MMC RESEARCH – SUBMISSION – AUSTRALIA 2020 CYBERSECURITY STRATEGY

30 September 2019

Cyber Security Policy Division
Department of Home Affairs
4 National Circuit
Barton ACT 2600

I'm writing to submit a response to Australia's 2020 Cyber Security Strategy call for views.

The 2020 Cyber Security Strategy discussion paper is an interesting document that poses many thought-provoking questions, and the 24 September public forum at Melbourne JCSC was a productive session. In this submission I would like to raise a concern that is specifically related to question 1 of the discussion paper:

What is your view of the cyber threat environment? What threats should Government be focussing on?

Australia is a country that is highly exposed to cybersecurity deficiency. Digital transformation is a double-edged sword; productivity gains are won, but cybersecurity risks naturally arise.

For discussion sake we may say that risk is the intersection between threat and vulnerability. But in a space where there is an abundance of vulnerability, where would a motivated threat focus?

What STUXNET, NotPetya, and the watering hole attacks targeting the Chinese Uighur diaspora have in common is that there was at least a desire from the adversary to target their attack in a discriminate way. There is a lot to be discussed with respect to the efficacy of this targeting (indeed the fact that these attacks were detected at all to some extent indicates that the degree of targeting was either insufficient by design or unsuccessful in execution), but what's also important is the intent, and the strategy underlying the intent.

Targeted attacks have several advantages for the attackers, such as:

- *Increased time to detection*: by targeting specific users or specific infrastructure, anomalous behavior will potentially go undetected for longer, which allows a campaign to complete all stages of the killchain without disruption.
- *Reduction of political risk*: to illustrate this point, many cybercrime ransomware authors specifically design their payloads not to detonate within jurisdictions which may expose them to law enforcement.
- *Ease of compromise*: a component that is used by few may be more likely to have vulnerabilities that are easier to compromise.
- *Avoidance of blowback*: if I unleash self-propagating malware on my opponent that attacks a common vulnerability that I am also exposed to, how do I avoid that same malware coming back to hurt me?

These factors taken together create a strong argument for targeting a vulnerability that is unique to the target, which is why M.E.Doc was an attractive vector to target Ukraine's economy.

By targeting a software package designed specifically for the tax regime in Ukraine, the attacker arguably found a vulnerability unique to Ukraine. As we know the attack caused damage well beyond Ukraine's borders, but it served as a demonstration that nation-specific vulnerabilities can be discovered.

The question is, whose job is it to discover and mitigate Australia's M.E.Doc before Australia's adversaries exploit it?

The vast majority of Australian businesses and consumers are more likely to suffer from a vulnerability in Office 365 or Chrome, and this is an important point which the discussion paper captures in question 16 (*How can high-volume, low-sophistication malicious activity targeting Australia be reduced?*), but the point is that Australia is not alone in facing those global exposures. We have the weight of the global technology and information security ecosystem, with its sometimes messy but substantial web of incentives, to address such risks. There is always the potential for gaps but as the industry gets better at coordinated disclosure processes, and as more threat research resources come online globally, as a whole there is a capability to deal with these global risks. It is commendable that the Australian government wants to do more to address these risks, but if the Australia government does nothing, the Australian community will have the global ecosystem to fall back on to address these risks.

However, vulnerabilities that pose a risk only within Australia may simply be Australia's problem. These will be the most attractive vulnerabilities for Australia's most sophisticated and motivated adversaries, and therefore these should be an area of priority for the Australian government.

Thank you for considering my submission. Please do not hesitate to reach out if I can be of any assistance.

Yours faithfully,

Tirath Ramdas
Director, MMC Research Pty. Ltd.