Банкоматы как они есть

Вячеслав Медведев
Старший аналитик отдела развития Компания «Доктор Веб»

Последний месяц Интернет был переполнен сообщениями, предрекавшими великие бедствия из-за прекращения поддержки компанией Microsoft операционной системы Windows XP. Озабоченность общественности вызвала возможность выявления новых уязвимостей уже после завершения поддержки и вероятное использование их злоумышленниками. Высказывались предположения о массовом переводе банкоматов на Linux в связи с невозможностью перехода под управление более ресурсоемкой Windows 7. Опасения понятны, вот только стоит отметить несколько моментов.

Начнем с того, что ОС Windows XP предназначена для использования на рабочих местах — компьютерах общего назначения. Почему вдруг она стала массово использоваться в системах, где по понятным причинам требуются серьезные меры безопасности? Кстати, у той же компании Microsoft есть целая линейка Microsoft Embedded, как раз специально предназначенная для использования во встраиваемых устройствах, в том числе в банкоматах. И она действительно используется, хотя распространена не так широко, как следовало бы.

Говоря об обновлениях безопасности настольной системы, нужно принимать во внимание, что банкоматы, как и иные встраиваемые устройства, устройства АСУТП, не могут перезагружаться в произвольный момент времени — они должны работать 24 часа в сутки, 7 дней в неделю, поскольку клиенту деньги могут потребоваться в любой момент. С другой стороны, никогда не известно, когда вендор выпустит обновления и потребуют ли эти обновления перезагрузки. Соответственно, применение обновлений производится в ходе регламентных работ — т. е. должно производиться. Проведение процедуры обновлений в ходе регламентов требует достаточно частых посещений, а это дорого и требует многочисленного и опытного персонала (мало ли что произойдет при обновлении), подготовки и проверки наборов обновлений, их пересылки обслуживающему персоналу (чаще всего на их домашние компьютеры, традиционно не защищаемые) с последующим переносом на сменных носителях.

Добавим, что стандарт СТО БР РФ в действующей версии не включает никаких требований к банкоматам и терминалам, а также к большинству организаций, их эксплуатирующим, и получим, что вопрос об актуальности обновлений для Windows XP в случае ее использования на банкоматах можно считать исчерпанным.

Тем не менее, вопрос безопасности банкоматов является актуальным, хотя и затуманен кучей мифов.

Первым и очень странным мифом является утверждение, что не существует требований по установке антивируса на банкоматы, в связи с чем можно обойтись системами на основе подсчета контрольных сумм. Даже не касаясь выходящей в скором времени новой версии СТО БР РФ, заглянем в стандарт PCI-DSS последней, третьей версии.

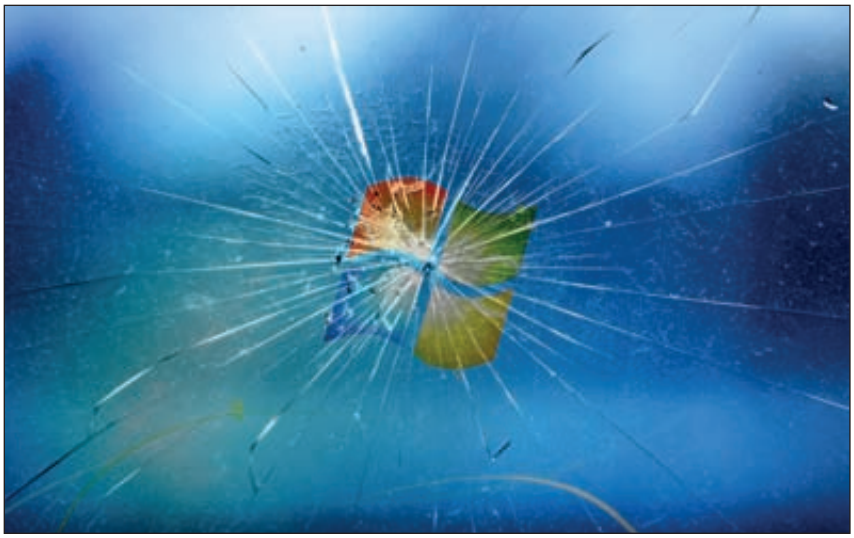
Требование 5. Защищать все системы от вредоносного ПО и регулярно обновлять антивирусное ПО

Большинство видов вредоносного программного обеспечения проникают в сеть через электронную почту сотрудников, сеть Интернет, съемные носители или мобильные устройства в результате использования системных уязвимостей.

5.1 Антивирусное программное обеспечение должно быть развернуто на всех системах, подверженных воздействию вирусов (особенно рабочих станциях и серверах).

5.1.1 Антивирусное программное обеспечение должно обеспечивать защиту от всех известных видов вредоносного программного обеспечения.

Более того, PCI DSS четко требует: *«Дополнительные решения для защиты от вредоносного ПО могут использоваться в качестве дополнения к антивирусному ПО; однако такие дополнительные решения не заменяют антивирусное ПО»*. Таким образом, никакие системы — в том числе действующие на основе контрольных сумм — не могут заменить антивирус. Вспомним, что в ранних версиях антивирусов также присутствовали утилиты, позволяющие следить за изменениями системы путем сравнения контрольных сумм. Но вот к настоящему моменту роль системы подсчета контрольных сумм файлов совершенно иная.



Дело в том, что современное вредоносное ПО (особенно предназначенное для заражения банкоматов, но об этом ниже) выпускается исключительно после тестирования на необнаружение актуальными системами защиты той целевой группы, на которую рассчитана атака. В результате начинается гонка «броня или снаряд»: быстрее антивирусная лаборатория получит новый тип вируса или быстрее пользователь, не соблюдающий требования по безопасности, занесет его в систему (о том, как вирусы попадают на банкоматы, тоже скажем ниже). В таких условиях всегда есть риск наличия в банкомате (да и в любом ином компьютере) вредоносного файла, пока не обнаруживаемого антивирусом. И контрольные суммы могут действовать только до ближайшего обновления — после запуска каждого обновления все файлы нужно перепроверять и суммы пересчитывать, ведь новости об обнаружении вредоносных файлов в поставляемом оборудовании не так редки, как хотелось бы... Кроме того, системы, действующие на основе контрольных сумм, исчезли из антивирусов, поскольку контроль над файлами не дает гарантии защиты от заражения. Первым звонком стало появление бестелесных или стелс-вирусов, сейчас наиболее опасные вредоносные программы делаются в виде руткитов — вредоносных программ, не видимых в зараженной системе и не обнаруживаемых при пофайловой проверке на наличие заражений.

Традиционным возражением против антивирусов являются их системные требования. Действительно, антивирусы требуют наличия оперативной памяти, но подавляющее количество банкоматов располагает 512 МБ, и Dr.Web ATM Shield — антивирусный продукт, специально разработанный для работы на встраиваемых устройствах, — отлично работает на таких конфигурациях. Естественно, остается вопрос, что делать для защиты устаревших систем, имеющих гораздо меньшее количество памяти. Чтобы на него ответить, нужно разобраться с тем, как вредоносные программы попадают на банкоматы и терминалы.

Если говорить о специализированных вредоносных программах для банкоматов, то они, как правило, попадают на устройство после его вскрытия с использованием универсального ключа. Но список вредоносных программ, обнаруживаемых на встраиваемых устройствах, не ограничивается только специализированными вредоносными программами. Чтобы в этом убедиться, не нужно обращаться к статистике антивирусных компаний — в сети Интернет достаточно фотографий банкоматов, зараженных «обычными» вредоносными программами. Если в банкоматах используется Windows XP, для которой до недавнего времени и разрабатывалось большинство вредоносных программ, отлично работающих на десктопах, то почему бы эти программы не установить на банкоматах? Пусть украсть деньги они не смогут, но зашифровать диск или вывести требование о выкупе — вполне. А это не просто «реклама» для владельцев банкомата в виде фотографий и возмущенных воплей, разлетающихся по Интернету, это еще и увеличение затрат на обслуживание устройств.

Вернемся к путям проникновения вирусов. Чаще всего обычные вредоносные программы попадают в банкомат со сменных носителей обслуживающего персонала — как правило, в связи с использованием этих сменных носителей для иных целей, кроме обслуживания встраиваемых устройств. В случае наличия доступа к встраиваемым системам из зараженной внутренней сети компании, через нее также происходит проникновение вредоносных программ. Возможно проникновение через уязвимости — в связи с отсутствием необходимых обновлений безопасности или неверной настройкой параметров выхода в Интернет. В качестве примера экзотического варианта проникновения можно назвать заражение с интернет-сайтов, посещаемых обслуживающим персоналом в период проведения регламентных работ.

Анализ путей заражения показывает, что антивирусная система защиты (в случае ее реализации на банкоматах) должна включать файловый монитор (проверка новых файлов, а также ранее проверенных на наличие неизвестных на момент проникновения угроз), проверку интернет-трафика (защита от посещения неразрешенных сайтов и ресурсов, а также от попадания вредоносных программ с разрешенных, но взломанных ресурсов), офисный контроль (защита от использования неразрешенных сменных носителей, система контроля за большинством участков, куда внедряются вредоносные программы), а также система проверки на руткиты — защита от уже активных угроз. В случае Dr.Web ATM Shield это соответственно SpIDer Guard, SpIDer Gate, Офисный

контроль и Антируткит — естественно, дополняемые системами обновления и управления, защищенными от возможного воздействия тех же вредоносных программ, а также действий обслуживающего персонала, желающего обойти ограничения защиты.

В случае недостаточного объема ресурсов на устройстве защита должна строиться по иному принципу. Естественно, придется забыть о запрете на использование неразрешенных сменных устройств — все, что не имеет системы самозащиты, использовать бессмысленно. Должны защищаться все компьютеры и устройства обслуживающего персонала, где — с разрешением или без него — персонал использует служебные сменные носители. Во-вторых, нужно ограничить доступ с устройств в Интернет в соответствии с Письмом Банка России от 24.03.2014 N 49-Т, требующим обеспечить защиту банкоматов, платежных терминалов. Необходимо заключить договоры с провайдерами доступа к Интернету, предусматривающие фильтрацию ими вредоносных программ. Ну и, естественно, необходимо периодически проверять устройства на наличие вирусов — например с помощью сетевой утилиты Dr.Web CureNet!

Выше уже говорилось о специализированных вредоносных программах, разработанных для заражения банкоматов. Отметим, что вирусами их называть некорректно: вирусов, т. е. программ, самостоятельно размножающихся и самостоятельно распространяющихся по сети, сейчас очень мало. Бал правят программы, распространяющиеся вследствие тех или иных действий пользователей, в основном — троянские. В качестве примера таких программ для банкоматов можно привести троянцев Trojan.Skimer.18 и Trojan.Plotus, Trojan.Plotus.2. В целях сохранения конфиденциальности разработчики банковского оборудования используют специальную технологию шифрования PIN-кода при его вводе пользователем. В открытом виде PIN-код не хранится ни на банковской карте, ни в банкомате, ни на серверах самого банка. Но троянцы семейства Trojan.Skimer обходят эту защиту, расшифровывая PIN-код с использованием программного обеспечения самого банкомата! Управление вредоносной программой осуществляется с помощью специальным образом подготовленных мастер-карт.

Подводя итог, можно констатировать: антивирусная защита банкоматов (и, тем самым, счетов клиентов банков от опустошения) — задача на сегодняшний день не только насущная, но и реализуемая, несмотря на активную деятельность киберпреступников. Банкомат по сути является лицом кредитной организации, по его работе судят о том, как организация относится к своим клиентам. Известно, что о любых недостатках люди сообщают куда большему количеству знакомых, чем о достоинствах — поэтому при недостаточном внимании к описанной проблеме нарабатываемая годами репутация банка может быть существенно подпорчена за считанные дни.