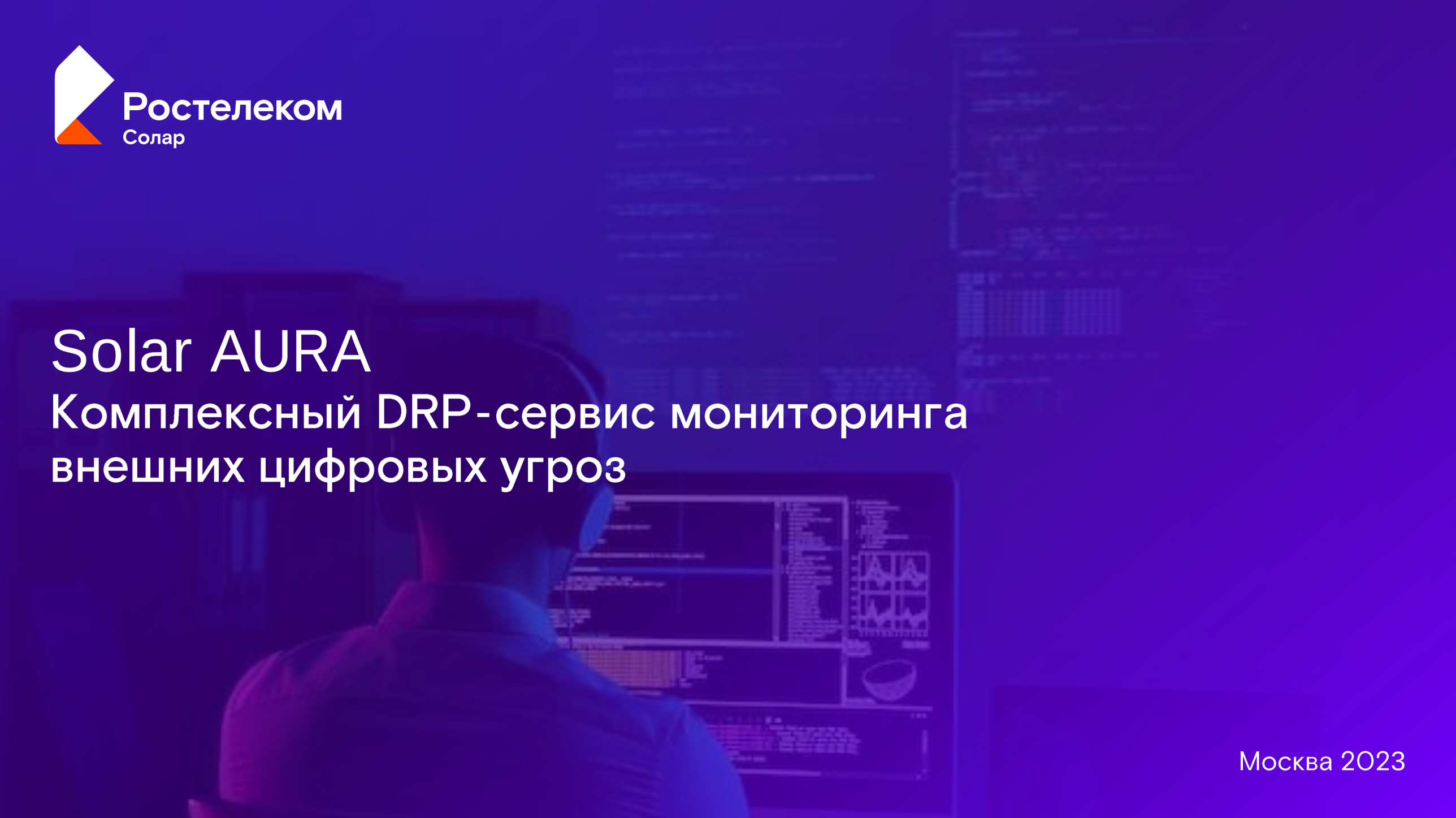
Ростелеком
Солар

Solar AURA

Комплексный DRP-сервис мониторинга внешних цифровых угроз



Москва 2023

Современный киберландшафт диктует необходимость мониторинга внешних цифровых угроз

x5

число атак, связанных
с хактивизмом,
в 2022-2023 годах

+26%

рост числа фишинговых атак
и социального мошенничества в апреле 2023 г.
по сравнению с аналогичным периодом 2022-го

7 из 9

zero-day-уязвимостей, выявленных Google Threat Analysis Group, исходят от акторов Access-as-a-Service

123

российские организации, данные которых попали в Сеть с января по апрель 2023 года

600

фишинговых ресурсов регистрируется
в год для атак на сотрудников, клиентов
и партнеров одной компании

18

атак на незащищенные ресурсы фиксируется в день

1,1 ТБ

общий объем
опубликованных данных

Данные:
- «Ростелеком-Солар»
- ENISA Threat Landscape
- Comparitech

Ростелеком Солар

Узнайте, насколько вы подвержены цифровым рискам

Отсканируйте QR-код и проверьте, сколько информации о вашей компании опубликовано в Сети*

* Сервис агрегирует обнаруженные данные в обобщенном виде

Ростелеком Солар

Решение - Solar AURA

Комплексный DRP*-сервис мониторинга внешних цифровых угроз

Для чего

Снижение цифровых рисков и предупреждение атак

Защита бренда компании и личного бренда ключевых сотрудников

Выявление факторов репутационных и финансовых рисков

Повышение уровня защищенности инфраструктуры

* DRP – Digital Risk Protection

Ростелеком Солар

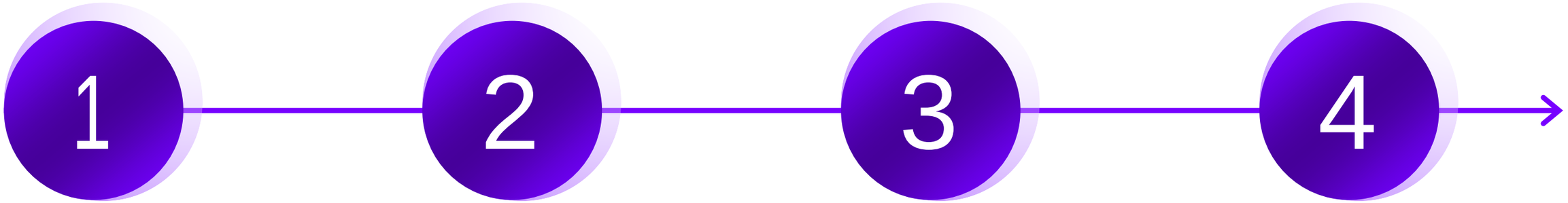
8 модулей в одном сервисе для максимальной защиты

Модули можно подключить отдельно или в комплексе

- Антифишинг
- Утечки
- Даркнет
- Бренд компании
- Личный бренд
- Медиаполе
- Безопасность финансов
- Мониторинг периметра

Ростелеком Солар

Как это работает



Получение данных через мониторинг

Оценка и верификация аналитиком

Уведомление об угрозах

Реагирование

Ростелеком Солар

Преимущества сервиса «Solar AURA»

01

Широкий функционал

8 векторов мониторинга в одном сервисе

02

Многовекторный мониторинг

публичных и закрытых сегментов интернета

03

Оперативная блокировка фишинга

минимальное время - 12 минут,

87% ресурсов - менее 24 часов

04

Аналитическое сопровождение

выявленных инцидентов

05

Сервис под ключ

подключение до 3 дней, доступность в работе - сервис не требует высокой квалификации специалистов заказчика

06

Продвинутая система статистики

наглядное представление динамики угроз для принятия оперативных решений

07

Удобный интерфейс

система оповещений, наглядные дашборды, эффективное управление обнаруженными угрозами

08

Интеграционные возможности

добавление событий через API, обработка большого количества запросов и двусторонняя интеграция с другими ИБ-системами

