GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

PO Box 12-209
Wellington 6144
P +64 4 472 6881
F +64 4 499 3701
www.gcsb.govt.nz

A13291786

18 November 2020

Carl Langan
fyi-request-13934-00523532@requests.fyi.org.nz

Dear Carl Langan

Official information request

I refer to your Official Information Act 1982 (OIA) request dated 8 October 2020 for information regarding cyber security services provided by the Government Communications Security Bureau (GCSB).

My responses to your questions can be found below.

Would the Malware Free Networks services have mitigated attacks such as the one on NZX?

The attack the NZX experienced in August 2020 was a Distributed Denial of Service (DDoS) attack. DDoS attacks seek to saturate a victim's network with significant volumes of internet traffic that block legitimate users from accessing websites.

The nature of this type of attack means that internet service and external security providers are best placed to provide and implement technical mitigations.

The GCSB's Malware Free Networks (MFN) capability is a cyber threat detection service. MFN is primarily focussed on the detection of malware. It would not have mitigated a DDoS attack, as that is not its specific purpose.

That said, the GCSB has a range of relevant expertise and has provided advice and guidance to a wide range of organisations to assist in ensuring their systems are resilient to malicious activity in general.

How many organisations currently receive the malware free networks service? How many organisations have been approached to receive it?

The GCSB offers the MFN capability to organisations of national significance across New Zealand. For security reasons, the GCSB does not disclose which organisations have been deemed to be nationally significant organisations (NSOs) as publishing information around the composition of NSOs may increase the targeting of malicious cyber actions towards them. NSOs include government departments, key economic generators, research institutions and operators of critical national infrastructure.

The GCSB's National Cyber Security Centre (NCSC) engages with NSOs to generate interest in the MFN capability.

I must withhold the exact number of organisations currently using MFN, or that have been approached to use MFN, under section 6(a) of the OIA, as the making available of the information would be likely to prejudice the security or defence of New Zealand.

What is the budget allocated for the malware free networks service?

Specific details about the GCSB's budget is sensitive and making this information available would be likely to prejudice the security or defence of New Zealand. Therefore I must refuse to provide the specific amount of funding allocated to developing the MFN capability under section 6(a) of the OIA.

However, I can say that Budget 2020 saw the intelligence agencies receive an extra $146m over the next four years, with just over $100m allocated to the GCSB. Around half of this extra funding is to deliver new capabilities for the GCSB.

This work will include putting extra resource into our cyber security resilience building activity and into upgrading our cyber defence capabilities.

Even with strong protections in place, it will not always be possible to fully mitigate large volume, highly targeted and sophisticated DDoS attacks. The nature of this type of attack means that internet service and external security providers are best placed to provide and implement technical mitigations.

The NCSC has published guidance for preventing and responding to Denial of Service attacks (https://www.ncsc.govt.nz/newsroom/general-security-advisory-ongoing-campaign-of-dos-attacks-affecting-new-zealand-entities/) and I encourage all organisations to follow the guidance.

Is the service available to all NZ organisations?

The MFN capability is only available to organisations which meet certain criteria as determined by the NCSC and the participating service providers. These criteria include the organisations level of technical capability to receive and act on the information contained in the feed.

NCSC has worked with a range of customers and network operators to identify how best to deliver the service, and to establish the technology platform that will enable the most effective cyber threat intelligence sharing and reporting. The GCSB's focus has been on promoting the service to selected NSOs. As the technology is developed further, the GCSB expects to increase the number of NSOs it can offer the MFN capability to. Other non-NSO organisations may be able to receive MFN services through their network operator.

Are ISPs compelled to provide the service to their customers?

The intention is for NSOs to be able to receive the MFN capability either directly from the NCSC, or via their network operator, depending on the NSO's own level of technological capability.

How many ISPs are participating in the service?

The NCSC is currently working with a number of ISPs and NSOs to deliver and scale the MFN capability. As the capability matures we will look to make MFN more widely available through other network operators and directly to NSOs that have the cyber security maturity and capability to ingest it.

At this point in time, we must refuse to provide the exact number of ISPs currently participating in the MFN service, as this information is confidential and would unreasonably the prejudice the commercial position of those ISPs (section 9(2)(b)(ii) of the OIA applies). The GCSB is willing to revisit this decision in the future, once there are no longer such commercial sensitivities in place.

How many cyber attacks has malware free networks blocked to date?

The GCSB has already seen the MFN capability detect malicious cyber activity targeting New Zealand's organisations. This will increase as the capability is released to more customers. However, I must refuse to provide the number of attacks detected to-date under section 6(a) of the OIA: the release of this information would be likely to prejudice the security or defence of New Zealand.

It may interest you to know that the GCSB has, for several years, calculated the harm avoided to organisations as a result of its existing CORTEX cyber security services. In the 2018/19 financial year, the detection and disruption of malicious cyber activity through CORTEX capabilities prevented $27.7 million in harm to New Zealand's NSOs, which brings the total value since 2016 to nearly $100 million.

The GCSB produces an annual Cyber Threat Report that provides information about the number of cyber security incidents recorded by the GCSB and discusses the work our National Cyber Security Centre has undertaken. These reports can be found online at ncsc.govt.nz. A report for the 2019/20 financial year is expected to be released in the coming weeks.

If you wish to discuss this response with us, please feel free to contact information@gcsb.govt.nz.

You have the right to seek an investigation and review by the Ombudsman of this decision. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Yours sincerely

Andrew Hampton
Te Tumu Whakarae mō Te Tira Tiaki
Director-General, Government Communications Security Bureau