Malware Tunneling in IPv6

US-CERT

The Internet Protocol, version 6 (IPv6)[1] was designed to alleviate the address space limitations of IPv4 and provide additional security and routing capabilities. The protocol itself, however, can be misused to deliver malware in a way that eludes detection by firewalls or intrusion detection systems (IDS) not configured to recognize IPv6 traffic. This problem can be amplified in cases where malware is used to reconfigure vulnerable hosts to allow IPv6 traffic.

Conditions and Technology

Misuse of IPv6 to deliver malware relies on several factors. These factors include

- malicious application of traffic "tunneling"
- incomplete or inconsistent support for IPv6
- the IPv6 auto-configuration capability
- malware designed to enable IPv6 support on susceptible hosts

Tunneling with IPv6

Tunneling is a method of internet data transmission in which the public internet is used to relay private network data.[2] This is achieved by encapsulating the private network data and protocol information within the public network packets. In doing so, the private network protocol information is handled normally by the public network.

This kind of data encapsulation, used in conjunction with encryption and authentication (as with a VPN), provides a legitimate benefit to those who need an efficient means to connect private networks. However, IPv6 can itself be used to encapsulate malware and distribute it by taking advantage of pre-existing network conditions and the auto-configuration feature of IPv6.

Incomplete and Inconsistent IPv6 Support Promotes Malware Tunneling Vulnerability

Most current operating systems now support IPv6 by default. Some filtering and monitoring devices only partially support IPv6. This limits their ability to filter or detect IPv6 traffic. Consequently, firewall and IDS equipment not configured to recognize IPv6 traffic can be bypassed.

The Role of IPv6 Auto-Configuration in Malware Tunneling

The auto-configuration feature of IPv6 makes malware tunneling possible. This feature permits IPv6-enabled devices to derive their own IP addresses from neighboring routers without administrator intervention. Further, the device may solicit and accept advertisements to route IPv6 traffic. No DHCP server is required for the device to assign itself an IP address, which is a characteristic of IPv4 deployments. Malicious external

[1] The Internet Protocol, version 6, is described in RFC 2460, http://www.ietf.org/rfc/rfc2460.txt.
[2] The specification for generic packet tunneling in IPv6 is described in RFC 2473, http://www.ietf.org/rfc/rfc2473.txt.

users or could send crafted IPv6 packets capable of passing undetected through perimeter security devices not configured to recognize IPv6 traffic, then exploit the auto-configuration capability of internal hosts supporting IPv6 to route the malicious packets.

Malware That Enables IPv6 on Compromised Hosts

There has been a recent increase of malicious code that enables IPv6 on a compromised host, creating a potentially undetected channel for an attacker to exploit. Nefarious web sites offer tools that can be used to exploit IPv6 for malicious purposes.[3] These tools include

- relay6
- 6tunnel
- nt6tunnel
- asybo

These tools can be used for legitimate purposes to facilitate communication between IPv6 and IPv4 devices and applications. However, they can be misused for malware tunneling and routing.

Managing Tunneling Attacks

Sean Convery and Darrin Miller provide an overview of the various threats and mitigations strategies for both IPv4 and IPv6 in their white paper "IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)."[4] Their specific advice on tunneling attacks includes the following practices:

- Use dual stack as your preferred IPv6 migration choice
- Use static tunneling rather than dynamic tunneling
- Implement outbound filtering on firewall devices to allow only authorized tunneling endpoints

Other IPv6 Security Risks

As with any software, feature, or protocol, IPv6 may introduce design or implementation vulnerabilities. IPv6 was designed with security in mind, but its implementation is currently less mature than IPv4. Consequently, in addition to malware tunneling, reconnaissance activity inbound (such as port scanning) or communication traffic outbound (such as botnet activity) could be facilitated in a network that does not control its IPv6 implementation.

Minimizing IPv6 Security Risks

You can determine if the operating systems within your environment support IPv6 the checking the following web site, which identifies operating systems supporting IPv6:

---

[3] Warfield, Michael H. 2003. Internet Security Systems, Inc. "Security Implications of IPv6." http://documents.iss.net/whitepapers/IPv6.pdf.

[4] Convery, Sean and Darrin Miller. Cisco Systems, Critical Infrastructure Group "IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)." http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf.

http://www.ipv6.org/impl/index.html

The best way to eliminate security risks associated with IPv6 is to manage IPv6 within your network. Convery and Miller suggest the following practices in their paper on IPv6 and IPv4 threats:

- Filter internal-use IPv6 addresses at organization border routers
- Use standard, but non-obvious static addresses for critical systems
- Filter unneeded services at the firewall
- Selectively filter ICMP
- Maintain host and application security

The Convery and Miller paper provides additional guidance for IPv6 implementations, summarized below.

Additional Security Recommendations for Firewalls

- Determine what extension headers will be allowed through the access control device
- Determine which ICMPv6 messages are required

Managing Fragmentation Attacks

- Deny IPv6 fragments destined to an internetworking device when possible
- Ensure adequate IPv6 fragmentation filtering capabilities
- Drop all fragments with less than 1280 octets (except the last one)

Managing Spoofing Attacks

- Implement RFC 2827-like filtering and encourage your ISP to do the same
- Document procedures for last-hop traceback
- Use cryptographic protections for critical systems

Managing Router Attacks

- Use traditional authentication mechanisms on BGP and IS-IS
- Use IPsec to secure protocols such as OSPFv3 and RIPng

Managing Worm and Virus Attacks

- Implement IPv4 best practices to include timely patching, host antivirus, and early detection followed by perimeter blocking

Additional Resources

The following resources present information about effective IPv6 management.

- "IPv6: The Next Generation Internet!" http://www.ipv6.org/
- Windows 95/98/NT http://www.trumpet.com.au/ipv6.htm
- Windows 2000 http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp
- Windows XP http://www.microsoft.com/technet/prodtechnol/winxppro/plan/faqipv6.mspx
- Windows Server 2003 http://www.microsoft.com/windowsserver2003/technologies/ipv6/default.mspx
- Cisco http://www.cisco.com/warp/public/732/Tech/ipv6/
- Quick-start IPv6 "HOWTOs" http://www.ipv6.org/howtos.html
- Convery, Sean and Miller, Darrin, "IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)" http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf
- US-CERT Vulnerability Notes VU#658859 "Juniper JUNOS Packet Forwarding Engine (PFE) IPv6 memory leak" http://www.kb.cert.org/vuls/id/658859
- US-CERT Vulnerability Note VU#472582 "Cisco IOS IPv6 denial-of-service vulnerability" http://www.kb.cert.org/vuls/id/472582

Last updated May 26, 2005