

Yet Another Big Week for FAKEAV

During the past week, Trend Micro researchers detected another spike in attacks resulting in FAKEAV. This scam, where users are tricked into buying non-functional AntiVirus software to deal with a fictitious infection, is still proving successful, and cyber criminals are becoming more innovative about how they push FAKEAV to unwitting users.

Today, there seems to be no end to the proliferation of FAKEAV. So far, The Trend Micro Threat Encyclopedia has over 2,000 related entries. According to Paul Ferguson, a Trend Micro Threat Researcher, hundreds of new FAKEAV domains appear every day.

Cyber criminal are becoming more innovative about how they push FAKEAV

Techniques Advancing Fast

In order to reach their victims, Cyber criminal are now poisoning search engine results of the latest and most popular search terms. They also use customized spammed messages containing malicious URLs or file attachments. And recently, FAKEAVs have even made their way onto iPhones.

FAKEAV Is Only the Beginning

Not only are infected users in danger of potentially being scammed by FAKEAV perpetrators, they could also become a direct participant in the perpetration of fraudulent activities and cyber crimes as part of a botnet. This is because FAKEAV peddlers now out source their propagation to botnets with already-installed bases.

Not only has this move allowed the cyber criminal behind FAKEAV to concentrate on devising new scare tactics and pay-per-install models, it has also paved the way for the creation of affiliations with KOOBFACE and BREDOLAB botnet groups. You can find more information about these affiliate programs in the following papers:

- “You Scratch My Back... BREDOLAB’s Sudden Rise in Prominence”
- “Show Me the Money! The Monetization of KOOBFACE”

How to Stay One Step Ahead of FAKEAV

As FAKEAV variants can now be seen everywhere and be delivered in a multitude of ways, it pays to be aware and observe the following precautions to avoid infection.

- Rely only on trusted sites for the latest news updates.
- Avoid clicking suspicious-looking URLs and downloading and opening file attachments, especially from people you do not know.
- Use a reputable security program that protects you wherever you connect. Programs that incorporate technology like the Trend Micro™ Smart Protection Network™ protects you against FAKEAV-related infections by blocking spammed messages with email reputation technology, prevents access to malicious sites and domains with web reputation technology, and detects and deletes malicious files with file reputation technology.
- iPhone users can protect themselves free with Trend Micro Smart Surfing for iPhone.