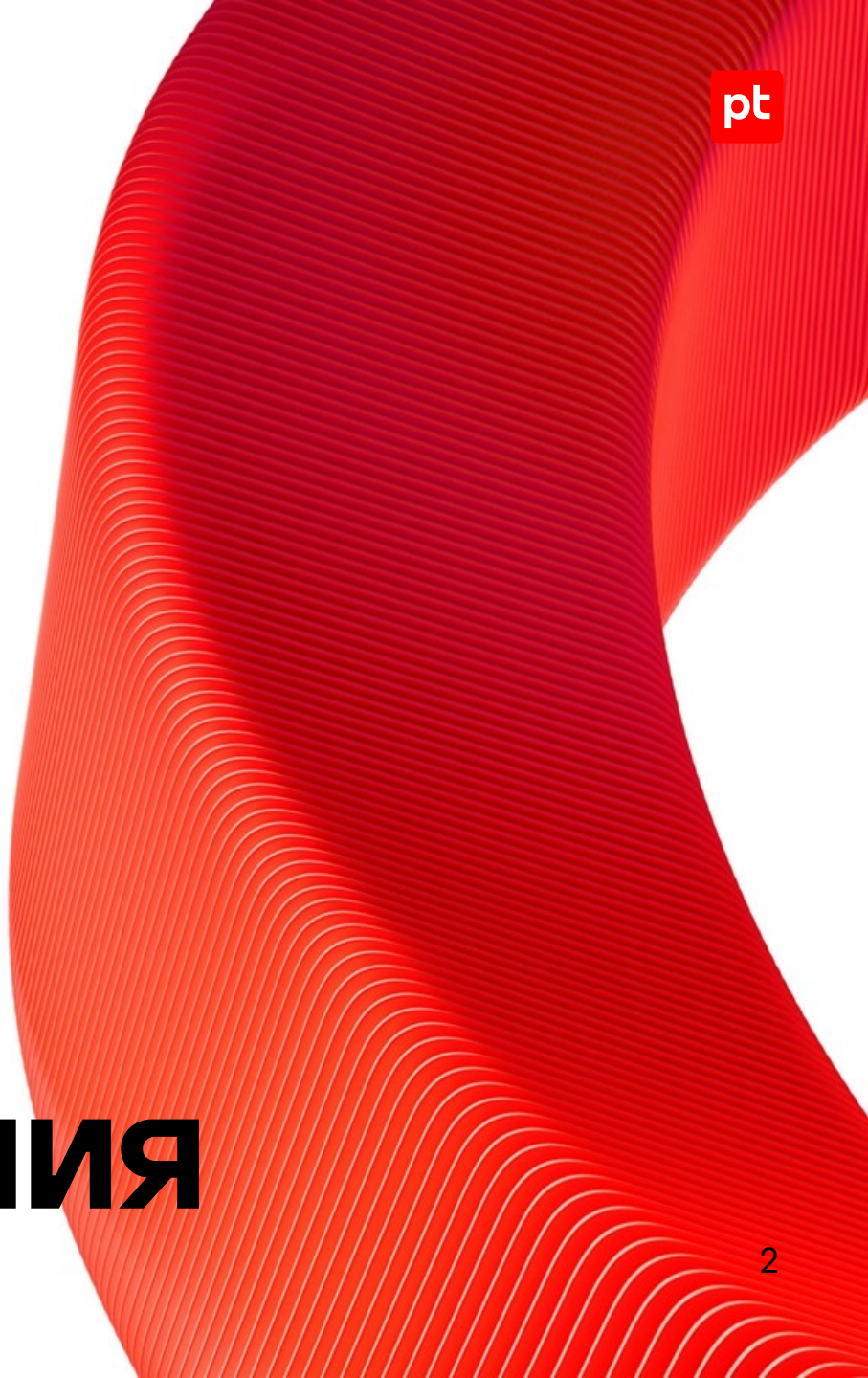
Алексей Лукацкий
Бизнес-консультант по безопасности
Positive Technologies

Биздата

О защите бизнес-данных не традиционными мерами, которые реализованы у всех

В качестве введения



Посмотрим непредвзято на утечки

Утечки информации
Суд в Ростове-на-Дону вынес приговор Андрею Лукьянову, который занимался незаконной продажей детализаций телефонных соединений клиентов регионального оператора связи.

В компанию связи мужчина устроился в 2015 году и тогда же один из коллег предложил ему подработку. Лукьянову нужно было выяснить, на кого зарегистрирован номер, скопировать список звонков абонента и передать его заказчику.

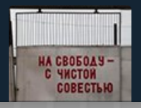
Против него было возбуждено уголовное дело (“*Неправомерный доступ к компьютерной информации с использованием служебного положения*”) по 12 задокументированным фактам преступлений. В 2017 году он был уволен из компании по компрометирующим обстоятельствам.

Лукьянов полностью признал свою вину и дал показания на своих сообщников. Учитывая его раскаяние и помощь следствию, суд приговорил бывшего сотрудника компании к одному году лишения свободы условно.

Про случаи задержания и осуждения лиц, так или иначе связанных с торговлей персональными данными читайте в отчете: 👇

https://www.devicelock.com/ru/blog/pojmat-i-nakazat-kak-v-rossii-lovyat-i-nakazyvayut-za-nezakonnuyu-torgovlyu-personalnymi-dannymi-chast-2.html

> **Devicelock**
> **Поймать и наказать! Как в России ловят и наказывают за незаконную торговлю пер...**
> Почти год назад я делал подборку сообщений



Легальный доступ

Утечки информации
Вечером 1-го февраля 2020 г. система DeviceLock Data Breach Intelligence обнаружила сервер с открытой MongoDB не требующей аутентификации для подключения.

В свободно доступной базе данных было две «коллекции»:

1️⃣ *alpha_config_db* – 35,787 записей (42 Мб)
2️⃣ *stavcredit* – 8,279 записей (9 Мб)

Каждая запись содержит:

- дата заявки
- интересующая сумма кредита
- интересующий срок кредитования
- канал привлечения
- ФИО
- эл. почта
- телефон
- дата рождения
- город
- регион

В процессе анализа утечки удалось выяснить, что в обнаруженной MongoDB находятся данные клиентов кредитного брокера «*Альфа-кредит*» (*alpha-credit.com*), который собирает заявки на кредиты и помогает получить заем в банке.

Через 10 минут после обнаружения открытой MongoDB мы оповестили компанию об уязвимости, но доступ к данным был закрыт только вечером 04.02.2020. 🙈👷🙅 По данным поисковика Shodan этот сервер попал в открытый доступ 31.01.2020. 😱

Корявый конфиг

📌Вот и закончились НОВОГОДНИЕ ПРАЗДНИКИ!
Мы, как и всегда работаем в прежнем режиме!

🏆 Скидка на все услуги 10% 🏆

💯 **Список услуг через ФНС**

ДРЕВО СВЯЗЕЙ:
- до 3-го колена
- до 6-го колена

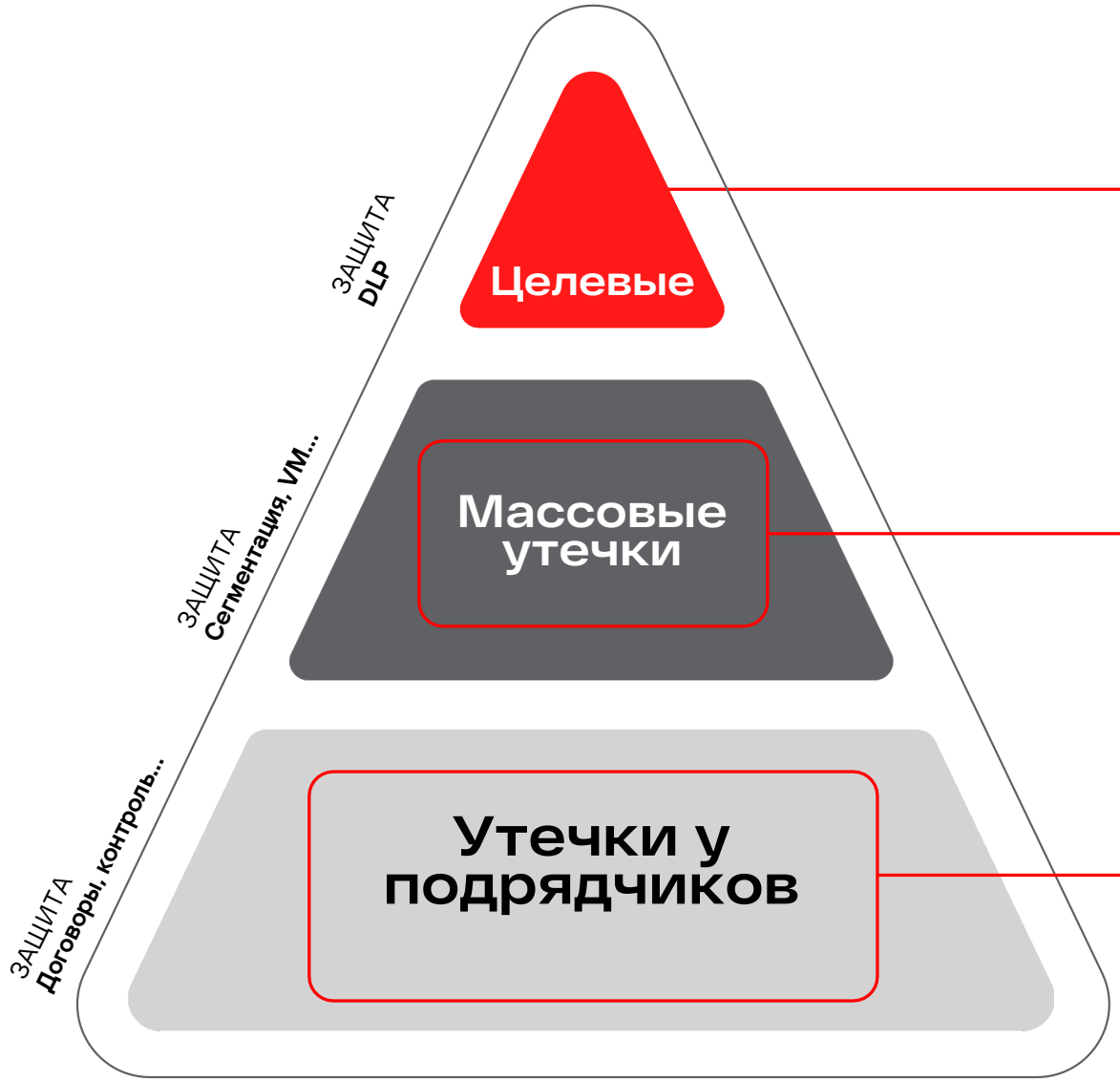
💯 *КНИГА ПОКУПОК/ПРОДАЖ:
-За все периоды сдачи отчетности

💯 *ВЫПИСКИ*:*
- Месяц
- 6 месяцев
- 12 месяцев
- больше 12 месяцев

💯 **БАНКИ:**
Альфа банк (физ/юр)
Тинькофф (физ/юр)
ВТБ (физ)
ПСБ (юр/физ)
Сбербанк (физ)
Убрир (юр)
Зенит (юр/мск)
Уралсиб (юр)
Авангард (юр)
Росбанк (юр/физ)

Пробив на заказ

С чем мы обычно боремся?



Считаются самыми опасными и именно на них фокусируются все

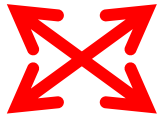
Обычно происходят по вине ИТ-службы и нечасто контролируются ИБ

Происходят «внезапно» и о них мы узнаем обычно из СМИ или Телеграм-каналов

Какие бывают утечки?

СЛУЧАЙНАЯ
Неверная конфигурация БД на периметре

НЕСЛУЧАЙНАЯ
Шифровальщик выгружает украденные данные

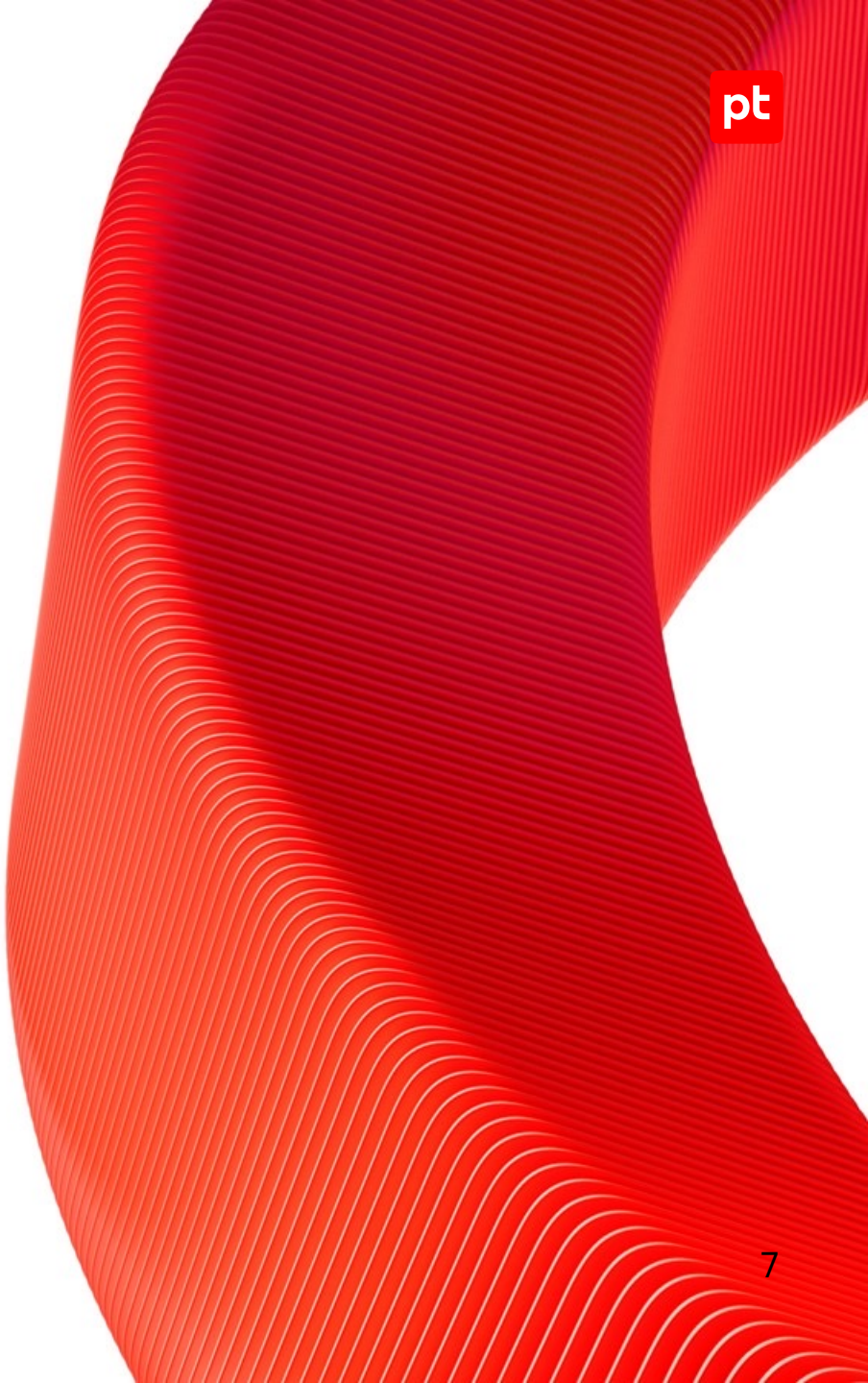


ЕДИНИЧНАЯ
Пробив конкретного клиента / абонента

МАССОВАЯ
Выгрузка всей базы данных с сайта

Если вы допустили утечку, то у вас что-то не так

Реальные кейсы



Кейс Equifax

- Утечка через известную уязвимость, эксплуатацию доверенных отношений
- Запуск эксплойта
- Скрытие активности в зашифрованном трафике
- Перехват паролей администратора в трафике

Кейс British Airways (3 версии)

- Взломан сайт компании и подменен JavaScript
- Взломан CDN и подменен JavaScript
- Взломан подрядчик и у него подменен подгружаемый JavaScript

Кейс Sea Turtle

- Утечка данных после заражения фишинговым письмом с аттачем (описание вакансии) с сайта-клона
- Канал утечки – DNS

gLtAGJDVIAJAKZXWY000[.]0ffice36o[.]com

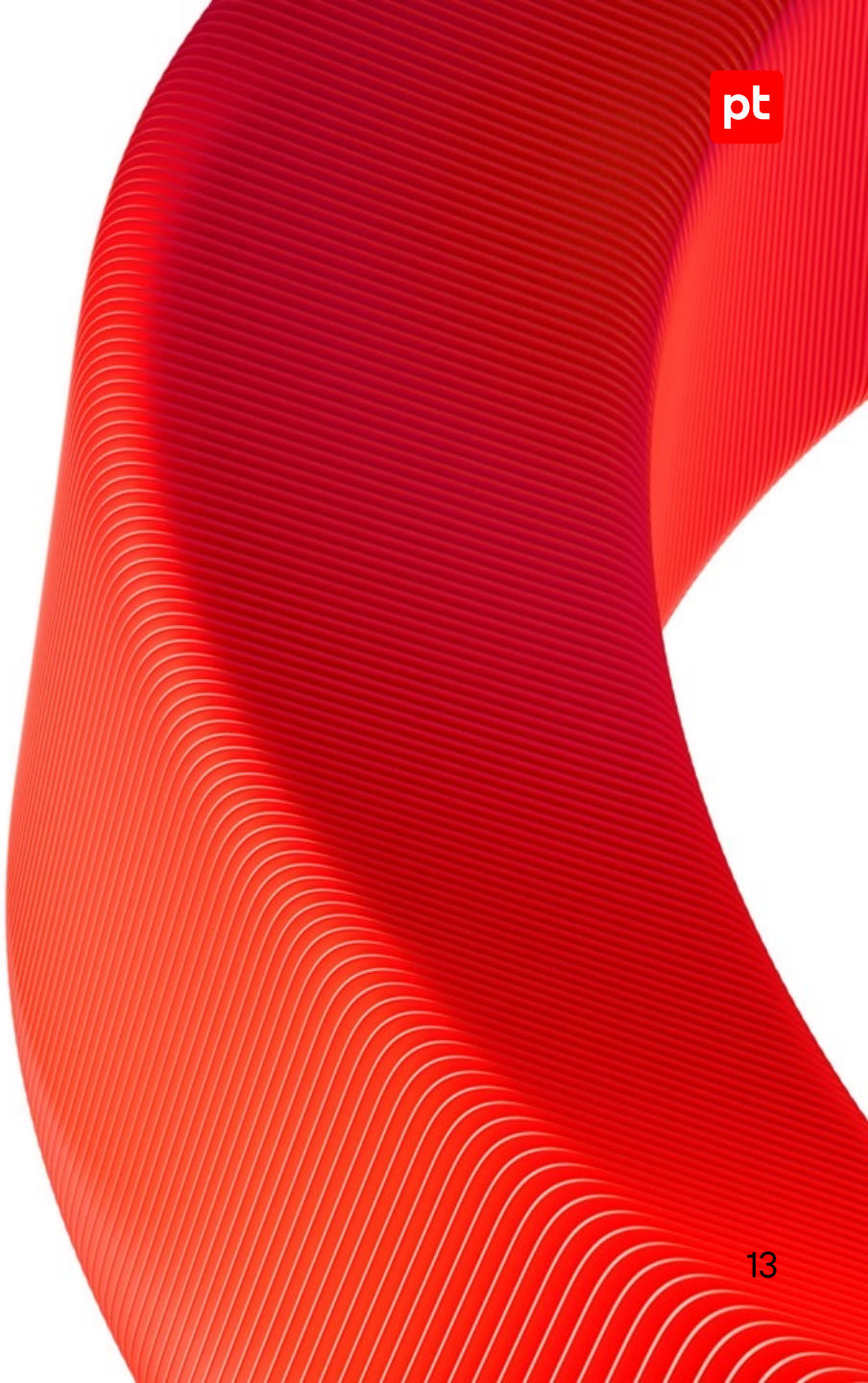
Кейс NASA

- Утечка данных через беспроводное соединение после установки во внутренней сети NASA миниатюрного компьютера на базе Raspberry Pi

Кейс Johnson Controls

- Утечка данных в результате проникновения шифровальщика внутрь корпоративной инфраструктуры
- Удаление всех резервных копий

Индикаторы утечек из кейсов



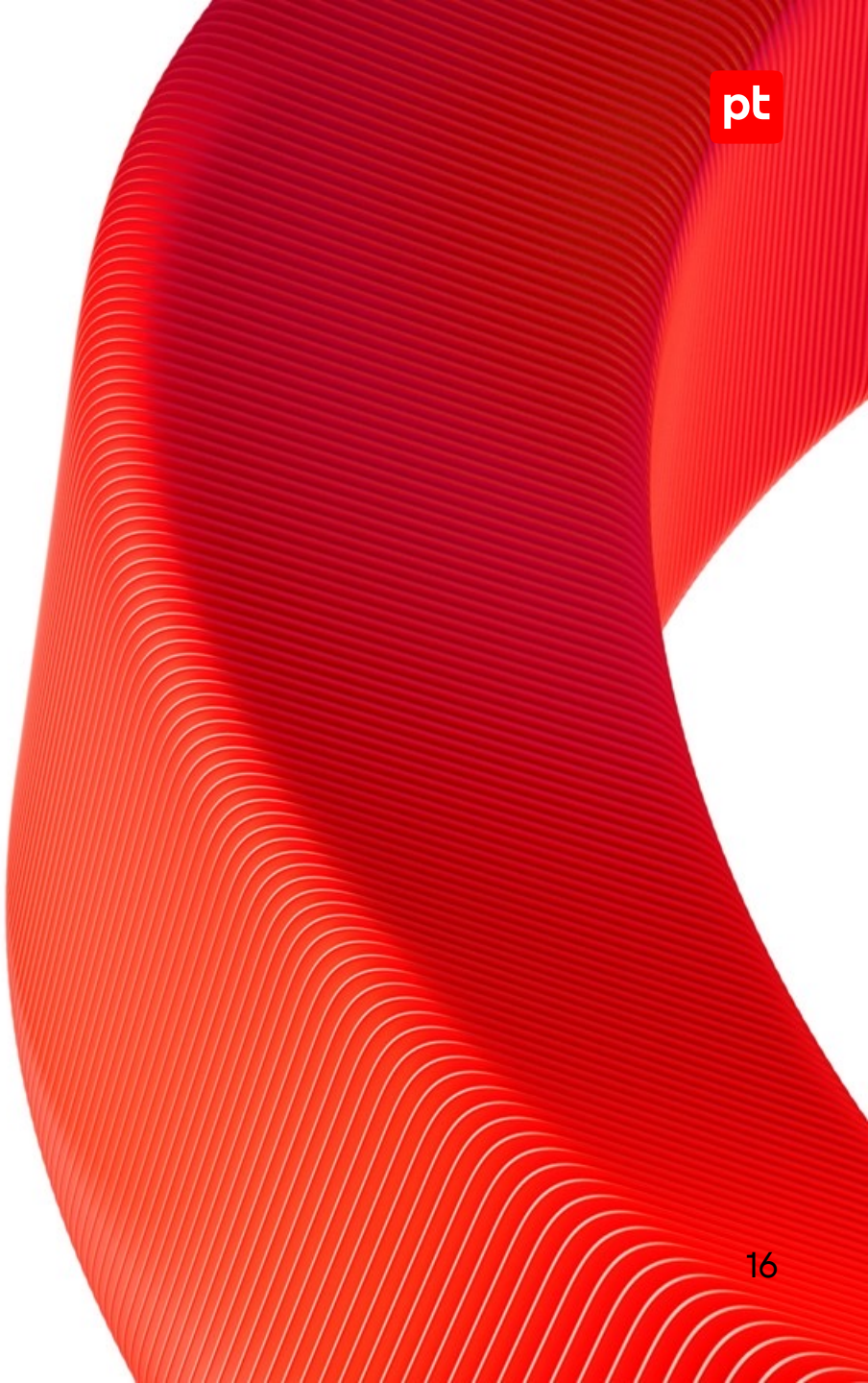
На что обращать внимание?

- Превышение объема исходящего трафика (NGFW)
- Соединения с редко используемыми доменами (NGFW, SWG)
- Необычный доступ с Web-сервера к оконечным устройствам в сети (NTA / NDR)
- Необычные взаимодействия родительского и дочернего процессов на узле (EDR, SIEM)

На что обращать внимание?

- Редкий процесс на узле (EDR)
- Удаление файлов резервных копий
- Сканирование внутренней сети с пользовательских узлов (NTA / NDR)
- Нетипичные домены, а также структура DNS-запросов/ответов, имена/энтропия/длина доменов (NGFW, NTA / NDR, DNS Firewall)
- Сайты-клоны / фишинговые домены (NGFW, NTA / NDR, DNS Firewall, SWG)

Рекомендации по защите от утечек из кейсов



Что могло бы помочь?

- Контроль объема исходящего трафика (NGFW, SASE)
- Блокирование соединений с редко используемыми доменами (NGFW, SWG, DNS Firewall, SASE)
- Закрытие открытых портов и установка патчей (ИТ)

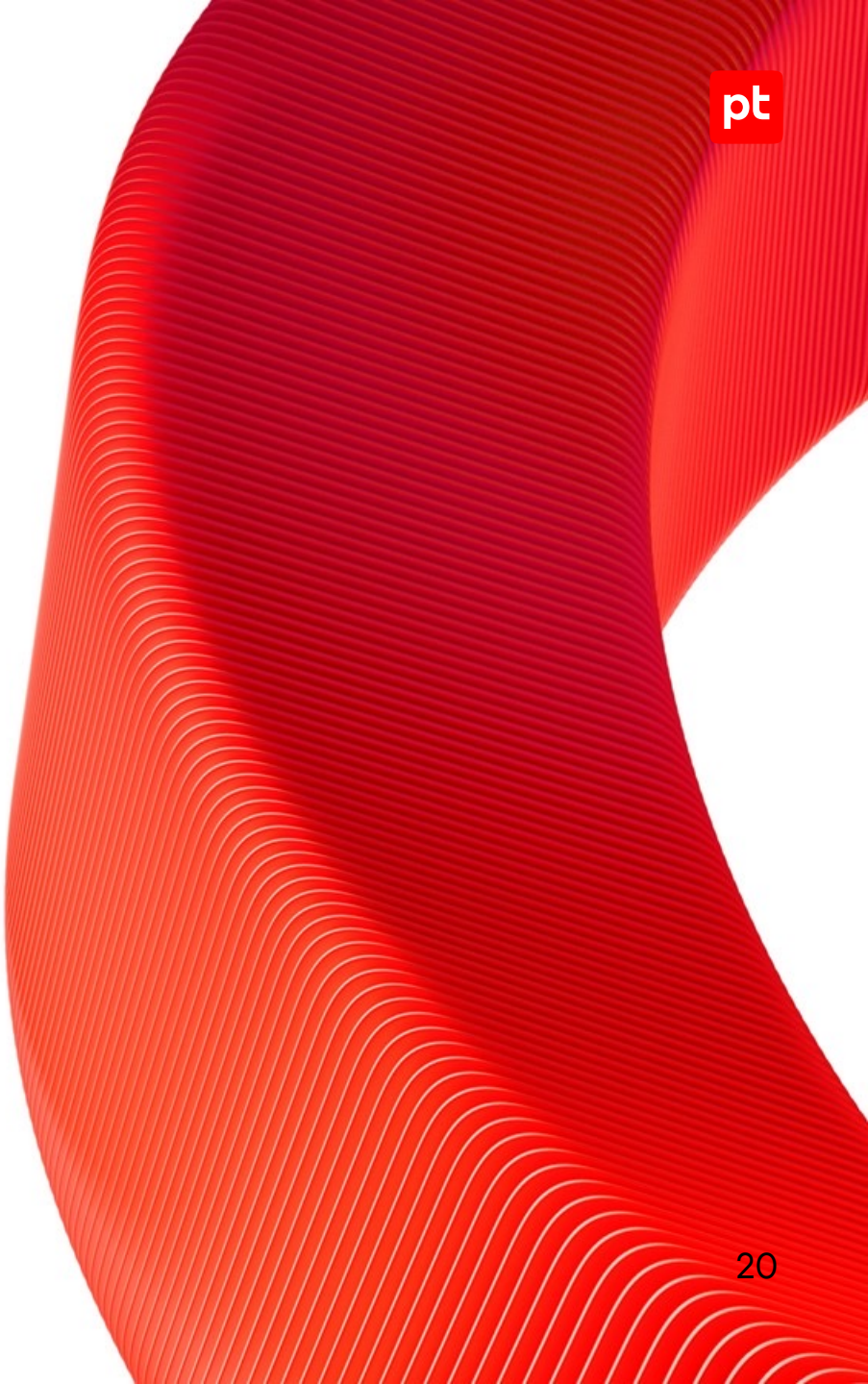
Что могло бы помочь?

- Выявление аномалий в сетевом трафике (NTA/NDR)
- Контроль изменений на серверах (EDR)
- Сегментация (NGFW, Zero Trust, 802.1x)
- Блокирование аномального DNS-трафика (NGFW, DNS Firewall, SASE)

Что могло бы помочь?

- Мониторинг беспроводного (Wi-Fi / 3G / 4G) эфира для обнаружения и блокирования посторонних устройств
- Контроль подрядчиков - инструментальный или через включение пункта в договорные обязательства (VM)

На закуску



Кейс War Thunder

- На форуме игры War Thunder выложены секретные чертежи европейского истребителя Eurofighter Typhoon
- В начале 2023 года там были выложены секретные чертежи американского истребителя F/A-18 Hornet
- Кстати, Джек Тейшера (аналитик BBC США) выкладывал секретные материалы о конфликте России и Украины в игровом чате на серверах Discord

Кейс Goldman Sachs

- Инвестиционные аналитик Goldman Sachs «сливал» инсайдерскую информацию через аудиочат игровой консоли Xbox

Но давайте начнем с того, что имеем

Спасибо!

alukatsky@ptsecurity.com