Hong Kong Security Watch Report

2017 Q2

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 enhance 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 constantly across the reporting period.

Highlight of Report

This report is for 2017 Q2.

In 2017 Q2, there were 9042 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.

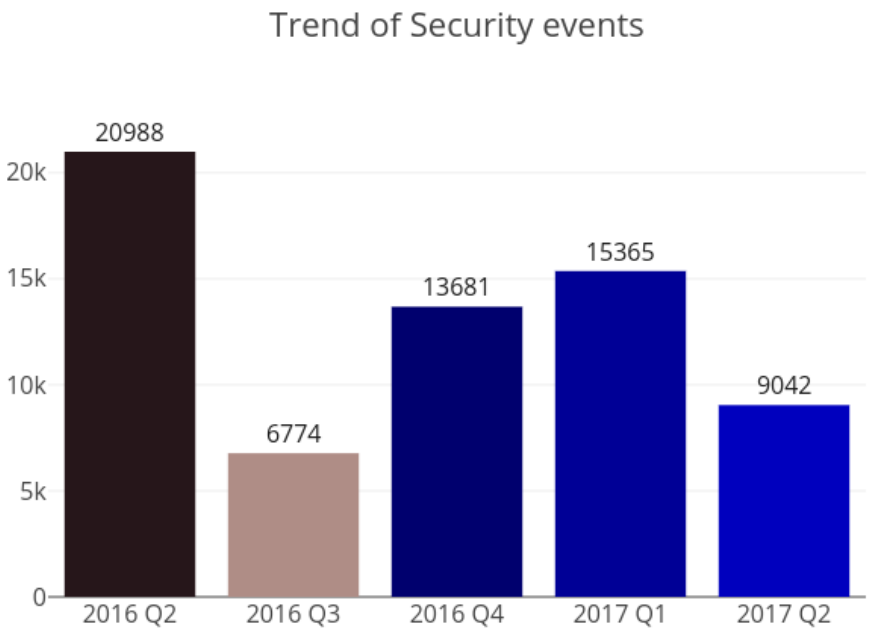

Figure 1: Trend of security events

The total number of security events in 2017 Q2 dropped by 41% or 6323 events. The decrease was due to a rather big drop in the counts of server related security events and botnet infection.

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

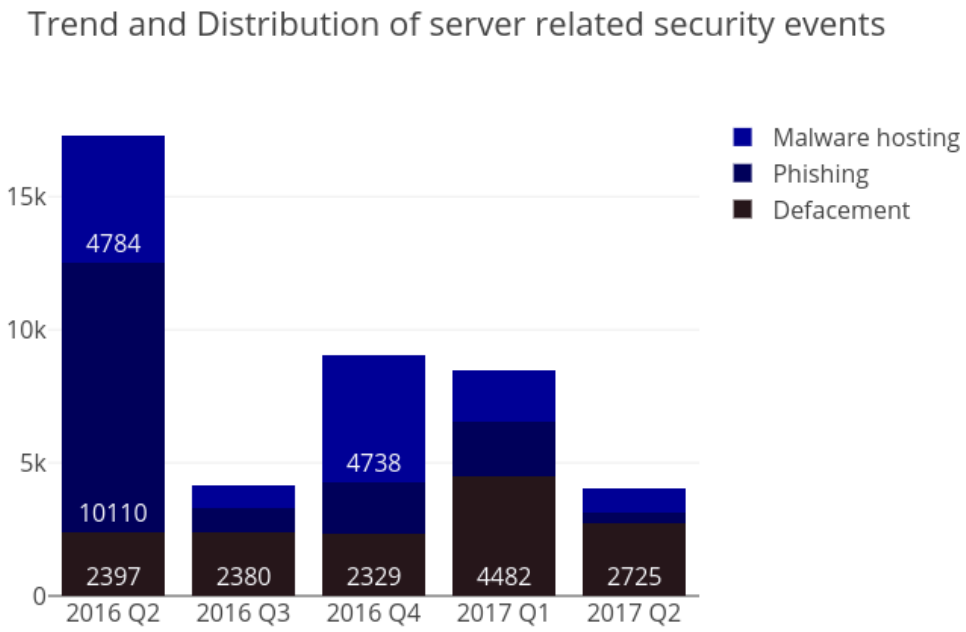

Figure 2: Trend and distribution of server related security events

The number of server related security events substantially decreased from 8,451 to 4,015 (decreased by 52%) in this quarter. The number of defacement events decreased by 39% while the number of and malware hosting events decreased by 55%. The phishing events even recorded an all-time low of 428, which was 79% lower than the previous quarter.

Given the considerable reduction in the defacement events, the relatively low URL/IP ratio, however, reflected a fact that there were actually quite many servers compromised in the reporting period (refer to P.11 Figure 6). The same applied to the phishing events (refer to P.13 Figure 8).

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, 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 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.

Botnet Command and Control Servers

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

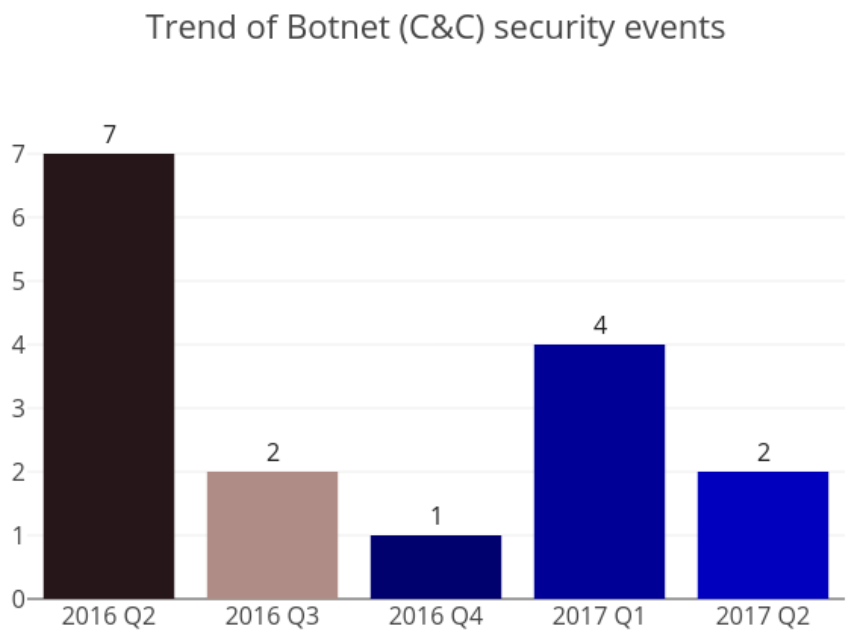

Figure 3: Trend of Botnet (C&Cs) security events

Servers dropped by half to 2 in this quarter. Both were identified as IRC bot C&C servers.

Botnet Bots

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

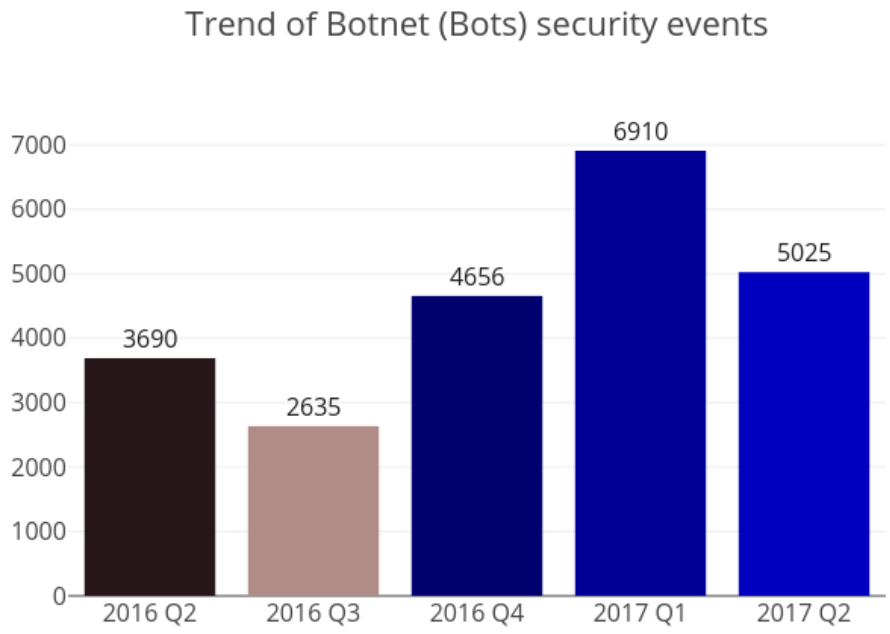

Figure 4: Trend of Botnet (Bots) security events

Number of Botnet (bots) on Hong Kong network decreased by 27% in Q2 this year.

Rank 1 was the infamous WannaCry ransomware. With a global outbreak on 12 May, it recorded a maximum connection count of 1566 unique IP addresses and a malware named Ghost Push, discovered in 2014, also made its way into HK's major botnet families in this quarter.

WannaCry

Ransomware is a type of malware which will encrypt a victim's files and demand a ransom in order to recover the files.

The 'WannaCry' variant possesses a worm's characteristic and is the first ransomware which can spread across home or office networks to infect much more devices by exploiting Microsoft Windows SMB vulnerabilities (EternalBlue and DoublePulsar). It scans for open TCP ports 139 and 445 on unpatched hosts and once detected, starts the nasty work to encrypt the files and propagate itself within the network.

Ghost Push

Ghost Push is a Android malware family discovered in 2014. Android devices get infected when a user installs a malicious app, mostly not from Google Play. Once installed, it tries to root the device and download other malicious apps. In December 2016, a mobile malware called "Gooligan"[4] which targeted Google services was exactly a variant of Ghost Push.

[4] `https://www.hkcert.org/my_url/en/blog/16120203`

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

- 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 WannaCry, 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

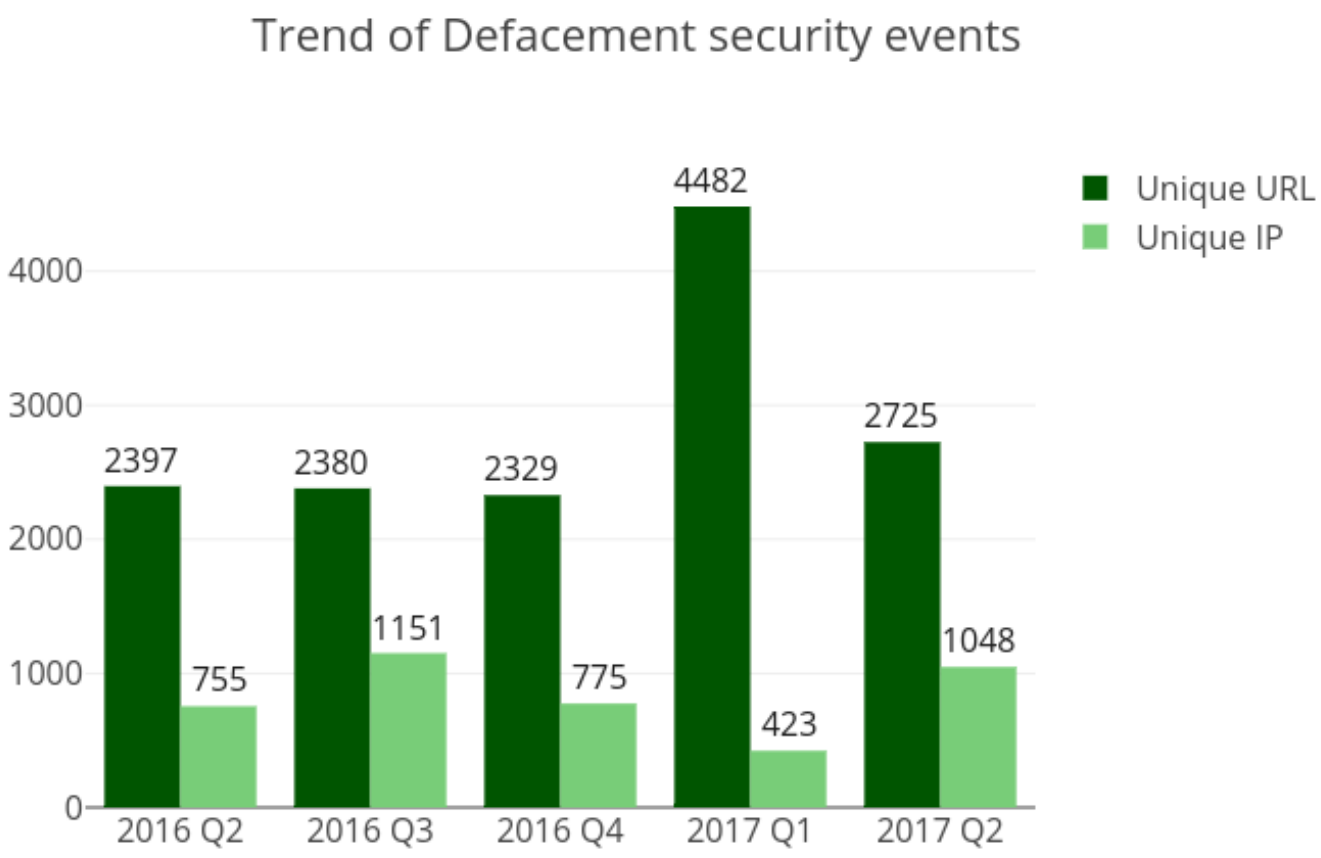

Figure 5: Trend of Defacement security events

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 mightbe further compromised by the hack to performed other attacks.

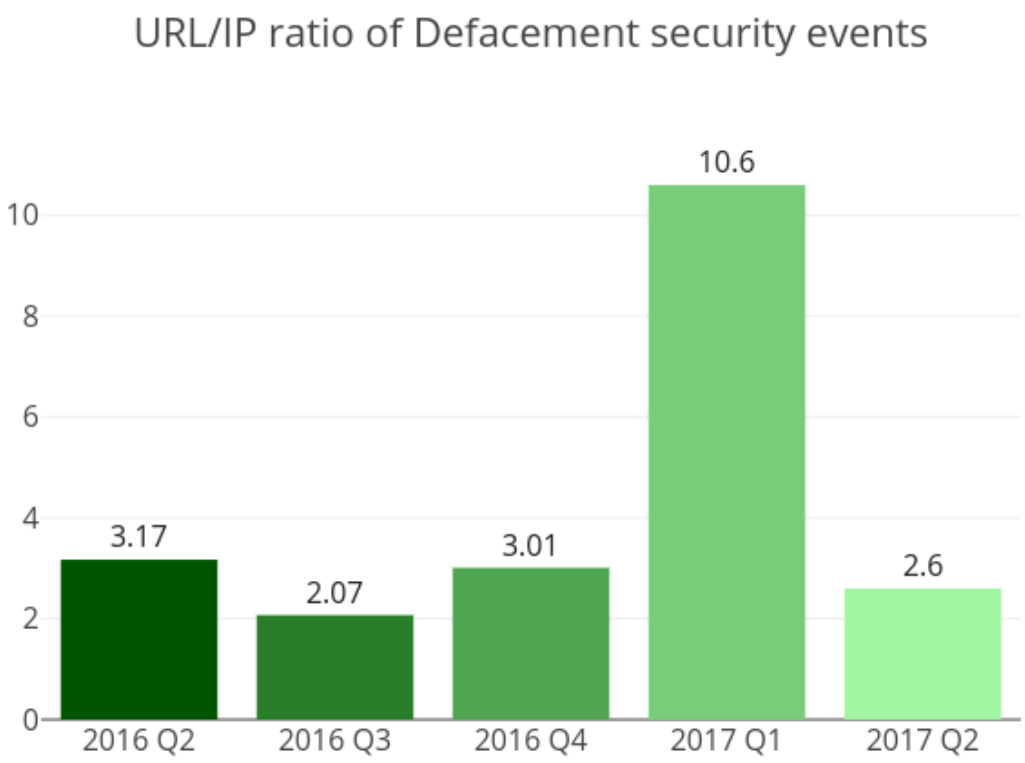

Figure 6: URL/IP ratio of defacement security events

What is URL/IP ratio?

- It is the number of security events count in unique URL divided by the number of security events coun tin 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

