Dr.WEB

«Доктор Веб»: обзор вирусной активности в IV квартале 2024 года

Статистика

Согласно статистике детектирований антивируса Dr.Web, в IV квартале 2024 года общее число обнаруженных угроз снизилось на **1,53%** по сравнению с **III** кварталом. При этом число уникальных угроз увеличилось на **94,43%**. Чаще всего детектировались рекламные приложения и рекламные трояны, вредоносные скрипты, а также трояны, распространяющиеся в составе других вредоносных приложений и применяющиеся для затруднения их обнаружения. В почтовом трафике наиболее часто выявлялись вредоносные скрипты, рекламные трояны и трояны-майнеры. Кроме того, отмечалась повышенная активность вредоносных программ со шпионской функциональностью.

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

Trojan.Encoder.35534 **Trojan.Encoder.35067** **Trojan.Encoder.26996**

На Anroid-устройствах самыми распространенными угрозами вновь стали рекламные трояны **Android.HiddenAds.**
В то же время наши вирусные аналитики выявили в каталоге Google Play множество новых вредоносных программ.

Главные тенденции IV квартала

Реклама

Рекламные приложения и рекламные трояны остались лидерами по числу детектирований

Новые угрозы

Уникальных угроз по сравнению с предыдущим кварталом стало больше

Почта

Повышенная активность троянских программ-шпионов в почтовом трафике

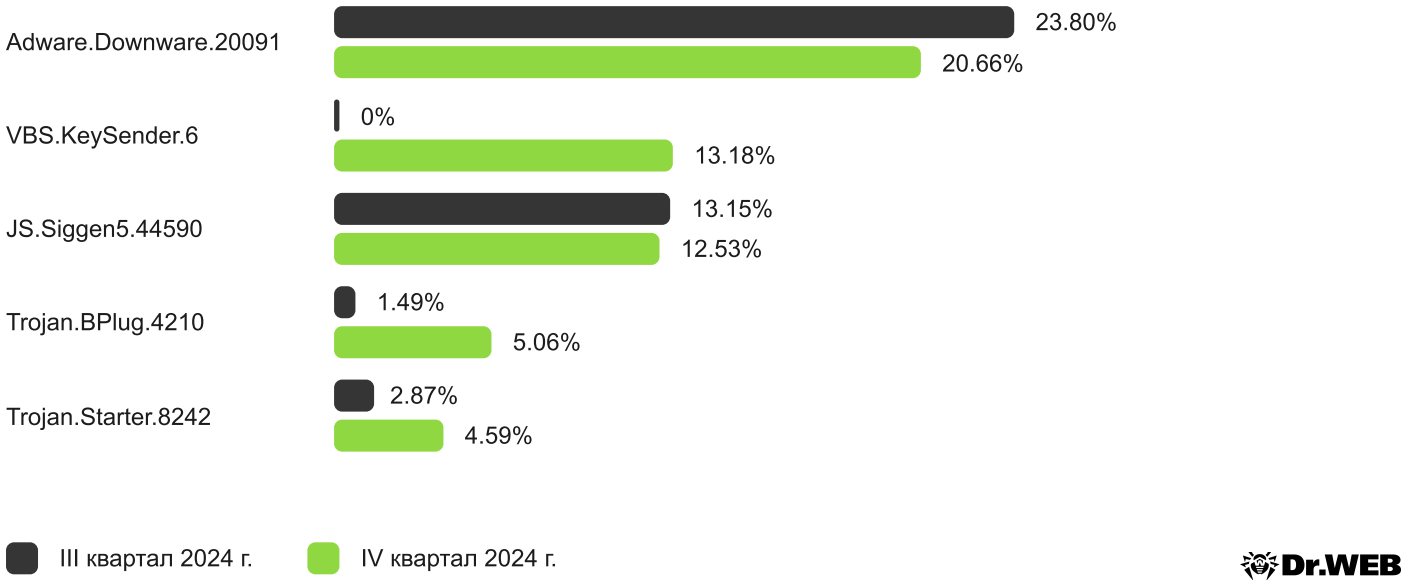
Google Play

Распространение множества троянских программ через Google Play

По данным сервиса статистики «Доктор Веб»

Наиболее распространенное

рекламное и вредоносное ПО согласно данным сервиса статистики



Adware.Downware.20091

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

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.

Trojan.Starter.8242

Вредоносная программа, обеспечивающая запуск трояна-майнера.

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.

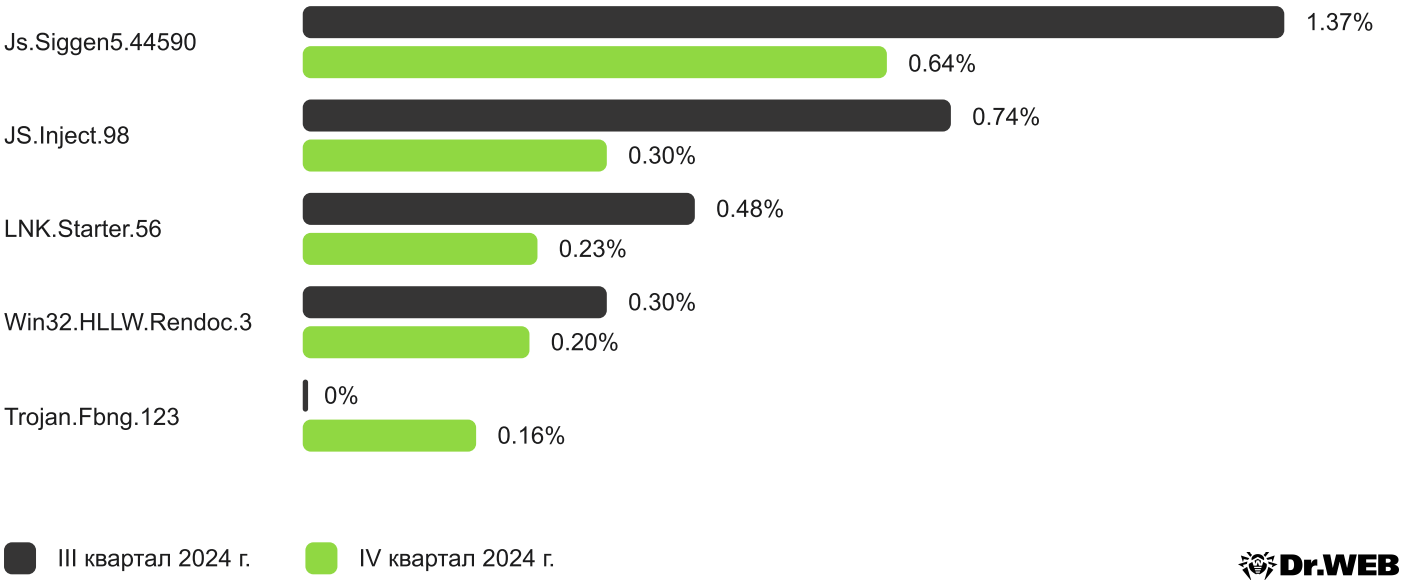
Trojan.BPlug.4210

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

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.

LNK.Starter.56

Детектирование специальным образом сформированного ярлыка, который распространяется через съемные накопители и для введения пользователей в заблуждение имеет значок диска. При его открытии происходит запуск вредоносных VBS-скриптов из скрытого каталога, расположенного на том же носителе, что и сам ярлык.

Win32.HLLW.Rendoc.3

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

Trojan.Fbng.123

Троянская программа-шпион, также известная как Formbook. Предназначена для кражи различных данных с зараженных устройств. Она похищает сохраненные пароли в браузерах, email-клиентах, онлайн-мессенджерах и другом ПО, перехватывает вводимые данные в веб-формах, отслеживает нажатия на клавиатуре (реализует функцию кейлоггера), создает скриншоты. Кроме того, она способна загружать и запускать другие программы, а также выполнять различные команды злоумышленников, работая как бэкдор.

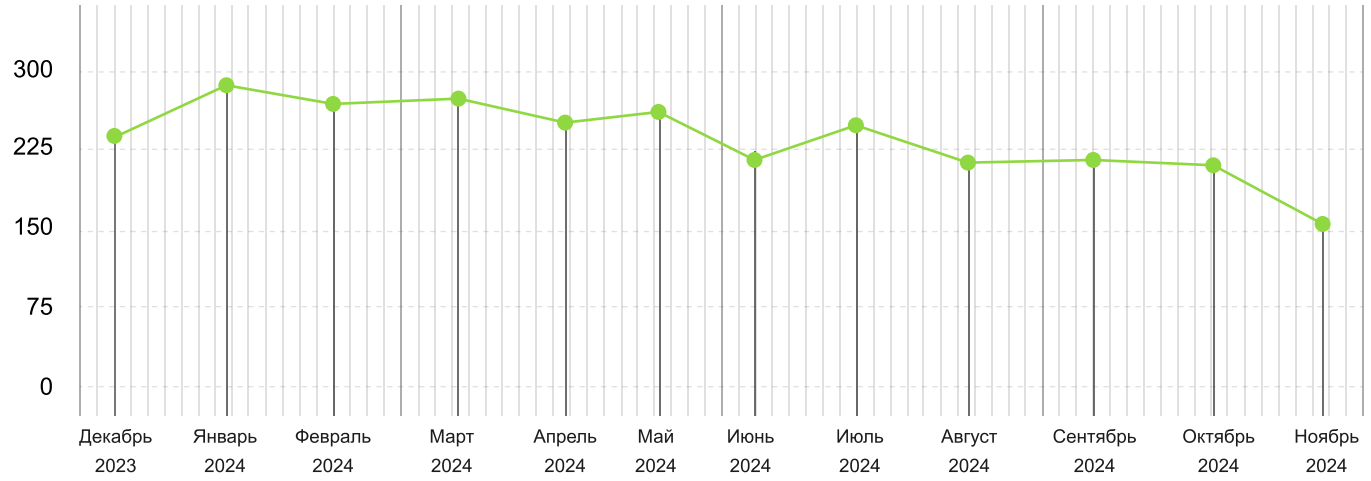
Шифровальщики

В IV квартале 2024 года число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, снизилось на 18,96% по сравнению с III кварталом.

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

Количество запросов

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

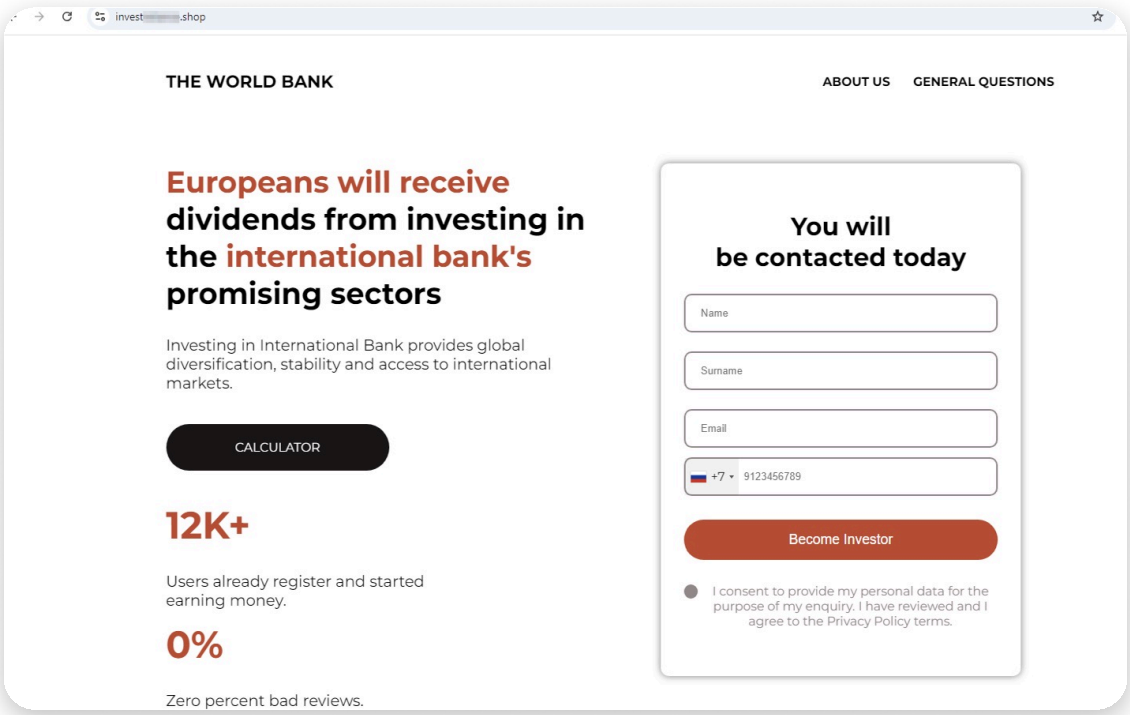


Наиболее распространенные энкодеры IV квартала:

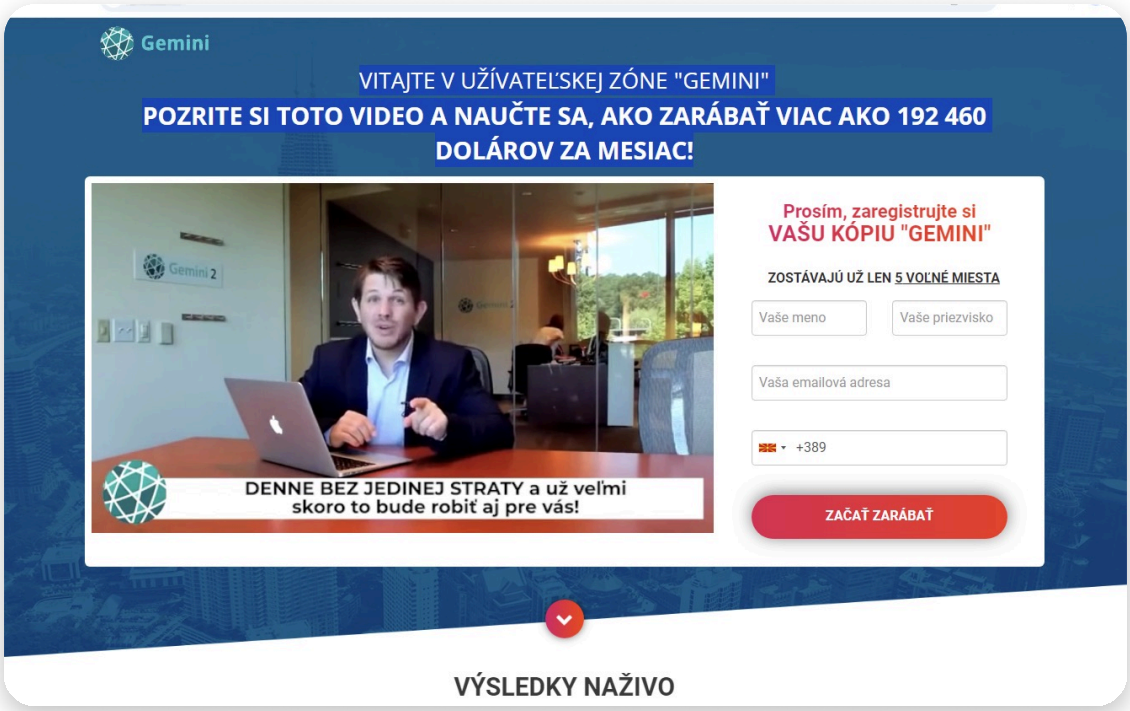
22.63%	**3.91%**	**3.35%**	**3.07%**	**3.07%**
Trojan.Encoder.35534	Trojan.Encoder.35067	Trojan.Encoder.26996	Trojan.Encoder.35209	Trojan.Encoder.38200

Сетевое мошенничество

В IV квартале 2024 года актуальной осталась мошенническая схема, в которой злоумышленники на специально созданных сайтах предлагали потенциальным жертвам заработать с помощью различных инвестиций. Для «доступа» к инвестиционным сервисам у пользователей запрашивается регистрация с указанием персональных данных, которые затем оказываются в руках мошенников. С такими сайтами сталкивались жители различных стран.

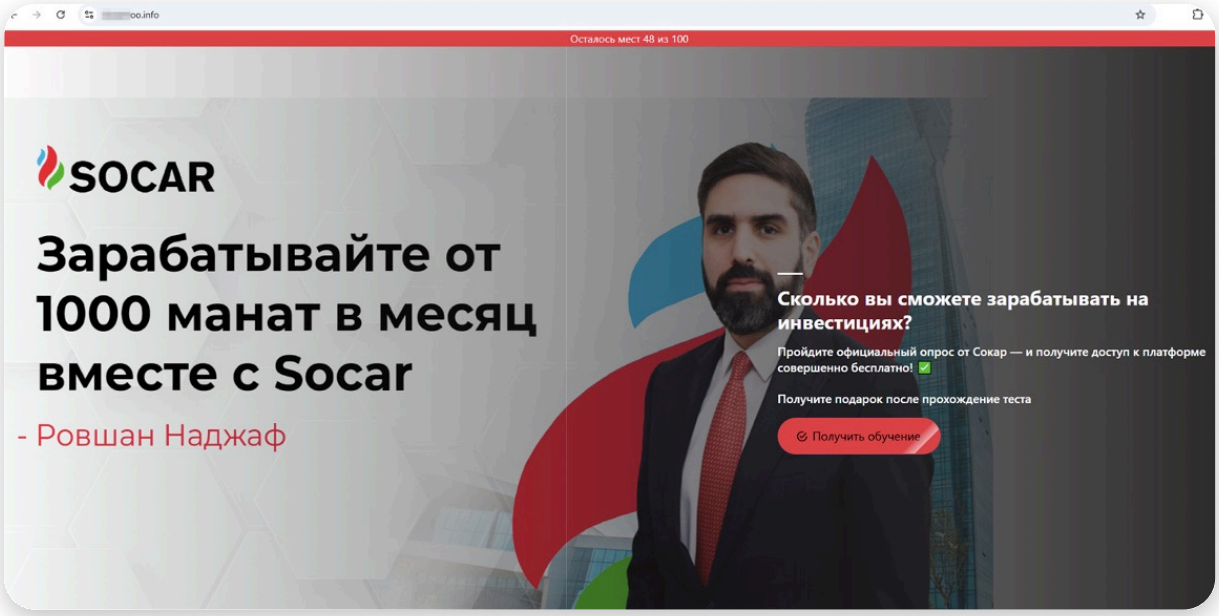


Мошеннический сайт, якобы имеющий отношение к Всемирному банку, обещает европейцам дивиденды за инвестирование в перспективные секторы экономики

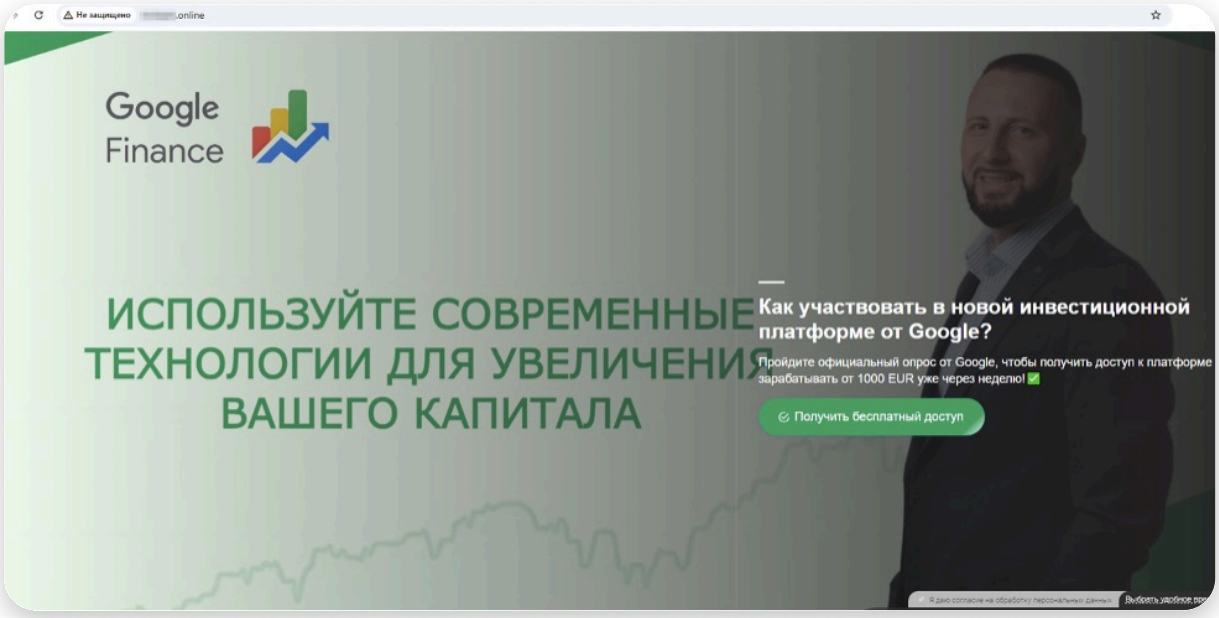


Мошеннический сайт предлагает словацким пользователям «заработать более $192 460 в месяц» с помощью некоего инвестиционного сервиса

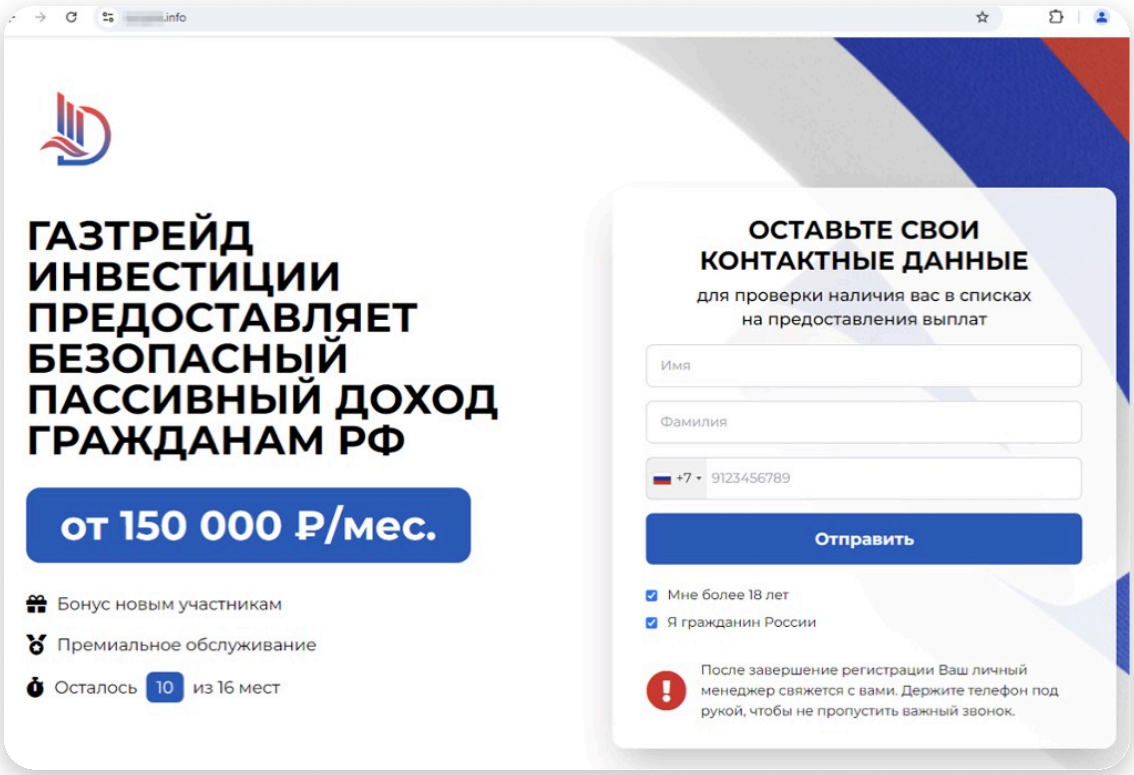
Мошенники выдают себя за крупные банки и нефтегазовые компании и предлагают пользователям из Армении и Молдовы «заработать на акциях»



