



Hong Kong Security Watch Report

2019 Q1

Foreword

Better Security Decision with Situational Awareness

Nowadays, a lot of “invisible” compromised systems (computers and other devices) are controlled by attackers with the owner being unaware. The data on these systems may be mined and exposed every day, and the systems may be utilized in different kinds of abuse and criminal activities. The Hong Kong Security Watch Report aims to provide the public a better “visibility” of the situation of the compromised systems in Hong Kong so that they can make better decision in protecting their information security.

The data in this report is about the activities of compromised systems in Hong Kong which suffer from, or participate in various forms of cyber attacks, including web defacement, phishing, malware hosting, botnet command and control centres (C&C) or bots. Computers in Hong Kong are defined as those whose network geolocation is Hong Kong, or the top level domain of their host name is “.hk”.

Capitalizing on the Power of Global Intelligence

This report is the fruit of the collaboration of HKCERT and global security researchers. Many security researchers have the capability to detect attacks targeting their own or their customers’ networks. Some of them provide the information of IP addresses of attack source or web links of malicious activities to other information security organizations with an aim to collaboratively improve the overall security of the cyberspace. They have good practice in sanitizing personal identifiable data before sharing information.

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

We remove duplicated events reported by multiple sources and use the following metrics for measurement to assure the quality of statistics.

Better information better service

We will continue to 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

The content of this report is provided under Creative Commons Attribution 4.0 International License. You may share and adopt the content for any purpose, provided that you attribute the work to HKCERT.

<http://creativecommons.org/licenses/by/4.0>

Contents

| | |
|---|-----------|
| Highlights of Report | 5 |
| Report Details | 10 |
| 1 Defacement | 10 |
| 1.1 Summary | 10 |
| 2 Phishing | 12 |
| 2.1 Summary | 12 |
| 3 Malware Hosting | 14 |
| 3.1 Summary | 14 |
| 4 Botnet | 16 |
| 4.1 Botnets - Command & Control Servers | 16 |
| 4.2 Botnets - Bots | 17 |
| 4.2.1 Major Botnet Families ¹ | 17 |
| Appendix | 19 |
| A Sources of information in IFAS | 20 |
| B Geolocation identification methods in IFAS | 20 |
| C Major Botnet Families | 21 |

¹Major 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 2019 Q1.

In 2019 Q1, there were 80,266 unique security events related to Hong Kong used for analysis in this report. The information is collected with IFAS² from 13 sources of information.³ They are not from the incidents reports received by HKCERT.

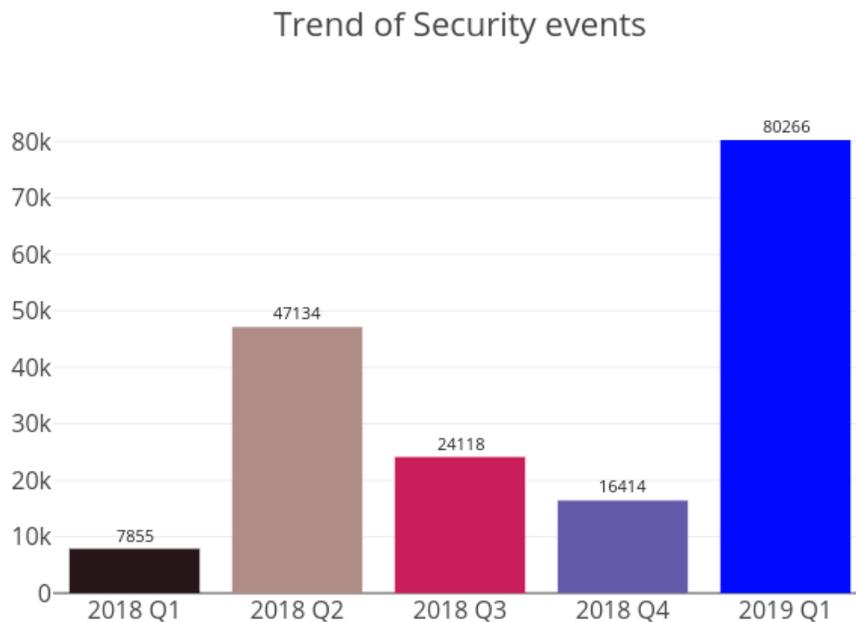


Figure 1: Trend of security events

| Event Type | 2018 Q1 | 2018 Q2 | 2018 Q3 | 2018 Q4 | 2019 Q1 |
|-----------------|---------|---------|---------|---------|---------|
| Defacement | 824 | 1,071 | 5,439 | 590 | 318 |
| Phishing | 634 | 34,391 | 319 | 365 | 289 |
| Malware Hosting | 649 | 4,359 | 7,773 | 8,152 | 72,201 |

The total number of security events in 2019 Q1 sharply increased by 389%, or 63,852 events compared to the previous quarter. While the number of defacement and phishing events showed a downward trend, the number of malware hosting events made a dramatic increase by nearly eight folds over 2018 Q4, which reached the peak of recent years. (See Figure 2)

Server related security events

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

²IFAS - 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.

