



LINKAGES – Edition 27 (IMPORTANT SECURITY ALERT)

A serious security vulnerability currently exists in most, if not all, Personal Computers in use across Local Government (and non-government PCs). This document describes the vulnerability, and the remedial action.

The Threat

Simply by viewing a webpage on an infected (or malicious) website, a Local Government employee's Laptop PC became infected with a Java based Keystroke logging trojan. The LCC team detected this trojan trying to send information out of a Laptop PC (which moves between two sites), to an intermediate site in the US, for subsequent harvesting by unknown persons in Ukraine.

The trojan has been observed (in other cases) to steal banking details, paypal account details and other sensitive information.

At this stage, it appears that no data has been lost from within the Local Government LANs; the LCC gateways appear to have successfully stopped the traffic from leaving the network.

However, if the laptop has been used to access the web from a home account, or from any other location which does not enforce the need to authenticate to a proxy prior to accessing the web, then it is extremely likely that information has been leaked via that external method.

The Vulnerability

The trojan was able to access the end user's system via two separate vulnerabilities, the first being a weakness in Internet Explorer (to do with iFrame handling), and the second via a weakness in the Java Virtual Machine.

Immediate Actions

1. The intermediate site in the US (www.sometimesidrink.com) has been added to the LCC Global Blacklist, and hence all councils with LCC Gateways have a further layer of protection against this specific threat variant.
2. The incident has been formally reported to AusCERT, including details of the original attack vector. AusCERT have passed it on to Federal Police, as the various ANZ, Commonwealth and St George Bank customers (amongst others) that have been compromised, will need to be advised.
3. The owner of the infected PC has been directly contacted, and the malicious code recovered for submission to AusCERT, for further laboratory analysis (this appears to be a new threat variant).
4. The information which this machine was attempting to send to the intermediate site, has been logged, but is encoded in some manner, so at present we are unable to identify the exact details that may have been compromised (or attempted to be compromised) in this case.

Required Council Actions

1. All PCs should be running up to date anti-virus software
2. All PCs should browse to <http://gw/java>¹ where a message regarding the vulnerability of their Java Virtual Machine (VM) will be displayed, and step-by-step instructions on how to update the Java VM. Note that the large update file associated with the Java VM update has been placed in the Gateway for direct, high-speed access. Also note that it appears that the Java VM update will not occur via Microsoft Windows Update.
3. Additionally, all PCs should be patched using Microsoft Update. The most efficient way of doing this, is to fully patch a single machine on the network, and then patch all other machines in the network. In this manner, most of the Windows Update .cab files are cached² in the LCC Gateway proxy cache, and hence update time on the second and subsequent PCs is significantly faster.

Summary

A dangerous and malicious Trojan has been detected "in the wild" on a Local Government LAN, and the underlying vulnerability currently exists on ALL Local Government PCs. A step-by-step guide to addressing the Java Virtual Machine weakness is available to all councils via their LCC Gateway, at <http://gw/java>

Please note that any Council which does NOT require users to authenticate against a proxy when accessing the web, is NOT protected against this threat. This probably includes all sites without an LCC Gateway; such sites will need to consult their IT Professionals, or may wish to contact the LCC Program to obtain an LCC Gateway.

Please also note that the ability of the LCC Gateways to trap and detect this malicious traffic, highlights the benefits of the "layered defence" approach that Local Governments have now adopted. It also highlights the value of the "annoying" need to authenticate when browsing the web.

This LCC Program newsletter *Linkages* is produced by the Western Australian Local Government Association and supported by the Australian Government through the Networking the Nation Program of the Department of Communications, Information Technology and the Arts.



An Australian Government Initiative

¹ This URL will only be effective for those Councils with an LCC Gateway. If you do not have a gateway, you are advised to contact your regular IT staff or IT service provider to determine an appropriate course of action; or contact the LCC team in relation to the managed gateway service on 1-300-766-542.

² This functionality is inherent to the LCC gateway, and may not be applicable to Councils without a LCC gateway or other suitable proxy.