Falling for the Fake (Part I)

By | Khairun 'Amira binti Khazali

Introduction

It is vital that all computers are installed with an anti-virus program whether it is used for professional or personal purposes. As users begin to understand the need of anti-virus software, cybercriminals found out ways they can profit out of this by distributing what is known as rogue security software. The rogue security software issue has long been a threat on the internet. It is a computer malware which pretends to provide security benefits; however, with intentions to lure users to involve in malicious activities. Distributors of rogue security software are always thinking of new ways to make users easily fooled with the fake product and service they provide. However, fear and anxiety had always been used to convince users in purchasing the rogue security software.

According to a report from Symantec, 43 million installation attempts from over 250 distinct programmes were found from July 2008 to June 2009 (Symantec, 2009). Rogue security software distributors are earning big from this business they do with charging a price of around $30 to $100 for a product. It also stated in the report that of the top 50 rogue security software scams, 93 percent was intentionally downloaded by the users themselves. This proves that the tactics used is able to effectively manipulate users to install the rogue security software.

This paper will be divided into two parts where the first part will discuss the various methods used by rogue security software distributors to trick users. The second part of this article will explain three different case studies on various forms of attacks. Ways to prevent and remove the rogue security software will also be discussed.

The Rogue Operation

The rouge security software can be installed on a user's system by either the act of the user manually downloading and installing the software which they believe is legitimate or by visiting a malicious website which automatically downloads and installs such software in the case of a drive-by-download exploitation. Figure 1 illustrates the procedures most rogue security software use to infect a computer. Each stage is described as follow.

Figure 1 *General overview of how the rogue security software infects a system*

Internet Browsing: The rogue security software may be encountered in many different situations such as while reading e-mails, interacting through social networking sites, or searching for information. While browsing through the internet, users might click on links or advertisements which redirect them to a malicious website.

Alert Message: When a user is redirected to a malicious website, the user will most likely come across legitimate looking pop-up windows which are actually alert messages notifying the user of a fake infection on their system. Figure 2 is an example of an alert message used to mislead users in believing that their computer is infected with malware.

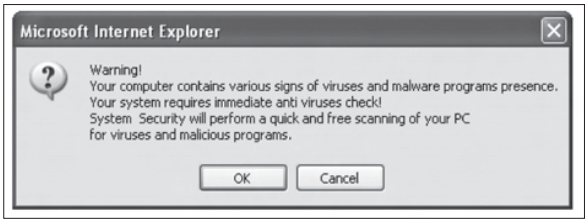

Figure 2 *Alert message of virus infection*

Computer Scan: Alert messages that appear will most likely suggest that a full computer scan is performed. If the user agrees to conduct the computer scan, a window will then appear conducting a fake computer scan.

Installation: Once the result of the scan is displayed, a message appears suggesting that the user installs a malware removal product which can be used to remove the malware detected on the user's computer. If the user agrees to install the software, they will have to first download the file to their computer. Once the user agrees on the installation, the rogue security software will be installed on their computer causing their system to be infected.

However, this is not the only way rogue security software can be installed on a user's computer. In search of an anti-virus product to use especially for free or trial version, users might come across websites of the rogue software which advertises a fake anti-virus product. Easily being tricked by how legitimate and professional the sites look, users would most likely download a trial version and end up getting their computer infected. Figure 3 displays the website of two rogue security software known as Virus Protector and AdwareALERT.

Figure 3 *Rogue security software website*

Attack Methods

Mentioned earlier, the tactic used to convince users is focused on fear. However, there are also other ways that have also proven to be effective. This section will describe the various tactics used to draw victims in installing the rogue security software.

Scareware

Early distribution of the rogue security software lured victims by fear; thus, making it famously known as scareware. Continuous pop-up displays and alert messages are used to convey warning of virus infections to frighten

users. What the users are not aware of is that the pop-up is just a fake message or a screensaver used to trick them in installing the rogue security software. Figure 4 shows a fake alert message used to notify the user that their computer is infected with viruses.

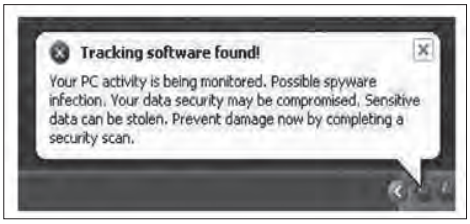

Figure 4 *Fake alert notification of virus infection*

Drive-by Download

Another tactic is known as drive-by download which allows a programme to automatically download itself to a computer without the user's consent or knowledge due to vulnerabilities of any application on a user's computer. This may occur when a user is visiting a website or viewing e-mail messages. The download of the malware can be done through exploitation of vulnerabilities on a web browser, e-mail client, or operating system which can be put on legitimate websites.

Fake Anti-virus

In the efforts to trick users, the rouge security software uses names which appear as realistic as possible or a name which is similar to well-known legitimate software. As a matter of fact, distributors of this software have gone to more rigorous extents in making it as realistic as possible by creating a website providing the ability to download and purchase the software and even sending e-mails to the victims with a receipt of their purchase. Other than that, users are also easily fooled by how the rouge security software is cleverly designed to mimic legitimate anti-virus software by using the same fonts, colors, and layouts. Figure 5 illustrates a comparison of the interface of a rogue security software known as Antivir with the legitimate anti-virus software, AVG.

Figure 5 *Interface of Antivir, a rogue security software and AVG*

A more advanced feature found in Live PC Care; another fake anti-virus, is a live online support. The Live!Chat feature allows victims to chat online with support agents for enquiries regarding the fake anti-virus product.

Social Engineering

Rogue security software is also distributed by using social engineering techniques. Social engineering can be carried out through e-mails, social networking sites, and search engine results.

Spam E-mail

Spam e-mails may contain links which directs the user to the rogue security software website. The content in the e-mails tries to trick users using various tactics like informing of newly available software updates or providing video links of famous celebrities. The e-mails might also contain an executable file that if opened will install the rogue software on the user's computer.

Social Networking Sites

In social networking sites, fake accounts can be created to impose as a user's friend. This allows messages to be sent with links that redirects users to a malicious website. A famous malware which implements this technique is called Koobface. This malware is capable of automating Internet Explorer to perform the task of creating and registering an account thus mimicking the process of a user. People are also enticed to click on a misspelled link to a video or picture which will then direct them to the website of the rogue security software.

Search Engine Results

Rogue security software distributors' other efforts is to make their websites more relevant to search engine results. A technique known as Search Engine Optimization (SEO) is used to increase traffic directed to a website by utilising the algorithms and functions used by popular web search engines. SEO puts focus on the way websites are developed especially in the usage of keywords. A keyword research is done to know what keywords are frequently used when users search for information. Another technique practiced in SEO is to build websites in a way which enables search engines to read as much of the content as possible and to rate it highly in relation to the selected keywords. Excessive repetition of highly ranked keywords in the website can also increase the rank of the website in search engine results. Being on top of search results increases the user's confidence to click on the links as it is found that most users usually click on the first three listings of search results.

Ransomware

To keep up with business, distributors of rogue security software have advanced to a more extreme technique which makes the user's files inaccessible. This is done by encrypting the files and in order for the user to recover the files, they will need to purchase the software or the key to decrypt the file. A term used for rogue security software which practices this tactic is ransomware.

Conclusion

Even though there are many types of methods used by cybercriminals to distribute the rogue security software, it has always revolved around the element of fear. For better understanding, three case studies will be presented and explained in the next e-Security bulletin release (Volume 25). ■

References

1. *Caraig, D. (2009). Rogue AV scams result in US$150M in losses. Retrieved from http://www.krypter.no/internasjonale-nyheter/1922.html*
2. *Coogan, P. (2010). Fake AV and talking with the enemy. Retrieved from http://www.symantec.com/connect/blogs/fake-av-talking-enemy*
3. *Microsoft. (2010). Watch out for fake virus alerts. Retrieved from http://www.microsoft.com/security/antivirus/rogue.aspx*
4. *Symantec. (2009). Symantec report on rogue security software July 08 – June 09. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-symc_report_on_rogue_security_software_WP_20100385.en-us.pdf*