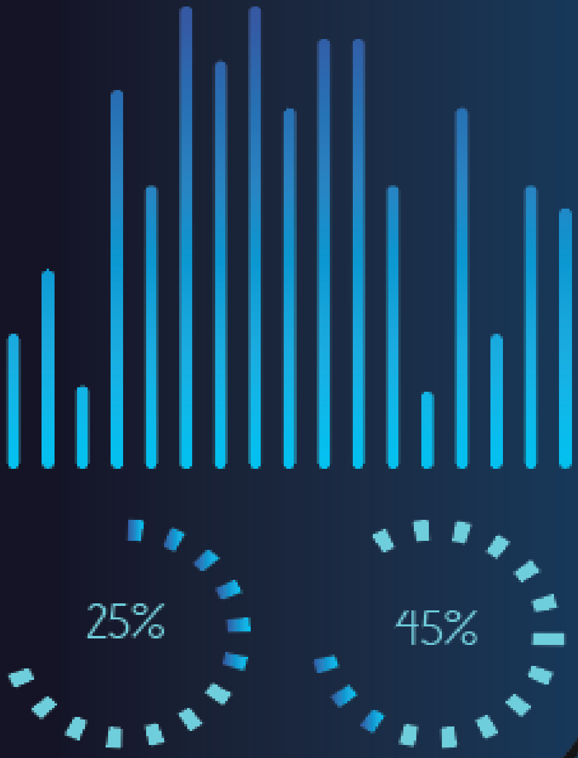
Hong Kong Security Watch Report

2020 Q3

Release date: Nov 2020



Foreword

Better Security Decision with Situational Awareness

Nowadays, many networked digital devices, such as computers, smartphones, tablets, are being compromised without the user's knowledge. The data on them may be mined and exposed every day, and even be 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 quarterly report focuses on 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".

Capitalising on the Power of Global Intelligence

This report is the result 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 collected information of IP addresses of attack source or web links of malicious activities 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 the information.

HKCERT collects and aggregates such 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.

HKCERT 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

HKCERT will continue to enhance this report with more valuable information sources and more in-depth analysis, and explore how to best use the data to enhance our services. *Please send your feedback via email (**hkcert@hkcert.org**).*

Limitations

Data collected for this report come 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

Report Highlights

In 2020 Q3, there were 6,753 unique security events related to Hong Kong used for analysis in this report. Data were collected through IFAS[1] with 10 sources of information[2], and not collected from the incident reports received by HKCERT.

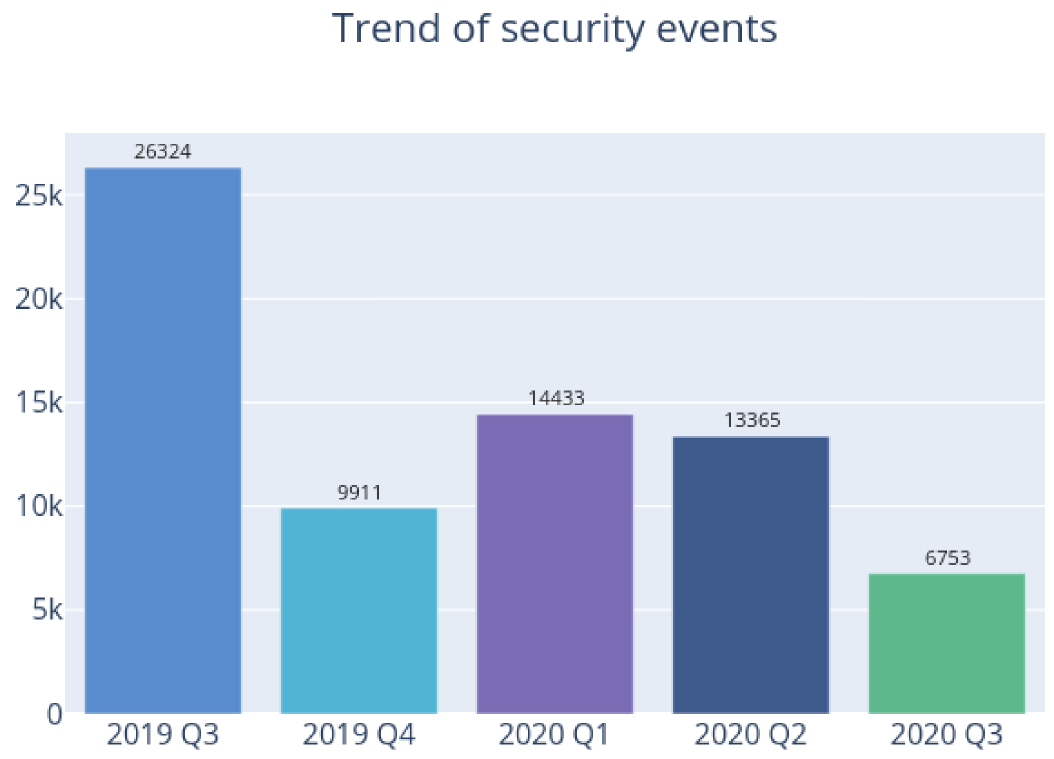


Figure 1: Trend of security events

Table 2: Trend of security events

Event Type	2019 Q3	2019 Q4	2020 Q1	2020 Q2	2020 Q3
Defacement	1,120	591	572	1,062	571
Phishing	849	257	399	2,017	552
Malware Hosting	17,273	1,185	5,445	4,334	934
Botnet (Bots)	7,078	7,878	8,017	5,952	4,696
Botnet (C2)	4	0	0	0	0
Total	**26,324**	**9,911**	**14,433**	**13,365**	**6,753**

The total number of cyber security events in the third quarter of 2020 fell by nearly 50%, from 13,365 in 2020 Q2 to 6,753 in this quarter. There are significant reductions in web defacement, phishing, malware hosting or botnet events.

[1] 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.

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

Server related security events

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

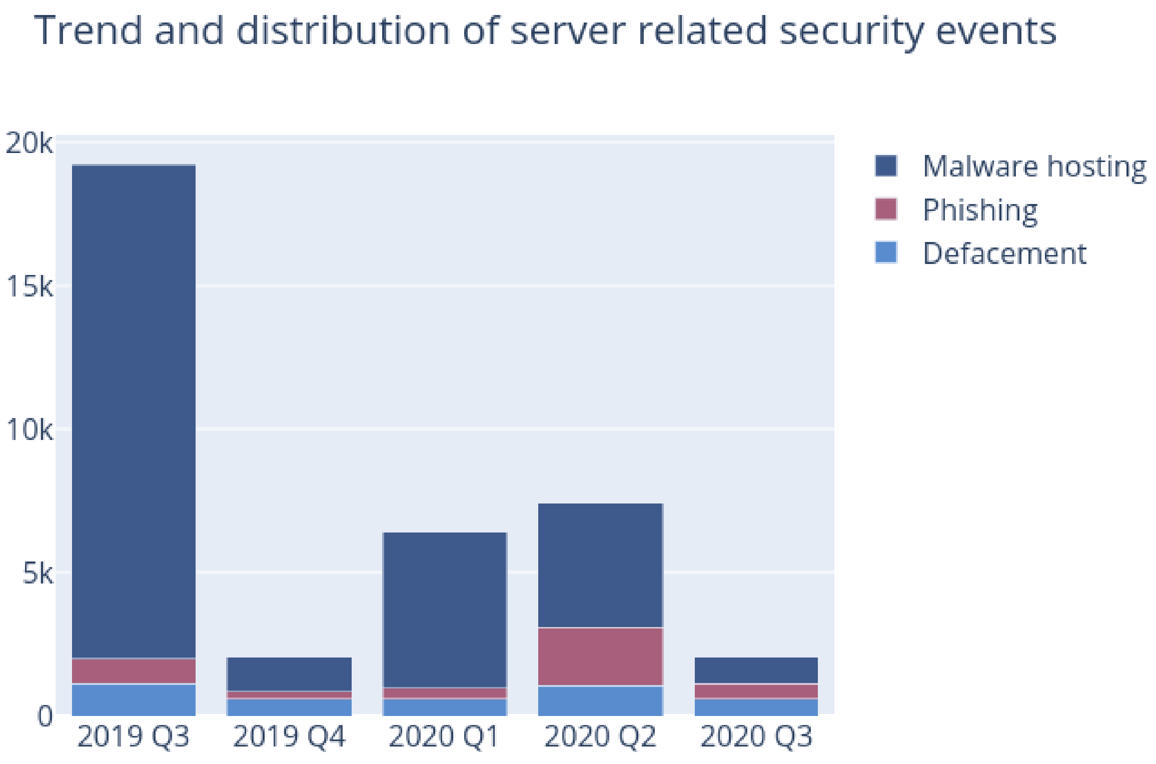


Figure 2: Trend and distribution of server related security events

As shown in Table 2, the number of phishing attacks has fallen by more than 70%, from 2017 cases in Q2 2020 to 552 cases in this quarter, and the number of unique IP addresses involved has also decreased by 38% to a total of 145 (Figure 7), while the unique URL/IP ratio decreased by 38% to 3.81 (Figure 8).

Compared with last quarter, the number of defacement event decreased by 46% to 571 cases. The number of unique IP addresses involved in defacement events also decreased by 32% to a total of 311 (Figure 5). The unique URL/IP ratio also decreased by 19% to 1.84 (Figure 6).

Although the phishing and defacement events have recorded a decrease, it only returned to the pre-COVID-19 level. Overall, the situation has not improved when compared with the beginning of this year.

In this quarter, the number of malware hosting events dropped by 88%, from last quarter's 4,334 cases to 934 cases, and the number of related unique IP addresses was also down 68% to 157 (Figure 9). The unique URL/IP ratio has also shortened from 8.81 to 5.95 (Figure 10). The data reveals that, besides targeting computers, a portion of malwares is targeting mobile devices, e.g. mobile phone, tablet, etc. Users are advised to verify the apps before downloading and installing. HKCERT recommends users to always download mobile applications from official apps store.

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 a small number of powerful computers, mostly servers, which give commands to bots
- Botnet (Bots) security events - involving a large number of computers, mostly personal computers which receive commands from C&Cs.

Botnet Command and Control Servers (C&C)

The trend of Botnet (C&C) security events is summarised as below:

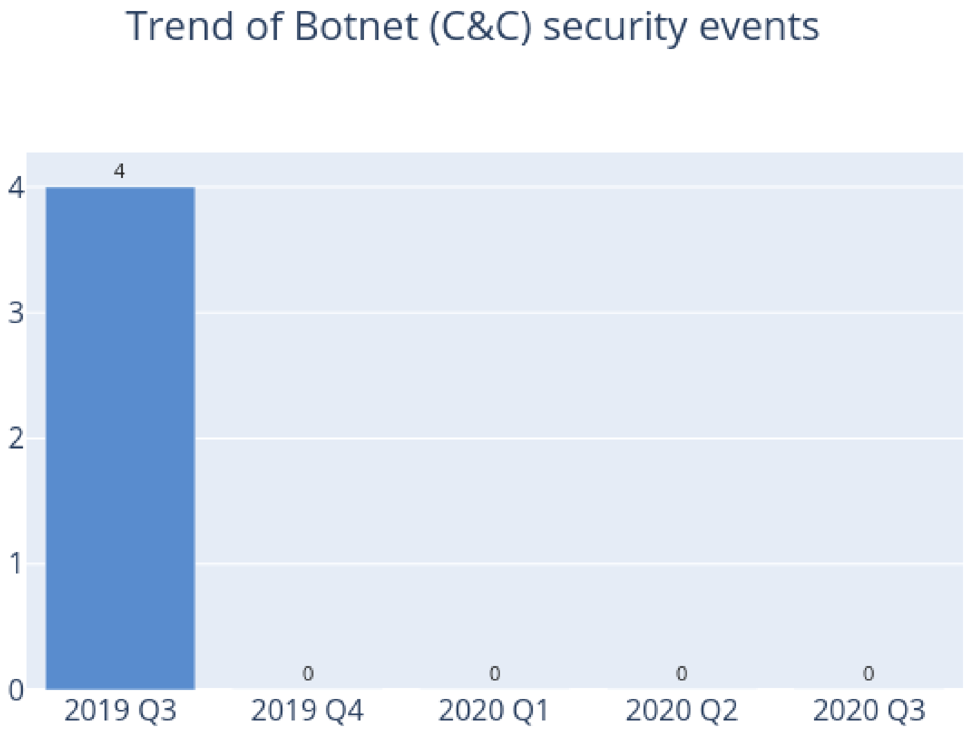


Figure 3: Trend of Botnet (C&Cs) security events

There was no Botnet Command and Control Centers (C&C) security events in this quarter.

Botnet (Bots)

The trend of Botnet (Bots) security events is summarised as below:

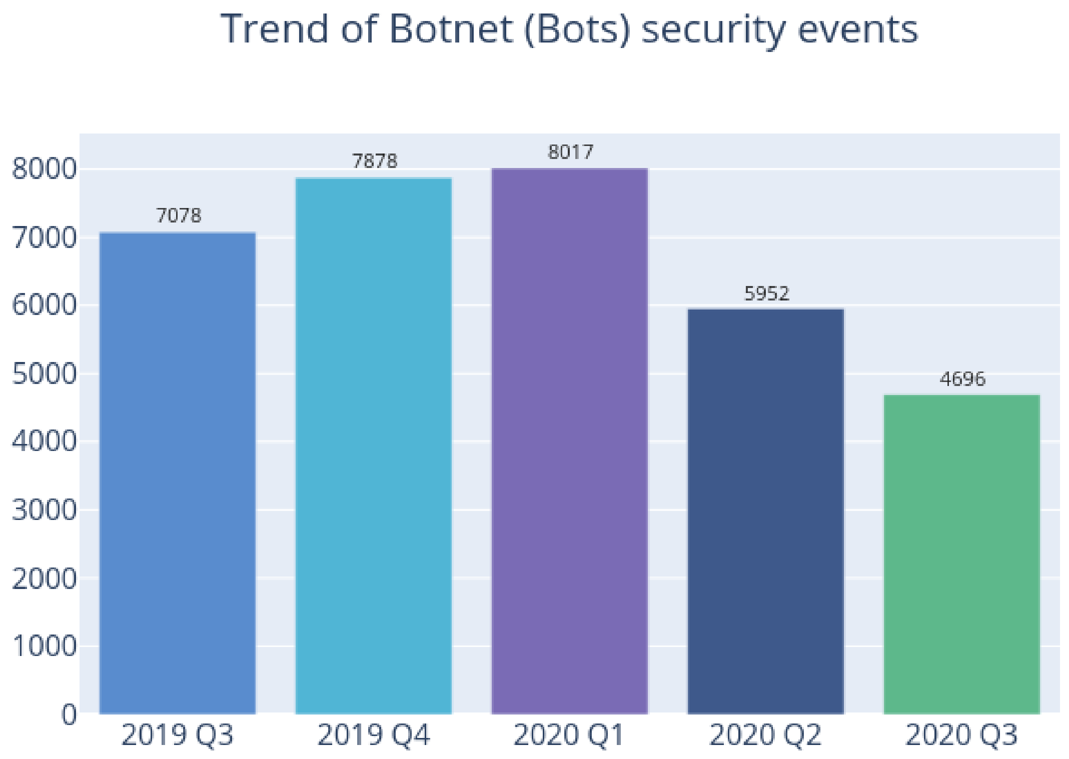


Figure 4: Trend of Botnet (Bots) security events

The number of botnet (bots) event decreased by 21% to 4,696 this quarter. Most botnet families have recorded a decrement. The ranking remains unchanged for most botnet families, while the Nymaim, Virut and Sality have swapped positions.

Although Mirai was the botnet family with the largest decline during the quarter, down 28% to 2,859, it is still the most numerous botnet family. The botnet family with the largest increase or decrease was Nymaim, with the number nearly doubled to 166 cases.

Nymaim is designed to distribute other viruses, such as ransomware, information stealers, and other exploit kits. It mainly spread via phishing email and website. HKCERT reminds users not to open suspicious attachment and file from an unknown sender or on the Internet.

HKCERT urges users to take action so as not to become part of the botnets

- Patch the computer
- Install security software and scan for malware
- 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 Avalanche, Pushdo, Citadel, Ramnit, ZeroAccess, GameOver Zeus, VPNFilter and Mirai are still ongoing.

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

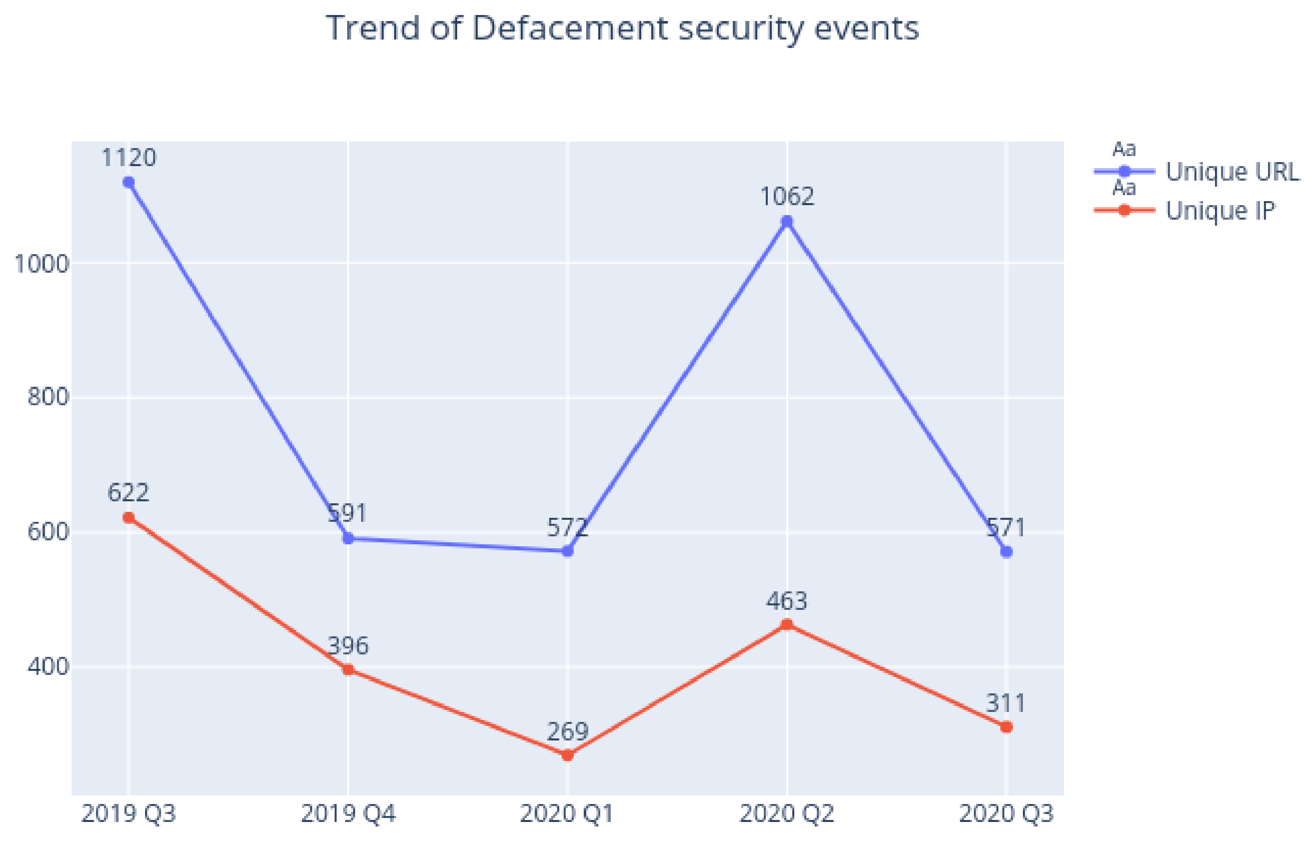


Figure 5: Trend of Defacement security events

What is defacement?

- Defacement is the unauthorised alteration of the content of a legitimate website using any hacking methods.

What are the potential impacts?

- The integrity of the website content is being damaged
- Original content may be inaccessible
- Reputation of the website owner may be damaged
- Other information stored/processed on the server may be further compromised by hackers to perform other attacks

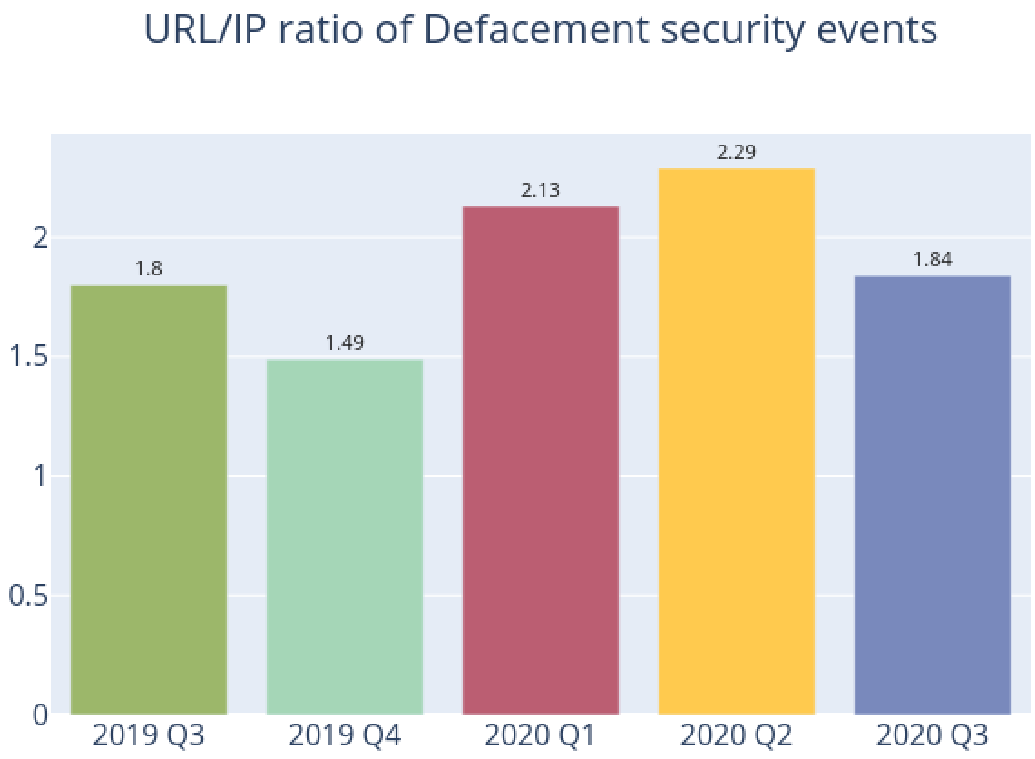


Figure 6: URL/IP ratio of Defacement security events

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

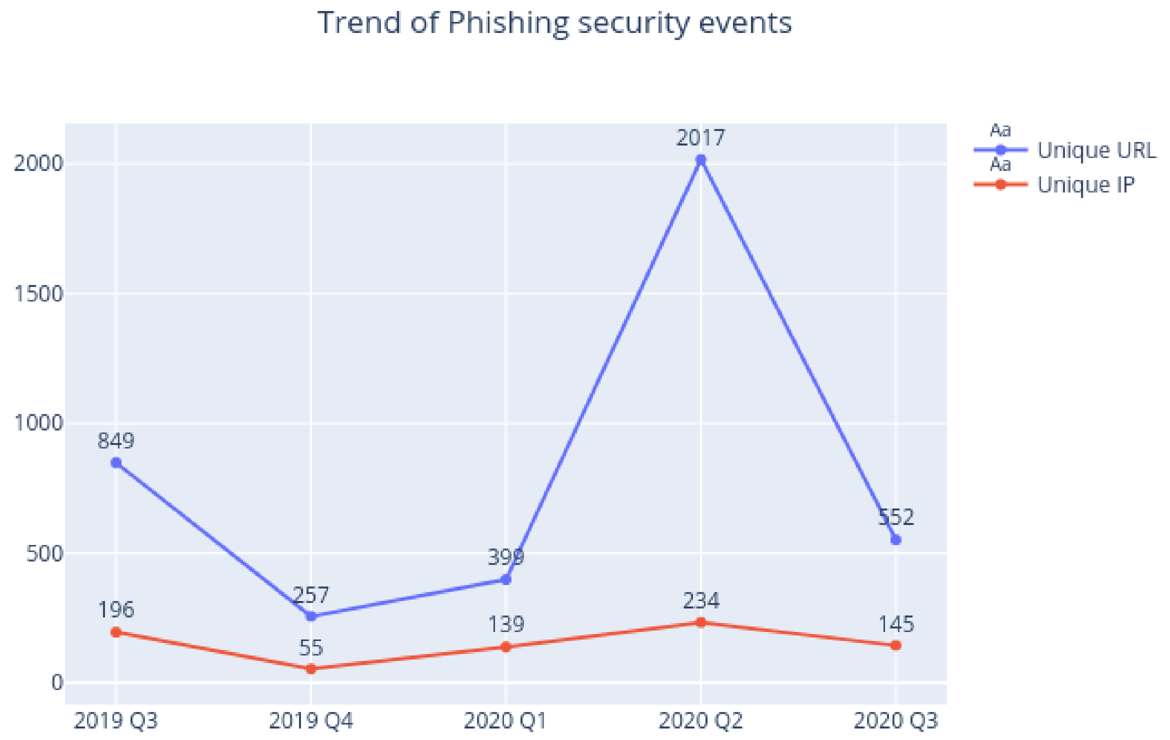


Figure 7: Trend of Phishing security events

What is phishing?

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

What are the potential impacts?

- Personal information or account credentials of visitors may be stolen, potentially leading to financial losses
- Original content may be inaccessible
- Reputation of the website owner may be damaged
- Server may be further compromised to perform other attacks

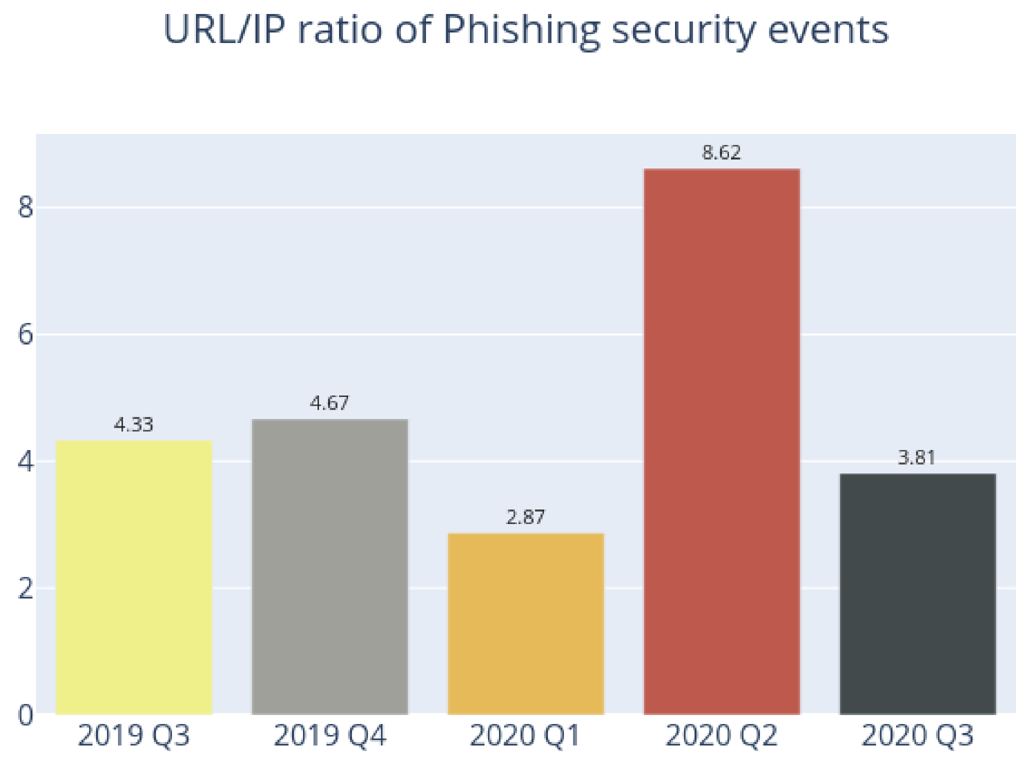


Figure 8: URL/IP ratio of Phishing security events

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

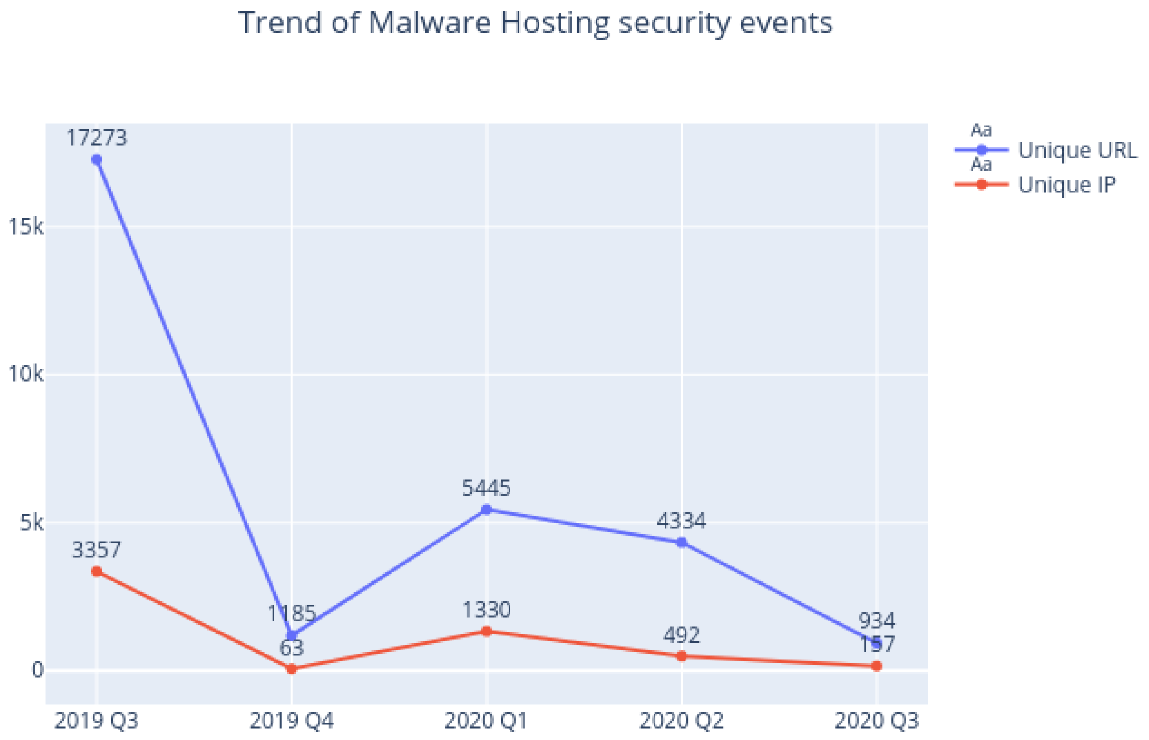


Figure 9: Trend of Malware Hosting security events

What is malware hosting?

- Malware hosting is the dispatching of malware on a website

What are the potential impacts?

- Visitors may download and install the malware, or execute the malicious script to have their devices hacked
- Original content may be inaccessible
- Reputation of the website owner may be damaged
- Server may be further compromised to perform other hacking or even criminal activities

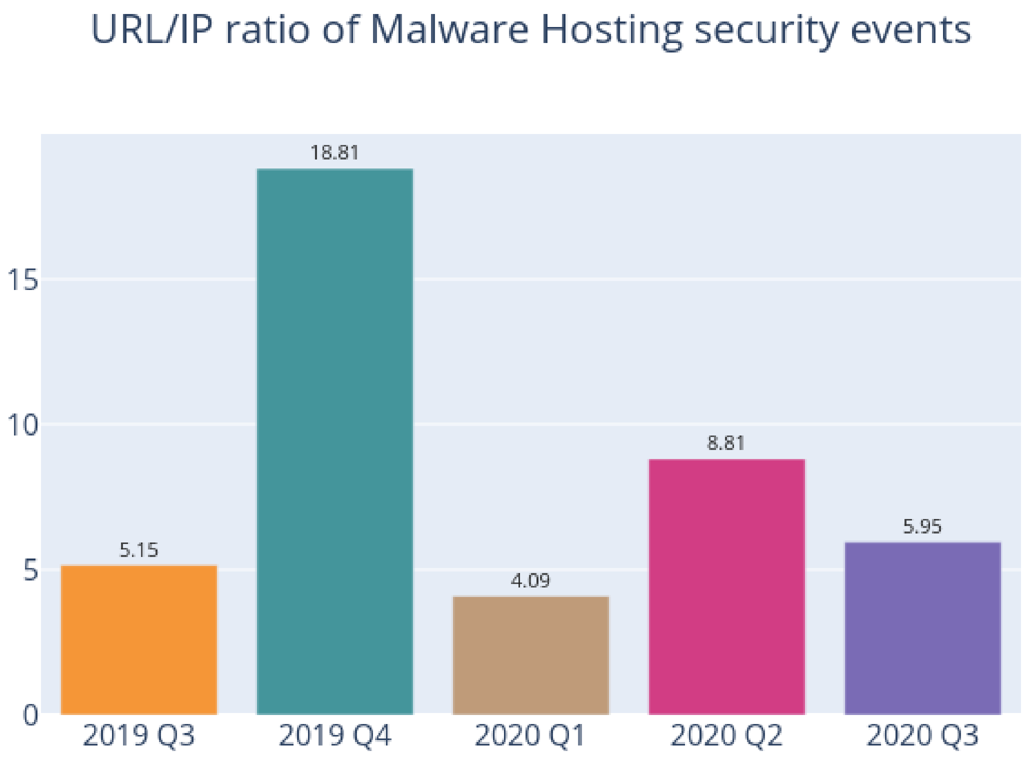


Figure 10: URL/IP ratio of Malware Hosting security events

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:

- CleanMX - Malware
- Malc0de
- MalwareDomainList

4 Botnet

4.1 Botnets Command & Control Centers (C&C)

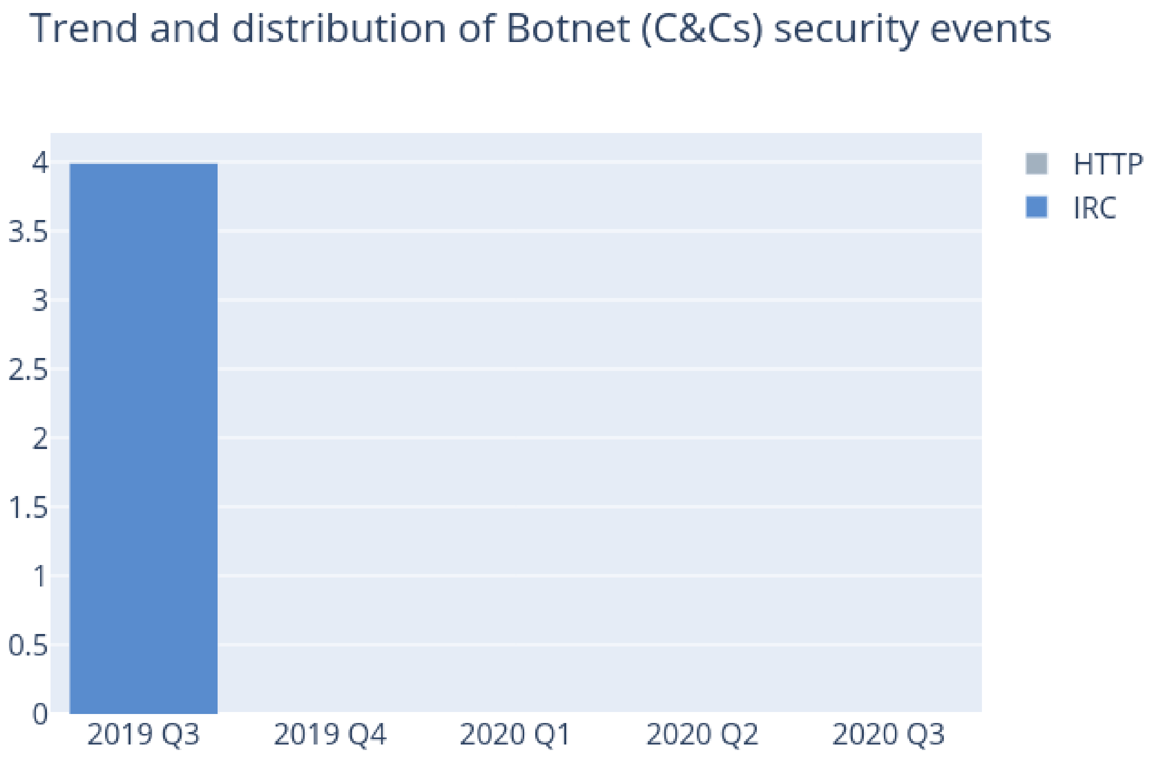


Figure 11: Trend and distribution of Botnet (C&Cs) security events

What is a Botnet Command & Control Center?

- 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?

- A server may be heavily loaded when many bots connect to it
- A server may have a large amount of personal and financial data stolen

Sources of Information:

- Shadowserver - C&Cs

4.2 Botnets (Bots)

4.2.1 Major Botnet Families

Major Botnet families are selected botnet families with a considerable amount of security events reported from the information sources consistently across the reporting period.

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 reporting period. In other words, the real botnet size should be larger because not all bots are activated on the same day.

