



# Internet Risk Impact Summary

for September 28 – December 31, 2002

## Executive Summary

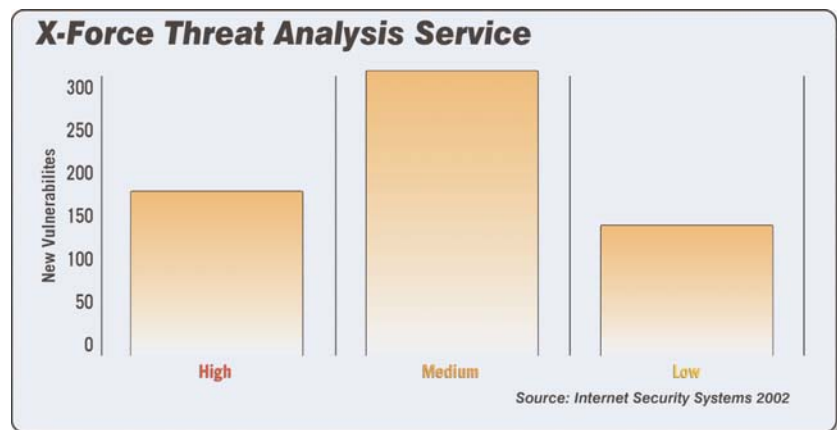
Hybrid threats created a significant increase in Internet risk throughout the first three quarters of 2002. This upward trend continued throughout the fourth quarter as well. The Klez, Slapper (OpenSSL), Nimda, Spida (SQL) worms and their variants continue to reflect a persistent and damaging presence on the Internet. The lack of up-to-date threat protection and poor patching policies within both corporate and home user environments continue to allow these worms to propagate and extend their lifespan. The introduction of Bugbear and Opaserv in this quarter, in conjunction with new variants of Nimda and Klez, reinforces the current trend of online security threats, as hybrid threats with massive distributions continue to increase in frequency. As a result, the damage from attacks is shifting from single Web site defacements to large-scale attacks affecting critical systems that are more damaging and costly.

X-Force observed a very noticeable trend concerning vulnerability exploitation this quarter - multiple hybrid threats released to attack the same vulnerability. This is in contrast to the past, where multiple exploits usually attacked different vulnerabilities. These new threats are generally more focused and more serious in nature since they select popular software on critical systems to deliver larger amounts of damage, and faster, wider worm propagation within each successful attack.

## Table Of Contents

Executive Summary  
Internet Risk Summary for  
September 28 through December  
31, 2002

- > Bottom Line
- > Outlook for 2003
- > AlertCon Risk Levels
- > Attack Activity Summary
- > Attack Sources
- > Internet Rogues
- > Destination Business Sectors
- > Homeland Security and Hactivism
- > Wireless LAN
- > Peer to Peer (P2P) Networks and Instant Messaging
- > .NET
- > Lotus Domino
- Risk Elements Added To AlertCon Baseline
- > Hybrid Threats and Worms Report Methodology and Sources of Information
- 2002 IRIS Year In Review
- > Long Lasting Threats
- > Critical Infrastructure
- > Hactivism
- > Internet Security Systems
- AlertCon Review



By targeting servers that are integral to an organization's infrastructure, attackers create massive disruption with minimal effort. For example, the attack on thirteen Domain Name Service (DNS) "root" servers on October 23, 2002 had the potential to shut down a large amount of Internet traffic by attacking only thirteen machines.

## About AlertCon™

Internet Security Systems provides a standardized scale that measures the relative threat status of active Internet risks. These **AlertCon™** levels — or “alert conditions” — are established on a daily basis through Internet Security Systems’ Global Threat Operations Center based on the previous 24 hours’ activity and anticipated activity for the next 48 hours.

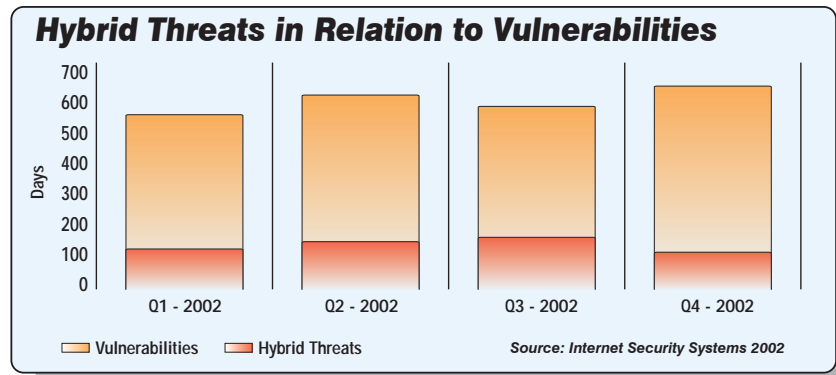
**AlertCon 1** — Internet risk baseline reflecting the malicious, determined, global, 24/7 attacks experienced by all networks connected to the Internet. In simple terms, AlertCon 1 indicates that a newly configured computer will be compromised within 24 hours of first being connected to the Internet.

**AlertCon 2** — Increased vigilance. The potential exists for increased risk because of new vulnerabilities or credible threats to the confidentiality, integrity, and/or availability of computer networks. Some degree of vulnerability assessment and potential corrective action is recommended.

**AlertCon 3** — Focused attacks. Internet attacks have been noted against specific vulnerabilities or inherent information system weaknesses. Immediate defensive action is required.

**AlertCon 4** — An actual or potentially catastrophic security situation has arisen within a network or group of networks whose survival depends on immediate and focused defensive action. This condition may be imminent or ongoing.

The rate at which hybrid threat and worm variants were released also trended upwards in the fourth quarter. Worm writers have begun to release the source code for their creations with greater frequency, enabling rapid mutations by other members of the underground. These variants often include a more powerful attack that may be able to evade protection systems previously updated to protect against the original worm.



Although the number of exploits found in the wild has not kept up with the number of vulnerabilities, the exploits that are developed and released are more concentrated (focusing on several critical systems) and more dangerous (in terms of capabilities) than the ones released several years ago.

Since the terrorist attacks on September 11, 2001, the online world has been on guard against the tangible threat of politically motivated attacks, which have the prospect of merging physical terror threats with cyber attacks. Hacktivism has taken center stage as we become aware of more attacks against government Internet properties belonging to the United States, Israel, and Britain. This topic has gained more attention in news outlets and will become an even greater concern as 2003 approaches. The U.S. government successfully deflected over 6,000 cyber attacks, of which a significant number were undisclosed to the general public.

## Internet Risk Summary for September 28 through December 31, 2002

### Bottom Line

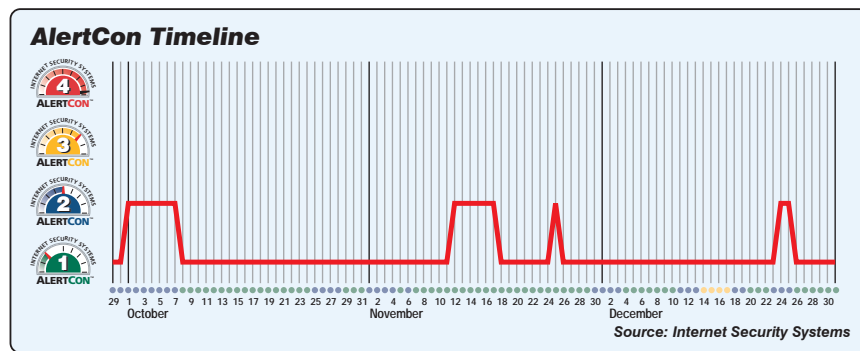
General Internet risk continues to rise, and the specific mix of threats seen in this reporting period continues to evolve. Introduction of the combined physical/cyber threat may become a reality as critical resources come under attack by highly focused hybrid threats. The risk components visible in this period are addressed below.

## Outlook for 2003

Overall, the outlook is that the upward risk trend will continue to rise. The greatest threats throughout the beginning of 2003 are expected to be continued introduction of new, mass-mailing and highly persistent worms, as well as the rising focus on hacktivism. Increasing demand for easily accessible Internet connections, such as consumer broadband and wireless Local Area Networks (LANs), will continue to grow as sources for exploitation. Critical systems required for basic connectivity and infrastructure will need protection as focused attacks and their variants target specific vulnerabilities and systems.

## AlertCon™ Risk Levels

During the fourth quarter of 2002, Internet Security Systems (ISS) observed 79 days at AlertCon 1, 16 days at AlertCon 2, and no days at AlertCon 3 or AlertCon 4. The fourth quarter did not experience high-risk levels typically brought about by the introduction of a new large-scale threat such as Nimda. However, the overall risk level has not diminished.



On October 1, 2002, the AlertCon was escalated to level 2 as X-Force monitored the propagation of several new worms. The Bugbear and Opaserv (Scrup) worms were accompanied by variants of the already prolific Slapper worm (Apache/mod\_ssl worm). The Bugbear worm had compromised over 7,500 machines by midday on October 1, and continued to spread rapidly for seven days until patching and cleanup began.

The AlertCon level returned to 2 on November 12, when multiple remote vulnerabilities in BIND4 and BIND8 were discovered and announced by X-Force. Since BIND is the most common implementation of the DNS (Domain Name Service) protocol, the vulnerabilities affect nearly all currently deployed recursive DNS servers on the Internet. However, at the time of this report, no exploits have been found in the wild.

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21469>

A vulnerability in the Sun Microsystems implementation of the X Window Font Service (XFS) was discovered by X-Force and announced on November 25, 2002. As an act of precaution, the X-Force Threat Analysis Service raised the AlertCon level to 2 for 24 hours.

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21541>

### Attack Activity Summary

Internet Security Systems observed 16,601,734 security events from monitored systems during this reporting period, resulting in 1,867 security incidents. A security incident is defined as an actual attack or a security event that contains an element of unusual risk.

This reflects a slight increase in the number of security events from the third quarter, which registered 16,342,620 security events and 1,385 security incidents.

The highest average daily traffic for the reporting period occurred on Wednesday, where 198,322 security events were triggered. 23.39 percent of all security events occurred during the weekend, when network administration centers generally operate with a reduced staff.

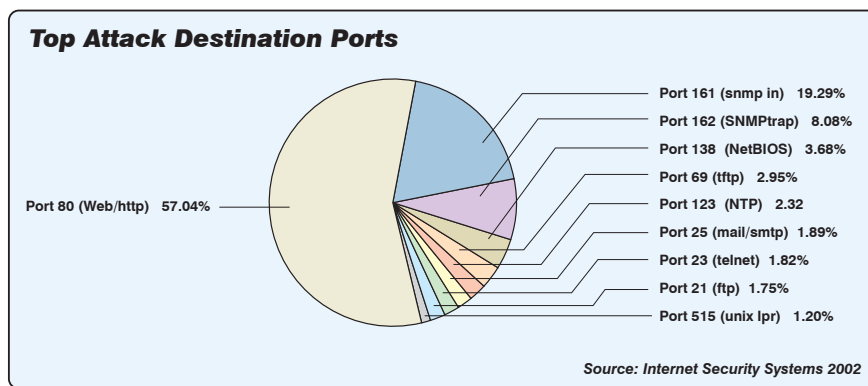
Sunday 141,828	Thursday 188,598
Monday 189,705	Friday 192,345
Tuesday 171,158	Saturday 145,260
Wednesday 198,322	

Additionally, holidays such as Thanksgiving, Christmas, and New Year's provide a significant period of downtime for support staffs, which leave hackers a substantial window of opportunity. This lends to an increased risk of physical and/or cyber threats.

There was a notable increase in the number of Events and Security Incidents occurring across the ISS Managed Security Services (MSS) customer base during the holidays. The events from the Thanksgiving 2001 timeframe equaled 803,734 with escalations of 94 Security Incidents. The Christmas and New Year's 2001 season brought a total of events equaling 2,387,185 and a Security Incident total of 221.

12/23/02 - 12/31/02 = 1,610,557 Events and 140 Security Incidents

11/26/02 - 11/30/02 = 884,794 Events and 83 Security Incidents



During the fourth quarter, increased attention was placed on the NetBIOS ports (ports 137, 138 and 139), with an emphasis on port 137 in particular.

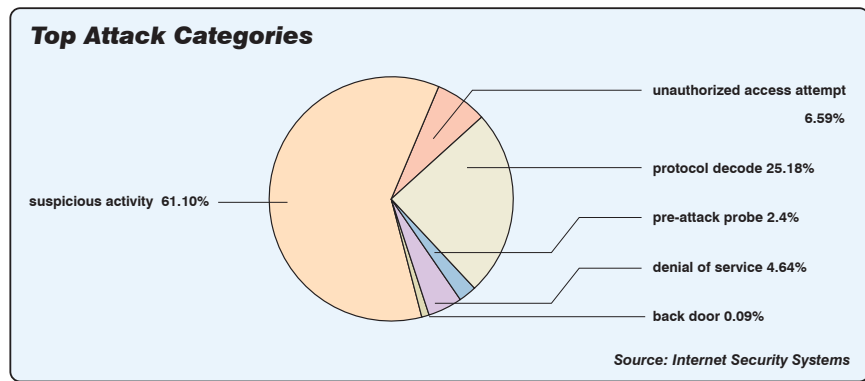
During the weekend of November 22-24, a large increase in ICMP and port 137 scanning was noted across the Internet. This resulted in numerous reports being submitted to Information Sharing and Analysis Centers (ISACs) and to the National Infrastructure Protection Center (NIPC). Similarly, there were a number of incident reports during that 48-hour timeframe regarding security breaches against commercial entities.

