S3K

Cyber Threat

WEEKLY REPORT

\ week 30/03/2026 - 5/04/2026

www.s3kgroup.it

Vulnerabilità critiche in Cisco e Citrix

Cisco e Citrix hanno rilasciato patch per vulnerabilità critiche che potrebbero consentire accessi non autorizzati, rappresentando un rischio significativo per le organizzazioni italiane.

Attacco agli Uffizi

L'attacco informatico agli Uffizi ha riacceso il dibattito sulla sicurezza delle infrastrutture culturali in Italia, evidenziando la necessità di una maggiore cyber resilienza.

Fuga di dati da portale fiscale italiano

Un database di 85.000 clienti di un portale fiscale italiano è stato trovato in vendita sul dark web, sottolineando vulnerabilità nei sistemi di gestione dei dati sensibili.

Campagna di phishing evoluta

Gli attacchi di phishing hanno visto un aumento significativo, con nuove tecniche che sfruttano codici QR e credenziali OAuth, aumentando il rischio per le aziende.

Attività ransomware in aumento

Gruppi come Qilin e LockBit 5.0 hanno rivendicato attacchi contro organizzazioni europee, inclusi enti italiani, evidenziando la crescente minaccia di multi-estorsione.

Esposizione di istanze F5 BIG-IP

Oltre 14.000 istanze di F5 BIG-IP APM sono state trovate vulnerabili a attacchi di esecuzione di codice remoto, richiedendo un'immediata verifica della sicurezza.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della sicurezza informatica ha visto un incremento significativo delle vulnerabilità e delle minacce, con un focus particolare su attacchi mirati e exploit di sistemi critici. Diverse organizzazioni, tra cui Cisco e Citrix, hanno dovuto affrontare gravi vulnerabilità, mentre le agenzie di sicurezza hanno lanciato avvertimenti su attacchi in corso e campagne di phishing. La situazione è ulteriormente complicata dalla crescente attenzione verso la sicurezza delle infrastrutture culturali, come dimostrato dall'attacco agli Uffizi.

- **Vulnerabilità critiche in Cisco:** Cisco ha rilasciato patch per vulnerabilità critiche, tra cui un bypass di autenticazione nell'Integrated Management Controller (IMC), che consente agli attaccanti di ottenere accesso amministrativo ai sistemi. Bleepingcomputer
- **Attacchi russi su infrastrutture già compromesse:** CERT-UA ha avvertito che i gruppi di hacker russi stanno riesaminando le infrastrutture compromesse in precedenti attacchi per verificare l'accesso e le credenziali valide, indicando preparativi per nuove offensive. Therecord
- **Esposizione remota dell'app-server Codex:** È stata identificata un'esposizione remota non autenticata nell'app-server di Codex, che consente l'esecuzione di comandi senza credenziali, rappresentando un grave rischio per le organizzazioni. CERT-AgID
- **Campagna di furto di credenziali automatizzata:** Talos ha rivelato una campagna di raccolta automatizzata di credenziali, nota come UAT-10608, che sfrutta un framework chiamato "NEXUS Listener". Talosintelligence
- **Vulnerabilità critica in Citrix NetScaler:** CISA ha esortato le agenzie federali a correggere una vulnerabilità critica in Citrix NetScaler classificata con un punteggio di 9.3 su 10, che potrebbe consentire accesso a informazioni sensibili. Therecord
- **Attacco agli Uffizi:** L'attacco informatico agli Uffizi, avvenuto in inverno, ha riacceso il dibattito sulla sicurezza delle istituzioni culturali in Italia, sottolineando l'importanza della cyber resilienza nel patrimonio culturale. Cybersecurity360
- **LinkedIn e la raccolta dati non autorizzata:** Un rapporto ha rivelato che LinkedIn sta scansionando segretamente oltre 6.000 estensioni di Chrome per raccogliere dati sui dispositivi degli utenti, sollevando preoccupazioni sulla privacy. Bleepingcomputer

La settimana ha evidenziato una serie di vulnerabilità critiche e attacchi mirati che potrebbero avere un impatto significativo sulle organizzazioni italiane ed europee. È fondamentale che le aziende rimangano vigili e adottino misure proattive per proteggere le loro infrastrutture e dati sensibili.

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama delle violazioni e delle fughe di dati ha visto eventi significativi che hanno coinvolto diverse organizzazioni, con un impatto potenzialmente grave per utenti e aziende, in particolare in Europa. Le autorità di sicurezza informatica hanno segnalato attacchi mirati da parte di gruppi di hacker, mentre numerosi portali e servizi online hanno subito compromissioni, esponendo dati sensibili di milioni di utenti.

85K

Clienti portale fiscale esposti

Database in vendita sul dark web da un portale fiscale legale italiano.

6.8M

Utenti Crunchyroll colpiti

Violazione con nomi, indirizzi email e dettagli di supporto esposti.

291K

Account SongTrivia2 compromessi

Email e password hash pubblicati su forum di hacking pubblico.

€31.8M

Multa Intesa Sanpaolo

Accessi non autorizzati per due anni sanzionati dal garante italiano per la protezione dei dati.

La settimana del 29/03/2026 – 05/04/2026 ha evidenziato un aumento preoccupante delle violazioni, sottolineando l'importanza di rafforzare le misure di protezione dei dati, con ulteriori incidenti che hanno coinvolto il **Parlamento Europeo** (attribuito al gruppo TeamPCP/ShinyHunters), la piattaforma **Cuties AI** (144.250 email esposte) e la società di telemedicina **Hims & Hers**.

Minacce per Settori Critici: Dettaglio Breach

Istituzioni Europee

CERT-EU ha attribuito un attacco al Parlamento Europeo al gruppo TeamPCP, con ShinyHunters responsabile della fuga di dati online. Potenziali ripercussioni sulla sicurezza delle informazioni istituzionali.

Settore Fiscale Italiano

Un database di 85.000 clienti di un portale fiscale legale italiano scoperto in vendita sul dark web, evidenziando vulnerabilità nei sistemi di gestione dei dati sensibili.

Settore Bancario

Intesa Sanpaolo ha subito accessi non autorizzati per due anni, con una multa di 31,8 milioni di euro da parte dell'autorità italiana per la protezione dei dati.

Streaming & Entertainment

Crunchyroll ha subito una violazione con circa 6,8 milioni di utenti coinvolti. SongTrivia2 ha esposto 291.739 email e password hash su forum di hacking pubblici.

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 professionisti e organizzazioni in tutto il mondo. Diverse campagne di malware, tra cui PXA Stealer e Venom Stealer, hanno messo in evidenza l'evoluzione delle tecniche di furto di dati, mentre attacchi alla supply chain hanno sollevato preoccupazioni sulla sicurezza delle librerie software.

Principali Incidenti e Minacce

1. **Campagna PXA Stealer:** Attori legati al Vietnam hanno lanciato una campagna globale utilizzando PXA Stealer per rubare dati sensibili da professionisti su LinkedIn, con tecniche di ingegneria sociale. 🔗 Thecyberexpress
2. **Attacco alla supply chain di Axios:** Un attacco ha compromesso il pacchetto npm Axios, utilizzato da milioni di sviluppatori, per distribuire malware cross-platform. 🔗 CAN
3. **Malware NoVoice su Google Play:** Un nuovo malware Android, NoVoice, scoperto in oltre 50 app con 2,3 milioni di download, eludendo i controlli di sicurezza su dispositivi obsoleti. 🔗 Bleepingcomputer
4. **Attacco di UNC1069:** Google ha attribuito un attacco supply chain a UNC1069, gruppo nordcoreano con malware basato su macOS risalente al 2023. 🔗 Therecord

Nuovi Malware Identificati

FvncBot su Android

Malware analizzato da CERT Polska che installa un secondo stadio di impianto, forza l'accessibilità e registra i dispositivi su backend per credenziali uniche. 🔗 Cert

Venom Stealer

Nuova piattaforma MaaS che ha ridefinito il cybercrime, rendendo il furto di dati un'attività automatizzata e scalabile per un pubblico più ampio. 🔗 Cybersecurity360

CrystalRAT

Nuovo MaaS promosso su Telegram con funzionalità di accesso remoto, furto di dati e keylogging, aumentando il rischio per le organizzazioni. 🔗 Bleepingcomputer

AVrecon Malware

L'FBI ha avvertito di AVrecon, che prende di mira dispositivi di rete in 163 paesi, compromettendo anche dispositivi comuni. 🔗 Thecyberexpress

Le organizzazioni italiane ed europee devono rimanere vigili e adottare misure proattive per proteggere i propri sistemi e dati da queste minacce in continua evoluzione. La crescente sofisticazione delle tecniche di attacco rende il monitoraggio costante delle infrastrutture digitali un imperativo.

Phishing & Social Engineering

Negli ultimi sette giorni, il panorama del phishing e del social engineering ha mostrato un incremento significativo delle attività malevole, con attacchi sempre più sofisticati e mirati. Le tecniche di phishing si sono evolute, sfruttando nuove modalità come i codici QR e l'abuso di credenziali OAuth, mentre le campagne di smishing e le truffe legate alla stagione fiscale hanno continuato a colpire duramente le vittime.

01

Truffe QR code sul traffico stradale

I truffatori inviano messaggi falsi su violazioni del traffico, spingendo le vittime a scansionare QR code che portano a siti di phishing per rubare informazioni personali e finanziarie.

02

Attacchi phishing con codice dispositivo OAuth 2.0

Gli attacchi che sfruttano il flusso di autorizzazione dei dispositivi OAuth 2.0 sono aumentati di oltre 37 volte quest'anno, rappresentando una minaccia crescente per le aziende.

03

Truffe fiscali in aumento

Durante la stagione fiscale, i criminali informatici utilizzano nuove tattiche di phishing per diffondere malware e rubare credenziali, con focus su truffe legate ai moduli fiscali.

04

Documenti d'identità italiani su Telegram

Un canale Telegram ha rilasciato un archivio con 500 documenti d'identità italiani, esponendo le vittime a rischi di furto d'identità e frodi online. (Fonte: CERT-AgID)

05

Attacchi AiTM e phishing via email compromesse

Le tecniche di phishing utilizzano account compromessi per inviare spam massivo e aggirare l'autenticazione a più fattori.

06

Kit EvilTokens per attacchi a Microsoft

Un kit malevolo chiamato EvilTokens è emerso, consentendo attacchi di phishing mirati a account Microsoft e facilitando frodi via email aziendali (BEC).

07

Phishing contro istituzioni ucraine

Un gruppo di hacker pro-Russi ha impersonato l'agenzia nazionale per la risposta agli incidenti informatici dell'Ucraina, mirando a enti governativi e aziende.

Tecniche Avanzate Emergenti

- Sfruttamento codici QR per redirect a siti di phishing
- Abuso del flusso OAuth 2.0 per furto di token (+37x)
- Attacchi AiTM per bypassare l'autenticazione MFA
- Kit EvilTokens per BEC e account Microsoft

Target Principali

- Utenti soggetti a violazioni del traffico (QR scam)
- Contribuenti durante la stagione fiscale
- Titolari di documenti d'identità italiani
- Istituzioni governative ucraine e aziende europee

RANSOMWARE

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama delle minacce ransomware ha mostrato un'attività intensa, con diversi gruppi che hanno rivendicato attacchi contro organizzazioni in Europa e negli Stati Uniti. I gruppi di ransomware come Qilin e Nova hanno continuato a colpire, mentre nuove tendenze come la multi-estorsione stanno guadagnando terreno. Le organizzazioni italiane devono rimanere vigili, poiché i bersagli includono sia enti pubblici che privati.

Attacco a Die Linke (Qilin)
Il partito politico tedesco Die Linke ha confermato un attacco da parte del gruppo Qilin, causando interruzioni IT e minacce di divulgazione di dati sensibili, evidenziando il rischio per le istituzioni politiche europee.

Multi-estorsione in aumento
I gruppi di ransomware stanno adottando strategie di multi-estorsione, utilizzando dati rubati per esercitare pressioni sulle vittime attraverso minacce di pubblicazione, aumentando il rischio per le organizzazioni con dati sensibili.

LockBit 5.0: vittime italiane
LockBit 5.0 ha aggiunto diverse nuove vittime al suo sito di leak, tra cui aziende italiane come Defcon 5 S.r.l e Consorzio Selenia, confermando la minaccia per le organizzazioni in Europa.

Attacco a Gaposa (thegentlemen)
Il gruppo thegentlemen ha rivendicato un attacco contro Gaposa, sottolineando la vulnerabilità delle aziende italiane, in particolare nel settore tecnologico.

Attacco a GEG-Telecomunicazioni
Il gruppo netrunner ha rivendicato un attacco contro GEG-Telecomunicazioni, evidenziando il rischio per le aziende di telecomunicazioni in Italia.

Attacco a irpea.it (incransom)
Il gruppo incransom ha rivendicato un attacco contro il sito irpea.it, mettendo in luce la vulnerabilità delle organizzazioni pubbliche e private in Italia.

Leak Bazaar: nuovo servizio di monetizzazione
È emerso Leak Bazaar, un nuovo servizio che si propone di monetizzare i dati rubati dai gruppi di ransomware, suggerendo un'evoluzione nel modo in cui i dati compromessi vengono gestiti e venduti.

Ransomware e AI: Google Drive
Google ha annunciato che la sua funzione di rilevamento ransomware su Google Drive è ora attiva per tutti gli utenti paganti, un passo importante per migliorare la sicurezza dei dati.