Поддельный сайт азербайджанской нефтегазовой компании, где посетителям обещают заработок от 1000 манат в месяц

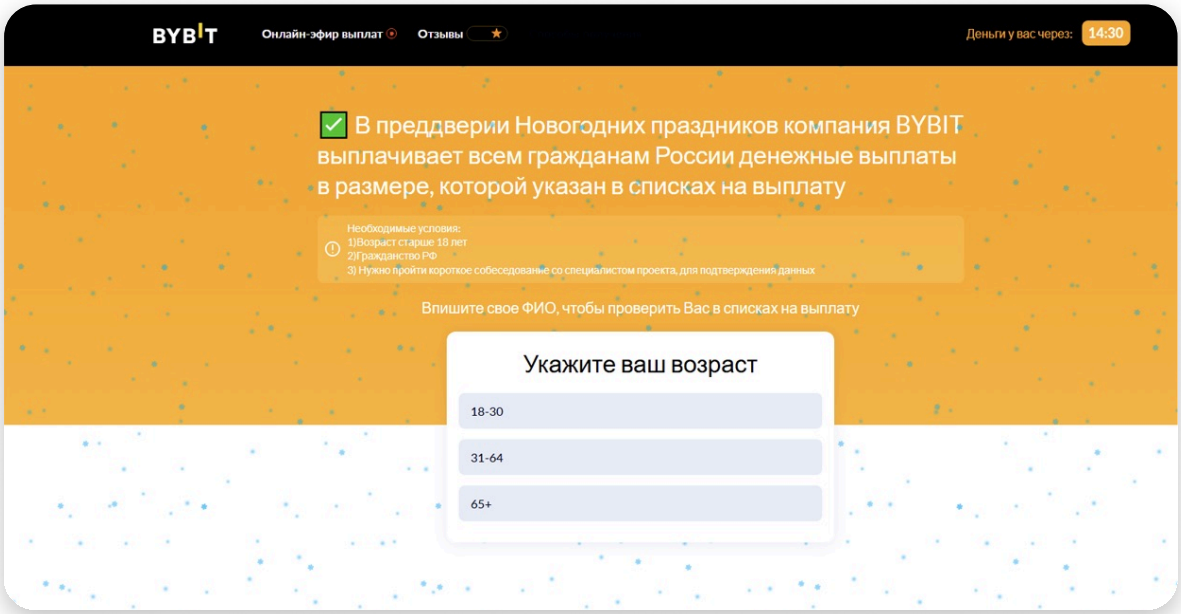


Сайт «новой инвестиционной платформы от Google» предлагает пройти опрос и получить доступ к сервису, якобы позволяющему зарабатывать от €1000



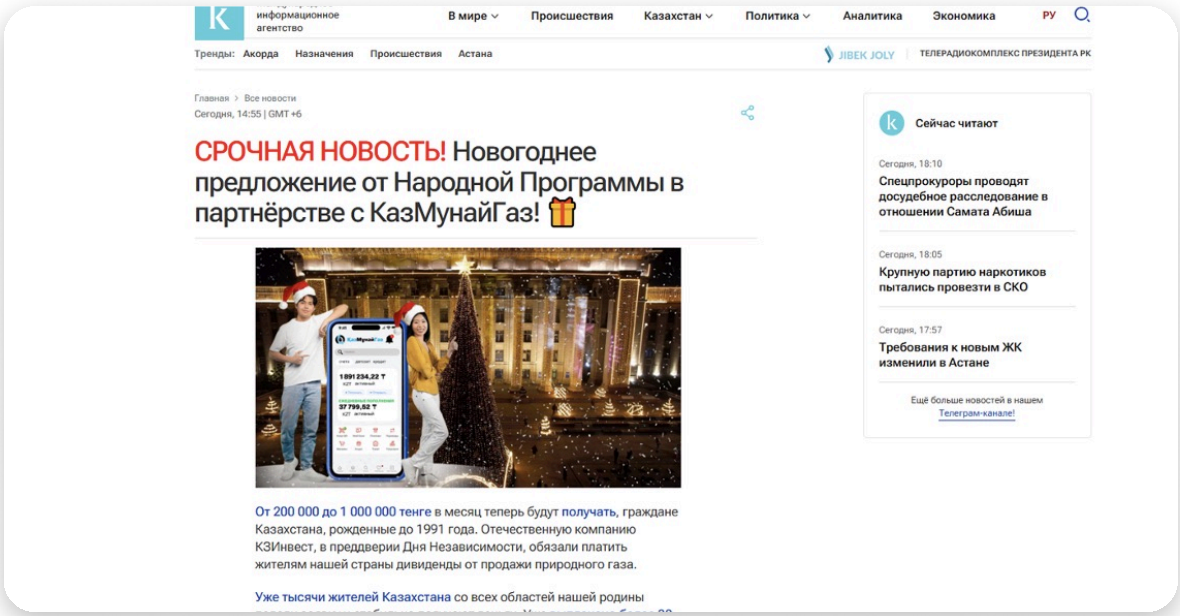
Один из мошеннических сайтов обещает российским пользователям «безопасный пассивный доход» от 150 000 рублей в месяц

Специалисты «Доктор Веб» отметили и сезонное изменение содержимого подобных сайтов. Так, в преддверии новогодних праздников мошенники стали чаще прибегать к тематике подарков якобы от имени банков, нефтегазовых компаний, криптобирж и других организаций. Например, на одном из поддельных интернет-ресурсов российские пользователи якобы могли получить денежные выплаты от криптобиржи в соответствии с некими «списками».
А для проверки доступности такой выплаты от них требовалось пройти опрос и указать персональные данные.



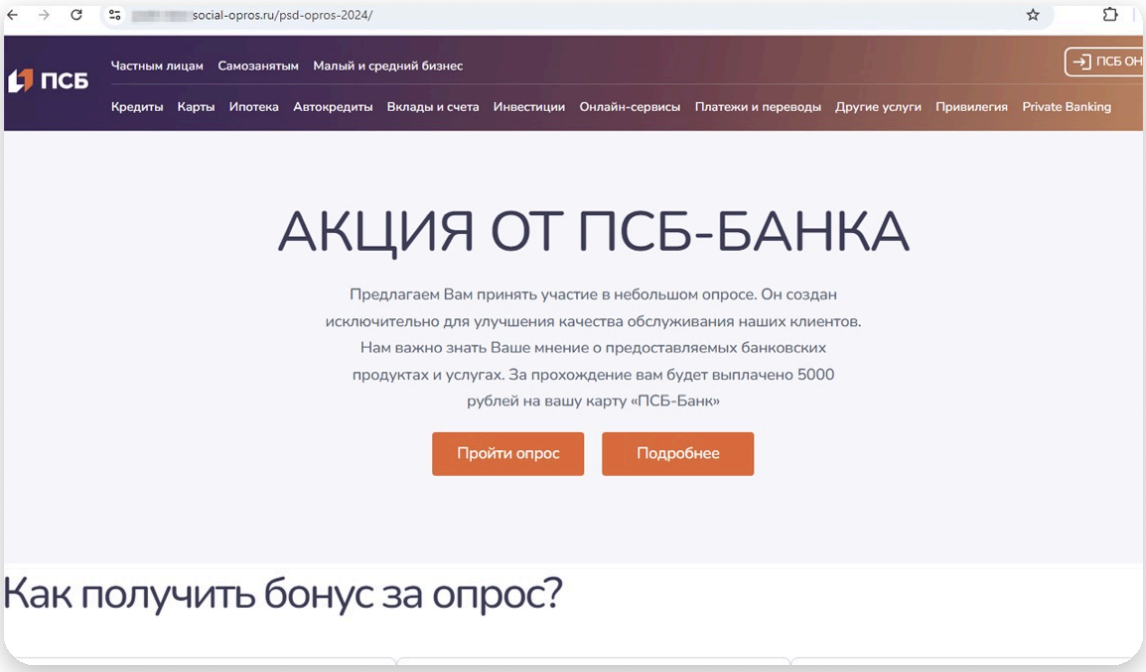
Поддельный сайт криптобиржи предлагает российским пользователям получить «новогодние выплаты»

Другой поддельный сайт сообщал о некоем «новогоднем предложении» от нефтегазовой компании, в рамках которого многие пользователи из Казахстана в честь Дня независимости страны якобы могли начать получать от 200 000 до 1 000 000 тенге в месяц. Для «получения» выплат потенциальные жертвы должны были подать «заявку», указав свои персональные данные на сайте.

