УДК 623.618

А.В. Снігуров, В.Ю. Балашов, А.Ю. Сердюк

Харківський національний університет радіоелектроніки, Харків

АНАЛІЗ МЕХАНІЗМІВ РЕАЛІЗАЦІЇ МЕРЕЖЕВИХ АТАК ПРИКЛАДНОГО РІВНЯ В ІНТЕРЕСАХ ПРОВЕДЕННЯ КРИМІНАЛІСТИЧНИХ РОЗСЛІДУВАНЬ КІБЕРЗЛОЧИНІВ

У статті описуються проблеми криміналістичного розслідування сучасних кібератак на елементи критичної інфраструктури України, акцентується увага, що одними з найбільш небезпечних є кібератаки на прикладному рівні моделі OSI. Приводиться аналіз механізмів реалізації найбільш розповсюджених типів кібератак прикладного рівня: SQL-ін'єкції, перехоплення сесії, отруєння кешу DNS, атаки на RDP та інші засоби віддаленого адміністрування. Особлива увага приділяється аналізу артефактів даних атак для створення методики проведення криміналістичного розслідування.

Ключові слова: *кібератаки, артефакти, криміналістичне розслідування.*

Вступ

З розвитком інформаційних технологій відбувається і розвиток кіберзлочинності, яка використовує у своїх протизаконних діях вразливості інформаційних систем. Останні три роки для України були особливо насичені інцидентами з порушення роботи елементів інформаційних та телекомунікаційних систем, що являють собою елементи критичної інфраструктури. Тільки за 2016 рік Службою безпеки України зафіксовано 247 кібератак на інформаційно-телекомунікаційні системи дипломатичних установ, правоохоронних структур, енергетичних ресурсів, ресурсів залізної дороги тощо [1]. Отримати подібну статистику для приватного та бізнес сектору на даний час не виявляється можливим, але можна впевнено стверджувати, що чисельні показники для даних секторів значно вищі.

Усі наведені вище факти свідчать про актуальність проблем забезпечення не тільки надійного захисту інформаційних систем, а й необхідності вивчення проблем сучасних інформаційних технологій, розуміння їх уразливостей, структуризації та систематизації інформації про методи нападу, і що особливо важливо, розвитку та удосконаленню методів та засобів криміналістичного розслідування складних кіберзлочинів.

На даний час існує значна кількість інформаційних джерел, які присвячені сучасним кібератакам та методам захисту від них інформаційних та телекомунікаційних систем [2–4 та інші]. Але недостатньо вивченим є аналіз кібератак з точки зору виявлення їх артефактів в інформаційній системі для проведення криміналістичного розслідування.

Метою дослідження є аналіз найбільш розповсюджених типів кібератак прикладного рівня мережевої моделі OSI (open system sinter connection basic reference model), вироблення розуміння на базі такого аналізу типів артефактів даних атак та місць їх зберігання в інформаційній системі для розробки методики проведення криміналістичного розслідування.

Виклад основного матеріалу

Класична класифікація мережевих атак базується на наслідковому факторі. Так, наприклад, окрему категорію становлять атаки "відмова в обслуговуванні» (Denial of Service, DoS), які призводять, як вбачається з назви, будь-яку мережну службу до такого стану, в якому вона не може відповідати своїм клієнтам вчасно і клієнти не дочікуються відповіді. Іншою категорією є атаки направлені на розкриття даних інформаційної системи, несанкціонований доступ до інформації, підвищення повноважень користувача, тощо. Таким чином, відповідно до такої класифікації атаки розділено на категорії за їх цільовою дією [5].

Також у сучасній науковій літературі часто можна зустріти класифікацію мережевих атак, в якій головним фактором є об'єкт атаки, наприклад атаки на інструментарій, на керуючі системи, на мережі, на головне обладнання тощо [6]. Крім зазначених, що зустрічаються найчастіше, можна знайти класифікації за різноманітними факторами, наприклад за характером впливу (активні та пасивні), за умовою початку здійснення впливу (по запиту від об'єкту, що атакується; по настанню очікуваної події на об'єкті, що атакується; безумовні), за наявністю зворотного зв'язку з об'єктом, що атакується (із зворотнім зв'язком, без зворотного зв'язку), за розміщенням атакуючого відносного об'єкту, що атакується (внутрисегментні та міжсегментні), за кількістю атакуючих (розподілені та нерозподілені), за рівнем моделі OSI, на якому здійснюється атака та ін.

На сьогоднішній день найбільша динаміка розвитку технологій, їх різноманіття та, як наслідок, найбільша кількість проблем забезпечення кібербезпеки зосереджені на сьомому, прикладному, рівні

моделі OSI. Вразливості перед різними типами атак частіше проявляються саме в програмних додатках, ніж в протоколах роботи мережі на нижчих рівнях (слід зазначити, що нижчі рівні також мають велику кількість технологічних проблем, що успішно експлуатуються зловмисниками, але вони краще вивчені та на ринку існує велика кількість методів їх вирішення). Глобальне вирішення проблем безпеки на сьомому рівні майже неможливе через відсутність уніфікації кінцевих програмних додатків. Кожен програмний додаток, що працює з мережею, піддатний у величезній мірі людському фактору – помилкам програмістів та інженерів, що створювали даний програмний продукт. Для зменшення ступеню людського фактору необхідно виконувати детальний аналіз кожного програмного додатку, що з'являється у світі, на предмет захищеності перед відомими методами атак. Звісно такий підхід на сьогоднішній день не уявляється можливим за безліччю причин, однією з яких є певні свободи в мережі. Слід відмітити, що деякі компанії, такі як Apple, частково реалізують даний підхід, вимагаючи від розробників мобільних додатків вихідні коди для аналізу. Надання вихідних кодів та їх відповідність певним стандартам, заданим компанією, включаючи аспекти безпеки, є обов'язковим для публікації додатку у AppleStore. Завдяки такому підходу, продукти Apple вже декілька років визнані одними з найбезпечніших. Враховуючи наведену вище характеристику сучасного стану на прикладному рівні моделі OSI, дуже важливо приділити особливу увагу атакам, що здійснюються на даному рівні, а точніше методам розслідування інцидентів в цілому.

Серед типових атак, які базуються на протоколах сьомого рівня, можна виділити: отруєння кешу DNS, маніпуляції з HTTP-сесіями, міжсайтовий скриптинг, розподілений відказ в обслуговуванні, SQL-ін'єкції тощо. При цьому слід пам'ятати, що у кожного протоколу прикладного рівня та кожного додатку, що працює за цим протоколом, завжди є індивідуальні вразливості, актуальні лише для певної версії програмного додатку [7]. Розслідування таких атак завжди складне, факт експлуатації таких уразливостей завжди важко доводити, чим завжди користується сторона захисту у судових процесах, захищаючи високотехнологічних злочинців. Для збільшення кількості артефактів, що свідчать про певні дії з експлуатації уразливостей та виконання атак, необхідно детально розглянути більшість типових атак прикладного рівня та визначити їх особливості, базуючись на яких можна достовірно стверджувати наявність атаки (тобто визначити їх артефакти).

SQL-ін'єкція

SQL-ін'єкція – це атака, при якій зловмисник виконує вставку шкідливого коду в рядки, що передаються на сервер СУБД для синтаксичного аналізу та виконання. Успішна реалізація SQL-ін'єкції, залежно від типу СУБД та умов впровадження, може дати можливість зловмиснику виконати довільний запит до бази даних (наприклад, прочитати вміст будь-яких таблиць, видалити, змінити або додати дані), отримати можливість читання та запису локальних файлів та виконання довільних команд на сервері. Як наслідок, зловмисник отримує доступ до конфіденційної інформації, що міститься в БД, і доступ до команд операційної системи сервера СУБД, тим самим роблячи його площадкою для подальших атак інших серверів, сервісів та застосувань, розташованих в корпоративній мережі організації.

Як правило, SQL-ін'єкції розглядають стосовно до веб-застосувань, але насправді до даних вразливостей схильні будь-які клієнт-серверні та сервіс-орієнтовані програми, що працюють з СУБД.

Типовими місцями зберігання артефактів SQL-ін'єкцій є файли журналів. Найважливішим серед усіх журналів при розслідуванні SQL-ін'єкцій є журнал веб-серверу. Саме його слід переглядати в першу чергу бо саме у ньому можна знайти записи як про факти виконаних атак, так і про їх невдалі спроби. Враховуючи, що у журналі містяться записи про невдалі спроби, то за допомогою журналу веб-серверу можливо встановлювати факт загрози на ранньому етапі.

Другим за важливістю є кеш планів виконання запитів. Виконання будь-якого запиту починається з його аналізу для складання плану його виконання. Складання плану виконання запиту дозволяє вибрати найбільш ефективний спосіб обробки даних з точки продуктивності. Після створення план виконання запиту кеширується в спеціальній структурі пам'яті – «процедурному кеші». Застосування такого кешу визволяє від необхідності повторного розбору аналогічних запитів [8].

Третім корисним джерелом артефактів є журнал транзакцій. Даний журнал уявляє собою послідовність записів про зміни в базі даних, починаючи з моменту її створення. З кожною операцією, що змінює дані, співвідноситься один запис у журналі. Принцип ведення журналу передбачає збереження запису про транзакцію до її фіксації. У разі виникнення збою та втрати частини бази даних, в журналі транзакцій повинно бути достатньо даних для її відновлення шляхом повторного виконання всіх операцій, що проводилися раніше.

Четвертим з найважливіших джерел артефактів є мітки часу в об'єктах бази даних. При оновлені чи створенні запису в базі даних одним з полів даних є мітка часу виконання даної події. Нажаль не всі бази даних автоматично фіксують такі мітки часу, так наприклад MySQL робить це лише частково, а PostgreSQL не фіксує міток часу у системній базі

даних взагалі. Не рідко таких функціонал реалізовується розробниками бази даних, що також доволі часто стає у нагоді при розслідуванні інцидентів, пов'язаних з базами даних.

Перехоплення сесії

Перехоплення сесії – це спосіб використання чужої сесії, при якому зловмисник вторгається в сесію між двома іншими вузлами. Зловмисник може отримати дійсний ідентифікатор сесії, який використовується для входу в систему і доступу до конфіденційної інформації.

Слід зазначити, що перехоплення сесій актуально на усіх рівнях моделі OSI, починаючи з транспортного (IP-spoofing), але у даній роботі розглянуті лише ті, що відносяться до прикладного рівня.

Процес викрадання сесії на прикладному рівні, як правило, може бути реалізований за допомогою одного з трьох способів:

1) Підбирання ідентифікаторів. Реалізується шляхом підбору потрібного ідентифікатора. Як правило, зловмисник має деякі знання про діапазон доступних значень ідентифікатора. Зловмисник може спиратись на використання HTTP-статистики веб-сайту, аналізатор трафіку, міжсайтовий скриптинг або шкідливі програми.

2) Викрадання ідентифікатора. Зловмисник може перехопити ідентифікатор за допомогою аналізатору трафіку або інших засобів.

3) Обчислення ідентифікаторів. Зловмисник спробує обчислити дійсний ідентифікатор сеансу проаналізувавши існуючі і виявивши послідовність.

Процес захоплення сесії відбувається наступним чином:

1. Спочатку виконується усе необхідне для отримання можливості прослуховування та подальшого аналізу трафіку між двома вузлами, між якими встановлена сесія, яку зловмисник намагається перехопити.

2. Моніторинг. Продовження аналізу трафіку з метою спостереження за поведінкою ідентифікаторів сесії.

3. Надалі – десинхронізація сесії, тобто розірвання сеансу між двома вузлами.

4. Прогнозування ідентифікатору сесії. Спроба відновлення сесії з новим ідентифіатором, але вже від імені зловмисника.

