Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в апреле 2021 года

«Доктор Веб»: обзор вирусной активности в апреле 2021 года

13 мая 2021 года

В апреле анализ данных статистики Dr.Web показал увеличение общего числа обнаруженных угроз на 1.73% по сравнению с мартом. При этом количество уникальных угроз снизилось на 35.6%. Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике по частоте распространения лидирует разнообразное вредоносное ПО, в том числе обфусцированные вредоносные программы, скрипты, а также приложения, использующие уязвимости документов Microsoft Office.

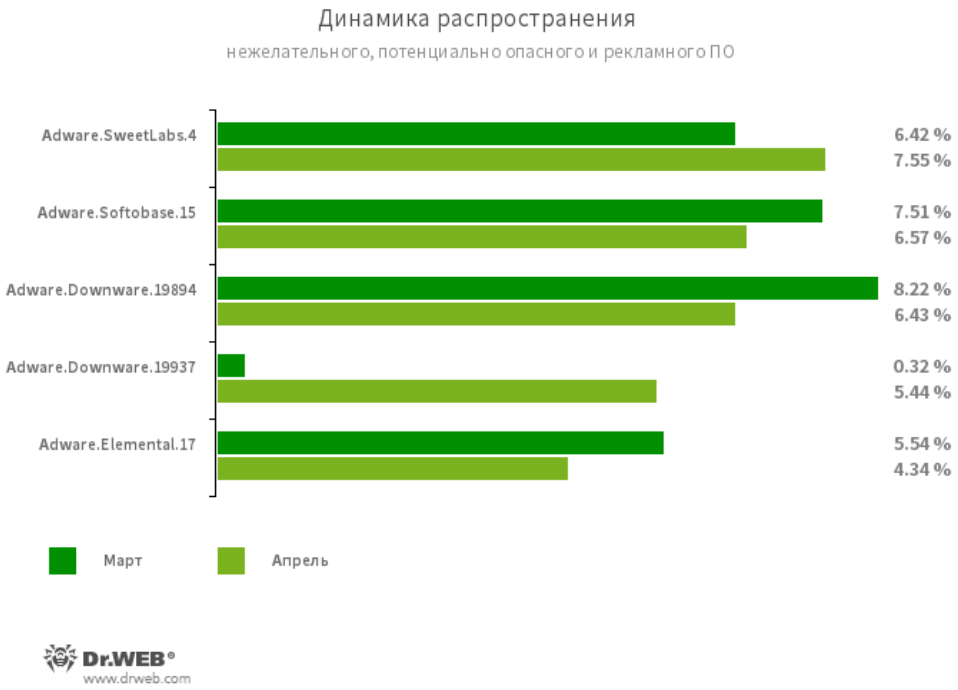
Число обращений пользователей за расшифровкой файлов уменьшилось на 2.73% по сравнению с мартом. Самым распространенным энкодером апреля оказался Trojan.Encoder.567, на долю которого приходится 15.71% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ АПРЕЛЯ

- Увеличение активности распространения вредоносного ПО
- Рекламные приложения – всё еще одна из главных угроз
- Появление новых угроз в почтовом трафике

«Доктор Веб»: обзор вирусной активности в апреле 2021 года

По данным сервера статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.SweetLabs.4

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

Adware.Softobase.15

Программа-установщик, распространяющая устаревшее программное обеспечение. Изменяет настройки браузера.

Adware.Downware.19894

Adware.Downware.19937

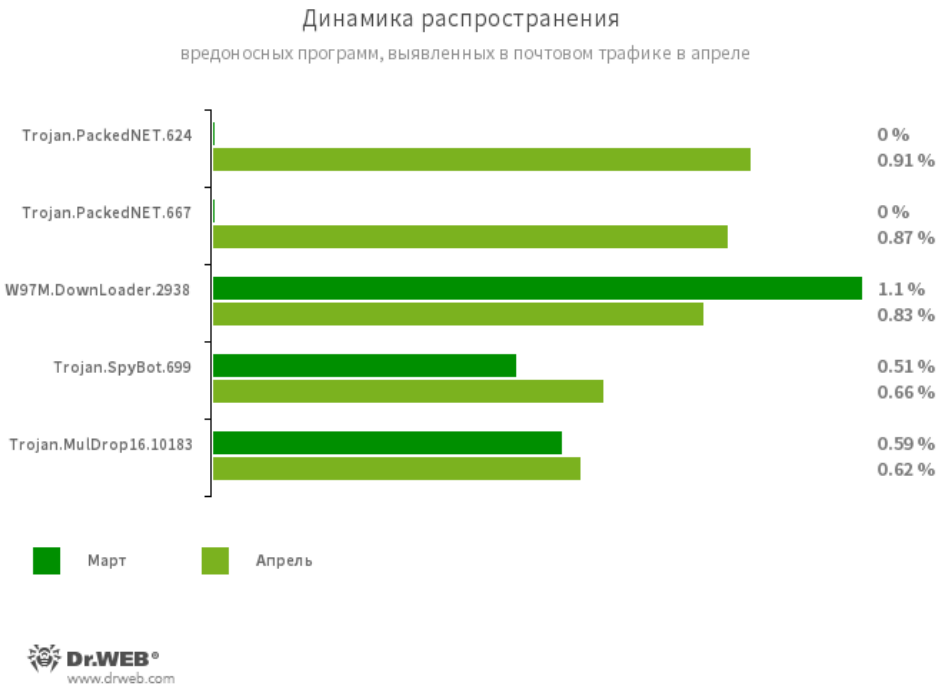
Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.Elemental.17

Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают приложения с рекламой, а также инсталлируют ненужное ПО.

