Symantec Internet Security Threat Report

Attack Trends for Q3 and Q4 2002

EDITOR
Mark Higgins
Manager, Trending and Analysis
Symantec Managed Security Services

RESEARCH & ANALYSIS TEAM
David Ahmad
Manager, Development
Symantec Security Response

Cori Lynn Arnold
Security Analyst
Symantec Managed Security Services

Brian Dunphy
Director, Analysis Operations
Symantec Managed Security Services

Michael Prosser
Principal Trend Analyst
Symantec Security Services

Vincent Weafer
Senior Director, Development
Symantec Security Response

MEDIA INQUIRES
Candice Garmoe
310-449-4324

FEEDBACK
threatreport@symantec.com

Executive Summary

The Symantec Internet Security Threat Report provides the Internet community with a deeper understanding of how Internet threats are evolving over time. The Report derives insights on cyber attack trends from the world's most extensive network of intrusion detection systems (IDSs) and firewalls deployed throughout the world. In addition to more thorough analysis of network-based attacks, this issue is expanded in scope, incorporating analysis of vulnerability and malicious code data as well. By combining these resources, the Internet Security Threat Report becomes the only report to provide a comprehensive view of the security landscape. This view is based on Symantec resources, which include one of the world's largest repository of security attack data, the world's most comprehensive vulnerability database, and millions of code submissions from antivirus customers. These findings can help IT managers understand the evolving nature of security threats, and how a variety of factors ultimately affect the risks experienced by their organizations.

As discussed throughout this report, Internet threats have intensified and evolved in many ways, while remaining relatively stable along other criteria. Excluding worm and blended threat activity, measured cyber attack volume declined slightly for the first time, dropping 6% since the prior six-month period. Despite the decline, many organizations, such as those in the financial services sector, experienced a sharp rise in attack volume and relative attack severity, while other companies, such as tenured security monitoring clients, substantially reduced their risk profile. Attack volume by country of origin was mostly consistent with past studies. 80% of attacks were launched from or through systems located in only 10 countries, and the United States was by far the largest source of attacks.

Adding to risks associated with cyber attacks, the discovery rate for new IT product vulnerabilities accelerated substantially over the past year. The total number of new, documented vulnerabilities in 2002 was 81.5% higher than in 2001. This rise was driven almost exclusively by vulnerabilities rated as relatively severe. Furthermore, approximately 60% of the documented vulnerabilities were easily exploitable either because sophisticated tools were widely available or because exploit tools were not required at all. Finally, by leveraging the vast supply of vulnerabilities, malicious code writers introduced several successful blended threats over the past six months. Within hours of release many of these threats spread rapidly among Internet-connected organizations, and several continue to infect thousands of systems throughout the world today.

In conclusion, the evidence clearly shows that the risk of cyber attacks and malicious code infections remains high for all Internet-connected organizations. In addition, the potential introduction of entirely new, and potentially more destructive, forms of malicious code and cyber attack tools represents a substantial future risk. The remainder of this report provides greater detail on major threat trends, as well as highlighting future concerns. The findings provide IT professionals with a greater understanding of the ever-evolving Internet threat environment, which they can then use to create more effective security postures.

About the Symantec Internet Security Threat Report

The Symantec Internet Security Threat Report provides the most accurate and comprehensive compendium of current trends in cyber security threats. Trends derive from the analysis of a broad range of threat data. The first section of the report provides insights into major trends in actual cyber attack activity. These insights are based on the statistical analysis of real-time cyber attacks detected by a sample set of more than 400 companies, which deploy over 1,000 intrusion detections systems and firewalls in more than 30 countries. The second section of the report provides insights into major trends in threat exposure by analyzing documented vulnerabilities and outbreaks of malicious code. Insights in these sections draw from the statistical analysis of malicious code submissions from millions of corporate and home users throughout the world and a vulnerability database consisting of more than 6,000 distinct entries.

The Symantec Internet Security Threat Report is firmly grounded on analysis of empirical data. Leveraging the full breadth of Symantec's technology and service offerings, these data and analysis now cover the full spectrum of information security, including vulnerability analysis, malicious code analysis, and network-based cyber attacks. By sharing this information, we provide members of the information security community with benchmarks and guidance to evaluate the effectiveness of their current and future security strategies within their own company, industry, and throughout the global Internet community.

Contents

Report Highlights

Overall threats in terms of cyber attacks, IT product vulnerabilities, and overall susceptibility to new forms of malicious code remained substantial and constantly evolving over the past six months. For companies who are not making use of appropriate countermeasures, these threats have increased their risk of compromise. Specific findings that support this observation are highlighted throughout this section under the following subtitles: Cyber Attack Trends, Vulnerability Trends, and Malicious Code Trends.

CYBER ATTACK TRENDS

Excluding worm and blended threat activity, the rate of network-based attacks over the past six months was 6% lower than the rate recorded during the prior six-month period.

- On average, companies experienced 30 attacks per company per week during the past six months, as compared with 32 attacks per company per week during the prior six-month period.
- Approximately 85% of this activity was classified as pre-attack reconnaissance, and the remaining 15% was classified as various forms of attempted (or successful) exploitation.
- Despite the decline in attack volume over the prior six-month period, average attacks per company during the past six months remained 20% higher than the rate recorded during the same six-month period in 2001.

The severe event incidence rate during the past six months was slightly lower than the rate recorded during the prior six-month period.

- 21% of companies in the sample set suffered at least one severe event over the past six months, as compared to 23% during the prior six-month period.
- The current severe event incidence rate remains far below the rate of 43%, which was recorded during the same six-month period in 2001.

Several notable patterns of attacker activity were observed during specific windows of time.

- Attack volume and severity were considerably lower on Saturdays and Sundays than on any other day of the week, which confirms observations from the prior six-month period.
- Fluctuations in attacker activity appeared to be a function of the approximate local times in which the attacking systems were located, rather than the local times in which the victims were located.
- Internet-connected organizations experienced a notable spike in attacker activity between the hours of 12:00 and 21:00 Greenwich Mean Time (GMT) independent of each network's location or time zone. This appears to be the result of several high-volume regional sources of attacks achieving peak activity at approximately the same time.

The volume and relative severity of attacks experienced by companies continued to vary based on characteristics, such as industry, size, and client tenure.

- Power and Energy companies continued to show the highest rate of attacks and severe event incidence.
- Both the nonprofit and financial services sectors experienced higher rates of overall attack volume and severe event incidence, respectively.
- Larger companies, measured in terms of employee count, consistently experienced a higher volume and greater severity of attacks.
- Companies continued to show risk reduction as security monitoring client tenure increased. The severe event incidence rate for companies with less than 12 months tenure was 29%, while the incidence rate for companies with more than 12 months tenure was 17%.

Overall attack activity by apparent country of origin remained relatively consistent over the past 18 months; however, a few notable fluctuations in activity were also detected.[1]

- The top ten attacking countries accounted for 80% of all attacks detected during the prior six months; the United States continued to show the highest attack volume, accounting for 35.4% of all attacks.
- Attacks from South Korea increased by 62% over the past six months, establishing this country as the second largest overall source of attacks and the highest source of attacks per 10,000 Internet users among Tier One countries.[2] One factor driving this trend may be South Korea's rapidly growing consumer broadband infrastructure. As broadband becomes more accessible in other nations, their exposure to and participation in malicious activity may also rise unless protection technologies are widely deployed.
- Several Eastern European countries showed high rates of attacks per 10,000 Internet users. Poland and the Czech Republic were number two and three, respectively, on the list of Tier One countries, while Romania, Latvia, Lithuania, and Slovakia were all represented on the list of Tier Two countries.

Symantec detected no verifiable cases of Cyber Terrorism during the past six months.

- Attacks from countries included on the Cyber Terrorist Watch List accounted for less than 1% of all activity.

Cases of internal misuse and abuse accounted for more than 50% of incident response engagements.

- In addition to exceeding external attacks in overall volume, the customer self-assessments of damage were particularly high for internal cases of abuse and misuse.
- High self-reported damage estimates, coupled with the relative simplicity with which the perpetrators acted, should be considered a warning sign that protecting against the internal threat is extremely important.

[1] Tracking the "true" source of attacks is extremely difficult. Attackers can jump through multiple systems and countries before hitting their intended target. Therefore, the data referenced in these findings only represents the last hop that the attacker took before hitting his/her intended target.

[2] When evaluating attacks per 10,000 Internet users, countries were separated into two tiers. Tier One countries include those with more than 1 million Internet users; Tier Two countries include those with between 100,000 and 1 million Internet users. These categorizations separate countries with relatively well-developed infrastructures from those with emerging Internet infrastructures.

VULNERABILITY TRENDS

Symantec documented 2,524 new vulnerabilities over the past year, which amounted to an 81.5% increase over 2001.

- On average, Symantec analysts documented 7 new vulnerabilities per day over the past year.
- Potential drivers of the increase include the establishment of the responsible disclosure movement, the use of several new methodologies to exploit software bugs, and increased media exposure for vulnerability researchers.

The increase in new vulnerabilities was driven by the sharp rise in moderately or highly severe vulnerabilities.

- The total number of moderate and high severity vulnerabilities documented in 2002 was 84.7% higher than the total documented in 2001. In comparison, the total number of low severity vulnerabilities was only 24.0% higher than the total documented in 2001.
- The rapid development and deployment of remotely exploitable web applications appears to be the most substantial driver of this trend.

The relative ease with which attackers could exploit new vulnerabilities remained unchanged over the past year.

- Approximately 60% of all new vulnerabilities could be easily exploited either because the vulnerability did not require the use of exploit code or because the required exploit code was widely available.
- However, of the subset of vulnerabilities that required the use of exploit code, only 23.7% actually had exploit code available in 2002, as compared with 30.0% in 2001.

Based on vulnerabilities that surfaced in 2002, a number of high-risk future threats have emerged, which attackers and malicious code writers are only beginning to leverage.

- Known blended threats are exploiting only a fraction of the vulnerabilities that are currently documented. Because past blended threats were able to successfully exploit vulnerabilities that were known for several months, it appears that many recently discovered vulnerabilities remain highly viable targets for future threats.
- A number of widely used open source applications were trojanized with backdoors over the past year. The attacks targeted high profile distribution sites that had taken significant efforts to protect themselves. This may serve as a warning not only to other open source projects, but also to commercial software vendors. Rather than targeting individual systems, attackers are clearly exploring alternative ways of impacting a large number of systems in a short period of time.
- Web client vulnerabilities, specifically those that affect Microsoft's Internet Explorer, should be closely watched over the next year. The volume and severity of these vulnerabilities increased substantially over the past year.

MALICIOUS CODE TRENDS

Blended threats continue to present the greatest risk to the Internet community.[3]

- Three blended threats (namely Klez, Bugbear, and Opaserv) were the source of nearly 80% of malicious code submissions to Symantec Security Response over the previous six months.
- In addition, a large percentage of cyber attacks detected by Symantec Managed Security Services clients were caused by only a handful of both old and new blended threats, such as Bugbear, Nimda, and Code Red.
- Because recent forms of malicious code, such as Bugbear, continued to successfully exploit vulnerabilities that were at least one month old, the Internet community as a whole still appears to be highly vulnerable to new blended threats that exploit known vulnerabilities as a method of propagation.

Infection vectors (method of exploitation) and payload preferences have changed over the past six months.

- Self-replicating mass mailers experienced a sharp increase in volume. Eight of the top 50 reported threats over the past six months were classified as self-replicating mass mailers, as opposed to only 1 out of the top 50 during the same six-month period in 2001.
- Malicious code that steals confidential information from users has increased substantially over the past year. The potential for exposing trade secrets, sensitive financial information, and other forms of proprietary data could easily increase the damage potential by orders of magnitude.

Technologies that are just now entering the mass market present highly attractive opportunities for malicious code writers.

- High market penetration and increasing unauthorized usage of instant messaging and peer-to-peer (P2P) applications make these programs an attractive infection vector for future blended threats.
- Mobile devices are expected to achieve stronger market penetration in 2003 and 2004. Often deployed with relatively weak security protection, these devices represent a highly attractive infection vector for future malicious code.

[3] Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By utilizing multiple methods and techniques, blended threats often spread rapidly and cause widespread damage.

Cyber Attack Activity

NETWORK-BASED CYBER ATTACK ACTIVITY

OVERVIEW

Symantec houses one of the world's largest and most detailed repositories of cyber attack data. These repositories consist of data collected from thousands of firewalls and intrusion detection systems (IDSs) throughout the world. The sample set studied in this report includes more than 400 companies, located in more than 30 countries. Complimenting this data set, Symantec analysts at four Security Operations Centers (SOCs) deployed throughout the world constantly review attack data and trends in order to identify and monitor the latest threats. The statistics and expert commentary in this section draw from these resources.

Overall, an analysis of attacks detected during the past six months reveals that network-based cyber attacks remain a substantial threat to organizations of all types. While the overall volume of activity declined by 6% during the past six months, Symantec noted several interesting developments related to topics, such as event severity, threat variance by company type, and patterns of activity by attack source. Findings are provided under the following sub-sections:

- General Attack Trends
- Attack Activity by Company Type
- Attacker Profiles
- Cyber Terrorism
- Internal Abuse and Misuse

As a reminder, unless otherwise stated, the statistics presented in this section exclude activity from major worms and blended threats, such as SQL Spida and Code Red. Only a handful of worms and blended threats accounted for 78% of all attack activity detected by Symantec over the past six months. While this is an important observation in and of itself, the topic of worms and blended threats is addressed adequately in the Malicious Code Section of the report. Eliminating this type of activity in this section enabled Symantec to identify underlying cyber attack trends of importance that would otherwise be obscured or completely hidden by the sheer volume of activity from major worms and blended threats.

GENERAL ATTACK TRENDS

Overall Attack Activity

The overall rate of cyber attack activity during the past six months was 6% lower than the rate recorded during the prior six-month period. While fluctuations occurred each week, on average, companies suffered approximately 30 attacks per company per week during the last six-month period, as compared to 32 attacks per company per week during the prior six-month period. Despite this decline, the rate of attack activity over the past six months remained 20% higher than the rate recorded during the same six-month period in 2001. **Figure 1** shows the average attacks per company per week over the past 12 months.

In terms of attack type, 85% of attacks were classified as pre-attack reconnaissance, which, in isolation, did not necessarily present an immediate threat to organizations. The remaining 15% of attacks consisted of attempted (or in some cases) successful exploitation attempts.[4] **Figure 2** shows a breakdown of all cyber attack activity detected by the sample set over the prior six-month period.[5]

Event Severity

All of the companies in the sample set experienced at least some form of attack activity on a daily basis over the past six months; however, the majority of this activity was determined to be relatively non-threatening in nature. When classifying malicious activity, severe events involve sequences of attack activity that have either caused a security breach on a company's network or present an immediate danger of a security breach if intervention is not taken. For example, if Symantec detects a successful scan for FTP followed by several exploit attempts, and the targeted network has multiple FTP servers with well-known, high-risk vulnerabilities, the activity is classified as a "severe" event. For a full description of this classification system, see **page 39** of **Appendix A**. Specific observations relating to trends in event severity are outlined below.

- More than 99% of all events detected by Symantec were classified as non-severe and did not represent an immediate threat to the companies in the sample set. These types of events typically consisted of reconnaissance activity that

[4] An example of reconnaissance activity is a scan launched by an attacker to detect a particular service, such as FTP. On the other hand, an exploit attempt is an action taken by an attacker to use a known vulnerability to gain unauthorized access to systems or create a denial of service.
[5] **Figure 2** includes worm and blended threat activity in the analysis simply to illustrate graphically the magnitude of this activity.

was not followed up with exploitation attempts, or probes for specific vulnerabilities that were known to be unavailable on the target systems.

- Companies were slightly less likely to experience a severe event during the past six months than they were during the prior six-month period. Specifically, 21% of companies suffered at least one severe event, as compared to 23% during the prior six-month period.
- Severe event incidence rates remained considerably lower than those observed during the same six-month period in 2001, in which the incidence rate was 43%. While several factors may have influenced this trend, observations from the past two studies strongly indicate that it is at least partially attributable to gradual strengthening of the security postures of companies represented in the sample set. Therefore, the apparent decline in risk for this sample set may not hold true for the Internet community as a whole. This observation is discussed in more depth on **page 14**.

Figure 1.
Attacks per Company per Week
(Jan 1, 2002 – Dec 30, 2002)

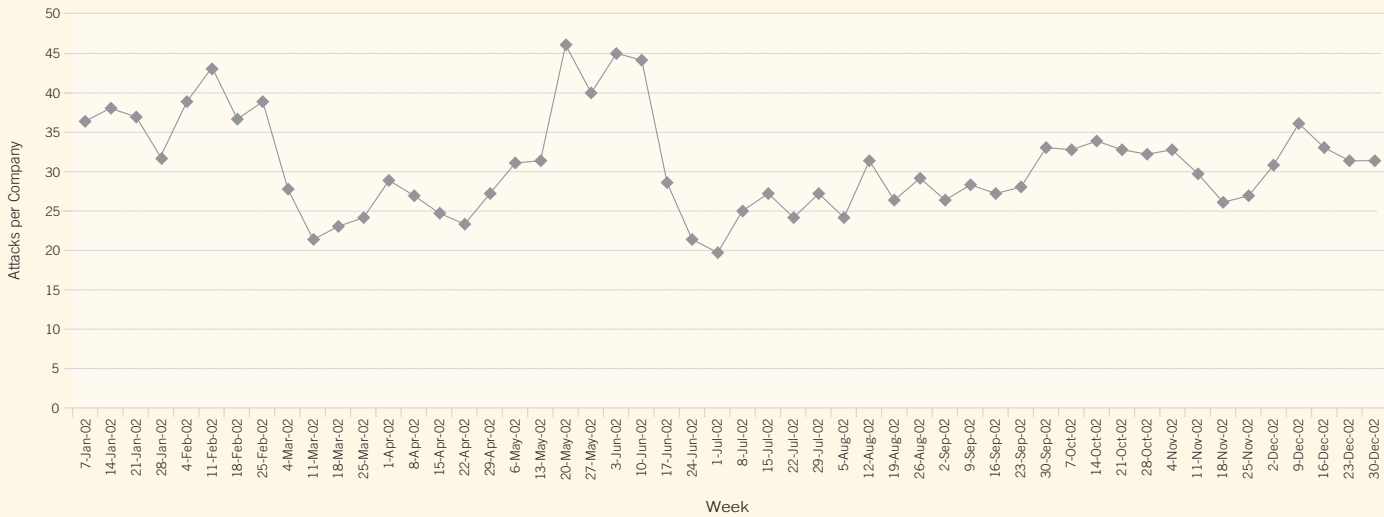


Figure 2.
Attack Activity by Type
(July 1, 2002 – Dec 31, 2002)

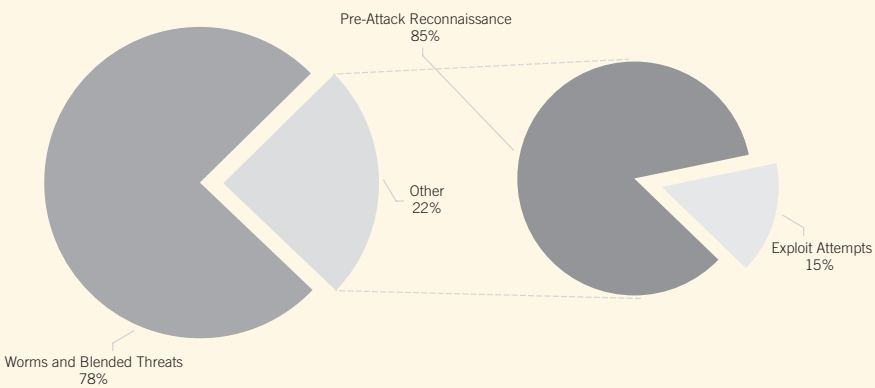


Figure 3 shows the severe event incidence rate at companies in the sample set over the past three six-month periods.

Attacker Aggression

In the July 2002 issue of the Internet Security Threat Report, a metric called attacker aggression, was used to reveal differences in the level of effort that attackers were willing to exert to penetrate network defenses and the extent to which those attackers were focused on a particular target. Analysis indicated a sharp drop in the occurrence of highly aggressive attacks. As a result, this analysis failed to yield a critical mass of highly aggressive events. Specifically, less than 2% of all companies in the sample set experienced a highly aggressive event, as compared to 10% during the prior six-month period. Lacking a sufficient sample of companies affected by highly aggressive events, comparisons across industry and by company size were not done.

Figure 3.
Severe Event Incidence by Study Period
(July 1, 2001 – Dec 31, 2002)

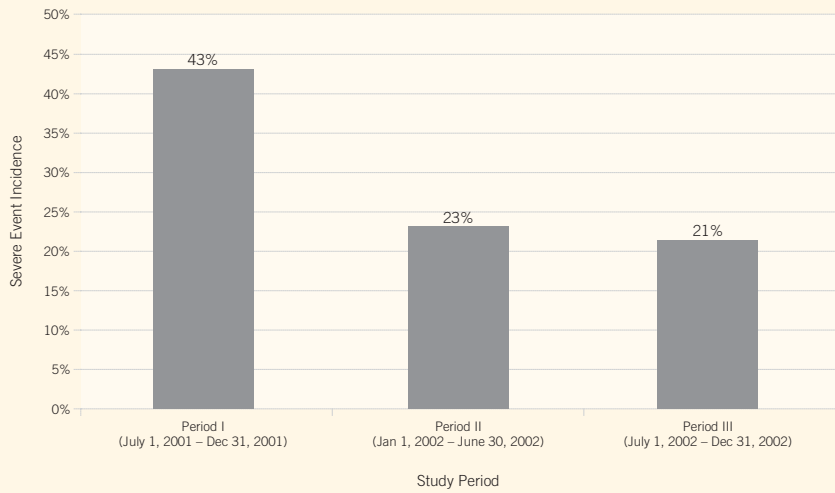
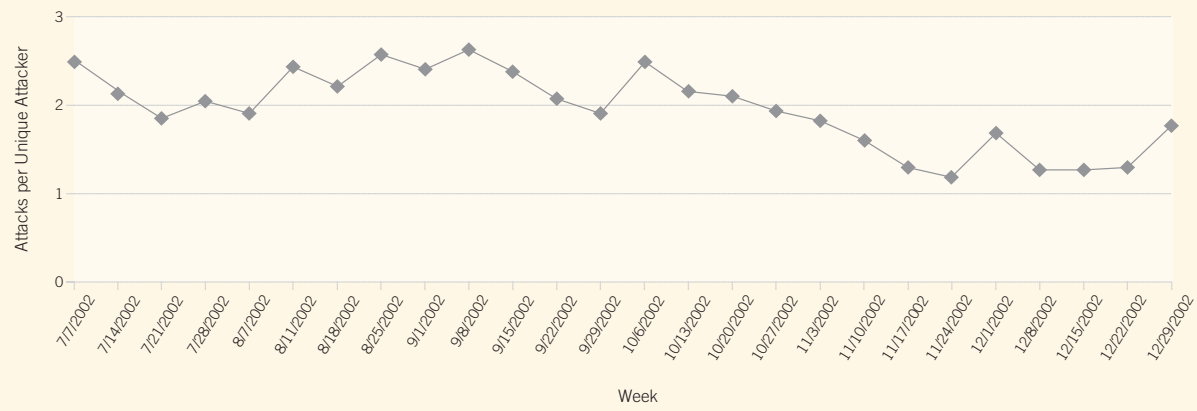


Figure 4.
Average Attacks per Unique Attacker
(July 1, 2002 – Dec 29, 2002)



Analysis using a second metric also suggested that there was a decline in aggression over the past six months. This metric measured the average number of attacks per unique attacking IP address. The more attacks per attacker, the higher the overall aggression of attackers. Results of this analysis revealed that in the fourth quarter attackers on average performed 15% less actions against companies in the sample set than they did in the third quarter. **Figure 4** tracks the average number of attacks per unique attacker over the past six months.

Based on the results of these two inquiries, it appears that attacker aggression declined during the past six months. This observation, coupled with observations by Symantec analysts, supports the conventional wisdom that most attackers search for a few vulnerabilities to exploit, and will abandon their efforts if these vulnerabilities are unavailable. However, even if this is true, companies should not find false comfort in the knowledge that, at any given moment, most attackers are probably only targeting a small subset of vulnerabilities. This is because the specific contents of an attacker's toolkit can change overnight. For example, the release of a new hacking tool or the emergence of a new blended threat can quickly transform unpopular vulnerabilities into top targets.

Threat Variance by Time

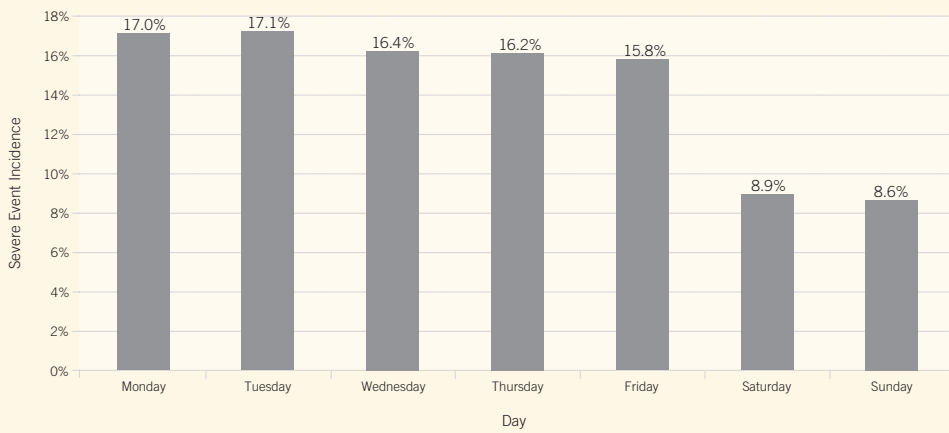
Maintaining adequate defenses against cyber attack activity is inevitably a 24x7x365 obligation. Attackers and malicious code can strike organizations from anywhere in the world, on any day of the week, and at any time of day. While it is indisputable that the overall threat of attacks never completely subsides during any specific time period, Symantec has isolated certain days of the week and certain hours of the day in which attackers show an unusually high or unusually low level of activity. These observations are explained in greater detail in the remainder of this section.

ATTACKER ACTIVITY BY DAY OF WEEK

Over the past six months, organizations experienced substantially lower levels of attack volume and attack severity during the weekends. These observations are consistent with those recorded during the prior six-month period. Statistics showing threat variance by day of week include:

- Total attacks on Saturdays and Sundays were 50% lower than total attacks on any other day of the week. This observation is illustrated in **Figure 5.**

Figure 5.
Attacks by Day of Week
(July 1, 2002 – Dec 31, 2002)



- The total number of unique attackers on Saturdays and Sundays was approximately 50% lower than the total on any other day of the week. This observation is illustrated in **Figure 6**.
- The total number of severe events on Saturdays and Sundays was at least 25% less than the total on any other day of the week. This observation is illustrated in **Figure 7**.

ATTACKER ACTIVITY BY TIME OF DAY[6]

Measurements of attacks by time of day are skewed by the fact that both victims and attackers may be located in multiple time zones. For the purpose of this report, we treated time of day as two distinct metrics: time of day from a victim's perspective and time of day from an attacker's perspective. The results strongly suggest that fluctuations in the rate of attack activity experienced by all Internet-connected organizations are largely a function of the local times in which the attacking systems are located, not the local time in which victims are located. This observation is explained in greater detail.

Figure 6.
Unique Attackers by Day of Week
(July 1, 2002 – Dec 31, 2002)

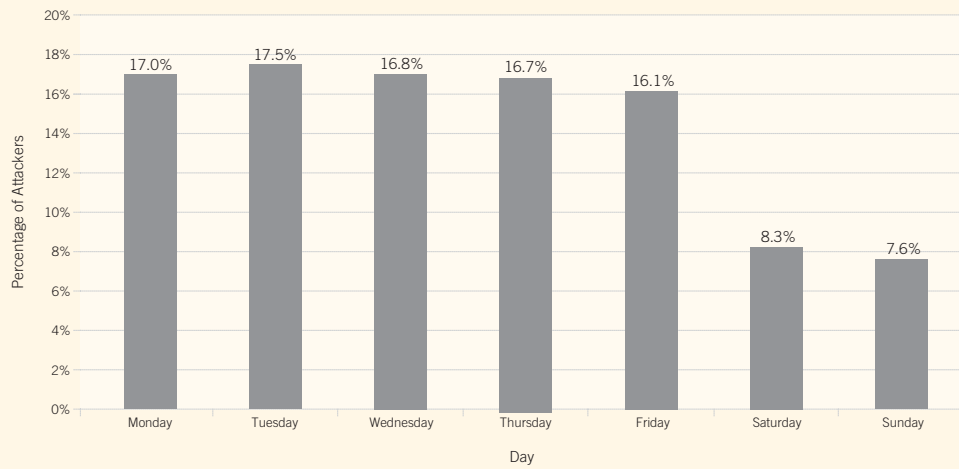
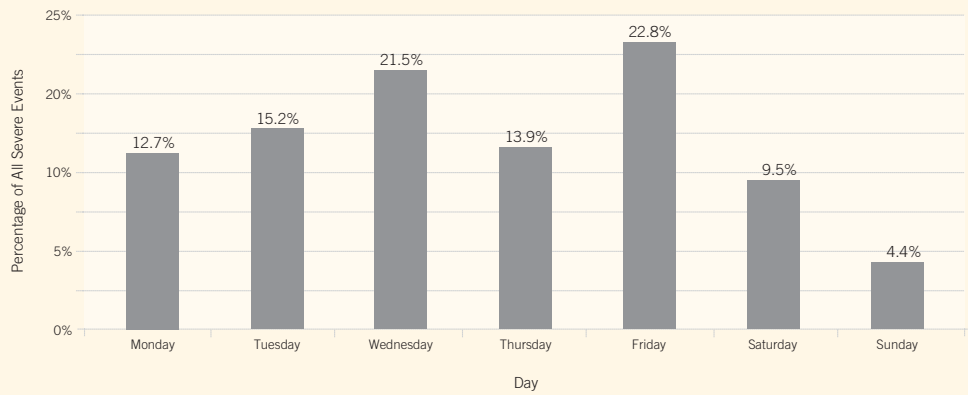


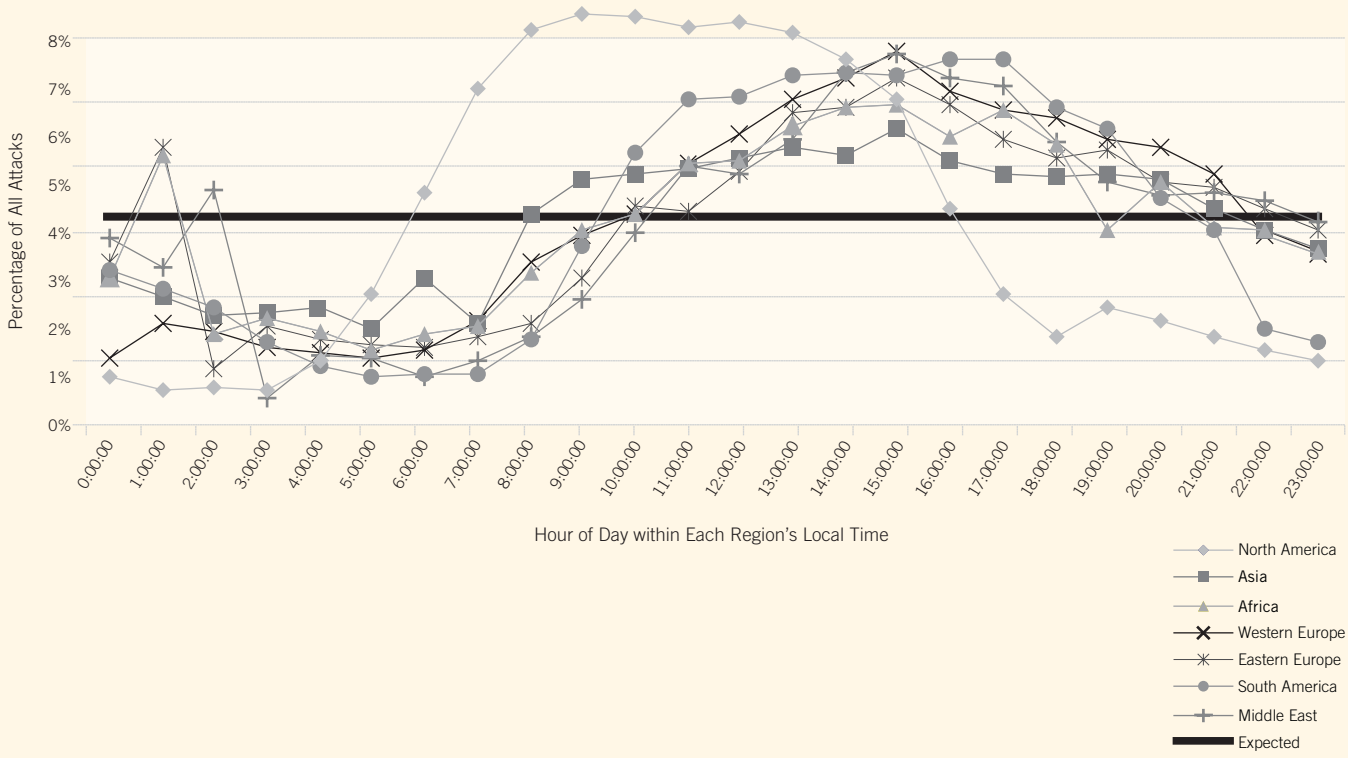
Figure 7.
Severe Events by Day of Week
(July 1, 2002 – Dec 31, 2002)



[6] Tracking the "true" source of attacks is extremely difficult. Attackers can jump through multiple systems and countries before hitting their intended target. Therefore, the data in this section only summarizes the last hop that the attacker took before hitting his/her intended target.

- Attacking systems are generally more active between the hours of 7:00 and 20:00 in their respective local time zones. **Figure 8** shows the percentage of total unique attackers detected per hour from 7 major regions throughout the world normalized to local time.[7]
- Due to the lack of geographic boundaries governing access to Internet-connected organizations, attackers often target victims on a global basis. As a result, variance in attack volume from the victim's perspective is a function of when attackers located in different regions throughout the world generally achieve peak activity.
- Several regions with relatively high attack volumes reach their peak levels of activity within the same general window of time each day. As a result, regardless of where a victim is located, attacker activity consistently peaks between the hours of 12:00 and 21:00 GMT. Individual organizations throughout the world must put this observation into the context of their local times to determine when they should expect to see peaks in attacker activity. For example, the peak hours of activity in New York City, USA are 7:00 AM to 4:00 PM (GMT–5 hours), while the peak

Figure 8.
Attacker Activity by Hour Normalized to Local Time
(July 1, 2002 – Dec 31, 2002)



[7] Oceania was not included in this analysis because this region contributed less than 1% of overall attack activity and was the only region that did not show a recognizable pattern of peak activity by hour of day.

hours of activity in Beijing, China are 8:00 PM to 5:00 AM (GMT +8 hours). **Figure 9** shows the percentage of unique attackers detected against the sample set by hour of day, and **Figure 10** shows when peak activity occurs in the corresponding local times for each major region used in this analysis.

ATTACK ACTIVITY BY COMPANY TYPE

Client Tenure

Symantec uses a metric, called client tenure, to assess how the effectiveness of a company's attack defenses evolves as they improve their security posture over time. Symantec analysts have historically provided anecdotal evidence that a relationship existed between client tenure and

Figure 9.
Attackers by Hour of Day
(July 1, 2002 – Dec 31, 2002)

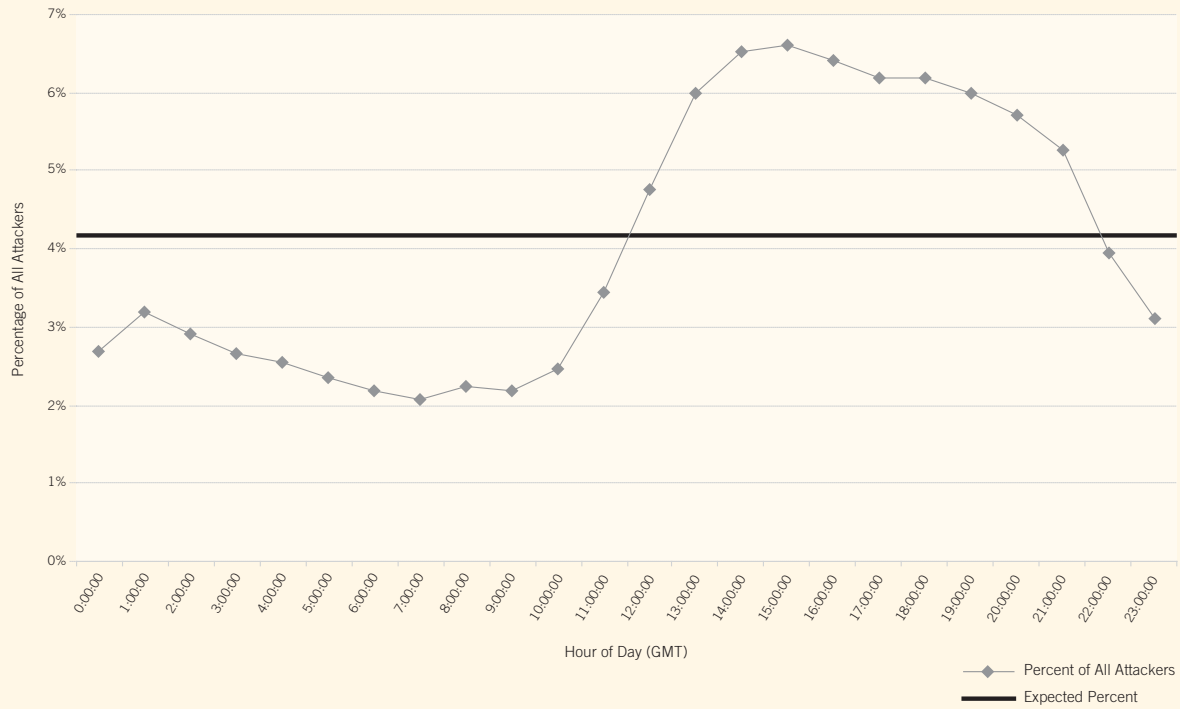


Figure 10.
Peak Activity

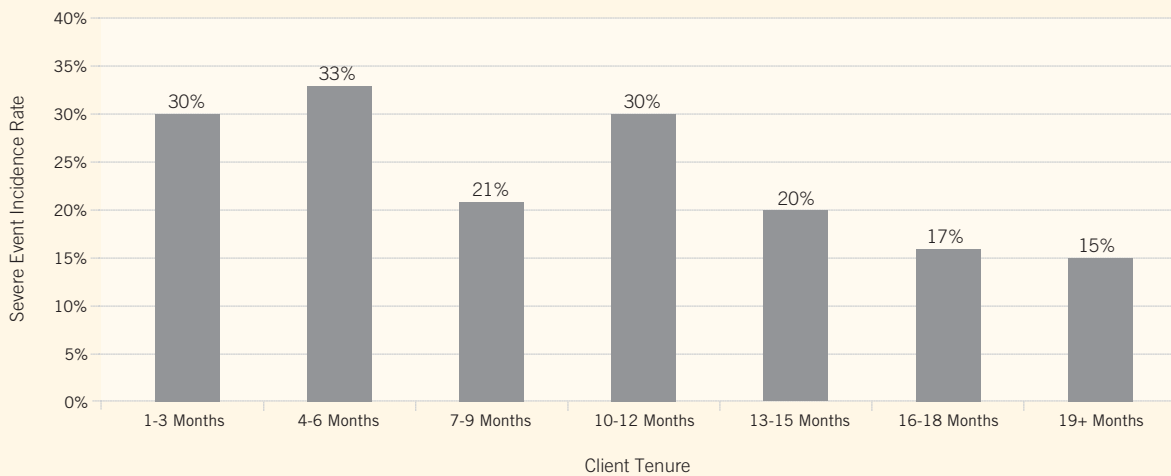
Region	Peak Activity
North America	12:00 to 21:00
Asia	2:00 to 13:00
Western Europe	11:00 to 21:00
Eastern Europe	8:00 to 21:00
South America	12:00 to 21:00
Middle East	8:00 to 19:00
Africa	8:00 to 16:00

the relative severity of attack activity. For example, analysts observed that as tenure increased, clients became much less likely to suffer security breaches. In order to quantify this observation, Symantec continually assesses the effect of client tenure on a company's likelihood of suffering one or more severe events.

Confirming observations from the previous study, as client tenure of companies in the sample set increased, the likelihood of suffering a severe event decreased. This is presumably due to the fact that clients strengthen their security posture as they improve their defenses against the types of attacks that they witness on a daily basis. Observations supporting this theory are outlined below.

- Approximately 29% of clients with less than 12 months of tenure experienced at least one severe event over the past six months, as compared to 17% with greater than 12 months tenure. These incidence rates are almost identical to those observed during the prior six month period, which recorded rates of 30% for clients with less than 12 months of tenure and 17% for clients with greater than 12 months of tenure. The results of this inquiry are presented in **Figure 11.**
- In addition to tracking differences in severe event incidence among clients with different levels of tenure, Symantec also tracked a control group over the past year to assess differences in severe event incidence as this group gained tenure. Symantec performed this analysis by calculating the severe event incidence rate for a control group that had 1-18 months of tenure during the study period ending on July 31, 2002, and 7-24 months of tenure during the last six-month period. The results revealed that the control group suffered an incidence rate of 28% in the period ending on July 31, 2002 and a rate of 20% during the last six months. These findings once again support the observation that the likelihood of suffering a severe event decreases as client's improve their security posture.

Figure 11.
Severe Event Incidence by Client Tenure
(July 1, 2002 – Dec 31, 2002)



Industry

Attack activity by industry was relatively similar to that reported during the prior two six-month periods. However, there were several interesting trends that were revealed by comparing historical rates of attack activity with current rates. Specific observations are presented below.[8]

- The Power and Energy industry continued to show the highest rate of both attack volume and severe event incidence. Attack volume for the entire six-month period was 987 attacks per company, and approximately 60% of power and energy companies experienced at least one severe event.[9]
- The financial services industry, which the Internet community often assumes to be an attractive target for attackers, showed a substantial increase in severe event incidence. Specifically, the severe event incidence rate for the six-month period ending December 31, 2001 was 28%, while the rate for the past six months was 48%.
- The nonprofit sample set, which included several high-profile activist groups, showed substantial increases in attack volume and a moderate increase in severe event incidence over the past three study periods. Specifically, attack volume over the past six months was 43% higher than volume during the six-month period ending December 31, 2001, while severe event incidence increased by only five percentage points over the same period of time. This trend is particularly noteworthy because many people do not instinctively believe that the nonprofit sector is a popular target for attackers. While it is inherently difficult to identify causality behind this trend, it is possible that the rise is related to cyber hacktivism.[10] Because the nonprofit sector in the sample set included several groups that are self-reported targets of cyber hactivist activity, it is possible that this rise is indicative of a more widespread increase in this type of activity.
- Telecommunications companies, which were not previously tracked as a distinct category of companies, showed high rates of both attack volume and severe event incidence. Telecommunications companies recorded attack volume of 845 attacks per company and 25% suffered at least one severe event.[11]

Figure 12 and **Figure 13** show attack volume and severe event incidence by industry over the past six months.

[8] Industries discussed in this section account for the following percentages of companies in the overall sample set: Financial Services (14%), Nonprofit (6%), Power and Energy (4%), and Telecommunications (3%).
[9] Symantec only monitors the corporate networks of power and energy companies; attacks contributing to these statistics did not necessarily endanger critical systems, such as SCADA systems.
[10] Hactivisim is defined as the misuse of computers in carrying out various objectives related to activist causes.
[11] Symantec only monitors the corporate networks of telecommunications companies; therefore, these statistics do not reflect attack activity against the infrastructure maintained by telecommunications companies.

Figure 12.
Attacks per Company by Industry
(July 1, 2002 – Dec 31, 2002)

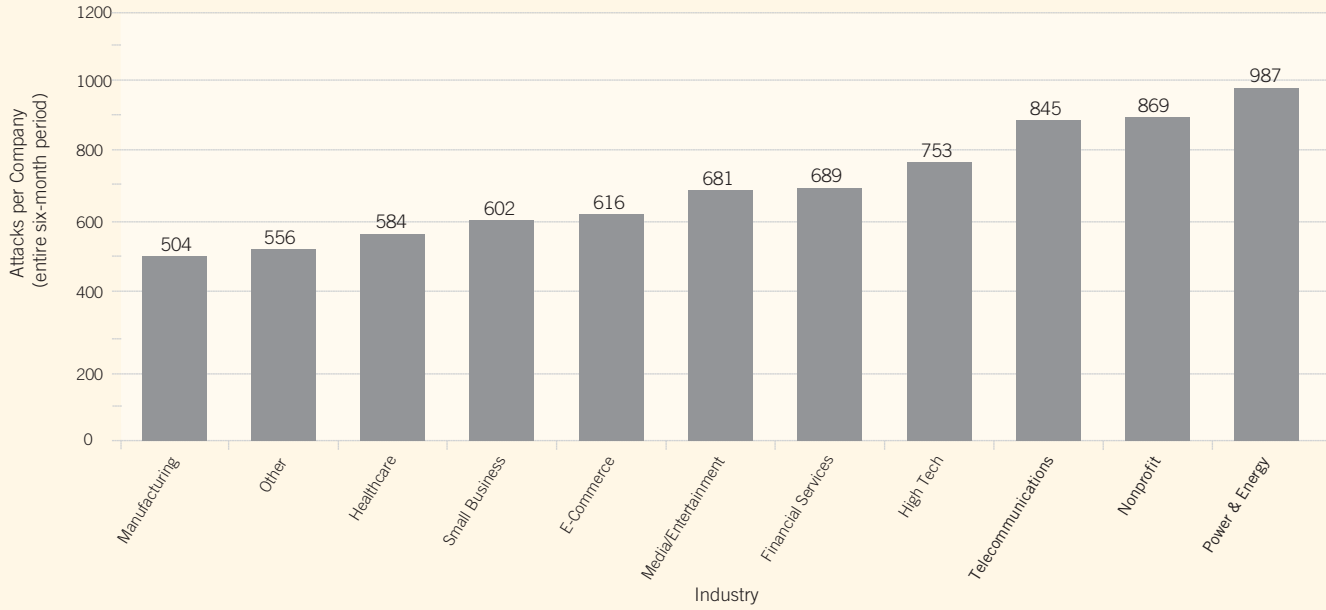
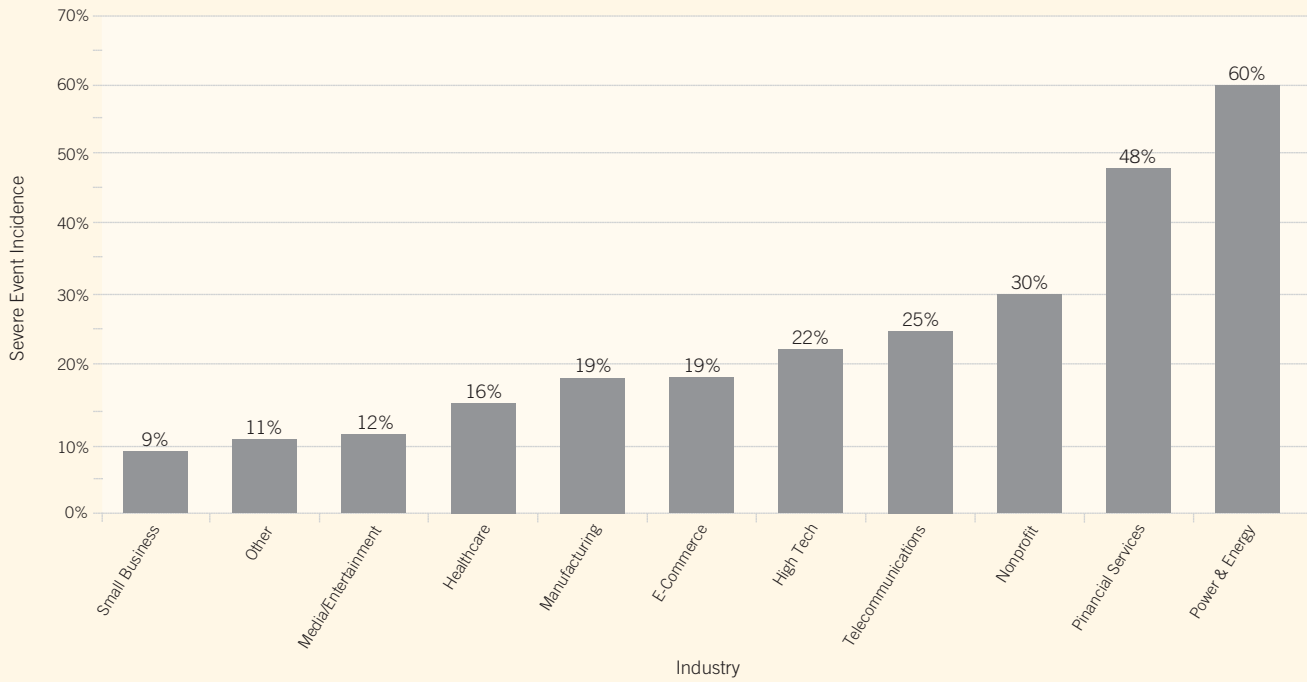


Figure 13.
Severe Event Incidence by Industry
(July 1, 2002 – Dec 31, 2002)



Company Size

In order to evaluate attack activity by company size, Symantec continues to use employee count as a proxy. The results of the current study mostly confirm past observations, which indicated that both attack volume and severe event incidence increased with company size.

This observation is logical for several reasons. First, larger companies by their very nature typically have bigger networks, which often attract more attacks simply due to their size. The more IP space and systems maintained by a company, the more attacks they will likely attract. Second, larger companies often have networks that are substantially more complex than those at smaller companies, and therefore may be more prone to security lapses that enable attackers to launch successful attacks. As a result, one would expect severe event incidence rates to rise with company size. Finally, larger companies have more public exposure than smaller companies, and therefore they may be more likely to attract attacks that are specifically targeted at them. If this is true, it would influence both attack volume and severe event incidence.

Figure 14 and **Figure 15** show attack volume and severe event incidence by company size over the past six months.

Figure 14.
Attacks per Company by Size
(July 1, 2002 – Dec 31, 2002)

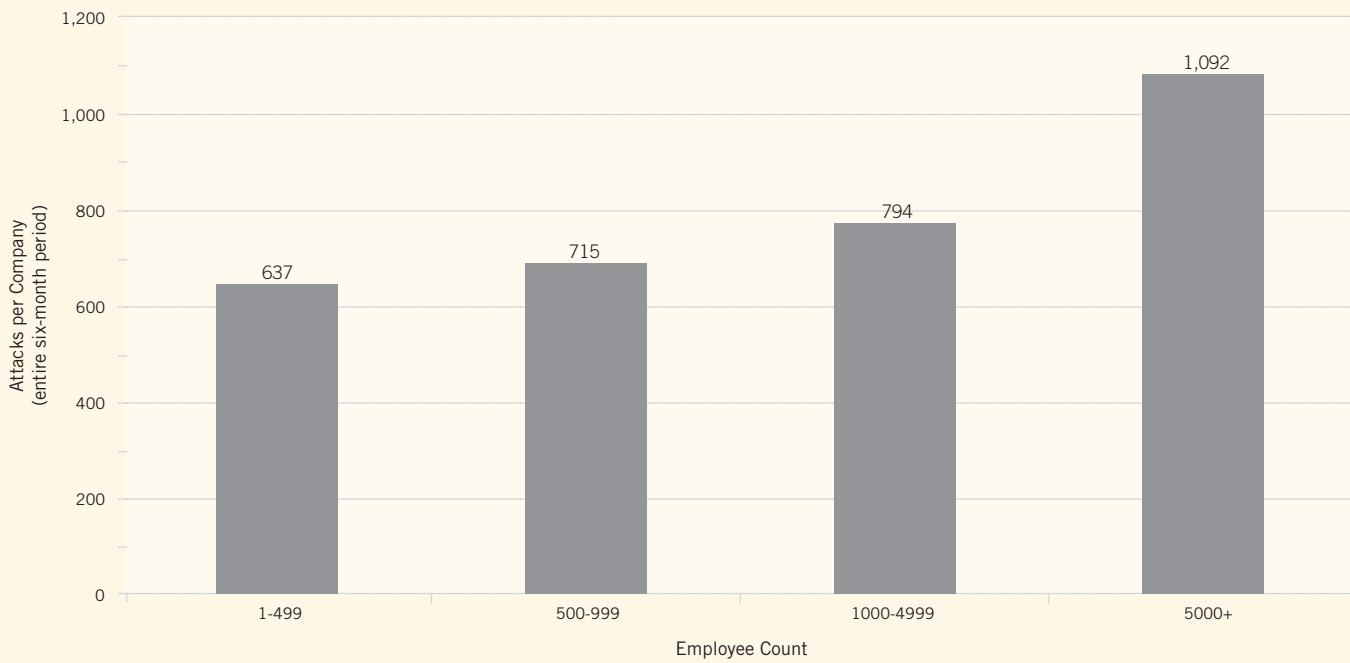
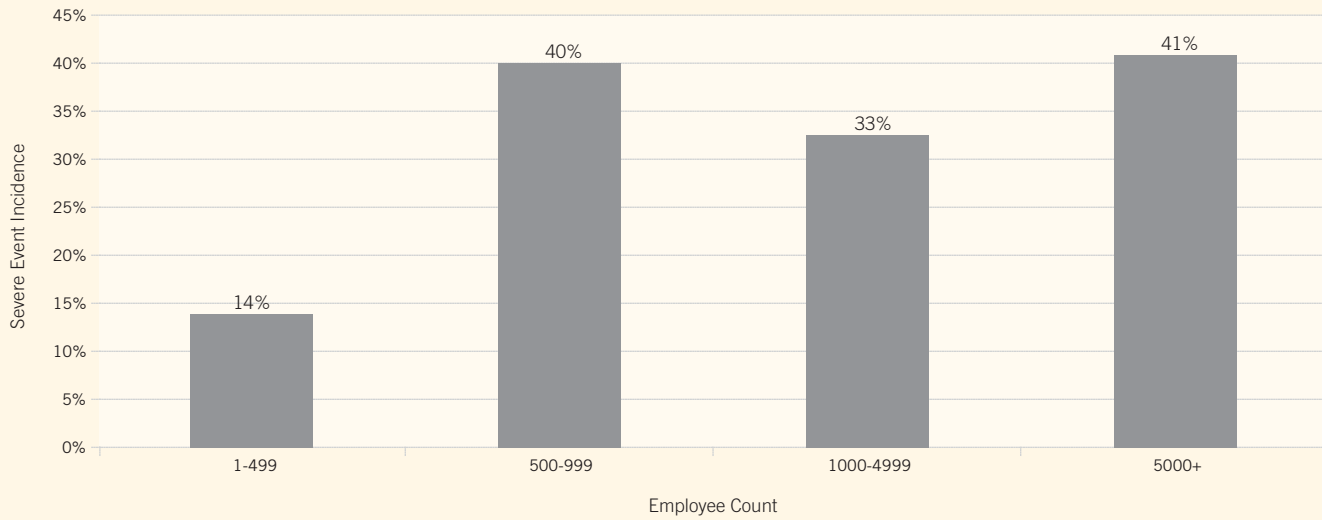


Figure 15.
Severe Event Incidence by Company Size
(July 1, 2002 – Dec 31, 2002)



ATTACKER PROFILES

Attacks by Source[12]

An analysis of attacks by country of origin revealed many similarities with the prior six-month period. Once again, the vast majority of attacks were launched from only a few countries. For example, the top ten countries alone accounted for 80% of all of the attacks detected against the sample set. In addition to this broad observation, there were a few countries that showed substantial shifts in attack activity. Several of the most notable observations include:

- South Korea had a substantial increase in attack volume over the past year (particularly in recent months). Total attacks launched from South Korea during the past six months were 62% higher than the total during the prior six-month period. Further, South Korea was the number one country in terms of attacks per 10,000 Internet users among Tier One countries,[13] as opposed to number six during the prior six-month period.
- There are several possible factors influencing this trend, many of which are difficult to measure. However, one such factor is the high rate of growth in the use of broadband connectivity. According to a recent survey by the *International Telecommunications Union*, South Korea is the leader in broadband usage, with 58% of home users currently connected.[14] This makes South Korean systems attractive launch points for attackers both within the country and throughout the world. The rise in attacks from South Korea may be an indicator of what network attack patterns will look like in other countries

[12] Tracking the "true" source of attacks is extremely difficult. Attackers can jump through multiple systems before hitting their intended target. The data in this section only summarizes the last hop that the attacker took before hitting his/her intended target. It is possible that many attacks contributing to these statistics do not represent the true source of origin.
[13] When evaluating attacks per 10,000 Internet users, countries were separated into two tiers. Tier One countries include those with more than 1 million Internet users; Tier Two countries include those with between 100,000 and 1 million Internet users. These categorizations separate countries with relatively well-developed infrastructures from those with emerging Internet infrastructures.
[14] "Asia-Pacific Telecommunications Indicators 2002." International Telecommunications Union. (December 2, 2002).

as broadband becomes more widely deployed. It also speaks to the importance of protecting home computers, especially when they have access to corporate resources through Internet-based VPNs.

- Israel, which was number one on the list of top ten attacking countries per 10,000 Internet users among Tier One countries during the first two study periods, dropped to number 10 during the last six months. Total attack volume from Israel dropped by approximately 50% during this time period.
- Several Eastern European countries have shown increases in both attack volume and attacks per Internet capita. For example, Poland moved from number eight in terms of attacks per 10,000 Internet users during the six-month period ending December 31, 2001 to number two in the past six months. In addition, four Eastern European countries (Latvia, Romania, Lithuania, and Slovakia) were listed on the top ten countries per 10,000 Internet users among Tier Two countries.
- Iran and Kuwait continue to top the list of the top ten attacking countries per 10,000 Internet users among Tier Two countries.

Tables 16, **17**, and **18** show the top ten attacking countries in terms of overall volume and per Internet capita for the past three study periods.

Figure 16.
Top Ten Attacking Countries in Terms of Overall Volume
(July 1, 2001 – Dec 31, 2002)

Country	Percent of Total (July 1, 2002 – Dec 31, 2002)	Percent of Total (Jan 1, 2002 – June 30, 2002)	Percent of Total (July 1, 2001 – Dec 31, 2001)
United States	35.4%	40.0%	29.6%
South Korea	12.8%	7.4%	8.8%
China	6.9%	6.9%	7.8%
Germany	6.7%	7.6%	5.9%
France	4.0%	5.2%	4.5%
Taiwan	3.9%	2.4%	2.6%
Canada	3.2%	3.0%	3.9%
Italy	3.0%	2.7%	2.5%
Great Britain	2.2%	2.1%	2.5%
Japan	1.8%	2.1%	2.0%
TOTAL	**80.0%**	**79.6%**	**70.1%**

Figure 17.
Top Ten Attacking Countries per Internet Capita (Tier-One Countries*)
(July 1, 2001 – Dec 31, 2002)

Ranking	Country	Attacks per 10,000 Internet users (July 1, 2001 – Dec 31, 2001)	Ranking in Period II (Jan 1, 2002 –Jun 30, 2002)	Ranking in Period I (July 1, 2001 – Dec 31, 2001)
1	South Korea	23.7	6	4
2	Poland	18.4	5	8
3	Czech Republic**	14.2	11	NA
4	France	14.2	3	5
5	Taiwan	14.0	7	9
6	Hong Kong	13.9	2	2
7	Belgium	13.3	4	17
8	Mexico	11.8	13	14
9	China	10.8	10	11
10	Israel	10.1	1	1

* The values for the top ten countries differ considerably from values reported in the prior report. This is due to the fact that the CIA World Fact Book reported new Internet user figures in August 2002. Since many countries have substantially more Internet users, the corresponding per capita attack rate is typically much lower than was previous recorded.
** Czech Republic was #11 on the Tier Two list in July 2002 and was not ranked in January 2002 because the reported number of Internet users during these time periods was less than one million.

Figure 18.
Top Ten Attacking Countries per Internet Capita (Tier-Two Countries*)
(July 1, 2001 – Dec 31, 2002)

Ranking	Country	Attacks per 10,000 Internet users (July 1, 2002 – Dec 31, 2002)	Ranking in Period II (Jan 1, 2002 –June 30,2002)
1	Iran	29.3	2
2	Kuwait	23.3	1
3	Puerto Rico	22.0	7
4	Romania	21.1	10
5	Latvia	18.7	17
6	Tanzania**	16.9	N/A
7	Peru	16.2	3
8	Lithuania	13.0	13
9	Ecuador**	10.9	N/A
10	Slovakia	10.7	23

* During the first study period, attacks per Internet capita were not calculated for Tier Two countries.
** Tanzania and Ecuador were not ranked in the July 2002 report because the reported number of Internet users in each of these countries at the time was less than 100,000.

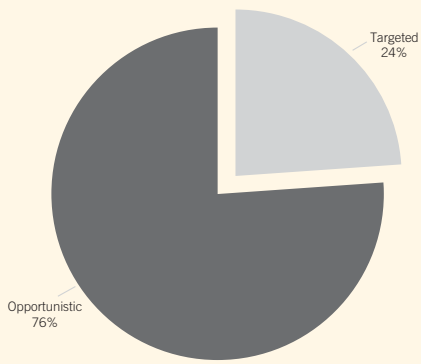
Attacker Intent

One of the most intriguing and challenging questions about cyber attacks is that of intent—was the attacker targeting a specific organization, or simply scanning the Internet in search of an opportunity to exploit vulnerable systems. Symantec's methodology to gauge intent separates attacks into two general categories: those that were opportunistic (i.e., the attack was intended to exploit any vulnerable organization discovered on the Internet), and those that were targeted specifically at a given organization. For a full description of the methodology, see **page 44 of Appendix A**.

Analysis over the past six months revealed that only 24% of attacks appeared to be targeted in nature, as compared with 37% during the prior six-month period. **Figure 19** shows the breakdown of opportunistic versus targeted attacks for the past six months.

While the percentage of targeted attacks has declined, the number still remains surprisingly high. Explaining the cause of the drop, however, is perhaps as difficult as explaining the specific motives of each attacker. The drop could be attributable to the fact that the companies in the sample set are not being specifically singled out by attackers as frequently as they were in the past. It could signal a general shift in mentality among attackers toward a more opportunistic approach. Unfortunately, due to the nature of this subject, causality is hard to determine with precision at this point.

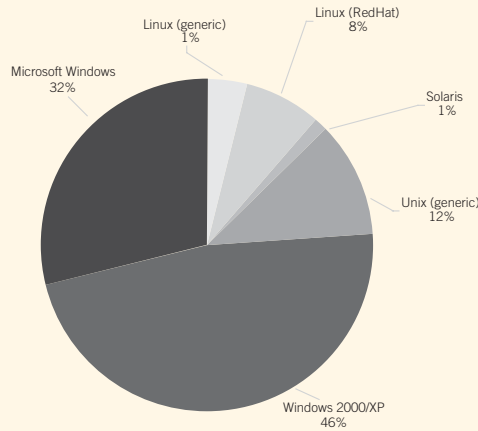
Figure 19.
Attackers by Attacker Intent
(July 1, 2002 – Dec 31, 2002)



Attacker Platform

Symantec maintains a system to identify and profile the platforms used by a random sample of attackers immediately after they are detected launching an attack. The intent of this system is to profile typical attackers both in terms of the systems that they most commonly use and the services that they most commonly run. The main insight from this analysis confirms previous findings—the Microsoft Windows suite of operating systems was used by a majority of attackers. Considering the dominant market penetration of Windows and the fact that most home users use Windows systems, this was lower than expectations. The breakdown of activity by attacker operating systems is presented in **Figure 20**.

Figure 20.
Breakdown of Attackers by Operating Systems Used
(July 1, 2002 – Dec 31, 2002)



Top 20 Scans

This section lists the 20 most frequent scans detected against companies in the sample set. The frequency of different types of scans provides a high-level snapshot of the types of reconnaissance activity in which attackers engaged over the past six months. It is important to note that worm and blended threat activity (most notably that associated with SQL Spida, Opaserv, and Bugbear) were included in this analysis.

Similar to previous reports, 99.9% of scanning activity was concentrated on only 20 services, each of which is listed in **Figure 21**. The substantial impact of both old and relatively new worms and blended threats on the scanning environment is also clearly illustrated in this table. For example, SQL Spida, which first emerged in May 2002, remained the single largest source of scanning activity during the past six months. Finally, it is important to note that services that are not included on this list can still become very popular targets with the discovery of a new vulnerability and development of exploit tools. For example, prior to the release of the SQL Spida worm in May 2002, Microsoft SQL was not included on the list of top 20 scans.

Figure 21.
Top 20 Scans
(July 1, 2002 – Dec 31, 2002)

Scan Type	Percent of Total Scans
Microsoft SQL Server	29.5%
HTTP	16.5%
FTP	13.3%
Netbios Name Service	13.0%
HTTPS	4.0%
SSH	3.2%
SMTP	3.1%
RPC (tcp)	2.5%
SubSeven	2.0%
Netbios (139/tcp)	1.8%
Netbios (445/tcp)	1.7%
SOCKS (1080/tcp)	1.3%
CDE Subprocess Control	1.1%
57/tcp	1.0%
Telnet	0.9%
Squid Proxy	0.9%
LPD	0.8%
135/tcp	0.6%
DNS	0.6%
1524/tcp (Ingreslock)	0.4%

Additional noteworthy shifts in attacker reconnaissance activity that are not immediately evident in **Figure 21** are explained below.

- **HTTPS**—Attackers scanned for HTTPS-enabled web servers at a higher rate over the past six months. This can be primarily attributed to a number of recently released Denial-of-Service (DoS) and Remote Access Buffer Overflow vulnerabilities affecting OpenSSL, an Apache web server extension that supports the HTTPS functionality. The most damaging of these vulnerabilities was the OpenSSL SSLv2 Malformed Client Key Remote Buffer Overflow Vulnerability (BID 5363), which the Linux.Slapper worm used to compromise vulnerable Apache servers. Therefore, a large portion of HTTPS scans is attributable to this worm.
- **SMB File Shares (445/tcp)**—Scans for SMB File Shares increased substantially over the past six months, which mostly reflects the widespread outbreaks of Opaserv variants. This protocol was introduced in Windows 2000 as an alternative to the use of Netbios for file sharing. As use of this protocol becomes more pervasive, it is becoming an increasingly popular infection vector for worms and blended threats. As systems continue to migrate to versions of Microsoft operating systems that use SMB file shares, attackers and malicious code writers will continue to target it on a more frequent basis.
- **SOCKS & Squid Proxies**—In order to disguise their true source of origin, attackers often route their connections through proxy services, such as SOCKS and Squid. This tactic allows them to launch attacks on third parties or view restricted websites with relative anonymity. In fact, automated tools on the Internet maintain databases of open proxies just to make it easier for such people to locate them. A large increase in scans for these proxies over the past six months suggests that attackers are increasingly searching for these services in order to disguise their identities.
- **57/tcp**—A popular methodology that attackers use to fingerprint a target's operating system requires the use of a closed TCP port. Over the past six months, at least one popular hacking tool emerged that uses port 57/tcp for this purpose.[15] Increases in scans for 57/tcp may indicate increasing usage of this reconnaissance tool. Prior to this six-month period, attackers rarely scanned for this port.
- **135/tcp**—The rise in port 135/tcp scans is primarily due to the increasing use of a new popular technique to deliver popup adds via the built in Windows System Alert. Spammers often use a built in Windows Remote Procedure Call (RPC) vulnerability on exposed Windows systems to deliver advertising messages. The rise in scans is most likely attributable to spammers who are searching for an audience.[16]

[15] Details on this tool are available at http://www.fx-tools.net/index.php.
[16] See http://online.securityfocus.com/news/1231 for more details on this vulnerability.

CYBER-TERRORISM

Overview

The question of whether cyber terrorism currently presents a real threat to companies and government organizations is the subject of much debate. Some individuals insist that not only is cyber terrorism a threat, it is actually happening today; others insist that this type of threat will probably not materialize in any meaningful form for several years.

Isolating and providing analysis of cyber terrorism cases has proven an extremely difficult task. The first challenge is that in order to truly isolate cyber terrorist activity, the intended results of individual attacks must be understood. Because Symantec typically identifies attacks in the early stages, it is often impossible to assess the intended results of attackers.

As an alternative, we have tracked activity from countries throughout the world that may be more likely than others to harbor cyber terrorists. Unfortunately, this technique introduces several sources of error. First, cyber terrorists (unlike conventional military attacks) can strike from any country in the world. Nobody knows if they will strike from the Middle East, the United States, Europe, or even from within one's own network. Further, even if we can reliably isolate likely source countries, cyber terrorists can disguise their identities by launching attacks from a compromised system in another, less suspicious country or by obfuscating the attack through open proxies.

Despite the potential flaws of tracking attacks from likely sources of cyber terrorism, we have decided that withholding this type of analysis was not a better alternative. This is mainly because understanding the overall volume and type of attack activity from countries that may be more likely than others to harbor cyber terrorists provides organizations with a general understanding of the level of technical sophistication of the population within these countries. For example, a review of scanning activity from countries on the Cyber Terrorist Watch List suggests that attackers from these countries rely on relatively antiquated hacking techniques. Whether or not this type of insight is truly relevant to investigations of cyber terrorism is hard to determine, but we believe that it is noteworthy.

With this in mind, the remainder of the section presents data measuring the volume and type of activity detected from systems located in countries on the Cyber Terrorist Watch List. For a full description of the methodology used to select countries on the list, see **Page 44**.

