На сегодняшний день, работа с дистанционным банковским обслуживанием (ДБО) признана одной из самых обсуждаемых и «болезненной» темой как среди компаний, занимающихся обеспечением информационной безопасности, так и среди самих банков.

Проблема существует давно, но стала острой только сейчас, а масштаб такой угрозы просто колоссальный. Каждый год по официальным сведениям у клиентов банков воруют десятки миллиардов рублей. Несомненно, банки инвестируют в проекты по безопасности ДБО десятки миллионов рублей, а ведущие компании в области информационной безопасности выводят на рынок новые средства по борьбе со «шпионажем» и утерей информации при работе в данной системе. Однако данные системы дорогостоящие, и многие банки, вынужденные использовать данные системы, чтобы обезопасить своих пользователей, используют менее дорогие и тем самым и менее эффективные средства по безопасности.

Наравне с этими разработками, так же и разрабатываются новые схемы хищения и новые способы заразить наши СВТ вредоносной программой, которая позволит злоумышленникам заполучить конфиденциальную информацию. Компании, которые являются разработчиками антивирусных программ, сами говорят о том, что вирусы рождаться и развиваться каждый день, и их база о вирусах бывает «устарелой». Причем ни для кого не секрет, что сегодня целый класс вредоносных программ нацелен именно на атаки на системы ДБО.

Рассмотрим один из «популярных» вариантов «хищения». Некий пользователь, сидел у себя дома, и искал нужную ему информацию в интернете. Поисковик обработал информацию и выдал нашему пользователю десятки ссылок на различные сайты. И переходя по одной из таких ссылок, наш пользователь случайно скачал вирус «А», причем ни пользователь, ни браузер, ни компьютер не сказали пользователю о скачивании данного файла, тем боле о том, что Вы скачали вирус. Спустя, некоторое время наш

пользователь обращается к системе ДБО, чтобы перевести себе любимому немного рублей на телефон. Заходит на сайт, вводит «логин-пароль», дальше переводит себе денежку и ждет смс о пополнении счета. Но смс нет, а на странице нашего банка, пользователь может заметить изменившуюся одну-две буквы в написании электронного адреса банка, и смс о том, что он (добрейший души человек) перевел, скажем, 1000 рублей на счет, совершено не знакомому человеку. Банк не чувствует своей вины, ведь с его точки зрения – он выполнил Ваш перевод.

Тогда возникает вопрос, как самому защитить свои деньги?

Можно, например, отключить интернет. И теперь вирус не сможет быть скачан. Хорошо, а как же наш онлайн банк? Допустим, что наш банк рядом с домом или работой, и теперь пользователь, только так и будит выполнять операции с банковским счетом. А если нужно пополнить счет, прямо сейчас, в три часа ночи? Да, мы можем выключить компьютер, подключить интернет, залезть только на сайт банка и сделать отправление денежных средств и сразу снова выключить компьютер. Мы знаем тех, кто именно так и делает! Но ведь нельзя упускать тот факт, что вирус может передаться на компьютер, через USB-устройство. Не спорю, можно поставить в антивирус опцию «проверять USB-устройства», но, если мы отключили наш ПК от интернета, то согласитесь, что через какое-то время, наша база антивируса устареет, и она не заметит «мутировавшего» вируса. В итоге мы получили зараженный ПК без доступа к интернету. Мы так же можем предложить запретить использовать USB-устройства и обклеить USB-входы на ПК. С таким же успехом мы можем убрать ПК в коробку, а ту в шкаф. Чем плоха такая защита?

Если серьезно, то на рынке информационной безопасности, давно есть продукты, которые могут защитить Ваши данные при работе с системами ДБО. В частности, можно установить доверенный сеанс связи, с помощью продукта СОДС «МАРШ!». Правда такая защита возможна, только на ПК,

ноутбуках, терминалах и отдельных планшетах. Именно «отдельных», и ограничения в этом смысле довольно существенные: в первую очередь, в настоящее время МАРШ! можно адаптировать для применения на планшетах исключительно x86, а таких – меньшинство. Кроме того, загрузка планшета с внешнего USB-устройства – не всегда тривиальная задача. Наконец, многим просто не нравится, «когда из планшета что-то торчит».

Конечно, можно поступить с планшетом так же как с нашим эталонным ПК: отключить его от интернета, запретить использовать SD-карту и так далее, и из мобильного устройства, мы получим оригинальную рамку для фотографий. Поэтому компанией Trusted Cloud Computers (TCC) была разработана линейка защищенных микрокомпьютеров, в которую также входит защищённый планшет TrustPad.

TrustPad – это планшет, у которого одна из трех микросхем памяти, на которую записана ОС, переведена в режим «только чтение». Этот режим обеспечивает неизменность ОС, тем самым делая данную ОС защищённой от программных действий «нарушителей», а также от возможности записи вируса в долговременную память планшета.

Вторым преимуществом данного планшета является в том, что у него две ОС, одна «защищённая» - для работы, вторая «незащищённая» - для личного пользования. Работа в разных ОС, загружающихся из разных, физически разделенных, разделов памяти, производится с помощью физического переключателя (то есть невозможно программное воздействие на выбор режима), расположенного снаружи корпуса устройства, то есть необходимый режим выбирает пользователь.

Работа с данным планшетом не вызывает никаких трудностей. Обе ОС – на базе Android 4.4.2, которая проста в работе, а также знакома многим.

Третьим преимуществом TrustPad’a является возможность использования двух слотов для карт памяти, один из которых не виден в режиме «незащищенной ОС».

Незащищенная ОС обновляется так же, как любой Android, а защищенная – в сервисном центре в специальном технологическом режиме, перевод устройства в который осуществляется физическим переключателем внутри корпуса, недоступным пользователю или программному воздействию.

Характеристики данного планшета, не уступают по характеристикам планшетам его ценовой категории известных брендов:

- ОЗУ: 1 ГБ DRR
- Дисплей: 10.1″, 1280*800, 16:9 IPS
- Фронтальная камера: 1 (0.3 MP)
- Тыловая камера: 1 (2.0 MP)
- Аудиовыход: 1 (3.5 mm)
- Батарея: 1 (6800mAh)
- Защищенный диск: 1
- Размер диска: 8 ГБ
- Незащищенный диск: 1
- Размер диска: 8 ГБ
- Диск для обновлений: 1
- Размер диска: 8 ГБ
- Порт питания: 1 DC
- Питание: DC 5V, 2.5A

А теперь вернемся к нашему банковскому сайту и потере денег. Как говорилась раньше на TrusTPade в режиме защищенной ОС не возможна запись. То есть наш вирус «А», который сидел на злополучном сайте не сможет записать себя на планшет, и тем самым не «представиться собой»

банковским сайтом. То есть, после просмотра «сомнительного» сайта, наш пользователь, обращаясь к системе ДБО, во-первых, не перейдет на «неправильный» банковский сайт, так и не потеряет деньги при переводе их себе на счет.

(Более подробную информацию про планшет TrustPad и всю линейку защищённых микрокомпьютеров Вы можете найти на сайте компании: http://www.trustedcloudcomputers.ru/).