Dr.WEB

«Доктор Веб»: обзор вирусной активности в III квартале 2025 года

Главное

Согласно статистике детектирований антивируса Dr.Web, в III квартале 2025 года общее число обнаруженных угроз снизилось на **4,23%** по сравнению со II кварталом. При этом количество уникальных угроз увеличилось на **2,17%**. Чаще всего на защищаемых устройствах обнаруживалось нежелательное рекламное ПО, рекламные трояны и вредоносные скрипты. В почтовом трафике преобладали вредоносные скрипты, бэкдоры, и различные троянские программы, такие как загрузчики, дропперы и похитители паролей.

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

Trojan.Encoder.35534 **Trojan.Encoder.35209** **Trojan.Encoder.35067**

Trojan.Scavenger

В июле эксперты компании «Доктор Веб» рассказали о семействе троянов **Trojan.Scavenger**, созданных для кражи криптовалюты и паролей. Злоумышленники распространяли их под видом модов, читов и патчей для игр. Эти трояны запускались с использованием легитимных приложений, в том числе через эксплуатацию в них уязвимостей класса DLL Search Order Hijacking.

Android.Backdoor.916.origin

В августе наши вирусные аналитики предупредили о распространении многофункционального бэкдора **Android.Backdoor.916.origin** для мобильных устройств, который был нацелен на представителей российского бизнеса. Киберпреступники управляли им дистанционно, похищая с его помощью конфиденциальные данные и следя за жертвами.

В этом же месяце антивирусная лаборатория «Доктор Веб» опубликовала исследование таргетированной атаки группировки Scaly Wolf на российское машиностроительное предприятие. Злоумышленники использовали целый ряд вредоносных инструментов, среди которых одним из основных стал модульный бэкдор Updatar. С его помощью атакующие пытались получить конфиденциальные данные с зараженных компьютеров.

В III квартале интернет-аналитики выявили очередные поддельные сайты месенджера Telegram, а также ряд мошеннических ресурсов финансовой тематики. Кроме того, в течение последних трех месяцев наши специалисты зафиксировали появление в каталоге Google Play десятков вредоносных и нежелательных приложений, среди которых были трояны **Android.Joker**, подписывающие пользователей на платные услуги, и программы-подделки **Android.FakeApp.**

Главные тенденции III квартала

Снижение числа угроз, выявленных на защищаемых устройствах

Рост числа уникальных угроз, атаковавших пользователей

Появление новых поддельных сайтов мессенджера Telegram и мошеннических интернет-ресурсов финансовой тематики

Распространение вредоносных приложений Trojan.Scavenger, похищавших криптовалюту и пароли

Использование бэкдора Android.Backdoor.916.origin для слежки за представителями российского бизнеса и кражи конфиденциальных данных

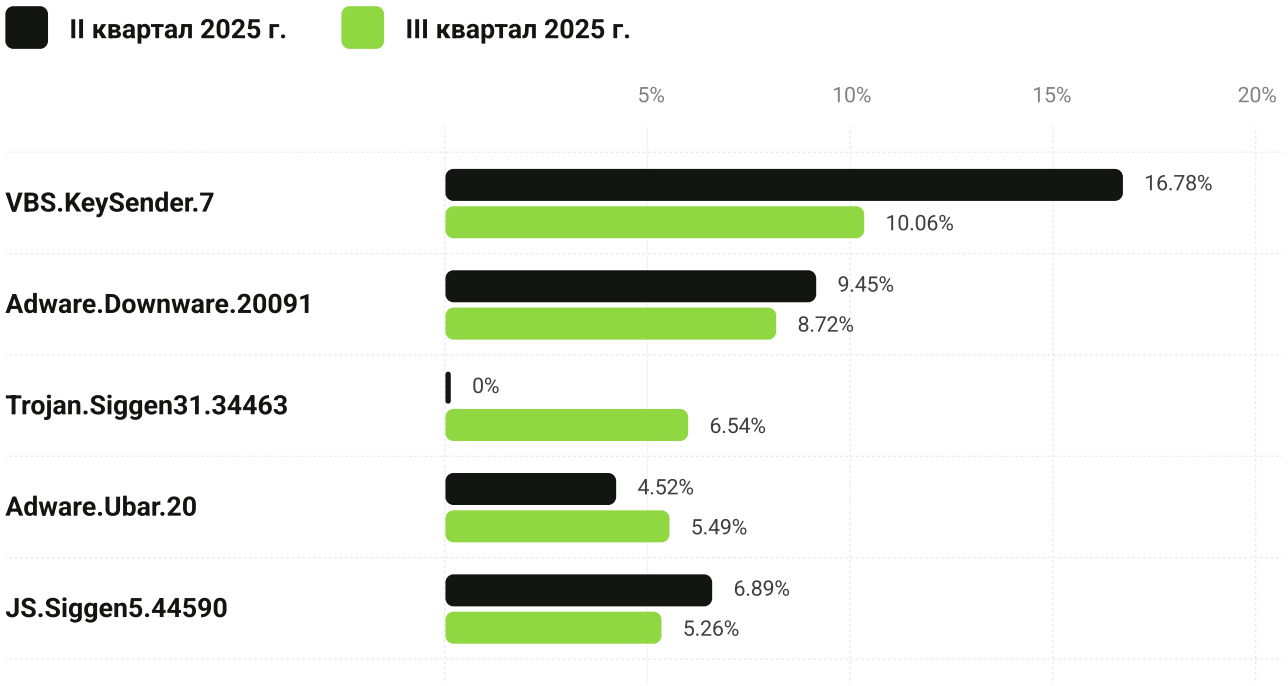
Рекламные трояны Android.MobiDash стали самой распространенной угрозой для Android-устройств

Снижение активности рекламных троянов Android.HiddenAds второй квартал подряд

Распространение множества угроз в каталоге Google Play

По данным сервиса статистики «Доктор Веб»

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



VBS.KeySender.7

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.Siggen31.34463

Троян, написанный на языке программирования Go и предназначенный для загрузки в целевую систему различных майнеров и рекламного ПО. Вредоносная программа является DLL-файлом и располагается в %appdata%\utorrent\lib.dll. Для своего запуска эксплуатирует уязвимость класса DLL Search Order Hijacking в торрент-клиенте uTorrent.

Adware.Ubar.20

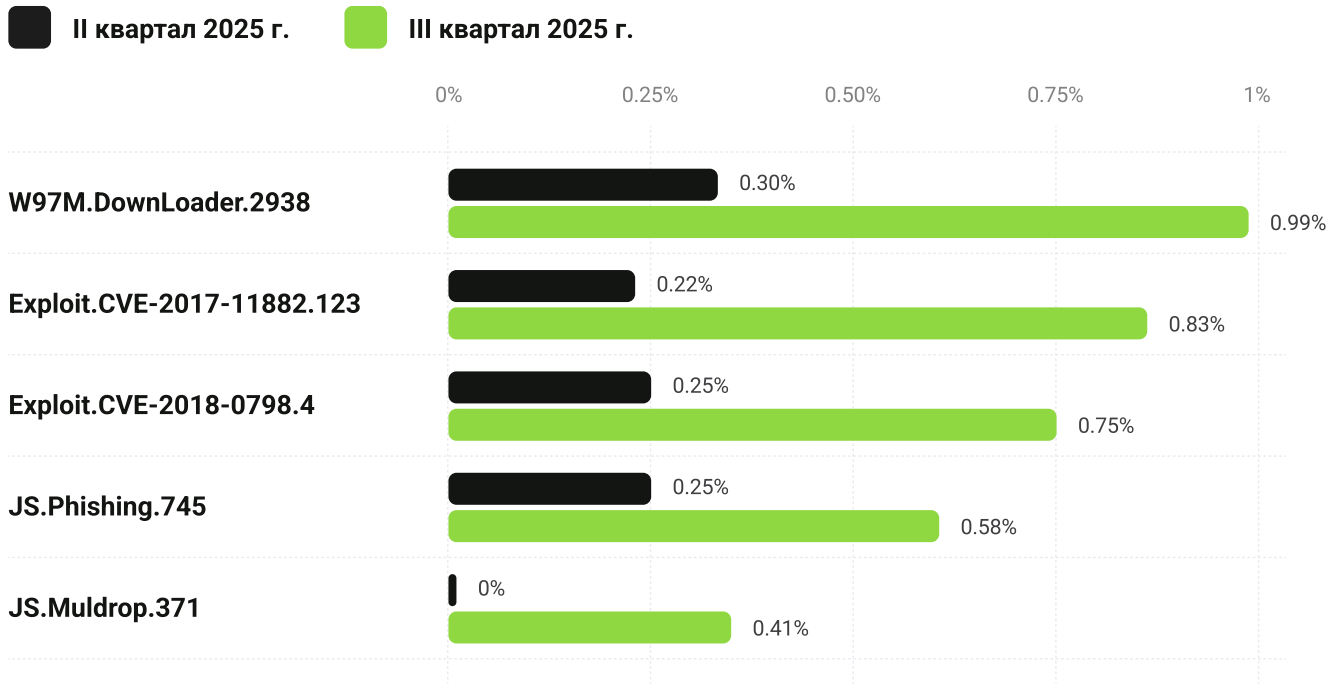
Торрент-клиент, устанавливающий нежелательное ПО на устройство.

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.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике



W97M.DownLoader.2938

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

Exploit.CVE-2017-11882.123 **Exploit.CVE-2018-0798.4**

Эксплойты для использования уязвимостей в ПО Microsoft Office, позволяющие выполнить произвольный код.

JS.Phishing.745

Вредоносный сценарий на языке JavaScript, формирующий фишинговую веб-страницу.

JS.Muldrop.371

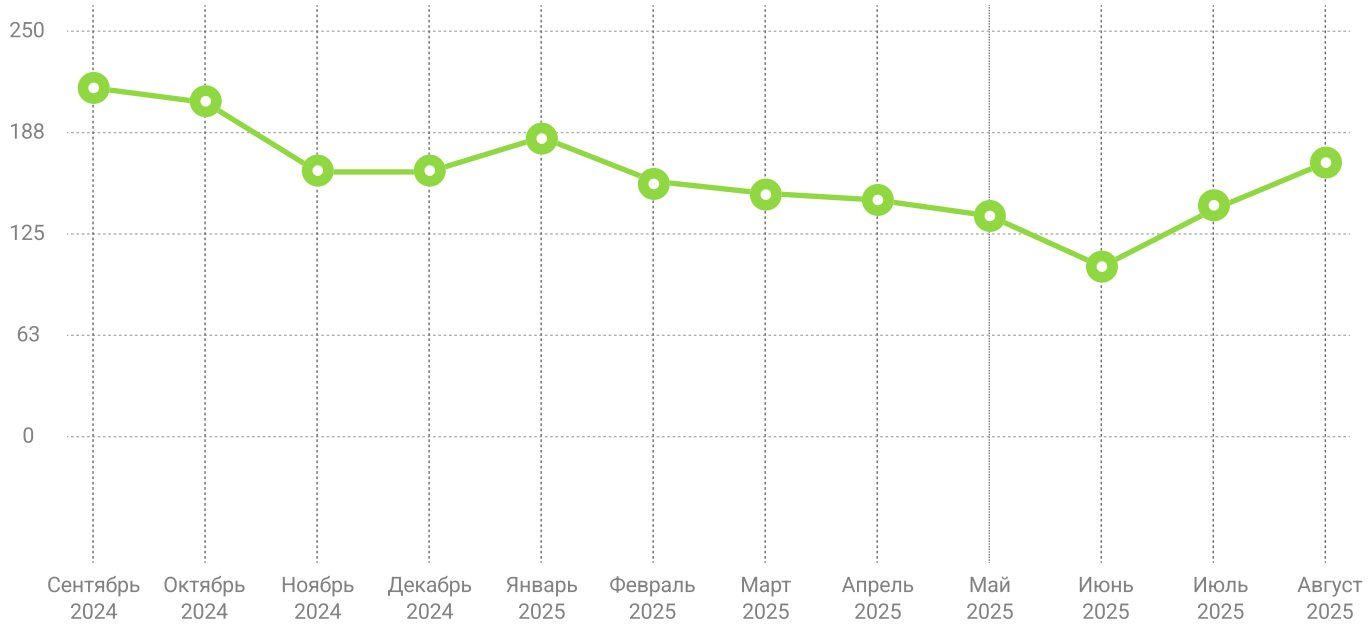
Вредоносный сценарий на языке JavaScript, устанавливающий в систему полезную нагрузку.

Шифровальщики

В III квартале 2025 года число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, выросло на **3,02%** по сравнению со II кварталом.

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

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

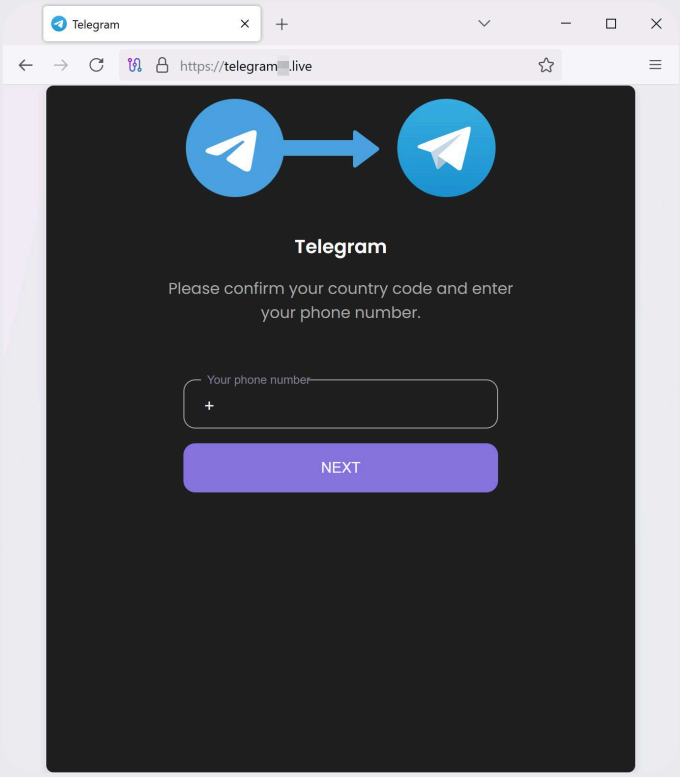


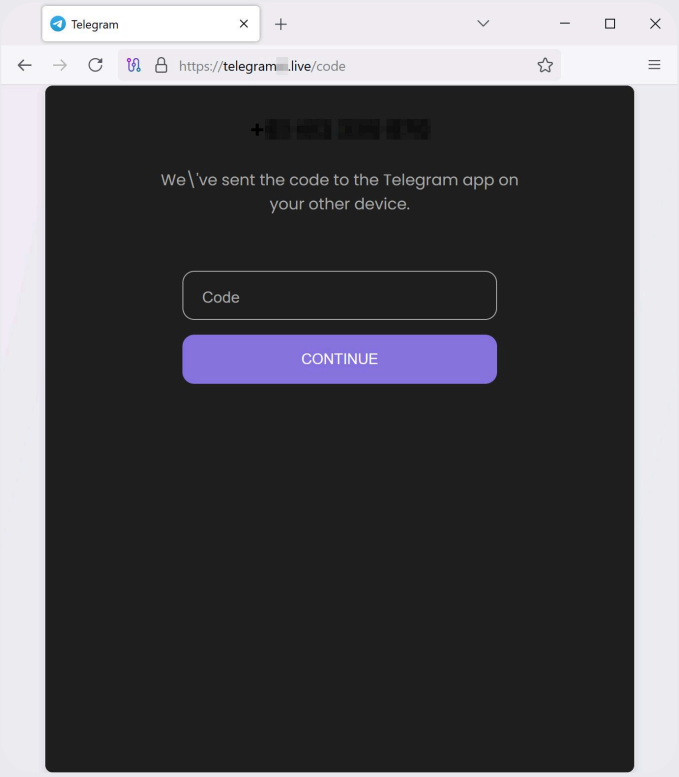
Наиболее распространенные энкодеры III квартала 2025 года:

