

Rogue Security Software in 2008

By Ryan Sherstobitoff and Sean-Paul Correll



Rogue security software are designed to prey on Web users, scaring them into believing that their computers are infected with malware and ultimately extorting cash and sensitive data from them.

There are many infection vectors, but the most common are fraudulent video websites, spam, and major online search engines displaying the malicious sites. In certain cases, top search results have been found to point to compromised websites hosting or redirecting the user to rogue anti-malware sites.¹ The rogue creators also utilize SEO poisoning/injection and optimization techniques to increase organic search rankings and compromise legitimate websites.² The tainted search result will appear to be



valid and show content relevant to the search, in this case often relating to antivirus software, which will in turn start to infect the computer. A pop-up will appear on the user's screen saying the computer is infected and that a scan should be run to clean the infection.

The page providing the pop-up, however, has been written in such a way that it is difficult to stop the process at this point because it will only bring more pop-ups until the user in frustration proceeds with the "scan." The user is then taken to a website that appears to be selling an anti-malware software product. A scan page will load and it will appear as if the scan found viruses on the computer. These fraudulent scans will simulate a genuine scan and removal protocol and provide access to the software needed to remove it. The download will automati-

cally start; since the user is concerned about being infected, he will typically allow the download.

Once executed, the malware starts downloading all needed files from different servers that are operated by the malware creators. The rogue program starts running and immediately scans the computer again. As before, malware is found on the system and in order to remove the infection users must purchase the software. Approximately 3% of "infected" users willfully hands over financial information along with the \$49-\$69. Most payment gateways are hosted in a country without legislative conse-

quences for this fraud, and most – if not all – of the stolen financial information ends up on the black markets for sale.

Affiliates

Affiliate systems such as Pandora or Bakasoftware allow individuals to sell rogue software at high commissions. Affiliate systems are of a malicious nature, though some will maintain a legitimate front in order stay under the radar.

These cash-fueled affiliate programs lead to the wide scale-proliferation of rogue security software. During 2008 the labs observed rogue anti-malware delivered using the following methods:³

- Botnet-controlled spam campaigns
- Exploited vulnerabilities via drive-by download
- Social engineered news, video, and software websites

- Ad network and search engine hijacking

Many of the rogue sites were hosted by a few service providers in the U.S. with McColo and Atrivo/InterCage being the largest,⁴ McColo hosting at least 75% of the world's spam and botnet C&C infrastructures.⁵

The ISP community got involved. In the Aug./Sept. timeframe, Atrivo's upstream providers shut them down. McColo's last upstream provider cut them off in November, leaving hundreds of thousands of botnet-controlled computers without a central C&C server to receive commands from.

The steep increase in December (see chart) is due to the rogue providers attempting to recoup the revenue loss endured during the takedown period. Rogues will continue to be one of the most prevalent threats in 2009.

About the Authors

Ryan Sherstobitoff is vice president PR and promotion - USA market for Panda Security USA. He can be reached at ryans@us.pandasecurity.com or through the PandaLabs blog at <http://pandalabs.pandasecurity.com>.

Sean-Paul Correll is a security researcher and evangelist for Panda Security, specializing in malware surveillance and emerging threat discovery. He can be contacted at Sean-Paul.Correll@us.pandasecurity.com or at <http://www.twitter.com/lithium>.



1 <http://malwaredatabase.net/blog/index.php/2008/08/05/sponsored-result-does-not-equal-safe>.

2 <http://ddanchev.blogspot.com/2008/03/massive-frame-seo-poisoning-attack.html>.

3 http://www.pandasecurity.com/img/enc/Boletines/%20PandaLabs3_en.pdf.

4 <http://hostexploit.com/downloads/Hostexploit%20Cyber%20Crime%20USA%20v%202.0%201108.pdf>.

5 http://voices.washingtonpost.com/securityfix/2008/11/the_badness_that_was_mccolo.html.