Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в апреле 2020 года

«Доктор Веб»: обзор вирусной активности в апреле 2020 года

18 мая 2020 года

В апреле анализ данных статистики Dr.Web показал снижение общего числа обнаруженных угроз на 34.5% по сравнению с мартом. Количество уникальных угроз снизилось на 11.42%. Большинство обнаруженных угроз по-прежнему приходится на долю рекламных программ и вредоносных расширений для браузеров. В почтовом трафике продолжает лидировать банковский троян Trojan.SpyBot.699, а также вредоносное ПО, использующее уязвимости документов Microsoft Office. Кроме того, в число самых распространенных угроз вошли вредоносные HTML-документы, распространяемые в виде вложений и перенаправляющие пользователей на фишинговые сайты.

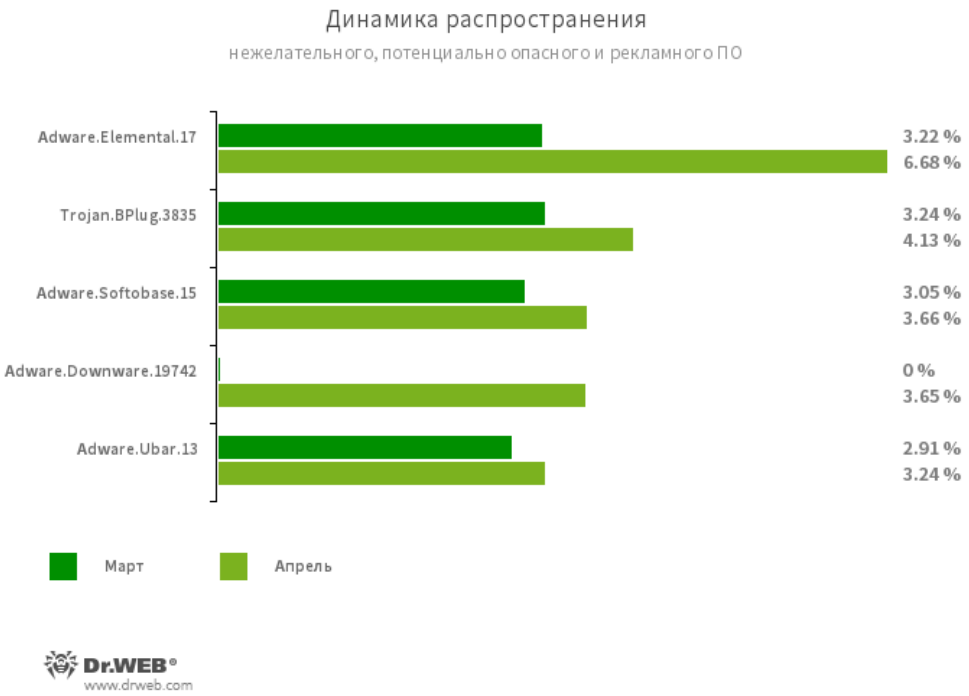
В апреле число обращений пользователей за расшифровкой файлов увеличилось на 34.27% по сравнению с мартом. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого пришлось 32.71% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ АПРЕЛЯ

- Снижение активности распространения вредоносного ПО
- Рекламные приложения остаются одними из самых активных угроз
- Значительное увеличение активности шифровальщиков

«Доктор Веб»: обзор вирусной активности в апреле 2020 года

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.Elemental.17

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

Trojan.BPlug.3835

Вредоносное расширение для браузера, предназначенное для осуществления веб-инжектов в просматриваемые пользователями интернет-страницы и блокировки сторонней рекламы.

Adware.Softobase.15

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

Adware.Downware.19742

Рекламное ПО, часто выступающее в роли промежуточного установщика пиратских программ.

Adware.Ubar.13

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

«Доктор Веб»: обзор вирусной активности в апреле 2020 года

Статистика вредоносных программ в почтовом трафике

Trojan.SpyBot.699

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

W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Exploit.CVE-2012-0158

Измененный документ Microsoft Office Word, использующий уязвимость CVE-2012-0158 для выполнения вредоносного кода.

HTML.Redirector.35

HTML.Redirector.32

Вредоносные HTML-документы, как правило маскирующиеся под безобидные вложения к письмам. При открытии перенаправляют пользователей на фишинговые сайты или загружают полезную нагрузку на заражаемые устройства.

«Доктор Веб»: обзор вирусной активности в апреле 2020 года

Шифровальщики

По сравнению с мартом в апреле в антивирусную лабораторию «Доктор Веб» поступило на 34.27% больше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

- Trojan.Encoder.26996 — 32.71%
- Trojan.Encoder.567 — 7.84%
- Trojan.Encoder.29750 — 2.73%
- Trojan.Encoder.858 — 2.39%
- Trojan.Encoder.31430 — 1.87%

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 течение апреля 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено 140 188 интернет-адресов.

Март 2020	Апрель 2020	Динамика
+ 186 881	+ 140 188	- 24.99%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В прошедшем месяце количество выявленных угроз на Android-устройствах увеличилось на 16.46% по сравнению с мартом. В каталоге Google Play вновь были найдены вредоносные программы, в том числе новые модификации троянов семейства Android.Circle. Они распространялись под видом безобидных программ и выполняли команды злоумышленников. Кроме того, в вирусную базу Dr.Web были добавлены записи для детектирования рекламного трояна Android.HiddenAds.2124 и вредоносной программы Android.Joker.164, которая подписывала пользователей на платные услуги и могла исполнять произвольный код.

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

- появление новых угроз в каталоге Google Play;
- рост числа угроз, обнаруженных на защищаемых Android-устройствах.

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

«Доктор Веб»: обзор вирусной активности в апреле 2020 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
125040, 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