Dr.WEB®
с 1992 года

Обзор вирусной активности в мае 2019 года

Обзор вирусной активности в мае 2019 года

3 июня 2019 года

В мае статистика серверов Dr.Web зарегистрировала повышение числа уникальных угроз на 1.49% по сравнению с прошлым месяцем, а общее количество обнаруженных угроз повысилось на 14.51%. Статистика по вредоносному и нежелательному ПО показывает преобладание рекламных программ и установщиков. В почтовом трафике по-прежнему доминирует вредоносное ПО, использующее уязвимости документов Microsoft Office, но в мае также усилилось распространение опасного троянца Trojan.Fbng.8 (FormBook).

Главные тенденции мая

- Повышение активности распространения вредоносного ПО
- Рассылка стилеров через почту

Угроза месяца

В мае специалисты «Доктор Веб» сообщили о новой угрозе для операционной системы macOS – Mac.BackDoor.Siggen.20. Это ПО позволяет загружать и исполнять на устройстве пользователя любой код на языке Python. Сайты, распространяющие это вредоносное ПО, также заражают компьютеры под управлением ОС Windows шпионским троянцем BackDoor.Wirenet.517 (NetWire). Последний является давно известным RAT-троянцем, с помощью которого хакеры могут удаленно управлять компьютером жертвы, включая использование камеры и микрофона на устройстве. Кроме того, распространяемый RAT-троянец имеет действительную цифровую подпись В мае специалисты «Доктор Веб» сообщили о новой угрозе для операционной системы macOS – Mac.BackDoor.Siggen.20. Это ПО позволяет загружать и исполнять на устройстве пользователя любой код на языке Python. Сайты, распространяющие это вредоносное ПО, также заражают компьютеры под управлением ОС Windows шпионским троянцем BackDoor.Wirenet.517 (NetWire). Последний является давно известным RAT-троянцем, с помощью которого хакеры могут удаленно управлять компьютером жертвы, включая использование камеры и микрофона на устройстве. Кроме того, распространяемый RAT-троянец имеет действительную цифровую подпись.

Подробнее об угрозе

Обзор вирусной активности в мае 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.InstallCore.3553

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

Trojan.Winlock.14244

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

Trojan.Starter.7394

Троянец, предназначенный для запуска другого вредоносного ПО на устройстве.

Статистика вредоносных программ в почтовом трафике

W97M.DownLoader.2938
Семейство троянцев-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

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.

Exploit.Rtf.435
Вредоносный документ Microsoft Office, использующий уязвимость CVE-2017-11882 для загрузки Trojan.Fbng.8 (FormBook) на устройство пользователя.

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

Возросла активность:

Trojan.Inject3.15480
Троянец, также известный как Trojan.Fbng.8 (FormBook). Предназначен для кражи персональных данных с зараженного устройства. Может получать команды с сервера разработчика.

Шифровальщики

- Trojan.Encoder.18000 — 15.38%
- Trojan.Encoder.858 — 9.89%
- Trojan.Encoder.11464 — 5.49%
- Trojan.Encoder.25574 — 5.49%
- Trojan.Encoder.11539 — 5.27%
- Trojan.Archivelock — 5.05%
- Trojan.Encoder.567 — 1.98%

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 мая 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 223 952 интернет-адреса.

Апрель 2018	Май 2019	Динамика
+ 345 999	+ 223 952	- 35.27%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В последнем весеннем месяце этого года злоумышленники вновь распространяли различные вредоносные программы через каталог Google Play. В начале мая специалисты компании «Доктор Веб» выявили троянца Android.HiddenAds.1396, который постоянно показывал рекламные баннеры и перекрывал ими интерфейс других приложений и операционной системы. Позднее были обнаружены троянцы-шпионы Android.SmsSpy.10206 и Android.SmsSpy.10263 — они крали входящие СМС и передавали их злоумышленникам.

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

- появление новых вредоносных программ в Google Play.

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

Обзор вирусной активности в мае 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