УДК 004.7

В.Ю. Зубок, Київ

РЕТРОСПЕКТИВНИЙ АНАЛІЗ ІНЦИДЕНТІВ КІБЕРБЕЗПЕКИ, ПОВ'ЯЗАНИХ З АТАКАМИ НА ГЛОБАЛЬНУ МАРШРУТИЗАЦІЮ

Abstract. There are several types of cyber incidents in the Internet, well-known as 'route hijack' and 'route leak'. They lead to blocking, redirecting or distorting network traffic of millions of users and network devices. Since there are no reliable defense mechanisms against this type of attack, a sound approach to assessing the risk of threats is necessary. In this regard, this article offers a review of incidents, both that have received wide publicity over the past five years, and earlier, including a description of the threat, a mechanism for its implementation, expected objectives and consequences in each case.

Вступ. В Інтернеті існує кілька типів кібер-інцидентів, відомих як "викрадення маршруту" (route hijack) та "витік маршруту" (route leak). Вони призводять до блокування, перенаправлення або спотворення мережевого трафіку мільйонів користувачів та мережевих пристроїв. Оскільки надійних захисних механізмів проти цього виду не існує, необхідний обґрунтований підхід до оцінки ризику загрози. В цій статті запропоновано огляд інцидентів, які отримали широкий розголос протягом останніх п'яти років. Огляд включає опис загрози, механізм її реалізації, очікувані цілі та наслідки в кожному конкретному випадку. Це є необхідним кроком в процесі оцінювання ризику [1].

Процес оцінювання ризику потребує його ідентифікації. Оскільки ризик обумовлений особливостями зовнішнього і внутрішнього середовища, розглядаються всі можливі джерела ризику, а також наявна інформація про сприйняття ризику (усвідомлення ризику) причетними сторонами, як внутрішніми по відношенню до компанії, так і зовнішніми. Особливі вимоги висуваються до якості інформації (максимально можливий рівень повноти, точності і тимчасової відповідності при наявних ресурсах на її отримання) та її джерел [2, 3]. Результат ідентифікації повинен бути структурованим та охоплювати чотири елементи:

- джерела виникнення;
- події, що виникнуть;
- причини цих подій;
- наслідки подій.

Рішенню цих задач сприятиме ретроспективний аналіз кіберінцидентів. Термін «ретроспективний» вжито саме тому, що інформація щодо наслідків, масштабу, засобів, а інколи і справжніх цілей атак стає відомою згодом.

Інцидент з AS3252. Перші випадки подій, пов'язаних з певною недосконалістю протокола BGP-4 і, як наслідок, захопленням маршрутів,

особисто відомі автору з середини 1990 років. Так, український Інтернет сервіс провайдер «Релком-Україна» з автономною системою AS3252 одним з перших побудував два міжнародні канали (став «multihomed»): перший – наземний канал до провайдера в Російській Федерації, яка була попереду в питаннях розвитку Інтернету; другий – супутниковий, пропускною здатністю 64 кбіт/с, до одного з європейських операторів (EUnet). Через помилку в налаштуванні BGP-4 у українського та російського провайдерів, відбувся витік (route leak) європейських маршрутів через канал до російського провайдера. ці маршрути, потрапивши в російську мережу, виявились кращими з точки зору BGP-4 (best route) для майже всіх російських мереж, підключених до Інтернет. Трафік російського походження, замість звичайних напрямків по магістральних міжнародних каналах з Москви та Санкт-Петербургу, намагався надходити до європейських мереж через AS3252. Схему інциденту наведено на рис. 1. В результаті вкрай недостатньої для такого обсягу трафіку пропускної здатності каналів, AS3252 утворила «чорну діру» для російського трафіку. Через недостатній досвід інцидент було припинено російським провайдером шляхом відключення каналоутворюючого обладнання (модему) на каналі з AS3252.

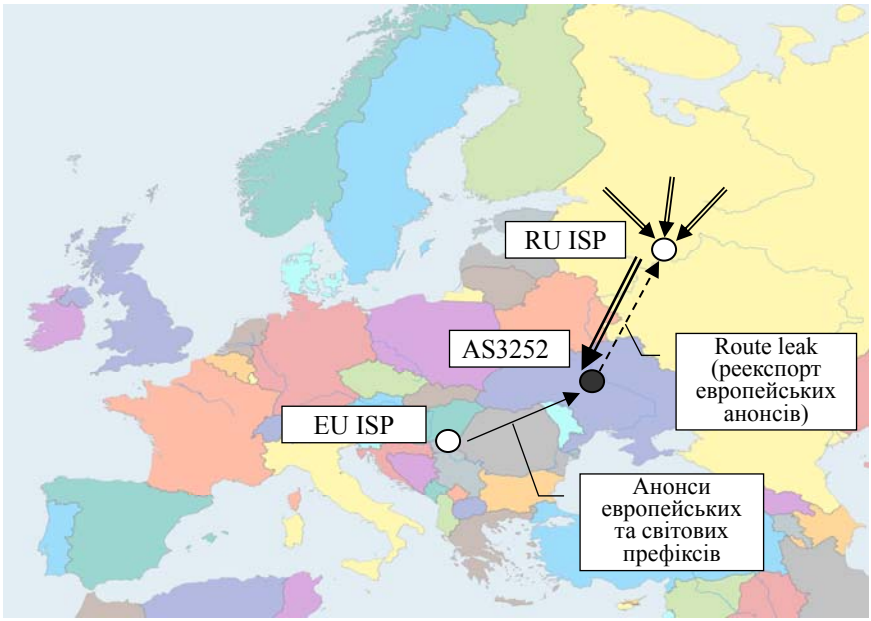

Рис. 1. Схема інциденту з AS3252. Подвійні стрілки – трафік, що потрапив в «чорну діру». Джерело мапи – https://mapswire.com.

На деякий час певна частка мереж РФ лишалась без доступу до закордонних Інтернет-ресурсів. Але в ті роки основними Інтернет-послугами

були електронна пошта та офлайн-форуми USENET (обидві послуги зазвичай передбачали сеансовий зв'язок з мережею, а не постійний, як зараз), тому звичайні користувачі навряд чи помітили такий збій.

Інцидент з AS7007. Маловідомий інцидент 1997 року, який стався у провайдера MAI (AS7007) в штаті Вірджинія, США, був відзначений в тогочасній пресі. Ця автономна система отримала від одного з своїх клієнтів не тільки префікси його мереж, а й всю глобальну таблицю маршрутизації (full view). Через нестачу досвіду адміністратори AS7007 досі не використовували фільтрацію маршрутів на клієнтських підключеннях, та взагалі припутились багатьох помилок. Так, через помилку в маршрутизаторі, отримані префікси було ще й деагреговано до найдрібніших префіксів з довжиною мережевої маски 24 біти. Загалом так було перекручено близько 23 000 префіксів різної довжини, з яких утворилось близько 73000 префіксів довжиною 24 біти. В результаті 73000 хибних маршрутів було анонсовано в Флорідську мережу обміном трафіком MAE-East (AS1790). Ці маршрути отримали всі учасники мережі обміну трафіком і стали в них кращими (best route). AS7007 отримала від інших учасників трафік, що був адресований всьому світові. Через нестачу пропускної здатності її каналів учасники інциденту лишались без Інтернет-доступу. Ефект «чорної діри» відчувався по всій мережі до 4 годин. Сьогодні такі атаки мають назву «route deaggregation» [4]. Схему інциденту наведено на рис. 2.

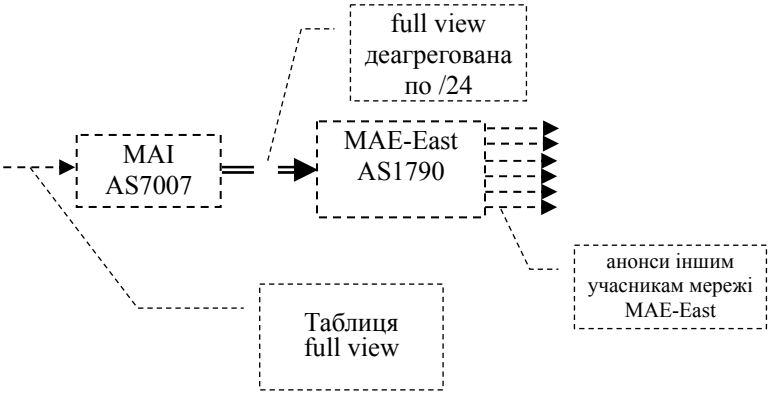

Рис. 1. Схема інциденту з AS7007.

Інцидент з AS9121 «Christmas Eve». В день Різдва, 24 грудня 2004 року ініціатором масштабного перехоплення маршрутів став національний телеком-оператор Туреччини TTNet. Цей випадок був першим, добре задокументованим в цифрах і графіках завдяки дослідженню MERIT [5].

Станом на час інциденту TTNet (AS9121) був транзитним провайдером

для 60 інших операторів та анонсував приблизно 200 IP-префіксів. Вже на той час мав оформлену політику маршрутизації в реєстрі маршрутів RIPE NCC. Нажаль, політика була сформована некоректно, а саме – не було обмежень на вхідні префікси від клієнтських AS.

На ранок 24.12.2004 AS9121 почала раптово анонсувати від власного імені (тобто анонсувати зі зміною атрибуту origin) до 105000 префіксів. Протягом понад годину ці префікси приймали та ретранслювали всі вищі провайдери та партнери (peers) TTNet, серед яких були великі трансрегіональні оператори: Telecom Italia (AS6762), Sprint (AS1239), Telia (1299), Cable & Wireless (1273). Кожен з них ретранслював по своїх інших каналах принаймні частку хибних маршрутів (рис. 3). Збій повторювався ще двічі з меншою кількістю префіксів, як показано на рис. 4 (можливо, то були невдалі спроби імплементувати коректну routing policy в TTNet).

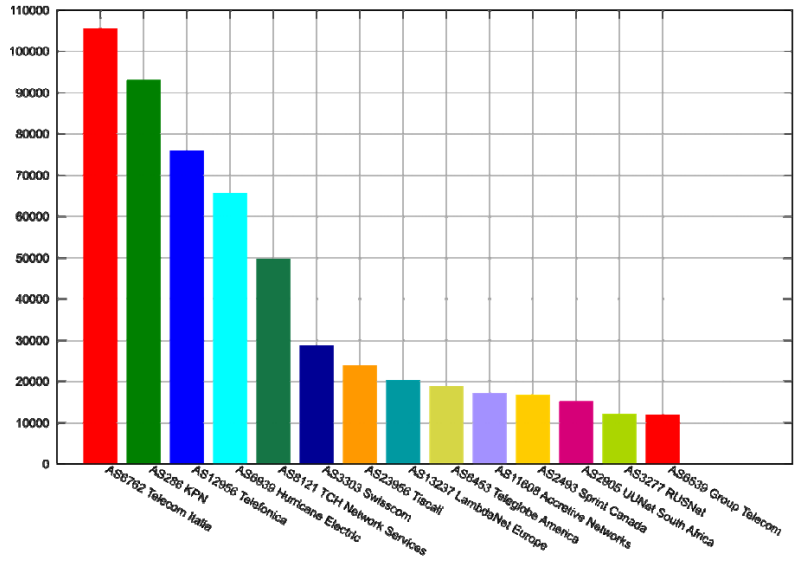

Рис. 3. Кількість ретрансльованих хибних префіксів (вісь ординат) через інші AS (вісь абсцис). Джерело даних – MERIT.

Як видно з рис. 4, інцидент з різною інтенсивністю тривав майже 9 годин. Завдяки тому, що TTNet та його апстрім провайдери мал чималі потужності, лише деякі частини Інтернету були тотально недоступними протягом того часу. Проте погіршення сервісу відчули більшість користувачів завдяки зміні маршрутів до Youtube, Amazon і т.і.

Інцидент з Youtube 2008 р. Згадані раніше інциденти за загальною думкою відбувались через помилку чи бездіяльність мережевих адміністраторів. Аж в лютому 2008 року відбулась перша широко відома умисна дія з блокування первних інтернет-ресурсів шляхом атаки на глобальну маршрутизацію.

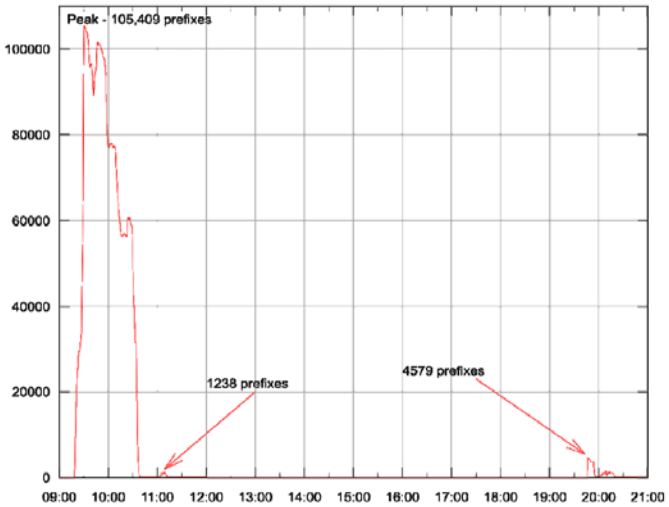

Рис. 4. Кількість хибних префіксів (вісь ординат), анонсованих AS9121 в ході інциденту 24.12.2004. Джерело даних – MERIT.

24 лютого 2008 року пакістанський державний національний оператор Pakistan Telecom (AS17557) намагався виконати завдання свого уряду по блокуванню якогось медіаконтенту, який було розміщено на сервісі YouTube (AS36561). Для цього було обрано такий шлях: часку IP-префіксу, який використовував YouTube, а саме – підмережу 208.65.153.0/24 з більшої мережі 208.65.152.0/22, AS17557 анонсувала від свого імені (тобто із зміною origin). Анонсував не тільки своїм пакистанським клієнтам, а й своєму апстрім-провайдеру PCCW (AS3491) з базою в Гонконзі. Нажаль, на той час не імплементувала фільтрацію BGP-анонсів.

Хибний префікс розповсюдився досить широко. Та, оскільки префікс з довжиною мережевої маски 24 є «more specific», маршрут до нього через PCCW (AS3491) та Pakistan Telecom став єдиним і, відповідно, кращим. Сервіс YouTube в результаті інциденту був недоступний протягом 2 годин (рис.5). Всі оператори, починаючи з AS3491, отримавши повідомлення від YouTube про проблеми з маршрутизацією, зафільтрували хибний анонс. Проте сам Pakistan Telecom не припинив виконувати наказ свого державного регулятора у цей спосіб.

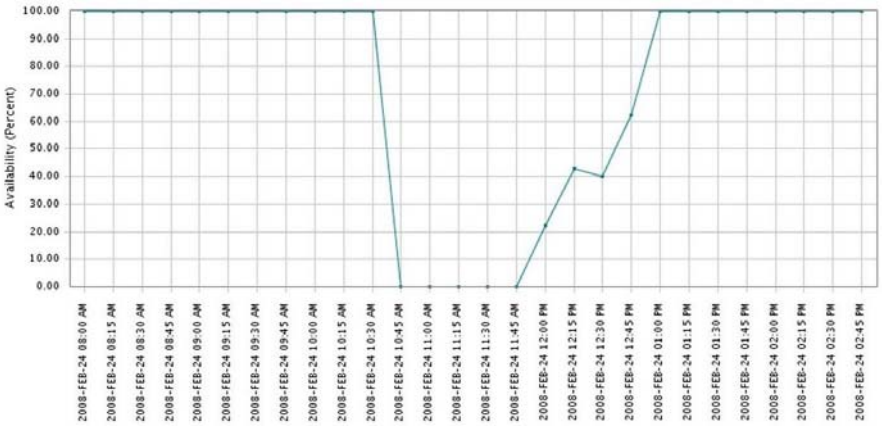

Рис.5. Падіння доступності сервісу YouTube в результаті інциденту з AS17557. Джерело – Keynote Systems [6].

Інші інциденти. В [7-9] наведено дані про резонансні інциденти, які трапились протягом 2014-2019 і були пов'язані з глобальною маршрутизацією:

– лютий-березень 2014 року: перехоплення трафіку до майнінгових пулів криптовалют Bitcoin, Dogecoin, HoboNickels та Worldcoin (умовна назва інциденту – Canadian Bitcoin Hijack);

– квітень 2017 року: Ростелекомом маршрутів шляхом анонсування протягом деякого часу значної кількості префіксів, які належали міжнародним платіжним системам та фінансовим сервісам (Rostelecom-Mastercard;

– серпень 2017: Google перехопив трафік багатьох операторів в Японії в наслідок технічної помилки конфігурування маршрутизаторів (Google Japan);

– грудень 2017: перехоплення трафіку Google, Facebook, VK.com та інших відомих контент-провайдерів телеком-оператором з Хабаровська (Khabarovsk-SM);

– квітень 2018 року: атака route hijack застосована до інфраструктурного IP-префіксу широко відомого хмарного сервісу Amazon AWS, метою якого була фішингова атака на криптовалютний сервіс "MyEtherWallet" шляхом перенаправлення трафіку (Amazon EtherWallet);

– листопад 2018 року: збій глобальної маршрутизації, що торкнувся сервісів G Suite, Google Пошук і Google Аналітика, стався завдяки невеликому нігерійському провайдеру за участю China Telecom та Ростелекому, визнаний фахівцями як умисні дії (China-Rostelecom);

– червень 2019 року: атака на відомий сервіс мережевого захисту CloudFlare.

Це дає достатньо даних для аналізу з метою ідентифікації ризику, а саме – визначення джерела виникнення; події, що виникнуть; причини цих подій;

наслідки подій. Структуровані за цими чотирма елементами дані про інциденти кібербезпеки, пов'язані з глобальною маршрутизацією, зведено в табл. 1.

Таблиця 1

Дані про інциденти кібербезпеки, пов'язані з глобальною маршрутизацією

Назва інциденту	**Джерело**	**Подія**	**Причина**	**Наслідки**
Інцидент з AS3252, 1994	приватний оператор	витік маршрутів	технічна помилка	Мінімальні (затримка передачі e-mail)
Інцидент з AS7007, 1997	приватний оператор	перехоплення маршрутів з деагрегацією	технічна помилка	Постраждалі – активні Інтенет-користувачі
Інцидент з AS9121, 2004	приватний оператор	витік маршрутів	технічна помилка	Постраждалі – 1/4 IP-мереж та їхні користувачі
Інцидент з Youtube, 2008	державний оператор	перехопдення маршруту з деагрегаією	зумисні дії	Постраждав сервіс YouTube та користувачі
Canadian Bitcoin Hijack, 2014	приватні особи	перехоплення маршруту	зумисні дії	Постраждалі – користуачі криптомайнерів та власники криптовалют
Rostelecom-Mastercard, 2017	державний оператор	перехоплення маршрутів	невідомо	Постраждалі – користувачі платіжних систем, здебільшого з РФ
Khabarovsk-SM, 2017	приватний оператор	витік маршрутів	невідомо	Постраждалі – соцмережі, контент-провайдери та їхні користувачі з РФ
Amazon EtherWallet, 2018	приватні особи	перехоплення маршрутів з деагрегацією	зумисні дії	Постраждалі – всі клієнти сервісу Amazon AWS, а також їхні користувачі з усього світу

China-Rostelecom, 2018	державний оператор	витік маршрутів	підозра на зумисні дії	Постраждалі – платіжні системи та клієнти
CloudFlare, 2019	приватний оператор	витік маршрутів	технічна помилка	Постраждалі – клієнти Cloudflare та їхні користувачі

З систематизованих даних можна пересвідчитись, що дедалі росте доля очевидних зумисних дій, спрямованих на скоєння атак на глобальну маршрутизацію, а наслідки атак стають більш глобальними.

Висновок. Систематизовані ретроспективні дані стосовно кіберінцидентів з глобальною маршрутизацією в Інтернеті свідчать, що дедалі зростає доля очевидних зумисних дій, спрямованих на скоєння атак на глобальну маршрутизацію, а наслідки атак стають більш глобальними.

1. *Зубок В.Ю., Мохор В.В*. Дослідження зв'язку між топологією та ризиком внаслідок кібератак на глобальну маршрутизацію. // Моделювання та інформаційні технології. Зб. наук. пр. ІПМЕ ім Г.Є. Пухова НАН України. – Вип. 85. – К.: 2018. – С.23-26.
2. Risk Management – Vocabulary (ISO Guide 73:2009, IDT) : ДСТУ ISO Guide 73:2013. – [Чинний від 2014–07–01] . – Київ : Мінекономрозвитку України, 2014. – 13 с. – (Національні стандарти України).
3. Information technology – Security techniques – Information security risk management (ISO/IEC 27005:2013 Cor 1:2014, IDT) : ДСТУ ISO/IEC 27001:2015. – [Чинний від 2016–01–01] . – Київ : УкрНДНЦ. – 2016. – 26 с. – (Національні стандарти України).
4. *Vincent J. Bono.* 7007 Explanation and Apology. [Електронний ресурс] Режим доступу: https://seclists.org/nanog/1997/Apr/444. Дата звернення: Лип.12,2019.
5. *Larry J. Blunk.* New BGP analysis tools and a look at the AS9121 Incident. – Merit Network, Inc. – IEPG Meeting – 62nd IETFю – Minneapolis. – March 6, 2005.
6. How Pakistan knocked YouTube offline (and how to make sure it never happens again). [Електронний ресурс] Режим доступу: https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/. Дата звернення: Лип.12,2019.
7. *Зубок В.* Визначення напрямків протидії кібератакам на глобальну маршрутизацію в мережі Інтернет // Електронне моделювання. – К.,2018. Т.40, №5.
8. *Зубок В.* Оцінювання ризиків кібернетичних атак на глобальну маршрутизацію в мережі Інтернет // Збірка праць конференції «Моделювання-2018», 12-14 вересня, Київ. – К., «Академперіодика». – С.147-150.
9. *Зубок В.* Використання моделей загроз та оцінка ризиків кібератак на глобальну маршрутизацію в Інтернеті // Зб. тез XXXVII наук.-техн. конф. молодих вчених та спеціалістів, м. Київ, 15 травня 2019 р. / ІПМЕ ім. Г.Є. Пухова НАН України. – 2019. – С.15-18.

http://doi.org/10.5281/zenodo.3610642

Поступила 19.08.2019р.