Dr.WEB®
с 1992 года

Обзор вирусной активности в июне 2018 года

Обзор вирусной активности в июне 2018 года

3 июля 2018 года

Первый летний месяц оказался относительно спокойным с точки зрения информационной безопасности. Во второй половине июня вирусные аналитики «Доктор Веб» зафиксировали почтовую рассылку, с использованием которой сетевые мошенники пытались обмануть пользователей Интернета. Также в течение месяца были выявлены новые вредоносные программы для мобильной платформы Android.

Главные тенденции июля

- Мошеннические почтовые рассылки
- Распространение вредоносных программ для Android

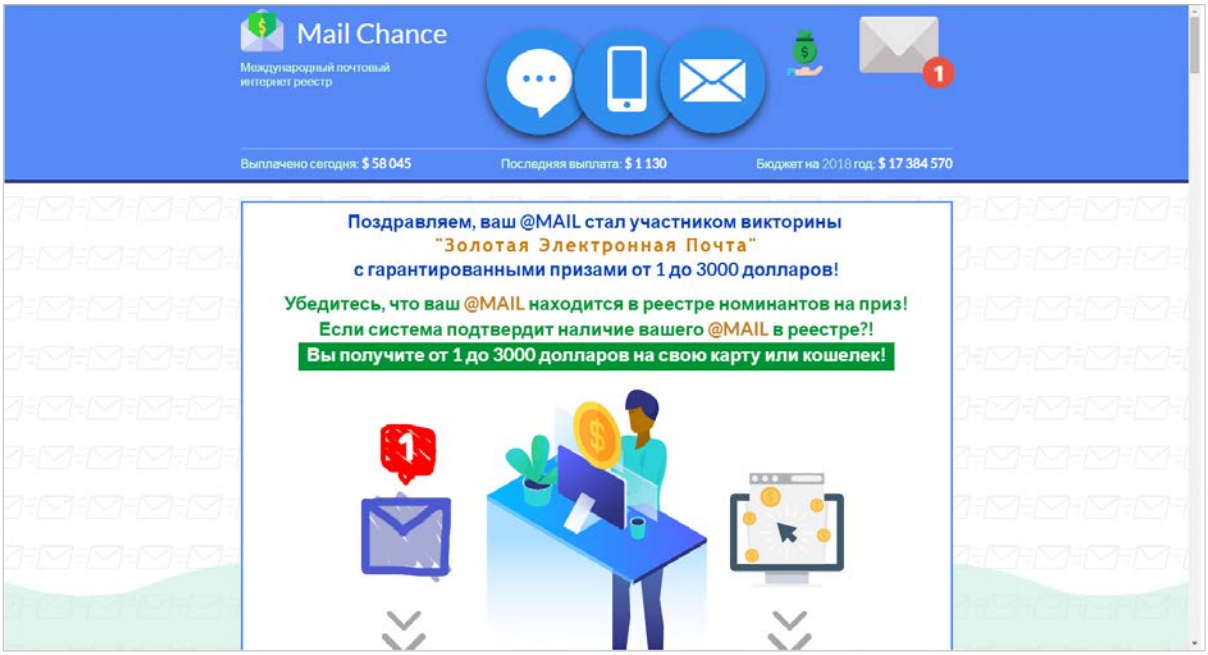
Угроза месяца

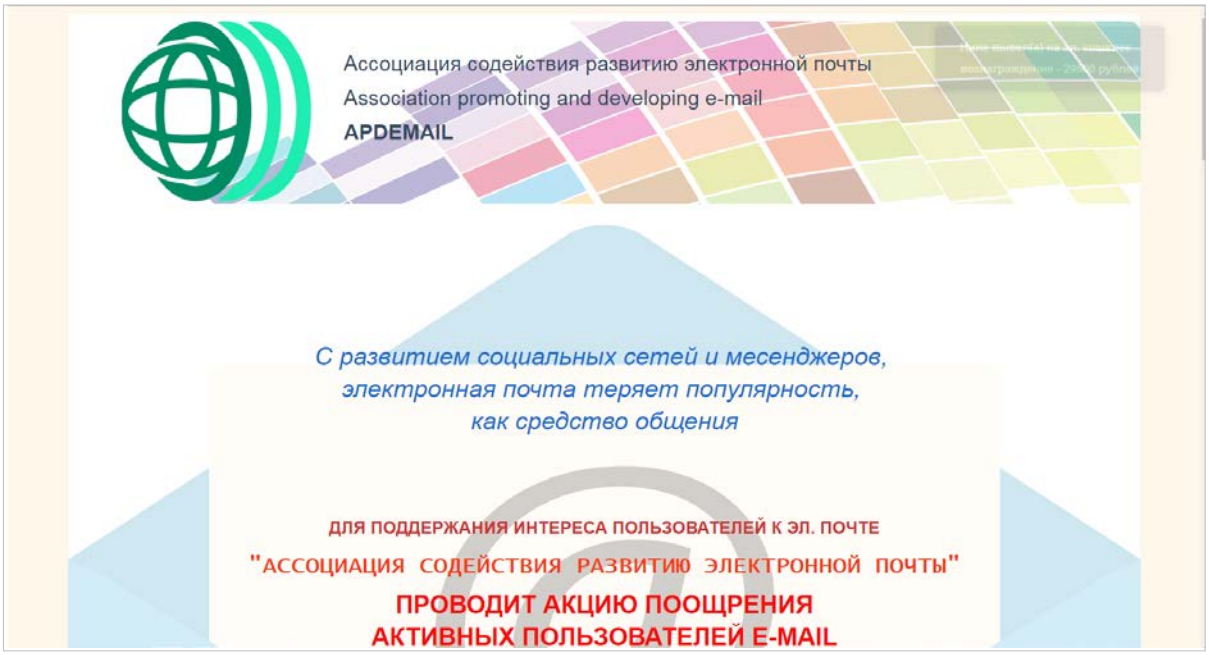
Во второй половине июня было зафиксировано несколько массовых почтовых рассылок, с использованием которых злоумышленники завлекали потенциальных жертв на мошеннические сайты. Помимо электронной почты киберпреступники активно использовали для рассылки спама формы обратной связи, размещенные на различных интернет-ресурсах, при этом их не останавливало даже наличие «капчи». Сообщения содержали стандартный текст о получении пользователем некой транзакции или денежного перевода. Вот несколько примеров подобных сообщений: «Здравствуйте, мы отправили платеж в размере $33,50 USD Код счета на оплату: 2478347616. Уведомляем, что на вашем балансе достаточно средств для автоматического продления», «Текущий баланс лицевого счёта равен 13 300 R. Информируем вас о зачислении оплаты по счёту № 97724 на сумму – 1 017 рублей», «Уведомляем вас о зачислении оплаты по счёту на сумму – 0 031 rub. Текущий баланс лицевого счёта равен 37 561 rub», «Детали Вашего заказа: Увеличение баланса - 2 шт. - 379. 03 $. Благодарим Вас за использование безопасной системы онлайн заказов». Примечательно, что все ссылки в подобных письмах вели на бесплатный сервис Google Docs, где злоумышленники заранее разместили PDF-документ с предложением забрать некий денежный приз.циального сайта steamcommunity.com вредоносная программа подменяет отображение игровых предметов на компьютере жертвы с помощью перехвата и модификации трафика. В результате пользователю будет казаться, что он приобретает некий дорогостоящий инвентарь, в то время как в действительности в его игровой учетной записи появится совсем другой, гораздо более дешевый предмет.

Угроза месяца

Нажав на ссылку в этом PDF-документе, потенциальная жертва попадала на один из мошеннических сайтов, предлагавших получить некий выигрыш или вознаграждение.

Угроза месяца





Угроза месяца

Дальнейшая схема жульничества довольно-таки проста, она используется сетевыми мошенниками уже очень давно: чтобы получить предлагаемый приз, посетителю сайта требуется перевести киберпреступникам небольшую сумму, после чего никакого вознаграждения жертва, разумеется, не получает. Адреса всех выявленных аналитиками «Доктор Веб» мошеннических интернет-ресурсов были добавлены в базы нерекомендуемых сайтов Родительского и Офисного контроля.

Обзор вирусной активности в июне 2018 года

По данным серверов статистики «Доктор Веб»

JS.BtcMine.36

Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.

Trojan.DownLoader

Семейство 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.Starter.7394

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

Trojan.Dimnie.5

Троянец-шпион, способный красть с зараженного устройства конфиденциальную информацию и предоставлять несанкционированный доступ к инфицированному компьютеру. Также имеет в своем составе банковский модуль.

Статистика вредоносных программ в почтовом трафике

Trojan.DownLoader

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

Trojan.Dimnie.5

Троянец-шпион, способный красть с зараженного устройства конфиденциальную информацию и предоставлять несанкционированный доступ к инфицированному компьютеру. Также имеет в своем составе банковский модуль.

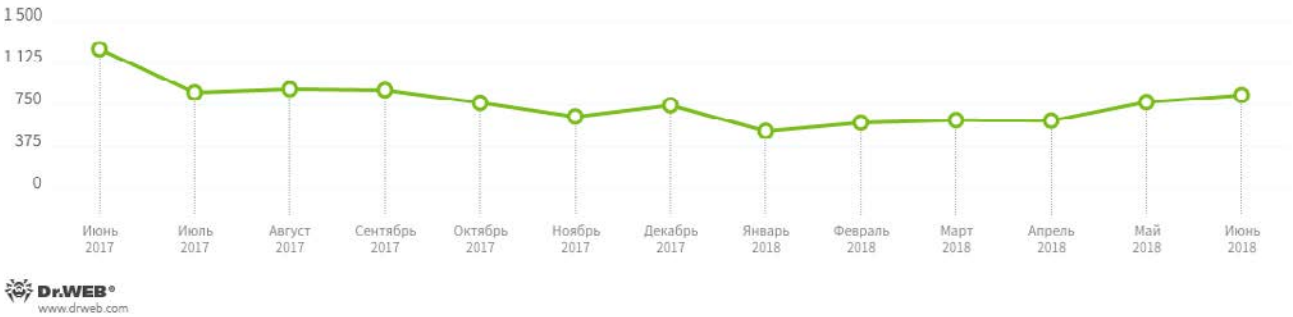
JS.BtcMine.36

Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.

Trojan.PWS.Stealer

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

Шифровальщики



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

- Trojan.Encoder.858 — 15,47% обращений;
- Trojan.Encoder.25574 — 12,31% обращений;
- Trojan.Encoder.11464 — 8,32% обращений;
- Trojan.Encoder.13671 — 5,99% обращений;
- Trojan.Encoder.24249 — 4,33% обращений;
- Trojan.Encoder.10700 — 2,32% 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 июня 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 395 477 интернет-адресов.

Май 2018	Июнь 2018	Динамика
+ 1 388 093	+ 395 477	71.5%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В прошедшем месяце вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play большое число программ со встроенным нежелательным рекламным модулем **Adware.Appalytic.1.origin**. Этот модуль показывал надоедливые уведомления, предлагая загрузить различное ПО, а также самостоятельно открывал в Play Маркет страницы рекламируемых приложений. Позднее наши специалисты выявили в Google Play несколько новых троянцев семейства Android.FakeApp, которые по команде злоумышленников загружали всевозможные веб-сайты. Также в июне преступники распространяли троянца Android.Spy.461.origin, которого вирусописатели использовали для кибершпионажа. Кроме того, среди угрожавших владельцам Android-смартфонов и планшетов вредоносных программ был СМС-троянец Android.SmsSend.1989.origin, подписывавший пользователей на платные услуги.

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

- выявление в Google Play новых Android-троянцев;
- распространение троянца-шпиона.

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

Обзор вирусной активности в июне 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