5. Експлуатація. На даному кроці зловмисник може відправляти власні команди на сервер для подальшого їх виконання.

Типи перехоплення сесій на прикладному рівні.

При спробі викрасти сесію на прикладному рівні, зловмисник може вибрати один з небагатьох видів атак: сніфінг сесії, передбачення маркерів сесії, «Людина-в-середені», «Людина-в-браузері».

Атака «сніфінг» сесії.Сніфінг сесії є варіацією сніфінгу, в цьому випадку, є конкретна задача, яку необхідно виконати – це визначення маркеру сеансу (також відомий як ідентифікатор сеансу). Після того, як зловмисник, знаходить цей маркер, використовує його, щоб отримати доступ до серверу або іншого ресурсу.

Атака «Прогнозування маркерів сесій».

Другий спосіб отримання ідентифікатору сеансу, це передбачити або зробити обґрунтоване припущення про те, яким буде справжній ідентифікатор. Найпростіший і найефективніший спосіб – це зібрати кілька ідентифікаторів сесії, які були використані до цього.

Атака «людина-по-середині».

Використовується для вторгнення у вже існуючий сеанс між вузлами для перехоплення повідомлень. Зловмисник використовує різні методи і розділяє TCP з'єднання на дві частини. Після успішного поділу TCP-з'єднання зловмисник може читати, змінювати та вставляти певні дані в перехоплені повідомлення.

Атака «Людина в браузері».

Четверта форма – браузерна атака, яка є особливо цікавою формою атак. Найбільш поширені форми загроз «людина в браузері» – міжсайтовий скриптинг, трояни і JavaScript. Міжсайтовий скриптинг (XSS), є типом атаки, який може виявлятися в різних формах, але зазвичай він задіяний, коли дані деякого типу вводяться в веб-застосування через неперевірені джерела (у більшості випадків – вебзапит). Зазвичай ці дані є частиною динамічного контенту, який не пройшов через перевірку гарантування захищеності. Особливість даних видів атака полягає в тому, що замість безпосередньої атаки сервера зловмисники використовують вразливий сервер для атаки на користувача.

Розслідування атак перехоплення сесій та міжсайтового скриптингу є надзвичайно складною задачею через дуже малу кількість артефактів та складність їх пошуку. Легше за все встановити первинні ознаки, що свідчать про факт перехвату сесії, це журнали веб-серверу та, в першу чергу, самого серверного програмного додатку. Артефактами можуть служити аномалії в хронології журналів та їх логіки. Наприклад, якщо користувач зазвичай використовує одну IP-адресу, але одноразово в журналі відображається інша, існує велика ймовірність, що мало місце перехоплення сесії користувача. При спробах виконання міжсайтового скриптингу часто можна знайти в журналах фрагменти JavaScript – коду.

Також артефакти деяких видів атак на перехоплення сесії можна знайти в кеші браузера, або ж, що простіше, знайти інструменти занесення до системи шкідливого програмного коду: файли троянів, клієнти ботнетів тощо, що може надати віддаленому

зловмиснику отримати доступ до сесії жертви. Слід звертати увагу на наявність таких артефактів серед видалених файлів системного розділу.

Отруєння кешу DNS

Отруєння кешу DNS – атака на DNS-сервер, для здійснення якої зловмисник, використовуючи недостатньо надійну конфігурацію служби серверу, вносить модифікації до DNS-кешу. Таким чином, усі клієнти DNS-серверу отримують контент зловмисника не зважаючи на те, що зверталися за вірним посиланням.

Виконання даної атаки зазвичай виконується за допомогою спеціальних сценаріїв (експлойтів). Такі сценарії експлуатують уразливість DNS-серверу в наслідок чого надають зловмиснику контроль над сервером або можливість запису у його кеш. Також зловмисник може використовувати з метою утворення зазначених вище наслідків недостатньо безпечну конфігурацію програмного забезпечення DNS-серверу.

Розслідування та доказування даного виду атаки на перший погляд виглядає простим: досить відобразити зміст кешу DNS-серверу та перевірити реальну відповідність доменних імен IP-адресам, зазначеним в кеші. Як свідчить практичний досвід, атака такого типу є складно доказуємою через недовговічність кешу та часті його перезаписи. Оскільки системні адміністратори зазвичай намагаються якомога скоріше виправити проблему і лише потім встановлювати причини її виникнення, кеш DNS-серверу, ймовірніше за все, буде очищений чи перезаписаний.

Найкращій спосіб доказування наявності даного типу атаки – це її невідкладне документування при свідках.

Атаки на RDP та інші засоби віддаленого адміністрування

Інструменти віддаленого адміністрування операційної системи набули сьогодні настільки великого поширення, що стали повсякденною нормою. Не зважаючи на це не рідко зустрічаються інциденти несанкціонованого втручання в систему через підбір слабкого паролю або через експлуатацію уразливостей програмного забезпечення.

Сервіси, що дозволяють віддалене підключення до операційної системи, завжди прослуховують певні порти, які доступні з публічних мереж, тобто до цих портів може підключитися будь-хто. Популярні засоби тестування на проникнення, наприклад Metasploit framework, містять в своїх колекціях велику кількість вже відомих експлойтів для несанкціонованого проникнення до системи шляхом експлуатації відомих уразливостей протоколів RDP, SSH, VNC, RAdmin та багатьох інших.

Розслідування подібних інцидентів, особливо у випадках підбору слабкого паролю, не є складним і найчастіше уся необхідна доказова база зберігається в журналах операційної системи або самого програмного засобу. У випадках експлуатації уразливостей розслідування стає набагато складніше і доказів може не залишитися взагалі. Для розслідування подібних випадків ефективним методом є пошук релевантних артефактів: корисних навантажень, що вкладаються до експлойтів. Це можуть бути трояни, засоби прихованого адміністрування, тощо. Тобто шукати треба програмні додатки чи сценарії, їх журнали, перевіряти їх наявність серед видалених даних, особливо в системних розділах. При знаходженні таких артефактів та їх співвідношенні з уразливою версією програмного забезпечення віддаленого адміністрування, можна робити певні висновки.

Висновки

Таким чином, аналіз наведених вище артефактів дозволяє розділити їх на типові групи за місцем зберігання, що надає можливості побудувати систему розпізнавання кібератак прикладного рівня:

1) самостійні файли;
2) файли інших програмних продуктів (порушення їх автентичності);
3) скритий простір файлових систем (видалені дані, slack-space, простір між розділами файлової системи);
4) файли журналів операційної системи та інших додатків;
5) файли підкачки;
6) оперативна пам’ять;
7) віддалені автоматизовані системи.

Очевидно, що артефакти кожного типу атак, що були проаналізовані у статті, можуть знаходитися у декількох перелічених групах (табл. 1).

Таблиця 1

Місяця зберігання артефактів атак прикладного рівня

Місця зберігання артефактів	Типи атак
1	2
самостійні файли	Перехоплення сесій; Отруєння кешу DNS; Уразливості до датків віддаленого адміністрування
файли інших програмних продуктів (порушення їх автентичності)	SQL-ін’єкції; Отруєння кешу DNS; Уразливості додатків віддаленого адміністрування
скритий простір файлових систем (видалені дані, slack-space, простір між розділами файлової системи)	Перехоплення сесій; Отруєння кешу DNS; Уразливості до датків віддаленого адміністрування

Закінчення табл. 1

1	2
файли журналів операційної системи та інших додатків	SQL-ін'єкції; XSS; Перехоплення сесій; Отруєння кешу DNS; Уразливості додатків віддаленого адміністрування
файли підкачки	XSS; Перехоплення сесій; Отруєння кешу DNS; Уразливості додатків віддаленого адміністрування
оперативна пам'ять	XSS; Перехоплення сесій; Отруєння кешу DNS; Уразливості додатків віддаленого адміністрування
віддалені автоматизовані системи	Перехоплення сесій; Отруєння кешу DNS; Уразливості додатків віддаленого адміністрування

Необхідно розуміти, що з перебігом часу артефакти можуть зникати з кожного із перелічених місць зберігання, тому оперативне реагування на інцидент та фіксація максимально можливої кількості артефактів у надійному місці зберігання, є надзвичайно важливою для успіху розслідування інциденту. Метою подальших досліджень є розробка методики розпізнавання кібератак прикладного рівня за їх артефактами для використання при проведенні криміналістичних досліджень.

Список літератури

1. Результати окремих напрямків роботи Служби безпеки України [Електронний ресурс] // Служба безпеки України. Офіційний веб-сайт. – 2016. – Режим доступу до ресурсу: https://ssu.gov.ua/ua/news/1/category/2/view/2474#sthash.ezdinA63.t38Oy3ez.dpbs.

2. Петренко С.С. Проблема обнаружения компьютерных атак в критически важных инфраструктурах / С.С. Петренко, А.В. Беляев // Защита информации. – 2008. – № 2. – С. 32-36.

3. Милокум Я.В. Метод последовательного обнаружения угроз компьютерной сети / Я.В. Милокум // Наукові записки Українського науково-дослідного інституту зв'язку. Науково-виробничий збірник. – 2008. – №4(6). – С. 79-88.

4. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы / А.Е. Боршевников // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). – Уфа: Лето, 2011. – С. 8-13.

5. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты / Ю.А. Родичев. – Учебное пособие. – Санкт-Петербург: Питер, 2008. – 272 с.

6. Надежны ли современные производственные системы? / Х. Тернер, Ж. Вайт, Х. Камелио та ін. // Открытые Системы. – 2015. – № 3. – С. 29-33.

7. Бирюков А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – М.: ДМК Пресс, 2012. – 474 с.

8. Вишневский А.В. Microsoft SQL Server. Эффективная работа / А.В. Вишневский. – Сакт-Петербург: Питер, 2009. – 541 с.

Надійшла до редколегії 27.05.2017

Рецензент: канд. техн. наук ст. наук. співробітник С.О. Сідченко, Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків.

АНАЛИЗ МЕХАНИЗМОВ РЕАЛИЗАЦИИ СЕТЕВЫХ АТАК ПРИКЛАДНОГО УРОВНЯ В ИНТЕРЕСАХ ПРОВЕДЕНИЯ КРИМИНАЛИСТИЧЕСКИХ РАССЛЕДОВАНИЙ КИБЕРПРЕСТУПЛЕНИЙ

А.В. Снегуров, В.Ю. Балашов А.Ю. Сердюк

В статье описываются проблемы криминалистических расследований современных кибератак на элементы критической инфраструктуры Украины, акцентируется внимание, что одними из самых опасных являются кибератаки на прикладном уровне модели OSI. Приводится анализ механизмов реализации наиболее распространенных типов кибератак прикладного уровня: SQL-инъекции, перехват сессии, отравление кэша DNS, атаки на RDP и другие средства удаленного администрирования. Особое внимание уделяется анализу артефактов данных атак для создания методики проведения криминалистического расследования.

Ключевые слова: *кибератаки, артефакты, криминалистическое расследование.*

ANALYSIS OF MECHANISMS OF NETWORK ATTACKS AT THE APPLICATION LAYER FOR CRIMINAL INVESTIGATIONS OF CYBER CRIMES

A. Snigurov, V. Balashov, A. Serdyk

The article describes problems of modern criminal investigation of cyber-attacks on elements of critical infrastructure in Ukraine. It is focused on cyber-attacks as one of the most dangerous attacks at the application level of the OSI model. The implementation mechanisms of the most common cyber-attack types at the application level are analyzed and include: SQL-injections, session interception, DNS cache poisoning, attacks on the RDP and other remote administration tools. Particular attention is paid to the analysis of these attacks artifacts in order to create methods of criminal investigation.

Keywords: *cyber-attacks, artefacts, criminal investigation.*