Dr.WEB®
с 1992 года

Обзор вирусной активности в апреле 2019 года

Обзор вирусной активности в апреле 2019 года

30 апреля 2019 года

В апреле статистика серверов Dr.Web зарегистрировала снижение числа уникальных угроз на 39.44% по сравнению с прошлым месяцем, а общее количество обнаруженных угроз снизилось на 14.96%. В почтовом трафике по-прежнему преобладает вредоносное ПО, использующее уязвимости программ Microsoft Office. Продолжает тенденцию прошлого месяца и статистика по вредоносному и нежелательному ПО: большая часть обнаруженных угроз приходится на долю вредоносных расширений для браузеров, нежелательных и рекламных программ.

Количество вредоносных и нерекомендуемых сайтов увеличилось на 28.04%. Один из таких ресурсов распространял банковского троянца и стилера вместе с программами для обработки видео и звука, о чем мы сообщили в начале месяца. Кроме того, специалисты «Доктор Веб» предупредили о фишинговой рассылке, отправленной с адресов известных иностранных компаний.

Главные тенденции апреля

- Снижение активности распространения вредоносного ПО
- Увеличение числа доменных имен, добавленных в базу нерекомендуемых и вредоносных сайтов

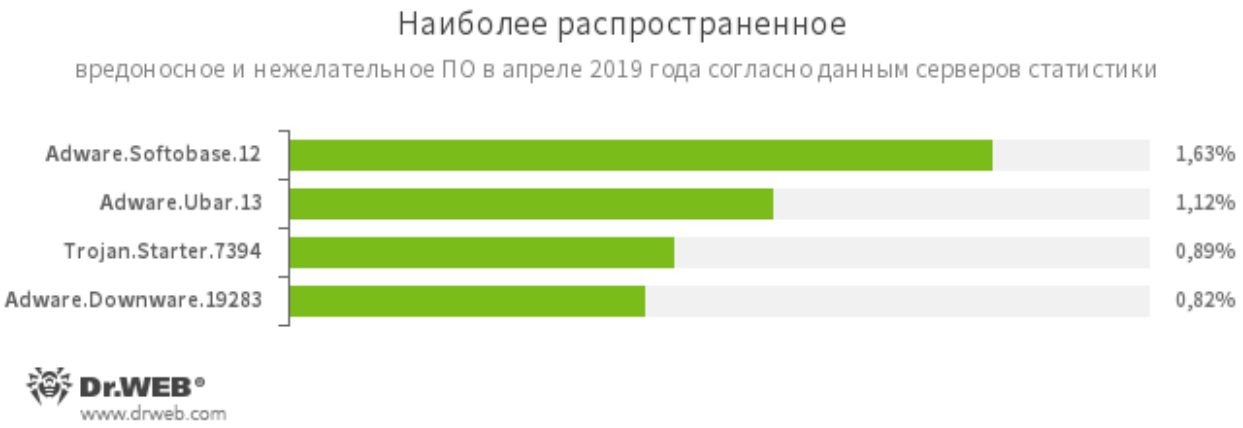
Угроза месяца

Специалисты компании «Доктор Веб» предупредили пользователей о компрометации официального сайта популярного ПО для обработки видео и звука. Хакеры заменили ссылку на скачивание, и вместе с редактором пользователи загружали опасного банковского троянца Win32.Bolik.2, а также стилера Trojan.PWS.Stealer (KPOT Stealer). Такие трояны предназначены для выполнения веб-инжектов, перехвата трафика, кейлоггинга и похищения информации из систем «банк-клиент» различных кредитных организаций. Кроме того, позднее хакеры заменили Win32.Bolik.2 на другое вредоносное ПО – один из вариантов Trojan.PWS.Stealer (KPOT Stealer).
Этот троянец крадет информацию из браузеров, аккаунта Microsoft, различных мессенджеров и других программ.

Подробнее об угрозе.

Обзор вирусной активности в апреле 2019 года

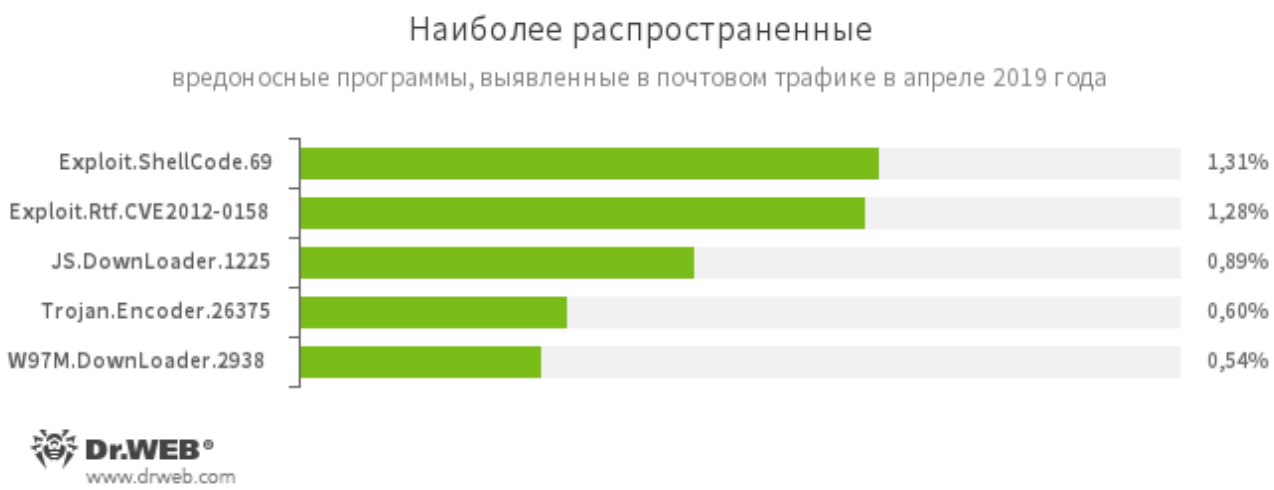
По данным серверов статистики «Доктор Веб»



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.

Статистика вредоносных программ в почтовом трафике



Exploit.ShellCode.69

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.DownLoader.1225

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

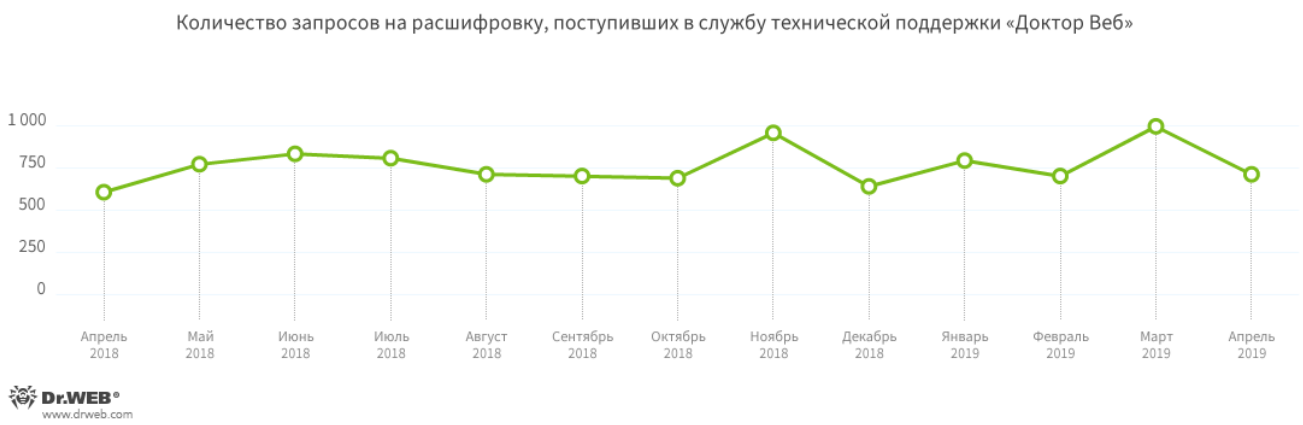
Trojan.Encoder.26375

Представитель семейства троянцев-вымогателей. Шифрует файлы на компьютере и требует от жертвы выкуп за расшифровку.

W97M.DownLoader.2938

Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Шифровальщики



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

- Trojan.Encoder.858 — 17.95%
- Trojan.Encoder.18000 — 14.65%
- Trojan.Encoder.11464 — 7.69%
- Trojan.Archivelock — 5.49%
- Trojan.Encoder.567 — 3.85%
- Trojan.Encoder.11539 — 3.85%
- Trojan.Encoder.25574 — 2.75%

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 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 345 999 интернет-адресов.

Март 2018	Апрель 2019	Динамика
+ 270 227	+ 345 999	+28.04%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В апреле компания «Доктор Веб» рассказала об опасном троянце Android.InfectionAds.1, который эксплуатировал несколько критических уязвимостей ОС Android. Благодаря им он мог заражать apk-файлы, а также самостоятельно устанавливать и удалять программы.

В течение месяца в каталоге Google Play были выявлены новые вредоносные программы, такие как троянцы-загрузчики и кликеры, а также похитители логинов и паролей от учетных записей Instagram, получившие имена **Android.PWS.Instagram.4** и **Android.PWS.Instagram.5**.

Кроме того, пользователям Android-смартфонов и планшетов угрожали банковские трояны – например, новые версии Android.Banker.**180.origin**, а также другие вредоносные приложения.

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

- обнаружение новых вредоносных программ в Google Play;
- распространение банковских троянцев.

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

Обзор вирусной активности в апреле 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