remote Code Execution

5

Apple Zero-Day

Aggiornamenti per diverse vulnerabilità, inclusa una zero-day che consente l'esecuzione di codice arbitrario. Rischio molto alto

6

Ivanti EPMM

83% degli attacchi recenti sfruttano due vulnerabilità critiche (CVE-2026-21962 e CVE-2026-24061) in Ivanti Endpoint Manager Mobile

Vulnerabilità Aggiuntive e Patch

Microsoft SCCM

CISA segnala vulnerabilità critica nel Configuration Manager, già patchata nel 2024, attivamente sfruttata

WordPress WPvivid

Plugin WPvivid Backup & Migration presenta vulnerabilità critica di RCE, esponendo oltre 900.000 siti web

Juniper Networks

Aggiornamenti di sicurezza per Juniper Secure Analytics, con vulnerabilità critica che richiede attenzione immediata

CVE-2026-26366

eNet SMART HOME: Due vulnerabilità critiche nel server consentono accesso non autorizzato e escalation dei privilegi

CISA KEV Catalog

CISA ha ordinato a tutte le agenzie federali di risolvere dieci nuove vulnerabilità sfruttate entro la prima settimana di marzo

Azione Immediata

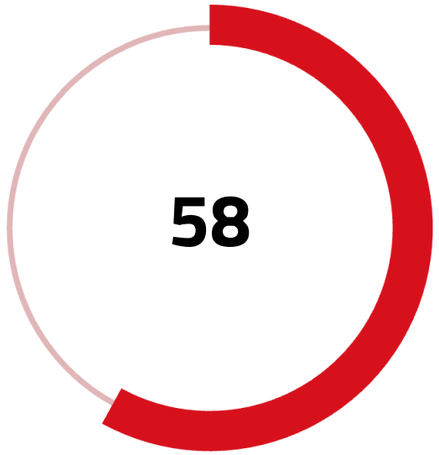
Mantenere aggiornati tutti sistemi, applicare patch tempestivamente, monitorare segnalazioni vulnerabilità attivamente

La settimana ha evidenziato l'importanza di mantenere aggiornati i sistemi e le applicazioni per proteggere le organizzazioni da attacchi informatici. Le vulnerabilità critiche e gli exploit attivi richiedono un'attenzione immediata per garantire la sicurezza delle infrastrutture IT. Gli aggiornamenti di sicurezza sono stati rilasciati da importanti fornitori come Microsoft, Apple, Ivanti e BeyondTrust.

ANALISI

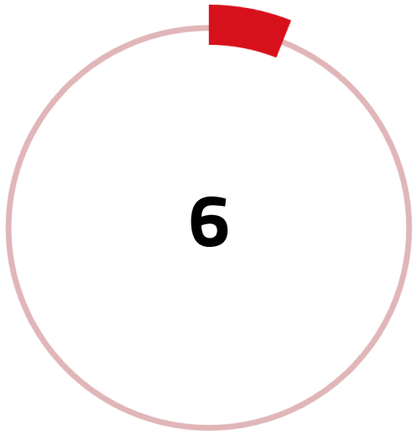
Analisi Trasversale e Tendenze

L'analisi della settimana rivela un incremento significativo delle minacce, con un focus particolare sulle infrastrutture critiche e sulle vulnerabilità software. Le autorità europee hanno sottolineato l'urgenza di rafforzare le difese contro attacchi informatici sempre più sofisticati. Rispetto alle settimane precedenti, si è registrato un aumento delle violazioni di dati e delle tecniche di phishing, con attaccanti che sfruttano metodi sempre più sofisticati, come l'ingegneria sociale e l'abuso di servizi legittimi.



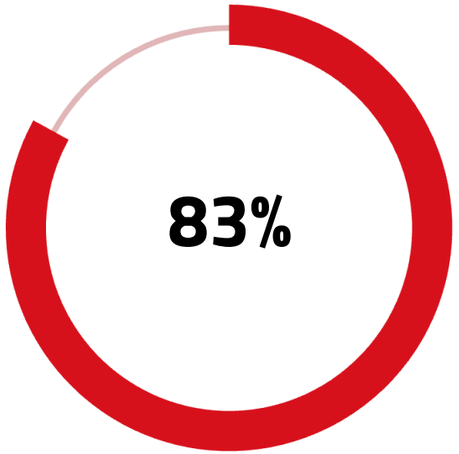
Patch Microsoft

Aggiornamenti di sicurezza rilasciati nel Patch Tuesday



Zero-Day Microsoft

Vulnerabilità zero-day risolte negli aggiornamenti Microsoft



Attacchi Ivanti

Percentuale attacchi attribuiti a un singolo attore malevolo

Tendenze Emergenti

- Aumento minacce alle infrastrutture critiche europee
- Vulnerabilità critiche in BeyondTrust e SharePoint
- Espansione malware su macOS con AMOS e infostealer
- Uso di Telegram per esfiltrazione dati di phishing

Settori più Colpiti

- Fintech: violazione Figure e ShinyHunters
- Telecomunicazioni: attacco Odido 6,2M clienti
- Marchi di lusso: multa 25M dollari per violazioni
- Infrastrutture energetiche: pipeline Romania

FOCUS

CVE-2025-53770 – SharePoint RCE

Descrizione:

Vulnerabilità di Remote Code Execution che consente l'esecuzione di codice arbitrario su server SharePoint vulnerabili.

CVSS:

Critico (RCE con impatto completo su confidenzialità, integrità e disponibilità).

Superficie di Attacco:

- Istanze SharePoint on-premise
- Ambienti ibridi integrati con Active Directory
- Server esposti su Internet

Impatto Tecnico:

- Compromissione completa del server
- Accesso ai documenti interni
- Movimento laterale nella rete
- Possibile distribuzione ransomware

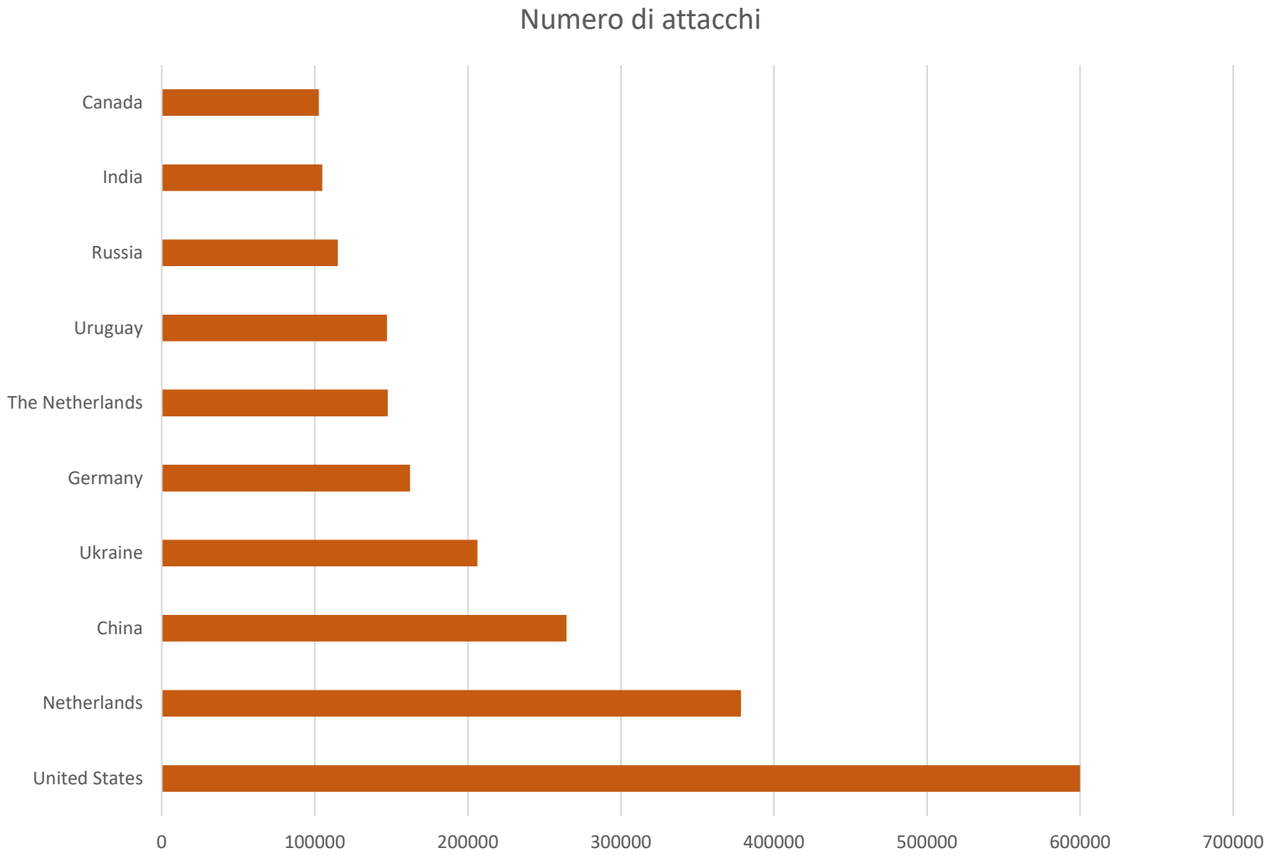
Rischio per la PA:

