(UPDATED) AUGUST 2012

Application whitelisting explained

1. Application whitelisting is one of the top four strategies in DSD's list of *Strategies to Mitigate Targeted Cyber Intrusions*. This document provides high-level guidance on what application whitelisting is, what it isn't, and how Information Technology Security Advisers can apply it effectively in a Windows-based environment.

Why implement application whitelisting?

2. Application whitelisting is designed to protect against unauthorised and malicious programs executing on a computer. It aims to ensure that only specifically selected programs and software libraries (DLLs) can be executed, while all others are prevented from executing.

3. While primarily implemented to prevent the execution and spread of malicious software (malware), it can also prevent the installation or use of unauthorised software.

4. Implementing application whitelisting across an entire organisation can be a daunting undertaking, however deployment to high-value and often targeted employees such as executive officers and their assistants can be a valuable first step.

What is application whitelisting?

5. Application whitelisting comprises the following technical steps:

   a. identifying specific executables and software libraries which should be permitted to execute on a given system;

   b. preventing any other executables and software libraries from functioning on that system;

   c. preventing users from being able to change which files can be executed.

6. An intermediate approach to application whitelisting is identifying entire directories from which users are allowed to execute programs, such as C:\Windows, C:\Program Files, or even C:\Program Files\Specific Application. This provides some measure of protection from applications executing outside the specified directories but it does not take into account a number of possible scenarios for compromise. This technique is better than not applying application whitelisting at all, but a more comprehensive approach should be considered at the earliest opportunity such as at the next Standard Operating Environment (SOE) refresh.

What application whitelisting is not

7. Providing a portal or other means of installation of only approved software is not application whitelisting. This does not prevent users from running software not listed on the portal, and will not prevent malware from executing and compromising a system.

8. Application whitelisting is not accomplished by simply preventing users from writing to locations such as C:\Windows or C:\Program Files. While this may prevent a user from installing some software, it does not prevent the execution of software residing in locations such as a user's desktop or temporary directories. These locations are commonly used by malware to infect a computer.

How to implement application whitelisting

9. Application whitelisting is commonly implemented using a combination of a software product for identifying and approving necessary executable and library files, and Access Control Lists preventing users from changing the approved files.

10. AppLocker is a set of group policy settings which are present in Microsoft Windows 7. Extending the capabilities of Software Restriction Policies in earlier versions of Windows, AppLocker allows multiple levels of enforcement as well as several methods of recognising whitelisted executables. Both AppLocker and Software Restriction Policies are free application whitelisting products that are provided with recent versions of Microsoft Windows.

11. There are a number of third party applications which provide similar functionality to AppLocker. Mention of these products does not imply endorsement by DSD. Among these are products such as Bit9 Parity Suite, CoreTrace Bouncer, Lumension Application Control and McAfee Application Control.

12. It is crucial that the software selected and configuration used covers both executables and software libraries. An omission of either of those could negate the security afforded by the whitelisting implementation.

13. Whitelisted executables should be positively identified via means other than merely by file name or directory location. This helps ensure malware cannot trivially masquerade as legitimate software.

Further information

14. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.dsd.gov.au/infosec/ism/index.htm

15. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies can be found at:

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.