Dr.WEB

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

Статистика

Согласно статистике детектирований антивируса Dr.Web, в III квартале 2024 года общее число обнаруженных угроз возросло на **10,81%** по сравнению со II кварталом. Число уникальных угроз снизилось на **4,73%**. Большинство детектирований вновь пришлось на рекламные приложения. Распространение также получили вредоносные скрипты, трояны, демонстрирующие рекламу, и трояны, которое распространяются в составе других вредоносных приложений и применяются для затруднения их обнаружения. В почтовом трафике чаще всего выявлялись вредоносные скрипты и приложения, эксплуатирующие уязвимости документов Microsoft Office.

На Android-устройствах наиболее распространенными угрозами стали применяемые в мошеннических целях трояны **Android.FakeApp**, рекламные трояны **Android.HiddenAds** и обладающие различной функциональностью вредоносные программы **Android.Siggen**. При этом в августе наши специалисты обнаружили нового трояна **Android.Vo1d**, который заразил почти 1 300 000 ТВ-приставок, работающих на ОС Android. Кроме того, специалисты вирусной лаборатории «Доктор Веб» в течение III квартала выявили множество новых угроз в каталоге Google Play.

Главные тенденции III квартала

Реклама

Рекламные приложения остались наиболее часто детектируемыми угрозами

Почта

Во вредоносном почтовом трафике по-прежнему преобладали вредоносные скрипты

Новая угроза

Обнаружено заражение более 1 000 000 ТВ-приставок на базе Android бэкдором Android.Vo1d

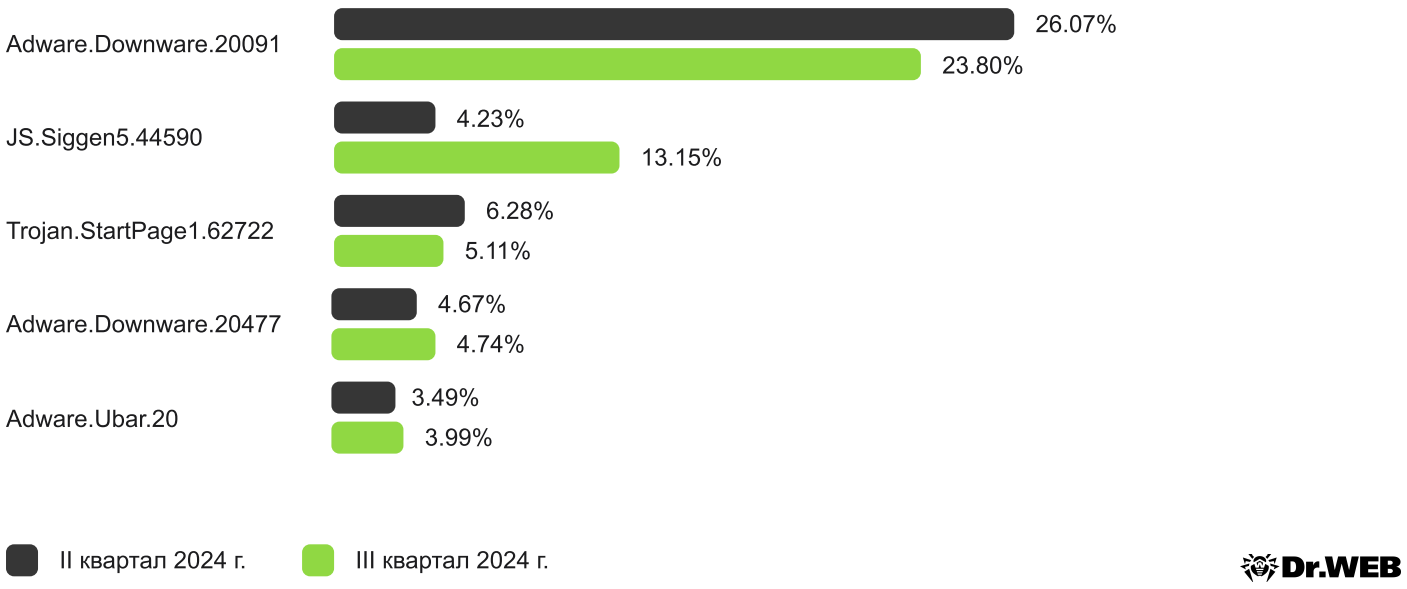
Google Play

Были зафиксированы новые угрозы в каталоге Google Play

По данным сервиса статистики «Доктор Веб»

Наиболее распространенное

рекламное и вредоносное ПО согласно данным сервиса статистики



Adware.Downware.20091

Adware.Downware.20477

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Trojan.StartPage1.62722

Вредоносная программа, подменяющая стартовую страницу в настройках браузера.

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.

Adware.Ubar.20

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

Статистика вредоносных программ 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.

W97M.DownLoader.6154

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

Trojan.AutoIt.1410

Детектирование упакованной версии троянской программы Trojan.AutoIt.289, написанной на скриптовом языке AutoIt. Она распространяется в составе группы из нескольких вредоносных приложений — майнера, бэкдора и модуля для самостоятельного распространения. Trojan.AutoIt.289 выполняет различные вредоносные действия, затрудняющие обнаружение основной полезной нагрузки.

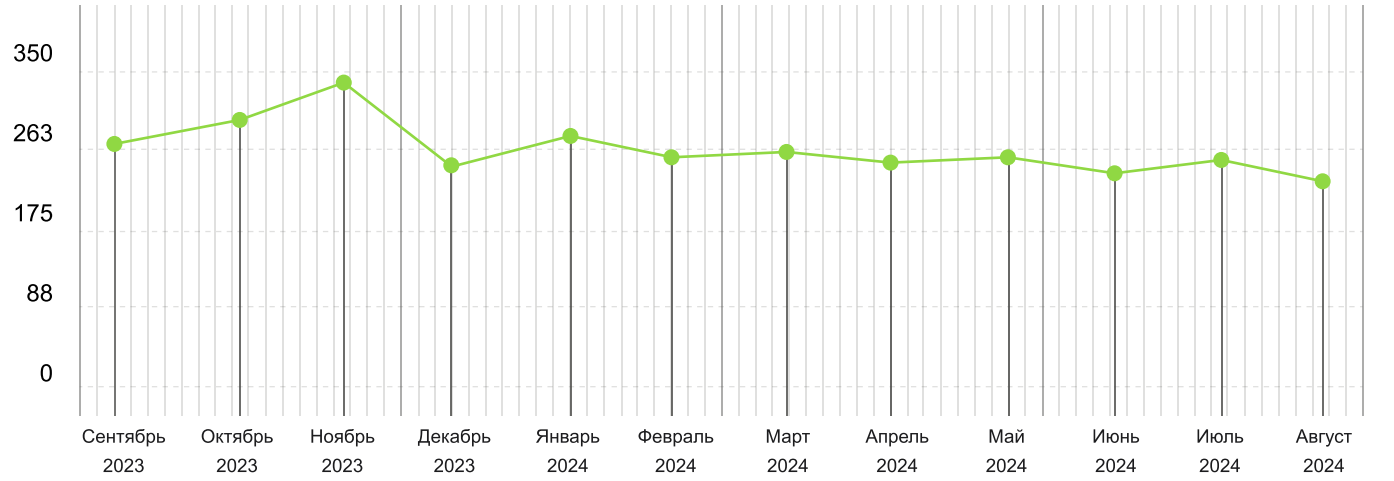
Шифровальщики

В III квартале 2024 года число запросов на расшифровку файлов, затронутых троянскими программами-шифровальщиками, снизилось на 15,73% 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»

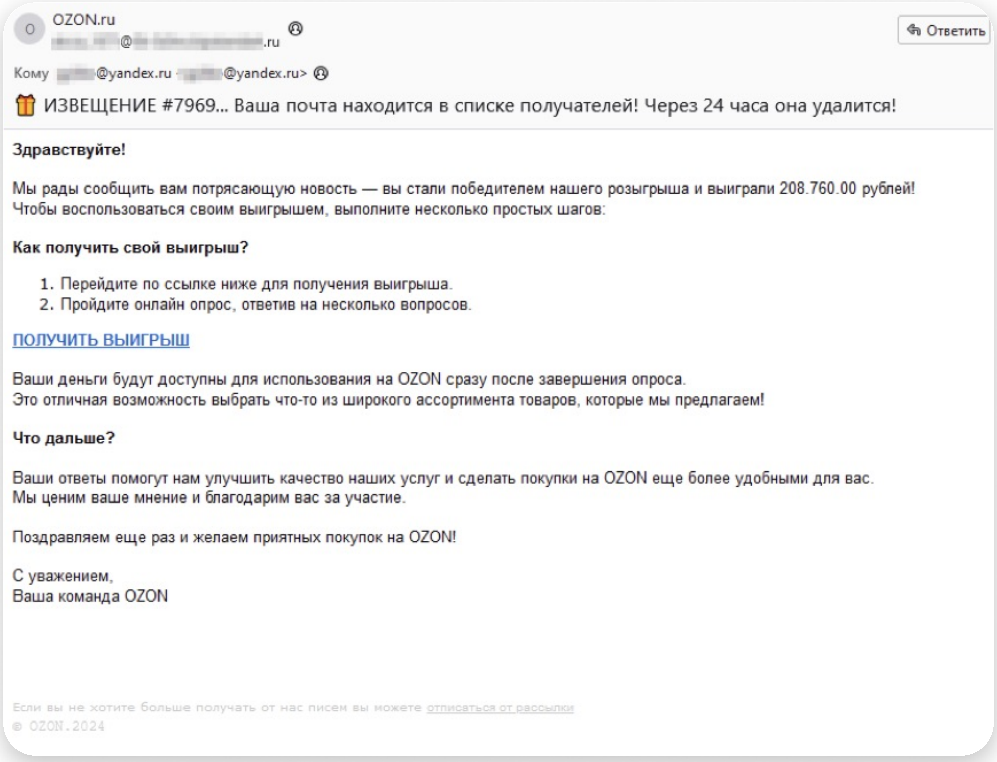


Наиболее распространенные энкодеры III квартала:

19.38%	**9.42%**	**3.99%**	**2.89%**	**2.72%**
Trojan.Encoder.35534	Trojan.Encoder.3953	Trojan.Encoder.38200	Trojan.Encoder.26996	Trojan.Encoder.35067

Сетевое мошенничество

В течение III квартала 2024 года интернет-мошенники продолжили распространять электронные спам-письма со ссылками на различные фишинговые сайты. Например, русскоязычные пользователи вновь сталкивались с сообщениями, якобы отправленными от имени известных интернет-магазинов. **В одних** им предлагалось принять участие в розыгрыше призов или получить подарок. **При переходе** по ссылкам из таких писем потенциальные жертвы попадали на мошеннические сайты, где для «получения» того или иного приза или выигрыша от них требовалось оплатить комиссию.



OZON.ru

Ответить

Кому @yandex.ru @yandex.ru>

ИЗВЕЩЕНИЕ #7969... Ваша почта находится в списке получателей! Через 24 часа она удалится!

Здравствуйте!

Мы рады сообщить вам потрясающую новость — вы стали победителем нашего розыгрыша и выиграли 208.760.00 рублей!
Чтобы воспользоваться своим выигрышем, выполните несколько простых шагов:

Как получить свой выигрыш?

1. Перейдите по ссылке ниже для получения выигрыша.
2. Пройдите онлайн опрос, ответив на несколько вопросов.

ПОЛУЧИТЬ ВЫИГРЫШ

Ваши деньги будут доступны для использования на OZON сразу после завершения опроса.
Это отличная возможность выбрать что-то из широкого ассортимента товаров, которые мы предлагаем!

Что дальше?

Ваши ответы помогут нам улучшить качество наших услуг и сделать покупки на OZON еще более удобными для вас.
Мы ценим ваше мнение и благодарим вас за участие.

