Dr.WEB®
с 1992 года

Обзор вирусной активности в августе 2018 года

Обзор вирусной активности в августе 2018 года

31 августа 2018 года

В августе специалисты «Доктор Веб» зафиксировали распространение троянцев-майнеров, предназначенных для добычи криптовалют без ведома пользователей. Подобные программы были предназначены как для устройств под управлением Windows, так и для Linux-устройств. В течение последнего летнего месяца киберпреступники рассылали мошеннические письма администраторам освобождающихся доменов в надежде обманным путем завладеть их деньгами. Кроме того, в августе вирусные базы Dr.Web пополнились новыми записями для Android-троянцев.

Главные тенденции августа

- Распространение троянцев-майнеров для Windows и Linux
- Мошеннические почтовые рассылки
- Обнаружение новых вредоносных программ для Android

Угроза месяца

Вредоносную программу, добавленную в вирусные базы под именем Linux.BtcMine.82, злоумышленники начали использовать еще в июне. Этот троянец написан на языке Go и представляет собой дроппер, в теле которого хранится упакованный майнер. Дроппер сохраняет его на диск и запускает, после чего майнер приступает к добыче криптовалюты Monero (XMR). На принадлежащем злоумышленникам сервере аналитики «Доктор Веб» обнаружили еще несколько майнеров для ОС Windows.

Все выявленные аналитиками вредоносные программы были добавлены в вирусные базы Dr.Web. Более подробную информацию об этом инциденте можно получить из новостного материала, опубликованного на нашем сайте.

По данным серверов статистики «Доктор Веб»

JS.BtcMine

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

Trojan.Encoder.11432

Червь-шифровальщик, также известный под именем WannaCry.

Trojan.BtcMine

Семейство вредоносных программ, которые втайне от пользователя применяют вычислительные ресурсы зараженного компьютера для добычи (майнинга) различных криптовалют, например Bitcoin.

Win32.HLLW.Shadow

Червь, использующий для своего распространения съемные носители и сетевые диски.

Статистика вредоносных программ в почтовом трафике

SMB. Способен загружать с управляющего сервера и запускать исполняемые файлы.

Trojan.PWS.Stealer

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

Trojan.Encoder.567, **Trojan.Encoder.25843**

Энкодеры, шифрующие файлы на компьютере и требующие у жертвы выкуп за расшифровку.

JS.BtcMine

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

Trojan.Inject

Шифровальщики

Семейство троянцев, встраивающих вредоносный код в процессы других программ.

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

- Trojan.Encoder.858 — 20,00% обращений;
- Trojan.Encoder.11464 — 14,23% обращений;
- Trojan.Encoder.25574 — 9,24% обращений;
- Trojan.Encoder.567 — 3,46% обращений;
- Trojan.Encoder.24249 — 3,45% обращений;
- Trojan.Encoder.10700 — 2,50% обращений.