29/03/2026 – 05/04/2026

VULNERABILITÀ

Vulnerabilità Critiche & Patch

Negli ultimi sette giorni, il panorama delle vulnerabilità e delle patch ha visto un'intensa attività, con diverse scoperte di vulnerabilità critiche e exploit attivi. Organizzazioni e aziende sono state avvisate di aggiornamenti urgenti per mitigare i rischi associati a vulnerabilità già sfruttate in attacchi reali. È fondamentale che le organizzazioni italiane ed europee prestino attenzione a queste segnalazioni per proteggere i propri sistemi.

1

CVE-2026-35616 – FortiClient EMS

Fortinet ha rilasciato un aggiornamento di emergenza per questa vulnerabilità critica attivamente sfruttata in rete, che consente esecuzione di codice arbitrario e elevazione dei privilegi. Patch immediata essenziale. CSIRT Italia

2

CVE-2025-55182 – React2Shell / Next.js

Un'ampia campagna ha sfruttato questa vulnerabilità in applicazioni Next.js per rubare credenziali in modo automatizzato. Le organizzazioni devono verificare la loro esposizione. Bleepingcomputer

3

CVE-2026-3055 – Citrix NetScaler

Vulnerabilità critica attivamente sfruttata per ottenere dati sensibili. Le aziende che utilizzano questi dispositivi devono aggiornare urgentemente il software. Bleepingcomputer

4

F5 BIG-IP APM – RCE Exposure

Oltre 14.000 istanze di F5 BIG-IP APM esposte ad attacchi di esecuzione di codice remoto (RCE). Fondamentale verificare la sicurezza delle configurazioni. Bleepingcomputer

5

CVE-2026-33309 – Langflow PoC disponibile

È stato reso disponibile un Proof of Concept per questa vulnerabilità nel LocalStorageService di Langflow, che consente la scrittura arbitraria di file. Applicare le mitigazioni disponibili. CSIRT Italia

6

Aggiornamenti di sicurezza Cisco

Cisco ha rilasciato aggiornamenti per diverse vulnerabilità, di cui due classificate come critiche, riguardanti l'esecuzione di codice remoto e l'elevazione dei privilegi. Aggiornare i sistemi il prima possibile. CSIRT Italia

7

CVE-2026-3502 – TrueConf Client

Rilevata attività di sfruttamento di questa vulnerabilità nel TrueConf Client, che consente l'esecuzione di codice arbitrario. Le organizzazioni devono aggiornare il software per mitigare il rischio. CSIRT Italia

Vulnerabilità Aggiuntive e Patch

CVE-2026-35616 – FortiClient EMS

Esecuzione di codice arbitrario ed elevazione dei privilegi. Sfruttamento attivo in rete confermato. Patch di emergenza rilasciata da Fortinet, applicazione immediata necessaria.

CVE-2025-55182 – Next.js / React2Shell

Furto automatizzato di credenziali tramite campagna massiva. Le organizzazioni che utilizzano Next.js devono verificare l'esposizione e applicare le patch disponibili.

CVE-2026-3055 – Citrix NetScaler

Sfruttamento attivo confermato per accesso a dati sensibili. Aggiornamento software urgente richiesto per tutti i dispositivi NetScaler in produzione.

F5 BIG-IP APM – RCE

14.000+ istanze esposte ad attacchi RCE. Verifica immediata della sicurezza delle configurazioni e applicazione delle patch necessaria.

CVE-2026-33309 – Langflow

PoC pubblicamente disponibile per scrittura arbitraria di file nel LocalStorageService. Applicare le mitigazioni CSIRT Italia immediatamente.

Cisco – Vulnerabilità Critiche

Due vulnerabilità critiche per RCE e elevazione dei privilegi. Aggiornamento urgente per tutti i prodotti Cisco in uso nelle organizzazioni.

CVE-2026-3502 – TrueConf Client

Sfruttamento attivo rilevato per esecuzione di codice arbitrario. Aggiornamento software necessario per mitigare il rischio per le organizzazioni.

La settimana ha evidenziato la necessità di un'attenzione costante alle vulnerabilità critiche e agli aggiornamenti di sicurezza. Le organizzazioni devono adottare misure proattive applicando tempestivamente le patch e monitorando le segnalazioni di exploit attivi.

