Information Security Updates

Internet Security 1

Issue 14

Related Article

Firefox vs. Chrome vs. Internet Explorer

Currently the Microsoft Internet Explorer ("IE") who dominates the market now has 60% market share retained. The other major competitors are Firefox and Chrome with 25% and 7% market share respectively.

Although speed and reliability are the imperative attributes for browser, there are growing concerns over security. Among the three contenders, IE hangs on to a reputation of safe and reliable with Microsoft at its helm and maybe it can explain why it remains favourites in the market.

(http://www.networkworld.com/news/2010/060710-tech-argument-browsers.html)

Related Article

Bulk of browsers found to be at risk of attack

About 8 out of every 10 Web browsers run by consumers are vulnerable to attack by exploits of already-patched bugs.

When browsers and their plug-ins are tabulated together, between 90% and 65% of all consumer systems scanned with Browser Check since June 2010 are reported to have at least one out-of-date component, depending on the month.

(http://www.computerworld.com/s/article/9209958/Bulk_of_browsers_found_to_be_at_risk_of_attack)

I. Background

Industry Story

Scaling Back Web Browser Security Expectations

Web browsers serve as the most popular interfaces for users to interact with the web-based applications. However, as it is always said, technology is the double-edged sword, the increasing importance of the web browsers in today's Internet technologies has also made web browsers the focus of cyber attack.

Security is one of the major concerns on the evolution of web browsing technologies and development of web browser market. Vulnerabilities of web browsers such as Microsoft Internet Explorer and Firefox are continuously discovered or exploited. It has been a challenging task for web browser vendors to incorporate latest web technologies and meanwhile to harden their products in order to protect the information security of its users.

See the article: (http://searchsecurity.techtarget.com/tip/Scaling-back-Web-browser-security-expectations)

Internet Security Overview

Internet security is an essential component for preserving the information security within universities. The Internet is an insecure channel for communicating and exchanging information. Therefore, the main objective is to protect the universities' information systems from various threats.

The most common approach for universities' students and staff members to interact with the Internet is through the use of web browsers. Nowadays, software vendors of the web browsers often incorporate different features to improve the user experiences when browsing the Internet, but sometimes may end up causing additional vulnerabilities and increasing the security risk exposed to malicious attacks.

As most of the threats aim at attacking the web browsers used by students and staff members of universities, it is important to understand various threats on the Internet and the corresponding consequences when those threats exploit the vulnerabilities of the web browsers, whether it is Internet Explorer, Mozilla Firefox, Opera, or Apple Safari.

Reference:
http://science4umore.blogspot.com/2009/08/understanding-internet-security-threats.html

Related Article

Evaluating Your Web Browser's Security Settings

Your web browser is your primary connection to the rest of the Internet, and multiple applications may rely on your browser, or elements within your browser, to function. This makes the security settings within your browser even more important.

Many web applications try to enhance your browsing experience by enabling different types of functionality, but this functionality might be unnecessary and may leave you susceptible to being attacked. The safest policy is to disable the majority of those features unless you decide they are necessary.

(http://www.us-cert.gov/cas/tips/ST05-001.html)

Statistical Report

Internet Browser Software Review

A comprehensive review of the popular browsers is performed in 2011. The reviewed browser products include Firefox, Google Chrome, Internet Explorer, Opera, Safari, Maxthon, Avant, PhaseOut, Deepnet Explorer and SpaceTime.

The review comprised of several major areas of the browsers' functionalities, including security (e.g. popup block, anti-virus, clear history), speed, supported operating systems and program features (e.g. password management, parental controls)

(http://internet-browser-review.toptenreviews.com/)

II. Management

Threats to Internet Security

While most of the network infrastructures and information systems maintained by universities have appropriate information security management (e.g. corporate firewall, change management and regular penetration tests), individual access to the Internet by students and staff members is often loosely controlled. Management should be aware of the following major threats that usually exploits the vulnerabilities of web browsers and may result in adverse impact on the overall security of universities' IT environment.

1. Phishing

Phishing is a way of attempting to obtain sensitive information (e.g. usernames, passwords and credit card details) by masquerading as a trustworthy entity when users are interacting with the Internet. It is typically initiated by directing users to fake websites through e-mail spoofing or by popping fake messaging windows to deceive users for downloading malware. Recent trends also indicate that social networking sites have become the prime target of phishing, since the personal details in such sites can be used in identity theft.

Impact

Successful phishing attempts can cause the leakage of sensitive information related to the universities or their students/staff. Access (i.e. usernames and passwords) to universities information systems may be released to unauthorised parties and lead to serious security breaches. Monetary loss may occur if credit card details are acquired by the attackers. Reputation damage or possible litigations may follow a phishing activity that steals the privacy data from universities' students, staff or third party personnel (e.g. contractors).

2. Trojan

A Trojan is a general term for malicious software that pretends to be harmless so that a user willingly allows it to be downloaded onto his or her computer. Unlike viruses, Trojans do not replicate themselves and spread to other hosts. Instead, they resemble themselves as useful programs that users wish to run. When being executed, they are doing something unrelated to the advertised purposes without users' knowledge. The most common ways to be infected by Trojans is downloaded files or e-mail attachments.

Impact

Consequences of Trojan infection come to many forms. A key logger Trojan logs the victim's keystrokes and then send the log files to the attacker. A remote access Trojan gives the attacker control over the victim's computer. The attacker can go through the files and access any sensitive information (e.g. personal data, credit card numbers and research information) that is stored in the files. A proxy/wingate Trojans converts the victim's computer into a proxy/wingate, which can be used by the attacker for anonymous access to commit illegal activities.

References:
http://www.mixthenet.com/browser-based-attacks/
http://science4umore.blogspot.com/2009/08/understanding-internet-security-threats.html

II. Management (Cont'd)

3. Spyware

Spyware refer to programs that surreptitiously monitor the activities of a user's computer and report such information back to the spyware owners without users' awareness. Originally spyware is a way for shareware authors to earn revenue from their free software by implanting advertising elements (e.g. banners, popup windows, etc). The downside is that such advertising elements perform additional tracking tasks on users' behaviours and report the statistical data back. Ideally, there will be no sensitive information being collected. However, the functions of spyware have been extended well beyond simple tracking today and are able to collect various types of personal information, such as Internet surfing habits, websites that have been visited, redirecting web browser activities, altering system configurations or even installing additional software.

Impact

Interference with users' control of their computers is one of the most dangerous consequences of spyware. Victims may frequently notice undesired behaviours, such as unknown CPU activity, disk usage and network traffic, which cause degradation of system performance and stability. In addition, spyware is closely related to identity theft as it sometimes record the victims' user accounts, passwords or bank information. For example, the "CoolWebSearch" spyware takes advantage of Internet Explorer's vulnerabilities to create popup ads, redirect web pages to pornography or gambling sites and collect private data.

4. Worm

Generally speaking, worms are viruses that can replicate themselves through the Internet by exploiting security flaws of victims' computer systems and perform malicious tasks. Unlike computer viruses, worms do not need to attach themselves to existing programs and therefore are more epidemic in nature.

Impact

Most worms are capable of hampering the working of the Internet, whether by altering web browsers' setting, consuming bandwidth, corrupting system files or installing backdoors to allow the creation of "zombie" computers, which comprise a network called "botnet" commonly used for sending junk e-mails and launching Denial of Service ("DoS") attacks.

In November 2008, a worm named "Conficker" exploited vulnerabilities in a number of Microsoft operating systems and infected millions of computers and business networks in countries around the world, creating a massive botnet that can be controlled by the author. Its infection also include web browser problems such as redirection of web pages to unintended websites, program crashes, DoS symptoms (e.g. "404 error" or "Page not found" when attempting to access security software websites).

Recent Incident

Virus attacks cripple university network

In January 2010, there was a massive virus attack hit the University of Exeter, United Kingdom and resulting in the entire network being shut down and no access to web, emails and online learning system over days.

It was reported that the lead of the incident was because the network administrator did not patched the exploitable computers with appropriate fixes therefore allowed virus to crack the system from the vulnerability in Windows Vista (including SP1 and SP2), along with Windows Server 2008 (SP1 and SP2).

