Dr.WEB®
с 1992 года

Обзор вирусной активности в ноябре 2018 года

Обзор вирусной активности в ноябре 2018 года

30 ноября 2018 года

Последний осенний месяц 2018 года был отмечен сразу несколькими интересными событиями в сфере информационной безопасности. В ноябре специалисты «Доктор Веб» исследовали троянца-майнера для Linux, способного удалять работающие на зараженном устройстве антивирусные программы. Вскоре был обнаружен троянец-кликер для ОС Windows, который отличается любопытным способом проникновения на компьютеры потенциальных жертв. Не снижается интерес вирусописателей и к мобильной платформе Android – в ноябре были обнаружены и добавлены в вирусные базы Dr.Web новые вредоносные программы для этой ОС.

Главные тенденции ноября

- Распространение троянца-кликера для ОС Windows
- Появление Linux-майнера, способного удалять антивирусы
- Обнаружение новых вредоносных программ для ОС Android

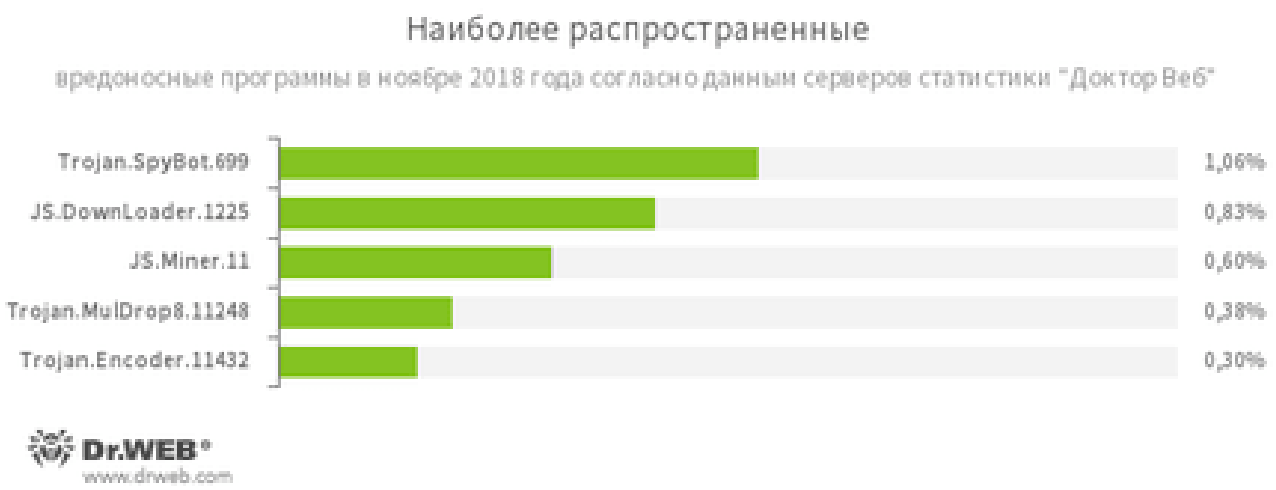
Угроза месяца

Троянец, добавленный в вирусные базы Dr.Web под именем Trojan.Click3.27430, представляет собой вредоносную программу, предназначенную для накрутки посещаемости различных веб-сайтов. Распространяется он под видом приложения DynDNS, позволяющего привязать субдомен к компьютеру, не имеющему статического IP-адреса. Для распространения троянца злоумышленники создали специальный веб-сайт.

С этого сайта загружается архив, содержащий исполняемый файл setup.exe, который на самом деле представляет собой загрузчик. Он, в свою очередь, скачивает из Интернета другой файл, маскирующийся под ARJ-архив. На самом деле файл представляет собой дроппер, который устанавливает в систему троянца и настоящее приложение DynDNS. Если впоследствии пользователь решит деинсталлировать его с зараженного компьютера, будет удалена только сама программа DynDNS, а Trojan.Click3.27430 по-прежнему останется в системе и продолжит свою вредоносную деятельность. Более подробная информация об этом троянце и принципах его работы изложена в опубликованной на нашем сайте статье.

Обзор вирусной активности в ноябре 2018 года

По данным серверов статистики «Доктор Веб»



Trojan.SpyBot.699

Многомодульный банковский троянец. Он позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и выполнять поступающие от них команды. Троянец предназначен для хищения средств с банковских счетов.

JS.DownLoader

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

JS.Miner

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

Trojan.MulDrop

Представитель семейства троянцев, предназначенных для установки на инфицированный компьютер других вредоносных программ.

Trojan.Encoder.11432

Червь-шифровальщик, также известный под именем WannaCry.

Статистика вредоносных программ в почтовом трафике

JS.DownLoader

Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.

Trojan.SpyBot.699

Многомодульный банковский троянец. Он позволяет киберпреступникам загружать и запускать на зараженном устройстве различные приложения и выполнять поступающие от них команды. Троянец предназначен для хищения средств с банковских счетов.

JS.Miner

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.

Шифровальщики

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

- Trojan.Encoder.858 — 32.15% обращений;
- Trojan.Encoder.11464 — 11.17% обращений;
- Trojan.Encoder.11539 — 10.80% обращений;
- **Trojan.Encoder.25574** — 4.91% обращений;
- Trojan.Encoder.567 — 1.35% обращений;
- Trojan.Encoder.10700 — 1.35% обращений.

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

Настрой-ка Dr.Web от шифровальщиков

Обучающий курс

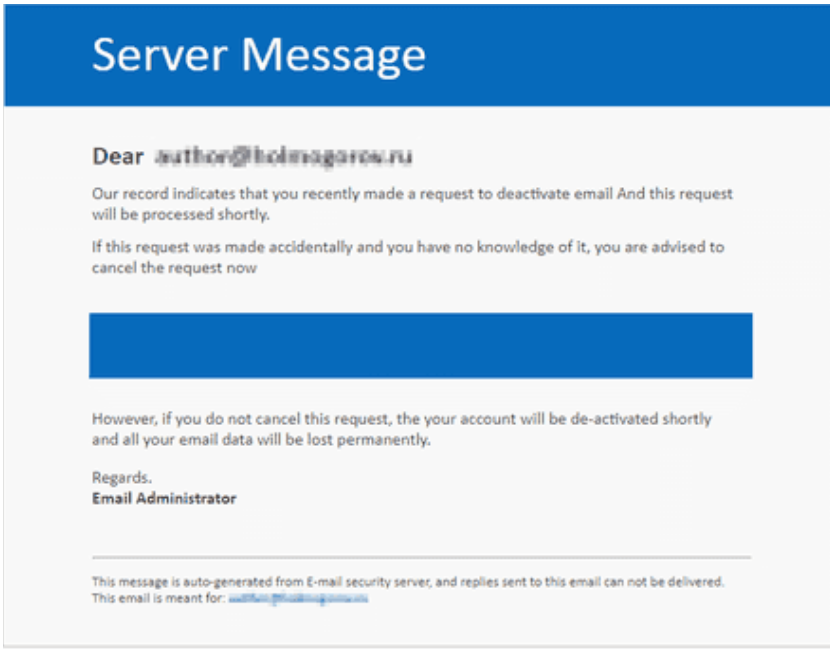
О бесплатном восстановлении

Dr.Web Rescue Pack

Опасные сайты

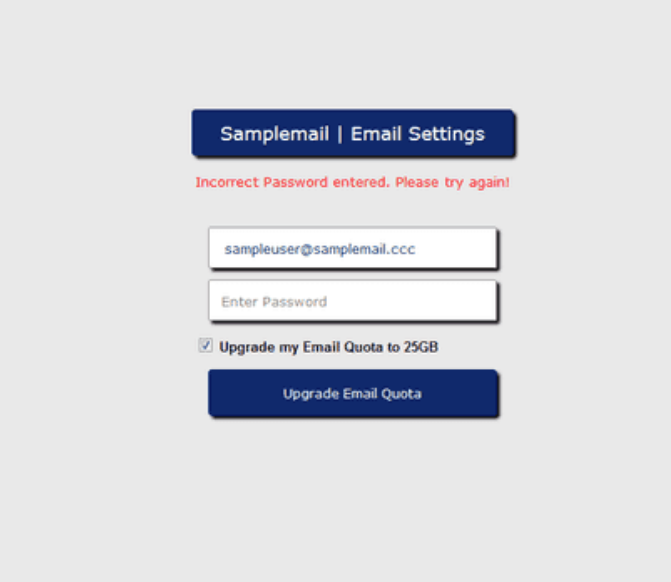
Среди прочих опасных и нерекомендуемых сайтов отдельную категорию составляют фишинговые интернет-ресурсы. Фишинг — это разновидность сетевого мошенничества, конечной целью которого является хищение у жертвы конфиденциальной информации – например, логинов и паролей от различных интернет-сервисов и учетных данных для авторизации в социальных сетях. Для этого злоумышленники создают поддельные сайты, имитирующие оформление настоящих интернет-ресурсов, и всевозможными методами завлекают туда пользователей. Впоследствии киберпреступники могут использовать полученную информацию для рассылки рекламных сообщений, в целях мошенничества или шантажа.

В ноябре специалисты «Доктор Веб» зафиксировали несколько случаев подобных мошеннических рассылок. Киберпресупники отправляли пользователям письма якобы от имени администраторов их почтового сервиса. В послании сообщалось, что от пользователя поступил запрос на деактивацию его почтового ящика, и, чтобы отменить его, нужно перейти по предложенной в письме ссылке.



Ссылка вела на фишинговый сайт, содержащий форму для ввода логина и пароля от электронного почтового ящика потенциальной жертвы. Какие бы данные ни ввел посетитель

мошеннической страницы, ему демонстрировалось сообщение об ошибке, в то время как указанная им информация незамедлительно передавалась злоумышленникам. Специалисты «Доктор Веб» выявили несколько таких фишинговых сайтов, их адреса были добавлены в базы нерекомендуемых интернет-ресурсов SpIDer Gate.



В течение ноября 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 231 074 интернет-адреса.

В течение октября 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 156 188 интернет-адресов.

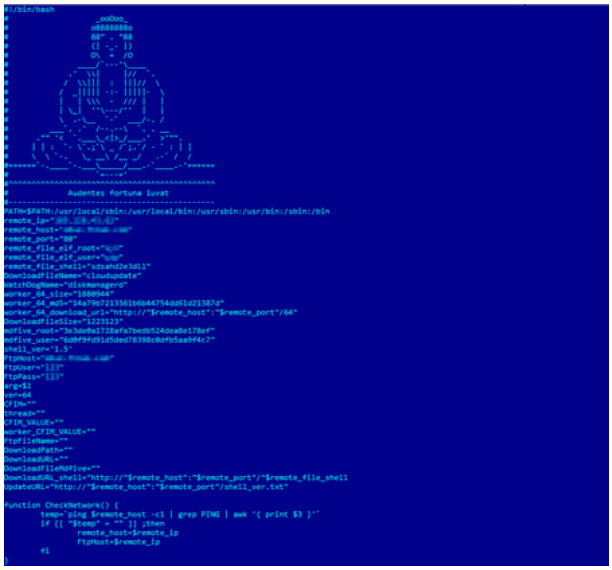
Октябрь 2018	Ноябрь 2018	Динамика
+ 156 188	+ 231 074	+ 47.94%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносные программы для ОС Linux

Linux.BtcMine.174 — далеко не первый из известных аналитикам «Доктор Веб» троянцев для Linux, использующих ресурсы зараженного компьютера для добычи криптовалют. Эта вредоносная программа интересна своей способностью искать и удалять установленные на инфицированном устройстве антивирусы.

Троянец представляет собой сценарий, написанный на языке командной оболочки sh и содержащий более 1000 строк кода. Он состоит из нескольких компонентов, которые скачивает с принадлежащего злоумышленникам сервера. После успешной установки на устройство вредоносный сценарий скачивает из Интернета одну из версий троянца Linux.BackDoor.Gates.9, предназначенного для организации DDoS-атак и способного выполнять поступающие от злоумышленников команды.



Установившись в системе, Linux.BtcMine.174 ищет конкурирующие майнеры и при обнаружении завершает их процессы. Если Linux.BtcMine.174 не был запущен от имени суперпользователя (root), для повышения своих привилегий он использует набор эксплойтов. Затем вредоносная программа пытается отыскать работающие сервисы антивирусных программ, завершить их, а потом с помощью пакетных менеджеров удаляет их файлы и директорию, в которой был установлен антивирусный продукт. Помимо этого троянец скачивает и запускает на инфицированном устройстве руткит, собирает информацию о сетевых узлах, к которым ранее подключались по протоколу ssh, и пробует заразить их. Более подробные сведения об этой вредоносной программе изложены в опубликованной на нашем сайте обзорной статье.

Другие события в сфере информационной безопасности

Согласно статистике, собранной серверами «Доктор Веб» на зараженных компьютерах и в почтовом трафике, одной из наиболее распространенных в ноябре вредоносных программ является Trojan.SpyBot.699. Она распространяется хакерской группировкой «RTM» и представляет собой многомодульного банковского троянца.

Вредоносные функции Trojan.SpyBot.699 сосредоточены в динамической библиотеке с внутренним именем core.dll, которую он загружает в память устройства. Троянец регистрирует себя в автозагрузке Windows, все передаваемые на управляющий сервер данные вредоносная программа шифрует.

По команде злоумышленников Trojan.SpyBot.699 может загружать, сохранять на диск и запускать исполняемые файлы, скачивать и запускать программы без сохранения, загружать в память динамические библиотеки, самообновляться, устанавливать цифровые сертификаты в системное хранилище и выполнять иные поступающие извне команды.

Эта вредоносная программа умеет искать банковские клиенты среди запущенных процессов, в именах открытых окон и среди хранящихся на дисках файлов. Также троянец ищет информацию о системах «банк-клиент» в файлах cookies браузеров. Получив нужные сведения, злоумышленники с помощью Trojan.SpyBot.699 и загружаемых им модулей могут детально исследовать атакуемую систему, обеспечить постоянное присутствие в ней других троянцев, внедрять вредоносное ПО в бухгалтерские программы и программы «банк-клиент». Конечной целью киберпреступников является хищение денег с банковских счетов жертвы. Антивирусные продукты Dr.Web успешно детектируют и удаляют Trojan.SpyBot.699 и известные на сегодняшний день вредоносные модули, которые злоумышленники используют совместно с этим троянцем.

Вредоносное и нежелательное ПО для мобильных устройств

В уходящем ноябре вирусные аналитики «Доктор Веб» выявили троянца Android.Banker.2876, который распространялся через каталог Google Play. Злоумышленники использовали его для кражи конфиденциальных данных клиентов нескольких европейских банков. Кроме того, в Google Play были найдены прочие угрозы. Среди них – загрузчик Android.DownLoader.832.origin. Он скачивал и пытался установить другие вредоносные программы. Также наши специалисты обнаружили троянцев семейства Android.FakeApp, которых кибермошенники использовали для незаконного заработка. Кроме того, были выявлены приложения со встроенными рекламными модулями Adware.HiddenAds.

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

- распространение вредоносных и нежелательных приложений в Google Play.

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

Обзор вирусной активности в ноябре 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