УДК 004.056.5

Слюсар Д. Ю.
Грицак А. В.

ВИЯВЛЕННЯ АТАК ОТРУЄННЯ DNS-КЕШУ З ВИКОРИСТАННЯМ МАШИННОГО НАВЧАННЯ

Вінницький національний технічний університет

Анотація

Проаналізовано проблему атак "отруєння кешу DNS" та їх вплив на безпеку комп'ютерних мереж. Розглянуто застосування методів машинного навчання для виявлення аномальних патернів у DNS-трафіку як підхід до боротьби з такими атаками.

Ключові слова: DNS-кеш, отруєння кешу, атаки, машинне навчання, виявлення аномалій, кібербезпека.

Abstract

The problem of "DNS cache poisoning" attacks and their impact on the security of computer networks is analyzed. The application of machine learning methods to detect anomalous patterns in DNS traffic is considered as an approach to combating such attacks.

Keywords: DNS cache, cache poisoning, attacks, machine learning, anomaly detection, cybersecurity.

Вступ

В епоху цифрових технологій і розповсюдження Інтернету, безпека комп'ютерних мереж та інформаційних систем стає все більш критичною. Одним з важливих компонентів, що забезпечує функціонування мережі Інтернет, є система доменних імен (DNS - Domain Name System). DNS перетворює людино-зрозумілі доменні імена в IP-адреси, необхідні для маршрутизації трафіку. Однак, DNS вразлива до атак «отруєння кешу», при яких зловмисники намагаються підмінити легітимні записи DNS невірними даними. Такі атаки можуть призводити до перенаправлення користувачів на шкідливі сайти, крадіжки конфіденційних даних, недоступність важливих мережевих служб, фінансові втрати та інших серйозних наслідків.

Постійність та еволюція атак DNS Cache Poisoning підкреслюють нагальну потребу у вдосконалених стратегіях виявлення та усунення наслідків. Традиційні заходи безпеки, хоча і є необхідними, виявилися недостатніми проти деяких складних атак, що призвело до нагальної потреби в інноваційних рішеннях. Метою цього дослідження є не тільки усунення безпосередніх загроз, пов'язаних з отруєнням кешу DNS, але й внесок у більш широку сферу кібербезпеки шляхом підвищення стійкості інфраструктури DNS за допомогою інтелектуальних, адаптивних засобів захисту.

У зв’язку з вище розглянутими аспектами, можна зробити висновок, що розробка ефективних методів виявлення та протидії атакам "отруєння кешу DNS" є актуальним завданням забезпечення кібербезпеки.

Результати дослідження

Атаки "отруєння кешу DNS" (DNS cache poisoning) є однією зі значних загроз безпеці інтернет-протоколів, особливо в контексті сучасного цифрового світу, де доступ до мережі є необхідністю. Ця форма атаки може призвести до серйозних наслідків, включаючи перенаправлення трафіку на веб-сайти зловмисників, крадіжку конфіденційних даних та порушення конфіденційності користувачів.

DNS дозволяє веб-користувачу повідомити доменне ім’я у своєму веб-браузері для доступу до веб-сайту. Потім браузер «розв’язує» це доменне ім’я, щоб отримати IP-адресу веб-сервера, який розміщує цей веб-сайт і відображає його. Даний процес називається «дозвіл DNS».

З основною функцією DNS (Domain Name System) пов'язані ключові аспекти функціонування інтернету, такі як перетворення доменних імен в IP-адреси. Однак, через цей процес також можуть виникати вразливості, які використовуються зловмисниками для отруєння кешу DNS. Це стає особливо

актуальним у сучасному світі, де безпека мережевих систем і захист від кіберзагроз стають все більшою проблемою [1].

На сьогоднішній день у світі Інтернету актуальність проблеми виявлення та реагування на атаки "отруєння кешу DNS" підкреслюється швидким розвитком технологій та зростаючою складністю мережевих середовищ. Сучасні атаки можуть бути здійснені з використанням різноманітних інструментів та методів, що вимагає від фахівців з кібербезпеки постійного вдосконалення методів виявлення та захисту [2].

У зв'язку з цим, розробка та впровадження ефективних та надійних захисних механізмів стають ключовим завданням для організацій, які прагнуть забезпечити безпеку своїх мереж та інфраструктури. Правильна реакція на потенційні загрози "отруєння кешу DNS" вимагає співпраці між фахівцями з кібербезпеки, мережевими адміністраторами та іншими зацікавленими сторонами, а також вдосконалення систем виявлення та моніторингу [3].

Так, використання машинного навчання для виявлення аномальних патернів може бути дуже корисним в контексті боротьби з атаками "отруєння кешу DNS". Машинне навчання може допомогти виявляти незвичайні та аномальні активності в мережі, які можуть свідчити про спроби атаки або зловмисну поведінку.

Машинне навчання (ML) є перспективним напрямком для покращення безпеки DNS, оскільки воно може виявляти аномальні патерни, що вказують на DoS-атаки. На відміну від традиційних механізмів безпеки, які покладаються на заздалегідь визначені підписи та шаблони, алгоритми ML можуть навчатися на даних і виявляти потенційні загрози на основі відхилень від встановлених норм. Ця функція особливо актуальна для отруєння кешу DNS, оскільки вектори атак постійно змінюються. За допомогою ML можна розробляти системи, які адаптуються до нових загроз і підвищують стійкість інфраструктури DNS до сучасних атак.

