УДК 004.056.5

АТАКА ІНФРАСТРУКТУРИ НА ОДНОРАНГОВУ ПІРИНГОВУ МЕРЕЖУ BITCOIN

П.І. СТЕЦЕНКО, О.О. ПЕРЕКОПСЬКИЙ, Г.З. ХАЛІМОВ

Представлена атака інфраструктури на однорангову пірингову мережу Bitcoin. Ця атака відноситься до класу атак на таблиці маршрутизації. Дозволяє зловмиснику контролювати трафік атакованого вузла. Проаналізовано три можливі теоретичні сценарії, які можуть мати місце при атаці інфраструктури: блок таблиці перевірених адрес від початку пустий, використання Bitcoin витискання та випадкового витискання. Отримані кількісні оцінки очікуваної кількості вставлених зловмисником адрес для кожного розглянутого сценарію. Встановлено, що найбільш сприятливим для зловмисника є сценарій від початку порожнього блоку. А найбільш ефективним з погляду безпеки є випадкове витискання.

Ключові слова: атака інфраструктури, криптовалюта Bitcoin, однорангова пірингова мережа, таблиця перевірених адрес, мережна інформація, одноранговий вузол.

ВСТУП

Сьогодні впроваджується широке коло децентралізованих систем у різні сфери економіки та бізнесу. У своїй більшості ці децентралізовані системи мають архітектуру, яка є аналогічною архітектурі криптовалюти Bitcoin. Як основа передачі інформації Bitcoin використовує коцепцію однорангової пірингової мережі. Взагалі архітектуру даної криптовалюти можна подати у вигляді трьох рівней: однорангова пірингова мережа, технологія Blockchain та протокол безносередньо криптовалюти Bitcoin.

Безпека однорангової пірингової мережі, зокрема, аналіз уразливостей окремих компонентів механіз-му зберігання мережної інформації, залишається маловивченою, в той час як безпека самого протоколу криптовалюти Bitcoin вивчена досить широко [1 – 5]. Атака інфраструктури належить до класу атак на таблиці маршрутизації. Успішна реалізація даної атаки дозволить зловмиснику реалізовувати атаки на вищі рівні архітектури з меншою складністю. Таким чином, аналіз проведення атаки інфраструктури в одноранговій піринговій мережі Bitcoin є актуальним завданням.

1. МЕХАНІЗМ РОЗПОВСЮДЖЕННЯ ТА ЗБЕРІГАННЯ МЕРЕЖНОЇ ІНФОРМАЦІЇ

Механізм розповсюдження та зберігання мережної інформації докладно описаний у роботах [6, 7].

Розповсюдження мережної інформації. Мережна інформація поширюється по мережі Bitcoin за допомогою DNS-сідерів і ADDR повідомлень.

Розмір списку обмежений рамками DNS, тому, максимально можлива кількість IP-адрес, які можуть бути повернуті за допомогою одного запиту DNS, становить близько 4000. DNS-сідер отримує адреси шляхом періодичного збору даних мережі Bitcoin. Мережа Bitcoin має шість DNS-сідерів, які запитуються лише у двох випадках. Перший випадок – коли новий вузол вперше приєднується до мережі. Вузол намагається підключитися до DNS-сідерів для отримання списку активних IP-адрес. Другий – коли існуючий вузол перезавантажується і перепідключається до нових однорангових вузлів. У цьому випадку DNS-сідер запитується тільки після 11 секунд з того моменту як вузол почав намагатися встановити з'єднання і має менше двох вихідних з'єднань.

Одноранговий вузол заноситься в чорний список, якщо з нього було відправлено ADDR повідомлення, що містить більше 1000 адрес. Вузли приймають незапрошені ADDR повідомлення. ADDR повідомлення запитується тільки при встановленні вихідного з'єднання з одноранговим вузлом. Одноранговий вузол відповідає на 1 – 3 ADDR повідомлень, кожне з яких містить до 1000 адрес, випадковим чином вибраних зі своїх таблиць. Одноранговий вузол відправляє в цілому n випадково вибраних адрес з таблиць перевірених і нових адрес, де n випадкове число в інтервалі $[x; 2500]$, а x – 23% від кількості адрес, що зберігаються одноранговим вузлом.

Вузли направляють ADDR повідомлення одноранговим вузлам у двох випадках. Перший випадок – кожен день вузол відправляє свою власну IP-адресу в ADDR повідомленні кожному одноранговому вузлу. Другий – коли вузол приймає ADDR повідомлення з не більше, ніж 10 адресами, повідомлення пересилається на два підключених однорангових вузла, обраних випадковим чином. Особливо, якщо ADDR повідомлення містить адреси, які не можуть бути маршрутизовані для однорангового вузла. ADDR повідомлення пересилатимуть тільки одному одноранговому вузлу, якщо, наприклад, одноранговий вузол з IPv4-адресою отримав IPv6-адресу. Для вибору цих однорангових вузлів, вузол приймає геш IP-адреси кожного підключеного однорангового вузла і секретне випадкове слово (nonce), пов'язане з днем. Вузол вибирає однорангові вузли з лексично першим і другим геш-значеннями. Кожен вузол зберігає відомий список адрес, які він відправив або дізнався від кожного з підключених до нього однорангових вузлів. Слід зазначити, що вузол ніколи не розсилає адреси за відомим списком своєму одноранговому вузлу. Це необхідно для запобігання нескінченного поширення

застарілих ADDR повідомлень. Відомі списки скидаються щодня.

Зберігання мережної інформації. Під мережною інформацією розуміють зовнішні IP-адреси. Адреси зберігаються в таблицях перевірених і нових адрес вузла. У таблиці перевірених адрес міститься 64 блоки, які, в свою чергу, можуть зберігати до 64 унікальних адрес для однорангових вузлів, з якими вузол успішно встановив вхідне чи вихідне з'єднання. Також вузол зберігає мітку часу, яка ставиться на останнє успішне підключення до даного однорангового вузла.

Слід зазначити, що кожна IP-адреса відображатиметься в окремому блоці в таблиці перевірених адрес. В свою чергу, кожна група відображатиметься не більше, ніж в чотири блоки. Після успішного підключення вузла до однорангового вузла, адреса однорангового вузла вставлятиметься до відповідного блоку в таблиці перевірених адрес. У разі, якщо блок повністю заповнений адресами, тобто містить 64 адреси, використовуватиметься механізм Bitcoin витискання. Даний механізм передбачає такі етапи:

- вибір чотирьох адрес з блоку таблиці перевірених адрес випадковим чином;

- заміна адреси з найстаршою міткою часу адресою нового однорангового вузла в таблиці перевірених адрес;

- вставка адреси в таблицю нових адрес.

Кожна адреса *a*, яка вставляється в таблицю нових адрес, відноситься до групи і групи джерел. Група містить IP-адресу підключеного однорангового вузла або DNS-сідера, від якого вузол дізнався адресу *a*.

Кожна пара (група, група джерел) гешуватиметься в один блок в таблиці нових адрес. Кожен блок містить унікальні адреси. Механізм Bitcoin витискання застосовуватиметься над усіма 64 адресами блоку, коли блок повністю заповнений. Витискання адреси на користь нової адреси буде здійснюватись у разі, коли:

- будь-яка з адрес має мітку часу, що перевищує 30 днів;

- будь-яка з адрес має занадто багато невдалих спроб підключення.

В іншому випадку механізм Bitcoin витискання використовується з невеликою зміною – адреса, яка витискатиметься, відкинеться. У разі, якщо адреса оголошується відразу декількома одноранговими вузлами, її можна відображати в кілька блоків.

2. АТАКА ІНФРАСТРУКТУРИ

Визначення. Атака інфраструктури – атака, що відноситься до класу атак на таблиці маршрутизації, в якій атакуючий контролює кілька блоків IP-адрес і може перехопити Bitcoin трафік, який надсилається на будь-яку IP-адресу в блоці, тобто він утримує множинні набори адрес в одній і тій же групі.

Зловмисник має адреси в *s* різних групах джерел. Група джерел містить IP-адреси передавальних одноранговых вузлів. Визначається, наскільки може бути заповнена таблиця перевірених адрес зловмисником, контролюючим *s* груп джерел, які містять *t* IP-адрес/груп.

Оцінка атаки інфраструктури. В атаці інфраструктури, кількість груп джерел *s* обмежена, а кількість груп *g* необмежена. Можемо розрахувати кількість блоків, заповнених групами джерел *s*, з використанням леми [8]:

$$\mathrm{E}[\mathrm{N}] = 256\left(1-\left(\frac{255}{256}\right)^{32s}\right). \qquad (1)$$

Таким чином, очікується заповнення ≈ 251 з 256 нових блоків із $s = 32$ групи.

Кожна пара (група, група джерел) відображає унікальний блок у таблиці нових адрес, і кожен з блоків у таблиці нових адрес може містити 64 адреси. Використовується Bitcoin витискання і передбачається, що кожний блок у таблиці нових адрес повністю заповнений легітимними адресами, які мають більш старі мітки часу, ніж усі адреси, що вставлені зловмисником за допомогою ADDR повідомлень. Оскільки всі *a* адрес у конкретній парі (група, група джерел) відображаються в одному блоці, то це означає, що число адрес, які насправді зберігаються в цьому блоці, задається $E[Y_a]$ за допомогою рекурентного співвідношення таких виразів:

$$E[Y_a \mid Y_{a-1}] = Y_{a-1} + 1 - \left(\frac{Y_{a-1}}{64}\right)^4, \qquad (2)$$

$$E[Y_1] = 1. \qquad (3)$$

При $a = 125$ адрес, зловмисник очікує перезапис $E[Y_a] = 63{,}8$ з 64 легітимних адрес у блоці. Таким чином, необхідно, щоб кожна група джерел мала 32 однорангових вузла, а кожен одноранговий вузол має відправляти ADDR повідомлення з вісьмома різними групами, що складаються з $a = 125$ адрес. Таким чином, існує $g = 32 \times 8 = 256$ груп у групі джерел, що є максимальним числом груп, доступних у блоці зі сміттям IP-адрес. Кожен одноранговий вузол передає рівно одне ADDR повідомлення з $8 \times 125 = 1000$ адресами, в цілому $256 \times 125 \times s$ різних адрес, які були надіслані усіма одноранговими вузлами. Слід зазначити, що існує 2^{24} адреси в 252.0.0.0/8 блоці, отже всі ці адреси різні, якщо $s < 524$.

Ресурси для початку атаки інфраструктури. Для того, щоб визначити які організації мають достатню кількість ресурсів (IP-адрес) для запуску атак інфраструктури, використовуються дані CAIDA's та AS [9, 10] з липня 2015 року, а також інформацію з бази даних RIPE [11]. Таким чином, отримані результати свідчать, що вже існувало 448 організацій з більш ніж $s = 32$ групами джерел і з, щонайменше, $t = 256$ адресами в кожній групі. Отже, якщо ці організації виділяють $\tau_\ell = 5$ годин на атаку з часом раунду $\tau_\alpha = 27$

хвилин, то ймовірність успіху атаки інфраструктури перевищує 80%.

Інтернет-провайдери в різних країнах утримують достатню кількість груп джерел ($s \geq 32$) для цієї мети; наприклад, Судан (Sudanese Mobile), Колумбія (ETB), ОАЕ (Etisalat), Гватемала (Telgua), Туніс (Tunisia Telecom), Саудівська Аравія (Saudi Telecom Company) і Домініка (Cable and Wireless). В США Міністерство внутрішніх справ має достатню кількість груп джерел ($s = 35$), так само як і в Південній Кореї Міністерство інформації і зв'язку має ($s = 41$) груп джерел тощо [9].

Оцінка кількості непустих блоків при заданій кількості груп джерел в атаці. Моделюється процес наповнення таблиці перевірених адрес (відповідно до розділу 1), ґрунтуючись на тому, що чотири незалежні геш-функції відображають кожну з s груп джерел в один із 64 блоків у таблиці перевірених адрес. Нехай $\Gamma \in [0,64]$ підраховує кількість непустих блоків у таблиці перевірених адрес. Знайдемо із використанням леми очікувану кількість непустих блоків при заданій кількості груп джерел s:

$$E[\Gamma] = 64\left(1-\left(\frac{63}{64}\right)^{4s}\right) \approx \left(1-e^{-\frac{4s}{64}}\right). \qquad (4)$$

Виходячи з виразу (4) очевидним є заповнення 55,5 з 64 блоків з $s = 32$, і всіх інших блоків, крім блоку з $s > 67$ груп джерел. Графік залежності очікуваного числа непустих блоків у таблиці перевірених адрес і кількості груп наведено на рис. 1.

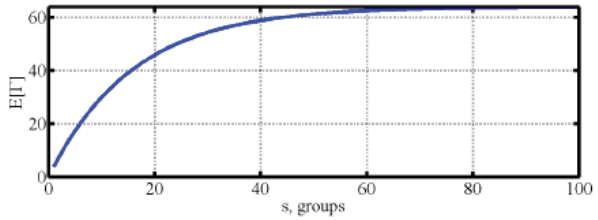


Рис. 1. Графік залежності очікуваного числа непустих блоків $E[\Gamma]$ в таблиці перевірених адрес і кількості груп джерел s

Успіх атаки інфраструктури залежить у великій мірі від τ_ℓ (часу, витраченого на реалізацію атаки) і f (частини, що складають адреси зловмисника в таблиці перевірених адрес). Щоб визначити скільки адрес повинен контролювати зловмисник для заданого значення f, в роботі використовується імовірнісний аналіз. Слід зазначити, що навіть якщо значення f мале, атакуючий все ще може досягти успіху шляхом збільшення τ_ℓ. Як було сказано в розділі 1, Bitcoin гарантує, що вузол не зберігає занадто багато IP-адрес з однієї і тієї ж групи (тобто /16 адрес IPv4 в блоці адрес).

Оцінка кількості адрес зловмисника у кожному блоці таблиці перевірених адрес. Визначимо тепер у в кожному блоці таблиці перевірених адрес, за умови, що t адрес міститься в кожній групі. Для цього спочатку необхідно знайти скільки різних адрес гешуються в даний блок, а потім знайти, скільки з цих адрес насправді зберігатиметься в блоці.

Кількість адрес, що гешуються в блок. Кожна група робить 4 рівномірних випадкових вибори одного з 64 можливих блоків у таблиці перевірених адрес. З огляду на окремий блок i, ймовірність того, що одна група гешується в блок i, становить:

$$P_{1/\alpha} = 1-\left(\frac{63}{64}\right)^4 \approx \frac{1}{16}, \qquad (5)$$

де α означає, що вибраний один із 64 можливих блоків.

Якщо G_i підраховує кількість різних груп, гешувальних в блок i, то G_i біноміально розподілено як $G_i \sim B(s, P_{1/\alpha})$. Кількість адрес, що гешуються в блок i, є випадковою змінною $A_i \sim B(gt, P_{1/4})$ за умови, якщо $G_i = g$ груп гешуються в блок i та кожна група містить t адрес, що гешуються в окремі блоки (кількість цих блоків може досягати чотирьох). Ця кількість адрес матиме такий розподіл:

$$\Pr[A_i = a] = \sum_{g=0}^{s} \Pr[B(gt, P_{1/4}) = a] \Pr[B(s, P_{1/\alpha}) = g], \qquad (6)$$

де A_i – кількість адрес, що гешуються в блок;

a – кількість адрес у групі;

s – кількість груп джерел;

g – кількість груп;

t – кількість адрес зловмисника у групі.

Очікуване значення кількості адрес, що гешуються в блок i дорівнює:

$$E[A_i] = \frac{t}{4}\frac{s}{\alpha}.$$

Ця оцінка є заниженою. Передбачається, що кожна група гешується рівно в 4 блоки. На практиці група може відображатися в Z блоків, де Z – випадкова величина в інтервалі $\{1,2,3,4\}$. Випадкова величина $Z-1 \approx B\left(3, \frac{63}{64}\right)$ має біноміальний розподіл і $E[Z] = 1+3\frac{63}{64} = 3.95$. Слід зазначити, що така занижена оцінка є доречною, тому що необхідно визначити скільки потрібно адрес атакуючому для заповнення блоку.

Розрахунок розподілу A_i проводився з виразу (6) та наведений на рис. 2 [7].

Розподіл має загострену форму, де перший пік відповідає $G_i = 1$, тобто, одна група гешується в блок i, другий пік відповідає $G_i = 2$ тощо. Більш того, в той час як важко побачити на графіку, існує також мала ймовірність того, що $A_i = 0$. Така ймовірність виникає, коли $G_i = 0$.

Кількість адрес, що зберігаються в блоці. Тепер, коли відомо, що A_i адрес гешуються в блок i, необх ідно з'ясувати, скільки з цих адрес насправді зберігатиметься в блоці. Розглянемо можливі теоретичні сценарії, у яких: блок від початку пустий, використо-

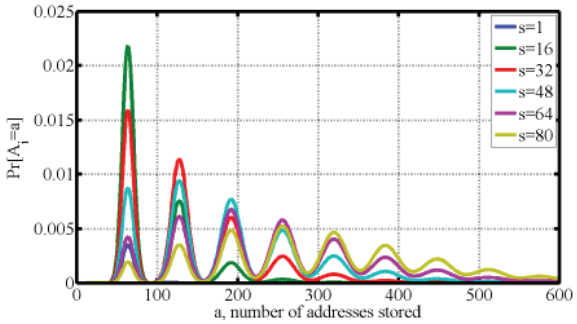


Рис. 2. Розподіл A_i для різної кількості груп s та з t = 256 адресами в групі

вується Bitcoin витискання та випадкове витискання.

1) Блок від початку пустий. У кращому випадку для атакуючого блок i спочатку пустий. Очікувана кількість адрес, які в кінцевому випадку зберігатимуться в блоці i, враховуючи, що, щонайменше, одна група гешується в блок i:

$$E\left[\min\left(64, A_i\right) | G_i > 0\right]. \quad (7)$$

Це величина, яка становить інтерес, тому що, якщо жодна з груп не відображається в блок i, блок не може бути заповнений за рахунок збільшення кількості адрес зловмисника в кожній групі t; замість цього необхідно збільшувати кількість груп джерел s.

2) Bitcoin витискання. У гіршому випадку для атакуючого, припускаємо, що блок i повністю заповнений 64 легітимними адресами. Нехай Y_a – кількість адрес зловмисника, котрі дійсно зберігаються в блоці i, враховуючи, що зловмисник вставив a унікальних адрес у блок i. Якщо використовується механізм Bitcoin витискання, $E\left[Y_a\right]$ задається рекурентним співвідношенням з виразів (2), (3). Очікувана кількість адрес, збережених у блоці i, за умови, що, щонайменше, одна група гешується в блок i, дорівнює:

$$\sum_{a=0}^{st} E\left[Y_a\right] \Pr\left[A_i = a \,|\, G_i > 0\right]. \quad (8)$$

Дану кількість адрес можна обчислити кількісно шляхом об'єднання рекурсії для $E\left[Y_a\right]$ і розподілу A_i з виразу (6).

3) Випадкове витискання. Передбачається, що блок i повністю заповнений легітимними адресами, але тепер щоразу, коли адреса вставляється, її витискає випадково вибраний адрес. Якщо Y_α визначається, як зазначено вище, то в силу леми і підставляючи вираз (9) в (8), отримуємо очікуване число адрес зловмисника, збережених у блоці i, за умови, що, щонайменше, одна група гешується в блок i:

$$E\left[Y_a\right] = 64\left(1 - \left(\frac{63}{64}\right)^a\right). \quad (9)$$

Ступінь заповнення таблиці перевірених адрес. Очікувана кількість адрес зловмисника, вставлених у таблицю перевірених адрес при атаці інфраструктури з 32 групами, для трьох теоретичних сценаріїв у співвідношенні з різною кількістю адрес в кожній групі наведено на рис. 3.

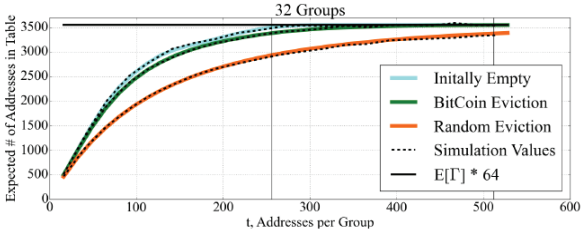


Рис. 3. Очікувані кількості вставлених адрес зловмисника для різних сценаріїв

Результати обчислені з виразів (4), (7) та (8). Горизонтальна лінія становить собою всі $E[\Gamma]$ блоки з виразу (4).

Отже, найпростішим теоретичним сценарієм для зловмисника сценарій від початку пустих блоків або коли проводиться достатня кількість раундів, одного раунду /24 блоку при t = 256 адрес. Цього достатньо, щоб заповнити кожен блок, використовуючи s = 32 груп. З 32 групами по 256 адрес кожна (8192 адреси в цілому) зловмисник може заповнити таблицю перевірених адрес на приблизно f = 86% після достатньої кількості раундів. Зловмисник майже так само ефективний в сценарії Bitcoin витискання, використовуючи тільки один раунд, але один раунд набагато менш ефективний порівняно зі сценарієм випадкового витискання.

Розмір таблиць перевірених адрес і нових адрес. У гіршому випадку для атаки таблиці перевірених і нових адрес мають бути повністю заповненими новими адресами. Таблиці нових адрес Bitcoin вузлів заповнюються досить швидко – ступінь заповнення 99% досягається протягом 48 годин. У таблиці перевірених адрес міститься невелика кількість нових адрес. Навіть після закінчення 43 днів, таблиця перевірених адрес була заповнена не більше, ніж на 300/4096 ≈ 8% [7]. Це пояснюється тим, що до вузлів приходить занадто мало вхідних з'єднань від публічних IP-адрес. Таким чином, більшість записів у таблиці перевірених адрес є результатом успішних вхідних з'єднань від публічних IP-адрес, узятих з таблиці нових адрес.

ВИСНОВКИ

Представлена атака інфраструктури на однорангову пірингову мережу Bitcoin. Атака відноситься до класу атак на таблиці маршрутизації, дозволяє зловмиснику контролювати трафік атакованого вузла. Головною вразливістю, що дозволяє реалізувати цю атаку, є механізм Bitcoin витискання. Механізм призначений для оновлення адрес у таблиці маршрутизації у випадку, коли вона повністю заповнена й існують нові адреси для підключень. Використовуючи механізм витискання, зловмисник має можливість вставити свої адреси у таблицю перевірених адрес цільового вузла.

У роботі розглянуто три можливі теоретичні сце-

нарії, які можуть мати місце при атаці інфраструктури: блок таблиці перевірених адрес від початку пустий, використання Bitcoin витискання та випадкового витискання.

Для зловмисника найпростішим сценарієм буде, коли всі блоки від початку порожні або коли атака проводиться в достатню кількість раундів. Цього достатньо, щоб заповнити кожен блок, використовуючи s = 32 груп. З 32 групами по 256 адрес кожна (8192 адреси в цілому) зловмисник може заповнити таблицю перевірених адрес на приблизно f = 86%, після достатньої кількості раундів.

Сценарій випадкового витискання є більш ефективним з точки зору складності реалізації атаки інфраструктури.

Підвищення складності реалізації атаки інфраструктури фактично полягає лише у збільшенні кількості необхідних зловмиснику ресурсів для досягнення прийнятного ступеня наповненості таблиці перевірених адрес.

Література:

[1] Courtois N. T. Bahack L. On subversive miner strategies and block with holding attack in Bitcoin digital currency / N. T. Courtois, L. Bahack. – arXiv preprint: 1402.1718. – 2014. – 29 p.

[2] Eyal I., Sirer E. G. Majority is not enough: Bitcoin mining is vulnerable / I. Eyal, E. G. Sirer // In Financial Cryptography and Data Security. – Springer. – 2014. – P. 436 – 454.

[3] Johnson B. Game-theoretic analysis of ddos attacks against Bitcoin mining pools / Johnson B., Laszka A., Grossklags J., Vasek M. and Moore T. // In Financial Cryptography and Data Security. – Springer. – 2014. – P. 72 – 86.

[4] Kroll J. A., Davey I. C., and Felten E. W. The economics of Bitcoin mining, or Bitcoin in the presence of adversaries. In Proceedings of WEIS (2013). – 2013. – 32 p.

[5] Shomer A. On the phase space of block-hiding strategies // IACR Cryptology ePrint Archive. – 2014. – 139 p.

[6] Decker C., Wattenhofer R. Information propagation in the Bitcoin network // In IEEE Thirteenth International Conference on Peer-to-Peer Computing (P2P). – IEEE. – 2013. – P. 1 – 10.

[7] Mille, A., Litton J., Pachulski A. Discovering bitcoin's network topology and influential nodes. Tech. rep., University of Maryland. – 2015. – 73 p.

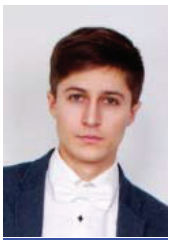
[8] Singh A., Ngan T.-W. J., Druschel P., Eclipse attacks on overlay networks: Threats and defenses. In IEEE INFOCOM. – 2006. – 68 p.

[9] CAIDA. AS to Organization Mapping Dataset. – (Дата звернення 27.10.2016).

[10] CAIDA. Routeviews prefix to AS Mappings Dataset for IPv4 and IPv6. – (Дата звернення 27.10.2016).

[11] RIPE. Ripestat // [Electronic resource]: https://stat.ripe.net/data/announced-prefixes.

Стеценко Павло Ігорович аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: захист інформації в децентралізованих системах.



Перекопський Олександр Олександрович аспірант кафедри БІТ ХНУРЕ. Область наукових інтересів: методи захисту інформації.

Халімов Геннадій Зайдулович, доктор технічних наук, професор кафедри БІТ ХНУРЕ. Область наукових інтересів: криптографія на групах.

УДК 004.056.5

Атака инфраструктуры на одноранговую пиринговую сеть Bitcoin. / П.И. Стеценко, А.А. Перекопский, Г.З. Халимов // Прикладная радиоэлектроника: науч.-техн. журнал. – 2016. – Том 15, №. 3 – С. 240 – 244.

Представлена атака инфраструктуры на одноранговую пиринговую сеть Bitcoin. Эта атака относится к классу атак на таблицы маршрутизации. Позволяет злоумышленнику контролировать трафик атакованного узла. Проанализированы три возможных теоретических сценария, которые могут иметь место при атаке инфраструктуры: блок таблицы проверенных адресов изначально пустой, применение Bitcoin вытеснения и случайного вытеснения. Получены количественные оценки ожидаемого количества вставленных злоумышленником адресов для каждого рассматриваемого сценария. Установлено, что наиболее благоприятным для злоумышленника сценарий изначально пустого блока. А наиболее эффективным с точки зрения безопасности является случайное вытеснение.

Ключевые слова: атака инфраструктуры, криптовалюта Bitcoin, одноранговая пиринговая сеть, таблица проверенных адресов, сетевая информация, одноранговый узел.

Ил.: 03. Библиогр. 11 наим.

UDC 004.056.5

Infrastructure attack on a Bitcoin peer-to-peer network. / P.I. Stetsenko, A.A. Perekopskiy, G.Z. Khalimov // Applied Radio Electronics: Sci. Journ. – 2016. – Vol. 15. №. 3 – P. 240 – 244.

An infrastructure attack on a Bitcoin peer-to-peer network is presented**.** This attack belongs to a class of attacks on routing tables. This attack allows an attacker to control the traffic of the attacked node. Three theoretical scenarios have been considered which could take place in an infrastructure attack: a block in the table with cheked addresses is initially empty, using of Bitcoin eviction and random eviction. Quantitative assessments of the expected number of embedded malicious addresses for each considered scenario have been obtained. It is found that the most favorable scenario for the attacker is the initially empty block. And the most effective in terms of security is random eviction.

Keywords: infrastructure attack, Bitcoin cryptocurrency, peer-to-peer network, table with checked addresses, network information, peer.

Fig.:03. Ref.: 11 items.