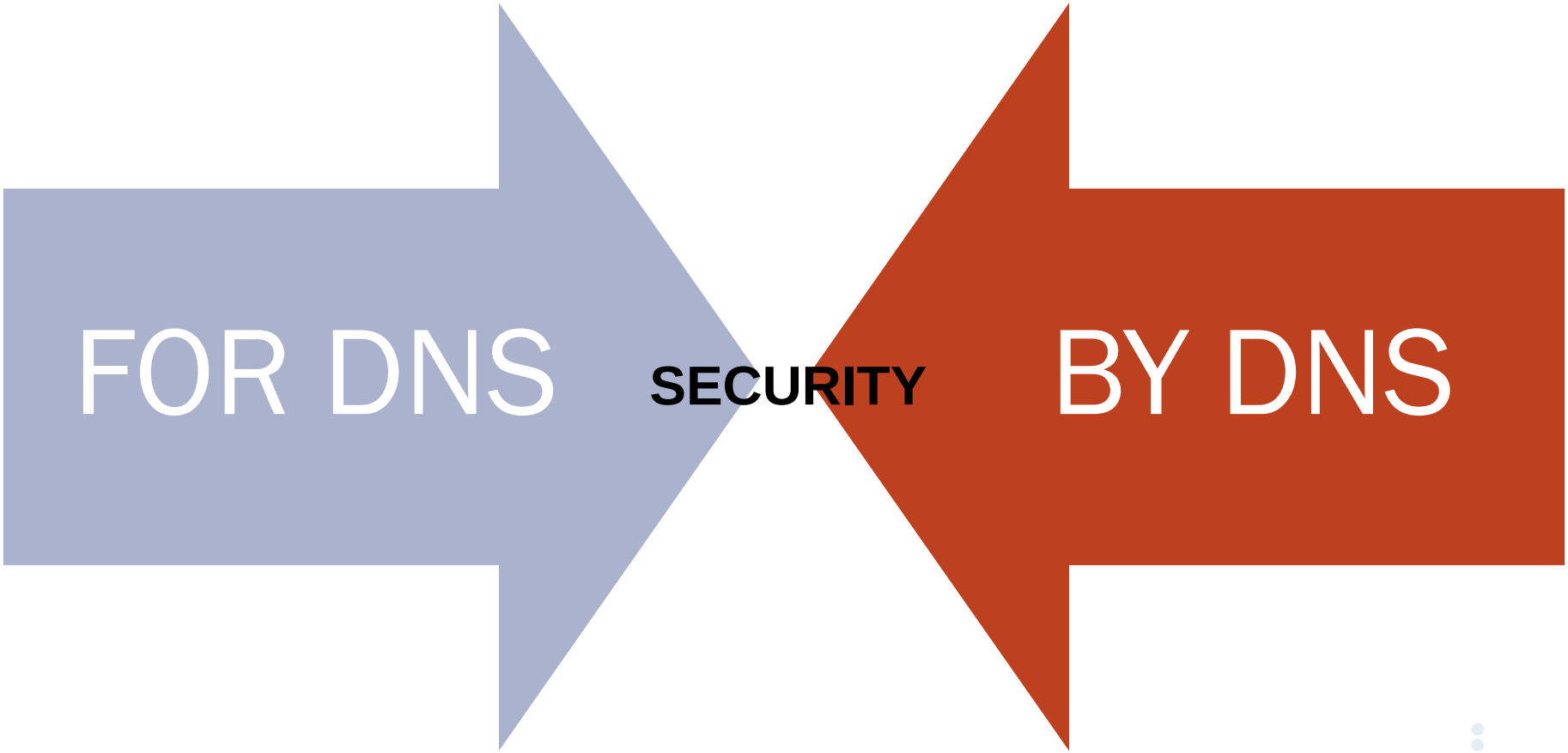
Security, For DNS and by DNS

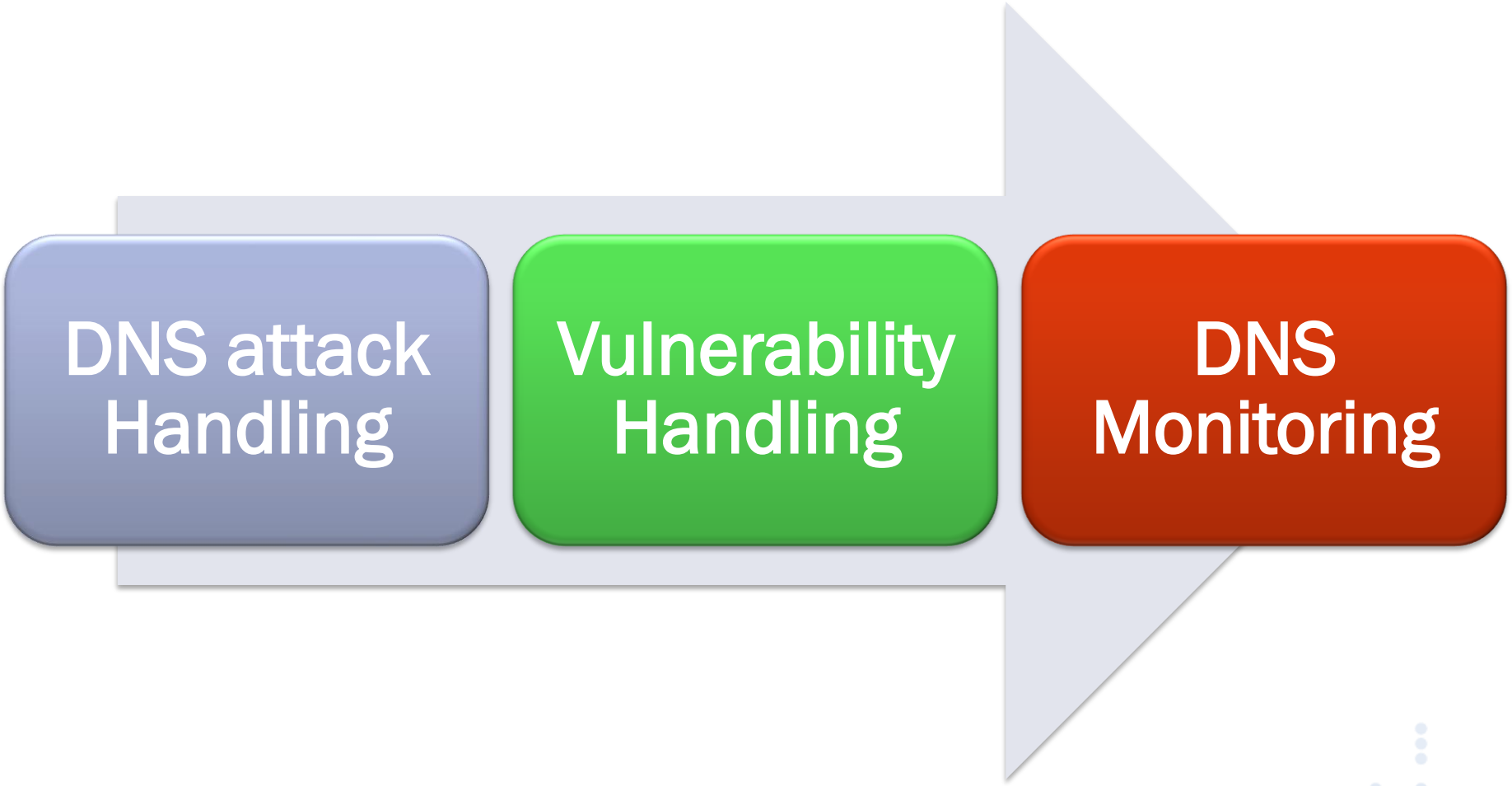
ZHOU Yonglin

Beijing, Nov 009

DNS and Security

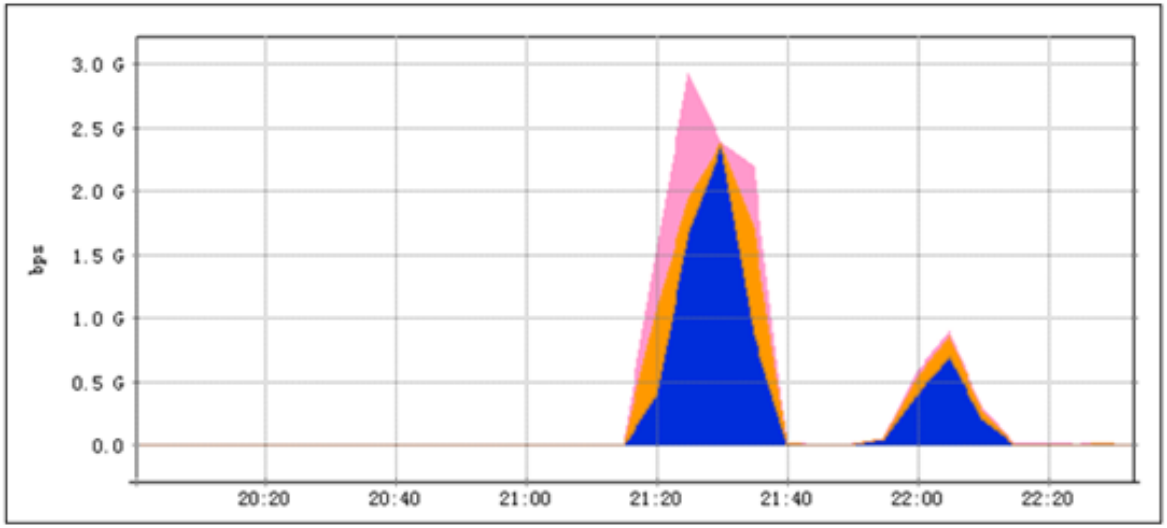


SECURITY, FOR DNS



5.19 “Storm Gate”: Attack Flow Against DNSPOD

2009/05/18 21:00

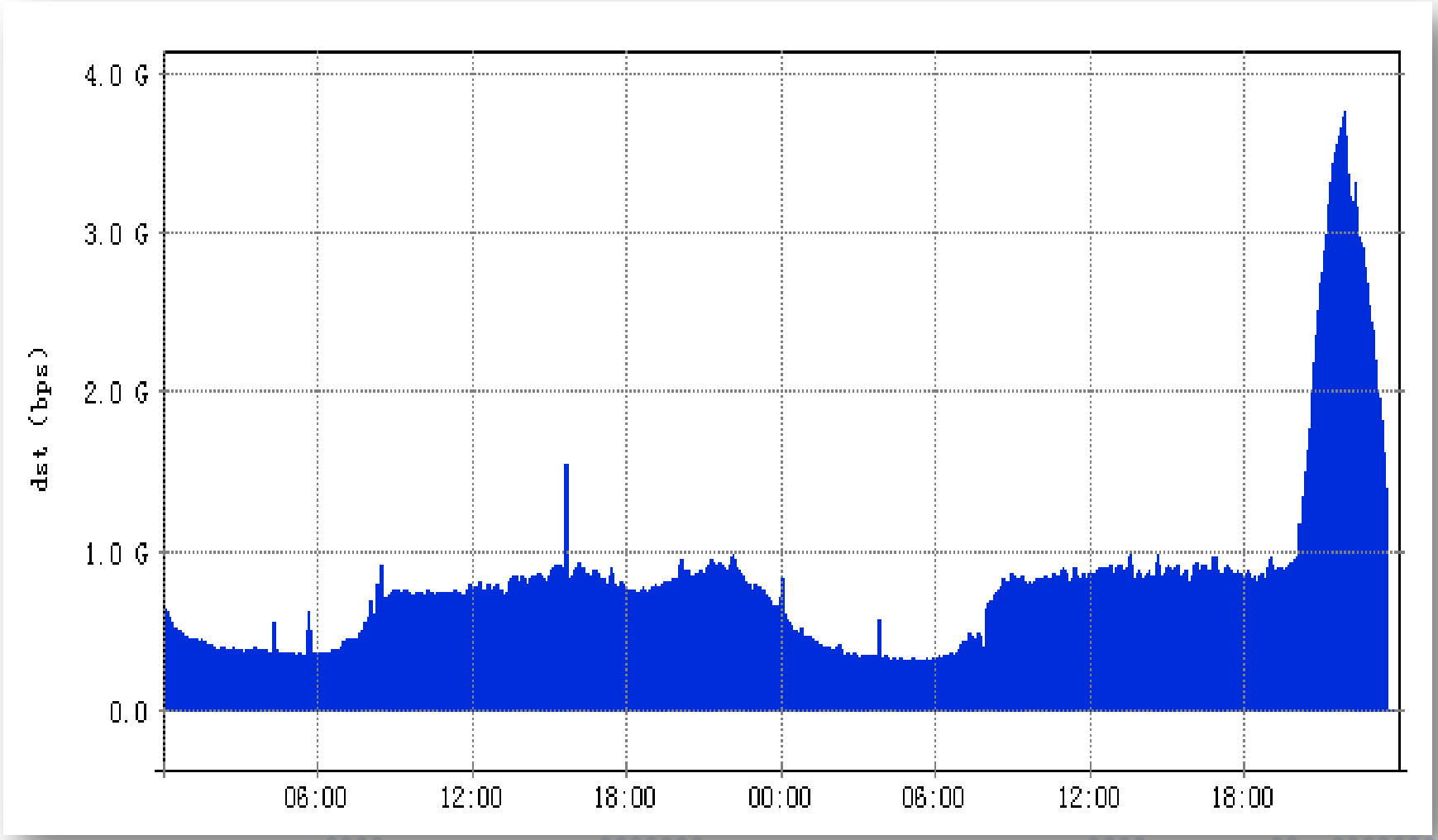


客户： DNSPod

Excel 导出

All	目的IP	流量	百分比
☑	61.160.200.160	225.19M	61.50%
☑	61.136.59.6	71.51M	19.53%
☑	222.216.28.18	69.49M	18.98%
☐	全部	366.19M	100.00%
All	目的IP	流量	百分比

5.19 “Storm Gate”: General View of Recursive DNS Query Flow of China networks



05/18-05/19

Emergency Response

- 2009/5/19
  - Monitor the abnormal flow against the DNS Servers
  - Analyze the abnormal flow against the DNS Servers
- 2009/5/22
  - Trace the attack origins against DNSPOD
- 2009/5/25
  - Provide evidence for case cracking, prosecution

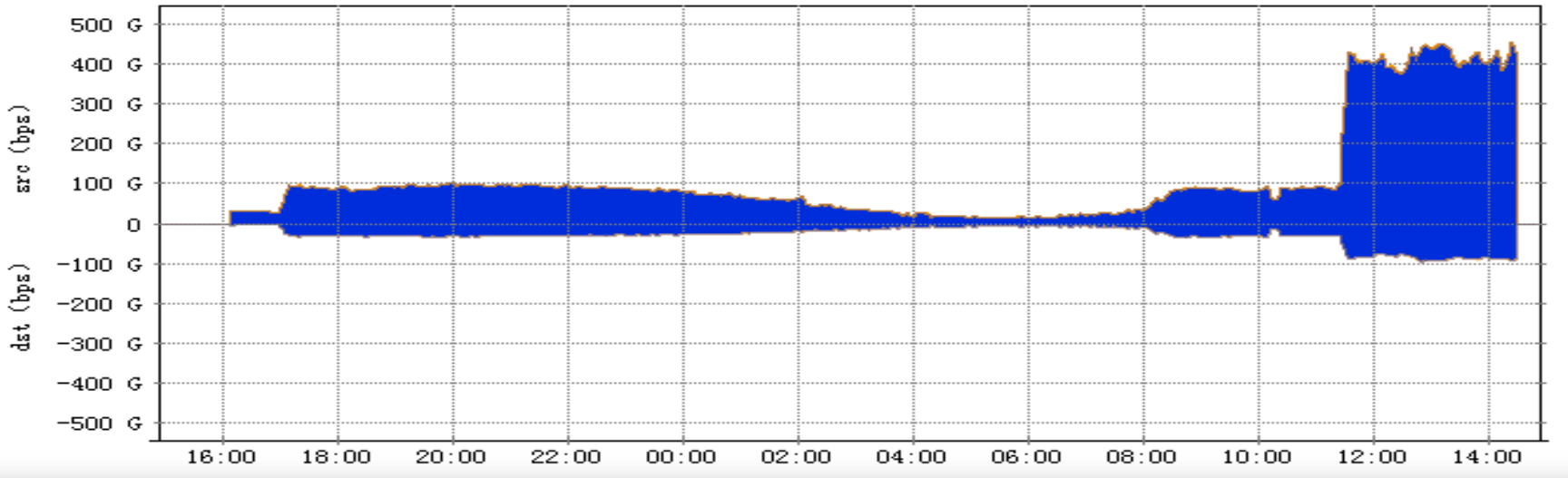
Other Attack Cases Against DNS

- 2009/6/9 9:30
  - DDos attack against 4 DNS servers of XinWangHuLian, Beijing(www.dns.com.cn)
  - 0.5 million domain names got resolution failures
- 2009/7/3 3:00
  - DDos attack against DongNanRongTong, Xiamen
  - Attack Volume 300M, service outage lasting 7 hours or so
- 2009/6/10- /6/12
  - DDos attack against XiWang Dynamic DNS Service System
  - Service outage influences millions of enterprises and customers

DNS Spoof Vul. Published by Dan Kaminsky

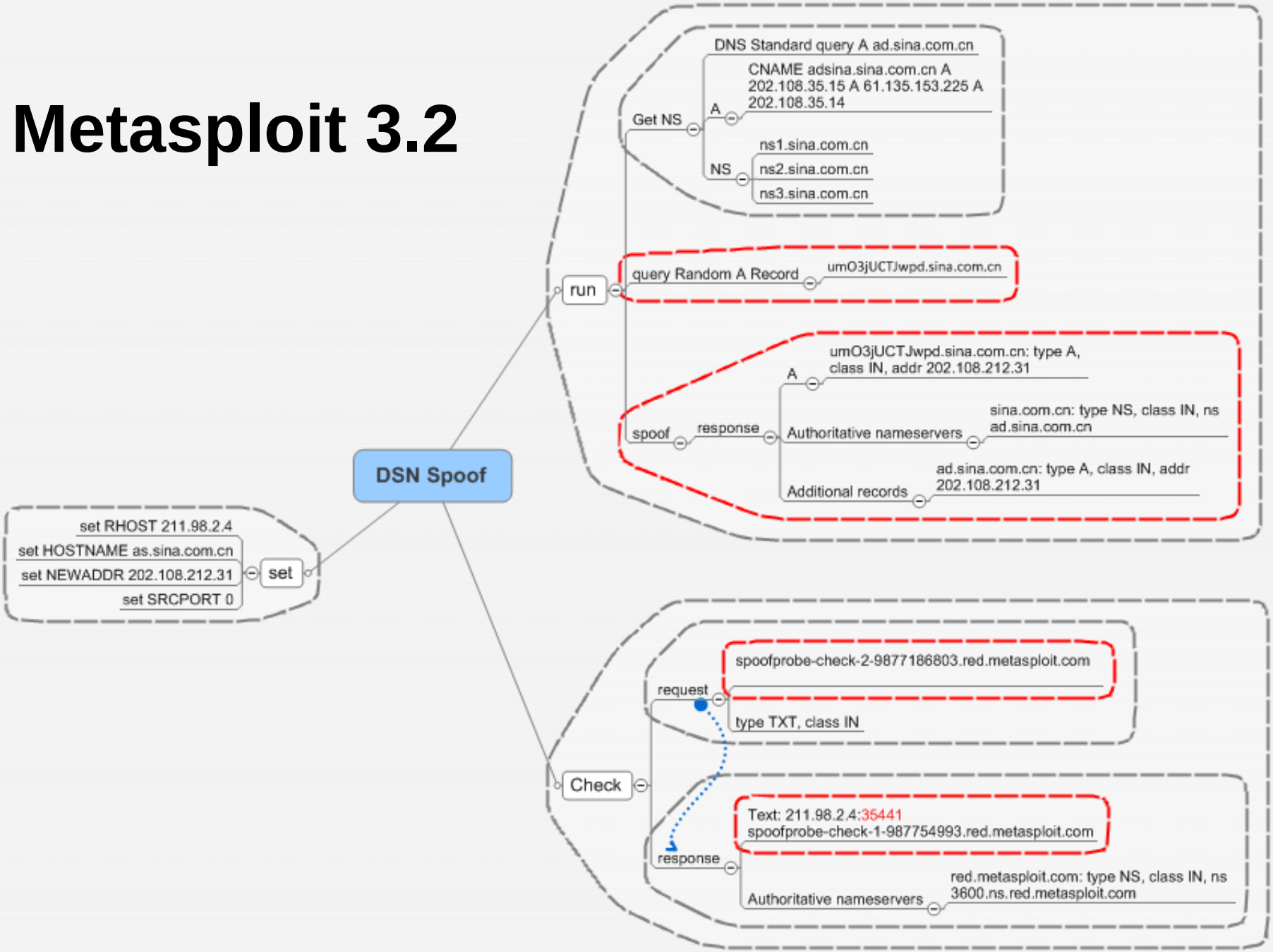
CNCERT/CC

CNCERT/CC



-::DATE	-::DESCRIPTION
2008-07-29	Cisco IOS 12.3(18) FTP Server Remote Exploit (attached to gdb)
2008-07-28	Trend Micro OfficeScan ObjRemoveCtrl ActiveX Control BOF Exploit
2008-07-28	Velocity web-server 1.0 Directory Traversal File Download Vulnerability
2008-07-25	BIND 9.x Remote DNS Cache Poisoning Flaw Exploit (c)
2008-07-24	Microsoft Access (Snapview.ocx 10.0.5529.0) ActiveX Remote Exploit
2008-07-24	BIND 9.x Remote DNS Cache Poisoning Flaw Exploit (py)
2008-07-23	BIND 9.4.1-9.4.2 Remote DNS Cache Poisoning Flaw Exploit (meta)

Metasploit 3.2



Emergency Response

- 2008/7/28
  - Publishing the Vulnerability Report on CNCERT web site
  - Convening telecommunication operators, DNS Registry/Registrar for information sharing
- 2008/7/29
  - Monitoring Domain Name Hijack
  - Monitoring attack flow against DNS service

Bind Dos Vul.(CVE-2009-0696)

- Report：2009/07/28
  - Debian Bug report logs - #538975
    bind9 dies with assertion failure (db.c:579)

- Detail:：
  - db.c:659: REQUIRE(type != ((dns_rdatatype_t)dns_rdatatype_any)) failed exiting (due to assertion failure).
- Affected Systems:
  - ISC BIND 9.x(0<=x<=6)

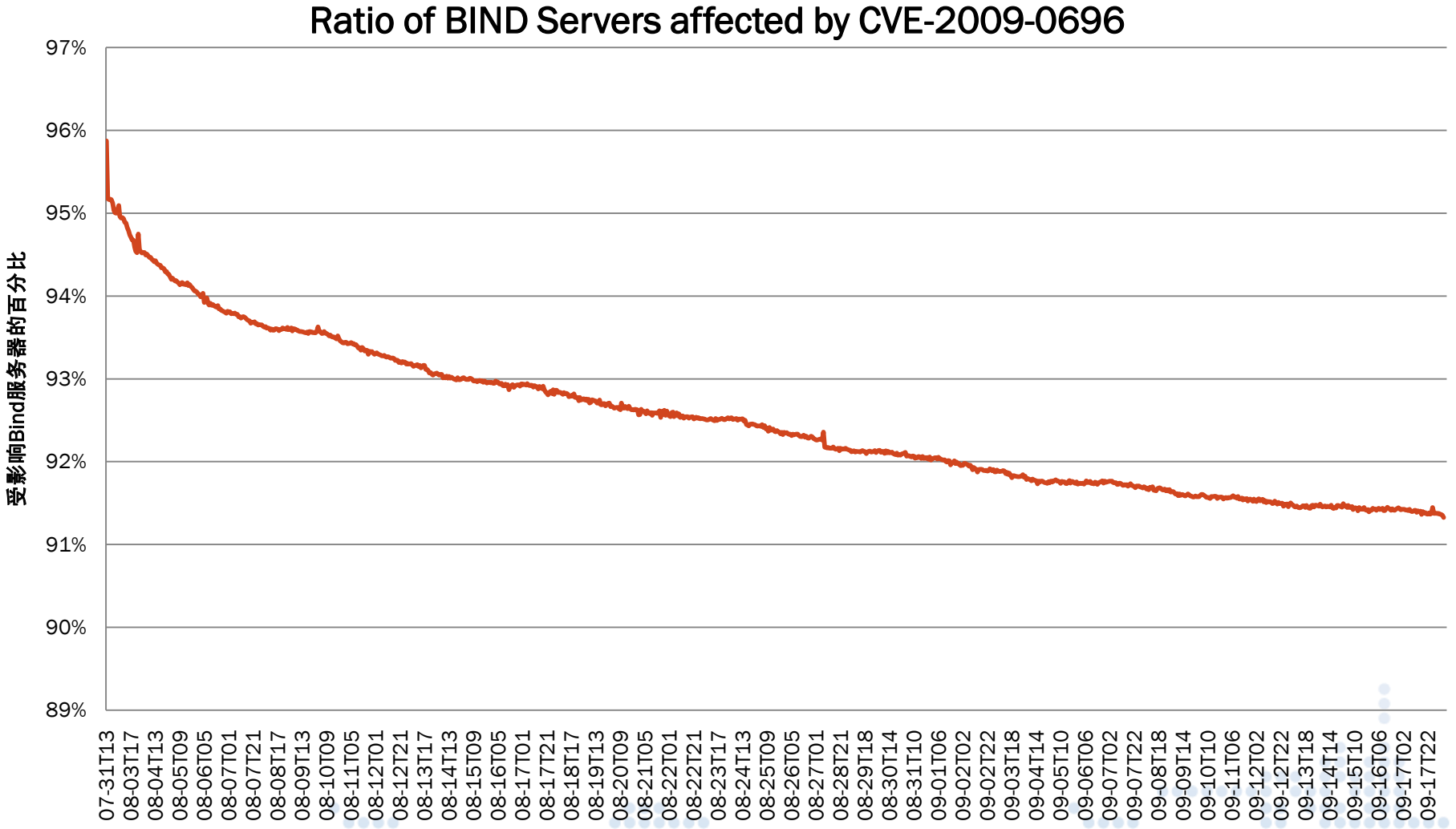
Emergency Response

- 2009/7/29
  - Verify and analyze vulnerability
  - Publish BIND 9 critical vulnerability report
  - Convene telecommunication operators for information sharing
- 2009/7/30
  - Publish BIND 9 Vulnerability danger level and scope
  - Convene registry and registrar for information sharing and response proposal
- 2009/7/31
  - Track the vulnerability patch progress

Bind Dos Vul. Patch Application Monitoring

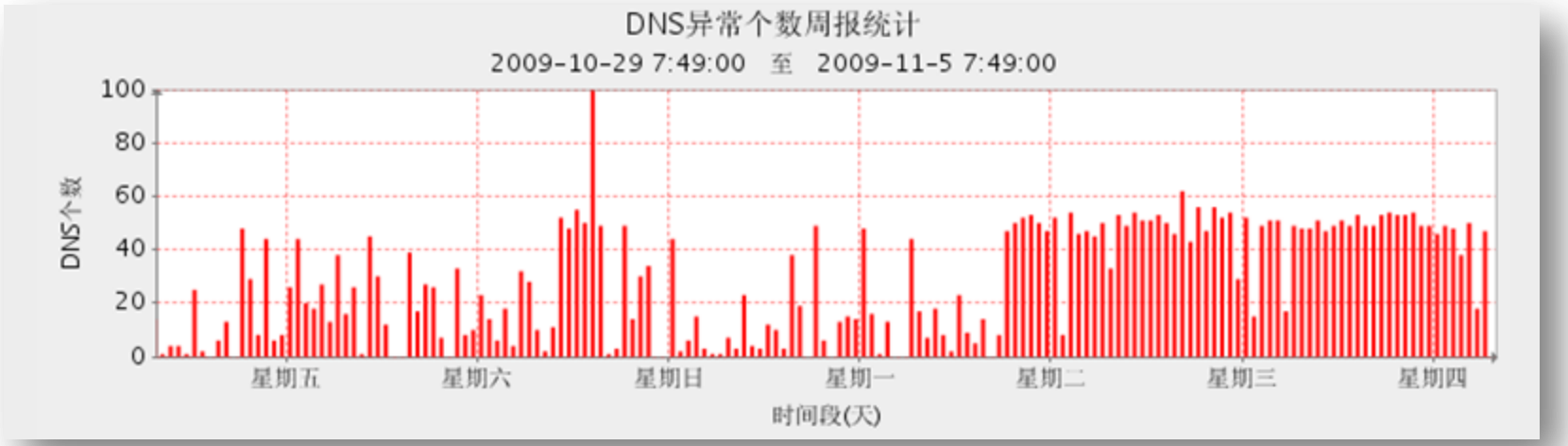
CNCERT/CC

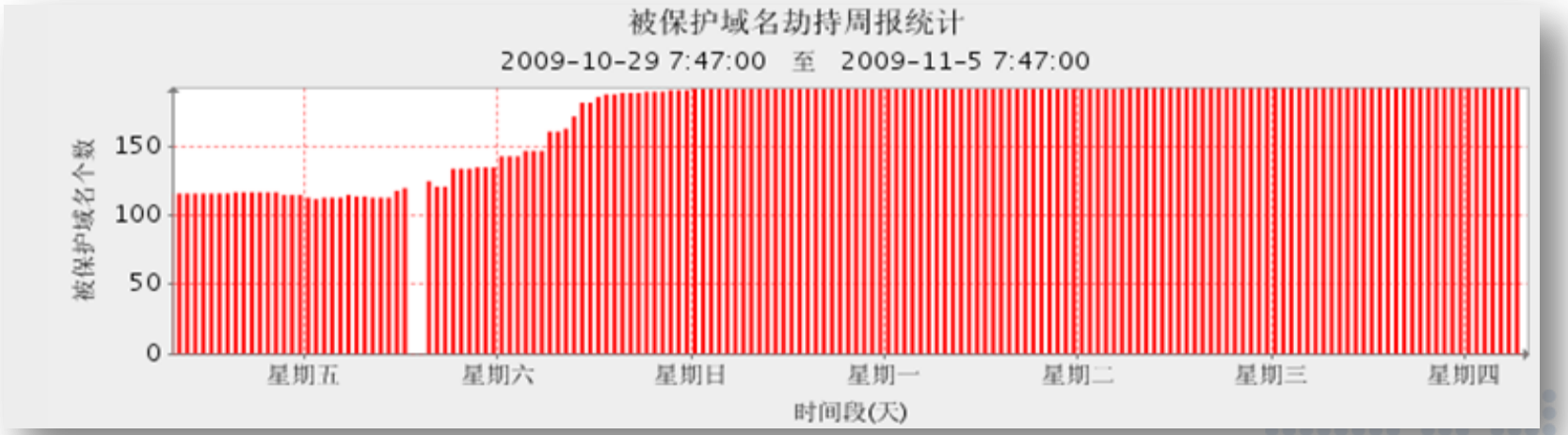
CNCERT/CC



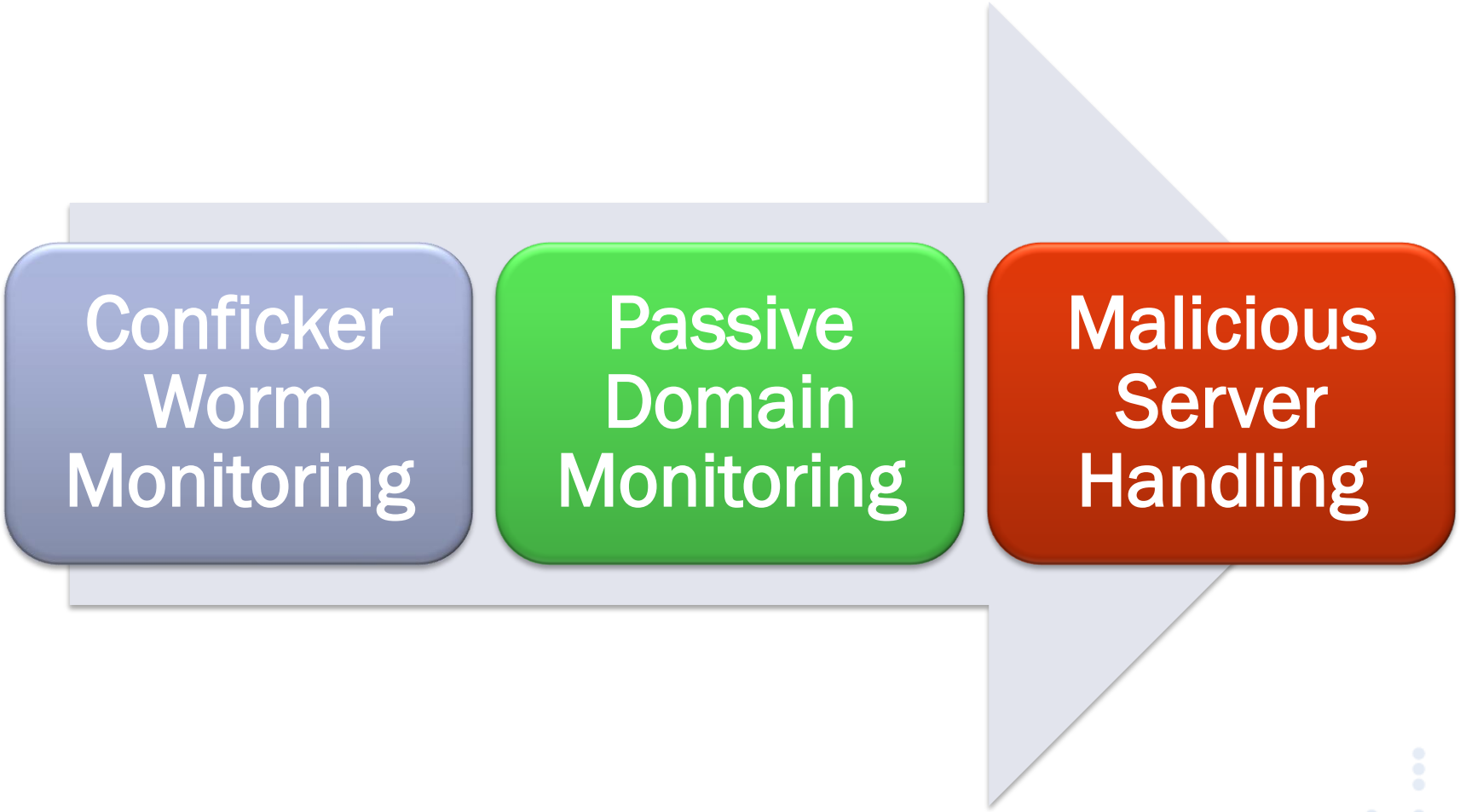
07/31-09/17

DNS Status and Domain Name Hijack Monitoring



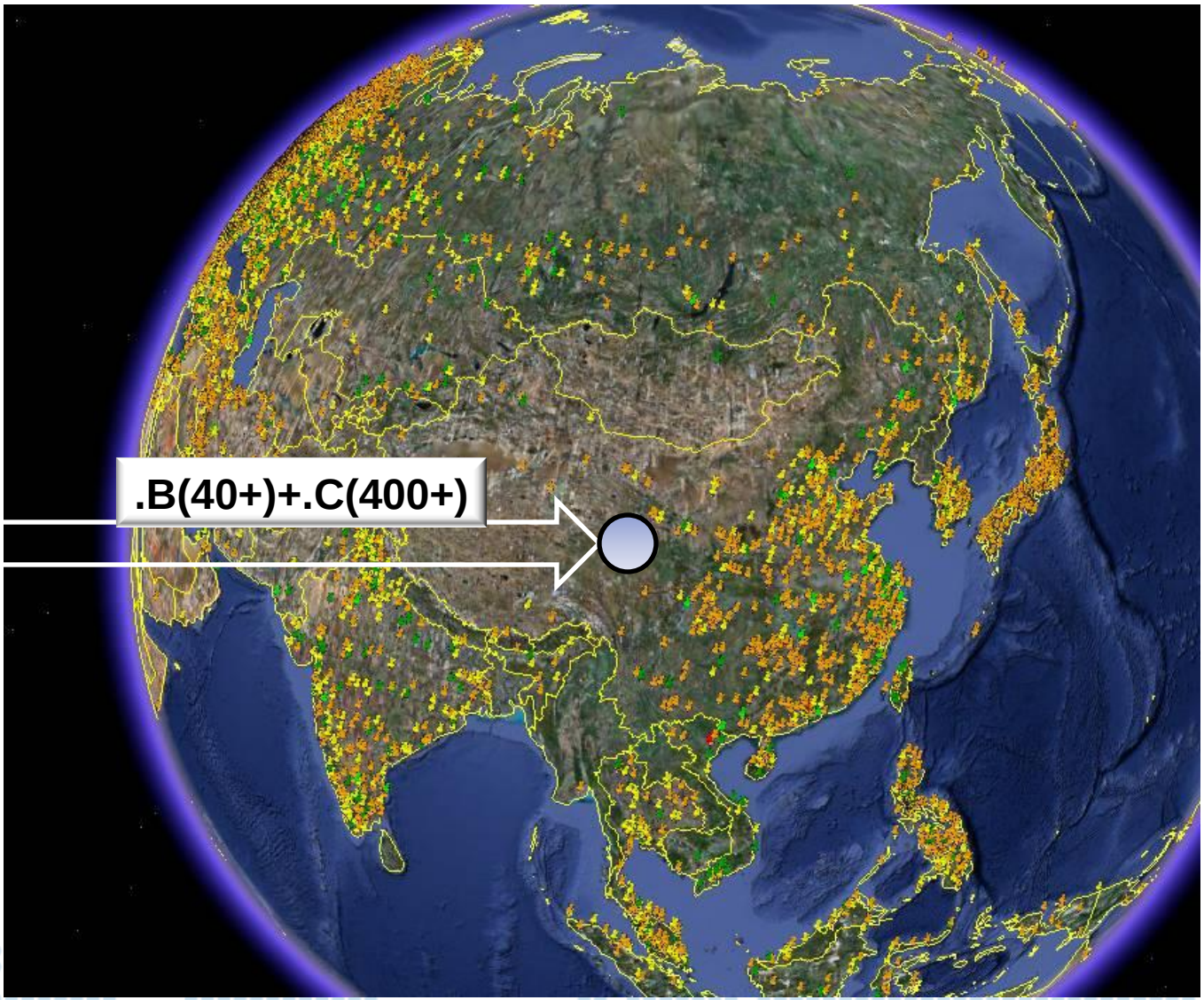


SECURITY, BY DNS



Conficker Sinkhole Based on DNS Support

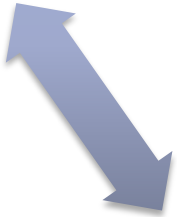

```
30.09.2009 rdufcwbxalh.cn B
30.09.2009 zvjvobgyho.cn B
30.09.2009 iqlzwsf.cn B
30.09.2009 noihybwi.cn B
30.09.2009 jtbwcfum.cn B
30.09.2009 elrnp.cn B
30.09.2009 hbfqkcvav.cn B
30.09.2009 zgzsczkisxz.cn B
30.09.2009 agqyw.cn B
30.09.2009 yrnjgurchpx.cn B
30.09.2009 lhyvjmjqes.cn B
30.09.2009 qkvybvug.cn B
30.09.2009 fjljulvhz.cn B
30.09.2009 rfllz.cn B
30.09.2009 uifccsxmy.cn B
30.09.2009 qheabp.cn B
30.09.2009 gzgpnesl.cn B
30.09.2009 wamkaiyebmz.cn B
30.09.2009 dcpksqow.cn B
30.09.2009 uohkvlzcziq.cn B
30.09.2009 gwqiz.cn B
30.09.2009 tqlgipui.cn B
30.09.2009 ewqjy.cn B
30.09.2009 ryeiu.cn B
30.09.2009 pxupn.cn B
01.10.2009 xjjqzawizh.cn B
01.10.2009 oukdihcspm.cn B
01.10.2009 ochqj.cn B
01.10.2009 clkggjln.cn B
01.10.2009 axexcen.cn B
01.10.2009 thhwwzektti.cn B
01.10.2009 wcydq.cn B
01.10.2009 noeqp.cn B
01.10.2009 awlxtt.cn B
```



Passive DNS Monitoring by Telecommunication Operator

Analysis on Abnormal Domain Name

- Behavior based Botnet Controller Analysis



IP Reverse Resolution

- Botnet Controller Domain Name Derived from IP
- Tracking of Malicious Domain Name

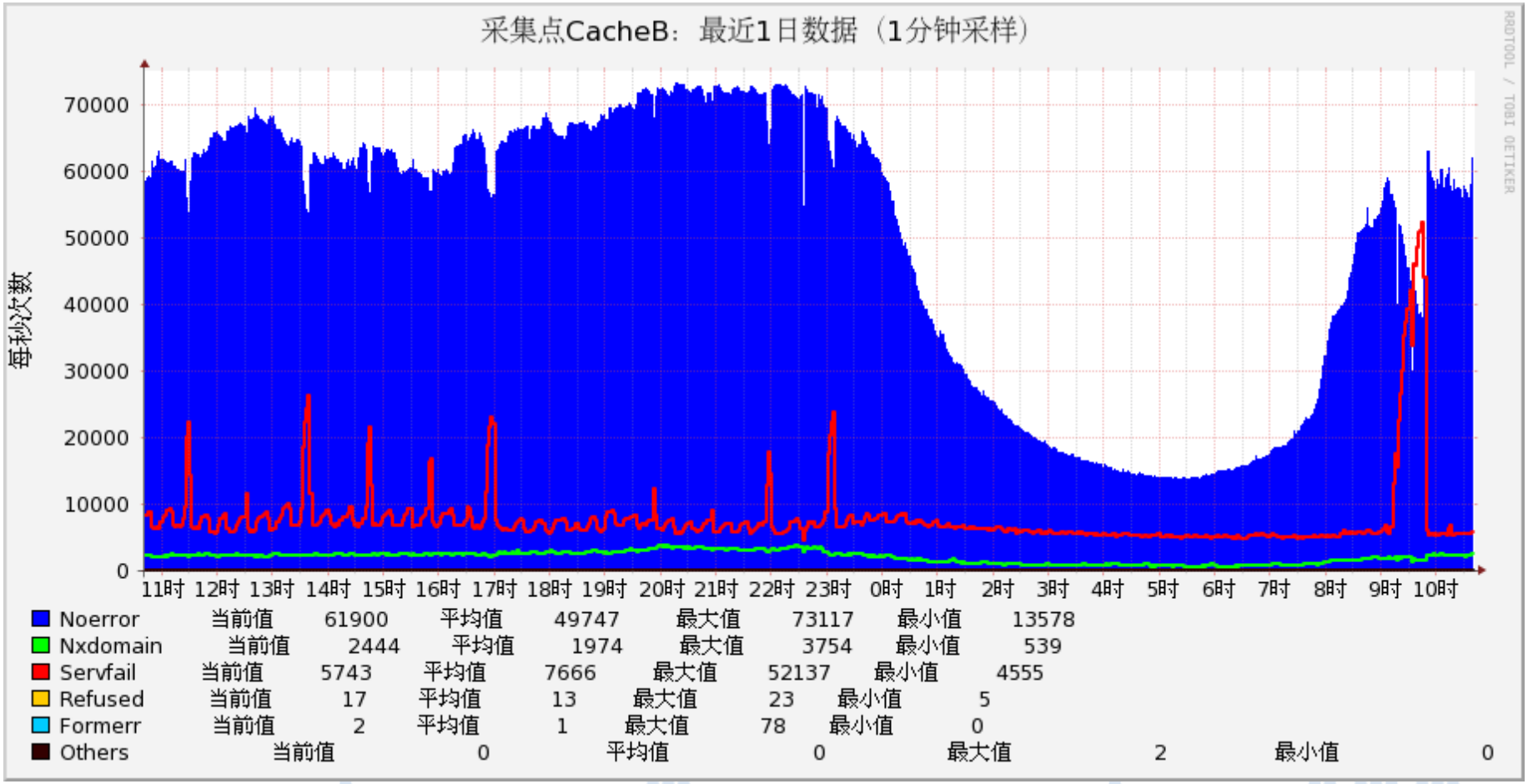
DNS Server Status Analysis

- Request number for specific domain names
- Request Client number for specific domain names

Behavior Based Controller Abnormal Domain Name Analysis

darkroot.3322.org	117.11.227.119
zjddos.3322.org	121.12.127.173
haoj8.3322.org	124.234.102.22
ashly.9966.org	221.236.6.230
magic365.9966.org	74.208.171.169

DNS Server Status Analysis



Statistics of TLD Request - TOP10

CNCERT/CC

CNCERT/CC

TLD	Request Times	Percentage
com	1004715	70.21%
cn	183685	12.84%
net	120863	8.45%
org	26518	1.85%
in-addr.arpa	25217	1.76%
info	6144	0.43%
tv	5843	0.41%
biz	4578	0.32%
cc	4538	0.32%
ws	4237	0.30%

2009-11-04T20-55

Statistics of Second Level Domain Name Request - TOP10

CNCERT/CC

CNCERT/CC

SLD	Request times	Percentage
qq.com	455506	31.83%
com.cn	59997	4.19%
sandai.net	40742	2.85%
baidu.com	30941	2.16%
tencent.com	28032	1.96%
360safe.com	20741	1.45%
xunlei.com	20521	1.43%
sohu.com	11543	0.81%
3322.org	11442	0.80%
taobao.com	10565	0.74%

2009-11-04T20-55

IP Reverse Resolution

Select distinct domain_name, time form pasv_dns_table where ip= ‘60.13.152.131’

- 2009-11-05T06-25 www3.caishow.com
- 2009-11-05T06-25 www.msjyfund.com.cn
- 2009-11-05T06-25 s18.wo99.com
- 2009-11-05T06-25 www.1mi1.cn
- 2009-11-05T06-25 wwwxjrsf.cn
- 2009-11-05T06-25 q8me.igap.bihu.com
- 2009-11-05T06-25 wap11.qqmail.com
- 2009-11-05T06-25 b0bfac4.iprophesy.com.cn
- 2009-11-05T06-25 event50.wanmei.com
- 2009-11-05T06-25 pfad.netmovie.com.cn
- 2009-11-05T06-25 www.60.13.152.131.com
- 2009-11-05T05-50 gxway168cn.net
- 2009-11-05T05-50 e891.p.akamaiedge.net
- 2009-11-05T05-50 www.ebank.95599.cn
- 2009-11-05T05-50 a1293.g.akamai.net
- 2009-11-05T05-50 a151.ce.w.tl88.net

Tracking Malicous Domain Name Record

- Select distinct time, domain_name, ip form pasv_dns_table where domain_name= ‘114pc1.3322.org’
  - 2009-11-05T06-05 114pc1.3322.org 61.164.109.4
  - 2009-11-05T06-10 114pc2.3322.org 60.191.196.227
  - 2009-11-05T06-15 114pc3.3322.org 61.164.108.213
  - 2009-11-05T06-20 114pc4.3322.org 60.191.239.123
  - 2009-11-05T06-25 114pc5.3322.org 60.191.196.227
  - 2009-11-05T06-30 114pc6.3322.org 60.191.232.166

Malicious Server Handling by Hitting Domains

- In the past 12 months, about 567 domains that used by malicious servers have been stopped.
  - WHO
    - CNCERT、CNNIC、Chinese Registrars
  - WHAT
    - Trojan or Botnet Control Serves
    - Maware sample download source
    - Phishing page host site, etc
  - WHEN
    - General Duty
    - Special Events Assuarance
      - Beijing Olympics
      - National Day Celeberation
      - National Games, … etc

Malicious Domain Name BlackList

CNCERT/CC

2009-11-05-domain-black-list.txt
rbl.efnet.org
rbl.efnetrbl.org
s.rizon.net
shrikehosting.Com
uploader.me.uk
waxs.kaist.ac.kr
www.AbleNET.Org
www.Thoing.com
www.a0hell.net
www.ablenet.org

SECURITY, FOR DNS AND BY DNS