Dr.WEB®
с 1992 года

Обзор вирусной активности в феврале 2019 года

Обзор вирусной активности в феврале 2019 года

1 марта 2019 года

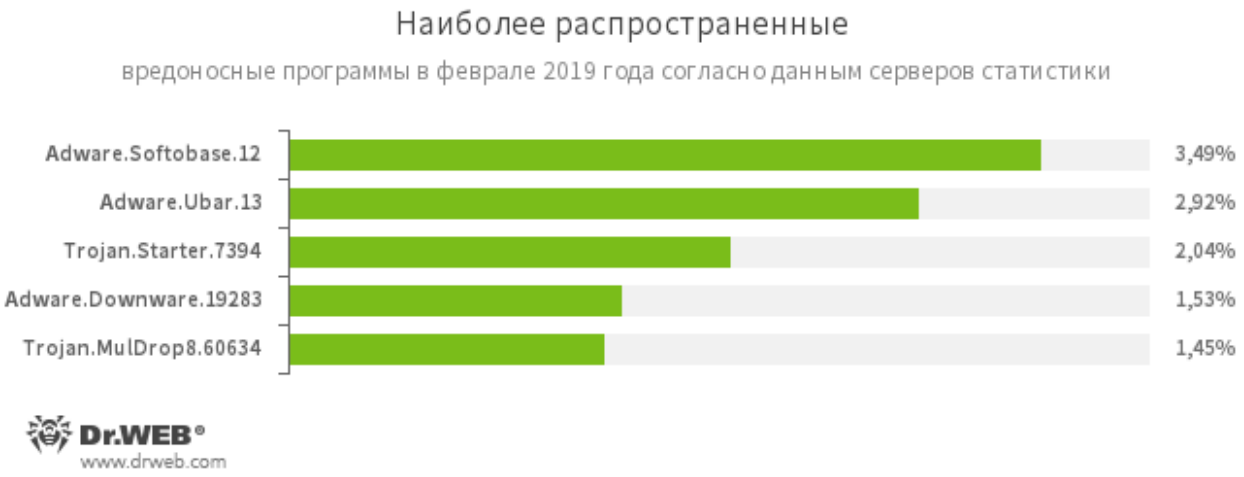
В феврале статистика серверов Dr.Web зарегистрировала снижение количества уникальных угроз на 9.73% по сравнению с прошлым месяцем. Активность вирусного программного обеспечения оказалась не сильно выше уровня декабря 2018, но среди некоторых угроз наблюдалась небольшая динамика. К примеру, **JS.Miner.28**, активность которого выросла в январе, продолжил расти и окончательно вытеснил своего конкурента **JS.Miner.11**. Троянец **Trojan.Starter.7394** вырос на 14.29% процентов по сравнению с январем, а **Trojan.DownLoader26.28109** снизил свою активность почти в три раза. Кроме того, в базу нерекомендуемых и вредоносных сайтов было добавлено на 1.68% меньшее доменов, а в техническую поддержку «Доктор Веб» поступило меньше запросов на расшифровку данных.

Главные тенденции февраля

- Уменьшилось количество угроз, найденных в почте
- Участилось использование рекламного ПО, торрент-клиентов и нежелательных программ

Обзор вирусной активности в феврале 2019 года

По данным серверов статистики «Доктор Веб»



Угрозы этого месяца:

Adware.Softobase.12
Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.
Adware.Ubar.13
Торрент-клиент, устанавливающий нежелательное ПО на устройство.
Trojan.Starter.7394
Троянец, предназначенный для запуска другого вредоносного ПО на устройстве.
Adware.Downware.19283
Программа-установщик, обычно распространяется с пиратским контентом. При установке может менять настройки браузеров и устанавливать другие нежелательные программы.
Trojan.MulDrop8.60634
Устанавливает других троянцев в систему. Все устанавливаемые компоненты содержатся в самом теле Trojan.MulDrop.

Снизилось количество угроз от:

Trojan.Encoder.11432
Известен так же как WannaCry. Блокирует доступ к данным с помощью шифрования. Для разблокировки требует перечислить деньги на счет разработчика. Массово поразил устройства по всему миру в мае 2017 года.
Trojan.DownLoader26.28109
Загружает и выполняет вредоносные программы без согласия пользователя.

Статистика вредоносных программ в почтовом трафике

JS.DownLoader.1225
Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
W97M.DownLoader.2938
Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.
Exploit.ShellCode.69
Еще один вредоносный документ Microsoft Office Word. Использует уязвимость CVE-2017-11882.
Exploit.Rtf.CVE2012-0158
Измененный документ Microsoft Office Word, использующий уязвимость CVE2012-0158 для выполнения вредоносного кода.
JS.Miner.28
Майнер под названием «CryptoLoot». Представляет собой написанный на языке JavaScript сценарий. Предназначен для скрытого майнинга в браузере и используется как альтернатива CoinHive.
Trojan.PWS.Stealer.23680
Семейство троянцев, предназначенных для хищения с инфицированного компьютера паролей и другой конфиденциальной информации.

Шифровальщики

В феврале в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих троянцев-шифровальщиков:

- Trojan.Encoder.858 — 31.39%;
- Trojan.Encoder.18000 — 10.18%;
- Trojan.Encoder.11464 — 4.67%;
- Trojan.Encoder.11539 — 4.67%;
- Trojan.Encoder.567 — 2.34%;
- Trojan.Encoder.25814 — 2.34%.

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 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 288 159 интернет-адресов.

Январь 2019	Февраль 2019	Динамика
+ 293 012	+ 288 159	-1.68%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В уходящем месяце специалисты компании «Доктор Веб» выявили множество вредоносных и нежелательных программ для ОС Android. В середине февраля вирусные аналитики зафиксировали рекламную кампанию, которою злоумышленники организовали для распространения троянцев Android.HiddenAds. В рекламе на популярных онлайн-ресурсах Instagram и YouTube потенциальным жертвам предлагалось установить программы для редактирования фотографий и видео. Однако в этих приложениях скрывались троянцы.

В течение февраля в вирусную базу было добавлено несколько новых записей для детектирования вредоносных приложений семейства Android.FakeApp. Эти троянцы загружали мошеннические веб-сайты, на которых пользователям за вознаграждение предлагалось пройти опросы. Для получения денег потенциальные жертвы должны были оплатить комиссию за перевод или выполнить некий проверочный платеж для подтверждения своей личности. Если они соглашались на это, то фактически отдавали мошенникам свои деньги и не получали никакого обещанного вознаграждения.

Кроме того, вирусописатели распространяли троянца Android.RemoteCode.2958, который скачивал на Android-устройства другие вредоносные приложения. Был выявлен троянец Android.Proxy.4, превращавший зараженные смартфоны и планшеты в прокси-серверы. Также вирусная база Dr.Web пополнилась записями для детектирования программ с нежелательным рекламным модулем Adware.Sharf.2 и новыми представителями семейства Adware.Patacore.

Наиболее заметное событие, связанное с «мобильной» безопасностью в феврале:

- распространение вредоносных программ в Google Play.

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

Обзор вирусной активности в феврале 2019 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