Dr.WEB®
с 1992 года

Обзор вирусной активности в феврале 2018 года

Обзор вирусной активности в феврале 2018 года

28 февраля 2018 года

В феврале распространялся троянец-шифровальщик, заражавший компьютеры под управлением Microsoft Windows. Он присваивает зашифрованным файлам расширение *.GDCB. Также последний месяц зимы запомнится появлением Android-майнера. Этот троянец мог распространяться самостоятельно, заражая сетевые устройства, на которых включен режим отладки. Среди них — смартфоны, планшеты, медиаплееры, роутеры и «умные» телевизоры.

Главные тенденции февраля

- Распространение нового энкодера для **Windows**
- Появление троянца-майнера для **Android**

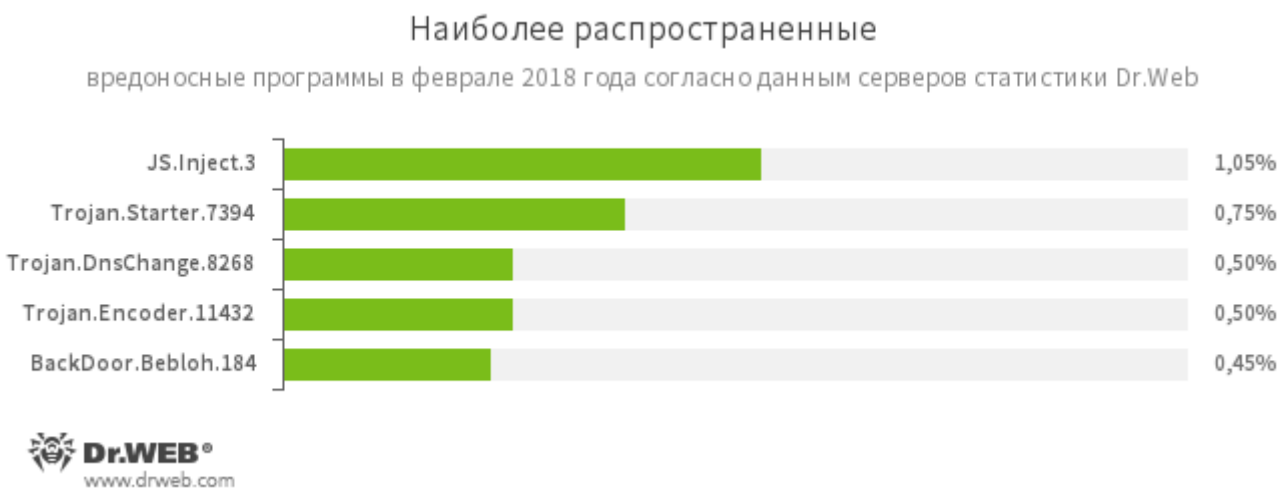
Угроза месяца

Нового троянца-шифровальщика, получившего наименование Trojan.Encoder.24384, вирусописатели назвали «GandCrab!». Он шифрует содержимое фиксированных, съемных и сетевых дисков, а зашифрованным файлам присваивает расширение *.GDCB. После запуска энкодер при определенных условиях проверяет наличие на зараженном компьютере антивирусов. Затем он завершает работающие программы по заданному вирусописателями списку и устанавливает себя в систему.

После перезагрузки компьютера Trojan.Encoder.24384 шифрует файлы на дисках, за исключением содержимого системных и служебных папок. Подробнее о принципах работы этой вредоносной программы мы рассказали в опубликованной на нашем сайте статье.

Обзор вирусной активности в феврале 2018 года

По данным статистики Антивируса Dr.Web



Trojan.Moneyinst.520

Вредоносная программа, устанавливающая на компьютер жертвы различное ПО, в том числе других троянцев.

Trojan.Starter.7394

Представитель семейства троянцев, основное назначение которых — запуск в инфицированной системе исполняемого файла с определенным набором вредоносных функций.

Trojan.Zadved

Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.

Trojan.DnsChange.8268

Вредоносная программа, подменяющая в настройках соединения на инфицированном устройстве адреса серверов DNS.

Trojan.Inject

Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.

Обзор вирусной активности в феврале 2018 года

По данным серверов статистики «Доктор Веб»

JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.

Trojan.Starter.7394

Представитель семейства троянцев, основное назначение которых — запуск в инфицированной системе исполняемого файла с определенным набором вредоносных функций.

Trojan.DnsChange.8268

Вредоносная программа, подменяющая в настройках соединения на инфицированном устройстве адреса серверов DNS.

Trojan.Encoder.11432

Сетевой червь, запускающий на компьютере жертвы опасного троянца-шифровальщика. Известен также под именем WannaCry.

BackDoor.Bebloh

Один из представителей семейства вредоносных программ, относящихся к категории банковских троянцев. Данное приложение представляет угрозу для пользователей систем дистанционного банковского обслуживания (ДБО), поскольку позволяет злоумышленникам красть конфиденциальную информацию путем перехвата заполняемых в браузере форм и встраивания в страницы сайтов некоторых банков.

Статистика вредоносных программ в почтовом трафике

BackDoor.Bebloh

Один из представителей семейства вредоносных программ, относящихся к категории банковских троянцев. Данное приложение представляет угрозу для пользователей систем дистанционного банковского обслуживания (ДБО), поскольку позволяет злоумышленникам красть конфиденциальную информацию путем перехвата заполняемых в браузере форм и встраивания в страницы сайтов некоторых банков.

JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.

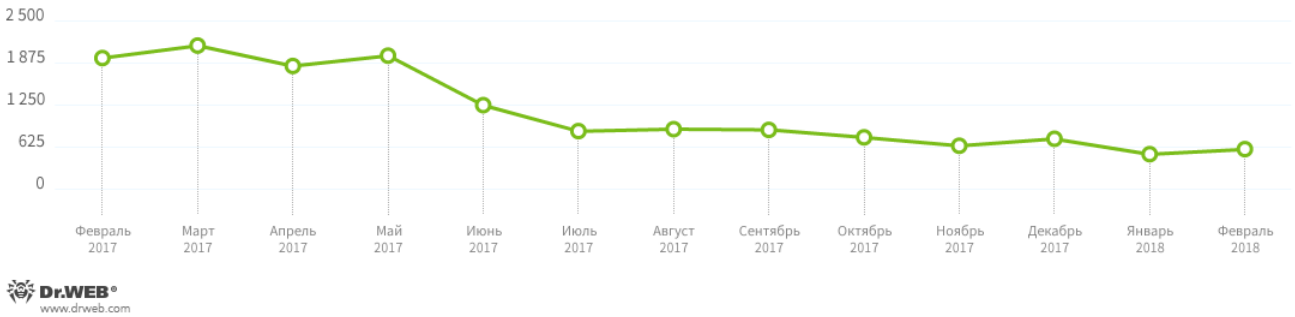
Java.Jrat.46

Вредоносная программа для удаленного управления компьютером (Remote Access Tools, RAT), написанная на языке Java.

Trojan.DownLoader

Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Шифровальщики



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

- Trojan.Encoder.858 — 24,33% обращений;
- Trojan.Encoder.567 — 8,25% обращений;
- Trojan.Encoder.24249 — 6,19% обращений;
- Trojan.Encoder.11539 — 3,92% обращений;
- Trojan.Encoder.11464 — 2,68% обращений;
- Trojan.Encoder.2667 — 2,67% обращений.

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 февраля 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено на 278,9% интернет-адресов больше, чем в предыдущем месяце.

Январь 2018	Февраль 2018	Динамика
+ 309 933	+ 1 174 380	+278.9%

Вредоносное и нежелательное ПО для мобильных устройств

В феврале специалисты по информационной безопасности обнаружили троянца-майнера Android.CoinMine.15. Он мог удаленно заражать подключенные к сети Android-смартфоны, планшеты, телевизоры, роутеры, а также медиаплееры с активным режимом отладки. Если заражение удавалось, вредоносная программа пыталась обнаружить другие подключенные к сети устройства и устанавливала на них свою копию. Кроме того, в уходящем месяце киберпреступники распространяли через каталог Google Play банковского троянца Android.BankBot.336.origin, который похищал у пользователей конфиденциальные данные и деньги.

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

- обнаружение троянца-майнера, способного автоматически заражать подключенные к сети Android-устройства;
- распространение нового банковского троянца.

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

Обзор вирусной активности в феврале 2018 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 страна