# Threat Intelligence Feeds

Описание продукта

Дата редакции документа: 23.08.2023

# Содержание

# 1. Общие сведения

PT Threat Intelligence Feeds (PT Feeds) позволяет командам SOC быть в курсе актуальных угроз ИБ. Продукт содержит широкий спектр индикаторов компрометации, включая:

— домены,

— IP-адреса,

— ссылки,

— хеш-суммы файлов.

Данные для PT Feeds формируют эксперты PT ESC, используя материалы расследований инцидентов, исследований хакерских группировок, а также обезличенные данные продуктов Positive Technologies.

# 2. Особенности и преимущества

## Уникальные данные о реальных угрозах

Обезличенная телеметрия с сотен инсталляций продуктов Positive Technologies позволяет формировать знания о том, что происходит в мире ИБ прямо сейчас.

## Репутация и оценка потенциального ущерба

Для каждого индикатора компрометации рассчитываются показатели «Репутация» и «Потенциальный ущерб». Это помогает приоритизировать угрозы, оценить возможный ущерб от их реализации и сфокусироваться на предотвращении самых опасных из них.

## Расширенные контекстные данные

Обогащение индикаторов компрометации дополнительными данными помогает аналитикам SOC принимать решения по реагированию на угрозы.

## Более 40 фидов

Индикаторы компрометации в составе PT Feeds объединены в коллекции по целям их применения: для таргетированных атак, относящиеся к определенным семействам ВПО, конкретным вредоносным кампаниям и т. д.

## Интеграция с продуктами разных вендоров

PT Feeds поддерживает разные форматы и широкий перечень средств защиты информации, который постоянно дополняется.

# 3. Доступный перечень фидов

В таблице ниже представлен доступный заказчикам перечень потоков данных с индикаторами компрометации. Перечень приведен для демонстрации возможных срезов данных репутационного сервиса Positive Technologies. По запросу заказчика могут быть сформированы индивидуальные потоки данных.

Таблица 1. Доступный перечень фидов

| № | Наименование | Описание |
|---|---|---|
| 1 | Malicious Domains / URLs / IPs / Hashes | Вредоносные индикаторы без дополнительной разметки |
| 2 | White List Domains / URLs / IPs / Hashes | Белый список индикаторов |
| 3 | High Severity Domains / URLs / IPs / Hashes | Вредоносные индикаторы высокой степени опасности с точки зрения влияния на инфраструктуру предприятия |
| 4 | Medium Severity Domains / URLs / IPs / Hashes | Вредоносные индикаторы средней степени опасности с точки зрения влияния на инфраструктуру предприятия |
| 5 | Current Activity Domains / URLs / IPs / Hashes | Вредоносные индикаторы, активные за последнюю неделю |
| 6 | Recent Activity Domains / URLs / IPs / Hashes | Вредоносные индикаторы, активные за последний месяц |
| 7 | Retrospective Domains / URLs / IPs / Hashes | Вредоносные индикаторы, активные за последний год |
| 8 | Current Activity Severity Domains / URLs / IPs / Hashes | Вредоносные индикаторы с разметкой по степени опасности, активные за последнюю неделю |
| 9 | Recent Activity Severity Domains / URLs / IPs / Hashes | Вредоносные индикаторы с разметкой по степени опасности, активные за последний месяц |
| 10 | Retrospective Severity Domains / URLs / IPs / Hashes | Вредоносные индикаторы с разметкой по степени опасности, активные за последний год |
| 11 | TOR IPs | IP-адреса, размеченные как узлы Tor |
| 12 | DynDNS Domains / IPs | Домены и IP-адреса, относящиеся к инфраструктуре DynDNS |
| 13 | Cloud IPs | IP-адреса, относящиеся к облачной инфраструктуре |
| 14 | VPN IPs | IP-адреса, относящиеся к VPN |

| № | Наименование | Описание |
|---|---|---|
| 15 | STUN IPs | IP-адреса, размеченные как STUN |
| 16 | Sinkhole Domains / IPs | Домены и IP-адреса, размеченные как sinkhole-узлы |
| 17 | Mail Domains / IPs | Домены и IP-адреса, относящиеся к почтовой инфраструктуре |
| 18 | CDN IPs | IP-адреса, относящиеся к CDN-инфраструктуре |
| 19 | Torrents IPs | IP-адреса, относящиеся к торрент-трекерам |
| 20 | Proxy IPs | IP-адреса, относящиеся к прокси-инфраструктуре |
| 21 | Exploiters IPs | IP-адреса узлов, связанных с эксплуатацией уязвимостей |
| 22 | CnC Malicious Domains / URLs / IPs | Вредоносные домены / URL / IP-адреса, связанные с управляющими серверами злоумышленников |
| 23 | Phishing Malicious Domains / URLs / IPs | Вредоносные домены / URL / IP-адреса, связанные с фишинговыми ресурсами злоумышленников |
| 24 | Download Malicious Domains / URLs / IPs | Вредоносные домены / URL / IP-адреса, используемые злоумышленниками для скачивания полезной нагрузки |
| 25 | Upload Malicious Domains / URLs / IPs | Вредоносные домены / URL / IP-адреса, используемые злоумышленниками для эксфильтрации данных |
| 26 | Malicious Class Domains / URLs / IPs / Hashes | Вредоносные индикаторы, размеченные по классам вредоносного программного обеспечения |
| 27 | Malicious Class Current Activity | Вредоносные индикаторы, размеченные по классам вредоносного программного обеспечения, активные за последнюю неделю |
| 28 | Malicious Class Recent Activity | Вредоносные индикаторы, размеченные по классам вредоносного программного обеспечения, активные за последний месяц |
| 29 | Malicious Class Retrospective | Вредоносные индикаторы, размеченные по классам вредоносного программного обеспечения, активные за последний год |

| № | Наименование | Описание |
|---|---|---|
| 30 | Malicious Family Domains / URLs / IPs / Hashes | Вредоносные индикаторы, размеченные по семействам вредоносного программного обеспечения |
| 31 | Malicious Family Current Activity | Вредоносные индикаторы, размеченные по семействам вредоносного программного обеспечения, активные за последнюю неделю |
| 32 | Malicious Family Recent Activity | Вредоносные индикаторы, размеченные по семействам вредоносного программного обеспечения, активные за последний месяц |
| 33 | Malicious Family Retrospective | Вредоносные индикаторы, размеченные по семействам вредоносного программного обеспечения, активные за последний год |
| 34 | Malicious Campaign Domains / URLs / IPs / Hashes | Вредоносные индикаторы, агрегированные по вредоносным кампаниям |
| 35 | Malicious Campaign Current Activity | Вредоносные индикаторы, агрегированные по вредоносным кампаниям, активные за последнюю неделю |
| 36 | Malicious Campaign Recent Activity | Вредоносные индикаторы, агрегированные по вредоносным кампаниям, активные за последний месяц |
| 37 | Malicious Campaign Retrospective | Вредоносные индикаторы, агрегированные по вредоносным кампаниям, активные за последний год |
| 38 | Malicious Group Domains / URLs / IPs / Hashes | Вредоносные индикаторы с разметкой по группировкам |
| 39 | Malicious Group Current Activity | Вредоносные индикаторы с разметкой по группировкам, активные за последнюю неделю |
| 40 | Malicious Group Recent Activity | Вредоносные индикаторы с разметкой по группировкам, активные за последний месяц |
| 41 | Malicious Group Retrospective | Вредоносные индикаторы с разметкой по группировкам, активные за последний год |
| 42 | Cybercrime Domains / URLs / IPs / Hashes | Вредоносные индикаторы, размеченные как имеющие отношение к массовым угрозам |
| 43 | APT Domains / URLs / IPs / Hashes | Вредоносные индикаторы, размеченные как имеющие отношение к целевым угрозам |
| 44 | Geo Anomaly IPs | IP-адреса, размеченные по GeoIP, без узлов, связанных с VPN, прокси, STUN, Tor, DynDNS |

| № | Наименование | Описание |
|---|---|---|
| 45 | FinCERT Domains / URLs / IPs / Hashes | Вредоносные индикаторы, передаваемые по линии ФинЦЕРТ |

# 4. Перечень атрибутов объектов

Ниже представлены атрибуты объектов, которые могут быть описаны в коллекции. Список не является исчерпывающим и может корректироваться в зависимости от схемы, согласно которой формируется коллекция.

Общий список атрибутов индикаторов компрометации:

— Репутация индикатора на момент выгрузки.

— Итоговый вердикт.

— Временные метки.

— Принадлежность или связь:

  • с классом вредоносного ПО,

  • с семейством вредоносного ПО,

  • с группировками APT / киберпреступностью,

  • с вредоносной кампанией.

— Потенциальный ущерб — опасность угрозы, связанной с индикатором, для инфраструктуры организации.

— Роли узла в сети.

— Доступность домена или IP-адреса.

— Вердикты антивирусов и песочниц.

— Результаты обогащений с помощью WHOIS/DNS.

Детальные описания атрибутов каждой сущности приведены ниже.

