
# Hong Kong Security Watch Report

2019 Q4

# 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 2019 Q4, there were 8,864 unique security events related to Hong Kong used for analysis in this report. Data were collected through IFAS[1] with 11 sources of information[2], and not collected from the incident reports received by HKCERT.

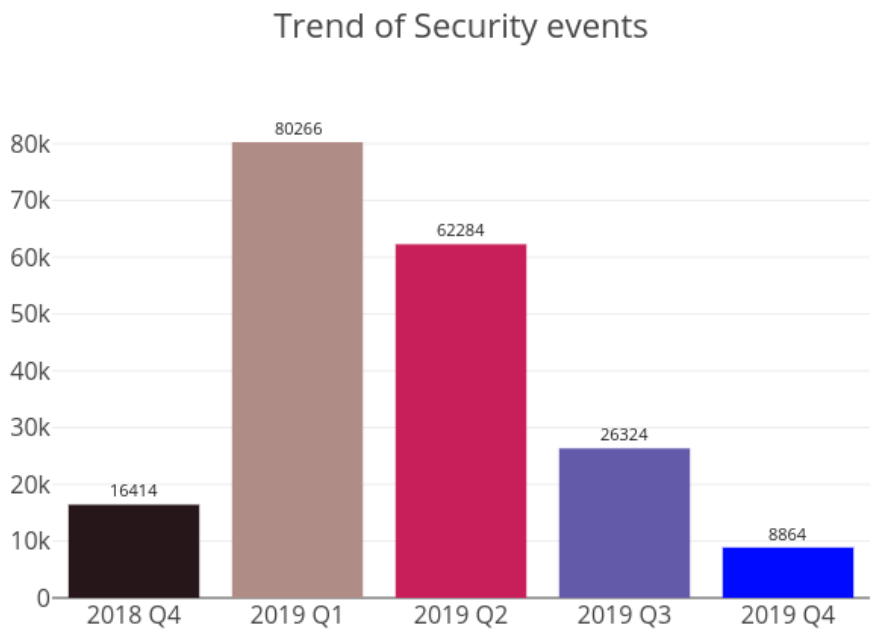


Figure 1: Trend of Security events

Table 2: Trend of Security events

| Event Type | 2018 Q4 | 2019 Q1 | 2019 Q2 | 2019 Q3 | 2019 Q4 |
|---|---|---|---|---|---|
| Defacement | 590 | 318 | 532 | 1,120 | 591 |
| Phishing | 365 | 289 | 1306 | 849 | 257 |
| Malware Hosting | 8,152 | 72,201 | 48,892 | 17,273 | 1,185 |
| Botnet (Bots) | 7,307 | 7,458 | 11,554 | 7,078 | 6,831 |
| Botnet (C2) | 0 | 0 | 0 | 4 | 0 |

In the last quarter of 2019, all types of security events have fallen back to relatively low levels as the total number of security events amounted to 8,864, down two-thirds on the previous quarter's figure. The most notable decline was seen in malware hosting events, which fell by more than 93%, while a 70% decrease was reported in phishing events.

### Server related security events

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

[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

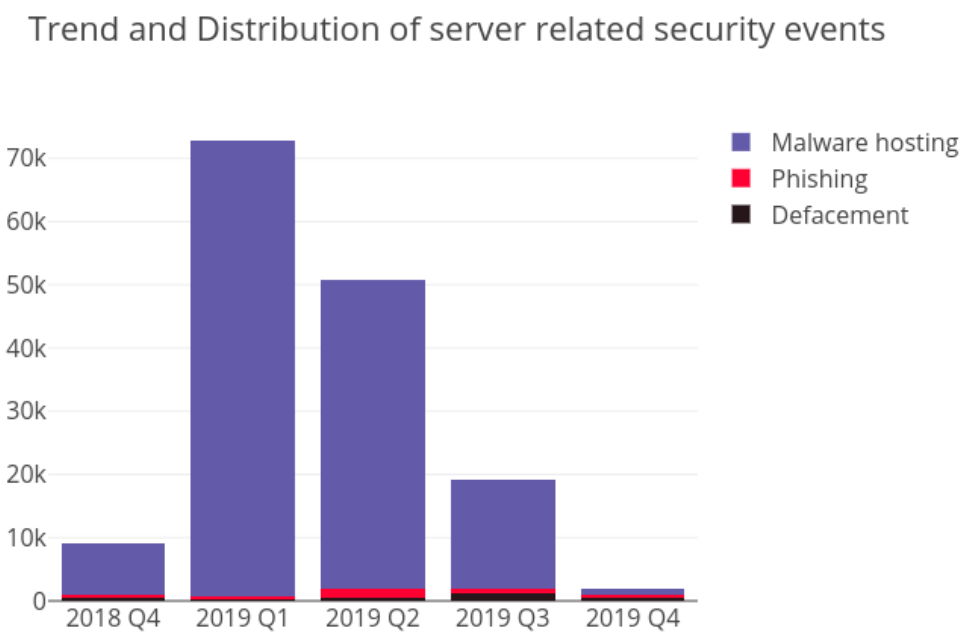


Figure 2: Trend and Distribution of server related security events

As shown in Table 2, having reached a peak of 72,201 events in the first quarter of 2019, malware hosting fell continuously to the lowest point of the year with 1,185 events only. The number of malware hosting IP addresses involved has also dropped sharply to 63 (see Figure 9), the first time since the first quarter of 2018 that double digits are recorded for its occurrence.

Phishing events also declined by nearly 600, while the number of phishing IP addresses involved fell from 196 in the previous quarter to 55 (see Figure 7). After analysing the data, we observed that while Apple iCloud continued to be the main target of such attacks, eBay-related phishing events have also increased. The rise might be attributed to the end-of-year sales, with fraudsters usually taking this opportunity to conduct phishing attacks against the branded online shopping platforms.

Meanwhile, defacement events and the number of defacement IP addresses involved fell by nearly half and 36% in this quarter respectively. Further analysis of these IP addresses in Zone-H and Shodan[3] revealed that around a quarter of servers on these IP addresses still carry security vulnerabilities, and some of them are even using End-of-Support (EOS) operating systems, which are deemed the possible main causes of defacement incidents.

*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

[3] Shodan is a search engine for Internet-connected devices: https://www.shodan.io/

**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 security events - involving a large number of computers, mostly personal computers which receive commands from C&Cs.

Botnet Command and Control Servers

The trend of botnet C&C security events is summarised as below:

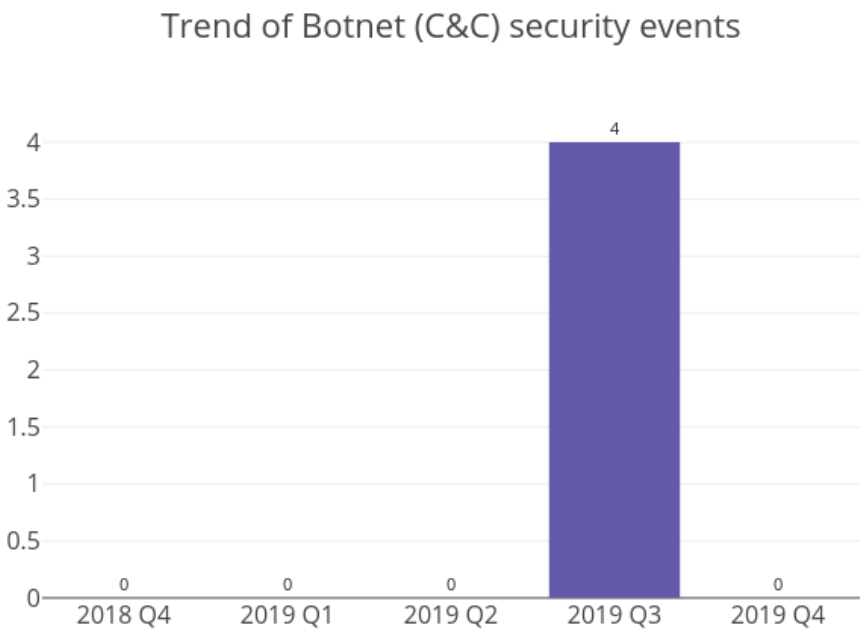


Figure 3: Trend of Botnet (C&Cs) security events

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:

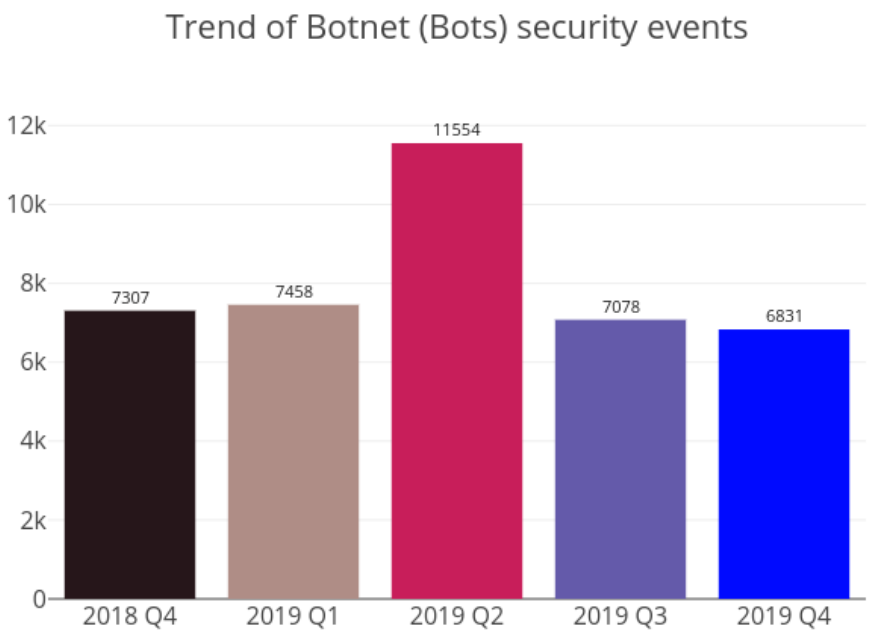


Figure 4: Trend of Botnet (Bots) security events

In 2019 Q4, the number of Botnets (bots) in Hong Kong network has receded slightly by 3%, or 247. Most Botnet events show a downward trend, with WannaCry bots falling by nearly half to just 354. Avalanche, on the other hand, increased dramatically from 277 in Q3 to 1,333 in Q4 (see Table 4). Avalanche is a cyber crime hosting platform serving multiple malware families. Hackers can use it to deliver various malwares (such as Gamarue, Tinba, Nymaim, and Matsnu, etc.). After further analysis, it emerged that the number of unique IP addresses attempting to connect the Avalanche sinkhole from the end of November to December was persistently high. In addition, by comparing the data of the previous three quarters, there have been notable increases in Nymaim and Matsnu malware events. These two malwares are trojan and both can be used as a springboard for further intrusions, such as ransomware attacks.

*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 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

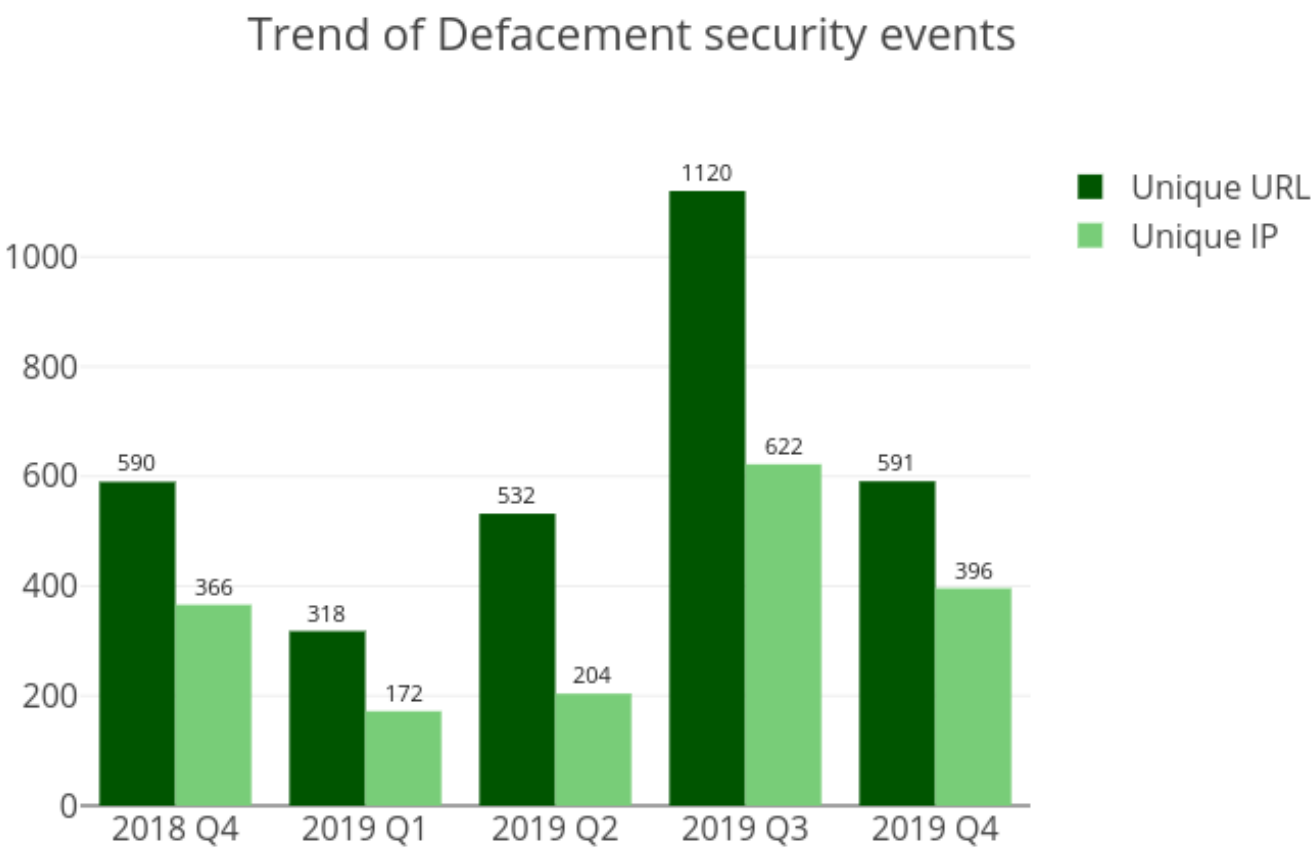


Figure 5: Trend of Defacement security events

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

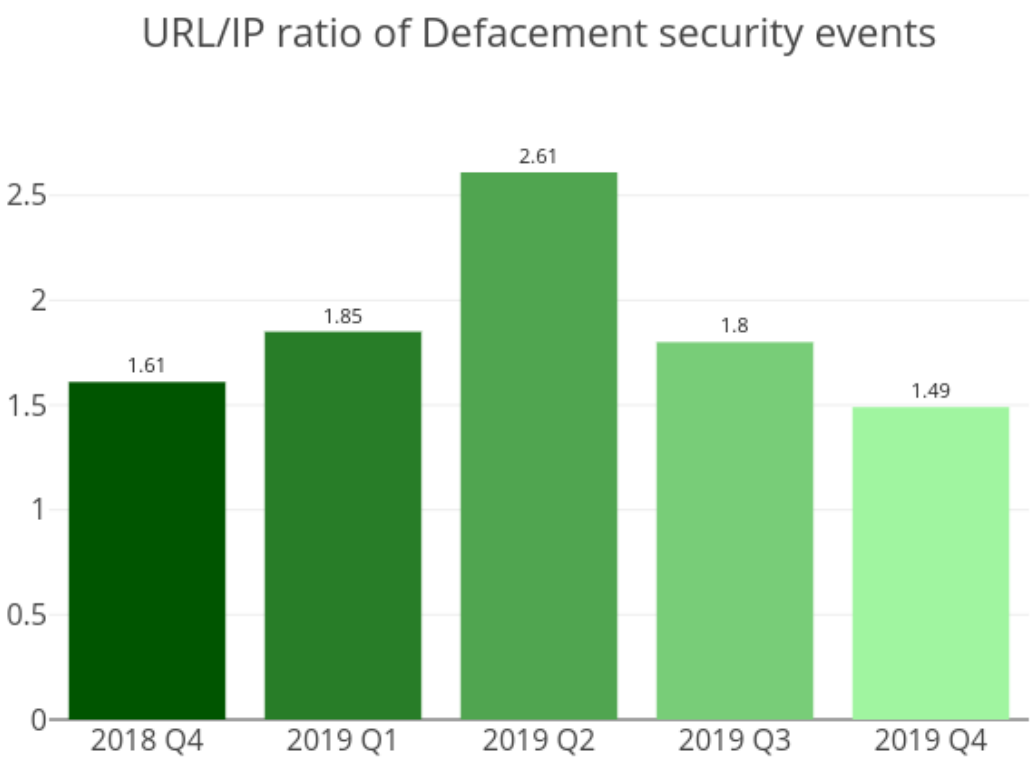


Figure 6: URL/IP ratio of Defacement security events

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

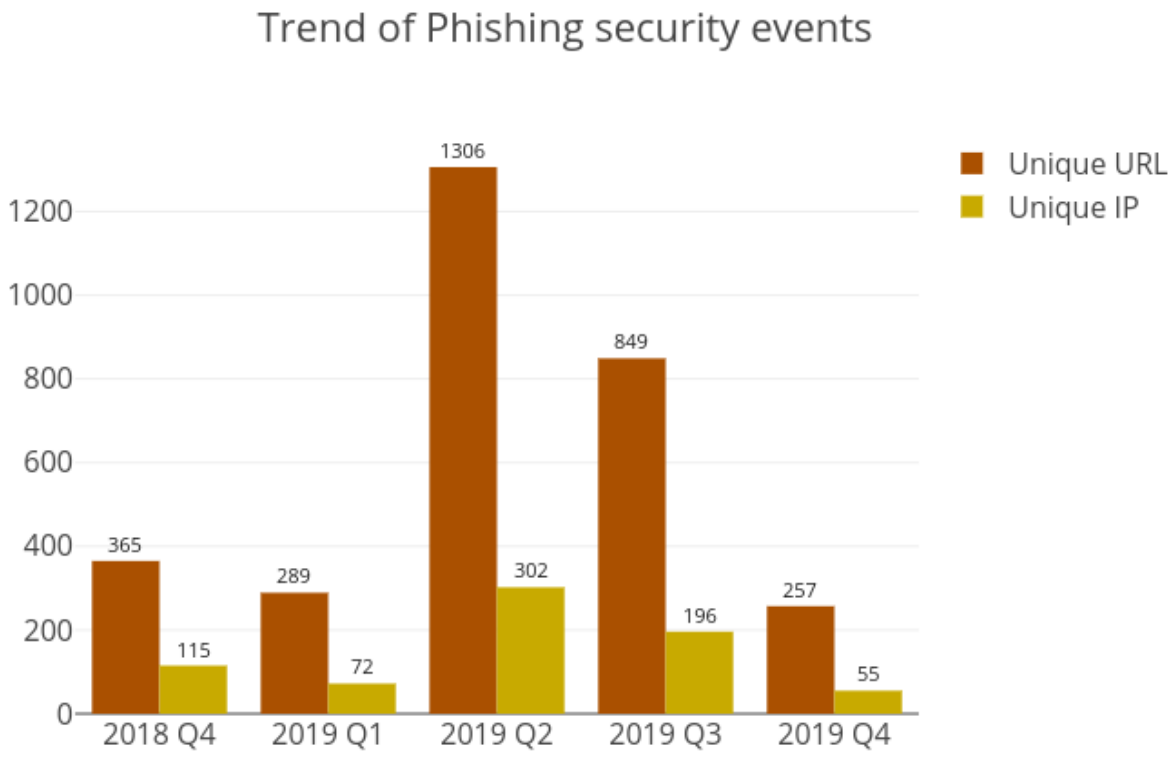


Figure 7: Trend of Phishing security events

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

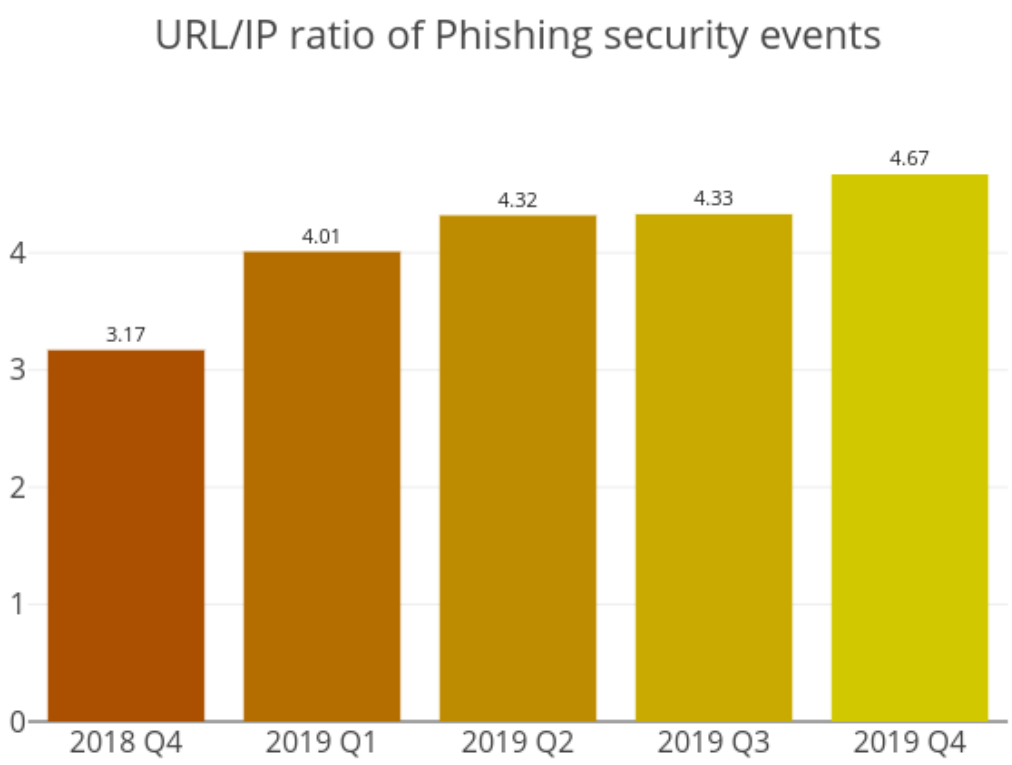


Figure 8: URL/IP ratio of Phishing security events

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

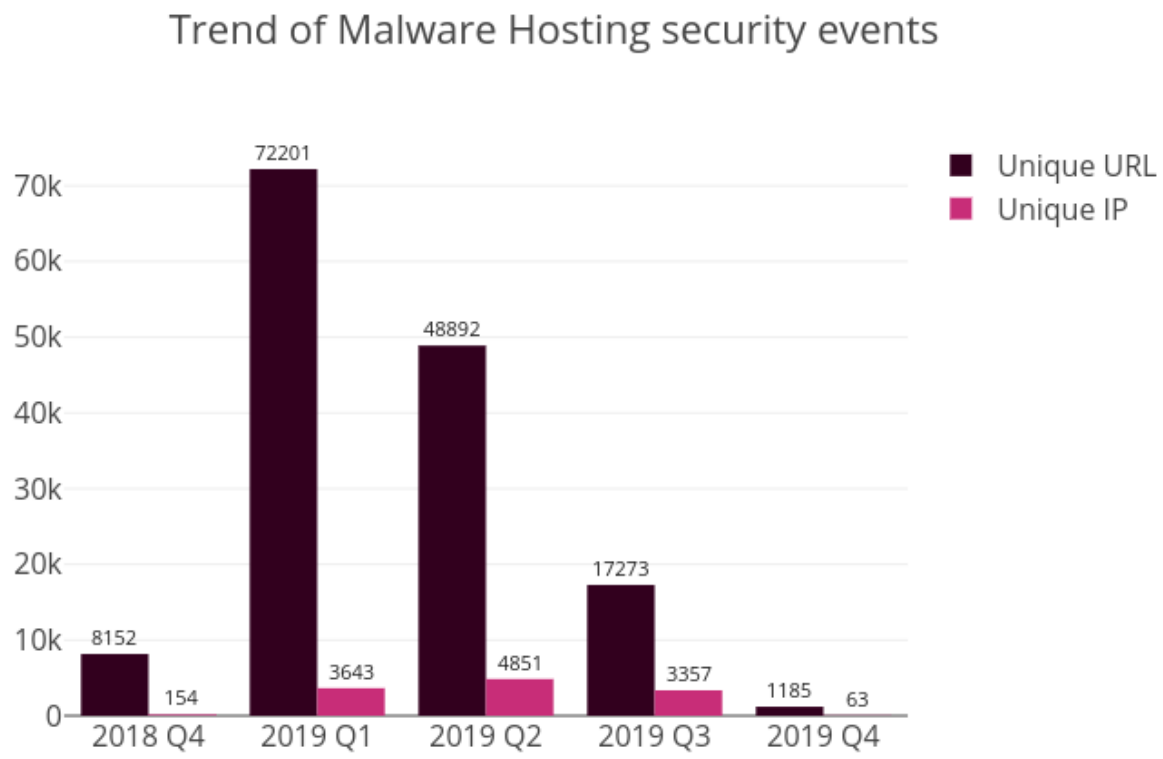


Figure 9: Trend of Malware Hosting security events

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

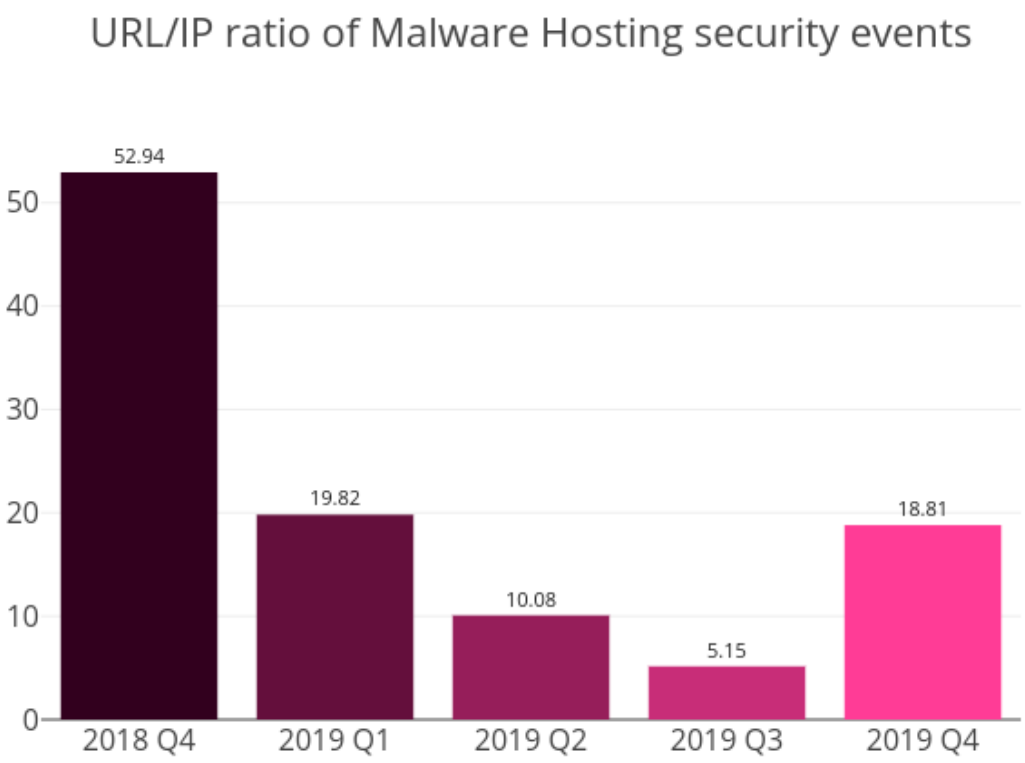


Figure 10: URL/IP ratio of Malware Hosting security events

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:

- Abuse.ch:Zeus Tracker - Binary URL
- CleanMX - Malware
- Malc0de
- MalwareDomainList

# 4 Botnet

## 4.1 Botnets - Command & Control Servers

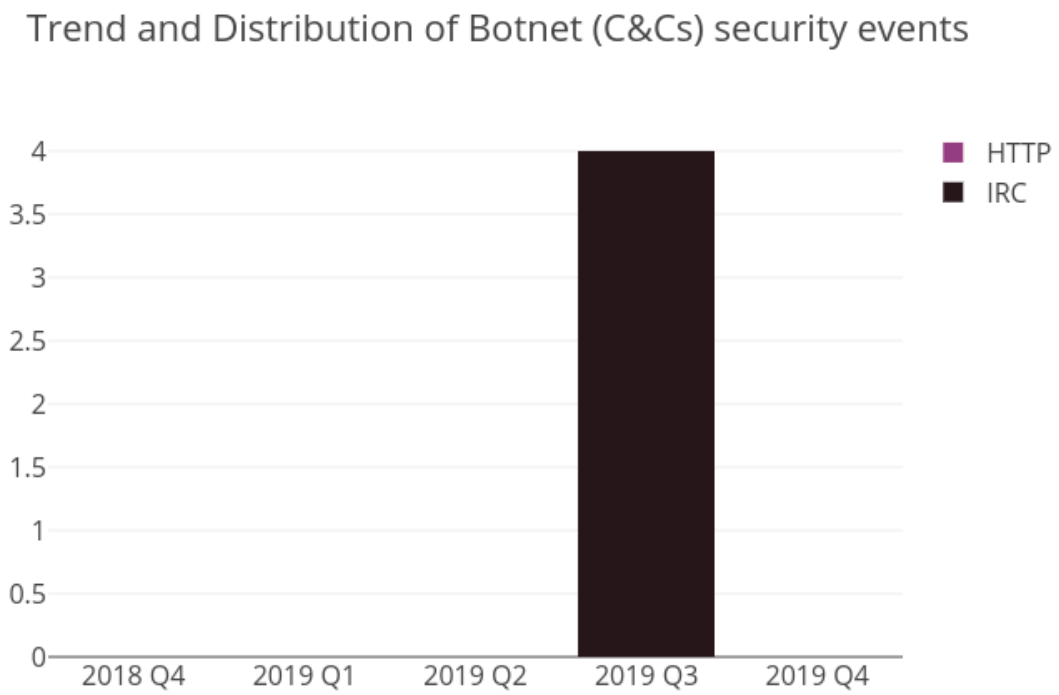


Figure 11: Trend and Distribution of Botnet (C&Cs) security events

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?

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

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.

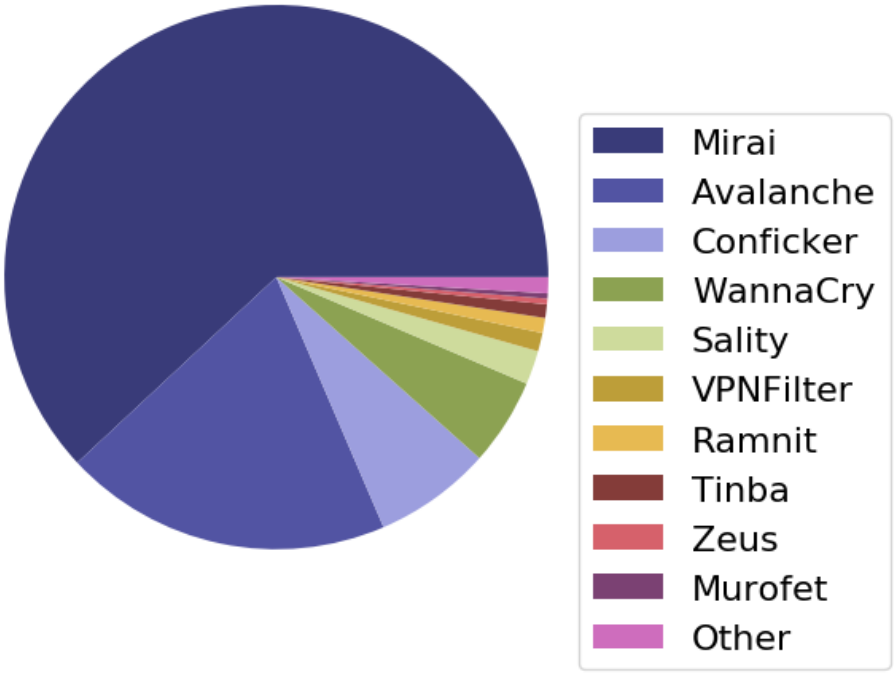


Figure 12: Major Botnet Families in Hong Kong Networks

Table 3: Major Botnet Families in Hong Kong Networks

| Rank | ⇑⇓ | Concerned Bots | Number of Unique IP addresses | Changes with previous period |
|---|---|---|---|---|
| 1 | → | Mirai | 4,231 | -7.9% |
| 2 | ⇑ | Avalanche | 1,333 | 381.2% |
| 3 | → | Conficker | 476 | -6.3% |
| 4 | ⇓ | WannaCry | 354 | -49.2% |
| 5 | ⇑ | Sality | 137 | -7.4% |
| 6 | ⇑ | VPNFilter | 75 | -6.3% |
| 7 | ⇑ | Ramnit | 61 | 24.5% |
| 8 | ⇑ | Tinba | 55 | -9.8% |
| 9 | ⇑ | Zeus | 23 | N/A |
| 10 | ⇑ | Murofet | 21 | -27.6% |

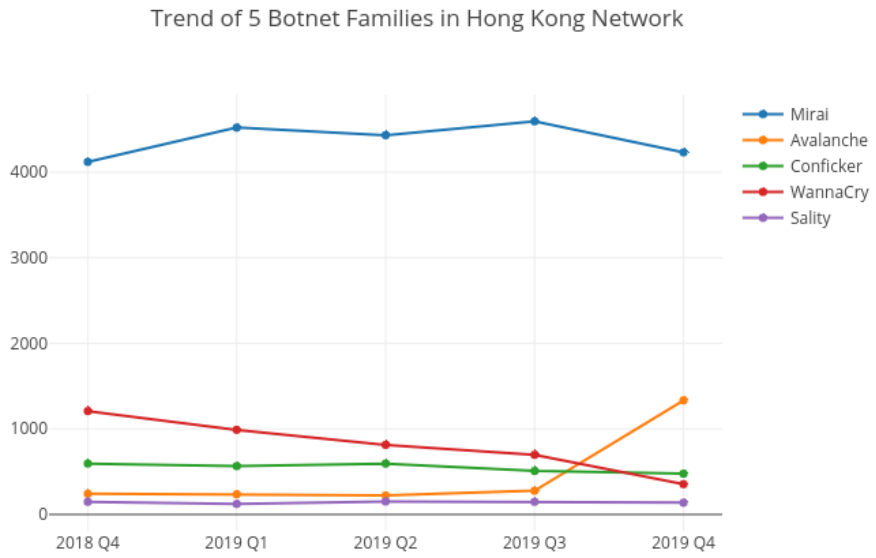


Figure 13: Trend of Top 5 Botnet Families in Hong Kong Network

Table 4: Trend of Top 5 Botnet Families in Hong Kong Network

| Name | 2018 Q4 | 2019 Q1 | 2019 Q2 | 2019 Q3 | 2019 Q4 |
|---|---|---|---|---|---|
| Mirai | 4,120 | 4,521 | 4,432 | 4,594 | 4,231 |
| Avalanche | 241 | 236 | 222 | 277 | 1,333 |
| Conficker | 595 | 565 | 594 | 508 | 476 |
| WannaCry | 1,208 | 989 | 813 | 697 | 354 |
| Sality | 148 | 123 | 152 | 148 | 137 |

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 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 | 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) | 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 | 2020-01-03 |

# 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<br>• host phishing sites<br>• host malware<br>• steal sensitive information |
| Bamital | Nil | Trojan | • drive-by download via exploit kit<br>• via P2P network | • Click fraud<br>• Search hijacking |
| BankPatch | • MultiBanker<br>• Patcher<br>• BankPatcher | Banking Trojan | • via adult web sites<br>• corrupt multimedia codecs<br>• spam e-mail<br>• 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<br>• malvertising | • Click fraud<br>• download other malwares |
| BlackEnergy | Nil | DDoS Trojan | • rootkit techniques to maintain persistence<br>• uses process injection technique<br>• strong encryption and modular architecture | • launch DDoS attacks |
| Citadel | Nil | Banking Trojan | • avoid and disable security tool detection | • steal banking credentials and sensitive information<br>• keystroke logging<br>• screenshot capture<br>• video capture<br>• man-in-the-browser attack<br>• ransomware |
| Conficker | • Downadup<br>• Kido | Worm | • domain generation algorithm (DGA) capability<br>• communicate via P2P network<br>• disable security software | • exploit the Windows Server Service vulnerability (MS08-067)<br>• brute force attacks for admin credential to spread across network<br>• 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<br>• install other malware<br>• 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<br>• send spams |
| Gamarue | • Andromeda | Downloader/ Worm | • via exploit kit<br>• spam e-mail<br>• MS Word macro<br>• removable-drives | • steal sensitive information<br>• allow unauthorised access<br>• install other malware |
| Ghost Push | Nil | Mobile malware | • via app installation | • gain root access<br>• 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<br>• launch DDoS attack<br>• send spams |
| Mirai | Nil | Worm | • telnet with vendor default credentials | • launch DDoS attacks |
| Murofet | Nil | Trojan | • file infection<br>• via exploit kits | • download other malware |
| Nivdort | Nil | Trojan | • spam e-mail | • steal login credentials and sensitive information |
| Nymaim | Nil | Trojan | • spam e-mail | • lock infected systems<br>• encrypt user data<br>• ask for ransom |
| Matsnu | Nil | Trojan | • spam e-mail | • backdoor capabilities that allow unauthorised access<br>• lock infected systems<br>• encrypt user data<br>• ask for ransom |
| Palevo | • Rimecud<br>• Butterfly bot<br>• Pilleuz<br>• Mariposa<br>• Vaklik | Worm | • spread via instant messaging, P2P network and removable drives | • backdoor capabilities that allow unauthorised access<br>• steal login credentials and sensitive information<br>• steal money directly from banks using money mules |

Table 9: Botnet Families (cont.)

| Major Botnets | Alias | Nature | Infection Method | Attacks / Impacts |
|---|---|---|---|---|
| Pushdo | • Cutwail<br>• Pandex | Downloader | • hiding its malicious network traffic<br>• domain generation algorithm (DGA) capability<br>• distribute via drive by download<br>• exploit browser and plugins' vulnerabilities | • download other banking malware (e.g. Zeus and Spyeye)<br>• launch DDoS attacks<br>• send spams |
| Ramnit | Nil | Worm | • file infection<br>• via exploit kits<br>• public FTP servers | • backdoor capabilities that allow unauthorised access<br>• steal login credentials and sensitive information |
| Sality | Nil | Trojan | • rootkit techniques to maintain persistence<br>• communicate via P2P network<br>• spread via removable drives and shares<br>• disable security software<br>• use polymorphic and entry point obscuring (EPO) techniques to infect files | • send spams<br>• proxying of communications<br>• steal sensitive information<br>• compromise web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking)<br>• install other malware |
| Slenfbot | Nil | Worm | • spread via removable drives and shares | • backdoor capabilities that allow unauthorised access<br>• download financial malware<br>• sending spam<br>• launch DDoS attacks |
| Tinba | • TinyBanker<br>• Zusy | Banking Trojan | • via exploit kit<br>• Spam e-mail | • steal banking credential and sensitive information |
| Torpig | • Sinowal<br>• Anserin | Trojan | • rootkit techniques to maintain persistence (Mebroot rootkit)<br>• domain generation algorithm (DGA) capability<br>• distribute via drive by download | • steal sensitive information<br>• 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<br>• launch DDoS attacks<br>• fraud<br>• data theft |
| VPNFilter | Nil | Worm | • possibly exploit device vulnerabilities | • launch network attacks<br>• leak network traffic flowing through the infected devices<br>• disrupt Internet connection |
| WannaCry | • WannaCrypt | Ransomware | • spread across network<br>• exploit Windows SMB vulnerabilities | • encrypt user data<br>• demand ransom<br>• data unrecoverable |
| Wapomi | Nil | Worm | • spread via removable drives and shares<br>• infects executable files | • backdoor capabilities<br>• download and drop additional destructive payloads<br>• alter important files causing unreliable system performance<br>• gather computer activity, transmit private data and cause sluggish computer |
| ZeroAccess | • max++<br>• Sirefef | Trojan | • rootkit techniques to maintain persistence<br>• communicate via P2P network<br>• distribute via drive by download<br>• distribute via disguise as legitimate file (eg. media files, keygen) | • download other malware<br>• bitcoin mining and click fraud |
| Zeus | • Gameover | Banking Trojan | • stealthy techniques to maintain persistence<br>• distribute via drive by download<br>• communicate via P2P network | • steal banking credential and sensitive information<br>• man in the browser attack<br>• keystroke logging<br>• download other malware (eg. Cryptolocker)<br>• launch DDoS attacks |