

Nov 2025

INTELLIGENCE INSIGHTS EUROPE

Protect yourself against future risks by uncovering the latest trends and insights into Europe's threat landscape (September - November)

Key insights

- On September 26, 2025, the ransomware gang Payouts King Group leaked corporate data belonging to Creditinfo Group, a leading provider of credit information and risk management solutions.
- The highest-revenue company listed by Initial Access Brokers was a Serbian firm in the marine shipping and transportation sector, with \$206 million in annual revenue.
- Threat actor Hezi Rash claimed responsibility for DDoS attacks targeting four German health-related organizations: the National Association of Statutory Health Insurance Physicians (Hartmannbund), the Association of Physicians of Germany (Virchowbund), the Association of Practicing Physicians of Germany, and the German Society for Hygiene and Microbiology.
- The most active adversary-in-the-middle phishing framework in September was Tycoon 2FA.

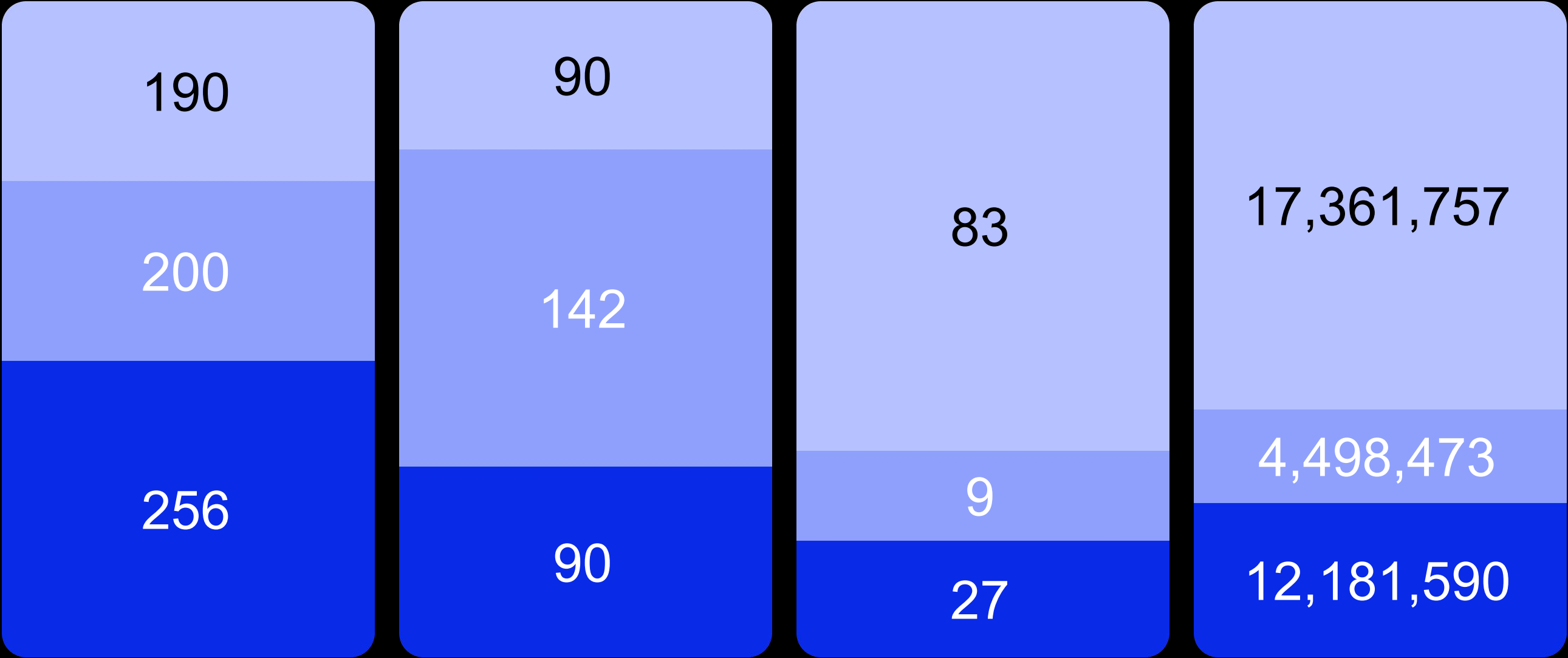


Val Shirko
Regional Business
Head, Europe

This report provides an overview of the latest threat landscape in Europe, covering key developments such as ransomware attacks, leaked credentials, data breaches, and more. It includes a month-over-month trend analysis to track evolving patterns. The report also spotlights recently identified threat actors, campaigns, and emerging techniques, and gives actionable insights for proactive defenses.

