Scumware (2):
Scumbody’s Changing my Web Page

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In this short series of articles, we’re looking at how some kinds of software make unauthorized changes to the appearance of Web pages.

Surf+ is an example of a product that adds unauthorized embellishments to Web pages. Using this product, ordinary words become hyperlinks; the scumware adds underlines and highlights keywords in green. It is thought that about 500,000 users have installed this product. The company makes money by selling links to competing sites; some Webmasters have reported noticeable declines in Web advertising as a result of the modification of user’s view of their Web pages. To the horror of some Webmasters, some of the added links send visitors to porn sites who have paid for the, ah, exposure.

TopText (also known as ContextPro) from eZula is bundled with other software (e.g., the KaZaa peer-to-peer file sharing software). Estimates of the installed base run as high as 2 million users. This toolkit is a browser plug-in that gives Internet Explorer the ability to show additional links underlined in yellow lines. The makers defend their product by pointing out that surfers know what they’re getting into if they read the end-user license agreements; that their service successfully provides a legal method for increasing business to their clients; and that their system helps to pay for free services for which users would otherwise have to pay.

Greg Searle reported in RISKS 21.47 on yet another way of annoying Web users. A company called Fastclick provides code that hides pop-up windows behind the windows already on screen. These pop-ups remain in place and are revealed only after one minimizes or closes the other windows on screen -- by which time it is difficult to determine where the pop-ups came from. The solution, such as it is, is to disable JavaScript; alternatively, if one can locate the offending sites, one can put them on a firewall's or browser's exclusion list.

Some products such as Gator deliberately _overlay_ banner ads; they insert their own choice of advertisement using exactly the same dimensions as the original banner add and fix their substitute to the same place on the Web page, thus obliterating the original entirely.

Some firewalls also allow the user to reject ads; for example, ZoneAlarm Pro v3.0 has a three settings for ad blocking: HIGH blocks all ads; MEDIUM blocks ads that don’t load within a user-stipulated time as well as all pop-up ads; and OFF lets all ads through. Ad-blocking software can perform the same function without firewall capabilities; type “ad blocker” into GOOGLE or another search engine and you’ll find dozens of such tools.

So here’s the essential problem: a Webmaster creates a Web page and includes links and advertisements. Some other company or person provides software to a user that alters the functions and appearance of the Web page before the user can see the intended Web page. Many vendors and users say that it’s the user’s own business what they do to the Web page once it
reaches the user’s own computer; however, many Webmasters and other content providers argue that their work is being modified without their permission.

* * *

For further reading:

Surf+:
TopText:
  http://www.suniltanna.com/ezula.html
Fastclick:
  http://catless.ncl.ac.uk/Risks/21.47.html#subj8

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@compuserve.com>. He invites inquiries about his information security and operations management courses and consulting services. Visit his Web site at <http://www.mekabay.com/index.htm> for papers and course materials on information technology, security and management.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.