Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer March 2009 | Volume 3, Issue 2

Web Browser Attacks

WHAT IS A WEB BROWSER?

The web browser is a software application that allows users to view and interact with content on a web page, such as text, graphics, video, music, games, or other material.[1] It is a very popular method by which users access the Internet. Of the various web browsers currently available, Internet Explorer, Mozilla Firefox, Opera, and Safari are the most prevalent. Plug-ins, also known as add-ons, are applications that extend the functionality of browsers. Some of the more familiar plug-ins include Flash Player, Java, Media Player, QuickTime Player, Shockwave Player, RealOne Player, and Acrobat Reader. Based on how a web page was designed, specific plug-ins may be required to view some content.

HOW CAN MY BROWSER PUT ME AT RISK?

According to a recent study, approximately 45% of people surfing the Internet are not utilizing the most secure version of their web browser.[2] Like other software, without the appropriate security patches applied, web browsers are vulnerable to attack or exploit. A fully patched web browser can still be vulnerable to attack or exploit if the browser plug-ins are not fully patched. It's important to remember that plug-ins are not automatically patched when the browser is patched.

Traditionally, browser-based attacks originated from *bad* websites. However, due to poor security coding of web applications or vulnerabilities in the software supporting web sites, attackers have recently been successful in compromising large numbers of trusted web sites to deliver malicious payloads to unsuspecting visitors.

Hackers add scripts that do not change the website's appearance. These scripts may *silently* redirect you to another web site without you even knowing about it. This redirect to another web site may cause malicious programs to be downloaded to your computer. These programs are generally designed to allow remote control of your computer by the attacker and to capture personal information, often related to obtaining credit card and banking information and other data that can be used to perform identify theft.

In April 2008, Panda Labs, a computer security and anti-virus publisher, announced that more than 280,000 web sites had been altered to redirect computers to malicious websites which would attack them in a variety of ways. The SANS Institute, a computer security research and training organization, recently declared browser attacks to be the *Top Cyber Security Menace* for 2008.

Not just desktop or laptop computers are vulnerable. As their popularity increases, smart phones such as Blackberries and iPhones may become targets of browser-based attacks because of the built-in browser's technology and Internet access.

Clearly, users must be aware of the issues and take proactive measures.

[1] Wikipedia, **en.wikipedia.org/wiki/Web_browser**

[2] Frei, S., Dübendorfer T., Ollmann G, May M., "Understanding the Web browser threat: Examination of vulnerable online Web browser populations and the 'insecurity iceberg' "

WHAT CAN I DO TO PROTECT MYSELF FROM BROWSER ATTACKS?

You can take a number of steps to protect yourself from browser attacks. Your company or agency's IT department should already have implemented these steps, but you can also apply them to your home computer:

- Keep your browser(s) updated and patched.
- Keep your operating system updated and patched.
- Use anti-virus and antispyware software, and keep your definitions up to date. Recommended software for the individual user includes Comodo (**www.comodo.com**), ZoneAlarm (**www.zonealarm.com**), and Blink (**www.eeye.com**).
- Keep your applications (programs), such as multi-media programs used for viewing videos, updated and patched, particularly if they work with your browser.
- Install a firewall between your computer and the Internet and keep it updated and patched.
- Block pop-up windows, some of which may be malicious and hide attacks. This may block malicious software from being downloaded to your computer.
- Tighten the security settings on your browsers. Check the settings in the security, privacy, and content sections in your browser. The minimum level should be *medium*.
- Consider disabling JavaScript, Java, and ActiveX controls.

Please note that a number of these tips may impede your use of the Internet or limit what content you can access. If you find that you really need ActiveX controls or you require JavaScript to be enabled, set your browser to prompt you before running scripts. If you find that you need to lower your security settings to be able to access what you need, lower them temporarily and then reset them.

NOTE: The Conficker worm's newest variant, which kills protective security processes, is set to activate on April 1. See **support.microsoft.com/kb/962007** for more information on this worm and how to prevent or remove it.

ADDITIONAL RESOURCES

For additional information on browser attacks, please visit:

- US-CERT Security Tip: **www.us-cert.gov/cas/tips/ST05-001.html**
- SANS Cyber Security Institute's Top Threats for 2008: **www.sans.org/2008menaces**
- PC World: Hackers Increasingly Target Browsers: **www.pcworld.com/businesscenter/article/144490/hackers_increasingly_target_browsers.html**
- Computer Weekly: Attacks By Criminals on Web Browsers **www.computerweekly.com/Articles/2008/02/14/229406/storm-worm-is-basis-for-most-cyber-attacks-says-ibm.htm**
- Panda Labs: **pandalabs.pandasecurity.com/archive/IFRAMES-Attack-_210021002100_.aspx**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.
For more information on Internet security, please visit the SecureTexas website at **www.dir.state.tx.us/securetexas**.
SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC www.msisac.org

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM www.us-cert.gov

Distributed by: DIR SecureTexas www.dir.state.tx.us/securetexas