Dr.WEB®
с 1992 года

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

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

19 марта 2020 года

В феврале анализ данных статистики Dr.Web показал рост общего числа обнаруженных угроз на 4.86% по сравнению с январем. При этом количество уникальных угроз снизилось на 8.38%. Большинство обнаруженных угроз по-прежнему приходится на долю рекламных программ. В почтовом трафике доминирует вредоносное ПО, использующее уязвимости документов Microsoft Office. Вместе с тем продолжает расти число обнаружений банковского трояна Trojan.SpyBot.699.

В феврале число обращений пользователей за расшифровкой файлов увеличилось на 12.32% по сравнению с январем. Самым распространенным энкодером остается Trojan.Encoder.26996, на долю которого пришлось 29.06% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ ФЕВРАЛЯ

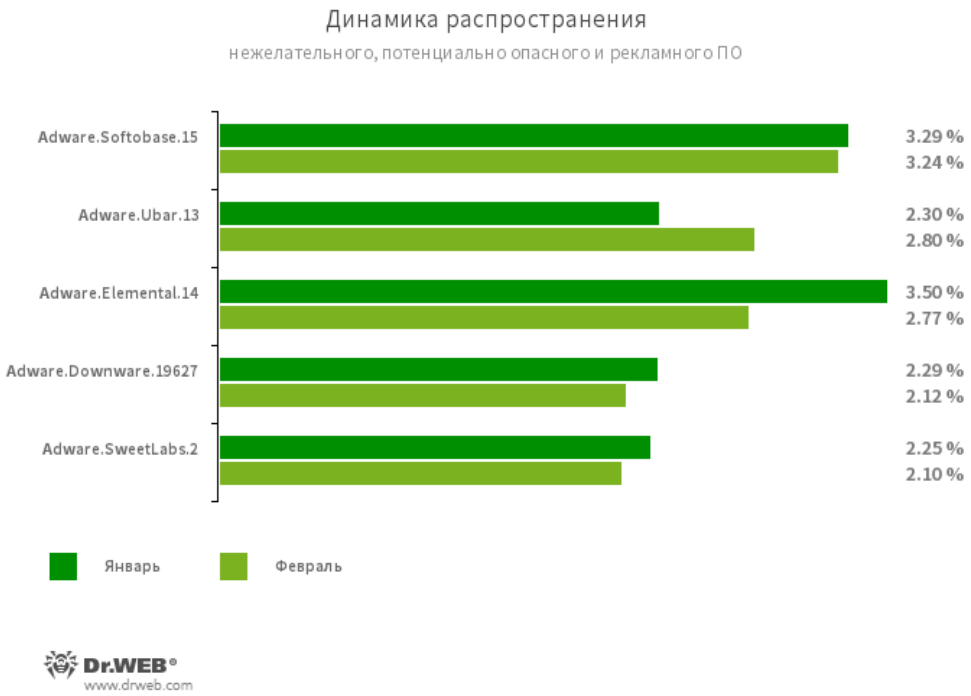
- Рекламное ПО остается в числе самых распространенных угроз
- Увеличение активности шифровальщиков

Угроза месяца

В феврале специалисты «Доктор Веб» сообщили о компрометации ссылки на скачивание программы для обработки видео и звука VSDC в каталоге популярного сайта CNET. Вместо оригинальной программы посетители сайта получали измененный установщик с легитимным набором файлов утилиты для удаленного администрирования TeamViewer и трояном-загрузчиком, который скачивал из репозитория дополнительные вредоносные модули. Таким образом на зараженный компьютер попадал троян семейства **BackDoor.TeamViewer**, устанавливающий несанкционированное соединение с зараженным компьютером, а также скрипт для обхода встроенной антивирусной защиты ОС Windows. С их помощью злоумышленники получали возможность доставлять на инфицированные устройства полезную нагрузку в виде вредоносных приложений, таких как стилеры, кейлоггеры, прокси и RAT-трояны.

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

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.Softobase.15

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

Adware.Ubar.13

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

Adware.Elemental.14

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.

Adware.Downware.19627

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

Adware.SweetLabs.2

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

«Доктор Веб»: обзор вирусной активности в феврале 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.

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.

Exploit.ShellCode.69

Вредоносный документ Microsoft Office Word. Использует уязвимость CVE-2017-11882.

Tool.KMS.7

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

Шифровальщики

По сравнению с январем в феврале в антивирусную лабораторию «Доктор Веб» поступило на 12.32% больше запросов на расшифровку файлов от пользователей, пострадавших от шифровальщиков.

- Trojan.Encoder.26996 — 18.48%
- Trojan.Encoder.567 — 10.38%
- Trojan.Encoder.29750 — 4.81%
- Trojan.Encoder.858 — 3.54%
- Trojan.Encoder.11464 — 2.78%

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 февраля 2020 года в базу нерекомендуемых и вредоносных сайтов было добавлено 90 385 интернет-адресов.

Январь 2020	Февраль 2020	Динамика
+ 97 166	+ 90 385	- 6.98%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В феврале антивирусные продукты Dr.Web для Android обнаружили на защищаемых устройствах почти на 12% меньше угроз по сравнению с январем. Число выявленных вредоносных, рекламных и потенциально опасных программ уменьшилось, при этом количество обнаруженных нежелательных приложений, наоборот, возросло.

В каталоге Google Play наши специалисты выявили новые угрозы, среди которых были рекламные трояны, мошеннические и другие вредоносные приложения.

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

- появление новых угроз в каталоге Google Play;
- снижение общего числа угроз, выявленных на защищаемых устройствах.

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

«Доктор Веб»: обзор вирусной активности в феврале 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