SECURITY DAYS

OD LOCKBITU K RANSOMHUBU

Dramatické zmeny vo svete ransomware za posledný rok

Tomáš Zvara
Malware researcher

Digital Security
Progress. Protected.

&

SME KONFERENCIE

Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť

Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť


LO
3.0

Dopad policajných operácií

- Operátor zľahčuje dopady
- Strata dôvery partnerov
- Ledva prežije
- Pokúša sa o návrat s verziou 4.0

- Operátor zľahčuje dopady
- Strata dôvery partnerov
- Hádže uterák do ringu
- Rebranding

Globálne zmeny v oblasti ransomware - 2024

+15%

Zverejnených útokov

5100

-35%

Celkový objem platieb

$813 M

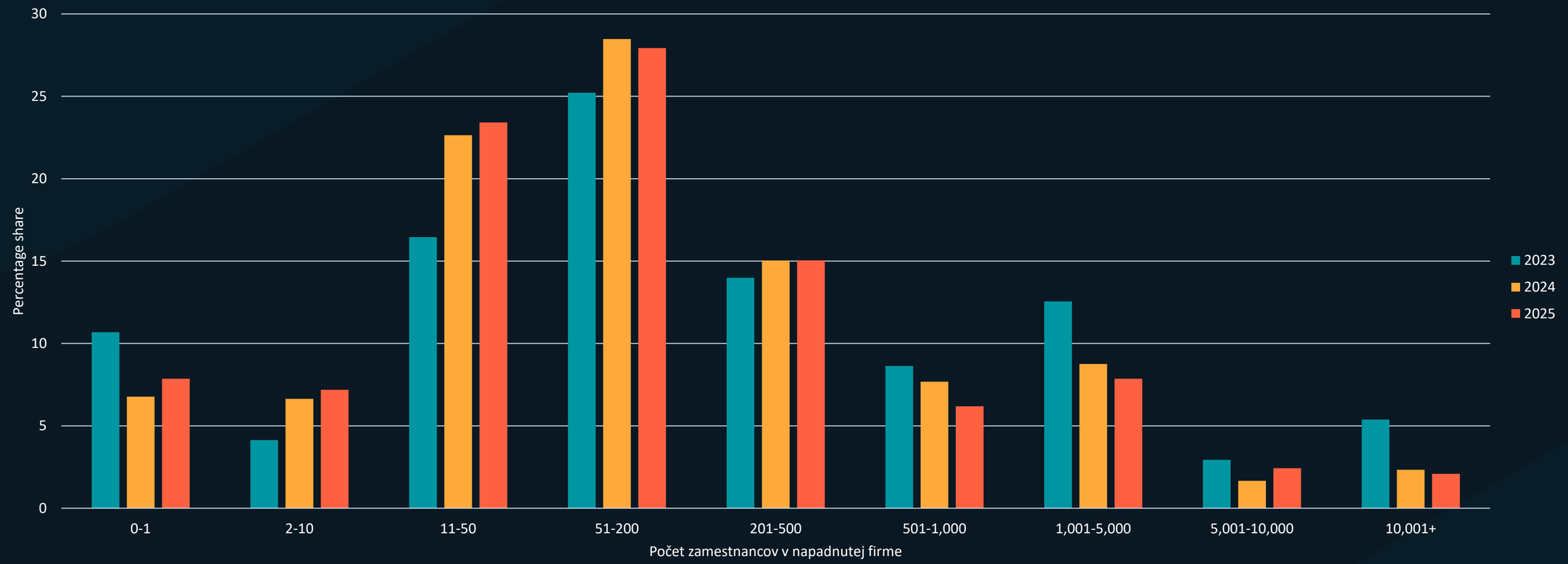
+43%

Nárast počtu operátorov

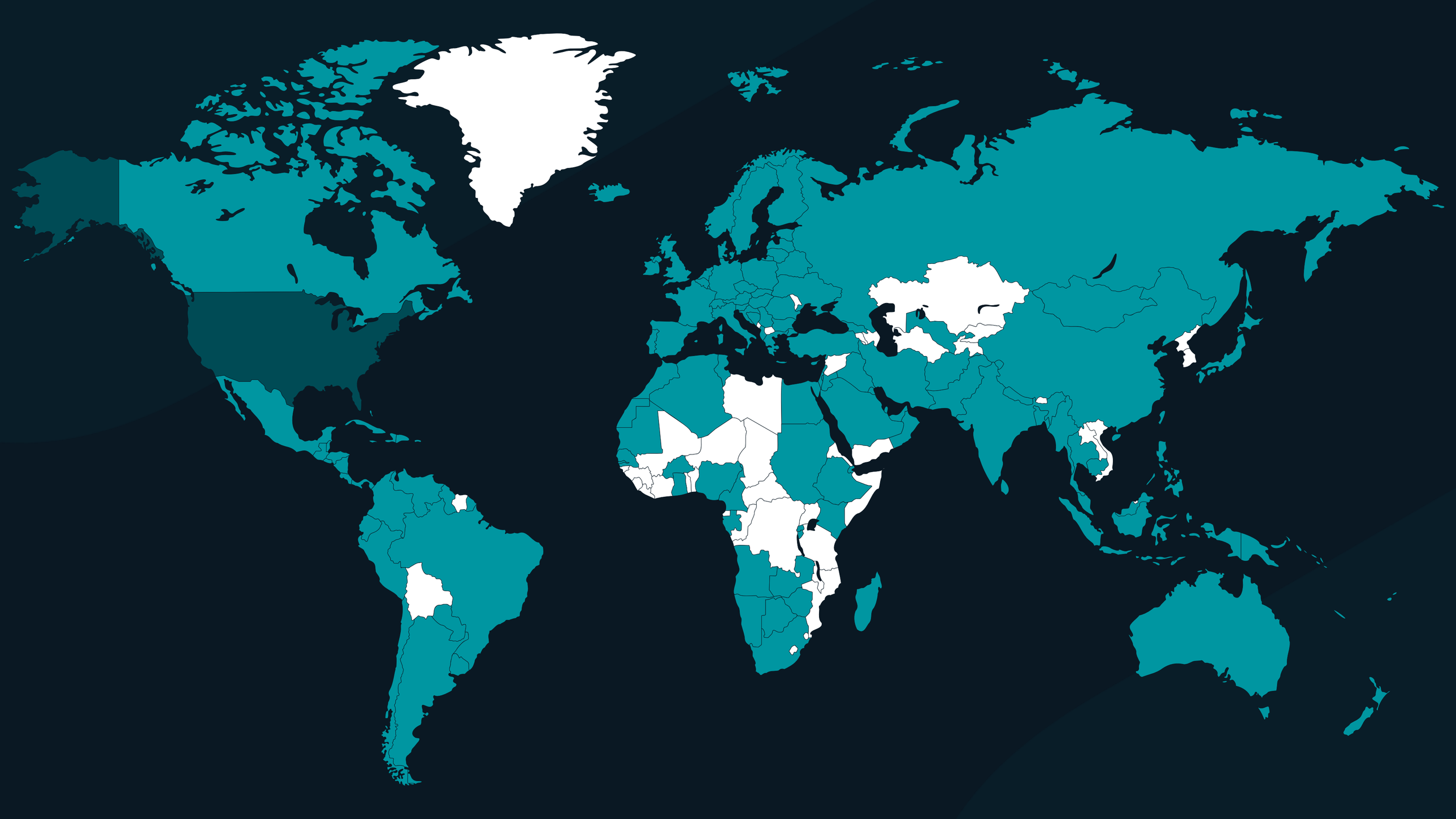
96

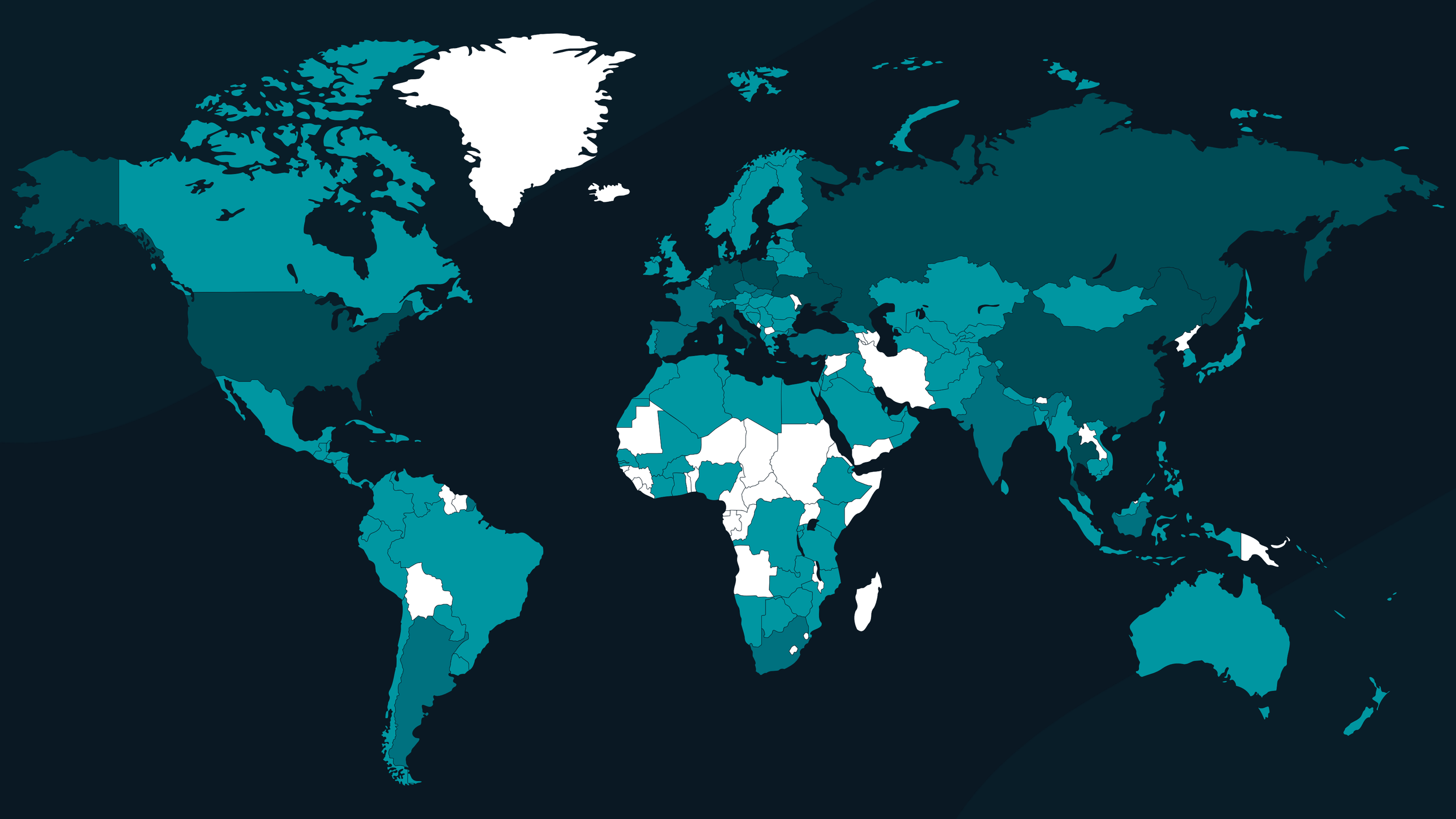

RansomHub
9D 5h 53m 11s
Visits: 3680
Data Size: 142GB
Last View: 01-21 06:04:18
2025-01-16 04:49:35
3D 5h 53m 11s
Visits: 3814
Data Size: 130GB
Last View: 01-21 06:05:22
2025-01-14 11:15:09
3D 5h 53m 11s
Visits: 4444
Data Size: 230gb
Last View: 01-21 06:06:20
2024-12-09 12:16:02
9h 53m 11s
Visits: 8390
Data Size: 2TB
Last View: 01-21 06:04:43
2025-01-01 06:31:22
6D 5h 53m 11s
Visits: 15101
Data Size: 45Gb
Last View: 01-21 06:05:02
2024-12-18 01:50:59
PUBLISHED
Visits: 5852
Data Size: 40 GB
Last View: 01-21 06:06:01
2025-01-08 14:54:02
PUBLISHED
Visits: 5621
