Dr.WEB

«Доктор Веб»:

обзор вирусной активности за 2023 год

«Доктор Веб»: обзор вирусной активности за 2023 год

В 2023 году одними из самых активных угроз вновь стали троянские приложения Trojan.AutoIt, созданные с использованием скриптового языка AutoIt. Они распространяются в составе других вредоносных приложений и затрудняют их обнаружение. Также наблюдалась высокая активность рекламных троянских программ Trojan.BPlug и различных вредоносных скриптов. В почтовом трафике чаще всего встречались вредоносные скрипты, а также фишинговые документы. Кроме того, злоумышленники активно распространяли вредоносные программы, эксплуатирующие уязвимости документов Microsoft Office. Часть распространяемых по электронной почте угроз пришлась на различные троянские приложения.

По сравнению с предыдущим годом, в 2023 снизилось число обращений пользователей за расшифровкой файлов. При этом также наблюдалось снижение количества детектирований банковских троянских программ.

Минувший год запомнился рядом событий в сфере информационной безопасности. Весной наши специалисты зафиксировали атаку Android-троянов, которые заражают смарт-телевизоры и приставки с Android TV. Летом вирусные аналитики «Доктор Веб» выявили трояна, предназначенного для кражи криптовалют. Он скрывался в некоторых пиратских сборках Windows 10 и при заражении компьютеров инфицировал системный EFI-раздел. Уже осенью мы сообщили об атаке шпионских троянских приложений на иранских пользователей Android. Эти вредоносные программы похищали персональные данные и деньги жертв. Кроме того, наша компания предупредила о распространении вредоносных плагинов для сервера обмена сообщениями Openfire. Они эксплуатировали одну из уязвимостей в ПО Openfire и выполняли различные команды злоумышленников.

Среди мобильных угроз наибольшее распространение получили рекламные троянские приложения, вредоносные программы-шпионы, а также нежелательное рекламное ПО. При этом в каталоге Google Play было выявлено множество новых вредоносных приложений с почти полумиллиардным суммарным числом установок. Также наши специалисты обнаружили очередных троянов — похитителей криптовалют, нацеленных не только на пользователей ОС Android, но и на владельцев устройств под управлением iOS.

Главные тенденции года

- Широкое распространение троянов, созданных с использованием скриптового языка AutoIt
- Широкое распространение вредоносных программ, демонстрирующих рекламу
- Снижение числа инцидентов с троянскими программами-вымогателями
- Появление новых семейств банковских троянов
- Появление множества новых угроз в каталоге Google Play
- Высокая активность интернет-мошенников

Наиболее интересные события 2023 года

В мае 2023 года компания «Доктор Веб» рассказала о троянском модуле Android.Spy.SpinOk, который предлагался разработчикам Android-игр и программ в качестве маркетингового инструмента, но при этом обладал шпионской функциональностью. Он собирал информацию о хранящихся на устройствах файлах и мог передавать их злоумышленникам, а также был способен подменять и загружать содержимое буфера обмена на удаленный сервер. Кроме того, он мог демонстрировать рекламу. Наши вирусные аналитики выявили этот модуль в более чем ста приложениях, загруженных из Google Play свыше 421 000 000 раз. После выхода соответствующей публикации разработчик SpinOk обратился в компанию «Доктор Веб» с целью проверки и устранения причин классификации модуля как вредоносного. Впоследствии он был обновлен до версии 2.4.2, в которой троянская функциональность отсутствовала.

В июне наши специалисты обнаружили вредоносное приложение Trojan.Clipper.231 для кражи криптовалюты. Оно было встроено в ряд пиратских сборок Windows 10 и при заражении компьютеров проникало в системный EFI-раздел. Стилер подменял адреса криптокошельков в буфере обмена на адреса, заданные мошенниками. На момент обнаружения злоумышленникам с его помощью удалось похитить криптовалюту на сумму, эквивалентную порядка $19 000.

Уже в июле компания «Доктор Веб» выявила атаку на пользователей Windows, в ходе которой применялась модульная троянская программа-загрузчик Trojan.Fruity.1. С ее помощью злоумышленники в зависимости от своих целей могли заражать компьютеры различными типами вредоносных приложений. При этом киберпреступники предприняли ряд мер для повышения шансов атаки на успех. Например, Trojan.Fruity.1 распространялся в составе специально подготовленных установщиков популярных программ, которые загружались с вредоносных сайтов, а процесс заражения целевых систем благодаря модульной архитектуре трояна был многоступенчатым. Кроме того, для запуска компонентов Trojan.Fruity.1 использовались безобидные приложения, а при заражении системы выполнялась попытка обойти антивирусную защиту.

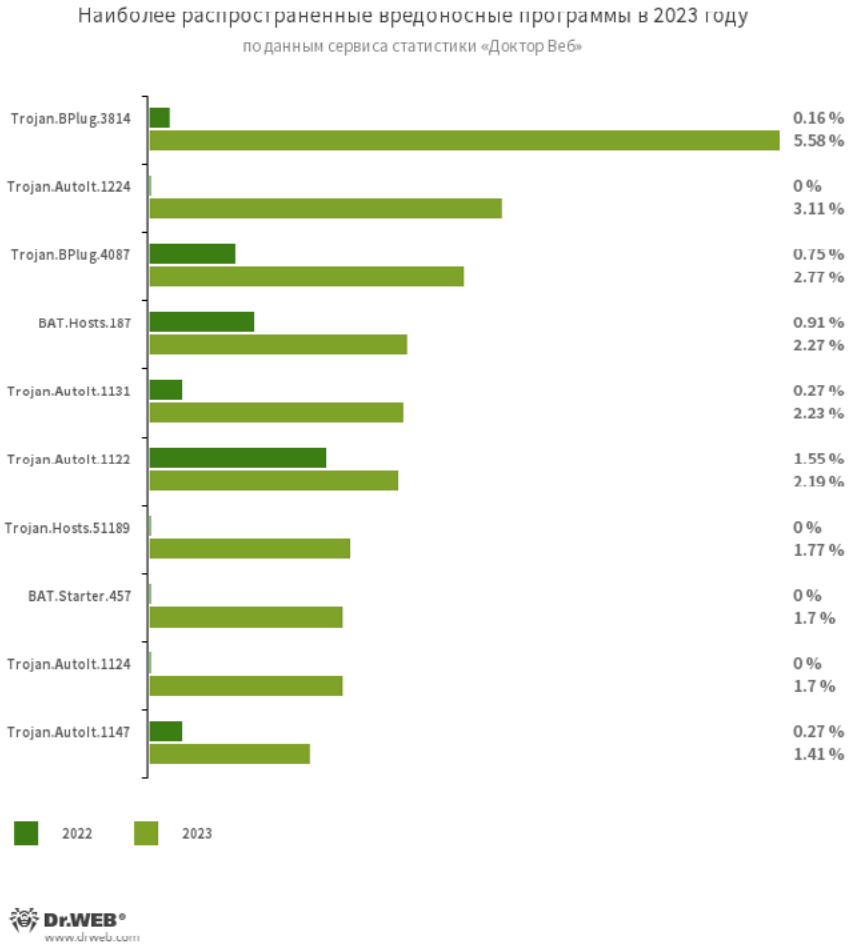
В начале сентября наша компания опубликовала исследование бэкдора Android.Pandora.2, который атаковал преимущественно испаноязычных пользователей. Различные модификации этого трояна заражают смарт-телевизоры и приставки с Android TV, куда попадают через скомпрометированные версии прошивок, а также при установке троянских версий ПО для нелегального просмотра видео онлайн. Массовые случаи атак с участием Android.Pandora.2 фиксировались в марте 2023 года. Первые модификации этой троянской программы были добавлены в вирусную базу Dr.Web еще в июле 2017 года.

