

Web Threat Spotlight

A Web threat is any threat that uses the Internet to facilitate cybercrime.

MARCH 30, 2009
ISSUE NO. 34

Fake Antivirus Scammers Now into Ransom

A new wave of rogue antivirus software has routines that allow cybercriminals to disable infected users from using their valuable files. This new threat, clearly an innovation from earlier rogue antivirus attacks and variants, features a cybercriminal operation that borrows from a real-world extortion technique adapted for the online world for the same old purpose of stealing precious money from users.

The Threat Defined

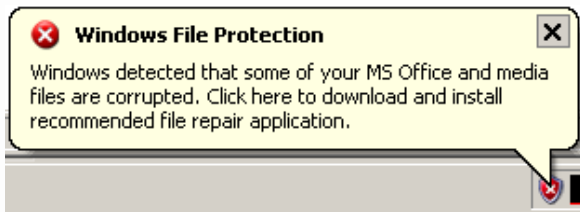


Figure 1. Fake error message says the user's files are corrupted.

Rogue antivirus programs have been plaguing unfortunate victims for years. These unwanted software programs arrive via the Web and are unwittingly installed onto computers via various social engineering techniques. Once installed, these programs display different infection signals meant to scare users into thinking something is wrong with their computer. These infection signals include error messages, dialogue boxes, even fake “blue screens of death” or blue-colored wallpapers that alarm users about the infection. The same

rogue antivirus programs offer to scan the system or to rid the system of the “infection.” However, the user has to first pay for the “full version” of the product.

In March of 2009, researchers discovered a new generation of malicious software that improves on these notorious rogue antivirus routines by adding a ransomware component to the attack. Cybercriminals have used ransomware in the past in another online extortion scheme: encrypting files on an infected PC and asking for payment for the decrypter. Ransomware can lock, encrypt or scramble files—in effect, holding them hostage—so that users are no longer able to access them. These malware typically include a routine to notify the user that if he or she wants to regain access to the files, payment should be made to the cybercriminal who will then provide the decrypter key.

Trend Micro detects the malware in this rogue antivirus-ransomware attack as [TROJ_FAKEALE.BG](#). Analysis by our engineers reveals that this threat has two distinct tracks, both ensuring that users are not only fooled but are victimized as well by an information-for-ransom operation.

The Trojan arrives through the Web, which is a common rogue antivirus infection vector. It has two components, a .DLL file and an .EXE file, which both play a role in the scam.

Ransomware Routine

The .DLL encrypts the following file types in a user's *My Documents* folder: DOC, DOCM, DOCX, DOTM, DOTX, JPEG, JPG, MDB, MP3, PDF, PNG, POTM, POTX, PPAM, PPSM, PPSX, PPT, PPTM, PPTX, PST, WMA, XLAM, XLS, XLSB, XLSM, XLSX, XLTM, and XLTX. These extensions are formats of common files—documents, images, music, slide presentations, spreadsheets—which for most users are not only valuable but have immediate use as well. When these files are encrypted, a user can no longer access them using the related applications.

Rogue Antivirus Routine

The .EXE component continues the show. After the .DLL performs the encryption, it displays a message box telling users that the files they are trying to open are corrupted. It also displays a message when a user tries to access the encrypted files. An error message may also appear at the task bar suggesting the same (*Figure 1*). A repair option is provided in the message boxes, but once users click this button, they are redirected to a website hosting software called *FileFix Professional 2009*.

As the name suggests, FileFix supposedly fixes the problem of the corrupted files, allowing infected users to open their files again. What the program does, in fact, is to decrypt only one file. To fix the entire problem users are told they must download the paid version of FileFix. This makes the software dubiously useful because it only fixes what it has also encrypted for the amount of [\\$50](#).



Web Threat Spotlight

A Web threat is any threat that uses the Internet to facilitate cybercrime.

FILEFIX PROFESSIONAL SCAM



Upon further analysis, our researchers observed that some of the domains where this rogue antivirus is hosted have been involved in click-fraud and other pay-per-click schemes that Trend Micro tracked in 2007. The same domains are also hosting recent variants related to the Storm/Waledac botnet. While the malicious domains suggest that the cybercriminals behind this attack have been in the business of fraud for quite some time, the rogue

antivirus-ransomware development poses a whole new frontier of risk to online users. People don't give a second thought to storing documents, images, and music files inside their computers, which may be anything from personal mementos to mission-critical business files. The idea of not being able to access these files could be enough for users to agree to hand over money to cybercriminals.

User Risks and Exposure

Rogue antivirus software exploits an already established mindset among net users that security threats are out there lurking the Web. Earlier variants are notable for tricking unknowing users into paying for empty software that do not accomplish anything except aid in the scam. This attack brings the level of risk a notch higher: not only is the computer's security at risk but so are the files contained therein. Users who encounter this threat lose money when they pay cybercriminals for the decrypter and set themselves up for further losses. In addition to enjoying the up-front profit, cybercriminals can store the entered credentials and payment information for their own use or to sell them in underground forums.

Trend Micro Solutions and Recommendations

The Trend Micro Smart Protection Network delivers security that is smarter than conventional approaches. It blocks the latest threats before they reach you. Leveraged across Trend Micro's solutions and services, Smart Protection Network combines unique in-the-cloud technologies and lightweight client architecture to immediately and automatically protect your information wherever you connect. It is also the only antivirus technology that is able to correlate threats and identify their roles in an entire threat.

In this case Smart Protection Network protects users through Web Reputation technology, which identifies known malicious or dangerous Web sites and blocks users' access based on domain reputation ratings. At the desktop level File Reputation technology assesses the integrity of all files downloaded unknowingly onto computers, detecting and removing TROJ_FAKEALE.BG and other dangerous rogue antivirus components.

Users who are already affected by this threat may download the Trend Micro fixtool to recover the encrypted files from the following link: <http://www.trendmicro.com/ftp/products/pattern/spyware/fixtool/MFileDecryptor.zip>

The following post at the Trend Micro Malware blog discusses this threat: <http://blog.trendmicro.com/data-for-ransom-syndicates-strike-online/>

The virus report is found here: <http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=TROJ%5FFAKEALE%2EBG&Vsect=Sn>