«Доктор Веб»: обзор вирусной активности в апреле 2021 года

Статистика вредоносных программ в почтовом трафике



Trojan.PackedNET.624
Trojan.PackedNET.667
Упакованное вредоносное ПО, написанное на VB.NET.

W97M.DownLoader.2938
Семейство троянов-загрузчиков, использующих уязвимости файлов Microsoft Office и предназначенных для загрузки на атакуемый компьютер других вредоносных программ.

Trojan.SpyBot.699
Многомодульный банковский троян. Позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения, а также исполнять произвольный код.

Trojan.MulDrop16.10183
Вредоносная программа, загружающая нежелательные приложения на компьютер жертвы.

«Доктор Веб»: обзор вирусной активности в апреле 2021 года

Шифровальщики

Запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков, в апреле в антивирусную лабораторию «Доктор Веб» поступило на 2.73% меньше, чем в прошлом месяце.

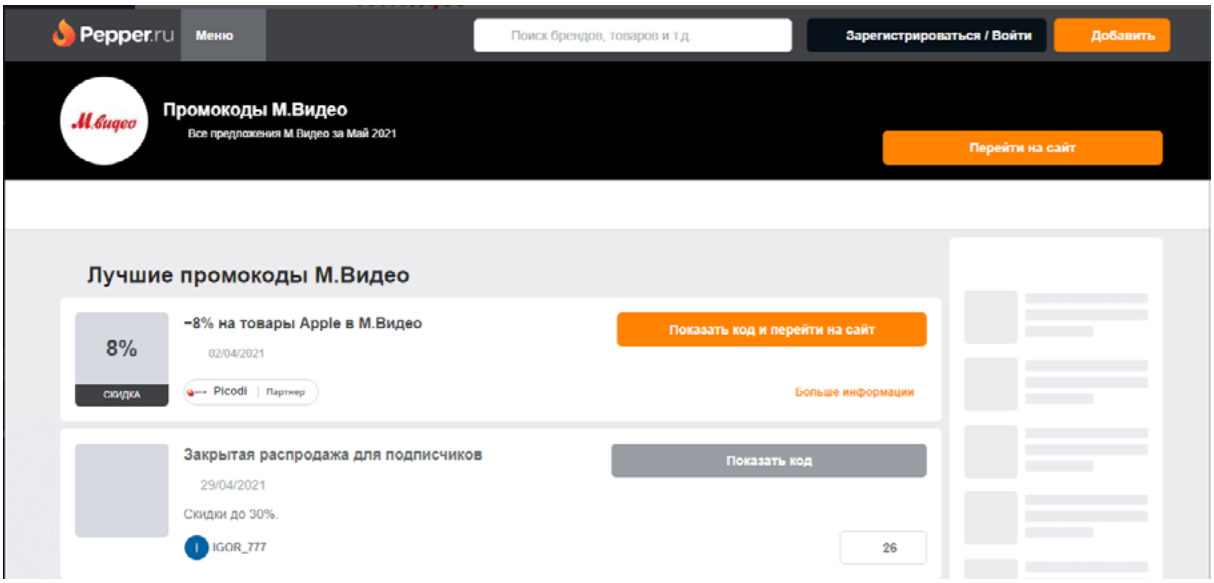
- Trojan.Encoder.567 — 15.71%
- Trojan.Encoder.26996 — 14.94%
- Trojan.Encoder.11539 — 1.53%
- Trojan.Encoder.741 — 1.15%
- Trojan.Encoder.11464 — 1.15%

Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении
Dr.Web Rescue Pack

Опасные сайты

В апреле 2021 года интернет-аналитики «Доктор Веб» обнаружили множество фишинговых сайтов. В числе прочего злоумышленники подделывали веб-страницы магазинов бытовой техники. Например, мошеннические сайты были замаскированы под официальные ресурсы «М.Видео». После нажатия кнопки «Перейти на сайт» пользователи оказывались в фальшивом интернет-магазине.



Злоумышленники заманивали жертв на фишинговые сайты, используя методы социальной инженерии. Они рассчитывали, что в надежде получить товары дешевле покупатели будут активировать специальные промокоды. Если пользователь попадался на уловку, мошенник получал его персональные данные, которые использовал для собственного обогащения, — например, списывал деньги с банковского счета жертвы.

Помимо этого, в апреле были зафиксированы случаи перенаправления на фейковые сайты платежных систем. Там пользователи вводили данные банковской карты, подтверждали платёж, но товар не получали.

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

Вредоносное и нежелательное ПО для мобильных устройств

В прошлом месяце вирусные аналитики компании «Доктор Веб» выяснили, что одна из версий клиентского приложения популярного стороннего каталога Android-программ APKPure содержит вредоносную функциональность. Обнаруженный в ней троян Android.Triada.4912 с помощью вспомогательного компонента загружал другие программы, а также демонстрировал различные веб-сайты.

Помимо этого, наши специалисты выявили первые вредоносные приложения в каталоге ПО AppGallery. Ими стали трояны из семейства Android.Joker, способные выполнять произвольный код, а также подписывать пользователей на платные мобильные сервисы.

Кроме того, в официальном каталоге Android-программ Google Play были найдены очередные трояны из семейства Android.FakeApp, применявшиеся в мошеннических целях.

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

- появление троянской функциональности в клиентском приложении стороннего каталога APKPure;
- обнаружение первых вредоносных программ в каталоге AppGallery;
- распространение новых троянов через официальный каталог Google Play.

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

«Доктор Веб»: обзор вирусной активности в апреле 2021 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
ВебIQметр | 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