The Imperative of Cybersecurity in Telecommunications: Are Our ISPs Keeping Up?

In an era where digital connectivity is the backbone of modern society, the security of our telecommunications networks has never been more critical. Yet, recent incidents, such as the StormBamboo attacks targeting Internet Service Providers (ISPs), raise pressing questions about the adequacy of the current cybersecurity measures related to our internet providers.

The StormBamboo Incident: A Wake-Up Call

StormBamboo, a sophisticated cyber-espionage group, has recently been in the spotlight for targeting ISPs across the globe. StormBamboo was altering DNS query responses for specific domains tied to automatic software update mechanisms. They appeared to target software that used insecure update mechanisms, such as HTTP, and did not properly validate digital signatures of installers. Therefore, when these applications went to retrieve their updates, instead of installing the intended update, they would install malware. I recently created a video (https://youtu.be/F7-J4-e6aLk) on my YouTube channel explaining some of these DNS attacks which are increasing in frequency.

While I understand the need to balance security against performance, especially in a scale as large as an ISP, there needs to be way for customers to sign up for better security if they wish. Th more savvy users might switch their DNS to Google (8.8.8.8) or Cloudflare (1.1.1.1) or even Quad9 (9.9.9.9) but the majority of end users would be using the default ISP DNS for their internet traffic.

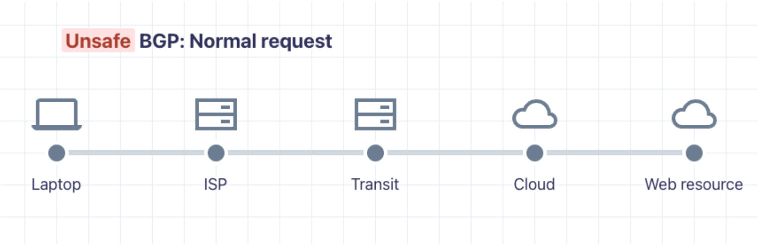
BGP Security: Protecting the Internet's Routing System

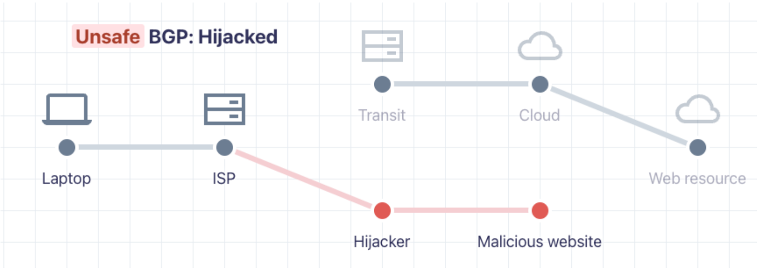
As explained by Cloudflare on their Border Gateway Protocol (BGP) security page (https://isbgpsafeyet.com), the BGP is another critical component of the internet's infrastructure, responsible for routing data between different networks. BGP hijacking, where malicious actors reroute traffic through compromised networks, can lead to data interception and large-scale disruptions. This lack of security in BGP can be a vulnerability that can be exploited by malicious actors to reroute traffic as it goes through the internet.

As we all know, the Internet isn't controlled by a single entity - it consists of thousands of autonomous systems with nodes located all around the world in a massive graph topology. The way BGP works is by having each node determine how to route packets based solely on the information received from its directly connected nodes ("from" and "to").

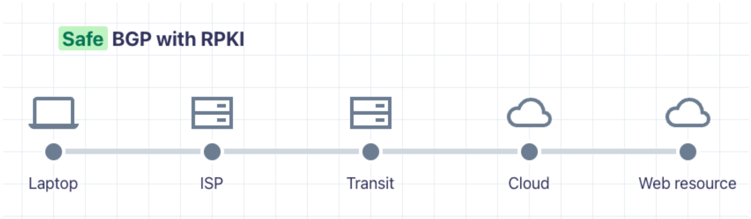
For example, in the simple 5 node network "A→B→C→D→E", node A can only determine how to reach E based on the information provided by B. and Node B, in turn, knows about the network via A and C, and so on.

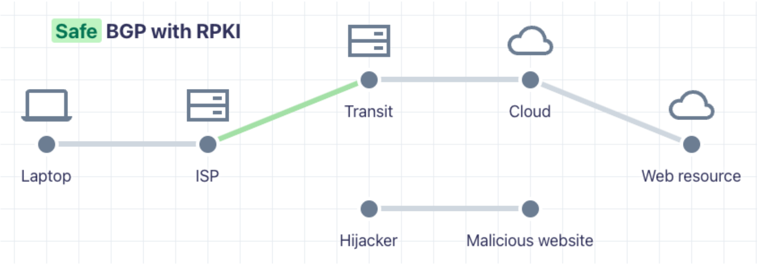
A BGP hijack occurs when a malicious node deceives another node by lying about the routes for its neighbours. Without security protocols, this setup can be used to spread misinformation from node to node, and in turn cause many nodes to attempt to use these incorrect, non-existent, or malicious routes. Courtesy of Cloudflare, this process is illustrated below.



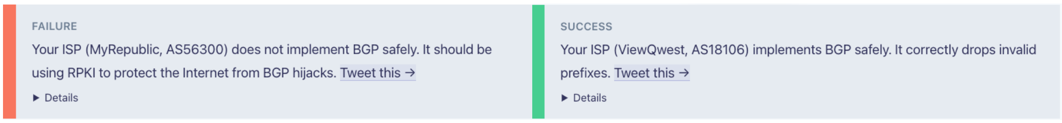


To mitigate these risks, ISPs should adopt more stringent BGP security measures. One of the tools available to ISPs is the Resource Public Key Infrastructure (RPKI, which can provide cryptographic verification of route origins to prevent hijacking as shown in the diagram below (courtesy of Cloudflare).





Despite its effectiveness, RPKI adoption remains inconsistent and very few ISPs are implementing it. ISPs must prioritise its implementation and ensure ongoing monitoring and verification of their routing tables. Some test results are shown below.



FAILURE

Your ISP (MyRepublic, AS56300) does not implement BGP safely. It should be using RPKI to protect the Internet from BGP hijacks. Tweet this →

▶ Details

SUCCESS

Your ISP (ViewQwest, AS18106) implements BGP safely. It correctly drops invalid prefixes. Tweet this →

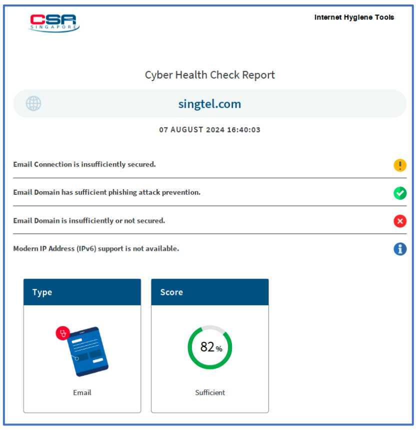
▶ Details

Cloudflare's site "Is BGP Safe Yet?" (https://isbgpsafeyet.com/) is a great resource for users to test the security of their ISPs BGP configuration, and sad to say, yet again our big ISPs in Singapore are deemed unsafe by not implementing RPKI, with the exception of ViewQwest, which has been deemed "safe" by the test with their implementation of RPKI.

Email Server Security: The First Line of Defence

Let's talk about the overall security posture of ISPs. The most obvious place to start looking is at email servers. ISPs manage vast amounts of sensitive information through their email servers, making them prime targets for cybercriminals. Effective security measures for these servers include the implementation of robust encryption protocols, regular software updates, and rigorous authentication processes. Despite these necessary precautions, a quick check using the Internet Hygine Portal (IHP) tool (https://www.csa.gov.sg/Tips-Resource/internet-hygiene-portal) offered by the Cyber Security Agency (CSA) of Singapore, we can see that some ISPs may still fall short in their defences.

Running a check using the IHP tool on the email domain of a few local Singapore ISPs, the results are surprising. Singtel and M1 got a score of 82%, while Starhub got a score of only 78%. The only local ISP on the CSA wall of fame is ViewQwest as the only ISP with a perfect score of 100%.



Internet Hygiene Tools

Cyber Health Check Report

singtel.com

07 AUGUST 2024 16:40:03

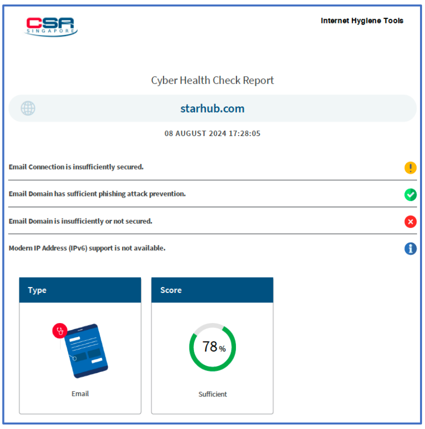
Email Connection is insufficiently secured. !

Email Domain has sufficient phishing attack prevention. ✓

Email Domain is insufficiently or not secured. ✗

Modern IP Address (IPv6) support is not available. ℹ

Type	Score
Email	82% Sufficient



Internet Hygiene Tools

Cyber Health Check Report

starhub.com

08 AUGUST 2024 17:28:05

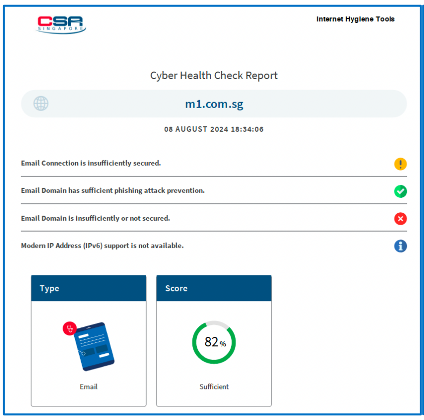
Email Connection is insufficiently secured. !

Email Domain has sufficient phishing attack prevention. ✓

Email Domain is insufficiently or not secured. ✗

Modern IP Address (IPv6) support is not available. ℹ

Type	Score
Email	78% Sufficient



Internet Hygiene Tools

Cyber Health Check Report

m1.com.sg

08 AUGUST 2024 18:34:06

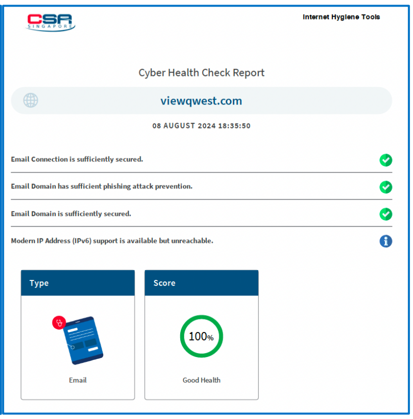
Email Connection is insufficiently secured. !

Email Domain has sufficient phishing attack prevention. ✓

Email Domain is insufficiently or not secured. ✗

Modern IP Address (IPv6) support is not available. ℹ

Type	Score
Email	82% Sufficient



Internet Hygiene Tools

Cyber Health Check Report

viewqwest.com

08 AUGUST 2024 18:35:50

Email Connection is sufficiently secured. ✓

Email Domain has sufficient phishing attack prevention. ✓

Email Domain is sufficiently secured. ✓

Modern IP Address (IPv6) support is available but unreachable. ℹ

Type	Score
Email	100% Good Health

Getting a perfect score shows that effort was put in to really fine tune the configuration of their email infrastructure to ensure all recommended best practices are implemented, include removing older compromised ciphers from their cipher pool.

Email servers are often the first point of entry for attackers. Phishing, spear-phishing, and other social engineering attacks exploit human vulnerabilities, bypassing technical defences. Therefore, I think as the organization that connects the public to the internet, there should be some effort put in to demonstrate to the consumer that they are taking cybersecurity seriously.

Taking Cybersecurity Seriously: A Call to Action

The StormBamboo incidents have highlighted that while some ISPs take cybersecurity seriously, there is still a considerable gap in the industry. Cybersecurity is not a one-time effort but an ongoing commitment. ISPs must adopt a proactive stance, regularly updating their security protocols and remaining vigilant against emerging threats.

Collaboration is also essential. ISPs should work closely with governments, cybersecurity firms, and other stakeholders to share information about threats and best practices. Public-private partnerships can enhance the overall security landscape, ensuring that ISPs are better equipped to defend against sophisticated attacks.

The Way Forward

As our reliance on digital networks continues to grow, the importance of securing our telecommunications infrastructure cannot be overstated. ISPs play a pivotal role in this ecosystem, and their commitment to cybersecurity is crucial.

In conclusion, the current state of ISP security (at least in Singapore) is a mixed bag. While some ISPs are making strides in securing their systems, the simple test with free tools reveal that others need to significantly step up their efforts. By focusing on implementing stringent BGP protections security, having a robust and securely configured email server, and fostering a culture of continuous improvement and collaboration, ISPs can better protect our digital lifelines. The time for complacency is over; proactive and comprehensive cybersecurity measures are imperative to safeguarding our interconnected world.

IAN LOE
IL
ARCHITECTURE · SECURITY · GOVERNANCE

DN: email=ian@ianloe.net
Date: 2024.08.15 10:13:21
+08'00'