The propagation of the Opaserv worm generated a huge fluctuation in port 137 (NetBIOS) and port 445 (Microsoft-DS) activity. This fluctuation was due to the fact that this worm spreads through open network shares and issues Windows Internet Naming Service (WINS) queries in order to find open network shares in order to propagate.

Increased usage of Messenger Spam accounted for an increase in NetBIOS activity during the fourth quarter. Messenger, not to be confused with MSN Messenger, is used by system administrators to transmit "net send" and Alerter service messages between clients and servers. This service is turned on by default and is part of the NetBIOS service, thus using the NetBIOS ports (137,138, and 139). However, systems behind a firewall or corporate network that have inbound NetBIOS restricted or blocked should be safe.

The announcement of the BIND 4 and 8 vulnerabilities accompanied by the Distributed Denial of Service (DDoS) attack on the root DNS on October 23 highlighted all port 53 activity. Though the timing seemed to indicate a direct correlation, it was purely coincidental. There has been no exploitation of the BIND vulnerabilities to date.

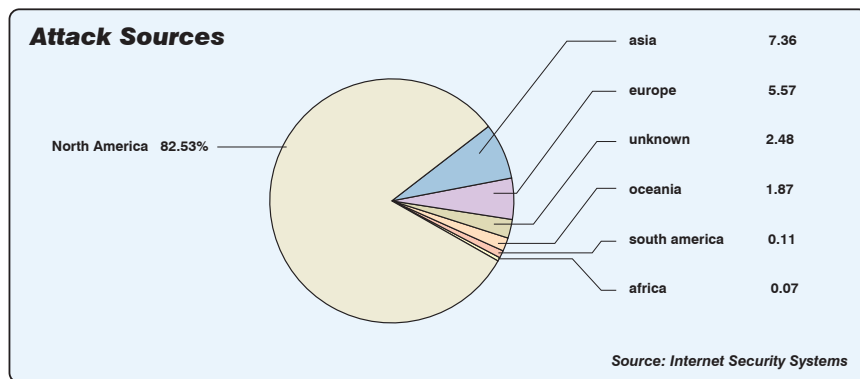
Some emphasis was placed on port 1812 (Radius) when the Slapper.F variant added a new twist to the worm's propagation by changing to this port. The concern was that the port is open on most firewalls.



The top three categories of attack continue to be associated with worm and other self-propagating hybrid threats, which exploit multiple vulnerabilities across desktops and servers.

## Attack Sources

During this reporting period, Internet Security Systems' monitored and managed Intrusion Detection Systems (IDS) customers reported the following top five source countries for attacks:



## Internet Rogues

Sources of hostile Internet activity may resolve to a registered owner of a particular Internet Protocol (IP) address. However, identification of an originating address does not mean malicious activity actually started at that particular location, nor does it tie a specific human being to the machine in question. This information, therefore, must be used with extreme caution when applied to online defense strategies.

Internet Security Systems defines hostile Internet threats only when they are identified by a primary source of information under Internet Security Systems' direct control. The primary source for this information are IDS sensors located around the world based on RealSecure® software and monitored on a 24/7 basis. Hostile activity is identified based on alarm information measured against attack templates installed on these sensors.

Identification of IP Address Ownership - Only official, publicly available lists are used to identify the registered owners of IP Addresses. This report will incorporate new official groups as they become available. The following organizations are among those used in the preparation of this report:

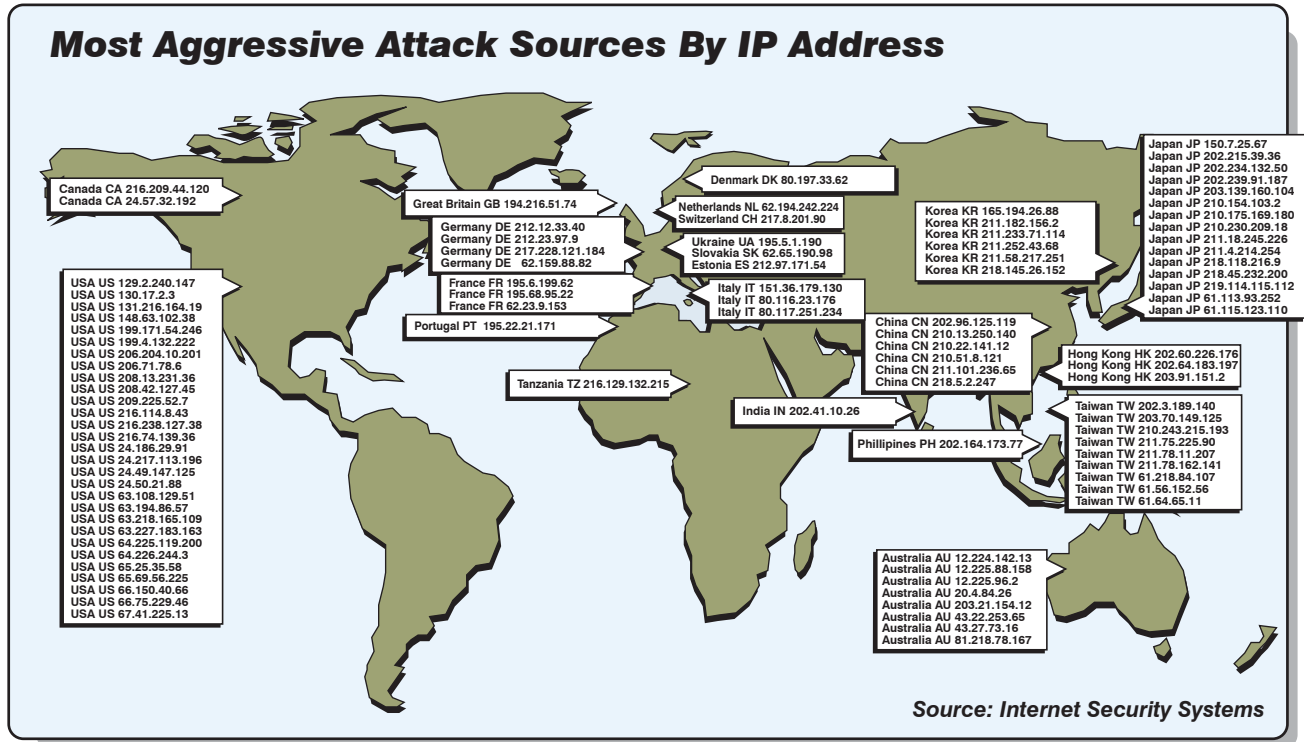
- The American Registry for Internet Numbers (ARIN) - <http://www.arin.net/index.html>
- Réseaux IP Européens (RIPE) - <http://www.ripe.net/ripe/about/index.html>
- Asia Pacific Network Information Centre (APNIC) - <http://www.apnic.net/>
- Internet Corporation for Assigned Names and Numbers (ICANN) - <http://www.icann.org/>

Quality Assurance - Every effort has been made to insure accuracy in reporting. The resolution of each IP Address owner is double checked, as is the IP address itself, and then matched to the original sensor report.

