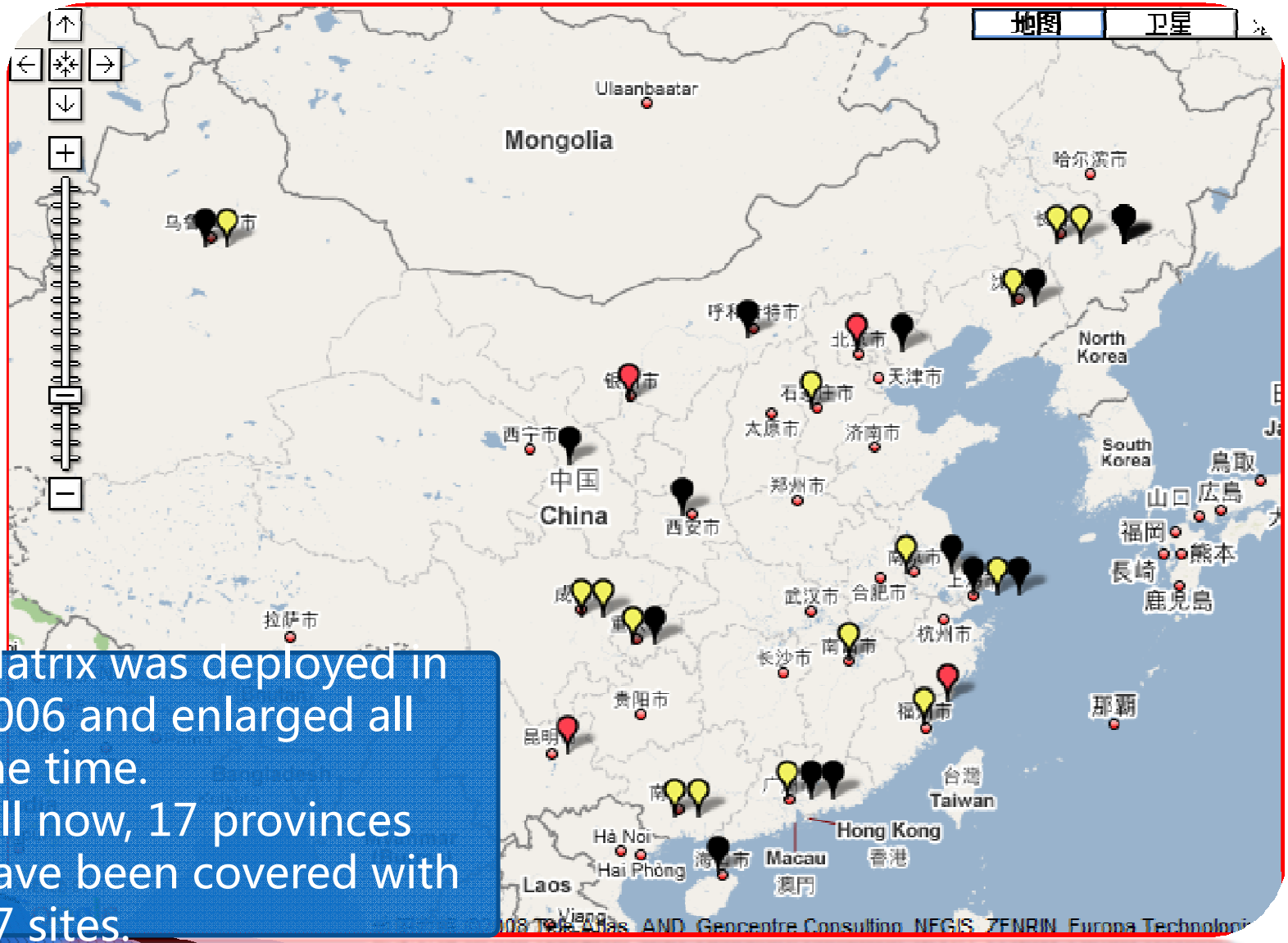
CNCERT/CC

Matrix, a Distributed Honeynet and its Applications

Yonglin ZHOU
CNCERT/CC

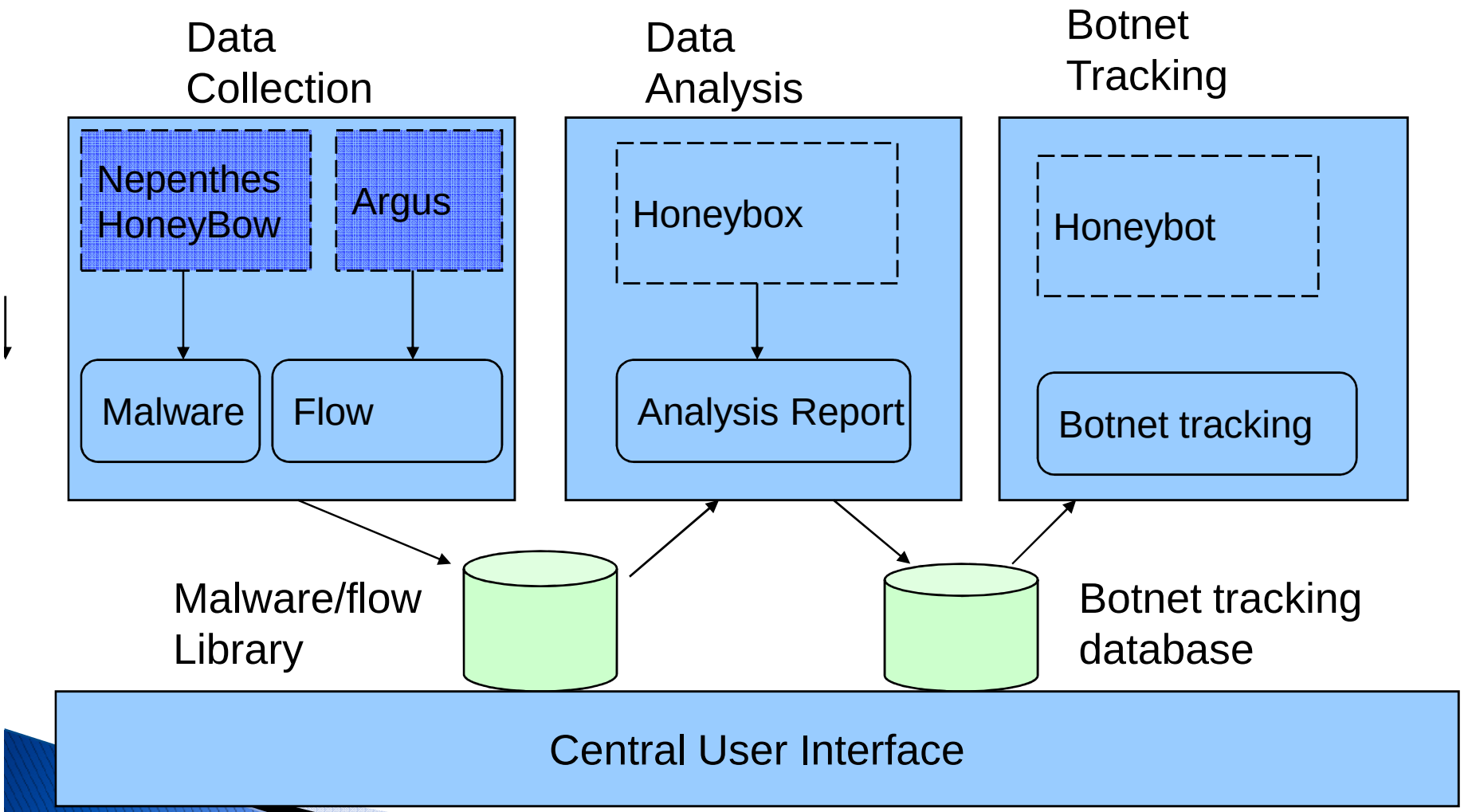
Distribution



Matrix was deployed in 2006 and enlarged all the time.
Till now, 17 provinces have been covered with 27 sites.

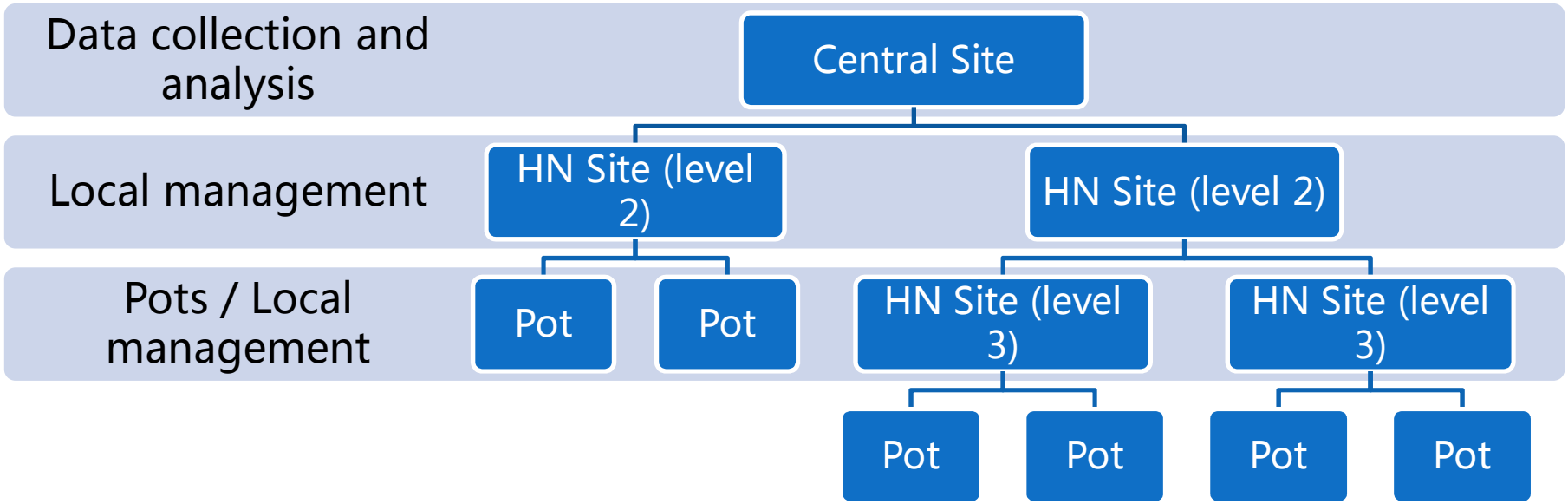
CNCERT/CC

Main Functions



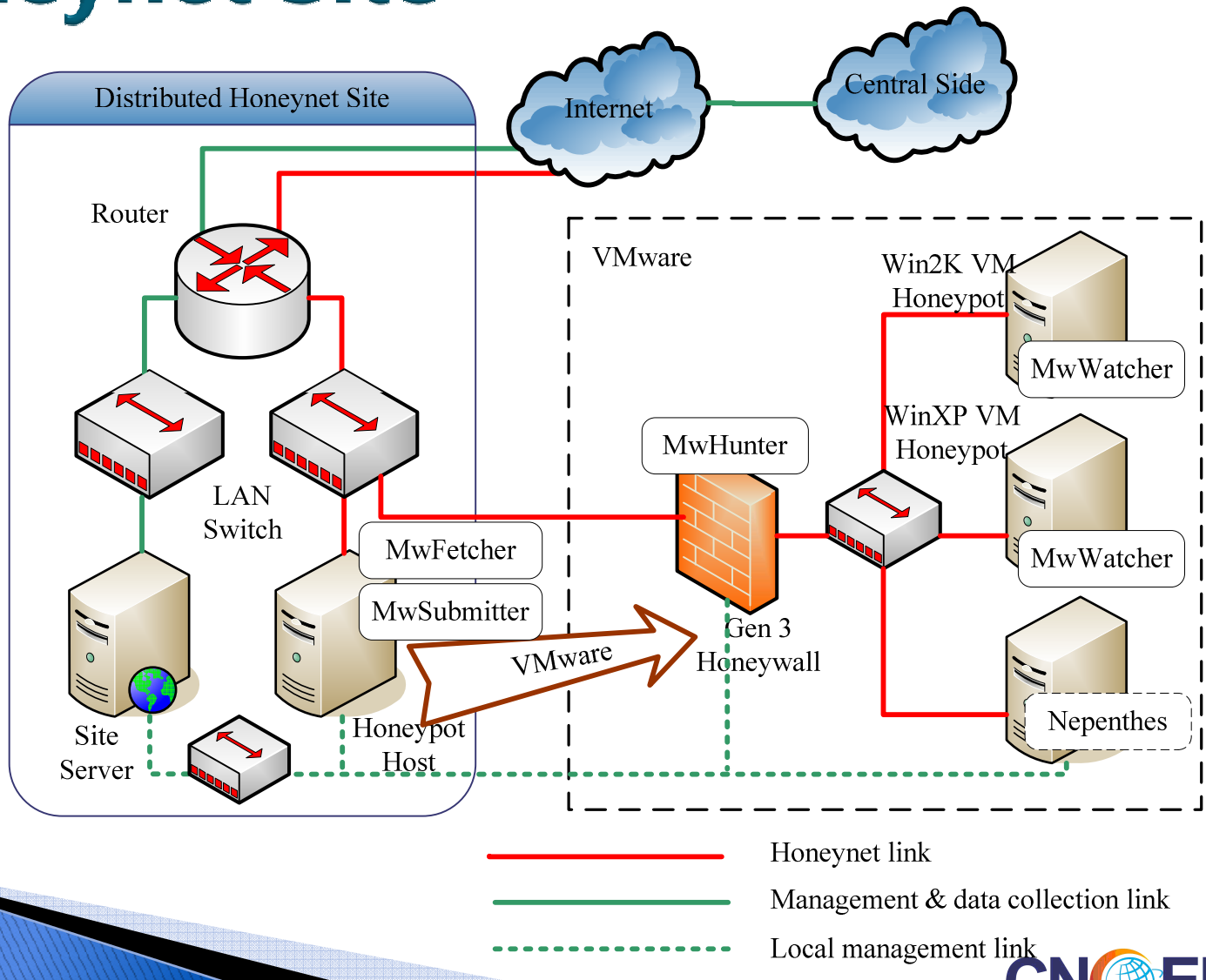
CNCERT/CC

General Architecture

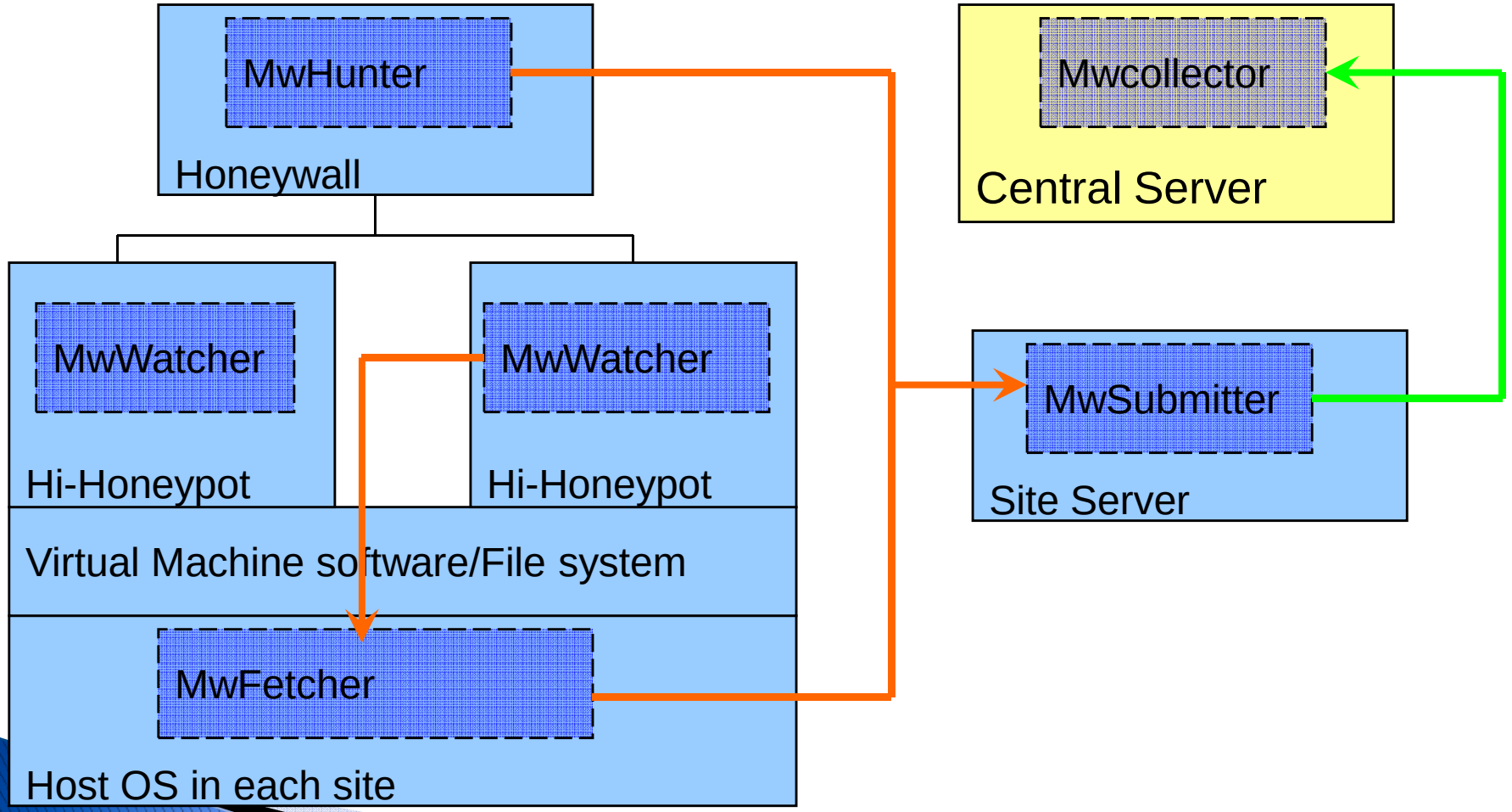


CNCERT/CC

Architecture of the Distributed Honeynet Site



Honeybow Architecture

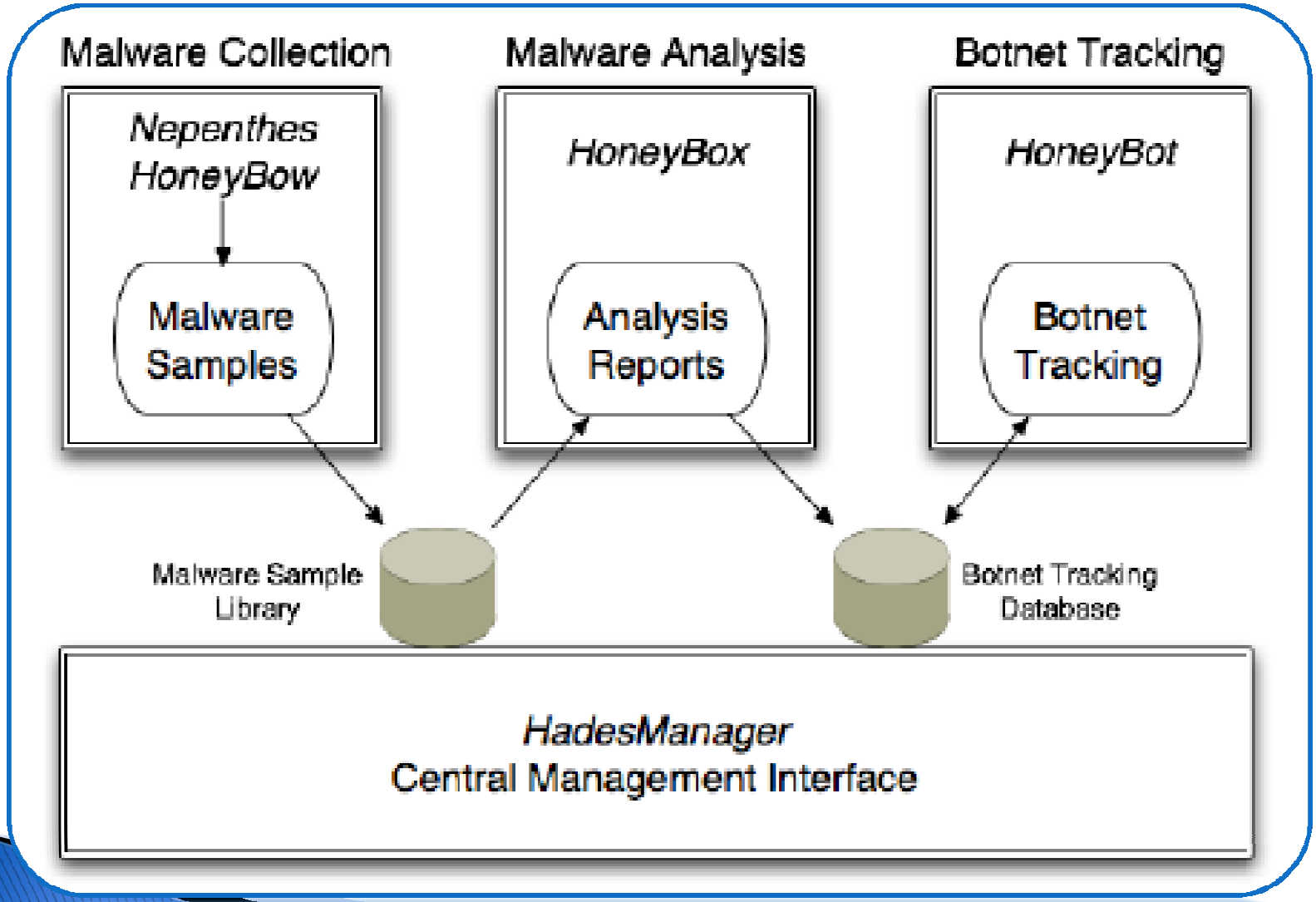


Compare the malware collection performance between Nepenthes and HoneyBow

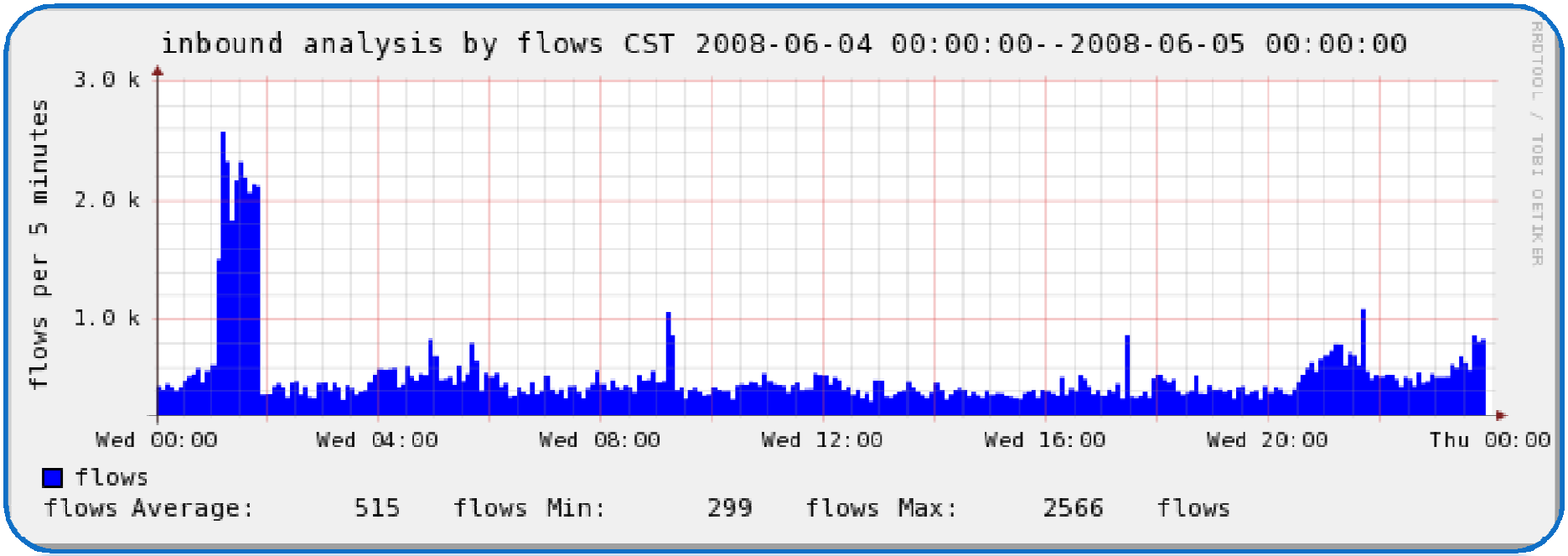
	Captures (hit count)	Binaries	Variants	Families
Nepenthes (Total)	427,829	17,722	467	64
HoneyBow (Total)	376,456	82,137	1,011	171
Nepenthes (Average per day)	1,539	63.7	15.0	8.2
HoneyBow (Average per day)	1,359	296.0	17.8	10.6

- hit count of about 800,000
- nearly 100,000 unique sample binaries
- about 2,800 collected and 360 new unique binaries per day.

The Central Site of Matrix

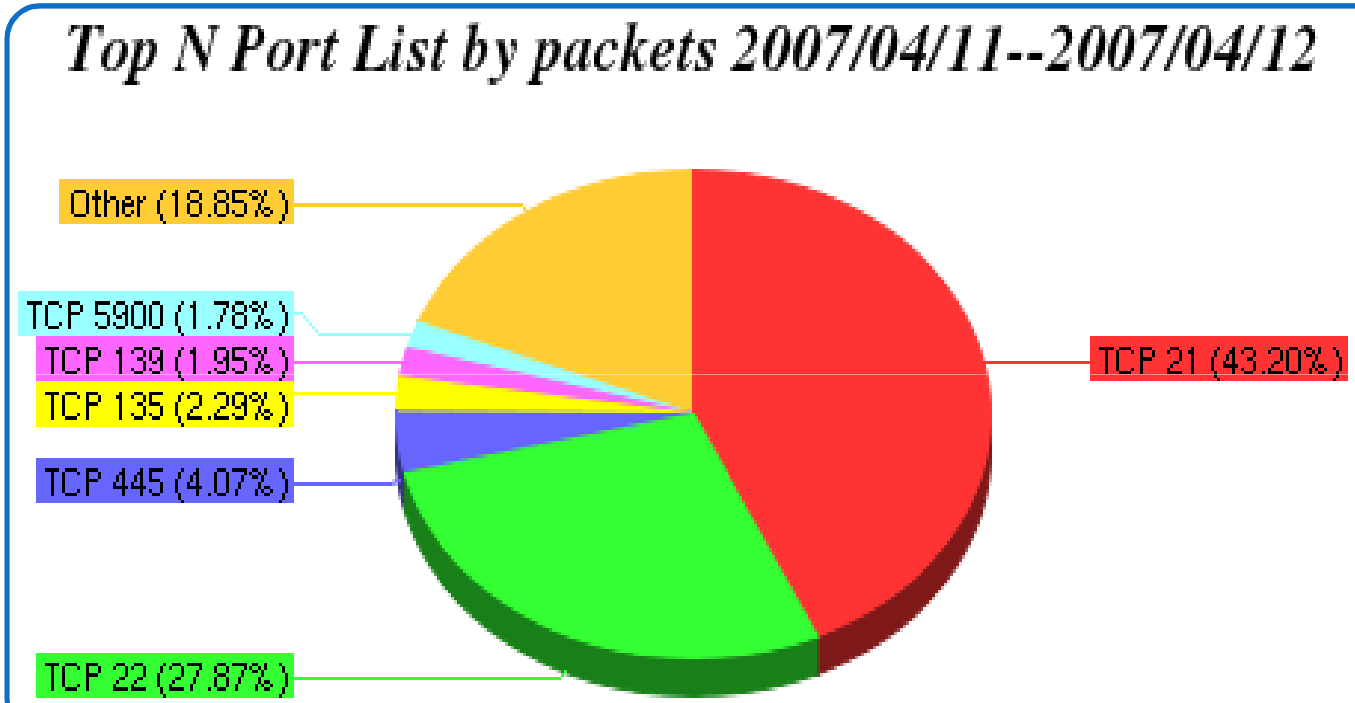


Function I: Log Attack Flows



CNCERT/CC

Distribution of target services (port)



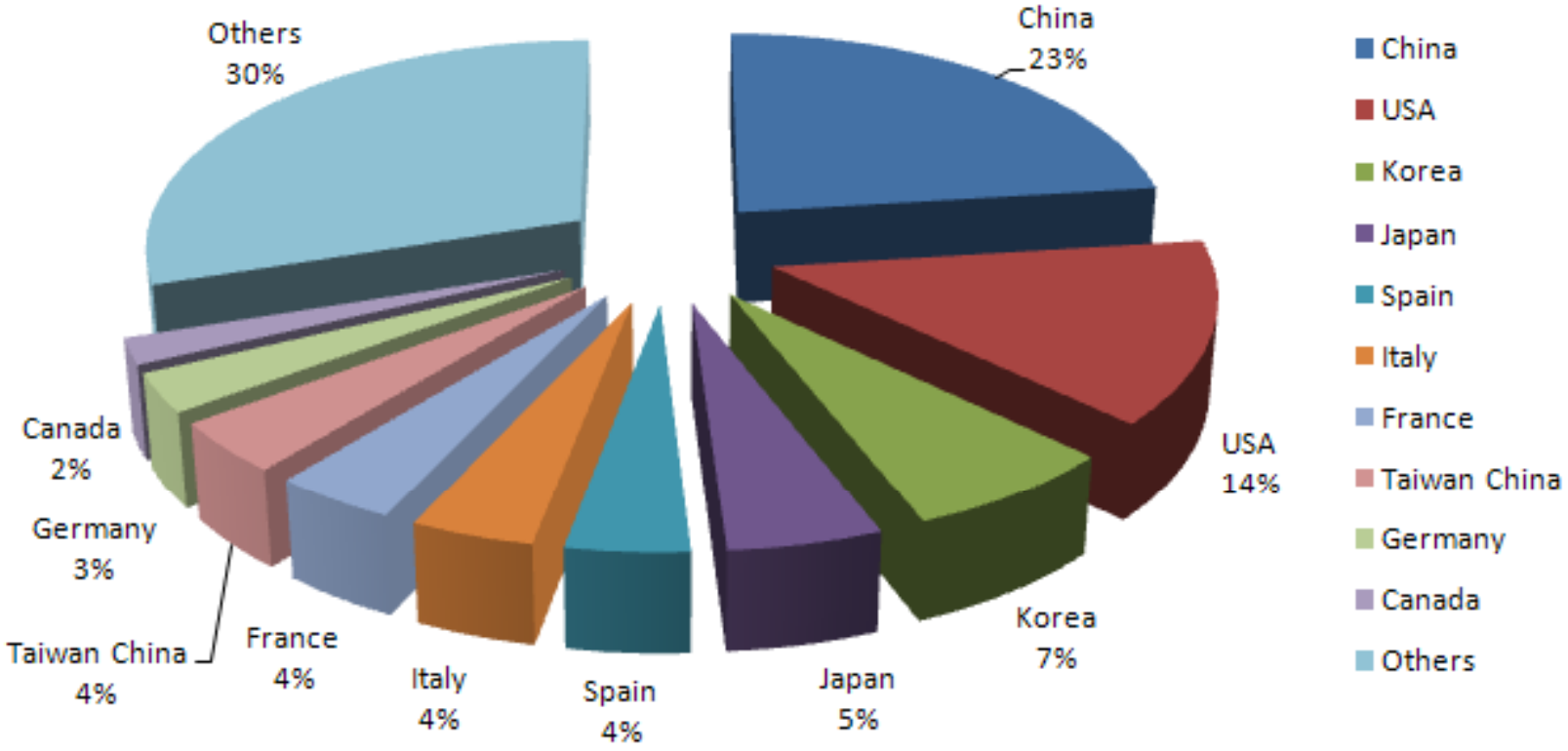
Port	Count
TCP 21	165448
TCP 22	106748
TCP 445	15574
TCP 135	8759
TCP 139	7454
TCP 5900	6824
Other	72211

CNCERT/CC

Origin of attack packets

攻击者IP	国家/地区	城市	最早攻击时间	最后攻击时间	被攻击的站点数量
24.87.27.184	CA	Saskatoon	2007-03-28 04:38:48	2007-04-11 14:19:53	13
24.82.14.3	CA	Surrey	2007-02-28 03:17:08	2007-04-11 15:50:05	12
222.73.255.58	CN	Beijing	2006-12-08 20:00:00	2007-04-11 15:40:37	12
219.132.138.237	CN		2006-11-13 17:10:29	2007-04-11 15:59:00	10
61.134.64.103	CN		2007-03-30 18:35:47	2007-04-11 14:37:18	9
204.16.209.120	US	Wasilla	2007-01-19 17:39:23	2007-04-11 15:44:12	8
61.153.139.254	CN	Jiaxing	2007-03-02 14:28:52	2007-04-11 12:06:45	9
204.16.209.160	US	Wasilla	2007-03-04 09:17:48	2007-04-11 12:22:50	7
220.178.32.78	CN	Beijing	2007-01-05 22:23:56	2007-04-11 11:36:44	8
222.222.72.244	CN	Beijing	2007-02-11 20:48:28	2007-04-11 12:33:22	7
66.232.146.143	KR		2007-04-03 17:32:38	2007-04-11 12:43:34	7
209.208.170.226	US	New York	2007-04-09 17:00:32	2007-04-11 15:27:08	7
192.83.249.73	US	Emeryville	2007-04-11 00:46:17	2007-04-11 05:53:49	6

Source of attacks to China

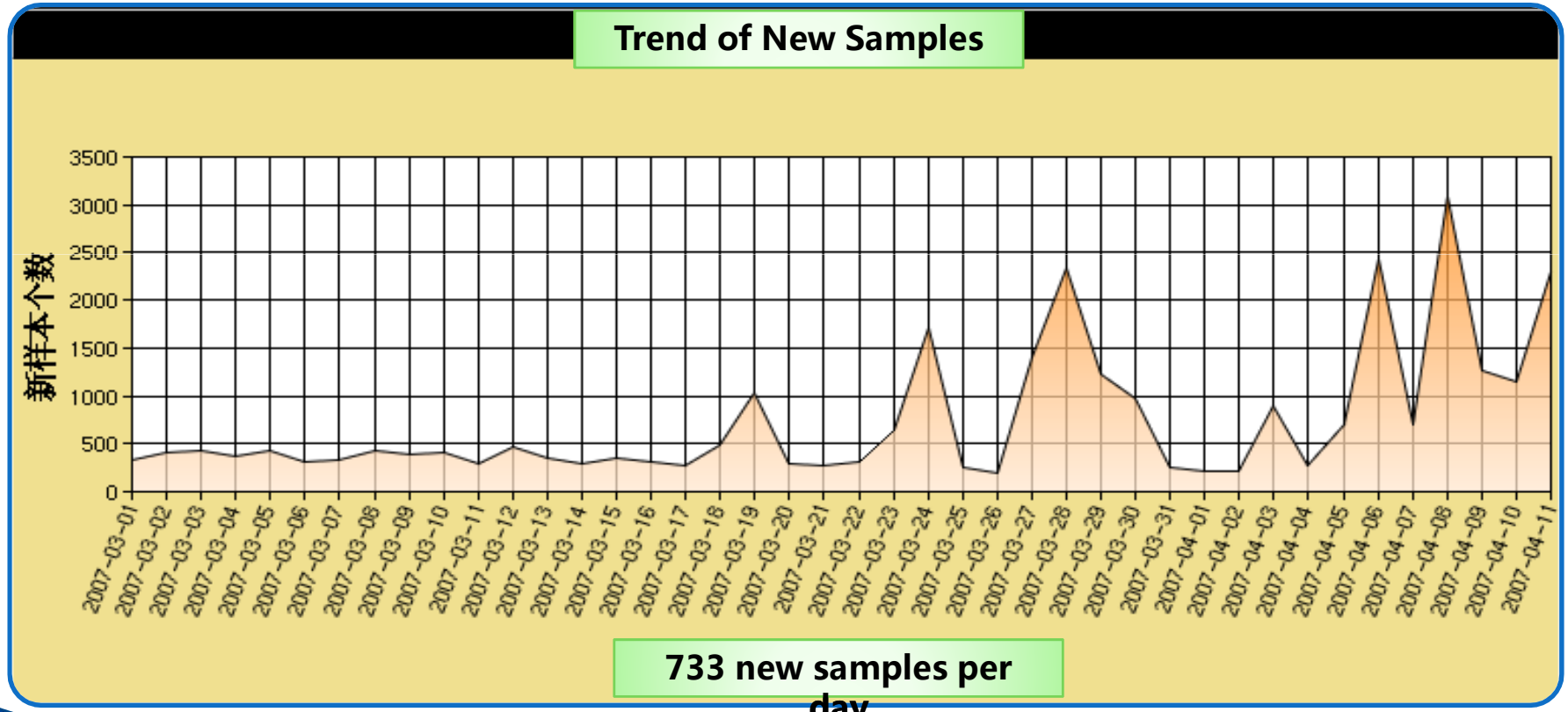


In 2007, attacks targeting Chinese mainland are mainly from inland (23%), USA (14%), Korea (7%), Japan (5%) and Spain (4%).

CNCERT/CC

Funtion II: Malware Capture

Trend of New Samples



CNCERT/CC

Scanning Result

No	ID	Hash	扫描软件	扫描时间	类型	平台	家族	名称
1	129621	1e25c9f9...	Kaspersky	2007-01-10 12:20	Virus	Win32	Virut	Virus.Win32.Virut.b
2	129620	8a3b6a2d...	Kaspersky	2007-01-10 12:10	Virus	Win32	Virut	Virus.Win32.Virut.a
3	129619	6f16155f...	Kaspersky	2007-01-10 12:00				CORRUPTED
4	129618	f0da5bfd...	Kaspersky	2007-01-10 11:20				Unknown
5	129617	8cb66390...	Kaspersky	2007-01-10 10:30				CORRUPTED
6	129616	da794604...	Kaspersky	2007-01-10 09:40				Unknown
7	129615	5671743e...	Kaspersky	2007-01-10 09:40				CORRUPTED
8	129614	c7b630e0...	Kaspersky	2007-01-10 09:00	Backdoor	Win32	Rbot	Backdoor.Win32.Rbot.rq
9	129613	105b0905...	Kaspersky	2007-01-10 08:10				CORRUPTED
10	129612	ecd141fd...	Kaspersky	2007-01-10 08:00	Net-Worm	Win32	Allaple	Net-Worm.Win32.Allaple.b
11	129611	76326eb3...	Kaspersky	2007-01-10 07:10				Unknown
12	129610	0c053769...	Kaspersky	2007-01-10 07:00	Virus	Win32	Virut	Virus.Win32.Virut.a
13	129609	f388d584...	Kaspersky	2007-01-10 05:30	Net-Worm	Win32	Allaple	Net-Worm.Win32.Allaple.d
14	129608	dccf55fa...	Kaspersky	2007-01-10 05:20				CORRUPTED

The AV-engines include main Chinese AV-vendors and some foreign vendors

CNCERT/CC

Malware collection in 2007

	hit count	Binaries	Variants	Families
Nepenthes (Distinct Total)	469,961	26,448	717	66
HoneyBow (Distinct Total)	774,313	153,097	4,662	241
Nepenthes (Average /day)	1,288	72	15	8
HoneyBow (Average /day)	2,121	419	37	16

CNCERT/CC

Fuction III: IRC-based Botnet Measurements

- **Discovery of IRC-based bots**

Bot Family	Number of Samples	Percentage
Rbot	1174	26.4 %
Virut	664	15.9 %
SdBot	335	7.5 %
Parite	187	4.2 %
Bobic	149	3.6 %
IRCBot	134	3.0 %
PoeBot	127	2.9 %

Fuction III: IRC-based Botnet Measurements

IRC bots in 2007

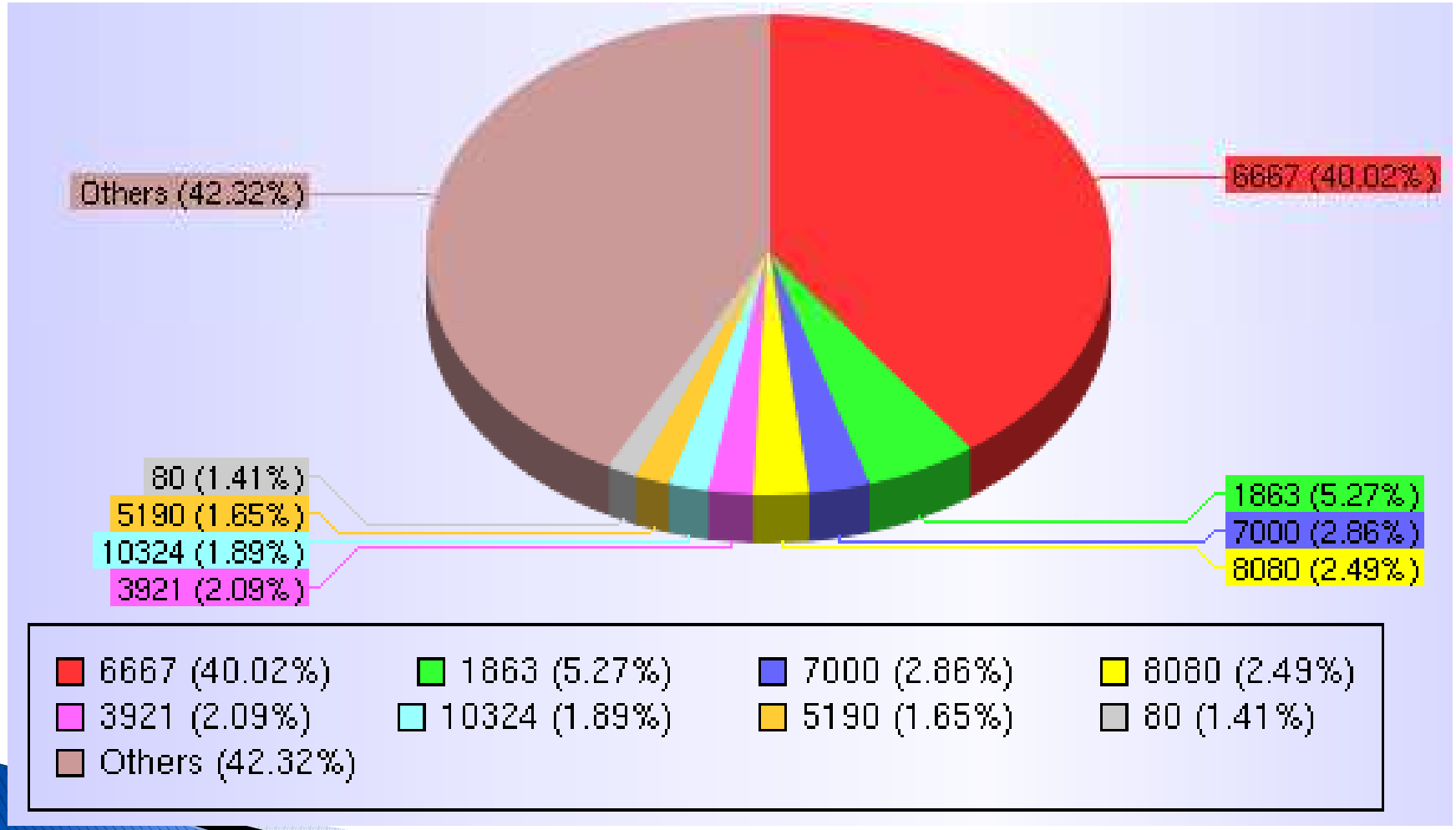
- In total, we could identify 6,720 IRC-based bots binaries, a rate of 3.74% of the overall malware binaries in 12 months.
- From those bots, we discovered 2,687 unique IRC botnets and track the activities.

Uniqueness is defined in this context as a unique combination of DNS name, port number and channel name.

IRC Bot family distribution in 2007

Bot Family	Number of Samples	Percentage
Rbot	2121	31.56%
Virut	1702	25.33%
Parite	258	3.84%
Agent	179	2.66%
SdBot	173	2.57%
IRCBot	166	2.47 %
Bobic	147	2.19%
others	904	13.45 %
Unidentified for AV	1070	15.92 %

Distribution of Control Port in 2007



CNCERT/CC

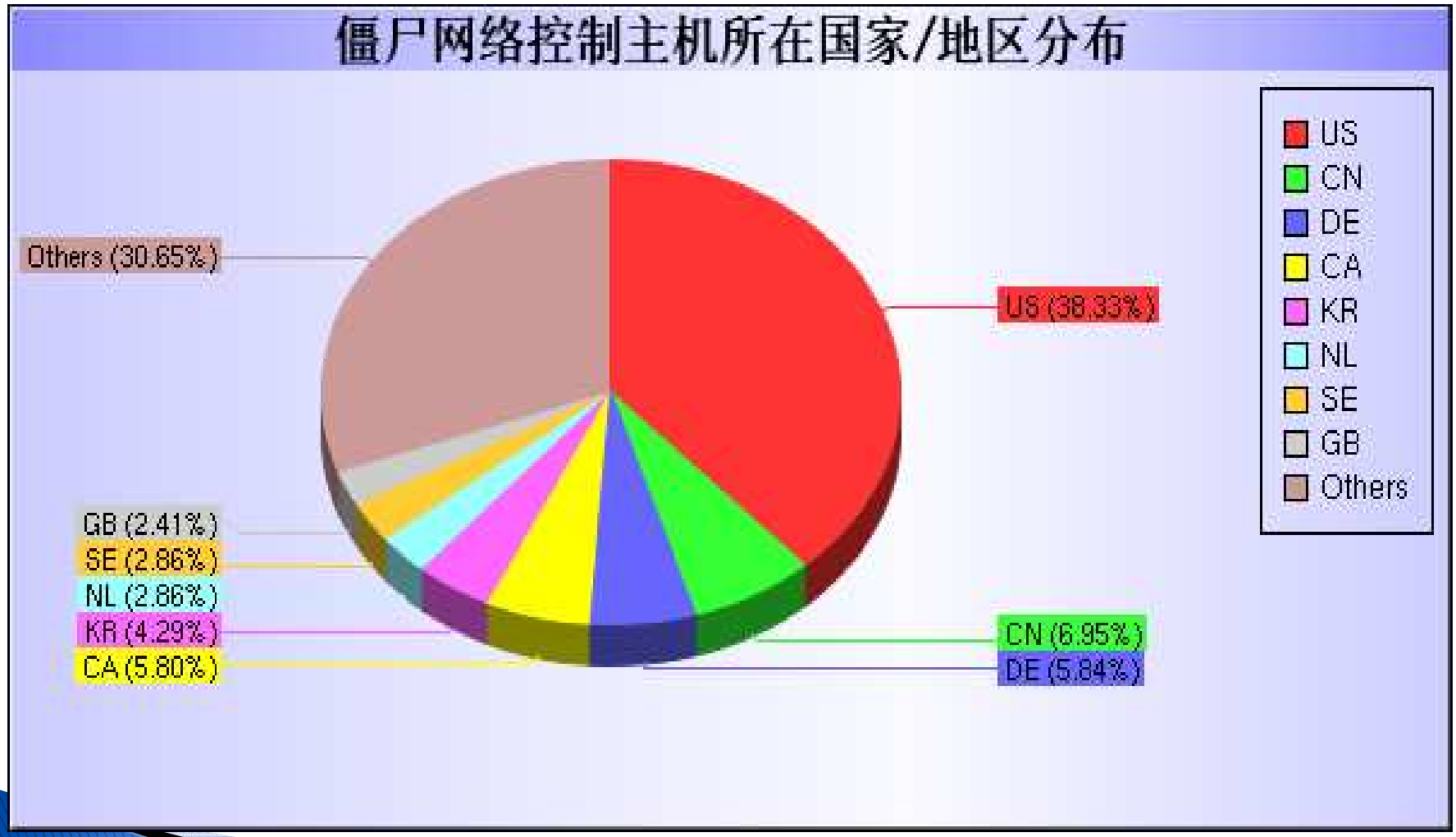
Botnet Command and Control Server Distribution

BotNet C&C Server Info

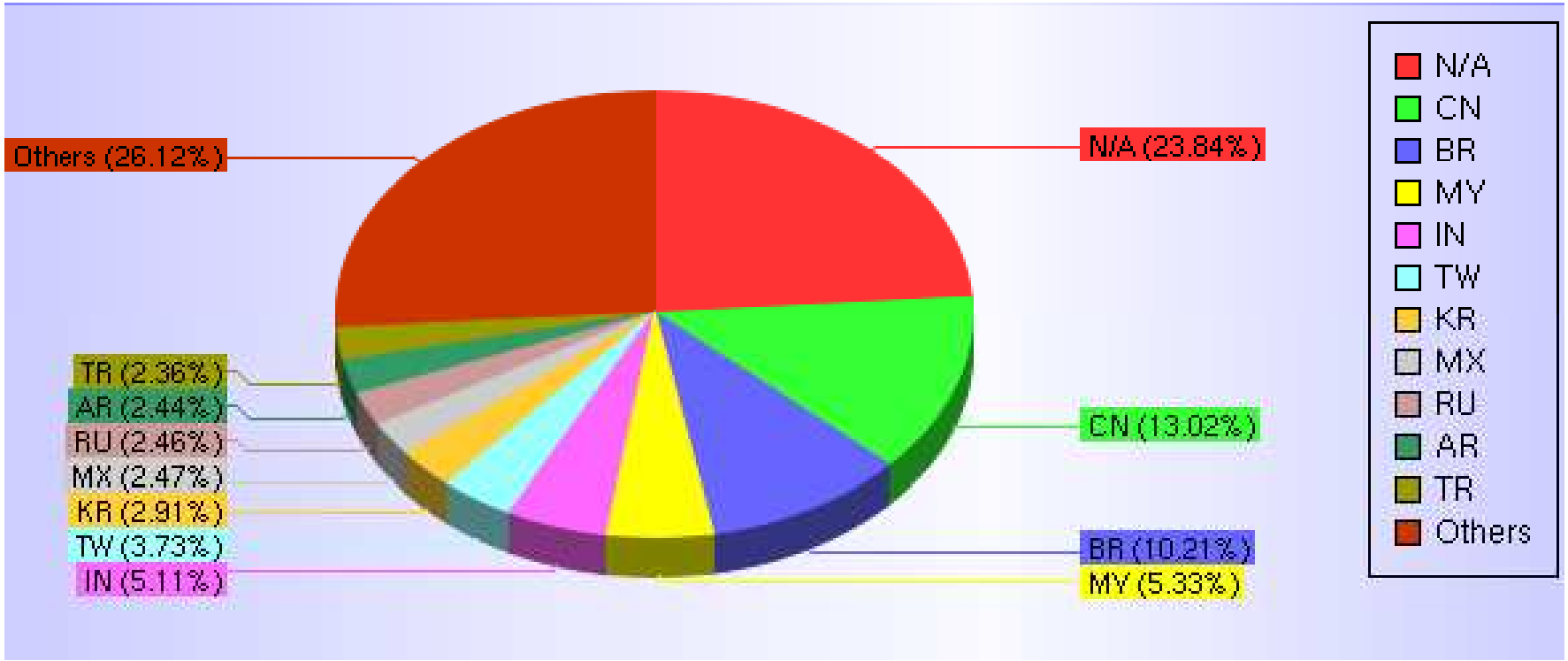
序号	C&C Server	Port	Channel	Country/Area	Malware	Timestamp
2745	ddos.undernix.com	3922	#danger#	DE	Rbot	2007-04-10 20:07
2744	symtec.easypwn.com	2007	#sql	CN		2007-04-10 19:34
2740	us.undernet.org	6667	#no-limits	US	unknown	2007-04-10 16:34
2739	85.8.130.201	6667	#asdf	GB	SdBot	2007-04-10 13:18
2738	atl.asian-heaven.net	6667	##ThisIsRuFF##	CN	unknown	2007-04-10 12:15
2737	n0j00m.dynu.net	6667	#hgat-5lg	CL		2007-04-10 10:06
2736	n0j00m.dynu.net	6667	#hgat-5lg	CL	Zapchast	2007-04-10 10:06
2735	net.onelan.org	9898	#hidden	--	Rbot	2007-04-10 09:42
2734	irc.kuonet.org	6667	##new	US	unknown	2007-04-10 08:05
2733	irc.kuonet.org	6667	#kuonet.	US	unknown	2007-04-10 08:05
2731	net.onelan.org	9898	#undertow	--	Rbot	2007-04-10 07:01
2730	221.130.182.184	8585	##cinto##	CN	Bobic	2007-04-10 06:44

CNCERT/CC

Distribution of CC servers in 2007



Distribution of bots in 2007



Activity Monitoring

Scan | Upgrade | Spam | Server Hosting | Login | Info theft

首页 | DDoS | 扫描扩散 | 下载/更新事件 | 发送垃圾邮件 | Clone | 架设服务器 | 黑客登陆 | 信息窃取

僵尸网络 DDos 事件列表

本列表为由僵尸网络监控程序监听到的僵尸网络DDoS事件列表。
本页面为测试页面，详细的搜索功能等正在完善中。

序号	C&C Server	Port	CH	CMD	Target	Location	Start TM	End TM
6449	ircd.darkroot.at	6667	##d0s##	.ddos.icmp	82.56.146.237	IT	2007-04-11 17:33:26	2007-04-11 17:33:26
6441	irleet.weedns.com	8641	#ac	.udpflood	82.73.123.238	NL	2007-04-11 17:17:55	2007-04-11 17:29:39
6446	save.staticcling.org	8641	#ac	.udpflood	82.73.123.238	NL	2007-04-11 17:17:55	2007-04-11 17:29:39
6440	irleet.weedns.com	8641	#ac	.udpflood	68.183.189.209	US	2007-04-11 17:16:52	2007-04-11 17:16:52
6445	save.staticcling.org	8641	#ac	.udpflood	68.183.189.209	US	2007-04-11 17:16:52	2007-04-11 17:16:52

CNCERT/CC

Botnet Activities in 2007

Command category	Number of events
Spreading	8,928
DDoS Attacks	10,988
Botnet Cloning	6,628
Download/update	6,155
Information theft	3,949
Spam	112

CNCERT/CC

Best Practice on Taking down Botnet and Malware Distributor

- Establish cooperation mechanism with local AV vendors and provide the samples and malicious URLs to ensure their product could be updated in time.
- Working with ISPs to stop some IPs used as CC server or malware distributor
  - If the IP locates in ISP’ s network, reach the users
  - If not, temporally block the IP or relevant domain names
- Working with local domain registrars to hold relevant domains which are registered by anonymous. *(According to Chinese regulations, anonymous register is not allowed.)*

CNCERT/CC

Future work

- Integrate pots of:
  - P2P file sharing
  - Spam collector
  - IM
- Track http-based botnet
- Extend to more ISP networks and CII systems

Conclusion

- Honeynet is an effective and efficient and easy deploy technical countermeasure on network attack and malware monitoring
- Malware and Botnet are still the top threats to network security, and getting more strong survivability by frequent updating and transition.
- By integrating low-interaction and high-interaction honeypot technology, we are able to collect nearly 180,000 unique malware binaries, discover and track 2687 IRC botnets in 2007.
- The final goal is to stop the threats at very beginning. So whether the data can be used effectively for incident handling team is the key issue.

CNCERT/CC

CNCERT/CC

Thank you!

CNCERT/CC

cncert@cert.org.cn

+86 10 8299 1000

Yonglin ZHOU

zyl@cert.org.cn

+86 10 8299 0355