



NORDIC

Regional Threat Landscape Report





Table of Contents

Executive Summary	3
Dark Web Threats Targeting Nordic Countries	5
Ransomware Attacks Targeting Nordic Entities	11
Stealer Log Statistics	22
Phishing Threats Targeting the Nordic Region	26
DDoS Attack Statistics	29
Lessons Learned: Key Insights and Strategic Recommendations	30

Executive Summary

As a hub of innovation and economic stability in Northern Europe, the Nordic Region—including Denmark, Finland, Iceland, Norway, and Sweden—is a prominent target for cyber threats. With economies driven by advanced industries such as technology, healthcare, renewable energy, and financial services, the region's digital transformation has created new opportunities and efficiencies and heightened its exposure to cyber risks. These risks pose significant challenges to critical infrastructure, national security, and economic resilience.

The Nordic countries face a dual-threat landscape comprising cybercriminals and state-backed actors. Cyber attackers frequently exploit the region's robust digital infrastructure vulnerabilities, targeting critical industries like finance, manufacturing, and information services. In 2024, **343 Dark Web posts** targeting Nordic countries were identified, with **Sweden** emerging as the most frequently targeted country and the **Finance and Insurance industry** as the primary focus.

Ransomware attacks remain a significant threat, with **105 incidents reported across the region**. Sweden again led as the most targeted country, while the **Manufacturing industry** was disproportionately affected, highlighting the strategic value of this sector to attackers.

Phishing attacks also surged, with **Finland** being the most targeted country and the **Information Services sector** bearing the brunt of these incidents. Such attacks have exposed sensitive data and disrupted organizational operations, underscoring the growing sophistication of adversaries in exploiting human vulnerabilities.

The Dark Web plays a crucial role in amplifying these threats by facilitating the exchange of stolen data, hacking tools, and attack strategies. This underground ecosystem enables attackers to innovate their tactics, techniques, and procedures, making the Nordic Region's cyber threat landscape increasingly complex.

This report delves into the evolving cyber threat landscape in the Nordic Region, drawing on open-source intelligence and proprietary research. It provides actionable insights to help governments and businesses strengthen their cybersecurity posture, mitigate risks, and build resilience in an ever-changing threat environment.

Top Takeaways

Dark Web Activity: In 2024, the Nordic Region was referenced in 343 distinct mentions on the Dark Web. Sweden emerged as the most impacted country, representing 41.11% of all activities, followed by Denmark at 23.62% and Norway at 16.91%. Among industries, the Finance and Insurance sector faced the highest exposure at 15.32%, followed by Information Technology at 11.80% and Retail Trade at 9.68%.

Ransomware Surge: Sweden bore the brunt of ransomware attacks, accounting for 49.52% of the total 105 incidents, followed by Norway and Denmark, each with 16.19%. The Manufacturing industry was hit hardest at 36.36%, with a significant impact also on Electrical Equipment Manufacturing at 18.18% and Professional Services at 13.64%.

Stealer Logs Impact: Information on Stealer Logs in the Nordic Region remains under investigation, reflecting ongoing risks.

Phishing Threats: 3,494 phishing attacks targeted Nordic enterprises, with Finland experiencing the highest share at 38.40%, followed by Sweden with 25.95%. The Information Services industry accounted for 29.08% of incidents, highlighting its growing vulnerability.

Record-Breaking DDoS Attacks: The Nordic Region faced 145,613 DDoS attacks in 2024. Sweden recorded the most significant bandwidth attack at 431.31 Gbps, while Norway experienced the peak throughput at 45.41 Mpps. The most complex attack involved 25 techniques, with ARMS and CLDAP Amplifications being the most common.

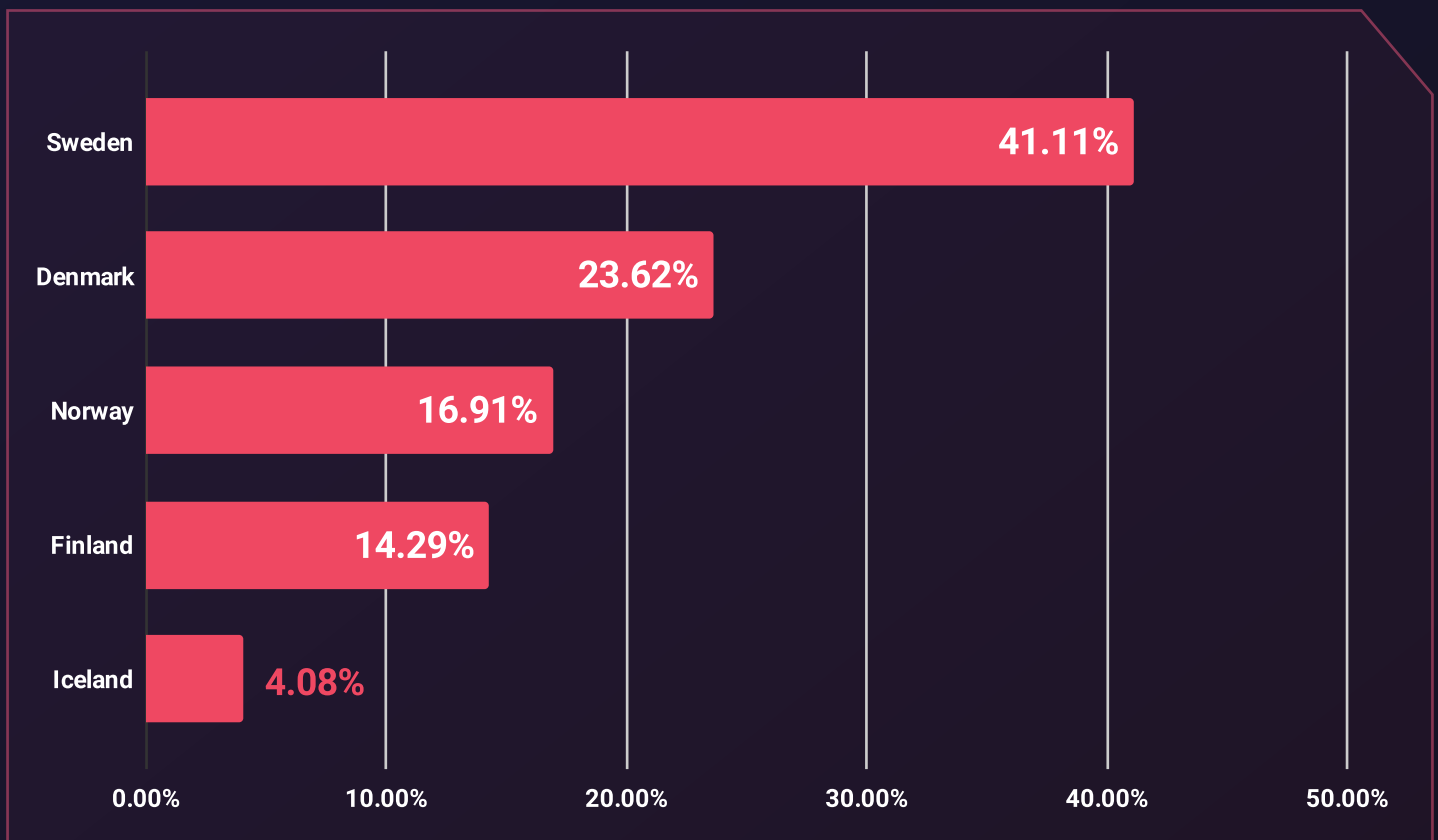
Dark Web Threats Targeting Nordic Countries

Distribution of Dark Web Threats by Target Country

Throughout 2024, SOCRadar's Dark Web Analysts closely monitored activity within the Dark Web, uncovering significant trends and identifying links between Nordic enterprises and covert threat actors. Nordic organizations faced a relentless wave of cyber threats, with malicious actors capitalizing on successful intrusions to trade or exploit their gains on Dark Web forums.

SOCRadar observed 344 Dark Web forum posts linked to 102 distinct threat actors during this period. **Sweden** emerged as the most affected country, representing **41.11%** of the identified cyber threats during this period. Denmark followed it with **23.62%**, **Norway** with **16.91%**, **Finland** with **14.29%**, and **Iceland** with 4.08%.

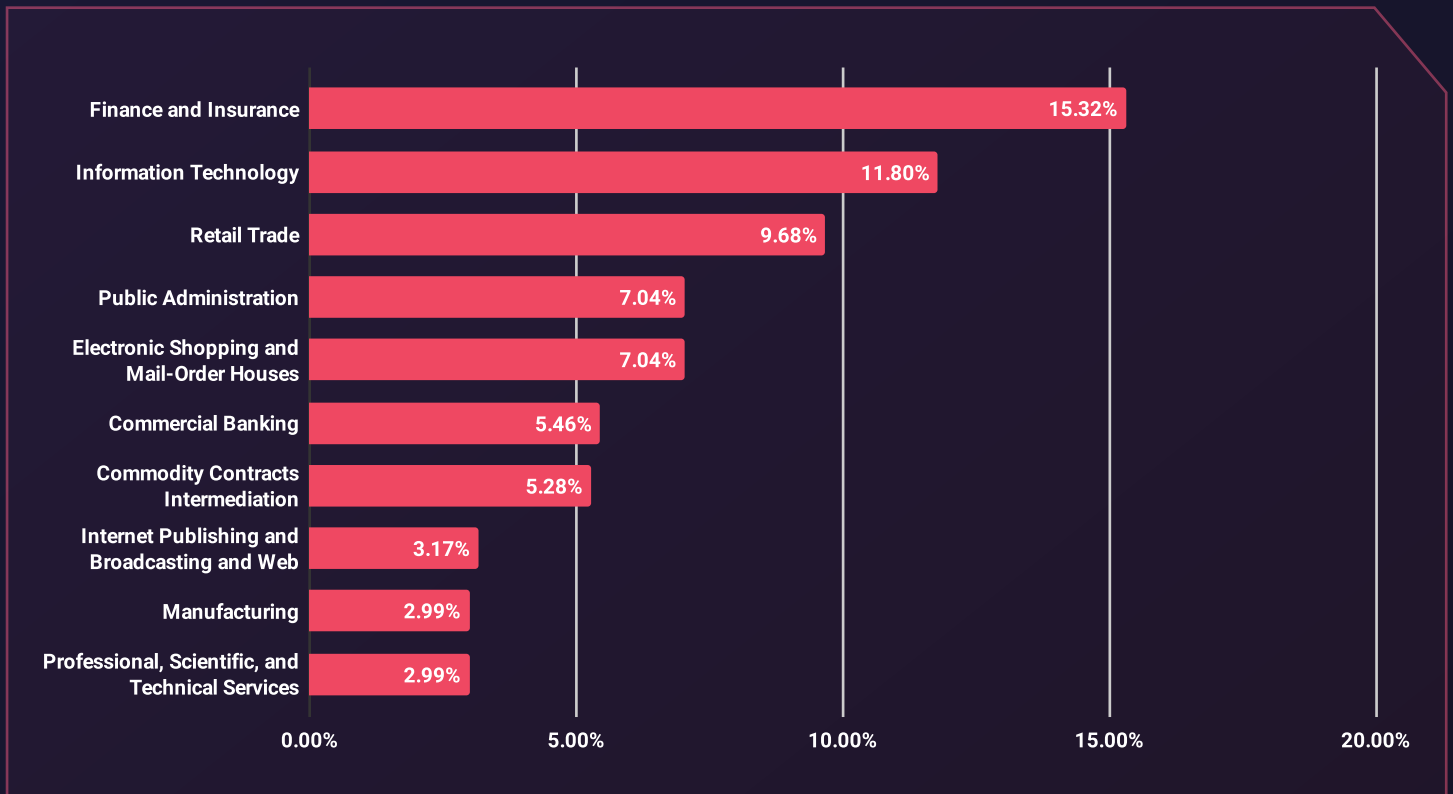
► Dark Web Threats - Distribution by Target Country



Industry Distribution of Dark Web Threats

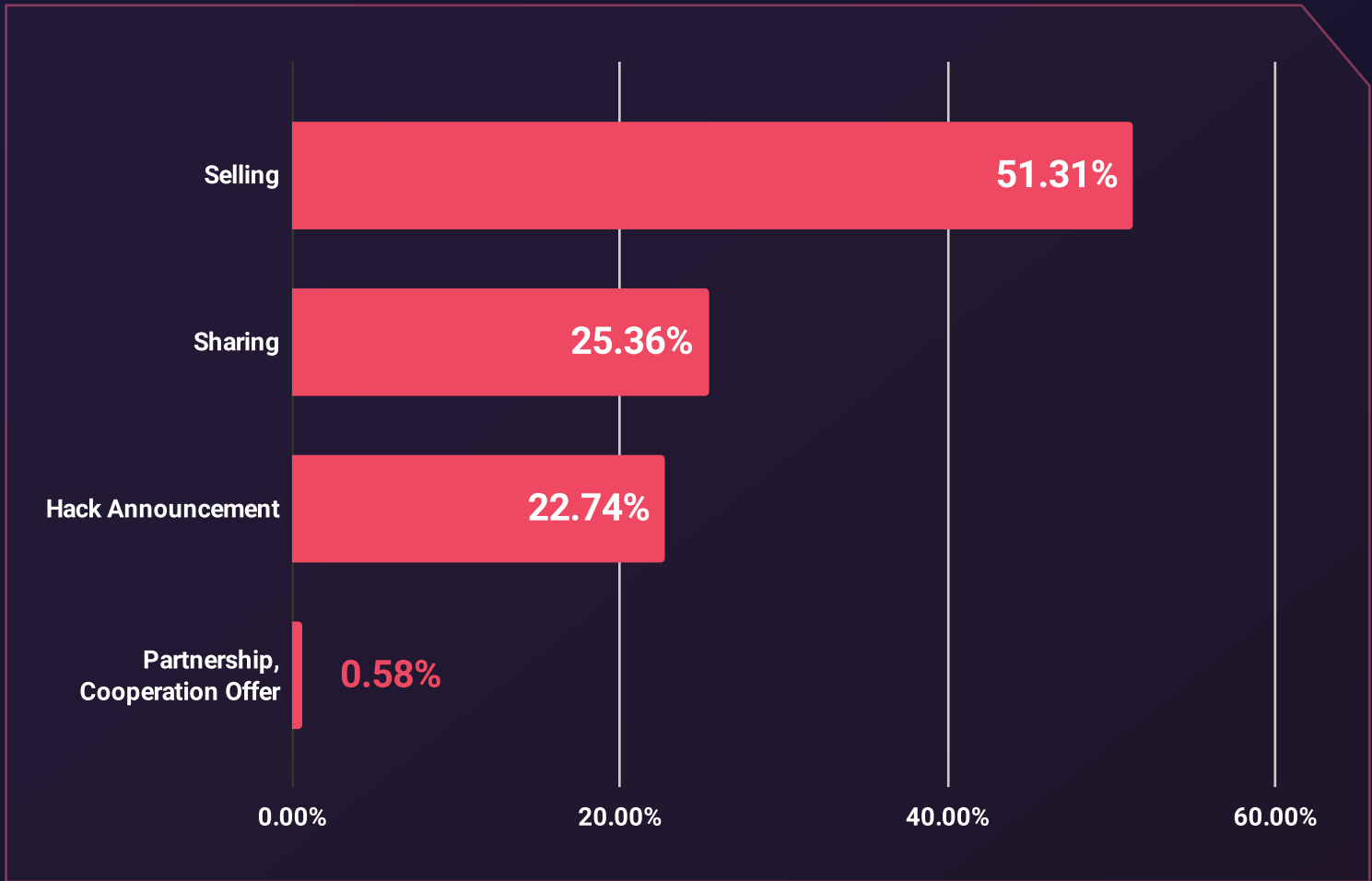
The Finance and Insurance sector was the most impacted, accounting for 15.32% of cyber threats. This was followed by Information Technology at 11.80% and Retail Trade at 9.68%. These findings underscore the critical vulnerabilities across both geographies and industries, highlighting the urgent need for robust cybersecurity measures.

▶ Dark Web Threats – Distribution by Industries



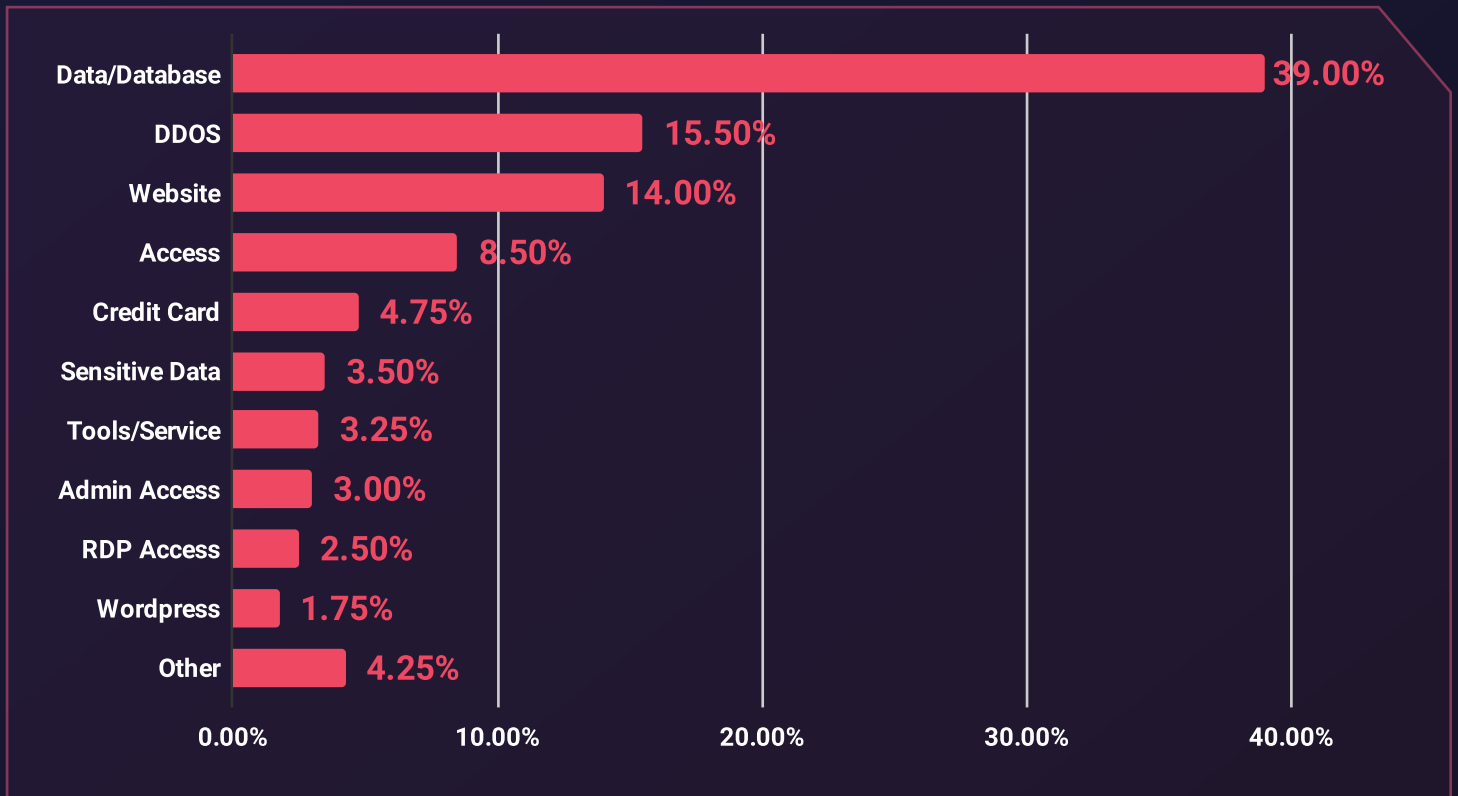
Distribution of Dark Web Threats by Post Type

▶ Dark Web Threats - Distribution by Post Type



Distribution of Dark Web Threats by Threat Type

▶ Dark Web Threats - Distribution by Threat Type



SOCRadar's Advanced Dark Web Monitoring equips organizations in Nordic countries with vital insights into hidden threats targeting key industries such as Finance, insurance, and Information Technology, which faced significant risks over the past year. By providing real-time monitoring of underground chatter and sensitive data exposure, SOCRadar empowers proactive defenses against Dark Web threats.

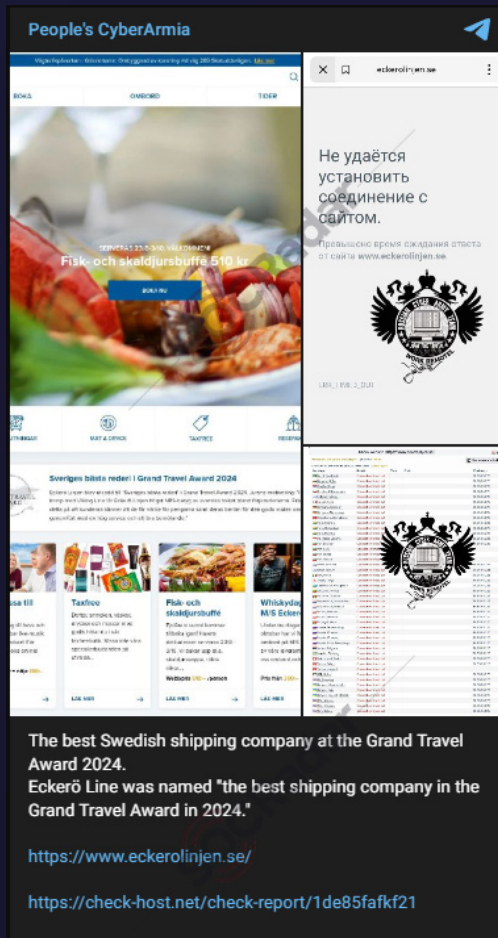
Activate your free demo today to safeguard your organization's most valuable assets.

Black Market ID	Related Asset(s)	Price	Status	Obtain Progress	Discovery Date	Related Alarm
Market-37823686	portal.n11.com	10.00 \$	Open	REQUEST OBTAIN	2024-09-24	Open
Market-37823685	portal.logo.com.tr	10.00 \$	Open	REQUEST OBTAIN	2024-09-24	Open
Market-37714877	rs.n11.com	10.00 \$	Open	REQUEST OBTAIN	2024-09-23	Open
Market-37714721	rs.n11.com	10.00 \$	Open	REQUEST OBTAIN	2024-09-23	Open
Market-37714738	magkadesisek.n11.com	10.00 \$	Open	REQUEST OBTAIN	2024-09-23	Open
Market-36739886	Related Assets Not Available!	10.00 \$	Closed	REQUEST OBTAIN	2024-09-09	Open
Market-36444479	portal.logo.com.tr	10.00 \$	Closed		2024-09-06	Open
Market-34107626	portal.logo.com.tr	10.00 \$	On Hold		2024-07-22	Open
Market-33973730	portal.logo.com.tr	10.00 \$	Open	REQUEST OBTAIN	2024-07-16	Open
Market-33114776	portal.logo.com.tr	10.00 \$	On Hold	REQUEST OBTAIN	2024-06-28	Open
Market-33114775	karlyerim.logo.com.tr	10.00 \$	On Hold	REQUEST OBTAIN	2024-06-28	Open

Recent Dark Web Activities Targeting Nordic Entities

CyberArmy Conducted DDoS Attack on Eckerö Linjen

05 Sep 2024



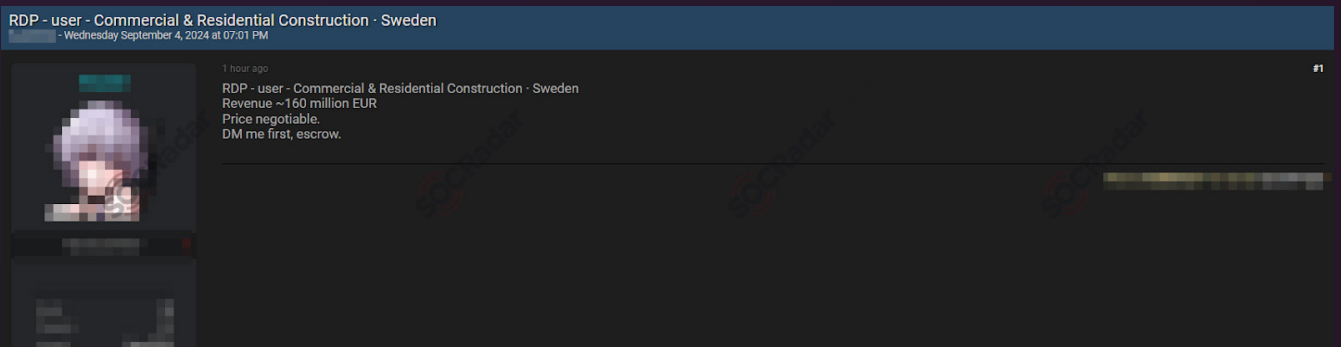
Screenshot of the Telegram Message

In the CyberArmy's telegram channel monitored by SOCRadar, the DDoS attack announcement for Eckerö Linjen was detected. CyberArmy is an active threat actor known for conducting DDoS attacks. This incident highlights the growing prevalence of DDoS attacks, which can disrupt critical services and cause significant financial losses.

Alleged Database of the Minister of Education of Jordan is on Sale

05 Sep 2024

In a hacker forum monitored by SOCRadar, an unauthorized RDP access sale was detected. The sale allegedly belongs to a commercial and residential construction company operating in Sweden. Unauthorized access to RDP can allow attackers to remotely control and access sensitive data and systems within the company's network.

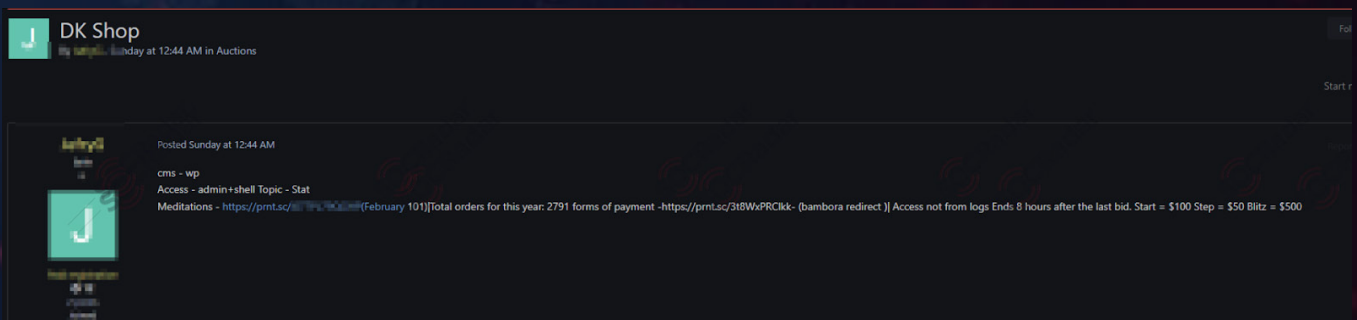


Screenshot of the forum post

Unauthorized Admin Access Sale is Detected for a Danish E-commerce Company

17 Mar 2024

In a hacker forum monitored by SOCRadar, an unauthorized admin access sale was detected. The access allegedly belongs to a Danish e-commerce company. The access includes admin credentials and shell access, potentially allowing attackers to compromise the company's systems and data. Unauthorized access to admin accounts can grant attackers extensive privileges within the company's network, enabling them to steal sensitive data, modify systems, or launch attacks.



Screenshot of the forum post

Ransomware Attacks Targeting Nordic Entities

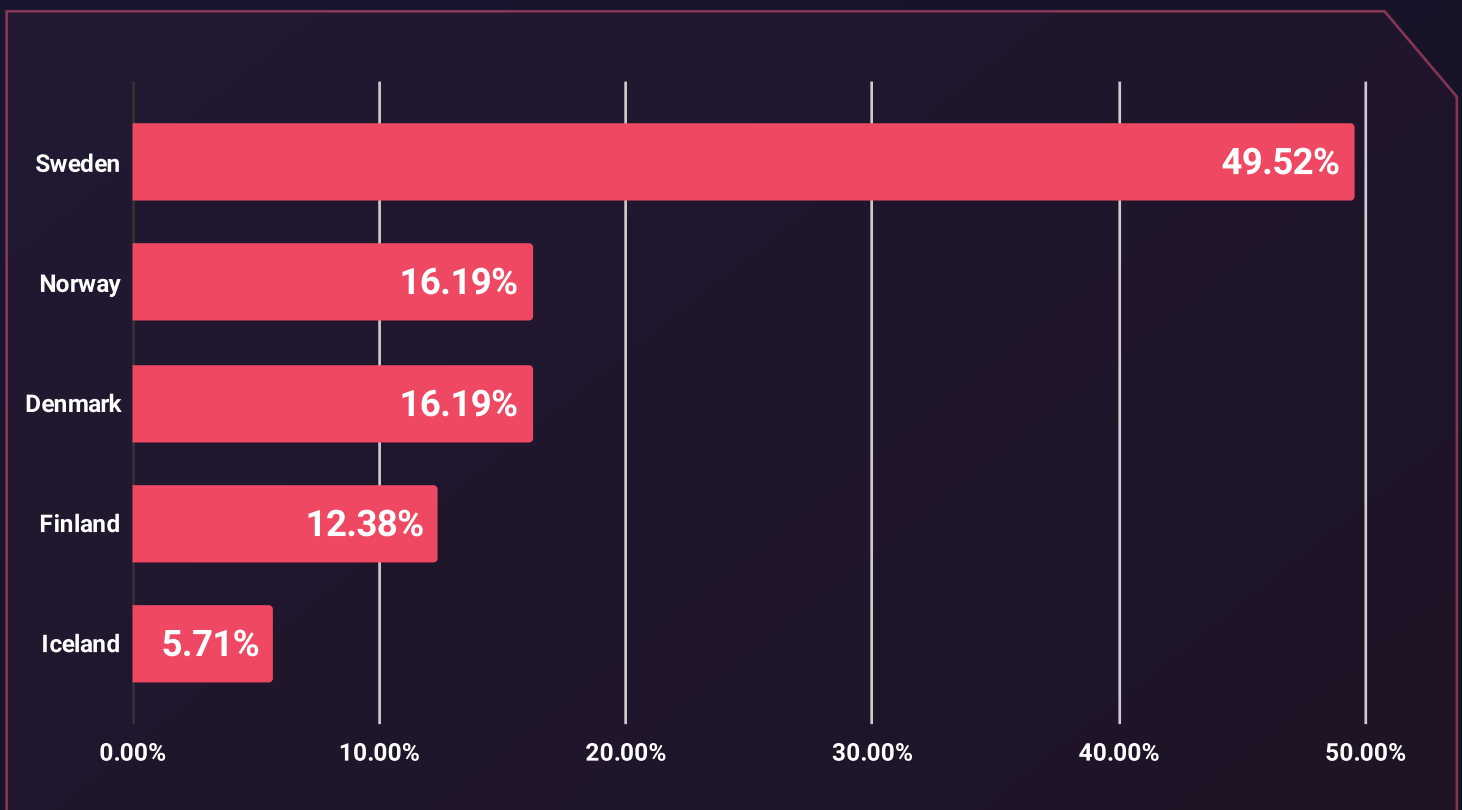
Ransomware attacks continue to pose significant threats to organizations, often leading to severe consequences such as extensive data loss and the exposure of sensitive information. SOCRadar's monitoring identified 105 ransomware victim notifications linked to various ransomware threat actors and/or groups.

Among these 105 ransomware attacks, **Sweden** emerged as the most targeted country, accounting for **49.52%** of the incidents, followed by **Norway** and **Denmark**, each with **16.19%**, **Finland** with **12.38%**, and **Iceland** with **5.71%**.

Regarding industries, the **Manufacturing** sector was the most affected, representing **36.36%** of the identified ransomware attacks. This was followed by **Electrical Equipment, Appliance, and Component Manufacturing** at **18.18%** and **Professional, Scientific, and Technical Services** at **13.64%**, underscoring the critical need for enhanced cybersecurity measures within these industries.

