Microsoft | Security Intelligence Report

# The evolution of malware and the threat landscape – a 10-year review

Microsoft Security Intelligence Report: Special Edition

February, 2012

## MICROSOFT SECURITY INTELLIGENCE REPORT: SPECIAL EDITION



## Authors and contributors

BILL BARLOWE – *Microsoft Security Response Center*
JOE BLACKBIRD – *Microsoft Malware Protection Center*
WEIJUAN SHI DAVIS – *Windows Product Management Consumer*
JOE FAULHABER – *Microsoft Malware Protection Center*
HEATHER GOUDEY – *Microsoft Malware Protection Center*
PAUL HENRY – *Wadeware LLC*
JEFF JONES – *Microsoft Trustworthy Computing*
JIMMY KUO – *Microsoft Malware Protection Center*
MARC LAURICELLA – *Microsoft Trustworthy Computing*
KEN MALCOMSON – *Microsoft Trustworthy Computing*
NAM NG – *Microsoft Trustworthy Computing*
HILDA LARINA RAGRAGIO – *Microsoft Malware Protection Center*
TIM RAINS – *Microsoft Trustworthy Computing*
ELIZABETH SCOTT – *Microsoft Security Response Center*
JASMINE SESSO – *Microsoft Malware Protection Center*
JOANNA SHARPE – *Microsoft Trustworthy Computing*
FRANK SIMORJAY – *Microsoft Trustworthy Computing*
HOLLY STEWART – *Microsoft Malware Protection Center*
STEVE WACKER – *Wadeware LLC*

In memory of TAREQ SAADE

## Contents

# Foreword

## Scope

The *Microsoft Security Intelligence Report (SIR)* focuses on software vulnerabilities, software vulnerability exploits, malicious, and potentially unwanted software. Past reports and related resources are available for download at www.microsoft.com/sir. We hope that readers find the data, insights, and guidance in this special edition of the *SIR* useful in helping them protect their organizations, software, and users.

## Reporting period

This special edition of the *SIR* provides summarized information from the last 10 years. Where possible, this report includes trend data for the full 10-year period; when data for the full 10-year period is not available, trend data for shorter periods is provided. Generally, because vulnerability disclosures can be highly inconsistent from quarter to quarter and often occur disproportionately at certain times of the year, statistics about vulnerability disclosures are presented on a half-yearly basis, as in recent volumes of the *SIR*.

Throughout the report, half-yearly and quarterly time periods are referenced using the nHyy or nQyy formats, respectively, where yy indicates the calendar year and n indicates the half or quarter. For example, 1H11 represents the first half of 2011 (January 1 through June 30), and 2Q11 represents the second quarter of 2011 (April 1 through June 30). To avoid confusion, please note the reporting period or periods being referenced when considering the statistics in this report.

## Conventions

This report uses the Microsoft Malware Protection Center (MMPC) naming standard for families and variants of malware and potentially unwanted software. For information about this standard, see the Microsoft Malware Protection Center Naming Standards page on the MMPC website.

## Introduction

As the Internet has extended its reach over the last 10 years, malware (malicious software) has evolved and become more complex. Early forms of malware sought to generate high-profile nuisance attacks, but today its aims are increasingly pernicious, focusing on theft and other illicit activities. Malware has become much more of a concern for organizations; Internet connectivity was still the exception to the rule for many organizations before 2002, but it quickly became the norm as the first decade of the 21st century unfolded.

Today, in addition to individual computers and the networks of organizations both large and small, Internet connectivity also extends to devices such as gaming consoles and smartphones. And as computing paradigms shift, protecting organizations, governments, and citizens from malware has become even more of a challenge.

Microsoft Trustworthy Computing, established in 2002, publishes the *Microsoft Security Intelligence Report (SIR)* to help keep customers and other interested parties informed about the changing threat landscape. The *SIR* provides comprehensive threat intelligence from around the world.

## Personal computing in 2002 and today

Even as malware and other significant challenges emerged, computer users continued to enjoy the benefits of technological innovation over the last 10 years. This section paints a basic "then and now" portrait of the state of computing in 2002 and today in 2012 in three areas: PCs, mobile computing, and online services, the precursor to the cloud.

### PCs

By 2002, PC CPUs used a single-core architecture and had just surpassed 2.0 GHz in processing speed. Windows XP, which was released in late 2001, required 64 MB of RAM but 128 MB was recommended; 512 MB was a fairly common configuration. Hard disk drives ranged to 120 GB in size, and LCD monitors were becoming increasingly popular. USB connectivity for peripheral devices was widespread, but the much faster USB 2.0 specification had only recently been ratified and was therefore not yet available.

At the outset of 2012, multi-core CPUs are common and speeds have surpassed the 4.0 GHz mark, several times faster than systems available in 2002. Windows 7, released in 2009, requires 1 GB of RAM but 2 GB is recommended. Typical hard disk drives range from 600 GB, a five-fold increase from 2002, to 1 TB or more in size. It's possible to obtain a 23-inch monitor for less than $200 USD in the United States, and monitors built with LED technology (an improvement over the older LCD technology) are widely available. USB 3.0 is the emerging connectivity technology, but USB 2.0 is still the most widely used standard.

### Mobile computing

In 2002, the fastest laptop CPUs had barely broken the 1.0 GHz mark. 512 MB of RAM was a common configuration, along with a 20 GB to 30 GB hard disk drive. Combination DVD/CD-RW drives were still a rarity and CD-ROM drives were still the norm. Sound quality and high-definition (HD) displays were still on users' wish lists, and smartphones did not emerge until 2005.

In 2012, laptop PC CPUs are three times as fast as those available in 2002; 3.0+ GHz clock speeds are widely available. Generally, 2 GB to 4 GB of RAM is available—4 to 8 times the amount in 2002—but high-end laptops offer as much as 8 GB. Typical hard disk drives range from 500 GB to 600 GB, some 25 times greater than laptop drives available in 2002, and new solid-state hard disk drives are significantly faster. HD displays with built-in webcams and facial recognition technology (in lieu of passwords) are a reality. DVD/RW drives are standard, and many support the high-resolution Blu-ray Disc technology for video playback. However, such accessories are being

sacrificed in some models to create very thin and lightweight laptops. High-quality audio options are also increasingly common.

Ethernet data transmission speed standards have continued to evolve. Gigabit Ethernet—which supports a data transmission rate of 1,000 megabits per second (Mbps)—became widely available during the decade, and 10 Gigabit Ethernet became certified as a standard by the Institute of Electrical and Electronics Engineers (IEEE). However, these standards apply to copper wire, cable (coaxial wire), and fiber optic connections. The widespread proliferation of wireless network connectivity, which accommodates the growing number of mobile devices that are available today, also occurred during the 2002–2012 time period. In 2012, both desktop and laptop computers typically offer wired and wireless connectivity options.

## Online services (precursor to the cloud)

From a consumer's perspective, a number of online payment services were available by 2002. These services facilitated the growth of Internet commerce (e-commerce) sites such as Amazon.com and eBay, both of which had been open for business since 1995. E-commerce exploded in popularity between 2002 and 2012.

A significant phenomenon occurred during the decade that had a considerable effect on popular culture and the entertainment industry. As music and video became available as digitized computer files, they also became shareable over the Internet. Napster, perhaps the most well-known file-sharing service, emerged in 1999 and ceased trading in July 2001. However, other file-sharing models also emerged and became popular.

The growth of the Internet and the emerging availability of broadband connectivity also resulted in online services such as Rhapsody, the first streaming on-demand music subscription service for a monthly fee, which was launched in December 2001.

Although the concept of cloud computing had existed for some time, the first cloud computing services became commercially available in 2002. Since that time, more flexible options have emerged that make cloud computing more attractive and feasible for large and small organizations alike, as well as for individuals. Cloud computing architectures currently include infrastructure as a service (IaaS), which provides components such as networking and storage; platform as a service (PaaS), which provides a platform such as a database or a web server for running applications; and software as a service (SaaS), which provides a software application or solution as a finished or complete service.

In 2012 there is little disagreement about the likelihood of cloud computing as the next significant computing paradigm. The technology is gaining acceptance from many organizations and cloud computing models continue to evolve.

## The origins of malware

Malware became known to many computer users through widespread infections caused by Melissa (in 1999) and LoveLetter (in 2000). Both were email-based, and LoveLetter spread via an infected email attachment. When the attachment was opened, the malware overwrote a variety of different types of files on the user's PC and emailed itself to others in the user's email address book.

LoveLetter quickly became the most costly incident of its kind to that point in time. Despite the damage that Melissa and LoveLetter caused, it could be argued that they had three positive effects: they caused computer malware to come under increasing scrutiny; they increased social awareness about computer malware (through peer pressure from many upset message recipients); and they underscored the importance of backups (because LoveLetter overwrote files which were lost if backups were not available).

A more devious and direct malware threat emerged into prominence in 2001: malware that could spread without any human interaction. One such form of malware was a worm, known as Code Red, which was released on the Internet in July of 2001 and which targeted servers running Microsoft Internet Information Services (IIS). Although worms had been detected since at least 1988, Code Red was considered by Microsoft Malware Protection Center (MMPC) researchers to be a perfect example of a worm because there was no file component. Code Red needed to be detected in transit or in the memory of an infected computer; at the time, traditional desktop antimalware products that looked for file-based malware could not detect it.

Code Red spread via TCP port 80, the same channel that is commonly used for Internet web queries, so web servers needed to be secured against such attacks. However, other computers require access to port 80 for web browser functionality. Code Red may not have caused as much damage as LoveLetter, although this is difficult to ascertain because some computers infected with Code Red were subsequently infected with Win32/Nimda, which also spread via TCP port 80.

Win32/Nimda was what some call a malware cocktail, or a blended threat—the start of a trend in malware development that continues to this day. It used at least five different attack vectors, including making use of backdoors left by previous malware. Because it followed so closely on the

heels of such malware, not much time was available for it to be developed. Therefore, it was widely believed that Win32/Nimda was developed by a team of people, not just a solitary malware coder.

Regardless of who created it, Win32/Nimda demonstrated that if networked computers are left unprotected they can be commandeered and used against their owners in a matter of hours, perhaps even minutes. Hundreds of thousands of computers were overcome by Win32/Nimda, many of which operated well-known websites and mail servers for medium to large companies. In total, more than 50,000 important Internet sites were infected. And more than one person noted that Win32/Nimda was released on Sept. 18, just one week after the terrorist attacks of Sept. 11, 2001, a fact that made many security experts uneasy.

In addition, 2001 saw the emergence of malware from email messages that appeared to be innocuous. Such malware emerged from messages that had no code or files attached—they used URLs instead. These messages would use social engineering tactics to entice users to click the URLs, which would then connect users to websites that were programmed with exploits designed to perform undesirable actions on the users' PCs.

2001 also saw the emergence of Win32/Sircam, the first widespread malware that exfiltrated information from computers, although it is not known whether this was the intent of the malware. However, the Ukrainian President's private itinerary was unexpectedly published publicly as a result of a Win32/Sircam infection.

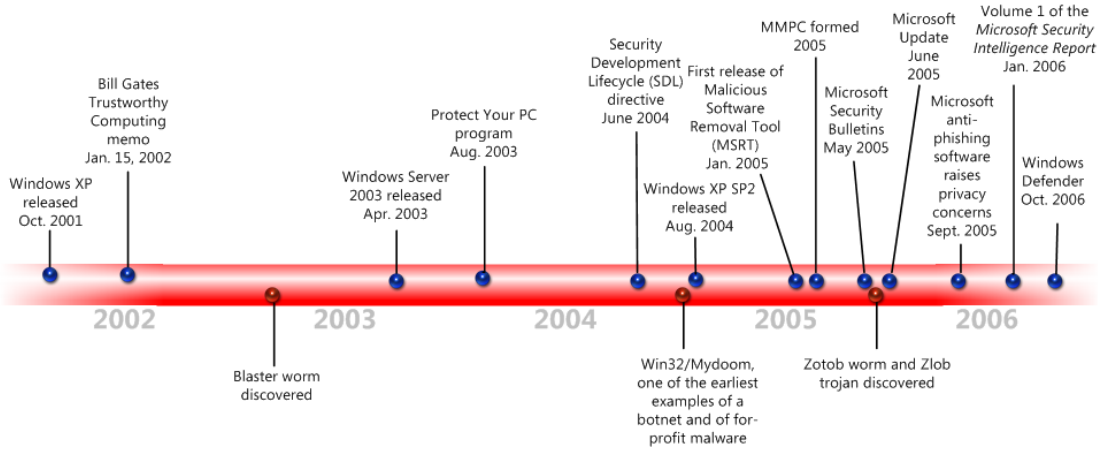
## Microsoft Trustworthy Computing

On January 15, 2002, the chairman of the board of directors at Microsoft, Bill Gates, sent a memo to all full-time employees of Microsoft and its subsidiaries. This memo proposed a fundamental shift in the company's approach to a central component of its business, a concept called Trustworthy Computing (TwC).

TwC is Microsoft's commitment to provide more secure, private, and reliable computing experiences based on sound business practices. Most of the intelligence that TwC publishes in the *SIR* comes from three security centers—the Microsoft Malware Protection Center (MMPC), the Microsoft Security Response Center (MSRC), and the Microsoft Security Engineering Center (MSEC)—which deliver in-depth threat intelligence, threat response, and security science. Additional information comes from product groups across Microsoft and from Microsoft IT (MSIT), the group that manages global IT services for Microsoft. The *SIR* is designed to give Microsoft customers, partners, and the software industry a well-rounded understanding of the threat landscape to help them to protect themselves and their assets from criminal activity.

The following figure shows significant actions and milestones during the first five years of TwC's existence, as well as some significant malware-related events.

**Figure 1. Significant events and milestones in the threat landscape from 2002 thru 2006**




### 2002-2003

The era of mass mailing malware that began with Melissa and LoveLetter extended to the 2002-2003 timeframe and caused significant increases in the volume of spam; much of this malware

used macros and Microsoft Visual Basic scripting functionality. Most of this malware was defeated by security features in the Microsoft Office XP version of Microsoft Excel and the Office 2003 version of Microsoft Word, when these programs adopted XML formats for their data files.

In 2003 Microsoft started its regular monthly process for issuing security updates, which continues today. Microsoft began this program to provide timely updates to customers on a regularly scheduled basis. Some updates are security related, but not all. Security updates are provided on the second Tuesday of each month, and optional updates as well as non-security updates are provided on the fourth Tuesday of each month.

### 2004

Microsoft released Windows XP Service Pack 2 (SP2) in 2004, which contained extensive security updates and improvements. SP2 was the result of considerable effort by Microsoft developers and security experts. It was perhaps the clearest indication from Microsoft to that point in time of how seriously the company was concerned about the growing problem of malware through the global connectivity of the Internet. SP2 was a significant accomplishment and a milestone in the journey that Microsoft and the rest of the industry is on to protect technology users from criminals.

2004 was also the year that the first significant for-profit malware emerged. The mass-mailing worm family Win32/Mydoom created one of the earliest examples of a *botnet*—a set of computers that are secretly and illicitly controlled by an attacker, who orders them to perform activities such as sending spam, hosting pages used in phishing attacks, stealing passwords or sensitive information, and distributing other malware.

## The criminalization of malware

Many of the early forms of malware were disruptive and costly in terms of cleanup costs and lost productivity, but most were created as pranks or as a means of raising the creators' status in the online hacker community. With the emergence of Win32/Mydoom in 2004, it became apparent that malware creators had seized on the opportunities malware provided for theft, blackmail, and other for-profit criminal activities.

### 2005

In 2005 the Win32/Zotob worm was released. Win32/Zotob was not as widespread as originally anticipated. It sought to reduce the security settings in Windows Internet Explorer and impede its pop-up blocking functionality to display ads for websites that would pay hackers for hits—another example of malware for profit.

Late in 2005 the Win32/Zlob trojan began spreading. It displayed pop-up ads that warned users about spyware and encouraged them to purchase fake antispyware, which actually redirected users to other sites and caused other problems. Win32/Zlob was yet another indicator that the days of malware pranksters were yielding to criminals motivated by potential profits. (For more information about Win32/Zlob, see the "How threats have evolved over time" section later in this paper.)

Prior to 2005, Microsoft released security updates to address specific forms of malware. For example, Microsoft Security Bulletin MS02-039, which addressed the malware known as Slammer, was made available in July of 2002. In January 2005, Microsoft released the first version of the Malicious Software Removal Tool (MSRT), which removes specific prevalent malicious software from computers running recent versions of Windows. Microsoft makes a new version of the MSRT available every month for automatic download to users' computers via Windows Update/Microsoft Update, after which it runs one time to check for and remove malware infections.

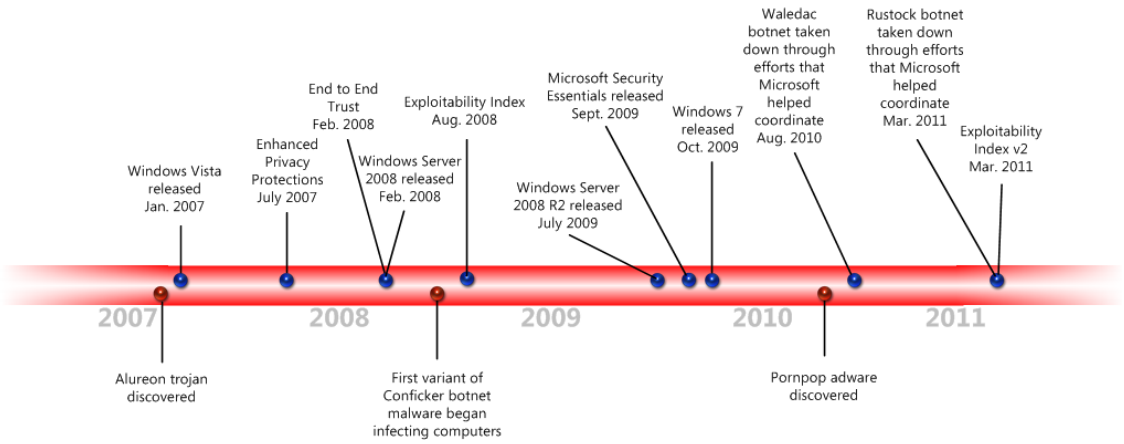
The consistent and automatic availability of the MSRT helps maintain a cleaner computing ecosystem. For example, in the first half of 2011 the MSRT ran on an average of more than 600 million individual computers around the world each month. However, the MSRT does not replace a preventive antimalware product; it is strictly a post-infection removal tool. Microsoft strongly recommends use of an up-to-date preventive antimalware product.

As technically sophisticated and organized criminals started leveraging technology to take advantage of technology users, the MMPC was established in 2005 with a twofold mission: to help protect Microsoft customers from emerging and existing threats, and to provide world-class antimalware research and response capabilities to support Microsoft security products and services.

More recently, Microsoft established the Microsoft Digital Crimes Unit (DCU), a worldwide team of lawyers, investigators, technical analysts, and other specialists. The mission of the DCU is to make the Internet safer and more secure through strong enforcement, global partnerships, policy, and technology solutions that help defend against fraud and other threats to online safety and also to protect children from technology-facilitated crimes.

The following figure shows some significant milestones during the second five years of TwC's existence, as well as some significant malware-related events.

Figure 2. Significant events and milestones in the threat landscape from 2007 thru 2011




In addition to creating the MMPC and the DCU, Microsoft has worked to foster deeper industry collaboration and share the lessons learned to help others with their security efforts. One such example is the Industry Consortium for Advancement of Security on the Internet (ICASI), which Microsoft cofounded in June of 2008 with Intel Corporation, IBM, Cisco Systems, and Juniper Networks. Since its founding, Amazon.com and Nokia have also become members.

ICASI fosters collaboration among global companies with the goal of addressing complex security threats and better protecting the critical IT infrastructures that support the world's organizations, governments, and citizens.

# Vulnerabilities

Vulnerabilities are weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of that software or the data it processes. Some of the worst vulnerabilities allow attackers to exploit a compromised computer, causing it to run arbitrary code without the user's knowledge.

The past 10 years represent a very interesting timeframe for reviewing vulnerability disclosures and ensuing changes that continue to affect risk management in IT organizations around the world. Before examining the charts and trends, a brief review of the past decade with regard to industry vulnerabilities is in order.

## A decade of maturation

In 2002 MITRE[1] presented A Progress Report on the CVE Initiative (PDF), which provided an update on a multi-year effort to create a consistent and common set of vulnerability information—with a particular focus on unique naming—to enable the industry to easier assess, manage, and fix vulnerabilities and exposures. The CVE effort and data later formed the core of the National Institute of Standards (NIST) National Vulnerability Database (NVD), the U.S. government repository of standards-based vulnerability management data that serves as the primary vulnerability index for industry vulnerabilities referenced in the *SIR*.

2002 also marked the beginning of a commercial market for vulnerabilities; iDefense started a vulnerability contributor program that paid finders for vulnerability information.

In 2003, the U.S. National Infrastructure Advisory Council (NIAC) commissioned a project "to propose an open and universal vulnerability scoring system to address and solve these shortcomings, with the ultimate goal of promoting a common understanding of vulnerabilities and their impact." This project resulted in a report recommending the adoption of the Common Vulnerability and Scoring System (PDF) (CVSSv1) in late 2004. Vulnerability severity (or scoring) information was a big step forward, because it provided a standard method for rating vulnerabilities across the industry in a vendor-neutral manner.

2007 brought an update to CVSS, with changes that addressed issues identified by the practical application of CVSS since its inception. *SIR* volume 4, which provided data and analysis for the second half of 2007, included vulnerability trends using both CVSSv1 and CVSSv2, and since then

[1] MITRE is a not-for-profit company that works in the public interest to provide systems engineering, research and development, and information technology support to the U. S. government.

CVSSv2 ratings have been used. As noted at the time, one practical effect of the new ratings formulas was that a much higher percentage of vulnerabilities were rated High or Medium severity.

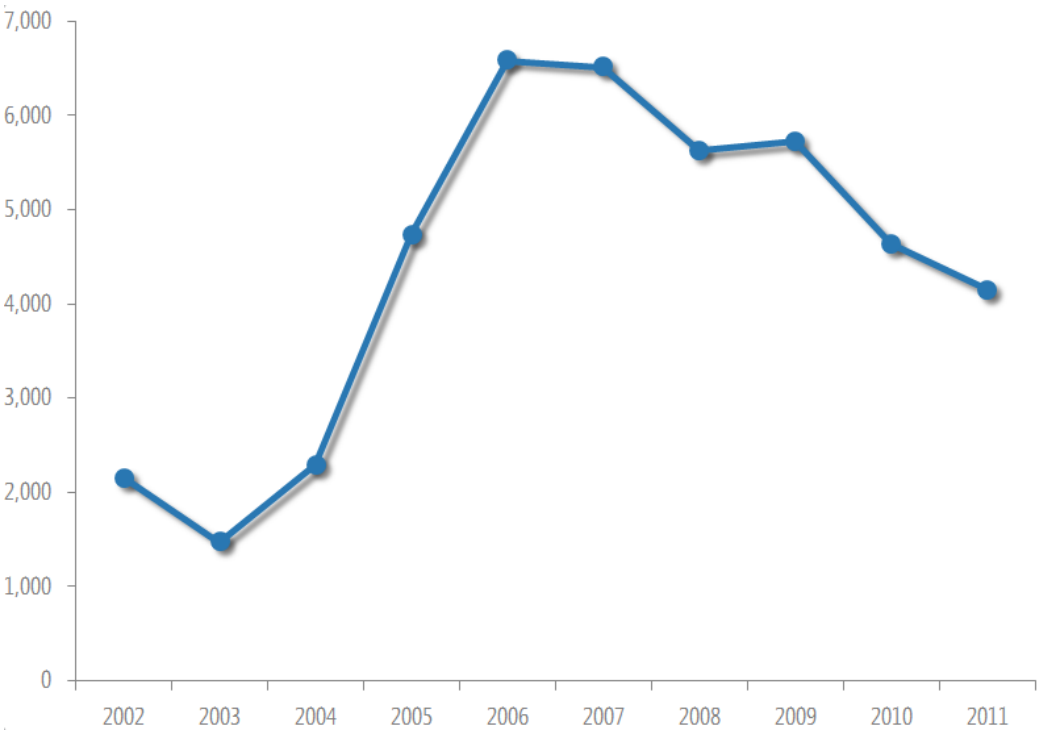
## Industry-wide vulnerability disclosures

A *disclosure*, as the term is used in the *SIR*, is the revelation of a software vulnerability to the public at large. It does not refer to any type of private disclosure or disclosure to a limited number of people. Disclosures can come from a variety of sources, including the software vendor, security software vendors, independent security researchers, and even malware creators.

Much of the information in this section is compiled from vulnerability disclosure data that is published in the NVD. It represents all disclosures that have a CVE (Common Vulnerabilities and Exposures) number.

The past decade has seen drastic growth in new vulnerability disclosures, which peaked in 2006 and 2007 and then steadily declined over the next four years to just over 4,000 in 2011, which is still a large number of vulnerabilities.

**Figure 3. Industry-wide vulnerability disclosures since 2002**



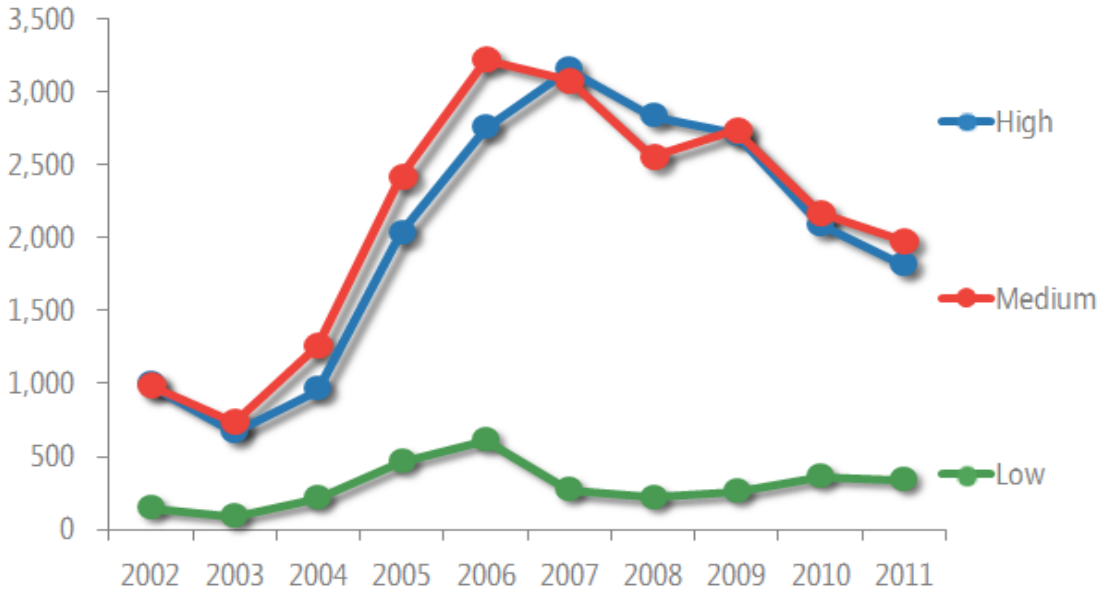
Vulnerability disclosure trends:

- Vulnerability disclosures across the industry in 2011 were down 11.8 percent from 2010.
- This decline continues an overall trend of moderate declines. Vulnerability disclosures have declined a total of 37 percent since their peak in 2006.

## Vulnerability severity

The Common Vulnerability Scoring System (CVSS) is a standardized, platform-independent scoring system for rating IT vulnerabilities. The CVSS assigns a numeric value between 0 and 10 to vulnerabilities according to severity, with higher scores representing greater severity. (See the Vulnerability Severity page on the *SIR* website for more information.)

**Figure 4. Relative severity of vulnerabilities disclosed since 2002**



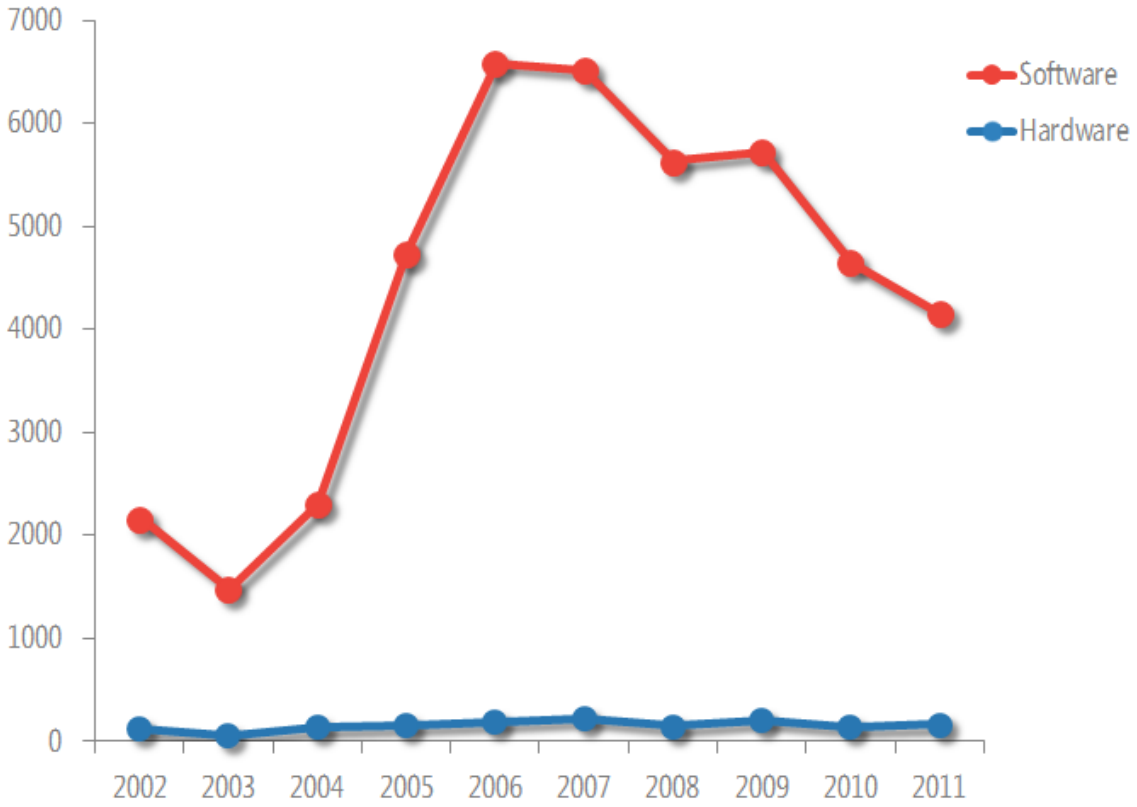

Vulnerability severity trends:

- The overall vulnerability severity trend has been a positive one. Medium and High severity vulnerabilities have steadily decreased since their high points in 2006 and 2007.
- Even as fewer vulnerabilities are being disclosed overall, the number of Low severity vulnerabilities being disclosed has been relatively flat. Low severity vulnerabilities accounted for approximately 8 percent of all vulnerabilities disclosed in 2011.

## Hardware and software disclosures

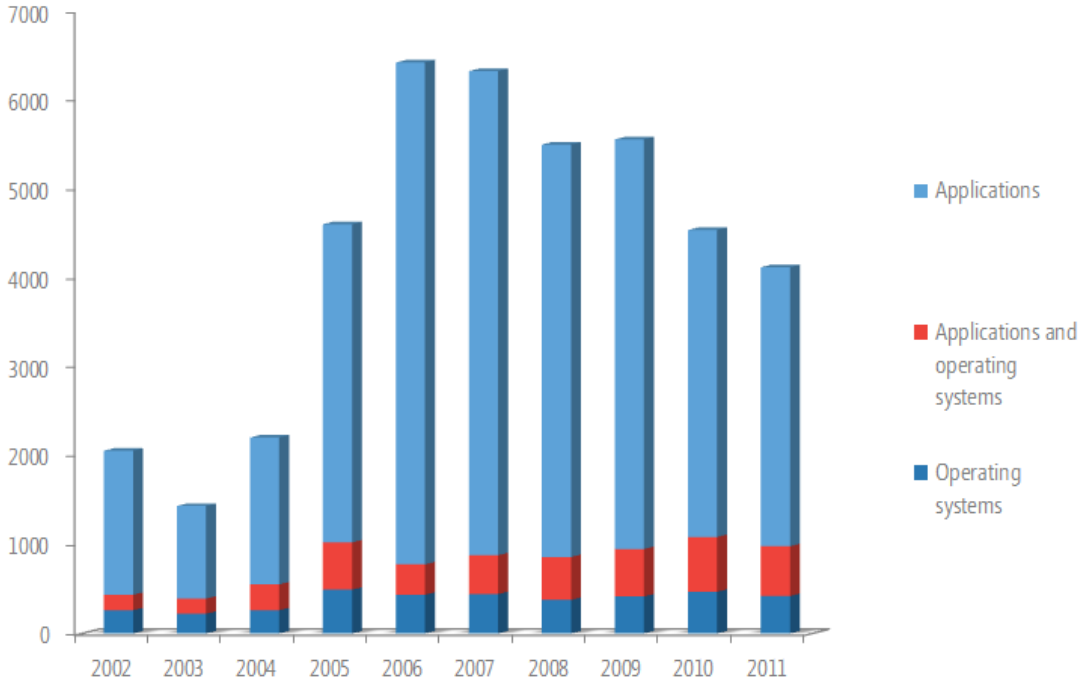
The NVD tracks both hardware and software vulnerabilities. The number of hardware vulnerabilities disclosed each year remains low, as shown in the following figure. The peak number was 198 (3.4 percent) hardware vulnerabilities disclosed in 2009.

**Figure 5. Hardware and software vulnerability disclosures since 2002**




Software vulnerabilities consist of vulnerabilities that affect operating systems, applications, or both. As in many other industries, one vendor's product can be another vendor's component. For example, CVE-2011-1089 affects GNU libc 2.3, which is listed as an application product from GNU. However, libc is also an integrated component in several operating systems and is therefore also an operating system vulnerability. For this reason, it is difficult to draw a distinct line between operating system and application vulnerabilities. In the following figure, vulnerabilities that affect both operating systems and applications are shown in red.

Figure 6. Application and operating system vulnerability disclosures since 2002

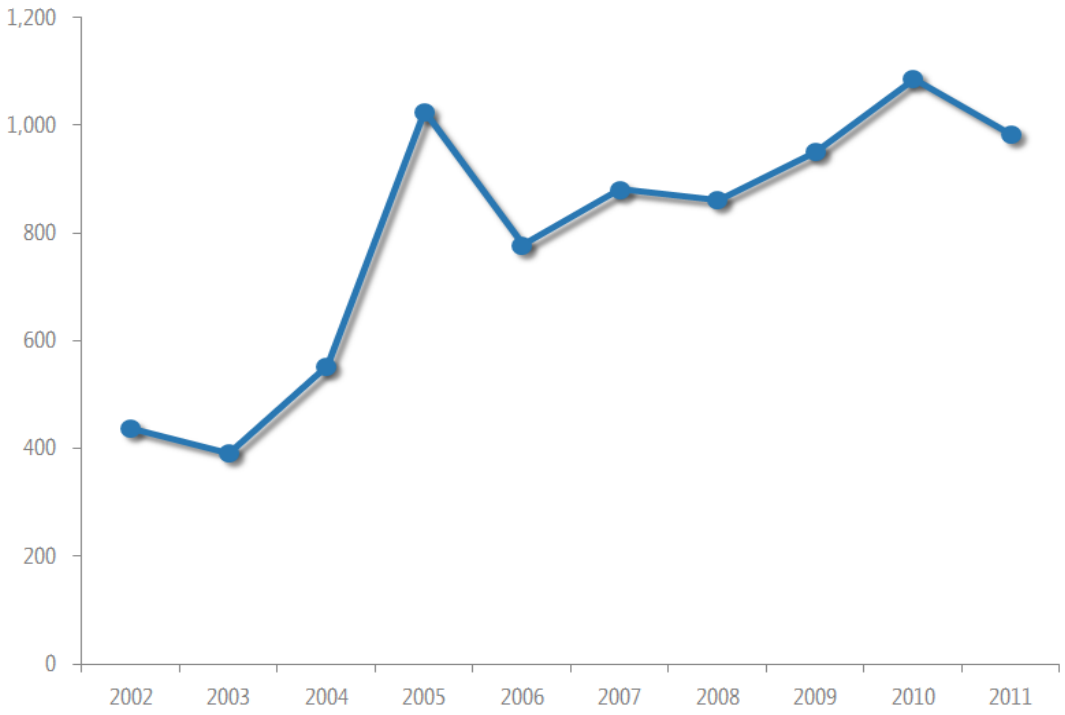



In 2010 and 2011, approximately 13 percent of software vulnerabilities affected both application and operating system products.

## Operating system vulnerability disclosures

To determine the number of vulnerabilities that affect operating systems (shown in the following figure), vulnerabilities were filtered for affected products that were designated as operating systems in the NVD.

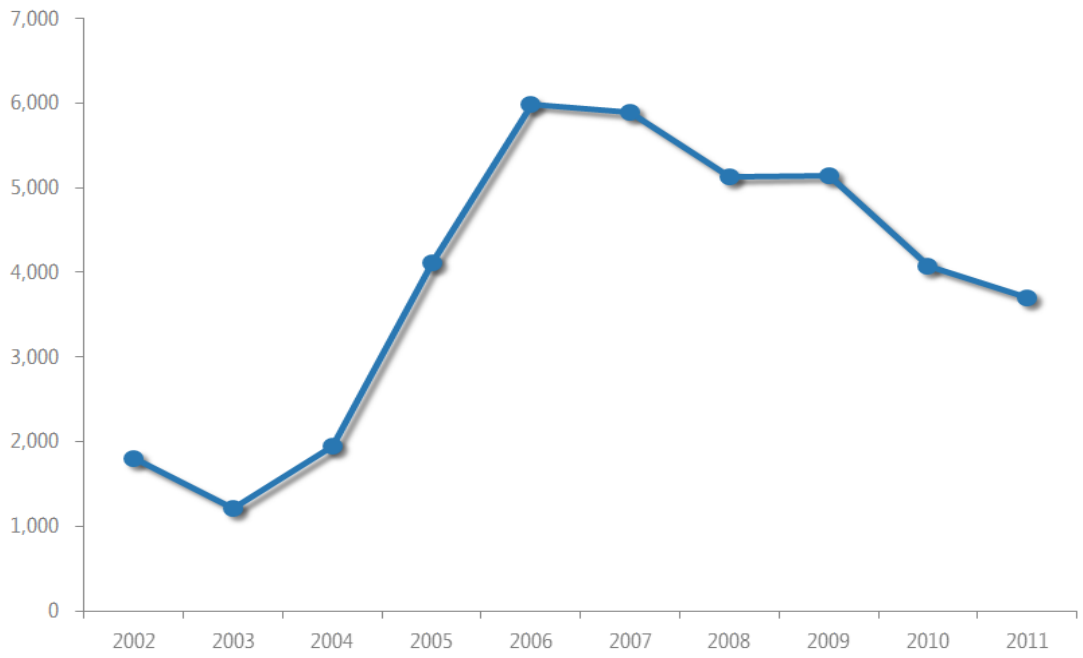
Figure 7. Operating system vulnerability disclosures since 2002




## Application vulnerability disclosures

To determine the number of vulnerabilities that affect applications (shown in the following figure), vulnerabilities were filtered for affected products that were designated as applications in the NVD.

Figure 8. Application vulnerability disclosures since 2002




## Exploit trends and security bulletins

The Microsoft Security Engineering Center (MSEC) is one of three security centers that helps protect customers from malware. The MSEC focuses on foundational ways to develop more secure products and services from the software engineering perspective, through efforts such as the Microsoft Security Development Lifecycle (SDL) and security science.

The Microsoft Security Response Center (MSRC) identifies, monitors, resolves, and responds to Microsoft software security vulnerabilities. The MSRC releases security bulletins each month to address vulnerabilities in Microsoft software. Security bulletins are numbered serially within each calendar year. For example, "MS11-057" refers to the 57th security bulletin released in 2011.

Security bulletins are typically released on the second Tuesday of each month, although on rare occasions Microsoft releases an "out-of-band" security update to address an urgent issue. Microsoft released one out-of-band update in 2011.

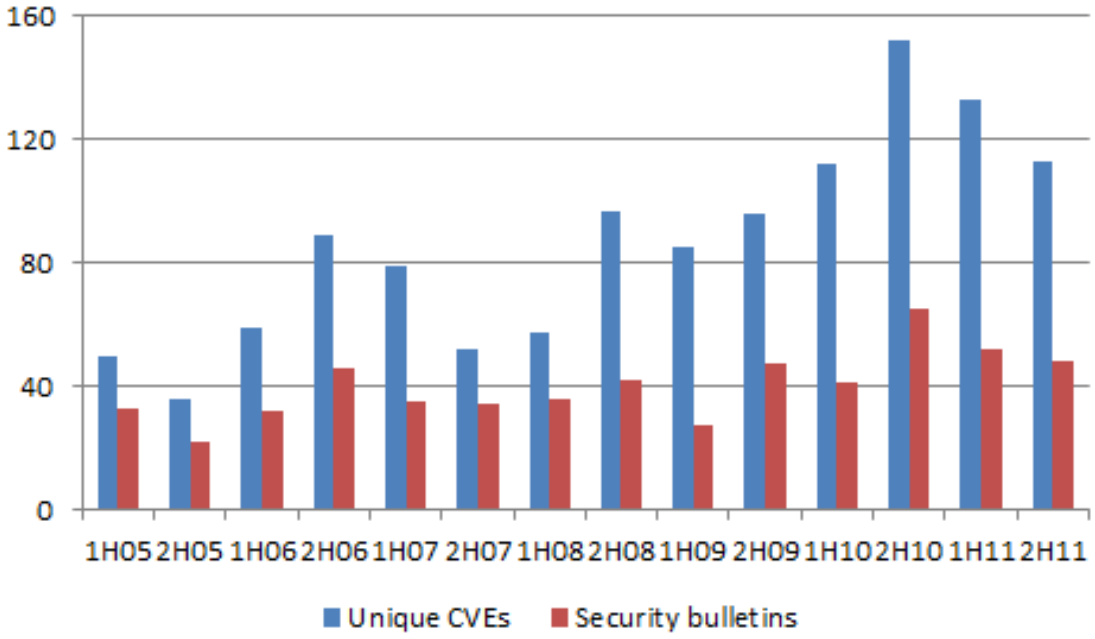
The following figure shows the number of security bulletins and out-of-band updates issued since 2005, which was when Microsoft released the first version of the Malicious Software Removal Tool (MSRT).

**Figure 9. MSRC security bulletins released since 2005**

| Period | Security bulletins | Out-of-band updates |
|---|---|---|
| 1H05 | 33 | 0 |
| 2H05 | 22 | 0 |
| 1H06 | 32 | 1 |
| 2H06 | 46 | 1 |
| 1H07 | 35 | 1 |
| 2H07 | 34 | 0 |
| 1H08 | 36 | 0 |
| 2H08 | 42 | 2 |
| 1H09 | 27 | 0 |
| 2H09 | 47 | 1 |
| 1H10 | 41 | 2 |
| 2H10 | 65 | 1 |
| 1H11 | 52 | 0 |
| 2H11 | 48 | 1 |

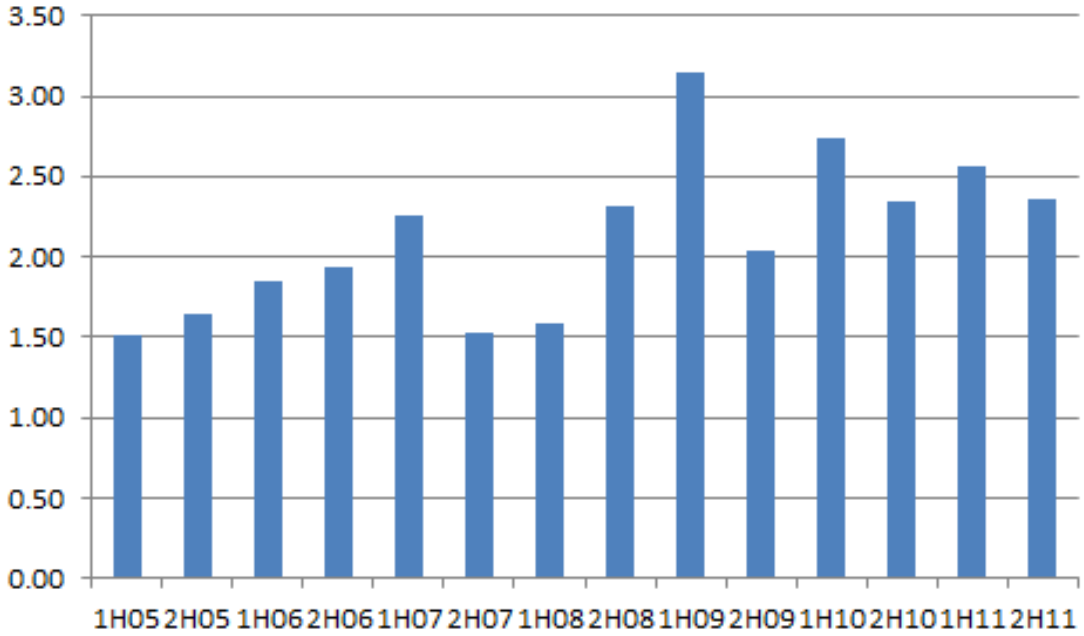
A single security bulletin often addresses multiple vulnerabilities from the CVE database, each of which is listed in the bulletin, along with any other relevant issues. The following figure shows the number of security bulletins released and the number of individual CVE-identified vulnerabilities that they have addressed in each half-year period since 1H05. (Note that not all vulnerabilities are addressed in the period in which they are initially disclosed.)

Figure 10. Number of MSRC security bulletins and CVE-identified vulnerabilities addressed




In 2011 the MSRC released 100 security bulletins that addressed 236 individual CVE–identified vulnerabilities, decreases of 7% and 6%, respectively, from 2010. As the following figure shows, the average number of CVEs addressed by each security bulletin has increased over time, from 1.5 in 1H05 to 2.4 in 2H11.

