



Internet Risk Impact Summary

for March 26, 2002 through June 24, 2002

Table Of Contents

Executive Summary Internet Risk Summary for March 26, 2002 through June 24, 2002

- > Bottom Line
- > Outlook
- > AlertCon Risk Levels
- > Attack Activity Summary
 - Top Attack Ports
 - Top Attack Categories
- > Attack Sources
 - Top Five Countries
 - Internet Rogues
- > Top Attack Destination Ports
- > Destination Business Sectors
- > Ten Most Serious Risk Issues
- Discussion of Old and New Risk Elements
- > Hacktivism
- > Peer to Peer Networks and Instant Messaging
- > Risk Elements Added To AlertCon Baseline this Period
 - Vulnerabilities
 - Viruses/Worms
 - Nimda Worm
 - Cross Platform Worms
 - Klez Worm
 - MS SQL Worm

Executive Summary

Internet risk continued upwards throughout this reporting period. Internet Security Systems' assessment from the last report indicating that an unprotected computer will be compromised within a day of connection to the Internet remains accurate.

Overall, trends established through the previous report should continue throughout 2002. Traditional Internet threats such as viruses and Denial of Service (DoS) attacks remained at or above previous levels. Hybrid threats that combine virus payloads with multiple, automated attack scripts against common computer vulnerabilities remain the most significant online risk. This continued escalation makes the implementation of effective security practices an increasing necessity to ensure uninterrupted online business operations.

Although the possibility exists for increased "hacktivism"—politically motivated attacks—against IT infrastructures related to international crises or ongoing anti-terrorism actions, such behavior has remained at unexceptional levels. As the anniversary of September 11, 2001 nears, however, this situation may rapidly change with little or no warning.

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.

Internet Risk Summary for March 26 through June 24, 2002

Bottom Line

General Internet risk continues to rise. The risk components visible in this period are addressed below. Internet Security Systems defines Internet risk as the probability that attack or misuse may happen because a given system is connected to the Internet. Employee and end user education has emerged as a critical component of any successful security strategy. Programs as simple as employee bulletins and start-up screen notices can help raise awareness of how rapidly the threat environment evolves. No network is stronger than its weakest link, which means corporate due diligence has become increasingly dependent on the behavior of individual employees.

Outlook

Adding to the persistence of Nimda are other aggressive worms, including a small but steady resurgence of the year-old Code Red. The coming months are expected to bring new and more sophisticated hybrid threats designed specifically to evade traditional network perimeter and antivirus defenses. Overall, the outlook is for an upward risk trend to continue, in part because the sluggish economy encourages organizations to restrain spending on items without a rapid return on investment. Malicious attackers will take advantage of this spending gap to exploit under-protected systems until organizations realize that it is less expensive to be prepared than to recover from business interruption after the fact.

AlertCon Risk Levels

As this report went to press at the end of June, Internet Security Systems had observed 56 days at AlertCon 1, 22 days at AlertCon 2, and 7 days at AlertCon 3, and no time at AlertCon 4. There is significant potential for a recently publicized vulnerability in the default installation of OpenSSH on the OpenBSD operating system, and an associated exploit that gives rise to serious new risk potential for vulnerable systems using this widespread software platform.

OpenSSH is a free version of the SSH (Secure Shell) communications suite, and is used as a secure replacement of protocols such as Telnet, Rlogin, Rsh and ftp. A vulnerability exists within the challenge-response authentication mechanism in the OpenSSH daemon. It is possible for a remote attacker to trigger a buffer overflow that results in remote denial of service or complete

remote compromise. The OpenSSH daemon runs with superuser privilege, to this vulnerability potentially grants an attacker superuser status when successfully implemented.

Also of significance this period is the Internet Security Systems X-Force research organization's discovery of a serious vulnerability in the default version of Apache Web Server. Apache is used on over half of all Web servers on the Internet. It may be possible for remote attackers to exploit this vulnerability and modify Web content or bring down the server.

Many commercial Web Application Servers such as Oracle 9ias and IBM Websphere use Apache HTTP Server to process HTTP requests. Additional products that bundle Apache HTTP Server for Windows may also be affected. The hacker community is in possession of the attack tools to take advantage of this security weakness.

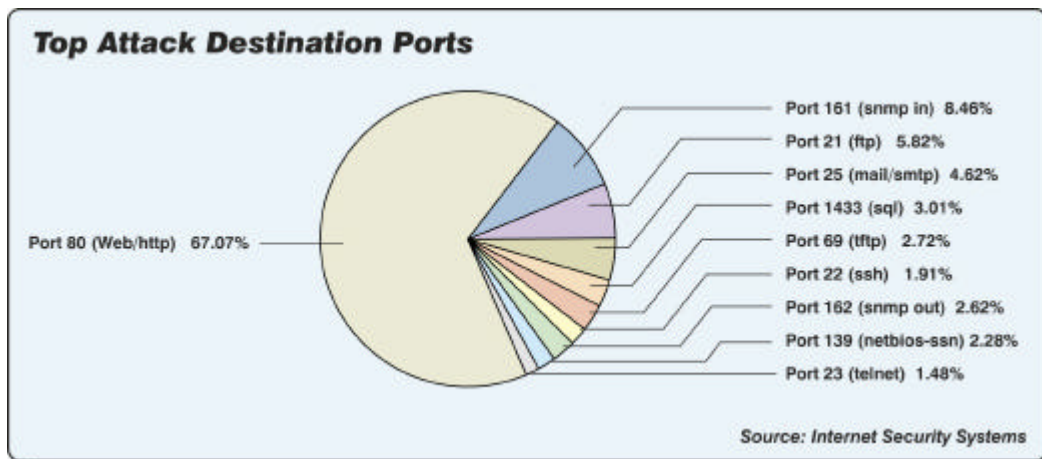
April was largely uneventful, with no major risk developments, 24 days at AlertCon 1 and only six days at AlertCon 2. Details can be seen at <https://gtoc.iss.net/graph.html>.

There was a small increase in risk noted in May. Two events caused temporary elevations to AlertCon 2 for a total of 6 days. A known exploit for the Microsoft IIS vulnerability was noted in the wild, and an SQL worm was released which automatically exploits SQL administrator accounts that do not have a password. Both of these episodes contained elements of imminent risk to the confidentiality and integrity of any systems vulnerable to those attacks.

June witnessed a significant rise in Internet risk components. Primary risks included a BIND vulnerability, and increasing attacks against IIS, SQL, and Apache installations. The risk to Apache Web servers constitutes the most serious security issue so far this year because it jeopardizes one of the most prevalent HTTP applications, and suggests that multiple open source applications may have been compromised by a single hacker group as far back as May 17th. At press time, June saw 7 days at AlertCon 1, 10 days at AlertCon 2, and 7 days at AlertCon 3.

Attack Activity Summary

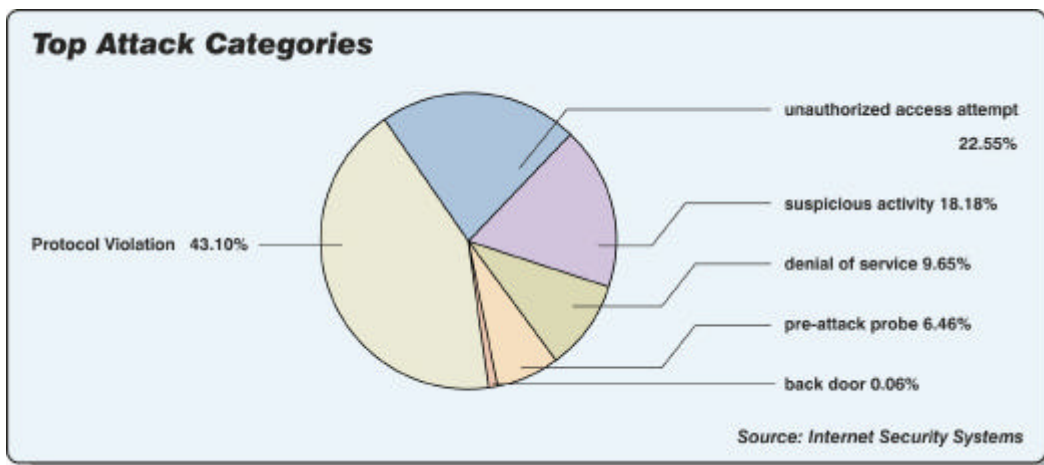
Internet Security Systems observed 21,982,672 alarms during this reporting period, resulting in almost 1,482 security incidents (defined as actual attacks or events containing elements of unusual risk).



