The Power of Cyber Threat Intelligence in the SOC: Case Studies and Insights

Shamil Alifov

netnordic
THE BEST COMPANION

whoami

- Education
  - BSc ”Applied Mathematics”, Azerbaijan
  - MSc ”Data Security and Cryptography”, Finland
- Community
  - TurkuSec/PersecCamp/DisArray
  - DisObey
- Threat Intelligence Specialist NetNordic Finland
- Dad of twin rascals, Nature walks, Reading, Cooking

netnordic
THE BEST COMPANION

Agenda

Threat Landscape

Threat Intelligence

Information Stealing Malware

Initial Access Brokers

Ransomware

netnordic
THE BEST COMPANION

Threat Landscape

Sweden investigates telecoms infrastructure sabotage following attacks at 30 sites

Cyberattack disrupts Finland's defence ministry website

Russia intensifies cyberattacks on Ukraine allies

Russian hackers seized control of Norwegian dam, spy chief says

Hundreds of Swedish municipalities impacted by suspected ransomware attack on IT supplier

netnordic
THE BEST COMPANION

Threat Intelligence

Actionable Relevant Timely

netnordic
THE BEST COMPANION

Information Stealing Malware

malicious software that harvest sensitive information/data from infected victims

netnordic
THE BEST COMPANION

The silent heist: cybercriminals use information stealer malware to compromise corporate networks

Snowflake Attacks: Mandiant Links Data Breaches to Infostealer Infections

Infostealers Cause Surge in Ransomware Attacks, Just One in Three Recover Data

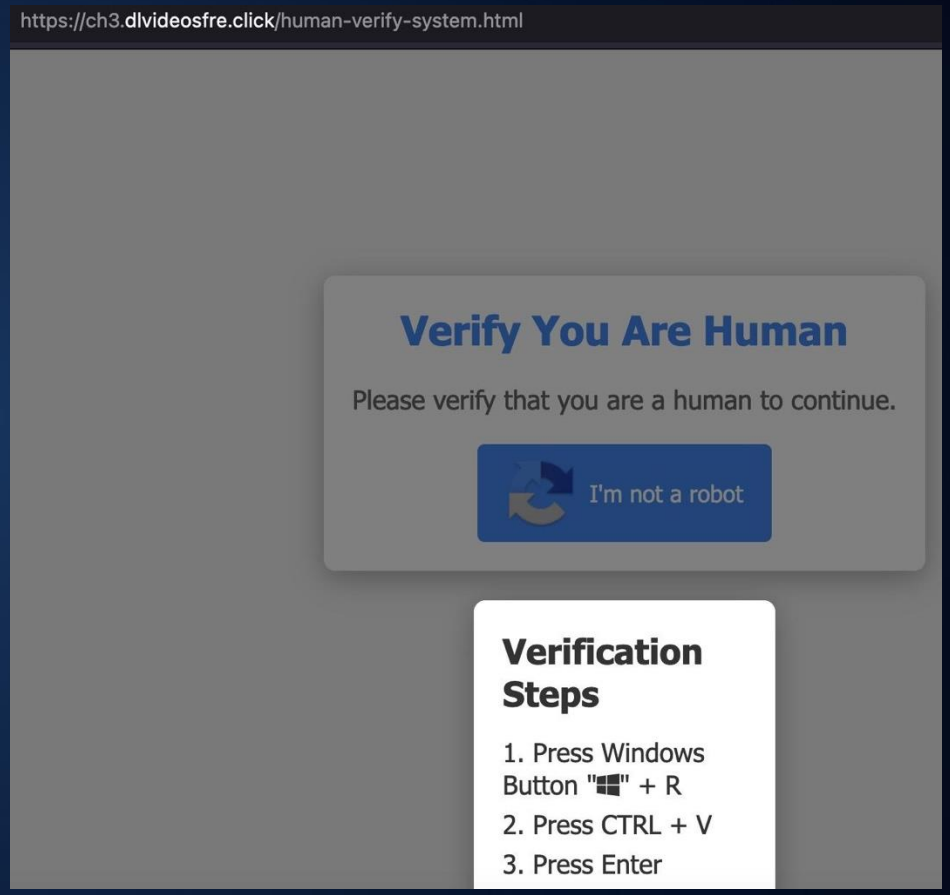
Gmail Passwords Confirmed Within 183 Million Account Infostealer Leak

netnordic
THE BEST COMPANION

Infostealers | Distribution

Various distribution channels:

- Phishing emails/social networks
- Pirated/Cracked software
- Malvertising/SEO poisoning
- Fake updates
- ClickFix/FileFix
- Vulnerabilities



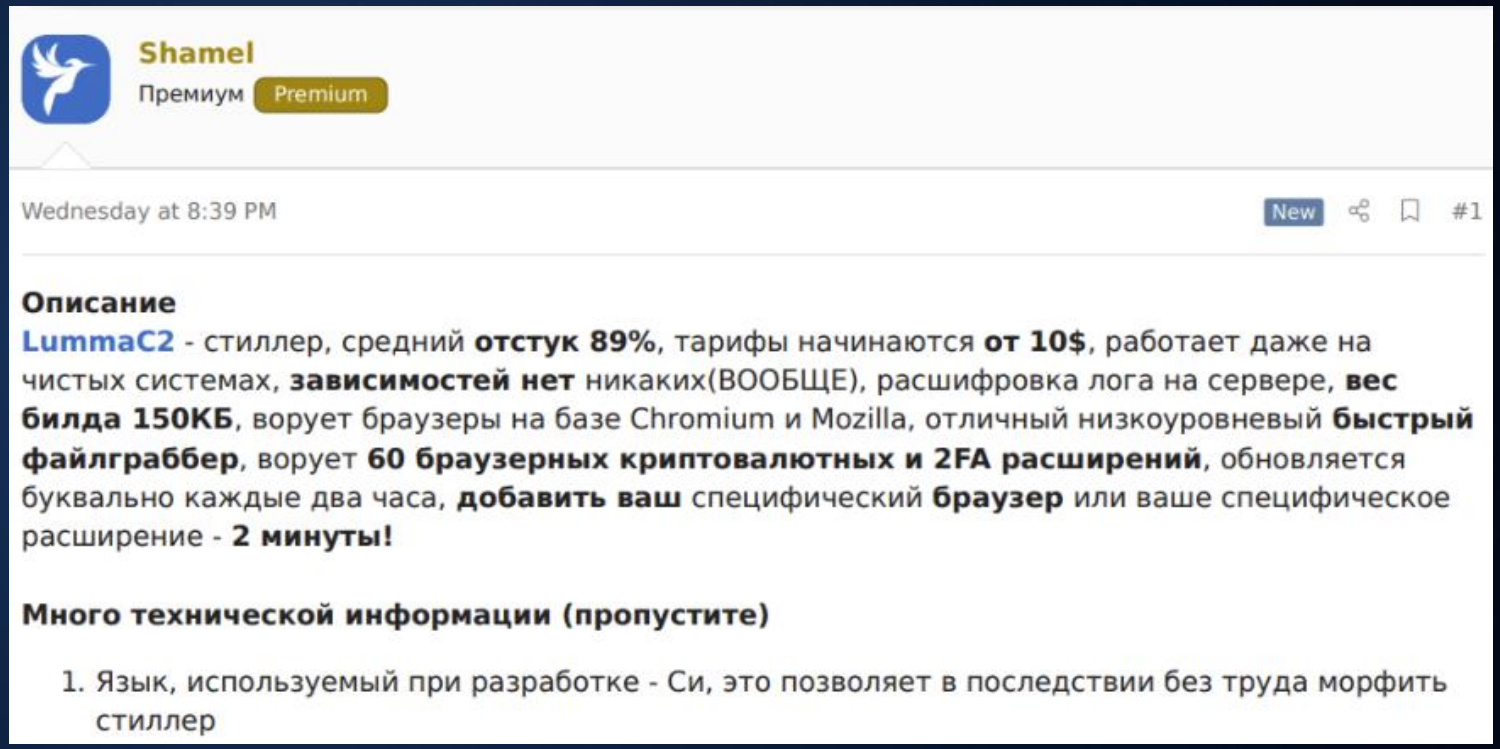
netnordic
THE BEST COMPANION

Infostealers | Variations

Malware-As-A-Service

Private Infostealers

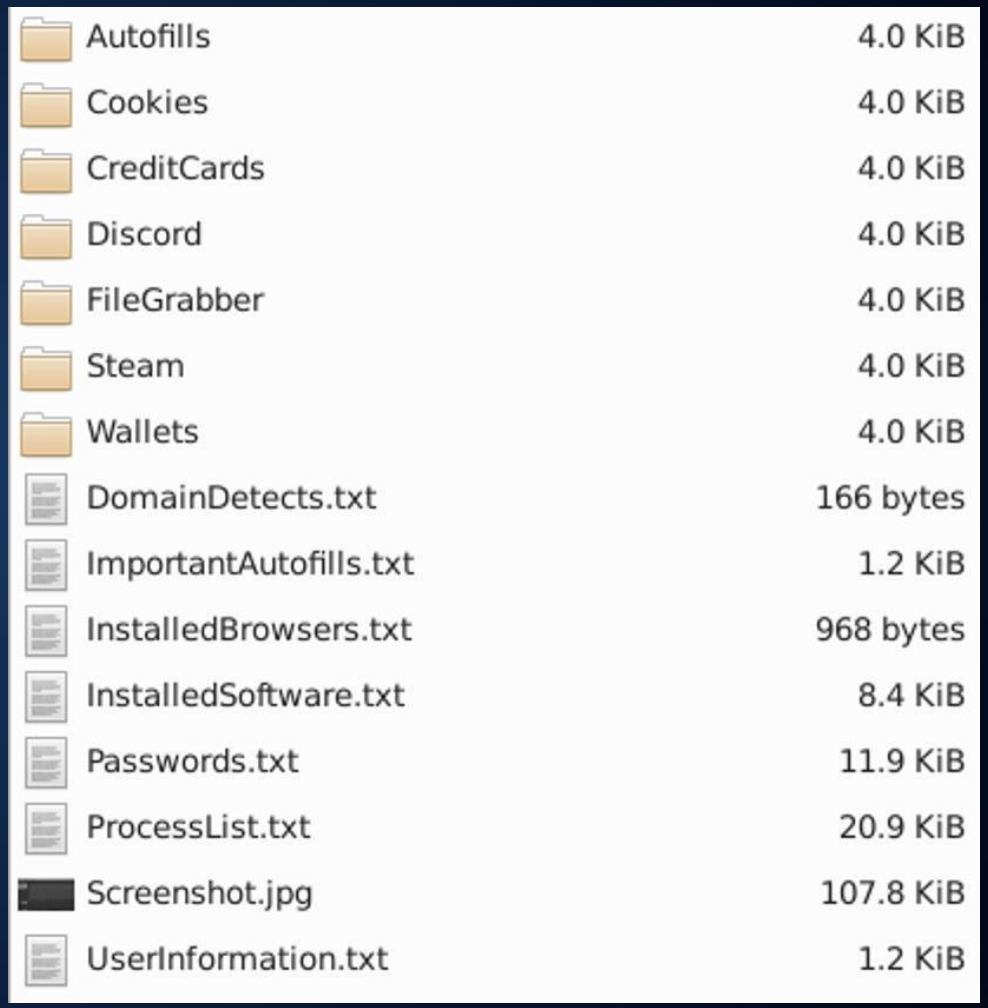
Open-source Infostealers



netnordic
THE BEST COMPANION

Infostealers | What do they steal

- System and User information
- Software/Running processes
- Browser data
- Credentials
- Credit cards
- Application configs
- Screenshot
- Files



netnordic
THE BEST COMPANION

Infostealers | What do they steal

system_info.txt

```
Network Info: Slurm Cloud | Private – The  on the market
    - IP: 212.10[redacted]
    - Country: DK

System Summary:
    - HWID: 67A15DCE-BC89-[redacted]
    - OS: Windows 10
    - Architecture: x64
    - UserName: [redacted]
    - Computer Name: DESKTOP-[redacted]
    - Local Time: 2025-09-20 00:36:40
    - UTC: 1
    - Language: da-DK
    - Keyboards: Dansk (Danmark) / Engelsk (USA) / Engelsk (USA)
    - Laptop: FALSE
    - Running Path: C:\Users\[redacted]\AppData\Local\Temp\Rar$EXb17340.2946.rartemp\DropCheats\DropCheats.exe
    - CPU: Intel(R) Core(TM) i5-10400F CPU @ 2.90GHz
    - Cores: 6
    - Threads: 12
    - RAM: 16 GB
    - Display Resolution:
       Monitor 1
           Device Name: \\.\DISPLAY1
           Device String: NVIDIA GeForce GTX 1660 SUPER
           Resolution: 1680x1050
           Color Depth: 32 bits per pixel
       Monitor 2
           Device Name: \\.\DISPLAY2
           Device String: NVIDIA GeForce GTX 1660 SUPER
           Resolution: 1920x1080
           Color Depth: 32 bits per pixel
    - GPU:
       -NVIDIA GeForce GTX 1660 SUPER
```

Information.txt

```
IP: 109.56.[redacted]
Country: DK - Denmark
Username: [redacted]
AntiVirus: Windows Defender, Sentinel Agent
Data Information: CK:3789|PW:72|AF:2508|CC:0|TK:1|FB:0|Sites:1|Wallets:0|Apps:0
```

netnordic
THE BEST COMPANION

Infostealers | What do they steal

- System and User information
- Software/Running processes
- Browser data
- Credentials
- Credit cards
- Application configs
- Screenshot
- Files

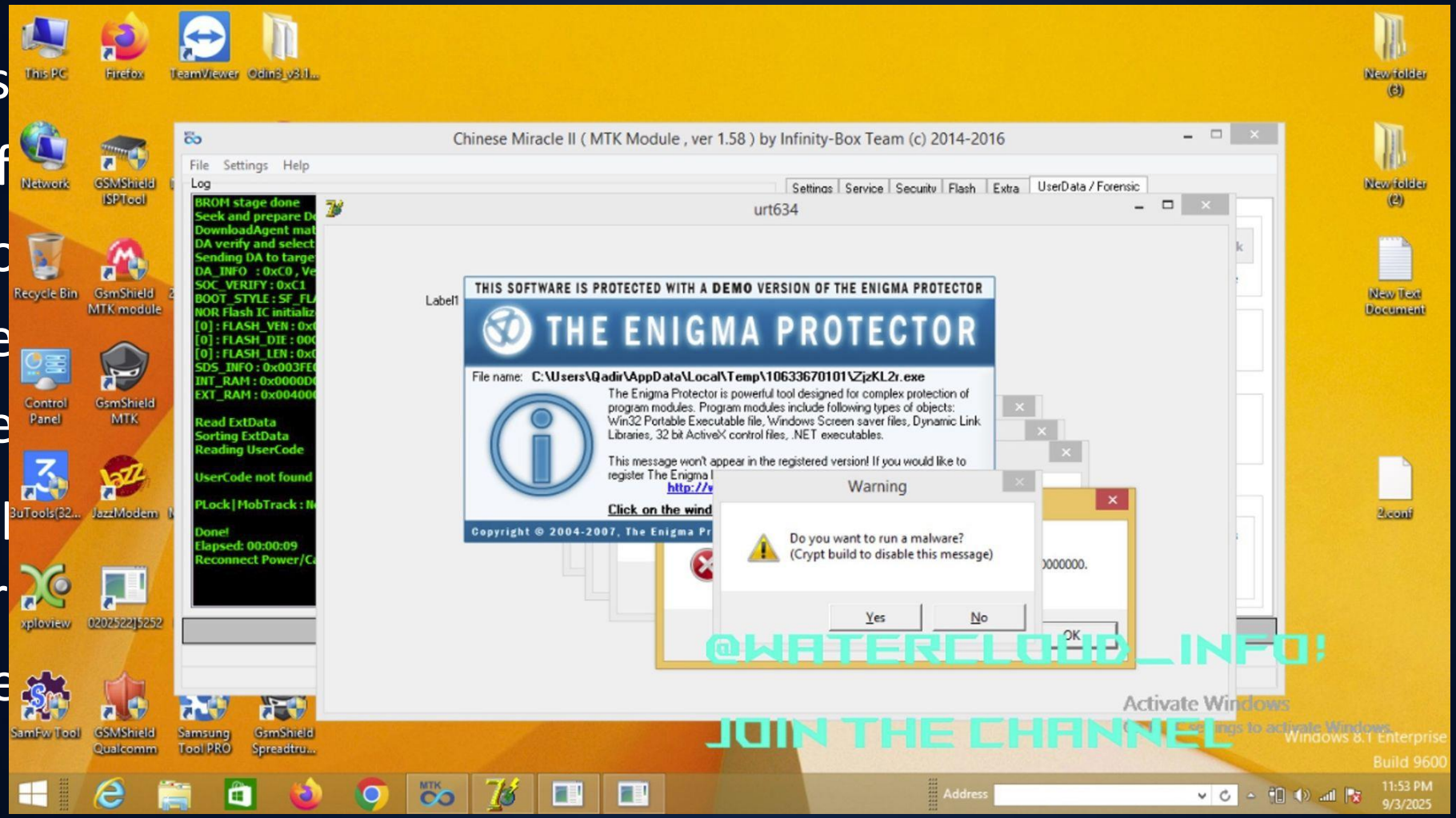
```
URL: https://vpn.fra.gov.eg/dana-na/auth/url_2/welcome.cgi
Username: [REDACTED]
Password: [REDACTED]
Application: Google_[Chrome]_Default
==============

URL: https://accounts.google.com/v3/signin/challenge/pwd
Username: [REDACTED]
Password: [REDACTED]
Application: Microsoft_[Edge]_Default
==============
```

netnordic
THE BEST COMPANION

Infostealers | What do they steal

- Sys
- Sof
- Bro
- Cre
- Cre
- Apl
- Scr
- File



netnordic
THE BEST COMPANION

Infostealers | Monetization of Data

Centralized Marketplaces

- Genesis Market
- 2Easy Shop
- Russian Market
- Lumma Market
- Exodus Market

Cloud of logs

- Telegram channels
- Free sample data sharing
- Subscriptions
- Logs aggregators

Infostealers | Russian Market

Biggest centralized infostealer marketplace

- Registration is kinda free
- Price per victim $0,50 - $10
- Over 9M victims
- Stealers: Lumma, Acreed, StealC, Vidar, Rhadamanthys
- Top 5: India, Brazil, Pakistan, Indonesia, Egypt

Infostealers | Russian Market

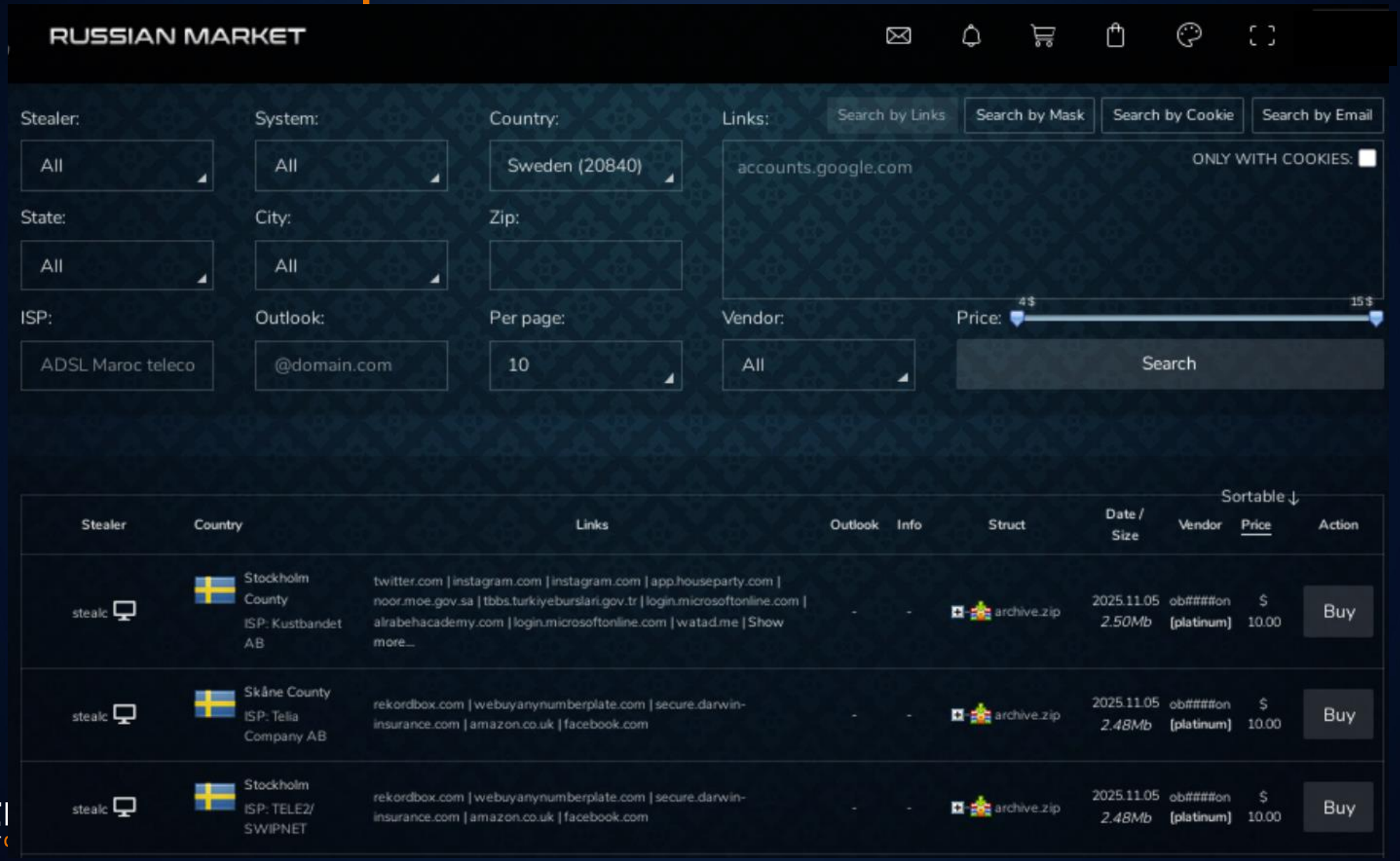
Biggest centralized infostealer marketplace

- Registration is kinda free
- Price per victim $0,50 - $10
- Over 9M victims
- Stealers: Lumma, Acreed, StealC, Vidar, Rhadamanthys
- Top 5: India, Brazil, Pakistan, Indonesia, Egypt

Infostealers | Russian Market

Country	Number of victims
Sweden	20,840
Denmark	11,284
Norway	9,209
Finland	7,471
Iceland	1,058
Greenland	150
Faroe	97
Åland	22

Infostealers | Russian Market



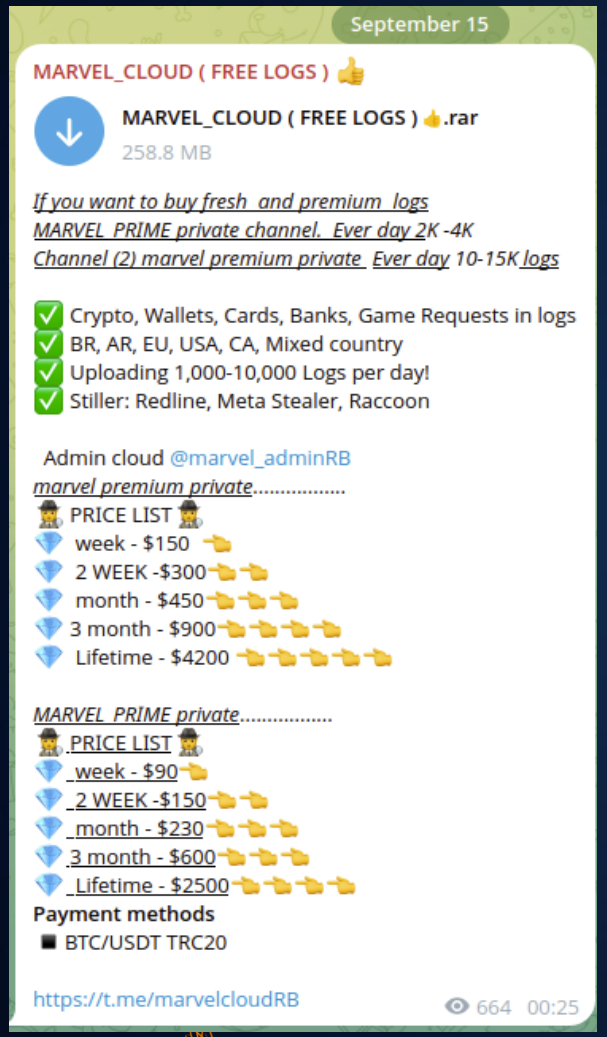
net
THE BEST

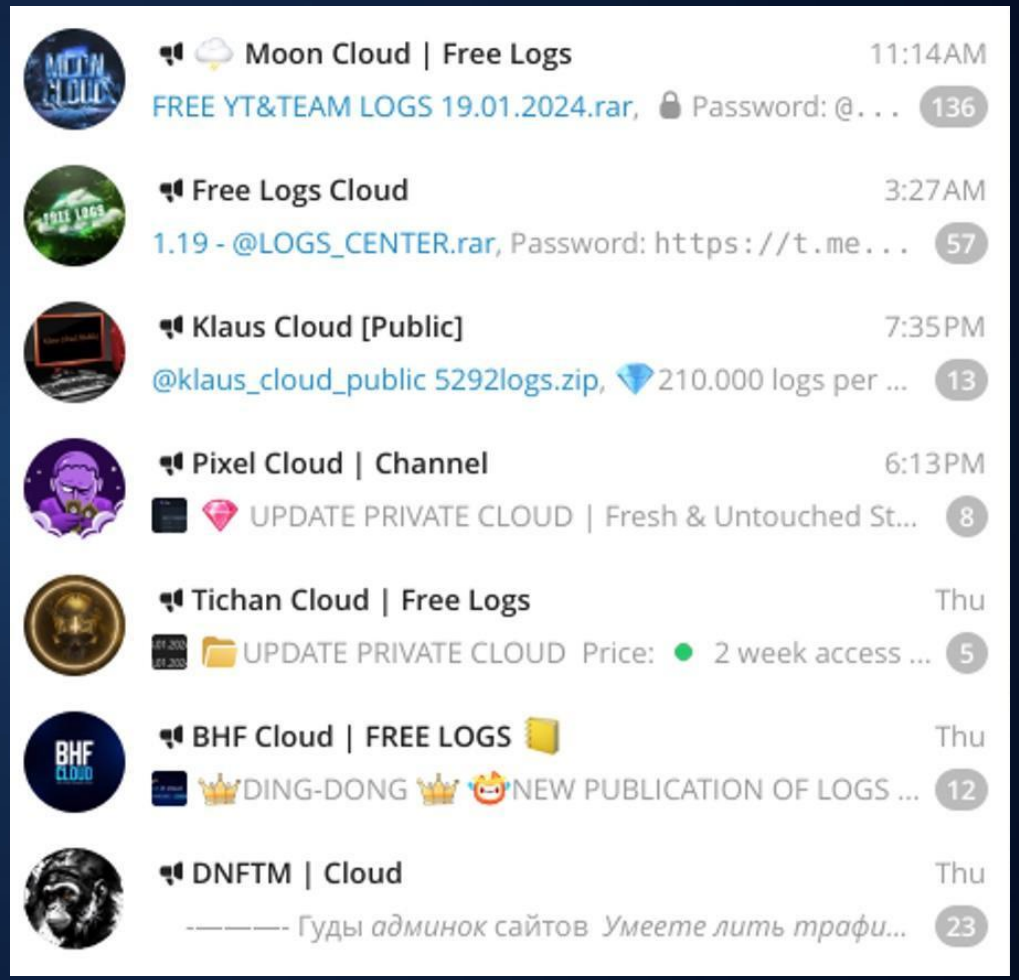
Infostealers | Russian Market

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price
stealc	Stockholm County ISP: Kustbandet AB	twitter.com | instagram.com | instagram.com | app.houseparty.com | noor.moe.gov.sa | tbbs.turkiyeburslari.gov.tr | login.microsoftonline.com | alrabehacademy.com | login.microsoftonline.com | watad.me | twitter.com | sarahah.com | sso.rumba.pearsoncmg.com | instagram.com | app.houseparty.com | e-services.qiyas.sa | accounts.google.com | cazasouq.com | twitter.com | instagram.com | e-services.qiyas.sa | m.facebook.com | najeh.online | tbbs.turkiyeburslari.gov.tr | noor.moe.gov.sa | sso.rumba.pearsoncmg.com | elearning.yu.edu.jo | auth0.openai.com | login.microsoftonline.com | accounts.google.com | tbbs.turkiyeburslari.gov.tr | auth.api.sonyentertainmentnetwork.com | auth.api.sonyentertainmentnetwork.com | accounts.google.com | login.microsoftonline.com | auth.api.sonyentertainmentnetwork.com | login.live.com | auth.api.sonyentertainmentnetwork.com | auth.api.sonyentertainmentnetwork.com	-	-	archive.zip brute.txt cookie_list.txt copyright.txt domain_detect.txt passwords.txt system_info.txt AccountTokens Google Chrome_Default.txt Google Chrome_Profile 1.txt autofill Google Chrome_Profile 1.txt Google Chrome_Profile 3.txt cookies Google Chrome_Default.txt history Google Chrome_Default.txt Google Chrome_Profile 1.txt Google Chrome_Profile 3.txt Microsoft Edge_Default.txt	2025.11.05 *2.50Mb*	ob####on **(platinum)**	$ 10.00

netnordic
THE BEST COMPANION

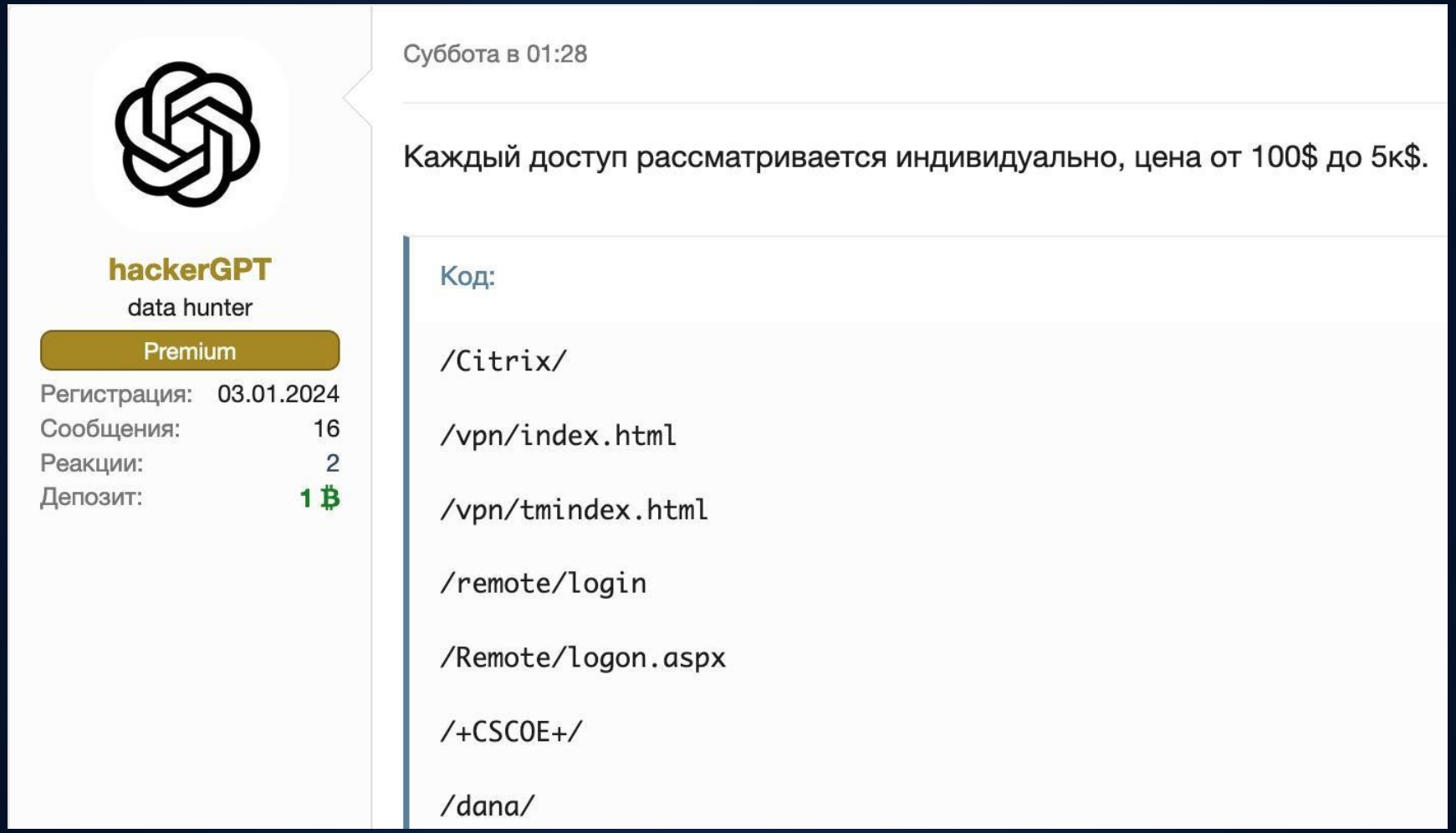
Infostealers | Cloud of Logs





netnordic
THE BEST COMPANION

Infostealers | Quiz time!



netnordic
THE BEST COMPANION

Initial Access Brokers

cybercriminals who specialize in gaining unauthorized access to networks and systems and then selling that access to highest bidders

netnordic
THE BEST COMPANION

IAB | Attack Vectors

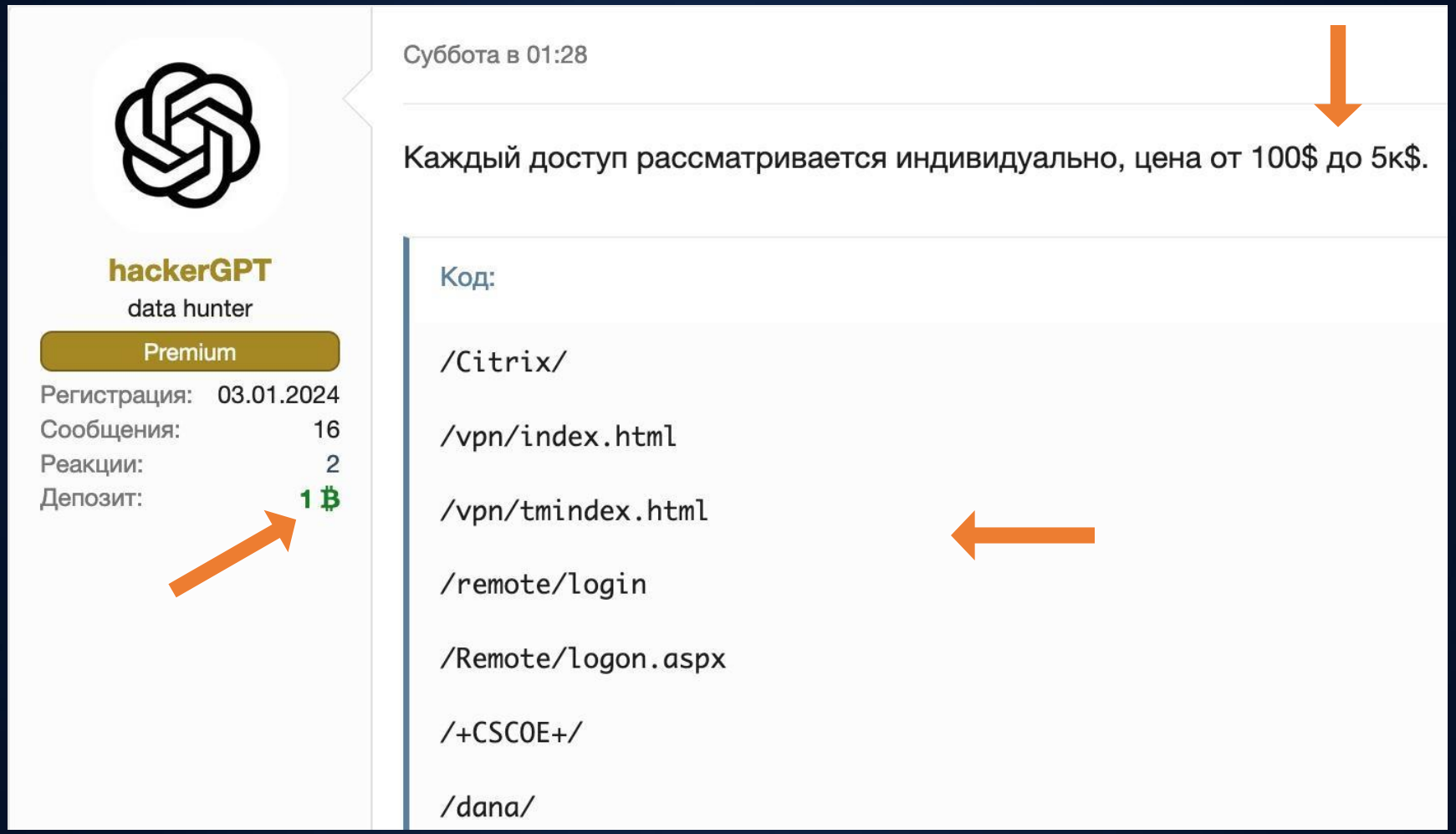
Exploitation of Vulnerabilities

Brute-force and Password Spraying Attacks

Social Engineering

Credential-based Attacks

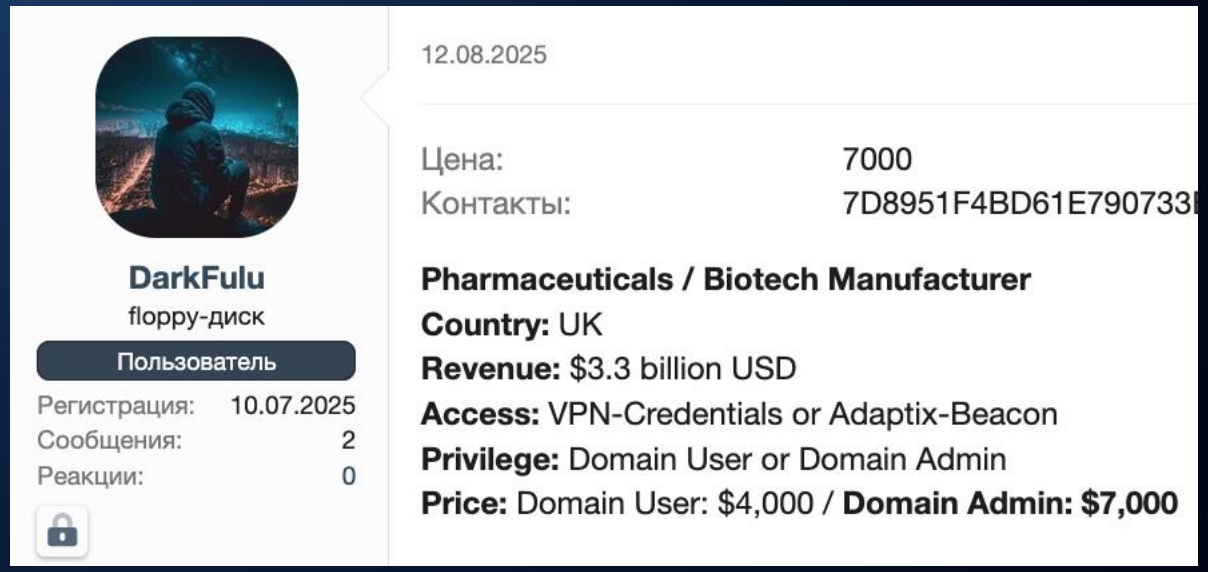
IAB | Attack Vectors



netnordic
THE BEST COMPANION

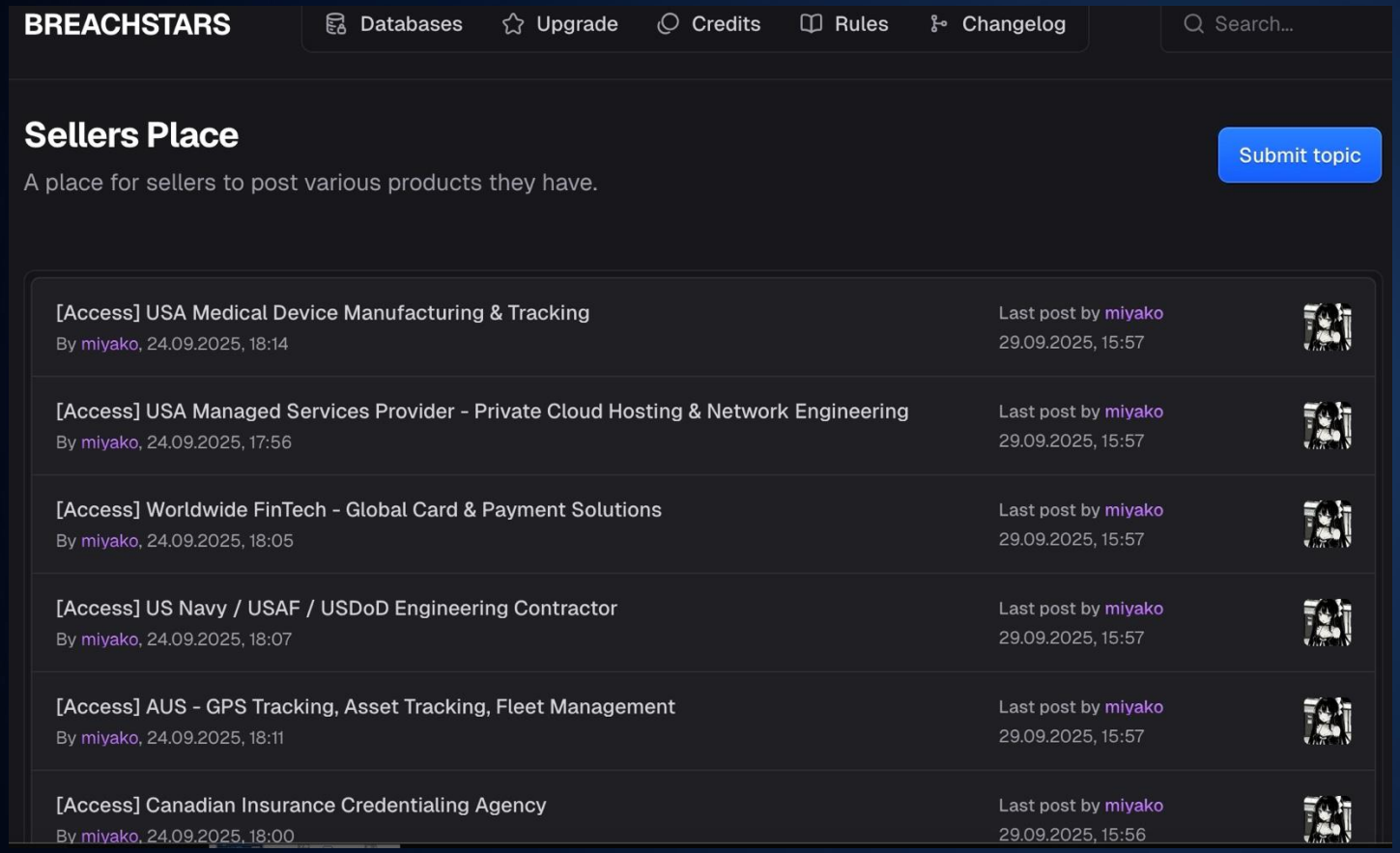
IAB | Access Types

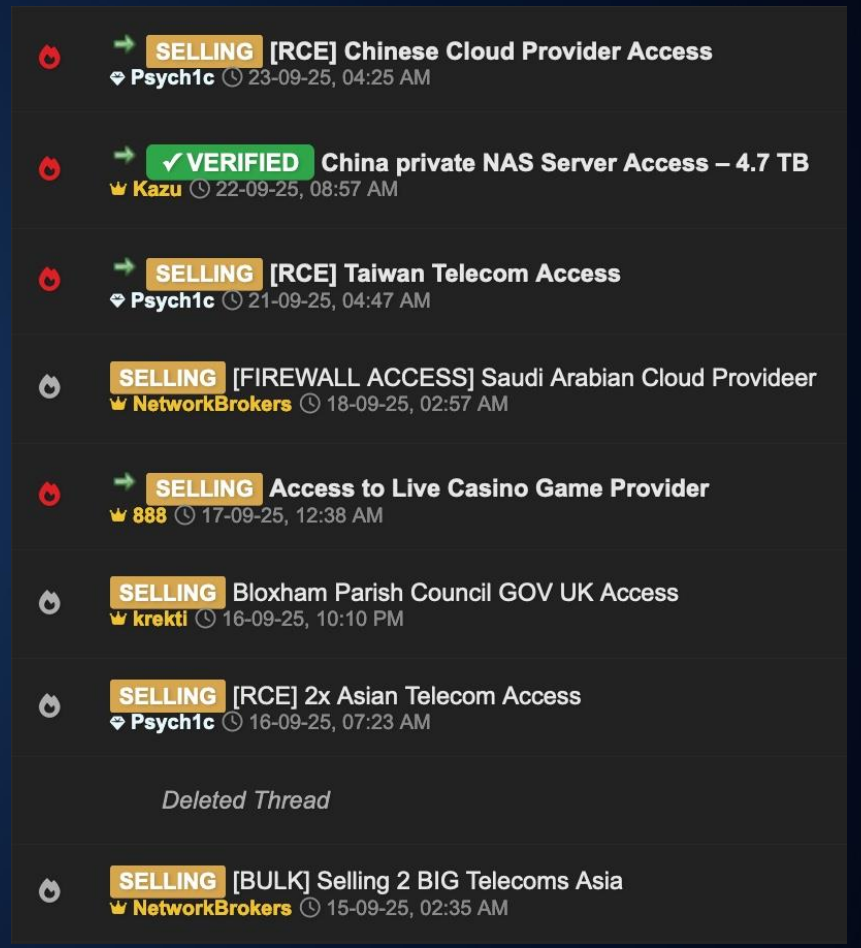
- Virtual Private Network (VPN)
- Remote Desktop Protocol (RDP)
- Web shell
- Shell/Commandline
- Remote Desktop Web Access (RDWeb)
- Email
- …



netnordic
THE BEST COMPANION

IAB | Scene





netnordic
THE BEST COMPANION

IAB | Scene

SELLING **NO HealthCare**
by Yrrrr - 13-09-25, 06:34 PM

Yrrrr

MVP

Posts	18
Threads	14
Joined	Sep 2025
Reputation	2

13-09-25, 06:34 PM (This post was last modified: 13-09-25, 06:34 PM by Yrrrr.)

Hello DarkForums

Today I'm selling an initial access to a **NO HealthCare company**

Revenue: **? (Can't find a relatable source)**
Employees: **? (Can't find a relatable source)**
Access Type: **Reverse-shell via exploitation script**
Others access: **MySQL, Grafana, Zabbix, PostgreSQL**
OS: **Linux (docker-in)**
User: **postgres**

Price: **Set a price in PM**
Contact: **Forum PM**

Idc about politics btw

FEED MEMBERS FAQ ESCROW DEPOSIT

B

Big-Bro
Perceptible
Local User

Joined: Sep 7, 2025
Messages: 34
Reaction score: 0
Visit site

Wednesday at 5:55 PM

Доступ Finland
~$19 Million
Manufacturing
forti
domain user

REPORT

B

Big-Bro
Perceptible
Local User

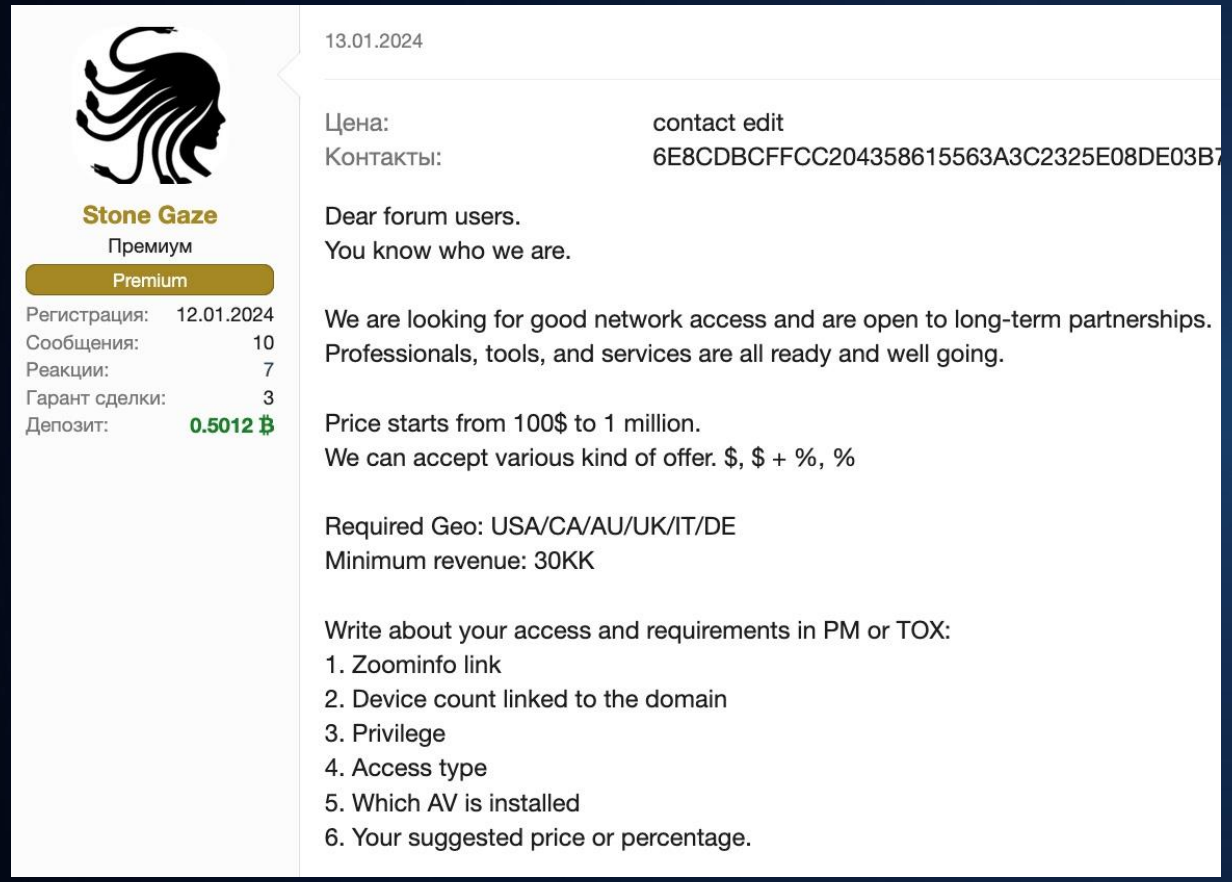
Joined: Sep 7, 2025
Messages: 34
Reaction score: 0

Wednesday at 5:56 PM

Доступ Finland
~$17 Million
Appliances
Manufacturing
forti
domain user

netnordic
THE BEST COMPANION

IAB | Scene



Stone Gaze
Премиум
Premium
Регистрация: 12.01.2024
Сообщения: 10
Реакции: 7
Гарант сделки: 3
Депозит: 0.5012 ₿

13.01.2024

Цена: contact edit
Контакты: 6E8CDBCFFCC204358615563A3C2325E08DE03B7

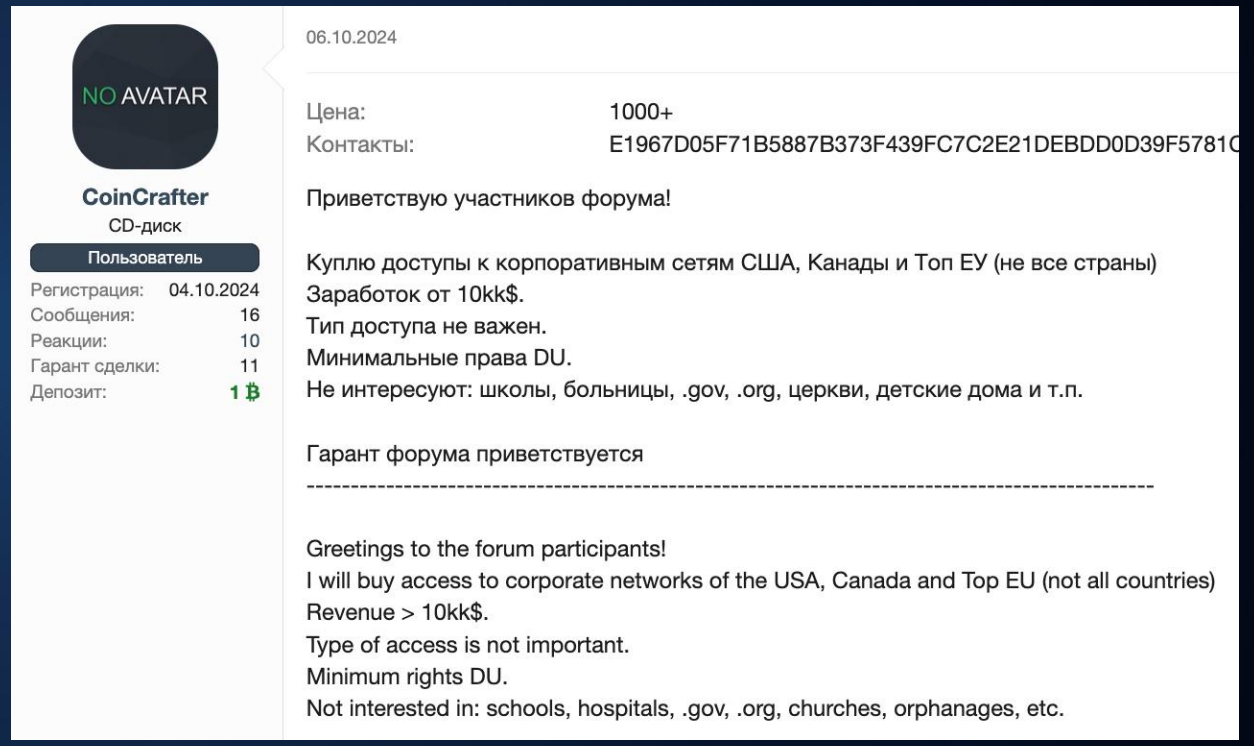
Dear forum users.
You know who we are.

We are looking for good network access and are open to long-term partnerships.
Professionals, tools, and services are all ready and well going.

Price starts from 100$ to 1 million.
We can accept various kind of offer. $, $ + %, %

Required Geo: USA/CA/AU/UK/IT/DE
Minimum revenue: 30KK

Write about your access and requirements in PM or TOX:
1. Zoominfo link
2. Device count linked to the domain
3. Privilege
4. Access type
5. Which AV is installed
6. Your suggested price or percentage.



NO AVATAR
CoinCrafter
CD-диск
Пользователь
Регистрация: 04.10.2024
Сообщения: 16
Реакции: 10
Гарант сделки: 11
Депозит: 1 ₿

06.10.2024

Цена: 1000+
Контакты: E1967D05F71B5887B373F439FC7C2E21DEBDD0D39F5781C

Приветствую участников форума!

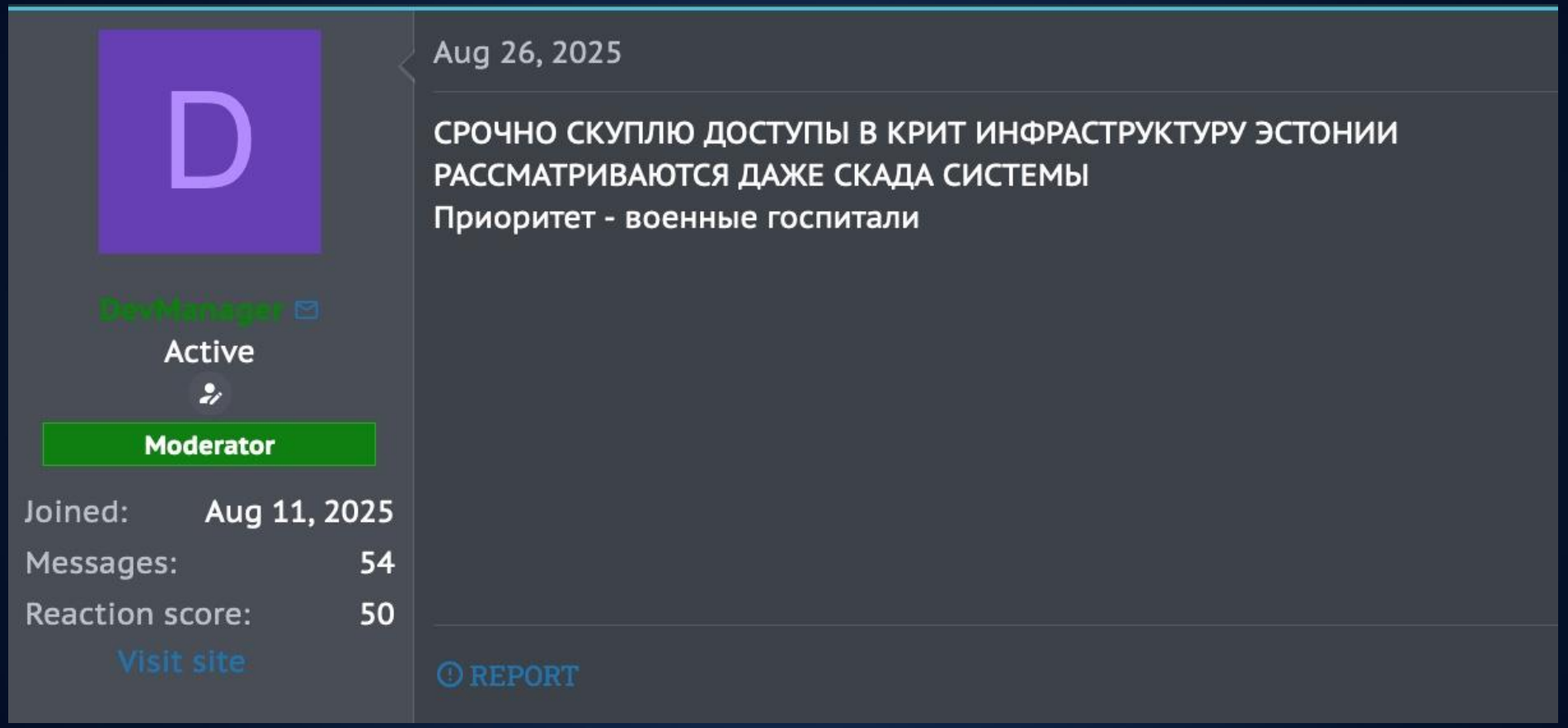
Куплю доступы к корпоративным сетям США, Канады и Топ ЕУ (не все страны)
Заработок от 10kk$.
Тип доступа не важен.
Минимальные права DU.
Не интересуют: школы, больницы, .gov, .org, церкви, детские дома и т.п.

Гарант форума приветствуется

Greetings to the forum participants!
I will buy access to corporate networks of the USA, Canada and Top EU (not all countries)
Revenue > 10kk$.
Type of access is not important.
Minimum rights DU.
Not interested in: schools, hospitals, .gov, .org, churches, orphanages, etc.

netnordic
THE BEST COMPANION

IAB | P.S.



netnordic
THE BEST COMPANION

Ransomware

Oh, what a menace

netnordic
THE BEST COMPANION

Ransomware | Headlines

Hackers Target Swedish Power Grid Operator

The hackers stole information from a file transfer solution and the country's power supply was not affected.

Hundreds of Swedish municipalities impacted by suspected ransomware attack on IT supplier

Finnish organisations targeted by Akira ransomware

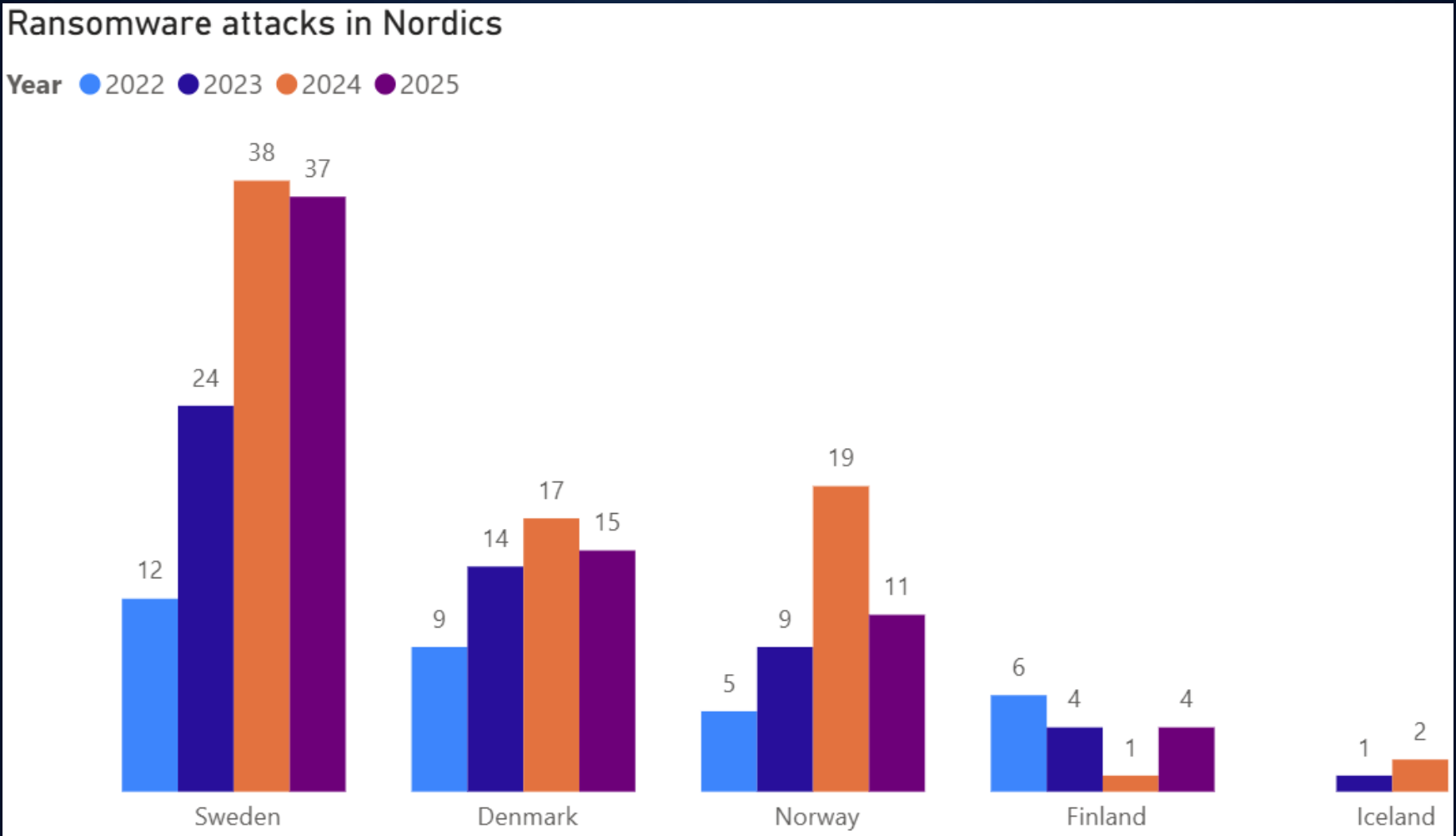
AKIRA RANSOMWARE ATTACK ON TIETOEVRY DISRUPTED THE SERVICES OF MANY SWEDISH ORGANIZATIONS

Devman Ransomware Attack On Danish Dairy Producer Naturmælk

Alles Lægehus tavse i ugevis om hackeres datatyveri fra patienter: 'Man holder det simpelthen skjult'

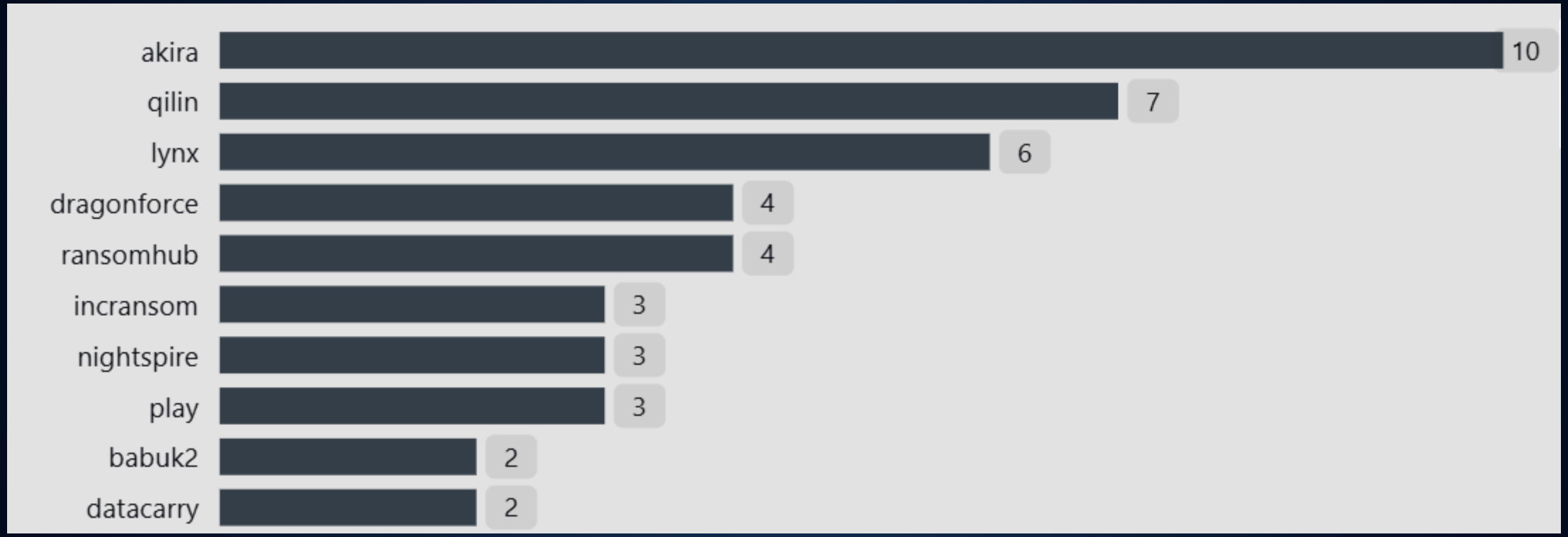
netnordic
THE BEST COMPANION

Ransomware | Nordics



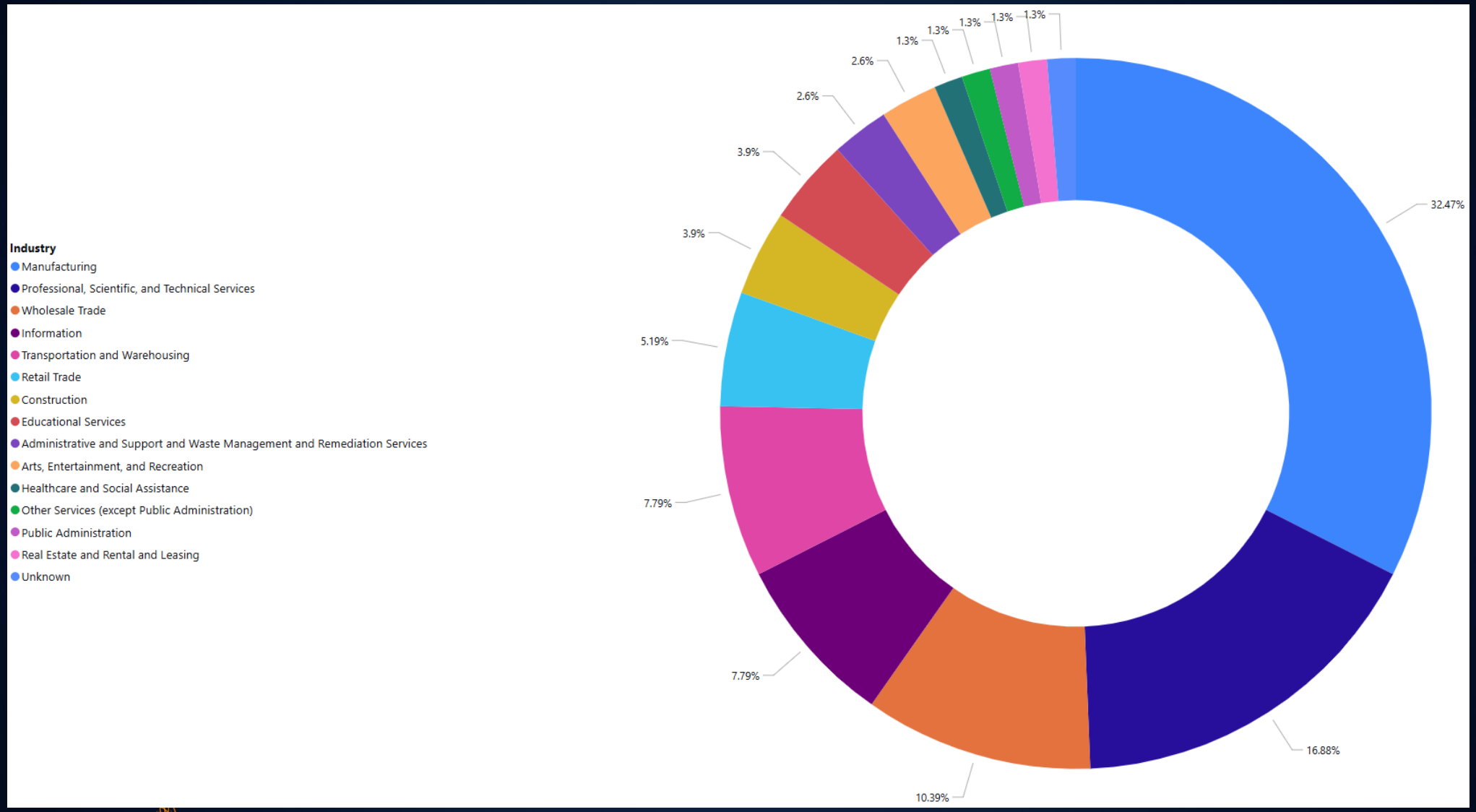
netnordic
THE BEST COMPANION

Ransomware | Nordics | Threat Actors



netnordic
THE BEST COMPANION

Ransomware | Nordics | Industry



netnordic
THE BEST COMPANION

How Can SOC Utilize All Of This?

netnordic
THE BEST COMPANION

WHO WHAT WHERE WHEN WHY HOW

Cyber Threat Intelligence

Intelligence for different audiences

- Strategic
- Tactical
- Operational
- Technical

netnordic