1. Trojan.Encoder.35534 — 26.99% обращений пользователей
2. Trojan.Encoder.35209 — 3.07% обращений пользователей
3. Trojan.Encoder.35067 — 2.76% обращений пользователей
4. Trojan.Encoder.41542 — 2.15% обращений пользователей
5. Trojan.Encoder.29750 — 1.84 % обращений пользователей

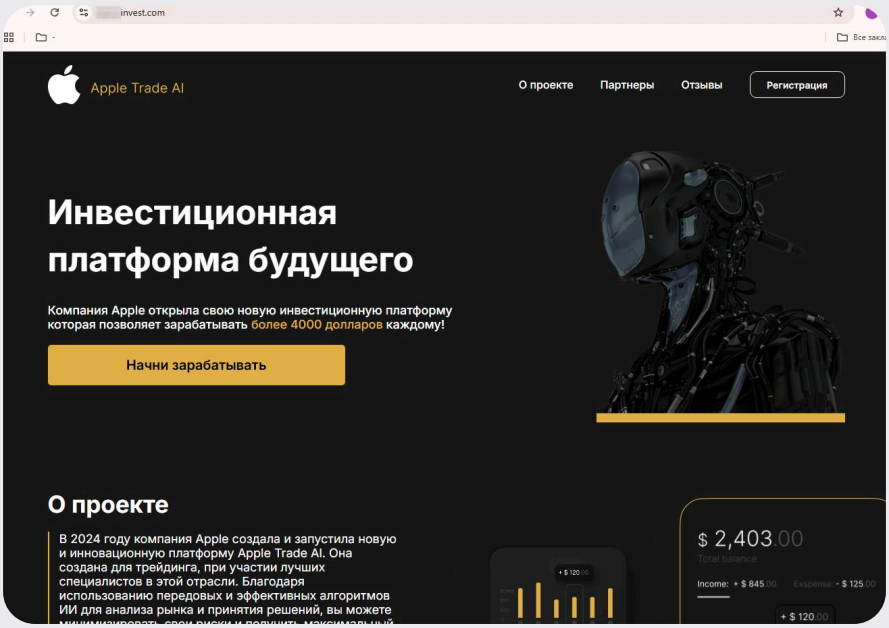
Сетевое мошенничество

В III квартале 2025 года интернет-аналитики «Доктор Веб» продолжили фиксировать появление поддельных сайтов мессенджера Telegram — в том числе тех, с помощью которых мошенники пытались получить доступ к учетным записям пользователей:

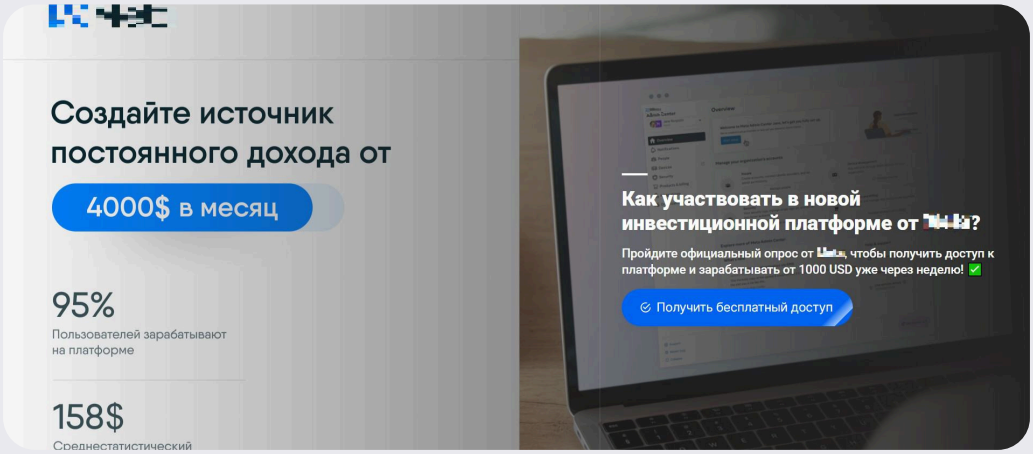




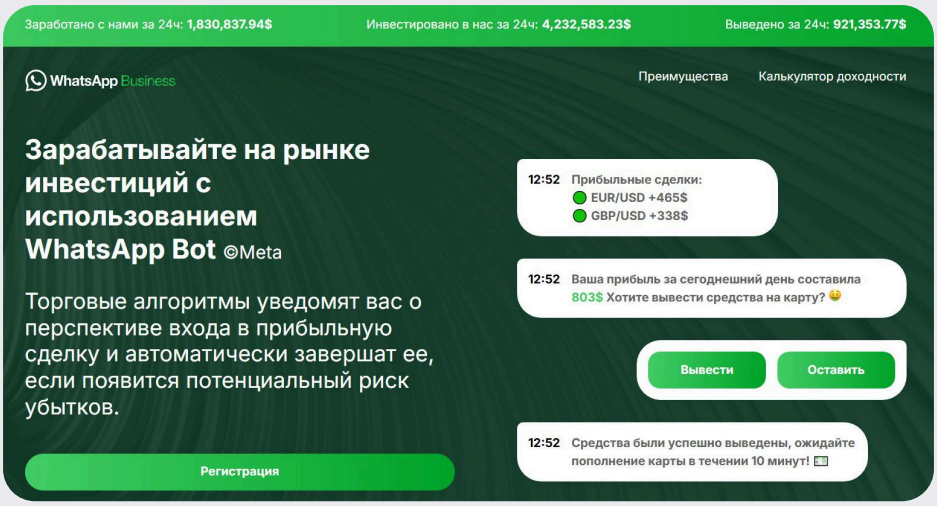
Кроме того, распространение вновь получили мошеннические сайты финансовой тематики. Один из них заманивал пользователей на «инвестиционную платформу будущего» Apple Trade AI, якобы созданную корпорацией Apple. Киберпреступники обещали потенциальным жертвам возможность зарабатывать более $4000 в месяц, а для «доступа» к сервису требовали зарегистрироваться, предоставив личную информацию.



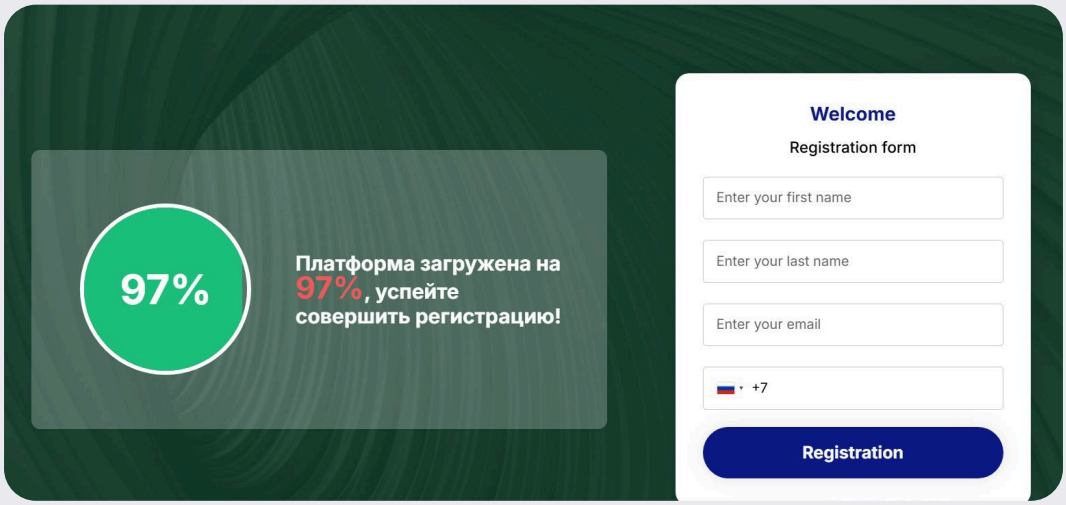
Другие интернет-ресурсы предлагали принять участие «в новой инвестиционной платформе от Meta» и «создать источник постоянного дохода от $4000 в месяц» (Meta признана экстремисткой организацией в Российской Федерации и запрещена). Чтобы получить доступ к «платформе», посетители таких сайтов должны были пройти опрос и регистрацию.



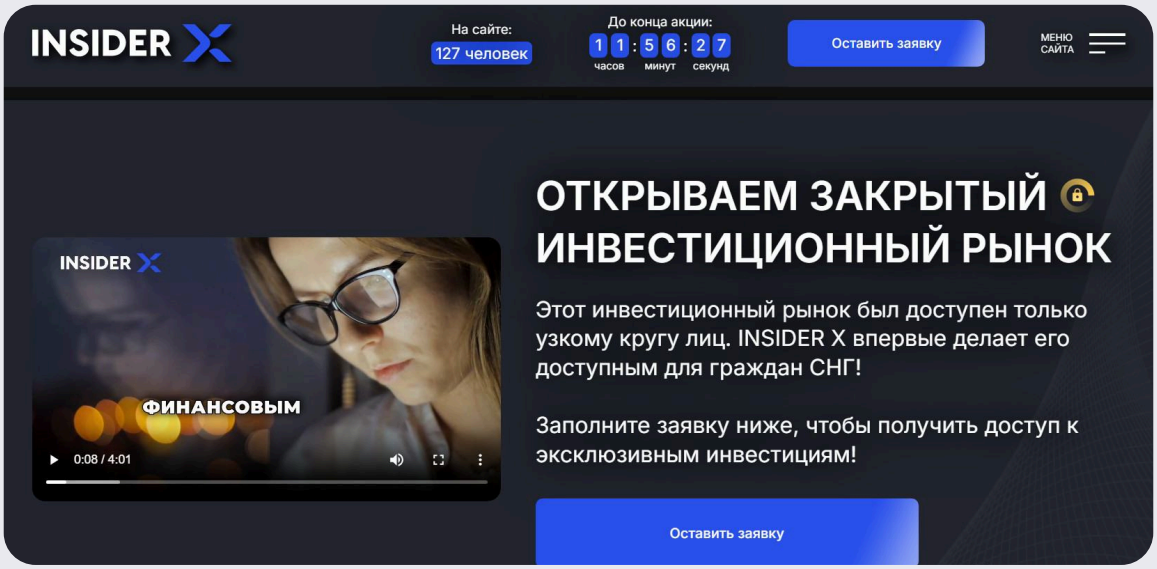
Наши эксперты выявили и очередные варианты поддельных инвестиционных платформ, якобы позволяющих зарабатывать при помощи торговых ботов в WhatsApp.



