



**Hong Kong
Security Watch Report**

Q2 2016

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 “.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	4
Report Details.....	9
1. Defacement	9
1.1 Summary	9
2. Phishing	11
2.1 Summary	11
3. Malware Hosting	13
3.1 Summary	13
4. Botnet.....	15
4.1 Botnets – Command & Control Servers.....	15
4.2 Botnets – Bots	16
Appendices.....	18
Appendix 1 – Sources of information	18
Appendix 2 – Geolocation identification methods.....	18
Appendix 3 – Major Botnet Families	19

Highlight of Report

This report is for Quarter 2 of 2016.

In 2016 Q2, there were 20,988 unique security events related to Hong Kong used for analysis in this report. The information is collected with IFAS¹ from 19 sources of information.² They are not from the incident reports received by HKCERT.

Trend of security events

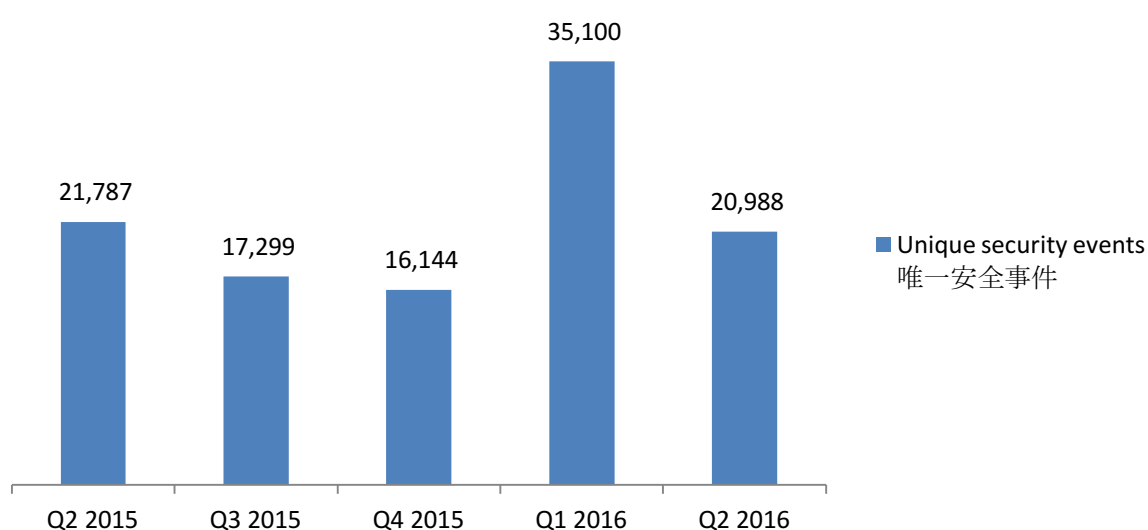


Figure 1-Trend of security events

The total number of security events in Q2 2016 decreased significantly by 40% or 20,988 events. It was mainly due to the decrease in server related events.

Server related security events

Server related security events include malware hosting, phishing and defacement. Their trends and distributions are summarized below:

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

Trend and Distribution of server related security events

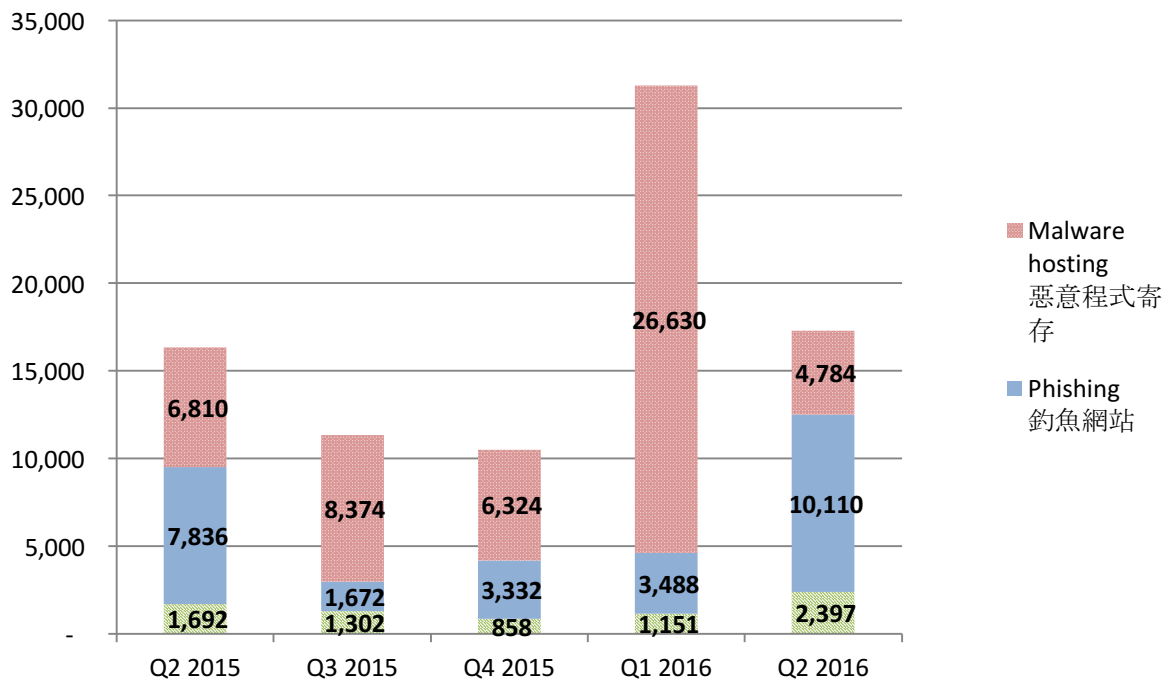


Figure 2 –Trend and distribution of server related security events

The number of server related security events decreased from 31,269 to 17,291 (decreased by 45%) in Q2 2016.

