



www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1 800.652.4020

Fidelis Threat Advisory #1002

IPv6

September 13, 2011

Document Status: FINAL
Last Revised: 2011-09-27

Executive Summary

IPv6 poses no inherent security risk, but on networks without explicit IPv6 controls it can be used to facilitate or conceal attacks and thus exacerbate other risks. IPv6 traffic and its associated tunneling protocols such as Teredo or ISATAP can be used to bypass firewalls and IPS devices that are not IPv6-aware or are not configured to inspect such traffic. This bypass can allow Botnet Command and Control or peer-to-peer (P2P) traffic to proliferate undetected.

Threat Overview

IPv6 traffic, either used natively or tunneled through IPv4, can be used to bypass traditional firewall and IPS defenses if those devices are not IPv6-aware or they are not properly configured to inspect such traffic. All modern operating systems come configured with IPv6 enabled by default. Thus if an organization has modern operating systems and no security policy around IPv6 traffic, or no security devices capable of enforcing said security policy, then the organization's workstations are susceptible to attacks carried out over IPv6.

Risk Assessment

IPv6 poses no inherent security risk, but it can be used to facilitate attacks and thus exacerbate other risks. Botnet Command and Control traffic can use IPv6 tunneled over IPv4, or natively, to bypass outbound firewall rules that do not block tunneling or are otherwise IPv6 unaware. Bittorrent clients and other P2P software can use IPv6 to bypass protocol filtering or network rate limiting. Because IPv6 uses a DHCP-style autoconfiguration by default, workstations are continually listening for routers sending autoconfiguration messages. If an organization does not explicitly control and manage its IPv6 implementation, an attacker can establish a rogue router and thus fool workstations into accepting the rogue autoconfiguration information allowing for easy man-in-the-middle (MITM) attacks and DNS spoofing.

Users are granted permission to copy and/or distribute this document in its original electronic form and print copies for personal use. This document cannot be modified or converted to any other electronic or machine-readable form in whole or in part without prior written approval of Fidelis Security Systems, Inc.

While we have done our best to ensure that the material found in this document is accurate, Fidelis Security Systems, Inc. makes no guarantee that the information contained herein is error free.



www.fidelissecurity.com

www.threatgeek.com

 @FidSecSys

+1 800.652.4020

Indicators & Mitigation Strategies

IPv6 traffic and associated tunneling protocols like Teredo and 6to4 are easy to detect. What is frequently more difficult for an organization is to determine which protocols, if any, should be in use and where. The greatest risk faces organizations that believe they don't have IPv6 enabled at all, or only on certain network segments under certain conditions, when in reality it pervades their network in ways they weren't aware of and have no visibility and control over. We recommend increased visibility into IPv6 network activity, and blocking of IPv6 traffic or traffic using unauthorized tunneling protocols, either network-wide or selectively as dictated by an organization's IPv6 security policy.

The Fidelis Take

Fidelis XPS sensors are fully IPv6-aware and can be used to block entirely, or detect the presence of, IPv6 traffic. An update to Fidelis XPS scheduled for Q4 2011 will bring detection improvements in the form of detection for Teredo, GRE, 6over4 and 6to4 tunneling.

Further Reading

- NetworkWorld, "Scariest IPv6 Attack Scenarios", Carolyn Marsan, 8/25/11. <http://goo.gl/tvAj5>
- NetworkWorld, "Invisible IPv6 traffic poses serious network threat", Carolyn Marsan, 7/13/09. <http://goo.gl/6cY6a>
- Threat Geek, "But IPv6 Solves Everything, Right?" Will Irace, 9/27/2011. <http://goo.gl/Sev2s>