PT Feeds

Как повысить защищенность при помощи threat intelligence

Алексей Вишняков

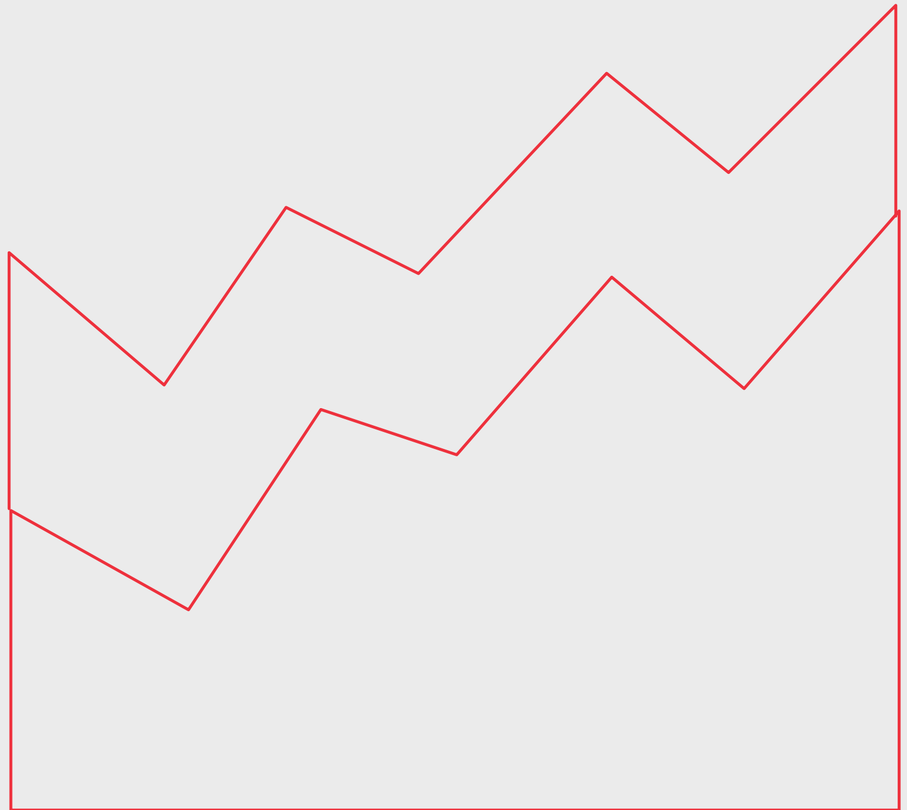
руководитель отдела обнаружения вредоносного ПО экспертного центра безопасности Positive Technologies

Максим Долгинин

руководитель направления по работе с данными о киберугрозах, Positive Technologies

Содержание

- Данные Positive Technologies о киберугрозах
- Статистика
- Как мы обрабатываем данные
- Состав данных в фидах
- Применение PT Feeds
- Ваши вопросы



Что такое cyberthreat intelligence?

- Информация, которая описывает **существующие или потенциальные угрозы** для безопасности информационных систем и пользователей

- **Существует в разных формах**:
  - отчеты, описывающие мотивацию, инфраструктуру и техники определенного злоумышленника;
  - IP-адреса, домены, URL и хеши файлов, связанные с известной угрозой

- **Используется организациями** для получения необходимого контекста событий безопасности и **позволяет быстро отреагировать** на угрозу

Почему

необходимо использовать внешние данные об угрозах

Сложно выявлять атаки

67% атак

носят целенаправленный характер*

96% организаций

не защищены от проникновения внешнего злоумышленника**

20,8%

рост общего количества инцидентов в 2022 году*

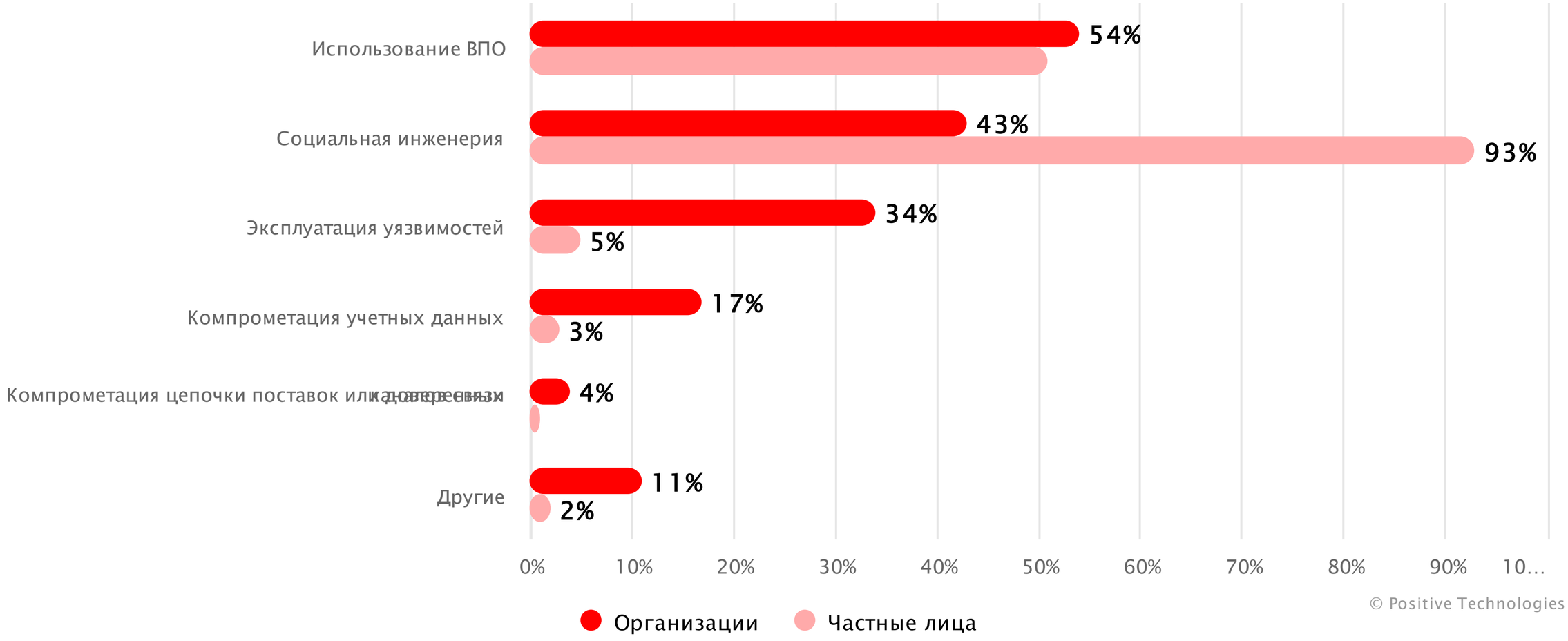
в 84% организаций

даже низкоквалифицированный злоумышленник может проникнуть в локальную сеть**

Средства защиты не обладают знаниями об угрозах

* «Актуальные киберугрозы: итоги 2022 года», Positive Technologies
** «Итоги пентестов 2022», Positive Technologies

