ENTERPRISE WIDE INCIDENT RESPONSE COORDINATION v1.0

CASE STUDY

Practical assignment for SANS GIAC
Security Essentials Certification (GSEC)
Version 1.4b
Option 2 – Case Study in Information Security

By Robin Palaje

Submitted Date: 18 June 2004

Abstract

This case study examines the process of coordinating the response to a large scale incident in an enterprise sized, technology diverse, educational government organisation. In July 2003 the organisation suffered a Blaster then Welchia virus outbreak resulting in a Distributed Denial of Service (DDoS) attack on its network and a loss of service at some point of all network dependant services and applications. I was appointed the incident coordinator and it was my role to manage the incident and its impact. At the time of the incident, I was employed with the Information Security Unit (ISU).

Background

The large educational government organisation involved in this case study consisted of:

- over 2,000 state wide educational institutions, colleges and corporate sites
- over 100,000 desktops and servers
- over 1,000,000 educational and corporate users and staff
- all sites connected via the organisation's Wide Area Network (WAN) which is supported by the organisation's Network Unit
- a WAN with no distinct segmentation or data flow controls between educational and corporate networks
- diverse hardware and software desktop and server platforms, including but not limited to various versions of Microsoft Windows, Apple Macintosh, Novell Netware, VMS and UNIX
- connection to the Internet and other external networks that were in the main accessed via a central corporate firewall infrastructure
- no formal information security policy or governance body and a general low level of security awareness

A key aspect of the organisation was that educational institutions (which accounted for over 90% of the organisation's sites) and college sites were effectively autonomous from the rest of the organisation and each other, but still came under the organisation's auspices. From an Information and Communications Technology (ICT) perspective, this effective autonomy resulted in:

- educational institutions managing their own Local Area Networks (LANs) and ICT infrastructure
- varying ICT standards throughout educational institutions
- externally sourced or temporary ICT support throughout educational institutions
- college sites with their own permanent ICT support structure and standards
- corporate ICT support units providing informal assistance to education institutions and colleges as required

The major information assets and services of the organisation consisted of student details and the delivery of on online learning, corporate and external workplace collaboration systems.

Factors Leading Up To The Incident

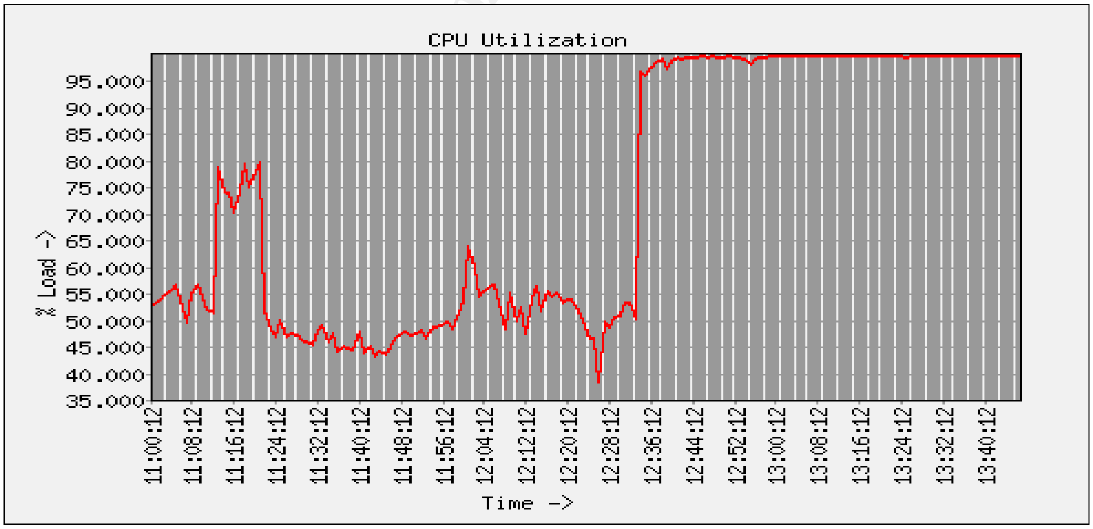
On June 2003 Microsoft posted 'Microsoft Security Bulletin MS03-026', a severe DCOM RPC vulnerability and recommended that its customers patch their systems to mitigate risk against this vulnerability [1]. Since the organisation's environment included tens of thousands of these affected systems, the organisation's ICT support staff began the lengthy process of patching these systems. In early August 2003, computer security services worldwide started to report the existence of exploit code for this vulnerability in the wild and warned of the potential development of a computer virus that could result in a similar impact to the Code Red virus [2]. It was at this time that ISU alerted educational and corporate ICT support units to the potential security risk, and recommended mitigation steps for responding to the Microsoft Security Bulletin.