Ростелеком Солар

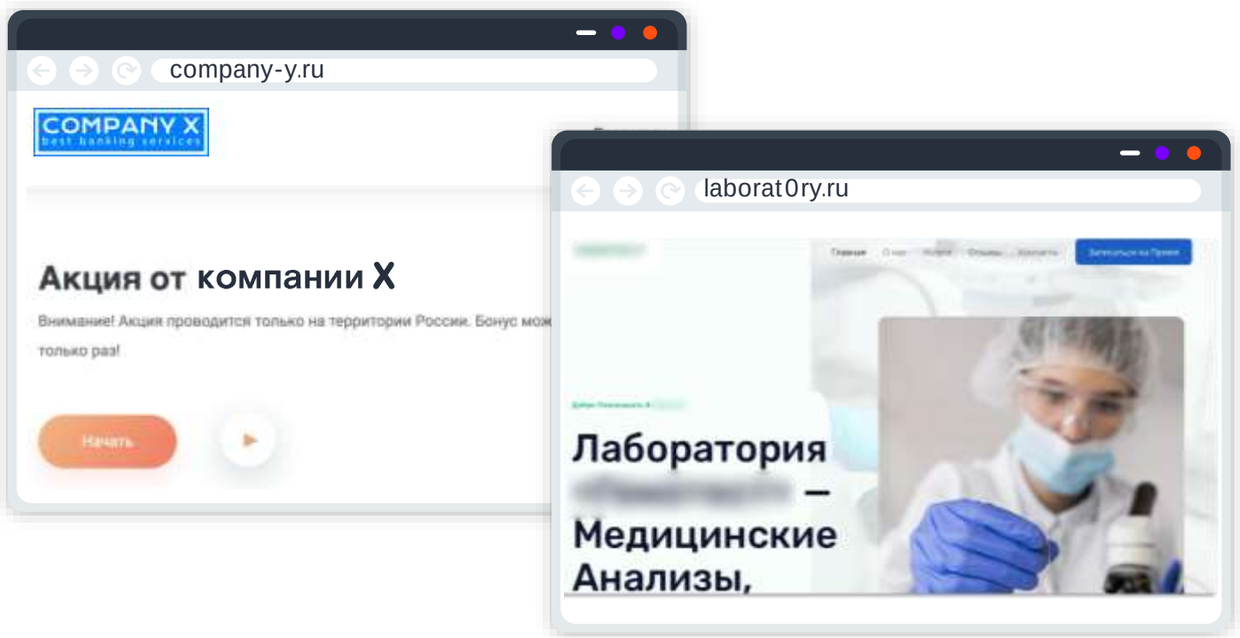
Антифишинг

Ростелеком
Солар

Антифишинг

Что мы ищем?

- Фишинговые сайты
- Мошеннические ресурсы
- Потенциально опасные домены



Где ищем?

- 200+ тыс. доменных имен
  из 1000+ доменных зон в сутки
- Реестры SSL-сертификатов
  1+ млн ресурсов в сутки
- Поисковые системы
- Данные DNS
- DarkNet

Ростелеком Солар

Противодействие фишингу

12
минут

минимальное время блокировки
с момента обнаружения
фишингового сайта

57%
ресурсов

блокируется менее
чем за 4 часа*

87%
ресурсов

блокируется менее
чем за 24 часа*

Инициируем блокировку через ресурсы

* Вне зависимости от юрисдикции ресурса

Ростелеком Солар

Утечки

Ростелеком
Солар

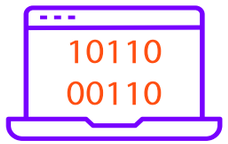
Ключевые направления и объекты поиска

Документы

Конфиденциальные сведения, ставшие общедоступными злонамеренно или по ошибке

Аккаунты

Корпоративные email и пароли, попавшие в базы данных публичных утечек



Программный код

Размещенные на сайтах для разработчиков фрагменты кода, публикация которых представляет угрозу для безопасности компании

Ростелеком Солар

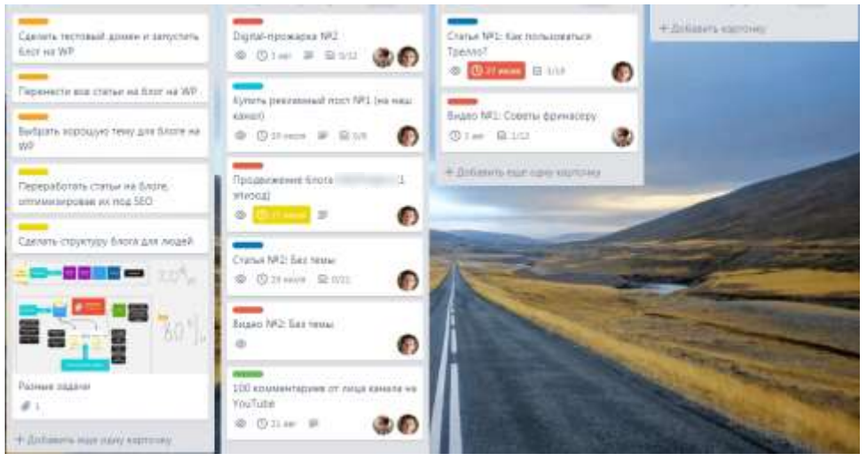
Утечки. Документы

Index of /TOSHIBA_EXT/Архив/

[parent directory]

Name	Size	Date modified
6. Гибель Богов-2. Книга 6. Прошедшая вечность.fb2	2.0 MB	2/14/20, 3:00:00 AM
Glen Cook/		4/6/20, 3:00:00 AM
Google Диск/		7/18/20, 3:00:00 AM
KMSAuto Net 2015 v1.3.6 Portable/		1/19/21, 3:00:00 AM
Photo.scr	1.5 MB	3/10/21, 3:00:00 AM
Васильев Владимир/		12/5/21, 3:00:00 AM
Гамильтон Питер - Сборник произведений/		2/9/22, 3:00:00 AM
Перумов Ник - Сборник произведений/		4/13/22, 3:00:00 AM
Прайс/		6/21/22, 3:00:00 AM
[redacted]		1/15/23, 3:00:00 AM
СКЛАД/		3/23/23, 3:00:00 AM

Размещенный в общем доступе массив внутренних документов компании



Публичная доска в менеджере задач Trello, которая содержит конфиденциальные сведения, документы и информацию об организации бизнес-процессов

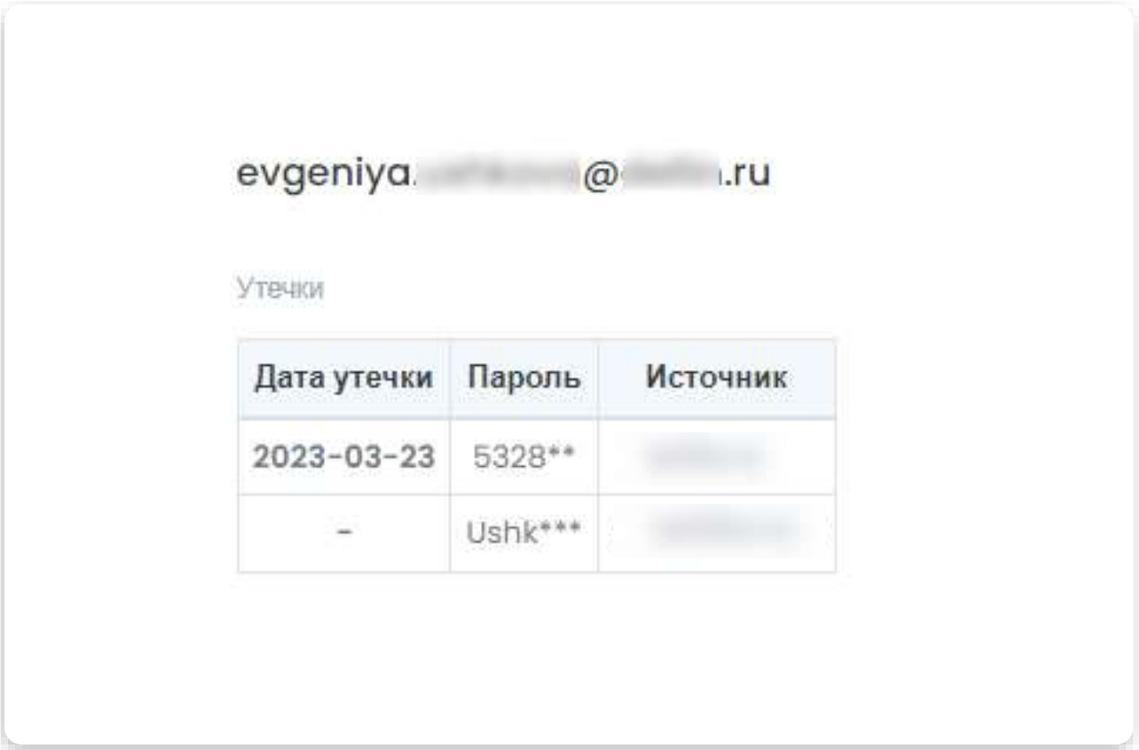
Источники данных:

- Telegram
- Социальные сети
- Файлообменники
- FTP и веб-серверы
- DarkNet & Deep web

Особенности функционала:

- Установление первоисточника утечки
- Сбор дополнительных сведений, помогающих в расследовании инцидента
- Взаимодействие с площадками в целях удаления контента из доступа

Утечки. Аккаунты



На этот раз пострадал **сервис** [redacted] и все **его зеркала.**

Утечка содержит **4.500.000 записей**, часть с **паролем без хэширования**, которые без пароля - **данные с их приложения.** Также имеются данные о **статусе, id, uuid, comment и затраты.**

База получена следующим образом: были найдены **исходники сайта**, в которых была **почта одного из администраторов**, пароль на данный email был **найден в других базах** и соответственно подходил.

