

IBM Internet Security Systems
Ahead of the threat.™



**The Evolving Threat:
Combat training for the new era of malicious code**

Contents	
1	<i>The Evolutionary Leap within the Threat Landscape</i>
2	<i>Is Your Existing Security Adequate?</i>
4	<i>Meet Your New Enemies</i>
8	<i>Evolving Threats in the Future</i>
9	<i>How to Protect Against the Evolving Threat</i>
11	<i>IBM Internet Security Systems (ISS) Protection Platform to Stop Evolving Threats</i>
12	<i>Service-based Protection Against the Evolving Threat</i>
13	<i>Learn More About Preventing Evolving Threats</i>
14	<i>The Evolving Threat Quick Reference Glossary</i>

The Evolutionary Leap within the Threat Landscape

Beginning in 2005, methods for executing Internet attacks have been quietly evolving. The shift has remained subtle to date, but enterprises that ignore newer attack methods may experience significant losses. Hackers' motivation for launching attacks has changed, causing the current threat evolution. Today attacks are profit driven, not glory and fame. The more organized attempts for financial gain are harnessing intellectual talent within the hacker community to devise new attack strategies and innovative malicious code (malcode) that invades enterprises systems without detection.

Information security solutions used to protect organizations from hackers intending to generate front page news about a successful denial of service attack or a web site defacement. In the new era of Internet threats, attackers are motivated by profit or politics and use cutting edge technology to probe networks undetected for as long as possible. The longer attacks go unnoticed, the more opportunity for success in data theft and other profit-generating activities.

Figure A illustrates how today's attacks are different from earlier attacks over the last couple of decades.

Figure A

Attack Characteristics	Earlier Attacks	New Era Attacks
Motivation	Glory and fame	Profits
Complexity	One dimensional	Multi faceted attack
Scope	Widespread for maximum publicity (carpet bombing or shotgun approach)	Targeted attacks to go unnoticed (surgical strikes or sniper approach)
Primary Risk	Network downtime to clean and repair	Direct financial loss; Theft of trade secrets or corporate strategy; Customer data breaches and disclosure
Targets of Attack	High profile / Widespread	Laser focus on firms or individuals
Effective Defense	AV Signatures; Reactive approach	Multi layer protection; Pre-emptive and behavioral approach required
Recovery	Scan and Remove	Not always possible; may require re-image of system
Types of Attacks	Virus, Worms, Spyware	Designer Malware, Root kits, Ransomware, Spear Phishing
Attack Approach	Network Traffic – Tell everyone the threat is here	Malicious Code – Stealth like operation to avoid discovery

Organizations should now be examining the adequacy of their existing security platforms in the face of new, profit-driven attacks. This whitepaper will provide further detail on new evolving threats using malicious code – an area where many firms have unprecedented levels of exposure and risk.

Is Your Existing Security Adequate?

The malicious code used in modern attacks has more devastating consequences than the headline-making worms and viruses of the previous era. Many existing protection systems are inadequately prepared to stop new forms of malicious code. Largely signature-based, these legacy security products rely on known attack signatures. When one of these attack signatures is recognized the older security systems sound an alarm and may attempt to block the attack. Signature-based protection can only prevent known attacks however. Hackers recognized the weakness of a signature-based defense and began to develop new zero-day attacks.

The question that security officers and directors need to be asking is: Can my existing platform protect against the latest evolution of innovative malicious code?

Can my existing platform protect against the latest evolution of innovative malicious code?

Modern Attacks Surpass Traditional Security Technology

Twenty years ago, signature anti-virus (AV) systems were able to successfully defend against malicious attacks the vast majority of the time. And for more than two decades, AV software did a good job of protecting against virus outbreaks. However, malicious code today is characterized quite differently from the viruses of the past. A virus is defined as *self-replicating code*, often designed to damage or shut down a network. The malicious code used today is low profile, highly targeted, and may or may not replicate. Attackers design new malcode to avoid detection by legacy AV software. Modern attacks penetrate legacy signature-based protection systems using multi-faceted techniques designed to compromise systems for profit.

Threats and Protection – First 20 Years



New Era Threats with Legacy Defense



For the past 20 years, signature AV systems protected enterprises from most attacks. However, threats today are more heavily armed, multi-faceted, and can be deployed more strategically to bypass legacy protection systems.

