

Spyware, Adware, & Mozilla Firefox

Sunbelt Software Spyware Research Center

March 10, 2005

Introduction

Over the past few months security experts have speculated that we could see new spyware and adware crafted for Mozilla Firefox, an alternative browser which is becoming more popular with users looking to avoid spyware problems previously thought to be exclusive to Microsoft's Internet Explorer (http://internet.newsforge.com/article.pl?sid=05/01/31/2121249). Until now most of this speculation has centered on the potential for security holes in Firefox that could be exploited by spyware and adware creators. But such speculation is arguably misguided. In fact, we already have seen instances of spyware and adware that can be installed through Mozilla Firefox. These cases haven't received much attention, however, largely because researchers have been too focused on security exploits instead of the more run-of-the-mill methods through which spyware and adware are typically delivered to users' desktops: namely, social engineering techniques that spring unwanted software on confused users who aren't careful enough about what they click.

Security Vulnerabilities & Firefox

It is understandable that security exploits have become a primary concern when discussing spyware and adware. Security holes in Internet Explorer have been used with great success to install spyware and adware surreptitiously on PCs without any notice or warning whatsoever to victims. Variants of CoolWebSearch and VX2/Transponder, for example, are notorious for exploiting security holes to "stealth install" on PCs and then wreak havoc. Currently there are credible reports that the "Searchmeup" CoolWebSearch variant is exploiting the "LoadImage" vulnerability that was discovered in December by Chinese researchers and patched in January by Microsoft (http://www.internetnews.com/security/article.php/3487251).

Security researchers are justified in predicting that we could see spyware and adware that is similarly designed to exploit security vulnerabilities in Mozilla Firefox, which recently surpassed 25 million downloads and is becoming ever more popular among users weary of the battle against virulent spyware and adware. The security research firm Secunia reports 11 advisories for Firefox over the past two years, the vast majority after August of 2004 (http://secunia.com/product/4227/%20(Firefox)). The most recent batch of Firefox security vulnerabilities included a flaw that could cause Firefox users to fall victim to phishing schemes (http://www.nwfusion.com/news/2005/0225mozilwarns.html). (Ironically, Microsoft's much maligned Internet Explorer was not affected by this particular vulnerability.) And though these latest security vulnerabilities are fixed in the recently released Firefox version 1.0.1, Secunia notes that Firefox is still affected by three vulnerabilities that are rated "less critical."

So, we have encountered security vulnerabilities in Firefox before. Moreover, it's a fair bet that we'll see even more of them as Firefox becomes more popular among users and starts receiving more attention from hackers. But this focus on security exploits risks distracting us from a potentially more serious problem in Firefox -- namely, the risk that users could be tricked into "consenting" to the installation of software that they don't fully understand, want, or need. If we look at the ways software can be installed in Firefox, we should recognize that this a very real danger.

The Boring Reality of Spyware & Adware

Despite the widespread attention that exploit-based installs of spyware and adware have received, the reality of spyware and adware is much more boring and depressing. The sad truth is that much if not most spyware and adware is installed on PCs after users "consent" to those installations, usually without fully understanding the nature of the software.

Internet Explorer has been justly criticized for facilitating such installations, because the ActiveX "Security Warning" box that pops up when web sites attempt to install software is enormously confusing to users (https://netfiles.uiuc.edu/ehowes/www/dbd-anatomy.htm). That "Security Warning" box names the software program and the company responsible for it, though even this information can be downright deceptive, as noted researcher Ben Edelman recently pointed out (http://www.benedelman.org/news/020305-1.html). The box also supplies a link to the software's End User License Agreement (EULA). As we all know, however, those EULAs often consist of long, dense blocks of legalese that only practicing attorneys can make sense of. Beyond this poor information, the box offers precious little guidance to users.

Many users mistake such software for browser plugins required to view content on the web sites they're visiting. Still others don't recognize that they can click the link to read the EULA. Even worse, because these "Security Warning" boxes frequently pop up at third-party web sites while users are concentrating on the content of the sites themselves, many users don't pay close enough attention to what little information that is provided about the software. And so they click through those "Security Warning" boxes willy nilly, effectively giving their consent to software they don't fully understand, want, or need. Only after that unwanted software begins blanketing their desktops with pop-ups do they finally realize something is amiss.

To its credit, Microsoft has taken several important steps to address the problems with those confusing "Security Warning" boxes. When users with Windows XP Service Pack 2, for example, land on web sites that attempt to install software on their computers, those users receive a discrete notice in the new "Information Bar" along the top of the Internet Explorer browser window. Service Pack 2 for Windows XP also adds a pop-up blocker to Internet Explorer, reducing the chances that users could be badgered by web sites into clicking through boxes for unwanted software. Microsoft bundled still other security improvements into Windows XP Service Pack 2, and the net effect is to make Internet Explorer much more "resistant" to spyware and adware.

Software Installation in Firefox

Like Internet Explorer, Mozilla Firefox also allows users to install software online, and there-in lies the risk. While security researchers have been looking for security holes in Firefox that could be exploited by spyware and adware (as will surely happen at some point), we ought to recognize that Firefox already has a spyware and adware problem. That problem arises because the information that Firefox gives users about software installed by web sites is just as poor as the information in that old Internet Explorer "Security Warning" box. When confused users aren't given enough information to assess the danger of software installed by web sites, they could very

well start clicking through boxes, merrily giving their consent to unwanted software just as they do now with older versions of Internet Explorer.

Users of Mozilla Firefox can install software in at least four different ways. (See example screenshots in "Figures: Firefox Installation Methods" at the end of this document.) First, they can download a traditional setup program to their hard drives and run it. Second, they can install browser plugins, like Macromedia Flash, that let Firefox display special types of content on web sites. Third, they can install "browser extensions," which are special add-on programs that provide extra functionality to Firefox. Fourth, they can consent to the use of Java applets that are loaded by web sites to add special features to web pages. We can set aside traditional setup programs because although there is always risk in downloading and running software from the internet, users must deliberately run such programs once those programs land on their hard drives. The other types of software installations are fraught with danger, though -- especially the "browser extensions" and Java applets.

When Firefox users visit web sites that require plugins to display special content, Firefox provides a discrete notice in a yellow information bar along the top of the browser window. It also embeds clickable notices within the web page itself. Once users click the yellow information bar or the embedded notices, they are stepped through an installation wizard that names the plugin to be installed and displays a EULA. As installation processes go, this one isn't too bad, though it could be improved to require vendors to supply a more readable summary or description of the plugin and its functionality. With only a long, legally dense EULA to read, many users could simply click through to install the plugin without fully understanding the nature and purpose of the software. At least such plugins can supply a EULA, though.

"Browser extensions," by contrast, are much more problematic. When web sites attempt to install "browser extensions," Mozilla Firefox again displays a notice in a yellow information bar along the top of the browser window. After users click the information bar, however, they are presented with prompt to add the web site to a list of sites allowed to install software. No information is provided about the web site or the software. If users elect to permit the site to install software, they are presented with another prompt to allow installation of the particular "browser extension." This installation prompt provides even less information than the old Internet Explorer "Security Warning" box -- there's not even a link for users to click to get more information or to read the EULA. Without such information, many users might click the "Install Now" button, not understanding that they've consented to the installation of adware or spyware. And although the "browser extension" installation process does require users to jump through several hoops, the utter lack of useful information all the way along is a potentially serious problem.

The greatest risk, though, comes from Java applets, which Firefox can install and run with the aid of Sun's Java Runtime Extension (JRE) (http://java.sun.com/). Many web sites use Java applets to enhance the functionality of web pages, and most Java applets are completely innocuous, though we have seen Java applets that are used to install spyware and adware. Thus, Java applets represent yet another means through which Firefox users could encounter such unwanted software, and even experienced users could unwittingly consent to the installation of spyware and adware delivered by rogue Java applets.

When Firefox loads a web site that wants to install and run a Java applet, it starts the Sun Java "virtual machine," which promptly displays a notice requesting the user's consent to the applet. This prompt box contains almost no useful information whatsoever beyond the name of the company responsible for the Java applet. That company name isn't helpful because most users won't recognize the names of the companies behind spyware and adware. Still worse, because many Firefox users will be accustomed to clicking through these Java applet installation prompts without thinking twice, most won't even <u>notice</u> the name of the company. Thus, many Firefox users who encounter Java applets that install spyware or adware simply won't realize what they've consented to until their screens start filling with pop-up ads and their PCs' performance begins deteriorating.

Conclusion: Firefox, Spyware, & Adware

How realistic is it to expect adware and spyware to be installed through the installation methods just described? As a matter of fact, we have already encountered and documented examples of spyware and adware that are installed through just these methods. One variant of the "Bridge" spyware program was being installed by popular music lyrics sites last year through the "browser extension" installation method (http://www.sophos.com/virusinfo/analyses/trojbrissa.html & http://www.trendmicro.com/vinfo/grayware/graywareDetails.asp?SNAME=SPYW_BRISS.A). We've also seen a variant of the well-known XXXToolbar installed by "crackz" sites as a "browser extension" through Mozilla-based browsers, which include Firefox. More recently, we've learned of still other music lyrics sites that launch Java applets to install multiple adware programs, including the 180search Assistant, ISTBar, PowerScan, Sidefind, PeopleOnPage, and the YourSiteBar (http://www.vitalsecurity.org/2005/03/firefox-spyware-infects-ie.html). Finally, we know of new software from iSearch/iDownload that specifically detects that Firefox is present on the PC and installs a special "browser extension" for it (http://sunbeltblog.blogspot. com/2005/03/idownload-legal-matter-more.html).

At present such examples of Firefox-enabled spyware and adware are few in number and not widespread. But these examples do illustrate the potential problems that Firefox users could face with spyware and adware as Firefox (like other Mozilla-based browsers) becomes more popular with web surfers and, consequently, becomes a more attractive target for spyware and adware pushers. Without better information about the software that web sites attempt to install, Firefox users could very well be clicking their way through to spyware and adware just as furiously as Internet Explorer users have over the past few years.

More importantly, though, these examples should serve as on object lesson to security researchers, who tend to slight security problems that aren't as "sexy" as full-blown security exploits and vulnerabilities. The story of spyware and adware is largely the unremarkable tale of users being tricked into consenting to the installation of unwanted software, and security researchers would do well not to ignore that reality, however boring and depressing it might be.

Eric L. Howes 10 Mar. 2005

References

Ben Edelman - How VeriSign Could Stop Drive-By Downloads http://www.benedelman.org/news/020305-1.html

Eric L. Howes - The Anatomy of a Drive-by-Download https://netfiles.uiuc.edu/ehowes/www/dbd-anatomy.htm

Experts predict Firefox spyware will show up this year http://internet.newsforge.com/article.pl?sid=05/01/31/2121249

Mozilla warns of security holes, patches Firefox http://www.nwfusion.com/news/2005/0225mozilwarns.html

Searchmeup Targets Weak PCs http://www.internetnews.com/security/article.php/3487251

Secunia - Mozilla Firefox 1.x http://secunia.com/product/4227/%20(Firefox)

Sophos - Troj/Briss-A http://www.sophos.com/virusinfo/analyses/trojbrissa.html

SunbeltBlog - iDownload legal matter http://sunbeltblog.blogspot.com/2005/03/idownload-legal-matter-more.html

TrendMicro - SPYW_BRISS.A http://www.trendmicro.com/vinfo/grayware/graywareDetails.asp?SNAME=SPYW_BRISS.A

VitalSecurity.org - Firefox Spyware infects IE? http://www.vitalsecurity.org/2005/03/firefox-spyware-infects-ie.html

Figures: Firefox Installation Methods

1. Traditional Software Executable



Figure 1: Browser pop-up w/ clickable link



Figure 2: Download executable setup program

2. Browser Plugin Installation

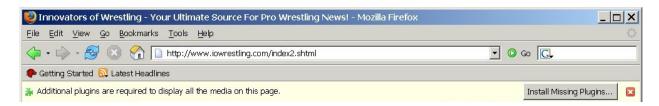


Figure 3: Browser plugin information bar

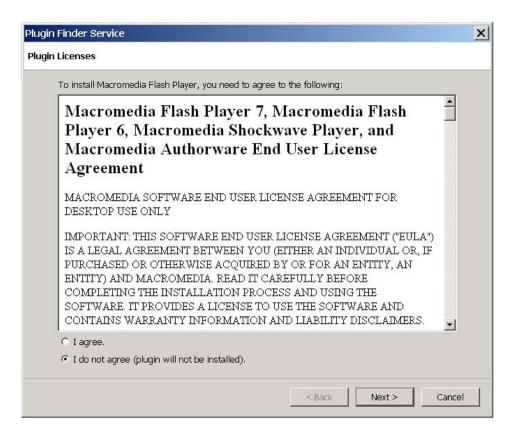


Figure 4: Browser plugin installation

3. Browser Extensions

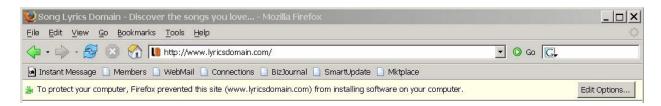
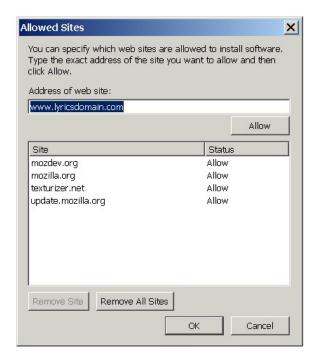


Figure 5: Browser extension information bar



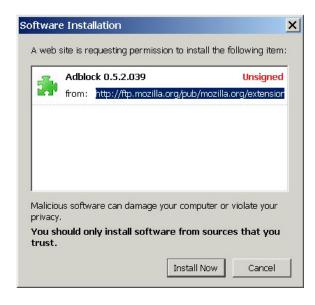


Figure 6: Allowed sites

Figure 7: Browser extension installation

4. Java Applets



Figure 8: Java applet warning # 1 (ISTBar)



Figure 9: Java applet warning # 2 (WebCT)

About Sunbelt Software

Headquartered in Tampa Bay (Clearwater), Fla., Sunbelt Software was founded in 1994 and offers products to protect and secure systems from costly inefficiencies including spam and spyware; as well as enterprise solutions to protect against system downtime and security vulnerabilities.

Sunbelt Software is part of the Sunbelt International Group, which includes Sunbelt Software, Inc. and Sunbelt System Software in Europe. The Sunbelt System Software group has offices in the UK, France, Netherlands, Sweden and Germany.

Primary Media Contacts

Laurie Murrell Marketing Communications Manager Sunbelt Software 888-NT UTILS (688-8457) lauriem@sunbelt-software.com

Heather Kelly heather@sspr.com 719-634-8274 Jason Ovitt jovitt@sspr.com 847-415-9326 S&S Public Relations for Sunbelt Software