Virus Prevention Without Signatures

INTERNET | SECURITY | SYSTEMS®
Ahead of the threat.™

Introduction

Viruses have been on the attack for more than 20 years, and the cost of dealing with them is escalating. Too many malcode (malicious code) attacks by viruses, worms, Trojans and the like are breaking through today's most prevalent system defenses — Antivirus (AV) programs. It is time for the next generation of virus prevention. This whitepaper will discuss the full impact of virus disasters and what historically has been done to combat the problem. It will show how ISS' new Virus Prevention System (VPS) represents a quantum leap in preemptive protection. Finally, it will show how VPS fits into a layered protection strategy, providing protection at the host/desktop and at the gateway.

The Very Real Threat of Virus Attacks

In 2004, virus disasters[1] increased 12 percent, although 99 percent of those surveyed had AV protection in place. The average cost of recovery increased more than 40 percent last year, to $130,000 per incident. It also took longer to recover: 7 more person days — a 25 percent increase — bringing the average time for full recovery to 31 person days.

The 2004 ICSA Labs survey polled only a handful of the number of businesses operating in the United States today. This report states: "Respondents in our survey historically underestimate costs by a factor of 7 to 10." If the full impact of a virus attack could be calculated, the costs would be astronomical — lost data and lost sales, customer dissatisfaction or breaches of confidentiality, employee downtime, increased network administration workload and system repair, to name a few. As the survey put it, "Based on the dollars reported,... complete cost of recovery would be in the range from $900,000 to more than $5,000,000 (in total costs of recovery alone)." [2]

Even with firewall and Antivirus protection in place, virus attacks can penetrate network security defenses. It can take hours, sometimes days, for traditional AV vendors to create a virus update. Add to this the time it takes for an organization to test the update, distribute it to all their systems and make it available to their remote laptop populations, and the whole signature update process can take days or weeks. During this waiting period, organizations' critical assets are exposed and at risk.

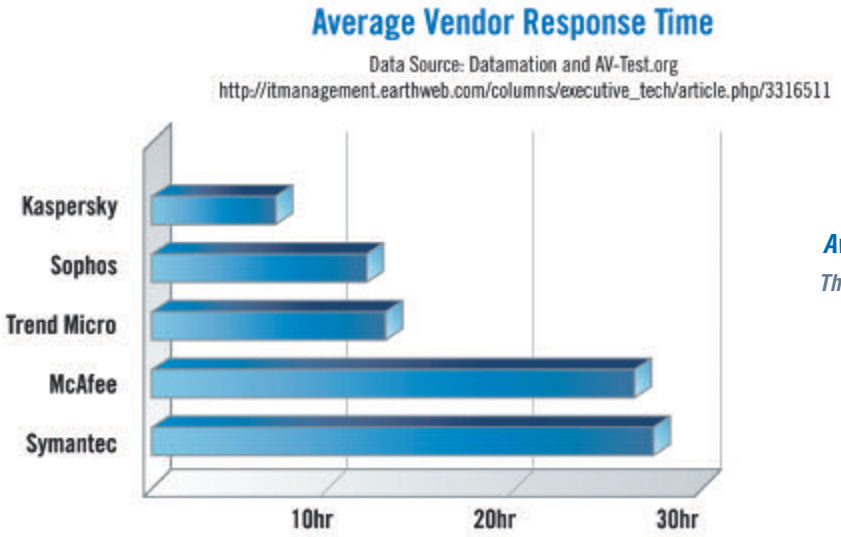
Andreas Marx of AV-Test.org,[3] a worldwide security software testing organization based in Germany, has published studies on Antivirus response times. A February 2004 test measured how long it took 23 traditional AV vendors to come up with updates to

1 ICSA Labs Virus Prevalence Survey 2004, www.icsalabs.com. A virus disaster is defined as **"an incident in which 25 or more machines experienced a single virus at or about the same time,"** and/or incidents **"that caused organizations significant damage or monetary loss."**

2 **Ibid.**

3 www.avtest.org

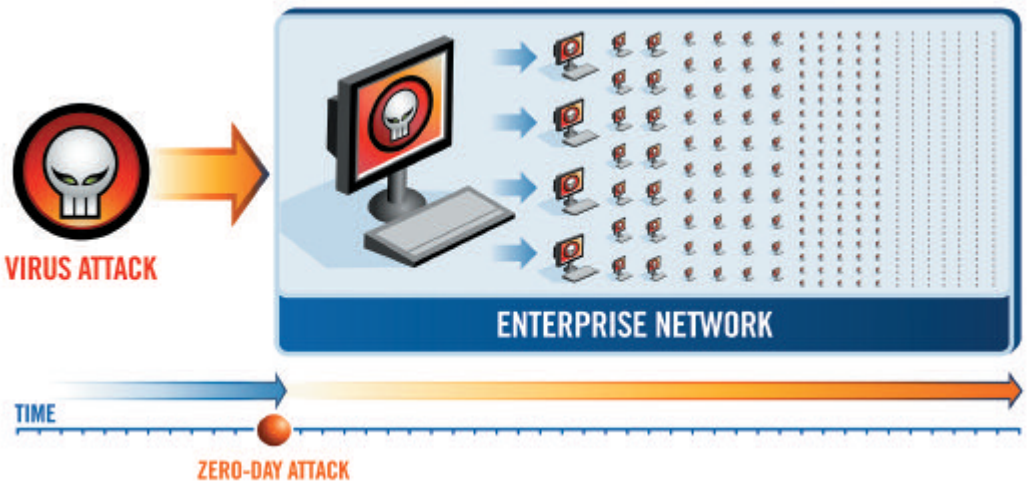
combat four viruses: Dumaru.Y, MyDoom.A, Bagle.A and Bagle.B. According to AV-Test.org data, these are the average lag times for each program during the test period: [4]



Average Antivirus Vendor Response Time

The top two AV vendors averaged more than 26 hours to respond to the threats.

What business can afford to wait that long for an effective virus update? Just one infected PC can easily reproduce at least 10 copies of the virus per second; exponentially, a virus can propagate worldwide in a matter of minutes. Because of the amount of time it takes to deliver, test and deploy signature updates, the window of exposure can extend from 7 to 30 hours — and that degree of risk should be unacceptable to any company.



Nevertheless, businesses have been forced to settle for less-than-adequate security solutions because, until recently, the industry didn't know what it didn't have – a preemptive choice.

---

[4] **"How Long Must You Wait for an Anti-Virus Fix?"** by Brian Livingston, February 23, 2004; http://itmanagement.earthweb.com/columns/executive_tech/print.php/3316511. See also www.avtest.org.

The Evolution of Antivirus (AV) Technology

In the early days of computer viruses, combating viruses, worms and Trojans was relatively straightforward. But as Internet threats have became more sophisticated through the use of social engineering and hybrid attacks,"first-generation" Antivirus protection has become too cumbersome and impractical.

This overview of AV technology development highlights the advantages and drawbacks of the most widely used methods for detecting malcode:

TECHNOLOGY	HOW IT WORKS	ADVANTAGES	DRAWBACKS
1. Integrity Checker	• On early DOS systems, used a checksum routine (such as MD5 or SHA128) to look for any sign of change, and would immediately flag any discrepancy.	• 100 % effective in recognizing any changes or infections on the system.	• Generates a warning on every file that is modified, not only virus infected files. • Too cumbersome to use with sophisticated computers. • Impractical to apply checksum in Windows environment where there are constant patches and updates and change is not necessarily bad.
2. Signature Scanner	• Compares code to signature – a "digital fingerprint." • AV researchers create "names" for each virus strain and variant.	• Easy to implement – proven method. • Low false positives.	• Does not find new or modified viruses. • Signature technique is inflexible. • Requires regular updates – raises cost of ownership. • Exposed to virus while waiting for signature update and distribution.
3. Heuristics (rule-based)	• Applies rules – e.g. Do not allow writes to EXE file, etc.	• Supporting method, not viable in itself.	• Misses most viruses and high rate of false positives.

4. Behavior Blocking/ Sandboxing	• Redirects API calls to a "safe" environment, applies rules to actions.
	• Halts malicious action as soon as it is recognized.
	• Redirects API and low-level calls and blocks dangerous actions, such as disk writes.
	• Halts malicious action as soon as it is recognized.
		• User configurable to perform a user-defined task.
		• May be effective in blocking unknown, unidentified threats.
		• May be effective in blocking unknown, unidentified threats.
			• High rate of false positives: Warning on every blocked API and asks user to Allow or Block – user dependency.
			• Constant updating, adjustment and fine-tuning of rules.
			  • High cost of ownership
			  • High security and system expertise required
			• Limited, incomplete view of what malcode is doing.
			• Cannot make a diagnosis in pre-execution space.
			• Collateral damage before detection.
			  • System memory
			  • Littered malicious files
			  • Changed system settings

Any next-generation virus prevention technology must leverage the strengths and overcome the weaknesses of earlier methods. In developing new solutions, several criteria should be weighed, including:

- **How well does it stop known attacks?**
- **How well does it stop unknown attacks?**
- **What is the potential for false positives?**
- **What is the likelihood of collateral damage?**
- **How frequently must it be updated or tuned?**
- **How much time and expertise is required for initial set-up?**
- **How much ongoing change management is required?**

New prevention technologies must be effective in preventing new threats, and must be cost-effective to boot. The next generation is Internet Security System's Virus Prevention System.

The Quantum Leap to Preemptive Protection: ISS' Virus Prevention System (VPS)

ISS' Virus Prevention System is designed to be ***Ahead of the Threat***™ – thwarting new and unknown malicious attacks before they have an opportunity to cause damage. VPS is effective, preemptive protection. With this proactive technology, the heyday of widespread virus attacks is over: More than 90 percent of new viruses are stopped dead at "moment zero."

ISS' Virus Prevention System is 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 no danger of compromising the actual system or sustaining any collateral damage during detection.

VPS performs a complete "granular" analysis to examine the fine points of virus behavior, uncovering subtleties and levels of specific detail. It gathers a complete picture of the entire code execution before making a diagnosis, so there is a high degree of detection and almost no false alarms (false positives). This avoids costly investigations and allows for uninterrupted business.

To be effective against unknown threats, VPS incorporates the expert knowledge of dedicated malcode analysts — ISS' X-Force® security research team. VPS looks for malicious behavior patterns as defined by ISS' malcode experts — behavior patterns that have been used before by other malcode. Having X-Force research and development built into security products is like having a full-time onsite security expert, removing the burden of having to be de facto malcode experts from an enterprise's IT department.

VPS' behavior-based testing analyzes what the code will do if executed on the real system. Its virtualization of executable code identifies the presence of attacking behaviors, so it can prevent malicious code even before it has been publicly identified and named — before "traditional" virus definitions have been developed. This protection occurs virtually instantaneously — at moment zero.

VPS does not require updates to detect new viruses. This "moment zero" protection can eliminate the window of exposure between the release of a new virus and AV vendors' update of virus definitions. In essence, VPS offers near "immunity" to threats.

How VPS Improves on Earlier Technology

The most valuable benefit of ISS' Virus Prevention System is that it takes IT organizations out of crisis mode. VPS is "hands off."

It does not require daily or weekly update maintenance, thus reducing update costs and bandwidth use, and it does not need user interaction for diagnosis, reducing the potential for human error. Ultimately, it reduces the need for IT departments to scramble in the face of a new virus outbreak. Since they no longer have to react immediately to threats, they can focus on business-oriented tasks and budget their time and resources more effectively.

