To: Secretariat – Parliamentary Joint Committee on Intelligence and Security

Paul Wilkins
24 October 2024

Re: Cyber Security Package 2024

We're all going to be left with silly expressions on our faces, if a class of a popular IOT device is captured by a control and command network, this multitude goes rogue, DDOS's the Australian internet, and the necessary fix requires a security update hosted on a server that's beyond Australia's DDOSd flooded internet cables.

Sadly address of this issue lies beyond the remit of Dep't Home Affairs, where responsibility for the development of national telecommunications infrastructure properly, and legislatively, lies with the Department of Infrastructure, Transport, Regional Development, Communications and the Arts.

This disaster scenario, cannot be dismissed as crying Cassandra. It is only one instance of systemic security weaknesses in Australia's telecommunications infrastructure (such as ransomware) that can only be addressed by building out architectural security for Australia's telecommunications. This approach is developed in the attached discussion paper, "A National Telecommunications Security Posture".

Regards securing IOT devices, the following should all appear in any proposal that represents as fit to address the scale of the threat and the complexity of the problem of delivering internet connectivity on a utility device:

1 – IOT devices be designated as a "System of National Significance", under the definition of s52b of the Security of Critical Infrastructure Act 2018, for its potential adverse impacts on "other critical infrastructure assets", to whit, national internet carriage
2 - ETSI EN 303 645 mandatory compliance
3 – IOT vendors commit to delivery of free security updates for the working life of the product
4 - IOT devices be enabled by default for automatic security updates
5 – The security update server to be hosted within Australian borders
6 – The security update server would ideally be hosted on a central server, managed by Dep't Communications, on a write once only, crypto hashed, file system
7 – Drivers and low level services for IOT devices to be written in Rust, or to be of demonstrated equivalence for strong memory protections
8 – Box and device sticker labelling for IOT devices whose operating system is immutable
9 – IOT devices to carry TPM for secure boot verification of operating system binaries
10 – IOT devices mandatory support for 802.1x(wired)/802.11i(wireless)
11 – IOT 802.1x/802.11i network access predicated on device's successful secure boot
12 – Printers should meet the definition of an IOT device
13 – Mandatory for service provider CPE routers to carry a separate VLAN for IOT devices, and a default TCP firewalling whitelist. Consequently, IOT devices by default only access their service provider, but not the wider internet, and not the customer's local network. Extra points for carriers whose CPE device hosts a Rust derived HTTPS proxy.
14 – Someone might like to have a quiet word to Intel and see if they can't persuade them to enable their management engine to compute binary checksums. Given the foreseeable injury consequent to the absence of this facility, and Intel's monopoly position to impose industry standards, this obvious security inadequacy in all likelihood meets the legal standard for a successful class action.

Apart from providing the necessary (and consistent with user expectations) belts and braces security for utility devices, the above ensures that should the device be hacked, it goes off the air. Realistically, you can’t build a security architecture for IOT predicated on passwords, managing device patching, or monitoring for security alarms.

Yours Sincerely

Paul Wilkins