Work with us: targets' providers, software engineers, pentesters, journalists.
Tox: A8AD0FD4C931CDAA1408D5A60CBF38CEDF46B41E19A8A55E4EF1F1848AF3416AE52D278D37DF
Email: deepmind@onionmail.org
Read more →
INC RANSOM
Leaks
Submit a feedback
Twitter
WWW Mirror
Blog / Leak
Leak
ANNOUNCEMENT
11.05.2024
6728
ANNOUNCEMENT
01.05.2024
PUBLISHED
PUBLISHED
AKIRA
[AKIRA]
Well, you are here. It means that you're suffering from cyber incident right now. Think of o
ns as an unscheduled forced audit of your network for vulnerabilities. Keep in mind that the
fair price to make it all go away.
Do not rush to assess what is happening - we did it to you. The best thing you can do is to f
ur instructions to get back to your daily routine, by cooperating with us you will minimize th
e that might be done.
hose who choose different path will be shamed here publicly. The functionality of this blog is
mely simple - enter the desired command in the input line and enjoy the juiciest information t
rporations around the world wanted to stay confidential.
emember. You are unable to recover without our help. Your data is already gone and cannot be tr
the place of final storage nor deleted by anyone besides us.
est@akira:~$ help
st of all commands:
eaks – hacked companies
ews – news about upcoming data releases
ontact – send us a message
Contact: (qtox.github.io) Tox id:19A549A57160F384CF4E36EE1A24747ED99C623C48EA545F343296FB7092795D00875C94
