McAfee
Product Management Statement

VirusScan Enterprise 8.0i
ScriptScan
Formal Issue: 22 June 2006

To: VirusScan Enterprise 8.0i Customers

From: McAfee Product Management

Subject: VirusScan Enterprise 8.0i ScriptScan Function

This Product Management statement is in response to concerns expressed by customers regarding the ScriptScan feature of VirusScan Enterprise 8.0i.

To date, upwards of 2000 script-based malware and variants have been detected in the wild. All of these malicious scripts will be detected and blocked by OAS when they access the file system. However, because the scripts can execute in memory before they touch the file system, ScriptScan was developed as a client-side feature to provide added protection for Java and Visual Basic scripts launched by client-side applications which use Microsoft scripting APIs. (ScriptScan is not intended or appropriate for server environments and can safely be disabled on servers.)

ScriptScan is sensitive to the way web pages are constructed, in particular, Java-based web pages. Jscript pages can be built from many component files, each of which must be scanned by ScriptScan. The processing time required for scanning these pages, and therefore the delay seen by the end-user in opening these pages, is directly related to the number of these individual components.

We recognize, however, that this can potentially put customers in the difficult position of making the trade-off between enhanced protection and end-user performance. By examining their ePO reports, customers can determine the relative concern of ScriptScan detections versus On Access Detections in their environment. For example, a customer data set provided to McAfee indicated that ScriptScan detections were about 3% of the total malware detections with the bulk of the detections from OAS. The customer's data also indicates, however, a significant degradation in end-user performance when ScriptScan is enabled. It is likely, therefore, that in this customer's environment, the benefits of running ScriptScan are out weighed by the negative impact on end-user performance and McAfee could concur that it was reasonable business practice for this customer to disable the VirusScan Enterprise 8.0i ScriptScan feature.

It is also likely that the script-base malware this customer had seen was from external sources not internal processes; otherwise, the percentage of ScriptScan detections would have been much higher. Therefore, this customer could elevate their protection level back to a comparable level by installing a Secure Web Gateway appliance just behind their externally-facing web-servers. This solution will provide the same protection as does ScriptScan, but directed only at the external web traffic and leaving the internal portal traffic unencumbered.

ScriptScan is a capability not currently provided by our major competitors. Customers can be confident that even though ScriptScan may not be right for all environments, VirusScan Enterprise 8.0i provides superior protection against blended threats, with integrated Buffer Overflow protection for common desktop applications and services, Access Protection rules to block and contain common threat models, true On-Access Scanning for malware, including Anti-Spyware, and rapid-response daily-DAT updates—backed by the power and performance of ePO.

Jae Pudewell, Sr. Product Manager *jae_pudewell@mcafee.com*