Hong Kong Security Watch Report

2017 Q1

Foreword

Better Security Decision with Situational Awareness

Nowadays, a lot of "invisible" compromised systems (computers and other devices) are controlled by attackers with the owner being unaware. The data on these systems may be mined and exposed every day, and the systems 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 systems 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 systems 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".

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.

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.

Table 1: Types of Attack

Type of Attack	Metric used
Defacement, Phishing, Malware Hosting	security events on unique URLs within the reporting period
Botnet (C&Cs)	security events on unique IP addresses within the reporting period
Botnet (Bots)	maximum daily count of security events on unique IP addresses within the reporting period

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

Contents

---

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

Highlight of Report

This report is for 2017 Q1.

In 2017 Q1, there were 15,365 unique security events related to Hong Kong used for analysis in this report. The information is collected with IFAS[2] from 19 sources of information.[3] They are not from the incidents reports received by HKCERT.
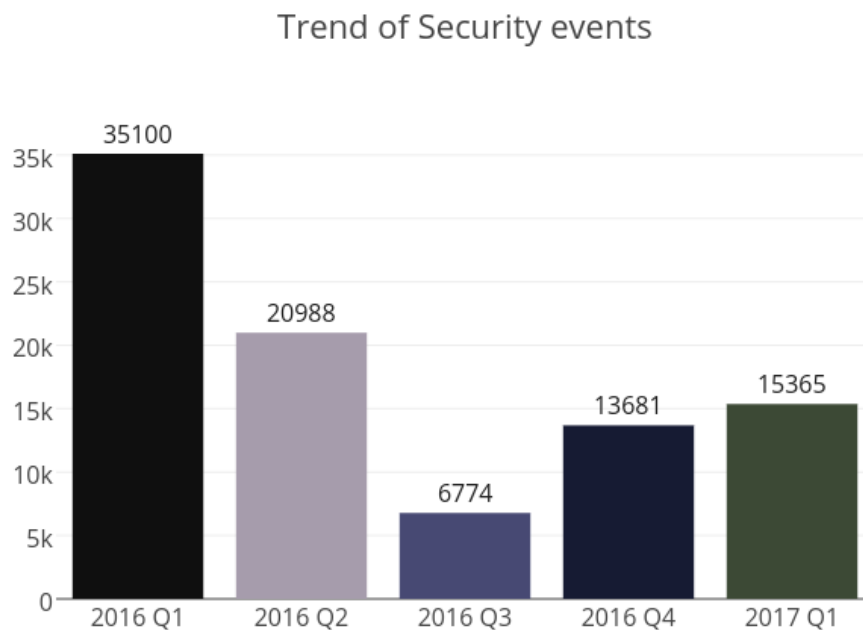

Figure 1: Trend of security events

The total number of security events in 2017 Q1 increased by 12% or 1,684 events. The increase was mainly due to botnet events.

Server related security events

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

---

[2]IFAS - Information Feed Analysis System is a HKCERT developed system that collects global security intelligence relating to Hong Kong to provide a picture of the security status.

[3]Refer to Appendix 1 for the sources of information

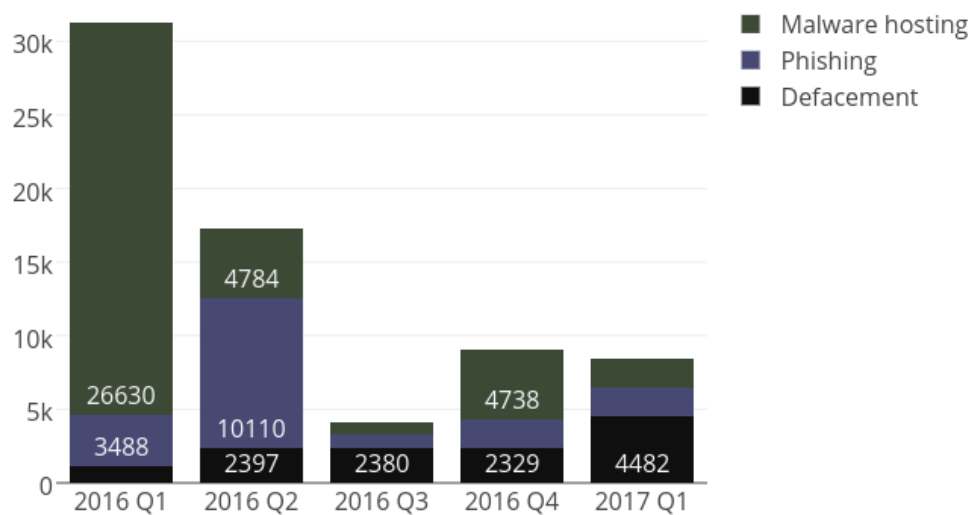Trend and Distribution of server related security events

Figure 2: Trend and distribution of server related security events

The number of server related security events decreased by 6% in Q1 2017. Phishing events and malware hosting events decreased by 5% and 59% respectively. However, the number of defacement events almost doubled.

2761 or 62% of all defacement events were from a single IP address. Most, if not all, affected domains would redirect users to an online gambling site.

According to the data from Zone-H, the server were compromised multiple times, by over 10 attack vectors, and over 20 attackers. It reflected that the server was maintained badly. Most of the attack vectors were very common, such as "known vulnerability", "SQL Injection" and "brute force attack".

"Known vulnerability" means the vulnerabilities that were already patched. This kind of vulnerability can be easily fixed by applying security patches. However, it is still one of the most common server vulnerabilities. HKCERT cannot emphasize more on the importance of patching. It is one of the most effective way of preventing intrusions.

"SQL Injection" is another common vulnerability. Attackers attempt to compromise the database by injecting SQL commands to various website inputs. To protect servers from SQL injections, administrators need to ensure all user inputs were filtered or properly handled before applying to the databases.

"Brute force attack" means guessing passwords or keys through a exhaustive search. Though the defacement report didn't show what is the attack target, we found from a vulnerable system report that the server's remote desktop (RDP) interface was open to the internet. It is possible that the attacker tried to login to the server through brute forcing the user accounts. To prevent brute force attack, strong passwords should be used in all user accounts, especially those with administrative rights. Moreover, administrators should not expose RDP and other services to the internet, unless necessary.

⚠️
- 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, administrative control interface
- do not expose unnecessary services to the internet

Botnet related security events

Botnet related security events can be classified into two categories:

- Botnet Command and Control Centers (C&C) security events - involving small number of powerful computers, mostly servers, which give commands to bots

- Botnet security events - involving large number of computers, mostly home computers which receive commands from C&Cs.

<u>Botnet Command and Control Servers</u>

The trend of botnet C&C security events is summarized below: The number of botnet Command and Control
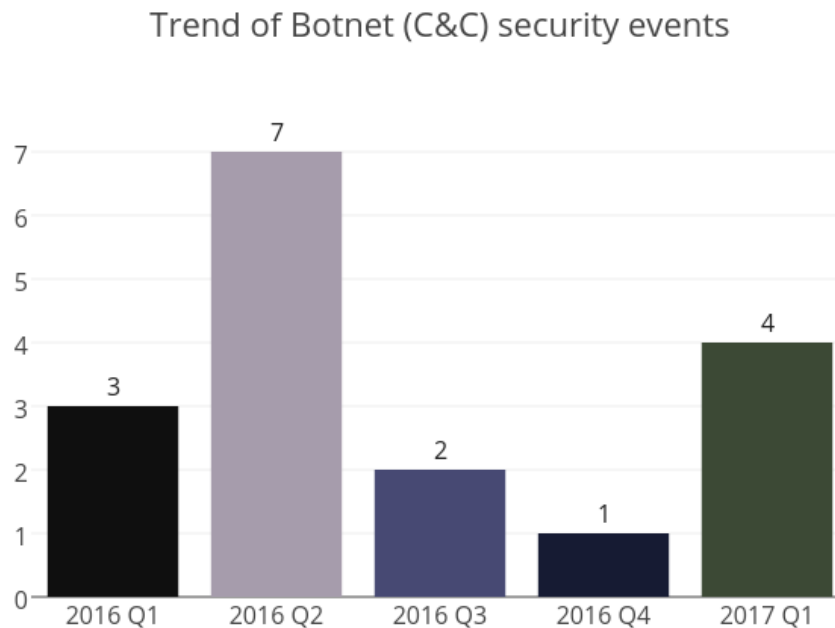

Figure 3: Trend of Botnet (C&Cs) security events

Servers incresaed this quarter. There were 4 C&C servers reported in this quarter. All were identified as IRC bot C&C servers.

<u>Botnet Bots</u>

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

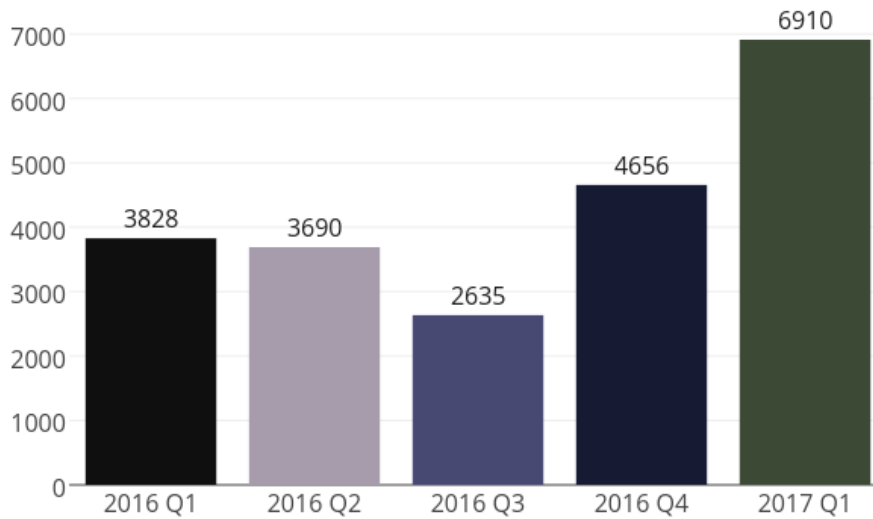## Trend of Botnet (Bots) security events

Figure 4: Trend of Botnet (Bots) security events

Number of Botnet (bots) on Hong Kong network significantly increased by 48% in this quarter. The number of Conficker events increased the most by 118.5%, and the Murofet botnet appeared in Hong Kong network for the first time. (Figure 12).

The number of Conficker event got a sudden increase in early March. It kept at a high level for about two weeks and then started to decrease. As of the time of writing, the number of events has resumed to the level of previous quarters. We can not yet found the reason of the sudden increase. We will keep monitoring the number of Conficker closely.

Murofet is a variant of Zeus first found in mid 2010. [4] It is a downloader that, once infected, would install other malwares from a pseudo-random generated domain name. [5] Similar to Conflicker, it uses domain generation algorithms (DGA) technique to avoid being shutdown.

DGA are algorithms that generate a large number of domain names every day. The malware would try to resolve those domain names in order to contact the C&C server. However, only a few of them can be resolved to the real IP address of the C&C server. To cut the communication of the malware to the C&C servers, law enforcement would need to preregister a large numbers of domain names every day, which is highly inefficient. Effectively, it is not possible to take down the C&C server by taking over its domain names.

Murofet spreads by exploit kits and infected files.

---

[4]`https://www.damballa.com/looking-back-at-murofet-a-zeusbot-variants-active-history/`
[5]`https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/W32~Murofet-A/`
`detailed-analysis.aspx`

- patch their computers
- install a working copy of the 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 Avalanche, XCode Ghost, Pushdo, Citadel, Mumblehard, Ramnit, 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
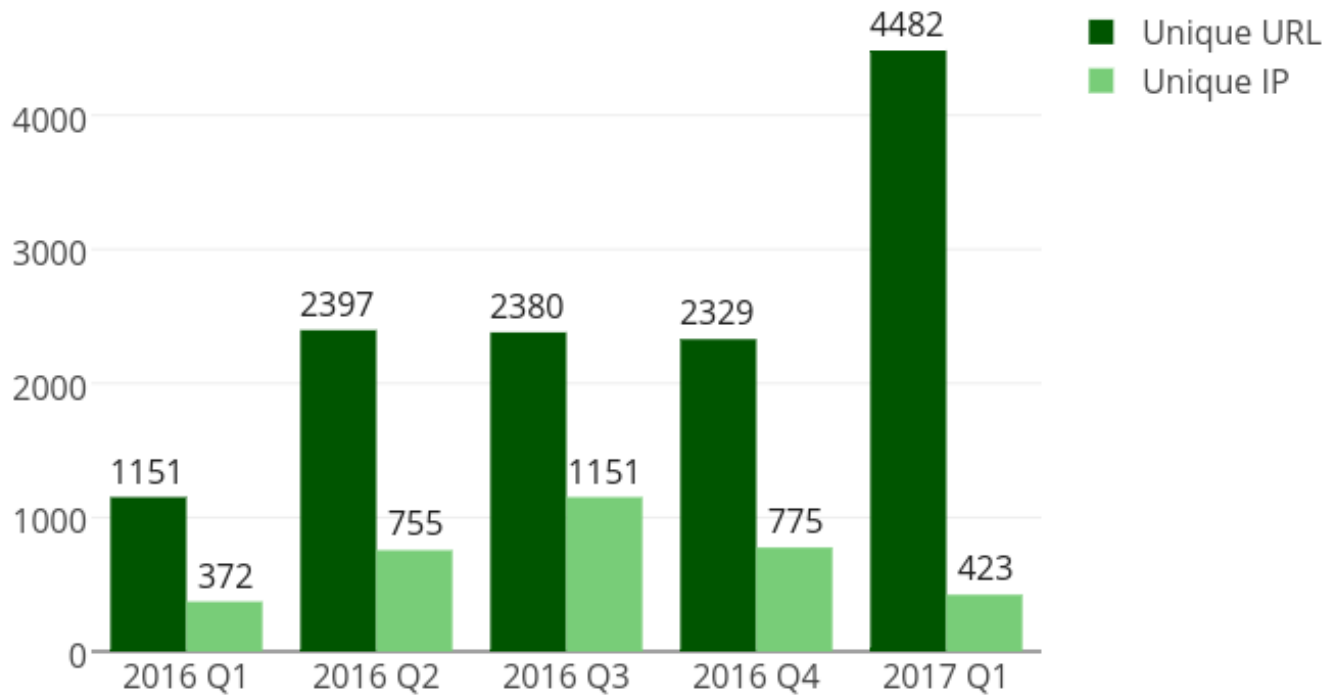
Report Details

1   Defacement

1.1   Summary

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 hack to performed other attacks.

URL/IP ratio of Defacement security events
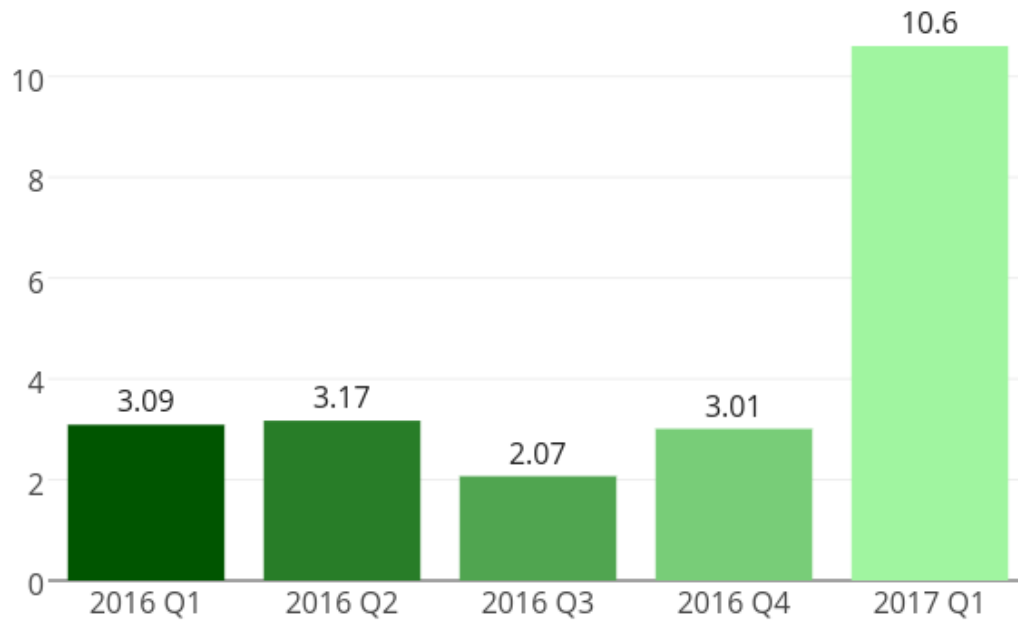
Figure 6: URL/IP ratio of defacement security events

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 be better related to the number of compromised servers
- The higher the ratio is, the more mass compromise happened

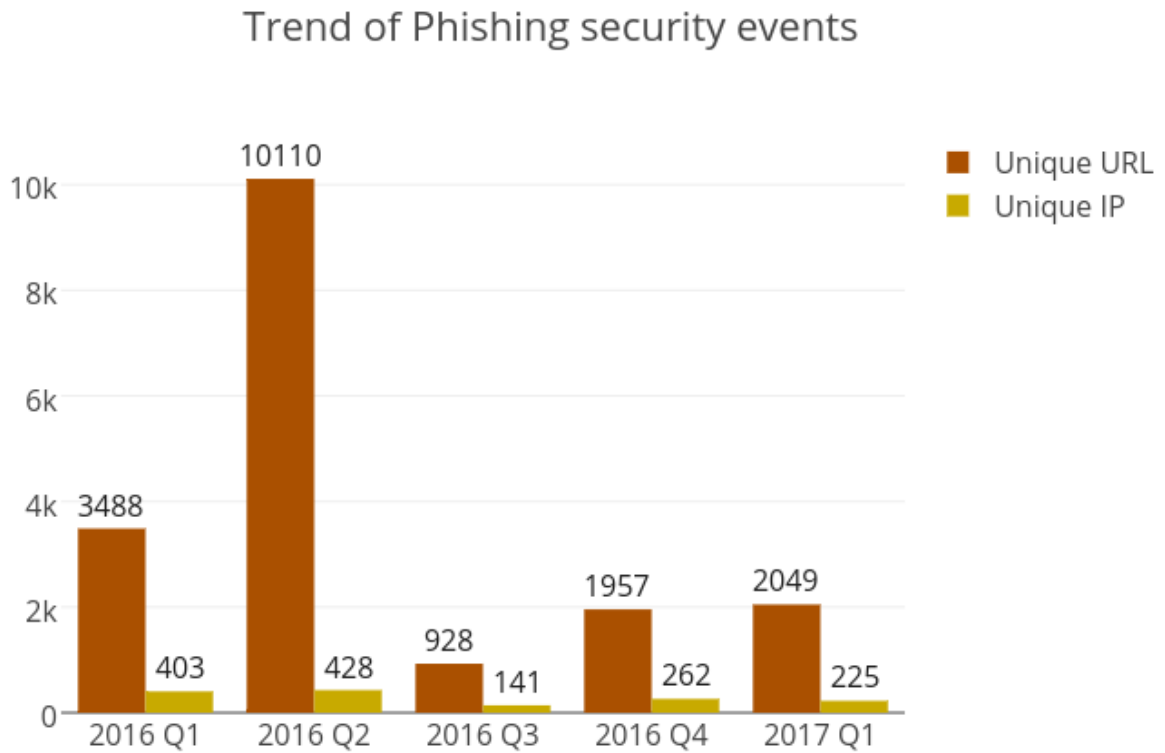Sources of Information:

- Zone-H

2 Phishing

2.1 Summary

Trend of Phishing security events

Figure 7: Trend of Defacement security events

What is Phishing?

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

What are the potential impacts?

- 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
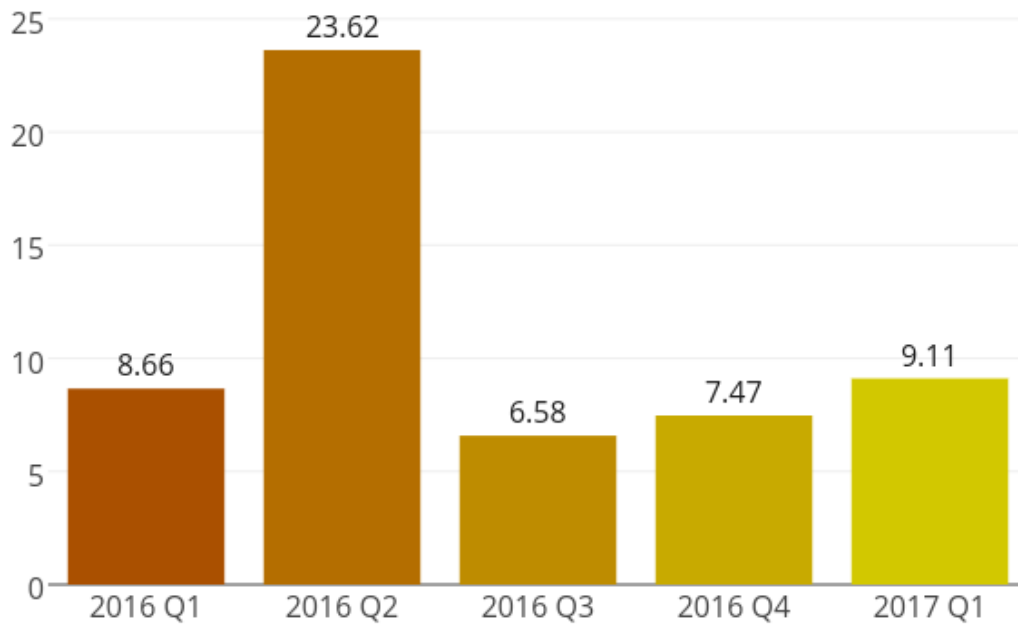
URL/IP ratio of Phishing security events

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 be 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
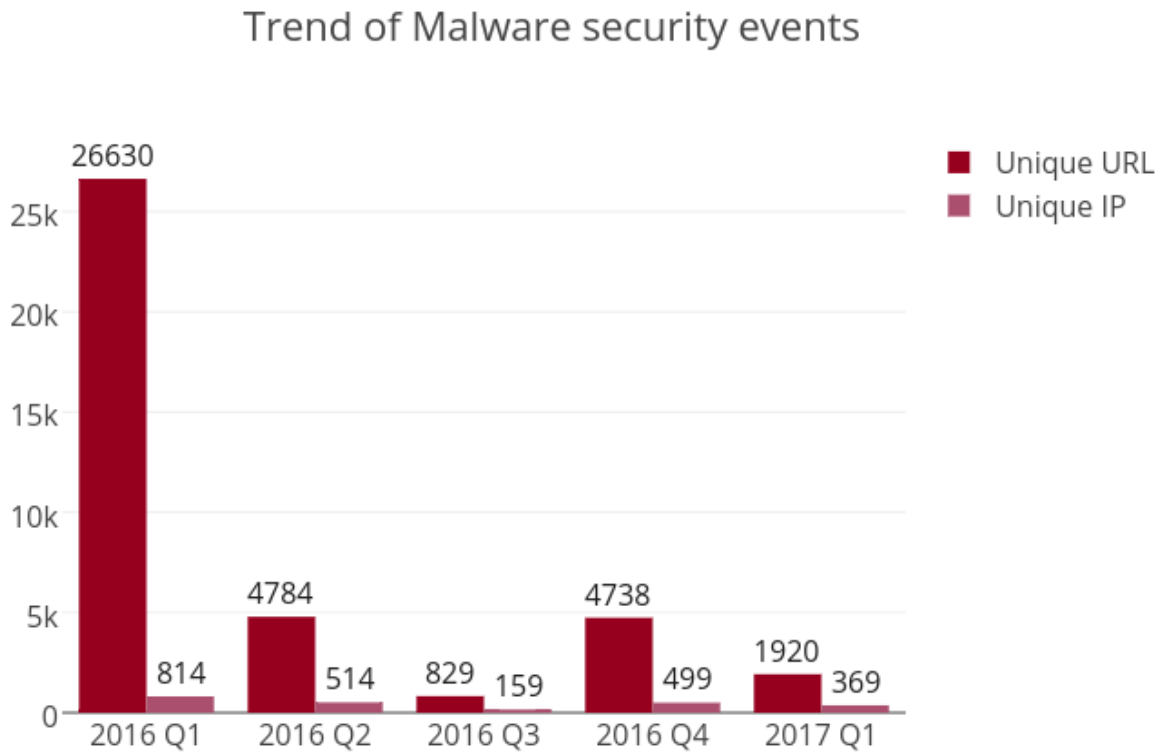- Millersmiles
- Phishtank

3 Malware Hosting

3.1 Summary

Figure 9: Trend of Malware Hosting security events

What is Malware Hosting?

- Malware Hosting is the dispatching of malware on a website

What are the potential impacts?

- 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 tbe damaged
- Server might be further compromised to perform other criminal activities
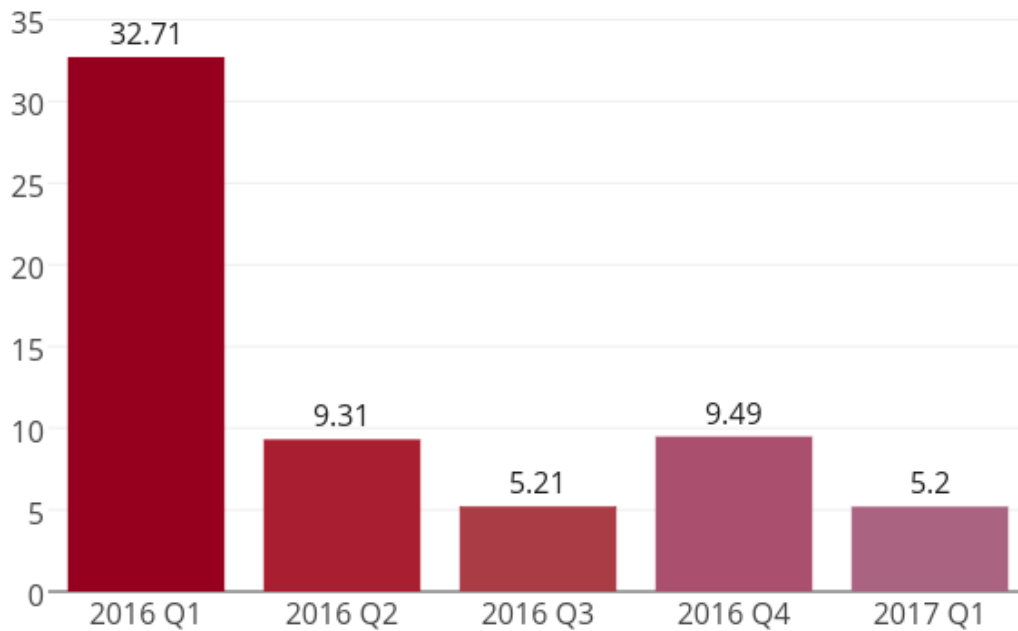
URL/IP ratio of Malware security events

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 be 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

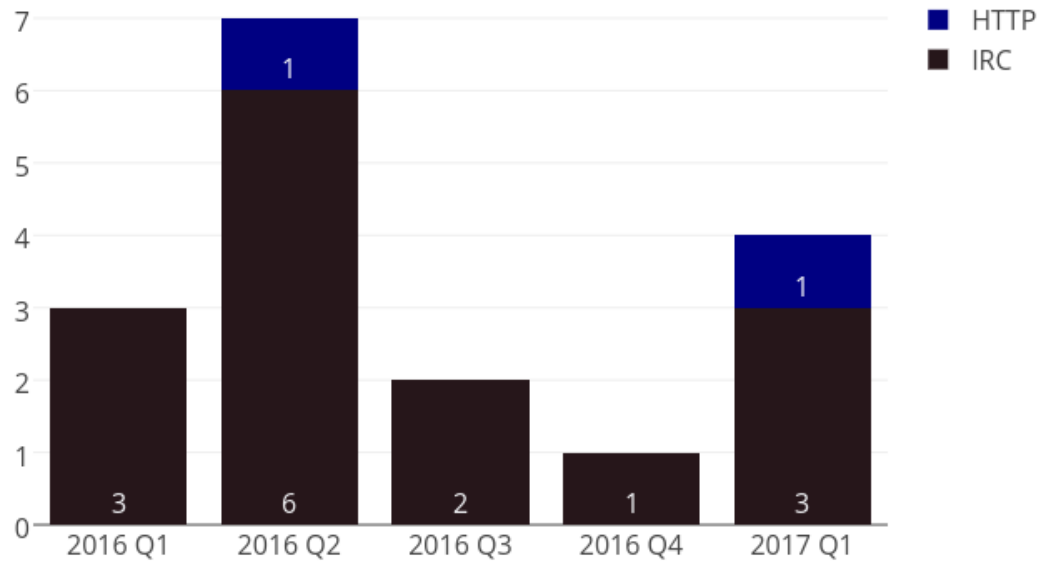## Trend and Distribution of Botnet (C&Cs) security events

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

---

What is a Botnet Command & Control Center?

- A Botnet Command & Control Center 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 financial information or launching DDoS attacks

What are the potential impacts?

- 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[6]

Individual botnet's size is calculated from the maximum of the daily counts of unique IP address 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 the same day.
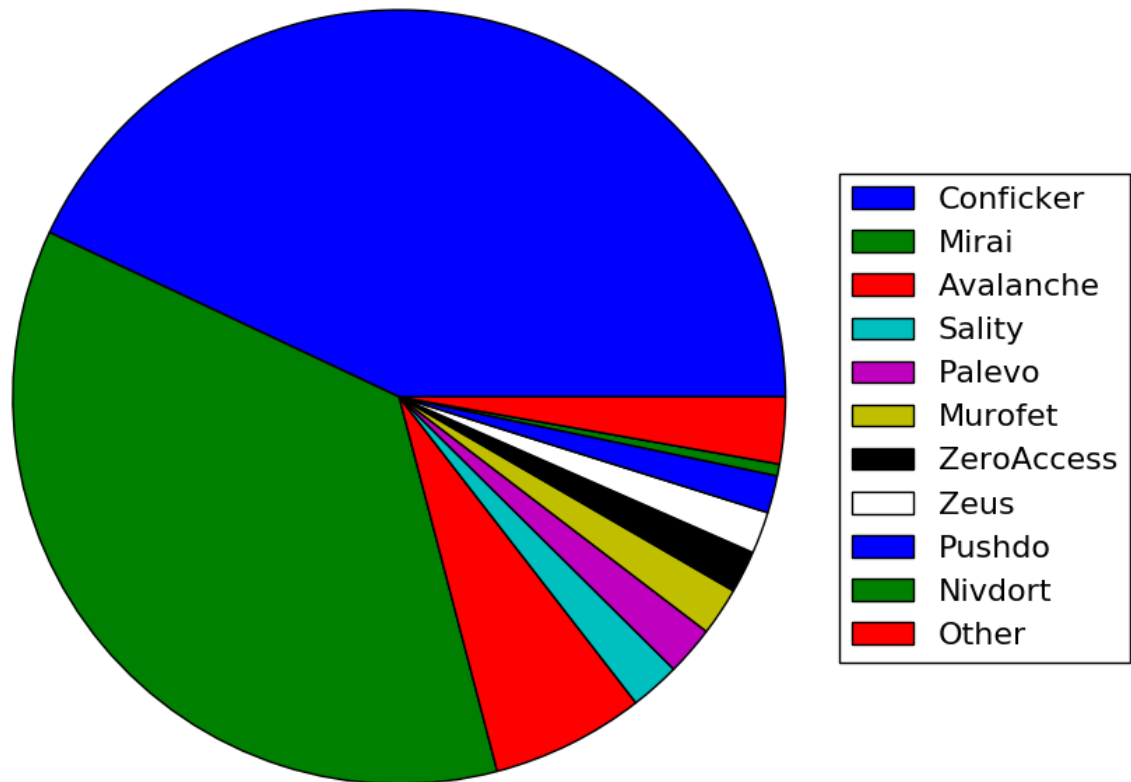

Figure 12: Major Botnet Families in Hong Kong Networks

Table 2: Major Botnet Families in Hong Kong Networks

Rank	⇑⇓	Concerned Bots	Number of Unique IP addresses	Changes with previous period
1	⇑	Conficker	2972	118.5%
2	⇓	Mirai	2493	29.0%
3	→	Avalanche	443	18.4%
4	⇑	Sality	144	-4.0%
5	⇑	Palevo	142	34.0%
6	NEW	Murofet	139	NA
7	⇓	ZeroAccess	122	-20.3%
8	⇓	Zeus	121	-45.0%
9	⇓	Pushdo	108	-21.7%
10	⇓	Nivdort	34	-24.4%

---

[6]Major Botnet Families are selected botnet families with considerable amount of security events reported from the information sources across the reporting period.
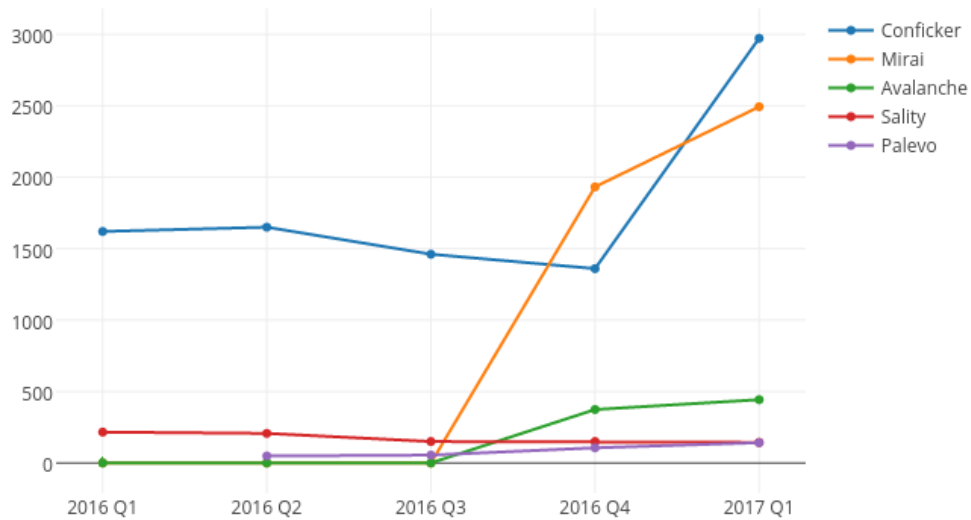
Figure 13: Trend of Top 5 Botnet Families in Hong Kong Network

Name	2016 Q1	2016 Q2	2016 Q3	2016 Q4	2017 Q1
Conficker	1620	1650	1461	1360	2972
Mirai	0	0	0	1932	2493
Avalanche	0	0	0	374	443
Sality	216	207	150	150	144
Palevo	0	49	55	106	142

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 hides itself, and stealthily connects to the Command & Control Server to get instructions from hackers.

What are the potential impacts?

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

Sources of Information:

- ArborNetwork - Atlas SRF - conficker

- ShadowServer - botnet_drone

- ShadowServer - sinkhole_http_drone

- Shadowserver - Microsoft_sinkhole

18

Appendix

A   Sources of information in IFAS

The following information feeds are information sources of IFAS:

Table 3: IFAS Sources of Information

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

B   Geolocation identification methods in IFAS

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

Table 4: Methods of Geolocation Identification

Method	First introduced	Last update
Maxmind	2013-04	2017-1-14

C Major Botnet Families

Table 5: Botnet Families

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Avalanche	Nil	Crimeware-as-a-service	Depends on underlying malwares	• send spams • host phishing sites • host malware • steal sensitive information
Bamital	Nil	Trojan	• drive-by download via exploit kit • via P2P network	• Click fraud • Search hijacking
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
Bedep	Nil	Trojan	• via adult web sites • malvertising	• Click fraud • download other malwares
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

Table 6: Botnet Families (cont.)

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Corebot	Nil	Banking Trojan	• via droppers	• steal sensitive information • install other malware • backdoor capabilities that allow unauthorized access
Dyre	Nil	Banking Trojan	• spam e-mail	• steal banking credential by tricking the victim to call an illegitimate number • send spams
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
Mirai	Nil	Worm	• telnet with vendor default credentials	• launch DDoS attacks
Murofet	Nil	Trojan	• file infection • via exploit kits	• download other malware
Nivdort	Nil	Trojan	• spam e-mail	• steal login credentials and sensitive information
Nymaim	Nil	Trojan	• spam e-mail • malicious link	• lock infected systems • stop victims from accessing files • ask for ransom
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

Table 7: Botnet Families (cont.)

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
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
Ramnit	Nil	Worm	• file infection • via exploit kits • public FTP servers	• backdoor capabilities that allow unauthorized access • steal login credentials and sensitive information
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
Tinba	• TinyBanker • Zusy	Banking Trojan	• via exploit kit • Spam e-mail	• steal banking credential and sensitive information
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

Table 8: Botnet Families (cont.)

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
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