Dr.WEB®
с 1992 года

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

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

19 июня 2020 года

В мае анализ данных статистики Dr.Web показал снижение общего числа обнаруженных угроз на 25.59% по сравнению с апрелем. Количество уникальных угроз также снизилось — на 5.35%. Чаще всего пользователей атаковали программы для показа рекламы, а также загрузчики и установщики вредоносного ПО. В почтовом трафике на первых позициях находится вредоносное ПО, использующее уязвимости документов Microsoft Office. Кроме того, в число самых распространенных угроз по-прежнему входит многомодульный банковский троян Trojan.SpyBot.699, а также вредоносные HTML-документы, распространяемые в виде вложений и перенаправляющие пользователей на фишинговые сайты.

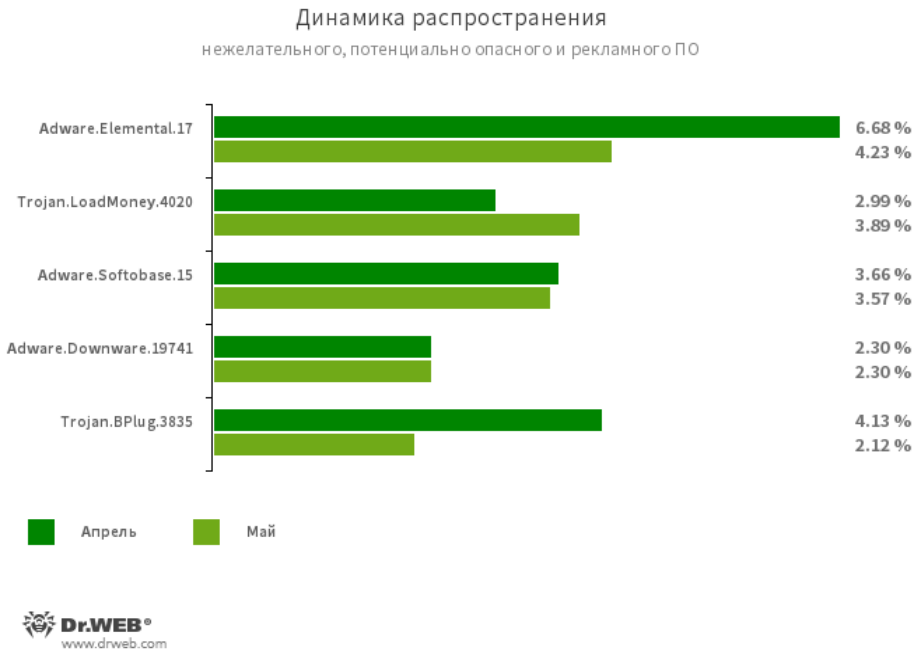
В мае статистика впервые с начала года зафиксировала снижение числа обращений пользователей за расшифровкой файлов — на 4.18% по сравнению с апрелем. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого пришлось 28.94% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАЯ

- Снижение активности распространения вредоносного ПО
- Рекламные приложения остаются в числе самых активных угроз
- Незначительное снижение активности шифровальщиков

«Доктор Веб»: обзор вирусной активности в мае 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.LoadMoney.4020
Семейство программ-установщиков, инсталлирующих на компьютеры жертв вместе с требуемыми приложениями всевозможные дополнительные компоненты. Некоторые модификации трояна могут собирать и передавать злоумышленникам различную информацию об атакованном компьютере.

Adware.Softobase.15
Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.

Adware.Downware.19741
Рекламное ПО, часто выступающее в роли промежуточного установщика пиратских программ.

Trojan.BPlug.3835
Вредоносное расширение для браузера, предназначенное для осуществления веб-инжектов в просматриваемые пользователями интернет-страницы и блокировки сторонней рекламы.

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

Статистика вредоносных программ в почтовом трафике

Exploit.CVE-2012-0158

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

W97M.DownLoader.2938

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

Trojan.SpyBot.699

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

Tool.KMS.7

Хакерские утилиты, которые используются для активации продуктов Microsoft с поддельной лицензией.

HTML.Redirector.33

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

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

Шифровальщики

По сравнению с апрелем в мае в антивирусную лабораторию «Доктор Веб» поступило на 4.18% меньше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

- Trojan.Encoder.26996 — 28.94%
- Trojan.Encoder.29750 — 5.39%
- Trojan.Encoder.567 — 4.39%
- Trojan.Encoder.858 — 2.40%
- Trojan.Encoder.25069 — 1.80%

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 мая 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено 107 082 интернет-адреса.

Апрель 2020	Май 2020	Динамика
+ 140 188	+ 107 082	- 23.62%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

По сравнению с апрелем в прошедшем месяце число угроз, обнаруженных на Android-устройствах, выросло чуть более чем на 3%. В течение мая вирусные аналитики компании «Доктор Веб» выявили множество вредоносных программ в каталоге Google Play. Среди них были новые рекламные трояны семейства Android.HiddenAds, а также различные модификации вредоносных приложений Android.Joker, подписывающих пользователей на платные услуги и выполняющих произвольный код.

В вирусную базу Dr.Web были добавлены записи для детектирования различных банковских троянов, а также трояна-шпиона, который распространялся под видом программы для отслеживания статистики заражений COVID-19. В конце месяца наши специалисты обнаружили вредоносное приложение Android.FakeApp.176, которое мошенники выдавали за мобильную версию игры Valorant. Оно использовалось для незаконной монетизации через партнерские сервисы.

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

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

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

«Доктор Веб»: обзор вирусной активности в мае 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