

## 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:

### Web

#### [Slashdot | Researchers Ponder \*\*Conficker's\*\* April Fool's Activation Date](#)

Researchers Ponder **Conficker's** April Fool's Activation Date -- article related to Security, The Internet, and Worms.

[tech.slashdot.org/article.pl?sid=09/03/21/1518248&from=rss](#) - 135k - [Cached](#) - [Similar pages](#)

#### [An Analysis of \*\*Conficker C\*\*](#)

This addendum provides an evolving snapshot of our understanding of the latest **Conficker** variant, referred to as **Conficker C**. The variant was brought to the ...

[mtc.sri.com/Conficker/addendumC/index.html](#) - 112k - [Cached](#) - [Similar pages](#)

#### [Windows: \*\*Conficker\*\*/Downadup Worm Spread&](#)

Jan 16, 2009 ... DESCRIPTION: It has been reported that the W32/**Conficker**.worm (also known as W32. ... ISC SANS - **Conficker's** autorun and social engineering ...

[www.hawaii.edu/technews/item/story/21135](#) - 9k - [Cached](#) - [Similar pages](#)

#### [Conficker cabal](#)

The anti-worm researchers have banded together in a group they call the **Conficker** Cabal. Members are searching for the malicious software program's author . ...

[www.granadino.edu/co/canada/conficker\\_cabal.html](#) - 18 hours ago - [Similar pages](#)

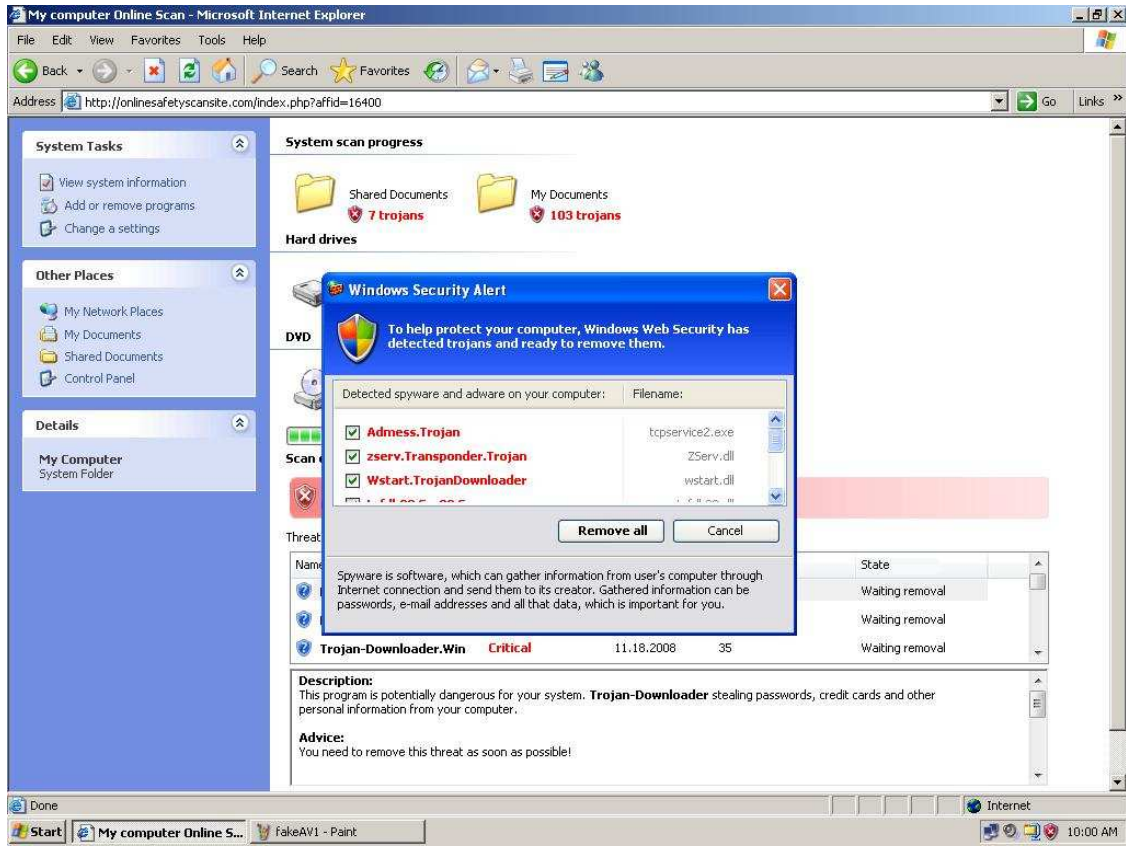
#### [Conficker c](#)

The latest variant of the worm, **Conficker C**, which was noticed in early March, is expected to launch its attack once the system date on an infected machine ...

[www.granadino.edu/co/canada/conficker\\_c.html](#) - 18 hours ago - [Similar pages](#)

[More results from www.granadino.edu.co »](#)

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.