1 Executive Summary

On 2012, NBNCERT logged an investigation related to a suspected infected host on the NBNCO internal network. The host was "beaconing" to a server located in

The malware was found to be from the Citadel/Zeus family. This is primarily a password stealing "banking Trojan" which is sold on the underground hacker economy. It is generally used to commit online banking frauds, and has the gained in prevalence in the Australian Finance sector, particularly over the last 2 months. While this Trojan is advanced in its capabilities, it is certainly not uncommon.

The infected host within the NBN environment was a PC used at the time by a contractor, within the The PC was primarily used for the application for purposes. The PC was located and isolated within of NBNCERT logging a case. Further analysis, including a forensic image of the infected host revealed the malware was not detected by Anti Virus software. The malware was submitted to who quickly updated their detection signatures.

Analysis of other logs indicates that while the host was indeed infected, attempts by it to contact the Command and Control servers in question were unsuccessful due to

Released under the FOI Act - NBN Co FOI1213-15 - Document 1

1 Executive Summary

On 2012, NBNCERT logged an investigation related to an infected host on the NBNCO **guest wireless network**.

The malware on the infected host is from the *Torpig* trojan family, with roots thought to be from . Torpig is primarily a password stealing "banking Trojan". It is generally used to commit online banking frauds, and has been prevalent in the Australian Finance sector since around 2005. While this Trojan is advanced in its capabilities, it is certainly not uncommon.

Released under the FOI Act - NBN Co FOI1213-15 - Document 2

1 Executive Summary

2012, NBNCERT logged an investigation related to a suspected infected host on the NBNCO internal network. The host was observed to be "beaconing"

The malware was found to be from the Citadel/Zeus family. This is primarily a password stealing "banking Trojan" which is sold on the underground hacker economy. It is generally used to commit online banking frauds, and has the gained in prevalence in the Australian Finance sector, particularly over the last 3 months. While this Trojan is advanced in its capabilities, it is certainly not uncommon.

The infected host within the NBN environment was a laptop used by a The laptop was located, and the infected binary identified, a sample was secured, and then cleaned from the laptop within . Particular attention was paid to ensuring that the could complete tasks, and not have critical delivery targets impacted while the laptop was cleaned.

Further analysis of the infected binary revealed the malware was not detected by even the most current version of signatures from Anti Virus software, The malware was submitted to who subsequently updated their detection signatures, ensuring that the rest of the NBN then had protection from this malware variant.

Released under the FOI Act - NBN Co FOI1213-15 - Document 3