CYBERОК

Как бы я взломал...Рунет

Первушин Игорь

Цель

Как бы я взломал Рунет

Как бы я сделал его безопаснее

Начнем с масштабов

1. >6.5M/45M IP-адресов
2. >71.7M значимых сервисов
3. >63.5M HTTP-сервисов
4. >125 различных протоколов
5. >3000 уникальных типов ПО

Не нужон нам этот...

censys | Hosts | location.country:russia and services.port:10050

Results | Try CensysGPT Beta

Host Filters

Labels:

Hosts

Results: 517 Time: 1.35s

SHODAN | country:"RU" port:10050

Note: No results found

location.country: "RU" and port: 10050

IP-адрес | Порт | Протокол | Дом

Всего хостов: 135 567

Города

Moscow	53K
St Petersburg	38K
Yekaterinburg	10K
Novosibirsk	8 127
Magnitogorsk	5 931
Krasnodar	4 827
Samara	3 334
Armavir	2 741
Chelyabinsk	2 121
Kaliningrad	2 025

Хост

83.69.237.9

Российская Федерация, Москва

17.03.2024 20:40:21 GMT+3

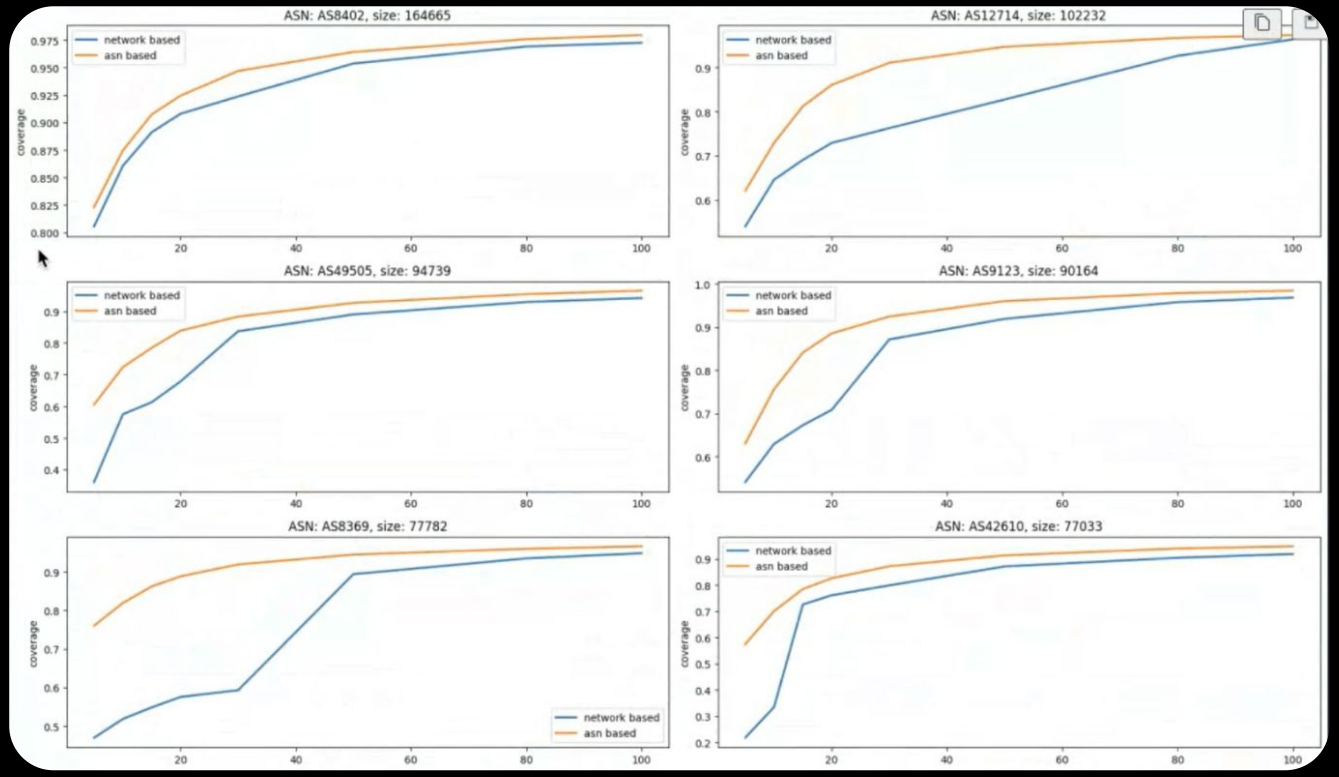
185.12.92.55

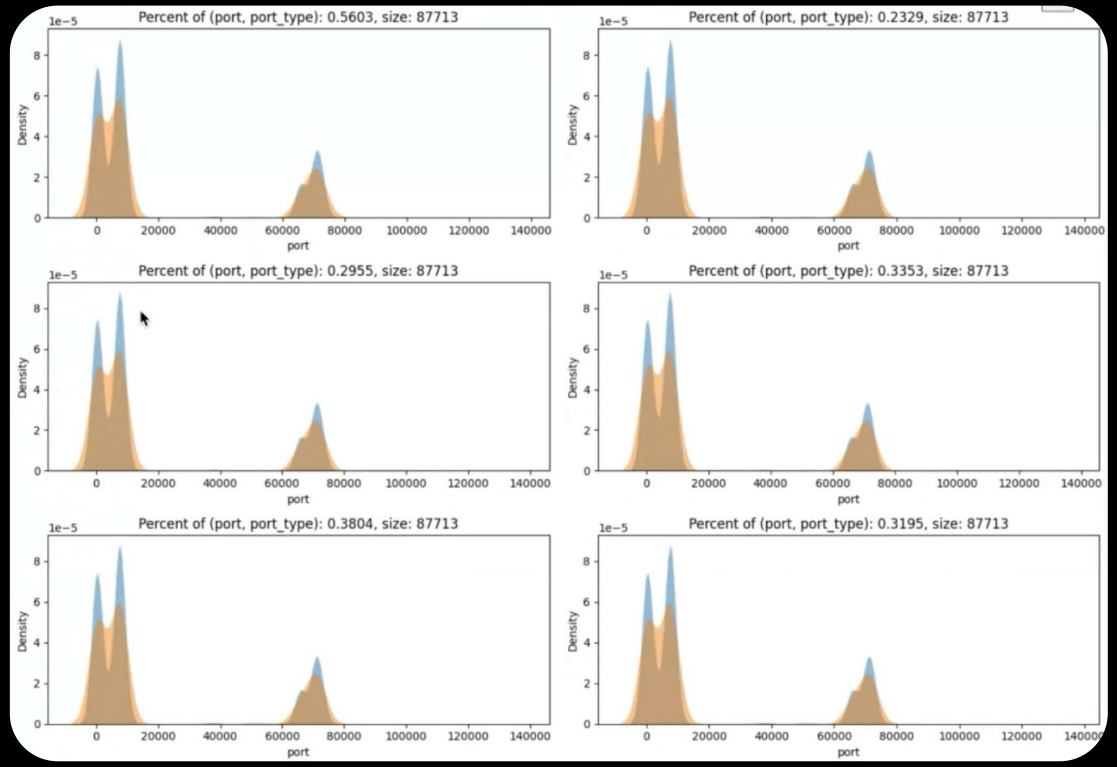
Российская Федерация, Москва

17.03.2024 20:40:21 GMT+3

Что нам помогает?

Можно ли стучаться не во все двери?





Что нам помогает?

Пусть программное обеспечение определится само...


```
"is_processed": false,
"num_of_matches": 177,
"re": "X-Powered-By: \\ Ratchet/0\\.4\\..*",
"re_match": "Ratchet/0.4.1",
"readability_test": {
    "flesch_reading": false,
    "is_first_upper": true,
    "ner": true,
    "num_is_alpha": true,
    "punct_ratio": false,
    "tokens_ratio": 10.0
},
"sample": [
    "HTTP/1.1 426 Upgrade header MUST be provided\r\nConnection:
    "HTTP/1.1 426 Upgrade header MUST be provided\r\nConnection:
    "HTTP/1.1 426 Upgrade header MUST be provided\r\nConnection:
    "HTTP/1.1 426 Upgrade header MUST be provided\r\nConnection:
    "HTTP/1.1 426 Upgrade header MUST be provided\r\nConnection:
]
```


```
0. Server: Synapse/1.96.1 is_processed=False Matches: 56
1. Server: Synapse/1.90.0 is_processed=False Matches: 8
2. Server: JAWS/1.0 is_processed=False Matches: 32
3. Server: Werkzeug/3.0.1 Python/3.12.1 is_processed=False Matches: 77
4. Server: Nimble/3.7.11-9 is_processed=False Matches: 51
5. X-Powered-By: Ratchet/0.4.1 is_processed=False Matches: 177
6. Server: IPC/2.0.0 is_processed=False Matches: 466
7. Server: Brovotech/2.0.0 is_processed=False Matches: 212
8. Server: Airee/Cloud is_processed=False Matches: 251
9. Server: BaseHTTP/0.6 Python/3.10.7 is_processed=True Matches: 38
10. Server: Microsoft-IIS/10.0 is_processed=False Matches: 97
11. X-Powered-By: ASP.NET is_processed=True Matches: 71
12. Server: WSGIServer/0.2 CPython/3.8.10 is_processed=False Matches: 46
```


```
-Version: 13\r\nUpgrade: websocket\r\nX-Powered-By: Ratchet/0.4.4",
-Version: 13\r\nUpgrade: websocket\r\nX-Powered-By: Ratchet/0.4.4",
-Version: 13\r\nUpgrade: websocket\r\nX-Powered-By: Ratchet/0.4.4",
-Version: 13\r\nUpgrade: websocket\r\nX-Powered-By: Ratchet/0.4.4",
-Version: 13\r\nUpgrade: websocket\r\nX-Powered-By: Ratchet/0.4.4"
```

Особенности национальной охоты

1	Трендовые уязвимости в международном сегменте
2	Типовое для региона программное обеспечение
3	Зачастую уязвимые технологии
4	Порты с «характером»
5	То, что пытаются скрыть

Трендовые уязвимости

Последние случаи:

1. TeamCity (CVE-2024-27198)
2. ConnectWise (CVE-2024-1709)
3. Fortinet (CVE-2024-21762)
4. Wordpress (...)
5. Gitlab (CVE-2023-7028)

Трендовые уязвимости

TeamCity (CVE-2024-27198)

GitLab (CVE-2023-5009)

Типовое для региона ПО

- 1C-Bitrix (уязвимости, мисконфиги, следы эксплуатации)
- Trueconf (CVE-2022-46764)
- Terrasoft/Creatio (BDU-2023-04519)
- Websoft HCM (BDU-2022-06939)

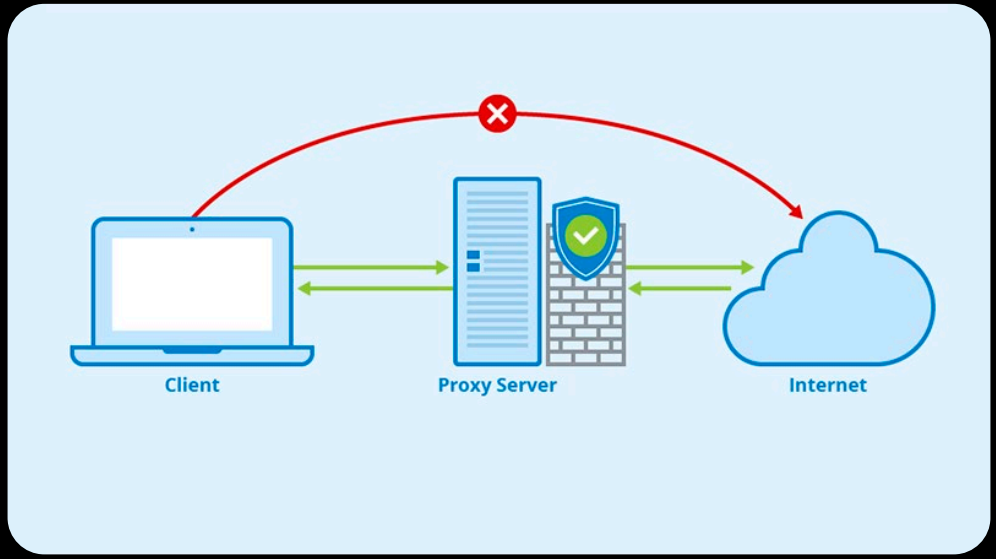
Типовое для региона ПО

Bitrix

Trueconf (CVE-2022-46764)

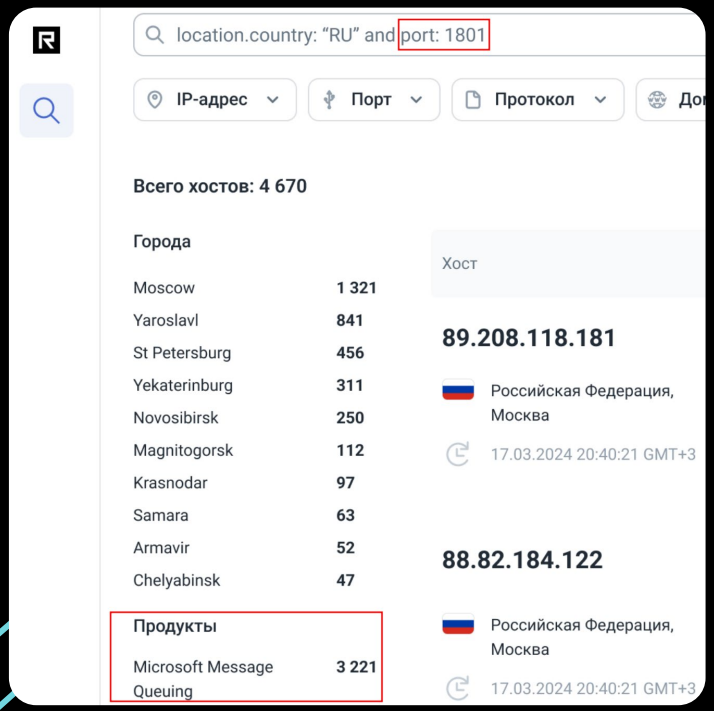
Зачастую уязвимые технологии

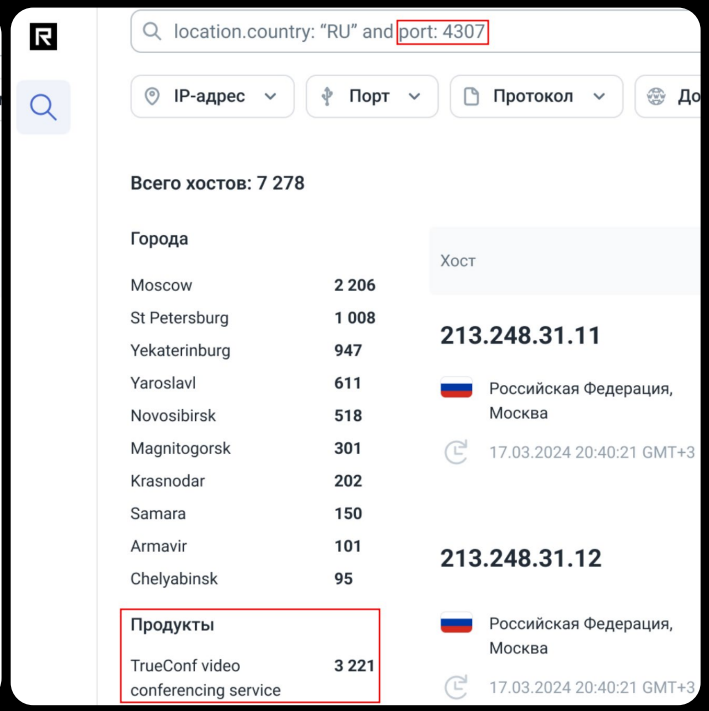
1. Mikrotik (CVE-2018-14847) – 94000+
2. Hikvision (CVE-2017-7921, CVE-2021-36260) - 3000/75000+
3. Dahua (CVE-2021-33044) - 10000+
4. Xiongmai (CVE-2017-7577, CVE-2018-10088) - 900/10000+

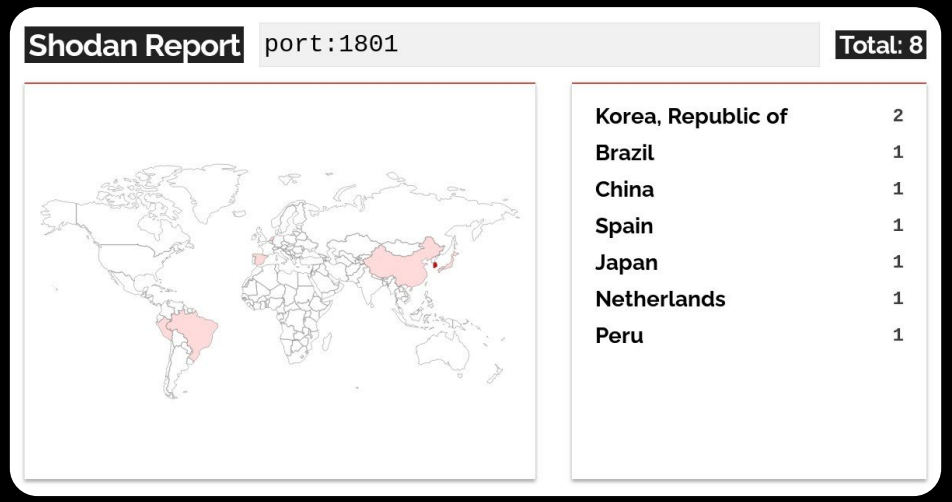


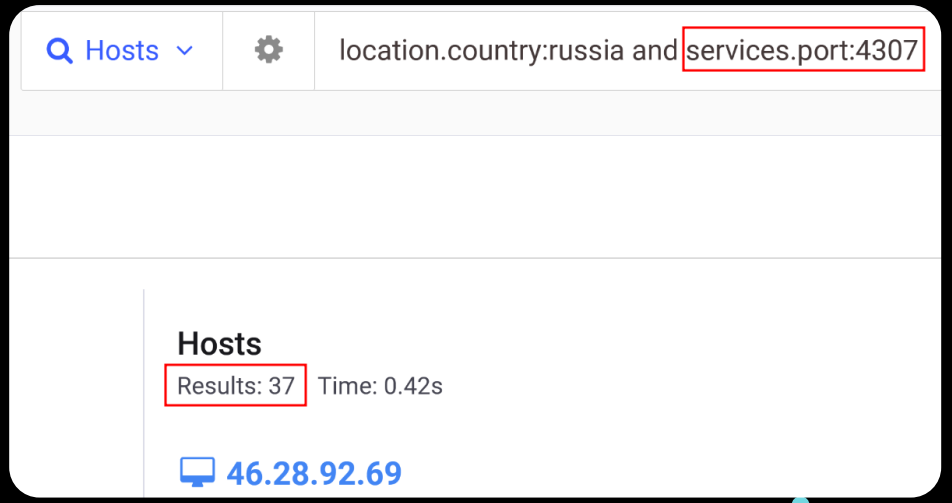
Порты с характерным ПО

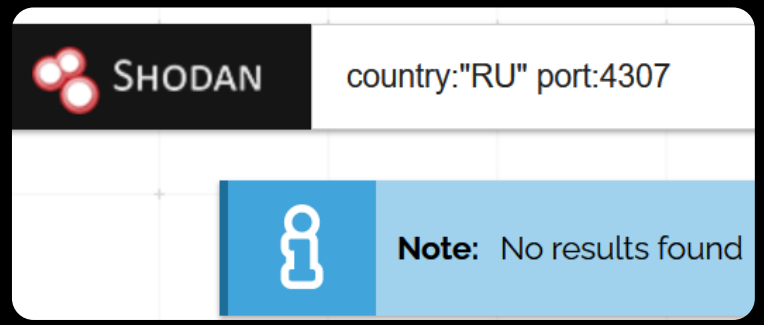
- 1801 – msmq (CVE-2023-21554)
- 4307 – Trueconf (CVE-2022-46764)
- 10050 – Zabbix agent
- 7547 - ?