Figure 11. Average number of CVEs per MSRC security bulletin

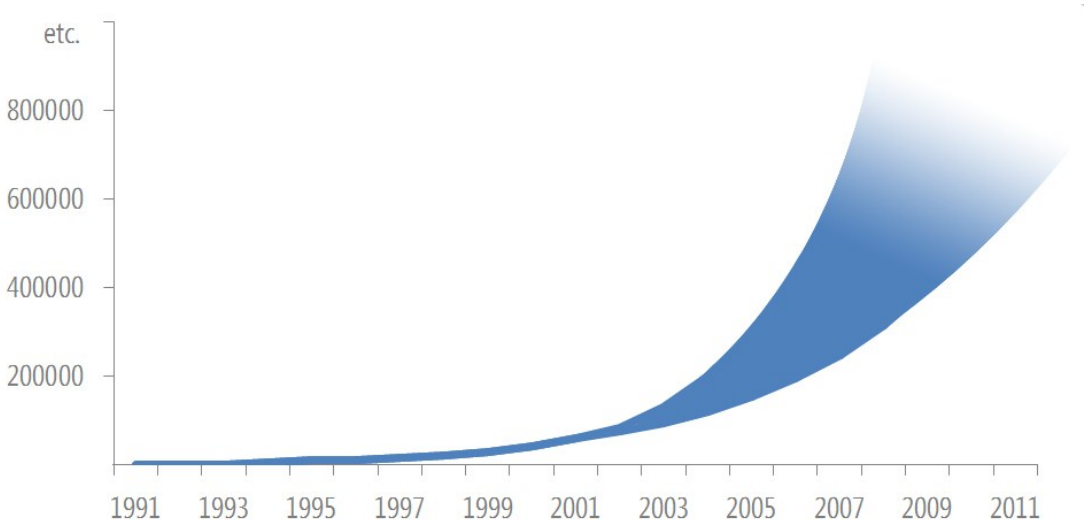



Whenever possible, the MSRC consolidates multiple vulnerabilities that affect a single binary or component to address them in a single security bulletin. This approach maximizes the effectiveness of each update and minimizes the potential disruption that customers face from testing and integrating individual security updates into their computing environments.

## The state of malware today

At the end of 2001, approximately 60,000 forms of malware or threats were known to exist. This number was a significant increase from 1996 (about 10,000) and 1991 (about 1,000).

**Figure 12. Approximate growth of malware since 1991**




Over the last decade, the proliferation of malware has become an online crime story. Today, estimates of the number of known computer threats such as viruses, worms, trojans, exploits, backdoors, password stealers, spyware, and other variations of potentially unwanted software range into the millions.

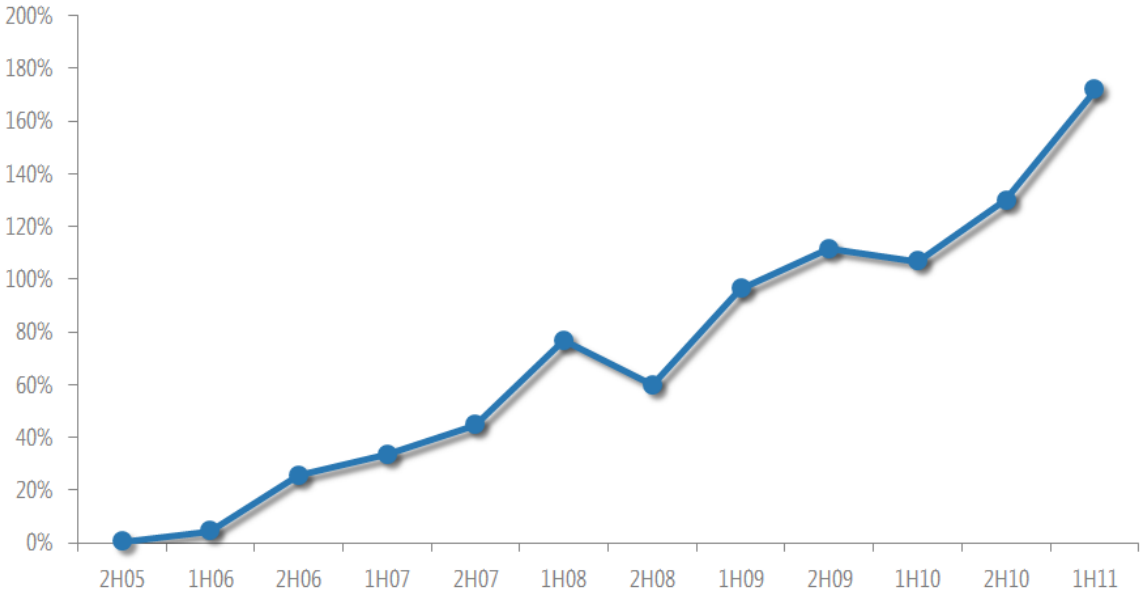
Ever since criminal malware developers began using client and server polymorphism (the ability for malware to dynamically create different forms of itself to thwart antimalware programs), it has become increasingly difficult to answer the question "How many threat variants are there?" Polymorphism means that there can be as many threat variants as infected computers can produce; that is, the number is only limited by malware's ability to generate new variations of itself.

It has become less meaningful to count the number of threat variants than it is to detect and eliminate their sources. In 2011, more than 49,000 different unique threat families were reported to the MMPC from customers. Many of these reported families were duplicates, polymorphic versions of key threat families; detecting and eliminating key threat families from infected computers is an ongoing activity.

In 2011 Microsoft added more than 22,000 signatures to detect key threat families. As criminal malware developers create more threats, the size of typical antimalware signature files increases; today antimalware signature files range to more than 100 MB in size. In 2002, typical antimalware signature files were less than 1 MB in size.

The number of files submitted to antimalware organizations has also increased. The following figure shows how the number of submitted files suspected of containing malware or potentially unwanted software to the MMPC has increased since 2005, an increase of more than 200 percent. (Suspected malware files can be submitted to the MMPC Submit a sample page.)

**Figure 13. Percentage increase in the number of files submitted to the MMPC since 2005**



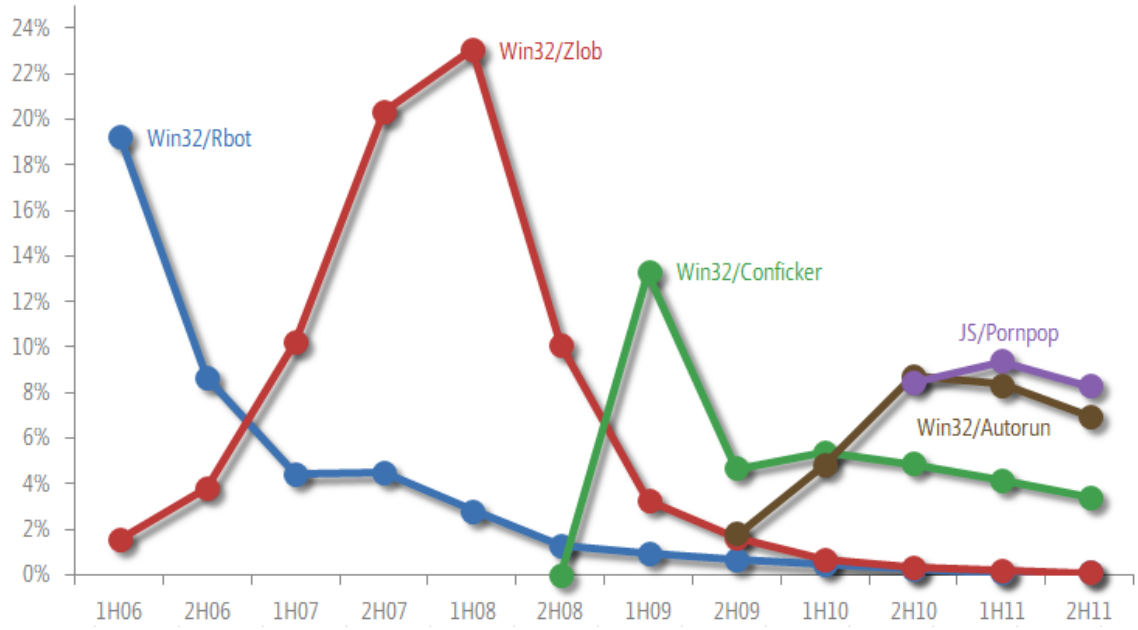
# Malware and potentially unwanted software trends

Malware continues to evolve, and the fluctuations in detections of different forms of malware sometimes indicate the successes at given points in time of the software industry's persistent antimalware efforts versus the efforts of malware developers.

## How threats have evolved over time

When viewed from a multi-year perspective, some malware and potentially unwanted software families tend to peak, or become quite prevalent, for short periods of time as antimalware vendors focus their efforts on detecting and removing these threats. These peak periods are followed by periods of decline as attackers change their tactics and move on. The following figure illustrates this phenomenon. (For Figures 14 through 18, the vertical axis represents the percentage of all computers that were infected with malware.)

**Figure 14. Malware and potentially unwanted software families that have peaked and declined since 2006**




Win32/Rbot was an early botnet family that gained notoriety in 2004 and 2005 after a number of high profile outbreak incidents that affected media and government networks, among others. Rbot is a "kit" family: Rbot variants are built from an open source botnet creation kit called RxBot, which is widely available among malware operators, and many different groups have produced

their own variants with different functionality. The MSRT was updated to detect Rbot in April 2005, and detections decreased sharply through 2006, falling below 2 percent of computers with detections by 2H08.

The trojan family Win32/Zlob was found on almost one of every four computers that was infected with malware in 1H08, a level of prevalence that no other family has equaled before or since. Zlob was typically distributed on webpages, posing as a media codec that visitors would have to install to watch video content downloaded or streamed from the Internet. After it is installed on a target computer, Zlob displays persistent pop-up advertisements for rogue security software. A Zlob variant detected at the end of 2008 included an encoded message, apparently written by the Zlob author and intended for MMPC researchers, indicating that the author would be ceasing development and distribution of the trojan:

> *For Windows Defender's Team:*
> *I saw your post in the blog (10-Oct-2008) about my previous message.*
> *Just want to say 'Hello' from Russia.*
> *You are really good guys. It was a surprise for me that Microsoft can respond on threats so fast.*
> *I can't sign here now (he-he, sorry), how it was some years ago for more seriously vulnerability for all Windows ;)*
> *Happy New Year, guys, and good luck!*
> *P.S. BTW, we are closing soon. Not because of your work. :-))*
> *So, you will not see some of my great ;) ideas in that family of software.*
> *Try to search in exploits/shellcodes and rootkits.*
> *Also, it is funny (probably for you), but Microsoft offered me a job to help improve some of Vista's protection. It's not interesting for me, just a life's irony.*

Indeed, detections of Zlob decreased significantly in 2H08, and by 2010 Zlob was no longer among the top 50 most-detected families worldwide.

Win32/Conficker is a worm family discovered in November 2008 that initially spread by exploiting a vulnerability addressed by security update MS08-067, which was released the previous month. Conficker detections peaked in 1H09 and declined to a much lower level thereafter, following coordinated efforts by the Conficker Working Group to contain the spread of the worm and clean infected computers. It has been detected on between 3 percent and 6 percent of infected computers in each 6-month period since then.

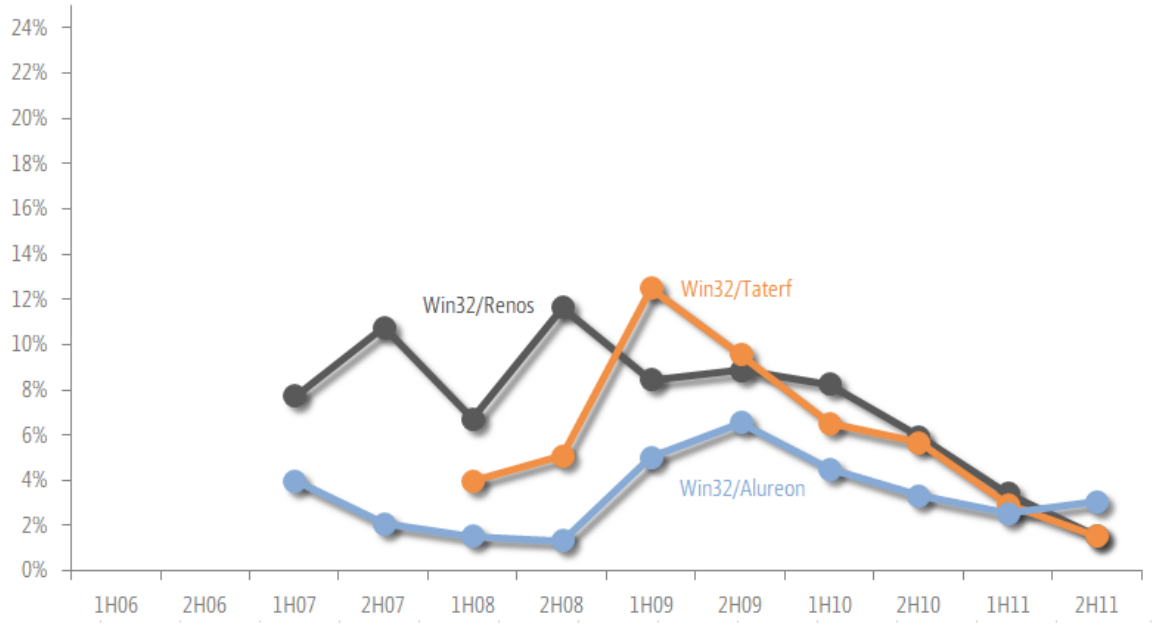
JS/Pornpop is adware that consists of specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements. First detected in August 2010, it was the second most commonly detected family in 2H10 and 1H11, and is likely to be the most commonly detected family in 2H11.

Win32/Autorun is a generic detection for worms that attempt to spread between mounted computer volumes by misusing the AutoRun feature in Windows. Detections of Win32/Autorun increased gradually for several periods before peaking in 2H10 as the most commonly detected family during that period.

Microsoft introduced a change to the way that the AutoRun feature works in Windows 7 and Windows Server 2008 R2 in an effort to help protect users from AutoRun threats. In these versions of Windows, the AutoRun task is disabled for all volumes except optical drives such as CD-ROM and DVD-ROM drives, which have historically not been used to transmit AutoRun malware. Subsequently, Microsoft published a set of updates that back-ported this change to Windows XP, Windows Server 2003, Windows Vista, and Windows Server 2008. These updates have been published as Important updates through the Windows Update and Microsoft Update services since February 2011, which may have helped contribute to the decline in Win32/Autorun detections observed throughout 2011.

Other malware and potentially unwanted software families aren't as prevalent as the peak families, but exist for longer periods of time. The following figure illustrates the prevalence of some of these more persistent malware families.

Figure 15. Malware families that have remained active at lower levels since 2007




Win32/Renos, assigned to the Trojan Downloaders & Droppers category in previous volumes of the *SIR*, was one of the four most commonly detected malware families in each six-month period from 1H07 to 2H10, taking the top slot in 2H08 and 1H10, and only dropped out of the top 25 in 2H11. Renos is a trojan downloader that installs rogue security software on infected computers.

Win32/Taterf, assigned to the Worms category in previous volumes of the *SIR*, was among the five most commonly detected malware families in each period from 2H08 to 2H10, and was the most commonly detected family in 2H09. Taterf is a worm that spreads via mapped drives to steal logon and account details for popular online games. The increasing popularity of massively multiplayer online role-playing games has created a market (usually discouraged by the makers of the games themselves) in virtual "gold" and in-game equipment, which players trade for real-world cash. This in turn has led to a class of threats like Taterf, which steal players' gaming passwords on behalf of thieves who can then auction the victims' virtual loot themselves. Taterf is a modified version of a similar threat, Win32/Frethog, which itself has been persistently prevalent over the same period of time.

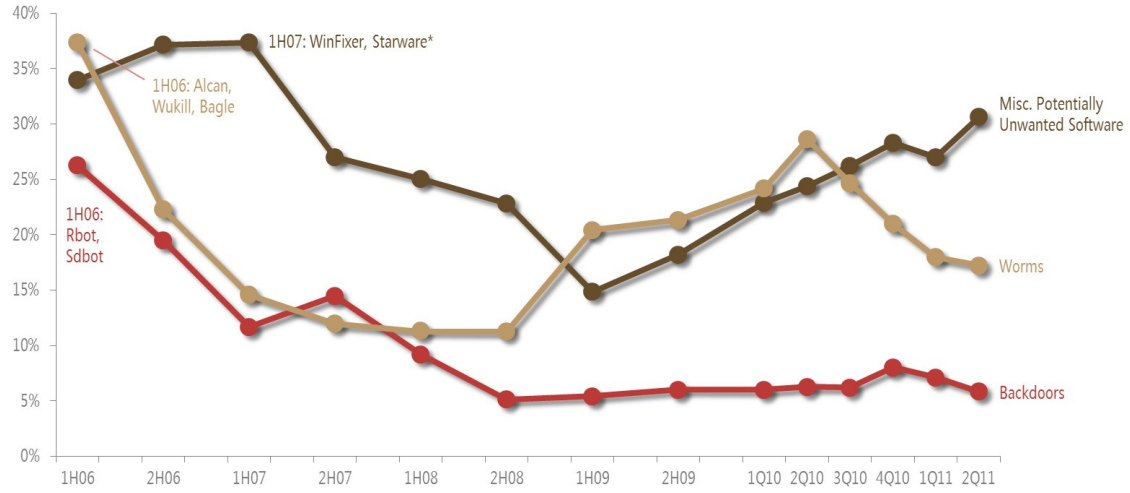
Win32/Alureon, assigned to the Miscellaneous Trojans category in previous volumes of the *SIR*, is a family of data-stealing trojans with rootkit characteristics. It was first discovered in early 2007 and

has been in or near the top 25 families in each half-year period since then. Alureon variants allow an attacker to intercept incoming and outgoing Internet traffic and gather confidential information such as user names, passwords, and credit card data.

## Different threats at different times

Another point that becomes apparent when malware and potentially unwanted software is viewed from a multi-year perspective is that different categories of malware—that is, different types of threats—have been prevalent at different times. The following figure illustrates the relative prevalence of three different categories of malware.

**Figure 16. Worms, Backdoors, and Miscellaneous Potentially Unwanted Software categories since 2006**

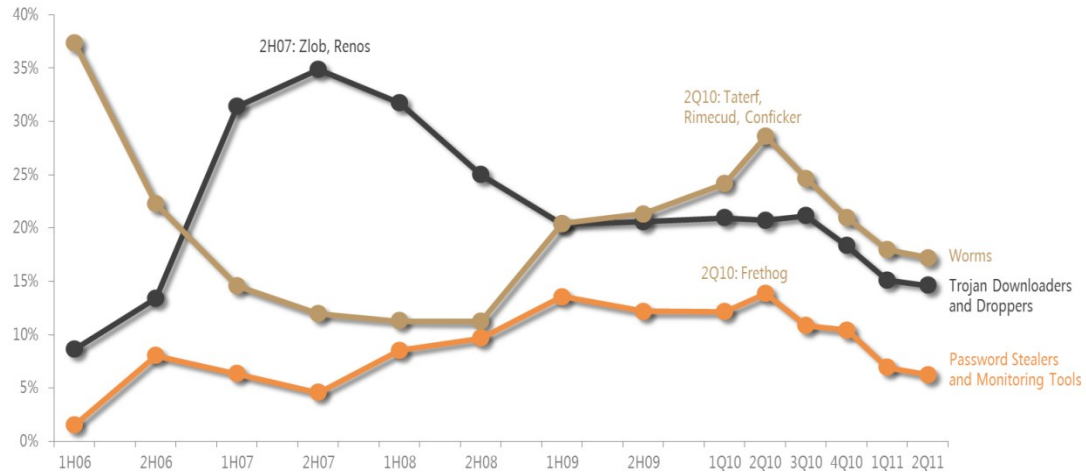



In 2006 and 2007, the malware landscape was dominated by the Worms, Miscellaneous Potentially Unwanted Software, and Backdoors categories. (The term "Miscellaneous Potentially Unwanted Software" refers to programs with potentially unwanted behavior that may affect a user's privacy, security, or computing experience.) By this time, large-scale outbreaks of worms such as Win32/Msblast and Win32/Sasser, which spread by exploiting vulnerabilities in network services, were mostly in the past. The most likely reason for their decline was the high-profile nature of these outbreaks, which caused antimalware vendors to increase their detection, cleaning, and blocking efforts and ultimately spurred widespread adoption of the security updates that addressed the affected vulnerabilities. Most of the prevalent worms in 2006 were mass-mailers, such as Win32/Wukill and Win32/Bagle, which spread by emailing copies of themselves to addresses discovered on infected computers.

Prevalent backdoors included a pair of related botnet families, Win32/Rbot and Win32/Sdbot. Variants in these families are built from botnet construction kits that are traded in the underground market for malware, and are used to control infected computers over Internet Relay Chat (IRC). Rbot and Sdbot have largely been supplanted by newer botnet families, but remain in active use nonetheless, probably because of the relative ease with which prospective botnet operators can obtain the construction kits.

Prevalent trojan families in 2006 and 2007 included Win32/WinFixer, an early rogue security software family, and the browser toolbar Win32/Starware. Unlike most modern rogue families, which typically pose as antimalware scanners, WinFixer masquerades as a utility that supposedly identifies "privacy violations" in the computer's registry and file system and offers to "remove" them for a fee. Win32/Starware is a browser toolbar that monitors searches at popular search engines, conducting its own search in tandem and displaying the results in an inline frame within the browser window.

**Figure 17. Worms, Trojan Downloaders and Droppers, and Password Stealers and Monitoring Tools categories since 2006**



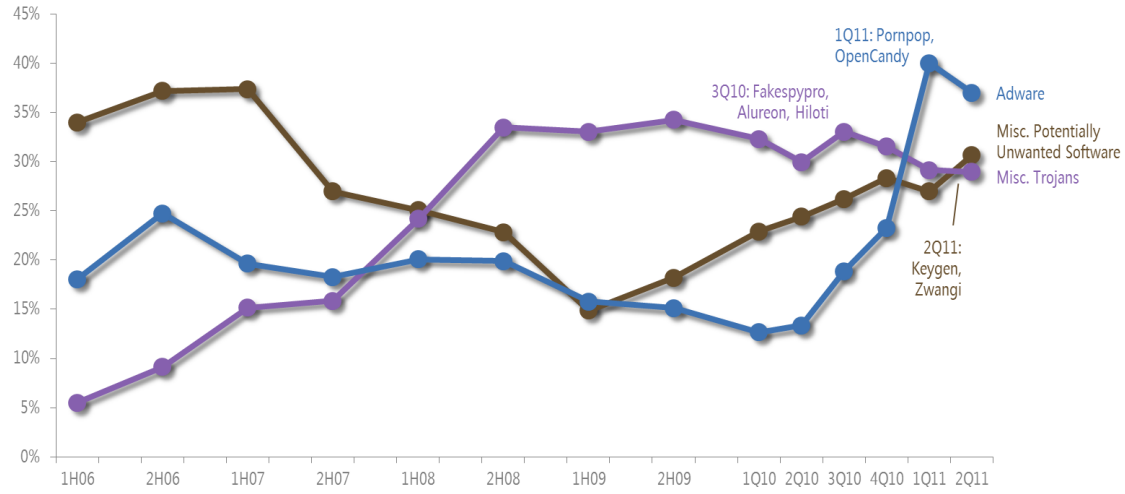

The Trojan Downloaders and Droppers category, which affected less than 9 percent of computers with detections in 1H06, rose rapidly to become one of the most significant threat categories in 2007 and 2008, primarily because of increased detections of Win32/Zlob and Win32/Renos.

After decreasing significantly from its 1H06 peak, the Worms category began to increase again in 2009 after the discovery of Win32/Conficker and reached a second peak in 2Q10 with increased

detections of Win32/Taterf and Win32/Rimecud. Rimecud is a family of worms with multiple components that spreads via removable drives and instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected computer.

Malware families in the Password Stealers and Monitoring Tools category, which were responsible for a negligible percentage of detections in 1H06, increased slowly but steadily through 2008 and 2009 before peaking in 2Q10. Game password stealers such as Win32/Frethog were responsible for much of this increase.

**Figure 18. Adware, Miscellaneous Potentially Unwanted Software, and Miscellaneous Trojans categories since 2006**




The Adware, Miscellaneous Potentially Unwanted Software, and Miscellaneous Trojans categories were the most commonly detected categories in 2010 and 2011. Adware detections increased significantly in 1H11, including the adware families Win32/OpenCandy and JS/Pornpop. OpenCandy is an adware program that may be bundled with certain third-party software installation programs. Some versions of the OpenCandy program send user-specific information without obtaining adequate user consent, and these versions are detected by Microsoft antimalware products. Pornpop is a detection for specially crafted JavaScript-enabled objects that attempt to display pop-under advertisements in users' web browsers. Initially, JS/Pornpop appeared exclusively on websites that contained adult content; however, it has since been observed to appear on websites that may contain no adult content whatsoever.

The Miscellaneous Potentially Unwanted Software category, which was the most commonly

detected category in 2006, declined in prevalence in 2007 and 2008, then increased again to become the second most prevalent category in 2Q11. Significant families in this category in 2Q11 were Win32/Keygen, a generic detection for tools that generate product keys for illegally obtained versions of various software products, and Win32/Zwangi, a program that runs as a service in the background and modifies web browser settings to visit a specific website.

The Miscellaneous Trojans category has consistently affected about a third of computers that were infected with malware in each period since 2H08. A number of rogue security software families fall into this category, such as Win32/FakeSpyPro, the most commonly detected rogue security software family in 2010. Other prevalent families in this category include Win32/Alureon, the data-stealing trojan, and Win32/Hiloti, which interferes with an affected user's browsing habits and downloads and executes arbitrary files.

## Threat categories by location

The malware ecosystem has moved away from highly visible threats, such as self-replicating worms, toward less visible threats that rely more on social engineering for distribution and installation. This shift means that the spread and effectiveness of malware have become more dependent on language and cultural factors. Some threats are spread using techniques that target people who speak a particular language or who use services that are local to a particular geographic region. Others target vulnerabilities or operating system configurations and applications that are unequally distributed around the globe. Infection data from several Microsoft security products for some of the more populous locations around the world demonstrates the highly localized nature of malware and potentially unwanted software.

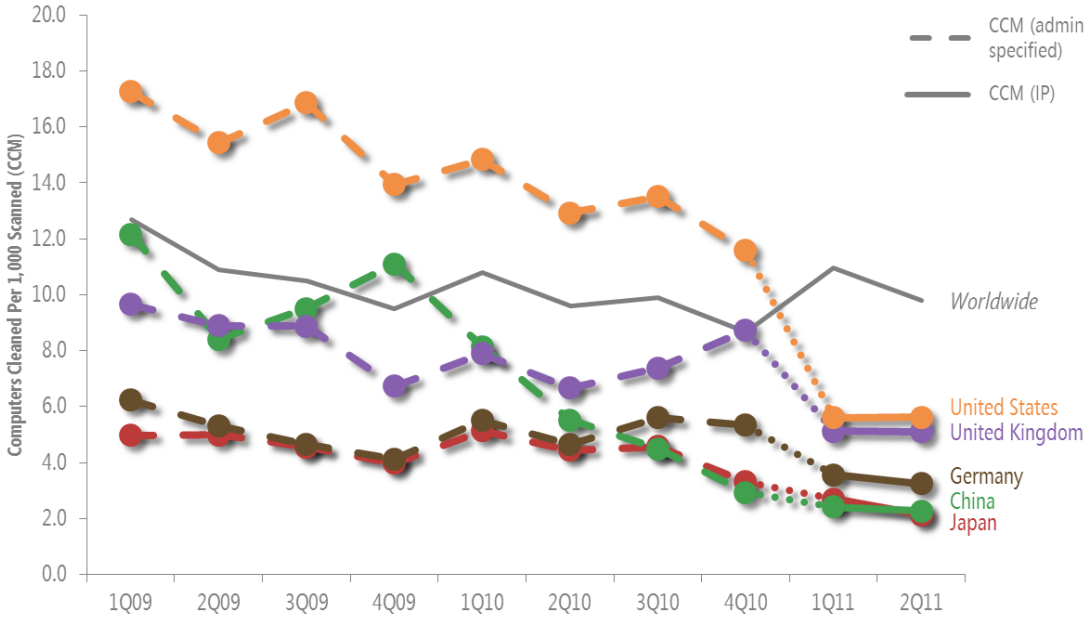
Accordingly, the threat landscape is much more complex than a simple examination of the biggest global threats would suggest.

### 2011 security intelligence

The following figure shows those countries/regions reporting significantly large numbers of computers cleaned by Microsoft desktop antimalware products since 2009.[2]

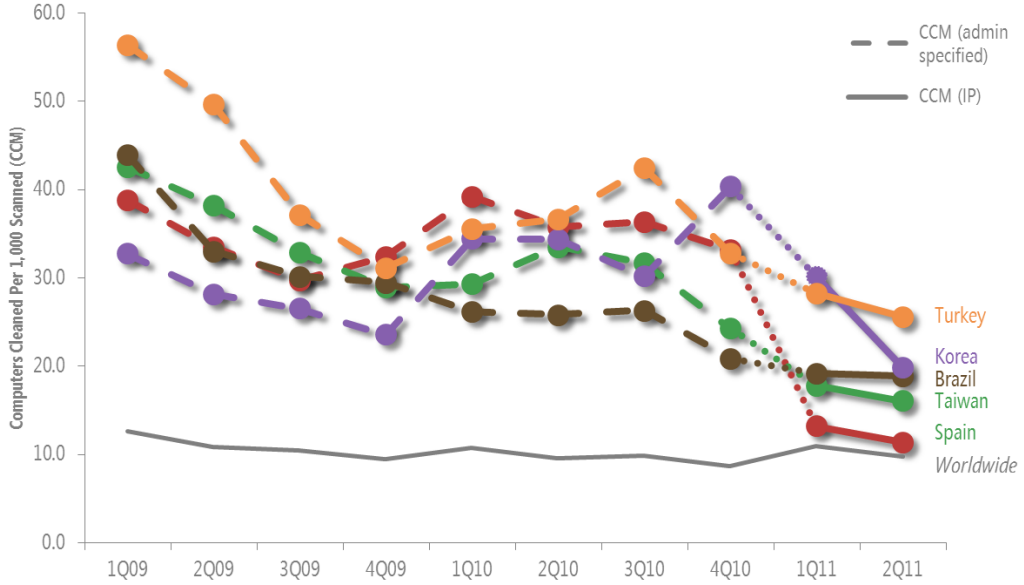
[2] For information about how PC locations are determined, see the blog post Determining the Geolocation of Systems Infected with Malware.

Figure 19. Countries/regions with significantly large numbers of computers cleaned since 2009



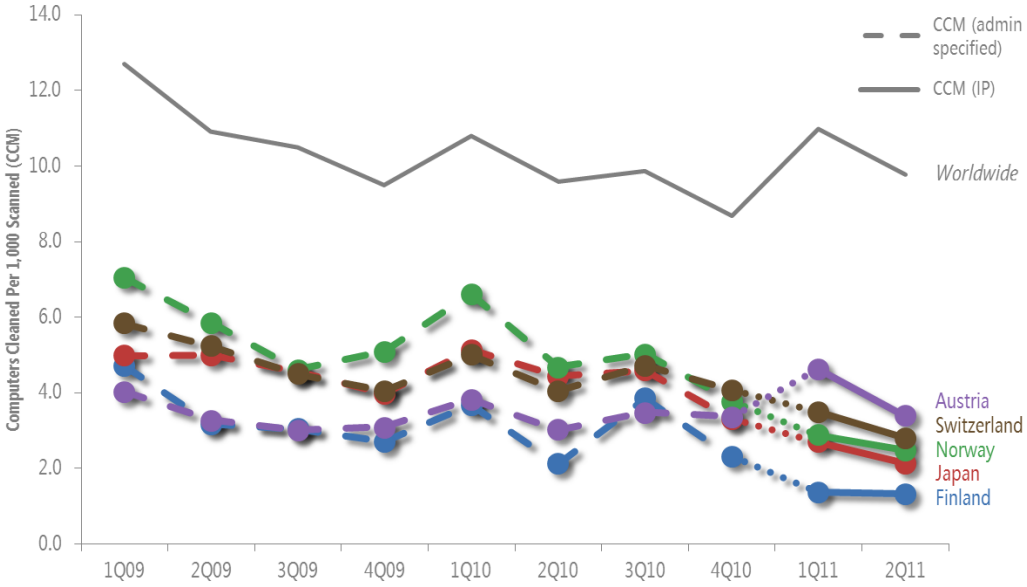

The following figure shows countries/regions that have historically reported high infection rates as compared to the average infection rate for all countries/regions.

Figure 20. Countries/regions with historically high infection rates as compared to the worldwide average since 2009




The following figure shows countries/regions that have historically reported low infection rates as compared to the average infection rate for all countries/regions.

Figure 21. Countries/regions with historically low infection rates as compared to the worldwide average since 2009



## Lessons from least infected countries/regions

Austria, Finland, Germany, and Japan have all enjoyed relatively low malware infection rates over the past several years. However, many of the same global threats that are prevalent in countries/regions with high malware infection rates, such as Brazil, Korea, and Turkey, are also prevalent in countries/regions with low infection rates.

- Adware is among the most prevalent categories of threats found in countries/regions with both high malware infection rates and low malware infection rates; it was observed as the top or second to top category in each. Both JS/Pornpop (detected on more than 6.5 million unique computers globally in the second half of 2010) and Win32/ClickPotato are very prevalent in these countries/regions.

- Win32/Renos was primarily responsible for the levels of trojan downloaders and droppers found in countries/regions with both high malware infection rates and low malware infection rates. Win32/Renos has been a prevalent family of trojan downloaders and droppers for a number of years, and was detected on more than 8 million unique computers around the world in 2010.

- Win32/Autorun, detected on more than 9 million unique computers globally in 2010, and Win32/Conficker, detected on more than 6.5 million unique computers globally in 2010, are in the top ten lists of threats for countries/regions with both high malware infection rates and low malware infection rates, except Finland.

The relatively low malware infection rates in Austria, Finland, Germany, and Japan does not necessarily mean that criminals are not active in these countries/regions. For example:

- More malware hosting sites (per 1,000 hosts) were observed in Germany than in the United States in 2010.

- The percentage of sites hosting drive-by downloads in Finland was almost twice that of the United States in the first half of 2010.

- In Q4 of 2010, the percentage of sites hosting drive-by downloads in Germany was observed to be 3.7 times higher than the number observed in the United States.

- The percentage of sites hosting drive-by downloads in Japan was 12 percent higher than that of the United States during the first half of 2010. Although this percentage went down precipitously in both locations by the fourth quarter of 2010, the percentage of sites hosting

drive-by downloads in Japan was 4.7 times higher than that of the United States in Q4.

