$('#14162915464037933').html(decodeURIComponent('%d0%a4%d0%be%d1%82%d0%be%3a%20%d0%90%d1%80%d1%82%d0%b5%d0%bc%20%d0%96%d0%b8%d1%82%d0%b5%d0%bd%d0%b5%d0%b2%20%2f%20%d0%a0%d0%98%d0%90%20%d0%9d%d0%be%d0%b2%d0%be%d1%81%d1%82%d0%b8'));

Терминалы для оплаты аренды велосипедов в системе московского городского велопроката содержали недостатки конфигурации, с помощью которых злоумышленники могли получить доступ к персональным данным пользователей. Об этом говорится в сообщении «Лаборатории Касперского».

Приложение для велосипедных паркоматов, работающих на базе операционной системы семейства Windows, позволяет пользователю зарегистрироваться и получить справочную информацию о местоположении паркомата и других велосипедных парковок. Отображение всего этого, а также баров, кафе и прочих объектов реализовано с помощью виджета компании Google, который разработчики приложения велопаркоматов используют в своем продукте.

Согласно сообщению компании, у пользователя нет возможности свернуть полноэкранное приложение и выйти за его пределы, а именно в нем кроется недостаток конфигурации, который позволяет скомпрометировать устройство, — в правом нижнем углу виджета содержатся ссылки «Сообщить об ошибке», «Конфиденциальность» и «Условия использования», нажатие на которые влечет за собой запуск браузера Internet Explorer.

Воспользовавшись возможностью из настроек браузера попасть в раздел со справочной информацией, пользователь может перейти в «Панель Управления» и раздел «Специальные возможности», в котором можно включить экранную клавиатуру. При помощи виртуальной клавиатуры существует возможность активировать системную утилиту «cmd.exe» — командную оболочку Windows, которая запускается с правами администратора — это открывает для пользователя возможность скачивания и запуска абсолютно любого приложения.

По мнению экспертов «Лаборатории Касперского», злоумышленники как угодно могут использовать такие недостатки конфигурации. Так, киберпреступник может извлечь пароль администратора, хранящийся в памяти в открытом виде, получить слепок памяти приложения велопарковки, из которого затем можно извлечь личную информацию его пользователей: ФИО, адрес электронной почты и телефон для последующей продажи данных на черном рынке.

Злоумышленник также может установить кейлоггер, перехватывающий все введенные данные и отправляющий их на удаленный сервер, или реализовать сценарий атаки, результатом которой станет получение еще большего количества персональных данных, добавив поля для ввода дополнительных данных.

По словам Дениса Макрушина, технологического эксперта «Лаборатории Касперского», для того, чтобы исключить вредоносную активность на публичных устройствах, разработчикам приложения велопарковки и администраторам терминалов следует запретить возможность открытия внешних ссылок в полноэкранном приложении и не допускать вызова каких-либо элементов интерфейса ОС Windows. Текущий сеанс операционной системы при этом должен быть запущен с ограниченными привилегиями пользователя, а учетные записи на каждом устройстве должны быть уникальными.

«Что касается пользователей терминалов, мы рекомендуем не вводить полные реквизиты своих платежных карт — к примеру, для осуществления платежа не требуются CVV2/CVC2 коды карточки. Требование их ввода должно настораживать», — отметил Макрушин.

Производитель паркоматов уведомлен обо всех выявленных недостатках конфигурации. Повторно проверенные терминалы в настоящий момент не содержат описанные недостатки, уточнили в «Лаборатории Касперского».

Источник - http://lenta.ru/news/2014/11/17/kasper/