Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в декабре 2019 года

«Доктор Веб»: обзор вирусной активности в декабре 2019 года

29 января 2020 года

В декабре статистика серверов Dr.Web зафиксировала повышение роста общего числа обнаруженных угроз на 83.26% по сравнению с ноябрем. При этом количество уникальных угроз незначительно снизилось — на 0.75%. Рекламные программы и установщики по-прежнему лидируют по общему количеству обнаруженных угроз. В почтовом трафике на первых позициях находится вредоносное ПО, использующее уязвимости документов Microsoft Office.

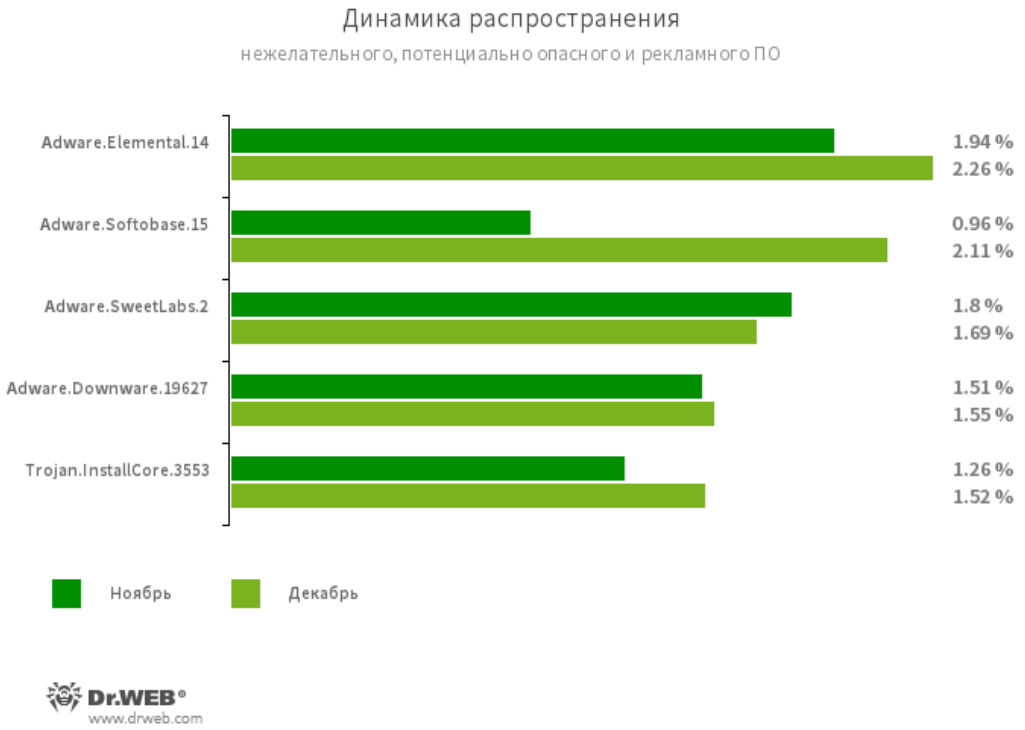
Незначительно снизилось число обращений пользователей за расшифровкой файлов, пострадавших от шифровальщиков. При этом самым активным энкодером остается Trojan.Encoder.26996 — на его долю пришлось 22.62% всех инцидентов.

ГЛАВНАЯ ТЕНДЕНЦИЯ ДЕКАБРЯ

- Повышение активности распространения вредоносного ПО
- Рекламные троянцы и рекламное ПО остаются одними из самых активных угроз
- Снижение активности шифровальщиков

«Доктор Веб»: обзор вирусной активности в декабре 2019 года

По данным серверов статистики «Доктор Веб»



Угрозы прошедшего месяца:

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.Softobase.15

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

Adware.SweetLabs.2

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

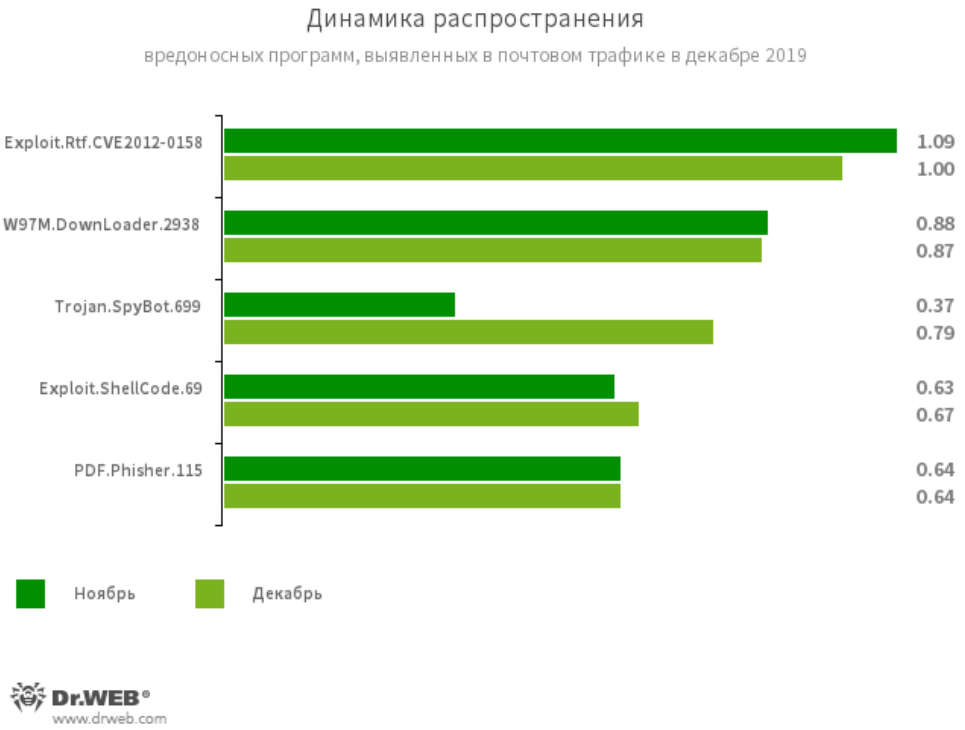
Adware.Downware.19627

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

Trojan.InstallCore.3553

Еще один известный установщик рекламного ПО. Показывает рекламу и устанавливает дополнительные программы без согласия пользователя.

Статистика вредоносных программ в почтовом трафике



Exploit.CVE-2012-0158

Измененный документ Microsoft Office Word, использующий уязвимость CVE2012-0158 для выполнения вредоносного кода.

W97M.DownLoader.2938

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

Trojan.SpyBot.699

Троянец-шпион, способный перехватывать вводимые на клавиатуре символы (кейлоггер).

Exploit.ShellCode.69

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

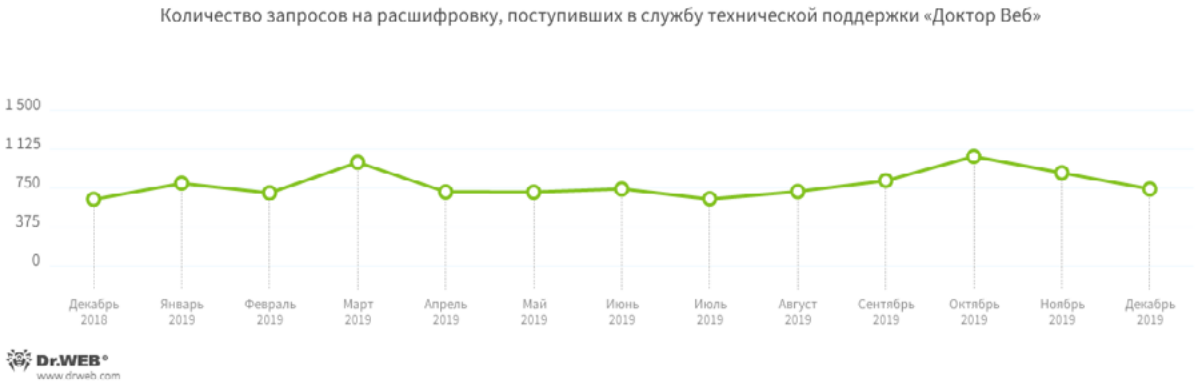
PDF.Phisher.115

PDF-документ, использующийся в фишинговой рассылке.

«Доктор Веб»: обзор вирусной активности в декабре 2019 года

Шифровальщики

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



- Trojan.Encoder.26996 — 22.62%
- Trojan.Encoder.567 — 8.75%
- **Trojan.Encoder.25574** — 6.08%
- Trojan.Encoder.858 — 3.99%
- Trojan.Encoder.28004 — 3.80%

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 декабря 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 162 535 интернет-адресов.

Ноябрь 2019	Декабрь 2019	Динамика
+ 162 581	+ 162 535	- 0.03%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В декабре злоумышленники продолжили распространять в Google Play новые модификации вредоносных программ семейства Android.Joker. Эти троянцы подписывают пользователей на платные сервисы и по команде сервера загружают и выполняют произвольный код. Кроме того, активными были и другие вредоносные приложения, основная задача которых — скачивание и запуск троянских модулей.

Наиболее заметным событием, связанным с «мобильной» безопасностью в декабре, стало обнаружение новых вредоносных программ в Google Play.

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

«Доктор Веб»: обзор вирусной активности в декабре 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