McAfee Malware Support - Best Practices Series

Avoid Potentially Unwanted Programs

What is a Potentially Unwanted Program?

Potentially Unwanted Programs (AKA PuP's), are non-malicious programs that have questionable content or behaviours, and as such are considered to be unsuitable to be installed on a corporate enterprise computer network. This content may be of an adult theme such as gambling or pornography, or online gaming, often this comes in the form of pop-advertisements. Other types of PuP's allow system/network administration functionality that may not be appropriate on the corporate environment and could be symptomatic of an attack from either an internal or external source.

How do PuP's get onto my machine?

Potentially Unwanted Programs are commonly downloaded and installed along with other software that has been intentionally downloaded, such as toolbars or other browser plugins. The installation of the PuP's may not be brought to the attention to the user during either the download or installation process, and is not always captured in the End-User License Agreement (EULA). PuP's can be difficult to remove, although some have fully functional uninstallers.

Hardening Actions

- Read EULA's carefully to understand the risk or likelihood of PuP's being included in the download.
- Only download reputable software for use on corporate networks.
- Ensure that McAfee VirusScan is configured to protect against PuP's with all categories enabled. These categories can be found in the Unwanted Programs Policy section. In environments where tools used for legitimate reasons are being detected as PuP's, exclusions can be put in place to avoid these detections without the need to disable either the specific category or the whole feature.
- Implementation of SiteAdvisor Enterprise (SAE) in your environment:
  - Based on McAfee Global Threat Intelligence (GTI) web reputation and web categorization services to identify sites that are hosting malware, infected by malware and hosting inappropriate content.
  - Identifies sites considered safe and not safe with a color scheme:
    - Green = Safe (Very low or no risk issues)
    - Yellow = Caution (Minor risk issues)
    - Red = Warning (Serious risk issues)
    - Grey = Unknown (Not rated yet, use caution)
    - McAfee Secure = Tested Daily for hacker vulnerabilities
  - Very easily deployed and configured through ePolicy Orchestrator.
  - FAQs for SiteAdvisor Enterprise (KB73457).
  - Provides authorization/blocking of websites and reactions based on safety ratings.
  - It provides another layer of protection. It can be used with IE, Firefox and Chrome.
  - As well as providing protection against malicious or compromised websites with varying degrees of web, e-mail or network reputation; it can help to educate users into safer browsing habits.
- If in doubt, submit a sample of the application to McAfeeLabs. Details of the process here.