

6 December 2008

By: Lucian Constantin, Web News Editor



Facebook worm
morphs again
Facebook (for the
logo)

[Facebook Worm Active Again](#)

The new variant passes Facebook's security filters

The writers of the Koobface worm that propagates on social networking websites have just released a [new variant](#) that is able to trick the security filters enforced by Facebook. In order to achieve this, the new strain makes use of the website's own features against itself.

The Koobface worm was [first detected](#) back in July, with the two original variants attacking MySpace and Facebook, respectively. The worm employs social engineering tactics and profits from the core design concepts of social networking websites. Instead of registering fake accounts on the websites in order to propagate, the worm uses the legit accounts accessed from the infected computers.

This technique is particularly effective against security features that allow certain actions to be performed only by users added to the friends list of an account. It also gives spam messages more credibility, since they come from what people might think is a trusted source.

The Koobface worm propagates by sending spam messages with links to fake video files and encourages the users to visit them. The links take them to a page that imitates an embedded video file. Attempting to view the file results in an error that instructs the users to install a video codec, which is actually the malicious executable that drops the worm onto the system.

In an attempt to mitigate these attacks, Facebook and MySpace have enforced special security policies and filters. Even though these actions did not kill the worm entirely, they significantly reduced its propagation rate. As a response, the worm's writers released new variants that featured new techniques of bypassing the security measures.

For example, one such variant, [released](#) in October, resorted to hosting the fake pages on Google's Picasa Web Albums service, relying on the fact that generic filtering of links on this domain would be difficult since it would also prevent users from sharing legit Picasa resources on Facebook. The latest variant is similar, but the hosting has been changed from Google's Picasa to Yahoo's Geocities service.

In addition, the spam messages do not contain direct links anymore. Instead, they are using Facebook's own redirect feature through links of the form http://www.facebook.com/l.php?u=http://geocities.com/account/fake_page. This redirects users from the social networking site to the malicious pages serving a fake Flash Player installer.

While keeping your security software updated should help prevent such attacks, being careful about what links you decide to visit, even if they are sent by a friend on a social networking website, is highly recommended.