Антифрод для банков становится все более актуален

Компания «Фродекс» специализируется на разработке собственного продукта, интеллектуальной системы обнаружения мошеннических операций FraudWall. Кроме непосредственно разработки, компания оказывает услуги по проведению расследований киберпреступлений и мошенничеств с использованием высоких технологий (определяет, как мошенники украли деньги банка или клиента). И по заказу банка-партнера может провести pen-test (тест на проникновение или взлом) его транзакционных систем. Сегодня мы беседуем с генеральным директором компании «Фродекс» (www.frodex.ru) Андреем Луцковичем.


Андрей Луцкович

– Насколько серьезны сегодня угрозы кибермошенничества для банков?

Андрей Луцкович: Весьма серьезны. По данным компании Group-IB, в 2012 году в России ежедневно совершалось 44 хищения из систем ДБО, а общий объем мошеннических операций в системах ДБО в 2012 году оценивается почти в $450 млн. По нашим данным, практически каждый банк на сегодняшний день сталкивается с мошенничеством. Чем больше клиентов, тем чаще. От двух-трех мошенничеств в год в мелком банке до десятков мошеннических платежей в месяц – в крупном.

– Неужели банки плохо защищены?

Андрей Луцкович: Скорее плохо защищены клиенты банков. Основной вектор атак направлен на клиента банка. Именно на его стороне выполняются действия по реализации киберпреступления, начиная от кражи учетных данных для работы в системе дистанционного банковского обслуживания (имя, пароль, ключи), заканчивая подменой платежного поручения, отправляемого на исполнение в банк.

– В чем главная проблема клиента?

Андрей Луцкович: По моему мнению, в отношении к собственной безопасности. В большинстве случаев люди не задумываются об этом, пока не произойдет инцидент. Что называется, пока гром не грянет. Все, вроде бы, освоили компьютер, но мало кто понимает, как на самом деле работают ИТ, почему необходимо тратить деньги и приобретать антивирусные продукты, что будет, если хранить ключи на диске ПК или оставлять специальный ключевой носитель постоянно подключенным к компьютеру. Поэтому, если говорить языком специалистов, на стороне компьютера клиента работает «недоверенная среда».

Развитие информационных технологий дает киберпреступникам возможность воспользоваться «открытой дверью», оставленной на компьютере клиента. 95% – инцидентов это результат работы специализированного вирусного программного обеспечения так называемых «банковских троянов». В последнем отчете антивирусной компании Trend Micro так и сказано: «уровень инфицирования банковскими троянами – наибольший за последние 11 лет».

– Разве банки не просвещают клиента?

Андрей Луцкович: Несомненно, каждый банк в той или иной мере старается информировать своих клиентов о возникающих рисках. Этим же занимаются профессиональные игроки рынка информационной безопасности, государство. Но этих усилий явно не достаточно: об этом свидетельствует статистика мошенничеств.

– Что делается не так?

Андрей Луцкович: Явно недооценивается развитие киберпреступности. Надо признать, что «на темной стороне» люди работают лучше. Они осознали, что их ждет огромное число клиентов банков, необходимы только технологии, позволяющие получить всё от устройства клиента.

И развитие этих технологий не заставило себя ждать. Сейчас известно не менее десятка специализированных банковских троянов. Они постоянно развиваются, наблюдается тесное взаимодействие

Текст:
Андрей Новиков

разработчиков со всего мира, ведь Интернет сделал общение более доступным для всех, в том числе, и для злоумышленников. Более того, новейшая история уже помнит случаи, когда последние достижения, продававшиеся на подпольном рынке за значительные деньги, вдруг выкладывались в сеть для безвозмездного изучения. Надо ли говорить, что это делает продукты всех остальных более совершенными.

Но и это еще не все. С одной стороны, мы наблюдаем явную специализацию и профессиональный рост разработчиков вирусного ПО, что говорит о хорошем финансировании и образцовом управлении. Пример скорости развития – повсеместный переход хакеров на модель продажи ПО в аренду. Мы только начинаем привыкать к SaaS (software as a service — программное обеспечение как услуга), преступность давно ее использует.

С другой стороны, отличительная особенность сегодняшнего дня – доступность инструментария. В какой-то момент цены на качественные специализированные продукты вирусной индустрии начали измеряться десятками тысяч долларов, что, несомненно, ограничивало их доступность. Выход был найден в помесячной аренде. На конференции PHD2013 называлась цифра в 595 долларов, этого достаточно, чтобы начать заниматься мошенничеством.

Следствием доступности, мы считаем, стал интерес к кибермошенничеству так называемого «традиционного» преступного мира. Теперь все стало проще. Не надо разбираться в компьютерных технологиях, достаточно вносить помесячно абонентскую плату, «очкарики» все сделают. Остается организовать вывод денег: регистрацию фирм-однодневок, работу с дропперами (людьми, снимающими деньги в банкоматах) – все то, что они и так делать давно умеют. Результат, что называется, налицо.

– Достаточно мрачная картина, Извечный вопрос: что делать?

Андрей Луцкович: Надо развиваться, делать это умнее и активнее. Отрасль уже отреагировала, в первую очередь, появлением нового поколения клиентских устройств авторизации платежей, главная цель которых – защитить пользователя от подмены реквизитов подписываемого платежного поручения и обеспечить надежное хранение криптографических ключей, вынесение операций подписывания за пределы не доверенного ПК. Но у подобных решений есть явные минусы – их надо раздать всем клиентам, а это достаточно дорого. Наше мнение: защиты только клиента уже явно не достаточно!

– Что же предлагаете вы?

Андрей Луцкович: Анализ информации на стороне банка. В настоящий момент очевидно, что как каждый ПК клиента должен быть оснащен антивирусным ПО, так и каждый банк должен быть оснащен системой выявления мошеннических платежей (системой «антифрод»). Необходим оперативный анализ всего, что поступает на сторону банка от клиента, на предмет выявления аномалий.

– Неужели банки этим не занимаются?

Андрей Луцкович: Занимаются, но не все, и с разной степенью успеха. В большинстве случаев банки пытаются реализовать некую простую логику обнаружения на основе доступных им параметров. Но эффективность подобных решений невелика. Попытка приобрести профессиональную систему наталкивается на значительную стоимость решений зарубежного разработчика и необходимость адаптации к российским реалиям и особенностям.

– В чем камень преткновения?

Андрей Луцкович: В эффективности обнаружения. Необходимо не только умение разработать систему, но и научить ее эффективно обнаруживать мошеннические операции. Здесь нужен опыт другого рода.

– У вашей компании он есть?

Андрей Луцкович: Мы считаем, что да. Специалисты нашей компании имеют опыт работы в службах информационной безопасности банков. Я сам проработал десять лет в крупной финансовой организации и занимался как реализацией мер защиты, так и непосредственно расследованиями инцидентов. У нас накоплен значительный опыт по этой проблематике. Кроме того, мы стараемся быть в курсе всех последних веяний в области компьютерного мошенничества.

– Не поделитесь чем-то новым из собственного опыта?

Андрей Луцкович: Вот свежий интересный случай из нашей практики, иллюстрирующий постоянный поиск и нестандартность подходов. Инцидент произошел недавно, буквально в октябре этого года. Злоумышленники получили удаленное управление компьютером клиента. Был создан поддельный платеж, но не в системе ДБО, а в системе бухгалтерского учета «1С:Бухгалтерия». Далее он был выгружен вместе со всеми остальными платежами клиента, импортирован в систему ДБО, подписан и отправлен в стандартном порядке. После успешной отправки был выполнен возврат на предыдущую

точку восстановления операционной системы, чтобы «замести следы». Но злоумышленникам это всё не помогло.

Подобных примеров можно привести много. Главное, что банки пока в роли догоняющих. Еще один пример: повсеместное внедрение банками использования одноразовых паролей присылаемых в виде СМС–сообщений. Пока это все внедрялось, клиенты обзавелись смартфонами, а злоумышленники научились писать вирусы под них. В итоге тренд этого года – двухфакторные атаки: как на ПК клиента с целью получения традиционных аутентификационных данных, так и на его мобильный телефон с целью перехвата интересующих СМС–сообщений.

– Что же предлагает ваша компания?

Андрей Луцкович: Весь наш опыт, знания и умения мы воплотили в системе антифрода собственной разработки – системе FraudWall. Наша система родилась не сразу, это результат длительного и не прекращающегося противостояния и расследования реальных инцидентов, что позволяет нам говорить о ее реальной эффективности.

– В чем, как вы считаете, главное отличие вашего продукта?

Андрей Луцкович: В подходе. Мы предоставляем не только программное обеспечение, способное решать намеченную задачу, мы предоставляем сервис по борьбе с мошенничеством. Наш продукт изначально поставляется с комплектом правил для обнаружения мошеннических платежей, что резко облегчает задачу банка по первоначальной настройке при внедрении. Поставляемая логика обнаружения – результат постоянной работы по расследованию инцидентов, консолидация нашего опыта работы по всем клиентам.

Обычно банк может полагаться только на собственный опыт и пытаться его реализовать в используемом ПО. В нашем случае банк получает гораздо больше. Очень важно, что в рамках поддержки приходят обновления по модернизации критериев обнаружения. «Горький опыт» реализованного мошенничества может быть не только собственным, и если мы открыли какую-то новую технику мошенничества, то информация о ней становится доступной сразу всем нашим клиентам. Можно сказать, что наш продукт – это своеобразный «антивирус» для банков, цель которого – обнаружение не вирусов, а мошенничества.

– Данный подход является инновационным?

Андрей Луцкович: В какой-то степени – да, но только у стороны защитников информации. Традиционно банки очень закрыты, они не спешат делиться своими проблемами и ориентированы на решение задачи только собственными усилиями.

Преступность же достаточно давно демонстрирует объединение усилий, интеграцию собственной деятельности. Мы пришли к мнению, что уже можно вводить в оборот выражение «Fraud as a Service» («мошенничество как услуга»). Необходимы адекватные меры борьбы и современная концепция защиты – «AntiFraud as a Service». В собственном продукте мы постарались реализовать консолидацию опыта борьбы с мошенничеством, сделать его более доступным, объединить усилия, наладив обмен информацией между разными источниками информации. Как пример, FraudWall автоматизирует задачу обработки межбанковской рассылки по «черным» спискам так называемого анти-дроп клуба. Информация по мошенникам используется системой с момента ее возникновения, исключается человеческий фактор.

– А если же у банка уже есть свой опыт борьбы с фродом, и он достаточно весом, могут ли они использовать ваш продукт?

Андрей Луцкович: Конечно, специалисты банка всегда могут дополнить логику обнаружения собственными наработками, для этого у нас предусмотрен конструктор правил. Более того, мы очень ценим обратную связь и внимательно выслушиваем пожелания клиентов. Здесь как нигде важно понимать, что качество продукта и, как следствие, эффективность обнаружения зависит от объединения усилий.

– На что еще можно обратить внимание?

Андрей Луцкович: Мы стараемся реализовать независимость от систем ДБО, используемых банком. В идеале, наш продукт должен уметь работать с любой системой ДБО. Мы достигаем это как за счет архитектурных решений FraudWall, так и за счет налаживания сотрудничества с разработчиками систем ДБО.

И наверное, для кого-то самое главное: мы предоставляем банкам возможность «тест-драйва». Наша маркетинговая политика предусматривает возможность установки полнофункциональной рабочей версии продукта FraudWall на срок до четырех месяцев бесплатно. Это позволяет потенциальному нашему клиенту не только проверить работоспособность связки ДБО и системы антифрода, но получить собственную статистику и оценить эффективность продукта в реальных условиях.