Summary of Findings

- Countries on the Cyber Terrorist Watch List produced no severe events against companies in the sample set, as opposed to one severe event that was produced by a system in Iran during the prior six-month period. Furthermore, Symantec detected no verifiable cases of cyber terrorist attacks during the past six months.
- Countries on the Cyber Terrorist Watch List generated less than 1% of all attacks detected during the past six months.
- Indonesia and Iran were the top two attacking countries on the Watch List, replacing Kuwait and Egypt, which topped the list during the prior six-month period. These four countries alone accounted for nearly 70% of all attack activity among Watch List countries.

Figures 22, 23, 24 show the volume and type of attacks launched from countries on the Cyber Terrorist Watch List.

Figure 22.
Attack Activity from Countries on Cyber Terrorist Watch List
(July 1, 2002 – Dec 31, 2002)

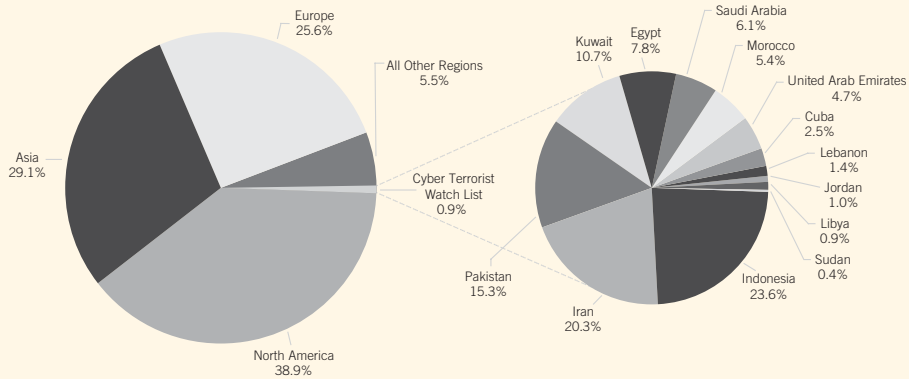


Figure 23.
Percent Rise in Attacks from Countries on Cyber Terrorism Watch List between 3rd and 4th Quarters
(July 1, 2002 – Dec 31, 2002)

Country	Change
United Arab Emirates	334%
Jordan	250%
Cuba	118%
Indonesia	35%
Saudi Arabia	26%
Lebanon	0%
Iran	-32%
Morocco	-48%
Kuwait	-61%
Egypt	-63%
Pakistan	-84%
Libya	-100%
Sudan*	N/A

* Sudan did not show any attacks during the third quarter; therefore, a growth rate could not be calculated.

Figure 24.
Top 20 Scans from Countries on Cyber Terrorist Watch List**
(July 1, 2002 – Dec 31, 2002)

Scan Type	Percent of Total Scans
FTP	32.2%
CDE Subprocess Control	13.6%
LPD	9.4%
SSH	8.6%
DNS	7.6%
HTTPS	5.2%
Hack Attack Trojan	5.0%
RPC (tcp)	4.1%
SubSeven	3.5%
57/tcp	2.9%
Telnet	2.4%
Netbios (445/tcp)	1.5%
SNMP	1.2%
Napster Proxy (8888/tcp)	0.9%
Netbios (139/tcp)	0.7%
AnalogX Proxy (6588/tcp)	0.4%
Squid Proxy	0.2%
SMTP	0.1%
SOCKS (1080/tcp)	0.1%
12345/tcp	0.1%

** Worm and Blended Threat-related attacks were not included in the analysis in order to reveal underlying attack trends.

INTERNAL MISUSE AND ABUSE

The vast majority of attacks detected by Symantec over the past six months were determined to be primarily external in nature. Although this report clearly demonstrates that external attacks are a substantial threat, organizations must also consider the threat of insiders.

Over the past few years, Symantec's Services Division has conducted numerous investigations of security incidents. A review of these cases suggests that the insider threat is just as severe as external threats. In fact, greater than 50% of all incidents to which Symantec responded involved abuse or misuse of company resources by employees. In addition, the amount of self-reported financial damage in these cases was significantly greater than that caused by external breaches. Over the course of the past two years, Symantec's team witnessed costly thefts of confidential information, cases of highly organized corporate espionage, cases of email harassment that led to multiple terminations (not to mention potential lawsuits), and even one case of email misuse that prompted criminal charges.

Perhaps the most frightening aspect of these incidents was the relative ease with which those responsible acted. Most perpetrators were not required to "hack" into any systems—system authorization was already granted to them as employees. In fact, system administrators, the employees typically responsible for granting levels of access, were often the guilty party.

Given the demonstrated danger of the internal threat, organizations must not ignore the need to maintain a high level of vigilance within their organization, as well as on the perimeter. Security administrators must not forget that issues, such as employee screening, segregation of IT responsibilities, and internal auditing are key aspects of an effective security posture. While internal breaches are often ignored and inherently difficult to detect, these types of incidents can be the most costly to an organization.

Vulnerability and Malicious Code Trends

EMERGENCE OF NEW VULNERABILITIES

OVERVIEW

The constant discovery of new IT product vulnerabilities continually adds to the complexity faced by the Internet community. The emergence of a single vulnerability can leave systems that are perceived to be secure at one moment rendered completely exposed to attack during the next. With multiple vulnerabilities emerging daily, the relative effectiveness of an organization's security posture is in a constant state of flux.

In addition to maintaining one of the largest repository of attack data, Symantec also maintains the most comprehensive vulnerability database and discussion forum. As this is the first time we have included such information in our Internet Security Threat Report, we are providing a high-level overview of the vulnerability environment during 2001 and 2002. The intent is to (1) outline several facts about IT product vulnerabilities, (2) highlight ways in which the discovery of new vulnerabilities is changing over time, and (3) discuss recent vulnerabilities that present the greatest risk to organizations.

GENERAL TRENDS

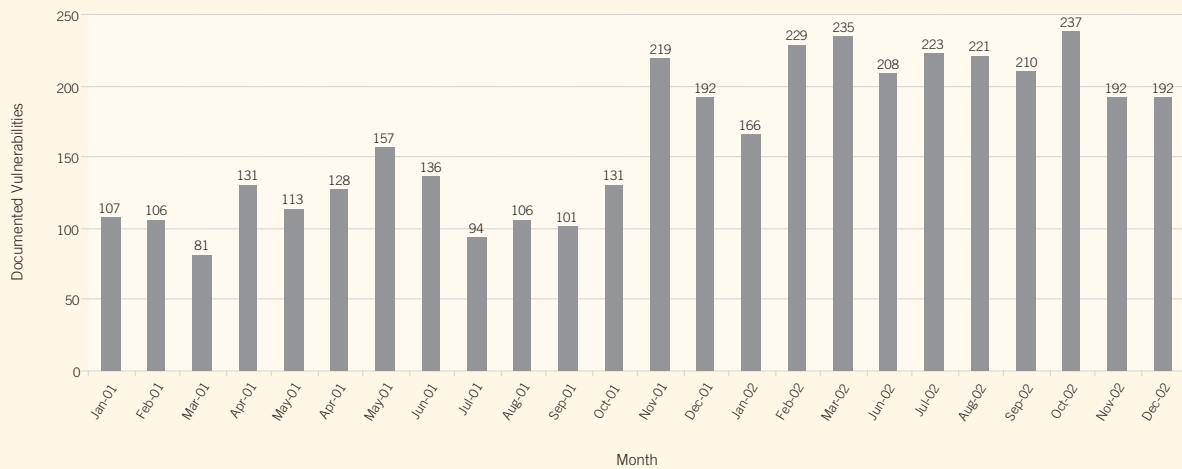
Overall Volume

In 2002, Symantec documented 2,524 vulnerabilities affecting more than 2,000 distinct products. This total was 81.5% higher than the total documented in 2001. **Figure 25** tracks this increase by showing the total number of new vulnerabilities documented monthly between January 1, 2001 and December 31, 2002.

The sharp rise in new vulnerability discoveries is probably attributable to a variety of factors, such as those listed below.

1. **Responsible Disclosure Movement**—In recent years, technology companies have increasingly adopted a policy of responsible disclosure. For example, many security research organizations and product vendors, including Symantec, have recently initiated a greater commitment to acknowledge and rectify emerging vulnerabilities with the formation of the Organization for Internet Safety. It is possible, therefore, that some of the rise may simply reflect the fact that vendors are now more likely to publicly acknowledge (and offer fixes for) new vulnerabilities that affect their products.

Figure 25.
Total New Vulnerabilities by Month
(January 1, 2001 - December 31, 2002)



2. **Lack of Vendor Prioritization of Security During Product Development Phase**—While open disclosure of vulnerabilities appears to be improving after products are available on the market, there still appears to be a persistent failure on the part of vendors to prioritize security concerns BEFORE new products and product versions are released. It is also possible that the declining economic conditions in the technology sector are exacerbating this issue.

3. **New Methods of Exploiting Software Bugs**—During the course of the past two years, vulnerability researchers have developed several new methods of exploiting programming errors, thus enabling them to identify a variety of vulnerabilities that were previously unknown. As a result, new threats, such as those involving advanced buffer overflows, heap overflows, and format strings, are now emerging more frequently.

4. **Increased Effort Among Vulnerability Researchers**—A portion of the rise may simply be a result of increased effort among individuals and organizations that dedicate their time to discovering new vulnerabilities. As more time and effort are invested, more vulnerabilities are discovered.

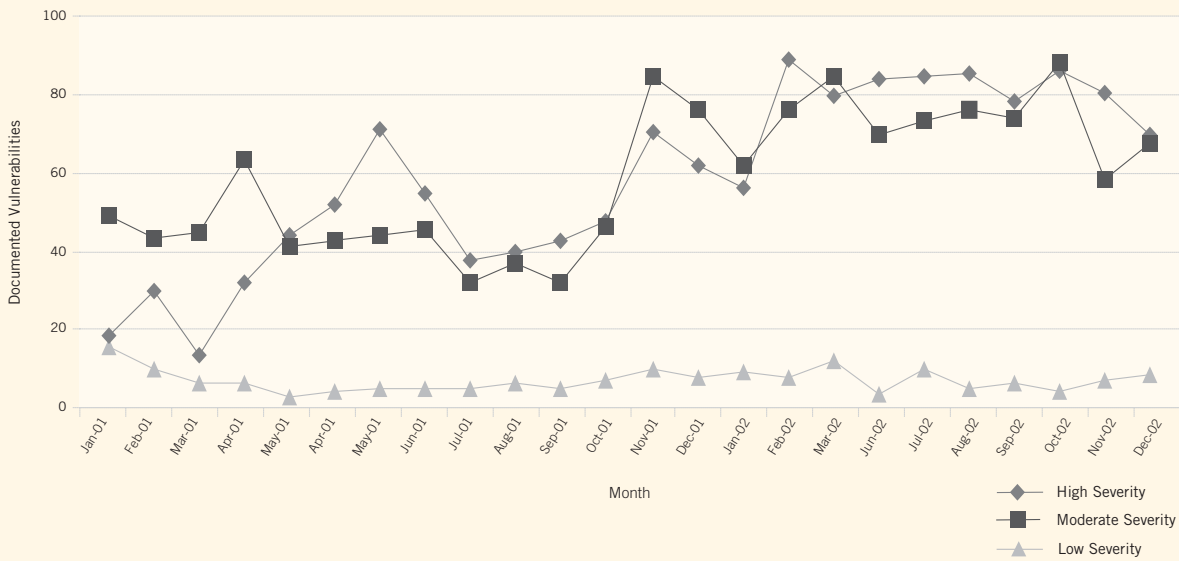
5. **Media Coverage**—Recent outbreaks of high-profile blended threats, which propagate by exploiting vulnerabilities, have increased the newsworthiness of vulnerability discoveries. The opportunity for publicity is frequently a motive of malicious code writers and hackers. Therefore, the promise of media coverage may be encouraging more intense searches for vulnerabilities, as well as more frequent public disclosures.

Regardless of cause, the number of vulnerabilities that attackers have at their disposal has increased substantially over the past two years. As a result, the potential exposure of corporate networks and systems to compromise by individual attackers and malicious code is also increasing.

Severity

Perhaps even more concerning than the overall increase of new vulnerabilities is the fact that this rise was driven almost exclusively by vulnerabilities rated as either moderately or highly severe.[17] In 2002, moderate and high severity vulnerabilities increased by 84.7%, while low severity vulnerabilities only rose by 24.0%. This trend is graphically illustrated in **Figure 26**.

Figure 26.
Vulnerability Volume by Severity
(Jan 1, 2001 – Dec 31, 2002)



[17] See **Page 47** of the **Appendix C** for a full description of how vulnerabilities are categorized by severity.

While it is difficult to isolate all of the factors driving this trend, Symantec believes that the following are the most critical:

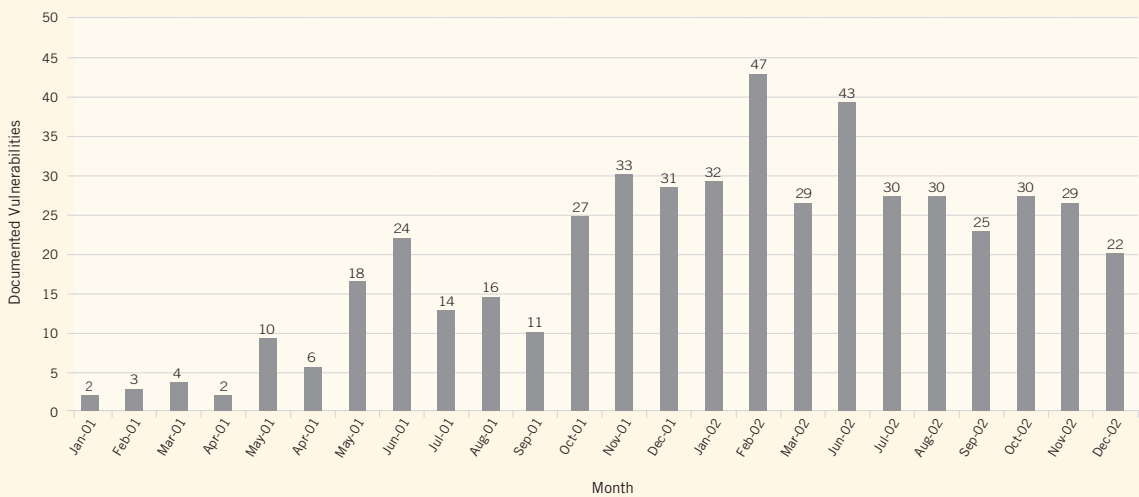
1. **Focused Research**—People dedicated to vulnerability research seem to spend more of their time looking for vulnerabilities with greater severity. This tendency is especially evident in vulnerability discussion forum conversations. In addition, the recent increase in searches for vulnerabilities affecting Internet Explorer is an excellent example of this tendency.
2. **Public Visibility**—Individuals and organizations that discover new vulnerabilities are much more likely to announce their discovery publicly if the vulnerability is relatively severe in nature. It is quite possible that the discovery of new, low-severity vulnerabilities is increasing at a comparable rate, but that these discoveries are not disclosed due to the lack of perceived impact.
3. **Proliferation of Web Applications**—Over the past few years, hundreds of new web applications have entered the market.[18] The nature of many of these applications renders them much more likely to have remotely accessible vulnerabilities that are relatively easy to exploit. Therefore, Web application vulnerabilities are almost universally classified as moderately to highly severe. Symantec observed a sharp rise in web application vulnerabilities over the past two years which accounted for many of the new moderate/high severity vulnerabilities. **Figure 27** illustrates this trend. Overall, the total number of web application vulnerabilities discovered in 2002 was 178% higher than the total discovered in 2001. Furthermore, 95% of these vulnerabilities were remotely exploitable and 99% were rated as highly or moderately severe.

Ease of Exploitation

The relative ease with which attackers can exploit a new vulnerability is a critical determinant of risk. In order to rank relative ease of exploitation, Symantec classifies all vulnerabilities according to the three categories, listed below.

1. **Exploit Available**—Indicates that sophisticated exploit code that enables the exploitation of the vulnerability is publicly available to all would-be attackers.

Figure 27.
Web Application Vulnerabilities by Month
(Jan 1, 2001 – Dec 31, 2002)



[18] Web applications are defined as any application that uses HTTP as the primary channel of input and/or output. This may include web-based email systems, web-based forums, website management tools, CGI scripts of any kind, web servers, web clients, application servers, etc.

2. **No Exploit Required**—Indicates that would-be attackers can exploit the vulnerability without having to use any form of sophisticated exploit code. In other words, the attacker does not need to create or use complex scripts or tools to exploit the vulnerability.[19]

3. **No Exploit Available**—Indicates that would-be attackers must use exploit code to make use of the vulnerability; however, no such exploit code is publicly available.

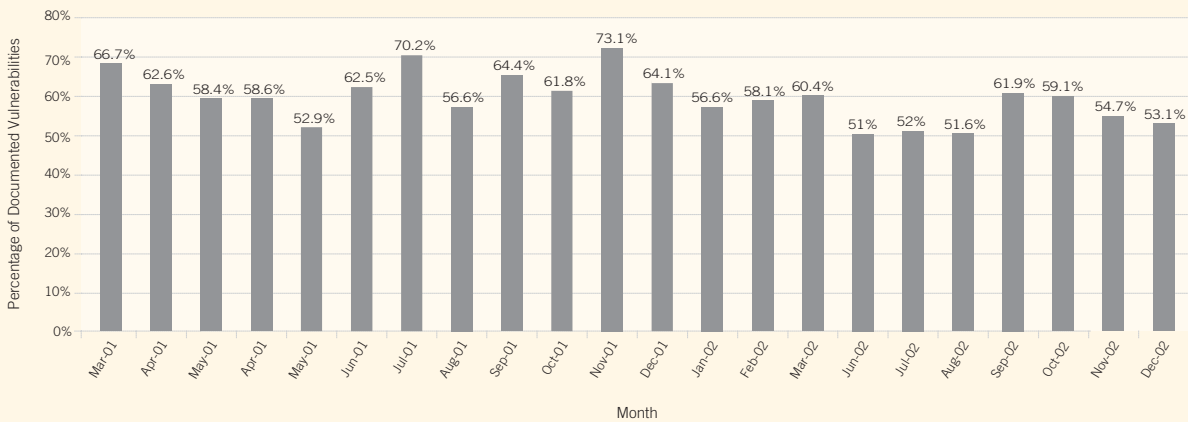
The first two types of vulnerabilities are generally considered "easily exploitable" because the attacker requires only limited sophistication to make use of them. The last type of vulnerability is considered "difficult to exploit" because the attacker must develop his/her own exploit code to make use of it.

