

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



CN@ERT/CC 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
- •





- 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



National Public Network Emergency Response System





NATIONAL PUBLIC NETWORK SECURITY EMERGENCY RESPONSE SYSTEM





CN@ERT/CC 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





- 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

CN ERT/CC





CNCERT/CC's Activities







CNCERT/CC's Activities

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





CNCERT/CC's Activities

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



CN@ERT/CC 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 recomendations, 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







LSASS Series Worms







MSBLAST.remove (NACHI)







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 antivirus software
- The payload is typically transparent the user notices nothing
 - "I clicked, but nothing happened!"
- Can be very creative











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

| CN() ERT/CC1 | Incid | ent Handle System | (IHS) | | | | 当前左绊田 | 户纪玉寿 | |
|---|----------|----------------------|------------|------------|---------|-----|---------------|----------|---|
| · T | | IP TTOO /- DATE /6 - | | | | | = #01ES/6/10/ | 50-1278° | |
| | R., | CN IFALM LIPHS | r/ Oligi | 917 | | | | | |
| €到我的任务 €到全部任务 | 范围 日期 | · 全部事件 ▼ · ▼ 起: - | 类型: | - | ▼ 上: | 🔽 | • | 状态: | 💌 |
| #件视图 | 被选 | 事件数: (5) | | | | | | | |
| 我的事件 公 大规模事件 | 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 | |
| → → → 小 井 小 本 か 来 寺 件 → 小 十 小 素 事 件 → 小 二 か ま 事 件 → 小 二 か ち の 、 の の 、 、 の 、 の 、 の 、 、 、 、 の 、 の 、 、 の 、 の 、 の 、 、 の の 、 の の の の の の の の の の の の の | 1 | MASS-1000042427 | asdfasdf | ۲ | 纪玉春 | 纪玉春 | 2005-06-21 | | <u>u</u> = 🕯 🥎 |
| ()我参与的事件 | 2 | MASS-1000042351 | 僵尸网络 | ۲ | 纪玉春 | 纪玉春 | 2005-06-06 | | 🥶 🗉 🦭 |
| | 3 | MASS-1000042329 | 123漏洞 | ۲ | 纪玉春 | 纪玉春 | 2005-05-26 | | <u>u I a V</u> |
| → | 4 | MASS-1000042304 | test0522 | ۲ | 纪玉春 | 宋轶男 | 2005-05-23 | | <u>u II 🕯 🦭</u> |
| 全部事件 | 5 | MASS-1000042292 | 1111111111 | ۲ | 纪玉春 | 纪玉春 | 2005-05-23 | | <u>u I i i i i i i i i i i i i i i i i i i </u> |
| | | | II II 1 | D D | Go | (总页 | 数:1, 当前页:1 | .) | |
| └── 🤣 公共个案事件 🧐 事件档案 | | | | | | | | | |

| the states of th | - | | | | | | | | |
|--|------|-------------------|----------------------|----------|----------|-----|--------------------|-------|-----------|
| 事件处: | T | 系统 | | | | | | | |
| | noid | ant Handle System | (1115) | | | | | | |
| CNU ERI/CUI | neio | ent Hanole System | (1115) | | | | 当前在线用 | 户:纪玉春 | |
| <u>首页</u> | | 🛃 IP定位 📄事件: | 表入 🗃 IODEF 导入 🚷 Trao | ert | | | | | |
|)任务视图 | ۹, | 大规模事件列表 | | | | | | | |
| | 范围 | 全部事件 🔻 | 类型: | | • | | | 状态: | |
| | 日期 | | | | • ⊥: | 🔻 | | | |
| - 本件加度] | an's | | | | | | | | |
| | 做选 | 争 1千致:(5) | | | | | | | |
| □ 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | 号 | 事件编号 | 事件名 | 状态 | 负责人 | 录入人 | 开始日期 | 结束日期 | |
| → 平台个案事件 | 1 | MASS-1000042427 | asdfasdf | ۲ | 纪玉春 | 纪玉春 | 2005-06-21 | | 🕛 🗉 🗟 🥎 |
| □ | 2 | MASS-1000042351 | 僵尸网络 | ۲ | 纪玉春 | 纪玉春 | 2005-06-06 | | 🕛 🗉 🗟 🥎 |
| | 3 | MASS-1000042329 | 123編洞 | ۲ | 纪玉春 | 纪玉春 | 2005-05-26 | | () II 🕯 🕥 |
| ☆公共个案事件 | 4 | MASS-1000042304 | test0522 | ۲ | 纪玉春 | 宋轶男 | 2005-05-23 | | () II 🕯 📎 |
| □-\$》本省爭件 □-\$》全部事件 | 5 | MASS-1000042292 | 1111111111 | ۲ | 纪玉春 | 纪玉春 | 2005-05-23 | | () II 🕯 🦭 |
| — — — | - | | | | <u> </u> | | | | |
| - · · · · · · · · · · · · · · · · · · · | | | II II I | D | Go | (恩贝 | 数:1, 当 前贝:1 |) | |
| □ | | | | | | | | | |
| A +卸填本/+ | | | | | | | | | |

| 事件处理 | 子 | 统 | | | | |
|---------------------|---------|------------|--------------------------|-----------------|------------|----------|
| CNC ERT/CC Inc. | ident l | Handle Sys | atem (IHS) | 当前在线用户 | :纪玉春 | |
| | | | | | | ●重新登录 |
| • 文档管理系统 | | 1000000682 | CNCERTCC_TM_2004- 029 | ∏tark应急小组的公开资料 | 2004-12-28 | 📥 🖻 🕸 🔋 |
| ∲ □ 国家中心 | | 1000000681 | CNCERTCC_TM_2004- 028 | Hark应急小姐工作流程 | 2004-12-28 | 🛓 🖻 🙁 🤋 |
| ♥ □ 数据组 - □ 平台建设 | | 1000000680 | CNCERTCC_TM_2004- 027 | Hark事件处理课堂练习 | 2004-12-28 | 📥 🖻 🕸 🤋 |
| 一〇数据监测 | | 1000000679 | CNCERTCC_TM_2004- 026 | Hark事件类型和举例 | 2004-12-28 | 📥 🖻 🕸 🤋 |
| | | 1000000678 | CNCERTCC_TM_2004- 025 | Mark事件处理生命周期 | 2004-12-28 | 📥 🖻 🛞 🤋 |
| ○ 响应组 | | 1000000677 | CNCERTCC_TM_2004- 024 | Mark数据库 | 2004-12-28 | 📥 🖻 🕸 s |
| - □ 统计报告 | | 1000000676 | CNCERTCC_TM_2004- 023 | Nark加至 | 2004-12-28 | 📥 🖻 🕸 🤋 |
| - □ 其它 ♀ □ 协调组 | | 1000000675 | CNCERTCC_TM_2004- 022 | Mark应急小组的基础设施 | 2004-12-28 | 📥 🖻 🛞 🤋 |
| | | 1000000674 | CNCERTCC_TM_2004- 021 | Mark应急小组的建设准备工作 | 2004-12-28 | 📥 🖻 🕸 🤋 |
| LEAR | | 1000000673 | CNCERTCC_TM_2004- 020 | Mark应急小组的核心问题 | 2004-12-28 | al 📆 😰 🤤 |
| | | 1000000672 | CNCERTCC_TM_2004- 019 | Mark安全事件趋势介绍 | 2004-12-28 | 📥 🖻 🛞 s |
| -〇 响应组 | | 1000000671 | CNCERTCC_TM_2004- | Mark培训介绍 | 2004-12-28 | 📥 🖻 🕸 🗴 |