Analisi Generale e Tendenze

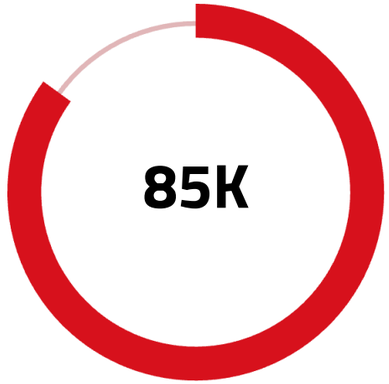
Negli ultimi sette giorni, il panorama della sicurezza informatica ha mostrato un incremento allarmante delle vulnerabilità e delle minacce, con un focus particolare su attacchi mirati e exploit di sistemi critici. Le organizzazioni italiane ed europee sono state colpite da una serie di attacchi, tra cui violazioni di dati e ransomware, evidenziando un trend comune di sofisticazione nelle tecniche di attacco. Rispetto alle settimane precedenti, si osserva un aumento della multi-estorsione e un uso crescente di malware come servizio, che rendono il furto di dati più accessibile a un pubblico più ampio.

La crescente attenzione verso la sicurezza delle infrastrutture culturali, come dimostrato dall'attacco agli Uffizi, sottolinea l'importanza di proteggere anche il patrimonio culturale. Le vulnerabilità critiche scoperte in Cisco e Citrix, attivamente sfruttate, richiedono aggiornamenti urgenti. L'esposizione di oltre 14.000 istanze F5 BIG-IP e la compromissione del pacchetto npm Axios evidenziano la vulnerabilità della supply chain e delle infrastrutture digitali.

Tendenze chiave: crescente uso del malware-as-a-service, adozione massiva di tecniche multi-estorsione, aumento degli attacchi QR e OAuth nel phishing, e intensificazione degli attacchi ransomware contro enti italiani pubblici e privati.

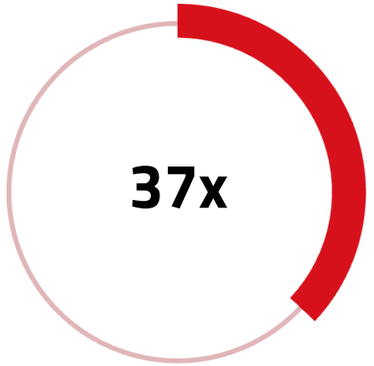
Istanze F5 BIG-IP vulnerabili

Esposte ad attacchi RCE, richiedendo verifica immediata della sicurezza



Clienti esposti sul dark web

Dati di clienti di portale fiscale italiano trovati in vendita



Aumento attacchi OAuth

Gli attacchi phishing via device code OAuth 2.0 sono aumentati di oltre 37 volte quest'anno

Tendenze Emergenti

- Multi-estorsione ransomware (Qilin, LockBit 5.0)
- Malware-as-a-Service in espansione (Venom Stealer, CrystalRAT)
- Phishing con QR code e abuso OAuth 2.0
- Attacchi supply chain (npm Axios, UNC1069)

Settori più Colpiti

- Patrimonio culturale e istituzioni pubbliche
- Settore bancario e finanziario (Intesa Sanpaolo)
- Telecomunicazioni e infrastrutture IT italiane
- Istituzioni politiche ed europee

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino misure proattive e strategie di sicurezza robuste. Il contesto in continua evoluzione delle minacce richiede particolare attenzione su più fronti.

Priorità immediate:

- Applicare immediatamente la patch di emergenza Fortinet per CVE-2026-35616 (FortiClient EMS), attivamente sfruttata in rete con esecuzione di codice arbitrario.
- Aggiornare urgentemente Citrix NetScaler (CVE-2026-3055) e TrueConf Client (CVE-2026-3502), entrambi con sfruttamento attivo confermato.
- Verificare e mettere in sicurezza tutte le istanze F5 BIG-IP APM esposte ad attacchi RCE: oltre 14.000 istanze risultano vulnerabili.
- Applicare le patch Cisco per le due vulnerabilità critiche RCE e testare le mitigazioni per Langflow (CVE-2026-33309, PoC disponibile pubblicamente).

Misure di sicurezza strutturali:

- Implementare un programma di patch management efficace, assicurandosi che tutte le vulnerabilità critiche vengano corrette tempestivamente.
- Investire in formazione continua per i dipendenti, sensibilizzandoli sulle tecniche di phishing con QR code, OAuth e social engineering in continua evoluzione.
- Monitorare costantemente le proprie infrastrutture per rilevare attività sospette, con particolare attenzione alla supply chain software (pacchetti npm e librerie open-source).
- Adottare soluzioni di rilevamento ransomware avanzate e definire un piano di risposta agli incidenti ben strutturato per minimizzare i danni potenziali in caso di attacco.
- Monitorare il dark web per rilevare esposizioni di dati aziendali e credenziali, considerando i recenti leak di portali fiscali italiani e database di clienti.

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