Dr.WEB

«Доктор Веб»: обзор вирусной активности за 2024 год

Главное

В 2024 году среди самых распространенных угроз вновь оказались вредоносные программы, созданные с использованием скриптового языка AutoIt и распространяемые в составе другого вредоносного ПО для затруднения его обнаружения. Наблюдалась высокая активность рекламных троянов и различных вредоносных скриптов. В почтовом трафике чаще всего также детектировались вредоносные скрипты. Кроме того, посредством нежелательных писем распространялись всевозможные троянские программы, фишинговые документы и эксплойты, позволяющие выполнять произвольный код.

Среди мобильных угроз наибольшее распространение получили рекламные троянские программы, трояны-шпионы и нежелательное рекламное ПО. В течение года наблюдался рост активности мобильных банковских троянов. При этом наша вирусная лаборатория обнаружила сотни новых вредоносных и нежелательных программ в каталоге Google Play.

Интернет-аналитики отмечали высокую активность сетевых мошенников, арсенал которых пополнился новыми схемами обмана.

По сравнению с 2023 годом сократилось число обращений пользователей за расшифровкой файлов, пострадавших от действий троянов-энкодеров. Вместе с тем наши специалисты наблюдали множество событий, связанных с информационной безопасностью. В течение года компания **«Доктор Веб»** расследовала несколько таргетированных атак, выявила очередное заражение ТВ-приставок, работающих на базе ОС Android, а также отразила атаку на собственную инфраструктуру.

Главные тенденции года

Трояны

Сохранение высокой активности троянов, созданных с использованием скриптового языка AutoIt

Скрипты

Одними из самых распространенных угроз были вредоносные скрипты

Почта

Среди почтовых угроз преобладали вредоносные скрипты и различные троянские программы

Атаки

Зафиксированы новые таргетированные атаки

ePBF

Злоумышленники стали чаще эксплуатировать технологию eBPF для сокрытия вредоносной активности

Снижение

Снижение числа запросов на расшифровку файлов, пострадавших от троянов-вымогателей

Интернет-мошенники

Высокая активность интернет-мошенников

Мобильные банковские трояны

Мобильные банковские трояны стали применяться чаще

Google Play

Обнаружение множества новых угроз в каталоге Google Play

Интересные события 2024 года

В январе специалисты «Доктор Веб» сообщили о трояне-майнере Trojan.BtcMine.3767, скрытом в пиратских программах, которые распространялись через специально созданный Telegram-канал и ряд интернет-сайтов. Вредоносная программа заразила десятки тысяч Windows-компьютеров. Для закрепления в атакуемой системе она создавала в планировщике задачу на собственный автозапуск и добавляла себя в исключения антивируса Windows Defender. Затем она внедряла в процесс `explorer.exe` (Проводник Windows) компонент, непосредственно отвечавший за добычу криптовалюты. Trojan.BtcMine.3767 также позволял выполнять ряд других вредоносных действий — например, устанавливать бесфайловый руткит, блокировать доступ к сайтам и запрещать обновления операционной системы.

В марте наша компания опубликовала исследование целевой атаки на российское предприятие машиностроительного сектора. Расследование инцидента выявило многоступенчатый вектор заражения и использование злоумышленниками сразу нескольких вредоносных приложений. Наибольший интерес представлял бэкдор JS.BackDoor.60, через который проходило основное взаимодействие между атакующими и зараженным компьютером. Этот троян использует собственный фреймворк на языке JavaScript и состоит из основного тела и вспомогательных модулей. Он позволяет красть файлы с зараженных устройств, отслеживать вводимую на клавиатуре информацию, создавать скриншоты, загружать собственные обновления и расширять функциональность через загрузку новых модулей.

В мае вирусные аналитики «Доктор Веб» выявили трояна-кликера Android.Click.414.origin в приложении Love Spouse для управления игрушками для взрослых, а также приложении QRunning для отслеживания физической активности — оба распространялись через каталог Google Play. Android.Click.414.origin маскировался под компонент для сбора отладочной информации и был внедрен в несколько новых версий этих программ. Позднее разработчики Love Spouse выпустили обновленную версию, которая более не содержала трояна. Реакции авторов второй программы не последовало. Android.Click.414.origin имел модульную архитектуру и с помощью своих компонентов мог выполнять различные вредоносные действия: собирать данные о зараженном устройстве, скрытно загружать веб-страницы, показывать рекламу, выполнять клики и взаимодействовать с содержимым загружаемых страниц.

В июле мы рассказали о появлении Linux-версии известного трояна удаленного доступа TgRat, который используется для целевых атак на компьютеры. Новый вариант вредоносного приложения, получивший имя Linux.BackDoor.TgRat.2, был выявлен в ходе расследования инцидента информационной безопасности, с которым к нам обратился один из хостинг-провайдеров. Антивирус Dr.Web выявил подозрительный файл на сервере одного из его клиентов — им оказался дроппер бэкдора, который и устанавливал трояна. Злоумышленники управляли Linux.BackDoor.TgRat.2 через закрытую Telegram-группу, используя подключенный к ней Telegram-бот. С помощью мессенджера они могли скачивать из скомпрометированной системы файлы, делать снимки экрана, удалённо выполнять команды или загружать файлы на компьютер, используя вложения в чате.

В начале сентября на сайте компании «Доктор Веб» вышел материал, рассказывающий о несостоявшейся таргетированной атаке на крупное российское предприятие отрасли грузовых железнодорожных перевозок. Несколькими месяцами ранее сотрудники отдела информационной безопасности этой компании зафиксировали подозрительное электронное письмо с прикрепленным к нему файлом. Его изучение нашими вирусными аналитиками показало, что это замаскированный под pdf-документ Windows-ярлык с прописанными в нем параметрами запуска командного интерпретатора PowerShell. Открытие этого ярлыка должно было привести к многоступенчатому заражению целевой системы сразу несколькими вредоносными программами для кибершпионажа. Одной из них был Trojan.Siggen27.11306, эксплуатировавший уязвимость CVE-2024-6473 Яндекс Браузера к перехвату порядка поиска DLL (DLL Search Order Hijacking). Троян помещал в каталог установки браузера вредоносную dll-библиотеку с именем системного компонента Wldp.dll, отвечающего за обеспечение безопасности запуска приложений. Поскольку вредоносный файл находился в папке приложения, при запуске последнего троянской библиотеке вследствие уязвимости браузера отдавался больший приоритет, и та загружалась первой. Она также получала все разрешения самого браузера. Данная уязвимость в дальнейшем была исправлена.

Чуть позже наши специалисты рассказали об очередной атаке на ТВ-приставки на базе ОС Android. В кампании была задействована вредоносная программа Android.Vo1d, заразившая почти 1 300 000 устройств у пользователей из 197 стран. Это был модульный бэкдор, который помещал свои компоненты в системную область и по команде злоумышленников мог скрытно скачивать и запускать другие приложения.

Кроме того, в сентябре была зафиксирована целевая атака на ресурсы нашей компании. Специалисты «Доктор Веб» оперативно пресекли попытку навредить инфраструктуре, успешно отразив атаку. При этом никто из наших пользователей также не пострадал.

В октябре вирусные аналитики «Доктор Веб» проинформировали об обнаружении ряда новых вредоносных программ для ОС Linux. Их удалось выявить благодаря исследованию атак на устройства с установленной системой управления базами данных Redis, которая все чаще становится объектом внимания киберпреступников, эксплуатирующих в ней различные уязвимости. Среди обнаруженных угроз были бэкдоры, дропперы и новая модификация руткита, устанавливавшего на скомпрометированные устройства троян-майнер Skidmap. Этот майнер активен с 2019 года, а его основной целью являются корпоративные ресурсы — крупные серверы и облачные среды.

В этом же месяце наша вирусная лаборатория выявила масштабную кампанию по распространению вредоносных программ для добычи и кражи криптовалюты. От действий злоумышленников пострадали свыше 28 000 пользователей, большинство из них — в России. Трояны скрывались в пиратском ПО, для распространения которого использовались созданные на платформе GitHub мошеннические сайты. Кроме того, вирусописатели размещали ссылки на загрузку вредоносных приложений под размещенными на платформе YouTube видеороликами.

В ноябре наши специалисты выявили ряд новых вариантов троянской программы Android.FakeApp.1669, задачей которой является загрузка сайтов. В отличие от большинства других аналогичных вредоносных программ, Android.FakeApp.1669 получает адреса целевых сайтов из TXT-записи вредоносных DNS-серверов, для чего использует модифицированный код открытой библиотеки dnsjava. В то же время троян проявляет вредоносную активность только при подключении к интернету через определенных провайдеров. В других случаях он работает как безобидное ПО.

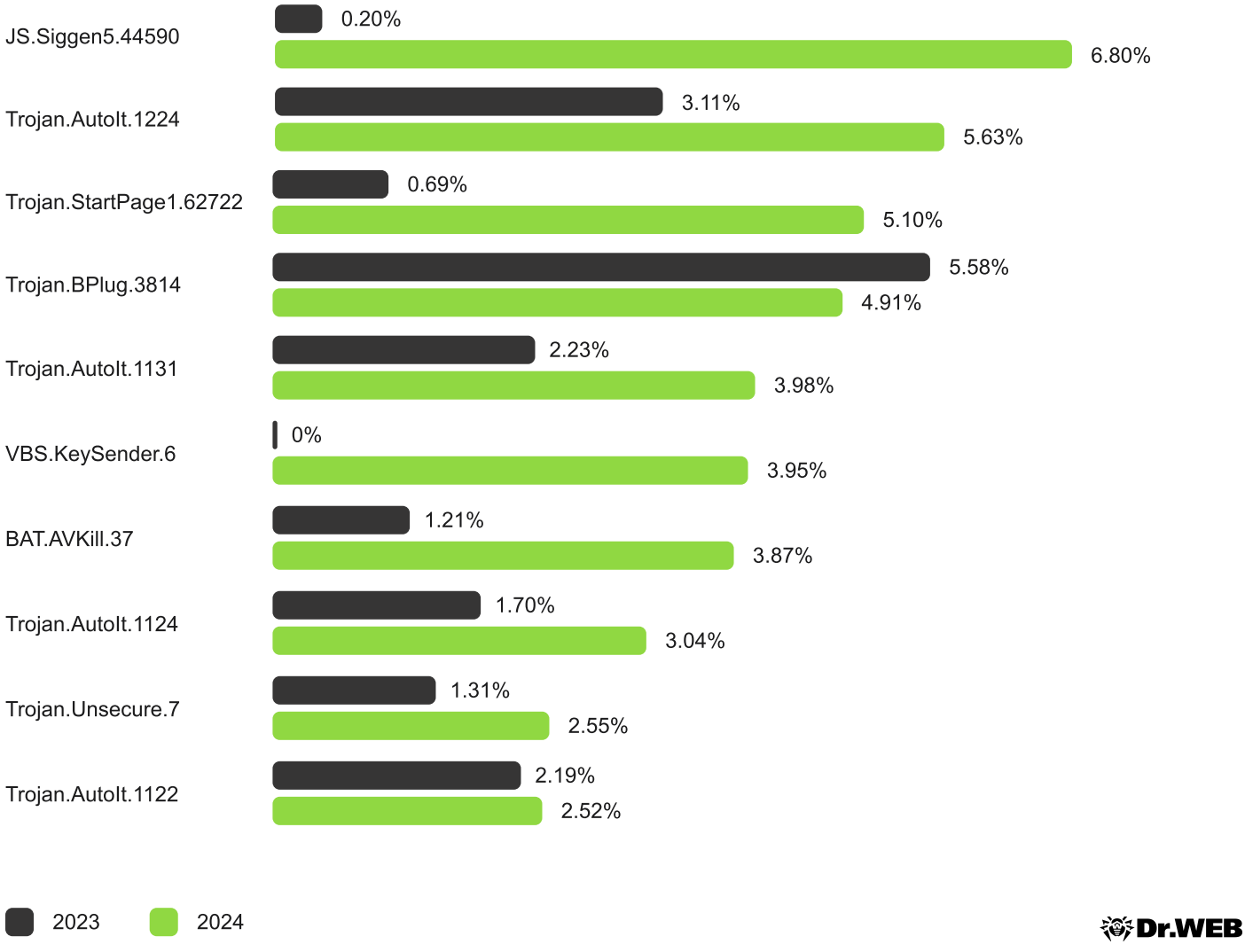
В конце 2024 года в процессе расследования обращения одного из наших клиентов специалисты вирусной лаборатории «Доктор Веб» выявили активную хакерскую кампанию, ориентированную главным образом на пользователей из Юго-Восточной Азии. В ходе атак киберпреступники применяли целый ряд вредоносных приложений, а также использовали методы и приемы, которые только набирают популярность в среде вирусописателей. Одним из них была эксплуатация технологии eBPF (extended Berkeley Packet Filter), созданной для расширенного контроля над сетевой подсистемой ОС Linux и работой процессов. Эта технология использовалась для маскировки вредоносной сетевой активности и процессов, сбора конфиденциальной информации, а также обхода сетевых экранов и систем обнаружения вторжений. Другой прием заключался в хранении настроек троянского ПО не на управляющем сервере, а на публичных площадках, таких как платформа GitHub и блоги. Третьей особенностью атак стало использование фреймворков постэксплуатации совместно с вредоносными приложениями. Хотя такие инструменты не являются вредоносными и применяются при аудите безопасности цифровых систем, их функциональность и наличие баз уязвимостей способно расширить возможности атакующих.

