

PT Threat Intelligence Feeds

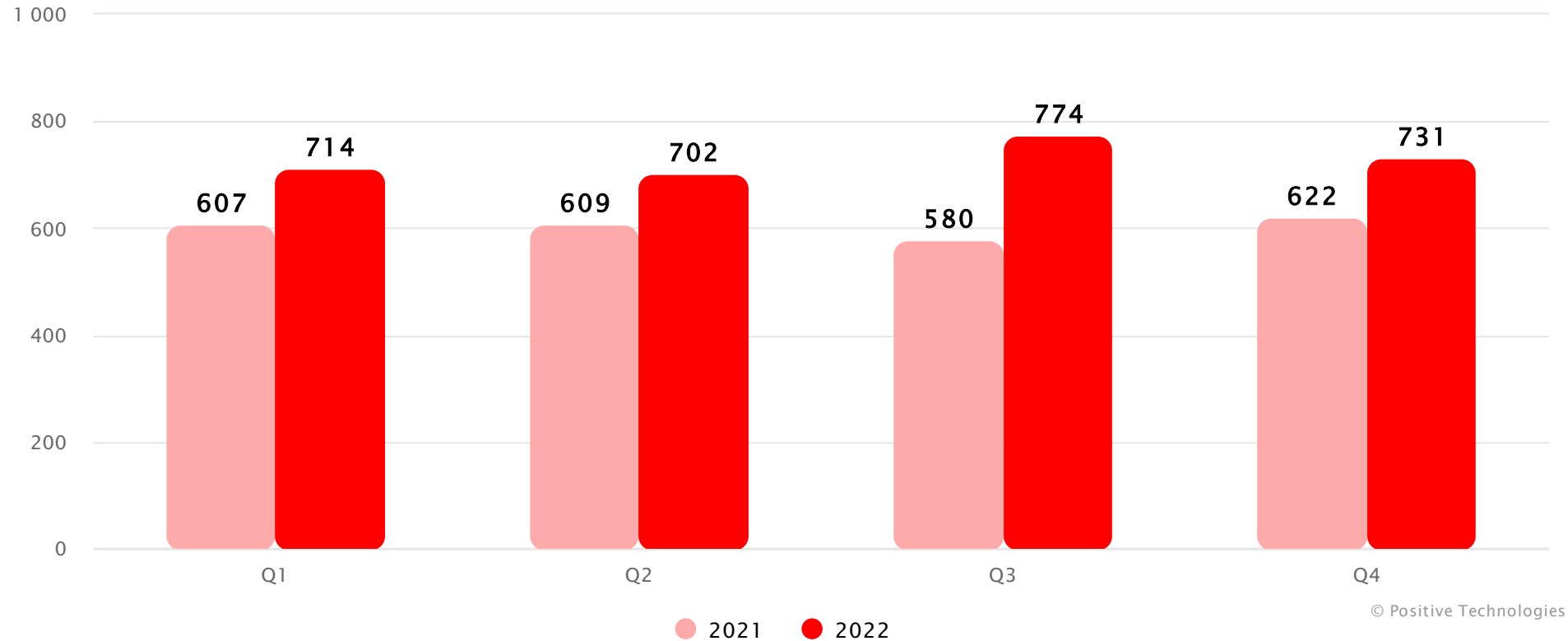
Что такое cyberthreat intelligence

- ➔ Cyberthreat intelligence (CTI) — информация, которая описывает **существующие или потенциальные угрозы** безопасности информационных систем и пользователей
- ➔ **Существует в разных формах:**
 - отчеты, содержащие сведения о мотивации, инфраструктуре и техниках определенного злоумышленника
 - IP-адреса, домены, URL и хеш-суммы файлов, связанные с известной угрозой
- ➔ **Используется организациями** для получения контекста событий безопасности и **позволяет быстро отреагировать** на угрозу

Атаки 2022

Актуальные киберугрозы: итоги 2022 года

Количество инцидентов в 2021 и 2022 годах (по кварталам)



Атакующие прогрессируют

Обнаружение атак — критически важная задача, которая с каждым днем становится все сложнее

67%

атак носят целенаправленный характер

96%

организаций не защищены от проникновения внешнего злоумышленника

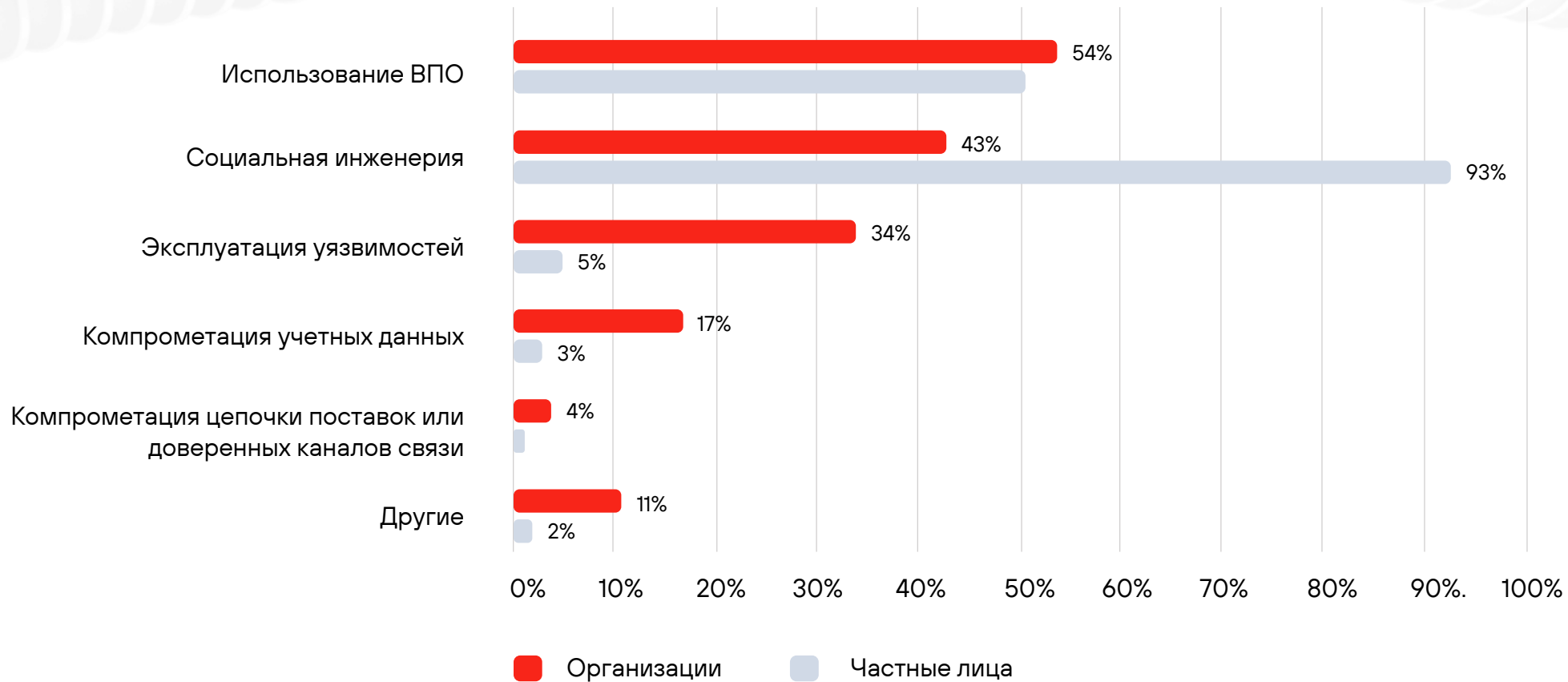
на **20,8%**

выросло общее количество инцидентов в 2022 году

в **84%**

организаций даже низкоквалифицированный злоумышленник может проникнуть в локальную сеть

Методы атак по итогам 2022 года



Для чего нам cyberthreat intelligence

Cyberthreat Intelligence предоставляет информацию о злоумышленниках



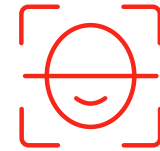
Инструментарий

ВПО и прочий инструментарий который используют злоумышленники



Инфраструктура

Серверы, веб-сайты, которые используют злоумышленники



Техники и тактики злоумышленников

Как злоумышленники используют свой инструментарий и инфраструктуру для атаки

Threat Intelligence 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 и повышают эффективность их работы

→ Позволяют предотвращать атаки на информационные системы

PT Feeds адаптирует систему защиты для противодействия актуальным киберугрозам



Показываем скрытые угрозы

Позволяем обнаружить атаку на ранних этапах



Блокируем актуальные угрозы

Проактивно блокируем критически опасные для организации угрозы на периметре



Ускоряем обработку событий

Экономим время, затрачиваемое на подтверждение, анализ и приоритизацию инцидента



Автоматизируем

Организуем работу с внешними данными



Интегрируемся

Автоматизируем доставку данных об угрозах в средства защиты и актуализацию информации



Предоставляем контекст

Дополняем данные об угрозах

Источники данных

PT NAD

Телеметрия, получаемая с инсталляций PT Network Attack Discovery

OSINT

Информация, полученная в ходе разведки по открытым источникам

ФинЦЕРТ

Данные, распространяемые центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере

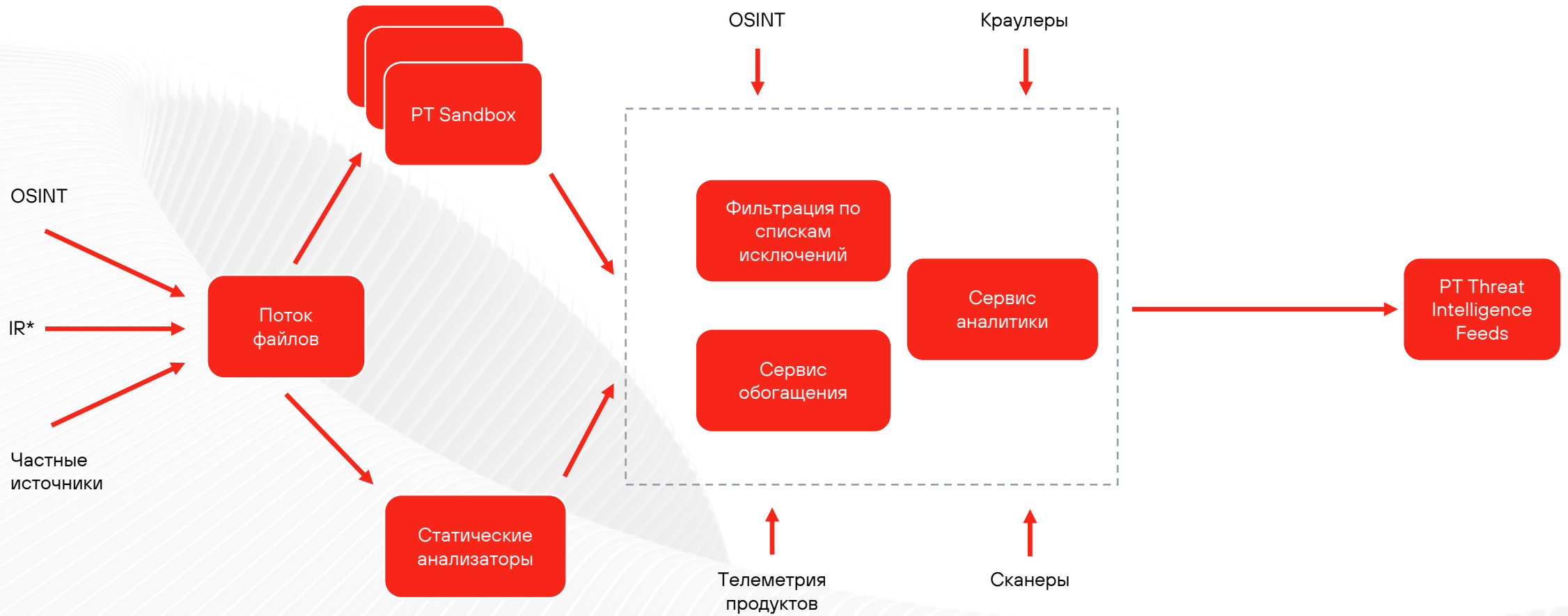
Расследования инцидентов

Результаты расследования инцидентов ИБ сотрудниками Positive Technologies

Исследования ВПО

Результаты анализа вредоносного программного обеспечения экспертным центром кибербезопасности Positive Technologies (PT ESC)

Схема обработки данных



Как использовать фиды

MaxPatrol SIEM

Обнаружение событий ИБ, в которых задействованы критически важные для клиента индикаторы компрометации

PT Network Attack Discovery

Обнаружение вредоносной активности в сетевом трафике

Threat Intelligence Platform

Расширение и дополнение контекстом уже существующей базы угроз

UTM-решение, NGFW, WAF

Обогащение используемых систем ИБ данными об угрозах, повышение эффективности этих систем и предотвращение атак

PT Threat Intelligence Feeds — это...

→ Данные, которые собраны
и обработаны специалистами
Positive Technologies

53 млн

файлов

2 млн

доменов

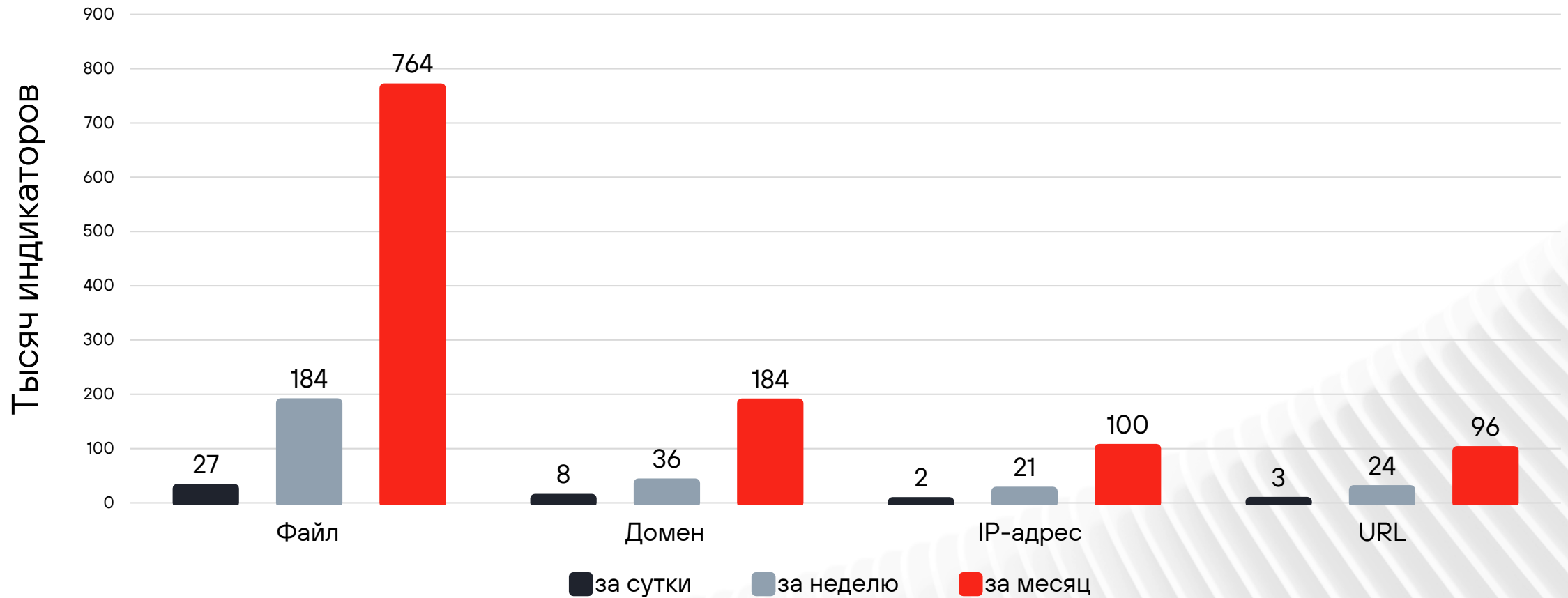
622 тыс.

URL

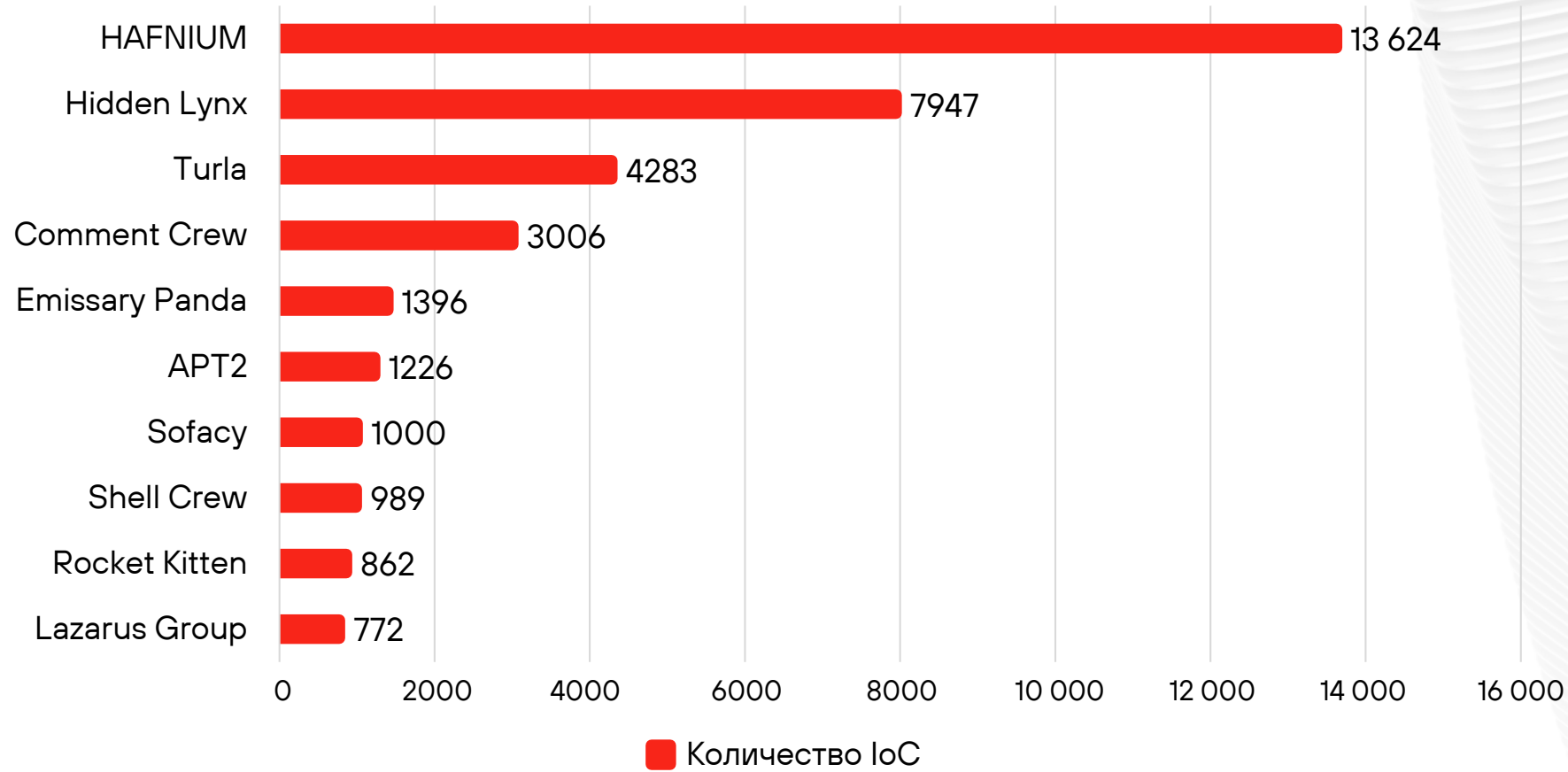
833 тыс.

IP-адресов

Среднее количество обрабатываемых данных



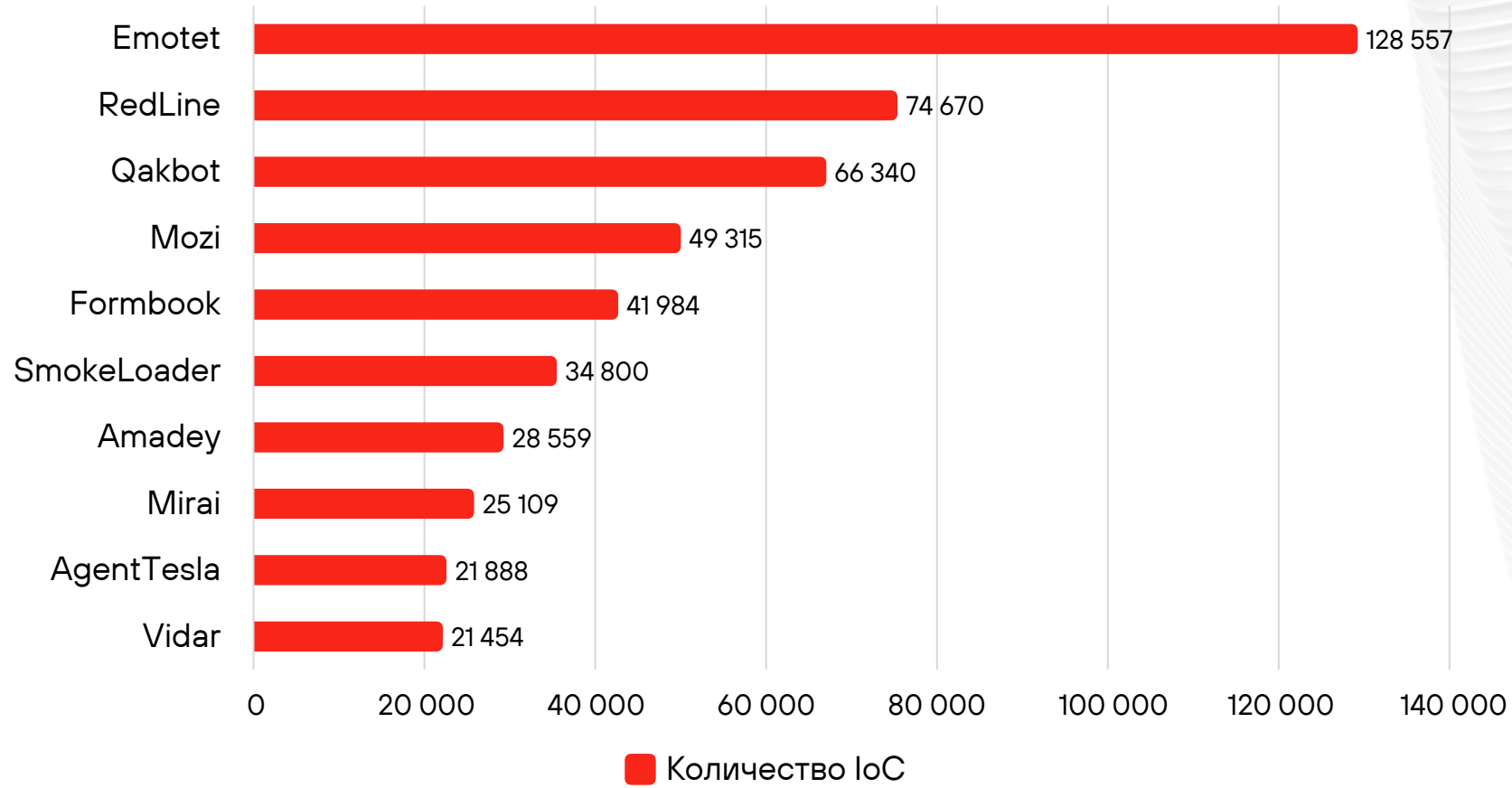
Топ-10 группировок



Более
150

вредоносных
группировок
в базе данных

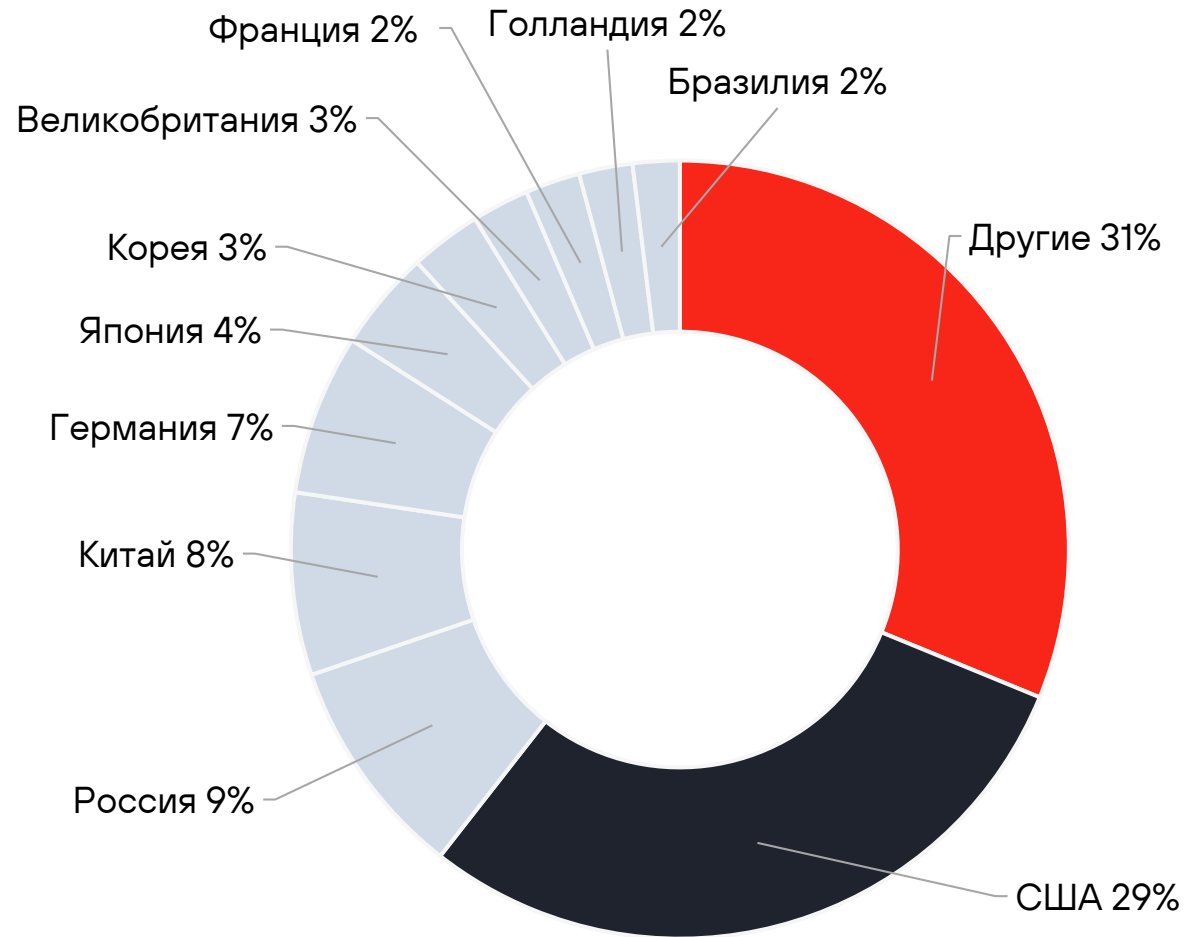
Топ-10 актуальных семейств ВПО



Более
1350

семейства ВПО в базе
данных

География распределения IP-адресов



В 196

странах
размещены
наблюдаемые IP-
адреса

PT Threat Intelligence Feeds — это...

→ Расширенный контекст, который помогает аналитикам быстрее интерпретировать данные

- Репутация индикатора на момент выгрузки
- Итоговый вердикт от Positive Technologies
- Временные метки
- Принадлежность к классу или семейству вредоносного ПО, к APT-группировке, вредоносной кампании или связь с ними
- Потенциальный ущерб — опасность угрозы, связанной с индикатором, для инфраструктуры организации
- Роли узла в сети
- Доступность домена или IP-адреса
- Вердикты антивирусов и песочниц
- Результаты обогащения WHOIS-, DNS-записей и т. д.

Какая информация есть в PT Feeds

Индикаторы, размеченные по степени опасности

Malicious

Вредоносные индикаторы без дополнительной разметки

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), tags, score, verdict

High Severity

Вредоносные индикаторы высокой степени опасности с точки зрения влияния на инфраструктуру предприятия

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), severity, malware_class, malware_family, tags, relations (hashes, domains, ips, urls), score, verdict

Medium Severity

Вредоносные индикаторы средней степени опасности с точки зрения влияния на инфраструктуру предприятия

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), severity, malware_class, malware_family, tags, relations (hashes, domains, ips, urls), score, verdict

Whitelist

Белый список индикаторов

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), verdict

Индикаторы, размеченные по времени активности

Current Activity

Вредоносные индикаторы, активные за последнюю неделю

md5 (для файловых индикаторов),sha256 (для файловых индикаторов),Domain / IP / URL (для сетевых индикаторов),timestamps (first_seen, last_seen),malware_class,malware_family,tags,score,verdict

Recent Activity

Вредоносные индикаторы, активные за последний месяц

md5 (для файловых индикаторов),sha256 (для файловых индикаторов),Domain / IP / URL (для сетевых индикаторов),timestamps (first_seen, last_seen),malware_class,malware_family,tags,score,verdict

Retrospective

Вредоносные индикаторы, активные за последний год

md5 (для файловых индикаторов),sha256 (для файловых индикаторов),Domain / IP / URL (для сетевых индикаторов),timestamps (first_seen, last_seen),malware_class,malware_family,tags,score,verdict

Индикаторы, размеченные по ролям узлов в сетевой инфраструктуре

TOR

Узлы сети TOR

IP, verdict

DynDNS

Инфраструктура DynDNS

Domain, verdict

Cloud

Облачная инфраструктура

IP/IP_range, verdict

Mail

Домены, относящиеся к почтовой инфраструктуре

Domain, verdict

STUN

STUN узлы

IP, verdict

Sinkhole

Sinkhole узлы

IP/IP_range, verdict

VPN

VPN инфраструктура

IP/IP_range, verdict

Exploiters

Эксплуатация уязвимостей

IP, verdict

CDN

CDN инфраструктура

Domain / IP / IP_range /
URL, verdict

Torrents

Торрент трекеры

Domain / IP / URL, verdict

Proxy

Прокси инфраструктура

Domain / IP / URL, verdict

Инфраструктура, используемая злоумышленниками

CnC

Вредоносные индикаторы, связанные с управляющими серверами злоумышленников

Domain / IP / URL (для сетевых индикаторов),timestamps (first_seen, last_seen),role,tags,score,verdict

Phishing

Вредоносные индикаторы, связанные с фишинговыми ресурсами злоумышленников

Domain / IP / URL (для сетевых индикаторов),timestamps (first_seen, last_seen),role,tags,score,verdict

Download

Вредоносные индикаторы, используемые злоумышленниками для скачивания полезной нагрузки

Domain / IP / URL (для сетевых индикаторов),timestamps (first_seen, last_seen),role,tags,score,verdict

Upload

Вредоносные индикаторы, используемые злоумышленниками для эксфильтрации данных

Domain / IP / URL (для сетевых индикаторов),timestamps (first_seen, last_seen),role,tags,score,verdict

Информация о вредоносном ПО

Malicious Class

Вредоносные индикаторы, размеченные по классам ВПО

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), malware_class, malware_family, tags, relations (hashes, domains, ips, urls), score, verdict

Malicious Family

Вредоносные индикаторы, размеченные по семействам ВПО

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), malware_class, malware_family, tags, relations (hashes, domains, ips, urls), score, verdict

Учитываем активность ВПО

Текущая активность

активные за последнюю неделю

Недавняя активность

активные за последний месяц

Ретроспектива

активные за последний год

Вредоносные кампании и группировки

Malicious Campaign

Вредоносные индикаторы, агрегированные по вредоносным кампаниям

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), malware_class, malware_family, tags, relations (hashes, domains, ips, urls), score, verdict

Malicious Group

Вредоносные индикаторы с разметкой по группировкам

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), malware_class, malware_family, tags, relations (hashes, domains, ips, urls), score, verdict

Учитываем активность кампаний и группировок

Текущая активность

активные за последнюю неделю

Недавняя активность

активные за последний месяц

Ретроспектива

активные за последний год

Индикаторы, размеченные по типам угроз

Cybercrime

Вредоносные индикаторы, размеченные как имеющие отношение к массовым угрозам

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), malware_class, malware_family, malware_group, tags, relations (hashes, domains, ips, urls), score, verdict, is_apr

APT

Вредоносные индикаторы, размеченные как имеющие отношение к целевым угрозам

md5 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), malware_class, malware_family, malware_group, tags, relations (hashes, domains, ips, urls), score, verdict, is_apr

Данные от регуляторов

FinCERT

Вредоносные индикаторы, передаваемые по линии ФинЦЕРТ

md5 (для файловых индикаторов), sha1 (для файловых индикаторов), sha256 (для файловых индикаторов), Domain / IP / URL (для сетевых индикаторов), timestamps (first_seen, last_seen), malware_class, malware_family, tags, role (для сетевых индикаторов), verdict

ГосСОПКА

Вредоносные индикаторы, передаваемые по линии НКЦКИ

скоро

PT Threat Intelligence Feeds — это...

→ Более 40 фидов
для разных целей

Примеры фидов

Домены, URL, IP-адреса, хеш-суммы, связанные с APT-атаками

- Вредоносные индикаторы, имеющие отношение к целевым угрозам

Семейства ВПО: недавняя активность

- Семейства ВПО: недавняя активность

Вредоносные кампании: недавняя активность

- Активные вредоносные индикаторы за последнюю неделю, агрегированные по вредоносным кампаниям

IP-адреса по географическому расположению

- IP-адреса, размеченные по GeoIP, без узлов, связанных с VPN, прокси-серверами, STUN, Tor, DDNS

PT Threat Intelligence Feeds — это...

- Донастройка потоков данных с индикаторами компрометации по пожеланиям заказчика



PT Threat Intelligence Feeds — это...

→ Онлайн-портал для проверки файлов и индикаторов компрометации

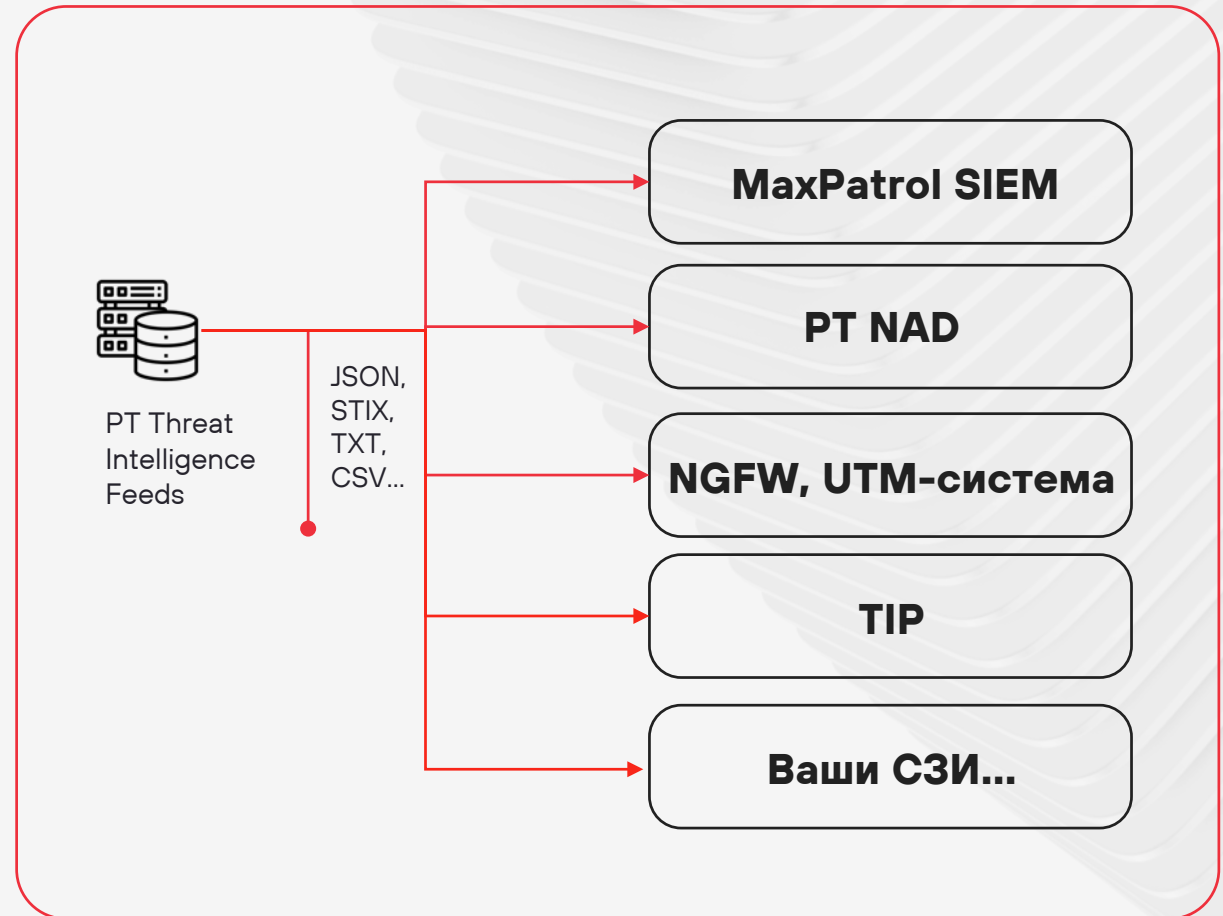
<https://iocportal.ptsecurity.com/>

The screenshot displays the PT IoC Portal web interface. The browser address bar shows the URL <https://iocportal.ptsecurity.com/report?ip=27.54.86.236>. The page title is "Отчет по IP-адресу" (Report by IP address). The main content area shows details for the IP address 27.54.86.236, including its IoC rating (39 из 100), potential damage (Высокий), first appearance (15 сентября 2022, 16:22), and last appearance (22 сентября 2023, 20:04). Below this, the "Общая информация" (General information) section lists various attributes: Address is pinged (Да), Role in network (download, upload), Verdict (malicious), WPO classes (Trojan-Spy, Trojan-Dropper, Trojan-PSW, Downloader), WPO families (Agent Tesla, Icedid), and Related groupings (Нет данных). The "Геоданные" (Geodata) section shows the server location (Australia) and the last update time (23 октября 2023, 11:14). The "Метки" (Tags) section lists two tags: "report:SPYWARE AgentTesla Exfiltration (Signature report)" and "report:TROJAN AgentTesla Exfil Via SMTP (Signature report)". The "Связи" (Connections) section is partially visible at the bottom.

Отчет по IP-адресу			
27.54.86.236			
Рейтинг IoC	Потенциальный ущерб	Первое появление	Последнее появление
39 из 100	Высокий	15 сентября 2022, 16:22	22 сентября 2023, 20:04
Общая информация			
Адрес пингуется	Да		
Роль узла в сети	download upload		
Вердикт	malicious		
Классы ВПО	Trojan-Spy Trojan-Dropper Trojan-PSW Downloader		
Семейства ВПО	Agent Tesla Icedid		
Связанные группировки	Нет данных		
Геоданные			
Расположение сервера	Australia		
Данные обновлены	23 октября 2023, 11:14		
Метки			
report:SPYWARE AgentTesla Exfiltration (Signature report) report:TROJAN AgentTesla Exfil Via SMTP (Signature report)			
Связи			

PT Threat Intelligence Feeds — это...

- Быстрая интеграция с СЗИ за счет широкого списка поддерживаемых продуктов и форматов



Способы интеграции

REST API

- Полностью документированный API
- Доступен [Python SDK](#)
- Подробности на [cybsi.cloud](#)

Коннектор ptFeeds

- Устанавливается в инфраструктуре заказчика
- Интегрирован с сервисом дистрибьюции
- Позволяет быстро организовать использование TI-данных

PT Feeds для периметровых СЗИ

Экспертиза Positive Technologies в вашем NGFW

Современные межсетевые экраны имеют возможность обрабатывать динамические репутационные списки с индикаторами компрометации

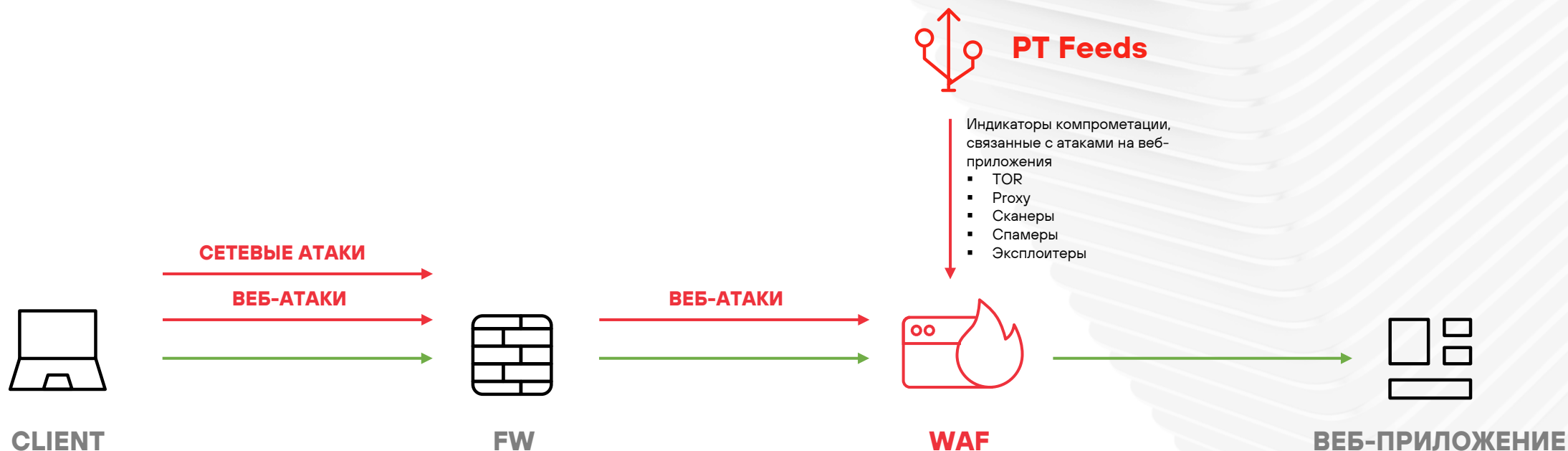


Обработка репутационных списков позволяет **автоматически реагировать на появляющиеся угрозы**

Репутационные списки Positive Technologies

- Основаны на данных, собираемых Positive Technologies
- Дополняют данные вендора
- Могут быть настроены по запросу заказчика

PT Feeds для Web-приложений



- Раннее обнаружение и блокировка источников вредоносной активности
- Информация об угрозах, актуальных для WEB-приложений

- Автоматизированная доставка информации об угрозах в реальном времени
- Автоматизированное обнаружение/блокировка вредоносного трафика на основе актуальных данных

PT Feeds для Web-приложений

Это IP адреса, с которых зафиксирована вредоносная активность по отношению к веб-приложениям

TOR

IP-адреса,
являющиеся узлами
TOR-сетей

Proxy

IP-адреса, относящиеся к
прокси-инфраструктуре

Сканнеры

любой брутфорс и пробники
(скан url path, перебор
логинов/паролей)

Спамеры

IP-адреса, с которых
отправляют спам
сообщения (в любые
веб-формы)

Эксплоитеры

IP-адреса, с которых происходят
попытки эксплуатации через
SQL injection, XSS и тд

PT Feeds для промышленных предприятий



Индикаторы компрометации, связанные с группировками специализирующихся на промышленном секторе

Отрасли

- Энергетическая
- Нефтегазовая
- Металлургия
- Машиностроение
- Химическая промышленность
- Легкая промышленность

Примеры состава фидов

Домены, URL, IP-адреса, хеш-суммы, связанные с APT-атаками

Онлайн-портал для проверки файлов и индикаторов компрометации

- 1 Связи с другими объектами
- 2 Теги
- 3 Рейтинг значимости

```
1 {
2   "is_apr": true,
3   "relations": {
4     "ips": [
5       "104.86.182.8",
6       "118.24.36.220",
7       "20.62.24.77",
8       "20.80.129.13",
9       "20.99.132.105",
10      "...",
11    ]
12  },
13  "tags": [
14    "vt:assembly",
15    "filescanio:obfuscated",
16    "hybrid:score:100",
17    "pe:SuspiciousRichHeader",
18    "...",
19  ],
20  "malware_group": [
21    "HAFNIUM"
22  ],
23  "malware_class": [
24    "Trojan"
25  ],
26  "malware_family": [
27    "CobaltStrike"
28  ],
29  "timestamps": {
30    "first_seen": "2022-01-17T02:41:03.020000+00:00",
31    "last_seen": "2022-12-09T20:26:46.336000+00:00"
32  },
33  "score": 47,
34  "verdict": "malicious",
35  "md5": "79c1cd9f78471c34a9fed7d12b838496",
36  "sha256": "552effa09cfc82eae0296e1b9c9f4a5a81122418f1bee8a1c44542b382670263"
37 }
```

Семейства ВПО: недавняя активность

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

1 Семейство ВПО

```
1- {  
2-   "timestamps": {  
3-     "first_seen": "2022-10-06T23:40:01.452000+00:00",  
4-     "last_seen": "2022-12-06T07:30:21.721000+00:00"  
5-   },  
6-   "malware_class": [  
7-     "Trojan-PSW"  
8-   ],  
9-   "malware_family": [  
10-    "AgentTesla"  
11-   ],  
12-   "tags": [  
13-     "tranco_pos:728421",  
14-     "vt:contacted_domain"  
15-   ],  
16-   "relations": {  
17-     "hashes": [  
18-       "32dd5c62c9ba03f651b221ed56d9e59e",  
19-       "ae2d12ab0f1df66d1ffe31ea65f7aae6",  
20-       "7e2acd5674194d4bf3f50e2d9000f184",  
21-       "b8aa1e8bb86854fbf2ae9a768183564f"  
22-     ],  
23-     "domains": [  
24-       "emailsrvr.com"  
25-     ],  
26-     "ips": [  
27-       "43.245.183.172"  
28-     ]  
29-   },  
30-   "score": 15,  
31-   "verdict": "malicious",  
32-   "domain": "lutanedukasi.co.id"  
33- }
```

Вредоносные кампании: недавняя активность

Активные вредоносные индикаторы за последнюю неделю, агрегированные по вредоносным кампаниям

1 Вредоносная кампания

```
1  {
2    "tags": [
3      "anyrun:emotet",
4      "file:zip",
5      "yara:win",
6      "...",
7    ],
8    "relations": {
9      "ips": [
10       "68.183.190.199",
11       "104.131.58.132",
12       "159.203.204.126",
13       "...",
14     ],
15     "urls": [
16       "http://68.183.190.199:8080/bml/acquire/cone/",
17       "http://104.131.58.132:8080/loadan/",
18       "http://159.203.204.126:8080/ringin/srvc/",
19       "...",
20     ]
21   },
22   "malware_campaign": [
23     "TA542/2022/12"
24   ],
25   "malware_group": [
26     "TA542"
27   ],
28   "malware_class": [
29     "Trojan-Banker",
30     "RiskTool"
31   ],
32   "malware_family": [
33     "Emotet"
34   ],
35   "timestamps": {
36     "first_seen": "2022-12-13T14:12:36.561000+00:00",
37     "last_seen": "2022-12-14T07:22:32.278000+00:00"
38   },
39   "score": 22,
40   "verdict": "malicious",
41   "md5": "90c5cdec503679354f35b0960bf69813",
42   "sha256": "89da7962c5ee659f243d397f94a32cacbf624cd9627c5e916a1532c26c35198c"
43 }
```

Индикаторы, сгруппированные по типам

- 1 IP-адреса инфраструктуры DDNS
- 2 IP-адреса облачной инфраструктуры
- 3 IP-адреса VPN-узлов
- 4 IP-адреса sinkhole-узлов

```
1 {  
2   1 "verdict": "dyndns",  
3     "ip": "70.92.127.134"  
4 }
```

```
1 {  
2   2 "verdict": "cloud",  
3     "ip_range": "188.226.143.0/24"  
4 }
```

```
1 {  
2   3 "verdict": "vpn_gate",  
3     "ip": "173.198.248.39"  
4 }
```

```
1 {  
2   4 "verdict": "sinkhole",  
3     "ip": "23.253.46.64"  
4 }
```

IP-адреса по географическому расположению

Активные вредоносные
индикаторы за последнюю неделю,
агрегированные по вредоносным
кампаниям

1 Код страны

```
1 {  
2   "geo": {  
3     1 "country_iso": "VG",  
4     "db_updated_at": "2022-04-07T21:20:19+00:00"  
5   },  
6   "tags": [  
7     "report:DROP Spamhaus DROP Listed Traffic Inbound group 8  
      (PT NAD sensors report)"  
8   ],  
9   "timestamps": {  
10     "first_seen": "2022-12-07T14:09:43.260668+00:00",  
11     "last_seen": "2022-12-07T14:09:43.260671+00:00"  
12   },  
13   "score": 11,  
14   "verdict": "suspicious",  
15   "ip": "203.29.52.150"  
16 }
```

```

2-  "data": {
3-    "file": {
4-      "anomalies": [
5-        {
6-          "description": "section has a name which is not a well-known",
7-          "name": "peanal:unpopular-section-name"
8-        },
9-        {
10-          "description": "File is packed by well-known packer",
11-          "name": "peanal:packed"
12-        },
13-        {
14-          "description": "Sandbox behaviour verdicts",
15-          "name": "dynamic_malicious"
16-        },
17-        {
18-          "description": "Sandbox behaviour verdicts",
19-          "name": "static_malicious"
20-        },
21-        {
22-          "description": "Sample has been matched by yara rule",
23-          "name": "static_malicious"
24-        },
25-        {
26-          "description": "Suricata rules",
27-          "name": "network_malicious"
28-        },
29-        {
30-          "description": "Sample with interesting tags",
31-          "name": "interesting_tags"
32-        },
33-        {
34-          "description": "malwareClass": [
35-            "Trojan"
36-          ],
37-          "malwareFamily": [
38-            "Sakula RAT"
39-          ],
40-          "malwareGroup": [
41-            "Hurricane Panda"
42-          ],
43-          "entropy": 5.136728490849057,
44-          "itw": [
45-            "https://212.41.6.23/tasks-v2/ff3f7db6-3379-11ed-98d1-1e4630ea5777",
46-            "https://tria.ge/220906-1ey3baffhk"
47-          ],
48-          "md5": "6c2a5e3bda43426781fbb5693fdf2a96",
49-          "mime": "application/octet-stream",
50-          "names": [
51-            "6c2a5e3bda43426781fbb5693fdf2a96"
52-          ],
53-          "normalizedScore": 41,
54-          "relations": [
55-            {
56-              "targetType": "FILE",
57-              "key": "f7896c34cdfb1aaf52ba35483e5210a"
58-            },
59-            {
60-              "targetType": "IP",
61-              "key": "173.254.226.212"
62-            },
63-            {
64-              "targetType": "URL",
65-              "key": "http://vpn.prempera.com:443/viewpre.asp?cstring=toduhepp-1735630215&tom=0&id=240656500"
66-            },
67-            {
68-              "targetType": "URL",
69-              "key": "http://vpn.prempera.com:443/photo/toduhepp-1735630215&tom=0&id=240698781"
70-            },
71-            {
72-              "targetType": "URL",
73-              "key": "http://vpn.prempera.com:443/photo/toduhepp-1735630215&tom=0&id=240656796"
74-            },
75-            {
76-              "targetType": "URL",
77-              "key": "http://vpn.prempera.com:443/viewpre.asp?cstring=toduhepp-1735630215&tom=25&id=2406731421"
78-            },
79-            {
80-              "targetType": "URL",
81-              "key": "http://vpn.prempera.com:443/viewpre.asp?cstring=toduhepp-1735630215&tom=25&id=240699093"
82-            },
83-            {
84-              "targetType": "URL",
85-              "key": "http://vpn.prempera.com:443/viewpre.asp?cstring=toduhepp-1735630215&tom=25&id=240667156"
86-            },
87-            {
88-              "targetType": "URL",
89-              "key": "http://vpn.prempera.com:443/photo/toduhepp-1735630215.jpg?id=240624859"
90-            },
91-            {
92-              "targetType": "DOMAIN",
93-              "key": "vpn.prempera.com"
94-            }
95-          ],
96-          "sandboxBehaviourVerdicts": [
97-            {
98-              "severity": "HIGH",
99-              "sha1": "32f70a92f99232b52e1f9683d2788c7c90ed5df0",
100-              "sha256": "1b5cce8b8a38d3caef308cb2200f7a3c5439f47936e63e0a9683e5c80f44116b",
101-              "sha512": "416964a622ad459b8875f45eb19f4750da1cf6d3cac2412c36c1918898a9d66a9750453bf2964f4cbbd311e804864f7fe97ed8d3f3ff80e7ce430d7a6953c4d",
102-              "size": 44032,
103-              "ssdeep": "384:MnyhSksAVndb4G3wZNMhG90qhyY3Q60VxYwvRhg7+1XXRodY6kLdAeMB:1hSksandb4GgyMsp4hyYtoVxYd17ZXqj",
104-              "suricata": [
105-                {
106-                  "name": "ET MALWARE Possible Deep Panda - Sakula/Mivast RAT CnC Beacon 5"
107-                },
108-                {
109-                  "name": "ET MALWARE Possible Deep Panda - Sakula/Mivast RAT CnC Beacon 5"
110-                },
111-                {
112-                  "name": "ET POLICY HTTP t
113-                },
114-                {
115-                  "name": "SUSPICIOUS [PTSe
116-                    http_client_body"
117-                }
118-              ],
119-              "tags": [
120-                "created_by:importer",
121-                "file:exe",
122-                "from:ptsandbox",
123-                "from:triage",
124-                "pe:exe",
125-                "pe:packed",
126-                "score:dynamic_malicious:1",
127-                "score:interesting_tags:0.5",
128-                "score:network_malicious:1",
129-                "score:static_malicious:1",
130-                "triage:10",
131-                "triage:family:sakula",
132-                "triage:persistence",
133-                "triage:rat",
134-                "triage:trojan",
135-                "triage:upx",
136-                "yara:BlackVine",
137-                "yara:Trojan",
138-                "yara:ZZ",
139-                "yara:apt",
140-                "yara:win"
141-              ],
142-              "timestamps": {
143-                "firstSeen": "2022-09-08T23:50:49.306000+00:00",
144-                "lastSeen": "2022-09-08T23:50:49.516000+00:00"
145-              },
146-              "verdict": "malicious"
147-            }
148-          ]
149-        }
150-      ]
151-    }
152-  }
153-}

```

Что будем добавлять в фиды

1 ✓

Группировки
злоумышленников

2 ✓

Инструменты
хакеров

3 ✓

Сферы
деятельности

4

ТТР

5

Уязвимости

6

Дарквеб

Спасибо!