

IPv6 Cyber Security Briefing May 27, 2010

Ron Hulen VP and CTO Cyber Security Solutions Command Information, Inc.

Command Information © 2010. All rights reserved. 2610:f8:ffff:2010:05:27:85:1



Attack Surfaces Protocol Translator IPv4 IPv6 Native Native **Dual-Stack Dual-Stack + Tunnels** IPv4 + IPv6 + **Tunnels Tunnels Tunnels** Encapsulation and/or Encryption

Command Information © 2010. All rights reserved.



Known IPv6 Vulnerabilities





The IPv6 Header is completely different



IPv6 Extension Headers can be Indefinite



How many combinations are there?

Command Information © 2010. All rights reserved.



Command Information © 2010. All rights reserved.



Command Information © 2010. All rights reserved.



IPv4 Security Must Account For IPv6!





IPv6 Tunnels are a Transition Mechanism

- Protocol 41 and 47 Tunnels
 - > 6in4
 - > 6to4
 - > 6RD
 - > IPv6 in GRE
- IPSec Tunnels
 - > AH
 - ESP Null

- Protocol 41 and 47 > UDP Based Tunnels
 - Teredo (Port 3544)
 - > AYIYA (Port 5072)
 - Heartbeat (Port 3740)
 - > TIC (Port 3874)
 - > TSP (Port 3653)



Tunneled Packet Processing is *Complex*

	IPv6	-in-	v4	-in-IPv4	4/IPv4/GRE
	V TC Flow Label Payload Length NH HLim	V L ToS Identifier	Total Length Fig Offset	V L To Identifier	S Total Length Fig Offset
	Src Address	Src Address Dest Address		Src Address Dest Address	
	Payload	V TC Payload Length	+ Padding) Flow Label NH HLim ddress	(Optic V H To: Identifier TTL	ons + Padding) S Total Length Flg Offset Dt Hdr Checksum
	Dest Address		Address	Src Address Dest Address (Options + Padding)	
		Pay	load	C Res0 Opt Checksur V TC Payload Leng	V Protocol Type m Res1 Flow Label th NH
				S	rc Address
low mang here?	y encapsulatic	ons are		Pa	yload



Tunnels Need to be Protected

ACL's can protect against Protocol 41, 47, IPSec and port specific UDP traffic

What if you don't know the Port?

Miredo: Teredo configured to run on any port GoGoNet6: TSP can listen on any UDP port (ie 53, 80, 443, etc)





uTorrent – Teredo and IPv6-Capable

- Uses ephemeral port for connections
- User may randomly choose port
- Port may be randomly chosen on restart
- IPv6 support "on by default"

Connection		0
Listening Port Port used for incoming connections: Enable UPnP port mapping		33444 Random port
General		0
Language Language:	(System Default)	▼ More
 Windows Integrat 	ion	
Associate with .torrent files		Check association on startup
Associate with .btsearch files		Start µTorrent on system startup
Associate with magnet URIs		Install IPv6/Teredo



uTorrent – Teredo Peers

- uTorrent runs well over Teredo
- BitTorrent community is discovering IPv6

μTorrent 2.0.1		-			
File Options Hel	p				
🖪 🖓 🛃	🗡 🗙 🝉 🕕 🔲 🔲 🛧 🔶 🌼				
📑 All (1)	Name # Siz	ze Done Status			
👆 Downloading	🗣 ubuntu-9.10-alternate-i386.iso 1 689 M	1B 0.5% Downloading			
 Completed (0) 	······				
将 Active (1)					
👫 Inactive (0)					
No Label (1)					
	< III				
🔝 All Feeds	🕕 General 🚑 Trackers 🌋 Peers 🕞 Piece	es 🔋 Files 🛃 Speed 🕖			
	IP	Client			
	2001:0:4137:9e74:2040:1278:b19a:7492	µTorrent 2.0			
	2001:0:4137:9e74:24d0:2ba5:9d12:3a6 [uTP]	µTorrent 2.0.1			
	2001:0:4137:9e74:3031:24ae:b85c:51b8 [uTP] µTorrent 2.0				
	2001:0:4137:9e76:9c:27a9:bb3e:f88c [uTP] μTorrent 2				
	2001:0:4137:9e76:845:246b:9cf2:eb1d [uTP] μTorrent 2.0				
	2001:0:4137:9e76:18be:39c6:9ce2:8dd6 [uTP] μTorrent 2.0 2001:0:5ef5:73b8:2c9b:198c:a7be:a8af [uTP] μTorrent 2.0.1				
	2001:0:5ef5:73ba:ca1:165a:26f6:a04b [uTP] µTorrent 2.0				
	2001:0:5ef5:73bc:4df:cf65:b29a:129c [uTP] µTorrent 2.0				
	2001:0:5ef5:73bc:2871:27a:a6b4:97cd [uTP]	µTorrent 2.0.1			
	2001:0:5ef5:73bc:384d:352c:b1e2:ef9f [uTP] μTorrent 2.0				
	2002:5f8d:e386::5f8d:e386 [uTP] µTorrent 2.0				
	24.210.207.207	Transmission 1.75			
	24.230.140.251	µTorrent 1.8.3			



IPv4 "AAAA" DNS Queries Broadcast IPv6

- Microsoft Dual Stack enabled on ALL Vista / Windows 7 systems
- > AAAA Queries present on every network we monitored.
- Considered 'harmless' by Security and Network Personal
- > Must be disabled by DoD MO2 guidelines





IPv4 "AAAA" DNS- loaded gun

- Remote Hacker sees an organization sending 100,000+ AAAA queries a day
- > Hacker Floods an organization's mail servers with SPAM
 - It only takes one user with elevated privileges to open one SPAM message to execute the encapsulated malware
 - > Consider <u>MS 10-009</u>
- Malware establishes an IPv6 in UDP tunnel through an organization's firewall to Remote Hacker on UDP port 53
 - > Such as Miredo or GoGoNet6
- Remote Hacker exfiltrates sensitive data from an organization's enterprise network





ICMPv6 is Required for IPv6





Malevolent RAs: the threat inside

- IPv6-enabled workstations (untouched Vista, 7, Linux, Mac, etc) always listen for Router Advertisements
- > User A downloads that pesky malware
 - > Sets up tunnel like the non-standard UDP port example (or port 53)
 - > Installs basic router advertisement daemon & IPv6 forwarding
- It sends RAs out to IPv6-enabled machines with User A as it's default gateway
- Now there are active IPv6 malware on an enterprise that can't be detected





Summary

- IPv6 Threats are Real both native and tunneled
- Hackers are using IPv6 to tunnel into networks undetected by current security tools
- Companies must develop a security policy to address IPv6.





IPv6 Cyber Security War Plan

- > Knowledge
- > Analysis
- > Planning
- Securing
- Monitoring
- > Lifecycle Management





Thank You

Ron Hulen Command Information <u>ron.hulen@commandinformation.com</u> 703-234-9363