Dr.WEB®
с 1992 года

Обзор вирусной активности в октябре 2018 года

31 октября 2018 года

В октябре компания «Доктор Веб» обнародовала результаты расследования деятельности одного из сетевых мошенников. Жертвами киберпреступника стали более 10 000 человек, которые потеряли в общей сложности не менее $24 000.

В течение месяца злоумышленники продолжали рассылать письма, в которых вымогали у пользователей деньги под угрозой компрометации их персональных данных. По всей видимости, в руки злоумышленников попало несколько баз данных с регистрационной информацией, содержащий адреса электронной почты и пароли. По этим адресам вымогатели и рассылали сообщения о том, что им известен пароль жертвы, и на их компьютерах якобы установлена вредоносная программа. Чтобы личная жизнь получателя не стала достоянием общественности, киберпреступники требовали выкуп в криптовалюте биткойн, эквивалентный сумме от 500 до 850 долларов США.

Жулики активно используют несколько биткойн-кошельков, и, судя по информации на сайте blockchain.com, несколько жертв уже купилось на угрозы мошенников.

Транзакции	
Число транзакций	30
Всего получено	3.223797 BTC
Итоговый баланс	3.223797 BTC

Транзакции	
Число транзакций	14
Всего получено	1.12686229 BTC
Итоговый баланс	1.12686229 BTC

Транзакции	
Число транзакций	5
Всего получено	0.37598285 BTC
Итоговый баланс	0.37598285 BTC

Обзор вирусной активности в октябре 2018 года

В последнее время этот способ вымогательства крайне популярен среди киберпреступников: они массово рассылают письма с различными угрозами, но с ограниченным количеством сочетаний адреса электронной почты и пароля. Разумеется, никаких вирусов и троянцев для добычи этих сведений вымогатели не использовали, а чтобы обезопасить себя от подобных посягательств, пользователям достаточно всего лишь сменить используемые пароли.

Главные тенденции октября

- Разоблачение деятельности опасного сетевого мошенника
- Массовая рассылка спама пользователям Интернета со стороны вымогателей

Угроза месяца

Специалисты компании «Доктор Веб» провели масштабное расследование, результатами которого поделились с читателями в уходящем октябре. Предметом внимания вирусных аналитиков стала деятельность киберпреступника, скрывающегося под псевдонимами Investimer, Hyipblock и Mmpower. Для достижения своих целей он использовал широчайший набор вредоносных программ, включающий различные стилеры, загрузчики, бэкдоры и троянца-майнера со встренным модулем для подмены содержимого буфера обмена.

Специализировался Investimer на мошенничестве в сфере криптовалют. Ассортимент применяемых им способов подпольного заработка весьма велик: он создавал поддельные сайты криптовалютных бирж, ферм для майнинга, партнерских программ по выплате вознаграждений за просмотр рекламы и онлайн-лотерей.

Угроза месяца

В целом используемая киберпреступником схема обмана такова. Потенциальную жертву различными методами заманивают на мошеннический сайт, для использования которого требуется скачать некую программу-клиент. Под видом этого клиента жертва загружает троянца, который по команде злоумышленника устанавливает на компьютер другие вредоносные программы. Такие программы (в основном троянцы-стилеры) похищают с зараженного устройства конфиденциальную информацию, с помощью которой жулик затем крадет с их счетов криптовалюту и деньги, хранящиеся в различных платежных системах.

Аналитики «Доктор Веб» полагают, что общее количество пользователей, пострадавших от противоправной деятельности Investimer'а, превышает 10 000 человек. Ущерб, нанесенный злоумышленником своим жертвам, наши специалисты оценивают в более чем 23 000 долларов США. К этому следует добавить более 182 000 в криптовалюте Dogecoin, что по нынешнему курсу составляет еще порядка 900 долларов. Более подробная информация об этом расследовании представлена в опубликованной на нашем сайте статье.

Обзор вирусной активности в октябре 2018 года

По данным серверов статистики «Доктор Веб»

JS.BtcMine

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

Trojan.SpyBot.699

Троянец-шпион, предназначенный для перехвата нажатий клавиш на зараженном устройстве, выполнения поступающих команд и кражи конфиденциальной информации.

