The Netherlands

Threat Landscape Report

SOCRadar®
Your Eyes Beyond

socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

Executive Summary

Top Takeaways

Over 830,000 credentials and 15,000 credit cards have been exposed through stealer logs, alongside thousands of victim IPs and password hashes—indicating widespread compromise and data monetization activity targeting Dutch users.

Ransomware threats are heavily skewed toward multinational organizations, with 80.2% of attacks affecting companies with a global footprint. The most targeted industries include Information (41.38%), Manufacturing, and Retail.

RansomHub, LockBit, and Akira are the most active ransomware groups in the region, though 73.5% of attacks are linked to lesser-known or emerging actors, suggesting a fragmented and rapidly evolving threat landscape.

Phishing campaigns remain persistent, especially against Information Services, Banking, National Security, and Cryptocurrency/NFT sectors, often mimicking brands like LinkedIn, iCloud, Telegram, and Nordea.

Dark web activity related to Dutch entities is dominated by data-related threats, with 59.3% of posts involving stolen data, followed by access sales (24.3%) and website compromises (11.9%). Retail, Finance, and E-commerce sectors are among the most frequently discussed industries.

The majority of dark web threat actor behavior (55.6%) involves selling data or access, while 35.1% involves sharing, often to gain reputation or collaborate with others.

Technical Details

This report based on data collected between April 2024 and March 2025

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

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 the Netherlands, their detailed profiles and the necessary data that summarizes the ransomware activities.

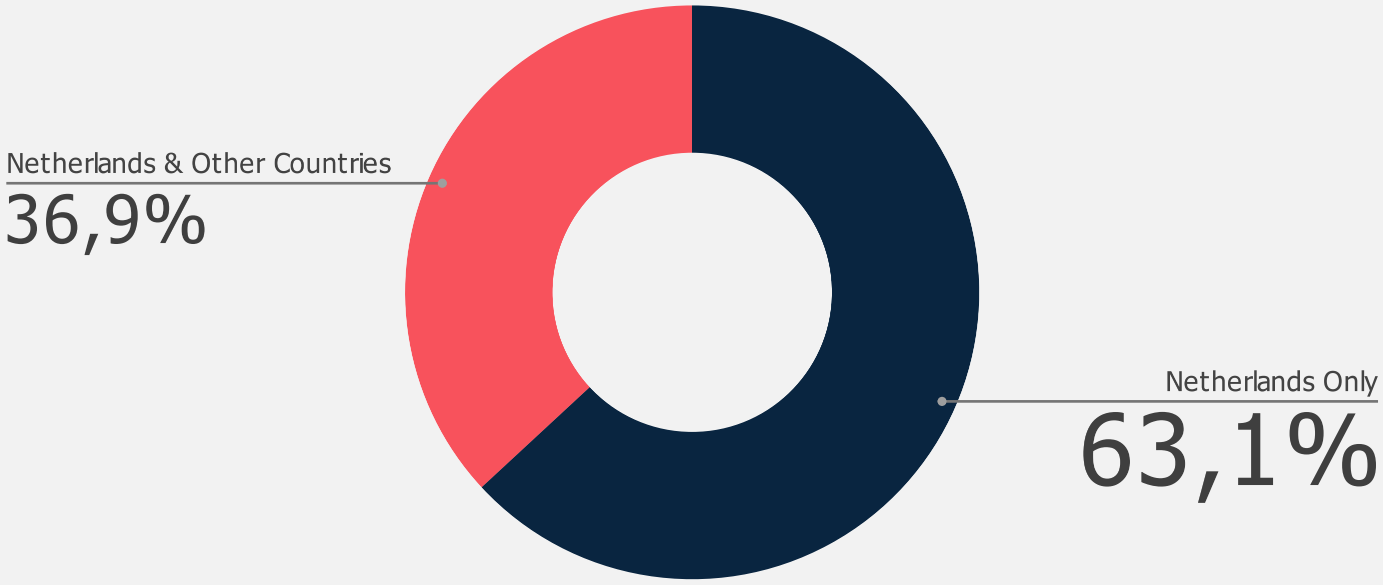
Stealer Logs Statistics chapter is all about stealer malware and the data around leaked credentials. These days, hackers don't hack, they log in. It is important to make sure that employee credentials are not compromised.

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.

And lastly, the DDoS Attack Statistics shows you the latest information about the intensity of DDoS attacks and how threat actors target organizations to disrupt their operations.

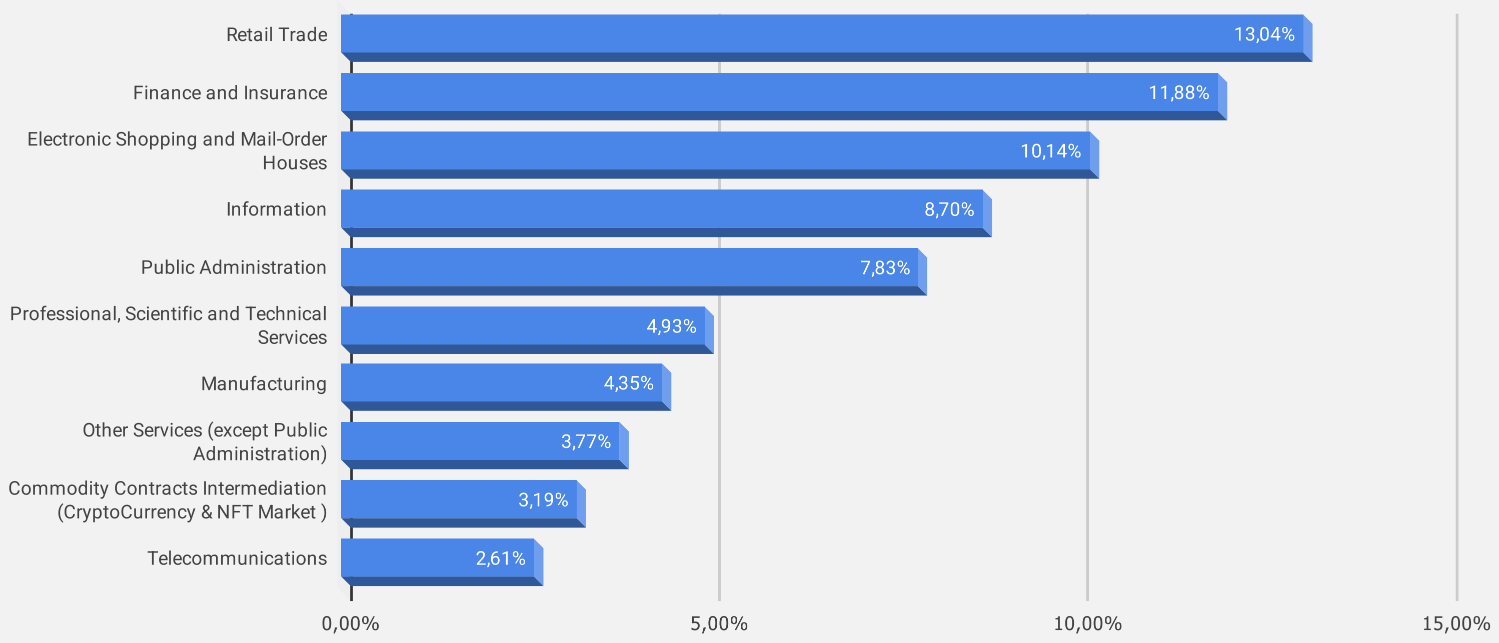
Dark Web Threats

Distribution of Dark Web Threats by Country



When we looked at cyber attacks targeting the Netherlands, we detected 36.9% of threats targeting other countries alongside the Netherlands. Analyzing the region of these countries, it is revealed that 52,90% of them are European countries, suggesting coordinated or broad campaigns by threat actors across the region.

Distribution of Dark Web Threats by Industry

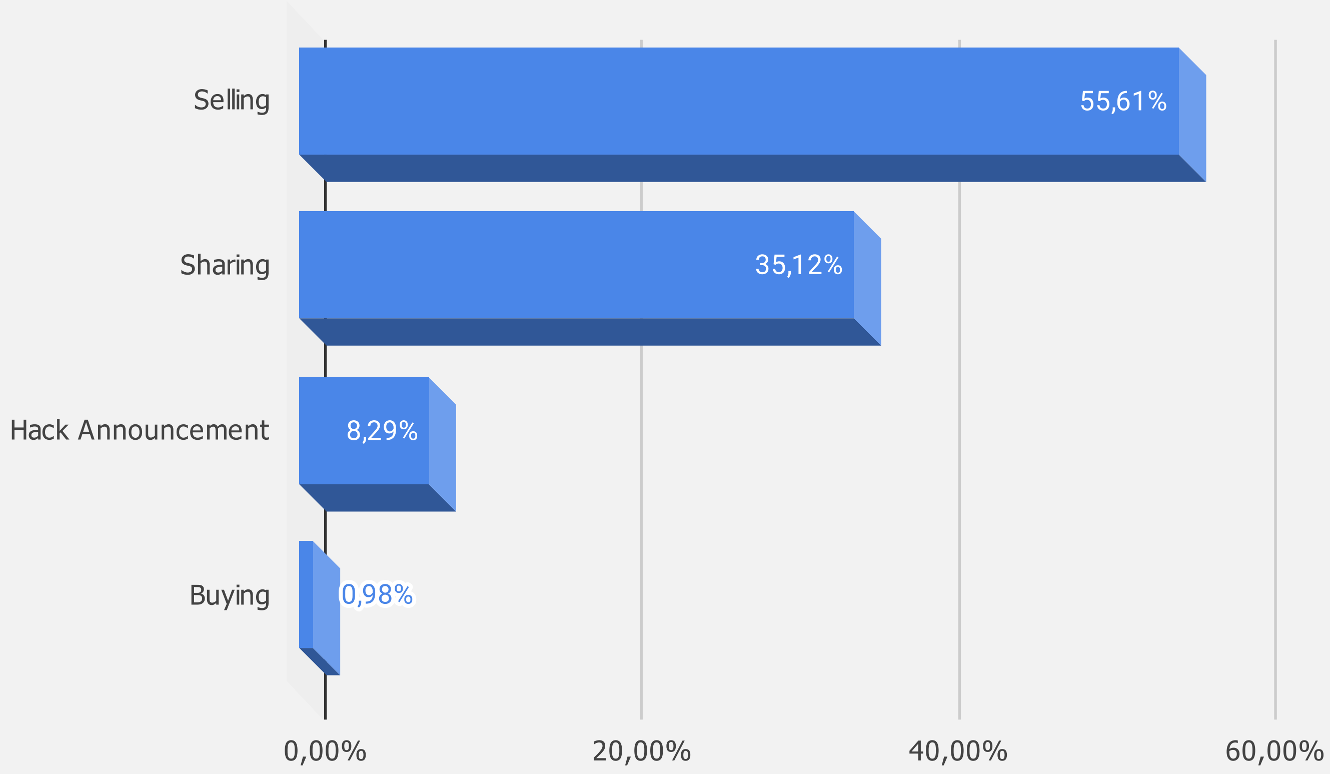


Our analysis of dark web activity highlights a concentration of threat actor interest in sectors with high-value data and digital infrastructure in the Netherlands. The Retail Trade sector is the most discussed, comprising 13.04% of observed posts, likely due to the sector's broad attack surface, volume of personal financial data, and increased e-commerce integration.

The Finance and Insurance sector follows closely at 11.88%, aligning with known priorities of financially motivated actors targeting banking credentials, payment card data, and access to financial systems. Notably, Electronic Shopping and Mail-Order Houses rank third (10.14%), suggesting a focus on digital retail platforms, possibly driven by credential stuffing, refund fraud, and API vulnerabilities.

These trends suggest that cybercriminal forums continue to prioritize industries with a blend of transactional volume, data value, and potential network pivot points. Organizations operating in or adjacent to these sectors in the Netherlands should remain alert to fraud, access brokerage, and ransomware precursor activities stemming from the dark web.

Distribution of Dark Web Threats by Threat Categories



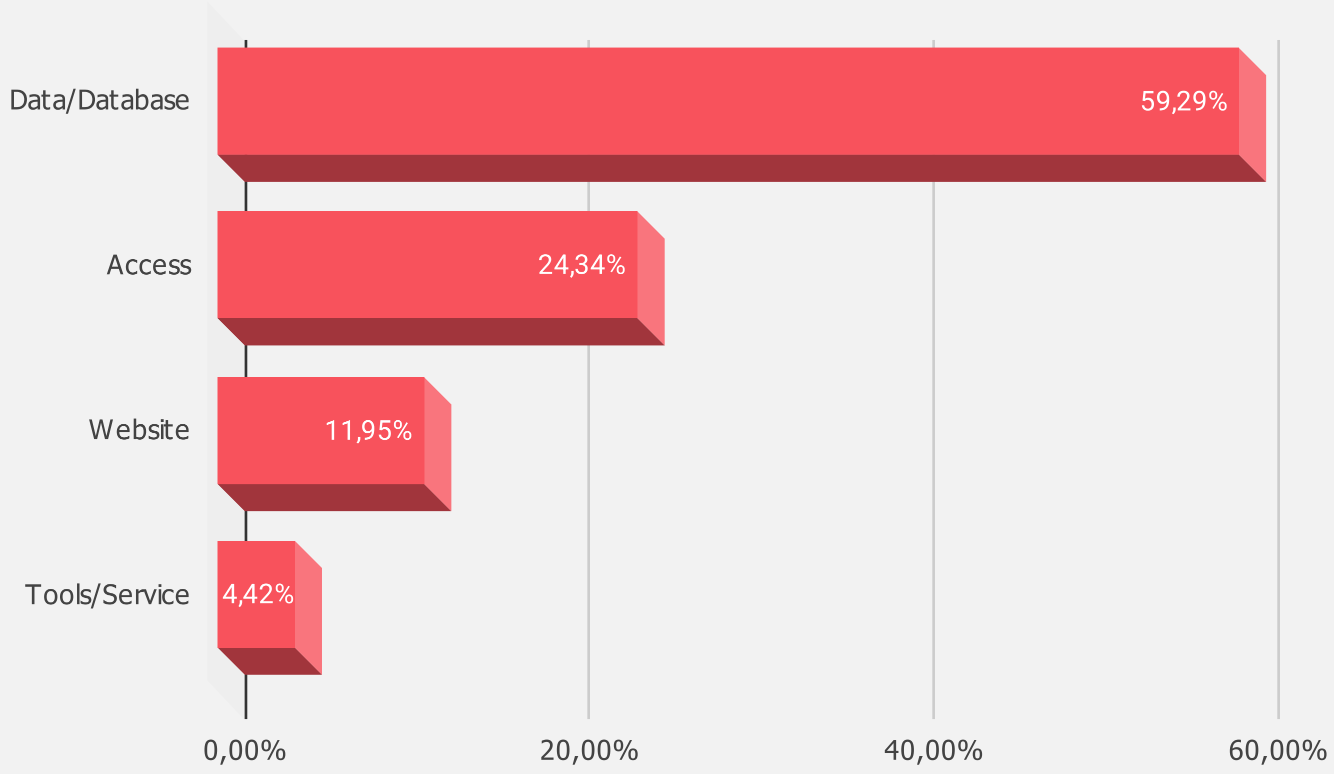
The latest analysis of threat activity indicates a clear pattern in the types of engagements, with Selling posts comprising the dominant share at 55.61%. This reflects an ongoing trend where threat actors primarily engage in the sale of illicit goods and services, including access to compromised systems, malware, and personal data.

Sharing posts follow at 35.12%, which includes the exchange of free data, intelligence, exploits, and collaboration between actors. This activity suggests a strong collaborative element within dark web communities, where actors often share tools, tactics, and information to advance their operations or exploit vulnerabilities.

A smaller portion, Hack Announcements (8.29%), typically signifies public disclosures of successful breaches or attacks, either to claim responsibility, gain notoriety, or taunt victims. This aligns with the broader trend of cybercriminals and hacktivists seeking recognition or leveraging breaches for reputational gain.

The overall distribution of these categories underscores a marketplace-centric dark web, where cybercriminals are focused on selling and exchanging access to cyber capabilities. This highlights the need for organizations to monitor not only the assets that might be targeted but also potential exposure on the dark web, especially in sectors with high-value data or digital assets.

Distribution of Dark Web Threats by Threat Types



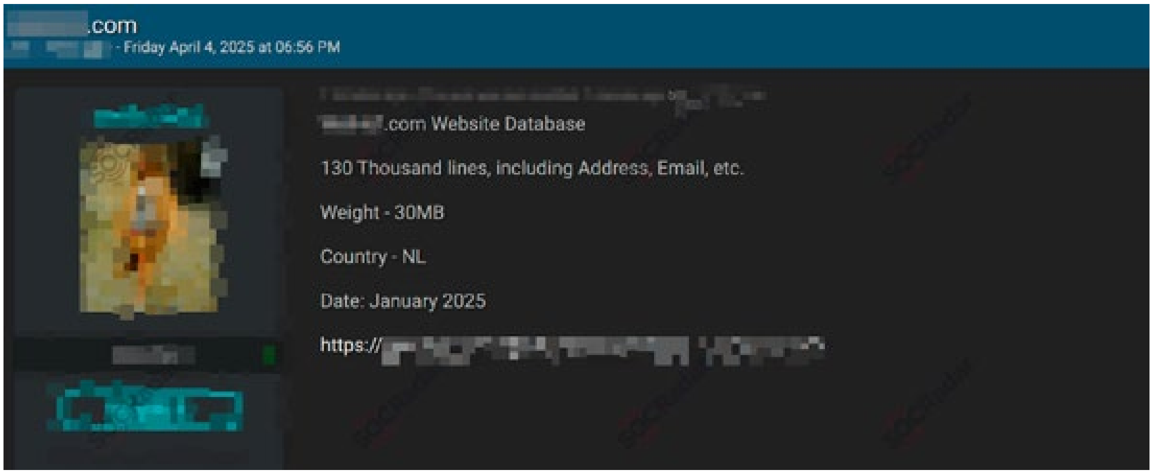
The analysis of threat types on dark web forums reveals a significant focus on high-value targets, with Data/Database threats dominating at 59.29%. This reflects the continuing priority placed by threat actors on obtaining sensitive, valuable data such as personal information, financial records, and proprietary business data.

Access threats follow at 24.34%, pointing to the growing demand for unauthorized access to networks, systems, and accounts.

The Website threat type accounts for 11.95% of posts. This involves exploiting vulnerabilities in website infrastructure, either for defacement, deploying malware, or using compromised websites as launching points for further attacks.

Recent Dark Web Activities Targeting the Entities in The Netherlands

Online Marketplace Focuses on Refurbished White Goods was Allegedly Breached



[redacted].com
[redacted] - Friday April 4, 2025 at 06:56 PM

[redacted]

[redacted].com Website Database

130 Thousand lines, including Address, Email, etc.

Weight - 30MB

Country - NL

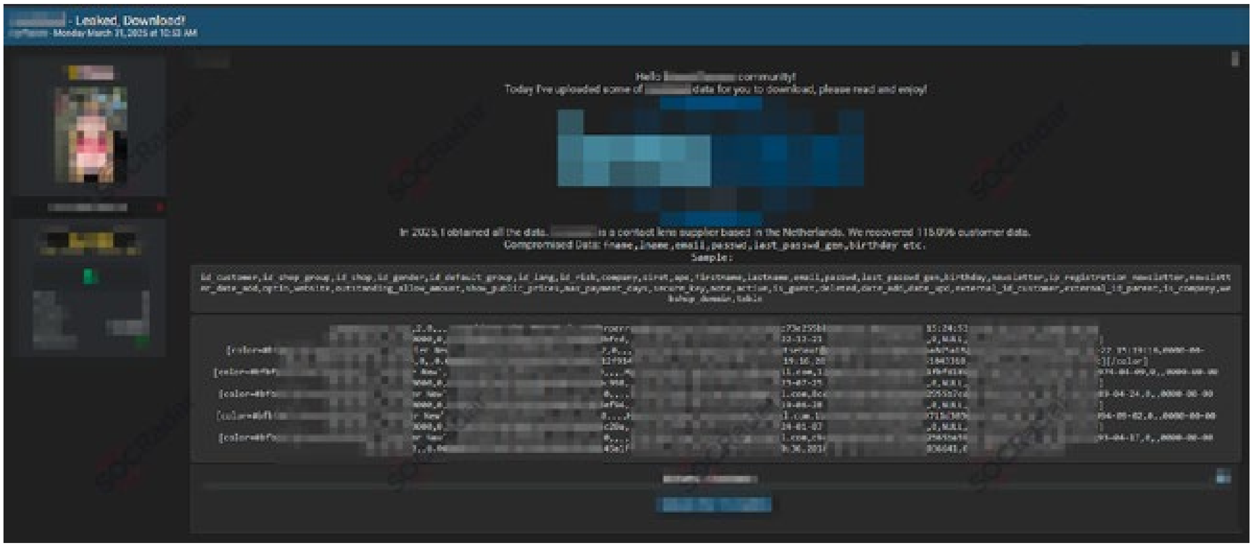
Date: January 2025

https://[redacted]

In a dark web forum monitored by SOCRadar, a threat actor published a database leak for an online marketplace.

The company is a retailer specializing in high-quality used and refurbished white goods, electronics, and bicycles. They focus on sustainability by giving pre-owned products a second life.

Contact Lens Supplier was Allegedly Breached



[redacted] - Leaked, Download!

[redacted] - Monday March 31, 2025 at 10:53 AM

Hello [redacted] community!
Today I've uploaded some of [redacted] data for you to download, please read and enjoy!

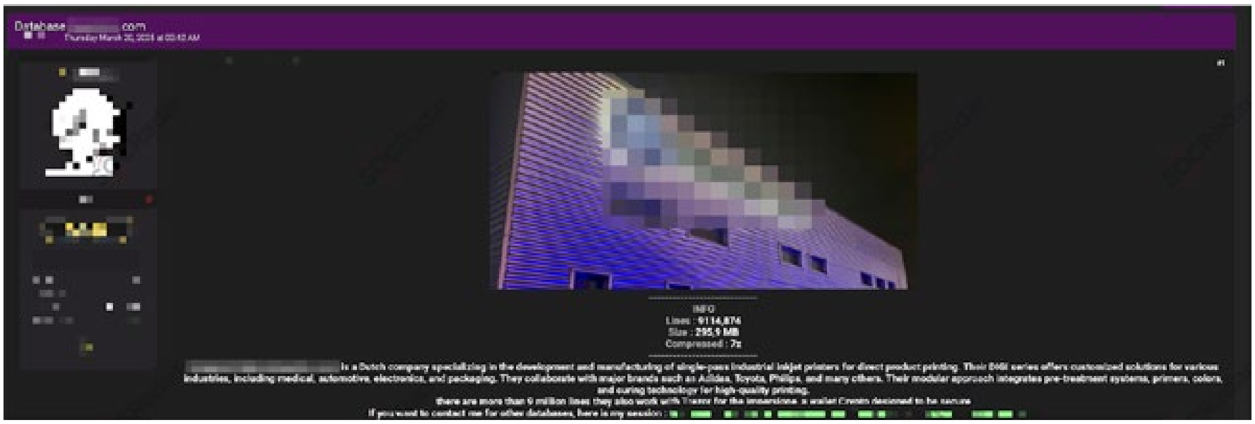
In 2025 I obtained all the data. [redacted] is a contact lens supplier based in the Netherlands. We recovered 115.096 customer data.
Compromised Data: fname,lname,email,passwd,last_passwd_gen,birthday etc.
Sample:

```
id_customer,id_shop_group,id_shop,id_gender,id_default_group,id_lang,id_risk,company,siret,ape,firstname,lastname,email,passwd,last_passwd_gen,birthday,newsletter,ip_registration_newsletter,newsletter_date_add,optin,website,outstanding_allow_amount,show_public_prices,max_payment_days,secure_key,note,active,is_guest,deleted,date_add,date_upd,external_id_customer,external_id_parent,is_company,webshop_domain,table
```

[redacted]

In a dark web forum monitored by SOCRadar, a new alleged database leak is detected for a lens supplier, based in the Netherlands.

Digital Services Company was Allegedly Breached



Database [redacted] .com

Thursday March 20, 2025 at 03:40 AM

INFO
Lines : 9114,874
Size : 295,9 MB
Compressed : 7z

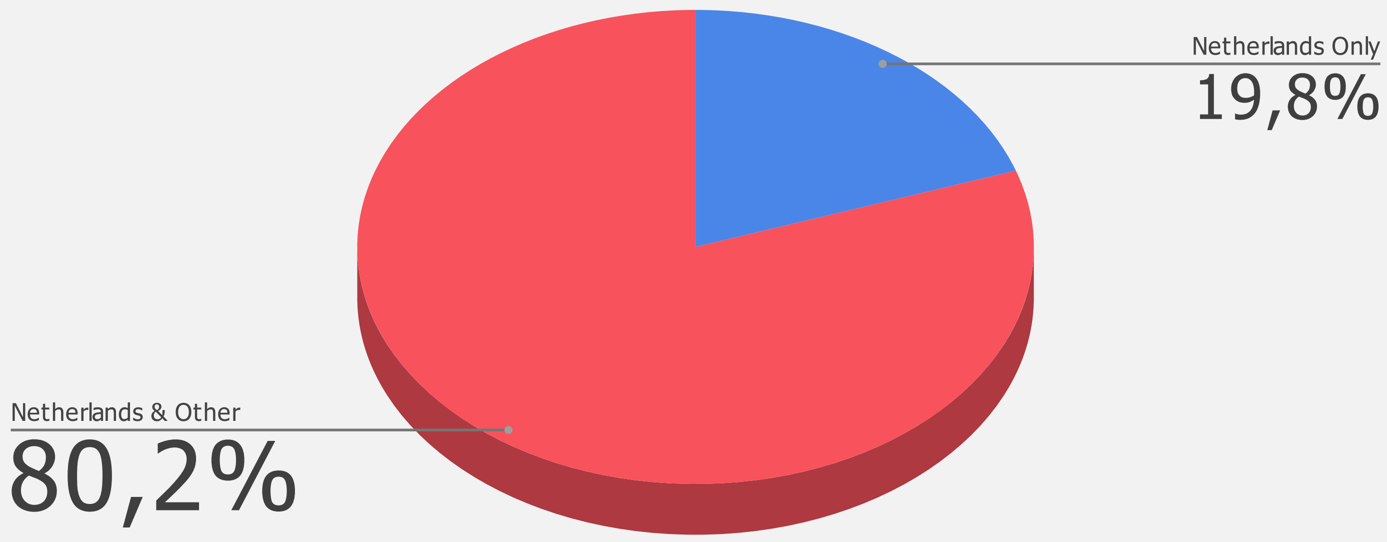
[redacted] is a Dutch company specializing in the development and manufacturing of single-pass industrial inkjet printers for direct product printing. Their [illegible] series offers customized solutions for various industries, including medical, automotive, electronics, and packaging. They collaborate with major brands such as Adidas, Toyota, Philips, and many others. Their modular approach integrates pre-treatment systems, primers, colors, and curing technology for high-quality printing.
there are more than 9 million lines they also work with Trezor for the immersions a wallet Crypto designed to be secure
If you want to contact me for other databases, here is my session : [redacted]

In a hacker forum monitored by SOCRadar, a new alleged database leak is detected for a digital services company.

It is a Dutch company specializing in the development and manufacturing of single-pass industrial inkjet printers for direct product printing. They offer customized solutions for various industries, including medical, automotive, electronics, and packaging. They collaborate with major brands such as Adidas, Toyota, Philips, and many others.

Ransomware Threats

Distribution of Ransomware Attacks by Country

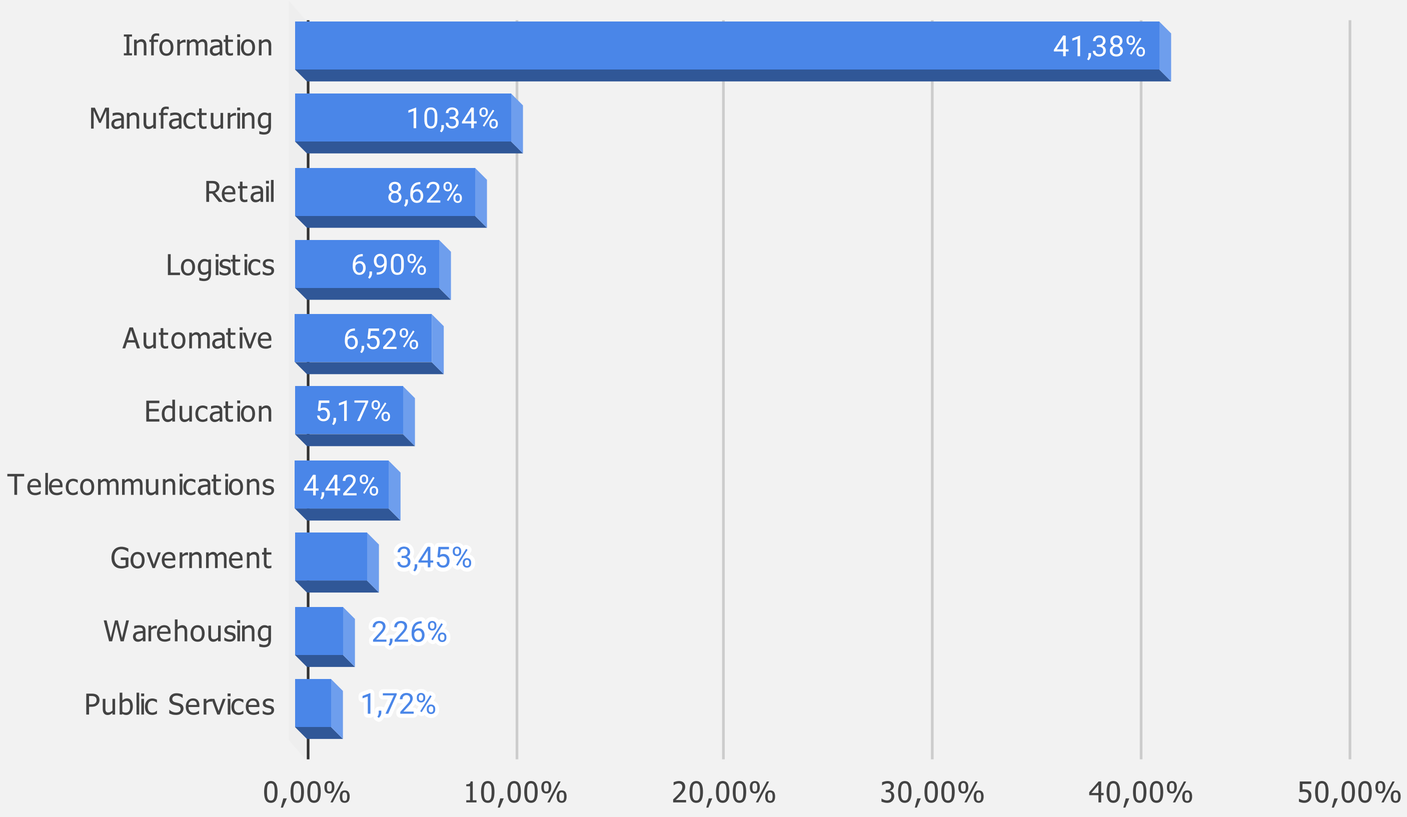


SOCRadar's data on ransomware attacks reveals a significant trend where 80.2% of ransomware attacks targeting organizations in the Netherlands also affect companies with branches in other countries.

Attacking companies with international operations provides broader leverage, as these organizations are often more dependent on interconnected systems and supply chains. The disruption of such organizations can have far-reaching consequences across various countries, amplifying the pressure on the victims to comply with ransom demands.

On the other hand, 19.8% of attacks are focused on companies with operations exclusively in the Netherlands. While this represents a smaller share, it still highlights the risk to local entities that may not have the complex, multinational infrastructure but could still be vulnerable due to insufficient cybersecurity measures or valuable data assets.

Distribution of Ransomware Attacks by Industry



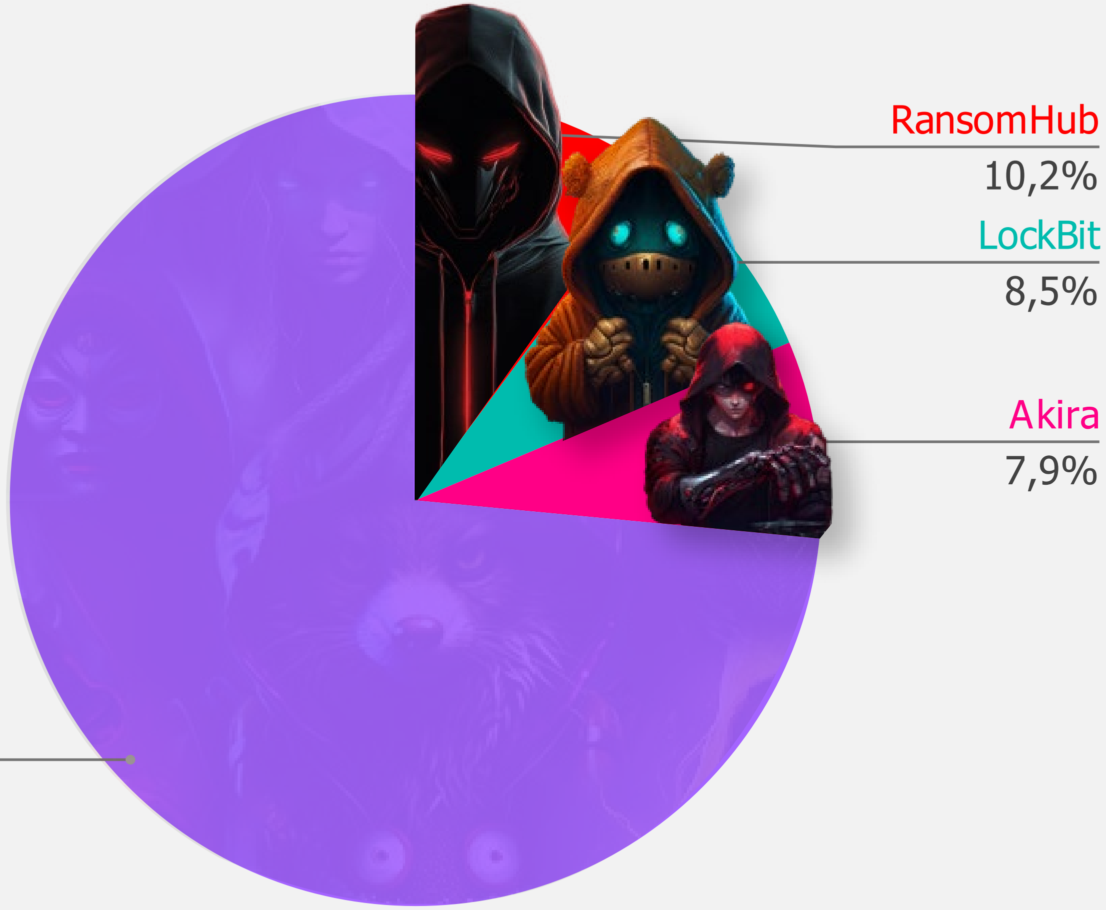
Recent data on ransomware attacks highlights significant targeting of high-value and digitally dependent sectors, with the Information industry leading the pack at 41.38%. This suggests that attackers continue to prioritize organizations in the information sector, which likely includes tech companies, data providers, and entities managing sensitive or high volumes of data.

Given the sector's critical role in infrastructure and the potential disruption caused by a ransomware attack, the focus here aligns with the broader trend of targeting entities with high operational dependencies on digital platforms.

Manufacturing follows at 10.34%, reflecting ongoing cyber threats to industrial sectors. Manufacturing entities are increasingly seen as valuable targets due to their reliance on operational technology and the growing trend of digital transformation, which introduces new vulnerabilities. Ransomware attacks here could have significant operational and financial impacts, particularly on supply chains.

Retail ranks third at 8.62%, which is consistent with broader trends where cybercriminals target retailers due to their handling of financial transactions and consumer data. Ransomware attacks in this sector often aim to disrupt services and extort payments, particularly during peak retail seasons.

Top Ransomware Groups Targeting The Netherlands



The current landscape of ransomware groups targeting the Netherlands reveals a diverse array of actors. RansomHub leads with 10.17% of the observed activity, indicating a notable presence of this group in targeting organizations within the Netherlands.

LockBit, a well-established and notorious ransomware group, accounts for 8.47% of the ransomware activity.

Akira Ransomware, with 7.86% of ransomware incidents, is another significant threat actor targeting the Netherlands.

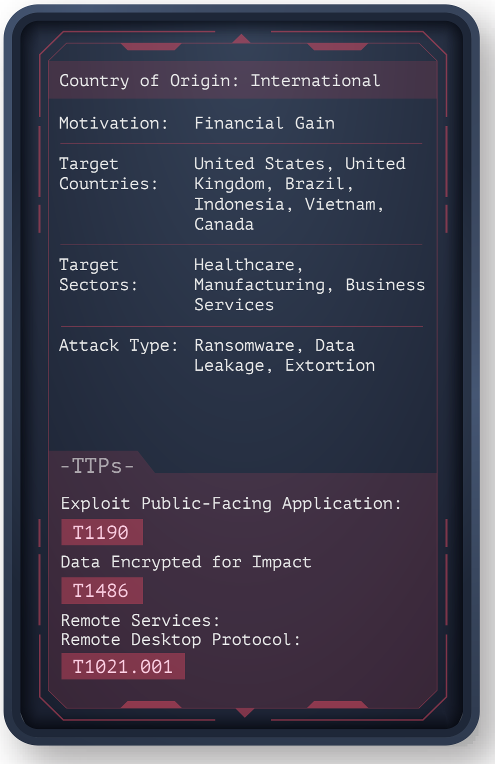
However, the largest share, 73.50%, is attributed to other, less identifiable groups. This broad category suggests a high level of activity from numerous smaller or emerging ransomware groups that may not yet have gained the notoriety of established players like LockBit or Akira but are nonetheless contributing significantly to the overall threat landscape.

In conclusion, while prominent groups like LockBit and Akira remain persistent threats, a significant portion of ransomware activity in the Netherlands comes from a wide array of smaller or less recognized groups. This underlines the need for comprehensive security measures and proactive threat detection to defend against both established and emerging ransomware actors.

A Closer Look into The Top 3 Ransomware Groups

RansomHub

RansomHub, emerging in early 2024, quickly became a major ransomware threat. Operating as a Ransomware-as-a-Service (RaaS), it targets diverse victims and exploits critical vulnerabilities, offering affiliates a large share of ransoms.



Country of Origin:	International
Motivation:	Financial Gain
Target Countries:	United States, United Kingdom, Brazil, Indonesia, Vietnam, Canada
Target Sectors:	Healthcare, Manufacturing, Business Services
Attack Type:	Ransomware, Data Leakage, Extortion

-TTPs-

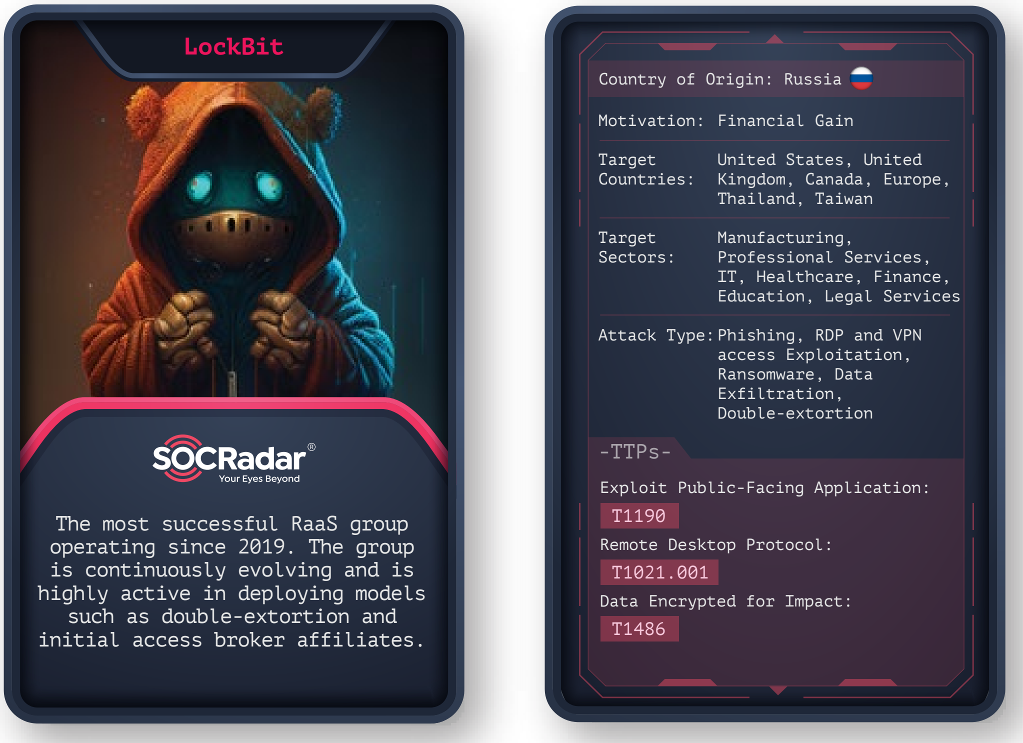
Exploit Public-Facing Application:
T1190
Data Encrypted for Impact
T1486
Remote Services:
Remote Desktop Protocol:
T1021.001

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.

LockBit



LockBit

The most successful RaaS group operating since 2019. The group is continuously evolving and is highly active in deploying models such as double-extortion and initial access broker affiliates.

Country of Origin: Russia

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

Threat Actor Card of Lockbit 3.0 Ransomware Group

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.

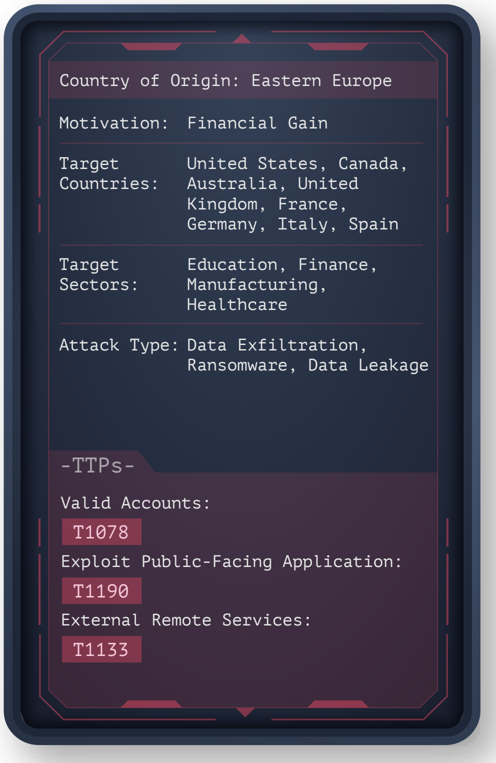
With over 1,500 victim disclosures on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's cessation. As of the first quarter of 2023, they retain their position as the most prolific group, with over 300 disclosed victims.

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

Akira

Akira Ransomware

Akira Ransomware, active since early 2023, known for its extortion strategy and distinctive data leak site, Akira has affected over 250 organizations and amassed approximately $42 million in ransomware proceeds.



Country of Origin: Eastern Europe

Motivation: Financial Gain

Target Countries: United States, Canada, Australia, United Kingdom, France, Germany, Italy, Spain

Target Sectors: Education, Finance, Manufacturing, Healthcare

Attack Type: Data Exfiltration, Ransomware, Data Leakage

-TTPs-

Valid Accounts: T1078

Exploit Public-Facing Application: T1190

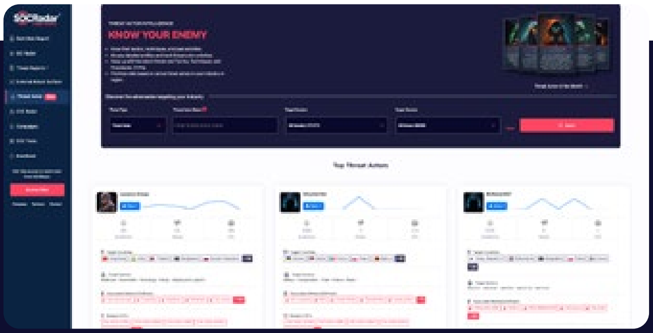
External Remote Services: T1133

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. This evolution and the unique aesthetic of its leak site and communications have drawn attention to its operations.

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.

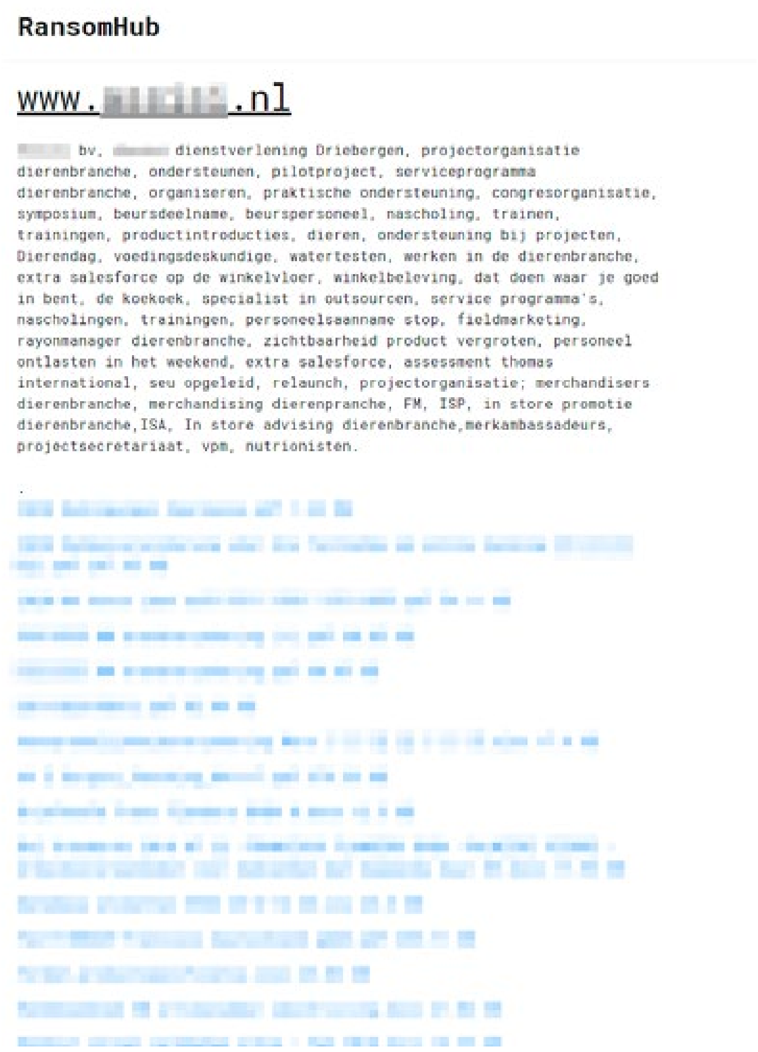


Threat Actor Intelligence Module

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.

Recent Ransomware Attacks Targeted Entities in The Netherlands

RansomHub Targets an Organization Company from the Netherlands



RansomHub

www.[redacted].nl

[redacted] bv, [redacted] dienstverlening Driebergen, projectorganisatie dierenbranche, ondersteunen, pilotproject, serviceprogramma dierenbranche, organiseren, praktische ondersteuning, congresorganisatie, symposium, beursdeelname, beurspersoneel, nascholing, trainen, trainingen, productintroducties, dieren, ondersteuning bij projecten, Dierendag, voedingsdeskundige, watertesten, werken in de dierenbranche, extra salesforce op de winkelvloer, winkelbeleving, dat doen waar je goed in bent, de koekoek, specialist in outsourcen, service programma's, nascholingen, trainingen, personeelsaanname stop, fieldmarketing, rayonmanager dierenbranche, zichtbaarheid product vergroten, personeel ontlasten in het weekend, extra salesforce, assessment thomas international, seu opgeleid, relaunch, projectorganisatie; merchandisers dierenbranche, merchandising dierenpranche, FM, ISP, in store promotie dierenbranche,ISA, In store advising dierenbranche,merkambassadeurs, projectsecretariaat, vpm, nutrionisten.

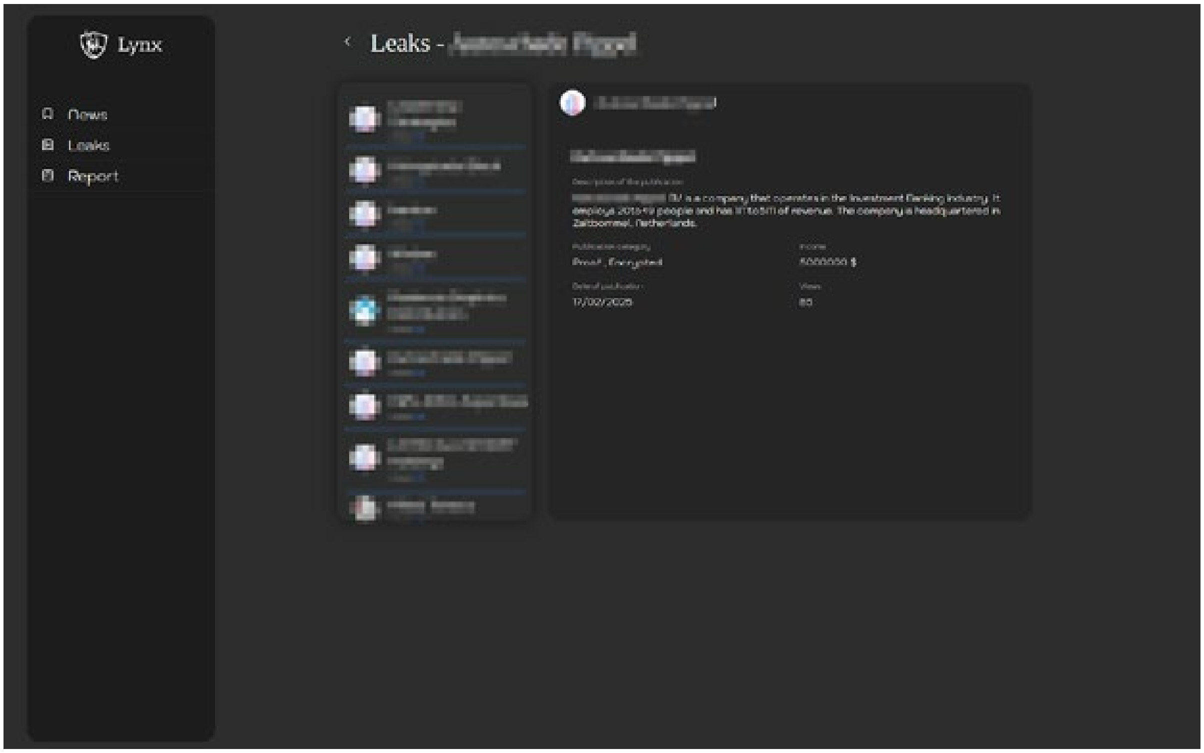
.

[redacted]

In the ransomhub ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as a consulting and organization firm.

The company specializes in practical support and field marketing for the animal industry. They provide customized service programs, organize events like trade shows and conferences, offer in-store promotions and merchandising, and supply trained professionals such as brand ambassadors, merchandisers, and nutritionists.

Lynx Ransomware Targets an Investment Bank



Leaks - [redacted]

[redacted]

[redacted]

Description of the publication

[redacted] BV is a company that operates in the Investment Banking industry. It employs 20 to 49 people and has $1 to 5M of revenue. The company is headquartered in Zaltbommel, Netherlands.

Publication category: Proof , Encrypted

Income: 5000000 $

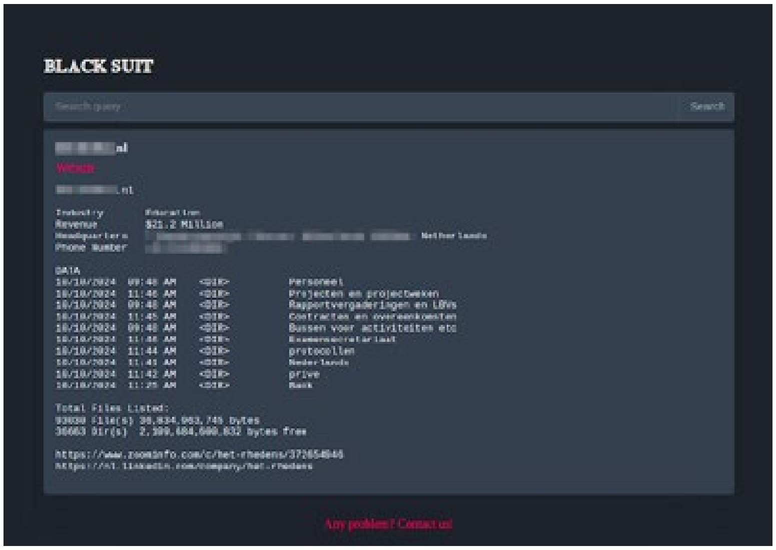
Date of publication: 17/02/2025

Views: 80

According to the Lynx ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as an investment bank.

The company that operates in the Investment Banking industry. It employs 20 to 49 people and it is headquartered in Zaltbommel, Netherlands.

Lynx Ransomware Targets an Investment Bank



```
[redacted].nl

[redacted].nl

Industry          Education
Revenue           $21.2 Million
Headquarters      [redacted] Netherlands
Phone Number      [redacted]

DATA
10/10/2024  09:48 AM    <DIR>         Personeel
10/10/2024  11:46 AM    <DIR>         Projecten en projectweken
10/10/2024  09:48 AM    <DIR>         Rapportvergaderingen en LOVs
10/10/2024  11:45 AM    <DIR>         Contracten en overeenkomsten
10/10/2024  09:48 AM    <DIR>         Bussen voor activiteiten etc
10/10/2024  11:46 AM    <DIR>         Examensecretariaat
10/10/2024  11:44 AM    <DIR>         protocollen
10/10/2024  11:41 AM    <DIR>         Nederlands
10/10/2024  11:42 AM    <DIR>         prive
10/10/2024  11:25 AM    <DIR>         Bank

Total Files Listed:
93030 File(s) 38,834,983,745 bytes
36663 Dir(s)  2,399,484,088,832 bytes free

https://www.zoominfo.com/c/het-rhedens/372654046
https://nl.linkedin.com/company/het-rhedens
```

The school has several locations and offers all types of secondary education, from practical learning to grammar school. They help students grow their talents and become confident, social, and involved people.

Stealer Log Statistics

Stealer Log Statistics: Most Visited Domains in The Netherlands

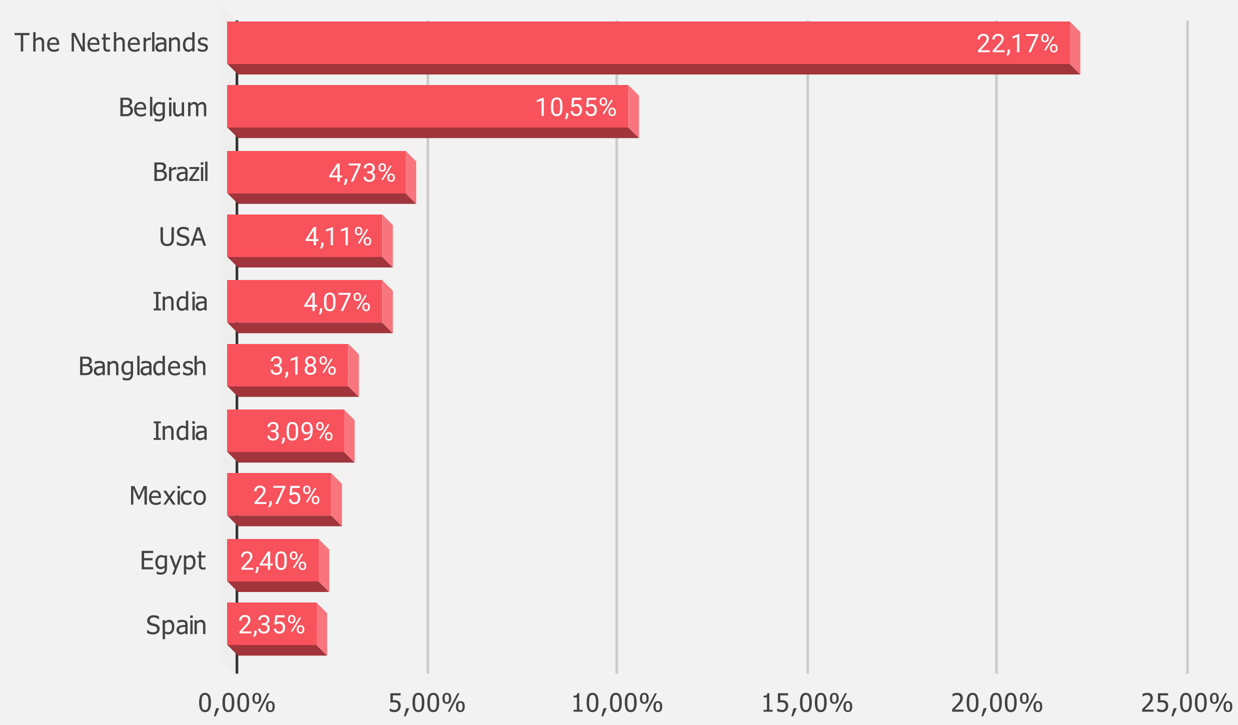
Stealers are a type of tool that collects sensitive data from victims' systems, primarily targeting login credentials, session tokens, and personal information. These logs, often produced by malicious software such as info stealers or keyloggers, can contain detailed information about the websites users visit, their login activities, and the credentials they input. Attackers use stealer logs to harvest credentials, gain unauthorized access to accounts, and orchestrate further attacks, including fraud, identity theft, or lateral movement within a network.

Monitoring and analyzing stealer logs is critical for identifying active threats and understanding attacker behavior, as these logs reveal which platforms are being targeted and how attackers are exploiting victims' data. By tracking these logs, organizations can gain valuable insight into high-risk domains, detect compromised accounts early, and implement targeted defensive measures to mitigate damage.

In order to detect these logs, it is useful to check the most visited domains in a specific country or industry. We analyzed the logs from the following domains in order to identify the leaked credentials that can be used to attack organizations in the Netherlands.

Most Visited Domains
ad.nl
ah.nl
amazon.nl
bol.com
buienradar.nl
destentor.nl
digid.nl
funda.nl
geenstijl.nl
gelderlander.nl

Stealer Logs - Distribution of the Compromised Data by Victim Country

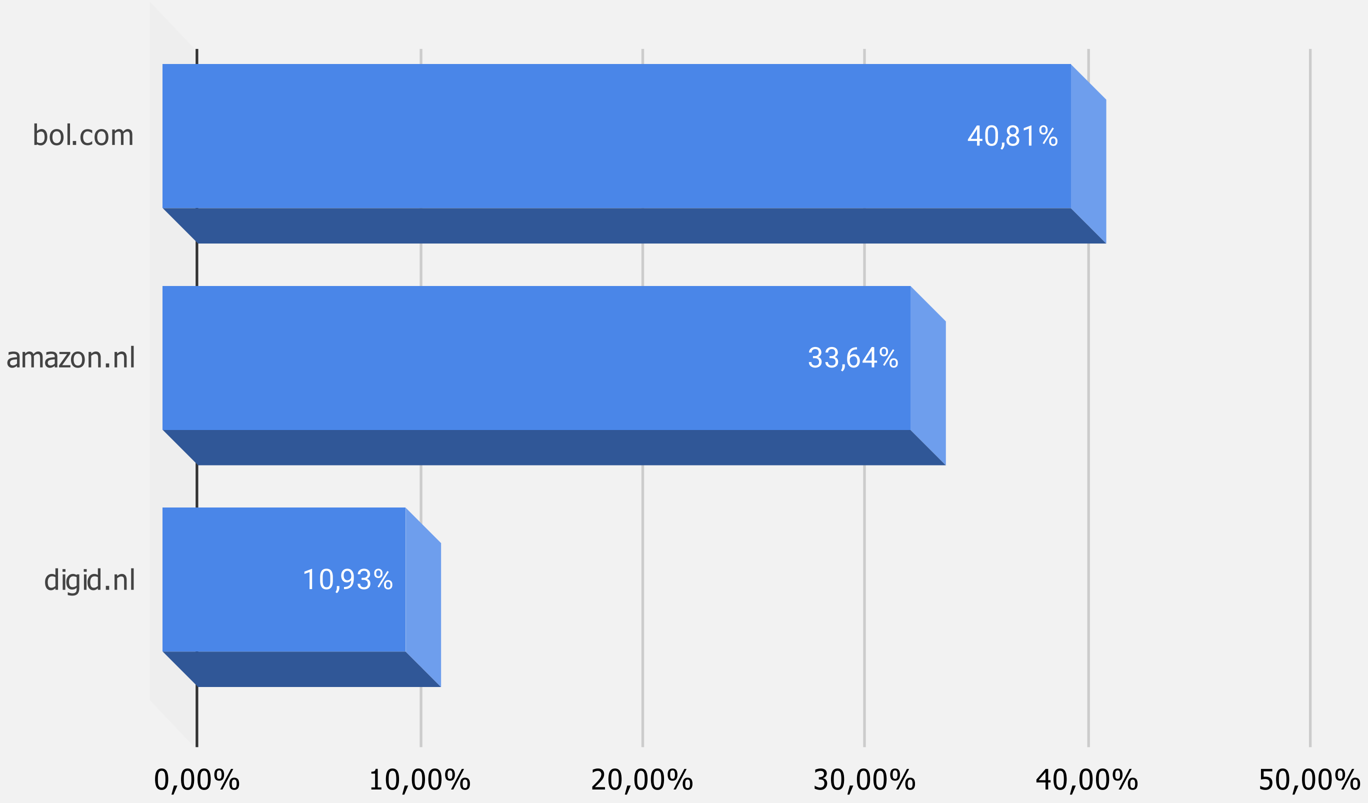


Analysis of stealer log data reveals the Netherlands as the most targeted country, accounting for 22.17% of all logged activity.

Belgium ranks second at 10.55%, which may reflect spillover from targeting campaigns in the Netherlands, given geographic proximity and linguistic overlap. Belgian users likely face similar risks due to comparable digital infrastructure and reliance on shared platforms and services.

Brazil follows at 4.73%, marking a notable presence of stealer malware in Latin America. The presence of Brazil in the top three shows the international impact of stealer malware and how employee data can be extracted from the most unexpected areas.

Stealer Logs - Distribution of the Compromised Data by Domains



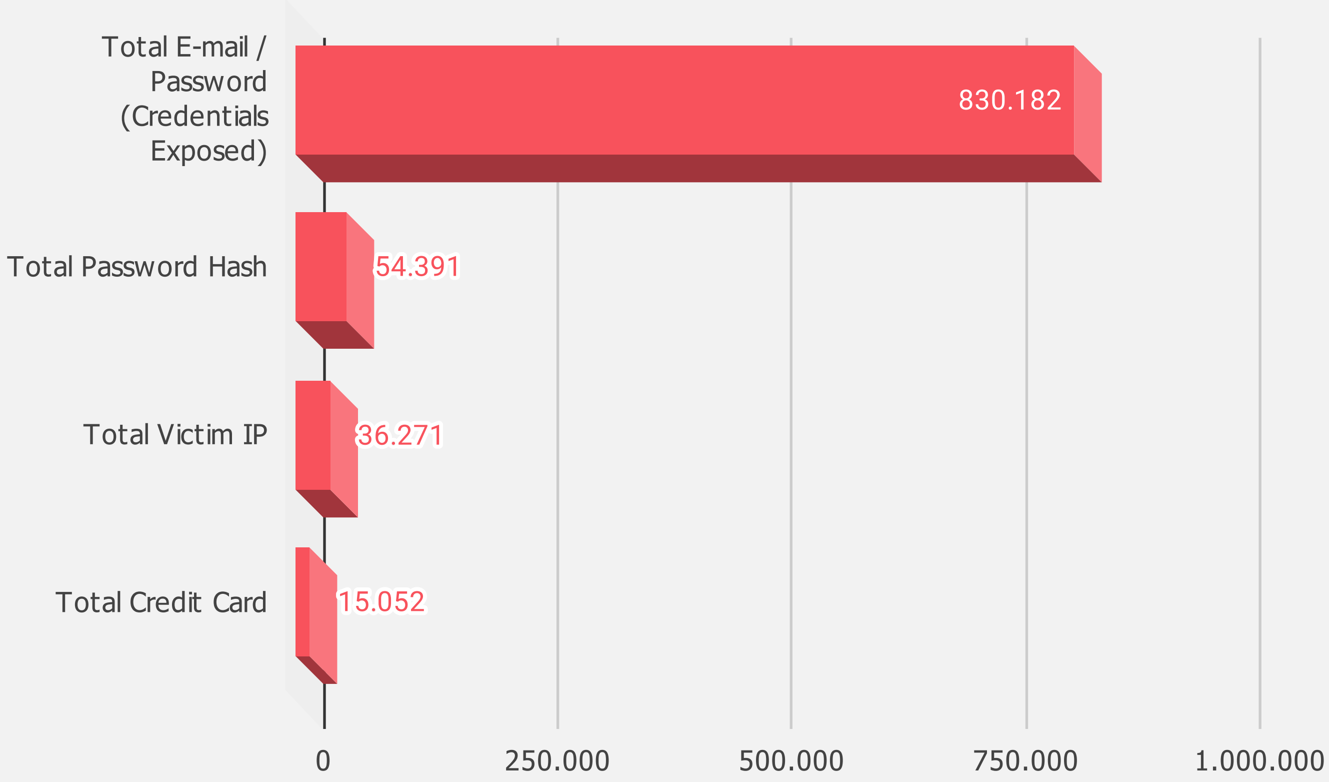
The latest data on stealer logs reveals a concentrated focus on a few key domains, with bol.com leading the list at 40.81%. It is one of the largest and most popular e-commerce platforms in the Netherlands.

amazon.nl follows closely at 33.64%, reflecting similar motivations behind the targeting of bol.com. Amazon.nl is a significant player in the Dutch e-commerce market, and the high number of stealer log searches related to this domain indicates its value to cybercriminals seeking to exploit accounts for unauthorized purchases, identity theft, or further exploitation in online marketplaces.

The third domain, digid.nl, is related to 10.93% of the stealer logs. DigiD is a crucial authentication platform for accessing government services in the Netherlands, which makes it an attractive target for cybercriminals looking to harvest personal information or gain access to sensitive governmental or social services.

85,38% of stealer logs from victim devices are related to most visited three domains. Organizations should consider using identity and access intelligence for detecting leaked employee credentials, to mitigate the risks posed by credential theft.

Stealer Logs - Distribution of the Compromised Data

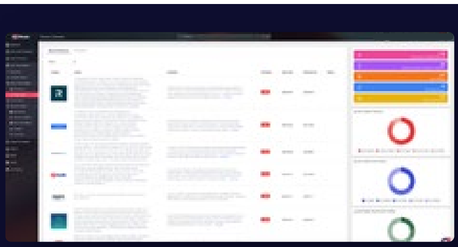


The analysis of stolen data from stealer logs reveals concerning quantities of sensitive information exposed to cybercriminals. The most significant category is Total E-mail/Password (Credentials Exposed), with a staggering 830,182 instances of compromised credentials. This represents a major risk, as the theft of email and password combinations can facilitate a wide range of malicious activities, including unauthorized access to accounts, identity theft, and further exploitation across multiple platforms (e.g., e-commerce, banking).

Total Password Hashes account for 54,391 stolen items, which could be used in credential stuffing attacks or cracked offline if the hashes are weak or unsalted. While password hashes are typically harder to exploit directly, they still pose a significant risk when paired with sufficient resources or weak hashing algorithms.

The theft of Total Victim IPs (36,271) also suggests the possibility of targeted attacks to victims.

In conclusion, the large volume of exposed credentials, passwords, and sensitive financial data highlights the con

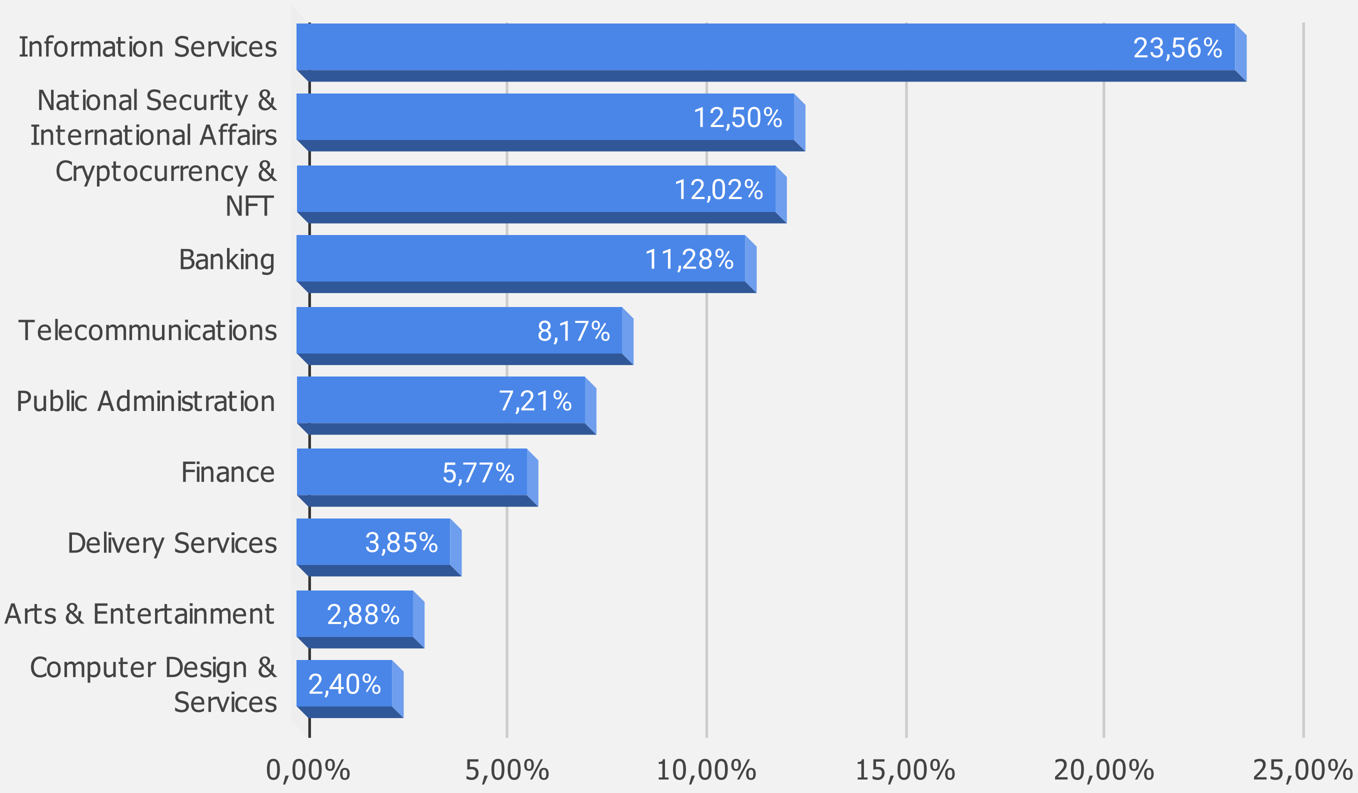


SOCRadar's Identity & Access Intelligence Module

SOCRadar's Identity & Access Intelligence Module can detect stealers on your devices and identify their location, facilitating a secure working environment. Changing passwords without eliminating stealers is insufficient to secure your organization, as it will only provide new passwords to threat actors.

Phishing Threats

Phishing Attacks - Distribution by Industry



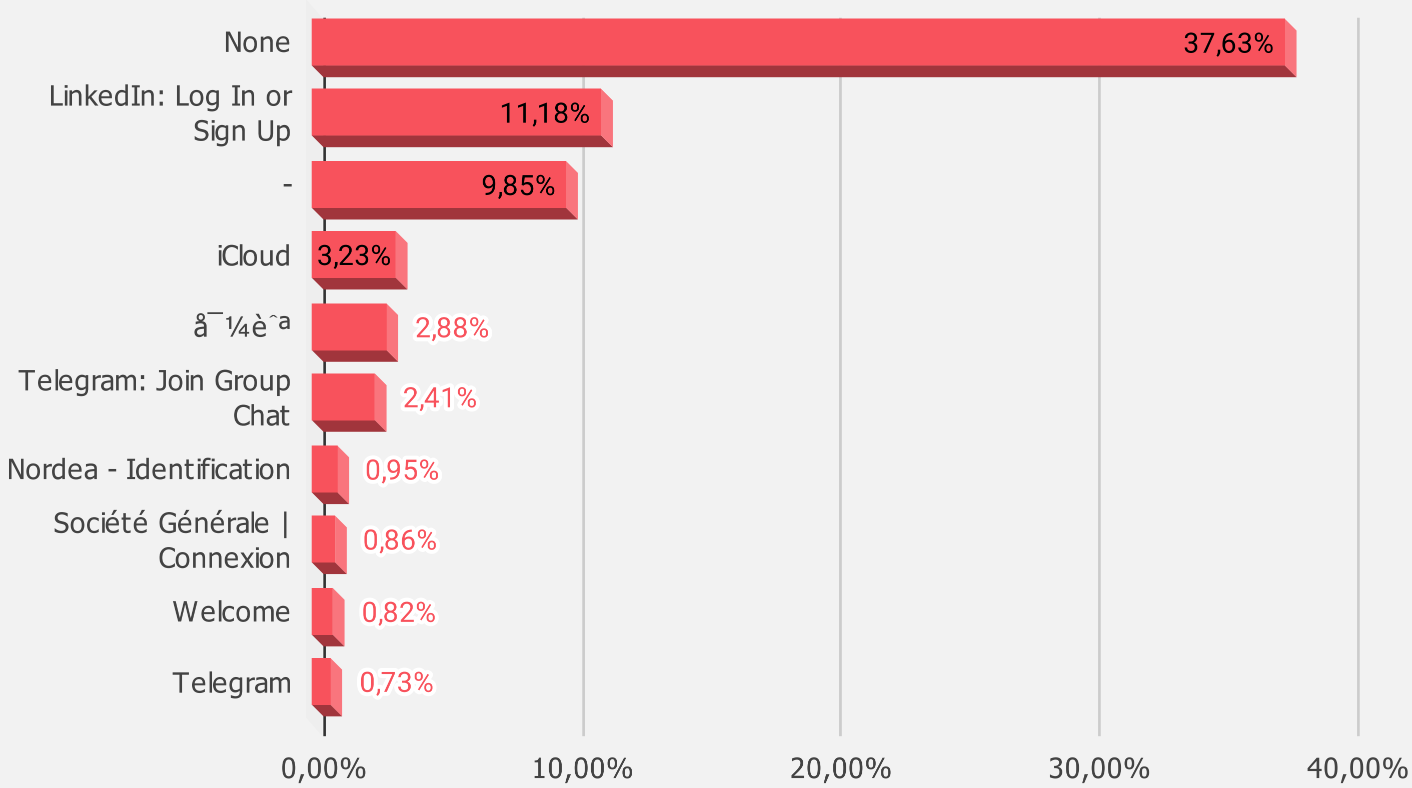
The distribution of phishing attacks across various industries reveals a concentrated focus on high-value, data-rich sectors. Information Services leads with 23.56% of observed phishing attempts. This suggests that threat actors are prioritizing the theft of data or access to systems within the information sector, likely due to the valuable data handled by organizations in this field, including intellectual property, business communications, and sensitive personal information.

National Security & International Affairs follows closely at 12.50%, reflecting ongoing geopolitical tensions and the potential for state-sponsored or hacktivist groups targeting governmental and international affairs entities. These attacks may be aimed at gathering intelligence, disrupting operations, or furthering political agendas through data theft or system disruption.

The Cryptocurrency & NFT sector account for 12.02% of phishing attacks, indicating a significant focus on industries dealing with financial transactions and digital assets. Cybercriminals are likely targeting individuals or organizations involved in cryptocurrency to steal login credentials, payment details, or to conduct fraud, especially given the increasing reliance on digital and decentralized finance systems.

In conclusion, phishing attacks in the Netherlands are concentrated in sectors with high financial value, sensitive data, or critical infrastructure. Organizations within these industries should prioritize phishing defense mechanisms such as advanced email filtering, user education, and multi-factor authentication (MFA) to mitigate the risk of data breaches and financial fraud through phishing.

Phishing Attacks - Distribution by Phishing Page Title



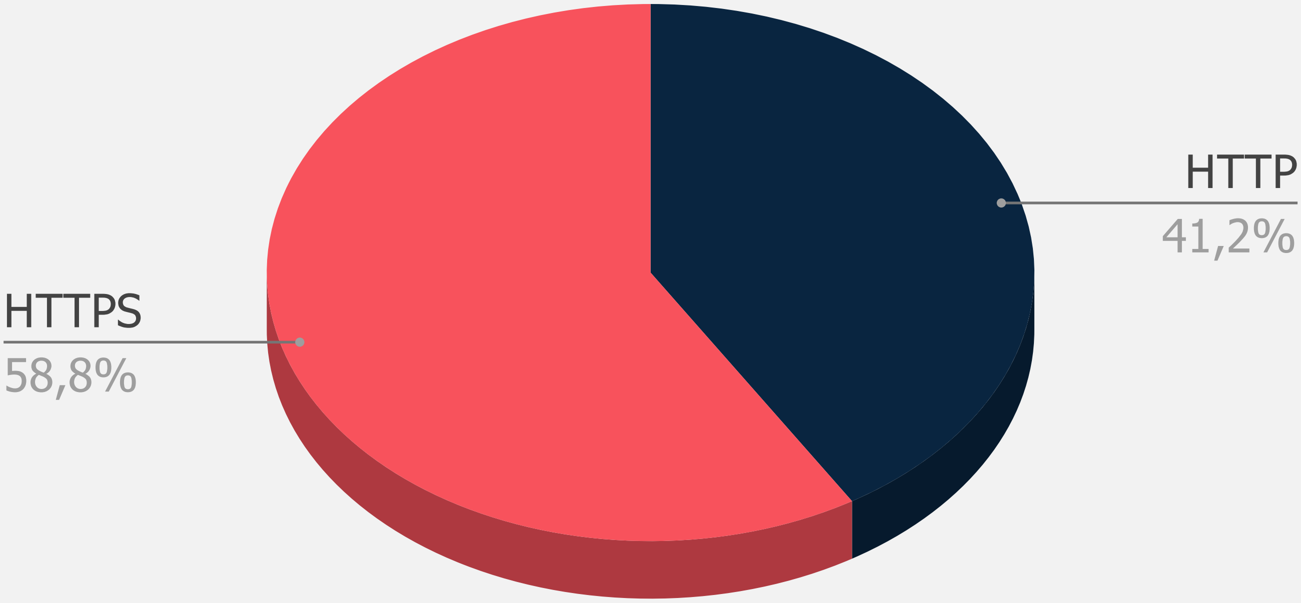
The title None is the most common, accounting for 37.63% of observed phishing attempts. This may indicate phishing campaigns where the page title is intentionally left blank or designed to resemble a generic or non-descript page, likely aiming to blend in and avoid suspicion.

"LinkedIn: Log In or Sign Up" appears in 11.18% of phishing attempts, reflecting the widespread targeting of professional networks.

"-" accounts for 9.85%, suggesting another form of generic or intentionally obfuscated page title. This may be used in phishing attempts to make the page appear legitimate or neutral, reducing the likelihood of immediate detection.

Phishing attempts in the Netherlands are focused on popular platforms like LinkedIn, iCloud, and Telegram, where users may be more likely to fall for fake login prompts or social engineering tactics. To mitigate these risks, organizations should invest in user awareness campaigns.

Phishing Attacks - Distribution by SSL/TLS Protocol



The analysis of SSL/TLS certificates used in phishing attempts reveals a clear distinction in the security posture of the fake sites. HTTPS is used in 58.8% of phishing attempts, indicating that a majority of phishing actors are attempting to provide a more convincing and secure-looking appearance by using SSL/TLS certificates. By utilizing HTTPS, these sites may appear legitimate to users who rely on the padlock symbol in the browser's address bar as a sign of security. Despite the encryption, these sites remain malicious, often using fraudulent certificates or misappropriated domain names to trick users.

On the other hand, HTTP is used in 41.2% of phishing attempts. While this is a significant proportion, it suggests that a notable portion of phishing actors still rely on non-secure HTTP connections, which are more easily identifiable by users as potentially dangerous, given the absence of the secure connection indicator in modern browsers.

DDoS Attack Statistics

- The peak bandwidth witnessed during a DDoS attack reached 475.59 Gbps, highlighting a significant capacity from the cyber threats.
- The highest recorded throughput during these incidents was 226.15 Mpps.
- Most DDoS attacks lasted between 27.5 minutes on average.
- 110,857 DDoS attacks were recorded, highlighting the high frequency of cyberattacks and illustrating the general threat landscape for the Netherlands.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks
DNS Amp	33,491
DNS	15,799
ICMP	15,688
NTP Amplification	11,204
ICP ACK	9,566

Lessons Learned: Key Insights and Strategic Recommendations

Strategic Recommendations

- **Invest in Comprehensive Threat Intelligence:** Staying informed about evolving threats and actors enables more proactive defenses.

- **Harden Authentication Mechanisms:** Deploy MFA and encourage password hygiene to protect against credential theft.

- **Enhance Incident Response Capabilities:** Develop and regularly test robust response and recovery plans, particularly for ransomware attacks.

- **Strengthen Employee Awareness:** Security awareness training is essential to combat phishing and social engineering attacks.

- **Collaborate for Greater Resilience:** Share intelligence with industry peers and cybersecurity alliances to stay ahead of emerging threats.

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

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.