УДК 681.32

С. Р. Сирцов
С. М. Захарченко

Методи виявлення передавання прихованої інформації в службових заголовках протокольних блоків даних комп'ютерних мереж.

Вінницький національний технічний університет

Анотація

Проаналізовано можливі методи приховування даних в службових заголовках протокольних блоків даних та розроблено методи для їх виявлення.

Ключові слова: стеганографія, стегоконтейнер, приховані повідомлення, службові заголовки, мережеві пакети, перехоплення пакетів,, ідентифікатор пакету, тести на псевдовипадковість.

Abstract

Methods of hiding data in the service headers of protocol data blocks are analyzed and methods for their detection are developed.

Keywords: *steganography, stegocontainer, hidden messages, service headers, network packets, packet interception, packet identifier, pseudo-randomness tests.*

Вступ

Сучасні системи безпеки повинні захищати дані від різного роду загроз, таких як шпигунство, видалення файлів та інших несанкціонованих дій. Кожен із цих факторів може негативно вплинути на коректне функціонування локальної чи глобальної, що в свою чергу, нерідко приводить до втрати та розголошення конфіденційної інформації. Однією з найпоширеніших загроз в комп'ютерних мережах є несанкціонований доступ ззовні, який проводиться з метою перехоплення та заволодіння певною персональною інформацією. Ця інформація може бути лікарською, комерційною, банківською чи державною таємницею. Тому дуже важливо знизити ризик її потрапляння до рук сторонніх осіб. Програмні засоби захисту стають все глобальнішими та складнішими, але при цьому в них може збільшуватись кількість вразливих місць на більш низькому рівні. Є багато низькорівневих технологій та методів, які хакери використовують для передачі їх шкідливого коду в комп'ютерній мережі, оминаючи різного роду фільтри та фаерволи. Серед них особливе місце займають криптографія та стеганографія, оскільки вони є дуже спірними, бо призвані з одного боку навпаки захищати персональні дані.

Метою роботи є дослідження та вдосконалення методів виявлення передавання прихованої інформації в комп'ютерних мережах за допомогою протокольних блоків даних.

Результати дослідження

З початку XX століття і до сьогодні дуже активно розвивалась як сама стеганографія, так і суміжна їй наука — стегоаналіз. Стегоаналіз — це наука про виявлення факту вбудовування прихованої інформації в контейнер.

Сьогодні ми спостерігаємо за невтішними і загрозливими тенденціями, що все більше розробників шкідливого програмного забезпечення і засобів кібершпигунства надають перевагу використанню стеганографії. Більшість сучасних антивірусних систем не можуть гарантувати надійного захисту від подібного ПЗ, або не захищають взагалі. Хоча потрібно розуміти, що кожен такий заповнений стегоконтейнер становить загрозу для будь-якої локальної мережі. Він може містити приховані дані, які перехоплюються і витягуються шпигунським програмним забезпеченням, для зв'язку центральним сервером або оновлення для модулів шкідливої програми.

Виявлення і усунення зловмисного використання стеганографії, що відбувається в комп'ютерній мережі, є дуже важким. Згідно з Барвайзом(2018): «Якщо зловмисник може успішно проникнути в

мережу і, не викликаючи підозри, встановити шкідливе ПЗ, що використовує цифрову стеганографію для приховування своєї присутності, тоді і мережа і всі дані, які містяться в ній, можна вважати повністю скомпрометованими.(Теоретична основа)». Це хороший опис того, наскільки важко виявити і відреагувати на використання методів, що приховують дані проти ваших інформаційних ресурсів.

Можна явно виділити три основні причини чому автори шкідливого програмного забезпечення використовують стеганографічні методи в своїх розробках:

— стеганографія дозволяє приховати сам факт завантаження/ вивантаження даних, а не лише самі дані;

— дозволяє обійти DPI-системи, що зазвичай використовують в корпоративних мережах, де це актуальним;

— антивірусні системи взагалі мало що можуть зробити із заповненими контейнерами, їх практично нереально виявити, оскільки вони виглядають як звичайні пакети.

Коли діло доходить до засобів протидії стеганографії, то виникає серйозна проблема у вигляді великої різноманітності існуючих методів приховування інформації. Мережева стеганографія може застосовуватись не лише до різноманітних протоколів і мультимедійних даних, що передаються, а й з використанням різного роду методів приховування таких як: RSTEG, LACK, TranSteg, HICCUPS тощо. На даний момент відомо понад декілька сотень методів приховування інформації, включаючи їх комбінації. Навіть якщо не брати до уваги методи, що використовують корисне навантаження пакетів, то залишається більше сотні методів, які передають секретні дані з використанням метаінформації, такої як елементи службових заголовків прокольних блоків даних.

З іншого боку, контрзаходи не можуть покривати усі доступні стеганографічні методи одночасно через високу складність та різноманітність протоколів і сервісів, і впливають тільки на один чи декілька методів приховування кожен. Водночас, якщо засіб протидії спрямований на декілька методів приховування одночасно, то забезпечення високої точності залишається невирішеною задачею. Якщо ж створювати комплексні системи на основі найоптимальніших методів, то виявлення, обмеження та запобігання мережевої стеганографії стане ще більш складною задачею.

Як було розглянуто вище при створенні та відправці пакетів в мережі частина полів службових заголовків може не використовуватись. Наприклад, поле «Ідентифікатор пакету», що знаходиться в заголовку протоколу IPv4, не використовується, якщо не виконується фрагментація пакетів. Зазвичай це відбувається коли розмір корисного навантаження не перевищує максимально допустимий в мережі і пакет не потрібно ділити на окремі частини для передачі. В цьому випадку вміст поля «Ідентифікатор пакету» заповнюється за допомогою генерації псевдовипадкової послідовності.

Усі генератори чисел діляться на два типи: генератор справжніх випадкових чисел (ГСВЧ) та генератор псевдовипадкових чисел (ГПВЧ). Основна відмінність їх відмінність полягає в тому, що ГСВЧ створює числа на основі непередбачуваних фізичних явищ, наприклад, таких як шуми атмосфери, радіоактивний розпад або космічне випромінювання. Проте такі системи зазвичай дуже затратні в установці та експлуатації. Вигіднішою, але менш точною, альтернативою є ГПВЧ, які генерують числа за допомогою використання математичних алгоритмів, які повністю залежать від комп'ютера. Оскільки генератори справжніх випадкових чисел мають ряд недоліків, частіше використовуються генератори псевдовипадкових чисел. Головними недоліками ГСВЧ є:

— час та трудовитрати при установці та налаштуванні;

— дороговизна;

— генерація випадкових чисел відбувається повільніше, ніж при програмній реалізації ГПВЧ;

— неможливість відтворення послідовності випадкових чисел, що була згенерована раніше.

Водночас ГСВЧ залишається затребуваним, оскільки ГПВЧ не може генерувати настільки ж рівномірні послідовності з «більш випадковими» бітами. Послідовні значення в генераторі псевдовипадкових чисел все ж не є незалежними.

Велику роль грає операційна система, мова програмування та математичний алгоритм, за якими будувалась числова послідовність. Більшість ГПВЧ добре справляються зі своєю задачею, деякі навіть відмінно, проте жоден з них не є істинним.

Головною особливістю справжніх випадково згенерованих чисел є те, що отримана послідовність буде максимально рівномірно розподілена. Тобто такою, де кількість бітів одиниць буде рівною

кількості бітів нулів, при чому за кожною одиницею зазвичай буде слідувати нуль. Для перевірки псевдовипадкових чисел на їх істинність існують спеціально розроблені набори методів.

Тестування псевдовипадкових послідовностей — це сукупність методів визначення тотожності заданої псевдовипадкової послідовності до випадкової. В якості міри зазвичай виступає наявність рівномірного розподілу, великого періоду, рівної частоти появи однакових підрядків тощо. Існує дві основних категорії тестів: графічні та статистичні. До графічних відносяться тести, результати яких відображаються у вигляді графіків, що характеризують властивості досліджуваної послідовності. Їх результати інтерпретуються людиною, тому висновки на їхній основі можуть бути неоднозначними. Статистичні тести, на відміну від графічних, видають чисельну характеристику послідовності і дозволяють сказати однозначно, чи пройдений тест. Серед найвідоміших можна виділити тести Д. Кнута, DIEHARD, NIST.

Найбільш підходящі методи для тестування службових полів на псевдовипадковість містить набір статистичних тестів NIST.

Висновки

Розглянуто та проаналізовано методику, за якою створюються повідомлення-контейнери з вбудованою прихованою інформацією. Поетапно розглянута процедура генерування пакетів з вбудованими стеганограмами та процес атаки комп'ютерної корпоративної мережі з їх використанням. Були виведені основні положення щодо комплексу дій, які потрібно зробити для виявлення стеганогрфічних повідомлень всередині корпоративної мережі..

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Применение сетевой стеганографии для скрытия даних передаваемых по каналам связи [Електронний ресурс] — Режим доступу до ресурсу: https://cyberleninka.ru/article/n/primenenie-setevoy-steganografii-dlya-skrytiya-dannyh-peredavaemyh-po-kanalam-svyazi

2. Szczypiorski, K., Steganography in TCP/IP Networks. State of the Art and a Proposal of a New System— HICCUPS, Institute of Telecommunications' seminar, Warsaw University of Technology, Poland,November 2003, URL:http://krzysiek.tele.pw.edu.pl/pdf/steg-seminar-2003.pdf

3. Kundur D., Ahsan K., Practical Internet Steganography: Data Hiding in IP, Proc. Texas Wksp. Security of Information Systems, Apr. 20034.

4. Фороузан Б. А Криптография и безопасность сетей: Учеб. пособие: с англ. под ред. А. Н. Берлина. — М.: Интернет-Университет Информационных Технологий: БИНОМ. Лаборатория знаний, 2010. — 784 с.

Сирцов Сергій Романович – студент групи 1КІ-20м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: serhiisyrtsov@gmail.com.

Науковий керівник: ***Захарченко Сергій Михайлович*** — кандидат технічних наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, м.Вінниця, e-mail: <zahar@vntu.net>

Serhii Syrtsov – a student of group 1CE-20m, Faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: serhiisyrtsov@gmail.com.

Scientific supervisor: ***Zakharchenko, S.M.*** — Candidate of Technical Sciences, Associate Professor of Computer Technology, Vinnytsia National Technical University, Vinnitsa, e-mail: <zahar@vntu.net>