Senate Finance and Public Administration Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Finance and Administration Portfolio

Department of Finance and Administration

Budget Estimates Hearings 2003-04 – 28 & 29 May 2003

Question: F69

Outcome: Cross Outcomes

Topic: DOFA Web site; Virus Attack.

Hansard page: Written Question on Notice

Written Question on Notice: 28 & 29 May 2003

Senator Lundy asked:

DOFA Web site

- Please outline the process surrounding the development of DOFA's Departmental web site.
- What was the entire cost of the web site development
- Please provide a breakdown of the Department's web site expenditure

Virus Attack

- Please outline by date the details of every computer virus to affect the Department in the last three months.
- Which viruses were they, and what was the nature of these viruses?
- Did these viruses impact on any work that was being done by the Department? If so, what work was affected and how?
- Did any of these viruses require new computer hardware or software to be purchased, leased or otherwise acquired by the Department, either on a permanent or temporary basis?

Answer:

DOFA Web site

The Department of Finance and Administration's (Finance) current web site was redeveloped and launched on 1 December 2000 to meet the Government Online Strategy, which included consistency in the presentation of the web site, accessibility standards for content and design to be met, application of Australian Government Locator Service (AGLS) metadata and inclusion of a privacy statement.

The Government Online Strategy requires that all Australian Government departments and agencies comply with a set of minimum web site standards. These standards aim to ensure a basic level of consistency and quality of service across all Australian Government web sites.

Senate Finance and Public Administration Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Finance and Administration Portfolio

Department of Finance and Administration

Budget Estimates Hearings 2003-04 – 28 & 29 May 2003

The process for the redevelopment of the Finance web site was:

- a small team was established in September 2000 to manage the project and to ensure that it met the Government online standards by the due date of 1 December 2000;
- a tender for the procurement of authoring software and web services was issued on 16 October 2000;
- the new software and graphic design template was implemented in the period 31 October 2000 to 1 December 2000; and
- the new site was launched on 1 December 2000.

The cost of web site redevelopment was $505,153.

Below is a breakdown of Finance's web site expenditure on development and maintenance of the web site since September 2000 (this also includes the costs of Web Services for the Finance intranet site).

Category (All amounts excluding GST)	**2000-2001**	**2001-2002**	**2002-2003**	**Total**
Web site development				
- Tender development/assessment, advertising	$33,890			
- graphic design	$25,480			
- web development	$364,601			
- software purchase				
- Net Objects authoring server	$64,000			
- Net Objects annual maintenance	$13,248			
- Microsoft backoffice	$2,285			
- Innoculate	$693			
- Arcserve	$956			
Sub total	**$505,153**			**$505,153**
Hardware lease and support	$69,210	$73,461	$51,479	**$194,150**
Web services*	$394,351	$408,669	$203,868	**$1,006,888**
Total	$968,714	$482,130	$255,347	**$1,706,191**

* This includes web site publishing, maintenance and administration for both the Finance Internet and intranet sites.

Senate Finance and Public Administration Legislation Committee

ANSWERS TO QUESTIONS ON NOTICE

Finance and Administration Portfolio

Department of Finance and Administration

Budget Estimates Hearings 2003-04 – 28 & 29 May 2003

Virus Attack

Firewall Reports

The firewall reports for March, April and May 2003 indicate the following virus types were detected:

March

HTTP Code Red / Code Red II Worm:

This virus exists in memory only (however, the .C variant does write a trojan program to the hard disk).

The virus spreads through TCP/IP transmissions on port 80. By making use of this exploit, the worm is able to send itself as a TCP/IP stream directly to its victims, which in turn scans the web for other systems to infect.

April

SQL SSRP Slammer Worm:

The SQL Slammer Worm is self-propagating malicious code that exploits a vulnerability in the Resolution Service of Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000.

HTTP Code Red / Code Red II Worm

Details as above.

May

No virus attacks reported.

- Note, all viruses were blocked and deleted. They did not impact upon any of the work performed by the Department, nor did any of the viruses force the Department to purchase, lease or otherwise new computer hardware or software on a permanent or temporary basis.

Scanmail Reports

In addition to the Firewall, the Department of Finance and Administration's Mail Exchange server has Scanmail check all email messages for infection. The following is a report covering the number of infected messages per week on the exchange server/s for March, April and May:

March 2003 -

07Mar 03	14 Mar 03	21 Mar 03	28 Mar 03
1	0	4	1

April 2003 -

04 Apr 03	11 Apr 03	18 Apr 03	25 Apr 03
8	1	26	80

May 2003 -

02 May 03	09 May 03	16 May 03	23 May 03	30 May 03
149	48	30	24	24

The following types of viruses were detected:

Yaha
This mass-mailing worm poses as a joke screen-saver, using a filename FRIENDS.SCR. It will arrive as a message formatted to fool people into believing it has been forwarded intentionally by someone subscribing to a screen-saver mailing list.

Joke Geschenk
This is a joke program identified as 'GESCHENK' that initiates the opening of your CD-ROM tray. This file has an icon resembling the logo for Coca-Cola softdrink and the original file name was "cokegift.exe". The "joke" is in the suggestion that the program is a cup holder for your can of Coca-Cola by ejecting the CD-ROM.

Magistr
This variant of W32/Magistr.a@MM is considered a medium risk due to the number of samples received by AVERT. The variant differs in several ways:

- It uses a more complex encryption technique;
- It deletes all .NTZ files on the local machine;
- It terminates the ZoneAlarm firewall user interface process if it is running (not the entire program);
- It creates a SYSTEM.INI [boot] shell value to run itself at startup;
- It uses random file extensions on the executables which it sends (.bat, .com, .exe, .pif);
- The file name of the attachment that it sends out may be derived from a word within files on the infected system; and
- It has also been reported to retrieve email addresses from Eudora mailbox files (.MBX), overwrite the WIN.COM/NTLDR file with a program to erase data from the hard disk (the trojan is detected as QZap195, the WIN.COM or NTLDR must be replaced from backups), and send .GIF files found on the local machine to others along with itself.

Ethan
W97M/Ethan.a is a Word97 Macro Virus. It is a fast moving infector and reported to numerous AVERT Labs around the globe. Infection takes place when an infected Word document is closed, allowing the virus to propagate itself to normal.dot template.

W97M/Ethan.A is a parasitic class module infector, which consists of one macro, and is approximately 50 lines of code in length. It infects documents and templates using an algorithm to input data, from a source file c:\ethan. to the host document. This source file is exported VBA code of the virus.

Redlof

This is a file infecting VBScript that sets a default, infected, stationary file for the Microsoft Outlook and Outlook Express email client programs. It exploits the Microsoft VM ActiveX Component Vulnerability.

The script arrives in an email message, hidden from the user, or can be present on websites that contain infected .HTM files. The virus uses the BODY ONLOAD event to trigger the infection. .HTM, and .HTT files on the local system are infected by appending them with the encrypted, viral code. .HTT files are prepended with the BODY ONLOAD trigger, while this action is placed at the beginning of the virus body in .HTM files. The default mail account is retrieved from the registry and a stationary file is created, "BLANK.HTM", and is set as the default stationary file.

Marker

The W97M/Marker family hooks system events Document_Open and Document_Close to run the infection routine - this is common among all variants. Opening an infected document will disable macro virus warning protection, and copy the viral macro code to the global NORMAL.DOT template file.

As with other variants in the W97M/Marker family, information is kept as comments appended to the virus code as a sort of "log" as an indication of who has been infected, and when. An example of this comment would be: ' 03:24:08 PM - Monday, 14 Feb 2000 ' John Doe.

On the first of the month, this log is saved to C:\hsf (%varying log file name%) .sys. The file c:\netldx.vxd is created which is a text file that contains FTP instructions to upload the local log file to an FTP server. The macro then calls "command.com /c ftp ..." to carry out this function, but fails as this server has been taken down.

Gibe

This worm (a new variant of W32/Gibe@MM) is written in Visual Basic and propagates through various channels:

1. Mass-mailing (message mimics a Microsoft Security Update);
2. Network shares (copies itself as WEBLOADER.EXE to startup folder on mapped drives);
3. IRC (via dropped SCRIPT.INI file); and
4. KaZaa peer-to-peer file sharing network.

Strings within the worm suggest it may also be intended to propagate via sharing itself through KaZaa file-sharing networks, and via sending itself to Newsgroups.

Tristate

This virus infects Excel97, Word97 and Powerpoint97 (if installed). In Excel97, a file "BOOK1." is loaded from the XLSTART folder to infect files opened or accessed in Excel97 - when infecting, this virus drops the BOOK1. file and also infects the global template for Word97 "NORMAL.DOT", and finally infects "BLANK PRESENTATION.POT" blank presentation Powerpoint97 template.

Fortnight

This virus spreads by inserting a bit of HTML code into every message sent through Microsoft Outlook Express. This is accomplished by creating a new HTML file, and setting it as the default signature file used by Outlook Express. This virus exploits an Internet Explorer vulnerability in order to propagate.

Wdialupd

This is not a virus or trojan. It is a "Potentially Unwanted Program". VirusScan 7 will detect this application when scanning for "Potentially Unwanted Programs". The purpose of the program is to connect users to a pornographic service. It is likely to be downloaded via separate component than has been spammed to hundreds of thousands of email addresses by the same company.

Sobig

This worm in similar to W32/Sobig.b@MM.The worm propagates via email and over network shares. It contains its own SMTP engine for constructing outgoing messages.

- Note, all viruses were blocked and deleted. They did not impact upon any of the work performed by the Department, nor did any of the viruses force the Department to purchase, lease or otherwise, new computer hardware or software on a permanent or temporary basis.