S3K

Cyber Threat

WEEKLY REPORT

\ week 16/03/2026 - 22/03/2026

www.s3kgroup.it

CTI WEEKLY

Aumento delle vulnerabilità critiche

Oltre 1.600 vulnerabilità registrate, con 24 difetti critici nei sistemi ICS, aumentando il rischio per le organizzazioni italiane ed europee.

Attacchi da gruppi sponsorizzati da stati

Il Lazarus Group ha colpito piattaforme crittografiche, sfruttando tecniche avanzate per il furto di ingenti somme di denaro.

Fughe di dati significative

Navia ha subito una violazione che ha coinvolto 2,7 milioni di persone, mentre diverse piattaforme italiane hanno registrato accessi non autorizzati.

Nuove campagne di malware

Emerso VoidStealer, un malware per Chrome che bypassa la crittografia estraendo la chiave master, aumentando i rischi per gli utenti.

Attività di phishing in aumento

Registrate 103 campagne di phishing, molte delle quali mirate a istituzioni italiane come l'Agenzia delle Entrate.

Vulnerabilità zero-day sfruttate

Il gruppo Interlock ha sfruttato una vulnerabilità critica nei firewall Cisco, evidenziando la necessità di aggiornamenti tempestivi.

Notizie cyber della Settimana

Negli ultimi sette giorni, il panorama della cybersecurity ha visto un incremento significativo delle vulnerabilità e delle minacce, con particolare attenzione a operazioni di attacco sponsorizzate da stati e a nuove tecniche di sfruttamento. Le autorità europee hanno intensificato le misure di sicurezza, mentre le organizzazioni devono affrontare un panorama in continua evoluzione, caratterizzato da attacchi mirati e sfruttamento di vulnerabilità critiche.

- **Aumento delle vulnerabilità:** Cyble ha registrato 1.641 vulnerabilità e 24 difetti critici nei sistemi ICS, con 175 Proof of Concepts (PoC) disponibili, aumentando il rischio per le aziende europee. 🔗 Cyble
- **Attacchi di Lazarus Group:** Il gruppo di hacker nordcoreano ha attaccato Bitrefill, evidenziando come sfruttino le piattaforme crittografiche e gli errori umani per rubare ingenti somme di denaro. 🔗 Cyble
- **Sanzioni europee contro attacchi informatici:** L'Unione Europea ha imposto sanzioni a tre entità e due individui per attacchi informatici contro infrastrutture critiche, sottolineando l'impegno a proteggere la sicurezza regionale. 🔗 Bleepingcomputer
- **Nuove norme di cybersecurity per infrastrutture idriche:** Gli Stati Uniti hanno introdotto nuovi standard di cybersecurity per i sistemi idrici, evidenziando che le minacce non si limitano più solo a reti energetiche e finanziarie. 🔗 Thecyberexpress
- **Operazione Alice:** Le forze di polizia internazionali hanno smantellato una rete di oltre 373.000 siti web fraudolenti sul dark web, utilizzati per traffico di contenuti di abuso sessuale infantile. 🔗 Bleepingcomputer
- **Attacco a Stryker:** Il Dipartimento di Giustizia degli Stati Uniti ha accusato il governo iraniano di operare un gruppo hacktivista responsabile di un attacco distruttivo contro Stryker. 🔗 Techcrunch
- **Aggiornamenti su Microsoft Intune:** CISA ha avvertito le organizzazioni statunitensi di rafforzare i sistemi Microsoft Intune dopo un attacco che ha compromesso i sistemi di Stryker. 🔗 Bleepingcomputer
- **Modifiche al Cybersecurity Act e NIS2:** L'EDPB e l'EDPS hanno approvato modifiche al Cybersecurity Act e alla Direttiva NIS2, richiamando l'importanza di rispettare i principi del GDPR. 🔗 Cybersecurity360

La settimana ha evidenziato un aumento delle vulnerabilità e delle minacce informatiche, con un focus su attacchi sponsorizzati da stati e su misure di sicurezza rafforzate a livello europeo.

