Dr.WEB®
с 1992 года

Обзор вирусной активности в июле 2018 года

Обзор вирусной активности в июле 2018 года

31 июля 2018 года

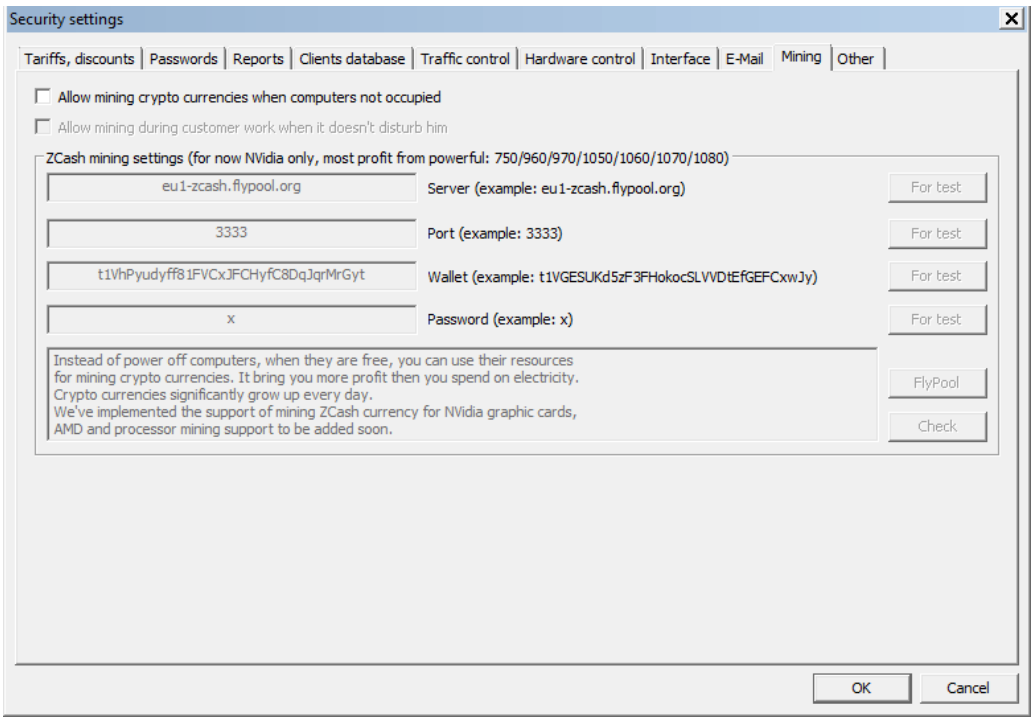
В начале июля вирусные аналитики «Доктор Веб» проанализировали нового троянца-майнера, который использовал необычную схему распространения. Также в течение месяца проявляли активность спамеры, рекламировавшие мошеннические сайты. Кроме того, в июле вирусные базы Dr.Web пополнились новыми записями для вредоносных программ, ориентированных на мобильную платформу Android.

Главные тенденции июля

- Обнаружение опасного троянца-майнера
- Распространение мошеннических почтовых рассылок
- Появление новых троянцев для Android

Угроза месяца

Специалисты по информационной безопасности уже сталкивались с распространением вредоносных программ при помощи механизма обновления приложений. Именно так попали к пользователям троянец-шифровальщик Trojan.Encoder.12544 (Petya, Petya.A, ExPetya и WannaCry-2) и бэкдор BackDoor.Dande. В июле в службу технической поддержки «Доктор Веб» обратился пользователь, на компьютере которого регулярно появлялось приложение для майнинга криптовалют, всякий раз удаляемое антивирусом. Проведенное аналитиками расследование показало, что виновником инцидента стала программа «Компьютерный зал» для автоматизации компьютерных клубов и интернет-кафе.



Механизм обновления этой программы автоматически скачивал из Интернета и устанавливал в систему троянца-майнера Trojan.BtcMine.2869. На 9 июля специалисты «Доктор Веб» обнаружили 2700 зараженных этим троянцем компьютеров. Более подробная информация об этом инциденте изложена в опубликованной на нашем сайте статье.

Обзор вирусной активности в июле 2018 года

По данным серверов статистики «Доктор Веб»

JS.BtcMine

Семейство сценариев на языке JavaScript, предназначенных для скрытой добычи (майнинга) криптовалют.

JS.Inject

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

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.

Статистика вредоносных программ в почтовом трафике

JS.Inject

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

JS.BtcMine

Семейство сценариев на языке JavaScript, предназначенных для скрытой добычи (майнинга) криптовалют.

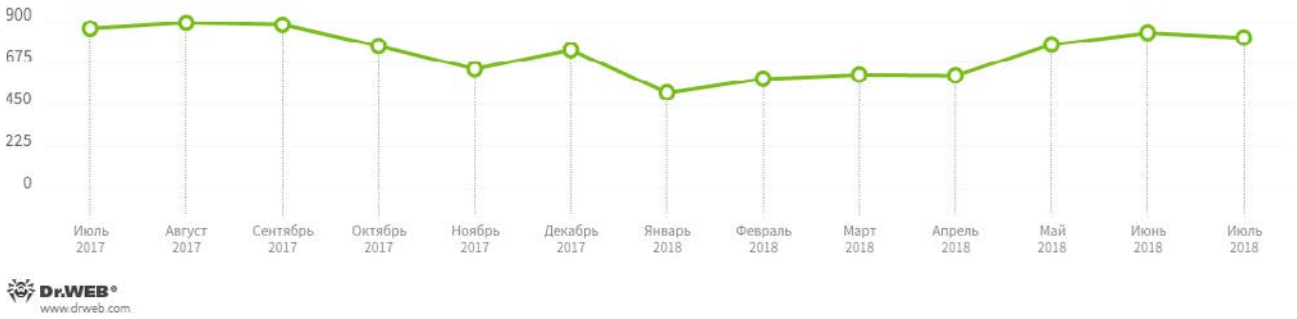
Trojan.PWS.Stealer

Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Trojan.Inject

Семейство троянцев, встраивающих вредоносный код в процессы других программ.

Шифровальщики



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

- Trojan.Encoder.858 — 17.69% обращений;
- **Trojan.Encoder.25574** — 11.38% обращений;
- Trojan.Encoder.11464 — 8.06% обращений;
- Trojan.Encoder.567 — 5.08% обращений;
- Trojan.Encoder.5342 — 3.85% обращений;
- Trojan.Encoder.24249 — 3.33% обращений.

