Автор:
29.06.14 20:44 -

Необычные средства для похищения Wi-Fi.

В ходе конференции DEF CON 22, которая в скором времени состоится в Лас-Вегасе, ИБ-эксперт Джин Брэнсфилд (Gene Bransfield) представит систему WarKitteh, разработанную для перехвата пакетов в Wi-Fi сети. При этом устройство якобы будет настолько маленьким, что поместится на ошейнике любого домашнего питомца, пишет The Register. В своем проекте Брэнсфилд использовал ошейник для кота. По его словам, подобная практика вовсе не является чем-то чрезвычайным. Кроме того, он уверен, что коты являются «идеальным средством для похищения Wi-Fi».

Случайно опубликовал пароль...

Идентификатор сети Wi-Fi (SSID) и пароль, принадлежащие центру по обеспечению безопасности Чемпионата мира по футболу, стали доступны широкой общественности. Так, на снимке, сделанном для местного печатного издания, случайно оказались вышеуказанные данные, написанные на белой доске.

Антипиратский закон касательно музыки...

Антипиратский закон, который вступит в силу летом этого года, не будет распространяться на музыкальный контент, рассказали два участника рабочей группы при Минкомсвязи. Законопроект будет распространяться на фильмы, книги и программное обеспечение. Предполагается, что борьба властей с пиратской музыкой может начаться не раньше января 2016 года.

Патчи для NTP серверов...

ИБ-эксперты выпустили исправления безопасности для NTP серверов, благодаря чему уменьшается возможность осуществления DDoS-атак. Согласно данным специалистов из NSFOCUS, после установления патчей количество уязвимых серверов сократилось с 432

120, зафиксированных в начале текущего года, до 17 647 в мае этого года.

McAfee: Для распространения вредоносного ПО...

Согласно отчету об угрозах безопасности, опубликованному экспертами из McAfee Labs во вторник, 24 июня, для распространения вредоносного ПО киберпреступники все чаще эксплуатируют бреши в доверенных мобильных приложениях и сервисах. В документе описываются три примера использования вредоносных приложений, а также уязвимости в легитимных программах и сервисах.

Google Glass - похищения паролей.

В последнее время «умные» устройства, предназначенные для ношения на теле, в частности Google Glass, вызывают беспокойство. По мнению исследователей из Массачусетского университета Лоуэлла (University of Massachusetts Lowell), гаджет можно использовать для подсматривания чужих паролей и кодов безопасности. Ученые считают, что если снять на камеру пользователя, набирающего пароль, то по записи можно определить вводимые им знаки. Об этом во вторник, 24 июня, сообщило издание Wired.

Генпрокуратуру просят проверить Twitter.

Депутат РФ от фракции «Единая Россия» Евгений Федоров направил в Генпрокуратуру запрос на проверку сервиса микроблогов Twitter. Евгений Федоров хочет узнать, соблюдает ли Twitter закон о противодействии экстремизма в Интернете.

Вот незадача, так нелепо попался.

Житель Минессоты по имени Джеймс Вуд (James Wood), вернувшись домой осознал, что в его доме кто-то был. Хозяин не обнаружил своих кредиток, наличных денег и

наручных часов. Тем не менее, Вуд нашел обувь, ремень и джинсы незваного гостя, которые тот, судя по всему, просто забыл. Определить личность злоумышленника получилось с помощью социальной сети Facebook. Воспользовавшись компьютером владельца дома, вор забыл закрыть свою учетную запись, что и помогло полиции поймать преступника.

В Сети появился новый архив XSS-уязвимостей.

На днях стало известно о начале работы нового архива XSS-уязвимостей. По словам создателей проекта XSSposed , архив станет некой альтернативой и продолжением ранее существовавшего ресурса xssed.org. XSSposed создавался по подобию своего предшественника. Так, это открытый некоммерческий каталог уязвимостей Cross-Site Scripting (XSS). Ожидается, что на сайте будут публиковать данные о брешах, найденных на всех доступных интернет-ресурсах.

За 7 дней более полумиллиона евро.

Эксперты из «Лаборатории Касперского» сообщили о таинственном банковском трояне Luuuk, который всего за неделю принес злоумышленникам более €500 тыс. По их словам, хакеры использовали данное вредоносное ПО для осуществления атаки «человек-в-браузере».

Read more http://www.linux-info.ru/novosti-23-06-29-06.html