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

Настрой-ка Dr.Web от шифровальщиков

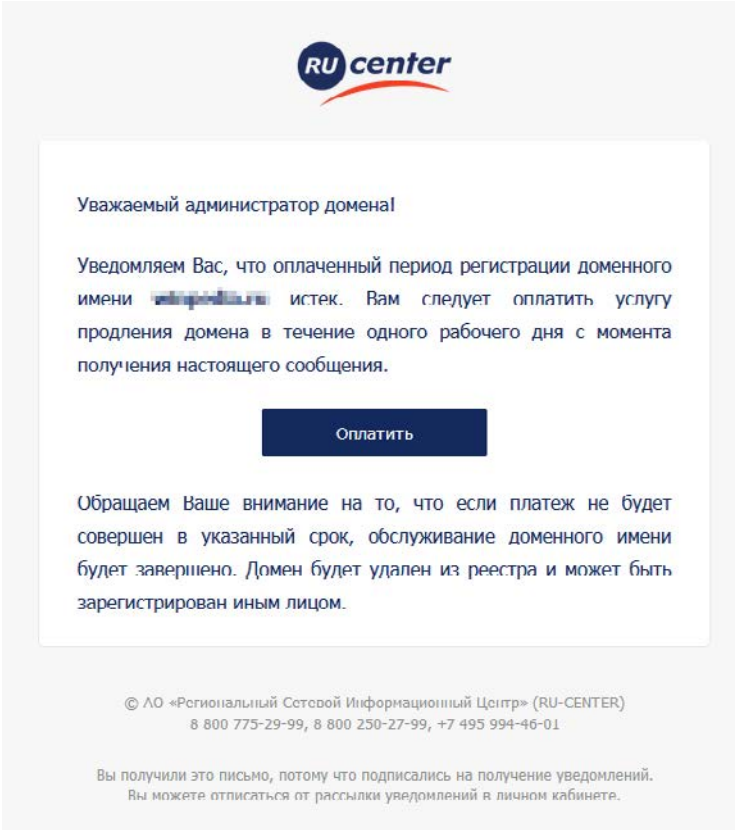
Обучающий курс

О бесплатном восстановлении

Dr.Web Rescue Pack

Опасные сайты

В августе активизировались кибермошенники, целью которых на этот раз стали администраторы освобождающихся доменов, ранее пользовавшиеся услугами регистратора «Региональный Сетевой Информационный Центр» (RU-CENTER). В середине месяца они стали получать по электронной почте сообщения якобы от имени этой компании. В письмах содержалось напоминание об окончании оплаченного периода регистрации доменного имени. Злоумышленники утверждали, что администратор должен оплатить услугу продления домена в течение одного рабочего дня с момента получения письма, иначе этот домен будет исключен из реестра.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.


RU center

Уважаемый администратор домена!

Уведомляем Вас, что оплаченный период регистрации доменного имени [redacted] истек. Вам следует оплатить услугу продления домена в течение одного рабочего дня с момента получения настоящего сообщения.

Оплатить

Обращаем Ваше внимание на то, что если платеж не будет совершен в указанный срок, обслуживание доменного имени будет завершено. Домен будет удален из реестра и может быть зарегистрирован иным лицом.

© АО «Региональный Сетевой Информационный Центр» (RU-CENTER)
8 800 775-29-99, 8 800 250-27-99, +7 495 994-46-01

Вы получили это письмо, потому что подписались на получение уведомлений.
Вы можете отписаться от рассылки уведомлений в личном кабинете.

Опасные сайты

Ссылка в письме вела на взломанный веб-сайт, адрес которого был добавлен в базы нерекомендуемых интернет-ресурсов Офисного и Родительского контроля. Установленный там сценарий перенаправлял получателя письма на страницу платежной системы Яндекс.Деньги, позволяющую перевести денежные средства на электронный кошелек мошенников. Подробнее об этой рассылке мы рассказали в опубликованной на нашем сайте статье.

Также в августе многие пользователи Интернета получали электронные письма, в которых сетевые жулики сообщали получателю его пароль, ранее использованный при регистрации на одном из сайтов, либо комбинацию логина и пароля. Авторы сообщения утверждали, что они якобы разместили вирус на одном из порносайтов, и при его посещении включили камеру устройства, с помощью которой записали видеоролик с участием получателя письма. Чтобы избежать рассылки этого ролика по списку адресов, будто бы скопированному из адресной книги потенциальной жертвы, ей предлагалось заплатить выкуп в биткойнах, эквивалентный нескольким тысячам долларов США.

Разумеется, подобные сообщения являются пустой угрозой: по всей видимости, в руки злоумышленников попала база данных зарегистрированных пользователей, похищенная с одного или нескольких интернет-ресурсов. Чтобы не попадаться в руки мошенников, специалисты «Доктор Веб» рекомендуют чаще менять пароли и не использовать одинаковые учетные данные для регистрации на разных сайтах.

Опасные сайты

В течение августа 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 538 480 интернет-адресов.

Июль 2018	Август 2018	Динамика
+ 512 763	+ 538 480	+5%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В августе 2018 года вирусные аналитики компании «Доктор Веб» обнаружили трояна-клиппера Android.Clipper.1.origin, подменяющего номера электронных кошельков в буфере обмена зараженных Android-устройств. Помимо этого, в каталоге Google Play было выявлено множество различных вредоносных программ. Среди них – банковские троянцы Android.Banker.2843 и Android.Banker.2855, распространявшиеся под видом безобидных приложений. Кроме того, киберпреступники пытались заразить мобильные устройства пользователей при помощи троянцев-загрузчиков Android.DownLoader.768.origin, Android.DownLoader.772.origin и Android.DownLoader.784.origin, которые скачивали на смартфоны и планшеты различные вредоносные приложения. Также в течение уходящего месяца специалисты компании «Доктор Веб» обнаружили в Google Play большое число троянцев семейства Android.Click. Злоумышленники использовали их в мошеннических целях и зарабатывали с их помощью деньги. Еще один троянец, созданный для мошенничества, получил имя Android.FakeApp.110. Он также распространялся через каталог Google Play. Среди выявленных в августе вредоносных программ оказался опасный троянец-шпион Android.Spy.490.origin, которого вирусописатели могли встраивать в любые приложения и распространять их под видом оригиналов.

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

- обнаружение трояна-клиппера, способного подменять номера электронных кошельков в буфере обмена Android-устройств;
- обнаружение множества вредоносных программ в каталоге Google Play;
- распространение банковских троянцев;
- выявление опасного трояна-шпиона.

Обзор вирусной активности в августе 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

Узнайте больше
Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека