Автоматы по продаже билетов Muni (San Francisco Municipal Railway, организация-оператор общественного транспорта в Сан-Франциско) весь день выводили на экраны только два сообщения: «Не работает» и «Бесплатный Muni». Компьютеры сотрудников организации сообщали следующее: «Вы взломаны, все данные зашифрованы. Контакт для получения ключа: cryptom27@yandex.com, ID:681».

По форме данная атака представляет собой стандартную вредоносную программу с требованием выкупа, которая шифрует все данные в системе или на устройстве и затем предлагает связаться с хакером по e-mail, чтобы договориться о сумме выкупа ключа шифрования файлов. В случае с Muni злоумышленники также пытались установить контакт с представителями организации, сообщает The Verge.

Журналисты издания связались с хакерами по указанному адресу электронной почты и получили следующий комментарий: «Наше программное обеспечение работает полностью автоматически, и мы никуда специально не направляли эту атаку! Муниципальное транспортное агентство Сан-Франциско было очень Уязвимо, и 2000 серверов/ПК было поражено программой! Поэтому мы ожидаем контакта с ответственным лицом в агентстве, но я думаю, что они не хотят идти на сделку с нами».

В самой мощной в истории DDoS-атаке, которая произошла этой осенью, хакеры также использовали автоматическое программное обеспечение. Программа находила IoT-устройства, владельцы которых не сменили заводские логины и пароли, в результате чего злоумышленникам удалось получить доступ более чем к 1,5 млн умных устройств. После этого случая крупнейшие ИТ-компании, включая Google, Intel, Microsoft, разработали собственный список рекомендаций по безопасности в сфере IoT.