BGP hijacking by Rostelecom

Threat Memo - Date: 09/04/2020 - Version: 1.0
TLP:AMBER

FOR INFORMATION	Category	Type	Domain(s)	Sector(s)	Confidence
	Accidental Cyberespionage	Interception	World	Digital Infrastructure	A1

Key Points

- Rostelecom, a large Russian telecom provider, has committed a BGP hijacking on April 1.
- BGP hijackings are myriad and often not intentional, although they can be used to obtain a man-in-the-middle position or to capture traffic for later decryption.
- It is unclear if this incident was accidental.
- Rostelecom has worked with one of the security firms reporting the incident on resolving it.

Summary

The Russian telecom provider Rostelecom was involved[1] in a BGP hijacking incident last week. On April 1, traffic routes intended for servers from Google, Amazon, Facebook, Cloudflare, GoDaddy, Digital Ocean, Akamai and other cloud hosting providers were diverted to Russian networks. Over 8800 routes from more than 200 networks were affected by this incident, that lasted about an hour.

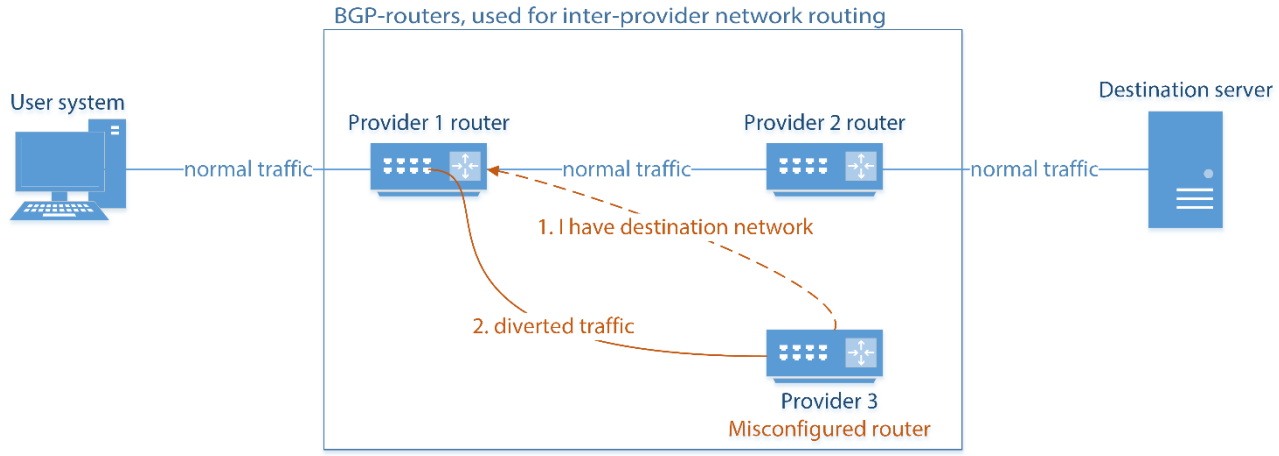

Figure 1. BGP hijacking attacks (simplified).

QRator, a network security provider, issued an article[2] stating they had detected the incident, reported it to Rostelecom and received a request from them to assist in the resolution of the incident. This leads the security provider to believe that the incident was, in fact, accidental. Historical BGP hijacking incidents were not always free of the suspicion of malicious intent. Furthermore, it can be difficult to discern an accidental from an intentional hijacking, as they will look the same on the technical level.

Comments

The BGP protocol is an old standard for routing traffic between networks. It is prone to error and does not contain inherent checks and safeguards. Mistakes are easily made and generally have grave consequences (routing issues in the home network or traffic diversion on the global internet, like in the current incident). This has resulted in quite a number of incidents. See TM-190611-1 for more details on a China Telecom BGP incident. A list can be found in Annex.

In 2017, BGP hijacking incidents involving Rostelecom have been suspected to be deliberate:

- In December 2017, a BGP hijacking incident affected internet communications associated with some US and international social media, technology, communications, gaming, and cloud storage providers. This traffic was rerouted to likely Russian telecommunications providers.
- In April 2017, Rostelecom reportedly engaged in large-scale BGP hijacking against financial service entities. Where accidental breaches usually indiscriminately take over netblocks, this last attack mostly took over blocks belonging to financial institutions[3].

[1] https://securityaffairs.co/wordpress/101134/security/rostelecom-telco-hijacks-internet-traffic.html
[2] https://radar.qrator.net/blog/how_you_deal_with_route_leaks
[3] https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/

Annex – Selection of recent BGP hijacking incidents

Date	Hijacker	Victim	Intent
June 2019	China	European Mobile traffic	Possibly accidental
May 2019	Brazil	Taiwan DNS traffic	Unknown
December 2018	China	US Department of Energy	Unknown
November 2018	Nigerian telecom	Google internet traffic	Unknown
December 2017	Russian Rostelecom	US tech giants	Possibly deliberate
August 2017	Google	Japanese ISP	Accidental
April 2017	Russia	Visa and Mastercard traffic	Possibly deliberate