Автор:
03.03.14 14:57 -

Запрет для «Яндекс.Браузера».

Как сообщает издание «Известия» со ссылкой на депутата Госдумы Елену Мизулину, чиновница обратилась в Роскомнадзор с требованием провести экспертную проверку в отношении web-обозревателя от поисковой компании «Яндекс». Причиной тому послужило наличие в «Яндекс.Браузере» функционала, позволяющего просматривать внесенные в черный список web-сайты.

Эксперты: большинство бесплатных...

Эксперты: большинство бесплатных мобильных приложений представляют угрозу безопасности. Согласно последнему отчету аналитической компании Appthority - Winter 2014 App Reputation Report - мобильные приложения (особенно бесплатные) представляют угрозу безопаснсти пользователей. По данным аналитиков, 95% топ-200 бесплатных и 80% платных приложений для iOS и Android демонстрируют подозрительное поведение. Под «подозрительным поведением» в Appthority подразумевают отслеживание местоположения, доступ к списку контактов на устройстве жертвы, доступ к уникальному UDID, обмен данными с рекламными и аналитическими компаниями и т. д.

Методы шифрования в WhatsApp - мечта АНБ.

Мобильное приложение WhatsApp, предназначенное для передачи сообщений и выкупаемое социальной сетью Facebook за $19 миллиардов, представляет собой крайне привлекательную для хакеров и государственных шпионов платформу. Об этом со ссылкой на исследователей безопасности из компании Praetorian сообщает издание Ars Technica. По словам экспертов, проблема заключается в неэффективной реализации методов шифрования, позволяющей третьим лицам с относительной легкостью осуществлять перехват пользовательского трафика. Речь идет о протоколе secure sockets layer (SSL) версии 2, которая подвержена ряду "широко известных атак".

Hacking Team продавала шпионское ПО.

Согласно исследованиям, проведенным некоммерческой организацией Citizen lab, многие страны мира используют шпионское ПО и осуществляют слежение за гражданами, нарушая права человека. В ходе исследований, в 21 стране, в том числе в Азербайджане, саудовской Аравии, Судане и Эфиопии, эксперты обнаружили инструменты для удаленного взлома, разработанные Hacking Team. Отметим, что Hacking Team, также известная как HT S.r.l, является итальянской компанией, специализирующейся на серьезном ПО для слежения - Remote Code System (RCS) – и его продаже правительствам и правоохранительным органам. Тем не менее, представитель Hacking Team Эрик Рейб (Eric Rabe) заявил, что компания не предоставляет ПО «репрессивным режимам».

Разведслужба Турции следила за иностранцами.

Центральный орган разведки Турции (Milli İstihbarat Teşkilatı, MİT) следил за 2473 людьми. При этом большинство из них составляли иностранцы, сообщает портал Security Week со ссылкой на слова вице-премьера государства Бесира Аталая (Besir Atalay). По утверждениям последнего, изначально слежка использовалась исключительно с целью вычисления потенциальных террористов.

«Яндекс»: В нашем браузере нет противозаконного функционала.

Как сообщает «Лента.ру» со ссылкой на представителей «Яндекса», в web-обозревателе компании не реализовано каких-либо технологий, предназначенных для обхода блокировки противоправных web-сайтов. При этом, по заверениям разработчиков, ранее Роскомнадзор уже отправлял им запрос в отношении «Яндекс.Браузера» с целью выяснить «некоторые особенности работы» программы. Среди прочего регулятор уже выяснял можно ли путем использования функции «Турбо» получить доступ к тем ресурсам, которые были внесены в Единый реестр и заблокированы операторами связи.

Недостаточная безопасность SSH-ключей.

Согласно последним исследованиям Понемонского института (Мичиган, США), многие компании подвергаются серьезным замаскированным расширенным постоянным угрозам

(Mask Advanced Persistent Threat), обнаруженным недавно. Причиной этому является недостаточное управление SSH-ключами, используемыми для входа в критические внутренние системы и сервисы. В ходе исследовательской кампании Global 2000, в которой приняло участие 2,1 тыс. системных администраторов, выяснилось, что системы трех из четырех организаций уязвимы к атакам на уровне ядра именно из-за недостаточной безопасности SSH-ключей.

Исследователям удалось скомпрометировать...

Как следует из сообщения в блоге Bromium, исследователям компании удалось обойти защиту Enhanced Mitigation Experience Toolkit (EMET) от компании Microsoft. Среди прочего, эксперты скомпрометировали механизм противодействия возвратно-ориентированному программированию (ROP), однако достичь этого удалось только для 32-битных процессов. «Мы выяснили, что EMET прекрасно подходит для обеспечения защиты от атак, основанных на повреждении памяти, однако нам стало интересно, сможет ли более подкованный в технических вопросах злоумышленник успешно провести атаку», - поясняет эксперт Джаред ДеМотт (Jared DeMott).

США следила за ...

Агентство Национальной Безопасности США (АНБ) следило за 320 политическими и бизнес-лидерами Германии, в том числе за министром обороны Томасом де Мезьером (Thomas de Maiziere), сообщает издание Bild am Sonntag . Американско-немецкие отношения ухудшились после того, как в Сети появились документы, предоставленные Эдвардом Сноуденом. Тогда сообщалось, что американские спецслужбы якобы прослушивали телефон канцлера Германии Ангелы Меркель (Angela Markel), а также перехватывали онлайн переписку и записи телефонных разговоров обычных граждан Германии.

Немецкие разработчики устранили...

Немецкие разработчики устранили критическую брешь в шифровании OS X Mavericks. Разработчики из немецкой компании по информационной безопасности SektionEins выпустили приложение для OS X Mavericks от Apple, которое, по словам создателей,

устраняет недавно обнаруженную брешь в системе шифрования платформы. Программа была выпущена через день после того, как в Купертино состоялся релиз обновления для мобильных прошивок iOS 7 и iOS 6, устраняющего брешь в протоколах шифрования SSL/TLS.

Read more http://www.linux-info.ru/novosti-24-02-03-03.html