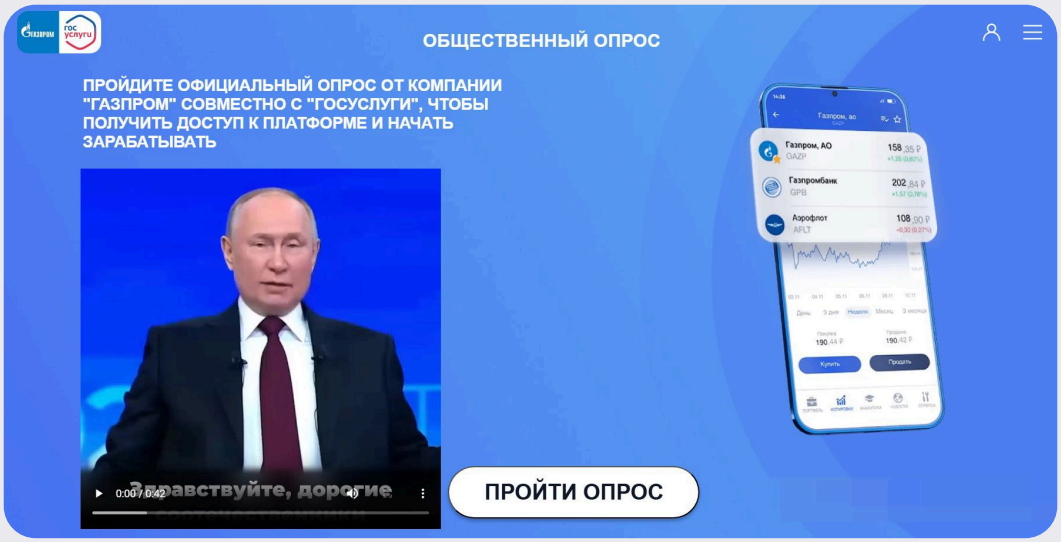
Для «работы» с обещанными сервисами у потенциальных жертв запрашивались персональные данные:



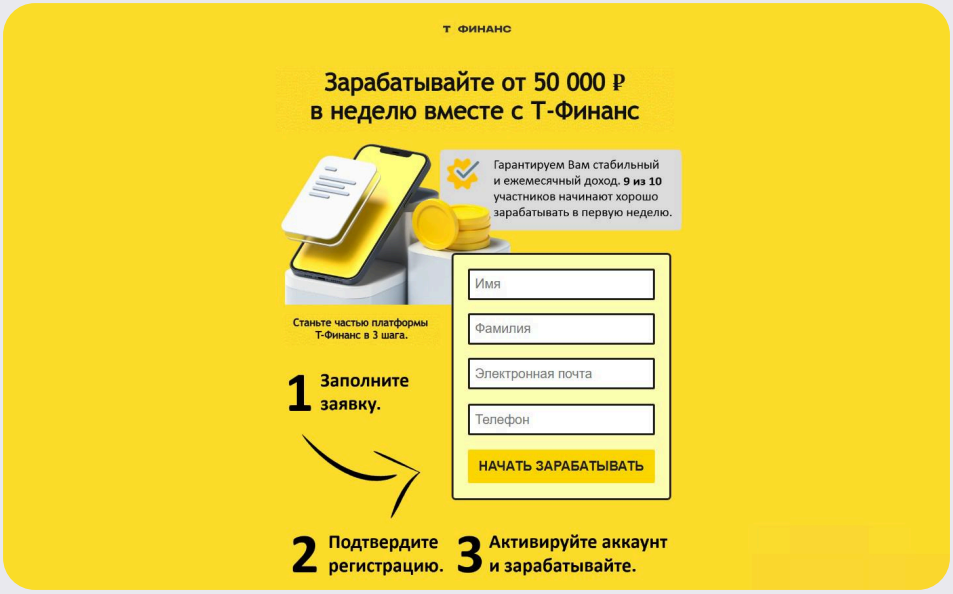
Ряд мошеннических сайтов был ориентирован на аудиторию в определенных странах. Некоторые из них были нацелены на пользователей из СНГ, которым злоумышленники предлагали «открыть закрытый инвестиционный рынок» и получить доступ к неким эксклюзивным инвестициям через финансовый сервис INSIDER X. Для этого посетители должны были «оставить заявку», указав персональные данные.



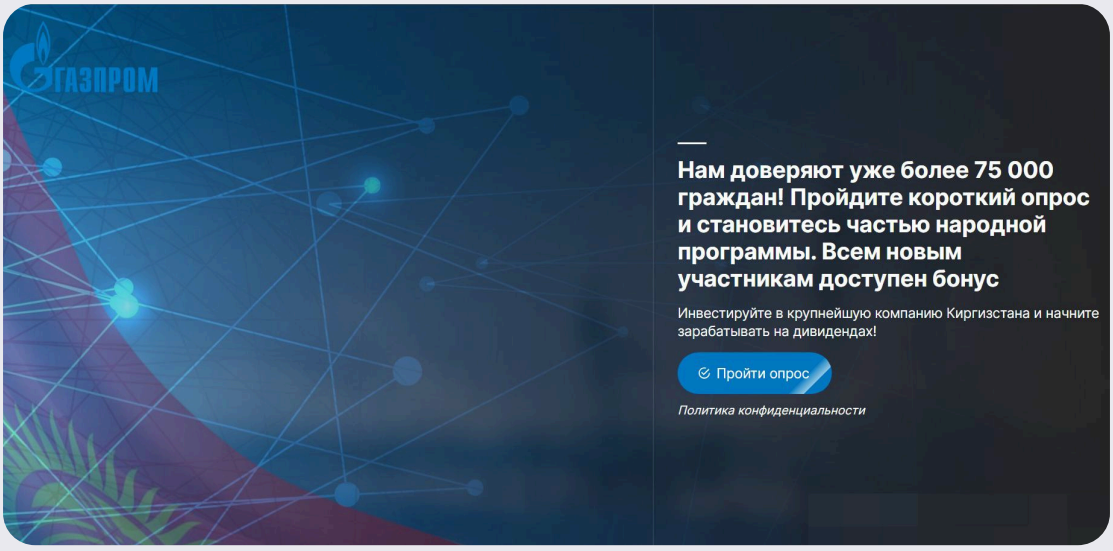
В одной из схем, предназначенных для российских пользователей, злоумышленники предлагали пройти опрос и получить доступ к «инвестиционной платформе», якобы имеющей отношение к крупным нефтегазовым компаниям и государственному порталу Госуслуги:



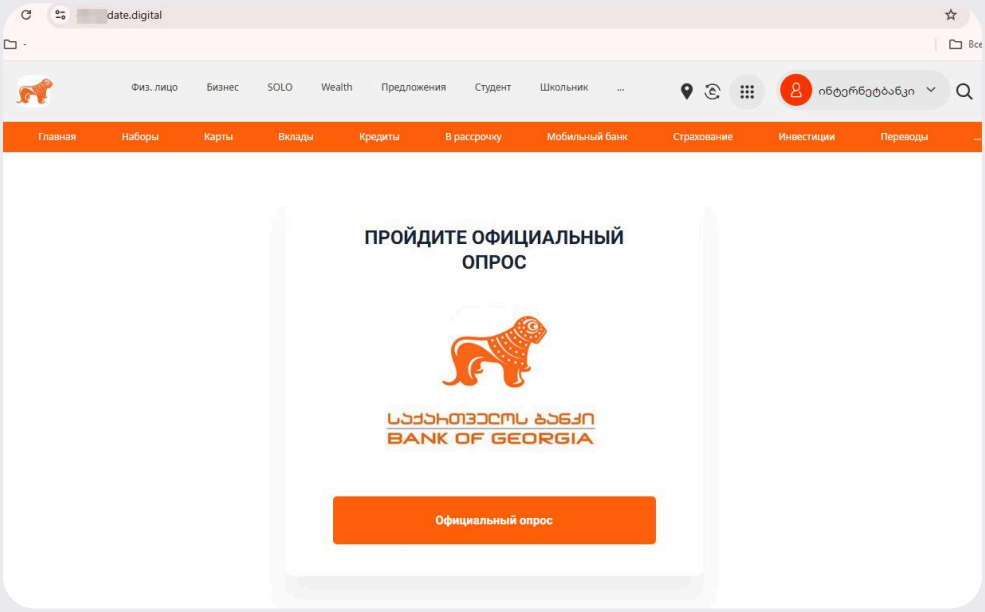
Другие сайты мошенники выдавали за настоящие сервисы российских банков и предлагали зарегистрироваться, чтобы «зарабатывать от 50 000 рублей в неделю»:



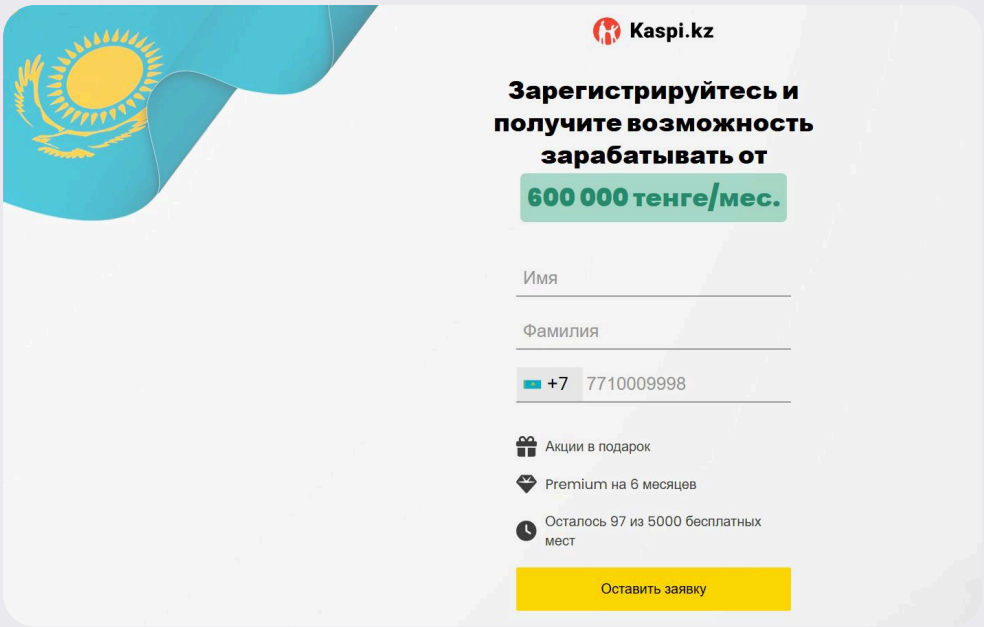
С похожими подделками вновь сталкивались жители ряда других государств. На одном из сайтов пользователям из Киргизии мошенники предлагали стать частью народной программы и инвестировать в крупнейшую, по их словам, компанию страны:

