SkyDNS

SkyDNS — лидер контентной фильтрации и DNS безопасности

Лидер DNS безопасности в РФ

4 млрд запросов

В СУТКИ ПО ВСЕМУ МИРУ

10+ млн

АКТИВНЫХ ПОЛЬЗОВАТЕЛЕЙ

2+ млн угроз

БЛОКИРУЕТСЯ ЕЖЕДНЕВНО

193.58.251.251

www.skydns.ru

Домен третьего уровня

Домен второго уровня

Домен верхнего уровня

FQDN

SkyDNS

ПРОБЛЕМАТИКА

DNS угрозы – недооцененный риск

>90%

вредоносных программ

используют DNS для развития атаки в какой-то момент жизненного цикла. techradar.com, 2024

SkyDNS

ПРОБЛЕМАТИКА

DNS угрозы – недооцененный риск

>90%

вредоносных программ

используют DNS для развития атаки в какой-то момент жизненного цикла. techradar.com, 2024

88% компаний

страдают от DNS атак каждый год, efficientip.com, 2023

SkyDNS

ПРОБЛЕМАТИКА

DNS угрозы – недооцененный риск

>90%

вредоносных программ

используют DNS для развития атаки в какой-то момент жизненного цикла. techradar.com, 2024

88% компаний

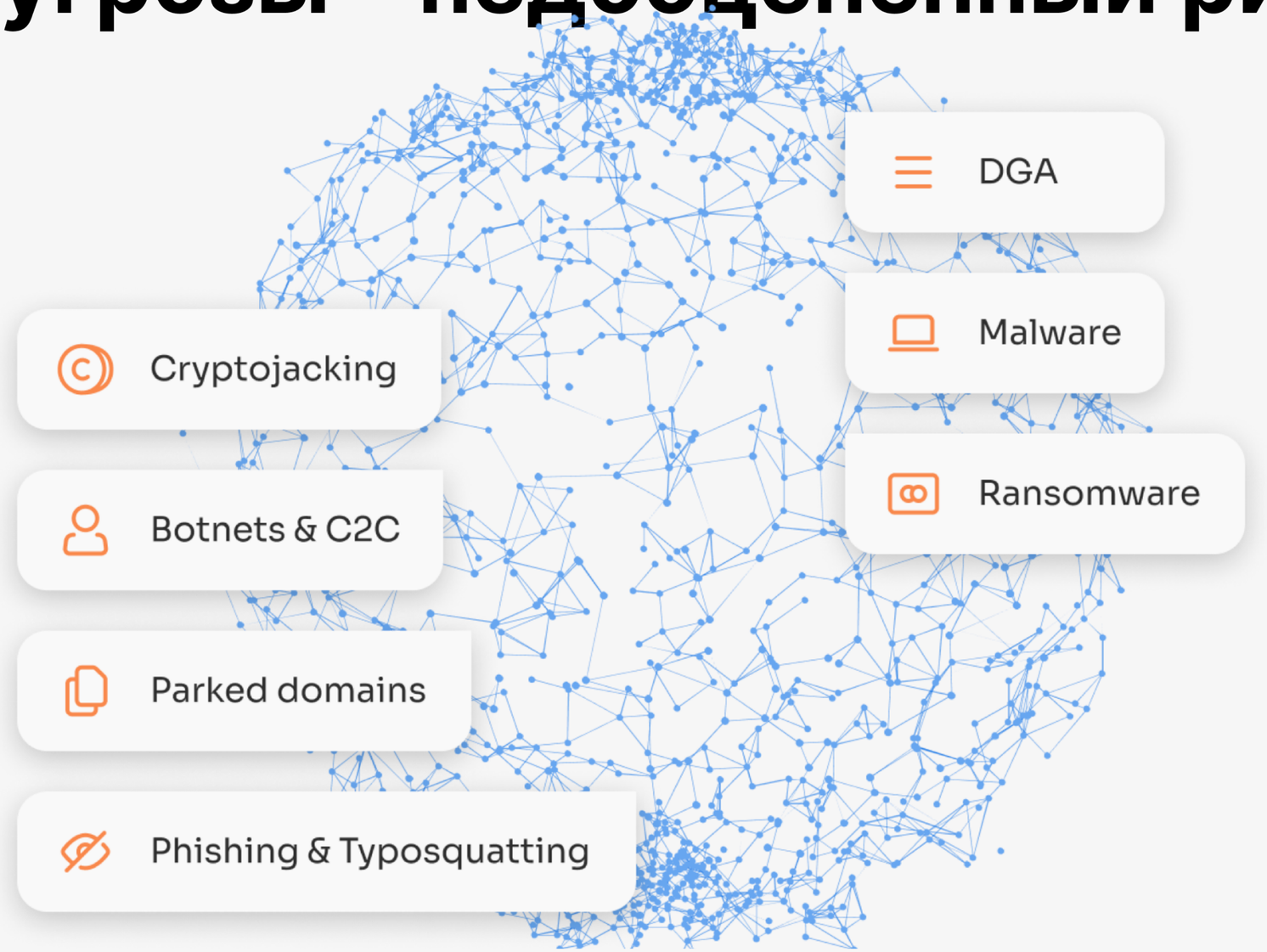
страдают от DNS атак каждый год, efficientip.com, 2023

34% всех атак может быть **предотвращено** на уровне DNS. cisco.com, 2024

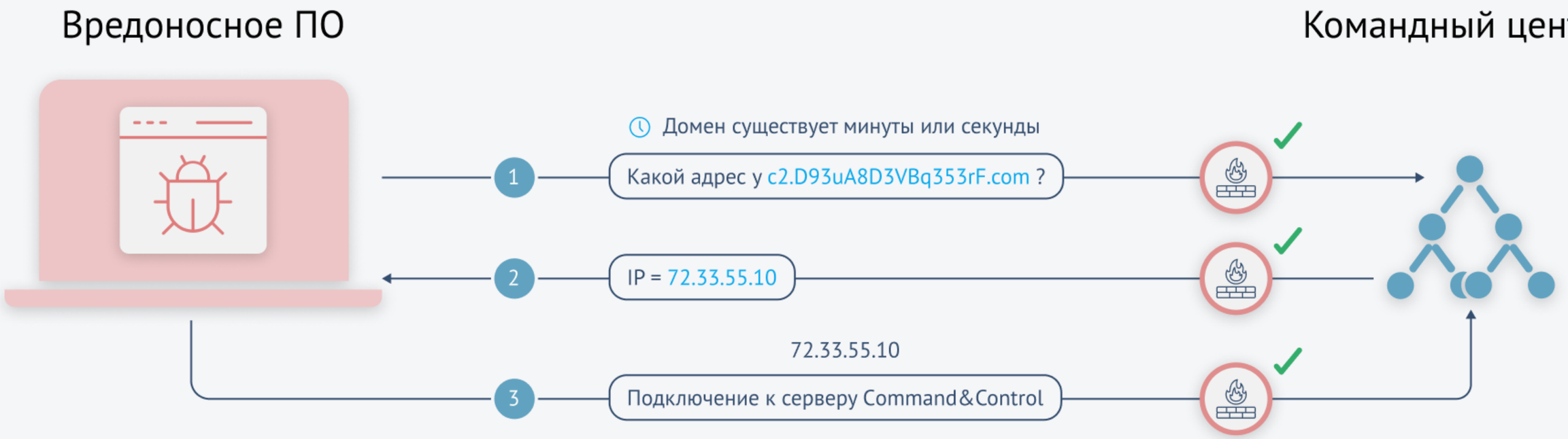
SkyDNS

ПРОБЛЕМАТИКА

DNS угрозы – недооцененный риск



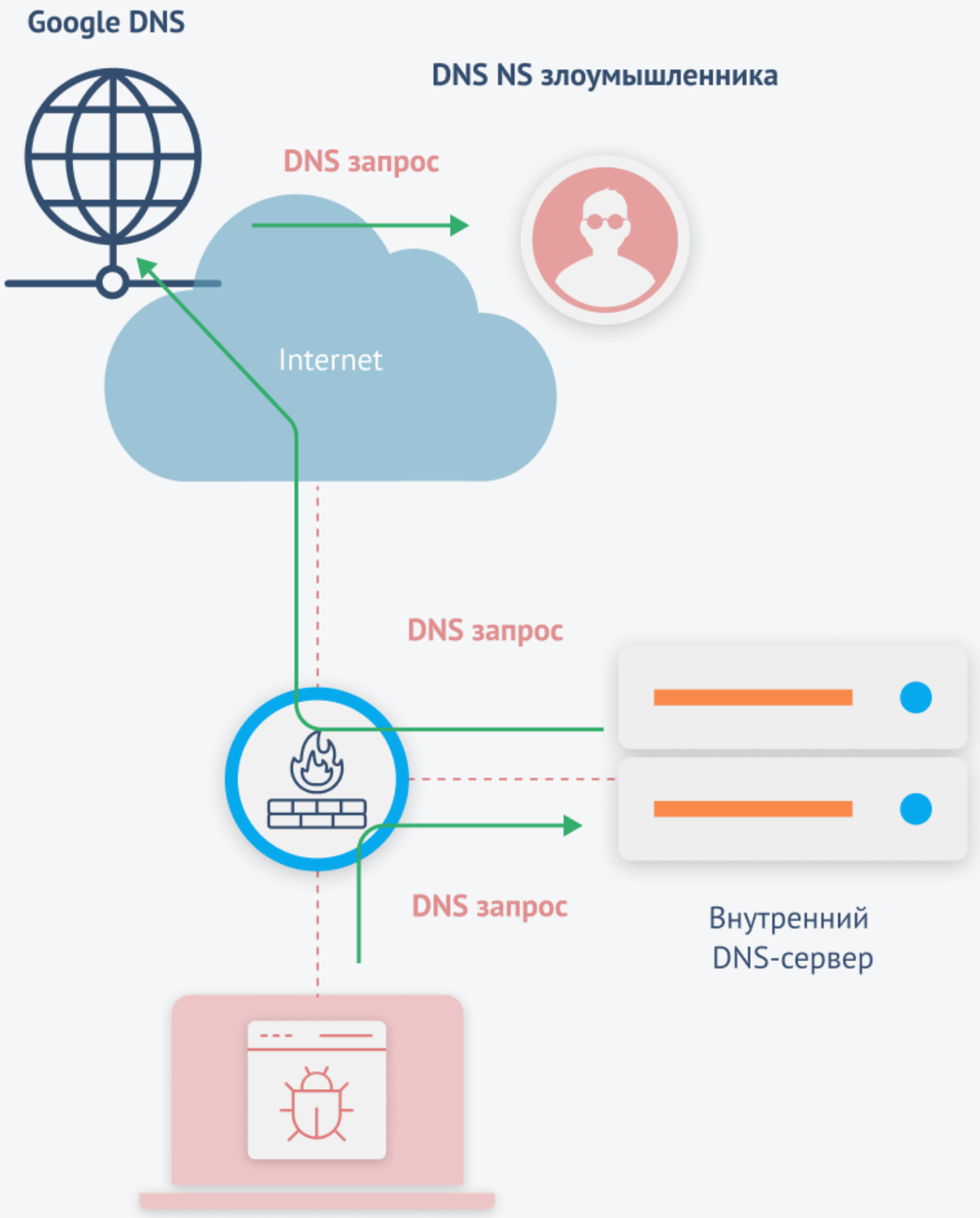
Обход списков плохих доменов используя DGA



Туннелирование внутри DNS

Туннелирование внутри DNS

- Канал от клиента - запрос разных поддоменов (пример: adminpassword.example.com)

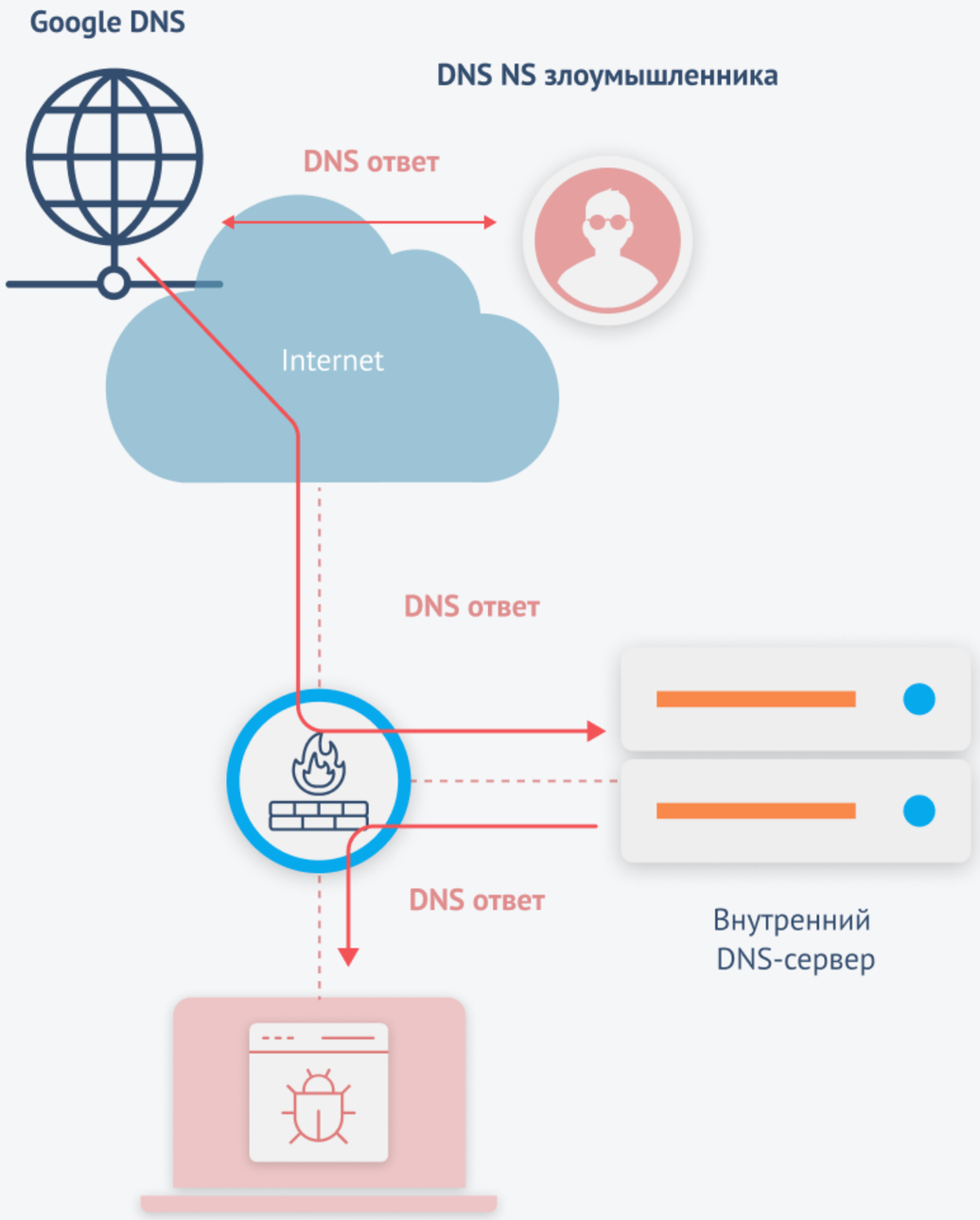


Туннелирование внутри DNS

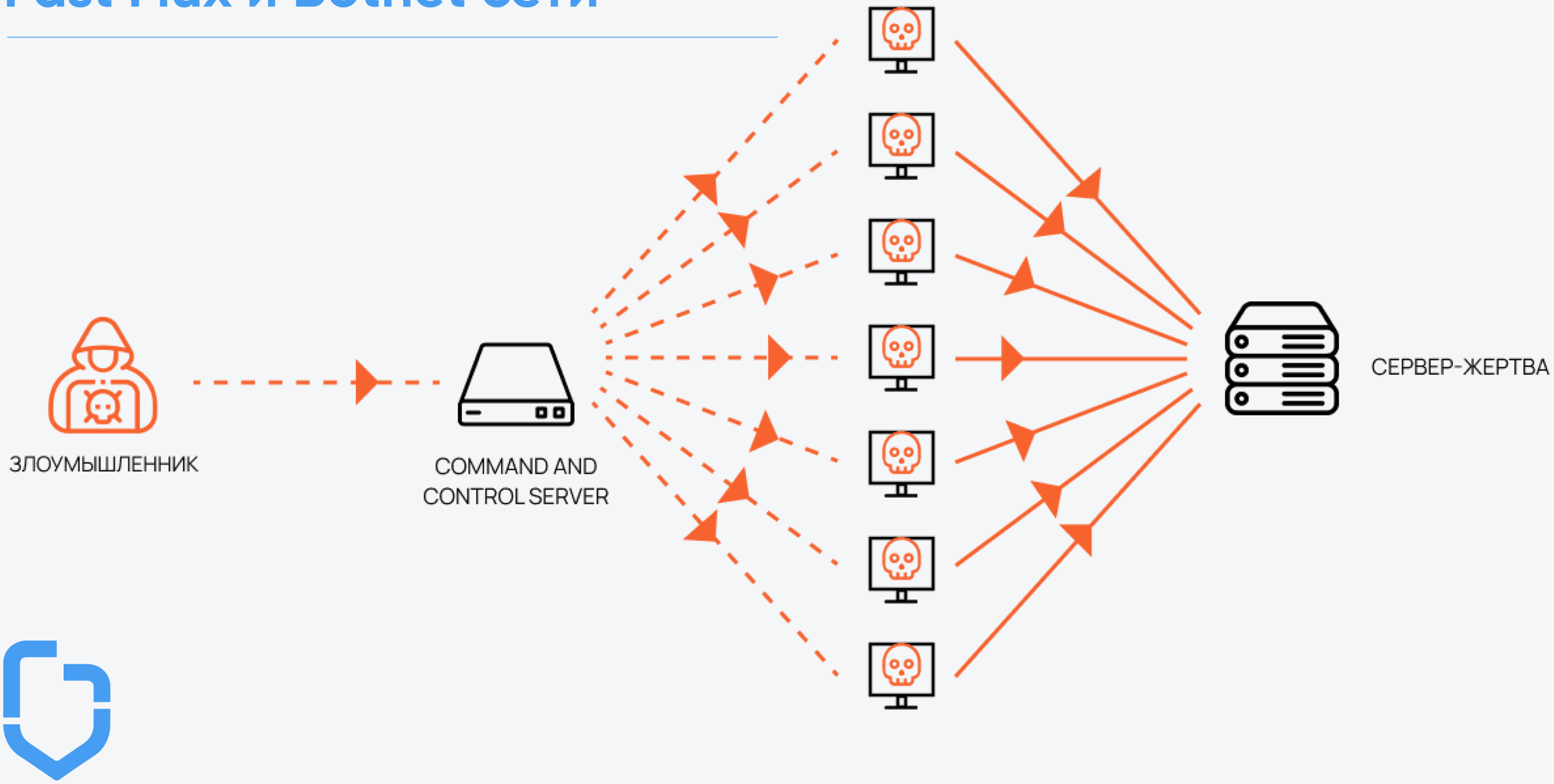
- Канал от клиента - запрос разных поддоменов (пример: adminpassword.example.com)

Инъекции в параметры запроса

- От DNS-сервера злоумышленника можно передавать данные, например, в записях TXT, SRV, MX, Null, EDNS, ответах CNAME

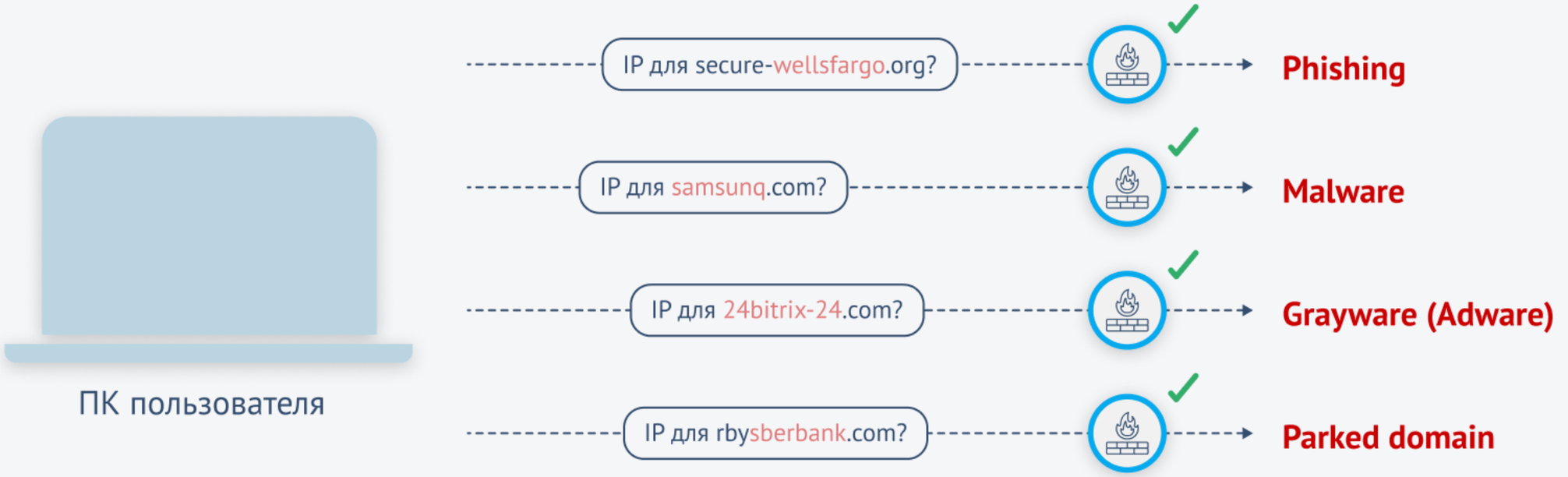


Fast Flux и Botnet сети



Typosquatting - как заставить пользователя нажать на плохую ссылку

Атакующие используют доменные имена популярных брендов и сервисов для методов социальной инженерии



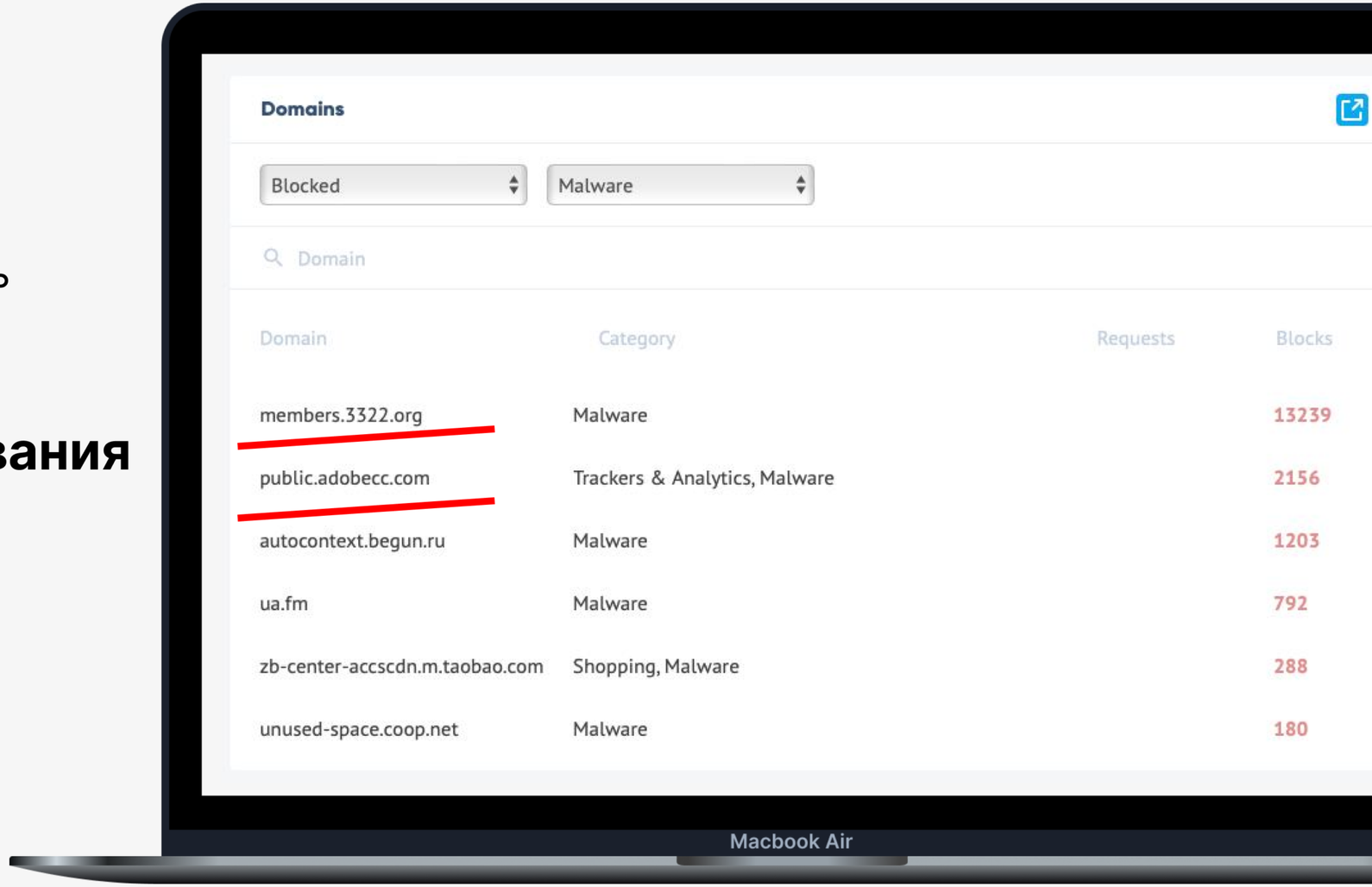
КЕЙСЫ

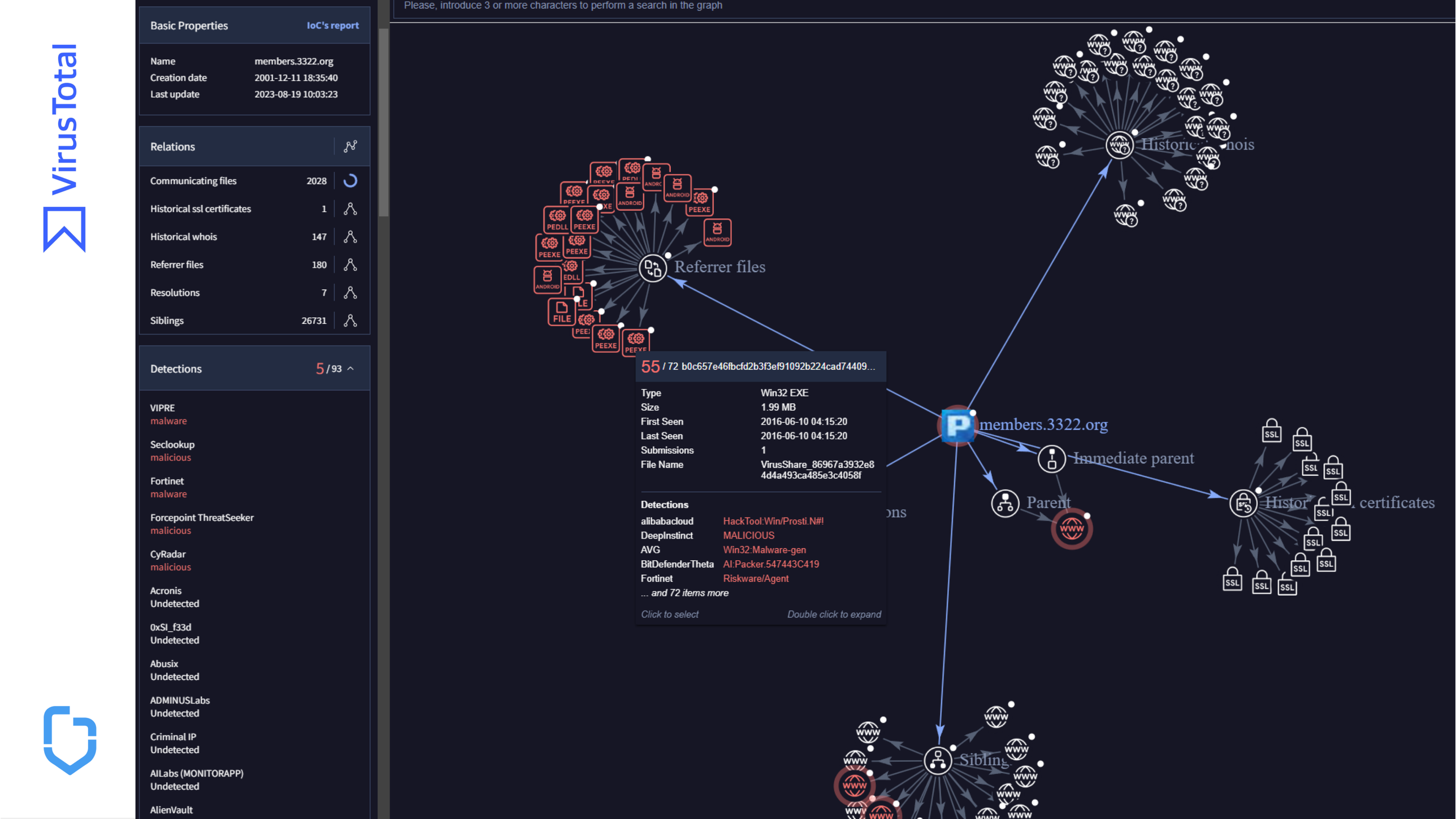
Статистика использования

1500+ устройств

Сфера: промышленность

30 дней использования

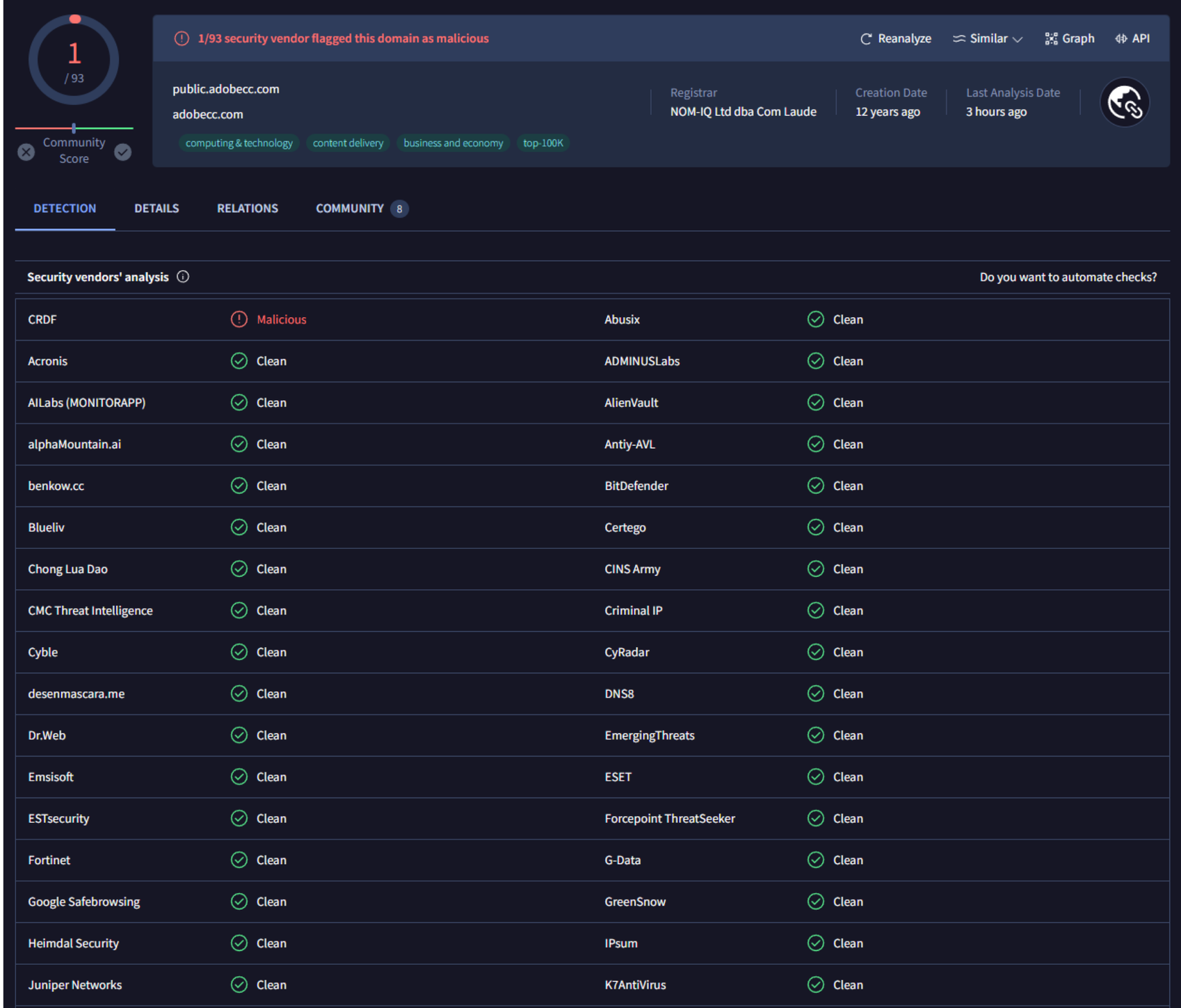


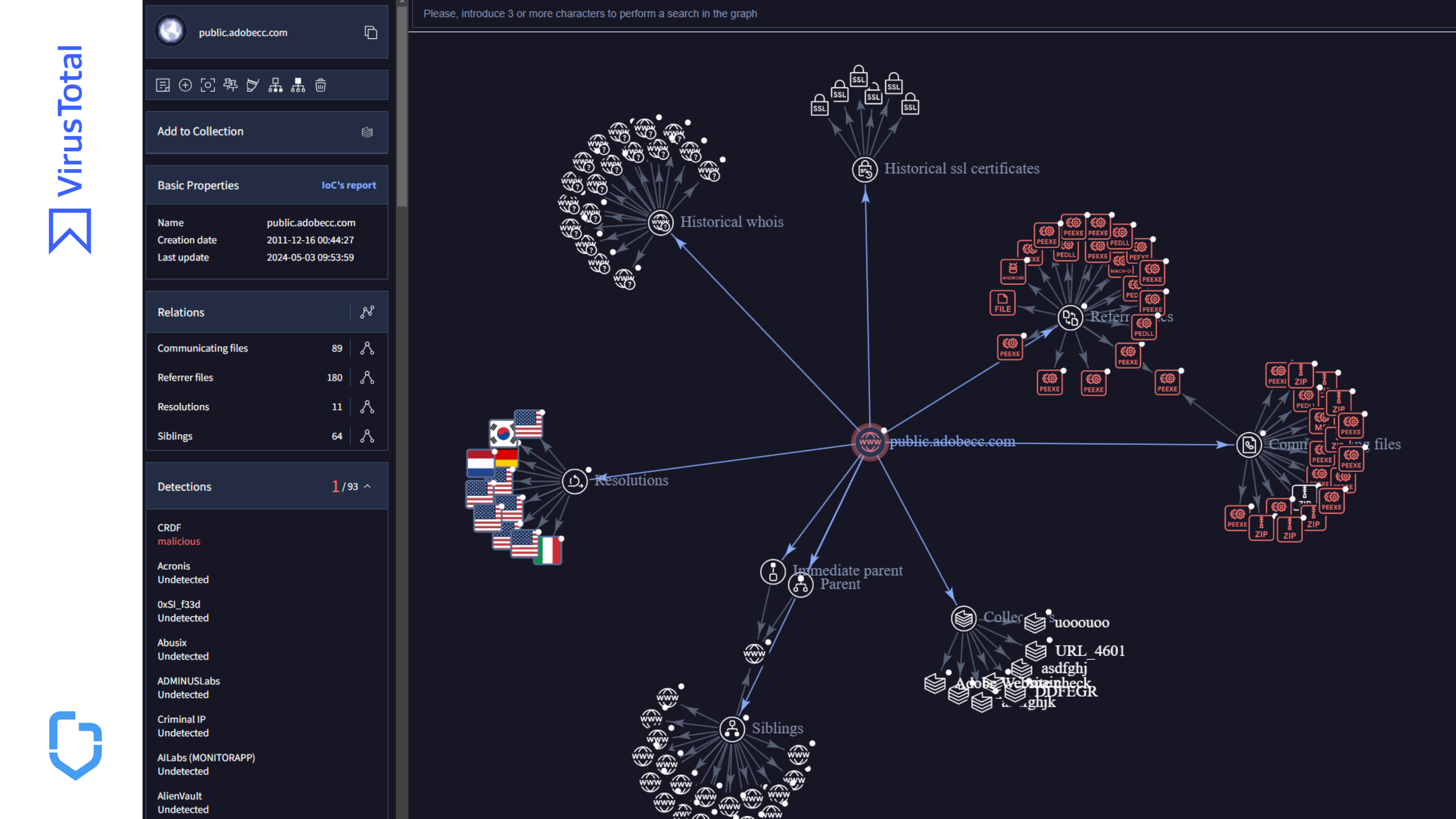

VirusTotal
Basic Properties
IoC's report
Name
members.3322.org
Creation date
2001-12-11 18:35:40
Last update
2023-08-19 10:03:23
Relations
Communicating files
2028
Historical ssl certificates
1
Historical whois
147
Referrer files
180
Resolutions
7
Siblings
26731
Detections
5 / 93
VIPRE
malware
Seclookup
malicious
Fortinet
malware
Forcepoint ThreatSeeker
malicious
CyRadar
malicious
Acronis
Undetected
0xSI_f33d
Undetected
Abusix
Undetected
ADMINUSLabs
Undetected
Criminal IP
Undetected
AILabs (MONITORAPP)
Undetected
AlienVault
Please, introduce 3 or more characters to perform a search in the graph
Referrer files
55 / 72 b0c657e46fbcfd2b3f3ef91092b224cad74409...
Type
Win32 EXE
Size
1.99 MB
First Seen
2016-06-10 04:15:20
Last Seen
2016-06-10 04:15:20
Submissions
1
File Name
VirusShare_86967a3932e84d4a493ca485e3c4058f
Detections
alibabacloud
HackTool:Win/Prosti.N#!
DeepInstinct
MALICIOUS
AVG
Win32:Malware-gen
BitDefenderTheta
AI:Packer.547443C419
Fortinet
Riskware/Agent
... and 72 items more
Click to select
Double click to expand
members.3322.org
Immediate parent
Parent
Sibling
certificates

VirusTotal

Эксперты !

92 вендора ИБ считает ресурс **легитимным**




public.adobecc.com
Add to Collection
Basic Properties
IoC's report
Name public.adobecc.com
Creation date 2011-12-16 00:44:27
Last update 2024-05-03 09:53:59
Relations
Communicating files 89
Referrer files 180
Resolutions 11
Siblings 64
Detections 1 / 93
CRDF malicious
Acronis Undetected
0xSI_f33d Undetected
Abusix Undetected
ADMINUSLabs Undetected
Criminal IP Undetected
AILabs (MONITORAPP) Undetected
AlienVault Undetected
Please, introduce 3 or more characters to perform a search in the graph
Historical ssl certificates
Historical whois
public.adobecc.com
Resolutions
Immediate parent
Parent
Siblings
uoooouoo
URL_4601
asdfghj
DDFEGR

SkyDNS

БАЗА ДАННЫХ

Точные данные в реальном времени

7 категорий ИБ

60 категорий контента

200+ приложений

SkyDNS

БАЗА ДАННЫХ

Точные данные в реальном времени

AI / ML

Ферма краулеров

Поисковые запросы

Трафик пользователей

7 категорий ИБ

60 категорий контента

200+ приложений

SkyDNS

БАЗА ДАННЫХ

Точные данные в реальном времени

AI / ML

Ферма краулеров

Поисковые запросы

Трафик пользователей

7 категорий ИБ

60 категорий контента

200+ приложений

Источники

ICANN

Вендоры ИБ

Гос. списки

Сообщества

SkyDNS

Основные показатели

Все запросы

181,340,567,923

Разрешенные запросы	Все заблокированные запросы	Предотвращенные угрозы
885,409,098	894	120

Общие сведения о потоке ваших запросов и общее количество конкретных типов запросов.

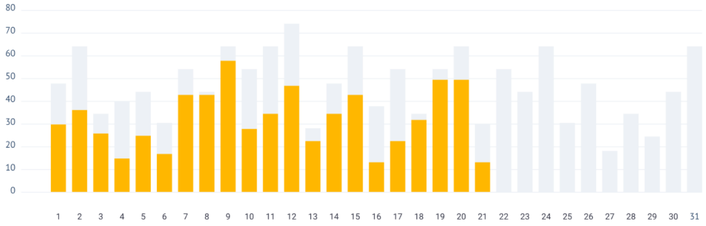
Разрешенные запросы
Запросы, прошедшие через веб-фильтр, поскольку наши алгоритмы не обнаружили киберугроз или ограничений в категориях вашей учетной записи или настройках домена.

Все заблокированные запросы
Запросы, которые помечены алгоритмами SkyDNS как потенциально опасные или ограничены на основании пользовательских настроек в вашей учетной записи.

Предотвращенные угрозы
Общее количество предотвращенных угроз включает в себя случаи, идентифицированные нашими алгоритмами как вредоносные или связанные с заблокированными категориями кибербезопасности в настройках вашей учетной записи.

Активность

Блокировок: 3 345 Запросов: 3 345

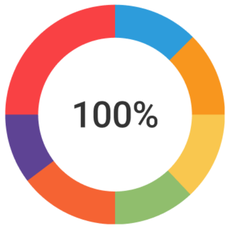


Обновлено 3 минуты назад

Категории

Безопасность | Остальные категории

Грубость, мат, непристойность	885	1045
Распространение вирусов	674	987
Запаркованные домены	536	2001
Фишинг	536	1234
Агрессия, расизм, терроризм	987	45692837
Криптомайнинг	674	987
Плагиат и рефераты	674	987



Обновлено 3 минуты назад

Основные показатели

ТОП ЗАБЛОКИРОВАННЫХ ДОМЕНОВ		ТОП ЗАБЛОКИРОВАННЫХ УСТРОЙСТВ		ТОП ЗАБЛОКИРОВАННЫХ КАТЕГОРИЙ	
youtube.com	32456	yellowmouse215	67493	Порнография и секс	67493
facebook.com	21684	silverduck32	53493	Знакомства	62098
vk.com	20387	whitegoose497	49863	Социальные сети	55857
linkedin.com	18045	whitefish664	34297	Чаты и мессенджеры	52765
twitter.com	16825	tinyleopard720	32107	Форумы	40876
tiktok.com	13825	silverlion355	21107	Торренты и P2P сети	37984
reddit.com	8825	beautifulbutterfly101	18002	Игры	32001
medium.com	4398	tinypanda866	12112	Астрология	29871
instagram.com	4386	whiterabbit554	10987	Фильмы и видео онлайн	21437
pinterest.com	3266	blueladybug463	8987	Казино, лотереи, тотализаторы	17043

10 самых заблокированных доменов, устройств с наибольшим количеством попыток доступа и заблокированных категорий по количеству запросов.

Топ заблокированных доменов
Список из 10 доменов, к которым ваши пользователи постоянно пытались получить доступ, попадающих в заблокированные категории или точечно заблокированных вами.

Топ заблокированных устройств
Список из 10 устройств, которые чаще всего пытались получить доступ к заблокированным вами доменам и категориям.

Топ заблокированных категорий
Список из 10 категорий, к которым ваши пользователи постоянно пытались получить доступ, подпадающих под настройки блокировки вашего аккаунта.

Устройства

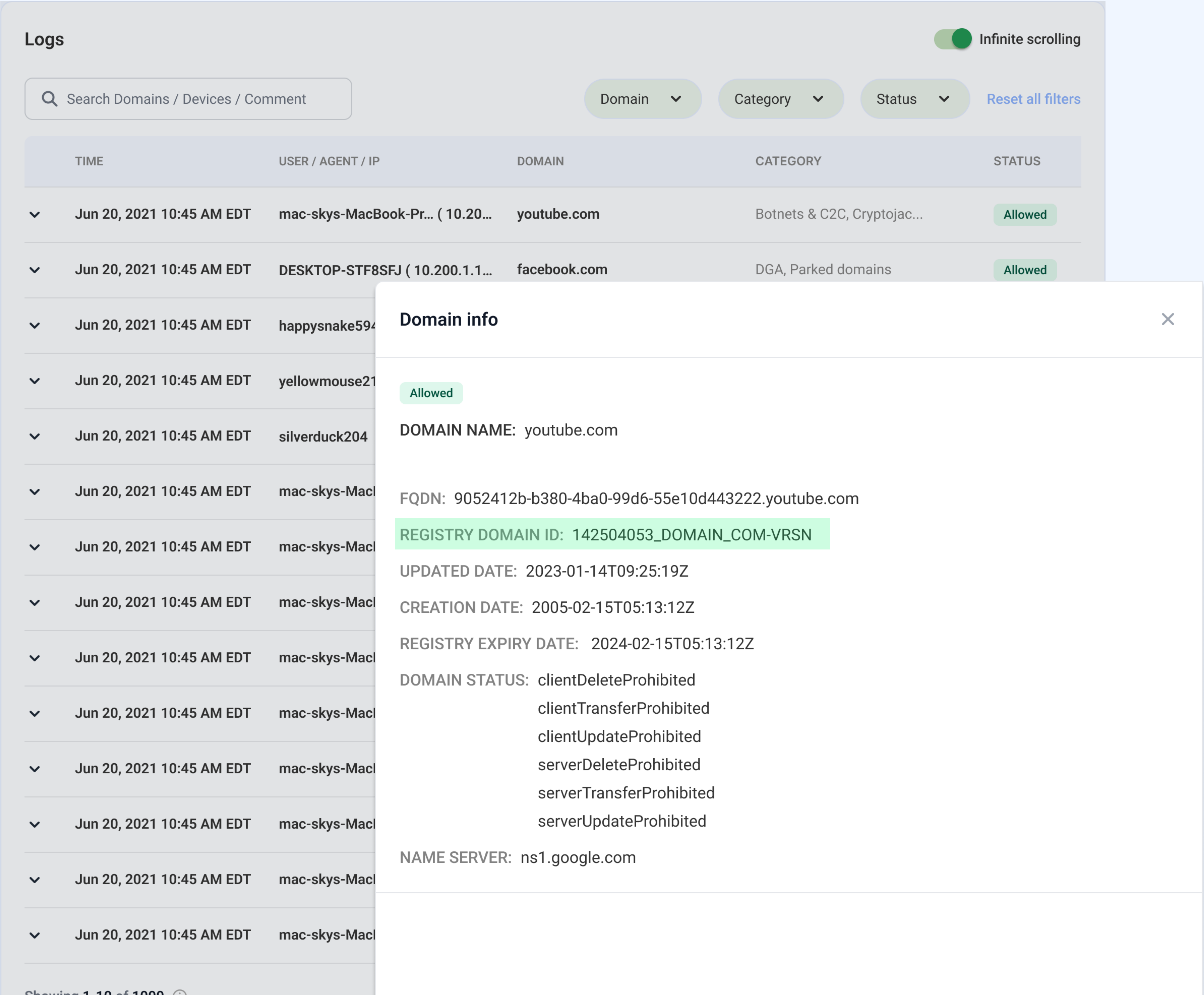
Подробная статистика >

Найти устройство

Устройства	Запросы	Заблокированные запросы
mac-skys-MacBook-Pr... (10.200.1.91)	3758	3758
DESKTOP-STF8SFJ (10.200.1.11)	76840	76840
happysnake594	83	83
google.com	543	543
yellowmouse215	6573	6573
silverduck204	1121	1121
mac-safe-MacBook-AIR... (10.275.1.91)	1121	1121
mac-safe-MacBook-AIR... (10.275.1.91)	1121	1121
mac-safe-MacBook-AIR... (10.275.1.91)	1121	1121
mac-safe-MacBook-AIR... (10.275.1.91)	1121	1121

< 1 ... 6 7 8 ... 14 >

Подробный отчет по 10 устройствам с самой высокой активностью.


Logs
Infinite scrolling
Search Domains / Devices / Comment
Domain
Category
Status
Reset all filters
TIME
USER / AGENT / IP
DOMAIN
CATEGORY
STATUS
Jun 20, 2021 10:45 AM EDT
mac-skys-MacBook-Pr... (10.20...
youtube.com
Botnets & C2C, Cryptojac...
Allowed
Jun 20, 2021 10:45 AM EDT
DESKTOP-STF8SFJ (10.200.1.1...
facebook.com
DGA, Parked domains
Allowed
Jun 20, 2021 10:45 AM EDT
happysnake59
Jun 20, 2021 10:45 AM EDT
yellowmouse21
Jun 20, 2021 10:45 AM EDT
silverduck204
Jun 20, 2021 10:45 AM EDT
mac-skys-Mac
Domain info
Allowed
DOMAIN NAME: youtube.com
FQDN: 9052412b-b380-4ba0-99d6-55e10d443222.youtube.com
REGISTRY DOMAIN ID: 142504053_DOMAIN_COM-VRSN
UPDATED DATE: 2023-01-14T09:25:19Z
CREATION DATE: 2005-02-15T05:13:12Z
REGISTRY EXPIRY DATE: 2024-02-15T05:13:12Z
DOMAIN STATUS: clientDeleteProhibited
clientTransferProhibited
clientUpdateProhibited
serverDeleteProhibited
serverTransferProhibited
serverUpdateProhibited
NAME SERVER: ns1.google.com

SkyDNS

ПОДКЛЮЧЕНИЕ

Легко проверить в действии

Поддержка

Подключение

Интеграция на сети занимает не более 15 минут

Тестирование

Инфраструктура не меняется, появляется инструмент для мониторинга

Выводы

Статистика по блокировкам и анализ данных

до 2х дней

SkyDNS

Вячеслав Новоселов
CEO SkyDNS

www.skydns.ru

@justnva

v@skydns.ru