Parliamentary Joint Committee on the Australian Crime Commission

Inquiry Into Cybercrime

Submission No:13
Received 9 May 2003
Mr John Donovan
Managing Director
Symantec Australia
Level2, 1 Julius Avenue
NORTH RYDE NSW 2113
☎02 8879 1105
E-mail: jdonovan@symantec.com

Symantec Australia
Submission to the Parliamentary Joint Committee on the Australian Crime Commission
Cybercrime Inquiry

Symantec Australia welcomes the opportunity to contribute to the Cybercrime Inquiry as part of our commitment to work with government and industry to make the global computing infrastructure safe and secure.

This submission focuses on:

- Symantec in Australia
- Cybercrime in Australia
- Protection of National Critical Infrastructure
- Private/Public Sector Co-operation Against Cybercrime
- Protection Against Cybercrime At All Levels

For further information about the contents of this submission, please contact:

John Donovan
Managing Director
Symantec Australia
Level 2, 1 Julius Avenue
North Ryde NSW 2113
Ph: + 61 2 8879 1105
email: jdonovan@symantec.com

or

Mina Silvestre
Government Relations
Symantec Australia
Level 2, 1 Julius Avenue
North Ryde NSW 2113
Ph: + 61 2 8879 1008
email: msilvest@symantec.com

Contents

1. About Symantec

Symantec is the world leader in Internet security technology[1]. We provide a wide range of security solutions to companies, government agencies and individuals around the world, including virus protection, firewall and virtual private networks, vulnerability assessment and management, intrusion detection, Internet content and e-mail filtering, remote management technologies and managed security services.

Symantec works with government and industries worldwide to help make the global computing infrastructure safe and secure. Symantec's range of products, services and research gives it the broadest view of the security landscape. Symantec's bi-annual Internet Security Threat Report is the most comprehensive analysis of global cyber-security trends. The malicious code activity results in the report were compiled by the Symantec Security Response which is based in Sydney.

Deleted: (is it relevant to mention that the malicious code part of the report is developed here in Sydney?)

Our commitment to partnership with governments internationally includes contributing expertise to government policy development, developing and delivering Internet security awareness programs and sharing information. In September 2002, President George W. Bush appointed Symantec's Global CEO and Chairman John Thompson to the National Infrastructure Advisory Committee (NIAC), to make recommendations regarding the security of the critical infrastructure of the United States. Symantec is also actively involved in the Information Sharing and Analysis Center in the United States whose role is to share, correlate, and analyse information in order to protect critical infrastructure.

Headquartered in Cupertino, California, Symantec has more than 4,000 employees in 36 countries. For more information, please visit www.symantec.com.

1.1 Symantec in Australia

Since the establishment of Symantec's first international office in Australia in July 1990, Symantec's operations have grown significantly. Symantec has more than 110 employees in Australia involved in Internet security protection strategies, research and development, customer service and support, sales and marketing.

The Asia Pacific Symantec Security Response lab opened in Sydney in 1997 to service the region. Its mission is to provide swift, global response to computer virus threats, proactively research and develop technologies that eliminate such threats, and educate the public on safe computing practices. The Sydney office also hosts a substantial Technical Support Centre with technicians and system engineers who provide local language support across Asia Pacific.

Symantec invests substantially in Australian IT research and development. This research includes antivirus research and development and research to support product development in the US. In addition, Symantec has a close working relationship with two Australian companies, PassMark and XtreamLok. Symantec has included Passmark's PerformanceTest software into our own web security solution and is currently using XtreamLok's Digital Rights Management software to reduce software piracy and ensure that Symantec's customers are receiving authentic software.

[1] Garnter "2001 Security Software Market Share" and IDC "Worldwide Internet Security Software Market Forecast and Analysis, 2002-2006: Vendor Views"

In March, 2003 Symantec launched a Security Operations Centre (SOC) in Sydney to provide Managed Security Services clients with security monitoring, management and response. Symantec's Managed Security Services practice offers a broad range of security services including monitoring and management of firewalls, intrusion detection systems, routers, VPNs, vulnerability scanners, antivirus and policy compliance to provide the most comprehensive security solution for its managed security services customers, independent of vendor relationships.

Symantec's long-term commitment to its Australian operation and willingness to partner with Australian companies is recognised through Membership of the Federal Government's Partnership for Development (PfD) program. Symantec was also awarded Graduate Partner status in the PfD program in 2001.

Recognising the importance of collaboration in the information technology industry, Symantec is member of the Internet Industry Association, Business Software Alliance of Australia and AusCERT.

Symantec's Australia/New Zealand Managing Director, John Donovan, was a guest speaker at the 2002 Prime Minister's Taskforce on Protection of Critical Infrastructure. He also continues to contribute his security expertise to industry forums and events.

