Dr.WEB®
с 1992 года

Обзор вирусной активности в октябре 2019 года

Обзор вирусной активности в октябре 2019 года

13 ноября 2019 года

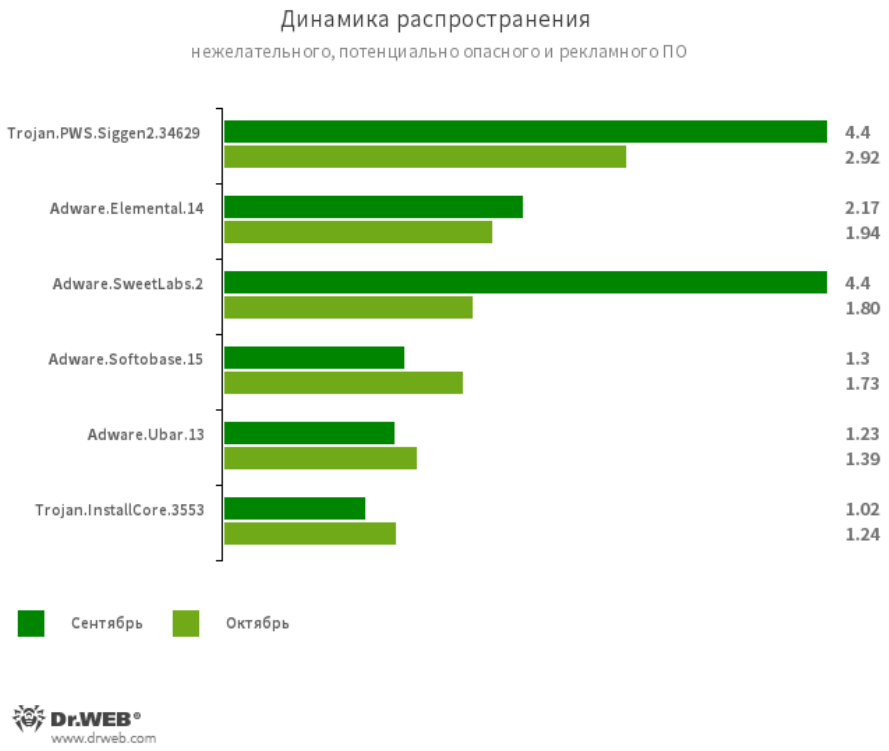
В октябре статистика серверов Dr.Web зафиксировала повышение роста общего числа обнаруженных угроз по сравнению с сентябрем. При этом количество уникальных угроз уменьшилось на 6.86%. В почтовом трафике на первых позициях находится вредоносное ПО, использующее уязвимости документов Microsoft Office, а также фишинговые рассылки. В статистике по вредоносному и нежелательному ПО лидирует троянец, предназначенный для кражи паролей, но большая часть обнаруженных угроз все еще приходится на долю рекламных программ.

Главные тенденции октября

- Снижение активности распространения уникального вредоносного ПО
- Повышение активности шифровальщиков

Обзор вирусной активности в октябре 2019 года

По данным серверов статистики «Доктор Веб»



Угрозы этого месяца:

Trojan.PWS.Siggen2.34629

Троянец, предназначенный для кражи паролей.

Adware.Elemental.14

Детектирование рекламных программ, которые путем подмены ссылок загружаются при попытке скачать те или иные файлы с файлообменных сервисов. 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.Softobase.15

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

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.Siggen2.34629
Троянец, предназначенный для кражи паролей.

Trojan.PWS.Stealer.19347
Семейство троянцев, предназначенных для хищения с инфицированного компьютера паролей и другой конфиденциальной информации.

Обзор вирусной активности в октябре 2019 года

Шифровальщики

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

Чаще всего обращения были связаны со следующими энкодерами:

- Trojan.Encoder.858 — 16.34%
- Trojan.Encoder.10700 — 6.27%
- Trojan.Encoder.29750 — 2.81%
- Trojan.Encoder.11539 — 2.64%
- Trojan.Encoder.25574 — 2.64%
- ACCDFISA v2 — 2.48%
- Trojan.Encoder.11464 — 2.15%

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 октября 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 254 849 интернет-адресов.

Сентябрь 2019	Октябрь 2019	Динамика
+ 238 637	+ 254 849	+ 6.79%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В прошедшем месяце вирусные аналитики компании «Доктор Веб» выявили большое число угроз в каталоге Google Play. Среди них были троянцы-кликеры из семейства Android.Click — они подписывали пользователей на платные услуги. Кроме того, злоумышленники распространяли рекламных троянцев Android.HiddenAds и вредоносные программы Android.SmsSpy, которые перехватывали входящие СМС-сообщения. В течение октября наши специалисты обнаружили новые модификации троянцев семейства Android.Joker. По команде злоумышленников они могли выполнять произвольный код, запускать дополнительные вредоносные модули и автоматически подписывали жертв на дорогостоящие мобильные сервисы.

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

- активное распространение вредоносных программ через каталог Google Play.

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

Обзор вирусной активности в октябре 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