ВПЛИВ РИЗИКІВ, ПОВ'ЯЗАНИХ З ПРОГРАМНИМ ЗАБЕЗПЕЧЕННЯМ, НА ФУНКЦІОНУВАННЯ ГЛОБАЛЬНОЇ МАРШРУТИЗАЦІЇ В ІНТЕРНЕТІ

Зубок Віталій Юрійович
к.т.н., докторант ІПМЕ ім. Г.Є.Пухова

Науковый консультант –
д.т.н., член-кор. НАН України Мохор В.В.

Сутність проблеми

- Інтернет порівнюють із складною екосистемою із переплетеними зв’язками, в якій втручання в будь-який зв’язок матиме непрогнозовані наслідки на інших рівнях системи.
- Протокол глобальної маршрутизації BGP-4 не має засобів авторизації та валідації маршрутів.
- **Атаки**
  - **BGP route leak** - несанкціоновані пропонування хибних “кращих маршрутів”.
  - **BGP route hijack** - захват маршрутів до чужих мережевих префіксів.
  - Призводять до викривлення, перехоплення, втрати трафіку.
  - Використовуються для дестабілізації телекомунікаційної мережі, шпигунства, крадіжок даних, нанесення матеріальної шкоди, дезинформації тощо.

Актуальність проблеми

- **2018**
  - Фішингова атака на криптовалютний сервіс "MyEtherWallet" шляхом перенаправлення трафіку
  - Іран перехопив трафік сервісу Telegram.
  - Листопад 2018. Збій глобальної маршрутизації за участю China Telecom та Ростелекому. Постраждали G Suite, Google Search та Google Analytics.
- **2019**
  - Перехоплення префіксів CloudFlare через відсутність достатньої фільтрації BGP-анонсів у американського телеком-оператора Verizon. «Постраждалими» визначено 2400 автономних систем.
  - Перехоплення префіксу з інфраструктури AMS-IX призвело до тимчасового руйнування BGP-взаємодії між учасниками.
- **2020**
  - Збій через головні інструменти захисту маршрутів

Реєстр маршрутів та валідація джерела маршруту

- Regional Internet Registries ведуть облік глобального розподілу адресного простору та добровільних даних про взаємодію мереж (Routing Registry)
- Новий механізм авторизації джерела маршруту ROA (Routing Origin Authority)
  - Електронний підпис, що зв’язує мережевий префікс і номер AS, яка має право анонсувати його:
    - route: 195.64.224.0/22
    - descr: Sample ISP networks
    - origin: AS8258

Опис інциденту 1 квітня 2020 р.

From: Nathalie Trenaman <nathalie@ripe.net>

Sender: ncc-announce <ncc-announce-bounces@ripe.net>

Date: 02.04.2020 10:54

To: ncc-announce@ripe.net

Dear colleagues,

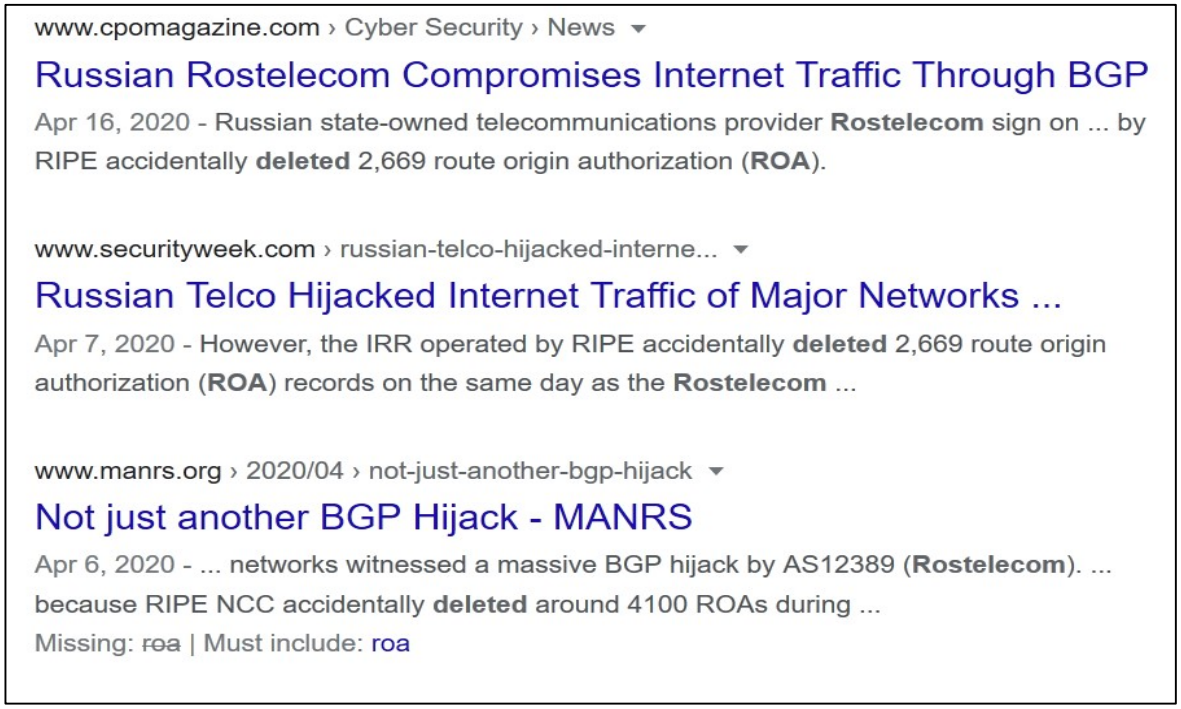
Yesterday at 18:17 (UTC+2) we accidentally deleted 4,100 RPKI Route Origin Authorisations (ROAs).
were related both to members' and sponsored resources. This happened while we were performing mair
our internal software.
We are currently investigating and will update you when we know more.
Apologies for the inconvenience.

Опис інциденту 1 квітня 2020 р.

- Ростелеком (AS12389) нелегітимно анонсував 8877 префіксів, що насправді належали 200 іншим AS
- Перевірка джерела по ROA була неможлива
- Перехоплення маршрутів тривало більше години
- Виявлення та усвідомлення проблем з БД ROA тривало понад добу.
- Відновлення БД ROA тривало понад 5 годин

Опис інциденту 1 квітня 2020 р.

- Помилки в роботі ПЗ мали глобальні наслідки.



www.cpomagazine.com › Cyber Security › News

Russian Rostelecom Compromises Internet Traffic Through BGP

Apr 16, 2020 - Russian state-owned telecommunications provider **Rostelecom** sign on ... by RIPE accidentally **deleted** 2,669 route origin authorization (**ROA**).

www.securityweek.com › russian-telco-hijacked-interne...

Russian Telco Hijacked Internet Traffic of Major Networks ...

Apr 7, 2020 - However, the IRR operated by RIPE accidentally **deleted** 2,669 route origin authorization (**ROA**) records on the same day as the **Rostelecom** ...

www.manrs.org › 2020/04 › not-just-another-bgp-hijack

Not just another BGP Hijack - MANRS

Apr 6, 2020 - ... networks witnessed a massive BGP hijack by AS12389 (**Rostelecom**). ... because RIPE NCC accidentally **deleted** around 4100 ROAs during ...

Missing: ~~roa~~ | Must include: roa

Принципи поводження з ризиками критичного програмного забезпечення

- Програмний комплекс БД ROA став єдиною точкою відмови для системи (SPoF) глобальной маршрутизації в Інтернеті.
- Інцидент стався при апгрейді ПЗ.
- Про апаратні проблеми чи зумисні дії персоналу не згадували => проблеми в ПЗ або в процесі оновлення.

Принципи поводження з ризиками критичного програмного забезпечення

Проектний ризик

- визначення ризиків та їх тригерів;
- класифікування та визначення пріоритетів ризиків;
- розробка плану з усунення чи мінімізації наслідків кожного ризику;
- моніторинг стану триггерів ризику в ході проекта;
- виконання плану з усунення чи мінімізації наслідків.

Принципи поводження з ризиками критичного програмного забезпечення

Моніторинг

- публікація звітів про поточний стан проекту;
- перегляд планів ризику відповідно до будь-яких основних змін в ході проекту;
- перегляд і репріорітізація ризиків;
- мозковий штурм щодо потенційно нових ризиків підчас непланованих змін в проекті.

Принципи поводження з ризиками критичного програмного забезпечення

Пом’якшення наслідків

- прийняти: визнати, що ризик впливає на проект;
- уникнути: коригувати масштаби проекту, графік чи обмеження, щоб мінімізувати наслідки ризику;
- контроль: вживання заходів для мінімізації впливу або зменшення інтенсифікації ризику;
- передача: здійснити організаційну зміну підзвітності, відповідальності, чи повноважень іншим зацікавленим сторонам, які приймуть ризик;
- продовжити моніторинг

Висновки

- Питання поводження з ризиками в процесі розробки та експлуатації програмного забезпечення для реєстрів глобальної маршрутизації в Інтернеті потребують значно більшої уваги через те, що впровадження нових технологій захисту призвело до появи нової єдиної точки відмови.
- Інцидент з перехопленням маршрутів Ростелекомом 1 квітня 2020 р. набув глобального масштабу через те, що в процесі розробки та впровадження оновлень ПЗ європейської БД реєстру маршрутизації бракувало моніторингу та програми пом'якшення наслідків ризику.