IPv6 Obfuscation and Attribution: Some Quick Framing Slides Emerging Trends, Challenges and Strategies Panel

Joe St Sauver, Ph.D.
joe@oregon.uoregon.edu or joe@internet2.edu
Nationwide Security Programs Manager, Internet2

NCFTA Canada, Montreal, Quebec
3:30-5:00PM November 17th, 2010
http://pages.uoregon.edu/joe/ipv6-for-panel/

Disclaimer: all opinions expressed are solely those of the author and should not be construed as necessarily representing the opinion of any other entity.

We Are Entering the IPv6 Era

- IPv4 exhaustion will occur in less than a year
- IPv6 adoption and deployment is underway (albeit with a few obstacles that people are still working through)
- The natural question is:

  "What does this mean for those who investigate and prosecute electronic crimes?"

- We'll do a "deeper dive" tomorrow, but for today's panel, let's just have a few framing slides…

Attribution Is A Key Element of Successfully Investigating and Prosecuting Electronic Crimes

- Traditionally this has meant:
  a) identifying the IPv4 address associated with a criminal incident
  b) mapping that address to an ISP
  c) serving legal paperwork on the ISP to obtain the customer's identity and billing information, connection history, account contents, netflow data, or whatever other information may be of interest
  d) interviewing the customer, or serving legal paperwork on the customer allowing law enforcement to search or seize the contents of the customer's home or office computer
  e) iterating/replicating as may be required (e.g., in the case of multiple IP addresses, proxies, etc.)

Cyber Criminals, Seeking To Avoid Investigation and Prosecution, Often Attempt to Obfuscate Their Network Connections (and Thus Their Identities)

- For example, cyber criminals may:

  -- bounce connections through anonymizing networks such as Tor, private VPN networks, bot networks, etc.

  -- search for and exploit open (or weakly protected) wireless access points

  -- more sophisticated cyber criminals may announce address space which they've not been assigned, etc.

- But it is not my desire to provide an inspirational cook book for the bad guys this morning. :-;

IPv6 And Abuse Today: Good News/Bad News

- Currently, even though we're only ten months away from exhausting the supply of IPv4 addresses, we're not seeing a tremendous amount of legitimate use of IPv6. That's the bad news.

- On the other hand, we're also not seeing a lot of abusive/criminal use of IPv6, either. That's the good news.

- If cyber criminals do turn toward IPv6, what might we see?

IPv6 Connectivity: Potentially More Complex

- A plethora of different methods may be used by legitimate or abusive customers to obtain IPv6 connectivity.
- For example, in addition to some sort of IPv4 connectivity, customers may also have:
  -- native IPv6 connectivity
  -- manually configured IPv6 tunnels (from a paid or free tunnel broker)
  -- automatically configured IPv6 connectivity via 6to4, Teredo, ISATAP or other mechanisms)
- It will be routine for you to see multiple IPv6 addresses associated with a single host
- Some IPv6 addresses, e.g., IPv6 privacy format addresses, should be expected to change frequently

Identities Associated with IPv6 Addresses

- Assignment of IPv4 addresses to customers is normally well documented (e.g., via the ISP's DHCP logs, customer signups, billing records, etc.)
- Some IPv6 users may be using free transition mechanisms provided anonymously by third parties (much like "open relays" or "open proxies" in the bad old days)
- Other users may have native IPv6 addresses, however, those addresses may be assigned via SLAAC, "stateless auto configuration." SLAAC intentionally does not maintain records of who was using what IPv6 address when.
- IPv6 customers may also use so-called "privacy format" addresses, addresses which intentionally change on a periodic basis. (Note: IPv6 privacy format addresses are enabled by default in Windows)

IPv6 Network Instrumentation

- Many ISPs routinely instrument their network, monitoring the traffic that's flowing over it. Network monitoring is critical for normal network operational purposes such as billing and traffic engineering, but also for detecting and resolving cyber abuse.
- The foundation for much such monitoring is Netflow or Sflow, creating one such records for each network flow.
- Unfortunately, collecting Netflow information in an IPv6 environment requires use of Netflow v9. Most ISPs remain "stuck" on Netflow v5 (which has no ability to handle IPv6 flows)
- Support for IPv6 may also be uneven in other ISP network management staples such as SNMP – some device MIBs may not have IPv6 constructs. ISPs also need to know to supplement arpwatch with ndpmon, etc.

Given That There's Little Native IPv6…

- If you do run into a (rare) native IPv6 address that is being abused, you can generally use the same tools you normally would (e.g., whois plus legal paperwork) to begin working your way to the customer's details. (Yes, whois works for IPv6 just as it does for IPv4)
- But if we (correctly) assume that there's currently rather little native IPv6 connectivity, the IPv6 attribution problem devolves to one of mapping an IPv6 address to the underlying associated IPv4 address that's providing the abuser's primary connectivity, and then proceeding as normal.
- If you have the IPv6 address that they were using, and they were using an automated tunneling mechanism such as 6to4 or Teredo, the IPv6 addresses it uses will often be built around the associated underlying IPv4 address…

Some Auto Tunneling IPv6 Embedded IPv4 Addrs

- 6to4 (2002:: addresses)

  Of the first 64 bits:
  -- first 16 bits: always 2002:,
  -- *the next 32 bits are the* ***IPv4 address***

- Teredo (2001:0000::/32 addresses)

  Bits 96 to 127 contain the IPv4 address, with all the bits inverted.

Conclusion

- IPv6 is upon us, but so far we're only seeing light drizzle, not a torrential deluge.

- The bad guys don't want to be found, and will try to hide. IPv6 may help them, but not as much as they might hope it will.

- Most of the techniques you currently use will continue to work in IPv6 space, albeit with some specific new tricks your technical folks may need to learn.

- We'll talk far more about IPv6 tomorrow, but now at least you have some beginning thoughts for our panel today.