Dr.WEB®
с 1992 года

Обзор вирусной активности в ноябре 2017 года

Обзор вирусной активности в ноябре 2017 года

30 ноября 2017 года

В ноябре специалисты компании «Доктор Веб» исследовали нового представителя семейства банковских троянцев Trojan.Gozi. В отличие от своих предшественников, обновленный троянец полностью состоит из набора модулей, а также лишился механизма генерации имен управляющих серверов: теперь они «зашиты» в конфигурации вредоносной программы.

Также в ноябре был обнаружен новый бэкдор для ОС семейства Linux и выявлено несколько мошеннических сайтов, выманивающих у доверчивых пользователей Интернета деньги от имени несуществующего общественного фонда.

Главные тенденции ноября

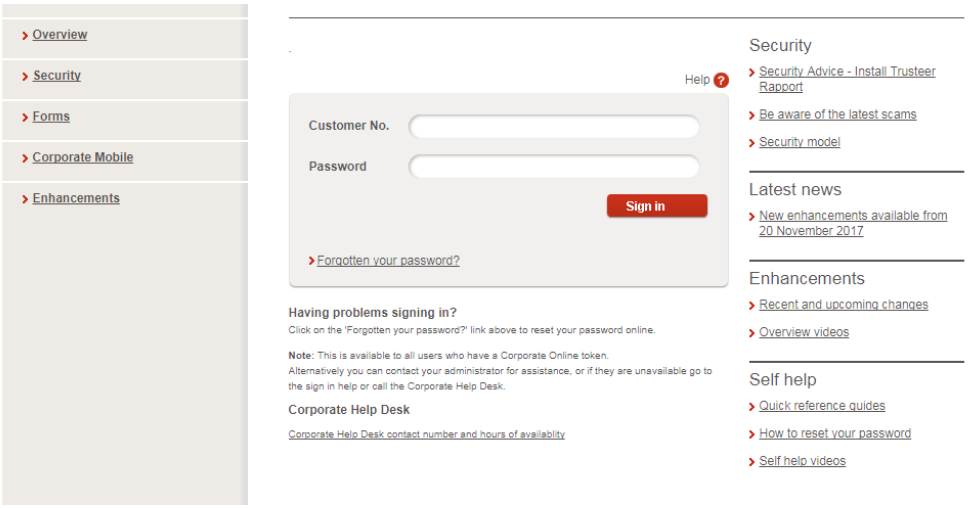
- Появление нового банковского троянца
- Распространение бэкдора для ОС семейства Linux
- Возникновение нового вида мошенничества в Интернете

Обзор вирусной активности в ноябре 2017 года

Угроза месяца

Семейство банковских троянцев Gozi хорошо знакомо вирусным аналитикам — один из его представителей запомнился тем, что использовал в качестве словаря для генерации адресов управляющих серверов текстовый файл, скачанный с сервера NASA. Новая версия банковского троянца, получившая наименование Trojan.Gozi.64, может заражать компьютеры под управлением 32- и 64-разрядных версий Microsoft Windows 7 и выше, в более ранних версиях этой ОС вредоносная программа не запускается.

Основное предназначение Trojan.Gozi.64 заключается в выполнении веб-инжектов, то есть он может встраивать в просматриваемые пользователем веб-страницы посторонее содержимое – например, поддельные формы авторизации на банковских сайтах и в системах банк-клиент.



