Europe
Regional Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

Executive Summary

Top Takeaways

- Finance and Insurance is the top exposed sector on the dark web with 14,08%, and when Commercial Banking and Crypto are added, total financial exposure reaches 22,8%.
- Retail and e-commerce follow closely with 19,5%, confirming criminals' focus on quick monetization. Selling dominates threat categories at 61,93%, while sharing stands at 24,34%, showing that over 70% of activity is trade-driven.
- Data leaks remain the most common threat type at 58,23%, with access sales at 21,90%, meaning more than 80% of threats revolve around stolen information and entry points.
- At the country level, France (5,62%), the UK (4,89%), and Germany (4,68%) lead in dark web targeting, while ransomware strikes are highest in the UK (22,94%), Germany (16,47%), and France (10,10%).
- Ransomware activity is fragmented: Akira (8,7%), Qilin (8,1%), and RansomHub (6,8%) are visible, but smaller groups make up 76,4%.
- Phishing shows a different pattern, with Bulgaria (24,26%) and Russia (21,06%) leading.
- Information Services (19,77%), National Security & International Affairs (13,31%), and Banking (11,45%) are the main phishing targets.
- 73,44% of phishing sites use HTTPS, showing how attackers exploit encryption to build trust.

Technical Details

This report based on data collected between August 2024 and August 2025

In the following chapters, you will be reading about the various aspects of the cyber threat landscape around Europe.

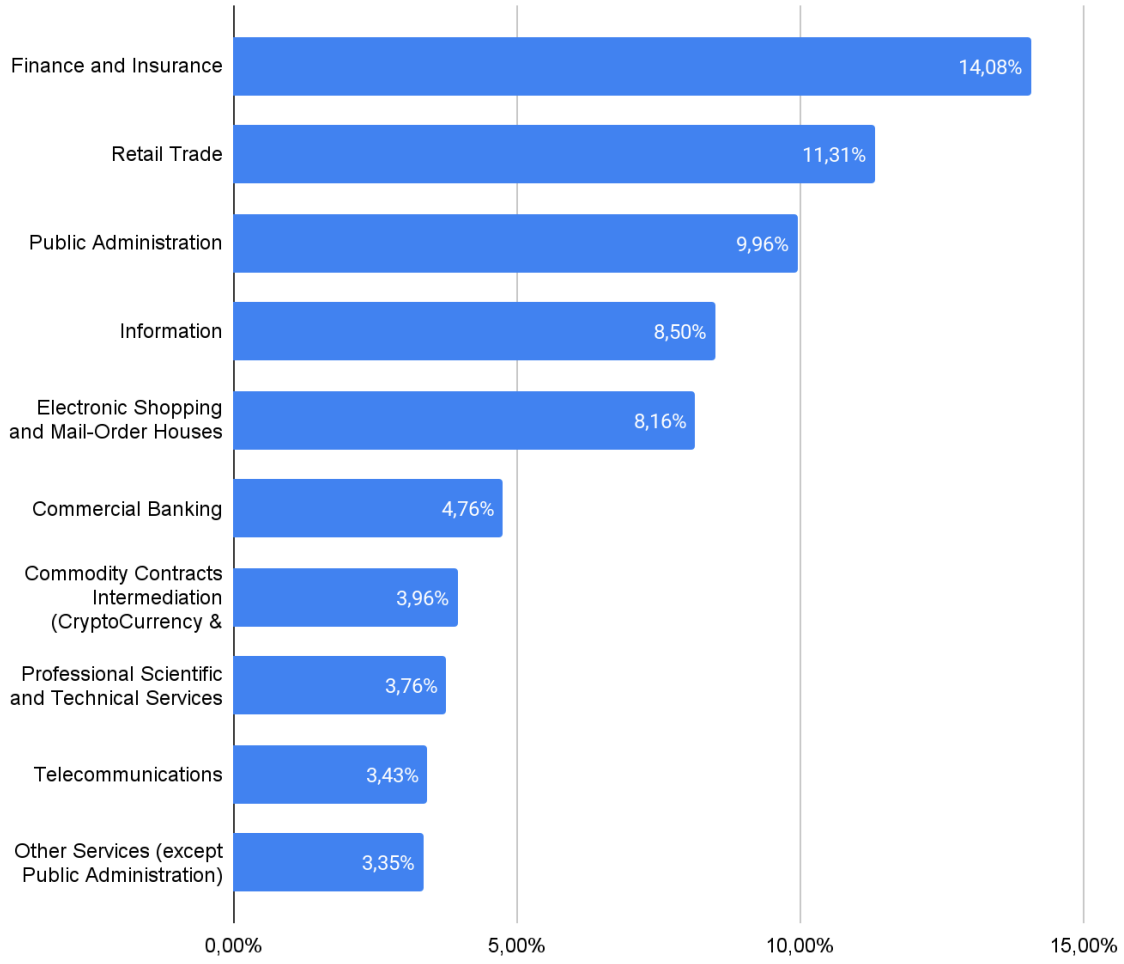
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups and so on. These are areas where threat actors with various skill sets come together, discuss, share tools and publish their alleged cyber attacks.

In the Ransomware Threats chapter you will find detailed information about ransomware actors targeting Europe, their detailed profiles and the necessary data that summarizes the ransomware activities.

The Phishing Threats chapter will show you how threat actors target various organizations with fake websites. By examining the data here, you can take the necessary steps to prevent your employees from falling into threat actors' traps.

Dark Web Threats Targeting Europe

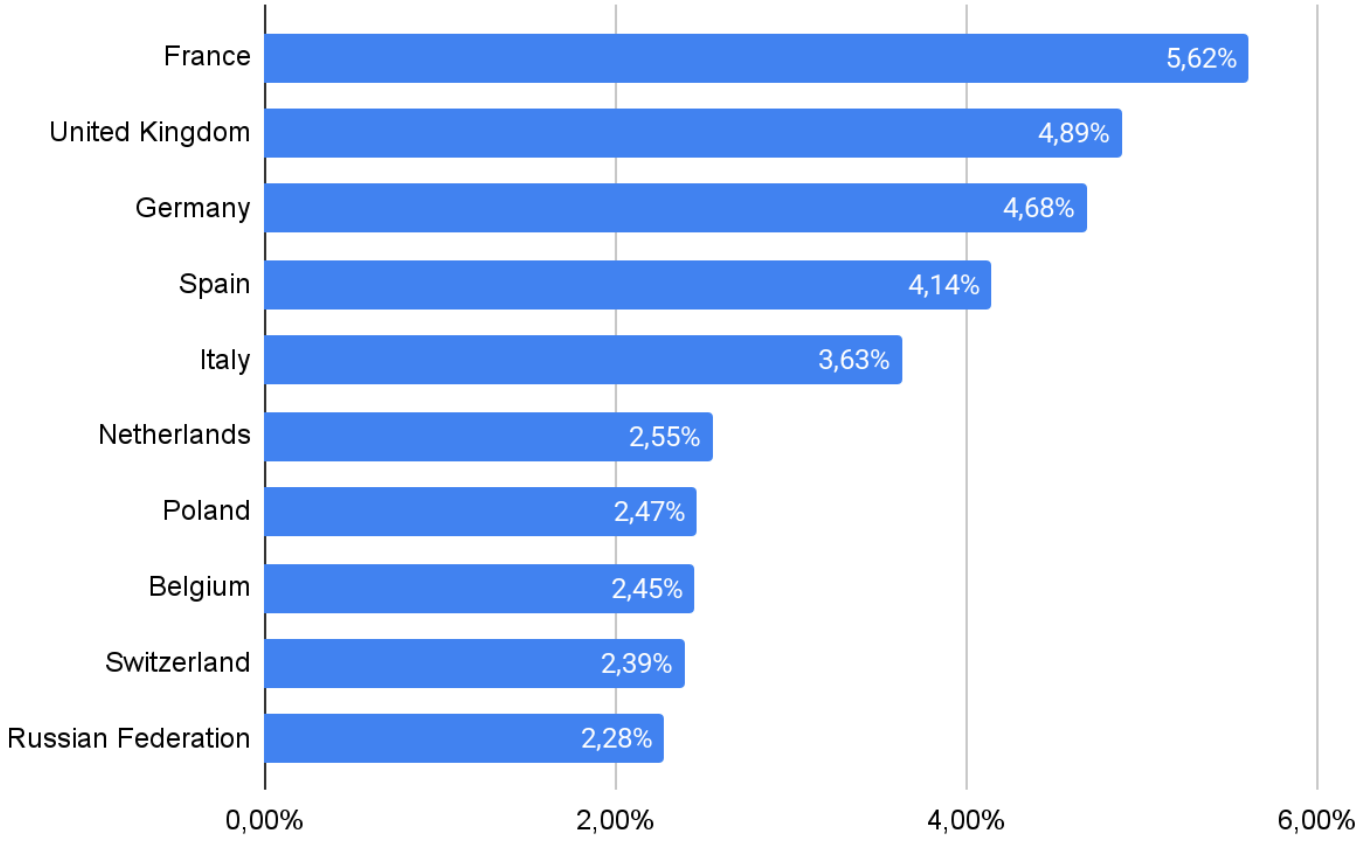
Industry Distribution of Dark Web Threats



Dark web threat activity clusters in sectors with fast cash-out paths. The Finance and Insurance industry leads with 14.08%. When we include Commercial Banking and crypto intermediaries, finance exposure reaches 22.8%. Actors chase direct monetization: account takeover, wire fraud, and sale of credentials. Retail and e-commerce together add 19.5%, another payment-rich target. Stolen cards, loyalty points, and checkout accounts drive carding and refund fraud.

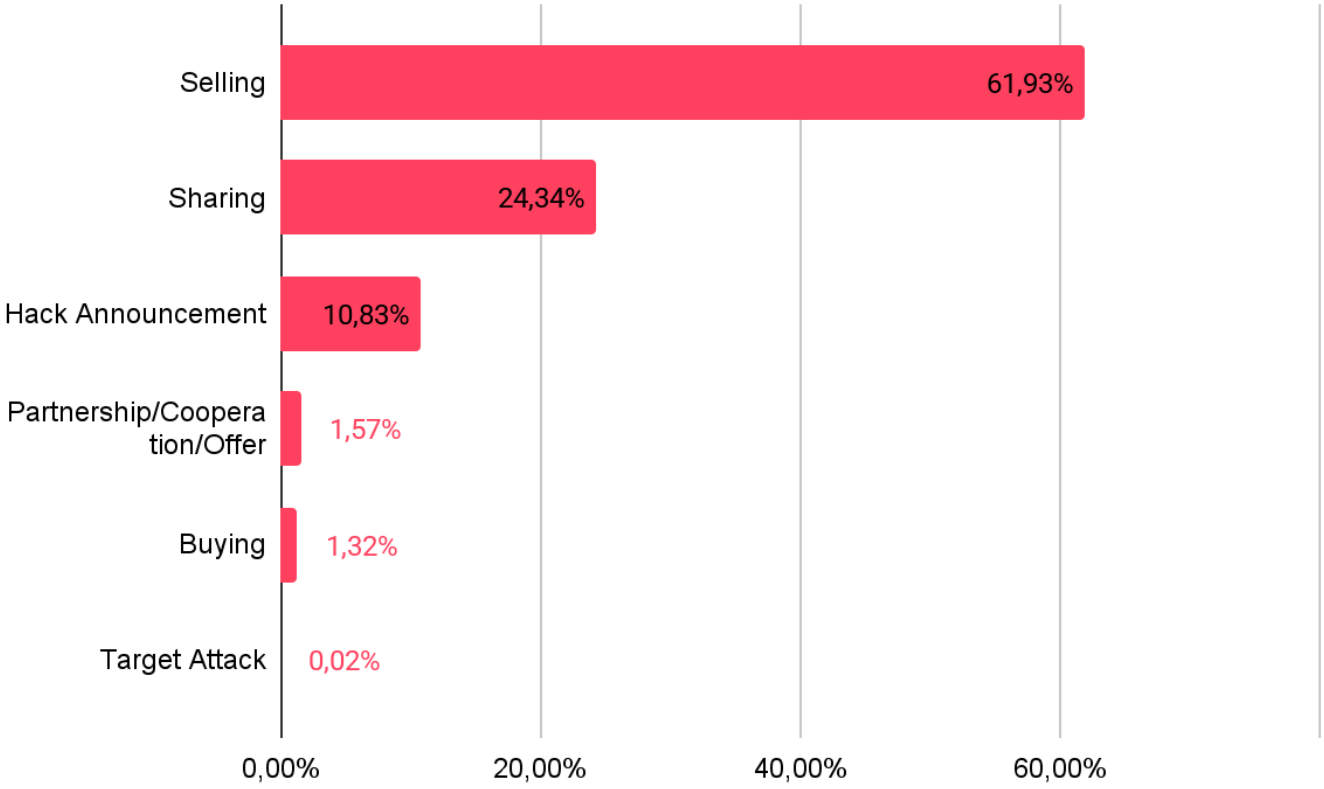
Public Administration sits near 10%. Leaks here often include identity data, internal emails, and access tokens that attackers can reuse across agencies. The Information sector follows close behind, likely for subscriber data and API keys that unlock other services.

Distribution of Dark Web Threats by Target Country



Threat actors on the dark web focus heavily on Western European economies. France tops the list with 5,62%, followed by the United Kingdom at 4,89% and Germany at 4,68%. These countries combine strong digital adoption with large financial and retail markets, which makes them attractive for fraud and credential theft. Spain and Italy, both above 3,5%, also show steady targeting, likely linked to their large consumer bases and high online payment activity.

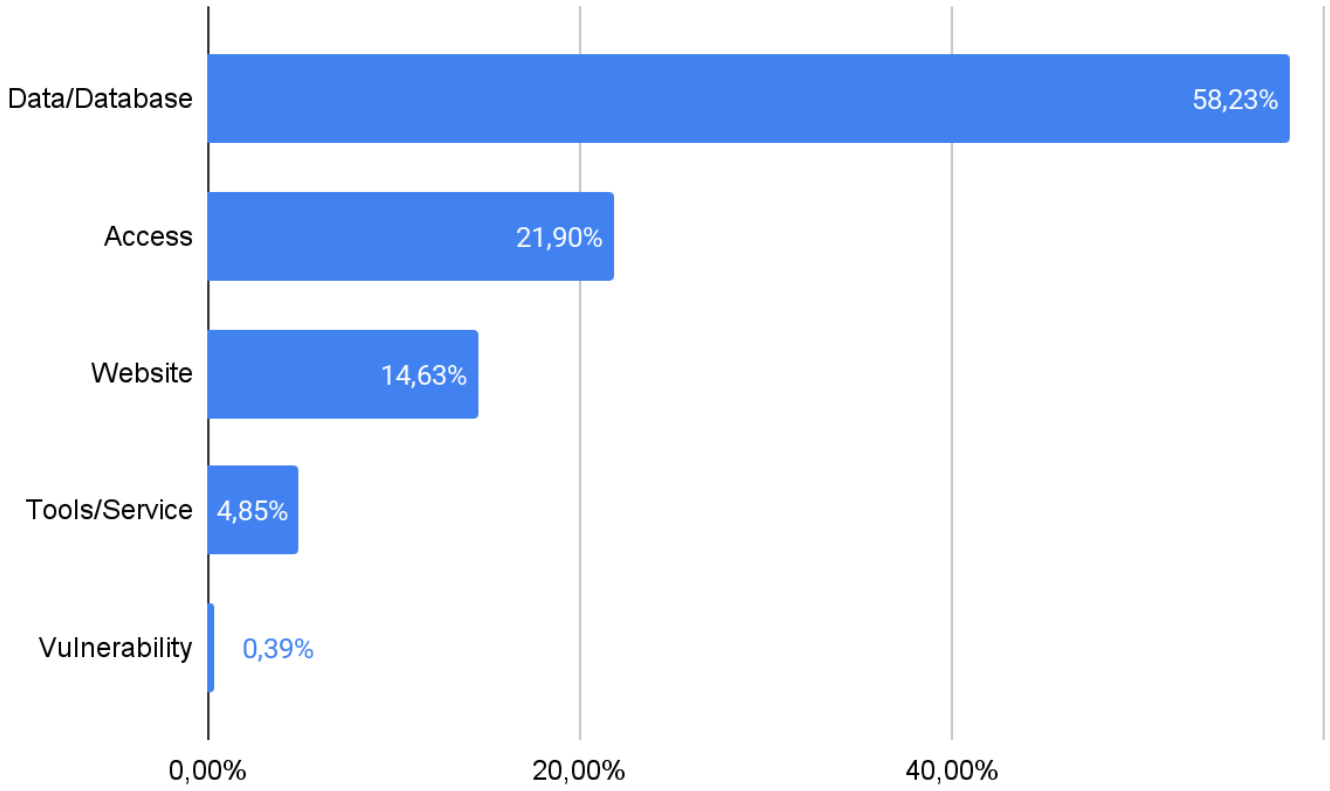
Distribution of Dark Web Threats by Threat Categories



The dark web ecosystem is still dominated by monetization. Selling makes up 61,93% of all activity, showing that threat actors focus on trading stolen data, credentials, malware, and access to systems. This underlines the maturity of underground markets, where criminal groups act much like regular vendors.

