Dr.WEB®
с 1992 года

Обзор вирусной активности в июне 2019 года

Обзор вирусной активности в июне 2019 года

3 июля 2019 года

В июне статистика серверов Dr.Web зарегистрировала значительное повышение числа общих и уникальных угроз по сравнению с маем. Рекламные программы и установщики все еще лидируют по общему количеству обнаруженных угроз, а наибольшая активность вредоносного ПО замечена в почтовом трафике. Возобновил активность опасный стилер — Trojan.PWS.Maria.3 (Ave Maria), использованный ранее в атаке на нефтегазовую компанию, а также через рассылки распространяется Trojan.Nanocore.23 — троянец с удаленным доступом, позволяющий контролировать зараженный компьютер. Кроме того, в июне прошла вирусная кампания с использованием шифровальщика Trojan.Encoder.858.

Главные тенденции мая

- Повышение активности распространения вредоносного ПО
- Рассылка стилеров и RAT-троянцев через почту
- Рост активности шифровальщиков

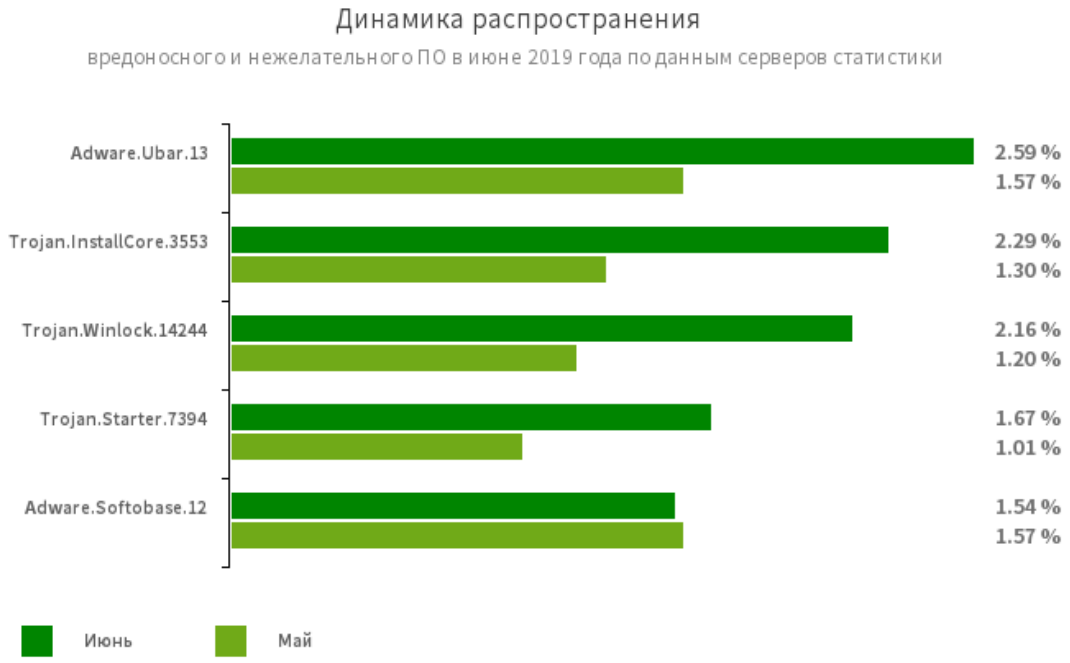
Угроза месяца

В июне в вирусной лаборатории «Доктор Веб» был изучен образец редкого Node.js-троянца — Trojan.MonsterInstall. Запустившись на устройстве жертвы, он загружает и устанавливает необходимые для своей работы модули, собирает информацию о системе и отправляет ее на сервер разработчика. После получения ответа от сервера он устанавливается в автозагрузку и начинает добычу (майнинг) криптовалюты TurtleCoin. Разработчики этого вредоносного ПО используют для распространения собственные ресурсы с читами к популярным играм, а также заражают файлы на других подобных сайтах.

Подробнее об угрозе

Обзор вирусной активности в июне 2019 года

По данным серверов статистики «Доктор Веб»



Угрозы этого месяца:

Adware.Ubar.13

Торрент-клиент, устанавливающий нежелательное ПО на устройство.

Trojan.InstallCore.3553

Еще один известный установщик рекламного ПО. Показывает рекламу и устанавливает дополнительные программы без согласия пользователя.

Trojan.Winlock.14244

Блокирует или ограничивает доступ пользователя к операционной системе и её основным функциям. Для разблокировки системы требует перечислить деньги на счет разработчиков троянца.

Trojan.Starter.7394

Троянец, предназначенный для запуска другого вредоносного ПО на устройстве.

Adware.Softobase.12

Программа-установщик, распространяющая устаревшее программное обеспечение. Меняет настройки браузера.

Статистика вредоносных программ в почтовом трафике

Exploit.Rtf.CVE2012-0158

Измененный документ Microsoft Office Word, использующий уязвимость CVE2012-0158 для выполнения вредоносного кода.

W97M.DownLoader.2938

Семейство троянцев-загрузчиков, использующих в работе уязвимости документов Microsoft Office. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Exploit.ShellCode.69

Вредоносный документ Microsoft Office Word. Использует уязвимость CVE-2017-11882.

Растущие угрозы месяца:

Trojan.PWS.Maria.3

Стилер, распространяющийся по почте через вредоносные файлы Excel. Использует популярную уязвимость CVE-2017-11882 для запуска исполняемого файла. Впервые был замечен в фишинговой кампании, нацеленной на предприятия нефтегазовой промышленности Италии.

Trojan.Nanocore.23

Опасный троянец с удаленным доступом. Он позволяет хакерам контролировать зараженный компьютер, в том числе включить камеру и микрофон на устройстве, если они доступны.

Шифровальщики

- Trojan.Encoder.858 — 30,31%
- Trojan.Encoder.567 — 7,02%
- Trojan.Encoder.11464 — 6,47%
- Trojan.Encoder.11539 — 3,33%
- Trojan.Encoder.18000 — 3,14%
- Trojan.Encoder.28004 — 2,59%
- Trojan.Encoder.25574 — 1,66%

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 июне 2019 года в базу нерекомендуемых и вредоносных сайтов было добавлено 223 952 интернет-адреса.

Май 2019	Июнь 2019	Динамика
+ 223 952	+ 151 162	– 32,5%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

В июне вирусные аналитики «Доктор Веб» вновь обнаружили в Google Play множество вредоносных и нежелательных программ. Среди них были рекламные троянцы Android.HiddenAds, которые показывали баннеры поверх окон других приложений и интерфейса операционной системы, а также мошеннические программы Android.FakeApp. Последние загружали веб-сайты, где потенциальным жертвам за вознаграждение предлагалось принять участие в онлайн-опросах. Для получения денег пользователи якобы должны были оплатить некую комиссию или проверочный сбор. Однако если они соглашались, то никакого вознаграждения не получали. Другой представитель этого семейства, получивший имя Android.FakeApp.174, загружал веб-сайты, на которых пользователей подписывали на надоедливые и мошеннические уведомления.

В течение месяца были найдены новые троянцы-загрузчики, такие как Android.DownLoader.3200 и Android.DownLoader.681.origin. Они скачивали на Android-устройства другие вредоносные приложения. Кроме того, специалисты «Доктор Веб» проанализировали новый рекламный модуль Adware.OneOceans.2.origin, который разработчики ПО встраивают в программы и игры.

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

- обнаружение новых вредоносных программ в Google Play.

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

Обзор вирусной активности в июне 2019 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