

Поверхность атаки: как сканирование помогает предотвратить угрозы

 Нуйкин Андрей Начальник управления ИБ ЕВРАЗ

 02.2025

Количество атак
постоянно растет

Периметр компании
это не только
межсетевые экраны

Нужно знать что
происходит вокруг
компании

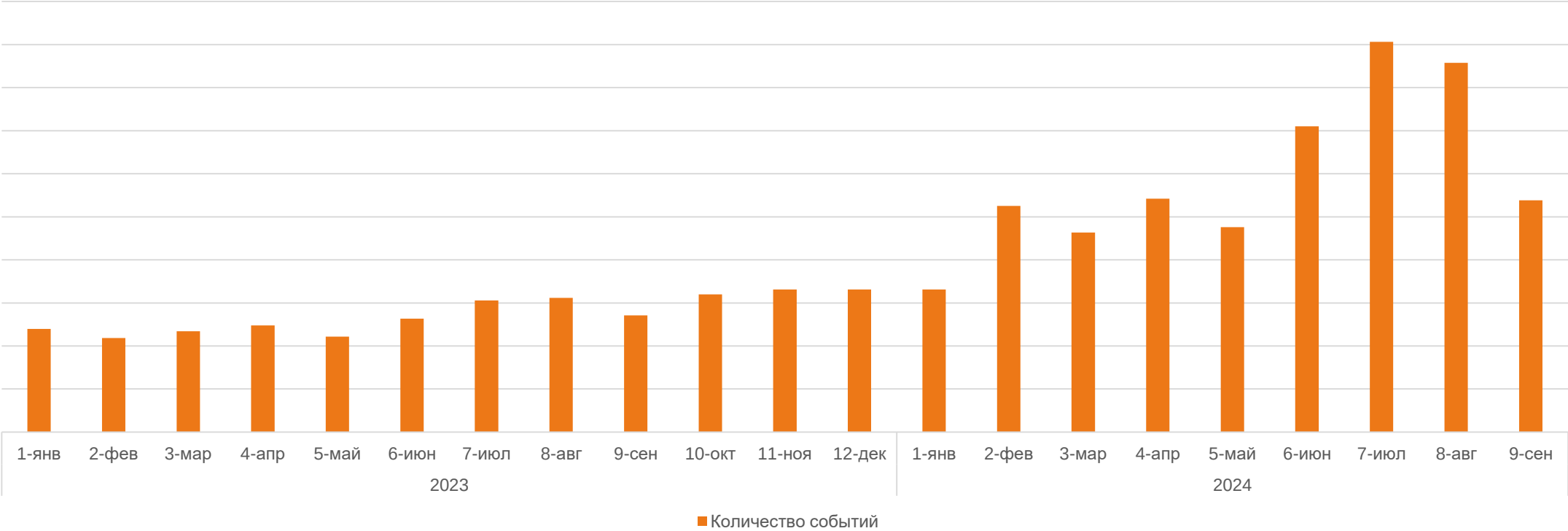
В 2023-24 году количество атак на
российские компании
увеличилось более чем на 200%



Рост количества событий

Количество событий выросло практически в два раза по сравнению с 2022-23 годами.

Динамика роста событий



F.A.C.C.T.

Увеличение
количества
фишинговых атак

и мошеннических доменов

Forbes

Применение ИИ

для генерации фишинговых сообщений, написания вредоносного кода, поиска уязвимостей, создания фейковых учетных записей и маскировки активности

AM

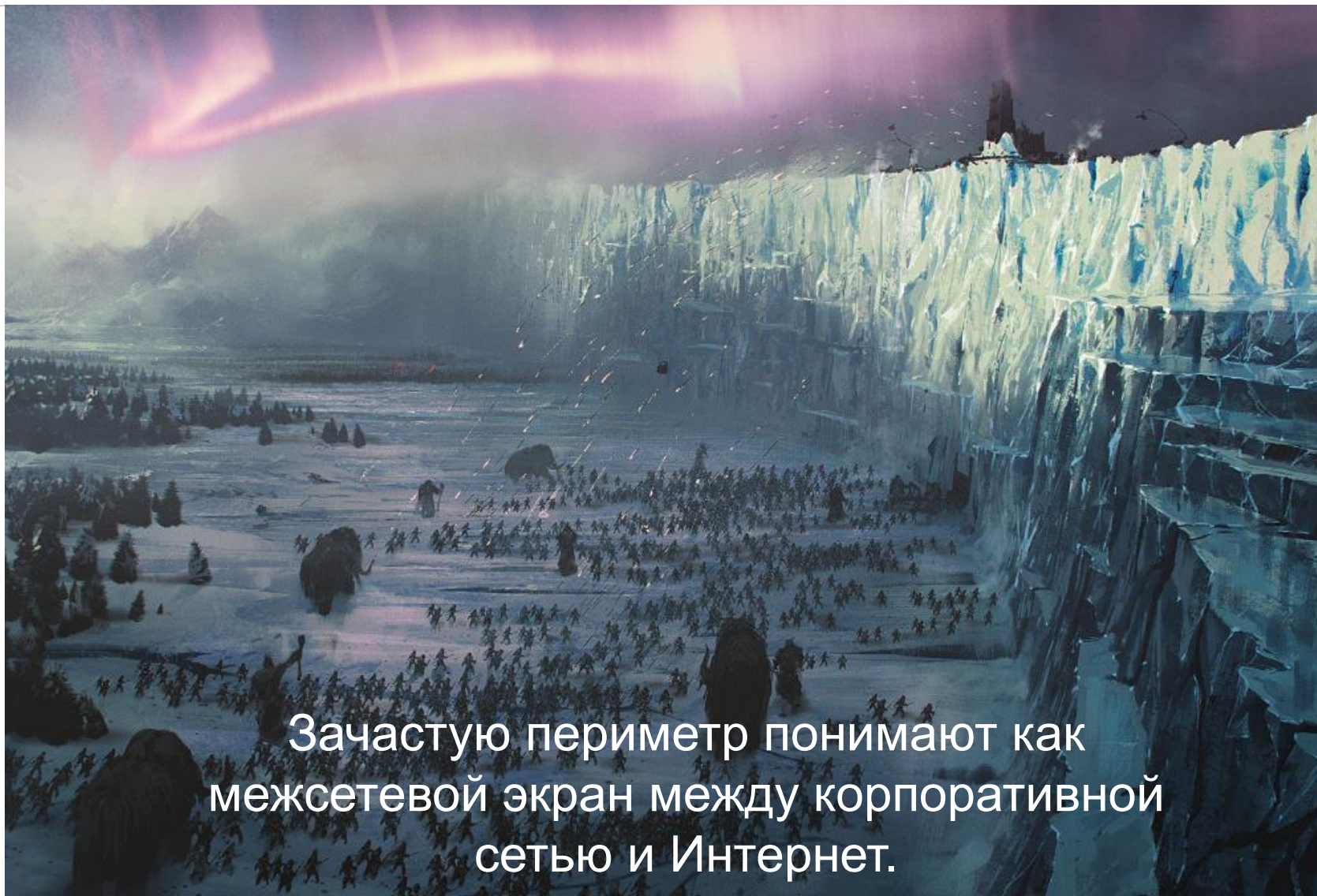
Активизация
APT-группировок

с целью кибершпионажа и феномен хактивизма, вследствие геополитической напряженности

F.A.C.C.T.

Рост числа атак
на цепочки поставок

направленных на поставщиков и посредников



На самом деле все гораздо сложнее...

- Вы знаете все опубликованные ресурсы?
- Вы знаете все свои домены?
- А фишинговые?
- Разработчики публикуют код в репозиториях?
- Утечки в DarkWeb?
- Вы начинаете работу с подрядчиком. А если на него готовится атака?

В РФ есть в основном два варианта сервисов:

1. Углубленное сканирование уязвимостей на периметре компании
2. Углубленное сканирование ресурсов вокруг компании (фишинговые домены, соцсети и т.д.)

Многие ли готовы к таким сервисам?



Что можно найти на периметре

Кто-то опубликовал уязвимый сервис в Интернет, о котором вы не знали

IP	VULNS_COUNT	CVE	CVSS	EPSS	CTI
		CVE-2022-1292	10	0,96	31,11
		CVE-2022-2068	10	0,96	31,11
		CVE-2021-26691	7,5	0,98	29,66
		CVE-2021-44790	7,5	0,95	29,6
		CVE-2022-23943	7,5	0,95	29,6
		CVE-2019-9641	7,5	0,92	29,54
		CVE-2013-2220	7,5	0,89	29,48
		CVE-2017-3167	7,5	0,87	29,43
		CVE-2022-31813	7,5	0,84	29,39
		CVE-2022-22720	7,5	0,81	29,33
		CVE-2021-39275	7,5	0,8	29,3
		CVE-2017-7679	7,5	0,8	29,29
		CVE-2013-4365	7,5	0,8	29,29
		CVE-2021-40438	6,8	1	29,27
		CVE-2017-15715	6,8	1	29,27
		CVE-2014-0226	6,8	0,99	29,27
		CVE-2007-4723	7,5	0,78	29,27

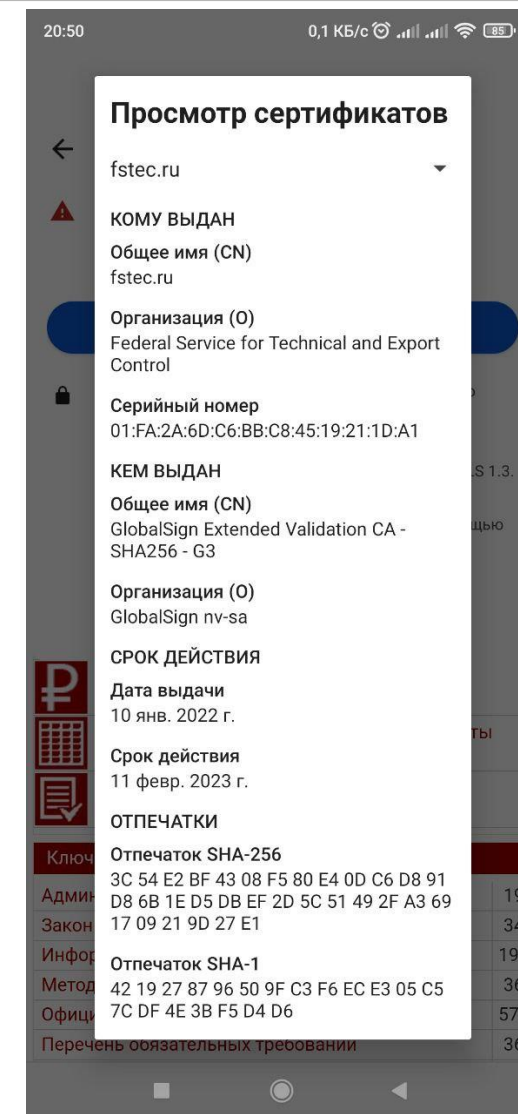
Маркетинг в рамках акции зарегистрировал домен и сделал лендинг.

Акция закончилась.

Лендинг забыли.



Легитимные домены компании. Но сроки регистрации или сроки действия сертификатов SSL заканчиваются.



Мошенники в ходе подготовки зарегистрировали домен похожий на Ваш.

euraz.com	Занят
evroz.com	Занят
evraz.com	Занят
esraz.com	Занят
eurvaz.com	Занят
evbaz.com	Занят

Разработчики опубликовали код во внешнем репозитории и не вычистили IP и учетные записи

```
private String url = "jdbc:jtds:sqlserver://[REDACTED]/AdventureWorks2014;loginTimeout=3";
private String user = "sa";
private String password = "[REDACTED]";

ds.setServerName("[REDACTED]evraz.com");

ds.setPortNumber(1433);

ds.setUser("[REDACTED]");

ds.setPassword("[REDACTED]");

ds.setDatabaseName("[REDACTED]");
```

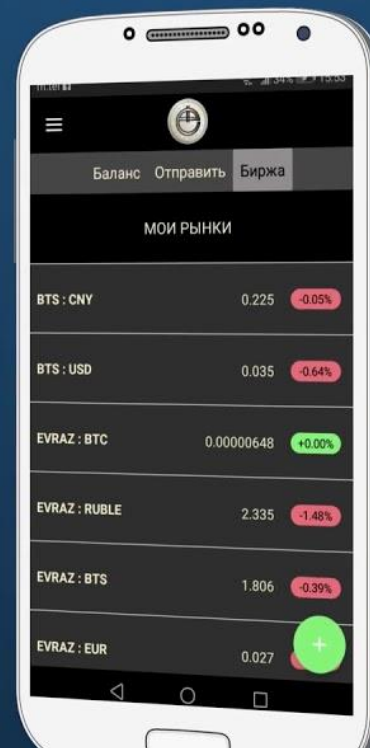
Появилось мобильное приложение с вашей
символикой или названием

EVRAZ Wallet



Идея проекта

Создание системы электронных платежей и взаимных расчетов для бизнеса и физических лиц в целях оптимизации налогооблагаемой базы и исключения посредников в лице банков.



Опубликовали утечку в которой содержатся
учетные записи пользователей Вашей
компании



[crt.sh](#) – поиск по сертификатам. Можем найти сертификаты и домены.

[backorder.ru](#) – поиск всех доменов по организации

[web-check.xyz](#) – информация о домене (DNS записи, порты, и т.д.)

[www.shodan.io](#) – сканер уязвимостей

[Github.com](#) – есть поиск по репозиториям

И др.

- Нужно использовать много разных порталов и скриптов
- Нет автоматизации
- Разные интерфейсы и синтаксис поиска
- Сложно анализировать результаты
- Сложности с доступом к DarkWeb



- Автоматический сканер поверхности атаки работающий по графику
- Выдает верхне-уровневую картину без подробностей
- Инженер не участвует
- Оплата по подписке за компанию, а не по IP\хостам\ресурсам
- Возможность при необходимости провести детальный анализ конкретных ресурсов за отдельную оплату



- В последнее время стали появляться такие сервисы
У некоторых есть бесплатный пробный вариант с ограничениями
- Единый интерфейс
- Позволяет автоматизировать работу
- Легко начать процесс анализа поверхности атаки
- Дает понимание куда двигаться дальше

- У многих компаний пока нет четкого плана по работе с уязвимостями
- Многим нужно просто понять картину своего периметра и окрестностей
«Спутниковый снимок» поверхности атаки
- Нужен недорогой сервис выдающий результат без глубокого анализа
- Подключение инженера по необходимости
- Автоматическая работа по графику

Знайте поверхность атаки

Проведите поиск по разным направлениям. Узнаете много нового.

☎ +7(495) 363-19-60

✉ Andrey.nuykin@evraz.com

🌐 www.evraz.com



Андрей Нуйкин

CISA, CISM

АПСИБ

RuSCADASec Coin #29