

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

Shamil Alifov

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

Agenda

Threat Landscape

Threat Intelligence

Information Stealing Malware

Initial Access Brokers

Ransomware

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

Threat Intelligence

Actionable Relevant Timely

Information Stealing Malware

malicious software that harvest sensitive information/data from infected victims

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

**Snowflake Attacks: Mandiant Links Data Breaches to
Infostealer Infections**

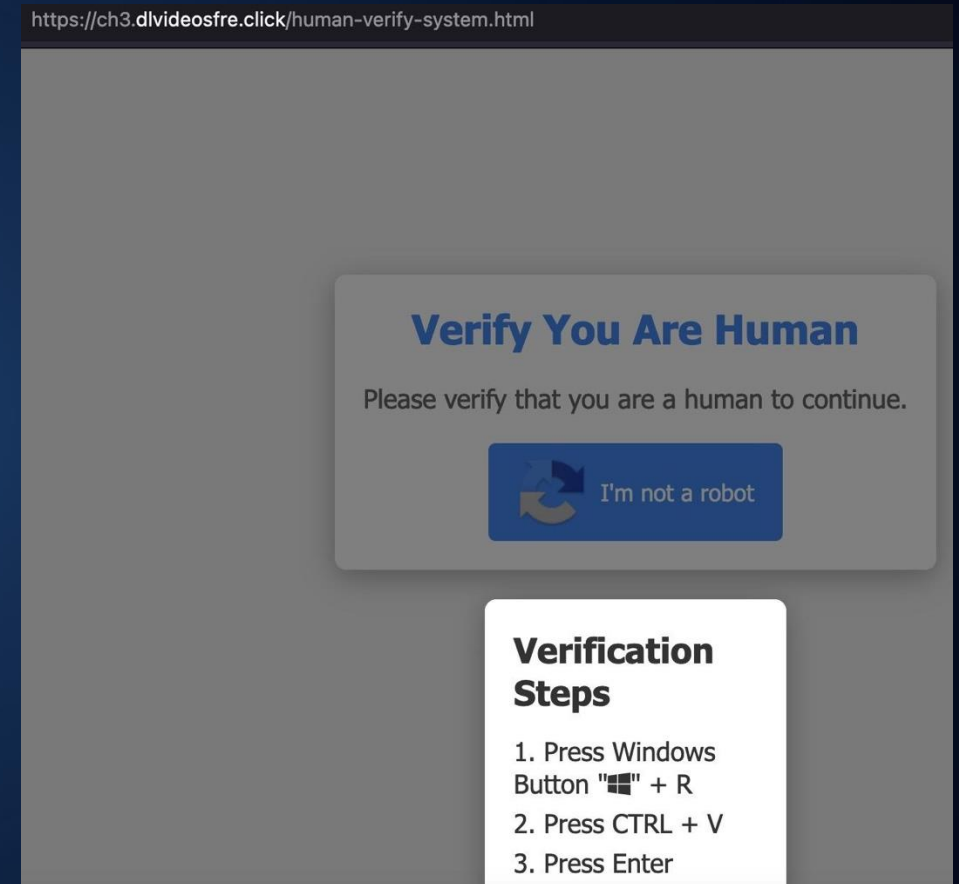
**Infostealers Cause Surge in Ransomware
Attacks, Just One in Three Recover Data**

**Gmail Passwords Confirmed Within 183 Million
Account Infostealer Leak**

Infostealers | Distribution

Various distribution channels:

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

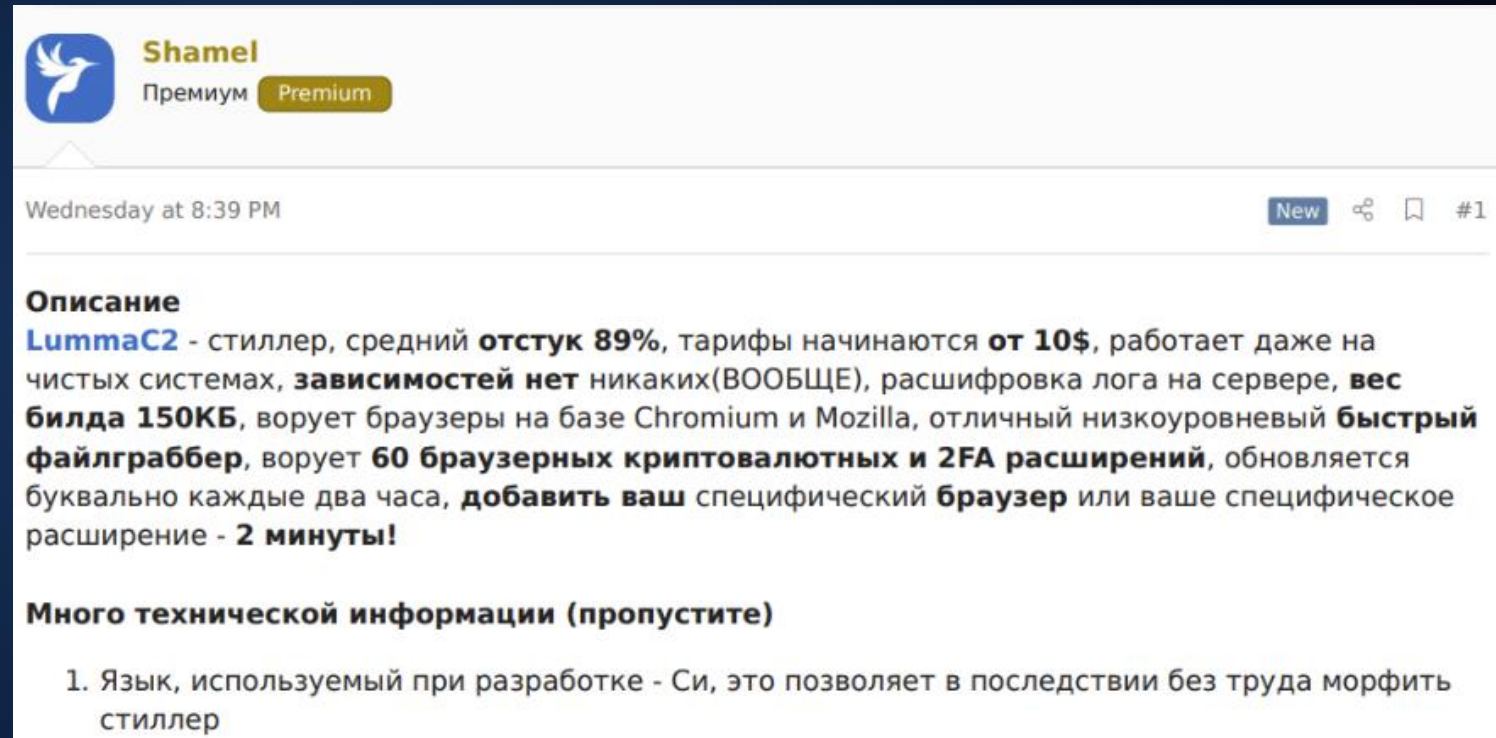


Infostealers | Variations

Malware-As-A-Service

Private Infostealers

Open-source Infostealers



The screenshot shows a Telegram chat interface. At the top, the user 'Shamel' is identified with a 'Premium' badge. The post is dated 'Wednesday at 8:39 PM'. The main text describes 'LummaC2' as a stiler with an 89% success rate, starting at \$10, and capable of stealing data from clean systems. It lists features like browser theft (Chromium, Mozilla), file grabbing, and 2FA extensions. A technical note mentions the use of the C# language for easy modification.

Shamel
Премиум Premium

Wednesday at 8:39 PM

Описание
LummaC2 - стилер, средний **отстук 89%**, тарифы начинаются **от 10\$**, работает даже на чистых системах, **зависимостей нет** никаких(ВООБЩЕ), расшифровка лога на сервере, **вес билда 150КБ**, ворует браузеры на базе Chromium и Mozilla, отличный низкоуровневый **быстрый файлграббер**, ворует **60 браузерных криптовалютных и 2FA расширений**, обновляется буквально каждые два часа, **добавить ваш** специфический **браузер** или ваше специфическое расширение - **2 минуты!**

Много технической информации (пропустите)

1. Язык, используемый при разработке - Си, это позволяет в последствии без труда морфить стилер

Infostealers | What do they steal

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

	Autofills	4.0 KiB
	Cookies	4.0 KiB
	CreditCards	4.0 KiB
	Discord	4.0 KiB
	FileGrabber	4.0 KiB
	Steam	4.0 KiB
	Wallets	4.0 KiB
	DomainDetects.txt	166 bytes
	ImportantAutofills.txt	1.2 KiB
	InstalledBrowsers.txt	968 bytes
	InstalledSoftware.txt	8.4 KiB
	Passwords.txt	11.9 KiB
	ProcessList.txt	20.9 KiB
	Screenshot.jpg	107.8 KiB
	UserInfoInformation.txt	1.2 KiB

Infostealers | What do they steal

```
system_info.txt ×
Network Info: Slurm Cloud | Private – The [REDACTED] 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
```

Infostealers | What do they steal

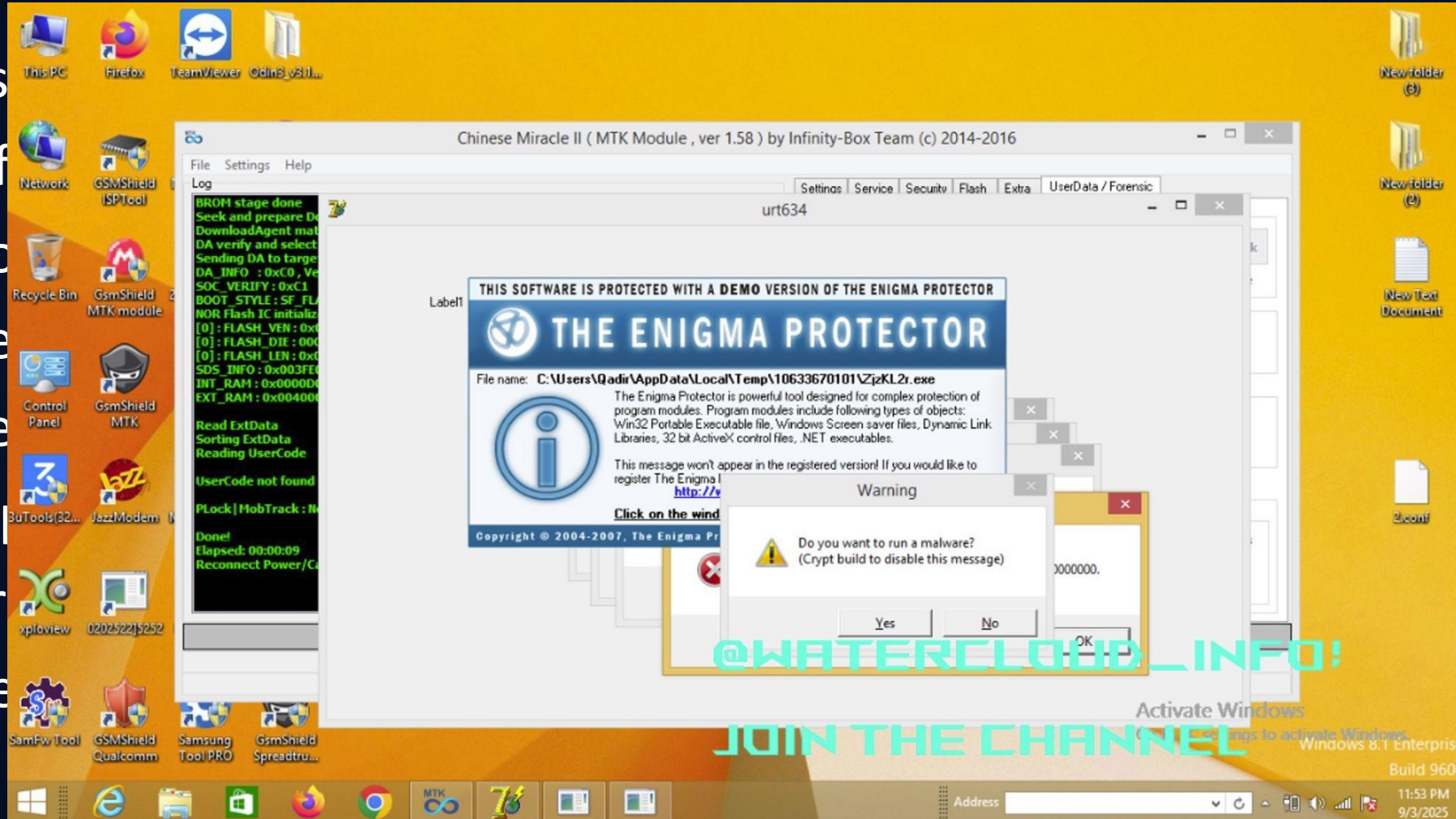
- System and User information
- Software/Running processes
- Browser data
- Credentials
- Credit cards
- Application configs
- Screenshot
- Files

```
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
=====
```

Infostealers | What do they steal

- Sys
- Sof
- Bro
- Cre
- Cre
- App
- Scr
- File



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, **Acreeed**, 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

RUSSIAN MARKET

Stealer:

All

System:

All

Country:

Sweden (20840)

Links:

accounts.google.com

State:

All

City:

All

Zip:

ISP:

ADSL Maroc teleco

Outlook:

@domain.com

Per page:

10

Vendor:

All

Search by Links

Search by Mask

Search by Cookie

Search by Email

ONLY WITH COOKIES:

☐

Price:

4\$

15\$

Search

Stealer	Country	Links	Outlook	Info	Struct	Date / Size	Vendor	Price	Action
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 Show more...	-	-	 archive.zip	2025.11.05 2.50Mb	ob####on [platinum]	\$ 10.00	Buy
stealc 	 Skåne County ISP: Telia Company AB	rekordbox.com webuyanynumberplate.com secure.darwin-insurance.com amazon.co.uk facebook.com	-	-	 archive.zip	2025.11.05 2.48Mb	ob####on [platinum]	\$ 10.00	Buy
stealc 	 Stockholm ISP: TELE2/SWIPNET	rekordbox.com webuyanynumberplate.com secure.darwin-insurance.com amazon.co.uk facebook.com	-	-	 archive.zip	2025.11.05 2.48Mb	ob####on [platinum]	\$ 10.00	Buy

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

Infostealers | Cloud of Logs

September 15

MARVEL_CLOUD (FREE LOGS) 👍

↓ **MARVEL_CLOUD (FREE LOGS)** 👍.rar
258.8 MB

*If you want to buy fresh and premium logs
MARVEL PRIME private channel. Ever day 2K -4K
Channel (2) marvel premium private Ever day 10-15K logs*

- ✓ Crypto, Wallets, Cards, Banks, Game Requests in logs
- ✓ BR, AR, EU, USA, CA, Mixed country
- ✓ Uploading 1,000-10,000 Logs per day!
- ✓ Stiller: Redline, Meta Stealer, Raccoon

Admin cloud @marvel_adminRB
marvel premium private.....

👤 PRICE LIST 👤

- 💎 week - \$150 👉
- 💎 2 WEEK - \$300 👉👉
- 💎 month - \$450 👉👉👉
- 💎 3 month - \$900 👉👉👉👉
- 💎 Lifetime - \$4200 👉👉👉👉👉

MARVEL PRIME private.....

👤 PRICE LIST 👤

- 💎 week - \$90 👉
- 💎 2 WEEK - \$150 👉👉
- 💎 month - \$230 👉👉👉
- 💎 3 month - \$600 👉👉👉👉
- 💎 Lifetime - \$2500 👉👉👉👉👉

Payment methods
■ BTC/USDT TRC20

<https://t.me/marvelcloudRB> 664 00:25

Moon Cloud | Free Logs 11:14AM
FREE YT&TEAM LOGS 19.01.2024.rar, Password: @. . . 136

Free Logs Cloud 3:27AM
1.19 - @LOGS_CENTER.rar, Password: https://t.me... 57

Klaus Cloud [Public] 7:35PM
@klaus_cloud_public 5292logs.zip, 💎 210.000 logs per ... 13

Pixel Cloud | Channel 6:13PM
UPDATE PRIVATE CLOUD | Fresh & Untouched St... 8

Tichan Cloud | Free Logs Thu
UPDATE PRIVATE CLOUD Price: ● 2 week access ... 5

BHF Cloud | FREE LOGS Thu
DING-DONG 🏰🏰 NEW PUBLICATION OF LOGS ... 12

DNFTM | Cloud Thu
----- Гуды админок сайтов Умеете лить трафи... 23

Infostealers | Quiz time!



hackerGPT
data hunter

Premium

Регистрация: 03.01.2024
Сообщения: 16
Реакции: 2
Депозит: 1 ₿

Суббота в 01:28

Каждый доступ рассматривается индивидуально, цена от 100\$ до 5к\$.

Код:

- /Citrix/
- /vpn/index.html
- /vpn/tmindex.html
- /remote/login
- /Remote/logon.aspx
- /+CSCOE+/
- /dana/

Initial Access Brokers

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

IAB | Attack Vectors

Exploitation of Vulnerabilities

Brute-force and Password Spraying Attacks

Social Engineering

Credential-based Attacks

IAB | Attack Vectors



hackerGPT
data hunter

Premium

Регистрация: 03.01.2024
Сообщения: 16
Реакции: 2
Депозит: 1 ₿

Суббота в 01:28

Каждый доступ рассматривается индивидуально, цена от 100\$ до 5к\$.

Код:

- /Citrix/
- /vpn/index.html
- /vpn/tmindex.html
- /remote/login
- /Remote/logon.aspx
- /+CSCOE+/
- /dana/

IAB | Access Types

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



DarkFulu
floppy-диск

Пользователь

Регистрация: 10.07.2025
Сообщения: 2
Реакции: 0



12.08.2025

Цена: 7000
Контакты: 7D8951F4BD61E7907331

Pharmaceuticals / Biotech Manufacturer
Country: UK
Revenue: \$3.3 billion USD
Access: VPN-Credentials or Adaptix-Beacon
Privilege: Domain User or Domain Admin
Price: Domain User: \$4,000 / **Domain Admin: \$7,000**

IAB | Scene

BREACHSTARS

Databases Upgrade Credits Rules Changelog

Search...

Sellers Place

A place for sellers to post various products they have.

Submit topic

[Access] USA Medical Device Manufacturing & Tracking

By [miyako](#), 24.09.2025, 18:14

Last post by [miyako](#)

29.09.2025, 15:57



[Access] USA Managed Services Provider - Private Cloud Hosting & Network Engineering

By [miyako](#), 24.09.2025, 17:56

Last post by [miyako](#)

29.09.2025, 15:57



[Access] Worldwide FinTech - Global Card & Payment Solutions

By [miyako](#), 24.09.2025, 18:05

Last post by [miyako](#)

29.09.2025, 15:57



[Access] US Navy / USAF / USDoD Engineering Contractor

By [miyako](#), 24.09.2025, 18:07

Last post by [miyako](#)

29.09.2025, 15:57



[Access] AUS - GPS Tracking, Asset Tracking, Fleet Management

By [miyako](#), 24.09.2025, 18:11

Last post by [miyako](#)

29.09.2025, 15:57



[Access] Canadian Insurance Credentialing Agency

By [miyako](#), 24.09.2025, 18:00

Last post by [miyako](#)

29.09.2025, 15:56



SELLING [RCE] Chinese Cloud Provider Access
👤 [Psych1c](#) ⌚ 23-09-25, 04:25 AM

✓ VERIFIED China private NAS Server Access – 4.7 TB
👑 [Kazu](#) ⌚ 22-09-25, 08:57 AM

SELLING [RCE] Taiwan Telecom Access
👤 [Psych1c](#) ⌚ 21-09-25, 04:47 AM

SELLING [FIREWALL ACCESS] Saudi Arabian Cloud Provider
👑 [NetworkBrokers](#) ⌚ 18-09-25, 02:57 AM

SELLING Access to Live Casino Game Provider
👑 [888](#) ⌚ 17-09-25, 12:38 AM

SELLING Bloxham Parish Council GOV UK Access
👑 [krekti](#) ⌚ 16-09-25, 10:10 PM

SELLING [RCE] 2x Asian Telecom Access
👤 [Psych1c](#) ⌚ 16-09-25, 07:23 AM

Deleted Thread

SELLING [BULK] Selling 2 BIG Telecoms Asia
👑 [NetworkBrokers](#) ⌚ 15-09-25, 02:35 AM

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 reliable source)
Employees: ? (Can't find a reliable 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



Big-Bro 
Perceptible

Local User

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

[Visit site](#)

Wednesday at 5:55 PM

Достын Finland
~\$19 Million
Manufacturing
forti
domain user

[REPORT](#)



Big-Bro 
Perceptible

Local User

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

[Visit site](#)

Wednesday at 5:56 PM

Достын Finland
~\$17 Million
Appliances
Manufacturing
forti
domain user

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.



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.

IAB | P.S.



DevManager 

Active



Moderator

Joined: Aug 11, 2025

Messages: 54

Reaction score: 50

[Visit site](#)

Aug 26, 2025

**СРОЧНО СКУПЛЮ ДОСТУПЫ В КРИТ ИНФРАСТРУКТУРУ ЭСТОНИИ
РАССМАТРИВАЮТСЯ ДАЖЕ СКАДА СИСТЕМЫ**

Приоритет - военные госпитали

 [REPORT](#)

Ransomware

Oh, what a menace

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

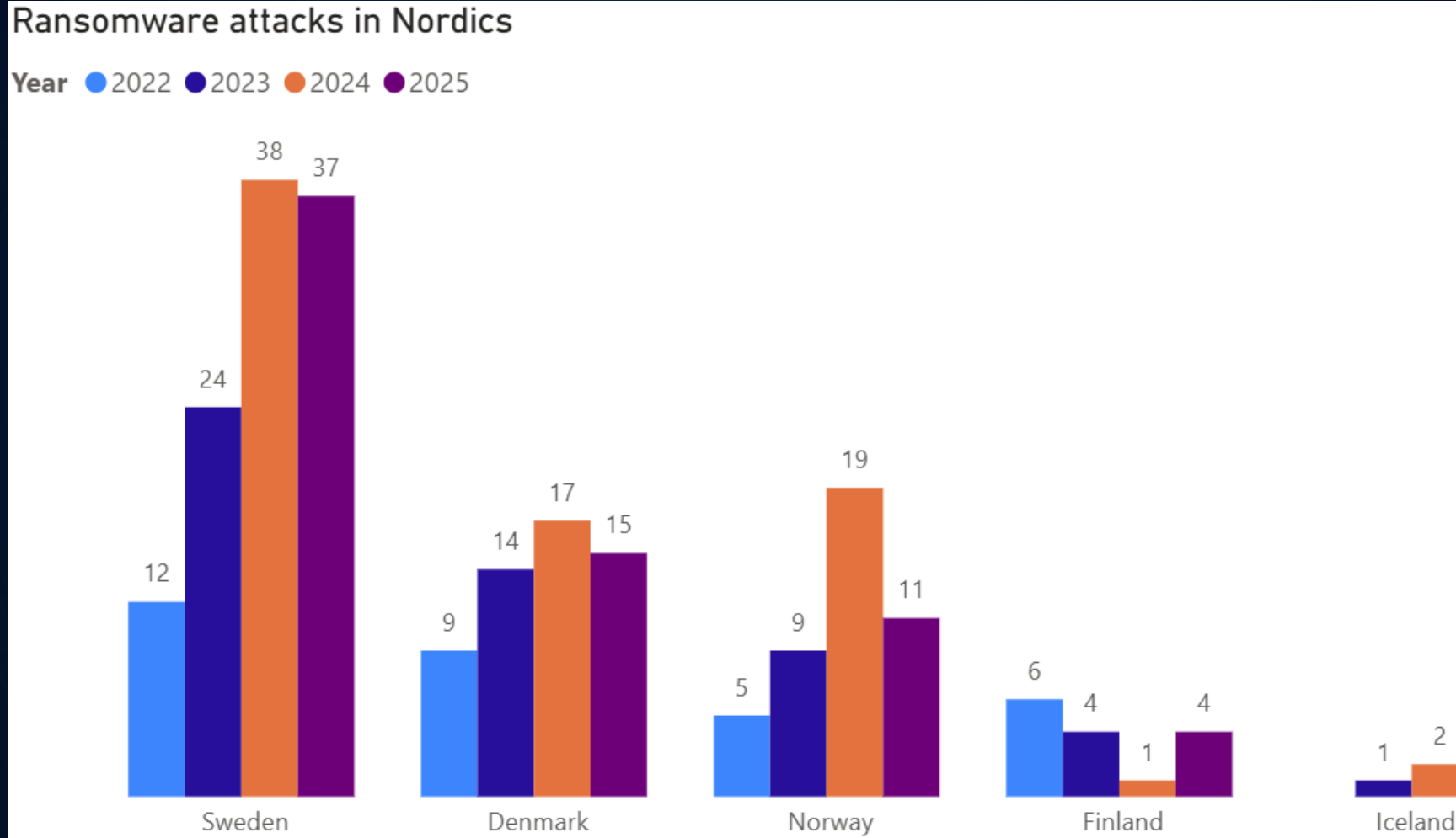
Finnish organisations targeted by Akira ransomware

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

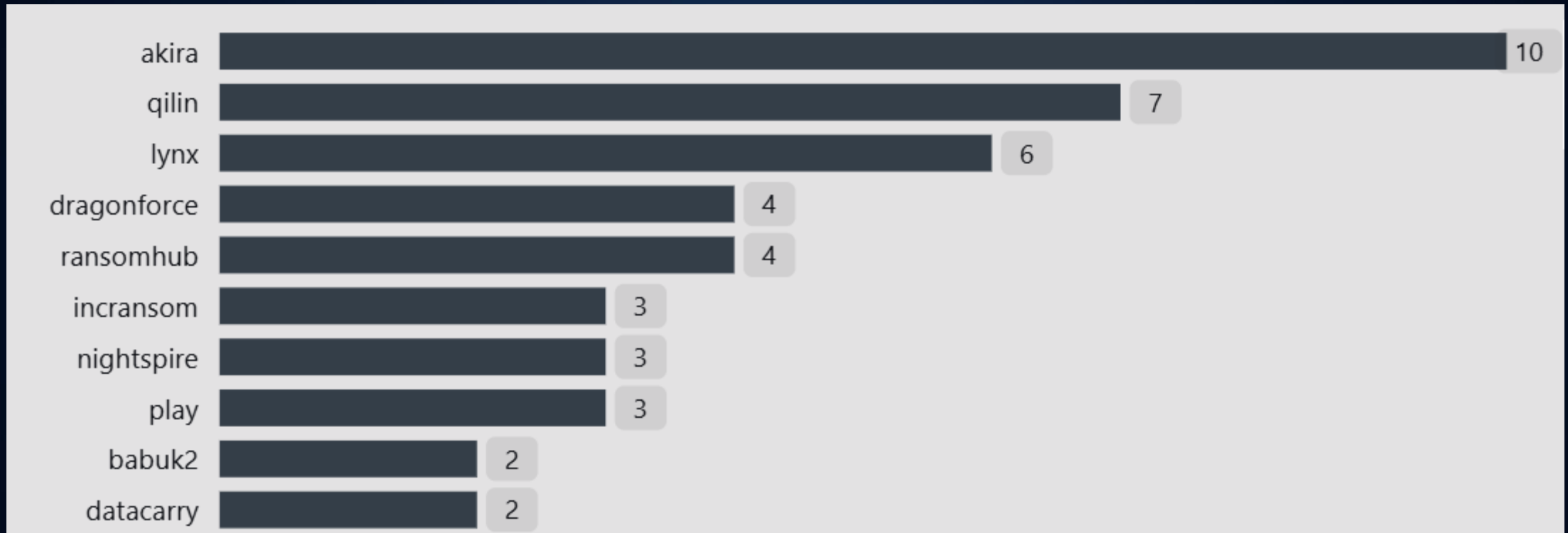
Devman Ransomware Attack On Danish Dairy Producer Naturmælk

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

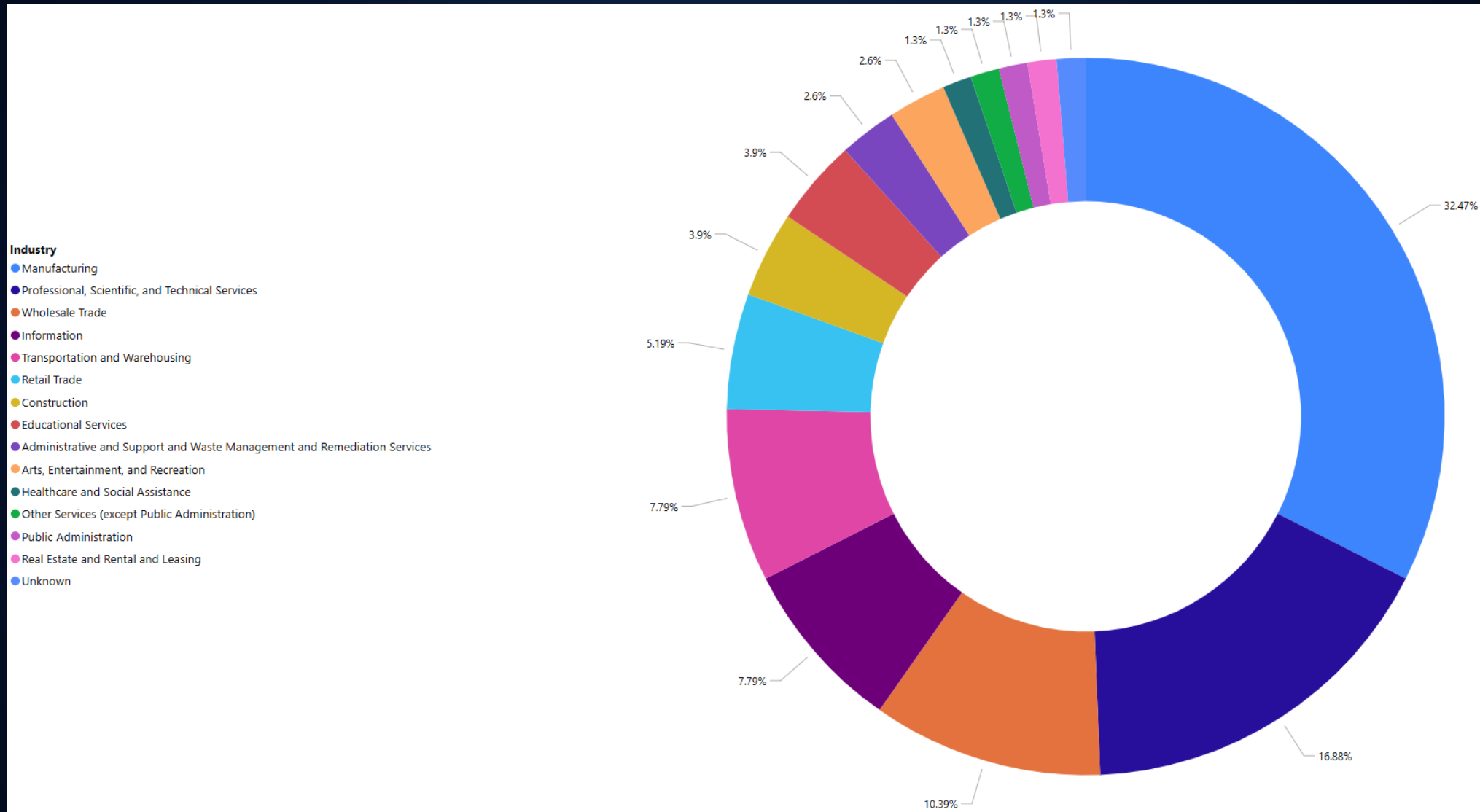
Ransomware | Nordics



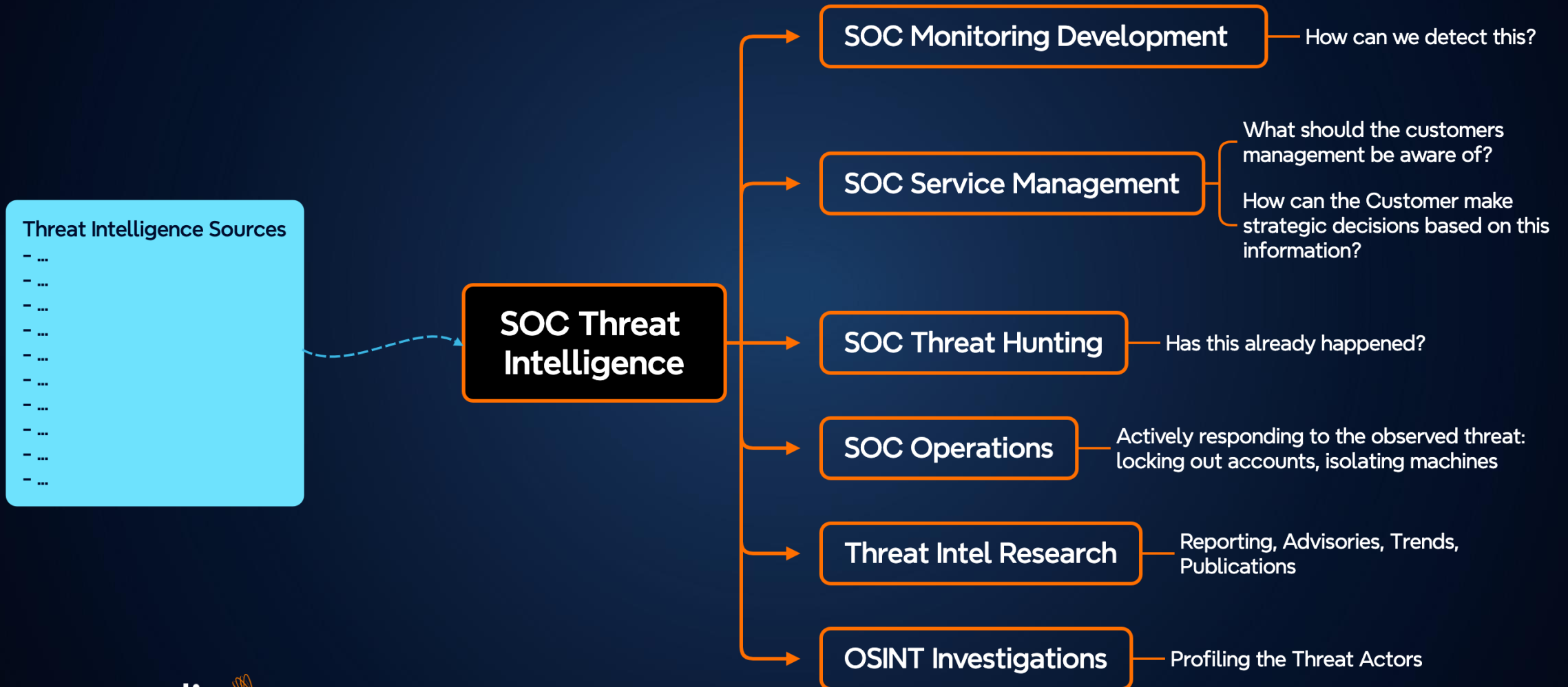
Ransomware | Nordics | Threat Actors



Ransomware | Nordics | Industry



How Can SOC Utilize All Of This?



WHO WHAT WHERE WHEN WHY HOW

Cyber Threat Intelligence

Intelligence for different audiences

Strategic

Tactical

Operational

Technical