Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности в мае 2022 года

«Доктор Веб»: обзор вирусной активности в мае 2022 года

14 июня 2022 года

В мае анализ данных статистики Dr.Web показал уменьшение общего числа обнаруженных угроз на 0.86% по сравнению с апрелем. При этом количество уникальных угроз незначительно увеличилось — на 1.73%. Большинство детектирований по-прежнему приходится на долю рекламных программ и нежелательных приложений. В почтовом трафике чаще всего распространялись вредоносные скрипты, стилеры, ссылки на фишинговые страницы, а также программы, использующие уязвимости документов Microsoft Office.

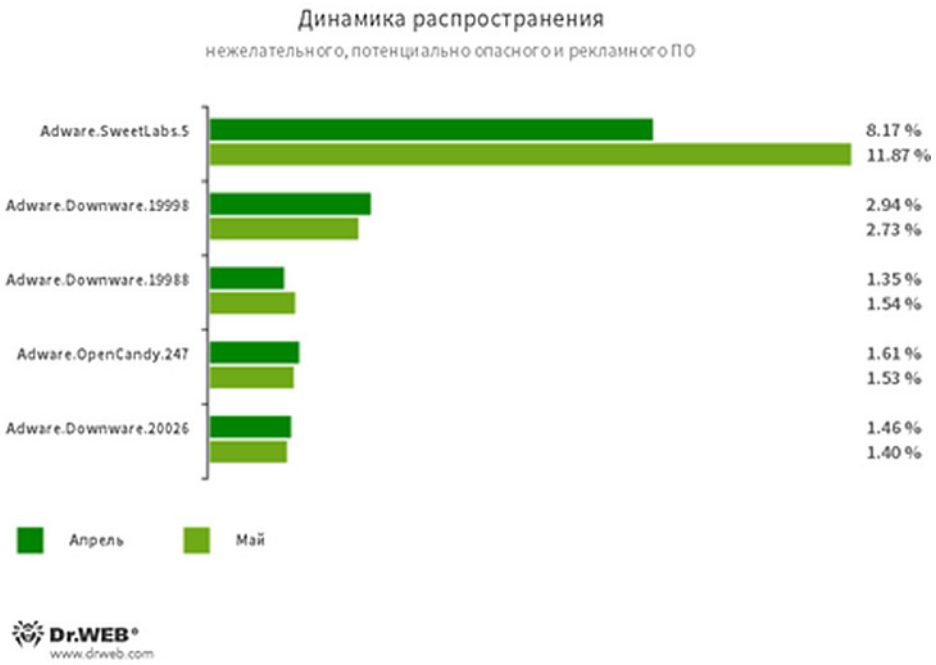
Число обращений пользователей за расшифровкой файлов уменьшилось на 2.53% по сравнению с апрелем. Самым распространенным энкодером месяца вновь стал Trojan.Encoder.26996, на долю которого пришлось 37.47% всех инцидентов.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАЯ

- Распространение вредоносного ПО в почтовом трафике;
- Рекламные приложения остаются самой массовой угрозой.

«Доктор Веб»: обзор вирусной активности в мае 2022 года

По данным сервиса статистики «Доктор Веб»



Угрозы прошедшего месяца:

Adware.SweetLabs.5
Альтернативный каталог приложений и надстройка к графическому интерфейсу Windows от создателей Adware.Opencandy.

Adware.Downware.19998
Adware.Downware.19988
Adware.Downware.20026
Рекламное ПО, выступающее в роли промежуточного установщика пиратских программ.

Adware.OpenCandy.247
Семейство приложений, предназначенных для установки на компьютер различного дополнительного рекламного ПО.

«Доктор Веб»: обзор вирусной активности в мае 2022 года

Статистика вредоносных программ в почтовом трафике

W97M.DownLoader.2938

Семейство троянов-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Они предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Trojan.PWS.Stealer.33179

Троянская программа, предназначенная для кражи паролей и другой конфиденциальной информации пользователя.

Exploit.CVE-2018-0798.4

Эксплойт, предназначенный для эксплуатации уязвимости в ПО Microsoft Office и позволяющий выполнить произвольный код.

HTML.FishForm.206

Веб-страница, распространяющаяся посредством фишинговых рассылок. Представляет собой фиктивную форму ввода учетных данных, которая имитирует авторизацию на известных сайтах. Введенные пользователем данные отправляются злоумышленникам.

JS.Redirector.435

Вредоносный скрипт, перенаправляющий пользователя на подконтрольную злоумышленникам веб-страницу.

«Доктор Веб»: обзор вирусной активности в мае 2022 года

Шифровальщики

По сравнению с апрелем, в мае число запросов на расшифровку файлов, затронутых шифровальщиками, уменьшилось на 2.53%.

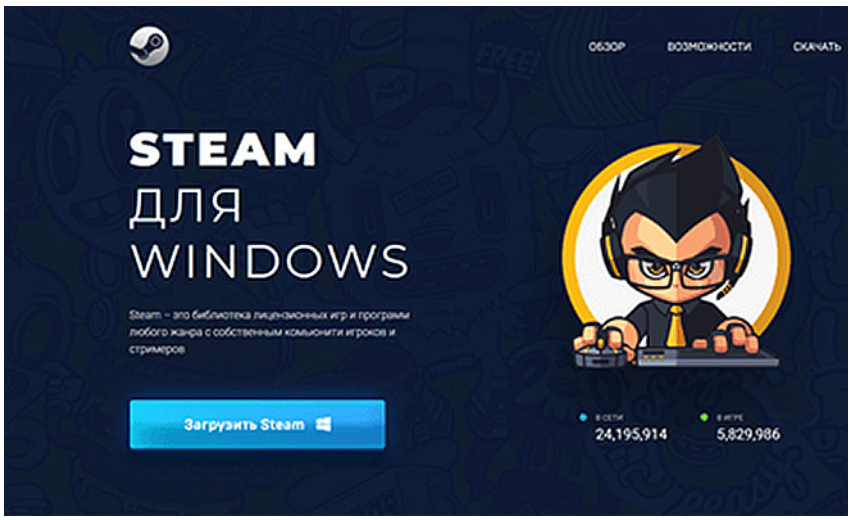
- Trojan.Encoder.26996 — 37,47%
- Trojan.Encoder.3953 — 13.93%
- Trojan.Encoder.567 — 3.72%
- Trojan.Encoder.11539 — 2.17%
- Trojan.Encoder.33749 — 1.86%

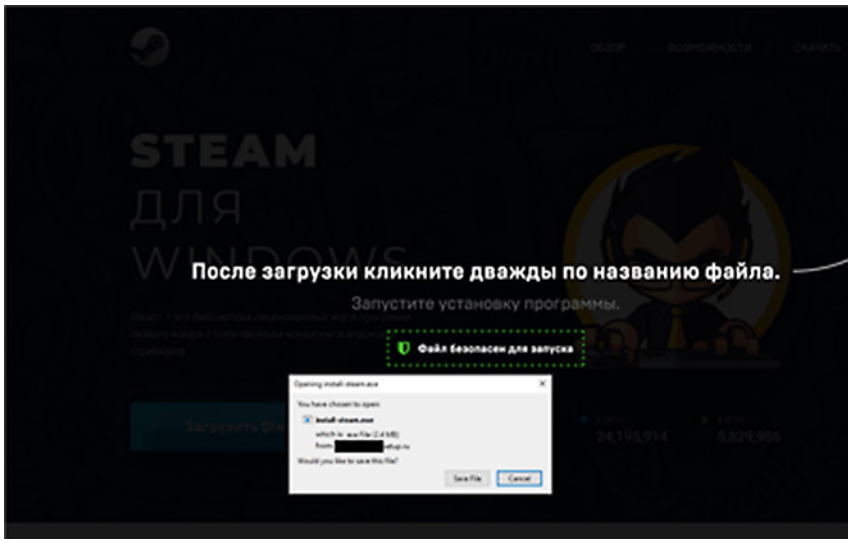
Dr.Web Security Space для Windows защищает от троянцев-шифровальщиков

Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении
Dr.Web Rescue Pack

Опасные сайты

В мае 2022 года продолжился рост числа сайтов, маскирующихся под официальные ресурсы разработчиков различного популярного ПО. Злоумышленники продолжали использовать подобные ресурсы для распространения поддельных установщиков с рекламными и вредоносными программами.





На скриншотах выше изображен пример описываемой страницы и загрузка поддельного установщика на компьютер пользователя. Сайт имеет сертификат с действительной цифровой подписью и дополнительно уведомляет пользователя о том, что файл якобы безопасен для запуска.

Узнайте больше о нерекомендуемых Dr.Web сайтах

«Доктор Веб»: обзор вирусной активности в мае 2022 года

Вредоносное и нежелательное ПО для мобильных устройств

В мае наиболее распространенной Android-угрозой вновь стал троян Android.Spy.4498, который крадет информацию из уведомлений от других приложений. В то же время его активность продолжает снижаться. Рекламные трояны Android.HiddenAds также не теряют актуальность. Их активность по сравнению с апрелем, напротив, несколько возросла.

В течение месяца специалисты компании «Доктор Веб» обнаружили в каталоге Google Play очередные вредоносные приложения. Среди них — мошеннические программы Android.FakeApp и трояны из семейства Android.Subscription, подписывающие пользователей на платные услуги. Кроме того, были выявлены новые представители семейства троянов Android.PWS.Facebook, которые крадут логины, пароли и другую информацию, необходимую для взлома учетных записей Facebook. Распространяли злоумышленники и рекламных троянов Android.HiddenAds.

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

- снижение активности трояна-шпиона Android.Spy.4498;
- рост активности рекламных троянов;
- появление новых угроз в каталоге Google Play.

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

«Доктор Веб»: обзор вирусной активности в мае 2022 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

© ООО «Доктор Веб», 2003-2022

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека