ANAPAYA

BGP Hijacking Throughout Time

April 2017–April 2018

In a daring con lasting 12 months, an ad fraud network dubbed "3ve" by investigators used BGP hijacking to co-opt more than **1.5 million IP addresses** belonging to reputable organisations, including the US Air Force[1].

A complex, fraudulent digital advertising infrastructure was used for the express purpose of misleading and defrauding companies.

The IP addresses were used to conceal fraudulent activity that impersonated **billions of ad views** hosted on pages run by the scammers themselves. Normally, such a scam would have seemed suspicious to advertisers, but the page viewing requests were funneled through the hijacked IP addresses. The attackers were able to con over **29 million dollars from ad networks.**

VISA

April 2017

Vast amounts of network traffic belonging to **MasterCard, Visa**[2] and more than 24 other **financial services** companies were incorrectly routed through a **Russian government-controlled** telecom under **unexplained circumstances**. The hijacking could have allowed individuals in Russia to decrypt **sensitive financial data** at the time of the hijacking or at a future date.

NETFLIX

November 2017

A route leak lasting **more than an hour and half**[3] caused large scale networking service degradation **across North America** late in 2017. The service outage caused users to experience extremely slow speeds or complete service denial. The incident affected companies like **Comcast, Bell Canada and Netflix**.

Microsoft

December 2017

Two BGP hijacking incidents[4] affected **high-profile sites** (Google, Apple, Facebook, Microsoft, Twitch, NTT Communications and Riot Games) when data and traffic was rerouted to a previously unused **Russian route**. It is still unknown whether this was a **coordinated attack** or simple mistake.

April 2018

Amazon was the victim of a BGP Hijack[5], losing a number of their **cloud services IP addresses** for over **two hours**.

Around **1300 IP addresses** were redirected to rogue destinations where unknown hijackers fronted as cryptocurrency website MyEtherWallet.com. Over $150 000 worth of digital currency was stolen from Amazon's end-users, leading to great reputational damage in terms of Amazon's security image.

amazon

12 November 2018

Google

Data routed to **Google** was rerouted to **China Telecom**[6], through a convoluted path which included Transtelecom in Russia, and a small ISP in Nigeria.

Many of Google's **core services** (G-suite, Google Search or Google Analytics) were globally unavailable for about **2 hours**. In addition to this, valuable private user-information is suspected to have fallen into the hands of the attackers, including business and user accounts and contact information.

21 November 2018

For nearly **30 months**, internet traffic going to **Australian Department of Defense** websites flowed through several of China Telecom's data centers.[7]

From 2015 to 2018 China Telecom, a **Chinese state-owned telecommunication company**, could see what devices were connecting to Australian defense sites, for how long and possibly more. A South Korean ISP quietly made an unannounced BGP change to cause sensitive Australian defence data to route through China Telecom's backbone network. Despite concerns over **Australia's national security**, neither China Telecom or the South Korean ISP have responded to the incident.

08 May 2019

Data traffic going through one of the Taiwan Network Information Centre's public DNS was rerouted to an entity in Brazil for three and a half minutes.[8]

During that time, **public and government-classified Taiwanese records** were leaked to the attacker, posing a serious threat to the **national security and sovereignty of Taiwan**. It is still not known who committed the deed, but it is widely recognised as a **willful attack**.

06 June 2019

A Swiss data center accidentally leaked over **70 000 internal routes** to **China Telecom**.[9]

This affected mobile operators in France, Switzerland and the Netherlands. For over **2 hours**, users on the affected mobile network experienced slow connections or the inability to connect to some servers. A much more troubling consequence is the possible **leaked private** information of users, which ultimately resulted in negative public perception of the mobile operators.It is still not known if this was an intentional attack or an error.

24 June 2019

CLOUDFLARE

Cloudflare recorded a **15% drop in global internet traffic** following a BGP incident[10] that lasted over an hour before the provider could rectify the issue.

Besides Cloudflare, Amazon, and Facebook, networks owned by Comcast, T-Mobile and Bloomberg were also affected, as well as networks attributed to at least nine American **banks or credit associations**.

01 April 2020

More than **200 of the world's largest CDNs** (Content Delivery Networks) suffered a BGP hijack that lasted for **over an hour**.[11]

Hundreds of thousands of web-users around the world instantly lost access to the services provided by companies such as Google, Amazon, Facebook, and Cloudflare. Many company websites and online services were unable to operate during this hour. The CDNs themselves suffered reputational damage for failing to adequately protect the privacy and information of their users. The attack was credited to **Russian telecom company, Rostelecom**.

17 April 2021

In a large BGP routing leak out of India, over 30,000 BGP prefixes were hijacked via Vodafone Idea Ltd (**AS55410**) causing a **13X spike** in inbound traffic[12].

Prefixes were from around the globe but mostly US including Google, Microsoft, Akamai, and Cloudflare.

03 February 2022

Hackers stole roughly **$1.9 million** from South Korean cryptocurrency platform KLAYswap after they pulled off a BGP hijack against the server infrastructure of one of the platform's providers.[13]

The attack lasted for two hours, and KLAYswap has confirmed the incident. Affected users have been issued compensation. This attack was unique, since hackers accessed KLAYswap's network through the third-party communication platform KakaoTalk.

25 April 2022

Some Twitter traffic was briefly funnelled through a **Russian ISP**, thanks to a BGP mishap. The mishap lasted for about 45 minutes before **RTCOMM**, a leading ISP in Russia, stopped advertising its network as the official way for other ISPs to connect to the widely used Twitter IP addresses.[14]

Even before RTCOMM dropped the announcement, safeguards prevented most large ISPs from abiding by the routing directive. The 45-minute hijacking was possibly an error, not an attack.

26 July 2022

For a 12-hour period on July 26 and 27, internet users trying to access a portion of **Apple's** network were sent in the wrong direction by instructions issued by Russian operator **Rostelecom**.[15]

Nothing Apple has said indicates any significant disruption to their business, as the company was quick to mitigate the problem by issuing routing instructions that countermanded those from Rostelecom. Nevertheless, Rostelecom's notification was widely disseminated around the world, publicly putting Apple's network security measures into question.

August 2022

amazon

Amazon recently lost control of IP addresses it uses to host cloud services and took more than **three hours** to regain control. An analysis showed that this lapse allowed hackers to steal **$235,000 in cryptocurrency** from users of one of the affected customers.[16]

The hackers seized control of roughly 256 IP addresses through BGP hijacking, a form of attack that exploits known weaknesses in the core Internet protocol.

Visit anapaya.net

to learn more on how SCiON can help protect your company from being the next victim

Sources

1. Ars Technica, *How 3ve's BGP hijackers eluded the Internet–and made $29M*, 21 December 2018
2. Ars Technica, Russian-controlled telecom hijacks financial services' Internet traffic, 27 April 2017
3. Oracle Developers, *Widespread Impact Caused by Level 3 BGP Route Leak*, 7 November 2017
4. Internet Society, *Another BGP Routing Incident Highlights an Internet Without Checkpoints*, 13 December 2017
5. Ars Technica, *Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency*, 24 April 2018
6. Thousand Eyes, *Internet Vulnerability Takes Down Google*, 12 November 2018
7. Bank Info Security, *Did China Spy on Australian Defense Websites?* 21 November 2018
8. MANRS, *Public DNS in Taiwan the latest victim to BGP hijack*, 15 May 2019
9. ZDnet, *For two hours, a large chunk of European mobile traffic was rerouted through China*, 7 June 2019
10. Catchpoint, *BGP Leak Highlights the Fragility of the Internet with Real Consequences*, 26 June 2019
11. ZDnet, *Russian telco hijacks internet traffic for Google, AWS, Cloudflare, and others* 05 April 2020
12. APNIC, *A major BGP route leak by AS55410* 26 April 2021
13. The Record, *KlaySwap crypto users lose funds after BGP hijack* 14 February 2022
14. Ars Technica, *Some Twitter traffic briefly funneled through Russian ISP, thanks to BGP mishap* 29 March 2022
15. Comms Risk, *Why Is Network Hijacking Not Considered a Threat to National Security?* 22 December 2022
16. Ars Technica, *How 3 hours of inaction from Amazon cost cryptocurrency holders $235,000* 23 September 2022