Hong Kong
Security Watch Report

Q4 2013

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 report provides data 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) and bots. Computers in Hong Kong is 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

Table of Content

Highlight of Report

This report is for Quarter 4 of 2013.

In this period, there were 12,536 unique security events related to Hong Kong. The information is collected with IFAS[1] from 19 sources of information.[2] They are not from the incident reports received by HKCERT.

Server related security events

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

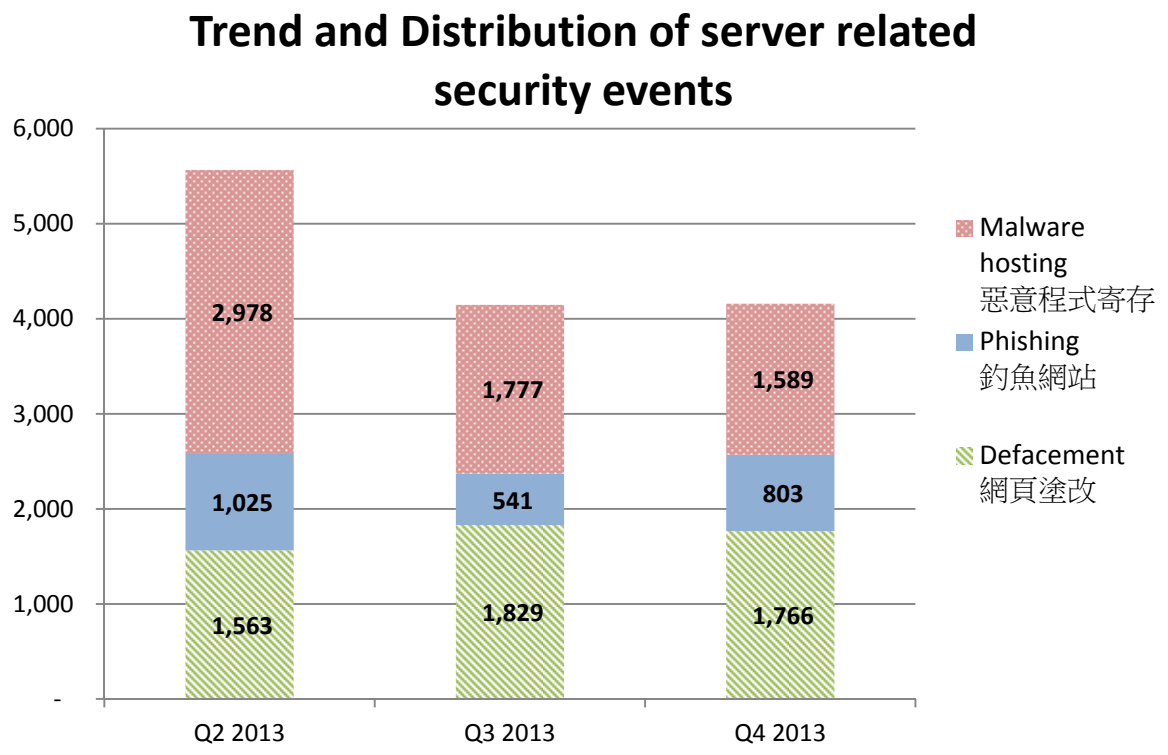


Figure 1 –Trend and distribution of server related security events distributions

[1] Information Feed Analysis System (IFAS) 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

The number of server related security events has been dropped since Q3 2013, and kept steady thru Q4 2013.

The number of malware hosting security events had a clear dropping trend across three consecutive quarters. The number of defacement security events held steady in this quarter while it was still slightly higher than that of Q2 2013. The number of phishing security events had grown significantly in this quarter by 48%. The number of phishing security events bloomed in Nov and Dec of Q4 2013 (Figure 2). It might be related to the holiday season which the cybercriminal took advantage to launch phishing campaigns to steal the consumers' accounts and credentials.

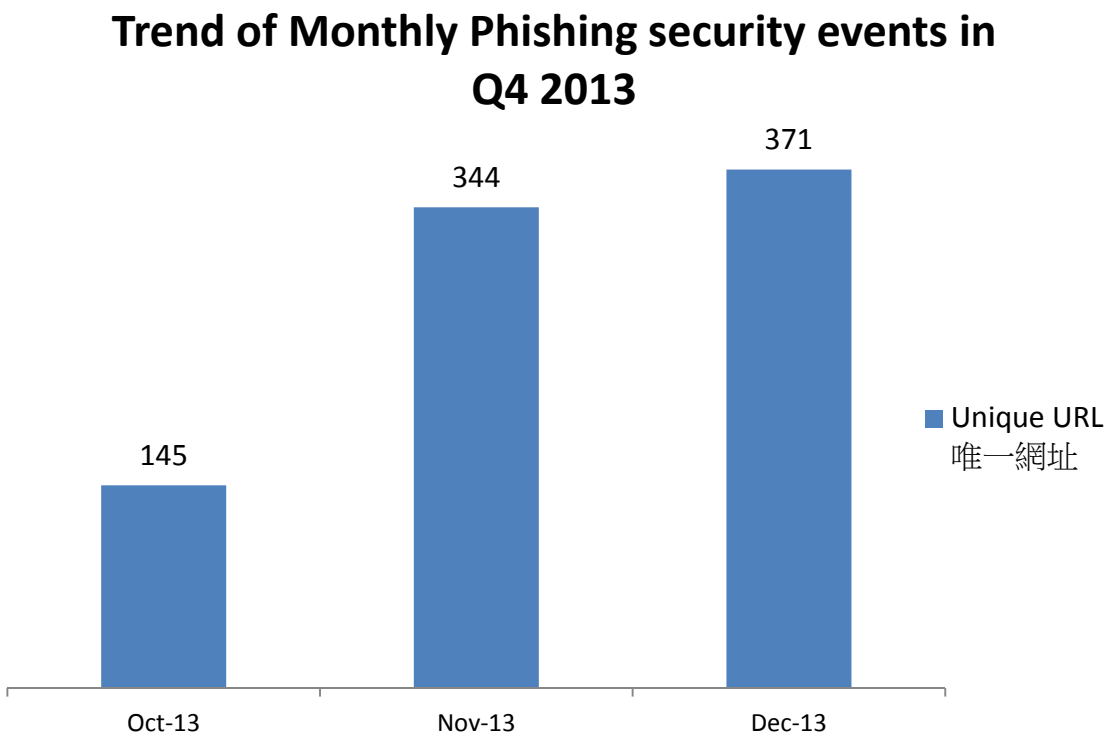


Figure 2 Trend of Monthly Phishing security events in Q4 2013

From HKCERT's experience in handling server related incidents, in about 50% of the reports, the server or application owners did not have good web application or server management. That opened opportunity for cybercriminals to take advantage of, resulting in their servers becoming launchpads of cyber crimes.

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

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:

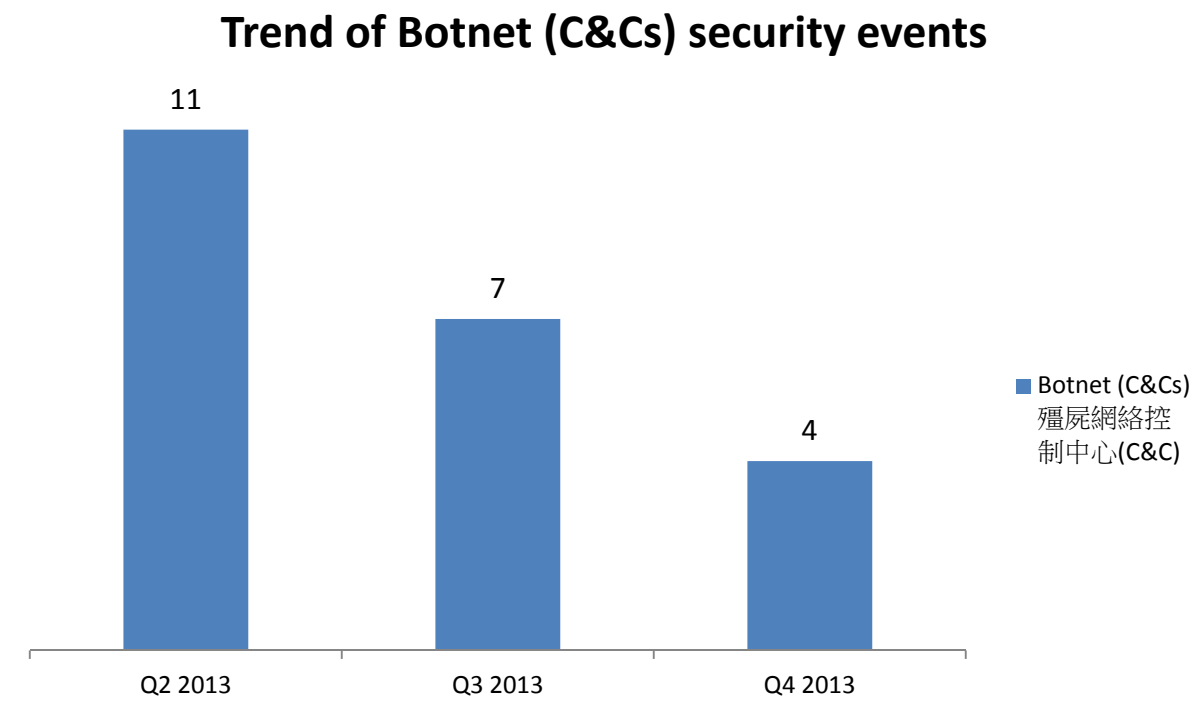


Figure 3 –Trend of Botnet (C&Cs) related security events

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

There were 4 C&C servers reported in this quarter. Two of the reported servers were identified as Zeus C&C servers, while 2 others were IRC bot C&C servers.

Botnet Bots

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

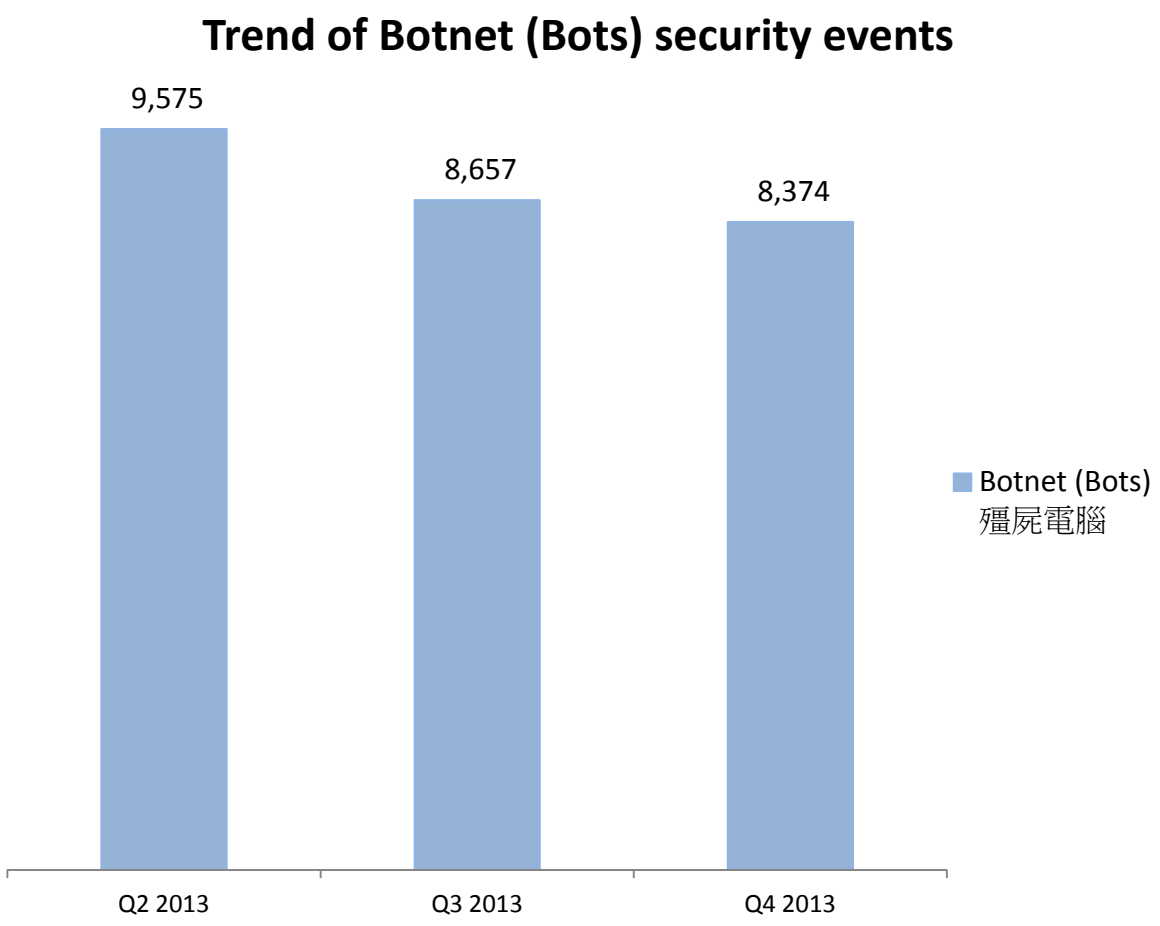


Figure 4 - Trend of Botnet (Bots) security events

Number of Botnet (bots) on Hong Kong network was decreasing across 3 quarters.

In Q4 2013, Conficker continues to be the largest botnet. The maximum number of Conficker machines online on a day in Q4 2013 was 3,175. It has to be noted that Conficker has been around since 2008 and it keeps a high infection rate till now. Some of the reasons are that users are using an unpatched or an unlicensed Windows system that has no security update, and without a working copy of security software. Other studies revealed that the biggest attack vector is credential based attack, then exploit of system vulnerability and

autorun[3]. According to the Security Intelligence Report (SIR), credential based attacks accounted for 54% to 89%; exploit of system vulnerability accounted for 19% to 43%, and attack via autorun accounted for 1% to 11%. Conficker is designed with a small dictionary to perform bruteforce attack to crack the admin password to propagate on the network.

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

- patch the computers
- install a working copy of security software and scan for malware on their machines
- set strong password to avoid credential based attack
- disable autorun features in Window[4]
- do not use software media files and software that have no proper licenses
- pay attention to the end of support of Windows XP in April 2014, and upgrade the operating system to one that has security updates

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

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

[3] According to Microsoft Security Intelligence Report (SIR), Volume 12, published on December 2011, credential-based attack account for 54% to 89% while exploit system vulnerability account for 19% to 43%, and attack via auto-run account for 1%-11%. (http://www.microsoft.com/security/sir/archive/default.aspx)

[4] How to disable the Autorun functionality in Windows, Microsoft, Knowledge Base http://support.microsoft.com/kb/967715

1. Defacement

1.1 Summary

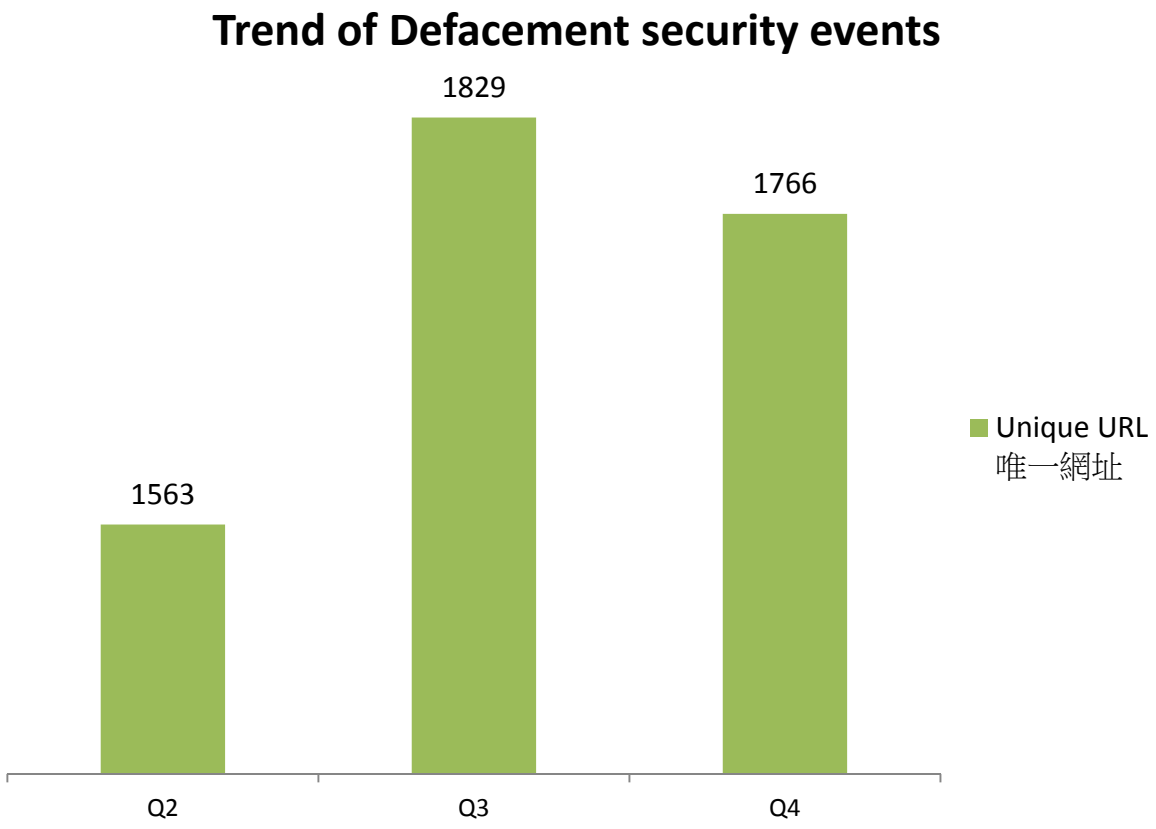


Figure **5** –Trend of Defacement security events

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

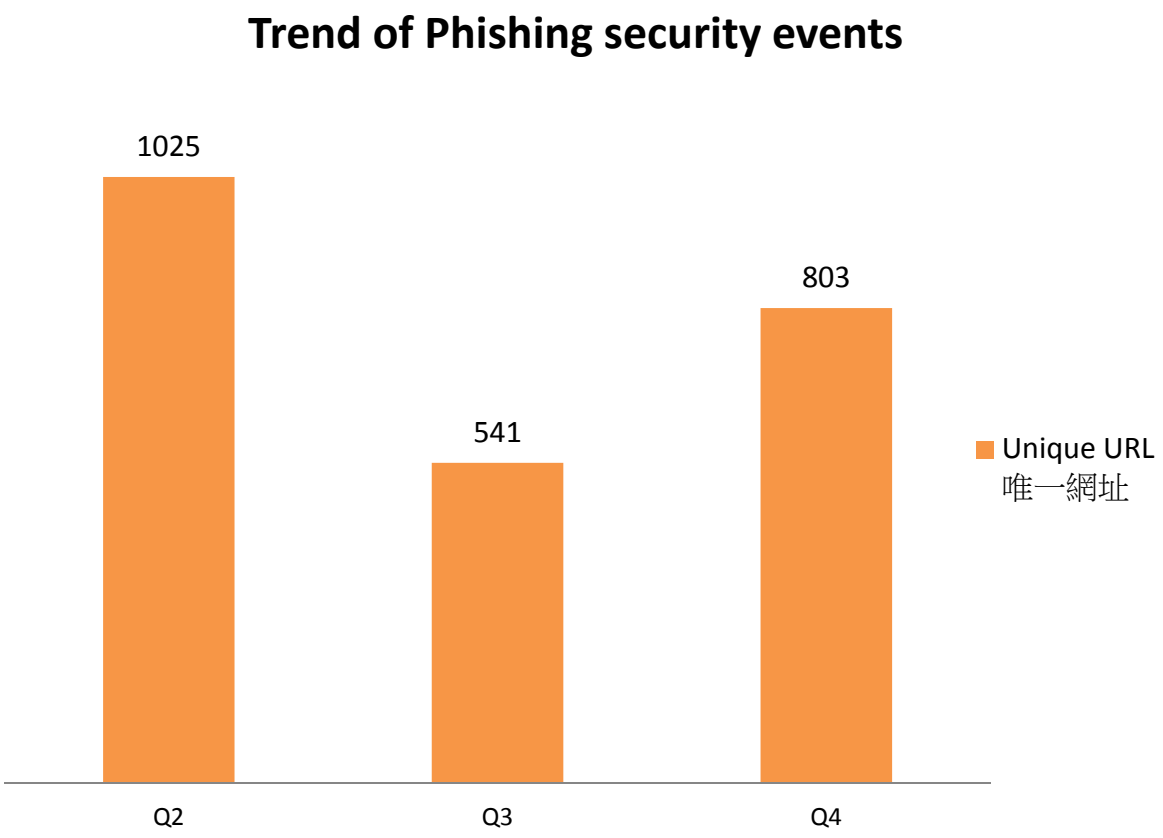


Figure 6 –Trend of Phishing Security Events

What is Phishing?

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

What is the 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

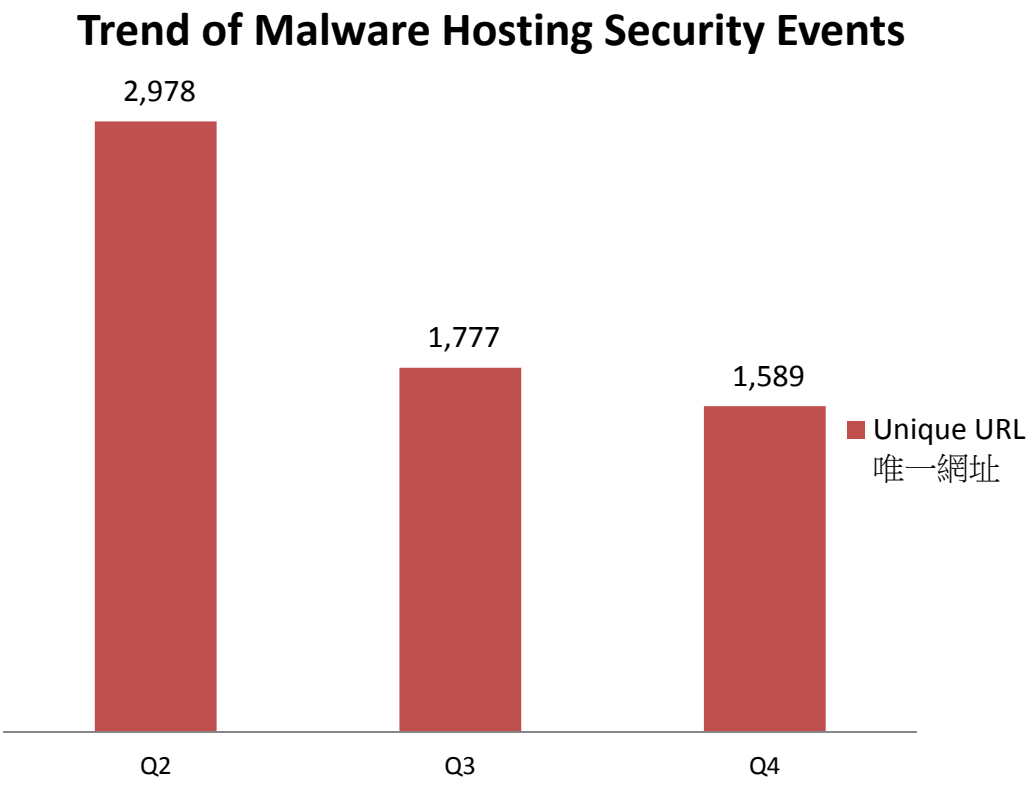


Figure 7 –Trend of Malware Hosting Security Events

What is Malware Hosting?

- Malware Hosting is the dispatching of malware on a website

What is the 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 Botnet – Command & Control Centre

4.1.1 Botnet(C&Cs) found in Hong Kong Networks

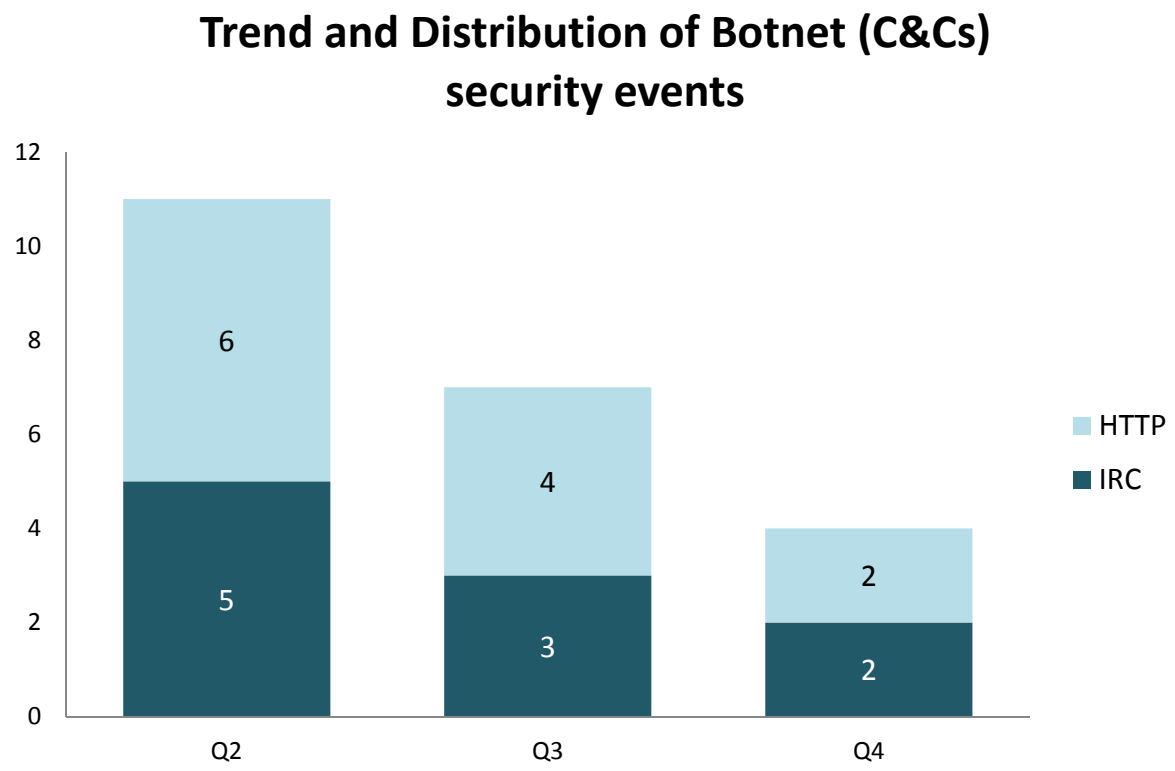


Figure 8 –Trend and Distribution of Botnet (C&Cs) security events

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 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.

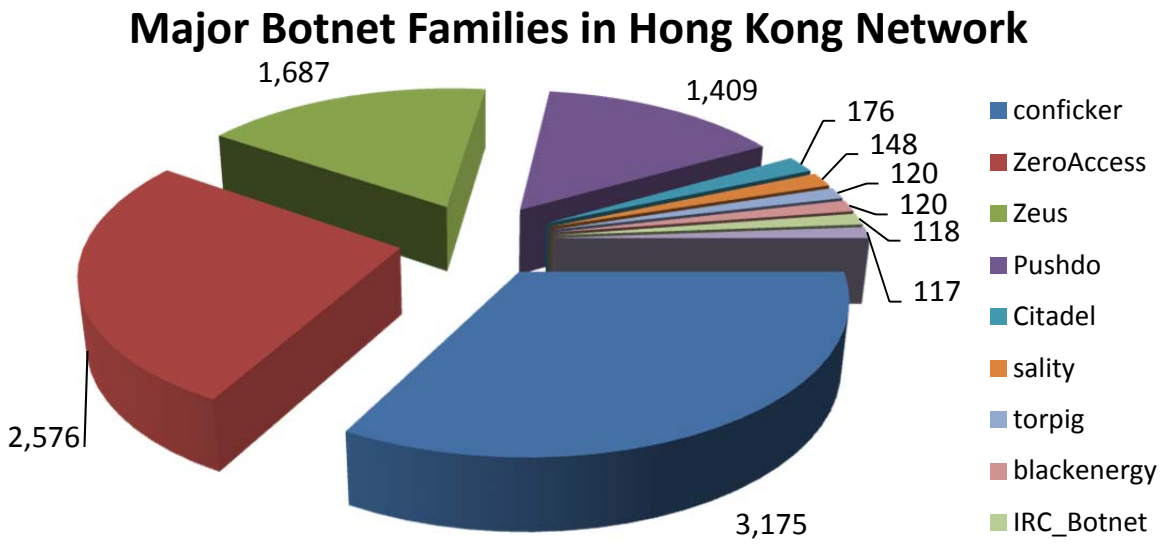
Sources of Information:

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

4.2 Botnet – Bots

4.2.1 Major Botnet Families[5] found on Hong Kong Networks

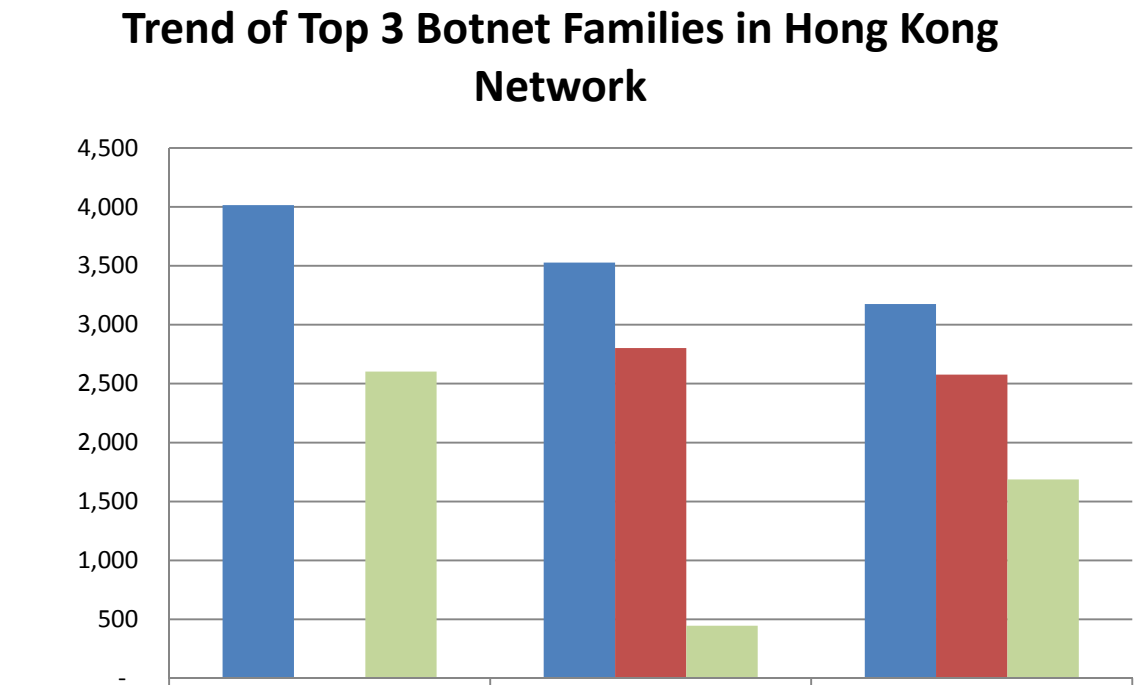
Individual botnet's size is calculated from the maximum of the daily counts of unique IP addresses attempting to connect to the botnet in the report period. In other words, the real botnet size should be larger because not all bots are powered on within the same day.



Rank	Concerned Bots	Unique IP (Max count in a Quarter)
1	conficker	3,175
2	ZeroAccess	2,576
3	Zeus	1,687
4	Pushdo	1,409
5	Citadel	176
6	sality	148
7	torpig	120
8	blackenergy	120
9	IRC_Botnet	118
10	Slenfbot	117

Figure 9 –Major Botnet Families in Hong Kong Networks

[5] 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
conficker	4,014	3,527	3,175
ZeroAccess	-	2,802	2,576
Zeus	2,602	446	1,687

Figure 10 – Trend of Top 3 Botnet Families in Hong Kong Network

*Note:
Information provided from sources for ZeroAccess only 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 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