

АНАЛІЗ АТАК НА ЛАНЦЮГИ ПОСТАЧАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Вінницький національний технічний університет

Анотація

Розглянуто найбільш критичні загрози безпеці в ланцюгах постачання програмного забезпечення, запропоновано методики зменшення ризиків цих загроз. Запропонований огляд дозволяє пріоритизувати напрямки захисту від найбільших загроз на ланцюги постачання. Звернено увагу на основні вектори атак, що використовуються зловмисниками для компрометації програмних компонентів та інструментів збірки. Проаналізовано методи раннього виявлення загроз, а також практики, спрямовані на посилення загальної безпеки процесу розробки та постачання.

Ключові слова: кібератака, компрометація, ланцюг постачання, безпека, вразливості, ризики, тенденції, заходи захисту.

Abstract

The most critical security threats in software supply chains are considered, and methodologies for mitigating these risks are proposed. The proposed review allows for prioritizing protection strategies against the most significant threats to supply chains. Attention is paid to the main attack vectors used by malicious actors to compromise software components and build tools. Methods for early threat detection are analyzed, along with best practices aimed at enhancing the overall security of the development and delivery process.

Keywords: cyberattack, compromise, supply chain, security, vulnerabilities, security risks, security methods

Вступ

Завдяки необхідності постійної підтримки та оновлення програм виникла низка атак на програмне забезпечення, які обирають об'єктом атаки не саме програмне забезпечення, а шлях його потрапляння до користувачів — ланцюг постачання (supply chain) [1]. Сучасний ланцюг постачання містить багато взаємопов'язаних компонентів та процесів, які забезпечують ефективне функціонування організацій. Попри це, саме складність і багатошаровість цих ланцюгів створює численні вразливості, що можуть використовуватися зловмисниками. У світлі останніх резонансних інцидентів [2-5], такі як атаки на великі компанії чи постачальників компонентів, «supply chain attacks» стають все більш актуальними. Водночас відсутня єдина методологія впровадження захисту як невід'ємної частини ланцюга постачання.

Відповідно, метою цього дослідження є зменшення часу на доставку програмного забезпечення за рахунок підвищення безпеки в ланцюзі постачання. Автоматизація аналізу вразливостей дозволяє виключити кроки, які застосовуються для дослідження та усунення вразливостей в робочій системі. Для цього необхідно визначити вектори атаки на ланцюги постачання.

Аналіз сучасних загроз

В дослідженні основна увага приділяється найбільш поширеним типам атак на ланцюги постачання програмного забезпечення. Зокрема, розглядаються атаки, пов'язані з компрометацією вихідного коду та включенням шкідливих модулів у легітимні оновлення, атаки на апаратні компоненти, які передбачають заміну оригінальних деталей або встановлення прихованих функцій, а також використання методів соціальної інженерії та фішингу для отримання доступу до внутрішніх систем компаній. Крім того, досліджуються тренди атак, такі як зловмисне використання відкритих бібліотек і фреймворків, ускладнення методів маскування шкідливих дій, а також орієнтація на людський фактор. Відповідно до проведених досліджень було визначено такі типи атак на ланцюги постачання програмного забезпечення:

- Компрометація програмного забезпечення

Внесення шкідливого коду у легітимні оновлення, або включення бекдорів [6] у вихідний код, з метою подальшого використання як вразливості. Наприклад, включення коду в репозиторії відкритого ПЗ або використання вразливостей сторонніх бібліотек [5].

- Атака на апаратні компоненти [3]

У разі апаратних ланцюгів постачання можлива заміна оригінальних компонентів шкідливими аналогами або встановлення недокументованих функцій у мікросхеми. Це створює загрозу на апаратному рівні яку складно виявити стандартними методами. Зазвичай загроза та її наслідки виявляється вже після того як атака здійснена [8].

- Соціальна інженерія та фішинг [9]

Людський фактор лишається одним із найслабших місць безпеки. Фішингові атаки на персонал компанії можуть відкрити доступ до внутрішніх систем та даних. Крім того, варто відзначити ланцюговий ефект таких атак: вразливості, знайдені в одному з ланок ланцюга постачання, дозволяють впливати на кінцевого користувача [10].

Ідентифікація трендів зміни загроз

У контексті динамічного технологічного розвитку, загрози в ланцюгах постачання програмного забезпечення еволюціонують, пристосовуючись до нових вразливостей та можливостей. Зокрема, багатофакторна взаємодія сучасних інструментів розробки та розгортання ПО створює дедалі складніший ландшафт безпеки, що вимагає адаптивних підходів до моніторингу та захисту. Усвідомлення цих тенденцій є критично важливим для ефективного захисту інфраструктури та мінімізації ризиків.

- Зростання кількості відкритих бібліотек та фреймворків

З кожним роком збільшується залежність розробників від зовнішніх бібліотек. Зловмисники шукають вразливості у цих компонентах, а також активніше використовують методи «Typosquatting» (реєстрація пакетів з подібною назвою) [11] для поширення шкідливого коду.

- Ускладнення методів маскування

Хакери впроваджують складніші механізми шифрування, стеганографії та приховування шкідливих модулів. Такі прийоми дозволяють атакам залишатися непоміченими тривалий час.

- Орієнтація на людський фактор

Збільшується кількість атак, спрямованих не лише на ІТ-системи, а й на співробітників компаній. Використовуються психологічні маніпуляції, дзвінки, фальшиві повідомлення в месенджерах тощо. Прослідковується збільшення кількості атак саме на облікові записи працівників, які дотичні до розробки чи доставки кодової бази [12]

- Консолідація зловмисних груп

Організовані угруповання працюють об'єднано, обмінюються інструментами і тактиками, що пришвидшує появу нових векторів атак. Інколи навіть виникають «Supply Chain Attack-as-a-Service» платформи [13].

- Поширення атак на нові сфери

Раніше здебільшого страждали ІТ-компанії та організації з критичною інфраструктурою, тепер же атаки часто спрямовані на медичні установи, логістичні корпорації та стартапи, що також мають цінні дані.

Рекомендації щодо врахування трендів

Прогнозування та постійна оцінка загроз відіграють центральну роль у формуванні стратегій безпеки ланцюгів постачання. Для того, щоб ефективно протидіяти динамічним загрозам, потрібна як глибока експертиза, так і комплексний підхід до управління ризиками. Розгляд нових тенденцій та їх своєчасне інтегрування у процедури розгортання і контролю дозволяють забезпечити більш високий рівень захисту.

- Необхідність комплексного підходу

Атаки на Supply Chain можуть відбуватися як на рівні «софт»-, так і «хард»-складових. Тому потрібні

одночасно і технічні, і організаційні засоби захисту. Автоматизація процесів розгортання з дотримання стандартів безпеки та встановлених процедур мінімізує можливість втручання в процес доставки програмного забезпечення

- Важливість прозорості та довіри

Із збільшенням кількості залучених сторін ефективний обмін інформацією про уразливості та підтримка довіри стають критично важливими. Прозорість та розуміння процесу розгортання дозволяє швидко реагувати на потенційні вразливості, а також усувати їх ще до моменту виявлення.

- Побудова безперервного процесу оцінки ризиків

Ризики в ланцюгах постачання динамічно змінюються, а отже потрібне регулярне оновлення політик, перевірка виробничих і логістичних процесів та проведення навчань для персоналу. Системи відстеження подій в ланцюзі постачання та їх безперервний аналіз знижує вірогідність подій що призводять до витоку даних або компрометації програмного забезпечення.

- Автоматизація моніторингу та аналізу

Використання систем SIEM, технологій машинного навчання, інструментів для аналізу мережних аномалій та автоматизація управління виправленнями (patch management) допомагають швидше виявляти спроби проникнення. Системи моніторингу є ключовим елементом в ланцюзі постачання, оскільки дозволяють оцінити стан системи до, після та в самому процесі доставки програмного забезпечення. Використання технологій штучного інтелекту дозволяє досягти значного рівня безпеки процесів.

- Співпраця на міжнародному рівні

Supply Chain зазвичай є глобальним підходом, тож взаємодія компаній, стандартизація, обмін досвідом та інформацією щодо кібератак допомагають формувати скоординовану політику безпеки. Особливо важливою є участь у міжнародних ініціативах та альянсах, які сприяють розробці загальновизнаних стандартів безпеки. Також доцільним є створення глобальних платформ для обміну даними про вразливості в реальному часі, що дозволить оперативно реагувати на нові загрози.

Висновки

Виконаний аналіз атак на програмне забезпечення дозволив обґрунтувати актуальність загроз на ланцюги постачання програмного забезпечення. Завдяки подальшому аналізу цих атак визначено об'єкти, які уражаються. Проаналізовано тренди атак, що дозволило визначити орієнтацію на людський фактор, як найбільш небезпечний тип атак, проти якого доцільно звернути особливу увагу дослідників в напрямку кібербезпеки. Одним із показників що свідчить про достатню захищеність системи є швидкість розгортання. Впровадження рекомендацій описаних вище, дозволить зменшити час, що витрачається на пошук, аналіз та тестування потенційних небезпек ланцюга розгортання.

На основі виконаного аналізу запропоновано рекомендації для зменшення ризиків внаслідок атак на ланцюги постачання. Подальшою перспективою досліджень є формалізація процесів атак для надання можливості забезпечення систематизованого підходу для розробки методів та засобів захисту від атак цього типу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Postmus D. The supply chain of enterprise software: strategy, structure, and coordination. [Thesis fully internal (DIV), University of Groningen]. PrintPartners Ipskamp B.V., Enschede, The Netherlands. 2009 – URL: <https://pure.rug.nl/ws/portalfiles/portal/13087368/01c1.pdf> (accessed 01.02.2025)
2. Marelli M. The SolarWinds hack: Lessons for international humanitarian organizations. *International Review of the Red Cross*. – 2022. – Vol. 104. – pp. 1–18. doi: 10.1017/S1816383122000194
3. Montasari R., Hill R., Parkinson S., Hosseinian-Far A., Daneshkhah A. Hardware-Based Cyber Threats: Attack Vectors and Defence Techniques. *International Journal of Electronic Security and Digital Forensics*. – 2019. – Vol. 12. doi: 10.1504/IJESDF.2020.10029857
4. Godin D. What we know about the xz Utils backdoor that almost infected the world. *ArsTechnica*, April 2024. – URL: <https://arstechnica.com/security/2024/04/what-we-know-about-the-xz-utils-backdoor-that-almost->

infected-the-world/ (accessed: 01.02.2025).

5. Nova Scotia. Public report - URL: <https://novascotia.ca/privacy-breach/docs/cyber-security-attack-moveit-public-report.pdf> (accessed: 01.02.2025).

6. Kara A., Dusman I., Arka K., Saldırları T. The Spy Next Door: A Digital Computer Analysis Approach for Backdoor Trojan Attack. *European Journal of Science and Technology*. – 2021. – pp. 125–129. doi: 10.31590/ejosat.897799

7. JFrog. How Supply Chain Attacks Work — and How to Secure Against Them. – Березень 2024. – URL: <https://media.jfrog.com/wp-content/uploads/2024/03/26163108/Dark-Reading-JFrog-Report-on-Software-Supply-Chain-Security.pdf> (accessed: 01.02.2025).

8. Arab Center for Research and Policy Studies. Israel Signals Escalation with Attacks on Hezbollah Communications Devices. URL: <https://www.dohainstitute.org/en/Lists/ACRPS-PDFDocumentLibrary/pager-massacre-implications-for-lebanon.pdf> (accessed: 01.02.2025).

9. Chhimwal M., Agrawal S., Kumar G. Measuring Circular Supply Chain Risk: A Bayesian Network Methodology. *Sustainability*. – 2021. – Vol. 13. doi: 10.3390/su13158448

10. Koyun A., Al Janabi E. Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)* 2017; 4(6): 7533–7538.

11. Moore T., Edelman B. Measuring the Perpetrators and Funders of Typosquatting. *Lecture Notes in Computer Science*. – Springer, 2010. – pp. 175–191. doi: 10.1007/978-3-642-14577-3_15

12. Anti-Phishing Working Group. Phishing Activity Trends Report 3rd Quarter 2024. URL: https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf (accessed: 01.02.2025).

13. Kern, E.; Szanto, A. Cyber Supply Chain Attacks. *Brandenburgisches Institut für Gesellschaft und Sicherheit*. BIGS Policy Paper No. 10, August 2022.

14. Breda F., Barbosa H., Morais T. Social Engineering and Cyber Security. *INTED2017 Proceedings*. – 2017. – pp. 4204–4211. doi: 10.21125/inted.2017.1008.

15. SlashNext. The State of Phishing. – URL: <https://slashnext.com/wp-content/uploads/2024/05/SlashNext-The-State-of-Phishing-24-Midyear-Report.pdf> (accessed: 01.02.2025).

16. NCSC (National Cyber Security Centre UK). Supply Chain Security Guidance. URL: <https://www.ncsc.gov.uk/collection/supply-chain-security> (accessed: 01.02.2025).

17. Lu G., Koufteros X., Lucianetti L. Supply Chain Security: A Classification of Practices and an Empirical Study of Differential Effects and Complementarity. *IEEE Transactions on Engineering Management*. – 2017. – Vol. 64, No. 2. – pp. 234–248. doi: 10.1109/TEM.2017.2652382

18. Ghadge A., Weib M., Caldwell N., Wilding R. Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management*. – 2019. doi: 10.1108/SCM-10-2018-0357

19. Abd Latif M. N., Abd Aziz N. A., Nik Hussin N. S., Abdul Aziz Z. A. Cyber security in supply chain management: A systematic review. *Logforum*. – 2021. – Vol. 17. – pp. 49–57. doi: 10.17270/J.LOG.2021555

20. Ojha R. et al. Bayesian network modelling for supply chain risk propagation. *International Journal of Production Research*. – 2018. – Vol. 56, No. 17. – pp. 5795–5819

Скін Андрій Володимирович — аспірант кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: phd@askip.me

Науковий керівник: **Барисhev Юрій Володимирович** — канд. техн. наук, доцент кафедри захисту інформації, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: yuriy.baryshev@vntu.edu.ua

Skip Andrii V. — Postgraduate Student of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: phd@askip.me

Supervisor **Baryshev Yuriy V.** — PhD. (Eng), Associate Professor of Information Protection Department, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua