



**Hong Kong
Security Watch Report**

Q2 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 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.....	10
1. Defacement.....	10
1.1 Summary.....	10
2. Phishing.....	12
2.1 Summary.....	12
3. Malware Hosting.....	14
3.1 Summary.....	14
4. Botnet	16
4.1 Botnets – Command & Control Servers.....	16
4.2 Botnets – Bots.....	17
Appendices.....	19
Appendix 1 – Sources of information	19
Appendix 2 – Geolocation identification methods	19
Appendix 3 – Major Botnet Families.....	20

Highlight of Report

This report is for Quarter 2 of 2014.

In 2014 Q2, there were 16,589 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.

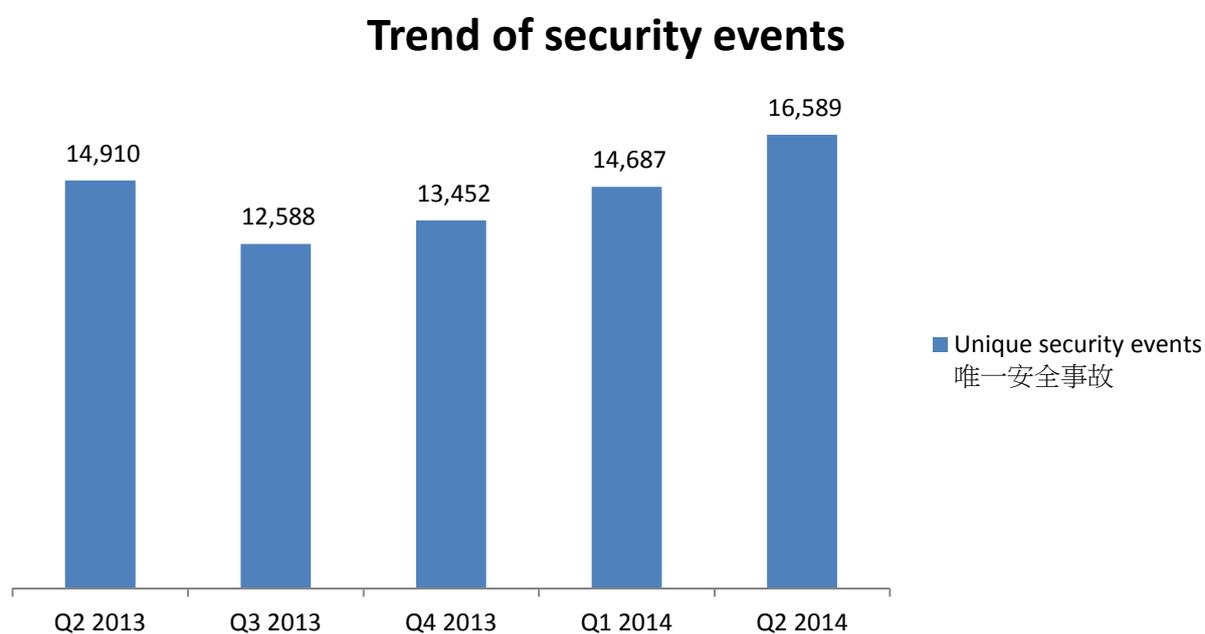


Figure 1-Trend of security events³

The total number of security events has increased in Q2 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

³ The numbers were adjusted to exclude the unconfirmed defacement events

Server related security events

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

Trend and Distribution of server related security events

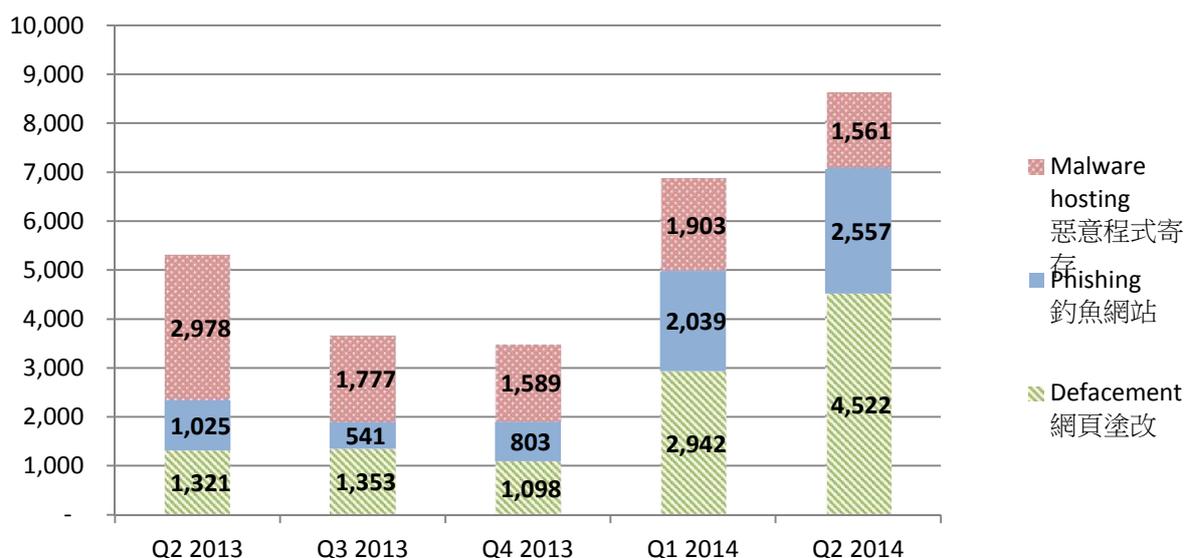


Figure 2 –Trend and distribution of server related security events⁴

The number of server related security events moderately increased in Q2 2014.

In this quarter, the number of malware hosting security events decreased by 18% while the number of phishing and defacement increased by 25% and 54% respectively.

This quarter, the URL/IP address ratio of defacement, phishing and malware hosting security events were added to the report. The server related security events in this report used to be counted in unique URL. However, this indicator may not be able to reflect the number of compromised servers since one compromised servers can contribute to hundreds or even thousands of events. For example, in this quarter, there is a mass defacement event on one single IP address that contributed 635 URLs. The URL/IP ratio can reflect the number of mass compromise events, the higher the ratio is, the more mass compromise happened.

According to the data from Zone-H (Figure 3), about one third of the defacements in this quarter were attacked through known vulnerabilities. Those vulnerabilities can be removed

⁴ The numbers were adjusted to exclude the unconfirmed defacement events

by applying latest security patches. System and application administrators should apply the latest security patches to avoid the known vulnerabilities being exploited.

Other than that, 11% of the events were attacked by social engineering. Social engineering⁵ means tricking people to perform certain actions or provide confidential information. In order not to fall into the traps of the cyber criminals, the awareness of information security should be raised. Server administrators, web sites owners and other related parties should obtain sufficient information security training. For servers that contains sensitive data or perform critical operations, measures such as segregation of duties should be deployed to limit the damage caused by one single staff.

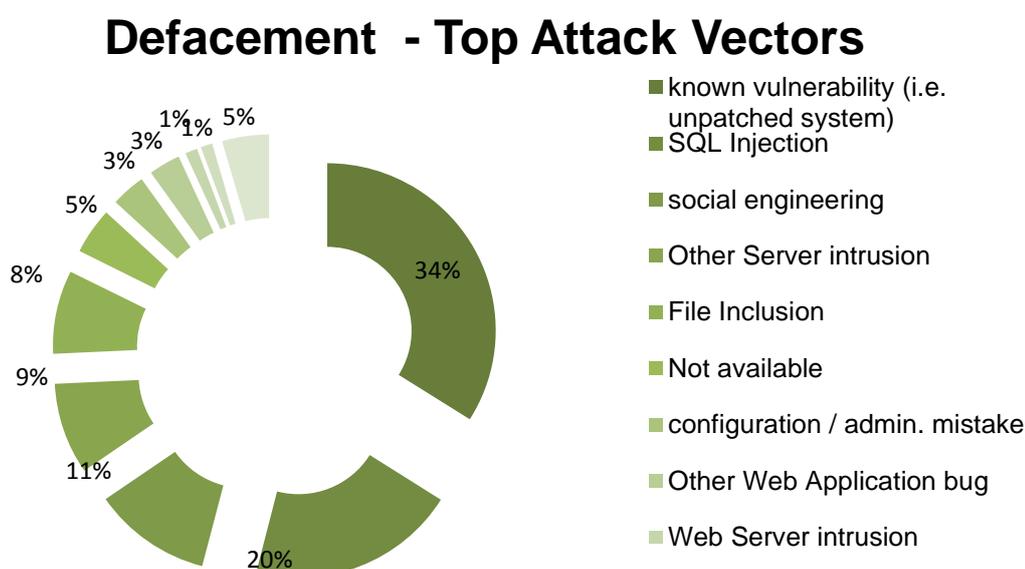


Figure 3 - top attack vectors of defacements



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

⁵ [http://en.wikipedia.org/wiki/Social_engineering_\(security\)](http://en.wikipedia.org/wiki/Social_engineering_(security))

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

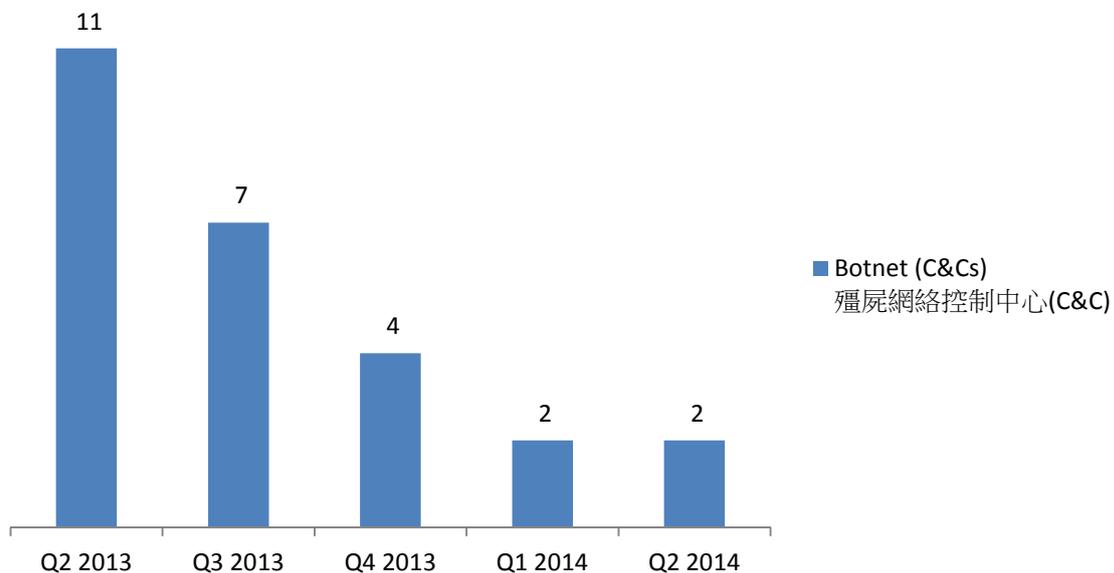


Figure 4 –Trend of Botnet (C&Cs) related security events

Number of botnet Command and Control Servers was the same as last quarter.

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:

Trend of Botnet (Bots) security events

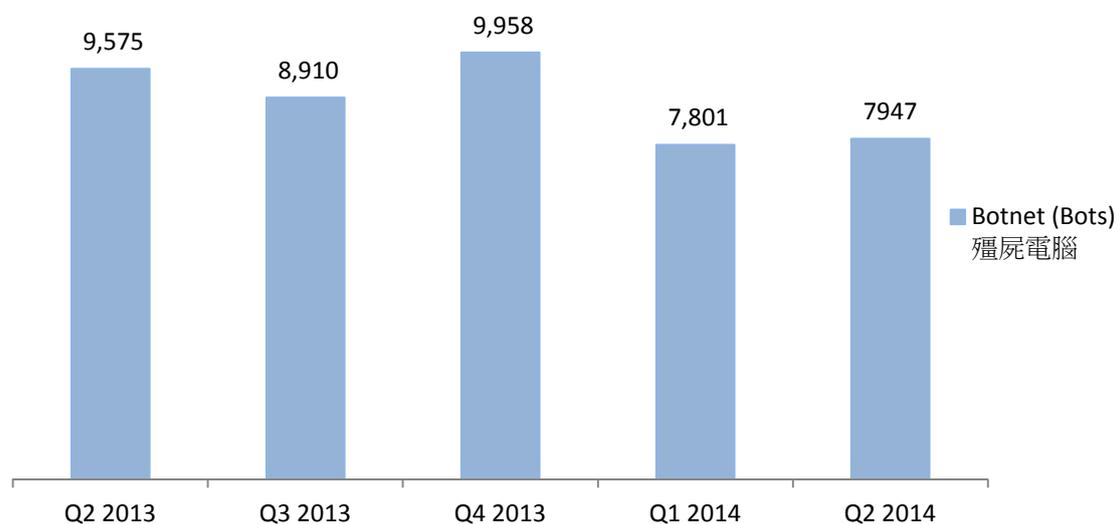


Figure 5 Trend of Botnet (Bots) security events⁶

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

In Q2 2014, the number of botnet infections in Hong Kong increased by 2%, though 7 of the previous top 10 botnets have their numbers decreased or roughly unchanged.

In this quarter, Conficker remains to be the top botnet in Hong Kong. A research⁷ pointed out that the high infection rate of conficker was “attributed to the fact that a number of companies are still using Windows XP, susceptible to this threat”. It reflects that the number of computers using Windows XP is still high in Hong Kong.

The events of Zeus increased the most in the top ten botnets. It increased by 58% or 927 events. The increase of Zeus events was mainly due to a takedown operation, which caused a lot of victim IP addresses surfaced. In June, U.S. law enforcement cooperated with law enforcement of other nations and network security companies to launch a joint operation named "Operation Tovar". In the operation, the communications between the infected computers were severed, re-directing these computers away from criminal servers to

⁶ The number botnet(bots) security events in Q4 2013 was adjusted due to the update of numbers of the Zeus botnet

⁷ <http://blog.trendmicro.com/trendlabs-security-intelligence/downad-tops-malware-spam-source-in-q2-2014/>

sinkholes that are under the US government's control⁸. FBI identified the IP addresses of the victim computers that connected to the sinkholes and to provide that information to Computer Emergency Readiness Teams (CERTs) around the world, including HKCERT. HKCERT has coordinated with the corresponding parties to clean up the infected computers.⁹

In late April, the events of Palevo botnet were recorded in IFAS for the first time. It soon grew to the fourth botnets in May and kept its rank in June. Palevo is a worm that spreads using instant messaging, P2P networks and removable drives. It opens a backdoor on the compromised computer and steals sensitive information of the victim. To stop it from further growing, all suspicious links and files should not be opened.

	HKCERT urges users to protect computers so as not to become part of the botnets.
	<ul style="list-style-type: none">• 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

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
	<ul style="list-style-type: none">• Botnet Detection and Cleanup Guideline https://www.hkcert.org/botnet

⁸ <http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted>

⁹ https://www.hkcert.org/my_url/blog/14061302

Report Details

1. Defacement

1.1 Summary

Trend of Defacement security events

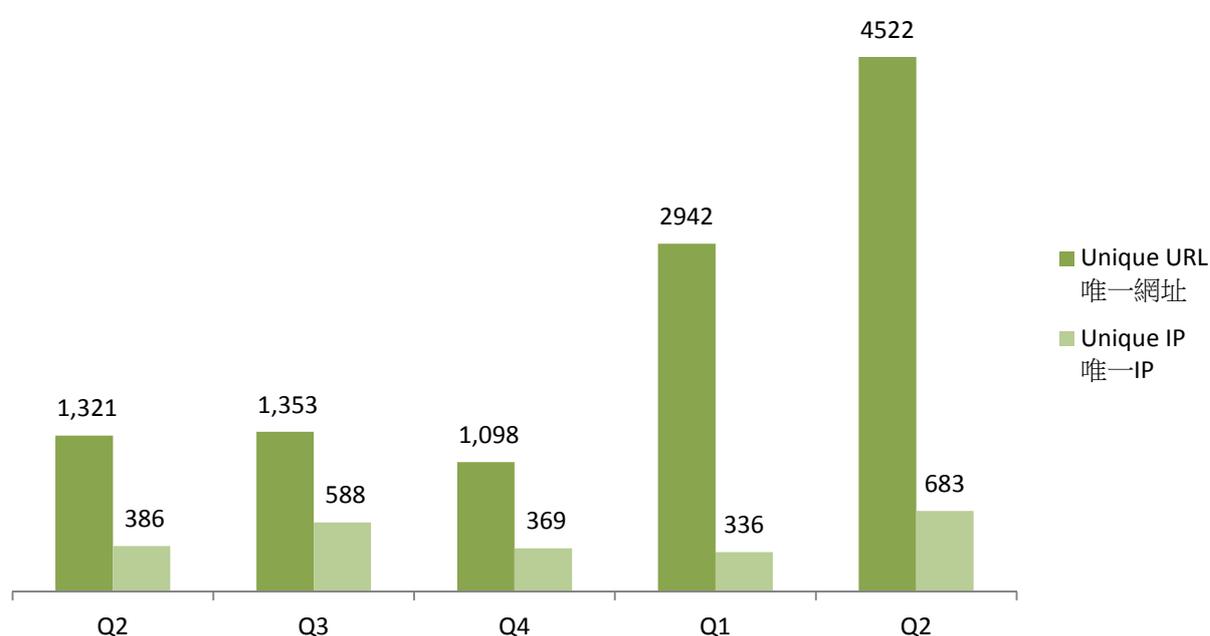


Figure 6 –Trend of Defacement security events¹⁰



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.

¹⁰ The numbers were adjusted to exclude the unconfirmed defacement events

URL/IP ratio of Defacement security events

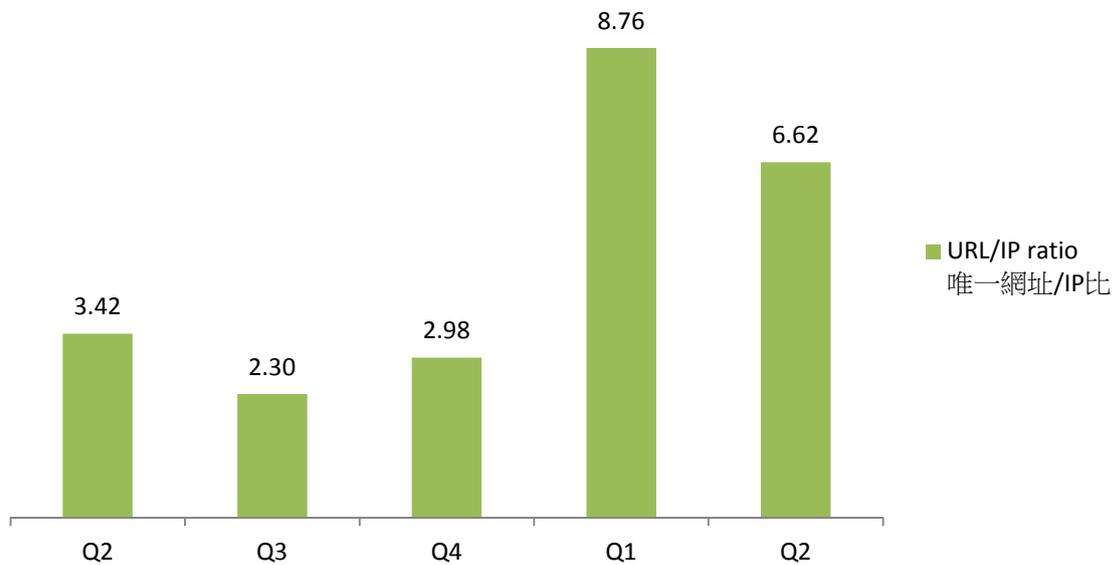


Figure 7 - URL/IP ratio of defacement security events



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

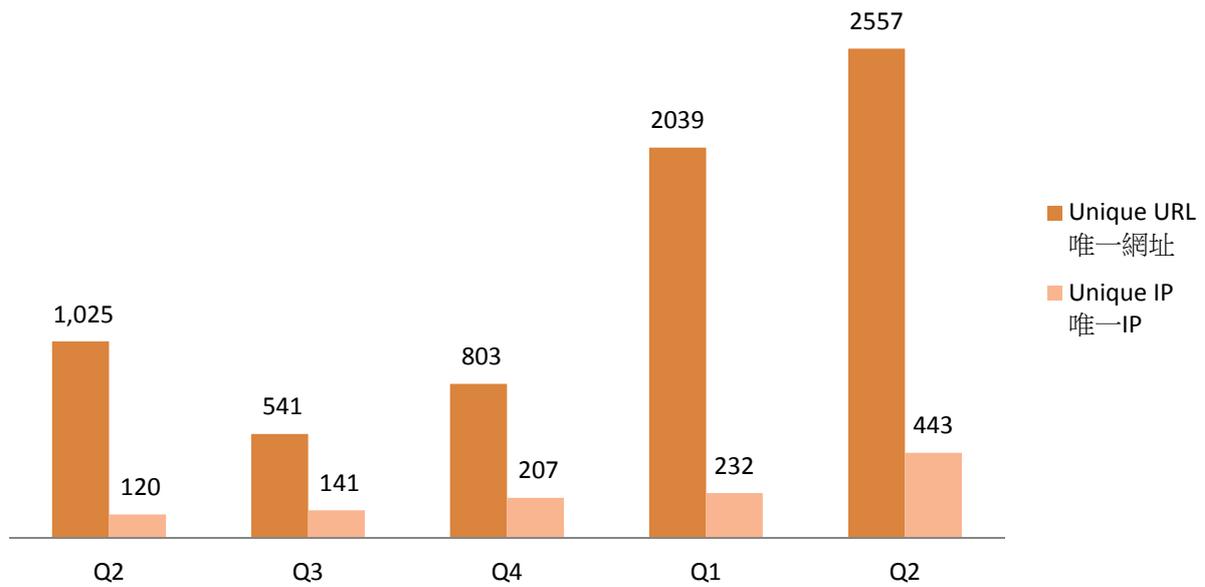


Figure 8 –Trend of Phishing Security Events



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.