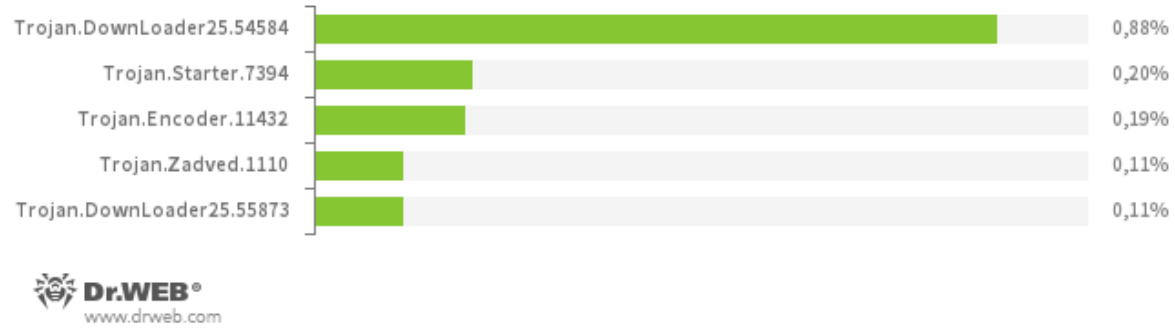
При этом, поскольку модификация веб-страниц происходит непосредственно на зараженном компьютере, URL такого сайта в адресной строке браузера остается корректным, что может ввести пользователя в заблуждение и усыпить его бдительность. Введенные в поддельную форму данные передаются злоумышленникам, в результате чего учетная запись жертвы троянца может быть скомпрометирована.

Более подробную информацию о функциях, принципах работы и возможностях Trojan.Gozi.64 вы можете получить, ознакомившись с опубликованной на нашем сайте статьей.

Обзор вирусной активности в ноябре 2017 года

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web

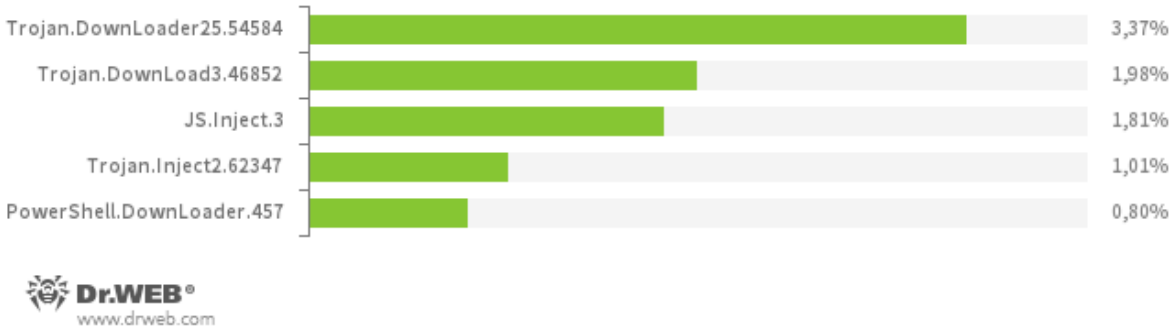


- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Starter.7394**
  Представитель семейства троянцев, основное назначение которых — запуск в инфицированной системе исполняемого файла с определенным набором вредоносных функций.
- **Trojan.Encoder.11432**
  Многокомпонентный сетевой червь, известный под именем WannaCry. Способен заражать компьютеры под управлением Microsoft Windows без участия пользователя. Шифрует файлы на компьютере и требует выкуп. Расшифровка тестовых и всех остальных файлов выполняется с использованием разных ключей – следовательно, никаких гарантий успешного восстановления поврежденных шифровальщиком данных даже в случае оплаты выкупа не существует.
- **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.

Обзор вирусной активности в ноябре 2017 года

По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в ноябре 2017 года согласно данным серверов статистики Dr.Web

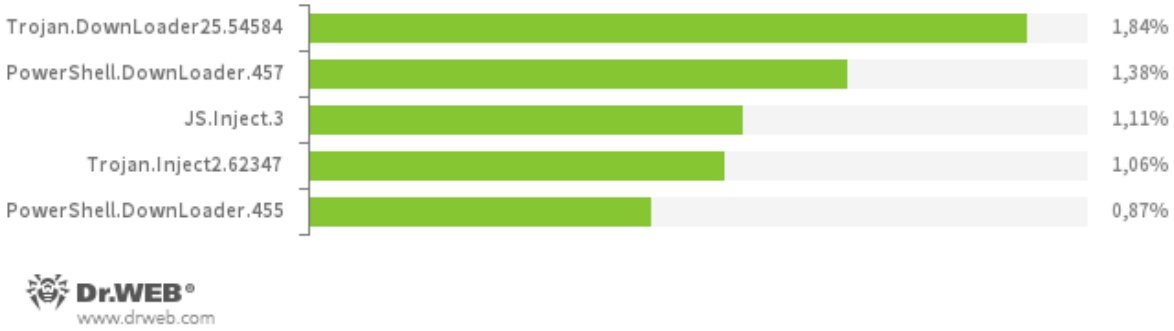


- **Trojan.DownLoader25.54584, Trojan.DownLoad3.46852**
  Представители семейств троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **JS.Inject**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.
- **PowerShell.DownLoader**
  Семейство вредоносных файлов, написанных на языке сценариев PowerShell. Загружают и устанавливают на компьютер другие вредоносные программы.

