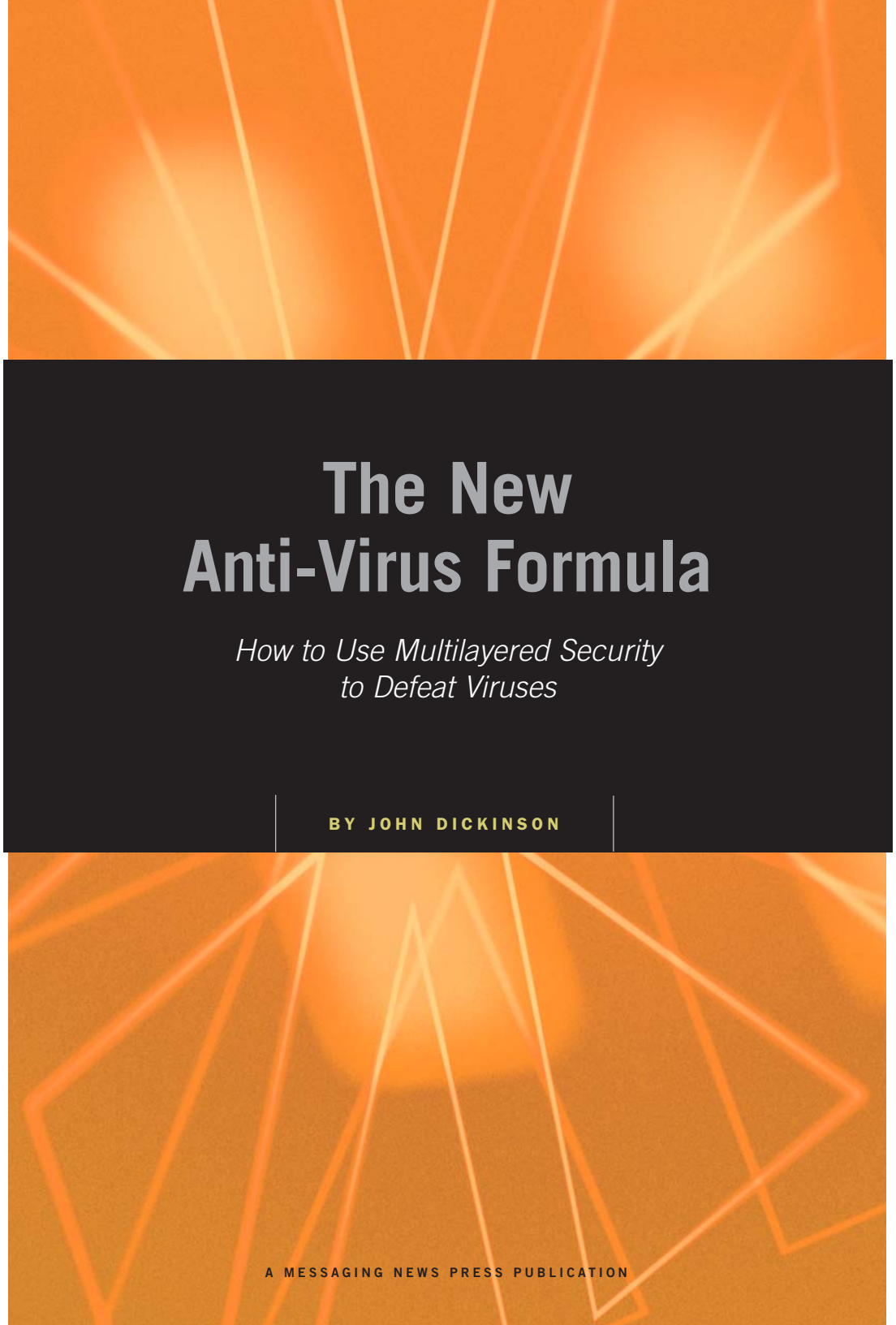

The New Anti-Virus Formula

How to Use Multilayered Security to Defeat Viruses

BY JOHN DICKINSON

A MESSAGING NEWS PRESS PUBLICATION

Table of Contents

"Email viruses are currently circulating at the rate of 900 million messages a day— and that number will increase to 4.2 billion by 2009, an increase of a staggering 466 percent."

MARCEK NIENHUIS
The Radicati Group

The New Anti-Virus Formula

It has become clear to enterprise users, ISPs and their customers, and the anti-virus community that current pattern recognition technologies lack the strength to fight off virus attacks. The weakness is primarily due to the time it takes for traditional virus signatures to be created and distributed. The unfortunate result is that the cost of virus attacks keeps going up. The Radicati Group* predicts the volume of virus attacks and the cost of such attacks will increase by a factor greater than four during the next few years.

The often long delay between the time a virus attack is launched, and its signature is distributed, results in hundreds of thousands of infected messages delivered to enterprise networks and communities of ISP users, prior to the availability of any protection from its deployment.

Users alone cannot be blamed for innocently opening email attachments, and the outcome is that the infected messages will almost certainly result in hundreds of infected PCs. That translates into tens or even hundreds of thousands of dollars in desktop clean up costs for each virus outbreak at each corporation, and untold costs to consumers.

An estimated rate of 900 million virally infected messages a day, from four to five serious virus attacks per month, makes that cost unacceptable. As a result, many companies and vendors are exploring preventive systems that can stop virus outbreaks before they happen, and minimize any damage or cost.

*The Radicati Group is a market research firm, covering all aspects of email security, email archiving, regulatory compliance, wireless technologies, web services, identity management, instant messaging, unified communications, VoIP, and more.

These preventive approaches to fighting virus attacks can be put into distinct classes:

Heuristic Filters

This technology looks at email messages for patterns that correlate with a message that is likely to be associated with a virus. Heuristic filters are based on artificial intelligence techniques in which programs are self-learning, and improve their efficacy with experience. Starting with a basic set of rules that define a virus-carrying email message, these filters gain knowledge as they make correct and incorrect judgments about which messages contain viruses and which do not.

A major advantage of Heuristic filters, over pattern scanners, is that they can catch a virus that hasn't been formed or identified as yet. However, their catch rate is significantly less than 100 percent and they are subject to false positives, a situation in which a message is identified as carrying a virus when in fact it is not.

Behavioral Analysis

These virus-detecting systems actually load and execute a program attached to an email message or downloadable from a web link embedded in a message, and analyze its behavior as if it were running on an end user's computer. There are two techniques for doing this. In one, execution is carried out by emulating execution of the program and analyzing what it does. In the other, the code is actually run on a separate virtual computer, usually called a "sandbox", to see what it does. The behavioral approach can be effective. However, it is very resource intensive and not easily scaled to enterprise levels.

Traffic Analysis

Virus outbreaks come in waves of email messages, and there are patterns of email traffic anomalies associated with a virus outbreak. Rapidly propagating viruses create these highly anomalous traffic patterns, which can be tracked and accurately detected by experienced and trained individuals. That information can then be relayed to security devices. The approach requires a very large, global dataset in order to identify patterns as they emerge. A simple examination of local email traffic at one enterprise will not yield a statistically significant sample of Internet email. Consequently, it cannot be useful in understanding if a particular traffic pattern is associated with a viral attack. By the time local traffic is large or anomalous enough to be identified as a virus attack, the damage will already be under way. Security companies that are monitoring a significant number of large networks for enterprise and ISP email traffic are the only organizations capable of creating a traffic analysis solution.

Traffic Data is Key

While all three of these approaches hold some promise of greater virus control, traffic pattern analysis is widely regarded as the most promising technique. It works, regardless of message or program content, and eliminates dependence on the ability of some system to recognize a virus program per se. This is important because virus writers use morphing algorithms to trip up pattern or signature-based systems by changing how they look and behave, and even where they are housed. Ironically, the more effective a virus is at avoiding detection by traditional signature-based filters, the faster it will propagate globally, and the more quickly a recognizable viral traffic pattern will emerge.

> "The rate of virus infections increased by nearly 50% from 2003—with a rate of 392 encounters per 1,000 machines per month."
>
> SOURCE:
>
> ICSA LABS 10TH ANNUAL VIRUS PREVALENCE SURVEY

The Formula for Successful Protection

An accurate and efficient predictive virus solution should have the following:

Global Traffic Data The key ingredient in creating an effective traffic-based virus detection system is a world view of email traffic patterns. The best solutions have a very large database and footprint of email traffic. These databases need to have messages from ISPs, enterprises, mid-market and small businesses, education, healthcare, and government, just to name a few. Recent virus outbreaks of such programs as *Sober, SoBig, Netsky,* and *Bagle,* are all examples of morphing viruses that have propagated rapidly because there were no preventive signatures in place for a long period of time. They have caused major disruptions to corporate and ISP networks, and in the process, created huge anomalous traffic patterns in worldwide email traffic. It is impossible for normal human email messaging to create traffic patterns like those in which a single virus program spreads around the globe in two hours or less.

