BGP Hijacking (Únos BGP)

BGP Hijacking je v podstatě „krádež digitální identity“ celých síťových rozsahů. Pokud útočník úspěšně přesvědčí sousední sítě, že nejkratší cesta k určité službě (např. Google, banka nebo DNS server) vede přes jeho autonomní systém, může provoz této služby odposlouchávat, upravovat nebo zcela zastavit.

Jak únos probíhá?

Útočník využívá mechanismus „nejkonkrétnější shody“ (Longest Prefix Match). Pokud legitimní vlastník oznamuje síť jako celek (např. `1.2.0.0/16`), ale útočník oznámí menší část (např. `1.2.3.0/24`), internetové směrovače upřednostní specifičtější cestu útočníka.

Scénáře útoku:

```
1. **Blackholing (Černá díra):** Útočník provoz přijme a zahodí. Služba se
pro uživatele stane nedostupnou (DoS).
2. **Impersonation (Podvržení):** Útočník provoz přijme a nasměruje
uživatele na falešnou kopii webu (phishing), aby získal přihlašovací údaje.
3. **Man-in-the-Middle (MITM):** Útočník data v tichosti odposlechne nebo
upraví a následně je přepošle skutečnému cíli, aby útok nebyl odhalen.
```

Příčiny vzniku

Únosy nemusí být vždy dílem hackerů, často vznikají lidskou chybou:

Příčina	Popis
Konfygurační chyba	Správce sítě omylem překlepne číslo AS nebo rozsah IP adres v konfiguraci routeru.
Záměrný útok	Státní aktéři nebo kriminální skupiny cíleně přesměrovávají provoz pro špionáž nebo krádeže (např. kryptoměn).
Route Leak	Lokální směrovací informace se kvůli chybě „vylijí“ do globálního internetu.

Reálné příklady z historie

- **YouTube vs. Pakistan Telecom (2008):** Pákistánský operátor chtěl zablokovat YouTube v

rámci země, ale omylem své blokovací pravidlo oznámil do celého světa. YouTube byl několik hodin celosvětově nedostupný.
- **Útok na MyEtherWallet (2018):** Útočníci unesli DNS servery Amazonu přes BGP, aby přesměrovali uživatele kryptoměnové peněženky na falešný web a vykradli jejich účty.
- **Rostelecom (2020):** Ruský operátor omylem oznámil stovky tras patřících firmám jako Google, Amazon či Facebook, což způsobilo velké výpadky.

Jak se bránit?

Obrana proti BGP hijackingu je náročná, protože vyžaduje spolupráci tisíců operátorů po celém světě.

- **RPKI:** Nejdůležitější obrana současnosti. Digitální podpisy, které ověřují, kdo smí které IP adresy oznamovat.
- **Prefix Filtering:** Operátoři by měli od svých zákazníků přijímat pouze ty rozsahy adres, o kterých vědí, že jim patří.
- **BGP Monitoring:** Služby (např. Cisco BGPStream), které v reálném čase sledují internet a varují vlastníky sítí, pokud se jejich adresy začnou oznamovat odjinud.
- **BGPsec:** Rozšíření protokolu, které podepisuje celou cestu (AS Path), zatím je však v praxi málo rozšířené.

Související pojmy: BGP, RPKI, Autonomní systém (AS), IP adresa, DoS útok, Phishing, Man-in-the-Middle.

From:
https://serviceit.cz/ - **IT ENCYKLOPEDIE**

Permanent link:
https://serviceit.cz/doku.php?id=bgp_hijacking

Last update: **2025/12/31 20:15**