

Death, Taxes and Worms White Paper



Dwaine van Vuuren,
Business
Development
Director, Global
Security Solutions

1 March 2004



Table of Contents

0.0	Introduction.....	3
1.0	Was 2003 the Vintage Year or just the beginning?.....	4
2.0	Predictions that were made for 2004.....	7
2.1	Gartner Report.....	7
2.2	The Multilayer Perimeter (Dimension Data).....	9
3.0	New for 2004 and beyond: MyDoom.....	11
3.1	Worm Description.....	11
3.2	Differences between Worms and Viruses.....	11
3.3	Propagation Speed.....	11
3.4	The Threat.....	13
4.0	Recommendations.....	14
4.1	Gartner.....	14
4.2	Dimension Data.....	14
5.0	Déjà Vu – Blaster Version 2.0?.....	16
6.0	Conclusion.....	17
7.0	Appendix A ‘NSS Group Inline IPS tests’.....	18
8.0	Appendix B ‘References’.....	20

0.0 Introduction

The spate of worm activity predicted for 2004 in various Dimension Data circulars in December 2003 is off to a dramatic start with the emergence of the new Internet worm, known as MyDoom/MiMail/Novarg/Shimgapi.

SYNOPSIS

The summer of 2003 will go down in the history books as a rough one for network security executives. According to Computer Economics, an IT research and consulting firm, hackers unleashed at least 50 viruses during August alone. These include the Blaster worm, which Symantec estimated infiltrated 330,000 systems within its first four days, and SoBig, to which email security tools vendor MessageLabs awarded the dubious honour of being the fastest-spreading virus ever. The company intercepted 12.8 million Sobig-laced emails for more than 65,000 business customers within 13 days of its release.

Computer Economics estimates that the financial effects of worms and viruses unleashed in August could reach \$2 billion. According to the 2003 Computer Security Institute/FBI Computer Crime and Security Survey, 75% of 530 respondents suffered financial losses as a result of computer crimes. Theft of proprietary information and denial-of-service attacks led to the highest losses, at \$70.2 billion and \$65.6 billion, respectively; losses from virus attacks reached \$27.4 billion. The reported number of newly discovered vulnerabilities doubles each year, according to CERT.

A toll like that leaves network executives struggling to answer two big questions: Will business always live in fear of virus writers? And what will it take to turn the tide against the bad guys?

Source: NetworkWorldFusion

This Dimension Data paper takes a look at the characteristics of the MyDoom worm, and how it sets the trend for future expectations and threats. It compares recommendations and suggestions made by various leading analysts and vendors to address this threat, and positions these, together with some Dimension Data recommendations, with the Intrusion Management Architecture (IMA).

1.0 Was 2003 the Vintage Year or just the beginning?

We already know that 2003 was a good year for worms.. According to an interesting Washington Post Article, dated 1 December 2003:

If the 2003 hit parade of Internet attacks is any indicator of what's to come in 2004, computer users can look forward to a bumper crop of lightning-fast viruses and worms engineered to evade security detection, attack corporate networks and fleece consumers.

The 'Slammer' worm kicked off the virus season in January, spreading with such unprecedented speed – it infected more than 300,000 vulnerable Microsoft servers in less than 15 minutes – that it clogged networks worldwide, crashing bank ATMs and delaying airline flights.

The 'Blaster' worm made headlines in August by crashing or infecting more than a half-million PCs worldwide, attempting to hijack and infect them for a coordinated attack on Microsoft's security Web site. That attack ultimately proved unsuccessful, but security experts soon had to deal with the 'Welchia' or 'Nachi' worm, a so-called good worm that was intended to patch the security hole exploited by Blaster. Welchia spread so quickly that it disabled many corporate networks for days on end.

Early in 2003, the 'Sobig' worm turned tens of thousands of infected PCs into a network of computers designed to do nothing but send out spam. Five more variants of the Sobig worm emerged over the next eight months to replenish the attackers' supply of spamming computers as anti-virus programs inoculated computers against previous versions of Sobig.

The 'Mimail' virus, which emerged in August as a relatively harmless but fast-spreading bug, soon morphed into an email urging PayPal users to update their PayPal credit card information via a Web page that mimics the design of the eBay subsidiary's member services page. Two weeks into November, the ninth version of Mimail took that ruse a step further, including a second Web page that asks users for their Social Security number, date of birth, and mother's maiden name, three pieces of data that financial companies rely on most to verify the identity of their customers. Security experts say Internet bugs like Mimail are part of a disturbing new trend by virus writers to use repeated attacks and social engineering to steal consumers' private information and to keep their creations alive as long as possible.

"Virus writers are increasingly switching to a hit-and-run approach, engineering viruses designed less for longevity than for duping as many people as possible before the anti-virus community catches up to them," said Mark Sunner, chief technology officer for New York City-based email security company MessageLabs. "This is a trend that's likely to become even more pronounced in the year ahead."

Source: Washington Post

Welchia/Nachi and Blaster still remain among the Top Five most prevalent worms to date, according to Symantec Security Response, and infections are still rearing their head five months later. Many corporations don't even know they are infected.

A TechWeb News article dated 26th November 2003, titled "Security Threats Will Continue to Plague Enterprises In '04" also made for some interesting reading:

This year has been rough on enterprise security managers, and next year won't be any better, according to an analyst who spoke Wednesday on security trends during 2003 and beyond.

"We're in for a repeat of this year [during 2004]," said Vincent Weafer, senior director of Symantec's security response centre.

"We should expect two to four MSBlast-sized [self replicating] events in 2004 and a major mass-mailed worm or virus every month on the average."

The hard times for security professionals has many explanations, but one of the most significant trends this year has been the rise in so-called 'blended' threats, exploits that use multiple modes of infection – ranging from hacking and computer worms to denial-of-service attacks and Web site defacements – to create a single, advanced assault that overwhelms defences. Older threats such as Code Red and Nimda, and newer ones like Sobig and MSBlast, Weafer said, are perfect examples of such assaults, which have been steadily increasing for the past three years, but in 2003 really caught the attention of security professionals in their numbers and sophistication.

"Such threats are likely to become the norm," said Weafer. What makes blended threats so dangerous is that they're much more difficult to defend against than, say, a single-vector exploit that propagates via email or can be stopped by simply plugging a port at the network firewall. "Yesterday's strategy of 'one threat, one cure' is no longer viable today," he said.

In response, enterprises will have to implement a more comprehensive, in-depth defence that goes beyond the traditional firewall and anti-virus protection, and takes a more proactive approach.

But blended threats aren't the only reason why security is the year's hottest topic among enterprises, and will continue to be next year. The numbers are also running against the good guys, Weafer noted. Vulnerabilities tracked by Symantec, he said, rose from an average of 40 a week at the beginning of the year to 50 per week by November. Worse, an increasing number of those vulnerabilities can be exploited remotely – 80 percent at the moment – which means that hackers can more easily insert malicious code and wreck havoc on systems.

And attackers have moved away from targeted assaults on the perimeter of the network, such as Web servers, and are now focusing on the Internet to infect a growing number of desktops, laptops, and workstations. "That opens up far more possible targets, which are typically far less well defended," he said.

Combine that with an increasingly robust set of hacker tools – which are shared much more freely than ever before – and you have the recipe for a continued security crisis. “There’s far more knowledge now available [to hackers] about how to create exploits,” he claimed, “and so the level of technical knowledge necessary to generate an exploit is falling. Hackers are standing on each other’s shoulders, just plugging in new code into old exploits and kicking it out.” That’s one of the reasons why the window between the disclosure of vulnerability and the release of exploit code – and then a self-replicated worm – continues to shrink.

“The notion that a company has months or even a year to deploy a patch is simply gone,” Weafer said.

“This was a tough year in enterprise security,” Weafer concluded.

And from all signs, 2004 won’t be any easier.

Source: TechWeb News

The Washington Post article concludes with the following:

Worms can be inconvenient and frustrating, but security experts say a far more disturbing trend this year is the surge in the number of worms and viruses created purely for financial gain. “We’re seeing a pattern emerge where an economic motive behind worms and viruses [is] starting to be the norm rather than the exception,” said Alan Paller, director of research for the SANS Institute, a security training group in Bethesda, Md.

Take for instance the ‘Bugbear.B’ worm, which security experts called the first Internet attack aimed directly at the financial services industry.

Bugbear contains a list of nearly 1,200 Internet addresses for some of the world’s biggest banks, including American Express, Bank of America, and Citibank. Bugbear was designed to tell if its victim used an email address that belonged to any of those financial institutions, and then steal passwords to make it easier for attackers to hack into bank networks. Bugbear surfaced in June and remains among Symantec’s Top Five list of most prevalent Internet attacks.

Source: Washington Post

Another reaffirmation of this disturbing trend is that hackers are now using ‘zombie’ effected PC’s across the globe as personal ‘armies’ to extort ‘protection money’ from online gambling organisations and other companies that rely exclusively on Internet presence for their revenue streams, under threats of distributed denial of service attacks. We can expect this trend to continue as organised crime becomes more involved. That these attacks can be devastating is borne out by the crushing denial of service attack delivered by the recent MyDoom virus on the SCO web site. But more on this later.

These trends are not new. There were many warning signs delivered by leading analysts almost 6 months ago. We will examine some of the ‘Predictions for 2004’ to give us a better understanding of the evolution of these threats and how they are likely to affect us in future.

2.0 Predictions that were made for 2004

2.1 Gartner Report

Gartner made accurate forward looking observations in their December 2003 Report, titled *'Predictions for IT Security Directors in 2004'*.

Last year, the Dimension Data Global Security Forum (GSF) created and formulated the Intrusion Management Reference Architecture (IMA). The Gartner report provided us with confirmation that we were on the right track, with the right strategies, right timing and right partners and product sets on the IMA to capitalise on 2004 growth phase and expand our market share and leadership position in the security space. This report aided greatly in positioning the IMA and showing customers they were on the right path with the IMA strategy.

Some interesting excerpts from the Gartner report:

Gartner

“During the past year, most organisations have learned that perimeter firewalls, antivirus software and intrusion detection systems are not enough to protect them from cyber attacks. Attacks have moved to the application level, circumventing network-based firewalls. ‘Worms’ propagate so quickly that signature-based antivirus protection is useless. Intrusion detection systems do not provide protection – only faster notification that your security has failed.”

“Prediction – Enterprises that implement a vulnerability management process will experience 90 percent fewer successful attacks than those that make an equal investment only in intrusion detection systems.”

“By first-half 2004, 90 percent of Global 1000 enterprises will experience an internal network disruption from a legacy worm or Trojan horse that gained entry through a personal or contractor system (0.8 probability).”

Source: Gartner

An interesting corroboration of the above statements came from the Vanson Bourne Global IT Security Report for 2003, a survey conducted during July and August 2003. Vanson Bourne interviewed, on behalf of NetScreen Technologies, Inc., over 1,380 IT managers around the globe about their organisation’s network security from both a current and a future perspective.

Which threats are you most fearful of creating havoc within your network?

Trojans/Worms	63%
Email/Web Attacks	53%
Database attacks	34%
Exploit known vulnerabilities	29%
Denial of service attacks	26%
Port/Network scans	19%
IM/Peer to peer attacks	16%
IP Spoofing	16%

The report concludes, among other things:

“Organisations are more concerned about attacks at the application level (trojans/worms, email/web attacks, database attacks, threats that exploit known software vulnerabilities) as they see them increasing in frequency and carrying significant threat. Meanwhile, they feel that their current security solutions are inadequate to protect against these application-level attacks.”

Source: Vanson Bourne/NetScreen Technologies

The December 2003 Gartner report concluded:

“The ideal form of protection requires hardened, locked-down server and desktop configurations with near-real-time patch deployment. However, most corporate systems are not, and will never be, locked down or hardened. Real-time patch management at the server level will never materialise. Therefore, a layered approach is required that shields vulnerable systems from attack during the vulnerability mitigation process.”

“Action Recommendations for 2004: Delay large investments in intrusion detection systems and event management, and pilot application defence and network intrusion prevention products. Harden critical servers with best-practice configurations and host intrusion prevention software.”

Source: Gartner

Looking at all the above statistics, we can only come to one conclusion:

**In today’s world there are only three things you can be certain of for 2004, namely:
“Death, Taxes & the proliferation of ever more sophisticated worms & malicious code”**

2.2 The Vanishing Perimeter

In October 2003 Dimension Data released a paper entitled 'The Multilayer Perimeter'. This paper discussed the fact that organisations' own networks could no longer be trusted and were an alternative source of compromise, even if the perimeter had been completely secured against worms. It discussed 'worm containment' on large campuses using a 'worm containment solution', as well as recommendations on segmenting the network into multiple trust zones. *The Multi-layer Perimeter – Dimension Data White Paper, October 2003* highlights the problem about internal network worm infection well.

In January 2004 Gartner released another report entitled "Scan, Block and Quarantine to Survive Worm Attacks". This report drew similar conclusions the Dimension Data White Paper in terms of the perimeter changing. It focused on the emerging 'scan and block' technologies, both from a point solution and from a network infrastructure perspective.

Scan and Block: "As soon as infected PCs attach to the internal network, worms can infect vulnerable internal PCs and servers within minutes. Because some internal PCs and servers will always be in vulnerable states, security policies must be enforced before network connections are established. The basic protection requirement is scanning the system as it attempts to connect to the network, and blocking the network connection if the scan discovers missing patches, out-of-date antivirus signatures, or a misconfigured or missing personal firewall. Scanning after a full network connection is established is too late, because attacks from a corrupted system can begin immediately at connection. Opportunities to deploy a scan-and-block process will vary based on whether the system is managed by the enterprise, as well as the method of connection. Thus, multiple scenarios must be explored."

Source: Gartner

On the point solutions options, they commented:

"Scan-and-block technology for direct LAN connections can be implemented in various ways. Sygate has announced an internal gateway approach, while companies such as ForeScout Technologies, Mirage Networks, Silicon Defence and Wholepoint Security Solutions are developing innovative approaches to detect, isolate and block infected nodes to prevent propagation. InfoExpress has a product for scanning PCs that request IP addresses and can block IP address assignment, if a PC appears to be infected or doesn't meet the enterprise's security policy."

Source: Gartner

On the network infrastructure solutions options, they commented:

“The best way to extend perimeter security across the internal network would be to have these security features built into the network and node infrastructure. Because Cisco Systems dominates the enterprise network, and Microsoft dominates the enterprise PC and server operating system arena, what these vendors do, and the speed at which they move, will be critical. Cisco has announced the Network Admission Control (NAC) program, which is an initiative to establish scan-and-block functionality within Cisco infrastructure. To be effective, NAC requires the presence of the Cisco Trust Agent on the scanned PC, which limits its use for unmanaged and non-Windows devices (see “Cisco’s New Program Is a Good Start to More Secure Networks”). Microsoft has spoken about its plans to enhance its limited Windows 2003 Server Network Access Quarantine capability. Future Gartner research will analyse these two approaches.”

Source: Gartner

The report observes:

“Because of the danger of blended threats to internal networks, evaluate scan-and-block solutions now, rather than waiting for the infrastructure vendors to fully develop their products.”

Source: Gartner

Note: Cisco recently announced their NIC (Network Infection Containment) initiative. This will address the issue of unmanaged desktops, and is likely to be a behaviour based IPS type solution to suppress and contain infection within a network (Similar to ForeScout, WormScout and Checkpoints’ Interspect).

3.0 New for 2004 and beyond: MyDoom

3.1 Worm Description

This sophisticated, well-engineered mass mailing worm (actually a virus!) propagates itself by carrying its own mail server and by taking advantage of Kazaa peer-to-peer file-sharing installations. It comes in a small 22-Kbyte package that can infect many machines before being detected. It only infects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003 and Windows XP systems.

The worm is carried by email attachments, and when the attached file is executed, the worm scans the user's system for email addresses (harvesting) and forwards itself to those addresses. If the victim has a copy of the Kazaa file-sharing application installed, it will also drop several files in the shared-files folder in an attempt to spread that way.

The worm also installs 'Trojan horse' software that could enable unauthorised parties to use targeted Windows-based PCs as servers. When a computer is infected, the worm will set up a backdoor into the system by opening TCP ports 3127 through 3198, which can potentially allow an attacker to connect to the computer and use it as a proxy to gain access to its network resources.

According to Symantec, the worm also installs a 'key logger' that can capture anything that is entered, including passwords and credit card numbers.

The worm performed a Denial of Service (DoS) on SCO Systems services which started on 1st February 2004. The worm was programmed to cease replication on 12th February 2004. These two events would only occur if the worm was run between or after those dates. The worm stopped spreading on February 12, 2004, but the backdoor component has continued to function after this date. It is this back-door function that is the most cause for concern.

3.2 Difference between a worm and a virus

It is important to understand the differences between worms and viruses as their terms are often misused or interchanged which causes confusion. Viruses [MiMail, SoBig and MyDoom] are typically propagated by attachments, more often than not through email. They require some action on behalf of the user (opening the mail or attachment) to start the infection process. Self-replicating worms [Slammer, Blaster and Nachi] on the other hand don't require specific user action and can propagate and exploit vulnerabilities on their own, either at the application level or network transport level. Viruses have the ability to 'morph' into worms after infection, a so-called 'blended threat'.

