

CYBEROK

Как бы я взломал...Рунет

Первушин Игорь



Цель



Как бы я взломал
Рунет



Как бы я сделал
его безопаснее


Начнем с масштабов

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



Не нужен нам этот...



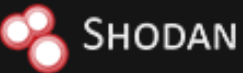


Results Try CensysGPT Beta


Host Filters

Labels:

Hosts
Results: 517 Time: 1.35s



Note: No results found




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

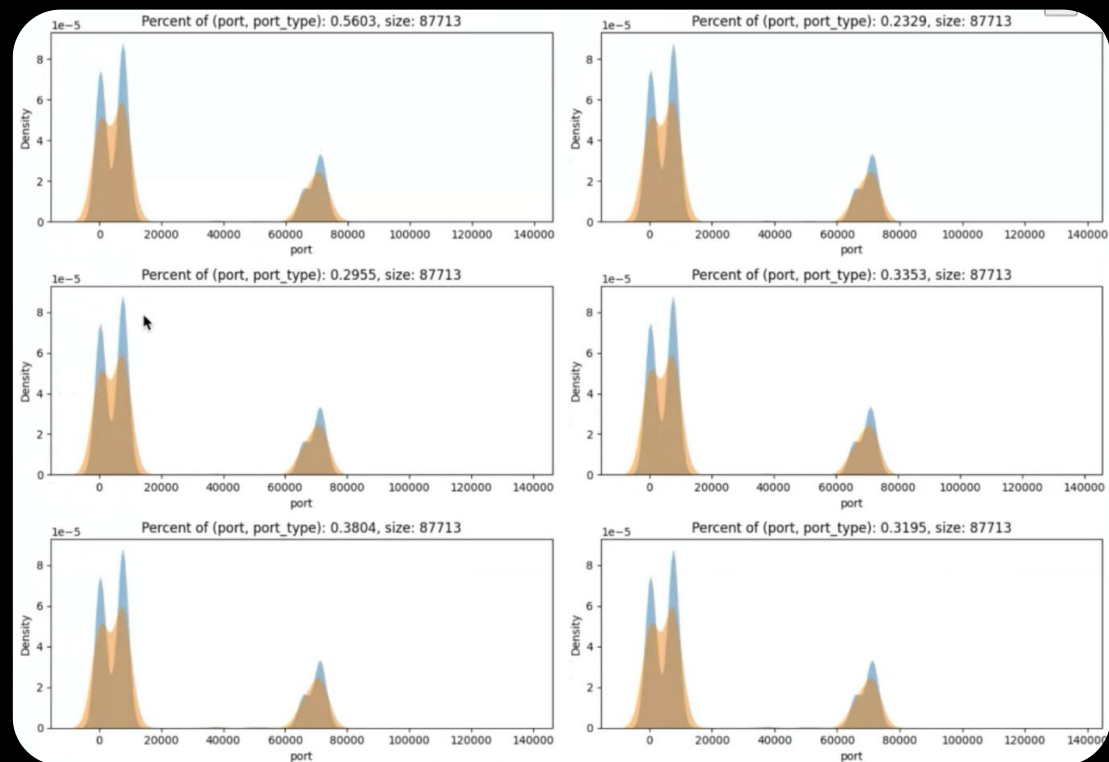
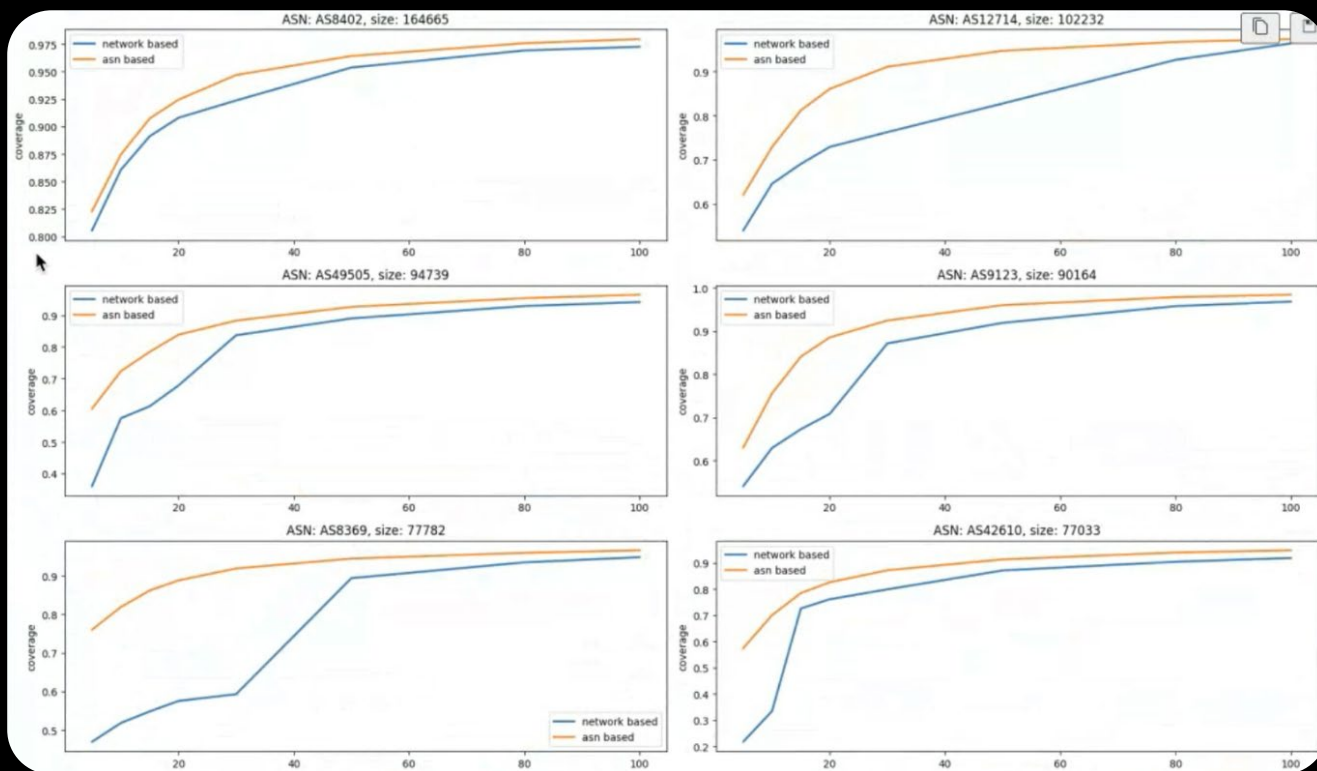
 Российская Федерация, Москва

 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

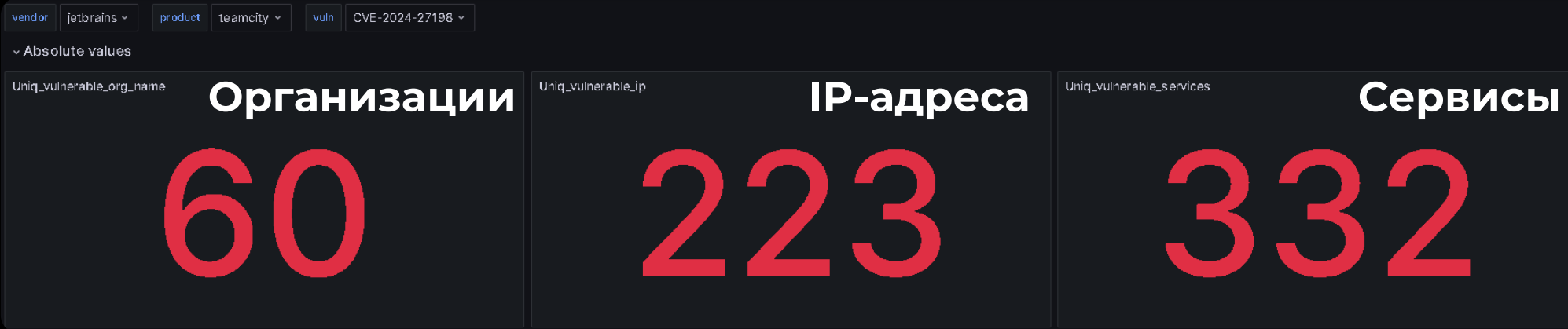
Последние случаи:

