РОСКОМНАДЗОР ВЫЯВИЛ 1,5 ТЫС. НАРУШЕНИЙ В РАБОТЕ ОБЩЕСТВЕННЫХ ТОЧЕК WI-FI

С начала 2017 г. Роскомнадзор провёл проверку 17,4 тыс. точек доступа к Wi-Fi в общественных местах. По итогам проверок надзорная служба выявила 1,5 тыс. нарушений закона об обязательной идентификации пользователей, что в 3,5 раза меньше по сравнению с предыдущим годом. С начала года Роскомнадзор составил 216 протоколов об административных нарушениях в отношении операторов связи.

С целью предотвращения использования террористами общедоступных сетей Wi-Fi в 2014 г. были приняты Федеральный закон № 97-ФЗ и Постановления Правительства РФ № 758 и № 801 об идентификации пользователей. Закон обязывает владельцев бесплатных точек Wi-Fi идентифицировать пользователей по номеру телефона или паспортным данным.

В ноябре минувшего года специалисты «Лаборатории Касперского» опубликовали (**http://www.securitylab.ru/news/484558.php**) результаты исследования, посвящённого безопасности общественных точек доступа Wi-Fi в различных странах мира. Лидером по числу незащищённых точек доступа Wi-Fi стала Корея (47,9%). Наиболее безопасной с точки зрения защищённости точек доступа страной стала Германия (84,91% точек доступа защищены WPA/WPA2). В России шифрованием оказались защищены до 83% общественных точек доступа.

Подробнее: **http://www.securitylab.ru/news/489205.php**

РОСКОМНАДЗОР СТАЛ АКТИВНО БОРОТЬСЯ СО ШПИОНАЖЕМ

В последнее время надзорное ведомство массово блокирует интернет-ресурсы, продающие шпионское аппаратное и программное обеспечение. Большая их часть была внесена в «чёрный список» в конце октября 2017 г. По многим сайтам решения суда были приняты ещё в начале текущего года, однако по неизвестным причинам блокировка произошла только осенью.

Как сообщает «Роскомсвобода» (**https://roskomsvoboda.org/32926**), выяснить причины блокировки возможно далеко не всегда. На сайтах судов представлена общая информация, а решения по тому или иному делу публикуются редко. Тем не менее «Роскомсвободе» удалось ознакомиться с вердиктами в отношении сайтов spytown.ru и spyline.ru, вынесенными Пушкинским районным судом г. Санкт-Петербурга и Гурьевским районным судом Калининградской области соответственно.

В решении Пушкинского районного суда от 4 июля 2017 г. упоминаются ст. 23 Конституции РФ, гарантирующая неприкосновенность частной жизни, и ст. 137, 138 УК РФ, предусматривающие уголовную ответственность за её нарушение. Кроме того, в документе есть отсылка к федеральному закону «О противодействии терроризму».

Согласно решению суда по делу spytown.ru, на сайте продавалось оборудование для прослушки. Как сообщается, предоставляемая услуга «носит противоправный характер и даёт возможность получить преступным путём сведения, которые впоследствии могут быть использованы для совершения преступления».

Как сообщается в решении Гурьевского районного суда Калининградской области от 28 июня 2017 г., сайт spyline.ru нарушает неприкосновенность частной жизни и поэтому должен быть заблокирован.

Источник: **http://www.securitylab.ru/news/489284.php**

ЛАБОРАТОРИЯ КАСПЕРСКОГО ОПУБЛИКОВАЛА ОТЧЁТ О РАЗВИТИИ КИБЕРУГРОЗ В ТРЕТЬЕМ КВАРТАЛЕ 2017 Г.

В третьем квартале 2017 г. резко возросло количество пользователей, атакованных мобильным банковским трояном Asacub. В июле текущего года количество жертв трояна выросло почти втрое, составив около 29 тыс. Также исследователи обнаружили новую модификацию мобильного трояна Svpeng, способного считывать введённый пользователем текст, отправлять SMS-сообщения и препятствовать своему удалению.

В отчёте говорится и о расширении списка мобильных приложений, атакуемых банковским трояном FakeToken. Если раньше троян и его модификации перекрывали фишинговым окном в основном банковские приложения и некоторые приложения Google, например, Google Play Store, то теперь в сферу их интересов вошли приложения для вызова такси, заказа авиабилетов и бронирования номеров в гостиницах. Основная цель трояна – сбор данных банковской карты пользователя.

Помимо этого, наблюдается рост активности троянов, похищающих деньги пользователей посредством подписок.

Данные трояны могут посещать сайты, позволяющие оплачивать услуги средствами со счёта мобильного телефона пользователя. Вредоносное ПО может нажимать кнопки на данных сайтах, используя специальные JS-файлы, таким образом осуществляя оплату неких услуг втайне от пользователя.

Странами с самым большим процентом атакованных мобильных устройств в третьем квартале 2017 г. стали Иран (35,12%), Бангладеш (28,3%) и Китай (27,38%). Россия заняла 35-е место, на её долю пришлось 8,68% мобильных угроз. В то же время Россия заняла первое место по количеству атак банковскими трояна: на её долю пришлось 1,2%, на втором и третьем местах расположились Узбекистан (0,4%) и Казахстан (0,36%).

Эксперты отметили рост количества атак с использованием вредоносных документов. Выросло число комбинированных документов (в которых содержится и эксплоит, и фишинговое сообщение) на тот случай, если встроенный в документ эксплоит не сработал.

В отчёте также говорится о новой волне атак шифровальщика Crysis, которая пришлась на август текущего года.

В июле 2017 г. авторы вымогательского ПО Petya опубликовали свой мастер-ключ, с помощью которого возможна расшифровка ключей Salsa, необходимых для расшифровки базы данных MFT и разблокировки доступа к системам, пострадавшим в ходе атак вредоносного ПО Petya/Mischa и GoldenEye. Произошло это вскоре после эпидемии заражения вымогательским ПО ExPetr, которое использовало часть кода от GoldenEye. Данный ход навёл исследователей на мысль, что авторы Petya/Mischa/GoldenEye попытались таким образом дистанцироваться от ExPetr. Хотя количество атак росло на протяжении квартала, оно остаётся ниже показателей мая и июня, когда прогремели две массовые эпидемии – WannaCry и ExPetr.

По количеству заражений вымогательским ПО первое место занимает Мьянма (0,95%), второе – Вьетнам (0,92%) и третье – Индонезия (0,69%). Россия, занимавшая 10-е место во втором квартале, теперь находится уже на 6-й позиции (0,51%).

Более подробно с данными отчёта можно ознакомиться по ссылке: **https://goo.gl/1dKHyG**. Это крайне важно знать библиотекам и доносить эту информацию до их пользователей.