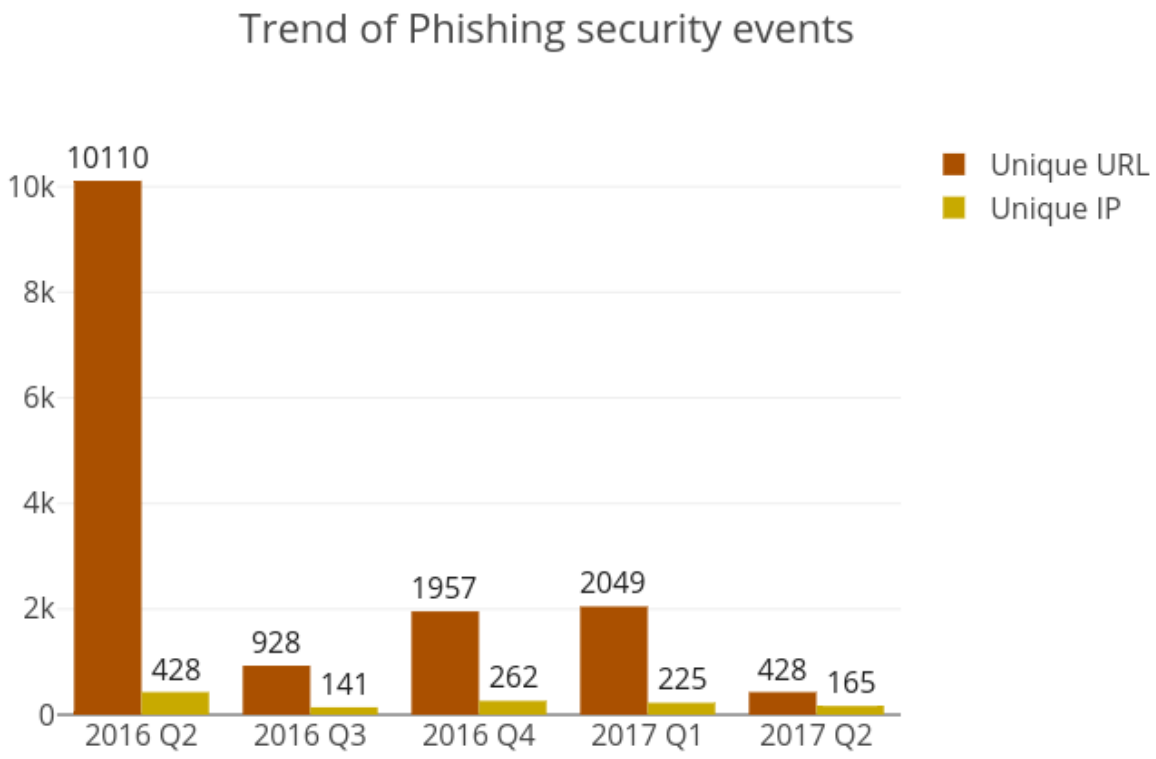

Figure 7: Trend of Defacement security events

What is Phishing?

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

What are the potential impacts?

- Personal information or accout credentials of visitors might be stolen, leading to financial loss.
- Original content might be inaccessible
- Reputation of the website owner might tbe damaged
- Server might be further compromised to perform other attacks

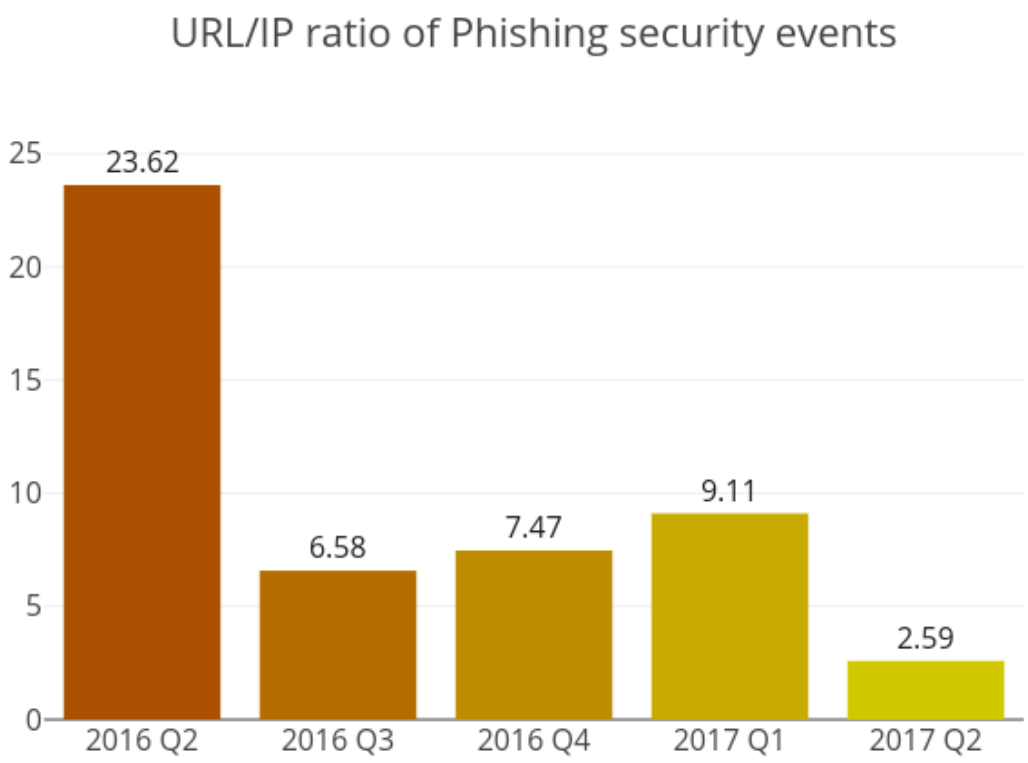

Figure 8: URL/IP ratio of Phishing security events

What is URL/IP ratio?

- It is the number of security events count in unique URL divided by the number of security events coun tin 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

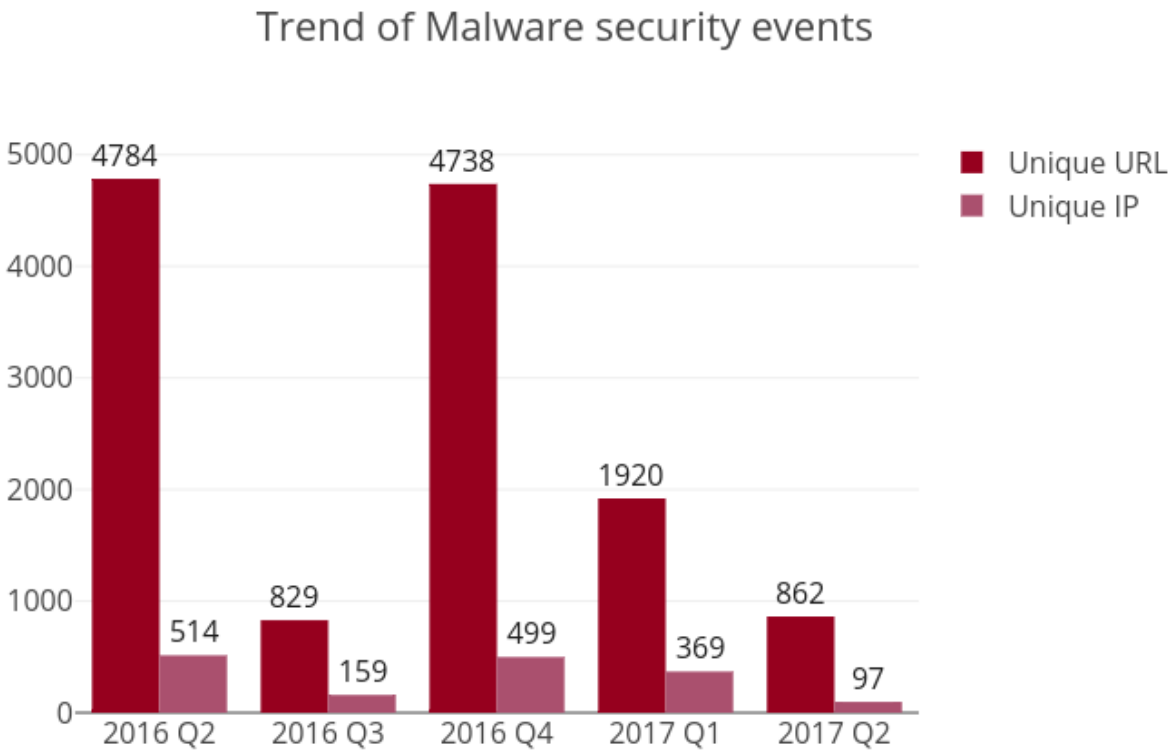

Figure 9: Trend of Malware Hosting security events

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

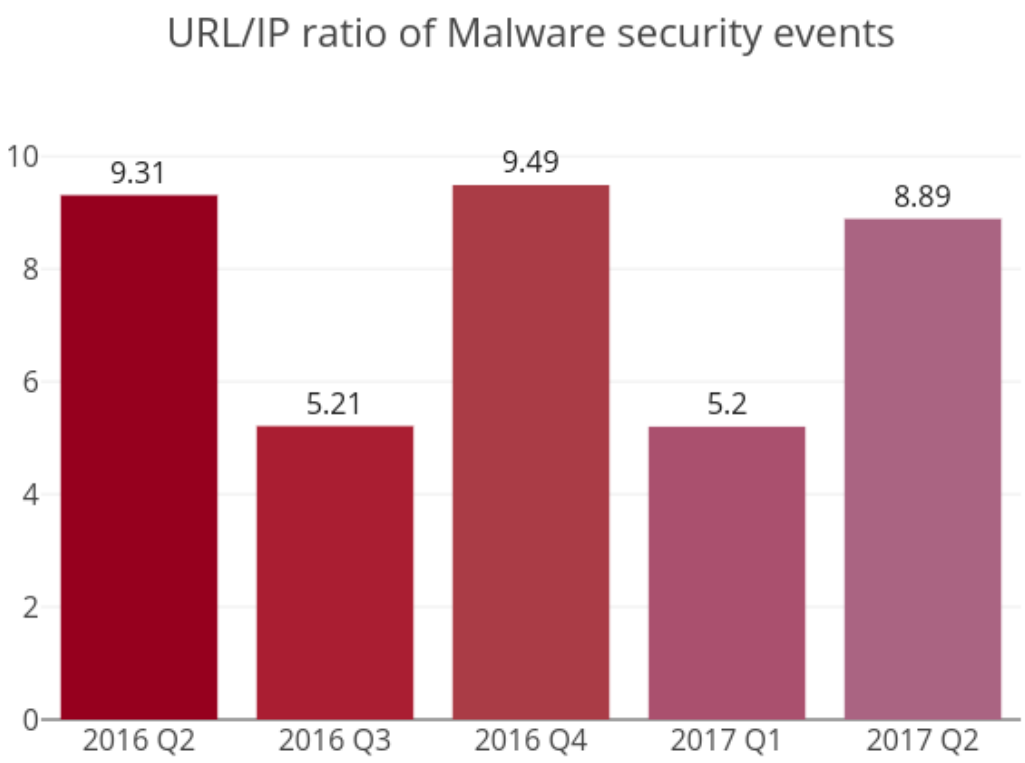

Figure 10: URL/IP ratio of Malware Hosting security events

What is URL/IP ratio?

- It is the number of security events count in unique URL divided by the number of security events coun tin 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

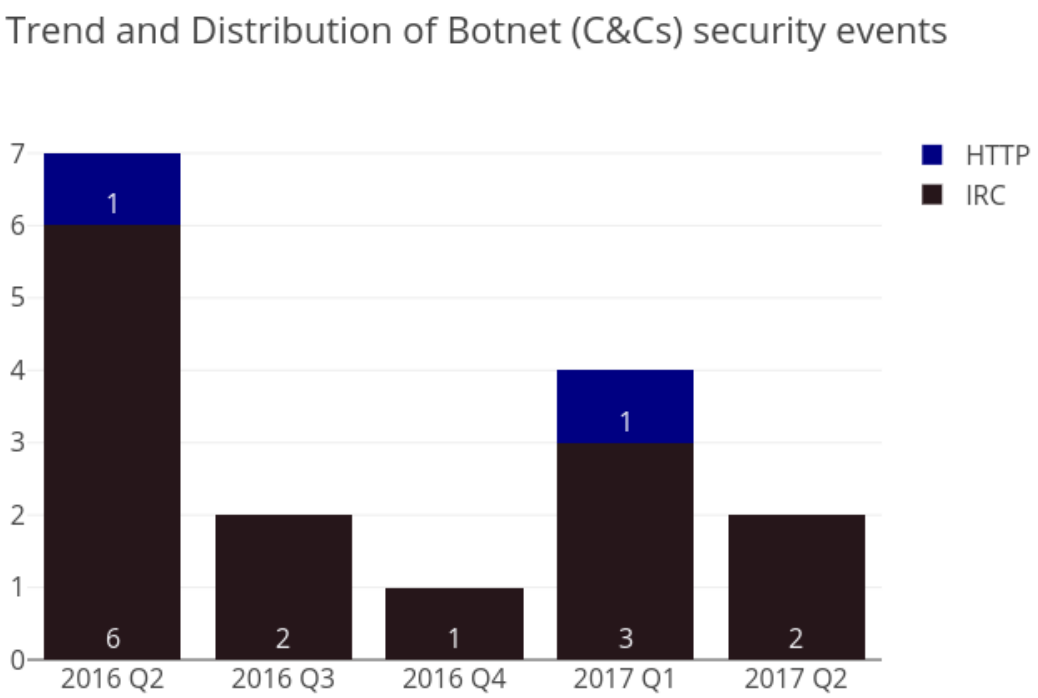

Figure 11: Trend and Distribution of Botnet (C&Cs) security events

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[5]

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.