ISS' Virus Prevention System is the next generation of virus prevention and its patent- pending design leverages the strengths of traditional methods while mitigating their drawbacks.

SIGNATURE SCANNER (TRADITIONAL AV)	ISS' Virus Prevention System
Reactive to recognized threats	Preemptive to unknown or unrecognized threats
Regular daily or weekly updates and maintenance required	No daily or weekly updates needed
Window of exposure until virus updates become available	"Moment zero" protection – not vulnerable
Low false positives	Less than .002% false positives
Inflexible "fingerprinting" technique (1 to 1)	Robust behavioral analysis (1 to many)

BEHAVIOR BLOCKER ("SANDBOX")	ISS' Virus Prevention System
Can block some unknown or unrecognized threats – but varies based on rule quality and/or investment - Forces Trade-off between FalseP and FalseN	Preemptive blocking unknown or unrecognized threats – does not vary – does not force trade off
Observes actions of suspicious code running in real time on a live system	Examines and analyzes code in milliseconds in a virtual environment
Allows code to run live, exposing system to significant collateral damage	Running code in a virtual environment protects system resources from risk
Provides a limited, incomplete view of what malcode has done	Provides a complete picture of what malcode can do
Can't see all code branches – may allow for unknowing transfer of dormant malicious code to others	Examines all code branches through on-the-fly changes in virtual environment to expose malicious behavior – does not allow transfer of dormant code to others
May use rough mathematical calculations or crude sequences of API calls and access control lists	Uses detailed granular analysis to examine subtle malcode techniques and levels of specific detail
Requires constant updating, adjustment and fine-tuning of rules (high maintenance/high cost of ownership)/ may need user input for protection	"Hands off" system does not need regular maintenance or user interaction for diagnosis
High rate of false positives is likely – resulting in unnecessary business interruptions	Very low rate of false positives – unlikely to impact flow of business
Must intercept behaviors for every execution	Needs to analyze code just once in the virtual machine

Why VPS Is Able to Identify "New" Viruses

There are more than 100,000 viruses in the wild. However, most "new" viruses are made up of snippets of malcode used in previous virus outbreaks.

In the words of virus expert Dr. Fred Cohen:

> ***"I've been…surprised by the lack of innovation in virus writers. There is a lot of potential for things that I wrote about in the late eighties that haven't been realized, largely because [virus writers] haven't really become very sophisticated yet."*** [5]

Because virtually all "new" viruses contain recycled material or common methods, VPS will recognize the malicious techniques — the combination of computer activities used in malicious code. Once VPS understands the technique, any new or unknown virus using that technique is eliminated.

ISS' X-Force team has identified hundreds of virus "families" exhibiting similar characteristics, so even a new variant, such as MyDoom.A and MyDoom.B, is likely to exhibit recognizable characteristics. During examination and analysis, VPS makes a "diary" of what the code tries to do, then categorizes it according to the most similar code family.

This preemptive protection works from moment zero — without having to wait for AV vendors to create a virus definition. In July 2004, during a regular internal test of VPS against threats from the wildlist[6], ISS measured the Virus Prevention System's signature-less protection capabilities. VPS caught 107 out of 110 viral threats: a 97% success rate. The total breaks down as follows:

- **89 out of 90 mass e-mails.**
- **12 out of 13 network exploits.**
- **3 out of 3 peer-to-peer infectors.**
- **1 out of 1 file infectors.**
- **2 out of 3 other types of threats, such as Phatbot.**

Today, ISS continually performs internal testing of VPS against the wildlist to ensure its signature-less capabilities stay well above 90%. In another study, ISS tested VPS on 40 million files, and had less than 0.0018% of false positives — certainly an acceptable amount by industry standards.

No other technology provides this degree of preemptive protection. VPS complements existing Antivirus programs most businesses currently have in place, and multi-layered protection is always the best policy. Using VPS and AV together, a system is far less likely to become infected. "Moment zero" protection plus AV updates on a manageable maintenance schedule equals virtual immunity at a low cost of ownership.

5 **"Three Minutes With Fred Cohen, Virus Trends Tracker,"** in PC World, Nov. 14, 2000.

6 **"In the wild"** malcode as reported by The Wildlist Organization and ISS customers (July 1,2004).

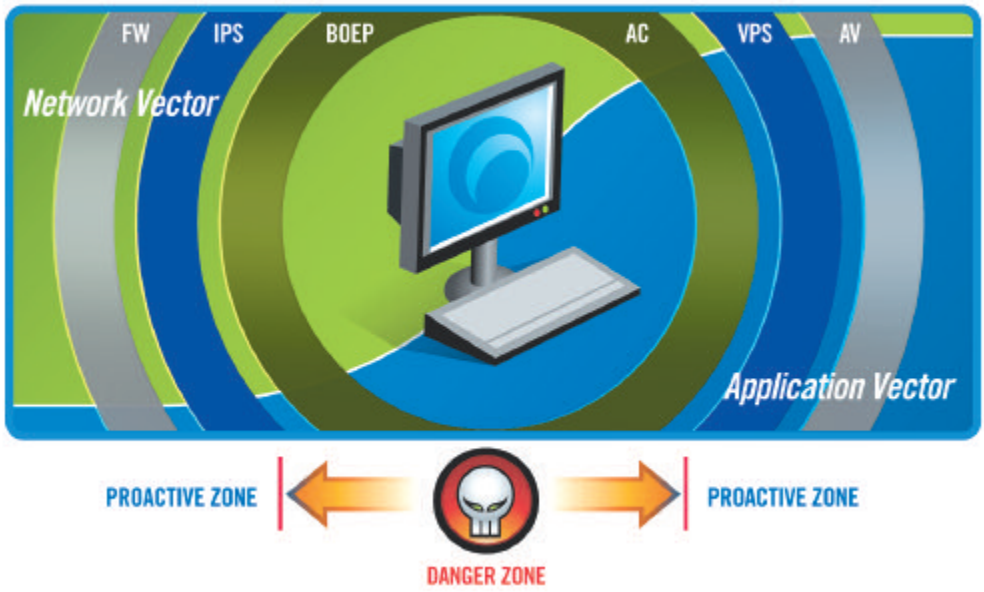
Using VPS in a Multi-layered Protection Strategy

At the Host:

Today's blended threats come from both the application side and the network side. Therefore, no one form of protection can eliminate every kind of threat. Application-based attacks require some form of user involvement to launch an attack. E mail, Web downloads, removable media and peer-to-peer applications are all common sources of attacks by viruses, e-mail worms, Trojan applications and spyware. VPS' moment-zero protection is designed to combat these threats.

Network-based attacks can penetrate, launch and propagate without human intervention. These malicious exploits include direct hacking and theft, network-based worms, denial of service (DoS) attacks, and the installation of remote access backdoors and robot (bot) footholds for future use by the attacker. VPS can assist in thwarting the propagation stage of a network-borne attack.

ISS recommends a multi-layered approach to ensure adequate protection for both network and application-based vectors. To adequately protect against network-based threats, a multi-layered approach to host security requires a firewall, an intrusion prevention system and buffer overflow exploit prevention. Multi-layered application-based security should include Antivirus protection, application control, communication control and the Virus Prevention System[7]. Newer blended threats, such as spyware, require both network and application based protection.



For more information on ISS' multilayered protection at the host:
http://documents.iss.net/whitepapers/ISS_Preemptive_Host_Protection_Whitepaper.pdf

---

[7] Please refer to the whitepaper, **"Defining the Rules for Preemptive Host Protection: Internet Security Systems' Multi-Layered Strategy,"** for more information on multi-layered system protection.

At the Gateway:

Because a threat can originate outside the network or from within, ISS' Virus Prevention System is a major element of both the Proventia® integrated security appliance and Proventia® Desktop. Working as a unified point of protection at the network level, the Proventia integrated security appliance combines VPS with intrusion prevention, Antivirus, antispam, virtual private networking (VPN), Web filtering and a firewall. VPS at the gateway helps protect desktops or servers that might not be adequately protected. Since the primary mechanism for virus propagation is through E-mail, by stopping malware at the gateway, organizations save money on network usage, E-mail disk space, E-mail system uptime and stability. VPS at the gateway, prevents viruses from penetrating into the network and utilizing valuable network resources like bandwidth and processing power.

The New Standard

With the proliferation of virus variants, today's businesses need more than "reactive" protection against unknown threats. During the window of exposure before the release of Antivirus remedies, the direct and indirect costs of infection, productivity loss, or being closed for business are hard to measure and may prove impossible to recover.

It is essential for businesses to have preemptive protection that stays ahead of the threat. Proactively blocking attacks by yet-to-be recognized malcode, allows networks and host systems to remain online and available, Internet traffic to flow, sales and services to continue unabated — in other words, maintaining business as usual without risk of disruption by viruses, worms and the like. ISS' Virus Prevention System technology helps assure that companies will be protected against the release of new, unknown malicious code attacks. Based on uncompromising research by ISS X-Force research and development, VPS recognizes and blocks malicious behavior even if Antivirus researchers have not yet identified and named the threat. It performs analysis in a virtual environment, removing all risk from network systems and end-user machines. And, VPS operates without needing updates — a boon for overworked IT departments.

Used as part of a multi-layered strategy at the host and gateway, VPS affords a level of protection not seen in other marketed security solutions, and represents a higher standard of protection that today's industry regulations and Internet-friendly business environments demand.

Appendix A – Detailed explanation of Virus Detection Technologies

Integrity Checking

Integrity checking detects changes made to executable files. By definition, a virus must change the files it is using in order to replicate. Generally, a virus will infect other files with its own code to perform this replication. In doing this, it modifies the header of the file, attaches to the file, inserts its own code in sections of the file or overwrites the entire file. Integrity checkers take a "snapshot" of all files on the hard disk during installation. Then they compare each file to this snapshot, either when the file is opened or on subsequent scans of the disk by the user. Any file that is modified is flagged as a potential virus. If the computer was already infected prior to the installation of the integrity checking software, then detection will take place the next time a file is modified. Integrity checkers are useless against many of the latest viruses. Viruses can modify a file in a manner not detectable by an integrity checker, for instance by inserting their code into a cavity (not file length increase) that is not checked by the integrity checker, or by spoofing the CRC32 check value. Macro viruses infect MS Office documents that can also be modified by the user. Integrity checkers are also useless against such macro viruses. Some integrity checkers incorporate other techniques to look inside documents and disable all auto-executing macros (including the ones that the user needs to perform specific tasks).

Signature Scanning

Signature scanning is one of the oldest and the most widely used method of detecting computer viruses. The scanning method is easy to defeat; any new virus, and most slightly modified viruses, will bypass the scanner and infect the computer system. The scanning method depends on a database of "signatures," which are short sequences of bytes taken from within the program code of each "known" virus. The signature scanner opens every file on the disk, compares the content of that file with every signature in its database and, when a match is found, displays a warning that a virus has been identified.

When all signatures in the database have been compared to all files and no match has been found, the signature scanner declares the system virus free, even if many viruses exist on the system. Viruses and other malicious code remain undetected if there is no signature present in the database. The success rate of scanners can therefore only be expressed as a percentage of a defined "zoo" of viruses. Any signature-based product will perform poorly where the "zoo" contains many viruses that have no signature representation in the database and excellent where all viruses have a matching signature representation.

