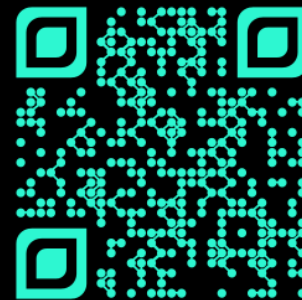


Útoky na firemní účty a VPN

23.1.2025





Kdo jsem?

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/>



Kdo je Alinet?



Jsme progresivní IT firma se specializací na kybernetické útoky.



DIGITAL FORENSICS AND INCIDENT RESPONSE

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

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelnosti
- ✓ 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



Reálné útoky v roce 2024?

Reálné útoky v roce 2024?

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

RANSOMWARE

- ✓ 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



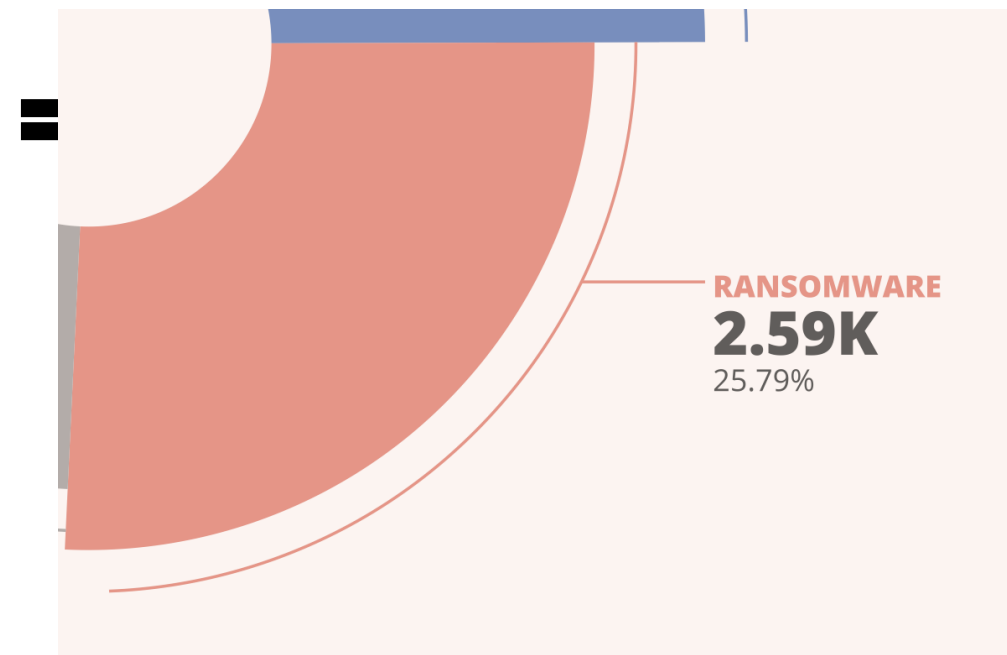
RANSOMWARE?

= 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>



RANSOMWARE?



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

Časová osa **RANSOMWARE** útoku ...



... ovládnutí sítě trvalo pouhých 88 minut !



Zpět k příběhu s VPN



Zaměstnanec

- ✓ uživatelské jméno
- ✓ heslo



Firemní VPN server



Interní služby



DODAVATEL
ADMIN oprávnění

- ✓ uživatelské jméno
- ✓ heslo

- ✓ nemáme kontrolu nad uživatelem
- ✓ ... zařízením



Firemní VPN server



Interní služby

lokální administrátor



Útočník
ADMIN oprávnění

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



Firemní VPN server



Interní služby

lokální administrátor

...88 minut

RANSOMWARE



Jak by to mělo dnes vypadat?



Zaměstnanec

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

Firemní VPN server

Interní služby



Už víme proč MFA na VPN

nebo

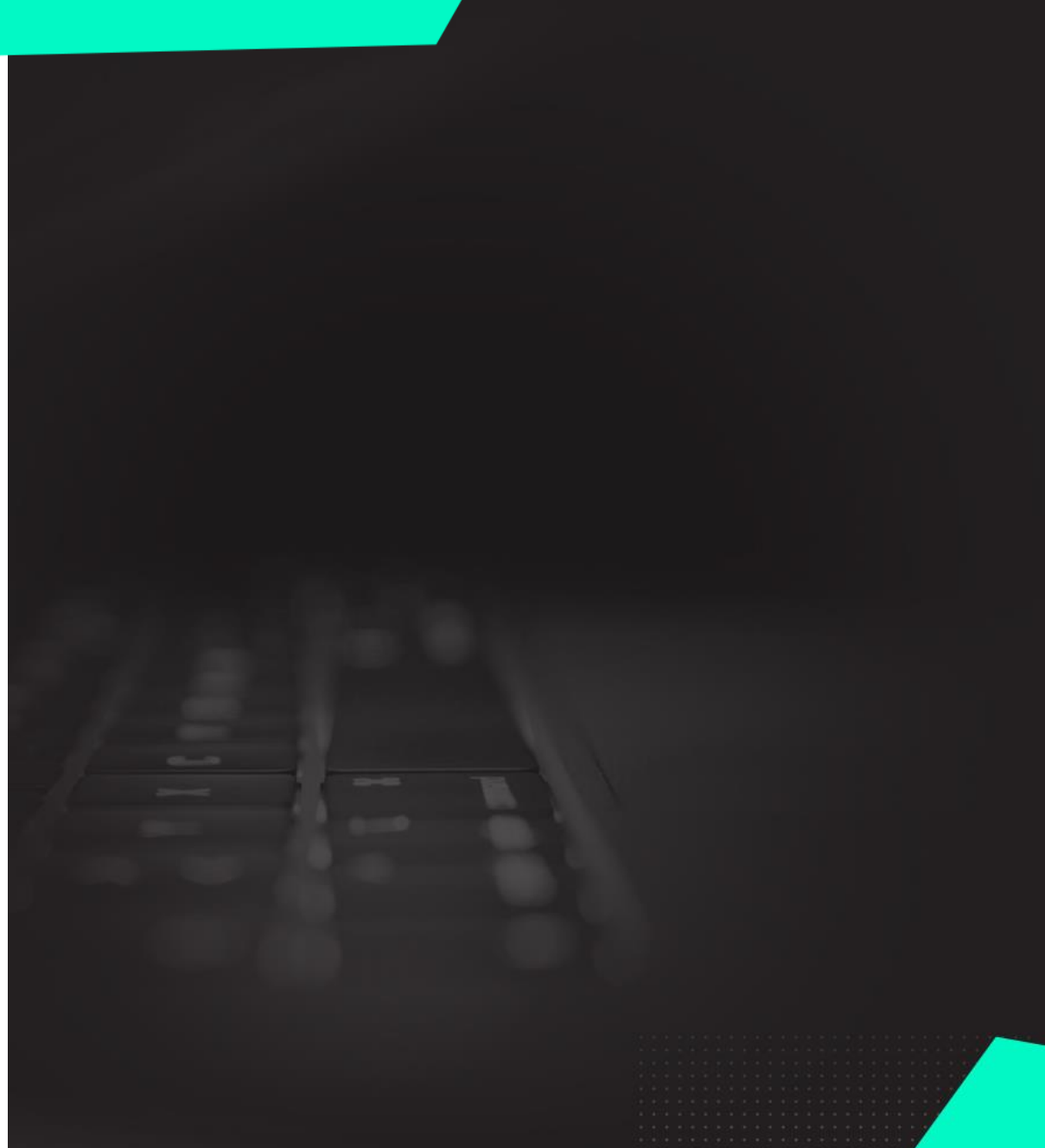
co se stane v roce 2025?