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

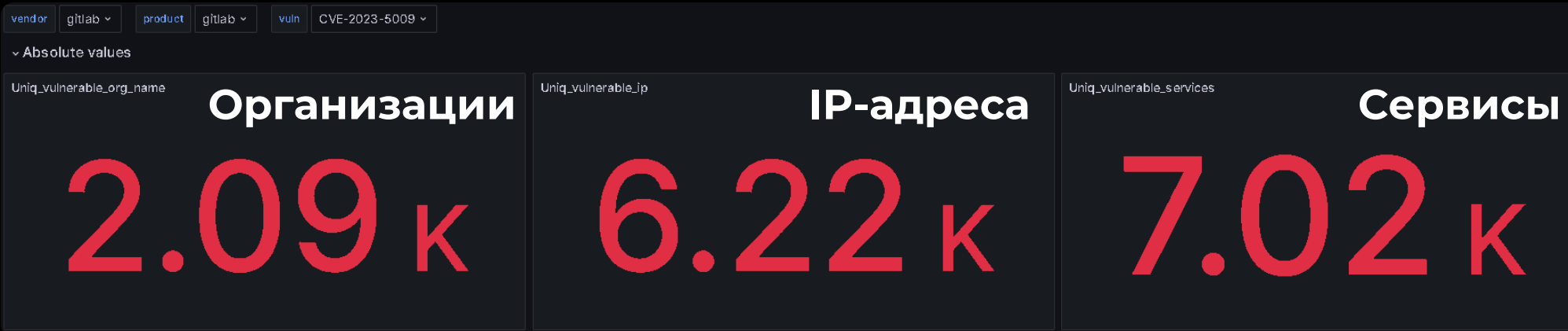


Трендовые уязвимости

TeamCity (CVE-2024-27198)



GitLab (CVE-2023-5009)





Типовое для региона ПО

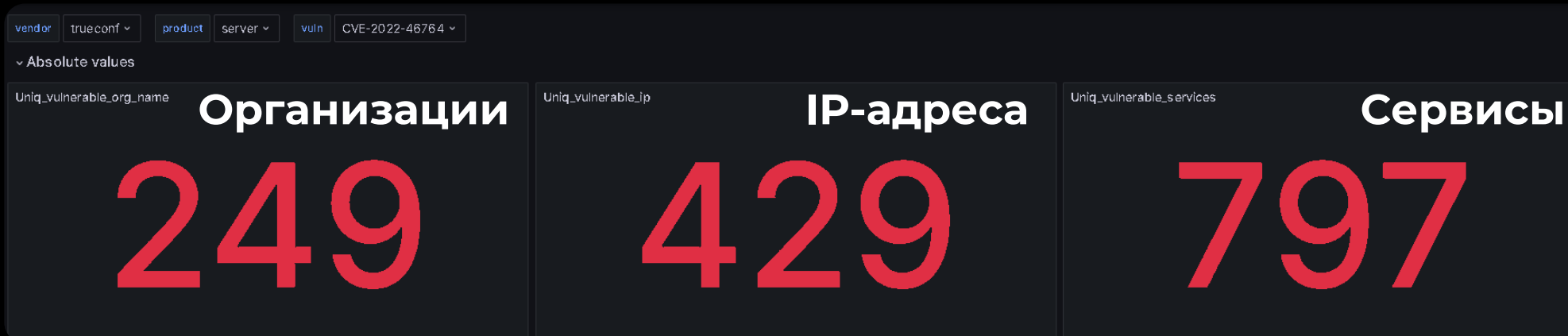
- 1С-Bitrix (уязвимости, мисконфиги, следы эксплуатации)
- Trueconf (CVE-2022-46764)
- Terrasoft/Creatio (BDU-2023-04519)
- Websoft HCM (BDU-2022-06939)

Типовое для региона ПО

Bitrix



Trueconf (CVE-2022-46764)



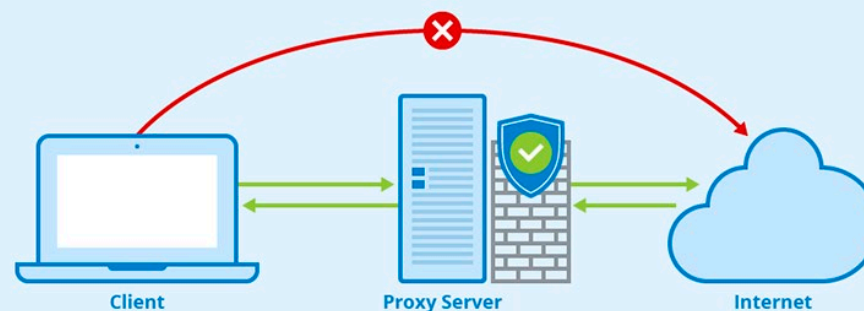
Зачастую уязвимые технологии

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 - ?

location.country: "RU" and port: 1801

Всего хостов: 4 670

Города	Хост
Moscow	1 321
Yaroslavl	841
St Petersburg	456
Yekaterinburg	311
Novosibirsk	250
Magnitogorsk	112
Krasnodar	97
Samara	63
Armavir	52
Chelyabinsk	47

89.208.118.181

Российская Федерация, Москва

17.03.2024 20:40:21 GMT+3

Продукты	Хост
Microsoft Message Queuing	3 221

88.82.184.122

Российская Федерация, Москва

17.03.2024 20:40:21 GMT+3

location.country: "RU" and port: 4307

Всего хостов: 7 278

Города	Хост
Moscow	2 206
St Petersburg	1 008
Yekaterinburg	947
Yaroslavl	611
Novosibirsk	518
Magnitogorsk	301
Krasnodar	202
Samara	150
Armavir	101
Chelyabinsk	95

213.248.31.11

Российская Федерация, Москва

17.03.2024 20:40:21 GMT+3

Продукты	Хост
TrueConf video conferencing service	3 221

213.248.31.12

Российская Федерация, Москва

17.03.2024 20:40:21 GMT+3

Shodan Report port: 1801 Total: 8

Korea, Republic of	2
Brazil	1
China	1
Spain	1
Japan	1
Netherlands	1
Peru	1

location.country: russia and services.port: 4307

Hosts

Results: 37 Time: 0.42s

46.28.92.69

SHODAN country: "RU" port: 4307

Note: No results found

Порты особого назначения

location.country:RU

IP-адрес Порт Протокол Домен

Порты:

7547	2M
80	1M
443	944K
22	701K
21	335K
53	270K
6881	265K
8999	246K
8000	219K
8080	199K

tutor.helix.ru
Российская Федерация
19.03.2024 00:44:34 GMT+3

185.152.81.167 ?

Российская Федерация
19.03.2024 00:44:34 GMT+3

location.country:RU AND port:"7547"

IP-адрес Порт Протокол Домен

Продукты:

gSOAP	283K
SERCOMM CPE	50K
ZTE CPE	47K
EasyCwmp	27K
Huawei Home Gate...	24K
CPE SERVER	11K
Apache httpd	9K
mini_httpd	8K

Российская Федерация
17.03.2024 20:40:21 GMT+3

213.248.31.13 ?

Российская Федерация
17.03.2024 20:40:21 GMT+3

То, что пытаются скрыть

https://9[redacted]70:444

Index of

Поиск

Наименование	Дата/Время	Размер
Назад		
ANGARA	09-Feb-2024 13:59	-
ZS_21042023	21-Apr-2023 15:35	-
Ангарскцемент	15-Feb-2023 15:58	-
ИНК	30-Nov-2023 15:11	-
Махонина	15-Nov-2022 11:30	-
Одежда Братск	07-Jun-2023 10:52	-
0811_шаг навстречу_РЖД.mp4	10-Nov-2023 10:22	8M
16.05 энерго ВЕЧЕР.mp3	17-May-2023 17:04	26M
Anons филма.mp4	27-Jun-2023 10:49	2M
Gazprom 26062023 в 2230 R24.mp4	27-Jun-2023 10:37	113M
Irkraion vipuskniki.mp4	30-Jun-2023 12:32	153M

8 [redacted] 05:57265

Главное меню

- Россия HD (+0)
- Россия HD (+1)
- Россия HD (+2)

Подключение к удаленному рабочему столу

Подключение к удаленному рабочему столу

Компьютер: 83 [redacted] 47:34568



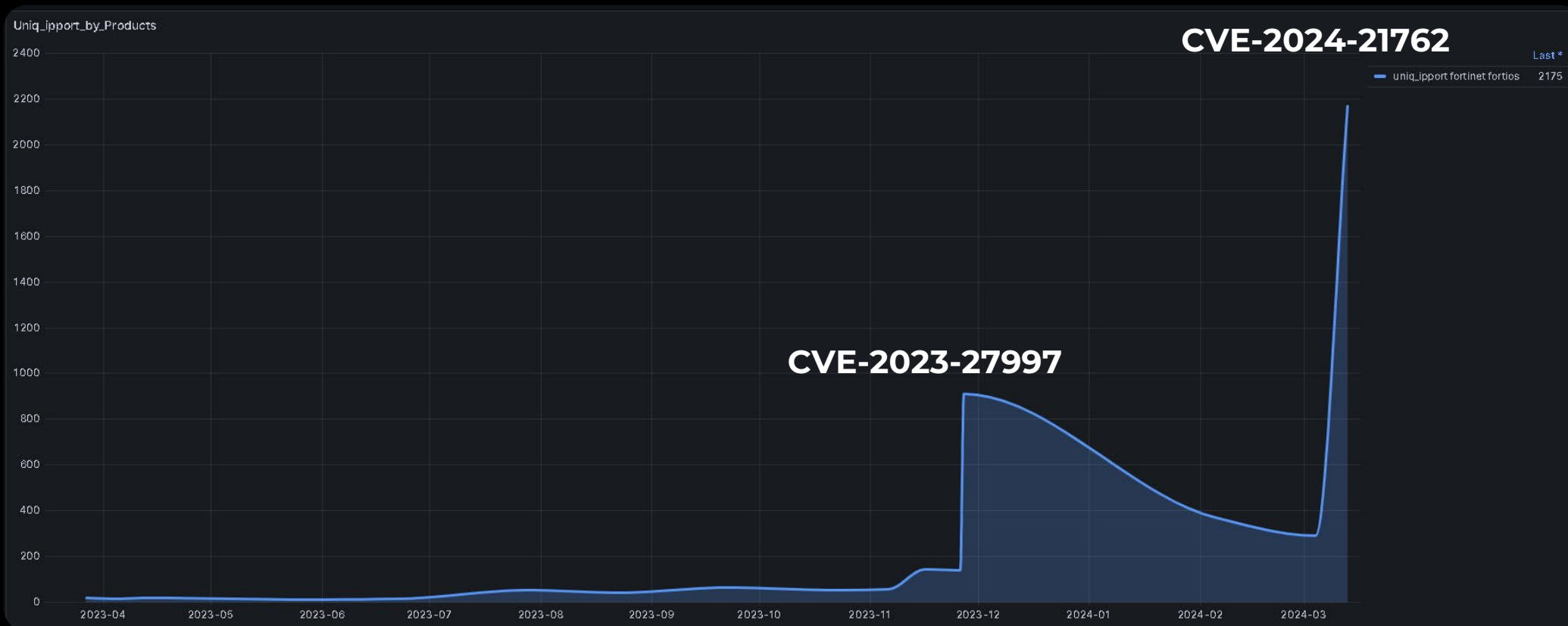


Про результаты

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

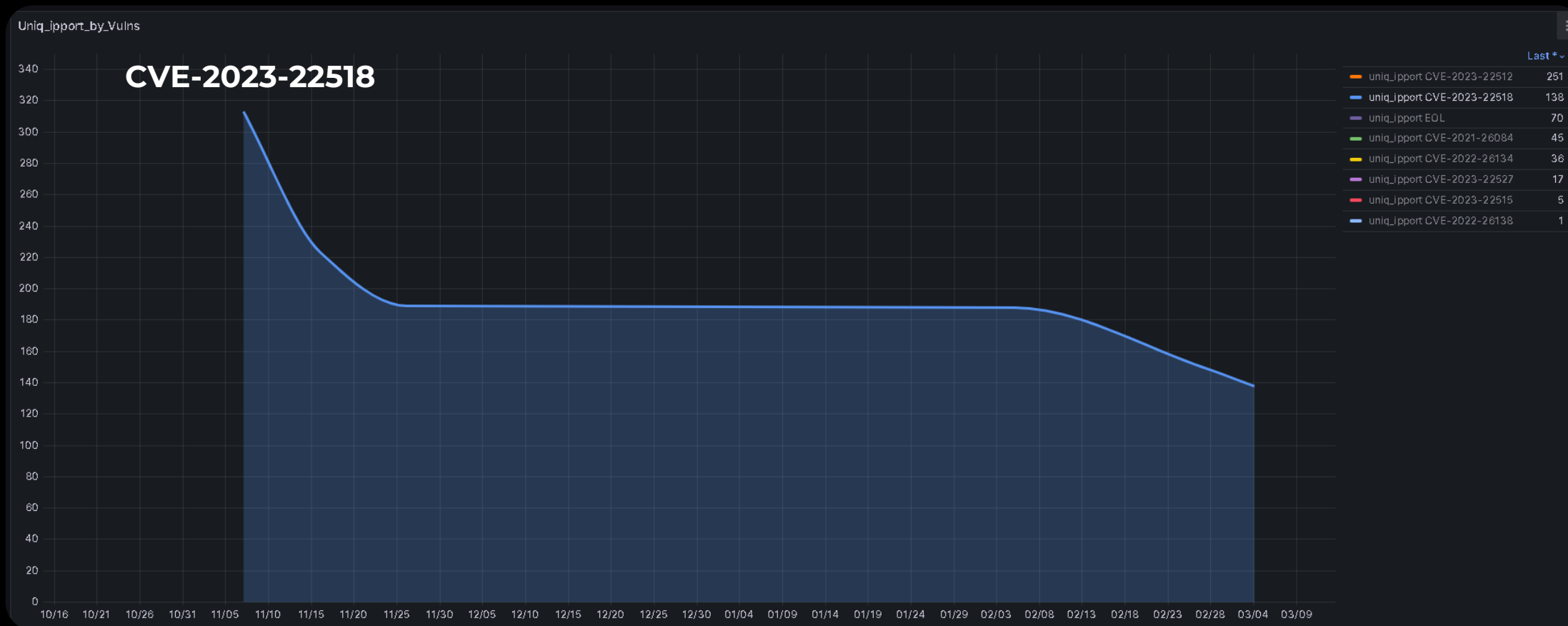
Трендовые уязвимости

Fortinet

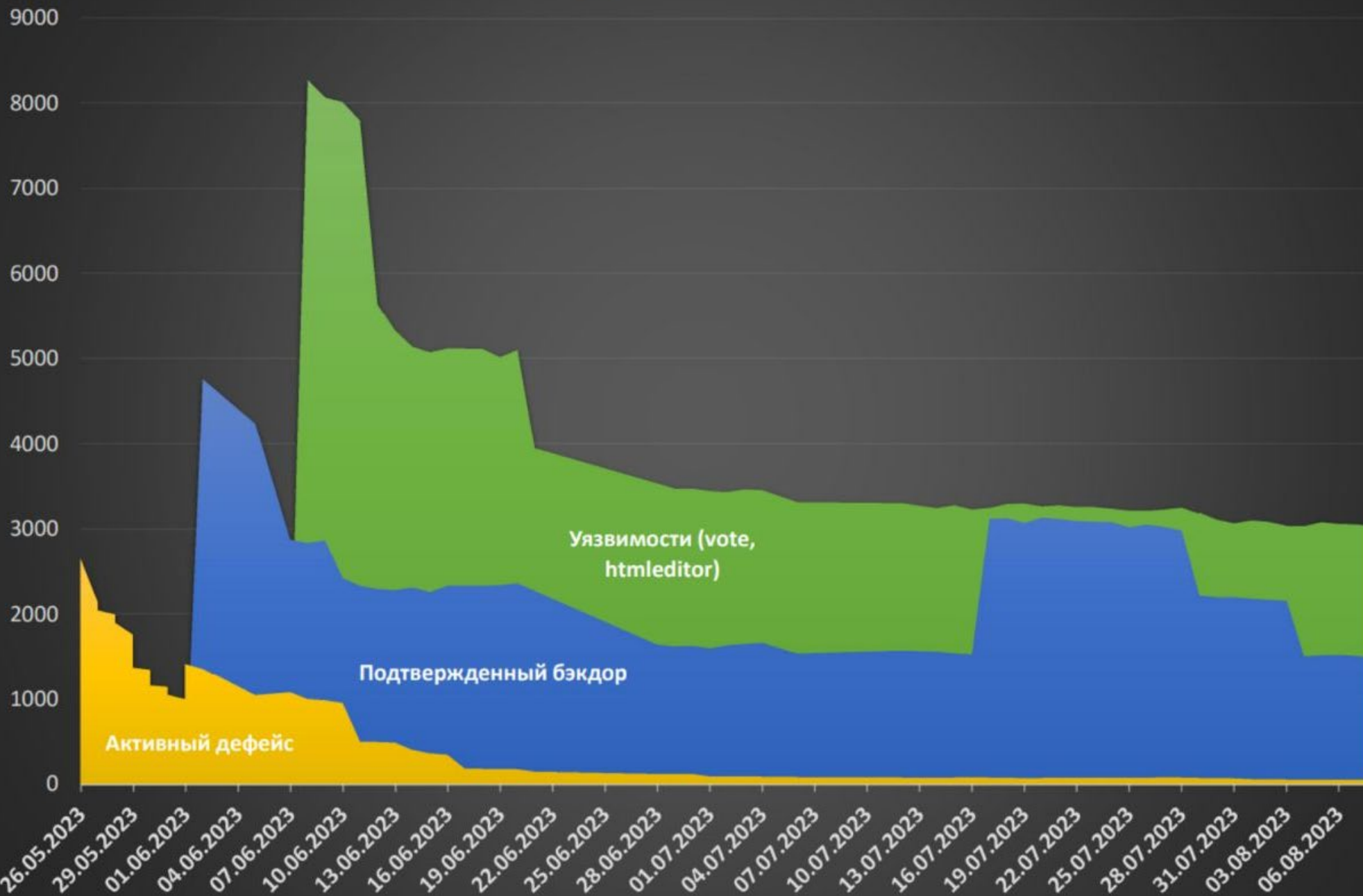


Трендовые уязвимости

Atlassian Confluence



Статистика по нарушениям ИБ в CMS 1С Bitrix



Типовое для региона ПО

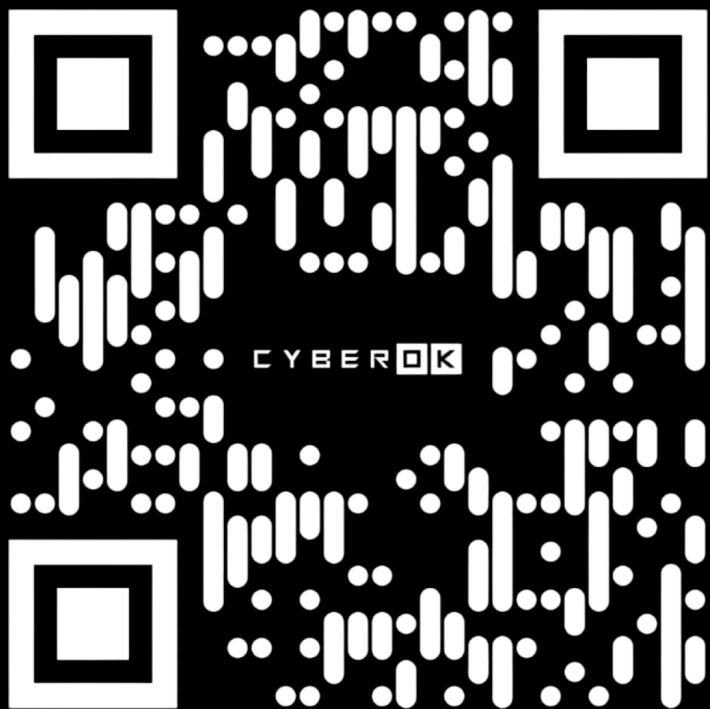
TrueConf





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