A few days after, several anti virus vendors began reporting the existence of the Blaster virus which exploited the vulnerabilities as detailed in MS03-026 [3]. The next day, the Blaster virus had worked its way into the organisation's systems. The Blaster virus was detected across both corporate, and to a much larger extent, educational environments. In order to contain the educational institutions virus outbreak from affecting the rest of the organisation, port 135 WAN access for educational institutions was blocked at each educational institutions router by the organisation's Network Unit, as recommended by anti virus vendors [4]. In addition, a letter from our corporate ICT Unit was sent to the heads of educational institutions alerting them to the potential security risk and mitigation steps for responding to the Blaster virus.

Incident Details

In mid August 2003, after the release of the Blaster virus, anti virus vendors began reporting the existence of a new virus, related to the Blaster virus, called Welchia [5]. The organisation's Helpdesk Unit then reported instances of the Welchia virus being detected throughout the organisation by our corporate anti virus software. Infected systems were rebooting and the network was performing very slowly. The following morning, the organisation's Firewall Unit reported an unusual increase in network traffic on the external services networks, with the firewall processing ICMP packets at a rate of over 1,000 hits per second. CPU usage had also increased from around 50% to 100% as 'Figure 1' (see below) supplied by the organisation's Firewall Unit graphically shows.

Figure 1



This saturation of the firewall immediately negatively impacted the availability of external services such as Internet DNS, web browsing and e-mail.

In order to alleviate the issue on the firewall, our Networks Unit applied an ACL on the network internal border router. This control, applied around midday, saw this device then become saturated with packet hit counts over a 2.5 hour period. Our Networks Unit provided a router log extract which I have summarized and tabled as

‘Figure 2’ (see below). This information also revealed the type and level of traffic flowing across the organisation’s WAN trying to reach external networks.

Figure 2

Control	@Count	Source IP	Source Port	Target IP	Target Port	Type	Threat Type
Deny	17,000	Any	any	Any	41170	UDP	Blubster
Deny	13,500	Any	any	Any	1863	TCP	MSNP
Deny	5,500	Any	any	Any	1214	TCP	Kazaa
Deny	8,500	Any	any	Any	6346	TCP	Gnutella
Deny	121,035	Education Institutions	any	Any	135-139	TCP	Blaster/ Welchia
Deny	6,400,000	Colleges	any	Any	135-139	TCP	Blaster/ Welchia
Deny	110,000,000	Education Institutions	any	Any	135-139	ICMP	Welchia
Permit	5,000,000	Any	any	Any	Any	IP	None

It now became apparent that the Blaster and Welchia virus outbreaks had caused systems instability on infected systems, a DDoS on the organisations network and a loss of Internet services. It was at this time that the organisation’s ICT support manager organised a crisis meeting within the ICT Unit to handle the virus outbreak.

The meeting resulted in recommending the appointment of a central incident coordinator from ISU to be responsible for the management of the incident response process.

Incident Response Procedure

The organisation’s information security incident management policy and procedure was being development at the time by ISU. The main incident management references used in the development of the procedure and for handling the incident included the following publications:

- Stephen Northcutt, ‘Computer Security Incident Handling’, Version 2.3.1, SANS Press, March 2003 [6]
- Danny Smith, ‘Forming an Incident Response Team’, AusCERT, 1st January 1995 [7]
- Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle and Mark Zajicek, ‘Handbook for Computer Security Incident Response Teams (CSIRTs)’, 2ND Edition, Carnegie Mellon Software Engineering Institute [8]

The lack of formal process resulted in a process that could best be described as in its initial stage of development and therefore ad hoc [9]. The process closely followed a phased approach as outlined by, Stephen Northcutt, ‘Computer Security Incident Handling’, Version 2.3.1, SANS Press, March 2003, but was modified to deal with the large scale of the incident as follows:

- preparation phase – There was virtually no time for preparation, so the usual tasks associated with this phased such as assigning responsibilities, listing key contacts and establishing a reporting chain, were performed in the identification phase.
- identification phase – logging initial incident reports, analysis of these reports, deciding on an initial strategy in order to respond appropriately to the incident and escalation of key issues to senior management
- containment phase – preventing the spread of the incident
- eradication phase – removing the means that led to the incident occurring
- recovery phase – restoring systems and information assets to a normal state
- follow-up phase – learning from the incident, recommend action to prevent its recurrence, improve general incident response and provide an incident report to the organisation's CIO

Preparation Phase

For this incident, there was virtually no traditional preparation phase. No formal organisational information security incident policy or procedure existed. The standing incident response team consisted of ISU, which consisted of two staff, myself and the manager who was on leave at the time.

Identification Phase

Reports of unstable windows systems and slow network performance were arriving at the Helpdesk, Networks and Firewall Units. Snapshots of these reports were being escalated to me. These reports coincided with the detection of the Welchia virus within the network.

Identifying the Welchia virus as the main cause of the network problems was made easier due to the fact that ICT support and I had already spent time researching the Blaster virus and analysing its affect on the organisation's network. Although both viruses used the DCOM RPC vulnerability to propagate through port 135, it was Welchia's target discovery behaviour that was found to be generating most of the network traffic. The Welchia virus would create an IP address range to target, as would Blaster in a different manner, but Welchia would then PING the potential target to determine its active state [10]. It was this PING traffic that was saturating the organisations network as each infected computer could potentially start a PING process through a whole range of Class B sized networks [11]. Other Welchia virus generated traffic was deemed trivial in comparison to this issue at the time.

Initially, advice on handling the incident was coming from all areas of the organisation. This was leading to confusion about technical details of the virus, its impact on the organisation and incident management of the virus. As stated earlier, the organisation's support manager organised a crisis meeting within the ICT unit to handle the virus outbreak. After the incident crisis meeting recommended that I be appointed incident coordinator, I requested that the CIO endorse the appointment. This was necessary as the organisation had no formal incident response procedure.

I advised the CIO of what the incident coordinator role and authority should involve, including:

- coordinating the organisation's combined effort in containing and eradicating the incident impact and cause
- participation in any key incident related decision making process
- authorisation to take appropriate action where standard operating procedures fail due to the impact of the Welchia virus,

and requested that the role of ICT unit managers be outlined to include:

- advising the coordinator of action being taken to counter the virus
- having all related correspondence intended for distribution to users, support staff and management reviewed by the coordinator
- providing a copy of all incident related correspondence and statistics to the coordinator
- using the coordinator as the central point for key related inter ICT Unit communication
- escalating any further key incident issues to the coordinator
- providing technical resources and input as required

It was also important to state that these processes did not override standard problem reporting via the Helpdesk Unit. This measure would help to ensure that I did not directly receive first level support requests from users.

I created a list of incident contacts including Helpdesk, Desktops, Servers, Networks, Applications, Software, Firewall, educational institution and college ICT support staff. I also provided a twice weekly report, informing relevant ICT managers and ICT executives of the incident status. I also kept a copy of all incident related correspondence for future reference.

There was no involvement with law enforcement with this incident.

Containment Phase

With the outbreak of the Blaster virus, port 135 was being blocked at all educational institution routers for containment purposes. It was observed that educational institutions did not require communications over this port at the time so operations would not be greatly affected by this control. There was also some doubt if educational institutions could respond quickly and effectively to the incident as no full time ICT support existed at these sites so it was important that these sites were contained. The Networks Unit was reporting that traffic from educational institution subnets appeared to be accounting for around 90% of affected systems and virus related traffic.

It was not possible to block port 135 for colleges and corporate sites as systems on these sites required this port open for Windows networking and authentication, to access desktop systems and shared resources. These sites were, in the main, supported by specialised ICT support staff. Automated and managed anti virus and software deployment systems were also implemented at these sites. They were expected to respond quickly to the incident and did so.

With the outbreak of the Welchia virus, I authorised the blocking at all educational institution routers of PING traffic to contain the effects of the virus on the WAN. There was a slight delay with this implementation as the port 135 router change was still being processed. The Networks Unit advised that each WAN router change process would take around 3 days to complete. The blocking of PING traffic resulted in PING no longer to be able to be used as WAN troubleshooting tool.

These steps resulted in containing the majority of worm related network traffic to local educational institution LANs, thereby protecting the rest of the organisation from DDoS. In addition, most of the organisation's WAN and Internet services were returned to normal.

Eradication

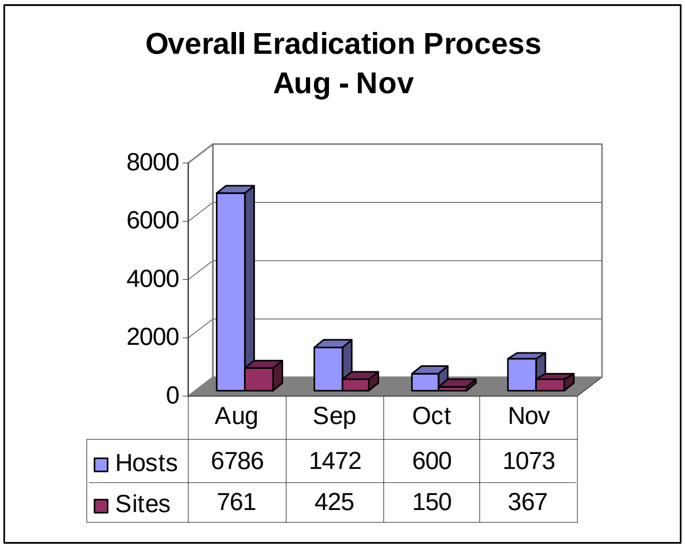
Eradication of the incident involved removing the Welchia and Blaster viruses from affected systems using the organisation's anti virus vendor supplied Welchia and Blaster virus removal tools. In order to prevent incident reoccurrence, I requested that all vulnerable systems have real time anti virus software and the Microsoft MS03-026 patch installed. This process was enabled by:

- establishing one point within the organisation as a high level technical authority in regards to the incident, the organisation's Software Unit
- using the Intranet and e-mail to make available the technical process to eradicate the Welchia an Blaster viruses and protect affected systems from reinfection
- provide educational institutions with additional technical support using information kits containing a CD with software and documentation
- ensuring that college and corporate units, which had failed to maintain their automated software deployment systems, had addressed this oversight and had updated and tested their systems accordingly

Since only around 10% of the organisation was using managed anti virus systems, it was decided to measure the incident using the number of un-patched MS03-026 systems as an incident metric. The organisation's Network Unit first used Microsoft's patch scanning tool, but I soon receiving reports that this tool was producing false positives with Windows 98 systems that were not affected. This behaviour seemed to be confirmed by a similar report appearing on the SANS Internet Storm Center [12]. After further research, the Network Unit implemented Internet Security Systems (ISS) scanning tool scanms.exe to detect vulnerable systems [13]. The Network Unit then provided the results of these scans to me twice a week.

Once the load on the networks routers began to decrease due to virus eradication, the organisation's Networks Unit began to provide more accurate virus statistics from the routers by monitoring traffic identified as virus related, which I have collated and tabled in 'Figure 3' (see below). Note the rise in statistics in October. This could be mainly attributed to the use of router logs for providing statistics and an implementation by educational institutions of new computers that were not MS03-026 patched prior to installation on the network.

Figure 3



	Aug	Sep	Oct	Nov
▨ Hosts	6786	1472	600	1073
■ Sites	761	425	150	367

Due to the large number of sites affected and limited ICT support resources involved, I decided on a strategy of reducing the number of infected systems at the worst affected sites as a priority. This would allow for the maximum use of ICT support resources and cause less support logistical issues. The worst 150 affected sites were identified from the network scans each week. All support staff responsible for those sites were requested to eradicate the virus and protect systems as a priority. This strategy seemed to be working well as there was a major reduction of affected systems (see ‘Figure 3’).

The point of entry of the virus was virtually impossible to ascertain due to the large number of non anti virus protected access points to the organisations WAN. Possible entry points included:

- over 2,000 educational institutions with no standard anti virus product or Standard Operating Environment (SOE)
- web browsing with no anti virus at the Internet gateway
- insecure wireless networks
- Virtual Private Networks (VPNs) with no anti virus at the VPN gateway
- Remote access services with no anti virus at the remote access gateway
- laptops with no SOE or configuration lockdown controls

Recovery

In the majority of cases, recovery from the virus on each system essentially only required the virus eradication and protection process as discussed earlier.

Once containment controls were in place, no further action was required for the WAN to recover to a normal state.

Impact

The incident had mainly effected the organisation with loss of ICT services as follows:

- loss or intermittent service for less than a day, affected systems included:
    - any one of thousands of infected Windows desktop and server platforms, which returned to normal service once the virus was removed
- loss or intermittent service for less than a week, affected systems included:
    - corporate sites, which returned to normal service once all viruses were removed
    - the WAN, which returned to normal status once containment measures were implemented
    - corporate systems requiring Internet access and other network dependant corporate applications, which returned to normal status once containment measures were implemented
- loss or intermittent service for over a week, affected systems included:
    - college sites, which returned to normal service once all viruses were removed
    - college online learning applications, which returned to normal status once containment measures were implemented and all viruses were removed
    - the majority of educational institutions, which returned to normal status once containment measures were implemented and all viruses were removed
    - some non broadband carrier links, which had to be migrated to alternate network services
- ongoing loss of or intermittent service, affected systems included:
    - around 100 educational institution sites, which despite best efforts, could not respond appropriately to the incident. I performed on site investigations of two of these educational institutions and found that one educational institution had arranged for a private contractor to eradicate the virus, who did not complete the job satisfactorily. In the other instance, the educational institution had over 200 PCs, one part time ICT support person and no automated software deployment tools or managed anti virus system. The patching of all these systems in a timely manner would not be feasible. It appeared from feedback received from the other infected educational institutions that they also faced similar issues. Fortunately I was able to arrange additional support for these two educational institutions and resolved their issues within a couple of days. They now both have Windows Software Update Services (SUS) and the organisations standard anti virus software installed.

Other impacts of the incident included lost productivity in corporate and educational areas affected by the network outage and recovery costs incurred by ICT support units, educational institutions and colleges.

Only one business function had to resort to a business continuity plan. This involved the email correspondence that was destined for distribution to all educational institutions. During the incident, all business units were advised that email distributions of this type should be supported by fax distributions to ensure delivery of the correspondence.

On a positive note, there was no known loss of critical data or impact of data integrity during the incident. This could be partly attributed to the virus not having a destructive payload.

Cost

Estimating the number of hours ICT support staff spent in responding to the incident proved difficult. Educational institution ICT support was provided by educational providers, on a part time basis, or external ICT contractors. Some educational institutions reported spending little time on the issue while others had used more considerable resources. Colleges and corporate sites had dedicated ICT support units so accurate information was more forthcoming. Lost revenue was not considered a factor in this case due to the essentially non profit and government nature of the organisation.

A simple formula was used, very loosely based on the CIC Incident Cost Analysis and Modeling Project I (I-CAMP I), to estimate the cost of incident response [14]. This formula required the number of hours spent responding to the incident times the average salary of the per ICT support unit. The total cost of each unit would then be added to provide a grand total (see ‘Cost Formula’ below).

Cost Formula

‘Unit incident response cost’ = ‘total unit hours spent’ x ‘average hourly salary of staff’

‘Total incident response cost’ = the sum of all ‘Unit incident response cost’

Lowest estimate figures were used to provide the most conservative cost estimate.

Follow-up

Once the incident was considered to be under control, an incident report, reviewed by my manager, was compiled for the CIO. This report included a description of the incident, impact, cost analysis and recommended incident risk reduction strategies.

As part of the previously mentioned ongoing development of a formal incident management policy and procedure, a series of workshops were run in partnership with an external security firm which included a lessons learnt session about this incident.

The following key recommendations were submitted to the CIO for improving incident response within the organisation and dealing with similar incidents:

- establishment of an information security policy, including incident management, to provide information security standards across the organisation
- implement an SOE that incorporated anti virus and patch management, especially on mobile and remote client computing devices (e.g. laptops)

- implement an automated vulnerability management solution, including anti virus and patch management, in educational institutions to enable timely incident response and prevention
- identify and secure entry points to the WAN in order to prevent and better control future similar network incidents
- form an incident response team to handle future incidents
- review network and key system business continuity plans (BCPs) and disaster recovery plans (DRPs) as a precaution in case of similar future incidents
- provide increased ICT support staff awareness training, especially at educational institutions, on computer viruses and the importance of patch management
- provide anti virus controls of information stores on non affected systems that unintentionally store viruses (e.g. UNIX and Novell disk shares)
- provide alternate Internet access methods for ISU so ability to research security sources on the Internet is maintained during loss of normal organisational Internet access

The organisation decided that implementation of the recommendations would be reviewed for suitability at a later stage as they could not be easily deployed without the use of extensive resources.

Summary

The key issues in coordinating this incident's response included:

- endorsement of the coordinator role, either by policy or the senior executive body, thereby allowing the coordinator access to the many units affected within the organisation, and to establish a single point of contact for major incident issues
- consulting with business, education and ICT representatives to create and implement a response plan, with clear roles for those involved, including methods of reporting and monitoring of the plans execution
- use of existing ICT support units and call centres to provide technical support so as not to overload the coordinator with non critical incident issues
- clarifying technical recommendations provided by multiple ICT units by personally researching information from external security authorities such as those referenced in this case study (see 'References' at the end of this document)
- resolve technical issues by working closely with involved ICT units
- noting the importance of collating, analysing, summarising and archiving technical and general incident information coming from many sources throughout the organisation
- prioritising the deployment of resources according to organisational needs
- ensuring owners of key business systems or ICT infrastructure are in a state of preparedness to implement BCPs or DRPs if required
- establishing clear lines of incident communication and reporting

Overall, the main impact of the incident, DDoS causing a loss of WAN services, was quickly brought under control in the containment phase. Eradicating the cause of the incident, the Welchia and Blaster viruses, proved to be more difficult due to the existing ICT support structure and the sheer size of the organisation. A strategy of identifying and concentrating support resources to the worst affected sites proved successful in rapidly reducing the large number of affected computers to acceptable levels, thereby allowing educational and corporate operations to continue as per normal. Draft information security incident management policy and procedure documents have now been completed by the organisation’s ISU as an initial step in improving the organisation’s incident response.

References

1. Microsoft Corporation, ‘Microsoft Security Bulletin MS03-026’, revised 10th September 2003, URL: http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx

2. Shavlik Technologies, ‘Media Advisory’, 31st July 2003, URL: http://www.shavlik.com/Press_Releases/Advisory%20Bulletin%20MS03-026%20Kit%207-31-03.pdf

3. Trend Micro, ‘Virus Encyclopedia’ - ‘WORM_MSBLAST.A’, URL: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_MSBLAST.A

4. Douglas Knowles, Frederic Perriot and Peter Szor, ‘Security Response’ – ‘W32.Blaster.Worm’, Symantec Corporation, updated 26th February 2004, URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html

5. Frederic Perriot and Douglas Knowles, ‘Security Response’ – ‘W32.Welchia.Worm’, Symantec Corporation, updated 26th February 2004, URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html

6. Stephen Northcutt, ‘Computer Security Incident Handling’, Version 2.3.1, SANS Press, March 2003

7. Danny Smith, ‘Forming an Incident Response Team’, AusCERT, 1st January 1995

8. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle and Mark Zajicek, ‘Handbook for Computer Security Incident Response Teams (CSIRTs)’, 2ND Edition, Carnegie Mellon Software Engineering Institute

9. COBIT, ‘Management Guidelines’, IT Governance Institute, 3rd Edition, July 2000

10. SANS Internet Storm Centre, ‘Handler's Diary August 18th 2003’, The SANS Institute,18th August 2003, URL: http://isc.sans.org/diary.php?date=2003-08-18

11. Frederic Perriot and Douglas Knowles, ‘Security Response’ – ‘W32.Welchia.Worm’, Symantec Corporation, updated 26th February 2004, URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html

12. SANS Internet Storm Centre, ‘Handler's Diary August 16th 2003’, The SANS Institute,17th August 2003, URL: http://isc.sans.org/diary.php?date=2003-08-16

13. Internet Security Systems, ‘Support’ – ‘Scanms - MS03-026 RPC Vulnerability Scanner’, URL: http://www.iss.net/support/product_utilities/ms03-026rpc.php

14. CIC Security Working Group, Virginia Rezmierski et al, 'Final Report' – 'Incident Cost Analysis and Modeling Project', Committee on Institutional Cooperation, URL: http://www.cic.uiuc.edu/groups/ITSecurityWorkingGroup/archive/Report/ICAMPReport1.pdf