Мошенничества, направленные на заражение устройства пользователя вредоносной программой

Мошенники, используя электронные адреса, схожие с адресами легальных организаций, рассылают от их имени сообщения, содержащие ссылку на скачивание открытки, музыки, картинки, архива или программы. Запуск вложения или переход по ссылке может инициализировать установку на устройство вредоносносной программы (вымогателя-блокиратора, шифровальщика, троянской программы) или же оформление подписки на платную услугу.

Пример хищений денежных средствсо счетов с использованием вредоносных программ

В сматрфон или компьютер жертвы тайно устанавливаются вредоносное ПО. Вредоносная программа проникает и устанавливается на телефон при открытии в сети Интернет страниц различных сайтов, адреса которых потерпевшие чаще всего получают в СМС или ММС сообщениях. Кроме того, потерпевшие сами неосознанно могут устанавливать на мобильные устройства вредоносные программы, замаскированные под игры и другие программные продукты. Одним из признаков наличия вредоносных программы на мобильном телефоне является направление «пустых» СМС или ММС сообщений на телефоны, имеющихся в контактах устройства. При открытии адресатом такого СМС или ММС сообщения, происходит дальнейшее заражение вирусом телефонов, получившее данное сообщение.

Это могут быть троянские программы, которые не размножаются и не рассылаются сами, они ничего не уничтожают. Задача троянской программы - обеспечить злоумышленнику доступ к устройству жертвы и возможность управления им. Все это происходит очень незаметно, без эффектных проявлений. Если к смартфону подключена услуга «Мобильный банк», то сведения о доступе в Личный кабинет становятся известны преступнику. Тайно входя в чужие Личные кабинеты он может перечислять денежные средства сотен потерпевших на свои счета, а затем обналичивать.

Тактика борьбы достаточно проста:

Не допускать, чтобы вредоносные программы попадали на компьютер или смартфон (чаще всего страдают владельцы смартфонов с ОС Андроид). Если они все-таки попали, ни в коем случае не запускать их. Принять меры, чтобы, по возможности, они не причинили ущерба. Использовать специальные антивирусные программы.

Отслеживать и блокировать опасные действия, которые могут выполнять вредоносные программы способны специальные программы-сторожа, обычно входящие в состав антивирусных пакетов. Они автоматически запускаются на выполнение при загрузке операционной системы и незаметно прослеживают действия программ.

Если деньги все-таки списались, разработан алгоритм действий потерпевшего: Немедленно прекратить любые действия с сотовым телефоном, принудительно

отключить его, извлечь СИМ карту. Обеспечить сохранность (целостность) сотового телефона, как возможного средства совершения преступления. Не предпринимать никаких действий для самостоятельного или с привлечением посторонних ИТ-специалистов поиска и удаления вирусов, восстановления работоспособности сотового телефона, не отправлять сотовый телефон в сервисные службы ИТ для восстановления работоспособности.
Незамедлительно обратиться в свой банк по телефону горячей линии с поручением о блокировки операции с расчетным счетом и отзывом криминального перевода.
Незамедлительно обратиться в свой банк с письменным заявлением об отзыве платежа, возврате средств и блокировании доступа к системе «Мобильный банк» (приложение 2). Заявление может быть направлено в банк по факсу или по электронной почте (скан-копия). Оригинал заявления должен быть доставлен в банк в течение одного дня. Оформляется в 2-х экземплярах.
Согласно полученной в банке детализации с расчетного счета обратиться в банк получателя (используемого преступником) по телефону с заявлением о приостановке исполнения платежа и возврате средств.
В течение одного дня обратиться с заявлением в правоохранительные органы о факте хищения денежных средств. Для полиции понадобиться документальное подтверждение хищения денежных средств, в том числе выписка по банковскому счету, справка из банка, иные документы, подтверждающие списание заявленной суммы ущерба. Существует возможность получение этих данных из «личного кабинета» пользователя услуг сотовой связи, банк-онлайн с письменного согласия потерпевшего. Эта информация может быть зафиксирована протоколом осмотра места происшествия.
Оперативно обратится в банк с заполненной справкой по факту инцидента информационной безопасности в системе дистанционного банковского обслуживания (приложение 3), которое оформляется в 2-х экземплярах.
Справочно: *ФЗ от 27.06.2011 № 161-ФЗ «О национальной платежной системе» предусматривает процедуру обращения в банк после незаконной транзакции и дает право на возмещение незаконно списанных денежных средств со счета. Так, п. 11 ст. 9 гласит «В случаи утраты электронного средства платежа и (или) его использования без согласия клиента, клиент обязан направить соответствующее уведомление оператору по переводу денежных средств в предусмотренной договором форме незамедлительно, после обнаружения факта утраты электронного средства платежа и (или) его использования без согласия клиента, но не позднее дня, следующего за днем получения от оператора по переводу денежных средств уведомления о совершенной операции».*
В п. 15 ст. 9 указано «В случае, если оператор по переводу денежных средств исполняет обязанность по уведомлению клиента - физического лица о совершенной операции в соответствии с частью 4 настоящей статьи и клиент - физическое лицо направил оператору по переводу денежных средств уведомление в соответствии с частью 11 настоящей статьи, оператор по переводу денежных средств должен возместить клиенту сумму указанной операции, совершенной без согласия клиента до момента направления клиентом - физическим лицом уведомления. В указанном случае оператор по переводу

денежных средств обязан возместить сумму операции, совершенной без согласия клиента, если не докажет, что клиент нарушил порядок использования электронного средства платежа, что повлекло совершение операции без согласия клиента - физического лица».