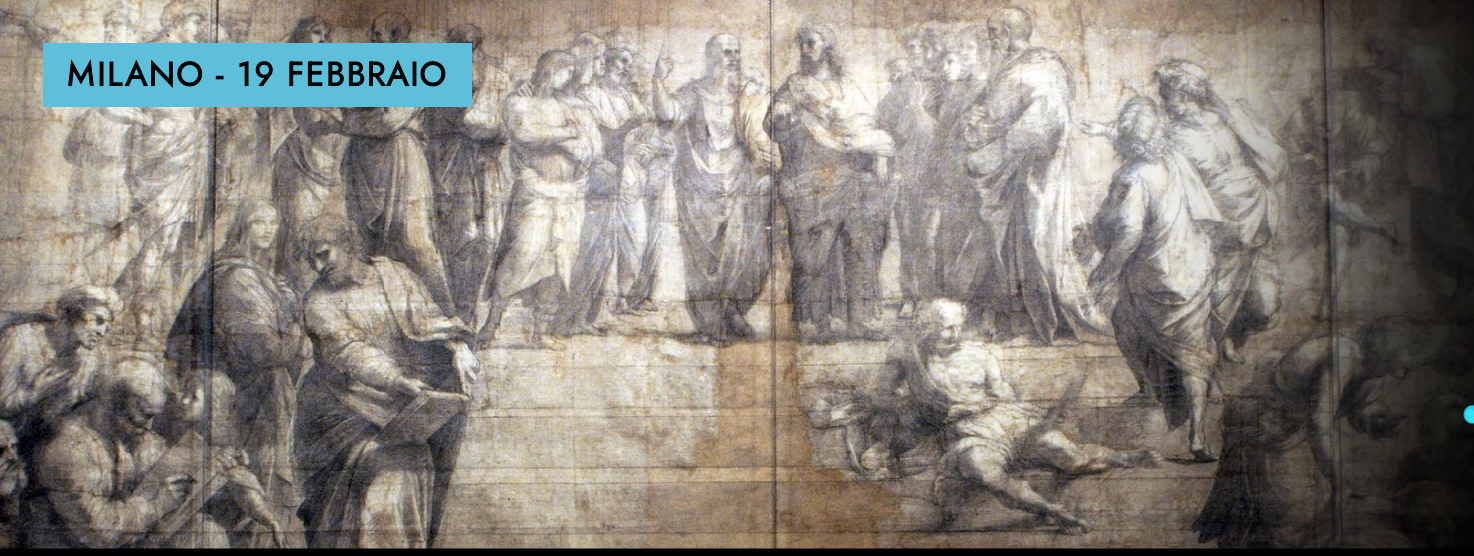


MILANO - 19 FEBBRAIO

Cybersecurity Conference 2026

Dalla Scuola di Atene alla Cybersecurity.

Ieri i grandi maestri del pensiero costruivano il futuro della conoscenza.
Oggi, filosofia e innovazione si incontrano per affrontare le sfide digitali del futuro.

cynet · Lenovo · Windows 11 · NOZOMI NETWORKS · OBJECT FIRST · proofpoint. · OTS

Lenovo consiglia Windows 11 Pro per le aziende

Il Gruppo OTS

Il Gruppo OTS è composto da 3 aziende all'avanguardia unite dalla stessa visione: trasformare il futuro attraverso l'unità e l'innovazione.

www.gruppoots.com

Athon Srl & Athon SA

Specializzati nella progettazione di soluzioni software e gestionali.
Il nostro obiettivo è fornirti gli strumenti per comprendere, semplificare e ottimizzare i tuoi processi aziendali e aumentarne le performance.

www.athon.eu | www.athon.ch

OTS Spa

La Capogruppo fondata nel 1996 è oggi Leader in Soluzioni ICT Servizi Gestiti e Full-Outsourcing.
Il nostro obiettivo è creare valore attraverso la condivisione delle nostre esperienze e competenze in ambito ICT.

www.ots-web.com

ITB Srl

Siamo partner italiano Salesforce, ci occupiamo dello sviluppo di soluzioni CRM, ma non solo. Con il nostro aiuto scoprirai come Salesforce può trasformare il tuo business, semplificando i processi, accelerando la crescita e portando risultati concreti.

www.itb-web.com

OTS SpA
20089 Rozzano Milanofiori (MI) Strada 4, Palazzo Q5, Piano 2. Telefono: +39 02 361611

Il Gruppo OTS

Il Gruppo OTS è composto da 3 aziende all'avanguardia unite dalla stessa visione: trasformare il futuro attraverso l'unità e l'innovazione.

athon
www.athon.eu

- **ERP (MS365 Business Central)**
- **Business Intelligence**
- **Data Analytics**
- **Document System**

OTS
www.ots-web.com

- **Cloud**
- **CyberSecurity**
- **Managed Services**
- **Professional Services**
- **Projects**

ITB
Salesforce inside
www.itb-web.com

- **CRM**
- **Sales**
- **Digital Marketing**
- **Service**
- **Field Service**

OTS SpA
20089 Rozzano Milanofiori (MI) Strada 4, Palazzo Q5, Piano 2. Telefono: +39 02 361611

Oãnšðèèhjlšßnlßßřhļ ðřř mettendo al sicuro le tue risorse IT.

Deep Cybersecurity Services

Rileviamo **in tempo reale** le recenti minacce globali. Interveniamo **proattivamente** utilizzando Tecnologie Intelligenti di Orchestrazione e Automazione della risposta.

Defensive Security

Blue Team

Controlliamo, analizziamo e correliamo eventi di sicurezza, come indicatori di attacco (IoA) e compromissione (IoC), per rilevare e mitigare reali minacce alla sicurezza dei tuoi dati e delle tue risorse IT.

- Security Operations Center (SOC) & Managed Detection & Response (MDR) 24/7
- Threat Intelligence
- Compromise Credential Monitoring
- Vulnerability Management

Offensive Security

Red Team

Scopri se sono presenti falle nella sicurezza mettendo alla prova le tue difese sia dall'esterno che dall'interno. Rileviamo i percorsi di attacco (Attack-Path) sfruttabili dagli attaccanti usiamo le fonti OSINT per verificare potenziali minacce imminenti o in corso.

- Vulnerability Assessment & Advanced Penetration Testing (VA/PT)
- RedTeaming & Gap Analysis
- Social Engineering, Phishing Simulation & Security Awareness.

Compliance & Governance

Value Team

Le tecnologie sono completamente inefficaci se non supportate da processi solidi e misurabili. Ti aiutiamo ad essere conforme con i principali standard di sicurezza rispettando i requisiti delle normative vigenti

- Security Risk Assessment & Posture
- Incident Response Planning & Testing
- ENISA, CIS, ISO27001, NIS2, NIST,
- Security Hardening.
- vCISO, CSIRT Outsourcing

OTS SpA
20089 Rozzano Milanofiori (MI) Strada 4, Palazzo Q5, Piano 2. Telefono: +39 02 361611

OTS

I nostri punti di forza

Numeri concreti che testimoniano l'affidabilità e l'impegno che mettiamo ogni giorno al servizio dei nostri Clienti.

30	3	300	H24
Anni di attività 1996/2026	Data Center sul territorio	Dipendenti in sede o Smart Working	Servizi IT erogati 365 Giorni/Anno

OTS SpA
20089 Rozzano Milanofiori (MI) Strada 4, Palazzo Q5, Piano 2. Telefono: +39 02 361611

I nostri principali Partners Tecnologici

Lavoriamo con tanti Partner perseguendo un singolo obiettivo, offrire la migliore soluzione alle tue esigenze

Microsoft
salesforce
Lenovo
cynet
CISCO
aws
NUTANIX
FORTINET
paloalto NETWORKS
NOZOMI NETWORKS
hp
SOCRadar Your Eyes Beyond
OBJECT FIRST
veeam
Cubbit
UBIQUITI NETWORKS
LIBRA ESVA email security virtual appliance
BROADCOM

OTS SpA
20089 Rozzano Milanofiori (MI) Strada 4, Palazzo Q5, Piano 2. Telefono: +39 02 361611

Why OTS?

Oggi le aziende hanno esigenze nuove e complesse, si afferma sempre di più la necessità di avere un interlocutore che sia in grado di **organizzare staff di risorse con competenze complementari** per risolvere i vari aspetti necessari ai progetti di **innovazione digitale**.

Il compito di **System Innovator e Managed Service Provider** diventa così quello di **integrare tecnologie e brand**, identificando e aggregando le migliori competenze e specializzazioni, in modo da portare al cliente **soluzioni mirate** che permettano di **raggiungere gli obiettivi**.

Interlocutore Unico

Riduciamo la complessità e semplifichiamo la **governance della infrastruttura IT**, proponendoci come **unico interlocutore** per la **gestione di tutte le risorse tecnologiche**.

Copertura H24

Operiamo sul territorio nazionale ed estero **sia in modalità smart sia on-site**.
Eroghiamo i nostri servizi dall'Italia con **copertura H24, sette giorni su sette**.

Trasparenza e Misurabilità

Utilizziamo strumenti di IT Service Management e Data Intelligence per **migliorare la qualità** e offrire un servizio **misurabile e trasparente**.

Esperienza ed Efficienza

Con 25 anni di esperienza nell'erogazione di servizi IT, siamo per i nostri Clienti un solido interlocutore, in grado di **soddisfare ogni esigenza di Business**.

OTS SpA
20089 Rozzano Milanofiori (MI) Strada 4, Palazzo Q5, Piano 2. Telefono: +39 02 361611

Cybersecurity Outlook 2026

A cura di:

Massimo Montedoro
OTS S.p.a.
Head of IT & Innovation | Pre-Sales | CyberSecurity Governance Manager
massimomontedoro@ots-web.com
https://www.linkedin.com/in/massimo-montedoro-1921288/

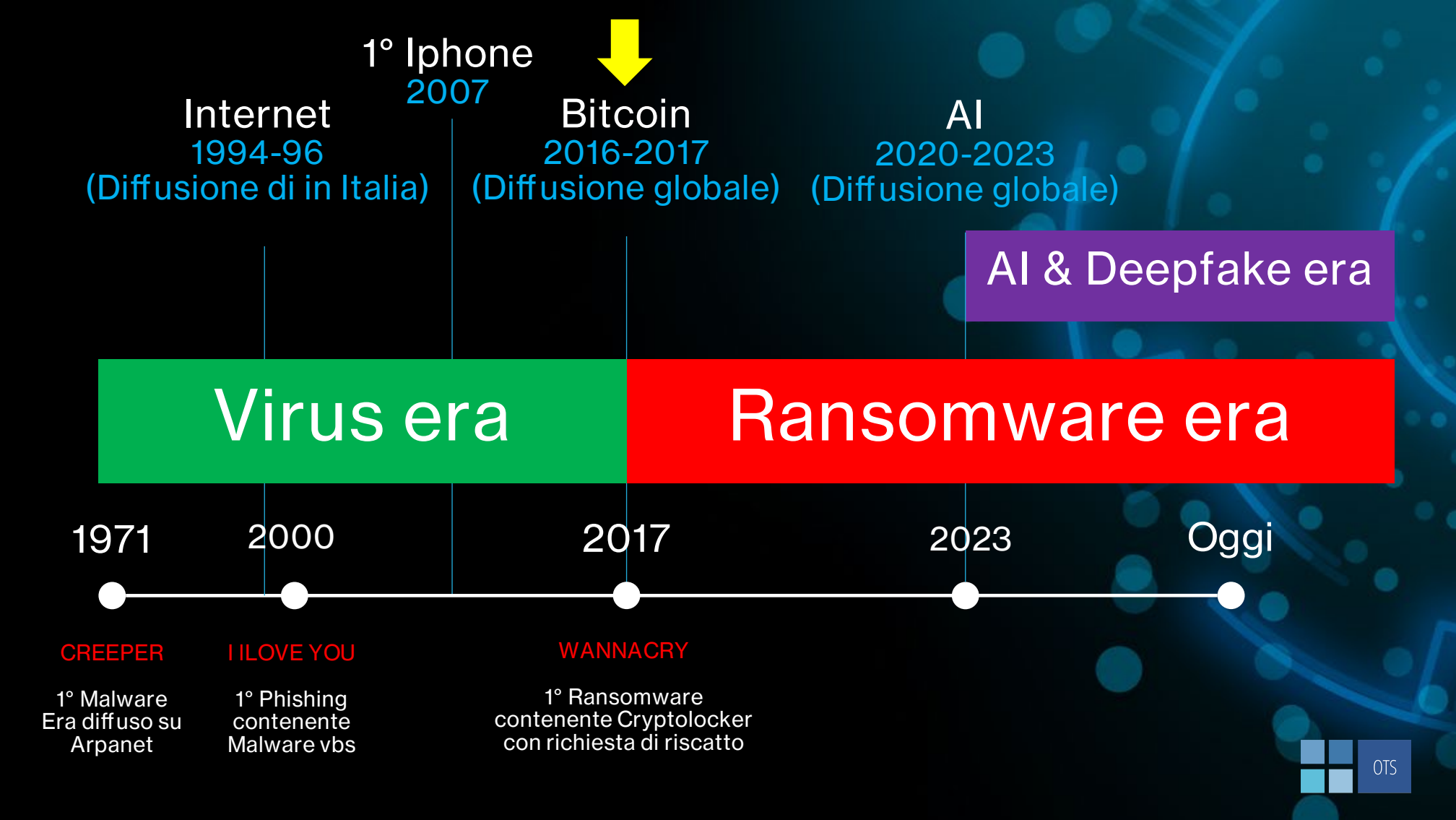
Marco Stefanini
OTS S.p.a.
Solution Architect | Pre-Sales | CyberSecurity Operation Manager
marcostefanini@ots-web.com
https://www.linkedin.com/in/marcostefanini/

OTS

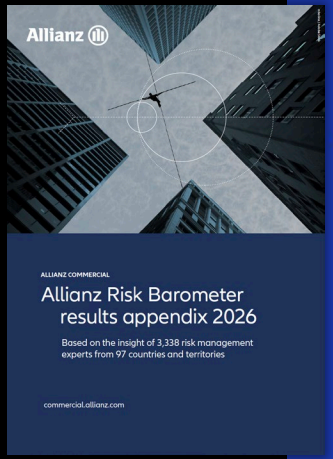
In questi anni lo scenario determinato da attaccanti, affiliati e minacce è completamente cambiato oggi ci troviamo di fronte ad organizzazioni criminali che dispongo di ingenti risorse, il cui unico obiettivo è massimizzare il profitto.

Domanda:
Quale tra i principali eventi nella storia ha determinato il più grande cambiamento nella Cybersecurity?

OTS


1° Iphone
2007
Internet
1994-96
(Diffusione di in Italia)
Bitcoin
2016-2017
(Diffusione globale)
AI
2020-2023
(Diffusione globale)
AI & Deepfake era
Virus era
Ransomware era
1971
2000
2017
2023
Oggi
CREEPER
1° Malware
Era diffuso su
Arpanet
I ILOVE YOU
1° Phishing
contenente
Malware vbs
WANNACRY
1° Ransomware
contenente Cryptolocker
con richiesta di riscatto
OTS

Domanda (facile):
Qual è il principale rischio per la Continuità del Business nelle aziende di oggi?



The most important business risks in 2026: Europe

1 46% → *2025: 1 (42%)*

Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)

2 30% ↗ *2025: 3 (33%)*

Business interruption

(Incl. supply chain disruption)

3 29% ↗ NEW

Artificial intelligence

(e.g., implementation challenges, liability exposures, misinformation / disinformation)

4 26% → *2025: 4 (25%)*

Changes in legislation and regulation

(e.g., tariffs, new directives, sustainability requirements)

5 22% ↘ *2025: 2 (33%)*

Natural catastrophes

(e.g., storm, flood, earthquake, wildfire)

6 20% ↘ *2025: 5 (19%)*

Climate change

(e.g., physical, operational and financial risks as a result of extreme weather)

7 17% → *2025: 7 (18%)*

Political risks and violence

(e.g., war, political instability, terrorism, polarization, coup d'état, civil unrest, strikes, riots, looting)

8 16% → *2025: 8 (13%)*

Macroeconomic developments

(e.g., inflation, deflation, monetary policies, austerity programs)

9 14% ↘ *2025: 6 (18%)*

Fire, explosion

10 13% → *2025: 10 (12%)*

Market developments

(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

Source: Allianz Commercial

Figures represent how often a risk was selected as a percentage of all responses for that region.
Respondents: 1,599
Figures don't add up to 100% as up to three risks could be selected.
NEW New entry in the top 10 risks

Threat & Trends 2026

Top 10 risks in Italy

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 168. Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2025 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network / service disruptions, malware / ransomware, data breaches, fines, and penalties)*	42%	*1 (55%)*	→
2	Business interruption *(incl. supply chain disruption)*	36%	*3 (34%)*	↗
3	Climate change *(e.g., physical, operational and financial risks as a result of extreme weather)*	34%	*4 (27%)*	↗
4	Artificial intelligence *(e.g., implementation challenges, liability exposures, misinformation / disinformation)*	33%	*9 (10%)*	↗
5	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire)*	26%	*2 (44%)*	↘
6	Changes in legislation and regulation *(e.g., tariffs, new directives, sustainability requirements)*	21%	*6 (16%)*	→
7	Political risks and violence *(e.g., war, political instability, terrorism, polarization, coup d'état, civil unrest, strikes, riots, looting)*	20%	*5 (20%)*	↘
8	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	15%	NEW	↗
9	Biodiversity and nature risks *(e.g., water scarcity)*	8%	NEW	↗
9	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation*	8%	*7 (15%)*	↘

Cybersecurity Threat & Trends 2026

Statistiche ed Evoluzione delle minacce informatiche

Threat & Trends 2026

OTS

Domanda:
Qual è il costo medio di un Data Breach in Italia?

La media globale del costo di una violazione dei dati è diminuita, e l'Italia è prima per diminuzione del costo.

Figure 2.
Measured in USD millions

#	Country		2025	2024
1	United States	↑	$10.22	$9.36
2	Middle East	↓	$7.29	$8.75
3	Benelux	↑	$6.24	$5.90
4	Canada	↑	$4.84	$4.66
5	United Kingdom	↓	$4.14	$4.53
6	Germany	↓	$4.03	$5.31
7	Latin America	↓	$3.81	$4.16
8	France	↓	$3.73	$4.17

#	Country		2025	2024
9	ASEAN	↑	$3.67	$3.23
10	Japan	↓	$3.65	$4.19
11	Italy	↓	$3.44	$4.73
12	South Korea	↓	$2.84	$3.62
13	Australia	↓	$2.55	$2.78
14	India	↑	$2.51	$2.35
15	South Africa	↓	$2.37	$2.78
16	Brazil	↓	$1.22	$1.36

The United States breaks a breach cost record
Average breach costs in the United States reached a record USD 10.22 million, a 9% increase over last year, driven in part by higher regulatory fines and detection and escalation costs. Most countries or regions recorded a decrease, due to lower detection and escalation costs. Some places, such as Saudi Arabia, were likely assisted by increased security spending and maturing security frameworks. Among the decliners were Italy (-27%), Germany (-24%) and South Korea (-21.5%). On the increase list were Canada, India, the Association of Southeast Asian Nations (ASEAN) and Benelux—the economic union of Belgium, the Netherlands and Luxembourg. Benelux made its debut in the 2024 study and witnessed a 6% increase in average breach cost. See Figure 2.

Threat & Trends 2026

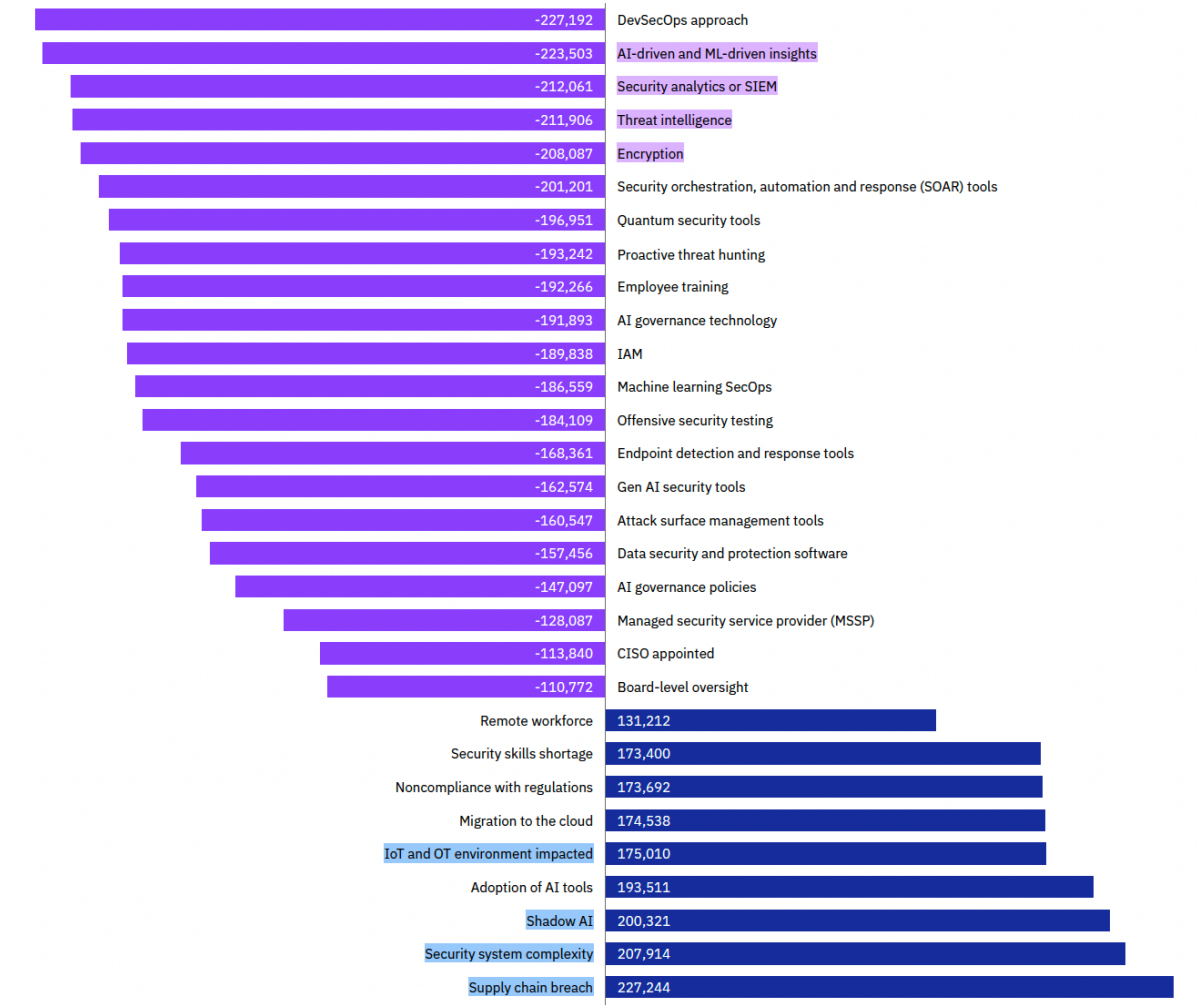
Factors that increase or decrease breach costs

When analyzing breach costs, it's important security leaders understand which technologies or events tend to lower or raise those costs. One constant we've found year over year: security AI and automation lowers costs. This year we also found the use of shadow AI raises costs. Our analysis examined 30 contributing factors and the impact of each in isolation against the global average. Also included are the top three factors found to amplify or mitigate the average data breach cost.

Key factors that reduced costs
Taking a DevSecOps approach to software development was the number one factor that reduced breach costs in this year's report. The use of AI and machine-learning insights, as well as having a security information and event management (SIEM) platform for detecting and responding to threats, rounded out the top three cost-reducing factors. All three of these security approaches center around and strengthen insight, intelligence and coordination. See Figure 39.

Key factors that increased costs
Security system complexity and supply chain breaches continue to challenge security teams and add to the average cost of a data breach. Both involve systems, networks and workflows with potential blind spots that can lead to vulnerability. The new addition to this year's top three costliest factors is shadow AI. Its presence within an organization is an added blind spot, another attack surface that is hard to police. As we've shown elsewhere in this report, organizations often don't look for shadow AI, so it remains undetected. See Figure 39.

Figure 39.
Cost difference from USD 4.88M breach average;
measured in USD

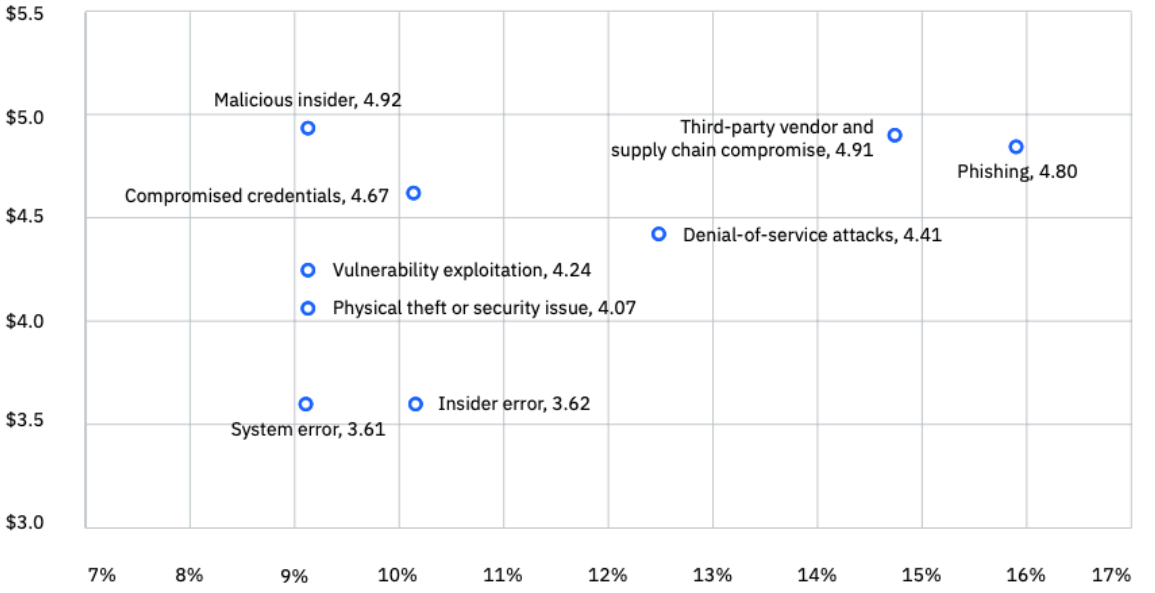


Vettori di Attacco iniziale più diffusi e più costosi.

For the third year in a row, phishing was among the top attack vectors. Vendor and supply chain compromise followed closely behind, overtaking compromised credentials as the number two attack vector. All three vectors, which can be gained through malware, data breaches and credential stuffing, carried heavy costs for breached organizations. Our research also compared the average time to identify and contain those breaches, with supply chain compromise taking the longest to resolve.

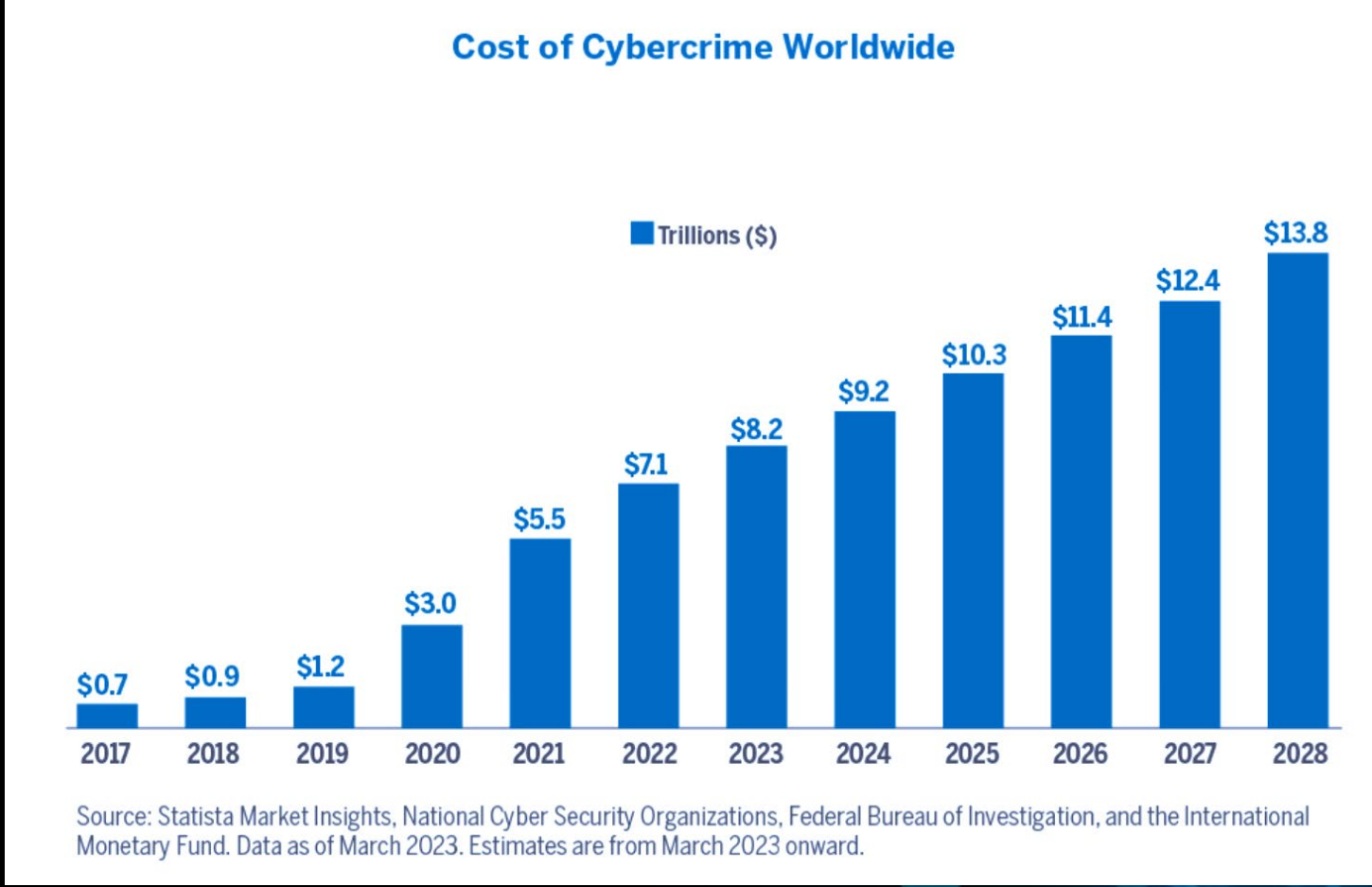
Phishing topped initial attack vectors
Phishing replaced stolen credentials this year as the most common initial vector (16%) attackers used to gain access to systems. At an average USD 4.8 million per breach, it was also one of the costliest. Meanwhile, supply chain compromise surged to become the second most prevalent attack vector (15%), and second costliest (USD 4.91 million) after malicious insider threats (USD 4.91 million). See Figure 9.

Figure 9.
Measured in USD millions; percentage of all breaches



Threat & Trends 2026

Report Incremento del Costo Globale per il Cybercrime e previsione di crescita.



Threat & Trends 2026 – @ Statista Market Insight

Principali Vettori di Accesso Iniziale

Summary of findings 1/4

Figure 5. Known initial access vectors in non-Error, non-Misuse breaches (n=9,891)

The exploitation of vulnerabilities has seen another year of growth as an initial access vector for breaches, reaching 20%. This value approaches that of credential abuse, which is still the most common vector. This was an increase of 34% in relation to last year's report and was supported, in part, by zero-day exploits targeting edge devices and virtual private networks (VPNs). The percentage of edge devices and VPNs as a target on our exploitation of vulnerabilities action was 22%, and it grew almost eight-fold[12] from the 3% found in last year's report. Organizations worked very hard to patch those edge device vulnerabilities, but our analysis showed only about 54% of those were fully remediated throughout the year, and it took a median of 32 days to accomplish.

CYBER SECURITY CONFERENCE 2026

Principali dati identificativi emersi dalle violazioni

Summary of findings 2/3

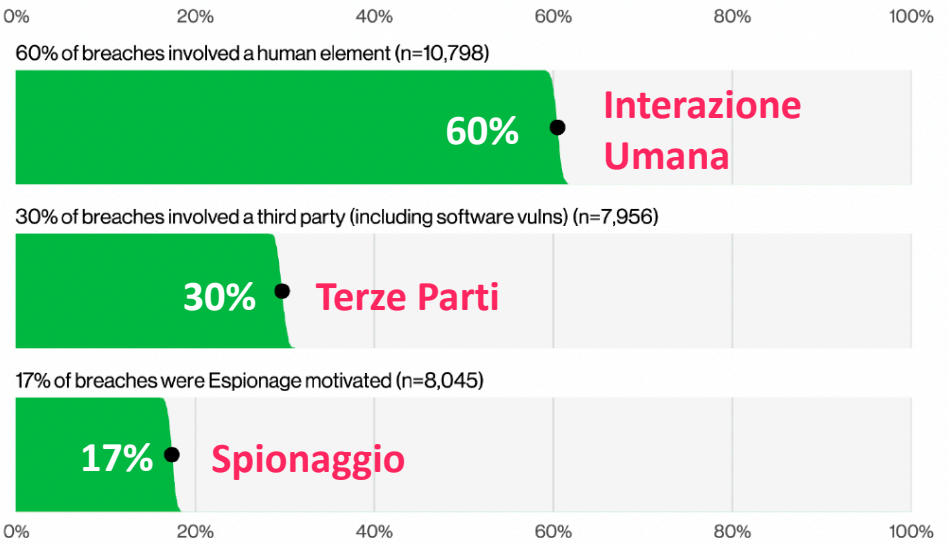


Figure 7. Select key enumerations in breaches

Although the involvement of the human element in breaches remained roughly the same as last year, hovering around 60%, the percentages of breaches where a third party was involved doubled, going from 15% to 30%.

There were notable incidents this year involving credential reuse in a third-party environment—in which our research found the median time to remediate leaked secrets discovered in a GitHub repository was 94 days.

We also saw significant growth in Espionage-motivated breaches in our analysis, which are now at 17%. This rise was, in part, due to changes in our contributor makeup. Those breaches leveraged the exploitation of vulnerabilities as an initial access vector 70% of the time, showcasing the risk of running unpatched services. However, we also found that Espionage was not the only thing state-sponsored actors were interested in—approximately 28% of incidents involving those actors had a Financial motive. There has been media speculation that this may be a case of the threat actors double-dipping to pad their compensation.

% Dispositivi (BYOD) compromessi da Infostealer che contenevano credenziali corporate

Summary of findings 3/3

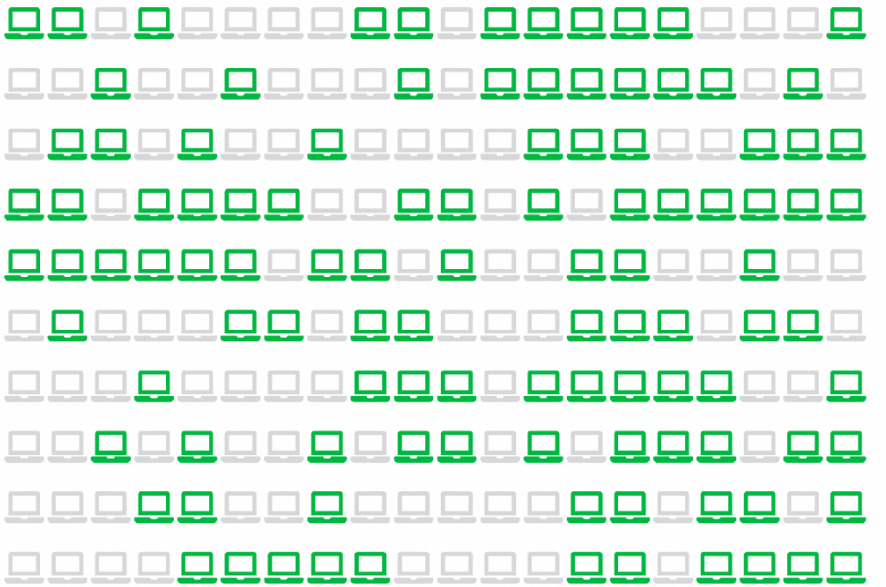


Figure 8. Percentage of non-managed devices with corporate logins in infostealer logs (each glyph is 0.5%)

46%

With regard to stolen credentials, analysis performed on information stealer malware (infostealer) credential logs revealed that 30% of the compromised systems can be identified as enterprise-licensed devices. However, 46% of those compromised systems that had corporate logins in their compromised data were non-managed and were hosting both personal and business credentials. These are most likely attributable to a BYOD program or are enterprise-owned devices being used outside of the permissible policy.

By correlating infostealer logs and marketplace postings with the internet domains of victims that were disclosed by ransomware actors in 2024, we saw that 54% of those victims had their domains show up in the credential dumps (for instance, as URLs the credentials allegedly gave access to), and 40% of the victims had corporate email addresses as part of the compromised credentials. This suggests these credentials could have been leveraged for those ransomware breaches, pointing to potential access broker involvement as a source of initial access vectors.

General Key Trends Europa

Phishing remains a primary initial intrusion vector ▶

- ClickFix-style scams
- Phishing-as-a-Service (PhaaS) platforms
- QR code phishing

Increasingly targeted cyber dependencies ▲

- targeted third-party providers
- exploiting the digital supply chain,

Continuous targeting of mobile devices ▶

- Exploitation of outdated devices,
- Android spyware KoSpy33, or Android spyware BoneSpy and PlainGnome.
- Vulnerability impacting its Qualcomm's Digital Signal Processor

Threat groups converging ▶

- Acktivist tooling and criminal ecosystems increasingly intersect.
- cybercriminals masquerading as other cybercriminal groups

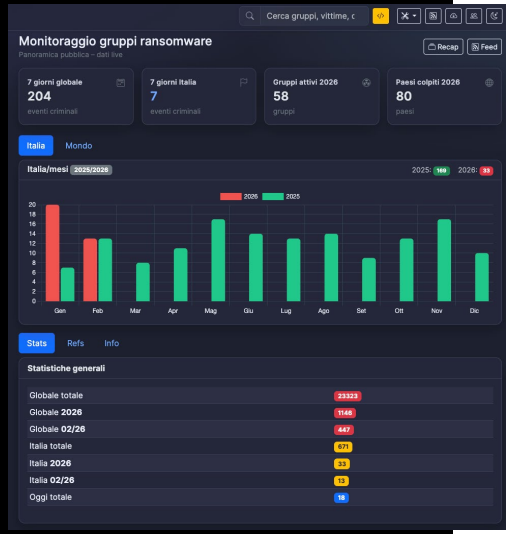
Predictable use of AI ▲

- 80% of all phishing emails identified between September 2024 and February 2025 using AI to some extent

CYBER SECURITY CONFERENCE 2026

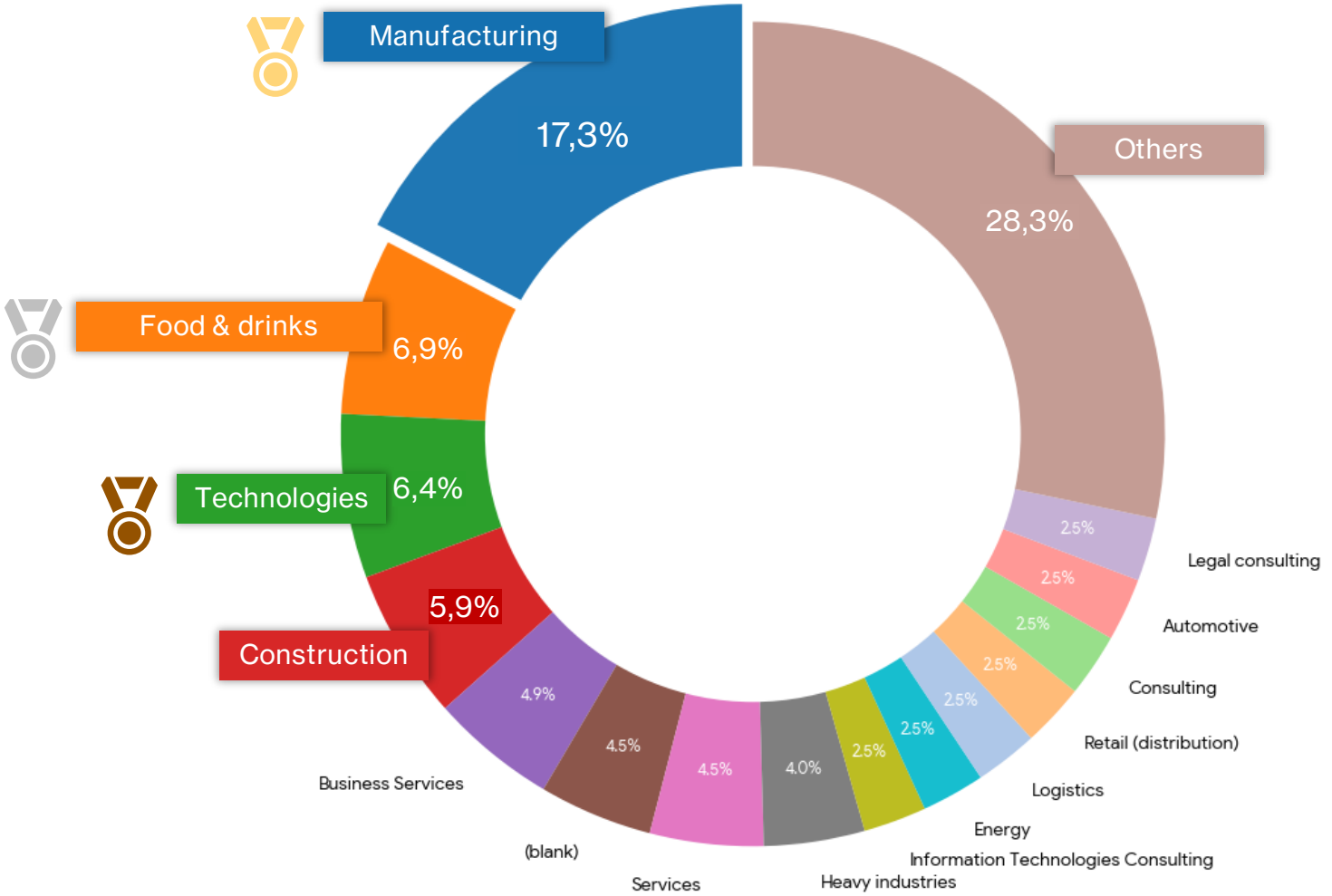
OTS

MBARO STANIA



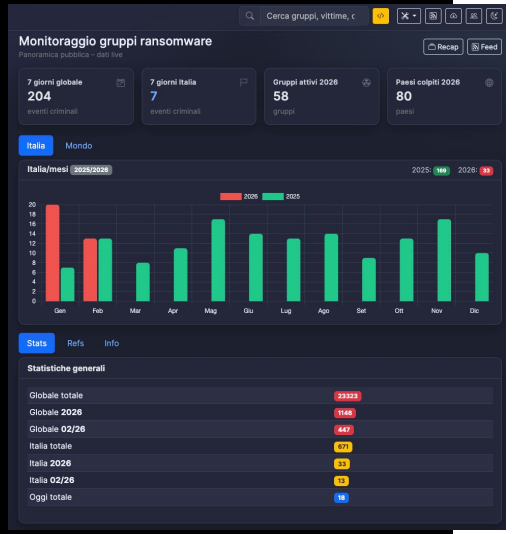
Threat & Trends 2026
@ Ransomfeed.it

Distribuzione delle Vittime per Settore in Italia nel 2025



Report: Vittime di Attacco da gruppo Ransomware negli ultimi 2 mesi

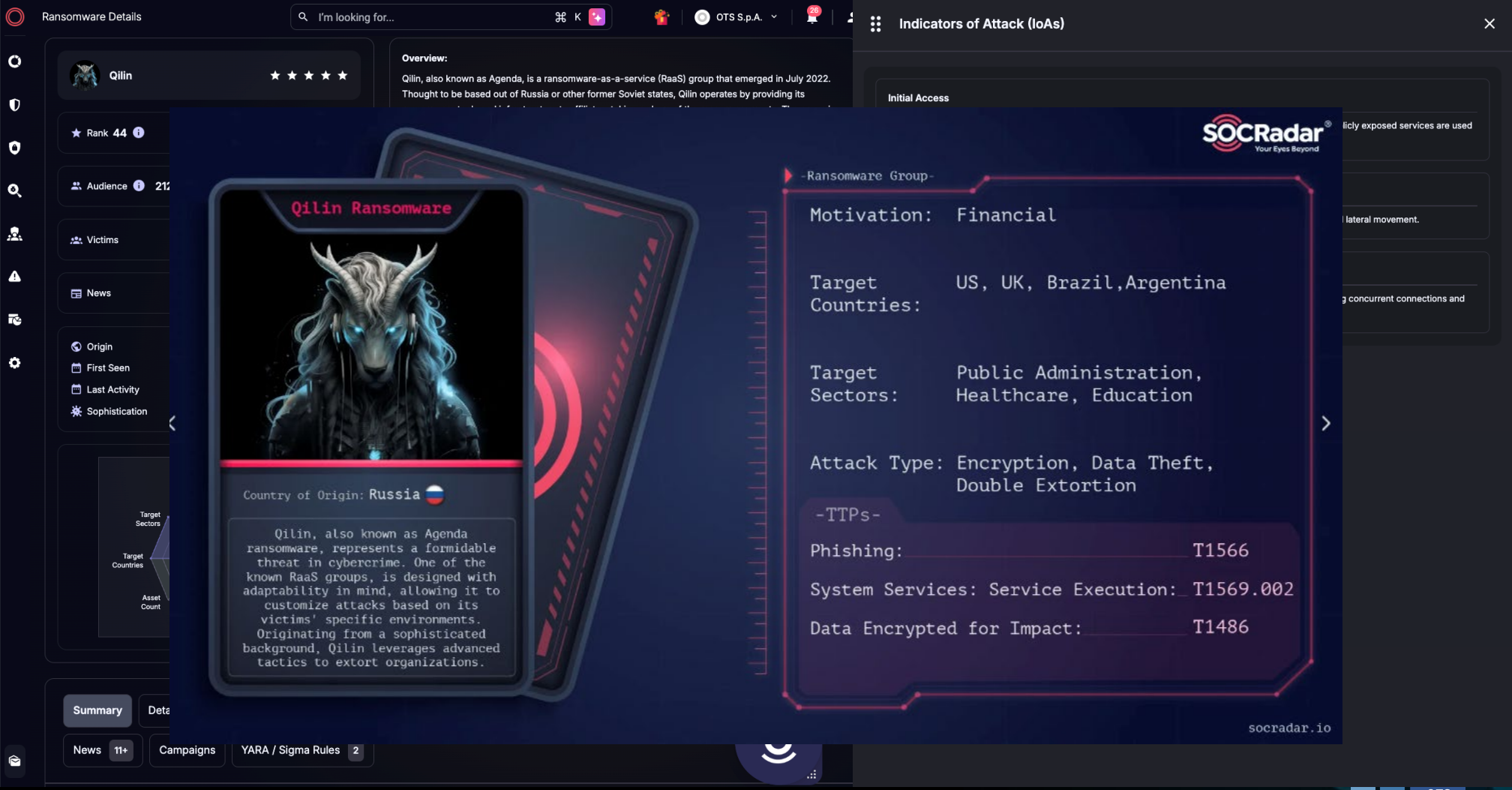
Data	Victim	Gang	Settore	Fatturato (Stima)
16/02/26	[redacted]	Qilin	Associazioni / Servizi	N/D (No profit)
16/02/26	[redacted]	Akira	Alimentare (Conserve)	€100M - €120M
16/02/26	[redacted]	Dragonforce	Logistica / Automazione	€80M - €100M
16/02/26	[redacted]	Akira	Automazione / Domotica	€20M - €30M
14/02/26	[redacted]	Incransom	IT / Fintech	€5M - €10M (Bitgo Srl)
14/02/26	[redacted]	Nightspire	Commercio / Idraulica	€10M - €15M
13/02/26	[redacted]	Spacebears	Avionica / Elettronica	€15M - €25M
07/02/26	[redacted]	LockBit3	Trasporti	€10M - €20M
07/02/26	[redacted]	Clop	Servizi IT / Sanità	€5M - €10M
06/02/26	[redacted]	Qilin	Intrattenimento	€5M - €10M
06/02/26	[redacted]	Thegentlemen	Edilizia / Costruzioni	€20M - €40M
03/02/26	[redacted]	Medusa	Pubblica Amministrazione	N/D (Ente Pubblico)
02/02/26	[redacted]	Akira	Costruzioni Industriali	€40M - €60M
30/01/26	[redacted]	Clop	Trasporti Marittimi	€100M - €150M
25/01/26	[redacted]	Clop	Ristorazione Collettiva	€50M - €70M
24/01/26	[redacted]	Safepay	Editoria / Servizi	€2M - €5M
21/01/26	[redacted]	LockBit3	Macchine Agricole	€10M - €15M
20/01/26	[redacted]	Thegentlemen	Trasporti	€100M - €120M
20/01/26	[redacted]	Sarcoma	Software Industriale	€2M - €5M
20/01/26	[redacted]	Thegentlemen	Alimentare (Snack)	€300M - €350M
19/01/26	[redacted]	Qilin	Calzature (Fashion)	€30M - €50M
17/01/26	[redacted]	Qilin	Materiali da Costruzione	€400M - €500M
17/01/26	[redacted]	Qilin	Chimica / Minerario	€300M - €400M
15/01/26	[redacted]	LockBit3	Logistica / Retail	€10M - €20M
14/01/26	[redacted]	Anubis	Trasporti (Portuale)	N/D (Ente Pubblico)
13/01/26	[redacted]	Incransom	Agricoltura	€15M - €25M
08/01/26	[redacted]	Qilin	Consulenza IT	€100M - €120M
08/01/26	[redacted]	Clop	Alimentare (Conserve)	€500M - €600M
08/01/26	[redacted]	Qilin	Attrezzature Subacquee	€40M - €60M
07/01/26	[redacted]	Akira	Manifatturiero (Tessile)	€10M - €20M
06/01/26	[redacted]	Brotherhood	Stampa / Etichette	€15M - €25M
05/01/26	[redacted]	Nova	Logistica / Trasporti	€20M - €30M
02/01/26	[redacted]	Qilin	Servizi / Cleaning	€10M - €20M



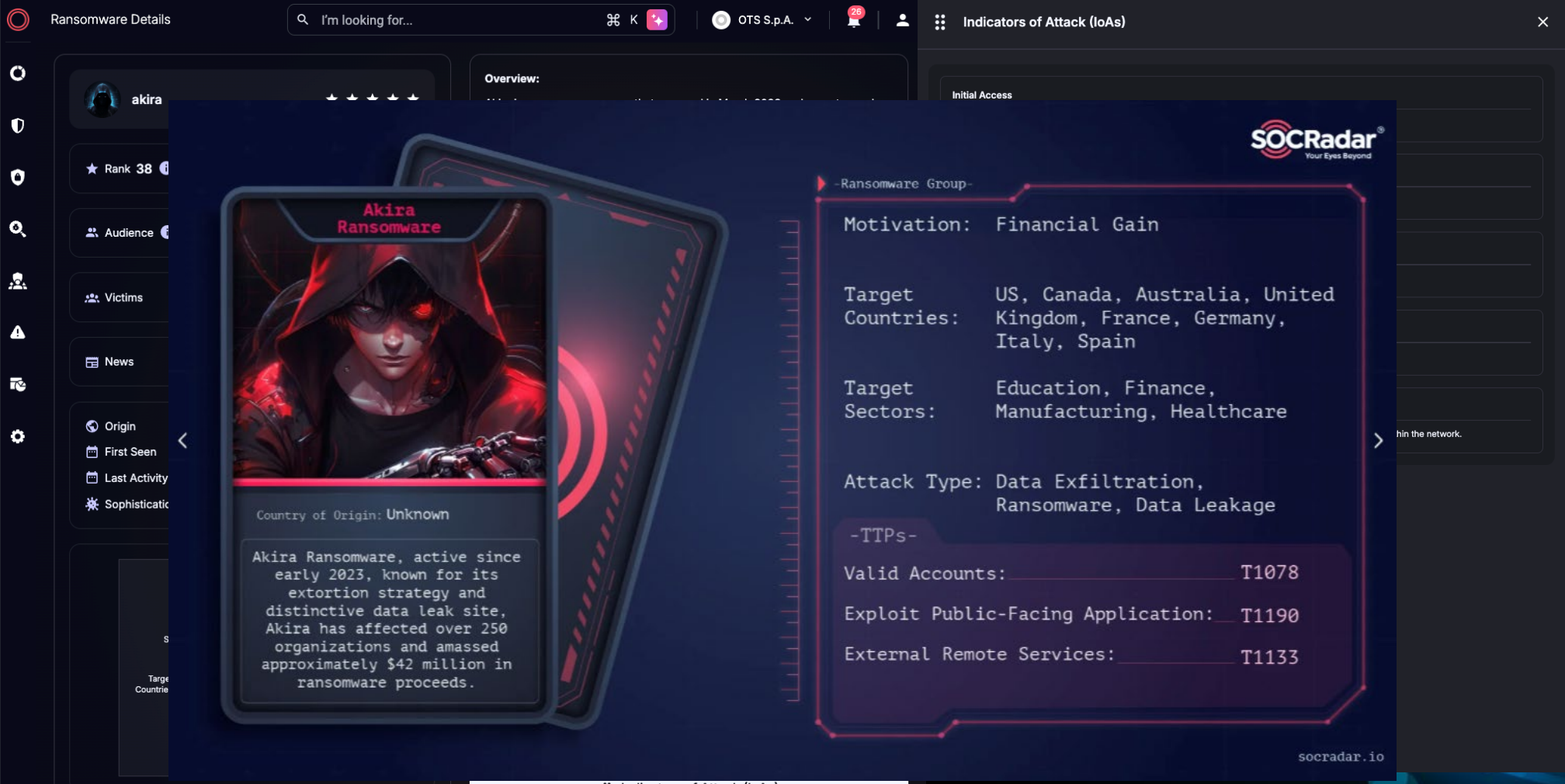
Threat & Trends 2026
@ Ransomfeed.it

Gruppi Ransomware più attivi nell'ultimo anno in Italia

Gruppo Ransomware	Incidenti (N)	Percentuale	Vettore di Attacco Principale	Tecniche Comuni (MITRE ATT&CK)
Qilin	39	19,31%	Phishing / Credenziali compromesse /RDP esposti	Crittografia personalizzata (Rust), Esfiltrazione dati
Akira	24	11,88%	Vulnerabilità VPN (Cisco)	Sfruttamento falle MFA, Eliminazione Shadow Copy
Sarcoma	11	5,45%	RDP esposti / Servizi vulnerabili	Movimento laterale rapido, Doppia estorsione
Everest	9	4,46%	Accesso iniziale via IAB (Brokers)	Accesso a livello di kernel, Vendita dati rubati
Dragonforce	8	3,96%	Vulnerabilità web (SQLi/XSS)	Defacement di siti e furto database massivo
Incransom	8	3,96%	Email malevole (Malspam)	Scripting PowerShell, Persistenza tramite Task
LockBit 3.0	7	3,47%	Vulnerabilità software (es. Citrix)	Self-spreading, Crittografia ultra-rapida



Threat & Trends 2026 – CTI SocRadradar



Threat & Trends 2026 – CTI SocRadradar

[AKIRA]

AKIRA

Well, you are here. It means that you're suffering from cyber incident right now. Think of our actions as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that there is a fair price to make it all go away.

Do not rush to assess what is happening - we did it to you. The best thing you can do is to follow our instructions to get back to your daily routine, by cooperating with us you will minimize the damage that might be done.

Those who choose different path will be shamed here publicly. The functionality of this blog is extremely simple - enter the desired command in the input line and enjoy the juiciest information that corporations around the world wanted to stay confidential.

Remember. You are unable to recover without our help. Your data is already gone and cannot be traced to the place of final storage nor deleted by anyone besides us.

```
guest@akira:~$ help

List of all commands:

 leaks      — hacked companies
 news       — news about upcoming data releases
 contact    — send us a message and we will contact you
 help       — available commands
 clear      — clear screen

guest@akira:~$
```

Evoluzione Tecniche di Estorsione 1/2

Ransomware extortion tactics have been evolving from single extortion (which is intrinsic to all traditional ransomware operations) to double extortion (e.g., the Maze ransomware group in 2019) to triple extortion (notably with the ALPHV/BlackCat in 2021) to quadruple extortion (e.g., CL0P in 2024; Figure 3).

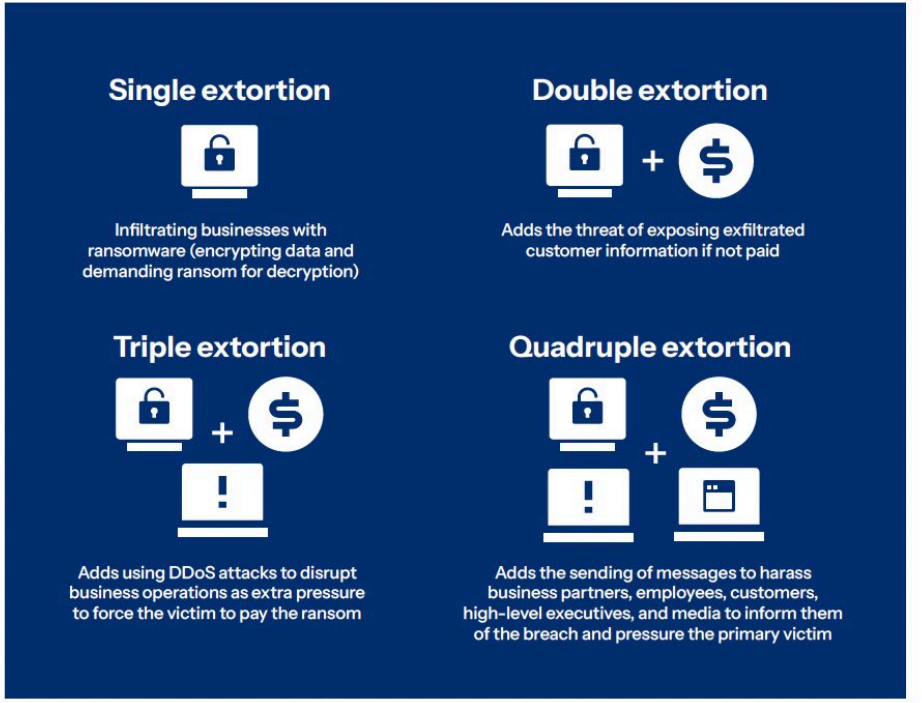


Fig. 3: Ransomware extortion tactics

Threat & Trends 2026

Evoluzione Tecniche di Estorsione 2/2

This evolution of tactics has proven effective for ransomware groups, resulting in escalated average ransom payments. While triple and quadruple extortion are growing more frequent, double extortion still appears to be the most common tactic (Figure 4). And a new trend among ransomware groups that are using double and quadruple extortion tactics is the use of government regulations as leverage.

Ransomware	Double Extortion	Triple Extortion	Quadruple Extortion
Abyss Locker	⚠		
Black Basta	⚠		
FunkSec	⚠		
HellCat	⚠		
Interlock	⚠		
Lynx	⚠		
Morpheus	⚠		
Nnice	⚠		
RansomHub	⚠		
XELERA	⚠		
Akira	⚠	⚠	
Medusa	⚠	⚠	
ALPHV/BlackCat	⚠	⚠	⚠
CL0P	⚠	⚠	⚠
LockBit 3.0	⚠	⚠	⚠

Fig. 4: Akamai researchers have observed these ransomware groups employing various extortion tactics

Domanda:

Quali sono i principali vettori di accesso iniziale in un incidente informatico?

- Email di Phishing
- Compromissione delle terze parti
- Furto e Copromissione di Credenziali
- Sfruttamento di Vulnerabilità
- Shadow AI

Quali sono le principali sfide per governare i processi e le politiche di sicurezza?

- Condividere la valutazione del rischio reale con il board.
- Definire una Strategia di Sicurezza pensata a partire dal Business.
- Ottenere un mandato forte per applicare la strategia in azienda.
- Essere conformi alle regolamentazioni.

OTS

Quali sono le principali sfide nell'adozione delle strategie di sicurezza

- Proteggere i dati, dalla compromissione ed esfiltrazione
- Definire e monitorare la superficie di attacco
  es: BYOD, Terze Parti, ShadowAI, Supply Chain, Darkweb, Infostealer
- Applicare le Best Practice di Sicurezza (Hardening)
  es: Least Priviledge, 0Trust, MFA, PAM, etc.
- Gestire le innumerevoli vulnerabilità pubblicate
- Testare le proprie difese per essere pronti a rispondere ad un attacco informatico e/o gestire un Data Breach.

OTS

Domanda:
Policy Area:

A quale framework o regolamentazione NIS 2 (Directive (EU) 2022/2555) appartengono queste politiche?

a) Risk Management
b) Roles and Responsibilities
c) Personnel Reliability
d) Security Compliance and Audit
e) Supply Chain Cybersecurity Risk Management
f) Asset Management
g) Vulnerability Management
h) Business continuity, disaster recovery, and crisis management
i) Authentication, digital identity, and access control management
j) Physical security
k) Personnel training and awareness
l) Data security
m) Information and network systems development, configuration, maintenance, and decommissioning
n) Network and communications protection
o) Security event monitoring
p) Incident response and recovery

OTS

Un caso reale

Nel 2023, la storica azienda di autotrasporti Knights of Old, con sede a Kettering nel Northamptonshire (UK), è stata costretta a chiudere a seguito di un attacco ransomware. Un attacco della portata gigantesca, evidentemente, che non ha lasciato scampo a una company pure solida, in vita da ben 160 anni.

"Sentivamo di essere in un'ottima posizione per quanto riguarda la nostra sicurezza, i nostri protocolli, le misure adottate per proteggere l'azienda", ha raccontato l'ex direttore Paul Abbott. Ma la percezione di "essere a posto" non era realistica: "Qualunque cosa pensiate di aver fatto, fatela controllare da degli esperti. La gente non pensa che possa succedere a loro".

All'epoca, l'attacco danneggiò dati chiave, rendendo impossibile rispettare le scadenze di rendicontazione stabilite dai finanziatori. Gli sforzi per gestire manualmente le operazioni furono vani, e alla fine Knights of Old dichiarò amministrazione controllata.

La sicurezza al 100% non esiste, ma con responsabilità e attenzione, possiamo renderla migliore di ieri ;)

OTS

Grazie per l’attenzione.

OTS