IODEF Exchange System

| | Incident handling | system - Microsoft Internet Explorer 🛛 📲 儒英 🤳 🗤 | |
|---|--|--|---|
| 文件 (2) 编辑 (2) 查看 (2) 収織 (4) 工具 (2) 帮助 (2) | 文件(2) 編輯(2) 査看(2) | 收藏(4) 工具(1) 帮助(9) | 1 |
| 3 ALL - O - 🗷 🖻 🏠 🔎 HAR 👷 WARA 🤣 🔗 - چ 🖾 - 🔜 🥂 📓 🦓 | G ## · 🕥 · 💌 | 🖻 🏠 🔎 1929: 🤺 1000000 🧭 🚱 🚱 🖄 🔝 🖉 🖉 🖉 🚳 | |
| i812 (1) 🚵 http://202.112.35.200/index.htm | · 图址 (1) 通http://202.112. | 35.200/cgi-bin/welcome.cgi | 🖌 新期 |
| Coogle - C 222 C 222 · C 222 | Google - | ✓ C 接索 ▼ 参 20545 个已把載 「今 拼写检查 ▼ 通法項 多 | |
| | ▲ ● 件记录 永武工具 ● | 汗查询 争仟號计 Whois管理 糸統管理 進出木統 報助 | ··· |
| | > 处理中的事件 | <(上一宮 井 13 宮 (第 1 宮) 下一宮>> | |
| | 编号 标题 | 级别 值班员 受理日期 受理人 🗌 发件人 主 | 題 时间 附件 |
| | 131 iddef_chinese 130 iddef_chinese | 低 DUTY 2005-06-21 IODEF Oregorigocort.edu CCERT Incident ID:13 好 DITY 2005-06-21 TODEF | 10 2005-06-21 17:29 |
| I INCIDENT TRANSACT | 129 iodef1_41k | 低 DUTY 2005-06-21 IODEF Opunbin@ccett.edu | 2005-06-21 17:29 |
| | 128 iodef1_41k 127 iodef5 | 低 DUTY 2005-06-21 IODEF 低 DUTY 2005-06-21 IODEF Oshew03@mails.tsi example | 2005-08-21 17:29 |
| STUDIO | 126 iodef2_40k | the DUTY 2005-06-21 IODEF CERT Incident ID:11 | 18 2005-06-21 17:29 |
| | 125 iodef5_32k 124 iodef5_32k | DUTY 2005-06-21 IODEF Perongeoen.eeu CCENT monent in 12 ## DUTY 2005-06-21 TODEE wnbin@ccent.edu iodef5 | 2005-06-21 17:29 |
| 用产名。duty | 123 iodef2_40k | the DUTY 2005-06-21 IODEF Opunbingscont.edu iodet2_40k | 2005-05-21 17:29 |
| · · · · · · · · · · · · · · · · · · · | 122 iodef3_37k | 低 DUTY 2005-06-21 IODEF Onunbingcost adu iode#5_32k | 2005-06-21 17:29 |
| | / 264931年11 | 《(王-英,英,0,英,0,英,0,年1,英)》 (Januaragena and Indem_State 級別 値班员 受理日期 受理人 (K 篇 1页 1 ▼ 表 2页>) | > |
| | | 秋儀 解析 | IODEF 过滤垃圾邮件 处理 |
| | | | <u>~</u> |
| | | | |
| | | | |
| | | | |
| | | | ×. |
| | | | ○ 删除(信件 |
| | | ○ 生成新事件 ×ML 解密 〕 以证 □ | ・垃圾邮件 ・ ドー步 ・ ・ ・ |
| | | | |
| | | | |
| | (1) 光中 | | Internet |
| | ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ | 配置 帮助 | |
| 株型 () () http://202.112 35.200/czi-bis/import i odef czi | ✓ ●】 特別 | | (|
| Google - C 接来 · 委 局 545 个已担根 等 拼写检查 · 通途项 多 | · Lhangbing · 收件箱 | <u>次</u> 件人 新信 王恕 | 友信日期 |
| vml version=11.0* encortion="ob2312* ? | ▲ 发件箱 | GreportBocer U ULEM Incident ID:172 | 2005-6-21 20 |
| <iodef-document version="1.0."></iodef-document> | | 孙彬 <sunbing iodef1_41k<="" td=""><td>2005-6-21 19:</td></sunbing> | 2005-6-21 19: |
| <pre>- <incidentd>CCERT#130</incidentd></pre> | | 孙彬 <sunbin@ iodef_chinese<="" td="" 🔲=""><td></td></sunbin@> | |
| - <incidentdata></incidentdata> | | hyn <iodef@cc cnexample<="" td="" 🛄=""><td>2005-6-21 19:</td></iodef@cc> | 2005-6-21 19: |
| Constitution of the product of the p | | | 2005-6-21 19: 2005-6-21 19: |
| <description>未自中国的扫描数据</description> <starttime>2004-05-26 11:00:00</starttime> | | hyn <i de="" example<="" flêcc="" jp="" o="" td="" 🔲=""><td>2005-6-21 19: 2005-6-21 19: 2005-6-21 19:</td></i> | 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: |
| <description:未自中間各目論影響、 opecraption=""></description:未自中間各目論影響、> <starttime>2004-05-26 11.00:00(%/StartTime></starttime> <endtime>2004-05-26 12:00:00(%/IndTime></endtime> < | | hyn≺iodef@cc 🔲 JFexample | 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: |
| - Obscription-#10*###19#8#@ | | hyn (i odef@cc D JPexample | 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: |
| Coscription.m2 d1 + ###11#88 (< >Coscription. < <p><idit (1):00.00="" (2)="" 2004-05.24="" at="" fait="" p="" times="" times<=""> <idiput(1):me (1):00.00="" (2)="" 2004-05.24="" fait="" p="" times<=""> <idiput(1):me (1):00.04="" (2)="" 2000-06.21="" fait="" p="" times<=""> <idiput(1):00.04 (2)="" (2)<="" td=""><td></td><td>hynxiodef8cc口 JPexample 初形结构 文本福武 </td><td>2005-6-21 19: 2005-6-21 19: 2005-6-21 19:</td></idiput(1):00.04></idiput(1):me></idiput(1):me></idiput(1):me></idiput(1):me></idiput(1):me></idit></p> | | hynxiodef8cc口 JPexample 初形结构 文本福武 | 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: |
| <pre>cbecorption.md for #df fo</pre> | | ym Godef@cc □ JP example 「 約7.%#約 文本格式 [□: 1002F*Decement <u>金物 类数</u> | 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: |
| <pre>cbesroption.3t 01 #001188.0t </pre> description: | | hyn Gradef@cc ☐ JFexanple 初光结构 [又本稿式] □ 100EF-Decement □ find dant ↓ Inn dant ↓ Inn dant ↓ Inn dant ↓ Inn dant | 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: 2005-6-21 19: |
| description:東白学規算計量機構《Description: description:東白学規算計量機構《Description: description:2001-05:60 21.00000.ftdffffffff description:2001-05:60 21.07:18:04-ABgortTimes - Copect copectation: comain-indef supporting containing and | | hyn Giodefflec 「別形信約」文正形成: □ IODET-Document □ IODET-Document □ Ionet and IO □ Hond and IO □ String String String | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 жл |
| Obscription.考古中特的目類機械(Obscription) Classify and an absolution of the second of the se | | hyn Gidef@cc ① JPerangle 利兆结构 文本格式 □ JDDIP-Document □ Jonident □ President ↓ Description ↓ Descrip | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 Xal |
| <pre>closcription:#10+##fifi###/closcription> clastTime>200+63><21 liabade/fitatTime> clastTime>200+63><21 liabade/fitatTime></pre> | | hyn Gindef@ec ☐ JPersonple 1975/849 [Xz=Rax] □ 100EP-Decommt □ Innident] □ Downthats □ | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-8-21 19 |
| <pre>cbecryption.mt df ###fiflest#clocecryption: classITimes2004-80-54 Jimoling/StaffTimes chappertImes2005-80-51 JiJiBiOt-/ReportTimes - Contact - Contact</pre> | | Nym Gedef@ec | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 |
| <pre>cdscription.#1d*##fiti#&@clearphono cdscription.#1d*##fiti#&@clearphono cdsportTime2006-02:110:00.0f*#tTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdcscription. cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-0*ReportTime3 cdsportTime2005-06-2117:10:00-0*ReportTime3 cdsportTime2005-0*ReportTime2005-0*ReportTime3 cdsportTime2005-0*ReportTime2005-0*ReportTime3 cdsportTime2005-0*ReportTime20</pre> | | hyn Gidef@ec ☐ JPerangle | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 ແລະ |
| <pre>c-becorption-#10*###fife#&cocception- c=tartimes200+6:05-21.10:000/sflattimes c-beportImes2005-05-21.17:80-04-AlegootTimes - <constants- c=tants-tool- c=tants-tool- c=tants-tool- c=tants-tool- c=tants-tool- c=tants-tool- c=tants-tool- c=tants-tool- c=tool-</constants- </pre> | | Nym Giode Riget □ JP example | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 |
| <pre>cdscription.#10*#bft#dsteverption> cdscription.#10*#bft#dsteverption> cdscription</pre> | | hyn Gidef@cc ↓ JPerangle | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 xal |
| <pre>c-becorption-#10*###fife#&corption- c-disput message = 100 money of a strategy = 100 money = 100 mone</pre> | | NymCided@ec | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 |
| <pre>cdscription=#10*###file##cocoptions cdsprtTme>200+8:0:42 intoRm0.file#Tmeo cdsportTme>200+8:0:42 intoRm0.file#Tmeo cdsportTme>200-8:21 if:ReportTmes cdsportTme>200-8:21 if:ReportTmes cdsportTme>200-8:21 if:ReportTmes cdsportTme>200+8:21 if:ReportTmes cdsportTme>200+8:21 if:ReportTme> cdsportTme>200+8:21 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cdsportTme>200+05-20 if:ReportTme> cds</pre> | | hyn Giodef@ec ① JPersongle 初形结构 文本格式 〕 □ IDEET=Document □ Incident □ | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-6-21 19 就就 |
| <pre>c-description.#df ###fif#df df cocceptors. c-description.#df ###fif#df df cocceptors. c-description.#df ###fif#df df cocceptors. c-description.df cocceptors. c-description.df cocceptors. c-description.df cocceptors. c-description.df cocceptor cocceptor cocceptors. c-description.df cocceptor cocceptor</pre> | | hyn Giodef@cc | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-8-21 19 |
| <pre>cdscription.#df ###file#& cocception: cdscription.#df ###file#& cocception: cdsportIme:2000-80-21.17:18:04-/ReportTimes cdsportIme:2000-80-21.17:18:04-/ReportTimes cdcstription: cdst</pre> | | Non Ci de Riec ① JP example | 2005-0-21 19 2005-0-21 19 2005-0-21 19 2005-0-21 19 xnl |
| <pre>description.ml 0+494bf1Bb8(c)0escriptions description.ml 0+494bf1Bb8(c)0escriptions deportTms:2000-05/10/11/0 deportTms:2000-05/21/12/18/04-AbgontTmss - Copectations - Compared to 1-3-3310-0000 / telephones - Compared to 1-3-3310-0000 / telephones - Compared to 1-3-3310-0000 / telephones - Copectations - Copectations</pre> | | hyn Giddef@cc Proceedings 文字形成了 □ 10007-Document □ 10007-D | 2005-6-21 19 2005-6-21 19 2005-6-21 19 2005-8-21 19 |





Virus Detection System







HONEYPOT





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 Hot Maricel Construct Enclose Sy Relpone to 1909 dination (ent) of China