



INTERNET
SECURITY
SYSTEMS™

Response Strategies
For Hybrid Threats

*A New Approach To Protecting
Online Information Resources*

Introduction

Businesses today are more networked – and more dependent on being networked – than ever before. The advantages are obvious. With more connections come innovative, cost-effective ways for corporations to better serve customers, suppliers, investors and employees.

Unfortunately, this growing dependence on network technologies also introduces more complexity, more interdependence and more exposure to increasingly sophisticated online threats. The purpose of this paper is to explore the most recent and frightening manifestation of online threat – the “hybrid” – and what organizations and individuals can do to protect against it.

The hybrid, as demonstrated by Code Red, Nimda, BadTrans, and others, is a malicious program composed of a combination of formerly “stand alone” information security threats. Viruses, worms, trojans and hacker techniques have been merged into automated, multi-headed attack tools that rapidly propagate across the Internet to cause huge amounts of economic damage. For example, Nimda infected over 2.2 million PCs and servers in 24 hours after its release to the wild in September 2001 (Computer Economics), incurring over \$530M in damages via downtime and cleanup. Code Red clocked in at an even more staggering figure – an estimated \$2.6 billion of damage.

Hybrids greatly complicate network security because they change the rules of the game. Their complex nature neutralizes point solutions aimed at stand-alone threats. In addition, they morph very quickly into more virulent and better hidden forms. As a result, hybrids require companies to diligently protect all parts of the network infrastructure, responding in a coordinated fashion at the network, server, desktop and gateway levels.

It takes a comprehensive set of security technologies, knowledge of best practices, and experienced staff – such as that provided by Internet Security Systems – to beat the hybrid threat. Let’s get started on understanding what needs to be done.

Malicious Code 101

Understanding the hybrid requires a quick lesson in the history of malicious code. Until the hybrid, there were three basic types of stand-alone software programs designed to damage servers or desktops: viruses, trojans and worms. Each entity uses a distinct strategy to infect its target, then propagate after the initial infection.

In addition, how a virus or worm affects a computer depends on the “payload” it carries. The payload can be an irritating message or it can be a destructive command. Even with no payload, viruses and worms can dramatically reduce network capacity as they scan systems and/or email attachments across multiple networks. The following sections describe each of these stand-alone threats in more detail.

Viruses

Viruses hide and replicate themselves in a computer’s file system. To trigger an infection, the virus must attach itself to a file being executed by the system. It therefore depends on human intervention/interaction before it can become active. Once enabled, viruses copy themselves into essential system files, making them hard to remove. Most viruses reside in memory and actively attempt to infect other programs. The objective of the virus writer, therefore, is to create damage via wide-scale propagation, such as overwhelming a corporate Exchange server.

Most viruses spread by tricking the user into running a program, most commonly sent as an attachment via email. In fact, over 85% of viruses now spread via email – a significant escalation from a few years ago when the only way to spread a virus was via an infected floppy disk that was unwittingly walked from one PC to another. The infected system then helps continue the virus’ spread by emailing it to everyone in the address book of the affected system.

| Source of Viruses (ICSA, 2000) | | | | | |
|---------------------------------------|-------------|-------------|-------------|-------------|-------------|
| | 1996 | 1997 | 1998 | 1999 | 2000 |
| Diskette | 74% | 88% | 67% | 39% | 7% |
| Email attachment | 9% | 26% | 32% | 56% | 87% |
| Download | 12% | 18% | 12% | 13% | 2% |
| Other | 15% | 20% | 11% | 13% | 4% |

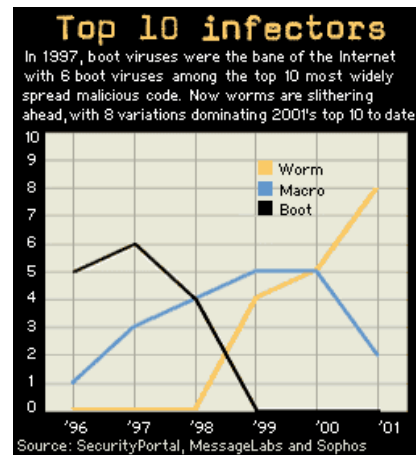
Trojans

Trojans are named after the mythical Trojan Horse. Like that famous masquerade, Trojans appear to be a useful piece of software, but carry a dangerous payload that executes on the target computer with all the privileges of the user. A trojan does not reproduce on its own, so it does not spread without assistance. Like a virus, however, it relies on fooling the user into running it as trusted software.

