Alinet

Útoky na firemní účty a VPN

23.1.2025

Alinet CZ s.r.o. **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Kdo jsem?

Alinet

Kdo jsem?

Jakub Alimov, CEH, CHFI

Lead Auditor

architekt kybernetické bezpečnosti,

RANSOMWARE hunter,

konzultant informační bezpečnosti,

více jak 15+ let prokazatelných zkušeností s kybernetickou bezpečností

https://www.linkedin.com/in/jakub-alimov-332b1020/

Alinet

Kdo je Alinet?

Alinet

Jsme progresivní IT firma se specializací na kybernetické útoky.

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelností
- ✓ ISO IEC 27001, ISO IEC 62443, NIST CSF, NIS2
- ✓ Zabezpečení kritické infrastruktury

SLUŽBA DETEKCE KYBERNETICKÝCH UDÁLOSTÍ

- ✓ Proaktivní monitoring kybernetické bezpečnosti
- ✓ Dohled kritických assetů ve společnosti
- ✓ Visibilita co se děje
- ✓ Ochrana perimetru

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Reálné útoky v roce 2024?

Alinet

Reálné útoky v roce 2024?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování z minulého roku.

- ✓ **Nepoužívání MFA na VPN s kombinací zneužití uživatelského jména a hesla mělo za důsledek nedostupnost několik měsíců**
- ✓ **Zranitelnost na perimetru v jednom systému zašifrovala celou firmu**
- ✓ **Neaktualizovaná webová služba umožnila přístup komukoliv do interní firemní sítě**

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

RANSOMWARE?

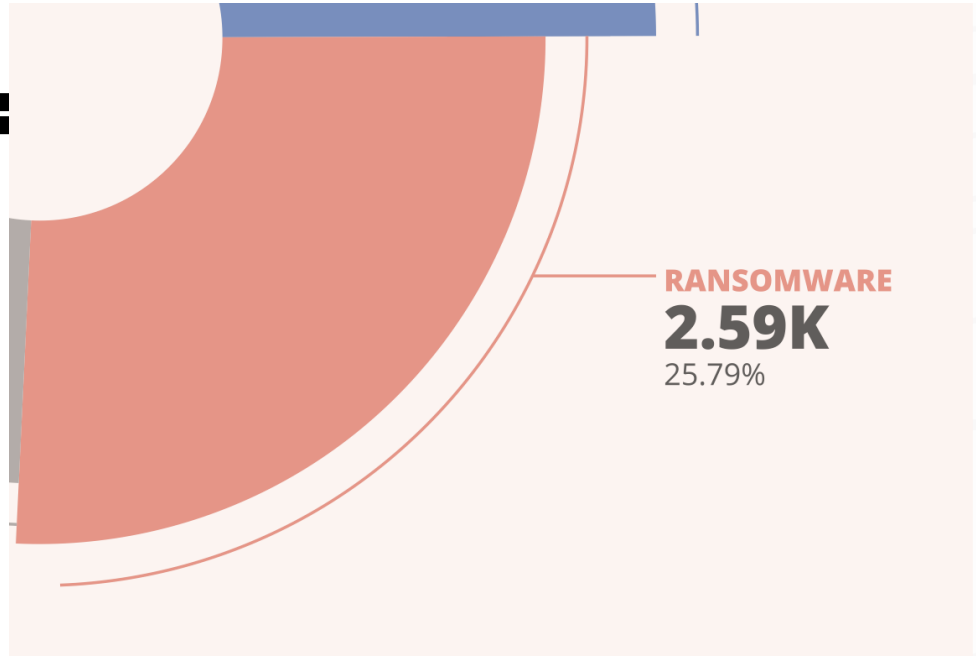
= šance 1 : 4

Zdroj: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

Alinet

RANSOMWARE?

=



Zdroj: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

Alinet

Časová osa RANSOMWARE útoku ...

... ovládnutí sítě trvalo pouhých 88 minut !

Alinet

Zpět k příběhu s VPN

Alinet

Zaměstnanec

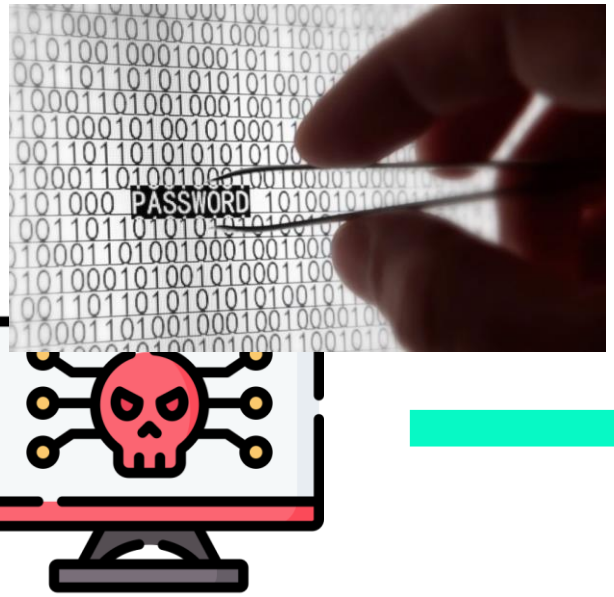
- ✓ uživatelské jméno
- ✓ heslo

Firemní VPN server

Interní služby

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet



DODAVATEL
ADMIN oprávnění

- ✓ **uživatelské jméno**
- ✓ **heslo**

- ✓ **nemáme kontrolu nad uživatelem**
- ✓ **… zařízenim**

Firemní VPN server

Interní služby

lokální administrátor

Alinet

Útočník
ADMIN oprávnění

- ✓ uživatelské jméno
- ✓ Heslo
- ✓ ????

Firemní VPN server

Interní služby

lokální administrátor

…88 minut

Alinet

Jak by to mělo dnes vypadat?

Alinet

Zaměstnanec

Firemní VPN server

Interní služby

- ✓ **Vyškolený – poslušný :)**
- ✓ **EDR – XDR**
- ✓ **Trusted device**
- ✓ **Klientský certifikát**
- ✓ **MFA !!!**

Alinet

Už víme proč MFA na VPN

nebo

co se stane v roce 2025?

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

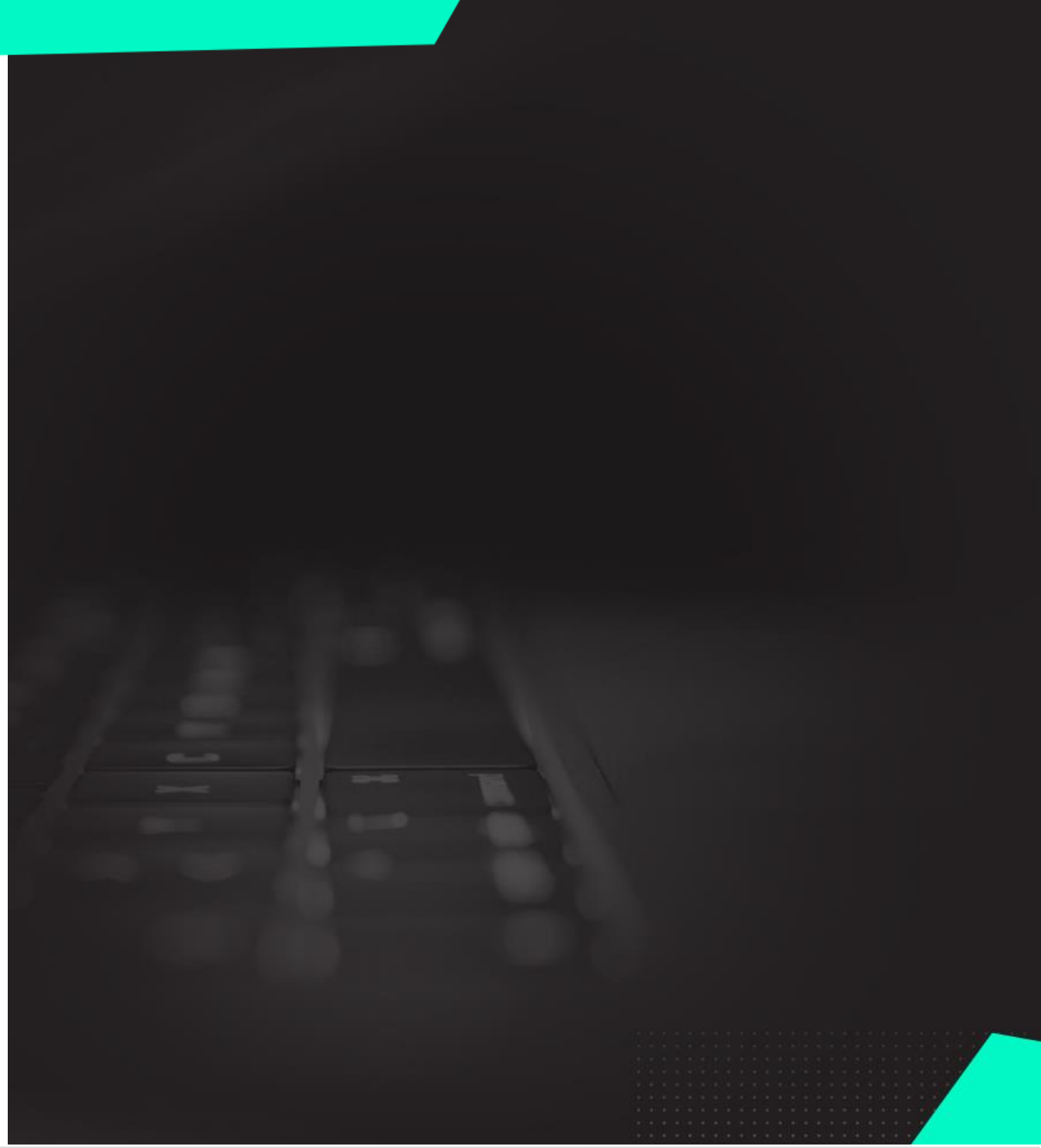
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

14.1.2025

FORTIGATE

Authentication bypass
CVE-2024-55591

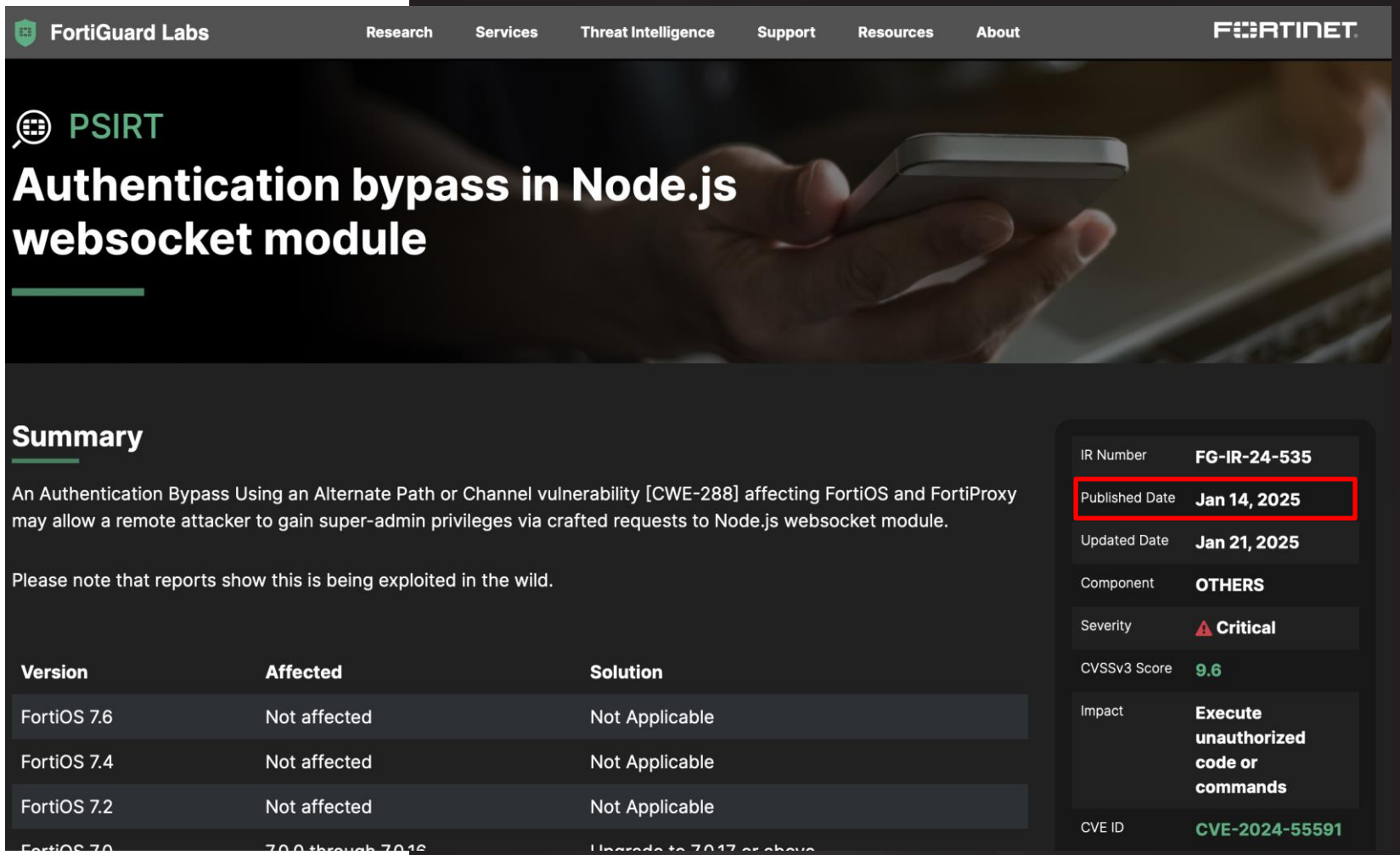


Alinet

14.1.2025

FORTIGATE

Authentication bypass **CVE-2024-55591**



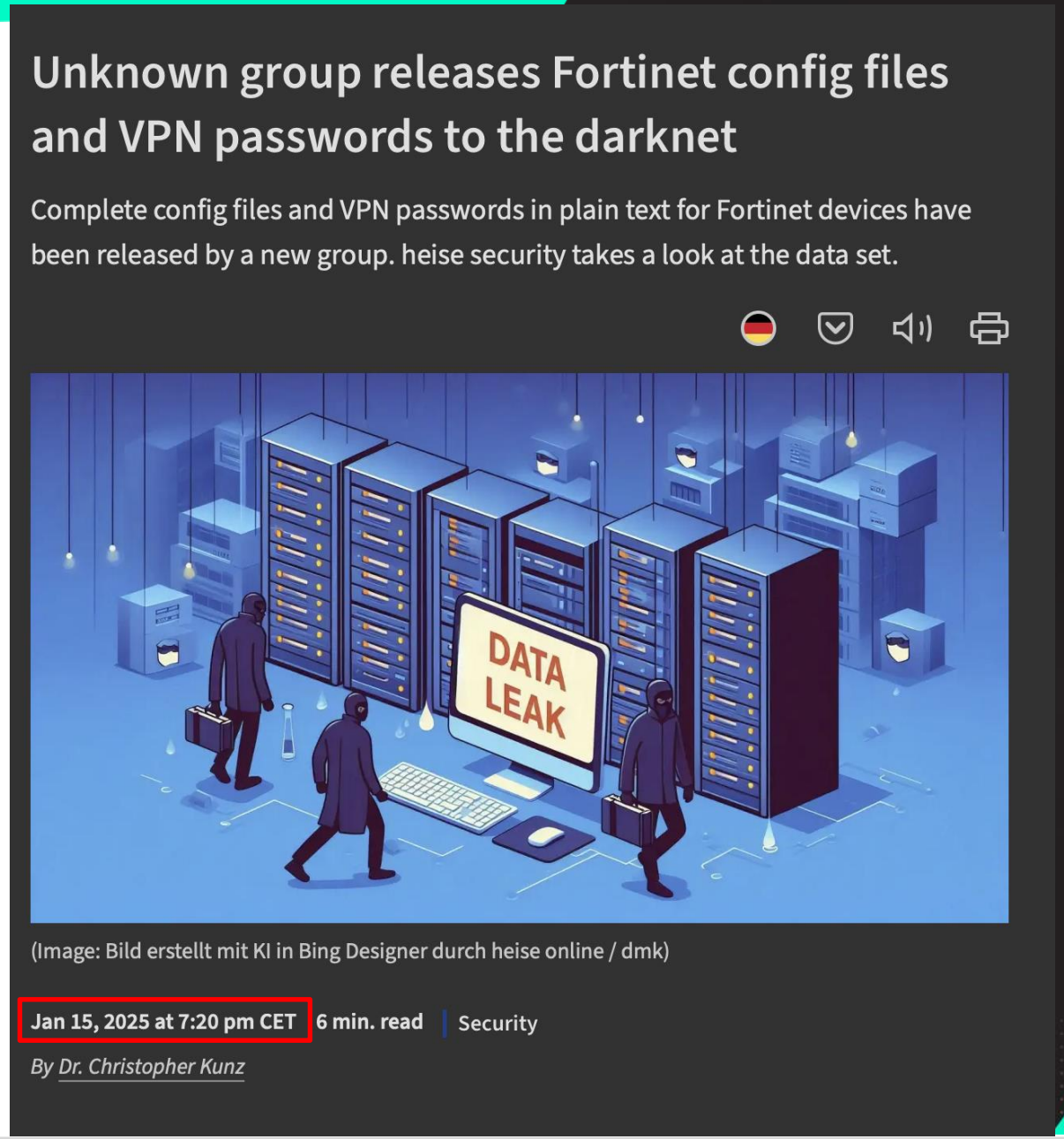
Zdroj: https://www.fortiguard.com/psirt/FG-IR-24-535

Alinet

15.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



Unknown group releases Fortinet config files and VPN passwords to the darknet

Complete config files and VPN passwords in plain text for Fortinet devices have been released by a new group. heise security takes a look at the data set.

(Image: Bild erstellt mit KI in Bing Designer durch heise online / dmk)

Jan 15, 2025 at 7:20 pm CET 6 min. read | Security

By Dr. Christopher Kunz

Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html

Alinet

15?.1

Passwo

Authent
bypass
CVE-2024-55591

Unknown group releases Fortinet config files and VPN passwords to the darknet

Complete config files and VPN passwords in plain text for Fortinet devices have

FortiGate 15K+ Targets (Configs+VPN Passwords)
by Belsen_Group - Tuesday January 14, 2025 at 04:43 PM

Belsen_Group

BG

Breached

MEMBER

Posts: 1
Threads: 1

30 minutes ago #1

2025 will be a fortunate year for the world.

At the beginning of the year, and as a positive start for us, and in order to solidify the name of our group in your memory, we are proud to announce our first official operation:
Will be published of sensitive data from over 15,000 targets worldwide (both governmental and private sectors) that have been hacked and their data extracted.

The data includes:
1.IPs.
2.Passwords.
3.Configs.

To make it easier for you, we have categorized the targets by country names.

And the biggest surprise: All this sensitive and crucial data is absolutely FREE, offered to you as a gift from the Belesn Group.

You can access the data here:
belsenacdodoy3nsmmyjfmtgjen6ipaqkti7dm2q57vabjx2vzq6tnad.onion

(Image: Bild erstellt mit KI in Bing Designer durch heise online / dmk)

Jan 15, 2025 at 7:20 pm CET **6 min. read** | Security

By Dr. Christopher Kunz

Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html

Alinet

15?.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591

- ✓ 15 474 Fortigate celý svět (136 CZ a 11 SK)
- ✓ Seznam je už z roku 2022 !!
  - ✓ založený na zranitelnosti CVE-2022-40684
  - ✓ Aktualizovaný 1/2024
  - ✓ Seřazen podle zemí RU
- ✓ Uživatelské jména
- ✓ Hesla (samozřejmě v plaintextu)
- ✓ Full config fortigate (včetně certifikátů)

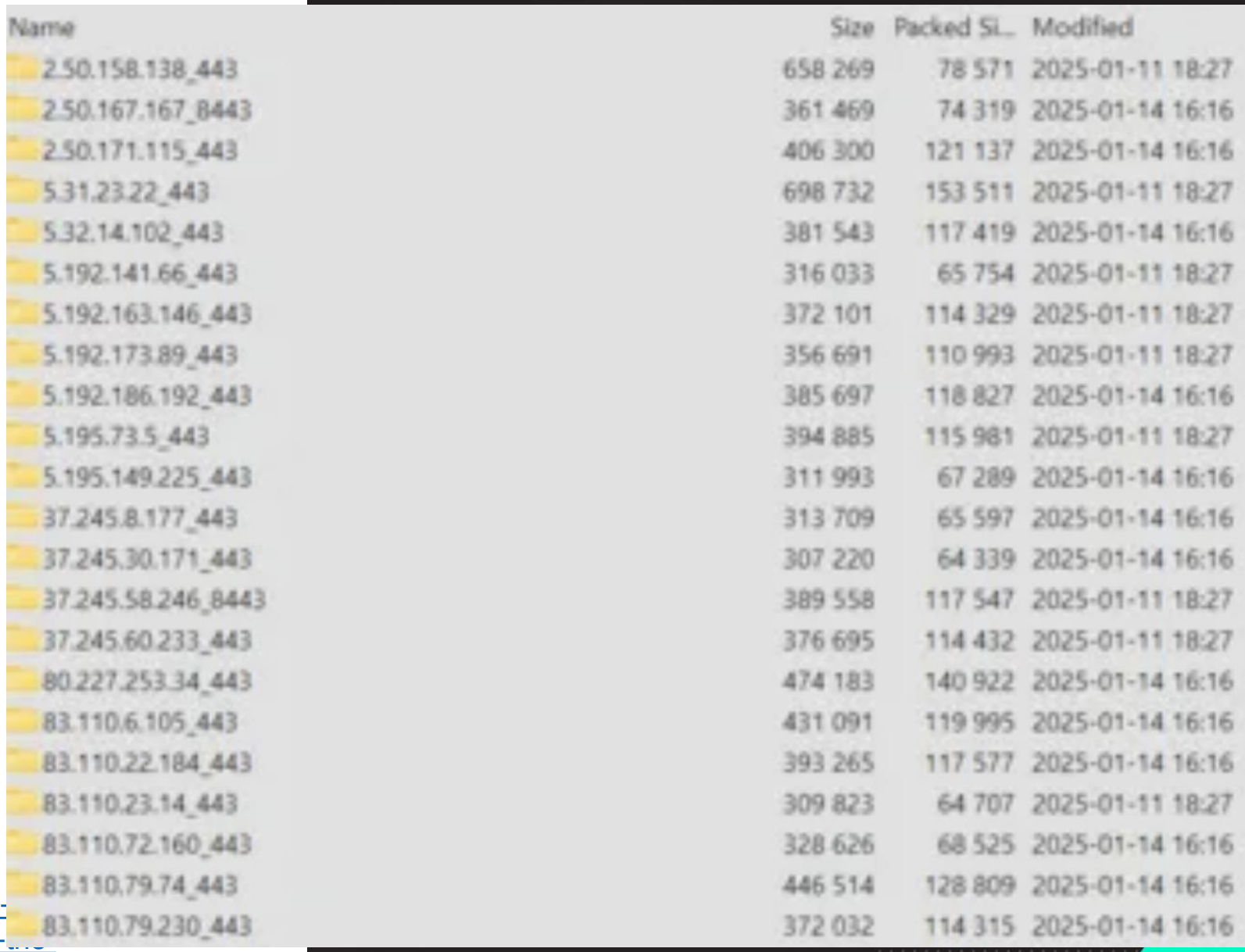
Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html