As expected Port 80, the port used for all Web traffic, leads the list and is virtually unchanged from the previous report. With most firewalls and other access controls defaulting port 80 as open to all comers, this route provides the path of least resistance for malicious activity. This data indicates that firewalls deployed without supplemental technology are increasingly marginalized as a security device.

The only significant new port this period is 1433, which is associated with the recently announced SQL Worm that exploits administrator accounts missing a password. This is a good example of a known weakness being exploited by a worm that automatically seeks out the weakness and exploits it instantly. Internet Security Systems saw over half a million SQL worm events from over 7500 different sources during this period. Each one of these sources of the SQL Worm attack represents an infected host, which means that there were a large number of SQL database administrator accounts without a password.

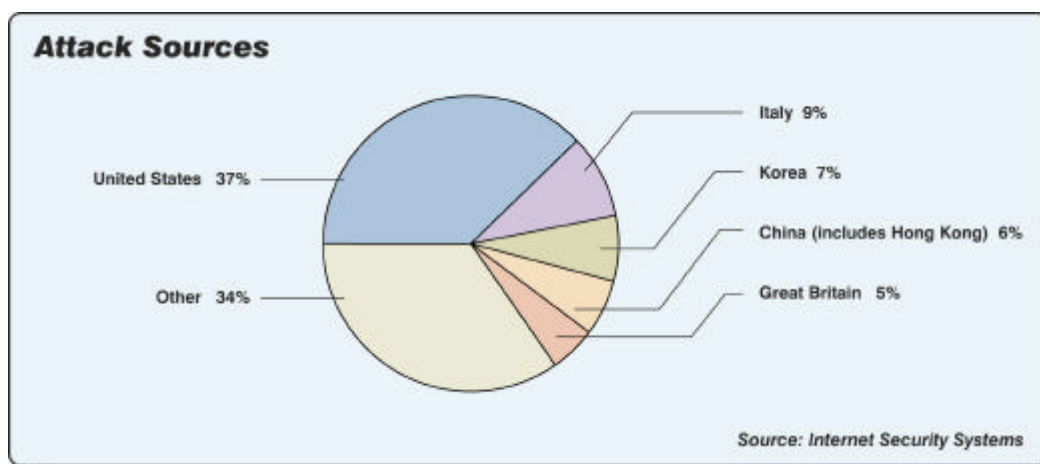
Also of note, this period recorded an increase in scans targeting networks running port 21(FTP), one of the oldest protocols and one of the most commonly exploited services on the Internet. Port 21 scans re-emphasize the X-Force recommendation that FTP be disabled unless explicitly required (http://www.iss.net/security_center/alerts/advise103.php).



The top three categories of attack are directly related to Nimda and other self-propagation hybrids exploiting multiple vulnerabilities across multiple desktops and servers with fast access to the Internet but little or no security. Denial of Service (DoS) attacks have been pushed into obscurity by the more prevalent hybrid worms, but they remain a real threat. As in the previous report, Internet Security Systems recommends a holistic strategy to protect across networks, servers and desktops to be fully prepared for both hybrids and DoS attacks.

Attack Sources

The top five source countries for attacks originating across the Internet, as recorded by Internet Security Systems' monitored and managed IDS customers during this reporting period were:



These five countries accounted for 64% of all serious security incidents. Surprisingly, only 48 of the roughly 150 countries currently online were associated with the serious attacks tracked during this period. This finding suggests that certain countries make attractive launching ramps for redirected attack, and may not always be the actual source.

The United States, the most Internet connected country in the world, is (not surprisingly) the source of most of the serious attacks monitored by Internet Security Systems. Attacks from these US-based networks and computers, real or camouflaged, represented a wide variety of attack types and business sectors. Italy was notable as the source for pre-attack reconnaissance against a broad range of business sectors. Attacks launched from China seemed focused on targeted exploits against Web resources across all business sectors, while attacks launched from Korea favored two approaches: pre-attack reconnaissance against financial sector targets, and exploitation of the SQL vulnerability in the IT sector. Rounding out the top 5, attacks launched from Great Britain showed a large percentage of reconnaissance against financial sector targets.

The remainder of the top ten source countries noted were Taiwan, Germany, Australia, Brazil, and Japan, in that order, all with less than 5% of the total each. Completing the top 20 countries, we noted Canada, The Netherlands, Russia, Austria, France, The Dominican Republic, India, Mexico, Spain, and Indonesia posting attacks around 1% of the total each.

Internet Rogues

Sources of hostile Internet activity may resolve to a registered owner of a particular 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 defensive 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.

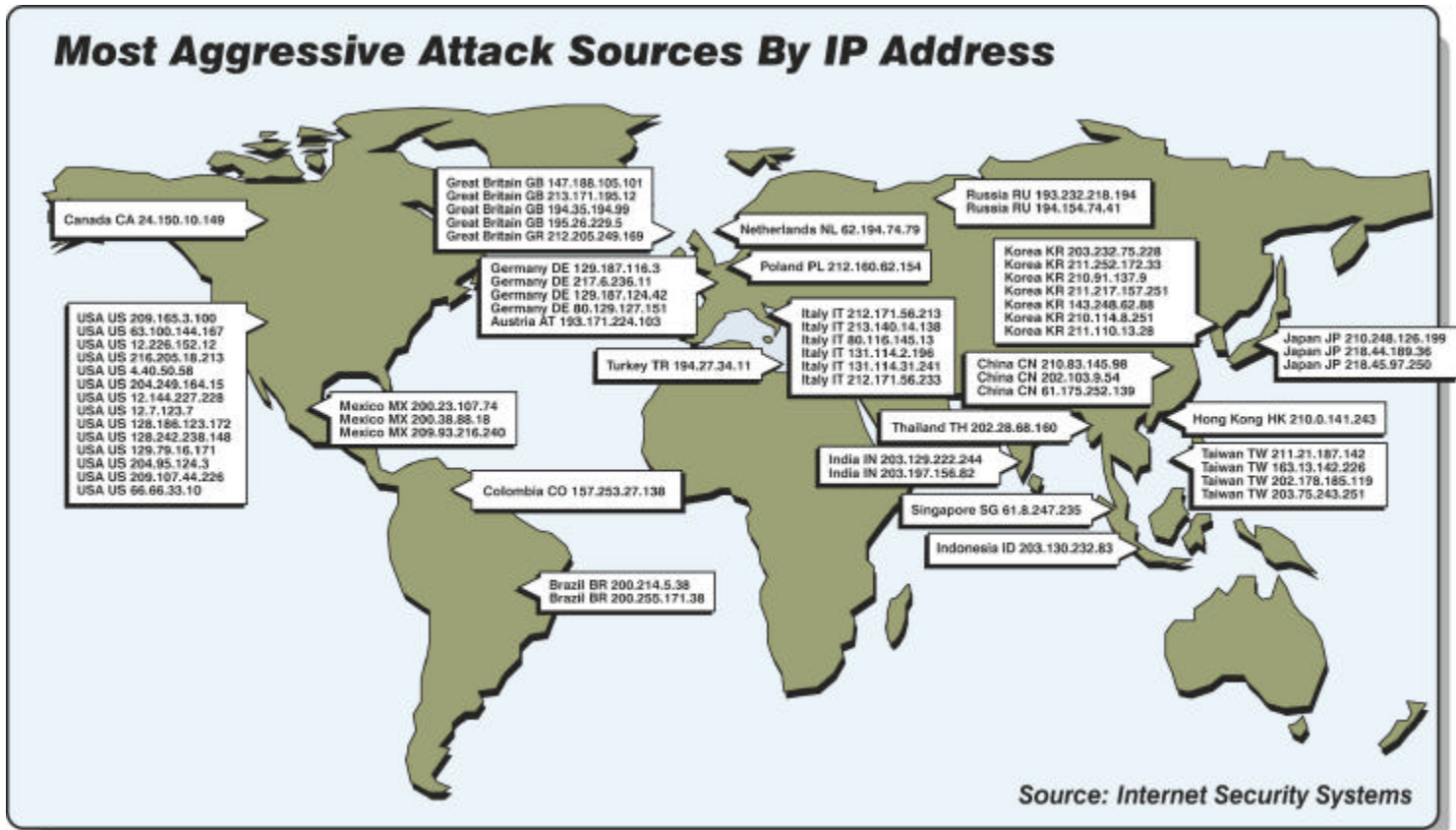
Identification of IP Address Ownership - Only official, publicly available lists are used to identify the registered owners of IP Addresses. This report will incorporate new official groups as they become available. The following organizations are among those used in the preparation of this report:

- 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.

