New Zealand

National Cyber Security Centre

2012 Incident Summary

National Cyber Security Centre – 2012 Incident Summary

Overview

The New Zealand National Cyber Security Centre (NCSC) provides enhanced services to government agencies and critical infrastructure providers to assist them to defend against cyber-borne threats.

As part of its functions, the NCSC receives and records cyber security incidents which are reported by these sectors. Reports are provided by victims, researchers, IT security partners as well as local and international partners. All reported incidents are treated as in-confidence and are notified via the reporting form located on the NCSC website.

The statistical information presented in these reports is provided to raise situational awareness and general understanding of the nature of the cyber-threat landscape facing New Zealand organisations and individuals.

Reporting

In its second year of operation, the NCSC saw an increase in the number of incidents reported, from a total of 90 in 2011, to a total of 134 in 2012.This increase is most likely attributable to greater awareness of the importance of reporting incidents, and of the role that the NCSC performs.

Incidents must meet certain criteria designed to differentiate them from other common events, experienced in the on-line environment, before they are logged by NCSC personnel. It is also important to establish that a single incident commonly includes multiple IP addresses, websites, networks and servers, organisations or affected parties.

P O Box 12-209, Wellington, New Zealand | incidents@ncsc.govt.nz | Phone: +64 4 498 7654 | Fax: +64 4 498 7655

Incident Types

The table 'Incident Reports – 2012' (Fig 1.1) provides a breakdown of the incident reports as categorised by type. The largest category of reported activity was scam & spam related which made up 31% of the incidents captured. Denial of service (DoS) attacks and Botnet/Malware activity were the second largest categories making up 16% and 14% of incidents respectively.

Other significant issues captured include website compromises, hijacking & defacement (10%), Spear Phishing (7%) and attempted network intrusions (which includes malicious scanning) (6%).

