УДК 004

АТАКА НА ЛАНЦЮГ ПОСТАВОК

В. А. Нікітюк[1], М. В. Грайворонський[2]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Проведено аналіз здійснених вдалих атак на ланцюг постачання та виявленно слабкі місця в побудові системи захисту для підприємств. Досліджено міжнародний стандарт ISO/IEC 27001 на виявлення та захист від атак на ланцюг постачання. Знайдено рішення для забезпечення захисту і не можливості ефективної реалізації цієї атаки.

Ключові слова: стандарт ISO/IEC 27001, кібер-атака, кібер-ризик, бекдор, атака на ланцюг поставок, скомпрометований код.

Вступ

Інформація дуже цінний ресурс, але розуміння цього з'являється з її втратою. У всьому світі розвинуті компанії витрачають великі гроші для створення максимального захисту для секретних даних компанії та персональних даних її співробітників та клієнтів. Але зловмисники, що здійснюють атаку на ланцюг поставок можуть викрасти кошти великої кількості користувачів за короткі проміжки часу, таким чином, що ніхто не зможе зафіксувати початок атаки. Використовуючи мої дослідження, компанії можуть запобігти виникненню атаки і зберегти в цілості конфіденційні дані.

1. Ціль атаки на ланцюг поставок та як її відрізнити

1.1 Ціль атаки

Ціль зловисників, що впроваджують скомпрометований код у програмний засіб, змінити сценарій дій і налаштування таким чином, щоб можна було контролювати систему віддалено і відкрити доступ до персональних даних користувачів (номер, дата видачі та CVV код) або розмістити інфіковане оновлення. Після отримання даних, здійснюють грошові переведання. Вони отримують кошти та інформацію, після цього виводять систему з ладу.

1.2 Принцип дії атаки

Атака на ланцюг поставок – це кібератака, що здійснюється, використовуючи довіру між компанією-виробником та її клієнтами. [6] Вона завдає шкоду організації, орієнтуючись на слабкі місця у ланцюгу постачання. Зловмисник ставить під загрозу один або кілька компонентів процесу розробки чи доставки. Така атака може використовувати підроблені чіпи, що задіяні у виробництві комп'ютера або мережевого обладнання. Або, атака може запровадити скомпрометований код у програмному засобі, що не викликає підозри. Є цілий ряд різних сценаріїв та методів, але головне, що ця атака використовує надійні канали для проникнення, щоб досягти своїх цілей.

1.3 Її особливості

Атака такого типу має свої особливості:

- Компанії, у яких було здійснено атаку на ланцюг постачання, помічають втрату персональних даних або важливої інформації набагато пізніше, ніж проведено було атаку, таким чином чим більше часу проводиться атака, тим більше даних клієнтів скомпрометовано.
- Здійснюється на основі довіри користувачів до продукту, який вони вже використовували, і бездоганної репутації компанії, що піклуючись про клієнтів випускає оновлення свого продукту.
- Зараження може відбутися ще в ланцюгу постачання компанії-постачальника, а інфікований продукт з'явиться вже в першій ланці ланцюга постачання компанії, що користується її послугами.
- Її можна порівняти з бомбою уповільненої дії, тобто на певному етапі ланцюга постачання впроваджується заражений компонент (виконуваний файл, спеціальний програмний засіб і т.п.), який пізніше, при завантажені користувачами програми, починає діяти за сценарієм зловмисників, і за короткий проміжок часу може інфікувати мільйони комп'ютерів користувачів. [3] [4]

1.4 Схема атаки

Отже, в який момент можна інфікувати комп'ютер злочинним кодом?! Ми можем роздивитися схему ланцюга поставок на рис. 1. Потенційно кожна сторона має вразливе місце і на будь-якому етапі можна замінити чіп на підроблений, встановити заражену програму, налаштувати обладнання так, щоб атаку