Signature databases need to be maintained by a significant human effort to obtain, analyze and extract a unique signature from as many new viruses as possible, test that signature for false positive detection, include the signature in a new database and distribute that database to customers.

Most newer signature scanners incorporate some form of heuristics, which will detect close to 20% of unknown viruses (20% of {3% to 15%} is 0.6% to 3%) leaving at best 2.4% and at worst 12% of all viruses undetectable. Unfortunately, heuristics show a high rate of false positives as well.

The high-detection rate of scanners declines rapidly when the user does not update the database at least once every month. After a 6-month period, at least 1,200 new viruses have been created. Whenever a large, new virus outbreak occurs, every computer protected by a signature scanner will have a huge risk of becoming infected. This is the most important drawback of this method. Other drawbacks are the constant reliance on signature updates, the reliance on the user to perform this function, and the need to scan all files on the computer system every time a signature update is performed.

Heuristic Detection

Heuristic detection of computer viruses relies on rules, defined by the manner in which the virus modifies a host program file. A program file is examined and the heuristic scanner will try to determine:

- **Does the program contain invalid instructions?**
- **Is the time and date stamp of the file valid (viruses are known to add 100 years to the date as an "infection flag")?**
- **Is the entry point close to the end of the program, in the last section (viral code added) or in a data or resource section?**
- **Is the version number is unchanged while code has been added to the file?**
- **The entry point has moved to the end, but the original entry point still exists.**
- **The added code terminates in a far jump back to the original entry point.**
- **Sections have been added to the program by moving the PE header up.**
- **Sections previously partly empty are filled with code.**
- **Code has been added in a relocation section that was previously stripped.**
- **Header fields are modified to point at a new section or code near the EOF.**
- **The build time stamp in the header is significantly different from the file time in the directory.**

This is just a list of examples. From these sample rules it is possible to make an educated guess whether a file has been infected by a computer virus or if a new version of the same file is found. Heuristic scanners can go as far as identifying how many bits of a viral signature match. Others scan for short function code signatures and match the result to the structure of the file. Of course, all these things are possible in a benign program file, hence the high rate of false positives that this method exhibits.

The problem is that heuristics can never be conclusive when used in solitary. If they are too conservative in applying the rule-set, they will miss most viruses. If they are too liberal in applying the rule-set, they will generate unacceptable numbers of false positives.

Behavior Blocker/Sandbox

In the behavior blocker/sandbox method, an "unknown" program is executed in the real Windows® environment, with the API addresses to Windows functions replaced with addresses pointing at a safe environment, the behavior blocker/sandbox. Each process is associated with a "monitor" function that replaces all unsafe API's. Configuration of the behavior blocker/sandbox relies on rules. The user or the network administrator defines this set of rules. These rules express what is and what is not allowed, and which APIs are blocked. For instance, a rule can be defined as: "Do not allow write to EXE files." When the behavior blocker/sandbox hooks a File-Write API, it examines the string pointer associated with the file-handle passed to the API. If the string contains ".EXE" then the action is blocked based on the rule given above.

Other concerns associated with behavior blocker/sandbox are:

- **The virus code has to be actively executed within the real Windows OS to trigger the rule.**
- **The low detection rate.**
- **If the action is missed, the computer is immediately infected.**
- **Only one event per rule is examined, not a sequence of events, causing many false positives if the rule set is comprehensive.**
- **If the rule set is limited, detection rates are extremely poor (1 in 1,600 out of the box, using default rules).**

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2600
e-mail: sales@iss.net

REGIONAL HEADQUARTERS

Australia and New Zealand
Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838 1555
Fax: +61 (0)7 3832 4756
e-mail: aus-info@iss.net

Asia Pacific
Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: jp-sales@iss.net

Europe, Middle East and Africa
Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America
6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236-2709
Fax: (509) 756-5406
e-mail: isslatam@iss.net

Distribution: General
PM-VPSWP605

INTERNET | SECURITY | SYSTEMS®

Ahead of the threat.™