Security Watch Report

HKCERT

July 21, 2015

Foreword

Better Security Decision with Situational Awareness

Nowadays, a lot of invisible compromised computers are controlled by attackers with the owner being unaware. The data on these computers may be mined and exposed every day, and the computers may be utilized in different kinds of abuse and criminal activities. The Hong Kong Security Watch Report aims to provide the public a better visibility of the situation of the compromised computers in Hong Kong so that they can make better decision in protecting their information security.

The data in this report is about the activities of compromised computers in Hong Kong which suffer from, or participate in various forms of cyber attacks, including web defacement, phishing, malware hosting, botnet command and control centres (C&C) or bots. Computers in Hong Kong are defined as those whose network geolocation is Hong Kong, or the top level domain of their host name is .hk or ..

Capitalizing on the Power of Global Intelligence

This report is the fruit of the collaboration of HKCERT and global security researchers. Many security researchers have the capability to detect attacks targeting their own or their customers networks. Some of them provide the information of IP addresses of attack source or web links of malicious activities to other information security organizations with an aim to collaboratively improve the overall security of the cyberspace. They have

Table 1: Types of Attack

Type of Attack	Metric used
Defacement, Phishing, Malware Hosting	security events on unique URLs within the reporting period
Botnet (C&Cs)	security events on unique IP addresses within the reporting period
Botnet (Bots)	maximum daily count of security events on unique IP addresses within the reporting period

good practice in sanitizing personal identifiable data before sharing information.

HKCERT collects and aggregates such valuable data about Hong Kong from multiple information sources for analysis with Information Feed Analysis System (IFAS), a system developed by HKCERT. The information sources (Appendix 1) are very distributed and reliable, providing a balanced reflection of the security status of Hong Kong. We remove duplicated events reported by multiple sources and use the following metrics for measurement to assure the quality of statistics.

Better information better service

We will continue to enhancing this report with more valuable information sources and more in-depth analysis. We will also explore how to use the data to enhance our services. *Please send us your feedback via email (**hkcert@hkcert.org**).*

Limitations

The data collected in this report is from multiple different sources with different collection method, collection period, presentation format and their own limitations. The numbers from the report should be used as a reference, and should neither be compared directly nor be regarded as a full picture of the reality.

Disclaimer

Data may be subject to update and correction without notice. We shall not have any liability, duty or obligation for or relating to the content and data contained herein, any errors, inaccuracies, omissions or delays in the content and data, or for any actions taken in reliance thereon. In no event shall we be liable for any special, incidental or consequential damages, arising out of the use of the content and data.

License

Contents

Highlight of Report

This report is for May 2015. In May 2015, IFAS[1] collected 144,431 security events related to Hong Kong from 19 data feed sources[2]. After data processing to remove duplications, there were 9,057 unique security events used for analysis in this report. The number of security events decreased significantly this month. However, the number of phishing events and malware hosting events remain high.

Server related security events

The distribution of server related security events is summarized below.

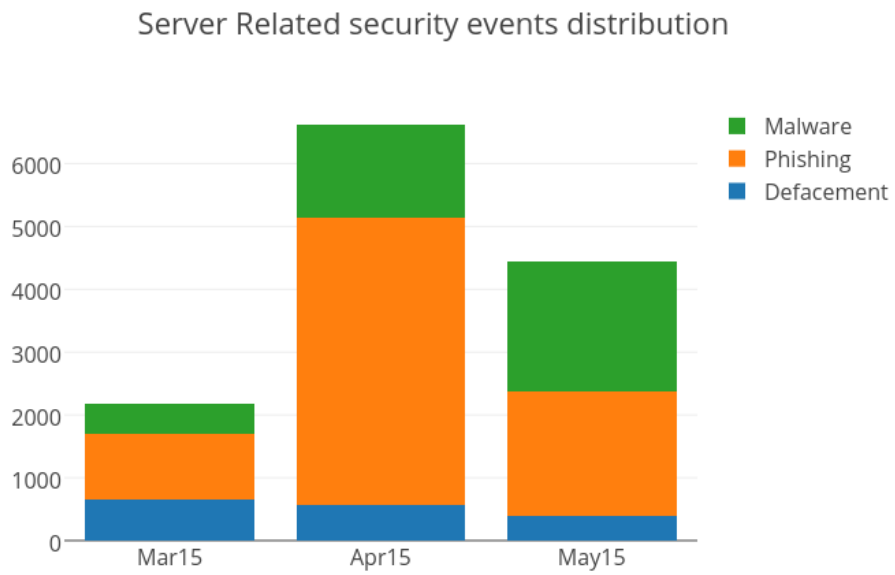

Figure 1: Distribution of Server related Security Events

[1] IFAS - Information Feed Analysis System is a HKCERT developed system that collects global security intelligence relating to Hong Kong to provide a picture of the security status.

[2] Refer to Appendix 1 for the feed sources

The server related security events decreased significantly by 33% or 2,174 events.

Defacement events and phishing events decreased by 31% and 56% respectively while malware hosting events increased by 40%. The 2062 malware hosting events were from single compromised sites, mass compromised sites and dedicated malware hosting sites.

The most serious single case was the compromise of http://conservancy.org.hk/, which was the website of a Hong Kong NGO. Its website was compromised to host 290 malware hosting URLs. The most serious mass compromise case was from the IP 210.245.166.72, under which, 43 legitimate websites was hosted. They were compromised to host 230 malware hosting URLs. IP address 14.136.137.103 was believed to be hosting a dedicated malware hosting site, under which, all URLs are IP Only.

Botnet related security events The distribution of botnet related security events are summarized below: Botnet Command and Control Servers There were two C&C servers reported in this month, both were IRC bot C&C server.

Botnet related security events

The distribution of botnet related security events are summarized below:

Total number of botnet(bots) security events showed a decrease of 7%. Conficker, Zeus and Virut were the top 3 of the chart.

This month, the positions of the top five botnets remain unchanged (Figure 14). The dropping trend of the top botnet, Conficker, was flattened. In the past three months, the number of Conficker events was roughly unchanged. The dropping trend of Zeus and ZeroAccess continued, they dropped for 8% and 4% respectively. On the other hand, the number of Virut event continued to rise. If the trend goes on, Virut will overtake Zeus as the second largest botnet next month.

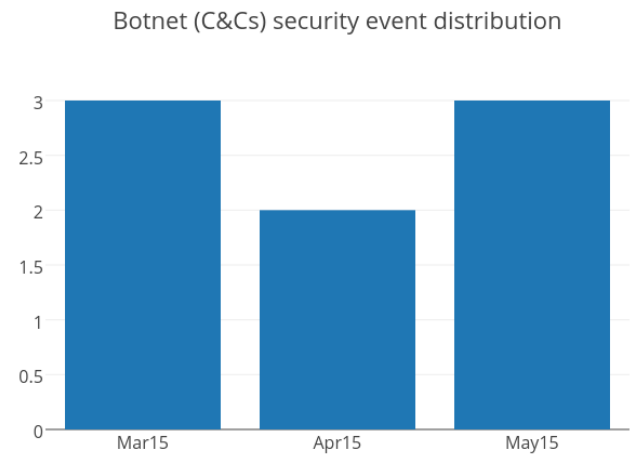

Figure 2: Distribution of Botnet (C&Cs) related security events

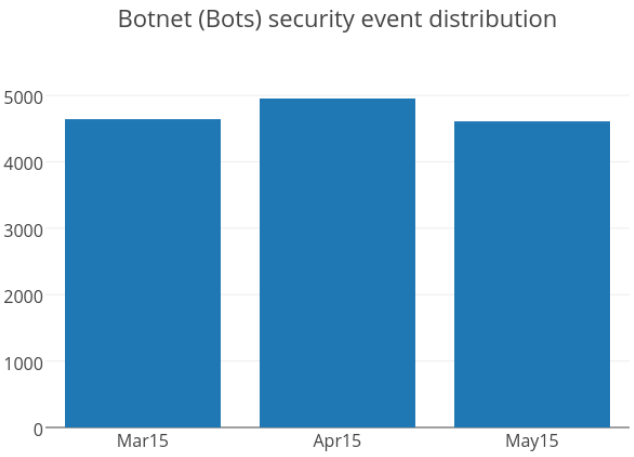

Figure 3: Distribution of Botnet (Bots) related security events

Top TLD and ISPs involved in security events

Among all Top Level Domains (TLDs), .com topped the TLD distribution of all security event types, which include defacement, phishing and mal-

ware hosting. .hk TLD related events contributions are: Defacement (7%); Phishing (3%); and malware hosting (1%)

AS number for New World Telephone Ltd was the top ISP in terms of total number of security events. For two consecutive months, an ISP other than PCCW Limited, which ranked 2 this month, topped the list.The number of events involving PCCW Limited kept decreasing, from over 1800 events at the beginning of 2015, to 1469 events this month.

AS number for New World Telephone Ltd was the top ISP for server related security events including malware hosting(754 events), phishing (497 events) and defacement (153 events). Sun Network (Hong Kong) Limited ranked the second ISP for server related security events of this monthwith defacement (13 events), phishing (364 events)and malware hosting (202 events) reported.

1 Defacement

1.1 Summary

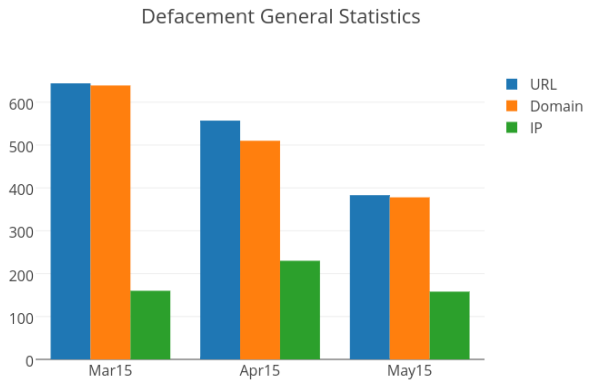

Figure 4: Defacement - General Statistics

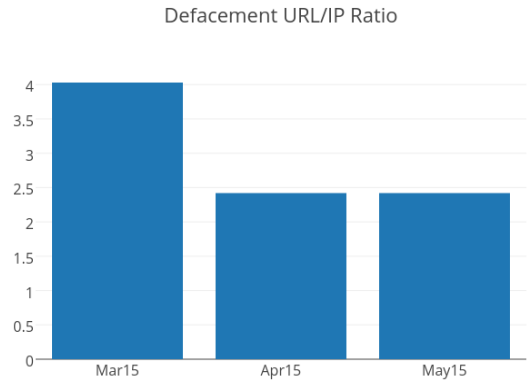

Figure 5: Defacement - URL/IP ratio

1.2 TLD Distribution

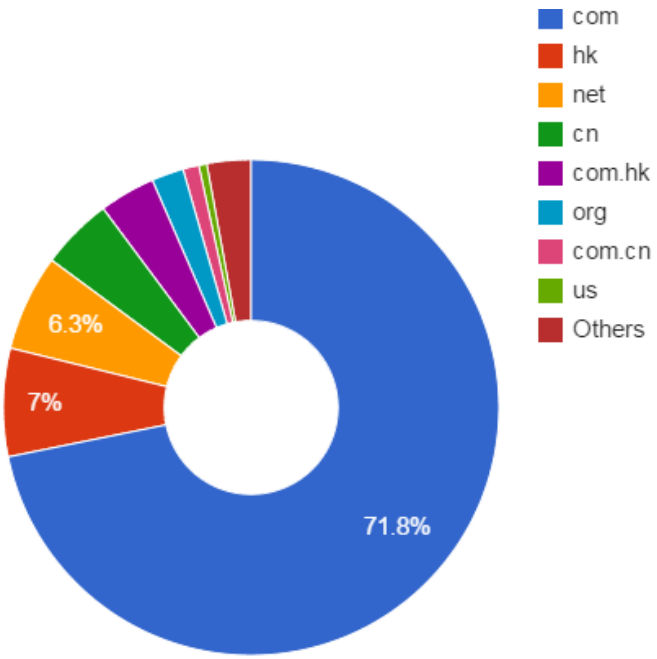

Figure 6: DefacementTld - TLD Distribution

Table 2: DefacementTld

Rank	Top Level Domain	count	%
1	com	388	51
2	com.hk	84	11
3	net	82	10
4	hk	58	7
5	cn	28	3
6	info	19	2
7	org	18	2
8	edu.hk	17	2
9	com.cn	16	2
10	hk.cn	8	1

2 Phishing

2.1 Summary

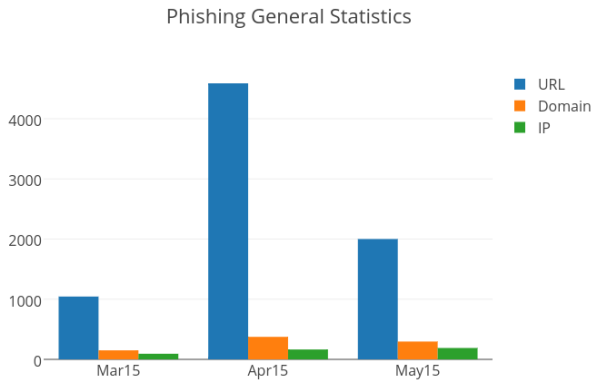

Figure 7: Phishing - General Statistics

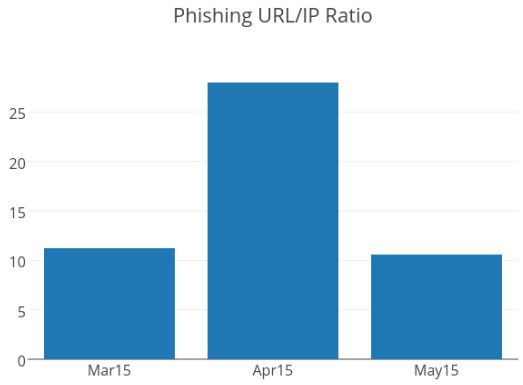

Figure 8: Phishing - URL/IP ratio

2.2 TLD Distribution

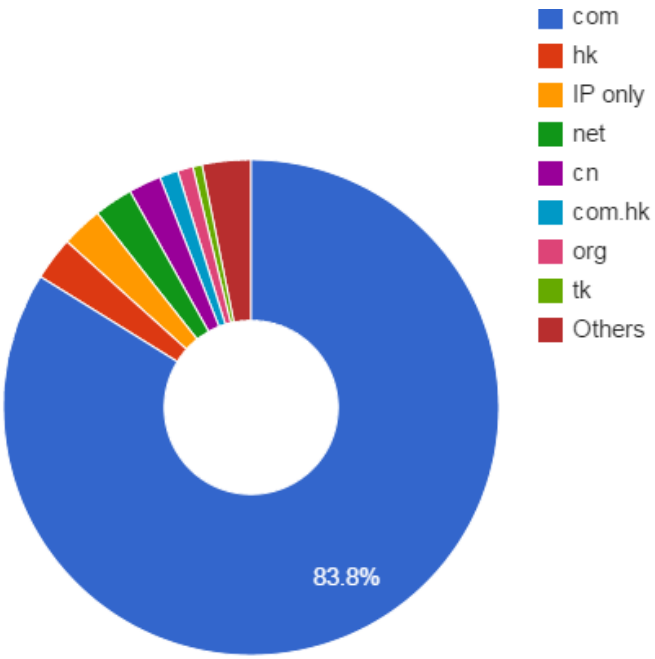

Figure 9: PhishingTld - TLD Distribution

Table 3: PhishingTld

Rank	Tld	Count	%
1	com	1263	79
2	science	126	7
3	net	33	2
4	info	31	1
5	ga	21	1
6	ml	18	1
7	hk	14	0
8	IP only	13	0
9	cn	10	0
10	cf	7	0

3 Malware

3.1 Summary

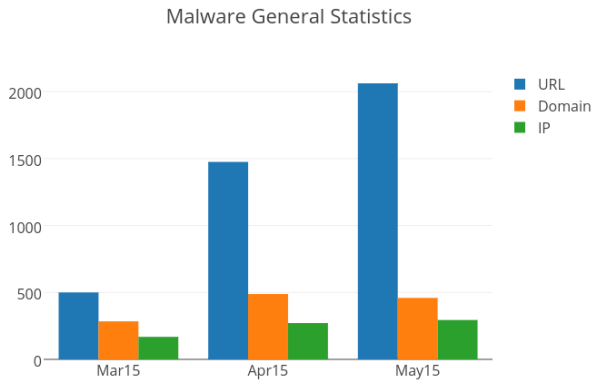

Figure 10: Malware - General Statistics

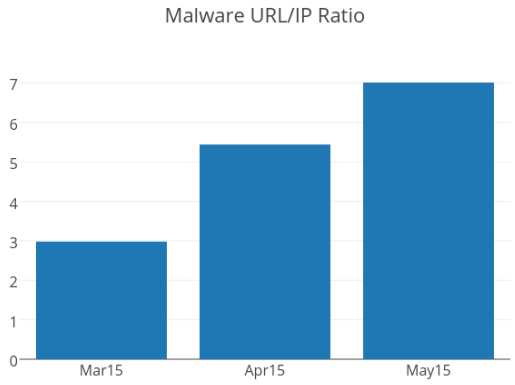

Figure 11: Malware - URL/IP ratio

3.2 TLD Distribution

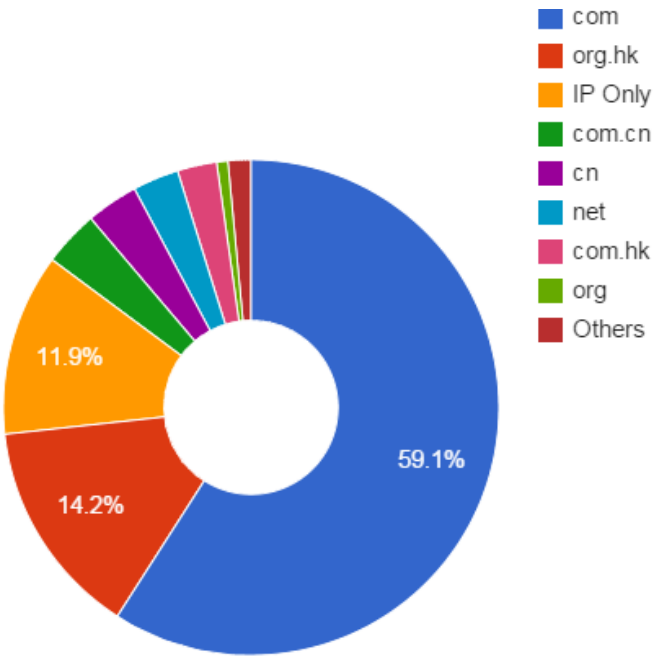

Figure 12: MalwareTld - TLD Distribution

Table 4: MalwareTld

Rank	Top Level Domain	count	%
1	com	2370	72
2	com.hk	197	6
3	cn	192	5
4	org	175	5
5	net	162	4
6	com.cn	54	1
7	hk	52	1
8	cc	16	0
9	-	12	0
10	top	10	0

4 Botnet

4.1 Botnet - Bots

4.1.1 Major Botnet Families found on Hong Kong Network

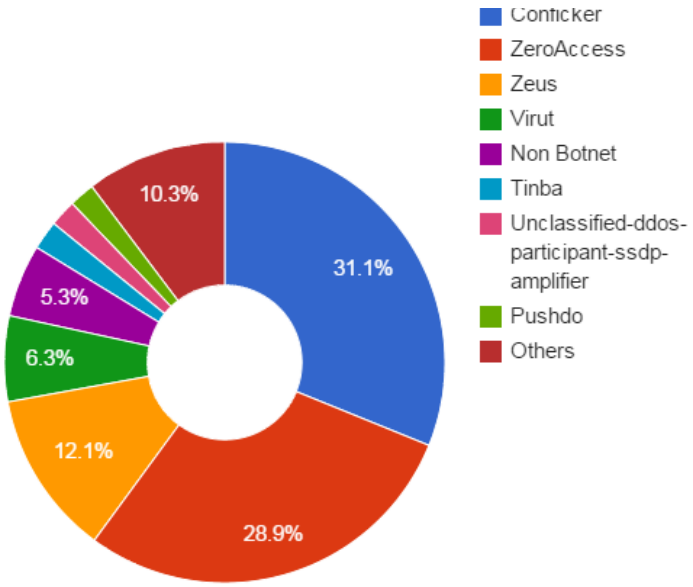

Figure 13: Botnet Unique IP (Monthly Max Count)

Table 5: listOfBotnets

Rank	Botnet Family	Count	%
1	Conficker	2018	42
2	Virut	1101	23
3	Zeus	648	13
4	ZeroAccess	499	10
5	Pushdo	81	1
6	Citadel	79	1
7	Tinba	56	1
8	Sality	49	1
9	Bankpatch	40	0
10	Dyre	40	0

4.2 Botnet - Command and Control Servers (C&Cs)

4.2.1 Botnet - C&C Servers by communication type

Figure 14: Botnet - C&C Servers by communication type

5 Internet Service Providers (ISP)

5.1 Top 10 ISPs hosting Defacement

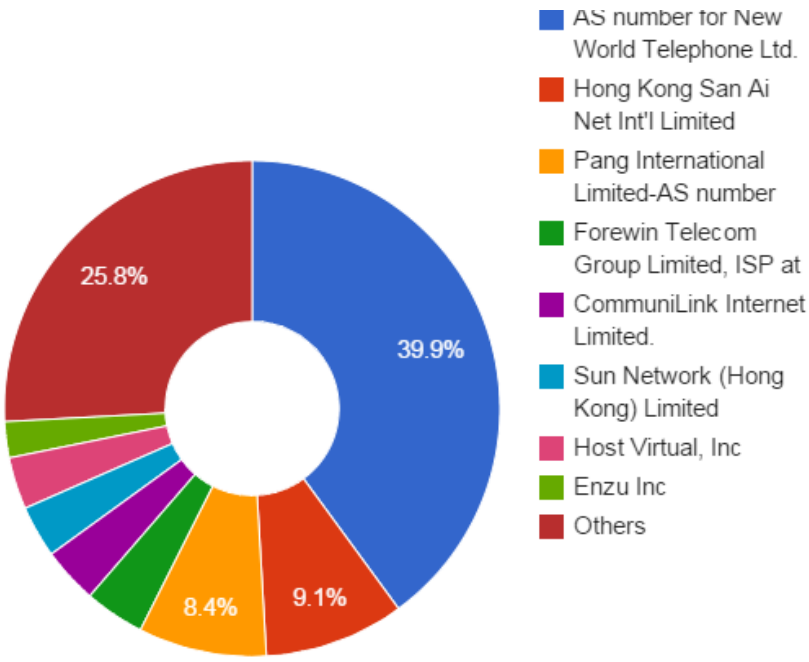

Figure 15: Defacement - Top ISPs

Table 6: ISPDefacement

Rank	ISP	count	%
1	HKNet Co. Ltd	286	38
2	AS number for New World Telephone Ltd.	213	28
3	Hutchison Global Communications	77	10
4	Pang International Limited-AS number	35	4
5	Sun Network (Hong Kong) Limited	21	2
6	NTT Com Asia Limited	10	1
7	CommuniLink Internet Limited.	10	1
8	Forewin Telecom Group Limited, ISP at	9	1
9	Rainbow network limited	8	1
10	NETWORK AND SECURITY SOLUTIONS LIMITED	8	1

5.2 Top 10 ISPs hosting Phishing

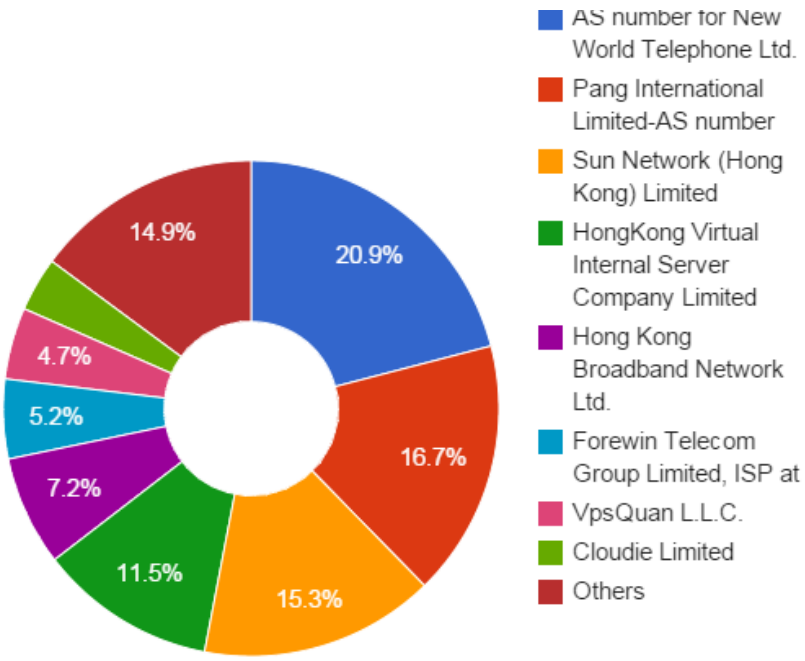

Figure 16: Phishing - Top ISPs

Table 7: ISPPhishing

Rank	ISP	count	%
1	AS number for New World Telephone Ltd.	853	52
2	Pang International Limited-AS number	242	14
3	Sun Network (Hong Kong) Limited	142	8
4	HongKong Virtual Internal Server Company L	131	8
5	Hutchison Global Communications	86	5
6	Henderson Data Centre Limited	34	2
7	Rainbow network limited	30	1
8	PCCW IMSBiz	21	1
9	Tele Asia Limited	12	0
10	SunnyVision Limited	8	0

5.3 Top 10 ISPs hosting Malware

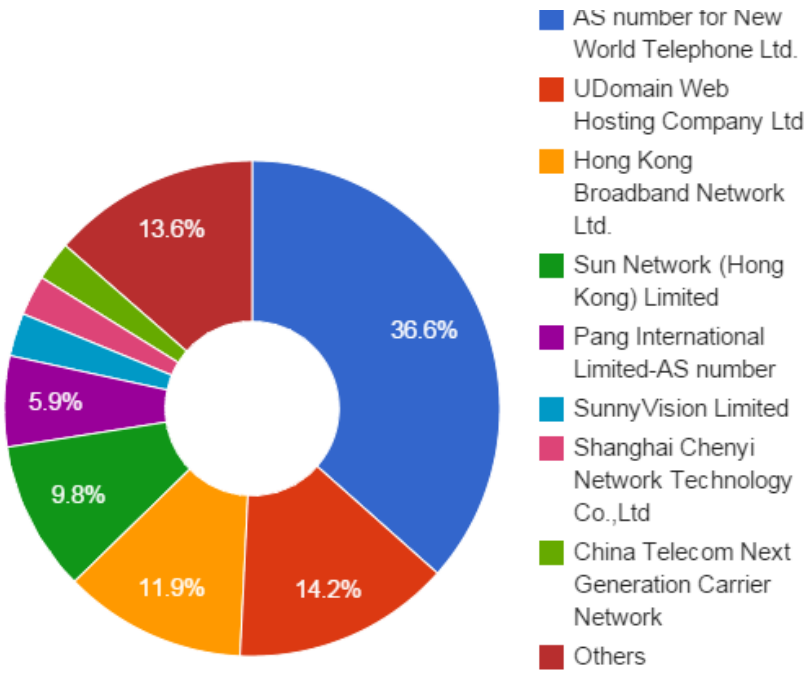

Figure 17: Malware Hosting - Top ISPs

Table 8: ISPMalware

Rank	ISP	count	%
1	AS number for New World Telephone Ltd.	1767	53
2	Pang International Limited-AS number	474	14
3	Sun Network (Hong Kong) Limited	184	5
4	Diyixian.com Limited	147	4
5	SunnyVision Limited	112	3
6	CLOUDHOST LIMITED	95	2
7	China Telecom Next Generation Carrier Netw	91	2
8	Rainbow network limited	87	2
9	Henderson Data Centre Limited	42	1
10	Shanghai Chenyi Network Technology Co.,Ltd	38	1

5.4 Top 10 ISPs of unique botnets (Bots)

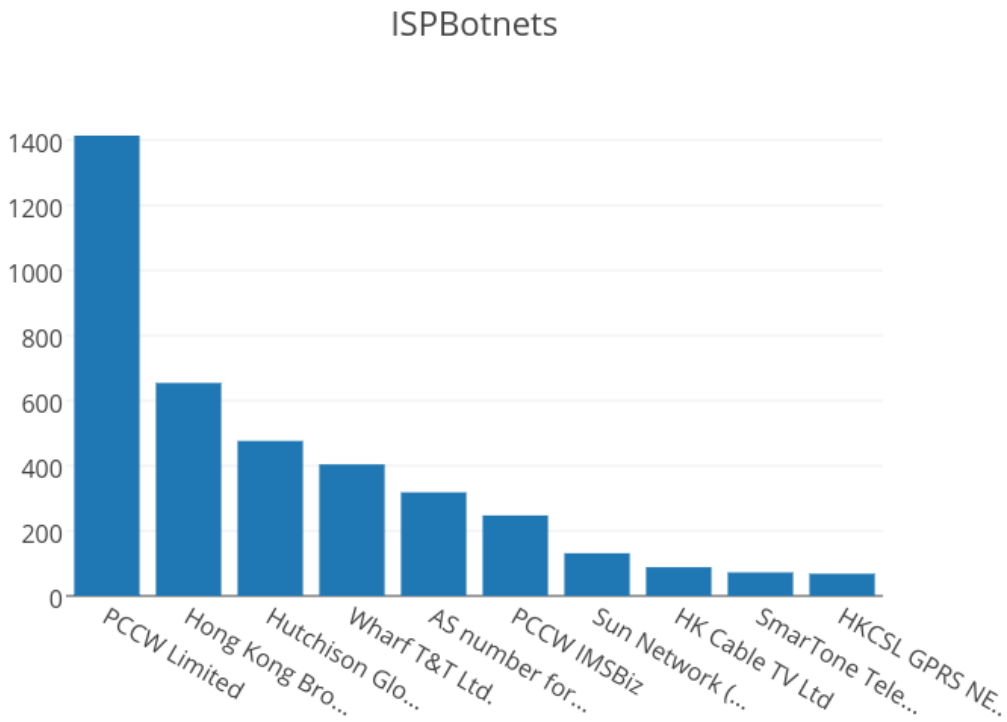

Figure 18: Botnet (Bots) - Top ISPs

Table 9: ISPBotnets

Rank	**ISP**	**count**	**%**
1	PCCW Limited	1414	28
2	Hong Kong Broadband Network Ltd.	654	13
3	Hutchison Global Communications	476	9
4	Wharf T&T Ltd.	404	8
5	AS number for New World Telephone Ltd.	318	6
6	PCCW IMSBiz	247	5
7	Sun Network (Hong Kong) Limited	131	2
8	HK Cable TV Ltd	88	1
9	SmarTone Telecommunications Ltd.	72	1
10	HKCSL GPRS NETWORK	68	1

5.5 Top 10 ISPs for all security events

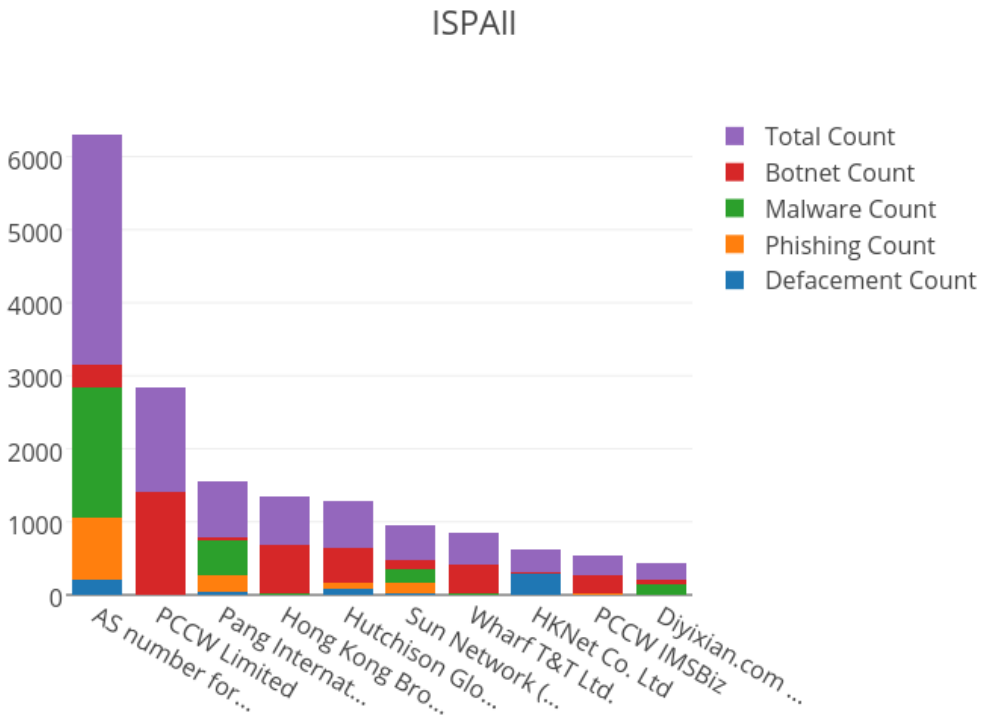

Figure 19: All Events - Top ISPs

Table 10: ISPAll

Rank	ISP	Def.	Phish.	Mal.	Bot.	Total	%
1	AS number for	213	853	1767	318	3151	29
2	PCCW Limited	0	0	4	1414	1418	13
3	Pang Internati	35	242	474	30	781	7
4	Hong Kong Broa	1	3	18	654	676	6
5	Hutchison Glob	77	86	3	476	642	6
6	Sun Network (H	21	142	184	131	478	4
7	Wharf T&T Ltd.	2	5	9	404	420	3
8	HKNet Co. Ltd	286	5	2	16	309	2
9	PCCW IMSBiz	5	21	1	247	274	2
10	Diyixian.com L	4	0	147	63	214	2

5.6 Top 10 ISPs for server related security events

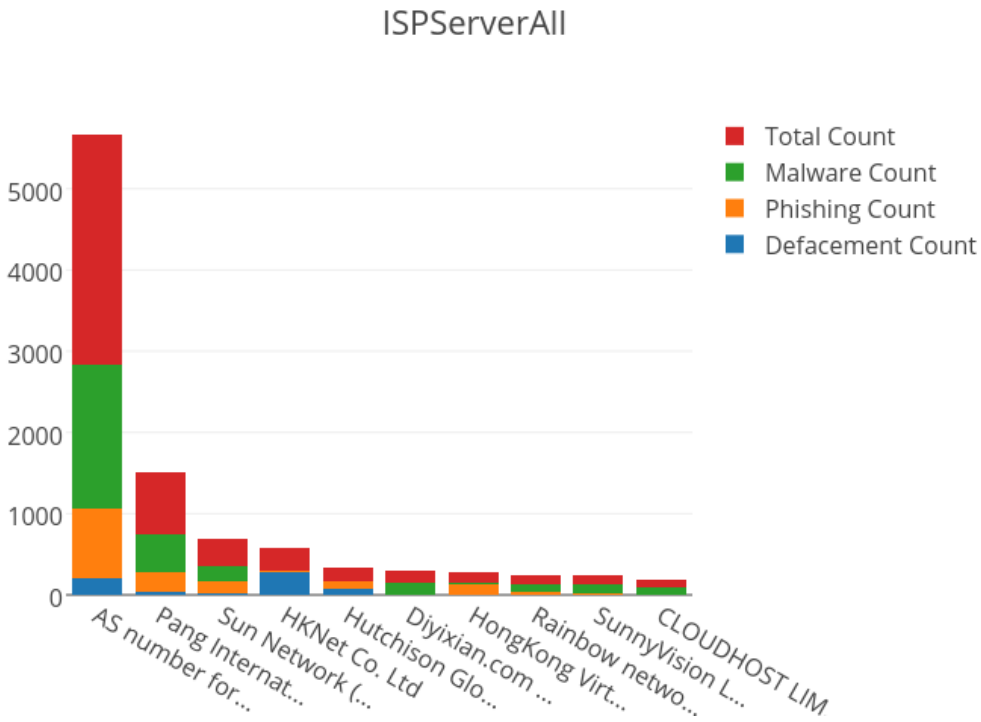

Figure 20: Server Related Events - Top ISPs

Table 11: ISPServerAll

Rank	ISP	Defacement	Phishing	Malware	Total	%
1	AS number for New Wor	213	853	1767	2833	50
2	Pang International Li	35	242	474	751	13
3	Sun Network (Hong Kon	21	142	184	347	6
4	HKNet Co. Ltd	286	5	2	293	5
5	Hutchison Global Comm	77	86	3	166	2
6	Diyixian.com Limited	4	0	147	151	2
7	HongKong Virtual Inte	1	131	8	140	2
8	Rainbow network limit	8	30	87	125	2
9	SunnyVision Limited	2	8	112	122	2
10	CLOUDHOST LIMITED	0	0	95	95	1

A Sources of information in IFAS

The following information feeds are information sources of IFAS:

Table 12: Methods of Geolocation Identification

Event Type	**Source**	**First introduced**
Defacement	Zone - H	2013-04
Phishing	ArborNetwork: Atlas SRF-Phishing	2013-04
Phishing	CleanMX - Phishing	2013-04
Phishing	Millersmiles	2013-04
Phishing	Phishtank	2013-04
Malware Hosting	Abuse.ch: Zeus Tracker - Binary URL	2013-04
Malware Hosting	Abuse.ch: SpyEye Tracker - Binary URL	2013-04
Malware Hosting	CleanMX - Malware	2013-04
Malware Hosting	Malc0de	2013-04
Malware Hosting	MalwareDomainList	2013-04
Malware Hosting	Savour.cn	2013-04
Botnet (C&Cs)	Abuse.ch: Zeus Tracker - C&Cs	2013-04
Botnet (C&Cs)	Abuse.ch: SpyEye Tracker - C&Cs	2013-04
Botnet (C&Cs)	Abuse.ch: Palevo Tracker - C&Cs	2013-04
Botnet (C&Cs)	Shadowserver - C&Cs	2013-09
Botnet (Bots)	Arbor Network: Atlas SRF-Conficker	2013-08
Botnet (Bots)	Shadowserver - botnet_drone	2013-08
Botnet (Bots)	Shadowserver - sinkhole_http_drone	2013-08
Botnet (Bots)	Shadowserver - microsoft_sinkhole	2013-08

B Geolocation identification methods in IFAS

We use the following methods to identify if a network's geolocation is in Hong Kong:

Table 13: IFAS Sources of Information

Method	**First introduced**	**Last update**
Maxmind	2013-04	2015-4-20

C Major Botnet Families

Table 14: Botnet Families

Botnet	**Alias**	**Nature**	**Infection Method**	**Attacks/Impacts**
BankPatch	• MultiBanker • Patcher • BankPatcher	Banking Trojan	• via adult websites • corrupt multimedia codecs • spam e-mail • chat and messaging systems	monitor specific banking websites and harvest user's passwords, credit card information and other sensitive financial data
BlackEnergy	Nil	DDos Trojan	• rootkit techniques to maintain persistence • uses process injection technique • strong encryption and modular architecture	launch DDos attacks
Citadel	Nil	Banking Trojan	• avoid and disable security tool detection	• steal banking credentials and sensitive information • keystroke logging • screenshot capture • video capture • man-in-the-browser attack
Conficker	• Downadup • Kido	Worm	• domain generation algorithm (DGA) capability • communnicate via P2P network • disable security software	• epxloit the Windows Server Service vulnerability (MS08-067) • brute force attacks for admin credential to spread across network • spread via removable drives using *"autorun"* feature