УДК 004.056.5

ОСНОВНЫЕ ВИДЫ КИБЕРАТАК НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМ ПРОЦЕССОМ И СРЕДСТВА ЗАЩИТЫ ОТ НИХ

Палаева Л.В., Хафизов А.М., Гилязетдинова А.М., Вахитова А.Р., Давыдова К.Н., Сиротина Е.Р.

Филиал ФГБОУ ВО «Уфимский государственный нефтяной технический университет», Салават, e-mail: 30lyubasha.palaeva@mail.ru

В данной статье производится обзор основных видов кибератак, таких как массовые и таргетированные, описаны известные методы их распознавания. Представлены несколько самых известных вредоносных программ: руткит Hacker Defender, черви Flame и Stuxnet, вредоносные программы «Троянский конь» и WannaCry, описаны их свойства и принципы работы. Приведены рекомендации для профилактики заражения оборудования. Представлен обзор основных видов антивирусных программ. Рассмотрены методы анализа данных на наличие вредоносных программ, применимых как к массовым, так и к таргетированным атакам: сигнатурный анализ, эвристический анализ, фаерволлы и белый список. Предложена ступенчатая система анализа данных, поступающих из внешних ресурсов, на наличие вирусов и других вредоносных программ. А также предложен способ реализации данной системы. Представлен пример расположения устройств, удовлетворяющий этому способу.

Ключевые слова: кибератака, вредоносная программа, червь, массовая атака, целевая атака, анализ, защита, антивирус, сеть, ступенчатая система

MAIN TYPES OF CYBERATACKS ON AUTOMATED CONTROL SYSTEM OF TECHNOLOGICAL PROCESS AND MEANS OF PROTECTION FROM THEM

Palaeva L.V., Khafizov A.M., Gilyazetdinova A.M., Vakhitova A.R., Davydova K.N., Sirotina E.R.

Branch of Ufa State Petroleum Technical University, Salavat, e-mail: 30lyubasha.palaeva@mail.ru

This article reviews the main types of cyber-attacks, such as mass and targeted, describes known methods for their recognition. Some of the most well-known malicious programs are presented: the Hacker Defender rootkit, Flame and Stuxnet worms, malware Trojan horse and WannaCry, their properties and operating principles are described. Recommendations for the prevention of infection of equipment are given. An overview of the main types of antivirus programs is provided. Methods of data analysis for the presence of malicious programs, applicable to both mass and targeted attacks are considered: signature analysis, heuristic analysis, firewalls and white list. A step-by-step system for analyzing data coming from external resources for the presence of viruses and other malicious programs is proposed. And also, the way of realization of the given system is offered. An example of the arrangement of devices is presented, which satisfies this method.

Keywords: cyber-attack, malware, worm, mass attack, target attack, analysis, protection, antivirus, network, step system

Современные автоматизированные системы управления технологическим процессом (АСУ ТП) представляют собой сложную многоуровневую систему, связанную с механизмом предприятия. В настоящее время высокая структурированность является важным свойством АСУ ТП. Но многоуровневые системы все еще уязвимы при атаках с нижних уровней, которые, в свою очередь, защищены очень плохо. Злоумышленник, способный обойти защиту компьютера предприятия, имеет не только доступ к остальным компьютерам, связанным с первым по локальной сети, но, что важнее всего, он способен нарушить работу самого производства, что вполне может привести к сбоям системы, авариям на самом предприятии, человеческим жертвам.

Несмотря на многообразие методов анализа угроз, зачастую достаточно сложно обнаружить и обезвредить вредоносные программы, попавшие каким-либо образом в программное обеспечение. Это занимает очень много времени и сил, что на руку злоумышленникам.

Целью данной статьи является исследование основных видов кибератак и методов их анализа, а также поиск путей для более точного анализа файлов, поступающих на предприятие из внешних источников. Задача – проанализировать принцип действия известных вредоносных программ, выявив при этом уязвимые точки современных компьютеров.

Виды кибератак

По способу распространения кибератаки можно поделить на массовые, целенаправленные [1].

Массовые кибератаки направлены на глобальное распространение вредоносных

программ, способных нарушить работоспособность компьютера, удалить важные файлы или повредить их. Примерами подобных программ являются: программа-шутка (вызывает отображение изображений и окон на мониторе), руткиты (устанавливают и выполняют в системе код без согласия или оповещения пользователя), вирусы («троянский конь», сетевые и т.д.), прочие [2].

Одним из известных руткитов является Hacker Defender [3]. Замаскировавшись и обойдя брандмауэра, он открывает тайные пути в интернет, позволяющие злоумышленникам управлять зараженным компьютером. Таким образом злоумышленник получает личные данные и может внедрять в систему другие вредоносные программы.

Наибольший вред приносят вирусы.

«Троянский конь» – это вирусная программа, являющаяся частью безвредной программы [4]. Она скрытно выполняет определенные действия с целью причинения ущерба пользователю. Ущерб самый различный: скачивание файлов, удаление данных и выведение из строя оборудования, сбор адресов и паролей социальных сетей и использование их для отправления спама, шпионаж за пользователем, кража паролей и номеров кредитных карточек, создание помех работе антивирусных программ.

Относительно предприятий применяются таргетированные атаки.

Таргетированные (или целенаправленные) атаки – это заранее продуманные действия для поражения информационных систем определенной организации [5]. В большинстве случаев массовые вирусные атаки не приносят какой-либо прибыли. В целевых же атаках средства кибернападения используются для прямой кражи денежных средств или информации. Целенаправленные атаки на информационную инфраструктуру обладают такой характеристикой, как многоступенчатость. Примером такой угрозы служит программа-шпион червь Flame [6]. Вредоносная программа Flame считается одной из опаснейших угроз. Основной задачей Flame является заражение систем управления нефтяной индустрии. Он содержит в себе большой пакет программных модулей, состоящих из большого количества библиотек. Завершив процесс распаковки, программа создает свою базу данных и заносит в нее файлы пораженного оборудования. Также червь делает скриншоты экрана зараженного компьютера и способен записывать разговоры в помещении, в котором непосредственно находится компьютер. В пассивном режиме работы червь производит сбор информации с компьютера. В активном режиме он удаляет информацию с оборудования, на которую была произведена кибератака.

До него был вирус Stuxnet, задачей которого было заражение, нарушение работы промышленных систем, сбора данных [7]. При заражении им компьютера предприятия оборудование переходит в неуправляемый режим работы или самоуничтожается.

Еще одним примером подобной программы может служить недавно нашумевшая вредоносная программа WannaCry [8]. Это сетевой червь, поражающий только компьютеры с операционной системой Microsoft Windows. Принцип его работы состоит в том, что он ищет через интернет устройства со слабым портом 445, данный порт, в свою очередь, отвечает за совместную работу Windows с файлами. Потом программа устанавливает дефект алгоритма, через который загружается код червя. Далее червь действует точно так же, как и классические программы-вымогатели. После запуска червь генерирует пару ключей асимметричного алгоритма. Потом, просканировав содержимое оборудования, червь зашифровывает каждый файл. Когда процесс шифрования завершится, на экране появится окно, извещающее о требовании перевода денежных средств. Если сумма не будет переведена в срок, файлы удаляются. Эта программа появилась в сети с начала 2017 г., однако уже более 150 стран подверглись ее нападению, в том числе Россия, Украина, Испания, Индия и прочие.

Способы обнаружения. Слабая защищенность АСУ ТП может вызвать увеличение числа кибератак оборудования промышленности. Самый простой способ защиты от них – применение сложных паролей и ограничение максимального количества элементов АСУ ТП от интернета. Однако более серьезные меры включают в себя частые аудиты безопасности, обновления уязвимого программного обеспечения и использование средств защиты, направленных на специфику конкретных АСУ ТП [9].

Лучший способ не допустить заражения оборудования – это придерживаться нескольких правил:

– необходимо проверять внешние носители информации, прежде чем начать им пользоваться;

– создавать надежные пароли;

– регулярно сканировать оборудование на наличие вредоносных программ с помощью антивирусов;

– не устанавливать программы от неизвестного поставщика;

– делать резервное копирование ценных данных.

Существует достаточное количество программ, предупреждающих и обезвреживающих атаки (антивирусы) [10]. Каждые из этих программ выполняют свои функции. Различают такие антивирусные программы, как:

– программы-детекторы (анализируют систему, сравнивая цифровые отпечатки программ с собственной базой) [10];

– программы-доктора (не только ищут, но и удаляют вредоносную программу, не повредив зараженные файлы) [10];

– программы-ревизоры (сравнивают исходные состояния программ, файлов и т.д. с текущим их состоянием) [10];

– программы-фильтры (обнаруживают подозрительные действия, характерные для вирусов) [10];

– программы-вакцины (изменяют программу или систему так, что вредоносная программа воспринимает оборудование зараженным и не внедряется) [10].

Но выявить таргетированные атаки гораздо сложнее. Для этого необходимы особые методы.

Основными методами обнаружения подобных атак являются: сигнатурный анализ, эвристический анализ, фаерволлы (брандмауэры), белый список [5].

Сигнатурный анализ

Осуществление сигнатурного анализа предполагает, что аналитики имеют файл, зараженный вирусом [11]. Изучив данную вредоносную программу, можно снять с нее сигнатуру (цифровой отпечаток). После занесения отпечатка в базу можно проверять файл на наличие этого вируса в оборудовании, сравнивая сигнатуры. Сигнатурный анализ обладает рядом преимуществ:

– используется не только для поиска вирусов, но и для фильтрации системного трафика;

– позволяет достаточно точно проводить испытания противостояния атакам.

Минусом сигнатурного анализа является потребность в постоянном обновлении сигнатурной базы.

Эвристический анализ

Роль эвристического анализа заключается в проверке кода на наличие свойств, характерных для вирусов [12]. То есть данный метод заключается в проверке программ на наличие соответствий с сигнатурами известных вирусов. Для этого антивирусная программа должна полностью контролировать работу, выполняемую программой. Этот способ хорош тем, что не зависит от актуальности баз. Минусом данного вида анализа является наличие ложных реагирований на безопасные файлы.

Фаерволлы

Метод выявления целенаправленных атак предполагает использование фаерволлов (брандмауэров), позволяющих фильтровать трафик [12]. Они действуют согласно определенным правилам, построенным по принципу «условие – действие». Трафик пройдет проверку, если к нему найдется соответствующее правило. Недостатком данного метода является большое число лжесрабатываний, из-за которых может затеряться необходимое предупреждение об атаке.

Белый список

Данный метод защиты используется для запуска приложений [12]. Суть заключается в том, что станция может запустить только определенные приложения, находящиеся в этом списке. Помимо защиты от кибератак, он запрещает установку нежелательных программ, которые могут мешать или отвлекать от рабочего процесса. Минус заключается в том, что «белый список» должен включать все приложения, которые нужны пользователю. Такой способ является достаточно надежным, но неудобным, так как замедляет рабочие процессы оборудования.

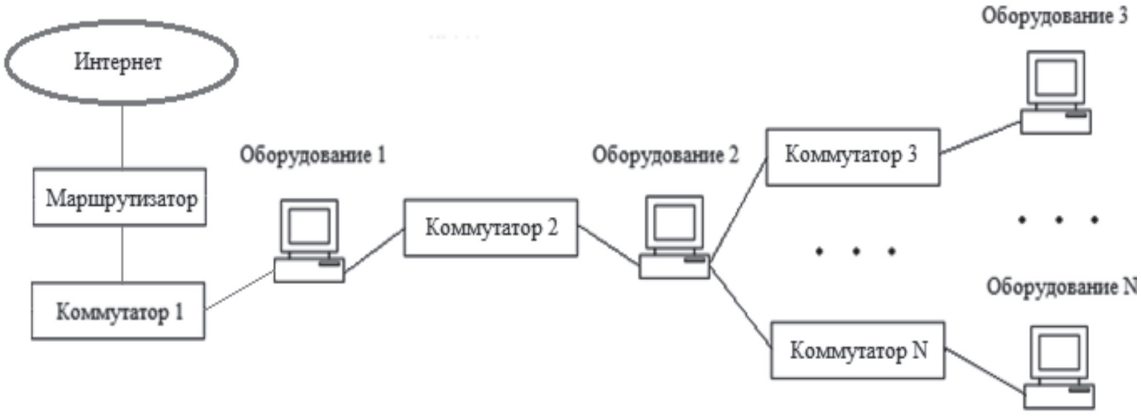
Следует заметить, что данные виды анализа применяются и для обнаружения массовых атак, и многие из них, например сигнатурный анализ и брандмауэры, входят в пакет современных антивирусных программ.

Среди отечественных антивирусных программ, предлагающих защиту АСУ ТП, можно выделить Kaspersky Anti-Virus, а именно Kaspersky Industrial CyberSecurity. Данный вид защиты направлен на защиту промышленных предприятий. Управление работой Kaspersky Industrial CyberSecurity осуществляется из единой консоли управления Kaspersky Security Center: это позволяет добиться оптимального контроля и прозрачности. Централизованное управление упрощает контроль безопасности не только на уровни производственной инфраструктуры, но и на уровне смежных сетей системы [13].

Однако использование по отдельности каждого из приведенных методов – не самый перспективный вариант. Появляется слишком большая вероятность кибератак.

Предлагаемый метод реализации

Предлагается использование ступенчатой системы защиты, состоящей из предыдущих методов. Этот способ предполагает пошаговую проверку файлов, поступающих с внешних источников, на наличие вредоносных программ.



Схематичный план соединения устройств: Интернет – система для хранения и передачи информации; Маршрутизатор – устройство обмена данными между Оборудованием 1 и сетью Интернет; Коммутатор 1…N – устройства соединения узлов данной сети; Оборудование 1 – сервер, обрабатывающий информацию из сети Интернет; Оборудование 2…N – рабочие компьютеры

Нижним уровнем защиты будут являться фаерволлы, так как его основной задачей является защита устройства от внешнего проникновения вредоносных файлов. Если же злоумышленнику удалось обойти первый уровень защиты, то следующим на его пути встанет анализ сигнатурный. Благодаря его базе можно будет выявить и обезвредить все известные вредоносные файлы. Однако вирусы совершенствуются изо дня в день. Следовательно, следующий этап проверки будет – эвристический анализ. Обнаруженный данным методом файл не всегда может являться вирусом, поэтому чтобы вручную проверить и при необходимости обезвредить файлы, необходимо воспользоваться методом «белый список» для того, чтобы системы работала непрерывно. В данном случае «белый список» применяется только как крайняя и краткосрочная мера защиты, так как ее постоянная работа в данной системе очень сильно замедлила бы процесс работы всего оборудования.

Для осуществления данного предложения необходим мощный сервер. Замена каждого оборудования предполагает большие расходы. Поэтому использование одноранговых сетей (состоящих из равноправных оборудований) в предприятии крайне нежелательно [14]. На рисунке представлен план расположения устройств, обеспечивающих безопасность от внешних атак.

Данный вид сети, представленный на рисунке, является сетью на основе серверов с топологией пассивное дерево [15]. Это сделано для того, чтобы минимизировать количество оборудований, имеющих выход в интернет. «Оборудование 1» является сервером высокой мощности, выполняющим роль «щита» стоящей за ним сетью. Далее следуют менее мощные оборудования (Оборудование 2, Оборудование 3… Оборудование N), которые действуют относительно их функций.

Предположив, что данное оборудование будет иметь ступенчатую систему защиты, описанную выше, можно будет описать его принцип работы следующим образом: при наличии известной вредоносной программы лечение происходит стандартным образом. Но как только на сервере обнаружится программа, по свойствам схожая с вредоносной, автоматически включается режим «белого списка», благодаря чему данная программа не попадет в другие компьютеры, связанные с данным, до тех пор, пока специалист по кибербезопасности не устранит проблему либо не выявит, что тревога ложная. Далее информация поступает на главный компьютер, на рисунке обозначенный как «Оборудование 2», и после доходит к остальным оборудованиям, в зависимости от указаний с главного компьютера.

Заключение

Деятельность промышленных компаний тесно связана с социумом. Поэтому способы защиты АСУ ТП требуют особого подхода к организации системы безопасности, чтобы при непрерывных технологических процессах различные проблемы устранялись незамедлительно. От этого зависит не только качество производства, но и жизни и здоровья людей.

Список литературы

1. Таргетированные атаки и как с ними бороться / Intelligent Enterprise. 05.02.2015. – URL: https://www.iemag.ru/analitics/detail.php?ID=32831 (дата обращения: 20.05.2017).

2. Вирусы и вредоносные программы / TREND MICRO. 2017. – URL: http://docs.trendmicro.com/ru-ru/smb/worry-free-business-security-90-sp1-agent-help/about/understanding-threat/viruses-and-malware.aspx (дата обращения: 20.05.2017).

3. Что такое руткиты. Программы для удаления руткитов / WINDXP.COM.RU Настройка и оптимизация операционных систем. – URL: https://www.windxp.com.ru/rotdel.htm (дата обращения: 20.05.2017).

4. Троянские программы (Trojans) / ANTY-MALWARE. – URL: https://www.anti-malware.ru/threats/trojans (дата обращения: 20.05.2017).

5. Таргетированные атаки: новое слово в мире угроз / KV.by High-Tech Club. 03.02.2016. – URL: https://www.kv.by/content/340248-targetirovannye-ataki-novoe-slovo-v-mire-ugroz (дата обращения: 20.05.2017).

6. Червь Flame – как новое оружие кибер-войн / Хабрахабр. 30.05.12. – URL: https://habrahabr.ru/sandbox/44712/ (дата обращения 20.05.2017).

7. Безопасность SCADA: Stuxnet – что это такое и как с этим бороться? / Digital Security Безопасность как искусство. – URL: https://dsec.ru/ipm-research-center/article/bezopasnost_scada_stuxnet_chto_eto_takoe_i_kak_s_nim_borotsya_/ (дата обращения 20.05.2017).

8. WannaCry ransomware used in widespread attacks all over the world / SECURELIST. 2017. – URL: https://securelist.com/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/78351/ (дата обращения: 20.05.2017).

9. Большев А.В. Атаки на низкоуровневые протоколы АСУ ТП на примере HART // Digital Security Безопасность как искусство. 2014. – URL: https://dsec.ru/ipm-research-center/article/attacks_on_low_level_protocols_apcs_for_example_hart/ (дата обращения: 20.05.2017).

10. Сервисное программное обеспечение ПК и основы алгоритмизации / Компьютерные вирусы и защита от компьютерных вирусов. – URL: http://www.lessons-tva.info/edu/e-inf1/e-inf1-4-1-3.html (дата обращения: 20.05.2017).

11. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.

12. Арефьев А.С. Таргетированные атаки на промышленный сектор: новое оружие в кибервойне / А.С. Арефьев // Автоматизация в промышленности. – 2015. – № 2. – С. 43–45.

13. Kaspersky industrial cybersecurity: обзор компонентов решения [Электронный ресурс]. – Режим доступа: http://media.kaspersky.com/pdf/KICS_Tech_Overview.pdf (дата обращения: 20.05.2017).

14. Одноранговые и иерархический сети: в чем отличие? / BLOGSISADMINA.RU. 06.02.2013 – URL: http://blogsisadmina.ru/seti/odnorangovye-i-ierarxicheskie-seti-v-chem-otlichie.html (дата обращения: 20.05.2017).

15. Варлатая С.К. Защита информационных процессов в компьютерных сетях / С.К. Варлатая, М.В. Шаханова. – М.: Проспект, 2015. – 216 с.