Six years on from the official launch, just how secure is IPv6?
07/06/18

The world launch of IPv6 happened back in June 2012, and World IPv6 Day is on Friday 8 June. But just how secure is IPv6 some six years after that fanfare deployment?



network-traffic-ddos

The world launch of IPv6 happened back in June 2012, and World IPv6 Day is on Friday 8 June. But just how secure is IPv6 some six years after that fanfare deployment?

Development of IPv6 first started in the early 1990's when it was realised that the physical limitation of 4.3 billion unique IP addresses in the IPv4 protocol wasn't going to be enough to support Internet growth. And that was before the Internet of Things had even been thought about. IPv6 addresses the problem, if you'll excuse the pun, by providing 340 trillion, trillion, trillion unique addresses.

The newly published Internet Society State of IPv6 Deployment report for 2018 points to the success of IPv6 deployment. More than 25 percent of all Internet-connected networks advertise IPv6 connectivity, for example. If you combine the top 15 ISPs across the world, nearly half a billion people are using IPv6 already. Six years ago, less than one in every 100 connections to Google were using IPv6, today that is one in four. The report does admit, however, that "enterprise operations tend to be the elephant in the room when it comes to IPv6 deployment."

Internet Society Chief Internet Technology Officer, Olaf Kolkman says that IPv6 is "increasingly seen as a competitive advantage, a market differentiator and an essential tool for forward-looking Internet applications and service providers of all kinds." But the question for enterprise security teams remains, just how secure is IPv6?

"In the sense of the protocol, IPv4 and IPv6 are roughly similar in terms of security" says Dr. Stephen Strowes, Senior Researcher at the RIPE NCC in conversation with SC Media UK. "The difference comes from other layers" Dr Strowes adds "it's the tools used and training that network operators get that makes all the difference."

Cricket Liu, VP of Infrastructure at Infoblox, agrees. "IPv6 isn't inherently more or less secure than IPv4." However, speaking to SC Media Liu suggests that the major security implications of moving to IPv6 are that "network administrators have substantially less experience managing the protocol than they do with IPv4." Throw in that network equipment vendors, security vendors,and so on often don't support IPv6 as completely as they do IPv4 and "the chance of making configuration mistakes increases, as does the likelihood that some whizzy feature of your firewall, IDS or IPS that works great over IPv4 isn't supported at all over IPv6."

Wicus Ross, Security Researcher with SecureData, admits that "It's possible that there are more misconfigurations present on IPv6 due to the relative lesser usages compared to IPv4." However, to balance that there's the small matter of the huge size of the IPv6 address space where a single IPv6 subnet can contain the entire IPv4 address space. "As such" Ross continues "IP Address enumeration or scanning through the IPv6 address space sequentially using current capability is not feasible." This should be good news, as it makes it less efficient for attackers to hunt for vulnerable devices.

Earlier this year, DDoS protection experts Neustar experienced and successfully mitigated its first recorded native IPv6 DDoS attack. This targeted the authoritative DNS service on the Neustar network, and originated from around 1,900 native IPv6 hosts on more than 650 different networks. "IPv6 attacks present a particular set of challenges that, at this moment, cannot easily be rectified" Barrett Lyon, General Manager of DDoS at Neustar, told SC media UK. "For example, the massive number of addresses available to an attacker allows them to exhaust the memory of modern day security appliances" Lyon continues "as a result, the potential volume of an IPv6 attack has the opportunity to create a mess."

Lyon concludes that, going forward "a great deal of work will need to be undertaken by security professionals to ensure that IPv6 is protected and that we are ahead of the curve when it comes to predicting a hacker's next move."