Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в мае 2021 года

«Доктор Веб»: обзор вирусной активности в мае 2021 года

22 июня 2021 года

В мае анализ данных статистики Dr.Web показал уменьшение общего числа обнаруженных угроз на 32.46% по сравнению с апрелем. При этом количество уникальных угроз увеличилось на 31.4%. Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике по частоте распространения лидирует разнообразное вредоносное ПО, в том числе обфусцированные вредоносные программы, скрипты, а также приложения, использующие уязвимости документов Microsoft Office.

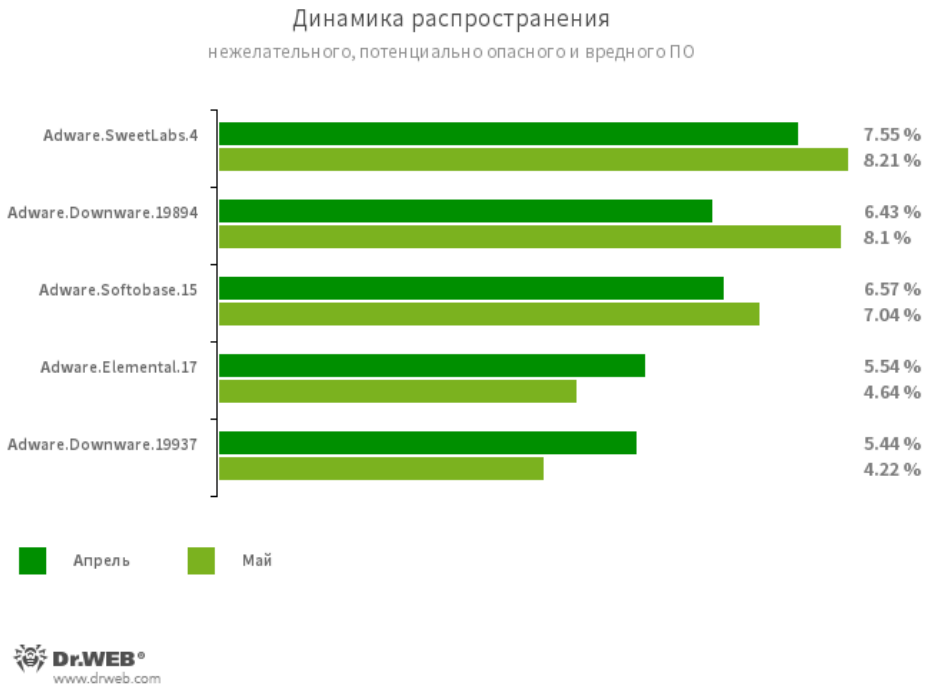
Число обращений пользователей за расшифровкой файлов увеличилось на 19.9% по сравнению с апрелем. Самым распространенным энкодером мая оказался Trojan.Encoder.26996, на долю которого приходится 25% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАЯ

- Уменьшение активности распространения вредоносного ПО
- Рекламные приложения по-прежнему являются главной угрозой
- Рост числа запросов на расшифровку файлов, затронутых шифровальщиками

«Доктор Веб»: обзор вирусной активности в мае 2021 года

По данным сервиса статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.SweetLabs.4

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

Adware.Downware.19894

Adware.Downware.19937

Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.Softobase.15

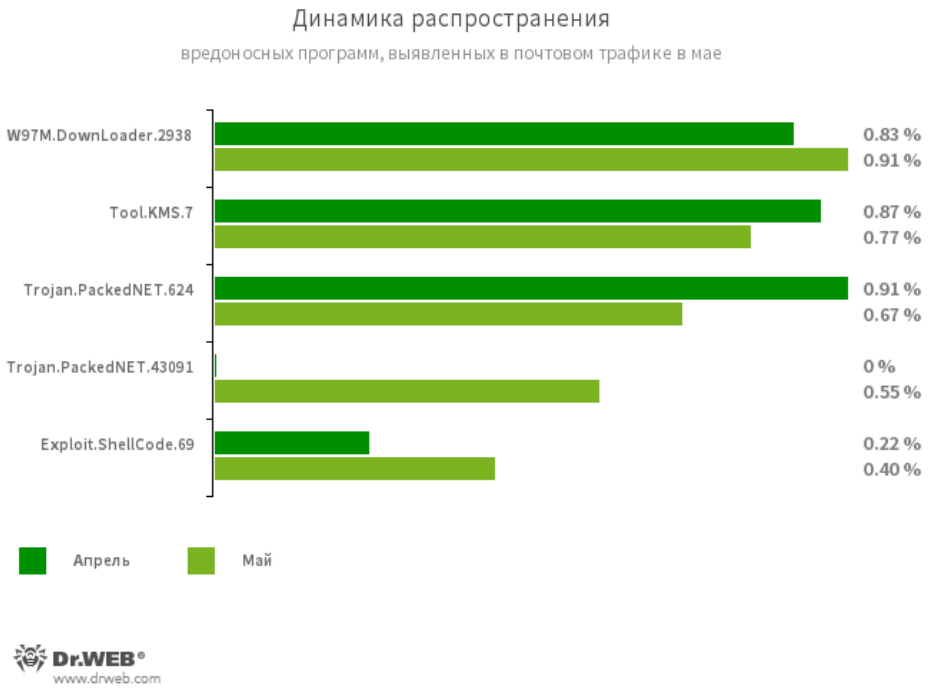
Программа-установщик, распространяющая устаревшее программное обеспечение. Изменяет настройки браузера.

Adware.Elemental.17

Семейство рекламных программ, попадающих на устройства путем подмены ссылок на файлообменных сервисах. Вместо ожидаемых файлов жертвы получают приложения с рекламой, а также инсталлируют ненужное ПО.

«Доктор Веб»: обзор вирусной активности в мае 2021 года

Статистика вредоносных программ в почтовом трафике



W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих уязвимости файлов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Tool.KMS.7

Хакерские утилиты, которые используются для активации продуктов Microsoft с поддельной лицензией.

Trojan.PackedNET.624

Trojan.PackedNET.43091

Упакованное вредоносное ПО, написанное на VB.NET.

Exploit.ShellCode.69

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

«Доктор Веб»: обзор вирусной активности в мае 2021 года

Шифровальщики

По сравнению с апрелем, в мае число запросов на расшифровку файлов, затронутых шифровальщиками, увеличилось на 19.9%.

- Trojan.Encoder.26996 — 25%
- Trojan.Encoder.567 — 13,6%
- Trojan.Encoder.11539 — 2,19%
- Trojan.Encoder.14940 — 1.75%
- Trojan.Encoder.858 — 1.35%

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 мае 2021 года интернет-аналитики «Доктор Веб» обнаружили множество сайтов, продающих поддельные документы. Злоумышленники предлагают всего за несколько тысяч рублей купить водительские права или фейковый прививочный сертификат.

Потенциальная жертва попадает на сайт после соответствующего запроса в поисковой системе. Дальше остается выбрать нужную справку — и поддельный документ почти готов.

Примечательно, что мошенники пытаются замаскировать свою деятельность под легальную, вставляя маленькие скриншоты сертификатов на осуществление медицинской деятельности, которые едва можно разглядеть. На сайтах настоящих клиник и медцентров всегда можно рассмотреть и внимательно изучить все имеющиеся лицензии.

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В мае специалисты компании «Доктор Веб» обнаружили в каталоге Google Play очередных троянов из семейства Android.FakeApp. Они распространялись под видом приложений с информацией о денежных выплатах от государства, а также программ, с помощью которых пользователи якобы могли получить бесплатные лотерейные билеты. Кроме того, были найдены новые модификации троянов Android.Joker, способных выполнять произвольный код и подписывать жертв на платные мобильные сервисы.

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

- выявление новых угроз в официальном каталоге Android-приложений Google Play;
- активность рекламных троянов, а также троянов, способных загружать и выполнять произвольный код.

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

«Доктор Веб»: обзор вирусной активности в мае 2021 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
Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124 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