Розробка та впровадження систем виявлення на основі ML вимагає суворої методології. Це включає збір і попередню обробку даних DNS-трафіку, вибір і навчання відповідних моделей ML, а також постійне оцінювання та вдосконалення моделей для підтримки високої точності виявлення. Ефективність таких систем залежить від їхньої здатності збалансувати чутливість (здатність виявляти атаки) і специфічність (здатність уникати помилкових спрацьовувань), щоб гарантувати, що легітимний DNS-трафік не буде перехоплений неналежним чином.

Для розробки інтелектуальної архітектури системи, яка виявляє аномальні патерни в DNS-трафіку, необхідно спроектувати діаграму активності для візуалізації та аналізу процесів і взаємодії компонентів системи.

Діаграми діяльності - це тип діаграм, що використовується для моделювання послідовних кроків або дій у процесі. Діаграми діяльності використовуються для візуалізації послідовності подій, дій та обміну інформацією в системі. Діаграми діяльності часто використовуються для моделювання бізнес-процесів, програмного забезпечення або інженерних систем, щоб зрозуміти і відобразити їх логіку і функції.

Оскільки метою даної роботи є розробка системи захисту від DNS Cache Poisoning, головна задача роботи є розробка сервісу, що надасть користувачеві можливість виявляти аномальні патерни в DNS-трафіку.

Виходячи з мети системи, опишемо структуру сервісу наступним чином, розбивши її на етапи:

– отримання DNS-трафіку від користувачів або мережевих пристроїв;
– передача до системи аналізу;
– система використовує алгоритми машинного навчання для виявлення незвичайних патернів у DNS-трафіку;
– виявлення аномальних або підозрілих шаблонів у трафіку;
– створення звітів або сповіщень;
– виконання дій блокування;
– моніторинг та оновлення.

Залежно від серйозності аномалії, система може автоматично вжити заходів для мінімізації потенційних загроз. Про виявлені аномалії можуть бути створені звіти або надіслані оповіщення адміністратору для подальших дій.

На етапі моніторингу відбувається збір даних про DNS-трафік у мережі за допомогою різних засобів моніторингу та захоплення трафіку.

Вхідні дані отримуються від системи моніторингу та проходять первинну обробку, таку як фільтрація, нормалізація та перетворення даних у формат, придатний для подальшого аналізу.

Кластеризація та виявлення аномалій - це ключовий етап, на якому застосовуються алгоритми машинного навчання та аналізу даних для виявлення відхилень від нормального трафіку. Передбачається групування (кластеризація) даних на основі подібних характеристик.

На кроці перевірки на аномалії система визначає, чи є виявлене відхилення справжньою аномалією, що вимагає втручання, чи це легітимна поведінка. Якщо відхилення класифіковано як аномалію, система ініціює процес оповіщення адміністратора через відповідні канали сповіщення. Адміністратор має можливість проаналізувати інформацію про аномалію та вжити необхідних дій, наприклад, заблокувати певні IP-адреси чи домени. Результати дій адміністратора записуються до бази даних разом з іншими деталями виявленої аномалії. Якщо ж відхилення не було класифіковано як аномалія, дані про нього все одно записуються до бази даних для подальшого аналізу та навчання моделей.

Вихідні дані формуються на основі зібраної інформації про DNS-трафік, виявлені аномалії та дії адміністратора. Ці дані можуть використовуватися для подальшого аналізу, покращення моделей та звітності.

Висновки

Отже, значущість системи доменних імен (DNS) для функціонування Інтернету робить її привабливою мішенню для зловмисників, що використовують тактики отруєння кешу для перенаправлення користувачів на шкідливі сайти, що може призвести до втрати даних та порушення конфіденційності. Традиційні методи захисту, такі як статичні брандмауери і системи виявлення за сигнатурами, виявляються неефективними проти динамічних і адаптивних характерів цих загроз, що зумовлює необхідність використання передових технологій як машинне навчання для виявлення аномалій і проактивне управління безпекою.

Зловмисники, використовуючи ці атаки, намагаються вплинути на процес перетворення доменних імен у відповідні IP-адреси, що може призвести до серйозних наслідків для безпеки мереж та конфіденційності користувачів.

Для ефективного захисту від таких атак необхідно використовувати комплексний підхід, який включає в себе використання різноманітних методів та інструментів. Машинне навчання виявляється одним із потужних інструментів, які можуть бути використані для виявлення аномальних патернів у мережевому трафіку та ефективного реагування на них.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. DNS Security Guide [Електронний ресурс]: What is DNS Security. – Режим доступу: https://www.varonis.com/blog/dns-security . – Назва з екрана.

2. Global DNS Threat Report [Електронний ресурс]: DNS Report.– Режим доступу: https://efficientip.com/resources/idc-dns-threat-report-2020/. – Назва з екрана.

3. Anagnostopoulos, M., Kambourakis, G., Kopanos, P., Louloudakis, G., & Gritzalis, S. (2016). DNS amplification attack revisited. Computers & Security, 62, 214-225.

Слюсар Дмитро Юрійович – студент групи 1КІТС-20б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: dima.slyusar.2003@gmail.com.

Науковий керівник: ***Грицак Анатолій Васильович*** — доцент кафедри менеджменту та безпеки інформаційних системи, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м.Вінниця, e-mail: grytsak.a.v@gmail.com.

Sliusar Dmitro Y. – Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, , e-mail: dima.slyusar.2003@gmail.com.

Supervisor: **Hrytsak Anatoliy V.** — Associate Professor of the Department of Information Systems Management and Security, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: grytsak.a.v@gmail.com.