Supply chain sotto attacco: compromissione repository GitHub

Campagna GlassWorm

Oltre 400 repository GitHub compromessi con inserimento di codice malevolo in estensioni e librerie open-source.

Target principali

Sviluppatori e aziende che riutilizzano codice open-source nelle proprie pipeline di sviluppo.

Trend in crescita

Aumento significativo degli attacchi di tipo supply chain e dependency poisoning nel panorama delle minacce.

Impatto operativo

Compromissione silente di ambienti aziendali con difficile individuazione, trattandosi di sorgenti considerate affidabili.

Insight CTI

- La fiducia nel codice open-source diventa vettore di attacco
- Diffusione indiretta su larga scala tramite dipendenze software
- Difficile rilevamento: il codice malevolo proviene da fonti trusted
- Monitorare le dipendenze software e adottare strumenti di Software Composition Analysis (SCA)

Verificare tutte le dipendenze open-source utilizzate nei progetti aziendali. Implementare controlli di integrità (hash, firma digitale) e adottare soluzioni SCA per rilevare componenti compromessi prima dell'integrazione in produzione.

Lazarus Group colpisce le piattaforme crittografiche: la minaccia nordcoreana

Il Lazarus Group, gruppo di hacker sponsorizzato dalla Corea del Nord, ha intensificato le proprie operazioni contro le piattaforme crittografiche, colpendo Bitrefill e sfruttando errori umani e tecniche avanzate per sottrarre ingenti somme di denaro digitale. Parallelamente, l'UE ha imposto sanzioni a entità responsabili di attacchi alle infrastrutture critiche, segnalando un cambio di passo nella risposta europea alle minacce cyber.

Attacco a Bitrefill

Il Lazarus Group ha compromesso la piattaforma crittografica Bitrefill sfruttando errori umani e tecniche avanzate, con l'obiettivo di sottrarre fondi digitali significativi.

Sanzioni UE contro cyber-attaccanti

L'Unione Europea ha sanzionato tre entità e due individui responsabili di attacchi a infrastrutture critiche europee, rafforzando la postura difensiva regionale.

Attacco a Stryker da parte di Handala

Il gruppo hacktivista Handala, ricollegabile all'intelligence iraniana, ha condotto un attacco distruttivo contro Stryker, azienda di tecnologia medica. L'obiettivo era la distruzione dei dati, non l'estorsione finanziaria.

Cybersecurity Act e NIS2 aggiornati

EDPB ed EDPS hanno approvato modifiche al Cybersecurity Act e alla Direttiva NIS2, integrando i principi del GDPR nella raccolta e condivisione delle informazioni sulle minacce.

Obiettivi prioritari identificati

- Piattaforme crittografiche e exchange di criptovalute
- Aziende di tecnologia medica e sanitaria
- Infrastrutture critiche: sistemi idrici, energetici e finanziari
- Sistemi con scarsa igiene informatica (patch mancanti, credenziali deboli)

Aggiornare tempestivamente le patch, rafforzare la gestione degli endpoint Microsoft Intune e formare il personale sulle tecniche di social engineering utilizzate dal Lazarus Group. La cooperazione internazionale resta fondamentale per rispondere a minacce sponsorizzate da stati.

Data Leak & Breach: Scenario Settimanale

Negli ultimi sette giorni, il panorama dei data leak ha mostrato un'attività intensa, con numerosi incidenti che coinvolgono organizzazioni italiane ed europee. Le informazioni trapelate includono credenziali di accesso, dati personali e informazioni sensibili di milioni di individui.

2.7M

Persone colpite da Navia

Navia Benefit Solutions ha confermato una violazione con esposizione di informazioni sensibili di circa 2,7 milioni di individui.

900K

Record Aura compromessi

Aura ha rivelato che un accesso non autorizzato ha compromesso quasi 900.000 record di clienti, inclusi nomi e indirizzi email.

670K

Persone colpite da Marquis

Marquis ha dichiarato che oltre 670.000 persone sono state colpite da una violazione avvenuta ad agosto, con implicazioni per 74 banche.

2.5K+

Documenti italiani in vendita

Su bdfclub.com sono stati segnalati database con oltre 2.500 set di documenti personali italiani in vendita sul mercato underground.

In aggiunta, il gruppo Handala ha annunciato la prossima pubblicazione di mappe delle infrastrutture **elettriche e idriche**, aumentando le preoccupazioni per la sicurezza nazionale. L'*FBI ha chiuso* diversi siti di leak legati all'intelligence iraniana, inclusi quelli utilizzati da Handala. La settimana del 15/03/2026 – 22/03/2026 ha evidenziato un aumento preoccupante delle violazioni, sottolineando l'importanza di rafforzare le misure di protezione dei dati.

Minacce per Settori Critici: Dettaglio Breach

Settore Benefit & HR

Navia Benefit Solutions ha subito una violazione che ha coinvolto circa 2,7 milioni di persone, con esposizione di informazioni personali sensibili. Una delle violazioni più significative della settimana.

Settore Finanziario

Marquis ha rivelato che una violazione avvenuta ad agosto ha colpito oltre 670.000 individui, con impatti sulle operazioni di 74 banche negli Stati Uniti. Aura ha esposto quasi 900.000 record di clienti.

Piattaforme italiane colpite

Diverse piattaforme italiane, tra cui loshermanositalianos.com e corsofrancia.it, hanno subito fughe di dati con accessi non autorizzati a credenziali di amministratori. Su bdfclub.com segnalate vendite di oltre 2.500 set di documenti italiani.

Infrastrutture critiche & Dark Web

Il gruppo Handala ha annunciato la pubblicazione di mappe di infrastrutture elettriche e idriche. Numerose fughe di dati relative a servizi IPTV sono state rilevate su canali di leak underground.

Malware & Infrastructure

Negli ultimi sette giorni, il panorama del malware e delle infrastrutture ha visto un'intensificazione delle attività malevole, con nuove tecniche di attacco e campagne mirate a rubare dati sensibili. Diverse vulnerabilità sono state sfruttate, in particolare nei dispositivi mobili e nelle piattaforme di gestione degli endpoint. Le autorità internazionali hanno anche compiuto significativi passi avanti nel contrastare botnet e attacchi DDoS.

Principali Incidenti e Minacce

1. **VoidStealer – Nuovo malware per Chrome:** Utilizza un approccio innovativo per bypassare la crittografia di Chrome, estraendo la chiave master per decrittografare dati sensibili degli utenti.
2. **Exploit DarkSword per iPhone:** Gli hacker russi hanno sviluppato un exploit per iPhone che consente di accedere a dati sensibili con scarsa interazione dell'utente, cancellando le tracce dell'intrusione.
3. **SEO poisoning e client VPN falsi:** Campagna malevola che sfrutta il SEO poisoning per indirizzare le vittime verso siti con client VPN falsi contenenti infostealer per credenziali aziendali.
4. **Disruptione di botnet DDoS:** Autorità statunitensi, tedesche e canadesi hanno collaborato per smantellare l'infrastruttura delle botnet Aisuru e KimWolf, utilizzate per attacchi DDoS.

Nuovi Malware e Tecniche Identificati

VoidStealer

Malware per Chrome che bypassa la crittografia del browser estraendo la chiave master, rappresentando un rischio critico per utenti aziendali.

DarkSword (iPhone exploit)

Exploit russo per iOS con capacità di zero/low-interaction e auto-cancellazione delle tracce, particolarmente pericoloso in contesti geopolitici tesi.

GlassWorm (Supply Chain)

Campagna di supply-chain che ha compromesso oltre 400 repository su GitHub tramite estensioni malevole, evidenziando i rischi del software open-source.

Malware Android (Streaming)

Nuove varianti di malware Android nascoste in app di streaming, progettate per rubare password e informazioni bancarie degli utenti.

La compromissione di piattaforme di Endpoint Management come Microsoft Intune tramite funzionalità legittime per la cancellazione massiva di dati rappresenta un'evoluzione preoccupante nelle tecniche di attacco, priva di malware tradizionale e quindi più difficile da rilevare.

Phishing & Social Engineering

Negli ultimi sette giorni, il CERT-AGID ha registrato 103 campagne di phishing, di cui 66 specificamente dirette verso obiettivi italiani. Le tecniche di phishing si sono evolute, con l'uso di loghi ufficiali e meccanismi sofisticati per ingannare le vittime, evidenziando la necessità di una vigilanza costante da parte delle organizzazioni.

01

Phishing Agenzia delle Entrate

Due campagne mirate a rubare credenziali e informazioni personali, con pagine fraudolente che imitano il portale ufficiale. IoC condivisi con le organizzazioni accreditate.

02

Attacco a Intuitive (robot da Vinci)

Il produttore del robot chirurgico da Vinci ha subito un attacco di phishing mirato con furto di dati di chirurghi e amministratori ospedalieri. Nessun impatto sui sistemi chirurgici.

03

Phishing assistito da AI

Campagne che sfruttano le autorizzazioni del browser per raccogliere dati sensibili, incluse immagini delle vittime. Nuova frontiera nel phishing difficilmente rilevabile.

04

Abuso avvisi Microsoft Azure

Gli avvisi di monitoraggio di Microsoft Azure sono stati sfruttati per inviare email di phishing spacciate per avvisi di sicurezza su presunti addebiti non autorizzati.

05

Attacchi a Signal e WhatsApp

L'FBI ha avvertito che attori legati all'intelligence russa stanno attivamente prendendo di mira utenti di app di messaggistica crittografate, compromettendo migliaia di account.

06

Smishing – Triadi cinesi

Analizzate triadi di smishing cinesi che utilizzano tecniche avanzate per ingannare le vittime, evidenziando l'importanza di una consapevolezza continua tra gli utenti.

07

Wallet drainer per sviluppatori

Attaccanti sfruttano l'infrastruttura di notifiche di GitHub per attirare sviluppatori verso pagine fraudolente, dove i loro portafogli crypto vengono immediatamente svuotati.

Tecniche Avanzate Emergenti

- Phishing assistito da intelligenza artificiale con raccolta biometrica
- Abuso di piattaforme legittime (Azure, GitHub)
- Smishing con tecniche di triadi cinesi
- Compromissione di app di messaggistica crittografata

Target Principali Italiani

- Utenti dell'Agenzia delle Entrate
- Personale sanitario e ospedaliero
- Sviluppatori su piattaforme GitHub
- Utenti di Signal e WhatsApp in ambito professionale

Operazioni Ransomware Attive

Negli ultimi sette giorni, il panorama dei ransomware ha visto un aumento significativo delle attività malevole, con gruppi di attacco che sfruttano vulnerabilità critiche e tecniche innovative. Il gruppo Interlock ha sfruttato una vulnerabilità zero-day nei firewall Cisco, mentre LeakNet, Medusa e Qilin hanno continuato a colpire diverse organizzazioni.

Interlock sfrutta zero-day Cisco
Il gruppo Interlock ha approfittato di CVE-2026-20131 nei firewall Cisco prima della sua divulgazione pubblica, eseguendo attacchi zero-day dal gennaio 2026. Implicazioni significative per le organizzazioni che utilizzano tali dispositivi.

LeakNet adotta tecniche stealth
Il gruppo LeakNet ha iniziato a utilizzare la tecnica ClickFix per ottenere accesso iniziale alle reti aziendali, combinandola con un loader malware basato su Deno, aumentando la difficoltà di rilevamento.

Attacco ransomware a Foster City
La città di Foster City ha segnalato un attacco ransomware con possibile compromissione di dati pubblici. Le autorità hanno esortato i cittadini a cambiare le proprie password per proteggere le informazioni personali.

Medusa colpisce il sistema sanitario
Il gruppo Medusa ha rivendicato un attacco contro il University of Mississippi Medical Center, esfiltrando un terabyte di dati e causando un'interruzione significativa nei servizi sanitari.

Marquis – Furto di dati massivo
Il fornitore di servizi finanziari Marquis ha rivelato che un attacco ransomware ha compromesso i dati di oltre 670.000 individui, influenzando anche le operazioni di 74 banche negli Stati Uniti.

Qilin rivela nuove vittime
Il gruppo Qilin ha pubblicato una serie di nuove vittime, tra cui J-E-Culp-Transport e Marc Dorcel, evidenziando la continua espansione delle loro operazioni.

Strumenti quotidiani come vettori
Un rapporto ha evidenziato come gli attaccanti stiano utilizzando strumenti di uso comune per il furto di dati, rendendo le tradizionali misure di rilevamento meno efficaci e richiedendo maggiore attenzione ai segnali comportamentali.

Vulnerabilità Aggiuntive e Patch

CVE-2026-1731 – BeyondTrust

RCE pre-autenticazione in BeyondTrust Remote Support. Aggiornare immediatamente per proteggere le sessioni di supporto remoto e prevenire compromissioni dei sistemi.

CVE-2026-21992 – Oracle Identity Manager

Vulnerabilità critica con aggiornamento di emergenza rilasciato da Oracle. Impatto su sistemi di gestione delle identità aziendali. Patch immediata raccomandata.

CVE-2025-32434 – PyTorch

PoC pubblico disponibile per esecuzione di codice arbitrario in PyTorch. Aggiornamento urgente per tutte le organizzazioni che utilizzano questa libreria AI/ML.

CVE-2026-20643 – Apple WebKit

Vulnerabilità critica in WebKit che interessa iOS e macOS. Aggiornare tutti i dispositivi Apple per mitigare il rischio di sfruttamento attivo.

CVE-2025-66376 – Zimbra

Sfruttamento attivo confermato. Applicare le patch disponibili per Zimbra Collaboration Suite per proteggere i sistemi di posta e collaborazione aziendali.

CVE-2026-32746 – GNU Inetutils

RCE nel demone telnetd. Migrare a SSH per tutte le istanze esposte e applicare le patch disponibili per GNU Inetutils.

CVE-2026-33293 – WWBN AVideo

Arbitrary File Deletion tramite path traversal. Aggiornare alla versione 26.0 di AVideo per risolvere la vulnerabilità.

CVE-2026-32828 – Kargo SSRF

Server-Side Request Forgery in Kargo consente accesso a dati sensibili. Aggiornare il software per prevenire esfiltrazioni di dati non autorizzate.

La settimana ha evidenziato un numero elevato di vulnerabilità critiche e PoC attivi. È essenziale che le organizzazioni italiane ed europee adottino misure proattive per proteggere i propri sistemi, applicando tempestivamente le patch e monitorando le reti per attività sospette.

Analisi Trasversale e Tendenze

Negli ultimi sette giorni, il panorama della cybersecurity ha mostrato un incremento allarmante delle vulnerabilità e delle minacce informatiche. Le operazioni di attacco sponsorizzate da stati, come quelle attribuite al gruppo Lazarus, e le nuove tecniche di malware, come VoidStealer e DarkSword, hanno messo in luce la crescente sofisticazione degli attaccanti. L'aumento delle fughe di dati, con eventi significativi come la violazione di Navia (2,7M persone) e Marquis (670K individui) — ha reso evidente la vulnerabilità delle organizzazioni italiane ed europee. Le recenti sanzioni UE e le nuove normative indicano un impegno crescente nella protezione delle infrastrutture critiche.

Le campagne di phishing, con 103 casi settimanali di cui 66 mirati all'Italia, e l'emergere di ransomware come Interlock (che sfrutta zero-day Cisco) e Medusa (con 1TB di dati esfiltrati dal settore sanitario), confermano un trend di attacchi sempre più mirati e tempestivi. La proliferazione di PoC pubblici per vulnerabilità critiche riduce drasticamente il tempo a disposizione delle organizzazioni per applicare le patch.

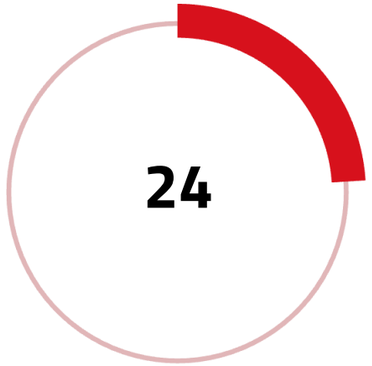
Tendenze chiave: sfruttamento zero-day prima della divulgazione pubblica, attacchi a infrastrutture sanitarie e finanziarie, phishing evoluto con supporto AI, e operazioni state-sponsored con obiettivi distruttivi piuttosto che estorsivi.

Campagne Malevole

Identificate nella settimana (15/03/2026 – 22/03/2026), di cui 66 dirette a obiettivi italiani

Vulnerabilità Registrate

Segnalazioni totali rilevate da Cyble, con 24 difetti critici nei sistemi ICS e 175 PoC disponibili



Difetti Critici ICS

Vulnerabilità critiche identificate nei sistemi di controllo industriale nei settori energia e produzione

Tendenze Emergenti

- Sfruttamento zero-day pre-divulgazione (es. Cisco CVE-2026-20131)
- Phishing con supporto AI e raccolta biometrica
- Attacchi distruttivi sponsorizzati da stati (Handala, Lazarus)
- Supply chain attacks su repository open-source (GlassWorm)

Settori più Colpiti

- Sanità e Servizi Medici (Medusa, Intuitive)
- Settore finanziario e bancario (Marquis, Aura)
- Piattaforme crittografiche (Lazarus Group)
- Infrastrutture critiche (Cisco, sistemi idrici ed elettrici)

Raccomandazioni Operative Prioritarie

Per affrontare le sfide della settimana, è fondamentale che le organizzazioni adottino un approccio proattivo alla sicurezza informatica. Il contesto in continua evoluzione delle minacce richiede particolare attenzione su più fronti.

Priorità immediate:

- Applicare immediatamente le patch critiche per CVE-2026-1731 (BeyondTrust), CVE-2026-21992 (Oracle Identity Manager), CVE-2025-32434 (PyTorch) e CVE-2026-20643 (Apple WebKit).
- Aggiornare i sistemi Zimbra Collaboration Suite per mitigare lo sfruttamento attivo di CVE-2025-66376, e migrare da telnetd a SSH per GNU Inetutils (CVE-2026-32746).
- Verificare e aggiornare i firewall Cisco per mitigare la vulnerabilità zero-day CVE-2026-20131 sfruttata dal gruppo Interlock.

Misure di sicurezza strutturali:

- Investire in programmi di formazione per sensibilizzare i dipendenti sui rischi del phishing (103 campagne settimanali, 66 italiane), in particolare riguardo alle campagne che imitano l'Agenzia delle Entrate.
- Implementare l'autenticazione a più fattori per proteggere le credenziali aziendali, in particolare per piattaforme Microsoft e sistemi di messaggistica aziendale.
- Monitorare attivamente il dark web per rilevare esposizioni di dati aziendali e credenziali, in particolare su bdfclub.com e canali di leak IPTV.
- Verificare l'integrità di repository GitHub e pacchetti open-source per prevenire attacchi supply chain come GlassWorm.
- Rafforzare la gestione degli endpoint con Microsoft Intune e proteggere i sistemi dall'uso improprio di funzionalità legittime per la cancellazione massiva dei dati.

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