Hong Kong
Security Watch Report

Q1 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 ".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 1 of 2015.

In 2015 Q1, there were 10,936 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.
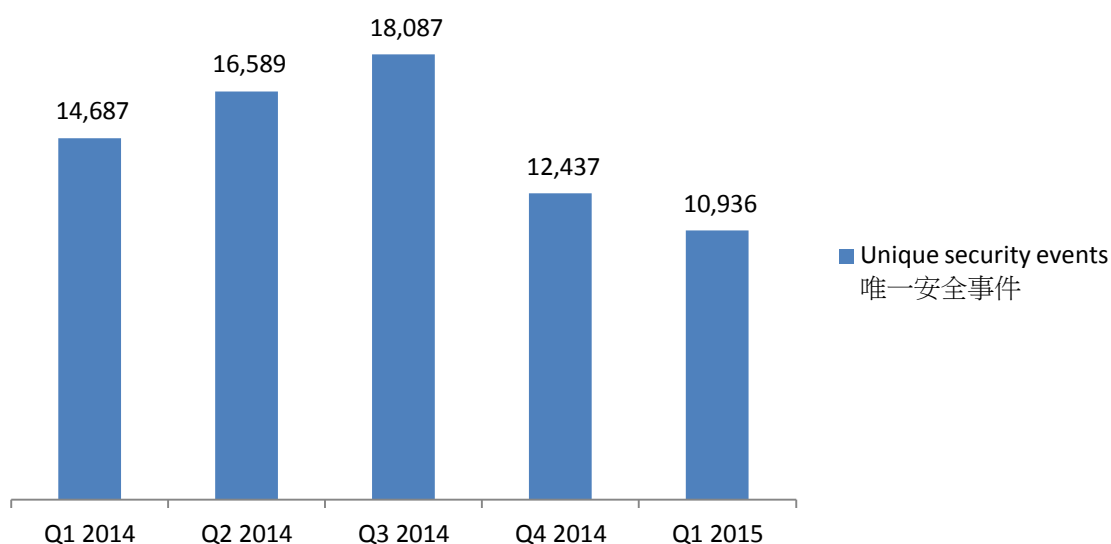
Trend of security events

Figure 1-Trend of security events[3]

The total number of security events in Q1 2015 decreased by 12% or 1501 events, continuing the drop since Q4 2014.

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

[3] The numbers were adjusted to exclude the unconfirmed defacement events

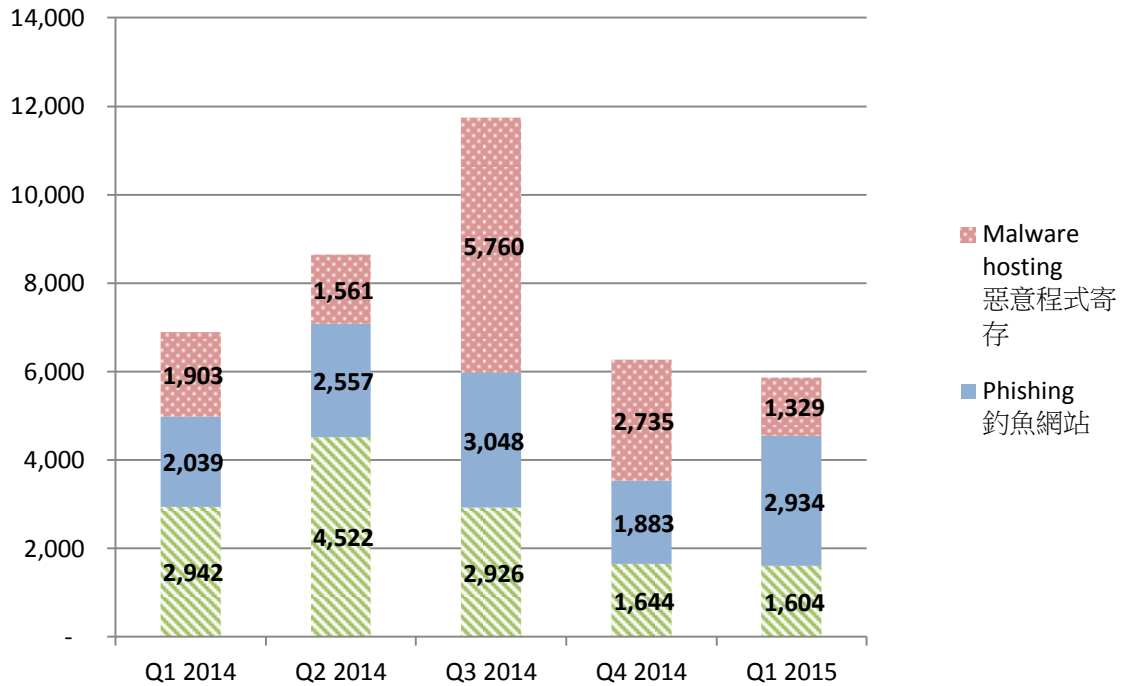# Trend and Distribution of server related security events

Figure 2 –Trend and distribution of server related security events[4]

The number of server related security events slightly decreased by 6% in Q1 2015.

