ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

ІМЕНІ ВАСИЛЯ СТУСА

КАФЕДРА РАДІОФІЗИКИ ТА КІБЕРБЕЗПЕКИ

**КУРСОВА РОБОТА**

з дисципліни «Стандартизація та сертифікація в галузі інформаційної безпеки»

на тему:

Методи деанонімізації при використанні TOR технологій

Студента 3 курсу

спеціальності/напряму підготовки

б17\_д/125А Кібербезрека

Рудого Максима Вікторовича

Науковий керівник:

к.т.н. Барибін О.І.

Національна шкала \_\_\_\_\_\_\_\_\_\_\_\_

Кількість балів \_\_\_\_\_\_\_\_\_\_\_

Шкала ECTS \_\_\_\_\_\_\_\_\_\_\_

Члени комісії:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ПІБ)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис) (ПІБ)

Вінниця 2020

**АНОТАЦІЯ**

Приховані сервіси Tor використовуються для надання послуг на основі TCP користувачам, при цьому не розкриваючи IP-адресу прихованого сервера, щоб отримати скритність і анти цензуру. Однак приховані сервіси використовуються різними способами. Приховані сервіси використовуються для незаконних цілей, таких як торгівля наркотиками, зброєю, розповсюдження порнографії і т. д. Через неправильне використання прихованих сервісів Tor, досліди для виявлення цих сервісів були неминучі.

У цій статті буде огляд існуючих атакуючих схем, їх порівняння, пояснення ключових ідей і показані їх взаємовідносини.

**ВСТУП**

Tor - це система анонімних комунікацій з малою затримкою, яка підтримує TCP-додатки через Інтернет, які надають користувачам такі послуги, як перегляд веб-сторінок, безпечна оболонка і обмін миттєвими повідомленнями. Він надає користувачам сервіс анонімності, допомагає обійти інтернет-цензуру і підтримує приховані сервіси для збереження анонімності веб-сервісів. В даний час Tor підтримує кілька мільйонів користувачів. Tor підтримує приховані сервіси, щоб зберегти непомітність цих веб-сервісів.

Приховані сервіси - це веб-сайти, розташовані всередині мереж Tor, які отримують вхідні повідомлення тільки через Tor. Tor необхідний для доступу до прихованим сервісів. Доступ до прихованих сервісів здійснюється через його цибульну адресу, що дозволяє користувачеві публікувати інтернет-сайти, приховуючи свою IP-адресу і місце розташування.

Однак приховані служби використовуються для незаконних сервісів, таких як інформація про торгівлю наркотиками, сайти дитячої порнографії, незаконна торгівля зброєю і т. д. На прихованих сервісах Tor існує багато чорних ринків. Шовковий шлях – був один з них, він широко займався контрабандою товарів з використанням біткоїнів в якості валюти.

Наразі існує безліч різних варіантів атак, що розкривають приховані служби Tor. Розкриваючи ці приховані сервіси з’явиться змога закрити ті приховані служби які розміщують нелегальний контент. Таким чином, у цій роботі ми зосередимось на існуючих схемах атак, їх порівнянні та принципах роботи. Порівнюючи їх, можна буде зрозуміти плюси і мінуси кожної схеми, і, таким чином, можна буде застосувати відповідну схему для деанонімізації прихованої служби.

**РОЗДІЛ 1. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ТЕХНОЛОГІЮ TOR**

* 1. **Мережа Tor**

Tor – це оверлейна мережа на рівні додатків, яка дозволяє здійснювати анонімний обмін даними між її клієнтами та довільними інтернет – адресами з допомогою цибулевої маршрутизації. Клієнти здійснюють анонімний зв’язок із сервером, тунелюючи свій трафік через ланцюжок із трьох ретрансляторів Tor. У цьому розділі ми спочатку ознайомимось із мережею Tor, а потім ознайомимось із її базовими операціями та протоколами прихованих сервісів.

1. **Огляд мережі**

Тор – це оверлейна мережа для анонімного зв’язку, в якій кожен цибулевий маршрутизатор (ЦМ) працює як звичайний процес на рівні користувача без будь – яких особливих привілеїв. Це проект із відкритим вихідним кодом який забезпечує сервіс анонімності для додатків TCP. Кожний (ЦМ) підтримує TLS з’єднання із кожним (ЦМ). Кожний користувач запускає локальне програмне забезпечення яке називається onion proxy (OP), для вибору каталогів, встановлення каналів в мережі і опрацювання з’єднань із клієнтськими додатками. Ці (OP) приймають TCP потоки і мультиплесують їх по каналам. (ЦМ) на іншій стороні ланцюга з’єднуються із запрошеними адресами і передають дані. Рисунок 1.2.1 ілюструє базову архітектуру мережі Tor. Наступні компоненти беруть участь в типовому використані мережі Tor.



Рисунок 1.2.1

* Tor клієнти: Клієнт Tor запитує дані для завантаження з сервера. Він встановлює локальне програмне забезпечення, onion proxy (OP), в якому дані додатки упаковуються в осередок однакового розміру (512 байт) і доставляють їх у мережу Tor. Осередок - це основний блок передачі Tor.
* Цибулеві маршрутизатори (onion router): OR - це реле, добровільно запропоноване різними волонтерами по всьому світу.
* Сервери каталогів: Сервери каталогів містять інформацію про операції OR і прихованих службах, таких як відкриті ключі маршрутизаторів і прихованих серверів.
* Сервери додатків: Він підтримує програми TCP, такі як веб-служба та служба IRC.

1. **Приховані сервіси**

Tor забезпечує анонімність для веб-сайтів та інших серверів. Сервери, призначені для прийому вхідних з'єднань тільки через Tor, називаються прихованими сервісами. Замість того, щоб розкривати IP-адресу сервера, до прихованого сервісу звертаються через його цибульний адрес, який є хешем його відкритого ключа. Прихований сервіс Tor складається з наступних важливих вузлів:

* Introduction Point (IP): Це реле Tor, які вибираються прихованими сервісами і використовуються для встановлення зв'язку з клієнтом.
* Rendezvous Poin (RPO): вони вибираються клієнтом Tor і використовуються для пересилання даних між клієнтом і прихованим сервером.
* Directory Server (DS): DS володіє інформацію про вузли мережі Tor, і ця інформація використовується для зв'язку з прихованими сервісами.
* Hidden server (HS): це сервер всередині мережі Tor, на якому розміщені приховані сервіси.

Принцип роботи прихованої служби заснований на підключенні двох ланцюгів, одного створеного клієнтом, а іншого - HS, на загально узгодженому реле Tor. Це реле Tor, таким чином, називається Rendezvous Poin, яка передає осередок шляхом пересилання вихідних повідомлень із схеми на стороні клієнта до ланцюга на стороні сервера та навпаки. Щоб захистити RPO від атак, прихована служба вибирає групу реле Tor як точки введення, які працюють так само, як RPO. IP-адреси використовуються виключно для передачі одного повідомлення, що містить розміщення обраного RPO. Що стосується лише прийняття запитів клієнта, прихована служба публікує прихований дескриптор служби, що містить підписаний список IP-адрес для DS, звідки клієнти можуть їх завантажувати.

Нормальне налаштування зв'язку між клієнтом та конкретним HS показано на рисунку 1.3.1. Процедура цього повідомлення полягає в наступному:

1. HS спочатку вибирає декілька OR в якості IP і будує схеми до цих IP, надсилаючи повідомлення RELAY\_COMMAND\_ESTABLISH\_INTRO, а IP у відповідь відповідає повідомленням RELAY\_COMMAND\_INTRO\_ESTABLISHED, щоб повідомити HS про те, що схема встановлена.
2. Як тільки схеми до IP встановлені, HS встановлює ланцюг до DS та оголошує дескриптор служби DS, включаючи відкритий ключ HS та інформацію щодо IP. Тоді власник HS може розмістити цибулеву адресу у громадському місці, щоб залучити користувачів до доступу до прихованого сервісу через Tor.
3. Коли клієнт Tor отримує цибулеву адресу, клієнт створює схему DS і отримує відповідну інформацію, оголошену прихованою службою. Потім клієнт дізнається IP прихованої служби.
4. Тепер клієнт вибирає RPO і створює схему для RPO. Клієнт відправить повідомлення RELAY\_COMMAND\_ESTA-BLISH\_RENDEZVOUS, яка містить cookie-файл рандеву, і RPO який відповідає повідомленням RELAY\_COM-MAND\_RENDEZVOUS\_ESTABLISHED, щоб підтвердити успішне встановлення каналу.
5. Клієнт створює схему трьох стрибків для одного з IP і передає повідомлення RELAY\_COMMAND\_INTRODUCE1 на обраний IP. В команді зберігається така інформація, як RPO, cookie-файли рандеву і дані Діффі-Хеллмана які генерується клієнтом Tor.
6. Як тільки IP отримує повідомлення RELAY\_COMMAND\_INTRODUCE1, він відповідає клієнтові RELAY\_COMMAND\_INTRODUCE\_ACK. Після того, як клієнт отримає це повідомлення ACK, він розриває цю схему до IP.
7. IP перепаковує повідомлення RELAY\_COMMAND\_INTRODUCE1 у повідомлення RELAY\_COMMAND\_INTRODUCE2, а потім відправляє повідомлення RELAY\_COMMAND\_INTRODUCE2 в HS. Як тільки HS отримує це повідомлення, вона знає інформацію про RPO, файли cookie та дані Діффі-Хеллмана . HS може генерувати дані Діффі-Хеллмана і отримати ключ K = .
8. Тоді HS будує ланцюг до RPO та посилає в RPO повідомлення RELAY\_COMMAND\_RENDEZVOUS1 до RPO. Коли RPO отримує це повідомлення, вона порівнює переглянуті cookie з повідомлення та те, що йде від клієнта Tor. Після того, як файли cookie, що переглядаються, збігаються, RPO видаляє файли cookie, що переглядаються, з повідомлення RELAY\_COMMAND\_ RENDEZVOUS1 і перепаковує рештe даних у повідомлення RELAY\_COMMAND\_RENDEZVOUS2, а потім пересилає повідомлення клієнту.
9. Коли клієнт Tor отримує повідомлення RELAY\_COMMAND\_RENDEZVOUS2, він може генерувати ключ K = ., використовуючи , і перевірити його на основі H (K). Таким чином клієнт та HS завершують рукостискання. Потім клієнт відправляє повідомлення RELAY\_COMMAND\_BEGIN для встановлення потоку в HS через шість стрибків.
10. Коли клієнт відправляє повідомлення RELAY\_COMMAND\_BEGIN до HS, щоб відкрити потік між клієнтом і HS, наш контрольований RPO виявляє це спеціальне повідомлення на основі прихованого протоколу обслуговування

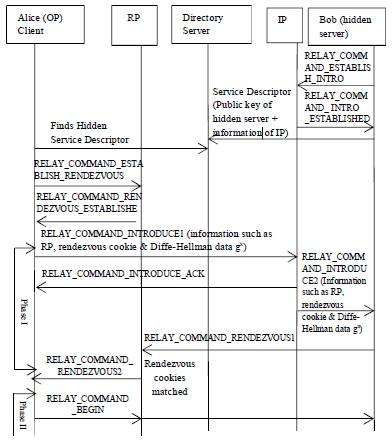


Рисунок 1.3.1