Sharing comes second at 24,34%. While it does not generate direct income, it helps attackers build reputation, gain trust, and spread tools that later support paid operations. Hack announcements account for 10,83%, often used to prove capability or advertise fresh breaches before selling the data.

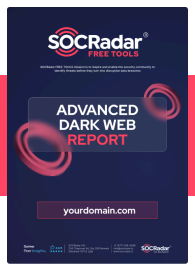
Distribution of Dark Web Threats by Threat Type



Data dominates the dark web threat landscape, making up 58,23% of activity. Leaked databases, stolen credentials, and personal records remain the most traded assets. These datasets fuel identity theft, fraud, and further intrusions.

Access listings stand at 21,90%, showing how initial access brokers play a central role. Selling entry into corporate networks or compromised accounts allows other actors to launch ransomware or data theft campaigns. Together, data and access form over 80% of observed threats, proving that attackers value both the end product and the entry point.

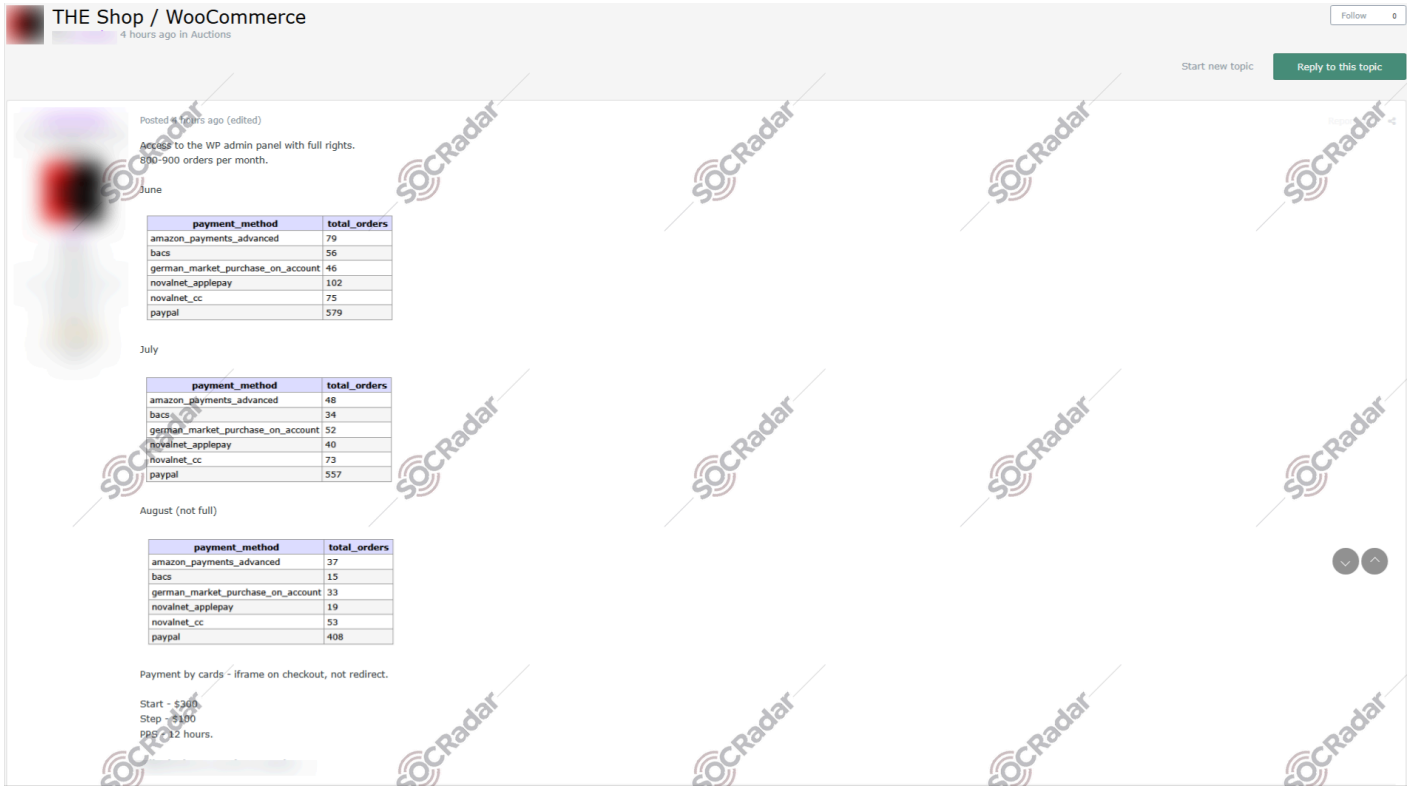
Website-related threats account for 14,63%. These often include defacements, cloned pages, or exploits aimed at e-commerce and service portals. They can serve both as direct fraud vectors and as a way to harvest more data.



Is Your Organization Exposed on the Dark Web?
Get your **free report** now and stay ahead of cyber threats: ***SOCRadar's Free Dark Web Report***

Recent Dark Web Activities Targeting Entities in Europe

The Alleged Unauthorized WordPress Access Sale is Detected for a German E-Commerce Company

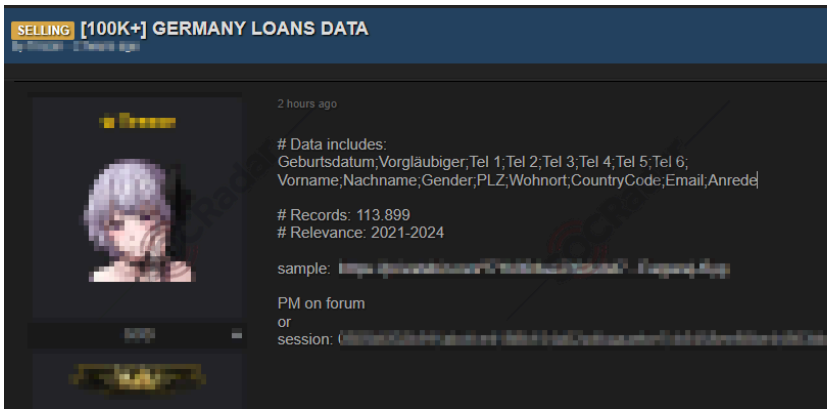


SOCRadar has identified a new post on an underground forum advertising unauthorized access to a WordPress-based e-commerce platform allegedly operating in Germany.

The listing claims to offer administrator-level credentials to the company's WordPress backend. According to the seller, the compromised store processes 800 to 900 orders per month, with order data cited from June, July, and part of August.

Payment processing is reportedly handled via card transactions through an embedded iframe on the checkout page, rather than through redirection to a third-party gateway — a setup that could expose sensitive customer and payment data if the access were abused.

The seller opened bidding at $300, with increments of $100 and a "pay-per-step" (PPS) timeframe of 12 hours.



An Alleged Loan Database of Germany is on Sale

SOCRadar has observed a new listing on a monitored underground forum advertising the sale of a loan-related database allegedly tied to individuals in Germany.

According to the post, the dataset contains 113,899 records spanning the period 2021–2024. Some of the leaked fields are date of birth, telephone numbers, first and last name, gender, postal code, residence, and email.

A sample was shared by the seller to demonstrate authenticity. The actor indicated that access could be arranged either via private messaging on the forum or through Session.

Alleged Database of a French Bank is on Sale

SOCRadar has identified a new underground forum post advertising the sale of a database allegedly linked to a banking company in France.

According to the listing, the files for sale reportedly include:

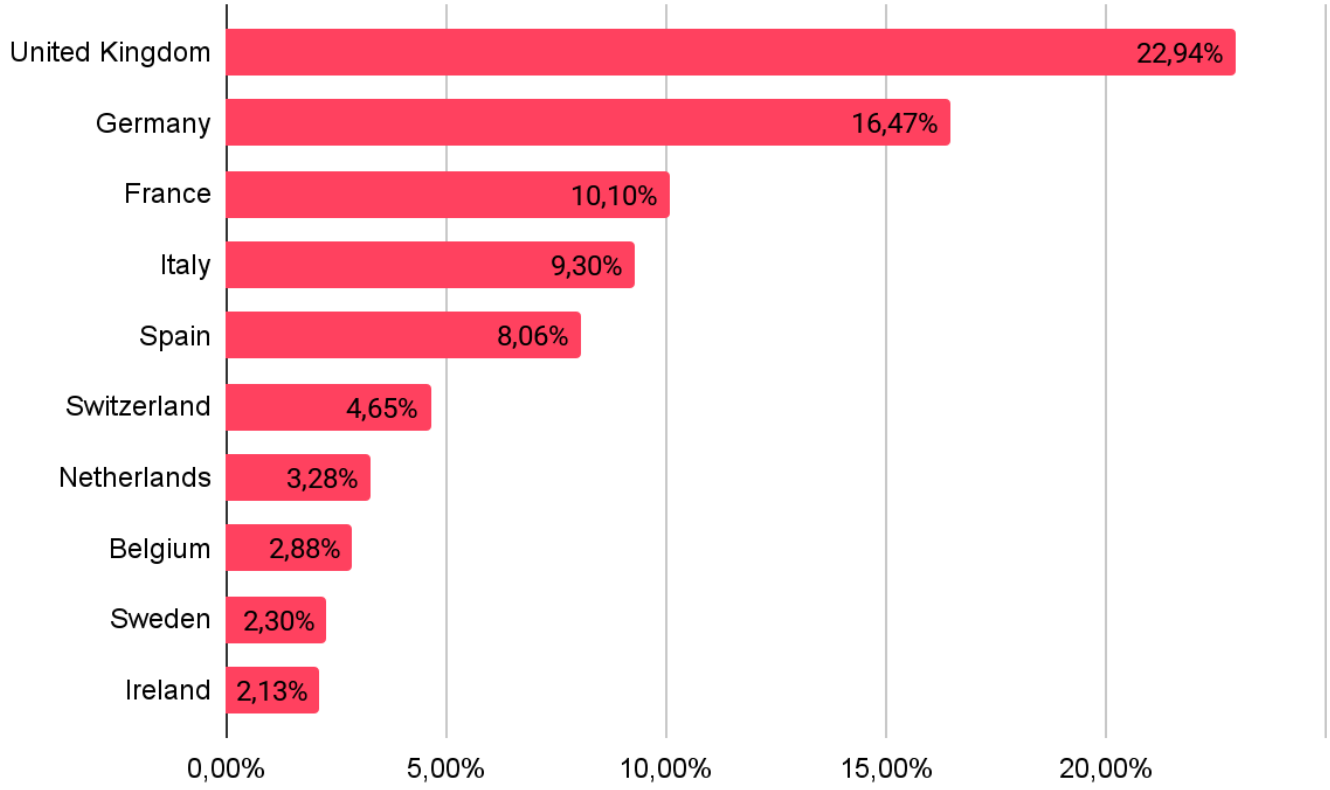
- Phone numbers
- Bank card codes
- Addresses
- Emails containing codes
- International Bank Account Numbers (IBANs)

The seller further claims that 6,000 client files have already been exploited, and that they also hold access to 10,000 additional email accounts tied to popular platforms such as Netflix, Amazon, and Booking.com.

The actor invites interested buyers to initiate contact via direct message or Telegram, specifying that transactions will be accepted only in cryptocurrency.

Ransomware Threats Targeting Europe

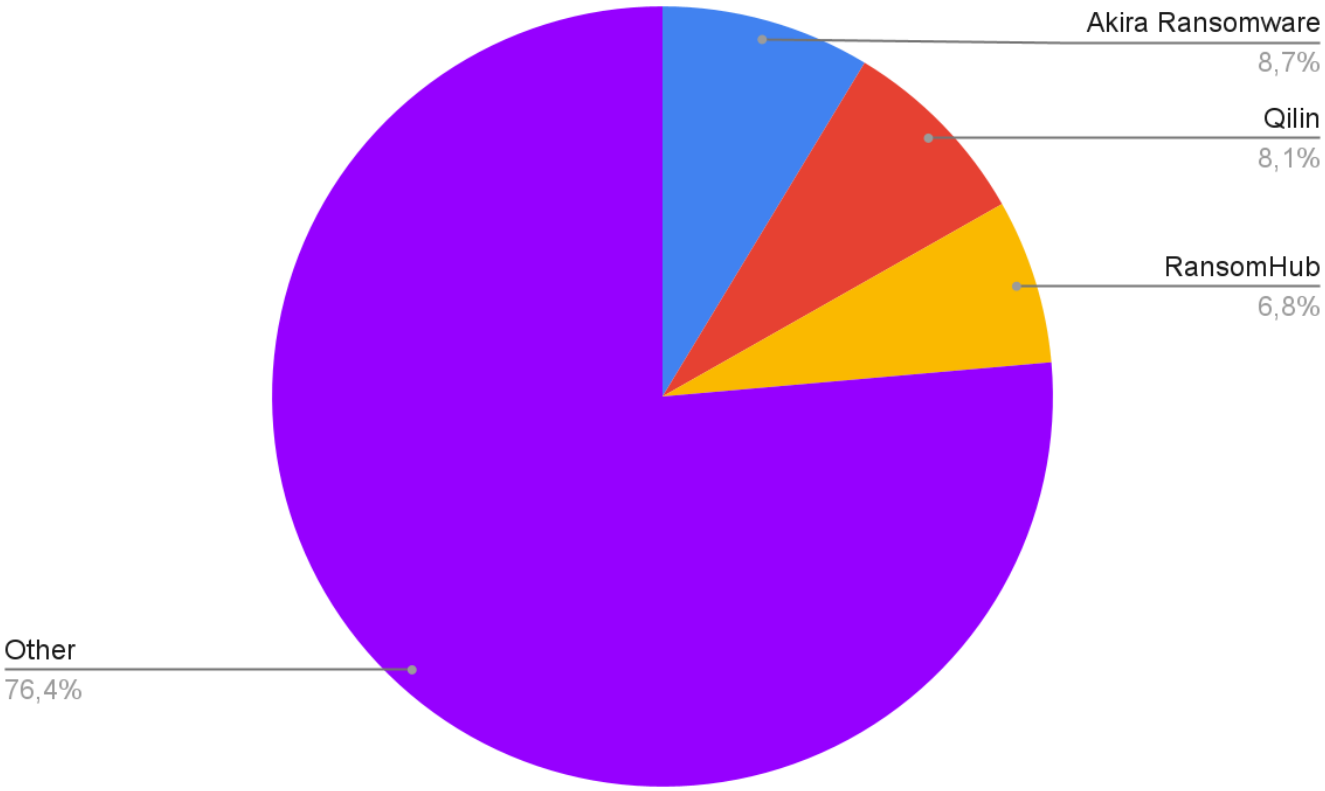
Distribution of Ransomware Attacks by Primary Target Country



Ransomware operators focus on Europe's largest economies. The United Kingdom leads with 22,94%, followed by Germany at 16,47% and France at 10,10%. Together, these three account for nearly half of all recorded attacks. Their strong digital dependence, large corporate sectors, and wide use of online services make them attractive targets for high-impact extortion.

Italy and Spain also face significant pressure, at 9,30% and 8,06%. Both countries host large manufacturing and service industries, which ransomware groups often disrupt to create operational and financial damage. Switzerland, at 4,65%, remains a consistent target due to its financial institutions and cross-border businesses.

Top Ransomware Groups Targeting Europe

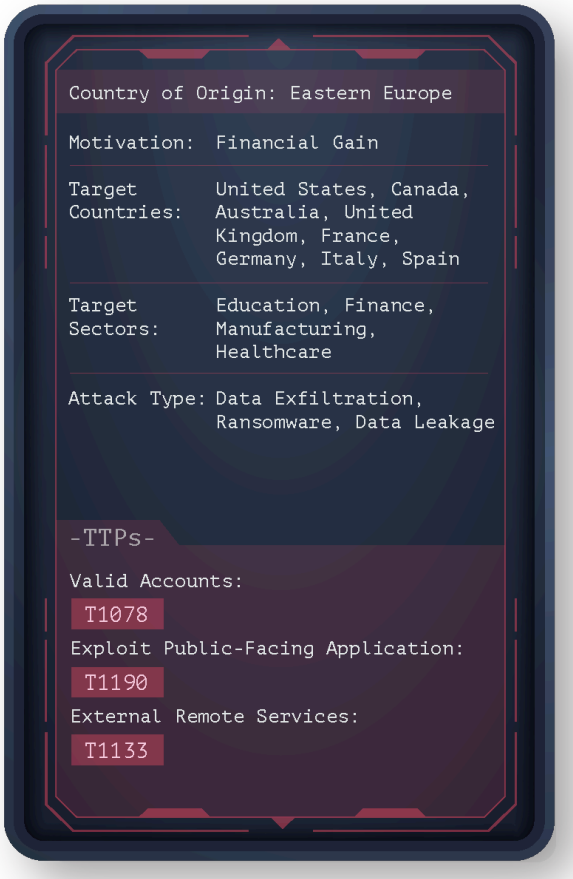


The ransomware ecosystem in Europe remains fragmented, with no single group dominating. Akira Ransomware leads with 8,7% of attributed attacks, followed closely by Qilin at 8,1% and RansomHub at 6,8%. Each of these groups has built visibility through high-profile breaches, but none controls a large share of the market.

The “Other” category accounts for 76,4%, showing that dozens of smaller or short-lived groups operate in parallel. This fragmentation makes the threat landscape harder to track, since groups often rebrand or splinter to avoid detection and sanctions.

A Closer Look into The Top 3 Ransomware Groups

Akira Ransomware



Since its discovery in early 2023, Akira ransomware has evolved from a seemingly ordinary addition to the ransomware landscape to a significant threat affecting many businesses and critical infrastructure entities.

The ransom group employs a double extortion strategy, first exfiltrating data and then encrypting devices within the targeted network. Payment is then demanded not only for decrypting files but also for preventing the exposure of leaked data.

The Akira ransomware group frequently demands hefty ransoms, primarily targeting large enterprises across North America, Europe, and Australia. The malware typically spreads through targeted threat campaigns using phishing emails or exploiting software vulnerabilities, focusing on industries such as education, finance, manufacturing, and healthcare.

You can visit our ***blog post*** to read the rest of the threat actor profile.

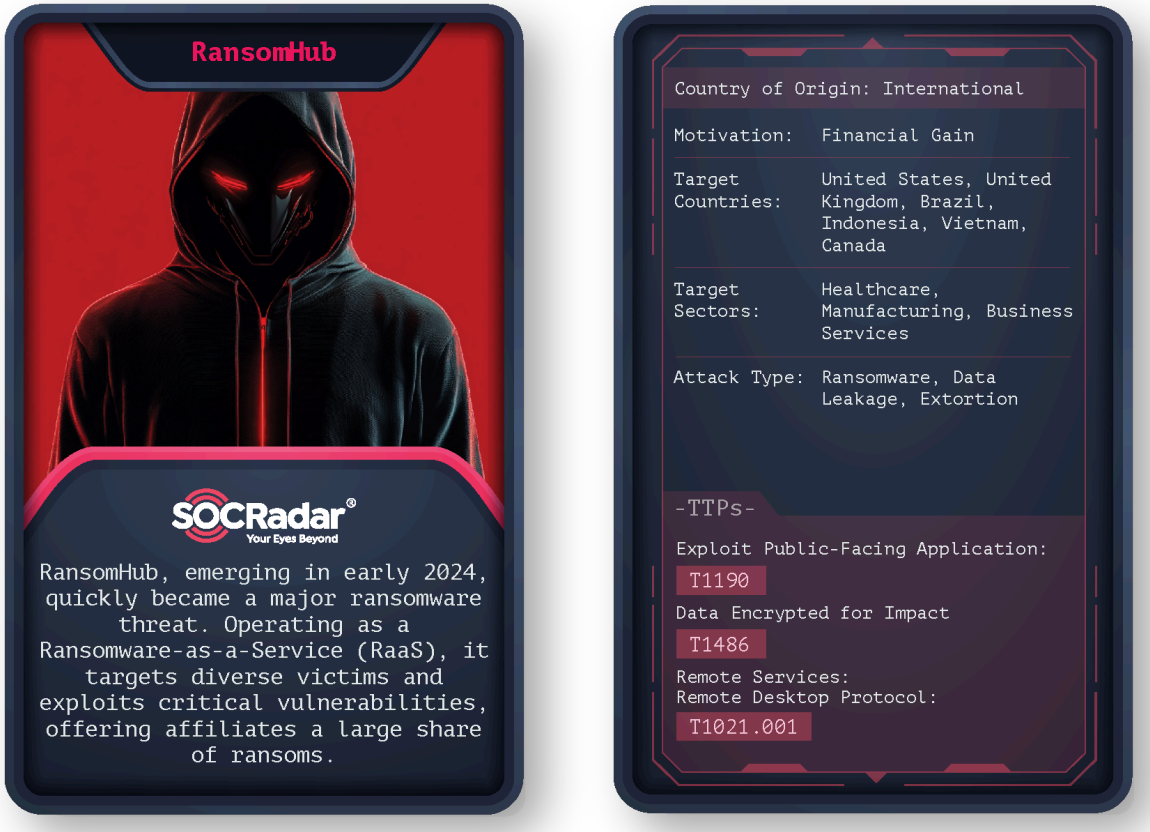
Qilin Ransomware

Qilin, also known as Agenda ransomware, represents a formidable threat in cybercrime. This ransomware, one of the known Ransomware-as-a-Service (RaaS) groups, is designed with adaptability in mind, allowing it to customize attacks based on its victims' specific environments. Originating from a sophisticated background, Qilin leverages advanced tactics to extort organizations.

The primary objective of Qilin ransomware is financial gain through extortion. It targets organizations across various sectors, with a particular focus on healthcare and education. These sectors are often chosen due to their reliance on critical data and the generally lower levels of cybersecurity compared to more financially-focused industries. By encrypting essential files and demanding a ransom for their decryption, Qilin aims to create significant operational disruptions, compelling victims to pay the demanded ransom to restore their systems.

You can visit our blog post to read the rest of the threat actor profile.

RansomHub



As stated on the group's About page, RansomHub is comprised of hackers from various locations united by a common goal of financial gain. The gang explicitly mentions prohibiting attacks on specific countries and non-profit organizations. In February 2024, RansomHub posted its first victim, the Brazilian company YKP.

The gang's website states that they refrain from targeting CIS, Cuba, North Korea, and China. While they suggest a global hacker community, their operations notably resemble a traditional Russian ransomware setup. Their stance on Russian-affiliated nations and the overlap in targeted companies with other Russian ransomware groups are also worth noting.

You can visit our ***blog post*** for more detailed information about RansomHub.

Recent Ransomware Attacks Targeting Entities in Europe

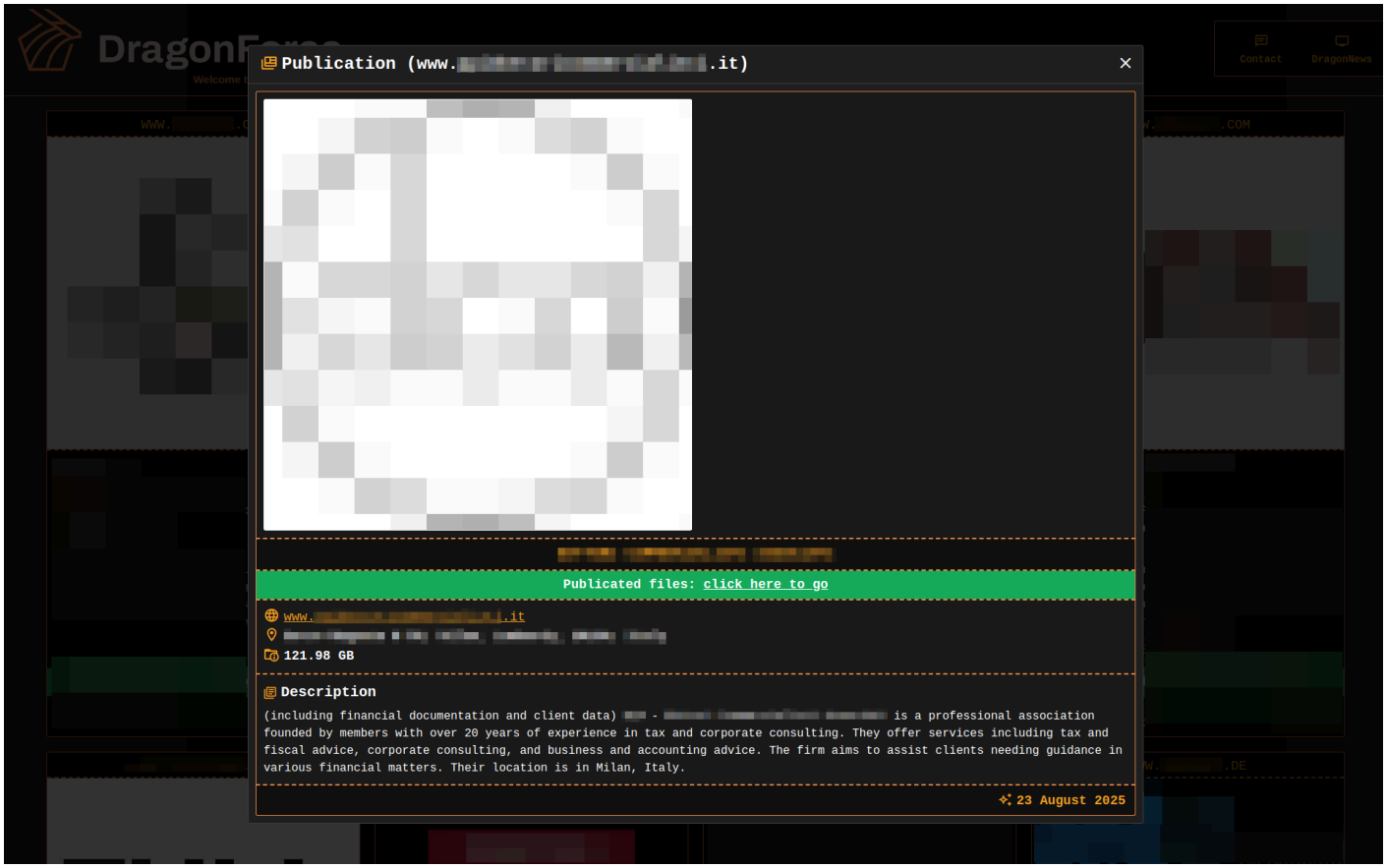
Qilin Ransomware Targets Spanish Packaging Manufacturer

