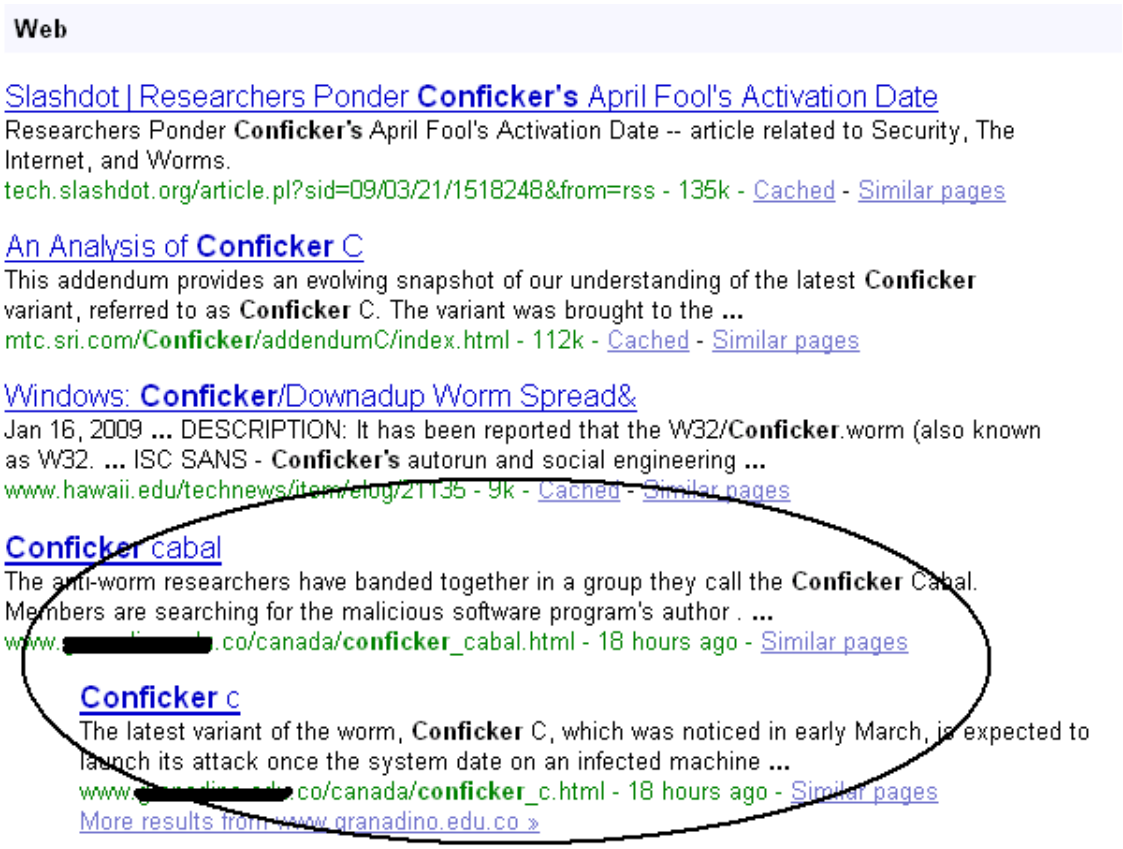
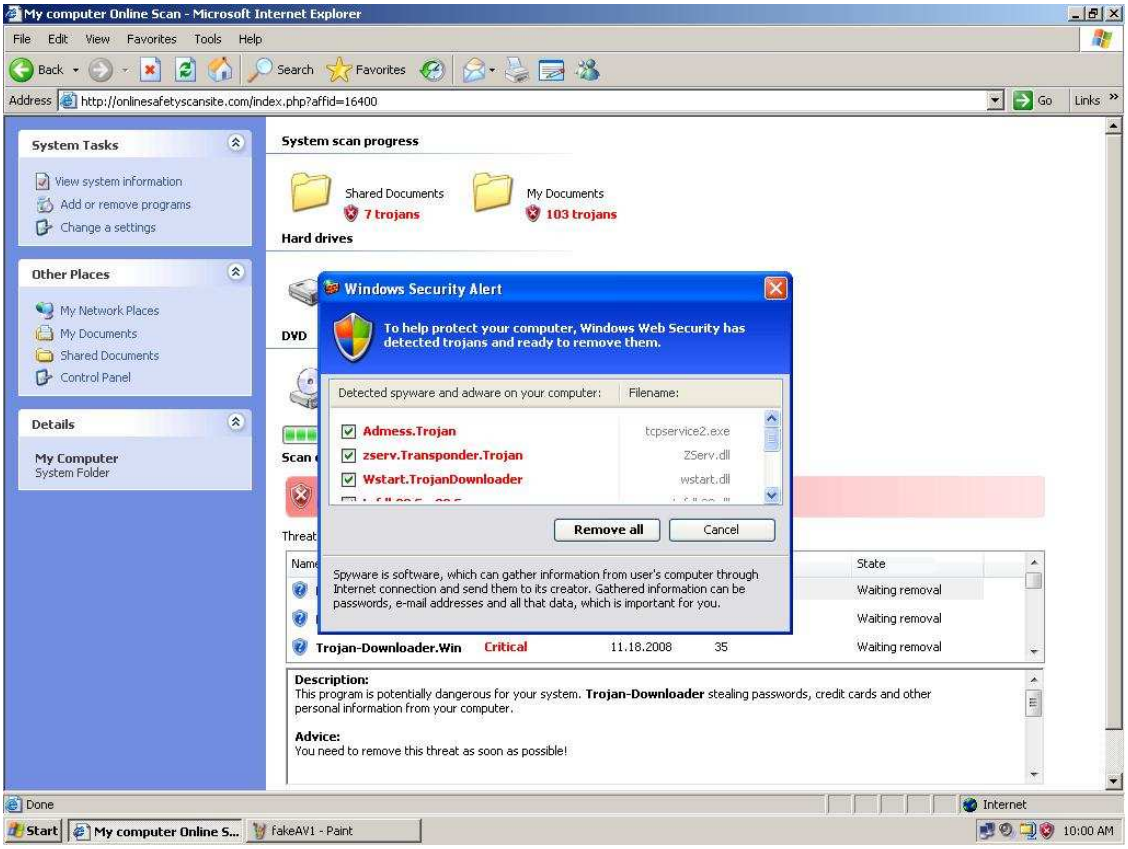
Downadup-Related Search Indexes Poisoned with Fake AV Sites

With Downadup/Conficker rising to celebrity status in the computer worm world, Symantec (along with other companies in the security industry) is hard at work, keeping our customers protected. But guess who else is hard at work at the moment? Yes, the authors of misleading applications. It isn't the first time that they have latched onto popular news to fuel their malicious intent using search engine optimization (SEO).

Let's say you are curious about Conficker, or you think your computer might be infected with Conficker. By simply searching for "Conficker C," page one of the results includes a link to an infected site being used to spread a fake antivirus program:



Following the malicious link eventually leads you to a rogue application installation website, as shown below (Note that this is not a screenshot of Windows Explorer, but is simply a picture inside the Web browser):



Symantec products that include network protection will trigger a signature named “HTTP Fake Scan Webpage” and block your computer from being able to visit this site. If you do somehow manage to get to the rogue application’s installer at the end of the tunnel, the file will be detected (and blocked) as Downloader.Misleadapp.

A few days ago, we blogged about the possibility of Downadup using misleading applications as its payload. Even though we do not think the author of this rogue application is related to the author of Conficker, this incident shows us that the authors and affiliates of misleading applications don't want to miss a single opportunity to capitalize on established media attention.

Some obvious words of advice: Be careful with the links you follow. A sincere effort of keeping abreast with the latest security information might contain some unwelcome surprises.