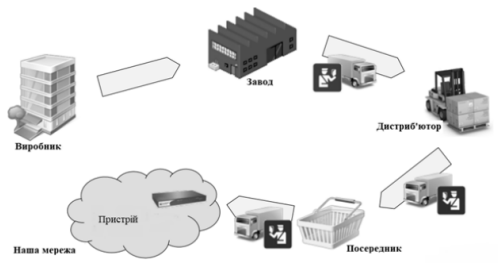

Рис. 1. Схема ланцюга поставок

можна було розпочати у будь-який момент. Але це не так просто, адже для ефективного проведення атаки потрібно знати:

- яким чином можна інфікувати сайт, де користувачі завантажують програму, або вводять персональні дані;
- які технічні засоби використовуються для роботи з веб-сайтом, або мають доступ до персональних даних користувачів;
- які є вразливі місця чи помилки в політиці безпеки компанії;
- з якими постачальниками співпрацює компанія;
- як інфікувати систему, щоб це не було виявлено завчасно і т.д..

2. Аналіз досвіду компаній, що постраждали від здійснених вдалих атак на ланцюг постачання

2.1 Аналіз фінансових втрат від атаки

Перші атаки були проведені у 2013 році, кожна наступна була хитрішою та витонченою. Їх стратегії ставали складнішими і не зрозумілими. Якщо спочатку злочинці викрадали дані користувачів невеликих компаній з метою отримати гроші, то з часом вони намагалися добратися до великих фірм, де кількість клієнтів набагато більше, використовуючи невеликі, як проміжний етап. [1] [3]

Результат не змусив чекати, компанії втрачають репутацію, клієнтів, і велику кількість грошей, в яку входить і штраф у розмірі 4 % від річного світового обігу за попередній фінансовий рік для підприємства або 20 мільйонів євро, в залежності що більше, бо починаючи з 25 травня 2018 року усі організації мають виконувати основні вимоги нового європейського законодавства із захисту персональних даних GDPR (General Data Protection Regulation). [3]

На діаграмі на рис. 2 зображено деякі випадки атак на ланцюг поставок великих компаній та їх приблизні фінансові втрати. Target була першою компанією, яка отримала збитки від цієї атаки, втрачено майже 162-мільйона доларів, скомпрометована персональна інформація (повне ім'я, адреса, електронна пошта, номер телефону) 110-мільйонів користувачів. В авіакомпанії пасажири очікували рейс, білети на який було продано, але компанія про це нічого не знала, тоді і була виявлена атака. 75 тисяч пасажирів не вирушило в дорогу, втративши гроші і особисті дані.[2]

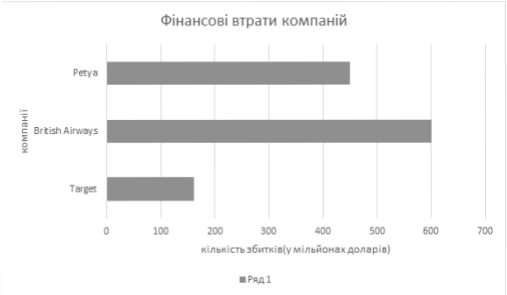

Рис. 2. Фінансові збитки компаній, після атаки на ланцюг поставок

Зловмисники змогли отримати доступ не тільки до основної інформації про банківські картки користувачів (ПІБ і номер картки), але також і до кодів перевірки дійсності карток (CVV). Виникло питання, як вони змогли отримати ці коди, якщо навіть сама авіакомпанія їх не зберігає.

Отже, був змінений скрипт на сайті авіакомпанії таким чином, щоб при здійсненні платежів хакери могли отримувати цей код разом з іншими даними. В результаті була здійснена крадіжка дуже великих масштабів та шкода репутації компанії. Схожий випадок був у компанії Ticketmaster, було скомпрометовано дані 40 тисяч клієнтів. Після встановленого оновлення від CCleaner більш ніж 2 мільйони користувачів під'єдналися до сервера зловмисників.

