White paper
Cisco public

Understanding the Risks of Traffic Hijacking

Gain visibility into how your networks are routed

© 2022 Cisco and/or its affiliates. All rights reserved.

Contents

© 2022 Cisco and/or its affiliates. All rights reserved.

Do you know where your traffic is going?

In the realm of network transit security, you read a lot about Distributed-Denial-of-Service (DDoS), data breaches, and phishing attacks, but another less known type of attack called BGP hijacking can be damaging as well. Border Gateway Protocol (BGP) manages how packets are routed across the internet, directing packets between the networks managed by enterprises or service providers. BGP hijacking is sometimes referred to as prefix hijacking, route hijacking, or IP hijacking, and it involves redirecting traffic by manipulating the internet routing tables that are maintained using BGP.

Downtime and loss of brand trust can have significant and lasting negative impacts on service providers.

How BGP works

Internet protocols are all based on trust. But the fact is, none of these protocols were designed with security in mind. For years, enterprises, service providers, and everyday internet users have trusted that the protocols that form the backbone of the internet will work in concert to send information where it's supposed to go. The unfortunate reality is that incorrect configurations and malicious actors can negatively affect these protocols by redirecting information and, ultimately, user intent.

BGP controls the exchange of routing and reachability information between edge routers. It addresses the problem of exchanging information between Autonomous Systems (ASs). BGP-speaking routers exchange routing information through a series of BGP updates. An originating BGP router announces an IP address prefix to its attached neighbors. Those routers then propagate the information to other routers until a target router learns about the prefix and a route to reach the destinations in that prefix.

The problem is that the BGP protocol doesn't have an authentication mechanism to verify routes. Any BGP router can announce any prefix as if it owns it. Network operators can explicitly configure BGP routers to establish peering relationships with other ASs to exchange routing information.

However, because of routing complexity, operators may not know who owns a prefix or the path to get there. Some BGP hijacking isn't malicious; route leaks can happen, with the same detrimental effect, through prefix and AS misconfiguration. Whether a route has been maliciously hijacked or accidentally leaked, traffic can be routed to different locations, potentially exposing access to sensitive information.

© 2022 Cisco and/or its affiliates. All rights reserved.

BGP and service providers

As a service provider, your IP address blocks are valuable assets that make it possible for your customers to connect to the internet. BGP is a key part of your infrastructure, and if BGP is hijacked or configured incorrectly, it can cause massive availability and security problems. It's your responsibility to track the health of prefixes as they propagate across the internet.

Keeping track of prefixes is not a small task because a typical service provider router carries hundreds of thousands of unique prefixes using tens of millions of paths. Routing pathways change constantly as various nodes suffer latency or downtime, as new packet services are added or removed from the network, or as new intelligent protocols like segment routing are implemented across ASs. As a result, real-time tracking of prefixes is difficult. Yet threats to your network infrastructure are real and the cost of an attack can be significant. If there were a security incident, would you be able to answer these questions?

- What would you do if someone accidentally or maliciously hijacked your prefixes or those of one of your customers?
- How quickly and accurately could you identify the party responsible?
- How quickly could you resolve the problem?

The answers to these questions typically involve customer complaints, manual operator troubleshooting, and a long Mean Time To Repair (MTTR). In some cases, these issues become public, which can create a public relations nightmare for you and your customers.

Gaining visibility into potential risks

As a service provider, you need tools to help assess the routing health of your network and potential risks to your data. For years, many companies used BGPmon to gain visibility into what's happening on their network. OpenDNS acquired BGPmon, and then Cisco acquired OpenDNS. Today, Cisco has leveraged the BGPmon real-time monitoring features, expanded its capabilities, and incorporated them into Cisco Crosswork® Network Insights through a cloud-based SaaS model.

This new cloud-based service is designed to proactively track the health of your network and the status of your prefixes. It shows how your prefixes are seen by the internet. Network Insights collects, stores, parses, and analyzes network routing data from many sources, so you can focus on your business instead of installing and maintaining complex software.

With Network Insights, tracking your prefixes is simple. Here's what you need to do:

- Subscribe to the service.
- Create your watch list.
- Create your alarm consumption model.

Network Insights is a hosted application that provides rich analysis, visualization, and alerting on actionable network events. It helps you assess the routing health of your network with information to determine the stability of your networks and potential risks to your IP routing assets. The Network Insights service has four main components.

© 2022 Cisco and/or its affiliates. All rights reserved.

Data streaming and storage

Network Insights uses live BGP data from both public and private data sources. The data streaming, ingestion, storage, parsing, and analytics are all done by Network Insights in the cloud.

Analytics engine

The Network Insights analytics engine tracks the health of your network and the status of your prefixes. Routing data is enriched with other data sources that include RPKI, IRR, WHOIS, and IP geolocation. Collectively they provide prefix ownership, identification, and geographic location information.

Event stream and alarm framework

Network Insights maintains a real-time event stream for tracking every change experienced on the internet. Alarms are generated based on alarm logic that is specific to the alarm type. The alarms are optimized to reduce the number of false positives.

Web portal and APIs

Network Insights is designed to be end to end and API driven. Well-defined, REST-based APIs make it easy to integrate with your existing operations support system and business support systems. You can send alarm notifications to collaboration tools such as Slack in addition to traditional tools like email. Using the web portal, you can configure your settings, browse summary and detailed information about your prefixes, and manage alarms.

Network Insights aggregates global and local routing information and identifies the source of anomalies based on a consensus of the routing databases. It provides a secure and low-risk method of collecting route information at a global scale.

Understand your routing assets

Cisco Crosswork Network Insights is designed for anyone who needs to understand how their networks are routed and how their prefixes are seen from hundreds of other networks worldwide. With live tools, you can see events as they happen. The service will continue to evolve over time with regular updates, keeping your network agile, while helping to limit potentially damaging exposure through negative routing events. Learn more about Network Insights at www.cisco.com/go/crosswork.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C11-2808537-00 04/22

© 2022 Cisco and/or its affiliates. All rights reserved.