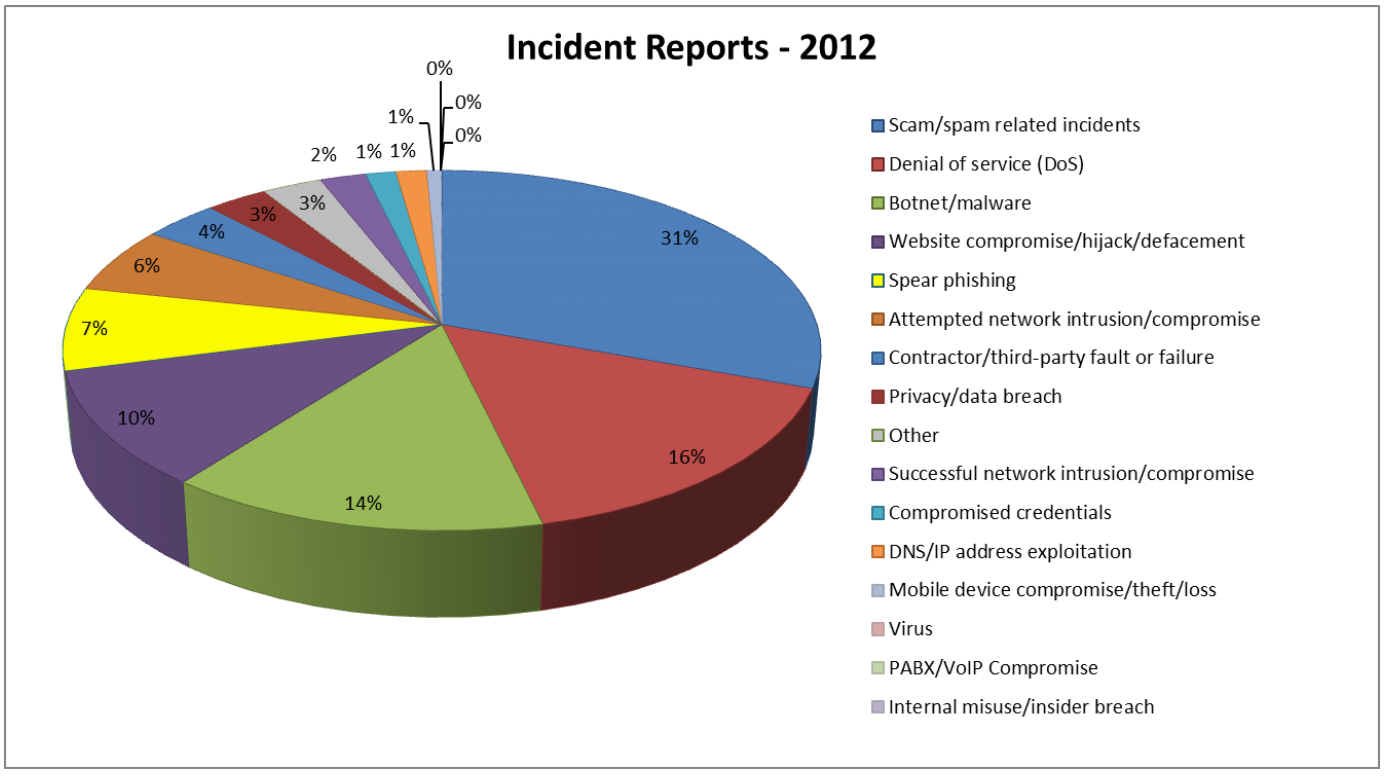

Fig 1.1

Fig 1.1 highlights that the New Zealand online environment continues to reflect global trends of the major cyber-security issues which have dominated the landscape in 2012.

Incident Attribution

Specific attribution of incidents can be problematic due to common measures used by malicious actors to obfuscate their identity and location. However through the combined efforts of the international IT security community, incidents like malware campaigns can often be ascribed a level of attribution.

In 2012, NCSC was able in general to attribute the majority of reported incidents (Fig 1.2). Specifically the bulk (60%) of the incidents reported to NCSC originated from an overseas source. Nearly a third of the incidents reported (31%) involved incidents originating from domestic sources. 9% of incidents were unable to be attributed to a specific origin.

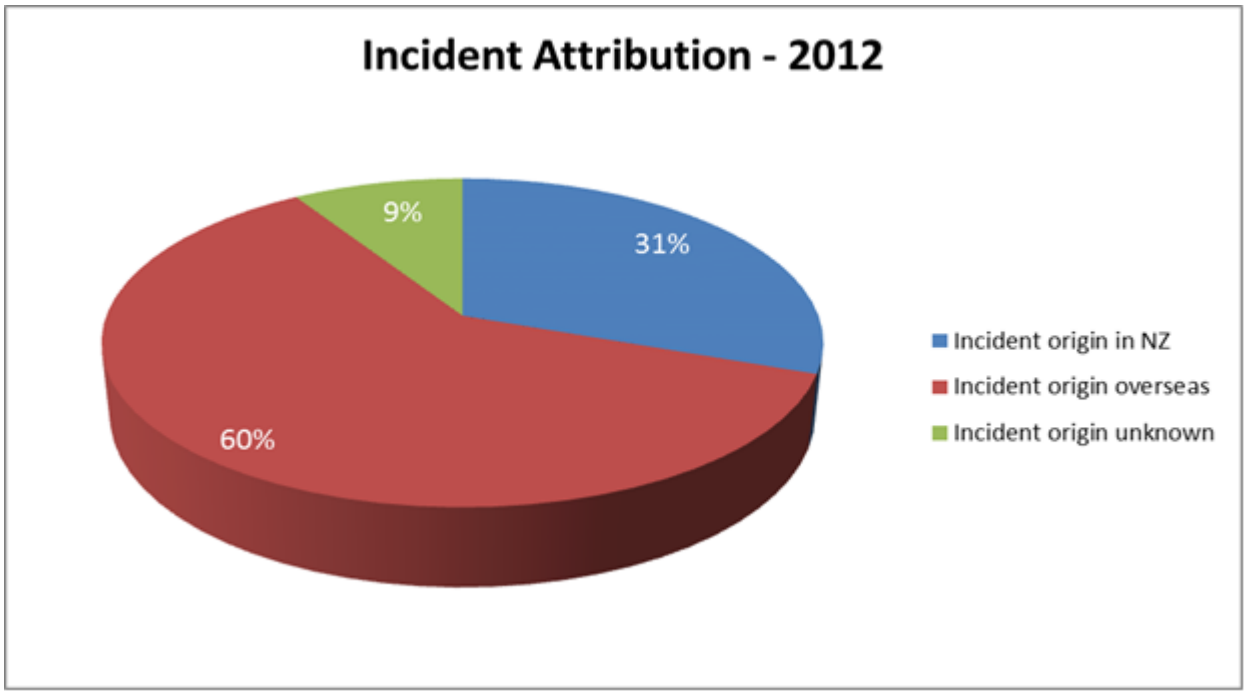

Fig 1.2

Incident Targets

After introducing increased granularity to the identification of incident targets, the dataset identified that the majority of incidents captured in 2012 were targeted towards the Private Sector (47%). Incidents targeted at Individuals were the second most targeted sector (26%), while Government (16%)andCritical National Infrastructure providers (6%) also reported significant numbers of incidents targeted at them.

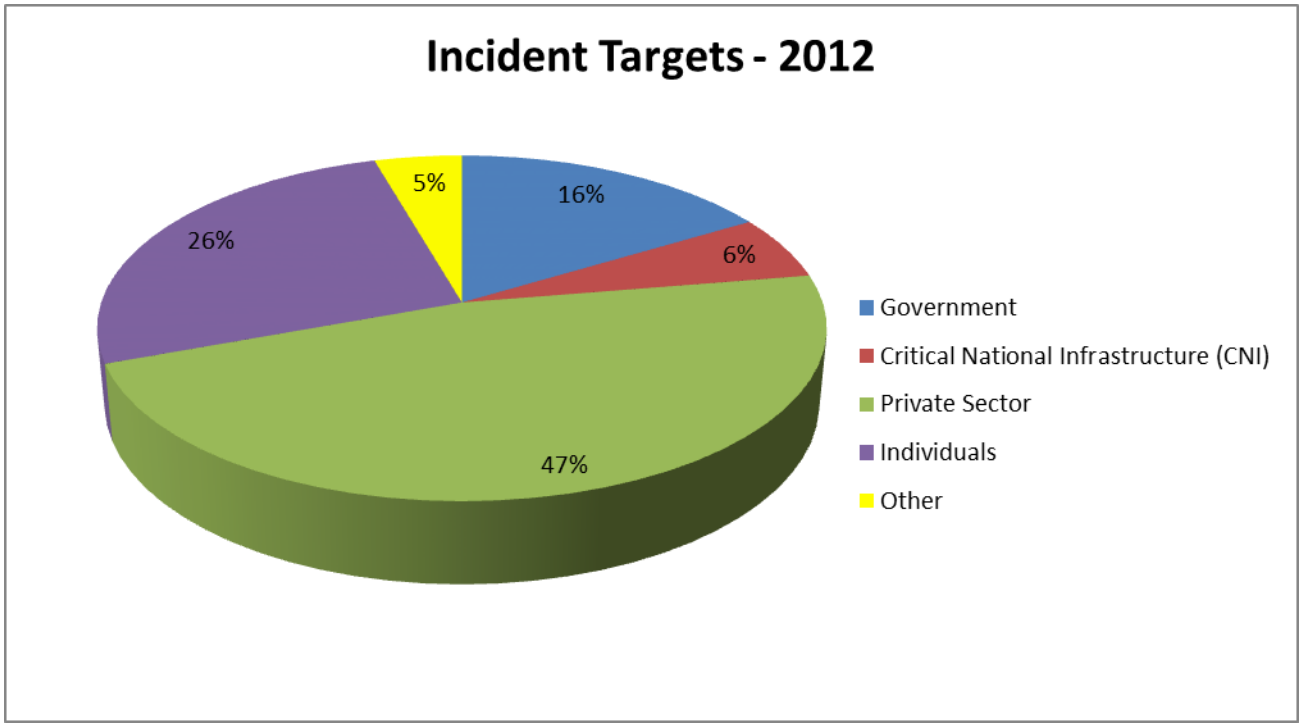

Fig 1.3

Concluding Remarks

While the reported data is based on a relatively small number of recorded incidents, the incidents captured fall into some of the more significant categories of incidents observed occurring in New Zealand's cyberspace.

Consequently, the on-going focus of the NCSC will remain the protection of core Government networks, the systems which support our critical national infrastructure, and

engagement with industry and business to protect our intellectual property and economic assets.

Contact Details:

If you or your organisation has experienced a cyber-security incident, this should be reported to the NCSC, as quickly as possible. All incidents must be reported via a completed Incident Reporting Form which is available on the NCSC website at: http://www.ncsc.govt.nz/incidents.html

Completed forms should be emailed to incidents@ncsc.govt.nz and if required you can speak with the NCSC directly on (04) 498-7654. All reports received are kept private.