2.2 Тенденції атак в ланцюжку поставок програмного забезпечення і різновид методів її здійснення

Отже, компанії отримують великі штрафи, втрачають клієнтів та багаторічну репутацію, яку відновити дуже складно, повинні змінювати політику безпеки та в принципі підхід до захисту даних, і знайти зловмисників, після того як пройшов певний час – майже нереально.

У презентації «Вектор несподіваних атак: засобу оновлення програмного забезпечення» на RSA Conference у 2018-му році було представлено діаграму на рис. 3, в якій зображено яка кількість атак була та як з кожним роком зростає їх кількість. [4]

Схема атаки CCleaner була досить складною і складалася як мінімум з трьох етапів. Шкідливе ПЗ, запроваджене в популярну програму зі 100 млн активних користувачів, поширювалося цілий місяць. Пізніше з'ясувалося, що на командному сервері працював простий скрипт, який вибирав жертв для другого етапу атаки: ними ставали ті, хто, судячи по доменних іменах, міг виявитися співробітником великих IT-компаній та постачальників. На цьому етапі відібрали всього 40 комп'ютерів, на які потім відправили додаткове шпигунське ПЗ.

На наступному етапі злочинці ще більше звузили список жертв: зібравши і проаналізувавши інформацію з цих 40 комп'ютерів (ймовірно, вже вручну), вони вибрали чотири найбільш цікаві цілі. На ці пристрої встановили спеціально доопрацьовану версію ShadowPad – відомого шкідливого ПЗ, яким вже користуються китайські кіберзлочинці. Це і бу-

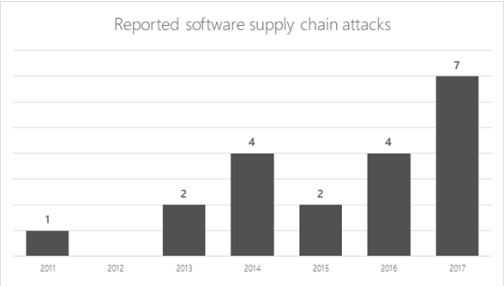

Рис. 3. Тенденції атак в ланцюжку поставок програмного забезпечення (джерело: презентація RSA Conference 2018 «Вектор несподіваних атак: засобу оновлення програмного забезпечення») Microsoft Security [7]

ло кінцевою метою атаки – доставити бекдор на комп'ютери певних співробітників великих компаній.

Це означає, що реалізувати атаку дуже складно і не під силу будь-кому. По-перше, для того, щоб знайти вразливе місце та проникнути в середу розробки програмного забезпечення, що є ціллю для зловмисника, потрібно багато часу, ресурсів та інформації про внутрішню роботу компанії. По-друге, сил та знань досвідчених програмістів, щоб створити атаку, що правдоподібно імітує усі процеси та непомітно впровадити злочинний код. Це має бути створена команда з фахівців, що знають яким чином захищена структура, яка є ціллю для нападу, зможуть написати заражений програмний код та впровадити його в певний комп'ютер, що є стратегічно важливим.

Також це потребує не малих коштів. Але якщо атаку вдасться здійснити, то зловмисники зможуть отримати персональні дані клієнтів, вивести з ладу техніку, знищити інформацію та викрасти велику суму грошей.

3. Дослідження міжнародного стандарту ISO/IEC 27001 і рішення для покращення захисту

Отже, атаки здійснюються успішно, але як можна від них захиститися?! Звісно, є стандарт ISO/IEC 27001, нова версія якого прийнята в 2013 році, але інформаційні технології розвиваються дуже швидко, тому виконання цього стандарту не гарантує захист від атаки здійсненної на ланцюг постачання. [5]

У стандарті прописано, як потрібно контролювати постачальників і поставлена конкретна задача: «Гарантувати захист активів організації, які доступні постачальникам та підтримувати узгоджений рівень інформаційної безпеки і надання послуг в відповідності з угодою з постачальником». [5] Але постачальник не обов'язково може мати доступ до активів компанії, він може бути роздрібним торговцем, або постачати певну техніку, та все одно його потрібно контролювати. Тим паче, часто постачальник вже передає заражене, але не активоване (тобто сценарій зловмисника ще не виконується) шкідливе програмне забезпечення, або технічне забезпечення, в яке встановлено підслуховуючий пристрій. Тобто загроза може надходити від постачальників, які працюють з постачальниками. Оскільки контрактні виробники часто працюють на тонкій маржі, вони іноді творчо підходять до створення додаткової маржі – наприклад, спокушаються більш дешевими запчастинами від незатверджених продавців. Компанія має уважно слідкувати за такими постачальниками та проводити періодичні перевірки, а також регулярно відвідувати їх співробітників в ділових цілях.

Будь-який тип атаки – це ризик, який жодна компанія не може собі дозволити. У той час як більшість компаній зосереджені на своїх внутрішніх кібер-ризиках, лише деякі в реальному часі можуть оцінити вразливість своїх ланцюжків поставок.

Всі компанії мають як мінімум два рівні (яруси) постачальників – Перший рівень (постачальники з прямим контрактом) та другий рівень (постачальники для постачальників першого рівня). Великі компанії чітко оцінюють схильність до ризику постачальників першого рівня в процесі первісної оцінки та укладання контрактів. Зазвичай на цьому етапі відбувається невеликий огляд постачальників другого рівня. В результаті цього завантаженого інтерфейсом процесу огляду ризику кібератак може різко зрости після перших кількох місяців терміну дії договору і може продовжувати збільшуватися протягом терміну дії договору.

Для уникнення цієї загрози краще співпрацювати з невеликою кількістю перевірених постачальників, заключати з ними договори про аудит зі сторони замовника та постійний звіт про здійснення усіх заходів для забезпечення ефективного захисту інформації.

4. Різносторонні підходи до зменшення ризиків бути жертвою атаки

Керівники невеликих компаній помилково вважають, що їх бізнес не такий великий, щоб злочинці продумували атаку на нього, але це не так. По-перше атаку легше провести на таку компанію, бо вони навряд витрачають гроші на захист даних та створення і впровадження КСЗІ. По-друге кожна маленька компанія намагається працювати з великою, бо це постійний заробіток, тому злочинці використовують малі компанії як транспорт для інфікованого об'єкту. Ряд додаткових факторів, які також сприяють збільшенню ризику ланцюжка поставок, в тому числі:

- Зростаючий обсяг і серйозність кібератак, що виходять від окремих осіб, організацій та державних установ;
- Самозаспокоєність і / або нездатність як компанії-покупця, так і постачальника у моніторингу та оцінці реального / поточного кіберризику;
- Підвищення складності кібератак – деякі з яких працюють від імені іноземних урядів;
- Збільшення сміливості кібератак через нездатність ідентифікувати і бути осудженими;
- Зміна рівня толерантності до ризику в компанії;
- Хоча ризик кібератак на ланцюжок поставок не може бути усунутий, можна значно знизити ризик, навчаючи своїх постачальників і, прово-

дячи постійні перевірки для них на всіх рівнях. Цей контроль дуже важливий, оскільки компанії продовжують передавати стороннім постачальникам критично важливі внутрішні і клієнтські процеси.

Конкретні кроки, які характеризують цей недогляд, включають наступне:

- Контроль даних постачальників;
- Контроль місця і інформації, де фізично зберігаються дані;
- Контроль кількісті і імен системних адміністраторів у постачальників, які керують системами, які містять ваші дані;
- Шифрування даних при передачі;
- Гарантування, що все виправлення програмного забезпечення від відповідних постачальників програмного забезпечення встановлені на комп'ютерах ваших постачальників своєчасно;
- Переконайтеся, що політики постачальника щодо доступу до систем як для активних, так і для звільнених співробітників (включаючи зміну / скасування імені користувача і пароля) часто розглядаються / переглядаються всіма співробітниками;
- Перевірка політики постачальника щодо портативних пристроїв і безпеки технічних пристроїв;
- Перевірка постачальника процедур безпеки бездротової мережі і можливості моніторингу;
- Резервне копіювання всіх важливих даних здійснюється часто;
- Контролювання, що постачальники підтримують всі брандмауери та антивірусне програмне забезпечення до останніх версій;
- Регулярно перевіряйте всі права доступу / доступу до «критично важливих» файлів (піврічний аналіз бізнес-вимог для авторизації);
- Перевірка, що у вас є документований і протестований план аварійного відновлення та оповіщення про ризики.

Якщо у ланцюжку поставок відбувається кібератака, переконайтеся, що ваші постачальники виконують, як мінімум, наступне:

- Вжити негайних заходів, щоб визначити і ізолювати джерело атаки;
- Негайно обмежити доступ до всіх даних;
- Негайно повідомити про характер і серйозність атаки;
- При необхідності повідомити інших потенційно зачеплених постачальників;
- Переконайтеся, що план аварійного відновлення та оповіщення про ризики дотримується, а дії виконуються;
- При необхідності і з вашого попереднього письмового дозволу повідомте про це у відділ по боротьбі з кіберзлочинністю ДБР (Державного бюро розслідувань);
- Негайно перевірте, що всі міжмережеві екрани та антивірусне програмне забезпечення оновлено до останньої версії.

Висновки

Інформаційне суспільство розвивається і створює нові і складні способи викрадення дорогоцінної інформації.Нещодавно Міжнародна організація зі стандартизації прийняла новий стандарт ISO 27001. Як подальший розвиток цієї роботи планується порівняння вимог цього стандарту з вимогами ISO/IEC 27001, ISO/IEC 27002, а також розроблення методики його впровадження в Україні. Створити абсолютно захищену систему на практиці неможливо, але максимально захищену можна спробувати. Дотримання обережності з постачальниками, то добре керований ланцюжок поставок може затримати успішну атаку.

Перелік використаних джерел

1. M. Blackmer. Attacking the Weakest Link in the Supply Chain — Cisco Blog изд. — 2017. — Режим доступа: `https://blogs.cisco.com/security/attacking-the-weakest-link-in-the-supply-chain?dtid=osscdc000283`.
2. P. Moorhead. That Time Of Year Again: Cisco Systems Releases Its Annual Cybersecurity Report — Forbes изд. — 2018. — Режим доступа: `https://www.forbes.com/sites/patrickmoorhead/2018/`.
3. Cyber-security risks in the supply chain — Cert-uk изд. — 2015. — Режим доступа: `https://www.cert.gov.uk/wp-content/uploads/2015/02/Cyber-security-risks-in-the-supply-chain.pdf`.
4. R. WAUGH. The terrifying rise of cyber crime: Your computer is currently being targeted by criminal gangs looking to harvest your personal details and steal your money. — Mail Online изд. — 2013. — Режим доступа: `https://www.dailymail.co.uk/home/moslive/article-2260221/Cyber-crime-Your-currently-targeted-criminal-gangs-lo html`.
5. ISO/IEC 27001:2013, Information technology – Security Techniques – Information security management systems – Requirements — ISO изд. — 2013. — Режим доступа: `https://www.iso.org/isoiec-27001-information-security.html`.
6. ISO/IEC 28001:2007, Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance. — ISO изд. — 2007. — Режим доступа: `https://www.iso.org/standard/45654.html`.
7. E. Florio. The Unexpected Attack Vector: Software Updaters — RSA Conference изд. — 2017. — Режим доступа: `https://www.rsaconference.com/videos/the-unexpected-attack-vector-software-updaters`.