



Building National Public Network Emergency Response Capability

Dr. Zhang Bing

*National Computer network Emergency Response
technical Team/Coordination Center of China*

(CNCERT/CC)



Outline

- *Threats and Trends of Network Security Problems*
- *Introduction of National Public Emergency Response System*
- *Experience & Lessons*
- *Global Problem Needs Global Solution*



Threats and Trends of Network Security Problems



Features & Trends of Network Security Threats

- *Cause large-scale congestion/break down in a short period of time*
- *Attackers can come from each corner of the world*
- *Usually use innocent hosts to attack*
- *More attackers, much easier, much more powerful*
- *Organized attacking or crime*
- *Some attacking behaviors are hidden well*



Common Security Incidents

- *Denial of Service*
- *Intrusion*
- *Virus/Worm*
- *Trojan horse/Back door/Spyware*
- *BOTNET*
- *Web Defacing*
- *Phishing/ID Theft*
- *Information stealing*
- *Spam/email bomb*
- *Scanning*
- *.....*



Is this serious enough?

- *Internet is becoming one of our information infrastructure but not just a 'toy' or 'tool' today:*
 - *More and more Internet-based traditional telecommunication services*
 - *More and more important applications that has relationship to great amount of users*
 - *Connected with the traditional telecommunication network*
 - ***Infrastructure of E-everything***
- *Security Incidents cause too much damage to us now:*
 - *Passengers jammed in the airport because virus or Internet worm destroyed the ticket system or Local Area Network*
 - *Factories can not produce anything because of the breaking of network*
 - *Online systems can not work : stock, education, etc.*
 - *Huge financial lost*
- *An insecure network will heavily hurt the confidence of the users, which will be the biggest barrier for building a valuable information society*

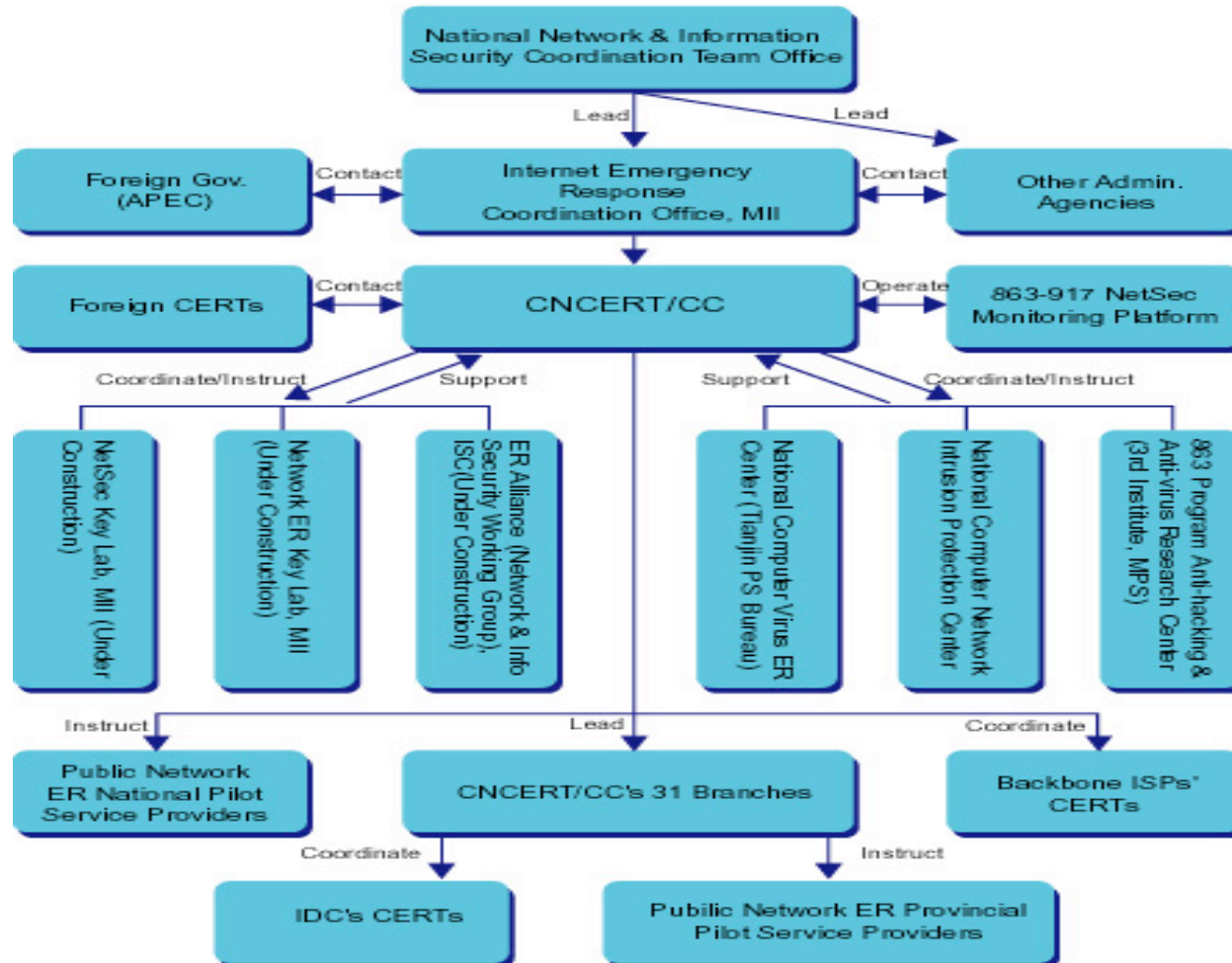
CN  ERT/CC

National Public Network Emergency Response System





NATIONAL PUBLIC NETWORK SECURITY EMERGENCY RESPONSE SYSTEM





Necessity of building an efficient cooperation system

- *Cooperate among multiple sides:*
 - *Government: law , standard, etc. related*
 - *ISPs: network related*
 - *Various CSIRTs : cover more end users*
 - *Labs: analysis, research, development related*
 - *Organizations with specialities: more professional support*
 - *Industry side: patch, tools, products, upgrade, etc.*
- *With such a scheme, we successfully restrained SQL SLAMMER in 2003. Jan.*
- *Only by multi-parties' cooperation according to a well-planed scheme can Internet security incidents be handled quickly and effectively*



