Solution Brief

Protecting Against Potentially Unwanted Programs

Potentially Unwanted Programs (PUPs) are discussed in depth in the **McAfee® Labs Threats Report: February 2015**. Any application a user may find beneficial but that exhibits a tangible underlying risk to the user may be considered a PUP. The applications generally do not inform users of these risks. Unlike Trojans, viruses, rootkits, and other forms of malware, PUPs typically do not harvest user credentials (social media, banking, and other credentials) or alter system files in a malicious manner. PUPs lie in a "gray zone" of classification because they often offer a benefit to the user in addition to being a risk. They are often difficult to detect and categorize.

Here are some common behaviors that PUPs typically undertake:

- Modify system settings, such as browser configuration, without authorization.
- Conceal an unsought program within a legitimate application.
- Covertly collect user information, browsing habits, and system configuration.
- Hide application installation.
- Make removal difficult.
- Distributed by confusing or deceptive advertisements.

PUPs can take a variety of forms:

- **Adware**: Serves advertisements mainly through browsers.
- **Password cracker/revealer**: Displays an application's hidden password.
- **Remote administration tool**: Monitors user activities on the installed machine or allows remote control of the system without user awareness or consent.
- **Keygen**: Generates product keys for legitimate applications.
- **Browser hijacker**: Changes the home page, search page, browser settings, etc.
- **Hack tools**: Standalone apps that can facilitate system intrusions or loss of critical data.
- **Proxy**: Redirects or hides IP-related information.
- **Tracking tools:** Spyware or keylogging applications that collect user keystrokes, log personal communications, monitor user online activities, or capture screens without user awareness.

Here are the key differences between PUPs and other malware such as Trojans, ransomware, bots, and viruses:

Techniques	Potentially Unwanted Programs	Other Malware: Trojans, Viruses, Bots
Installation method	Standard application installation procedure, at times with license agreement. Often needs user acceptance and input to completely install on a system.	Installed as a standalone program without any user input. Mostly operates as an independent file.
Packaging	Bundled with clean applications and covertly installed along with the clean apps.	Standalone files with few additional components. Not packaged as installers.
Uninstallation	Sometimes the package contains an uninstaller, allowing removal. Often the uninstall procedure is difficult.	Executables add more complexity in removing the malware due to hooks into other processes, process handles, and other complex linkages. Because these are not installer packages, they do not appear in Control Panel.
Behavior	Displays unintended advertisements, pop-ups, pop-unders. Modifies browser settings, collects user and system data, or allows remote control of the system without user awareness or consent.	Steals personal identity and banking information, modifies system files, makes system unusable, asks for ransom, etc.
Stealth nature	Behavior is usually not stealthy.	Can hide files, folders, registry entries, and network traffic.

Among all the PUP categories, adware has attracted the greatest attention from security vendors—not because of annoying advertisements but because of the way in which adware abuses trust. Adware has become smarter by implementing various techniques to ensure its continuous presence on infected systems. Here are some of the methods:

- Standalone process running in memory.
- Component object model (COM) and non-COM DLL files with functions built specifically for the app.
- Browser helper objects registry keys.
- DLLs hooked to system processes.
- Browser extensions and plug-ins.
- Registered system services.
- Device driver components performing device control functions.
- Low-level filter drivers.
- Trojans delivered as payload.

PUPs are typically propagated by abusing the trust of innocent users as explained in the **McAfee Labs Threats Report: November 2014**. The most common distribution techniques for PUPs include:

- Covertly piggybacking on a legitimate application.
- Social engineering.
- Selling Facebook likes.
- Posting scam messages on Facebook.
- Hijacking Google AdSense.
- Unintended browser extensions and plug-ins.
- Forced installation along with legitimate applications.

How Intel Security Can Help Protect against PUPs

McAfee Application Control

McAfee Application Control lets your business control which applications are allowed to run in your environment through dynamic whitelisting and enforcement policies on both connected and disconnected endpoints. It can help protect your company from PUPs.

- **Dynamic whitelisting**: Enable your organization to efficiently manage your whitelisted applications by developing your whitelist automatically as systems are patched and updated. McAfee Application Control reduces your exposure to PUPs by not allowing known adware to run.
- **File reputation**: Integration with **McAfee Global Threat Intelligence** (McAfee GTI) allows McAfee Application Control to query real-time feeds of known good, bad, and unknown file types to help with whitelisting and help your company stay aware of applications that are known to be PUPs.
- **Protection whether connected or disconnected**: Enforce controls on connected or disconnected servers, virtual machines, endpoints, and fixed devices such as point-of-sale terminals.

McAfee Web Gateway

Malvertising, drive-by-downloads, and malicious URLs embedded in trusted websites are just some of the attack methods used to deliver PUPs. **McAfee Web Gateway** is a robust product that will boost your company's protection against this type of threat.

- **McAfee Gateway anti-malware engine**: Signatureless intent analysis filters out malicious content from web traffic in real time. The McAfee Gateway anti-malware engine inspects files and blocks them from being downloaded by users if the files are malicious.
- **Integration with McAfee GTI**: Real-time McAfee GTI file reputation, web reputation, and web categorization feeds offer protection against the latest threats because McAfee Web Gateway will deny attempts to connect to known malicious websites or websites that use malicious ad networks.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence (McAfee GTI) is a comprehensive, real-time, cloud-based threat intelligence service that enables McAfee products to block cyberthreats across all vectors—file, web, message, and network. Proactively protect against PUPs with these features:

- **Intelligence through vector correlation**: Collects and correlates data from and across all key threat vectors, including file, web, email, and network, to detect blended threats such as ad networks delivering signed malware.
- **Comprehensive threat intelligence platform**: Collects threat intelligence from millions of sensors on customer-deployed McAfee products such as endpoint, web, mail, network intrusion prevention systems, and firewall devices.

- **Certificate reputation**: Query real-time feeds of known good and bad certificates to protect your company against threats such as signed malware that can be delivered by malicious ad networks.
- **Security Connected**: Integrated with other McAfee security products to provide the broadest threat data, deepest data correlation, and most complete product integration available today to ensure protection against adware.

McAfee SiteAdvisor® Enterprise

Staying on top of the ever-changing threat landscape is challenging, especially when trying to protect online users against threats such as PUPs without imposing harsh policies that ruin the user experience.

- **Easily identify threats such as malicious websites posing as legitimate**: Featuring an intuitive color-coded rating system, **McAfee SiteAdvisor Enterprise** gives an extra layer of protection at the desktop. It will deny connections to known malicious websites and inform users of the danger.
- **Enhanced security powered by McAfee GTI**: McAfee GTI provides real-time threat intelligence information to McAfee SiteAdvisor Enterprise, which assesses websites based on the most current information.

McAfee Threat Intelligence Exchange

Having an intelligence platform that can adapt over time to suit your environment's needs is important. **McAfee Threat Intelligence Exchange** significantly reduces exposure to these types of attacks thanks to its visibility into immediate threats such as unknown files or applications being executed in the environment.

- **Comprehensive threat intelligence**: Easily tailor comprehensive threat intelligence from global intelligence data sources. These can be McAfee GTI or third-party feeds, with local threat intelligence sourced from real-time and historical event data delivered via endpoints, gateways, and other security components.
- **Execution prevention and remediation**: McAfee Threat Intelligence Exchange can intervene and prevent unknown applications from being executed in the environment. If an application that was allowed to run is later found to be malicious, McAfee Threat Intelligence Exchange can disable the running processes associated with the application throughout the environment due to its powerful central management and policy enforcement capabilities.
- **Certificate reputation**: Integration with McAfee GTI protects your company in real time against attacks that leverage signed malicious code by querying real-time feeds of known good and bad certificates. McAfee Threat Intelligence Exchange can safeguard your endpoints against malicious certificates through centrally managed policies that can be deployed to protect both connected and disconnected endpoints.

McAfee VirusScan® Enterprise

Detecting and cleaning malware, including adware, is simple with **McAfee VirusScan Enterprise**. McAfee VirusScan Enterprise uses the award winning McAfee scanning engine to protect your systems from viruses, worms, rootkits, Trojans, and other advanced threats.

- **Proactive protection from attacks**: Integrates antimalware technology with intrusion prevention to protect against exploits that leverage buffer overflow exploits targeted at vulnerabilities in applications.
- **Unbeatable malware detection and cleaning**: Protects against threats such as rootkits and Trojans with advanced behavioral analysis. Stops malware in its tracks through techniques like port blocking, filename blocking, folder/directory lockdown, file share lockdown, and infection trace and block.
- **Real-time security with McAfee GTI integration**: Protection against known and emerging threats across all threat vectors—file, web, email, and network—with the support of the most comprehensive threat intelligence platform in the market.

Protecting your company against PUPs that seek to circumvent the traditional trust model with underhanded and unwanted behaviors can be a challenge. Combining industry-leading research from McAfee Labs with Intel Security technology can help your company protect itself from PUPs.

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee, the McAfee logo, SiteAdvisor, and VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2015 McAfee, Inc. 61739brf_pups_0215_ETMG

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com