Поздравляем еще раз и желаем приятных покупок на OZON!

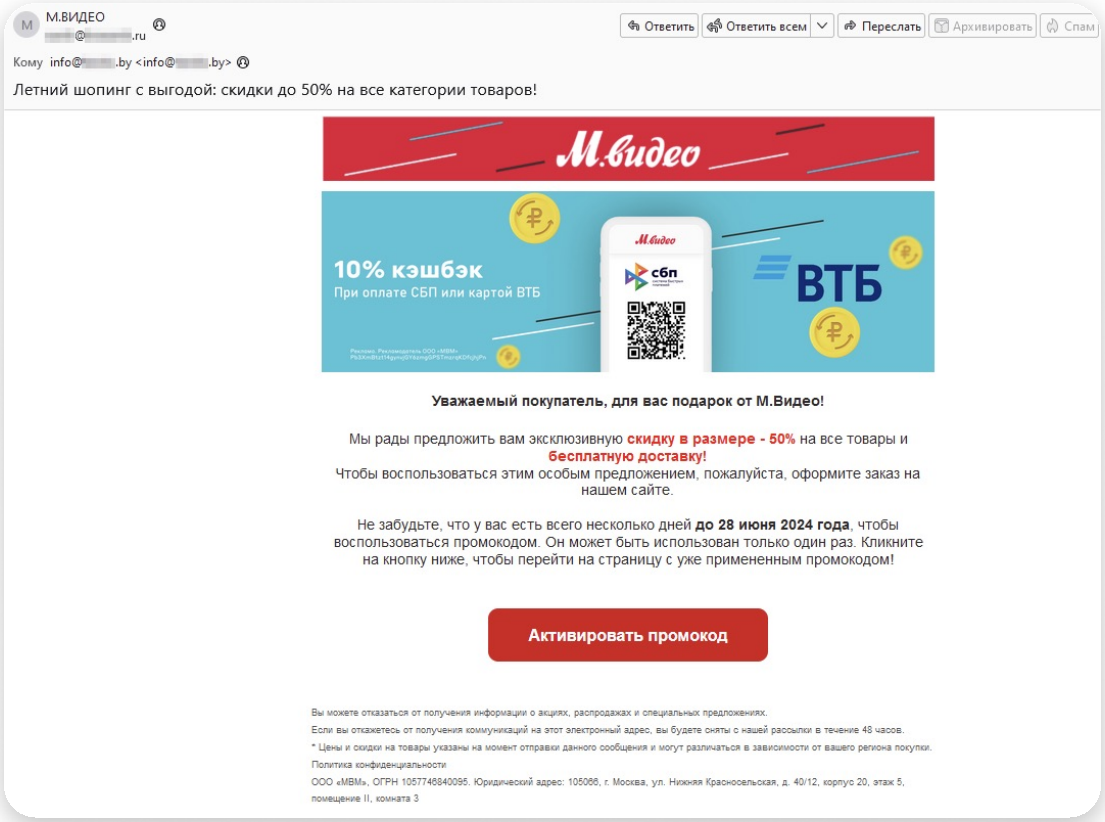
С уважением,
Ваша команда OZON

Если вы не хотите больше получать от нас писем вы можете отписаться от рассылки

© OZON.2024

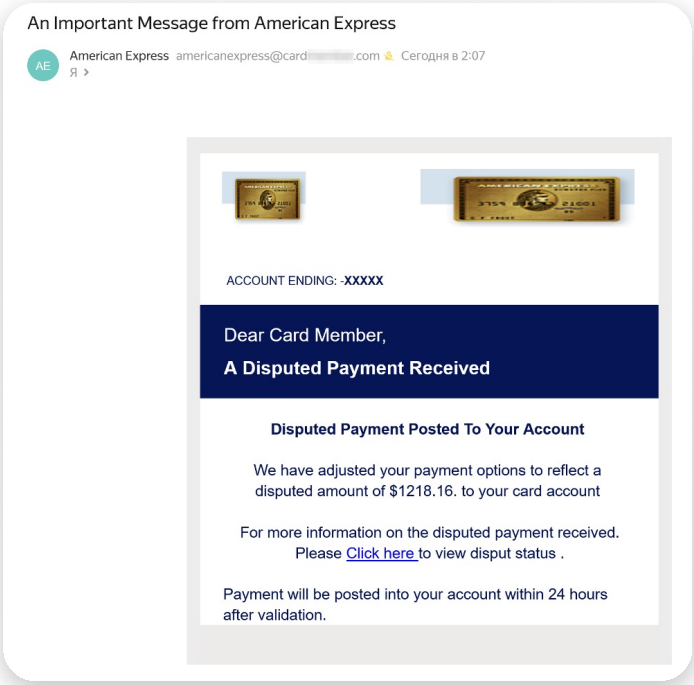
Мошенники якобы от имени онлайн-магазина предлагают потенциальной жертве «получить выигрыш» в размере 208 760 рублей

В других письмах пользователей якобы ждала скидка на покупку товаров в крупном магазине электроники. Ссылки из этих сообщений вели на поддельный сайт, оформленный в стиле настоящего интернет-ресурса площадки. **При оформлении** «заказа» на нем