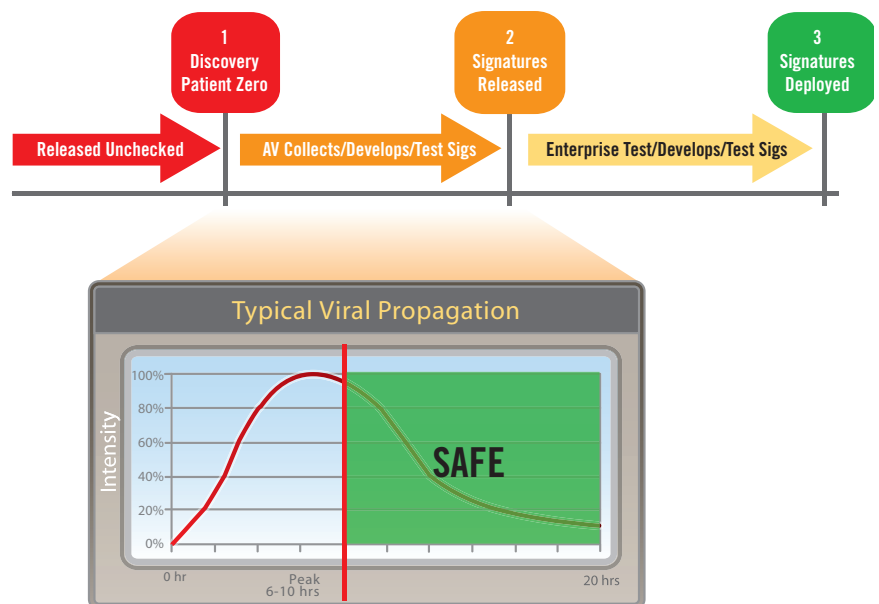
The Traditional Protection Process

Innovative hackers first examined how traditional security solutions worked to develop new malware that would exploit blind spots. Consider a virus outbreak for example. As a virus propagates, the virus signature process moves through three development stages:

1. Discovery
2. Signature development and release
3. Signature deployment

In the first step of an attack, a new self-replicating virus finds its way to the network and begins to execute. Since these attacks were designed to generate highly visible network issues, viruses were usually discovered quickly.

AV Signature Lifecycle



Upon discovery of a virus, AV software vendors would move into the next phase – signature development and release. They would design a signature that protects against further outbreaks. Once the signature development was complete, signature deployment occurred to push the protection update out to customers. While the process is methodical, the development and deployment stages could last hours and even days – leaving enterprises vulnerable in the meantime. In addition to the AV software vendor response time, the enterprise is faced with added deployment time to fully test and deploy a new signature. The impact and spread of a particular virus often drives the speed of the signature development and deployment process.

Malicious Code Undermines Traditional Signature Lifecycle

Today's threats are designed to undermine traditional security systems as well as the networks and data they protect. First, malware that can delay or avoid discovery foils the entire process. By using stealth and precision, malicious code often avoids the first prioritization criteria used by most AV software vendors, since it does not infect a large number of systems. Bypassing or delaying the AV discovery stage delivers a crippling blow to the outdated defense strategy of signature AV.

Second, hackers are actively leveraging technology to create variations of multi-faceted attacks. The more complex attacks combine several malicious techniques, including designer malware, ransomware, root kits, and Trojans. Multi-faceted attacks improve the chances of bypassing an existing protection system and remaining unnoticed. Each evolving threat has a unique approach or attribute that can increase enterprise risk. In order to reduce risk of successful malware attacks, security officers should know the enemy. Security professionals must understand the key attributes, characteristics, and potential deployment scenarios of modern attacks to shore up their defenses.

Meet Your New Enemies



Designer Malware: A piece of malware written to infect or compromise either one or a small number of organizations with similar profiles. For example, designer malware can be a Trojan written specifically for a single bank.

Threats using designer malware are very targeted and specific. Targeted attacks and designer malware take a laser-focused approach on which organization to infect, and at the most simplistic level may target a single company or user population. In the past, AV vendors would always prioritize threats by the "total number of infected systems." As a more targeted attack mode, designer malware takes advantage of the old view of risk and flies under the radar of AV systems.

It is possible to develop AV signatures for designer attacks. However, attackers have come to understand the traditional responses to virus outbreaks and have crafted attacks that carefully avoid the trigger points that start the typical response. When the attack doesn't propagate beyond a small user community, it greatly decreases its chance of being detected at all.

Although most modern hackers eschew headlines in favor of profits, designer malware is responsible for several notable attacks. In Israel, a Trojan attack was used to conduct industrial espionage and remained undetected for 18 months. This attack directly mirrors the trend of new attacks to fly under the radar of existing protection and steal data for as long as possible before being found. In the Israeli incident, intellectual property was stolen during 18 months of infection.

With millions of dollars invested in proprietary research, the biotech industry is a prime target of designer malware. Imagine the value of stealing the recipe for the next wonder drug. Two biotech firms were infected with designer malware specifically targeted to steal research secrets for new projects. Designer malware has the potential to steal research findings and trade secrets – undetected and in a relatively short period of time.



Spear Phishing: Spear phishing is a combination of phishing and social engineering that targets a single person or a single group of people. Spear phishing is hyper-focused to lend added credibility to the attack.

Spear phishing combines the standard phishing attack with additional social engineering techniques to build super targeted attacks. Spear phishing is used heavily in state sponsored attacks and attacks against financial institutions. The attacker leverages personal or public information about individuals to customize an email which appears to come from a legitimate source and tricks people into responding with personal information such as usernames and passwords. In a sample spear phishing scenario, John Smith's name and professional contact information is published in an industry magazine based on his recent promotion. A spear phishing attacker leverages Smith's information to send a spoofed, but official-looking, e-mail to Smith posing as a professional service and requesting that he activate his new, complimentary account. In responding, Smith inadvertently allows the attacker to install a Trojan or backdoor on his computer. Or, Smith simply provides his personal username and password, which may be the same for his private online banking account.



Ransomware: Ransomware is malware that packs important files into an encrypted archive and deletes the original files thereby making access impossible unless a ransom is paid. More advanced ransomware scenarios now leverage multiple forms of end user manipulation and extortion.

Ransomware is a growing and significant trend dealing with data, file, and end user manipulation. With Ransomware, attackers encrypt a user's documents and force the user to pay a ransom to gain access to the files again. Only after paying the 'ransom' will the user be given the password to unlock the files. Typically, users will pay the ransom by going to a Web site devised by the hacker and making a 'purchase' of some high-priced product.

Ransomware attacks also employ fear and embarrassment by telling victims the ransomware was caused by visiting inappropriate Web sites or from storing pornography on their computers. Whether these accusations are true or false, such ransomware tactics can prevent end users from working with security teams to cure the problem. New threats like ransomware employ technology as well as engaging the user, which escalates damage beyond traditional Internet worm outbreaks.

Certain ransomware uses stealth tactics that cause code to self destruct after encrypting a user's files. This makes unlocking the files even more difficult without dealing with the attacker.



Root kits: With the ability to make malware completely invisible to operating system (OS) and AV signature scans, root kits can be combined with multiple types of malicious code to enter enterprise systems undetected and launch multifaceted attacks.

The root kit is one of the most significant threats in practice today due to its stealthy nature and its ability to work with other malware. Root kits help make malware invisible to signature AV scans. A root kit is simply a shielding technology that can be used by any type of malware. By insinuating itself into the operating system of the compromised system, it can effectively prevent detection of whatever elements of the attack it wants to hide. Basic requests like asking for a list of all files in a directory may be unreliable since the root kit may hide files in the directory. Dealing with root kits can be a little like a game of hide-and-seek. If you

watch the person hide, you have a much better chance of finding him. If the person hides and you did not see where, you may never find the person. Using behavior-based protection technology can help to identify root kits before they can establish themselves. After the root kit hides, it may be too late and damage could be irreversible.

Many firms will attempt to clean up the root kit after infection. However, best practices suggest that re-imaging is preferable to restoring the system. Even if the time is taken to restore the system, the real damage to the enterprise has already been done. If the root kit enabled the theft of strategic corporate data or intellectual property, the enterprise cannot retrieve information that becomes public or is revealed to their competition.



Trojan: Trojans are very old threats now returning to the forefront. A Trojan is a piece of code that uses “trickery” to get people to run it for a different purpose, but in reality the code may perform key logging or password stealing activities.

Now that the motives driving today's threats have shifted to profit, Trojans are becoming more and more significant. As of 2006, Trojans became the vast majority of malicious code at 75 percent. Stealth like Trojans may not replicate and are intended to help steal data or gain access to systems for future exploitation. Examples include keyloggers and password stealers that will enable financial profit through inappropriate access to accounts.