Helldown Leaks
Companies
News
Companies
All 251
Stocks 22
Unicorn 28
US 128
Europe 58
Asia 24
Exfiltrated 239
Encrypted
Latvia
Revenue $150M
Employees 1,000
Disclosures 1/1
Latvia
Revenue $150M
Employees 1,000
Disclosures 1/1
United Kingdom
Revenue $250M
Employees 500
Disclosures 7/7
Wall of Shame
24738
Full database
2025-02-12 06:27:01
24665
full leak
2025-02-11 06:40:42
36187
Full leak
2025-01-30 19:00:28
36218
Full leak
2025-01-30 15:35:56
38266
full leak
2025-01-29 00:22:27
37919
full leak
2025-01-28 23:12:35
HELLCAT
Contact us
PUBLISHED
PUBLISHED
07 Nov, 2024, 10:12 UTC
PLAY NEWS
CONTACT
Play ransomware HAS NEVER PROVIDED AND DOES NOT PROVIDE THE RaaS, read the FAQ page.
If the company has not contacted within 72 hours after the attack, it is added to the portal.
New main links:
ipi4tiumgzjsym6pyuzrfqrtwskokxokqannmd6sa24shvr7x5kxdvqd.onion
j75o7xvvsm4lpsjhkjvb4wl2q6ajegvabe6oswthuaubbykk4xkzgpid.onion
United States
views: 364
added: 2025-02-26
Canada
views: 367
added: 2025-02-26
publication date: 2025-03-02
2 DAYS BEFORE PUBLICATION
United States
views: 383
added: 2025-02-26
publication date: 2025-03-02

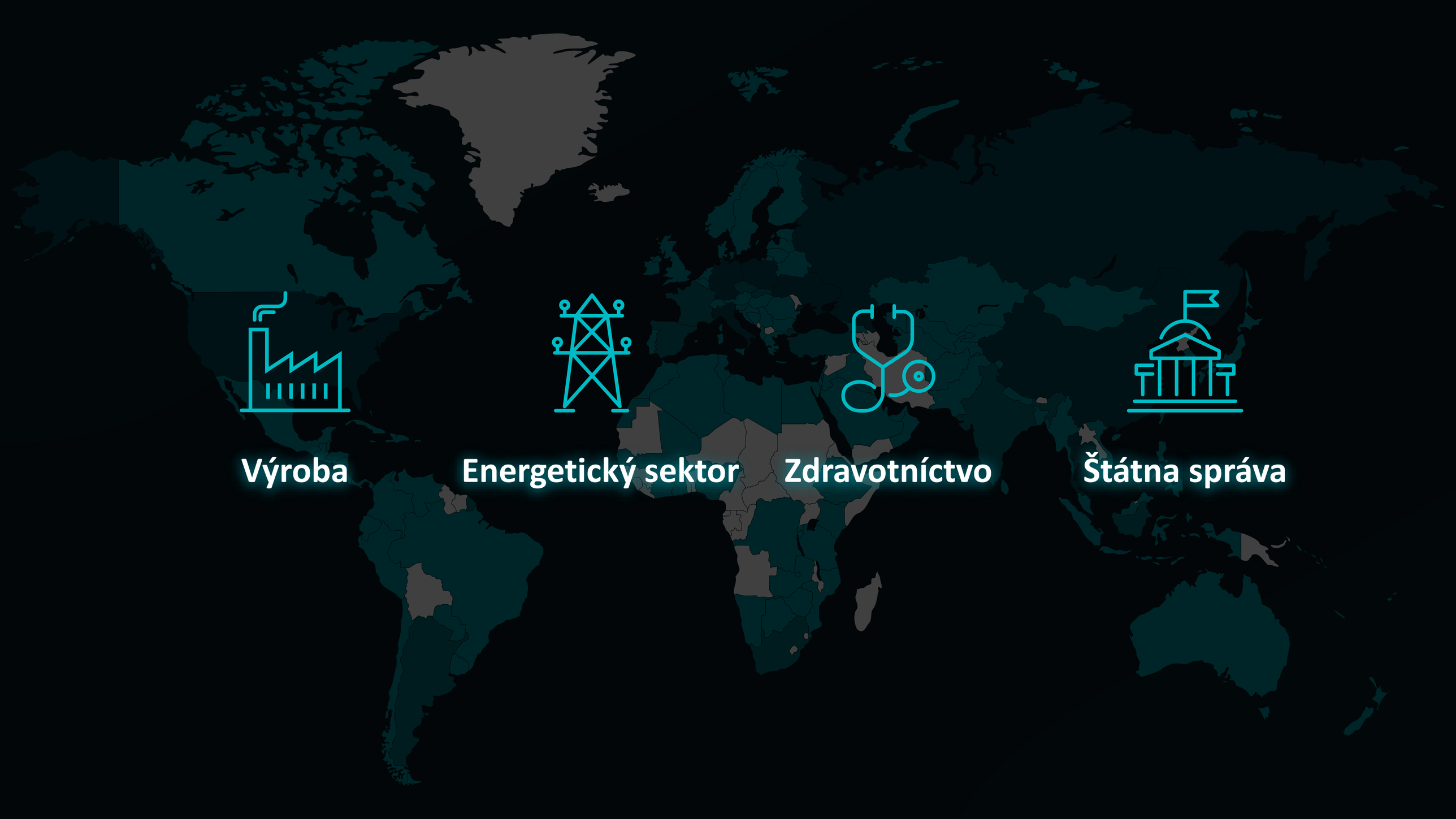
Rozdelenie obetí ransomware útokov podľa veľkosti



Zdroj: ecrime.ch






Výroba
Energetický sektor
Zdravotníctvo
Štátna správa

Ransomware ako služba

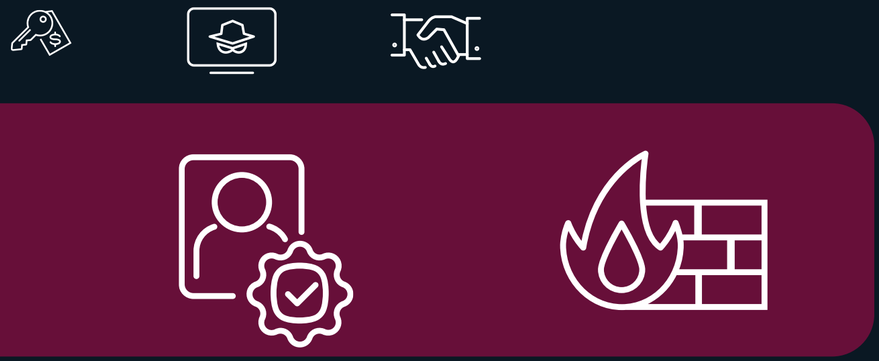
Ransomware as a service (RaaS)

