TrendLabs is Trend Micro’s global network of research, development, and support centers committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery.

A Trend Micro White Paper  |  June 2010
INTRODUCTION

FAKEAV INFECTION VECTORS

Spammed Messages
Posing as Legitimate Antivirus or Anti-Spyware Programs
Fake Codecs
Search Engine Optimization Poisoning
Social Networking Sites
Malvertisements
Sponsored Sites

FAKEAV PROLIFERATION VIA MALICIOUS ROUTINES

Iframes
Compromised Websites
Infected .HTML Files
Supporting Malware
Droppers
Downloaders
Infectors
Exploits

MALWARE TRANSFORMATION

EVOLUTION OF FAKEAV

NOTABLE MALWARE BEHAVIORS

Utilizes Various Stealth Routines
Terminates Processes
Displays Pop-Up and Fake Warning Messages
Displays Warning Messages When Viewing Search Results
Drops Files
Displays Program Installation Prompts
Unmasking FAKEAV

Redirects to FAKEAV Download Sites ................................................................. 18
Modifies the Layered Service Provider ............................................................... 19
Utilizes Registry Shell Spawning ......................................................................... 19
Blocks Access to Sites and Displays a Warning Page ........................................... 21
Connects to Porn Sites .......................................................................................... 21

ONLINE AND LOCAL FAKEAV TYPES ................................................................ 22
Online FAKEAV Variants ....................................................................................... 22
Local FAKEAV Variants ......................................................................................... 23

PROTECTION AGAINST FAKEAV INFECTIONS .................................................. 24
RECOVERING FROM A FAKEAV INFECTION ....................................................... 28
CONCLUSION ........................................................................................................... 29
REFERENCES ........................................................................................................... 30
INTRODUCTION

This white paper aims to educate companies’ IT department staff on how rogue antivirus or FAKEAV applications arrive on systems. It aims to arm them with the right Trend Micro solutions that can help them combat these threats.

FAKEAV threats have been rampant in the past few years and are definitely here to stay. Various FAKEAV variants have, in fact, infected millions of PCs and are continuously spreading worldwide.

One key weakness in an organization is a user who may unknowingly open a malicious email attachment or click a URL that redirects to a malicious site. This paper aims to educate users on the different social engineering techniques cybercriminals use to proliferate their malicious creations, particularly FAKEAV. An educated user will be more cautious with what he/she does, which will result in fewer malware infections.

The primary reason why FAKEAV infections have become well-known to users is because they have visual payloads. Variants of the malware family often display pop-up messages telling users that their machines have been infected. This may cause panic among users, pressuring them to purchase rogue antivirus applications in hopes of resolving the issue. Users should, however, never purchase antivirus software from unknown sources.
FAKEAV INFECTION VECTORS

Cybercriminals use different social engineering techniques to trick users into downloading and installing FAKEAV onto their systems. User education is thus key to understand and battle this type of malware. The most common FAKEAV infection vectors will be discussed in more detail in the following sections.

Spammed Messages

Cybercriminals often use spammed messages that entice users to click embedded links that lead to the download of FAKEAV.

![Sample FAKEAV spam](image)

**Figure 1. Sample FAKEAV spam**

Posing as Legitimate Antivirus or Anti-Spyware Programs

Users who surf the Web in search of downloadable antivirus or anti-spyware programs may end up with links to FAKEAV sites in their search results. Using popular search engines like Google and Yahoo! is, after all, no guarantee that they will not come across malicious links as results. A lot of FAKEAV applications like *XP Antivirus*, *Antivirus 2008*, and *Antivirus 2009*, in fact, became popular since they could be easily downloaded from innocent- and professional-looking sites.
Fake Codecs

Codecs are plug-ins for applications that can easily be downloaded off the Internet. Certain codecs are needed to play some types of media files that is why some video-streaming sites require users to download video codecs. Cybercriminals have identified this routine as another social engineering approach to push FAKEAV disguised as codecs that unsuspecting users could download and install onto their systems.
Unmasking FAKEAV

Search Engine Optimization Poisoning

Search engine optimization (SEO) is a process to increase traffic to a website in order to improve its ranking, thus allowing it to appear among the top search results. Cybercriminals often use this technique to easily redirect users to the malicious sites they create.

In July 2009, a FAKEAV variant rode on the popularity of a solar eclipse. Internet users searching for “solar eclipse 2009 in America” using popular engines like Google were led to a site where a script-based FAKEAV was hosted.

**Figure 4. Malicious link that led to a FAKEAV download**

Social Networking Sites

Social networking sites such as Twitter and Facebook have also become notable sources of FAKEAV variants. Fake social network accounts were created to host messages like the one below, which contain links that lead to FAKEAV sites.

**Figure 5. Malicious links embedded in social network messages**

Malvertisements

Some malicious advertisements aka malvertisements in compromised sites can also lead to a FAKEAV infection. A popular newspaper website has, in fact, fallen prey to this scheme in September last year.
Sponsored Sites

In September 2009, malicious links that led to the download of a FAKEAV variant were discovered as one of several search engines’ sponsored sites.

Figure 6. Malicious FAKEAV download link to a supposed sponsored site
FAKEAV PROLIFERATION VIA MALICIOUS ROUTINES

Iframes

An iframe is a Web page element that functions as a document within a document or like a floating frame. It loads another .HTML document in-between <iframe> tags. Cybercriminals have currently been using iframes to lead users to compromised sites where FAKEAV variants are hosted.

Compromised Websites

Legitimate websites are hacked to inject iframe codes that lead to FAKEAV download links. When a user visits a compromised site, a FAKEAV binary is automatically downloaded onto his/her system. Most hackers target sites that have large numbers of visitors such as government sites, search engines like Google and Yahoo!, educational sites, and the like.

Infected .HTML Files

Like websites, local .HTML files on an affected machine can be infected by malicious iframe codes. As a result, a FAKEAV malware is downloaded upon opening infected .HTML files.

Iframe infections from websites and .HTML files are similar since the former are created using .HTML files. Iframe codes are usually injected at the end of .HTML files but there are also cases wherein these are injected in-between the original codes of an infected file.

Supporting Malware

Droppers

Droppers are malware whose primary routine is to drop and execute FAKEAV binaries. They usually embed the file in the malware body. Alternatively, other malware drop FAKEAV variants as only one of their numerous malicious routines. An example of this type of malware is TROJ_EMBED.AM, which is a .GIF file with an embedded XP Antivirus 2008 installer.

Downloaders

Downloaders are malware that do not directly drop FAKEAV variants but instead require Internet access in order to download the said variants. Downloaders rely on Internet connection in order to infect a machine. They are popularly distributed via spammed messages that purport to be software update and other notifications.
Unmasking FAKEAV

Figure 7. FAKEAV spam purporting to be a Microsoft update notification

Upon execution, users may see a prompt (see Figure 8) telling them that the new security software has been installed onto their systems.

Figure 8. Sample FAKEAV prompts
Other variants also used pop-up windows such as the one shown in Figure 9 to notify users that their systems have been infected by some malware.

![Sample FAKEAV pop-up window alert](image)

**Figure 9. Sample FAKEAV pop-up window alert**

**Infectors**

File infectors’ primary task is to search for all .HTML files on an infected system and to inject an iframe code into the files found.

**Exploits**

FAKEAV variants also take advantage of software vulnerabilities like PDF and SWF exploits, SQL injections, and the like. Most of the time, the exploited files become droppers or downloaders of not only FAKEAV variants but also of other malware.

One example of such an attack targeted an *Adobe Reader* vulnerability, which could cause the application to crash and could potentially allow an attacker to take control of an affected system. After successfully exploiting the said vulnerability, the Trojan drops and executes various embedded malicious binaries, one of which is a FAKEAV variant—**TROJ_PIDIEF.IN**.
Cybercriminals employ various social engineering tactics to profit. They continuously devise new techniques to compel users to purchase rogue antivirus software. In essence, the evolution of FAKEAV malware is being driven by cybercriminals’ sole purpose—to gain profit—as shown in the following flowchart.

Figure 10. FAKEAV cycle
## EVOLUTION OF FAKEAV

The following table shows the characteristics of each generation of FAKEAV variants.

<table>
<thead>
<tr>
<th>Generation</th>
<th>Characteristics</th>
</tr>
</thead>
</table>
| First      | • Downloads FAKEAV variants  
             • Uses graphical user interface (GUI) and purports to be a legitimate antivirus application  
             • Is manually installed by users  
             • Comes from innocent-looking sites  
             • First appeared when FAKEAV variants were still relatively unknown  
             • Is continuously updated up to now |
| Second     | • Is unknowingly installed on user systems  
             • Is more discreet in terms of installation  
             • Has no visual payloads |
| Third      | • Uses scareware tactics (e.g., fake blue-screen errors and desktop wallpapers) |
| Fourth     | • Purports to be a .DLL file in order to hide its malicious routines, making it harder to terminate |
| Fifth      | • Uses ransomware tactics such as encrypting files to force affected users to buy fake antivirus software  
             • Terminates .EXE files and warns users of file corruption  
             • Displays prompts to entice affected users to purchase a fake antivirus software in order to retrieve ransomed files |
| Sixth      | • Is script based  
             • Is hosted on sites related to specific search strings |
| Seventh    | • Modifies Layered Service Provider (LSP) to prevent affected systems’ Web browsers from accessing certain sites and to display fake security alert messages |
| Eighth     | • Is capable of registry shell spawning whenever .EXE files are executed  
             • Has autostart techniques  
             • Connects to a malicious domain and sends an HTTP GET request to inform a remote server of the infection  
             • Waits for the remote server to send “OK” as reply in order to execute malicious routines |
| Ninth      | • Creates random folders and registry entries  
             • Drops random files  
             • Blocks connections to certain sites  
             • Displays fake security warning pages  
             • Connects to several porn sites  
             • Prevents the execution of .EXE files |

*Table 1. Evolution of FAKEAV*
NOTABLE MALWARE BEHAVIORS

Utilizes Various Stealth Routines

FAKEAV variants use stealth mechanisms such as injecting their DLL or SYS rootkit components into legitimate processes (e.g., explorer.exe, winlogon.exe, etc.) or into their own running processes. These make them capable of hiding dropped files and/or their components from users or antivirus software, thus preventing deletion. Stealth routines also prevent their processes from being easily terminated as long as their DLL or SYS components remain injected into running processes.

Terminates Processes

More recent FAKEAV variants are capable of terminating processes in order to force users to purchase fake antivirus software. These display pop-up messages (see Figure 11) that inform the user that the .EXE file he/she is accessing has been infected and cannot run when, in reality, it has only been terminated by the malware.

Displays Pop-Up and Fake Warning Messages

The most obvious sign of FAKEAV infection is the continuous appearance of pop-ups and warning messages.

Another popular example is using Windows XP Security Center and other such icons though these are nonnative Microsoft Windows icons. In fact, these have been especially created for rogue antivirus applications.
Unmasking FAKEAV

Displays Warning Messages When Viewing Search Results

Some FAKEAV variants display warning messages in affected users’ Web browsers while viewing search results from engines like Google. Users should also keep in mind that the first search result, usually a fake YouTube link, is almost always malicious.

Users should keep in mind that the first search result, usually a fake YouTube link, is almost always malicious.
Drops Files

A few examples wherein FAKEAV utilized dropped files are:

- **Screensaver/Blue screen wallpaper.** Some FAKEAV variants drop .SCR files, some of which are detected as JOKE_BLUESCREEN. Such a screensaver displays a fake blue screen commonly seen when fatal errors such as hardware failure and the like occur.

  ![Figure 14. FAKEAV variant that displays a blue screen wallpaper](image)

- **Desktop wallpaper.** Another sign of FAKEAV infection is a sudden change in one’s desktop wallpaper. Such a wallpaper displays a warning that one’s system has been infected by a malware.
Some FAKEAV variants employ program installation prompts to infect systems.

**Displays Program Installation Prompts**

Modern FAKEAV variants act as legitimate antivirus applications and usually come with installers. They create a folder in the *Program Files* or the user’s *Application Data* directory. One should thus check these directories to confirm if their systems have been infected by FAKEAV. Sometimes, the downloaded programs may also try to mimic valid *Windows Update* message boxes.
The following are a few examples of rogue antivirus programs. Note, however, that this list is limited and that new names are generated every week:

- Antivirus Live
- Antivirus Pro 2010
- Antivirus XP Pro
- Antivirus Soft
- Desktop Defender 2010
- Internet Security 2010
- Malware Defense
- Personal Security
- Total Security
- Security Tool
- XP Guardian
- Virus Heal

**Redirects to FAKEAV Download Sites**

Infected PCs sometimes display pop-ups or are redirected to websites where rogue antivirus software is sold. Some users may think the FAKEAV can clean their PCs but should note that this is just a ploy to capture their credit card information. Do not purchase antivirus software from untrustworthy sources nor provide any personal or credit card information to untrustworthy sites.

![Sample FAKEAV download site](image)

*Figure 17. Sample FAKEAV download site that asks users to key in their credit card information*
Modifies the Layered Service Provider

By inserting itself into the Layered Service Provider (LSP) chain, a FAKEAV variant can load whenever an application uses WinSock. Note that applications that use Winsock are usually browsers. LSP technology is often exploited by malware, primarily to prevent Web browsers from accessing certain sites. In this case, a FAKEAV variant inserts itself into the LSP chain so that it can display fake security messages whenever a user tries to access a certain site.

Figure 18. A site that has been replaced by tweaking with the LSP

This FAKEAV variant thus has a tendency to cause more panic on users' part, as accessing any of the sites in the malware’s script will display a fake alert, making them believe that the site they are trying to access is indeed restricted.

Utilizes Registry Shell Spawning

This FAKEAV malware type adds and modifies several registry entries to ensure that it runs every time an .EXE file is executed. It modifies the following registry entry with the use of registry shell spawning:

```
HKEY_CLASSES_ROOT\exe
@ = "sexitfile"
```

Note that the default value for the said registry entry is "exefile."
It also adds the following registry entries in order to execute every time an .EXE file is executed via registry shell spawning:

```
HKEY_CURRENT_USER\Software\Classes\.exe
  @ = "secfile"

HKEY_CURRENT_USER\Software\Classes\.exe\shell\open\command
  @ = "\{malware path and filename\} /START "%1" %*"

HKEY_CURRENT_USER\Software\Classes\secfile\shell\open\command
  @ = "\{malware path and filename\} /START "%1" %*"

HKEY_CURRENT_USER\Software\Classes\secfile\shell\open\command
  IsolatedCommand = "%1" %*"

HKEY_CLASSES_ROOT\secfile\shell\open\command
  @ = "\{malware path and filename\} /START "%1" %*"

HKEY_CLASSES_ROOT\.exe\shell\open\command
  @ = "\{malware path and filename\} /START "%1" %*"
```

Figure 19 shows a snapshot of a system’s registry.

![Sample computer registry](image)
Unmasking FAKEAV

Blocks Access to Sites and Displays a Warning Page

When a user opens an Internet browser window and tries to visit any website (except certain porn and other sites the FAKEAV variant allows access to), he/she will see a fake warning message. This variant intercepts requests sent by the browser and redirects it instead to a proxy server on the local host. It then connects to its server and returns the data sent to the browser. The said data when displayed shows a fake warning message in order to trick users into purchasing FAKEAV software.

![Warning shown by FAKEAV variants that blocks access to sites](image)

Connects to Porn Sites

Some FAKEAV variants continuously trigger the opening of porn sites at certain time intervals while running in the affected systems’ memory. This annoying technique aims to pressure users of infected systems to purchase full versions of rogue antivirus applications.