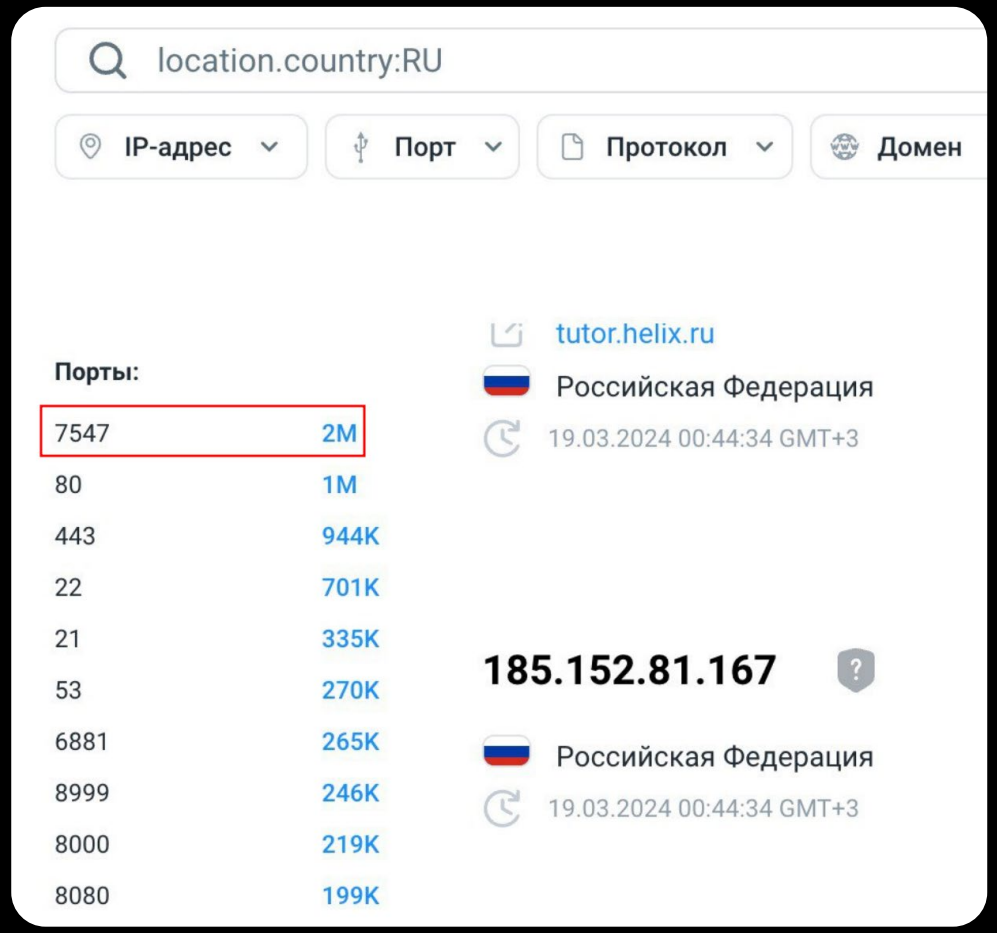


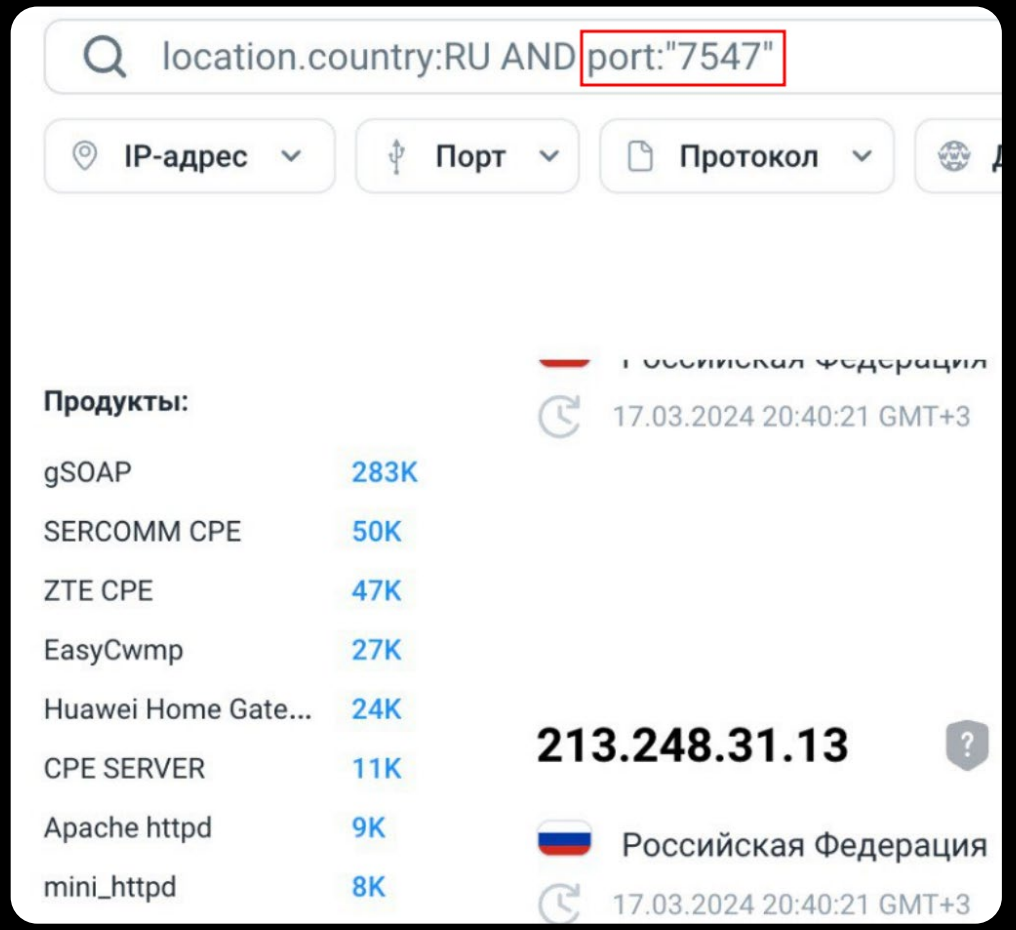




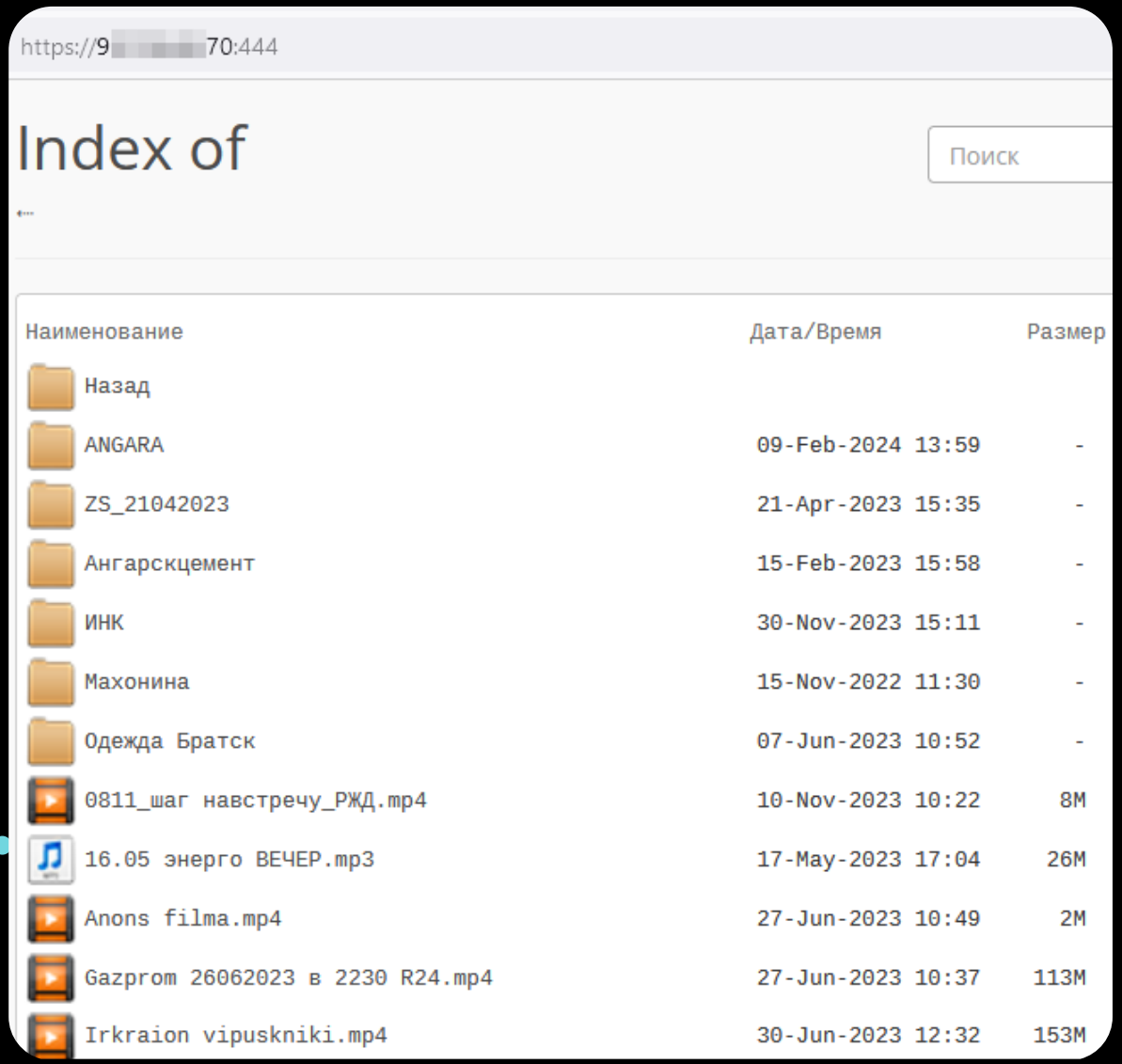


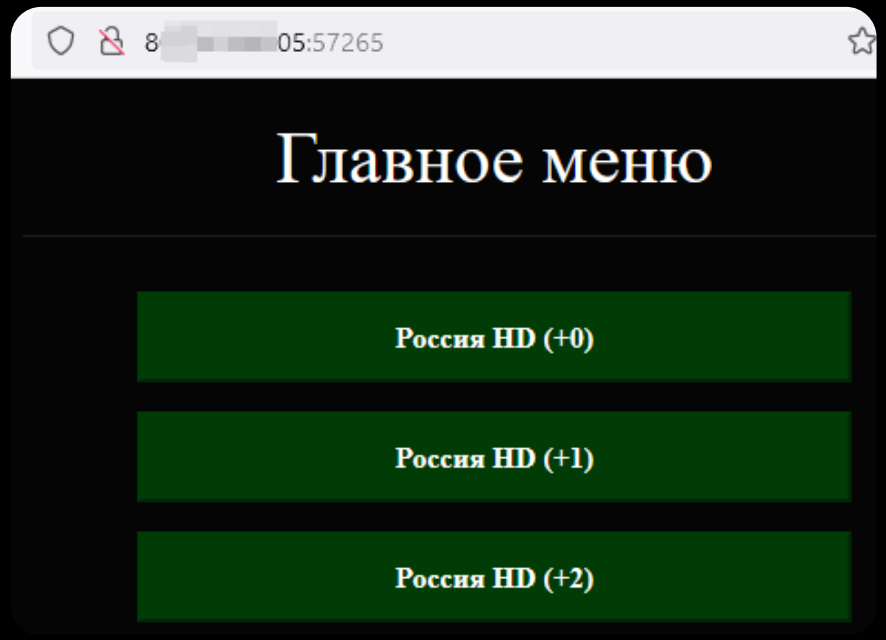
Порты особого назначения

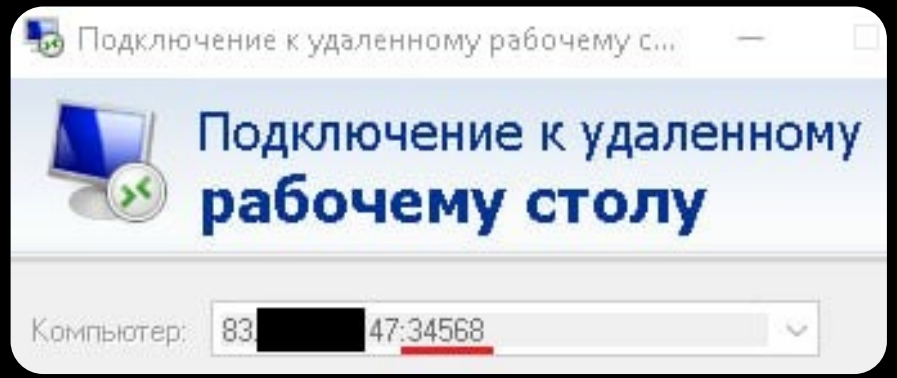




То, что пытаются скрыть





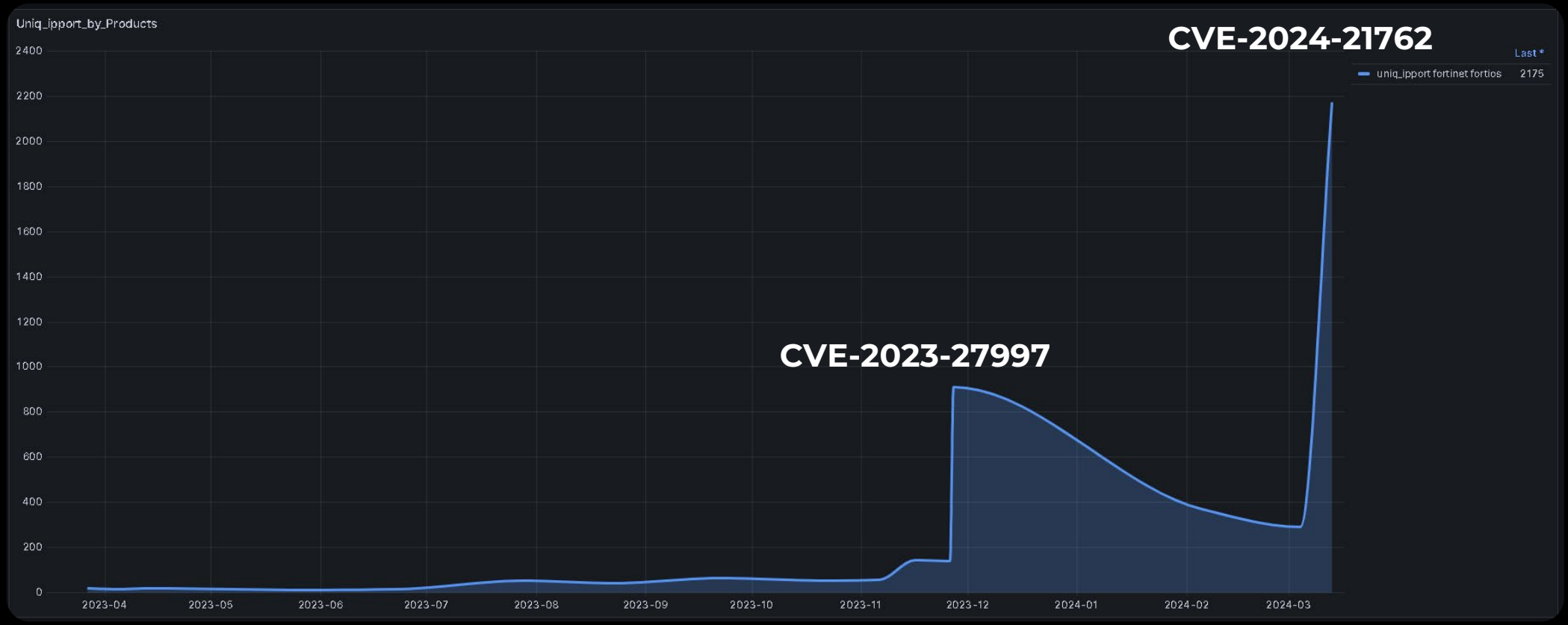


Про результаты

1. Организационные выводы
2. Технические выводы
3. Наблюдение за статистикой

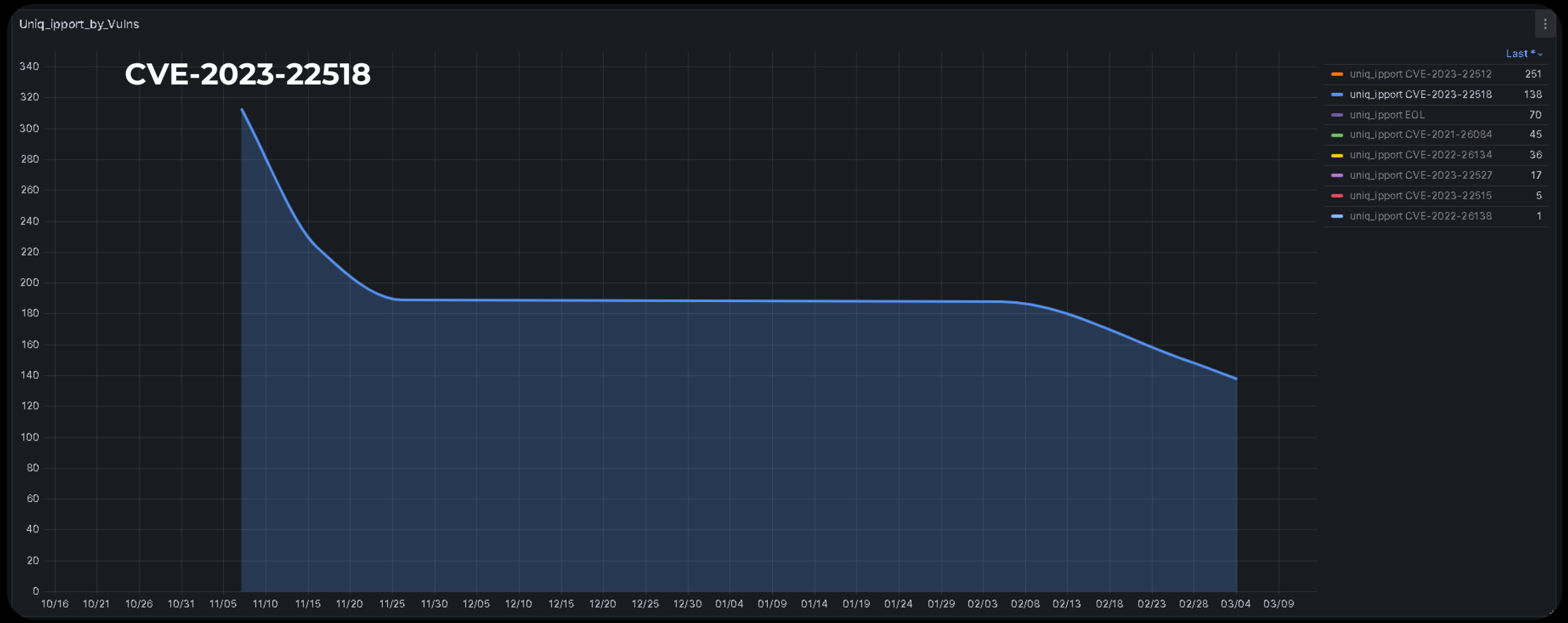
Трендовые уязвимости

Fortinet



Трендовые уязвимости

Atlassian Confluence



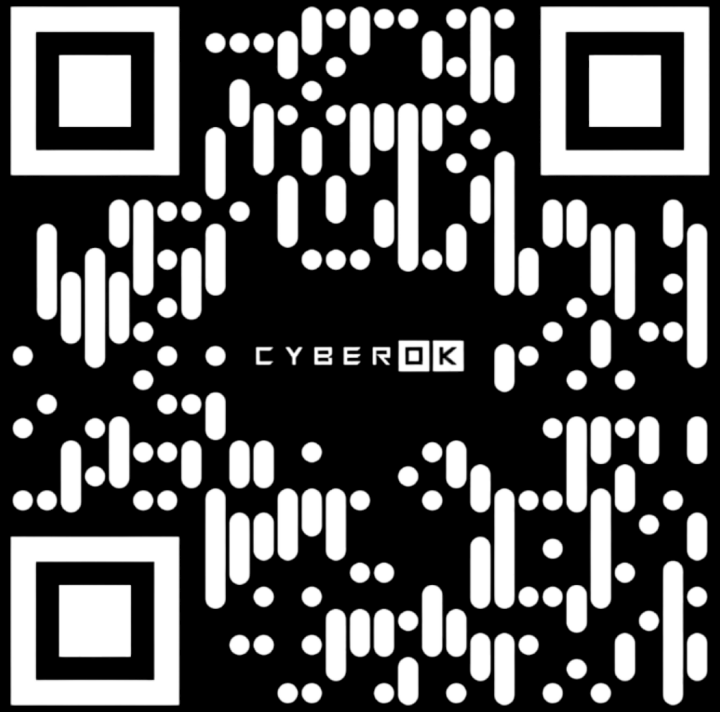

Статистика по нарушениям ИБ в CMS 1C Bitrix
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
Уязвимости (vote, htmleditor)
Подтвержденный бэкдор
Активный дефейс
26.05.2023
29.05.2023
01.06.2023
04.06.2023
07.06.2023
10.06.2023
13.06.2023
16.06.2023
19.06.2023
22.06.2023
25.06.2023
28.06.2023
01.07.2023
04.07.2023
07.07.2023
10.07.2023
13.07.2023
16.07.2023
19.07.2023
22.07.2023
25.07.2023
28.07.2023
31.07.2023
03.08.2023
06.08.2023

Типовое для региона ПО

TrueConf

Про выводы

1. Следить за новыми угрозами
2. Знать свой периметр
3. Оперативно действовать
4. Стараться не только скрываться, но и становиться безопаснее



CYBEROK

info@cyberok.ru

+7 (495) 137-7337

123112, г. Москва, Пресненская набережная, д.12

конференция РусКрипто