Duration - This list is published quarterly and covers the previous quarter. Each list will be retained, along with the source data, for three years. However, the dynamic nature of the Internet makes it imperative to publish only three months' data at any given time. What follows are the most aggressive sources of malicious or potentially malicious activity noted during this period.

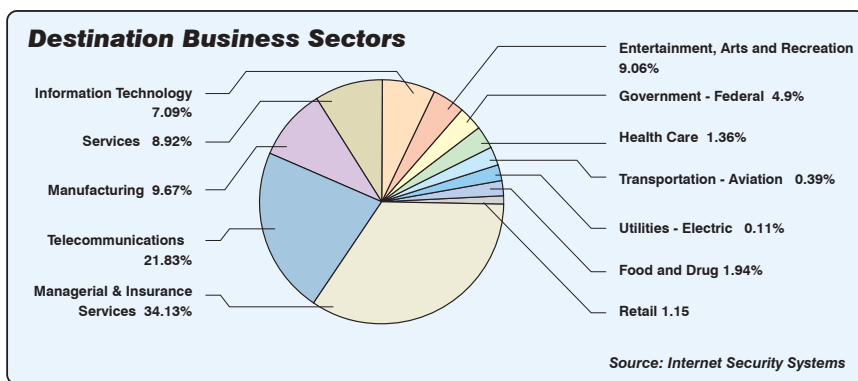
The graphical list represents only security incidents that show multiple attempts directed from the same source IP addresses against monitored customers and include pre-attack reconnaissance, back doors, and scripted Web attacks. Many of the sources resolve to Internet Service Providers (ISPs) who are unsuspecting participants in these exchanges.

Anyone wishing to use this list as a reference for defensive IP blocking should take these constraints into account. It is usually impractical to block a single IP Address from an ISP since they are typically randomly assigned to a customer only for the duration of a session.



### Destination Business Sectors

Sectors of industry targeted are as follows:



These numbers should be viewed with some caution, since adoption of security products is not evenly distributed across the global industrial base. Financial sector customers, having arguably the most to lose in an online commercial environment, were early adopters of Internet security. This also holds true for the IT community, which is expected to be more effective at online

protection than less technology-driven businesses. A substantial awareness of the need for Internet security, coupled with a prominent online presence, make these sectors disproportionately represented in these statistics.

### **Homeland Security and Hacktivism**

As political tensions intensify between the United States and other nations, the risk of cyber warfare becomes more tangible. Hacker groups continue to launch digital attacks on the United States, the U.K., and Israel for political reasons. Global industries that deal directly with the United States and its supporters have received several threats from terrorist organizations. The act of political hacking continues to rise worldwide. Open-source sites and security agencies have published countless warnings and alerts throughout the fourth quarter highlighting the acts of Hacktivism.

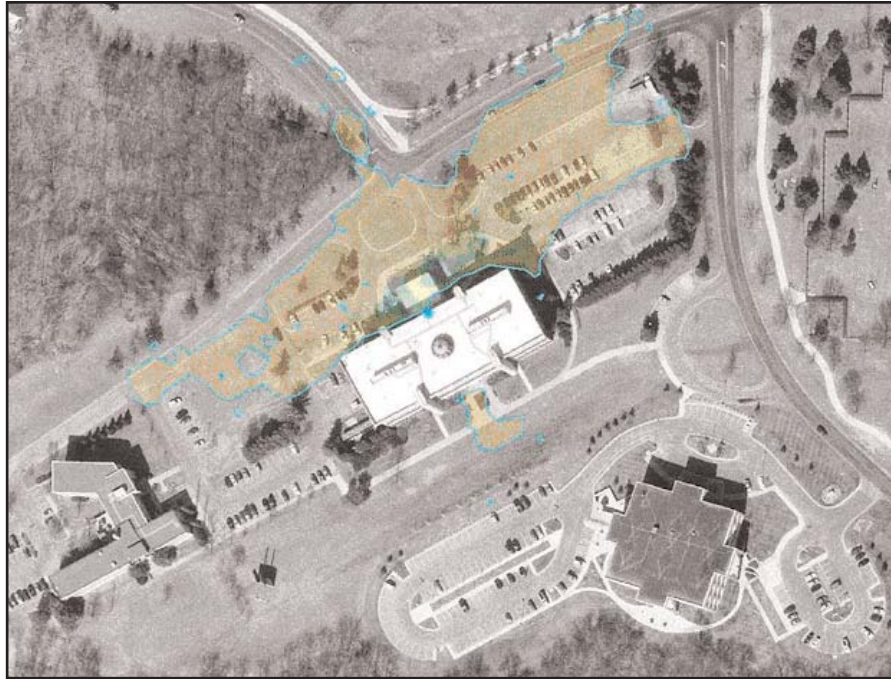
On November 18, 2002, during an exclusive interview with *Computerworld* magazine, the founder of the Jama'at Al-Muhajirun and a spokesman for Osama bin Laden's International Islamic Front for Jihad against Jews and Crusaders, Sheikh Omar Bakri Muhammad announced that all avenues of technology were being reviewed for the global jihad. Just eleven days before the U.S. Thanksgiving holiday, he highlighted Osama Bin Laden's interest in cyber weapons. The stock markets in New York, London, and Tokyo were noted as possible targets. These threats are not unprecedented, since organizations in this sector are usually among the most commonly targeted.

Several unclassified U.S. military sites were successfully targeted throughout 2002. In November, the media outlet *CNN* announced that Federal authorities had identified the hacker as a British citizen. Since the September 11 attacks, United States anti-hacking laws have been strengthened, including the possible extradition of the hacker, an act that has not been commonplace until now.

On November 14, 2002, Movladi Udugov, a Chechen separatist, made claims that Russia's FSB security service attacked the two politically motivated Web sites kavakz.org and chechenpress.com. On the October 26, an attack coincided with the Russian security forces attempts to regain control over a Moscow theater filled with armed rebels and hostages.

### **Wireless LAN**

Wireless LANs, or Wi-Fi (802.11a, 802.11b, and 802.11g), utilize high-frequency radio waves rather than wires to communicate between hosts. WiFi is a relatively new technology that has been adopted by many global institutions. The ease with which WiFi technologies can be deployed should be of concern to all system administrators. A wireless access point could be deployed by anyone within a corporation with access to a network drop. This could potentially expand the network perimeter to include an area outside the physical walls of a company. Compounding this problem is that many of these access points (APs) have security options that are not enabled by default or are very difficult to implement. This presents a window of opportunity for a would-be hacker, who would no longer need to use skills to break into a network, but would just need to be in close proximity to a target.



In this image a single AP is isolated from the network and a signal strength field is shown for this device.

Copyright © 2002 Information & Telecommunications Technology Center Kansas Applied Remote Sensing Program



A single network composed of nine access points (AP's). Each AP is denoted by an asterisk. The complete network coverage is shown by the shaded area while the unique field for each AP is bounded by its respective color.

Copyright © 2002 Information & Telecommunications Technology Center Kansas Applied Remote Sensing Program

## Peer-to-Peer (P2P) Networks and Instant Messaging

Popular peer-to-peer clients such as KaZaA, Morpheus, and Gnutella have been used to spread worms and malicious code. Worm.P2P.Duload, W32.Efno.Worm, and W32.HLLW.Electron are just a few of the worms that rely on the accessibility of peer-to-peer file sharing.

Internet Security Systems' X-Force organization published a white paper on the "Risk Exposure Through Instant Messaging and Peer-To-Peer (P2P) Networks" on April 22, 2002. [http://documents.iss.net/whitepapers/X-Force\\_P2P.pdf](http://documents.iss.net/whitepapers/X-Force_P2P.pdf). The paper explains the risks individuals take by allowing access to their computers via these information sharing programs.

## .NET

Microsoft's .NET technology provides powerful functionality to developers, these services can represent a potential threat to the security of a Web server. .NET applications and services can provide potential intruders with a new vector of attack, since many firewalls do not process HTTP traffic at a sufficient level to recognize malicious activity. Furthermore, these applications can possibly be used as a gateway for attackers to communicate with the .NET application servers.

Internet Security Systems' X-Force organization published a white paper detailing some security considerations for Microsoft's ASP .NET framework. [http://documents.iss.net/whitepapers/asp\\_net\\_whitepaper.pdf](http://documents.iss.net/whitepapers/asp_net_whitepaper.pdf). The paper explains the functionality of .NET and the application and services that can be deployed via the Web.

## Lotus Domino

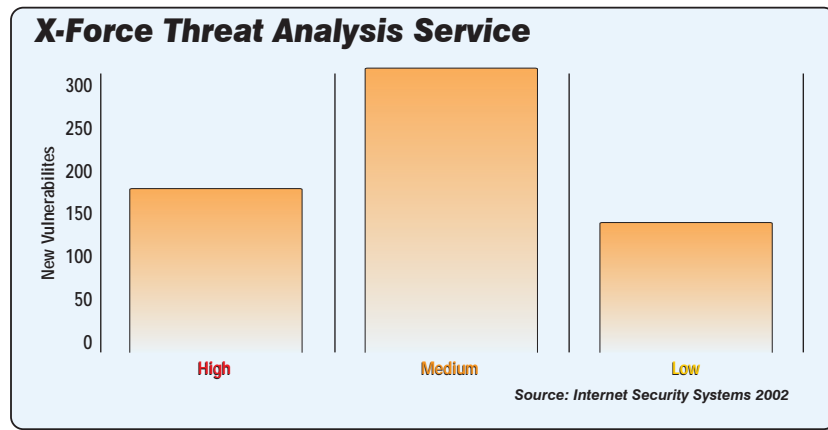
Lotus Domino provides groupware functionality and development tools to create messaging, collaboration, workflow, tracking, Internet, and intranet applications. Lotus Domino 6 currently supports Microsoft Windows NT 4.0, Microsoft Windows 2000, Sun Solaris SPARC, IBM AIX, IBM OS/400, and Red Hat Linux platforms.

The services and options included with Lotus Domino combine to create an application server that is powerful and customizable for many different tasks. If not configured properly, these servers can become gateways to an internal corporate network or may disclose sensitive or restricted information to a malicious user. Security administrators must ensure that the Domino server and the underlying operating system have current patches installed and are configured as securely as possible. This process must include using encryption for communication, disabling unused services, and proper permissions to directories and files that contain sensitive information.

Internet Security Systems' X-Force organization published a white paper on xxx xxDecember 20, 2002 detailing the security architecture and services of Lotus Domino 6.0. <http://documents.iss.net/whitepapers/domino.pdf>.

## Risk Elements Added to the AlertCon Baseline During this Reporting Period

Internet Security Systems added 644 new vulnerabilities to the X-Force Database, broken into risk levels as follows: 179 High, 327 Medium and 138 Low. The most common of these vulnerabilities continues to involve buffer overflows that can be exploited for unauthorized access.



Over the last year there have been several incidents in which the source code of a popular open source site was intentionally and maliciously altered. This compromised source code often contained a trojan that could be downloaded by an unsuspecting user. During the month of November, multiple releases of tcpdump and libpcap (located at [www.tcpdump.org](http://www.tcpdump.org)) were successfully trojaned. The modified distributions were only available for download on November 11-13, 2002. The [www.tcpdump.org](http://www.tcpdump.org) Web site has several mirrors; it is believed that the distribution of trojaned code had made it to at least one of the mirrored sites and the availability of these distributions from the mirror sites was not known.

On October 21, 2002, a DDoS attack DDoS was launched targeting DNS root servers, successfully affecting seven of the thirteen servers. Though the effects of the incident were minimal and most Internet connections saw no noticeable effect, the general public was bombarded by media coverage and possible ties to terrorism. Subsequently, one of the root servers was relocated. The activity was traced to Korea, which is a frequent source of cyber attacks. This pattern is due to a large number of users with broadband Internet access, since Korea has a huge and rapidly growing base of installed DSL lines. The Korean sources were likely jump points, having no direct association to any specific hacking group.

The Internet Security Systems X-Force discovered a vulnerability in the Sun Microsystems implementation of the X Window Font Service, or XFS. The XFS service was designed as a component of the X Windows systems to establish a common mechanism to export font data to all computers on an X Windows network. A buffer overflow vulnerability exists within the XFS service (fs.auto) that potentially allows remote attackers to run arbitrary commands on a target system. Attackers must exploit this vulnerability in conjunction with another attack to gain root access because the fs.auto service does not run with superuser privilege. The service is configured to run by default and is bound to a high TCP port. Though normally blocked on perimeter firewalls, networks that are not filtering high TCP ports as well as internal networks are potentially at risk. <http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21541>

On November 12, the Internet Security Systems X-Force released a Security Advisory that detailed multiple remote vulnerabilities in BIND4 and BIND8. Since BIND is the most common implementation of the DNS protocol, the vulnerabilities affect nearly all currently deployed recursive DNS servers on the Internet. The vulnerabilities include a BIND SIG Expiry Time DoS, OPT DoS, and SIG Cached RR Overflow. There is currently no known exploit, although hacking groups have acquired the patch and are currently trying to formulate an exploit.  
<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21469>

Internet Software Consortium (ISC) has made new versions of BIND available. ISC recommends that BIND installations should be upgraded to BIND version 4.9.11, 8.2.7, 8.3.4 or to BIND version 9. BIND 9 was not affected by any of the vulnerabilities described in this advisory  
<http://www.isc.org/products/BIND/bind-security.html>.

The Internet Security Systems X-Force issued a Security Alert detailing Microsoft Security Bulletin MS02-065. The Alert contains information on a buffer overrun in Microsoft Data Access Components (MDAC) that could lead to the execution of malicious code. The Microsoft Security Bulletin states that the security vulnerability results from an unchecked buffer in the Data Stub. The versions affected are those prior to 2.7, the version that shipped with Windows XP. A malformed HTTP request is sent to the Data Stub with which an attacker could cause the data of choice to overrun onto the heap.

Web servers are vulnerable if a version of MDAC prior to 2.7 is running. An attacker would need to establish a connection with the server and then send a specially malformed HTTP request. Once the request was sent it would overrun the buffer with the chosen data. The code would run in the security context of the Internet Information Server (IIS) service.

Web clients are vulnerable in almost every case because the RDS Data Stub is packaged with all current versions of Internet Explorer and the option to disable it is not available. For successful exploitation of this vulnerability, an attacker would need to host a Web page that, when opened, could send an HTTP reply to the user's system and overrun the buffer with the chosen data. The Web page must be hosted on a Web site or sent directly to users as an HTML email. The code then runs in the security context of the user. Note: RDS is disabled by default on installations of Windows XP and Windows 2000, and can be disabled on other systems by following the IIS Security Checklist.

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis4cl.asp>  
IIS Security Checklist: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-065.asp>

### **Hybrid Threats and Worms**

Internet Security Systems added 101 new entries to the X-Force Threat Analysis Service during this period, broken into risk levels as follows: 1 High, 6 Medium and 94 Low. These numbers are a slight decrease from the 141 recorded in the third quarter. These new threats, combined with the persistent worms and hybrid threats reported in previous IRIS reports, continue to increase the overall risk.

### **Bugbear Worm**

On October 3, 2002, ISS X-Force released a Security Alert on the Bugbear Internet worm, which was first discovered in Malaysia on September 30, 2002. Bugbear is a worm that propagates through email (SMTP) and open NetBIOS shares. The worm, written in Microsoft Visual C/C++ and packaged with UPX, contains a backdoor trojan component with key logging functionality and attempts to disable all security/antivirus software on each host.

As with most mass-email worms, propagation can cause network congestion. Information about the backdoor installation has been made public. Thus, accessibility to the back door is not limited to the author but to third-party attackers as well. A clean-up tool has been provided by McAfee. Those individuals whose computers are infected with the worm should download McAfee's Stinger tool. <http://vil.nai.com/vil/stinger/>

### **Opaserv Worm**

The Opaserv worm (also known as Scrup) affects machines connected to a network running Windows 95, 98, and Me operating systems. The worm spreads through open network shares. This generates large amounts of NetBIOS traffic, issuing WINS queries to find open network shares through which to propagate. After finding a network share, the worm copies itself to a remote computer, creating a file in the system root directory (C:\WINDOWS\ by default). The worm attempts to connect to a designated site (determined by the specific version of the worm) and updates itself to a newer version. These sites are generally disabled within a reasonable amount of time after discovery. Microsoft has made patches for the vulnerability exploited by this worm available at:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-072.asp>

Highly-Persistent Worms: Klez, Slapper, Nimda, and Spida  
Information describing each of these worms is listed below.

### **Klez Worm**

Since the first infection of Klez in October 2001, new variants of the worm continue to proliferate across the Internet. The worm spreads as an internal mass-mailing engine or via shared drives connected to a Local Area Network (LAN). While the worm wraps itself in a relatively standard email message, its ability to elude most antivirus products has enabled it to spread quickly and extensively. Variants of the Klez worm have been among the top 3 virus threats since the worm's release in January 2002. This applies especially to the Klez.E variant, which appeared in February and is highlighted as one of the fastest-spreading worms on the Internet. The worm attempts to infect potential victims and deactivate antivirus products by deleting registry keys, disrupting running processes, and removing virus definition files.

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20289>

### **Slapper Worm**

Internet Security Systems X-Force released a Security Alert on September 13, 2002, detailing the active propagation of the Linux.Slapper.Worm. The worm exploits a previously disclosed vulnerability in the Secure Sockets Layer 2.0 (SSLv2) handshake process. The worm is a modified derivative of the Apache Scalper worm and targets Linux servers running Apache with mod\_ssl.

Slapper has DDoS capabilities as well as backdoor functionality. Several new variants were released during this reporting period. The newest members of the family use the same exploit and payload. However, they report to a different Web distribution server, the scanning engine has been altered, and some variants do not have peer-to-peer control. Slapper.D, also known as Linux/DDoS-Kaiten, began propagation late Monday, September 30, 2002, until its Web distribution server was taken offline. The association to Kaiten occurred during analysis when particular attributes of the worm fit a known DDoS tool. The source code was altered, which appeared to take place in less than an hour and Slapper.E began its propagation. Slapper.F, which is most like variant .C, added a new twist by changing to a widely open port 1812 (Radius). The concern is that this port is open on most firewalls.

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21130>.

A clean-up tool has been provided by ISS X-Force. Those individuals whose computers are infected with the worm should download the tool at [http://www.iss.net/support/product\\_utilities/](http://www.iss.net/support/product_utilities/).

### **Nimda Worm**

IIS worms such as Nimda and Code Red continue to compromise unpatched systems. Corporate networks and home users constantly activate and connect to the Internet with old versions of software. These machines are especially vulnerable since they are connected to the Internet without correct service patches.

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20301>

### **Spida Worm**

The SQL/Spida worm affects Microsoft's SQL server and attempts to log in with the administrator (sa) account and a blank password. The worm will infect a vulnerable target, send its configuration and password information to an external host, and begin scanning for new targets. Although the Spida worm is not destructive to the infected host, it may generate a damaging level of network traffic when it scans for additional targets. The scanner bundled with the worm is multi-threaded and is capable of scanning with 100 threads. This worm exploits weak passwords, which cannot be remedied through patching.

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20209>

## **Report Methodology and Sources of Information**

Internet Security Systems monitors high-volume RealSecure intrusion detection sensors on client networks through five Security Operations Centers (SOCs) operating on three continents, on a 24/7 basis. This information is aggregated, anonymized, and analyzed at Internet Security Systems' Global Threat Operations Center (GTOC) in Atlanta, Georgia. These sensors are aggressively monitored and updated to detect even newly emergent attack techniques. As a result, these sensors provide a primary source of Internet threat information. Additional information comes from aggregate data collected from firewalls monitored at the SOC's, professional services, and forensic investigations performed for Internet Security Systems, corporate clients, research from Internet Security Systems X-Force knowledge services organization, and liaison contacts in industry, government, academia, and public media. These results are posted daily along with an AlertCon determination of Internet risk at <http://www.iss.net>, and are available via email alerts and daily email risk notifications.

Additional information is obtained from the Internet Security Systems' X-Force Database (XFDB). The XFDB is the world's most comprehensive threat and vulnerability database and provides the intellectual capital that underlies Internet Security Systems' market-leading, award-winning products and services. The database contains over 10,000 unique vulnerabilities, threats, and security checks, compiled from such resources as the Internet and thousands of hours of original X-Force research collected over more than eight years of operations. A public version of the database is available online at [http://www.iss.net/security\\_center/search.php](http://www.iss.net/security_center/search.php). With more than 250 years of combined experience, the X-Force organization possesses a wide range of expertise in security management strategies and tactics. This deep understanding of distributed computing, global networking, programming and forensics keeps the X-Force at the forefront for combating the latest developments in online security.

### **About Internet Security Systems, Inc. (ISS)**

Internet Security Systems, Inc. (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical information assets from an ever-changing spectrum of threats and misuse. Software from Internet Security Systems dynamically detects, prevents and responds to sophisticated threats to networks, servers and desktops. Services include 24/7 system monitoring, emergency response and access to the X-Force, Internet Security Systems' renowned research and development team. Headquartered in Atlanta, GA, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at [www.iss.net](http://www.iss.net) or call 888-901-7477.

Copyright © 2001 - 2002, Internet Security Systems, Inc.

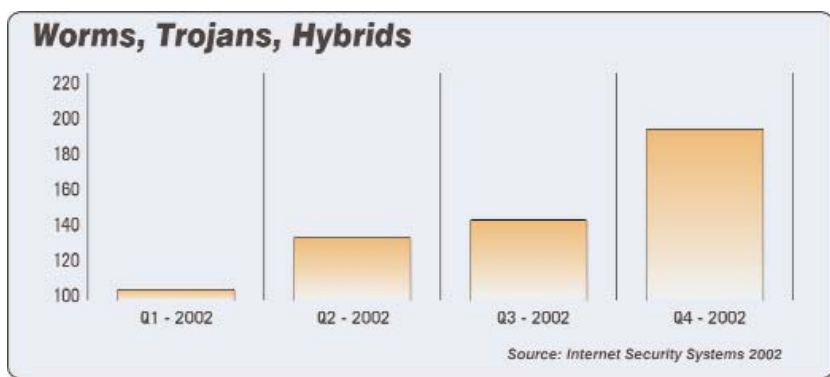
All rights reserved worldwide. Internet Security Systems, the Internet Security Systems logo, AlertCon and X-Force are trademarks, and RealSecure a registered trademark, of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice. Permission is hereby granted for the electronic redistribution of this document. It is not to be edited or altered in any way without the express written consent of Internet Security Systems. If you wish to reprint the whole or any part of this document in any other medium excluding electronic media, please contact Internet Security Systems for permission. Disclaimer: The information within this paper may change without notice. Internet Security Systems provides this information on an AS IS basis, with NO warranties, implied or otherwise. Any use of this information is at the user's risk. In no event shall Internet Security Systems be held liable for any damages whatsoever arising out of or in connection with the use or dissemination of this information.



# 2002 IRIS Year In Review

## Long Lasting Threats

Multiple large-scale hybrid threats and mass-mailing propagations occurred with regularity throughout 2002. Hybrid threats, which exploit multiple vulnerabilities across desktops and servers, enjoyed longer than expected individual lifespans, growing at a steady rate for months rather than days or weeks. These highly persistent worms, including Slapper, Klez, and Nimda, spread rapidly across the Internet. As a result, they generated large amounts of network congestion. For example, Nimda was released in September 2001 and is still a persistent threat fifteen months later. The continual propagation of Code Red and Nimda variants, as well as the introduction of Klez, Opaserv and Bugbear, affects both corporate and home users.



## Table Of Contents

- Long Lasting Threats
- Critical Infrastructure
- Hactivism
- Internet Security Systems
- AlertCon Review
- > 2002 X-Force Security Alerts
- > 2002 X-Force Security Advisories

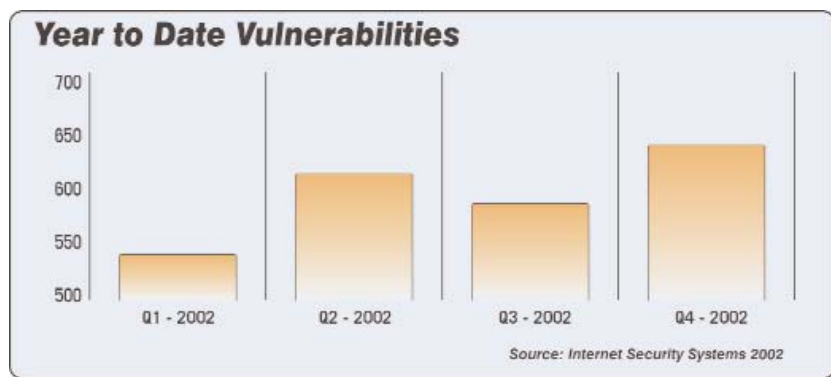
The focus of these attacks changed as well. Rather than multiple threats mapping to multiple vulnerabilities, 2002 saw the emergence of multiple threats targeted at the same vulnerability. These new threats are very serious in nature, attacking a specific vulnerability on either a popular software package or a system critical for operations or infrastructure.

## Critical Infrastructure

Attackers clearly hope to target more systems with less effort, resulting in attacks that spread quickly and affect as many systems as possible. For example, the attack on thirteen Domain Name Service (DNS) root servers on October 23, 2002 had the potential to shut down a large amount of Internet traffic by attacking just thirteen machines.

Two standout vulnerabilities were OpenSSL, which led to the propagation of Slapper and the remote compromise vulnerability in the Apache HTTP server. Each of these had the potential to affect and disrupt Internet traffic for thousands of users. Although the BIND4/BIND8

vulnerability has the potential to be more devastating, no exploit has been developed in the wild as of this time.



## Hactivism

Hactivism became a hot topic among security news forums and publications during the fourth quarter of 2002. Hactivism refers to network attacks that are politically, ideologically, or theologically motivated. Since September 11, 2001, cyber warfare has become an increasingly realistic threat. Although the overall success of these attacks has been minimal, there is evidence that these threats will increase substantially next year.

## Internet Security Systems AlertCon™ Review

The year began at AlertCon level 2, as X-Force released an advisory addressing a buffer overflow vulnerability in /bin/login. The AlertCon level returned to 1 as this new vulnerability joined newly released Code Red and Nimda variants to become part of the everyday baseline activity.

In February, the AlertCon level rose to 3 as an exploit for a vulnerability in SNMP v1 (Simple Network Management Protocol) was published. The risk level was reduced to 2 during the initial stages of patching.

The risk level fluctuated between AlertCon 1 and 2 with announcements of vulnerabilities in PHP, Microsoft IIS and SQLXML. These vulnerabilities, combined with new variants of Klez and Nimda, did not affect the AlertCon level, which stayed constant until the end of the second quarter.

In June, X-Force discovered a serious vulnerability in several versions of the Apache Web Server that allow a remote attacker to modify or bring down the server. The AlertCon level rose to 3 as exploit code, possibly in development for several months, was released and servers came under active attack.

During the third quarter, AlertCon 3 was maintained for seven days as the Slapper worm was released and began propagating rapidly. The threat level was reduced to AlertCon 2 as patching to protect systems against Slapper slowed its spread. AlertCon 2 was observed during the rest of the third quarter due to a vulnerability in Microsoft Exchange, FBI warnings of hacker attacks, the threats from hackers of a DDoS (Distributed Denial of Service) against federal and major news sites and in observance of the anniversary of the terrorist attacks on September 11, 2001.

AlertCon 2 was the highest level observed during the fourth quarter. New hybrid worms such as Bugbear, Opaserv and several variants of Slapper began propagation in the beginning of October 2002. X-Force discovered vulnerabilities in BIND4/BIND8 and the Sun Microsystems implementation of the X Window Font Service (XFS). Since BIND is the most common implementation of a DNS (Domain Name Service) server, the vulnerabilities affect nearly all currently deployed recursive DNS servers on the Internet. The vulnerabilities include a BIND SIG Expiry Time DoS, OPT DoS, and SIG Cached RR Overflow.

X-Force released 22 Security Alerts and nine Security Advisories, highlighting original research and serious security threats that require immediate attention:

### **2002 X-Force™ Security Alerts:**

- Microsoft MDAC Remote Compromise Vulnerability - (November 21, 2002)
- Bugbear Hybrid Threat Propagation - (October 03, 2002)
- Propagation of "Slapper" OpenSSL/Apache Worm Variants - (September 22, 2002)
- Flaw in Internet Scanner Parsing Mechanism - (September 18, 2002)
- "Slapper" OpenSSL/Apache Worm Propagation - (September 14, 2002)
- Microsoft Windows SMB Denial of Service Vulnerability - (August 29, 2002)
- Multiple Vulnerabilities in Microsoft Office Web Components - (August 22, 2002)
- Remote Compromise and Denial of Service Vulnerability in PHP - (July 22, 2002)
- Apache HTTP Server Exploit in Circulation - (June 19, 2002)
- Heap Overflow in IIS HTR Chunked Encoding - (June 14, 2002)
- Remote Denial of Service Vulnerability in ISC BIND - (June 04, 2002)
- Microsoft SQL Spida Worm Propagation - - (May 21, 2002)
- Increased Hacking Activity Associated with Underground File-Sharing Networks - (May 03, 2002)
- Remote Denial of Service Vulnerability in RealSecure Network Sensor - (April 30, 2002)
- Outbreak of Klez Family Hybrid Threats - - (April 26, 2002)
- Multiple Remote Vulnerabilities in Microsoft IIS - (April 10, 2002)
- Multiple PHP Vulnerabilities: Remote Compromise Exploit in Circulation - (February 27, 2002)
- Buffer Overflow in Microsoft Internet Explorer - (February 25, 2002)
- PROTOS Remote SNMP Attack Tool - (February 12, 2002)
- Remote Denial of Service Vulnerability in BlackICE Products - (February 05, 2002)
- Remote Denial of Service Vulnerability in Snort IDS - (January 28, 2002)
- AOL Instant Messenger Remote Buffer Overflow - (January 02, 2002)

**2002 X-Force Security Advisories:**

- Solaris fs.auto Remote Compromise Vulnerability - (November 25, 2002)
- Multiple Remote Vulnerabilities in BIND4 and BIND8 - (November 12, 2002)
- Multiple Remote Vulnerabilities in Polycom Videoconferencing Products - (September 04, 2002)
- Remote Denial of Service Vulnerability in Oracle9i SQL\*NET - (August 13, 2002)
- Remote Buffer Overflow Vulnerability in Sun RPC - (July 31, 2002)
- Remote Buffer Overflow Vulnerability in Microsoft Exchange Server - (July 24, 2002)
- OpenSSH Remote Challenge Vulnerability - (June 26, 2002)
- Remote Compromise Vulnerability in Apache HTTP Server - (June 17, 2002)
- Remote Buffer Overflow Vulnerability in IRIX SNMP Daemon - (April 03, 2002)

**About Internet Security Systems, Inc. (ISS)**

Internet Security Systems, Inc. (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical information assets from an ever-changing spectrum of threats and misuse. Software from Internet Security Systems dynamically detects, prevents and responds to sophisticated threats to networks, servers and desktops. Services include 24/7 system monitoring, emergency response and access to the X-Force, Internet Security Systems' renowned research and development team. Headquartered in Atlanta, GA, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at [www.iss.net](http://www.iss.net) or call 888-901-7477.

Copyright © 2001 - 2002, Internet Security Systems, Inc.

All rights reserved worldwide. Internet Security Systems, the Internet Security Systems logo, AlertCon and X-Force are trademarks, and RealSecure a registered trademark, of Internet Security Systems, Inc. Other marks and trade names mentioned are the property of their owners, as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice. Permission is hereby granted for the electronic redistribution of this document. It is not to be edited or altered in any way without the express written consent of Internet Security Systems. If you wish to reprint the whole or any part of this document in any other medium excluding electronic media, please contact Internet Security Systems for permission. Disclaimer: The information within this paper may change without notice. Internet Security Systems provides this information on an AS IS basis, with NO warranties, implied or otherwise. Any use of this information is at the user's risk. In no event shall Internet Security Systems be held liable for any damages whatsoever arising out of or in connection with the use or dissemination of this information.