Обзор вирусной активности в ноябре 2017 года

Статистика вредоносных программ в почтовом трафике

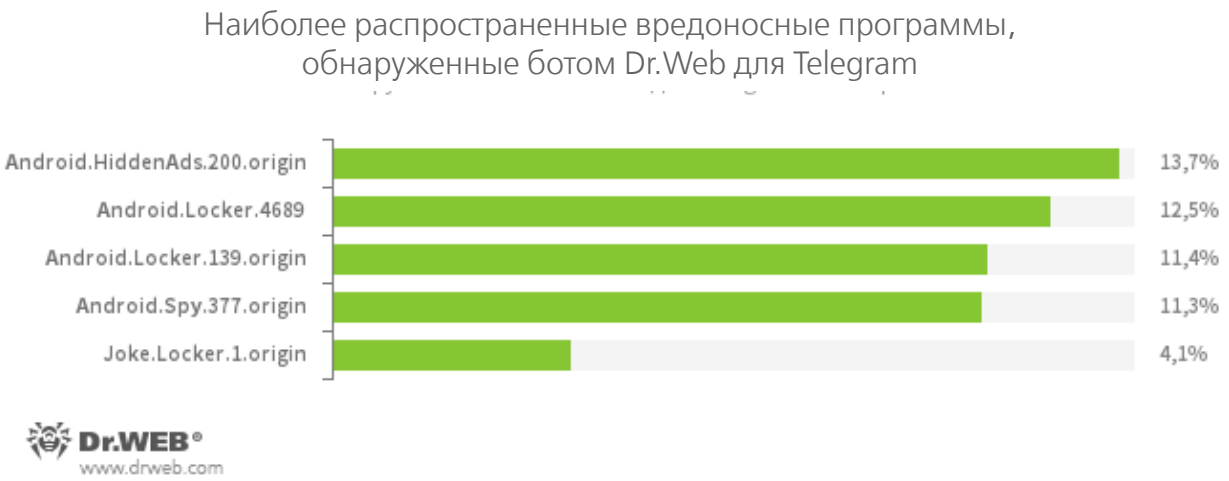
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в ноябре 2017 года



- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **PowerShell.DownLoader**
  Семейство вредоносных файлов, написанных на языке сценариев PowerShell. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Inject**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.

Обзор вирусной активности в ноябре 2017 года

По данным бота Dr.Web для Telegram



- **Android.HiddenAds.200.origin**
  Троянец, предназначенный для показа навязчивой рекламы. Распространяется под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают его в системный каталог.
- **Android.Locker**
  Семейство Android-троянцев, предназначенных для вымогательства. Они показывают навязчивое сообщение якобы о нарушении закона и о последовавшей в связи с этим блокировке мобильного устройства, для снятия которой пользователю предлагается заплатить определенную сумму.
- **Android.Spy.337.origin**
  Представитель семейства троянцев для ОС Android, способных похищать конфиденциальную информацию, в том числе пользовательские пароли.
- **Joke.Locker.1.origin**
  Программа-шутка для ОС Android, блокирующая экран мобильного устройства и выводящая на него изображение «синего экрана смерти» ОС Windows (BSOD, Blue Screen of Death).

Шифровальщики

Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»

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

- **Trojan.Encoder.3953** — 17,88% обращений;
- **Trojan.Encoder.858** — 8,39% обращений;
- **Trojan.Encoder.11539** — 6,39% обращений;
- **Trojan.Encoder.567** — 5,66% обращений;
- **Trojan.Encoder.3976** — 2,37% обращений;
- **Trojan.Encoder.761** — 2,37% обращений.

Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows
Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении

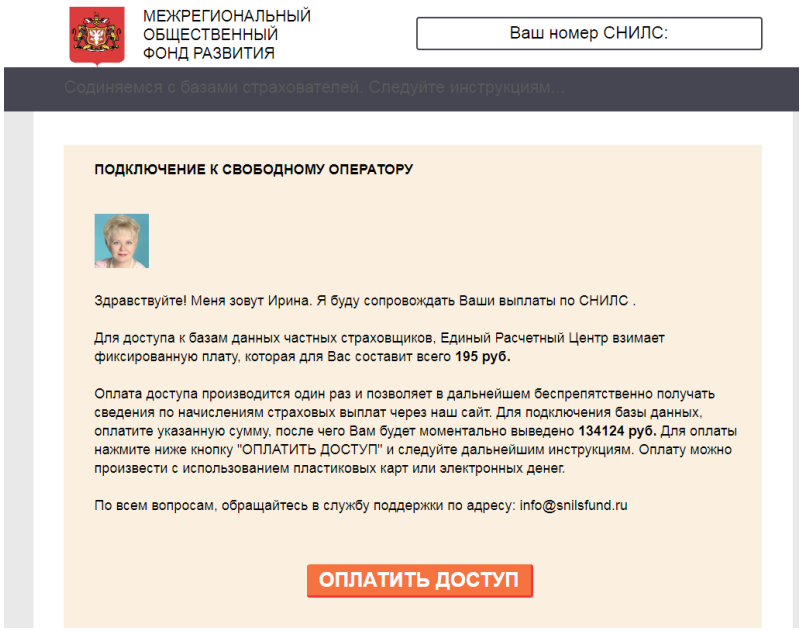
Dr.Web Rescue Pack

Опасные сайты

В течение ноября 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 331 895 интернет-адресов.

октябрь 2017	ноябрь 2017	Динамика
+256 429	+331 895	+29.4%

В ноябре компания «Доктор Веб» рассказала о новом виде мошенничества, получившем распространение в российском сегменте Интернета. Злоумышленники рассылали спам со ссылкой на сайт, якобы принадлежащий некоему «Межрегиональному общественному фонду развития». Ссылаясь на несуществующее постановление Правительства РФ, мошенники предлагали посетителям проверить якобы причитающиеся им выплаты от различных страховых компаний по номеру пенсионного страхового свидетельства (СНИЛС) или паспорта. Независимо от того, какие данные введет жертва (это может быть даже произвольная последовательность цифр), она получит сообщение о том, что ей положены страховые выплаты на достаточно крупную сумму, — несколько сотен тысяч рублей, однако для вывода этих «накоплений» жулики требовали оплатить денежный взнос.



Нерекомендуемые сайты

Обзор вирусной активности в ноябре 2017 года

Вредоносные программы для ОС Linux

В конце последнего осеннего месяца вирусные аналитики «Доктор Веб» исследовали новый бэкдор для Linux, получивший название Linux.BackDoor.Hook.1. Троянец может скачивать заданные в поступившей от злоумышленников команде файлы, запускать приложения или подключаться к определенному удаленному узлу. О других особенностях этой вредоносной программы мы рассказали в посвященном Linux.BackDoor.Hook.1 новостном материале.

Вредоносное и нежелательное ПО для мобильных устройств

В ноябре вирусные аналитики «Доктор Веб» выявили в каталоге Google Play троянца Android.RemoteCode.106.origin, скачивающего дополнительные вредоносные модули. Они загружали веб-сайты и нажимали на расположенные на них рекламные ссылки и баннеры. Кроме того, в каталоге были обнаружены вредоносные программы семейства Android.SmsSend, которые отправляли дорогостоящие СМС. Также в прошедшем месяце в Google Play распространялся троянец Android.CoinMine.3, использовавший зараженные смартфоны и планшеты для добычи криптовалюты Monero. Помимо этого в официальном каталоге Android-приложений было найдено большое число банковских троянцев семейства Android.Banker, предназначенных для кражи конфиденциальных данных и хищения денег со счетов владельцев Android-устройств.

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

- обнаружение множества троянцев в каталоге Google Play.

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

Обзор вирусной активности в ноябре 2017 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 | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах