A project aims to help ISPs mind their routing security manners

reader comments

5 with 4 posters participating

Share this story

When my kids were younger, we used to tell them we were going to send them to “manners camp” if they didn’t behave properly at the dinner table. An Internet Society-supported initiative, the Mutually Agreed Norms for Routing Security (MANRS), has tried to coax Internet service providers into minding their manners as well—particularly when it comes to how they use the Border Gateway Protocol (BGP), the occasionally abused communications method that drives much of how Internet traffic is routed.

On August 13, the MANRS initiative launched the MANRS Observatory, a new Web tool that provides insight into just how well networks comply with routing security standards. The observatory provides a semblance of transparency into a part of the Internet invisible to most users.

- The MANRS Observatory’s dashboard gives a general view of how well the Internet is doing at securing its routing.
- A map view allows drill-down by nation or region on routing security data.
- A historical view shows spikes in incidents and progress

toward MANRS guideline compliance.
- A view by each entity or nation shows which metrics need work to bring up ratings.

Last year, there were more than 12,000 routing outages or attacks, according to the Internet Society, including the use of BGP to hijack or misdirect traffic and internal BGP “leaks” from poorly configured routers. Deliberate BGP attacks can be used to steal data or redirect requests to hostile “spoofed” websites, as some state actors have been known to do.

But even leaks can cause widespread service outages. For instance, a routing leak by a Nigerian ISP in 2018 rerouted some Google traffic through China, causing service outages in parts of the world. A similar event hit Amazon last April. And a BGP leak in June had a cascading effect across the Internet.

According to Andrei Robachevsky, senior technology program manager at the Internet Society:

> *Routing security is based almost entirely on trust between networks… One of the advantages of the MANRS Observatory is that it adds an element of accountability. MANRS is seeing steady adoption, but we need more networks to implement the actions and more customers to demand routing security best practices. The more network operators applying MANRS actions, the fewer incidents happening, the less damage done. Our hope is that the MANRS Observatory will help drive greater participation.*

Robachevsky told Ars that MANRS got a slow start five years ago, but “we’re now seeing a doubling every year in membership.” Currently, more than 200 members collectively manage over 800 Internet exchange points. Google and Microsoft are among the notable recent additions, but other members range from Tier 1 network giants such as Equinix down to small regional network operators.

The MANRS initiative promotes technical collaboration among network providers to reduce the most common types of threats to routing security. To join, network providers must meet certain guidelines regarding security and resilience of their networks. And as the project rolls forward, MANRS is hoping to provide deeper transparency into how well providers are doing. The MANRS Observatory is a first cut at public disclosure of how well providers are complying.

Currently, the MANRS observatory tracks the number of routing incidents by region and by country, as well as metrics for how well providers are doing at meeting MANRS guidelines. That data is aggregated from multiple trusted third-party sources (such as BGPStream.com) into a Web dashboard that allows network operators to identify weaknesses and problems in order to improve their networks' routing security. They can also see how well peers are doing and see if the networks that want to partner with them are up to snuff on security. The MANRS Observatory is also a helpful tool for showing government policymakers what the state of routing security is and what the impact of adopting MANRS best practices can be.

Listing image by Getty Images | deepblue4you

https://arstechnica.com/?p=1562379