McAfee®

Protect what you value.

McAfee Avert Labs
Top 10 Threat Predictions for 2008

Table of Contents

1. Adware on the Decline 3
2. Botnets Piggyback on Storm's Success 4
3. Crimeware and Phishing Move on to Secondary Targets 5
4. Instant Malware: A Different Kind of IM 5
5. Parasitic Crimeware Takes Root 6
6. Virtual Threat Growth to Outpace Real-World Growth 6
7. Virtualization Radically Changes Security 7
8. Windows Vista Joins the Party 8
9. VoIP Attacks Speak Up 9
10. Web 2.0: Interactivity Yields More Productive Malware 9

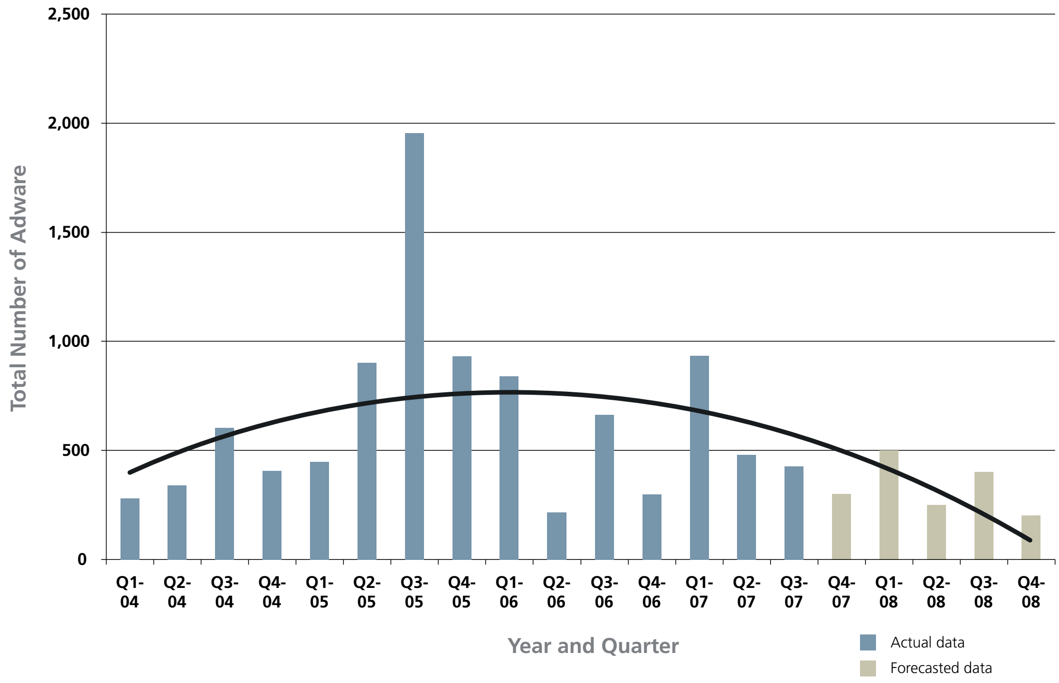
McAfee Avert Labs
Top 10 Threat Predictions for 2008

As 2007 comes to a close, it's a good time to reflect on the current threat landscape. The past 12 months comprised a record-breaking year. McAfee® recorded well over 100,000 new viruses and Trojans, a 50 percent jump in the total number of threats ever cataloged. The Nuwar virus (a.k.a. Storm Worm) grew into the largest peer-to-peer (P2P) botnet to date, while TJ Max revealed the largest data breach in history. Other areas saw significant growth as well, from phishing attacks to crimeware, from vulnerabilities disclosed to zero-day exploits; 2007 was a big year for threats. At the same time, there was an explosion in the adoption and usage of new technologies such as voice over IP (VoIP), virtualization, and, of course, Web 2.0. As we look ahead to 2008, we expect the threat landscape to continue to expand. Attackers will exploit the new technologies while revisiting tactics that were successful in the past. McAfee Avert® Labs has identified the following ten noteworthy trends expected to unfold in 2008:

1. Adware on the Decline

Adware will diminish in 2008. The combination of lawsuits, better defenses, and the negative connotation associated with advertising through adware helped start the decline of adware in 2006. In 2007, the Federal Trade Commission settled cases against several adware makers, the most important of which was Direct Revenue. With major players such as Direct Revenue and Claria out of the game, adware growth is expected to decline by 30 percent in 2008.

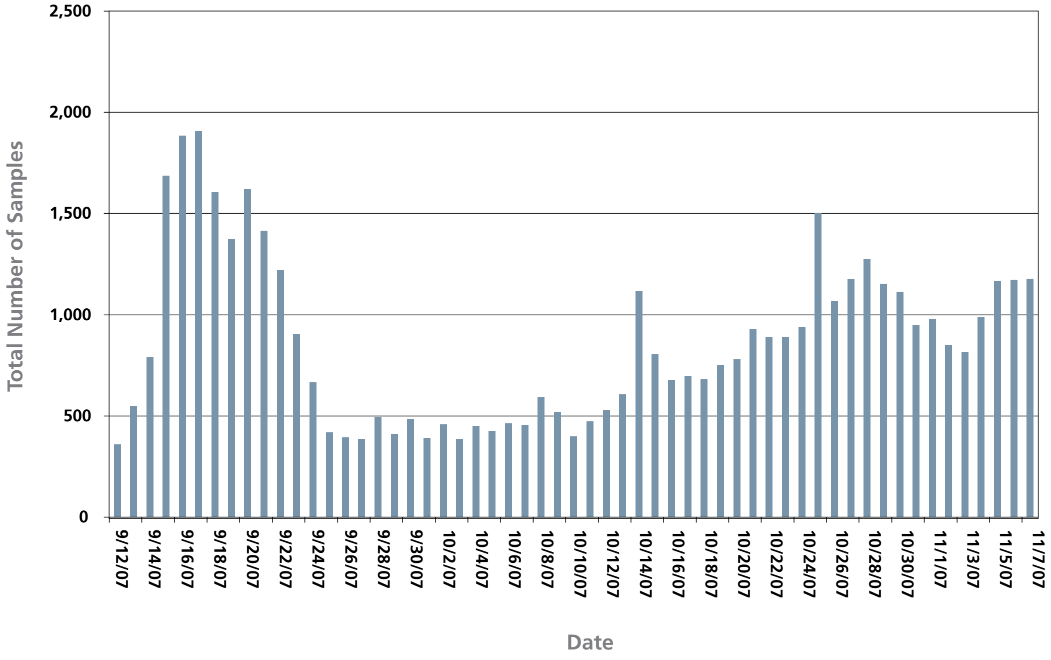
Adware Classified Per Quarter



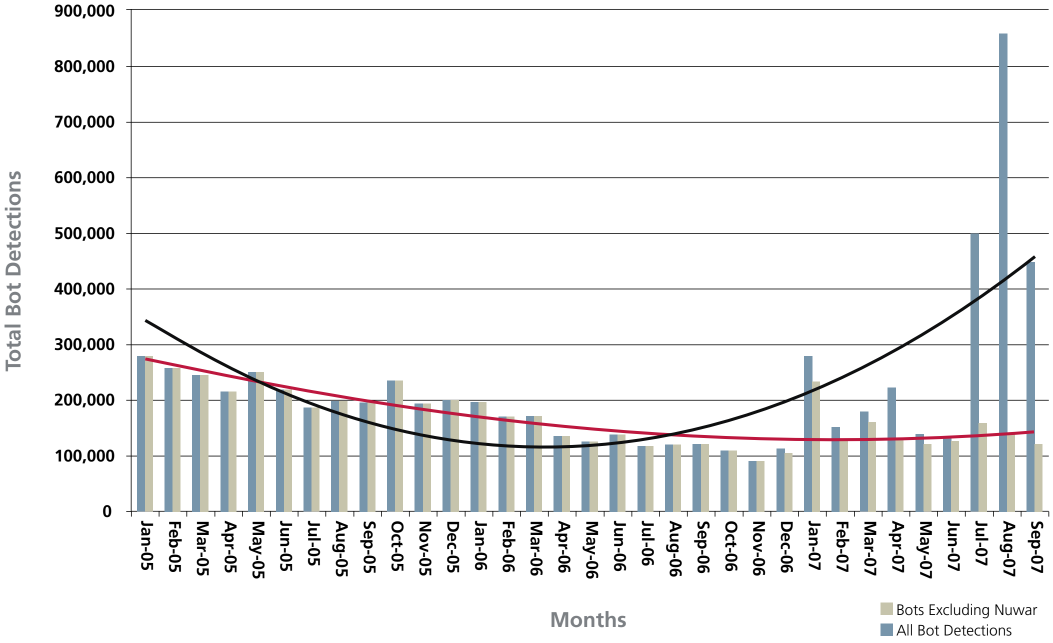
2. Botnets Piggyback on Storm's Success

Without a doubt, Nuwar (a.k.a. the Storm Worm) is the most versatile virus on record. The authors have released thousands of variants, and have changed coding techniques, infection methods, and social-engineering schemes far more often than for any other threat in history. While other bots have toyed with using P2P networks for command and control, Nuwar managed to successfully amass the largest-ever P2P botnet. With legal officials having prosecuted four high-profile bot masters in 2007, criminals will be seeking better ways to cover their tracks. McAfee Avert Labs expects other authors to take note and ride the coattails of Nuwar's success.

Unique Nuwar Samples Trapped Per Day By One Sensor



McAfee Consumer Bot Detections



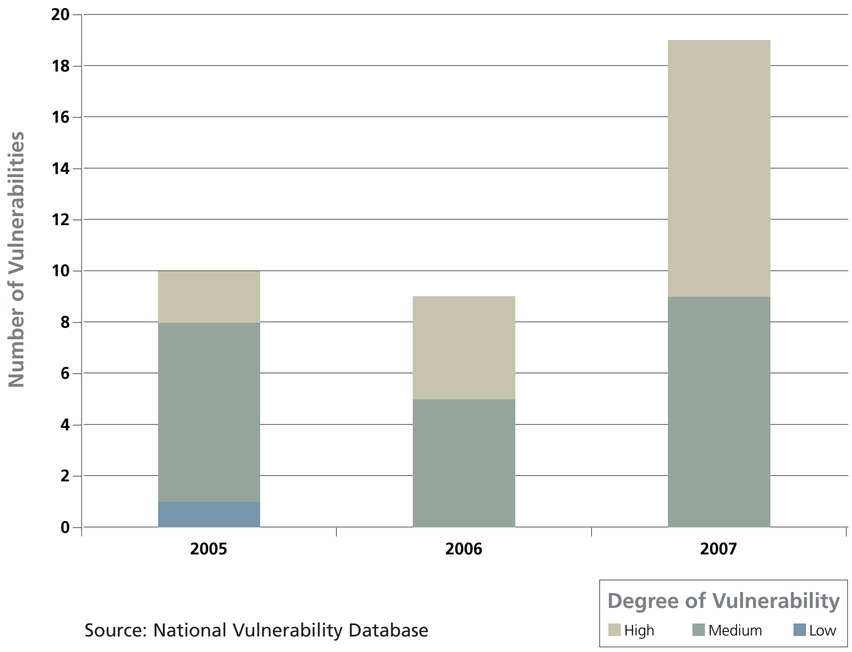
3. Crimeware and Phishing Move on to Secondary Targets

Cybercriminals have learned that it's risky to target top-tier sites, which are attacked regularly and are prepared to respond more quickly. Knowing that a large percentage of people reuse their user names and passwords, malware writers are likely to target less-popular sites more frequently than before. Criminals can then gain access to primary targets using information gained from secondary-target victims.

4. Instant Malware: A Different Kind of IM

For several years, researchers have warned of the risk of a self-executing instant-messaging (IM) worm. This threat could spawn millions of users and circle the globe in a matter of seconds. Although IM malware has existed for years, we have yet to see such a self-executing threat. While it's anyone's guess exactly when this threat will emerge, the stars may be starting to align. The National Vulnerability Database reports more than twice the number of AIM, YIM, and MSN Messenger vulnerabilities for 2007 over the prior year. More important, there were 10 high-severity risks in 2007, compared with zero in 2006. Additionally, the top IM virus families of 2005 and 2006 were replaced with new active threats, signifying an "out with the old and in with the new" milestone. With nearly a quarter-billion users, Skype suffered its first batch of worms in 2007. Many more are expected to follow.

Instant Messenger Vulnerabilities

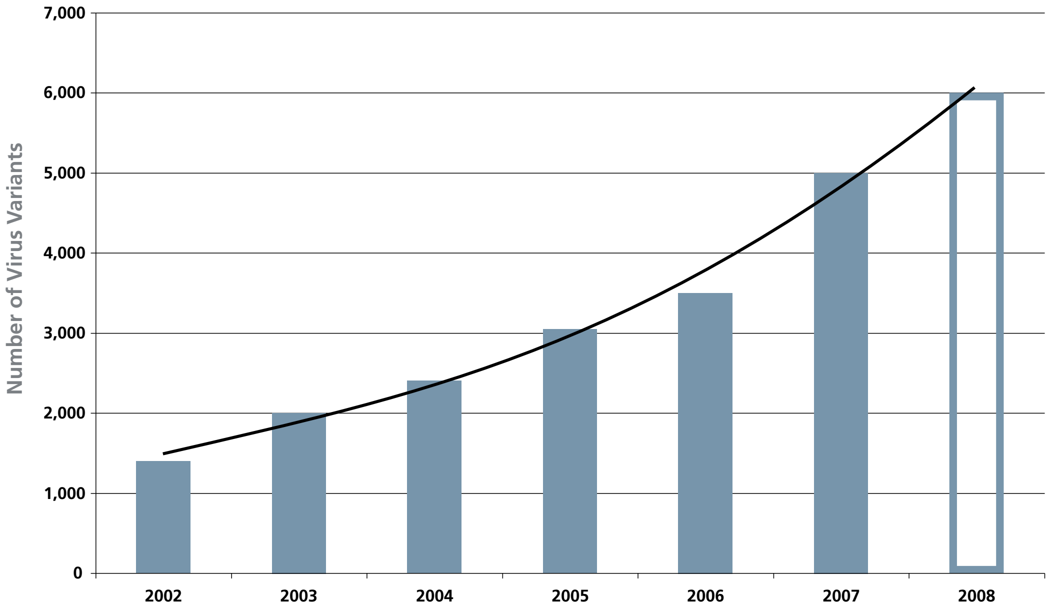


Source: National Vulnerability Database

5. Parasitic Crimeware Takes Root

While crimeware was storming ahead in recent years, parasitic malware faded to the background. In 2007, several crimeware authors turned old-school to deliver threats such as Grum, Virut, and Almanahe—parasitic viruses with a monetary mission. The number of variants of an old parasitic threat, Philis, grew by more than 400 percent; meanwhile, we cataloged more than 400 variants of a newcomer, Fujacks. The author of Fujacks was apprehended, yet we foresee a continued interest in parasitics from the crimeware community. Overall, we expect parasitic malware to grow by 20 percent in 2008.

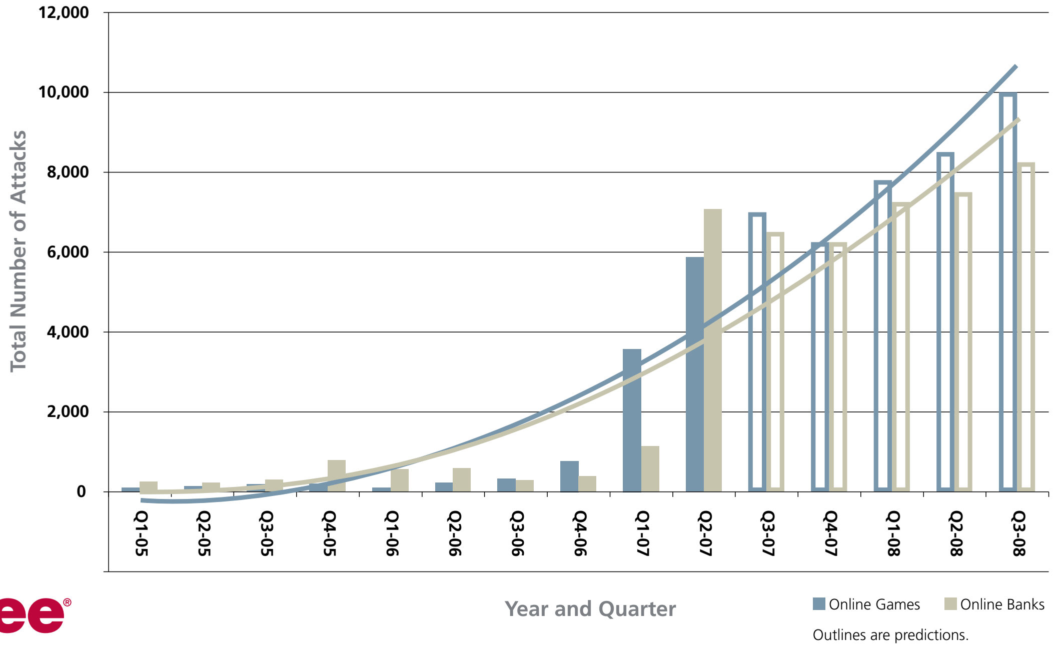
Parasitic Viruses



6. Virtual Threat Growth to Outpace Real-World Growth

As virtual objects continue to appreciate in value, more attackers will look to capitalize on the situation. We see this already in the number and type of password-stealing Trojans that were classified in 2007. These crimeware have two favorite targets: online gaming and banking.

Top Crimeware Targets Gaming and Banks

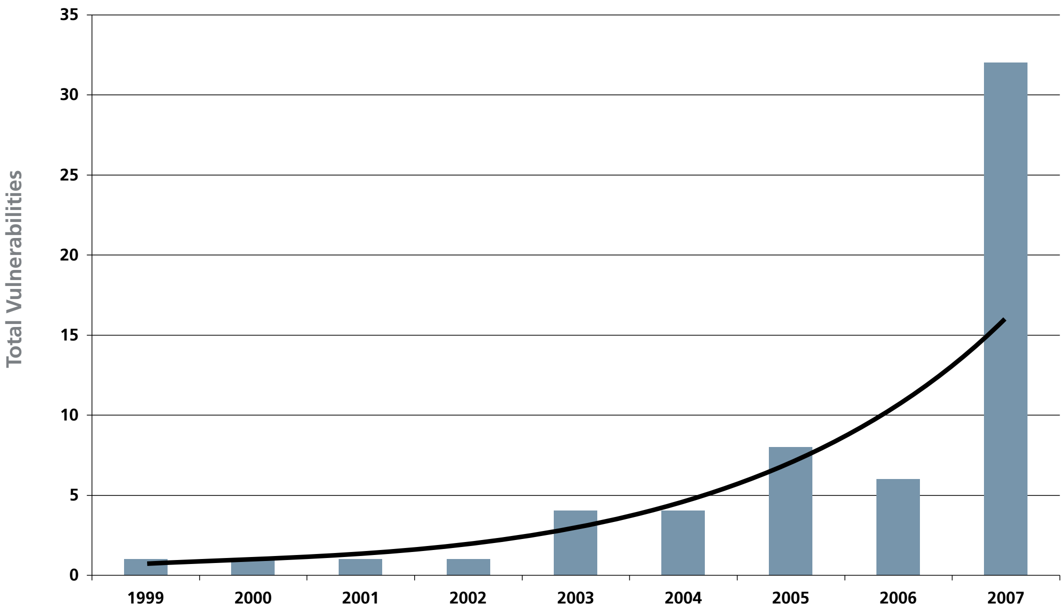


Outlines are predictions.

7. Virtualization Radically Changes Security

Security vendors will embrace virtualization to create more resilient defenses. Today's complex threats, such as rootkits, will be easily defeated, but researchers, professional hackers, and malware authors will begin looking at ways to circumvent this defensive technology. The number of VMware vulnerability records in the National Vulnerability Database increased fivefold between 2006 and 2007. Historically, such an increase in the application vulnerabilities we track has led to increased exploitation of those applications.

VMware Vulnerabilities



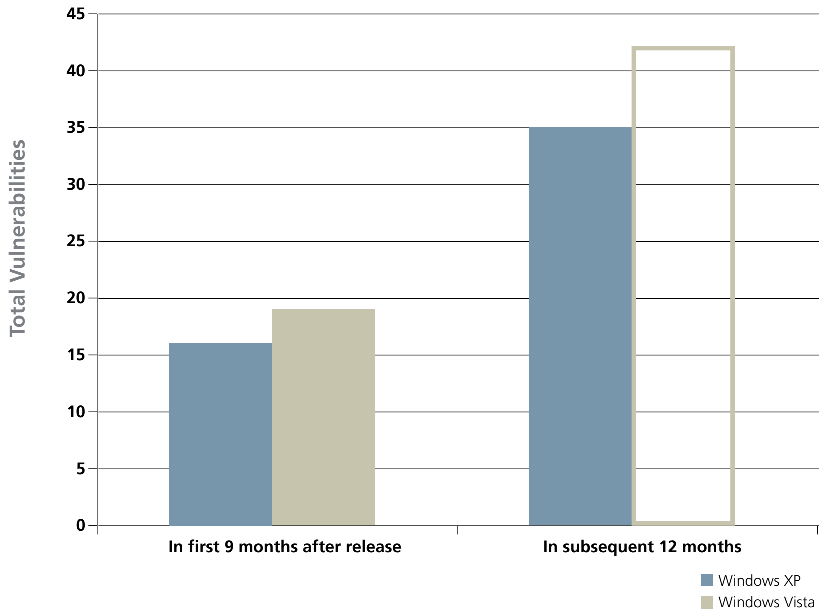
Source: National Vulnerability Database

8. Windows Vista Joins the Party

In 2007, the market share of Windows Vista sat below 10 percent.[1] This threshold will be crossed in 2008. The release of Service Pack 1 for Windows Vista is also likely to accelerate its adoption rate. Professional attackers and malware authors may begin to see an impact on their businesses and expend some effort in exploring ways to circumvent the new operating system. (This does not mean older threats will disappear, however. It was several years after the Java vulnerability named in Microsoft® Security Bulletin MS03-011 was patched before exploits targeting that vulnerability fell off the list of McAfee Avert Labs' top 10 threats to consumers.) The old threats will persist, but a new crop is on its way. The National Vulnerability Database reports 19 Windows Vista vulnerabilities in the first nine months after the OS was released. This compares with 16 Windows® XP vulnerabilities during a comparable period. The number of reported Windows XP vulnerabilities more than doubled in the following 12 months. If history repeats itself, we can expect far more than 20 Windows Vista vulnerabilities to be reported in 2008.

[1] *http://marketshare.hitslink.com/report.aspx?qprid=5*

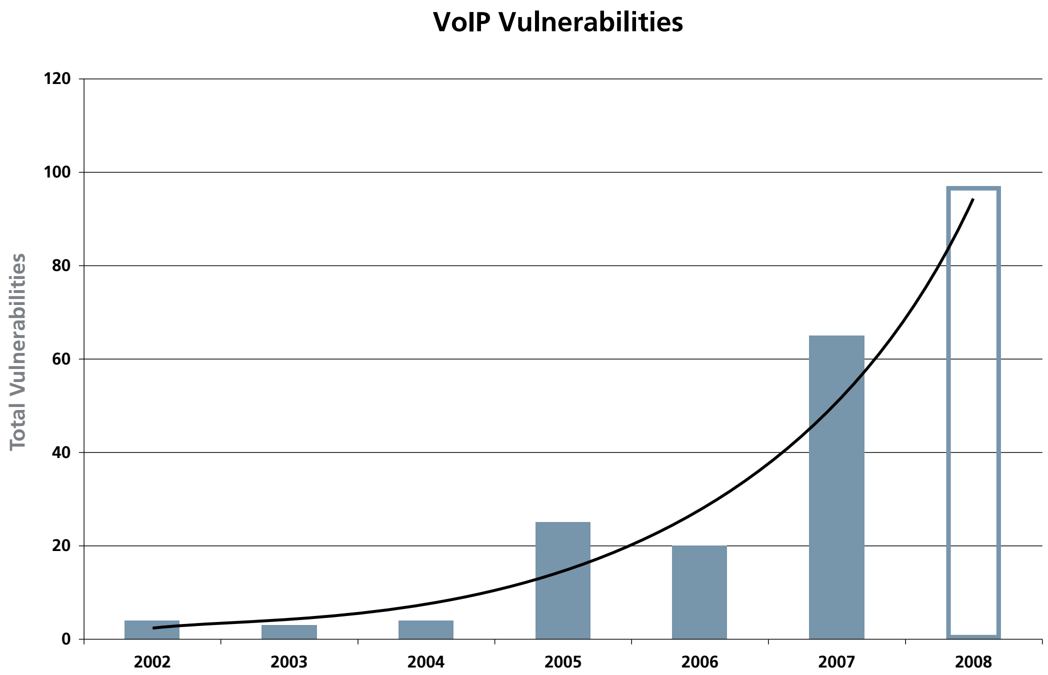
Windows Vulnerabilities



Source: National Vulnerability Database

9. VoIP Attacks Speak Up

VoIP attacks should increase by 50 percent in 2008. More than twice the number of VoIP-related vulnerabilities were reported in 2007 versus the previous year—several high-profile “vishing” attacks, and a criminal phreaking (or fraud) conviction—so it’s clear that VoIP threats have arrived and there’s no sign of a slowdown. Although ABI Research estimates 1.2 billion VoIP users by 2012 (with $150 billion annual service revenues), the technology is still new to many and implementing defense strategies is lagging.



Source: National Vulnerability Database

10. Web 2.0: Interactivity Yields More Productive Malware

Web 2.0 and social networking sites will be targeted in a big way. A number of social business sites were compromised in 2007, including Salesforce.com and Monster.com. Cybercriminals explored precision-targeted attacks using personal information gleaned from sites such as LinkedIn. Attackers pursue the tidbits of information users share about themselves to help make their threats feel more authentic. McAfee Avert Labs believes these examples are not isolated events, but rather the beginning of a trend in which proficient attackers are data mining this wealth of personal information.

Another cause for concern is an increase in spam that targets social networking sites. This blog spam is growing at an alarming rate. In March 2007, *WebmasterWorld* reported that 75 percent of Google’s Blogspot blogs are spam. Automated posting tools are maturing; spammers are moving on to audio and video spam. Blog spam will continue to grow in 2008, and video spam is likely to become significant. In many cases video spam will be obvious to most viewers, but well-crafted videos will blur the lines between spam and advertising.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888.847.8766
www.mcafee.com