SOCRadar
Your Eyes Beyond

Finance Industry

Threat Landscape Report

Market Cap: Billions. Market Price: $10.

CISO Statement

The financial sector continues to sit at the center of the global cyber threat economy. As this report demonstrates, adversaries targeting financial institutions are no longer driven by technical experimentation but by scale, speed, and monetization. Data theft dominates the threat landscape, with stolen customer records, credentials, and internal databases representing the primary currency of the underground ecosystem. Ransomware activity remains highly fragmented, with no single dominant actor, increasing unpredictability and operational risk for banks, insurers, and financial service providers worldwide. At the same time, phishing campaigns have matured, exploiting trusted brands, urgency-driven narratives, and even HTTPS to bypass user skepticism. These patterns point to a threat model that prioritizes efficiency and impact over sophistication.

Looking ahead, we expect financial institutions to face increased pressure from multi-extortion ransomware operations, AI-assisted social engineering, and faster weaponization of exposed data. The institutions that will remain resilient are those that treat threat intelligence as a strategic capability rather than a reactive function, combining external visibility, dark web intelligence, and continuous attack surface awareness with strong operational discipline. This report is intended to support security leaders in making informed, forward-looking decisions by grounding strategy in real-world adversary behavior. In an environment where trust is the core asset of the financial industry, proactive intelligence, collaboration, and preparedness are no longer optional, they are foundational.

Ensar Seker (PhD)
Chief Information Security Officer (CISO)

Executive Summary

Top Takeaways

The United States is the primary hotspot across multiple datasets. It leads both dark web threat activity at **23.52% and phishing activity at 48.02%,** which shows sustained focus on US financial targets.

Dark web activity is mainly driven by monetization. Selling alone accounts for **74.49% of posts,** supported by 20.23% sharing activity. This shows an active underground market for financial data and access.

Data theft is the main objective. **Data and database related posts represent 80.91%** of all threat types, far exceeding access, tools, or vulnerability discussions.

Ransomware targeting is distributed across many groups. **While Qilin, Akira, and LockBit are visible, 70.9%** of cases come from other actors, which increases unpredictability.

Phishing campaigns rely on trusted brands and urgent messages. Delivery services and generic system alerts are the most used lures.

62.1% of phishing pages use HTTPS. Attackers use SSL to increase credibility and bypass basic user suspicion.

Financial threats show a pattern focused on scale, speed, and monetization rather than technical complexity.

Technical Details

This report is based on data collected between February 2025 and February 2026

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

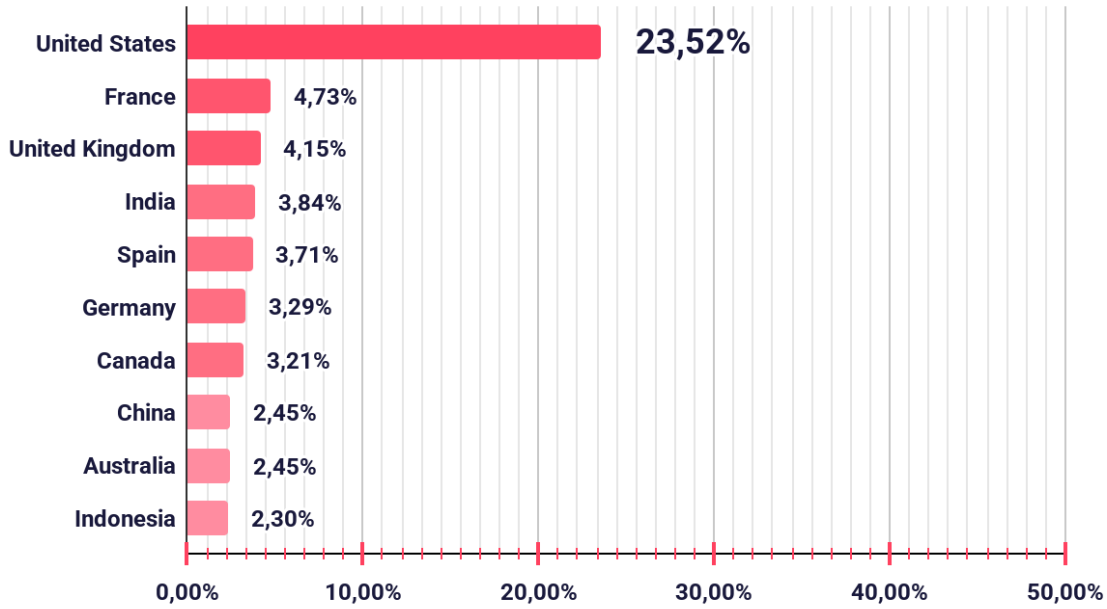
In the Dark Web Threats chapter, we will be covering the news and developments from Dark Web Forums, Telegram channels, Discord groups, and so on. These are areas where threat actors with various skill sets come together, discuss, share tools, and publish their alleged cyber attacks.

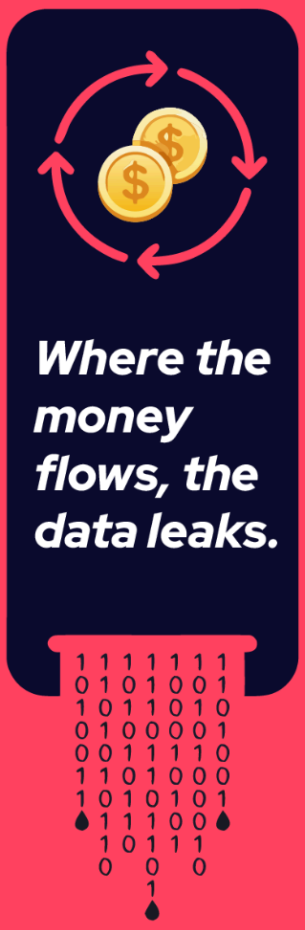
In the Ransomware Threats chapter you will find information about ransomware threats targeting the Finance Industry.

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

Distribution of Dark Web Threats by Country



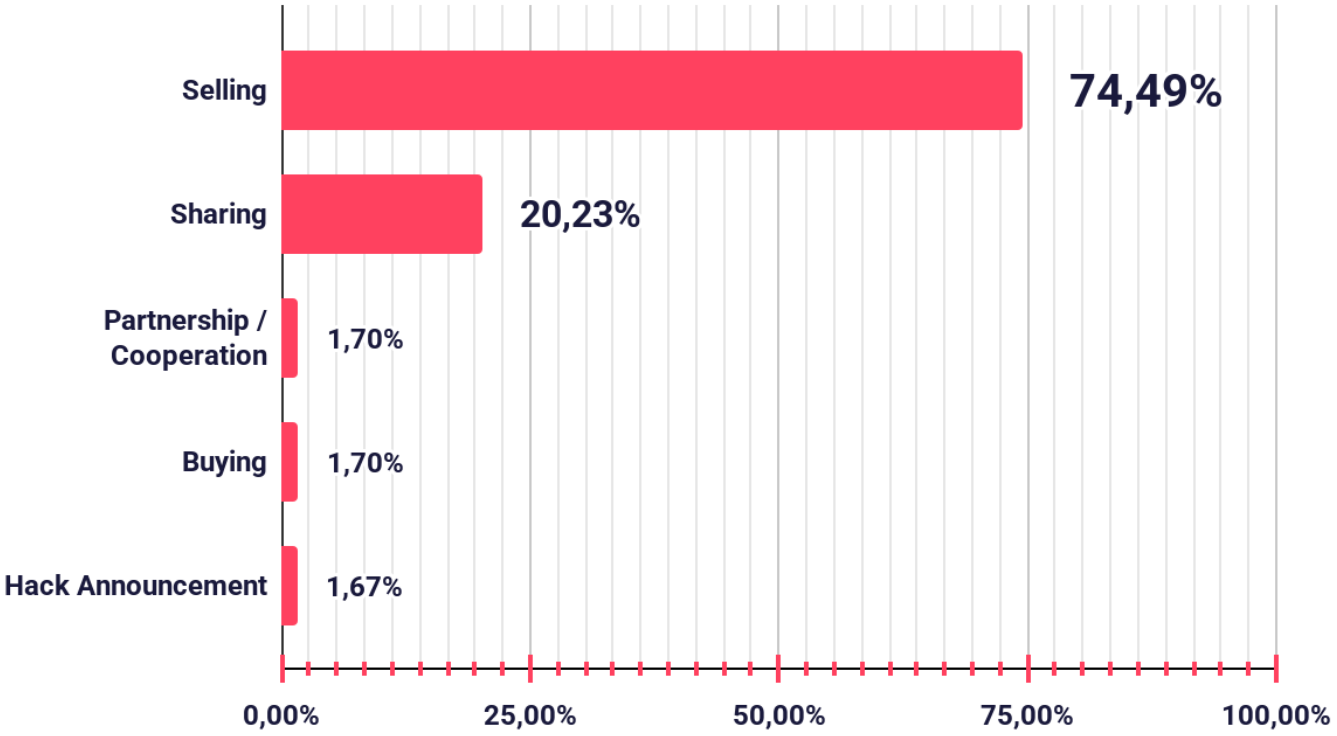


Dark web threat activity linked to the finance sector shows a strong geographic concentration. The United States alone accounts for 23.52% of observed activity. This is far higher than any other country in the dataset. It signals that US financial entities remain a primary focus for threat actors. This is likely due to the size of the financial market, high digital adoption, and the value of financial data.

European countries such as France, the United Kingdom, Spain, and Germany appear next, each ranging between 3% and 5%. This cluster shows that Western Europe is a consistent secondary target region.

Overall, threat actors show a clear preference for countries with mature financial infrastructure, high transaction volumes, and large customer datasets.

Distribution of Dark Web Threats by Threat Categories



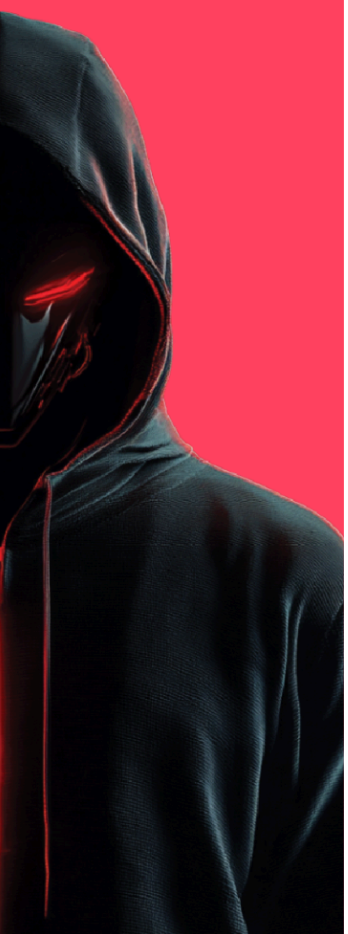
Dark web activity affecting the finance sector is dominated by monetization driven behavior. Selling accounts for 74.49% of all observed threat posts. This shows that most threat actors are focused on turning stolen financial data, access credentials, and fraud related assets into direct profit.

Sharing follows with 20.23%. This indicates that threat actors often distribute data, tools, or access among peers before monetization. This behavior supports collaboration and increases the speed at which financial data spreads across different groups.

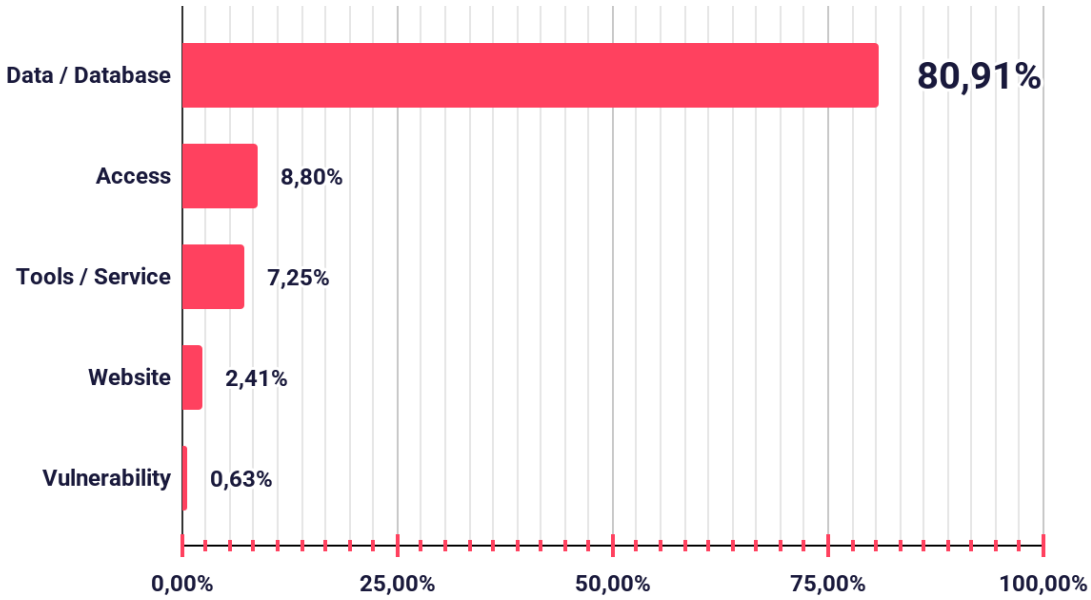
The data shows that financial threats on the dark web are driven mainly by data trade and peer distribution.

Attackers aren't after your vault.

They are after your databases (80.91%).



Distribution of Dark Web Threats by Threat Types



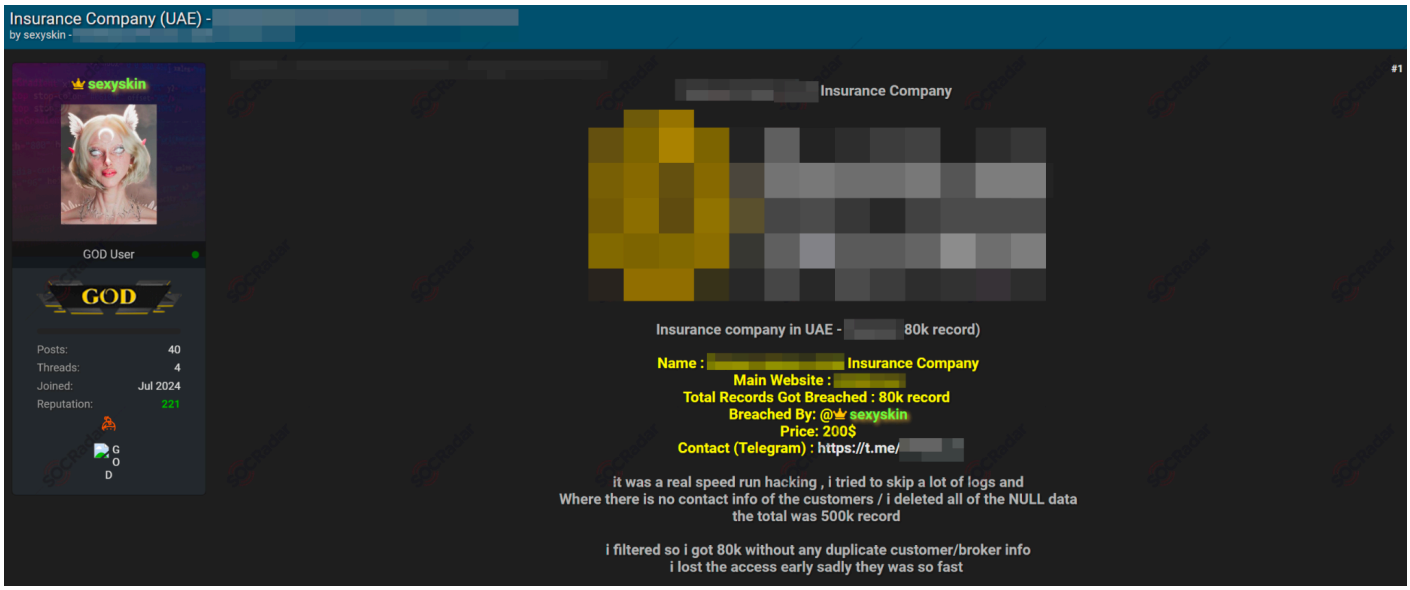
Dark web threats targeting the finance sector are strongly centered on data exposure. Posts related to data or databases account for 80.91% of all activity. This shows that stolen customer records, account details, and internal financial datasets are the primary assets traded in underground markets. Data remains the main objective of most attacks against financial organizations.

Access related posts follow at 8.80%. These often refer to compromised RDP, VPN, or admin panels that can later be used to extract data or deploy fraud operations. Tools and services appear at 7.25%, which indicates an ecosystem that supports these attacks with ready to use kits and services.

This distribution shows that financial threats are outcome driven. The goal is data theft, supported by access sales.

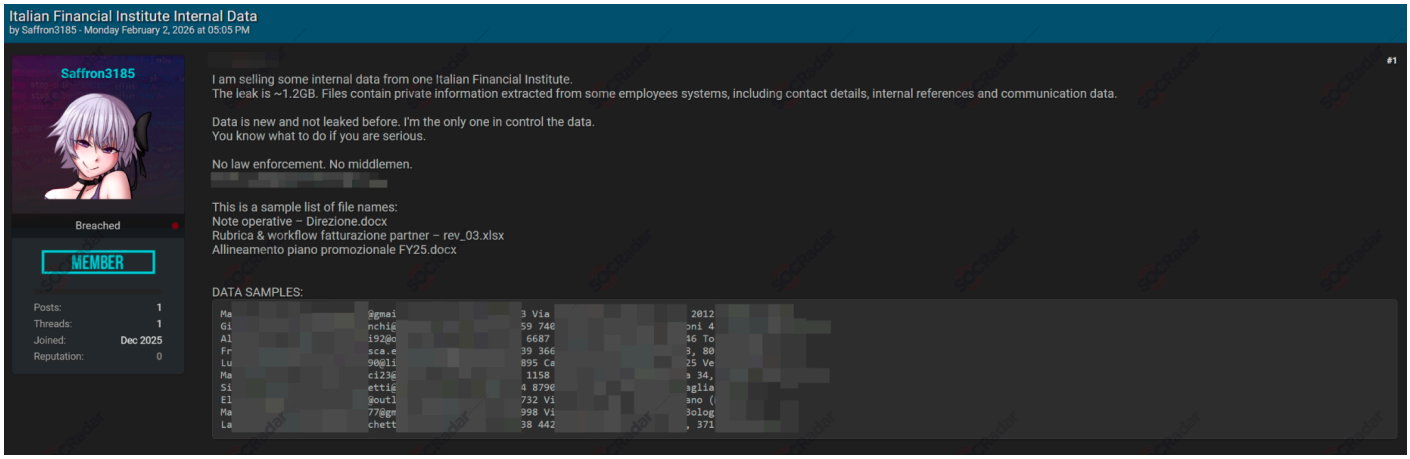
Recent Dark Web Activities Targeting the Finance Industry

Alleged Database Sale Targets Insurance Services in UAE



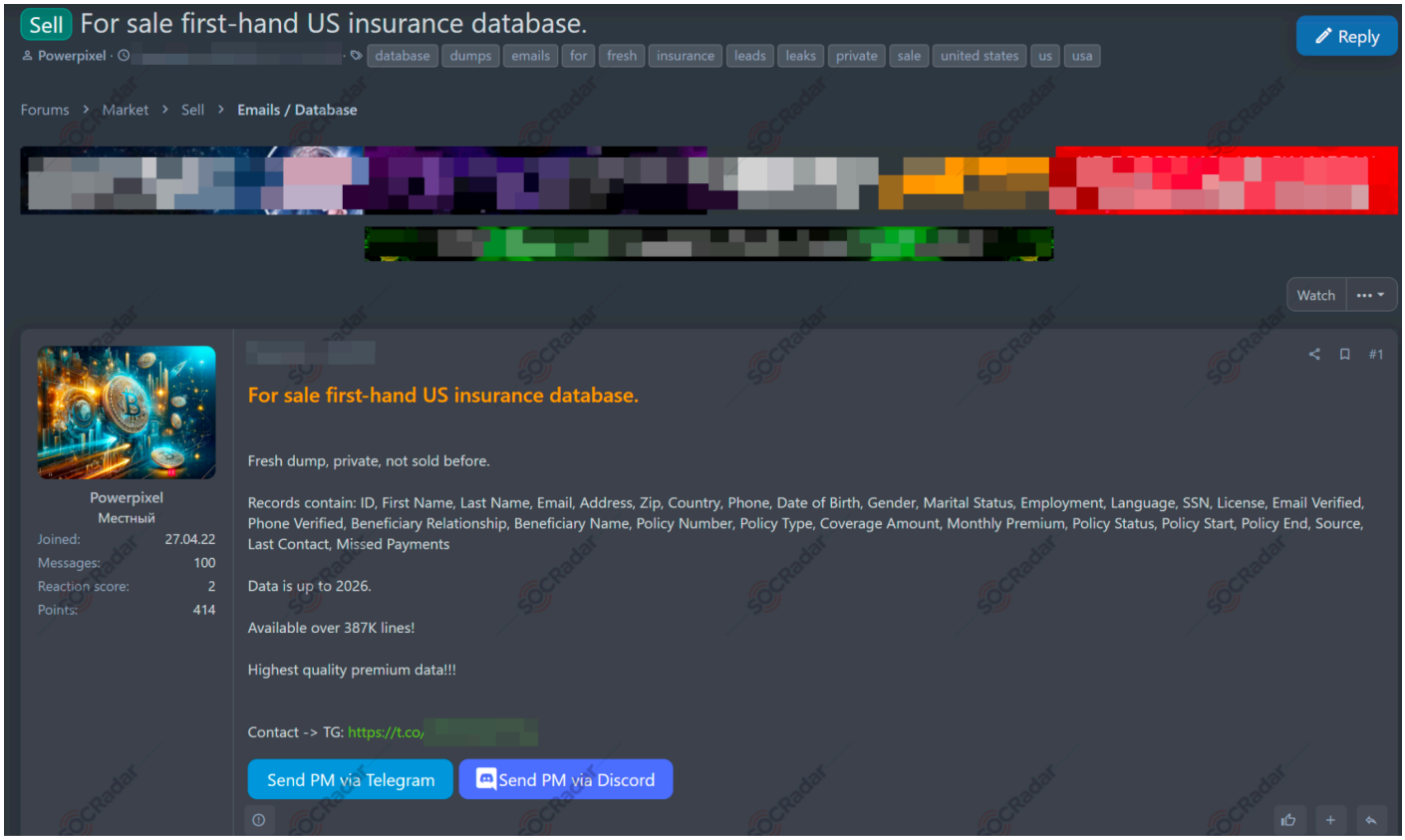
SOCRadar detected an alleged database sale shared on a Dark Web forum. The post claims to offer data linked to an insurance company operating in the UAE. The dataset reportedly contains around 80,000 customer records filtered from a larger breach. The seller offered samples and set a price for access, raising concerns about customer data exposure and misuse.

The Alleged Database of an Italian Financial Institution is on Sale



SOCRadar identified an alleged internal data sale posted on a Dark Web forum. The post claims to offer files taken from employee systems of an Italian financial institution. The dataset is said to include contact details, internal references, and communication records, with a total size of about 1.2 GB. The seller shared file name samples and offered the data for private negotiation.

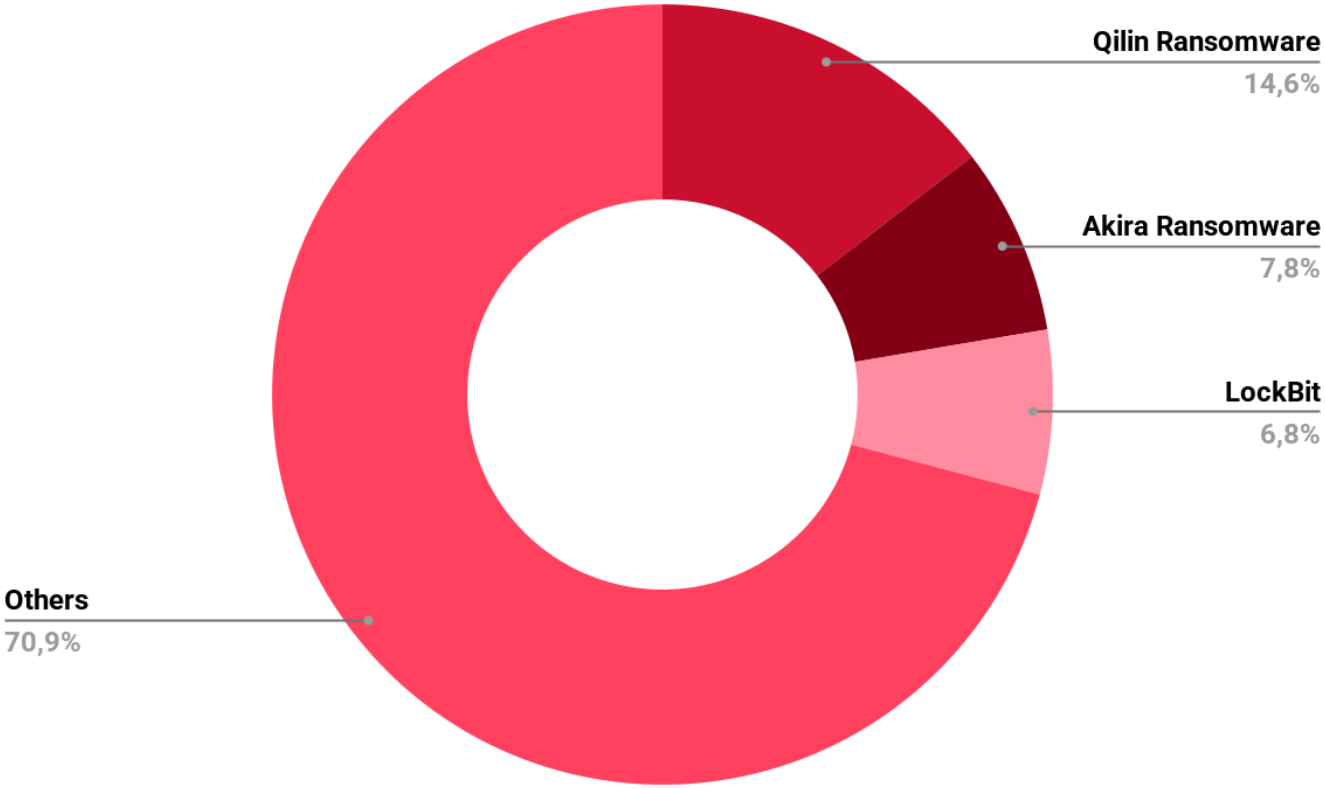
The Alleged Insurance Database of the United States is on Sale



SOCRadar detected an alleged insurance database sale shared on a Dark Web forum. The post claims to offer a US insurance dataset containing detailed personal and policy information. The dataset reportedly includes over 387,000 records dated up to 2026. The exposed fields include identity details, contact data, policy numbers, and payment history, raising serious risks of identity fraud and targeted abuse.

Ransomware Threats

Top Ransomware Groups Targeting the Finance Industry



Ransomware activity against the finance sector is led by a small number of active groups, with **Qilin** at the top at 14.6% of observed cases. **Akira** follows with 7.8%, and **LockBit** with 6.8%. Both are known for targeting organizations where operational disruption can quickly lead to ransom pressure.

A large portion, 70.9%, falls under other groups. This indicates that the finance industry is not targeted by only a few dominant ransomware brands. Instead, it faces attention from a wide range of operators, including smaller or less known groups.

A Closer Look into The Top 3 Ransomware Groups

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.

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.

LockBit

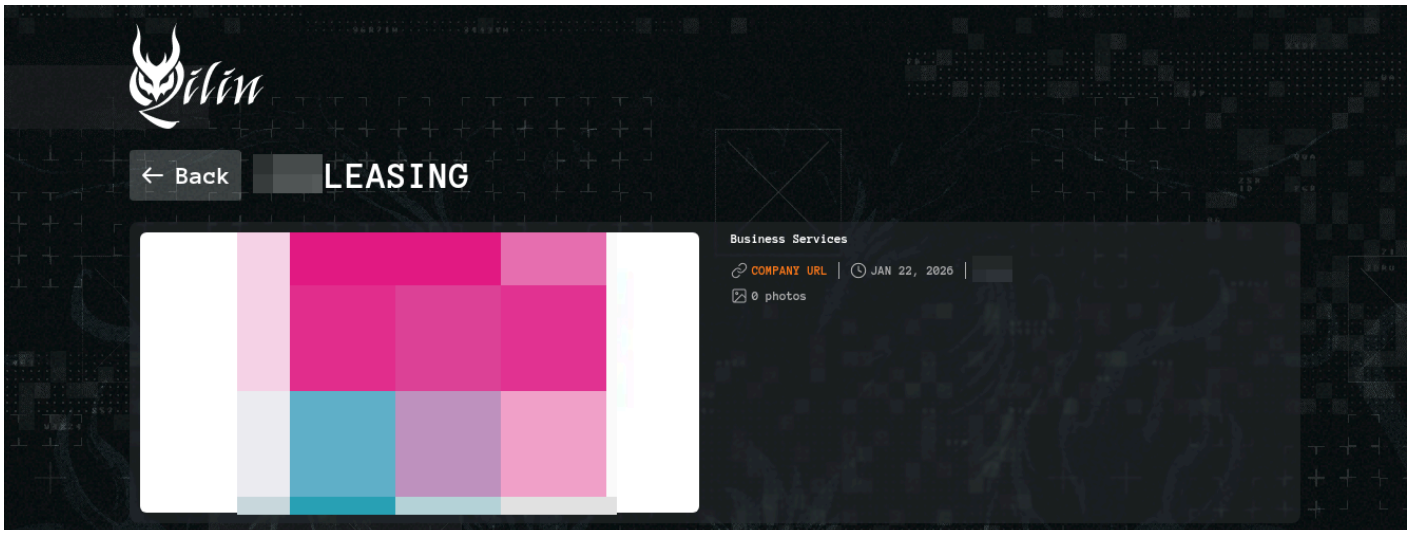
LockBit is a ransomware-as-a-service (RaaS) gang first observed in 2019, now operating through successive variants (LockBit 2.0, 3.0, 4.0 and 5.0). It provides malware to affiliates worldwide, enabling coordinated attacks on businesses, healthcare, government and critical infrastructure. LockBit is known for double extortion and employs professional tactics like hiring initial-access brokers, recruiting insider agents, and even sponsoring hacker contests and bug bounty programs to improve its code. The group has extorted hundreds of millions of dollars from thousands of victims, making it one of the most prolific ransomware operations.

By 2024 LockBit was widely recognized as a leading ransomware threat. More than 2,000 organizations (in healthcare, finance, retail, government and other sectors) have been targeted by LockBit affiliates. Even as its leaders face charges and some operations are disrupted, LockBit's ongoing development shows that this RaaS operation remains a major cybercrime menace.

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

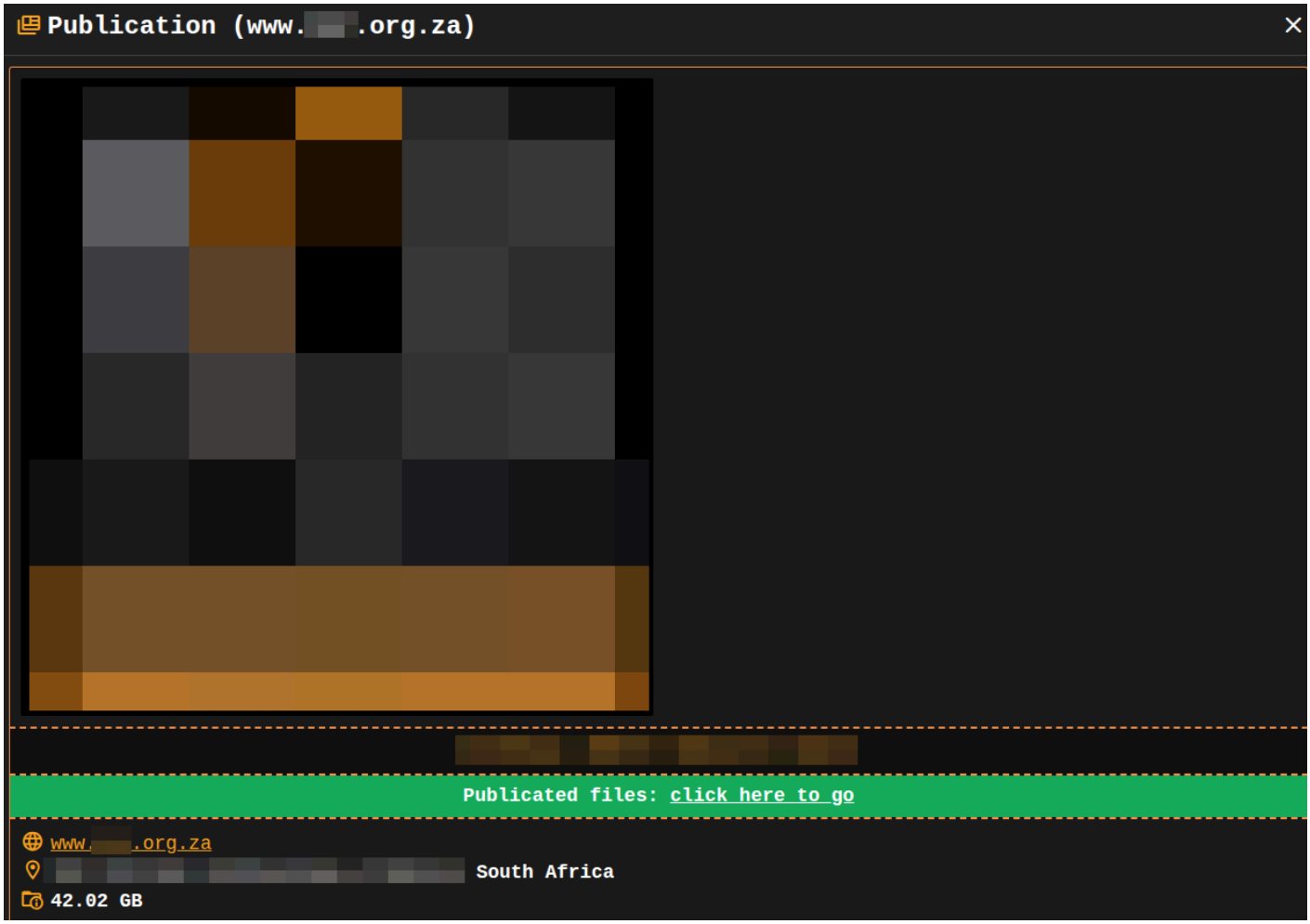
Recent Ransomware Activities Targeting the Finance Industry

Ransomware Group Claims Attack on Leasing Services in Romania



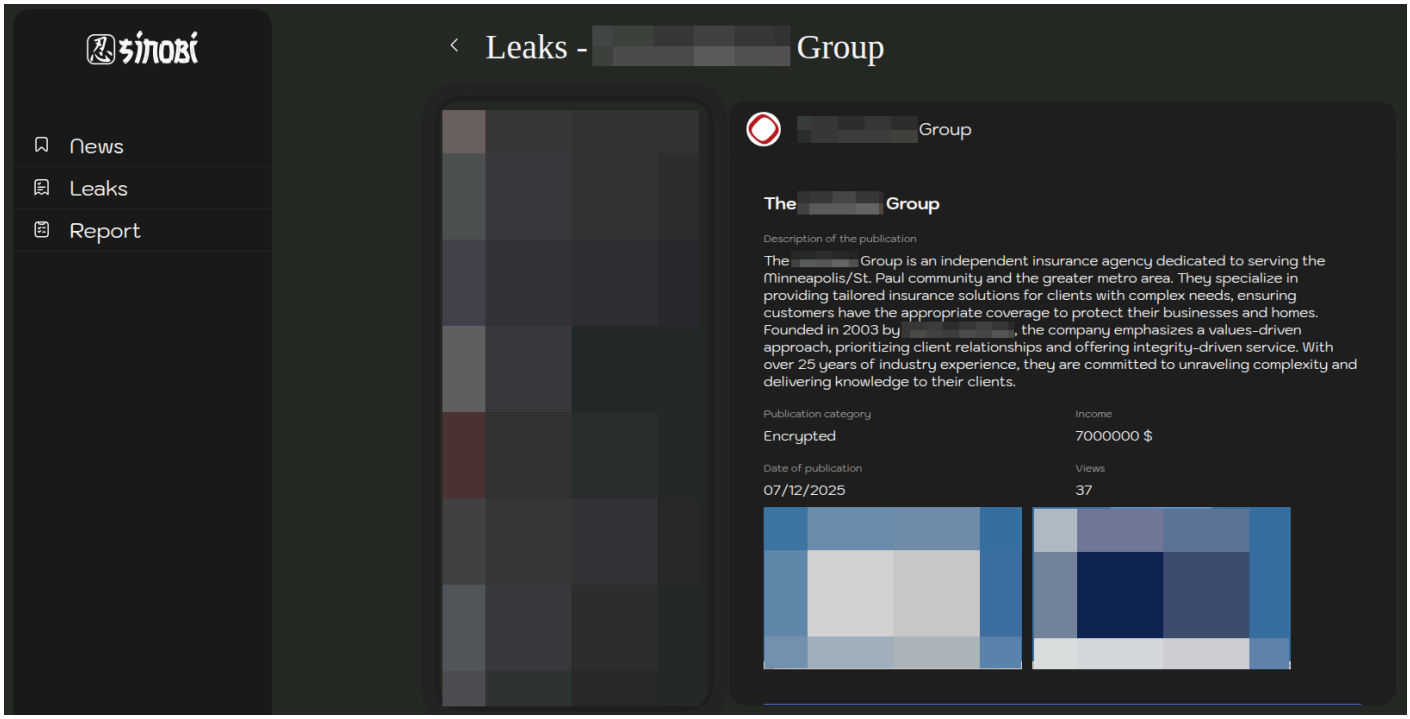
SOCRadar detected a new alleged ransomware victim listed on Qilin Ransomware group's leak site. The post claims a company in Romania providing leasing services was compromised. Such incidents may affect regulatory data and consumer protection records.

Ransomware Group Claims Attack on Credit Industry Regulator

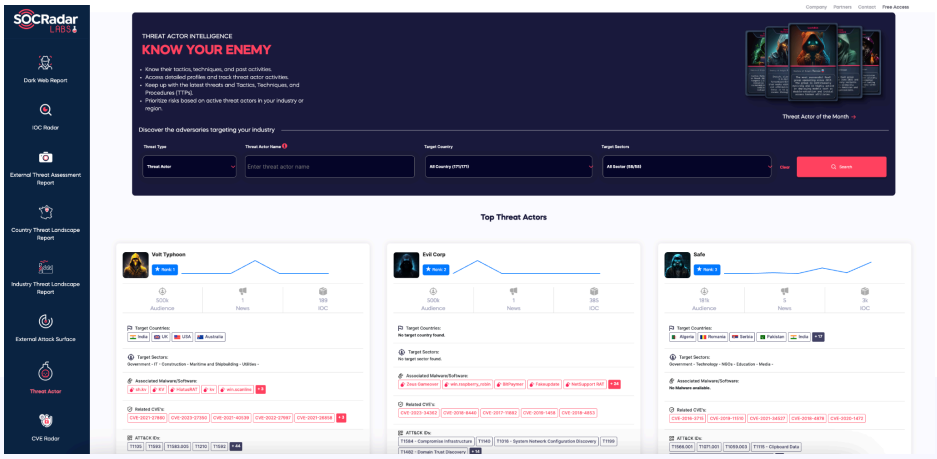


SOCRadar observed a new alleged ransomware victim listed by the DragonForce group. The post claims a statutory body in the public sector that regulates the credit industry was compromised. The organization oversees credit providers, bureaus, and debt counselors. Such incidents may affect regulatory data and consumer protection records.

Ransomware Group Claims Attack on Insurance Agency Services



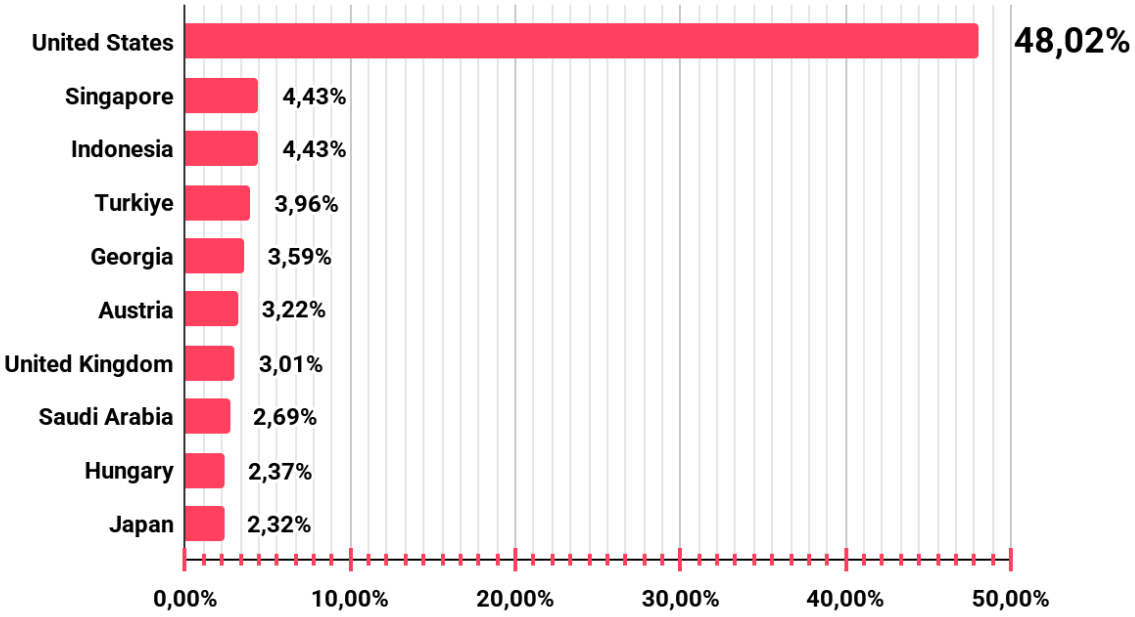
SOCRadar observed a new alleged ransomware victim listed by the Sinobi group. The post claims an independent insurance agency serving a metropolitan community was compromised. The organization provides tailored insurance coverage for businesses and homes. Such incidents may expose customer policy data and disrupt insurance service 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 the Finance Industry

Phishing Attacks - Distribution by Country

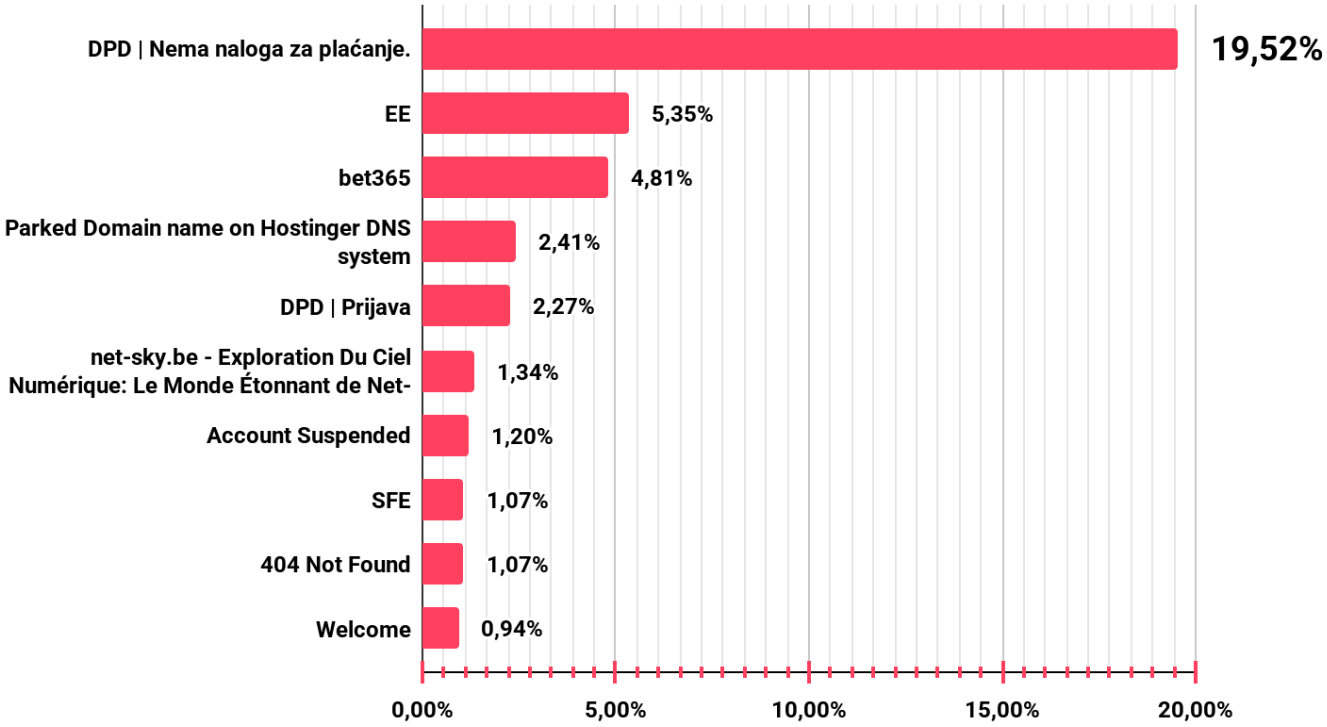


Phishing activity targeting the finance sector shows a very strong concentration in the United States, which accounts for 48.02% of all observed cases. This level is far above any other country. It shows that US financial users and institutions are primary targets for credential theft and fraud campaigns.

Several countries in Asia and Europe follow at much lower but notable levels.

One country. Half the risk. 48.02% concentration.

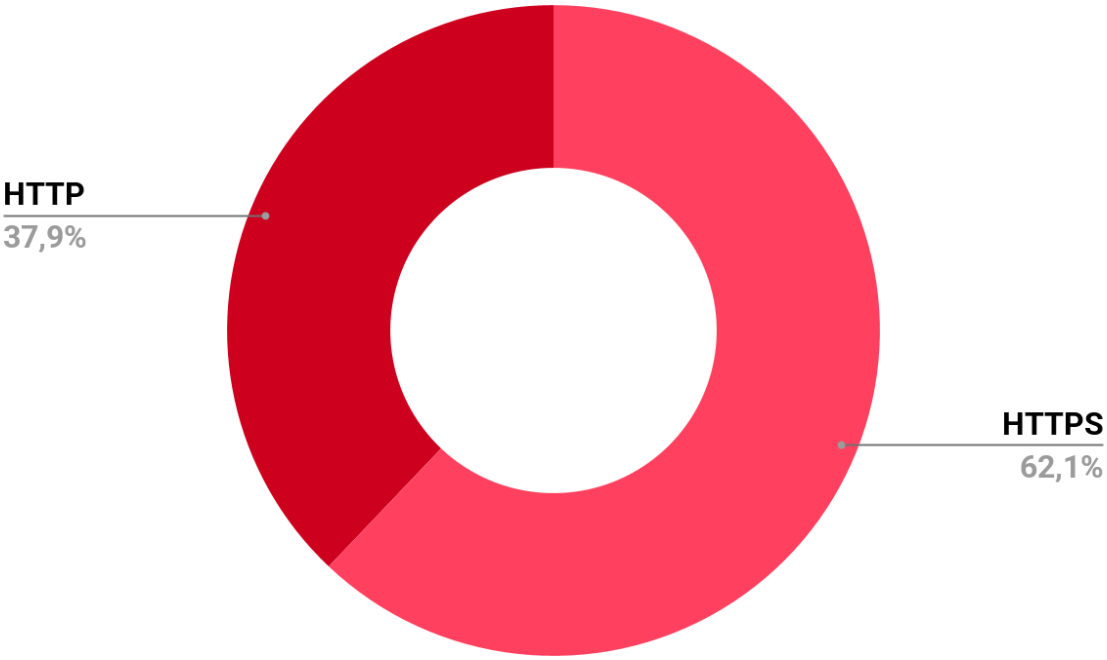
Phishing Attacks - Distribution by Phishing Page Title



Phishing pages targeting the finance sector often impersonate delivery services, betting platforms, and generic system messages. The most common title, “DPD | Nema naloga za plaćanje.” at 19.52%, shows a strong use of parcel delivery themes to trick users into entering credentials or payment data. A similar title, “DPD | Prijava,” also appears, which confirms repeated abuse of the same brand.

This distribution shows that phishing actors focus on familiar brands and urgent looking system messages. The goal is fast user interaction and credential harvesting rather than complex social engineering.

Phishing Attacks - Distribution by SSL/TLS Protocol



The padlock is a lie: 62% of phishing sites use HTTPS to hide in plain sight.

Most phishing pages targeting the finance sector are hosted over HTTPS, which accounts for 62.1% of observed cases. This shows that attackers actively use SSL certificates to make their pages look legitimate. Users often associate the padlock icon with safety, and threat actors exploit this trust to increase success rates.

A significant portion, 37.9%, still operates over plain HTTP. This indicates that many phishing campaigns do not rely on technical sophistication. They rely on speed, scale, and user inattention rather than advanced infrastructure.

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.