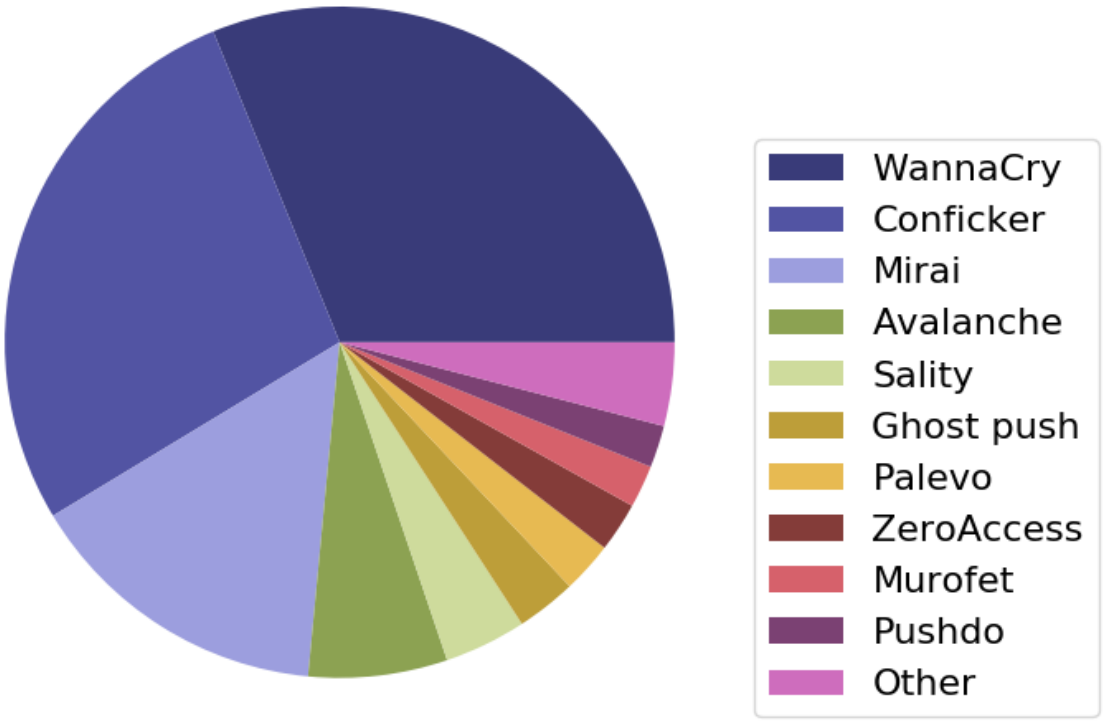

Figure 12: Major Botnet Families in Hong Kong Networks

Table 2: Major Botnet Families in Hong Kong Networks

Rank	⇑⇓	**Concerned Bots**	**Number of Unique IP addresses**	**Changes with previous period**
1	NEW	WannaCry	1566	NA
2	⇓	Conficker	1381	-53.5%
3	⇓	Mirai	746	-70.1%
4	⇓	Avalanche	337	-23.9%
5	⇓	Sality	199	38.2%
6	NEW	Ghost push	145	NA
7	⇓	Palevo	124	-12.7%
8	⇓	ZeroAccess	120	-1.6%
9	⇓	Murofet	103	-25.9%
10	⇓	Pushdo	102	-5.6%

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

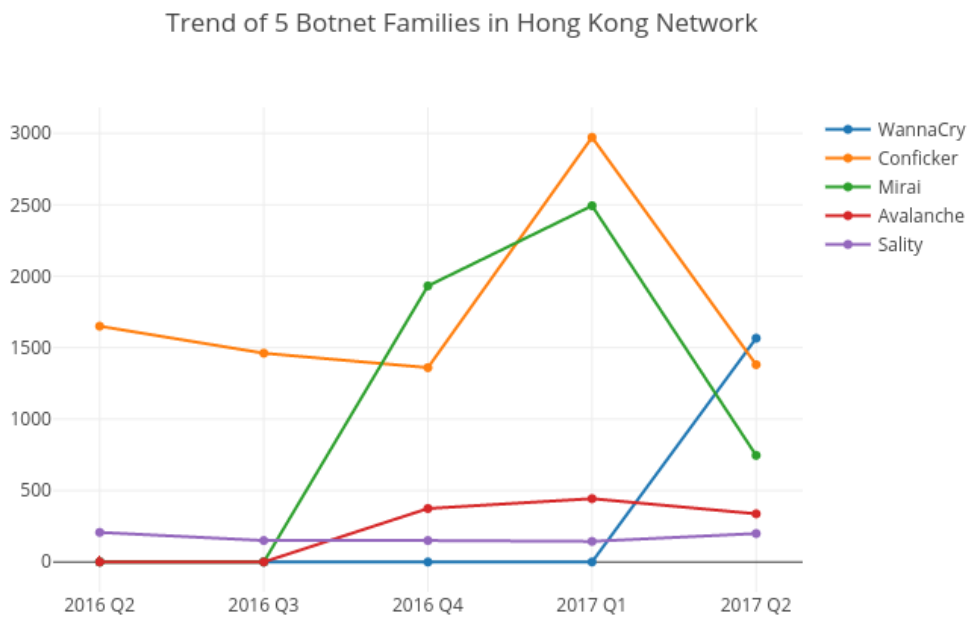

Figure 13: Trend of Top 5 Botnet Families in Hong Kong Network

Name	2016 Q2	2016 Q3	2016 Q4	2017 Q1	2017 Q2
WannaCry	0	0	0	0	1566
Conficker	1650	1461	1360	2972	1381
Mirai	0	0	1932	2493	746
Avalanche	0	0	374	443	337
Sality	207	150	150	144	199

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

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	2017-7-22

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
Ghost Push	Nil	Mobile malware	• via app installation	• gain root access • download 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
WannaCry	• WannaCrypt	Ransomware	• spread across network • exploit Windows SMB vulnerabilities	• encrypt user data • demand ransom • data unrecoverable
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