IP-SCAN-TCP-80□CODERED□NIMDA

Unordered List ItemAccording to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report. Thank you!

- Symantec□Linux.Slapper.Worm
- Symantec□NIMDA
- Symantec□CODERED
- Symantec□W32.Mydoom.B@mm
- Symantec□W32.Welchia.C.Worm
- Symantec□W32.Gaobot.gen!poly (2004/04/29)
- Trend Micro□WORM_AGOBOT.HM (2004/04/29)
- Symantec□W32.Spybot.Worm (2004/09/01)

IP-SCAN-UDP-137

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- W32/Opaserv.worm
- W32/Bugbear@MM
- Internet Storm Center: Bugbear & Scrup
- NIMDA

IP-SCAN-TCP-443□IP-SCAN-TCP-1052□IP-SCAN-UDP-1812□IP-SCAN-UDP-1978 □IP-SCAN-UDP-2002□IP-SCAN-UDP-4516

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- Symantec: Linux.Slapper.Worm
- Red Hat: Linux.Slapper.Worm–What Red Hat customers can do about it
- F-Secure: Slapper

IP-SCAN-TCP-445□IP-SCAN-TCP-1025□IP-SCAN-TCP-139

According to the network system records, your computer may be infected with one of the following

viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- Symantec: W32.HLLW.Lovgate.G@mm (2003/03/24)
- Trend Micro: WORM_LOVGATE.F (2003/03/23)
- Trend Micro: WORM_DELODER.A (2003/03/09)
- CERT Advisory CA-2003-08: Increased Activity Targeting Windows Shares (2003/03/11)
- Symantec: W32.HLLW.Deloder (2003/03/08)
- Trend Micro: WORM_LIOTEN.A (2002/12/17)
- Symantec: W32.HLLW.Lioten (2002/12/16)
- Alert:IraqiWorm tcp/445 worm
- CERT: W32/Lioten Malicious Code
- Symantec: W32.HLLW.Gaobot (2002/10/22)
- Trend Micro□TROJ_KILLWIN.C (2002/12 /30)
- Symantec□W32.Welchia.C.Worm
- Symantec□W32.Gaobot.gen!poly (2004/04/29)
- Trend Micro□WORM_AGOBOT.HM (2004/04/29)
- Symantec□W32.Sasser.B.Worm (2004/05/20)
- Symantec□W32.Spybot.Worm (2004/09/01)

IP-SCAN-TCP-1433

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- Digispid.B.Worm

IP-SCAN-TCP-25□DOS-TCP-25□EMAIL-VIRUS

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- W32.Sobig.B worm (2003/05/31)
  - Symantec W32.Sobig.C@mm
- W32.Sobig.B worm (2003/05):
  - Symantec W32.Sobig.B@mm
- Brid.A worm (2002/11):
  - Symantec W32.Brid.A@mm
  - Trend Micro□PE_BRID.A
- Myparty worm :
  - Symantec w32.myparty@mm
- Shoho worm :

    - Trend Micro□WORM_SHOHO
- Shoho worm :
    - Symantec w32.shoho@mm
    - Trend Micro□WORM_SHOHO.A
- Nimda worm :
    - Symantec: W32.Nimda.E@mm
    - Trend Micro: PE_NIMDA.E
- Nimda worm :
    - CERT Advisory CA-2001-26 Nimda Worm

IP-SCAN-UDP-1434

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- W32.SQLExp.Worm
    - Symantec□W32.SQLExp.Worm
    - Trend Micro□WORM_SQLP1434.A
    - Symantec□W32.Spybot.Worm(2004/09/01)

IP-SCAN-TCP-3127□IP-SCAN-TCP-3128□IP-SCAN-TCP-2766□IP-SCAN-TCP-8080□IP-SCAN-TCP-10080

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- W32.HLLW.Deadhat.B
    - Symantec□W32.HLLW.Deadhat.B
- W32.Mydoom.A
    - Symantec□W32.Mydoom.A@mm
- W32.Mydoom.B
    - Symantec□W32.Mydoom.B@mm

IP-SCAN-TCP-135

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- W32.Blaster.Worm

    - Symantec：W32.Blaster.Worm
- W32.Welchia.C.Worm
    - Symantec：W32.Welchia.C.Worm
- W32.Gaobot.gen!poly
    - Symantec：W32.Gaobot.gen!poly（2004/04/29）
    - Trend Micro：WORM_AGOBOT.HM (2004/04/29)
- W32.Spybot.Worm
    - Symantec：W32.Spybot.Worm (2004/09/01)

IP-SCAN-ICMP-0

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- W32.Welchia.Worm
    - Symantec：W32.Welchia.Worm
    - W32.Welchia worm
    - Microsoft Security Bulletin MS03-026，MS03-007 - Critical

IP-SCAN-TCP-32773

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- TW-CA-2002-178-[CERT Advisory CA-2002-26:Buffer Overflow in CDE ToolTalk]
    - TWCERT (Taiwan Computer Emergency Response Team/Coordination Center)
    - CERT Advisory CA-2002-26

IP-SCAN-TCP-5554，IP-SCAN-TCP-9996

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- W32.Sasser.B.Worm
    - Symantec：W32.Sasser.B.Worm

IP-SCAN-TCP-22

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- Symantec□Trojan.Linux.Typot
- Symantec□Trojan.Linux.Zab

IP-SCAN-TCP-3306

According to the network system records, your computer may be infected with one of the following viruses. However, with rapid growth of the number of viruses, we do not guarantee all types of viruses are included in our list. Please refer to the relevant network security information for the latest information. After fixing the problem, please inform us by online report.

- MySQL UDF Worm (Wootbot/Spybot)
- Symantec□W32.Spybot.IVQ
- 趨勢科技□WORM_WOOTBOT.FV

IP-SCAN-TCP-10000□IP-SCAN-UDP-0□SSH-ATTACK

According to a system log, due to a computer virus or some other problem on your computer. For more information, please contact us on extension 31134(Teaching Network) or 31178(Dormitory Network).

MAIL-SPAM□OPEN-PROXY□OPEN-RELAY

According to a system log, your computer has a problem of sending mail spam, serving an open-proxy, or serving as an open-relay. Please resolve the issue and report to ___.

1. What is mail spam?
   Mail spam, also known as junk e-mail or unsolicited bulk e-mail (UBE), is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail.

http://en.wikipedia.org/wiki/E-mail_spam

1. How to prevent your computer from being a relay?
   If you have sendmail installed, please upgrade your sendmail to v8.9. If you have Microsoft Exchange installed, please upgrade it to the latest version. You should limit your SMTP server to be accessible from local IPs only.
2. Will proxy servers send mails? They maight be dangerous open proxies.
   If the scope of the clients of a proxy is not restricted, a hacker may use the proxy to spam

others. Such proxies would be banned by Department of Education.
3. Is your computer banned? Your computer may be infected with a virus or has backdoor planted. Although some users themselves did not send out spams, or try to hack others' computers, they are still banned. When this happens, we would suggest the users to do a full virus scan, though the scan might not successfully detect the virus or backdoor programs.

PCRI

1. Unable to useWeb Report Form
2. Teaching, Administration Area: Suspected infringement must be reported in writing. Please download the “Suspected Infringement Report and IP Address Recovery Application Form” from Network Systems Division/Download Forms, and submit the form to the service counter on 2F of the Computer and Communication Center (Contact number: extension 31225). Thank you!
3. Dormitory Area: Suspected infringement must be reported in writing after a 30 day suspension. Please download the “Student Dormitory Network Recovery Application Form” from Network Systems Division/Download Forms, and submit the form to the service counter on 2F of the Computer and Communication Center (Contact number: extension 31178). Thank you!

DNS-DoS

According to a system log, due to a computer virus or some other problem on your computer, the computer is repeatedly attacking the DNS with a lot of queries, please contact us on extension 31134. The following lists possible reasons for your computer be banned,

- Trojan horse virus has been planted in your computer, and the trojan has been attempting to constantly search for an invalid domain name.
- Your computer has BitComet installed. The software would constantly search for invalid tracker servers.

TACERT

1. Unable to useWeb Report Form
2. The Ministry of Education Information and Communication Security Contingency Platform has notified us that your computer has generated a security issue due to a virus or other cause. You are required to email the following equipment information to the Computer and Communication Center at abuse@cc.nthu.edu.tw so that we may report the issue to the Ministry of Education Information and Communication Security Contingency Platform. This is also required for unblocking the network.
3. If you live on-campus, please check the inbox of the email address you designated when you applied for dormitory Internet access. Thank you.

(□ Required□◎ Not required)

	Field	Example

	Field	Example
□	IP address□	ex: 140.114.22.33
◎	Internet site□web-url□□	ex: https://www.xxx.edu.tw/cba.index
□	Equipment make and model□	ex1: Asus TS100 E6
		ex2: Acer AT110 F1
□	OS name and version□	ex1: Centos Linux 5.4
		ex2: Windows XP SP2
◎	Compromised software (name/version)□	ex: sendmail server
□	Antivirus software (name/version)□	ex: Avira 10.0.0.561
□	Firewall (name/version)□	ex: iptables
◎	IPS/IDS (name/version)□	ex: snort 2.8.3
◎	Else (name/version)□	
□	Extent of damage□	
□	Event and disposal description□	
□	Assessment of possible affected area and damages□	
□	Solutions□	ex: Reinstall operation system

For any questions, please contact Mr. Lee directly at ext. # 31225, thank you.

OPEN-DNS-RESOLVER

1. Able to useWeb Report Form
2. According to the network system records, your computer has an **open DNS resolver problem**. If you wish to understand its cause and effects, please refer to open DNS resolver. Thank you!
3. **3. If you are running Windows 7 or 8 as your operating system, please seeDNS problemin the FAQ section of this website for possible solutions.**

OTHERS

Your computer has displayed improper Internet use behavior that is possibly due to a virus, a report by a party outside of the school, or other cause. Due to the special circumstances, the Web Report Form may not be used to unblock your network. For details, please contact us directly at ext. # 31225 for the academic area, or 31178 for the dormitory area. Thank you!