DOI 10.36622/VSTU.2022.25.1.011
УДК 004.056

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СВЯЗАННЫХ С АТАКАМИ НА ЦЕПИ ПОСТАВОК

С.С. Куликов, В.И. Белоножкин, Н.А. Юкин

В данной статье представлен анализ угроз информационной безопасности, связанных с атаками на цепи поставок, которые могут использоваться для нарушения информационной безопасности организации без прямых воздействий на ее информационно-технологическую инфраструктуру. В контексте информационной безопасности, атака на цепь поставки предполагает целенаправленные злоумышленные воздействия на активы поставщика с целью последующего нарушения информационной безопасности потребителя. Этот тип атак сегодня приобретает особую актуальность как наиболее эффективный среди всего множества угроз информационной безопасности ввиду принципиальных особенностей, существенно затрудняющих противодействие им: возможность злоумышленника по выбору наиболее незащищенного элемента для атаки, необходимость координации действий нескольких организационных структур для противодействия таким атакам, устранения последствий от их реализации и расследования их причин. Также приведен анализ научной, методической и технической литературы, описывающей сценарии известных атак на цепи поставок программного и аппаратного обеспечения.

Ключевые слова: угрозы информационной безопасности, цепи поставок, атаки на цепи поставок, риски информационной безопасности

Введение

Стремление компаний максимально ускорить и удешевить разработку, производство и внедрение новых информационных технологий в абсолютном большинстве случаев приводит к взаимодействию организаций-потребителей и организаций-поставщиков в сетевой форме. Подобные сетевые структуры с географическим, функциональным и компетентностным распределением их участников требуют исследования новых типов рисков информационной безопасности [1].

На сегодняшний день масштабирование и развитие информационно-технологической инфраструктуры, автоматизация исполнения бизнес-процессов и решения бизнес-задач практически невозможны без привлечения компетенций и ресурсов сторонних лиц, например, вендоров программного обеспечения и аппаратных платформ, провайдеров услуг связи и хранения данных. Одновременно с этим передача сторонним организациям обеспечения ключевых, а иногда и критических для организации процессов, например, таких как облачные вычислительные услуги, защита от DDoS-атак и мониторинг информационной безопасности, только усиливают зависимость информационной безопасности самой организации от внешних и неподконтрольных для нее факторов.

Понятийный аппарат

Подобные отношения между организациями образуют так называемую цепь поставки (англ. Supply chain), то есть совокупность организаций со взаимосвязанным набором ресурсов и процессов, каждая из которых выступает в качестве приобретающей стороны, поставщика или одновременно в качестве обеих сторон, для формирования последовательных отношений с поставщиками. установленных при размещении заказа на поставку, заключения договора или другого официального контракта на поставку [2].

Цепь поставки образуют четыре элемента: поставщик(и) (организация, которая поставляет другой организации продукт или услугу), активы поставщика (ценные элементы, используемые поставщиком для производства продукта или услуги), потребитель (организация, которая

потребляет продукт или услугу, произведенные поставщиком), активы потребителя (ценные элементы, принадлежащие потребителю).

В контексте информационной безопасности, под атакой на цепь поставки следует понимать целенаправленные злоумышленные воздействия на активы поставщика с целью последующего нарушения информационной безопасности потребителя.

При этом традиционное понятие информационной безопасности организации (потребителя), определенное в [3] как состояние, при котором обеспечены конфиденциальность, целостность, доступностью информационных активов и инфраструктуры организации, в условиях существования угроз для цепей поставок необходимо уточнить, явно выделив в нем необходимость обеспечения непрерывности бизнес-процессов этой организации.

Актуальность

Задокументированным примером первой атаки на цепь поставки можно считать исследование Кена Томпсона, проведенное в 1984 году, в рамках которого был создан компилятор для языка C, который внедрял во все компилируемое им программное обеспечение вредоносный код. Не остановившись на достигнутом, автор затем создал компилятор, который скомпилировал компилятор для языка C таким образом, что его код уже не имел явных признаков наличия вредоносного кода [4]. Данная «атака» носила исследовательских характер и показывала, что безусловное доверие к любому стороннему программному обеспечению порождает существенные риски информационной безопасности.

Масштабность атак на цепи поставок была продемонстрирована в 2015 году. В доверенном источнике мобильных приложений «App Store», который на официальном сайте обозначен как «надёжный и безопасный источник приложений, которые отвечают высоким стандартам качества, конфиденциальности и защиты данных», пройдя все проверки безопасности, было размещено содержащее вредоносный код программное обеспечение «XCodeGhost», способное внедрять вредоносный код в другую программу «XCode», а также во все создаваемые с его помощью приложения. Данная атака затронула 128 миллионов пользователей мобильных телефонов под управлением операционной системы «iOS», а в итоге оказались заражены более 300 мобильных приложений.

Потенциальная величина ущерба от угроз, связанных с атаками на цепи поставок, была продемонстрирована уже в мировом масштабе в 2017 году, когда злоумышленники скомпрометировали сервер обновлений программного обеспечения для подачи бухгалтерской отчётности «M.E.Doc», используемой 90% компаний в Украине. Вместе с обновлением для программы от доверенного поставщика все пользователи этой программы загрузили вирус-шифровальщик NotPetya (версия вредоносного программного обеспечения Petya), без возможности расшифрования информации.

Высокой эффективности атаки на цепи поставок достигли в 2020 году. Через доверенную, но уже скомпрометированную платформу автоматического обновления компании «SolarWinds» в обновлении для программного обеспечения «Orion» устройства пользователей получили уязвимость, позволяющую осуществлять удаленное управление зараженным устройством. Несмотря на относительно небольшое количество зараженных организаций (порядка 18 000, по других данным, – всего 60), значительную их часть составили органы государственной власти и крупные технологические компании из США.

В 2021 году было зафиксировано максимально количество атак на цепи поставок: им подверглись инфраструктура технологических компаний «SYNNEX» и «SITA», интегрированная платформа для централизованного управления «Kaseya», программное обеспечение для анализа кода «Codecov», система электронного документооборота органов государственной власти Украины, инфраструктура разработчика систем физической безопасности «Verkada», инфраструктура

разработчика облачных систем управления электронной почтой «Mimecast» и другие [5].

По данным исследования [6] общее количество обнаруженных атак на цепи поставок в 2021 году увеличилось в три раза по сравнению с 2020 годом.

В начале 2022 года компания «DeepMind» объявила о том, что разработанная программная платформа «AlphaCode», основанная на искусственном интеллекте, способна самостоятельно разрабатывать программное обеспечение. Обучение нейросети происходило на общедоступном программном коде, размещенном в отрытом репозитории «GitHub» [7]. Подобный подход также допускает реализацию атаки на цепь поставки, например, через модификацию модели машинного обучения путем искажения обучающих данных, что в дальнейшем может привести к разработке нейросетью программного обеспечения, содержащего критические уязвимостями.

Сценарии атак на цепи поставок

В ряде иностранных технических и методических документов анализируются атаки на цепи поставок. В работе [8] содержится первая достойная каталогизация атак на цепи поставок программного обеспечения и технических средств, которая несколько устарела ввиду появления новых информационных технологий, прежде всего технологий искусственного интеллекта. Представленная информация о 41 типе атак на цепи поставок может стать фундаментом для разработки таксономии подобных атак. Каталогизация атак на цепи поставок основана на следующих атрибутах: уникальный идентификатор, целевой актив, описание процесса и вектор атаки, категория нарушителя, тип и характеристика последствий атаки, источник получения информации об атаке, описание соответствующей угрозы и уязвимости, объект атаки. Все описанные сценарии соотнесены с фазами жизненного цикла актива, на которой может быть реализована соответствующая угроза (табл. 1), а также с уязвимыми элементами цепи поставки (табл. 2).

Анализ этих данных показывает, что на первой и второй фазе создания уязвимого актива угрозе подвержены прежде всего данные, используемые для выбора проектного решения или для проектирования уже конкретного технологического решения. Доля атак, связанных с подменой технических средств и внедрением вредоносного кода в программное обеспечение максимальна на третьем и четвертом фазах жизненного цикла ввиду наибольшей глубины цепи поставки (максимального количества организаций поставщиков). В работе [5] с практической точки зрения описаны сценарии обнаруженных за последние 2 года (период «расцвета») атак на цепи поставок программного обеспечения. В отчете [9] представлен анализ 19 типов атак на цепи поставок интегральных микросхем и их элементов, а также вычислительных систем.

Таблица 1

Распределение количества сценариев атак на цепи поставок по фазам жизненного цикла активов и целям атак

	Цель атаки			
Фаза	SW	HW	FW	SID
MSA	0%	0%	0%	20%
TD (TMRR)	12%	13%	4%	27%
EMD	37%	32%	35%	20%
P&D	24%	30%	35%	20%
O&S	27%	25%	26%	13%

где: MSA – Materiel Solution Analysis (фаза анализа существующих решений), TD – Technology Development (фаза разработки технологического решения), TMRR – Technology Maturity and Risk Reduction (фаза проверки технологического решения), EMD – Engineering and Manufacturing Development (фаза разработки прототипа технологического решения и подготовки его производства), P&D – Production and Deployment (фаза производства и развертывания технологического решения), O&S – Operations and Support (фаза эксплуатации и поддержки технологического решения), SW – Software (программное обеспечение), HW – Hardware (аппаратное обеспечение), FW – Firmware (встроенное программное обеспечение), SID – System

Information and Data (системная информация и данные).

Таблица 2

Распределение количества сценариев атак на цепи поставок по фазам жизненного цикла активов и уязвимым элементам цепи поставки

	Элемент цепи поставки					
Фаза	ПО	ГП	СП	СИ	РП	РА
MSA	17%	0%	0%	0%	0%	0%
TD (TMRR)	22%	12%	16%	10%	11%	8%
EMD	17%	30%	36%	33%	37%	33%
P&D	17%	24%	20%	30%	26%	33%
O&S	27%	34%	28%	26%	26%	26%

где: ПО – проектный офис, ГП – генеральный подрядчик, СП – субподрядчик, СИ – системный интегратор, РП – разработчик программного обеспечения. РА – разработчик аппаратного обеспечения.

Стоит также отметить, что российские методические документы по защите информации в явном виде не содержат упоминания об атаках подобного вида. При этом в Банк данных угроз ФСТЭК России включены некоторые угрозы, связанные с атаками на цепи поставок, например, УБИ.215 Угроза несанкционированного доступа к системе при помощи сторонних сервисов, УБИ.217 Угроза использования скомпрометированного доверенного источника обновлений программного обеспечения, УБИ. 221 Угроза модификации модели машинного обучения путем искажения («отравления») обучающих данных.

Таким образом, можно констатировать, что отсутствуют как российские, так и зарубежные комплексные научные исследования актуальных сценариев реализации подобных атак, тяжести последствий от их реализации и эффективных методов противодействия им.

Феномен атак на цепи поставок и перспективы исследований

На сегодняшний день в научной литературе достаточно широко представлены научные исследования отдельных категорий атак с использованием недекларированных возможностей и применением вредоносного программного обеспечения и технических средств [11], атак предполагающих реализацию методов социальной инженерии и влияния на процессы принятия решений [12], целенаправленных атак известных «хакерских» группировок на корпоративные информационные системы [1313].

Атаки на цепи поставок из всего множества других атак выделяет ряд значимых характеристик:

1) при реализации атаки на цепь поставок фактически совершаются как минимум две связанные результатом, но реализуемые независимо атаки – на поставщика и потребителя, что требует высокого потенциала нарушителя и его соответствующей мотивации;

2) организация-потребитель может быть уязвима для атаки на цепь поставки, даже если ее система защиты информации достаточно эффективна, так как эксплуатируются уязвимости, управление которыми для нее не доступно;

3) величина ущерба от атак на цепи поставок свидетельствует об их высокой эффективности, так как нарушение информационной безопасности одной организации приводит к нарушению информационной безопасности значительного количества других организаций;

4) устранение последствий, расследование и предотвращение атак на цепи поставок требует значительно больших ресурсов, высокой компетенции специалистов и координации работы нескольких организационных структур;

5) предотвращение атак на цепи поставок требует моделирования соответствующих угроз, в том числе за счет оценки и анализа соответствующих рисков информационной безопасности, однако достойный математический аппарат для этого на сегодняшний день отсутствует.

Сочетание этих особенностей с недостаточной научной проработанностью темы атак на цепи поставок в аспекте информационной безопасности открывает перспективы для возможных исследований.

Так, ввиду принципиальной невозможности организации-потребителя управлять уязвимостями всей цепи поставки (в первую очередь уязвимостями, находящимися в зоне ответственности организаций-поставщиков) и гарантированно предотвратить реализацию угроз, использующих эти уязвимости, видится необходимой разработка методологии анализа соответствующих рисков информационной безопасности через их вероятностные оценки.

Это, в свою очередь, позволит:

1) оценить кибер-устойчивость потребителей к атакам на цепи поставок;

2) спрогнозировать ущерб от реализации атак на цепи поставок;

3) ранжировать угрозы, связанные с атаками на цепи поставок, например, для целенаправленного противодействия наиболее актуальным;

4) выбирать эффективную стратегию по управлению рисками информационной безопасности, в том числе его принятие, страхование и отказ;

5) оценить эффективность внедренных мер;

6) управлять бюджетом информационной безопасности организации.

Список литературы

1. Остапенко А.Г. К вопросу о трендах и инструментарии социо-информационного глобального противоборства. / А.Г. Остапенко, А.А. Остапенко, Н.М. Лантюхов, С.Д. Трубицын, И.А. Боков. // Информация и безопасность. 2020. Т. 23. Вып. 4. С. 519-524.

2. Информационная технология. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 1. Обзор и основные понятия : ГОСТ Р ИСО/МЭК 27036-1-2021. Введ. 2021-05-20. М. : Стандартинформ, 2021. – 15 с.

3. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения : ГОСТ Р 53114-2008. Введ. 2009-10-01. М. : Стандартинформ, 2018. 16 с.

4. Thompson K. Reflections on Trusting Trust / K. Thompson // Communications of the ACM. 1984. Volume 27. Issue 8. P. 761–763.

5. Threat Landscape For Supply Chain Attacks. ENISA, 2021. P. 57.

6. 2021 Software Supply Chain Security Report. Aqua Security, 2021. P. 9.

7. Solving novel problems and setting a new milestone in competitive programming // Сайт DeepMind URL: https://www.deepmind.com (дата обращения: 20.12.2021).

8. Miller J.F. Supply Chain Attack Framework and Attack Patterns. MTR 14-0228. MITRE, 2013. P. 86.

9. Areno M. Supply Chain Threats Against Integrated Circuits White Paper. – Intel White Paper. Intel Corporation, 2020. P. 15.

10. Барабанов А.В. О систематике информационной безопасности цепей поставки программного обеспечения. / А.В. Барабанов, А.С. Марков, В.Л. Цирлов // Безопасность информационных технологий. 2019. Т. 26. №. 3. С. 68-79.

11. Остапенко А.Г. Сетевая вирусология: прогнозирование развития двувирусных эпидемических процессов в сетях. / А.Г. Остапенко, Е.В. Зарочинцев, О.А. Остапенко, К.В. Сибирко, В.В. Сафронова, П.Д. Федоров. // Информация и безопасность. 2021. Т. 24. Вып. 2. С. 203-222.

12. Остапенко А.Г. «Инфодемия» и социальные сети: модели эпидемического процесса. / А.Г. Остапенко, Е.А. Шварцкопф, А.А. Остапенко, Д.А. Нархов, П.Д. Федоров, Р.В. Сорокин. // Информация и безопасность. 2020. Т. 23. Вып. 2. С. 285-290.

13. Сердечный А.Л. Моделирование, анализ и противодействие сценариям компьютерных атак, реализуемых группировкой apt3 в распределенных компьютерных системах. / А.Л. Сердечный, А.В. Айдаркин, М.А. Тарелкин, А.Е. Дешина. // Информация и безопасность. 2021. Т.24. Вып. 1. С. 35-46.

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 11.01.2022

Информация об авторах

Куликов Сергей Сергеевич – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: kulikov.serg@yandex.ru

Белоножкин Владимир Иванович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Ююкин Николай Алексеевич – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

ANALYSIS OF INFORMATION SECURITY THREATS, ASSOCIATED WITH SUPPLY CHAIN ATTACKS

S.S. Kulikov, V.I. Belonozhkin, N.A. Yuyukin

This article presents an analysis of information security threats associated with attacks on the supply chain, which can be used to violate the information security of an organization without direct impacts on its information technology infrastructure. In the context of information security, an attack on the supply chain involves targeted malicious impacts on the supplier's assets with the aim of further violating the consumer's information security. This type of attacks is becoming particularly relevant today as the most effective among all the many threats to information security due to the fundamental features that significantly complicate countering them: the possibility of choosing the most unprotected element of the chain for an attack, the need to coordinate the actions of several organizational structures to counter such attacks, eliminate the consequences of their implementation and investigate their causes. The analysis of scientific, methodological and technical literature describing scenarios of known attacks on the supply chain of software and hardware is also given.

Keywords: information security threats, supply chains, supply chain attacks, information security risks.

Submitted 11.01.2022

Information about the authors

Sergey S. Kulikov – Cand. Sc. (Technical), Assistant Professor, Voronezh State Technical University, e-mail: kulikov.serg@yandex.ru

Vladimir I. Belonozhkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Nikolay A. Yuyukin – Cand. Sc. (Technical), Assistant Professor, Voronezh State Technical University, e-mail: mnac@comch.ru