Dr.WEB®
с 1992 года

Обзор вирусной активности в ноябре 2019 года

Обзор вирусной активности в ноябре 2019 года

11 декабря 2019 года

В ноябре статистика серверов «Доктор Веб» зафиксировала повышение общего числа обнаруженных угроз на 3.66% по сравнению с октябрем. При этом количество уникальных угроз возросло на 9.59%. В почтовом трафике на первых позициях находится вредоносное ПО, использующее уязвимости документов Microsoft Office, а также троянцы-загрузчики и стилеры. Большинство обнаруженных угроз приходится на долю рекламных программ. В течения месяца в каталоге Google Play были найдены новые вредоносные приложения для Android-устройств. Среди них — опасный бэкдор, рекламные троянцы и троянцы, которые подписывали жертв на платные услуги.

Главные тенденции ноября

- Рост активности распространения вредоносного ПО
- Снижение активности шифровальщиков

Обзор вирусной активности в ноябре 2019 года

По данным серверов статистики «Доктор Веб»

Угрозы этого месяца:

Adware.Elemental.14

Детектирование рекламных программ, которые путем подмены ссылок загружаются с файлообменных сервисов при попытке скачать с них те или иные файлы. Вместо ожидаемых файлов жертвы получают эти приложения, которые показывают рекламу, а также инсталлируют ненужное ПО.

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.

Adware.Ubar.13

Торрент-клиент, устанавливающий на устройство нежелательное ПО.

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.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 документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

PDF.Phisher.115
: Pdf-документ, использующийся в фишинговой рассылке.

Exploit.ShellCode.69
: 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.

Шифровальщики

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

- Trojan.Encoder.26996 — 34.31%
- Trojan.Encoder.858 — 10.42%
- Trojan.Encoder.567 — 3.19%
- Trojan.Encoder.28004 — 3.06%
- Trojan.Encoder.10700 — 2.08%

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

Семейство троянцев, предназначенных для хищения на инфицированном компьютере

Опасные сайты

В течение ноября 2019 года в базу нерекомендуемых и вредоносных сайтов был добавлен 162 581 интернет-адрес.

Октябрь 2019	Ноябрь 2019	Динамика
+ 254 849	+ 162 581	- 36.2%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В ноябре в каталоге Google Play были выявлены очередные вредоносные программы. Пользователям снова угрожали рекламные троянцы семейства Android.HiddenAds, которые показывают надоедливые баннеры и мешают нормальной работе с Android-устройствами. Кроме того, злоумышленники распространяли вредоносные приложения семейства Android.Joker. Эти троянцы шпионят за жертвами, подписывают их на платные услуги, а некоторые модификации могут выполнять произвольный код и запускать дополнительные вредоносные модули.

Также вирусные аналитики «Доктор Веб» обнаружили новую версию бэкдора Android.Backdoor.735.origin, который выполняет команды злоумышленников и предназначен для кибершпионажа.

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

- появление новых угроз в каталоге Google Play.

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

Обзор вирусной активности в ноябре 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