Dr.WEB®
с 1992 года

Обзор вирусной активности в январе 2019 года

Обзор вирусной активности в январе 2019 года

1 февраля 2019 года

Ушедший 2018 год выдался интересным для сферы информационной безопасности. Но, как и ожидалось, к концу года наступило затишье. Киберпреступники если не ушли в спячку, то ослабили на время активность. Однако несмотря на ожидаемое спокойствие в период новогодних праздников, наша статистика зафиксировала несколько интересных и немного тревожных тенденций января.

В середине месяца владельцев криптовалют атаковал троянец, распространявшийся под видом полезной программы. По сравнению с прошлым месяцем на 28% увеличилось количество устройств, зараженных Trojan.Winlock.14244. Кроме того, через почту было отправлено на 50% больше вредоносных файлов, использующих уязвимость Microsoft Office.

Главные тенденции января

- Увеличилось число заражений блокировщиками системы
- Участилось использование уязвимостей Microsoft Office
- Выросла активность распространения рекламного ПО

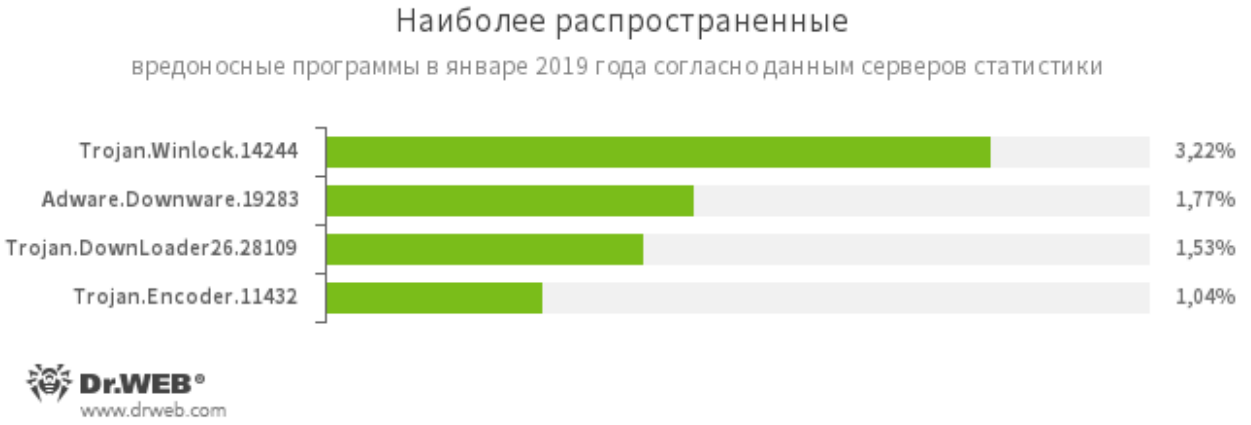
Угроза месяца

В январе аналитики «Доктор Веб» обнаружили троянца в программе для отслеживания курса криптовалют. Вредоносная программа распространялась вместе с утилитой и устанавливала на зараженные устройства других троянцев. Используя эти программы, хакеры получали возможность красть личные данные пользователей, в том числе пароли от кошельков криптовалют.

Подробнее о троянце.

Обзор вирусной активности в январе 2019 года

По данным серверов статистики «Доктор Веб»



Растущие угрозы этого месяца:

Trojan.Winlock.14244

Блокирует или ограничивает доступ пользователя к операционной системе и её основным функциям. Для разблокировки системы требует перечислить деньги на счет разработчиков троянца.

Adware.Downware.19283

Программа-установщик, обычно распространяется с пиратским контентом. При установке может менять настройки браузеров и устанавливать другие нежелательные программы.

Trojan.DownLoader26.28109

Загружает и выполняет вредоносные программы без согласия пользователя.

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.

Снизилось количество угроз от:

Trojan.Starter.7394

Троянец, предназначенный для запуска другого вредоносного ПО на устройстве пользователя.

Trojan.MulDrop8.60634

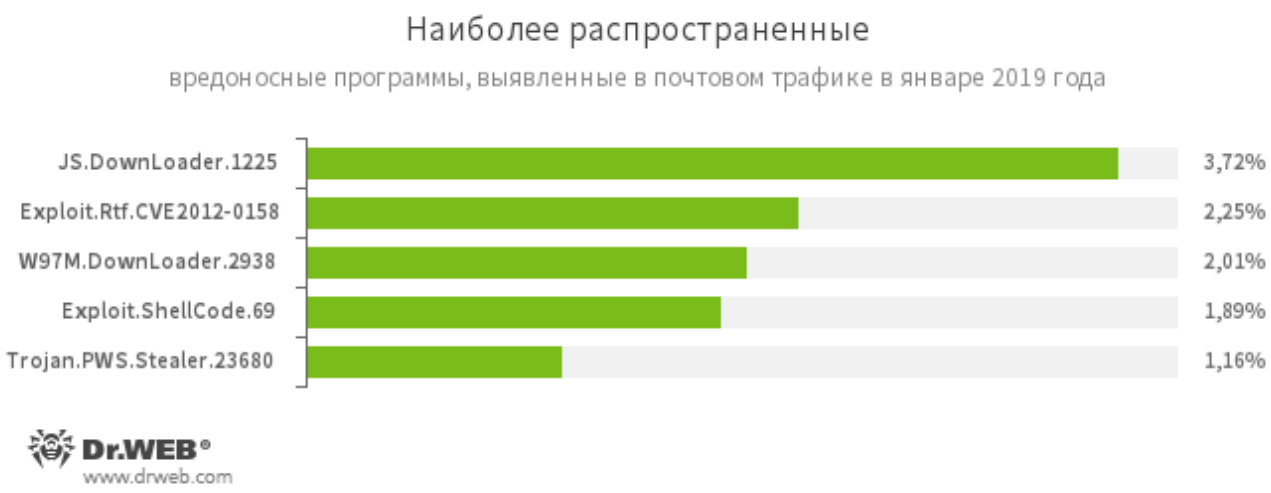
Устанавливает других троянцев в систему. Все устанавливаемые компоненты содержатся в самом теле Trojan.MulDrop.

Trojan.Zadved.1313

Рекламное ПО. Подменяет поисковую выдачу, перенаправляет пользователя на сайты рекламодателей и показывает назойливую рекламу.

Обзор вирусной активности в январе 2019 года

Статистика вредоносных программ в почтовом трафике



Выросло число заражений:

JS.DownLoader.1225

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

Exploit.Rtf.CVE2012-0158

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

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.

Trojan.PWS.Stealer.23680

Семейство троянцев, предназначенных для хищения с инфицированного компьютера паролей и другой конфиденциальной информации.

Статистика вредоносных программ в почтовом трафике

Возросла активность следующих угроз:

Trojan.Nanocore.23

Этот опасный троянец с удаленным доступом заразил почти в 4 раза больше устройств, чем в прошлом месяце. Он позволяет хакерам удаленно контролировать зараженный компьютер, в том числе включить камеру и микрофон на устройстве, если они доступны.

JS.Miner.28

Сценарий, написанный на языке JavaScript. Предназначен для скрытого майнинга в браузере. Используется как альтернатива CoinHive.

Сократилось использование такого вредоносного ПО как:

Trojan.Fbng.8

Троянец, также известный как FormBook. Предназначен для кражи персональных данных с зараженного устройства. Может получать команды с сервера разработчика.

Trojan.Encoder.26375

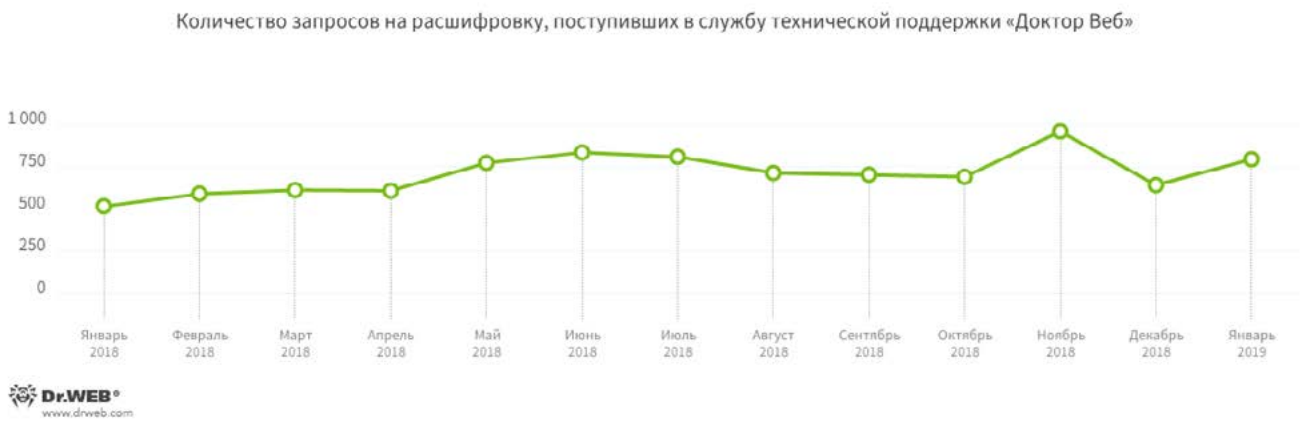
Представитель семейства троянцев-вымогателей. Шифрует файлы на компьютере и требует от жертвы выкуп за расшифровку.

JS.Miner.11

Группа сценариев, написанных на языке JavaScript. Тоже предназначены для скрытого майнинга в браузере. Используют популярный майнер — CoinHive.

Активность Trojan.SpyBot.699 незначительно снизилась в декабре, но он продолжает оставаться актуальным в последние три месяца. Этот банковский троянец позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и выполнять поступающие от них команды. Троянец предназначен для хищения средств с банковских счетов.

Шифровальщики



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

- Trojan.Encoder.11464 — 12.63%
- Trojan.Encoder.11539 — 7.72%
- Trojan.Encoder.25574 — 1.58%
- Trojan.Encoder.567 — 5.96%
- Trojan.Encoder.5342 — 0.88%

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 января 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 293 012 интернет-адресов.

Декабрь 2018	Январь 2019	Динамика
+ 257 197	+ 293012	+13.93%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

На протяжении всего января в каталоге Google Play было обнаружено множество вредоносных программ. Среди них — загрузчики семейства Android.DownLoader, которые скачивали на мобильные устройства Android-банкеров. Также злоумышленники распространяли троянцев Android.HiddenAds.361.origin и Android.HiddenAds.356.origin — после запуска они скрывали свои значки и начинали показывать рекламу. В конце месяца вирусные аналитики выявили несколько новых троянцев-кликеров семейства Android.Click, способных по команде управляющего сервера загружать любые веб-сайты. Кроме того, пользователям угрожал троянец-шпион Android.Spy.525.origin, который похищал конфиденциальную информацию.

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

- выявление в Google Play множества новых вредоносных программ;
- распространение троянца-шпиона.

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

Обзор вирусной активности в январе 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