Threat Landscape Report

DENMARK

June 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cybercrime has become an actual and everlasting threat to all public authorities, specialized organizations, and residents in Denmark. The capability of cybercriminals to design and adjust their techniques to new realities and private collaboration on dark web forums raises the threat.

SOCRadar Threat Landscape Report provides organizations with an understanding of evolving cyber threats relevant to their geographical operating locations to enable security leaders to make better decisions.

The intelligence provided in this report can help plan enterprise-wide security programs, make investment decisions, and define cybersecurity requirements.

SOCRadar characterizes the threat landscape based on recently observed threat actor activities, malware campaigns, new critical vulnerabilities, exploits, data gathered from open threat sharing platforms, and leveraging the comprehensive data monitoring, collection, classification, and analysis capabilities.

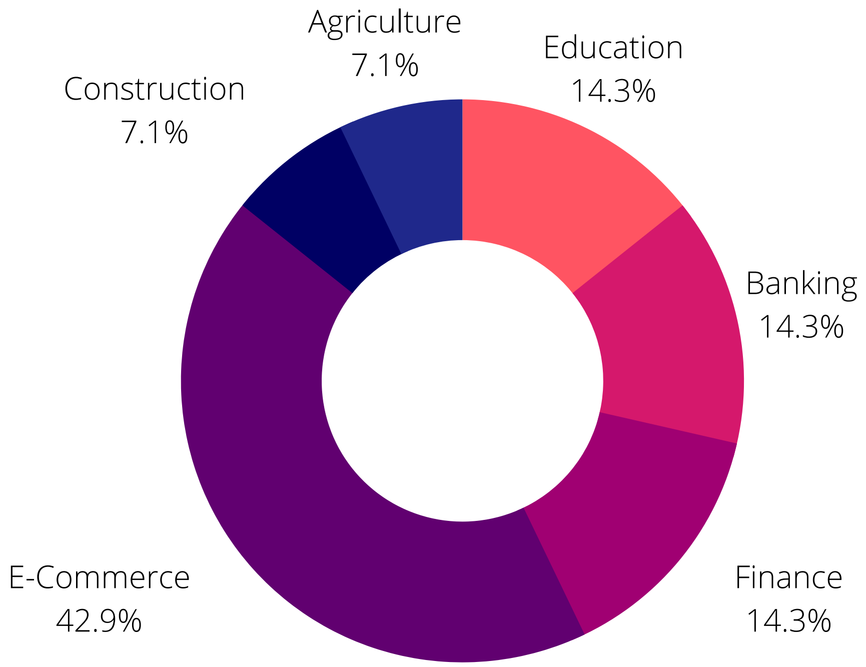
SOCRadar CTIA Team performs deep/dark web threat research, HUMINT observations, cybersecurity vendor blogs, and aggregating information gathered on social media trends, thanks to its unique perspective on understanding its competitors.

KEY FINDINDS

- **29 different threat actors targeting the Denmark entities shared posts on the deep web.**
- **Top ransomware gangs targeting Denmark are "LockBit 2.0, Conti, and Pysa".**
- **12 APT groups that have targeted government and private sectors in the past from Denmark.**
- **SOCRadar has detected 2,593 phishing attacks targeting Denmark**
- **DDoS attacks in the last year impacted critical emergency services and Denmark generate 20 TBit/sec DDoS traffic, ranking 36th in the world.**

Deep Web Threats

The deep web underground ecosystem is the number one communication channel and a global marketplace with various hacking tools and stolen databases available for purchase. Twenty-nine different threat actors targeting the Denmark entities shared posts on the dark web. Most of these posts were sales of unauthorized network access (RDP and VPN). These campaigns have exposed an extensive dataset belonging to different organizations from various verticals, including e-commerce, banking & finance, construction, and education.



