New Zealand
National Cyber Security Centre
2014-2015 Incident Summary

9 December, 2015

190 cyber incidents for year to 30 June 2015

The National Cyber Security Centre (NCSC) recorded a total of 190 cyber security incidents for the 12 months to 30 June 2015.

GCSB Acting Director, Una Jagose says that of the 190 recorded incidents, 114 were identified as targeting government systems, 56 targeting private sector – with a further 20 where the sector targeting was not identified in the reporting.

Ms Jagose said that while the total number of incidents is slightly lower than for the 12 month period to December 2013, where 219 incidents were recorded, this was likely to be due to changes to recording and reporting practices, rather than a reduction in incidents.

"In fact I believe the reverse to be true and that serious incidents are continuing to increase. Over the past few months the NCSC incident response team is recording an average of one serious incident a day," she says.

Of total incidents recorded by the NCSC for 2014/15 period spear phishing made up 30.5 percent, with 58 incidents, followed by network intrusion/compromise with 21.5 percent (41 incidents) and botnets, 9.5 percent (18 incidents).

Denial of service and drive by download incidents were both equal at 5.8 percent, with 11 recorded incidents each, followed by credentials compromise with 9.

The NCSC 2014/15 statistics record significantly fewer spam, and scam and web site defacement incidents than in previous years.

The NCSC recorded just 7 scam/spam incidents in the 2014/15 period, which was just 4 percent of reporting, compared with 30 percent and 31 percent of reporting in the 2013 and 2012 calendar years.

There were 35 other recorded incidents, including virus (2), website hack (5) and internal misuse/breach/loss of device (4).

Ms Jagose, says the slight reduction in overall incidents (when compared to previous calendar year figures) is likely to be as a result of chances in approach - both victims and ours - rather than actual incident numbers.

"For example the reduced reporting of spam, scam and website defacement incidents is likely to be as a result of these type of incidents being now being reported to other organisations like Netsafe instead of the NCSC.

"We have also made changes to our own recording approach, specially relating to less advanced cyber threats, which will have reduced the total slightly," she says.

The NCSC is an operating unit of the Government Communications Security Bureau.

Definition of Incident Types

Cyber Security Incident

The NCSC defines an incident as an occurrence or activity that impacts on the confidentiality, integrity or availability of an information system (infrastructure).

Network Intrusion

A network intrusion is an incident of unauthorised access to a computer network by malicious actors.

Botnet

Botnet is a group or network of machines that have been infected with malicious software and are controlled as a group without the owner's knowledge. These are usually used to send spam or initiate DDoS attacks.

Drive-by download

A drive-by download usually occurs when a user visits a website they have been directed to by a threat actor, generally via a phishing or spear phishing email. The download will usually take advantage of a security flaw in a browser, app, or operating system that is out of date. This will be without the owner's knowledge or approval with the objective to install malware.

Phishing/Spear phishing

Email, often a carefully engineered – to reflect a particular interest of the receiver - which contain a threat, or a hyperlink to a threat, which when opened enables the adversary to access the user's device or network.

Denial of Service

A denial-of-service (DoS) attack is where an attacker prevents legitimate users from accessing information or services through a flaw in the service, e.g. by "crashing" a web server. A distributed denial-of-service (DDoS) attack is a more blunt form of this where the attacker uses multiple computers to flood a service to achieve the DoS outcome. The computers involved are usually co-opted in some way, either by being part of a botnet or by unwittingly responding to a seemingly legitimate request that is forged so that the victim is flooded with responses.