![Sample porn site some FAKEAV variants access while running in an affected system's memory](image)

Some FAKEAV variants block access to sites and display a FAKEAV warning page while others connect to porn sites.
ONLINE AND LOCAL FAKEAV TYPES

More recent FAKEAV versions (as of November 2009) can be classified as either of two types—online or local. These new versions still exhibit the same old behaviors like displaying fake alert messages about false system infections, which requires users to purchase full versions of rogue antivirus software in order to remove the said threats.

Online FAKEAV Variants

Online FAKEAV variants refer to script files that are usually hosted on malicious sites and run whenever a user accesses the said sites. Part of their routine is displaying fake alert messages though their main purpose is to convince a user to download the main FAKEAV executable file onto his/her system.

Figure 22. Sample online FAKEAV variants
Local FAKEAV Variants

Local FAKEAV variants refer to executable files that can be downloaded off the Internet. These executable files are the main FAKEAV malware components that feature the old routines. They display fake alert messages then ask users to give out their credit card information to purchase full versions of the rogue product in order to fully remove the threats from their systems. Some of these .EXE files have payloads like changing a system’s wallpaper or screensaver and terminating processes.

![Sample warning message a local FAKEAV variant displays](image)

*Figure 23. Sample warning message a local FAKEAV variant displays*
PROTECTION AGAINST FAKEAV INFECTIONS

There are a myriad of ways by which users can protect their systems from any and all kinds of rogue antivirus threats that lurk in the Web today.

- **Practice safe browsing habits.** Avoid visiting suspicious-looking sites. Do not download and install software from untrustworthy sources.

- **Stay abreast of the latest threats and threat trends.** Familiarizing oneself with the current threat landscape is a great way to stay informed about the latest scams so as not to become victims of malicious attacks. The most popular malware today tend to prey on unsuspecting users. It is also worthwhile to familiarize oneself with the security solutions that are available in the market. Keeping in mind that any other software that presents itself as an antivirus program but has been installed without one's knowledge or the knowledge of the network administrator is most likely a rogue antivirus application is also critical. To know more about the latest threats and threat trends, read the latest posts by security experts in the *TrendLabs Malware Blog*.

- **Download and install the latest Microsoft patches.** Unpatched machines are more prone to malicious attacks, particularly zero-day vulnerability exploits. it is a good computing habit to regularly patch Windows-based PCs every “Patch Tuesday,” that is, the second Tuesday of each month when Microsoft releases security patches and updates for its OSs and other key software. Enabling the automatic Windows update feature is also recommended. Those who are still using legacy OSs should check if they have applied the latest roll-up patches. Several patch management utilities or vulnerability scanners exist that may already be implemented on the network can help identifying these.

- **Download and install the latest patches from third-party software vendors.** As there is no perfect software, applying the latest security patches can help ensure that the software installed on systems cannot be exploited for known vulnerabilities. Just make sure that the latest patches for the third-party software installed on a system still support the OS they run on.

- **Disable JavaScript in *Adobe Acrobat Reader*.** Some of the most-exploited vulnerabilities are related to the JavaScript function of *Adobe Acrobat Reader*. For better protection, disable JavaScript. To do this, click *Edit > Preferences > JavaScript* and uncheck *Enable Acrobat JavaScript.*
• **Install an effective anti-spam solution.** Spammed messages are the most common FAKEAV infection vectors. As such, installing an effective anti-spam solution will mitigate the risks FAKEAV programs pose.

To scan emails at the gateway level, enterprise users can download and install any of the following solutions:


Small and medium-sized business (SMB) users, on the other hand, can use the following applications:


To scan email messages at the mail server level, enterprise users can download and install any of the following solutions:


Users who do not have any anti-spam solution installed at the gateway or in the mail server can optionally install a standalone Trend Micro spam filter called the **Anti-Spam Toolbar for Outlook/Outlook Express** for free from [http://www.trendmicro.com/download/antispam.asp](http://www.trendmicro.com/download/antispam.asp).
• **Install a Web-filtering solution at the gateway.** Web threats are the most common sources of FAKEAV infection today. A few examples are:

  • Clicking a URL from an email that redirects a user to a malicious site
  • Simply browsing a compromised site
  • Being asked by a friend to click a link that leads to a malicious site in an instant message (IM)
  • Accidentally loading a software that automatically downloads malicious applications from the Internet

Trend Micro offers the following solutions to make Web browsing a lot safer. Any of these products provide multilayered protection at the Internet gateway in order to dynamically defend against Web-based attacks. Enterprise users can download and install the following solutions:

  
  


• **Install a desktop antivirus program.** Conventional antivirus programs do not totally protect desktops nowadays. Right now, detecting malicious software components is no longer enough. It is more efficient to block malware in multiple ways—by blocking the infection vector, the behavior, and the software components.


• **Install a threat discovery appliance.** One of the components of *Trend Micro Threat Management Services* is *Trend Micro™ Threat Discovery Appliance*, a next-generation network (NGN) monitoring device that uses a combination of intelligent rules, algorithms, and signatures to detect a variety of malware, including worms, Trojans, backdoor programs, viruses, spyware/grayware, adware, and other threats. The detection is done at layers 2–7 of the Open Systems Interconnection (OSI) Reference Model.

This appliance delivers high-performance throughput and availability and provides critical security information, alerts, and reports to IT administrators. *Trend Micro Control Manager* can help manage *Trend Micro™ Threat Discovery Appliance*.

*Trend Micro Threat Management Services* also offer more advanced service components utilizing the expertise of a threat management advisor and threat containment and remediation advisory services.


*Trend Micro Deep Security* protects confidential data and critical applications to help prevent data breaches and to ensure business continuity while enabling compliance with important standards and regulations such as *PCI, the Federal Information Security Management Act (FISMA)*, and the *Health Insurance Portability and Accountability Act (HIPAA)*. Whether implemented as software, virtual appliances, or as hybrid solutions, this application equips enterprises to identify suspicious activities and behaviors and to take proactive or preventive measures to ensure datacenter security.
RECOVERING FROM A FAKEAV INFECTION

After ridding one’s system of FAKEAV infections, the following steps may prove useful, too:

• **Run HouseCall.** *HouseCall* is Trend Micro’s highly popular and capable on-demand scanner for identifying and removing viruses, Trojans, worms, unwanted browser plug-ins, and other malware. To download this software, visit [http://housecall.trendmicro.com/](http://housecall.trendmicro.com/).

• **Run the System Information Collector (SIC) tool.** For clients who suspect that their systems have been compromised, it is advisable to run the SIC tool available for free at [http://www.trendmicro.com/download/sic.asp](http://www.trendmicro.com/download/sic.asp) then submit the SIC log to Trend Micro for analysis.

• **Restoring the LSP.** For clients who remain unable to access the Internet after suffering from a FAKEAV infection, follow these steps to restore access to the Internet by resetting the LSP to its default configuration:

  1. Open a command prompt window. Click *Start > Run*, type *CMD*, then press *Enter*.
  2. In the command prompt window, type “netsh Winsock reset.”
  3. Press *Enter*. A message should indicate that the service has been successfully stopped.
  4. Close the command prompt window.
  5. Restart your computer for the changes to take effect.
CONCLUSION

Cybercriminals are motivated by only one thing, that is, to profit from their malicious schemes. As such, they will continue to use different social engineering techniques to lure users into their well-devised traps.

As more users fall into cybercriminals' traps, the greater they will profit and their malware businesses will continue to thrive. Education is still a key factor to combat the threats FAKEAV applications pose. User awareness will go a long way to ensure safe computing.

Trend Micro is committed to combating the threats that FAKEAV and other malware variants pose with the help of the Trend Micro™ Smart Protection Network™, an infrastructure that delivers security, which is smarter than conventional approaches. Leveraged across Trend Micro’s solutions and services, Smart Protection Network combines unique in-the-cloud reputation technologies with patent-pending threat correlation technology to immediately and automatically protect your information wherever you connect.
REFERENCES


Unmasking FAKEAV