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

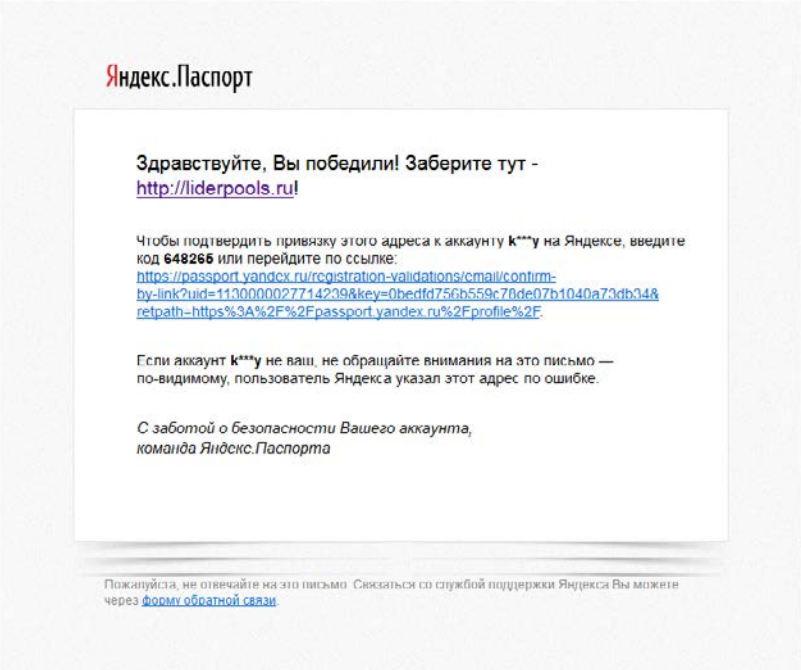
Настрой-ка Dr.Web от шифровальщиков

Обучающий курс

О бесплатном восстановлении Dr.Web Rescue Pack

Опасные сайты

В июле специалисты «Доктор Веб» зафиксировали несколько массовых почтовых рассылок с рекламой различных мошеннических ресурсов. В частности, спамеры отправляли сообщения якобы от имени компании «Яндекс» с предложением подтвердить привязку почтового адреса к аккаунту на портале passport.yandex.ru. При этом ссылка, по которой мошенники предлагали перейти получателю письма, действительно вела на портал «Яндекс». А вот другая ссылка, якобы анонсировавшая получение некоего приза, приводила потенциальную жертву на сайт сетевых мошенников, требовавших оплатить за обещанный подарок небольшой денежный взнос.


Яндекс.Паспорт

Здравствуйте, Вы победили! Заберите тут - http://liderpools.ru!

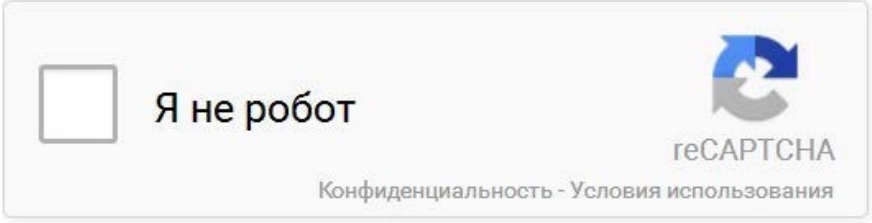
Чтобы подтвердить привязку этого адреса к аккаунту k***y на Яндексе, введите код **648265** или перейдите по ссылке: https://passport.yandex.ru/registration-validations/email/confirm-by-link?uid=1130000027714239&key=0bedfd756b559c76de07b1040a73db34&retpath=https%3A%2F%2Fpassport.yandex.ru%2Fprofile%2F.

Если аккаунт k***y не ваш, не обращайте внимания на это письмо — по-видимому, пользователь Яндекса указал этот адрес по ошибке.

С заботой о безопасности Вашего аккаунта,
команда Яндекс.Паспорта

Пожалуйста, не отвечайте на это письмо. Связаться со службой поддержки Яндекса Вы можете через форму обратной связи.

В ряде других мошеннических сообщений встречались ссылки на страницы публичных сервисов, подобных Google Docs, где злоумышленники размещали веб-страницу с картинкой, имитирующей стандартную панель автоматической защиты от роботов reCAPCHA. Щелчок мышью по этой картинке перенаправлял пользователей на различные фишинговые сайты.



Опасные сайты

Адреса всех выявленных аналитиками «Доктор Веб» мошеннических ресурсов были добавлены в базы нерекомендуемых сайтов Родительского и Офисного контроля Dr.Web.

В течение июля 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 512 763 интернет-адреса.

Июнь 2018	Июль 2018	Динамика
+ 395 477	+ 512 763	+ 29.6%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В уходящем месяце в каталоге Google Play было обнаружено несколько опасных вредоносных программ. Одной из них стал троянец Android.Banker.2746, который показывал поддельное окно ввода персональных данных при запуске банковских приложений. Другой троянец, получивший имя Android.DownLoader.753.origin, скачивал Android-банкеров с сервера злоумышленников, чтобы избежать обнаружения основной вредоносной программы в Google Play. Среди распространявшихся в июле троянцев были и другие банкеры. Один из них – Android.BankBot.279.origin. Он загружался на мобильные устройства при посещении мошеннических сайтов. Также в июле злоумышленники вновь распространяли вредоносное приложение-бэкдор, известное вирусным аналитикам «Доктор Веб» с апреля 2017 года. Оно шпионило за пользователями и распространяло червя, который заражал компьютеры под управлением ОС Windows. Кроме того, в уходящем месяце специалисты «Доктор Веб» обнаружили и исследовали несколько новых программ, предназначенных для кибершпионажа. Они получили имена Program.Shadspy.1.origin и Program.AppSpy.1.origin.

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

- обнаружение троянцев в каталоге Google Play;
- распространение Android-банкеров;
- распространение Android-бэкдора, которого злоумышленники использовали для заражения компьютеров под управлением Windows;
- выявление новых коммерческих программ-шпионов

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

Обзор вирусной активности в июле 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 странах