Alinet

15?.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



Name	Size	Packed Si...	Modified
2.50.158.138_443	658 269	78 571	2025-01-11 18:27
2.50.167.167_8443	361 469	74 319	2025-01-14 16:16
2.50.171.115_443	406 300	121 137	2025-01-14 16:16
5.31.23.22_443	698 732	153 511	2025-01-11 18:27
5.32.14.102_443	381 543	117 419	2025-01-14 16:16
5.192.141.66_443	316 033	65 754	2025-01-11 18:27
5.192.163.146_443	372 101	114 329	2025-01-11 18:27
5.192.173.89_443	356 691	110 993	2025-01-11 18:27
5.192.186.192_443	385 697	118 827	2025-01-14 16:16
5.195.73.5_443	394 885	115 981	2025-01-11 18:27
5.195.149.225_443	311 993	67 289	2025-01-14 16:16
37.245.8.177_443	313 709	65 597	2025-01-14 16:16
37.245.30.171_443	307 220	64 339	2025-01-14 16:16
37.245.58.246_8443	389 558	117 547	2025-01-11 18:27
37.245.60.233_443	376 695	114 432	2025-01-11 18:27
80.227.253.34_443	474 183	140 922	2025-01-14 16:16
83.110.6.105_443	431 091	119 995	2025-01-14 16:16
83.110.22.184_443	393 265	117 577	2025-01-14 16:16
83.110.23.14_443	309 823	64 707	2025-01-11 18:27
83.110.72.160_443	328 626	68 525	2025-01-14 16:16
83.110.79.74_443	446 514	128 809	2025-01-14 16:16
83.110.79.230_443	372 032	114 315	2025-01-14 16:16

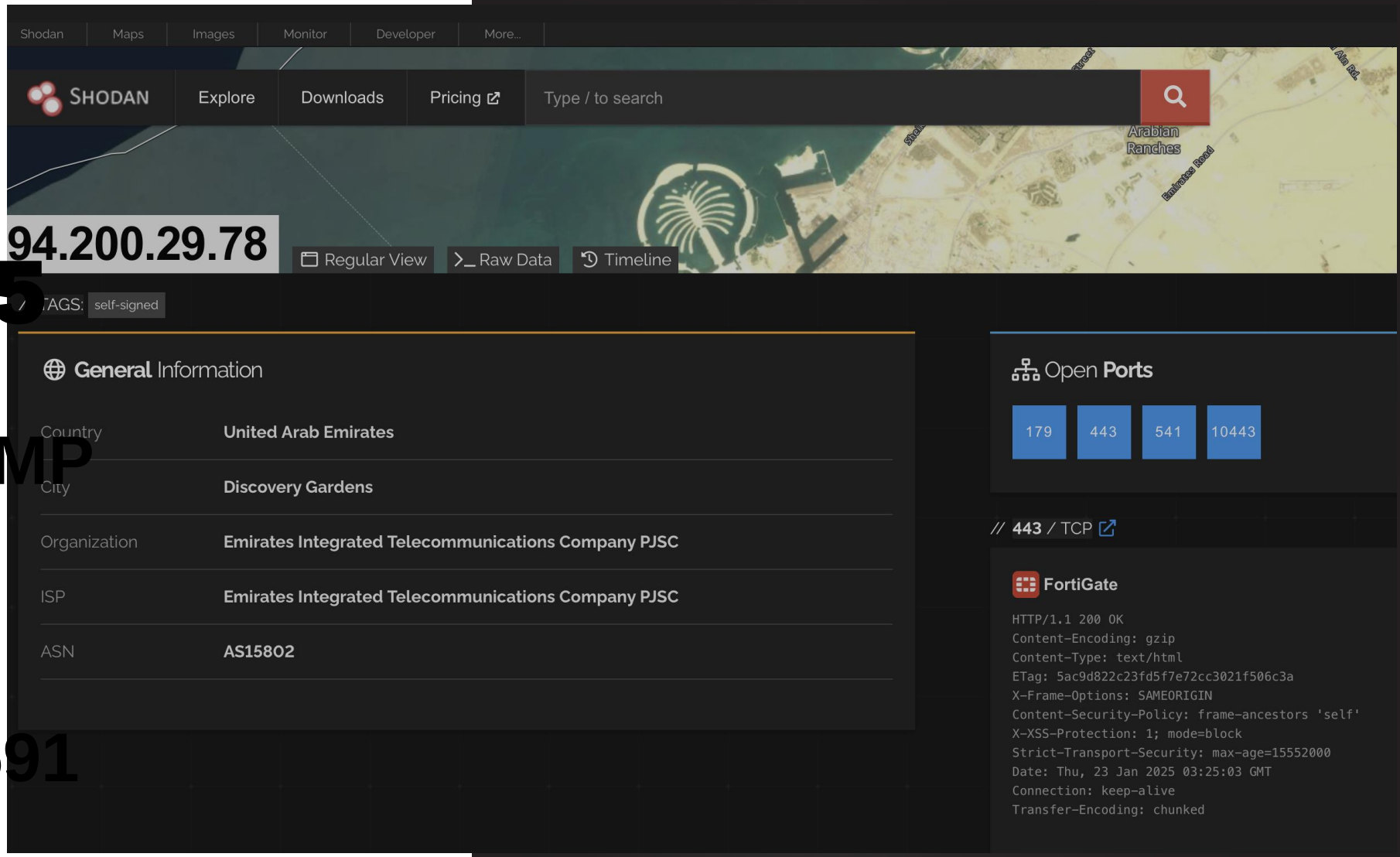
Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html

Alinet

15?.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



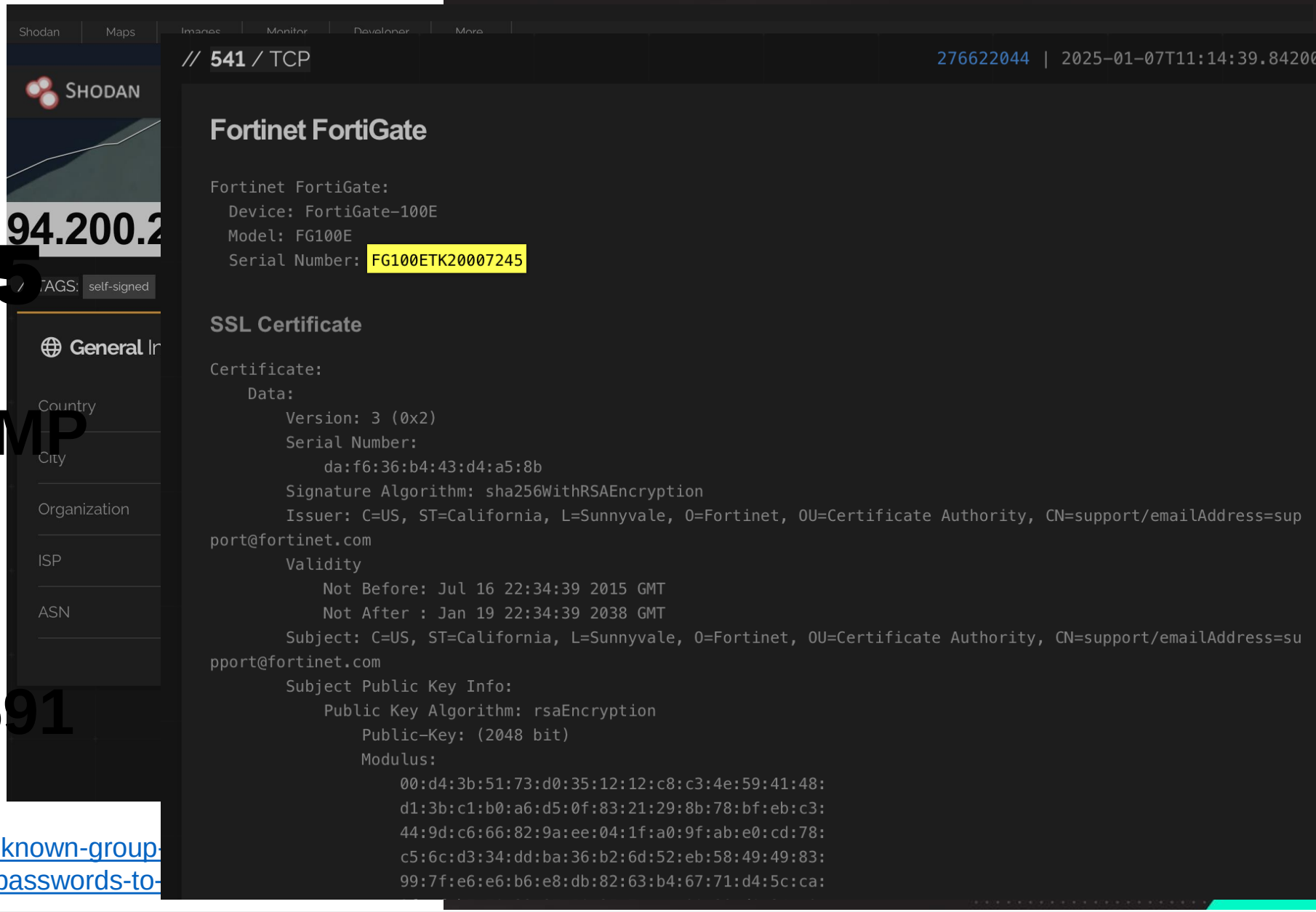
Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html

Alinet

15?.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



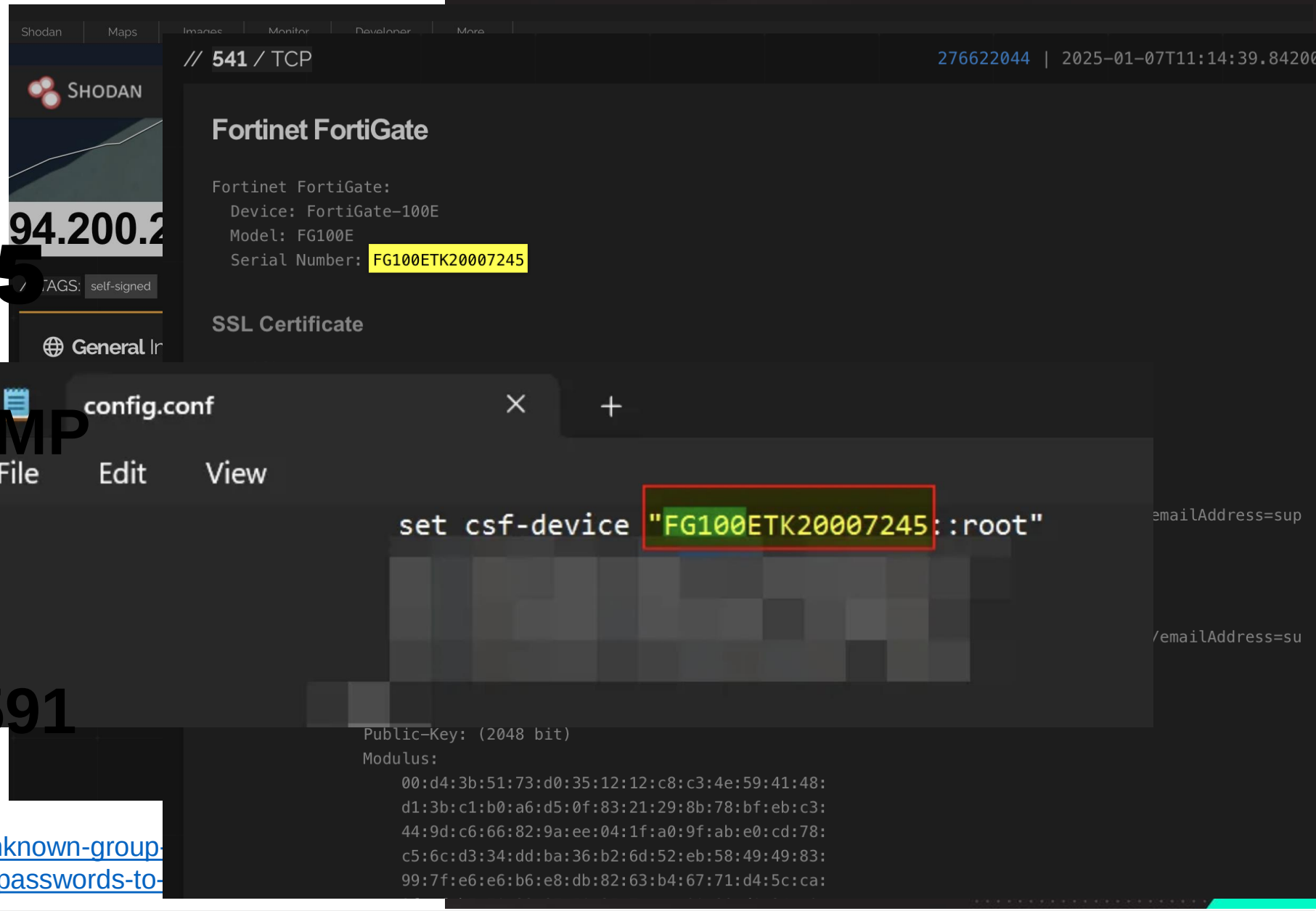
Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-darknet-10244238.html

Alinet

15?.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



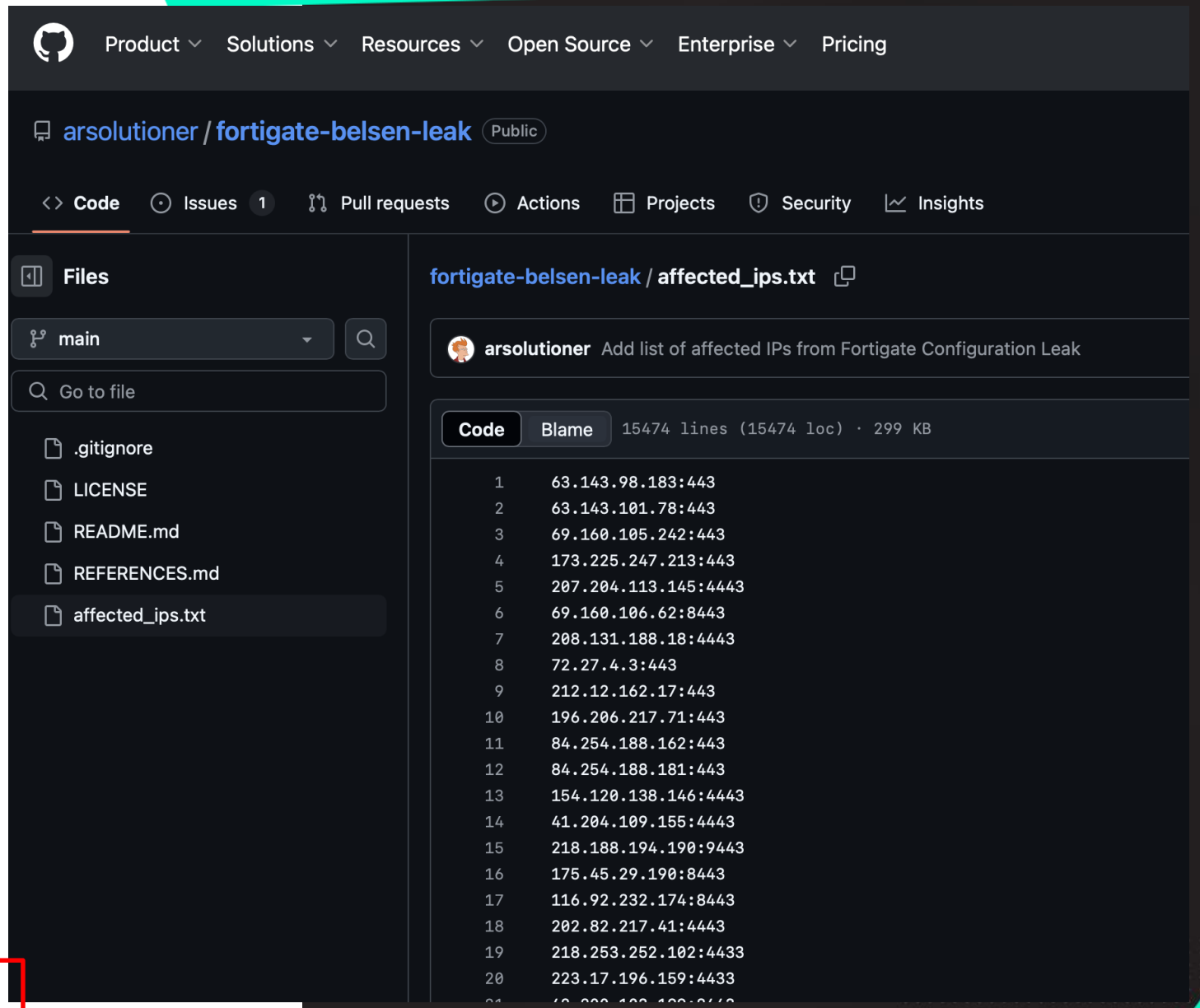
Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-darknet-10244238.html

Alinet

15?.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



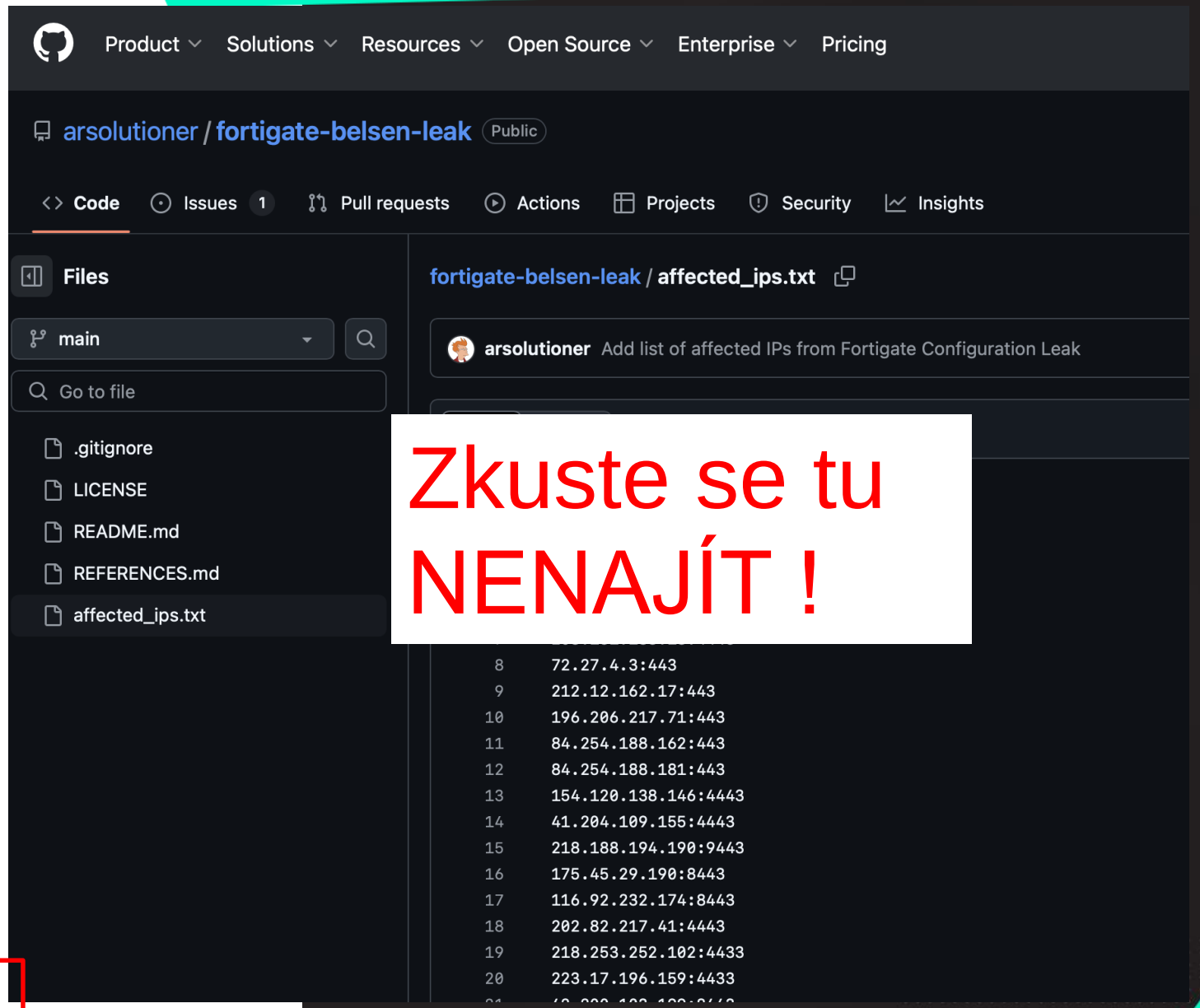
Zdroj: https://github.com/arsolutioner/fortigate-belsen-leak/blob/main/affected_ips.txt