Security experts in these countries/regions indicate that the following factors contribute to consistently low malware infection rates in their countries/regions:

- Strong public–private partnerships exist that enable proactive and response capabilities.
- Computer emergency response teams (CERTs), Internet service providers (ISPs), and others who actively monitor for threats enable rapid response to emerging threats.
- An IT culture in which system administrators respond rapidly to reports of system infections or abuse is helpful.
- Enforcement policies and active remediation of threats via quarantining infected systems on networks in the country/region is effective.
- Educational campaigns and media attention that help improve the public's awareness of security issues can pay dividends.
- Low software piracy rates and widespread usage of Windows Update/Microsoft Update has helped keep infection rates relatively low.

This list has striking similarities to the Collective Defense concept outlined in a paper written by Scott Charney, Corporate Vice President of Trustworthy Computing at Microsoft, in 2010. "Collective Defense: Applying Public Health Models to the Internet" (PDF) outlines a model to improve the health of devices connected to the Internet. To accomplish this, governments, the IT industry, and ISPs should ensure the health of consumer devices before granting them unfettered access to the Internet. The approach offered in the paper is to look at addressing online security issues using a model similar to the one society uses to address human illness. The public health model encompasses several interesting concepts that can be applied to Internet security.

The consistently least infected countries/regions in the world appear to be already doing many of the things that the Collective Defense health model proposes. A video that examines the model is available on the Trustworthy Computing website here.

## Windows Update and Microsoft Update

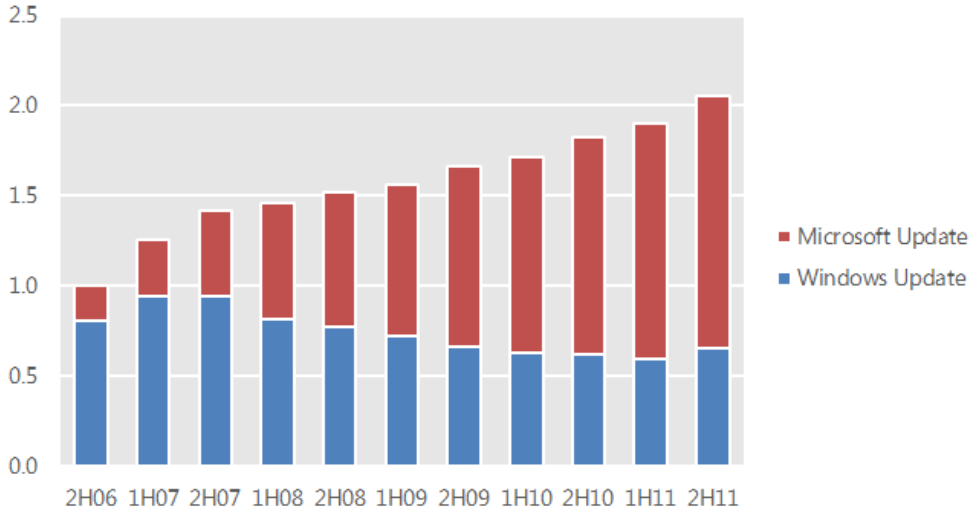
Microsoft provides several tools and services that enable systems or their users to download and install updates directly from Microsoft or, for business customers, from update servers managed by their system administrators. The update client software (called Automatic Updates in Windows XP and Windows Server 2003, and simply Windows Update in Windows 7, Windows Vista, and Windows Server 2008) connects to an update service for the list of available updates. After the update client determines which updates are applicable to each unique system, it installs the updates or notifies the user that they are available, depending on the way the client is configured and the nature of each update.

For users, Microsoft provides two update services that the update clients can use:

- Windows Update provides updates for Windows components and for device drivers provided by Microsoft and other hardware vendors. Windows Update also distributes signature updates for Microsoft antimalware products and the monthly release of the MSRT. By default, when a user enables automatic updating, the update client connects to the Windows Update service for updates.
- Microsoft Update provides all of the updates offered through Windows Update as well as updates for other Microsoft software, such as the Microsoft Office system, Microsoft SQL Server, and Microsoft Exchange Server. Users can opt in to the service when installing software that is serviced through Microsoft Update or at the Microsoft Update website.

Enterprise customers can also use Windows Server Update Services (WSUS) or the Microsoft System Center 2012 family of management products to provide update services for their managed computers.

Figure 22. Usage of Windows Update and Microsoft Update, 2H06-2H11, indexed to 2H06 total usage




- Since its introduction in 2005, usage of Microsoft Update has increased dramatically.

## In conclusion

This special edition of the *SIR* provides information about how malware and other forms of potentially unwanted software have evolved over the last 10 years.

Computing has become part of the fabric of our everyday lives, and the foundations of modern society are becoming more digital every day. Information and communications technology (ICT) has transformed for the better how we live, but society still confronts some long-standing and evolving challenges.

As the number of people, computers, and devices that connect to the Internet continues to increase, cyberthreats are becoming more sophisticated in their ability to gather sensitive data, disrupt critical operations, and conduct fraud.

Cyberthreats today are often characterized as technically advanced, persistent, well-funded, and motivated by profit or strategic advantage. Security intelligence is a valuable asset to all Internet users, organizations, governments, and consumers alike, who face a myriad of threats that are anything but static. Because we live in a world that is so dependent on IT, Microsoft's dedication to security, privacy, and reliability might be more important today than it was than when Trustworthy Computing was established in 2002.

Many industries and organizations, including Microsoft, are investing in research intelligence, software development methods, and tools to help governments, industry, and individuals better reduce and manage the risks that result from the uncertainty of the rapidly changing threat landscape. Microsoft Trustworthy Computing continues to contribute to the computing ecosystem as we face a new world of devices, services, and communications technologies that continue to evolve.

## Appendix A: Computer protection technologies and mitigations

Addressing threats and risks requires a concerted effort on the part of people, organizations, and governments around the world. The "Managing Risk" section of the Microsoft Security Intelligence Report (SIR) website presents many suggestions for preventing harmful actions from malware, breaches, and other security threats, and for detecting and mitigating problems when they occur. Topics in this section of the website include:

- "Protecting Your Organization," which offers guidance for IT administrators in small, medium-sized, and large organizations seeking to improve their security practices and to stay current on the latest developments.
- "Protecting Your Software," which offers software developers information about developing secure software, including in-house software, and securing Internet-facing systems from attack.
- "Protecting Your People," which offers guidance for promoting awareness of security threats and safe Internet usage habits within an organization.

Additional helpful information about vulnerability and malware protection efforts is available in the following documents:

- Information Sharing and MSRC 2010, a report by the Microsoft Security Response Center
- Mitigating Software Vulnerabilities white paper
- Malware research and response at Microsoft. This report focuses on the role and activities of the Microsoft Malware Protection Center and our vision to provide thorough, ongoing malware research and response.
- Introducing Microsoft Antimalware Technologies. This white paper helps IT professionals to understand the overall malware landscape and how to take advantage of the features in their antimalware technology.

## Appendix B: Threat families referenced in this report

The definitions for the threat families referenced in this report are adapted from the Microsoft Malware Protection Center Malware encyclopedia, which contains detailed information about a large number of malware and potentially unwanted software families. See the encyclopedia for more in-depth information and guidance for the families listed here and throughout the report.

**Win32/Alureon**. A data-stealing trojan that gathers confidential information such as user names, passwords, and credit card data from incoming and outgoing Internet traffic. It may also download malicious data and modify DNS settings.

**Win32/Autorun**. A family of worms that spreads by copying itself to the mapped drives of an infected computer. The mapped drives may include network or removable drives.

**Win32/Bagle**. A worm that spreads by emailing itself to addresses found on an infected computer. Some variants also spread through P2P networks. Bagle acts as a backdoor trojan and can be used to distribute other malicious software.

**Win32/ClickPotato**. A program that displays pop-up and notification-style advertisements based on the user's browsing habits.

**Win32/Conficker**. A worm that spreads by exploiting a vulnerability addressed by Security Bulletin MS08-067. Some variants also spread via removable drives and by exploiting weak passwords. It disables several important system services and security products, and downloads arbitrary files.

**Win32/FakeSpyPro**. A rogue security software family distributed under the names Antivirus System PRO, Spyware Protect 2009, and others.

**Win32/Fixer**. Malware that locates various registry entries and other types of data, misidentifies them as privacy violations, and prompts the user to purchase a product to remove the alleged violations.

**Win32/Frethog**. A large family of password-stealing trojans that target confidential data, such as account information, from massively multiplayer online games.

**Win32/Hiloti**. A family of trojans that interferes with an affected user's browsing habits and downloads and executes arbitrary files.

**Win32/Keygen**. A generic detection for tools that generate product keys for illegally obtained versions of various software products.

**Win32/Msblast**. A family of network worms that exploits a vulnerability in Microsoft Windows 2000 and Windows XP, and may also attempt denial of service (DoS) attacks on some server sites or create backdoor programs that allow attackers to access infected computers.

**Win32/Mydoom**. A family of mass-mailing worms that act as backdoor trojans and allow attackers to access infected systems. Win32/Mydoom may be used to distribute other malicious software, and some variants launch DoS attacks against specific websites.

**Win32/Nimda**. A family of worms that targets computers running certain versions of Windows and exploits the vulnerability described in Microsoft Security Bulletin MS01-020 to spread by infecting web-content documents and attaching itself to email messages.

**Win32/OpenCandy**. An adware program that may be bundled with certain third-party software installation programs. Some versions may send user-specific information, including a unique machine code, operating system information, locale, and certain other information to a remote server without obtaining adequate user consent.

**JS/Pornpop**. A generic detection for specially-crafted JavaScript-enabled objects that attempt to display pop-under advertisements, usually with adult content.

**Win32/Rbot**. A family of backdoor trojans that targets certain versions of Windows and allows attackers to control infected computers through an IRC channel.

**Win32/Renos**. A family of trojan downloaders that install rogue security software.

**Win32/Rimecud**. A family of worms with multiple components that spread via fixed and removable drives and via instant messaging. It also contains backdoor functionality that allows unauthorized access to an affected system.

**Win32/Rustock**. A multi-component family of rootkit-enabled backdoor trojans that were first developed around 2006 to aid in the distribution of spam email.

**Win32/Sasser**. A family of network worms that exploit the Local Security Authority Subsystem Service (LSASS) vulnerability fixed in Microsoft Security Update MS04-011.

**Win32/Sdbot**. A family of backdoor trojans that allow attackers to control infected computers.

**Win32/Sircam**. A family of mass-mailing network worms that targets certain versions of Windows and spreads by sending a copy of itself as an email attachment to email addresses found on infected computers.

**Win32/Starware**. A web browser toolbar that monitors searches at popular search engines, conducts its own search in tandem, and displays the results in an IFrame within the browser window.

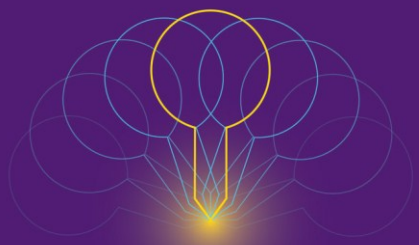
**Win32/Taterf**. A family of worms that spread through mapped drives to steal login and account details for popular online games.

**Win32/Wukill**. A family of mass-mailing email and network worms that spreads to root directories on certain local and mapped drives. It also spreads by sending a copy of itself as an email attachment to email addresses found on infected computers.

**Win32/Zlob**. A large multicomponent family of malware that modifies Windows Internet Explorer settings, alters and redirects users' default Internet search and home pages, and attempts to download and execute arbitrary files (including additional malicious software).

**Win32/Zotob**. A network worm that primarily targets computers running Windows 2000 that do not have Microsoft Security Bulletin MS05-039 installed; it exploits the Windows Plug-and-Play buffer overflow vulnerability.

**Win32/Zwangi**. A program that runs as a service in the background and modifies web browser settings to visit a particular website.


TwC Next