3.3 MyDoom Propagation Speed

The worm was first detected on Monday 26th January 2004. In the first 36 hours, it had infected over 100 million emails, prompting the F.B.I. and the U.S. Secret Service to launch investigations. Massive spreading of the worm slowed down performance of the top 40 U.S. business websites by Monday afternoon.

By Tuesday 27th January, MyDoom had reached more than 160 countries and, at one point, had represented more than one-tenth of all email traffic worldwide. By contrast, Sobig-F, the most virulent worm topping the charts of last year, topped out at one in every 28 messages.

The SCO Group Inc. said, on Tuesday 27th January 2003, that it was experiencing a distributed denial-of-service (DDoS) attack apparently related to the Novarg/MyDoom worm that first appeared Monday. They offered a reward of up to \$250,000 “for information leading to the arrest and conviction of the individual or individuals responsible for creating the MyDoom virus.”

On Tuesday 27th January, Symantec upgraded the worm to a Category 4 Threat (Severe) whilst Network Associates had rated it ‘High Risk Outbreak’ on AVERT.

On Wednesday 28th January, anti-virus and Internet security firms were warning of a new variant to the MyDoom worm, and this time the author had it wired to not only launch a denial-of-service attack against SCO Group Inc.’s website, but against Microsoft.com as well. The new variant, known as MyDoom.B, began to appear late Tuesday. Its threat level was raised by many anti-virus companies from low risk to medium risk by Wednesday afternoon.

While MyDoom.B is similar to the earlier version – aside from adding Microsoft to its denial-of-service list – it also attempts to block users from being able to access 65 Web sites run by anti-virus and security companies, security firm iDefense Inc. said in an advisory. This means that infected machines would not be able to receive anti-virus updates and would therefore result in untold aggravation for network administrators.

iDefense’s advisory also theorised that the new version could be using computers infected with MyDoom.A to help itself spread. The new variant apparently evades detection measures for the original virus.

The trend of virus writers tweaking viruses and worms to quickly produce new, more-destructive variants is gaining momentum.

By late afternoon Friday 30th January, MyDoom.A accounted for 30% of all email traffic globally with an estimated one to four million infections.

On Monday 9th February, after unsuccessfully trying to defend itself from a massive denial of service attack from infected PC’s, the SCO site was taken offline.

Many analysts predict that due to the size of the infection, the effects of the MyDoom virus and its variants are likely to be with us for many months. And then of course there is the back-door...

This makes the MyDoom outbreak one of the fastest-spreading attacks in history and may also prove to be one of the most dangerous and lingering.

Whilst initial indications are that the damage from the worm may run close to \$1Bn, it is limited to the slow down of public and private network infrastructure, mail server resources and performance, and the costs and effort associated with cleanup. This is in contrast to Blaster and more specifically Nachi, which had more direct devastating effects on customers networking infrastructure and servers.

3.4 The Threat

MyDoom may be an attempt to create a large population of 'zombies' – infected PCs that can be used as servers in future attacks. A coordinated zombie attack against public systems could cause extreme damage and enable the attackers to commit password or identity theft on a massive scale. In a report released on 28th January, entitled 'How to limit Damage from the MyDoom Worm' Gartner states that:

“Behavioural changes likely offer the only direct indication that such an attack is under way.”

Source: Gartner

Users are still dealing with inboxes crammed with copies of the MyDoom worm, but the greater danger lies in the ports the worm leaves exposed once a system is infected. On 29th January, hackers were already scanning for the ports opened by MyDoom and would be able to upload any kind of executable code to infected systems.

The ability of a mail-borne worm to infect and open up TCP based vulnerabilities for other hackers and/or malicious code to exploit brings a new definition to the word 'blended threat', and is what makes this worm particularly dangerous.

The 12th February DOS attack did clog up certain corporates, network infrastructure and internal networks, and slow down PCs.

4.0 Recommendations

4.1 Gartner Recommendations

The Gartner report 'How to Limit Damage from the MyDoom Worm' states that they believe that this type of 'blended' attack is "now one of the fastest-spreading attacks in history and may prove to be one of the most dangerous as well". They conclude that it is:

"The most serious malicious-code threat facing enterprises."

Source: Gartner

And their predictions from last year are coming true.

Gartner recommends limiting damage from the MyDoom worm by *immediately*:

- ▲ Quarantining all incoming mail containing attachments until desktop and email anti-virus signatures have been updated
- ▲ Scanning all Windows PCs to detect any Trojan horse programs that have been installed
- ▲ Blocking most attachments to external email
- ▲ Reviewing exposed systems for vulnerability to coordinated zombie attacks
- ▲ Seizing the opportunity to remove any unauthorised file-sharing applications, such as Kazaa, which cause continual security exposures.

Furthermore, they state:

"In the long term, move to intrusion prevention systems (IPS) at the perimeter to block attacks of this type, and augment reactive, signature-based antiviral protection with host-based intrusion prevention (H-IPS) on all PCs."

Source: Gartner

4.2 Dimension Data Recommendations

Dimension Data support the above sound recommendations for customers. This is reflected in our global IMA strategy, which was developed last year. (See Intrusion Management Architecture – Dimension Data White Paper, September 2003)

With our own direct customer experience on some of the more 'emerging' technologies, we offer additional recommendations.

4.2.1 IPS ready for prime time

We are more bullish about IPS technology and believe this to be ready for prime time. As a minimum, we urge customers to start piloting this technology directly after having followed Gartner's immediate recommendations.

We have had success with *ForeScout* in the field and high levels of customer satisfaction. For those customers seeking a painless, non intrusive, quick and cost effective solution at the perimeter, we recommend installing ForeScout's ActiveScout IPS, the industries first and only 'non-inline' IPS.

For those customers seeking a more complete solution, and have the time and budget for a more complex installation process and more sophisticated technology, we recommend installing an Enterprise Inline IPS such as *Intruvert* or *Tipping Point*. Our vindication of this is based on over 13 successful deployments we have had in the US and a recent findings report from research group NSS, Europe's foremost independent network and security testing organisation. They have completed the industries' first exhaustive tests of enterprise class inline IPS systems. The executive summary on the report declares:

"There are network-based intrusion-prevention systems that work so accurately and so reliably that network managers who decline to even consider using them out of worry of IPS generating false positives or in-line equipment crashing must now seriously re-think that position."

Source: NSS

Excerpts from a Network World article summarising these findings are in Appendix-A.

4.2.2 Internal Security

We also feel that we support the Gartner 'Scan & Block' recommendations as part of an overall bolstering of internal security measures. The first part of the *The Multi-layer Perimeter – Dimension Data White Paper, October 2003* clearly spells out the threat and experience from Blaster and other 2003 Worms that highlighted the need for a re-think in internal security. Customers should be encouraged to start bolstering their **internal security** with the following measures:

- ▲ Log collection and correlation tools to detect and report on anomalous activity from within the enterprise (Network Intelligence or NetForensics) that may arise from both email-borne viruses and self-replicating malicious code as well as to detect internal DDoS activity.
- ▲ H-IPS on all critical servers and high-risk laptops (Cisco CSA).
- ▲ Where practical, H-IPS on every desktop (Cisco CSA)
- ▲ Worm detection, containment & suppression technology on large campuses (ForeScout, WormScout or Checkpoint Interspect) as described in the second part of *The Multi-layer Perimeter*.

Additionally we feel that aggressive, ongoing **user-awareness programs** will go a long way as part of a pronged defence tactic. In the long term, we recommend all the modules of the Intrusion Management Architecture as part of a multilayered threat management strategy, especially an ongoing Vulnerability Management programme.

5.0 Déjà Vu – Blaster Version 2.0?

On 10 February 2004, Microsoft acknowledged a critical security flaw in all versions of the Windows operating system. The vulnerability affects a technology called abstract syntax notation (ASN), which enables computers to share data and is used by many Windows security processes. eEye Digital Security reportedly informed Microsoft privately about the ASN flaw in July 2003 to give the company an opportunity to take remedial action. A patch for the flaw is now available at Microsoft.com

On Thursday 12th February 2004, Gartner released a public report entitled 'Prepare for Yet Another Critical Windows Vulnerability', referring to "A huge security flaw, which Microsoft has known about since July 2003, means enterprises must once again block and patch all Windows servers and PCs."

Gartner's first take on this is summarised as:

Gartner believes this latest Windows vulnerability — a 'Very High' risk, according to their Internet Vulnerability Risk Rating Methodology — presents attackers with the opportunity to unleash another MSBlast-class worm outbreak.

Many Microsoft and third-party components use the ASN module. It is remotely accessible through multiple ports and vulnerable to direct execution of attachments.

Enterprises must once again undertake the extremely expensive process of patching all Windows-based PCs and servers.

Source: Gartner

No sooner has the globe had to contend with the MyDoom mass-mailing virus (where direct damage was mainly limited to time, computing bandwidth and resources and nuisance factor for corporates), when the threat of a self-replicating worm as damaging as Blaster is now bearing down upon us. Being a self-replicating threat, it can cause far more direct damage to PC's and Servers than mass mailing worms, as witnessed by Blaster last year. However, direct damage is not to be confused with the potential threat posed by MyDoom, which could easily itself turn into a self-replicating threat.

Gartner Recommendations

To avoid the mass attacks that will almost inevitably attempt to exploit this vulnerability within the next few weeks, enterprises must immediately:

- Install the Microsoft patch on all PCs and servers
 - Block vulnerable ports as they are identified
 - Configure enterprise firewalls correctly to limit exposure
 - Install personal firewalls on all PCs
 - Install intrusion prevention software (IPS) on all business-critical Windows servers
-

6.0 Conclusion

The events described in this paper can leave no-one in **ANY** doubt as to what we can expect for 2004 and beyond.

Enterprises are urged to start aggressive planning for solutions that address both:

- ▲ Email virus infection and propagation
- ▲ Self-replicating malicious code and worms.

Enterprises are also urged to look at solutions that address both:

- ▲ The perimeter (internet facing)
- ▲ The internal network.

For those organisations that possess large quantities of unmanaged desktops, contractors, remote workers, laptops and third party connections, or for organisations who will not have the logistics resources to implement a large scale patching, AV or personal firewall rollout programme, we offer the following suggestions:

Short term tactical measures

- ▲ Non-inline IPS at perimeter (*ForeScout ActiveScout*)
- ▲ Host intrusion prevention (H-IPS) on all critical servers and high-risk laptops (*Cisco CSA*).
- ▲ 'Scan and Block' technology (*Sygate, InfoExpress*) to supplement patch management
- ▲ Worm detection, containment & suppression technology on selected areas on large campuses and networks (*WormScout or Checkpoint Interspect*)

Medium term measures

- ▲ Inline IPS (*Tipping Point, Intruvert*) at the perimeter
- ▲ Correlation tools for SysLog collection and event correlation to detect and report on anomalous activity from within the enterprise (*Network Intelligence or NetForensics*) that may arise from both email-borne viruses and self replicating malicious code as well as to detect internal DDoS activity.
- ▲ Where practical, H-IPS on every desktop (*Cisco CSA*) to augment signature based AV
- ▲ Worm detection, containment & suppression technology on all areas on large campuses (*WormScout or Checkpoint Interspect*)

It is highly recommended as part of a long term program that enterprises start planning for a robust Armour, Patch and Manage approach to Server patch management and deploy best practices measures to ensure that endpoint PC patch management can be controlled and deployed from a single point. This is to ensure rapid response to patch releases with least disruption to your business.

7.0 Appendix A

NSS Group Inline IPS tests

"Lab test gives most IPS products high marks"

By Ellen Messmer, Network World Magazine, 26th January 2004

A comprehensive lab evaluation of six intrusion-prevention systems that automatically block attacks suggests IPS is ready for enterprise use despite concerns that false positives will lead to the blocking of legitimate traffic.

Network-equipment evaluation lab NSS Group lobbed a battery of high-speed attack and evasion tests for two weeks at network-based IPS appliances from Internet Security Systems, NetScreen Technologies, Network Associates, TippingPoint Technologies and Top Layer Networks. Separately, NSS tested one host-based product, Enterscept from Network Associates. All but NetScreen's IDP-500 won an 'approval' rating from NSS.

The results of the examination, among the first of its kind, indicate that network-based IPS in most cases performed flawlessly or near flawlessly – and network managers should abandon exaggerated worries about it. "These tests verify the stability of the IPS device under various extreme conditions," NSS concluded, adding, "The group of tests verified that network IPS will not block legitimate traffic and is capable of detecting and blocking a wide range of common exploits."

NSS has had extensive experience testing intrusion-detection systems (IDS), which, unlike the IPS offerings, are limited to monitoring for attacks. It took a year of planning to devise the test methodology for its first IPS evaluations, says lab director Bob Walder.

"It's very hard to establish a test regimen when creating a new group test from scratch," Walder says. "There is strong justification for our latest test methodologies to be adopted as de facto standards when testing these types of products."

NSS' lab used Spirent Communications' network performance analysis systems SmartBits SMB-6000 and SMB-600 to test IPS at up to multi-gigabit speeds, when the IPS could handle it.

NSS tested for load balancing of IPS and used the SmartBits SmartWindow and SmartFlow features to generate background traffic for the 64- and 1,514-byte tests. Avalanche and Reflector gear from Spirent simulated real-world network traffic with connection speeds, packet loss and browser emulation. This helped determine performance bottlenecks, if any, by setting up Web, FTP and other connections.

NSS tested for 1 million simultaneous connections at up to 1G bit/sec while throwing hundreds of different attacks at each IPS appliance.

The results can be obtained in a 300-page report at the NSS site www.nss.co.uk.

In most instances, the testing found IPS held its own against denial-of-service attacks, computer worms, evasion tactics such as 'Whisker' and other types of attacks.

"As an integral part of the network fabric, the network IPS device must perform much like a network switch. It must meet stringent performance and reliability requirements as a prerequisite to deployment, since very few customers are willing to sacrifice network performance and reliability for security," NSS says.

In most cases, the IPSs passed the test. However, as the report notes, there were a few instances where NSS came up with an attack that the IPS equipment didn't expect, causing a failure to detect the attack. NSS gave each vendor a chance to update its equipment for the new attack within 24 hours to detect and stop it. All the vendors except NetScreen managed to do this, according to the report.

Ajit Sanchetti, product line manager, attributed the problems NetScreen's IPS had in the tests to the fact that NetScreen had submitted beta code of new features. "We had some bugs that caused some problems in attack coverage and latency," Sanchetti says. He says it was a 'temporary setback' and that NetScreen believes it has fixed the problems and is eager to participate in future NSS tests.

The report underscores the fact that the IPS equipment under review relies on knowledge of attacks to stop them. That means that while IPS can respond accurately to known attacks, it's the fear of unknown attacks that might still concern users.

However, the NSS report sums up why network managers should consider a switch from IDSs that simply monitor to IPSs that block: "One point in favor of IPS when compared with IDS is that because it is designed to prevent the attack rather than just detect and log them, the burden of examining and investigating the alerts – and especially the problem of rectifying damage done by successful exploits – is reduced considerably."

8.0 Appendix B

References

1. Washington Post, "The Year of the Worm", 1 December 2003; 12:00 AM
<http://www.washingtonpost.com/>
2. TechWeb News, "Security Threats Will Continue To Plague Enterprises In '04", 26 November 2003 (1:47 p.m. EST), By Gregg Keizer
<http://www.techweb.com/>
3. Gartner Strategic Planning, SPA-21-6630, "Predictions for IT Security Directors in 2004", 8 December 2003, M. Nicolett
<http://www3.gartner.com/lnit>
4. Gartner Technology, T-21-7550, "Scan, Block and Quarantine to Survive Worm Attacks", 26 January 2004, M. Nicolett, J. Pescatore, J. Girard
5. Gartner Events, E-20-8177, "MSBlast and a Model for Threat Response", 19 August 2003, M. Nicolett, J. Pescatore, R. Stiennon
6. Gartner Note Number: FT-22-0911, "How to Limit Damage from the MyDoom Worm", 28 January 2004, John Pescatore, Martin Reynolds, Arabella Hallawell
7. Vanson Bourne Limited, "Global IT Security Report 2003", December 2003, On behalf of NetScreen Technologies, Inc.
8. Gartner First Take: FT-22-2096, "Prepare for Yet Another Critical Windows Vulnerability", February 2003, John Pescatore, MartinD. Stiennon
9. Network World Magazine "IT vs. the mischief makers" By Linda Leung, Network World, 22 December 2003, 12/22/03
<http://www.nwfusion.com/power/2003/1222mischief.html>
10. Network World Magazine "Lab test gives most IPS products high marks", By Ellen Messmer , Network World, 26 January 2004
<http://www.nwfusion.com/news/2004/0126ipstest.html>

Recommended Reading

1. Dimension Data "The Multilayer Perimeter", October 2003, Dwaine van Vuuren
2. Dimension Data "IMA Reference Architecture", October 2003, Dwaine van Vuuren

For more information or to obtain copies of these white papers, email dwaine.vanvuuren@za.didata.com or karen.pretorius@za.didata.com