Over the past two years the percentage of vulnerabilities classified as "easily exploitable" consistently hovered around 60%. Essentially, this statistic means that relatively unsophisticated attackers could exploit more than half of all of the vulnerabilities that emerged over the past two years either because exploit code was widely available, or because the vulnerability did not require the use of exploit code. **Figure 28** illustrates this trend.[20]

While the percentage of easily exploitable vulnerabilities on the whole was relatively consistent over the past two years, the two types of easily exploitable vulnerabilities experienced different rates of change. Specifically, the total number of vulnerabilities with no exploit available or no exploit required increased substantially. However, at the same time, the total vulnerabilities with exploits available remained relatively steady. This trend is illustrated in **Figure 29**.

As evidenced in **Figure 29**, of those vulnerabilities that required an exploit, a smaller percentage actually had an exploit available in 2002. Specifically, the percentage of new vulnerabilities with exploits declined from 30.0% in 2001 to 23.7% in 2002. This trend may be a function of several factors. First, it may reflect the recent movement by members of the information security

Figure 28.
Percent of Vulnerabilties Classified as Easily Exploitable by Month
(Mar 1, 2001 – Dec 31, 2002)



[19] For example, the Microsoft Extended Unicode Directory Traversal Vulnerability (BID #1806) is easily exploited by hand with the simple substitution of a few characters.
[20] **Figure 28** does not include data from January and February 2001 because Symantec did not begin tracking "ease of exploitation" consistently until March 2001.

community to withhold exploit code from the public. In the past, many individuals willingly posted exploit code to public forums (often just to achieve proof of concept). Recently, however, many of these same individuals have encouraged one another to embrace a greater sense of collective responsibility and to avoid publicizing exploit code. It is possible that the drop in the percentage of vulnerabilities with exploit code is evidence that this movement is truly gaining momentum.

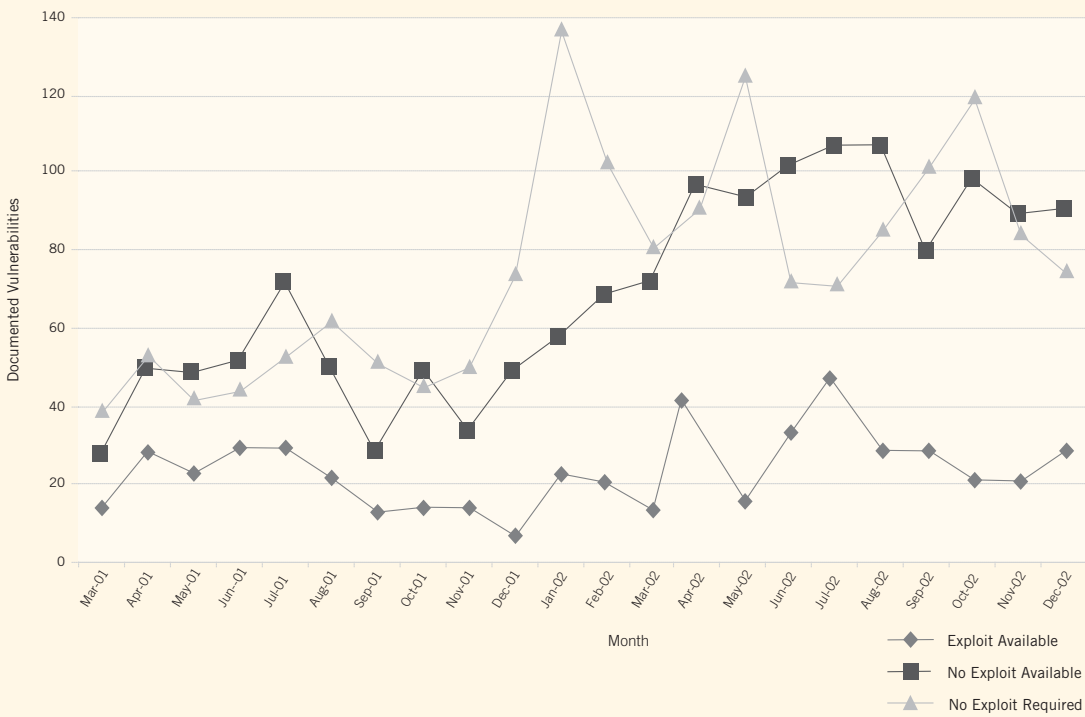
This trend can be viewed as both a positive and negative development. From a positive perspective, the decreasing availability of exploit code makes it more difficult for relatively unsophisticated attackers, such as script kiddies, to exploit new vulnerabilities. From this perspective, the overall threat to an organization declines. On the other hand, because many new exploits are not being released publicly, it is possible that some highly sophisticated attackers are developing and using exploit code without public knowledge. By keeping exploit code secret, these attackers are better able to avoid detection. From this perspective, the threat to individual organizations may actually increase.

A second factor driving this trend may simply be that sophisticated organizations and individuals (i.e., those that create exploit code for new vulnerabilities) are not keeping pace with the sheer volume of new vulnerability discoveries. As a result, the percentage of vulnerabilities with exploits is declining.[21]

FUTURE CONCERNS

In 2002, Symantec documented nearly 50 new vulnerabilities each week, a rate that was more than 80% higher than the rate recorded during the prior year. Fortunately, despite the overall rise in new vulnerability discoveries, many present a relatively low level of risk to corporations. This may be due to the fact that the vulnerability itself is not particularly severe in nature or, more likely, because the vulnerability affects a product that is rarely deployed in a corporate environment. Rather than overwhelming the reader with descriptions of the 2,000+ vulnerabilities that emerged in 2002, Symantec has isolated three types of vulnerabilities that we believe warrant more detailed discussion.

Figure 29.
Overall Volume of Vulnerability by Ease Breakout
(Mar 1, 2002 – Dec 31, 2002)



[21] This trend may also be partially a function of time required to produce an exploit. Therefore, the percentage of vulnerabilities discovered in 2002 that have exploit code publicly available may rise with time.

Blended Threat Targets

Evidence gathered from monitoring malicious code outbreaks and cyber attack activity clearly indicates that blended threats present one of the most substantial (and potentially costly) threats to the Internet community.[22] During the past two years, blended threats, such as Code Red and Nimda, infected millions of hosts and caused estimated billions of dollars in damages.[23]

The most damaging threats exploited vulnerabilities for which vendors had created patches long before the threat emerged. **Table 30** illustrates this point, by listing the vulnerabilities targeted by several major blended threats that spread over the past three years, as well as the time delay that each experienced before it was first targeted by a blended threat.

In essence, the time delay between a vulnerability discovery and its first use in a blended threat, coupled with the rising number of highly severe vulnerabilities, reinforces the need for companies to improve their security configuration and patch management practices. Known blended threats are exploiting only a fraction of the vulnerabilities that are currently documented. Symantec remains highly concerned that vulnerabilities enabling future blended threats are widely available and just waiting to be exploited. As a result, we expect that at least a few vulnerabilities that emerged over the past year will become targets of future blended threats. Also, despite the current lack of precedence, it is quite possible to consider a scenario in the near future where blended threats exploit vulnerabilities that have not been published and are completely unknown to vendors.

Figure 30.
Blended Threat Vulnerabilities and Time Delays Before First Use

Bugtraq ID	Vulnerability Name	CVE Reference Number	Relevant Blended Threats	Date of Vulnerability Discovery	Date of First Blended Threat Outbreak	Time Delay from Discovery to First Outbreak (days)
2524	Microsoft IE MIME Header Attachment Execution Vulnerability	CVE-2001-0154	1. W32.Brid 2. W32.Bugbear 3. W32.Klez 4. W32.Aliz 5.W32.Nimda 6. W32.Badtrans 7. W32.Frethem 8. W32Yaha 9. W32.Manymize 10. W32.Chir 11. W32.Holar 12. W32.Appix 13. W32.HLLW.Winevar	03/29/2001	05/22/2001	54
1754	Microsoft Virtual Machine com.ms ActiveX Component Arbitrary Program Execution Vulnerability	CVE-2000-1061	W32.HLLW.Winevar	09/05/2000	11/23/2002	809
4231	Microsoft SQL Server Multiple Extended Stored Procedure Buffer Overflow Vulnerabilities	CVE2002-0154	Digispid Worm	03/05/2002	05/21/2002	77
3597	Microsoft Internet Explorer Spoofable File Extensions Vulnerability	CAN-2001-0875	W32.Appix	12/13/2001	09/17/2002	278
5362	OpenSSL SSLv3 Session ID Buffer Overflow Vulnerability	CAN-2002-0656	Linux Slapper	07/30/2002	09/13/2002	45
2880	MS Index Server and Indexing Service ISAPI Extension Buffer Overflow Vulnerability	CVE-2001-0500	Code Red	06/18/2001	07/16/2001	28
2302	ISC Bind 8 Transaction Signatures Buffer Overflow Vulnerability	CVE-2001-0010	1. Linux Lion Worm 2. Linux.Adore Worm	01/29/2001	03/23/2001	53
2708	MS IIS/PWS Escaped Characters Decoding Command Execution Vulnerability	CVE-2001-0333	Nimda	05/15/2001	09/18/2001	126
1806	Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability	CVE-2000-0884	1. Nimda 2. Sadmind/IIS Worm	10/17/2000	09/18/2001	336
866	Solaris Sadmind Buffer Overflow Vulnerability	CVE-1999-0977	Sadmind/IIS Worm	12/14/1999	05/11/2001	514
1387	Wu-Ftpd Remote Format String Stack Overwrite Vulnerability	CVE-2000-0573	1. Linux Ramen Worm 2. Linux.Adore Worm	06/22/2000	01/17/2001	209
1480	Multiple Linux Vendor rpc.statd Remote Format String Vulnerability	CVE-2000-0666	1. Linux Ramen Worm 2. Linux.Adore Worm	07/16/2000	01/17/2001	185
1780	Microsoft Windows 9x / Me Share Level Password Bypass Vulnerability	CVE-2000-0979	W32.Opaserv	10/10/2000	09/20/2002	710
5033	Apache Chunked-Encoding Memory Corruption Vulnerability	CVE-2002-0392	FreeBSD.Scalper Worm	07/30/2002	09/13/2002	45

[22] Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By utilizing multiple methods and techniques, blended threats often spread rapidly and can cause widespread damage.
[23] According to estimates from Carlsbad, Florida-based Computer Economics, variants of Code Red alone infected several million hosts worldwide within a matter of hours, and cost organizations more than $2 billion in clean up expenses and lost productivity. Jesdenun, A. "Despite More Security Spending, Internet a More Dangerous Place." Associated Press. (January 16, 2002).

Backdoors Affecting Open Source Applications[24]

Over the past year, a single group of attackers compromised web sites hosting a wide variety of open source software packages. In many cases, the attackers proceeded to make subtle malicious changes to the posted source code of the hosted applications with the hope that they would be downloaded and used by unsuspecting users. These modifications typically opened a "back door" and communication channel to a remote host on the affected systems, which presumably enabled the attacker to gain remote control of the system via the Internet. Several popular open source software packages, including Mail Transfer Agents (MTAs), security tools, peer-to-peer applications, and IRC clients announced that backdoors were planted in their 2002 product distributions as a result of these incidents. **Table 31** lists some of the more notable applications affected by these incidents.

The most concerning fact about these incidents is not necessarily the applications affected—many are not used at the enterprise level—but rather the rapidity of the attacks and the fact that the sites affected were known to be highly conscious of security issues. These incidents should be considered a warning not only to other open source projects, but also to commercial software vendors. Rather than targeting individual systems, attackers are clearly exploring alternative ways of impacting a large number of systems in a short period of time.

Web Client Vulnerabilities

Over the past year, Symantec noticed increased effort among vulnerability researchers to identify web client vulnerabilities. As a result, Symantec has recorded a sharp increase of new web client vulnerabilities. Further, Symantec has observed that individuals are developing exploit code for web client vulnerabilities more frequently than for other applications.

Of particular concern among web client vulnerabilities were those that affected Microsoft Internet Explorer—largely because of its widespread use. Over the past year, Symantec documented 59 new Internet Explorer vulnerabilities, 31 of which are considered highly severe and at least six of which would qualify as attractive targets for future blended threats. The most concerning aspect about the Explorer vulnerabilities is that several enable attackers to completely bypass "security zones," which are a critical element protecting client systems when users browse the Internet. In effect, vulnerabilities such as the Microsoft Internet Explorer IFRAME dialogArguments Cross-Zone Access Vulnerability (BID #6205), enable attackers to run code of their choice on a user's system through acts as simple as redirecting the user to a malicious web page.[25] Attackers can leverage these vulnerabilities for a range of malicious acts, such as data theft, installation of trojans, and modification of files. Furthermore, malicious code writers can potentially use these vulnerabilities as a propagation mechanism for high impact malicious code, such as blended threats.

Figure 31.
Open Source Applications Affected by Hosting Site Attacks

Application	Type	Links to Relevant Information and Recommendations
IRSSI	Unix-based IRC Client	http://online.securityfocus.com/bid/4831
Fragroute	Network Intrusion Detection Evasion Toolkit	http://online.securityfocus.com/archive/1/274892
OpenSSH	Free version of the SSH Protocol	http://online.securityfocus.com/bid/5374
Fragrouter	Network Intrusion Detection Evasion Toolkit	http://online.securityfocus.com/bid/6022 http://online.securityfocus.com/archive/1/296407
Sendmail	email	http://online.securityfocus.com/bid/5921
LibPCap and TCPDump	Packet Sniffing	http://online.securityfocus.com/bid/6171

[24] A backdoor is a small program that is intentionally hidden inside a program/application that appears to have a legitimate function. The backdoor program permits unauthorized access to the system by a knowledgeable user.
[25] Details on Microsoft Internet Explorer IFRAME dialogArguments Cross-Zone Access Vulnerability (BID 6205) can be accessed at the following link: http://online.securityfocus.com/bid/6205

In conclusion, the rapid discovery of new web client vulnerabilities is a trend that Symantec will continue to monitor over the next year. In the meantime, the potential exposure to web client attacks and outbreaks of destructive forms of malicious code appears to have increased substantially in recent months. This is particularly concerning at the enterprise level, as companies deploy web clients on virtually all client systems and rarely encourage or require frequent updates by employees.

SQL Database Vulnerabilities

Vulnerabilities that affect relational databases are another class of threats that experienced substantial growth over the past year. Many of these vulnerabilities were highly severe in nature because they enable attackers to gain complete control of a database. This year, Symantec documented over 65 vulnerabilities affecting database products from Microsoft, Oracle and IBM. Microsoft issued 11 security bulletins for SQL Server 2000 and 7.0 in 2002, while Oracle published 20 security alerts.

Compounding this threat is the growing insecurity of web-based applications, which often utilize databases as their back-end. For example, numerous well-known e-commerce applications and web sites employ this type of architecture. In sum, the combined increase of database and web application vulnerabilities has made mission-critical databases more vulnerable than ever to remote attackers. This greatly increases risk for the many companies that maintain remote access to sensitive client and corporate data.

EMERGENCE OF MALICIOUS CODE

OVERVIEW

Methodologically, there are few credible analytical techniques that researchers can use to predict future malicious code activity. It is well known (particularly among members of the anti-virus community) that entirely new types of threats often emerge without any warning signs. Often these are the types of threats that spread the most rapidly because many (if not all) targeted systems lack the required defenses. Recognizing the inherent limitations of relying solely on past activity, this section of the Internet Security Threat Report points out key areas of concern in which we reasonably expect future malicious code and activity. These observations draw heavily from the analysis of:

- Existing systems and applications
- Emerging systems and applications under development
- Intelligence gathering and adversary profiling
- Behavioral analysis

Reliance on this type of analysis yields a more comprehensive picture of the current and future threat environment. With this understood, the remainder of this section outlines several current trends that are affecting organizations, as well as three future concerns.[26]

CURRENT TRENDS

Several of the following trends and analysis are based on malicious code submissions to Symantec AntiVirus Research Automation (SARA) system. For a more detailed description of this system, see **page 46** in **Appendix B**.

Blended Threats

Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with host and Internet vulnerabilities to initiate, transmit, and spread. By utilizing multiple methods and techniques for propagation, blended threats often spread rapidly and cause widespread damage. Examples of blended threats include, but are not limited to: Code Red, Nimda, and Bugbear.

In terms of damage potential, the multiple propagation mechanisms of blended threats enable them to compromise a company's security posture, and also frequently eat up system resources and network bandwidth. Unfortunately, following good

[26] Additional details on all worms cited in this section can be obtained at http://securityresponse.symantec.com.

security practices such as requiring strong, non-default passwords, is often not enough to prevent this type of attack. Blended threats exploit IT product vulnerabilities, and so long as systems maintain a vulnerability targeted by a specific blended threat, infection is possible. While not guaranteed effective, maintaining good security and patch management practices seems to be among the best defense mechanisms against this type of threat.

During the past six months, three blended threats—Klez, Opaserv, and Bugbear—accounted for nearly 80% of all malicious code submissions. Additionally blended threat submissions were approximately twice as high as in the same six-month period of 2001. Finally, the Internet community also witnessed the emergence of two new blended threats of note, Bugbear and Opaserv. Although neither caused a volume of damage that was comparable with that caused by the 2001 outbreaks of Code Red and Nimda, widespread propagation of these threats (as evidenced by their inclusion in the list of Top Five Submissions), is a sobering reminder that blended threats continue to present a substantial risk.

Finally, a review of the major blended threats that emerged over the past several years revealed that all of these threats targeted known vulnerabilities, some of which were well documented for more than six months before the blended threat was created. If future blended threats reasonably follow a similar pattern, there already are numerous known vulnerabilities that are perfectly viable candidates for the next major blended threat.

In conclusion, despite the fact that the damage potential of the most recent blended threats was considerably less that that of past threats such as Nimda, Symantec still expects that the relative risk presented by these threats will rise over the next year. Of particular concern is the seemingly endless supply of known vulnerabilities that malicious code writers can readily exploit. On a positive note, organizations can take several steps to improve their defenses against future blended threats.[27]

Figure 32.
Top Five Malicious Code Submissions by Percentage of Overall Submissions
(October 1, 2001 – Dec 31, 2002)

Rank	Occurrence	Threat
1	47.6%	W32.Klez.h@mm
2	21.8%	W32.Bugbear@mm
3	7.5%	W32.Opaserv.Worm
4	7.2%	JS.Exception.Exploit
5	3%	W95.Hybris.Worm

Windows 32 Viruses/Worms

Over the past year, 1,200 new 32-bit Windows viruses and worms were released, a substantial rise from the prior year. Maintaining this trend, malicious code submissions during the fourth quarter of 2002 consisted predominantly of Windows 32 threats, as opposed to script- or macro-based threats. Furthermore, three of the Top Five virus/worm threats reported by Symantec Security Response during the fourth quarter were classified as Win32. **Table 32** shows the top five malicious code submissions during the fourth quarter.

Fortunately, even with the complexity of Win32 threats, and the volume of data they tend to generate, most market-leading anti-virus products have robust Win32 detection. Provided that anti-virus products are implemented correctly and well maintained on all platforms and across all tiers of a corporate network, proactive companies should be well protected from the majority of Win32s.

Linux Threats

One trend that remains somewhat subtle is the recent increase in malicious code targeting Linux systems. In 1998 we saw the first widespread example of a successful Linux threat, the Linux.ADM.Worm. In addition to its worm-like characteristics, it also exploited a widely known vulnerability, causing the compromise of a large number of systems. Until recently, however, there were relatively few successful malicious code outbreaks on Linux.

In September 2002 this trend shifted when the Linux.Slapper worm emerged and caused significant outbreaks on Linux systems. The infection vector of the worm and its variants is based on a

[27] To assist, Symantec has outlined a comprehensive set of tactical recommendations, which can be obtained by downloading the white paper at the following link. http://securityresponse.symantec.com/avcenter/reference/blended.pdf.

remote buffer overflow vulnerability in the OpenSSL implementation of the SSL protocol targeting Apache web servers on various versions of the Linux operating environment. In addition to Slapper, a number of highly sophisticated zoo-based Linux viruses and worms emerged in recent months.[28] Many of these threats were concerning because they demonstrated that malicious code writers are developing a higher level of sophistication in programming and increased familiarity with the Linux operating system and its applications. The evolution of the Linux threat landscape will be observed with great interest during the next twelve months. This threat is especially concerning as Linux-based solutions are brought to the consumer market.[29] As opposed to individuals already familiar with various flavors of the Unix operating systems, home users are likely unaware of appropriate security practices.

Self-Replicating Mass Mailers

Another trend that has escalated over the past six months is the increase in mass-mailing worms that propagate by using their own SMTP engine.[30] Most old forms of email threats used email clients such as Microsoft Outlook to propagate. However, many of the more recent mass-mailer worms follow the following sequence. First, they exploit known vulnerabilities to infect a system. Next, they harvest email addresses from the infected system. Finally, they propagate by using an email engine that is independent of the client email. In effect, this methodology enables the code to propagate without requiring user interaction.

As a result, users are often unaware of the e-mails generated from their infected systems. Furthermore, because these threats spoof the "From" address on e-mails, victims of the infection are often unable to determine the true origin of the threat. This makes tracking down sources of infection extremely difficult.

During the past six months, eight of the top 50 malicious code submissions carried their own SMTP engines. This is a stark contrast to the same time period in 2001, when only 1 of the top 50 malicious code submissions had its own SMTP engine. In response to the increasing presence of mass mailers with SMTP engines, several market-leading anti-virus products have created new types of technology that detect and eliminate this type of threat more effectively.

Use of Network Shares as Infection Vector

Over the past six months, Symantec noted a rise in malicious code that spread via network shares. The W32.Opaserv worm variants, which spread rapidly in the wild during the last few weeks of September 2002, were excellent examples of this type of worm. Unlike Klez and Bugbear, Opaserv infected vulnerable Windows 9x systems over Windows shares even if the password was set for the share. Previously, the W32.Funlove virus used a similar infection vector; however, Funlove did not use a vulnerability exploit, and thus the attack of the worm could be stopped with passwords alone.

Carrier Viruses and Worms

Over the past year, Symantec noted an increase of carrier viruses and worms, which are forms of malicious code that enable other forms of malicious code to propagate in addition to itself. An example

[28] Zoo-based threats are those that exist only in virus and anti-virus labs, not in the wild. Most zoo threats never get released into the wild, and as a result, rarely threaten users.
[29] In 2001, according to IDC, the Linux Client Operating Environment (COE) grew at a 49% rate, especially in the emerging Asia/Pacific market. Latin America has also shown strong growth. As Linux becomes more of a "packaged" offering with equivalent component offerings to Windows and major Unix variants, this trend is forecasted to continue. "Worldwide Linux Operating Environments Forecast and Analysis, 2002-2006: A Market in Transition." IDC. July 2002. <http://www.idc.com>.
[30] Malicious code that has its own SMTP engine is able to spread without using an existing email application. For example, after infecting a personal computer with Microsoft Outlook, this type of malicious code can propagate via email without using the Outlook application.

is the Opaserv worm, which replicates by creating e-mails from bits of files/e-mails from the infected system. If one or more of the files selected by Opaserv happens to be infected with other viruses, these viruses are also transmitted with the Opaserv infected file. As a result of the rise of new carrier viruses and worms, Symantec has seen relatively old viruses re-emerge in the wild. In the case of Opaserv, for example, Symantec saw a re-emergence of infections by older viruses, such as W95.Spaces and W32.Funlove.

The recent increase of carrier viruses and worms is concerning because they can cause old threats to re-emerge with much higher impact. Many past forms of malicious code that had the potential for high impact failed to spread widely. However, when they are "carried" by malicious code that is capable of wide scale propagation, suddenly they can spread much more effectively and cause a considerable amount of damage. Fortunately, while the use of carrier viruses occasionally breathes new life into old threats, users can usually defend adequately against these threats simply by keeping anti-virus products up to date with the latest signatures.

Theft of Confidential Data

Over the past year, Symantec noted a rise in malicious code that steals confidential data from users. For example, there was a sharp increase in malicious code that extracts “To” and “From” names from a user’s address book, thereby enabling misuse and further theft of data by the creator. While older viruses, such as W32/Sircam.@mm, compromised confidentiality by exporting random documents, more recent viruses and blended threats not only export confidential documents, but also export system data that can be used to inflict further damage. For example, blended threats, such as Bugbear export confidential data including lists of file names, lists of processes, user names, processor type, OS version, memory information, local drives, and network resource and type. Additionally, Bugbear can deliver logged keystrokes to a third party, which may yield important information such as passwords and other details.

The implications of this trend are inherently difficult to quantify. In order to better understand the impact within their organization, companies should pay closer attention to whether or not confidential data has been compromised when investigating major malicious code incidents. In addition, users need to be aware of their browser privacy policies and protection mechanisms to minimize the ability of malicious code to export confidential data.

FUTURE CONCERNS

The variety of threat types that facilitate compromises of data/system availability, confidentiality, and integrity is clearly increasing. While historical data analysis indicates that Windows 32 threats, blended threats, and self-replicating mass-mailers are all on the rise, there are several risks based on market analysis that also warrant close attention. The remainder of this section outlines several threats that Symantec views as high risks in the future.

Instant Messaging

According to Gartner Research, by the fourth Quarter of 2002 approximately 70% of enterprises used unmanaged consumer instant messaging on their networks to conduct business.[31] In addition, Symantec Managed Security Services noted a similar rise in usage of instant messaging applications among clients, many of whom maintain strict policies forbidding such action.

As both legitimate and unauthorized usage rises, the threat of malicious code that uses instant messaging clients for propagation is becoming more significant. While this threat is not entirely new—a few viruses that use AIM, ICQ, Yahoo and MSN exist today—the market penetration of instant messaging usage is now sufficient to make viable the use of Instant Messenger as a primary and efficient infection vector for malicious code that has a much more devastating impact.[32]

[31] Grey, M. “Instant Messaging in the Enterprise Will Remain a Puzzle.” COM-18-7979. 22 Nov. 2002. Gartner Research. <http://www.garner.com>.
[32] Fortunately, there are many steps that organizations can take to better protect against this threat. For a more complete description of the security risks of using instant messaging and guidelines for securing this application a white paper is available at: http://securityresponse.symantec.com/avcenter/reference/secure.instant.messaging.pdf

Peer-to-Peer Applications

In 1999, Napster emerged as the first widely used peer-to-peer (P2P) application designed to allow widespread sharing of files over the Internet. Since the creation of Napster, the use of new P2P applications, such as LimeWire, Morpheus, and various versions of KaZaA, has increased dramatically. Symantec analysts have also noted a disturbing rise in unauthorized usage of P2P applications among company employees despite security polices that strictly forbid this practice. Finally, compounding this trend, several recent worms began using P2P file-sharing networks as a primary infection vector in 2002.

The combination of wide deployment and increasing usage, coupled with the fact that most of the current P2P networking applications actually circumvent enterprise security policy by bypassing controls such as firewalls, makes these applications a highly attractive target for future cyber attackers and malicious code writers. Symantec strongly encourages organizations to prohibit P2P use among employees or establish clear and enforceable usage restrictions if business need dictates that P2P usage is required.

Mobile Devices

Another area that should be watched with care is the mobile device arena. Gartner Research predicts that 2004 will be the major breakthrough year for the mobile email/personal information manager (PIM) market globally.[32] The "always on" nature of the connectivity, remote access to critical sensitive data, and the increasingly computational nature of these devices, sets the stage for a potential virus or worm of significance.

[32] Dulaney, K. Clark, B.. "E-Mail/PIM Is Still No. 1." SPA-18-5839. 20 Nov. 2002.Gartner Research. <http://www.gartner.com>.

Appendix A—Network-Based Cyber Attack Methodology

OVERVIEW

Appendix A outlines key components of the methodology that Symantec used to measure and report trends in cyber attack activity. The data and insights are derived from a subset of companies that subscribe to Symantec Managed Security Services (MSS) and, in some cases, the Symantec DeepSight Threat Management System (TMS). The subset studied for this report includes a majority of Symantec Managed Security Service customers with the exception of statistical outliers, which were removed from this analysis. The appendix is divided into the following sections:

- Company Demographics
- Attack Metrics
- Individual Research Inquiries

COMPANY DEMOGRAPHICS

The sample set from which the cyber attack trends in this report were derived consists of a subset of more than 400 companies, located in more than 30 countries throughout the world. Combined, the security infrastructure at these companies protects millions of Internet-connected hosts. In terms of diversity, the sample set includes a broad array of organizations as measured by criteria such as industry, ownership type, company size, and length of time as security monitoring clients. A subset of company characteristics is outlined in greater detail below.

Industry

Figure 33 presents the industry break down of the sample set in percentage terms. Industry groups are based on the review of a variety of public and private references, as well as direct client interactions. It is important to note that several classifications were altered since the July 2002 issue of the Report. These changes were necessary to create a new, standardized classification methodology that is now employed by both the Symantec Managed Security Services and Threat Management Services.

Company Size

Employee count was used as a proxy to measure company size. This metric was selected as the best proxy for company size because the number of employees typically correlates best to the relative size of a company's network. Employee counts were gathered from public sources, as well as engaging in direct, client interactions. **Figure 34** indicates the break down by company size for the sample set.

Figure 33.
Breakdown of Companies by Industry
(July 1, 2002 – Dec 31, 2002)

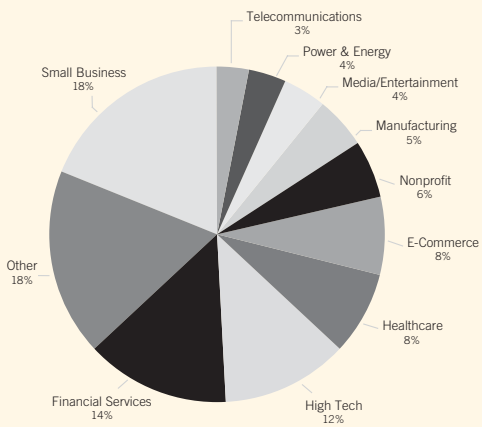
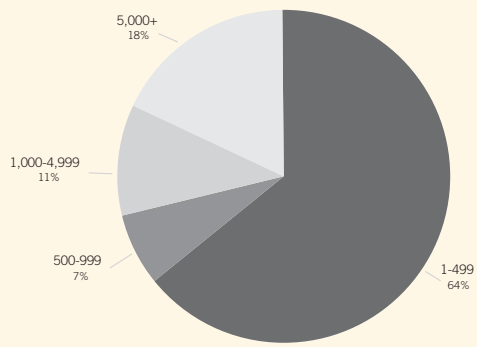


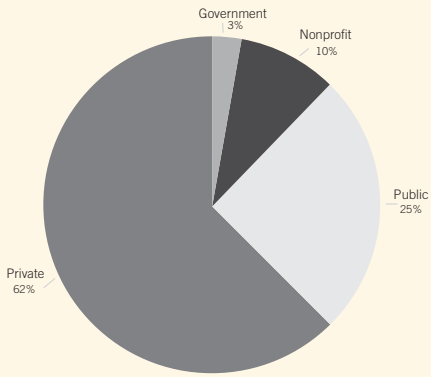
Figure 34.
Breakdown of Companies by Employee Count
(July 1, 2002 – Dec 31, 2002)



Company Ownership Status

Company ownership status was gathered mainly from public sources, as well as engaging in direct, client interactions. **Figure 35** indicates the breakdown by company ownership status for the sample set.

Figure 35.
Breakdown of Companies by Ownership Status
(July 1, 2002 – Dec 31, 2002)



ATTACK METRICS

Overview

Several reports analyzing cyber attack activity are currently circulating the information security community, and each report claims to offer the most accurate depiction of key trends. Unfortunately, benchmarking findings among studies is difficult (if not impossible) because each report attempts to capture "attack activity" in a different way. For example, the *CERT Annual Report* relies on "security breaches' that were detected and voluntarily reported to CERT by corporations and individuals. The annual *CSI/FBI Computer Crime and Security Survey* also captures trends in attack activity by measuring "security breaches" that were detected and reported by survey respondents. In order to avoid ambiguity with our findings, Symantec's methodology for identifying various forms of "attack activity" is outlined clearly on the following pages and applied consistently throughout our monitoring and analysis.

Attack Definitions

The first step in analyzing cyber attack activity is to define precisely what is an "attack." Rather than limiting our analysis to only one metric of attack activity, Symantec uses several different metrics, each of which is uniquely appropriate under a certain set of circumstances. Presented below is a high-level summary of the four metrics that are commonly used in the Report.

- **Attacks**—Attacks are individual signs of malicious activity that are isolated by the Symantec Secure Operations Center technology platform and validated by Symantec analysts. Attacks can consist of one or more IDS alerts and/or firewall logs that are indicative of a single type of attacker action. For example, multiple firewall logs often indicate the occurrence of a single network scan. Attacks do not include false positive indicators of attack activity, as technology and expert human analysts exclude this type of activity from the data set.
- **Events**—Security events are logical groupings of multiple attacks. A security event may include a group of similar, but non-threatening, signs of attack activity experienced by companies during the course of a day (e.g., all non-threatening HTTP scans experienced during a single day are grouped into an event); or a security event may include multiple attacks against a single company by a single attacker during a specified period of time.
- **Unique Attackers**—The Unique Attacker metric is the most reliable indicator of the actual number of attackers detected by the sample set. The metric captures the total number of unique source IP addresses that launched attacks against companies over a set time (e.g., day, week, month, etc.).

- **Attacks per Company**—The attacks per company metric captures the average volume of attacks that companies experience over time. Symantec generates these statistics by taking the average attacks per company each day, and then averaging the sum of these averages over specified periods of time. By calculating the average number of attacks per company in the sample sets each day, Symantec accounts for clients that were added to the sample set throughout the study period, thereby ensuring that these additions do not falsely inflate the apparent volume of activity.

Because "attacks" and "events" involve the use of complex technology and extensive validation, these two metrics are outlined in greater detail throughout the remainder of this appendix.

Attack and Event Data

Identification and Classification Process

One of the most valuable attributes of the findings in this report is the fact that each possible sign of attack activity is evaluated by Symantec analysts to validate whether it truly represents malicious activity. Identification and classification of attacks and events is the end result of a sophisticated process that involves the use of complex technology and expert human analysis. During this process Symantec analyzes every firewall log and IDS alert generated by client devices and isolates and investigates entire attack sequences in real time. The combination of sophisticated technology and expert human analysis ensures that the identification and classification process is comprehensive and consistent over time. **Figure 36** outlines the key steps of the attack and event identification and classification process.

Figure 36.
Attack Identification and Classification Process for Companies in the Sample Set

Stage of Analysis	Description
Stage #1—Collection and Normalization of Security Data from Clients' Firewalls and IDSs	Security data is imported from firewalls and/or IDSs, normalized into a standard format, and stored in a dedicated database.
Stage #2—Data Mining of Normalized Security Data	Security data is continuously mined by the Secure Operations Center Technology Platform to isolate occurrences and/or patterns of potentially malicious activity. Once identified, such patterns or occurrences of malicious activity are stored as attacks in a separate table within the database.
Stage #3—Security Event Correlation and Presentation	Attacks generated during the data mining stage are linked by logical criteria, such as attack type, attack direction, and source IP. For example, a correlated security event may present all signs of attacks detected from a single IP address in China. Security events are then posted to a graphical user interface (GUI) in the Symantec Secure Operations Center, and security analysts review and investigate each event to determine the type and severity of the event.
Stage #4—Event Classification	After completing an investigation of the possible event, those that are determined to be "false positive" are eliminated from consideration.* Based upon the apparent intent and sophistication of the activity, attacks are validated and assigned a severity level. Only events that are judged to be valid occurrences of malicious activity are analyzed in this report. Each action contributing to an event is considered an "attack," while the sequence of attacks in its entirety is considered an "event."

* False positive attacks represent attacks that were initially flagged as potentially malicious, but later determined to be benign after evaluation by a Symantec security analyst.

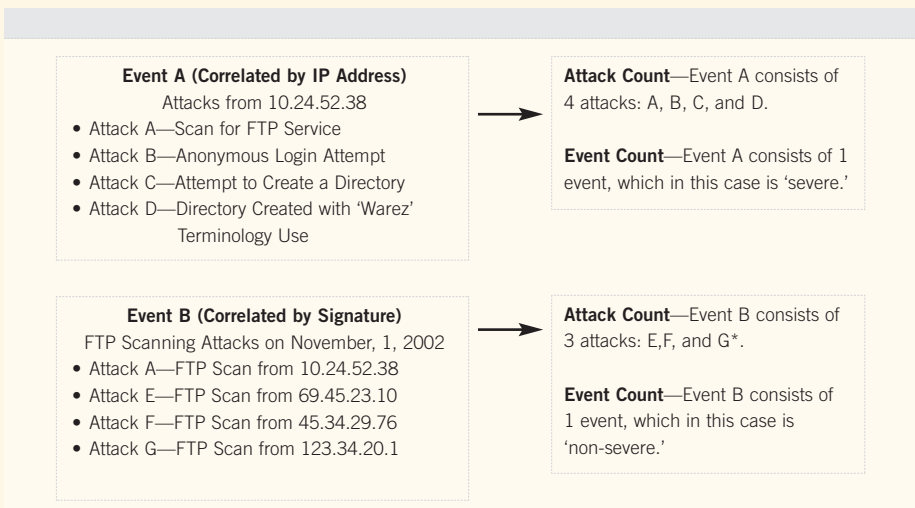
DISTINCTION BETWEEN ATTACKS AND EVENTS

The best way to view the attack and event metrics used in this report is as follows: **Attacks** represent each individual action taken by attackers; and **Events** represent logical groupings of attack activity that are either similar in nature or are taken by a single attacker within a continuous time sequence. To provide greater clarity, each metric is summarized graphically in **Figure 37**.

Symantec uses both "attacks" and "events" to evaluate malicious activity because reliance on a single metric in all situations inevitably generates inaccuracies. For example, suppose Symantec only used the "attack" metric to measure the frequency of "severe" activity. This approach would lead to inaccuracies because severe activity is really a function of attack sequences (or events), not individual signs of attack activity. In fact, analysts have analyzed several severe events that consist of hundreds of individual attacks, each of which in isolation may not indicate a severe threat. It would be misleading, therefore, to count this series of related activity as hundreds of individual severe attacks. Therefore, in this case, evaluating "events" rather than "attacks" yields a more accurate measure of severe activity.

On the other hand, when looking at total attack activity over time, the amount of distinct attacker actions would be grossly underestimated if we were to base the analysis solely on events. This is because "events" may consist of hundreds (or even thousands) of individual attacker actions. For example, clients often experience hundreds of non-threatening scans caused by blended threats on a daily basis; however, rather than overwhelming clients by reporting each individual scan, Symantec aggregates this activity into a single event that is reported to clients once per day. While this is the most practical reporting strategy for clients, it inherently underestimates the amount of attack activity that companies are experiencing. If Symantec were to use the number of "events" reported to clients over time, scanning activity (which is a valid indicator of malicious activity) would be grossly underestimated.

Figure 37.
Symantec Security Events versus Attacks



* To avoid double counting, the scan from 10.24.52.38 is not counted as an attack because it is already counted as an attack within Event A.

INDIVIDUAL RESEARCH INQUIRIES

The following section outlines several specific inquiries discussed in the cyber attack activity section of the report.

Event Severity

Every event validated by a Symantec security analyst is assigned to one of four severity classifications: informational, warning, critical, and emergency. The primary purpose of this rating system is to prioritize client responses to malicious activity based on the relative level of danger that the event presents to their environment. A determination of severity is based on characteristics of an attack, defensive posture of the client, value of the assets at risk, and the relative success of the attack.

For the Internet Security Threat Report, these four severity levels are further grouped into two classifications: severe and non-severe events. Severe events include activity classified as either "emergency" or "critical", while non-severe events include activity classified as either "informational" or "warning." In simple terms, a severe event demands IMMEDIATE countermeasures from an organization, while a non-severe event is mainly informative. The severity classification system is explained in greater detail in **Figure 38**.

Attacks by Time of Day

Each attack detected by Symantec has a corresponding time stamp (expressed in Greenwich Mean Time), which describes the precise time that the attack was detected. This time is extracted from the log data (i.e., firewall or IDS) produced by the device that Symantec is monitoring. However, in order to evaluate when attackers are most active within specific locations throughout the world, Symantec normalized these time stamps to the local time in which the attacking system was located. For example, suppose Symantec detects an attacker at 12:00 GMT, and the attacking system was located in New York City; the local time of the attacker in this example is 7:00 (GMT –5).

Figure 38.
Event Severity Metrics

Severity Classification	Severity Level	Description
Non-Severe	Informational	These events consist of scans for malicious services and IDS events that do not have a significant impact on the client's network. **Example:** • Scans for vulnerable services where all connection attempts are dropped by the firewall.
	Warning	These events consist of malicious attacks that were successful in bypassing the firewall, but did not compromise the intended target systems. **Example:** • Scans/horizontal sweeps where some connections were allowed, but a compromise has not occurred.
Severe	Critical	These events are malicious in nature and require action on the part of Symantec or the client to remedy a weakness or actual exploit of the client network or devices. By definition, if a critical event is not addressed with countermeasures, it may result in a successful compromise of a system. **Examples:** • Continuous attacks by a single IP address against the client network. • A significant vulnerability on the client's network that was identified by either an attacker or the Security Operations Center (SOC). For example, a web exploit is observed and appears to be successful, but there is no observed follow-up activity to take advantage of the vulnerability. • Unknown suspicious traffic that warrants an investigation by the client to track or eliminate the traffic flow.
	Emergency	These events indicate that a security breach has occurred on the client's protected network. An emergency event requires the client to initiate some form of recovery procedure. **Examples:** • Successful exploit of a vulnerable web server.

In order to produce **Figure 38** on **page 43**, which illustrates the rate of all attackers normalized to the local time within 7 regions, Symantec used the following local times.

Region	Local Time
Africa	GMT +2
Asia	GMT +7
Eastern Europe	GMT +2
Middle East	GMT +3
North America	GMT -6
Oceania[34]	GMT +11
South America	GMT -3
Western Europe	GMT +1

These local times were selected because they represented a logical average point for regions that extend across several time zones. However, it is important to understand that this limitation makes these statistics a rough visualization of attack activity by region.

Attack Source

Symantec identified the national and regional source of attacks by automatically cross-referencing source IP addresses of every attack with several third-party, subscription-based databases that link the geographic location of hosts to source IP addresses. While these databases are generally reliable, there is a small margin of error. Currently, Symantec cross references source IP addresses of attacks against every country in the world and also analyzes attack trends according to the following regions:

- Africa
- Asia
- Caribbean
- Eastern Europe
- Latin America
- Middle East
- North America
- Oceania
- South America
- Western Europe

It is important to note that while Symantec has a reliable process for identifying the source IP of the host and/or network block that is directly responsible for launching an attack, it is impossible to verify whether the attacker is actually physically present at this location. It is probable that many apparent sources of attacks are, in fact, systems that were used by attackers as a platform to disguise his/her identity and true location.

Attacker Intent

In order to determine a general sense of attacker objectives, Symantec looked at a sample of more than 100 Managed Security Services clients who share a common Class B network block. Symantec then examined all attacks launched against these companies, and determined the percentage that suffered targeted and opportunistic attacks. **Figure 39** outlines how each type of attack was categorized.

Top Network Scans

When evaluating attacks, Secure Operations Center analysts separate activity into several different categories. At the highest level, attacks are separated into “reconnaissance” and “exploits.” As the terms suggest, reconnaissance is an indicator of the types of systems and/or services that attackers seek for attempted compromise, while exploits indicate the actual actions that attackers undertake to compromise a system that they identify as potentially vulnerable. The listing of the top network scans is an indicator of reconnaissance activity. The metric reveals the types of services for which attackers most frequently search for exploitation.

Attacker Platform

Symantec employs an automated system that profiles a subset of attackers immediately after they attack one or more clients. The profiler gathers public data, such as the attacker’s operating system and services available on the attacker’s system. Combined with other metrics of attack activity, the profiler provides deeper insight into attackers’ modus operandi. It is important to note, however, that many of the systems identified as “attackers,” may actually be systems that were themselves compromised and then used as a launching point by attackers located elsewhere.

Cyber Terrorism Watch List

In response to warnings issued by the United States Department of Homeland Security indicating that terrorists may be exploring the use of cyber-

[34] Oceania was not included in the figures summarizing this analysis because this region contributed less than 1% of overall attack activity and was the only region that did not show a recognizable pattern of peak activity by hour of day.

terrorism, Symantec created the Cyber-Terrorism Watch List. The Watch List tracks cyber attack activity from two types of countries: those designated by the U.S. State Department as State Sponsors of Terrorism and those from which terrorists have reportedly operated and recruited in the past. Countries selected for the latter category were based on a review of a variety of public sources that indicate possible "hot spots" of terrorist activity.

It is important to note that, while Symantec does not claim to have specific expertise in terrorism, we believe this list presents an adequate starting point for tracking potential cases of cyber terrorism by monitoring some of the more likely sources. Countries included on the Cyber-Terrorism Watch List are listed in **Figure 40**.

Figure 39.
Definitions of Attacker Intent

Objective	Description
Opportunistic	Opportunistic attacks appear to be intent on locating any vulnerable system that exists on the Internet regardless of who owns the system or the specific function of the system. In this situation the victim of the attack was not identified in advance, but rather was selected after being identified as a vulnerable system. Typically, these attacks are preceded by a scan of many systems on the Internet until the attacker pinpoints a system that has vulnerabilities that he/she knows how to compromise.
Targeted	Targeted attacks appear to be directed at a specific organization. In theory, attackers who launch these types of attacks have identified the target company in advance and have made a conscious and deliberate attempt to gain access to their network. In this situation, the attacker is not looking for a specific vulnerability to gain access to ANY organization, but rather is looking for ANY vulnerability that will enable them to gain access to a specific system. For this report, these include all attacks in which the attacker did not perform any scan on any other networks within the network block of the sample set. In this situation, the attacker has only shown signs of malicious activity against one client.*

* It is possible that some attacks that appear targeted are actually opportunistic in nature. This is due to the fact that some attackers may use tools that randomly select a target without systematically scanning an entire network block for vulnerable systems.

Figure 40.
Countries Currently on the Cyber-Terrorist Watch List
(July 1, 2002 - December 31, 2002)

U.S. State Department Designated State Sponsors of Terrorism	Countries with Reported Terrorist Activity
Cuba	Afghanistan
Iran	Egypt
Iraq	Indonesia
Libya	Jordan
North Korea	Kuwait
Sudan	Lebanon
Syria	Morocco
	Pakistan
	Saudi Arabia
	United Arab Emirates

Appendix B—Malicious Code Methodology

Observations in this section were based, in part, on empirical data and expert analysis. The data and analysis draw primarily from two databases, described below.

INFECTION DATABASE

As part of its continuing effort to detect and eradicate computer viruses, Symantec developed the Symantec AntiVirus Research Automation (SARA) technology. Symantec uses this technology to analyze, replicate, and define a large subset of the most common computer viruses that are quarantined by Symantec AntiVirus customers. In an average month SARA receives hundreds of thousands of suspect files daily from both enterprise and individual consumers located throughout the world. These suspect files are then analyzed by Symantec and matched with virus definitions. An analysis of this aggregate data set provides Symantec with statistics on infection rates for different types of malicious code.

MALICIOUS CODE DATABASE

In addition to infection data, Symantec Security Response analyzes and documents attributes for each new form of malicious code that emerges both in the wild and in a zoo environment. Descriptive records of new forms of malicious code are then entered into a database for future reference. For this report, historical trend analysis was performed on this database to reveal trends, such as the use of different infection vectors and the frequency of various types of payloads.

Appendix C—Vulnerability Methodology

OVERVIEW

Symantec Threat Analysts search hundreds of security vendor, industry, and underground web sites and mailing lists, looking for information about possible new security vulnerabilities. Following the discovery of a new vulnerability, threat analysts gather all information related to the new vulnerability and create an alert. Within the alert are numerous fields that describe characteristics of the vulnerability, such as severity, ease of exploitation, and products affected. To date, Symantec's Security Response Service maintains a database that contains detailed reports describing more than 6,000 distinct vulnerabilities, and is generally considered to be the largest and most accurate such database.

VULNERABILITY CLASSIFICATIONS

The remainder of this appendix outlines several of the classifications that Symantec uses when documenting new vulnerability discoveries. The majority of these classifications are used either directly or indirectly for various research inquiries in the current issue of the Report.

Vulnerability Type

After discovering a new vulnerability, Threat Analysts classify the vulnerability into one of 12 possible categories. The classification system is based on Taimur Aslam's white paper, entitled "A Taxonomy of Security Faults in the Unix Operating System," which defines the taxonomy used to classify vulnerabilities.[35] Possible values are indicated below, and the previously mentioned white paper provides a full description of the meaning behind each classification.

- Boundary Condition Error
- Access Validation Error
- Origin Validation Error
- Input Validation Error
- Failure to Handle Exceptional Conditions
- Race Condition Error
- Serialization Error
- Atomicity Error
- Environment Error
- Configuration Error
- Design Error

[35] Aslam, T. "A Taxonomy of Security Faults in the Unix Operating System."Purdue University. (1995).

Severity

Symantec analysts calculate a severity score on a scale of 1 to 10 for each new vulnerability discovery. The severity score is based on the following factors:

- **Impact**—This measures the relative impact on the affected systems if the vulnerability is exploited. For example, if the vulnerability enables the attacker to gain full, root access to the system, the vulnerability is classified as "high impact." Vulnerabilities with a higher impact rating contribute to a higher severity score.
- **Remote Exploitability**—This measure indicates whether or not the vulnerability can be exploited remotely. Remotely exploitable vulnerabilities occur when it is possible using at least one method to exploit the vulnerability from a host, distinct from the vulnerable system, via some type of communication protocol, such as TCP/IP, IPX, or dial-up. Vulnerabilities that are remotely exploitable contribute to a higher severity score.
- **Ease of Exploitation**—This measures the relative ease with which vulnerabilities can be exploited. Vulnerabilities for which an exploit is widely available or for which an exploit is not required, contribute to a higher severity score. This metric is described in greater detail later in this section.
- **Authentication Requirements**—This metric indicates whether the vulnerability can be exploited only after providing some sort of credentials to the vulnerable system, or whether it is possible to exploit it without supplying any authentication credentials. Vulnerabilities that require no authentication on the part of the attacker contribute to a higher severity score.

After gathering information on these four attributes, analysts use a pre-established algorithm to generate a severity score that ranges from 1 to 10. For the purposes of this report, vulnerabilities are rated as high, moderate, or low severity based on the following scores.

Severity Level	Severity Score Range
High	$X \geq 7$
Moderate	$4 \leq X < 7$
Low	$X < 4$

Ease of Exploitation

The ease of exploitation metric indicates how easily vulnerabilities can be exploited. The vulnerability analyst assigns the ease rating after thoroughly researching the need for and availability of exploits for the vulnerability. All vulnerabilities are classified into one of three possible categories, listed below.

- **Exploit Available**—Indicates that sophisticated exploit code that enables the exploitation of the vulnerability is publicly available to all would-be attackers.
- **No Exploit Required**—Indicates that would-be attackers can exploit the vulnerability without having to use any form of sophisticated exploit code. In other words, the attacker does not need to create or use complex scripts or tools to exploit the vulnerability.
- **No Exploit Available**—Indicates that would-be attackers must use exploit code to make use of the vulnerability; however, no such exploit code is publicly available.

In this report, the first two types of vulnerabilities are considered "easily exploitable" because the attacker requires only limited sophistication to make use of it. The last type of vulnerability is considered "difficult to exploit" because the attacker must develop his/her own exploit code to make use of the vulnerability.

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product Information

In the U.S., call toll-free
800-456-9949.

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.

P/N. 10059685