(http://www.zdnet.com/blog/igeneration/virus-attack-hits-vista-machines-cripples-university-network/3954)

Related Article

7 Tips to Use the Internet Safely

There are millions of things we can do via internet to make our lives easier such as online shopping, reading news, connect with friends etc. However, there are risks associated with it such as virus, hackers and cyber-crooks. All of these can ruin our internet experience and cause loss and damage.

So here are some tips to help keep you and your information as safe as possible when you go online. Although none of these methods is foolproof, they will help protect you against the potential dangers associated with the Internet.

(http://www.securitynewsdaily.com/7-tips-use-internet-safely-0847/1)

References:
http://www.spychecker.com/spyware.html
http://www.cse.buffalo.edu/~qiao/cse620/fall04/worms.ppt
http://www.thedailybeast.com/articles/2010/12/11/hackers-10-most-famous-attacks-worms-and-ddos-takedowns.html

III. General Users

Security of Web Browsers

Most of the popular web browsers today have integrated some fundamental security features that can largely lower the risk of threats on the Internet. The followings functions are highly recommended to be enabled for general users:

- **Enable Popup Blocker** – Enabling "Popup Blocker" can effectively reduce the possibilities of being compromised by malicious content in the popup windows. Most web browsers have this function enabled by default and users are strongly recommended not to disable it unless the popup windows are from trusted websites.

- **Control Cookies** – Cookies are widely used by websites to track users' activities, personalisation settings, browsing status, login user accounts or even encrypted passwords. Many attacks on the Internet utilise cookies to spread malicious activities, steal user identifies and passwords. Most web browsers can perform automated purge of cookies and general users are recommended to enable them. For example, check "Cookies" in the "Delete browsing history" configuration page of Internet Explorer 9.

- **Anti-Virus and Anti-Malware** – A good habit to maintain the health and security of computer systems is to install anti-virus and anti-malware programs. General users should regularly (e.g. weekly) update the virus/malware definitions and perform system scans to detect / quarantine / remove any viruses and malware programs on their computers.

- **Be Cautious to Social Websites** – The development of social websites, such as Facebook, MySpace and Twitters, creates opportunities for attackers to conduct activities including phishing, personal data theft or clickjacking. General users should be cautious about suspicious links either available on the social websites (e.g. news feeds from friends) or received through e-mails. They should check with their friends through alternative means (e.g. instant messaging, e-mails or SMS) before clicking on the doubtful links. Moreover, be aware that most social websites do not ask users to re-login simply to view material or access web applications. Always to change the passwords of the social websites immediately if a user believes that he or she has already fallen victim to malicious attacks.

Conclusion

The Internet is a double-edged sword. It is an excellent source of information and a convenient means of communication. Yet, the freedom of the Internet and lack of monitoring exposes universities to great threats. Management should well understand the potential consequences resulted from the Internet threats and cultivate general users' awareness on information security when surfing on the Internet through web browsers.

References:
http://www.ecu.edu/cs-itcs/itsecurity/Web-Browsers.cfm
http://www.mixthenet.com/browser-based-attacks/
http://www.it.northwestern.edu/security/browser-management/

Related Article

Web browser security tutorial: Safari, IE, Firefox browser protection

If not properly secured, web browsers can serve as a gateway for malicious hackers who want to infect your network.

This tutorial discusses how to harden your web browser security efforts, identifies the inherent flaws of Internet Explorer, Mozilla Firefox and Safari, introduces viable Web browser alternatives, and provides tools and tactics to maximise web browsers' functionalities

(http://searchsecurity.techtarget.com/tutorial/Web-browser-security-guide-Safari-IE-Firefox-browser-protection)

Related Article

Facebook users subjected to more clickjacking

Facebook users have been subjected to another round of clickjacking attacks that force them to authorise actions they had no intention of approving.

The latest episode in this continuing saga, is a set of campaigns aimed at Italian-speaking users of the social network. The come-ons promise shocking videos about such things as the real ingredients of Coca Cola. Instead, they are forced into registering their approval of the videos using Facebook's "Like" button.

(http://www.theregister.co.uk/2011/02/22/facebook_clickjacking_attacks/)