Threat Operations Center (TOC) A predictive system, by definition, is responding to unknown threats. Global data and sophisticated algorithms are very powerful tools to combat these threats, but there is no substitute for human oversight in helping to identify new anomalies and new outbreaks. The most sophisticated preventive solution will include a fully staffed 24x7 threat operations center, that has multi-lingual analysts and statisticians reviewing dynamic email traffic data.

Dynamic Quarantine The key concept behind predictive virus systems is that they can take action earlier than traditional systems, but with lower confidence. Thus, a sophisticated quarantine is an essential ingredient to mitigate false positives. This quarantine should have tools to allow administrators to easily address exceptions, release certain messages, or "opt-out" certain users. More advanced systems will have a dynamic quarantine which can rescan messages as new rules are released. This eliminates the time consuming task of manual quarantine management and review. ■

> "Using email, web, and multi-lingual tactics, today's viruses are truly 'blended threats'."

"The *Bagel.Q* virus brought every single person in the company down. It was a nightmare... It blew us apart for the better part of a day."

MATT BROWN
IT Manager, ExecuScribe, Inc.

History, Motives, Trends, and Transmission

History

The basic technology of computer viruses is based on the very simple programming technique of creating a program that makes a copy of itself in another location, and then jumps to that location and runs itself again. Early computer engineers used the technique to test out mainframe hardware to ensure that all memory locations were functioning properly.

By itself, an innocent enough thing to do, and so was the earliest definition of computer viruses, first set down by Dr. Fred Cohen in his computer science dissertation, written at University of Southern California in 1983. He defined a computer virus as, "a computer program that can affect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of itself."

The technique and the concept of computer viruses lost their innocence in the second half of the 1980's, when hackers began distributing floppy disks with viruses on them. Such programs would create a copy of themselves that stayed resident in a computer, which in turn made another copy of itself on any floppy disk that was written to by that computer. Instead of remaining within the confines of the author's computer, these viruses would hop from computer to computer as users exchanged other data on floppy disks.

The paradigm for spreading a virus program was quickly extended to local area networks, and proprietary wide area networks. Viruses would quickly spread throughout an enterprise network, infecting any computer attached to it. The first invasion of ARPANet (later known as the Internet) occurred in 1988, when a worm virus brought some 6,000 connected computers to a halt.

If the virus programs did nothing more than spread themselves around by making copies of themselves and pulling off the occasional practical joke, it would have been bad enough. But malicious virus writers began creating programs that would destroy data and programs, including operating systems, sometimes wiping out entire hard drives and knocking computers off of networks.

Motives

There are three classes of beneficiaries of computer viruses. One class is a benevolent recipient, while the other two are nothing short of pernicious. The benevolent beneficiaries are the anti-virus companies. There are over twenty of them worldwide, and they all make money by helping users and IT professionals prevent viruses from infesting and damaging their computers. But they are as blameless for the occurrence of viruses as aspirin companies, when they make money from the onrush of headaches caused by fighting viral attacks.

> "The profile of the virus writer is changing. Today they are older and work in the computing industry."

The two pernicious categories are the coders and the spammers. Coders, who write viruses "for fun," are often on an ego trip. In the same way that hackers get thrilled by breaking into corporate databases, coders delight in spreading their code around in ways that are difficult to control. Even if the code does no damage, technological thrill seekers get excited by seeing the widespread results of their work. With this knowledge, viruses are evolving more quickly and in ways that were never expected. Enter the spammers — who, upon recognizing the profit potential of viruses, have begun paying coders to write virus programs that help do their dirty work.

The Professional Virus — Phase I of How Viruses Have Evolved

In the early days, there virus writers (coders) and there were spammers. Virus writers were technical kids that were looking for fame and thrills. Spammers were individuals who figured out how to set up a bank of servers and blast 100 million messages per day from them. Spam quickly became a problem, and most people adopted some type of spam defense that could stop mail coming from these dedicated spam servers. Since the spammers had a profit motive, and since capitalism has proven to be the engine of innovation, spammers began to look for other ways to get their mail delivered. And they noticed that the virus writers were very effective at getting mail delivered.

What happened? Spammers brought virus writers into their world to write programs that create the robot PCs (often called "zombies") that make up the BotNets responsible for most of the world's spam email messages. Most of these robot PCs are housed in consumer locations, but many also get created in the enterprise environment.

Spammers started paying virus writers to write viruses that would leave behind a "zombie"— a piece of code that would spend spam from a legitimate server, and therefore bypass spam filters. The infected robot computers are instructed, usually in the middle of the night and most often only once, to send out a large number of spam messages. In combination with other zombies, a BotNet can easily send out millions of email messages in a very short period of time.

