White Paper

McAfee®

Three Best Practices to Protect Against Fake Alerts, Fake Anti-Virus, and Other Rogue Programs

Table of Contents

Executive Summary

Fake alerts, fake anti-virus, and "scareware" are unwanted "rogue" programs that have recently increased in number and sophistication, with thousands of variations released every day. These programs are part of a larger category of rogue programs that rely on user actions to insert themselves onto unprotected endpoints. Unsuspecting users are being infected by these programs in drive-by installs or by choosing "yes" when a pop-up says they are infected and choosing to install one of these programs.

Here we discuss how these programs work and recommend three best practices to keep these unwanted programs out of your networks.

Recommended Best Practices

- *Easiest method*—Use McAfee® VirusScan® Enterprise access protection rules and deploy free McAfee SiteAdvisor® Enterprise via McAfee ePolicy Orchestrator® (McAfee ePO™) software. This solution will block most rogue programs, and SiteAdvisor will help warn users to stay away from known bad sites that host these programs. This method is detailed later in this document.
- *Easy method*—Deploy McAfee endpoint URL filtering. This feature will add blocking to the SiteAdvisor technology mentioned above. This will block known bad sites but may not catch all rogue programs, because many use drive-by or hidden i-frames.
- *Best protection*—Deploy McAfee Web Gateway. Your best protection against rogue programs is McAfee Web Gateway, which will stop the vast majority of these programs before users can get to them. Care must be taken when configuring McAfee Web Gateway, as modifications to policies by the administrator can make it less sensitive to infection. Remote users are a particular challenge for appliance-based customers. For remote users, McAfee offers a hybrid solution that funnels traffic through our cloud gateway if the users are not on the corporate network. This method is not detailed in this document, so we recommend that you contact McAfee or your reseller for more information on this technology.

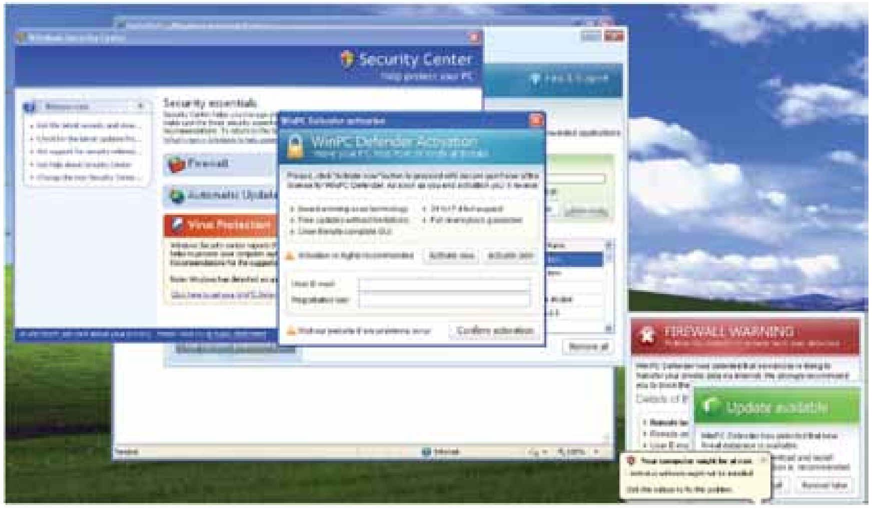


Figure 1. Fake alerts, fake anti-virus, and other scareware programs are an increasing threat.

Source and Motives

McAfee research has shown us that cybercriminals have set up multinational companies mirroring the usual procedures used by commercial industry to execute financial transactions online. Given the amount of money cybercriminals can earn, this type of business is certain to grow. Today, the sale of fake anti-virus software appears to be at the top of the fraudulent software market. However, fake alerts are not the only category offered on suspicious websites and through dubious commercial approaches in the past few years. Many software programs—such as fake video codecs, fake registry cleaners, and fake PC accelerators—are also available to unsuspecting users.

Infection Mechanism

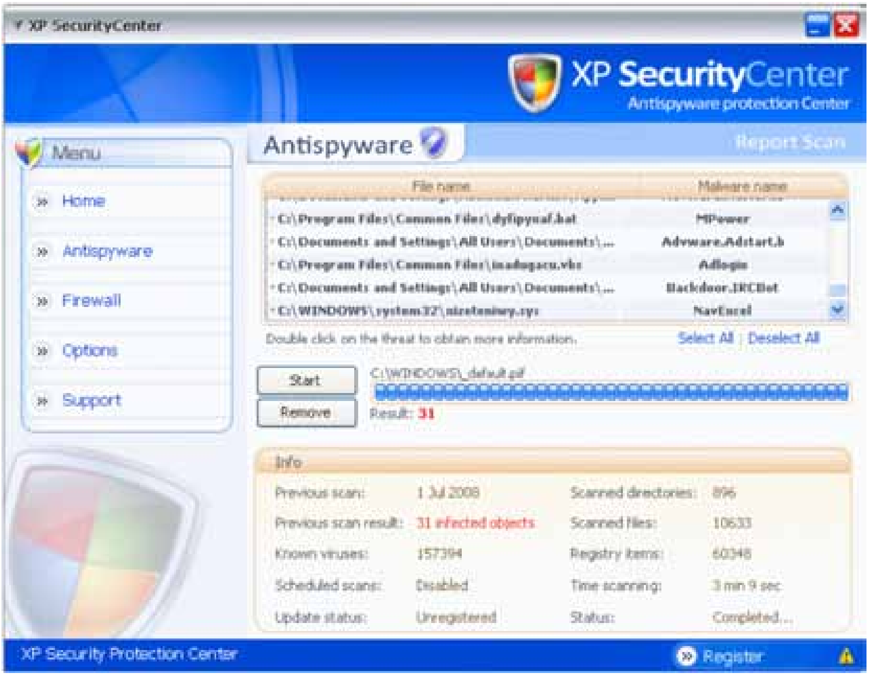
The rogue programs all operate in a similar way: either a drive-by install or a downloader will silently install either part of or the whole rogue security application.

Often the initial infection is a simple browser help object or process that performs a pop-up or sends the user an alert saying the system is infected and would you like to protect the system by installing x, y, or z application. The full application may be then installed if not before.

Many of these fake alert programs use a background bmp to falsely notify the user the system is infected. They also install screensavers and even Joke Bluescreen.c, which leads some users to believe the machine has crashed.

It often prompts a user that the system is infected with some spurious piece of malware and asks them to "Please *pay* to download the full version of our product in order to remove the threat."

All of these fake alert Trojans attempt to look like Microsoft Windows XP, Microsoft Windows Vista, or Microsoft Windows 7 native applications, often mimicking the Microsoft Security Center Control Panel applet. Several versions are now installing their own Control Panel applets.



File name	Malware name
C:\Program Files\Common Files\dyfipyaf.bat	MPower
C:\Documents and Settings\All Users\Documents\...	Adware.Adstart.b
C:\Program Files\Common Files\inadagacu.vbs	Adlogin
C:\Documents and Settings\All Users\Documents\...	Backdoor.IRCBot
C:\WINDOWS\system32\nizetaniwy.sys	NavExcel

Double click on the threat to obtain more information.

C:\WINDOWS_default.pif

Result: 31

Previous scan:	1 Jul 2008	Scanned directories:	896
Previous scan result:	31 infected objects	Scanned files:	10633
Known viruses:	157394	Registry items:	60348
Scheduled scans:	Disabled	Time scanning:	3 min 9 sec
Update status:	Unregistered	Status:	Completed...

Figure 2. Many fake anti-virus products are designed to look like legitimate products. They quickly move from an "alert" to the purchase prompt to extract money from the victim.

The McAfee Philosophy on Rogue Applications

McAfee VirusScan Enterprise detects most fake anti-virus, fake alerts, and other scareware, labeling them as "fake alerts." McAfee VirusScan Enterprise will detect these programs along with all of the "accessories" they use in setup (downloaders, droppers, hidden scripts within booby-trapped web pages, and more). Not all are detected by default, however, as most of these programs operate exactly like many legitimate business applications, such as WebEx, which require user action to install. McAfee designs its products with default settings that provide protection against major threats, while minimizing false positives. Some specialty security tools specialize in detecting these applications but do not provide comprehensive protection against the vast majority of threats. McAfee focuses on 100 percent of the threats in the wild, offering protection against malware going back to more than 10 years. Several McAfee products can be deployed to minimize the impact of these rogue programs, including access protection rules (in McAfee VirusScan Enterprise), SiteAdvisor, and the McAfee Web Gateway appliance.

Recommended Protection Strategies

Controlling scareware with McAfee VirusScan Enterprise's access protection rules

To increase your protection against fake alerts and the various side effects they impose on a system, we suggest that access protection rules in McAfee VirusScan Enterprise be enabled on your endpoints to block their known malicious behavior like modifying user favorites or spoofing Microsoft Windows processes. The list below includes a list of rules that are already in McAfee VirusScan Enterprise by default as well as some custom rules that can be created that will prevent the fake alert files from being created on the system. For each rule, it indicates whether the rule is expected to have end-user impact. In all cases, we recommend that the rules be tested before deployment

The following default rules should have no impact on end-user experience:

1. Lock down Microsoft Internet Explorer Favorites and settings.
2. Registry Editor and Task Manager from me disabled.
3. Prevent User Rights policies from being edited.
4. Prevent hijacking of exe and other executable extensions.
5. Prevent Windows process spoofing.
6. Prevent alteration of file extensions.

The following may have some impact on the end-user experience:

1. Prevent installation of browser helper objects and SHee extensions.
2. Prevent programs registering to autorun.
3. Prevent programs registering as a service.

We also recommend that custom rules be generated to prevent exe, dll, and sys files from being generated in user data directories where executable files should not be created.

For your convenience, McAfee has created comprehensive instructions for McAfee users in the following McAfee KnowledgeBase articles:

https://kc.mcafee.com/corporate/index?page=content&id=PD23178

https://kc.mcafee.com/corporate/index?page=content&id=PD23177

Deploying SiteAdvisor

SiteAdvisor (free edition) offers in-browser warnings to help users avoid malicious sites. If you have a grant number for any product with McAfee ePO software, you will have access to the free version of SiteAdvisor, which can be deployed to users via McAfee ePO software. For a fully managed experience, you will need SiteAdvisor Enterprise, which offers management and blocking of malicious sites. This product is available with any current McAfee endpoint product suite and is included in your software grant. The installation guide for SiteAdvisor Enterprise can be found here.

General Tips for Users: Use Caution When Browsing

The following tips can be sent to your user community to help educate them on proper web usage:

1. Don't click without thinking.
2. Never believe pop-up windows or banner ads that unexpectedly appear on your screen alerting you of a viral threat.
3. Never accept a random online scan of your computer's hard drives. Security developers such as McAfee offer such online services, but they are never activated unexpectedly. They require you to voluntarily visit their sites.
4. Never buy anti-virus products online from a computer that is possibly or actually infected. The malicious program on your computer could intercept your bank data or secretly direct you to a fraudulent site.
5. If you must buy online anti-virus software on a merchant or bank site from a healthy workstation, check that it is secure and is using a digital certificate that guarantees its authenticity. For this, the browser displays two pieces of information that must be checked:
   - The site's URL must start with https://, and the site name must match what the user expects
   - A small padlock should appear to the right of the site address or on the bottom right of the status bar (depending on your browser and version). It symbolizes a secure connection. Clicking on it will display the site's digital certificate and the organization's name.
6. A legitimate site should never ask you to enter your PIN for your bank account.

How to Submit Malware Samples to McAfee

Please use your support portal to submit files that you suspect are fake anti-virus, fake alerts, or other scareware. Here is a McAfee Knowledgebase article about the process.

Conclusion

Studying scareware has shown us that, to reach their financial goals, cybercriminals have set up multinational companies mirroring the usual procedures used by financial and industry entrepreneurs. For the past two years, police departments have had undeniable success apprehending them. The indictment of several leaders and the hard work of researchers have repeatedly disrupted these establishments, which have had to redeploy to more discrete, though equally effective, entities. Given the amount of money cybercriminals can earn, this type of business is certain to grow. Today, the sale of fake anti-virus software appears to be at the top of the fraudulent software market. However, scareware is not the only category offered on suspicious websites and through dubious commercial approaches in the past few years. Many software programs—such as fake video codecs, fake registry cleaners, and fake PC accelerators—are available to unsuspecting users.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com