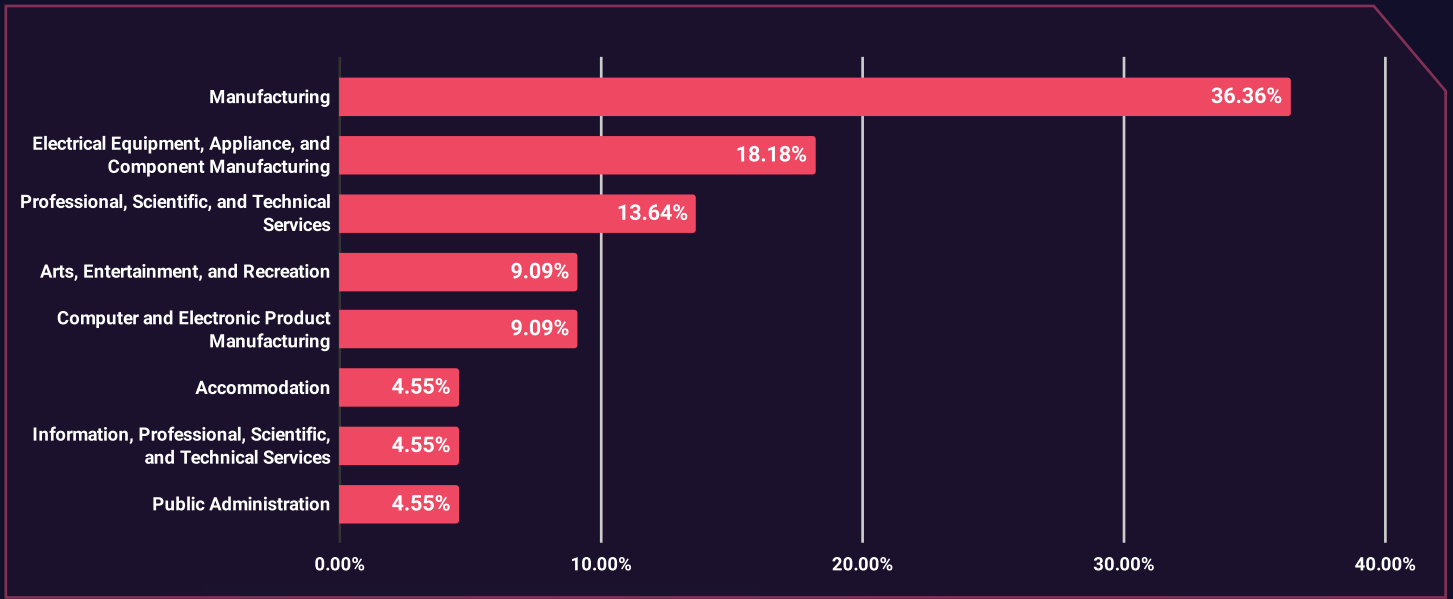
Distribution of Ransomware Attacks by Target Country

► Ransomware Attacks - Distribution by Target Country



Distribution of Ransomware Attacks by Industry

► Ransomware Attacks - Distribution by Industries

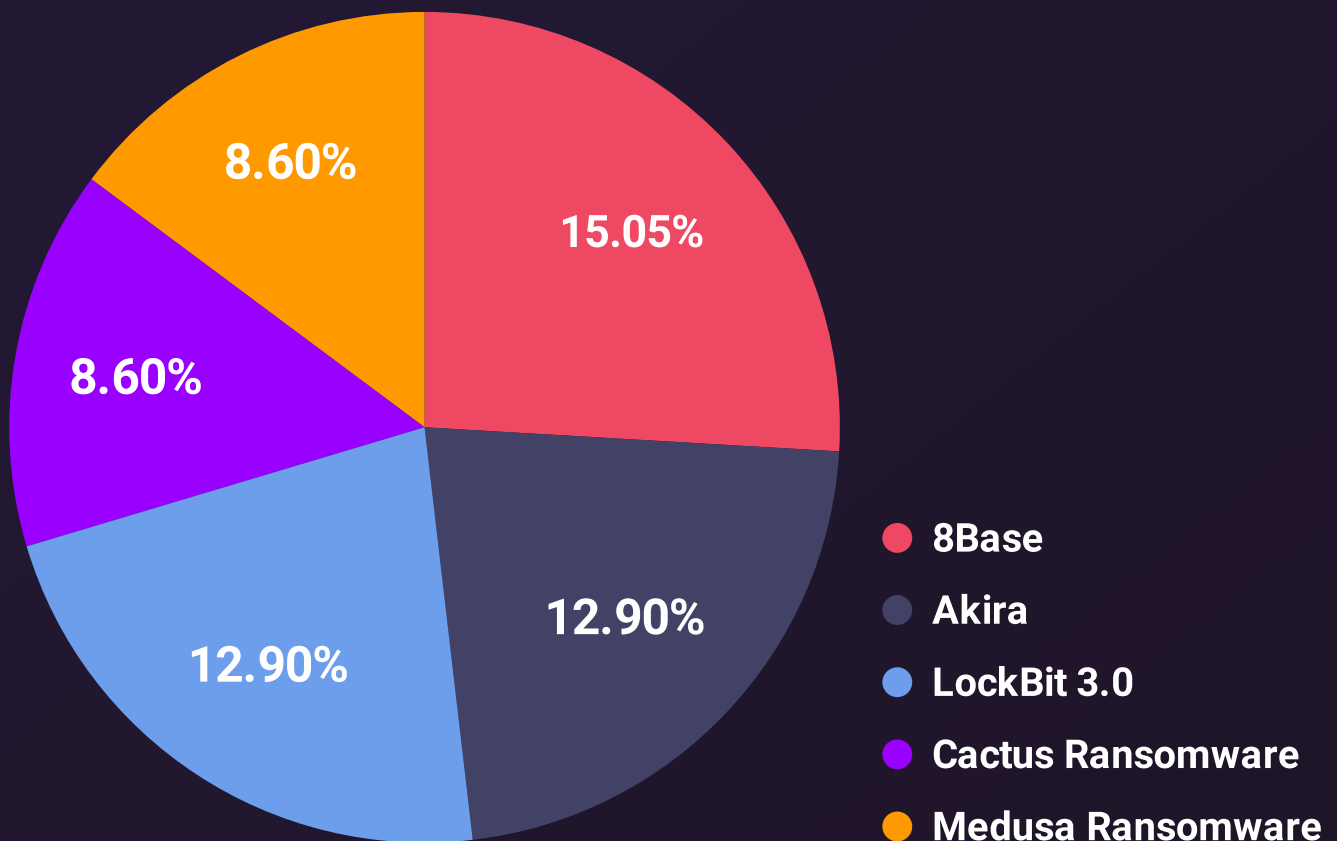


Top Ransomware Groups Targeting the Nordic Region

When examining the top ransomware groups targeting the Nordic Region, **8Base** emerges as the most prolific threat, accounting for **15.05%** of the attacks. Following this, **Akira Ransomware** and **LockBit 3.0** represent **12.90%** of the ransomware incidents. **Cactus Ransomware** and Medusa Ransomware follow, each contributing **8.60%** of the ransomware activity.

This analysis highlights the dominant presence of **8base**, followed by a diverse range of other ransomware groups, underscoring the evolving complexity of the ransomware threat landscape.

▶ Top Ransomware Groups Targeting Nordic Region



Recent Ransomware Attacks Targeting Nordic Entities

The New Ransomware Victim of Akira: Bjuvs Kommun

26 Feb 2024

In the Akira ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Quik Bjuvs Kommun, a Swedish municipality. Akira ransomware group is threatening to leak 200GB of sensitive data, including confidential documents, contracts, agreements, personal HR files, and more

date	title	content
2024-02-26	Bjuvs kommun	We will upload almost 200GB of Bjuvs kommun organization. Confidential documents, contracts, agreements, personal HR files and so on.

Screenshot from Akira ransomware group's website

The New Ransomware Victim of 8base: Axel Johnson

20 Feb 2024

The screenshot shows the 8Base ransomware group's website. At the top, the logo '8BASE' is displayed with the tagline 'YOUR DATA IS NOT SAFE.' and a red square icon containing a white '8'. Below the logo are navigation links: 'Main', 'Contact', 'FAQ', and 'Rules'. The main content area features a post titled 'Axel Johnson' with a timestamp of 'Downloaded: 21.02.2024 Publish: 28.02.2024 views: 126'. The post text describes Axel Johnson as a leading Swedish family-owned group with a major footprint in Food, and with businesses spanning across sectors as diverse as Industrial and IT Solutions, Health and Wellness, and Solar energy. A 'Comment:' section lists the types of data stolen: Invoice, Receipts, Accounting documents, Personal data, Certificates, Employment contracts, A huge amount of confidential information, Confidentiality agreements, Personal files, and Other. A red timer at the bottom of the post indicates '6d 16h 59m 19s'.

On the 8Base ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Axel Johnson. The 8base ransomware group has allegedly targeted Axel Johnson, a Swedish family-owned group, and published stolen data on its website. The data includes sensitive information such as invoices, accounting documents, personal data, and employment contracts.

Screenshot from 8Base ransomware group's website

LockBit 3.0 Ransomware Group Leaked The Data of Tura Scandinavia

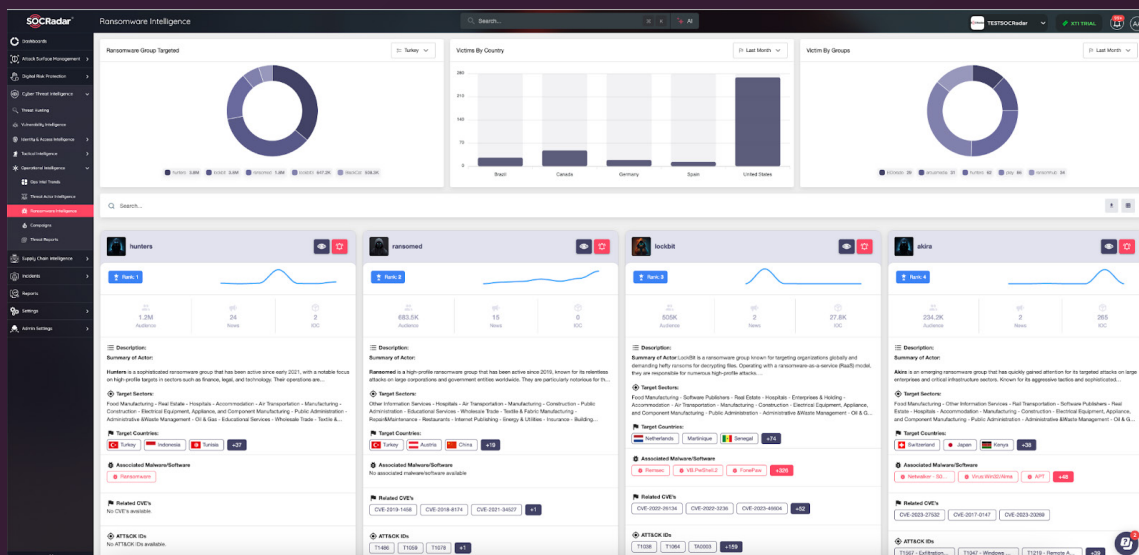
15 Jan 2024

New data leaks detected on the LockBit 3.0 ransomware group website monitored by SOCRadar allegedly belong to Tura Scandinavia. The ransomware group exploited vulnerabilities in Tura Scandinavia's corporate network, highlighting the importance of maintaining strong network security and patching vulnerabilities promptly.



Screenshot from Lockbit3.0 ransomware group's website

Explore SOCRadar's Ransomware Intelligence module and gain comprehensive insights with detailed group profiles, MITRE Visualizer, and actionable IOCs. These insights will empower you to stay ahead of evolving threats and enhance your cybersecurity strategy.



Top Threat Actors Targeting Nordic Organizations

8Base Ransomware Group:



The image shows a digital threat actor card for the 8Base Ransomware Group. On the left, there is a stylized illustration of a hooded figure with a mask, sitting at a laptop. The card is titled '8Base' and includes a description of the group's activities. On the right, there is a list of key attributes and TTPs (Tactics, Techniques, and Procedures) for the group.

8Base

Country of Origin: Unknown

8Base is a ransomware group active since April 2022, targeting small and medium-sized businesses (SMBs) across various sectors, including business services, finance, manufacturing, and IT.

-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

Threat Actor Card of 8Base Ransomware Group

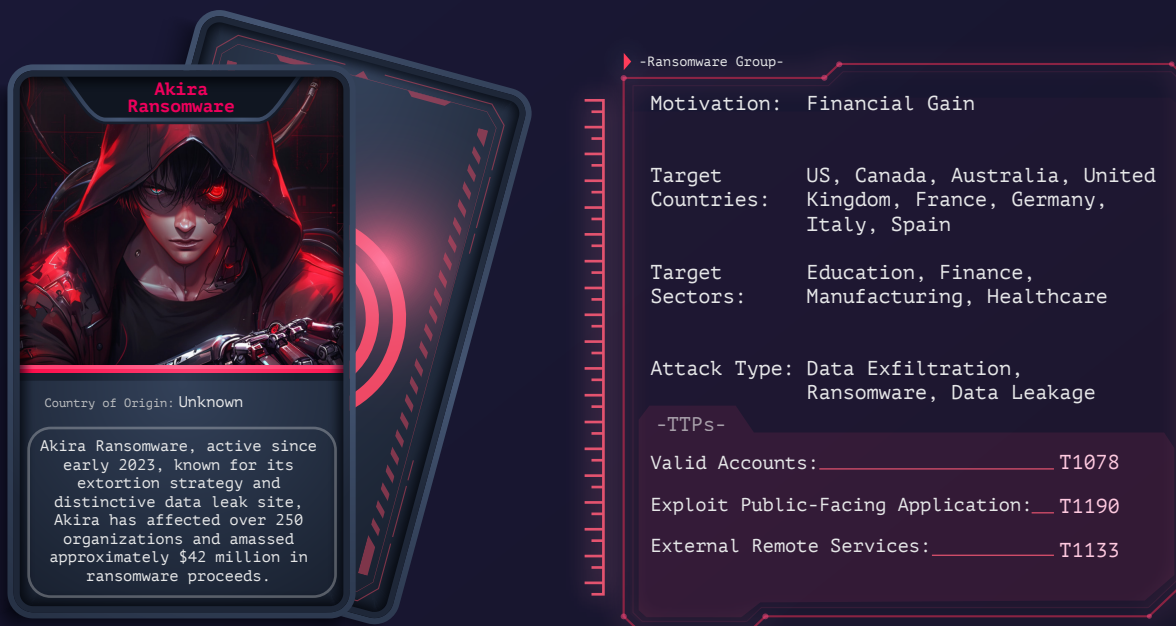
The **8Base Ransomware Group** is a sophisticated Ransomware-as-a-Service (RaaS) group known for its calculated and impactful attacks on businesses across various industries. First observed in **2022**, 8Base quickly garnered attention for its highly structured operations and technical capabilities. Employing the **double extortion model**, the group encrypts victim data and threatens to publish sensitive information on its leak site if ransom demands are not met.

8Base primarily targets organizations with weak or outdated cybersecurity defenses, exploiting vulnerabilities in IT infrastructures to gain unauthorized access. Their attacks are characterized by precision and speed, often leaving victim organizations scrambling to respond. The group's Dark Web leak site frequently publishes victim data to pressure organizations into compliance while also serving as a platform to market stolen information to other malicious actors.

By 2024, 8Base has firmly established itself as a persistent threat in the ransomware ecosystem, affecting organizations across multiple sectors and geographies. Its strategic use of ransomware-as-a-service tools and collaboration with other threat actors continues to elevate its profile within the cybercrime community.

[You can visit our blog post for more detailed information on 8Base Ransomware Group.](#)

Akira Ransomware Group:



The image displays a 'Threat Actor Card' for the Akira Ransomware Group. On the left is a card with a red and black illustration of a hooded figure with glowing red eyes. The card contains the following text: 'Akira Ransomware', 'Country of Origin: Unknown', and a paragraph describing the group's activities since early 2023. On the right is a larger, dark-themed card titled '-Ransomware Group-' containing technical details: Motivation (Financial Gain), Target Countries (US, Canada, Australia, United Kingdom, France, Germany, Italy, Spain), Target Sectors (Education, Finance, Manufacturing, Healthcare), Attack Type (Data Exfiltration, Ransomware, Data Leakage), and TTPs (Valid Accounts: T1078, Exploit Public-Facing Application: T1190, External Remote Services: T1133).

Akira Ransomware

Country of Origin: Unknown

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.

-Ransomware Group-

Motivation: Financial Gain

Target Countries: US, 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

Threat Actor Card of Akira Ransomware Group

Akira Ransomware Group operates as a Ransomware-as-a-Service (RaaS) group, gaining prominence through its targeted attacks on businesses across various industries. Since its emergence, Akira has adopted advanced encryption techniques and the double extortion model, threatening victims with data encryption and sensitive information exposure if ransom demands are not met.

With numerous victim announcements, Akira has positioned itself as a growing threat in the ransomware landscape. As of 2024, the group continues to expand its operations, targeting organizations globally and exploiting vulnerabilities in their IT infrastructures while actively selling stolen data on Dark Web marketplaces to maximize financial gain.

[You can visit our blog post for more detailed information on Akira Ransomware Group.](#)

Lockbit 3.0 Ransomware Group:



The image shows a digital threat actor card for the Lockbit 3.0 Ransomware Group. On the left, there is a character illustration of a person in a brown hoodie with glowing blue eyes. Below the illustration, it says 'Country of Origin: Russia' with a Russian flag icon. A text box contains a description of the group as a successful RaaS group since 2019, active in double-extortion and initial access broker affiliates. On the right, a larger panel titled '-Ransomware Group-' lists details: 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), and TTPs (Exploit Public-Facing Application: T1190, Remote Desktop Protocol: T1021.001, Data Encrypted for Impact: T1486).

-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

Threat Actor Card of Lockbit 3.0 Ransomware Group

LockBit 3.0, a successor to LockBit and LockBit 2.0, operates as a Ransomware-as-a-Service (RaaS) group. Since January 2020, LockBit has shifted to an affiliate-based model, employing various tactics to target businesses and critical infrastructure organizations. They are known for employing strategies like double extortion and initial access broker affiliates, recruiting insiders, and hosting hacker recruitment contests.

With over 1,500 victim announcements on the SOCRadar platform, LockBit emerged as the most active ransomware group in 2022 following Conti's shutdown. As of the first quarter of 2023, they remain the most prolific group, boasting over 300 announced victims.

[You can visit our blog post for more detailed Lockbit 3.0 Ransomware Group information.](#)

Cactus Ransomware Group:



The image displays a 'Threat Actor Card' for the Cactus Ransomware Group. On the left is a card with a green-hooded hacker icon, the title 'Cactus Ransomware', and a text box describing the group's emergence in March 2023 and its targeting of U.S. manufacturing companies. On the right is a larger card titled '-Ransomware Group-' containing a list of attributes: Motivation (Financial Gain), Target Countries (U.S., U.K., Canada, Australia, France, Italy, Switzerland, Germany, Portugal), Target Sectors (Manufacturing, Professional Services, Wholesale, Finance, Transportation), Attack Type (Ransomware, Exploiting VPN Vulnerabilities, Double-extortion), and TTPs (Exploit Public-Facing Application: T1190, Account Discovery: T1087, Exfiltration to Cloud Storage: T1567.002).

-Ransomware Group-	
Motivation:	Financial Gain
Target Countries:	The U.S., The U.K., Canada, Australia, France, Italy, Switzerland, Germany, Portugal
Target Sectors:	Manufacturing, Professional Services, Wholesale, Finance, Transportation
Attack Type:	Ransomware, Exploiting VPN Vulnerabilities, Double-extortion
-TTPs-	
Exploit Public-Facing Application:	T1190
Account Discovery:	T1087
Exfiltration to Cloud Storage:	T1567.002

Threat Actor Card of Cactus Ransomware Group

The **Cactus Ransomware Group** is a highly targeted and methodical ransomware operation that leverages advanced techniques to infiltrate and disrupt organizations. Emerging in **early 2023**, Cactus has become known for using encryption algorithms to lock victim data while simultaneously threatening to release sensitive information through its **double extortion model**.

What sets Cactus apart is its sophisticated evasion tactics, including encrypting its ransomware binary to bypass traditional security defenses. This meticulous approach allows the group to operate under the radar, precisely targeting organizations across various industries. Victim data is often uploaded to the group's dedicated leak site, serving as a key pressure point to compel ransom payments while also monetizing stolen information through Dark Web marketplaces.

By **2024**, Cactus Ransomware has demonstrated a growing capacity to exploit vulnerabilities in corporate IT infrastructures, focusing on organizations with insufficient defenses. Its calculated and professional operational model places it among the more sophisticated ransomware groups, highlighting the evolving complexity of ransomware threats in the cybersecurity landscape.

[You can visit our blog post for more detailed information on Cactus Ransomware Group.](#)

Medusa Ransomware Group:



The image shows a digital threat actor card for the Medusa Ransomware Group. On the left is a card with a hooded figure's face and glowing green eyes. To the right is a detailed information panel with a red border and a vertical scale on the left side.

Medusa Ransomware

Country of Origin: Unknown

Medusa is a RaaS group operating since June 2021 and known for its many variants. The group is primarily targeting North American and European organizations.

-Ransomware Group-

Motivation: Financial Gain

Target Countries: United States, United Kingdom, Canada, India, Turkey, Australia

Target Sectors: Manufacturing, Education, Professional Services, Finance and Insurance

Attack Type: RDP, Phishing, Ransomware, Double Extortion, Exploiting Google Chrome Vulnerabilities (CVE-2022-2295)

-TTPs-

External Remote Services: T1133

PowerShell: T1059.001

Exfiltration Over Alternative Protocol: T1048

Threat Actor Card of Medusa Ransomware Group

Medusa Ransomware Group operates as a Ransomware-as-a-Service (RaaS) entity, gaining significant attention within the cybercrime ecosystem. Since its emergence, Medusa has employed various sophisticated tactics to target businesses and organizations across different sectors. Known for using double extortion methods, the group pressures victims by threatening to leak stolen data and encrypting their systems.

With a growing number of victim announcements, Medusa Ransomware Group has become a formidable player in the ransomware landscape. As of 2024, the group continues to target high-profile organizations, leveraging advanced tactics like exploiting vulnerabilities in network infrastructure and selling access to sensitive data on the Dark Web.

[You can visit our blog post for more detailed Medusa Ransomware Group information.](#)

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

THREAT ACTOR INTELLIGENCE

KNOW YOUR ENEMY

- Know their tactics, techniques, and past activities.
- Access detailed profiles and track threat actor activities.
- Keep up with the latest threats and Tactics, Techniques, and Procedures (TTPs).
- Prioritize risks based on active threat actors in your industry or region.

Discover the adversaries targeting your industry

Threat Type: Threat Actor Name: Enter threat actor name Target Country: All Country (171/171) Target Sectors: All Sector (56/56) Clear Search

Top Threat Actors

WIRTE Rank: 1

1M Audience, 7 News, 243 IOC

Safe Rank: 2

231k Audience, 1 News, 3k IOC

hunters Rank: 1

22M Audience

Target Countries: Jordan, Israel, Egypt

Target Sectors: Food Manufacturing - Real Estate - Hospital

Associated Malware/Software: Ransomware

Related CVE's: No CVE's available.

ATT&CK IDs: No Attack IDs

underground Rank: 2

974k Audience

Target Countries: Global

Target Sectors: Energy & Utilities - Manufacturing - Financial HealthCare & Social Assistance

Associated Malware/Software: No Malware available.

Related CVE's: CVE-2021-26855, CVE-2021-34512

ATT&CK IDs: T1059.003, T1021.002, T1018

medusa

Summary of Actor Medusa is a ransomware group known for its sophisticated attacks on various organizations and industries. They typically employ advanced tactics to encrypt victim data and then demands ransom for decryption. They have been active in the cybercriminal landscape, often targeting high-profile entities globally.

General Features: Medusa ransomware attacks are characterized by their use of advanced encryption algorithms and obfuscation techniques. The group is known for spreading their ransomware through phishing campaigns, exploiting vulnerabilities, and leveraging remote desktop protocols (RDP).

Related Other Groups: REvil, DarkSide, Conti

Indicators of Attack (IoA):

- Unexpected encryption of files
- Ransom notes demanding payment
- Unusual network traffic
- Phishing emails with malicious attachments or links

Target Countries: Algeria, Bosnia and Herzegovina, Brazil, Kenya, Senegal +54

Target Sectors: Food Manufacturing, Other Information Services, Credit Unions, Software Publishers, Real Estate +59

Associated Malware/Software: apk.medusa, ALF-HeraklezEval:Backdoor:Linux/Mirai, elf.mirai

Related CVEs: CVE-2023-46604, CVE-2021-26855, CVE-2023-34039, CVE-2023-38831, CVE-2023-38035 +13

ATT&CK IDs: T1566, T1036, T1574, T1140, T1047 +4



Stealer Log Statistics: Top Domains in Nordic Region

Throughout 2024, thousands of users' user IDs/email addresses, passwords, credit card data, password hashes, and victim IP address information were compromised via Stealer Logs from the computers of users with accounts or access to some of the highest traffic domains in the Nordic Region.

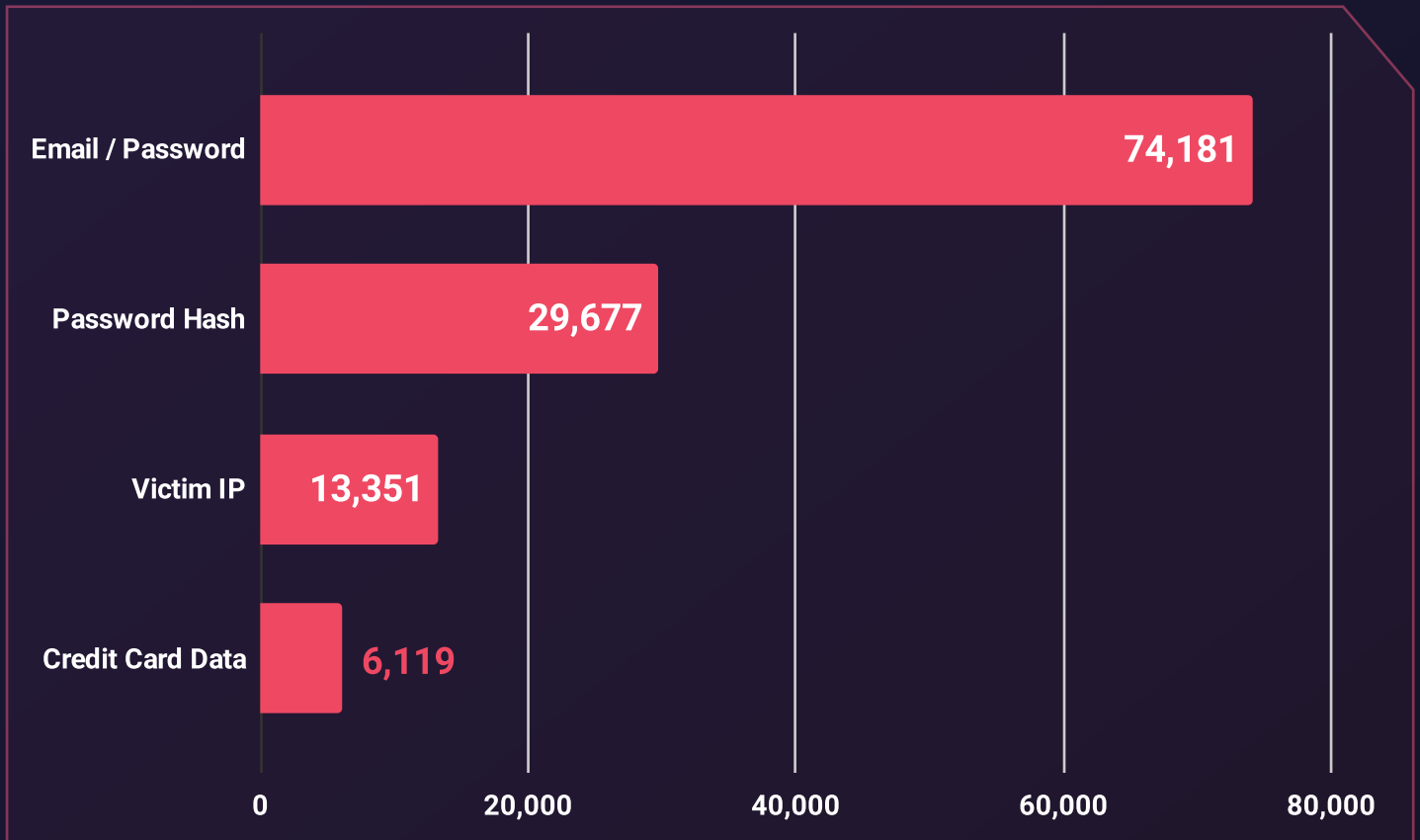
The table below lists the domains that receive the highest traffic from countries within the Nordic Region.

tv2.dk	is.fi
dr.dk	iltalehti.fi
mitid.dk	yle.fi
ekstrabladet.dk	hs.fi
bt.dk	tori.fi
elko.is	vg.no
visir.is	dagbladet.no
mbl.is	finn.no
byko.is	bankid.no
landsbankinn.is	nettavisen.no
ica.se	aftonbladet.se
svt.se	expressen.se
amazon.se	di.se

The graph below displays the distribution of compromised user data obtained through Stealer Logs across the domains with the highest traffic from the Nordic Region.

Stealer Logs - Distribution of the Compromised Data

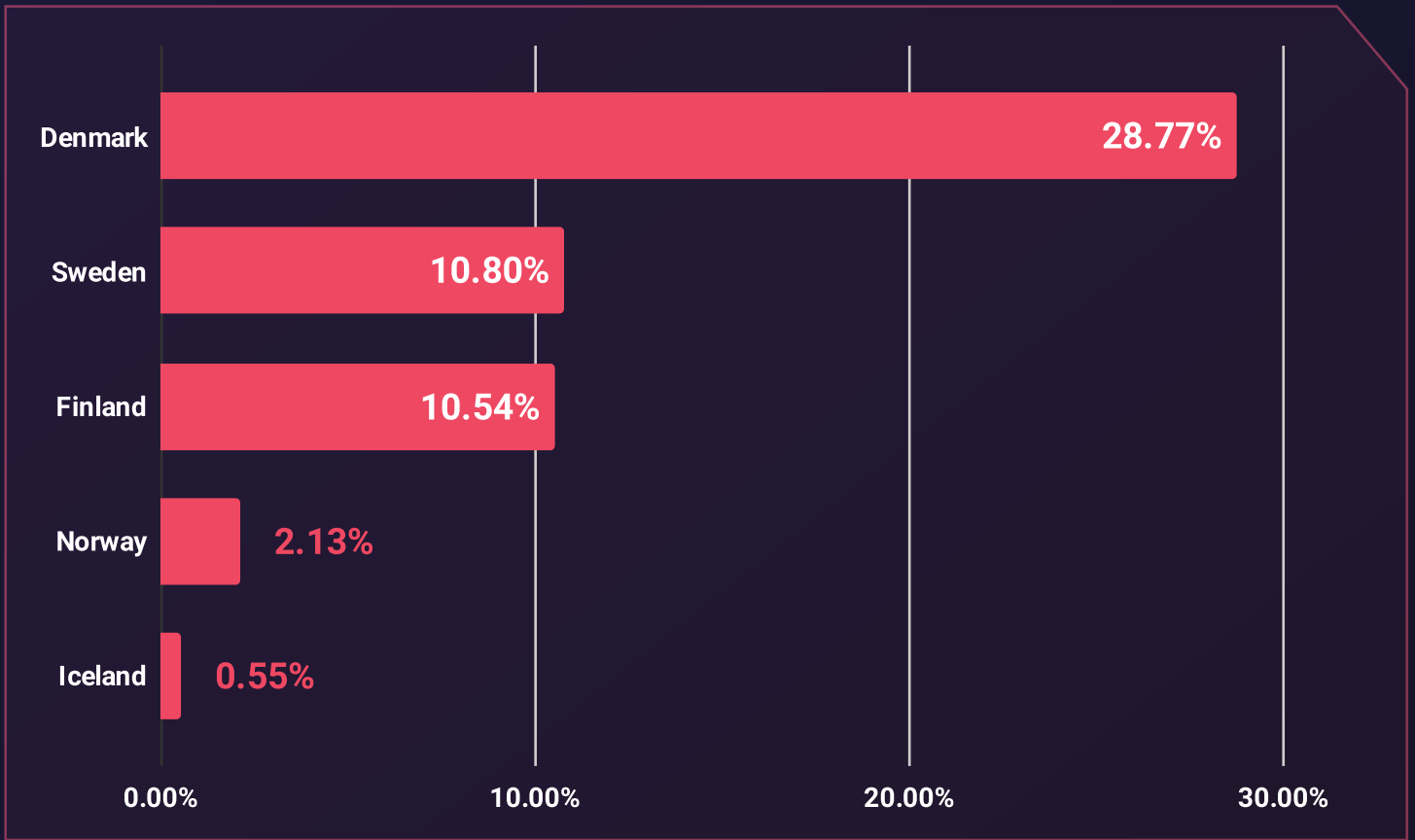
▶ Stealer Logs - Compromised Data



The data reveals significant dissemination of compromised information, including **74,181** email/password combinations, **29,677** password hashes, **13,351** compromised victim IPs, and **6,119** credit card data entries, each representing significant instances of compromise.

Stealer Logs - Distribution by Victim Countries

▶ Stealer Logs - Distribution by Victim Countries



The majority of stealer malware victims in the Nordic Region are from Denmark, with 28.77% of the credentials belonging to victims from there. Sweden ranks second, with 10.80% of the credentials exposed in stealer logs, followed closely by Finland at 10.54%. Norway and Iceland account for 2.13% and 0.55%, respectively.

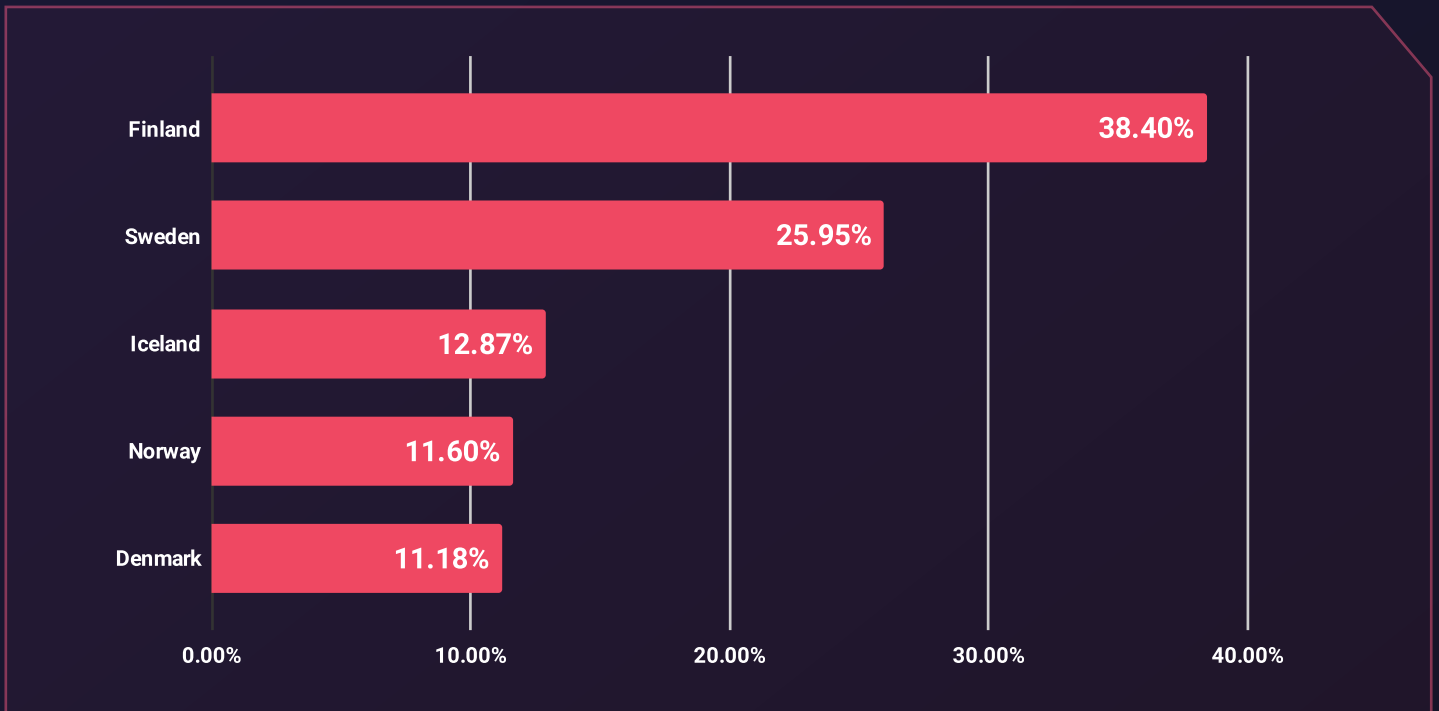
These discoveries emphasize the gravity of data compromises that impact users, highlighting the urgent need for robust cybersecurity protocols to mitigate such risks efficiently.

Phishing Threats Targeting the Nordic Region

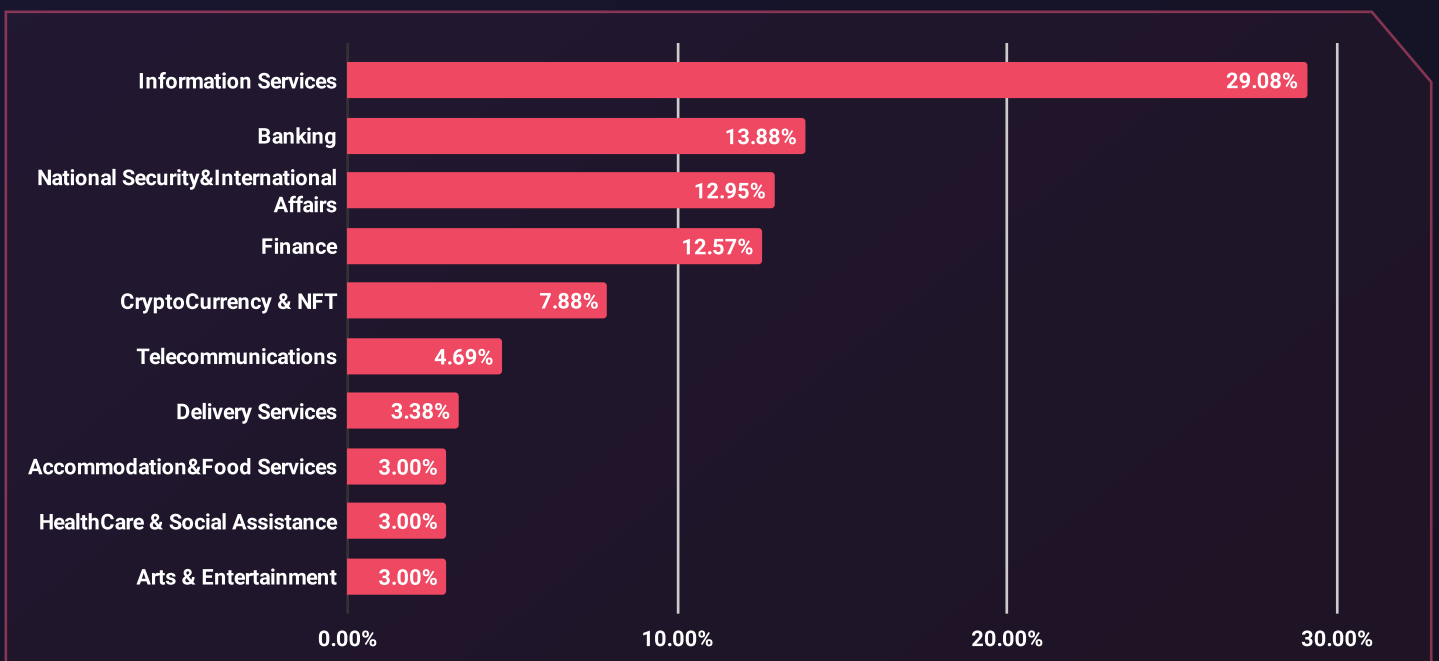
Phishing remains a highly effective tactic for breaching an organization's infrastructure. It often involves tricking individuals into providing sensitive credentials on fake websites.

Typically, phishing attacks are coupled with social engineering tactics to acquire such credentials. In 2024, Nordic enterprises have encountered **3,494 distinct instances of phishing attacks**, primarily targeting the **Information Services** industry.

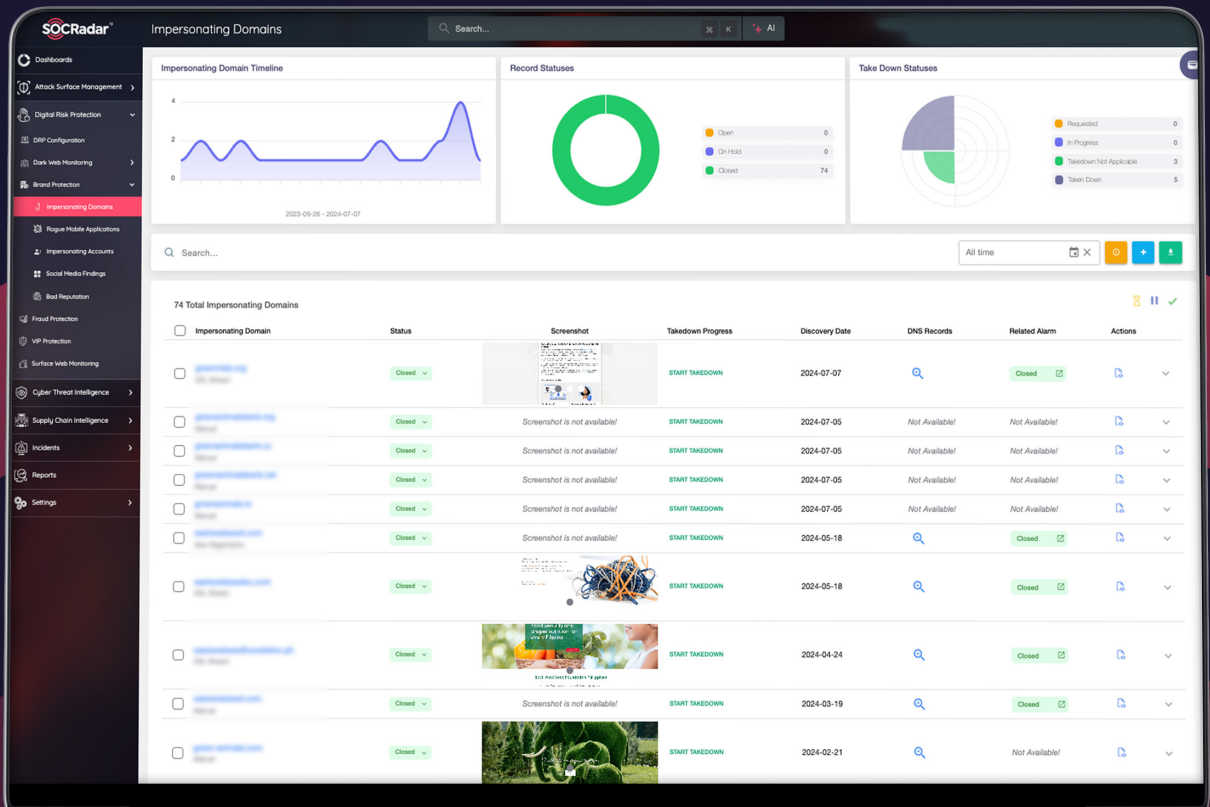
► Phishing Attacks – Distribution by Target Country



► Phishing Attacks – Distribution by Industry

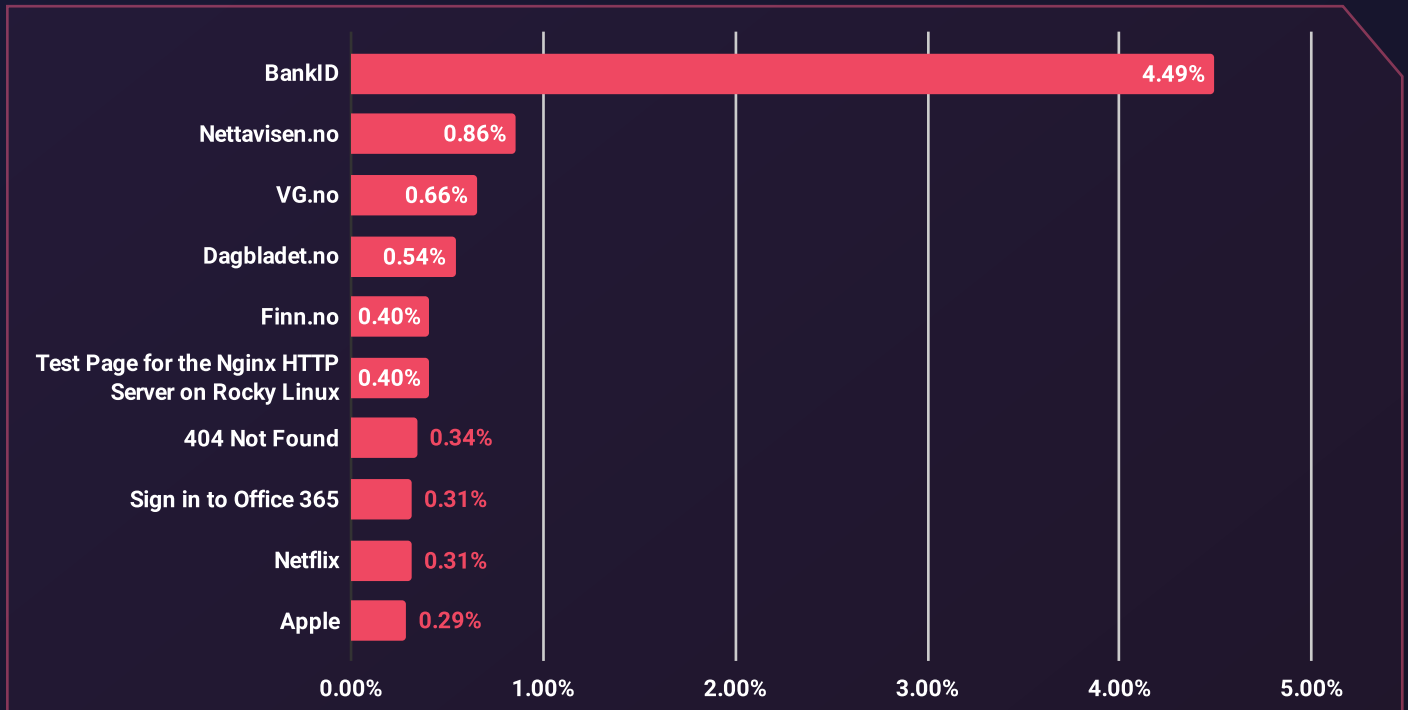


With **SOCRadar's AI-powered Phishing Domain Detection module**, you can swiftly identify malicious domains and protect your brand from phishing threats. **Start safeguarding your digital presence today with SOCRadar—request a free demo** and see the platform in action.



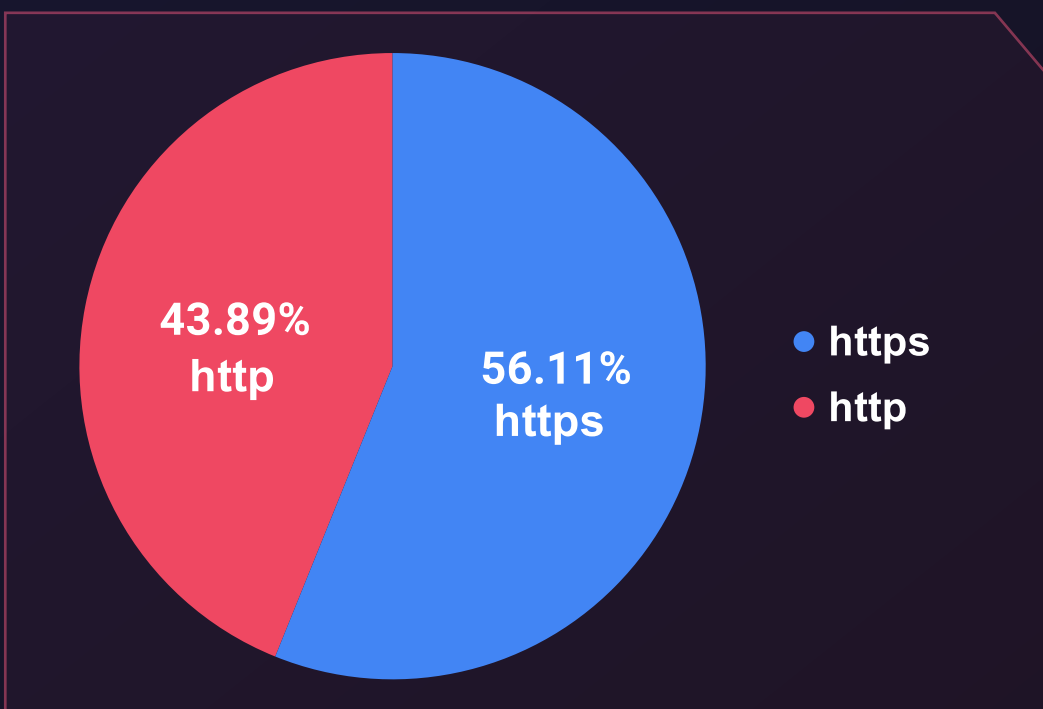
The graph below illustrates the distribution of Page Titles used by threat actors for phishing attacks. Notably, the data reveals a predominant usage of the BankID page title.

▶ Phishing Attacks – Distribution by Phishing Page Title



When closely examining the SSL/TLS protocols of domains prepared for phishing attacks by threat actors, we observe an increasing trend in the usage of HTTPS compared to the past.

▶ Phishing Attacks – Distribution by SSL/TLS Protocol



DDoS Attack Statistics

In 2024, the Nordic region experienced 145,613 DDoS attacks, marked by significant cyber activity across Sweden, Norway, Denmark, Finland, and Iceland.

Key Metrics:


- **Maximum Multi-Vector Attack:** Sweden recorded the most extensive multi-vector DDoS attack, encompassing 25 vectors, including prevalent techniques such as ARMS Amplification and CLDAP Amplification.
- **Maximum Bandwidth:** The highest bandwidth observed during a DDoS attack was 431.31 Gbps in Sweden, indicating the severe capacity of these cyber threats.
- **Maximum Throughput:** Norway experienced the highest recorded throughput at 45.41 Mpps, underscoring the intense rate at which data packets were sent.
- **Average Attack Duration:** On average, each DDoS attack lasted 51.66 minutes in Norway, indicating a strategy aimed at prolonged and effective service disruption.
- **Total Number of Attacks:** Denmark recorded 45,910 DDoS attacks throughout the year, illustrating a high frequency of cyber-attacks aimed at regional targets.

Top DDoS Attack Vectors

Attack Vector	Number of Attacks in 2024
DNS Amplification	49,426
TCP ACK	41,641
TCP SYN/ACK Amplification	26,333
DNS	21,752
TCP RST	21,169

Check For
DoS Resilience

Enter your domain or IP block



The DoS Resilience Service allows you to check your domain's or subnet's resilience against DoS attacks such as slowloris attack, etc.

“SOCRadar is a cloud-based, AI-powered Digital Risk Protection Platform enhanced by cyber threat intelligence capabilities.”

Enhance your DDoS defense with [SOCRadar's DoS Resilience Free Tool](#). Our Free DoS Resilience Service allows you to check your domain's or subnet's resilience against DoS attacks, such as slowloris attacks.

Lessons Learned: Key Insights and Strategic Recommendations

Several critical insights have emerged in evaluating the cybersecurity challenges faced by organizations in the Nordic Region. These findings and SOCRadar's comprehensive capabilities provide a strategic roadmap to enhance cyber resilience and ensure operational continuity. Below are the key takeaways from our analysis:

Adapting to an Evolving Cyber Threat Landscape

The Nordic Region's constantly evolving cyber threat landscape, characterized by significant Dark Web activity and ransomware incidents, demands heightened vigilance. Organizations must continuously adapt their security strategies to address emerging threats. By leveraging [***SOCRadar's Extended Threat Intelligence solution***](#), businesses can obtain real-time threat insights and proactively counter cyber adversaries.

Comprehensive, Multi-layered Security

The diverse range of industries targeted by cyber threats highlights the need for multi-layered security defenses. SOCRadar supports these initiatives with its proactive [***Cyber Threat Intelligence***](#) and [***Advanced Dark Web Monitoring***](#) services, ensuring organizations are well-protected across various threats.

Addressing and Mitigating Ransomware Threats

Ransomware remains a significant threat, emphasizing the importance of robust defensive and responsive strategies. [***SOCRadar's Attack Surface Management***](#) capabilities enable businesses to identify potential ransomware vulnerabilities and develop effective countermeasures.

Raising Employee Awareness

Phishing continues to be a pervasive threat, making ongoing employee education essential. Training staff to recognize and respond to phishing attempts is critical for maintaining organizational security. [***SOCRadar's Brand Protection suite***](#) provides comprehensive VIP Protection, addressing the growing challenge of identity-based threats.

Strengthening Defenses Against Stealer Malware

Stealer malware poses a growing risk to Nordic enterprises. Enhanced defenses against this threat are essential to safeguarding sensitive data. [***SOCRadar's Identity & Access Intelligence Module***](#) is vital in detecting and mitigating data breach risks, strengthening the overall security posture.

Mitigating DDoS Attacks

The increasing scale and complexity of DDoS attacks in the Nordic Region require robust mitigation efforts. Implementing advanced DDoS protection technologies is critical for managing high-volume traffic and multi-vector attacks. [***SOCRadar's DoS Resilience Free Tool***](#) offers a sophisticated solution to assess and strengthen infrastructure against these threats, utilizing AI and cloud technologies for optimal protection.

SOCRadar's Recommendations: A Comprehensive Path to Cyber Resilience

- Adopting a proactive cybersecurity approach supported by SOCRadar's Threat Intelligence, Dark Web Monitoring, and Brand Protection solutions.
- Building a culture of cybersecurity awareness and prioritizing ongoing risk mitigation strategies to counter dynamic threats.
- Leveraging Cyber Threat Intelligence (CTI) to enhance immediate threat response and long-term preparedness.
- Fostering collaboration among cybersecurity professionals and leveraging robust CTI frameworks to safeguard digital assets and maintain operational continuity.

By following these recommendations, organizations in the Nordic Region can significantly strengthen their cyber defenses and confidently navigate the complexities of today's 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.

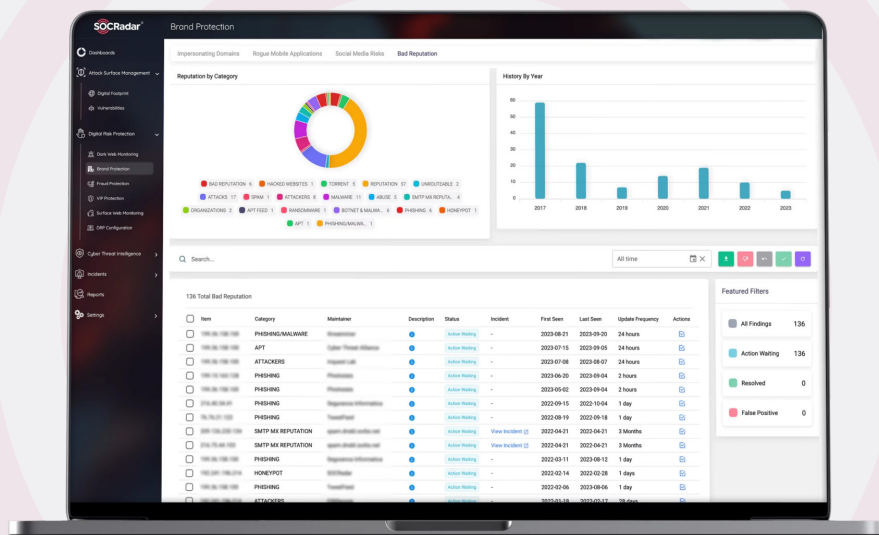
Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

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

START YOUR PERSONALIZED DEMO

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.



Start Your Demo



SOCRadar[®]

Your Eyes Beyond

SOCRadar HQ

HQ Office: 254 Chapman Rd, Ste
208 Newark, Delaware 19702 USA

Call

+1 (571) 249-4598

Email

info@socradar.io

socradar.io

Virtual Addresses

London, UK

167 City Road Old Street,
London EC1V 1AW

Dubai, UAE

8W building 5th Floor,
DAFZA, Dubai

São Paulo, Brasil

7th & 8th Floors Torre
Joao Salem, Av. Paulista
1079 São Paulo

Bangalore, India

The Estate, 8th Floor
Dickenson Road 560042
Bangalore Karnataka

