

The Changing Face of Vulnerabilities

By Rahul Kashyap



Although social engineering does not play a role in all forms of security threats, McAfee Avert Labs has observed a growing trend recently: malware writers using social engineering to exploit software vulnerabilities.

Most of the infamous Internet worms in the first half of this decade typically exploited one or more vulnerabilities in Microsoft applications. The notorious Sasser, Blaster, Code Red, and SQL Slammer had a common factor. (By the way, Avert Labs discovered Sasser and Blaster, as well as other significant malware.) They all exploited server vulnerabilities. The intent of these worms was to destroy servers via quick self-propagation after exploiting the flaws. Although products from many vendors have suffered from similar security holes, we will primarily focus on vulnerabilities and trends in Microsoft products in this article. We're not singling out Microsoft as being particularly vulnerable, but rather acknowledging that the popularity of Microsoft products among consumers and businesses attracts malware writers and data thieves like no other target.

Avert Labs has seen that server vulnerabilities that can be exploited by worms have diminished in the past few years thanks to increased use of security measures that protect remote procedure calls. To illustrate, Figure 1 lists all the remotely exploitable vulnerabilities via Microsoft Windows remote procedure calls during a 10-year period through the first quarter of 2008. The trend has fallen dramatically in the last two years. We see a similar trend if we sample remotely exploitable vulnerabilities for other popular Microsoft server platforms, such as IIS Web Server, SQL Server, and others.

Microsoft further increased its defenses with the release of Service Pack 2 for Windows XP. Along with other protection mechanisms, SP2 included data execution prevention,² which—though not foolproof³—definitely helped in curbing the network worm

propagation that plagued Windows at that time. The effects of XP's SP2 became much more visible a couple of years later, as many users migrated to the updated operating system.

However, malware writers were not to be outdone. They quickly shifted their focus from server to clients, uncovering vulnerabilities in Microsoft Office, Microsoft Internet Explorer, and various proprietary file formats. The client assault gave birth to a host of fuzzers⁴ (which search for security holes by throwing random data at an application), scripting-language parsing bugs, and ActiveX control-related vulnerabilities. Projects such as the "Month of Browser Bugs"⁵ (and others), axfuzz,⁶ COMRaider, and hamachi⁷ increased interest in this area and helped expose the innumerable issues plaguing client software. Bug discovery and the exploitation of client applications has been at its peak

Microsoft remote vulnerability patches

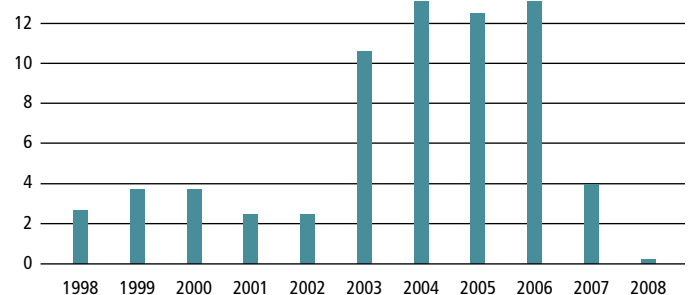


Figure 1: Microsoft has significantly tightened the security of its remote procedure calls since 2006. (Source: Microsoft!).

Office vulnerability patches

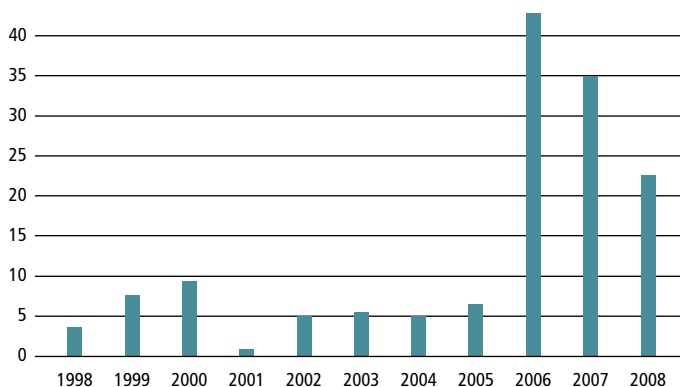


Figure 2: Microsoft Office vulnerabilities increased in 2006 and have remained high in the two successive years. (Source: Microsoft).

during this period; this trend continues even as we prepare this journal. The numbers of client software being exploited is hard to determine, but some sources claim the figure to be in the hundreds of millions.⁸

Figure 2 offers a vivid picture on the sudden spike of vulnerabilities for Microsoft Office. These peaked in 2006 and continue to keep Microsoft busy.

The majority of these vulnerabilities have affected Office 2000. This version is widely used, thus it has been more widely exploited. In the economics of malware writers, vulnerabilities in Office 2000 offer a better return on investment. This is primarily because this suite has long had a major security disability: Office 2000 users must visit Microsoft's "Office update" page to download patches⁹, and the automatic online updates do not serve Office 2000 or Office 97. This oversight creates a terrific opportunity for malware writers to exploit the fact that many users are unlikely to regularly update their Office suites.¹⁰ The number of "zombie" machines taken over because of this type of security hole could be in the tens of thousands.

Although we're focusing on vulnerabilities in Microsoft products in this article, the trend affects other popular client software vendors, such as Adobe, Mozilla, Apple, and more. The "Month of Apple Bugs" highlighted many client problems, and there has been a big spike in the vulnerabilities found in widely used software, such as Apple QuickTime, Adobe Flash Player, and Adobe Reader, to name just a few. The recent exploitation of the PDF mailto: vulnerability (CVE-2007-5020)¹¹ and of Flash using ActionScript (CVE-2007-0071) were among some of the critical flaws that affected thousands of users.

Targeted Attacks

The key to client vulnerabilities is that they need user interaction to be exploited. Hence malware authors have had to come up with more innovative ideas to lure users into clicking links and downloading images and documents from the Internet. One of the main thrusts for exploiting client systems has been a rapid growth in spam that relies on social engineering.

Social engineering and the focus on client vulnerabilities go hand in hand. The connection between these two factors is obvious, and the threat has recently become more complex.

Part of that complexity lies in targeted social engineering attacks, which are the emerging trend in the threat landscape. Targeted attacks are especially popular in defense and military establishments.¹² Ever since the rash of Office vulnerabilities in 2006, multiple reports have appeared about government agencies receiving emails with malicious Word, PowerPoint, or Access files. It looks like the combination of social engineering and vulnerabilities has found another target: espionage.

Spying, of course, is stealthier and much more difficult to uncover than a merely profit-driven attack. On multiple occasions, the vulnerabilities discovered in these malicious embedded documents have been zero-day attacks, which make these document files even more difficult to detect: these vulnerabilities are often found only after the damage is done. Because these zero-day vulnerabilities have targeted specific government or military installations, it's possible that these attacks could be sponsored by foreign agents or governments. Custom-designed social engineering, zero-day vulnerabilities, money, and power sound like elements of a John le Carré novel. Some security analysts think this is not fiction. Many theorists have predicted that the next generation of warfare will be in cyberspace. Perhaps all of these events are just test cases for a cyberwar?

Stealthy Web Hacks

Other exploits that have changed in recent years are web server hacking and hijacking. Earlier attackers used to deface web sites after they hacked them—usually leaving a note on the site in the hope of becoming famous. That's no longer the case, at least not with today's new generation of sophisticated hackers. With the plethora of client vulnerabilities, hackers have started exploiting these in a coordinated manner, spreading malware by first compromising popular web sites, stealthily planting malware, and luring users via social engineering tricks.

As a leading example, the Super Bowl (American football final) hack in February 2007 deserves mention, as it involved the insertion of a malicious JavaScript into the home page of the

official site.¹³ The script exploited two flaws in Internet Explorer and infected unpatched users with a Trojan that connected to a Chinese server, giving full access to the compromised machine. Similar stealthy hacks have been reported for many popular web sites, including embassies, newsgroups, and corporations.

Another emerging threat that made millions of homes vulnerable was exploiting home routers via Universal Plug and Play, which allowed a malicious Flash file embedded in a web page to reconfigure the victim's router.¹⁴ (The fact that the vast majority of Internet users use the default passwords in their home routers helps make this attack possible.) In this situation the victim could be lured by any seemingly innocuous link to pay bills online or read more about some topic. Most likely the user would have no clue that the router had been compromised, with all traffic—including sensitive passwords—being sent to someone else.

New Vectors of Exploitation

The early half of this decade saw extensive exploitation of stack, heap, and integer overflows, format-string vulnerabilities, and other weaknesses, most of which were relatively easy to exploit from a technical viewpoint. Now, however, most of these simple stack overflows are no longer a big threat in widely used software, such as Windows, because of superior software development and quality assurance testing. In addition, technologies like address space layout randomization have challenged hackers to go beyond traditional exploitation mechanisms.

Attacking vulnerabilities has entered a new phase, where exploiting concepts such as null pointers¹⁵ and race conditions¹⁶—as well as developing reliable exploitation techniques like heap spray¹⁷—are gaining popularity. Many of these bugs have been around for a long time and had been thought unexploitable.

This could be the perfect time for these techniques to leverage social engineering tricks as one of the attack vectors for several reasons:

- Currently there aren't any publicly known reliable, automated ways to exploit these new techniques (mainly for mass propagation)
- They can be easily tested on targeted individuals or groups via social engineering as a part of the development process
- The return on investment for these techniques is higher using social engineering than in putting the effort into further research to achieve mass propagation

Conclusion

With the recent trends in vulnerabilities, social engineering is a force that is difficult to combat. No matter how many protection mechanisms vendors implement in their software and operating systems, effective social engineering can subvert them all as long as users continue to click on any link that they come across. We can't expect cyber laws to thwart social engineering any time soon (except for filing charges for fraud), but increased education can definitely help minimize losses and the impact on unsuspecting victims.

In the meantime, think twice when you're asked to click to "accept" that prize you've just won!



Rahul Kashyap is the Manager, Vulnerability Research and IPS Security for McAfee Avert Labs. He is responsible for vulnerability research, zero-day analysis, intrusion prevention system content, and emergency response. Kashyap is a big Dilbert fan and hopes to start his own geeky security-focused comic strip some day.

ENDNOTES

- 1 <http://www.microsoft.com/technet/security/current.aspx>
- 2 "How to Configure Memory Protection in Windows XP SP2." <http://www.microsoft.com/technet/security/prodtech/windowsxp/depcnfxp.mspx>
- 3 "Analysis of GS protections in Microsoft Windows Vista." http://www.symantec.com/avcenter/reference/GS_Protections_in_Vista.pdf
- 4 "Browser Fuzzing for fun and profit." <http://blog.metasploit.com/2006/03/browser-fuzzing-for-fun-and-profit.html>
- 5 "Month of Browser Bugs," <http://blog.metasploit.com/2006/07/month-of-browser-bugs.html>
- 6 "AXFUZZ: An ActiveX/COM enumerator and fuzzer." <http://sourceforge.net/projects/axfuzz/>
- 7 "Hamachi," by H D Moore and Aviv Raff. <http://metasploit.com/users/hdm/tools/hamachi/hamachi.html>
- 8 "637 million Users Vulnerable to Attack," Frequency X. <http://blogs.iss.net/archive/TheWebBrowserThreat.html>
- 9 "Keep your operating system updated: Frequently asked questions." <http://www.microsoft.com/protect/computer/updates/faq.mspx>
- 10 "MS Office Flaws Ideal Tools for Targeted Attacks." http://blog.washingtonpost.com/securityfix/2006/04/ms_office_flaws_ideal_tools_fo_1.html
- 11 <http://www.gnucitizen.org/blog/0day-pdf-pwns-windows/>
- 12 "The New E-spying Threat." http://www.businessweek.com/print/magazine/content/08_16/b4080032218430.htm
- 13 "Dolphins' Web sites hacked in advance of Super Bowl." <http://www.networkworld.com/news/2007/020207-dolphins-web-sites-hacked-in.html>
- 14 "Hacking the interwebs," January 12, 2008. <http://www.gnucitizen.org/blog/hacking-the-interwebs/>
- 15 "Application-Specific Attacks: Leveraging the ActionScript Virtual Machine." http://documents.iss.net/whitepapers/IBM_X-Force_WP_final.pdf
- 16 "Unusual Bugs," Ilya van Sprundel. http://www.ruxcon.org.au/files/2006/unusual_bugs.pdf
- 17 "Heap Feng Shui in JavaScript." <http://www.determina.com/security.research/presentations/bh-eu07/bh-eu07-sotirov-paper.html>