³Refer to Appendix 1 for the sources of information

Trend and Distribution of server related security events

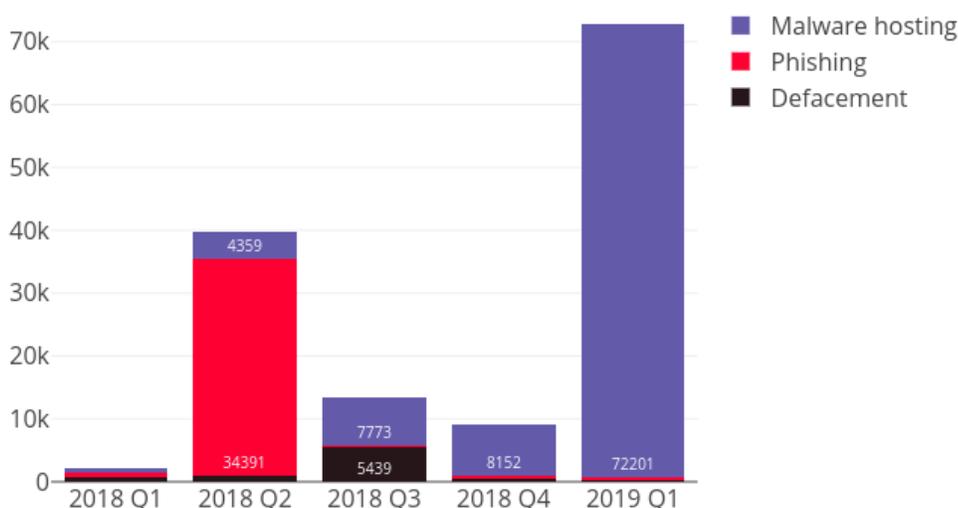


Figure 2: Trend and distribution of server related security events

The number of malware hosting events, each involving a unique malware hosting URL, wildly surge from 8,152 in 2018 Q4 to 72,201 in 2019 Q1, or 786% increase. Although the URL/IP ratio halved to 20, the top two IPs 43.240.13.41 and 45.124.72.40 accounted for 5,366 and 4,586 events respectively. Meanwhile, the number of unique malware hosting IP significantly climbed up from 154 to 3,643.

Based on the log records, there was an intermittent Ramnit campaign started from Mar 2019. The number of events reached a peak of 11,464 on 6 Mar 2019. Part of infected IPs (within same IP block) registered large numbers of similar domain names. It can be seen that those IPs were infected in same network and contributed to massive events. Another phenomenon we noticed that there are 138 IPs involved over 100 unique malware hosting URLs, totally accounted for 53,801, or 75% events. As Ramnit can generate pseudo-random link to host malware, large number of malware hosting URLs were produced. Despite the infected IPs were located in Hong Kong, the major of malware hosting websites came from China. Part of them contained illegal gambling content. The malware campaign did not mainly target Hong Kong. HKCERT has notified the affected operators to clean up their malware hosting links and to find out if there were security vulnerabilities in their servers.

On the other hand, the number of phishing events, each involving a unique phishing URL, slightly dropped from 365 in 2018 Q4 to 289 in 2019 Q1, or a 21% decrease; the involved phishing IP also decreased to 72. At the same time, the number of defacement events also gradually declined to 318 and the URL/IP ratio of defacement remained to 2. In 2019 Q1, both phishing and defacement event amounts are lower than the previous quarters.



- 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:

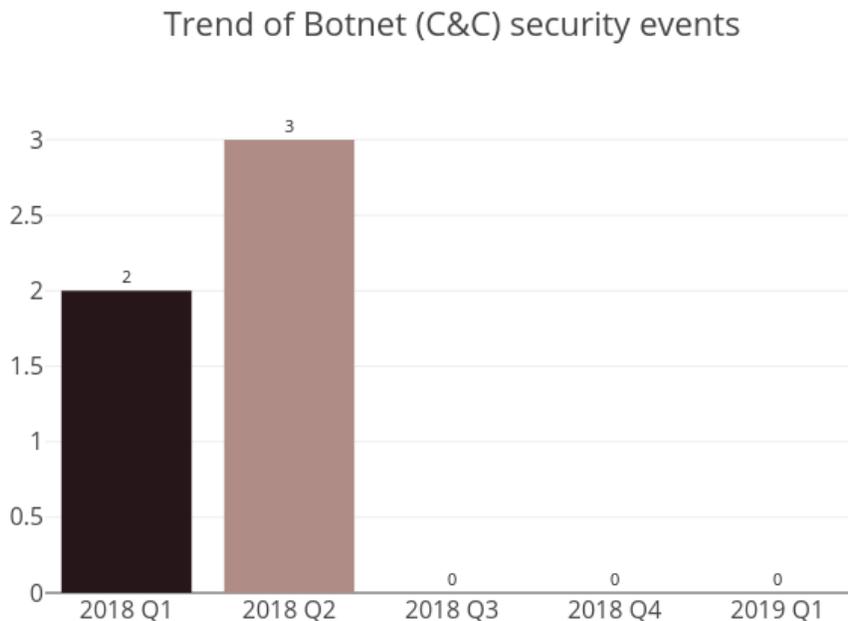


Figure 3: Trend of Botnet (C&Cs) security events

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

Botnet Bots

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

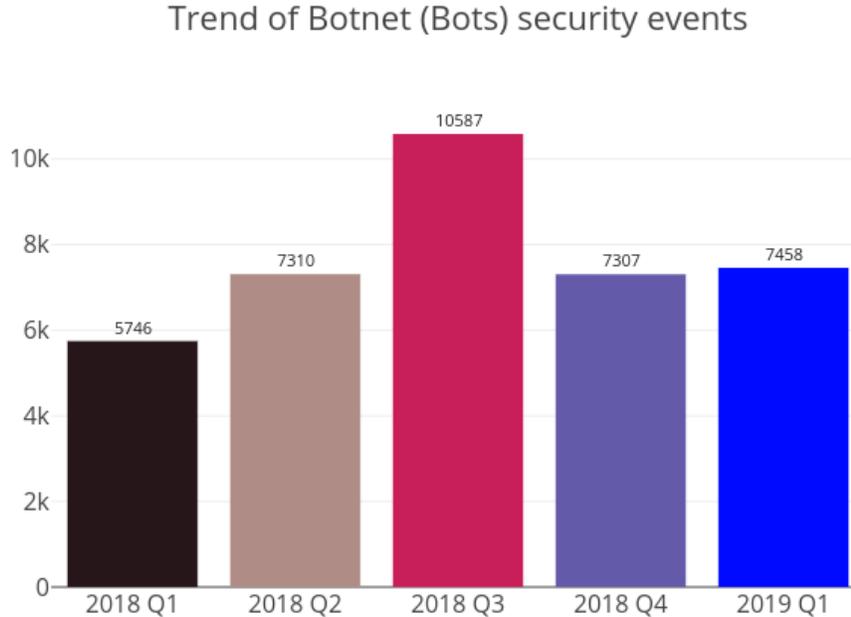


Figure 4: Trend of Botnet (Bots) security events

The number of Botnet (bots) in Hong Kong network only slightly increased by 2% in 2019 Q1. The top five major botnet remained constant, Mirai is still top botnet and accounted for 4,521, or 61% of total events; the second and third botnet family are WannaCry and Conficker, with the number of unique IP address 989 and 565 respectively.

Compared with the last quarter, Gamarue got a significant increase from 1 to 112 unique IP addresses. There are various infection methods of Gamarue, it can spread via USB, email, exploit kit, software installations, etc. HKCERT urges the public to raise their security awareness for protecting their servers and devices.

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, XCodeGhost, 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

Trend of Defacement security events

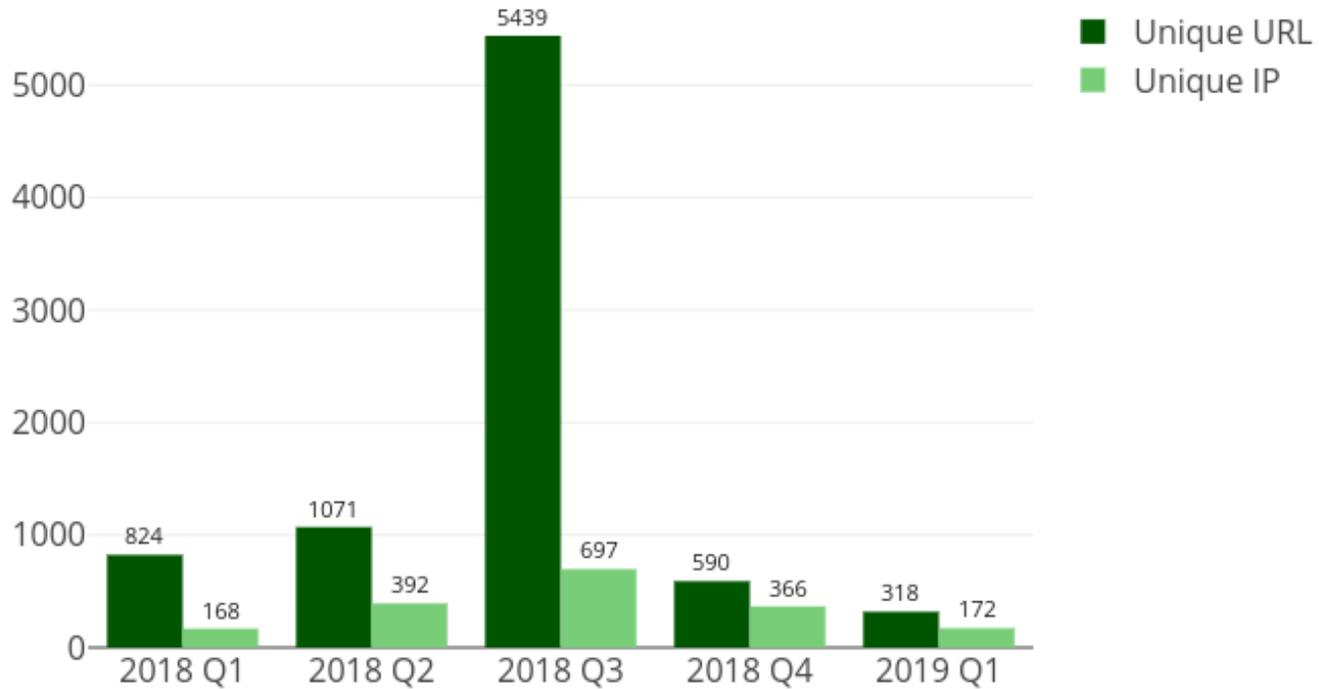


Figure 5: Trend of Defacement security events



What is defacement?

- Defacement is the unauthorized alteration of the content of a legitimate website using hacking method.

What are the potential impacts?

