SOCRadar®
Your Eyes Beyond

# SOCRadar Annual

# EUROPE

## Threat Landscape Report 2024

SOCRadar®
Your Eyes Beyond

# Table of Contents

# Executive Summary

Businesses worldwide are increasingly facing the threat of severe cyberattacks as the cyber threat landscape evolves and becomes more sophisticated. This escalation in cyber threats is a global phenomenon, but Europe, with its diverse and interconnected digital economy, is particularly vulnerable. Europe's significance in global finance, technology, and industry makes it a prime target for sophisticated cybercriminal activities.

To effectively navigate these challenges, European organizations must stay informed about the specific risks and threats relevant to their region. The SOCRadar Annual Europe Threat Landscape Report offers an essential resource for understanding these regional cyber threats and potential dangers. This report provides detailed insights into recent ransomware attacks, phishing schemes, and Dark Web activities specific to Europe. It equips businesses with the critical information needed to bolster their cybersecurity defenses.

For any organization operating within Europe or interacting with European entities, leveraging SOCRadar's Annual Europe Threat Landscape Report is crucial. With SOCRadar's support, businesses can safeguard operations and ensure long-term protection against cyberattacks in an increasingly challenging landscape.

# Top Takeaways

Retail Trade is the most targeted industry in Europe, accounting for **21,02%** of all posts on Dark Web forums monitored by SOCRadar. The Electronic Shopping and Mail-Order Houses industry takes second place, while the Information sector ranks third.

The United Kingdom was the most targeted country in Europe, accounting for **19,48%** of all Dark Web posts. France was second, and Spain came in third.

Ransomware groups in Europe most targeted the Manufacturing industry, accounting for **30,49%** of all attacks. The Information industry took the second spot, while Professional, Scientific, and Technical Services ranked third.

Ransomware groups most targeted the United Kingdom in Europe, with **30.33%** of the attacks targeting organizations there. Germany was in second place, and France ranked third.

Our analysis shows that the most active ransomware group targeting the European region was LockBit (all versions combined), responsible for **24,5%** of all attacks. The second most active group was 8Base and in third place, Black Basta appeared.


The majority of the data from stealer logs belong to users from the Netherlands. They allocate **14,43%** of the stealer log data. In second place, we have Norway and in the third, Belgium.

Latvia suffered a heavy DDoS attack spree this year. When we don't include the attacks on Latvia, we see that attacks lasted an average of **19** minutes for the rest of Europe. When we do, the time frame jumps to **101** minutes on average.

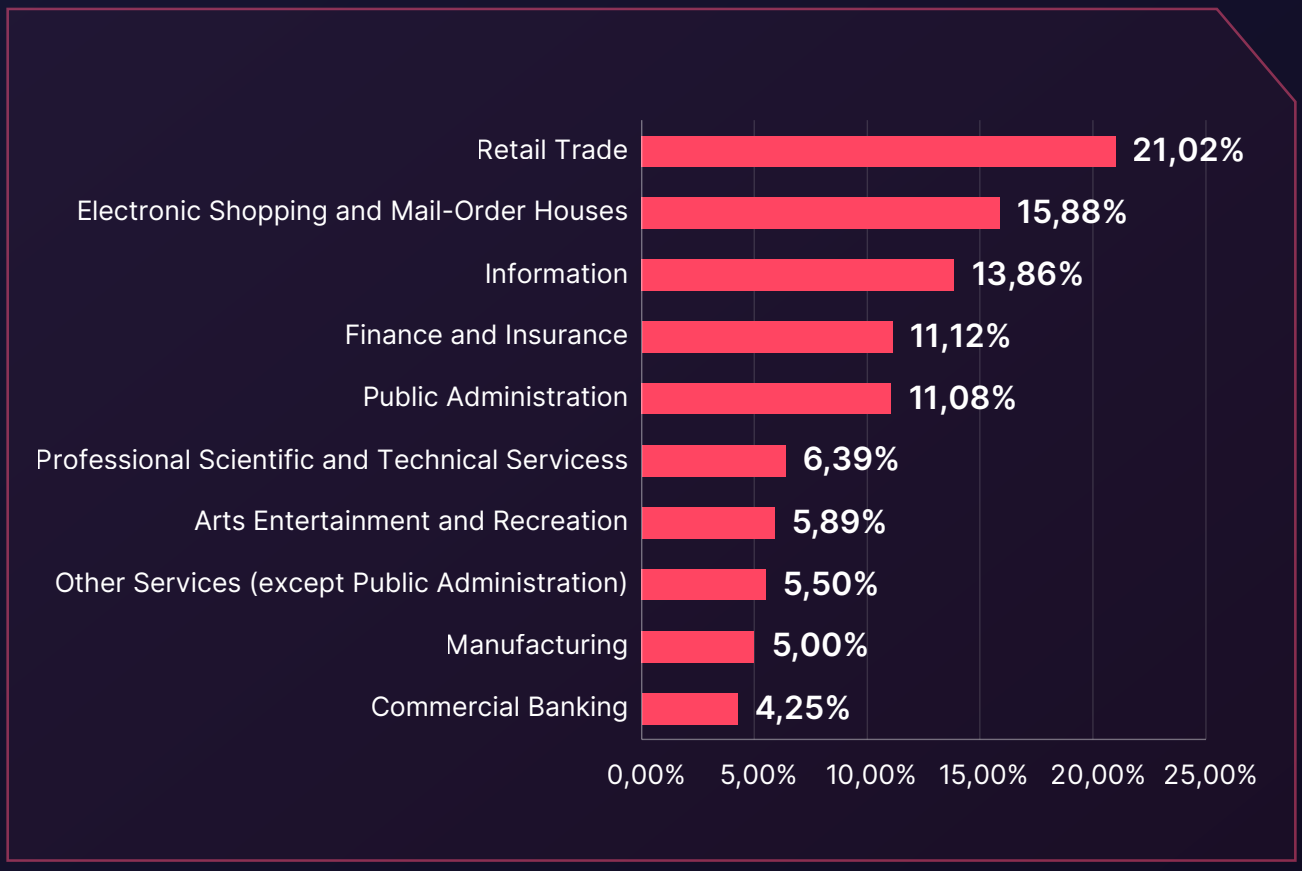
# Technical Details

In the past year, SOCRadar's Dark Web Analysts closely monitored the Dark Web to identify patterns related to threat actors' actions against European enterprises.

In 2023 and 2024, businesses faced a continuous bombardment of cyberattacks. SOCRadar detected 4,428 Dark Web forum posts targeting Europe during this time, and 1,581 threat actors were linked to them.

## Dark Web Threats Targeting Europe

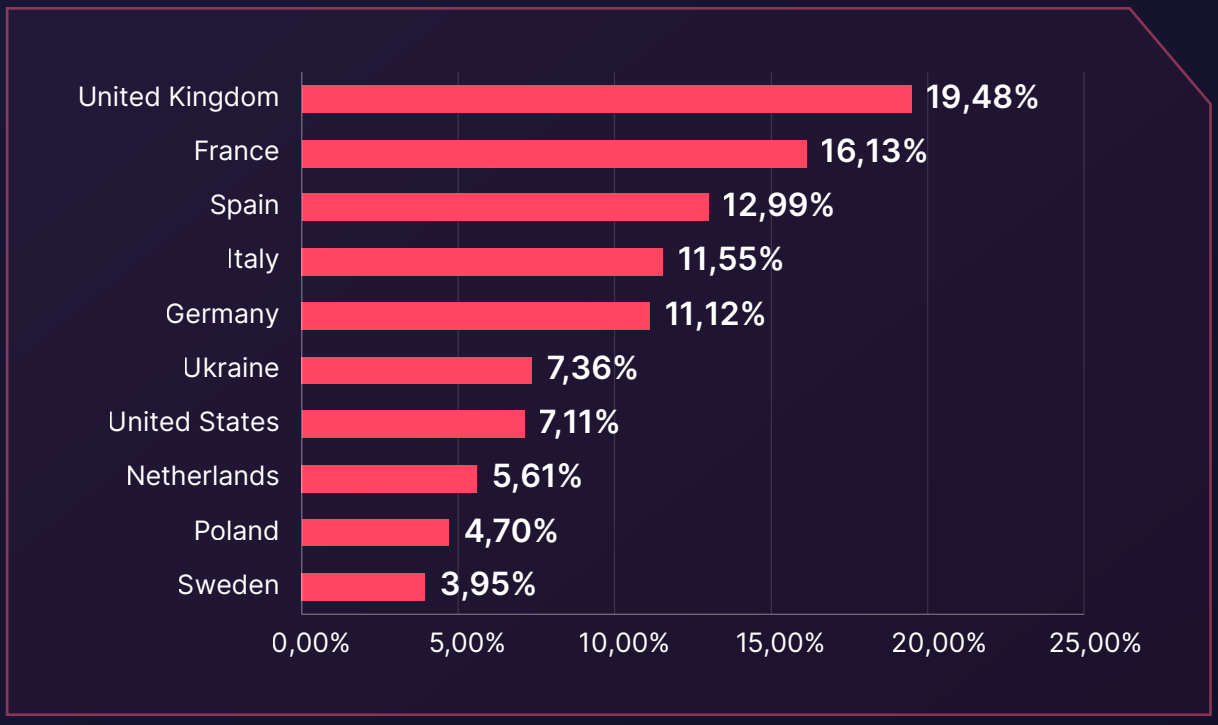
### Industry Distribution of Dark Web Threats




*Most targeted industries in the European Region based on the Dark Web forum posts monitored by SOCRadar*

**Retail Trade** is the most targeted industry in Europe, accounting for **21,02%** of all posts on Dark Web forums monitored by SOCRadar. The **Electronic Shopping and Mail-Order Houses** industry takes second place with **15,88%** of the posts, while the **Information** sector ranks third with **13,86%** of all Dark Web forum posts.

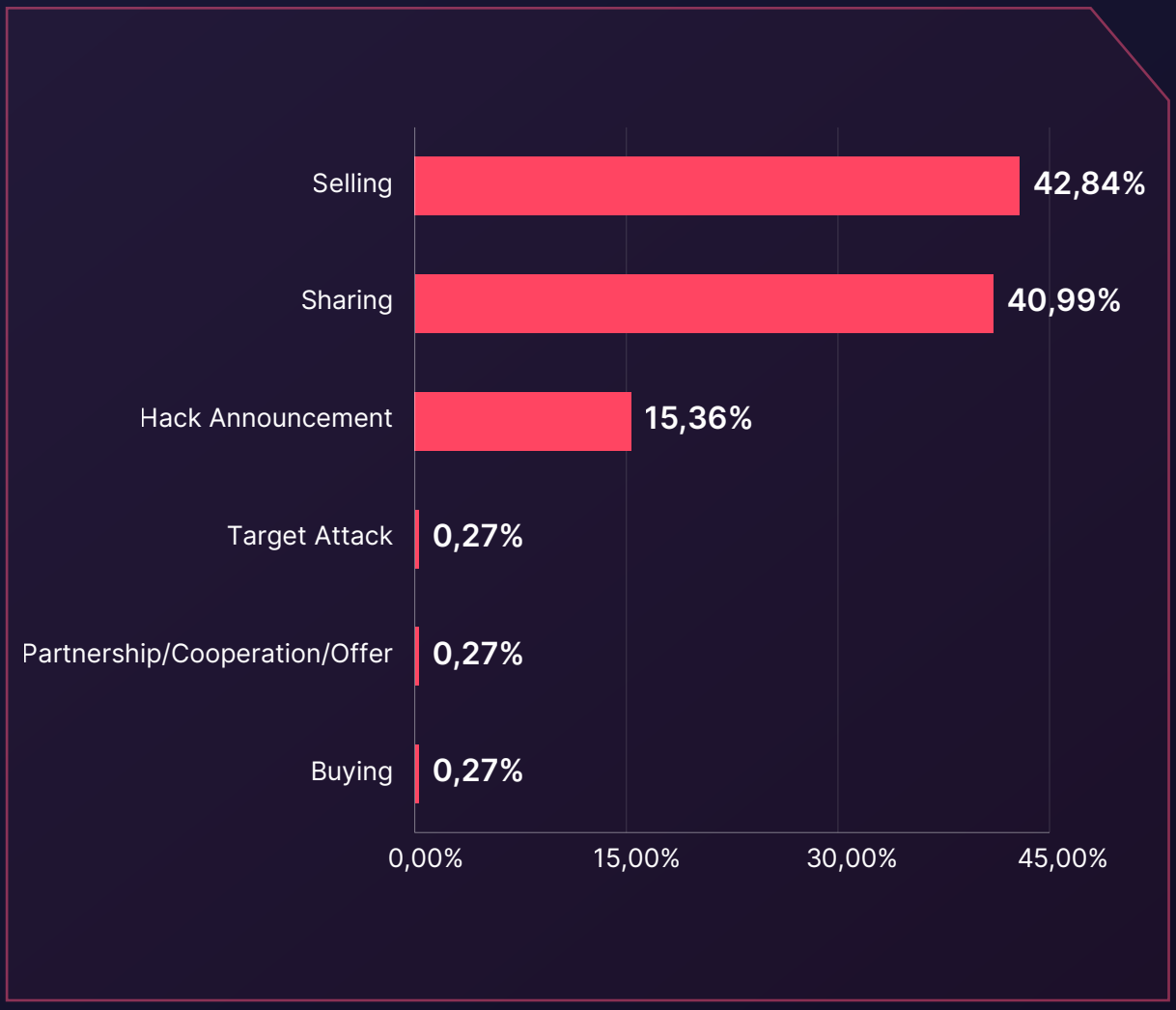
## Distribution of Dark Web Threats by Primary Target Country




*Most targeted countries in the European Region based on the Dark Web forum posts monitored by SOCRadar*

The **United Kingdom** was the most targeted country in Europe, accounting for **19,48%** of all Dark Web posts. **France** was second, with **16,13%** of the posts targeting it. **Spain** came in third, with **12,99%** of the posts targeting Spanish organizations

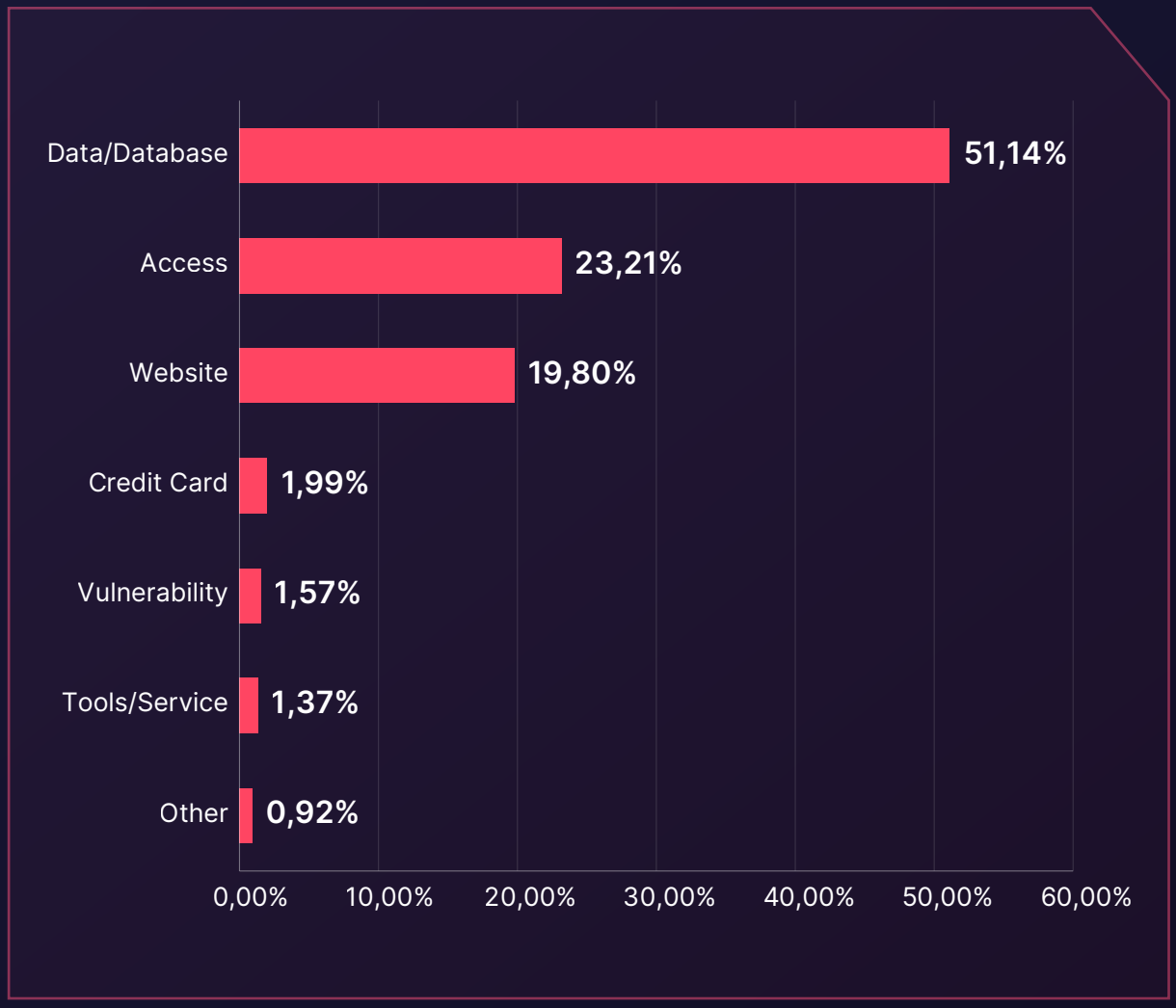
## Distribution of Dark Web Threats by Threat Categories




*Category based analysis of the Dark Web forums monitored by SOCRadar*

Threat actors targeting Europe mostly sold the product of their illicit activities. The **"Selling"** category is in first place, comprising **42,84%** of all posts from Dark Web forums. The **"Sharing"** category follows with **40,99%** of the posts. In third place are **"Hack Announcements,"** which account for **15,36%** of the posts.

## Distribution of Dark Web Threats by Threat Type

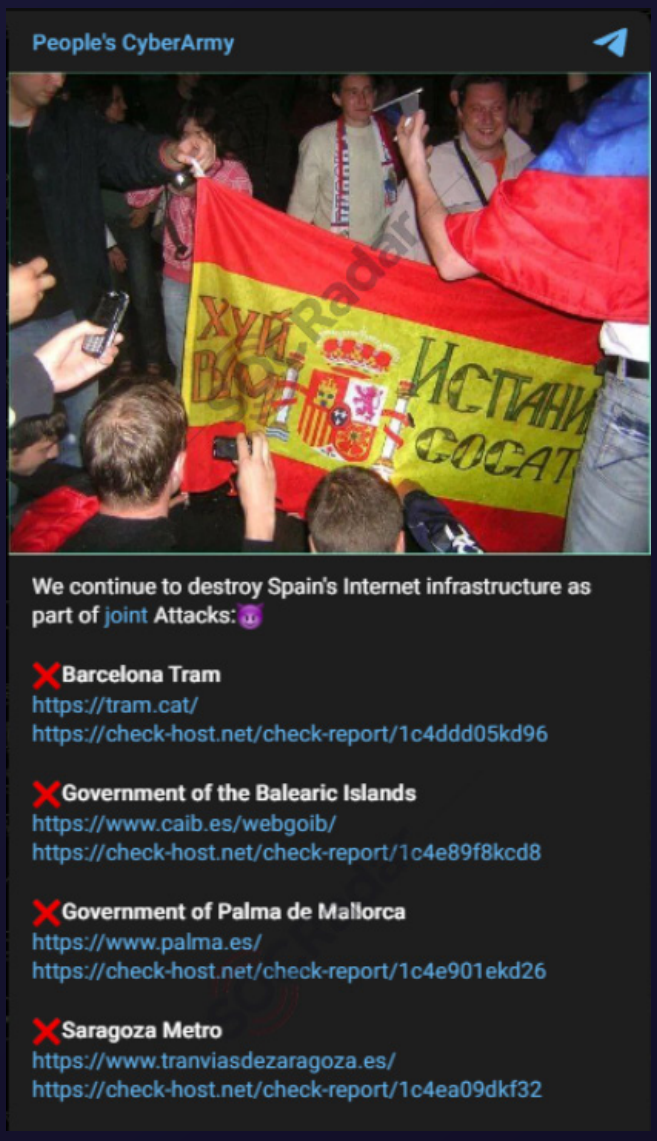



*Analysis of the content types in posts from Dark Web forums monitored by SOCRadar*

When examining the type of information published on Dark Web forums, **Databases** take the top spot, accounting for **51,14%** of all posts. The second most popular type of information shared by threat actors is related to **Access** information (sales, shares, etc.), which comprises **23,21%** of the posts. Lastly, posts related to **Website** attacks (defacements, DDoS attacks, etc.) make up **19,80%** of the posts.

# Recent Dark Web Activities Targeting Entities in Europe

## Russian Threat Actors Allegedly Targeted Spain




Several threat actors published alleged attacks on their Telegram channels after 2 cyber criminals attached to them got arrested in Spain. Here, one threat actor claimed to have attacked the websites of several Spanish organizations. Threat actors continued with their allegations for around two weeks.

## European Parliament Elections were Threatened by Russian Threat Actors


On June 6, a pro-Russian hacker group announced plans to launch a cyberattack on Europe's internet infrastructure, citing alleged Russophobia and double standards by European authorities. The group accuses the European Parliament of ignoring the "genocide" in Donbas for eight years and implementing anti-Russian sanctions following Russia's actions in Crimea and Donbas.

For more detailed information on the threats against the European Parliament Elections, you can visit our blog post.

## European Parliament Elections were Threatened by Russian Threat Actors

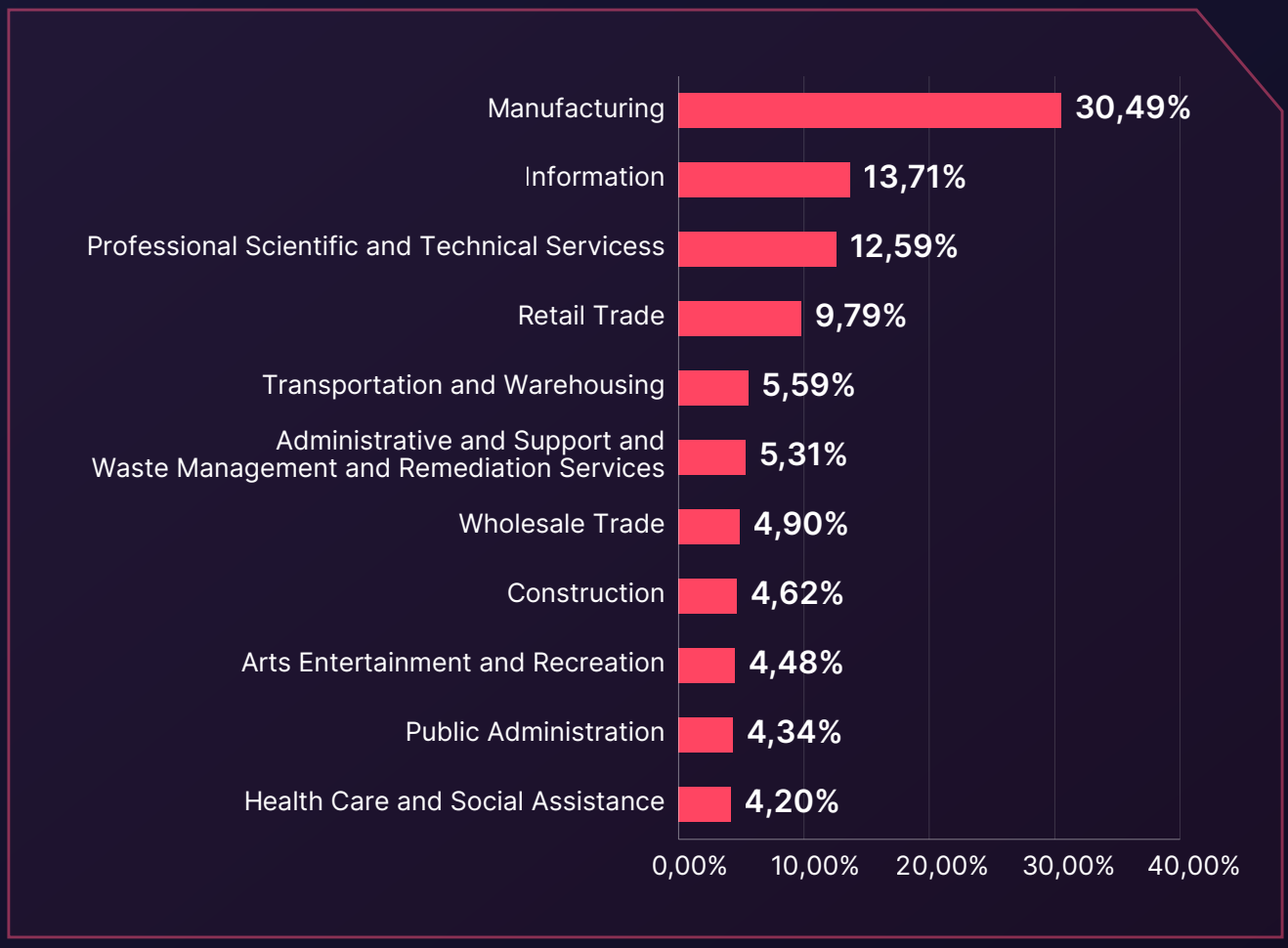

On May 10, 2024, a threat actor published a post on a Dark Web forum monitored by SOCRadar, claiming to have breached Europol. The allegedly compromised data includes many sensitive materials ranging from alliance employee information to FOUO source code, PDFs, documents for reconnaissance, and operational guidelines.

Later on, Europol made an announcement about the alleged breach and confirmed the web portal was breached, but no operational data was stolen according to BleepingComputer. You can read more about this on our blog.

# Ransomware Threats Targeting Europe

SOCRadar's monitoring services detected 1,290 ransomware attacks towards the organizations in the European region. In this chapter, we will be reviewing these numbers in detail.

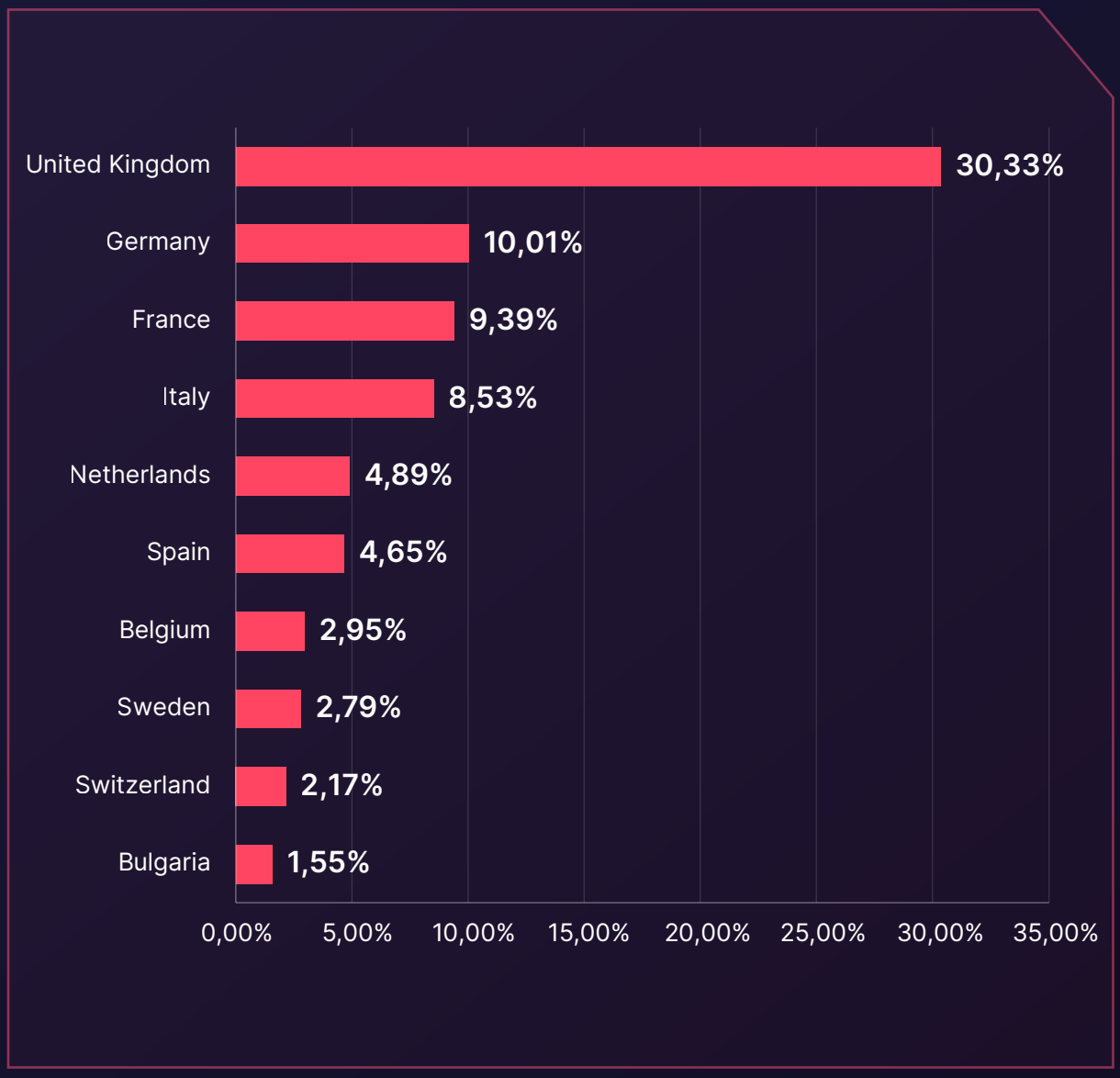
## Distribution of Ransomware Attacks by Industry




*Most targeted industries by ransomware groups in Europe*

Ransomware groups in Europe most targeted the **Manufacturing** industry, accounting for **30,49%** of all attacks. The **Information** industry took the second spot with **13,71%** of the attacks, while **Professional, Scientific, and Technical Services** ranked third with **12,59%** of the attacks.

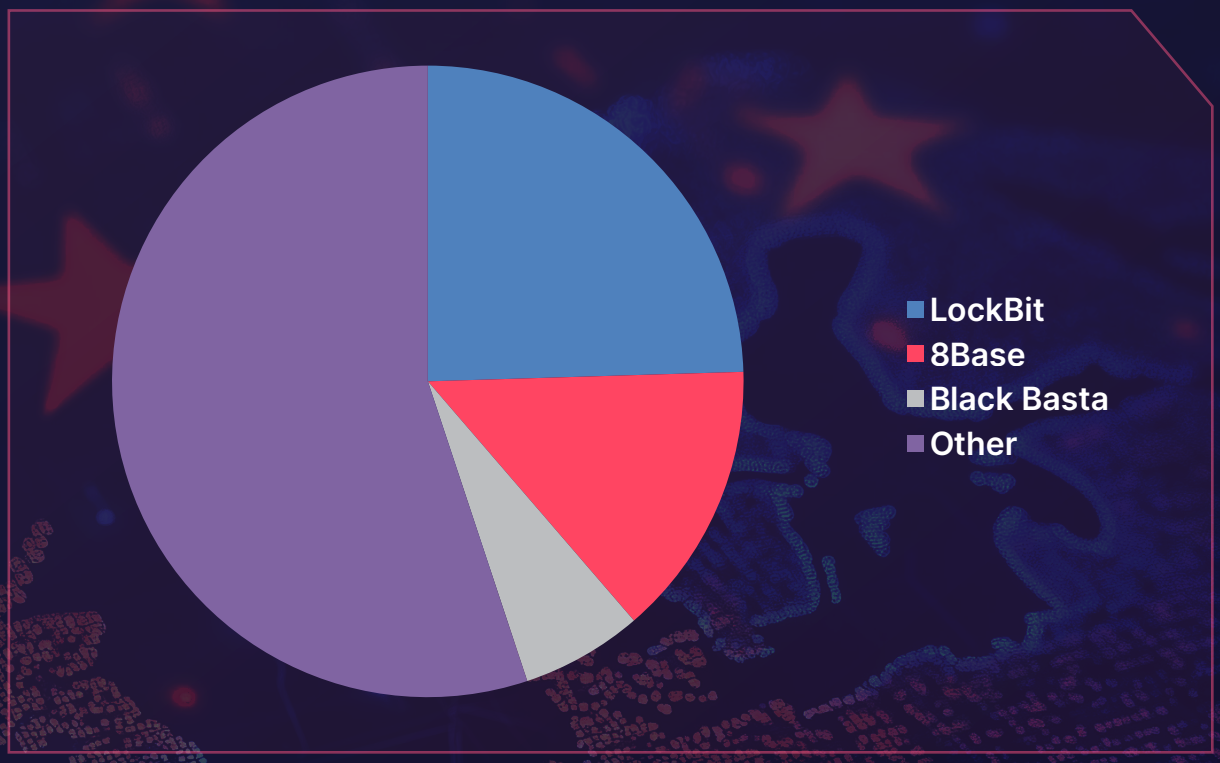
## Distribution of Ransomware Attacks by Primary Target Country




*Most targeted countries by ransomware groups in Europe*

The **United Kingdom** was the most targeted country in Europe by ransomware groups, with **30,33%** of the attacks targeting organizations there. **Germany** was in second place, suffering from **10,01%** of the ransomware attacks. **France** ranked third, targeted by **9,39%** of the ransomware attacks.

## Top Ransomware Groups Targeting the European Region




*Most active ransomware groups targeting the European region*

Our analysis shows that the most active ransomware group targeting Europe was **LockBit** (all versions combined), responsible for **24,5%** of all attacks. The second most active group was **8Base**, accounting for **14,2%** of the attacks. In third place, **Black Basta** appeared, being responsible for **6,2%** of all ransomware attacks to the organizations in the region.

# A Closer Look into The Top 3 Ransomware Groups

## Lockbit 3.0 Ransomware Group


-Ransomware Group-

| | |
|---|---|
| Motivation: | Financial Gain |
| Target Countries: | United States, United Kingdom, Canada, Europe, Thailand, Taiwan |
| Target Sectors: | Manufacturing, Professional Services, IT, Healthcare, Finance, Education, Legal Services |
| Attack Type: | Phishing, RDP and VPN access Exploitation, Ransomware, Data Exfiltration, Double-extortion |

-TTPs-

| | |
|---|---|
| Exploit Public-Facing Application: | T1190 |
| Remote Desktop Protocol: | T1021.001 |
| Data Encrypted for Impact: | T1486 |

LockBit 3.0, succeeding LockBit and LockBit 2.0, functions as a Ransomware-as-a-Service (RaaS) entity.

Since January 2020, LockBit has transitioned to an affiliate-based model, employing diverse methodologies to target businesses and critical infrastructure entities. Noteworthy tactics include double extortion and the utilization of initial access broker affiliates, alongside recruitment efforts involving insiders and hacker recruitment competitions.

You can visit our blog post for more detailed information about the Lockbit 3.0 Ransomware Group.

# 8Base


-Ransomware Group-

| | |
|---|---|
| Motivation: | Financial Gain |
| Target Countries: | United States, Brazil, UK, Australia, Germany, Canada, Spain, Italy, Belgium |
| Target Sectors: | Professional Services, Manufacturing, Construction, Finance, Healthcare, Transportation |
| Attack Type: | RaaS, Ransomware, Double Extortion |

-TTPs-

| | |
|---|---|
| Phishing: Spearphishing Attachment: | T1566.001 |
| OS Credential Dumping: | T1003 |
| Exfiltration Over C2 Channel: | T1041 |

8Base is a ransomware group that has been active since April 2022. Despite its relatively recent emergence, the group has rapidly gained notoriety due to its aggressive tactics and the significant number of victims it has claimed. The group primarily targets small and medium-sized businesses (SMBs) across various sectors, including business services, finance, manufacturing, and information technology.

The group's identity, methods, and motivations largely remain a mystery. However, based on its leak site and public accounts, along with the group's communications, researchers think the group's verbal style is quite similar to that of RansomHouse, a group that typically purchases already compromised data or works with data leak sites to extort victims. This has led to speculation that 8Base may be an offshoot of RansomHouse.

For more detailed information about the 8base Ransomware Group, you can visit our blog post.

# Black Basta Ransomware Group


-Ransomware Group-

Motivation: Financial Gain

Target Countries: North America and Europe

Target Sectors: Manufacturing, Construction, Professional Services, Finance, Healthcare

Attack Type: Valid Credentials, RaaS, Ransomware, Double-extortion

-TTPs-

Valid accounts: T1078

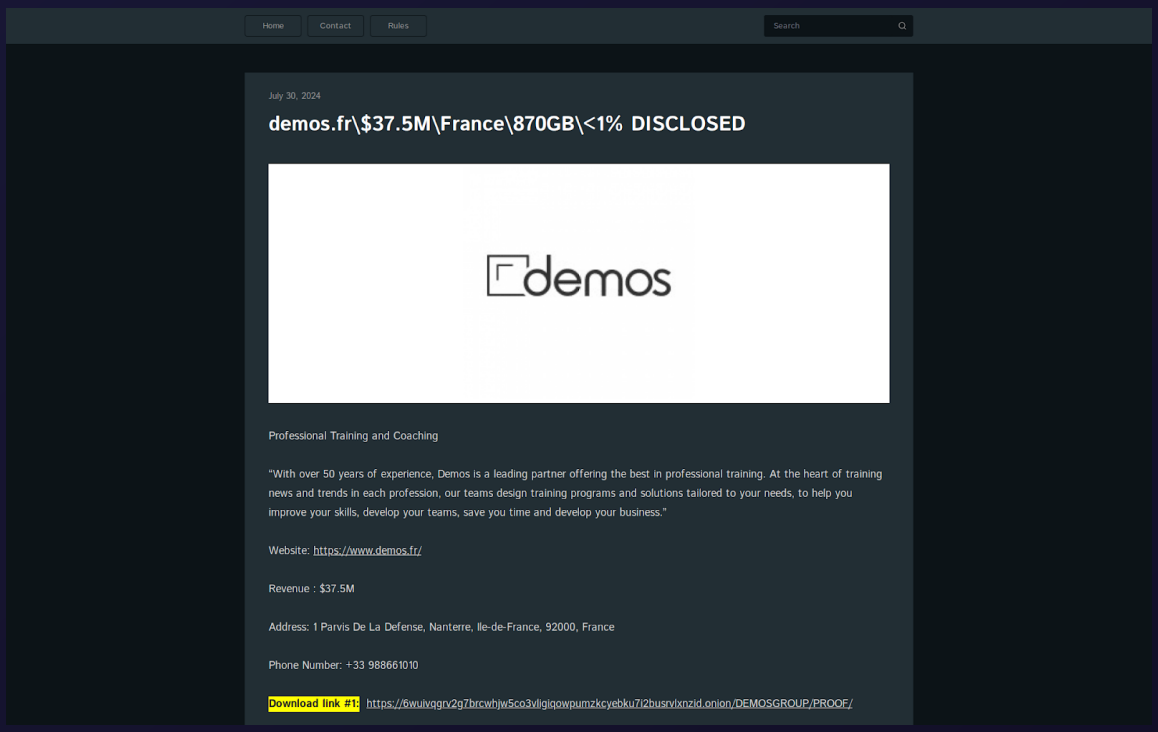
Phishing: Spear-phishing attachment: T1566.001

Exfiltration over C2 channel: T1041

> The Black Basta ransomware group, emerging onto the scene in April 2022, rapidly established itself as a formidable player in the cyber threat landscape, utilizing a Ransomware-as-a-Service (RaaS) model. The group distinguishes itself by its swift and assertive attack strategies, targeting diverse sectors such as manufacturing, financial services, and healthcare. Black Basta employs sophisticated double extortion techniques, wherein the victims' data is not only encrypted but also threatened with public release unless a ransom is paid. Known for their efficiency, the group has successfully orchestrated numerous high-profile attacks shortly after its inception, accumulating over 50 victims by the end of 2022. Black Basta's continued operations underscore their persistent threat and capability to cause significant disruptions to impacted organizations.
>
> For more detailed information about the Black Basta Ransomware Group, you can visit our blog post.

# Recent Ransomware Attacks Targeting Entities in the European Region

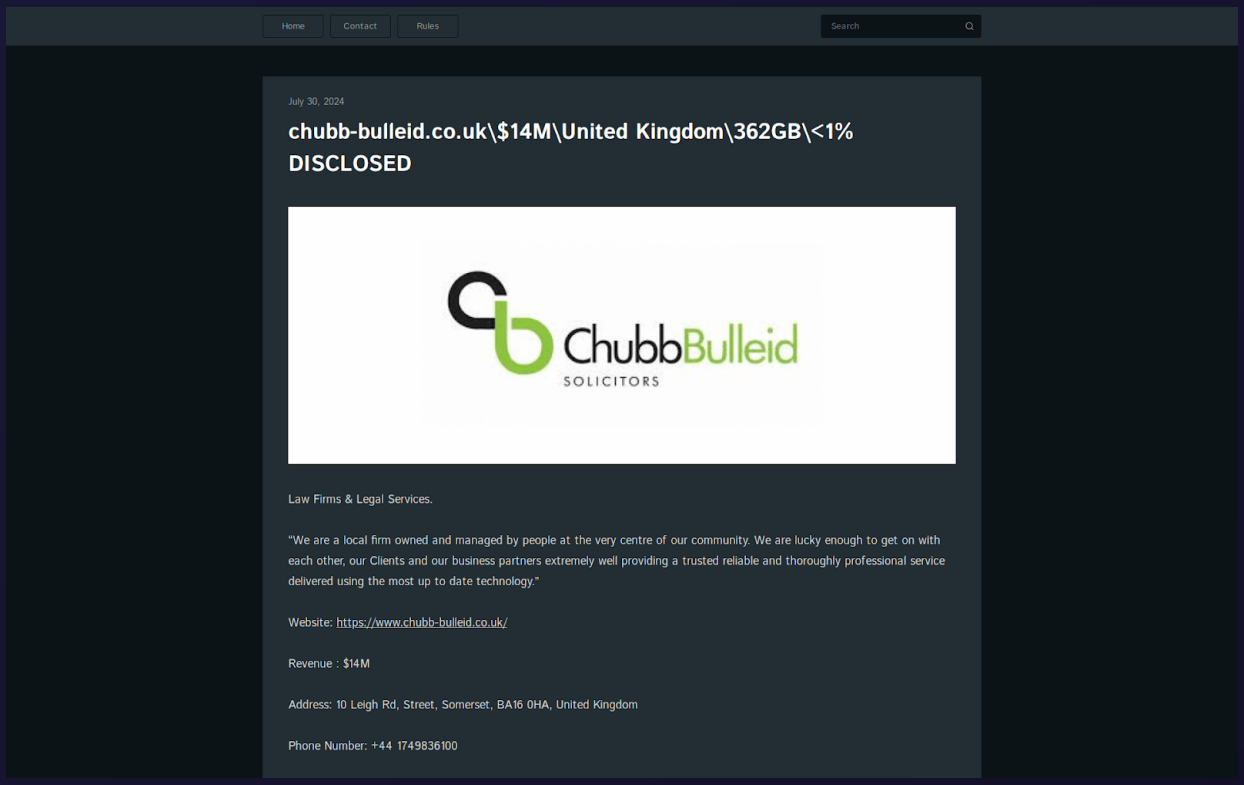
## The New Ransomware Victim of Cactus: demos




On the website of the Cactus ransomware group, monitored by SOCRadar, demos.fr has allegedly been announced as a victim. The company provides various trainings for corporate teams.

According to the alleged post, the threat actors obtained around 870 GB of data from the victims and threatened them to release the data. Considering the relations of demos with other companies and the data they might have, such a situation can cause serious risks not only for demos but also for various sectors and companies.

## The New Ransomware Victim of Cactus: ChubbBulleid



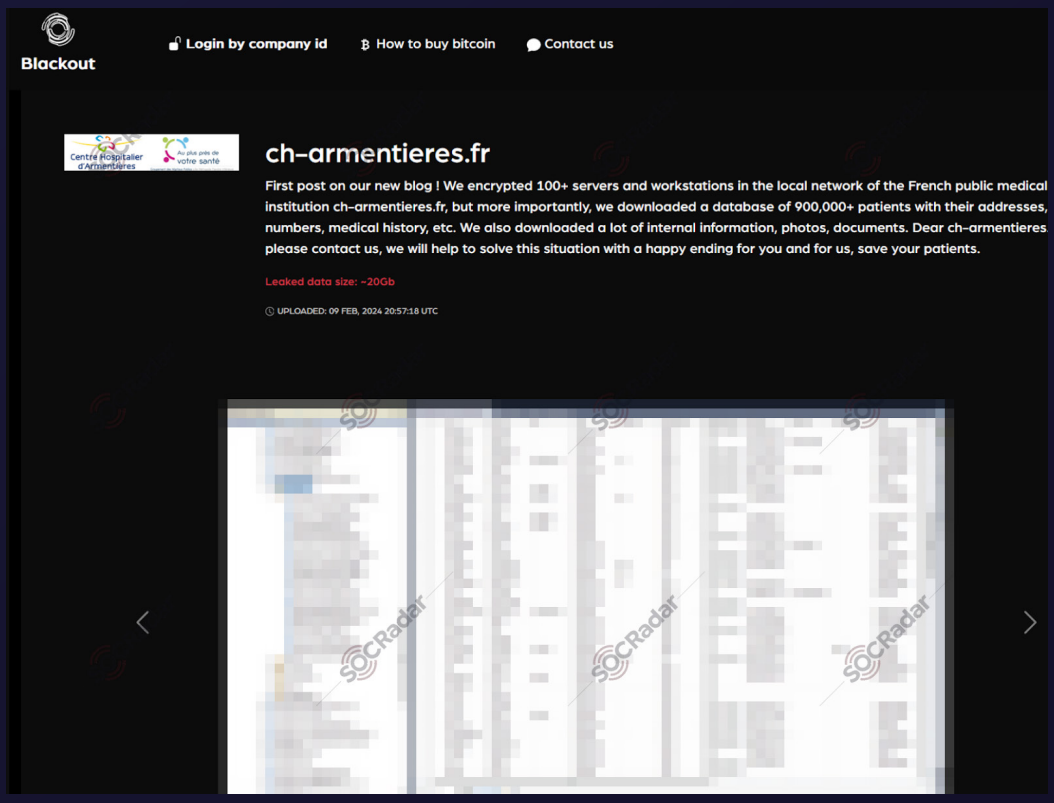

On the website of the Cactus ransomware group, monitored by SOCRadar, chubb-bulleid.co.uk has allegedly been announced as a victim.

The data reportedly includes a wide range of sensitive information, such as personal information, customer confidential information, litigation documents, corporate confidential data, NDAs, contracts, employees' and executives' personal files, financial documents and statements, and corporate correspondence.

The nature of the services provided by Demos.fr underscores the critical value of the documents and data they handle. This incident highlights the necessity for a comprehensive approach to cybersecurity. In today's interconnected business environment, safeguarding only your own organization is insufficient.

To address this need, SOCRadar has developed the Supply Chain Intelligence module. This advanced tool enables organizations to assess the security risks associated with their business partners and vendors. By gaining visibility into the security posture of third-party entities, organizations can enhance their overall security framework and better protect against potential vulnerabilities within their supply chain.

## Blackout Ransomware Group Leaked The Data of Centre Hospitalier d'Armentières




According to the alleged attack, over 100 servers and workstations within the local network of the French public medical institution ch-armentieres.fr were encrypted.

Additionally, a database containing sensitive information of over 900,000 patients, including their addresses, phone numbers, and medical history, was downloaded. The attackers claim that a substantial amount of internal information, photos, and documents was exfiltrated.

# Stealer Log Statistics

## Top Domains in Europe

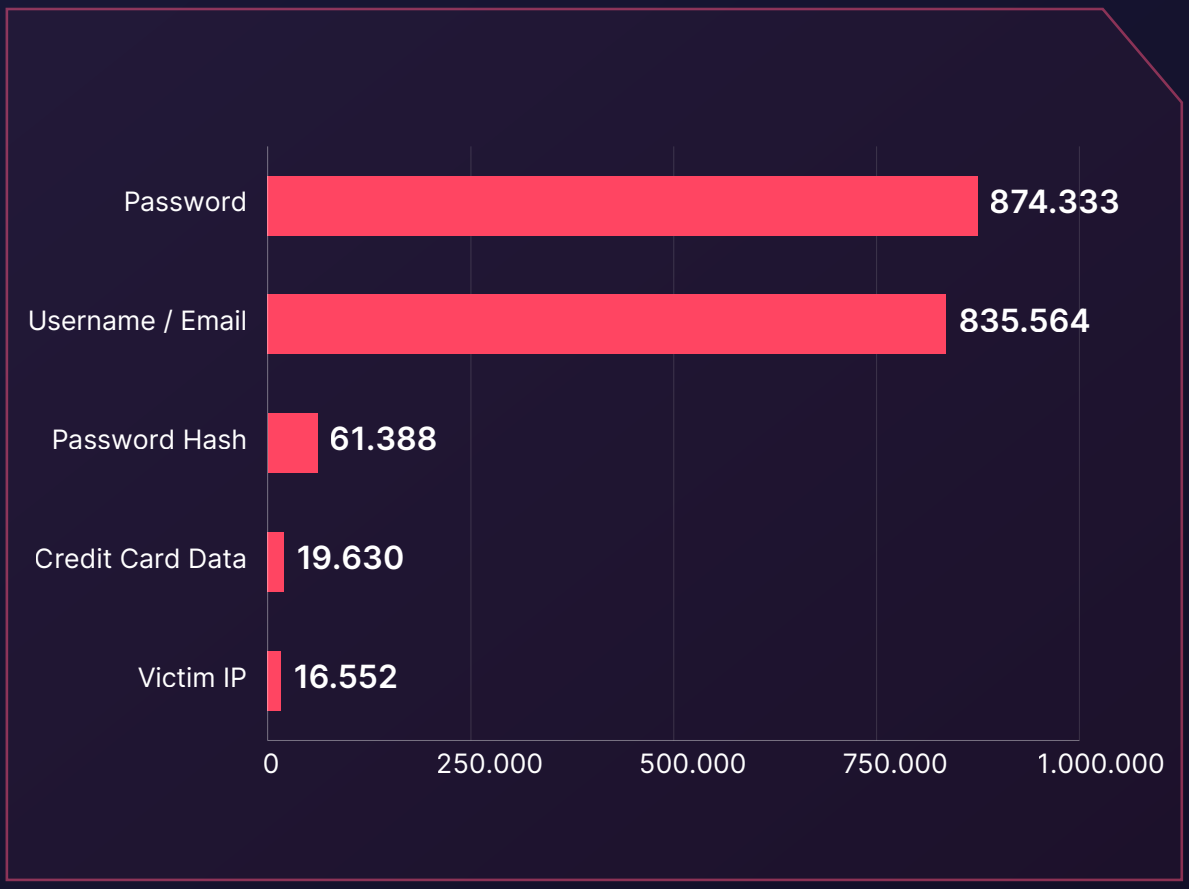
Thousands of users' IDs, email addresses, passwords, credit card data, password hashes, and victim IP addresses were compromised via Stealers from some of the most popular domains in the European region.

The table below lists the domains in Europe with the highest traffic in various parts of the region.

| | | |
|---|---|---|
| bbc.co.uk | allegro.pl | gazzetta.it |
| service.gov.uk | onet.pl | ansa.it |
| gov.uk | interia.pl | aniworld.to |
| vg.no | olx.pl | kleinanzeigen.de |
| nrk.no | gazeta.pl | leboncoin.fr |
| finn.no | corriere.it | lemonde.fr |
| dagbladet.no | repubblica.it | hln.be |

| | |
|---|---|
| vrt.be | ad.nl |
| belgium.be | delfi.ee |
| marca.com | postimees.ee |
| as.com | err.ee |
| elmundo.es | swedbank.ee |
| nu.nl | srf.ch |
| nos.nl | 20min.ch |

## Stealer Logs - Distribution of the Compromised Data*




*Note: This is a sampling of our dataset.*

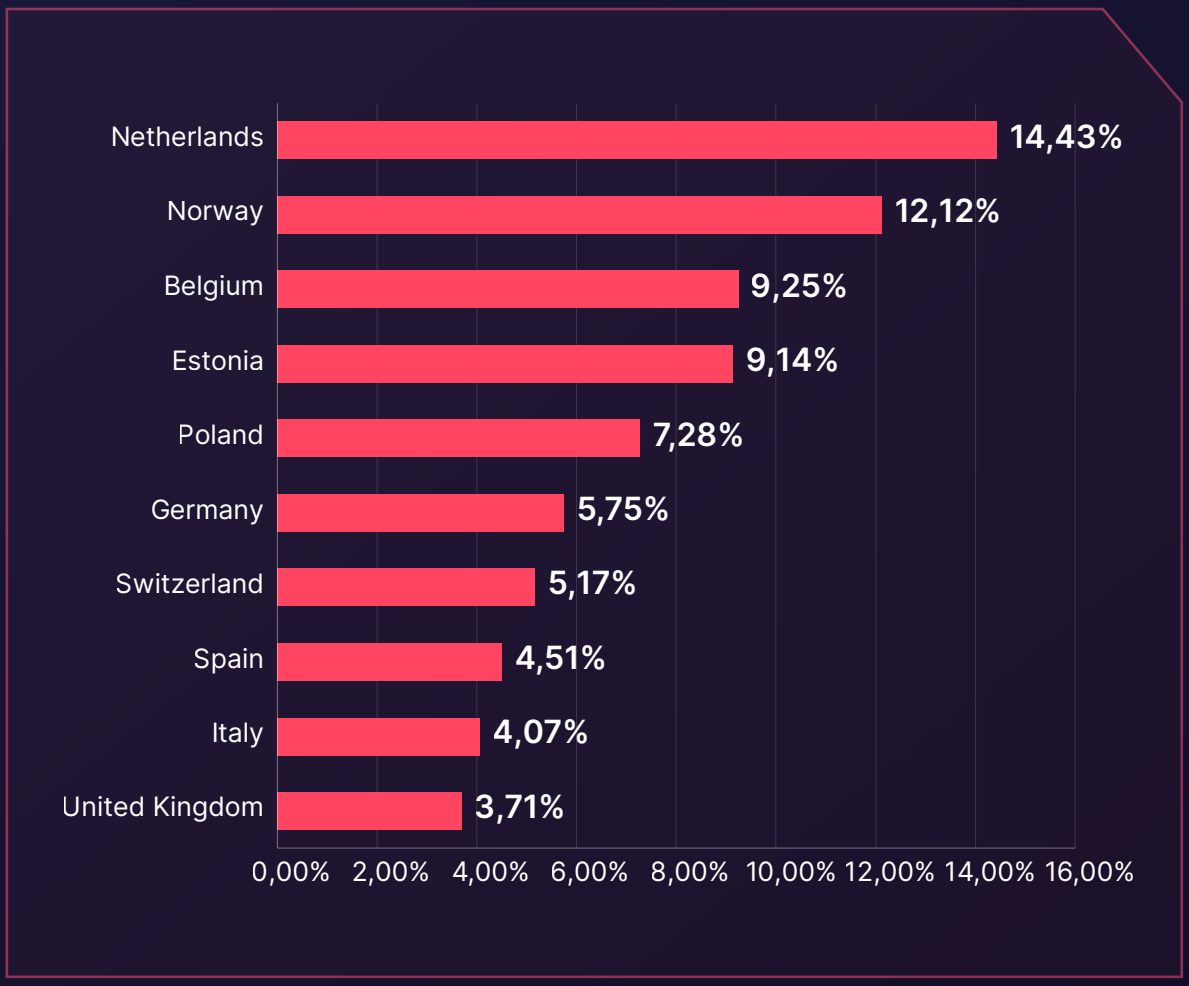
Stealer logs reveal victims' information in plain text, indicating a significant risk for organizations in Europe. The information in these logs, including employees' data, can be used to target their workplaces.

Organizations should implement strict password policies and utilize robust Identity & Access intelligence solutions. The SOCRadar Identity & Access Intelligence module can show you the location of stealers in your systems, helping to create a more secure working environment. Simply changing passwords without removing the stealers is inadequate, since doing so provides the new credentials to threat actors directly.

**Strengthen your security by removing stealers and implementing robust Identity & Access Intelligence;let SOCRadar guide you!**

Secure Your Access

## Stealer Logs - Distribution of the Victims' Countries




Stealers are types of malware that track and save your activity, including credentials. They infiltrate your system and compromise sensitive information. This information can be sold on by threat actors later on.

