ВЫЯВЛЕНИЕ И БЛОКИРОВКА ФИШИНГА, ЗАТРАГИВАЮЩЕГО БРЕНД КОМПАНИИ

wildberries

Антон Жаболенко
Директор по безопасности
Wildberries

«Учитывая популярность бренда Wildberries, неудивительно, что мошенники пытаются использовать его для обмана пользователей. Однако мы совместно с Solar AURA применяем все возможные инструменты блокировки фишинговых ресурсов для защиты наших клиентов и партнеров».

Профиль организации

WILDBERRIES

Крупнейший в России маркетплейс

Отрасль: ретейл

Размер: офис + 2 млн кв. м складских помещений

Данные о проекте

Solar AURA

О сервисе: комплексный DRP-сервис мониторинга внешних цифровых угроз

Модуль: антифишинг

Период мониторинга: март 2023 – февраль 2024

Покрытие: 76817 интернет-ресурсов, которые могут быть использованы для атак, затрагивающих бренд Wildberries

110+ МЛН

пользователей

7293

потенциально опасных ресурса выявлено

10+ МЛН

заказов в день

783

фишинговых сайта обнаружено и успешно заблокировано

1 МИН. 46 СЕК.

минимальное время блокировки фишинга, связанного с Wildberries

SOLAR

Цель

Выявление и блокировка фишинговых ресурсов

Задача

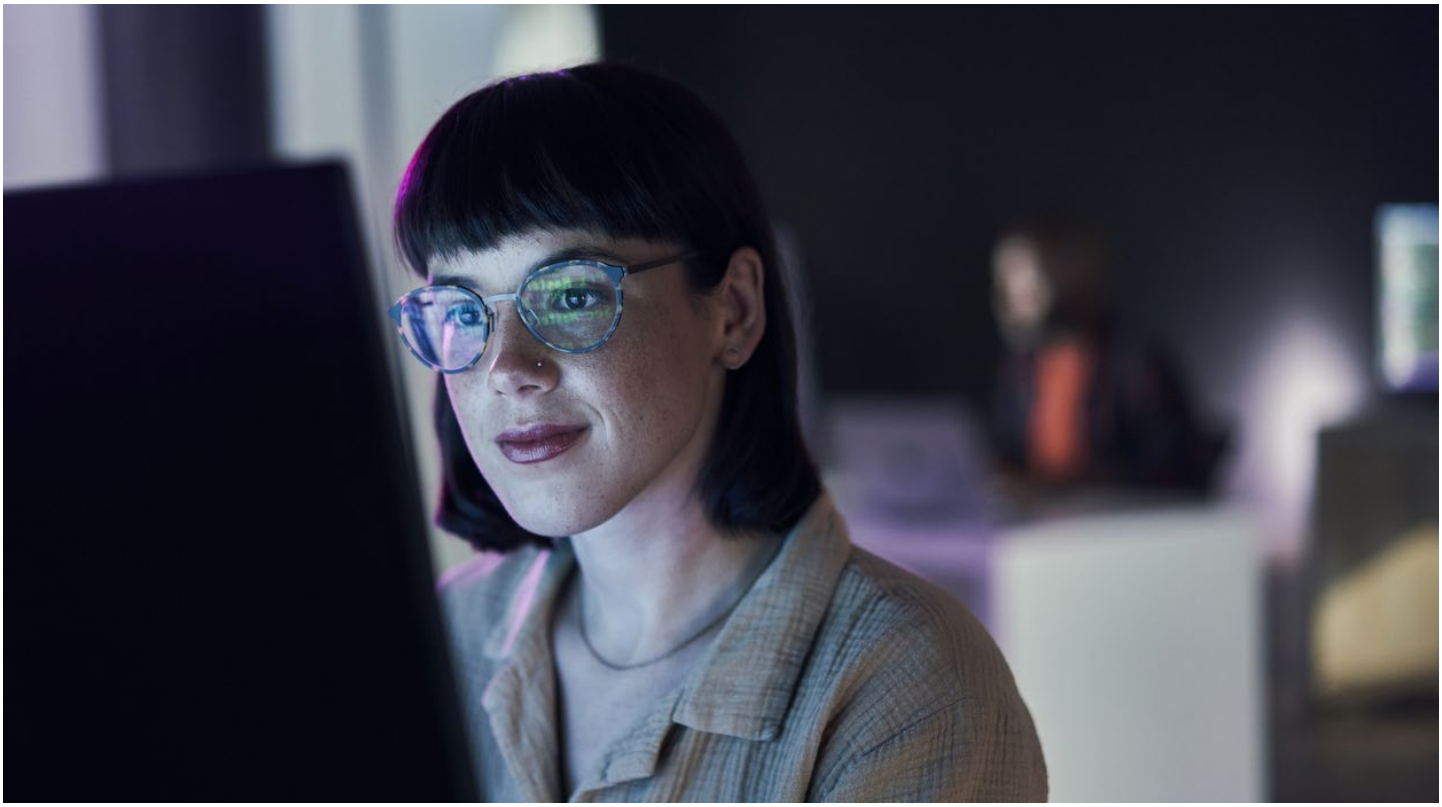
- Противодействие атакам мошенников, эксплуатирующих бренд Wildberries на фиктивных интернет-ресурсах и несущих угрозу для клиентов и партнеров компании
- Защита репутации Wildberries

Решение

- Непрерывный мониторинг публичных и закрытых сегментов интернета с максимально широким покрытием
- Оценка и верификация аналитиком обнаруженных потенциально опасных ресурсов
- Оперативная блокировка выявленных фишинговых сайтов

Результат

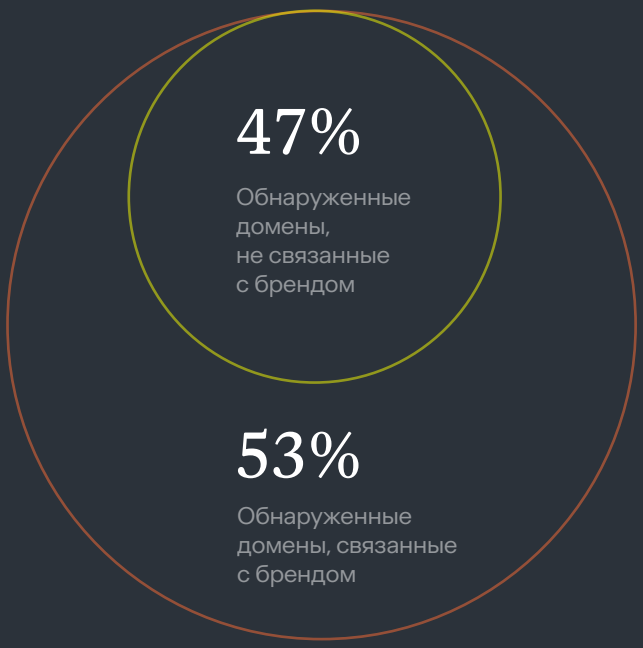
- 99,2% фишинговых сайтов, эксплуатирующих бренд Wildberries, выявлено сервисом Solar AURA
- 100% обнаруженных фишинговых сайтов заблокировано



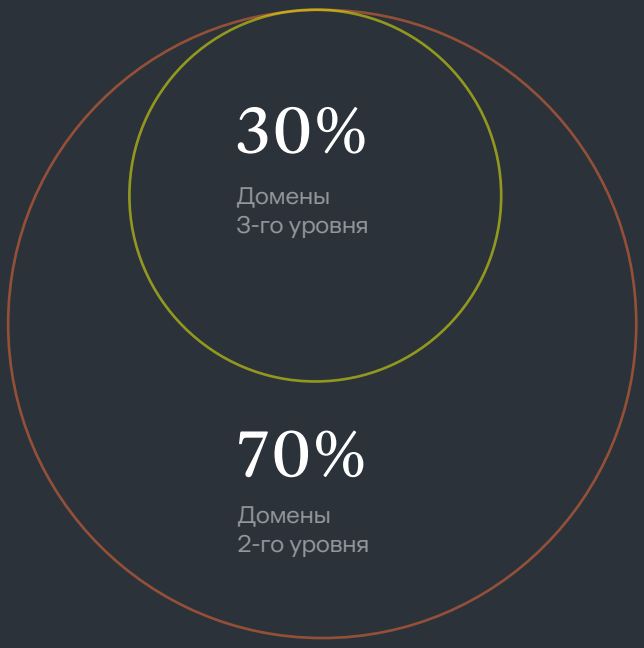
SOLAR

Выявление небрендированных доменов

Почти половина обнаруженных доменных имен не имела отношения к бренду и не была связана с ним семантически



Ярко выражена тенденция к использованию доменов 3-го уровня, выявлять которые значительно сложнее, чем аналогичные домены 2-го уровня



Противодействие наиболее опасным фишинговым атакам

01

Помимо фишинга, направленного на клиентов – покупателей Wildberries, компания столкнулась с новым видом атак, цель которых – получение доступа в личный кабинет продавцов маркетплейса

02

Особенность таких атак – использование кириллических доменов, не имеющих отношения к торговой марке

03

Новый вид атак затрагивает партнеров, которые находятся в продолжительных отношениях с Wildberries и имеют средства на привязанных к личному кабинету виртуальных банковских счетах

SOLAR

75 сайтов, предназначенных для кражи доступа в ЛК партнера Wildberries, выявлено и заблокировано

Скорость блокировки обнаруженных сайтов:

Выводы

Круглосуточный автоматизированный мониторинг, оценка и верификация обнаруженных угроз опытными аналитиками, налаженные отношения с регистраторами доменных имен и хостинг-провайдерами позволили команде сервиса Solar AURA продемонстрировать высокую эффективность выявления и блокировки большого объема фишинговых ресурсов, связанных с одним из самых популярных российских брендов.

Обнаружение небрендированных, в том числе кириллических, доменов потребовало особого подхода к формированию правил, настройке технических средств и аналитическому сопровождению, который был успешно реализован благодаря высокой экспертизе и многолетнему опыту специалистов сервиса.