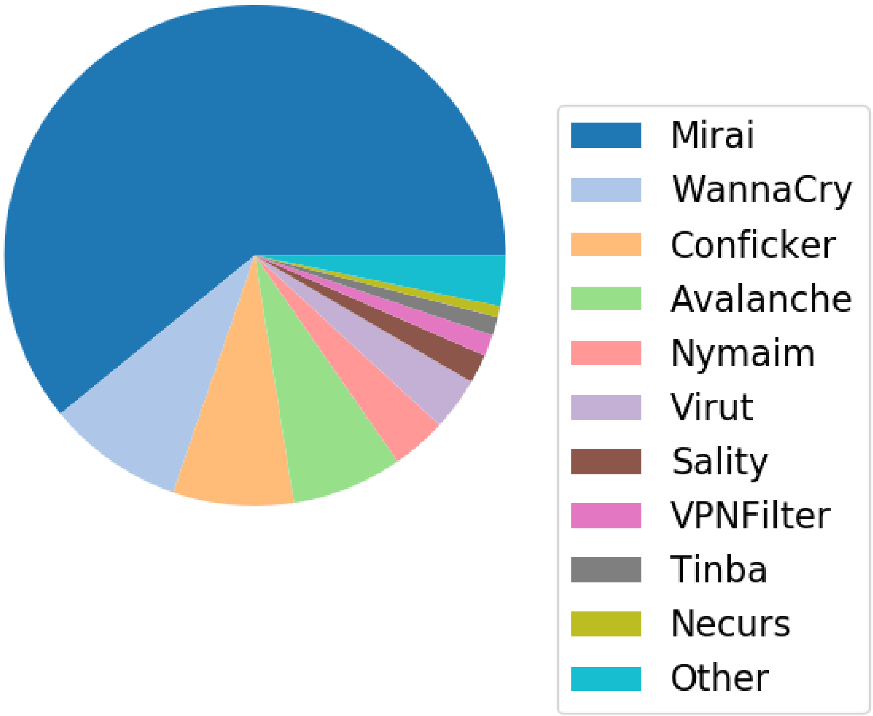


Figure 12: Major Botnet families in Hong Kong network

Table 3: Major Botnet families in Hong Kong network

Rank	⇑⇓	Concerned Bots	Number of Unique IP addresses	Changes with previous period
1	→	Mirai	2,859	-28.0%
2	→	WannaCry	415	-19.1%
3	→	Conficker	365	-8.8%
4	→	Avalanche	336	-2.6%
5	⇑	Nymaim	166	90.8%
6	⇓	Virut	160	0.0%
7	⇓	Sality	88	-9.3%
8	→	VPNFilter	65	-9.7%
9	→	Tinba	56	9.8%
10	→	Necurs	33	-23.3%

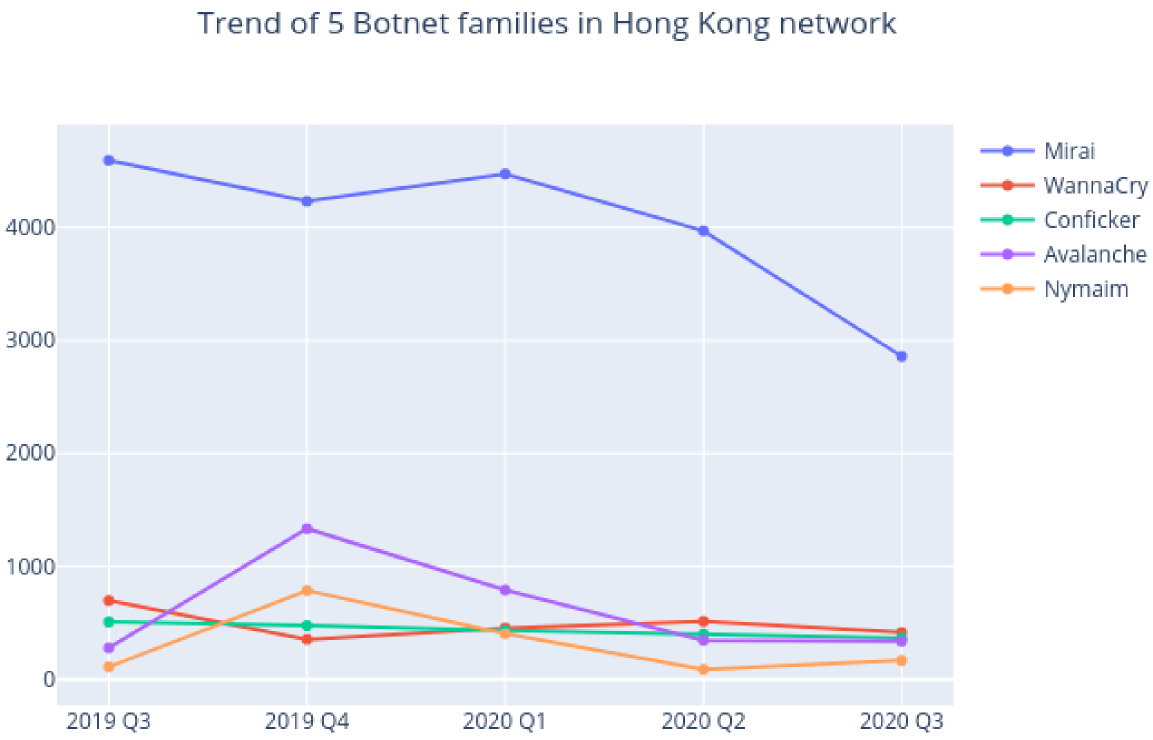


Figure 13: Trend of top 5 Botnet families in Hong Kong network

Table 4: Trend of top 5 Botnet families in Hong Kong network

Name	2019 Q3	2019 Q4	2020 Q1	2020 Q2	2020 Q3
Mirai	4,594	4,231	4,474	3,969	2,859
WannaCry	697	354	454	513	415
Conficker	508	476	432	400	365
Avalanche	277	1,333	790	345	336
Nymaim	110	786	403	87	166
Total	**6,186**	**7,180**	**6,553**	**5,314**	**4,141**

What is a Botnet (Bots)?

- A Botnet (Bots) 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 the hackers.

What are the potential impacts?

- Computers may be commanded to perform other hacking or criminal activities
- Computer owner's personal and financial data may be stolen which may lead to financial loss
- Commands from hackers may 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 5: 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	CleanMX - Malware	2013-04
Malware Hosting	Malc0de	2013-04
Malware Hosting	MalwareDomainList	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 6: Methods of Geolocation Identification

Method	First introduced	Last update
Maxmind	2013-04	2020-11

C Major Botnet Families

Table 7: 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 8: 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 unauthorised 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 unauthorised 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 unauthorised 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
Matsnu	Nil	Trojan	• Spam e-mail	• Backdoor capabilities that allow unauthorised access • Lock infected systems • Encrypt user data • Ask for ransom
Palevo	• Rimecud • Butterfly bot • Pilleuz • Mariposa • Vaklik	Worm	• Spread via instant messaging, P2P network and removable drives	• Backdoor capabilities that allow unauthorised access • Steal login credentials and sensitive information • Steal money directly from banks using money mules

Table 9: 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 unauthorised 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 unauthorised 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 10: 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