# New Zealand

# National Cyber Security Centre


# 2011 Incident Summary

# National Cyber Security Centre – 2011 Incident Summary

**Summary**
The National Cyber Security Centre (NCSC) is responsible for providing enhanced services and assistance to protect government institutions and critical infrastructure from cyber threats. As part of these functions, NCSC records the cyber security incidents which are reported to it, the analysis of which contributes to a qualified understanding of the cyber-threat landscape in New Zealand.

## Reporting

NCSC became operational in September 2011, absorbing the functions of the Centre for Critical Infrastructure Protection (CCIP) into its expanded operations. The combined incident reports from CCIP and NCSC for the 2011 reporting period saw a total of 90 cyber-security incidents reported which varied in levels of scope and significance.

All recorded incidents must meet criteria designed to differentiate them from common incidents experienced in the on-line environment, and include only incidents which have been reported or identified by NCSC.

## Incident Types

The table below (Fig. 1.1) details the breakdown of incidents by type. The largest category of threat activity identified was Botnet related incidents which made up a total of 23% of all incidents reported. The second, third and fourth categories reveal that Phishing Related (18%), Compromised Credentials (16%) and Denial of Service attacks (16%) account for 50% of the reported incidents.



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

**National Cyber Security Centre:**
**2011 Incident Summary**

These incidents have all been identified as significant current global issues, which suggest that the New Zealand's threat landscape is experiencing similar challenges to those facing the other nations in Asia Pacific region[1].

Other incidents reported include Compromised Websites (12%), Intrusion Attempts (6%), PABX compromises (4%), Attempts to exfiltrate (leak) information (3%), Scanning & Spamming Incidents (1%) and Identified Viruses (1%).

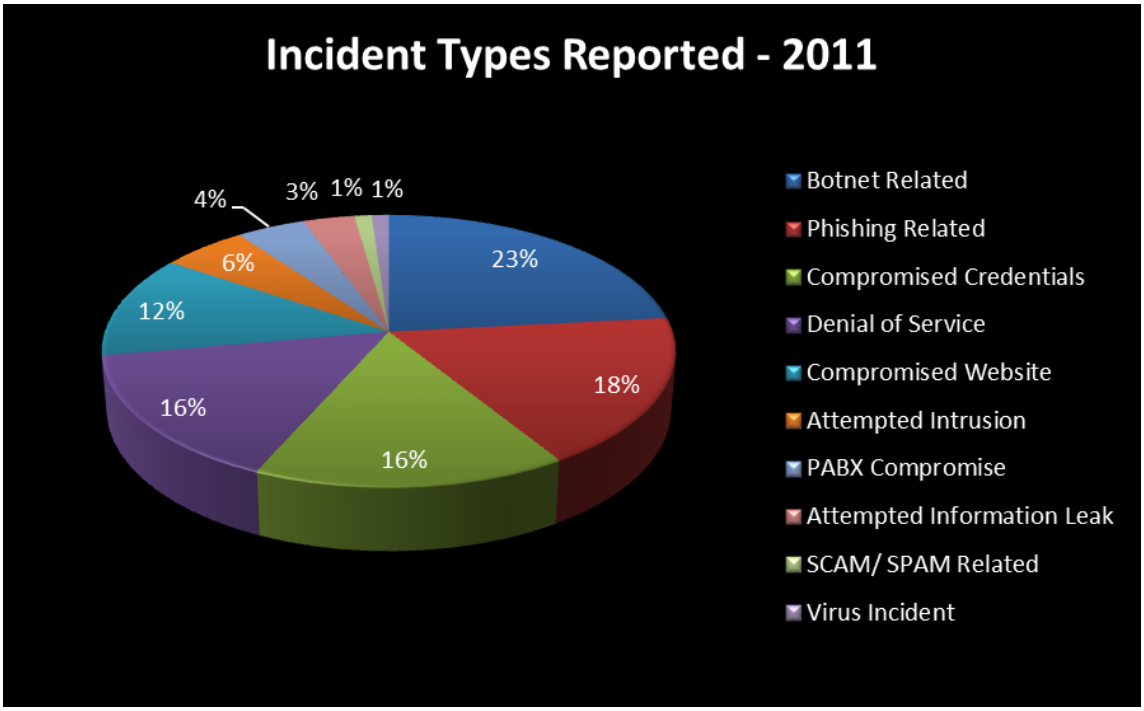


**Fig 1.1**

[1] APCERT annual report 2011 at: http://www.apcert.org/documents/pdf/APCERT_Annual_Report_2011.pdf



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

## Incident Attribution

Determining the attribution of incidents can be difficult because threat actors often seek to disguise their actions and seek to obfuscate their origins when engaging in cyber incident activity.

In 2011, NCSC was able to determine the attribution of a significant portion of incidents (Fig 1.2), determining that 46% of attacks originated from Non New-Zealand threat actors.

In addition, 51% of the recorded incidents were determined to involve compromised machines or websites within New Zealand, although these potentially relate to foreign threat actors. 3% of incidents were unable to be attributed to a specific origin.

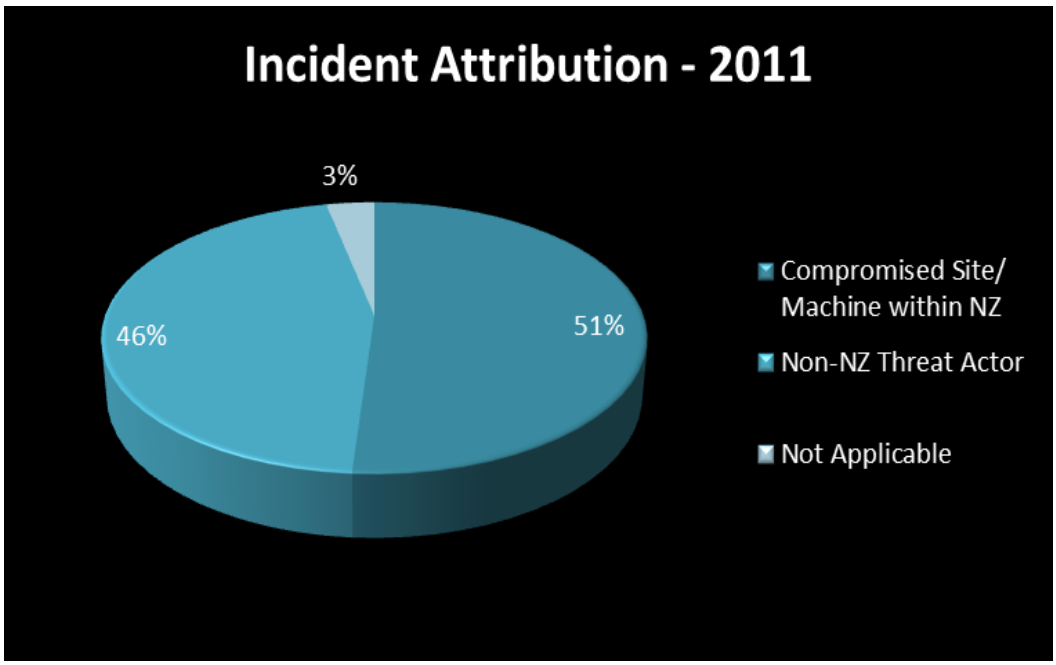


**Fig 1.2**



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

## Incident Targets

Cyber security issues affect the entire New Zealand cyber-environment, ranging from government agencies to critical infrastructure providers, other private sector entitites and to the wider population.

NCSC examines serious cyber security threats to core national agencies and critical infrastructure. In 2011, of the incidents reported to NCSC (Fig 1.3), 27% of the incidents reported were directly targeted at government agencies, while 4% were directly targeted at critial national infrastructure providers.

The remaining 69% of reported incidents were targeted at wider cyber-landscape targets, highlighting that all sectors of New Zealand face cyber security threats and challenges to improve IT security.

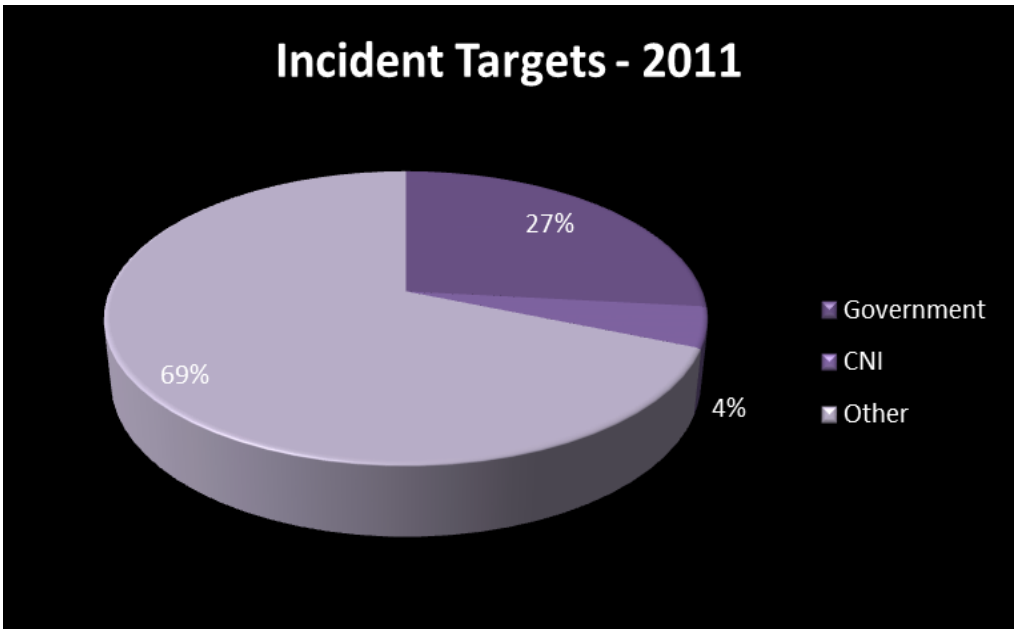


**Fig 1.3**



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



## Concluding Remarks

This report is aimed at providing a snapshot of the nature of the security threats facing New Zealand in 2011. The data is based on a relatively small number of recorded incidents, however the incidents measured fall into the most significant category of incidents observed in New Zealand's cyberspace.

The incidents observed reveal that there is considerable scope for NCSC to continue developing capabilities for protecting government systems and information, to capture, plan for and respond to significant cyber-security incidents, and to work with critical national infrastructure providers to improve the protection and computer security against evolving cyber- threats.

## Contact Details:

If you identify evidence of a cyber-security incident, it should be reported immediately to the NCSC. An Incident Reporting Form is available from the NCSC website.

Completed forms should be emailed to incidents@ncsc.govt.nz. Alternatively, you can contact us directly on (04) 498 7654.



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