IPv6 Security Best Practices and the Future of Cyber Defence

David Kennedy – Arkenox
david@arkenox.com

Arkenox
IPv6 Security Solutions

UK IPv6 Council Annual Meeting
London 19th November 2024

Motivation

Security is often seen as the fun police – absolutely true!

- Usually pushing back on advancements and technology adoption, including IPv6.
- Very common to see advice on LinkedIn or Reddit to "Disable IPv6" - not even an option.

Research has shown that when it comes to defending an IPv6 network:

- 14x less likely to receive email spam over IPv6 compared to IPv4.[1]
- IPv6 based filters 204% more likely to stop malicious traffic when compared to IPv4.[2]

Common security issues in IPv6 deployments are well documented

- Scanning strategies in IPv6 constantly evolving.
- Vast majority of issues we have seen are because we do not understand our IPv6 network architecture and use cases as well as we do for IPv4.

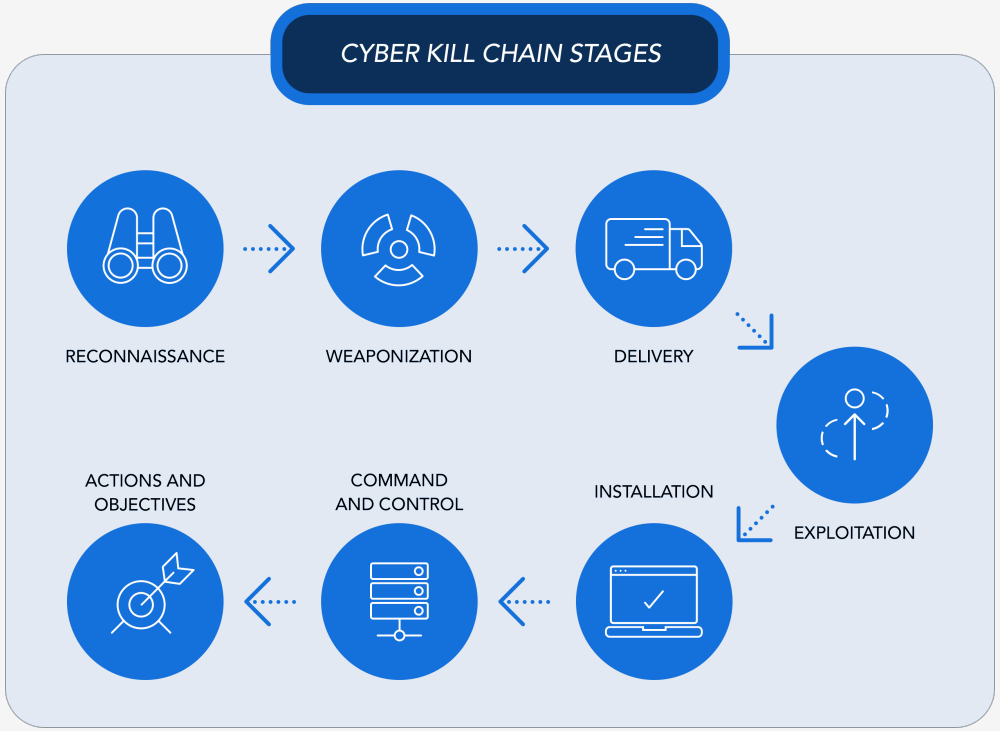
1– Not that simple: Email delivery in the 21st century (2023), 2 - Towards A User-Level Understanding of IPv6 Behavior (2020)

You Can’t Protect What You Don’t Know

Every attack starts with understanding the target – reconnaissance

- Aim is to understand the target better than target does - find oversight or weaknesses.

If we can build a network that is easy to understand then we can implement features that limit the ability to perform reconnaissance, stopping attacks from progressing.



Reconnaissance in IPv4

For public IPv4 addresses – strategy is brute force. Very easy.

- We all know about the risks of exposing services in IPv4 and *should* account for that with ACL's.
- Even using obscure ports, your service will get found.

For RFC1918 addresses – bit trickier.

- NAT provides obscurity not security.
- Port forwarding, DNS enumeration.
- Tricking devices behind NAT to connect to your services. Phishing, Supply Chains.

Reconnaissance in IPv6

Common myth that IPv6 is not scanned – due to size of space.

- Wrong! Active scanning of global unicast addresses is occurring and happening against your networks now.
- But scanning strategy is different to IPv4, not feasibly possible to brute force entire IPv6.
- Means that some organisations do not implement correct network filters or ACL's.

IPv6 reconnaissance aims to find "IPv4 addressing strategies or thinking applied in IPv6"

- Architectures with common and predictable patterns
- Combined with limited/no filtering and access control
- Aided by the ability for an attacker to rotate their source IP

Reconnaissance – Network Prefix

Aim - Reduce the scope of reconnaissance by identifying active network prefixes.

- Fixed part of your allocation.
- Detect via DNS, rDNS, routing tables, common allocation patterns.

Identifying the prefix relatively easy, but still far too massive to perform IPv4 reconnaissance strategies against.

Reconnaissance – Interface ID (IID)

Should be very difficult if we all followed RFC7217 or RFC8981. But there are still legacy global addressing strategies in use such as:

- EUI-64 - OUI = 24 bits, fffe = 16 bits

Or addressing strategies that use easy to remember addresses, i.e.

- Low Byte – 2001:db8::1, 2001:db8::f
- Service Exposing Addresses - 2001:db8:1::22
- Words - 2001:db8:bad::beef
- Aliasing – Device responds to entire subnet or multiple addresses.

Rule of thumb – If an address is easy to remember, then it is easy to find. Not a bad thing if like in IPv4, we implement filtering + ACL's.

What is the Underlying Problem?

We don’t fully understand our IPv6 networks:

- Might have been set up a long time ago.
- Expanded without a consistent plan.
- Security as an after thought – or used to “safety net” of NAT.
- Which means attackers can find areas of oversight.

But IPv6 allows us to create a network with security at the foundation, with a structure that is easy to expand and defend.

How? Going to take inspiration from Forts for this.

Your IPv6 Network is a Fort - Perimeter

Perimeter that is more clearly defined than IPv4.

- Prefix(es) allocation from RIR, LIR.
- Continuous address space, unlike with IPv4.
- Could also ask for reservation of next adjacent address space, if possible.

We can implement rules on the network edge:

- Silently drop unsolicited inbound traffic.
- Enforce IPv6 RFCs, best practices, rate limits.
- Hierarchical nature of IPv6 means that these rules are enforced on rest of the network

Network Infrastructure

Hierarchical nature of IPv6, segment network at logical points and implement additional controls at each level:

- Based on specific use cases of each network segment.
- Sensitivity of that network segment – Guest WiFi.
- Implement monitoring for each segment – alerting based on average inbound/outbound

Network Based Traps:

- Research has shown that leaving the first and last 10% of your allocation empty reduces reconnaissance by XYZ% <to add>.
- You can go further with this, if you know part of your network is purposefully empty. You can build filters based off any activity in those areas.
- Block strategy – start with /64, then move to /54 and finally /48 should traffic continue.

Endpoints

Addressing strategy where possible:

- /64 IPv6 subnet prefix per endpoint
- Temporary addresses – blocking unsolicited inbound to temporary addresses.

Defence in Depth:

- EDR and IDS/IPS
- But make sure that these properly support IPv6 including different IPv6 address types and lifetimes.

Built in local Firewalls:

- Often either disabled or enabled with default configurations. Especially important if using static addresses with easy to remember addressing strategies.

Summary

Spend time planning your IPv6 network, embedding security where possible from the start.

Using various features of IPv6 we can stop a lot of attacks right at the reconnaissance stage i.e. Hierarchy, Temporary Addresses

We need to change the narrative that IPv6 is a security burden to a security opportunity – we saw in August how quickly that narrative can run away and become detrimental to IPv6.

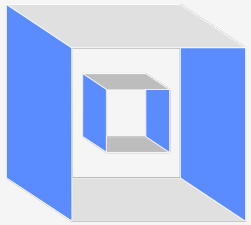
Thank You.

Any questions?

Follow our LinkedIn page for regular updates about IPv6

linkedin.com/company/arkenox

www.arkenox.com



Arkenox