Чуть позже мы сообщили о троянах семейства Android.Spy.Lydia, главной целью которых были иранские пользователи Android. Эти вредоносные программы предоставляли злоумышленникам удаленный доступ к инфицированным устройствам, обладали шпионской функциональностью и применялись для кражи персональной информации и денег.

А в конце сентября компания «Доктор Веб» предупредила о распространении вредоносных плагинов JSP.BackDoor.8 для сервера обмена сообщениями Openfire — они эксплуатировали уязвимость CVE-2023-32315 в этом продукте. Данная уязвимость позволяла хакерам получать доступ к файловой системе зараженных серверов и использовать их в составе ботнета. Троянские плагины специалисты вирусной лаборатории «Доктор Веб» обнаружили в ходе расследования атаки трояна-шифровальщика на инфраструктуру одного из клиентов нашей компании. Именно с помощью такого плагина на сервер с установленным уязвимым ПО Openfire и была совершена атака энкодера. Плагины JSP.BackDoor.8 являются созданными на языке Java бэкдорами, позволяющими выполнять ряд команд в виде GET- и POST-запросов, которые отправляют злоумышленники. С их помощью атакующие также могут получать информацию о скомпрометированном сервере — например, сведения о сетевых подключениях, IP-адресе, пользователях и версии ядра системы.

Вирусная обстановка

Анализ статистики детектирований антивируса Dr.Web за 2023 год показал увеличение общего числа обнаруженных угроз на 12,27% по сравнению с 2022 годом. Число уникальных угроз при этом возросло на 21,70%. Наиболее заметную активность проявили троянские приложения, которые распространяются в составе других вредоносных программ с целью затруднить их обнаружение. Кроме того, пользователи часто сталкивались с рекламными троянами и всевозможными вредоносными скриптами.



- Trojan.BPlug.3814
- Trojan.BPlug.4087

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

- Trojan.AutoIt.1224
- Trojan.AutoIt.1131
- Trojan.AutoIt.1124
- Trojan.AutoIt.1122
- Trojan.AutoIt.1147

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.

- BAT.Hosts.187

Вредоносный скрипт, написанный на языке командного интерпретатора ОС Windows. Модифицирует файл hosts, добавляя в него определенный список доменов.

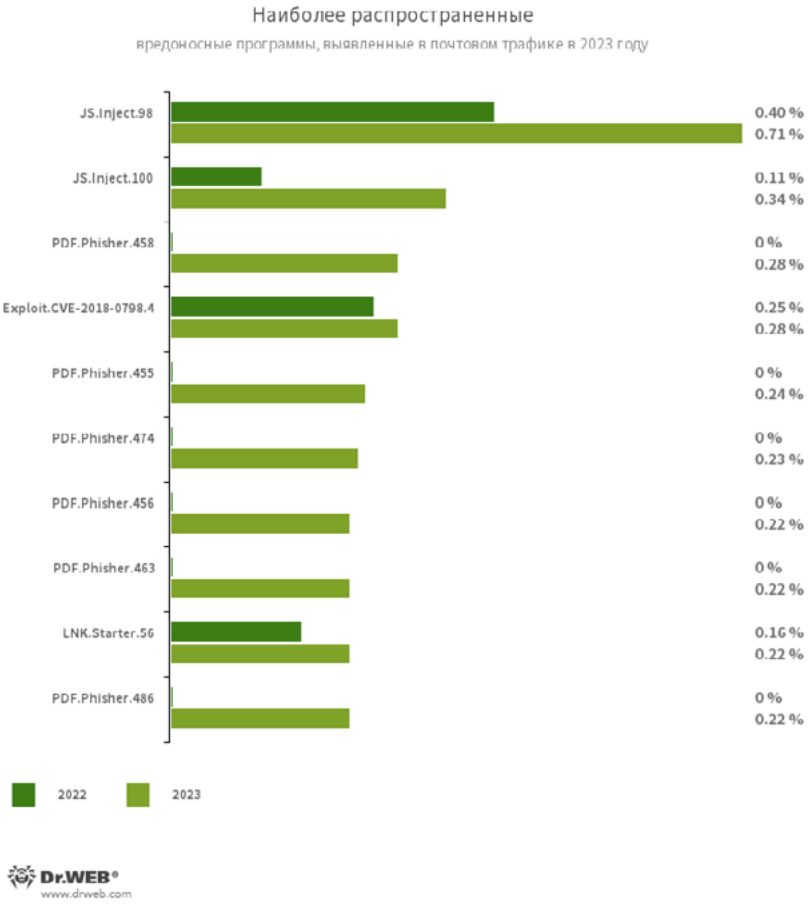
- Trojan.Hosts.51189

Троянская программа, которая изменяет содержимое файла hosts на компьютерах под управлением ОС Windows.

- BAT.Starter.457

Вредоносный скрипт, написанный на языке командного интерпретатора ОС Windows. Предназначен для запуска различных вредоносных приложений на целевых компьютерах.

В почтовом трафике в 2023 году наиболее распространенными угрозами стали вредоносные скрипты и фишинговые документы, которые часто представляют собой поддельные формы ввода учетных данных. Такие документы имитируют авторизацию на популярных сайтах и передают злоумышленникам вводимые жертвами данные. Широкое распространение вновь получили и вредоносные программы, эксплуатирующие уязвимости документов Microsoft Office.



- JS.Inject

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

- PDF.Phisher.458
- PDF.Phisher.455
- PDF.Phisher.474
- PDF.Phisher.456
- PDF.Phisher.486
- PDF.Phisher.463

PDF-документы, используемые в фишинговых email-рассылках.

- Exploit.CVE-2018-0798.4

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

- 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.

Шифровальщики

По сравнению с 2022, в 2023 году в вирусную лабораторию «Доктор Веб» поступило на 28,84% меньше запросов от пользователей, пострадавших от троянских приложений-шифровальщиков. На следующем графике представлена динамика регистрации запросов на расшифровку файлов:

Наиболее распространенные шифровальщики в 2023 году:

- Trojan.Encoder.26996 (21,35% обращений пользователей)

Шифровальщик, известный как STOP Ransomware. Он пытается получить приватный ключ с удаленного сервера, а в случае неудачи пользуется зашитым. Это один из немногих троянов-вымогателей, который шифрует данные поточным алгоритмом Salsa20.

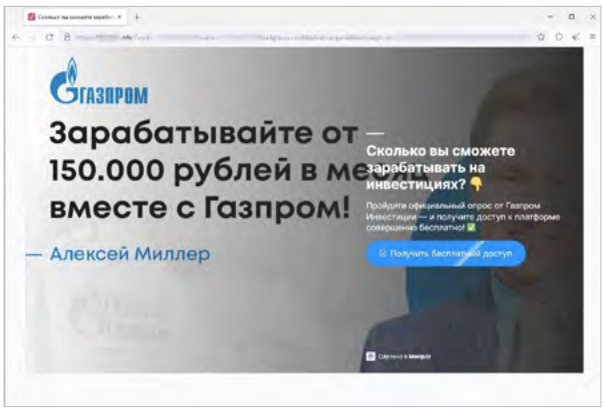
- Trojan.Encoder.3953 (18,87% обращений пользователей)
  Шифровальщик, имеющий несколько различных версий и модификаций. Для шифрования файлов применяет алгоритм AES-256 в режиме CBC.
- **Trojan.Encoder.35534** (6,00% обращений пользователей)
  Шифровальщик, также известный как Mimic. При поиске целевых файлов для шифрования троян использует библиотеку everything.dll легитимной программы Everything, предназначенной для мгновенного поиска файлов на Windows-компьютерах.
- Trojan.Encoder.34027 (2,18% обращений пользователей)
  Шифровальщик, также известный как TargetCompany или Tohnichi. Для шифрования файлов использует алгоритмы AES-128, Curve25519 и ChaCha20.
- Trojan.Encoder.35209 (2,01% обращений пользователей)
  Шифровальщик, известный как Conti (один из вариантов трояна — **Trojan.Encoder.33413**). Для шифрования файлов применяет алгоритм AES-256.

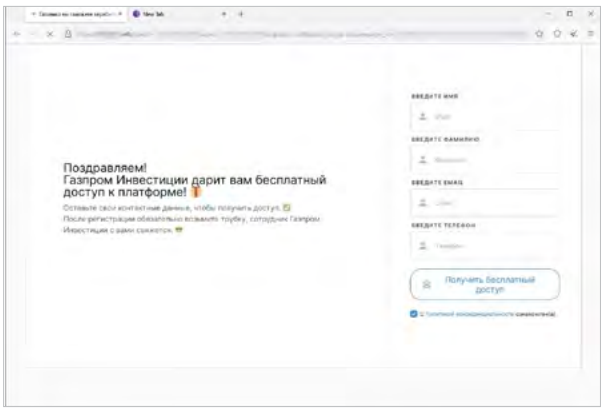
Сетевое мошенничество

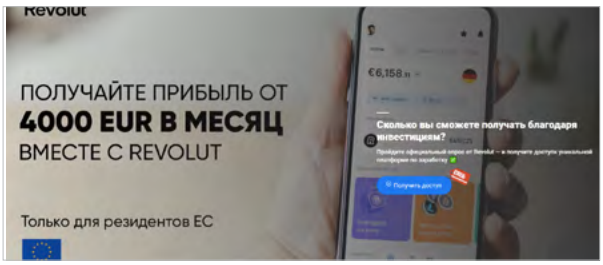
В 2023 году интернет-аналитики компании «Доктор Веб» наблюдали высокую активность мошенников и обнаружили множество фишинговых сайтов. Наиболее востребованной среди злоумышленников стала финансовая тематика: около 60% выявленных нежелательных интернет-ресурсов имитировали настоящие сайты кредитных организаций. Распространенными вариантами среди них были поддельные личные кабинеты для входа в онлайн-банк и страницы с псевдоопросами. С помощью таких подделок киберпреступники пытались заполучить персональные данные пользователей и реквизиты для доступа к учетным записям в интернет-банках.

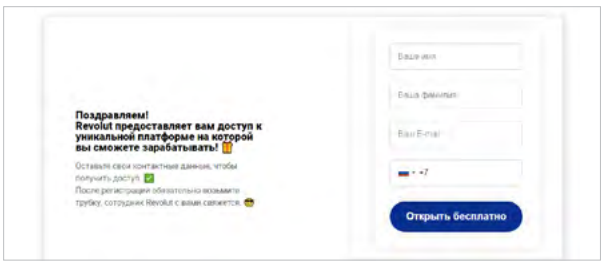
Кроме того, злоумышленники продолжили заманивать потенциальных жертв на мошеннические сайты с предложениями помочь улучшить финансовое положение. В одних случаях им предлагалось заработать на инвестициях в сервисах, якобы имеющих отношение к крупным нефтегазовым компаниям. В других — получить доступ к неким автоматизированным торговым платформам, якобы гарантирующим высокую прибыль. Популярностью вновь пользовались и вариации с «получением» социальных выплат от государства. Фишинговая схема на таких сайтах сводится к тому, что пользователи после ответа на ряд простых вопросов должны указать персональные данные для регистрации учетной записи, а в случае с якобы получением тех или иных выплат — еще и заплатить «комиссию» за перевод на их банковский счет в действительности несуществующих денег.

На скриншотах ниже показаны примеры мошеннических сайтов финансовой тематики. В первом случае пользователям якобы от имени крупной российской нефтегазовой компании предлагается получить доступ к «инвестиционной платформе». Во втором — к инвестиционному сервису, якобы имеющему отношение к одному из европейских банков. В третьем — к псевдоторговой «автоматизированной системе», известной под именами Quantum UI, Quantum System и т. п.

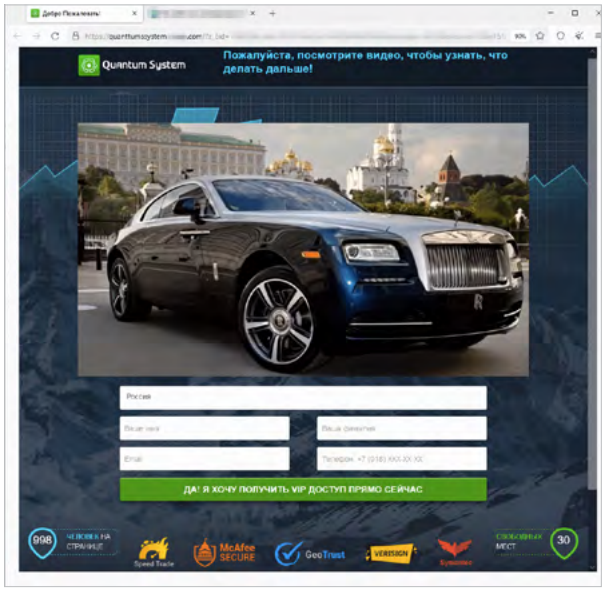


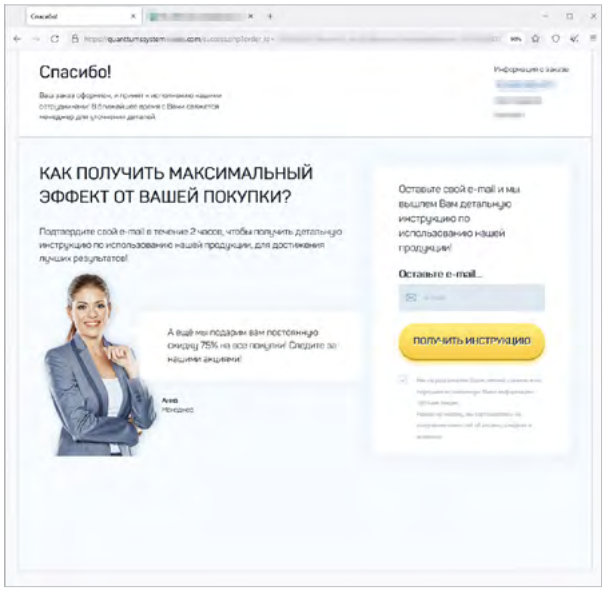






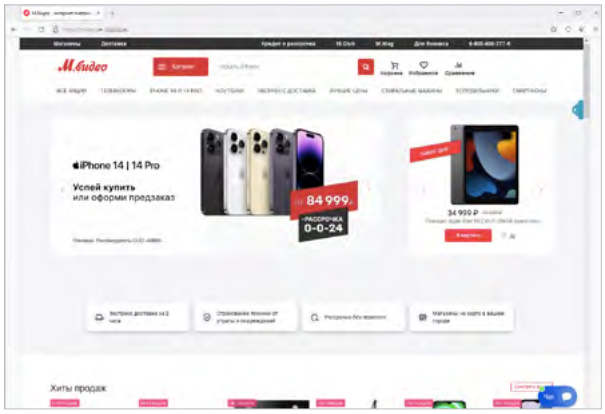
«Доктор Веб»: обзор вирусной активности за 2023 год

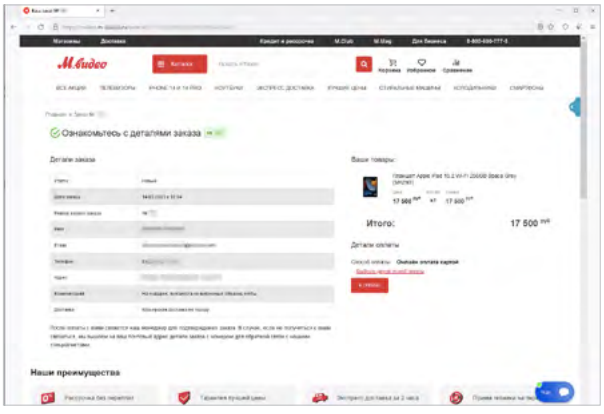




Распространенными вновь были фишинговые схемы, связанные со всевозможными «акциями», «бонусами» и «подарками». Мошенники заманивали потенциальных жертв на поддельные веб-сайты интернет-магазинов, ритейлеров, онлайн-касс для продажи билетов и т. п., где якобы можно было принять участие в розыгрыше призов, получить подарок или бонусы, либо приобрести тот или иной товар по более выгодной цене. Злоумышленники вводили пользователей в заблуждение, пытаясь украсть у них деньги и данные банковских карт. Примеры таких мошеннических сайтов представлены на скриншотах ниже.

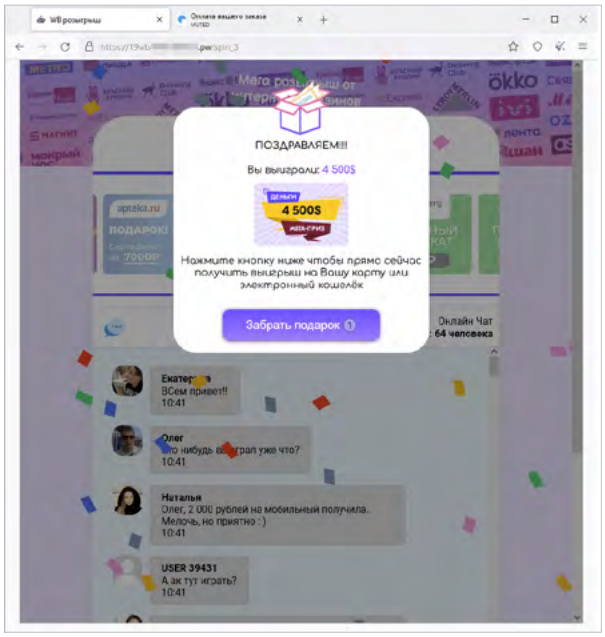
Поддельный сайт, имитирующий внешний вид настоящего интернет-ресурса российского магазина бытовой техники и электроники:

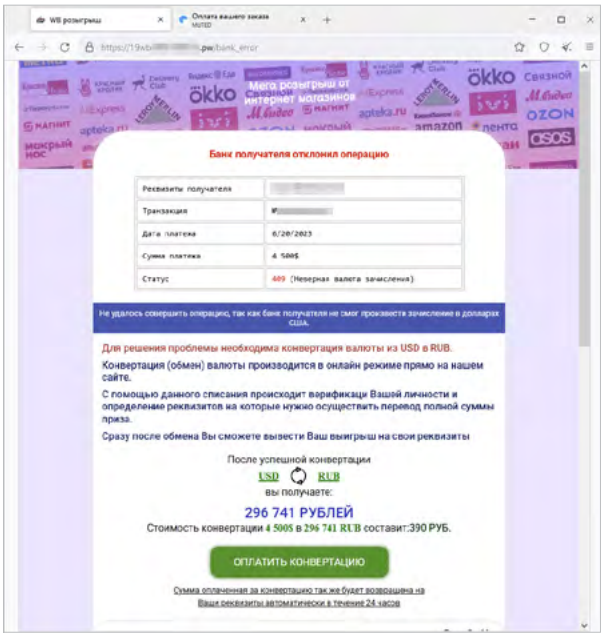




Мошенники предлагают потенциальным жертвам «приобрести» товар со скидкой, оплатив его банковской картой или переводом средств через онлайн-банк.

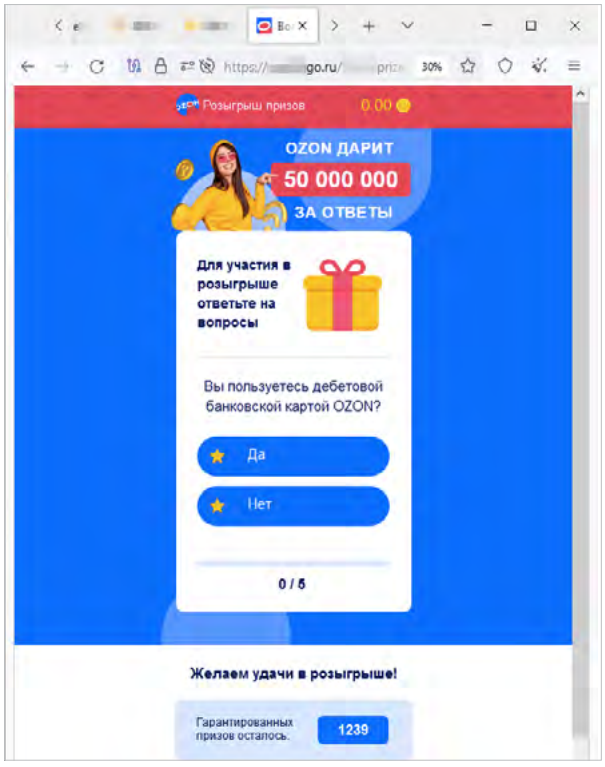
Мошеннический сайт, на котором посетителям якобы от имени интернет-магазинов предлагается принять участие в «розыгрыше призов»:

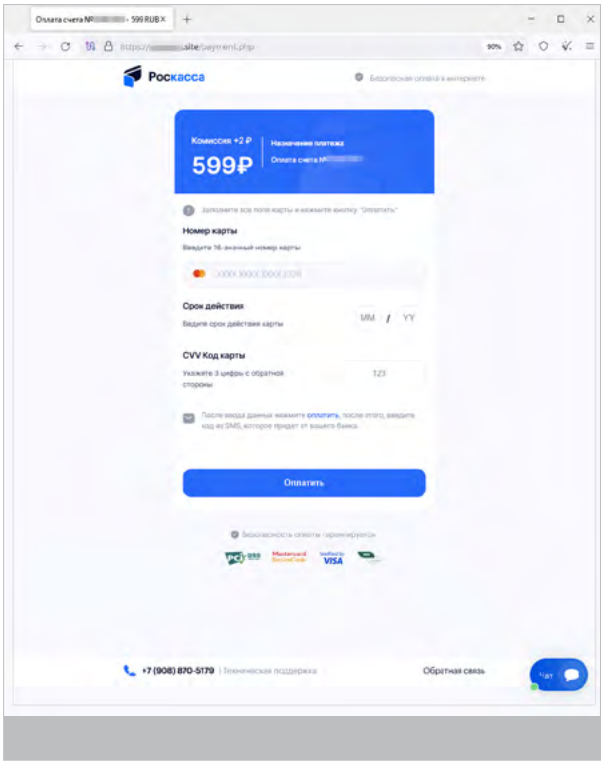




После того как потенциальная жертва «выигрывает» крупный денежный приз, для его «получения» она якобы должна заплатить комиссию за конвертацию валюты.

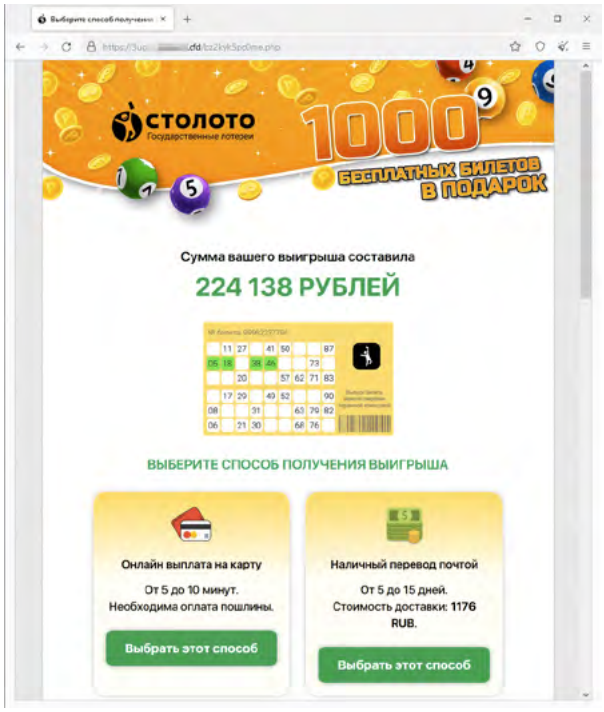
Мошеннический интернет-ресурс, оформленный в стиле официального сайта одного из российских интернет-магазинов:

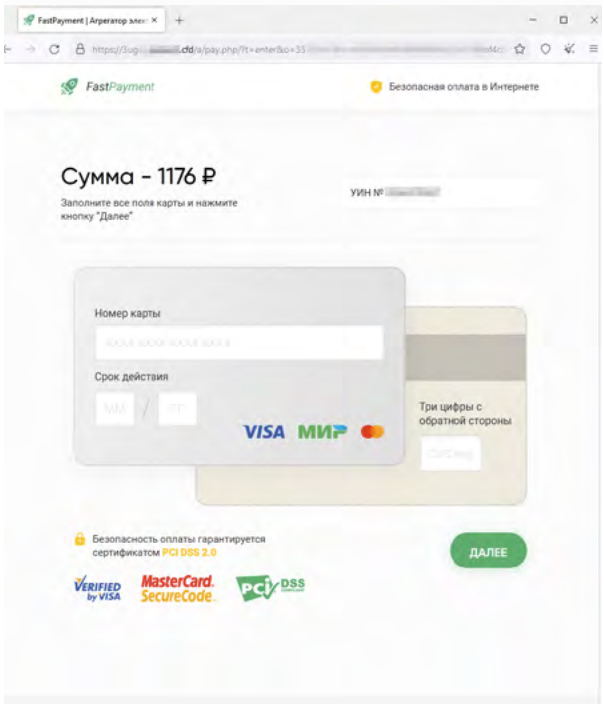




Пользователю для участия в «розыгрыше» денежного приза предлагается ответить на несколько вопросов. После того как сайт имитирует розыгрыш приза, жертва якобы выигрывает, но для «получения» выигрыша ей необходимо заплатить «комиссию».

Фишинговый сайт, предлагающий посетителям «бесплатные» лотерейные билеты:



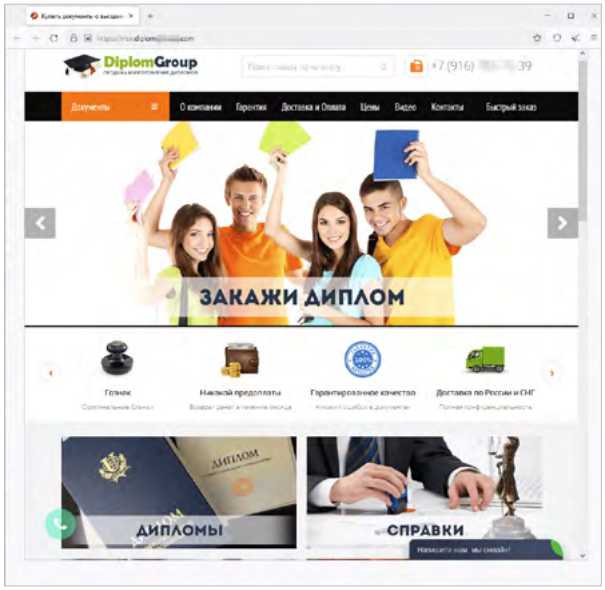


Якобы победивший в лотерею пользователь для получения выигрыша должен заплатить «комиссию».

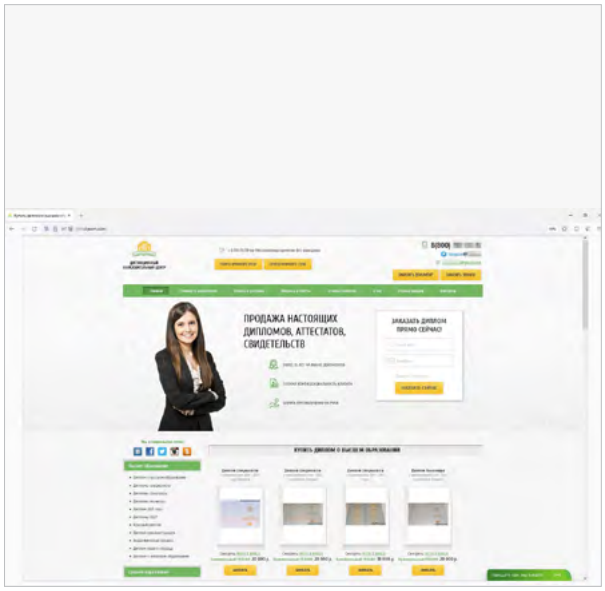
Летом 2023 года активизировались мошенники, которые на различных сайтах предлагали якобы легальные услуги по восстановлению утраченных или продаже совершенно новых документов государственного образца России, стран СНГ и других государств. В ассортименте таких сайтов значились дипломы о высшем образовании, водительские удостоверения, всевозможные справки, свидетельства и т. д. Пользователи, решавшиеся прибегнуть к сомнительным сервисам, не только рисковали потерять деньги при оплате несуществующей услуги, но и могли столкнуться с утечкой своих персональных данных. Кроме того, в случае приобретения поддельного документа они нарушали закон, что в дальнейшем могло привести к проблемам с правоохранительными органами. Ниже представлены скриншоты с примерами сайтов, на которых предлагались сомнительные услуги.

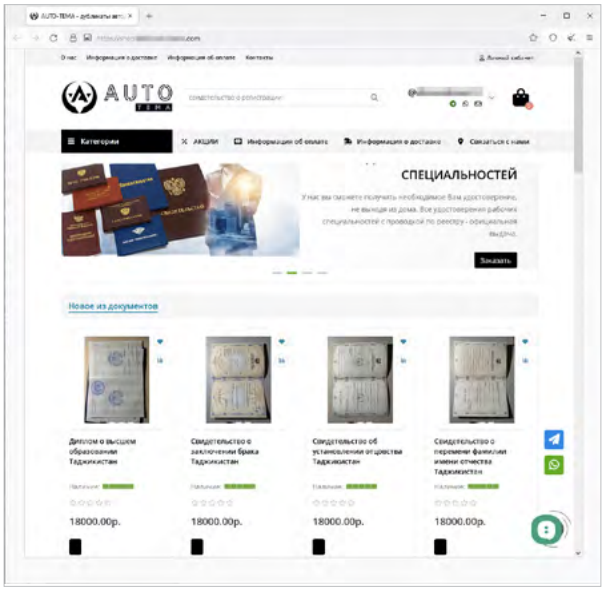
Сайт, предлагающий приобрести паспорт гражданина Российской Федерации:

Сайты, предлагающие приобрести дипломы о высшем образовании, аттестаты, водительские удостоверения и другие документы:

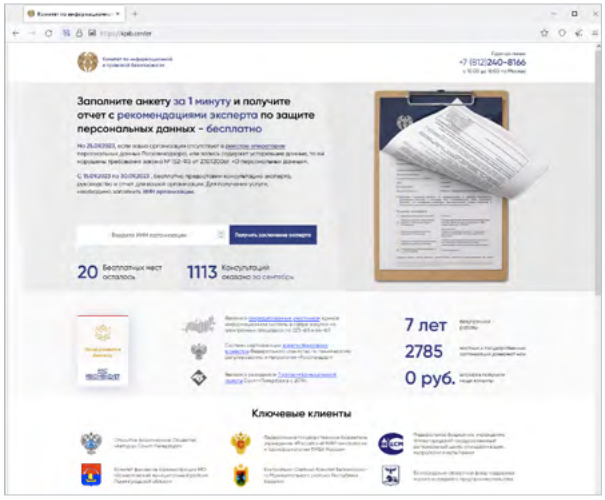


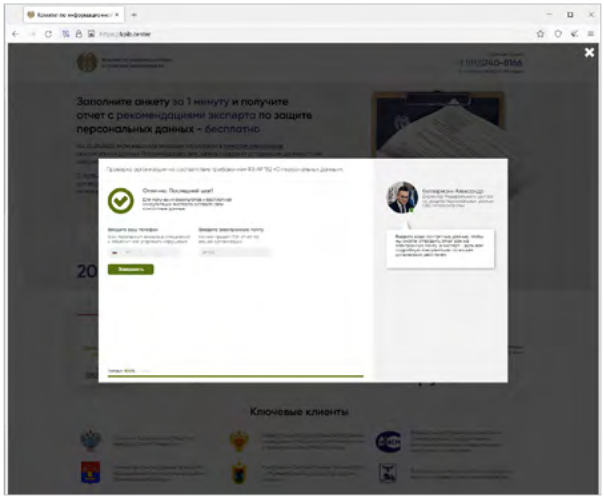
«Доктор Веб»: обзор вирусной активности за 2023 год





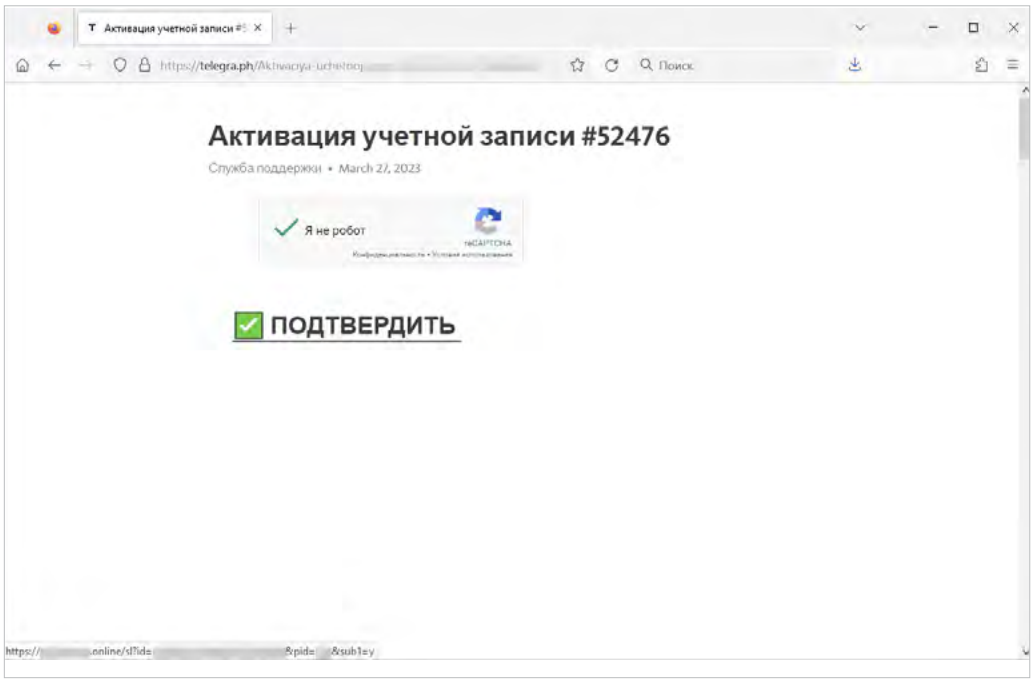
Уже осенью интернет-аналитики «Доктор Веб» зафиксировали рассылку фишинговых писем якобы от имени налоговых органов. Эти письма содержали ссылку на сайт, где пользователям предлагалось проверить организации и предприятия на соответствие требованиям закона о персональных данных (№ 152-ФЗ «О персональных данных»). Для этого от них вначале требовалось пройти опрос, после чего указать персональные данные «для получения результатов и бесплатной консультации эксперта». После ответа на вопросы сайт запрашивал у посетителей номер телефона и email.





Вместе с тем в минувшем году наши специалисты отметили рост случаев использования мошенниками блог-платформы Telegraph. Злоумышленники публикуют в ней фишинговые записи со ссылками, ведущими на различные нежелательные сайты. При этом ссылки на сами страницы с мошенническими публикациями перед распространением предварительно преобразуются через сервисы сокращения ссылок.

Пример такой мошеннической публикации представлен на скриншоте ниже. Пользователю предлагается активировать некую учетную запись, но при нажатии на элемент с текстом «ПОДТВЕРДИТЬ» он перенаправляется на фишинговый сайт.



Для мобильных устройств

Согласно статистике детектирований Dr.Web для мобильных устройств Android, в 2023 году самыми распространенными вредоносными Android-программами стали демонстрирующие нежелательную рекламу трояны Android.HiddenAds, на долю которых пришлось 31,61% обнаруженного вредоносного ПО. При этом наиболее активной угрозой стал Android.HiddenAds.3697 — он детектировался на защищаемых устройствах в 10,72% случаев. На втором месте с долей 28,22% расположились обладающие шпионской функциональностью троянские программы Android.Spy. Среди них чаще всего выявлялся троян Android.Spy.5106 (20,80% случаев). Третьими с показателем 10,06% стали рекламные трояны Android.MobiDash.

Наиболее активной нежелательной программой оказалась Program.FakeMoney.7 (29,90% детектирований нежелательного ПО). Она предлагала пользователям заработать на выполнении различных заданий, но на самом деле не выплачивала никаких вознаграждений. Второй по распространенности (19,42% детектирований) стала Program.FakeAntiVirus.1. Она имитировала работу антивирусов, обнаруживала несуществующие угрозы и предлагала пользователям приобрести полную версию программы для «устранения» проблем. Третье место с долей 9,46% заняли приложения, которые прошли модификацию через облачный сервис CloudInject. К таким программам (антивирус Dr.Web детектирует их как Program.CloudInject.1) добавляются опасные разрешения и обфусцированный код, назначение которого нельзя проконтролировать.

Как и годом ранее среди потенциально опасных программ лидирующие позиции по числу детектирований вновь заняли утилиты Tool.SilentInstaller (48,89% случаев обнаружения потенциально опасного ПО). Они позволяют запускать Android-приложения без установки и могут использоваться киберпреступниками для запуска вредоносных программ. Вторыми с долей 14,02% стали утилиты Tool.LuckyPatcher — с их помощью возможна модификация Android-приложений с добавлением в них загружаемых из интернета скриптов. На третьем месте с долей 10,14% расположились приложения, защищенные программным упаковщиком Tool.ApkProtector.

Самым распространенным семейством рекламных программ в 2023 году стало Adware.Adpush — на него пришлось 35,82% детектирований нежелательного рекламного ПО. Вторым наиболее часто встречавшимся стало семейство Adware.MagicPush с долей 9,58%. Третью строчку заняло семейство рекламных модулей Adware.Airpush, на долю которых пришлось 8,59% детектирований.

В течение минувшего года вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play свыше 440 вредоносных приложений, которые суммарно были загружены по меньшей мере 428 000 000 раз. Среди обнаруженных угроз оказалось более 100 программ со встроенным троянским модулем Android.Spy.SpinOk, который обладал шпионской функциональностью. Кроме того, наша вирусная лаборатория зафиксировала свыше 300 троянских приложений Android.FakeApp, которые использовались при реализации различных мошеннических схем. Также наши специалисты выявили троянские программы Android.Proxy.4gproxy — они превращали зараженные устройства в прокси-серверы и незаметно передавали через них сторонний трафик. Среди обнаруженных угроз были рекламные трояны семейства Android.HiddenAds, вредоносная программа-шпион Android.Spy.1092.origin и похититель криптовалют Android.CoinSteal.105. Не обошлось и без появления новых представителей Android.Subscription — семейства троянов, подписывающих пользователей на платные услуги. При

этом в Google Play вновь распространялись трояны Android.Joker и Android.Harly, которые также предназначены для подписки жертв на платные сервисы.

По сравнению с 2022, в 2023 году почти наполовину сократилось число детектирований банковских троянских приложений для платформы Android. Тем не менее география их атак вновь охватила множество стран. Более того, наряду с активностью известных банковских троянов вирусные аналитики компании «Доктор Веб» фиксировали появление и новых семейств, многие из которых были нацелены на российских и иранских пользователей.

Вместе с тем наши специалисты продолжили выявлять вредоносные сайты, распространяющие поддельные приложения криптокошельков для Android- и iOS-устройств с целью кражи криптовалюты.

Более подробно о вирусной обстановке для мобильных устройств в 2023 году читайте в нашем обзоре.

Перспективы и вероятные тенденции

Широкое распространение рекламных троянских приложений в 2023 году показало, что для киберпреступников одним из приоритетов по-прежнему остается получение нелегального заработка. Подтверждением этому служит и активное использование троянских программ на скриптовом языке AutoIt, которые в том числе применяются в составе троянов-майнеров для затруднения их обнаружения. В этой связи вероятно, что вредоносные программы, которые помогают вирусописателям обогащаться за счет своих жертв, останутся в арсенале киберпреступников и в 2024 году.

При этом несмотря на снижение общего числа атак с использованием банковских троянов развитие этого типа вредоносных приложений не останавливается, о чем говорит появление новых семейств. Эта тенденция, скорее всего, продолжится.

Не потеряет актуальности и сетевое мошенничество. С развитием технологий злоумышленники вместе с использованием зарекомендовавших себя схем обмана наверняка станут все чаще применять новые, в том числе задействуя нейросети.

Следует ожидать появления очередных угроз для мобильных устройств, в том числе и в официальных магазинах приложений, таких как Google Play. При этом вероятно появление новых вредоносных программ для устройств под управлением не только Android, но и других платформ, в частности, iOS.

Атака на ПО Openfire в очередной раз показала важность установки обновлений и поддержания используемых программ в актуальном состоянии. Не исключено, что в 2024 году киберпреступники предпримут новые попытки атак с применением всевозможных эксплойтов, в том числе и таргетированные атаки.

«Доктор Веб»: обзор вирусной активности за 2023 год

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
Центр противодействия кибер-мошенничеству

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