URL/IP ratio of Phishing Security Events

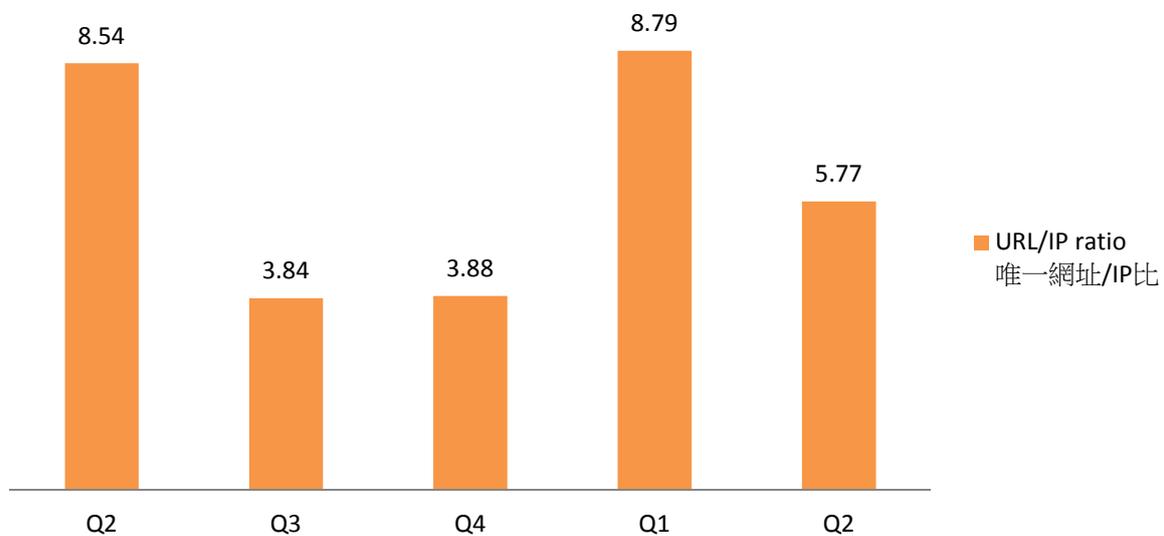


Figure 9 - URL/IP ratio of phishing security events



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

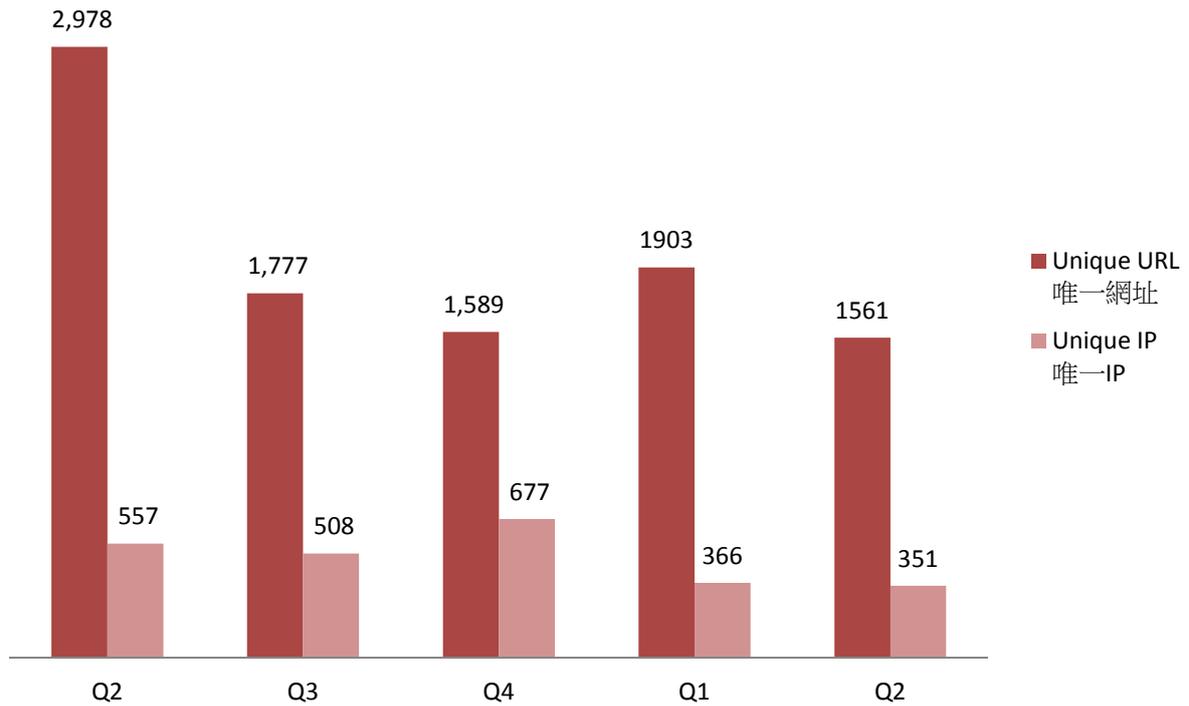


Figure 10 –Trend of Malware Hosting Security Events



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

