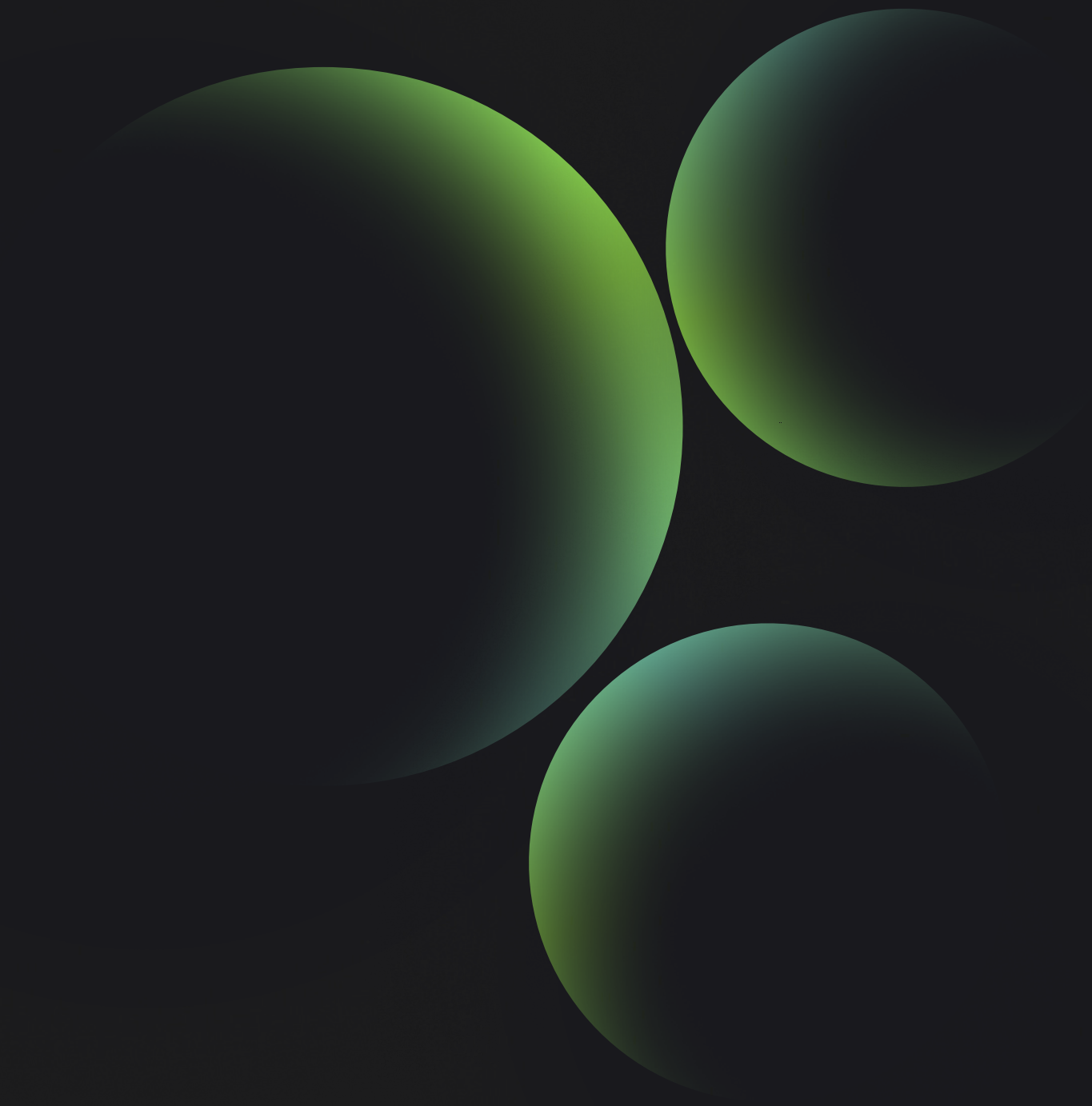
Dr.WEB

«Доктор Веб»: обзор вирусной активности во II квартале 2025 года



Главное

Согласно статистике детектирований антивируса Dr.Web, во II квартале 2025 года общее число обнаруженных угроз снизилось на **7,38%** по сравнению с I кварталом. Число уникальных угроз при этом также сократилось — на **23,10%**. Наиболее часто на защищаемых устройствах выявлялось нежелательное рекламное ПО, бэкдоры, рекламные трояны и вредоносные скрипты. В почтовом трафике самыми распространенными угрозами стали трояны-загрузчики, различные вредоносные скрипты и трояны-дропперы.

Пользователи, чьи файлы были затронуты троянами-шифровальщиками, чаще всего сталкивались с энкодерами

Trojan.Encoder.35534 **Trojan.Encoder.35209** **Trojan.Encoder.29750**

В апреле вирусные аналитики компании «Доктор Веб» сообщили о трояне, найденном в прошивке ряда моделей Android-смартфонов. С его помощью киберпреступники похищали криптовалюту. Кроме того, наши специалисты выявили Android-трояна, которого злоумышленники внедрили в одну из версий популярной картографической программы и использовали для слежки за российскими военнослужащими.

В течение II квартала наши интернет-аналитики обнаружили множество новых мошеннических сайтов. Среди них — сайты несуществующих образовательных площадок, якобы позволявших потенциальным жертвам пройти онлайн-обучение и повысить свою квалификацию, а также очередные сайты инвестиционной тематики, обещавшие быстрый и легкий заработок.

Статистика детектирований на мобильных устройствах продемонстрировала снижение активности рекламных троянов Android.HiddenAds, однако данное семейство вредоносных программ по-прежнему остается наиболее распространенной Android-угрозой. Вместе с тем во II квартале наша вирусная лаборатория обнаружила в каталоге Google Play множество новых угроз.

Главные тенденции II квартала

Снижение числа угроз, выявленных на защищаемых устройствах

Снижение числа уникальных угроз, задействованных в атаках

Появление множества мошеннических сайтов, якобы связанных со сферой образования и финансами

В каталоге Google Play выявлены очередные вредоносные и нежелательные программы

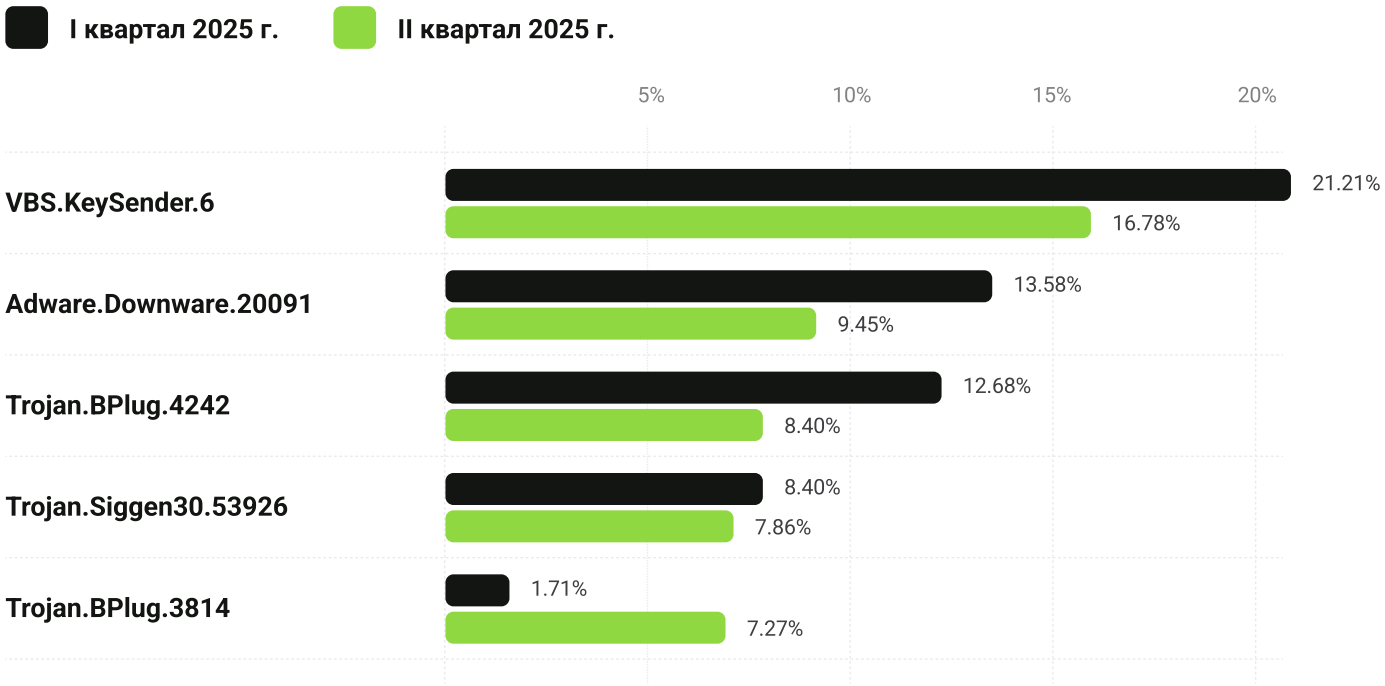
Рекламные трояны Android.HiddenAds остаются одними из наиболее распространенных Android-угроз

Обнаружение в прошивке ряда моделей Android-смартфонов трояна, предназначенного для кражи криптовалюты

Фиксация атаки трояна-шпиона на российских военнослужащих, использующих популярное картографическое ПО для Android-устройств

По данным сервиса статистики «Доктор Веб»

Наиболее распространенное вредоносное и рекламное ПО согласно данным сервиса статистики «Доктор Веб»



VBS.KeySender.6

Вредоносный скрипт, который в бесконечном цикле ищет окна с текстом mode extensions, разработчика и розробника и шлет им событие нажатия кнопки Escape, принудительно закрывая их.

Adware.Downware.20091

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Trojan.BPlug.4242 **Trojan.BPlug.3814**

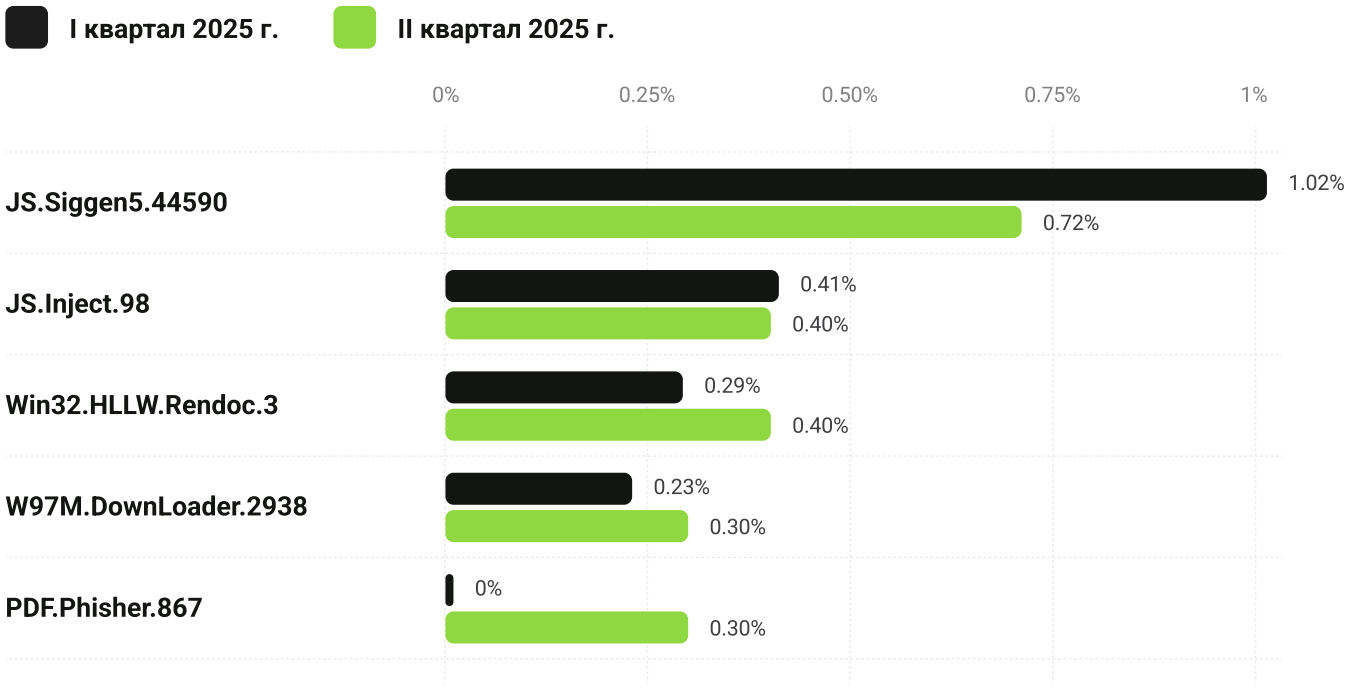
Детектирование вредоносного компонента браузерного расширения WinSafe. Этот компонент представляет собой сценарий JavaScript, который демонстрирует навязчивую рекламу в браузерах.

Trojan.Siggen30.53926

Хост-процесс модифицированного злоумышленниками фреймворка Electron, мимикрирующий под компонент приложения Steam (Steam Client WebHelper) и загружающий JavaScript-бэкдор.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике



JS.Siggen5.44590

Вредоносный код, добавленный в публичную JavaScript-библиотеку es5-ext-main. Демонстрирует определенное сообщение, если пакет установлен на сервер с часовым поясом российских городов.

JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Они встраивают вредоносный скрипт в HTML-код веб-страниц.

Win32.HLLW.Rendoc.3

Сетевой червь, распространяющийся в том числе через съемные носители информации.

W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих уязвимости документов Microsoft Office. Они предназначены для загрузки других вредоносных программ на атакуемый компьютер.