Пример атаки с использованием данных публичных утечек

Источники данных:

- Агрегаторы публичных утечек
- Общедоступные массивы данных, содержащие логины и пароли

Особенности функционала:

- Возможность постановки на контроль конкретных адресов, в том числе личных
- Информация об источнике публикации
- Регулярное обновление данных

Ростелеком Солар

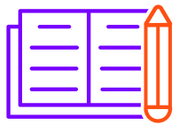
Даркнет

Ростелеком
Солар

Ключевые направления и объекты поиска

Базы данных

Массивы конфиденциальной информации, выставленные на продажу или размещенные в открытом доступе

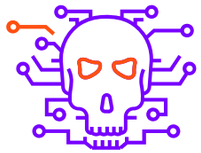


Противоправные услуги

Все, что может угрожать заказчику в зависимости от специфики его деятельности

Недобросовестные сотрудники

Данные, которые подтверждают распространение конфиденциальной информации сотрудниками и их связь с киберкриминальными структурами

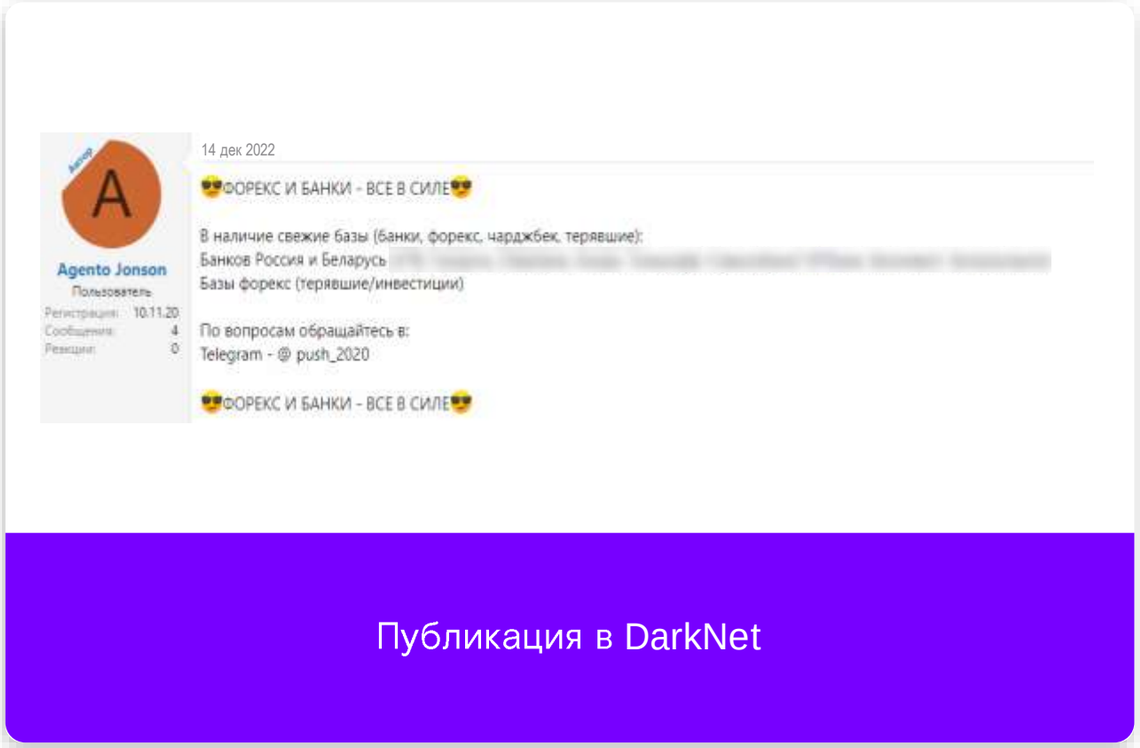


Вероятные атаки

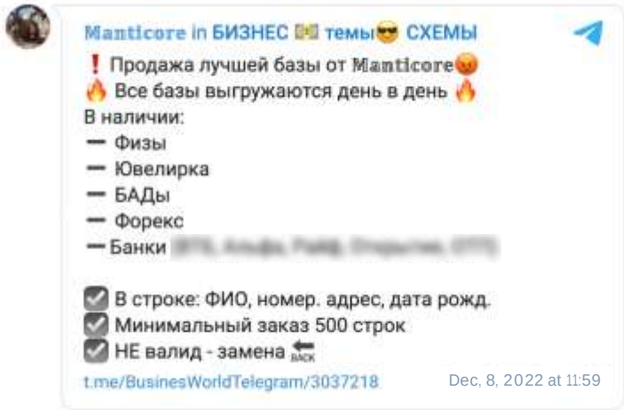
Обнаружение призывов к осуществлению атак на компанию или случаев координации подобных атак

Ростелеком Солар

Даркнет. Базы данных



Публикация в DarkNet



Публикация в Telegram

Источники данных:

- DarkNet & Deep web
- Telegram
- Социальные сети
- Торговые площадки

Особенности функционала:

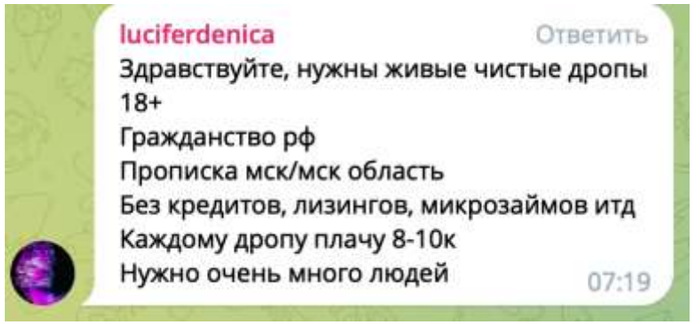
- Получение образцов данных
- Аналитическая оценка распространяемых сведений
- Сбор сведений о причастных лицах
- Подготовка отчета по итогам анализа

Даркнет. Услуги

Пример объявления

Публикация в DarkNet

Пример выявления готовящейся атаки на кредитную организацию*



* Массовый наем «чистых» дропов свидетельствует о планируемом выводе крупных сумм денег на территории Московского региона.
Обнаружение такого рода событий позволяет заранее подготовиться к возможным атакам и начать использовать антифрод для выявления такого рода аномалий.

Публикация в Telegram

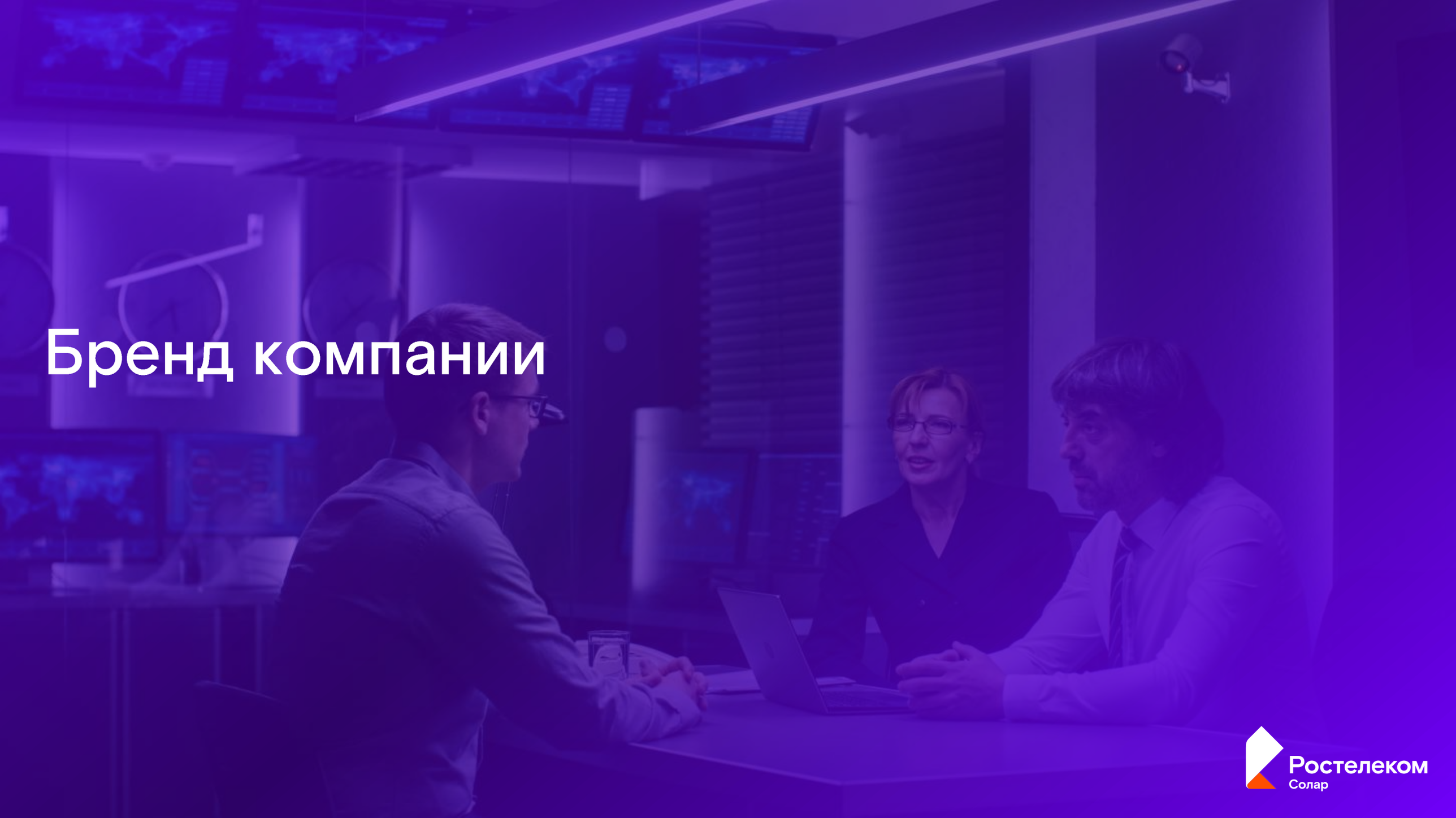
Источники данных:

- DarkNet & Deep web
- Telegram
- Социальные сети
- Торговые площадки

Особенности функционала:

- Установление дополнительных обстоятельств и раскрытие подробностей инцидента
- Сбор сведений о причастных лицах

Бренд компании



Ростелеком
Солар

Ключевые направления и объекты поиска

Защита бренда в соцсетях

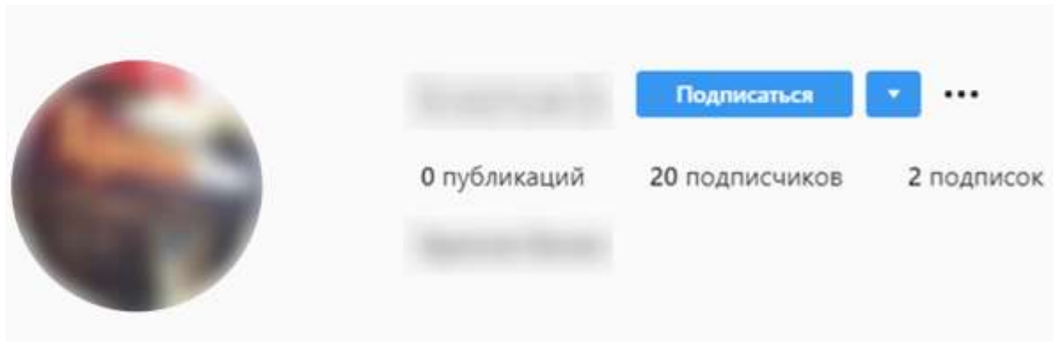
Обнаружение страниц и аккаунтов в соцсетях и мессенджерах, ассоциирующих себя с компанией заказчика, и взаимодействие с администрацией соцсетей в целях устранения нарушений

Фейковые приложения

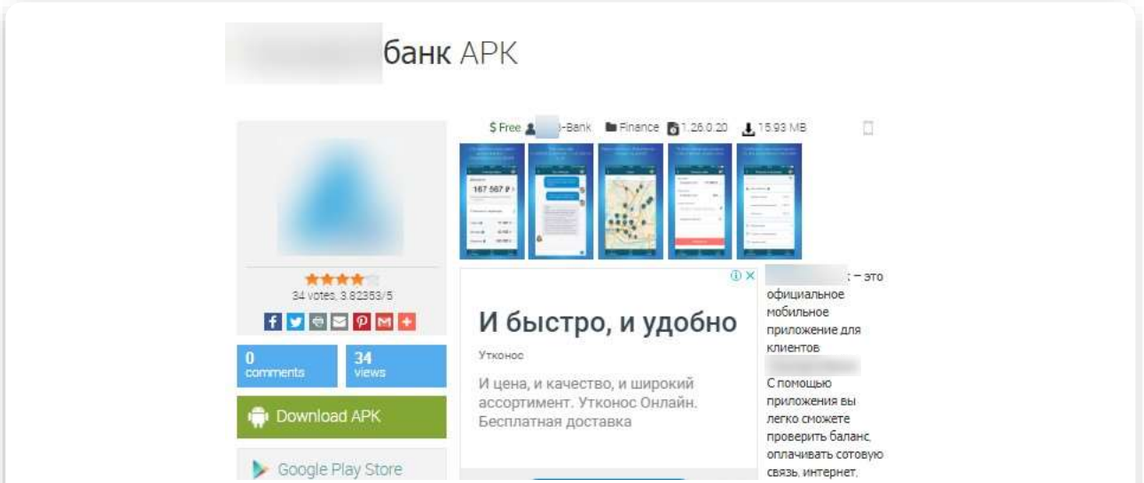
Обнаружение вредоносных клонов официальных приложений и официальных программ, размещенных на неавторизованных площадках. Взаимодействие с администрацией площадок в целях устранения нарушений

Ростелеком Солар

Защита бренда компании



Использование наименования и логотипа



Размещенное на неофициальном ресурсе мобильное приложение организации

Источники данных:

- VK
- Одноклассники
- Facebook*
- Instagram*
- Площадки распространения приложений
- Telegram
- YouTube
- Skype
- TikTok

Особенности функционала:

- Сбор дополнительных сведений об инциденте и причастных лицах
- Взаимодействие с площадками в целях устранения нарушений

* Принадлежит Meta, признанной на территории России запрещенной и экстремистской организацией

Личный бренд

Ростелеком
Солар

Ключевые направления и объекты поиска

Фейковые аккаунты

Поиск и содействие в удалении поддельных страниц и аккаунтов, выдающих себя за аккаунты защищаемых персон в социальных сетях и мессенджерах

Адреса электронной почты

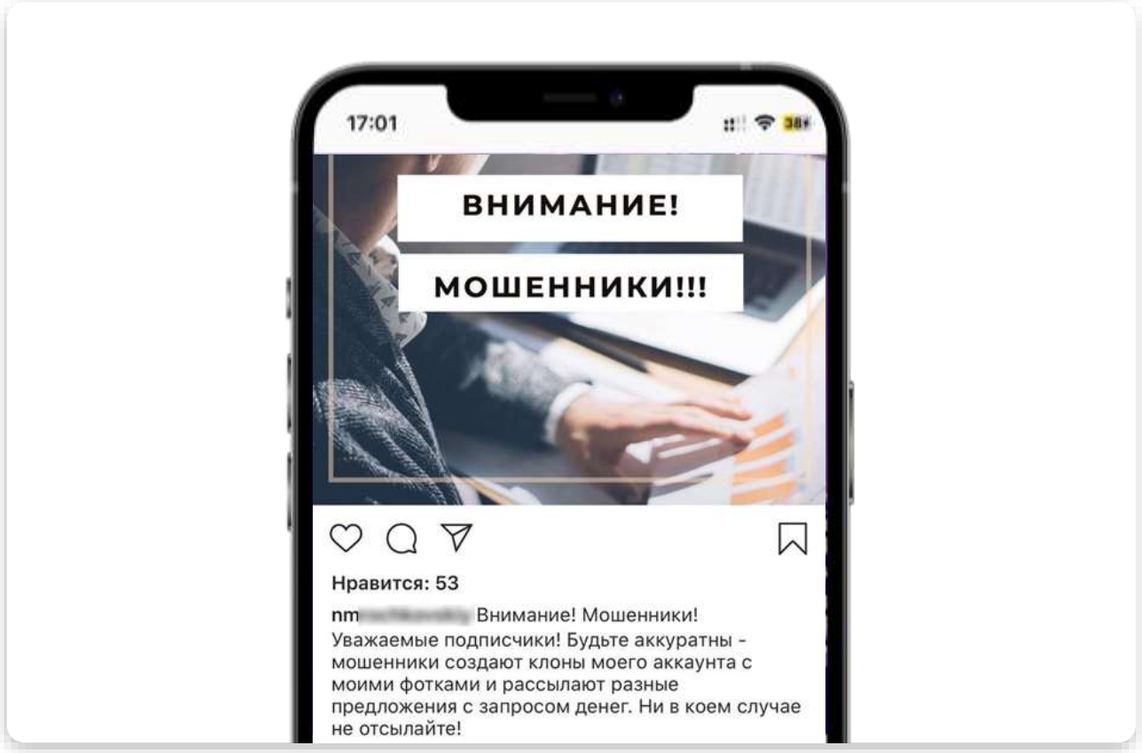
Постановка корпоративных и личных учетных данных на мониторинг
с целью выявления фактов их компрометации и публикации в базах утечек

Упоминания в публичном пространстве

Анализ упоминаний в СМИ и на публичных ресурсах

Ростелеком
Солар

Защита личного бренда VIP-персон



Источники данных:

- VK
- Одноклассники
- Facebook*
- Instagram*
- Агрегаторы публичных утечек
- Telegram
- YouTube
- Skype
- TikTok

Особенности функционала:

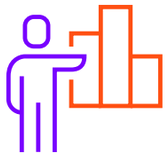
- Сбор дополнительных сведений об инциденте и причастных лицах
- Взаимодействие с площадками в целях устранения нарушений

* Принадлежит Meta, признанной на территории России запрещенной и экстремистской организацией

Медиаполе

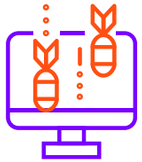
Ростелеком
Солар

Ключевые направления и объекты поиска



Упоминания бренда в публичном пространстве

Мониторинг упоминаний компании
и ее ключевых продуктов, определение тональности публикации, анализ авторства



Обнаружение признаков информационных атак

Обнаружение массовых вбросов негативной информации и других целенаправленных медийных атак

Мониторинг рисков ИБ

Поиск публикаций, угрожающих безопасности компании (информация об используемых СЗИ, детали ИТ-инфраструктуры, данные о персонале)

Анализ распространения информации

Предоставление сведений о первоисточнике информации, базовая оценка широты охвата инфоповода

Ростелеком Солар

Медиаполе

[redacted] запретил продажу приглашений в соцсеть Clubhouse

Сервис по размещению объявлений [redacted] запретил продажу приглашений для новой социальной сети Clubhouse. Причиной стало большое количество предложений от мошенников.

«Поскольку за последние несколько дней вместе с интересом пользователей резко выросло и число объявлений с предложением инвайтов (приглашений.— "Ъ") в Clubhouse, среди которых появились явно спекулятивные, при этом проверить подлинность товара не представляется возможным, мы приняли решение запретить продажу инвайтов, чтобы защитить наших пользователей от возможного мошенничества»,— говорится в сообщении (цитата по «РИА Новости»).

СМИ: Публикация на сайте kommersant.ru

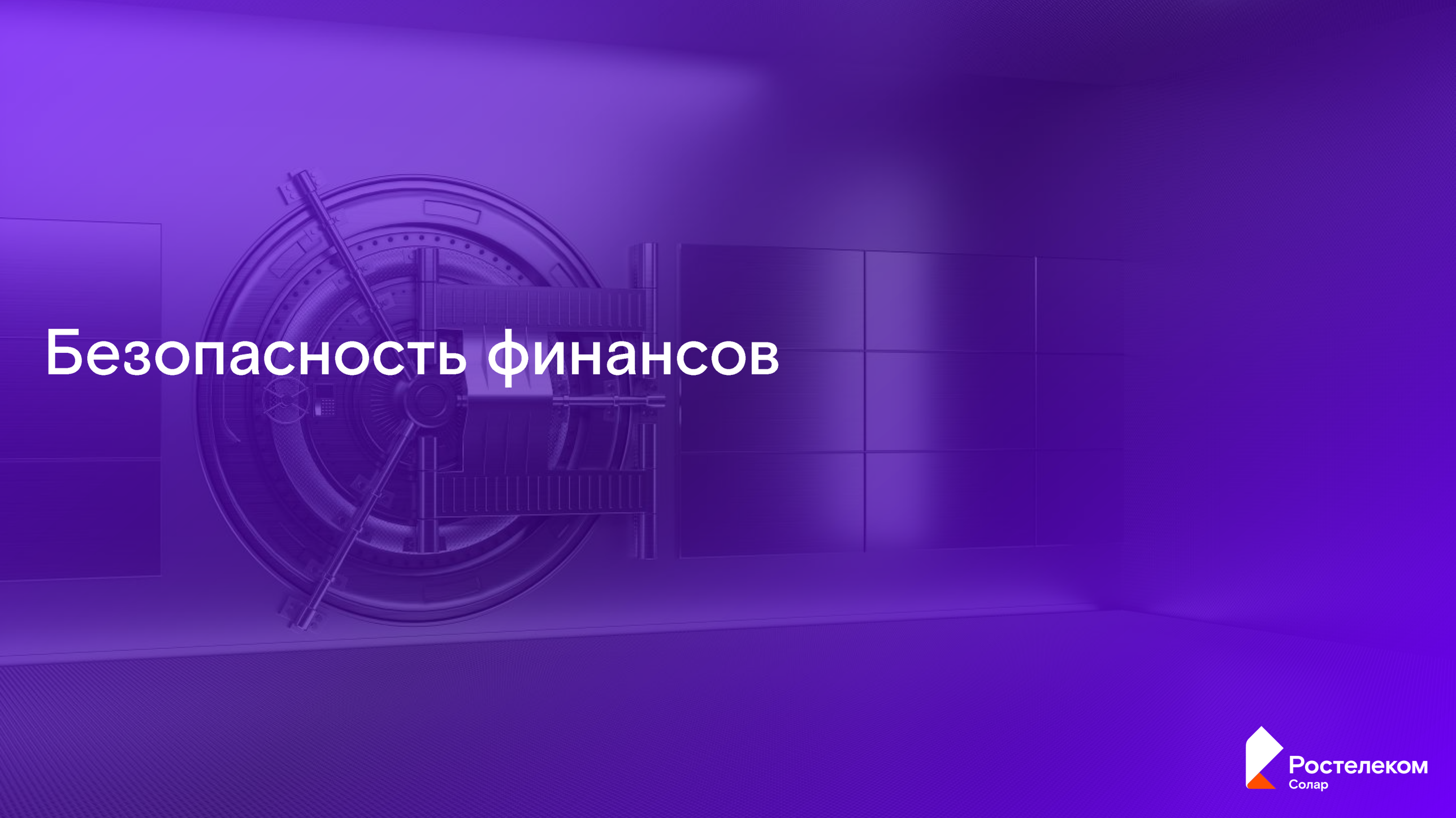
СМИ: Французский телеканал подвергся хакерской атаке в прямом эфире по причине того, что во время одного из интервью за спиной спикера была отчетливо видна доска с паролями от корпоративных ресурсов.