Методы атак по итогам 2022 года *



* «Актуальные киберугрозы: итоги 2022 года», Positive Technologies

Реагирование на инциденты неэффективно

75% компаний

тратят на разбор ложноположительных инцидентов такое же или большее время, как и на работу с реальными инцидентами

Долгий процесс реагирования

Даже при успешном обнаружении инцидента ИБ эксперты могут тратить много времени на уточнение угрозы: кто конкретно атаковал компанию, с какой целью и какие дальнейшие действия злоумышленник может предпринять

Не хватает специалистов

SOC работает в режиме 24/7/365,

поэтому нужно минимум 3 человека на позицию аналитика L1–L2

Что мешает эффективно использовать данные об угрозах?

TI — это сложно

Сбор, актуализация и распространение знаний об угрозах — сложная задача, требующая большого объема ресурсов команды SOC

Не хватает аналитиков

ИБ-специалисты сталкиваются с необходимостью вручную разбираться с потоком данных об угрозах, приоритизировать их, отсеивать ложные срабатывания и устаревшую информацию

Данные об угрозах не интегрированы в систему защиты

Нарушается комплексность подхода к обеспечению ИБ, средства защиты пропускают атаки, которые могли бы закрыть получив данные от других систем ИБ

Недостоверные данные

Используя открытые источники данных об угрозах организации сталкиваются с большим количеством ложных срабатываний

Отсутствие контекста

Часто данные поставляются без контекста, который позволил бы оценить степень опасности угрозы и помог приоритизировать инцидент

TI в Positive Technologies

PT Threat Intelligence Feeds — потоки данных с индикаторами компрометации, предназначенные для информирования команды SOC об актуальных угрозах ИБ

Содержат:

Домены


Файлы

URL

IP-адреса

Обогащают используемые средства защиты информации и повышают эффективность их работы

Позволяют предотвращать атаки на информационные системы

Статистика

База индикаторов Positive Technologies*

53 млн
файлов

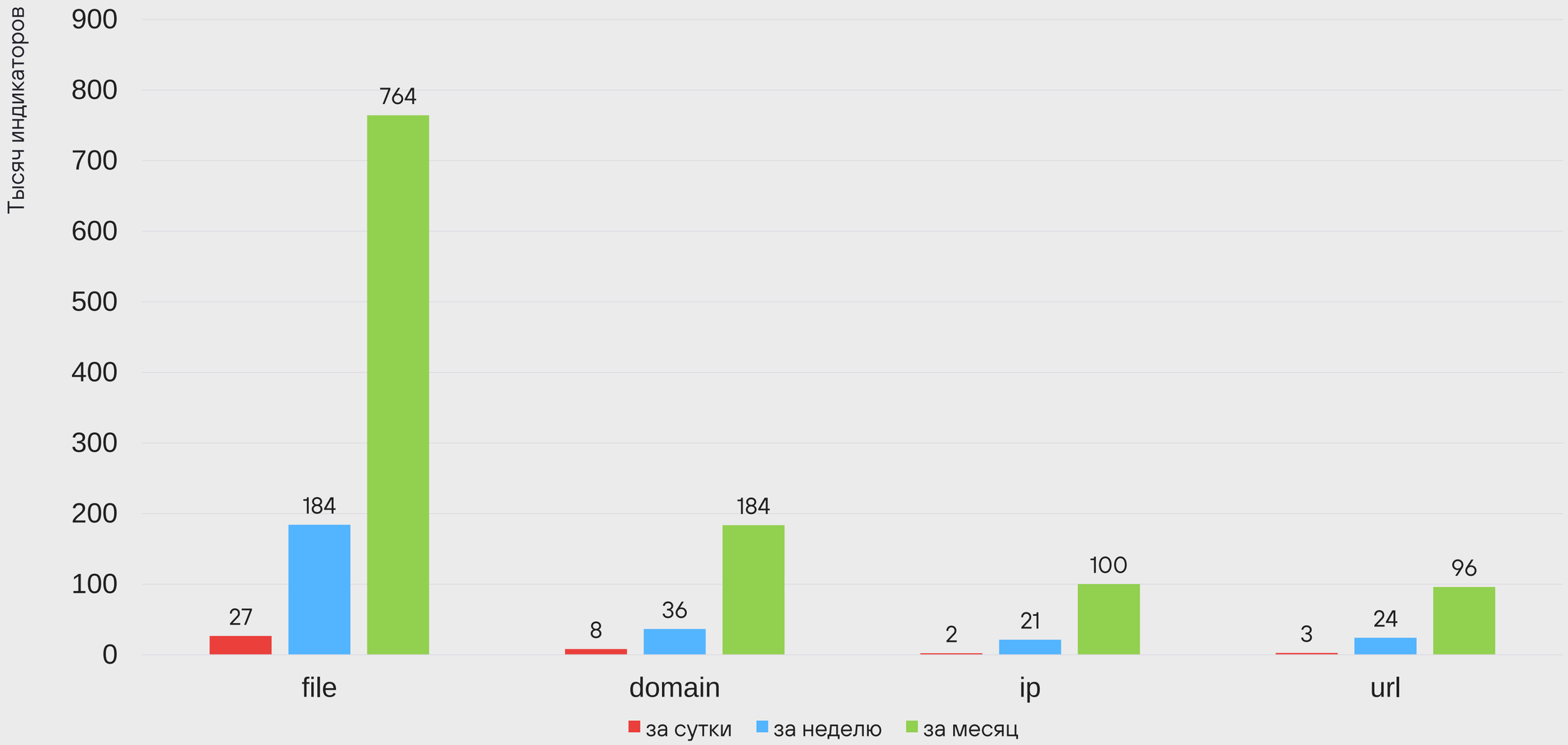
833 тыс.
IP-адресов

2 млн
доменов

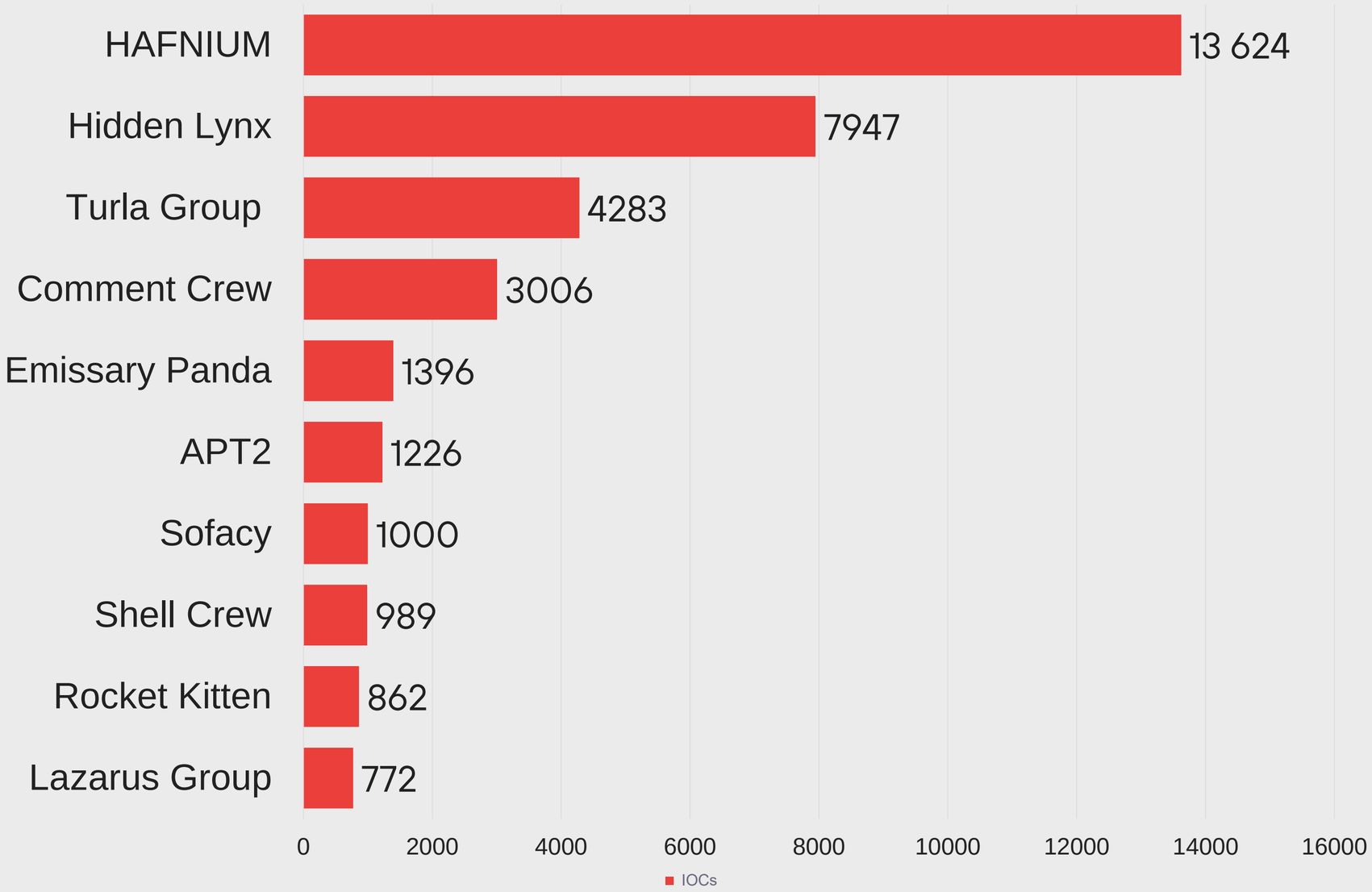
622 тыс.
URL

* - по состоянию на 17.03.2023

Среднее количество обрабатываемых данных



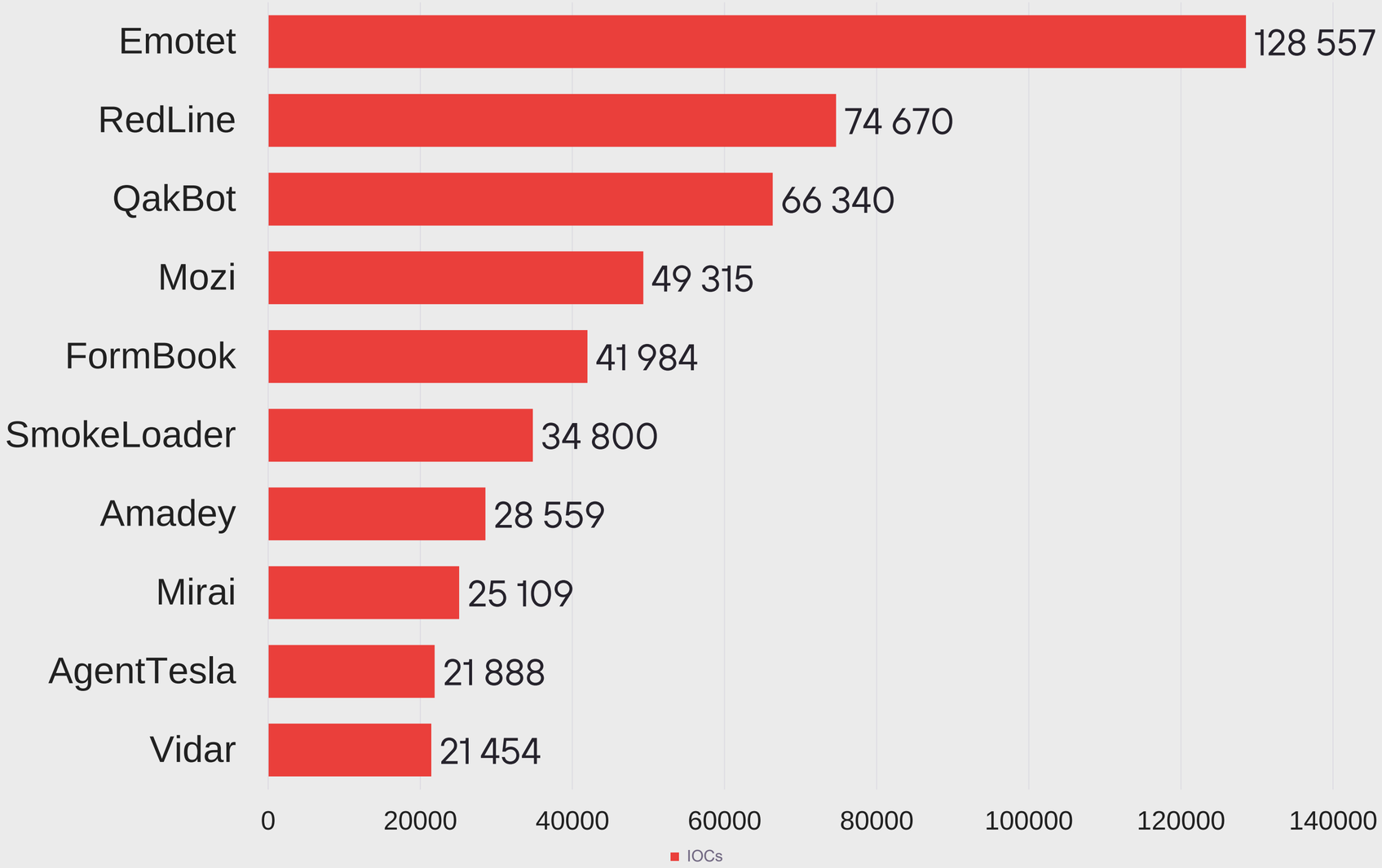
Топ-10 группировок



99

вредоносных группировок в базе

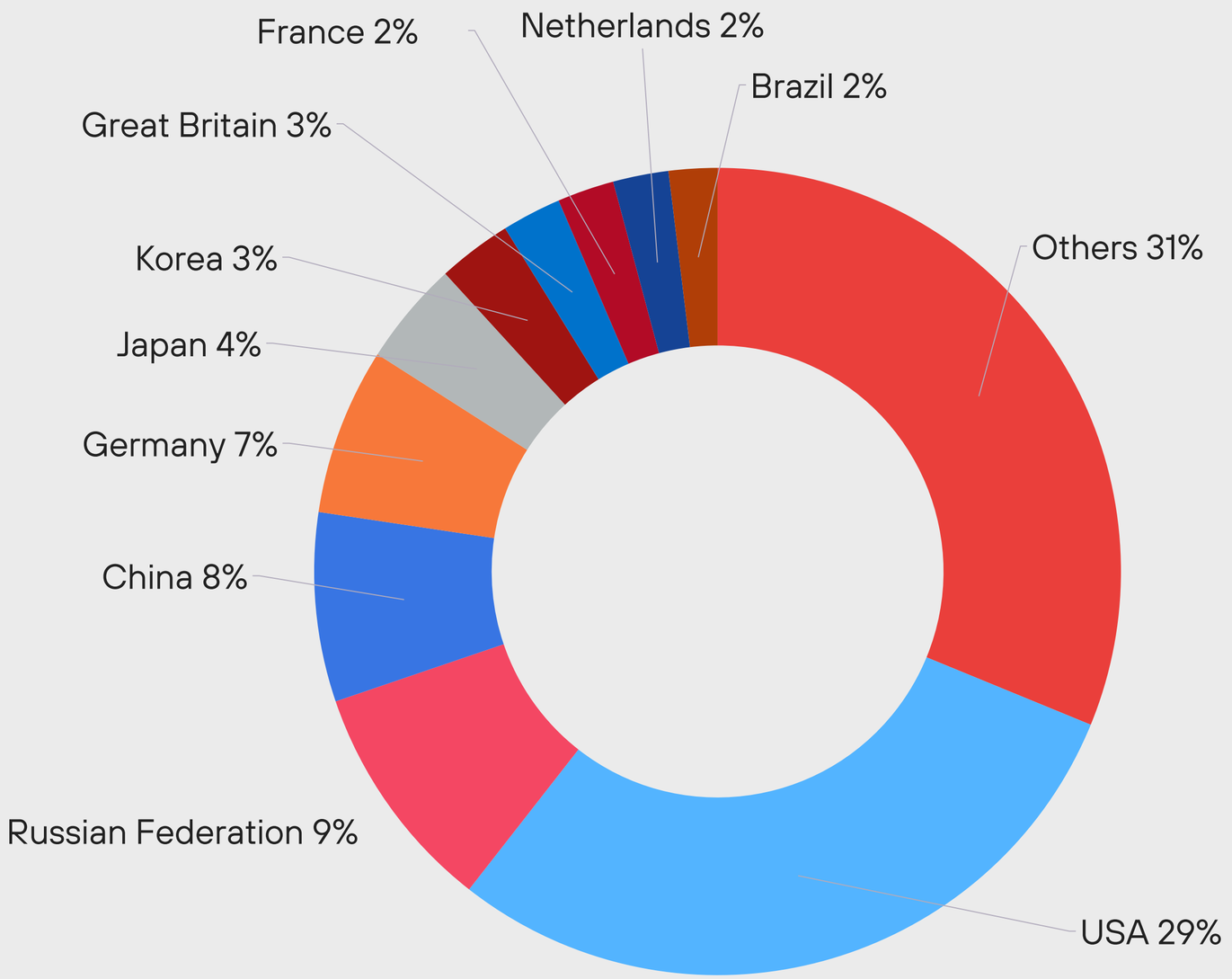
Топ-10 актуальных семейств ВПО



824

семейства ВПО в базе

География распределения IP-адресов*



В **196**

странах размещены
наблюдаемые IP-адреса

* - не является атрибуцией

Схема обработки данных

Схема обработки данных

Примеры состава фидов

APT domains / URLs / IPs/ hashes

Вредоносные индикаторы, имеющие отношение к целевым угрозам

Связи с другими объектами

Теги

Рейтинг значимости


```
{
    "is_apt": true,
    "relations": {
        "ips": [
            "104.86.182.8",
            "118.24.36.220",
            "20.62.24.77",
            "20.80.129.13",
            "20.99.132.105",
            "..."
        ]
    },
    "tags": [
        "vt:assembly",
        "filescanio:obfuscated",
        "hybrid:score:100",
        "pe:SuspiciousRichHeader",
        "..."
    ],
    "malware_group": [
        "HAFNIUM"
    ],
    "malware_class": [
        "Trojan"
    ],
    "malware_family": [
        "CobaltStrike"
    ],
    "timestamps": {
        "first_seen": "2022-01-17T02:41:03.020000+00:00",
        "last_seen": "2022-12-09T20:26:46.336000+00:00"
    },
    "score": 47,
    "verdict": "malicious",
    "md5": "79c1cd9f78471c34a9fed7d12b838496",
    "sha256": "552effa09cfc82eae0296e1b9c9f4a5a81122418f1bee8a1c44542b382670263"
}
```

Malicious family recent activity

Активные вредоносные индикаторы за последний месяц, размеченные по семействам вредоносного программного обеспечения

Семейство ВПО

Malicious campaign current activity

Активные вредоносные индикаторы за последнюю неделю, агрегированные по вредоносным кампаниям

Вредоносная кампания


```
{
    "tags": [
        "anyrun:emotet",
        "file:zip",
        "yara:win",
        "..."
    ],
    "relations": {
        "ips": [
            "68.183.190.199",
            "104.131.58.132",
            "159.203.204.126",
            "..."
        ],
        "urls": [
            "http://68.183.190.199:8080/bml/acquire/cone/",
            "http://104.131.58.132:8080/loadan/",
            "http://159.203.204.126:8080/ringin/srvc/",
            "..."
        ]
    },
    "malware_campaign": [
        "TA542/2022/12"
    ],
    "malware_group": [
        "TA542"
    ],
    "malware_class": [
        "Trojan-Banker",
        "RiskTool"
    ],
    "malware_family": [
        "Emotet"
    ],
    "timestamps": {
        "first_seen": "2022-12-13T14:12:36.561000+00:00",
        "last_seen": "2022-12-14T07:22:32.278000+00:00"
    },
    "score": 22,
    "verdict": "malicious",
    "md5": "90c5cdec503679354f35b0960bf69813",
    "sha256": "89da7962c5ee659f243d397f94a32cacbf624cd9627c5e916a1532c26c35198c"
}
```

Type feeds

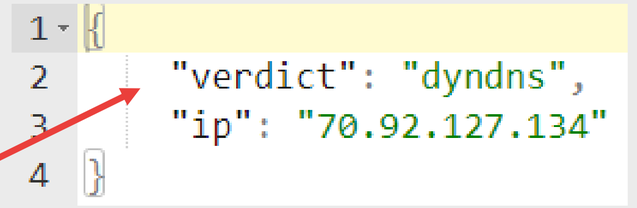
Категорированные IP-адреса

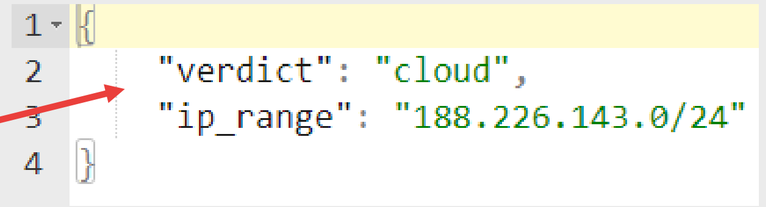
IP-адреса инфраструктуры DynDNS

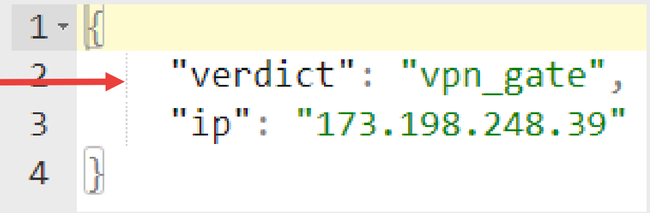
IP-адреса облачной инфраструктуры

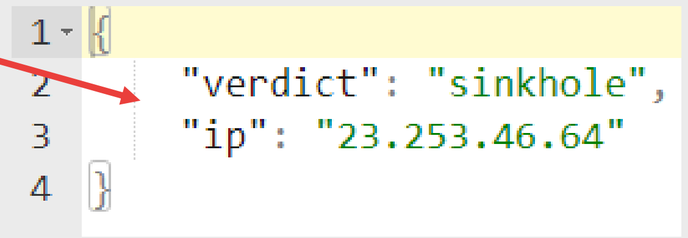
IP-адреса VPN-узлов

IP-адреса sinkhole-узлов





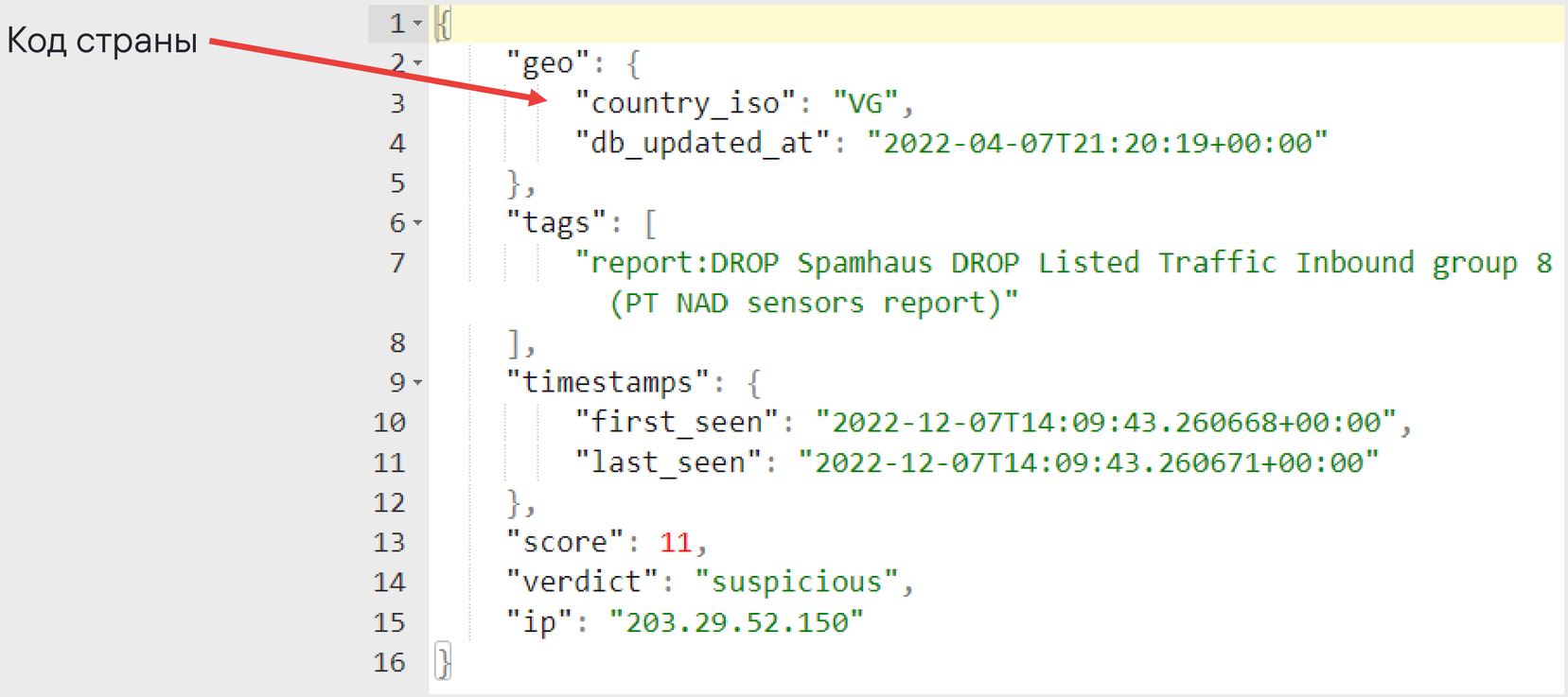




Geo anomaly IPs

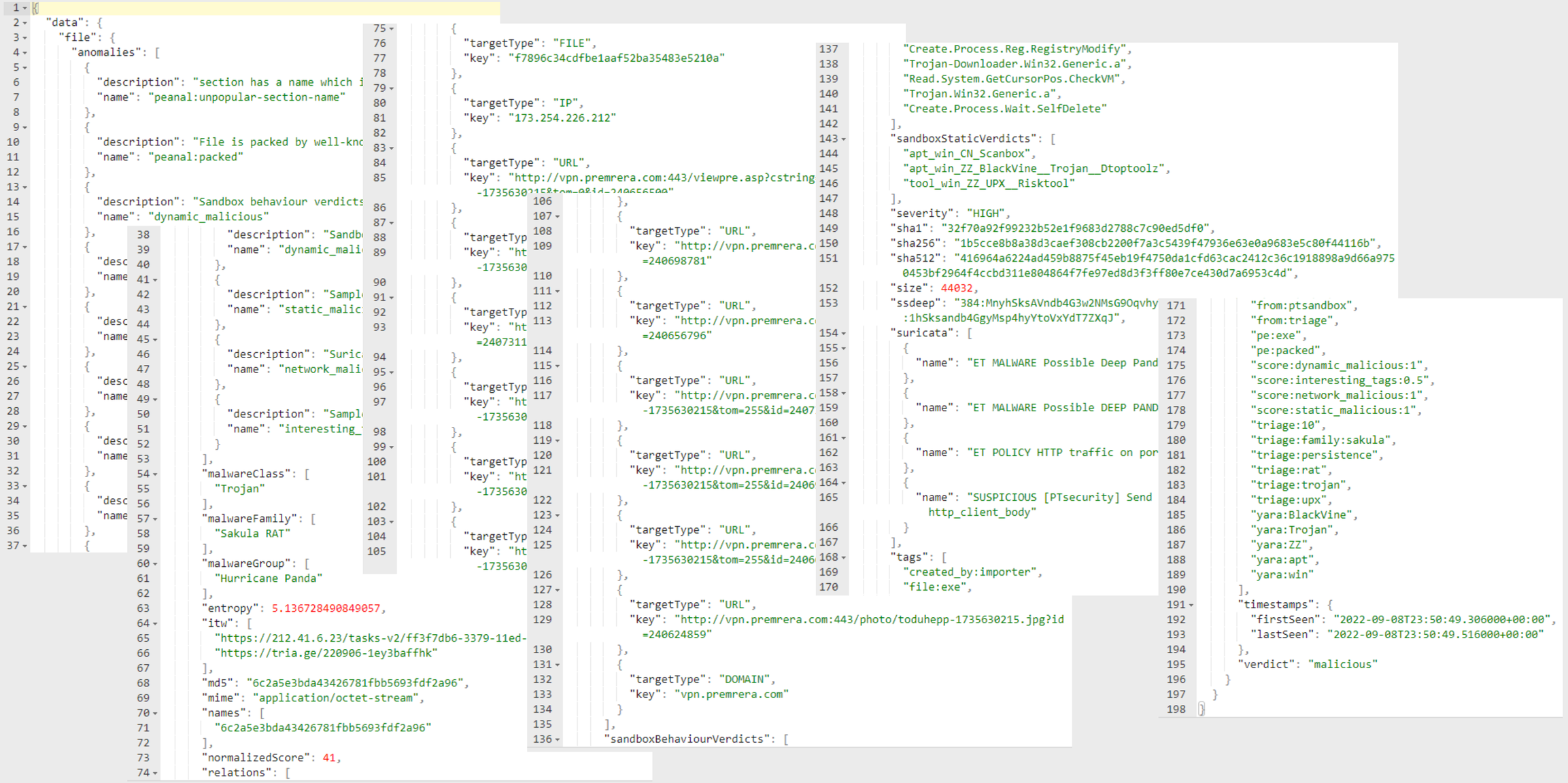
IP-адреса, размеченные по GeoIP,
без узлов, связанных с VPN, Proxy,
STUN, TorNode, DDNS

Код страны



```
{
    "geo": {
        "country_iso": "VG",
        "db_updated_at": "2022-04-07T21:20:19+00:00"
    },
    "tags": [
        "report:DROP Spamhaus DROP Listed Traffic Inbound group 8
          (PT NAD sensors report)"
    ],
    "timestamps": {
        "first_seen": "2022-12-07T14:09:43.260668+00:00",
        "last_seen": "2022-12-07T14:09:43.260671+00:00"
    },
    "score": 11,
    "verdict": "suspicious",
    "ip": "203.29.52.150"
}
```

Пример полного контекста



Какие еще есть фиды

1. White list domains / URLs / IPs/ hashes
2. Medium severity domains / URLs / IPs / hashes
3. CDN IPs
4. Upload malicious domains / URLs/ IPs
5. Cybercrime domains / URLs / IPs/ hashes
6. **... Здесь может быть фид, собранный специально для вас!**

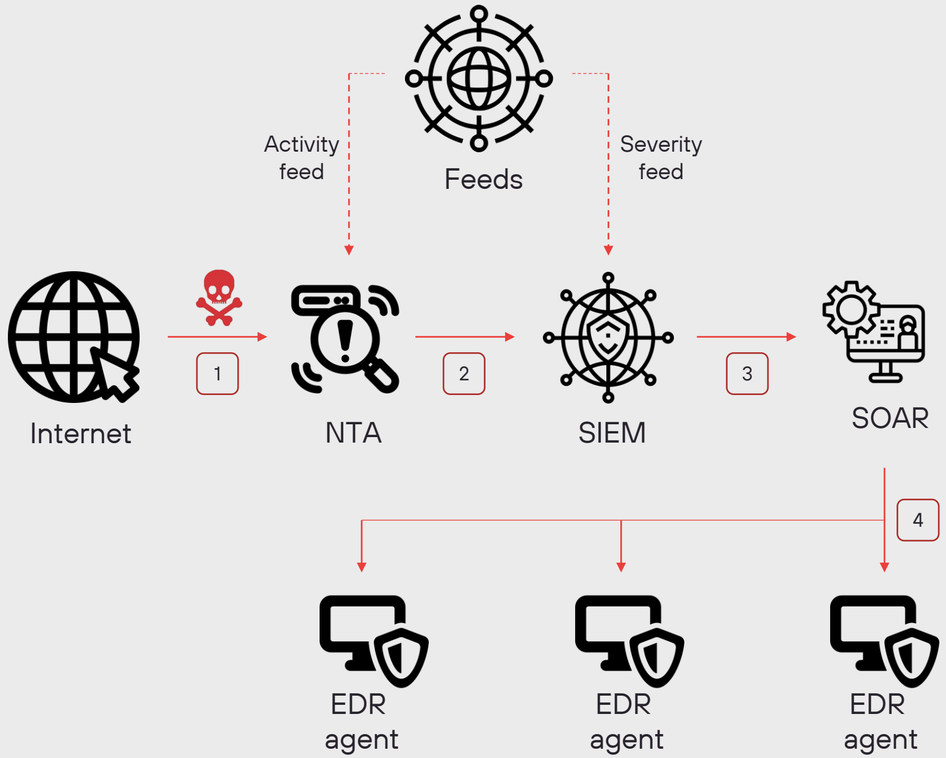
Что добавляем в фиды дальше

1. Группы злоумышленников
2. Инструменты хакеров
3. Отрасли
4. TTP
5. Уязвимости
6. Даркнет

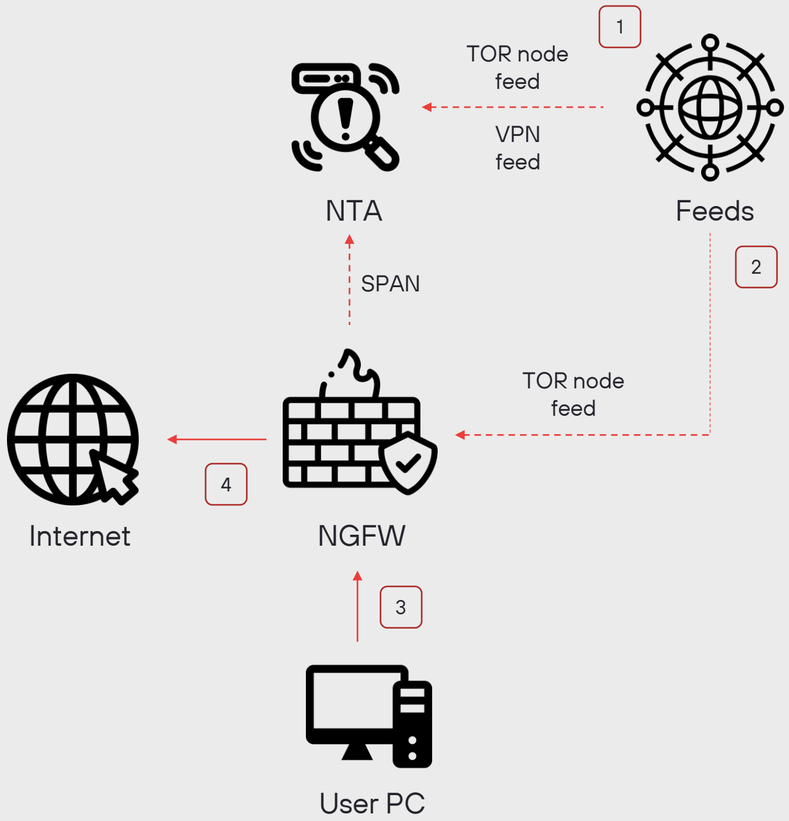
Сценарии использования фидов

Сценарий № 1

1. Детектирование вредоносной активности на NTA с помощью activity feed. Информация передается в SIEM
2. В SIEM инцидент приоритизируется с помощью severity feed. Карточка инцидента передается в SOAR
3. В SOAR создается задание на EDR с целью поиска связанных индикаторов на конечных узлах
4. Запускаются сценарии реагирования на агентах EDR



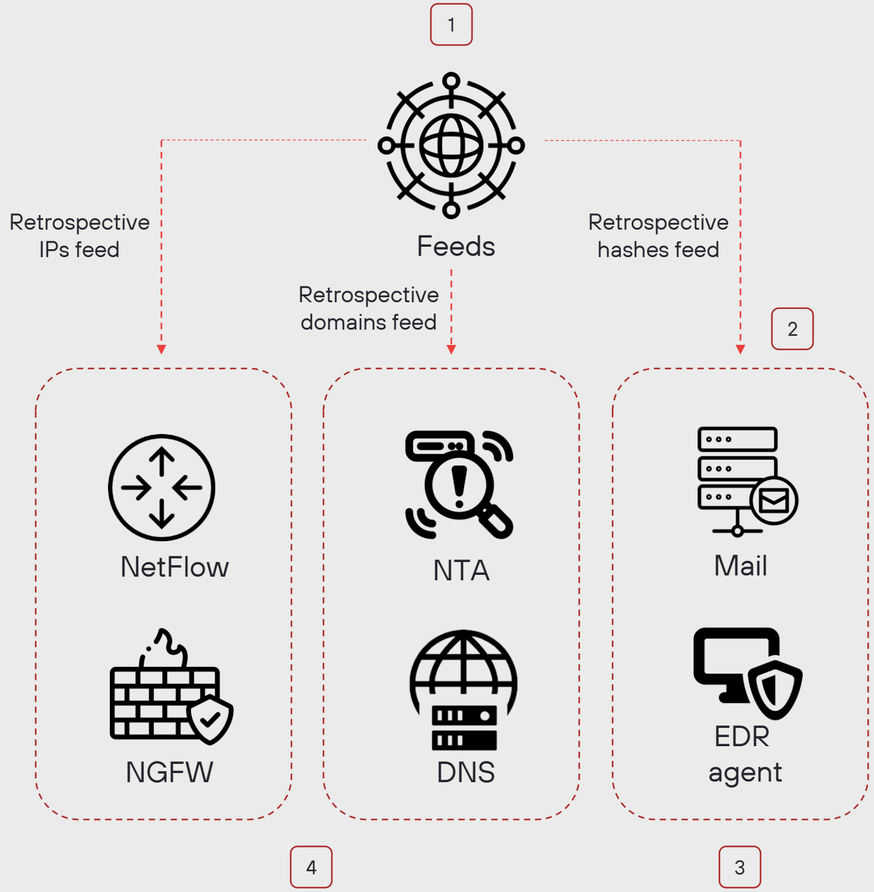
Сценарий № 2



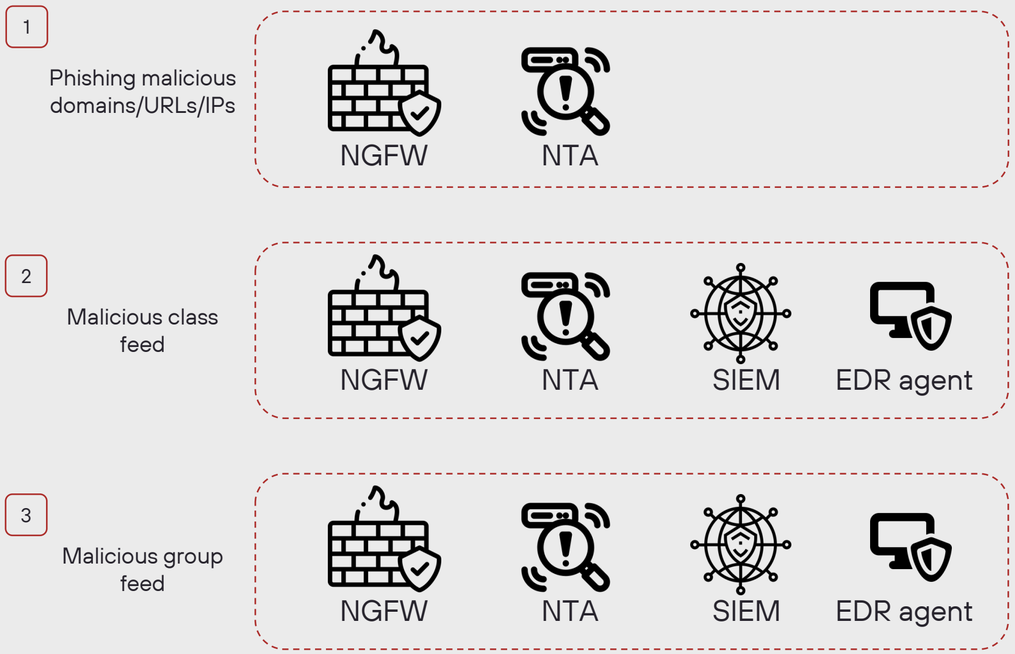
1. Для обнаружения попыток взаимодействия с ресурсами TOR и VPN на NTA в качестве источников информации служат TOR node feed и VPN feed
2. Для блокирования доступа на NGFW используется TOR node feed
3. Инсайдер предпринимает попытку установки вредоносного ПО с теневого форума
4. Взаимодействие с TOR-сетью заблокировано

Сценарий № 3

1. При проведении ретроспективного анализа фиды используются для поиска событий:
   - Retrospective IPs feed — в NetFlow и логах МСЭ;
   - Retrospective domains feed — в NTA и логах DNS;
   - Retrospective hashes feed — при анализе почтовых вложений или сканировании конечных узлов с помощью EDR
2. Обнаруживается ранее пропущенная фишинговая рассылка
3. По найденным образцам выявляются скомпрометированные узлы
4. Скомпрометированные узлы дополняются информацией из сетевых анализаторов



Сценарий № 4



1. Для предотвращения наиболее опасного вектора атаки — фишинга — используется фид Phishing malicious domains/URLs/IPs
2. Для противодействия наиболее опасному классу ВПО — ransomware — используется Malicious class feed
3. Для обнаружения атак конкретной активной группировки (Cloud Atlas) используется Malicious group feed

Подведем итоги

1. Внешние данные об угрозах помогают защищаться от кибератак

2. Фиды Positive Technologies помогают держать в фокусе актуальные угрозы

3. Поставщик данных подстраивает свои данные под заказчика, а не заказчика под данные

Регистрация на пилот

https://clck.ru/33t5NK

Спасибо!