Security Spotlight articles discuss recent noteworthy threats that users may encounter and should be aware of while surfing the Web.

WHY FAKEAV PERSIST

Written by: Erika Mendoza, Jasper Manuel, and Roland Dela Paz

Abridged by: Ria Boquiron

Rogue antivirus aka FAKEAV remains one of the most notorious and pervasive malware threats today. In the white paper, "Unmasking FAKEAV," TrendLabs researchers delved deeper into FAKEAV technology and presented data on how the malware arrives on systems. To better understand why FAKEAV works and why it persists, a closer look at its various infection vectors and the technology behind it is necessary.

Social Engineering: Keeping FAKEAV Alive

In a span of just one year, Trend Micro has added approximately 2,500 detection names for new FAKEAV variants and 1,600 new FAKEAV downloader variants to its ever-growing list. One of the primary reasons for FAKEAV's persistence is its use of social engineering techniques to proliferate.

Rogue antivirus aka FAKEAV remains one of the most notorious and pervasive malware threats today.

Figure 1. *Typical FAKEAV infection diagram*

TREND MICRO

Blackhat SEO

Cybercriminals employ various social engineering techniques to carry out their malicious schemes. At present, blackhat search engine optimization (SEO) or the use of various techniques to increase the page ranking of malicious sites is proving to be an effective social engineering tactic. FAKEAV malware often ride on the popularity of hot topics in search engines like *Google, Yahoo!,* or *Bing*. As such, unwitting users searching for information encounter malicious links mixed with those leading to legitimate sites.

Blackhat SEO, spamming in social networking sites, and malvertising are just some of the social engineering techniques that cybercriminals commonly employ to distribute FAKEAV malware.

Spamming in Social Networking Sites

The rise of social networking sites did not go unnoticed in the cybercrime business. In initial runs, cybercriminals utilized the KOOBFACE worm to post malicious links that led to the download of a FAKEAV variant detected as TROJ_FAKEAV.DAP. More recently, some FAKEAV variants come disguised as *Facebook* applications.

In such an attack, a notification email or a direct message containing a malicious link arrives or appears. Allowing this *Facebook* application to execute will display a warning message indicating system infection and urging users to download and install a rogue antivirus software.

Malvertising

Cybercriminals also use malicious advertisements aka malvertisements to propagate FAKEAV malware via malicious links such as that which leads to a TROJ_FAKEAV.DMZ download page. Since the malicious link comes in the guise of an ad, it is posted at the top of the search results page. Its strategic location can thus lead users to click the malvertisement instead of a legitimate search result.

Looking Beyond the Surface: The Technology Behind FAKEAV

FAKEAV malware are designed to fool users into thinking that they are legitimate antivirus applications. They pretend to do what typical antivirus software do—scan systems, display warning messages, and perform signature updates. Users may only realize that something is amiss once the supposed antivirus software begins displaying persistent warning messages and reminders urging them to purchase a full version.

These visible behaviors act as FAKEAV markers that enable users and security experts to spot the malware variants when encountered in the wild. Beneath the surface, however, lies the mechanism that enables cybercriminals to repeatedly profit from FAKEAV malware.

Interestingly, FAKEAV programs do not employ particularly unique or complicated codes. In fact, these use a simple algorithm to carry out their malicious routines. If solely based on the FAKEAV process dump, it can be said that most variants are built using embedded scripts. In this regard, the executable file acts as a script interpreter of the embedded scripts.

Routines are activated by creating threads that are triggered by events. These threads are called in sequential order. This means that after one thread has finished executing, it will send a signal to the next thread, which contains the next routine that should be executed. This is continuously done in a loop, which may then lead annoyed users to purchase a full copy of the FAKEAV program.

The threads created contain the code for already-familiar routines such as scanning systems, preventing applications from executing, displaying warning messages, and connecting to adult sites.

Scanning Systems

FAKEAV malware are designed to fool users into thinking that they are legitimate antivirus applications. As such, they usually pretend to scan systems, prevent certain applications from executing, display warning messages, and connect to adult sites.

One of the most notable features of FAKEAV malware is their use of a convincing graphical user interface (GUI). Like other antivirus applications, these malware also utilize a GUI that shows users what the software has supposedly identified on a system.

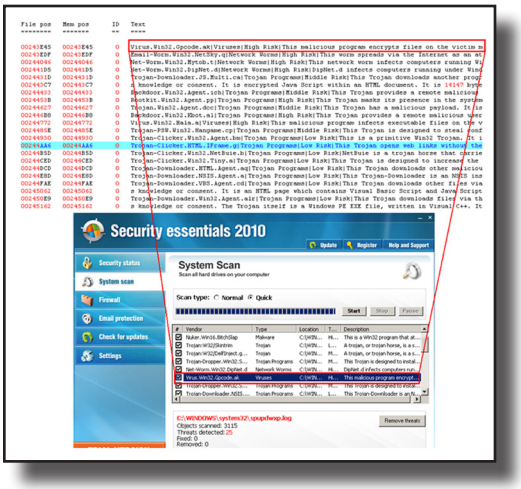

Figure 2. *Fake infection hard-coded into the FAKEAV malware's body*

Looking at the FAKEAV GUI, users may be led to believe that the software is actually scanning a system. A quick look at its memory dump, however, reveals that the software does not even have a malware database or a pattern file to update. The detection names, malware descriptions, and even the malware file sizes are merely hard-coded into the malware body.

Some FAKEAV variants such as TROJ_FAKEAV.BUH and TROJ_FAKEAV.BPE also have the ability to detect and delete known malware by executing embedded scripts. The said technique is merely another ruse to fool users into thinking that they are legitimate antivirus software.

Preventing Applications from Executing

Apart from using a typical FAKEAV GUI, some variants also prevent certain applications from executing. These typically display a message informing users that a file has been infected and thus cannot execute. In reality, however, the malware themselves terminate the application being executed, obtain its file name, and display a pop-up warning.

A common technique of doing this is using *Windows Management Instrumentation (WMI)* to monitor new processes. As a result, the system becomes virtually useless, leaving the user no choice but to purchase the rogue antivirus software.

TREND MICRO

Displaying Warning Messages

Another FAKEAV routine designed to persuade users to purchase a rogue antivirus product involves intercepting their Internet connection and replacing it with a warning message instead. The FAKEAV malware creates a completion port that acts as a proxy server on the local machine.

Furthermore, these variants create registry entries to ensure that requests from the Internet browser are intercepted. Once an Internet browser is launched, the request is redirected to the local proxy server, contacts to its own server, and returns the reply from the server to the Internet browser.

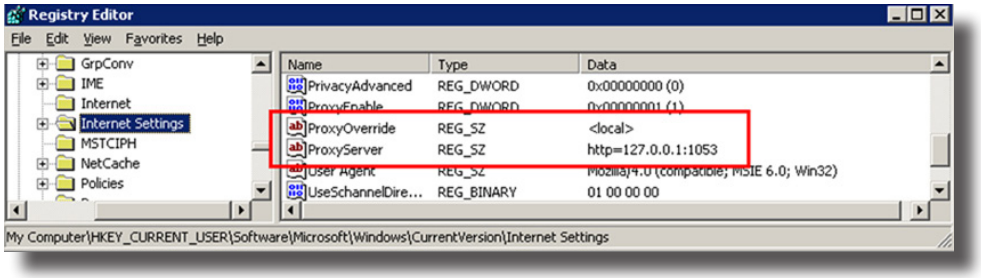

Figure 3. *Registry entries some FAKEAV variants create to ensure that Internet browser requests are intercepted*

Behind the various schemes cybercriminals employ to distribute FAKEAV malware is a single goal—information theft.

Connecting to Adult Sites

In addition to repeated warnings about nonexistent threats, some FAKEAV malware also launch an instance of *Internet Explorer (IE)* that connects to certain porn sites. Examples of FAKEAV variants that use this routine include TROJ_FAKEAV.TAD, TROJ_FAKEAV.BPE, and TROJ_FRAUDPAC.LI. This can be problematic in some countries where pornographic materials may lead people to face legal issues.

This behavior is continuously triggered at certain time intervals as long as the FAKEAV malware runs in a system's memory. Since this recurs in a loop, users who leave their systems unattended for several minutes may find their screens filled with browser windows opened to porn sites upon their return. The said scenario may consequently lead users to pay for the bogus software with their hard-earned cash just to resolve the problem.

The FAKEAV Business

Behind the various schemes cybercriminals employ is a single goal—information theft. Apart from taking away about US$40–100 from a user's account as payment for rogue software, what is even more dangerous is the fact that a victim is literally handing over his/her credit card details and other personal information to cybercriminals. Once a user fills in the form to activate a rogue antivirus software, the information he/she provides is sent via HTTP POST to a remote server.

As discussed in the Trend Micro white paper, "The Business of Cybercrime: A Complex Business Model," FAKEAV malware play an important part in the complex botnet business model. The intertwined relationship among some of the biggest threats today proves that cybercrime is, first and foremost, a business.

Stay Informed, Stay Protected

With Trojans like FAKEAV variants, our best weapons are awareness and presence of mind.

As blackhat SEO is the main FAKEAV proliferation technique, it is best to watch out for suspicious links while browsing the Internet. Seeing warning messages or fake system scan results in browsers, however, does not indicate system infection. Take note that FAKEAV malware are usually manually installed as a result of various scareware tactics. Once panic prevails and users run the malicious application, that is the only time that their systems become infected. With Trojans like FAKEAV variants, our best weapons are awareness and presence of mind.

Users should also look out for malicious spammed messages though these may not be widely used anymore. Just like other malware, FAKEAV variants may also come disguised as harmless applications attached to email messages. Users should thus avoid executing attachments, especially if the messages come from unknown senders.

Below are other helpful tips to keep one's system safe.

- Enable the firewall to protect one's system from Web threats.
- Do not trust the top results on a search page. It is still best to go directly to news sites to avoid clicking malicious links.
- Ensure that programs and users of the computer have the lowest level of privileges necessary to complete a task.
- When a system has been compromised, immediately isolate it from the network.
- Always keep patches up-to-date.
- Avoid visiting unknown sites that may redirect to malicious sites or lead to the download of FAKEAV malware.

Finally, always keep an antivirus product's signature files updated. This helps identify and terminate malicious files, including new FAKEAV variants.

References:

- Trend Micro Incorporated. (April 15, 2010). *Threat Encyclopedia.* "TROJ_FAKEAV.TAD." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEAV.TAD (Retrieved August 2010).
- Trend Micro Incorporated. (April 10, 2010). *Threat Encyclopedia.* "TROJ_FAKEAV.BUH." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEAV.BUH (Retrieved August 2010).

TREND MICRO

- Trend Micro Incorporated. (April 2010). *Threat Encyclopedia.* "TROJ_FRAUDPAC.LI." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FRAUDPAC.LI (Retrieved August 2010).
- Trend Micro Incorporated. (March 11, 2010). *Threat Encyclopedia.* "TROJ_FAKEAV. BPE." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEAV.BPE (Retrieved August 2010).
- Trend Micro Incorporated. (March 2010). *TrendWatch.* "The Business of Cybercrime: A Complex Business Model." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/wp04_cybercrime_1003017us.pdf (Retrieved August 2010).
- Trend Micro Incorporated. (September 22, 2009). *Threat Encyclopedia.* "TROJ_ FAKEAV.DMZ." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEAV.DMZ (Retrieved August 2010).
- Trend Micro Incorporated. (July 27, 2009). *Threat Encyclopedia.* "TROJ_FAKEAV.DAP." http://threatinfo.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ_FAKEAV.DAP (Retrieved August 2010).
- Trend Micro Incorporated. (June 2010). *TrendWatch.* "Unmasking FAKEAV." http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/unmasking_fakeav__june_2010_.pdf (Retrieved August 2010).

TREND MICRO