Источники данных:

- Сайты-отзовики
- СМИ
- Telegram-каналы
- Социальные сети

Особенности функционала:

- Выбор площадок для сбора данных
- Выбор окраски публикаций (негативная, позитивная, нейтральная)
- Определение категорий выявляемых событий и критериев их отбора



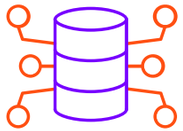
Безопасность финансов

Ростелеком
Солар

Ключевые направления и объекты поиска

Платежные средства и инструменты

Фиксация фактов использования интернет-эквайринга в целях оплаты услуг, запрещенных на территории Российской Федерации



Карты дропов

Сбор сведений о банковских картах, потенциально используемых для совершения незаконных действий

Юридические лица

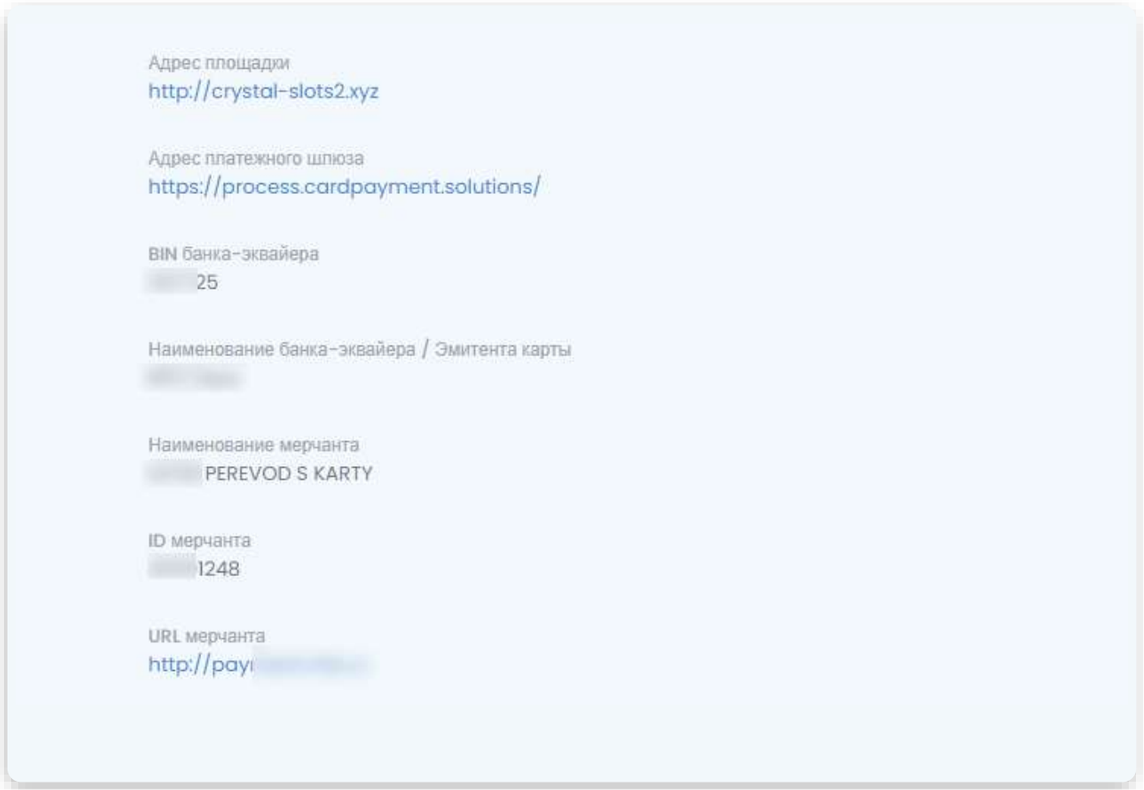
Предоставление данных о юридических лицах, выставленных на продажу на специализированных площадках и используемых в мошеннических схемах

Соответствие виду деятельности

Мониторинг сайтов, использующих интернет-эквайринг, на предмет соответствия контента заявленному виду деятельности

Ростелеком Солар

Безопасность финансов. Эквайринг



Использование модуля позволяет существенно снизить риски наступления штрафных санкций для финансового учреждения, предусмотренных новой статьей 15.48 КоАП РФ (не менее 5 млн ₽) за переводы денег в пользу онлайн-казино и других нелегальных игорных сервисов.

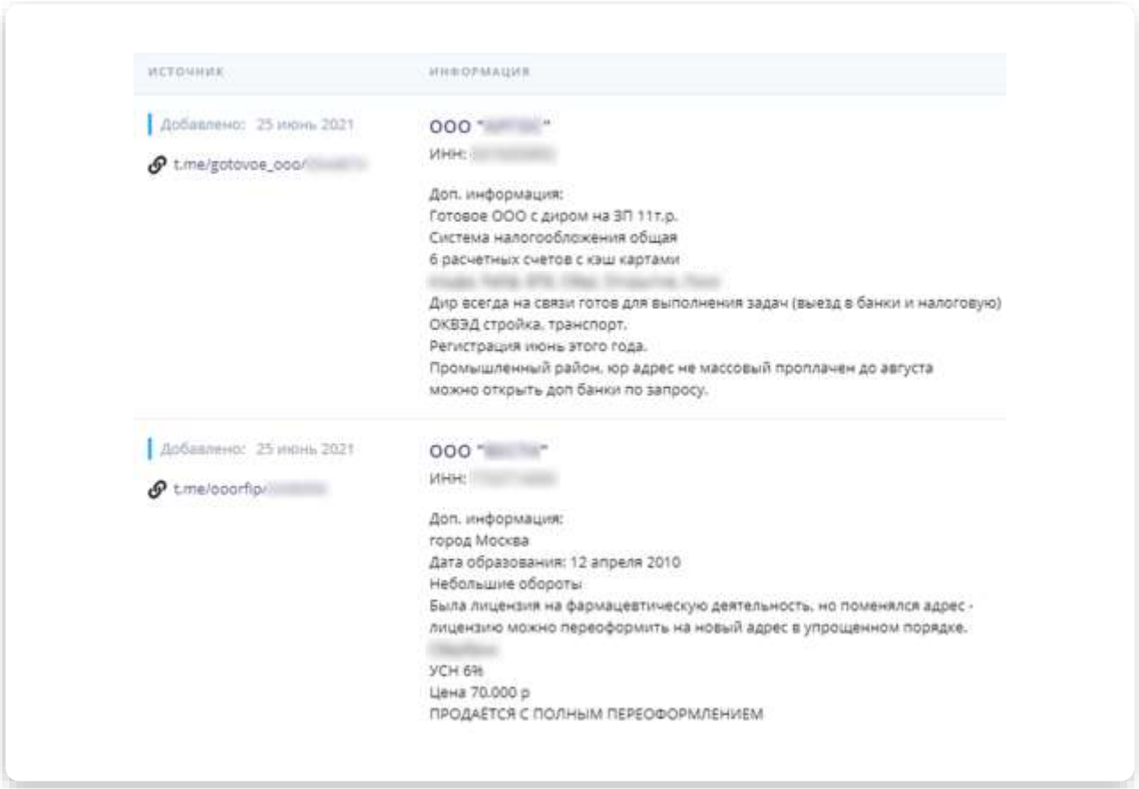
Источники данных:

- Онлайн-казино, фишинговые сайты, лжеброкеры и т. д.
- Криптовалютные обменники
- Telegram-каналы

Особенности функционала:

- Сбор дополнительных сведений об инциденте и причастных лицах
- Взаимодействие с площадками в целях устранения нарушений

Безопасность финансов. Юридические лица



ИСТОЧНИК	ИНФОРМАЦИЯ
Добавлено: 25 июнь 2021 t.me/gotovoe_ooo/	ООО " Инн: Доп. информация: Готовое ООО с диром на ЗП 11т.р. Система налогообложения общая 6 расчетных счетов с кэш картами Дир всегда на связи готов для выполнения задач (выезд в банки и налоговую) ОКВЭД стройка, транспорт. Регистрация июнь этого года. Промышленный район, юр адрес не массовый проплачен до августа можно открыть доп банки по запросу.
Добавлено: 25 июнь 2021 t.me/ooorfip/	ООО " Инн: Доп. информация: город Москва Дата образования: 12 апреля 2010 Небольшие обороты Была лицензия на фармацевтическую деятельность, но поменялся адрес - лицензию можно переоформить на новый адрес в упрощенном порядке. УСН 6% Цена 70.000 р ПРОДАЁТСЯ С ПОЛНЫМ ПЕРЕОФОРМЛЕНИЕМ

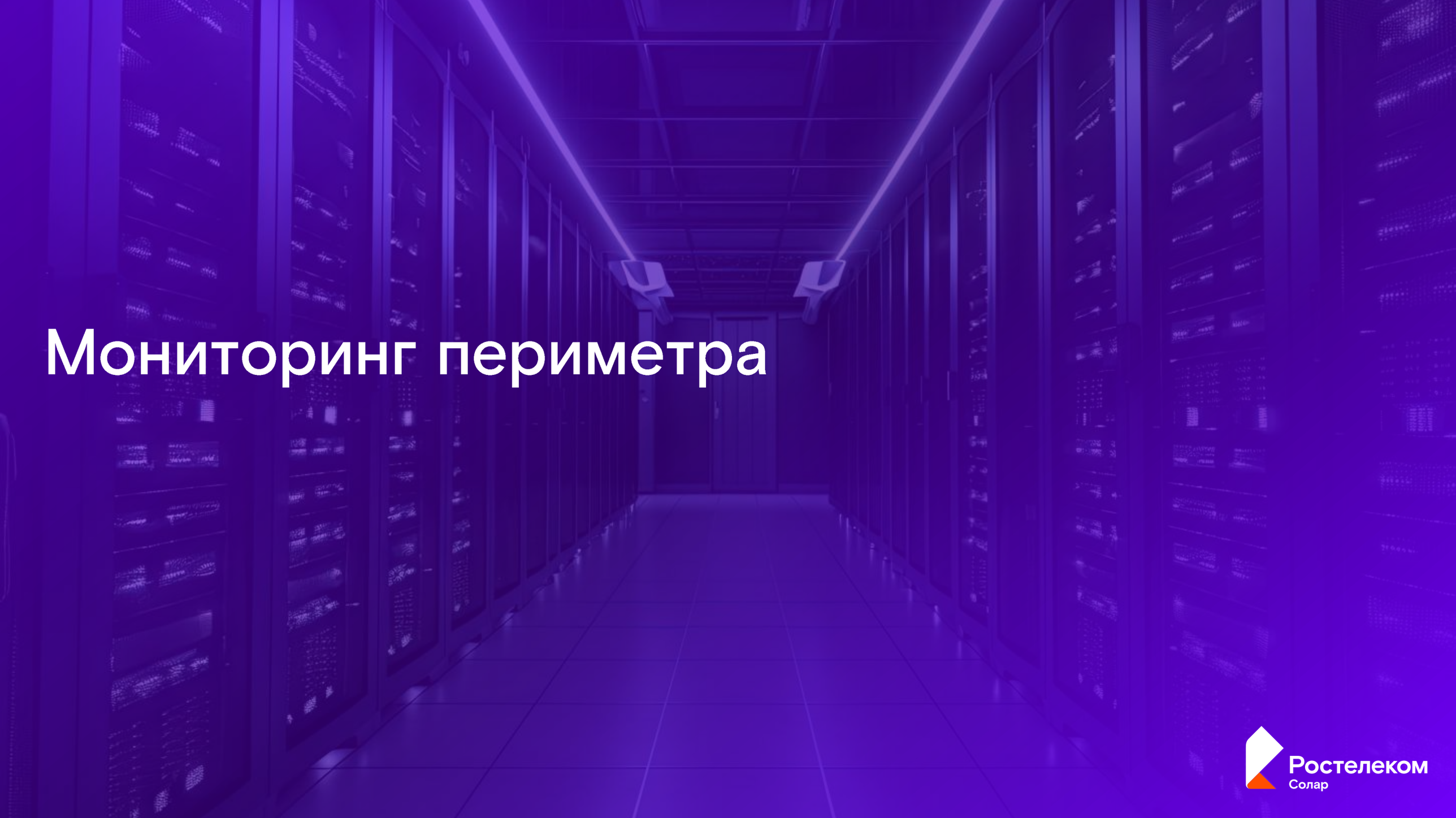
Источники данных:

- DarkNet и Deep web
- Telegram-каналы
- Специализированные интернет-площадки по продаже ООО и ИП

Особенности функционала:

- Верификация реквизитов компании
- Предоставление сведений о возможном наличии счетов в российских банках

Ростелеком Солар



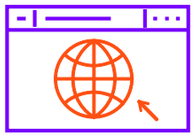
Мониторинг периметра

Ростелеком
Солар

Ключевые направления и объекты поиска

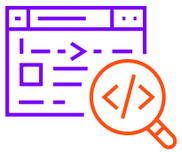
Домены и сертификаты

Выявление новых опубликованных ресурсов, контроль сроков действия SSL-сертификатов и регистрации доменных имен, оповещение о смене удостоверяющего центра



Теневое ИТ

Мониторинг диапазонов IP-адресов с целью выявления новых и некорректно выведенных из эксплуатации хостов и опубликованных на них сервисов

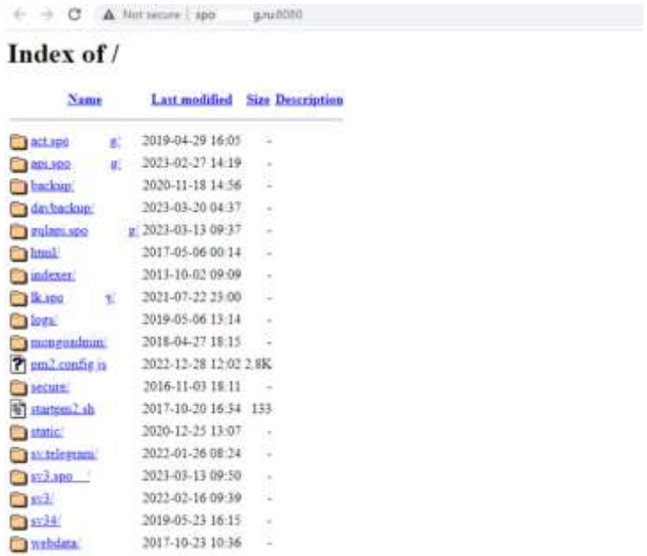


Контроль контента

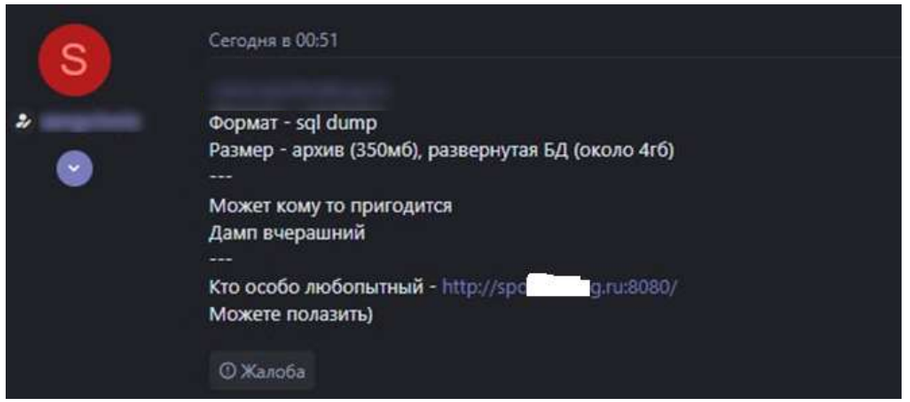
Мониторинг официальных сайтов на предмет обнаружения признаков несанкционированных изменений, содержащих маркеры угрозы

Ростелеком Солар

Мониторинг периметра



Наблюдение:
Выявленный открытый индекс файлов на сервере



Последствия:
База данных скачана и выставлена на даркнет-форуме

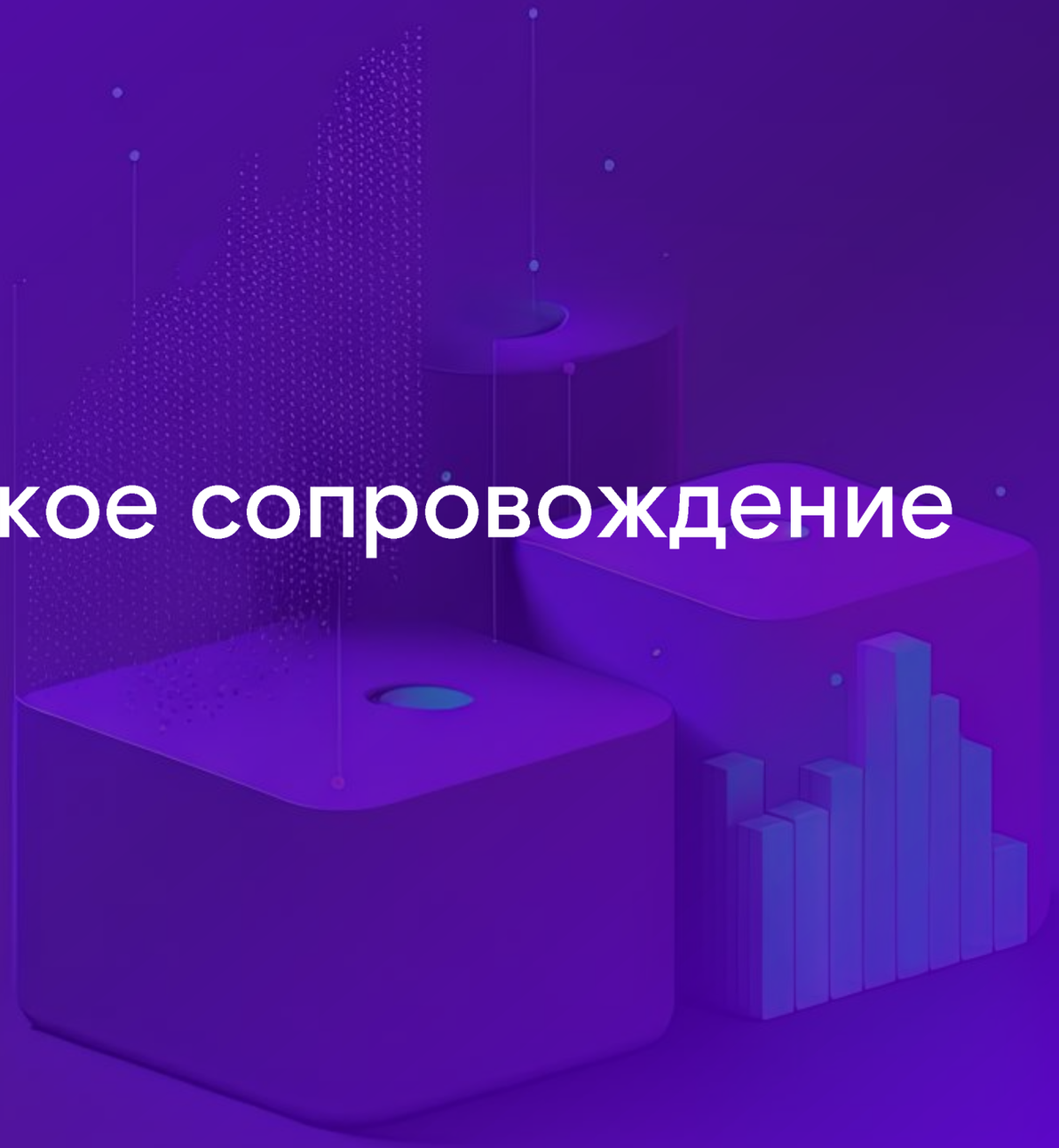
Источники данных:

- Открытые и самописные инструменты
- Публичные сервисы (Censys, Shodan, ZoomEye, Criminalip, Netlas)
- Регистраторы
- Удостоверяющие центры

Особенности функционала:

- Подготовка дифференциальных отчетов
- Сопоставление полученной информации с результатами анализа даркнета на предмет выявления готовящихся атак

Аналитическое сопровождение



Ростелеком
Солар

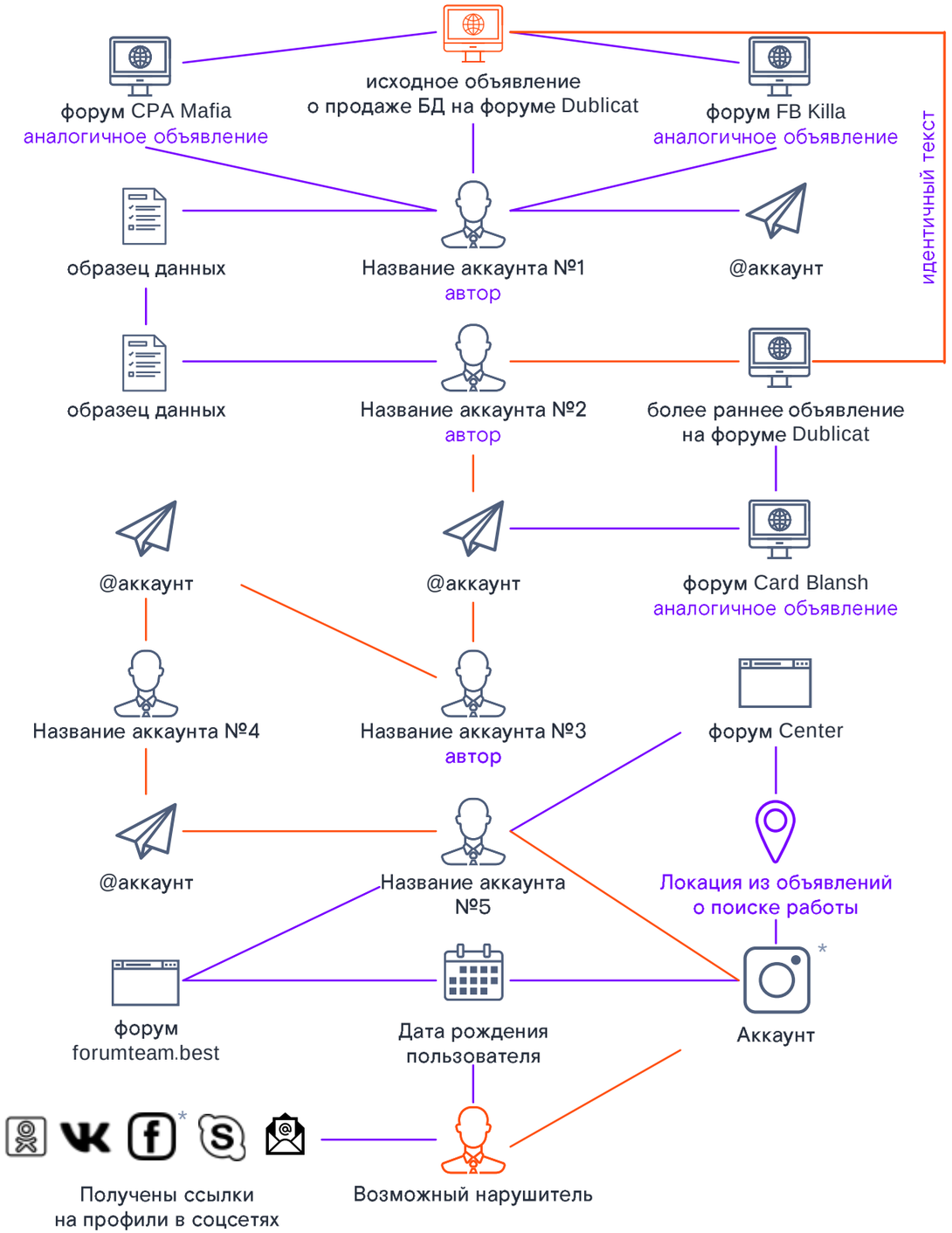
Традиционные DRP только оповещают об угрозах. Solar AURA в рамках дополнительного модуля предлагает полный комплекс аналитики, позволяющий:

- Собрать сведения об инциденте
- Раскрыть сеть-аккаунтов, замешанных в атаках
- Выявить особенности схемы злоумышленников
- Проанализировать утекшие данные и оценить угрозу от их распространения

Аналитические данные могут быть использованы для:

- Проведения проверки и идентификации внутреннего нарушителя
- Расследования причин инцидента
- Подготовки материалов для обращения в правоохранительные органы или суд

* Принадлежит Meta, признанной на территории России запрещенной и экстремистской организацией



Ростелеком
Солар

rt-solar.ru

Задать вопрос или попробовать сервис