Typically well-behaved, trojans draw little attention to themselves in order to monitor a network or to provide a backdoor into an affected system at a later date. The first Trojans appeared in the 1950s in university settings as students, out of time-share resources on their mainframe accounts, used simple Trojans to “backdoor” other accounts and appropriate other users’ time allotments.

Worms

Prior to the arrival of the hybrid, worms were the fastest growing form of threat (see chart at right), and later became a key piece of the hybrid threat’s foundation. A worm is a software program that propagates, by itself, across a network. Unlike viruses or trojans, it executes on a system without human intervention, and typically performs a task in which it attempts to find other potentially vulnerable systems. It enters a system by exploiting bugs or overlooked features in commonly used network software already running on the target, using an automated approach very similar to those employed by human attackers. Worms often exist purely in memory, avoiding the file system and making them invisible to file-scanning antivirus software.



Evolution, Not Revolution

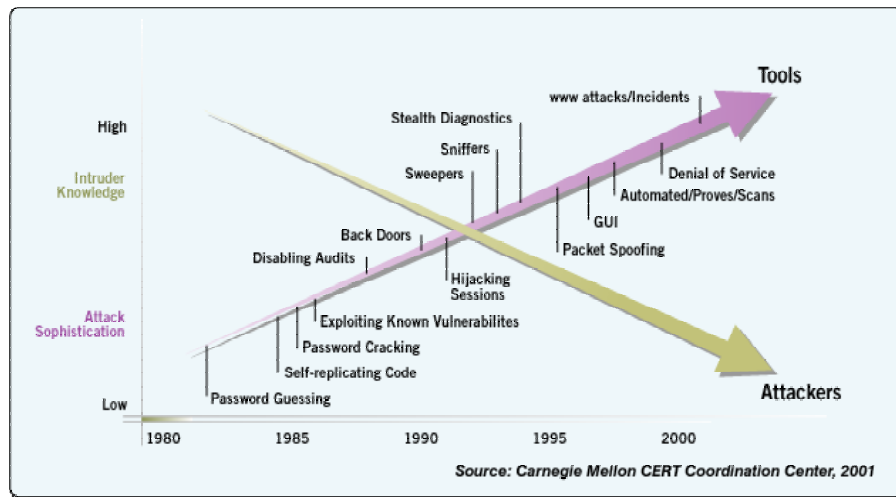
Over the years, virus authors have learned how to make their viruses spread faster. This process has been accelerated by the wide adoption of business networks and the Internet. Needless to say, as viruses have become smarter and spread faster the cost to control them has increased dramatically. In response, the protection focus has shifted from the corporate desktop to the gateway, since viral outbreaks are fed mainly by email and Internet-based (i.e., HTML) services.

| Time Required For Virus To Become Most Prevalent Virus In World (ICSA, 2000) | | | | |
|---|-------------|--------------------------|-------------------|------------------|
| Virus | Year | Type | Time to #1 | Damage |
| Jerusalem | 1990 | .EXE boot sector | 3 years | \$50M |
| Concept | 1995 | Word macro | 4 months | \$50M |
| Melissa | 1999 | Email-enabled Word macro | 4 days | \$93M to \$385M |
| Love Bug | 2000 | Email-enabled .VBS | 5 hours | \$700M to \$6.7B |

Meanwhile, worm writers and intruders continued to advance their trade. Looking to do more damage, they began to exploit multiple vulnerabilities per worm, not just a single vulnerability as

in the past. In fact, the number of attackers who are gifted enough to discover a major exploit (e.g., some weakness in a major operating system) is relatively small. At the same time, the number of hackers/intruders who are able to fully leverage this knowledge and put it to work against vulnerable systems around the world is large and growing.

This is not a paradox. In March of 2001, the well-publicized AnnaKournikova worm (not a virus!) struck. While mostly an annoyance, the true significance of “Anna” was that it was the first worm released into the wild that was built using an automated tool, the “VBS Worm Generator.” The program, which is widely available on sites frequented by attackers, highlights another disturbing trend in information security – the growing availability of powerful tools to assist relatively unsophisticated malicious users. In an era where businesses are more dependent than ever on network infrastructure for competitive advantage, this development represents a very dangerous escalation.



Finally, worm authors have learned from virus writers, and have begun to leverage email propagation techniques as a means to broaden the reach and accelerate the spread of their worms. The stage was now set for the hybrid threat to appear. In 2001, it did – the direct result of combining automated tools with the most effective, specialized skills from the virus, trojan, worm and hacker underground communities.

So What, Exactly, Is a Hybrid?

Since no two hybrids are the same, it may be easier to describe a hybrid than to define one. For example, a simple hybrid may expand a basic email attachment virus technique to include peer-to-peer (P2P) communications such as instant messaging (e.g., ICQ, IRC, AIM or Microsoft Messenger) to propagate. The hybrid uses the P2P chat network to transfer itself through the “file send” process, persuading the unwary (and overly curious) user to run the malevolent code.

Regardless of the exact combination of techniques, automation greatly expands an individual attacker’s reach, allowing hundreds or even thousands of compromised systems to methodically test and infect ever-larger number of victims. Prior to the invention of the hybrid, each of those systems would need to have been probed individually by the attacker, one at a time – a much more laborious, time-consuming process.

Case Study: Nimda

Nimda combined many malicious code techniques into a devastating punch that infected 2.2 million systems in its first 24 hours in the wild. Nimda, which is “Admin” spelled backwards, used four means of spreading (“propagation vectors,” in industry-speak):

- **Scanning** – Nimda-infected systems scan a network looking for unpatched Microsoft Internet Information Server (IIS) systems. Nimda then uses a specific exploit, called Unicode Web Traversal exploit, to gain control of the target server.
- **Email** – Nimda gathers email addresses from the mailboxes of any MAPI-based email system. Nimda then formats messages to these addresses using both the To: and the From: fields so the From: address will not be from the infected user. The worm also has its own SMTP server to send out the emails, thus avoiding Exchange or Notes servers. When Nimda arrives in an email, it uses a MIME exploit that allows it to execute just by reading the infected message or opening the message in a preview pane.
- **Browsing** – Visitors to a Nimda-infected Web server are asked to download an Outlook Express email file which contains the worm as a “readme” attachment. It then activates using the email technique described above.
- **Network Shares** – Nimda creates open network shares on the target system (desktop or server), allowing complete access to that system at a later date.

After the Infection

In the past, viruses existed mainly to propagate themselves, although some were specifically crafted to perform damage – via the delivery of their payload – to the infected system. Hybrid threats are much more dangerous. In fact, so many servers and desktops were infected with Nimda that the email traffic and constant scanning for new targets created a mini-“denial of service” condition for those networks.

Typical post-infection actions include: Increasing the remote access exposure of the infected machine; Hiding evidence of infection and removing audit trails; Placing backdoors for future unauthorized access; Rolling back existing security measures; Or hiding the presence of malicious code by moving the illicit program into “stealth,” or hibernation, mode until it is needed. Other hybrid threat activities include clearing system logs of evidence of infection, changing file and registry settings, reformatting or altering drives, files and data, corrupting databases, denying access to critical system functions or applications, and enabling remote access and control of the infected host.

Stand-Alone Security: Necessary, but Not Sufficient

One of the most maddening aspects of hybrids is how rapidly new versions appear. Many current information security strategies do not address the ever-changing nature of the threat. Divided into specific tools for a specific security needs, these applications, services and processes do not have the ability to recognize broader patterns of attack, or to work cooperatively across operational boundaries to provide a coordinated defense.

Combine this operational myopia with the increasing number of remote and mobile workers and the possibility of multi-vector attack propagation becomes much easier to envision. Corporate networks no longer have a single point of entry, so untrusted/ unauthorized access, improperly configured virtual private networks (VPNs), unsecured wireless connections and poorly identified and protected ISP access points (dial-up, cable modem or DSL) introduce a dizzying variety of new vulnerabilities, each accessible from a constantly changing range of external devices.

The usual security solutions fail to fully address these needs on several fronts:

- For antivirus, the majority of the focus has been detecting and stopping passive viruses via email, at either the server, desktop or gateway level. Other avenues of propagation, such as P2P chat systems, introduce new vulnerabilities that traditional antivirus solutions only partially address. Additionally, antivirus cleanup focuses on removing email attachments. With hybrid threats installing backdoors, applying new vulnerabilities, and modifying the system, antivirus software lacks the ability to patch and protect against these types of damage.

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 – with 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 includes the following critical elements, all designed to interact seamlessly to create a “closed loop” protection system:

- **Network, server and desktop vulnerability scanners** – Regular use of these products allows administrators to proactively identify potential avenues of attack, and then take appropriate measures to ensure the security exposures are properly repaired.
- **Network, server and desktop intrusion detection systems (IDS)** – IDS is the online burglar alarm for any network, signaling that an attack or misuse is underway. Host-based and network-based IDS remains the primary work horse for all “non-email” attack vectors. High-speed networks will require gigabit (Gb) capability in order to ensure that the IDS system can keep up with the speed and volume of the network traffic. Desktop IDS should be required for all remote or mobile devices that connect to corporate networks.
- **Gateway, server and desktop antivirus** – Some hybrid threats will always use email and similar mechanisms to propagate. Therefore, antivirus, particularly at the gateway, will be a critical defense for the foreseeable future.
- **Firewall** – By blocking many of the incoming connections against services and applications that the outside world does not need to access, firewalls continue to play an important access control role in reducing the risk from these hybrid threats.
- **Centralized administration, deployment, configuration and management** – All are critical for controlling the total cost of ownership (TCO), a key issue in today’s business environment. The ability to automatically and remotely coordinate device configuration and response based on intelligent analysis of local and global security data also significantly improves response time to any significant security event.

From a process perspective, “patching” is not a practical option for many organizations. Ideally, maintaining operating systems and applications current with the latest security patches protects systems from attack and can slow the spread of a hybrid. While it sounds simple, the “patch process” for corporations with thousands of production servers (and tens of thousands of fixed and mobile desktops) is far from a trivial operation. Therefore, the security solution must be logistically realistic, as well as functional.

Likewise, forensics tools that log, report, correlate and analyze event activity are important. Understanding that forensic information in real time is even more critical. Rapid access to threat experts can ensure rapid identification and analysis of newly emergent threats before they reach the corporate perimeter.

Finally, for those organizations that lack the infrastructure and resources to manage information protection on a 24/7 basis, managed security services are both logistically and financially attractive. Services typically include:

- Policy development
- Remote scanning to identify vulnerabilities and establish remediation needs
- Intrusion protection monitoring and response
- Gateway antivirus
- VPN management and firewall services

Since the services provider is responsible for recognizing and responding to hybrid threats, the client receives both cost-effective protection and a degree of liability protection should the protection system not prove 100% effective.

The Internet Security Systems Answer

Internet Security Systems provides products and services geared towards the individualized needs enterprise, smaller enterprise, small office/home office (SOHO) and consumer markets.

Enterprise Solutions

Internet Security Systems' enterprise software and services solutions provide proactive, centrally deployed and managed protection against online business interruption and loss, all designed to operate with minimal administration or interference with normal network operations. These comprehensive protection offerings are the first to merge network, server and desktop protection into an integrated threat management environment. This powerful combination of software and services enables centralized management across multiple locations and network segments, including wireless networks, branch offices and mobile workers. Most importantly, Internet Security Systems' proactive approach keeps staff apprised on newly discovered security issues, ensuring that the protection solution is quickly updated to account for newly evolved threats.

Enterprise solutions include the **RealSecure® Protection System**, a unique software offering that encompasses vulnerability assessment and threat detection, prevention and response across networks, servers and desktops, all coordinated through the **RealSecure® SiteProtector™** centralized management platform. In addition, Internet Security Systems' Managed Security Services extends this protection strategy through managed security offerings and expert 24/7 management, for situations where additional flexibility and support are required. Extensive professional services and emergency response ensure an appropriate, effective security solution, regardless of business environment.

Smaller Enterprises

In addition, Internet Security Systems provides a full range of security solutions that provide enterprise-quality protection for smaller enterprises, ranging in size from roughly \$50 million to \$500 million in annual revenue. These solutions are also based on the **RealSecure Protection System** to provide integrated intrusion detection and response, vulnerability assessment, policy compliance, and data collection and analysis, all coordinated through the **RealSecure SiteProtector** centralized management platform. Managed Security Services extends this protection strategy through managed security offerings and expert 24/7 management, for situations where additional flexibility and support are required. Finally, the **Secure StepsSM** program provides scalable, affordable risk management solutions based on Internet Security Systems' Managed Security Services that establish the security practices necessary to obtain insurance coverage for online business operations.

Small Office/Home Office & Consumer

Small office/home office and consumer customers require a security solution that is as cost-effective and easy-to-use as possible. Internet Security Systems' **BlackICE™** products provide comprehensive firewall, intrusion protection and reporting solutions designed specifically for remote workers, telecommuters or consumers in smaller office environments. These straight forward applications combine firewall, intrusion protection and report management into a simple, powerful protection solution. BlackICE products are widely available through retail and online outlets.

| Hybrid Threat Comprehensive Solution Matrix | | | |
|--|---|--|---|
| | Network Protection | OS Protection | Application Protection |
| Products | <ul style="list-style-type: none"> ▪ Network Vulnerability Scanners ▪ Network IDS ▪ Gigabit Network IDS ▪ Active IDS ▪ Gateway Antivirus ▪ Firewall | <ul style="list-style-type: none"> ▪ Server and Workstation Vulnerability Scanners ▪ Server and Workstation IDS ▪ Desktop IDS ▪ Server and Desktop Antivirus | <ul style="list-style-type: none"> ▪ Application based Vulnerability Scanner ▪ Database Scanner ▪ Application based IDS ▪ Email Antivirus Apps (Exchange, Notes, Sendmail) |
| Protection Services | <ul style="list-style-type: none"> ▪ Remote Scanning Service ▪ IDS Mgt and Monitoring ▪ Gateway Antivirus Mgmt ▪ Gateway VPN Mgmt ▪ Firewall Mgt | <ul style="list-style-type: none"> ▪ Remote Scanning Service ▪ IDS Mgt and Monitoring ▪ Gateway Antivirus Mgmt | <ul style="list-style-type: none"> ▪ Remote Scanning Service ▪ Host Application Monitoring and Protecting |
| Consulting | <ul style="list-style-type: none"> ▪ Policy Development and Enforcement ▪ Security Assessment ▪ Penetration Testing ▪ Deploying and Configuring Burglar Alarm System ▪ Hardening and Locking down ▪ Emergency Response Services | <ul style="list-style-type: none"> ▪ Policy Development and Enforcement ▪ Security Assessment ▪ Penetration Testing ▪ Deploying and Configuring Burglar Alarm System ▪ Hardening of OS ▪ Emergency Response Services | <ul style="list-style-type: none"> ▪ App Policy Development and Enforcement ▪ App Security Assessment ▪ Penetration Testing ▪ Deploying and Configuring Burglar Alarm System ▪ Emergency Response Services |
| Education | <ul style="list-style-type: none"> ▪ Security Policy and Standards ▪ Ethical Hacking Class ▪ IDS Classes ▪ Vulnerability Assessment Classes ▪ Firewall Classes | <ul style="list-style-type: none"> ▪ Security Policy and Standards ▪ Ethical Hacking Class ▪ IDS Classes ▪ Vulnerability Assessment Classes | <ul style="list-style-type: none"> ▪ Security Policy and Standards ▪ Ethical Hacking Class ▪ IDS Classes ▪ Vulnerability Assessment Classes |

Conclusion

Hybrids are a dangerous costly escalation in the ongoing battle between good and evil, both on corporate networks and across the Internet. These threats not only aren't going away – they will actually increase, in prevalence, complexity and virulence. Organizations that rely on network technologies to conduct business operations have no option but to deal with this threat. The key to an effective defense is vigilance (i.e., early warning), process (“best practice”), skilled people (both in-house and 3rd party experts) and comprehensive security products. It’s a tall order – but help is available via Internet Security Systems, who provides a full range of software and services that dynamically detect, prevent and respond to hybrid threats, across networks, servers and desktops.

About Internet Security Systems (ISS)

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical online resources from attack and misuse. ISS is headquartered in Atlanta, GA, with additional operations throughout the United States and in Asia, Australia, Europe, Latin America and the Middle East.

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

Internet Security Systems, the Internet Security Systems logo and SiteProtector 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 marks and names 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.