Comprehensive Alerting for Route Leaks and Hijackings

Posted by Young Xu (https://blog.thousandeyes.com/author/young/) on September 20, 2016

AddThis

In past blogs, we've explored a specific BGP issue that can have far-reaching, large-scale impacts on networks across the Internet: route leaks and hijackings (https://blog.thousandeyes.com/finding-and-diagnosing-bgp-route-leaks/). In this post, we'll discuss alerting for leaks and hijacks, which is the first step in the process of detecting, diagnosing and ultimately mitigating these notoriously difficult-to-troubleshoot events. While we've touched on BGP alerts for prefix hijacking (https://blog.thousandeyes.com/proactive-bgp-alerting/) in the past, we'll now go into more detail about why route leaks and hijacks may happen and the wide variety of alert rules you can set up to effectively detect these events.

Why Leaks and Hijacks Happen

Before taking steps to detect leaks and hijacks, it can often be useful to understand the reasons why they may happen. In general, the root causes of leaks and hijacks can be divided between unintentional misconfigurations and intentional, malicious hijacks.

Unintentional Misconfigurations

While human error is a common and simply understood cause, it can manifest itself in a variety of different misconfigurations that cause improper route filtering and incorrect routing policies.

For example, one easy way to botch your routes is by mishandling the NO-EXPORT community, which is a community used to tell the recipient not to propagate the route to other autonomous systems (ASes). It isn't uncommon for operators to forget to attach the NO-EXPORT community to their prefix advertisements and accidentally initiate a route leak.

Another common scenario we've seen crop up recently has been the case of misconfigured route optimizers. Route optimizers take other ASes' prefixes and break them up into smaller, more specific prefixes in order to more finely control internal routing. These covered prefixes are never meant to be used outside the route optimizer's AS, but if the covered prefixes are leaked, the route optimizer's AS may inadvertently hijack the prefixes of another AS. We've seen a number of these events in the past, including one where Enzu, a hosting provider, leaked dozens of more specific prefixes (https://blog.thousandeyes.com/finding-and-diagnosing-bgp-route-leaks/) for AWS services like Spotify and Tinder due to the improper filtering of a route optimizer.

Intentional and Malicious Hijacks

Intentional route hijacks can be used for a variety of malicious purposes. Perhaps the most obvious is using hijacks to deny service, as a targeted attack or as a blanketed censorship effort. One of the most infamous examples occurred in 2008, when Pakistan's ISPs hijacked YouTube's routes with a more specific prefix pointing to a null interface, blackholing traffic and thus blocking the site within Pakistan. Unfortunately, the covered prefix was mistakenly leaked to the rest of the Internet, blocking YouTube for everyone else too. The practice of null routing commonly appears as a part of censorship efforts, including the Great Firewall of China (https://blog.thousandeyes.com/deconstructing-great-firewall-china/).

Route hijacks can also be used to inspect or modify traffic for purposes including traffic interception and impersonation, corporate and state espionage, and cryptocurrency theft. BGP man-in-the-middle attacks (http://research.dyn.com/2013/11/mitm-internet-hijacking/) are one type of route hijack commonly used for these malicious activities, where hijackers advertise preferred routes to the destination AS, changing the path entirely to flow through their own AS, or inserting their own network into a legitimate AS path. They then inspect or modify the victim's traffic as it passes through, and then pass the traffic on to its intended destination. Man-in-the-middle attacks are difficult to detect for this very reason, since service isn't disrupted and performance impacts are negligible.

There have also been instances where hijackers choose to re-route only on the reverse path back to the victim so that their attacks are undetectable by traceroute. For this case, use ThousandEyes Agent-to-Agent Tests to give you both network- and routing-layer visibility in both directions (https://blog.thousandeyes.com/network-visibility-for-the-reverse-path/), so you can spot an unwanted AS on both the forward and reverse paths. You'll also want to set up a Private BGP Monitor (https://blog.thousandeyes.com/monitoring-bgp-routes-thousandeyes/) in your own AS to see routing changes on the path from your network to the target, complementing our Public BGP Monitors which provide visibility from the Internet into your environment.

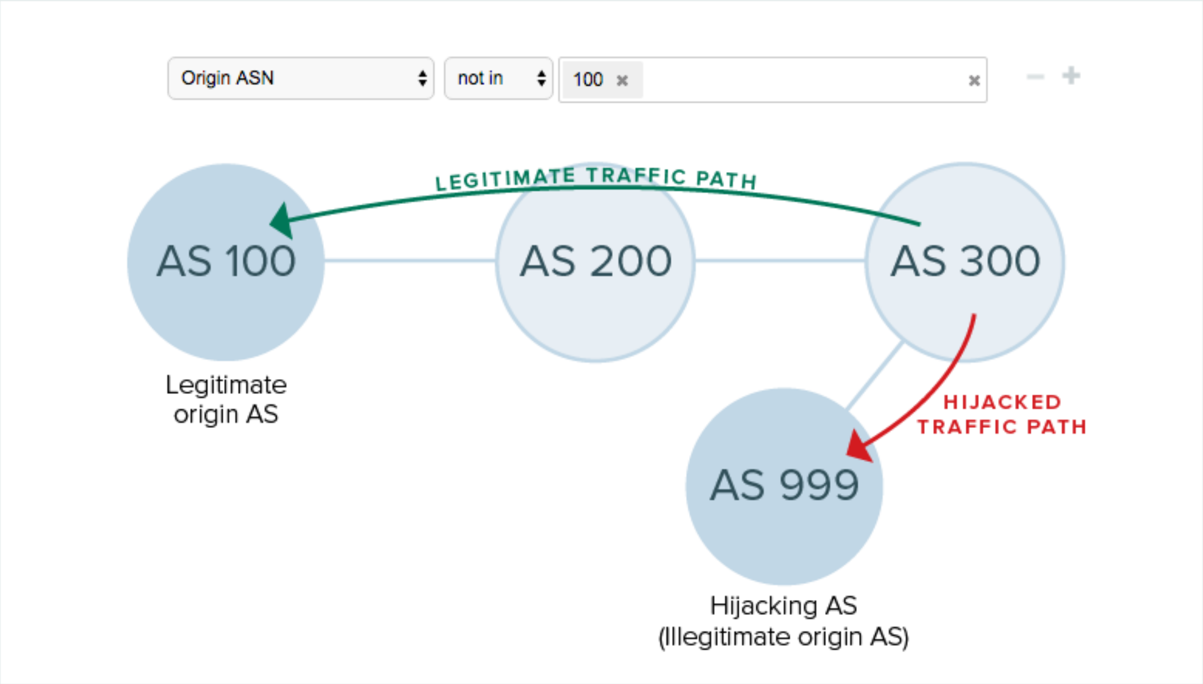
In addition, route hijacks are used for IP squatting and spamming. Hijackers will announce previously unused address space that they don't own, effectively borrowing IP addresses for the purpose of sending spam. By the time the IP space is added to the various spam lists, the hijackers have already moved on to other unannounced addresses.

Comprehensive Alerting

With a good understanding of why leaks and hijacks happen and the mechanisms of how they happen (https://blog.thousandeyes.com/finding-and-diagnosing-bgp-route-leaks/), we can now set up a comprehensive alerting system for specific route leak and hijack scenarios.

Origin ASN

Perhaps the most obvious BGP alert rule is to trigger when the origin autonomous system number (ASN) is not the one you expect (i.e., the service's or its hosting provider's ASN). This catches the most blatant route leaks and hijacks in which the service's prefixes are claimed by another AS entirely.



Origin ASN ⬍ not in ⬍ 100 ×

Figure 1: An alert rule for when the origin AS unexpectedly changes will catch the most blatant route leaks and hijacks where prefixes are claimed by another AS entirely.

Because these events often disrupt service and are easily traceable, they're more likely to be the result of error or censorship rather than targeted, malicious intent. Simply alerting on origin ASN will catch most accidental leaks caused by misconfigurations, as well as many attempts to deny service or squat on IP space, but not the more sophisticated, stealthy activities of hijackers trying to inspect or modify traffic. Read on to learn about other alert types that can catch the more nefarious types of route hijacks.

Next Hop ASN

You can set another BGP alert rule to trigger when the next hop ASNs are not the ones you expect (i.e., the upstream ISPs directly upstream from the origin AS). Because it detects the case where the origin AS doesn't change but the next hop AS does, this alert provides a better threshold for more concealed hijacks that don't disrupt service, including man-in-the-middle attacks, and can also detect inadvertent events that change your routes, but not the origin AS, in unexpected ways.

As an example, consider the case of a man-in-the-middle (MITM) attack. The attacker attempts to insert his network into your routes to a given origin AS by advertising a better (likely shorter) route for that origin AS to you. Because BGP is based on trust, the attacker can make the claim that he is the next hop AS, even if he doesn't actually peer with the legitimate origin AS.

An alert rule for an unexpected change in next hop AS will guard against the majority of MITM attacks, because longer AS paths where the attacker is more than one hop away from the origin AS are less likely to be accepted by would-be victims. When used with Agent-to-Agent Tests, this alert rule will catch unexpected changes in the ASes one hop away from both the source and target networks. This will guard against the often-unnoticed case where smarter attackers hijack only the reverse path.

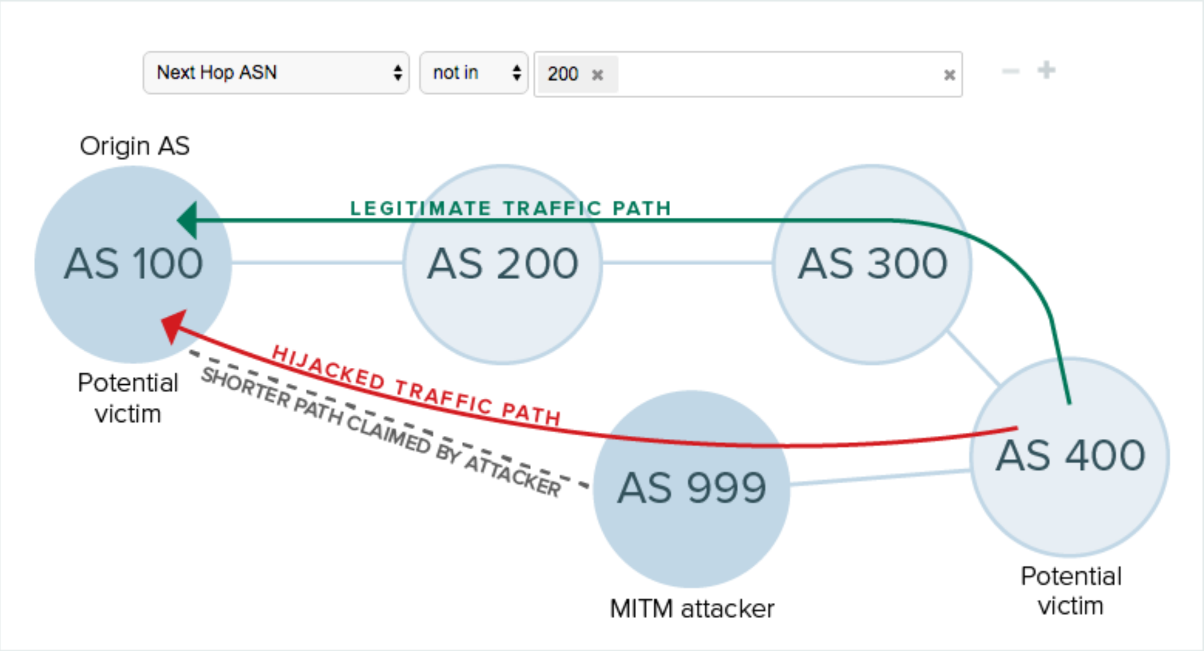

Next Hop ASN | not in | 200 ×

Figure 2: An alert rule for when the next hop AS unexpectedly changes will detect more concealed events that don't disrupt service, like man-in-the-middle attacks.

Covered Prefix

There are also a number of situations, both unintentional and malicious, in which illegitimate prefixes more specific than the legitimate prefixes are leaked and propagated, as in the cases of censorship, misconfigured route optimizers and other errors, and often, ill-intentioned hijackers. Because covered prefixes are always preferred over their covering prefixes, illegitimate covered prefixes are of particular concern, as they can be accepted into routing tables and propagated very quickly.

To guard against this scenario, set BGP alerts for when a covered prefix exists when you don't expect it to. Or, if you do expect covered prefixes, set an alert to trigger when the covered prefix is not one of the sub-prefixes you expect. In this way, you'll always be alerted when a new, more specific prefix appears in routing tables on the Internet when it shouldn't.

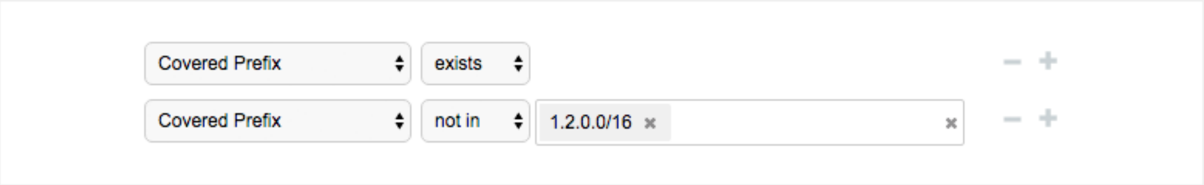
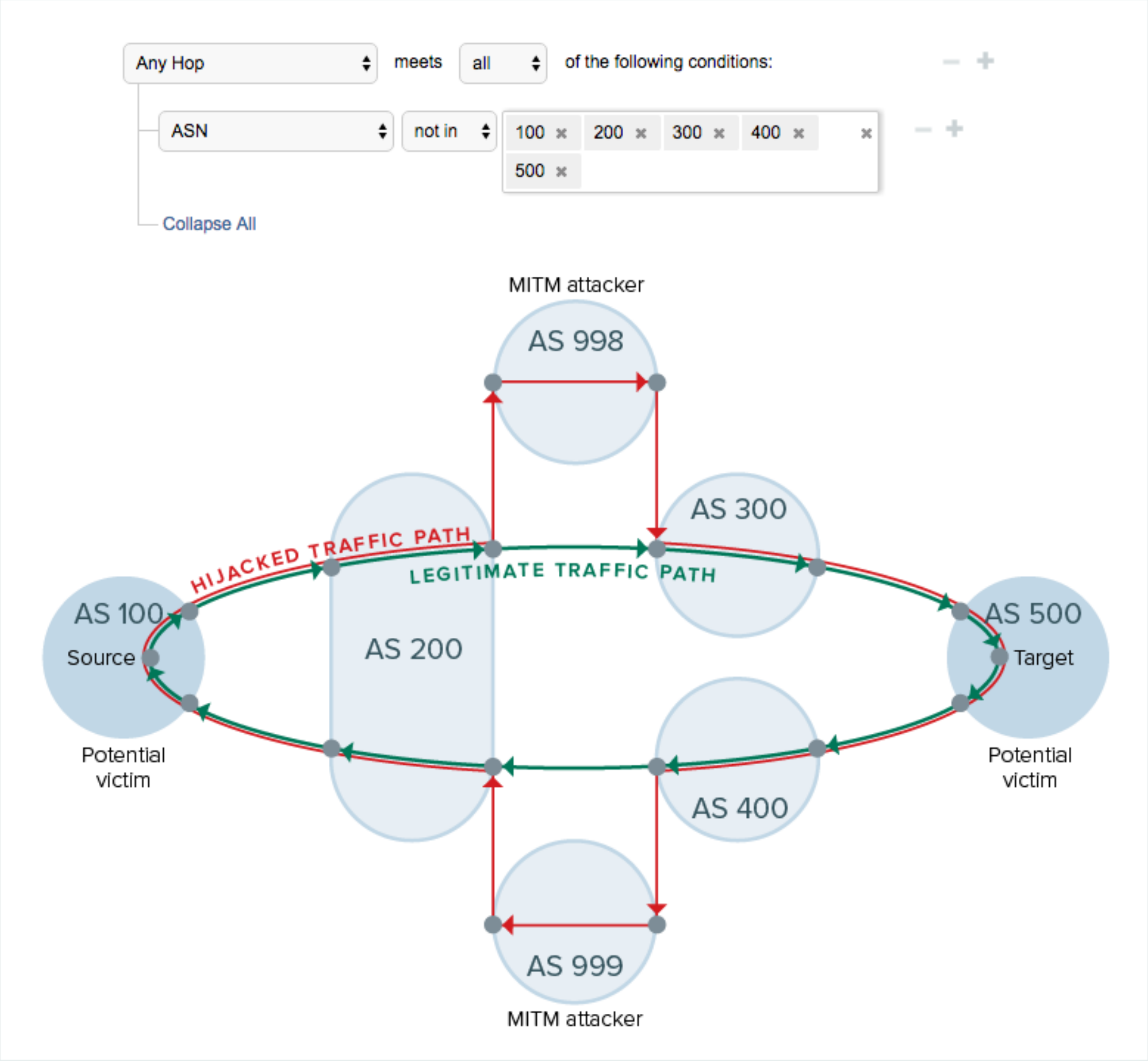

Covered Prefix | exists
Covered Prefix | not in | 1.2.0.0/16 ×

Figure 3: Alert on the appearance of unexpected covered prefixes to catch a variety of events where illegitimate, more specific prefixes are propagated.

Hop-by-hop Path Trace

To alert with hop-by-hop granularity on traffic paths, set up a Path Trace alert in the network layer. As with BGP alerts, using this alert type with Agent-to-Agent Tests will allow you to detect unexpected changes in both the forward and reverse paths from source to target, so you can catch unwanted hijackers on both paths. In addition, you can designate alert conditions for a specific hop number, the last hop or all hops on the path, which allows for the flexibility to alert on changes in any part of your traffic paths. Use alert conditions that trigger when the given hop's ASN or IP address is not as expected to detect both accidental route leaks and malicious hijacks.



Any Hop meets all of the following conditions:

ASN not in 100 200 300 400 500

Figure 4: Use Path Trace alerts to detect unexpected changes in any part of your forward and reverse traffic paths.

You can think of the Path Trace alert type as a more granular, network-layer alert analogous to the origin ASN and next hop ASN alert rules we discussed above. Since you can designate specific hop numbers, this alert type can also detect path changes more than one hop away from the origin AS.

Next Steps

With a thorough alerting system in place constantly combing your data for worrisome changes, you can rest assured that route leaks and hijacks will be detected, whether accidental or malicious. To learn more about the mechanisms of route leaks and hijacks and how you can best detect them, watch our BGP webinar on Detecting Hijacks and Leaks (https://www.thousandeyes.com/resources/detecting-hijacks-and-leaks-webinar).

But keep in mind that the work is not done once you've detected a leak or hijack affecting prefixes you care about. You still need to mitigate the leak—a difficult task, as you'll need to influence the AS paths that other networks choose. Stay tuned for our next blog on mitigating route leaks and hijacks affecting your prefixes and securing BGP to guard against future events.

AddThis

Categories: Product (https://blog.thousandeyes.com/category/product/)

Tags: Alerts (https://blog.thousandeyes.com/tag/alerts/), BGP (https://blog.thousandeyes.com/tag/bgp/), BGP Hijack (https://blog.thousandeyes.com/tag/bgp-hijack/), Peering (https://blog.thousandeyes.com/tag/peering/)

Subscribe to the Blog

Stay connected with blog updates and outage reports delivered while they're still fresh.

Email Address

Subscribe

« Previous Post (https://blog.thousandeyes.com/monitoring-ftp-servers/)

Next Post » (https://blog.thousandeyes.com/monitoring-voip-rtp-enterprise-wan/)

0 Comments **ThousandEyes** 1 **Login**

♡ **Recommend** 1 **Share** **Sort by Best**

Start the discussion…

Be the first to comment.

ALSO ON **THOUSANDEYES**

Finding and Diagnosing BGP Route Leaks
3 comments • 2 years ago•
avinash — Thank you nick for the explanation...apologize for the delay in reply...

How Virtual Private Networks Impact Performance
1 comment • 2 months ago•
gravitysystems — Informative blog. thank you for sharing with us..

Troubleshooting Path MTU and TCP MSS Problems
1 comment • 2 years ago•
skalwani — Very useful!

Benchmarking Network Performance in China
2 comments • 2 months ago•
Young Xu — We don't currently have a Cloud Agent in Shenzhen, but you can monitor from Cloud Agents in Zhuhai, Foshan or Guangzhou which are …

✉ **Subscribe** **Add Disqus to your siteAdd DisqusAdd** 🔒 **Privacy**

Subscribe to the Blog

Stay connected with blog updates and outage reports delivered while they're still fresh.

Product

Product Overview (https://www.thousandeyes.com/product/tour/overview)
Network Data (https://www.thousandeyes.com/product/tour/network-data)
Visual Analysis (https://www.thousandeyes.com/product/tour/visual-analysis)
Network Insights (https://www.thousandeyes.com/product/tour/network-insights)
Shared Knowledge (https://www.thousandeyes.com/product/tour/shared-knowledge)

Network Intelligence (https://www.thousandeyes.com/network-intelligence)

Enterprise Agents (https://www.thousandeyes.com/product/enterprise-agents)
Cloud Agents (https://www.thousandeyes.com/product/cloud-agents)
Endpoint Agents (https://www.thousandeyes.com/product/endpoint-agents)

Pricing (https://www.thousandeyes.com/pricing)

Solutions

Enterprise WAN & LAN (https://www.thousandeyes.com/solutions/enterprise-it)
Application Delivery (https://www.thousandeyes.com/solutions/application-delivery)
Cloud Migration (https://www.thousandeyes.com/solutions/cloud-migration)
Network Monitoring (https://www.thousandeyes.com/network-monitoring)

BGP (https://www.thousandeyes.com/solutions/bgp)
CDN (https://www.thousandeyes.com/solutions/cdn)
DDoS (https://www.thousandeyes.com/solutions/ddos)
DNS (https://www.thousandeyes.com/solutions/dns)
ISP (https://www.thousandeyes.com/solutions/isp)
SaaS (https://www.thousandeyes.com/solutions/saas)
VoIP (https://www.thousandeyes.com/solutions/voip)
Website (https://www.thousandeyes.com/solutions/website)

Customers

Customer Overview (https://www.thousandeyes.com/customers)

Carriers & Hosting (https://www.thousandeyes.com/customers/carriers-and-hosting)
Consumer Web (https://www.thousandeyes.com/customers/consumer-web)
Financial Services (https://www.thousandeyes.com/customers/financial-services)
Healthcare (https://www.thousandeyes.com/customers/healthcare)
Media & Entertainment (https://www.thousandeyes.com/customers/media-and-entertainment)
Retail (https://www.thousandeyes.com/customers/retail)
Software (https://www.thousandeyes.com/customers/software)

Resources

Resource Center (https://www.thousandeyes.com/resources)
Upcoming Webinars (https://www.thousandeyes.com/events)

Industry Events (https://www.thousandeyes.com/events)
ThousandEyes Connect (https://www.thousandeyes.com/events/connect)

Search (https://www.thousandeyes.com/search)

Blog (https://blog.thousandeyes.com)

About

Company (https://www.thousandeyes.com/about)
Board & Investors (https://www.thousandeyes.com/board-and-investors)
Management (https://www.thousandeyes.com/management)
Customers (https://www.thousandeyes.com/customers)
Partners (https://www.thousandeyes.com/partners)
Contact (https://www.thousandeyes.com/contact)

Careers (https://www.thousandeyes.com/careers)

Newsroom (https://www.thousandeyes.com/newsroom)
Media Kit (https://www.thousandeyes.com/media-kit)

Support

Support Login (https://app.thousandeyes.com/sfdc/community/home/)
Product Login (https://app.thousandeyes.com)
API Reference (http://developer.thousandeyes.co

Trust (https://www.thousandeyes.com/trust)
Service Status (https://www.thousandeyes.com/trust/status)
Confidentiality & Integrity (https://www.thousandeyes.com/trust/confidentiality-and-integrity)
Privacy (https://www.thousandeyes.com/trust/privacy)

USA Sales: +1 (800) 757-1353 (tel:18007571353)
301 Howard Street Suite 1700 San Francisco, CA USA 94105

Terms of Use (https://www.thousandeyes.com/website-terms-of-use) | Privacy Policy (https://www.thousandeyes.com/privacy)

(https://www.facebook.com/ThousandEyes)

(https://www.twitter.com/thousandeyes)

(https://www.linkedin.com/company/thousandeyes)

(https://plus.google.com/+Thousandeyes)