The Criminal Virus—Phase II of How Viruses Have Evolved

Again, driven by the profit motive, professional engineering talent has been poured into techniques to obfuscate the true identity of an email sender. This was done primarily to deliver spam, but we now see a more criminal application of these techniques—online fraud. Those hapless coders that wrote viruses for fun, have now cashed in by writing viruses that send spam. The net effect? Spammers are now paying virus writers to make new viruses that

create zombie networks that are used to send fraudulent or "phishing" emails. These emails ask receivers for personal information—and receivers are giving it.

Spam makes money. Not only do people opt in to offers and spend money on useless items, or even on nothing, the so-called phishing variant induces people to turn over the keys to their financial accounts, leading to outright theft.

The Political Virus—Phase III of How Viruses Have Evolved
There are organizations in the world, who view it as their mission to disrupt Western economies. And while blowing up a building or hijacking a plane has a big psychological impact, they make only a tiny blip economically. Imagine if someone harnessed the same techniques used by the virus writers, but instead of a profit motive, they had a political motive—to cause havoc in Western economies. Imagine if these viruses didn't leave a zombie, but instead wiped out the hard drives of every infected PC. The economic impact could be billions of dollars lost in a matter of hours. *Sober-N* was just the beginning. *(see Case Study: Sober—The Virus/Worm Trojan that Doesn't Quit)*

Trends

Viruses are traditionally detected by scanning programs that search the contents of files looking for a recognized pattern of data, or a "signature", which is the virus program itself. Virus writers have come up with various methods to escape detection by changing their programs around to make it hard for virus scanners to recognize them. The two major categories of self-changing viruses are Polymorphic Viruses and Metamorphic Viruses.

Polymorphic Viruses Polymorphic viruses make detection difficult for signature-based virus scanners, by changing their appearance with each new infection. They do so by swapping various processor instructions with equivalent instructions and by inserting junk code between essential instructions.

Metamorphic Viruses Metamorphic viruses thwart detection by truly morphing their code as they propagate. Whereas polymorphic programs make simple modifications, metamorphic viruses change the structure of the program by swapping blocks of code, and by changing program instruction sequences. Both are done in ways that do not affect the operation of the virus, but do make it unrecognizable.

Virus Transmission Media In order for a virus to work, it has to be transported from one computer to another. There are several methods of transmission that are used by virus writers.

- **Disk** The earliest viruses were transmitted by removable floppy disk. By the time other removable media such as CD-ROMs became generally available, virus transmission had moved on to other media. Disk transmission is rare today.

- **Network** Local and wide area networks are used to spread worms from computer to computer, especially worms that are designed to just use up network resources and deny essential services to users.

- **Email** The most common medium for transmitting viruses, Trojans, and worms today is email. Attached viral programs are usually disguised as "free utilities" or "free anti-virus programs," or as tempting photographs or financial offers, that naïve users click on and execute.

- **Instant Messaging** As instant messaging use increases more viruses are being transmitted through that medium, which can send programs and other files that may contain viral code, directly from user to user.

- **Peer-to-Peer File Sharing** Users of systems designed to enable sharing of entertainment and other files are frequently victimized by virus programs embedded in these files.

- **Web-Based Downloads** Virus writers often load a viral program to a webpage, and then induce email or instant messaging recipients to go to the page, download the program, and run it. ■

"Ten years of compelling data clearly indicates the virus problem shows no sign of abating. Real progress will be made when companies rely less on defensive technologies and more on proactive security polices and practices."

LARRY BRIDWELL
Content Security Programs Manager, ICSA Labs

Traditional Anti-Virus Scanning Techniques

The late 1980's and early 1990's saw the emergence of an anti-virus software segment in the personal computer industry. Several small startups, in the United States and Israel, created programs that scanned all the files on a computer disk, and scanning the computer's memory, looked for a match between a known set of virus program patterns and the contents of files stored there.

As the number of viruses in the industry grew, the problem of finding them became larger as well, and more resources were needed to develop the technology to do the job. The result was a series of consolidations that saw a few large companies become competitive leaders in the anti-virus segment.

All of these competitors used the same basic technique of scanning files for viral content, based on virus profiles, which are often called virus signatures. The technology was expanded to include scans of files being transferred to and from a computer, as well as files already housed on the computers disk storage or resident in memory. As the Internet grew, it was especially important to scan email messages and their attachments as well as files being downloaded from the Web.

There are two important weaknesses to the scanning technique for detecting and handling virus programs. The first is the ability of viruses to change their appearance, so as to become unrecognizable by scanners. The second is the inability for anti-virus companies to react quickly enough when new viruses are transmitted through email or in other ways across the Internet.

Viral Morphology

Almost as soon as programs that could discover the presence of viruses were invented, virus writers began inventing ways to disguise their wares—to make them undetectable. The earliest result was the creation of metamorphic viruses, which changed their appearance by inserting useless chunks of code and swapping register and variable assignments as the viruses moved around. The second result was the emergence of polymorphic viruses which use more sophisticated morphing techniques that change a programs appearance entirely. They move chunks of code around and change instruction sequences, in ways that make the program unrecognizable but do not affect its operation. Both morphing techniques are recognized by the anti-virus community, and both can be overcome with pattern-matching programs that are equally intelligent. However, creating virus signatures takes more time when sophisticated morphology has to be accounted for.

The Essence of Time

When virus transmission required a computer user to pass a floppy disk on to a colleague, there was plenty of time in which to diagnose viral code and create virus signatures for use in scanning programs. In the early days, new signature files were produced monthly, a period during which a virus transmitted via floppy disk could not spread very far. As computer usage grew, the frequency became weekly, but as faster transmission media came into use by virus writers, even daily updates of virus profiles are usually not frequent enough to stop a widespread viral outbreak. That is because virus writers and distributors now use spamming techniques that make it relatively simple to send out millions of virus-carrying email messages in a matter of a few hours or even minutes. The Radicati Group estimates that currently some 900 million email messages per day carry a virus of some sort, a number the analysts expect to grow to 4.2 billion messages per day in 2009.

Even at a smaller rate, this means that it only takes a very small amount of time for hundreds of thousands of computers to become infected with a virus. A small percentage of recipients, running the virus-containing program sent out to millions of recipients, is all it takes to create a major virus outbreak. Even the fastest virus sleuths take the better part of a day to get a new virus diagnosed and create a signature for it, and then it takes time to distribute the signature file. Most anti-virus programs in use today require the user or IT administrator to request updates, and most enable that to happen automatically.

But even more aggressive update schemes leave users and enterprise networks vulnerable to virus attacks for anywhere from twelve hours to three days, more than enough time for a virus attack to do serious damage.

According to AV-Test, a German virus research group at the Otto von Guericke University in Magdeburg, the response times of anti-virus vendors to the emergence of a new virus vary dramatically. The group studies anti-virus vendor performance by measuring the time after a new virus is first spotted, to the time the vendor makes a signature file available. The researchers mark the outbreak as when a British consulting group first notes the virus. Then, AV-Test checks anti-virus databases every five minutes for the presence of a new profile

The results shown here are the average response times of anti-virus vendors reported by AV-Test. These data were based on four virus outbreaks, *Dumaru.Y, MyDoom.A, Bagle.A and Bagle.B.*

AVERAGE RESPONSE TIMES OF ANTI-VIRUS VENDORS

Hrs:Mins	Anti-Virus
06:51	Kaspersky
08:21	Bitdefender
08:45	Virusbuster
09:08	F-Secure
09:16	F-Prot
09:16	RAV
09:24	AntiVir
10:31	Quickheal
10:52	InoculateIT-CA
11:30	Ikarus
12:00	AVG
12:17	Avast
12:22	Sophos
12:31	Dr. Web
13:06	Trend Micro
13:10	Norman
13:59	Comman
14:04	Panda
17:16	Esafe
24:12	A2
26:11	McAfee
27:10	Symantec
29:45	InoculateIT-VET

The results vary from nearly seven hours to more than a day, and do not take into account that as much as three days have passed for some vendors to find the correct profile. The data also does not reflect the fact that heuristic techniques, used by some of the vendors, do not require new signatures to be developed and published.

Even in the speediest case, the potential for a serious amount of destruction to occur while waiting for new virus signature files to be developed is considerable.

If you would like further information about anti-virus response times, you can visit AV-Test at: www.avtest.com

Viral Costs

The exact cost of a virus attack depends on what the virus does. If there is data destruction where backup has been inadequately carried out, the costs can be immense, possibly immeasurable.

But, even in cases where the virus results are nothing more harmful than a practical joke, there are serious costs to contend with. The first is the cost of lost productivity as an employee tries to understand what is going on with his or her computer, and then seeks help. Subsequently, the cost of clearing computers of viral infection requires manpower and other resources to carry out. Exact numbers are impossible to obtain, but estimates in the mid-to-high tens of billions of U.S. dollars are often cited as the cost of virus attacks to U.S. businesses. That includes the cost of anti-virus programs, but it is weighted heavily towards the cost of repairing damage to computers, and lost productivity. ■

"For a typical mid-sized enterprise, per disaster recovery time rose from two to seven person-days and clean-up cost was $130,000 per network—an increase of over 40% from 2003."