### В этом разделе



## 4.1. Итоговые вердикты по индикаторам

Класс `Verdict` — это перечисление, объекты которого принимают следующие значения:

— `unscored` — вердикт индикатора не определен;

— `suspicious` — подозрительный индикатор, который нельзя явно отнести к `clean` или `malicious`;

— `clean` — индикатор, признанный безопасным по итогам анализа контекста;

— `malicious` — вредоносный индикатор;
— `whitelisted` — индикатор, признанный безопасным на основе белых списков;
— `torrent_tracker` — индикатор, связанный с инфраструктурой торрент-трекеров;
— `sinkhole` — индикатор, относящийся к sinkhole-узлам;
— `parking` — индикатор, используемый для парковки незарегистрированных доменов;
— `public_dns_server` — индикатор, относящийся к общедоступным DNS-серверам;
— `scanner` — индикатор, связанный с активностью сканеров сетевых ресурсов;
— `cloud` — индикатор, относящийся к облачной инфраструктуре крупных компаний;
— `stun` — индикатор, относящийся к STUN-серверам;
— `tor_node` — индикатор, относящийся к узлам Tor;
— `crawler` — индикатор, относящийся к краулерам информации веб-сервисов;
— `cdn` — индикатор, относящийся к инфраструктуре CDN;
— `vpn_gate` — индикатор, относящийся к инфраструктуре VPN;
— `proxy` — индикатор, относящийся к прокси-инфраструктуре;
— `exploiter` — индикатор, связанный с эксплуатацией уязвимостей.

## 4.2. Роль сетевого индикатора в инфраструктуре злоумышленника

Класс `Role` — это перечисление, объекты которого принимают следующие значения:

— `unknown` — роль узла не определена;
— `cnc` — управляющий сервер злоумышленников;
— `phishing` — сетевой узел, связанный с фишингом;
— `download` — сетевой узел, связанный с загрузкой вредоносного ПО;
— `upload` — сетевой узел, связанный с эксфильтрацией данных.

## 4.3. Перечень атрибутов индикаторов компрометации

Ниже представлено описание имеющихся атрибутов для различных типов индикаторов компрометации.

### В этом разделе



## 4.3.1. File и URL

Таблица 2. File и URL

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| `normalized_score` | Integer | Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный |
| `verdict` | String | Результат проверки. Возможные значения: `suspicious`, `clean`, `malicious`, `whitelisted`, `torrent_tracker`, `sinkhole`, `parking`, `public_dns_server`, `port_scanner`, `dyndns`, `cloud`, `stun`, `tor_node`, `crawler`, `cdn`, `ad_server`, `crl_ocsp`, `free_email`, `vpn_gate`, `ip_to_domain`, `free_proxy` |
| `timestamps` | Object | Временные метки |
| `timestamps → first_seen` | String (date-time) | Дата и время первого упоминания объекта |
| `timestamps → last_seen` | String (date-time) | Дата и время последнего упоминания объекта |
| `malware_class` | Array of strings | Классы вредоносного ПО, к которым относится файл |
| `malware_family` | Array of strings | Семейства вредоносного ПО, к которым относится файл |
| `malware_group` | Array of strings | Файл используется злоумышленниками |

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| malware_campaign | Array of strings | Файл замечен во вредоносных кампаниях |
| severity | String | Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения:<br>— High — большой;<br>— Medium — средний;<br>— Low — малый;<br>— None — неизвестен |
| is_apt | Boolean | Объект связан с активностью APT-группировок |
| relations | Array of objects | Информация о связях объекта с другими объектами |
| relations → target_type | String | Объект — цель связи. Возможные значения: IP, DOMAIN, FILE, URL, IP_RANGE |
| relations → type | String | Тип связи. Возможные значения: none, dropped_file, ip_resolved, called_ip, called_domain, called_url, downloaded_file, subdomain, ip_range, url_parent_domain, url_parent_ip, url_resolved, ptr_resolve, spf_domain |
| relations → key | String | Ключевой атрибут объекта — цели связи |
| relations → direction | String | Направление связи. Возможные значения: NONE, SOURCE, RECEIVER |
| av_verdicts | Array of strings | Результат проверки файла средствами антивирусной защиты |

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| tags | Array of strings | Метки |

## 4.3.2. IPaddress

Таблица 3. IPaddress

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| normalized_score | Integer | Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный |
| verdict | String | Результат проверки. Возможные значения: suspicious, clean, malicious, whitelisted, torrent_tracker, sinkhole, parking, public_dns_server, port_scanner, dyndns, cloud, stun, tor_node, crawler, cdn, ad_server, crl_ocsp, free_email, vpn_gate, ip_to_domain, free_proxy |
| timestamps | Object | Временные метки |
| timestamps → first_seen | String (date-time) | Дата и время первого упоминания объекта |
| timestamps → last_seen | String (date-time) | Дата и время последнего упоминания объекта |
| malware_class | Array of strings | Классы вредоносного ПО, к которым относится файл |
| malware_family | Array of strings | Семейства вредоносного ПО, к которым относится файл |
| malware_group | Array of strings | Файл используется злоумышленниками |
| malware_campaign | Array of strings | Файл замечен во вредоносных кампаниях |

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| severity | String | Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения:<br>— High — большой;<br>— Medium — средний;<br>— Low — малый;<br>— None — неизвестен |
| role | Array of strings | Роли узла в сети. Возможные значения атрибута: unknown, cnc, phishing, download, upload |
| is_apt | Boolean | Объект связан с активностью APT-группировок |
| geo | Object | Географические данные |
| geo → country_iso | String | Двухбуквенный код страны согласно ISO 3166-1 |
| geo → city | String | Название города |
| geo → db_updated_at | String (date-time) | Дата и время обновления информации о геолокации |
| geo → country | String | Название страны |
| relations | Array of objects | Информация о связях объекта с другими объектами |
| relations → target_type | String | Объект — цель связи. Возможные значения: IP, DOMAIN, FILE, URL, IP_RANGE |
| relations → type | String | Тип связи. Возможные значения: none, dropped_file, ip_resolved, called_ip, called_domain, called_url, downloaded_file, subdomain, ip_range, url_parent_domain, |

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| | | `url_parent_ip`, `url_resolved`, `ptr_resolve`, `spf_domain` |
| `relations → key` | String | Ключевой атрибут объекта — цели связи |
| `relations → direction` | String | Направление связи. Возможные значения: `NONE`, `SOURCE`, `RECEIVER` |
| `av_verdicts` | Array of strings | Результат проверки файла средствами антивирусной защиты |
| `tags` | Array of strings | Метки |

## 4.3.3. DomainName

Таблица 4. DomainName

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| `normalized_score` | Integer | Репутация объекта на момент выгрузки. От 0 до 100, где 100 — вредоносный, 0 — безопасный |
| `verdict` | String | Результат проверки. Возможные значения: `suspicious`, `clean`, `malicious`, `whitelisted`, `torrent_tracker`, `sinkhole`, `parking`, `public_dns_server`, `port_scanner`, `dyndns`, `cloud`, `stun`, `tor_node`, `crawler`, `cdn`, `ad_server`, `crl_ocsp`, `free_email`, `vpn_gate`, `ip_to_domain`, `free_proxy` |
| `timestamps` | Object | Временные метки |
| `timestamps → first_seen` | String (date-time) | Дата и время первого упоминания объекта |
| `timestamps → last_seen` | String (date-time) | Дата и время последнего упоминания объекта |
| `malware_class` | Array of strings | Классы вредоносного ПО, к которым относится файл |

| Атрибут | Тип (формат) | Описание |
|---|---|---|
| malware_family | Array of strings | Семейства вредоносного ПО, к которым относится файл |
| malware_group | Array of strings | Файл используется злоумышленниками |
| malware_campaign | Array of strings | Файл замечен во вредоносных кампаниях |
| severity | String | Потенциальный ущерб — возможное негативное влияние объекта на инфраструктуру организации. Возможные значения:<br>— High — большой;<br>— Medium — средний;<br>— Low — малый;<br>— None — неизвестен |
| role | Array of strings | Роли узла в сети. Возможные значения атрибута: unknown, cnc, phishing, download, upload |
| is_apt | Boolean | Объект связан с активностью APT-группировок |
| relations | Array of objects | Информация о связях объекта другими объектами |
| relations → target_type | String | Объект — цель связи. Возможные значения: IP, DOMAIN, FILE, URL, IP_RANGE |
| relations → type | String | Тип связи. Возможные значения: none, dropped_file, ip_resolved, called_ip, called_domain, called_url, downloaded_file, subdomain, ip_range, url_parent_domain, url_parent_ip, url_resolved, ptr_resolve, spf_domain |
| relations → key | String | Ключевой атрибут объекта — цели связи |
| relations → direction | String | Направление связи. Возможные значения: NONE, SOURCE, RECEIVER |

| Атрибут | Тип (формат) | Описание |
| --- | --- | --- |
| av_verdicts | Array of strings | Результат проверки файла средствами антивирусной защиты |
| tags | Array of strings | Метки |

positive
technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.