«Доктор Веб»:

обзор вирусной активности в апреле 2023 года

«Доктор Веб»: обзор вирусной активности в апреле 2023 года

14 июня 2023 года

Анализ статистики детектирований антивируса Dr.Web в апреле 2023 года показал снижение общего числа обнаруженных угроз на 2,08% по сравнению с мартом. Число уникальных угроз при этом также снизилось — на 17,40%. Наиболее активными среди них вновь оказались рекламные программы и троянские приложения различных семейств. В почтовом трафике преобладали вредоносные скрипты и PDF-документы, применяемые в фишинг-атаках.

Число обращений пользователей за расшифровкой файлов снизилось на 13,75% по сравнению с предыдущим месяцем. Наиболее часто жертвы троянов-шифровальщиков вновь сталкивались с энкодерами Trojan.Encoder.26996, Trojan.Encoder.3953 и Trojan.Encoder.35534.

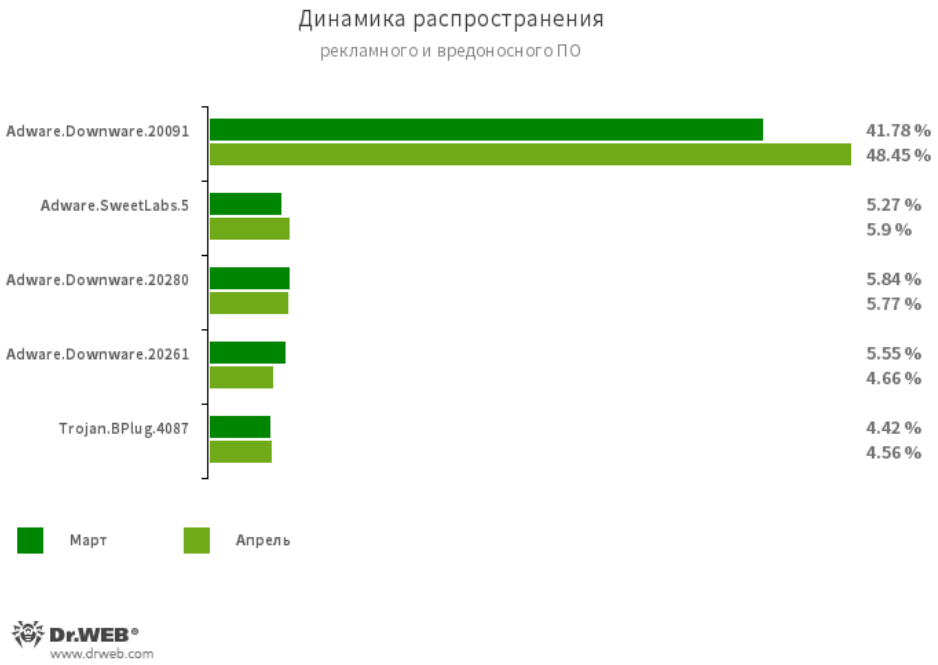
В течение апреля в каталоге Google Play было выявлено множество угроз. Среди них — троянские программы Android.FakeApp, используемые в мошеннических целях, а также вредоносное приложение из семейства Android.Joker, которое подписывало жертв на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ АПРЕЛЯ

- Снижение общего числа обнаруженных угроз
- Снижение количества обращений пользователей за расшифровкой файлов, поврежденных шифровальщиками
- Распространение вредоносных приложений через каталог Google Play

«Доктор Веб»: обзор вирусной активности в апреле 2023 года

По данным сервиса статистики «Доктор Веб»



Наиболее распространенные угрозы апреля:

Adware.Downware.20091

Adware.Downware.20280

Adware.Downware.20261

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.SweetLabs.5

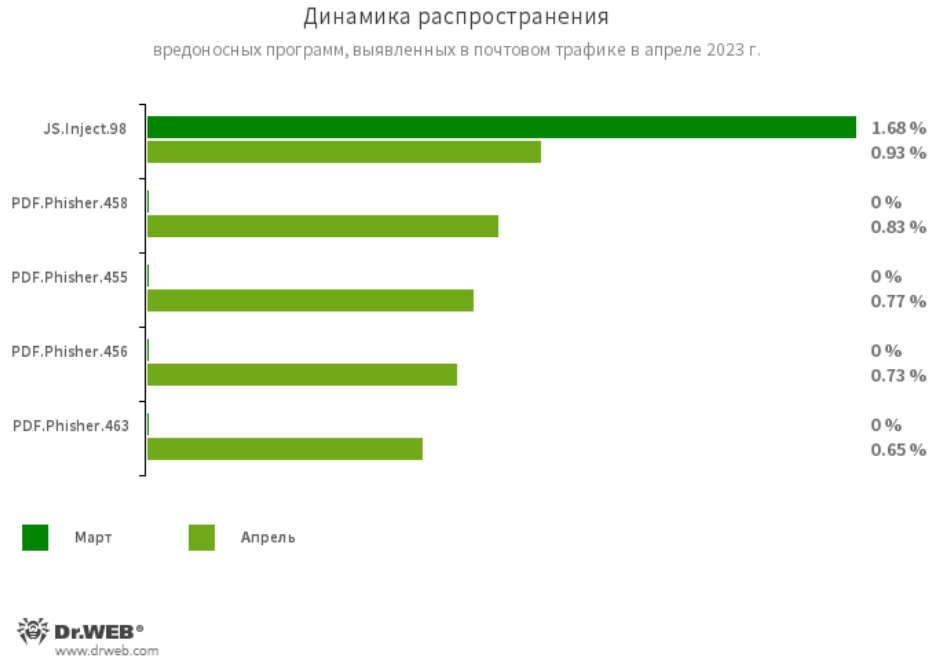
Альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy.