Trojan.Starter.7394

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

Trojan.Encoder.11432

Червь-шифровальщик, также известный под именем WannaCry.

Статистика вредоносных программ в почтовом трафике

JS.BtcMine

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

W97M.DownLoader

Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Trojan.Encoder.26375

Представитель семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.

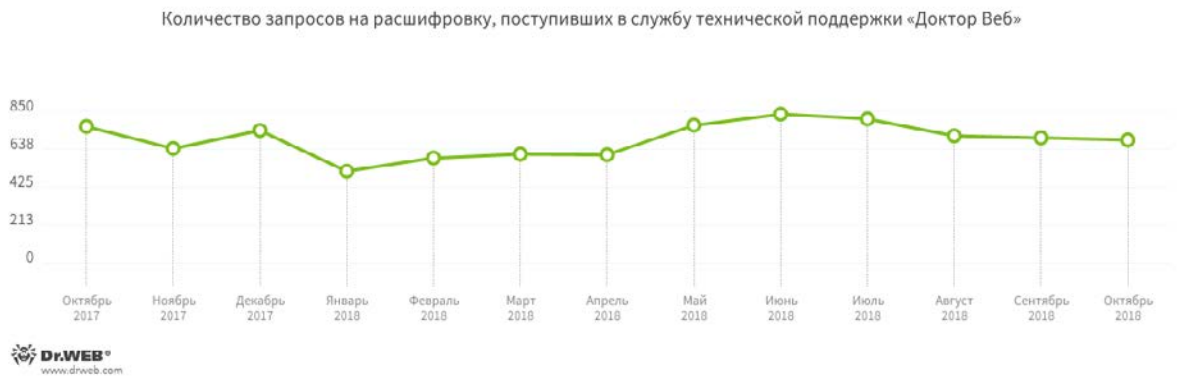
Trojan.PWS.Stealer

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

Trojan.SpyBot.699

Троянец-шпион, предназначенный для перехвата нажатий клавиш на зараженном устройстве, выполнения поступающих команд и кражи конфиденциальной информации.

Шифровальщики



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

- Trojan.Encoder.858 — 20,04% обращений;
- Trojan.Encoder.11464 — 11.67% обращений;
- Trojan.Encoder.567 — 6.23% обращений;
- **Trojan.Encoder. 25574** — 5.84% обращений;
- **Trojan.Encoder.1539** — 4.86% обращений;
- Trojan.Encoder.5342 — 1.75% 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 октября 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 156 188 интернет-адресов.

Сентябрь 2018	Октябрь 2018	Динамика
+ 271 605	+ 156 188	- 42.49%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В начале октября в вирусные базы Dr.Web была добавлена запись для детектирования Android-банкера **Android.BankBot.1781**. Он способен скачивать и запускать вспомогательные модули, а также компилировать и выполнять получаемый от злоумышленников код, написанный на C#. Позже специалисты «Доктор Веб» выявили в официальном каталоге приложений для ОС Android несколько троянцев. Среди них были вредоносные программы **Android.FakeApp.125** и **Android.Click.245.origin**, которые загружали и демонстрировали мошеннические веб-сайты.

В конце месяца в Google Play были найдены троянцы-загрузчики **Android.DownLoader.818.origin** и **Android.DownLoader.819.origin**. Они скачивали на мобильные устройства и пытались установить других Android-троянцев. Также вирусные аналитики исследовали вредоносные приложения **Android.RemoteCode.192.origin** и **Android.RemoteCode.193.origin**, распространявшиеся под видом безобидного ПО. Троянцы показывали рекламу, могли загружать вспомогательные модули и открывать заданные злоумышленниками видео, размещенные на портале YouTube. Тем самым они «накручивали» счетчик просмотров и повышали популярность видеороликов.

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

- выявление в Google Play вредоносных приложений;
- распространение опасного банковского троянца, способного компилировать и выполнять вредоносный код «на лету».

Обзор вирусной активности в октябре 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