The most targeted verticals in the Denmark based on DarkMirror Intelligence data

29

Dark web threat actors / aliases

9

Danish companies are targeted every 9 days on the dark web

E-Commerce

The most targeted vertical

59%

of illegal downloads are movies

Unauthorized Network Access

The most common threat category

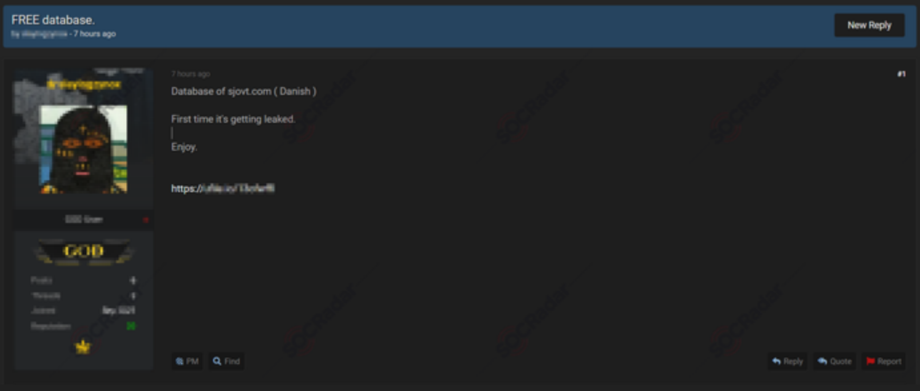
7

number of customer or user database sale posts on the dark web

Major Dark Web Incidents of the last year

Database of a Danish Website is Leaked

On September 21, 2021, SOCRadar detected a database leak of sjovt.com in a hacker forum. The threat actor did not specify the leak's contents but stated that the database was not leaked before; this was the first time it was getting spread. The leak is not for sale; the actor posts the leak directly with the title "FREE database."



FREE database.
By [redacted] - 7 hours ago

7 hours ago

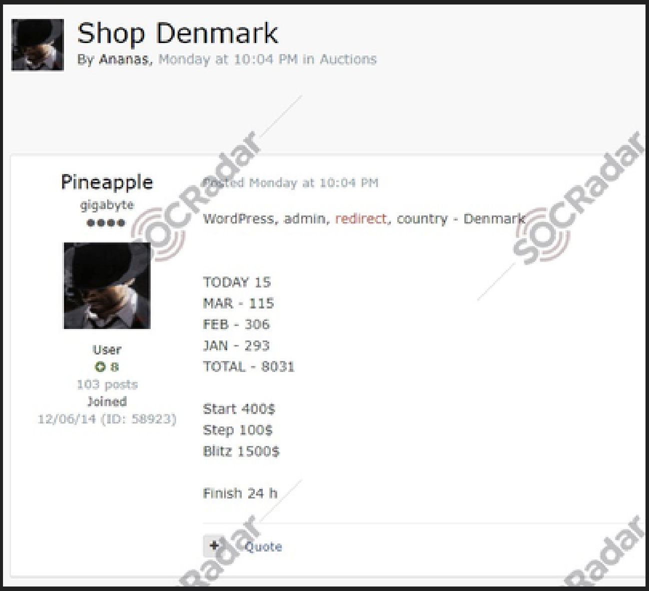
Database of sjovt.com (Danish)

First time it's getting leaked.

Enjoy.

https://[redacted]

WordPress Admin Access of Danish Websites are on Sale



Shop Denmark
By Ananas, Monday at 10:04 PM in Auctions

Pineapple
gigabyte
User
8
103 posts
Joined
12/06/14 (ID: 58923)

Posted Monday at 10:04 PM

WordPress, admin, redirect, country - Denmark

TODAY 15
MAR - 115
FEB - 306
JAN - 293
TOTAL - 8031

Start 400$
Step 100$
Blitz 1500$

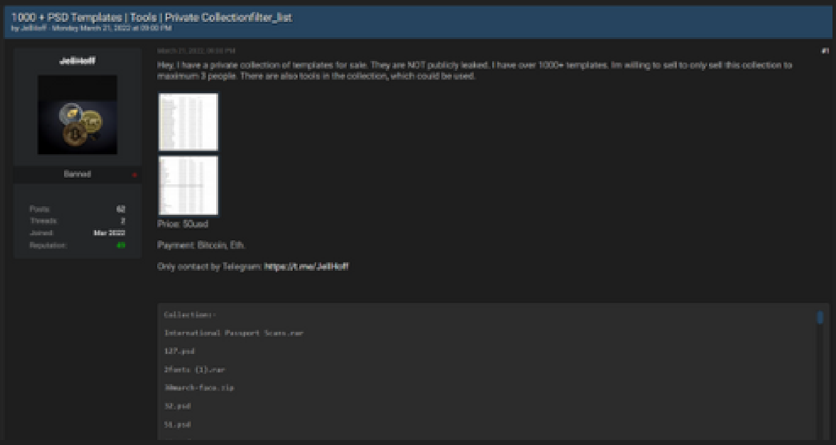
Finish 24 h

On March 8, 2021, an unauthorized network access sale allegedly belonging to companies in Denmark was put on sale in a hacker forum monitored by SOCRadar. The threat actor was attempting to sell WordPress admin access to 8,031 websites, possibly belonging to multiple Danish companies. The auction's starting price was 400USD with a 100USD increment in each offer. The instant buying price was 1500USD, and the auction lasted for 24 hours.

Major Dark Web Incidents of the last year

Official Templates Leaked on Breach Site

On March 21, 2022, 1000+ PSD templates of different countries and tools to utilize them were leaked on a breach forum. The breacher put the data on sale for a limited count of buyers. Templates include a variety of licenses, country bills, passports, etc.



1000 + PSD Templates | Tools | Private Collectionfilter_list
by JellHoff · Monday March 21, 2022 at 09:00 PM

JellHoff
Banned
Posts: 62
Threads: 2
Joined: Mar 2022
Reputation: 40

March 21, 2022, 09:00 PM #1

Hey, I have a private collection of templates for sale. They are NOT publicly leaked. I have over 1000+ templates. Im willing to sell to only sell this collection to maximum 3 people. There are also tools in the collection, which could be used.

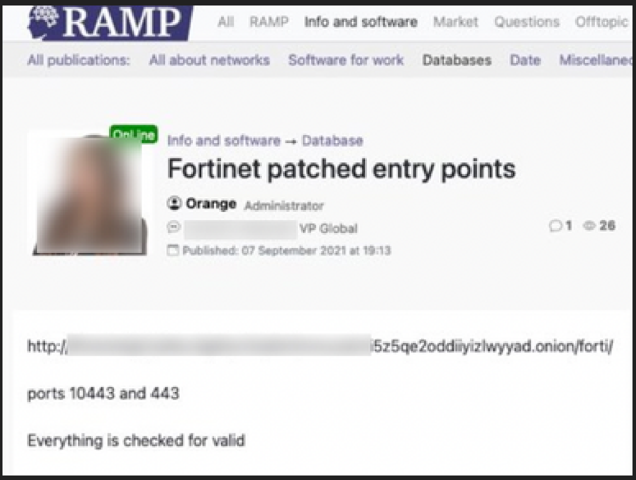
Price: 50usd

Payment: Bitcoin, Eth.

Only contact by Telegram: https://t.me/JellHoff

```
Collection:-
International Passport Scans.rar
127.psd
2fonts (1).rar
30march-face.zip
32.psd
51.psd
```

Fortinet VPN Login Credentials Leaked:



Info and software → Database

Fortinet patched entry points

Orange Administrator

[redacted] VP Global

1 26

Published: 07 September 2021 at 19:13

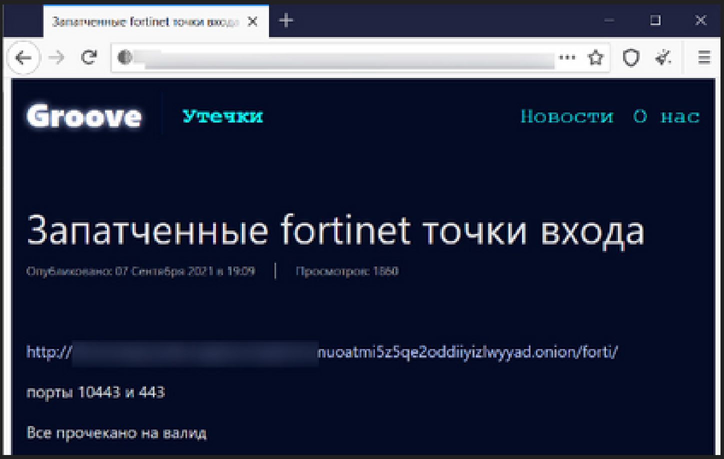
http:/[redacted]5z5qe2oddiiyizlwyyad.onion/forti/

ports 10443 and 443

Everything is checked for valid

Fortinet credentials were leaked for free on the hacker forum RAMP by a threat actor known as "Orange." The same link was also posted at the same time by the ransomware organization Groove Gang. Both posts lead to a file hosted on a Tor storage server Analysis (done by BleepingComputer) of this file shows that it contains VPN credentials for 498,908 users over 12,856 devices. The victim list is available on GitHub.

Because the VPN credentials could give threat actors access to a network to exfiltrate data, install malware, and launch ransomware attacks, this leak is a severe incident. The threat actor claims many VPN credentials are still valid, although the exploited Fortinet vulnerability has subsequently been patched.



Запатченные fortinet точки входа

Опубликовано: 07 Сентября 2021 в 19:09 | Просмотров: 1860

http://[redacted]nuoatmi5z5qe2oddiiyizlwyyad.onion/forti/

порты 10443 и 443

Все прочекано на валид

Disney+ Accounts Leaked:

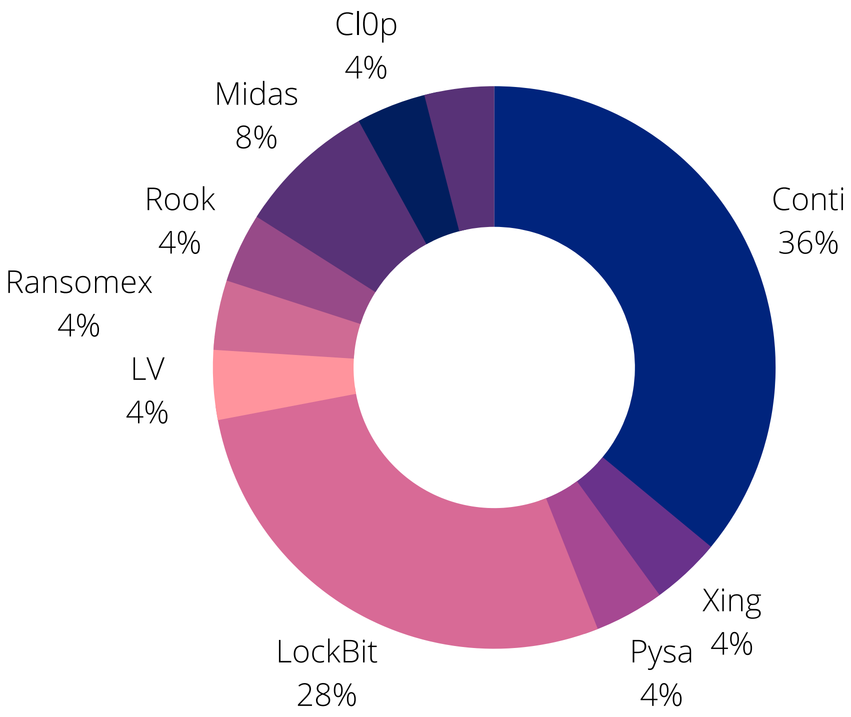
Thousands of Disney+ accounts were leaked and sold on various hacker forums. There are plenty of Danish accounts among them. The data was shared on hacker forums and Telegram. On Telegram, the hackers proclaimed that they had thousands of active Disney + reports in stock. The seller offered 200 accounts free, just for example.

Ransomware Threats

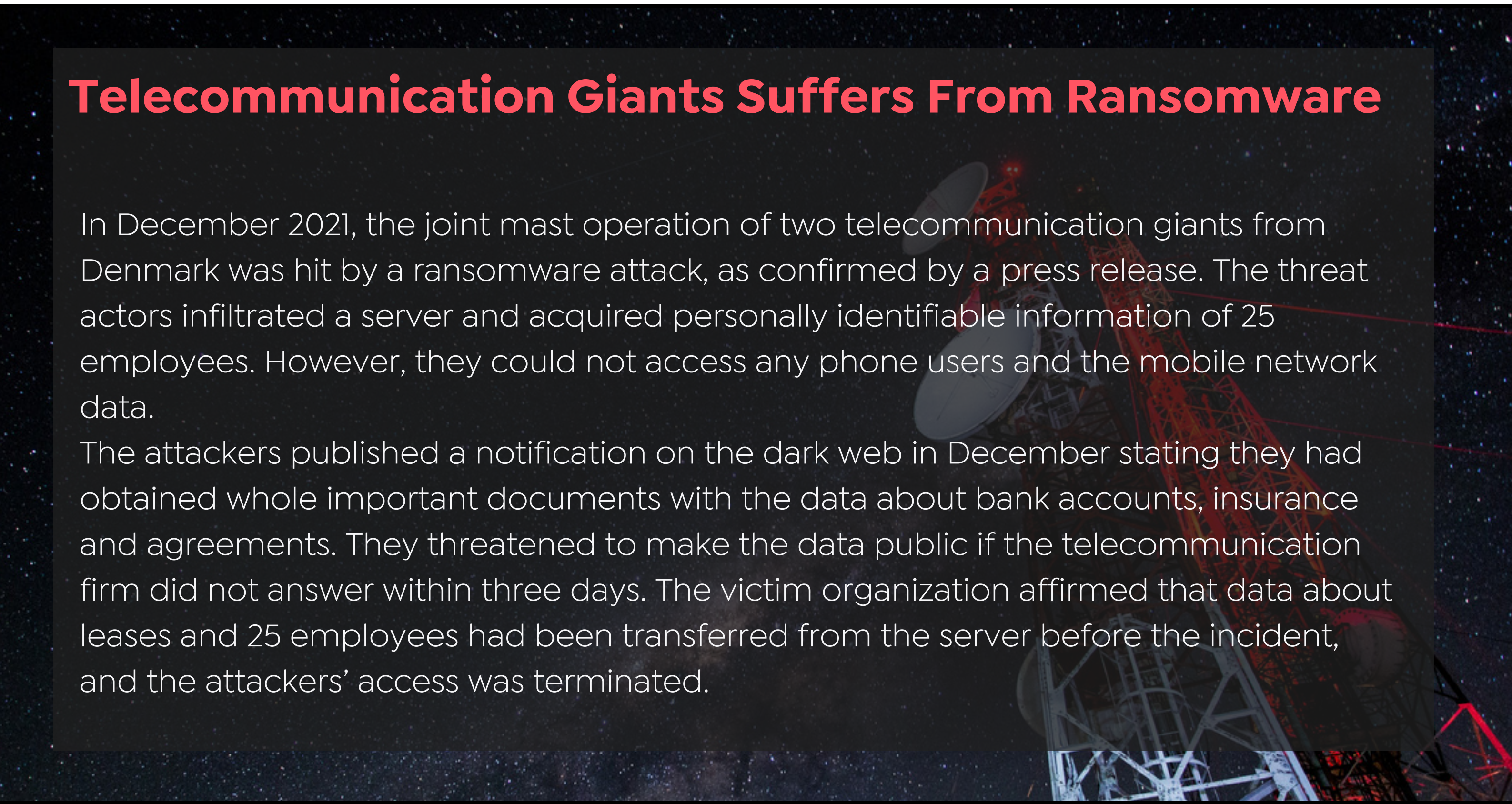
As in previous years, the threat level for cybercrime is considered the highest status due to targeted ransomware attacks affecting companies from Denmark. To put pressure on their victims, various threat groups initiated threatening to leak stolen sensitive information.

9 different ransomware gangs' incidents affected organizations from Denmark

Most preferred methods to gain initial access in ransomware attacks in the last year



Telecommunication Giants Suffers From Ransomware



In December 2021, the joint mast operation of two telecommunication giants from Denmark was hit by a ransomware attack, as confirmed by a press release. The threat actors infiltrated a server and acquired personally identifiable information of 25 employees. However, they could not access any phone users and the mobile network data.

The attackers published a notification on the dark web in December stating they had obtained whole important documents with the data about bank accounts, insurance and agreements. They threatened to make the data public if the telecommunication firm did not answer within three days. The victim organization affirmed that data about leases and 25 employees had been transferred from the server before the incident, and the attackers' access was terminated.

Top Ransomware Gangs Targeting Denmark

LockBit 2.0

- Ransomware-as-a-service (RaaS) operator.
- Most victims are from the enterprise and are expected an average ransom of $85k
- Behind Accenture ransomware attack

Conti

- Ransomware-as-a-service (RaaS) operator, operating out of Russia.
- The group has pulled off multiple high-profile attacks on Danish companies.
- A playbook related to Conti was allegedly released by an affiliate upset with Conti in September 2021.

Pysa

- First disclosed and patched in 2018.
- A new version of Pysa has been defined in open sources since 2019 December.
- Lately, the long list of victims has lately included production firms from Denmark.

State-Sponsored APT Activities

Organizations in Denmark continue to be targets of advanced persistent threat actors with diverse motivations. Specific APT groups from Russia and China have recently targeted leading organizations in the military, government, high-tech, and finance verticals. To reach the state goals through the collection of strategic intelligence is believed to be the primary motivation of the state-sponsored actors.

The international Solarwinds cyber-attack hacked Denmarks Nationalbank in December 2020. Russian origin threat attackers infiltrate the systems of Denmarks Nationalbank. They even remained their accessibility to the victim network for more than six months. The SolarWinds supply chain attack, which the Nobelium APT carried out (APT29, Cozy Bear, and The Dukes), resulted in a security compromise. According to the statements of Denmark's central bank to Version 2, the response to the attack was systematic and immediate in a comprehensive manner, and the attack had any actual impacts considering the analyses conducted.

Significant APT Groups

APT41

Last activity:
December, 2021

Nobelium

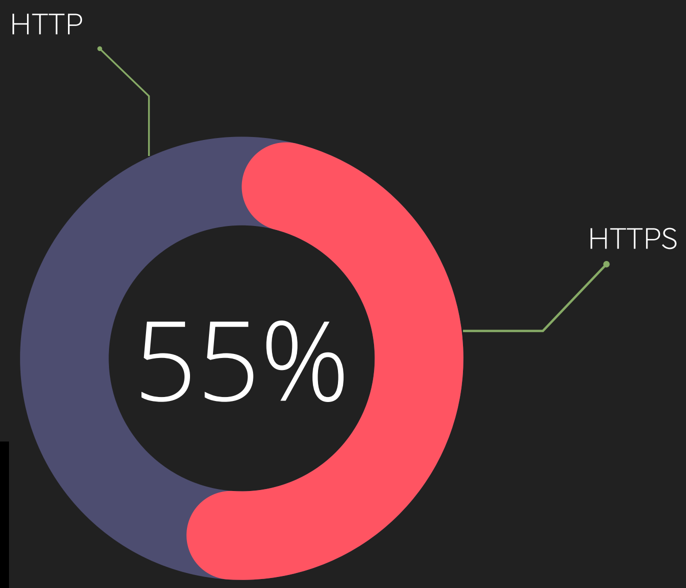
Last activity:
December, 2021

APT28

Last activity:
October, 2021

Phishing Threats

Email phishing remains the top ransomware attack vector. The typical tactic is to deliver malicious macro-enabled Office documents attached to the email. The effects can increase dramatically with business email compromise (BEC) scams and social engineering methods.



Attackers are increasingly using HTTPS to lure their victims into clicking malicious links

Most used phishing lure keywords: "Whatsapp, Facebook, USPS, Instagram, Event Mobile Legend, DHL"

SOCRadar has detected 183 primary phishing attacks targeting organizations from Denmark in the last year. SOCRadar CTIA team is seeing a phishing-enabled fraud trend targeting fast-growing digital industries, including e-commerce, booking, and cloud/SaaS.

2,593 | 183

Total phishing attacks detected over the last 6 year and the last year

Microsoft

Top SaaS phishing scheme for credential harvesting

Banking & Finance
Transportation
Energy

Top targeted sectors in Denmark

Search On Phishing Radar

Enter your domain

Critical Asset Exposures & Vulnerabilities

When SOC analysts, vulnerability management teams, and security leaders have limited time and budget, prioritizing vulnerabilities to reduce the public attack surface becomes paramount. Following is a high-level statistical view of the critical ports and vulnerabilities in the internet-facing infrastructure and technologies. According to a recent analysis by security research firms, Denmark is the most cyber-secure country in the world.

Various surveys looked at how vulnerable different countries are to security weaknesses to see which ones are best prepared for cyberattacks, and Denmark came out on top. The study's results were based on vulnerability markers such as the percentage of infected mobile devices and the number of infected systems in a country.

Vulnerability | CVE ID | CVSSv3

The most commonly exploited vulnerabilities in Denmark.

BIOS Insufficient control flow management	CVE-2021-0157 #BIOS	CVSS: 8,2
Microsoft Exchange Server RCE Vulnerability	CVE-2019-26857	CVSS: 9,8
SolarWinds Serv-U Execute CodeGain privileges	CVE-2021-35211	CVSS: 10,0

632,433

Open port number

80, 443, 7547

Most used ports

GAIN VISIBILITY INTO HACKERS’ PERSPECTIVE

Identity & Credentials Intelligence

Using stolen credentials is one of the most common initial access techniques leveraged by your adversaries. C-level certificates are significantly more helpful for BEC attackers. Last year, SOCRadar detected more than 1 billion exposed credentials by analyzing the breach datasets shared on the deep and dark web forums, which are tied to plain-text passwords.

However, according to the statistics, digital identity theft is not a significant threat. The Genesis Marketplace is a dark web underground avenue for threat actors to buy digital identities.

CHECK FOR ACCOUNT BREACH

Enter your domain/email

3104

Bots for sale
Denmark

424K

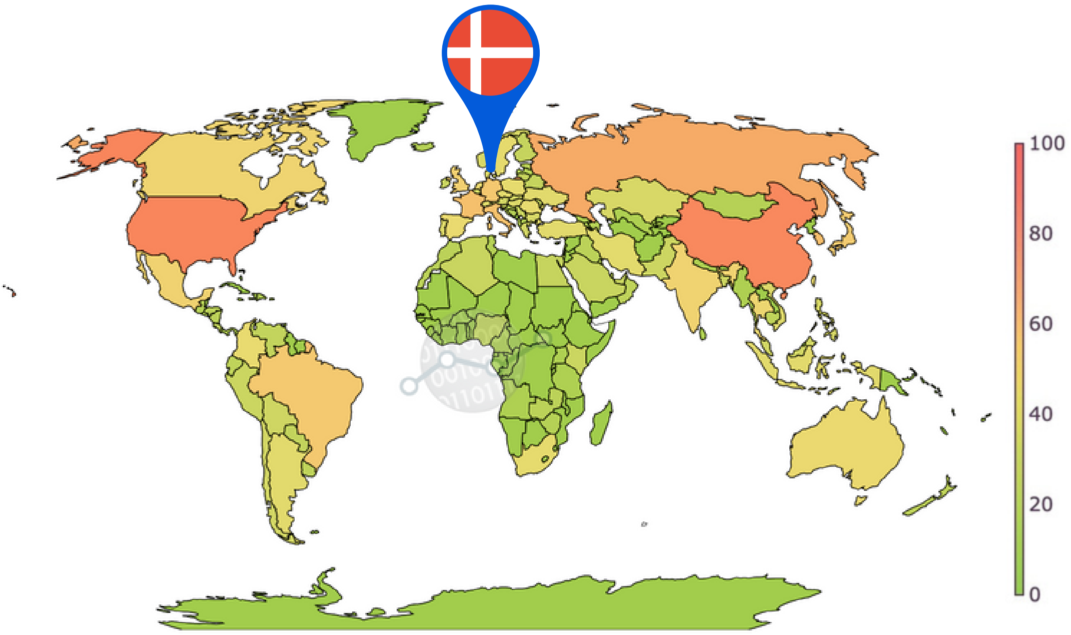
Total bots for sale

DDoS | Risk-to-others

The global internet ecosystem is currently vulnerable and carrying high malicious traffic. Sophisticated threat actors take advantage of these weak points for amplifying disruptive DDoS attacks against businesses, resulting in financial losses and critical service disruptions.

Denmark's e-commerce and financial entities were also among the victims of DDoS attacks in the last year. Based on the global risk condition dataset provided by Cyber Green Initiative, Denmark can generate 20 Tbit/sec DDoS traffic, ranking 36th globally.

DDoS | Risk-to-others



Global heatmap view of total potential DDoS bandwidth by country

Data source: Cyber Green

CHECK FOR DoS RESILIENCE

Enter your domain/IP Block

20 TBit/Sec

Denmark | Total DDoS Potential

7,471
Open Recursive DNS

3,045
Open SNMP

35,361
Open NTP

44,034
Open Vulnerable Devices

1,054
Open SSDP

ABOUT SOCRadar®

SOCRadar platform is an all-in-one solution that provides Extended Threat Intelligence, Digital Risk Protection, and External Attack Surface Management. Its false-positive free platform helps companies proactively defend themselves against cyber incidents. SOCRadar is empowered with robust AI algorithms and a highly talented analyst team; together, they eliminate false positives.

FOLLOW US!

DISCOVER SOCRADAR® FREE EDITION

With SOCRadar® Free Edition, you'll be able to:

- Discover your unknown hacker-exposed assets
- Check if your IP addresses tagged as malicious
- Monitor your domain name on hacked websites and phishing databases
- Get notified when a critical zero-day vulnerability is disclosed

GET FREE ACCESS

CONTACT US ✉ info@socradar.io ☎ +1 (571) 249-4598

651 N Broad St, Suite 205,
Middletown, DE 19709