Введение

На страницах журнала «Автоматизация в промышленности» регулярно обсуждаются разнообразные темы, связанные с созданием и применением контрольно-измерительных приборов и аппаратуры, специализированного промышленного ПО, протоколов передачи данных. Эти компоненты промышленной автоматизации присутствуют на всех без исключения промышленных объектах, поэтому данные вопросы актуальны и понятны инженерам в не зависимости от отрасли промышленности.

В настоящее время в связи с активным развитием различных классов ПО, использованием Internet и беспроводной связи при автоматизации промышленных предприятий значительное внимание уделяется сервисным функциям, позволяющим получать оперативную информацию не только в диспетчерской, но и в любой точке предприятия, страны и даже мира. Такой подход добавляет удобство менеджменту, устраняет пространственные ограничения и делает управление предприятием более гибким и оперативным. Но при этом появляются и новые проблемы, о которых ранее не приходилось задумываться. К таким проблемам в первую очередь относится кибербезопасность. Серьезность кибератак сообщество промышленной автоматизации впервые ощутило в 2010 г. в результате активизации вируса Stuxnet. Но жизнь не стоит на месте. Год от года совершенствуются технологии создания программного кода, появляется инновационное полезное для общества ПО, расширяется его функционал. Но при этом не дремлют и создатели небезопасных «игрушек». И здесь очень уместно всем известное выражение: «Предупрежден, значит вооружен». И промышленным предприятиям необходимо понимать всю серьезность ситуации, возможные пути атаки на промышленные системы, а также способы защиты средств и систем автоматизации от злоумышленников.

Предлагаем вниманию читателям подборку материалов, подготовленных специалистами отечественных фирм, работающих в области информационной безопасности. В представленных статьях описана существующая ситуация по промышленной информационной безопасности, затронуты правовые аспекты, показаны пути проникновения боевого кода в системы автоматизации, рассмотрены механизмы, позволяющие предотвратить кибератаки.

Редакции известно, что западные и отечественные разработчики средств и систем автоматизации также озабочены проблемой информационной безопасности. Многие из них уже наладили взаимодействие с разработчиками средств защиты от кибератак. Надеемся, что в следующих выпусках по данной проблематике будут присутствовать также сообщения от вендоров о результатах подобного сотрудничества.

Таргетированные атаки на промышленный сектор: новое оружие в кибервойне

А.С. Арефьев (Компания InfoWatch)

Анализируется понятие таргетированной атаки и механизмы их проникновения в промышленную систему. Предлагаются методики выявления таргетированных атак, рассматриваются их преимущества и недостатки.

Ключевые слова: таргетированные атаки, промышленный сектор, сигнатурный анализ, эвристический анализ, фаерволлы, белый список, технология динамического обнаружения атак.

После откровений бывшего сотрудника АНБ Эдварда Сноудена не остается сомнений в том, что на сегодняшний день «гонка вооружений», если не сказать «война», ведется в киберпространстве. Очевидно, что безопасность и контроль критически важных объектов имеет стратегическое значение для государства, поэтому одним из главных средств ведения кибервойн являются атаки на промышленные предприятия.

Целенаправленные (или таргетированные) атаки впервые стали предметом активных дискуссий мирового сообщества еще в 2009 г. Тогда стало известно об атаке Stuxnet, основной целью которой было сдерживание иранской ядерной программы. Насколько известно, суверенное государство контролировало обогатительные ядерные центрифуги, и ряд объектов при этом был переведен во внештатный режим. Центрифуги быстро выходили из строя, их ремонт требовал времени и денег, поэтому обогащение урана откладывалось. Как удалось выяснить, данная атака была спланирована заранее, осуществлялась и проводилась в течение длительного времени.

Можно сказать, что с нее и началась новейшая история целенаправленных кибератак.

Что такое таргетированные атаки?

Таргетированные (или целенаправленные) атаки — это заранее спланированные действия против конкретной государственной или негосударственной структуры либо организации. Как правило киберпреступники, занимающиеся таргетированными атаками, — это профессионалы.

Даже сама деятельность хакеров сегодня обладает всеми чертами традиционного бизнеса. На российском рынке существует своеобразный «черный рынок» — теневые схемы и места реализации программных средств, необходимых для атаки на ИТ-инфраструктуру той или иной компании. По данным независимых исследований, число утилит, которые

применяются для построения ботнетов, возросло за последние годы в десятки раз.

Можно говорить о том, что современная индустрия ботнетов обладает всеми признаками полноценных коммерческих продуктов. Существуют сформированные «продуктовые линейки», злоумышленники расширяют воронку продаж, готовят отдельные модификации решений с учетом различных целевых сегментов, анонсируют новые версии «продуктов». В Internet легко найти фиксированные расценки на ботнеты, можно даже приобрести услугу целенаправленной атаки как сервис.

За последние годы характер атак значительным образом изменился — они весьма усложнились и часто имеют разветвленную, многоступенчатую структуру. Атака может начинаться на компьютере секретаря, а конечной целью при этом будет установка вредоносного ПО на компьютере бухгалтера.

Перед началом атаки злоумышленники тщательно изучают систему защиты предприятия, чтобы затем обойти ее и незаметно внедриться в ИТ-инфраструктуру. Для сокрыти атаки и невозможности предотвратить ее на ранней стадии, то есть до того, как злоумышленники достигнут своей цели, вредоносное ПО работает максимально незаметно, маскируя свою деятельность под легитимные процессы информационной системы предприятия.

В качестве промежуточного итога можно отметить, что если видимых признаков атаки на ИТ-инфраструктуру компании не наблюдается, это еще не означает, что ее не атакуют.

Механизм таргетированных атак

Вредоносное ПО представляет собой программу, которая позволяет получить несанкционированный доступ к конфиденциальной информации при помощи уязвимостей. Применяются подобные программы обычно для получения первичного доступа к сети предприятия. Как утверждает ряд открытых источников, для внедрения троянской вирусной программы «точкой входа» часто становится инсайдерская деятельность нелояльных сотрудников компании. Как правило, внедрение вредоносной программы означает ее допуск к данным при перезагрузке системы. «Пропиской» исполняемого модуля при этом каждый раз является его перезапуск.

Вредоносное ПО может попасть на компьютер сотрудника компании не только по злому умыслу последнего, но и вследствие применяемой хакерами социальной инженерии (например, киберпреступник может попросить жертву перейти по той или иной ссылке или посетить сторонний ресурс).

В результате жертва становится открытой для атаки, и злоумышленники получают доступ к операционной системе рабочего компьютера сотрудника. Теперь можно запустить вредоносные файлы, чтобы в дальнейшем получить контроль над компьютерами организации. Как уже говорилось, вредоносные файлы часто разрабатываются специально для атаки конкретной компании, поэтому имеющиеся средства защиты не способны им противодействовать. Хакеры используют так называемую «уязвимость нулевого дня».

Какие данные чаще всего похищают?

Во многом это зависит от профиля деятельности компании. Целью хакеров могут быть промышленные секреты и стратегические разработки закрытого плана, контроль над определенными промышленными объектами. Любопытно, что, согласно исследованиям Аналитического центра InfoWatch, 63% опрошенных понимают, что таргетированная атака на их предприятие — всего лишь вопрос времени.

Методики выявления таргетированных атак

1. *Сигнатурный анализ.*

Проведение сигнатурного анализа подразумевает, что у аналитиков есть какой-либо файл, пораженный вирусом. Изучение такой вредоносной программы позволяет снять с нее сигнатуру (цифровой отпечаток). После того, как сигнатура занесена в базу, можно проверять файлы на предмет заражения этим вирусом, просто сравнивая сигнатуры. Преимущество сигнатурного анализа в том, что он позволяет точно диагностировать атаку. Если имеется файл с совпадающей сигнатурой, то можно смело говорить о том, что компьютер поражен.

Сигнатурный анализ обладает рядом преимуществ:

- он может быть использован не только для сканирования вирусов, но и для фильтрации системного трафика;
- позволяет контролировать наличие тех или иных непроверенных сигнатур на шлюзе;
- позволяет с большой точностью осуществлять диагностические комплексы мер по противодействию атакам.

Существенным недостатком сигнатурного анализа является необходимость обновления сигнатурной базы. Большинство компаний вынуждено обновлять сигнатурную базу каждые 15 мин. При этом каждые полчаса в мире появляется новый вирус. Пока он не будет зарегистрирован, изучен и занесен в базу разработчиками антивирусов, компания беззащитна перед новой угрозой.

2. *Эвристический анализ*

Другой метод изучения уже выявленного ранее вредоносного ПО — это эвристический анализ. Функция эвристического анализа заключается в проверке исполняемого кода на наличие подозрительной активности, характерной для деятельности вирусов. Подобная методика хороша тем, что не зависит от актуальности каких-либо баз. Однако и у эвристического анализа есть свои минусы.

Ввиду того, что все основные антивирусы известны и доступны для использования всем желающим, хакеры могут производить тестирование написанного ПО и видоизменять его до тех пор, пока он не будет обходить все известные средства антивирусной защи-

ты. Тем самым эффективность основных эвристических алгоритмов сводится на нет.

3. *Фаерволлы*

Следующий метод обнаружения целенаправленных атак подразумевает использование так называемых фаерволлов нового поколения, которые в дополнение к традиционным возможностям также позволяют фильтровать трафик. Основным недостатком фаерволлов является чрезмерная «подозрительность» — они генерируют большое число ложноположительных срабатываний, в массе которых может затеряться то самое предупреждение об атаке. Кроме того, фаерволлы используют технологии, которые можно обмануть («песочница», эвристический анализ и сигнатурный анализ).

4. *Белый список*

Существует также иной метод защиты, применяемый для запуска приложений. Идея его весьма проста: станция может запустить только отдельные приложения (это носит название White Listening). Минус в том, что такой «белый список» должен содержать все без исключения приложения, которые могут понадобиться пользователю. На практике такой способ, конечно, довольно надежен, но очень неудобен, так как замедляет рабочие процессы.

5. *Технология динамического обнаружения атак*

Наконец, есть недавно разработанная технология динамического обнаружения атак, которая используется в продукте InfoWatch Targeted Attack Detector. Данная технология базируется на том, что действия злоумышленников неизбежно приводят к модификации ИТ-систем предприятия. Поэтому решение InfoWatch периодически сканирует ИТ-систему организации, собирая информацию о состоянии критических объектов. Полученные данные сравниваются с результатами прошлых сканирований, затем осуществляется интеллектуальный анализ произошедших изменений на предмет наличия аномалий. При обнаружении неизвестного вредоносного ПО к анализу его действий и возможного вреда для инфраструктуры предприятия привлекается аналитик InfoWatch.

Фактически выявление аномалий является первичным признаком того, что компанию атакуют. При этом в атаке не обязательно должен быть задействован вирус уровня Stuxnet. Как показывает практика, достаточно небольшого трояна, периодически пересылаемого дальше, чтобы злоумышленники достигли своей цели.

В заключение хотелось бы подчеркнуть, что организации должны своевременно отвечать на новые вызовы. Таргетированные атаки представляют собой хотя и сравнительно новую, но весьма серьезную угрозу, поэтому противостоять подобным типам киберпреступлений необходимо планомерно и тщательно, выстраивая в организации продуманную и надежную систему обороны.

Арефьев Андрей Сергеевич *— менеджер по развитию продуктов компании InfoWatch.*
Контактный телефон (495) 229-00-22.
Http://www.infowatch.ru

Разработка эксплойтов для АСУТП: двойная игра

Д.С. Евдокимов (Исследовательский центр Digital Security)

Приведен анализ уровня защищенности ПО для АСУТП. Предложены механизмы защиты ПО данного класса. Рассмотрены варианты проникновения вредоносного кода в АСУТП. Отмечается, что в условиях иерархической организации современных АСУТП компрометация одного из уровней неизбежно ведет к компрометации соседних уровней, а атаки возможны во всех направлениях вплоть до уровня управления производством.

Ключевые слова: эксплойт, кибератака, боевая нагрузка, защита, АСУТП.

Для поиска уязвимостей в ПО команда Digital Security использует различные подходы: анализ исходного кода (если он доступен), различные техники обратного проектирования (reverse engineering) и стресс-тестирование (fuzzing). Все эти техники применимы к различным видам ПО: от браузеров до ПО для АСУТП. Далее для демонстрации найденных уязвимостей специалисты компании пишут эксплоиты, показывающие возможность реализации атаки через определенные недостатки системы.

Под эксплойтом (англ. exploit, эксплуатировать) подразумевается компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в ПО и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение ее функционирования (DoS-атака).

Опираясь на собственный серьезный опыт и компетенцию в области написания эксплойтов для широкого круга ПО, специалисты компании Digital Security могут сравнивать как уровень защищенности разного вида ПО, так и уровень сложности написания соответствующих эксплойтов.

Рассмотрим взгляд эксплоитописателя на АСУТП: какие моменты упрощают процесс написания эксплоитов, какие усложняют, и приведем некоторые советы по повышению уровня безопасности ПО такого класса. Естественно, разговор будет затрагивать также ПО из других областей.