Internet Risk Impact Summary
for December 22, 2001 through March 21, 2002

Executive Summary

Internet risk rose significantly in 2001, and continued upwards through the early months of 2002. While the traditional Internet threats such as viruses and Denial of Service (DoS) attacks remained at or above previous levels, especially virulent forms of hybrid threat that combine virus payloads with multiple, automated attack scripts against common computer vulnerabilities are now the most significant online risk.

The outlook is for this trend to continue throughout the first half of 2002. Hybrid threats require an energetic, multifaceted, defense. The key to protecting critical online information resources from attack or misuse remains strong security policy and procedure. This continued escalation makes the implementation of effective security practices an increasing necessity to ensure uninterrupted online business operations.

Copyright © 2001 - 2002, Internet Security Systems, Inc. All rights reserved worldwide.
Internet Risk Summary

Bottom Line
Internet risk is up since Fall 2001. Organizations that have assessed the effectiveness of their Internet risk countermeasures but have not improved network, server and desktop protection since the beginning of last quarter have fallen behind the threat curve, and have probably suffered some sort of exploitation.

Outlook
Internet risk will continue to increase as long as fundamental Internet risk factors are not lessened in some way. Software vulnerabilities and exploitations are announced almost daily, the hacker community is constantly improving its game, and physical threats, including terrorism, are always part of the equation. The software community, including developers, vendors and users, is beginning to raise the profile of security within the development process. Improvements, however, will take time. As a result, the medium and long term risk assessment for the Internet remains significantly less than optimistic, with hybrid threats continuing as the most dangerous form of attack or misuse.

AlertCon Risk Levels

AlertCon 1 - Internet risk baseline. It reflects the malicious, determined, global, 24/7 attacks experienced by all networks connected to the Internet. In simple terms, AlertCon 1 indicates the possibility that any system connected to the Internet is likely to be exploited within a day if it is using common software and has no protective measures in place.

AlertCon 2 - Increased vigilance. Internet activity has been detected indicating the potential for focused or patterned attacks. Some additional defensive action is required.

AlertCon 3 - Focused attacks. Unusually heavy Internet traffic indicates an obvious attempt to exploit specific vulnerabilities. Immediate defensive action is required.

AlertCon 4 - Concerted, ongoing attacks. A catastrophic security situation has arisen within a network or group of networks whose survival depends on immediate, focused defensive action. This condition may be imminent or ongoing.

In practical terms, this risk profile means that a completely unprotected device is likely to be compromised in less than a day after connecting it to the Internet.

Attack Activity
The Nimda worm has become a dominant, expensive and enduring threat. Many corporate networks, of all sizes, suffered significant down time for Nimda cleanup because organizations underestimated their exposure to this threat and did not meet it with a credible, multi-layered defense.
Over time, Nimda has proven to be the most visible of the new hybrid worms that self-propagate, self-activate and attack multiple vulnerabilities. The damage comes both through a virtual Denial of Service situation because of the hybrid's mass propagation algorithm and through malicious activity that opens desktop files to sharing, and creates guest accounts on networks.

The lowest attack rate for Nimda at the Internet Security Systems Global Threat Operations Center was 600 an hour and the high was 8,000 and hour, with the average hitting around 3,500. These rates of attack remain ongoing and consistent. Overall, hybrid threats were monitored at an average of 3500 per hour, accounting for approximately 7,665,000 attacks over the duration of the quarter.

Before the introduction of the hybrid threat in the summer of 2001, Denial of Service activity dominated all attack statistics. While DoS numbers have not gone down, they are now pressed into graphical insignificance by the activity of the hybrid worms, but remain no less important as a threat. Automated pre-attack probes are another attack type of real concern. This cyber reconnaissance activity is very visible to anyone running intrusion detection sensors, but hard to detect any other way.