Вирусная обстановка

Согласно данным статистики детектирований антивируса Dr.Web, в 2024 году общее число обнаруженных угроз увеличилось на **26,20%** по сравнению с 2023 годом. Число уникальных угроз возросло на **51,22%**. Среди наиболее часто встречавшихся вредоносных программ были созданные на скриптовом языке AutoIt трояны, которые распространяются в составе другого вредоносного ПО для затруднения его обнаружения. Кроме того, пользователи сталкивались с различными вредоносными скриптами и рекламными троянами.

Наиболее распространенные

вредоносные программы в 2024 году по данным сервиса статистики «Доктор Веб»



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.StartPage1.62722

Вредоносная программа, подменяющая стартовую страницу в настройках браузера.

Trojan.AutoIt.1224 **Trojan.AutoIt.1131** **Trojan.AutoIt.1124** **Trojan.AutoIt.1222**

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.

Trojan.BPlug.3814

Детектирование вредоносных компонентов браузерного расширения WinSafe. Эти компоненты представляют собой сценарии JavaScript, которые демонстрируют навязчивую рекламу в браузерах.

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.

BAT.AVKill.37

Компонент троянской программы Trojan.AutoIt.289. Этот скрипт запускает другие компоненты вредоносного ПО, устанавливает их в автозагрузку через планировщик задач Windows, а также добавляет их в исключения антивируса Windows Defender.

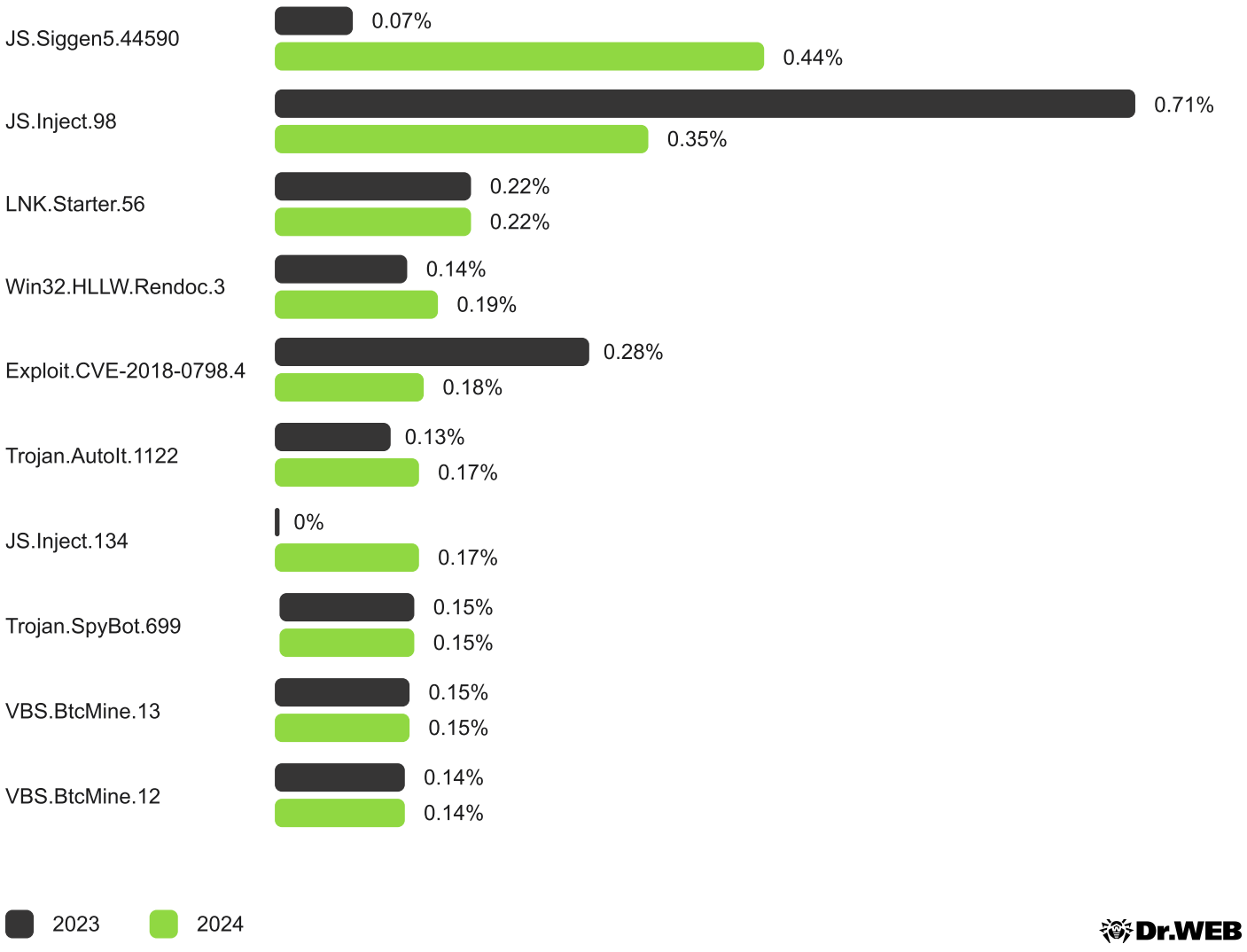
Trojan.Unsecure.7

Троян, блокирующий запуск антивирусного и прочего ПО через политики AppLocker в ОС Windows.

Среди почтовых угроз наибольшее распространение получили различные вредоносные скрипты и всевозможные троянские программы, такие как бэкдоры, загрузчики и дропперы вредоносного ПО, трояны со шпионской функциональностью, вредоносные приложения для добычи криптовалюты и прочие. Злоумышленники также рассылали фишинговые документы, часто представляющие собой поддельные формы авторизации на популярных сайтах. Кроме того, пользователи сталкивались с червями и вредоносными приложениями, которые эксплуатируют уязвимости в документах Microsoft Office.

Наиболее распространенные

вредоносные программы, выявленные в почтовом трафике в 2024 году



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.

Exploit.CVE-2018-0798.4

Эксплойт для использования уязвимостей в ПО Microsoft Office, позволяющий выполнить произвольный код.

Trojan.AutoIt.1122

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.

Trojan.SpyBot.699

Многомодульный банковский троян. Позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и исполнять произвольный код.

VBS.BtcMine.13

VBS.BtcMine.12

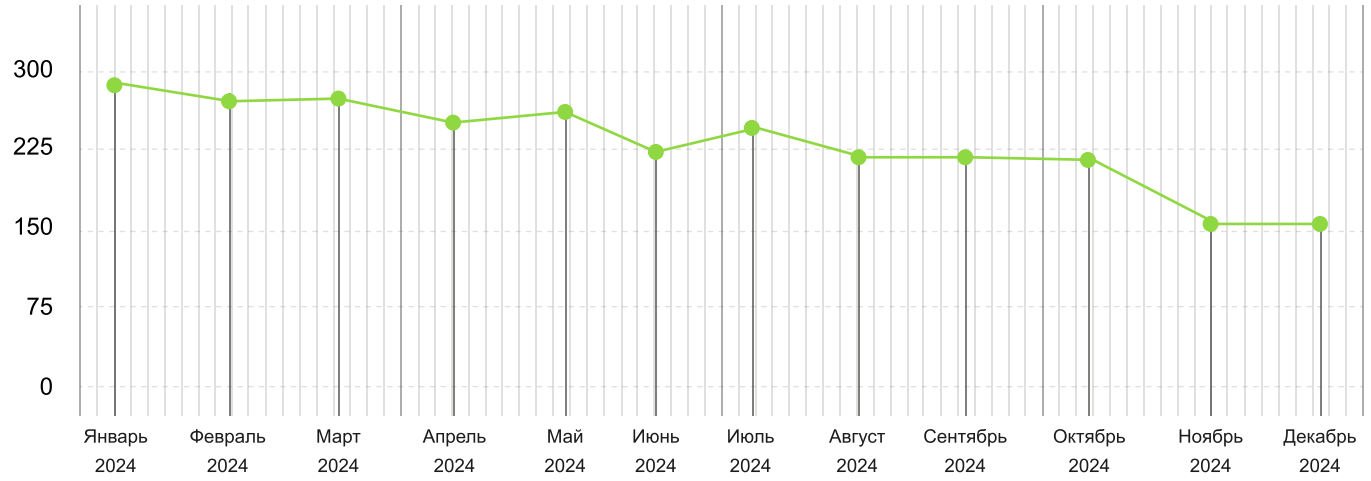
Вредоносный сценарий на языке VBS, выполняющий скрытую добычу криптовалют.

Шифровальщики

По сравнению с 2023, в 2024 году в службу технической поддержки «Доктор Веб» поступило на 33,05% меньше запросов от пользователей, которые пострадали от троянских программ-шифровальщиков. Динамика регистрации запросов на расшифровку файлов представлена на диаграмме ниже:

Количество запросов

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



Наиболее распространенные шифровальщики в 2024 году:

Trojan.Encoder.35534 — **13,13% обращений пользователей**

Шифровальщик, также известный как Mimic. При поиске целевых файлов для шифрования троян использует библиотеку everything.dll легитимной программы Everything, предназначенной для мгновенного поиска файлов на Windows-компьютерах.

Trojan.Encoder.3953 — **12.10% обращений пользователей**

Шифровальщик, имеющий несколько различных версий и модификаций. Для шифрования файлов применяет алгоритм AES-256 в режиме CBC.

Trojan.Encoder.26996 **7.44% обращений пользователей**

Шифровальщик, известный как STOP Ransomware. Он пытается получить приватный ключ с удаленного сервера, а в случае неудачи пользуется зашитым. Для шифрования файлов троян использует поточный алгоритм Salsa20.

Trojan.Encoder.35067 **2.21% обращений пользователей**

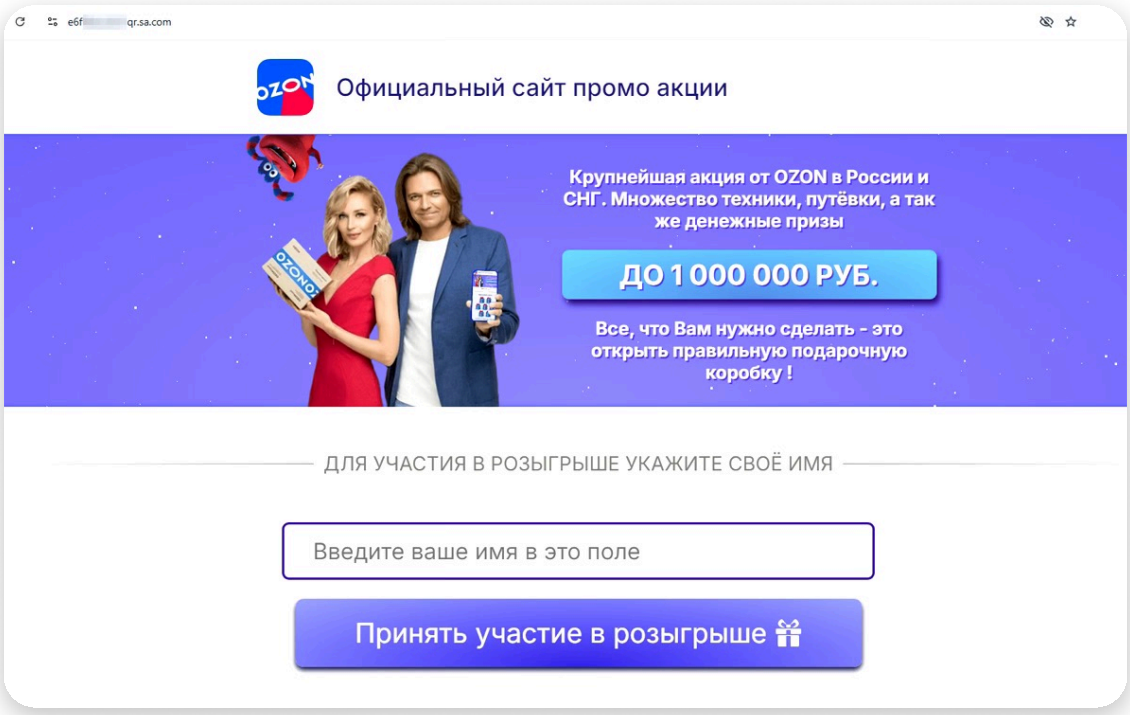
Шифровальщик, известный как Macop (один из вариантов этого трояна — Trojan.Encoder.30572). Обладает небольшим размером, порядка 30-40 Кбайт. Отчасти это обусловлено тем, что троян не несет с собой сторонних криптографических библиотек, а для шифрования и генерации ключей пользуется исключительно CryptoAPI-функциями. Для шифрования файлов применяет алгоритм AES-256, а сами ключи шифруются RSA-1024.

Trojan.Encoder.37369 **2.10% обращений пользователей**

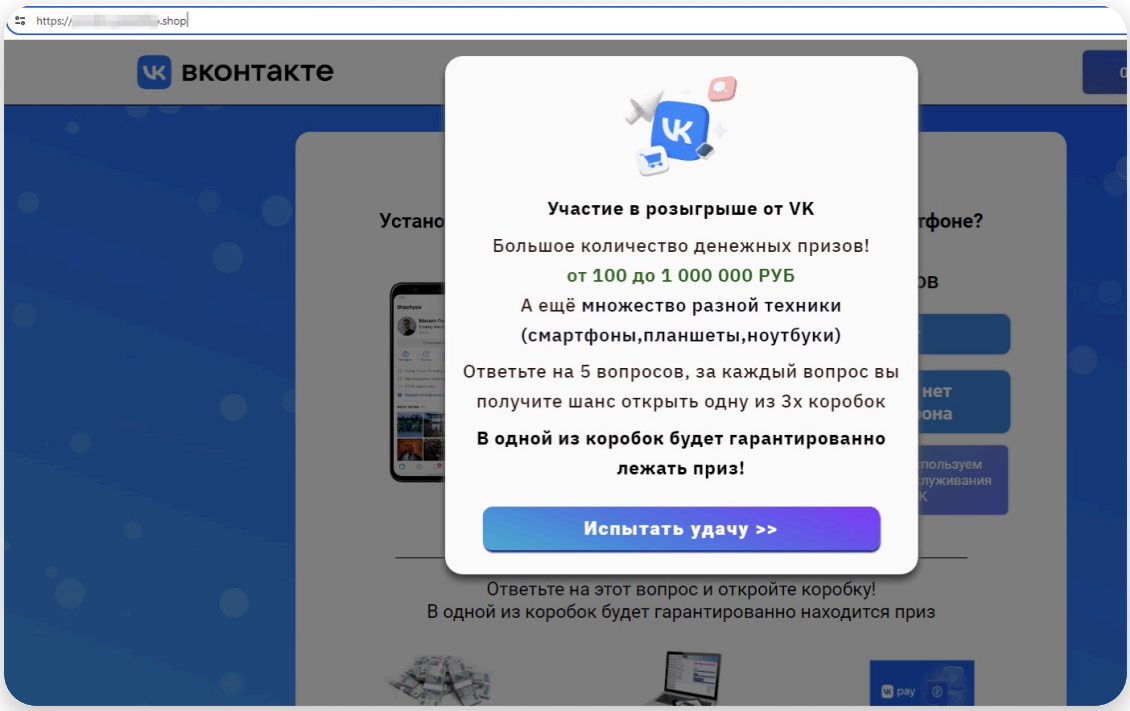
Одна из множества модификаций вымогателя #Cylance ransomware. Для шифрования файлов использует алгоритм ChaCha12 со схемой обмена ключами на основе эллиптической кривой Curve25519 (X25519).

Сетевое мошенничество

В течение 2024 года интернет-аналитики компании «Доктор Веб» наблюдали высокую активность кибермошенников, использующих как уже ставшие традиционными, так и новые сценарии обмана пользователей. В российском сегменте интернета наибольшее распространение вновь получили схемы с применением мошеннических сайтов нескольких форматов. Одними из них были поддельные интернет-ресурсы онлайн-магазинов и социальных сетей с промоакциями и розыгрышами подарков якобы от их имени. Потенциальные жертвы на таких сайтах всегда «выигрывают», но для получения несуществующего приза от них требуют оплатить «комиссию».

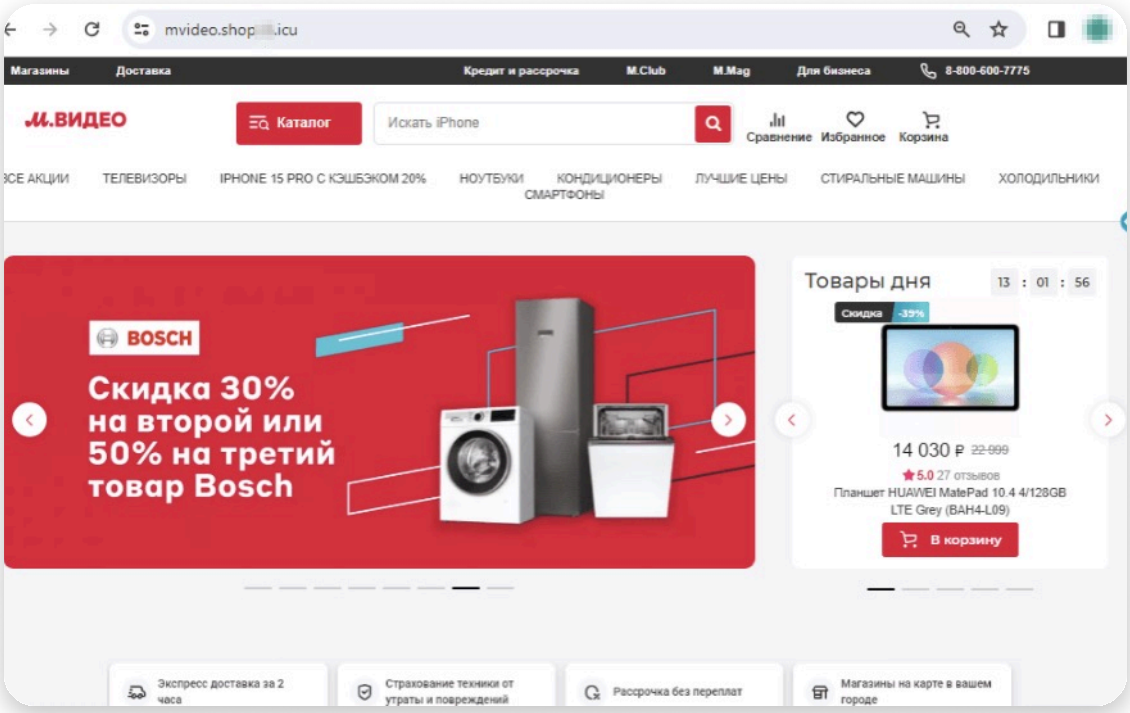


Мошеннический сайт, якобы имеющий отношение к российскому интернет-магазину, предлагает посетителю принять участие в несуществующем розыгрыше призов

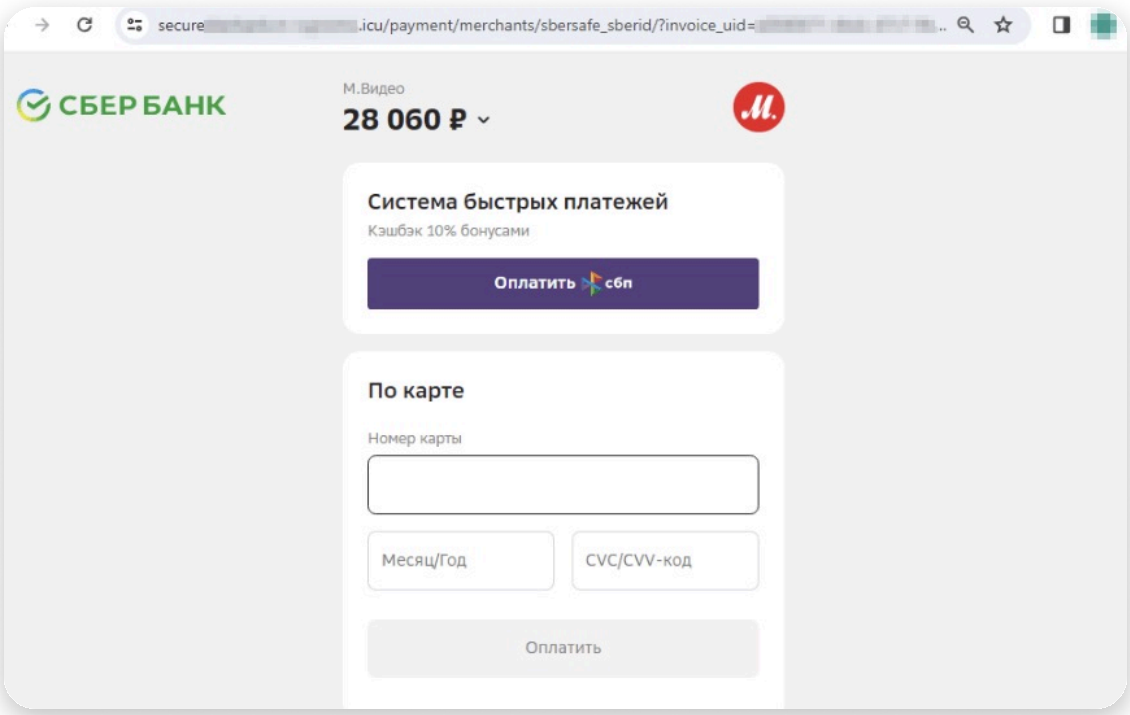


Поддельный сайт социальной сети предлагает «испытать удачу» и выиграть крупные денежные призы и другие подарки

Одним из актуальных вариантов такой схемы остаются поддельные сайты ритейлеров и магазинов бытовой техники и электроники, предлагающие приобрести товары со скидкой. Обычно для оплаты «заказов» на них предлагается воспользоваться интернет-банком или банковской картой, но в минувшем году мошенники стали прибегать к СБП — Системе быстрых платежей.

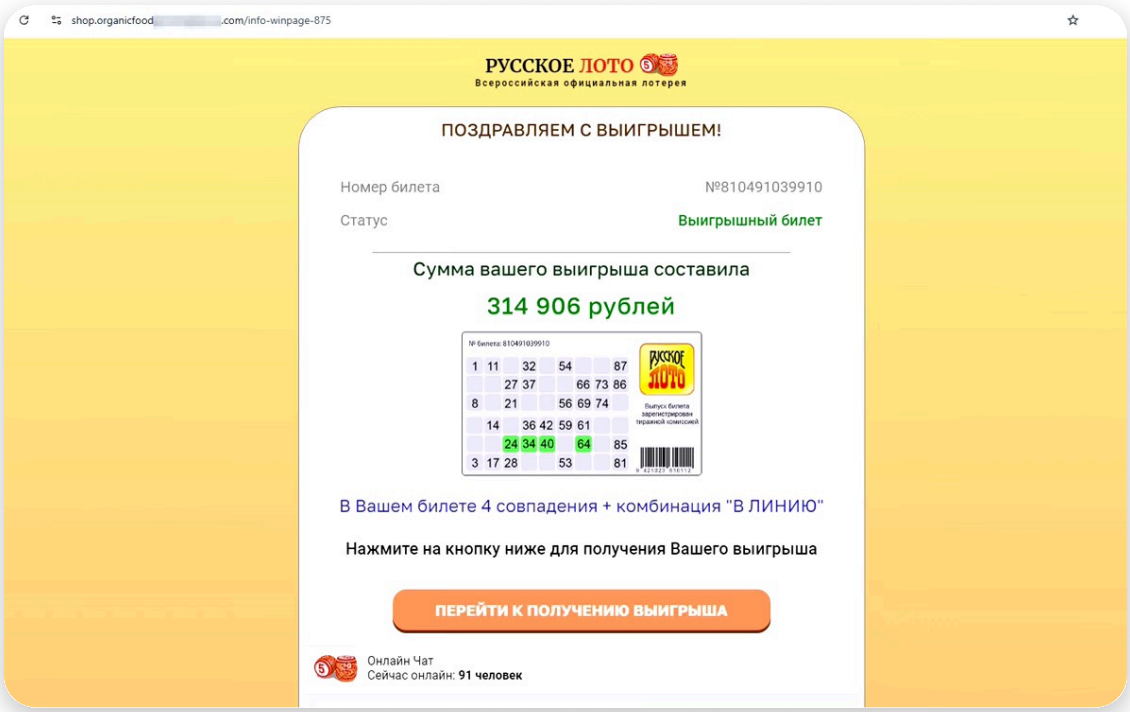


Поддельный сайт магазина бытовой техники и электроники обещает потенциальным жертвам большие скидки



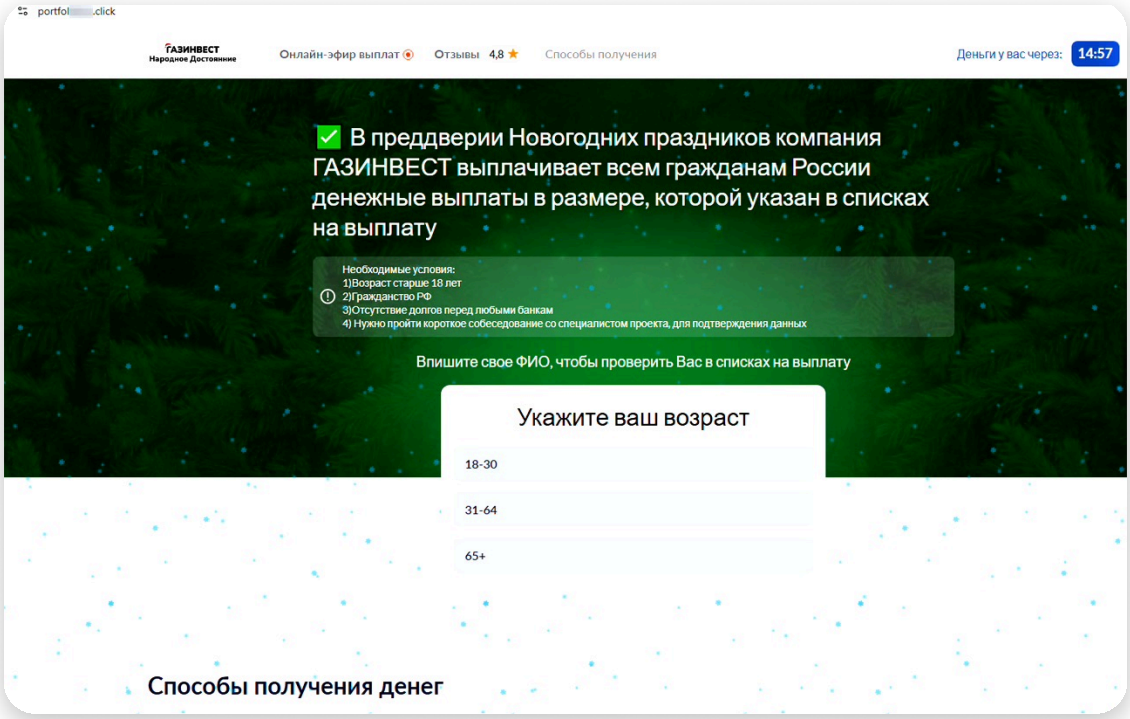
Мошеннический сайт предлагает воспользоваться СБП в качестве одного из способов оплаты «заказа»

Сохранила популярность и схема с «бесплатными» лотерейными билетами. Якобы проводимые онлайн-розыгрыши для потенциальных жертв всегда заканчиваются «победой». Чтобы получить приз, пользователи также должны оплатить «комиссию».

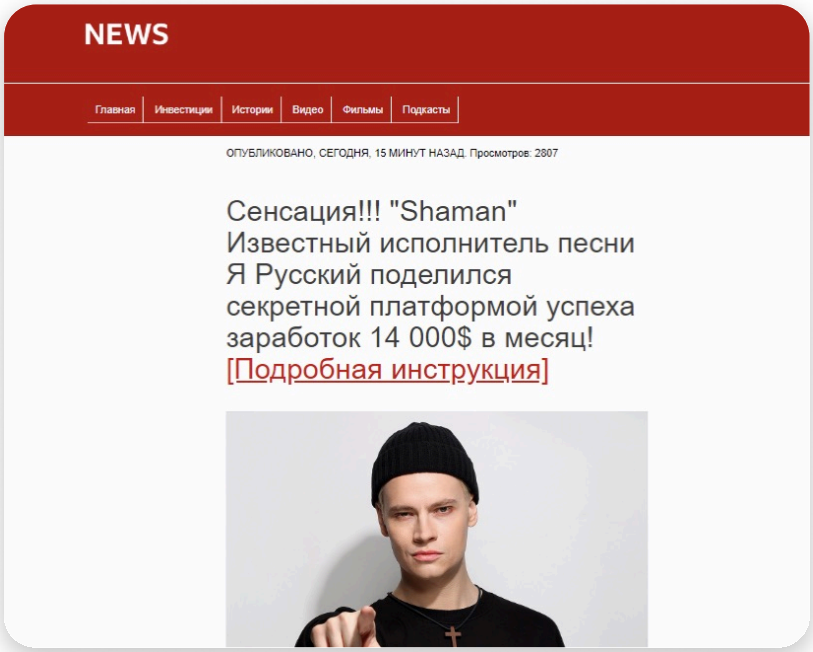


Пользователь якобы выиграл 314 906 рублей в лотерею и для «получения» выигрыша должен будет оплатить «комиссию»

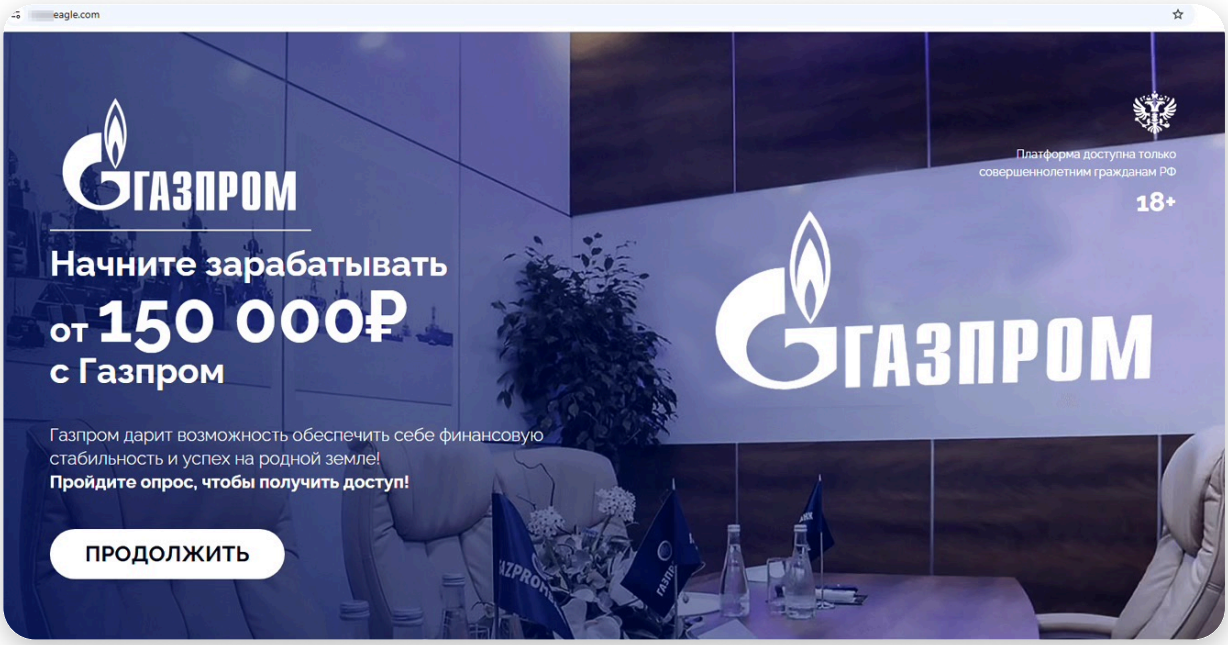
Поддельные сайты финансовой тематики тоже остались в арсенале мошенников. Популярностью пользовались такие темы как получение неких выплат от государства или частных компаний, инвестиции в нефтегазовый сектор, обучение финансовой грамотности, торговля криптовалютой и акциями с использованием «уникальных» автоматизированных систем или «проверенных» стратегий, якобы гарантирующих прибыль, и другие. Злоумышленники в том числе эксплуатировали имена медийных персон для привлечения внимания пользователей. Примеры таких сайтов представлены ниже.



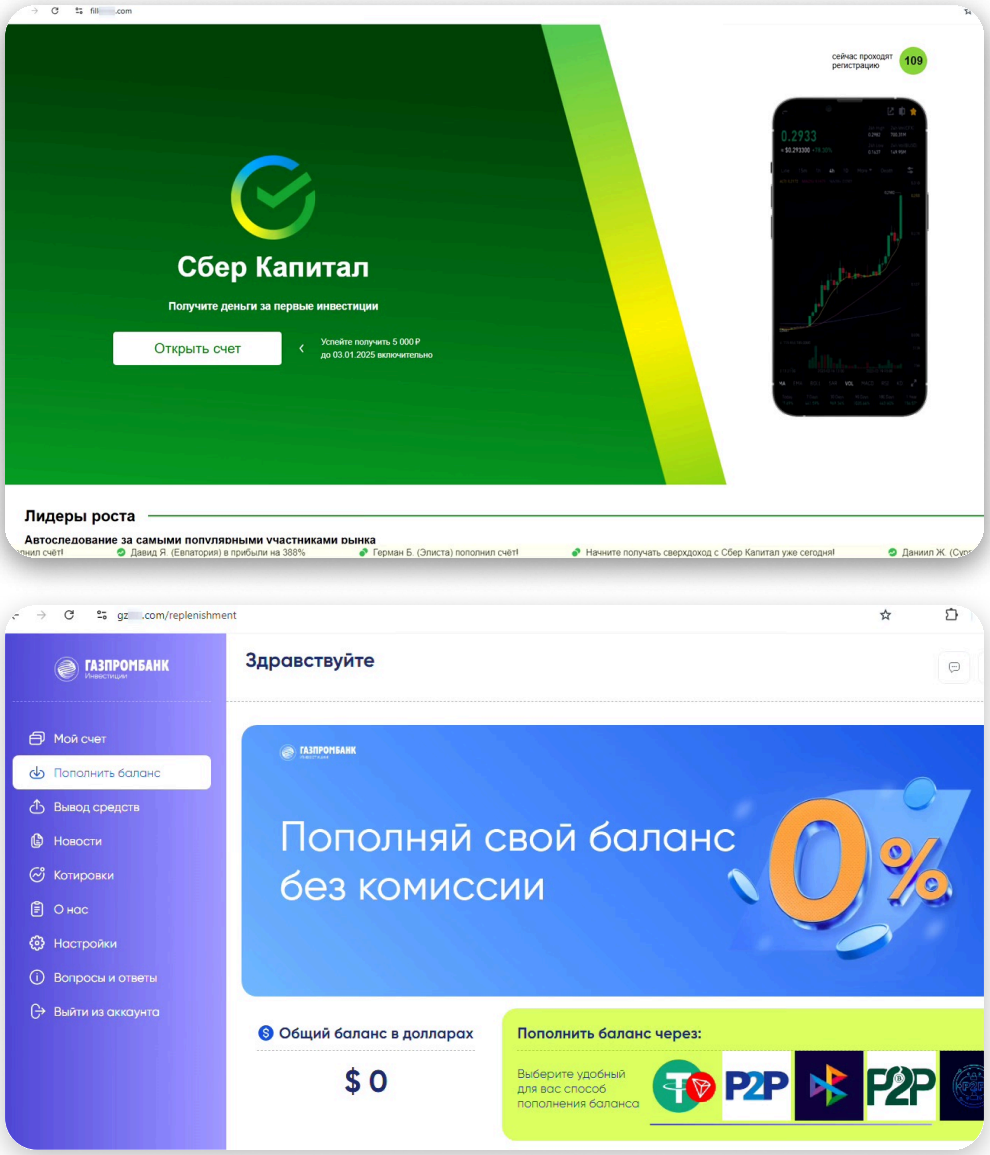
Мошеннический сайт предлагает посетителю «заработать до €10 000 в месяц на уникальной платформе WhatsApp»



Российский исполнитель Shaman «поделился секретной платформой успеха», которая якобы может принести заработок в $14 000 в месяц

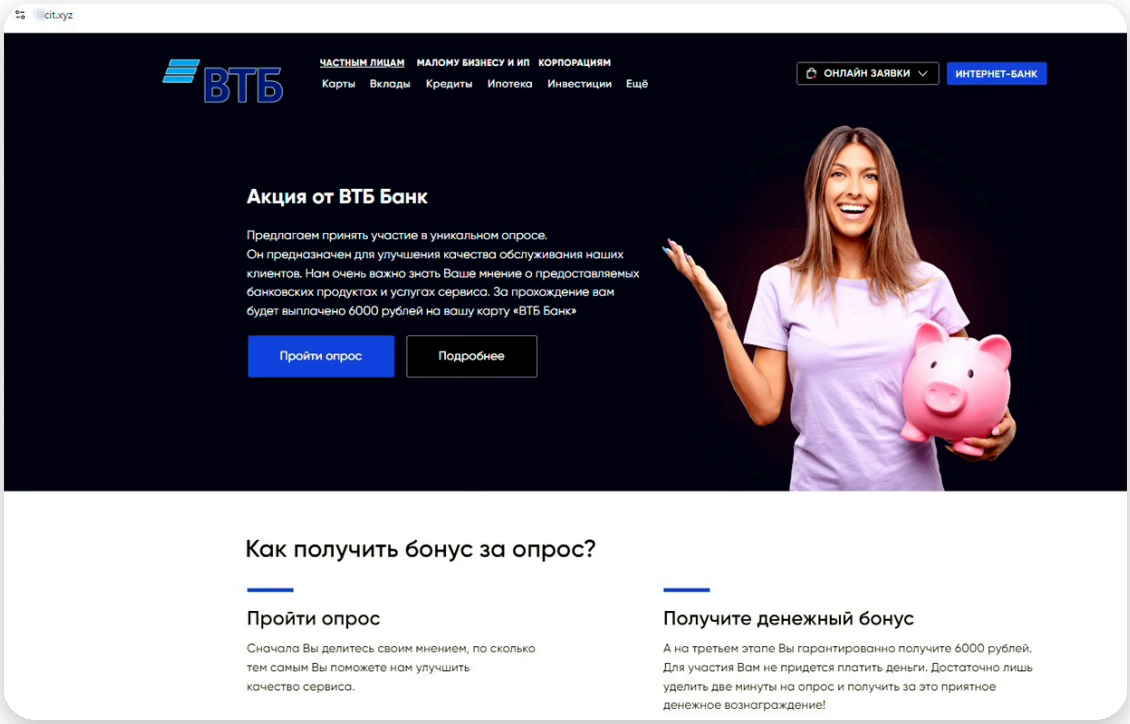


Поддельный сайт нефтегазовой компании предлагает получить доступ к инвестиционному сервису и обещает заработок от 150 000 рублей



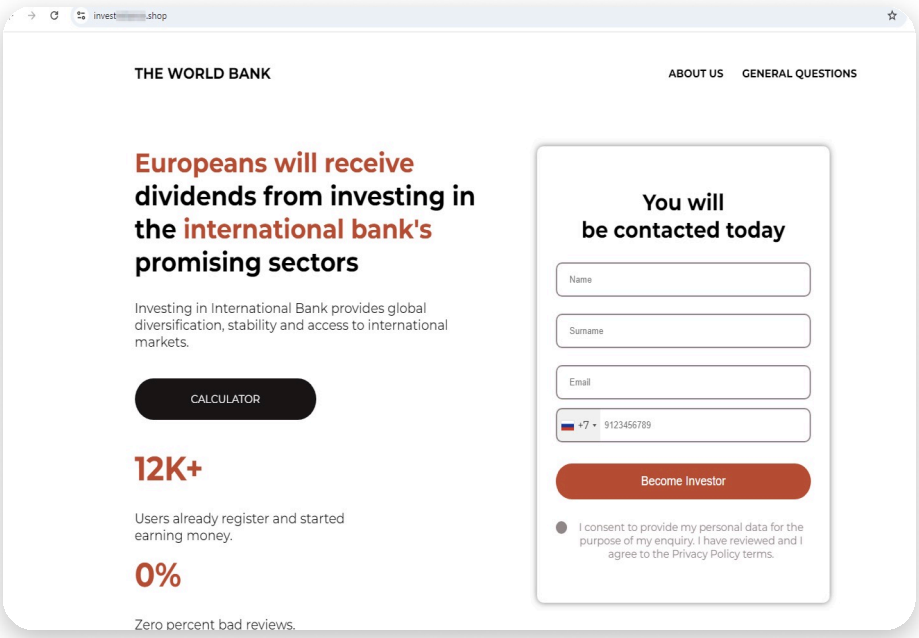
Мошеннические сайты, имитирующие настоящие инвестиционные сервисы банков

Вместе с тем наши специалисты выявили и новые схемы. Например, мошенники якобы от имени крупных компаний предлагали пользователям за вознаграждение принять участие в опросах о качестве предоставляемых услуг. Среди таких подделок встречались фиктивные сайты кредитных организаций, где у пользователей запрашивались чувствительные персональные данные, которые могли включать полное имя, привязанный к учетной записи банка номер мобильного телефона и номер банковской карты.

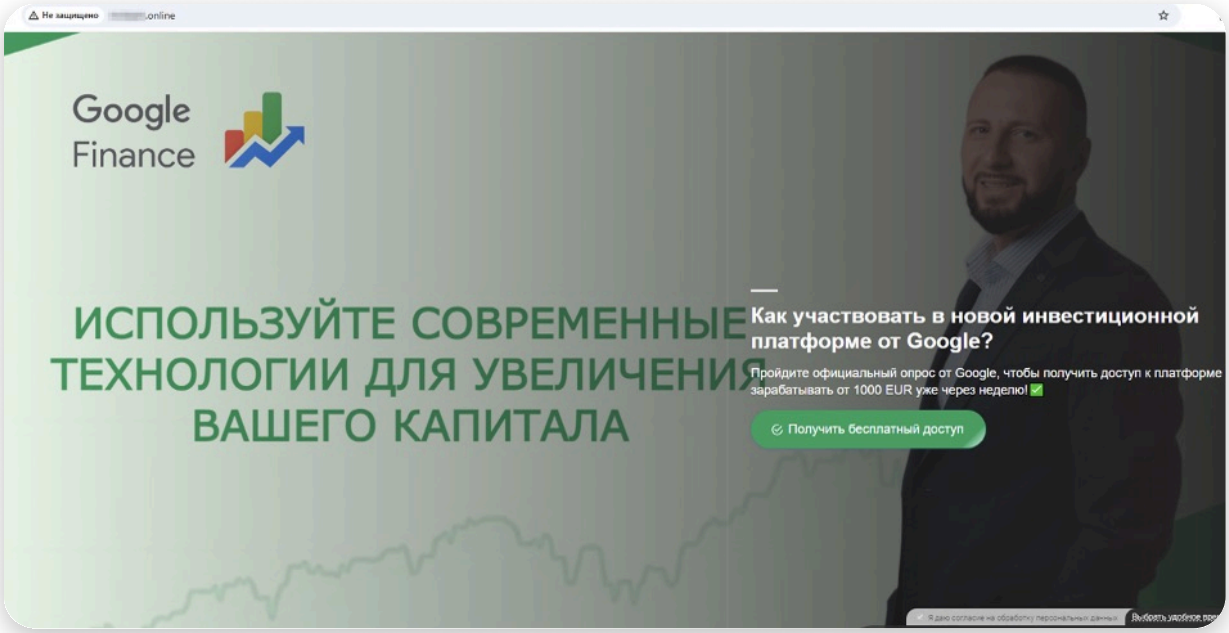


Поддельный сайт банка предлагает за вознаграждение в 6 000 рублей принять участие в опросе для «улучшения качества обслуживания»

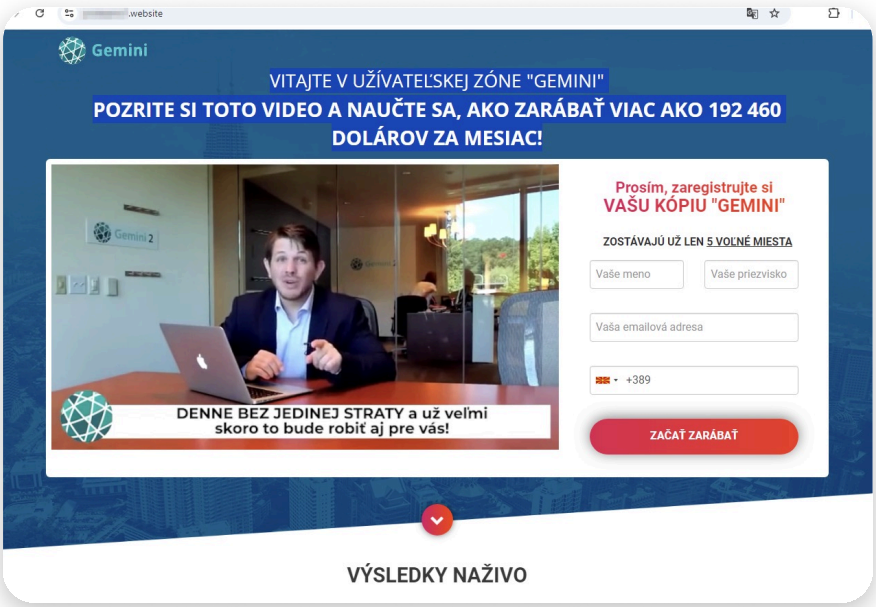
В то же время подобные подделки не обошли стороной и пользователей из других стран. Например, представленный ниже сайт обещал европейским пользователям дивиденды за инвестирование в перспективные секторы экономики:



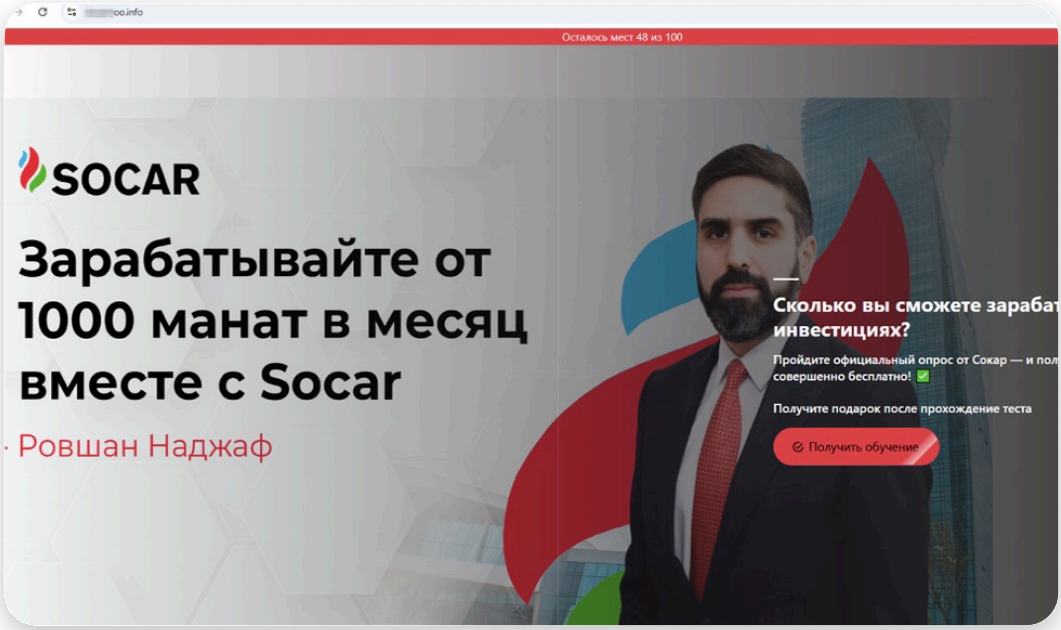
А этот сайт рекламировал «новую инвестиционную платформу от Google», с помощью которой якобы возможно зарабатывать от €1000:



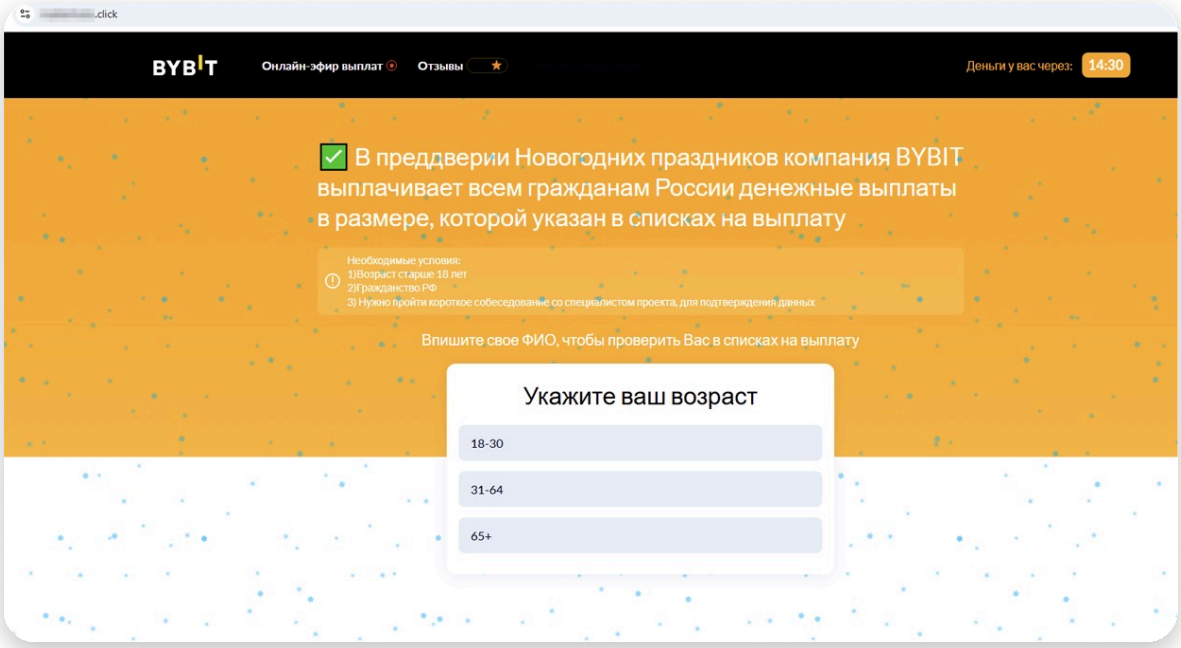
Другой мошеннический интернет-ресурс предлагал словацким пользователям «заработать более $192 460 в месяц» с помощью некоего инвестиционного сервиса:



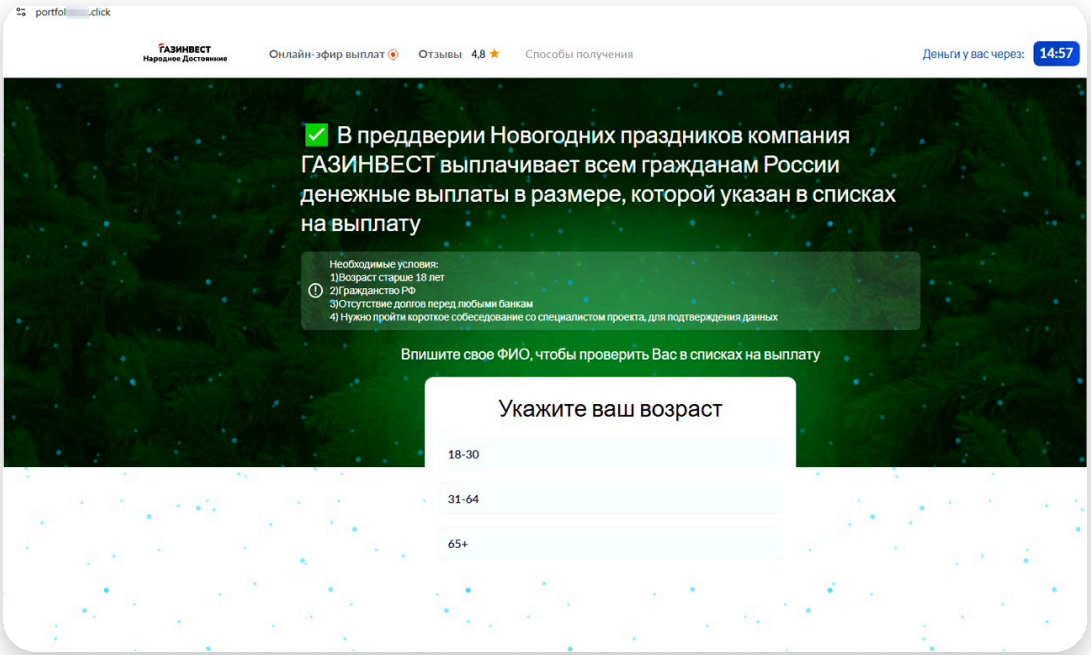
Жители Азербайджана тоже якобы могли существенно улучшить свое материальное положение, зарабатывая от 1000 манат в месяц. От них требовалось лишь пройти небольшой опрос и получить доступ к сервису, якобы имевшему отношение к азербайджанской нефтегазовой компании:



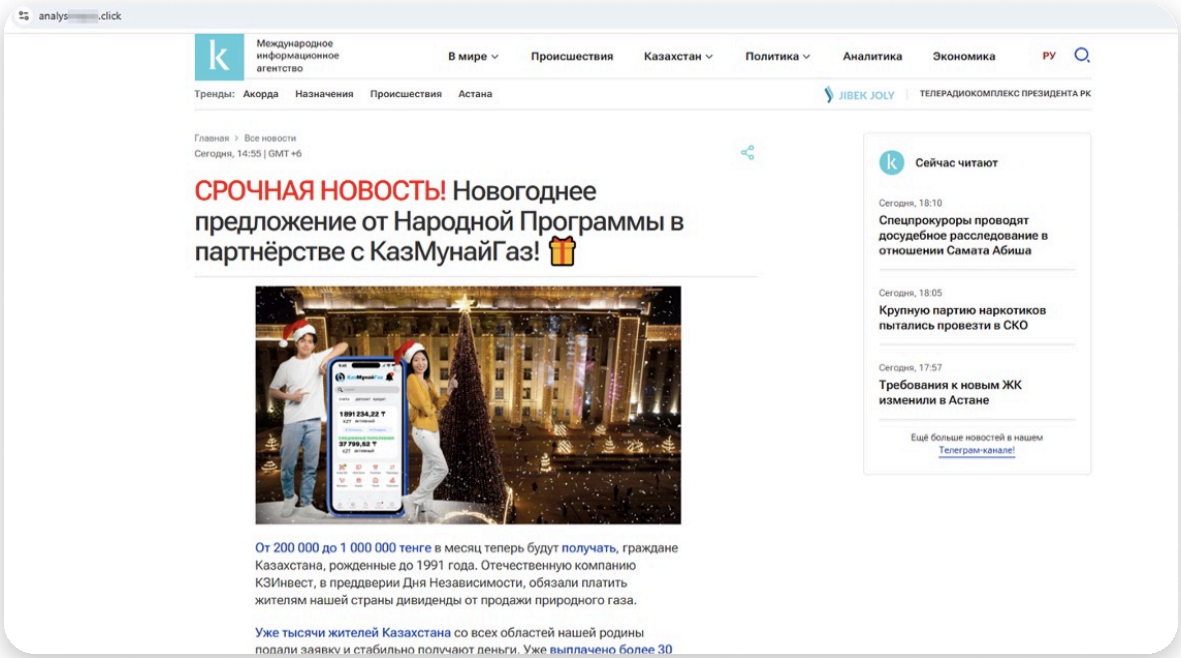
В конце года мошенники традиционно стали адаптировать такие сайты-подделки под тематику новогодних праздников. Например, следующий поддельный интернет-ресурс криптобиржи обещал российским пользователям новогодние выплаты:



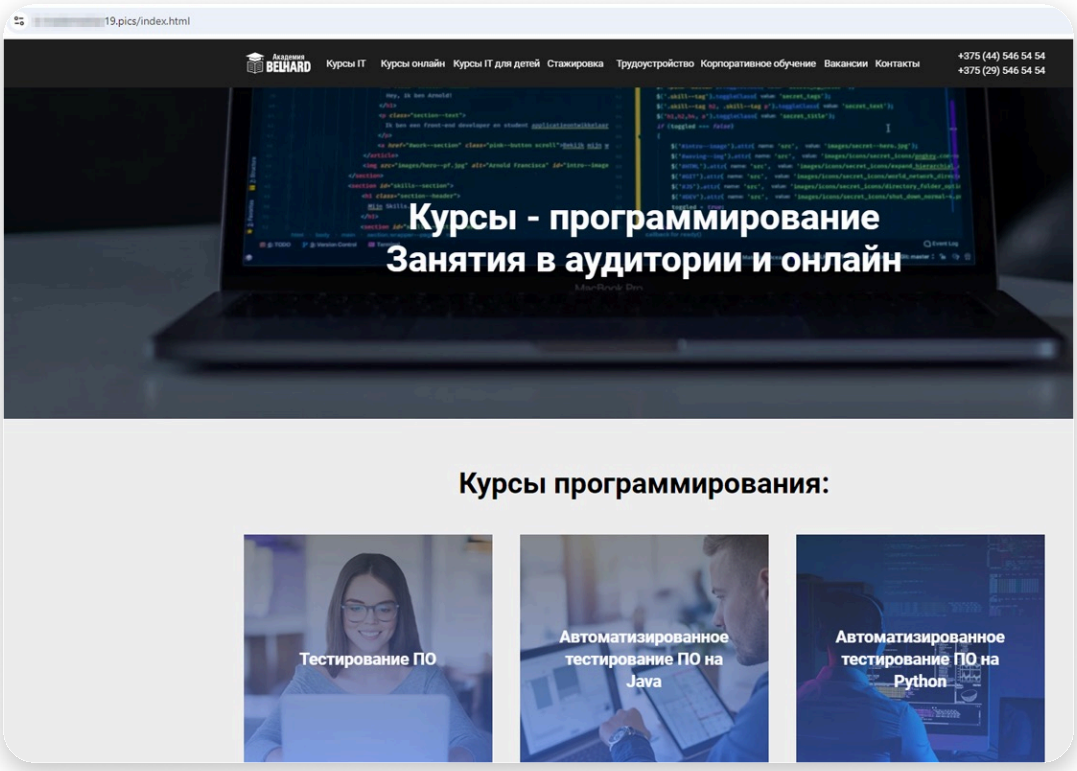
Другой сайт предлагал им праздничные выплаты якобы от имени инвестиционной компании:



А этот мошеннический интернет-ресурс сулил пользователям из Казахстана крупные выплаты в честь Дня независимости в рамках «новогоднего предложения»:

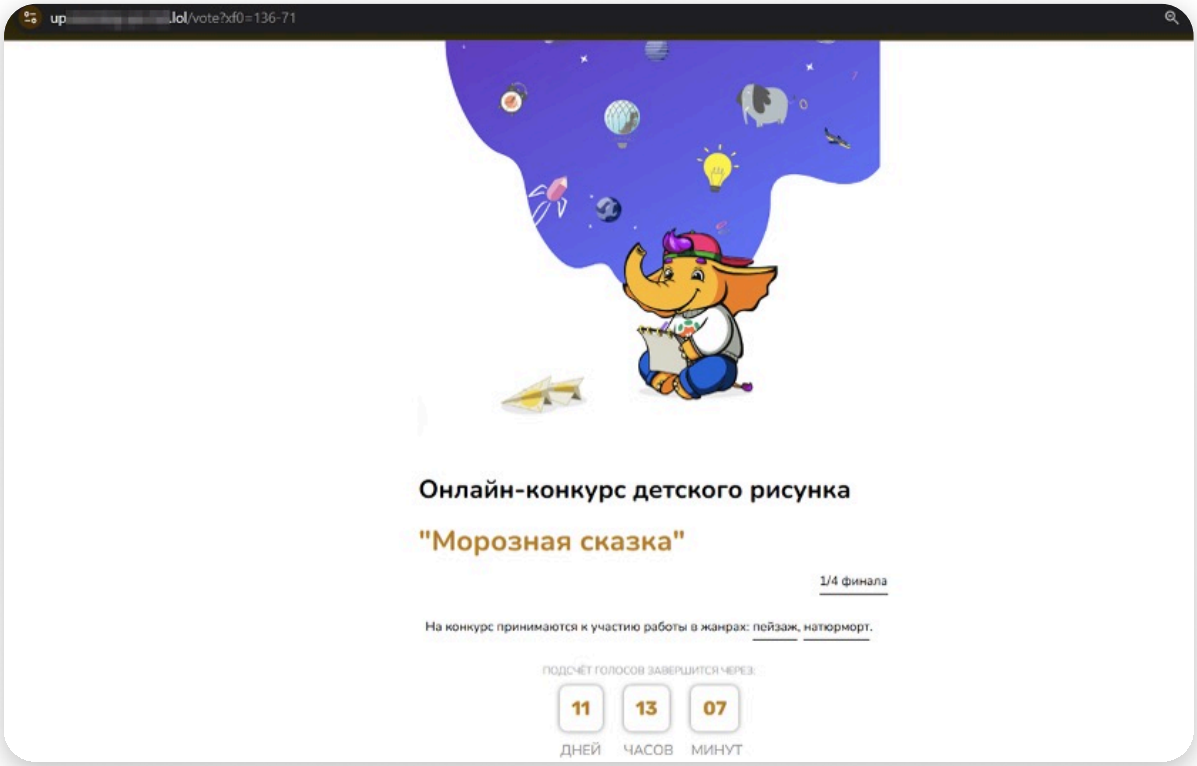


На протяжении всего года наши интернет-аналитики выявляли и другие фишинговые сайты. Среди них были поддельные сайты сервисов онлайн-обучения. Один из них, например, имитировал внешний вид настоящего интернет-ресурса и предлагал курсы по программированию. Для «получения консультации» от пользователей требовалось указать персональные данные.



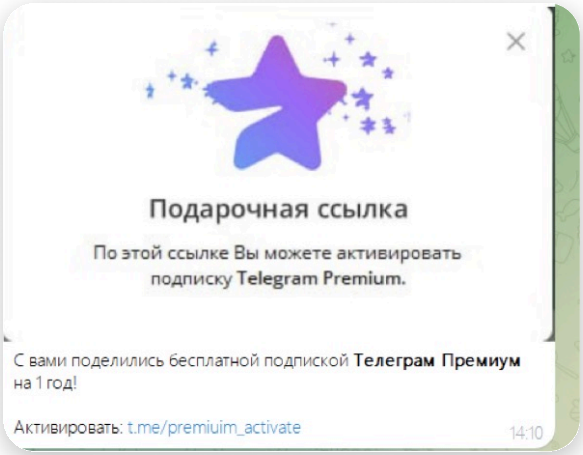
Поддельный сайт, который маскировался под настоящий онлайн-ресурс образовательного сервиса

Кроме того, не прекращались попытки похитить учетные записи пользователей Telegram с применением фишинговых сайтов, замаскированных под различные онлайн-голосования. Среди них распространение вновь получили сайты с «голосованиями в конкурсах детских рисунков». У потенциальных жертв запрашивается номер мобильного телефона — он якобы нужен для подтверждения голоса и получения одноразового кода. Однако при вводе этого кода на таком сайте пользователи открывают мошенникам доступ к своим учетным записям.

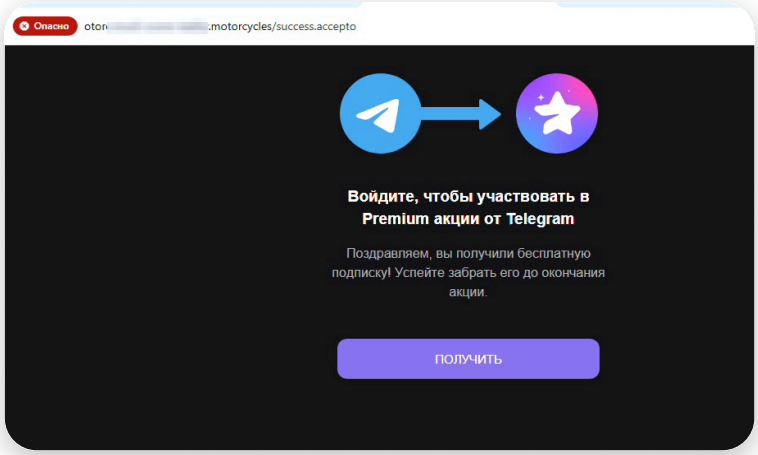


Фишинговый сайт для «голосования» в онлайн-конкурсе детских рисунков

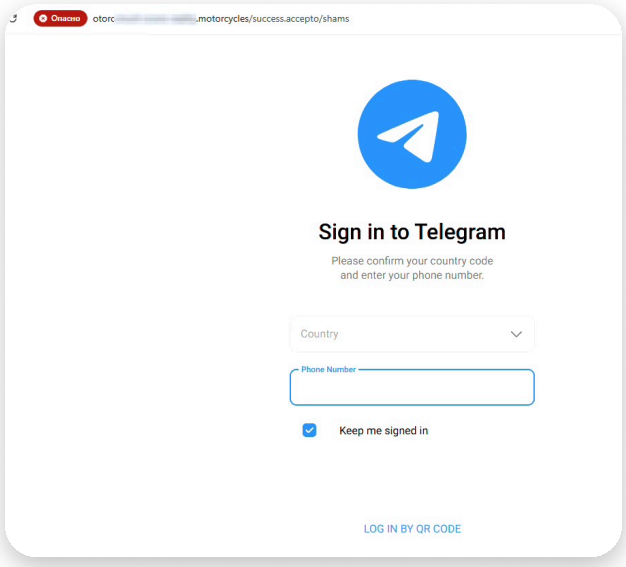
На других подобных сайтах предлагалось «бесплатно» получить подписку на Telegram Premium. Пользователей просят войти в свою учетную запись, однако вводимые на этих сайтах конфиденциальные данные передаются злоумышленникам, которые затем похищают аккаунты. Примечательно, что ссылки на эти интернет-ресурсы распространяются в том числе через сам мессенджер. При этом реальный адрес целевого сайта в сообщениях часто не совпадает с тем, что видят пользователи.



Фишинговое сообщение в Telegram, в котором для «активации» подписки на Telegram Premium предлагается перейти по указанной ссылке. Текст ссылки на самом деле не совпадает с целевым адресом



Фишинговый сайт, загруженный при переходе по ссылке из мошеннического сообщения

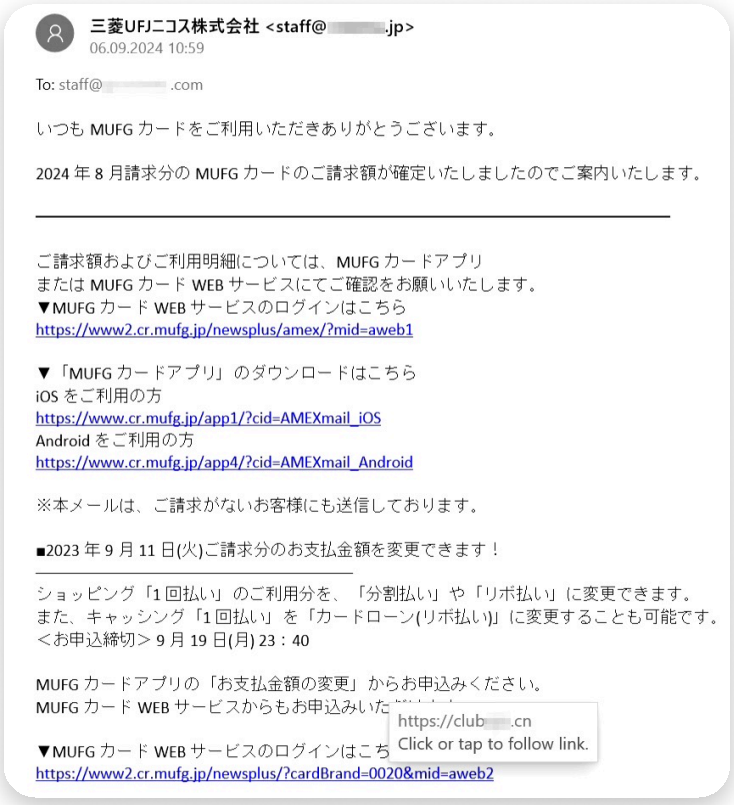


После нажатия на кнопку на предыдущей странице сайт демонстрирует форму авторизации, которая выглядит как настоящая форма авторизации Telegram

Для распространения ссылок на мошеннические сайты киберпреступники используют в том числе почтовый спам. В течение года наши интернет-аналитики фиксировали множество различных спам-кампаний. Так, наблюдалось активное распространение фишинговых писем, нацеленных на японских пользователей. Например, мошенники якобы от имени той или иной кредитной организации информировали потенциальных жертв о некой покупке и предлагали им ознакомиться с деталями «платежа», перейдя по предоставленной ссылке. На самом деле она вела на фишинговый интернет-ресурс.

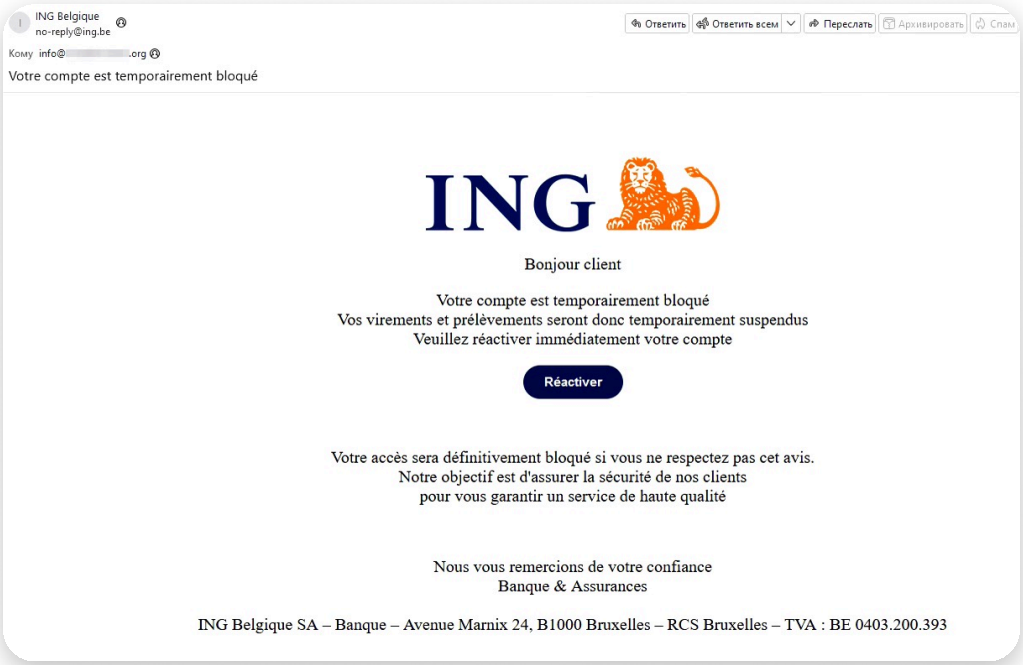
Фишинг-письмо, якобы от имени банка предлагающее японским пользователям ознакомиться с деталями некоего платежа

В другом популярном сценарии злоумышленники якобы от имени кредитных организаций рассылали поддельные уведомления с информацией о расходах по банковской карте за месяц. При этом ссылки на фишинговые сайты часто маскировались и в тексте писем выглядели безобидно.



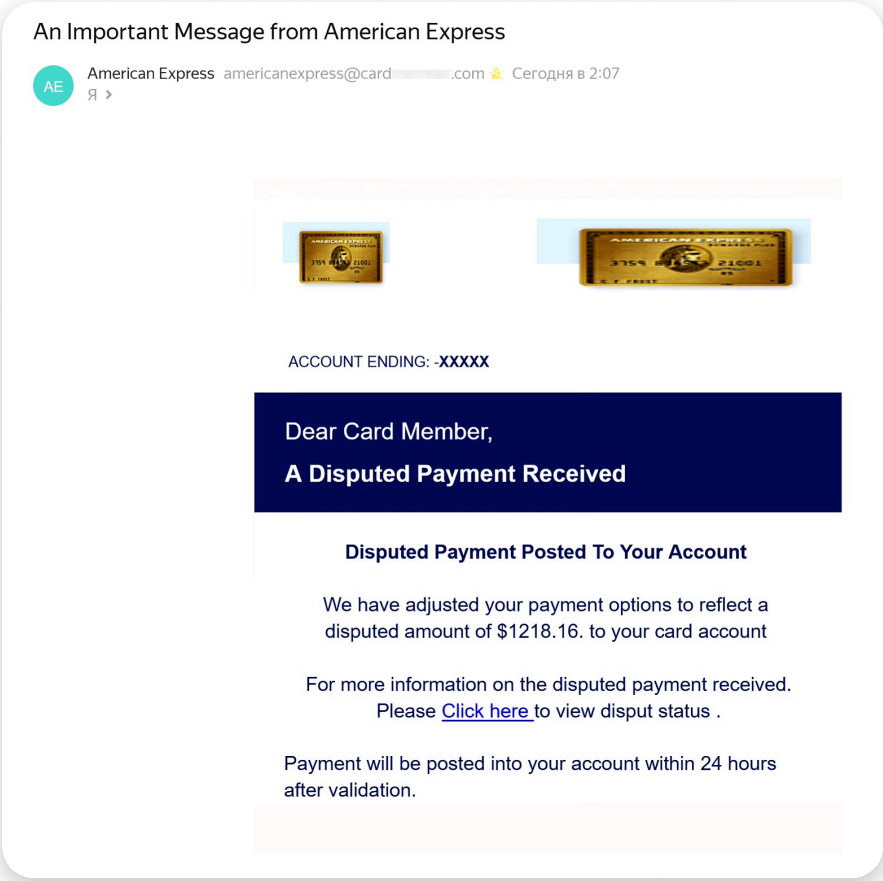
Пользователи в текстах спам-писем видели ссылки на настоящие адреса сайтов банков, но те при нажатии вели на мошеннический интернет-ресурс

Одна из спам-кампаний была нацелена на европейских пользователей. Например, пользователи из Бельгии сталкивались с фишинговыми письмами, которые сообщали о «блокировке» их банковских счетов. Для «разблокировки» им предлагалось перейти по ссылке, которая на самом деле вела на сайт мошенников.



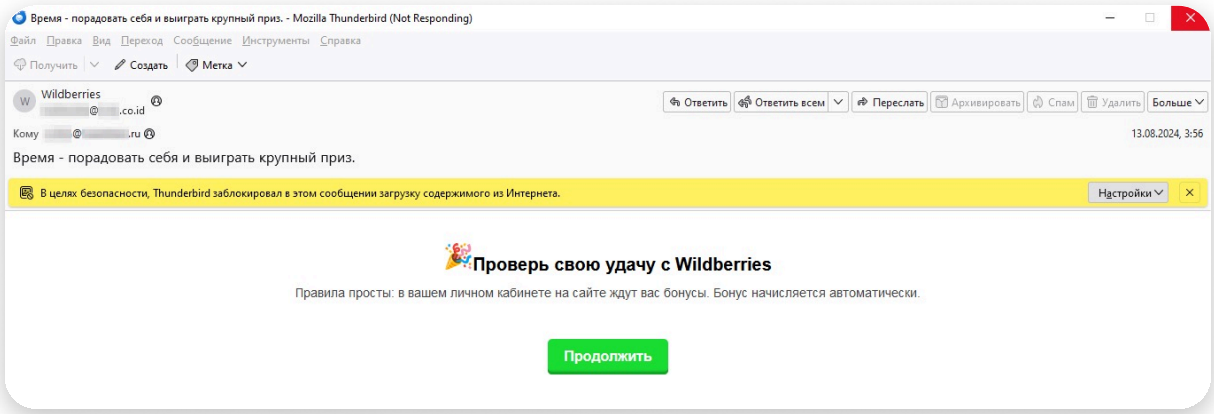
Нежелательное письмо пугает потенциальную жертву «заблокированным» банковским аккаунтом

Фиксировались и другие массовые рассылки нежелательных писем — например, рассчитанных на англоязычную аудиторию. В одной из спам-кампаний потенциальные жертвы получали сообщения, в которых предлагалось подтвердить получение крупного денежного перевода. Однако ссылка в них вела на фишинговую форму авторизации в онлайн-банке, которая напоминала настоящую страницу сайта кредитной организации.

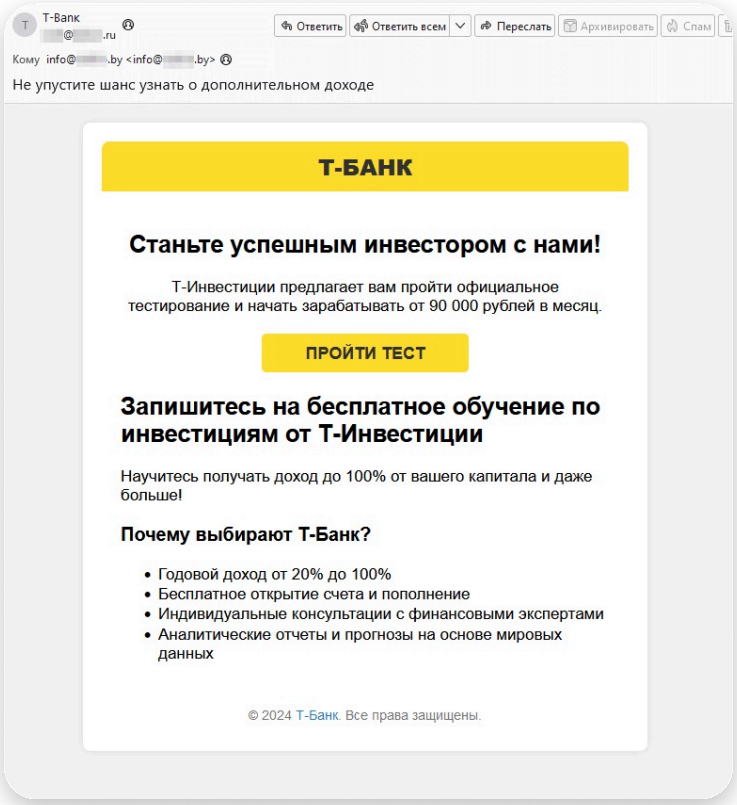


Спам-письмо сообщает, что пользователю якобы необходимо подтвердить получение $1218,16 США

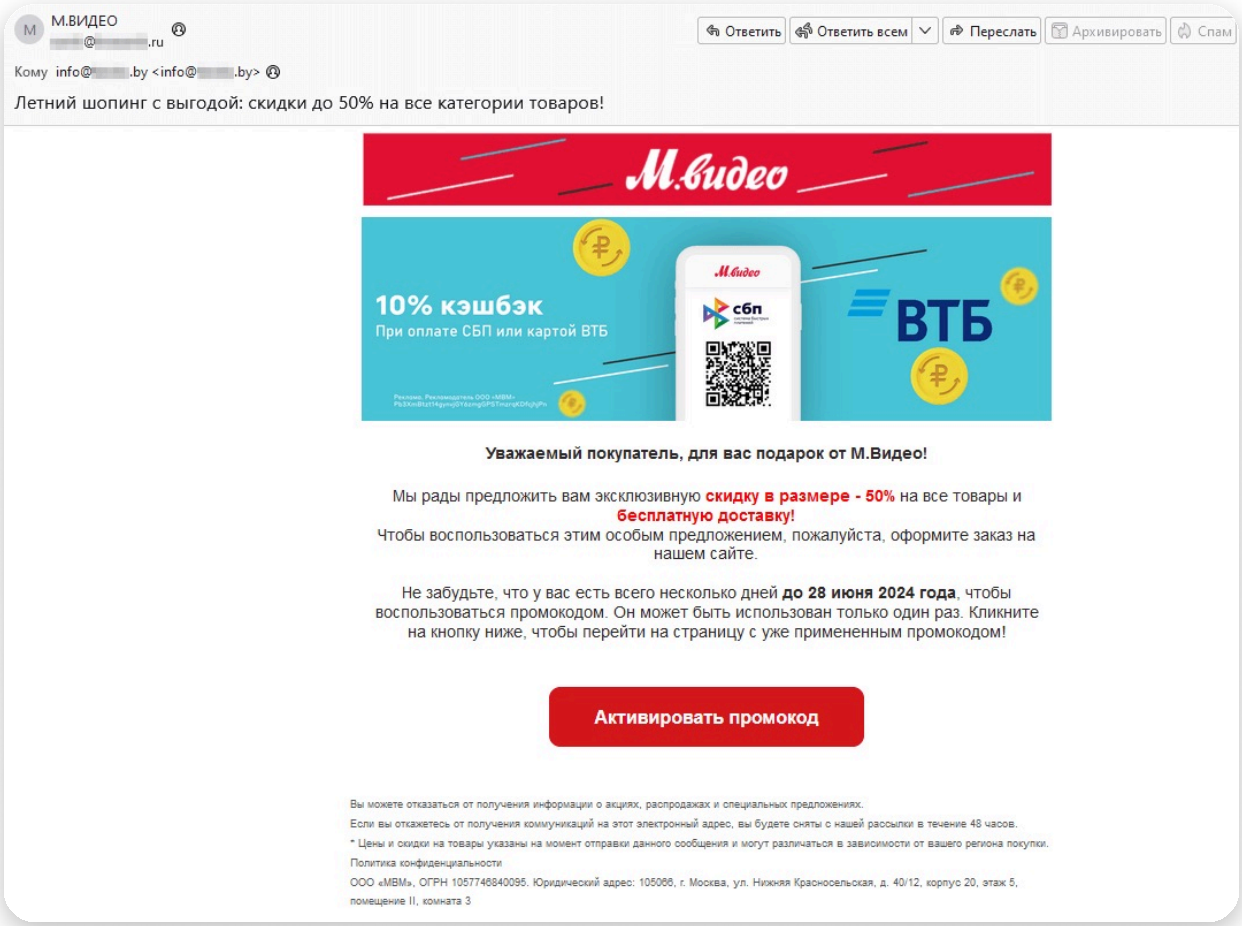
Российские пользователи чаще всего сталкивались со спам-письмами, которые помогали мошенникам заманивать потенциальных жертв на ранее отмеченные популярные фишинговые сайты. Распространенной тематикой нежелательных сообщений были призы и скидки от интернет-магазинов, бесплатные лотерейные билеты, доступ к инвестиционным сервисам. Их примеры показаны на скриншотах ниже.



Письмо якобы от имени интернет-магазина, в котором предлагается участие в «розыгрыше призов»



Письмо якобы от имени кредитной организации, предлагающее «стать успешным инвестором»



Письмо, отправленное якобы от имени магазина электроники, в котором предлагается активировать промокод и получить скидку на товары

Для мобильных устройств

Согласно статистике детектирований Dr.Web Security Space для мобильных устройств, самыми распространенными вредоносными Android-программами в 2024 году вновь стали трояны Android.HiddenAds, которые скрывают присутствие на зараженных устройствах и показывают рекламу. На них пришлось более трети детектирований вредоносного ПО. Среди наиболее активных представителей этого семейства оказались Android.HiddenAds.3956, Android.HiddenAds.3851, Android.HiddenAds.655.origin и Android.HiddenAds.3994. В то же время пользователи сталкивались с вариантами троянов Android.HiddenAds.Aegis, способными после установки запускаться автоматически. Другими распространенными вредоносными приложениями были используемые в различных мошеннических схемах трояны Android.FakeApp и шпионские трояны Android.Spy.

САМЫЕ РАСПРОСТРАНЕННЫЕ ВРЕДОНОСНЫЕ ANDROID-ПРОГРАММЫ

- Android.HiddenAds
- Android.FakeApp
- Android.Spy

Наиболее активными нежелательными программами стали представители семейств Program.FakeMoney, Program.CloudInject и Program.FakeAntiVirus. Первые предлагают выполнять различные задания за виртуальные вознаграждения, которые в дальнейшем якобы можно вывести в виде настоящих денег, однако на самом деле пользователи никаких выплат от них не получают. Вторые являются модифицированными программами, в которые при модификации через специализированный облачный сервис добавляются неконтролируемый код и ряд опасных разрешений. Третьи имитируют работу антивирусов, обнаруживают несуществующие угрозы и предлагают приобрести полную версию для исправления «проблем».

Утилиты Tool.SilentInstaller, которые позволяют запускать Android-приложения без их установки, вновь стали самыми часто детектируемыми потенциально опасными программами — на них пришлось более трети случаев обнаружения этого типа программ. Распространение также получили приложения, модифицированные при помощи утилиты NP Manager (детектируются как Tool.NPMod). В такие программы встраивается специальный модуль, позволяющий обходить проверку их цифровой подписи после модификации. Нередко выявлялись защищенные упаковщиком Tool.Packer.1.origin приложения, а также фреймворк Tool.Androlua.1.origin, позволяющий модифицировать установленные Android-программы и исполнять Lua-скрипты, которые потенциально могут быть вредоносными.

Самым распространенным рекламным ПО стало новое семейство Adware.ModAd — его доля составила почти половину детектирований. Это специальным образом модифицированные версии мессенджера WhatsApp, в функции которых внедрен код для загрузки рекламных ссылок. Вторыми оказались представители семейства Adware.Adpush, а третьими — еще одно новое семейство, Adware.Basement.

По сравнению с 2023, в 2024 году несколько возросла активность банковских троянов для ОС Android. При этом наши специалисты отмечали рост популярности ряда техник, которые киберпреступники применяли для защиты вредоносного ПО — в частности банкеров — от анализа и детектирования. Среди таких методик были различные манипуляции с форматом ZIP-архивов (являются основой APK-файлов) и файлом конфигурации Android-программ `AndroidManifest.xml`.

Отдельно стоит отметить широкое распространение вредоносного приложения Android.SpyMax. Злоумышленники активно использовали эту программу-шпиона в качестве банковского трояна, в частности против российских пользователей (46,23% случаев детектирования), а также владельцев Android-устройств из Бразилии (35,46% случаев) и Турции (5,80% случаев).

На протяжении всего года вирусные аналитики «Доктор Веб» выявляли свыше 200 различных угроз в каталоге Google Play. Среди них — подписывающие на платные услуги трояны, трояны-шпионы, мошенническое и рекламное ПО. Суммарно их загрузили по меньшей мере 26 700 000 раз. Кроме того, наши специалисты зафиксировали очередную атаку на ТВ-приставки с ОС Android: модульный бэкдор Android.Vo1d заразил почти 1 300 000 устройств у пользователей из 197 стран. Этот троян помещал свои компоненты в системную область и по команде злоумышленников мог скрытно загружать из интернета и устанавливать стороннее ПО.

Более подробно о вирусной обстановке для мобильных устройств в 2024 году читайте в нашем обзоре.

Перспективы и вероятные тенденции

События минувшего года в очередной раз продемонстрировали разнообразие современного ландшафта киберугроз. Злоумышленников интересуют как крупные цели — корпоративный и государственный сектор, — так и рядовые пользователи. Функциональность многих вредоносных программ, задействованных в проанализированных нами таргетированных атаках, говорит о постоянном поиске вирусописателями новых возможностей в совершенствовании методов проведения вредоносных кампаний и развития своего инструментария. Со временем новые приемы неизбежно переносятся на более массовые угрозы. В этой связи в 2025 году возможно появление большего числа троянов, которые для сокрытия вредоносной активности будут эксплуатировать технологию eBPF. Кроме того, стоит ожидать и новых таргетированных атак, в том числе с применением эксплойтов.

Одной из главных целей киберпреступников является незаконное обогащение, поэтому в новом году возможен рост активности банковских и рекламных троянов. Кроме того, пользователям может угрожать больше вредоносных программ со шпионской функциональностью.

В то же время под прицелом окажутся пользователи не только Windows-компьютеров, но и других операционных систем, таких как Linux и macOS. Продолжится распространение и мобильных угроз. Владельцам Android-устройств в первую очередь следует опасаться появления нового шпионского ПО, банковских троянов, а также вредоносных и нежелательных рекламных приложений. Не исключены новые попытки заражений телевизоров, ТВ-приставок и другого оборудования на базе Android. Кроме того, вероятно 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