1.2 From LoveLetter to Bugbear - A Case Study in Local Security Expertise

The VBS LoveLetter worm was detected on the night of May 4, 2000.

Symantec system engineers, account managers and communications teams worked directly with the Australian Symantec Security Response team to ensure the provision of up-to-the minute information to our partners, corporate customers and industry organisations in Australia and the Asia Pacific region.

All corporate accounts were contacted directly to alert them to the coming threat, and anti-virus definitions were proactively distributed within a few hours of the virus being detected.

With Symantec's support, IT management companies like IBM were able to protect the security systems of government departments and other client organisations before Australia woke-up and went to work on May 5. Due to the overnight discovery of the virus and the quick reactions of the Symantec team in Australia and New Zealand, a great deal of damage was averted.

Since then the Australian team has been at the leading edge of the industry in the analysis and development of solutions for most of the high profile computer viruses and worms; for example the, Klez, Nimda, CodeRed and Bugbear worms were all discovered and managed in Australia.

The most recent of these was W32.Bugbear, where the Australian team discovered, analysed, named and developed fixes for this high profile worm that was most prevalent in South East Asia.

2. Cybercrime in Australia: Analysing the Internet Security Threat

There is no question that cyber security issues are becoming more complex. Vulnerabilities are on the rise and blended threats doubled in number between July and December 2002 creating many more ways for a network to be attacked.

Malicious activity is increasing in complexity and in the potential damage it can cause. Interdependencies between organisations means the security chain can easily be compromised by weaker links.

Symantec's Internet Security Threat Report provides a comprehensive analysis of trends in cyber security activity over a six-month period. The latest February 2003 report is the result of analysis of more than 30 terabytes of data and covers network-based attack activity, vulnerability discovery, and malicious code.[2]

The report also found that damage caused by recent blended threats, such as Opaserv, was considerably less than that caused by old threats, such as Code Red. Mixed with the encouraging news, Symantec also documented 2,524 new vulnerabilities in 2002, an increase of 81.5 percent over 2001. Symantec believes that the possibility of future, high impact, blended threats continues to represent one of the greatest risks to the Internet community.

Additional key findings include:

2.1 Vulnerabilities Trends

- Symantec documented 2,524 new vulnerabilities in 2002, an increase of 81.5% over the prior six-month period. This sharp rise appears to be a function of factors, such as the responsible disclosure movement, greater media coverage, and possibly increased effort among vulnerability researchers.

- Moderate and high severity threats drove the growth of new vulnerabilities. The relative ease with which attackers are able to exploit new vulnerabilities remained unchanged over the past year. Approximately 60% of all new vulnerabilities could be easily exploited either because the vulnerability did not require the use of exploit code or because the required exploit code was widely available. However, of the subset of vulnerabilities that required the use of exploit

---

[2] Cyber attack trends are drawn from the analysis of attack data collected in real time from a subset of thousands of intrusion detection systems and firewalls. These sensors are deployed in more than 40 countries as part of the Symantec's Worldwide Managed Security Services Operations. Vulnerability trends are based on statistical analysis of the Symantec Response teams extensive vulnerability database, which houses more than 6,000 vulnerabilities affecting more than 13,000 distinct products. Finally, malicious code trends are based on analysis of information generated by Symantec's Digital Immune System, which draws submitted virus data from more than 100 million antivirus products.

Trends derive from the analysis of a broad range of threat data, using statistical techniques as well as interpretive commentary from industry experts. The first section of the report provides insight into major trends in threat exposure by analysing recently discovered vulnerabilities and malicious code.

code, only 23.7% actually had exploit code available in 2002, as compared with 30 percent in 2001.

2.2 Malicious Code Trends

- Blended threats, continued to constitute the most frequently reported threat. Blended threats combine the characteristics of two or more of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack.

- 80% of all malicious code submissions were caused by only three blended threats: Klez, Opaserv, and Bugbear. Further, 78% of all cyber attack activity detected by Symantec was related to both old and recent blended threats.

- While damage caused by more recent blended threats, such as Opaserv, was considerably less than that caused by old threats, such as Code Red, Symantec believes that the possibility of future, high impact blended threats continues to represent one of the greatest risks to the Internet community.

- Instant Messaging and Peer-to-Peer applications now represent a highly attractive propagation mechanism for future malicious code. The emergence of several new high-risk vulnerabilities coupled with relatively permissive usage policies and high market penetration are increasing the severity of this threat. Virus/worm writers have targeted these applications to spread high-impact blended threats.

2.3 Cyber terrorism

- There are many ways to define cyber terrorism because the term means different things to different people. Symantec has developed a white paper that includes some of the definitions associated with cyber terrorism and details how it impacts home computer users.

- Cyber terrorists (unlike conventional military attacks) can strike from any country in the world. Nobody knows if they will strike from the Middle East, the United States, Europe, or even from within one's own network. Even if it is possible to reliably isolate likely source countries, cyber terrorists can disguise their identities by launching attacks from a compromised system in another, less suspicious country or by obfuscating the attack through open proxies.

- Attacks from countries on the Cyber Terrorist Watch List accounted for less than 1% of all activity.

2.4 Cyber Attack Trends

- The majority of cyber attacks were launched from a relatively small number of countries. The top ten countries alone accounted for 80% of all attacks detected over the past six months. These countries in order of overall volume of attacks are the United States, South Korea, China, Germany, France, Taiwan, Canada, Italy, Great Britain and Japan.

- For the first time, the level of total cyber attack activity has decreased, falling 6 percent in the second half of 2002. Companies averaged 30 attacks per company

per week over the past six months, as compared to 32 attacks per company per week during the prior six-month period.

- Power and Energy companies continue to show the highest rate of both attack activity and severe event incidence. In addition, the no-profit and financial services sectors experienced an elevation in overall attack volume and severe event incidence, respectively.

- 85% percent of all attacks reported during the past six months were classified as pre-attack reconnaissance, while the remaining 15% were classified as various forms of exploitation attempts.

- Cyber attacks from Australia constituted less than 1% of all attacks over the past six months; and in terms of attacks per 10,000 Internet users, attacks from Australia were the fifth lowest among countries with more than 1 million Internet users**.** [From countries where Internet penetration is more established]. It should be noted that this data does not indicate how many of these attacks are made against Australia.

- As a country's Internet usage grows, the potential for compromise grows; this is illustrated by the rise in incidents from countries like South Korea, where incident reports grew 62% over the previous six-month period.

Further information about the Threat Report is found at Appendix 1.

3. Protection of the National Infrastructure

The potential of cyber terrorism or other Internet attacks on the national infrastructure to cause catastrophic disruption and destruction is increasing. However, to date, the most common threats actually arise from vulnerabilities or viruses that exploit these vulnerabilities, such as Bugbear, Nimda and CodeRed.

With more than 85% of the world's critical infrastructure owned and operated by private entities, public/private cooperation is critical to securing our critical data from the rising incidence and impact of malicious activity.

Initiating the effective protection of critical infrastructure involves consideration and implementation of fundamental Internet security best practices.

3.1 Best Practice Internet Security

Best practice information security for governments and enterprises involves:

- Establish security policies
- Risk assessments
- Standards, procedures, and metrics
- Security roadmap
- Selection and implementation of solutions
- Training of security professionals and employees
- Security management
- Incident response and recovery

3.2 International Security Standards

The ISO 17799 is an international security standard that contains 10 domains with suggested policies, procedures, and technological implementation methodologies. It is relevant to government as well as enterprise. Both government departments and enterprises should establish multi-departmental teams to design, develop, implement, and enforce corporate information security policies. These teams may be similar to teams established to prepare for Y2K and must reflect strong support of top management to be successful.

Within the enterprise, an Audit Committee can be created to shoulder the responsibility of ensuring that proper audit and control procedures are documented, implemented, and enforced. This committee can set down rules to co-ordinate security policies and procedures across the organisation, determining ways to implement best practise via technology, policies, procedures, and training.

4. Private/Public Sector Co-operation Against Cybercrime

Companies such as Symantec already play a vital role in the prevention and early detection of cybercrime and vulnerabilities. Symantec assists in alerting industry and government to threats, providing tools and advice on best practice for managing security threats and methods of recovery after an attack. Symantec is also very active in educating organizations and end users about security issues and prevention through Symantec Education Services and involvement in consumer activities such as National Cyber Security Day in the United States.

4.1 IT Security Alerts

Symantec's Virus and Security Alert Services deliver instant notifications of the latest virus threats, and network and computer vulnerabilities to any device anywhere in the world, 24 hours a day, 7 days a week. When a new threat or vulnerability is discovered, Symantec Security Response experts provide rapid emergency response, delivering up-to-the minute information and advice so that security staff can proactively stop the threat before it impacts the network.

Alerts are sent to one wireless device, as well as a back-up email. Customers may choose to be notified of all alerts, or a sub-set, based upon the threat category level selected for each wireless device. This service was initially setup and trialled in Australia for local customers before being adopted worldwide.

4.2 Informal Liaison With Crime Agencies and Beyond

Symantec has a long-term informal information sharing relationship with the Australian law enforcement agencies. For example, during the recent W32.Bugbear crisis, Symantec contributed to a seminar arranged for banking IT security professionals to discuss and learn about the threats and mitigation strategies of Bugbear. These relationships are maintained through informal discussions at security-focused events, telephone calls and where security is not a concern online via email.

Symantec welcomes recent Federal Government initiatives to improve liaison between the private and public sectors with the goal of improving security of national critical infrastructure.

While formal networks are important, too great levels of complexity can reduce efficiency. In Symantec' experience in Australia, informal information sharing networks can often work most effectively, even in highly competitive environments.

4.3 AusCERT

Symantec has an ongoing relationship with AusCERT, often sharing information about viruses and other computer security issues. Symantec led the initiative to create the Australian Anti-virus Research Forum (AAVRF) which AusCERT hosts and chairs. This is an electronic forum where security agencies and vendors can exchange time-critical information about computer-based threats.

Symantec supports initiatives such as the National Information Security Advice Scheme pilot. We believe that Australia's critical infrastructure protection relies on ongoing input from various organisations like AusCERT as well as Internet security vendors to deliver proactive, comprehensive and timely information about the very latest security threats.

This year, the Association of Anti Virus Asia Researchers conference is being hosted by Symantec in Sydney in November.

4.4 Become the Role Model for Enterprises and Consumers

There is no question that the need for improved security is as much an issue for the private sector as it is for the government. There is a role for government, in consultation with information security players, on best practices for both private and government departments and for consumers.

Symantec believes the Australian government has a role in sending out a clear message that securing its cyber security infrastructure is critical and that budgetary support must be part of the implementation of a cyber security strategy to be successful.

In addition, the Australian government should take a leadership position by ensuring all government departments conduct ongoing vulnerability assessments of their information systems and find better ways to protect those systems. Agencies would be required to utilise best practices to improve their information security. This could be cemented with the introduction of legislation requiring federal government departments to implement these measures.

4.5 Leverage The Expertise of Internet Security Companies

Governments can benefit from companies like Symantec that are at the forefront of Internet security and provide the latest Internet threat information and expertise. Symantec has also gained great expertise and played a pivotal role in helping to secure the critical infrastructure of countries around the world. We would welcome greater outreach from the Australian Federal Government to security vendors on national Internet security initiatives and programs.

4.6 Corporate Responsibility For Information Security

CEOs, Boards of Directors, and Corporate Executives are increasingly being held personally accountable for the business needs of shareholders, customers, and employees. The growing reliance on the Internet as a way of doing business has resulted in a dependency imperiled by dangers from both within and without the organisation's information technology infrastructure. Organisations must defend against today's threats and have the resolve to prepare for and respond to future threats. They must rely on trusted suppliers of integrated and complementary information security products and services to ensure the long-term viability of the organization.

Enterprises should be encouraged to be accountable for delivering adequate information security protection through the reporting of their information security posture to the Australian Security and Investment Commission provisions and in their own annual reports.

The Australian Federal Government, with help from security vendors, must continue educating enterprises about the imperatives of implementing and maintaining adequate information security measures for their information technology ecosystem. Enterprises must vigilantly incorporate the management of information security protection as part of their ongoing responsibility to shareholders, partners and employees.

5. Protection Against Cybercrime At All Levels

While protection of the national infrastructure understandably is attracting increased attention, there are many aspects of cybercrime at other levels that can significantly damage the national online economy and beyond.

Consumer education about simple security measures is vital to protect against online fraud and cybercrime. Every personal computer with an Internet connection is an onramp to the information superhighway, and therefore a potential security threat.

In the United States, the National Cyber Security Alliance, a group of businesses and government organizations, including Symantec, that have aligned to educate consumers on the importance of protecting PCs from online intruders, has also chosen daylight savings as a time to encourage consumers to conduct twice-yearly checks of their home computers' security.

Locally, Symantec has created a program to leverage National Cyber Security Day reminding consumers to check their PC security when they adjust their clocks. To make this easy, Symantec has a free Security Check service available online. We would encourage a similar Cyber Security Day to be established in Australia via collaboration between government and industry.

5.1 Educating Employees

Many employees in today's workforce are not aware that they play an important role in their organisation's security. They download programs from the Internet, open unsolicited e-mail attachments, participate in file-swapping programs, engage in instant messaging, and neglect to update passwords and antivirus protection – all activities that could put the corporate network at risk.

Symantec has launched a comprehensive, measurable training and communications program designed for organisations to implement over the course of one year to increase employee security awareness. The program enables organisations to improve security posture by reducing information security risk posed by employees.

The Symantec Corporate Security Awareness Program provides participating organisations with materials on CD-ROMs that include recommendations for program implementation, electronic files of printed materials that can be used to internally promote and support the success of the initiative, technology-based security awareness training modules, as well as mechanisms to measure and track the participation and progress of employees. The program aims to empower all employees to take an active role in the protection of their organization's resources.