потенциальные жертвы должны были указать свои персональные данные, а также данные банковской карты.

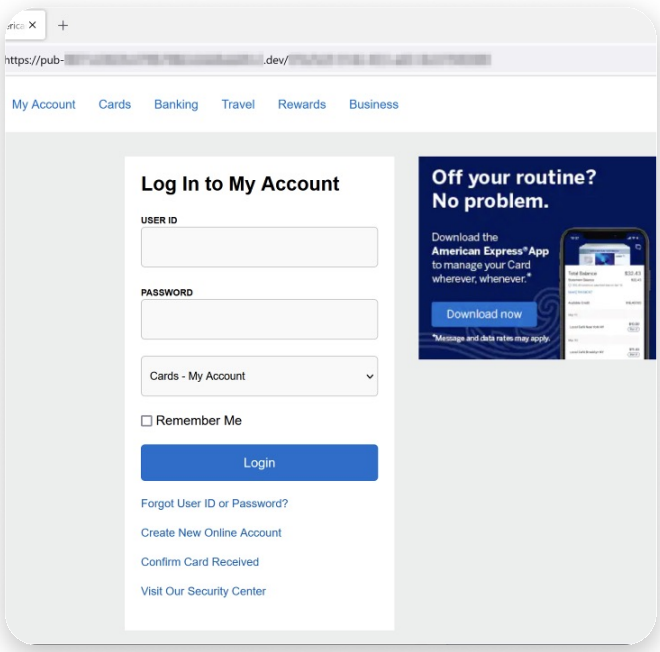


Мошенническое письмо, предлагающее «активировать промокод» для покупки электроники

Популярным среди мошенников остается спам финансовой тематики. Так, злоумышленники рассылали нежелательные письма для «подтверждения» получения крупных денежных переводов. Пример такого письма, нацеленного на англоязычных пользователей, представлен ниже. Ссылка в нем вела на фишинговую форму входа в учетную запись клиента банка, внешне напоминающую подлинную страницу на сайте кредитной организации.



Пользователю якобы необходимо подтвердить получение $1218,16 США



Фишинговый сайт банка, выдаваемый мошенниками за настоящий

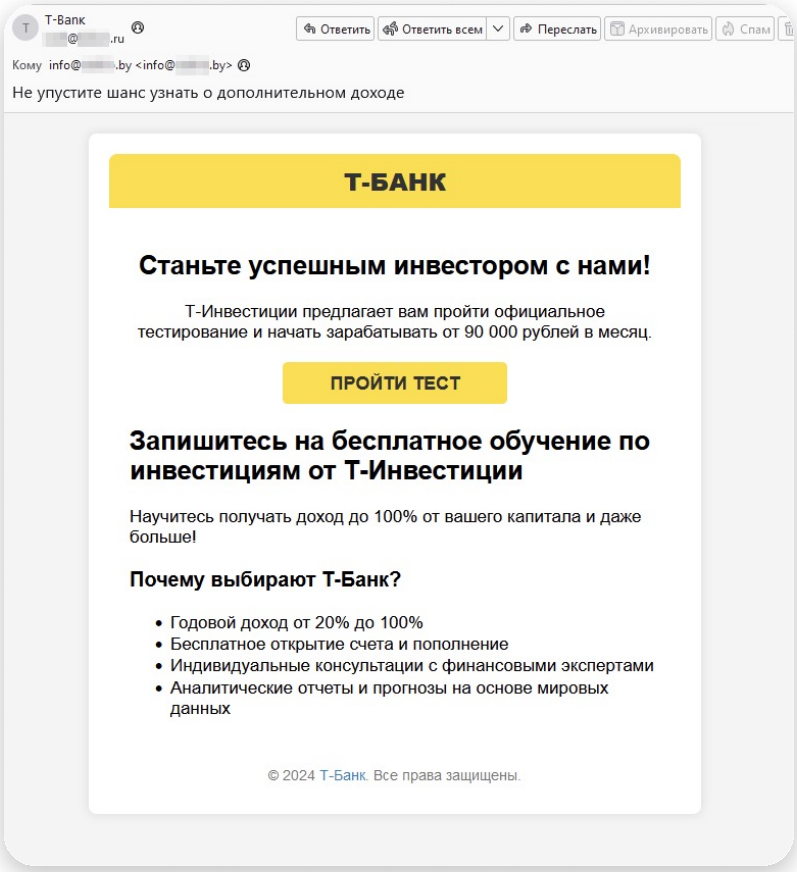
Среди нежелательных писем, предназначенных для японской аудитории, наши специалисты зафиксировали очередные поддельные уведомления кредитных организаций — например, с информацией о расходах по банковской карте за месяц. В одном из таких сообщений мошенники замаскировали ссылку на фишинговый сайт: пользователи в тексте письма видели ссылки на настоящие адреса сайта банка, но те при нажатии вели на мошеннический интернет-ресурс.

Все ссылки в письме на самом деле ведут на фишинговый сайт

Франкоязычные пользователи (в частности, из Бельгии) сталкивались с фишинговыми письмами, которые сообщали о «блокировке» их банковских счетов. Для **«разблокировки»** им предлагалось перейти по ссылке, которая в действительности вела на сайт мошенников.

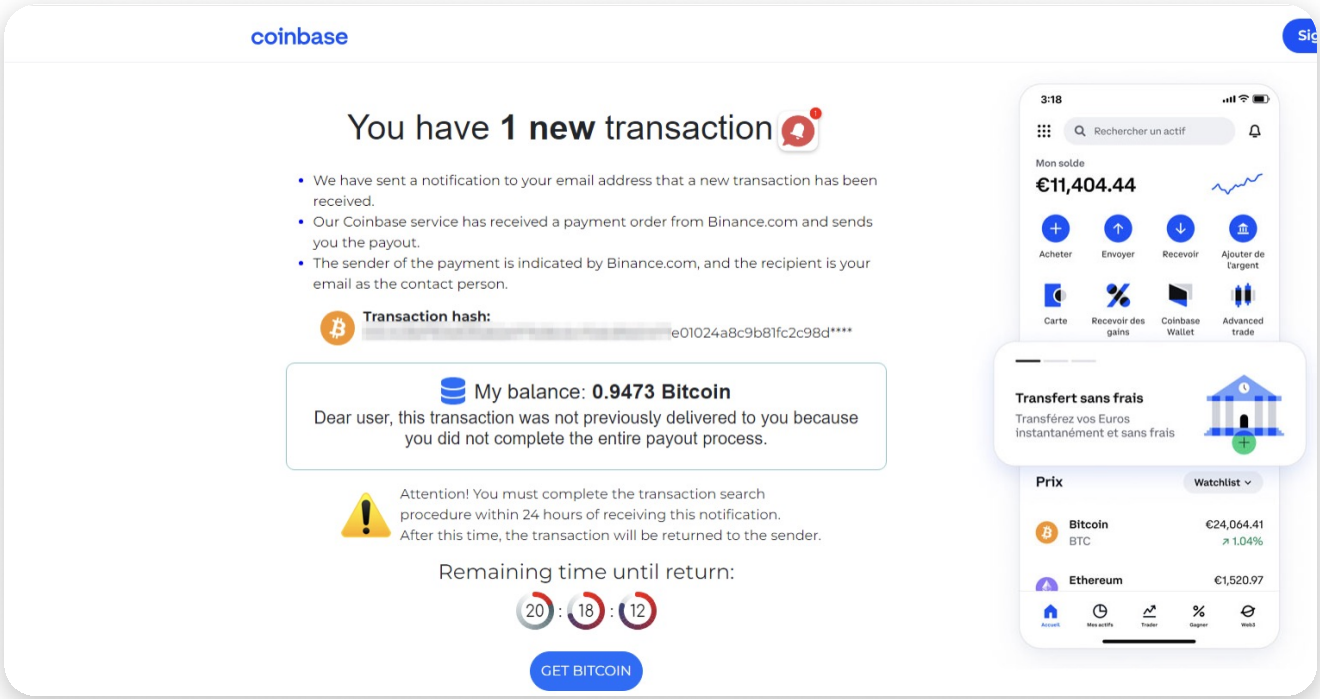
Мошенники пугают потенциальную жертву «заблокированным» банковским аккаунтом

А среди российских пользователей вновь активно распространялся почтовый спам, в котором потенциальным жертвам якобы от имени известных банков предлагалось стать инвесторами. Ссылки в таких нежелательных письмах ведут на мошеннические сайты, где у посетителей под видом получения доступа к инвестиционным сервисам запрашиваются персональные данные.



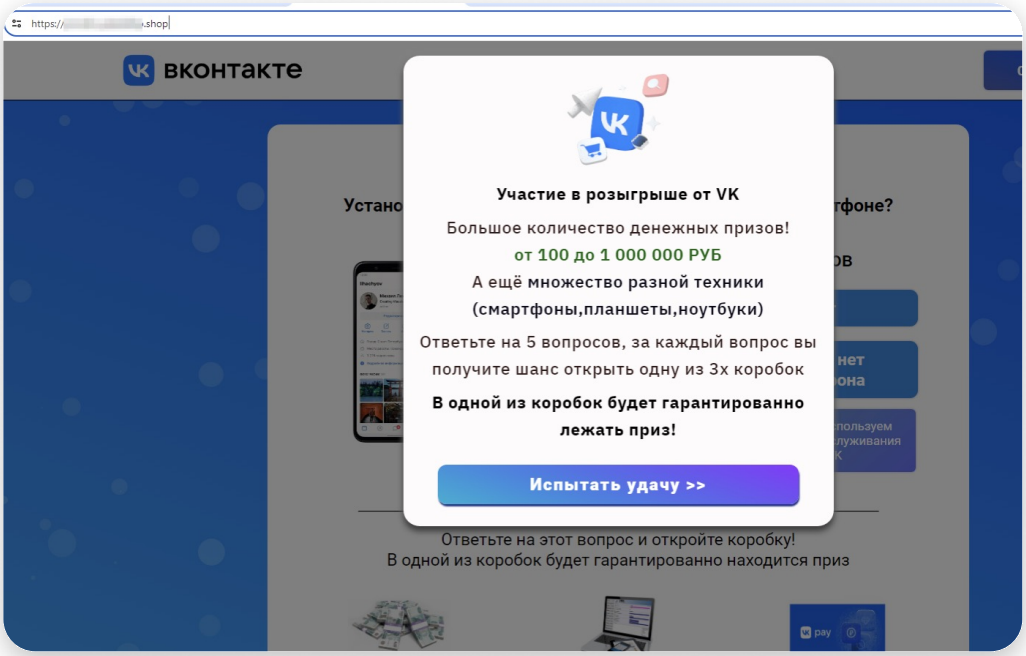
Пользователю якобы от имени банка предлагается пройти тест и стать инвестором