Pre-attack reconnaissance (discussed in greater depth in the Attack Sources section below) also accounts for a significant amount of alarm activity, second only to hybrid threats. Vulnerabilities associated with port 21 (file transfer protocol) and port 22 (ssh remote login protocol) were two of the most prevalent reconnaissance targets. Software vulnerabilities also remain high on the target list for automated and individual reconnaissance. The statistics that follow reflect how hybrid threats and network pre-attack reconnaissance account for over 80% of detected attacks, with the first three categories reflecting these two malicious activities.

![Pie chart showing attack sources]

**Attack Sources**

Rogue Internet attack sources are an inescapable part of the Internet landscape. The only sound defensive approach is to adopt a strategy that balances operational needs with sensible restrictions on inbound traffic. Unless rogue traffic is coming from inside an organization's own network, it is nearly impossible to identify the actual source. For example, much rogue traffic is launched from a network already compromised by rogue activity.
Internet Security Systems tracks potential rogues through a variety of Internet information resources (see Sources Of Information, below) to identify the source of the attacks that are confirmed as suspicious activity. These addresses are added to a watch list to enable historical traffic analysis and to assess ongoing impact on client networks.

Backtracing rogue activity can provide at least partial information about the source of the attack. A popular (and free) look-up/identification service is run by the American Registry of Internet Numbers (ARIN). Enter any IP address to find out to whom it is registered. The URL is http://www.arin.net/whois/index.html.

Even if the source can be identified, it is difficult to identify the person behind the rogue activity. In other words, there is no simple method to prove a specific individual is using any given computer at any given point in time. The most effective means to control an attack at the source is to hold the identified network responsible, even if it isn’t the originating source of an attack, and block access to and from those Internet addresses.

Rogue activity was noted from every country with Internet connectivity, but certain patterns present themselves. As described above, these behaviors may show actual attack sources, or merely the final launch point in a longer chain. Some examples of rogue activity from the last several months include an elementary school in Korea, a rented computer from an Internet cafe in New England, a teachers’ university in China and numerous other academic institutions around the world. Not surprisingly, the most automated and Internet-connected countries or regions are the sources of most rogue attacks, including the United States, China, and Europe.

Destination Ports
Attackers follow the paths of least resistance. They use the most open avenues of approach into networks, the most open of all being traditionally port 80, dedicated to Web traffic. Nearly 70% of all attacks in Winter 2002 exploited port 80. While most network operators shy away from inhibiting port 80 traffic, there are effective strategies to minimize exposure. For example, file servers should not offer Web services, and vice versa. Likewise, organizations should limit access to authorized networks or individuals, when this is practicable. Since almost 70% of malicious activity occurs as a result of entry through port 80, it is obvious and imperative that firewalls should be augmented with additional intrusion and defense technology, since firewalls can not prevent this form of unauthorized access in their own right.
Hourly Breakout
The hourly distribution chart below reflects how pervasive automated scripts continue to accelerate the trend towards ever-present, 24/7 attack behavior. These computer-driven attacks execute their commands according to preprogrammed code, rather than requiring operator intervention. Net result - attacks are now global in scope and round-the-clock in incidence. As a result, defensive measures must also be available 24/7 to prevent or limit interruption of online business operations.

2001 Internet Risk Summary

Because this is Internet Security Systems’ first seasonal report, the following is a review of events impacting Internet Risk in 2001. Internet risk was high overall in 2001, and general trends indicate it is getting worse. Internet Security Systems noted 830 million alarm events and dealt with 2,185 security Incidents covering an extremely broad range of possible attack activity in 2001. Internet Security Systems began making formal AlertCon assessments of the Internet threat on May 1, 2001. We spent 52% of the remainder of the year at levels higher than AlertCon 1. Simply stated, the attacks are real, and we do not see the situation getting better.

The events of 9/11 had no apparent effect on malicious Internet activity, but interest in security was up. Thus far, there have been no cyber attacks we can relate directly to the physical attacks of September 11. The real message of September 11 for IT staff and online business operations is that physical threats remain serious, and no cyber security program can be complete without effective business continuity and business recovery plans that consider both cyber and physical risks equally.

2001 saw the introduction of the hybrid threat, a dangerous new escalation in automated attack technology that frequently circumvents antivirus and firewall defenses by exploiting multiple vulnerabilities in email, Web, chat, file transfer and similar popular applications. By definition, these worms self-install and self-propagate. They have caused a significant, permanent rise in the overall number of attacks. In practical terms, a dynamic, proactive defense that combines antivirus, firewall and intrusion detection, coupled with strong policies and procedures and a strict regime of software updates and security patching should now be standard practice. The best publicized hybrids were Code Red in July and August, and Code Blue and Nimda in September.
Poorly administered networks are poorly secured. Because risk is high and getting worse, failure to adequately resource network operations and security invites embarrassing questions about confidentiality, integrity, and availability within business networks. Educating users and administrators is paramount if organizations are to have a credible defense against Internet threats.

Home users and small office users, and their ISPs, are now a significant part of the overall threat equation. The rise of computer power and high speed Internet access have introduced a user population not resourced or trained to properly administer or secure their computers. Hybrid threats count on unsecured home, remote or mobile systems to help penetrate the corporate perimeter. We saw this problem manifest itself when the hybrid worms hit in the middle of 2001. We saw it again in late December and early January, perhaps as a result of new computers given as Christmas presents coming on line. These systems generally shipped with months-old, unpatched operating systems and outdated antivirus software. As a result, they were easily infected with Nimda without the knowledge of their owners.

Discussion Of New Threats

Hybrid Threats
Hybrid threats are advanced, automated, attack programs that self-propagate and leverage both virus techniques and intruder exploits. Other names for hybrid threats are blended threats, hydra attacks, and advanced worms. Older forms of threats could be met with a single defensive solution. The hybrid, with its multiple attack strategies, must be met with matching, multi-layered defensive solutions. These solutions are not trivial and demand focused attention by network operations and security staffs, and by individual computer users.

Because the new hybrids look and act like viruses, at some stage of their lives, antivirus solutions can stop some hybrids. However, the majority of the focus to date has been detecting and stopping passive viruses via email. Hybrid threats also propagate through additional methods like peer-to-peer (P2P) chat systems, and by active intruder exploit techniques. Antivirus does not address these methods. Additionally, antivirus cleanup focuses on removing email attachments. This tactic does not work in the hybrid environment because hybrid threats install backdoors, apply new vulnerabilities and modify the system.

Another popular misconception is that “the firewall does it all” for network security. Although firewalls remain a critical front-line defensive component, this false assertion is particularly dangerous for hybrid threats. We noted above that some 70% of all malicious traffic comes in via port 80, which is commonly left wide open in firewalls because so much business is done via the Web protocol. In other words, if you can do business through it, you can do malicious business through it. Access control lists on gateway and internal routers are effective ways to limit traffic and thereby mitigate risks but this solution can be resource intensive to manage. As with antivirus, firewalls form only part of the solution.

Virtual Private Networks (VPNs) are also vulnerable to a hybrid threat attack. VPNs ensure that the data streams from remote, telecommuter and mobile systems have been safely encrypted.
However, systems that have been compromised by a hybrid threat are still regarded as trusted by the corporate network. In other words, malicious traffic from the hybrid will itself by encrypted and safely transmitted inside the corporate perimeter, where it is less likely to encounter an active defense.

Intrusion Detection Systems (IDS) are extremely effective at identifying intruders via either active or passive attack techniques. As a result, IDS can actually detect hybrid threats due to hybrids’ use of known vulnerabilities and exploit techniques. Code Red, for example, was propagated by a well-known Web server exploit detectable by IDS months before Code Red itself was ever released. IDS have played an important role in tracking new hybrid threats and helping companies identify which machines are infected. IDS’ weakness is an inability to clean up an active infection, and a limited ability to prevent the malicious activity from starting in the first place.

Vulnerability assessment technology is a proactive measure that provides a detailed report of potential security exposures for network and system administrators to correct. Unfortunately, many organizations do not have the staff, resources or process to develop an institutionalized standard for routine scans and remediation. Hybrid threats rely on a significant time lapse between vulnerability assessments and remediation to locate and infect systems.

Hybrid threats are not invincible. Their emergence means that the stakes are higher and the game is played faster, but cost-effective, dynamic protection is already a reality for many organizations. Protection against hybrid threats is an ongoing process that combines best practices, skilled people and best-of-breed products covering a range of security technologies. All layers of the IT infrastructure – networks, servers, desktops, gateways and applications – require defense against hybrid threats. Across all these layers, vulnerabilities should be identified, prioritized and fixed (audit). Deploying and operating real-time defenses in a coordinated way using emergency response services to block and/or contain the threat is also a key tactic. Any in-depth strategy must also include remote and mobile access. In other words, successfully fending off the hybrid in real-time requires a comprehensive, technical solution. For more information on how to combat hybrid threats, please download the free whitepaper, “Response Strategies For Hybrid Threats,” available with other Internet Security Systems whitepapers at http://www.iss.net/support/documentation/otherwhitepapers.php.
Threats Added To AlertCon Baseline During Winter 2002

Viruses
• Internet Security Systems tracked 112 new viruses of concern to client networks. Antivirus protection remains critical, and it must be updated throughout the enterprise whenever a vendor publishes an antivirus signature update.

• Many viruses that spread via email now utilize social engineering to lure in unsuspecting victims via compelling catch phrases intended to stimulate interest in opening the attachment. Opening the attachment then launches the viral payload. An example of the many out there this season was the My Party virus with email subject lines: “New photos from my party!” and “Predictions for 2002”.

Vulnerabilities and Exploitations
• The Internet Security Systems X-Force™ research organization reported 537 significant new vulnerabilities during this quarter.

• A Finnish university published an exploit for a vulnerability in SNMP version 1 (Simple Network Management Protocol). This attack tool is actively circulating in the computer underground. The exploit is significant because it affects the most common management protocol on the Internet. Nearly every operating system, router, switch, cable or DSL modem and firewall is shipped with an SNMP service and Internet Security Systems estimates that 95% of these are running SNMP v1. The exploitation causes these managed devices to crash.

• X-Force verified that an exploit for a PHP (Popular Hypertext Preprocessor) vulnerability was circulating among various hacker groups. This is serious because PHP is a common scripting language used heavily throughout the Internet for Web applications. The exploitation allows outsiders access to the host network.

• The hacker underground released the exploit code for a serious vulnerability in a login function for a large number of Unix based operating systems. This vulnerability allows remote attackers to execute arbitrary commands on a target system with super-user privileges.

• An easily exploitable vulnerability in America On-Line’s Instant Messenger (AIM) could allow remote attackers to execute arbitrary commands on a victim’s system. As a matter of course, Internet Security Systems advises that users disable all types of instant messaging where there is no demonstrated need for it because so many of these applications are vulnerable to exploitation and are so popular within the hacker community.

• Attackers may gain complete control of a remote system through a successful exploitation of a vulnerability in the Common Desktop Environment (CDE), used in many Unix systems. This exploit has been seen widely across the Internet.
Miscellaneous
• Microsoft announced five vulnerabilities that were covered by a cumulative security patch. The key here of course is that until the patch is actually installed on all affected systems they remain vulnerable to such well-publicized methods of exploitation.

• A vulnerability was found in the Symantec LiveUpdate feature that allows attackers to see authentication data in the clear because the information is stored in the accessible Windows registry.

• Cisco announced a vulnerability in Cisco Catalyst switches, Series 4000, 5000, 6000 and 2948G and 2900. Cisco warned that attackers have already exploited this vulnerability.

• A vulnerability was found in Internet Security Systems’ BlackICE™ Defender and BlackICE™ Agent products, as well as RealSecure™ Server Sensor installations, that could allow a denial of service attack on Windows 2000 or Windows XP. Patches were released to cover these vulnerabilities.

Sources Of Information
Internet Security Systems monitors over 350 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 over 400 managed firewalls monitored at the SOCs, 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 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.