THE
LAST
WORD

THERE'S A FLY IN MY DIGITAL SOUP

By Gregory Conti

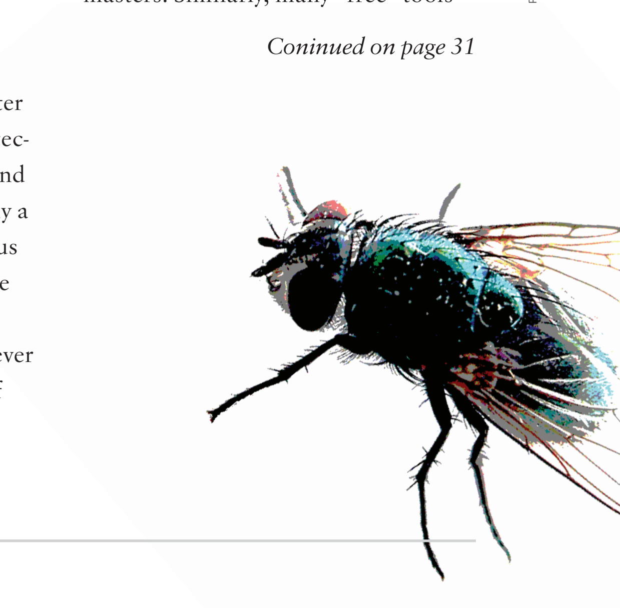
A dysfunctional online experience is no accident.

I may not like the taste, but I can't live without my digital soup. Life online once meant unfettered access to information, the ability to publish and share information, and instant global communication, but today much of the Internet, particularly the Web, is a mess. Not a random mess, nor a mess created by lack of aptitude on the part of its designers, but much of it—sometimes visible, sometimes surreptitous—is quite deliberate.

Regardless of operating system or hardware platform, users should not blithely trust their computers. Make no mistake, every computer is constantly under attack online, and the defenses are notoriously porous. Computer security is not a solved problem and will likely remain a significant weakness and source of compromised information for the foreseeable future. Consider how many processor cycles your computer expends on antivirus, intrusion-detection, antispyware, spam filtering, and firewall functions just to detect only a portion of the attacks and suspicious behavior coming your way. You have more power than a Cray supercomputer on your desktop, but you'd never know it because the computer itself has become a self-licking ice cream cone of partially effective security countermeasures.

Network security has enjoyed marked improvement over the past decade. However, this improvement has also motivated a shift away from low-level network attacks and toward an attacker strategy targeting Web browsers and the humans using the computers. This trend will continue, as more and more tools migrate from the desktop to the Web (or to the "cloud" if you prefer). Users everywhere are increasingly dependent on a single application—the browser—making it a high-payoff and oft-compromised target for attackers. But the browser isn't the end of the insecurity story. Many mainstream desktop software applications "phone home" to provide information to their corporate masters. Similarly, many "free" tools

Coninued on page 31



PHOTOGRAPH BY JOHN TALBOT

Coninued from page 32

we employ online are simply honeypots deliberately designed to collect user data and display advertising. The most effective countermeasure is still to question our trust for each organization whose software we use, on the desktop or online.

Another trend involves more subtle attacks against users. Conventional wisdom regarding interface design says the role of the interface is to facilitate the accomplishment of a user's task. In practice, however, this academic philosophy is typically not enforced. Some interface designers are potent adversaries simply putting their goals ahead of yours. Perhaps you've encountered flying vodka bottles covering the news story you were trying to read, fake hyperlinks that triggered pop-up ads, Web forms that coerced you into divulging sensitive information, or Web spam sites that contain little more than pseudo-content whose sole reason for existence is to make you click on ads. The end result is a usability nightmare that should make any self-respecting interface designer cringe, all in the name of increasing ad click-throughs and gathering personal information that can be sold or resold to parties unknown.

Behind the distracting veneer of the interface, large portions of the Web are instrumented to tag and track user activities as we browse. Web bugs aren't new, but the simple 1990s-era 1x1 transparent GIF tracking bug has evolved into rich-media objects employing enabling technologies like Flash, JavaScript, and Silverlight designed to avoid detection by end users. This evolution fuels yet another trend toward content itself becoming a Web bug. Webmasters today have a great deal of incentive to embed third-party content in their sites in the form of free media (think YouTube videos), analytics tools, social-networking applications, and maps—all potentially generating significant advertising revenue. Unfortunately, each content download leaves footprints behind on third-party servers users didn't intend to visit or were unaware their visit had even taken place. Similarly, ISPs, as well as some governments, are increasingly aware of the value of the information flows traversing the networks under their control and are beginning to leverage their power to restrict access to information, collect user data, and alter information flows on the fly.

EXPECT TO RECEIVE PRECISELY TARGETED ADS THROUGH OUR DESKTOP AND MOBILE DEVICES THAT KNOW OUR DEEPEST WANTS AND DESIRES, PERHAPS EVEN BEFORE WE RECOGNIZE THEM IN OURSELVES.

Life online is thus increasingly unpleasant and promises worse. Behavioral targeting (using user profiling data to deliver precisely targeted ads) will evolve and gain strength. We see a glimpse of it today in the eerily accurate book recommendations suggested during visits to online booksellers. Tomorrow, expect to receive precisely targeted ads through our desktop and mobile devices that know our deepest wants and desires, perhaps even before we recognize them in ourselves. The rampant targeting and exploitation of users outlined here is not the path forward. However, they are indeed opportunities to seek a better recipe for our digital soup. The end result will be well worth the effort. ◀

Gregory Conti is an assistant professor of computer science at the United States Military Academy, West Point, NY, who conducts research into Web-based information disclosure, secure and usable interface design, and information visualization. He is the author of *Googling Security* and *Security Data Visualization.* He can be reached at conti@acm.org.

The views expressed here are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

DOI: 10.1145/1540392.1540402