SCION Day

Zurich, Switzerland

22 October 2024

Who am I?

Chris Gibson

CEO/Executive Director, Forum of Incident Response and Security Teams, Inc. aka FIRST

Chris spent over 12 years working in the Computer Emergency Response Team (CERT) whilst at Citigroup and, for 10 years, was part of the leadership of the Forum of Incident Response and Security Teams (FIRST); 2 as Chair.

Within FIRST he implemented the Fellowship program. This was created to fund CERTs from UN-designated “Least Developed Countries” (LDCs) allowing them both to join FIRST and attend conferences and training.

Chris joined the UK's Cabinet Office, in 2013, to build, launch and lead the UK’s first formally chartered national CERT - CERT-UK.

When CERT-UK was subsumed, in 2016, into the UK's National Cyber Security Centre he spent some time as a CISO.

Chris joined FIRST as it’s Executive Director in May 2019.

Chris’ experience has allowed him to work with colleagues from both inside some of the world’s largest global financial institutions with the complexities that brings and also with colleagues from the incident response community, with members ranging from Microsoft and Oracle through to the national CERTs of Azerbaijan to Zambia.

Why Am I Here?

FIRST is the Forum of Incident Response and Security Teams. The idea of FIRST goes back until 1989, only one year after the CERT(r) Coordination Center was created after the infamous Internet worm. Back then incidents already were impacting not only one closed user group or organization, but any number of networks interconnected by the Internet.

It was clear from then on that information exchange and cooperation on issues of mutual interest like new vulnerabilities or wide ranging attacks - especially on core system like the DNS servers or the Internet as a critical infrastructure itself - were the key issues for security and incident response teams.

Since 1990, when FIRST was founded, its members have resolved an almost continuous stream of security-related attacks and incidents including handling thousands of security vulnerabilities affecting nearly all of the millions of computer systems and networks throughout the world connected by the ever growing Internet.

FIRST brings together a wide variety of security and incident response teams including especially product security teams from the government, commercial, and academic sectors.

What is the root cause of the problems we face?

- The internet's fundamental design prioritised openness and resilience over security, and retrofitting security onto this foundation is a complex task.
- New technologies and protocols aim to address some of the core security issues in internet architecture. However, their adoption and implementation on a global scale will take time.
- The internet is more secure than it has ever been but it's not universally or absolutely secure. Security on the internet is an ongoing process of identifying vulnerabilities, developing protections, and adapting to new threats as they emerge.

So, really, Why Am I Here?

I’m here to highlight real world cyber incidents that could have been mitigated or defeated by the SCION technology

BGP Hijacking of YouTube (2008): Pakistan Telecom accidentally blocked YouTube worldwide by announcing false BGP routes.

Why did this happen?

After receiving a censorship order from the telecommunications ministry directing that YouTube.com be blocked, Pakistan Telecom went even further. By accident or design, the company broadcast instructions worldwide claiming to be the legitimate destination for anyone trying to reach YouTube's range of Internet addresses.

The security weakness lies in why those false instructions, which took YouTube offline for two hours on Sunday, were believed by routers around the globe. That's because Hong Kong-based PCCW, which provides the Internet link to Pakistan Telecom, did not stop the misleading broadcast--which is what most large providers in the United States and Europe do.

China Telecom's BGP Route Leak (2010): China Telecom incorrectly announced BGP routes that led to a significant portion of global internet traffic being routed through China for about 18 minutes.

Why did this happen?

The incident occurred because of a BGP route leak at Swiss data center colocation company Safe Host, which accidentally leaked over 70,000 routes from its internal routing table to the Chinese ISP.

The Border Gateway Protocol (BGP), which is used to reroute traffic at the ISP level, has been known to be problematic to work with, and BGP leaks happen all the time.

However, there are safeguards and safety procedures that providers usually set up to prevent BGP route leaks from influencing each other's networks.

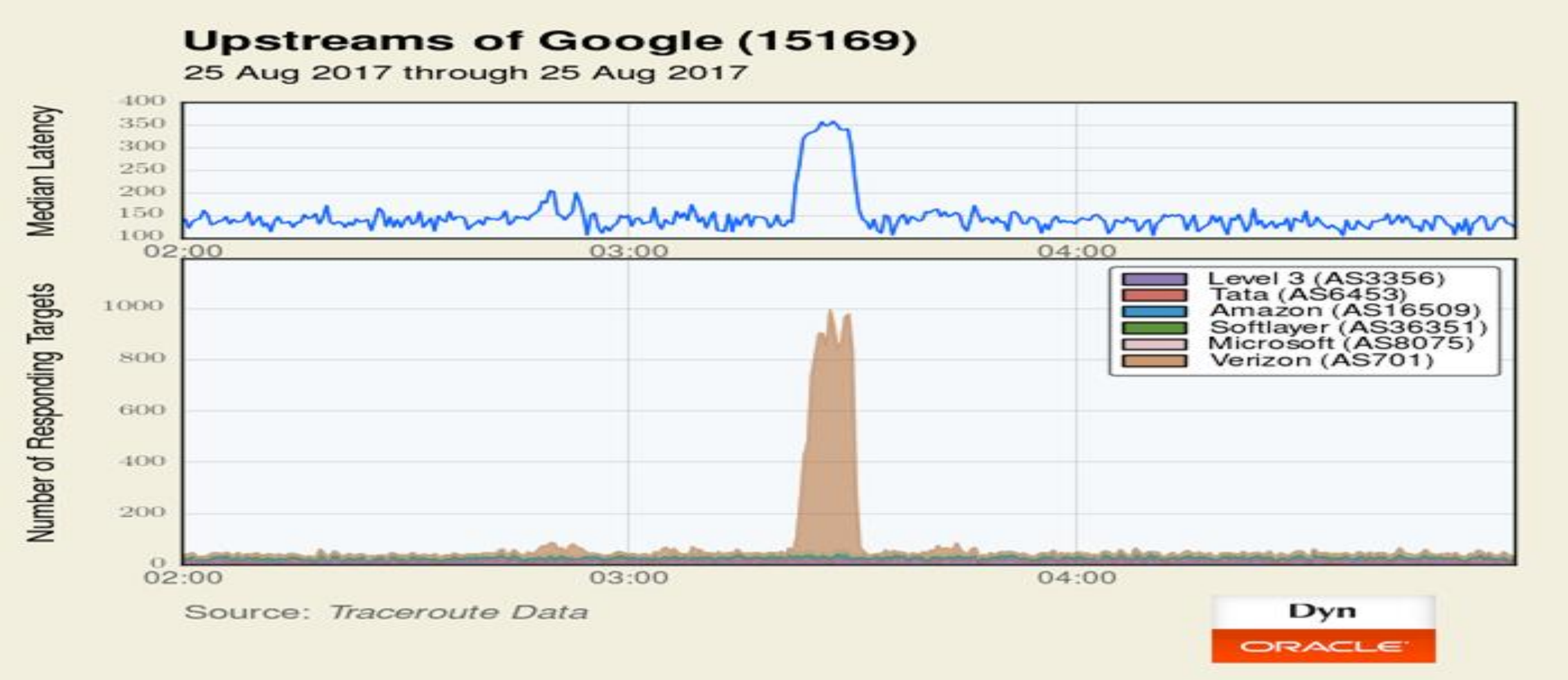
But instead of ignoring the BGP leak, China Telecom re-announced Safe Host's routes as its own, and by doing so, interposed itself as one of the shortest ways to reach Safe Host's network and other nearby European telcos and ISPs.

For the subsequent hours, until China Telecom operators realized what they have done, traffic meant for many European mobile networks was rerouted through China Telecom's network.

An academic paper published by experts from the US Naval War College and Tel Aviv University in October last year blamed China Telecom for "hijacking the vital internet backbone of western countries."

The report argued that the Chinese government was using local ISPs for intelligence gathering by systematically hijacking BGP routes to reroute western traffic through its country, where it can log it for later analysis.

BGP Leak by Google (2017): A Google BGP configuration error caused internet traffic destined for major CDNs to be routed through Google's network, leading to widespread service disruptions.



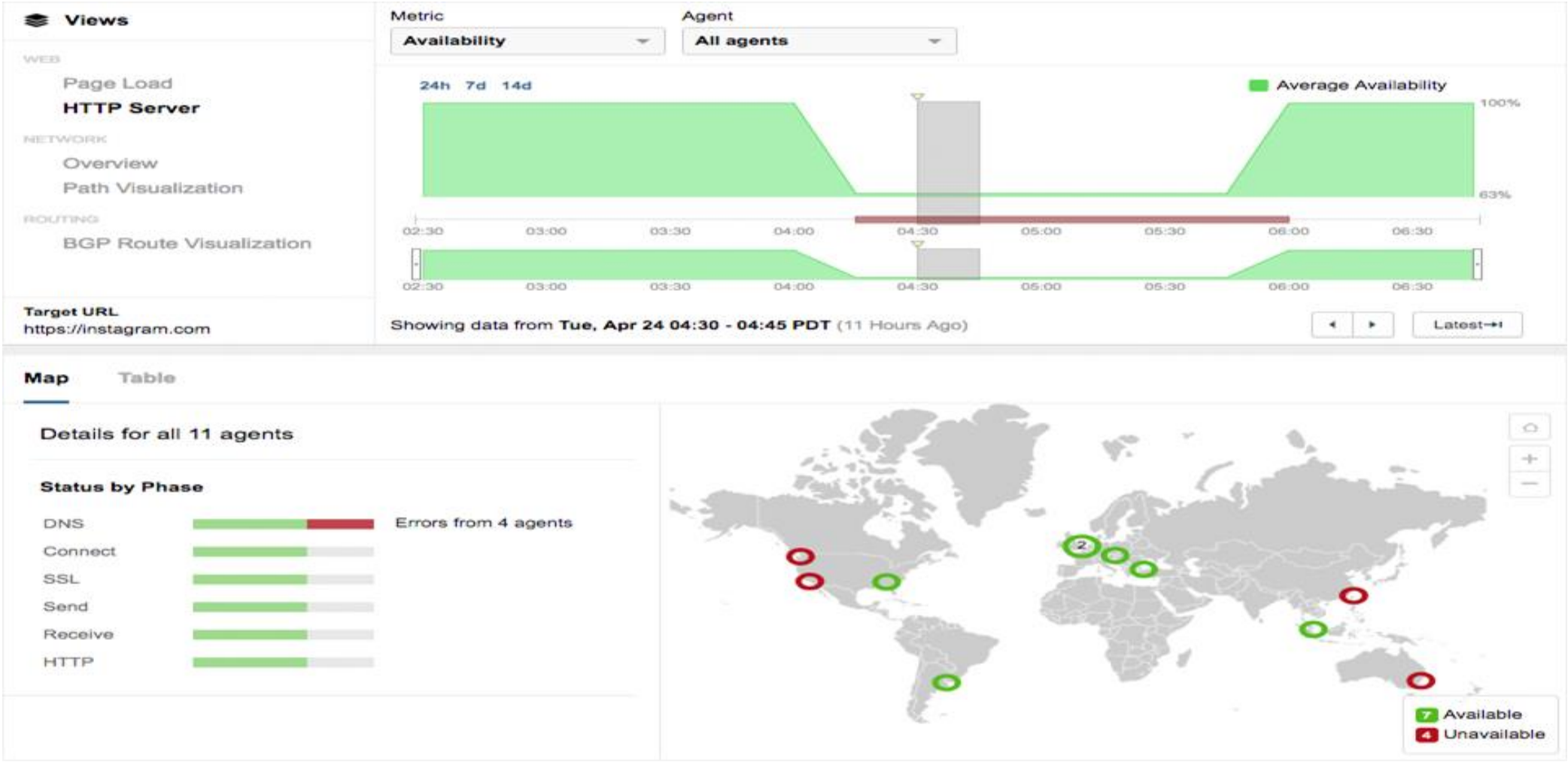
Why did this happen?

The routing incident caused large-scale internet disruption. It hit Japanese users the hardest, slowing or blocking access to websites and online services for dozens of Japanese companies.

Google accidentally leaked BGP prefixes it learned from peering relationships, essentially becoming a transit provider instead of simply exchanging traffic between two networks and their customers. This also exposed some internal traffic engineering that caused many of these prefixes to get de-aggregated and therefore raised their probability of getting accepted elsewhere.

The incident technically lasted less than ten minutes, but spread quickly around the Internet and caused some damage. Connectivity was restored, but persistently slow connection speeds affected industries like finance, transportation, and online gaming for several hours. Google apologized for the trouble, saying it was caused by an errant network setting that was corrected within eight minutes of its discovery.

Route 53 BGP Hijack (2018): Amazon's Route 53 DNS service was briefly hijacked to redirect users of a cryptocurrency website to a phishing site.

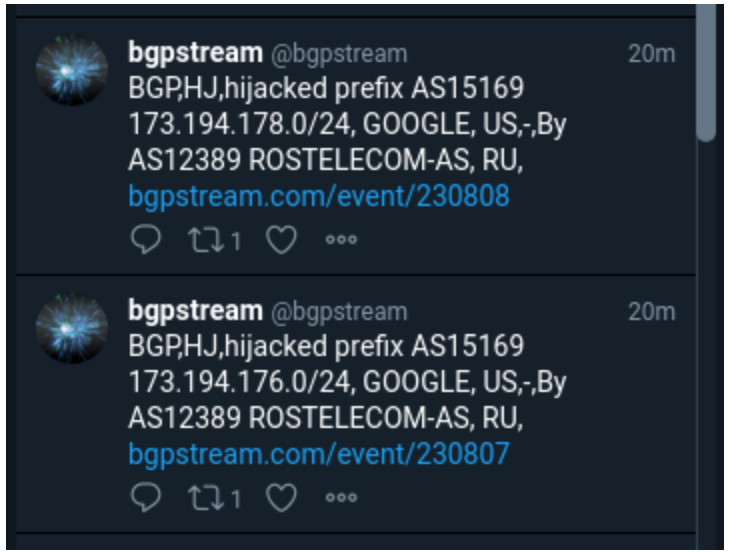


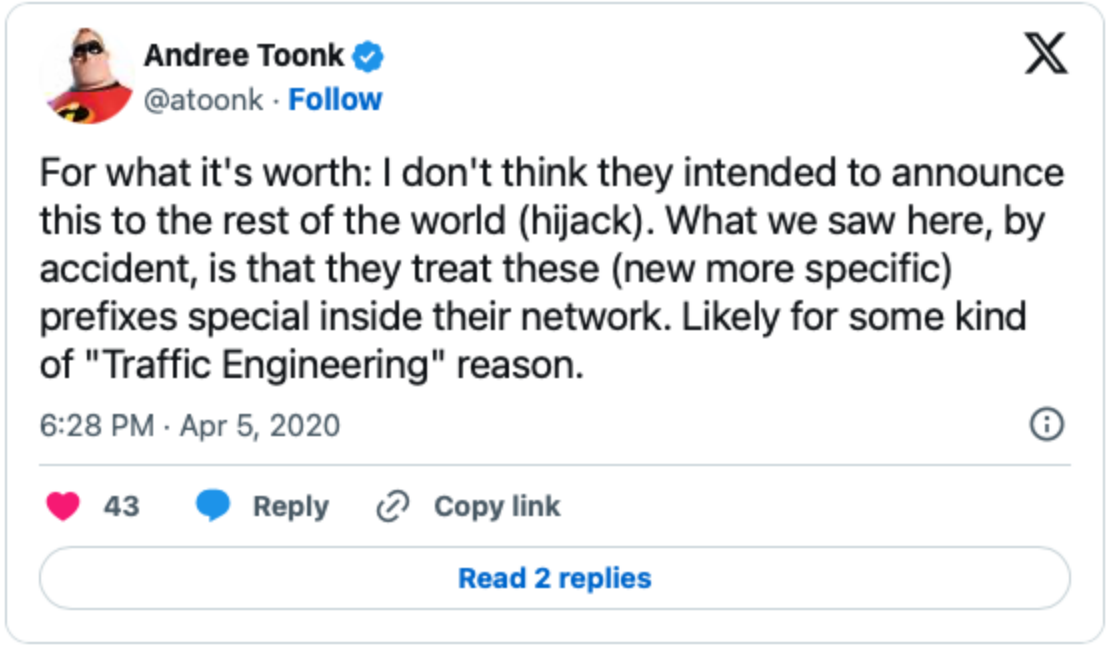
Why did this happen?

A well-known weakness in Border Gateway Protocol routing was exploited this week, as Amazon Web Services' DNS traffic was hijacked for two hours, enabling the attacker to steal about $150,000 in cryptocurrency from users of a cryptocurrency wallet.

The attack, which rerouted traffic for five Class C networks registered to Amazon Web Services from 11 a.m. until 1 p.m. (UTC), could have affected as many as 1,280 IP addresses. During the incident, some traffic to the cryptocurrency website MyEtherWallet was redirected to a server in Russia, where the cryptocurrency was stolen from unwitting customers, according to Kevin Beaumont, a U.K.-based security researcher.

Rostelecom BGP Leak (2020): Russian ISP Rostelecom incorrectly announced BGP routes that led to misrouting of traffic for major services like Google, Amazon, and Cloudflare





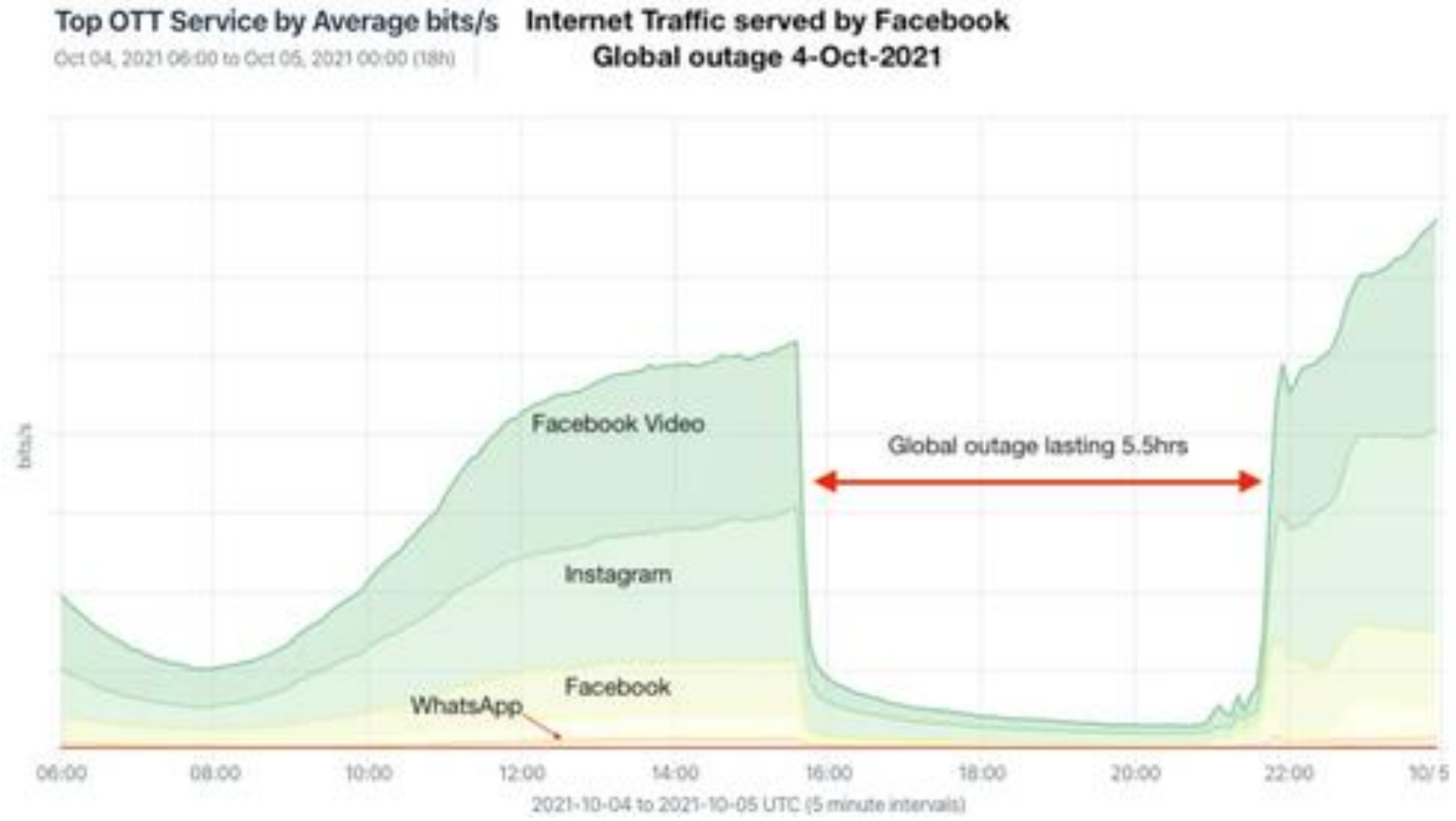
Why did this happen?

BGP-enabled devices advertise, or share, information on the routes they can offer to the BGP devices on neighboring networks. These networks then share that information to their own neighboring networks. Changes to ‘best routes’ thus rapidly get promulgated throughout the internet. But BGP was first created in 1989 and in use 1994 — at a time when the internet was still largely a club of friends who did not require security. It is based on trust between devices, and when one network advertises a new ‘best route’, it is implicitly accepted by neighboring networks and re-advertised.

The incident affected more than 8,800 internet traffic routes from 200+ networks, and lasted for about an hour.

Impacted companies included big names such as Google, Amazon, Facebook, Akamai, Cloudflare, GoDaddy, Digital Ocean, Joyent, LeaseWeb, Hetzner, and Linode.

Facebook Global Outage (2021): A configuration error led to Facebook withdrawing its BGP routes, effectively disconnecting its services from the internet.



And the impact of this?

Security experts identified the problem as a Border Gateway Protocol (BGP) withdrawal of the IP address prefixes in which Facebook's Domain Name System (DNS) servers were hosted, making it impossible for users to resolve Facebook and related domain names, and reach services.

The outage cut off Facebook's internal communications, preventing employees from sending or receiving external emails, accessing the corporate directory, and authenticating to some Google Docs and Zoom services. The New York Times reported that employees were unable to access buildings and conference rooms with their security badges.

Conclusions

There are fundamental weaknesses in the design of the internet - we all know this. The internet is more secure than it has ever been but it's not universally or absolutely secure. Security on the internet is an ongoing process of identifying vulnerabilities, developing protections, and adapting to new threats as they emerge.

In all these cases mentioned, Scion's key features – path awareness and control, multi-path communication, cryptographic verification of routing information, and the isolation domain structure – would have provided more resilience, faster recovery, and better containment of routing issues.