IPv6, "New" Kid on the Block

The Internet has relied on IPv4 addresses since its earliest days, but the exhaustion of these addresses has long been predicted. That day came in 2017.

Today, IPv6 finally has the public's attention. The shift to IPv6 is now a necessary one, but it also presents new opportunities for cyber criminals.

Every Internet-enabled device has a unique numerical address called an "IP address." The Internet Protocol relies on these unique addresses to route traffic to the correct destination. IPv6 is the sixth revision to the Internet Protocol. It works like IPv4 by assigning the unique, numerical IP addresses for devices to communicate online.

<table>
<thead>
<tr>
<th>IPv6</th>
<th>IPv4</th>
</tr>
</thead>
<tbody>
<tr>
<td>128 bits</td>
<td>32 bits</td>
</tr>
<tr>
<td>3.4 x 10^38 IP addresses</td>
<td>4 billion IP addresses</td>
</tr>
</tbody>
</table>

IPv6 enables 7.9 x 10^28 more IP address than IPv4 which expands the attack surface dramatically.

The first IPv6 DDoS attack of significance was recorded in March 2018. The attack occurred on more than 650 networks and targeted the DNS service Neustar®. It won't be the last. Over 1,900 IPv6 addresses attacked a DNS server.

IPv6 introduces a frustrating reality in which bad actors have a much larger playground for malicious activity. However, that doesn't make them untraceable. Using DNS, we can still unveil the many tracks left behind and it's as easy as:

2. Investigate the same domains seen in IPv4 and IPv6.
3. Investigate the domains seen separately from IPv4 and IPv6 addresses.

NEW SECURITY RISKS

HOW TO AVOID THE SECURITY RISKS OF IPV6

USING DNS FOR IPV6 RELATED INVESTIGATIONS

While the Internet community has dedicated efforts to plugging holes in IPv4 DNS open resolvers, the IPv6 space is new and far larger. Additionally, DNS configuration for IPv6 differs greatly from IPv4, which may create plenty more opportunities for DNS-based amplification attacks.

Amplification Attacks

Most software applications support both IPv4 and IPv6, or "dual stacking." However, developers primarily focus on resolving vulnerabilities on the IPv4 stack of the software and often fail to patch the IPv6 code. Attackers, knowing the IPv6 path is likely wide open, therefore see patch announcements as opportunities.

Dual Stacking

IPv4 addresses are limited and static, which means bad actors can easily be blacklisted by their IP address. In the IPv6 world, the host identifier randomly generates every 12-24 hours, constantly updating the unique address of connected devices and subsequently making it difficult to identify and block malicious devices.

Host Identifier

Reassess IP Address Configuration and Tracking

IPv6 fundamentally changes IP address assignment and management and organizations must reassess their IP assignment and tracking methods. IPv6 address length will make manual management impossible.

Understand Network Infrastructure

IPv6 should not begin without full awareness of the current IPv4 network. IT must have in-depth understanding of its network infrastructure and how traffic is routed.

Review DNS Architecture

IT organizations will need to run a DNS infrastructure capable of supporting both IPv4 and IPv6. IPv6 requires configuring domain support, server addresses, and more.

Track Network Performance

IPv6 introduces nuances that may affect network performance. For example, IPv6 header size is double IPv4's. Applications reliant on smaller packet sizes will face significant impact.

Contact Farsight Security today and learn how DNSDB can help.

farsightsecurity.com  +1-650-489-7919

Passive DNS can be used to correlate IPv4 and IPv6 related information.

Farsight collects Passive DNS data from its global sensor array and then filters and verifies the DNS transactions before inserting them into the DNSDB along with ICANN-sponsored zone file access download data. The result is the highest-quality and most comprehensive Passive DNS data service of its kind. DNSDB is engineered and operated by leading Farsight DNS experts.

Farsight offers the world's largest passive DNS intelligence solution.