National CSIRT: The technical center of the cooperation system

- *Information Gathering & Analyzing*
- *Tech. & Info. Support*
- *Research Related Activities*
- *Coordination Center for Incidents Handling*

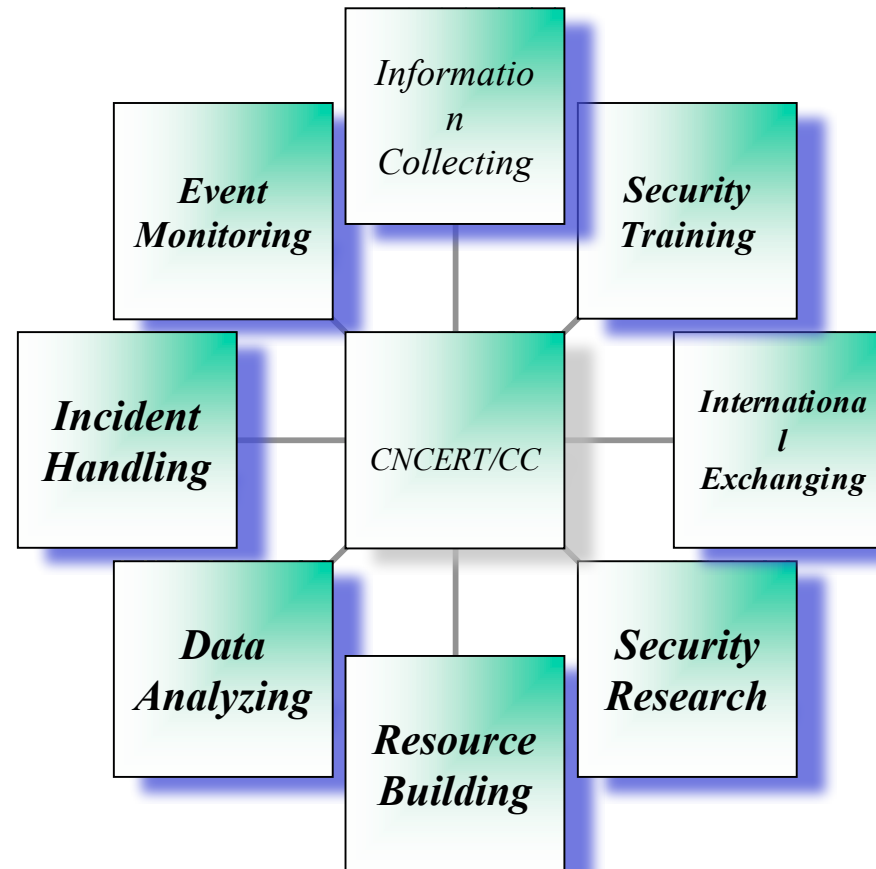


CNCERT/CC

- *Established in 2000*
- *became a full member of FIRST in 2002*
- *At APSIRC2002, initiated APCERT (Asia Pacific Computer Emergency Response Team) with AusCERT, JPCERT/CC.*
- *At APSIRC2003, was nominated and elected as the Steering Committee member of APCERT*
- *At APSIRC2005, Dr Du Juejin elected as vice-Chair of APCERT*
- *In 2004, built up 31 branches across the country*



CNCERT/CC's Activities





CNERT/CC's Activities

<i>Information Collecting:</i>	Collect various timely information on network security events via various communication ways and cooperative system
<i>Event Monitoring:</i>	Detect various highly severe security problems and events in time, and deliver information to related organizations or users.
<i>Incident Handling:</i>	Leverage domestic CSIRTs to handle various incidents, and act as a premier window to accept and handle incident reports from homeland and world.
<i>Data Analyzing:</i>	Conduct comprehensive analysis with the data of security events, and produce trusted reports.



CNCERT/CC's Activities

<i>Resource Building:</i>	Collect and maintain various basic information resources, including vulnerabilities, patches, defending tools and latest network security technologies for supporting purpose.
<i>Security Research:</i>	Research on various security issues and technologies as the basic work for security defense and emergency response.
<i>Security Training:</i>	Provide training courses on emergency response and handling technologies and the construction of CERT.
<i>Technical Consulting:</i>	Offer various technical consulting services on security incident handling.
<i>International Exchanging:</i>	Organize domestic CERTs to conduct international cooperation and exchange.



How Does CNCERT/CC Act?

- *As an exchange center of information*
 - *From national network security monitoring platform*
 - *From public incident warning and reports*
 - *To set up reliable and expedite communication channels to all domestic and international CERTs.*
- *To direct all the regional branches to work together*
- *To cooperate with Internet carriers closely*
- *As a security technology research center*
- *To provide the most trusted data to government and the society*



Some work of CNCERT/CC in 2004

- *During the year of 2004, CNCERT/CC:*
 - *Published 65 security alerts, 130 vulnerability bulletins, 125 virus/worm warnings, 164 network security notes, 30 network security recommendations, etc*
 - *Received 64686 incident reports, including 223 phishing incidents, 26 DDoS, 2059 web defacements, etc*
 - *Coordinated the branch to handle 1000 network security incidents*
 - *Provided courses training, invited reports, or conference address at more than 40 network security related domestic and abroad meetings*



Experience & Lessons



Lessons Learned

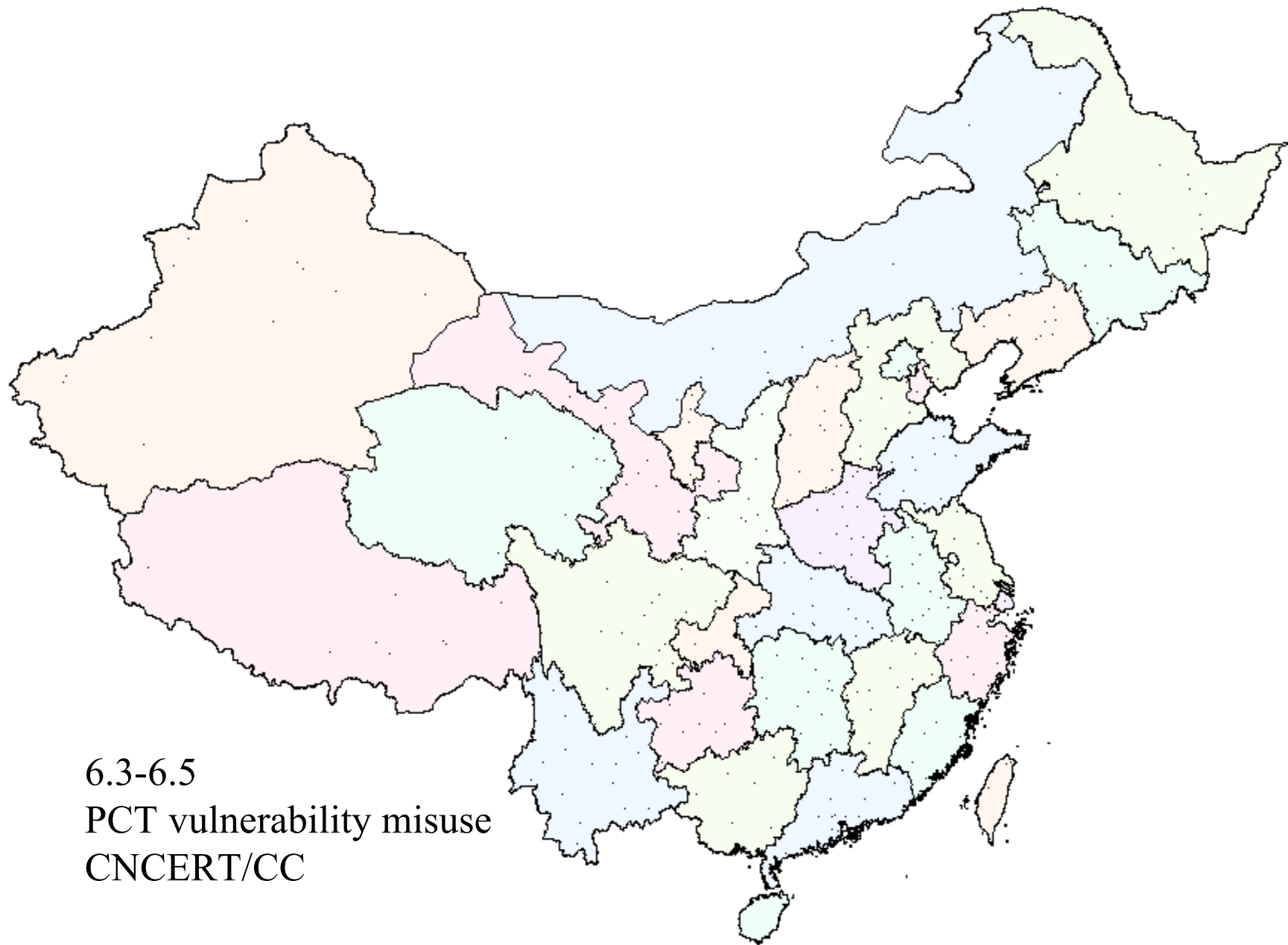
- *2001. Codered/Nimda Worm*
 - *Emergency Response Mechanism must be built up between CNCERT/CC and all the Internet providers*
- *2003.SQL Slammer Worm*
 - *The emergence response system must face the threat of worm more faster, there is the need for more powerful monitoring system and larger emergency response system*
- *2003 Deloader*
 - *Vulnerability is not prerequisite of large scale network security incidents,*
 - *The attacker try to collect and control large amount PCs*
- *2003 RPC Series Worms(MsBlaster/Nachi) & 2004 Lsass Series Worms*
 - *Corperation with SW vendors*
 - *Worm-driving super large DDoS attack turned to be reality*
- *2004 Witty Worm*
 - *Attack to the prepared users*
- *2004.growth of Phishing*
 - *The attackers are getting more and more interest centric*
 - *More cooperative relationship within the different hackers/criminals*



Monitoring system

- *Gather information in time*
 - *Abnormal traffic*
 - *Severe attacking behaviors (DDoS, etc.)*
 - *Misuse situations*
 - *etc.*
- *To :*
 - *Get early warning capability*
 - *Judge the effectiveness of the control methods*
- *A lot of countries or areas are doing this*
- *863-917 NetSec Monitoring System*

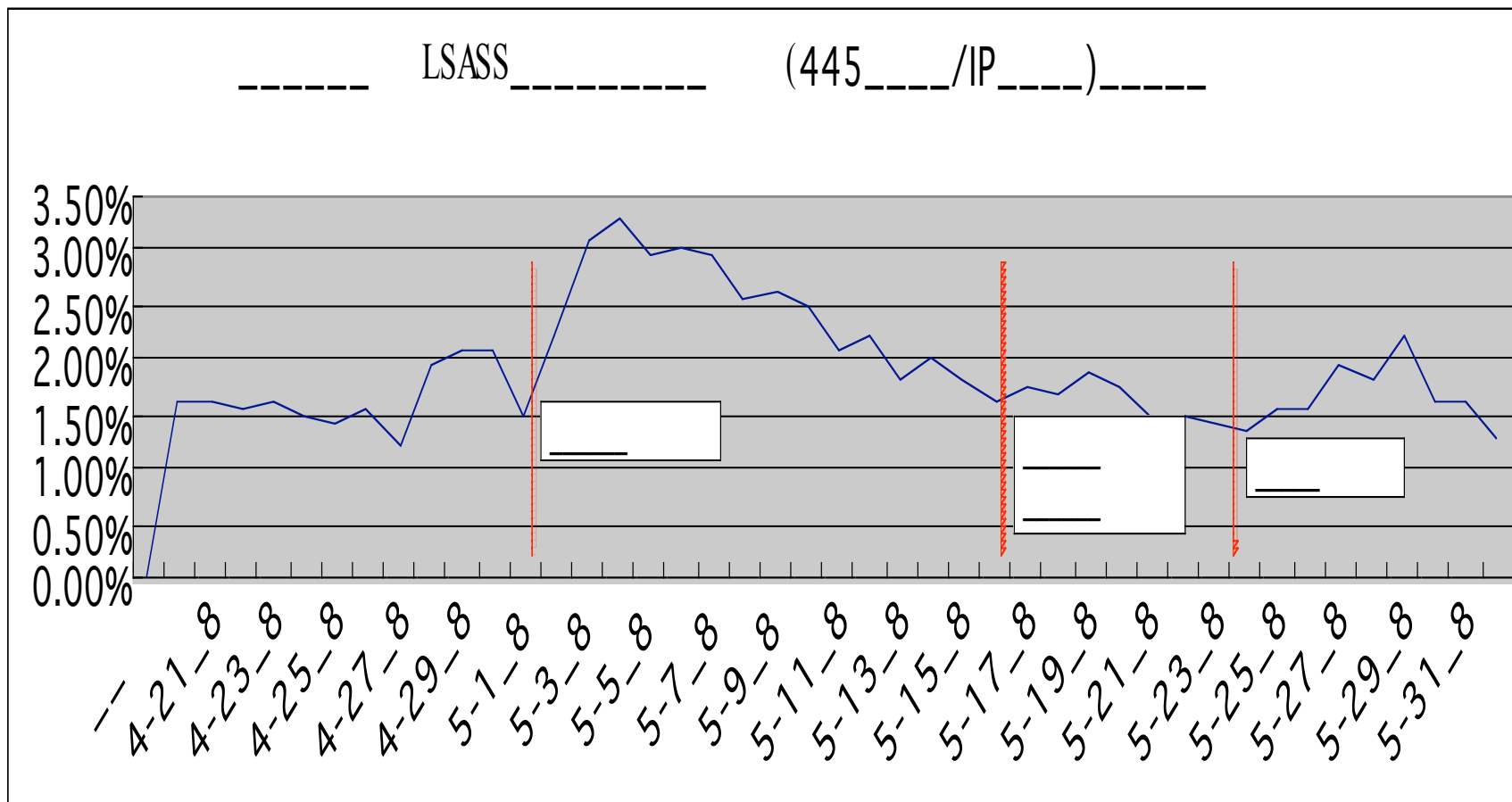
2004-6-3 2:0:0



6.3-6.5
PCT vulnerability misuse
CNCERT/CC



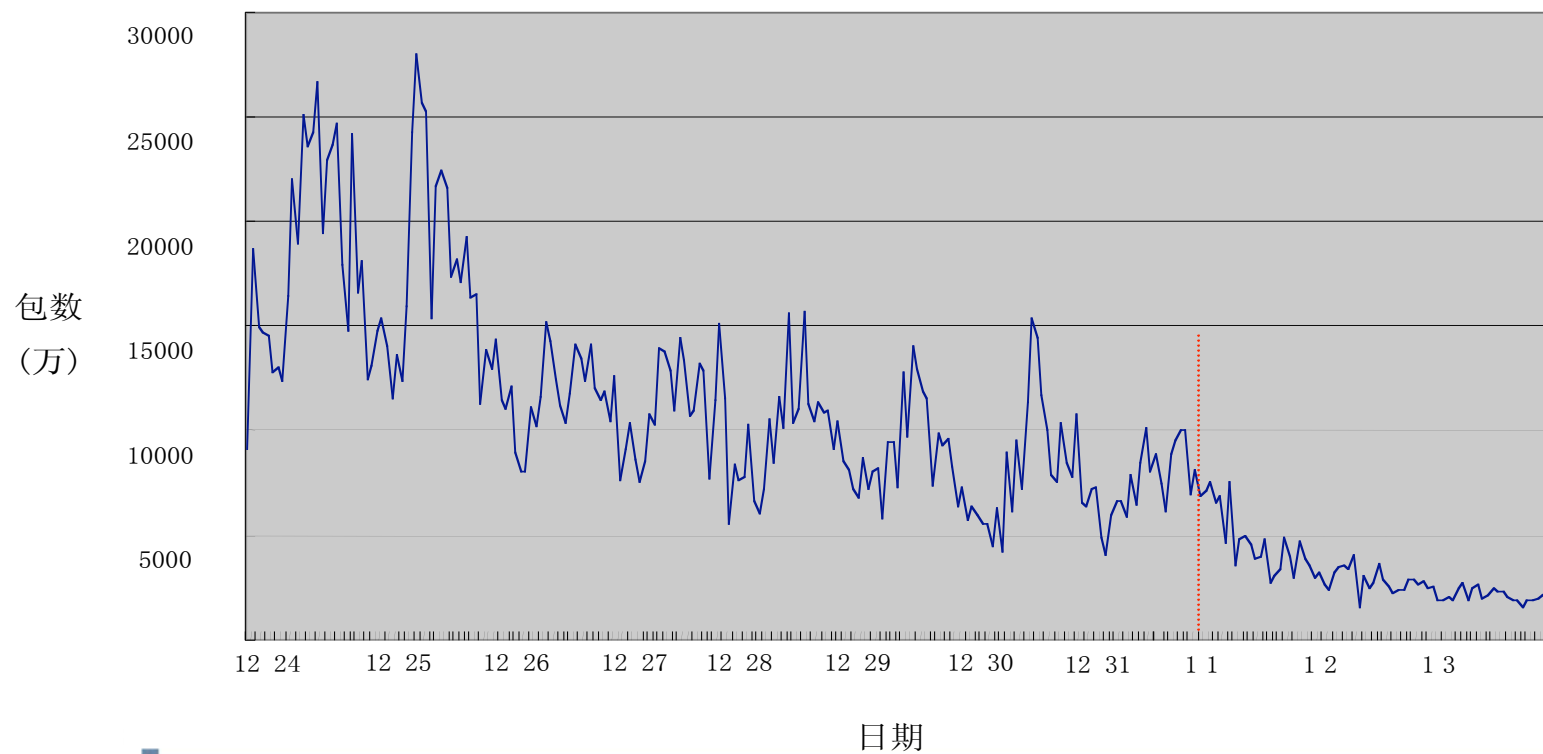
LSASS Series Worms





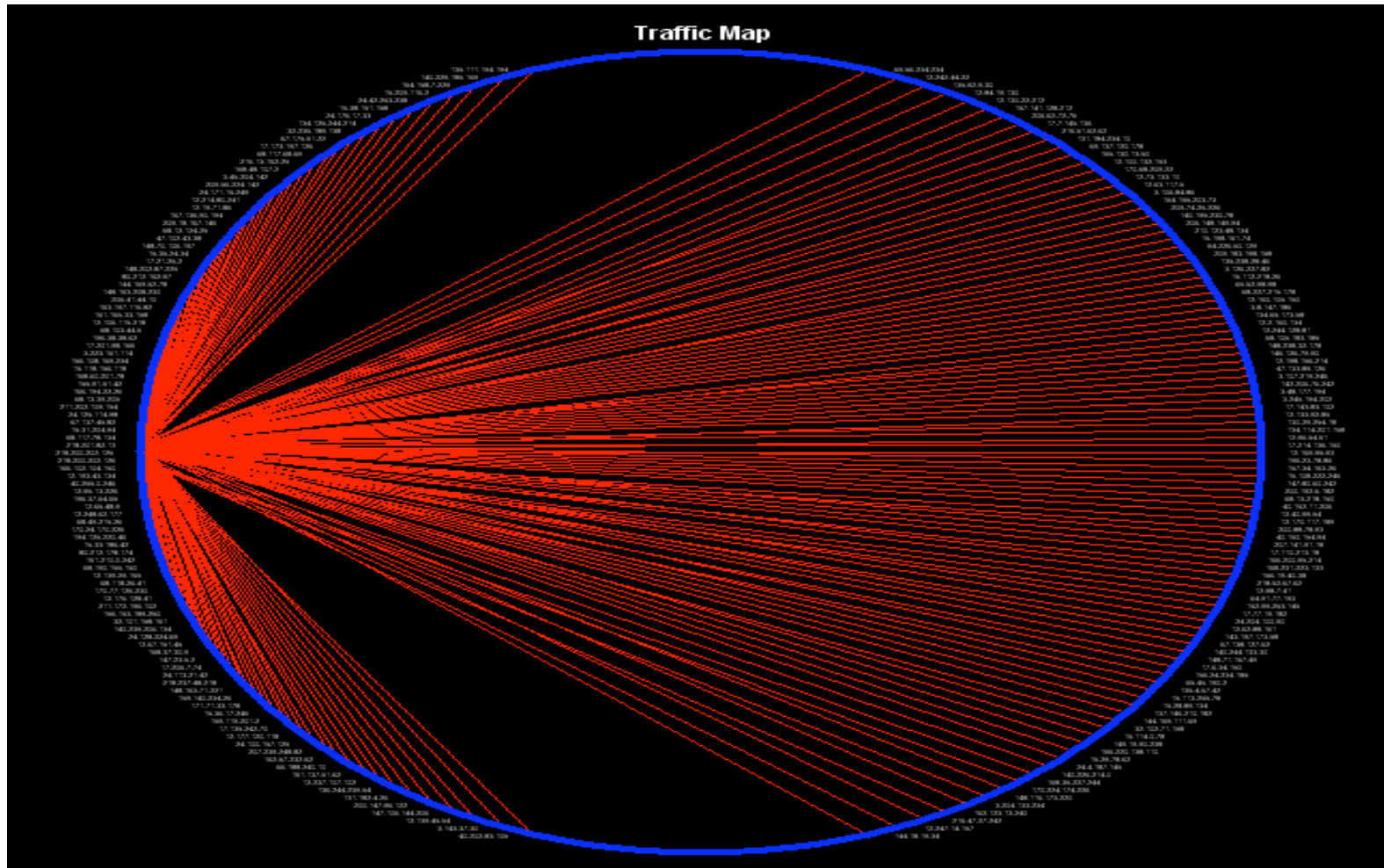
MSBLAST.remove (NACHI)

icmp 回境流量图





Traffic Map





Fighting the BOTNET

- ***What is the Bot?***
 - *A piece of software that connects back to a centralized control channel.*
 - *Allows unauthorized control of many machines from a single point.*
 - *Typically lies dormant, waiting for commands from its controller.*
 - *The single greatest threat facing humanity.*
- ***Also known as Zombie Army***
- ***Botnet is used to***
 - ***DDoS/extortion***
 - ***Spam Relay***
 - ***rent-a-network.....***



Initial Infection Vectors

- *Un-patched operating systems with remotely exploitable vulnerabilities*
 - *LSASS, RPC-DCOM, etc.*
- *Weak/non-existent administrator passwords*
- *Malicious websites exploiting vulnerable browsers*
- *Social engineering exploiting vulnerable users*

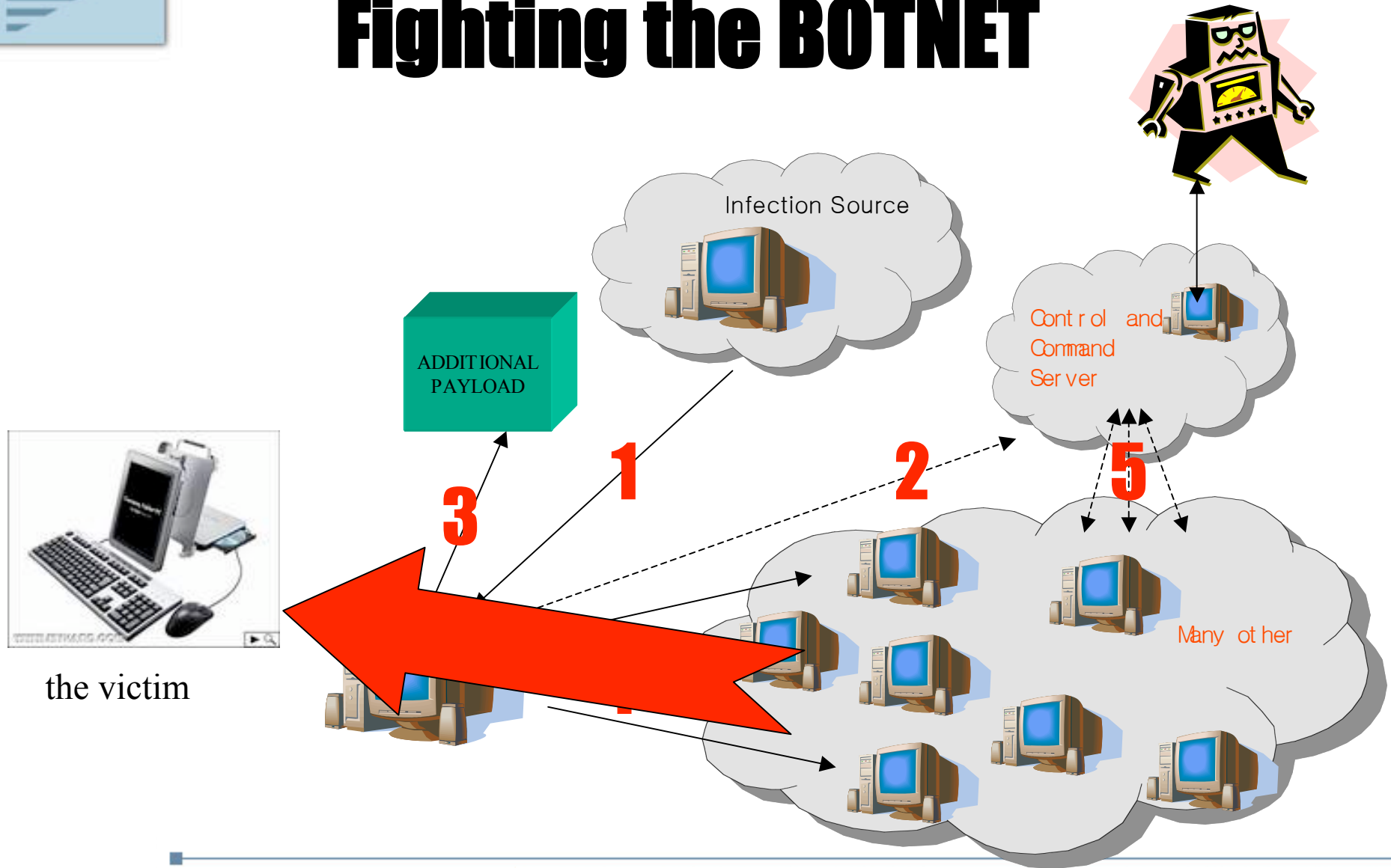


Social Engineering

- **The Goal** – Convince the user to download and execute an evil payload
- The payload changes often, avoiding anti-virus software
- The payload is typically transparent – the user notices nothing
 - “I clicked, but nothing happened!”
- Can be very creative



Fighting the BOTNET





Fighting the BOTNET

- **CNCERT/CC found one BOTNET with more than 1000k PCs in the end of Dec, 2004**
 - Maybe more.....
- **On-sites Investigation**
- **Collaborate with two tech teams Analyzing several Bot program and kill methods**
- **Support the MPS's forensic and investigation**
- **Turn to be a daily monitoring work of CNCERT/CC**



Incident Handling System

事件处理系统
CNCERT/CC Incident Handle System (IHS)

当前在线用户: 纪玉春

首页 | IP定位 | 事件录入 | 10000导入 | TraCERT

任务视图: 我的任务 | 全部任务

事件视图: 我的事件 | 大规模事件 | 平台个案事件 | 公共个案事件 | 我参与的事件 | 大规模事件 | 平台个案事件 | 公共个案事件 | 本省事件 | 全部事件 | 大规模事件 | 平台个案事件 | 公共个案事件 | 事件档案

大规模事件列表

范围: 全部事件 | 类型: | 状态: |

日期: -- -- 起: -- -- -- -- 止: -- -- -- --

被选事件数: (5)

序号	事件编号	事件名	状态	负责人	录入人	开始日期	结束日期
1	MASS-1000042427	asdflandf	▶	纪玉春	纪玉春	2005-06-21	
2	MASS-1000042351	僵尸网络	▶	纪玉春	纪玉春	2005-06-06	
3	MASS-1000042329	123漏洞	▶	纪玉春	纪玉春	2005-05-26	
4	MASS-1000042304	test0522	▶	纪玉春	宋秩男	2005-05-23	
5	MASS-1000042292	1111111111	▶	纪玉春	纪玉春	2005-05-23	

(总页数:1, 当前页:1)

事件处理系统
CNCERT/CC Incident Handle System (IHS)

当前在线用户: 纪玉春

首页 | IP定位 | 事件录入 | 10000导入 | TraCERT

任务视图: 我的任务 | 全部任务

事件视图: 我的事件 | 大规模事件 | 平台个案事件 | 公共个案事件 | 我参与的事件 | 大规模事件 | 平台个案事件 | 公共个案事件 | 本省事件 | 全部事件 | 大规模事件 | 平台个案事件 | 公共个案事件 | 事件档案

大规模事件列表

范围: 全部事件 | 类型: | 状态: |

日期: -- -- 起: -- -- -- -- 止: -- -- -- --

被选事件数: (5)

序号	事件编号	事件名	状态	负责人	录入人	开始日期	结束日期
1	MASS-1000042427	asdflandf	▶	纪玉春	纪玉春	2005-06-21	
2	MASS-1000042351	僵尸网络	▶	纪玉春	纪玉春	2005-06-06	
3	MASS-1000042329	123漏洞	▶	纪玉春	纪玉春	2005-05-26	
4	MASS-1000042304	test0522	▶	纪玉春	宋秩男	2005-05-23	
5	MASS-1000042292	1111111111	▶	纪玉春	纪玉春	2005-05-23	

(总页数:1, 当前页:1)

事件处理系统
CNCERT/CC Incident Handle System (IHS)

当前在线用户: 纪玉春

首页 | IP定位 | 事件录入 | 10000导入 | TraCERT

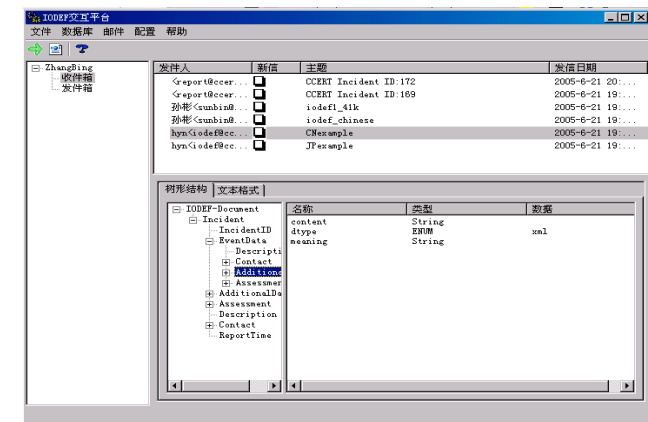
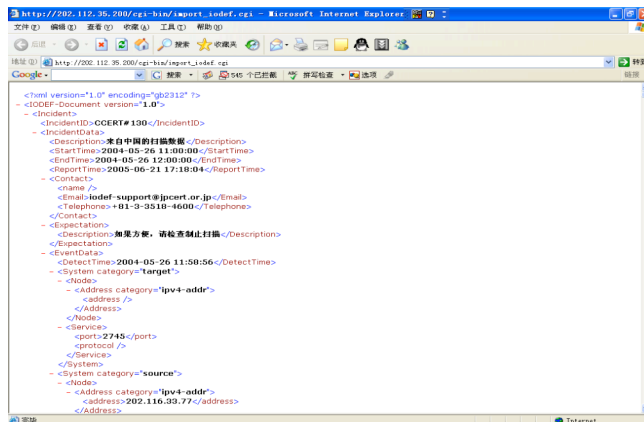
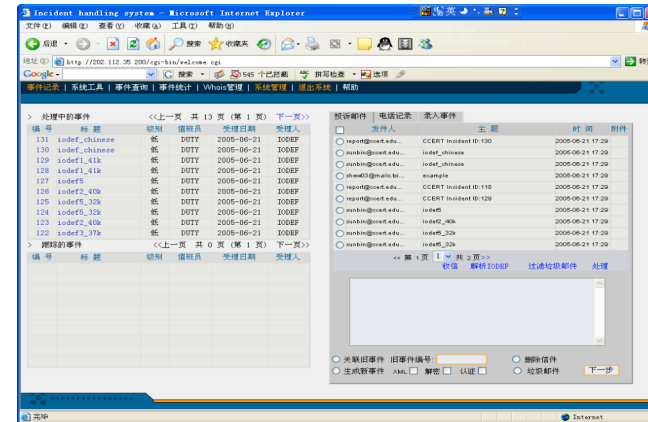
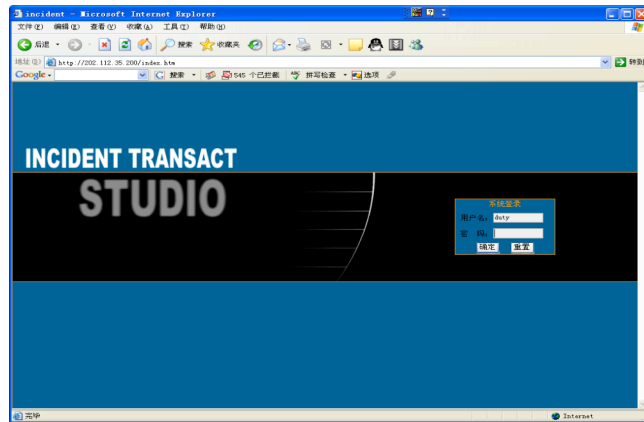
文档管理系统

- 国家中心
 - 平台建设
 - 数据监测
 - 分析报告
 - 其它
- 响应组
 - 事件处理报告
 - 统计报告
 - 其它
- 协调组
 - 事件总结报告
 - 应急体系
 - 其它
- 总结及计划
 - 数据组
 - 响应组

序号	事件编号	事件名	状态	负责人	录入人	开始日期	结束日期
1	1000000682	CN.MEXI..._TM_2004-029	▶			2004-12-28	
2	1000000681	CNCERTCC_TM_2004-028	▶			2004-12-28	
3	1000000680	CNCERTCC_TM_2004-027	▶			2004-12-28	
4	1000000679	CNCERTCC_TM_2004-026	▶			2004-12-28	
5	1000000678	CNCERTCC_TM_2004-025	▶			2004-12-28	
6	1000000677	CNCERTCC_TM_2004-024	▶			2004-12-28	
7	1000000676	CNCERTCC_TM_2004-023	▶			2004-12-28	
8	1000000675	CNCERTCC_TM_2004-022	▶			2004-12-28	
9	1000000674	CNCERTCC_TM_2004-021	▶			2004-12-28	
10	1000000673	CNCERTCC_TM_2004-020	▶			2004-12-28	
11	1000000672	CNCERTCC_TM_2004-019	▶			2004-12-28	
12	1000000671	CNCERTCC_TM_2004-018	▶			2004-12-28	

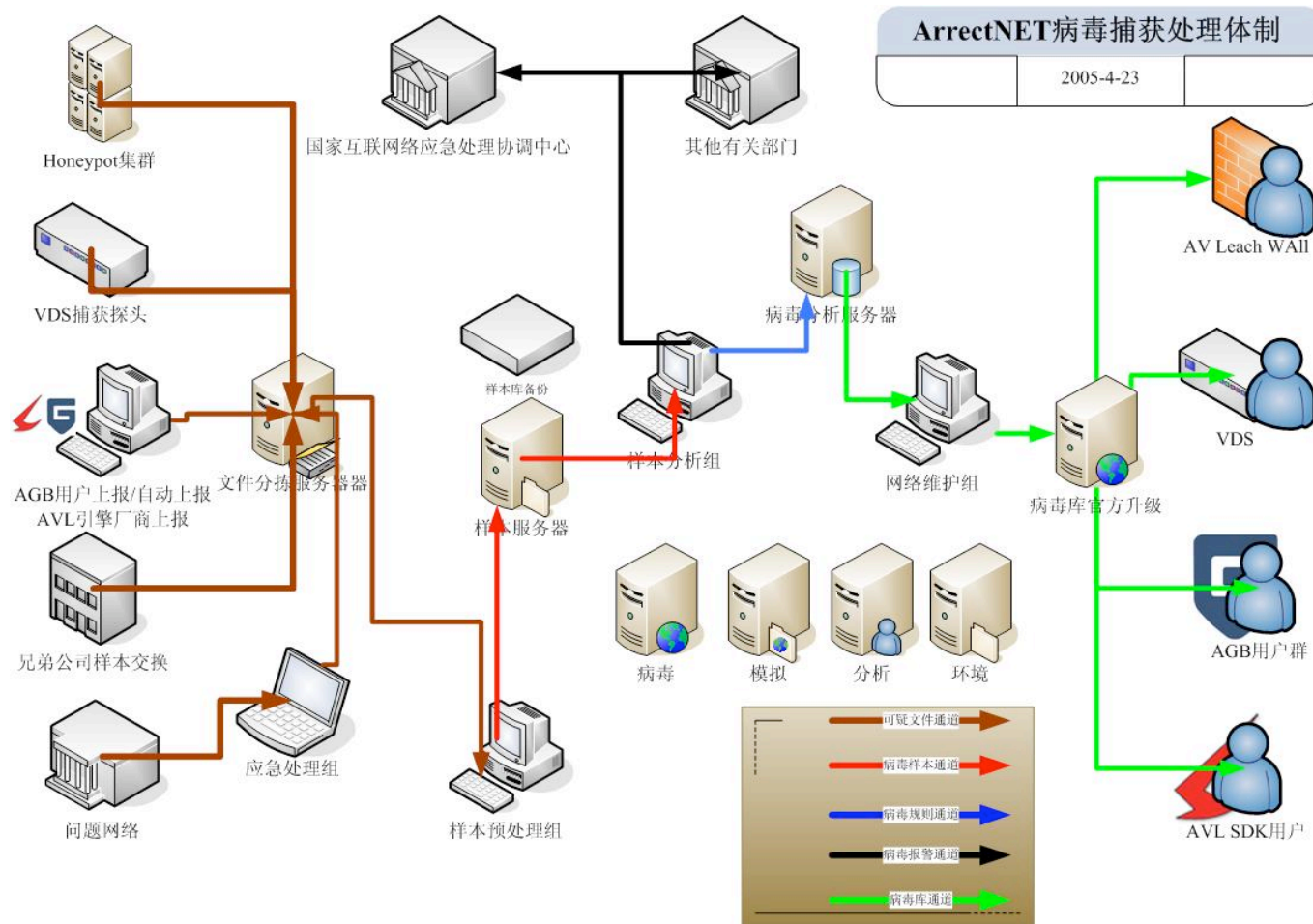


IODEF Exchange System














Virus Detection System





HONEYPOT

Honey Pot 节点

运行状态			
部署示意图	节点1	节点1	节点1
设备列表			
添加新节点	节点1	节点1	节点1
用户管理			
	节点1	节点1	节点1

总计: 37
运行: 26
中断: 11
失控: 0

CN  ERT/CC

*Global Problem Needs Global
Solution*



'Global problem, global solution'

- *With global cooperation, we can:*
 - *Get earlier warning*
 - *Data sharing (increase the analysis capability)*
 - *Tech. and info. sharing*
 - *Stop the attacking from other country or trace the sources of attackers*
- *We get early information from JPCERT/CC and AusCERT for MSBLAST(DDoS traffic) and NACHI(abnormal traffic increasing)*
- *We helped AusCERT and other CSIRTs to handle dozens of phishing incidents*
- *More and more international organizations now: FIRST, APCERT, EGC, TF-CSIRT, etc.*
- *CJK Drill & Co-sponsored projects*



Thank You!

Zhang Bing

+86-10-82990361

+86-10-82990399(Fax)

zhangbing@cert.org.cn

CNCERT/CC Hotline 7*24: +86-10-82991000

National Computer network Emergency Response technical Team/Coordination Center of China