Trojan.BPlug.4087

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

«Доктор Веб»: обзор вирусной активности в апреле 2023 года

Статистика вредоносных программ в почтовом трафике



JS.Inject

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

PDF.Phisher.455

PDF.Phisher.456

PDF.Phisher.458

PDF.Phisher.463

PDF-документы, используемые в фишинговых email-рассылках.

«Доктор Веб»: обзор вирусной активности в апреле 2023 года

Шифровальщики

В апреле число запросов на расшифровку файлов, поврежденных троянскими программами-шифровальщиками, снизилось на 13,75% по сравнению с мартом.

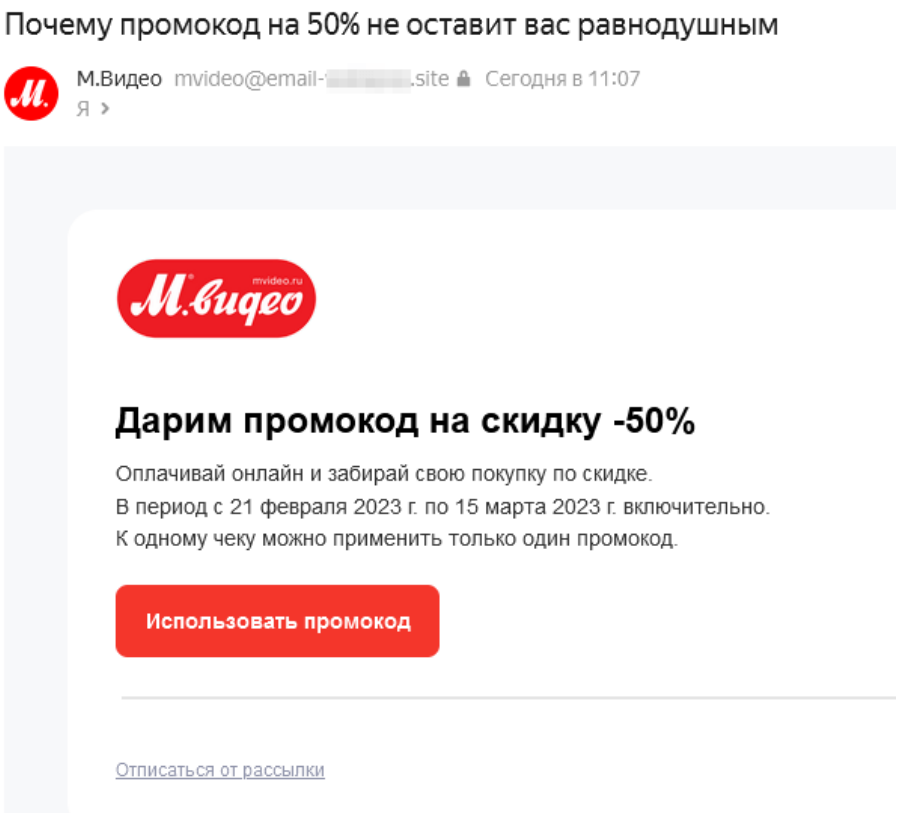
- Trojan.Encoder.26996 — 24.31%
- Trojan.Encoder.3953 — 19.92%
- Trojan.Encoder.35534 — 4.38%
- Trojan.Encoder.35209 — 3.59%
- Trojan.Encoder.11539 — 3.19%

Опасные сайты

В апреле 2023 года интернет-мошенники не оставляли попыток заманить пользователей на фишинговые сайты — например, на поддельные ресурсы интернет-магазинов. Так, для российских пользователей злоумышленники вновь организовывали спам-рассылки электронных писем с ненастоящими купонами на скидку якобы от имени магазина «М.Видео».

Для «покупки» понравившихся товаров посетители должны были указать персональные данные, а также данные банковской карты. На самом деле жертвы обмана лишь предоставляли злоумышленникам личную информацию и рисковали потерять деньги, «оплачивая» несуществующий товар.

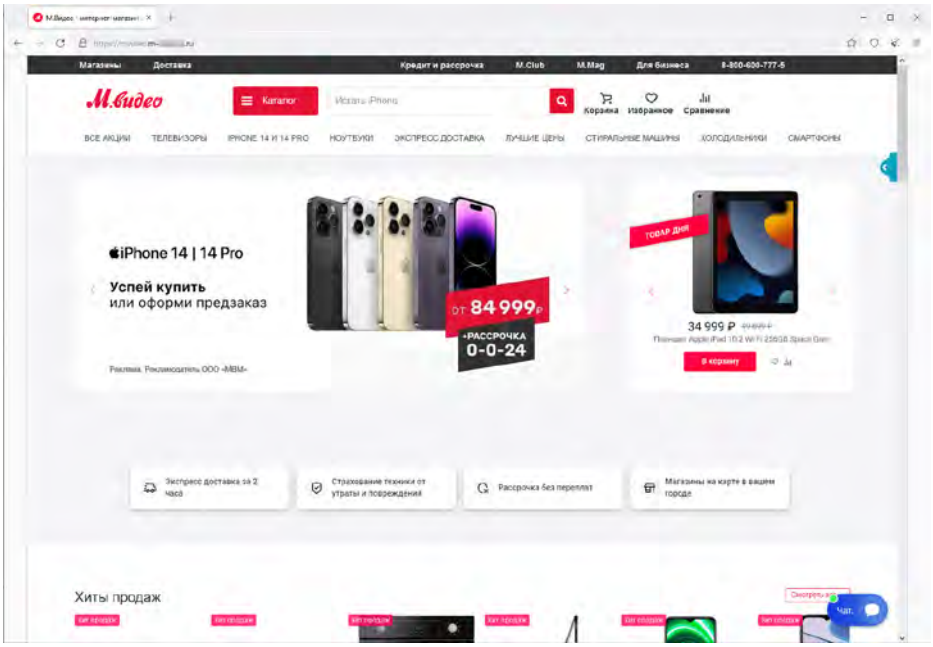
Пример содержимого спам-письма с ложной информацией о промокоде на скидку и ссылкой на поддельный интернет-ресурс магазина:

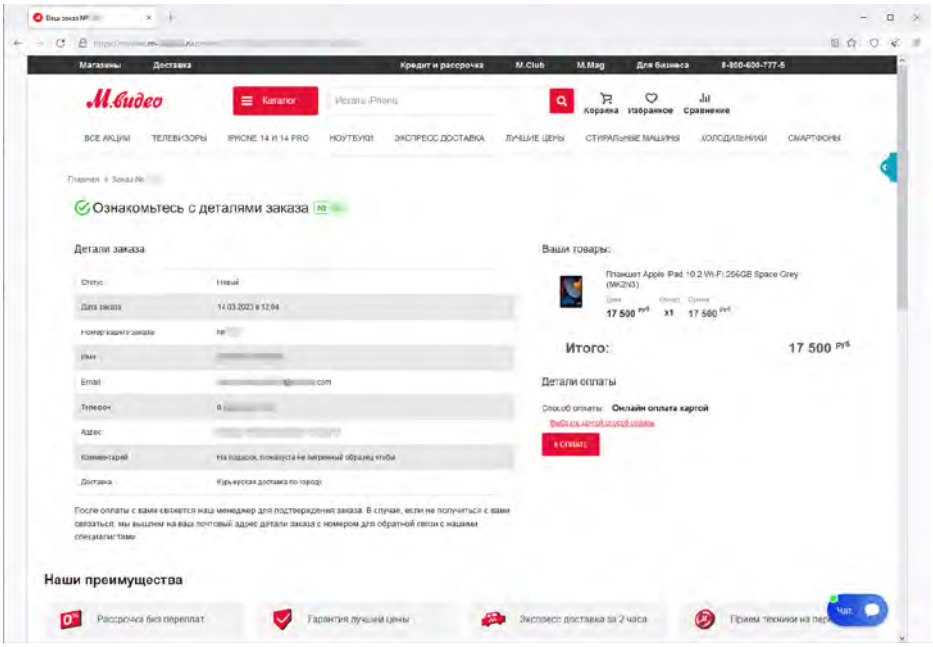


Примеры страниц фишингового интернет-ресурса, имитирующего внешний вид настоящего сайта магазина, представлены ниже. Посетителям предлагается указать персональную информацию и «оплатить» заказ.

«Доктор Веб»: обзор вирусной активности в апреле 2023 года

Опасные сайты





Вредоносное и нежелательное ПО для мобильных устройств

Согласно данным статистики детектирований Dr.Web для мобильных устройств Android, в апреле 2023 года рекламные троянские программы вновь стали одними из наиболее распространенных Android-угроз. По сравнению с мартом пользователи чаще сталкивались с программами-вымогателями, а также банковскими троянскими приложениями. Вместе с тем наблюдалось снижение активности шпионских троянских программ.

В течение апреля в каталоге Google Play были выявлены очередные угрозы. Среди них — программы-подделки из семейства Android.FakeApp, применяемые в различных мошеннических схемах, а также представитель опасного семейства Android.Joker, подписывавший жертв на платные услуги.

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

- рекламные троянские программы остаются одними из наиболее распространенных Android-угроз,
- рост активности банковских троянских программ и приложений-вымогателей,
- распространение угроз через каталог Google Play.

Более подробно о вирусной обстановке для мобильных устройств в апреле читайте в нашем обзоре ссылка на обзор.

Узнайте больше о нерекомендуемых Dr.Web сайтах

«Доктор Веб»: обзор вирусной активности в апреле 2023 года

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, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека