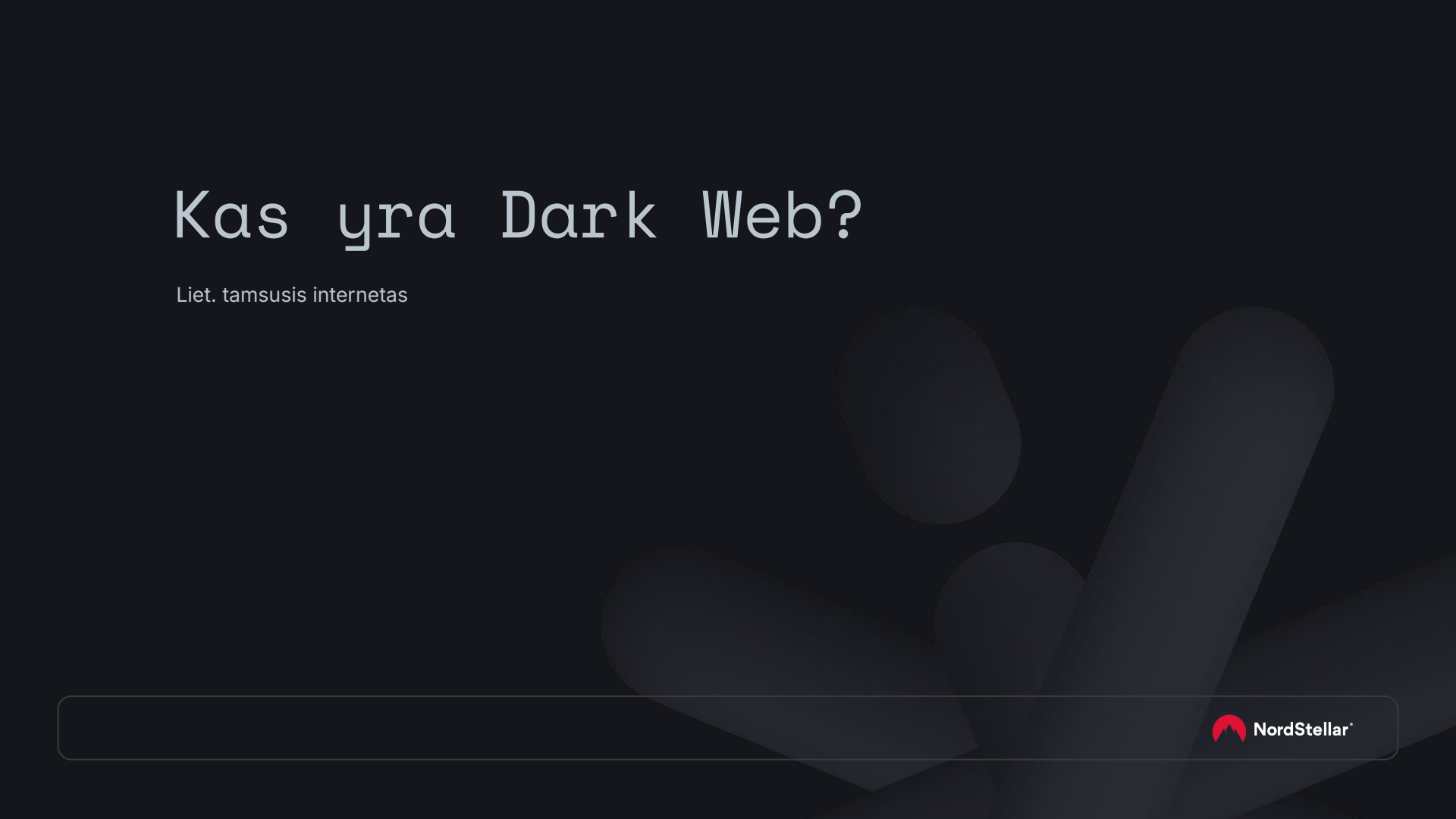

# NORDSTELLAR – PROAKTYVUS GRĖSMIŲ VALDYMAS

**Laurynas Janušonis,**
Nord Security verslo vystymo vadovas

# Kas yra Dark Web?

Liet. tamsusis internetas



NordStellar

# Ar jūsų verslo informacija gali atsidurti dark web'e?

Ticketmaster Hacked: Customer Data Stolen and Shopped on Dark Web by 'Criminal Threat Actor,' Live Nation Discloses

AT&T data breach: Millions of customers caught up in major dark web leak

With hundreds of Snowflake credentials published on the dark web, it's time for enterprises to get MFA in order

User data stolen from genetic testing giant 23andMe is now for sale on the dark web

Data from 3m Avast users on dark web

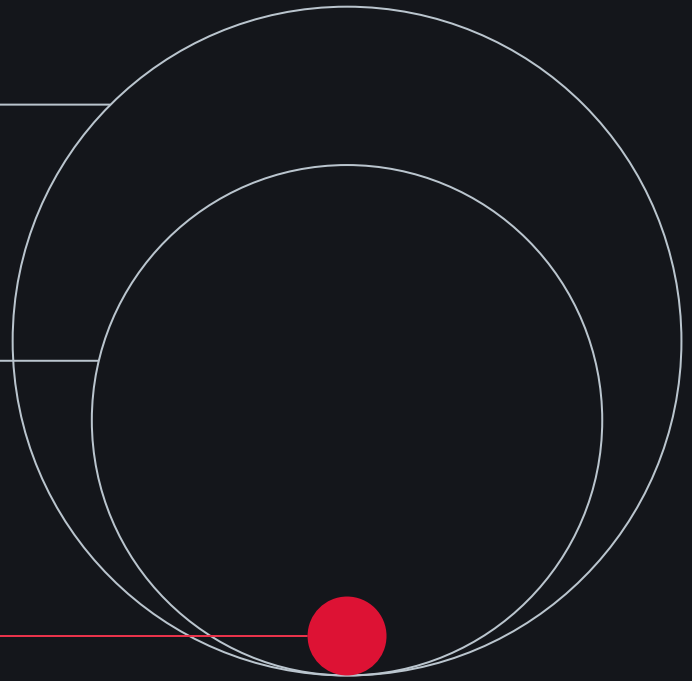
Hospital system to pay $65 million for dark web data leak,

# Kas yra Dark Web?

**10%**
Surface web

**90%**
Deep web

**<1% of deep web**
Dark web



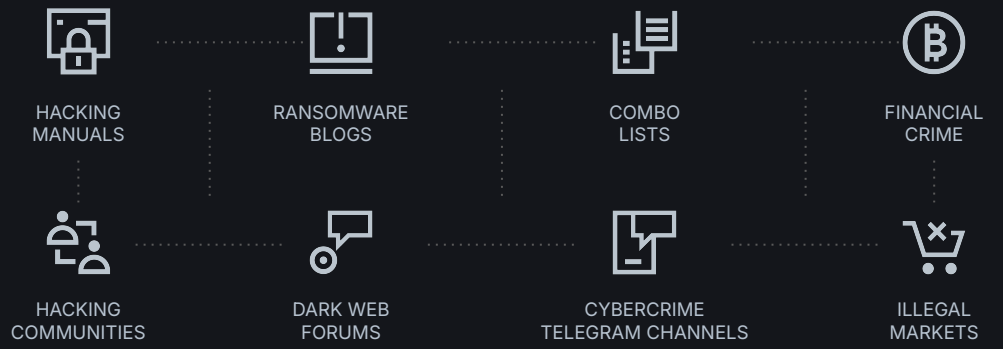
## Ką galima rasti Dark Web'e?

- Tor network
- Dark web marketplaces
- Forums and social networks
- Whistleblower platforms
- Cryptocurrency exchanges and wallets

# NordStellar turi prieigą prie vienos didžiausios pavogtų duomenų bazės

| 36k+ | 60m+ | 90bn+ | 90bn+ | 80bn+ | 77bn+ |
|---|---|---|---|---|---|
| Nutekėjusių duomenų bazių | Malware infostealers | Nutekėjusių prisijungimų | Slaptažodžių | El. paštų | Cookies |

**Deep & Dark Web Underground** → **Nutekėjusi informacija**



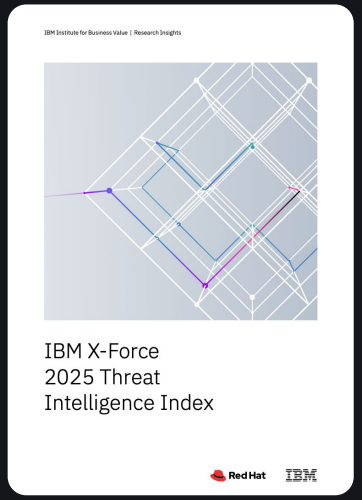

- El. paštai
- Slaptažodžiai
- Sesijų slapukai
- Kreditinės kortelės
- Tel. Nrs
- Tapatybės ID
- Failai
- Kita

# Karščiausia tema dark web’e: Infostealer malware

Liet. informaciją vagianti kenkėjiška programa

NordStellar

# Infostealer Malware: augimas ir naminių įrenginių pažeidžiamumas




84% malware infostealer užsikrėtimų augimas


Viena didžiausia šiuolaikinio kibernetinio saugumo problema

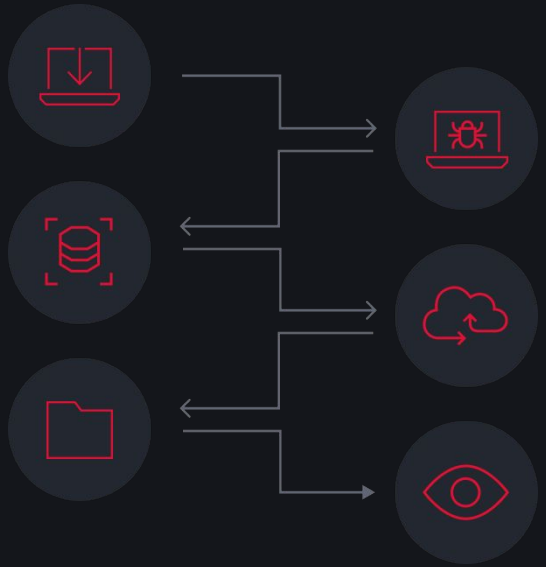

Nutekėjusios informacijos augimas dėl užsikrėtimų naminiuose įrenginiuose

# Infostealer malware: kenkėjiška programa apie kurią (ne) girdėjote

Vartotojas atsisiunčia nulaužtą programinę įrangą

Infostealer pavogia:
- Prisijungimo duomenis
- Naršyklės duomenis
- Failus...

Atskiri incidentai sujungiami į paketus



Užkrėsta programa paleidžiama vartotojo kompiuteryje

Duomenys išsiunčiami į C2 infrastruktūrą

Incidentų failai platinami deep ir dark web'e

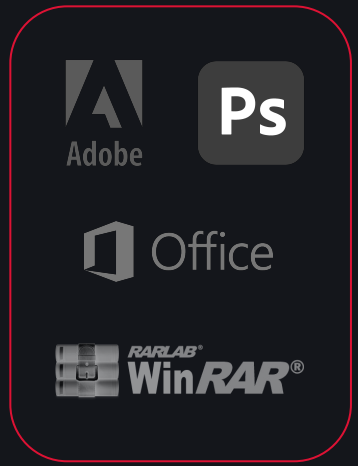
Admin teisės NEREIKALINGOS ir programa nepastovi

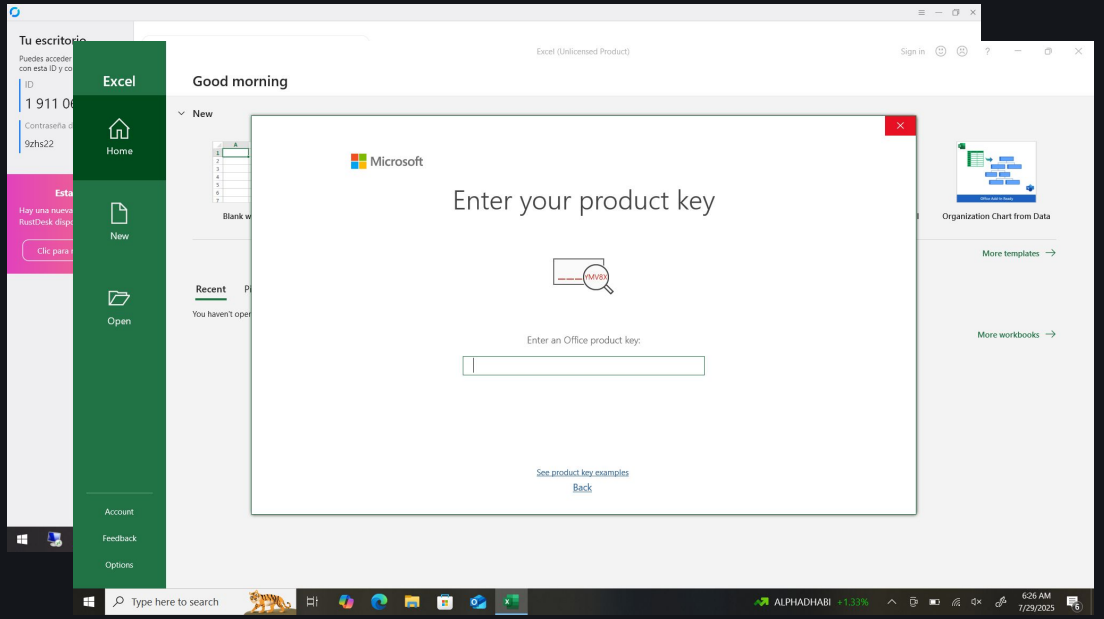
# Infostealer malware pavogiami duomenys

- *** Credentials (emails, passwords, URLs)
- Cookies and session tokens
- Credit cards and crypto wallets
- Screenshots and webcam pictures
- Autofills and Personal Identifiable Information (PII)
- Files

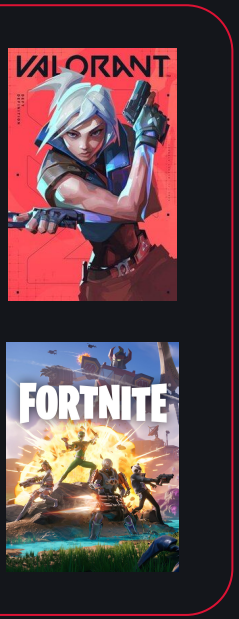
They don’t just steal passwords—they steal access

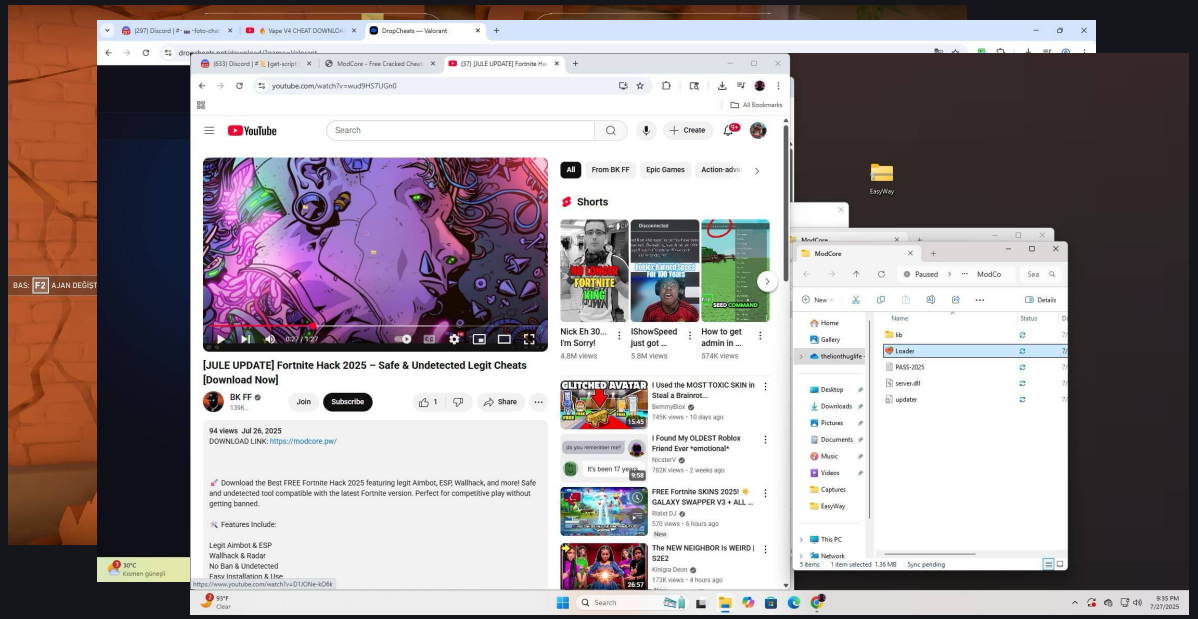
# Kaip užsikrečiama infostealer malware: nulaužta programinė įranga



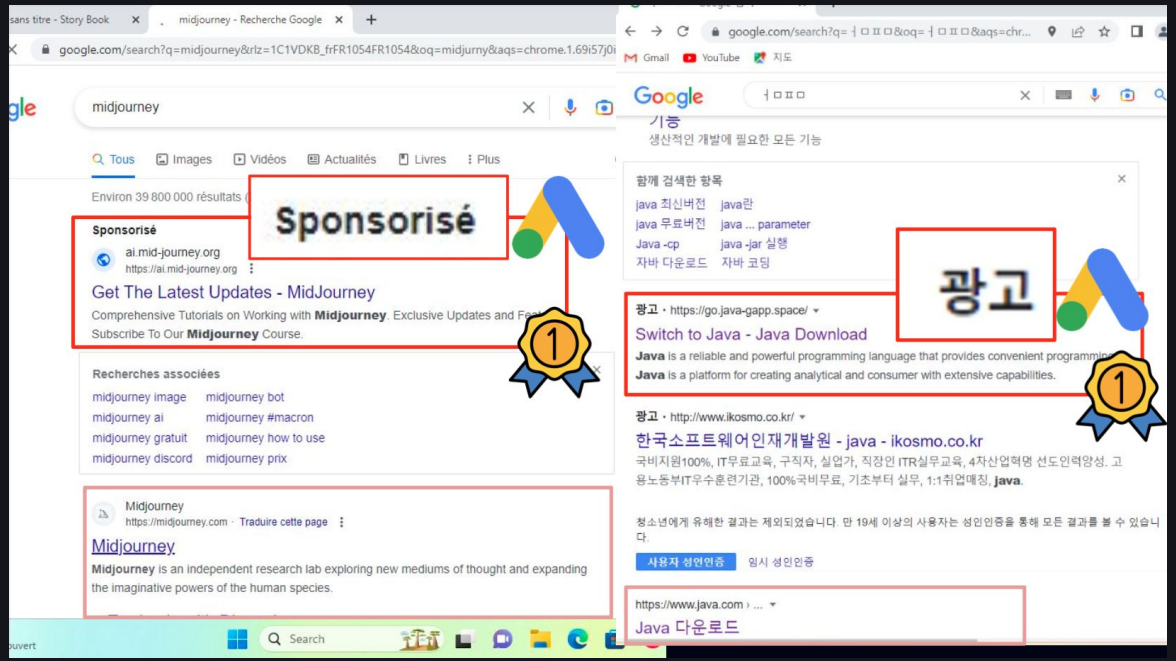



# Kaip užsikrečiama infostealer malware: žaidimų “cheats & mods”



# Kaip užsikrečiama infostealer malware: Google Ads



# Infostealers – statistika iš 2024

## Populiariausios duomenų kategorijos

| | |
|---|---|
| Cookies | 51,058,866,236 |
| Autofills | 5,939,861,393 |
| Credentials | 1,537,226,295 |
| Passwords | 346,453,140 |
| Emails | 216,519,234 |
| Grabbed Files | 66,888,742 |
| Credit Cards | 1,448,471 |

## Populiariausi prisijungimų domenai

| Rank | Credential domain | Count |
|---|---|---|
| 1 | Facebook | 13,695,693 |
| 2 | Microsoft | 11,763,108 |
| 3 | Google | 9,229,057 |
| 4 | Instagram | 5,658,990 |
| 5 | Netflix | 5,203,901 |

# NordStellar - Threat exposure management platform

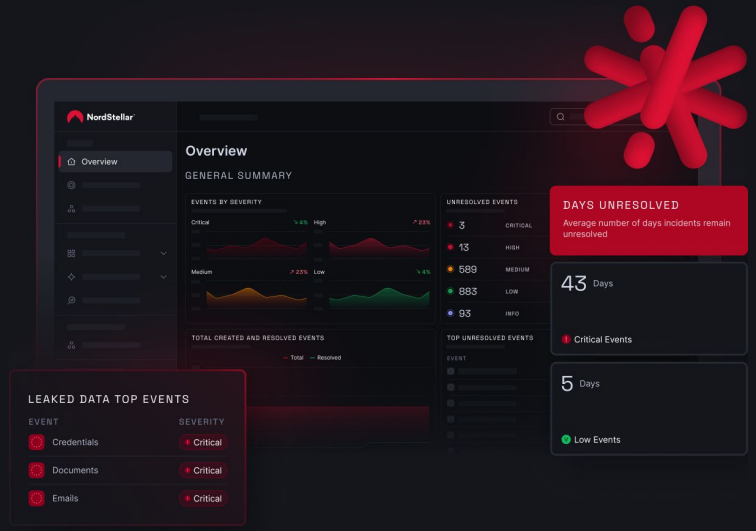
Liet. Kibernetinių grėsmių valdymo platforma

NordStellar

# Kibernetinių grėsmių valdymo platforma

Aptikite ir užbėkite už akių kibernetinėms grėsmėms, kurios kelia pavojų jūsų įmonei.

Su NordStellar pagalba galite realiu laiku stebėti grėsmes, kylančias dark web’e ir apsaugoti darbuotojus, vartotojus, prekės ženklą bei infrastruktūrą.




NordStellar

# Kaip NordStellar padeda kibernetinio saugumo ir IT komandoms

Leaked data management

Darbuotojų ir vartotojų apsauga

Dark web monitoring

Įmonės ir prekės ženklo apsauga

Attack surface management

Infrastruktūros apsauga

Cybersquatting detection

Reputacijos apsauga

NordStellar

# Live DEMO

NordStellar