Alinet

15?.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



Zdroj: https://github.com/arsolutioner/fortigate-belsen-leak/blob/main/affected_ips.txt

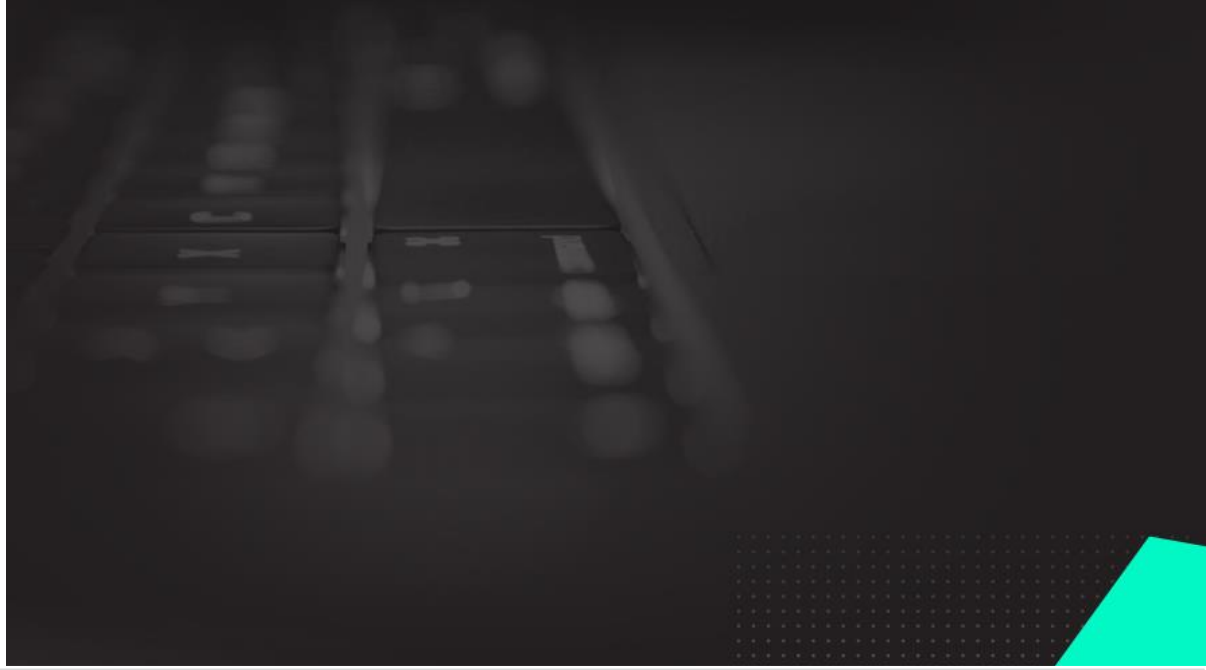
Alinet

Jak se nedostat na seznam!!! ?

Alinet

Jak se nedostat na „seznam“ ?

- ✓ MUSÍME být PROAKTIVNÍ ne REAKTIVNÍ
- ✓ Ochrana zranitelností na perimetru
- ✓ Zálohy !
- ✓ MFA !!!



Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Ochrana perimetru

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

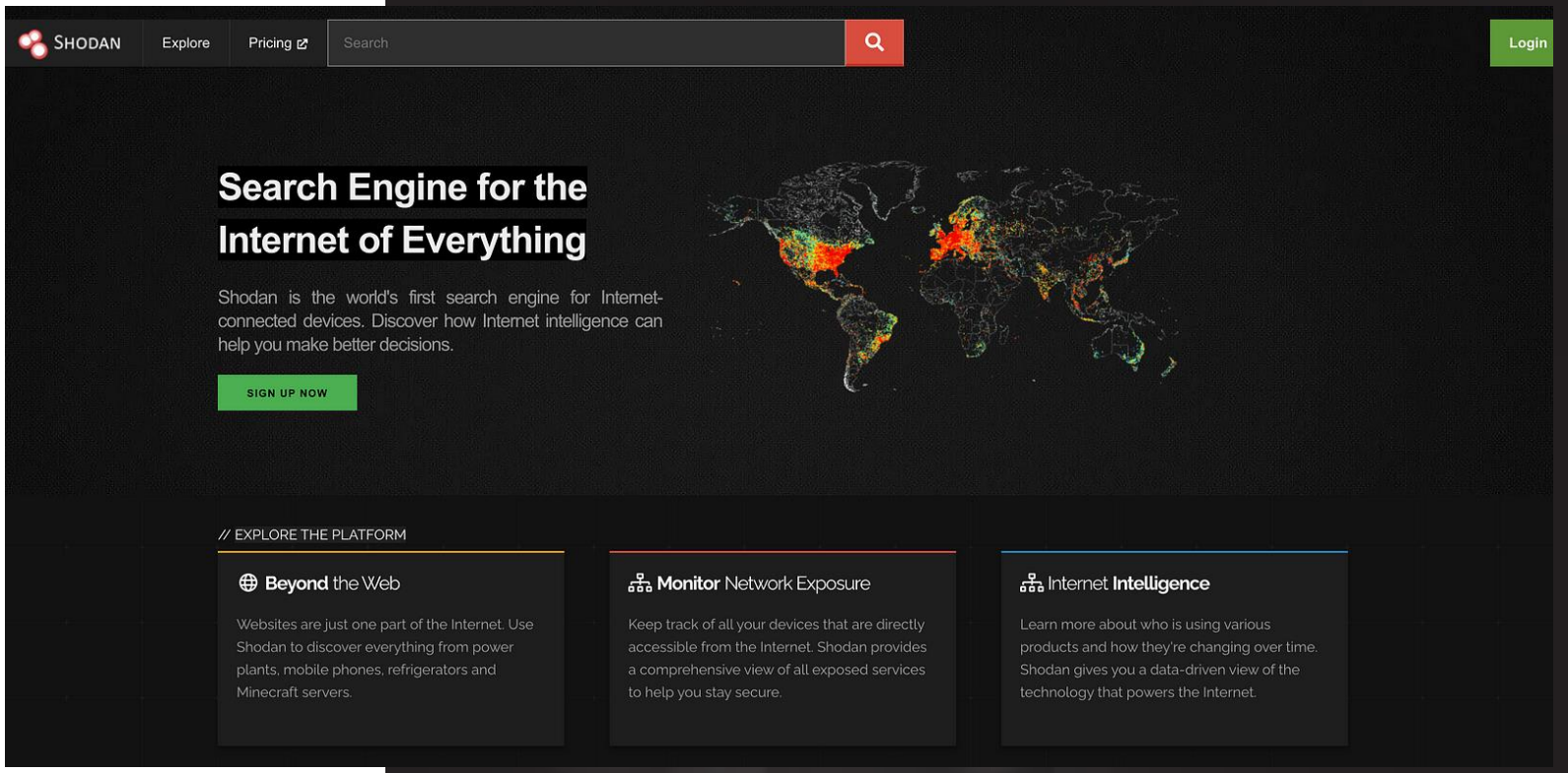
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Shodan.io

ZDARMA

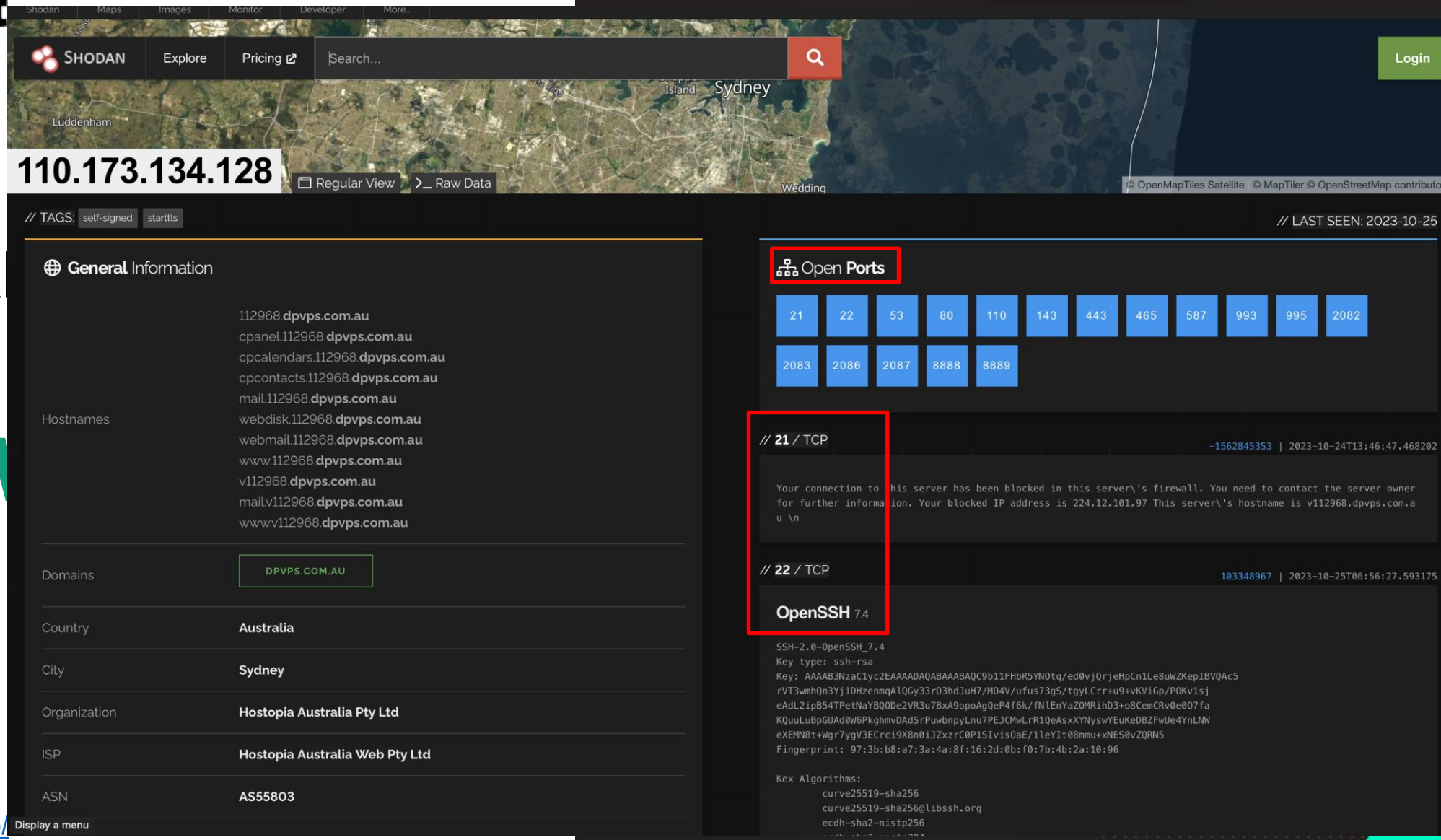


Zdroj: https://www.shodan.io/

Alinet

Shoda

ZDARM



Zdroj: https://www.shodan.io/

Alinet

Zabezpečení záloh

Alinet

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočníkovi získat přístup k zálohám a zničit je.

Checklist záloh:

- ✓ Pravidlo 3-2-1+1
- ✓ OFFLINE záloha !!!
- ✓ Pravidelná kontrola úplnosti a funkčnost záloh
- ✓ Oddělení záloh a virtualizace od Windows domény
- ✓ Vlastní VLAN pro zálohování s minimálními prostupy
- ✓ Historie záloh
- ✓ Co cloud? Zálohujete? např. o365
- ✓ Disaster Recovery plán

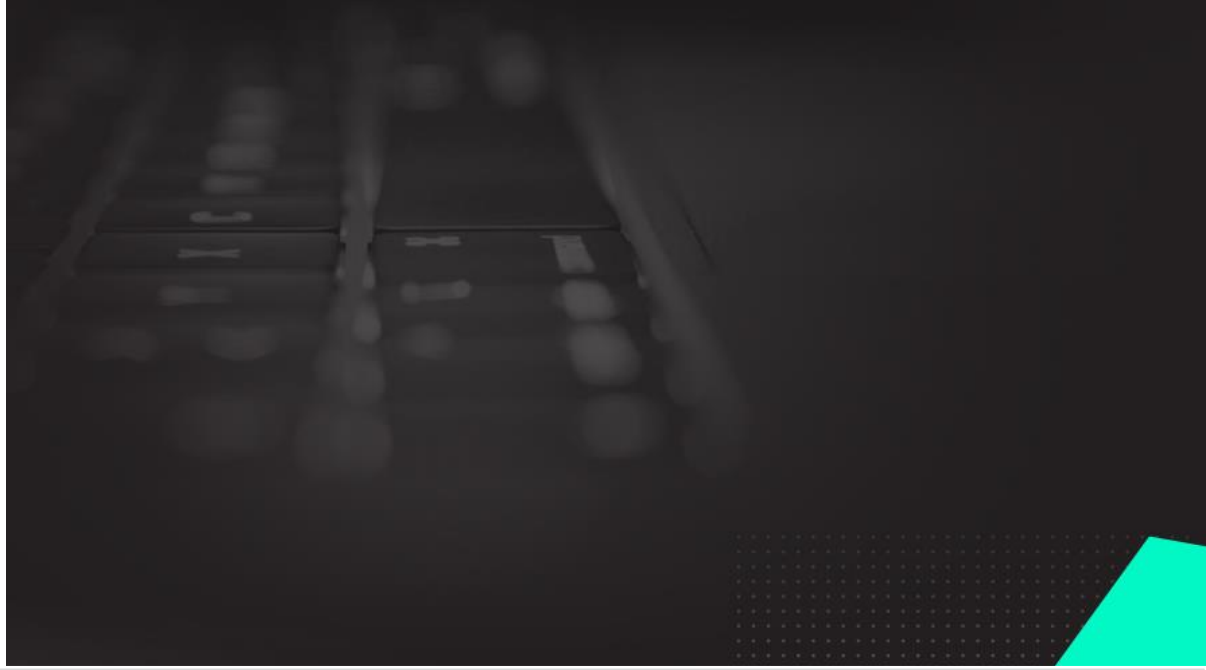
Alinet

Multifaktorové zabezpečení

Alinet

Multifaktorové ověření

- ✓ MFA vždy když je to možné !!
- ✓ SAML, FIDO, OTP, autentizační servery a aplikace
- ✓ Oddělení typy MFA administrátorů od uživatelů. PROČ?
- ✓ Phishing resistant MFA



Alinet

Potřebujete pomoci?

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Cyber Security, **Ransomware Incident Response**

Jakub Alimov

www.alinet.cz jakub.alimov@alinet.cz +420 774 077 108