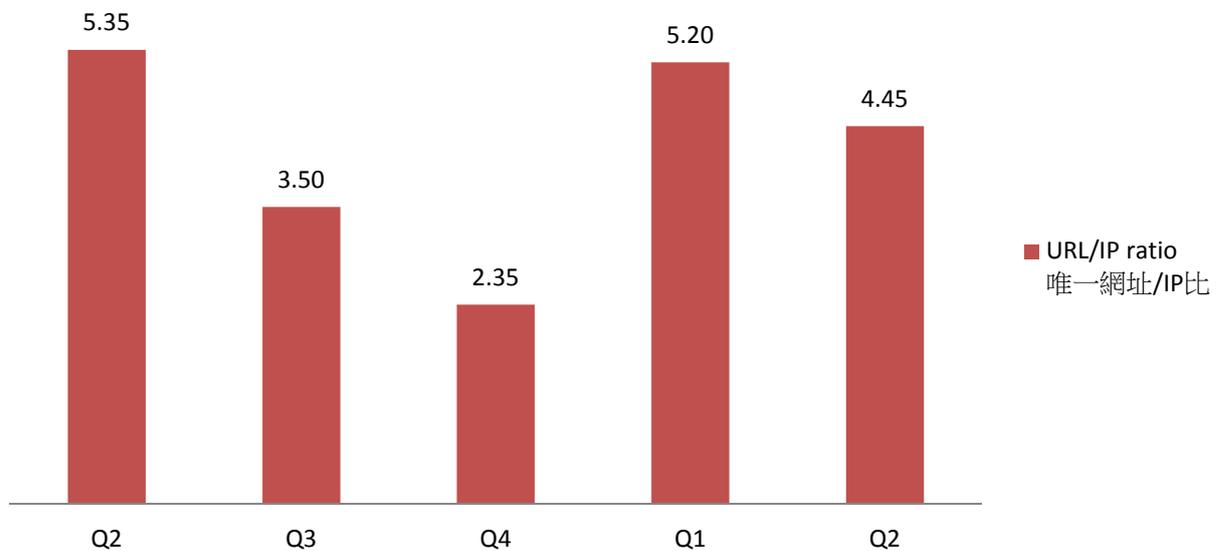


Figure 11 - URL/IP ratio of malware hosting security events



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

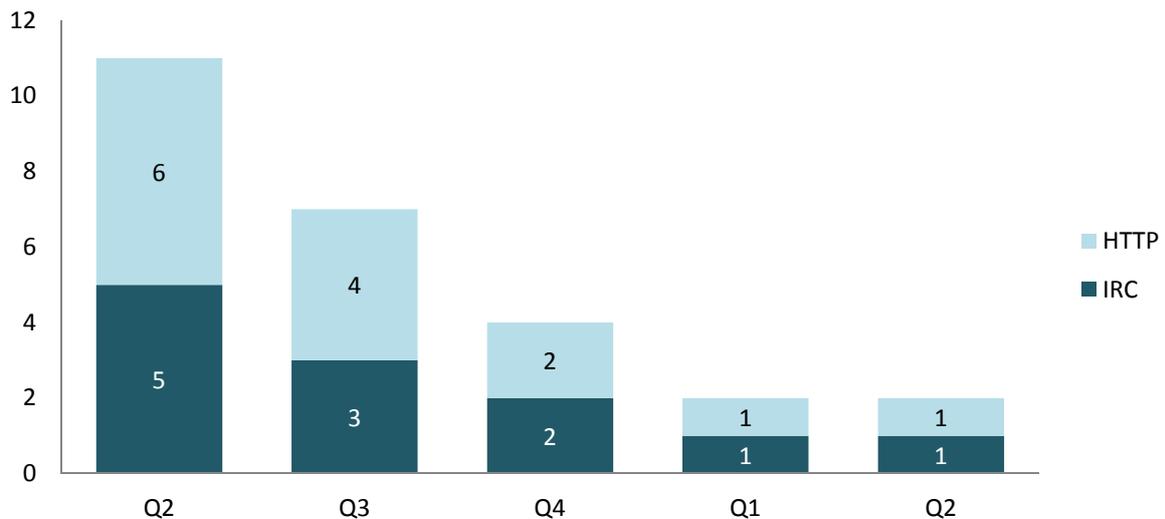


Figure 12 –Trend and Distribution of Botnet (C&Cs) security events



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:

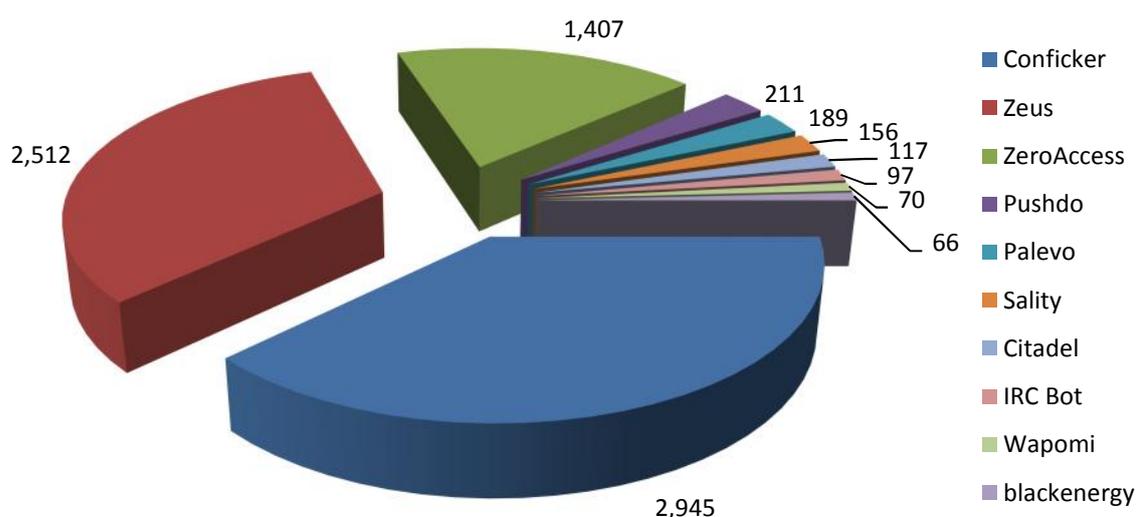
- Zeus Tracker
- SpyEye Tracker
- Palevo Tracker
- Shadowserver – C&Cs

4.2 Botnets – Bots

4.2.1 Major Botnet Families¹¹ 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	2,945	1%
2	↑	Zeus	2,512	58%
3	↓	ZeroAccess	1,407	-26%
4	-	Pushdo	211	-69%
5	NEW	Palevo	189	NA
6	-	Sality	156	15%
7	↓	Citadel	117	-30%
8	↓	IRC Bot	97	-11%
9	↑	Wapomi	70	30%
10	↓	blackenergy	66	-6%

Figure 13 –Major Botnet Families in Hong Kong Networks

¹¹ 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

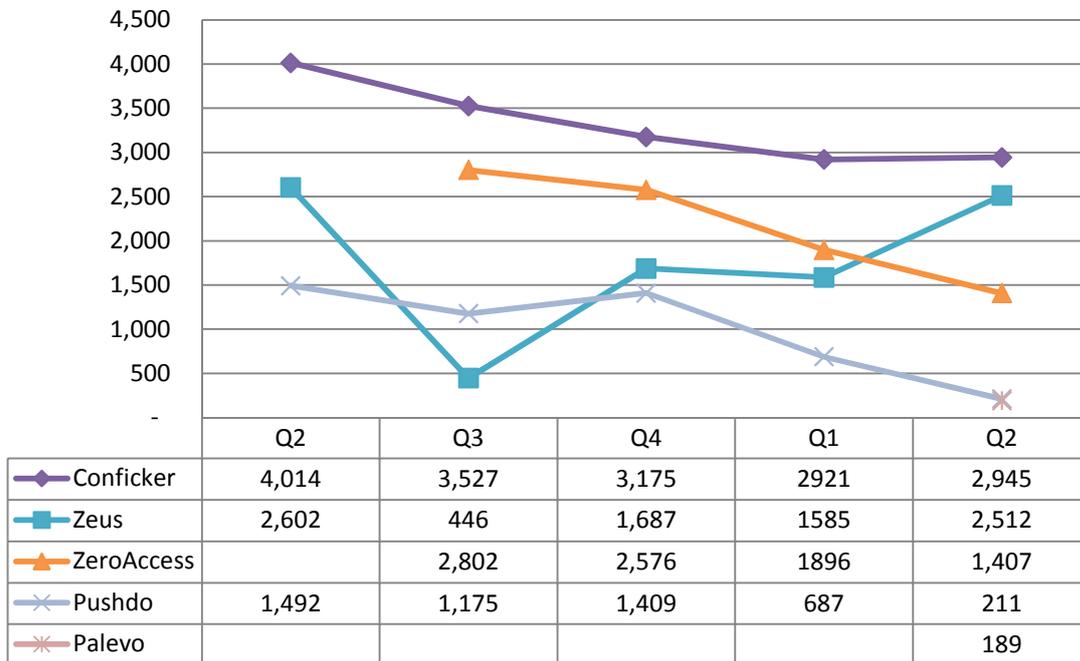


Figure 14 – Trend of Top 3 Botnet Families in Hong Kong Network

Note:

Information provided from sources for ZeroAccess became stable since Q3 2013; hence, it cannot be compared 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
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 and harvest user's passwords, credit card information and other sensitive financial data
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 	<ul style="list-style-type: none"> • 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
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
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 Spyeye) • launch DDoS attacks • send spams
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
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
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
------	--	----------------	--	--