- The integrity of the website content is damaged.
 - Original content might be inaccessible
 - Reputation of the website owner might be damaged
 - Other information stored/processed on the server might be further compromised by the hack to performed other attacks.
-

URL/IP ratio of Defacement security events

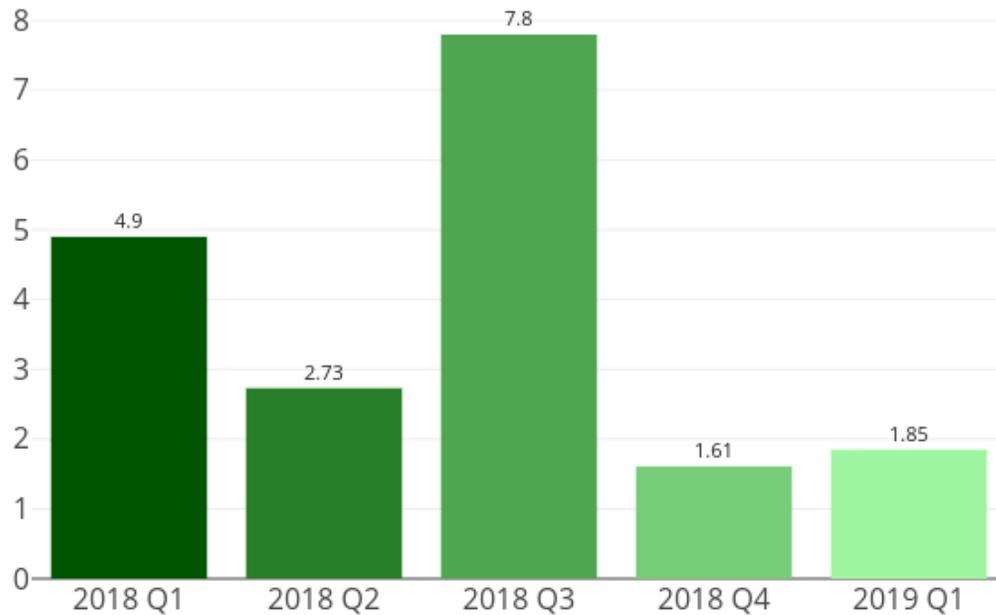


Figure 6: URL/IP ratio of defacement security events



What is URL/IP ratio?

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

What can this ratio indicate?

- Number of events counted in unique URL cannot reflect the number of compromised servers, since one server may contain many URL
- Number of events counted in unique IP address can be better related to the number of compromised servers
- The higher the ratio is, the more mass compromise happened

Sources of Information:

- Zone-H

2 Phishing

2.1 Summary



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 might be stolen, leading to financial loss.
 - Original content might be inaccessible
 - Reputation of the website owner might be damaged
 - Server might be further compromised to perform other attacks
-

URL/IP ratio of Phishing security events

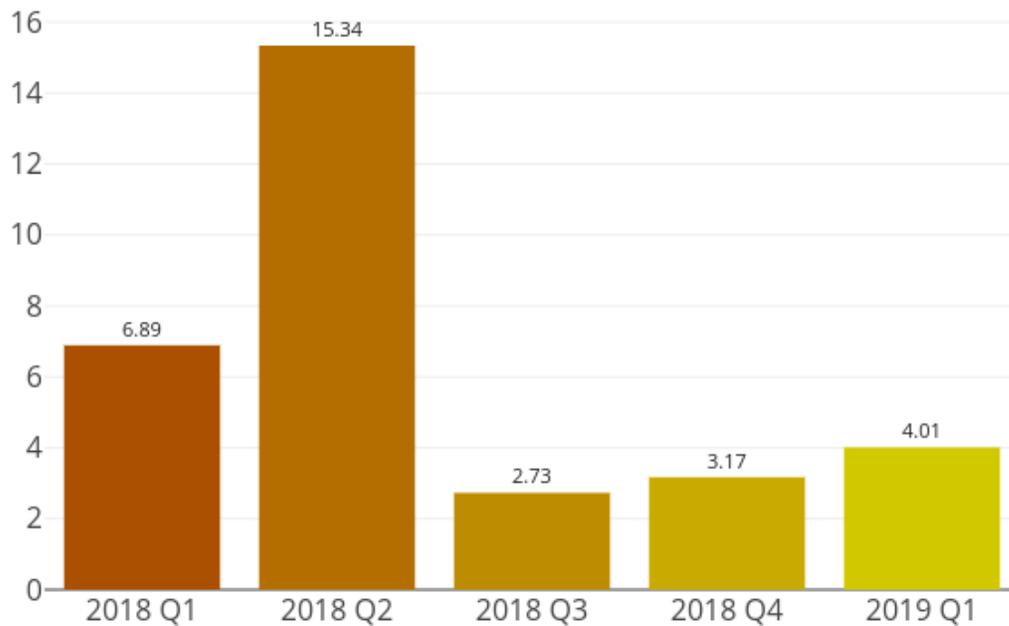


Figure 8: URL/IP ratio of Phishing security events



What is URL/IP ratio?

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

What can this ratio indicate?

- Number of events counted in unique URL cannot reflect the number of compromised servers, since one server may contain many URL
 - Number of events counted in unique IP address can be better related to the number of compromised servers
 - The higher the ratio is, the more mass compromise happened
-

Sources of Information:

- CleanMX - phishing
- Phishtank

3 Malware Hosting

3.1 Summary

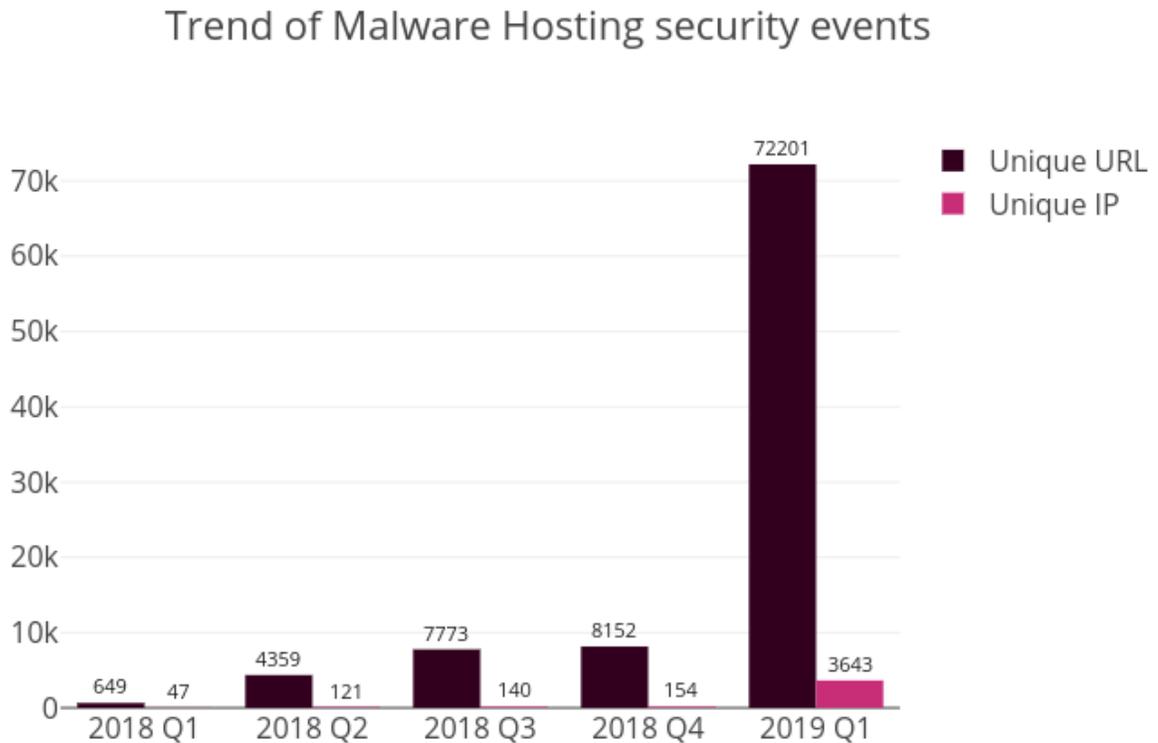


Figure 9: Trend of Malware Hosting security events



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

URL/IP ratio of Malware Hosting security events

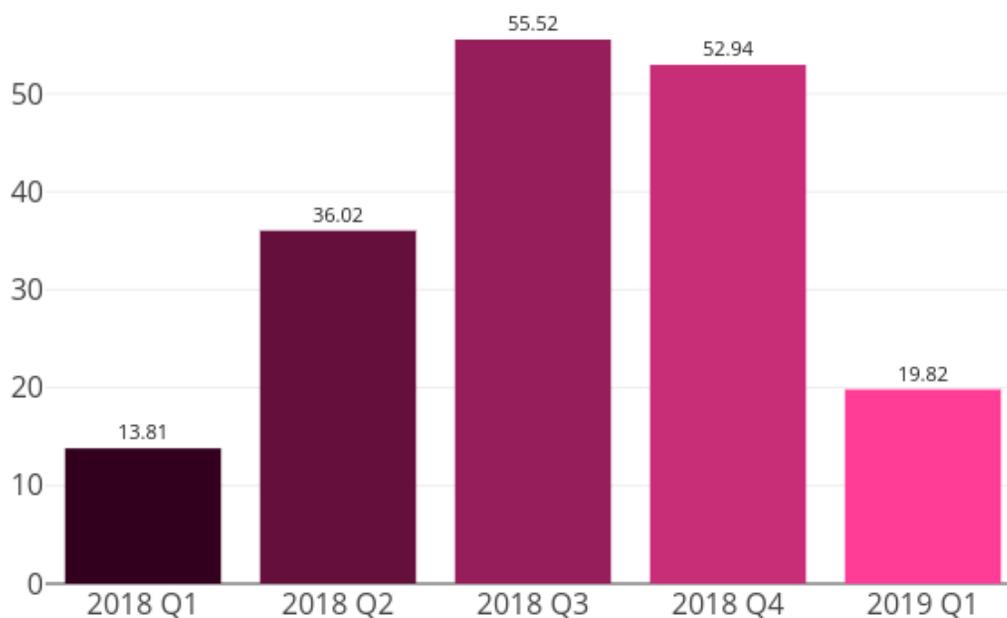


Figure 10: URL/IP ratio of Malware Hosting security events



What is URL/IP ratio?

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

What can this ratio indicate?

- Number of events counted in unique URL cannot reflect the number of compromised servers, since one server may contain many URL
 - Number of events counted in unique IP address can be better related to the number of compromised servers
 - The higher the ratio is, the more mass compromise happened
-

Sources of Information:

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

4 Botnet

4.1 Botnets - Command & Control Servers

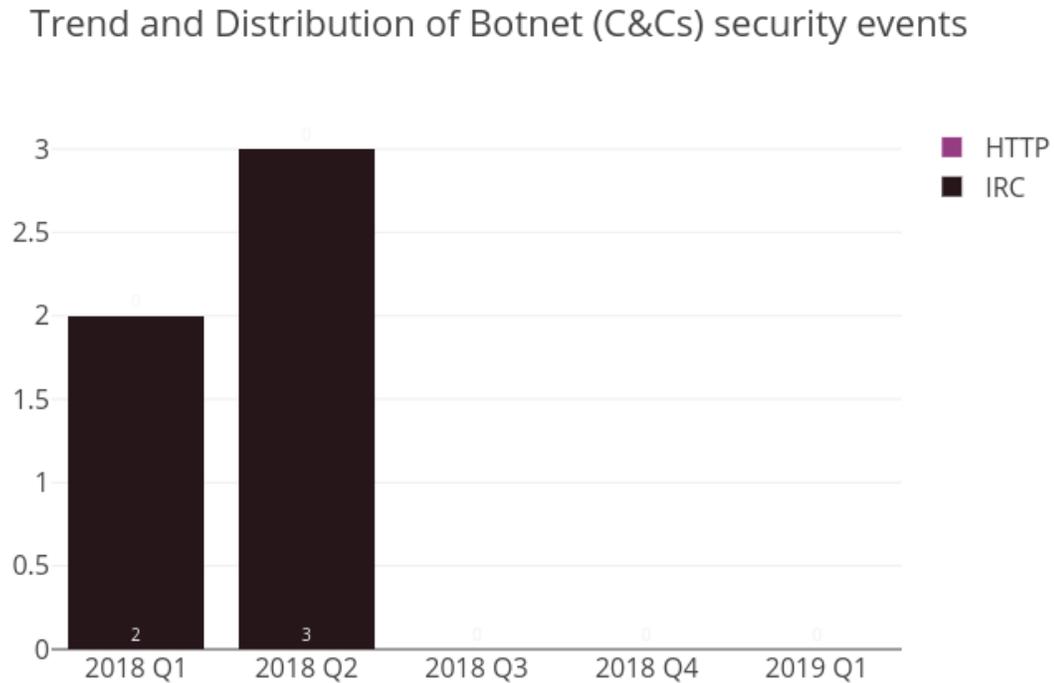


Figure 11: Trend and Distribution of Botnet (C&Cs) security events



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 Families⁴

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.

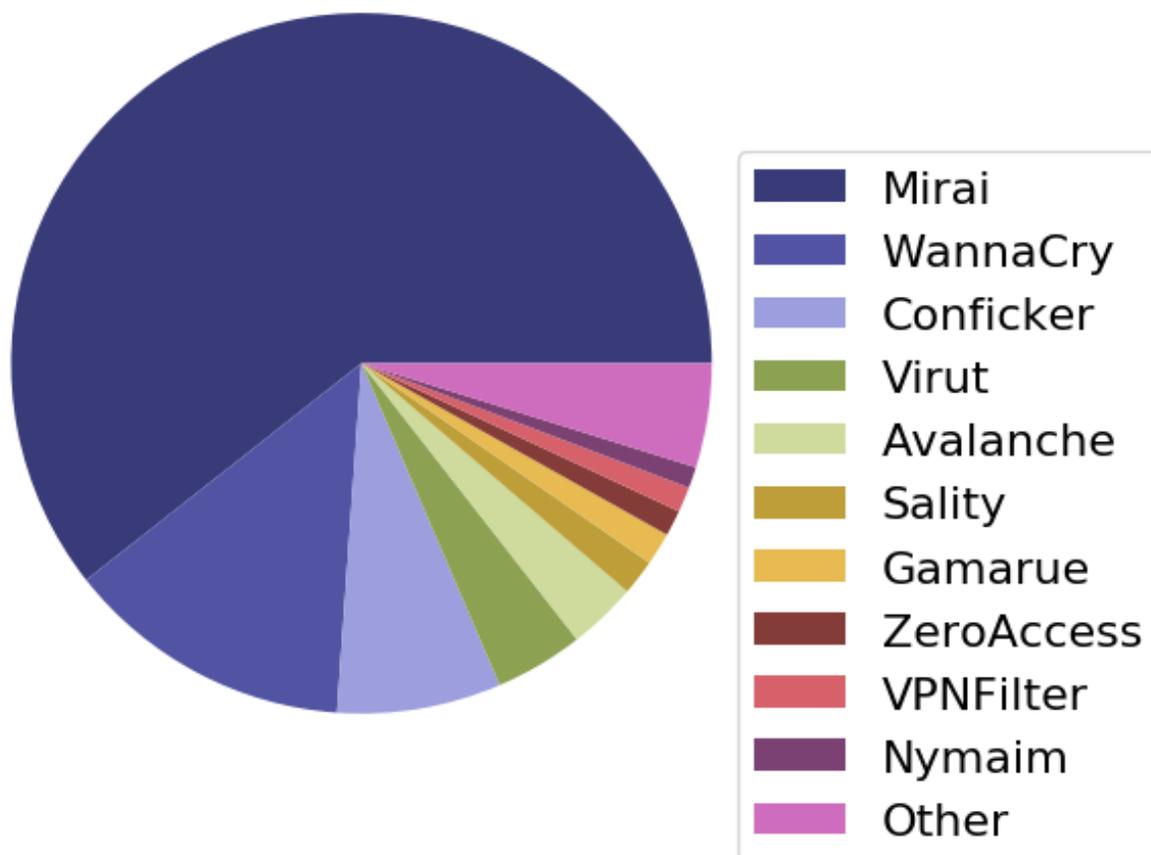


Figure 12: Major Botnet Families in Hong Kong Networks

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

Table 2: Major Botnet Families in Hong Kong Networks

| Rank | ↑↓ | Concerned Bots | Number of Unique IP addresses | Changes with previous period |
|-------------|-----------|-----------------------|--|---|
| 1 | → | Mirai | 4,521 | 9.7% |
| 2 | → | WannaCry | 989 | -18.1% |
| 3 | → | Conficker | 565 | -5.0% |
| 4 | → | Virut | 305 | 9.7% |
| 5 | → | Avalanche | 236 | -2.1% |
| 6 | → | Sality | 123 | -16.9% |
| 7 | ↑ | Gamarue | 112 | 11,100.0% |
| 8 | ↑ | ZeroAccess | 89 | 78.0% |
| 9 | ↓ | VPNFilter | 87 | 3.6% |
| 10 | ↓ | Nymaim | 73 | 15.9% |

Trend of 5 Botnet Families in Hong Kong Network

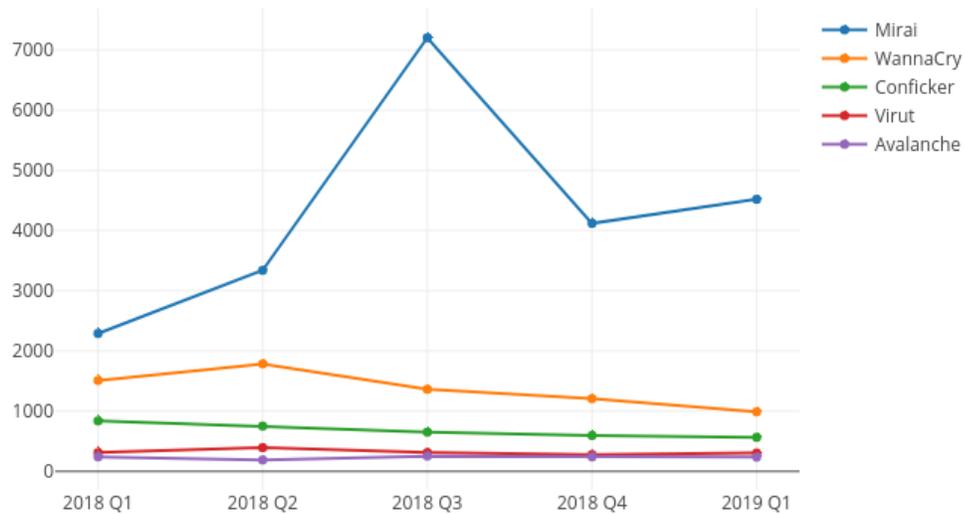


Figure 13: Trend of Top 5 Botnet Families in Hong Kong Network

| Name | 2018 Q1 | 2018 Q2 | 2018 Q3 | 2018 Q4 | 2019 Q1 |
|-----------|---------|---------|---------|---------|---------|
| Mirai | 2,291 | 3,340 | 7,205 | 4,120 | 4,521 |
| WannaCry | 1,510 | 1,786 | 1,364 | 1,208 | 989 |
| Conficker | 838 | 752 | 651 | 595 | 565 |
| Virut | 311 | 394 | 313 | 278 | 305 |
| Avalanche | 241 | 189 | 254 | 241 | 236 |



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:

- 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 | 2019-4-2 |

C Major Botnet Families

Table 5: Botnet Families

| Major Botnets | Alias | Nature | Infection Method | Attacks / Impacts |
|---------------|---|------------------------|--|---|
| Avalanche | Nil | Crimeware-as-a-service | <ul style="list-style-type: none"> • Depends on underlying malwares | <ul style="list-style-type: none"> • send spams • host phishing sites • host malware • steal sensitive information |
| Bamital | Nil | Trojan | <ul style="list-style-type: none"> • drive-by download via exploit kit • via P2P network | <ul style="list-style-type: none"> • Click fraud • Search hijacking |
| BankPatch | <ul style="list-style-type: none"> • MultiBanker • Patcher • BankPatcher | Banking Trojan | <ul style="list-style-type: none"> • via adult web sites • corrupt multimedia codecs • spam e-mail • chat and messaging systems | <ul style="list-style-type: none"> • monitor specific banking websites and harvest user's passwords, credit card information and other sensitive financial data |
| Bedep | Nil | Trojan | <ul style="list-style-type: none"> • via adult web sites • malvertising | <ul style="list-style-type: none"> • Click fraud • download other malwares |
| BlackEnergy | Nil | DDoS Trojan | <ul style="list-style-type: none"> • rootkit techniques to maintain persistence • uses process injection technique • strong encryption and modular architecture | <ul style="list-style-type: none"> • launch DDoS attacks |
| Citadel | Nil | Banking Trojan | <ul style="list-style-type: none"> • avoid and disable security tool detection | <ul style="list-style-type: none"> • steal banking credentials and sensitive information • keystroke logging • screenshot capture • video capture • man-in-the-browser attack • ransomware |
| Conficker | <ul style="list-style-type: none"> • Downadup • Kido | Worm | <ul style="list-style-type: none"> • domain generation algorithm (DGA) capability • communicate via P2P network • disable security software | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • via droppers | <ul style="list-style-type: none"> • steal sensitive information • install other malware • backdoor capabilities that allow unauthorized access |
| Dyre | Nil | Banking Trojan | <ul style="list-style-type: none"> • spam e-mail | <ul style="list-style-type: none"> • steal banking credential by tricking the victim to call an illegitimate number • send spams |
| Gamarue | <ul style="list-style-type: none"> • Andromeda | Downloader/ Worm | <ul style="list-style-type: none"> • via exploit kit • spam e-mail • MS Word macro • removable-drives | <ul style="list-style-type: none"> • steal sensitive information • allow unauthorized access • install other malware |
| Ghost Push | Nil | Mobile malware | <ul style="list-style-type: none"> • via app installation | <ul style="list-style-type: none"> • gain root access • download other malware |
| Glupteba | Nil | Trojan | <ul style="list-style-type: none"> • drive-by download via Blackhole Exploit Kit | <ul style="list-style-type: none"> • push contextual advertising and clickjacking to victims |
| IRC Botnet | Nil | Trojan | <ul style="list-style-type: none"> • communicate via IRC network | <ul style="list-style-type: none"> • backdoor capabilities that allow unauthorized access • launch DDoS attack • send spams |
| Mirai | Nil | Worm | <ul style="list-style-type: none"> • telnet with vendor default credentials | <ul style="list-style-type: none"> • launch DDoS attacks |
| Murofet | Nil | Trojan | <ul style="list-style-type: none"> • file infection • via exploit kits | <ul style="list-style-type: none"> • download other malware |
| Nivdort | Nil | Trojan | <ul style="list-style-type: none"> • spam e-mail | <ul style="list-style-type: none"> • steal login credentials and sensitive information |
| Nymaim | Nil | Trojan | <ul style="list-style-type: none"> • spam e-mail • malicious link | <ul style="list-style-type: none"> • lock infected systems • stop victims from accessing files • ask for ransom |
| Palevo | <ul style="list-style-type: none"> • Rimecud • Butterfly bot • Pilleuz • Mariposa • Vaklik | Worm | <ul style="list-style-type: none"> • spread via instant messaging, P2P network and removable drives | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • Cutwail • Pandex | Downloader | <ul style="list-style-type: none"> • hiding its malicious network traffic • domain generation algorithm (DGA) capability • distribute via drive by download • exploit browser and plugins' vulnerabilities | <ul style="list-style-type: none"> • download other banking malware (e.g. Zeus and Spyeye) • launch DDoS attacks • send spams |
| Ramnit | Nil | Worm | <ul style="list-style-type: none"> • file infection • via exploit kits • public FTP servers | <ul style="list-style-type: none"> • backdoor capabilities that allow unauthorized access • steal login credentials and sensitive information |
| Sality | Nil | Trojan | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • 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 | <ul style="list-style-type: none"> • spread via removable drives and shares | <ul style="list-style-type: none"> • backdoor capabilities that allow unauthorized access • download financial malware • sending spam • launch DDoS attacks |
| Tinba | <ul style="list-style-type: none"> • TinyBanker • Zusy | Banking Trojan | <ul style="list-style-type: none"> • via exploit kit • Spam e-mail | <ul style="list-style-type: none"> • steal banking credential and sensitive information |
| Torpig | <ul style="list-style-type: none"> • Sinowal • Anserin | Trojan | <ul style="list-style-type: none"> • rootkit techniques to maintain persistence (Mebrook rootkit) • domain generation algorithm (DGA) capability • distribute via drive by download | <ul style="list-style-type: none"> • steal sensitive information • man in the browser attack |

Table 8: Botnet Families (cont.)

| Major Botnets | Alias | Nature | Infection Method | Attacks / Impacts |
|---------------|--|----------------|---|--|
| Virut | Nil | Trojan | <ul style="list-style-type: none"> spread via removable drives and shares | <ul style="list-style-type: none"> send spams launch DDoS attacks fraud data theft |
| VPNFilter | Nil | Worm | <ul style="list-style-type: none"> possibly exploit device vulnerabilities | <ul style="list-style-type: none"> launch network attacks leak network traffic flowing through the infected devices disrupt Internet connection |
| WannaCry | <ul style="list-style-type: none"> WannaCrypt | Ransomware | <ul style="list-style-type: none"> spread across network exploit Windows SMB vulnerabilities | <ul style="list-style-type: none"> encrypt user data demand ransom data unrecoverable |
| Wapomi | Nil | Worm | <ul style="list-style-type: none"> spread via removable drives and shares infects executable files | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> max++ Sirefef | Trojan | <ul style="list-style-type: none"> rootkit techniques to maintain persistence communicate via P2P network distribute via drive by download distribute via disguise as legitimate file (eg. media files, keygen) | <ul style="list-style-type: none"> download other malware bitcoin mining and click fraud |
| Zeus | <ul style="list-style-type: none"> Gameover | Banking Trojan | <ul style="list-style-type: none"> stealthy techniques to maintain persistence distribute via drive by download communicate via P2P network | <ul style="list-style-type: none"> steal banking credential and sensitive information man in the browser attack keystroke logging download other malware (eg. Cryptolocker) launch DDoS attacks |