SOURCE:

ICSA LABS 10TH ANNUAL VIRUS PREVALENCE SURVEY

"These hackers aren't kids on a digital joyride. It's clear that their motive is financial gain."

JOHANNES ULRICH
SANS Institute

A Very Viral Future

It's been over twenty years since viruses began roaming across computer boundaries and doing damage to computer networks. The technology of viruses has changed, from simple programs that scrambled files on a single personal computer, to massively orchestrated attacks on large networks of computers, including the Internet itself.

It's not going to stop, certainly not any time soon. Viruses will continue to expand in scope, and their ability to move will continue to be enhanced by diabolically clever programmers who send them on their evil missions. New technologies emerge all the time, most recently the ability of *Sober* to invoke old copies of itself, and locate chunks of itself in different locations, including web pages, FTP sites, and the traditional email attachment. Recent innovations also include time delays that are programmed to lapse between the time a virus payload is delivered and when it is activated to do its work.

BotNets of zombie PCs, which have been created by Trojan viruses, are not used to distribute new viruses using the spamming techniques for which the BotNets were created. And those viruses in turn send more spam, which sends more viruses, and on it goes.

The end of the line for scanning techniques that detected viruses by matching program files to signature files, came the day a virus first crossed a network wire. The simple change in transportation technology that made disk-based transmission of viruses obsolete began the time compression that has led to the situation today—in which a virus can be doing worldwide damage in a matter of a few hours.

That even happened in the late 1980's, but it took years before any other method of detecting viruses could be found. The irony is that it took the conjunction of a consistent set of behaviors on the part of virus writers with the establishment of large networks of email monitoring systems to find a satisfactory solution.

Today, those email monitoring networks can recognize a pattern of virus attack, and detect that one has been launched, without even knowing what the virus looks like or what it might do. That information doesn't matter, because all it takes is the information that a massive amount of email traffic carrying a suspect type of attachment or other content is "on the wire" for these systems to detect a virus outbreak.

In a matter of a few minutes, the attack can be blocked. And, at worst, a very small number of virus-laden messages will reach their destination. Unchecked, the virus attack will reach millions of computers before the traditional virus scanning companies will unpack and diagnose the code, and develop a signature file that can be used to identify the virus.

As of now, the only limitation to the usefulness of such virus detection systems is the number of enterprise and ISP sites that have the equipment and services necessary to do the job. All it will take is time before that will be corrected—the cost of viruses is simply too great. ■

"Today, virus writers can download virus writing kits and tutorials from the Internet."

"At it's peak, the *Sober* variant was responsible for 1 in every 28 messages (3% of all email traffic)."

IRONPORT SYSTEMS THREAT OPERATIONS CENTER

CASE STUDY

Sober: The Virus/Worm/Trojan that Doesn't Quit

The year 2003 marked the first outbreak of the *SoBig* worm, which spawned a family of worms during the year. The most significant variant was *SoBig.f*, which came in August and created the largest viral attack in history, when it was found in 3 percent of all email messages. The objective of the *SoBig* family of worms was to create a network of robotized computers that could launch massive denial of service (DoS) attacks, and that could also be used to build a network suitable for spam attacks.

As significant as *SoBig* was, its notoriety has been superseded by *Sober*, a family of worms based on the *SoBig* model that first appeared in October 2003, and that has recently accounted for well over 3 percent of email traffic. The original *Sober* was a relatively simple worm that was written in Germany, but one that has evolved into a complicated program capable of morphing itself and spreading by both email messages and downloads from the Web.

While it is a *SoBig* clone, and is intended to send spam, *Sober* is innovative. Its most famous feature is that the virus-laden emails came in many languages, and the language chosen is determined by the recipient's IP address. *Sober* also exploits psychological techniques by pretending to be a removal tool for *SoBig*.

The virus is also metamorphic in a couple of different ways. It moves its code around so as to make itself unrecognizable. It also moves itself to various locations. One piece of the worm might be on a Web server, while another piece is in an email attachment, and that pattern might change the next time it moves. It's also the case that new variants of *Sober* invoke old variants to do part of their work.

A recent variant (*Sober.q*) sent neo-Nazi-tinged spam in both English and German into inboxes. Most of these messages contain links to extreme

right-wing news stories but other messages contain links to a website that tries to infect the visiting machines with the virus. In one variant (*Sober-N*) the worm was used to infect computers by posing as a way to get tickets for the 2006 World Cup in Germany. The infected computers were later usedto send out massive amounts of spam.

> "The spam problem is an enormous drain on worker productivity and on computer and network resources."

Another variation of the Trojan version of *Sober,* installs a file into infected computers with links to online stories about previous versions of the *Sober* worm and the text "Ich bin immer noch kein Spammer! Aber sollte vielleicht einer warden." In English that means, "I'm not a spammer, but perhaps I should become one." Another perniciously clever version of the program deletes update files from anti-virus vendors that contain new *Sober* signatures.

Virus programs like *Sober,* which use in BotNets to send spam, do no great harm to the computer on which they are run. However, the spam problem is an enormous drain on worker productivity and on computer and network resources. As such, anything that can be done to contain it should be done. That includes destroying virus attacks that create BotNets.

How quickly did all this happen?

Timeline

May 2nd, 2005 at 15:58 GMT

IronPort Systems saw an increase in traffic for this *Sober* variant and began to quarantine their customers' email messages that met the *Sober* criteria, enabling protection for these customers.

May 2nd, 2005 at 17:19 GMT

The first wave of signatures were released by traditional anti-virus vendors and protection begins to be deployed. After that, all was quiet.

May 14th 2005

Approximately 12 days later on May 14th, 2005 computers installed with *Sober-N* began "phoning home", to download a Trojan that installed a mass mailing spam engine and initiated monitoring servers on the Internet, to synchronize the time of a computer or server clock to reference another time source.

May 15th, 2005

The Trojan enabled the coordinated activation of the zombie computers and initiated a massive surge in polymorphic spam. ■

DEFINITIONS

Viruses and Virus Variants

There are several types of viruses that have evolved over the years. The common ones are the basic Virus, the Trojan, and the Worm.

Virus Software used to infect a computer, commonly implemented within a program that purports to do something else. Once that program is executed, the virus code, often called "the payload", is activated and attaches copies of itself to other programs in the system. When a virally infected program is run, it copies the virus to other programs.

The effect of a virus may range from literally nothing, to a practical joke or simple prank, on up to total destruction of all data on the infected computer. Sometimes viruses are written such that their destructive force is delayed until a specified date. ▸▸

Trojan Named for Homer's poetically famous Trojan Horse, these programs are similar to viruses except that they do not replicate themselves. A Trojan appears to be a legitimate program, but when it is run it performs some illicit activity, such as locating the system password or making the system more vulnerable to a future action by another program. One form of Trojan in use by spammers creates an email server on the target computer that is later used to send large numbers of spam messages.

Worm This virus variant replicates itself in such a way that a computer's disk and memory resources, or a network's bandwidth, are overloaded. Such activity will inevitably bring the system or network down.

Containers for Viruses

Viruses are usually contained within other files, usually program files. Other types of files are also capable of containing virus programs.

Programs This is the most traditional container for virus programs is a program, typically in the form of a .EXE (executable file), .DLL (dynamic link library file), .COM (executable file), .VBS (Visual Basic Script), .BAT (DOS batch file), .PIF (shortcut to an executable), .SCR (screen saver), .SHS (OLE object package), .LNK (shortcut to DOS file).

Documents Some types of document files may include programs, either written in a format specific to that document type, or as a program file of the type indicated above. Microsoft Word .DOC files and Excel document .XLS files can contain macro programs which may be viruses.

Graphics Files Multimedia and graphics files can contain viruses that execute when the file is played or opened. Some versions of Adobe Acrobat enable .PDF files to contain executable programs, including viruses, and some forms of .JPG graphics files will launch viruses when opened.

Zip Files Any of these may appear in the form of a "Zipped" file, that includes a compressed version of the program or document. ■

IronPort. Power and Innovation.

IronPort Virus Outbreak Filters™ are the world's most effective defense against evolving virus outbreaks. IronPort Virus Outbreak Filters take advantage of IronPort's global SenderBase® data to spot viruses before they strike. This data is utilized by IronPort's email security appliances, which contain sophisticated dynamic quarantines that stop suspect messages before they can do harm.

The IronPort SenderBase Network is the first, largest, and most accurate email traffic monitoring network—tracking more than 25 percent of the world's email traffic, from 75,000 contributing organizations. This database includes multiple data sources: global volume data, message composition data, spam traps and complaint data, blacklists, third party email accreditation, open proxy data along with other information such as history of IP addresses, and domains. This large and diverse dataset provides a statistically significant view into the world's email traffic.

IRONPORT EXCLUSIVE

SECURITY MODELING

IronPort is the only company with access to global email traffic data through SenderBase, the world's largest email traffic monitoring network. IronPort applies advanced security modeling algorithms to this data, resulting in sophisticated threat analysis and visualization.

This massive and diverse database is used by the IronPort Threat Operations Center to look for anomalies in real-time message traffic that indicate a virus breakout. Patterns of anomaly that identify a virus outbreak include such things as an increase in messages with a particular attachment file that are of a particular size, type or name. Other anomalies may include these messages crossing many different sources of data or company types, messages with a similar attachment size coming from a single IP, and a sudden increase in mail from a single IP address that has never sent mail. This is just the tip of the iceberg of the types of abnormal

traffic IronPort's Threat Operations Center looks for, and is critical in providing virus protection at the perimeter. This knowledge powers IronPort Virus Outbreak Filters, the world's most effective preventive security solution. Customers who are using Virus Outbreak Filters from IronPort are notified of a virus outbreak when their IronPort C-Series™ email security appliances begin to quarantine the identified email traffic. IronPort Virus Outbreak Filters have been consistently identifying outbreaks from anywhere between 1 and 40+ hours before virus signatures have become available.

Dynamic Quarantining

When IronPort's Threat Operation Center detects an anomaly that appears to be an outbreak, a rule is created and pushed out to all IronPort appliances. The first instance of an outbreak rule may be very broad such as "Quarantine all JPEGs". As the outbreak develops, new information becomes available that results in more detailed rules such as "Quarantine all JPEGs of 100K or greater". With more time, a third rule might be generated which says "Quarantine all JPEGs of 100K or greater with a filename of XYZ." As each of these new rules is generated, IronPort's Dynamic Quarantine will rescan all messages and release any that do not match the new rules. This Dynamic Quarantine combines the most immediate protection with the highest accuracy possible.

> "In the past six months, preventive virus solutions provided protection against close to 40 unique outbreaks."
>
> SOURCE:
> IRONPORT SYSTEMS
> THREAT OPERATION CENTER

IronPort's Dynamic Quarantine also contains powerful tools that let administrators examine messages, address exceptions, and change status of certain users. Administrators can be as "hands-on" or they can leave the system alone and let the Dynamic Quarantine take care of blocking, scanning, and releasing messages.

Proven Performance

In the twelve months since IronPort Virus Outbreak Filters were introduced, this technology has stopped more than 100 virus outbreaks an average of 16 hours ahead of traditional signature availability. This literally means that at a typical Global 2000 company, more than 10,000 infected messages were blocked per outbreak. Stopping this many infected messages allows the IronPort Virus Outbreak Filters solution to pay for itself in a single outbreak. A sample of response times is provided below.

Virus	Date	Virus Threat Level Raised	First Anti-Virus Signature Available	Outbreak Filter Lead Time
Sober.N	5/2/2005	15:58 PM	17:19 PM	**1:21 hours**
MYTOB.J	3/25/2005	23:30 PM (3/24)	22:38 PM (3/25)	**23:08 hours**
Bagel.BB	2/27/2005	10:39 AM (2/27)	4:22 AM (3/1)	**41:43 hours**
MyDoom.bb	2/15/2005	18:08 PM (2/15)	22:54 PM (2/16)	**28:46 hours**
Sober.J	1/30/2005	23:01 PM	10:04 AM (Next Day)	**10:57 hours**
Atak.d	12/3/2004	16:29 PM	21:04 PM	**4:35 hours**
Mugly.a	11/30/2004	2:57 AM (11/30)	9:08 AM (12/1)	**30:11 hours**
NetSky.AG	10/21/2004	21:34 PM (10/21)	11:42 AM (10/22)	**14:08 hours**

* all times in Coordinated Universal Time

For more information about IronPort Email Security Appliances and IronPort Virus Outbreak Filters, visit **www.ironport.com/leader** ■

ABOUT THE AUTHOR

JOHN DICKINSON is the editor of Messaging Pipeline, a Techweb site that focuses on messaging technologies. Coverage includes email, instant messaging, and collaboration tools, as well as the systems and security issues that go with them.

Dickinson has substantial computer industry, technology magazine and Internet experience – including several senior management, editorial, and writing positions. He has launched and re-launched, as well as created, written, and edited, articles for many magazines and websites. Hundreds of his articles have appeared in computer, automobile, and business magazines.

MNP MESSAGING NEWS PRESS
www.messagingnews.com