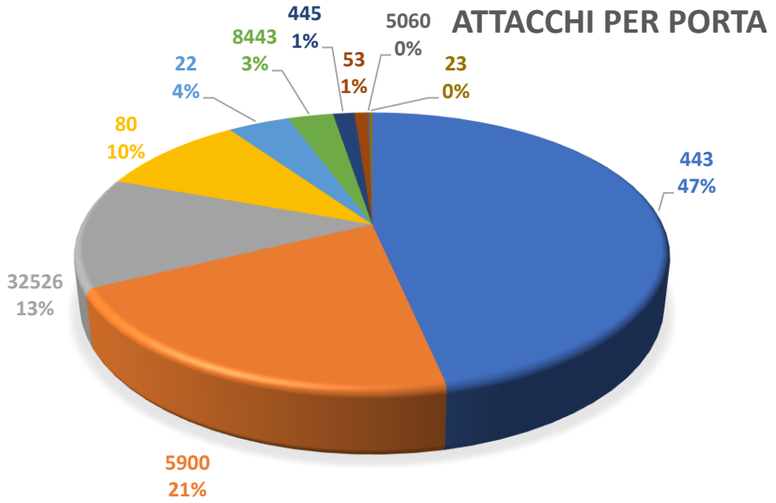
Ampia diffusione di SharePoint negli enti pubblici aumenta il rischio sistemico in caso di ritardo nel patching.

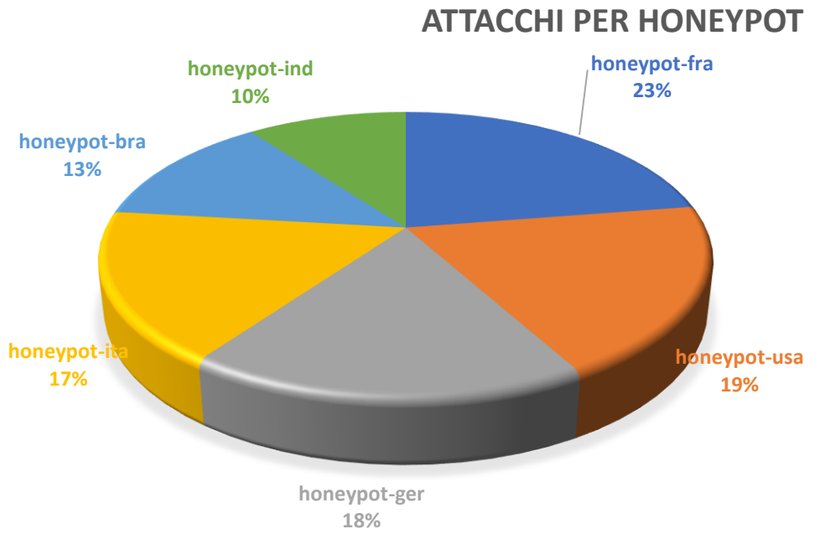
PRIORITÀ OPERATIVA: Verifica immediata versioni installate, applicazione patch di sicurezza e controllo log per indicatori di compromissione.

ANALISI

Honeypot : una panoramica di quanto successo nella settimana 9/2 – 15/02







RACCOMANDAZIONI

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino misure proattive. Il contesto in continua evoluzione delle minacce informatiche richiede particolare attenzione. Solo attraverso un approccio integrato e collaborativo sarà possibile affrontare efficacemente il panorama in continua evoluzione delle minacce informatiche.

01

Patch Management Rigoroso

Implementare programma di patch management rigoroso, assicurando che tutte le vulnerabilità note siano risolte tempestivamente, priorità a BeyondTrust e SharePoint

02

Formazione Continua

Investire in formazione continua per il personale, sensibilizzando i dipendenti sui rischi del phishing e delle truffe online, inclusi attacchi via Telegram

03

Monitoraggio Infrastrutture

Monitorare costantemente le proprie infrastrutture per rilevare attività sospette e rispondere rapidamente a eventuali incidenti, focus su dark web leak

04

Piano Risposta Incidenti

Rafforzare piani di risposta agli incidenti per garantire reazione rapida ed efficace in caso di attacco ransomware o violazione dati

05

Collaborazione con Autorità

Collaborare con le autorità competenti e condividere informazioni sulle minacce per migliorare la resilienza collettiva contro le cyber minacce

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