In this quarter, the number of defacement events and phishing events increased by 108% and 189% respectively, while the malware hosting events decreased by 82%. The number of malware hosting events became normal after being extraordinarily high last quarter. The URL/IP ratio of malware hosting events dropped from 32.71 to 9.31.

On the other hand, phishing events reached a record high of 10,110 events with URL/IP ratio increased from 8.66 to 23.62. The high number was contributed by a few compromised websites and a free domains registrar.

In this quarter, most of the events were in compromised servers. The most serious case was from the domain hitsem.com, which contributed 5,142 events (50.9%). We have reported this domain in Hong Kong Security Watch Report 2015 Q4, in which it contributed to 1,085 events. The major phishing target was a Brazilian company aircompanybalonismo.com.br. This story reflected that security incidents should be handled in time, otherwise they may continue to cause even more damage. As of the time of writing, the websites associated to this domain were shut down and could not be reached.

The second largest source of phishing events were a few domains from a Korean online shop FREEMURA hosted 1296 phishing events. Those domains include lovemura.net,

muralove.net, luxmura.com, lovemura.com, muralove.com, luxmura.net and freemura1.kr. All of them resolved to the same IP address. These phishing events were targeting Google accounts.

The third largest source of phishing events was the domain usa.cc. It is a free domains registrar that allow its users to register unlimited free subdomains. Free domains registrar and Dynamic DNS provider has long been abused by criminals to register domains for phishing URLs. In order to lure the potential victims to click on the phishing links, criminals will use domains very similar to the original link. Free domains registrars provide a way to register new domains in low cost.

This quarter there were 993 phishing events utilizing usa.cc, most of them targeting a Japanese gaming site hiroba.dqx.jp. This domain was reported to be a major phishing target in Hong Kong Security Watch Report 2015 Q2.



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, e.g. two factor authentication, at administrative control interface
- acquire information security knowledge to prevent social engineering

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:

Trend of Botnet (C&Cs) security events

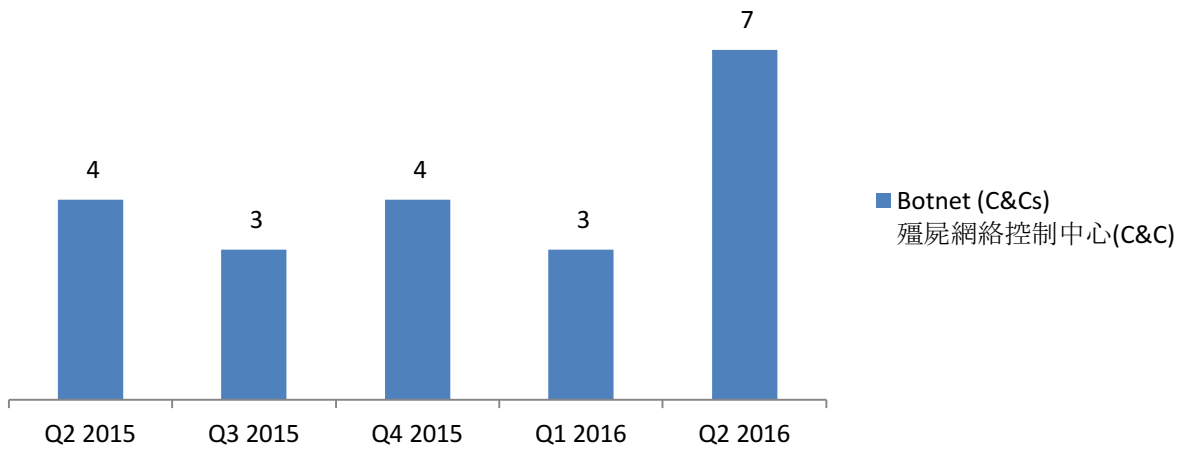


Figure 3 –Trend of Botnet (C&Cs) related security events

The number of botnet Command and Control Servers increased this quarter.

There were 7 C&C servers reported in this quarter. Six were identified as IRC bot C&C servers while one was identified as HTTP server.

Botnet Bots

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

Trend of Botnet (Bots) security events

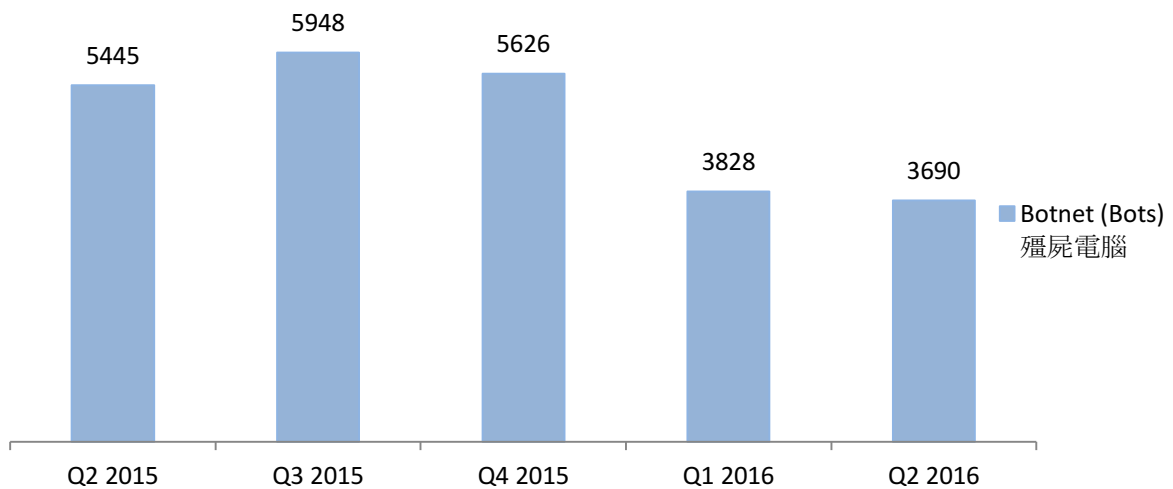


Figure 4 - Trend of Botnet (Bots) security events

Number of Botnet (bots) on Hong Kong network decreased slightly this quarter. Bedep grew from the eighth to the third this quarter. (Figure 12) However, the number reached the peak at April. Its number has dropped significantly to 139 events in May and 69 events in June.

We have reported last quarter that Bedep was believed to have strong connection with Angler Exploit Kit. The drop of Bedep may be due to the disappearance of Angler Exploit Kit. In early June, the banking malware gang behind the Lurk banking Trojan was busted by Russian police. Researchers found that the same group was also linked to the Angler Exploit Kit. After the arrest, activities from Angler Exploit Kit effectively disappeared until now.³ Though the botnet may be disrupted by the arrest, cyber criminals will certainly find alternatives. HKCERT will keep monitoring this botnet.



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
- do not use Windows and software that have no security updates
- do not open files from unreliable sources

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, ZeroAccess, GameOver Zeus and Ramnit are still in action.

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>

³ <http://www.infoworld.com/article/3094034/security/angler-exploit-kit-may-be-dead-but-malware-lives-on.html>

Report Details

1. Defacement

1.1 Summary

Trend of Defacement security events

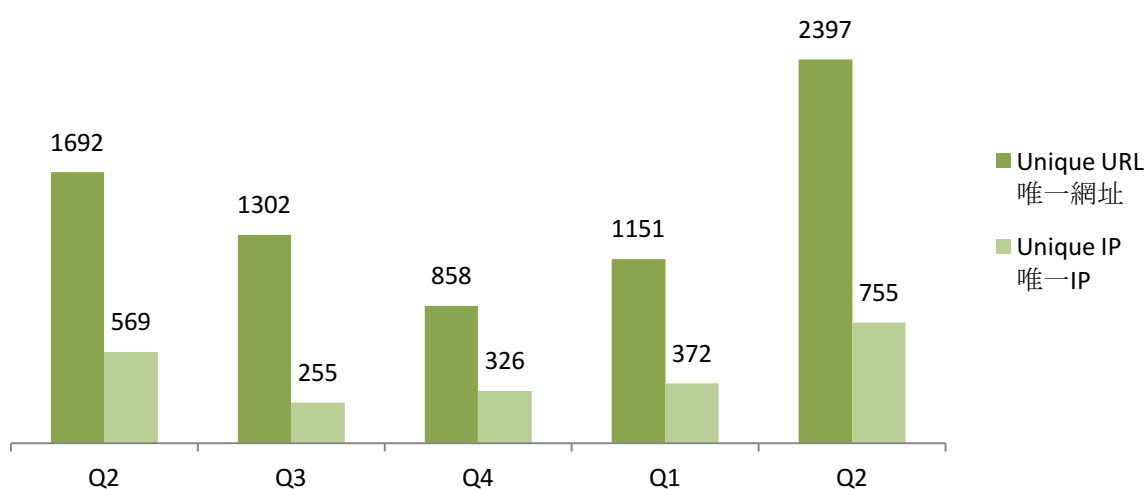


Figure 5 –Trend of Defacement security events



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.

URL/IP ratio of Defacement security events

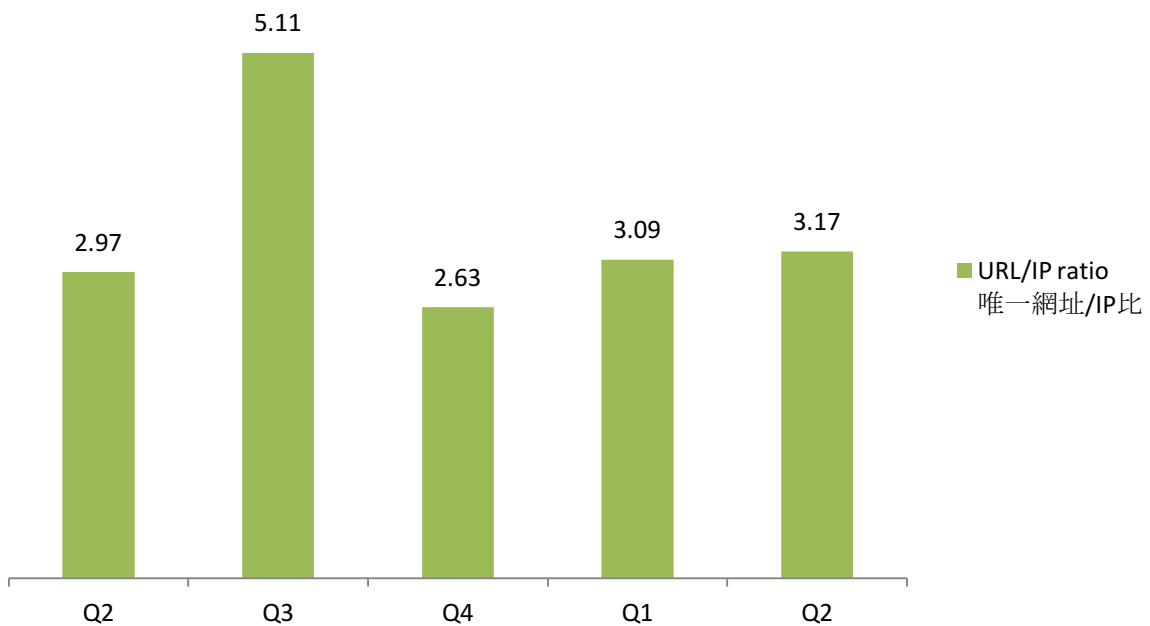


Figure 6 - URL/IP ratio of defacement security events



What is URL/IP ratio?

- It is the number of security events count in unique URL divided by the number of security events count in unique IP addresses

What can this ratio indicate?

- Number of events counted in unique URL cannot reflect the number of compromised servers, since one server may contain many URL
- Number of events counted in unique IP address can better related to the number of compromised servers
- The higher the ratio is, the more mass compromise happened

Sources of Information:

- Zone - H

2. Phishing

2.1 Summary

Trend of Phishing Security Events

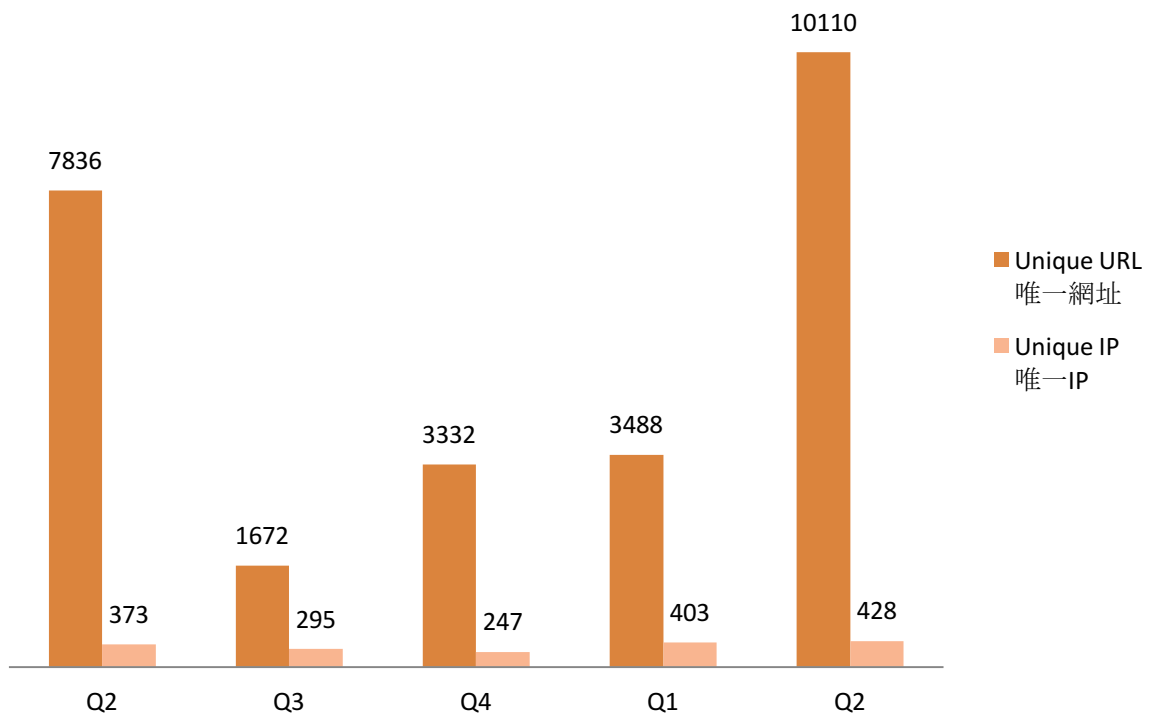


Figure 7 –Trend of Phishing Security Events



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.

URL/IP ratio of Phishing Security Events

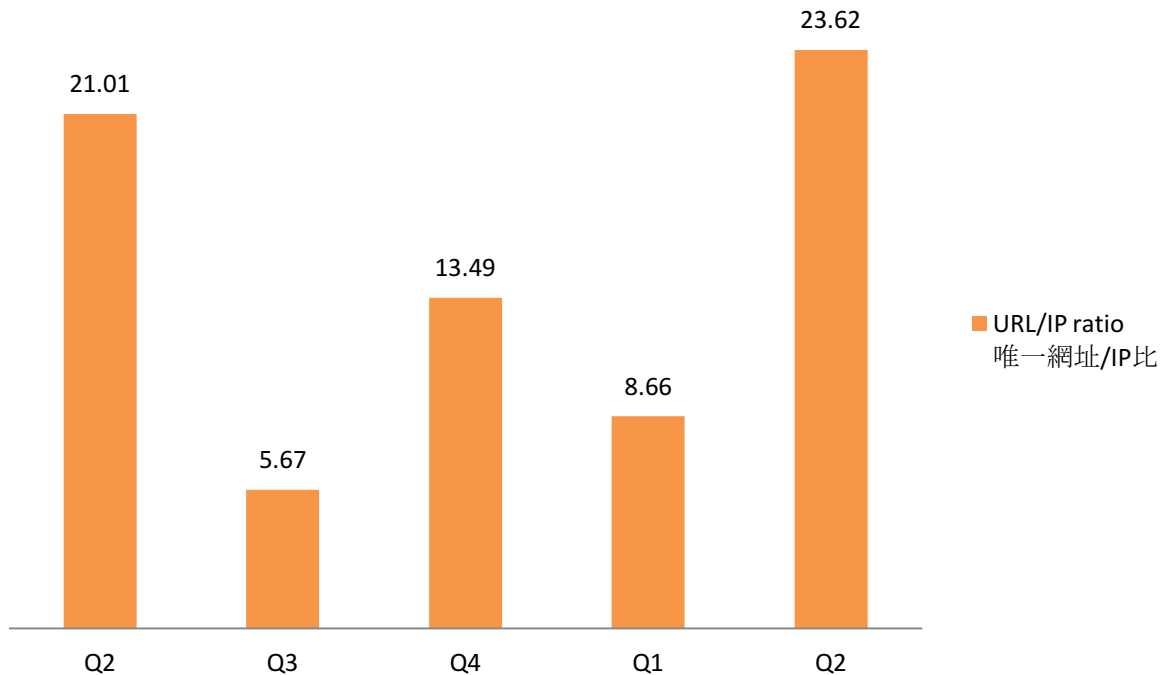


Figure 8 - URL/IP ratio of phishing security events



What is URL/IP ratio?

- It is the number of security events count in unique URL divided by the number of security events count in unique IP addresses

What can this ratio indicate?

- Number of events counted in unique URL cannot reflect the number of compromised servers, since one server may contain many URL
- Number of events counted in unique IP address can better related to the number of compromised servers
- The higher the ratio is, the more mass compromise happened

Sources of Information:

- ArborNetwork – Atlas SRF
- CleanMX – phishing
- Millersmiles
- Phishtank

3. Malware Hosting

3.1 Summary

Trend of Malware Hosting Security Events

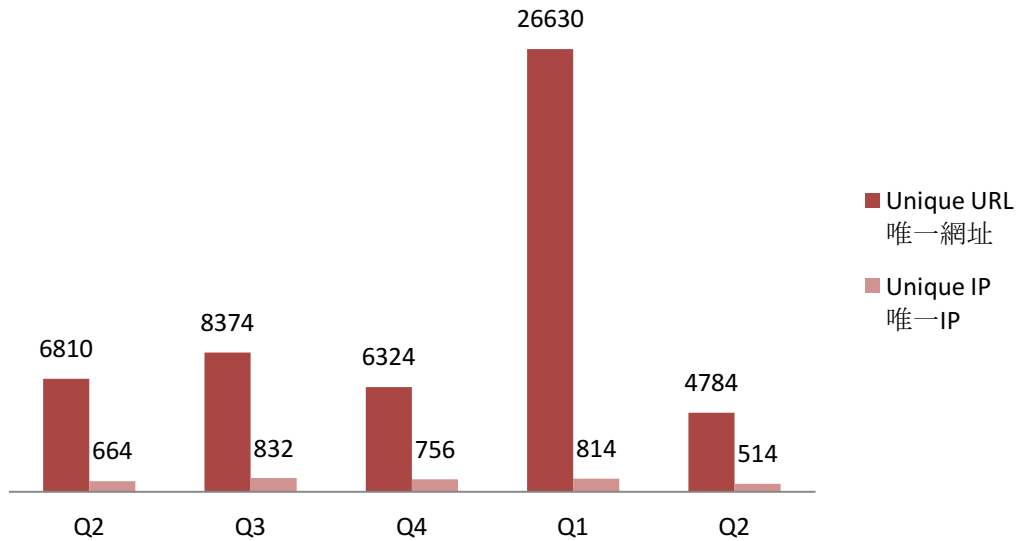


Figure 9 –Trend of Malware Hosting Security Events



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.

URL/IP ratio of Malware Hosting Security Events

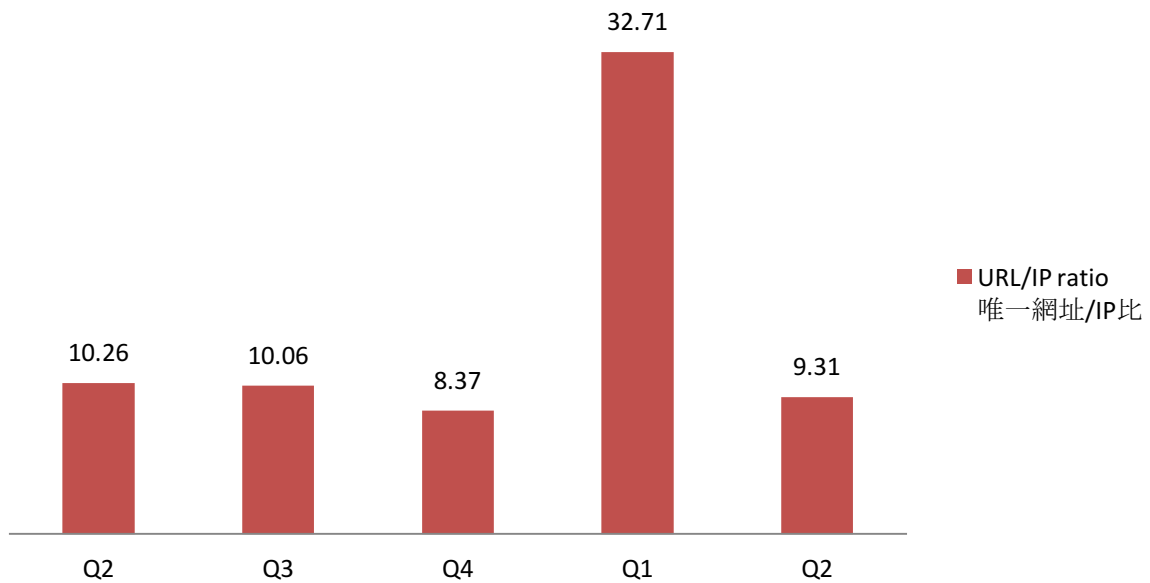


Figure 10 - URL/IP ratio of malware hosting security events



What is URL/IP ratio?

- It is the number of security events count in unique URL divided by the number of security events count in unique IP addresses

What can this ratio indicate?

- Number of events counted in unique URL cannot reflect the number of compromised servers, since one server may contain many URL
- Number of events counted in unique IP address can better related to the number of compromised servers
- The higher the ratio is, the more mass compromise happened

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

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

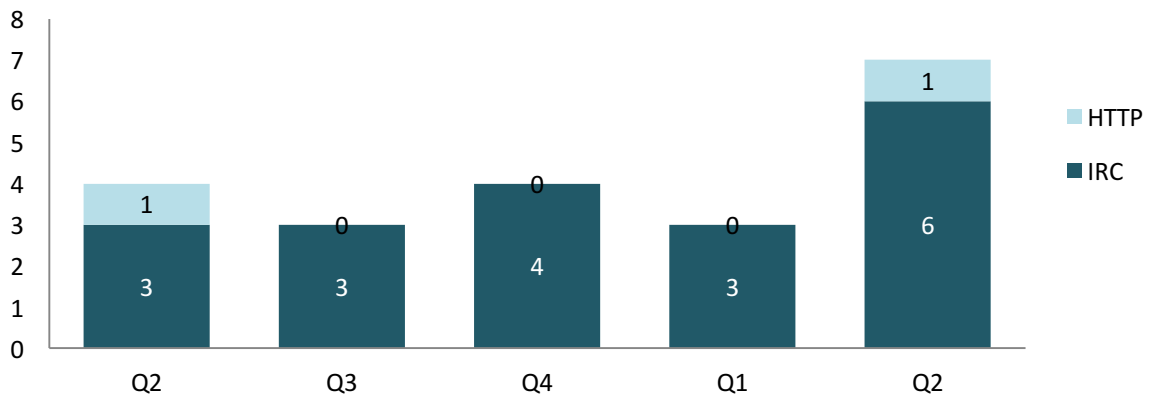


Figure 11 –Trend and Distribution of Botnet (C&Cs) security events



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 connect to it.
- Server might contain large amount of personal and financial data stolen by other bots.

Sources of Information:

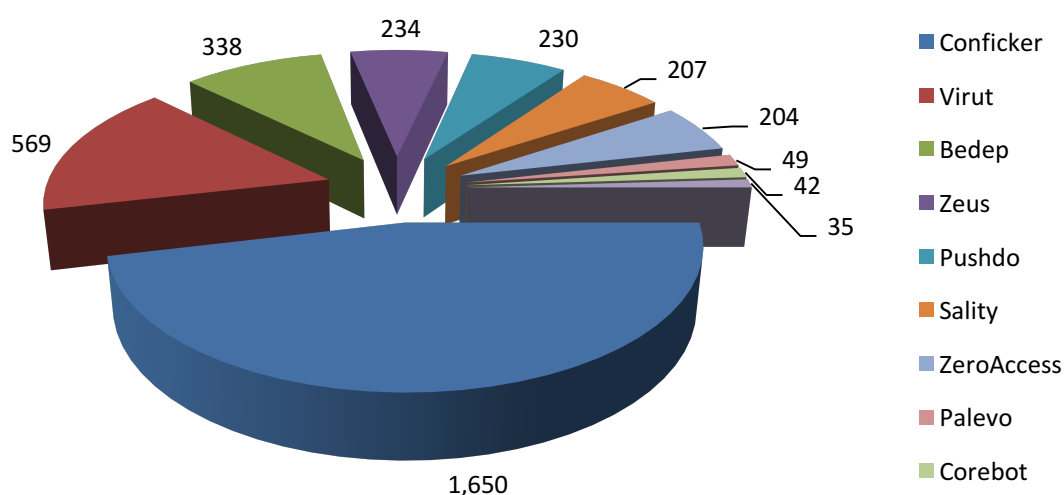
- Zeus Tracker
- SpyEye Tracker
- Palevo Tracker
- Shadowserver – C&Cs

4.2 Botnets – Bots

4.2.1 Major Botnet Families⁴ 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.

Major Botnet Families in Hong Kong Network



Rank	↑↓	Concerned Bots	Number of Unique IP addresses (Max count in a Quarter)	Changes with previous period
1	-	Conficker	1,650	2%
2	-	Virut	569	-11%
3	↑	Bedep	338	46%
4	↓	Zeus	234	-51%
5	↑	Pushdo	230	4%
6	↑	Sality	207	-4%
7	↓	ZeroAccess	204	-11%
8	↑	Palevo	49	NA
9	NEW	Corebot	42	NA
10	↓	Tinba	35	-34%

Figure 12 –Major Botnet Families in Hong Kong Networks

⁴ Major Botnet Families are selected botnet families with considerable amount of security events reported from the information sources constantly across the reporting period.

Trend of Top 5 Botnet Families in Hong Kong Network

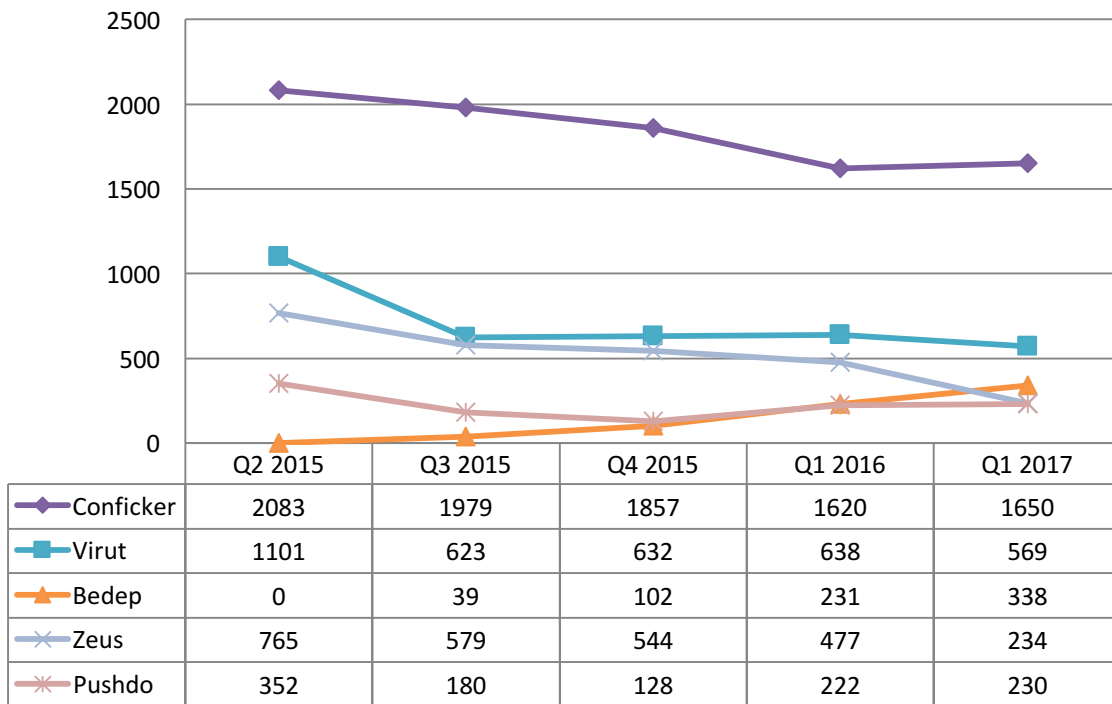


Figure 13 – Trend of Top 5 Botnet Families in Hong Kong Network



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 SRPhishing	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	2016-7-7

Appendix 3 – Major Botnet Families

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Bamital	Nil	Trojan	<ul style="list-style-type: none"> • drive-by download via exploit kit • via P2P network 	<ul style="list-style-type: none"> • Click fraud • Search hijacking
BankPatch	<ul style="list-style-type: none"> • MultiBanker • Patcher • BankPatcher 	Banking Trojan	<ul style="list-style-type: none"> • via adult web sites • corrupt multimedia codecs • spam e-mail • chat and messaging systems 	<ul style="list-style-type: none"> • monitor specific banking websites • steal banking credentials and sensitive information
Bedep	Nil	Trojan	<ul style="list-style-type: none"> • via exploit kit • malvertising 	<ul style="list-style-type: none"> • Click fraud • download other malwares
BlackEnergy	Nil	DDoS Trojan	<ul style="list-style-type: none"> • rootkit techniques to maintain persistence • uses process injection technique • strong encryption and modular architecture 	<ul style="list-style-type: none"> • launch DDoS attacks
Citadel	Nil	Banking Trojan	<ul style="list-style-type: none"> • avoid and disable security tool detection 	<ul style="list-style-type: none"> • steal banking credentials and sensitive information • keystroke logging • screenshot capture • video capture • man-in-the-browser attack • ransomware

Conficker	<ul style="list-style-type: none"> • Downadup • Kido 	Worm	<ul style="list-style-type: none"> • domain generation algorithm (DGA) capability • communicate via P2P network • disable security software • spread via removable drives using "autorun" feature 	<ul style="list-style-type: none"> • exploit the Windows Server Service vulnerability (MS08-067) • brute force attacks for admin credential to spread across network
Corebot	Nil	Banking Trojan	<ul style="list-style-type: none"> • Via droppers 	<ul style="list-style-type: none"> • steal sensitive information • install other malwares • backdoor capabilities that allow unauthorized access
Dyre	Nil	Banking Trojan	<ul style="list-style-type: none"> • spam e-mail 	<ul style="list-style-type: none"> • steal banking credential by tricking the victim to call an illegitimate number • send spams
Gamarue	<ul style="list-style-type: none"> • Andromeda 	Downloader/Worm	<ul style="list-style-type: none"> • via exploit kit • spam e-mail • MS Word macro • removable-drives 	<ul style="list-style-type: none"> • steal sensitive information • allow unauthorized access • install other malware
Glupteba	Nil	Trojan	<ul style="list-style-type: none"> • drive-by download via Blackhole Exploit Kit 	<ul style="list-style-type: none"> • push contextual advertising and clickjacking to victims
IRC Botnet	Nil	Trojan	<ul style="list-style-type: none"> • communicate via IRC network 	<ul style="list-style-type: none"> • backdoor capabilities that allow unauthorized access • launch DDoS attack • send spams

Nymaim	Nil	Trojan	<ul style="list-style-type: none"> • spam e-mail • malicious link 	<ul style="list-style-type: none"> • lock Infected systems • stop victims from accessing files • ask for ransom
Palevo	<ul style="list-style-type: none"> • Rimecud • Butterfly bot • Pilleuz • Mariposa Vaklik	Worm	<ul style="list-style-type: none"> • spread via instant messaging, P2P network and removable drives 	<ul style="list-style-type: none"> • backdoor capabilities that allow unauthorized access • steal login credentials and sensitive information • steal money directly from banks using money mules
Pushdo	<ul style="list-style-type: none"> • Cutwail • Pandex 	Downloader	<ul style="list-style-type: none"> • hiding its malicious network traffic • domain generation algorithm (DGA) capability • distribute via drive by download • exploit browser and plugins' vulnerabilities 	<ul style="list-style-type: none"> • download other banking malware (e.g. Zeus and Spyeeye) • launch DDoS attacks • send spams
Ramnit	Nil	Worm	<ul style="list-style-type: none"> • file infection • via exploit kits • public FTP servers 	<ul style="list-style-type: none"> • backdoor capabilities that allow unauthorized access • steal login credentials and sensitive information

Sality	Nil	Trojan	<ul style="list-style-type: none"> ● 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 	<ul style="list-style-type: none"> ● 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	<ul style="list-style-type: none"> ● spread via removable drives and shares 	<ul style="list-style-type: none"> ● backdoor capabilities that allow unauthorized access ● download financial malware ● sending spam ● launch DDoS attacks
Tinba	<ul style="list-style-type: none"> ● TinyBanker ● Zusy 	Banking Trojan	<ul style="list-style-type: none"> ● via exploit kit ● spam e-mail 	<ul style="list-style-type: none"> ● steal banking credential and sensitive information
Torpig	<ul style="list-style-type: none"> ● Sinowal ● Anserin 	Trojan	<ul style="list-style-type: none"> ● rootkit techniques to maintain persistence (Mebrook rootkit) ● domain generation algorithm (DGA) capability ● distribute via drive by download 	<ul style="list-style-type: none"> ● steal sensitive information ● man in the browser attack

Virut	Nil	Trojan	<ul style="list-style-type: none"> • spread via removable drives and shares 	<ul style="list-style-type: none"> • send spams • launch DDoS attacks • fraud • data theft
Wapomi	Nil	Worm	<ul style="list-style-type: none"> • spread via removable drives and shares • infects executable files 	<ul style="list-style-type: none"> • backdoor capabilities • download and drop additional destructive payloads • alter important files causing unreliable system performance • gather computer activity, transmit private data and cause sluggish computer
ZeroAccess	<ul style="list-style-type: none"> • max++ • Sirefef 	Trojan	<ul style="list-style-type: none"> • rootkit techniques to maintain persistence • communicate via P2P network • distribute via drive by download • distribute via disguise as legitimate file (eg. media files, keygen) 	<ul style="list-style-type: none"> • download other malware • bitcoin mining and click fraud
Zeus	<ul style="list-style-type: none"> • Gameover 	Banking Trojan	<ul style="list-style-type: none"> • stealthy techniques to maintain persistence • distribute via drive by download • communicate via P2P network 	<ul style="list-style-type: none"> • steal banking credential and sensitive information • man in the browser attack • keystroke logging • download other malware (eg. Cryptolocker) • launch DDoS attacks