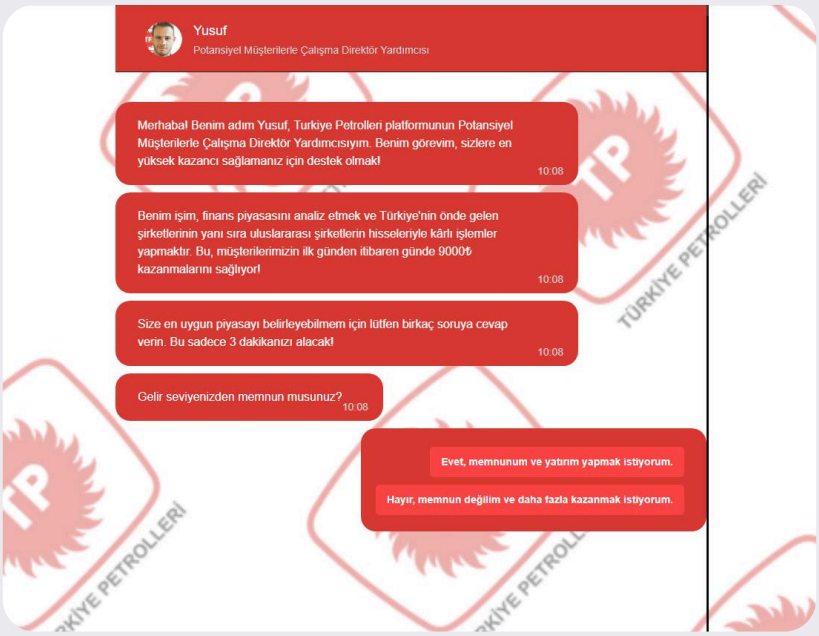


Другой якобы имел отношение к одному из банков Грузии и позволял присоединиться к его «инвестиционной платформе»:

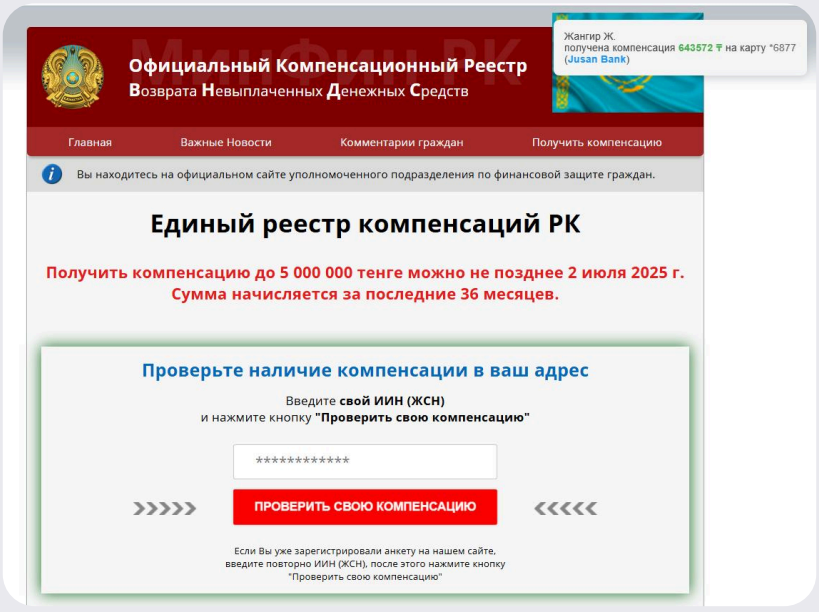


Похожий поддельный сайт мошенники выдавали за принадлежащий одному из казахстанских банков и обещали пользователям доход от 600 000 тенге в месяц:





На одном из интернет-ресурсов злоумышленники якобы от имени турецкой нефтегазовой компании предлагали потенциальным жертвам стать участниками инвестиционной платформы и зарабатывать «до 9000 турецких лир в день».



Вместе с тем мошенники продолжили эксплуатировать тематику всевозможных государственных выплат и компенсаций. На одном из нежелательных сайтов, ориентированных на пользователей из Казахстана, посетители якобы могли проверить наличие денежной компенсации и получить до 5 000 000 тенге.

Вредоносное и нежелательное ПО для мобильных устройств

По данным статистики детектирований Dr.Web Security Space для мобильных устройств, в III квартале 2025 года пользователи чаще всего сталкивались с рекламными троянами **Android.MobiDash**. При этом лидировавшие ранее трояны **Android.HiddenAds** опустились на второе место, существенно снизив активность. Третьими по распространенности стали вредоносные программы-подделки **Android.FakeApp.**

По сравнению со II кварталом число детектирований банковских троянов **Android.BankBot** увеличилось, а троянов **Android.Banker** и **Android.SpyMax** — уменьшилось.

В августе эксперты компании «Доктор Веб» рассказали о многофункциональном бэкдоре **Android.Backdoor.916.origin**, которого злоумышленники использовали для кражи конфиденциальных данных и слежки за представителями российского бизнеса.

За минувшие 3 месяца в каталоге Google Play было выявлено свыше 70 вредоносных и нежелательных программ. Среди них — трояны **Android.Joker**, которые подписывают пользователей на платные услуги, программы-подделки **Android.FakeApp** и ПО **Program.FakeMoney.16**, якобы позволявшее конвертировать виртуальные награды в настоящие деньги.

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

1. Рост активности рекламных троянов
   Android.MobiDash
2. Снижение активности рекламных троянов
   Android.HiddenAds
3. Возросшая активность банковских троянов
   Android.BankBot
4. Снижение числа атак банковских троянов
   Android.Banker и Android.SpyMax
5. Использование злоумышленниками многофункционального бэкдора для слежки за представителями российского бизнеса
   Android.Backdoor.916.origin
6. Распространение множества 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