14.1.2025

FORTIGATE

Authentication
bypass

CVE-2024-55591

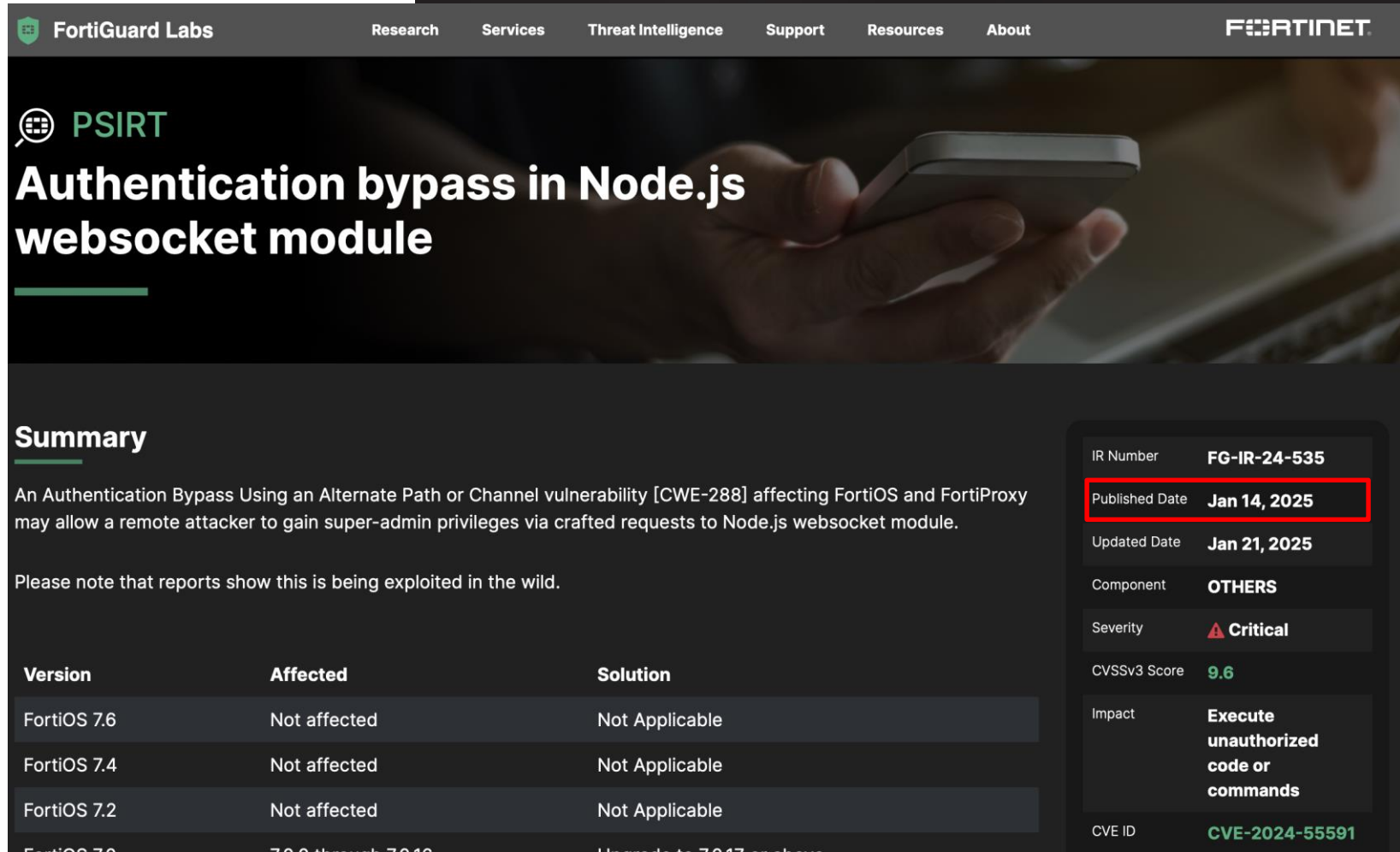


14.1.2025

FORTIGATE

Authentication bypass CVE-2024-55591

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



FortiGuard Labs | Research | Services | Threat Intelligence | Support | Resources | About | **FORTINET**

PSIRT

Authentication bypass in Node.js websocket module

Summary

An Authentication Bypass Using an Alternate Path or Channel vulnerability [CWE-288] affecting FortiOS and FortiProxy may allow a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module.

Please note that reports show this is being exploited in the wild.