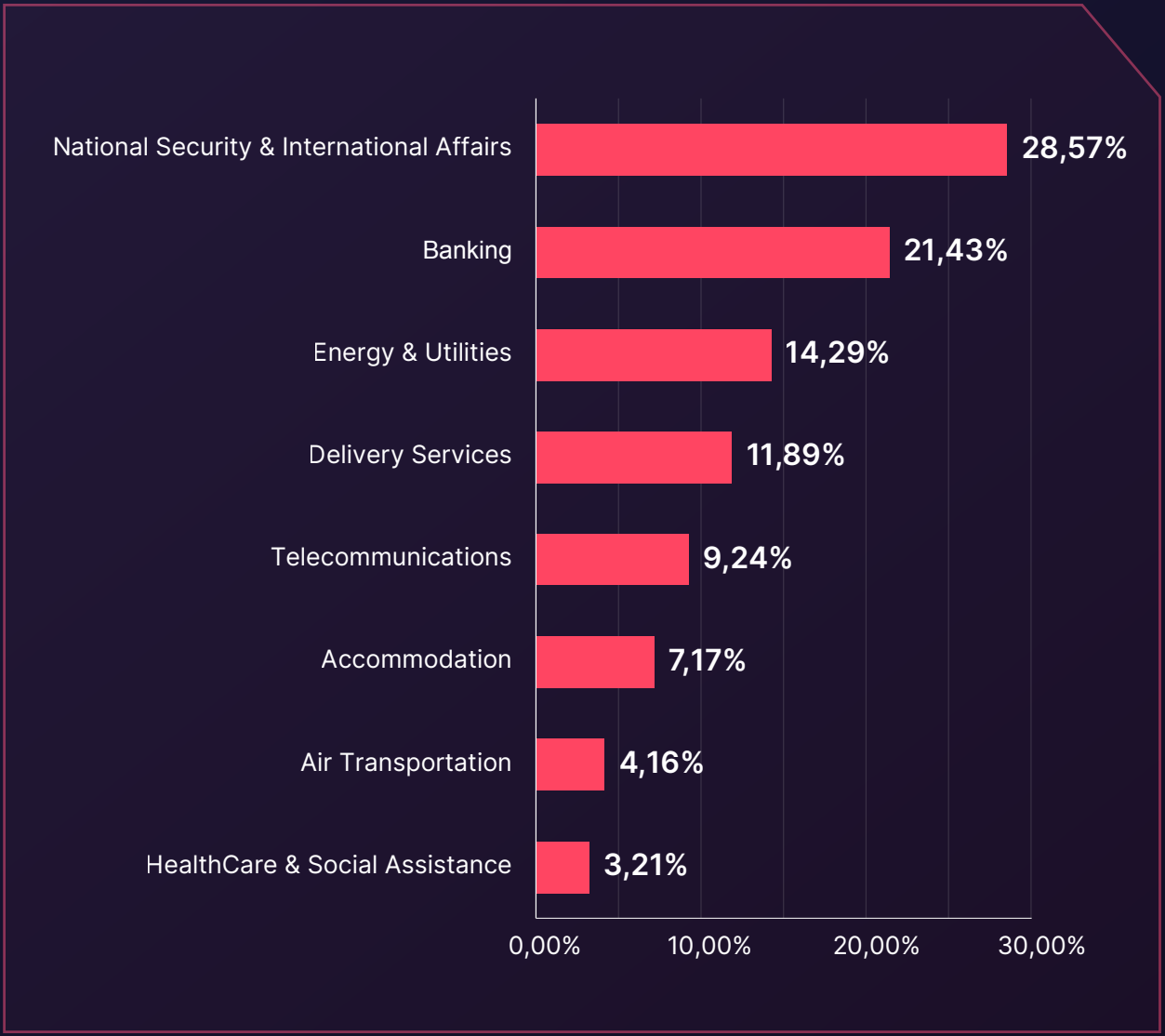
Regardless of your organization's size or location, it is crucial to prioritize robust password management and maintain a secure, organized work environment. Maintaining strong, unique passwords and keeping your digital work environment secure from malicious software can significantly reduce the risk of unauthorized access and data breaches.

**SOCRadar's "Snapshot of 70 Million Stealer Logs" whitepaper can help organizations stay up to date on the latest trends surrounding stealer malware and their dangers**

Read Now

# Phishing Threats Targeting Europe

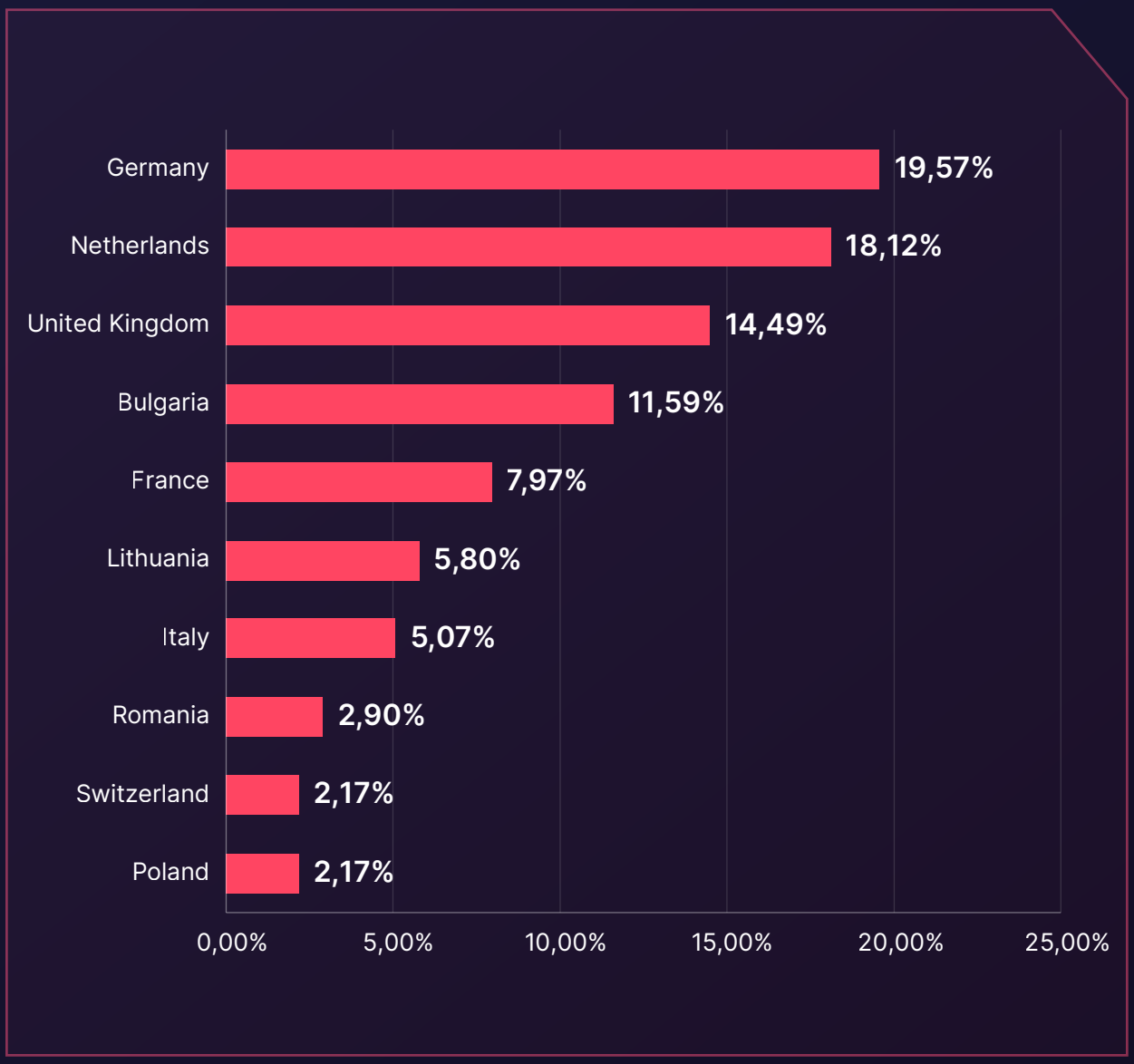
## Phishing Attacks - Distribution by Industry




*The most targeted industries in the European region with phishing attacks*

The **National Security & International Affairs** industry in Europe faced the most phishing attacks, accounting for **28,57%** of the total attempts. The **Banking** industry was second, with **21,43%** of the attacks. The **Energy & Utilities** sector experienced **14,29%** of the phishing attacks targeting the Europe.

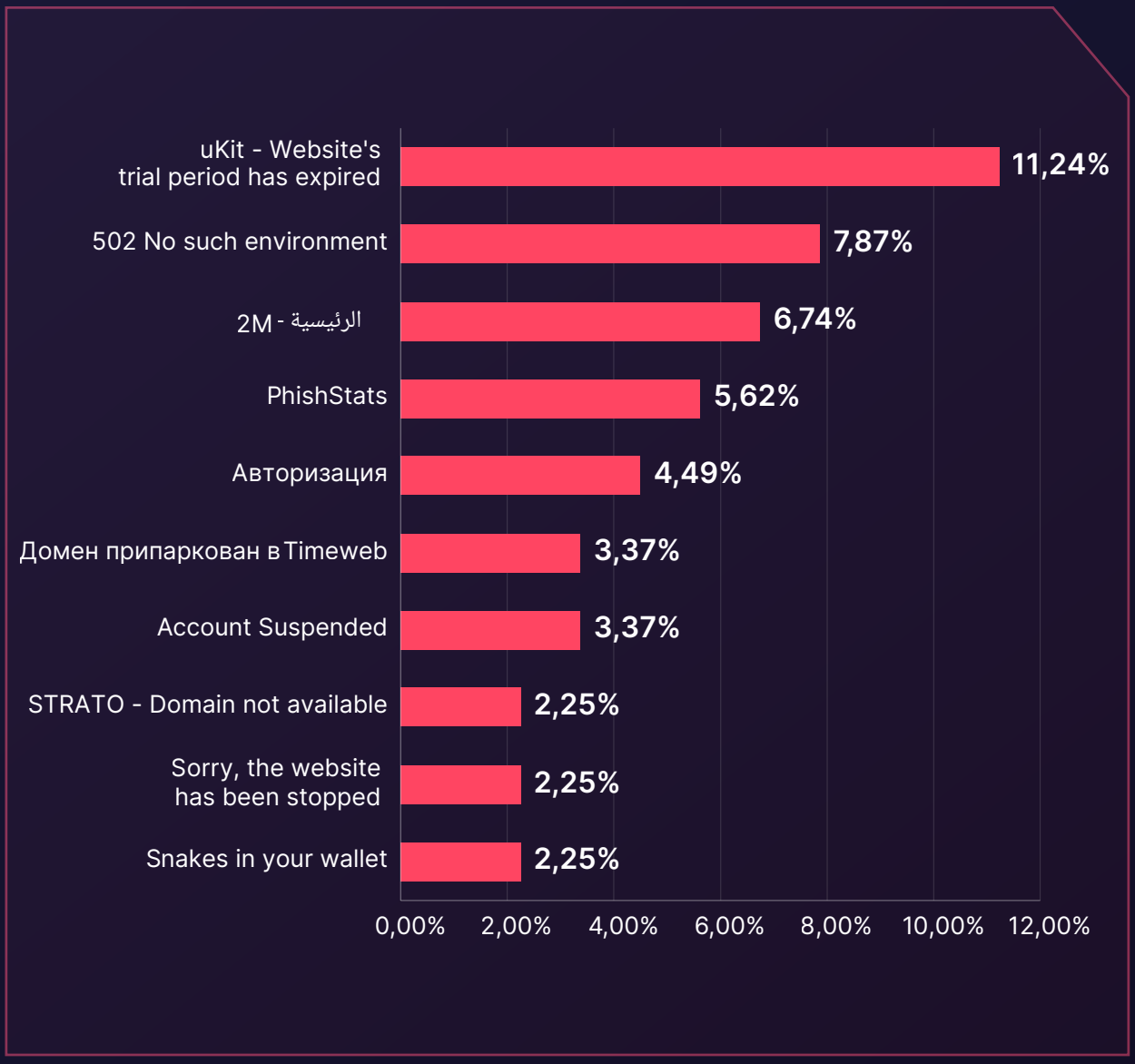
## Phishing Attacks - Distribution by Target Country




*The most targeted countries in the European region with phishing attacks*

**Germany** was targeted the most by phishing attacks, with **19,57%** of the attacks compared to other countries in Europe. The **Netherlands** was in the second spot, being the victim of **18,12%** of phishing attacks. On the third spot, we had the **United Kingdom** suffering from **14,49%** of the phishing attacks.

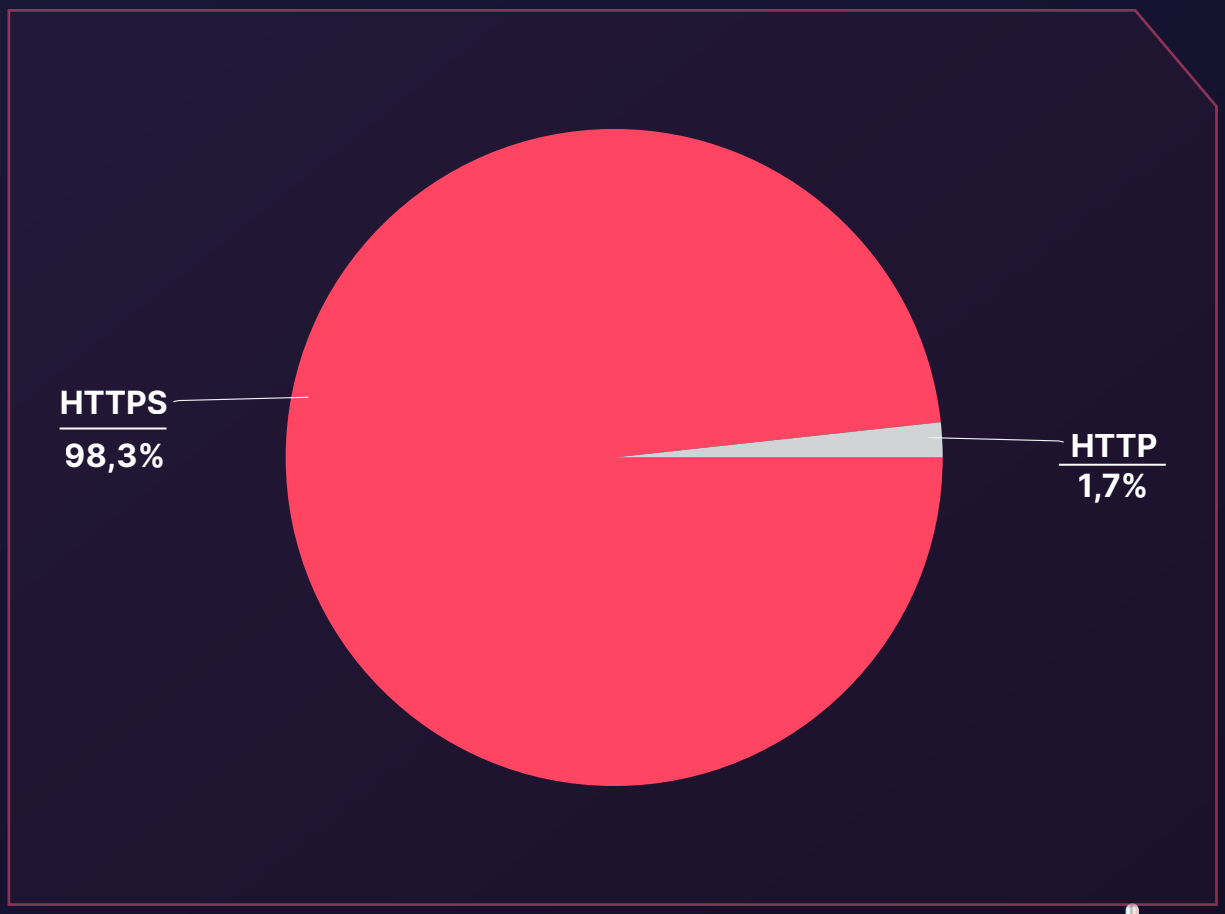
## Phishing Attacks - Distribution by Phishing Page Title




*The most used pages in phishing attacks targeting the European region*

Our analysis shows the most used pages in phishing attacks. The data reveals a predominant usage of the “uKit — Website's trial period has expired”. This title shows that threat actors are mimicking a website’s error message and might trick individuals to re-enter their credentials.

## Phishing Attacks- Distribution by SSL/TLS Protocol




*Distribution of protocols used in phishing attacks in the European Region*

When analyzing the protocols used by phishing websites, we see a predominant use of HTTPS. This is typically done to enhance the websites' perceived legitimacy.

## DDoS Attack Statistics

The threat landscape was pretty active for Europe.

- The peak bandwidth witnessed during a DDoS attack in Europe reached **993.54 Gbps**, highlighting a significant capacity from the cyber threats. Threat actors were targeting **Germany**.
- The highest recorded throughput during these incidents was **87.91 Mpps**, which belongs to **Germany**.
- DDoS attacks towards European entities lasted for **101 minutes** on average.
- **1.412.919** DDoS attacks were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for European targets.

The numbers above show that Europe faces a severe DDoS risk. The average time span for a DDoS attack is 101 minutes, but it is around 100 minutes because of the heavy and long attacks Latvia suffered. When we don't include the attacks on Latvia, we see that for the rest of Europe, attacks lasted for 19 minutes on average. The number of attacks and their size are considerable threats to organizations.

| Attack Vector | Number of Attacks (2H 2023) |
|---|---|
| TCP ACK | 495.200 |
| TCP SYN | 229.501 |
| TCK RST | 215.899 |
| DNS Amplification | 350.167 |
| ICMP | 107.456 |

# Lessons Learned: Key Insights and Strategic Recommendations

Upon reflection of the cyber threat landscape impacting organizations in Europe, several pivotal lessons and recommendations emerge. These insights, coupled with the capabilities of SOCRadar, offer a roadmap for enhancing cyber resilience and preserving operational integrity. The following are the top 5 takeaways from our analysis:

**Maintain vigilance regarding the evolving cyber threat landscape**

The cyber threat landscape is dynamically evolving, as evidenced by the surge in Dark Web activity related to Europe and the proliferation of ransomware incidents. Organizations must stay abreast of these developments and adapt their security strategies accordingly. Leveraging SOCRadar's Cyber Threat Intelligence provides businesses with real-time insights into emerging threats, enabling them to stay ahead of cyber adversaries.

**Emphasize multi-layered security measures:**

The diverse range of industries targeted by cyber threats underscores the necessity for multi-layered security measures. As demonstrated, threat actors do not discriminate based on industry, necessitating a comprehensive security approach across all industries, from Information Technology to Public Administration. SOCRadar can support this effort through proactive threat intelligence and monitoring services.

**Maintain vigilance against ransomware:**

Ransomware remains a significant threat, highlighting the importance of robust defenses and response plans. SOCRadar's threat intelligence capabilities enable businesses to identify potential ransomware threats and develop effective response strategies.

**Educate and train employees:**

Given the persistent threat of phishing attacks, continuous employee education and training are essential. Familiarity with phishing tactics and detection methods is critical. SOCRadar's solutions can assist by identifying potential phishing domains and raising awareness of the latest phishing techniques.

**Ensure defense against Stealers:**

Organizations must enhance their defenses against these malicious software. SOCRadar's advanced threat intelligence aids in detecting and mitigating Stealer Threats, bolstering the organization's overall security posture. Adopting a proactive, informed, and comprehensive approach to cybersecurity is paramount. By partnering with solutions such as SOCRadar, European organizations can fortify their defenses and effectively navigate the evolving cyber threat landscape.

# Who is SOCRadar®?

Your Eyes Beyond

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**

## MEET THE NEW MOBILE APP

Access threat intelligence, act on-the-go, and be instantly notified of new threats.View alerts, breaking Dark Web news, and new ransomware attacks

Download on the App Store

GET IT ON Google Play


Gartner Peer Insights™ 4.9/5