In this quarter, the number of defacement events and malware hosting events decreased by 2% and 51% respectively; while the number of phishing events increased significantly by 55.8%.

The increase of phishing events was due to the increase in URL/IP ratio (Figure 8). The ratio this quarter (14.11) almost doubled the average ratio of the previous four quarters (7.48). The rapid increase of this number reflected that the number of URLs hosted in each IP address increased. In fact, the number of involved IP addresses actually decreased (Figure 7).

---

[4] The numbers were adjusted to exclude the unconfirmed defacement events

	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

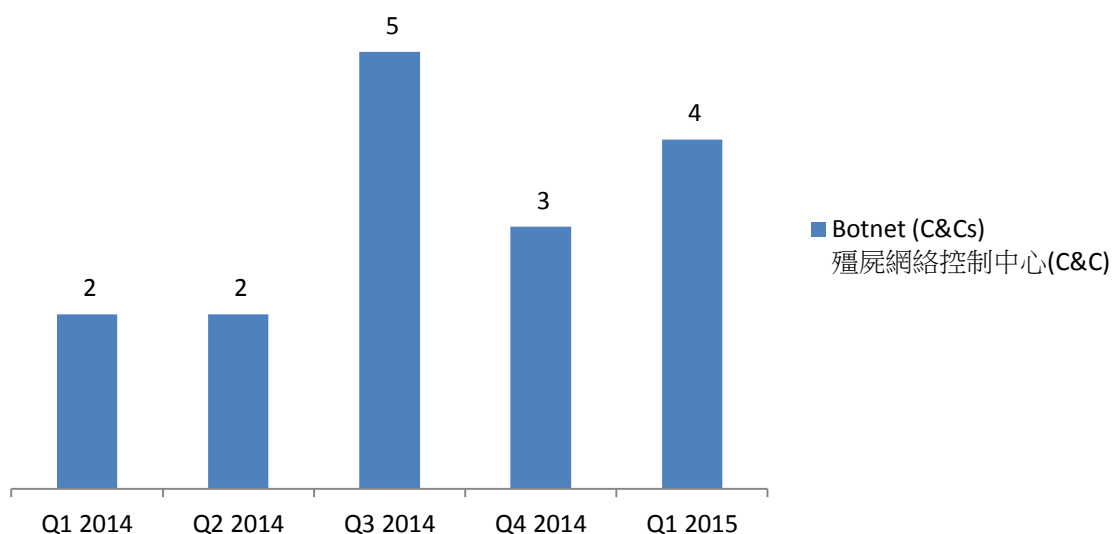

Legend: ■ Botnet (C&Cs) 殭屍網絡控制中心(C&C)

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

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

There were 4 C&C servers reported in this quarter. One of the reported servers was identified as Zeus C&C server, while the other three were identified as IRC bot C&C servers.

Botnet Bots

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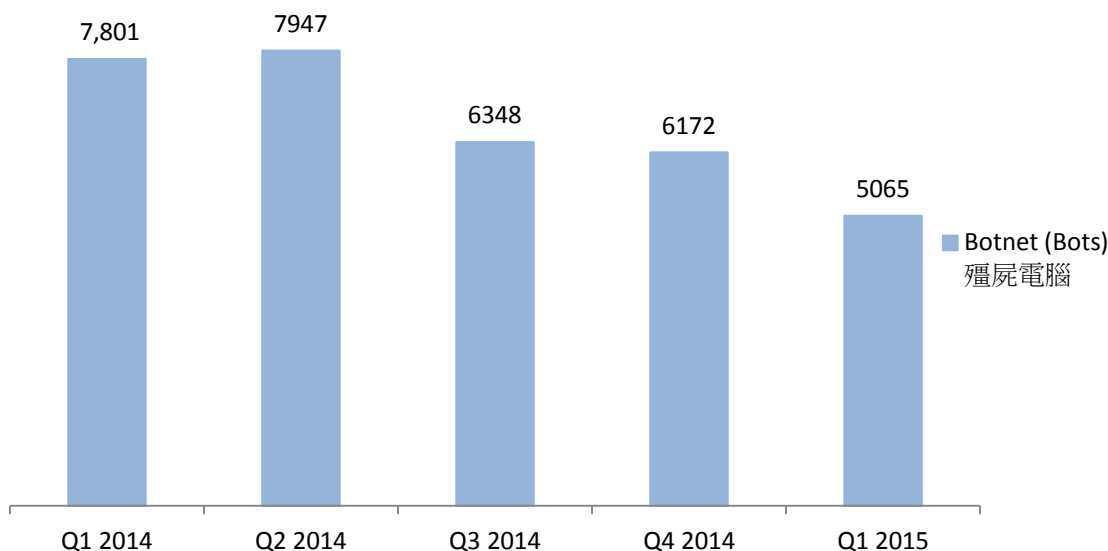
Trend of Botnet (Bots) security events

Figure 4 - Trend of Botnet (Bots) security events

Number of Botnet (bots) on Hong Kong network continued to decrease in this quarter since Q3 2014.

In Q1 2015, the number of botnet infections in Hong Kong decreased by 17.9%. Out of the top 10 botnets, 8 had double digit decreases in percentage (from 10% to 32%). However, the number of Gamarue botnet events increased by 206%. (Figure 12)

The top three botnets of the previous quarter, Conficker, Zeus and ZeroAccess continued their dropping trends (Figure 13). Among them, ZeroAccess events dropped the most. It dropped 32% or 569 events. In the same period, the fourth botnet of the previous quarter, Virut continued to rise. Its number increased 5% and took over ZeroAccess as the third botnet in Hong Kong. It is the first time ZeroAccess dropped out of the top three.

However, researchers[5] found out that ZeroAccess was reactivated after being silent for six months. ZeroAccess was once much stronger than today in 2013. Security researchers from Symantec found a flaw in the P2P communication mechanism in the botnet that enabled them to detect and clean up a large amount of botnets in July 2013. Law enforcements and other security vendors then launched another operation against ZeroAccess in December of the same year. After some struggling, the botnet operators surrendered and were silent since July 2014.

On 15 January, the botnet came back to life and started distributing click-fraud templates to compromised systems. Though the botnet operators didn't attempt to infect new systems for more than one year, the reactivation of the botnet proved that the operators are putting new efforts to the botnet. Though we still have not yet detected the rise of ZeroAccess infection, we will pay more attention to its revival.

The eighth botnet, Gamarue, is another botnet that caught our eyes. Its number increased two folds to 52 events, which was a record high since Q2 of 2013. Researchers[6] found that the botnet operators now use a new approach to spread the botnet – through macro[7] in Microsoft Word documents. When a victim opens a malicious document, which was often sent via spam email, the document content will urge the user to enable macro. Once it is enabled, the macro will perform a multi-staged decoding and program execution to infect the computer.

Gamarue can steal sensitive information, allow hackers to remotely control the target system and further infect the victim with other malwares. In order to avoid being infected, HKCERT urges computers users not to open the attachments in any suspicious emails and do not enable macros in MS office documents that are from unreliable sources.

	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

[5] http://www.computerworld.com/article/2877923/the-zeroaccess-botnet-is-back-in-business.html
[6] https://blog.gdatasoftware.com/blog/article/the-andromedagamarue-botnet-is-on-the-rise-again.html
[7] Macros here mean the embedded codes in Microsoft Office documents. It's intention is to improve document handling

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 and GameOver Zeus 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

Report Details

1. Defacement

1.1 Summary

Trend of Defacement security events
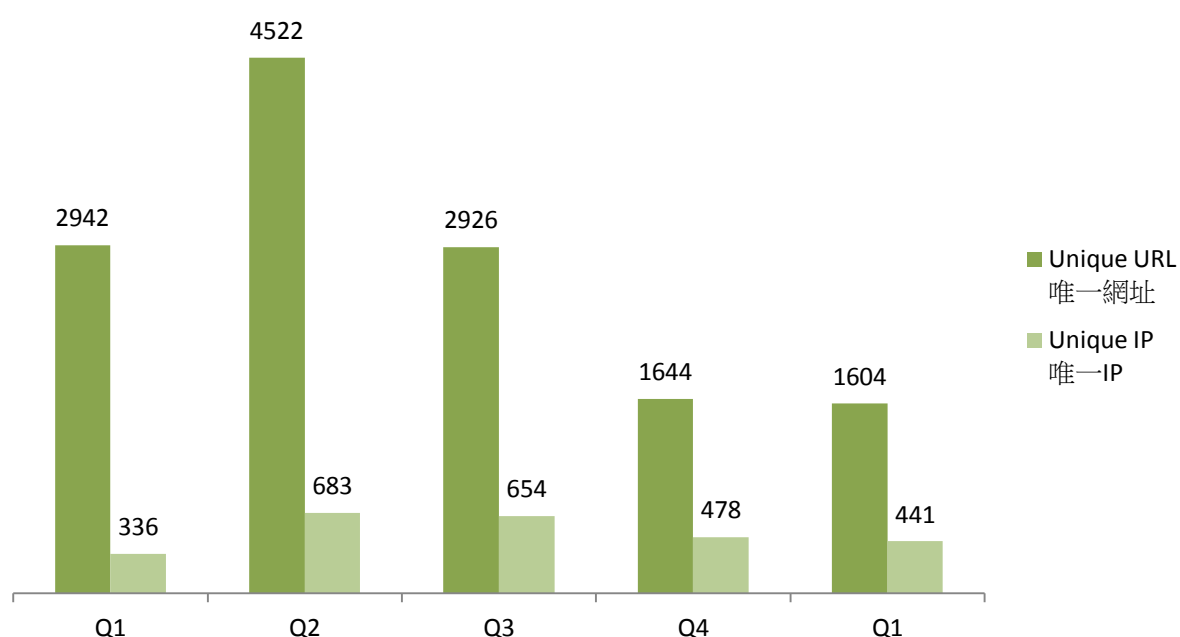
Figure **5**   –Trend of Defacement security events[8]

	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.

---

[8] The numbers were adjusted to exclude the unconfirmed defacement events
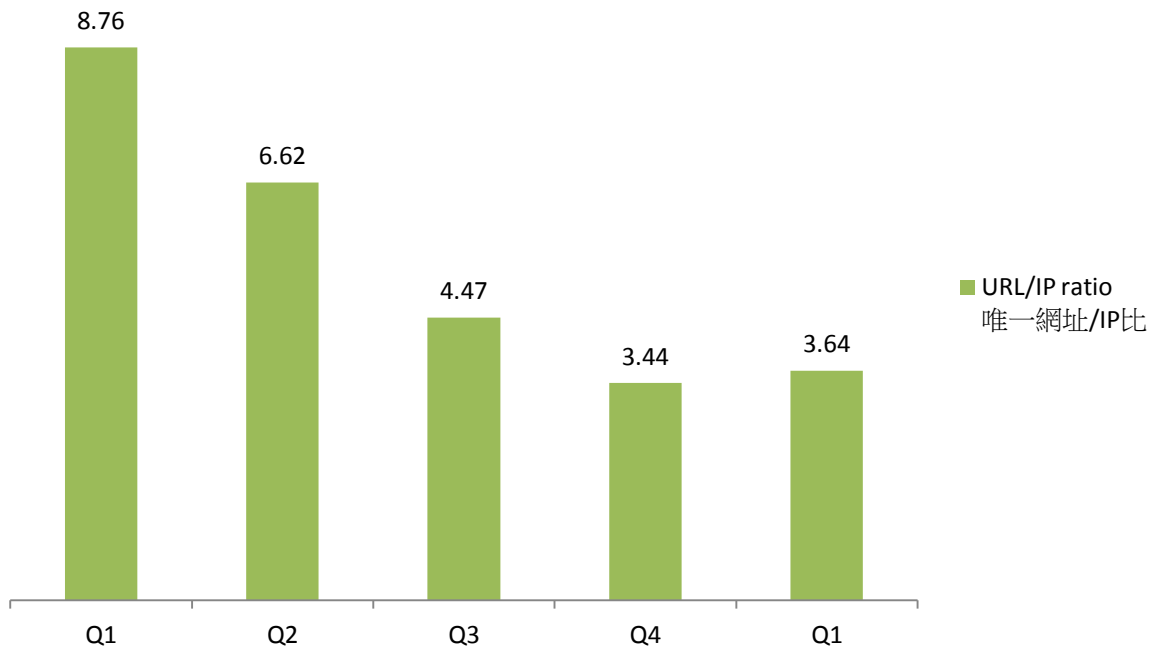
URL/IP ratio of Defacement security events

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

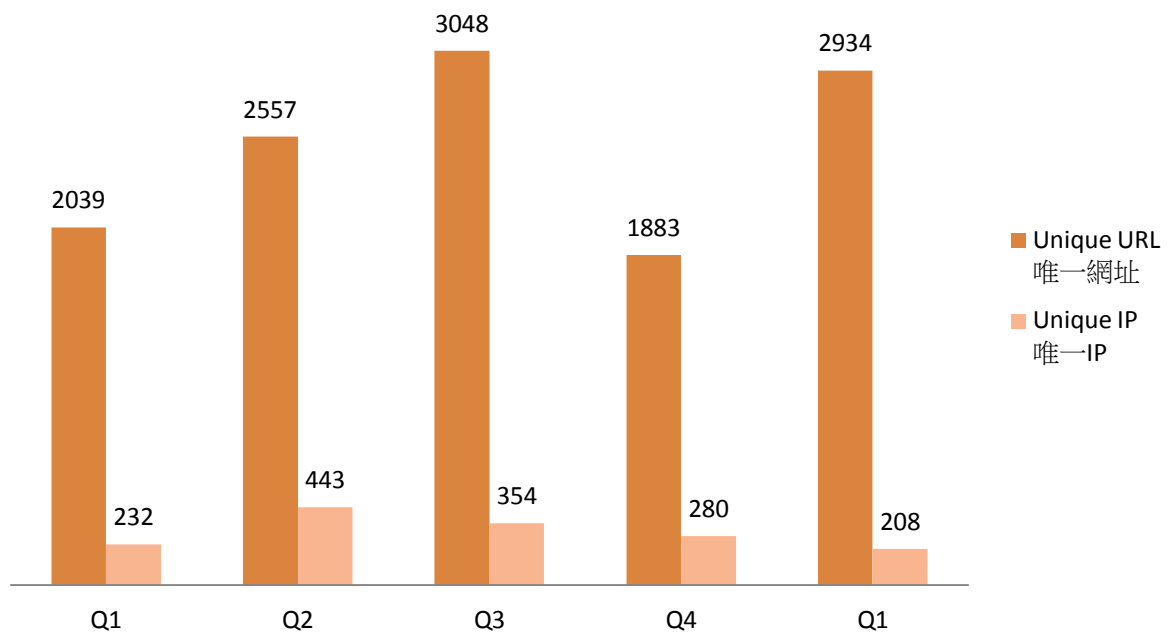## 2.1 <u>Summary</u>

Trend of Phishing Security Events

Figure 7 –Trend of Phishing Security Events

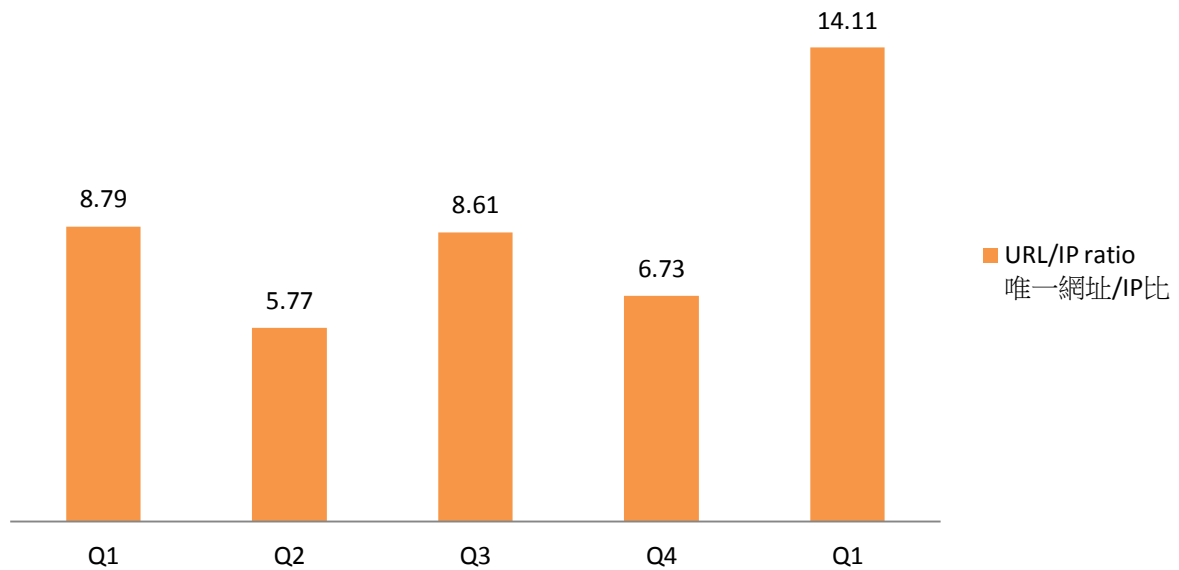|	What is Phishing?
	● Phishing is the spoofing of a legitimate website for fraudulent purpose
	What is the potential impact?
	● Personal information or account credentials of visitors might be stolen, leading to financial loss.
	● Original content might be inaccessible
	● Reputation of the website owner 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 <u>Summary</u>

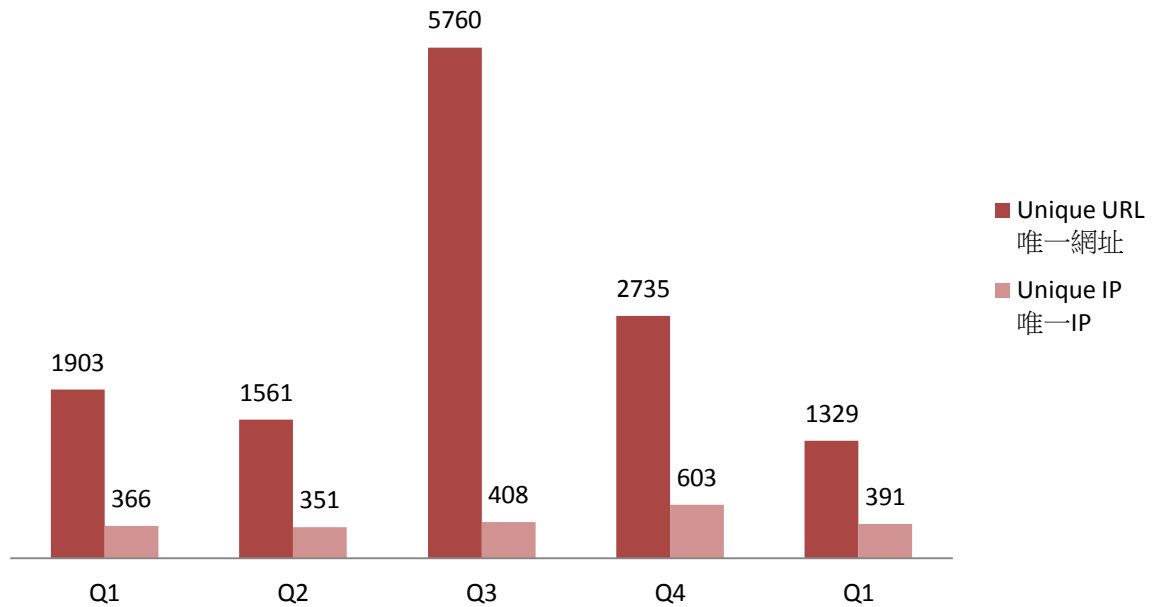## Trend of Malware Hosting Security Events

Figure 9 –Trend of Malware Hosting Security Events

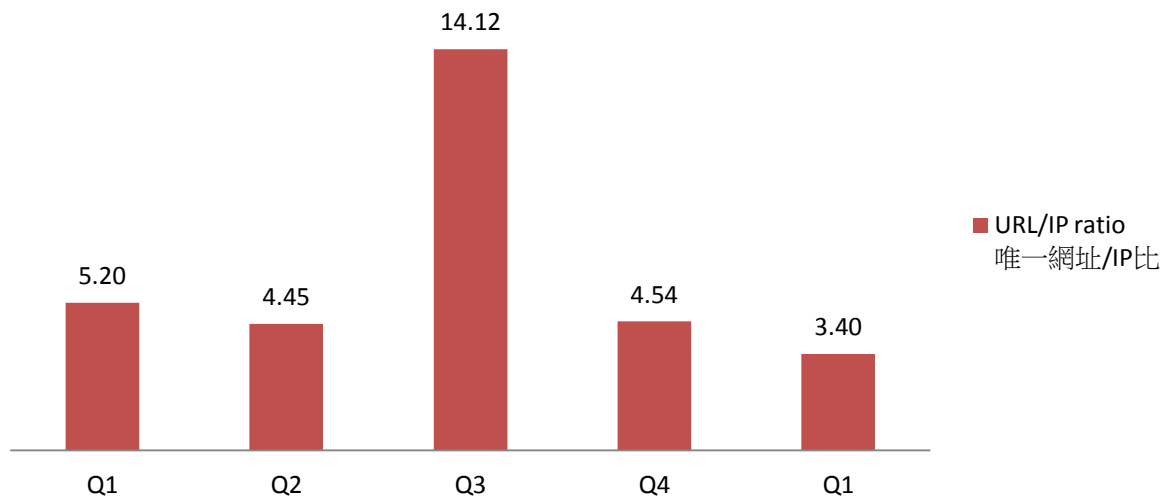|	What is Malware Hosting?
	● Malware Hosting is the dispatching of malware on a website
	What is the potential impact?
	● Visitors might download and install the malware, or execute the malicious script to get compromised.
	● Original content might be inaccessible
	● Reputation of the website owner 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 <u>Botnets – Command & Control Servers</u>

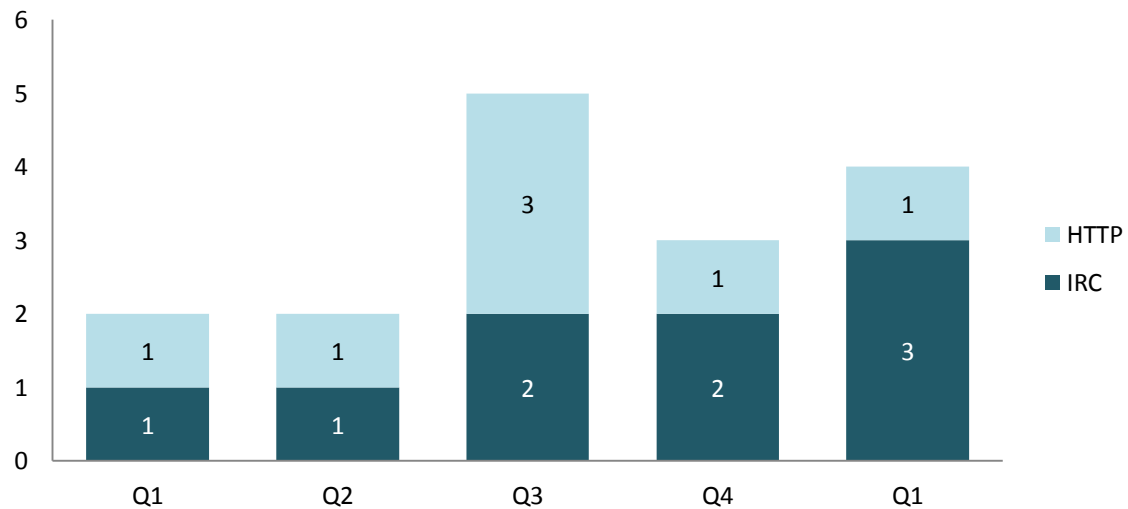## Trend and Distribution of Botnet (C&Cs) security events

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 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.

Major Botnet Families in Hong Kong Network
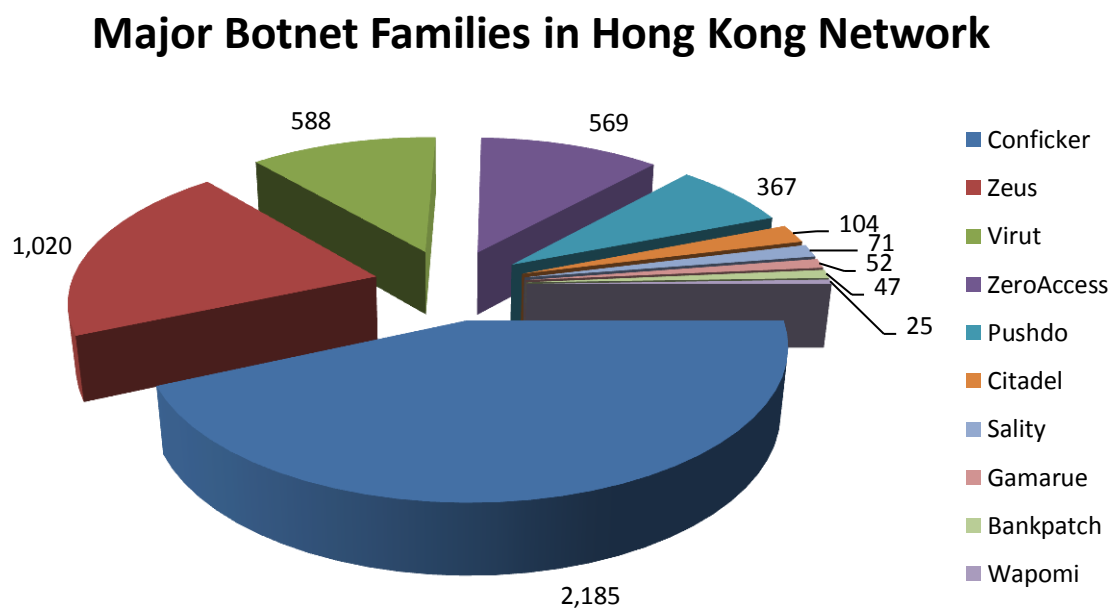
Rank	↑↓	Concerned Bots	Number of Unique IP addresses (Max count in a Quarter)	Changes with previous period
1	-	Conficker	2,185	-10%
2	-	Zeus	1,020	-31%
3	↑	Virut	588	5%
4	↓	ZeroAccess	569	-32%
5	-	Pushdo	367	-10%
6	-	Citadel	104	-13%
7	-	Sality	71	-23%
8	↑	Gamarue	52	206%
9	-	Bankpatch	47	-25%
10	↑	Wapomi	25	-22%

Figure 12 –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.

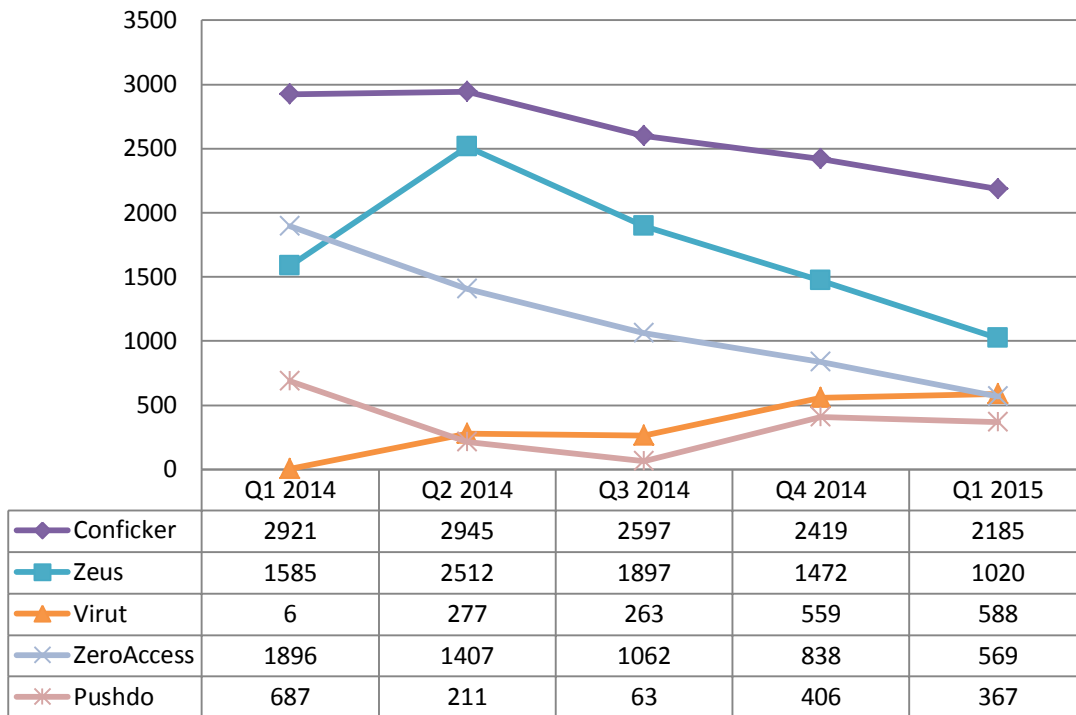# Trend of Top 5 Botnet Families in Hong Kong Network

	Q1 2014	Q2 2014	Q3 2014	Q4 2014	Q1 2015
Conficker	2921	2945	2597	2419	2185
Zeus	1585	2512	1897	1472	1020
Virut	6	277	263	559	588
ZeroAccess	1896	1407	1062	838	569
Pushdo	687	211	63	406	367

Figure 13 – Trend of Top 5 Botnet Families in Hong Kong Network[10]

💡	**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

---

[10] The numbers of Virut events in Q2 and Q3 were adjusted.

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	2015-3-17

Appendix 3 – Major Botnet Families

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
BankPatch	● MultiBanker ● Patcher ● BankPatcher	Banking Trojan	● via adult web sites ● 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 ● 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

Gamarue	● Andromeda	Downloader/ Worm	● via exploit kit ● spam e-mail ● MS Word macro ● removable-drives	● steal sensitive information ● allow unauthorized access ● install other malware
Glupteba	Nil	Trojan	● drive-by download via Blackhole Exploit Kit	● push contextual advertising and clickjacking to victims
IRC Botnet	Nil	Trojan	● communicate via IRC network	● backdoor capabilities that allow unauthorized access ● launch DDoS attack ● send spams
Palevo	● Rimecud ● Butterfly bot ● Pilleuz ● Mariposa Vaklik	Worm	● spread via instant messaging, P2P network and removable drives	● backdoor capabilities that allow unauthorized access ● steal login credentials and sensitive information ● steal money directly from banks using money mules
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
Virut	Nil	Trojan	● spread via removable drives and shares	● Send spams ● Launch DDoS attacks ● Fraud ● Data theft

Wapomi	Nil	Worm	● spread via removable drives and shares ● infects executable files	● 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	● 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