Dr.WEB®
с 1992 года

Обзор вирусной активности в мае 2018 года

Обзор вирусной активности в мае 2018 года

31 мая 2018 года

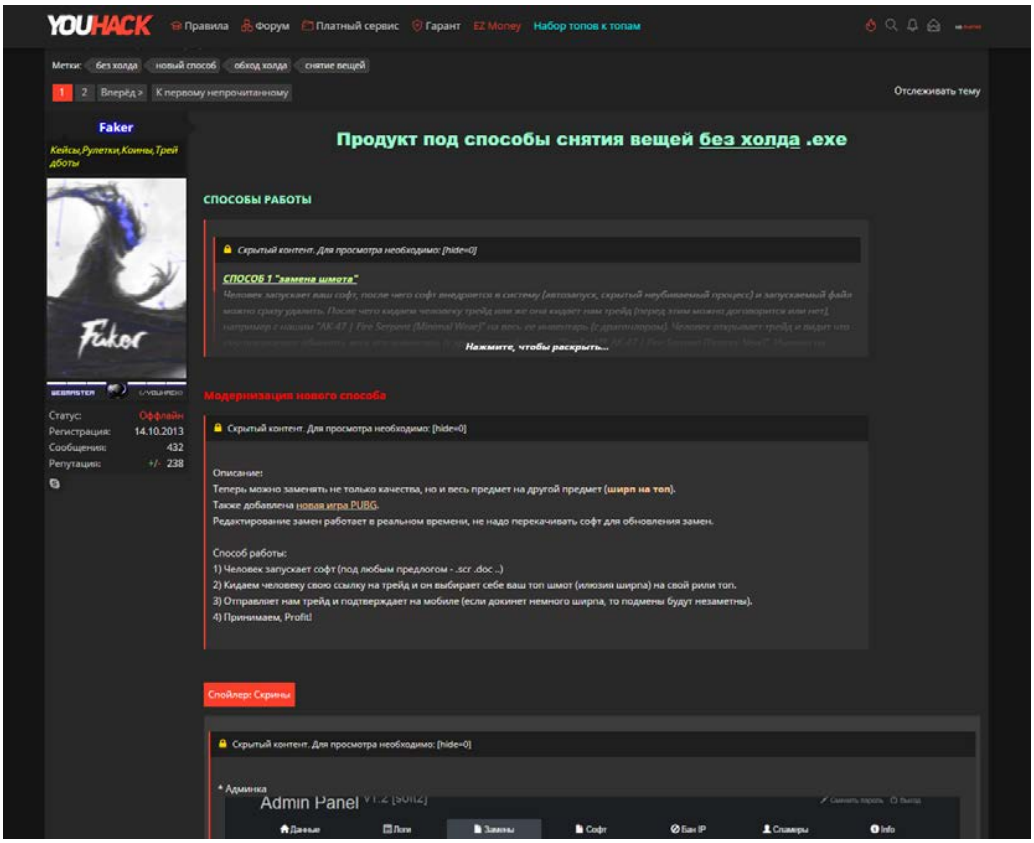
В мае компания «Доктор Веб» завершила исследование нескольких троянцев, угрожавших пользователям популярной игровой платформы Steam. Они похищали данные учетных записей поклонников компьютерных игр, а также подменяли игровые предметы при совершении сделок обмена. Также в течение последнего месяца весны было выявлено множество мошеннических сайтов, адреса которых пополнили базы нерекомендуемых интернет-ресурсов. Среди них нередко встречались веб-страницы, активно эксплуатирующие тематику грядущего Чемпионата мира по футболу 2018 года. В начале мая вирусные аналитики исследовали несколько троянцев-стилеров, кравших с зараженных устройств конфиденциальную информацию.

Главные тенденции мая

- Распространение троянцев, угрожающих пользователям Steam
- Обнаружение множества мошеннических сайтов
- Появление троянцев-шпионов, ворующих приватную информацию

Угроза месяца

Создатель вредоносных программ, добавленных в вирусную базу Dr.Web под наименованиями Trojan.PWS.Steam.13604 и Trojan.PWS.Steam.15278, разработал специальную схему для их распространения. От злоумышленников, пожелавших освоить незаконный заработок, не требуется ничего, кроме денег и, в некоторых случаях, домена: вирусописатель предоставляет им самого троянца, доступ к административной панели и техническую поддержку.



Угроза месяца

Заразив компьютер, Trojan.PWS.Steam.13604 отображает поддельное окно авторизации Steam. Если жертва вводит в него свои логин и пароль, троянец пытается авторизоваться с их помощью в сервисе Steam. Если эта попытка увенчалась успехом и на компьютере включен Steam Guard — система двухфакторной аутентификации для защиты учетной записи пользователя, — троянец выводит на экран поддельное окно для ввода кода авторизации. Вся эта информация отсылается на сервер злоумышленников.

Другая вредоносная программа того же автора, Trojan.PWS.Steam.15278, нацелена на хищение инвентаря в Steam. Для этого на многих обменных площадках троянец подменяет получателя игровых предметов с помощью веб-инжектов, в результате чего артефакты достаются злоумышленникам. А при обмене инвентаря с использованием официального 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.

Более подробную информацию о методах распространения этих троянцев и принципах их работы рассказано в опубликованной на нашем сайте статье.

Обзор вирусной активности в мае 2018 года

По данным серверов статистики «Доктор Веб»

JS.BtcMine.36

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

JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.

Trojan.PWS.Stealer

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

Trojan.MulDrop8.25070

Троянец-дроппер, устанавливающий в систему другие вредоносные программы.

Win32.HLLW.Shadow

Червь, использующий для своего распространения съемные носители и сетевые диски. Кроме того, может распространяться по сети с использованием стандартного протокола SMB. Способен загружать с управляющего сервера исполняемые файлы и запускать их.

Статистика вредоносных программ в почтовом трафике

Trojan.Dimnie.14

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

JS.DownLoader

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

JS.Inject

Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.

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.

Шифровальщики

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

- Trojan.Encoder.11464 — 15.90% обращений;
- Trojan.Encoder.858 — 11.33% обращений;
- Trojan.Encoder.24249 — 6.16% обращений;
- Trojan.Encoder.10700 — 3.78% обращений;
- Trojan.Encoder.13671 — 3.70% обращений;
- Trojan.Encoder.4592 — 2.39% 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

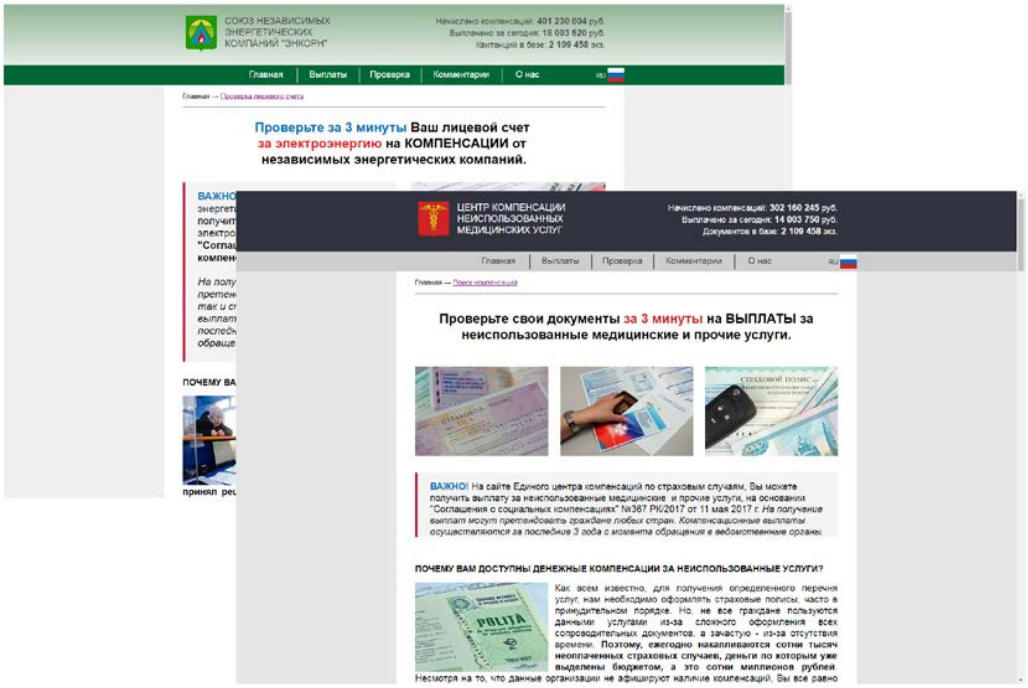
С приближением Чемпионата мира по футболу активизировались многочисленные сетевые мошенники, которые начали использовать чрезвычайно актуальную тематику мундиаля. Чтобы привлечь посетителей, жулики размещают на своих веб-страницах официальную символику Чемпионата. Они предлагают всем желающим принять участие в розыгрышах призов, якобы организованных FIFA, крупными банками и международными инвестиционными фондами.

В качестве призов мошенники обещают дорогие автомобили, значительные денежные суммы, туристические путевки на зарубежные курорты, и, конечно, же, бесплатные билеты на футбольный чемпионат. Схема, которую используют киберпреступники, в целом

Опасные сайты

не нова: потенциальной жертве сообщают о крупном выигрыше, для получения которого необходимо перевести на их счет несколько сотен рублей. Несложно догадаться, что, расставшись с деньгами, никакого приза жертва мошенников не получит. В мае 2018 года специалисты «Доктор Веб» добавили в базы Родительского и Офисного контроля несколько десятков адресов подобных ресурсов, однако похожие по тематике и оформлению сайты продолжают появляться с завидной регулярностью.

В мае участились случаи распространения ссылок на мошеннические сайты с использованием СМС и сообщений в программах-мессенджерах. Жулики предлагают потенциальным жертвам получить якобы полагающуюся им компенсацию за переплату предоставляемых населению коммунальных, медицинских услуг, либо услуг обязательного страхования.



Для «проверки» возможности получить компенсацию посетителю сайта предлагается ввести в специальную форму последние цифры какого-либо документа, а также свое имя и фамилию. Какие бы данные ни указал пользователь, на сайте появляется сообщение о возможности получить выплату, для чего мошенники просят перевести им не-

Опасные сайты

большую денежную сумму. Более подробно об этой популярной схеме обмана интернет-пользователей мы рассказали в нашей статье.

В течение мая 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 1 388 093 интернет-адреса.

В течение марта 2018 года в базу нерекомендуемых и вредоносных сайтов было добавлено 624 474 интернет-адреса.

Апрель 2018	Май 2018	Динамика
+ 287 661	+ 1 388 093	+ 382.5%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Другие события в сфере информационной безопасности

В мае вирусные аналитики «Доктор Веб» исследовали несколько новых модификаций троянцев, похищавших конфиденциальную информацию. Один из них, получивший наименование Trojan.PWS.Stealer.23370, сканирует диски инфицированного устройства в поисках сохраненных паролей и файлов cookies браузеров, основанных на Chromium. Кроме того, этот троянец ворует информацию из мессенджера Telegram, FTP-клиента FileZilla, а также копирует файлы изображений и офисных документов по заранее заданному списку. Полученные данные троянец упаковывает в архив и сохраняет его на Яндекс.Диск.

Другая модификация этого троянца-шпиона получила наименование Trojan.PWS.Stealer.23700. Она крадет пароли и файлы cookies из браузеров Google Chrome, Opera, Яндекс.Браузер, Vivaldi, Kometa, Orbitum, Comodo, Amigo и Torch. Помимо этого, троянец копирует файлы ssfn из подпапки config приложения Steam, а также данные, необходимые для доступа к учетной записи Telegram. Кроме того, шпион создает копии изображений и документов, хранящихся на Рабочем столе Windows. Всю украденную информацию он упаковывает в архив и загружает в облачное хранилище pCloud.

Третья модификация стилера получила наименование Trojan.PWS.Stealer.23732. Этот троянец состоит из нескольких компонентов. Один из них представляет собой шпионский модуль, как и его предшественники, написанный на языке Python и преобразованный в исполняемый файл. Он ворует конфиденциальную информацию. Все остальные компоненты троянца написаны на языке Go. Один из них сканирует диски в поисках папок, в которых установлены браузеры, а еще один упаковывает похищенные данные в архивы и загружает их в хранилище pCloud.

Более подробно о методах распространения этих вредоносных программ мы рассказали в опубликованной на нашем сайте статье.

Вредоносное и нежелательное ПО для мобильных устройств

В мае было выявлено немало новых вредоносных и потенциально опасных программ для мобильных устройств, многие из которых распространялись через официальный каталог программ для ОС Android. В начале месяца вирусные аналитики компании «Доктор Веб» обнаружили в Google Play троянца Android.Click.248.origin, загружавший мошеннические веб-страницы, на которых пользователей подписывали на дорогостоящие услуги. Позднее там же наши специалисты зафиксировали троянца Android.FakeApp. Он переходил по ссылкам, которые получал от вирусописателей, и загружал веб-страницы, искусственно увеличивая их посещаемость. Кроме того, в Google Play распространялись вредоносные программы семейства Android.HiddenAds, предназначенные для показа рекламы. Среди обнаруженных в мае троянцев были также и шпионы Android.Spy.456.origin и Android.Spy.457.origin, применявшиеся для слежки за пользователями. А в конце месяца вирусные аналитики «Доктор Веб» добавили в вирусную базу запись для детектирования коммерческой программы-шпиона Program.Onespy.3.origin.

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

- выявление в Google Play новых Android-троянцев;
- обнаружение новой версии потенциально опасной шпионской программы для ОС Android.

Обзор вирусной активности для мобильных устройств в мае 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

© ООО «Доктор Веб»,
2003-2018