Would you like to help us improve the report? Click here to take a one-minute survey.

THREAT LANDSCAPE



DDoS/Hacktivism attacks

Ransomware

Initial access brokers

Leaked corporate
accounts

September 2025 October 2025 November 2025

DDOS AND HACKTIVISM BY COUNTRY

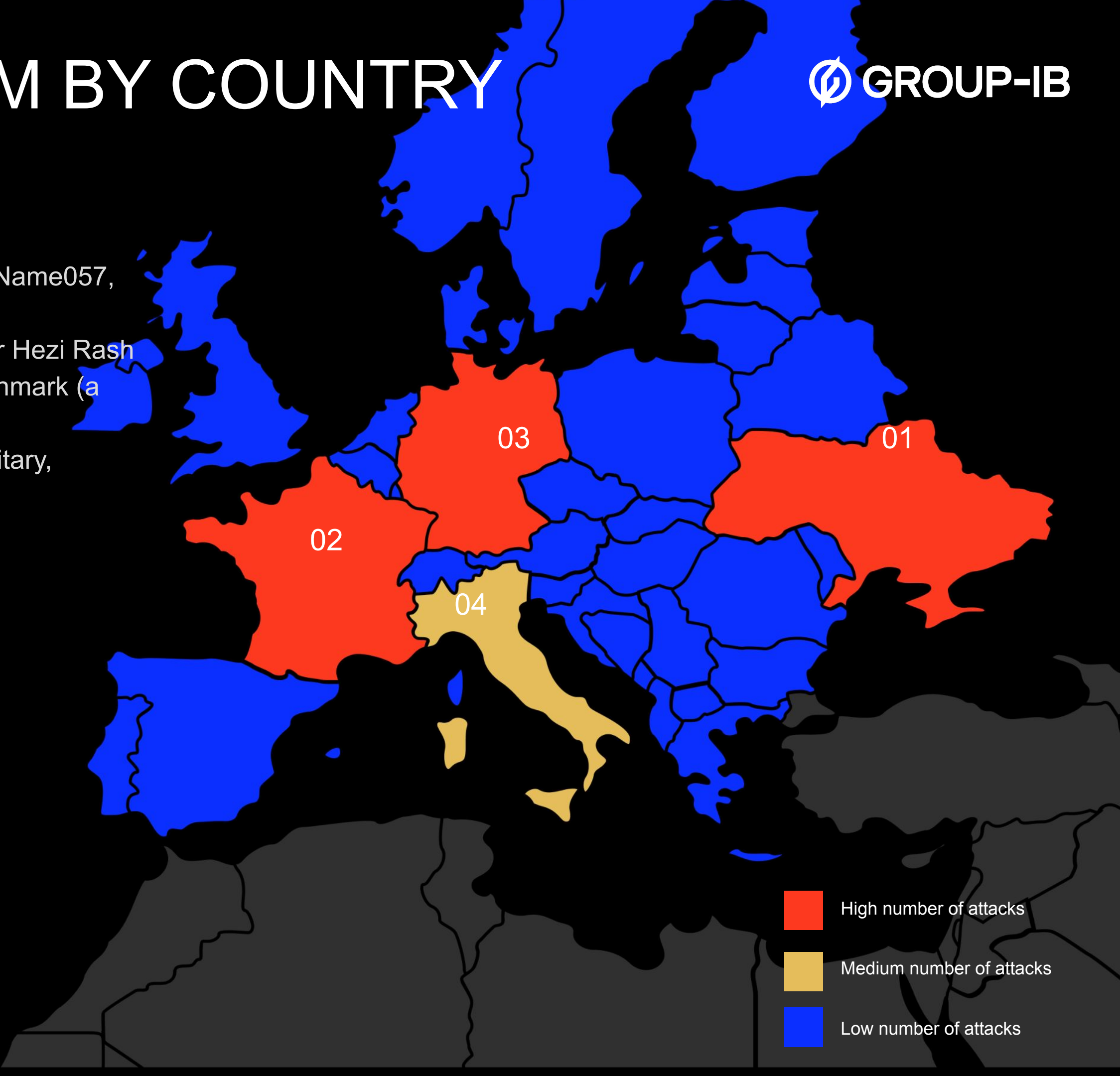


Key events

- The most prolific threat actors behind these attacks are NoName057, Hezi Rash, and DarkStorm Team.
- According to Group-IB's Threat Intelligence, the threat actor Hezi Rash claimed DDoS attacks on the Court of Denmark and Topdanmark (a leading insurance company in Denmark).
- The most often attacked industries are government and military, manufacturing, transportation and energy.

Most attacked countries

Ukraine	France	Germany	Italy
85 attacks	67 attacks	63 attacks	51 attacks



RANSOMWARE ACTIVITIES

Key events

- On November 23, 2025, the ransomware group Everest claimed responsibility for an attack targeting Agfa-Gevaert Group, a Belgian-German multinational corporation that develops, manufactures, and distributes analogue and digital imaging products, software, and systems.
On October 14, 2025, the ransomware group Qilin claimed responsibility for an attack targeting Sice, a leading multinational company in technology integration for public infrastructure management.

322
ransomware incidents

Most active threat actors

Qilin	Everest
96 attacks 30% of all attacks	16 attacks 5%
INC Blog	Dragon Force
16 attacks 5%	15 attacks 5%
	SafePay
	11 attacks 3%

Most targeted industries

Manufacturing	Real estate	Logistics and transportation
	44 attacks 14%	25 attacks 8%
	Financial services	Travel
61 attacks 19% of all attacks	21 attacks 7%	17 attacks 5%

INITIAL ACCESS BROKER

ACTIVITY ON THE DARK WEB

Initial access to a company’s systems can lead to data theft, corporate espionage, and the deployment of malware for various malicious purposes. This page shows the volume and geographic distribution of corporate infrastructure access currently for sale on the dark web.

119
sales

Key events

- France is the primary target of the threat actor lacrim. Most of the affected companies report annual revenues of around \$5 million, with the overall revenue range of targeted organizations spanning from \$5 million to \$250 million.

Most active threat actors

lacrim	SantaAd	R-W-M Group
59 attacks mostly in	9 attacks mostly in	6 attacks mostly in
• France (28) • Greece (11) • Italy (7)	• UK (2) • Italy (2) • Switzerland (1)	• Switzerland (3) • Italy (2) • Netherlands (1)

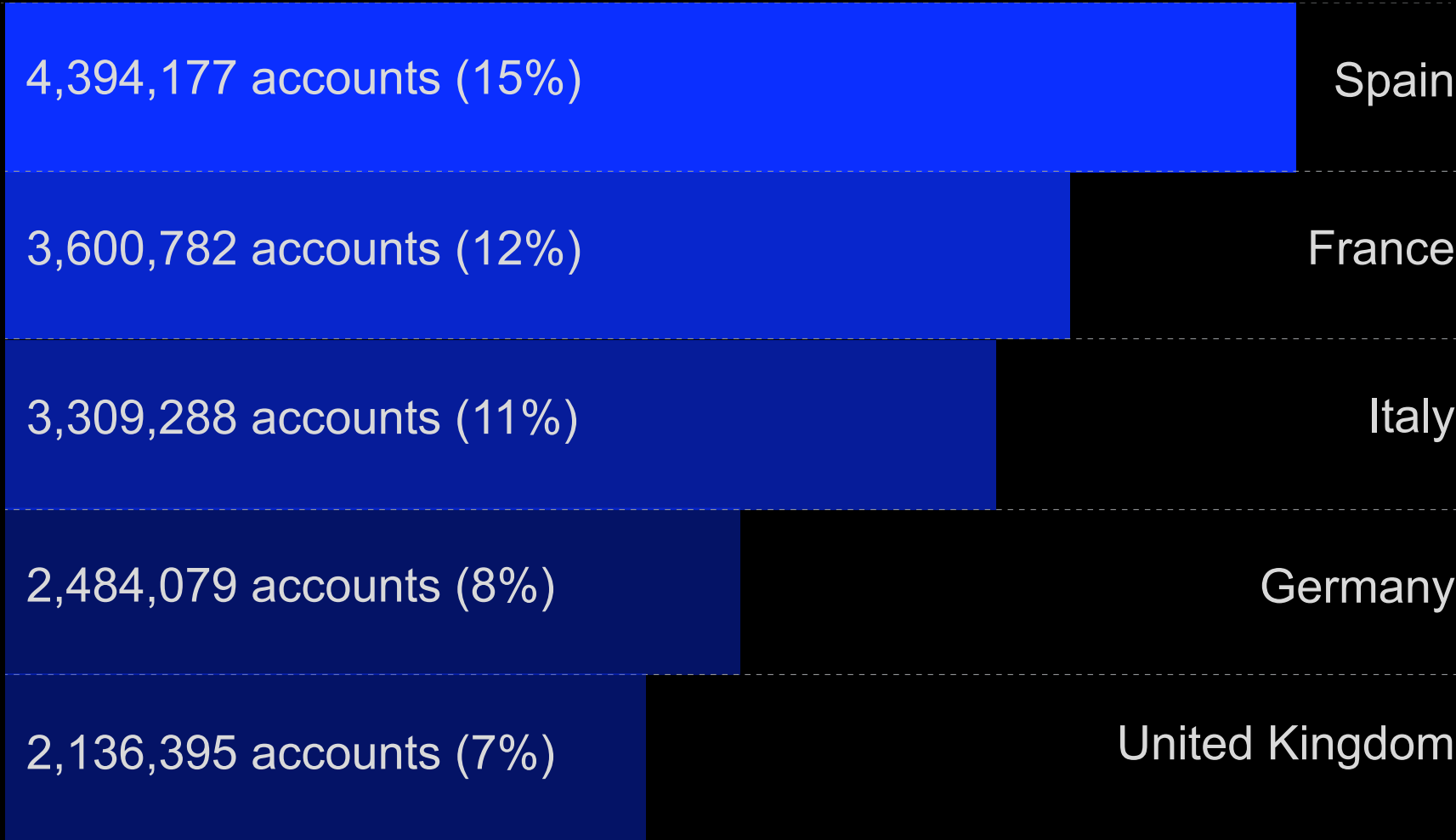
LEAKED CORPORATE CREDENTIALS



Key events

- On October 3, 2025, members of the united group “Scattered Spider/ShinyHunters/Lapsus” (the group now abbreviates its name to SLSH) launched a Dedicated Leak Site (DLS) on breachforums[.]hn - Scattered LAPSUS\$ Hunters.
- Phishing kit attributed to M3tri impersonated Argenta, a rapidly growing bank and insurance company in Belgium.

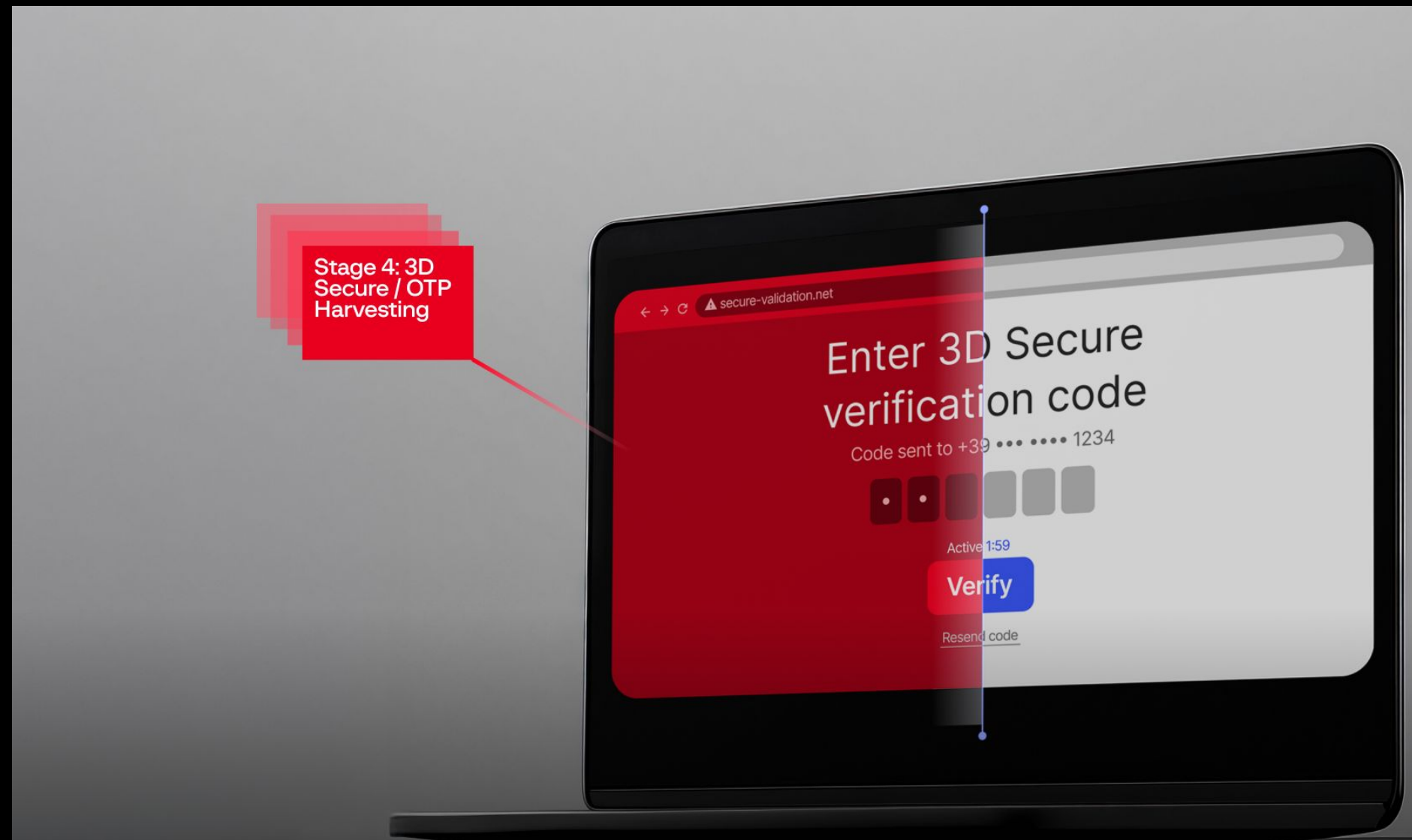
Countries with the most compromised accounts



30,178,963
compromised accounts

PHISHING SPOTLIGHT

Multi-stage phishing kit



Four stages

- Spear-phishing lures were sent to customers of an Italian company, warning of expiring services or failed payments.
- Pre-filled login URLs embedding the victim's email address were used to make messages look more realistic.
- The phishing kit is built for efficiency and evasion. It is a comprehensive, multi-stage application designed to guide victims through a full data harvesting process.
- Telegram chats were used as exfiltration channels to steal information about the payment details.

[Read more](#)

Would you like to help us improve the report?
Click here to take a one-minute survey.

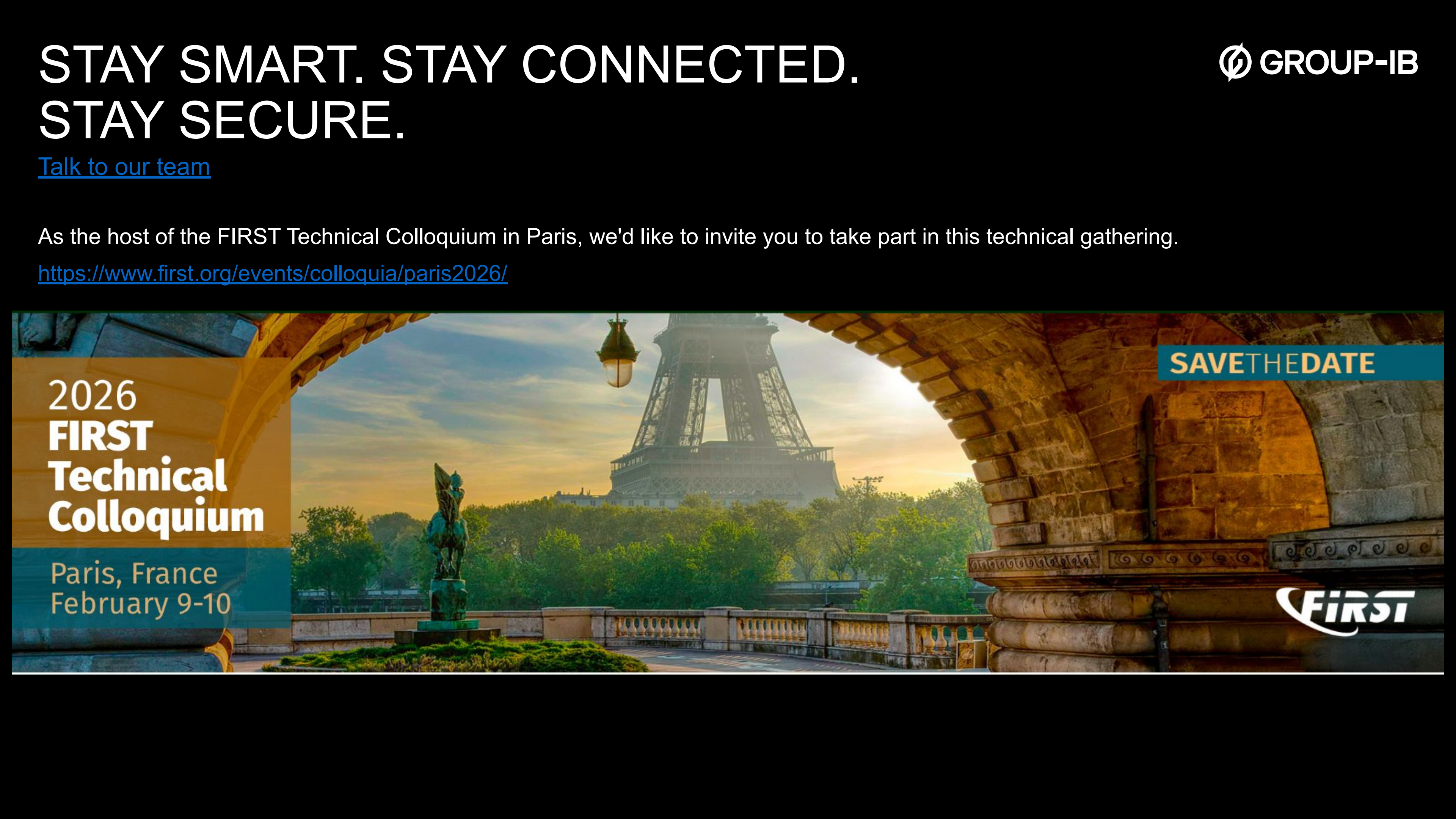
STAY SMART. STAY CONNECTED. STAY SECURE.



[Talk to our team](#)

As the host of the FIRST Technical Colloquium in Paris, we'd like to invite you to take part in this technical gathering.

<https://www.first.org/events/colloquia/paris2026/>

A scenic view of the Eiffel Tower in Paris, France, seen through a stone archway. The tower is partially obscured by a large, ornate stone archway in the foreground. The scene is set during sunset or sunrise, with a warm, golden light illuminating the sky and the tower. A statue of a winged figure stands on a pedestal in the foreground, to the left of the archway. The overall atmosphere is serene and historic.

2026
FIRST
Technical
Colloquium

Paris, France
February 9-10

SAVETHEDATE

