Как не попасть в руки мошенников потребителям финансовых услуг

Банковская ассоциация Республики Татарстан совместно с Министерством внутренних дел по Республике Татарстан провели семинар на тему: «Как не попасть в руки мошенников портребителям финансовых услуг. Виды мошенничества. Механизмы защиты».

На семинар были приглашены специалисты банков, работающие в данном направлении, руководитель департамента по информационной политке Торгово-промышленной палаты РТ Елена Агзамова, руководитель Лаборатории кибербезопасности и управления инцендентами Дмитрий Ермишин, представители организации по обеспечению информационной безопасности «МГА-Секьюрити» (г.Казань) (http://mga-security.com).

Семинар провел начальник специальной группы по выявлению и раскрытию высокотехнологичных преступлений МВД по Республике Татарстан Максим Машин.

В приветственном слове Председатель Совета БАТ РТ Людмила Китайцева подчеркнула важность мероприятия и попросила собравшихся выстроить диалог со специалистами, так как это поможет улучшить финансовую безопасность и защиту представляемых здесь организаций.

В своем выступлении Максим Машин подробно остановился на организационных и правовых аспектах информационной безопасности финансово-кредитных учреждений, разобрал виды мошенничества и механизмы защиты.

Максим Юрьевич проинформировал собравшихся, что спецгруппа в МВД по Республике Татарстан (прим.автора - подобных спец.групп в России не имеется) создана год назад в связи с участившимеся случаями кибератак на сайты, расчетные счета банковских структур, иных предприятий. При этом существует много аспектов в противодействии мошенничеству, сложности в раскрытии преступлений, так как они совершаются в виртуальном пространстве. Как подчеркнул Машин, продвинутые пользователи находят возможности внедрения зловредов - программ, наносящих ущерб компьютеру или хранящейся на ней информации, практически во все финструктуры. Количество атак на территории России находится в так называемой «красной зоне», то есть ситуация достаточно опасная.

До 2014 года хищения денежных средств производились с использованием скиммингового оборудования на банкоматах, которое копирует все данные с магнитной полосы. Сотрудниками МВД по Республике Татарстан были задержаны пять мошеннических групп, изъято спецоборудование, и хищения в республике пошли на спад.

Следующий опасный вид хищения – это хищение денежных средств с банковских карт при помощи мобильного банка. Здесь Машин порекомендовал банкирам не навязывать данную услугу потребителям.

В 2014-2015 годах зафиксированы хищения с использованием системы удаленного воздействия на банкомат. Так в Набережных Челнах произошло шесть хищений, не все они раскрыты.

Серьезные обороты набрал способ проникновения в систему дистанционного банковского обслуживания, и схемы здесь достаточно сложные. В большинстве случаев компрометация электронных ключей происходит с помощью вредоносного ПО, которое проникает через Интернет. Этот код обнаруживает, что на данном ПК ведется работа с системой ДБО и осуществляет копирование ключей и логина/пароля пользователя, а затем передает данную информацию злоумышленникам. Кроме того, возможны случаи, когда перевод денежных средств осуществляется непосредственно с ПК жертвы посредством ПО для удаленного администрирования, также установленного мошенниками через сеть Интернет. Здесь важно помнить, что электронные улики недолговечны и требуют особого бережного отношения в момент сбора и анализа, чтобы не уничтожить данные и обеспечить их юридическую значимость.

Максим Юрьевич рассмотрел в своем выступлении новые виды вредоносных программ. Так, специалисты BAE Systems обнаружили новую версию ботнета Qbot, задача которого - кража учетных данных и создание «черных ходов» на зараженных системах. В состав ботнета входит 54,5 млн. инфицированных ПЭВМ в тысячах организаций. Qbot запрограммирован на автоматическое распространение и не обнаруживается многими антивирусными решениями. Попав в компьютер, Qbot пытается заразить другие ПЭВМ в сети, а если они защищены паролем, зловред осуществляет попытки доступа к диспетчеру паролей, а если и это не получается, применяет список с распространенными сочетаниями логин/пароль, находящемся в теле трояна, для реализации брутфорс-атаки. Qbot ориентирован на заражение неограниченного числа компьютеров. Программа обновляется каждые шесть часов, что не позволяет модифицировать его структуру и эффективно ему противоборствовать.

Специалистами IBM диагностирован новый вид вредоносов, получивший наименование GozNym, поскольку включает в себя коды двух троянов Nymaim и Gozi, что делает его весьма стабильным и эффективным. Так, часть первого вируса (Nymaim) обеспечила скрытность и стабильность его работы, а часть второго (Gozi) - позволила осуществлять хищение, используя «зараженные» браузеры. Вредонос включает в себя элементы, схожие с известными троянами Zeus и SpyEye, имеет возможность применения weblnject для IE, Firefox, Chrome.

В конце мероприятия подполковник Машин призвал кредитные учреждения четко выполнять требования и инструкции федеральных центров по кибербезопасности, рассмотреть предложение по совместному аудиту надежности информационных систем финансово-кредитных учреждений.

ТПП Республики Татарстан