Виртуализация рыцарей плаща и кинжала, или Промышленный шпионаж в XXI веке

Промышленный шпионаж как явление существует уже тысячи лет. Мелкие ремесленники, крупные компании и даже целые государства на протяжении веков шпионили друг за другом, дабы получить определенные преимущества, конкурентные, политические и т.д. При этом неизменным условием являлось наличие инсайдера – подкупленного или специально внедренного человека, который, находясь внутри системы, добывал всю необходимую информацию. Однако развитие современных технологий позволило не только превратить в реальность "шпионские штучки" Джеймса Бонда, значительно облегчившие работу агента, но и заменить его самого компьютерной программой. Тем самым были снижены риски для человека, а в некоторых случаях и повышена эффективность проводимых операций.

Как добывались секреты

Прежде чем говорить об актуальных методах промышленного шпионажа, сделаем небольшой экскурс в недалекое прошлое. Когда большинство людей слышит об угрозах информационной безопасности, в голове первым делом возникает образ хакеров. Это стереотип. Однако просто так стереотип не рождается. В 90-х годах прошлого века именно внешние угрозы, хакеры и вирусы считались основным источником опасности для информационных ресурсов компаний. Именно от них компании и защищались, выстраивая неприступные бастионы по периметру своей корпоративной сети. Увлекшись строительством эдаких современных "линий Мажино", специалисты пропустили рост угрозы... с обратной стороны периметра.

Между тем, именно инсайдеры, собственные сотрудники компаний с легальным доступом к конфиденциальным данным стали наиболее серьезной угрозой безопасности. Если хакеру необходимо сначала проникнуть за серьезно укрепленный контур корпоративной сети, чтобы найти интересующие его сведения, инсайдеры уже знают, где какая информация хранится, и в большинстве случаев имеют к ней доступ. Соответственно, задача инсайдера сводится к тому, чтобы найти способ вынести данные. Для этого сотрудники располагают многочисленными каналами связи с высокой пропускной способностью, как то Интернет, электронная почта, программы обмена мгновенными сообщениями. А миниатюризация и увеличение емкости мобильных накопителей предоставили еще один способ копирования больших объемов информации.

"В современных компаниях, использующих высокотехнологичные решения, чрезвычайно трудно однозначно определить границы корпоративной сети, – замечает Тарас Пономарёв, партнер консалтингового бюро "Практика Безопасности". – Развитие беспроводных технологий, облачных вычислений, широкое применение мобильных устройств и накопителей не позволяет возвести барьер между сотрудниками компании и внешних миром, исключив таким образом возможность утечки данных".

Тенденцию подтверждает и недавнее исследование Cisco, проведенное в августе-сентябре 2010 года, согласно которому 60 % респондентов считают, что пребывание в офисе не является залогом продуктивной работы. Однако чтобы сотрудник был эффективным вне офиса, он не должен быть изолирован от корпоративной инфраструктуры. Ему по-прежнему нужен доступ к информации, в том числе и конфиденциальной. Но в таком случае получается, что информация, попавшая на ноутбук удаленного сотрудника, покидает защищенные границы организации в привычном понимании.

Примеров использования инсайдеров для промышленного шпионажа немало. Можно вспомнить громкую историю 2006 года, когда компания Lockheed Martin обвинила в краже секретных сведений своего конкурента, компанию L-3 Communications. Переданные тремя сотрудниками Lockheed Martin сведения должны были помочь L-3 Communications выиграть контракт Пентагона на 1 млрд долларов! Неудивительно, что когда речь идет о таких поистине астрономических суммах, сравнимых с ВВП Фарерских островов, в ход идут все средства.

Что день грядущий нам готовит

Судьба раскрытого агента во все времена могла быть весьма печальной. Даже сегодня, в относительно цивилизованное время, шпиона, в зависимости от тяжести содеянного, могут ожидать крупные штрафы, тюремное заключение или депортация из страны. Поэтому закономерно желание заменить человека на таком опасном участке работы. Бестелесная програм-

Таблица. География распространения червя Stuxnet

Иран	Индонезия	Индия	Пакистан	Узбекистан	Россия	Казахстан	Беларусь
52,2%	17,4%	11,3%	3,6%	2,6%	2,1%	1,3%	1,1%
Киргизстан	**Азербайджан**	**США**	**Куба**	**Таджикистан**	**Афганистан**	**Остальные страны**	
1,0%	0,7%	0,6%	0,6%	0,5%	0,3%	4,6%	

Источник: ESET, октябрь 2010

ма, которая не боится экзекуций и значительно менее заметна, как нельзя лучше подходит на эту роль. Тем не менее, громких инцидентов с использованием программ-шпионов до недавнего времени было немного. Однако история с червем Stuxnet вновь сделала вопрос о программном шпионаже актуальным. Напомним ход событий. Летом 2010 года одна за другой антивирусные компании рапортовали об обнаружении крайне интересного экземпляра вредоносной программы, названного Stuxnet. Первоначальный интерес к Stuxnet объяснялся тем, что червь использовал неизвестную ранее Windows-уязвимость в обработке LNK/PIF-файлов. Однако при ближайшем рассмотрении троян оказался гораздо более хитроумной программой, нежели большинство из тех, что ежедневно попадают из Интернета к вирусным аналитикам.

Прежде всего, Stuxnet не предназначается для широкого круга пользователей. Его целью являются SCADA-системы Siemens, используемые на крупных промышленных объектах. Кроме того, для проникновения на компьютеры Stuxnet использует сразу 5 неизвестных ранее уязвимостей "нулевого дня". По оценкам специалистов антивирусной компании ESET, стоимость подобных уязвимостей на черном рынке может оставлять более 100 тыс. евро. Наконец, Stuxnet оказался способным обходить многие реализации технологии защиты от внешних воздействий HIPS (Host Intrusion Prevention System). Такая способность у вредоносного ПО появилась благодаря тому, что отдельные модули Stuxnet были подписаны легальными цифровыми сертификатами уважаемых компаний Realtek и JMicron. Скомпрометированные сертификаты были отозваны компаниями лишь тогда, когда история Stuxnet получила широкую огласку. "Мы впервые столкнулись со столь хорошо спроектированной и продуманной до мелочей вредоносной программой, – комментирует ситуацию Александр Матросов, руководитель Центра вирусных исследований и аналитики российского представительства ESET. – Каждый нюанс работы Stuxnet преследует определенную цель. Червь располагает механизмами контроля количества заражений и самоликвидации. Атаки с использованием столь сложного программного обеспечения готовятся длительное время. Я не сомневаюсь, что Stuxnet имеет целевую направленность".

По мнению экспертов, Stuxnet разработан группой высококвалифицированных специалистов, которые хорошо ориентируются в слабых местах современных средств информационной безопасности. Червь создан таким образом, чтобы оставаться незамеченным как можно дольше. Первые версии Stuxnet могли распространяться лишь через обычные USB-флэшки, вирус не мог использовать Интернет для проникновения в другие компьютеры. На первый взгляд, это может показаться странным. Однако суть в том, что червю, в отличие от большинства современных вирусов, не нужно было охватывать максимальное число пользователей, а отсутствие возможности распространяться по сети снижало его заметность. Распространяясь с помощью USB-накопителей, Stuxnet скрытно проникает в защищенные промышленные сети, проверяет наличие сетевого соединения и только после этого начинает передачу найденной информации.

Куда целил Stuxnet

Наиболее распространенная версия о назначении Stuxnet заключается в том, что червь должен был атаковать иракскую атомную станцию в Бушере. Статистические данные (таблица) являются косвенным фактом, подтверждающим эту гипотезу. Большинство других выводов также строится на довольно логичных, но все же предположениях. "Несмотря на большое количество заражений в Иране, мы не можем делать однозначных выводов о том, что целью злоумышленников была Бушерская АЭС, – говорит Александр Матросов. – Мы можем утверждать лишь то, что стоимость этой атаки очень велика, а для обычных киберпреступников не видно мотивов ее осуществления. Вполне вероятно, что за атакой может стоять какая-нибудь влиятельная организация".

Итак, вполне вероятно, что за атакой стоит какая-то влиятельная организация. Или даже государство. По крайней мере, так считают официальные лица Ирана. По мнению чиновников, Stuxnet – это хорошо спланированная акция Западного мира, направленная против страны с целью сорвать программу "мирного атома". Имеются подтверждения, что некоторые компьютеры Бушерской АЭС действительно были заражены червем, однако эти компьютеры не относились к числу тех, что задействованы в процессе управления реактором или контроля параметров оборудования.

То есть, в сеть АЭС вирус все-таки проник. Каким образом? Во-первых, его мог принести кто-то из сотрудников преднамеренно. Тогда более вероятно, что речь идет об атаке на АЭС. В то же время существует вероятность, что червь был подсажен случайно. К тому

же функционал Stuxnet не является очевидным даже для аналитиков, разобравших программу "по косточкам". Дело в том, что Stuxnet обладает возможностью дозагружать дополнительные модули и тем самым расширять свои возможности.

Вместо заключения

Благодаря узкой направленности, способности скрываться и большому количеству используемых уязвимостей для проникновения Stuxnet уже вошел в историю компьютерных вирусов. Однако для нас он интересен тем, что имеет выраженную направленность на осуществление шпионажа. Причем шпионажа промышленного, явления гораздо более серьезного, чем подглядывание паролей от аккаунтов в социальных сетях или даже кража данных кредитных карт.

Наблюдаем ли мы возврат вектора угроз в сторону внешних атак в корпоративной среде? Говорить об этом пока сложно. Интересно посмотреть, как будут развиваться события. К сожалению, сегодня нет предпосылок к тому, чтобы ситуация принципиально изменилась. Производители программного обеспечения, в том числе и для крупных промышленных объектов и критически важной инфраструктуры, не могут исключить уязвимостей в своих продуктах. А потому покуда никуда не деться от всевозможных антивирусов, сканеров и экранов.

Владимир Ульянов

НОВОСТИ

Инновации Oracle представлены в России

Российское представительство Oracle объявило ключевые направления инновационного развития и анонсировало глобальные премьеры продуктов корпорации. Стратегия корпорации по обеспечению клиентам доступа к технологиям последнего поколения и лучшим в своих классах продуктам позволила Oracle сформировать наиболее полный стек программного и аппаратного обеспечения корпоративного класса. В зависимости от потребностей клиенты могут выбрать полную систему или приобрести у Oracle компоненты и интегрировать их самостоятельно. Открытая архитектура Oracle обеспечивает выбор продуктов, выбор среды, а также выбор вариантов внедрения.

Продукты Oracle объединяет совместная разработка, совместное тестирование, совместная сертификация, совместная поставка, совместное развертывание, совместное обновление, единое управление и единая поддержка. Причем инновационные разработки охватывают все продуктовые направления корпорации.

Мировые премьеры в России

Самым громким глобальным анонсом стала Oracle Exalogic Elastic Cloud, первая в мире интегрированная машина связующего программного обеспечения (middleware machine), разработанная, протестированная и настроенная Oracle для выполнения приложений, написанных на Java и других языках, с высочайшей производительностью. Эта машина предоставляет полнофункциональную инфраструктуру "облачных" вычислений, отвечающую самым жестким требованиям к уровню обслуживания. Новая разработка может поддерживать тысячи приложений с разными требованиями к безопасности, надежности и производительности, что делает эту машину идеальной платформой для консолидации ресурсов центра обработки данных в масштабе предприятия.

Флагманской разработкой в области СУБД и инфраструктуры является новейшая конфигурация машины баз данных Oracle Exadata Database Machine X2-8, наиболее успешного нового продуктового направления Oracle. Поддерживая Oracle Database 11g, Oracle Real Application Clusters, Oracle Enterprise Manager и Oracle Exadata Storage Software, машина Oracle Exadata Database Machine X2-8 предоставляет программное обеспечение, серверы, устройства хранения данных и сетевую инфраструктуру для любых требований к базе данных.

Развитие технологического наследства Sun

Oracle увеличивает инвестиции в операционную систему Oracle Solaris и выпускает ОС Solaris 11 Express, начиная подготовку к запланированному на 2011 год выпуску Oracle Solaris 11. Согласно плану в новую ОС будут включены результаты более чем 2700 проектов, насчитывающих более 400 инновационных разработок. Эта операционная система станет результатом более 20 миллионов человеко-часов разработки.

Oracle расширяет инвестиции в платформу JavaFX и поддержку сообществ разработчиков Java и Open Source. Планы дальнейшего развития JavaFX включают усовершенствованные графические возможности, воспроизведение высококачественных мультимедиа и отображение HTML-контента в Java-приложениях; планы развития JDK реализуются в целях совершенствования платформы Java SE.

Новинки аппаратных систем

Первый в отрасли 16-ядерный серверный процессор и новые системы семейства SPARC T3 определяют направление инноваций. Представленная линейка включает системы от одно-процессорного 16-ядерного блейд-сервера и до 4-процессорного 64-ядерного сервера в компактном корпусе высотой 5U, способного одновременно обрабатывать 512 вычислительных потоков.

Два новых тонких клиента Sun Ray 3 Client и Sun Ray 3i Client специально созданы для повышения уровня безопасности, максимального удобства доступа сотрудников, а также снижения затрат на техническое обслуживание, обновление и администрирование по сравнению с традиционными рабочими местами на базе ПК.

Настоящее и будущее бизнес-приложений

Бизнес-приложения нового поколения Oracle Fusion Applications пополнят ассортимент существующих приложений компании, развитие, выпуск новых версий и поддержку которых Oracle неуклонно продолжает.

Нововведения Oracle CRM On Demand Release 18 включают возможности привлечения перспективных клиентов с меньшими издержками, улучшения бизнес-планирования независимо от рыночной конъюнктуры, безопасность среды "облачных" вычислений корпоративного класса, контроль сетевой активности и доступа.

Новая версия Primavera P6 Enterprise Project Portfolio Management 8 является на 100 % web-ориентированным решением для управления проектными портфелями и предоставляет крупным предприятиям платформу для организации управления и контроля, которая поддерживает процесс принятия решений по стратегическому корпоративному портфелю проектов.