Most AV signature software is only slightly effective in the detection of Trojans since the focus of AV signatures is to detect replicating malware. Without reliable behavior-based methods to detect Trojans, organizations such as financial institutions are at risk.

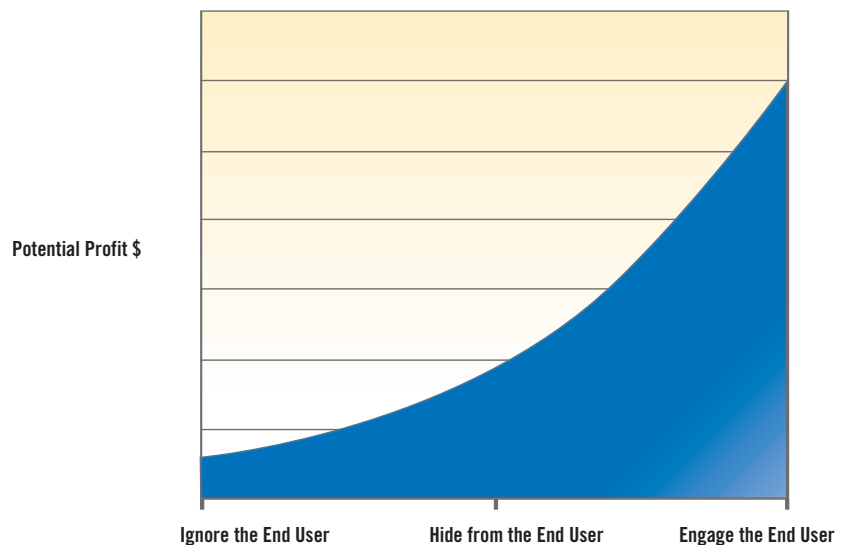
The crisis with Brazilian bank fraud gangs is a prime example of new Trojans at work. The Brazilian banking industry is facing rampant attacks by hackers using custom Trojans to empty customer bank accounts. Common attacks combine phishing scams to place a Trojan on end user computers. Once infected with the Trojan, the malicious code can monitor when users visit a bank site and either display a fake login page or capture bank login information. The key innovation of modern Trojans is that they utilize legitimate web sites. In many cases, users may not be tricked into giving up information on a fake site. Rather, the Trojan can steal authentication information when the user visits the genuine financial institution site.

Brazilian banks were only able to detect that a new custom Trojan had been placed on their systems after a customer reported the fraud. Once the specific problem is detected, a new signature could be developed from an AV vendor. However, when another custom Trojan is built and used again, the existing signature would fail since the new threat is not a known signature. In this scenario, the Trojan is also known as designer malware.

Evolving Threats in the Future

The game has changed – threats continue to evolve and motivations to create new threats have shifted from glory to profit. If unprepared for the innovative new threats, organizations and their users will be exploited.

Threats are no longer simple – most attacks now combine multiple threats and if you are not prepared to cover the full spectrum you will be impacted. Using only systems like legacy signature scanning will not be able to protect and defend against the majority of new attacks. Organizations that focus only on known threats will be at risk as attackers continue to innovate and design malware to bypass older protection technology and current AV signature scans. While the actual threat technology has evolved, the application of how malware is used to influence victims is also rapidly evolving.



Older attacks would ignore the end users and attempt to get fame and glory by causing widespread downtime. Gradually, attacks began to hide from users as the opportunity for profit was discovered. Today, creative deployment of malicious code can engage the user for the greatest financial profit opportunity.

The Satan virus is an example of malicious code deployed creatively to generate profit. In a report, the University of Cambridge reported that the Satan virus uses deeper interaction with users to keep the virus alive and increase potential profits.

The Satan Virus

At a high level, the Satan virus user interaction plays off human emotions. First, the attacker will convince a user of a perceived advantage or benefit the user may gain if the virus is executed. As an example, the virus may offer an employee the ability to view documents or e-mails from his boss. If the employee accepts the offer and deploys the virus, he may indeed gain access to his boss's e-mails or documents.

Over time, the virus records how many of the emails or documents the employee is viewing and later uses that information to blackmail the employee. Unless the employee keeps the virus alive, the employee may be exposed and risk the consequences of his actions. Since this started as a very targeted virus, the attacker may use blackmail to spread the virus vs. extracting immediate profit. The employee could be asked to target additional employees for the same purpose, thereby increasing the potential for blackmail profits.






















































How to Protect Against the Evolving Threat

Given the advances in technology and the ways threats are being deployed, enterprise systems must use layers of protection to mitigate the risk of attacks from profiteering hackers. With the increasing number of multifaceted attacks, the odds are one facet will eventually succeed unless you are prepared.

Figure B highlights the conceptual levels of protection that are provided against each type of threat using a defending technology. Each defending technology is designed to safeguard against certain types of threats, but can also offer additional protection across threat types in certain situations.

For a general understanding of capabilities, the chart rates three levels of protection:

Figure B




		 Full Protection	 Partial Protection	 Less Protection or not used as primary threat protection product							
		         									
Defending Technology											
Signature AV								 *			
Virus Prevention System (VPS)											
Anti-Spyware											
Content Filtering											

Historically, the signature AV providers have been successful at preventing the spread of most attacks once a signature is developed. The focus of signature AV technology makes it effective against a virus, worm and bot. Signature AV is only moderately effective against Trojans. In fact, most AV product certifications do not test AV scanners for Trojan detection that could identify designer threats. Security departments should confirm the level of protection they are actually receiving against designer malware or custom Trojans. For example, ICSCA Labs tests only for replicating malcode, and The WildList and WildCore test only for viruses and worms.

Anti-spyware and content filtering technologies are effective against spyware and spam respectively, but offer little protection against the evolving threats discussed in this paper.

IBM's virus prevention system (VPS) technology is behavioral anti-malcode technology designed to stop zero day attacks by pre-executing code in a virtual space and stopping it from compromising its target if it exhibits malicious behavior. Detecting bad behavior is critical to protecting against the latest threats in practice today. Using behavioral technology, VPS is able to provide extra protection and broader coverage against attacks.

* While some signature AV vendors can provide some partial protection for Trojans, this protection is often post infection and only for Trojans that infect their customers. This level of protection is not always effective against new era threats.

Key Differences between VPS and Signature AV			
Protection Against New Era Threats	 Designer Malware	 Ransomware	 Root Kit
Virus Prevention System (VPS)	Can protect patient zero	Preemptive detection	Prevents establishment of root kit
Signature AV	Needs patient zero first	Can detect, but cannot clean up after infection (i.e. "stolen data")	Cannot clean up after taking root

IBM Internet Security Systems (ISS) Protection Platform to Stop Evolving Threats

The IBM protection platform is a simple, integrated solution that puts preemptive protection within the reach of all security-conscious organizations.

Given the hackers' motivation, organizations must be prepared with a platform that can grow and adapt to constantly evolving threats. The IBM family of advanced security products and services works together as an integrated system. Each available security module enables advanced protection for different types of threats and situations. Each offering is effective when used alone, but enhances protection even further when used as part of the integrated protection platform.

IBM protection solutions incorporate the most advanced security technologies to combat new threats. Its patented virus prevention system (VPS) focuses on detecting malicious behavior and requires no signature updates to identify malicious attacks. IBM's entire preemptive approach to protection focuses on preventing bad behavior vs. protecting against only known threats. The IBM protection platform provides end-to-end coverage of the enterprise with solutions for desktops, servers, networks and gateways – all centrally managed from a single console. Specific features of the IBM protection platform designed to effectively prevent evolving threats include:

- VPS technology – a unique technology that takes preemptive action against suspicious code even before it is publicly known. VPS examines and runs code in pre-execution space using a virtual environment – so there is almost no danger of compromising the actual system or sustaining any collateral damage during detection. Using behavior-based detection vs. pre-developed signatures, VPS enables increased protection against even the latest designer malcode, root kits and ransomware. VPS technology is included in many IBM products including IBM Proventia® Desktop Endpoint Security, Proventia Network Mail Security System, and the Proventia Network Multi-Function Security (MFS) appliance.

- Proventia Desktop is a multilayered solution that delivers preemptive protection against multiple types of threats from a single agent. Proventia Desktop lives up to its industry recognition as being the most comprehensive multi-layered protection agent by incorporating personal firewall, vulnerability-based intrusion prevention, buffer overflow exploit prevention, application control, signature anti-virus and VPS technology. These technologies work together to stop Internet threats before they can penetrate desktops and impact business – averting downtime, lost revenues, or the planting of malcode that could steal data or cause direct financial loss.
- Proventia Server Intrusion Prevention is also a multilayered solution that preempts multiple types of threats from a single agent. Today's hybrid threats and sophisticated attacks regularly bypass and thwart conventional defenses that rely on attack-specific security technology. With Proventia Server's multilayered approach, if a single protection technology is insufficient against a specific threat, another technology is employed to protect.
- Proventia Network Mail provides preemptive protection and spam control for the enterprise messaging infrastructure. Scaling to support large environments with minimal appliance deployments, Proventia Network Mail leverages VPS technology to keep malicious code and traffic at bay.
- The Proventia Network MFS appliance combines IBM's industry-leading intrusion prevention technology with both traditional signature anti-virus and the behavioral anti-malcode abilities of VPS. The appliance also includes firewall, Web filtering, and anti-spam technology to proactively combat a variety of threats all at once, such as unauthorized access, network attacks, malicious code and blended threats.

Service-based Protection Against the Evolving Threat

IBM further protects against the latest threats impacting enterprise systems with IBM Professional Security Services and Managed Security Services. As a managed service provider, IBM directly observes new malcode and malicious behavior trends, making IBM well positioned to deliver increased protection with superior service.

IBM Professional Security Services deliver expert security consulting, helping organizations of all sizes reduce risk, achieve regulatory compliance, maintain business continuity and reach their security goals. IBM Professional Security Services consultants are 100 percent security-focused and utilize proven consulting methods, based on ISO 17799 best security practices. Supported by the IBM Internet Security Systems X-Force® research and development team, IBM Professional Security Services consultants are highly-skilled,

senior security professionals. This team of security experts employs proprietary toolsets, the latest threat intelligence and advanced countermeasures to build effective security programs that help protect against ever-changing threats and enhance business operations.

IBM's award-winning Managed Security Services are ideal for organizations looking to improve their information security. IBM Managed Security Services provide the expertise, knowledge and infrastructure needed to secure enterprise information assets from Internet attacks 24x7x365.

Learn More About Preventing Evolving Threats

To learn more about evolving threats and products and services designed to prevent them from disrupting enterprise networks, please visit www.ibm.com/services/us/iss.

For additional Evolving Threat education and awareness including solution sheets, regional thought leadership forums, and the latest threat information discussed in this white paper, please visit www.iss.net/evolvingthreat

The Evolving Threat Quick Reference Glossary

This section provides additional context for the key threats or key threat attributes discussed throughout this whitepaper.

Signature Anti-virus (AV) – a computer program designed to detect and respond to malicious software, such as viruses and worms. Responses may include blocking user access to infected files, cleaning infected files or systems, or informing the user that an infected program was detected.



Blended Threats – multiple malcode types combined to increase the abilities and success of an attack.



Designer Malware – a piece of malcode written to infect or compromise either one or a small number of organizations with similar profiles. For example, a Trojan written specifically for a single bank.

Malcode – malicious code that fulfills the deliberately harmful intent of an attacker when executed.



Ransomware – malcode whose payload is often to password-protect files on a user's system until a ransom is paid. More advanced scenarios now leverage multiple forms of end user manipulation and extortion.



Root Kit – root kits have the ability to hide malcode from the operating system, user, and protection agents. Numerous types of root kits exist, including, user space, kernel space, virtual machine based, hypervisor based, Network Driver Interface Specification (NDIS), and those which even hide in Electronically Erasable Programmable Read-Only Memory (EEPROM) and video memory.



Spear Phishing – a combination of phishing and social engineering in which the phishing attack targets one person or one group of people; very focused to lend added credibility to the attack.



Targeted Attacks – similar to designer malware, targeted attacks may also focus on a specific user population or demographic.



Trojans – a Trojan is a piece of code that uses “trickery” to get people to run it for a supposedly legitimate purpose. In reality the code may perform key logging or password stealing activities.



Virus – a parasitic replication, via host files, of code planted illegally in a computer program, often to damage or shut down a system or network.



Worm – a self-replicating program that uses a network to send copies of itself to other computer terminals—potentially doing so without any user intervention. Unlike a virus, a worm does not need to attach itself to an existing program or require any user intervention to spread. Worms can damage the network (e.g. consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.



© Copyright IBM Corporation 2007

IBM Global Technology Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
04-07
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia and X-Force are trademarks or registered trademarks of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.
