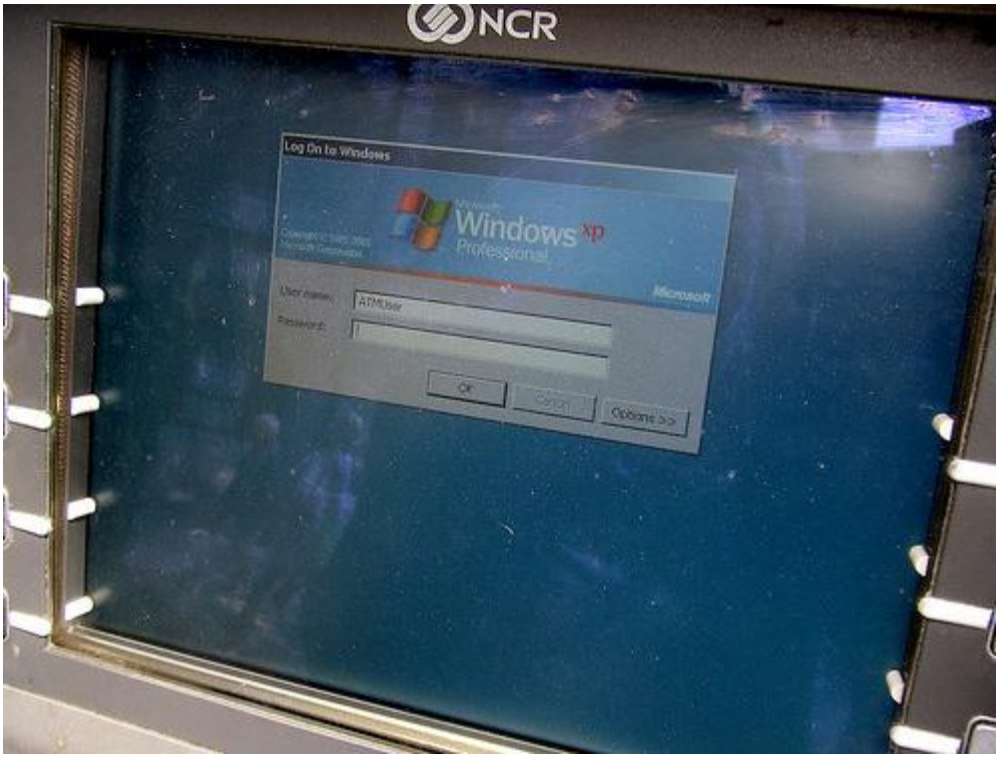
ЛЕКЦИЯ 11. УЯЗВИМОСТИ БАНКОВСКОЙ СИСТЕМЫ, ПЛАТЁЖНЫХ ТЕРМИНАЛОВ

Банкоматы и платежные терминалы быстро переходят на системы с элементной базой Intel, операционные системы на базе Microsoft Windows и используют протоколы TCP/IP. Все это серьезно увеличивает риски атак на данные устройства.

В погоне за чужими деньгами криминальная активность направлена по двух основным векторам. Первый из них - массовые персональные пользователи. Здесь активно применяются различные вредоносные программы, социальная инженерия, вымогательство и множество других видов интернет-мошенничества, включая популярные последнее время методы с использованием SMS-платежей.

Иногда под массовый застрел попадают крупные финансовые организации. Так, например, знаменитый червь Slammer заблокировал в 2003 году работу 13.000 банкоматов Bank of America, и всех банкоматов канадского Imperial Bank of Commerce. Ситуация повторилась с червем Welchia, когда также были поражены банкоматы Diebold нескольких коммерческих банков, работающих под управлением операционной системы Windows XP Embedded. Зараженные банкоматы начинали активно искать другие машины, в операционной системе которых имелась уязвимость RPC DCOM и в результате, Welchia сначала выводил из строя систему банковской защиты от внешних вторжений, а затем и вовсе отключал банкоматы.



«Как такое возможно, - спросите вы, - чтобы банкоматы заражались подобно простым домашним компьютерам?» Все дело в массовом переводе банкоматов с IBM OS/2 из-за окончания ее поддержки со стороны вендора на модифицированные версии Microsoft Windows. Это привело к тому, что банкоматы подобно обычным рабочим станциям или домашним компьютерам стали уязвимы перед вредоносными программами, использующими уязвимости базовых компонентов Windows.

В августе 2009 года европейское агентство по сетевой и информационной безопасности (ENISA) опубликовало отчет под названием «Преступления со взломом банкоматов: Обзор ситуации в Европе и методы предотвращения» (ATM crime - Overview of the European situation and golden rules on how to avoid it). В отчете обращается внимание

на растущее число преступлений со взломом банкоматов и приводятся средства защиты от них. С точки зрения ENISA наличие нескольких сторон, участвующих в эксплуатации сетей банкоматов, приводит к проблемам их коммуникации, в частности, по вопросам безопасности. Часто бывает сложно определить, кто именно ответственен за эту проблему.

Кроме этого после установки банкоматы редко обновляются и плохо управляются. В соответствии с требованиями регуляторов, в том числе «О защите персональных данных», обновления для операционной системы (в данном случае для модифицированных версий Microsoft Windows) сначала должны быть протестированы, сертифицированы, а только затем распространены, что создает дополнительные затруднения.

По данным из отчета компании VDC для директоров по информационным технологиям компаний, занимающихся розничной торговлей, в 43% от общего числа систем кассовых терминалов использовалась операционная система Microsoft Windows. В отчете по розничным сетям кассовых терминалов в Северной Америке, подготовленном IHL Group и выпущенном в марте 2008 года, 76 % всех новых кассовых терминалов были поставлены с предустановленной операционной системой Microsoft Windows, в 2007 г. этот показатель составлял 71%.

Быстрое увеличение доли Windows на рынке объясняется не только ростом количества банкоматов, но и заменой старых по причине несоответствия новым требованиям платежных систем Europay/Mastercard и Visa, в частности поддержке встроенных компьютерных чипов, а также требованиям законодательства развитых стран о равных возможностях для инвалидов.

В итоге кассовые терминалы и банкоматы из-за использования в них старых версий Microsoft Windows (как правило, это NT 4.0 и XP) становятся в один ряд с простыми персональными компьютерами для потенциальных атак злоумышленников.

11.1 Целевые атаки

Второй вектор атаки - это предприятия государственного и финансового сектора, которые непосредственно работают с денежными средствами или ликвидными на черном рынке персональными данными граждан. Главной мишенью здесь становятся банки. Где же, как не у них, можно быстро разжиться большими деньгами? Но массовые технологии на этом направлении не так эффективны, данные хорошо защищаются, есть служба безопасности, к тому же каждая организация по-своему уникальна, имеет свои бизнес-процессы и набор технологий защиты. Чтобы быть успешным на этом направлении киберпреступникам приходится осваивать «творческий подход», разрабатывать индивидуальные или, как принято говорить, целевые (таргетированные, от анг. targeted) атаки.

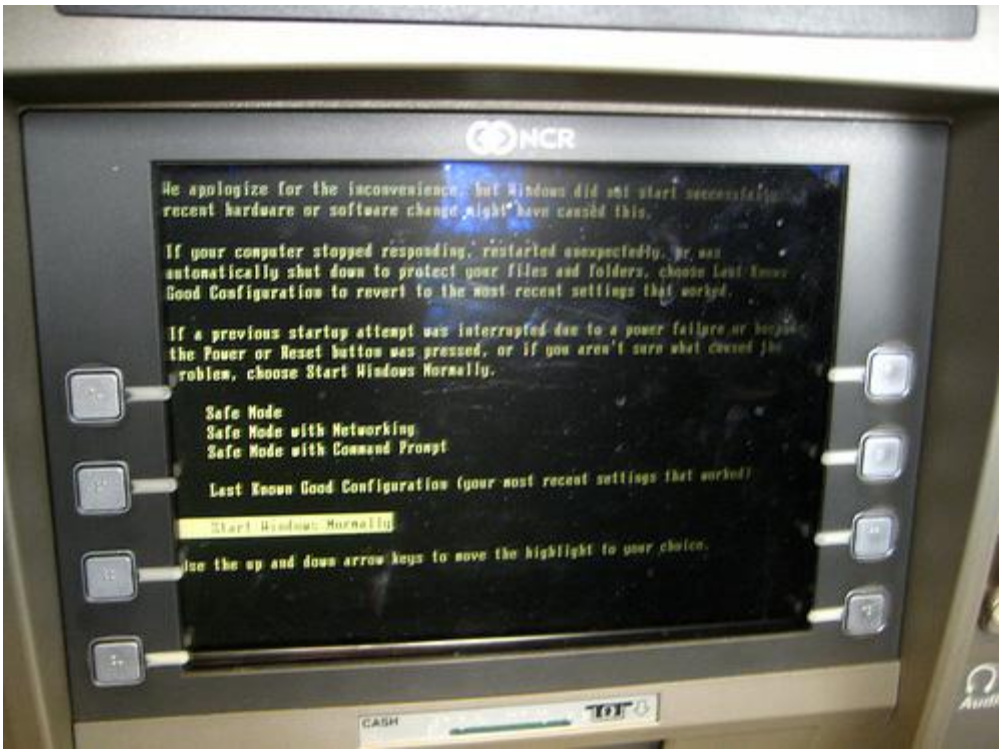
Часто атаки на информационные системы банков проводятся через халатно оставленные лазейки или элементарно непроработанной модели рисков. Это могут быть недокументированные сетевые подключения, открытые беспроводные сети, необновленное программное обеспечение, незаблокированное подключение внешних устройств, отсутствие регламента доступа к важной информации и т.п.

Несмотря на то, что переход от закрытых систем обработки транзакций к открытым предлагает ряд преимуществ (легкость в использовании, низкая стоимость установки и эксплуатации и т.д.), он создает множество уязвимых мест (это особенно касается автоматических терминалов), что повышает риск известных и неизвестных угроз.

Частые обновления и перезагрузки системы, которые необходимы для работы традиционных средств защиты от вредоносных программ в целях обеспечения непрерывной безопасности, просто неосуществимы в автоматических системах, таких как банкоматы и POS-терминалы.

Хорошим примером целевой атаки является взлом платежной системы RBS WorldPay в ноябре 2009 года, когда в банкоматах 280 городов мира за 15 минут была украдена сумма, приблизительно равная 9 млн. долл. США.

Но наиболее интересный случай был зафиксирован в марте 2009 года, когда специалисты антивирусных компаний Sophos, «Доктор Веб» и «Лаборатории Касперского» обнаружили троянскую программу (Troj/Skimer-A, Trojan.Skimer и Backdoor.Win32.Skimer.a соответственно), похищавшую информацию о владельцах банковских карт прямо в банкоматах под управлением Diebold Agilis.



Согласно опубликованной информации заражения банкоматов были зафиксированы в сетях Росбанка, Бинбанка и «Петрокоммерца». По данным самой компании Diebold, этот вирус был обнаружен в январе 2009 года, тогда же производитель внес необходимые изменения в ПО и предупредил банки-клиенты. Никто доподлинно не знает, когда именно были заражены банкоматы и сколько еще модификаций есть и будет у этого банковского трояна. Антивирусные аналитики склонны считать, что данная троянская программа активно развивается и дорабатывается злоумышленниками для дальнейшего использования.

Буквально через несколько месяцев, летом 2009 года, банковское сообщество и его

клиенты, снова была встревожена новостью об обнаруженной в банкоматах Восточной Европы троянской программе. Согласно исследованию аналитиков Trustwave, эти вредоносные приложения считывают данные магнитных полос банковских карт, а также PIN, и одновременно предоставляют преступникам удобный интерфейс управления и возможность распечатать украденную информацию посредством встроенного принтера для печати чеков.

Важно отметить, что заражение банкоматов и банковские трояны - не только региональная проблема. Угроза одинаково актуальна во всех странах мира, где используются платежные карты и установлены банкоматы.

В итоге 2009 год оказался черным для безопасности в банковской отрасли. Если раньше речь шла о том, что вирусы могли, в худшем случае, привести к некорректной работе банкоматов, то сегодня мы говорим о том, что атаки на банкоматы способны нанести ущерб клиентам банков. Разумеется, подобного рода инциденты крайне негативно сказываются на репутации банков, поэтому требования к качественным характеристикам банкоматов и их защите постоянно усиливаются.

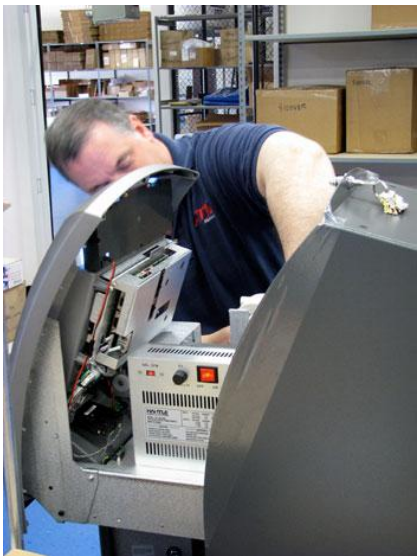
11.2. Инсайдерский след

Во всех описанных выше печальных историях не стоит исключать пресловутый человеческий фактор. Многие крупные кражи денежных средств и данных клиентов явно были бы невозможными без участия сообщников (инсайдеров) внутри самой атакуемой компании.

Представители Diebold прямо заявляли о том, что для того чтобы внедрить вредоносное ПО, мошенники должны были иметь физический доступ к «начинке» конкретного банкомата, и такого рода аспекты безопасности банкоматов, как ограничение доступа к ним, смена заводского пароля, установка видеокамер и т.д. находятся уже в компетенции банков.

В случае с банкоматами Diebold злоумышленники должны были знать, как работают банкоматы Diebold и их программное обеспечение Agilis Software на базе Microsoft Windows XP, иметь доступ к описанию API и другим техническим деталям.

Более того, для повышения вероятности успеха целевой атаки злоумышленникам неплохо было обладать информацией об установленных средствах защиты в банке-жертве и процессах обслуживания и обеспечения безопасности информационных систем. Без помощи инсайдера получить такую информацию сложно.



Не стоит думать, что всегда к краже денег причастны текущие сотрудники банка, продавшиеся злоумышленникам. Инсайдерами могут выступать бывшие сотрудники банка, прекрасно осведомленные о внутренних делах, или же сотрудники банка, используемые «втемную». Категория бывших сильно пополнилась в период глобального экономического кризиса, а халатных и некомпетентных в вопросах безопасности рядовых сотрудников будет много во все времена.

11.3. Проблемы с стандартом PCI DSS

Одним из требований индустриального стандарта безопасности для организаций, работающих с платежными карточками (PCI DSS Requirements and Security Assessment Procedures, v1.2, октябрь 2008), является «обеспечение защиты системы от существующих и развивающихся угроз, в частности, вредоносных программ».

Требования PCI DSS обязательны и вынуждают как финансовые, так и розничные организации стремительно переходить на новые операционные системы и программы для того, чтобы обеспечить выполнение требований стандартов, под угрозой штрафов со стороны компаний-эмитентов кредитных карт или со стороны федеральных или местных органов в случае утечки данных. Требование 7. Предоставление доступа к информации о владельцах карт строго с учетом производственной необходимости обязывает ввести системы контроля доступа, защищающие от непредумышленных ошибок или злонамеренных действий инсайдеров. Кроме того, Требование 10. Отслеживание и мониторинг всех операций доступа к данным сети и информации о владельцах карт направлено на максимальное снижение убытков от действий инсайдеров. Данное требование предусматривает ведение контрольного журнала по пользовательским и системным компонентам.

Было много написано о необходимости и эффективности стандарта PCI DSS и содержащихся в нем требованиях о том, чтобы все компании, занимающиеся обработкой платежей с использованием дебетовых и кредитовых карт, должны обеспечить защиту своих систем от "существующих и вероятных угроз атаки с применением вредоносного программного обеспечения". Очевидно одно, стандарт PCI DSS на практике ничего ровным счетом не гарантирует.

Пострадавшие Royal Bank of Scotland (RBS WorldPay) и Heartland Payment Services (жертва уже ставшего легендарным Альберта Гонсалеса) были PCI DSS Compliant и им это не помогло. Зараженные троянскими программами банковские системы были также сертифицированы по PCI DSS и им это не помогло.

Очевидно, что никакие стандарты все равно не помогут от целевых атак на конкретный банк. Точно также против целевых атак по определению бесполезны стандартные традиционные средства защиты. Понятно и то, что нужно использовать какой-то абсолютно иной подход к защите система обработки транзакций. О том, каким он может быть, я расскажу в следующей главе.

11.4. Системы обработки транзакций требуют особого подхода к защите

Последние годы корпоративные решения в области защиты от вредоносных программ принципиально оставались неизменными. Классический сигнатурное обнаружение дополнялось проактивными компонентами, такими как эвристика, эмуляция кода или поведенческий анализ. С учетом того, что в вирусные лаборатории вендоров ежедневно прибывают десятки тысяч новых образцов вредоносных программ, традиционные технологии не в состоянии обеспечить надежный уровень защиты для критически важных информационных систем, к каковым относятся банковские системы.

Во-первых, злоумышленники всегда могут оттестировать свои вредоносные программы на стандартных антивирусных средствах защиты, чтобы обеспечить успешное проникновение в систему. Во-вторых, специально написанные вредоносные программы из-за своей уникальности могу очень долго оставаться незамеченными в системе обработки транзакций, так как антивирусным вендорам просто неоткуда будет получить образец для анализа и обеспечения детекта.

Очевидно, что в таких условиях необходим иной подход к защите, полностью основанный на проактивной защите всех точек системы обработки транзакций не только от внешних, но и от внутренних угроз (установить вредоносные программы, похитить информацию или нарушить работу системы вполне может и кто-то из обслуживающего персонала). Это становится возможным только благодаря жесткому контролю над программным обеспечением в режиме реального времени, гарантирующему, что в работу разрешенных приложений не сможет вмешаться никто и ничто.

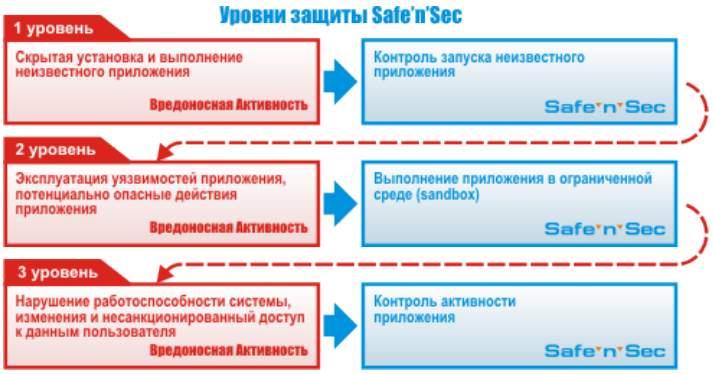
Только обеспечив безопасную работу приложений, можно гарантировать, что система будет непрерывно находиться в исправном состоянии, будет защищена от вмешательства в ее работу известных и новых вредоносных программ и не станет жертвой утечки данных - случайной или злонамеренно спровоцированной изнутри организации. Более того, решение должно предоставлять все эти возможности без необходимости непрерывного обновления, корректировки и перезагрузки для гарантии работоспособности защиты.

Решением в полной мере отражающим такой новый подход является, например, Safe'n'Sec TPSecure российской компании S.N.Safe&Software. Это решение во многом является уникальным на рынке и специально предназначено для защиты системы обработки транзакций, поэтому хотелось бы остановиться на нем подробнее.

11.5. Защита банкоматов и POS терминалов с помощью Safe'n'Sec TPSecure

Защита банкоматов с помощью Safe'n'Sec TPSecure осуществляется в соответствии с политиками контроля активности приложений. Продукт контролирует каждое действие в процессе работы системы, блокирует все подозрительные действия и разрешает исполняться только доверенным процессам из так называемого «белого» списка (списка доверенных процессов). Именно такой подход, пожалуй, наиболее эффективен для обеспечения защиты банкоматов и POS-терминалов, так как набор активных процессов в них очень стабилен. При установленном Safe'n'Sec TPSecure запуск неопознанных приложений невозможен до тех пор, пока пользователь с соответствующими правами не укажет степень доверия к этому приложению.

На самом деле Safe'n'Sec TPSecure - это не просто блокирование по белым спискам. Он основан на технологии V.I.P.O. (Valid Inside Permitted Operations), которая объединяет в себе адаптивное профилирование, выполнение приложений в защищенной среде (sandbox - «песочница») и подсистему поведенческого анализа.



Технология V.I.P.O. основана на перехвате вызовов системных функций на уровне ядра операционной системы (Ring 0) и загружается раньше всех остальных приложений. Она позволяет идентифицировать, анализировать и, при необходимости, блокировать доступ к файловой системе, объектам системного реестра, к запуску приложений и к другим операциям, способным воздействовать на целостность защищаемых приложений. Таким образом, технология V.I.P.O. создает защиту ядра операционной системы для предотвращения запуска любого нежелательного кода.

После установки Safe'n'Sec TPSecure и его первоначальной настройки оперативное администрирование больше не потребуется, так как решение не нуждается в постоянном обновлении. Safe'n'Sec TPSecure будет полностью автоматически блокировать все несанкционированные действия, поскольку для восстановления оборудования и возобновления его работы не потребуется перезагрузка системы.

Выполнения несанкционированного кода, пытающегося внедриться в операционную систему, предотвращается при помощи изолированной виртуальной среды - «песочницы». В ней код может выполняться безопасно для вычислительной системы, не воздействуя на другие ее части. На практике это означает, что вредоносная программа не может получить доступ к операционной системе, разрешенным приложениям или буферу обмена данными для внедрения перехватчиков, клавиатурных шпионов и других нежелательных программ. Это также означает невозможность изменить код и данные, принадлежащие другим процессам, а также несанкционированно модифицировать исполняемые файлы.

Функциональные возможности Safe'n'Sec TPSecure:

- Блокировка любой возможности несанкционированного подключения и внедрения всякого рода ПО со стороны обслуживающего банкоматы персонала.
- Защита доступа к критически важным данным (владельцы карт, PIN-коды, пароли).
- Контроль всех событий в сети, событий в банкоматах и генерирует консолидированный аналитический отчет с широкими возможностями фильтрации с целью ретроспективного анализа и расследования конкретного инцидента вторжения вредоносного кода.
- Мобильная консоль централизованного управления (позволяет существенно снизить временные затраты на развертывание системы безопасности).
- Автономная работы (без связи с сервером управления).

Важно отметить, что настройка Safe'n'Sec TPSecure осуществляется специалистами S.N. Safe&Software под запросы и нужды конкретного заказчика. При этом общая стоимость владения комплексным продуктом остается для клиентов на уровне стандартных продуктов.

11.6. Сравнение решений для защиты банкоматов

В принципе для защиты работающих на базе Microsoft Windows банкоматов могут использоваться любые совместимые продукты, предназначенные для защиты конечных точек корпоративной сети. Однако в силу описанных в предыдущих главах причин они, все-таки, должны быть специальными.

Ограничимся сравнением следующие продукты:

- McAfee SolidCore Kiosk and ATM Security & Control (SolidCore);
- Safe'n'Sec TPSecure (S.N. Safe&Software) - обзор продукта;
- Symantec EndPoint Protection - обзор продукта.

Эти продукты могут использоваться для защиты различных банкоматов, включая следующие модели:

• Diebold ATMs: Opteva 500, Opteva 510, Opteva 720 (Windows XP, Agilis® Software, DORS) ;

• NCR ATMs: NCR 5674, NCR 5675, NCR 5877, NCR Self Service 32 (Windows NT, Windows XP, software: S4I; Aptra Advance NDC; Aptra Active XFS; Aptra Advance);

• Smart Card Service terminals: ITT 522, ITT 522.18, ITT 550;

• Wincor Nixdorf ATMs: ProCash Compact, ProCash 1500, ProCash 1500xe (Microsoft Windows NT 4.0, Microsoft Windows XP, software: NDC, DDC, ProChip/EMV).

	Safe'n'Sec TPSecure	McAfee SolidCore	Symantec EndPoint Protection
Классическая сигнатурная и проактивная защита	Опционально, движки VBA32, Dr.Web, BitDefender*	Опционально, собственный движок McAfee	Собственный движок Symantec
Белые списки приложений (whitelisting)	+	+	+
Контроль доступа приложений к данным	+	+	+
Защищенная виртуальная среда для недоверенных приложений (sandbox)	+	-	-
Ограничение доступа к устройствам и данным	Политики доступа на уровне ПО или устройств (ID, производитель, тип и т.д)	Политики доступа на уровне ОС и файлов	Политики доступа на уровне ПО или устройств (ID, производитель, тип и т.д)
Контроль целостности приложений	+	+	+ System Lockdown
Совместимость с банковским ПО	+	+	+
Отсутствие необходимости постоянного обновления модулей или антивирусных баз	+	+ Кроме случая опционального использования антивирусного движка	+ Кроме антивирусного движка
Интеграция с банковскими системами обновления ПО	+	+	+

Поддержка различных механизмов обновления банковского ПО, замены устройств банкоматов и самой защиты	+	+	+
Специфика продукта	Специализированное решение, большие возможности кастомизация, модульная архитектура, возможность установки доп. модуля DLP Guard	Специализированное решение, есть возможности кастомизации, несколько вариантов поставки	Универсальное решение, простое внедрение и высокий уровень совместимости

* - классический антивирусный движок используется только один раз перед установкой самого Safe'n'Sec TPSecure.

Как видно из таблицы выше, выбранные три продукта не так сильно отличаются технологически, как по своей идеологии. Все три продукта поддерживают белые списки приложений и имеют возможности ограничения доступа к данным и контроля целостности приложений. Однако, Symantec EndPoint Protection - для многих известный и привычный продукт для защиты корпоративных рабочих станций.

С другой стороны, подробно рассматриваемый нами выше Safe'n'Sec TPSecure и McAfee SolidCore созданы специально для защиты банкоматов. Safe'n'Sec TPSecure имеет в своем арсенале дополнительный уровень защиты в виде защищенной виртуальной среды.

11.7. Вирус, ворующий данные банковских карт через платежные терминалы

«Лаборатория Касперского» обнаружила нетипичную модификацию вируса-троянца Neutrino, который атакует POS-терминалы для кражи данных банковских карт.

Neutrino известен уже давно, и он не раз менял свои функции и методы распространения. На этот раз троянец охотится за данными банковских карт, которые проходят через зараженные платежные терминалы.

В зону интересов Neutrino попали Россия, Алжир, Казахстан, Украина и Египет. Neutrino не сразу приступает к сбору информации. Попав в операционную систему POS-терминала, вирус некоторое время выжидает для обхода защитных технологий.