Ransomware ako služba

Operátor

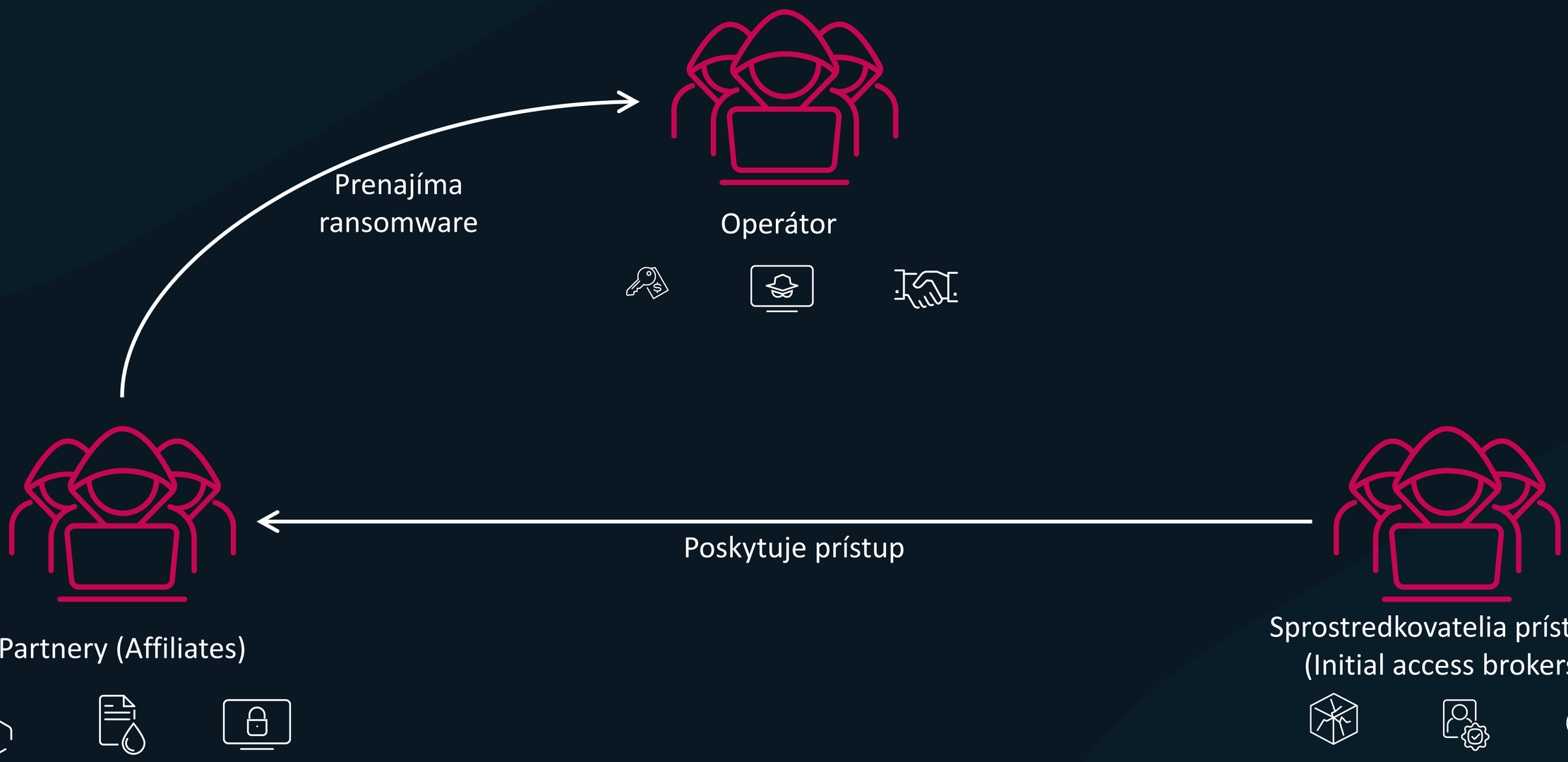
Ransomware ako služba

Operátor

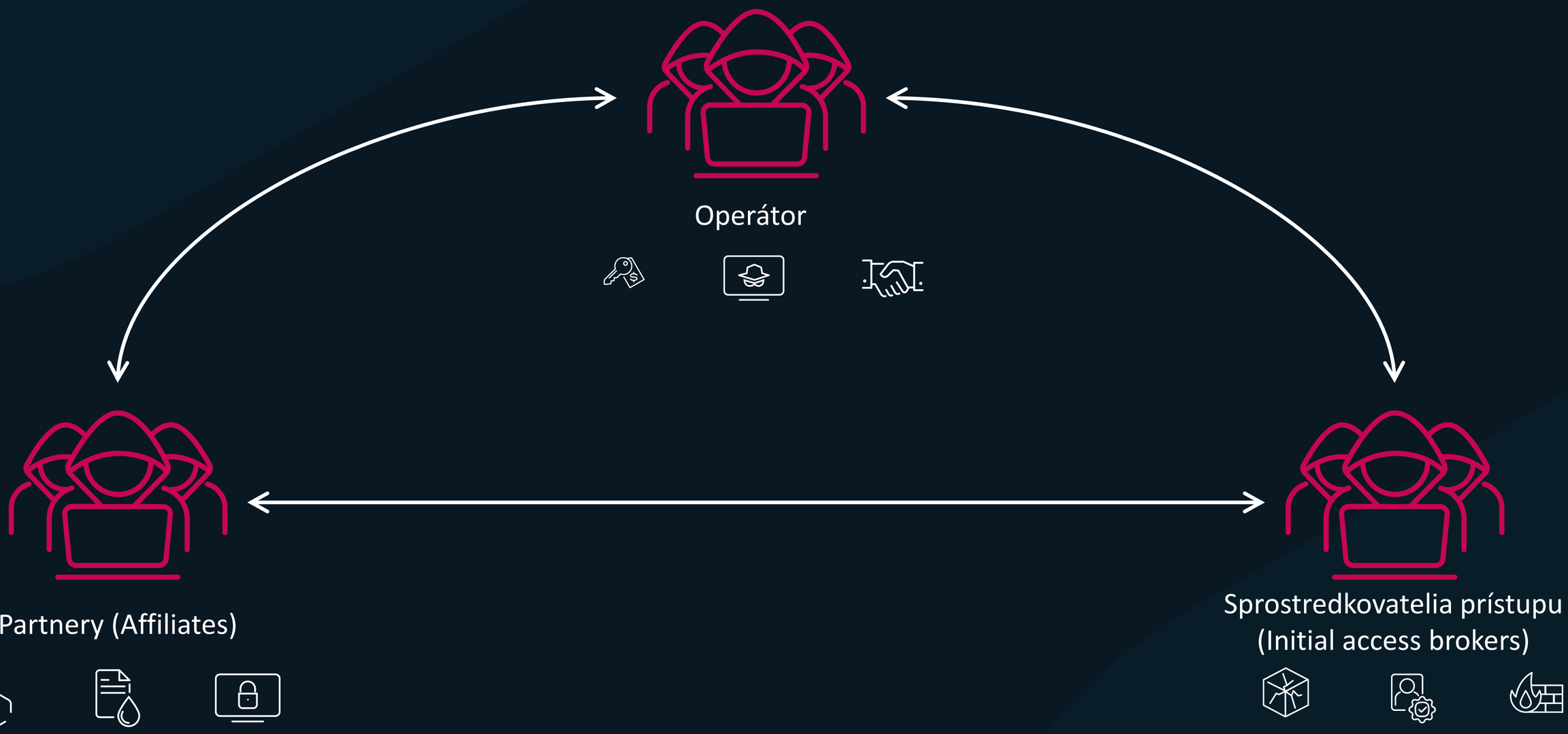


Partnery (Affiliates)

Ransomware ako služba



Ransomware ako služba



Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť

Globálné zmeny

Vzostup skupiny RansomHub

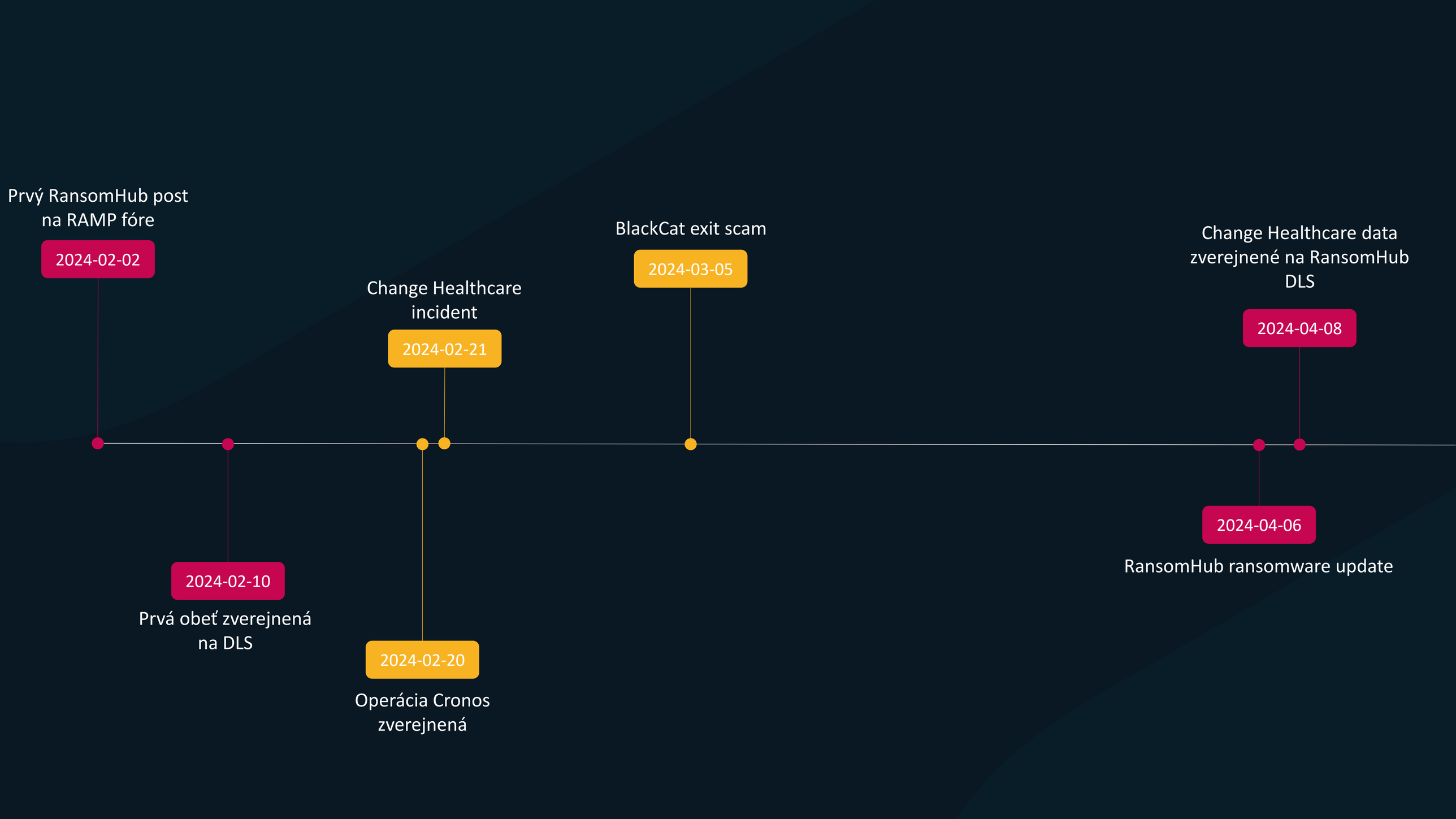
Využitie EDRKillShifteru

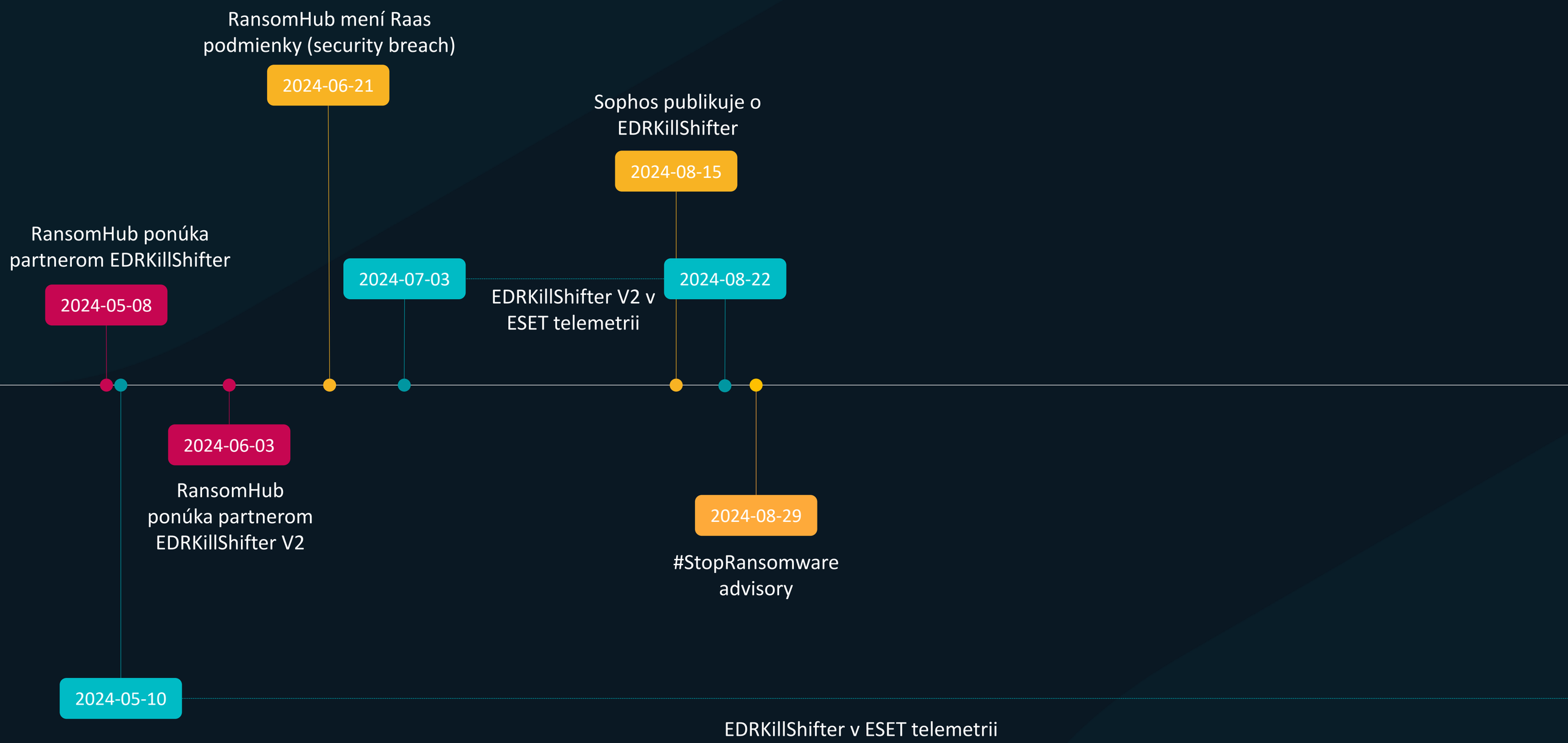
Ako sa brániť?

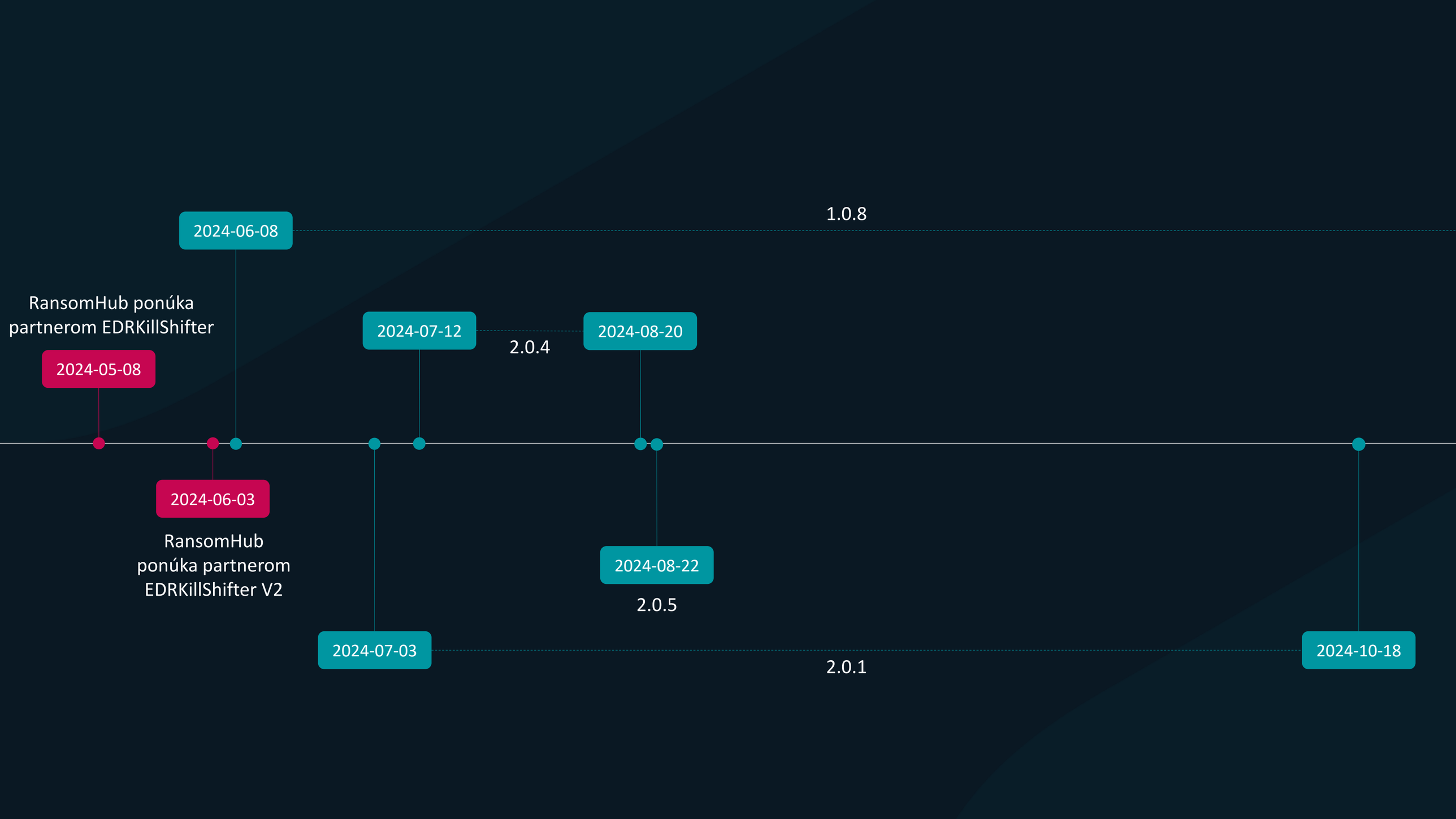
Budúcnosť

RansomHub

- “Nový LockBit”?
- Prevzatie partnerov
- Uvoľnenie podmienok partnerských kontraktov
- Nepúta pozornosť


Prvý RansomHub post na RAMP fóre
2024-02-02
2024-02-10
Prvá obeť zverejnená na DLS
Change Healthcare incident
2024-02-21
2024-02-20
Operácia Cronos zverejnená
BlackCat exit scam
2024-03-05
Change Healthcare data zverejnené na RansomHub DLS
2024-04-08
2024-04-06
RansomHub ransomware update


RansomHub mení Raas podmienky (security breach)
2024-06-21
Sophos publikuje o EDRKillShifter
2024-08-15
RansomHub ponúka partnerom EDRKillShifter
2024-05-08
2024-07-03
EDRKillShifter V2 v ESET telemetrii
2024-08-22
2024-06-03
RansomHub ponúka partnerom EDRKillShifter V2
2024-08-29
#StopRansomware advisory
2024-05-10
EDRKillShifter v ESET telemetrii


2024-06-08
1.0.8
RansomHub ponúka partnerom EDRKillShifter
2024-05-08
2024-07-12
2.0.4
2024-08-20
2024-06-03
RansomHub ponúka partnerom EDRKillShifter V2
2024-08-22
2.0.5
2024-07-03
2.0.1
2024-10-18

Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť

Globálné zmeny

Vzostup skupiny RansomHub

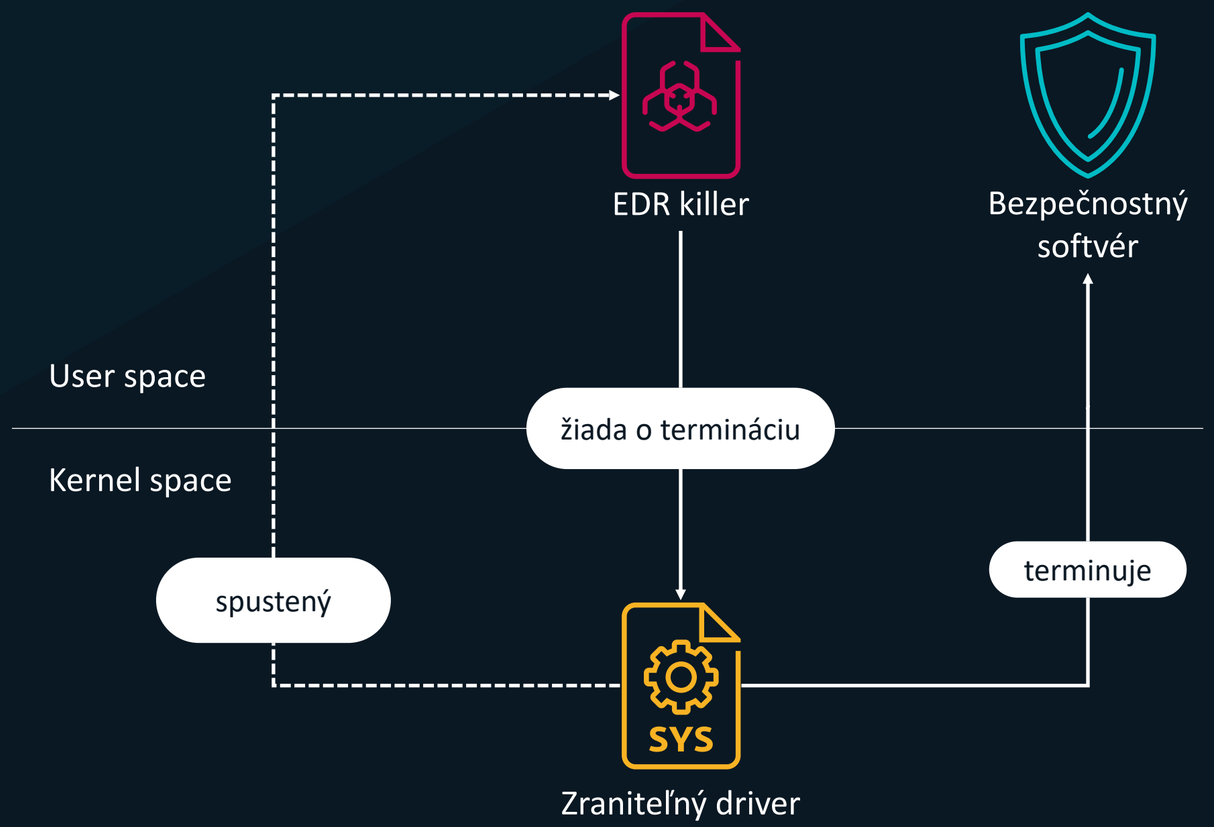
Využitie EDRKillShifteru

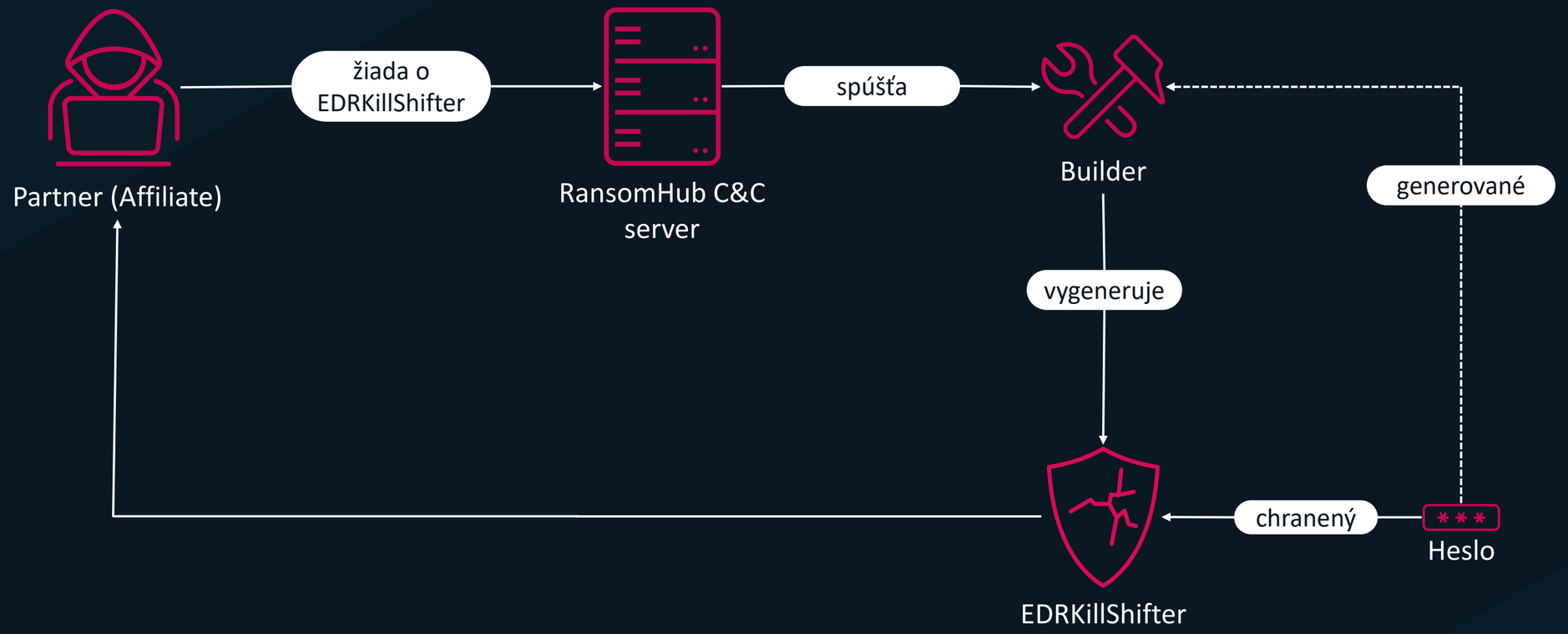
Ako sa brániť?

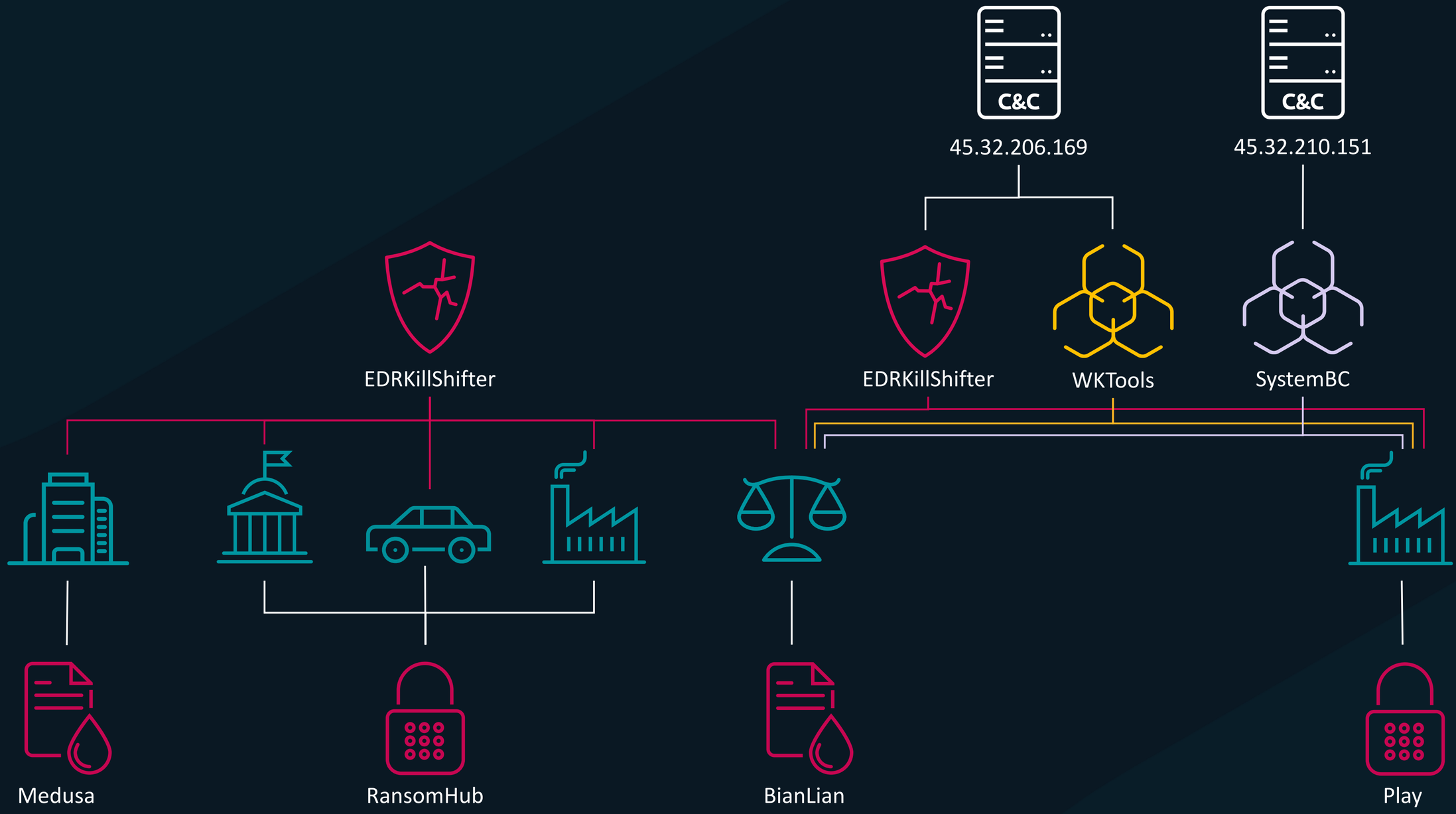
Budúcnosť

EDRKillShifter

- EDR killer
- Vyvinutý operátorom RansomHub
- Obfuskovaný, heslom chránený kód
- Ponúkaný vrámci RansomHub RaaS


EDR killer
Bezpečnostný softvér
User space
Kernel space
žiada o terminációu
spustený
terminuje
SYS
Zraniteľný driver


Partner (Affiliate)
žiada o EDRKillShifter
RansomHub C&C server
spúšťa
Builder
generované
vygeneruje
chranený
***
Heslo
EDRKillShifter

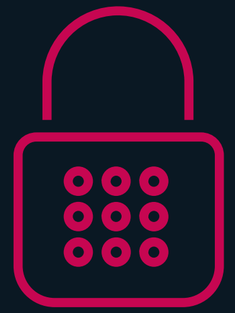

C&C
45.32.206.169
C&C
45.32.210.151
EDRKillShifter
EDRKillShifter
WKTools
SystemBC
Medusa
RansomHub
BianLian
Play

EDRKillShifter

Medusa

RansomHub

BianLian



Play

Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť

Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť

Patch management

MFA

Ochrana infraštruktúry

Odolnosť proti phishing útokom

Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť

Globálné zmeny

Vzostup skupiny RansomHub

Využitie EDRKillShifteru

Ako sa brániť?

Budúcnosť

Zameranie sa na partnerov (affiliates)

Spolupráca s policajnými zložkami

Posilnenie obrany potenciálnych obetí

SECURITY DAYS

Ďakujem za pozornosť!

Digital Security
Progress. Protected.

& SME KONFERENCIE