SOLAR

Итоги 2023. Тренды 2024

Сергей Газизов, заместитель директора по развитию региональных продаж B2G

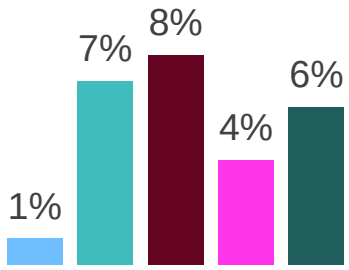
Ландшафт киберугроз 2023

SOLAR

- Заражение ВПО
- Эксплуатация уязвимостей
- Компрометация УЗ
- Веб-атаки
- Сетевые атаки
- НСД к ИС и сервисам

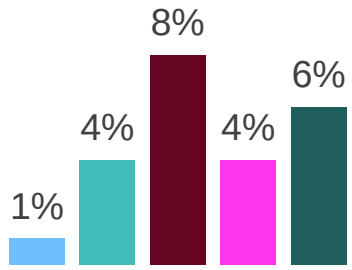
Q1

56%



Q2

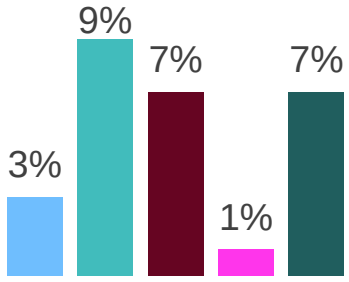
49%



Рост фонового шума – необходимость правильной приоритезации инцидентов

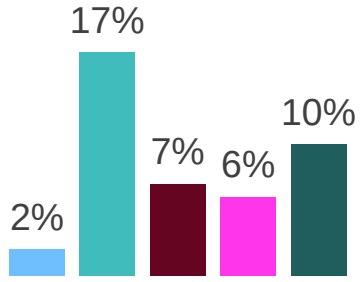
Q3

36%



Q4

17%



Тщательная подготовка хакеров к проведению атак, совершенствование техник, использование продвинутого инструментария

Тренд 2023

SOLAR

+7%

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

единственный тип инцидента, который продемонстрировал рост в 2023 году

КАКИЕ ФАКТОРЫ НА ЭТО ПОВЛИЯЛИ:

отсутствие регламентированного и выстроенного на постоянной основе процесса патч-менеджмента

смена фокуса хакеров: они научились использовать уязвимости в отечественном ПО, которых не меньше (а иногда и больше), чем в западных аналогах

повышение роли сенсоров SOC за счет усложнения кибератак и попыток злоумышленников вести скрытое распространение в инфраструктурах атакуемых компаний

Карта трендов 2023

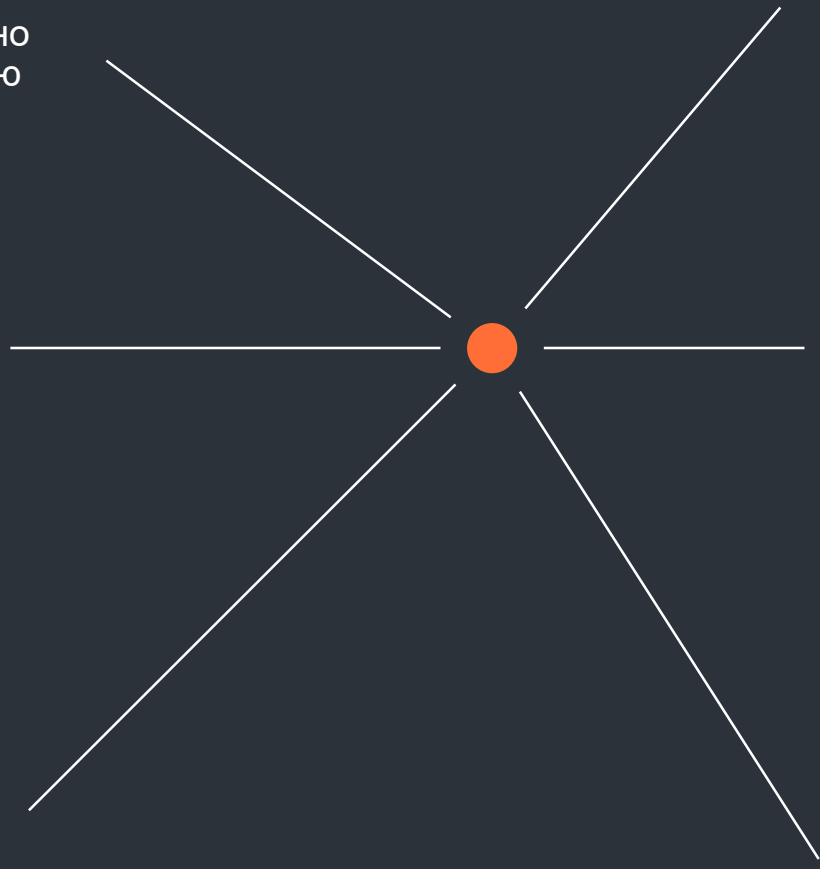
SOLAR

«КИБЕРМИР» ЯВЛЯЕТСЯ ОТРАЖЕНИЕМ РЕАЛЬНОГО

все изменения в нем происходят зеркально и с максимально быстрой обратной связью

ИСПОЛЬЗОВАНИЕ НЕЛЕГИТИМНОГО ПО

один из новых векторов атаки, актуальный и для внутреннего, и для внешнего нарушителя



ФИШИНГ И ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ

являются основными инструментами злоумышленников

АТАКИ ПОСТЕПЕННО УСЛОЖНЯЮТСЯ

базовых средств защиты становится недостаточно

УРОВЕНЬ ЗАЩИЩЕННОСТИ

российских компаний за 2023 год существенно возрос

КИБЕРРАЗВЕДКА, СКАНЫ ПЕРИМЕТРА

то, что позволяет хакерам тщательно подготовиться к атаке и действовать наверняка

Продуктовый портфель ГК «Солар»

SOLAR

Сервисы

Solar MSS
управляемые сервисы кибербезопасности

- Защита от сетевых угроз (UTM)
- Защита электронной почты (SEG)
- Защита от продвинутых угроз (Sandbox)
- Защита веб-приложений (WAF)
- Защита от DDoS-атак (Anti-DDoS)
- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)

Экосистема управляемых сервисов кибербезопасности для комплексной защиты от массовых киберугроз (MSS)

Solar JSOC
экспертные сервисы кибербезопасности

- Мониторинг, реагирование и анализ инцидентов ИБ
- Комплексный контроль защищенности: пентест, RedTeaming, анализ защищенности
- Техническое расследование инцидентов ИБ
- Эксплуатация систем ИБ и реагирование на атаки
- Построение SOC и его частных процессов
- Мониторинг АСУ ТП и объектов КИИ (SOC OT)
- Анализ угроз и внешней обстановки (Aura)
- Защита конечных точек (EDR)
- Анализ сетевого трафика (NTA)

Первый и крупнейший в России коммерческий центр мониторинга и реагирования на киберинциденты (SOC)

Технологии

- Solar Dozor (DLP)
- Solar appScreener (SAST, DAST, SCA)
- Solar inRight (IdM/IGA)
- Solar webProxy (SWG)
- Solar addVisor (EM)
- Solar Safeinspect (PAM)
- Solar NGFW (FW+IPS+DPI)
- Solar DAG (Управление доступом к данным)
- Solar SafeConnect (Защищенный удаленный доступ)

Услуги

- Solar Интеграция
- Киберполигон
- Соответствие требованиям
- Кибербезопасность АСУ ТП
- Сервисная поддержка
- Консалтинг
- Импортозамещение
- Солар ТЗИ

SOLAR

Анализ кода приложений на уязвимости

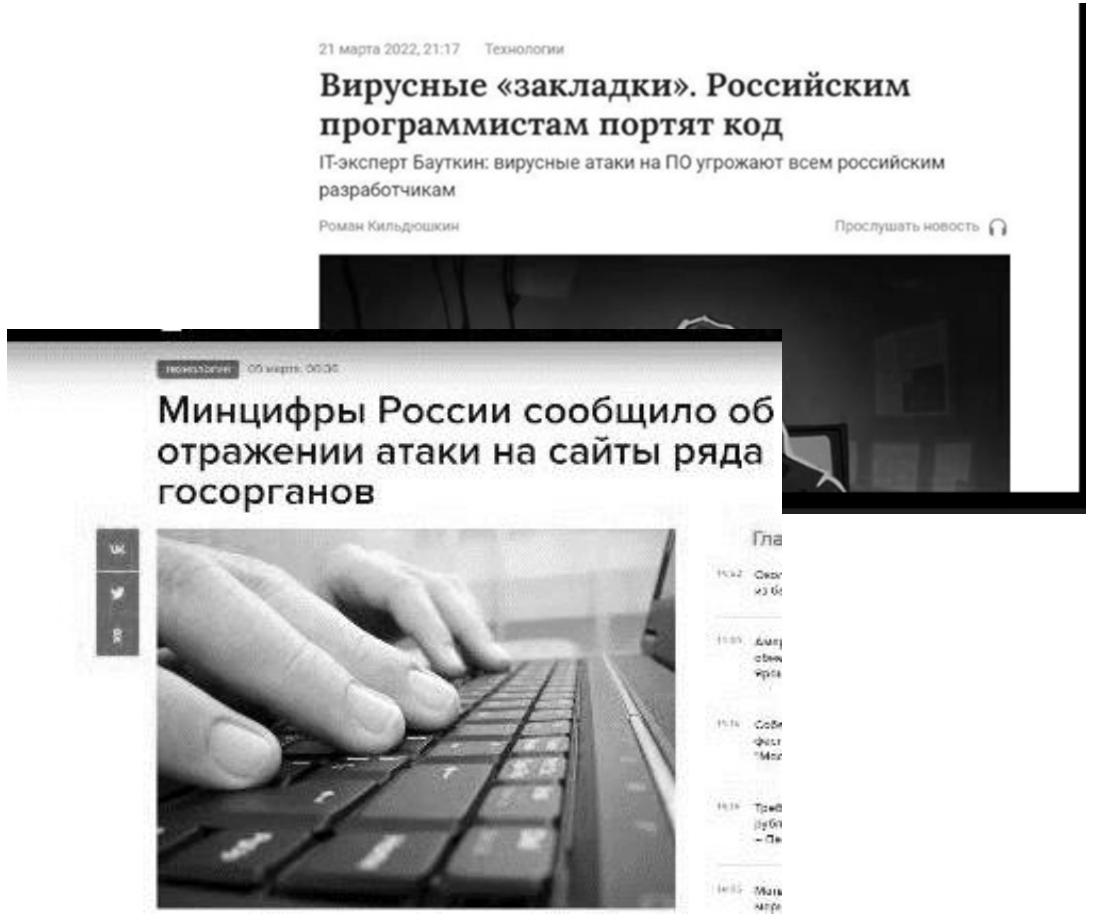
БЕЗОПАСНАЯ РАЗРАБОТКА – ГЛАВНЫЙ ШАГ

с которого начинается
кибериммунитет организации

88% ПРИЛОЖЕНИЙ СОДЕРЖАТ КАК МИНИМУМ ОДНУ КРИТИЧЕСКУЮ УЯЗВИМОСТЬ*

УЯЗВИМОСТИ В ПРИЛОЖЕНИЯХ - ОСНОВНОЙ ВЕКТОР АТАК ПО НАЦИОНАЛЬНОМУ ПРИЗНАКУ

- Атаки на сайты организаций из РФ
- Внедрение вредоносного кода в open-source-библиотеки



*Данные отчета Solar JSOC

ПРОБЛЕМЫ, С КОТОРЫМИ СТАЛКИВАЮТСЯ…

SOLAR

НОВИЧКИ В КИБЕРБЕЗОПАСНОСТИ

- Не знают, **с чего начать** внедрение процессов безопасной разработки
- **Нет понимания методологий** и опыта внедрения безопасной разработки, приходится «наступать на грабли»
- Непонятно, **какие инструменты нужны** в первую очередь, как их выбрать и использовать
- Сложно самим разобраться с нюансами настройки решения, нужна помощь экспертов
- **Сложно разобраться** в требованиях регуляторов в части анализа кода
- У разработчиков **нет экспертизы** по безопасности, их учили писать код
- Непонятно, **как убедить разработчиков**, что в разработке нужна безопасность

ОРГАНИЗАЦИИ С ВЫСТРОЕННЫМИ ПРОЦЕССАМИ БЕЗОПАСНОЙ РАЗРАБОТКИ

- **Нет единой базы** полезной информации и best practices по интеграции сканеров в цикл DevOps
- **Сложно найти** качественное российское решение по анализу кода, сравнимое с западными по техническим характеристикам
- **Надо предотвратить утечки** данных пользователей и избежать репутационных потерь
- Нужен инструмент по написанию и **тестированию собственных правил**

КОМПЛЕКСНАЯ КИБЕРБЕЗОПАСНОСТЬ – НАШ ВЕКТОР РАЗВИТИЯ

SOLAR

ГК «Солар» имеет **центр экспертизы по безопасной разработке** для бизнеса любого размера и уровня зрелости, а также многолетний опыт в области построения процессов безопасной разработки и внедрения инструментов анализа защищенности ПО в цикл DevOps.

Методологии, основанные на лучших практиках AppSec и проверенные на десятках успешных проектов

Готовые фреймворки аудита, консалтинга, построения и гармонизации процессов разработки защищенного ПО (SSDLC)

Собственная технологическая платформа для контроля безопасности ПО с использованием ключевых методов анализа (SAST, DAST, SCA, SCS)

Апробированные методики обучения сотрудников безопасной разработке и работе с технологиями анализа кода

Сервис и техподдержка на всех этапах реализации комплексного проекта

СОБСТВЕННЫЕ ТЕХНОЛОГИИ

SOLAR

В основе подхода - единая технологическая платформа для комплексного анализа безопасности приложений

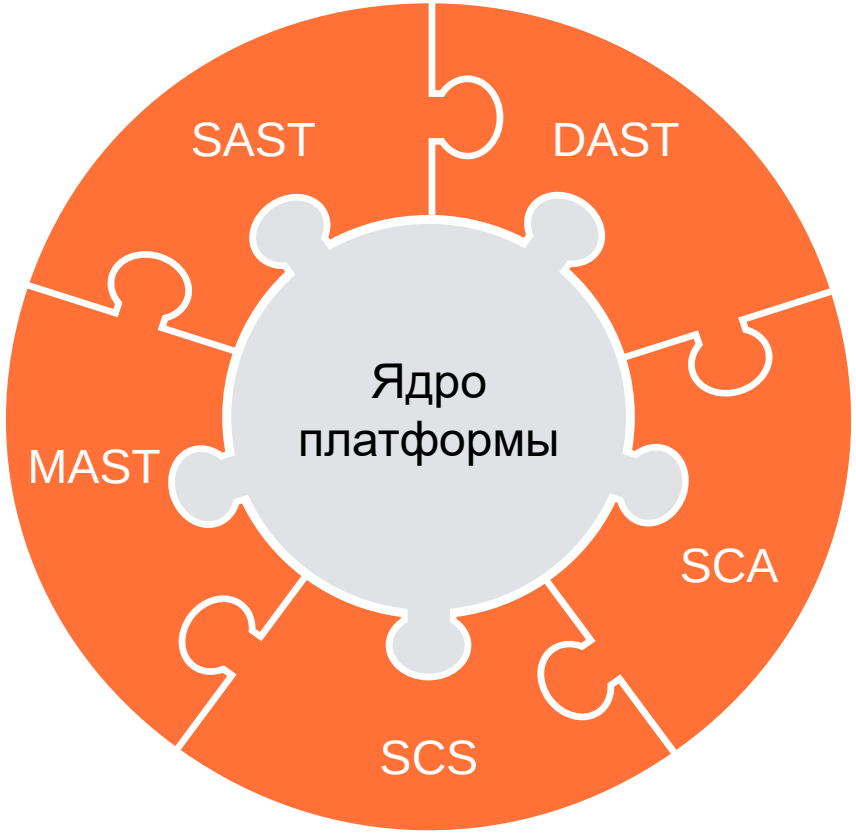
ЯДРО ПЛАТФОРМЫ SOLAR APPSCREENER

- Единый интерфейс для удобного управления сканированиями
- Корреляция результатов разных видов анализа и единый отчет
- Технология Fuzzy Logic Engine для сокращения ложных срабатываний

ТЕХНОЛОГИЧЕСКИЕ МОДУЛИ

- Статический анализ кода (SAST)
- Динамический анализ кода (DAST)
- Анализ состава ПО (SCA)
- Анализ мобильных приложений (MAST)
- Анализ безопасности цепочки поставок ПО (SCS)

Результаты сканирований между ядром и технологическими модулями передают коннекторы к технологическим модулям



36
языков программирования

10
форматов исполняемых файлов

5
модулей анализа кода в одном решении

Удобная интеграция с Git и Subversion, серверами CI/CD, Jira и другими инструментами

Выполнение требований регуляторов

SOLAR

Внесен в Единый реестр отечественного ПО (№ 6119) и сертифицирован ФСТЭК России на соответствие требованиям по 4-му уровню контроля отсутствия НДВ (сертификат № 4007) и ТУ.

Помогает выполнять постановления 683-П, 717-П, 757-П Банка России в части анализа защищенности ПО и оценки соответствия по требованиям ОУД 4.

Банк России

Соответствует приказам 239, 76 и требованиям ГОСТ Р 56939-2006 ФСТЭК России в части анализа защищенности и исходного кода ПО.

СХЕМА ВНЕДРЕНИЯ КОМПЛЕКСНОГО ПРОЕКТА

SOLAR

Схема внедрения проекта может варьироваться в зависимости от задач и особенностей заказчика

1 АУДИТ ПРОЦЕССОВ И СИСТЕМ ЗАКАЗЧИКА

- Сбор данных и аудит
- Создание ролевой модели
- Распределение зон ответственности

2 ВНЕДРЕНИЕ В SOLAR APPSCREENER

- Подготовка вычислительных мощностей для Solar appScreener
- Подготовка доступа к инфраструктуре
- Внедрение продукта

3 АДАПТАЦИЯ МЕТОДОЛОГИИ АНАЛИЗА КОДА

- Уточнение требований к безопасности ПО
- Создание регламентов проверки кода
- Адаптация методологии проверки ПО

4 ОБУЧЕНИЕ СОТРУДНИКОВ

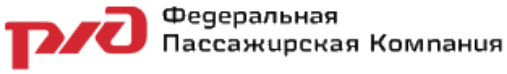
- Создание программы обучения и определение состава участников
- Обучение специалистов заказчика

5 ЗАПУСК НЕПРЕРЫВНОГО АНАЛИЗА ПО НА УЯЗВИМОСТИ И ЗАКЛАДКИ

- Запуск непрерывного контроля ПО
- Консультация и техническая поддержка на всех этапах

КЛЮЧЕВЫЕ ЗАКАЗЧИКИ

SOLAR



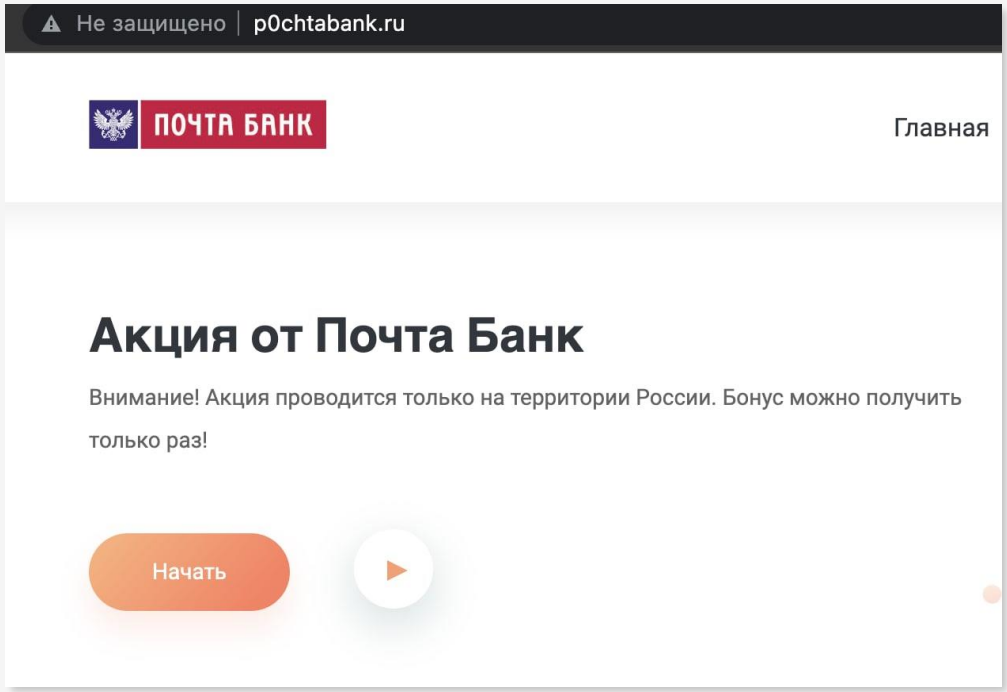
SOLAR

Киберразведка

Антифишинг

SOLAR

p0chtabank.ru

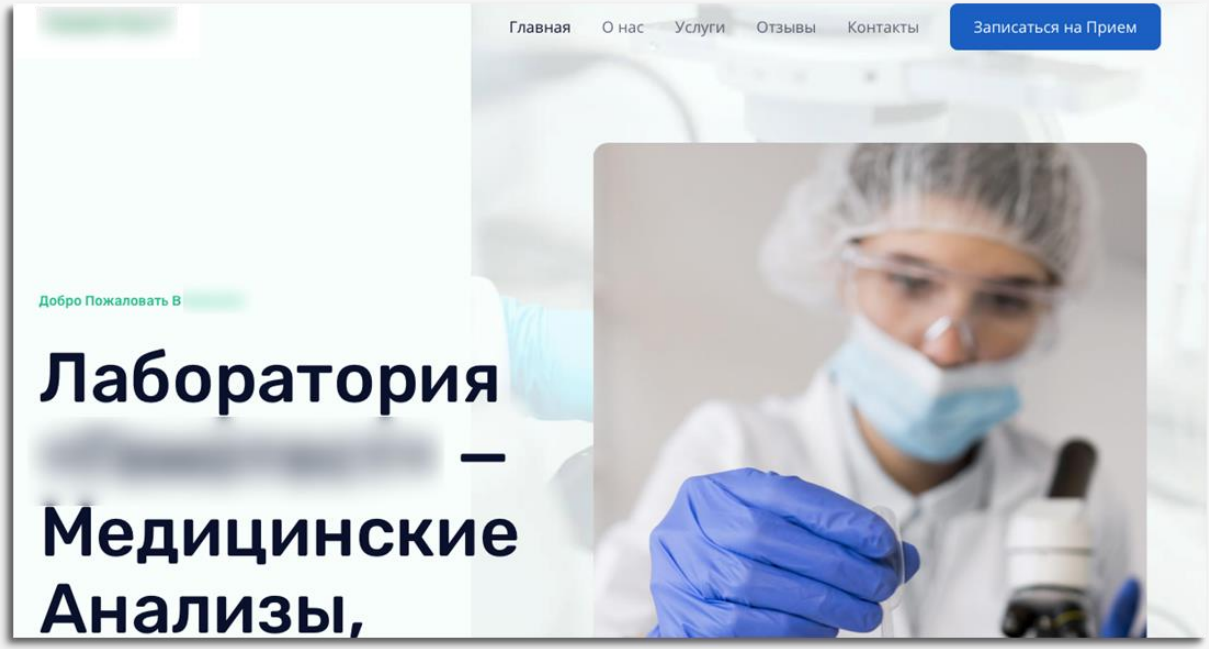


Обнаружен: **14.12.2022**

Регистратор: **DNSPod**

IP-адрес: **152.136.26.198**

*****test.moscow



Обнаружен: **30.06.2021**

Регистратор: **Regtime**

IP-адрес: **95.216.78.217**

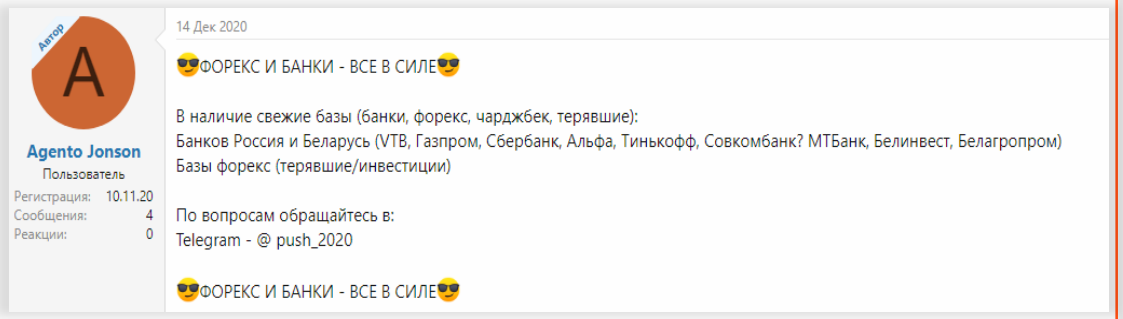
Источники данных:

- Реестры доменных имен (1000+ доменных зон, более 200 тыс. доменных имен в сутки)
- Реестры SSL-сертификатов (более 10 млн ресурсов в сутки)
- Поисковые системы
- Данные DNS

Базы данных

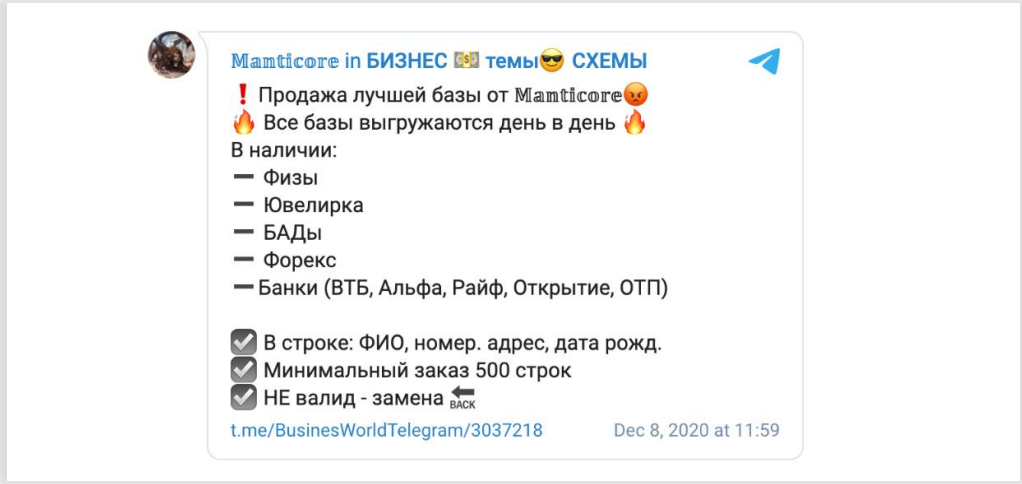
SOLAR

Пример объявления



Публикация в **DarkNet**

Пример объявления



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

Утечки документов

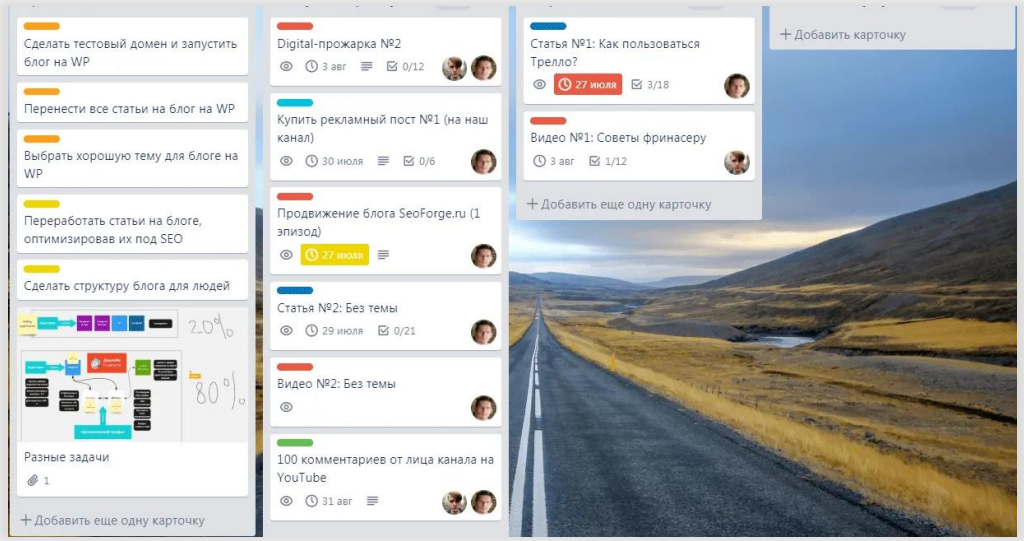
SOLAR

Index of /TOSHIBA_EXT/Архив/

[parent directory]

Name	Size	Date modified
6. Гибель Богов-2. Книга 6. Прошедшая вечность.fb2	2.0 MB	5/28/18, 3:00:00 AM
Glen Cook/		2/14/20, 3:00:00 AM
Google Диск/		2/14/20, 3:00:00 AM
KMSAuto Net 2015 v1.3.6 Portable/		9/5/19, 3:00:00 AM
Photo.scr	1.5 MB	3/1/20, 3:00:00 AM
Васильев Владимир/		9/5/19, 3:00:00 AM
Гамильтон Питер - Сборник произведений/		9/5/19, 3:00:00 AM
Перумов Ник - Сборник произведений/		9/5/19, 3:00:00 AM
Прайс/		1/30/20, 3:00:00 AM
Ростсельмаш/		1/6/20, 3:00:00 AM
СКЛАД/		1/30/20, 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:

- Darknet & Deep Web
- Telegram
- Социальные сети
- Файлообменники
- FTP и веб-серверы

Возможное реагирование:

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

Выявленные аккаунты

SOLAR

evgeniya[redacted]@[redacted].ru

Утечки

Дата утечки	Пароль	Источник
2023-03-23	5328**	avito.ru
–	Ushk***	yugopolis.pro

На этот раз пострадал **сервис** nomer.io 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

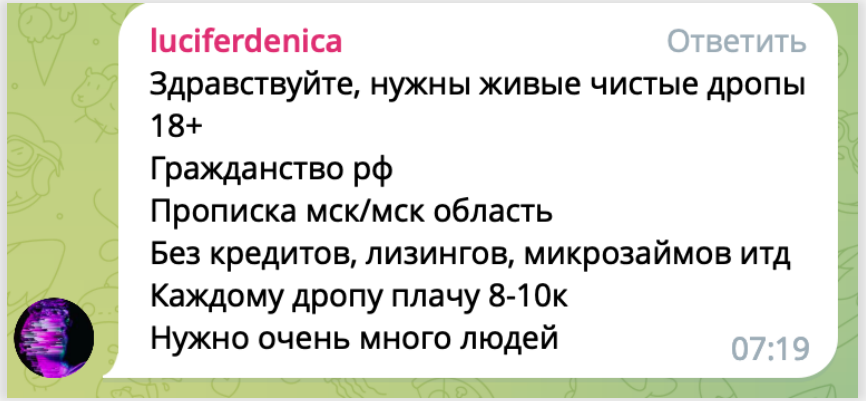
Нелегальные услуги

SOLAR

Пример объявления

Публикация в **DarkNet**

Пример выявления готовящейся атаки на кредитную организацию*



Публикация в **Telegram**

*Массовый найм «чистых» дропов свидетельствует о планируемом выводе крупных сумм денег на территории Московского региона.

Обнаружение такого рода событий позволяет заранее подготовиться к возможным атакам и подготовить антифрод для обнаружения такого рода аномалий.

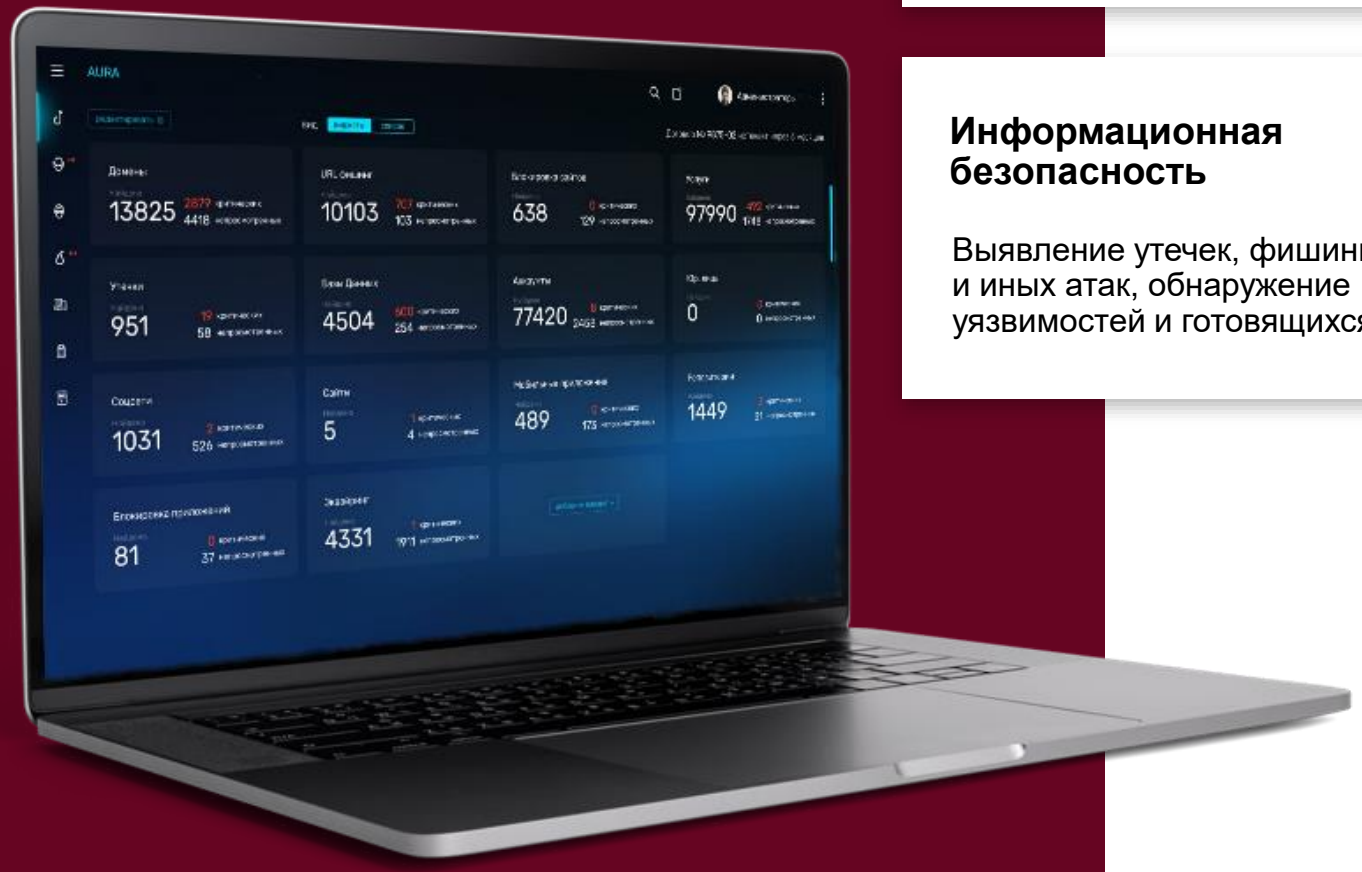
Источники данных:

- Darknet & Deep Web
- Telegram
- Социальные сети
- Торговые площадки

Возможное реагирование:

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

Как работает киберразведка



Экономическая безопасность

Обнаружение атак на цепочки поставок, ложного партнерства, махинаций с сервисами, услугами, продуктами

Защита бренда

Выявление фейковых страниц и аккаунтов, фактов неправомерного использования товарного знака и пр.

Информационная безопасность

Выявление утечек, фишинговых и иных атак, обнаружение уязвимостей и готовящихся атак

Безопасность первых лиц организации

Комплекс услуг по защите личного бренда и приватности руководителей в сети

Репутационные риски

Обнаружение информационных атак, негативных публикаций, кражи личности

SOLAR

Преимущества использования сервиса

01

Отчеты и статистика

Сервис имеет возможность гибкого формирования отчетов исходя из заданных критериев и данных статистики по выявленным событиям

02

Команда экспертов

Для работы с сервисом не требуются высококвалифицированные специалисты. Процесс анализа и обработки информации осуществляется аналитиками сервиса

03

Простота работы

Отсутствие необходимости внесения изменений в инфраструктуру заказчика и сервисная модель обеспечивают предоставление услуг под ключ без дополнительных затрат на интеграцию

04

Непрерывность процессов

Сервис функционирует в режиме 24/7/365, обеспечивая непрерывное выявление угроз и оперативное оповещение о выявленных событиях

05

Реагирование на инциденты

Подписка включает в себя проведение работ по блокированию вредоносных ресурсов, сбору дополнительной информации и устранению нарушений, связанных с брендом

06

Источники данных

Сервис осуществляет сбор данных как из публичных, так и узкоспециализированных источников, доступ к которым закрыт для большинства интернет-пользователей. Перечень источников постоянно обновляется и актуализируется

+7 (499) 755-07-70
info@rt-solar.ru

SOLAR

Центральный офис.
125009, Москва,
Никитский переулок, 7с1