Hong Kong
Security Watch Report

Q1 2014

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 everyday, 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 “.香港”.

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 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.

Type of Attack	**Metric used**
Defacement, Phishing, Malware Hosting	Number of security events on unique URLs within the reporting period
Botnet command and control centres (C&C)	Number of security events on unique IP addresses within the reporting period

Bots	Sum of the number of individual bots as recorded with the reporting period. The number of individual bots is the maximum of the daily number of security events on unique IP addresses.

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

The content of this report is provided under Creative Commons Attribution 4.0 International License. You may share and adopt the content for any purpose, provided that you attribute the work to HKCERT.

http://creativecommons.org/licenses/by/4.0/

Table of Content

Highlight of Report

This report is for Quarter 1 of 2014.

In 2014 Q1, there were 15,235 unique security events related to Hong Kong used for analysis in this report. The information is collected with IFAS[1] from 19 sources of information.[2] They are not from the incident reports received by HKCERT.

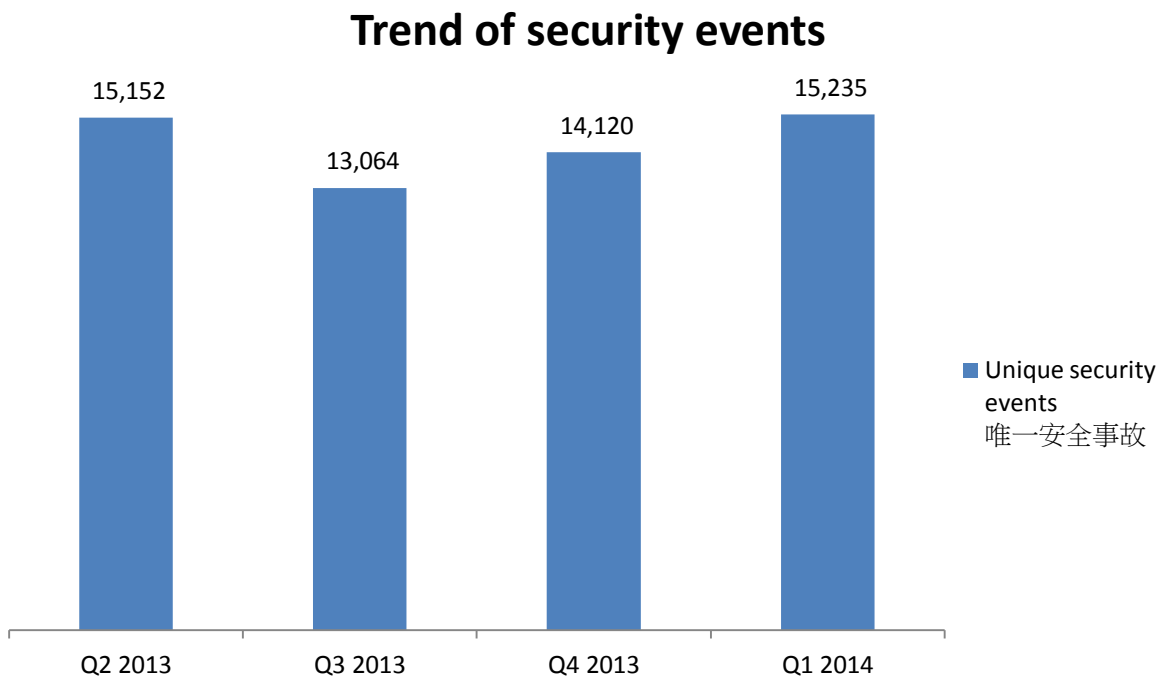


Figure 1-Trend of security events

The total number of security events has increased in Q1 2014 and the increases have been carrying on since Q3 2013.

[1] IFAS Information Feed Analysis System is a HKCERT developed system that collects global security intelligence relating to Hong Kong for analysis.

[2] Refer to Appendix 1 for the Sources of Information

Server related security events

Server related security events include malware hosting, phishing and defacement. Their trend and distribution is summarized below:

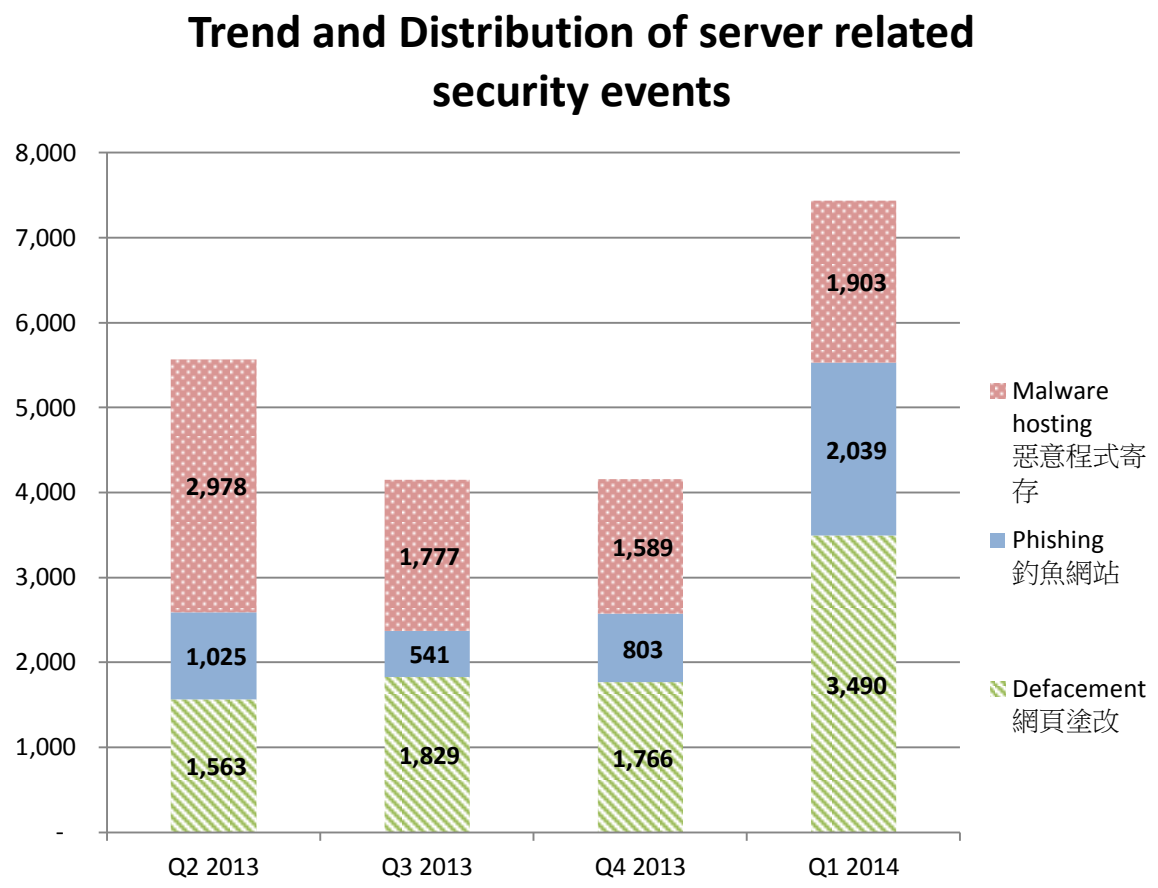


Figure 2 –Trend and distribution of server related security events

The number of server related security events significantly increased in Q1 2014.

In this quarter, the number of malware hosting security events had increase of 20% while the number of phishing and defacement increased significantly, by 154% and 97% respectively.

The number of malware hosting and defacement showed a sharp increase in March. The number of malware hosting was increased by 227% in March 2014. The number of phishing showed a sharp increase by 62% in January and kept the increasing trend through the whole quarter. (Figure 3)

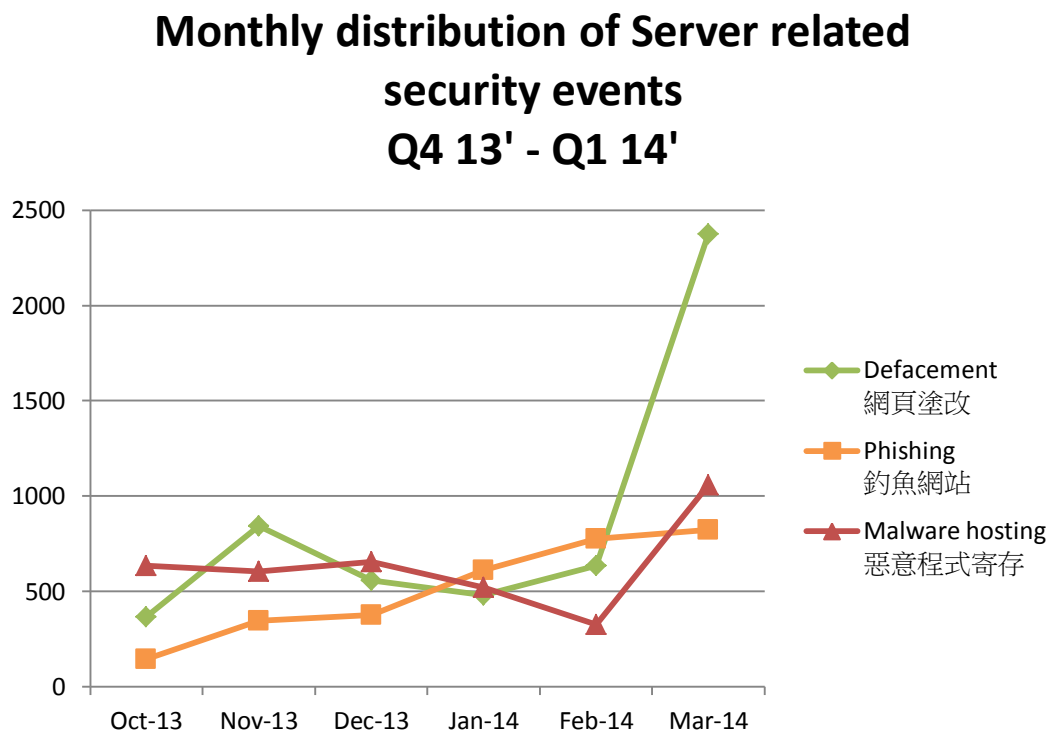


Figure 3 - Monthly Distribution of Server Related Security Events Q4 13' - Q1 14'

The growth in number of server related security events is alarming. The numbers implies there were lots of traps on the Internet serving malicious activities. In other words, users might be at risks when visiting the vulnerable websites.

Recent study[3] showed that some of the exploited servers were not compromised by attacks against their vulnerabilities or misconfigurations; but by theft of the administrators' credentials. Security researchers pointed out that "while anti-virus and two factor authentication is common on the desktop, it is rarely used to protect servers, making them vulnerable to credential stealing and easy malware deployment."

HKCERT urges system and application administrators to protect the servers.

- patch server up-to-date to avoid the known vulnerabilities being exploited.
- update web application and plugins to the latest version
- follow best practice on user account and password management
- implement validation check for user input and system output
- provide strong authentication, eg. two factor authentication, at administrative control interface

[3] OPERATION WINDIGO The vivisection of a large Linux server-side credential stealing malware campaign http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf

Botnet related security events

Botnet related security events can be classified into two categories:

- Botnet Command and Control Centres (C&C) security events – involving small number of powerful computers, mostly servers, which give commands to bots
- Bots security events – involving large number of computers, mostly home computers, which receive commands from C&C.

Botnet Command and Control Servers

The trend of botnet C&C security events is summarized below:

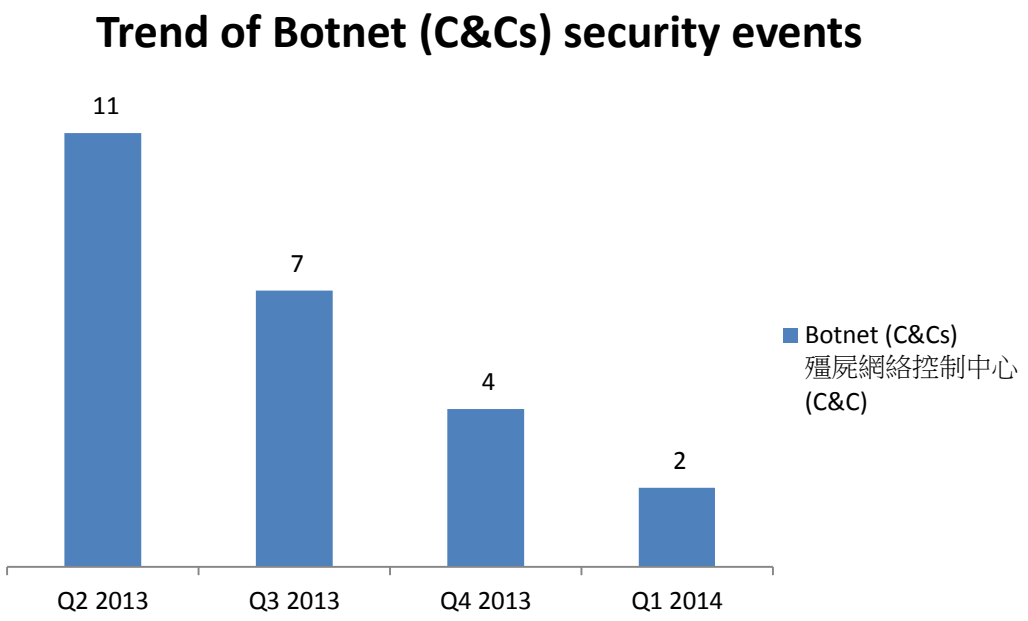


Figure 4 –Trend of Botnet (C&Cs) related security events

Number of botnet Command and Control Servers was decreasing across the four quarters.

There were 2 C&C servers reported in this quarter. One of the reported servers was identified as Zeus C&C servers, while the other was IRC bot C&C servers.

Botnet Bots

The trend of botnet (bots) security events is summarized below:

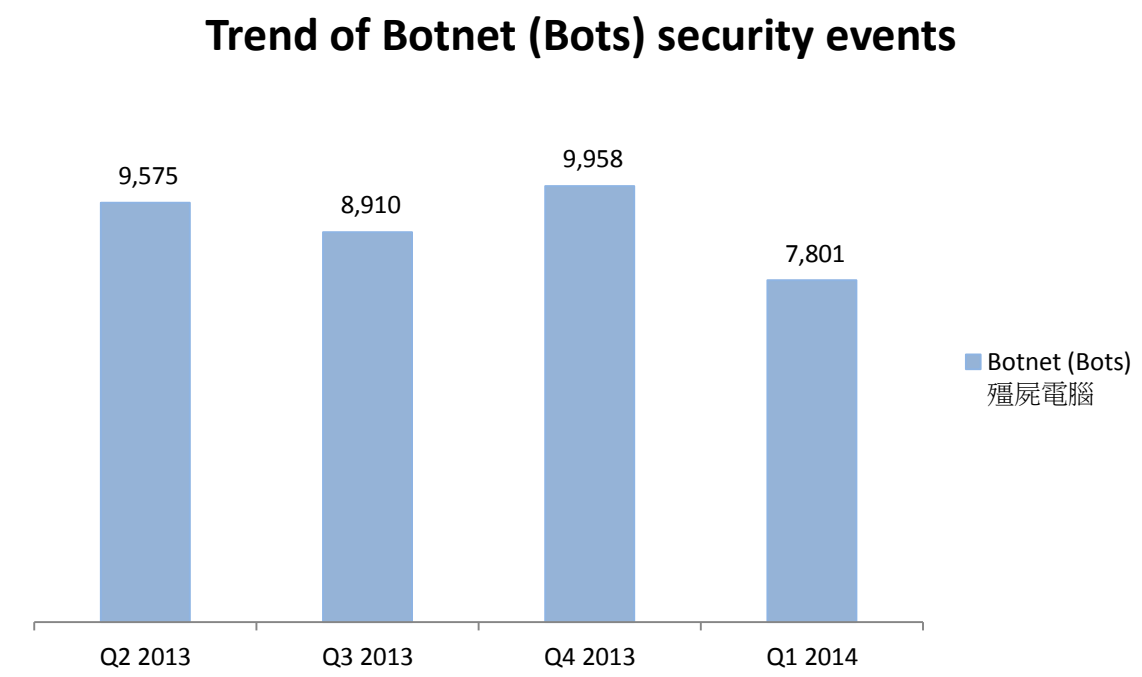


Figure 5 Trend of Botnet (Bots) security events[4]

Number of Botnet (bots) on Hong Kong network decreased in this quarter.

In Q1 2014, the number of botnet infection in Hong Kong decreased by 21.7%. Nine out of the top ten botnet showed a decrease in infection number. Among which, Pushdo showed the most significant decrease of 51.24%. (See section 4.2.1 for more details)

HKCERT has been following up the security events received and proactively engaged local ISPs for the botnet clean up since June 2013. Currently, botnet cleanup operations against major botnet family - Pushdo, Citadel and ZeroAccess are in action.

HKCERT urges users to protect computers so as not to become part of the botnets.

- patch their computers
- install a working copy of security software and scan for malware on their machines
- set strong passwords to avoid credential based attack
- do not use Windows, media files and software that have no proper licenses

[4] The number botnet(bots) security events in Q4 2013 was adjusted due to the update of numbers of the Zeus botnet

Among all the botnet family, Zeus has brought to our attention since Q4 2013. Zeus botnet security events in Oct 2013 had started to grow, and continued to soar through Q1 2014 despite a marginal drop in February 2014 (Figure 6). It implied that Zeus botnet had been active or more users were infected with Zeus.

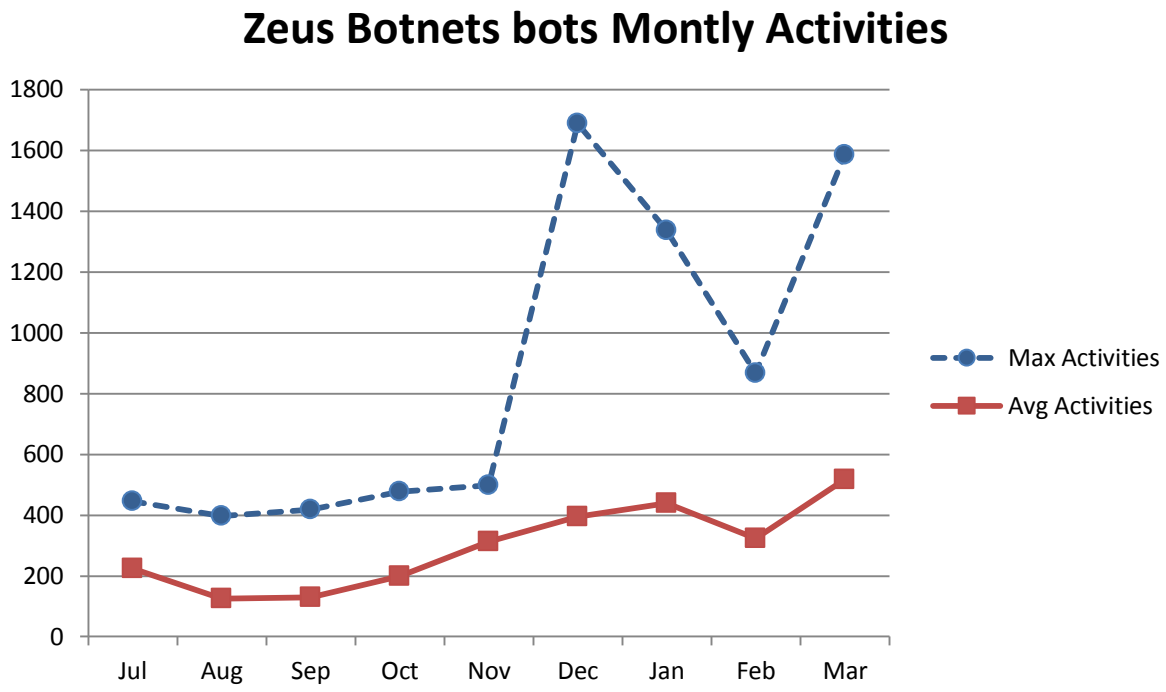


Figure 6 - Zeus Botnets Bots Monthly Activities

One of the reasons may be Zeus was being use to download the recent infamous ransomeware – Cryptolocker[5]. Security researchers observed a connection between Zeus botnet and Cryptolocker. The Cutwail-UPATRE-ZEUS-CRILOCK infection chain was believed to be the most common ways to spread Cryptolocker[6]. Also, with the arrest of the author of BlackHole Exploit Kit, "Paunch", in October 2013, researchers observed the kit was replaced by the Cutwail-UPATRE-ZEUS-CRILOCK infection chain. It also leads to an increase of Zeus botnet.

Besides acting as downloader of other malware, Zeus is a famous financial trojan. It was designed to steal confidential information, e.g. target system information, online credential,

[5] CryptoLocker – A ransomeware that encrypt files on the local and mapped drivers of the compromised machine randomly and will ask for ransome money.

[6] According to TrendMirco Blog, CryptoLocker: Its Spam and ZeuS/ZBOT Connection published on Oct 21 2013, The infection chain initiated with spam mail with malicious attachment (UPATRE). Once the attachment file being executed, it will download the Zeus malware to the compromised machines. Zeus, then, downloads other malware, in this case, Cryptolocker to the infected machine.
http://blog.trendmicro.com/trendlabs-security-intelligence/cryptolocker-its-spam-and-zeuszb, ot-connection/

bank details. Recently, news reported that the attacks by Zeus botnet are not only against financial institutions, but also against websites and services with ample of personal information. For example, the attack detected against Salesforce.com[7], a widely adopted CRM platform, in Feb 2014, and attacks against famous recruitment websites, Monster.com and Careerbuilder.com[8] in March 2014.

HKCERT urges general users to join the cleanup acts. Ensure your computers are not being infected and controlled by malicious software.

Protect yourself and keep the cyberspace clean.

Users can use the HKCERT guideline to detect and clean up botnets

- Botnet Detection and Cleanup Guideline
  https://www.hkcert.org/botnet

[7] News reports on the attack against Salesforce.com
http://thehackernews.com/2014/02/Salesforce-malware-attack-zeus-trojan.html

[8] News reports on the attack against Monstor.com and CareerBuilder.com
http://www.computerworld.com/s/article/9247206/Gameover_malware_takes_aim_at_Monster.com_and_CareerBuilder.com

Report Details

1. Defacement

1.1 Summary

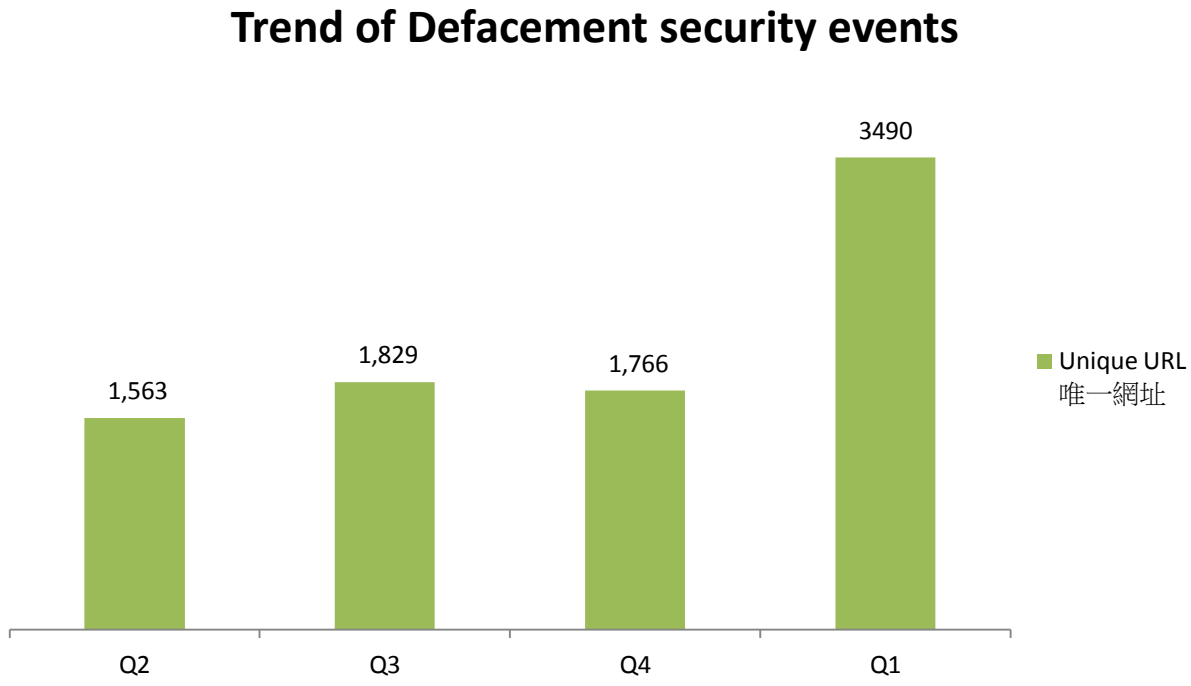


Figure **7** –Trend of Defacement security events

What is defacement?

- Defacement is the unauthorized alteration of the content of a legitimate website using hacking method.

What are the potential impacts?

- The integrity of the website content is damaged.
- Original content might be inaccessible
- Reputation of the website owner might be damaged
- Other information stored / processed on the server might be further compromised by the hacker to perform other attacks.

Sources of Information:

- Zone - H

2. Phishing

2.1 Summary

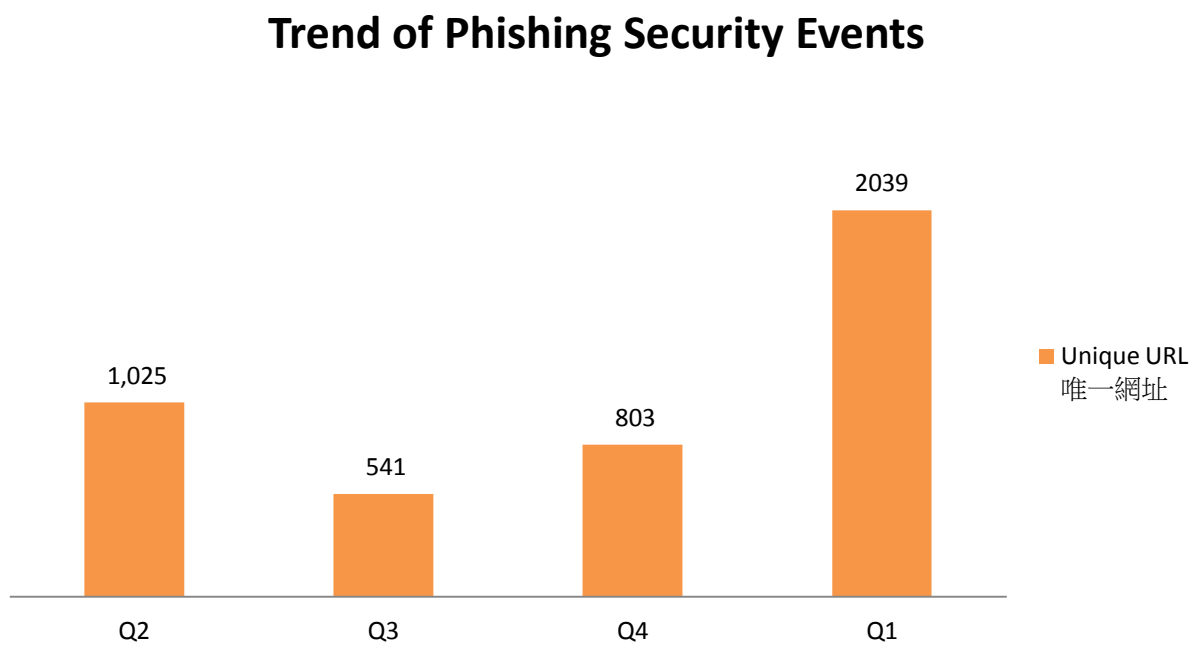


Figure 8 –Trend of Phishing Security Events

What is Phishing?

- Phishing is the spoofing of a legitimate website for fraudulent purpose

What is the potential impact?

- Personal information or account credentials of visitors might be stolen, leading to financial loss.
- Original content might be inaccessible
- Reputation of the website owner might be damaged
- Server might be further compromised to perform other attacks.

Sources of Information:

- ArborNetwork – Atlas SRF
- CleanMX – phishing
- Millersmiles

- Phishtank

3. Malware Hosting

3.1 Summary

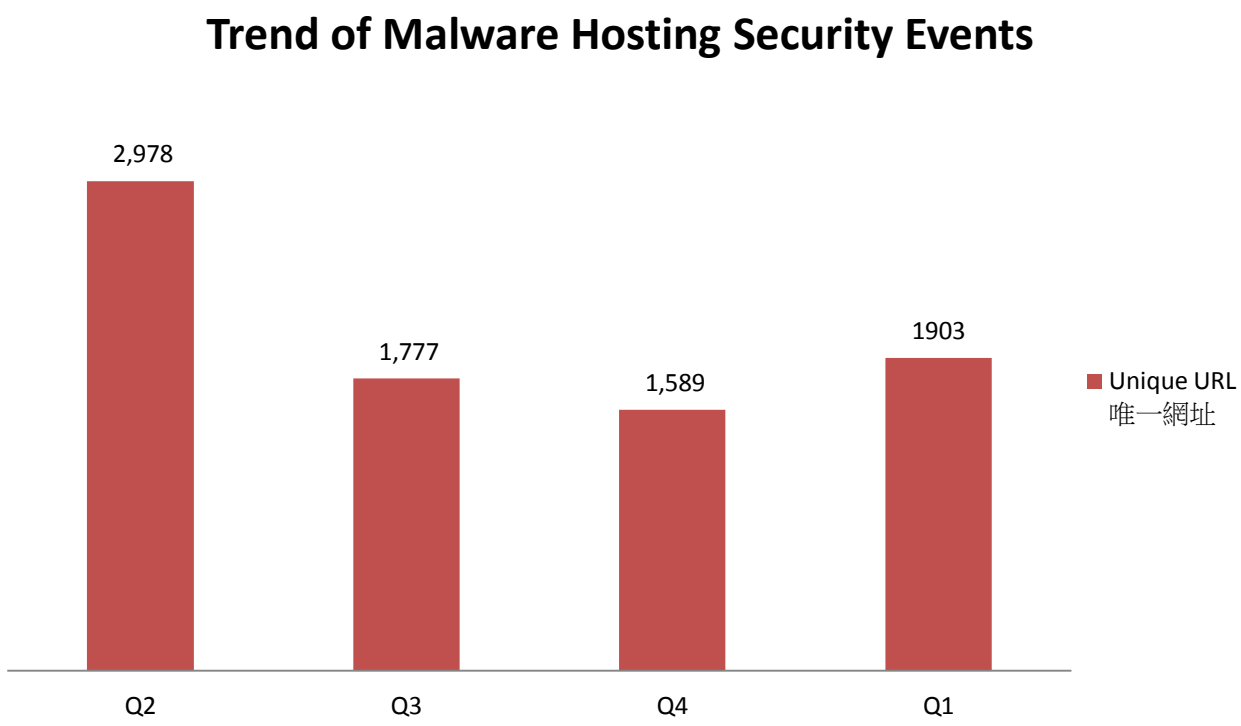


Figure 9 –Trend of Malware Hosting Security Events

What is Malware Hosting?

- Malware Hosting is the dispatching of malware on a website

What is the potential impact?

- Visitors might download and install the malware, or execute the malicious script to get compromised.
- Original content might be inaccessible
- Reputation of the website owner might be damaged
- Server might be further compromised to perform other criminal activities.

Sources of Information:

- Abuse.ch: Zeus Tracker – Binary URL
- Abuse.ch: SpyEye Tracker – Binary URL
- CleanMX – Malware
- Malc0de
- MalwareDomainList
- Sacour.cn

4. Botnet

4.1 Botnets – Command & Control Servers

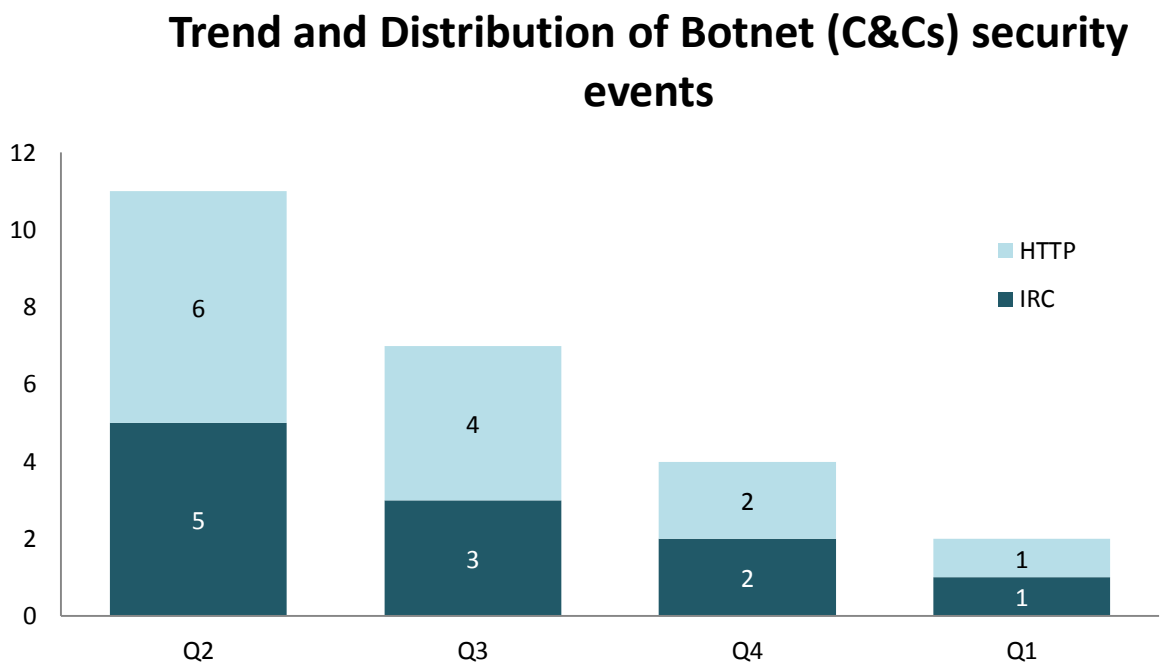


Figure 10 –Trend and Distribution of Botnet (C&Cs) security events

What is a Botnet Command & Control Centre?

- A Botnet Command & Control Centre is a server used by cybercriminals to control the bots, which are compromised computers, by sending them commands to perform malicious activities, e.g. stealing personal and financial information or launching DDoS attacks.

What is the potential impact?

- Server might be heavily loaded when many bots connecting to it.
- Server might contain large amount of personal and financial data stolen by other bots.

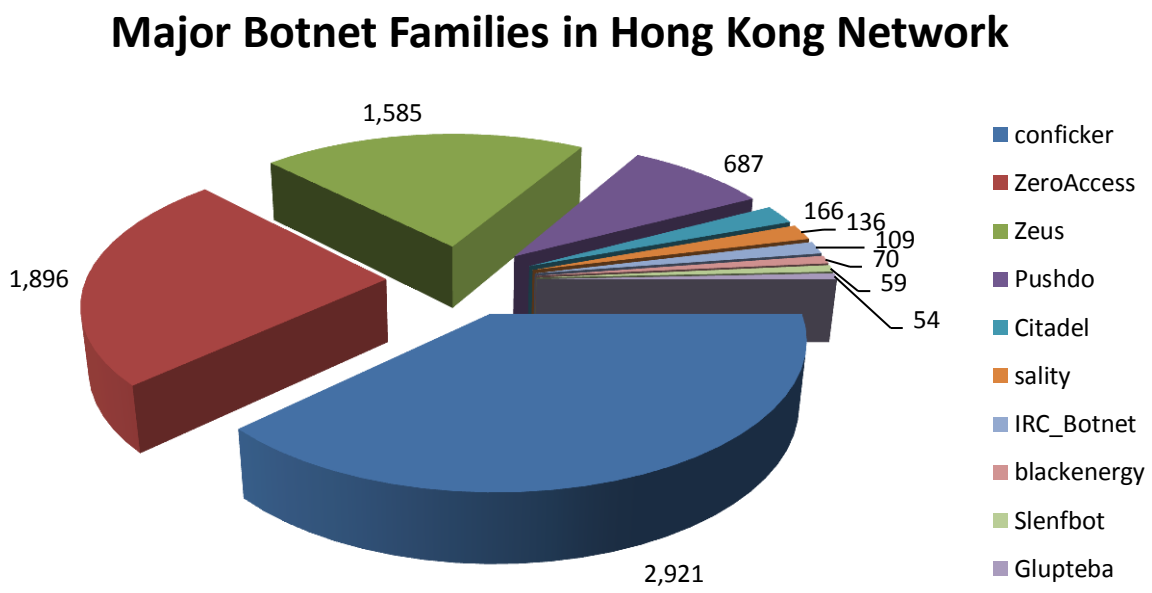
Sources of Information:

- Zeus Tracker
- SpyEye Tracker
- Palevo Tracker
- Shadowserver – C&Cs

4.2 Botnets – Bots

4.2.1 Major Botnet Families[9] found on Hong Kong Networks

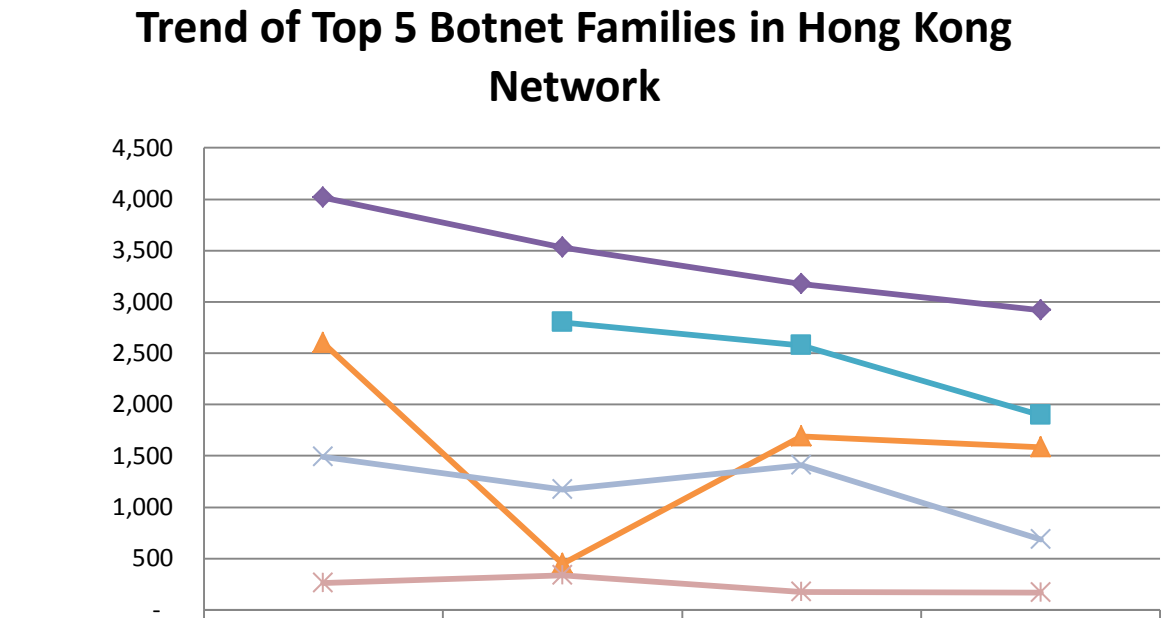
Individual botnet's size is calculated from the maximum of the daily counts of unique IP addresses attempting to connect to the botnet in the report period. In other words, the real botnet size should be larger because not all bots are powered on within the same day.



Rank	↑↓	Concerned Bots	Number of Unique IP addresses (Max count in a Quarter)	Changes with previous period
1	-	conficker	2,921	-8%
2	-	ZeroAccess	1,896	-32%
3	-	Zeus	1,585	-6%
4	-	Pushdo	687	-51%
5	↑	Citadel	166	-6%
6	↑	sality	136	-8%
7	↑	IRC_Botnet	109	-8%
8	-	blackenergy	70	-42%
9	↑	Slenfbot	59	-50%
10	NEW	Glupteba	54	NA

Figure 11 –Major Botnet Families in Hong Kong Networks

[9] Major Botnet Families are selected botnet families with considerable amount of security events reported from the information sources constantly across the reporting period.



	Q2	Q3	Q4	Q1
conficker	4,014	3,527	3,175	2921
ZeroAccess		2,802	2,576	1896
Zeus	2,602	446	1,687	1585
Pushdo	1,492	1,175	1,409	687
Citadel	261	334	176	166

Figure 12 – Trend of Top 3 Botnet Families in Hong Kong Network

Note:

Information provided from sources for ZeroAccess became stable since Q3 2013; hence, it cannot be compare with that of Q2 2013

What is a Botnet - Bot?

- A bot is usually a personal computer that is infected by malicious software to become part of a botnet. Once infected, the malicious software usually hide itself, and stealthy connect to the Command & Control Server, to get the instruction from hackers.

What is the potential impact?

- Computer owner's personal and financial data might be stolen which may lead to financial loss.
- Computer might be commanded by attacker to perform other criminal activities.

Sources of Information:

- ArborNetwork – Atlas SRF – conficker
- ShadowServer – botnet_drone
- ShadowServer – sinkhole_http_drone
- ShadowServer – Microsoft_sinkhole

Appendices

Appendix 1 – Sources of information

The following information feeds sources

Event Type	Source	First introduced
Defacement	Zone - H	2013-04
Phishing	ArborNetwork: Atlas SRFPhishing	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	Sacour.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

Appendix 2 – Geolocation identification methods

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

Method	Last update
Maxmind	2013-10-29

Appendix 3 – Major Botnet Families

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
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 • ransomware
Conficker	• Downadup • Kido	Worm	• domain generation algorithm (DGA) capability • communicate via P2P network • disable security software	• exploit the Windows Server Service vulnerability (MS08-067) • brute force attacks for admin credential to spread across network • spread via removable drives using "autorun" feature
IRC Botnet	Nil	Trojan	• communicate via IRC network	• backdoor capabilities that allow unauthorized access • launch DDoS attack • send spams

Pushdo	• Cutwail • Pandex	Downloader	• hiding its malicious network traffic • domain generation algorithm (DGA) capability • distribute via drive by download • exploit browser and plugins' vulnerabilities	• download other banking malware (e.g. Zeus and Spyeye) • launch DDoS attacks • send spams
Sality	Nil	Trojan	• rootkit techniques to maintain persistence • communicate via P2P network • spread via removable drives and shares • disable security software • use polymorphic and entry point obscuring (EPO) techniques to infect files	• send spams • proxying of communications • steal sensitive information • compromise web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking) • install other malware
Slenfbot	Nil	Worm	• spread via removable drives and shares	• backdoor capabilities that allow unauthorized access • download financial malware • sending spam • launch DDoS attacks
Torpig	• Sinowal • Anserin	Trojan	• rootkit techniques to maintain persistence (Mebroot rootkit) • domain generation algorithm (DGA) capability • distribute via drive by download	• steal sensitive information • man in the browser attack

ZeroAccess	● max++ ● Sirefef	Trojan	● rootkit techniques to maintain persistence ● communicate via P2P network ● distribute via drive by download ● distribute via disguise as legitimate file (eg. media files, keygen)	● download other malware ● Bitcoin mining and click fraud
Zeus	● Gameover	Banking Trojan	● stealthy techniques to maintain persistence ● distribute via drive by download ● communicate via P2P network	● steal banking credential and sensitive information ● man in the browser attack ● keystroke logging ● download other malware (eg. Cryptolocker) ● launch DDoS attacks