Вместе с тем интернет-аналитики «Доктор Веб» выявили новые фишинговые сайты, нацеленные на владельцев криптовалют. Так, на одном из них посетителям якобы от имени крупной криптобиржи сообщалось о неполученном Bitcoin-переводе. Для «завершения» транзакции потенциальным жертвам предлагалось оплатить «комиссию». Никакой криптовалюты пользователям, конечно же, не поступало — они лишь отдавали мошенникам собственные активы.

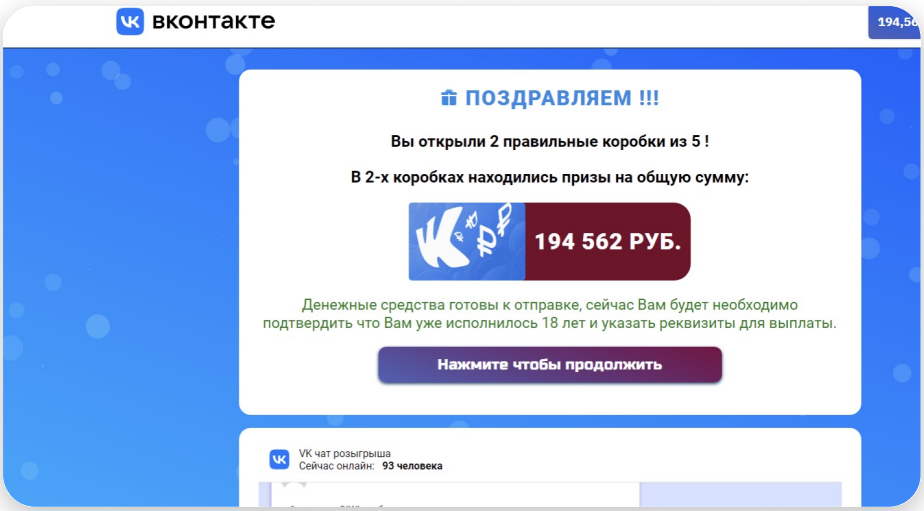


Мошеннический сайт сообщает, что у пользователя якобы имеется неполученный Bitcoin-перевод

Кроме того, были обнаружены фишинговые сайты, имитировавшие внешний вид социальной сети «ВКонтакте». Их посетителям предлагалось принять участие в некоем розыгрыше призов, открыв для этого несколько виртуальных коробок с подарками. После того как потенциальные жертвы открывали «правильные» коробки и якобы выигрывали крупную сумму денег, сайт предлагал им заплатить комиссию для получения «выигрыша».



Мошеннический сайт предлагает посетителям «испытать удачу»



Пользователь якобы выиграл приз в размере 194 562 рубля

Вредоносное и нежелательное ПО для мобильных устройств

Согласно данным статистики детектирований Dr.Web Security Space для мобильных устройств, в III квартале 2024 года на защищаемых устройствах чаще всего обнаруживались:

Первое место	Второе место	Третье место
Android.FakeApp	Android.HiddenAds	Android.Siggen

За прошедший период наши специалисты выявили множество новых угроз в каталоге Google Play. Среди них — различные варианты троянов **Android.FakeApp** и **Android.HiddenAds**. Кроме того, была зафиксирована атака на ТВ-приставки с ОС Android—бэкдор **Android.Vo1d** заразил около **1 300 000** устройств у пользователей из **197 стран**. Он помещал свои компоненты в системную область приставок и по команде злоумышленников мог незаметно скачивать и устанавливать сторонние программы.

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

Android.Vo1d

Обнаружение бэкдора Android.Vo1d, заразившего более миллиона ТВ-приставок

Android.FakeApp

Высокая активность вредоносных программ Android.FakeApp

Android.HiddenAds

Высокая активность рекламных троянов Android.HiddenAds

Google Play

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
«Доктор Веб» в других странах