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	Not affected	Not Applicable
FortiOS 7.2	Not affected	Not Applicable
FortiOS 7.0	7.0 through 7.0.16	Upgrade to 7.0.17 or above

IR Number	FG-IR-24-535
Published Date	Jan 14, 2025
Updated Date	Jan 21, 2025
Component	OTHERS
Severity	▲ Critical
CVSSv3 Score	9.6
Impact	Execute unauthorized code or commands
CVE ID	CVE-2024-55591

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>

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](#)

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

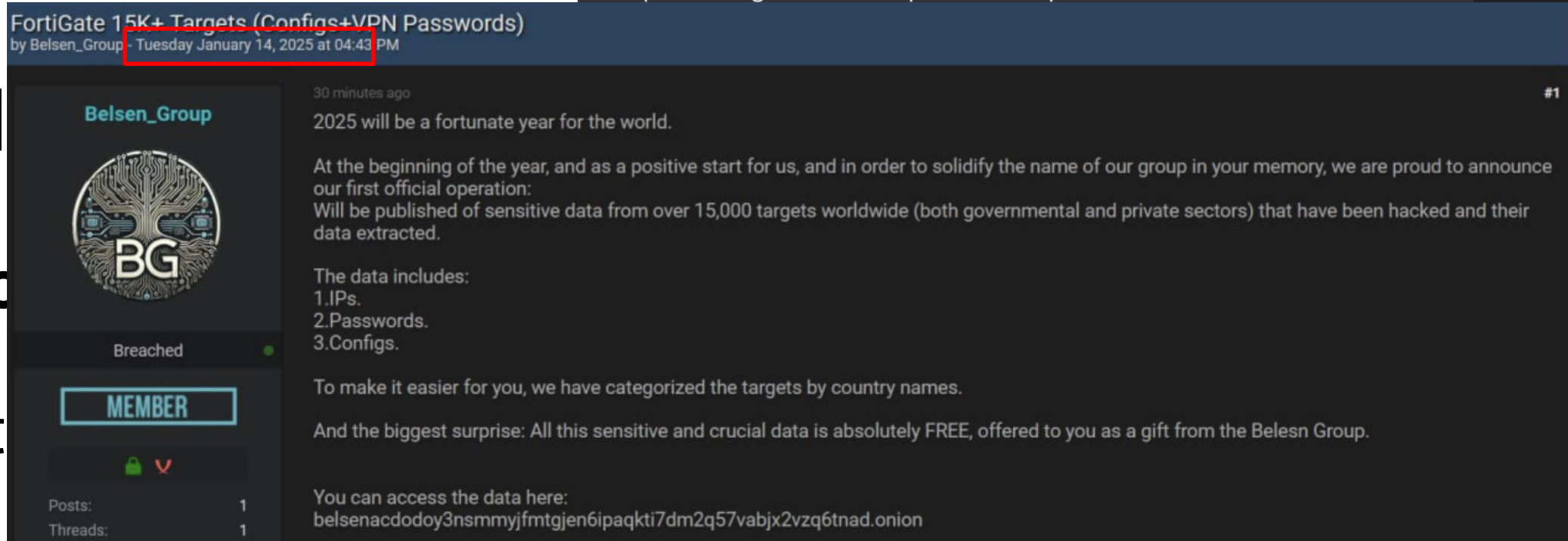
Complete config files and VPN passwords in plain text for Fortinet devices have

15?..1

Passwords

Authent bypass

CVE-2024-55591



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

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>

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>

- ✓ 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)

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

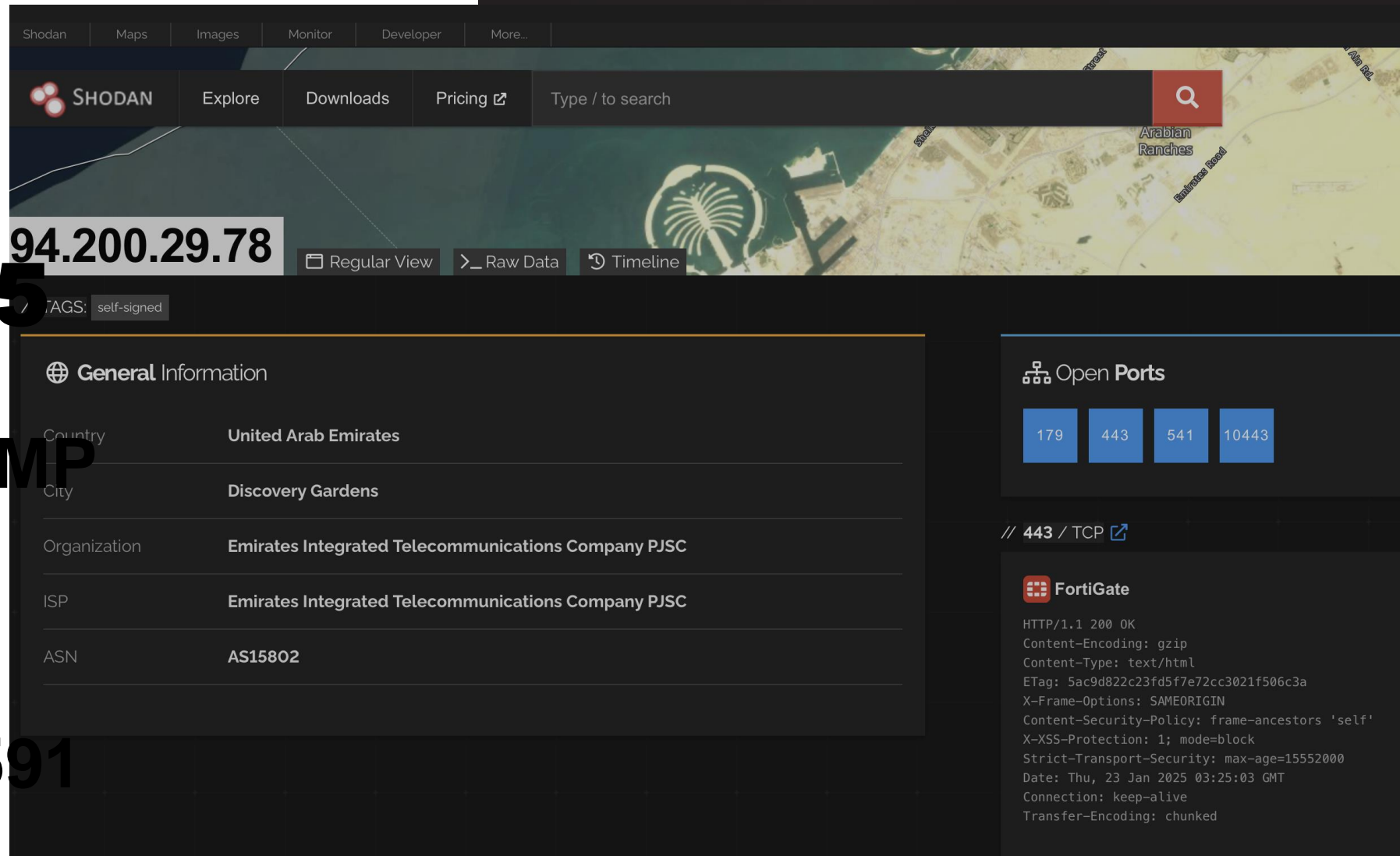
Zdroj: <https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-darknet-10244238.html>

15?.1.2025

Password DUMP

Authentication bypass

CVE-2024-55591



Shodan interface showing search results for IP 94.200.29.78. The interface includes a search bar, navigation tabs (Shodan, Maps, Images, Monitor, Developer, More...), and a search bar with the text 'Type / to search'. The main content area displays the IP address 94.200.29.78, a 'Regular View' button, and a 'Raw Data' button. Below the IP address, there is a 'TAGS: self-signed' section. The 'General Information' section lists the following details:

Country	United Arab Emirates
City	Discovery Gardens
Organization	Emirates Integrated Telecommunications Company PJSC
ISP	Emirates Integrated Telecommunications Company PJSC
ASN	AS15802

On the right side, there is an 'Open Ports' section showing four ports: 179, 443, 541, and 10443. Below this, there is a section for '443 / TCP' with a 'FortiGate' icon and a list of HTTP headers:

```
HTTP/1.1 200 OK
Content-Encoding: gzip
Content-Type: text/html
ETag: 5ac9d822c23fd5f7e72cc3021f506c3a
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=15552000
Date: Thu, 23 Jan 2025 03:25:03 GMT
Connection: keep-alive
Transfer-Encoding: chunked
```

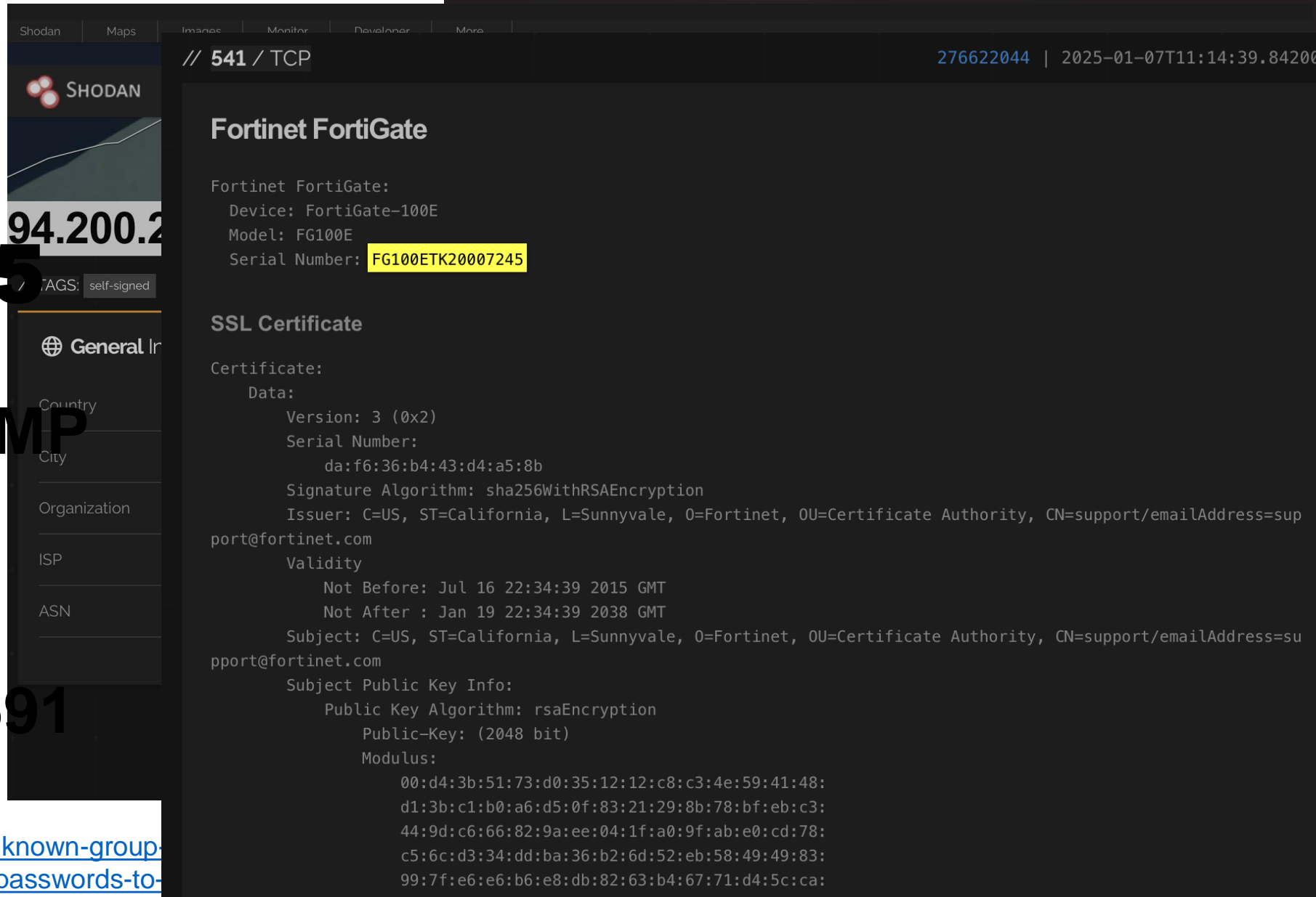
Zdroj: <https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html>

15.1.2025

Password DUMP

Authentication bypass

CVE-2024-55591



Shodan // 541 / TCP 276622044 | 2025-01-07T11:14:39.84200

SHODAN

Fortinet FortiGate

Fortinet FortiGate:
Device: FortiGate-100E
Model: FG100E
Serial Number: **FG100ETK20007245**

SSL Certificate

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
da:f6:36:b4:43:d4:a5:8b
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate Authority, CN=support/emailAddress=support@fortinet.com
Validity
Not Before: Jul 16 22:34:39 2015 GMT
Not After : Jan 19 22:34:39 2038 GMT
Subject: C=US, ST=California, L=Sunnyvale, O=Fortinet, OU=Certificate Authority, CN=support/emailAddress=support@fortinet.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:d4:3b:51:73:d0:35:12:12:c8:c3:4e:59:41:48:
d1:3b:c1:b0:a6:d5:0f:83:21:29:8b:78:bf:eb:c3:
44:9d:c6:66:82:9a:ee:04:1f:a0:9f:ab:e0:cd:78:
c5:6c:d3:34:dd:ba:36:b2:6d:52:eb:58:49:49:83:
99:7f:e6:e6:b6:e8:db:82:63:b4:67:71:d4:5c:ca:

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

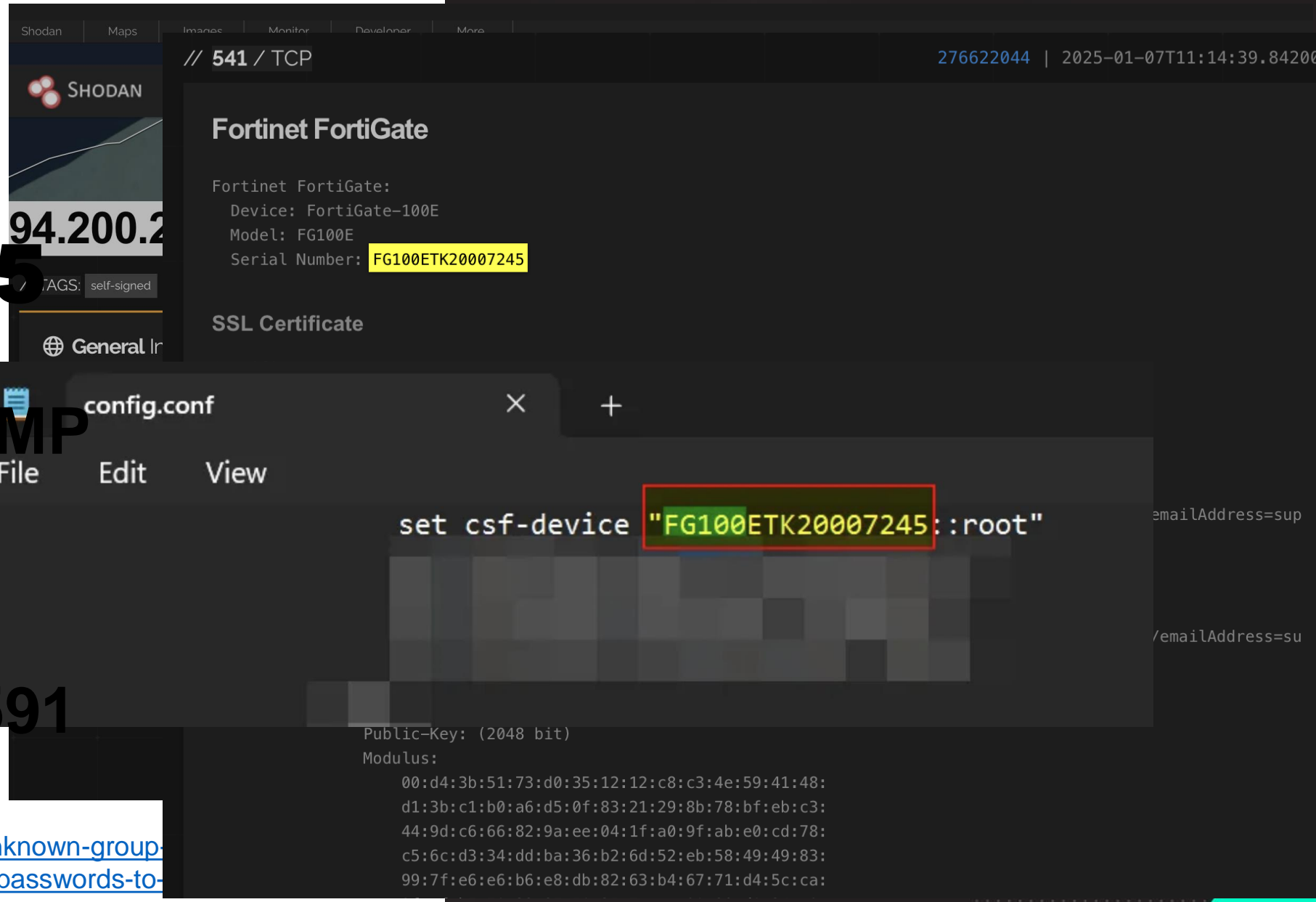
15.1.2025

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>



The screenshot shows a Shodan search result for a Fortinet FortiGate device. The device details include: Device: FortiGate-100E, Model: FG100E, and Serial Number: FG100ETK20007245. Below this, an SSL Certificate section is visible. A configuration file dump (config.conf) is shown, containing the line: `set csf-device "FG100ETK20007245::root"`. The serial number and the password in the configuration file are highlighted with red boxes. The background of the screenshot is dark with a teal header.

15?.1.2025

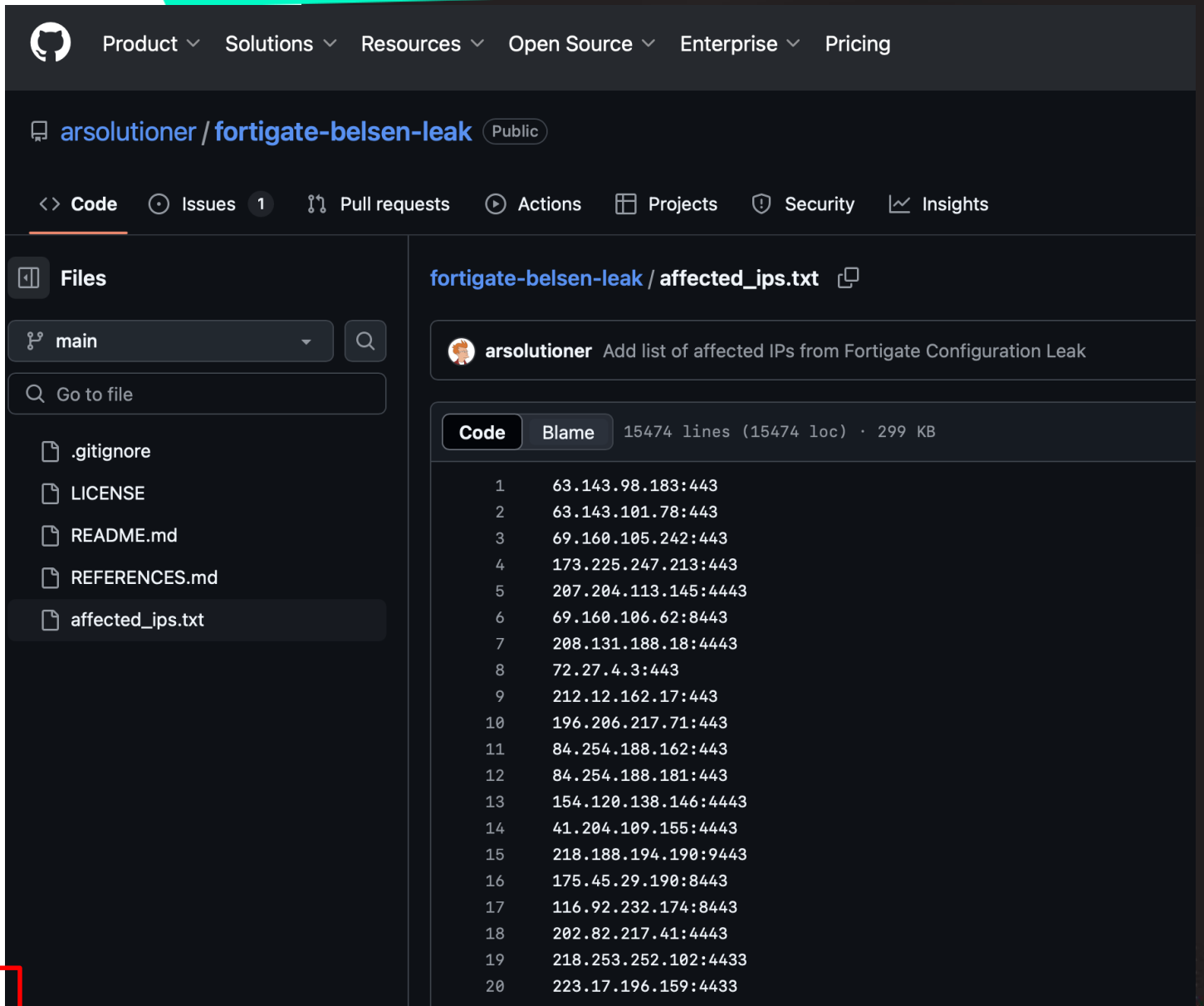
Password DUMP

Authentication

bypass

CVE-2024-55591

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



The screenshot shows a GitHub repository page for 'arsolutioner/fortigate-belsen-leak'. The repository is public and has 1 issue, 0 pull requests, 0 actions, 0 projects, 0 security issues, and 0 insights. The file 'affected_ips.txt' is selected in the file browser, showing a list of 20 IP addresses. The commit message is 'Add list of affected IPs from Fortigate Configuration Leak' by 'arsolutioner'.

Product Solutions Resources Open Source Enterprise Pricing

arsolutioner / fortigate-belsen-leak Public

Code Issues 1 Pull requests Actions Projects Security Insights

Files

main

Go to file

- .gitignore
- LICENSE
- README.md
- REFERENCES.md
- affected_ips.txt

fortigate-belsen-leak / affected_ips.txt

arsolutioner Add list of affected IPs from Fortigate Configuration Leak

Code Blame 15474 lines (15474 loc) · 299 KB

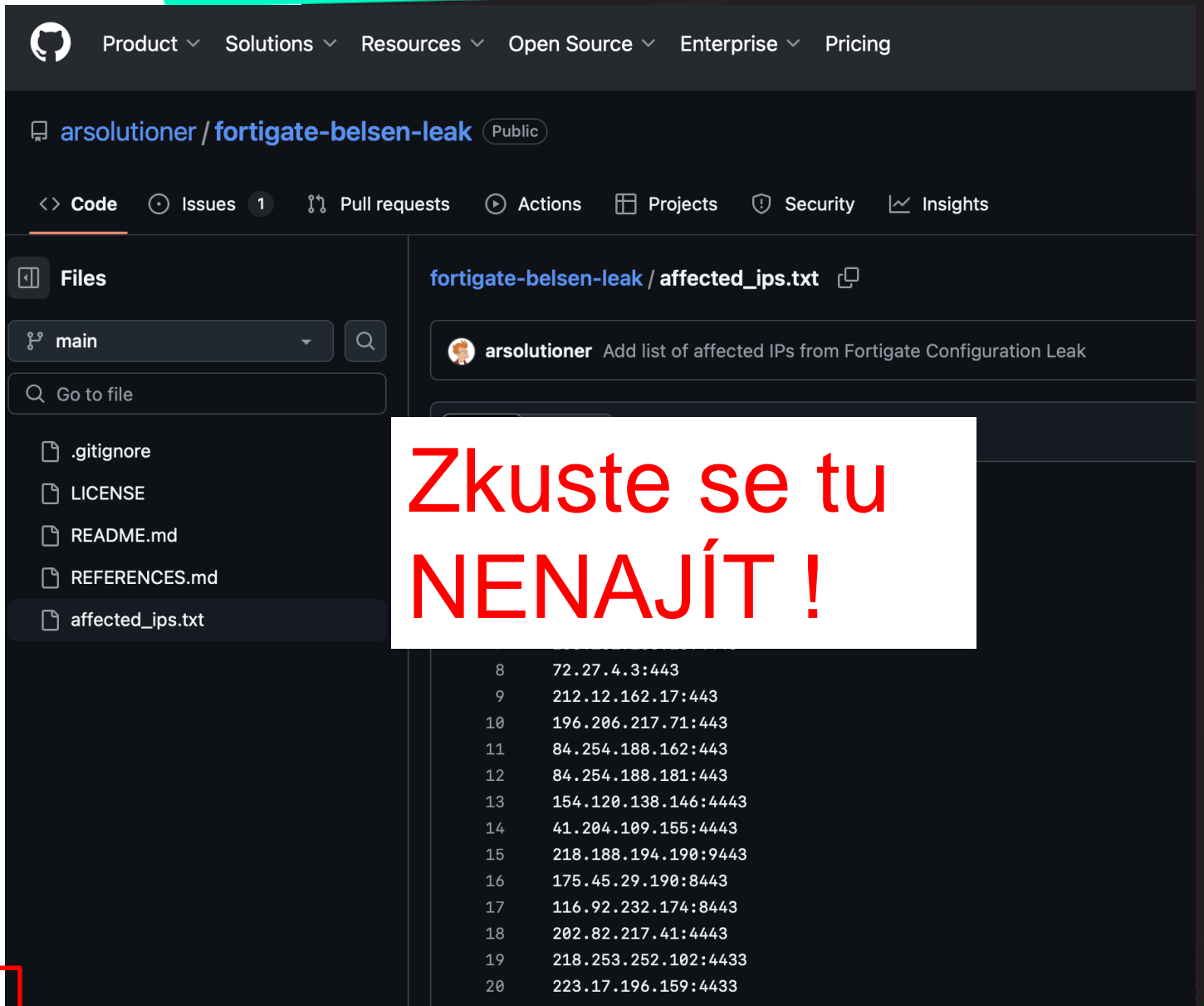
Line	IP Address
1	63.143.98.183:443
2	63.143.101.78:443
3	69.160.105.242:443
4	173.225.247.213:443
5	207.204.113.145:4443
6	69.160.106.62:8443
7	208.131.188.18:4443
8	72.27.4.3:443
9	212.12.162.17:443
10	196.206.217.71:443
11	84.254.188.162:443
12	84.254.188.181:443
13	154.120.138.146:4443
14	41.204.109.155:4443
15	218.188.194.190:9443
16	175.45.29.190:8443
17	116.92.232.174:8443
18	202.82.217.41:4443
19	218.253.252.102:4433
20	223.17.196.159:4433

15?.1.2025

Password DUMP

Authentication bypass CVE-2024-55591

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



The screenshot shows a GitHub repository page for 'arsolutioner/fortigate-belsen-leak'. The repository is public and has one issue. The 'affected_ips.txt' file is highlighted in the file list. The content of the file is a list of IP addresses with their corresponding ports, each on a new line, numbered 8 through 20.

```
8 72.27.4.3:443
9 212.12.162.17:443
10 196.206.217.71:443
11 84.254.188.162:443
12 84.254.188.181:443
13 154.120.138.146:4443
14 41.204.109.155:4443
15 218.188.194.190:9443
16 175.45.29.190:8443
17 116.92.232.174:8443
18 202.82.217.41:4443
19 218.253.252.102:4433
20 223.17.196.159:4433
```

**Zkuste se tu
NENAJÍT !**



Jak se nedostat na seznam!!! ?

Jak se nedostat na „seznam“ ?

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

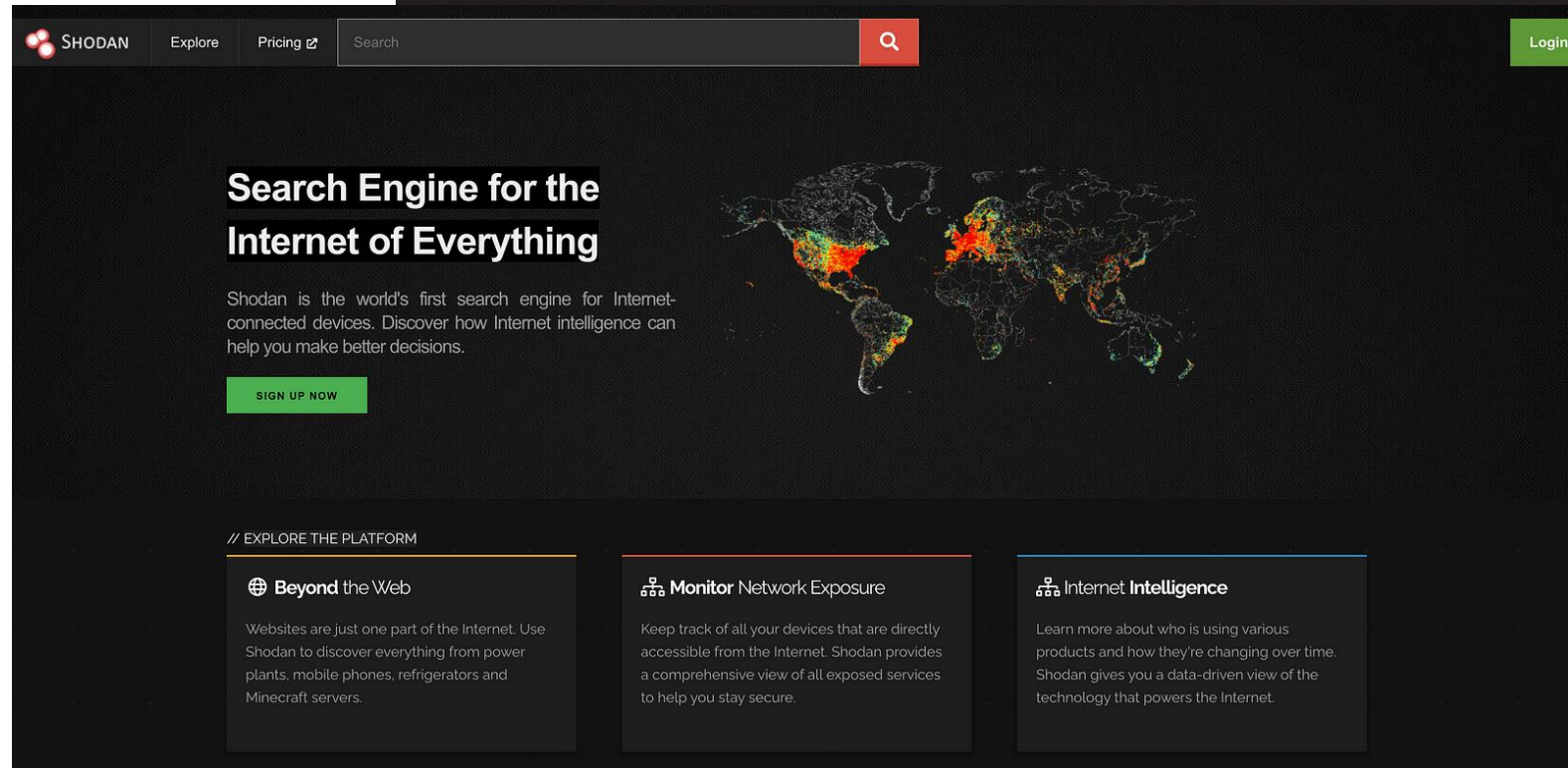


Ochrana perimetru



Shodan.io

ZDARMA



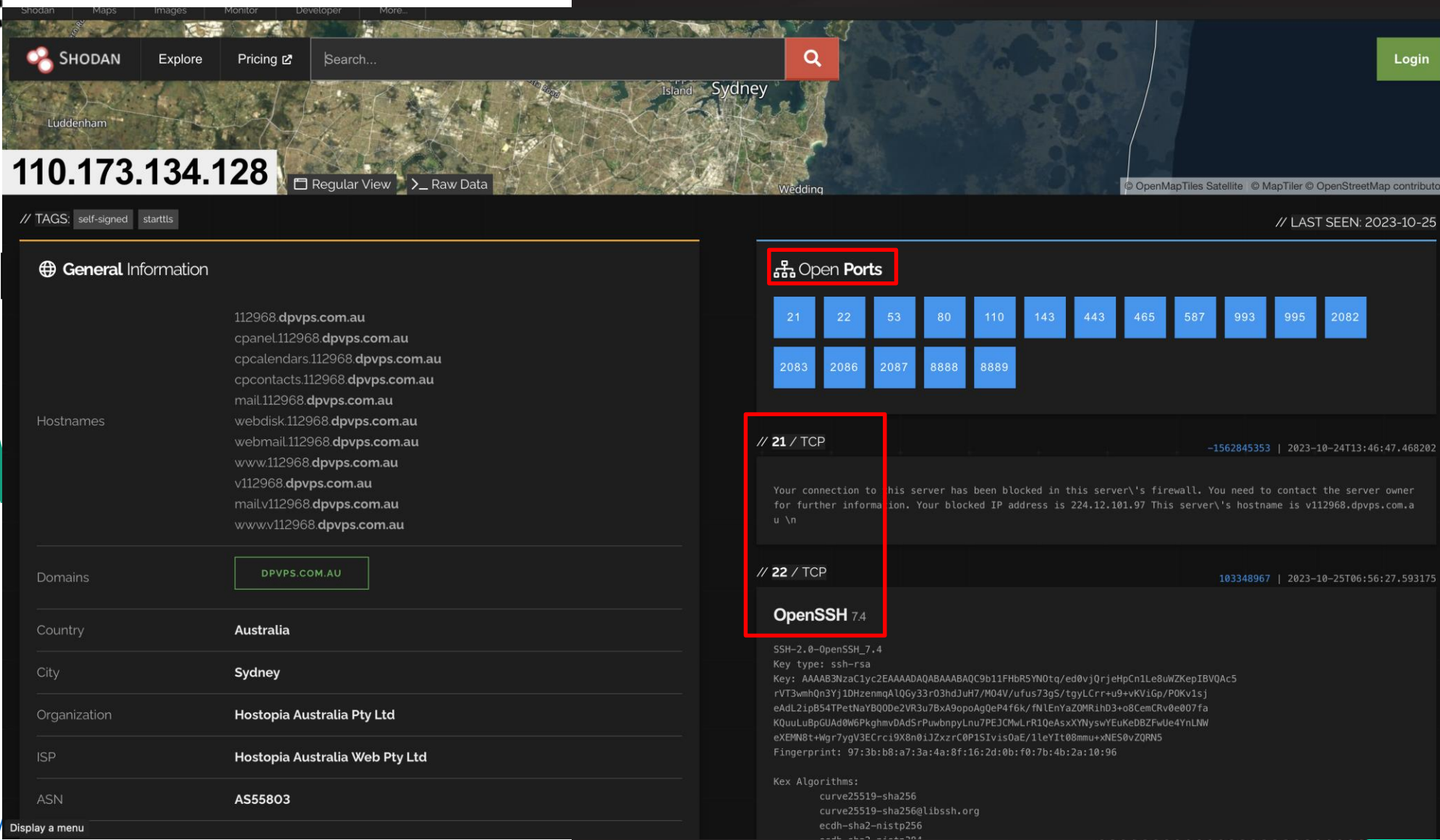
The screenshot shows the Shodan.io homepage with a dark theme. At the top, there is a navigation bar with the Shodan logo, 'Explore', 'Pricing', a search bar, and a 'Login' button. The main heading reads 'Search Engine for the Internet of Everything'. Below this, a paragraph describes Shodan as the world's first search engine for Internet-connected devices. A 'SIGN UP NOW' button is prominently displayed. To the right, there is a world map with glowing nodes. Below the main content, a section titled 'EXPLORE THE PLATFORM' features three cards: 'Beyond the Web', 'Monitor Network Exposure', and 'Internet Intelligence', each with a brief description of its capabilities.

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

Shodan

ZDARMA

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



The screenshot shows a Shodan search result for IP 110.173.134.128. The interface includes a search bar with the IP address, a map of the location (Sydney, Australia), and a list of open ports. The 'Open Ports' section is highlighted with a red box, showing ports 21 and 22. The details for port 21 are also highlighted with a red box, indicating a connection to the server has been blocked by a firewall. The details for port 22 show it is OpenSSH 7.4.

110.173.134.128

Regular View Raw Data

TAGS: self-signed starttls // LAST SEEN: 2023-10-25

General Information

112968.dpvps.com.au
cpanel.112968.dpvps.com.au
cpcalendars.112968.dpvps.com.au
cpcontacts.112968.dpvps.com.au
mail.112968.dpvps.com.au

Hostnames
webdisk.112968.dpvps.com.au
webmail.112968.dpvps.com.au
www.112968.dpvps.com.au
v112968.dpvps.com.au
mail.v112968.dpvps.com.au
www.v112968.dpvps.com.au

Domains
DPVPS.COM.AU

Country
Australia

City
Sydney

Organization
Hostopia Australia Pty Ltd

ISP
Hostopia Australia Web Pty Ltd

ASN
AS55803

Open Ports

21	22	53	80	110	143	443	465	587	993	995	2082
2083	2086	2087	8888	8889							

// 21 / TCP -1562845353 | 2023-10-24T13:46:47.468202

Your connection to this server has been blocked in this server's firewall. You need to contact the server owner for further information. Your blocked IP address is 224.12.101.97 This server's hostname is v112968.dpvps.com.au \n

// 22 / TCP 103348967 | 2023-10-25T06:56:27.593175

OpenSSH 7.4

SSH-2.0-OpenSSH_7.4
Key type: ssh-rsa
Key: AAAAB3NzaC1yc2EAAAADAQABAAQCA9b11FHbR5YN0tq/ed0vjQrjeHpcN1e8uWZKepIBV0Ac5rVT3wmhQn3Yj1DHzenmqALQgy33r03hdJuH7/M04V/ufus73gS/tygLcrr+u9+uKViGp/P0Kv1sj eAdL2ipB54TPetNaYBQ0de2VR3u7BxA9opoAg0eP4f6k/fNLEnYaZOMRi1hd3+o8CemCRv0e007fa KQuuLUbpGUAd0W6PkgmvdAd5rPuwbnpYLnu7PEJCMwLrR1QeAsxYNYswYEuKeDBZFwUe4YnLNN eXEMN8t+Wgr7ygV3ECrci9X8n0iJZzrC0P1SIVis0aE/1leYIt08mmu+xNES0vZQRN5
Fingerprint: 97:3b:b8:a7:3a:4a:8f:16:2d:0b:f0:7b:4b:2a:10:96

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp256



Zabezpečení záloh

Jak zabezpečit zálohy?

Správně nastavená zálohovací architektura znemožní útočnickovi 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



Multifaktorové zabezpečení

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



Potřebujete pomoci?



Alinet

Cyber Security, **Ransomware Incident Response**



Jakub Alimov

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