Hong Kong Security Watch Report

2019 Q2

Foreword

Better Security Decision with Situational Awareness

Nowadays, many "invisible" compromised systems (computers and other devices) are being hacked and seized control without their owners' knowledge. The data on these systems may be mined and exposed every day, and even used for various criminal activities. The Hong Kong Security Watch Report aims to raise public awareness of the problem of compromised systems in Hong Kong, enabling them to make better decision in information security.

The data in this report is about the activities of compromised systems in Hong Kong which suffer from, or have participated in various types of cyber attacks, including web defacement, phishing, malware hosting, botnet command and control centres (C&C) or bots. "Computers in Hong Kong" refer to 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 collaboration between the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and global security researchers. Many security researchers have the ability to detect attacks against their own or clients networks. Some will provide the information of IP addresses of attack source or web links of malicious activities collected to other information security organisations with an aim to collectively improve the overall security of the cyberspace. They have good practice in sanitising personal identifiable data before sharing information.

HKCERT collects and aggregates such valuable data about Hong Kong from multiple information sources for analysis with the Information Feed Analysis System (IFAS), a system developed by HKCERT. The information sources (Appendix 1) are very diverse 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.

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

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

Data collected for this report is from multiple sources with different collection periods, presentation formats and their own limitations. The numbers from the report should be used as a reference only, 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

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.

Report Highlights

In 2019 Q2, there were 62,284 unique security events related to Hong Kong used for analysis in this report. Data is not collected from the incident reports received by HKCERT, which came from IFAS[2] with 13 sources of information.[3]

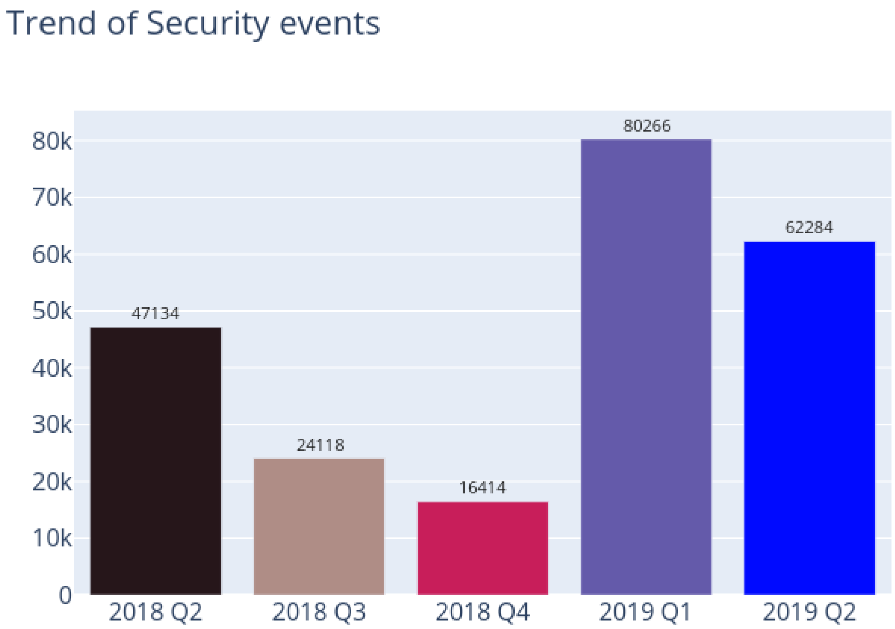

Figure 1: Trend of security events

Event Type	**2018 Q2**	**2018 Q3**	**2018 Q4**	**2019 Q1**	**2019 Q2**
Defacement	1,071	5,439	590	318	532
Phishing	34,391	319	365	289	1306
Malware Hosting	4,359	7,773	8,152	72,201	48,892
Botnet (Bots)	7,310	10,587	7,307	7,458	11,554
Botnet (C2)	3	0	0	0	0

The total number of security events in 2019 Q2 (17,982 events) fell by 22% from the previous quarter. Although there was a notable decline in malware hosting events, other events had reported ascendant trends during this quarter. The most obvious increase was phishing events, which rose over three-fold. Meanwhile, defacement and botnet events had reported growths of 67% and 55% respectively. The total number of security events has remained relatively high in the first two quarters of 2019. As such, HKCERT will notify the affected operators to check and clean up their servers in August 2019.

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

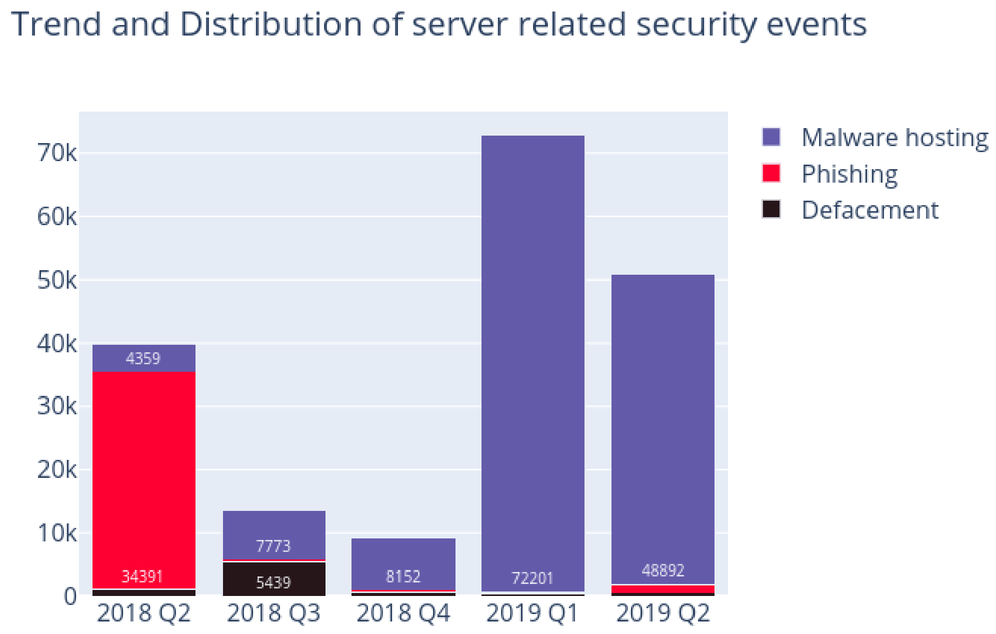

Figure 2: Trend and distribution of server related security events

From the report for 2019 Q1, we have observed the emergence of malware hosting events from March 2019. Such events continued their presence in Q2. Although the number of malware hosting events has considerably reduced from 72,201 in Q1 to 48,892 in Q2, while the URL/IP ratio of malware hosting halved to 10 (see Figure 10), the number of involved malware hosting IP addresses rose by 33%, 4,851 in total. (see Figure 9). Therefore, it stated that the actual malware hosting trends did not show signs of decline. ASN AS38197 (Sun Network) hosted the most malware hosting URL, accounting for 36% of total events. HKCERT had notified the affected operators to check and clean up their servers in April 2019. We noted that 70% involved malware hosting IP addresses in Q1 were not found in Q2.

The number of phishing events, each involving a unique phishing URL, rose over three-fold from 289 in Q1 to 1,306 in Q2. It is worth noticing that over 40% of phishing events targeted apple.com and icloud.com, by adding them as subdomain to a legitimate domain name (for instance http://www.icloud.com.example.com), in order to mislead victim to believe that it belongs to that organisation, being the most common phishing method. At the same time, there has been a concurrent rise in the number of the involved phishing IP addresses to 302 (see Figure 7). The top IP address 103.65.182.5 accounted for 198 events (15%); followed by 103.65.182.89 which accounted for 151 events (12%); and both were registered under AS38197 (Sun Network).

For defacement events, there has been a marked overall increase from 318 in Q1 to 532 in Q2; while the involved defacement IP addresses slightly rose by 18% to 204 (see Figure 5). Top 5 IP addresses hosted accounted for 209 events (39%). Many of these defacement events could be attributed to attackers compromising those vulnerable servers which hosted multiple websites.

HKCERT urges system and application administrators to strengthen the protection of 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 attack

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:

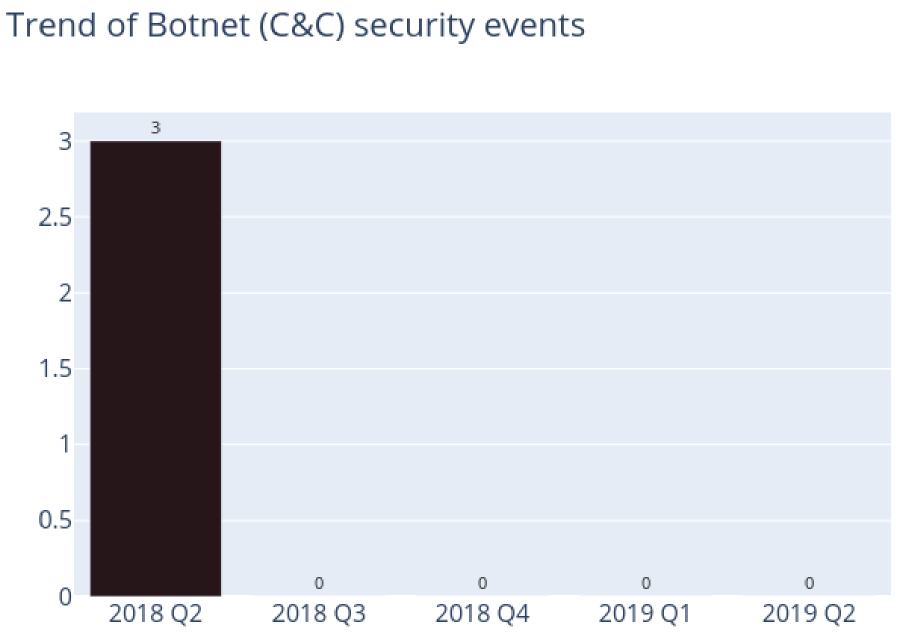

Figure 3: Trend of Botnet (C&Cs) security events

There was no Command and Control Server event received in this quarter.

Botnet Bots

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

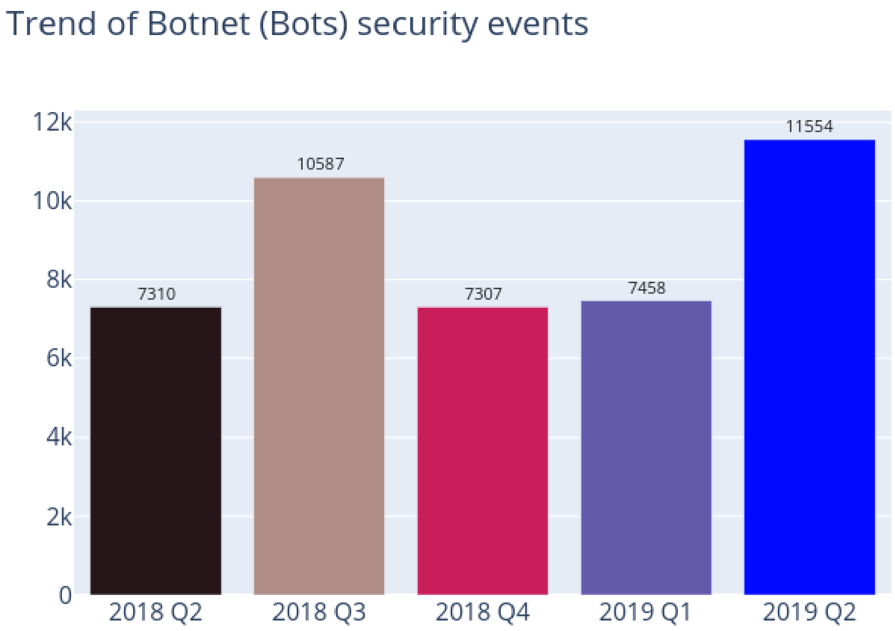

Figure 4: Trend of Botnet (Bots) security events

Compared with the previous quarters, the number of Botnet (bots) in Hong Kong network reached a record high of 11,554 in 2019 Q2; caused mainly by a surge in Ramnit bots, from 57 in Q1 to 4,522 in Q2, up more than seventy-eight times in the first quarter. (see Table 2).

Also, Ramnit overtook Mirai at the top of Major Botnet Families in Hong Kong Networks. Ramnits operators are primarily focused on stealing sensitive information, such as passwords and online banking login credentials. It also functions as a backdoor capabilities that allow unauthorised access.

Based on the data in 2019 Q2, the counts of unique IP address attempting to connect to the Ramnit sinkholes soared sharply on both 12 and 14 June. Over 99% of infected IP addresses registered under ASN AS138979 (AresFlare CO., Ltd (Cambodia)) and AS138570 (AresFlare Network Limited). HKCERT has notified all the affected ASN during the regular botnet cleanup operations.

HKCERT urges users to take action 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 cleanup since June 2013. Currently, botnet cleanup operations against major botnet family WannaCry, Avalanche, XCodeGhost, Pushdo, Citadel, Mumblehard, Ramnit, ZeroAccess and GameOver Zeus are still ongoing.

HKCERT urges general users to join the cleanup acts, ensuring their computers not being infected and controlled by malicious software, and protecting their personal data for a clean cyberspace.

Users can follow 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

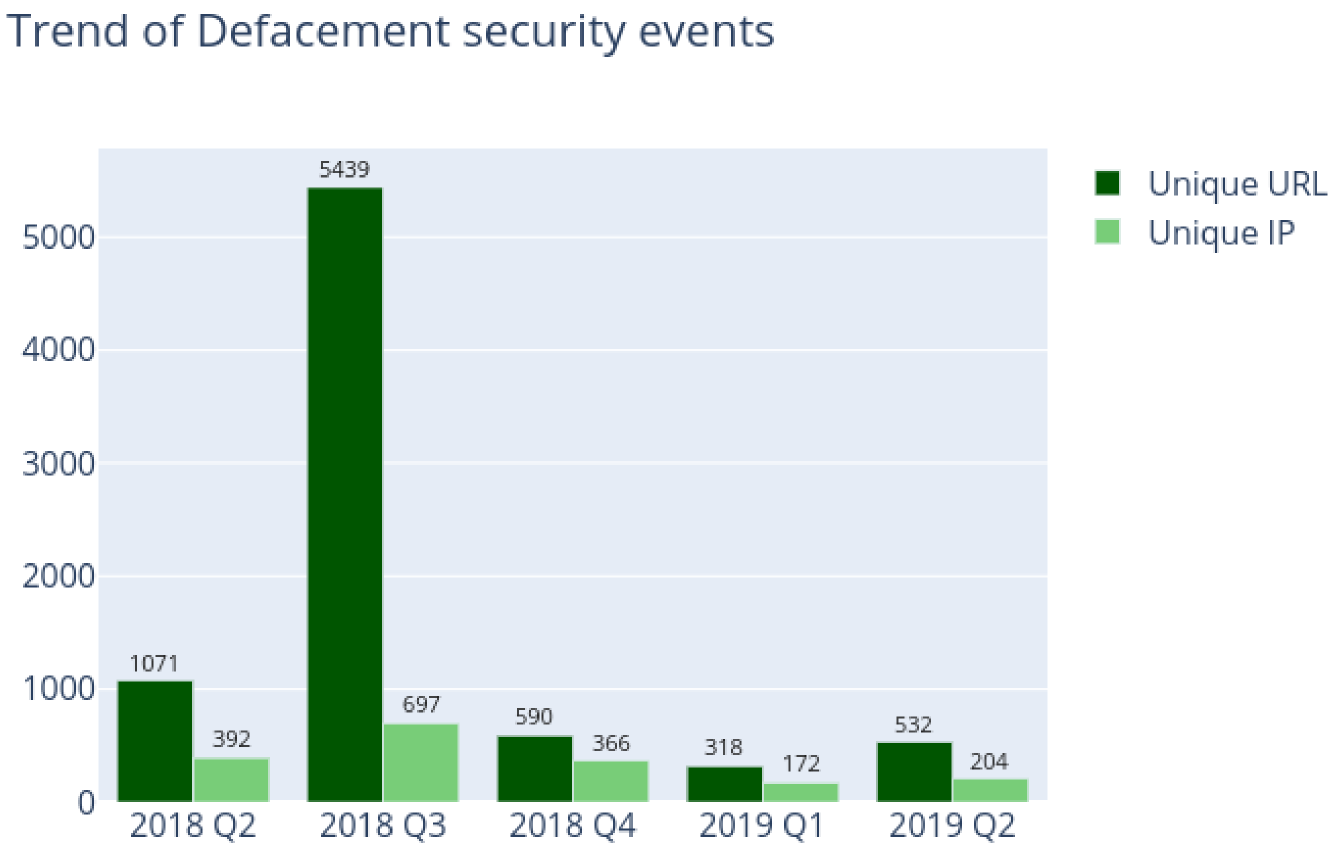

Figure 5: Trend of Defacement security events

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 hackers to perform other attacks

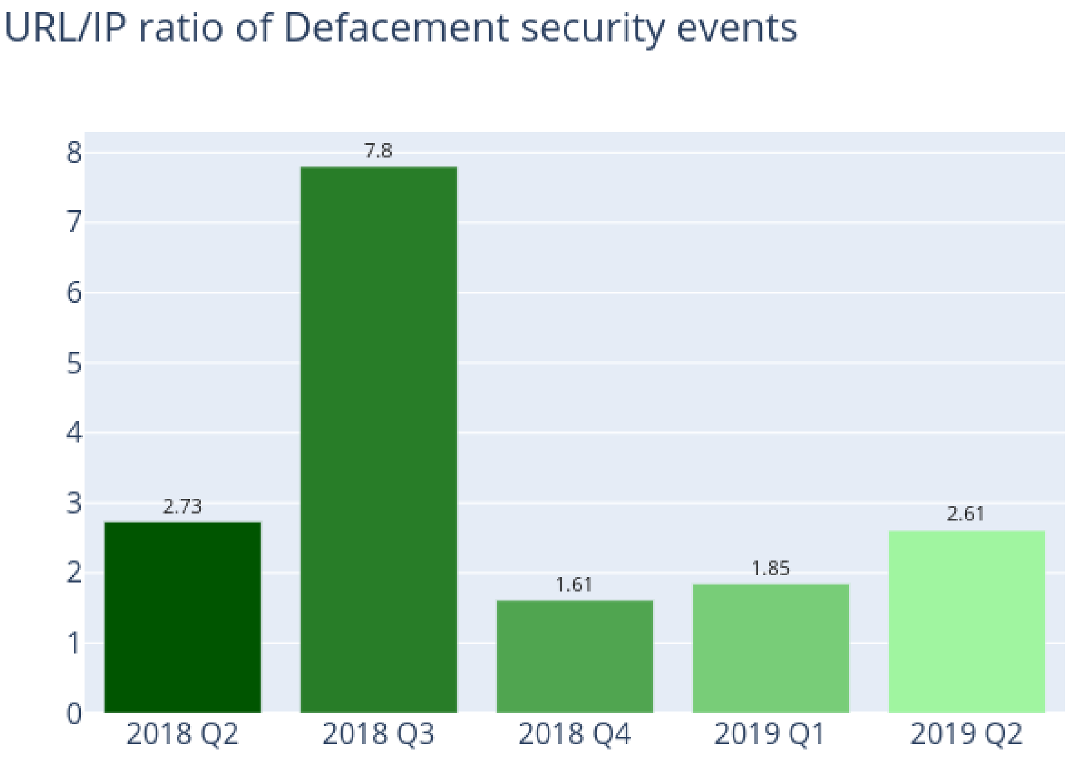

Figure 6: URL/IP ratio of defacement security events

What is URL/IP ratio?

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

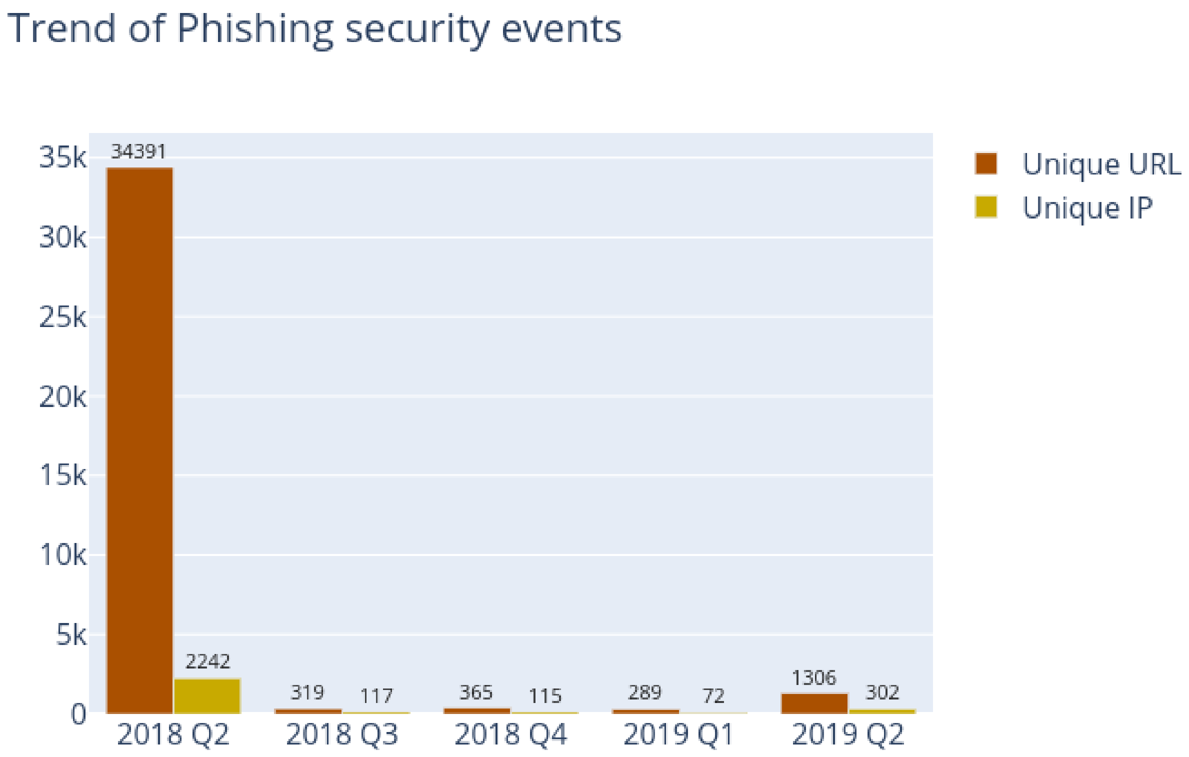

Figure 7: Trend of Phishing security events

What is Phishing?

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

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

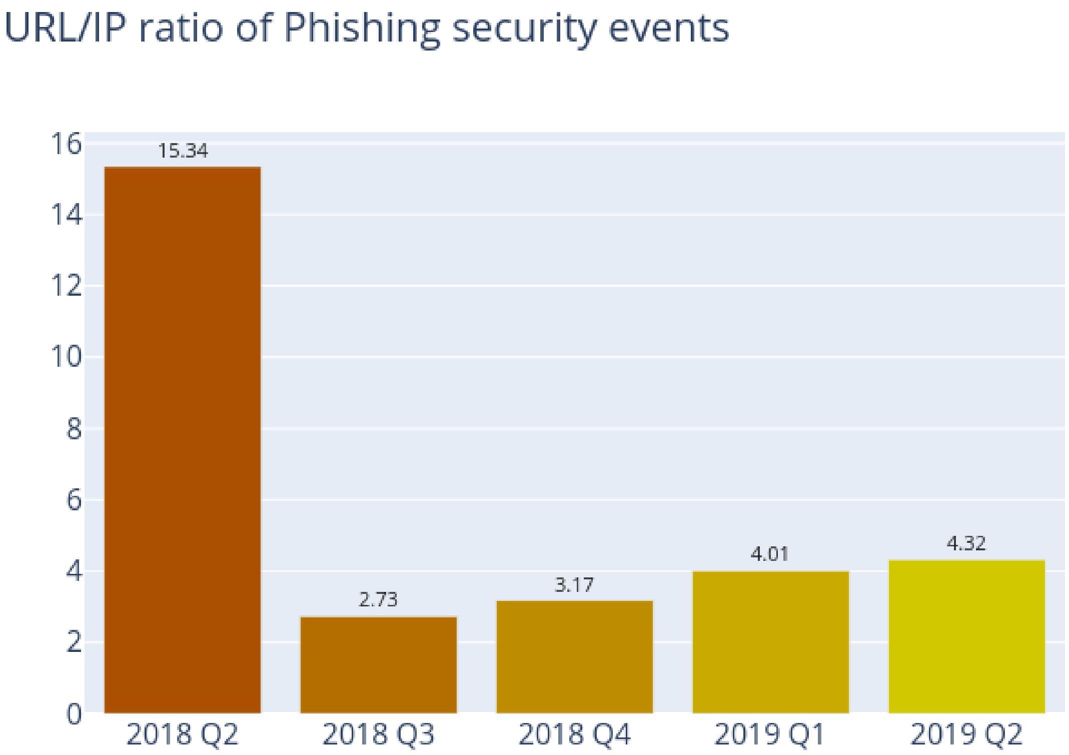

Figure 8: URL/IP ratio of Phishing security events

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:

- CleanMX - phishing
- Phishtank

3 Malware Hosting

3.1 Summary

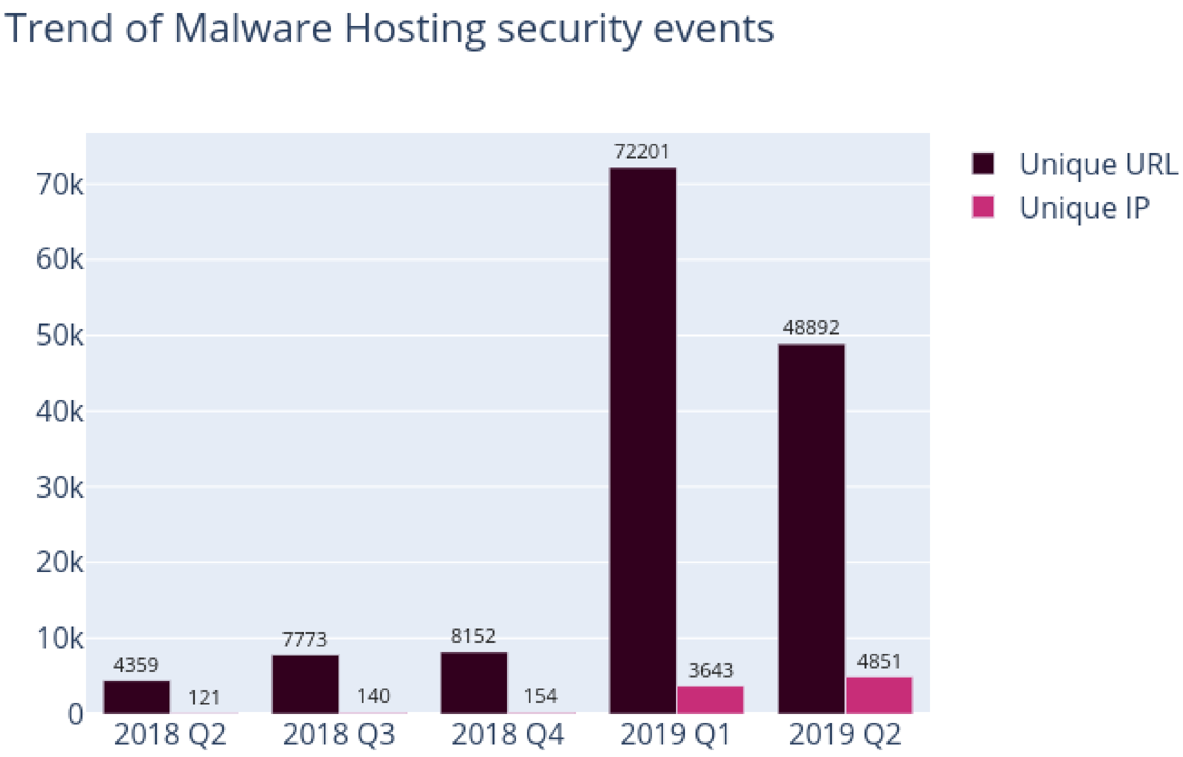

Figure 9: Trend of Malware Hosting security events

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 hacked
- Original content might be inaccessible
- Reputation of the website owner might be damaged
- Server might be further compromised to perform other criminal activities

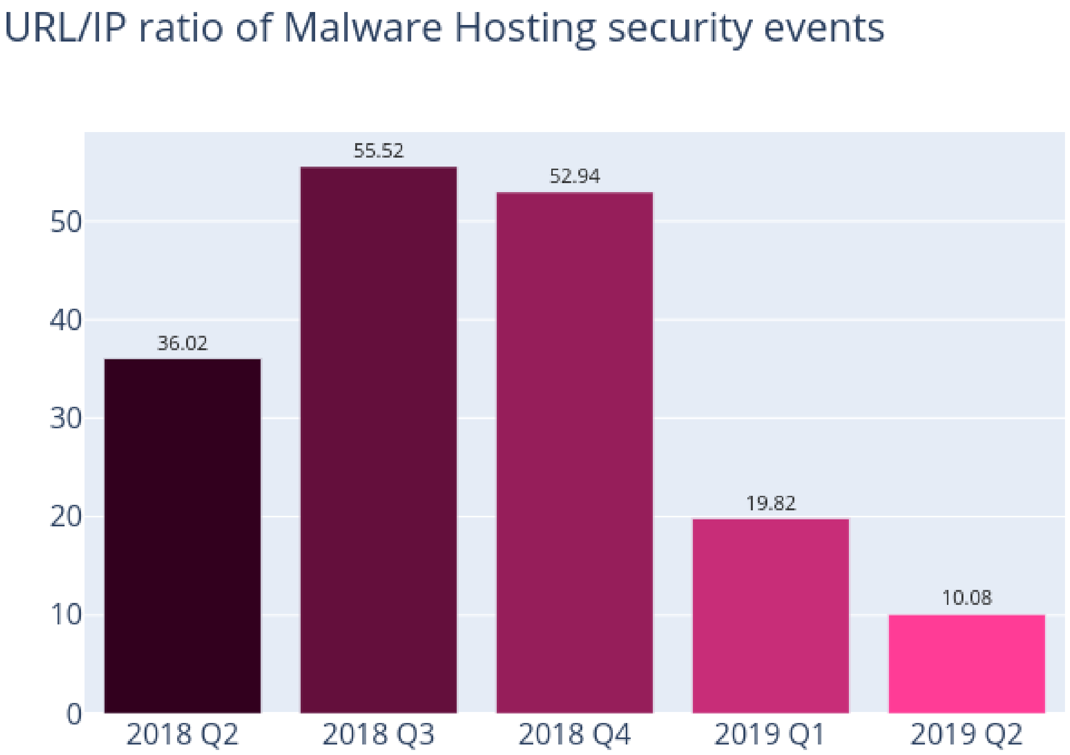

Figure 10: URL/IP ratio of Malware Hosting security events

What is URL/IP ratio?

- It is the number of security events count in unique URL divided by the number of security events 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
- CleanMX - Malware
- Malc0de
- MalwareDomainList

4 Botnet

4.1 Botnets - Command & Control Servers

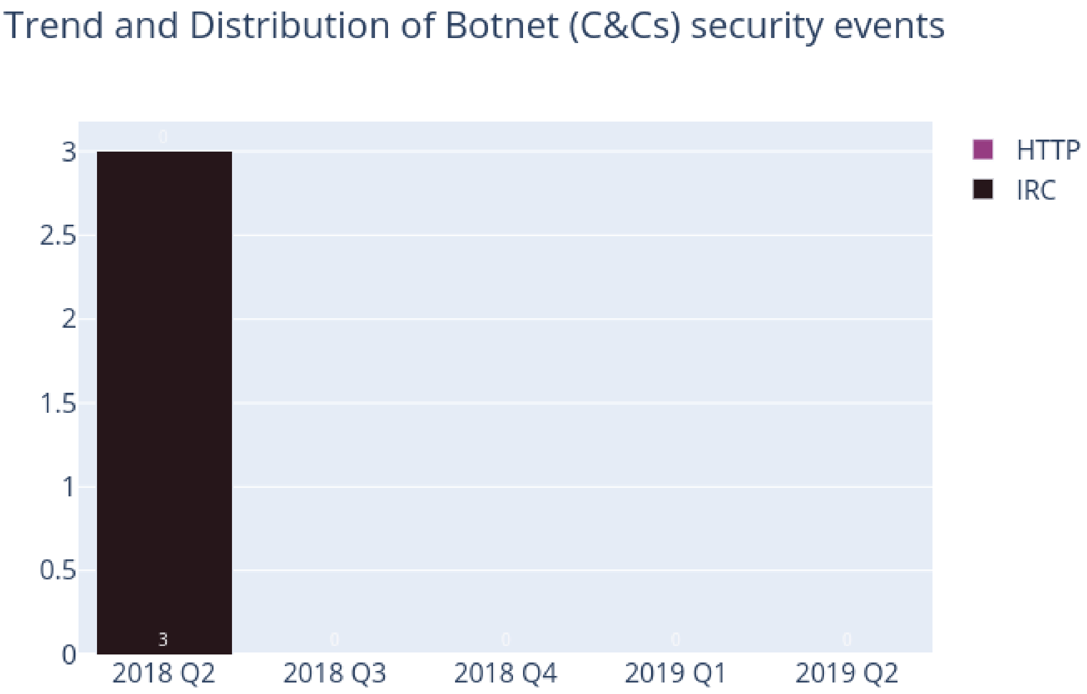

Figure 11: Trend and Distribution of Botnet (C&Cs) security events

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
- Palevo Tracker
- Shadowserver - C&Cs

4.2 Botnets - Bots

4.2.1 Major Botnet Families[4]

Individual botnets 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 activated on the same day.