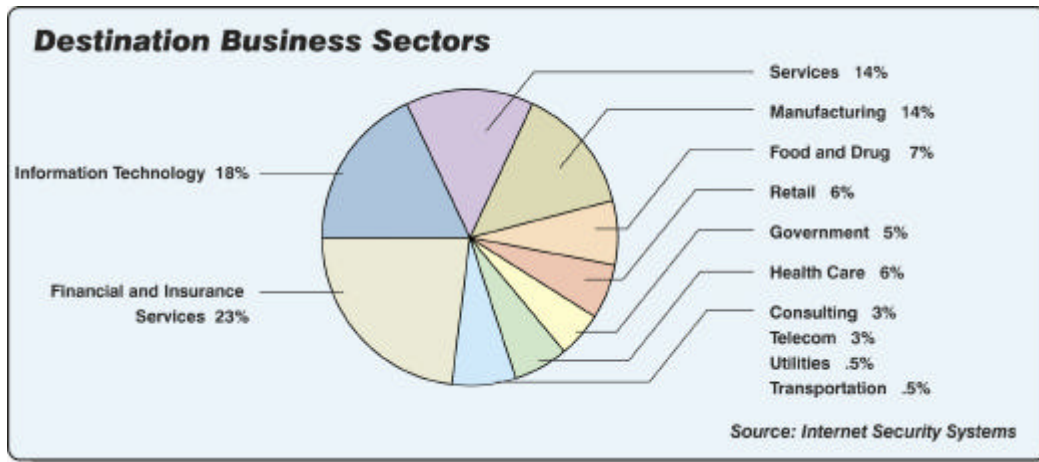
Duration - This list is published quarterly, and covers the previous quarter. Each list will be retained, along with the source data, for 3 years. However, the dynamic nature of the Internet makes it imperative to only publish three months' data at any given time.

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 who are unwitting participants in these exchanges. Anyone wishing to use this list as a reference for defensive IP blocking should take this 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 that session.



Destination Business Sectors

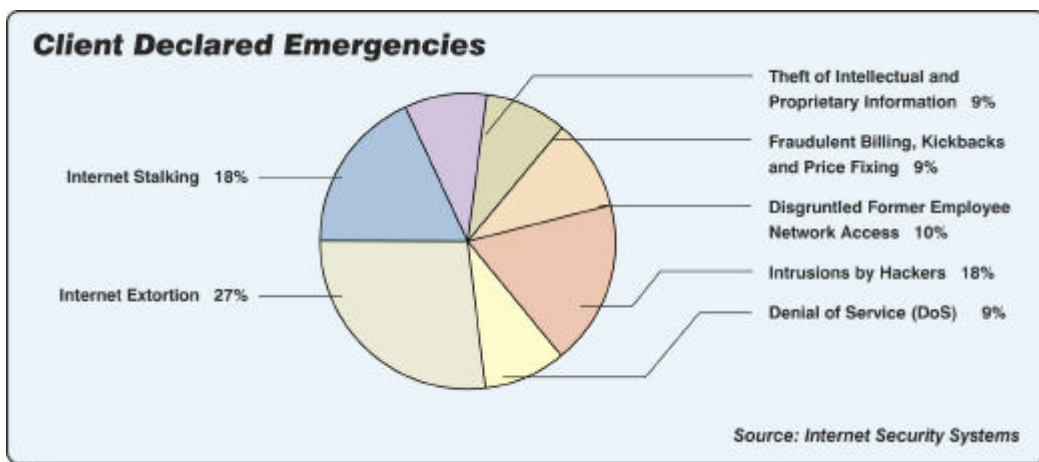
Industries targeted in this period include:



These numbers should be viewed with some caution since Internet Security Systems' client base does not broadly reflect 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. End result – a greater awareness of the need for online security plus a more prominent online presence make these sectors disproportionately represented in these statistics.

Internet Emergencies

X-Force Emergency Response and Forensics teams handled the following types of client-declared Internet Emergencies during this period. Client-declared emergencies arise from a variety of circumstances. Most do not begin via sensor activation. The emergencies noted below typically come to the surface after someone notices a network or data problem that cannot be explained by hardware or software glitches.



Discussion of Old and New Risk Elements

Hactivism

Hactivism has remained limited to the traditional groups in India/Pakistan, Israel/Palestinian Territories, the Balkans, Brazil, anti-World Economic Forum, and most recently, animal rights activists, with little effect on the general Internet population. According to the FBI, cyber-attacks on U.S. and Taiwanese computer networks by both Chinese military and students are possible in the last weeks of Q2 and in early Q3. Officials are concerned that the planned attacks are aimed at damaging and/or disrupting computer systems through the use of Internet hacking and computer viruses.

It seems reasonable to assume that, if the information in the warning is correct, it will constitute a test of some sort of attack script. Internet Security Systems was not informed if these attacks were to be exploitative in nature (goes after information or elevated privileges) or disruptive (denial of service).

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

Each node in a P2P network is both a client and a server, making the exploitation of a system that much easier. These machines are well suited for compromise by hybrid threats, as they are connected across the width and breadth of the Internet with many different vulnerable peers. Inasmuch as they continually transfer large files, they constitute a target-rich environment for miscreants. The programs are usually executed on desktops as opposed to servers and often contain sensitive information such as credit card numbers, files and passwords.

For example, Kazaa, a popular P2P file sharing network, boasts millions of users who are performing tens of millions of downloads a day. Few users realize that the files they are downloading are recursively sharing many other files on their computer. In other words, files which may contain sensitive personal data are nestled in amongst the MP3s.

The popularity of Instant Messaging and peer-to-peer networking technologies has risen dramatically in recent years. These services are prolific not only because of the instant communication that they provide, but the increased deployment of broadband has led to a rise in the availability of movies, music, and other media for download. As these services increasingly penetrate corporate networks, they need to be included as part of the overall online risk management process.

Many of these technologies were not designed to carry sensitive data in a corporate environment, and therefore do not have encryption or other security features. Software clients for certain chat networks are actually designed to help evade filtering and policy control. The three major instant messaging vendors (AOL, Yahoo! And Microsoft) all have noted problems with inadvertent privacy violations and well-publicized security holes. Other peer-to-peer clients such as Morpheus, KaZaa, and Gnutella clients have also been harnessed to distribute worms and malicious code.

Organizations may address the IM issue in many ways - block the technology entirely through firewall permissions or disable it on sensitive computers being simplest solutions (if not the most popular with employees). Internet Security Systems recommends blocking file transfer and gaming capabilities at the firewall. Personal IDS and firewall applications at the desktop level is another method of improving the security of Instant Messaging.

In addition to the issues noted above, Internet Security Systems has seen an increase in attack activity associated with underground file sharing. For more information on peer-to-peer networks and instant messaging, please consult the X-Force whitepaper, *Risk Exposure through Instant Messaging and Peer-To-Peer (P2P) Networks*, available at http://documents.iss.net/whitepapers/X-Force_P2P.pdf.

Risk Elements Added to AlertCon Baseline during This Reporting Period

Vulnerabilities

Internet Security Systems' X-Force recognized 610 new vulnerabilities in this period, a figure notable not just for the number of new vulnerabilities, but also for how often these vulnerabilities were exploited in the wild. Microsoft alone issued more than a dozen security bulletins this period. The most common theme of all these security vulnerabilities involves buffer overflows that can be easily exploited to gain unauthorized user access to networks. Exploitations that result in denial of service attacks were also noted.

A common flaw in Microsoft's popular database SQL Server enables an attacker to cause SQL Server services to fail, or allow unauthorized access to the SQL Server itself. As a result of this problem, Internet Security Systems saw an increase in the scanning of Port 1433 (SQL) across our managed networks.

The most serious risk issues for the period arose mid to late June. These were the vulnerabilities and associated exploits for Apache web server and OpenSSH.

X-Force has verified that Apache HTTP Server for Windows (Win32) version 1.3.24 as well as Apache version 1.3.24 for OpenBSD are vulnerable. It has been reported that exploit code has been developed for the following operating systems and platforms: Sun Solaris 6-8 (sparc/x86); FreeBSD 4.3-4.5 (x86); OpenBSD 2.6-3.1 (x86); and Linux (GNU) 2.4 (x86). Impact: These vulnerabilities may lead to modified Web content, denial of service, or further compromise. Apache accounts for over 63% of all active Web servers. The X-Force has released an advisory, <http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20524>, with patching instructions for the default setting of the Apache HTTP Server. This advisory requires immediate action on behalf of all system users with Apache HTTP Server.

X-Force has also discovered a serious vulnerability in the default installation of OpenSSH on the OpenBSD operating system. OpenSSH is a free version of the SSH (Secure Shell) communications suite and is used as a secure replacement for protocols such as Telnet, Rlogin, Rsh, and Ftp. OpenSSH employs end-to-end encryption (including all passwords) and is resistant to network monitoring, eavesdropping, and connection hijacking attacks. X-Force is aware of active exploit development for this vulnerability. Impact: OpenBSD, FreeBSD-Current, and other OpenSSH implementations may be vulnerable to a remote, superuser compromise. X-Force recommends that system administrators disable unused OpenSSH authentication mechanisms. For more information see <http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20584>.

Viruses/Worms

Internet Security Systems, X-Force recognized 134 new viruses in this reporting period.

Nimda Worm

Nimda continues to infect networks around the world. The tenacity of this hybrid threat is incredible. It has maintained its presence across the Internet since last September using at least five methods of propagation. It infects Web servers from infected client machines by scanning for IIS vulnerabilities, copies itself across open network shares, scans for back doors left behind by Code Red II and the "Sadmind" worm, it mails itself to others via the infected host's email program, and, finally, adds exploit code on Web pages of infected servers in order to infect those who browse the page. When a computer is infected, Nimda opens file sharing and establishes a guest account, in addition to using the computer as a launching ramp to infect more computers.

Internet Security Systems noted an average of 2223 hits an hour against our client sensor base during this period, as compared to 3500 per hour last report. This decrease is attributed to better clean-up efforts and more effective defenses leading to fewer infections in the corporate environment. Infected machines in small businesses and homes with fast Internet connections are assumed to continue to be the source of most ongoing Nimda attacks, because the bulk of the 59,697 different source IP Addresses for Nimda attacks resolve to Internet Service Providers.

For more information on viruses noted during this period: <https://gtoc.iss.net/viruses.php>

Cross Platform Worms

A Cross Platform Worm is a self-propagating and self-installing piece of malicious code that can infect more than one operating system. Most worms in the past have targeted single operating platforms, often variants of Microsoft Windows. These worms target many. A new virus called Simile.D may not be much of a threat to computer systems, but some of its technical tricks could lead to a rethinking of the principles underlying antivirus software. The program utilizes code that hides the virus, presence, plus also randomizes the program's size to make it harder to identify. The fourth, and most recent, variant of the virus can spread to both Windows and Linux operating systems, according to recent public analyses.

Klez Worm

Klez is an especially virulent family of worms that has been spreading across the Internet since October 2001. The Klez family currently contains nine variants with four distinct viral payloads. All Klez worms spread via email. They carry either no viral payload or one of four variants of the Elkern file-infecting virus. The Elkern virus is destructive and is triggered on certain dates to destroy data on all accessible drives, as well as disable antivirus software. Klez has the following characteristics:

- Contains file-infecting virus
- Disables antivirus software
- Logic bomb that is capable of destroying all files
- Automatically executes/infects a system when email is previewed
- Creates registry keys to continue running after reboot
- Starts itself as a service

- Spoofs its origins
- Attaches random files to outbound infected emails

For Additional Information on this threat go to: http://www.iss.net/security_center/static/8937.php

MS SQL Worm

Internet Security Systems continues to observe a strong presence of this worm. An analysis confirms that there are two separate worms with distinctively different data packages actively propagating via port 1433. The worm looks for any SQL database administrator account that has no password. Once a system is compromised it adds a temporary account to the local group administrator's list and then executes a Java Script using a third party email program which sends a password file and the victim's network configuration settings to an offshore e-mail forwarding service.

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, all 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 are a tremendous 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, and academia, and public media. These results are posted daily along with an AlertCon determination of Internet risk at www.iss.net, and are available via email alerts, and daily email risk notifications.

About Internet Security Systems (ISS)

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a pioneer and world leader in software and services that protect corporate and personal information from an ever-changing spectrum of online threats and misuse. Internet Security Systems is headquartered in Atlanta, GA, with 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 or call 888-901-7477.

Statistical data on Internet threat trends and risk analysis was generated primarily through information gathered at Internet Security Systems, five Security Operations Centers. These centers, located on three continents for global coverage, feed security intelligence into Internet Security Systems, Global Threat Operations Center (GTOC) on a 24/7 basis. Data is aggregated, anonymized, and analyzed by the Internet Security Systems X-Force research and development organization, and posted via the Internet Security Systems Web site at www.iss.net and through daily email risk notifications.

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. BlackICE is a licensed trademark of Network ICE Corporation, a wholly owned subsidiary 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.