CERT-EU
Memo
11/06/2019 - TLP:WHITE

High volume of European network traffic re-routed through China Telecom

Reference: Memo [190611-1] Date: 11/06/2019 - Version: 1.0
Keywords: BGP, digital infrastructure, China
Sources: publicly available information

Key Points

- A routing incident led to 70 000 routes used for European traffic being redirected through China Telecom for over 2 hours.
- Border Gateway Protocol (BGP) errors are a relatively common issue but usually last just a few minutes.
- China Telecom has still not implemented some basic routing safeguards to detect and remediate them in a timely manner.

Summary

On June 6, a routing incident led to over 70 000 routes used for European mobile networks being redirected through China Telecom for over two hours. The incident began at 09:43 UTC when Swiss data centre colocation company Safe Host (AS21217) unintentionally leaked over 70 000 routes to China Telecom (AS4134) in Frankfurt, Germany. China Telecom then announced these routes on to the global internet redirecting large amounts of traffic destined for some of the largest European mobile networks through China Telecom's network. Some of the most impacted European networks included Swisscom (AS3303) of Switzerland, KPN (AS1136) of Holland, Bouygues Telecom (AS5410) and Numericable-SFR (AS21502) of France.

Often routing incidents only last for a few minutes, but in this case, many of the leaked routes were in circulation for over two hours.

Comments

China Telecom, a major international carrier, has still not implemented neither the basic routing safeguards necessary to prevent propagation of routing leaks nor the processes and procedures necessary to detect and remediate them in a timely manner when they inevitably occur.

The Border Gateway Protocol (BGP) is an old standard that was not designed with security in mind. Internet service providers (ISP-s) announce which IP addresses are available on their networks and that information is treated with trust by other internet infrastructure providers. It means that if an entity has enough leverage, it can hijack traffic even if it is geographically far away from its target. The Internet Society's Mutually Agreed Norms for Routing Security (MANRS) project has however developed routing hygiene practices.

BGP errors are a relatively common issues and are usually results of a human error. However, deliberate BGP hijacking is used by criminal actors to facilitate many types of online fraud. BGP hijacking is also a way for nation-state actors to monitor, corrupt, steal, copy, or modify data, as well as possibly to decrypt internet traffic. Until these issues are resolved by the international community, they will remain a severe security risk for any entity relying on the internet.

Some recent high-profile routing incidents have been observed.

- December 28, 2018: beginning at 08:33 UTC, an internet routing path that was usually advertised by an Autonomous System Number (ASN) associated with the US Department of Energy was changed by an ASN associated with China Telecom. The incident comprised more than 374 events over a period of 2 hours and 15 minutes.
- November 12, 2018: Nigeria's Main One Cable Company inadvertently caused a glitch that temporarily misrouted Google internet traffic through China and Russia. The error was caused by a misconfigured BGP filter, which misdirected internet traffic for 74 minutes through Main One's partner, China Telecom. A particularly noteworthy aspect of this incident is that it went undetected until end users began reporting dropped traffic, revealing glaring security limitations of BGP.
- December 12, 2017: Traffic to some of the world's largest tech companies was briefly rerouted through a Russian ISP. Eighty prefixes associated with companies including Google, Apple, Facebook, Microsoft, Twitch, NTT Communications and Riot Games were affected. The autonomous Russian system added itself to entries in BGP tables, claiming it was the rightful origin of the prefixes. The autonomous system involved in this incident appears to be the same that hijacked traffic from companies and financial services including Visa and MasterCard earlier this year. It is likely that the traffic redirection was a deliberate choice.
- August 25, 2017: An error by Google caused widespread internet outages in Japan for about one hour. The mishap occurred due to incorrect BGP configuration. Google advertised that a large block of Japanese IPs was available at its own network. That information propagated and soon service providers started to send traffic destined for Japan to Google. About 8 million Japanese connections became unavailable.
- April 26, 2017: Traffic belonging to more than twenty financial services, including Visa and MasterCard, was routed through Rostelecom, a Russian government-controlled telecommunications company. The routing anomaly resulted from a BGP misconfiguration when Rostelecom wrongly broadcast their ownership of thirty-six network blocks. The anomaly lasted for about seven minutes. According to open sources, some affected networks were rerouted in a way which indicates that their prefixes had been manually inserted into BGP tables. In this case, financial institutions seem to have been specifically targeted.