doi:https://doi.org/10.15407/emodel.40.05.067

УДК 004.7

В.Ю. Зубок, канд. техн. наук
Ін-т проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України
(Україна, 03164, Київ-164, вул. Генерала Наумова, 15,
тел. (+38044) 4241063, e-mail: vitaly.zubok@gmail.com)

Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі інтернет

Атака на глобальну маршрутизацію здатна нанести шкідливий вплив на мільйони мережевих пристроїв (і користувачів) значно меншими зусиллями, ніж широко відомі атаки класу DoS чи Ransomware. Попри фундаментальність протокол глобальної маршрутизації BGP-4 не є безпечним, оскільки оснований на довірі між учасниками глобальної маршрутизації. Розглянуто напрямки протидії, які дозволяють досягти зменшення можливих збитків від атак на глобальну маршрутизацію на рівні великого оператора, галузі, регіону. Запропоновано два напрямки: запобігання перехопленню маршрутів до власних префіксів та виявлення маршрутів до перехоплених префіксів і блокування трафіку до цих префіксів. Перший напрямок сформульовано як задачу пошуку найбільш ефективної топологічної організації зв'язків на рівні глобальної маршрутизації в мережі Інтернет, що забезпечить мінімізацію втрат від перехоплення маршруту в межах певної цільової групи вузлів.

К л ю ч о в і с л о в а: глобальна маршрутизація, перехоплення маршрутів, оптимізація зв'язків, кібербезпека.

Про предмет дослідження. Глобальна маршрутизація забезпечується десятками тисяч Інтернет-провайдерів. Протокол маршрутизації BGP-4 забезпечує поширення інформації про зв'язність і доступність мереж серед всіх вузлів Інтернету. За допомогою BGP-4 кожна мережа повідомляє своїм «сусідам» (peers) інформацію про підключені до неї сусідні мережі, а також про ті мережі, які опосередковано доступні через сусідів [1]. Ця інформація постійно оновлюється в процесі обміну між автономними системами і формує для кожного вузла так звану глобальну таблицю маршрутизації. В результаті кожна мережа знає (з різним ступенем деталізації), як досягти будь-якої ділянки глобальної мережі.

Незважаючи на фундаментальність протокол BGP-4, закладений на довірі між з'єднаними мережами, сприймає отриману від них інформацію за щиру правду. Більш того, ця довіра має транзитивну властивість, а саме: сусіди довіряють своїм сусідам, ті, в свою чергу, — своїм, і в підсумку всі

довіряють всім. На рівні протоколу BGP-4 немає перевірок достовірності даних, перевірок авторства анонсів або повноважень робити певний анонс. Також немає механізмів перевірки автентичності атрибутів шляху, які можуть вплинути на перевагу маршруту. Тобто вузол мережі (на рівні глобальної маршрутизації він називається автономною системою) може повідомити про те, що знає маршрут до префікса, до якого не має відношення; що маршрут через нього є коротшим, а отже,— кращим; що певну підмережу підключено безпосередньо до нього. Це призводить до випадків так званого перехоплення маршрутів (route hijacking, prefix hijacking, BGP hijacking). Колись ці перехоплення носили характер випадкової помилки конфігурації, але є впевненість, що протягом п'яти років зросла частка ворожих дій, тобто атак, для реалізації яких використовувалося перехоплення маршрутів.

Попри різноманіття сучасних кібератак найбільш небезпечними вважаються найбільш поширені, а саме атаки, спрямовані на відмову (Denial of Service (DoS)), і атаки, спрямовані на здирництво (Ransomware) [2]. Ці атаки є комплексними, бо мають принаймні дві фази: фазу інфікування та активну фазу. Фаза інфікування є відносно довгою. В деяких випадках вона триває декілька діб, а в деяких — місяці, в залежності від вибірковості зараження. У випадку атак класу DoS інфіковані елементи однієї підмережі (так звані боти) часто використовуються для атак на іншу мережу. У випадку атак класу Ransomware активна фаза атаки спрямована безпосередньо на користувачів тієї мережі, де ці боти «оселилися».

За даними Cybersecurity Ventures втрати від Ransomware в 2017 р. сягнули п'яти мільярдів доларів США [3]. Але в останні роки все частіше спостерігаються інциденти з глобальною маршрутизацією в Інтернеті, які перетворюються на нову масштабну кіберзагрозу. Дотепер жодного разу офіційно не заявлено, що ці інциденти були атаками. Втім, масштаб цих інцидентів на кілька порядків перевищує широко відомі атаки класу DoS і Ransomware. Таким може стати і масштаб збитку, оскільки атака на глобальну маршрутизацію здатна нанести шкідливий вплив на мільйони мережевих пристроїв (і користувачів) значно меншими зусиллями, ніж згадані вище популярні атаки.

Актуальність проблеми. Операторам та провайдерам Інтернет добре відомі деякі інциденти з перехопленням маршрутів [4—6]. Зокрема відомі такі випадки успішної атаки на сектор криптовалют та підозри про атаку на фінансовий сектор:

лютий 2008 р. — «захоплення» сервісу YouTube, що трапилось через дії пакістанських провайдерів, які виконували завдання свого уряду по блокуванню контенту в цьому сервісі;

лютий—березень 2014 р. — перехоплення трафіку до майнінгових пулів криптовалют Bitcoin, Dogecoin, HoboNickels та Worldcoin через передачу фальсифікованих анонсів;

квітень 2017 р. — перехоплення Ростелекомом маршрутів через анонсування протягом деякого часу значної кількості префіксів, які належали міжнародним платіжним системам та фінансовим сервісам;

серпень 2017 р. — перехоплення трафіку Google багатьох операторів в Японії внаслідок технічної помилки конфігурування маршрутизаторів (за поясненням винуватця);

грудень 2017 р. — перехоплення трафіку Google, Facebook, VK.com та інших відомих контент-провайдерів оператором з Хабаровська.

Одним з основних завдань системи розподілу адресного простору Інтернет є забезпечення унікальності розподілених ресурсів в глобальному масштабі. Використання в глобальному Інтернеті одного і того ж адресного простору кількома мережами призводить до порушення функціонування цих мереж, оскільки система маршрутизації Інтернет діє за принципом: кожний кінцевий пристрій має унікальну адресу. Для контролю за глобальним розподілом понад 20 років тому було введено в експлуатацію кілька баз даних Інтернет-маршрутів (Internet Routing Registry (IRR)), якими опікуються п'ять авторизованих регіональних реєстрів, що уповноважені виконувати розподіл IP-адрес і номерів автономних систем [7].

Структура взаємодії мереж в Інтернеті в багатьох випадках не є ієрархічною або не відповідає структурі розподілу адрес. Прикладом є пірингові взаємодії між мережами, або відносини клієнта з Інтернет сервіс-провайдером, в разі, коли клієнт має власний незалежний адресний простір. У таких випадках провайдери покладаються на публічно доступні реєстраційні дані, які мали б міститись в IRR. Але якість інформації, що розміщена у цих джерелах, є суттєво різною. Чим менші об'єкти реєстрації (мережі, маршрути та ін.) та чим ближче вони до кінцевого користувача, тим менше довіри до того, що наведені дані дійсно відображають поточну політику маршрутизації суб'єктів, до яких ці дані мають відношення.

Іншою проблемою є те, що достовірність даних неочевидна для третіх осіб. Найчастіше перевірка достовірності перетворюється в детективне розслідування з залученням різних джерел. Для валідації джерел анонсів розроблено та адаптовано інфраструктуру публічних ключів для ресурсів (RPKI) [8]. Але це вирішує лише питання авторизації внесення змін в IRR та валідації інформації про приналежність мережевих префіксів. Залишається проблемою добровільність реєстрації та актуалізації даних в IRR і, як наслідок, — відсутність повноти та достовірності даних, необов'яз-

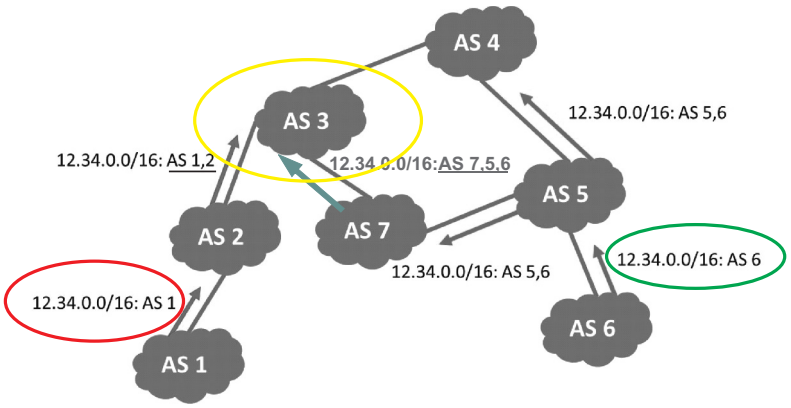

Рис. 1. Перехоплення маршруту вибором коротшого шляху: AS6 надсилає істинний анонс, AS1 — хибний, який конкурує з істинним за критерієм коротшого шляху; для AS3 хибний маршрут матиме перевагу через меншу довжину

ковість імплементації даних IRR для конфігурації маршрутизаторів та погана масштабованість процесу такої побудови.

Постановка задачі. Проведені дослідження американського Національного інституту стандартів та технологій свідчать про те, що підозріла активність не припиняється, особливо в нерозподіленому адресному просторі. Масштаб загроз, пов'язаних з атаками на Інтернет-маршрутизацію, дозволяє зробити висновок про необхідність всебічного аналізу цієї проблеми.

На даний час відсутні перспективи впровадження в світовому масштабі нового, більш захищеного протоколу глобальної маршрутизації. З огляду на це актуальними задачами є:

аналіз механізмів проведення атаки в залежності від її цілей;

визначення напрямків протидії, що зможуть позитивно вплинути на зменшення масштабу атаки та на розміри її наслідків.

Аналіз механізмів проведення атаки в залежності від її цілей. Атака класу BGP hijacking має кілька варіантів реалізації:

1. Захоплення префіксу, коли вузол анонсує у якості джерела адресний простір, який йому не належить. При виборі маршруту BGP віддасть перевагу більш короткому маршруту, вимірюваному числом мереж між джерелом і одержувачем. Цей маршрут конкуруватиме з істинним (рис.1). Така атака може бути швидко виявлена, бо з точки зору глобальної маршрутизації наявність двох джерел в одного префікса є помилкою.

2. Захоплення маршруту, в якому вузол ретранслює легально отриманий анонс чужого адресного простору, пропонуючи транзит через себе.

Цей маршрут буде також конкурувати з істинним, проте, на відміну від попереднього випадку, джерело не підмінюється і виявити такий інцидент значно складніше.

3. Захоплення підмереж через анонсування більш специфічних префіксів. При виборі маршруту BGP обирає той, який вказано більш специфічним префіксом, і таким чином атакуючий виграє, незважаючи на топологічну віддаленість. За відсутності конкуруючих префіксів такого ж розміру захоплення має глобальний ефект (рис. 2).

4. Захоплення нерозподіленого або невикористаного адресного простору. Анонсований префікс не зустрічає конкуренції і має високі шанси поширення по всьому Інтернету.

5. Перенаправлення трафіку. Трафік доставляється коректному одержувачу, але передається шляхом, відмінним від істинного.

Наслідки цих атак можуть бути різними. Захоплення маршруту призводить до перетягування трафіку, призначеного для захопленої мережі, який зазвичай потім відкидається. Така стратегія має назву створення «чорної діри» (blackholing). Таким чином відбувається DoS-атака на всі сервіси мережі. У цю категорію потрапляє більшість помилок конфігурації. Якщо атака анонсує фрагмент нерозподіленого адресного простору (нічиї мережі), вона може бути використана для короткострокової генерації не просто трафіку, а для доставки шкідливого контенту, тобто елементарно — для розсилки спаму.

Інший варіант стратегії — перенаправлення трафіку. Трафік йде не в «чорну діру», а перехоплюється і аналізується. Іноді атака ще більш глибока, і перехоплений трафік не тільки не йде в «чорну діру» і аналізується,

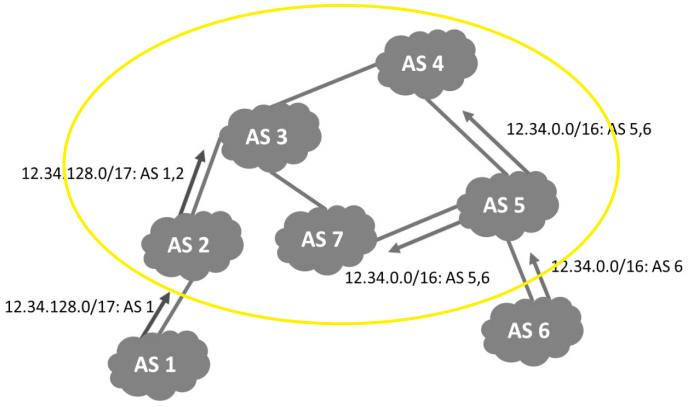

Рис. 2. Захоплення маршруту через анонсування більш специфічного префіксу: AS6 надсилає істинний анонс, AS1 — більш специфічний та перехоплює трафік у глобальному масштабі

але після перехоплення повертається знову в Інтернет, щоб бути доставленим істинному одержувачу. Таку атаку важче виявити. Метою може бути не тільки підслуховування, але і модифікація переданих даних. У більш витонченому вигляді захоплення маршруту може бути спрямоване на захоплення деякого інформаційного ресурсу, наприклад веб-сайту, з наданням користувачам підробленого сайту.

Визначення напрямків протидії атакам на глобальну маршрутизацію. Система RPKI може спростити варіанти атак 1—3 і 5. Однак слід зазначити, що система RPKI не є вирішенням проблем безпеки, оскільки рішення про впровадження додаткових заходів (наприклад, додаткових перевірок при наданні транзиту мережі або фільтрація маршрутів) залишається за мережевим оператором. Хід імплементації захищеного протоколу DNS Security Extensions (DNSSEC), основною метою якого є перевірка цілісності та валідації джерела DNS-відповіді, свідчить про те, що повному переходу на DNSSEC досі заважають відносна складність налаштування доменних зон та відсутність готових рішень рівня Інтернет-користувача, хоча впровадження DNSSEC відбувається понад десять років [9].

З урахуванням відсутності швидких перспектив впровадження в світовому масштабі нового, більш захищеного, протоколу глобальної маршрутизації, маючи знання про будову і динаміку топології Інтернет, необхідно, поєднавши теорію з практикою, розробити напрямки протидії, які можна було б застосовувати на рівні великого оператора, галузі, регіону, і досягти зменшення можливих збитків від атак на глобальну маршрутизацію. З цією метою пропонується два загальних напрямки:

запобігання перехопленню маршрутів до власних префіксів;

виявлення маршрутів до перехоплених префіксів та блокування трафіку до цих префіксів.

Як свідчать принципи організації глобальної маршрутизації та протокол BGP-4, основним транзитивним параметром, який характеризує привабливість маршруту, є довжина шляху (AS_PATH) (див. рис. 1). Довжина шляху — це фактор, який дозволяє маршрутам конкурувати до однакових префіксів. Інтернет на цьому рівні являє собою незважений граф, вершинами якого є автономні системи. В загальному випадку граф є циклічним та обов'язково зв'язним. Математично цей граф можна представити або квадратною матрицею суміжності, або квадратною матрицею відстаней розмірності N, де N — кількість вузлів [10].

Якщо існує підмножина вузлів, об'єднана якоюсь сутністю, топологію цієї підмножини можна розглядати окремо. Назвемо цю підмножину цільовою групою вузлів. Такою групою можуть бути вузли — учасники

будь-якої мережі обміну трафіком чи вузли-клієнти одного провайдера доступу до мережі Інтернет. Якщо зловмисник вдало провів перехоплення маршруту чи захоплення префіксу, це означає, що для певної цільової групи вузлів маршрут до префікса жертви через вузол зловмисника став коротшим, ніж інші природні маршрути, а отже, буде перехоплено трафік до цього префіксу від згаданої групи вузлів. Відтак, задачу запобігання перехопленню власних маршрутів слід визначити як пошук найбільш ефективної топологічної організації зв'язків, що забезпечить мінімізацію втрат від перехоплення маршруту в межах певної цільової групи вузлів.

Висновки

Масштаб загроз, пов'язаних з атаками на Інтернет-маршрутизацію, свідчить про те, що необхідний всебічний аналіз даної проблемної області та пошук методів моніторингу і оперативного виявлення не тільки поодиноких, але і групових відхилень в глобальній маршрутизації. Ці методи матимуть важливе значення для кіберзахисту як на корпоративному рівні, так і на рівні критичної інфраструктури держав.

Розуміння принципів функціонування протоколу глобальної маршрутизації і практичних завдань, які стоять при побудові взаємодії з Інтернет, а також механізмів кібератак на маршрутизацію надає можливість пошуку вирішення задачі мінімізації втрат від перехоплення маршруту з використанням найбільш ефективної топологічної організації зв'язків на рівні глобальної маршрутизації мережі Інтернет.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. *Rekhter Y., Li T., Hares S.* A Border Gateway Protocol 4 (BGP-4). [Електронний ресурс] Режим доступу: https://tools.ietf.org/html/rfc4271. Дата доступу: 29 червня, 2018 р.
2. *Internet* Security Threat Report 2018. [Електронний ресурс]. Режим доступу: https://www.symantec.com/security-center/threat-report. Дата звернення: 10 травня, 2018 р.
3. *Cybercrime Magazine*. Global Ransomware Damages Predicted To Exceed $5 Billion In 2017. [Електронний ресурс] Режим доступу: https://cybersecurityventures.com/ ransomware-damage-report-2017-5-billion/. Дата звернення: 05 травня, 2018 р.
4. *The Next Web.* Google made a tiny error and it broke half the internet in Japan. [Електронний ресурс] Режим доступу: https://thenextweb.com/google/2017/08/28/google-japan-internet-blackout/. Дата звернення: 20 квітня, 2018 р.
5. *Goodin D.* Russian-controlled telecom hijacks financial services' Internet traffic. [Електронний ресурс] Режим доступу:https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/. Дата звернення: 1 грудня, 2017 р.
6. *Hijacking Bitcoin*: routing attacks on cryptocurrencies. [Електронний ресурс] Режим доступу: ttps://blog.acolyer.org/2017/06/27/hijacking-bitcoin-routing-attacks-on-cryptocurrencies/. Дата звернення: 1 грудня, 2017 р.

7. *MERIT.* List of Routing Registries. [Електронний ресурс] Режим доступу: http://www.irr.net/docs/list.html. Дата звернення: 29 червня, 2018 р.
8. *RIPE* NCC. BGP Origin Validation. [Електронний ресурс] Режим доступу: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/hgp-origin-validation. Дата звернення: 29 червня, 2018 р.
9. *Зубок В.* Використання технології DNSSEC для захисту доменних імен в українському сегменті мережі Інтернет // Information Technology and Security. 2017, Vol. 5, Iss. 2, p. 43—50.
10. *Зубок В.* Практические аспекты моделирования изменений в топологии глобальных компьютерных сетей // Реєстрація, зберігання і обробка даних. 2012, **14**, № 2, с. 67—78.

Отримано 13.07.18

REFERENCES

1. Rekhter, Y., Li, T. and Hares, S. (2006), A border gateway protocol 4 (BGP-4), avalable at: https://tools.ietf.org/html/rfc4271 (accessed June 09, 2018).
2. Symantec (2018), Internet security threat report 2018, available at: www.symantec.com/security-center/threat-report (accessed May 10, 2018).
3. Global ransomware damages predicted to exceed $5 billion in 2017, *Cybercrime Magazine*, avalable at: https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/ (accessed May 10, 2018).
4. The Next Web (2017), Google made a tiny error and it broke half the internet in Japan, avalable at: https://thenextweb.com/google/2017/08/28/google-japan-internet-blackout/ (accessed Apr. 28, 2018).
5. Goodin, D. (2017), Russian-controlled telecom hijacks financial services' Internet traffic, avalable at: https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/ (accessed Dec. 1, 2017).
6. Apostolaki, M., Zohar, A. and Vanbever, L. (2017), Hijacking bitcoin: Routing attacks on cryptocurrencies", available at: https://btc-hijack.ethz.ch/files/btc_hijack.pdf (accessed Apr. 28, 2018).
7. MERIT, List of routing registries, available at: http://www.irr.net/docs/list.html (accessed Apr. 28, 2018).
8. RIPE NCC, BGP origin validation, available at: https://www.ripe.net/manage-ips-and-asns/resource-management/certification/bgp-origin-validation (accessed Apr. 28, 2018).
9. Zubok, V. (2017), "Use of DNSSEC technology for protection of domain names in the Ukrainian segment of Internet", *Information Technology and Security,* Institute of Special Communication and Information Protection, Vol. 5, Iss. 2, pp. 43-50.
10. Zubok, V. (2012), "Practical aspects of modeling changes in the topology of the global computer network", *Reyestratsiya, zberigannya i obrobka danykh*, Vol. 14, no. 2, pp. 67-78.

Received 13.07.18

В.Ю. Зубок

ОПРЕДЕЛЕНИЕ НАПРАВЛЕНИЙ
ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ НА ГЛОБАЛЬНУЮ
МАРШРУТИЗАЦИЮ В СЕТИ ИНТЕРНЕТ

Атака на глобальную маршрутизацию способна нанести вредное воздействие на миллионы сетевых устройств (и пользователей) значительно меньшими усилиями, чем широко известные атаки класса DoS или Ransomware. Несмотря на фундаментальность, протокол глобальной маршрутизации BGP-4 не является безопасным, так как основан на доверии между участниками глобальной маршрутизации. Рассмотрены направления противодействия, позволяющие достичь уменьшения возможных убытков от атак на глобальную маршрутизацию на уровне крупного оператора, отрасли, региона. Предложены два направления противодействия: предотвращение перехвата маршрутов собственных префиксов и выявление перехваченных маршрутов и блокировки трафика до соответствующих префиксов. Первое направление сформулировано как задача поиска наиболее эффективной топологической организации связей на уровне глобальной маршрутизации в сети Интернет, которая обеспечит минимизацию потерь от перехвата маршрута в пределах определенной целевой группы узлов.

К л ю ч е в ы е с л о в а: глобальная маршрутизация, перехват маршрутов, оптимизация связей, кибербезопасность.

V.Yu. Zubok

DETERMINING THE WAYS OF COUNTERACTION
TO CYBERATTACKS ON THE INTERNET GLOBAL ROUTING

Attacking global routing is capable of harming millions of network devices (and also users) with much less effort than the well-known DoS or Ransomware attacks. The global routing protocol BGP-4, despite its fundamental significance, is not secure, because it is based on trust between the participants of global routing. In the absence of fast prospects for implementing a more secure global routing protocol, it is necessary to suggest approaches that could be applied at the scope of a large operator, industry, region, to mitigate the possible losses from attacks on global routing. For this purpose, two general directions of counteraction are proposed: a) prevention of own prefixes hijacking; b) identification of hijacked routes and blocking outbound traffic to the compromised prefixes. The first direction is proposed to be described as the task of searching for the most effective topological organization of inter-node links, which can reduce losses from route hijacking within a certain target group of nodes.

K e y w o r d s: global routing, route hijacking, link optimization, cyber security.

ЗУБОК Віталій Юрійович, канд. техн. наук, ст. наук. співроб. Ін-ту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. У 1994 р. закінчив Київський політехнічний ін-т. Область наукових досліджень — глобальні інформаційні мережі, Інтернет, теорія складних мереж.