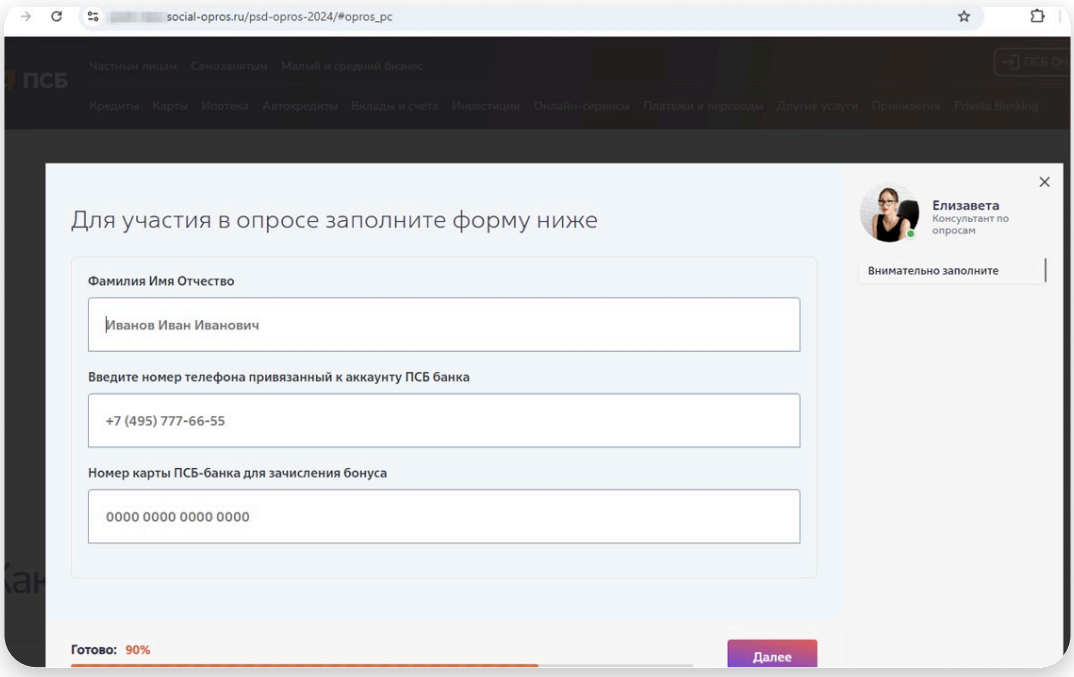


Мошеннический сайт обещает казахстанским пользователям крупные выплаты в честь Дня независимости в рамках «новогоднего предложения»

Вместе с тем наши интернет-аналитики зафиксировали появление поддельных сайтов российских банков, где потенциальным жертвам предлагается принять участие в опросе о качестве обслуживания и якобы получить за это денежное вознаграждение. Для этого у пользователей запрашиваются персональные данные, такие как имя, фамилия и отчество, привязанный к учетной записи банка номер мобильного телефона, а также номер банковской карты.

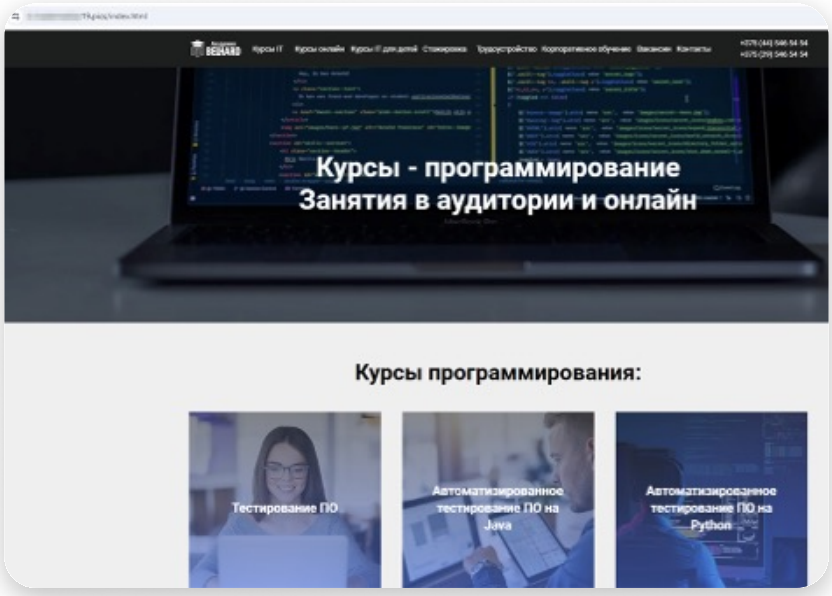


Пример поддельного сайта банка, который копирует оформление настоящего сайта кредитной организации и предлагает потенциальным жертвам пройти опрос за вознаграждение

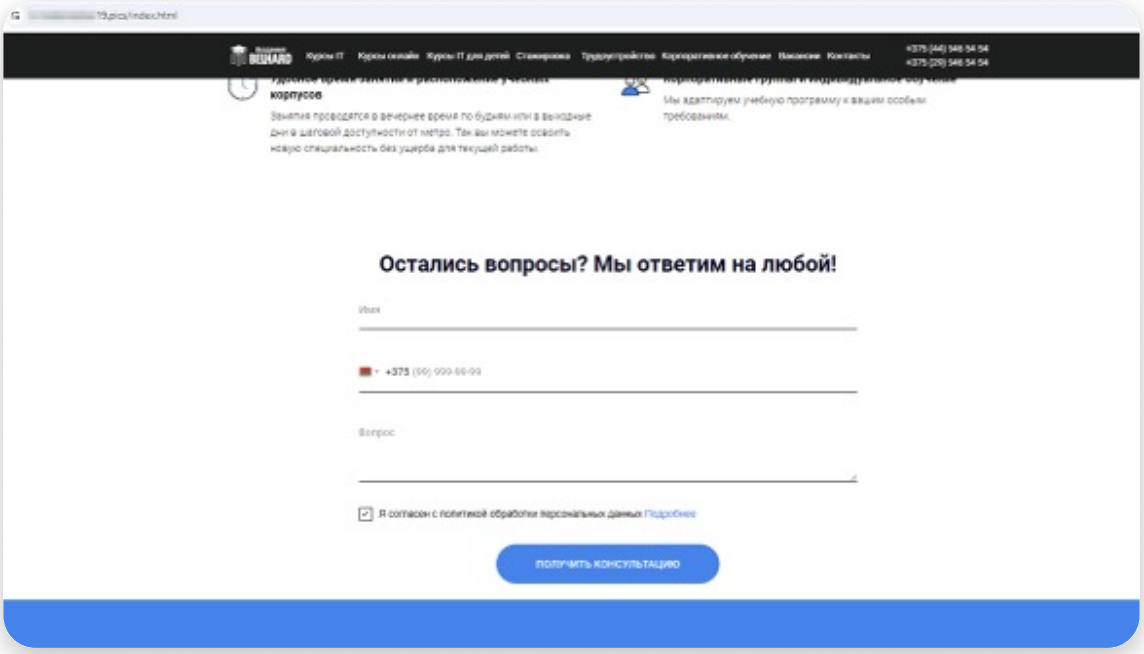


Для «участия» в опросе пользователь должен заполнить форму, предоставив свои данные

Кроме того, были выявлены мошеннические сайты, предлагающие пройти онлайн-обучение — например, программированию. Заинтересовавшимся посетителям предлагалось оставить контактные данные для «получения консультации».

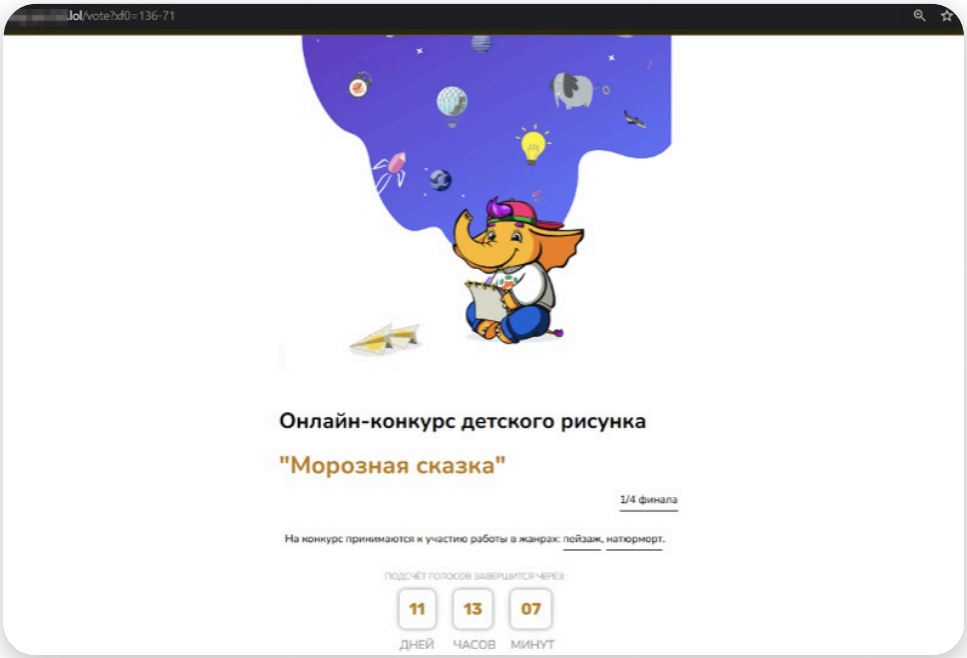


Сайт, предлагающий онлайн-курсы по программированию

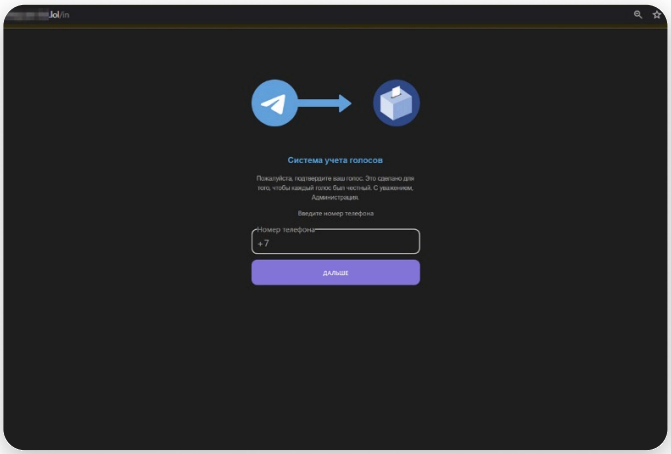


Для «получения консультации» пользователи должны указать персональные данные

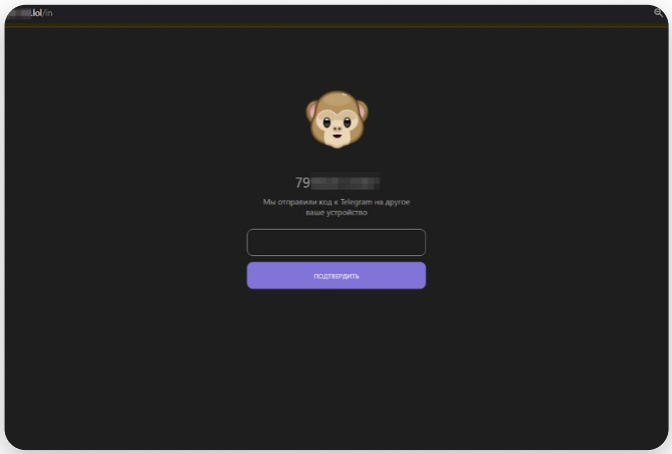
Интернет-мошенники не оставляют попыток похитить учетные записи Telegram. Так, в IV квартале 2024 года были обнаружены очередные фишинговые сайты, замаскированные под различные онлайн-голосования — например, в «конкурсах детских рисунков». Для «подтверждения» голоса пользователи должны указать номер мобильного телефона, на который поступит проверочный код. Однако, указав этот код на поддельном сайте, они открывают мошенникам доступ к своим учетным записям.



Сайт мошенников, на котором посетителям предлагается проголосовать в детском конкурсе рисунков



«Система учета голосов» требует номер мобильного телефона для «подтверждения голоса» и отправки одноразового кода



При вводе полученного кода жертвы предоставляют мошенникам доступ к своим учетным записям Telegram

Вредоносное и нежелательное ПО для мобильных устройств

Согласно данным статистики детектирований **Dr.Web Security Space для мобильных устройств**, в IV квартале 2024 года пользователи чаще всего сталкивались с рекламными троянами **Android.HiddenAds**, вредоносными приложениями **Android.FakeApp** и **Android.Siggen**. Вместе с тем за прошедший период специалисты компании «Доктор Веб» обнаружили множество новых угроз в каталоге Google Play.

Наиболее заметные события, связанные с «мобильной» безопасностью в IV квартале:

Рекламные трояны

Высокая активность рекламных троянов Android.HiddenAds и мошеннических вредоносных программ Android.FakeApp

Google Play

Появление новых вредоносных приложений 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
«Доктор Веб» в других странах