The Qilin ransomware group has claimed responsibility for a cyberattack against a family-owned Spanish manufacturer specializing in corrugated cardboard and packaging solutions.

Leaked materials on the group's site include a variety of sensitive corporate documents:

- Utility bills and financial records
- An internal equality and workforce plan containing demographic and salary statistics
- Technical maintenance reports with contractor bank details, order numbers, and staff information
- Historical financial statements from affiliated entities
- Approved process flow diagrams from the company's food safety and quality assurance system (HACCP)

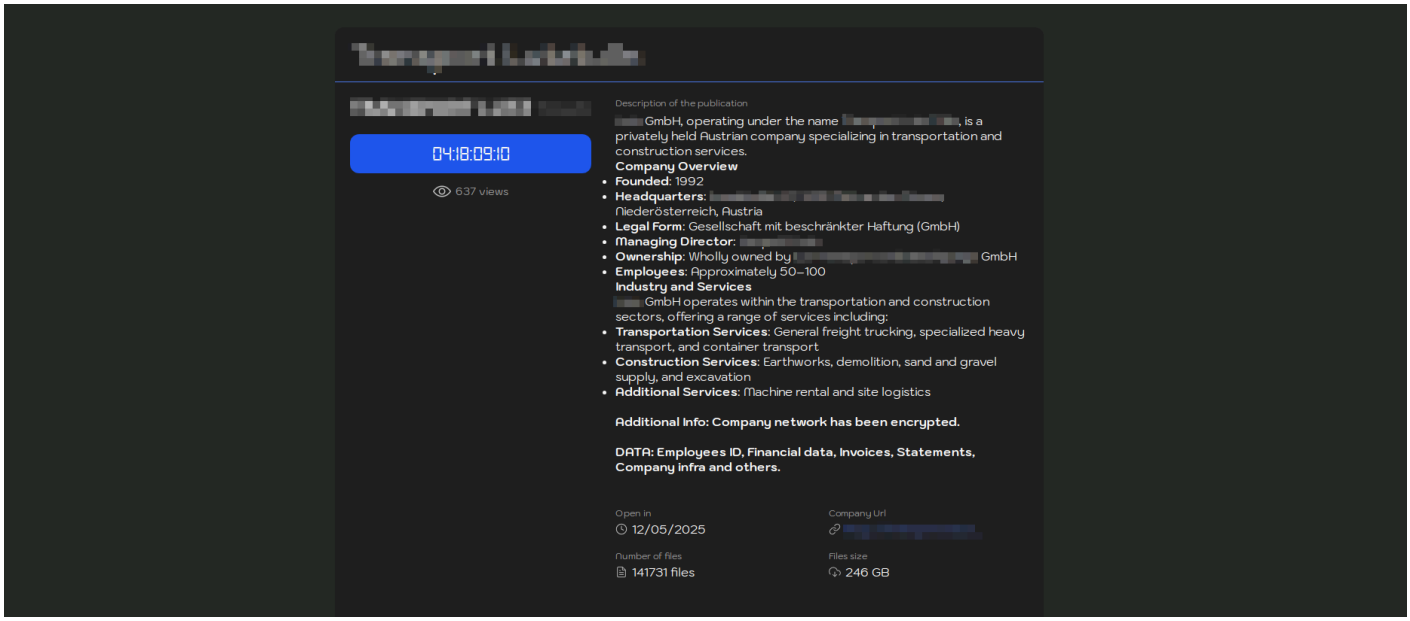
DragonForce Ransomware Targets Italian Tax and Corporate Consulting Firm



The DragonForce ransomware group has claimed responsibility for an attack on a Milan-based professional association specializing in tax, corporate, and business consulting services.

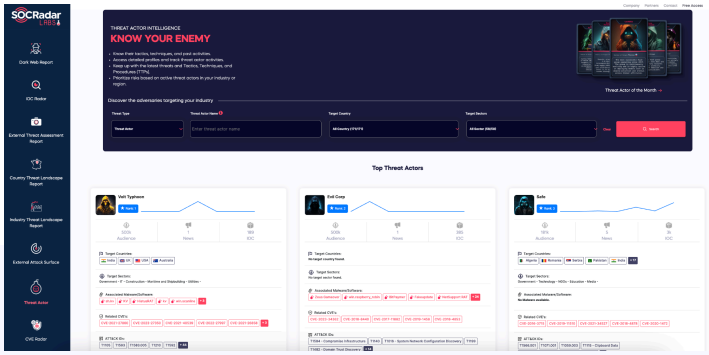
According to the group, the leaked data includes financial documentation and client information, raising concerns over the potential exposure of sensitive records belonging to individuals and businesses that relied on the firm for tax and accounting guidance.

Orca Ransomware Hits Austrian Transportation and Construction Firm



The Orca ransomware group has claimed responsibility for a cyberattack on an Austrian company specializing in transportation and construction services.

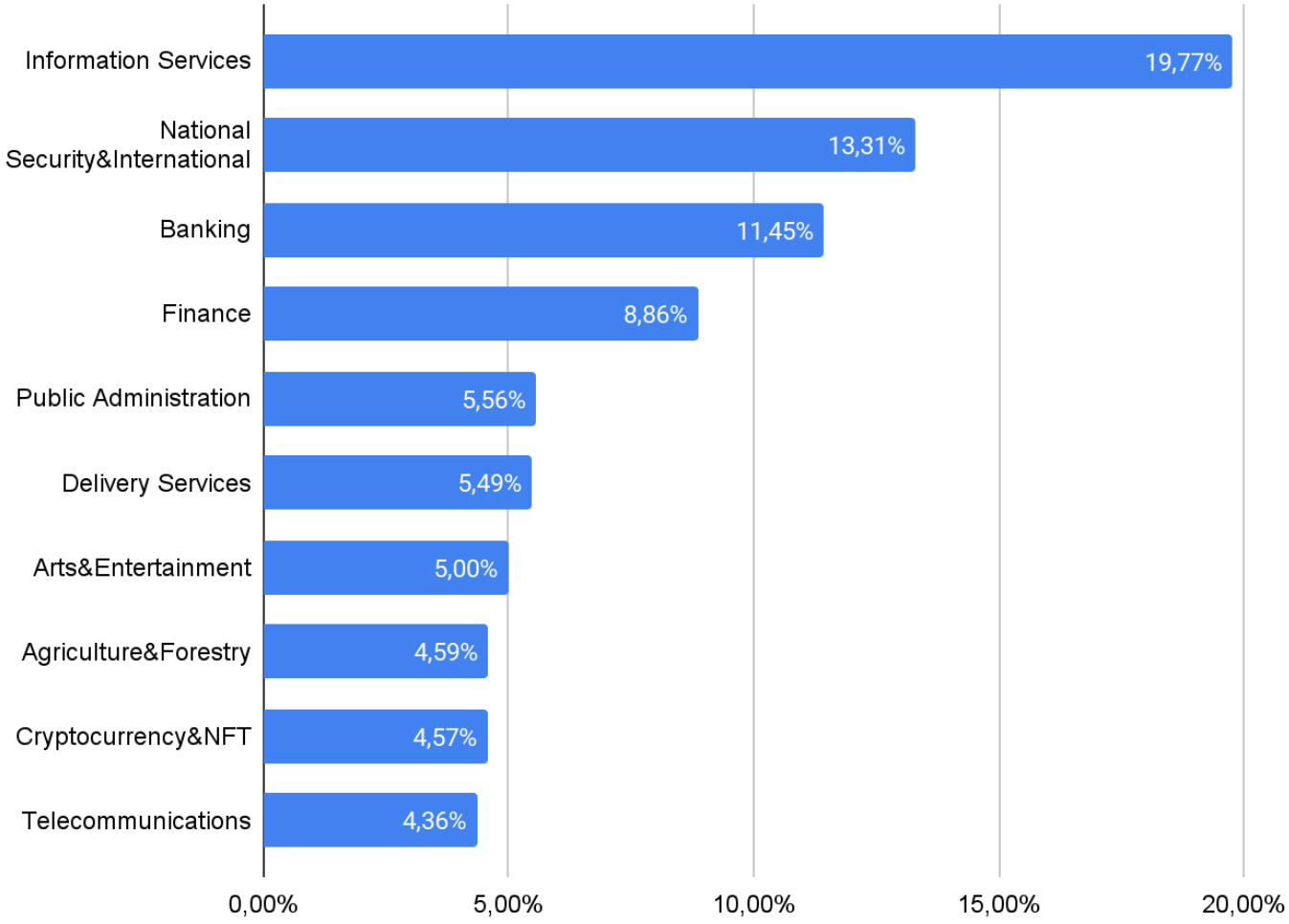
The targeted organization, based in Tulln an der Donau, provides a range of offerings including general freight trucking, heavy transport, container logistics, earthworks, demolition, and excavation, as well as sand and gravel supply and machinery rental. The firm employs an estimated 50–100 staff and plays a notable role in regional construction and logistics operations.



*SOCRadar enhances cybersecurity measures with its **Threat Actor Intelligence Module**, which features advanced Threat Actor Tracking capabilities for organizations that want to stay ahead of cyber threats in real time.*

Phishing Threats Targeting Europe

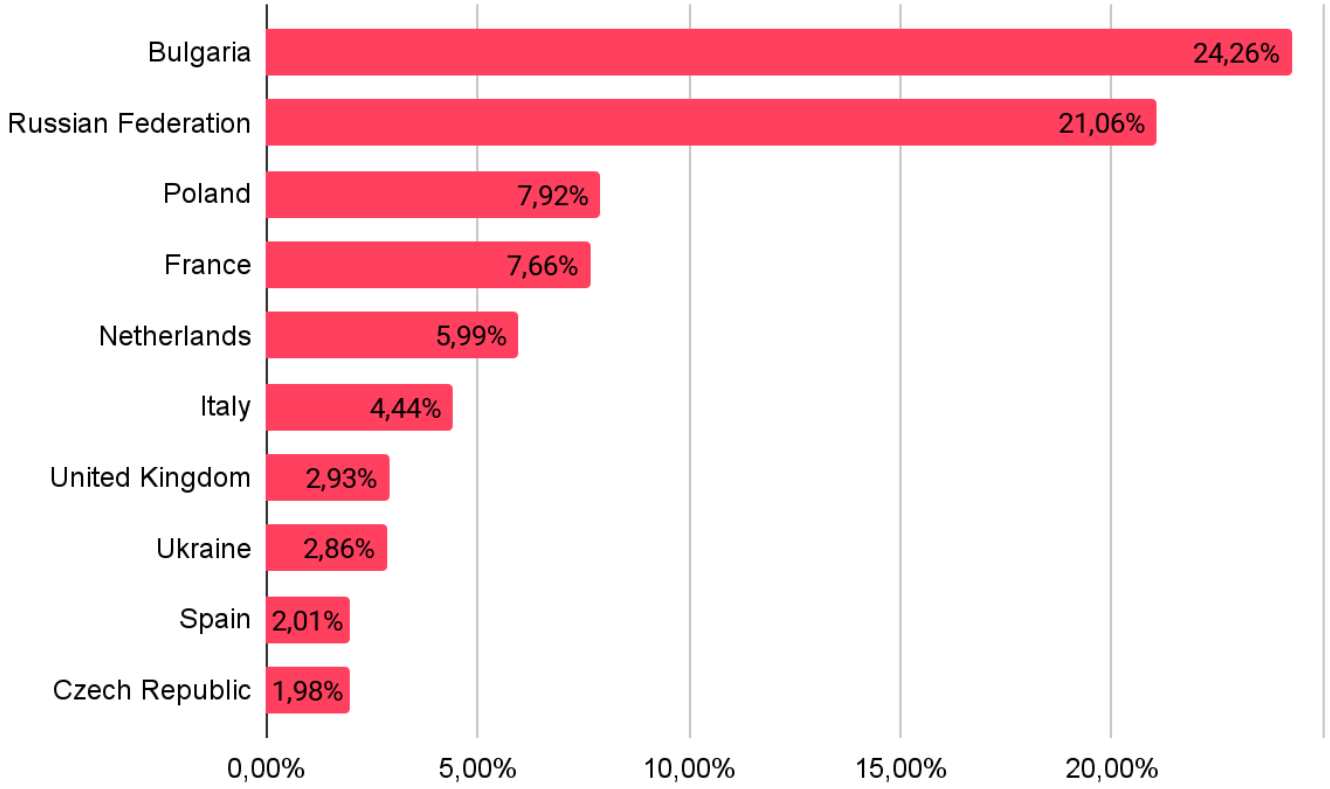
Phishing Attacks - Distribution by Industry



Phishing campaigns hit industries that combine sensitive data with high user interaction. Information Services is the top target at 19,77%, showing how attackers exploit digital platforms, cloud providers, and online services to harvest credentials and spread malware.

National Security and International Affairs follows with 13,31%. This high share points to phishing being used for espionage and influence operations, not just financial gain. Banking (11,45%) and Finance (8,86%) together make up over 20%, proving that direct access to money and payment systems remains a core driver.

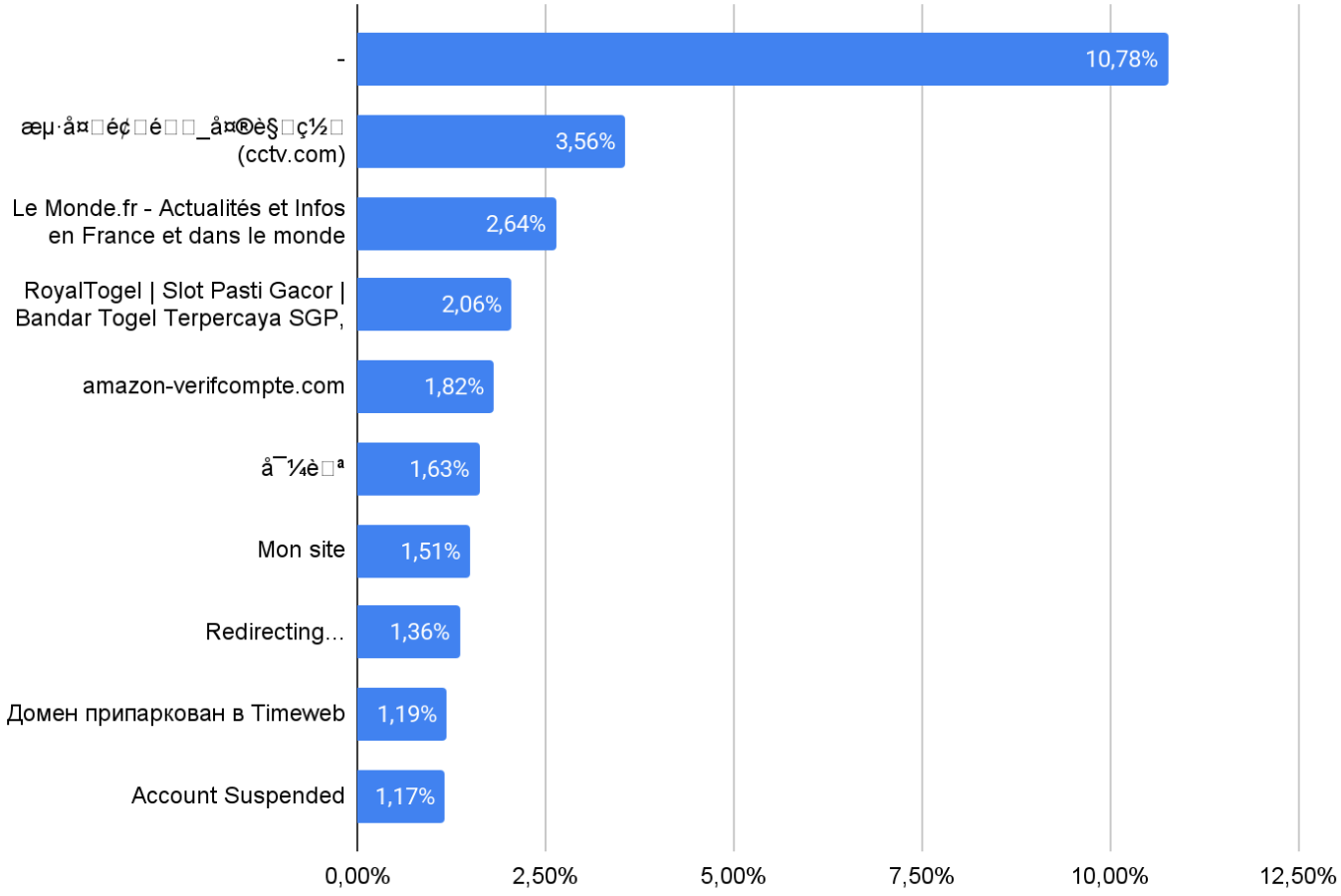
Phishing Attacks - Distribution by Target Country



Phishing activity in Europe shows a different distribution compared to ransomware. Bulgaria leads with 24,26%, followed by the Russian Federation at 21,06%. Both stand out as key hotspots, suggesting either strong local targeting or the use of infrastructure within these countries to run campaigns.

Poland and France rank next, at 7,92% and 7,66%. These numbers highlight the spread of phishing into both Eastern and Western Europe. The Netherlands (5,99%) and Italy (4,44%) also see steady activity, reflecting their roles as financial and e-commerce centers.

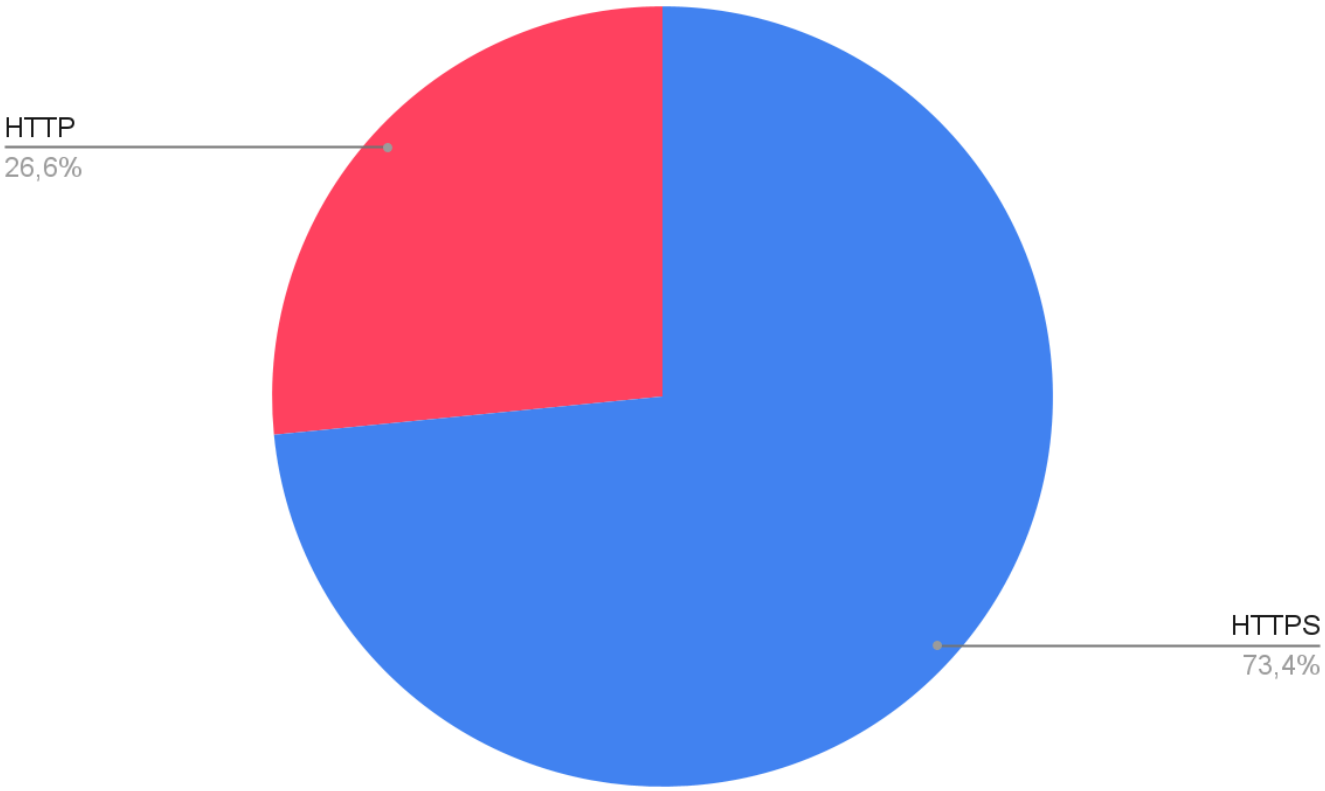
Phishing Attacks - Distribution by Phishing Page Title



Phishing pages show high variety, with many designed to look generic or poorly branded. The largest share, 10,78%, has no clear title, which reflects the use of automated kits or hastily built sites. This lack of polish does not reduce effectiveness, since many victims focus on the content of the lure rather than the page title.

Some campaigns mimic trusted media and commerce platforms. Fake references to CCTV (3,56%) and Le Monde (2,64%) show attempts to exploit news credibility for clicks and credential theft. Fraudulent gambling and lottery sites also appear, like RoyalTogel at 2,06%, which target users seeking quick financial gains.

Phishing Attacks - Distribution by SSL/TLS Protocol



Most phishing sites now use HTTPS, with 73,44% of observed pages showing a valid certificate. This reflects a clear shift in attacker tactics. Criminals take advantage of free or low-cost certificate services to make their sites look legitimate. For many users, the presence of a padlock icon is still seen as proof of safety, which attackers exploit to increase click-through and credential theft success.

HTTP-only phishing sites remain at 26,56%. These are often short-lived or mass-generated pages where attackers prioritize speed over credibility. Despite their lower share, they still pose risks, especially when spread through email or SMS where users may not check the URL closely.

Strategic Recommendations

- **Enhance Endpoint Security:** Implement advanced anti-malware, regular device audits, and employee training on safe browsing practices.
- **Strengthen Phishing Defense:** Invest in phishing detection systems, web filtering tools, and employee training on recognizing phishing attempts.
- **Enforce Multi-Factor Authentication (MFA):** Apply MFA across critical systems to protect against stolen credentials.
- **Fortify Ransomware Defenses:** Regularly back up data, segment networks, and develop incident response plans for ransomware attacks.
- **Monitor Dark Web Activity:** Use dark web monitoring to detect exposed company data early and respond quickly to breaches.
- **Collaborate on Cyber Threat Intelligence:** Share insights with industry peers and stay informed about emerging threats and new attack vectors.
- **Secure Communications and Data:** Ensure encryption for sensitive communications and transactions, and train employees on secure data handling.
- **Proactive Vulnerability Management:** Regularly apply patches and conduct penetration testing to address potential system vulnerabilities.
- **Build a Cybersecurity Culture:** Foster ongoing employee training, phishing simulations, and establish clear security policies to ensure a security-first mindset across the organization.

Who is SOCRadar?

SOCRadar provides Extended Threat Intelligence (XTI) that combines: **"Cyber Threat Intelligence, Brand Protection, External Attack Surface Management, and Dark Web Radar Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

Trusted by
21.000+ companies
in 150+ countries

Dark Web Monitoring: SOCRadar's fusion of its unique Dark Web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and Dark Web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS FOR FREE

START YOUR FREE TRIAL

Discover SOCRadar's powerful tools and easy-to-use interface to enhance cyber threat intelligence efforts. Schedule a demo with our experts to see it in action, and we'll show you what SOCRadar can do.