PDF.Phisher.867

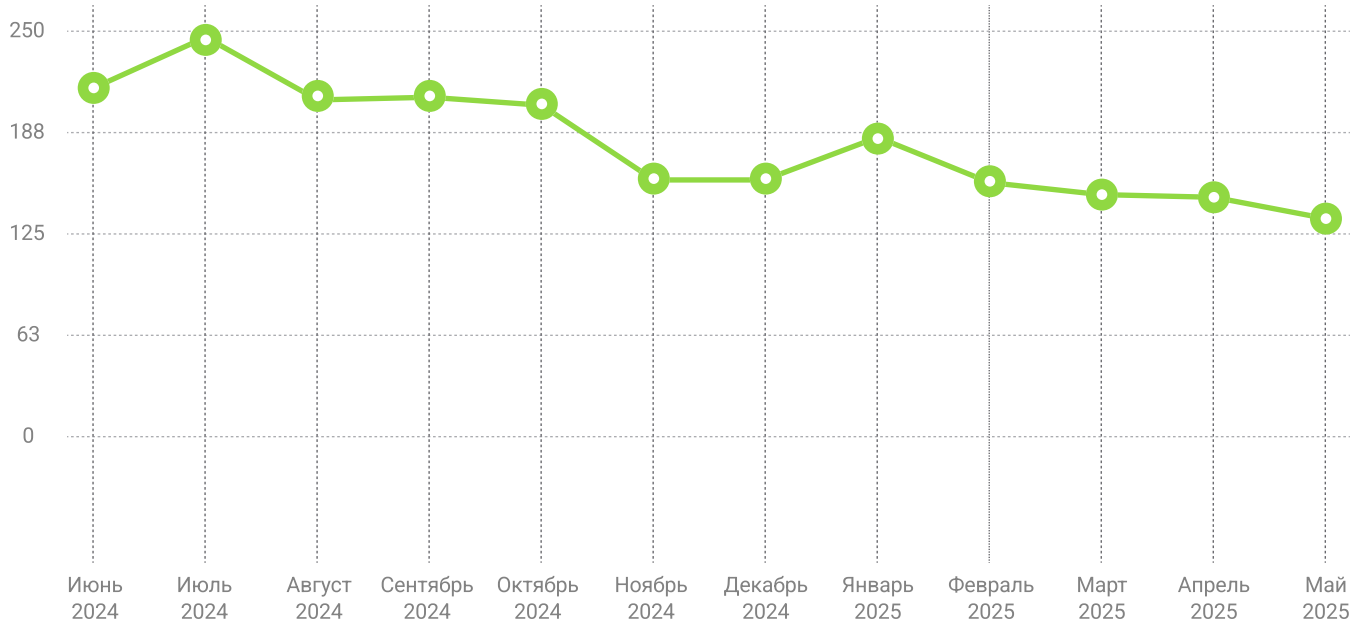
PDF-документы, используемые в фишинговых email-рассылках.

Шифровальщики

Во II квартале 2025 года число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, снизилось на 14,65% по сравнению с I кварталом.

Динамика поступления запросов на расшифровку в службу технической поддержки «Доктор Веб»:

Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»

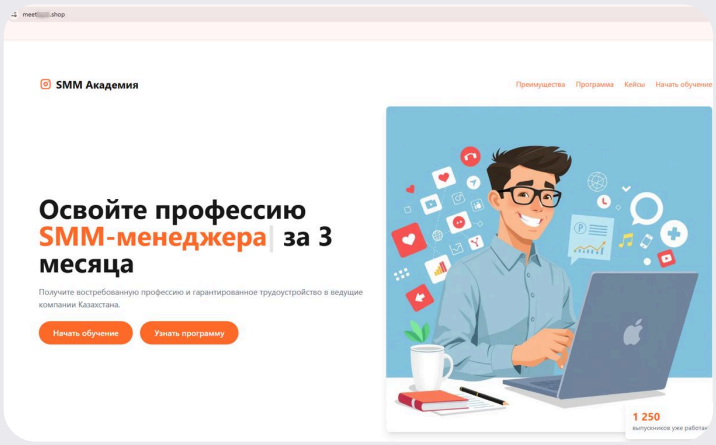


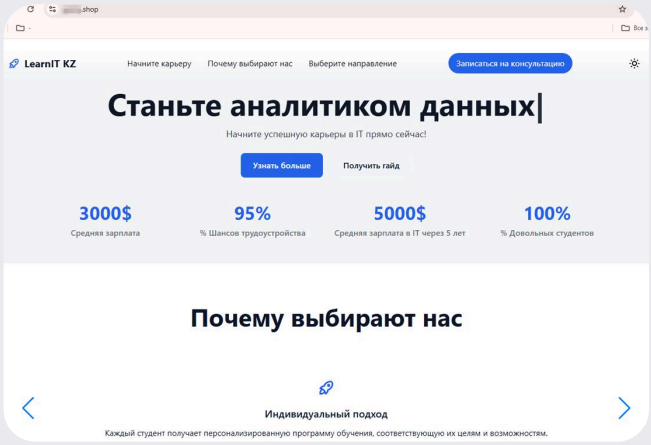
Наиболее распространенные энкодеры II квартала 2025 года:

1. Trojan.Encoder.35534 — 24.41% обращений пользователей
2. Trojan.Encoder.35209 — 4.41% обращений пользователей
3. Trojan.Encoder. 29750 — 2.71% обращений пользователей
4. Trojan.Encoder. 35067 — 2.71% обращений пользователей
5. Trojan.Encoder.41868 — 2.71% обращений пользователей

Сетевое мошенничество

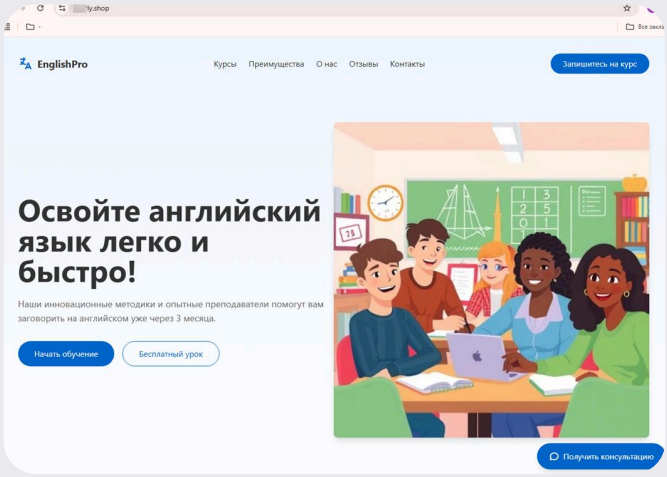
В течение II квартала 2025 года интернет-аналитики компании «Доктор Веб» выявили множество мошеннических веб-сайтов, якобы связанных со сферой образования. Так, распространение получили интернет-ресурсы, предлагавшие пройти обучение тем или иным профессиям.

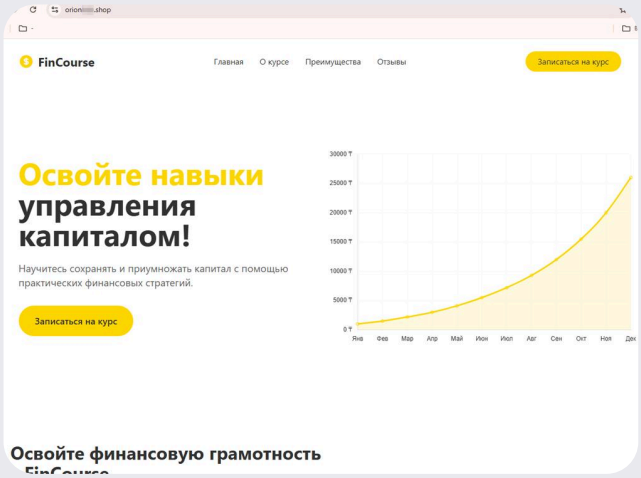




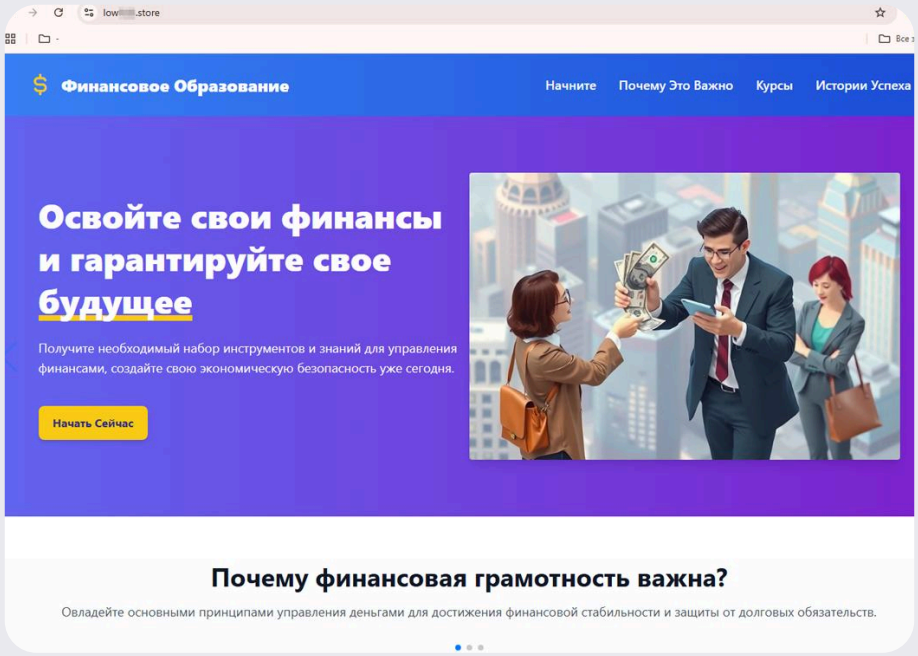
Например, рассчитанные на казахстанских пользователей платформы SMM Академия и LearnIT KZ якобы позволяли «освоить профессию SMM-менеджера за 3 месяца» и «стать аналитиком данных».

На других сайтах потенциальные жертвы якобы могли ознакомиться с различными курсами. Среди них были курсы английского языка и получения навыков управления капиталом — от «платформ» EnglishPro и FinCourse соответственно:



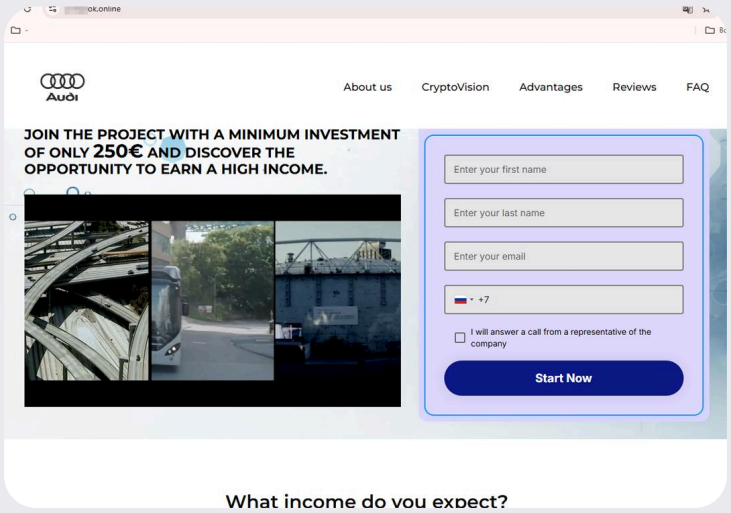


А мошеннический сайт некоего сервиса «Финансовое Образование» якобы мог помочь повысить финансовую грамотность — на нем посетителям предлагалось «освоить свои финансы и гарантировать свое будущее»:

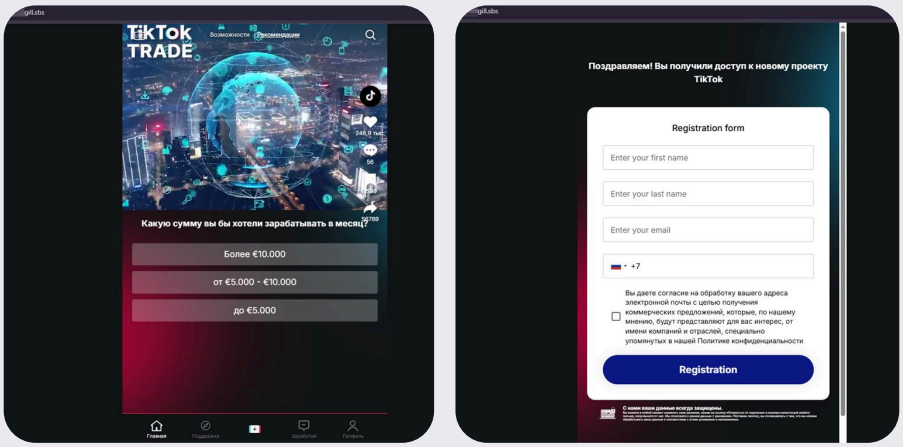


Для «доступа» к рекламируемым услугам такие сайты требуют регистрацию с указанием персональных данных — например, имени, номера мобильного телефона, адреса электронной почты и т. д. Они аккумулируются в руках злоумышленников и в дальнейшем могут использоваться в различных мошеннических схемах.

Вместе с тем появились новые мошеннические сайты псевдоинвестиционных проектов, которые киберпреступники часто преподносят как якобы имеющие отношение к известным компаниям и сервисам.

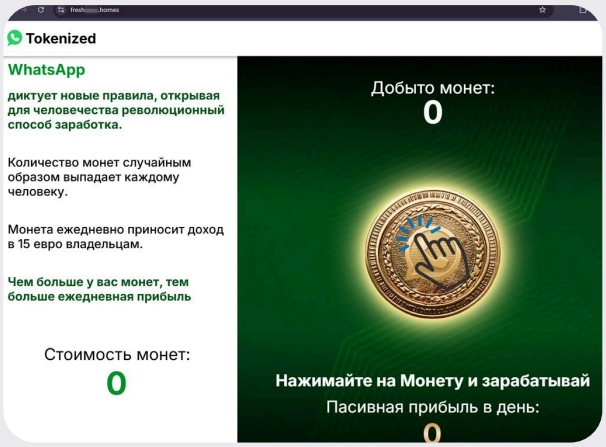


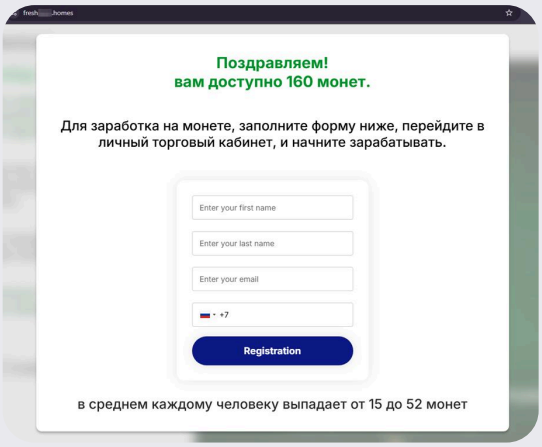
Например, на одном из них пользователям предлагали стать участниками инновационного проекта на основе технологий искусственного интеллекта. Этот ресурс выдавался за сервис автоконцерна Audi и якобы позволял в автоматическом режиме торговать криптовалютами и получать гарантированный высокий доход. Для «доступа» к сервису требовалось внести стартовую сумму в €250.