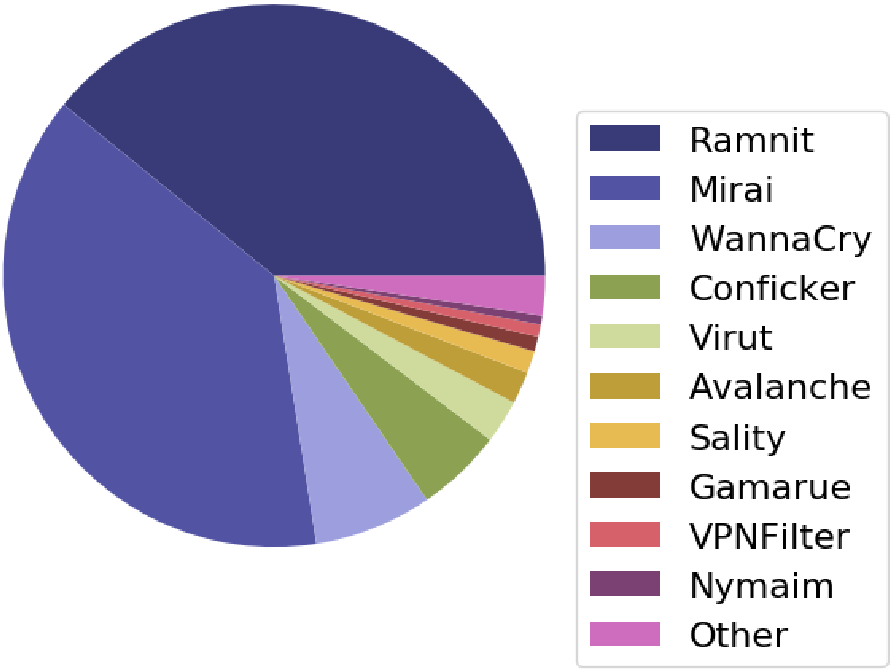

Figure 12: Major Botnet Families in Hong Kong Networks

Table 2: Major Botnet Families in Hong Kong Networks

Rank	⇑⇓	Concerned Bots	Number of Unique IP addresses	Changes with previous period
1	⇑	Ramnit	4,522	7833.3%
2	⇓	Mirai	4,432	-2.0%
3	⇓	WannaCry	813	-17.8%
4	⇓	Conficker	594	5.1%
5	⇓	Virut	299	-2.0%
6	⇓	Avalanche	222	-5.9%
7	⇓	Sality	152	23.6%
8	⇓	Gamarue	103	-8.0%
9	→	VPNFilter	84	-3.4%
10	→	Nymaim	62	-15.1%

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

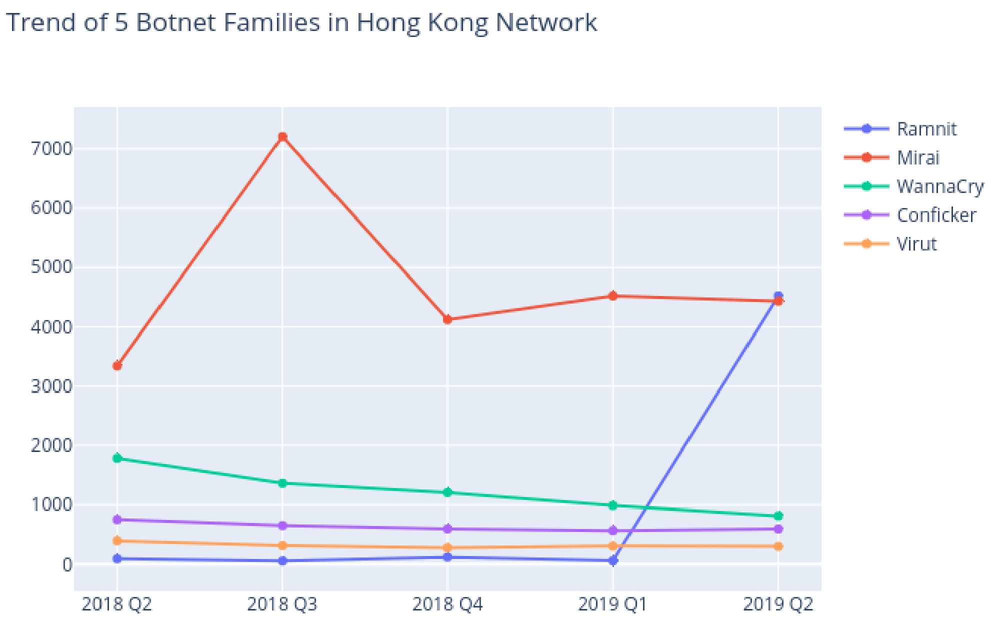

Figure 13: Trend of Top 5 Botnet Families in Hong Kong Network

Name	**2018 Q2**	**2018 Q3**	**2018 Q4**	**2019 Q1**	**2019 Q2**
Ramnit	90	53	118	57	4,522
Mirai	3,340	7,205	4,120	4,521	4,432
WannaCry	1,786	1,364	1,208	989	813
Conficker	752	651	595	565	594
Virut	394	313	278	305	299

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?

- Computers might be commanded to perform other criminal activities
- Computer owners personal and financial data might be stolen which may lead to financial loss
- Commands from hackers might lead to other malicious activities, e.g. spreading malicious software or launching DDoS attacks

Sources of Information:

- 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	CleanMX - Phishing	2013-04
Phishing	Phishtank	2013-04
Malware Hosting	Abuse.ch: Zeus Tracker - Binary URL	2013-04
Malware Hosting	CleanMX - Malware	2013-04
Malware Hosting	Malc0de	2013-04
Malware Hosting	MalwareDomainList	2013-04
Botnet (C&Cs)	Abuse.ch: Zeus 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)	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	2019-7-9

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
VPNFilter	Nil	Worm	• possibly exploit device vulnerabilities	• launch network attacks • leak network traffic flowing through the infected devices • disrupt Internet connection
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