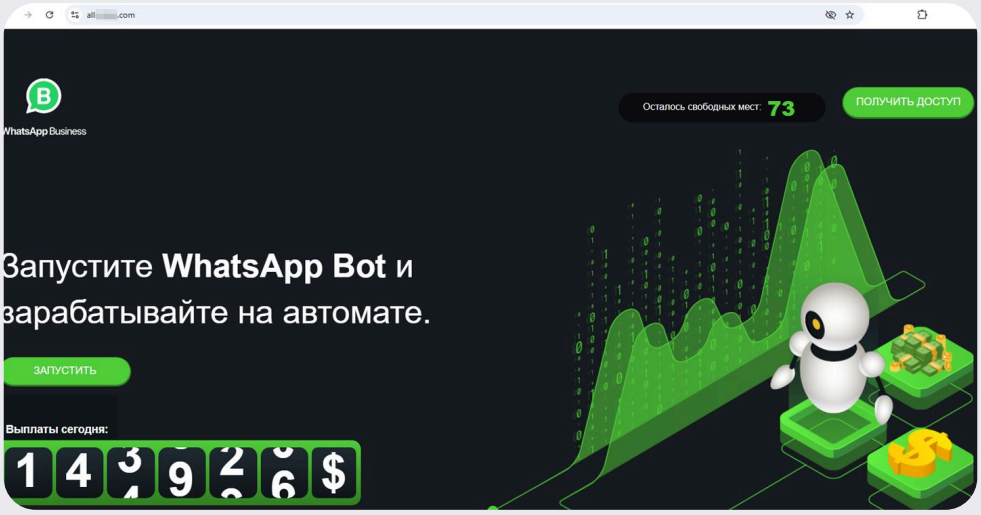
Другой «инвестиционный проект» якобы имел отношение к социальной сети TikTok. Посетителей мошеннического сайта просили пройти небольшой опрос, после чего указать персональные данные для регистрации и доступа к обещанному сервису.

Кроме того, были выявлены очередные мошеннические сайты, замаскированные под официальные веб-ресурсы мессенджера WhatsApp.



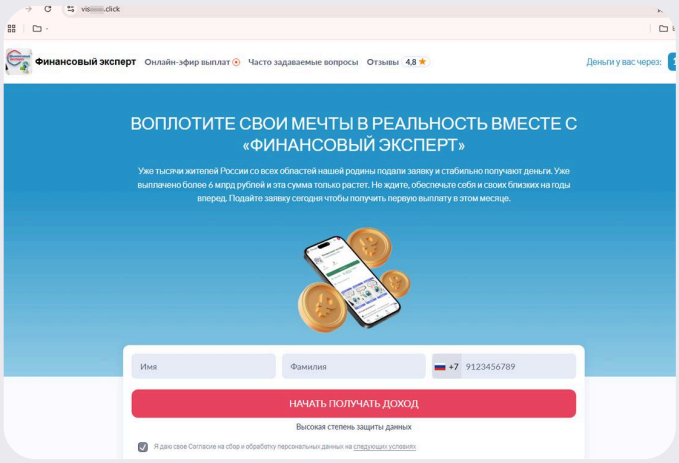


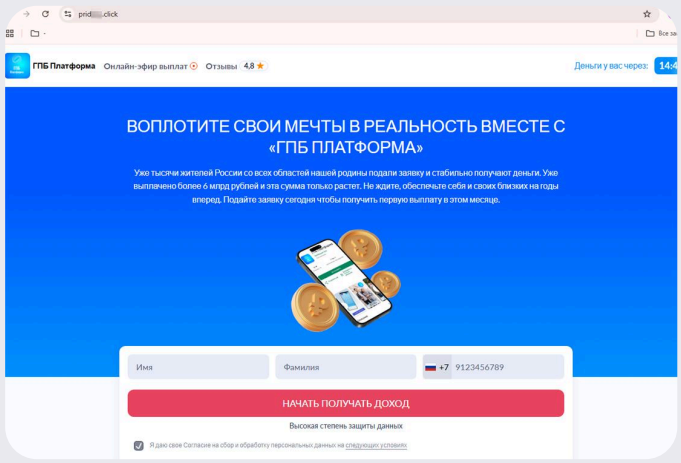
На одном из них посетителям предлагали получить цифровые монеты, каждая из которых «приносит владельцу €15 в день». Пользователю якобы становились доступны 160 таких монет, но чтобы тот начал «зарабатывать на них», ему требовалось зарегистрировать учетную запись, указав персональные данные. На самом деле никаких цифровых активов потенциальная жертва не получала, а ее данные оказывались у мошенников.



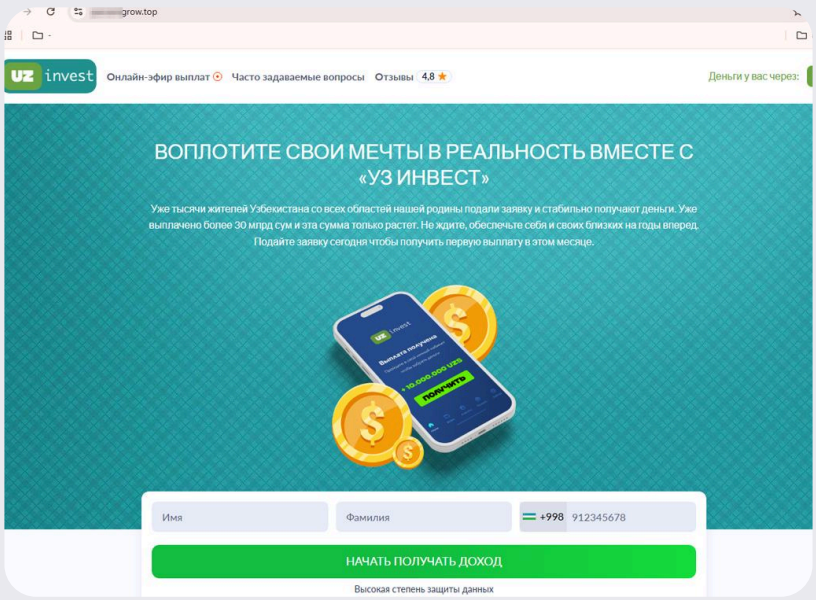
Еще один поддельный сайт WhatsApp якобы предоставлял доступ к очередному торговому боту, основанному на неких уникальных разработках. Пользователям рекомендовали «запустить WhatsApp Bot и зарабатывать на автомате». Для этого от них традиционно требовалась регистрация с указанием личных данных, которые затем передавались злоумышленникам.

Мошенники также нацеливались и на пользователей из определенных стран.



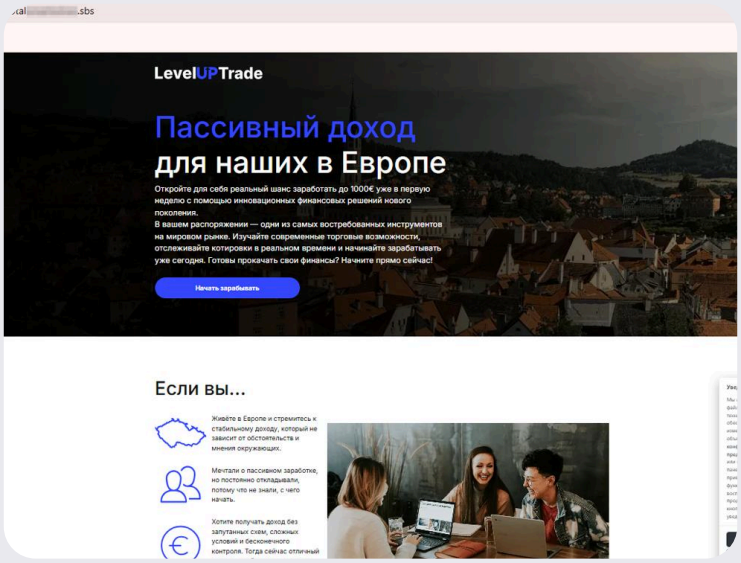


Например, жители России могли столкнуться с сайтами, предлагавшими «воплотить свои мечты в реальность» вместе с тем или иным инвестиционным сервисом. Злоумышленники использовали одинаковый шаблон для оформления таких ресурсов, меняя лишь их внешний вид, а также названия несуществующих площадок.

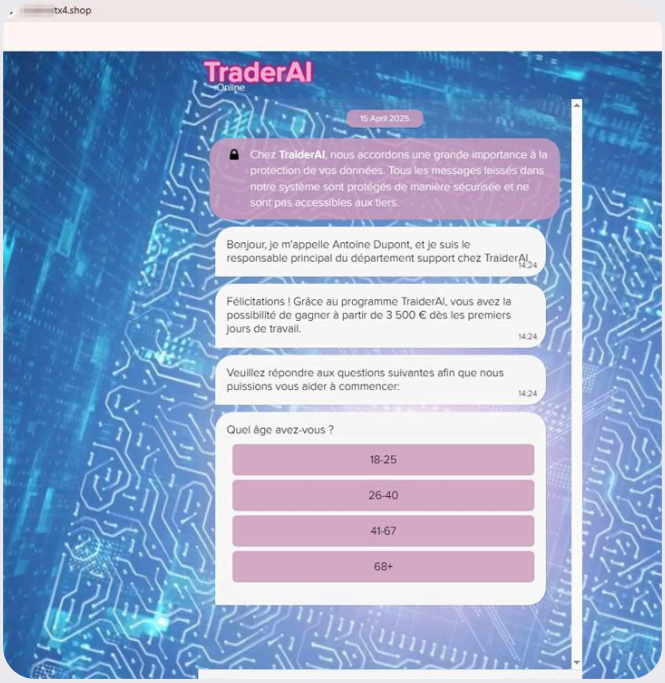


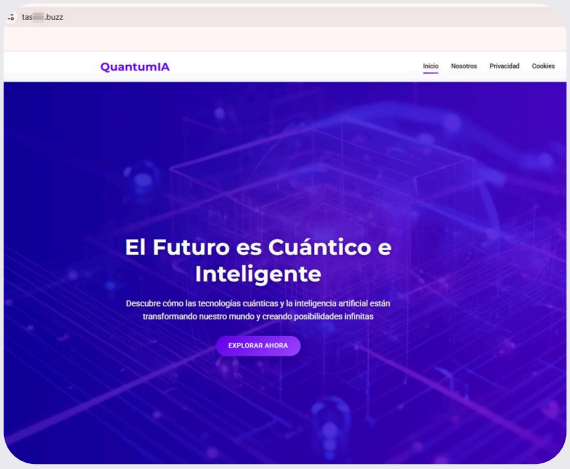
Примечательно, что сайты на основе такого же шаблона создавались и для жителей других государств — например, Узбекистана.

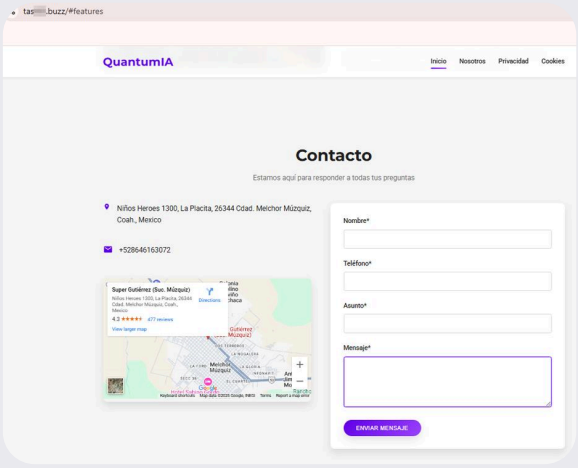
Один из выявленных мошеннических сайтов завлекал русскоязычных пользователей, проживающих в Европе. На нем киберпреступники обещали потенциальным жертвам пассивный доход до €1000 в неделю «с помощью инновационных финансовых решений нового поколения» от некой площадки LevelUPTrade:



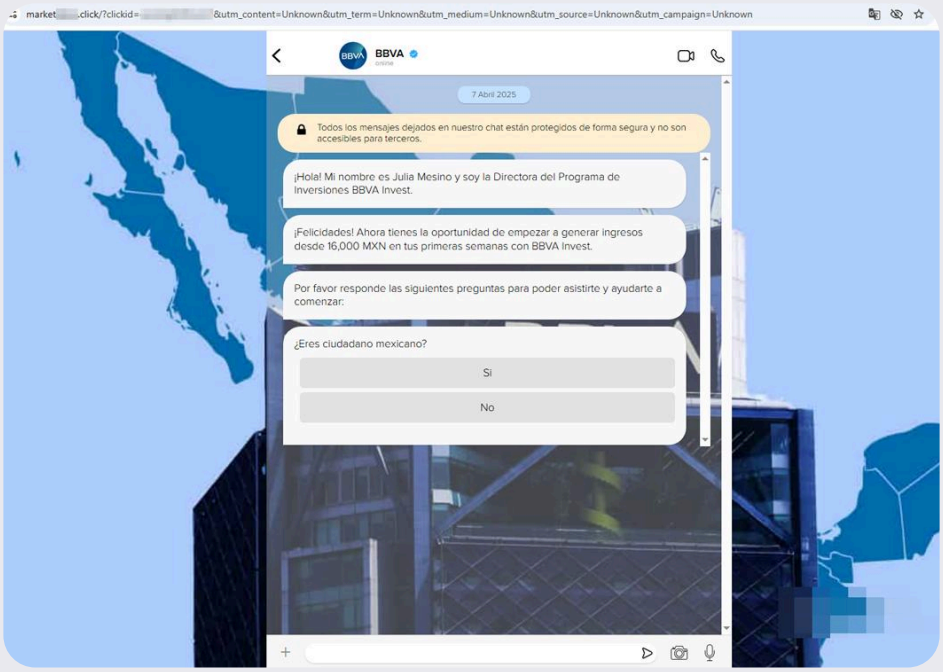
Пользователи из Франции могли стать жертвами злоумышленников, предлагавших доступ к несуществующему автоматизированному торговому ПО TraderAI. С его помощью потенциальные жертвы якобы имели возможность зарабатывать от €3500:





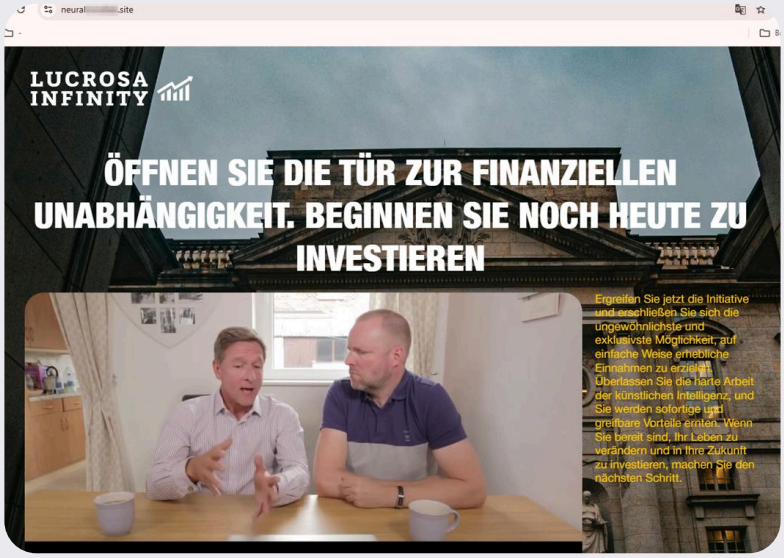


Для жителей Мексики мошенники также приготовили «интеллектуальную торговую систему» — QuantumIA. Это один из вариантов хорошо из вестной псевдоторговой системы Quantum System или QuantumAI, якобы позволяющей автоматически торговать на финансовых рынках с использованием квантовых вычислений и технологий искусственного интеллекта.

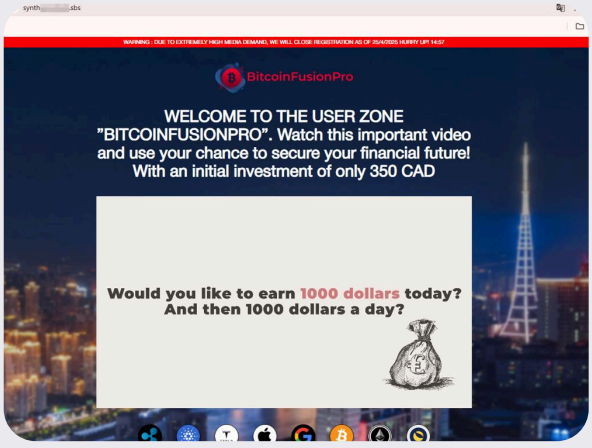


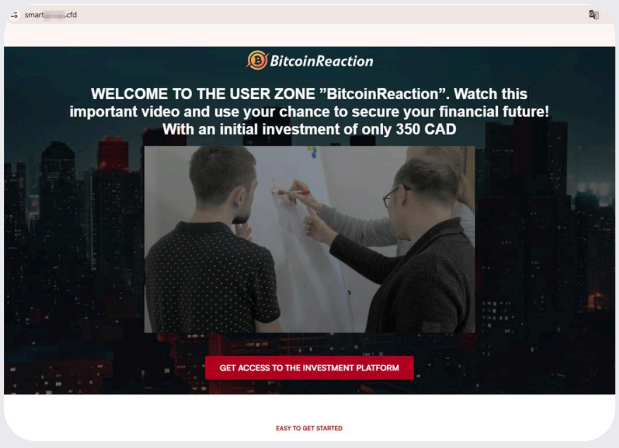
На другом сайте мошенники якобы от имени крупного банка предлагали мексиканским пользователям инвестиционные услуги — обещали шанс заработать 16 000 мексиканских песо в течение короткого срока после регистрации. Для этого нужно было указать свои персональные данные.

Германские пользователи рисковали стать жертвами поддельной торговой платформы Lucrosa Infinity, образ которой в том или ином виде киберпреступники эксплуатируют на протяжении нескольких лет. На одном из мошеннических сайтов злоумышленники предлагали «начать инвестировать и открыть дверь к финансовой независимости»:

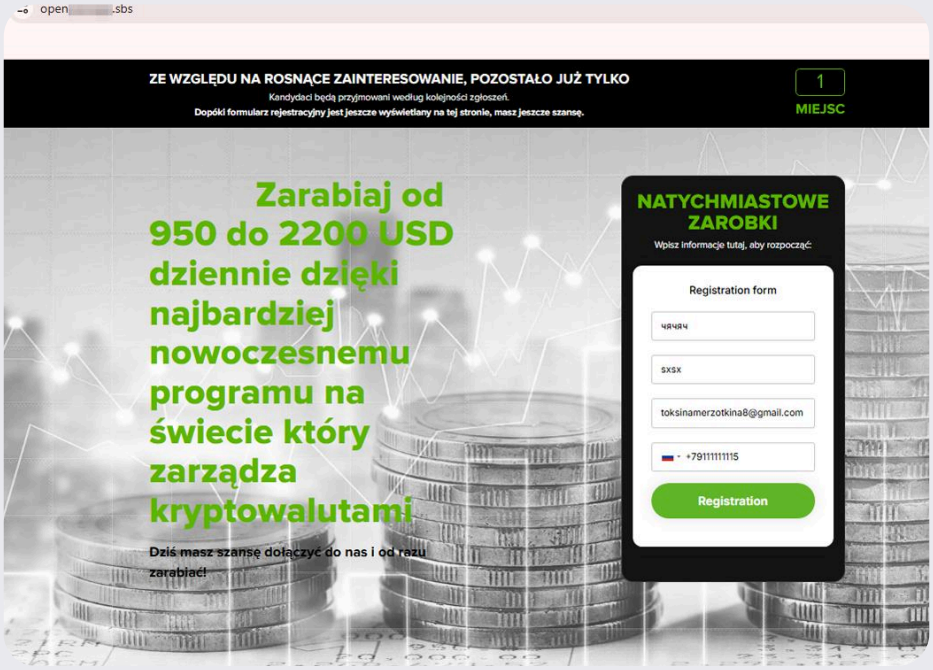


Жителям Канады киберпреступники также предлагали воспользоваться «уникальными» сервисами, якобы обеспечивающими высокий доход через инвестиции и торговлю криптовалютами. Например, выявленные мошеннические сайты рекламировали такие «платформы» как BitcoinFusionPro и BitcoinReaction. Они якобы давали возможность клиентам зарабатывать от 1000 канадских долларов в день, вложив «всего лишь» 350 долларов:

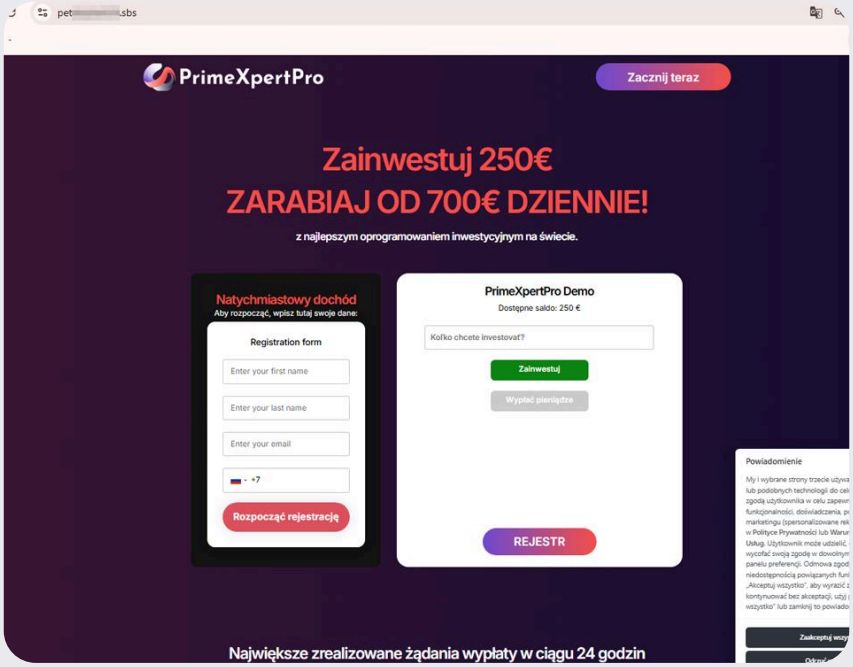




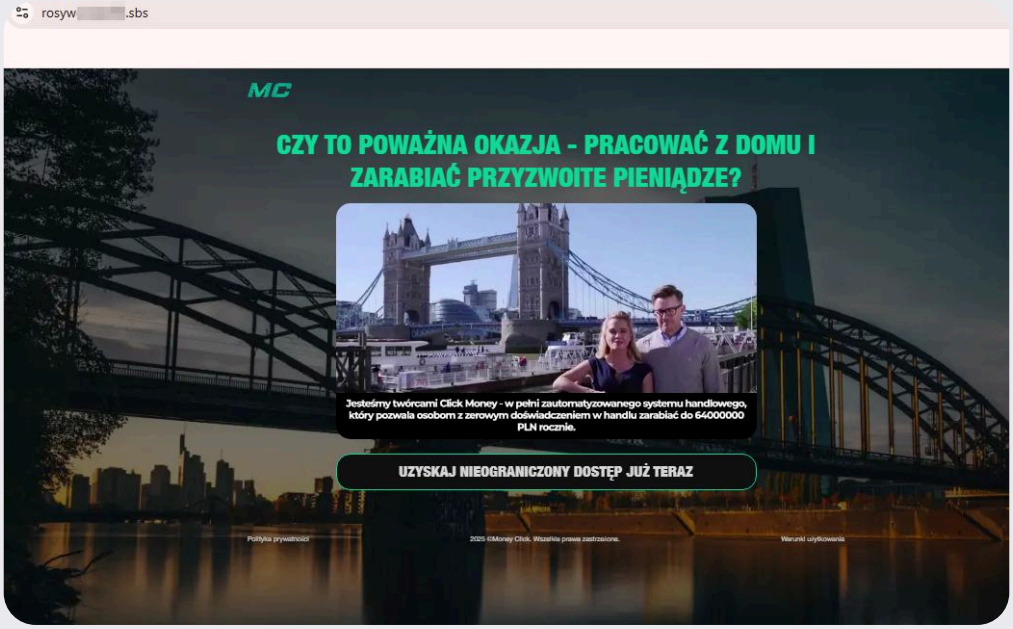
С похожими сайтами-подделками сталкивались и жители Польши. На одном из них мошенники обещали потенциальным жертвам, что те смогут зарабатывать от $950 до $2200 в день с «самым передовым программным обеспечением для управления криптовалютой в мире»:



Другой сайт предлагал инвестировать €250 и ежедневно зарабатывать уже €700:



Один из мошеннических ресурсов обещал польским пользователям «возможность работать из дома и зарабатывать приличные деньги» благодаря автоматизированной системе Click Money. С ее помощью люди без опыта торговли якобы могут получать до 64 000 000 польских злотых в год:



Вредоносное и нежелательное ПО для мобильных устройств

По данным статистики детектирований Dr.Web Security Space для мобильных устройств, во II квартале 2025 года наиболее часто на защищаемых устройствах обнаруживались рекламные трояны **Android.HiddenAds**. По сравнению с предыдущим кварталом пользователи сталкивались с ними несколько реже. Следом расположились рекламные трояны **Android.MobiDash** и вредоносные программы-подделки **Android.FakeApp**. При этом активность первых увеличилась, а вторых — снизилась.

Среди банковских троянов также наблюдалась разнонаправленная динамика. Например, было зафиксировано больше атак со стороны представителей семейства **Android.Banker**. В то же время трояны семейств **Android.BankBot** и **Android.SpyMax** детектировались на защищаемых устройствах реже.

Во II квартале в прошивках ряда моделей Android-смартфонов специалисты компании «Доктор Веб» обнаружили трояна **Android.Clipper.31**. Эта вредоносная программа скрывалась в модифицированной злоумышленниками версии мессенджера WhatsApp и использовалась для кражи криптовалют у владельцев зараженных устройств. Кроме того, наши вирусные аналитики выявили вредоносную программу **Android.Spy.1292.origin**. Киберпреступники внедрили ее в одну из версий картографического ПО Alpine Quest и с ее помощью шпионили за российскими военнослужащими.

За последние 3 месяца десятки угроз были найдены в каталоге Google Play. Среди них — вредоносные программы-подделки **Android.FakeApp** и новое нежелательное рекламное ПО **Adware.Adpush.21912**.

Наиболее заметные события, связанные с «мобильной» безопасностью во II квартале:

1. Снижение активности рекламных троянов
   Android.HiddenAds
2. Рост активности рекламных троянов
   Android.MobiDash
3. Участившиеся случаи детектирования банковских троянов
   Android.Banker
4. Снижение числа атак банковских троянов
   Android.BankBot и Android.SpyMax
5. Обнаружение трояна для кражи криптовалют, который скрывался в прошивках ряда моделей Android-смартфонов
6. Обнаружение трояна-шпиона, нацеленного на российских военнослужащих
7. Появление новых угроз в каталоге Google Play

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы

- Антивирусная правда
- Обучающие курсы
- Просветительные проекты

Пресс-центр

- Официальная информация
- Контакты для прессы
- Брошюры
- Галерея

Контакты

Центральный офис
125124, Россия, Москва, 3-я улица Ямского Поля, д.2, корп.12А

www.антивирус.рф
www.drweb.ru