



# Hong Kong Security Watch Report

2018 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](mailto: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

<b>Highlights of Report</b>	<b>5</b>
<b>Report Details</b>	<b>10</b>
<b>1 Defacement</b>	<b>10</b>
1.1 Summary . . . . .	10
<b>2 Phishing</b>	<b>12</b>
2.1 Summary . . . . .	12
<b>3 Malware Hosting</b>	<b>14</b>
3.1 Summary . . . . .	14
<b>4 Botnet</b>	<b>16</b>
4.1 Botnets - Command & Control Servers . . . . .	16
4.2 Botnets - Bots . . . . .	17
4.2.1 Major Botnet Families <sup>1</sup> . . . . .	17
<b>Appendix</b>	<b>18</b>
<b>A Sources of information in IFAS</b>	<b>19</b>
<b>B Geolocation identification methods in IFAS</b>	<b>19</b>
<b>C Major Botnet Families</b>	<b>20</b>

---

<sup>1</sup>Major Botnet Families are selected botnet families with considerable amount of security events reported from the information sources constantly across the reporting period.

## Highlight of Report

This report is for 2018 Q1.

In 2018 Q1, there were 7,855 unique security events related to Hong Kong used for analysis in this report. The information is collected with IFAS<sup>2</sup> from 19 sources of information.<sup>3</sup> They are not from the incidents reports received by HKCERT.

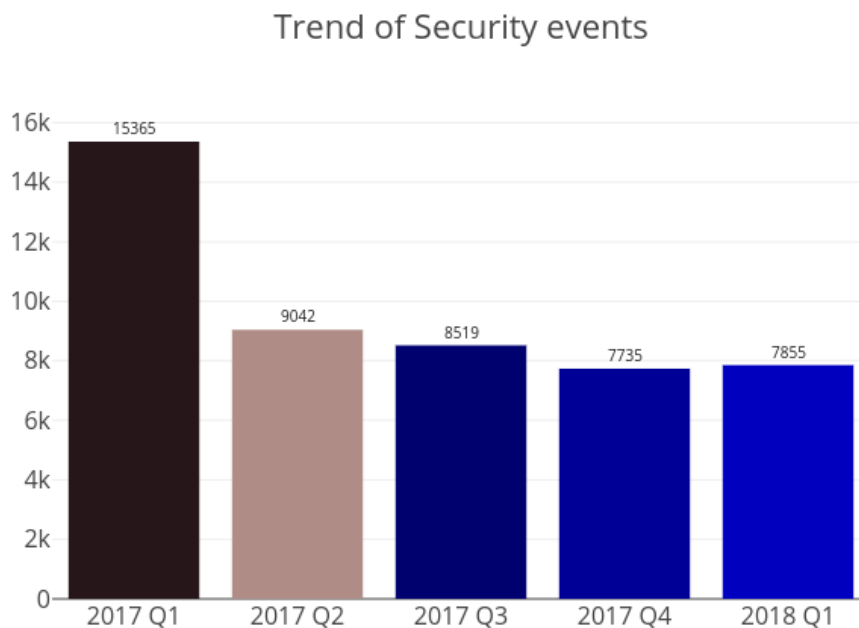


Figure 1: Trend of security events

The total number of security events in 2018 Q1 increased by 1.5% or 120 events compared to the previous quarter. The decreases in Malware hosting and Defacement events were compensated by the increase of Botnet events. Even though the number of events was increased slightly, the trend of security events is stable in the last half year.

### Server related security events

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

---

<sup>2</sup>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.

<sup>3</sup>Refer to Appendix 1 for the sources of information

## Trend and Distribution of server related security events

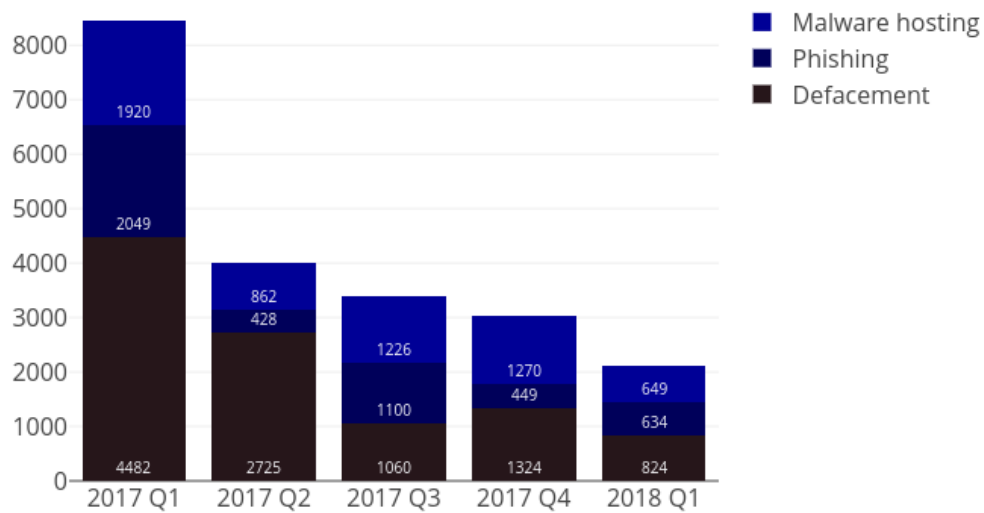


Figure 2: Trend and distribution of server related security events

The number of server related security events decreased from 3,043 to 2,107 (decreased by 31%) in this quarter. Though the overall count decreased, the number of Phishing was actually increased by 41%. If comparing with all quarters in 2017, the number of events is in decreasing trend, with the number of defacement events drops significantly during the year.

The URL/IP ratio of malware hosting events dropped from a very high value of 16 in the last quarter to 14 in this quarter, with the number of unique URL dropped sharply from 1,270 to 649, or by 49%, and the number of unique IP continued to decrease from 77 to 47, or by 39%. When comparing this quarter with all quarters in 2017, it can be seen that the number of unique IP decreased from 369 in 2017 Q1 to 97 in 2017 Q2, and then continued to decrease to 77 in 2017 Q4 and 47 in 2018 Q1 respectively. That means fewer servers are used for malware hosting.

---

*HKCERT urges system and application administrators to protect the servers*

---



- patch server up-to-date to avoid the known vulnerabilities being exploited
  - update web application and plugins to the latest version
  - follow best practice on user account and password management
  - implement validation check for user input and system output
  - provide strong authentication e.g. two factor authentication, administrative control interface
  - acquire information security knowledge to prevent social engineering
-

## Botnet related security events

Botnet related security events can be classified into two categories:

- Botnet Command and Control Centers (C&C) security events - involving small number of powerful computers, mostly servers, which give commands to bots
- Botnet security events - involving large number of computers, mostly home computers which receive commands from C&Cs.

### Botnet Command and Control Servers

The trend of botnet C&C security events is summarized below:

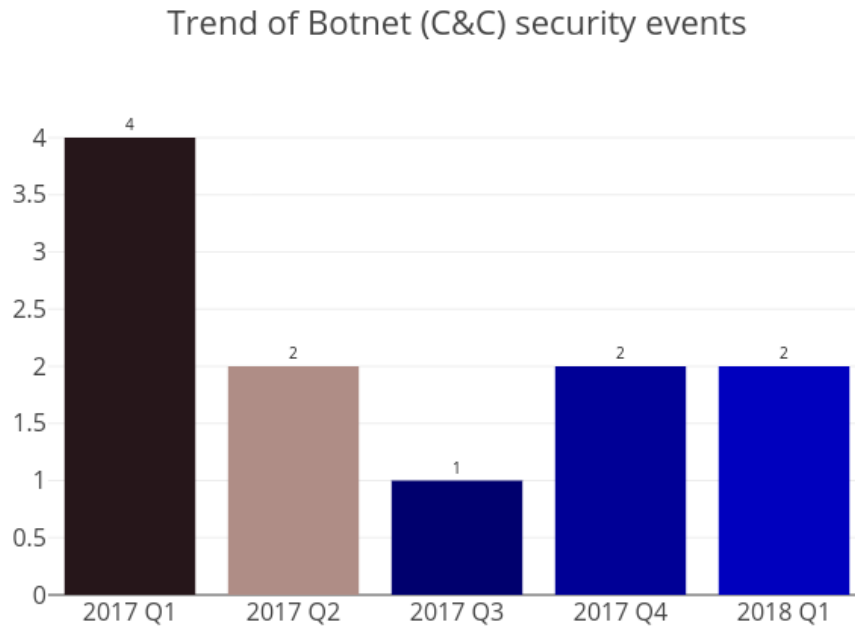


Figure 3: Trend of Botnet (C&Cs) security events

The number of botnet Command and Control Servers remained unchanged in 2 in this quarter. Both of them were identified as an IRC bot C&C server.

### Botnet Bots

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

## Trend of Botnet (Bots) security events

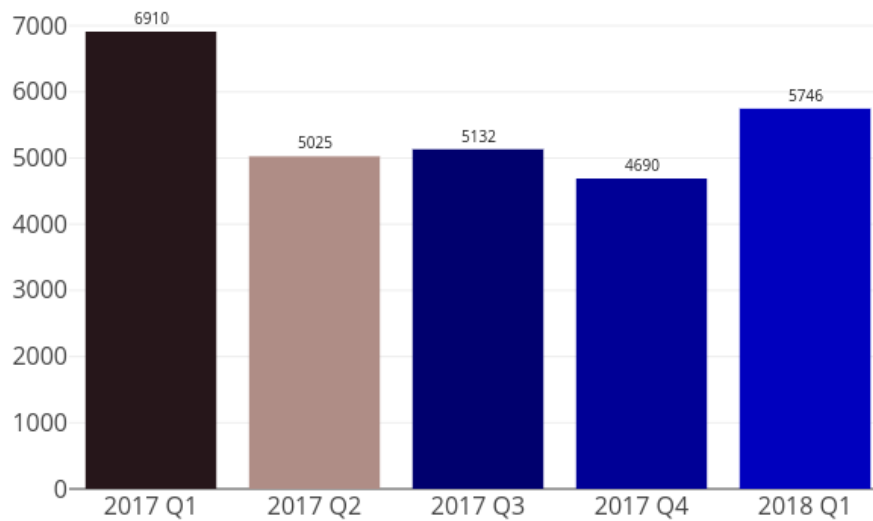


Figure 4: Trend of Botnet (Bots) security events

The number of Botnet (bots) in Hong Kong network increased by 23% in 2018 Q1. Mirai contributed to the increase of total count of Botnets by 275% and thus, this family takes the first place in the rank of Major Botnet Families in Hong Kong Networks. On the other hand, the count of WannaCry family is decreased by 25%, and thus, this family becomes the second in the rank. There is a note that Virut has increased by 6120%, with the number of unique IP address increased from 5 in 2017 Q4 to 311 in 2018 Q1.

Mirai botnet became active at the end of 2016. Global security organizations started to clean up in 2017 Q1. The number of events dropped sharply from 2,493 in Q1 to 746 in Q2 and steadily decreased in Q3 and Q4. That means Mirai botnet is on a decrease trend. But we note that since the end of 2017, there is an increase of Mirai events. We regularly saw reports on Mirai variants or recent attacks, but cannot confirm the increase is related to these variants and attacks. HKCERT will keep monitoring on the trend and continue the cleanup.

WannaCry ransomware outbreak occurred in May 2017. The WannaCry-bots are machines infected by WannaCry ransomware with the encryption mechanism not activated. HKCERT had handled 1,210 cases for WannaCry-bot in 2017 to try to clean up these machines infected by malware.

Virut botnet became active in 2006 and in 2013, its operations were disrupted by the Polish organization Naukowa i Akademicka Sie Komputerowa. According to security researcher<sup>4</sup>, its comeback was related to a recent campaign delivering 'Avzhan DDoS bot'. The researcher found that the server used for attack was infected with Virut, which was therefore attached on Avzhan and infected the targets.

### WannaCry

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

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

<sup>4</sup><https://blog.malwarebytes.com/threat-analysis/2018/03/blast-from-the-past-stowaway-virut-delivered-with-chinese-ddos-bot/>



network.

---

*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

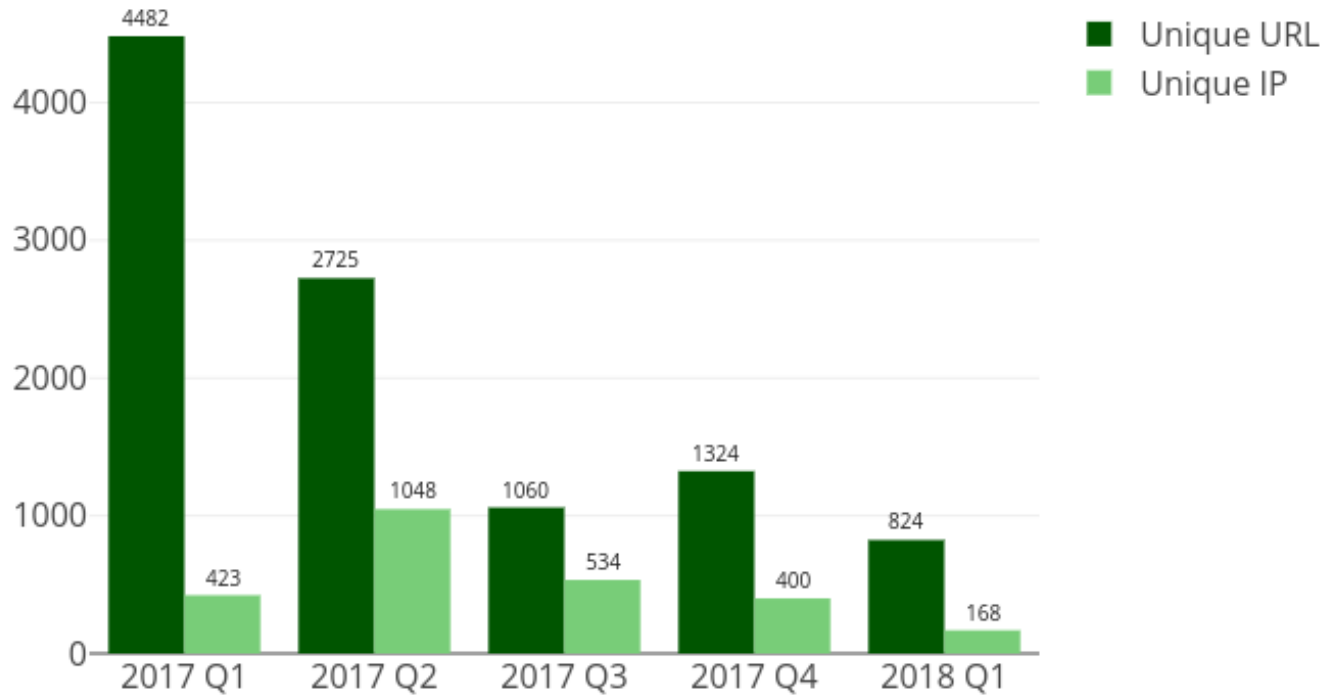


Figure 5: Trend of Defacement security events



---

#### 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

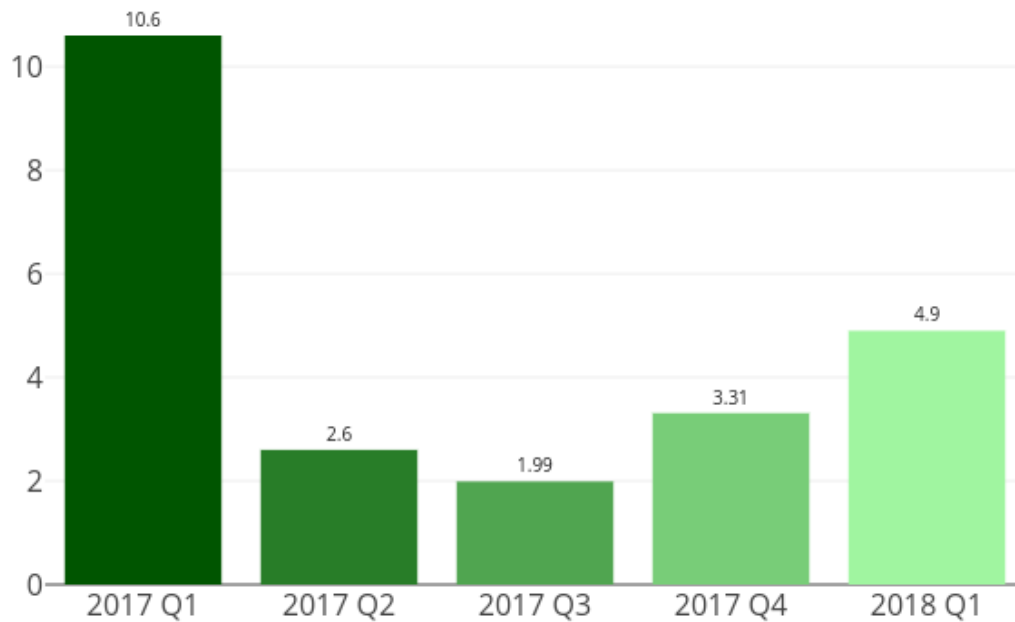


Figure 6: URL/IP ratio of defacement security events



---

### 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 Defacement security events



---

#### What is Phishing?

---

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

---

#### What are the potential impacts?

---

- Personal information or 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

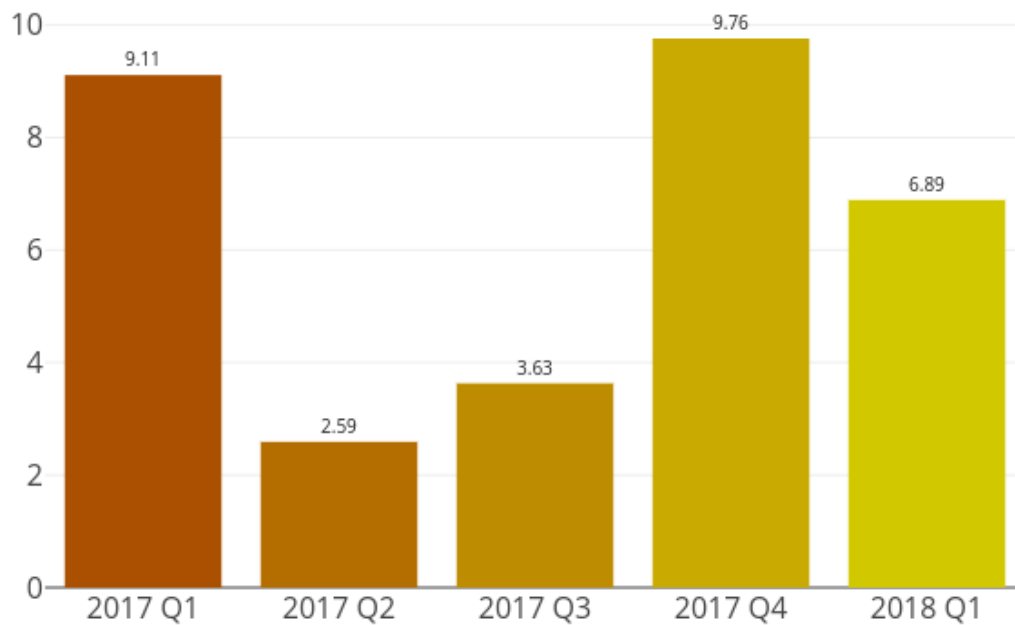


Figure 8: URL/IP ratio of Phishing security events



---

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

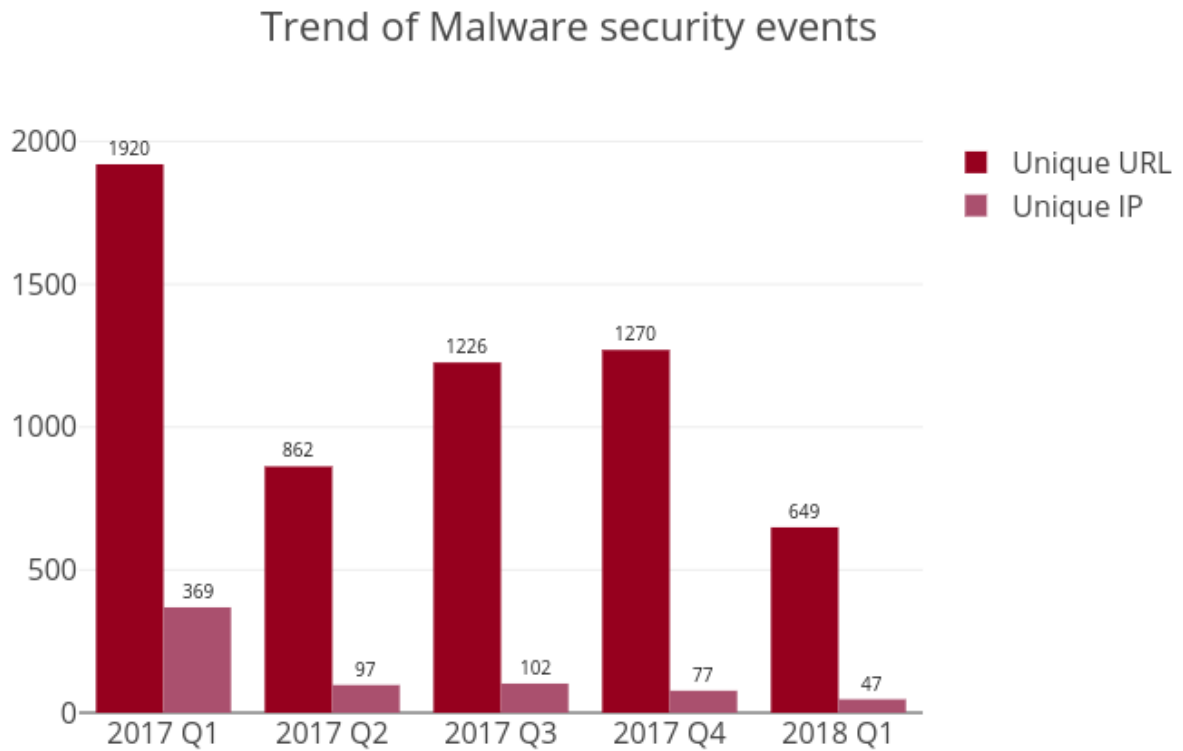


Figure 9: Trend of Malware Hosting security events



---

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 security events

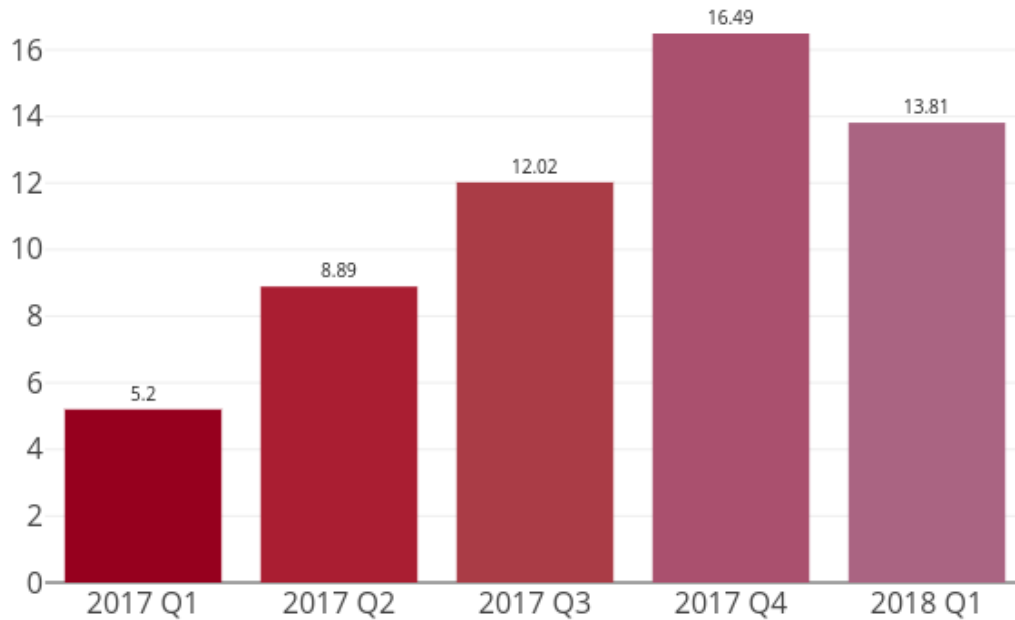


Figure 10: URL/IP ratio of Malware Hosting security events



---

### 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

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

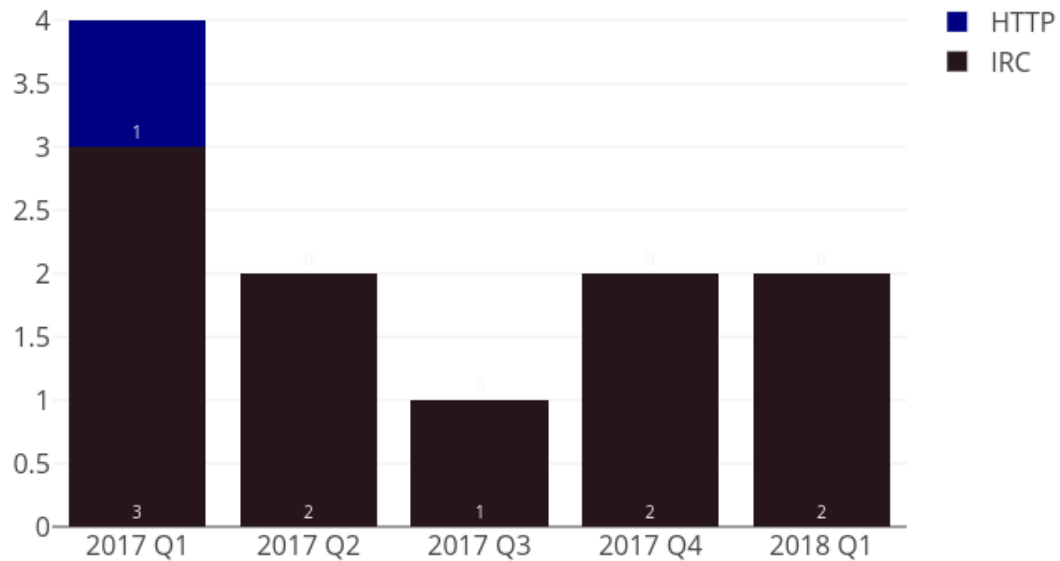


Figure 11: Trend and Distribution of Botnet (C&Cs) security events



---

#### 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<sup>5</sup>

Individual botnet's size is calculated from the maximum of the daily counts of unique IP address attempting to connect to the botnet in the report period. In other words, the real botnet size should be larger because not all bots are powered on the same day.

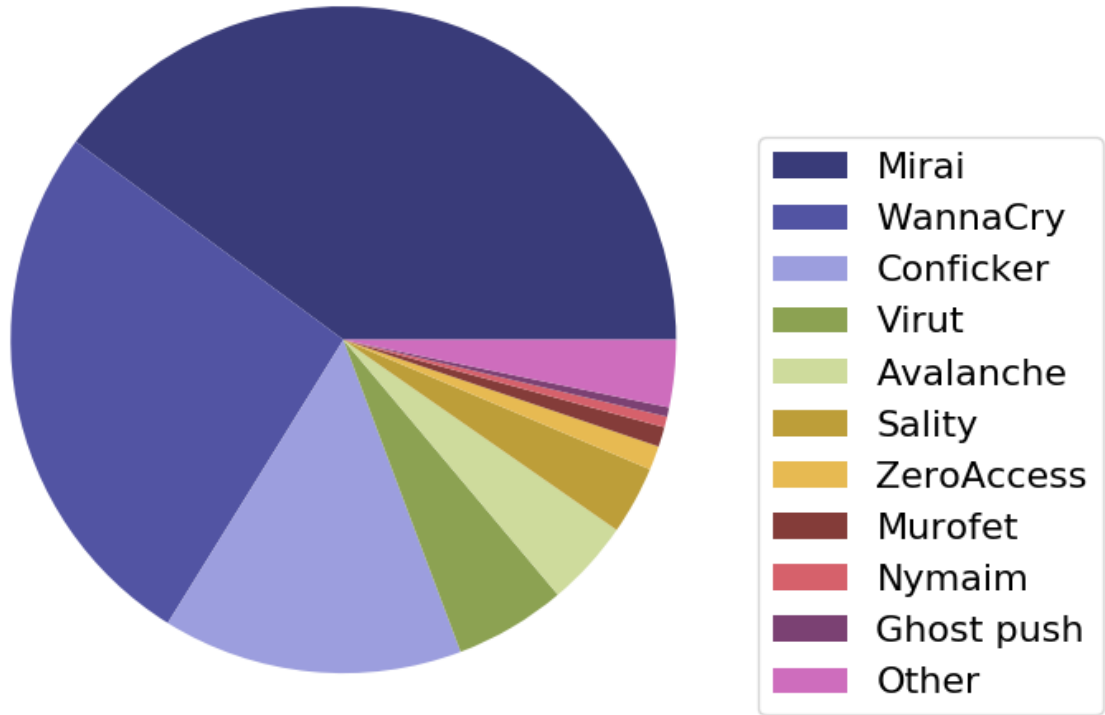


Figure 12: Major Botnet Families in Hong Kong Networks

Table 2: Major Botnet Families in Hong Kong Networks

Rank	↑↓	Concerned Bots	Number of Unique IP addresses	Changes with previous period
1	↑	Mirai	2291	275.0%
2	↓	WannaCry	1510	-24.5%
3	↓	Conficker	838	-29.0%
4	↑	Virut	311	6120.0%
5	↓	Avalanche	241	-2.0%
6	↓	Sality	190	11.8%
7	↓	ZeroAccess	67	-21.2%
8	↓	Murofet	55	-16.7%
9	↑	Nymaim	30	11.1%
10	↓	Ghost push	26	-18.8%

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

Trend of 5 Botnet Families in Hong Kong Network

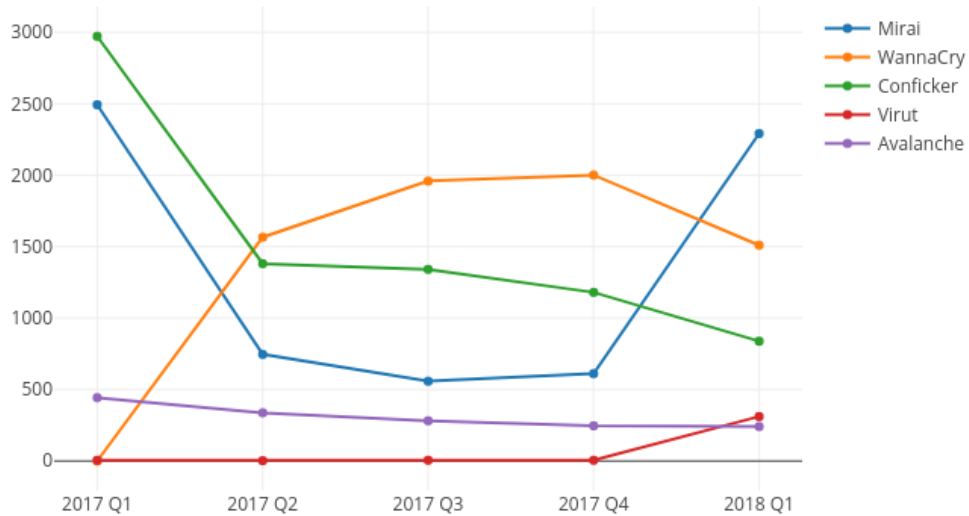


Figure 13: Trend of Top 5 Botnet Families in Hong Kong Network

Name	2017 Q1	2017 Q2	2017 Q3	2017 Q4	2018 Q1
Mirai	2493	746	558	611	2291
WannaCry	0	1566	1959	2001	1510
Conficker	2972	1381	1341	1180	838
Virut	5	2	5	5	311
Avalanche	443	337	281	246	241




---

#### 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

<b>Event Type</b>	<b>Source</b>	<b>First introduced</b>
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

Since 2017 Q4, the following information sources are confirmed retired, so they will be removed from IFAS.

Table 4: IFAS Sources of Information obsoleted

<b>Event Type</b>	<b>Source</b>
Phishing	ArborNetwork: Atlas SRF-Phishing
Phishing	Millersmiles
Malware Hosting	Abuse.ch: SpyEye Tracker - Binary URL
Malware Hosting	Savour.cn
Botnet (C&Cs)	Abuse.ch: SpyEye Tracker - C&Cs
Botnet (Bots)	Arbor Network: Atlas SRF-Conficker

### B Geolocation identification methods in IFAS

We use the following methods to identify if a network’s geolocation is in Hong Kong:

Table 5: Methods of Geolocation Identification

<b>Method</b>	<b>First introduced</b>	<b>Last update</b>
Maxmind	2013-04	2018-03-27

## C Major Botnet Families

Table 6: Botnet Families

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Avalanche	Nil	Crimeware-as-a-service	<ul style="list-style-type: none"> <li>• Depends on underlying malwares</li> </ul>	<ul style="list-style-type: none"> <li>• send spams</li> <li>• host phishing sites</li> <li>• host malware</li> <li>• steal sensitive information</li> </ul>
Bamital	Nil	Trojan	<ul style="list-style-type: none"> <li>• drive-by download via exploit kit</li> <li>• via P2P network</li> </ul>	<ul style="list-style-type: none"> <li>• Click fraud</li> <li>• Search hijacking</li> </ul>
BankPatch	<ul style="list-style-type: none"> <li>• MultiBanker</li> <li>• Patcher</li> <li>• BankPatcher</li> </ul>	Banking Trojan	<ul style="list-style-type: none"> <li>• via adult web sites</li> <li>• corrupt multimedia codecs</li> <li>• spam e-mail</li> <li>• chat and messaging systems</li> </ul>	<ul style="list-style-type: none"> <li>• monitor specific banking websites and harvest user's passwords, credit card information and other sensitive financial data</li> </ul>
Bedep	Nil	Trojan	<ul style="list-style-type: none"> <li>• via adult web sites</li> <li>• malvertising</li> </ul>	<ul style="list-style-type: none"> <li>• Click fraud</li> <li>• download other malwares</li> </ul>
BlackEnergy	Nil	DDoS Trojan	<ul style="list-style-type: none"> <li>• rootkit techniques to maintain persistence</li> <li>• uses process injection technique</li> <li>• strong encryption and modular architecture</li> </ul>	<ul style="list-style-type: none"> <li>• launch DDoS attacks</li> </ul>
Citadel	Nil	Banking Trojan	<ul style="list-style-type: none"> <li>• avoid and disable security tool detection</li> </ul>	<ul style="list-style-type: none"> <li>• steal banking credentials and sensitive information</li> <li>• keystroke logging</li> <li>• screenshot capture</li> <li>• video capture</li> <li>• man-in-the-browser attack</li> <li>• ransomware</li> </ul>
Conficker	<ul style="list-style-type: none"> <li>• Downadup</li> <li>• Kido</li> </ul>	Worm	<ul style="list-style-type: none"> <li>• domain generation algorithm (DGA) capability</li> <li>• communicate via P2P network</li> <li>• disable security software</li> </ul>	<ul style="list-style-type: none"> <li>• exploit the Windows Server Service vulnerability (MS08-067)</li> <li>• brute force attacks for admin credential to spread across network</li> <li>• spread via removable drives using "autorun" feature</li> </ul>

Table 7: Botnet Families (cont.)

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Corebot	Nil	Banking Trojan	<ul style="list-style-type: none"> <li>• via droppers</li> </ul>	<ul style="list-style-type: none"> <li>• steal sensitive information</li> <li>• install other malware</li> <li>• backdoor capabilities that allow unauthorized access</li> </ul>
Dyre	Nil	Banking Trojan	<ul style="list-style-type: none"> <li>• spam e-mail</li> </ul>	<ul style="list-style-type: none"> <li>• steal banking credential by tricking the victim to call an illegitimate number</li> <li>• send spams</li> </ul>
Gamarue	<ul style="list-style-type: none"> <li>• Andromeda</li> </ul>	Downloader/ Worm	<ul style="list-style-type: none"> <li>• via exploit kit</li> <li>• spam e-mail</li> <li>• MS Word macro</li> <li>• removable-drives</li> </ul>	<ul style="list-style-type: none"> <li>• steal sensitive information</li> <li>• allow unauthorized access</li> <li>• install other malware</li> </ul>
Ghost Push	Nil	Mobile malware	<ul style="list-style-type: none"> <li>• via app installation</li> </ul>	<ul style="list-style-type: none"> <li>• gain root access</li> <li>• download other malware</li> </ul>
Glupteba	Nil	Trojan	<ul style="list-style-type: none"> <li>• drive-by download via Blackhole Exploit Kit</li> </ul>	<ul style="list-style-type: none"> <li>• push contextual advertising and clickjacking to victims</li> </ul>
IRC Botnet	Nil	Trojan	<ul style="list-style-type: none"> <li>• communicate via IRC network</li> </ul>	<ul style="list-style-type: none"> <li>• backdoor capabilities that allow unauthorized access</li> <li>• launch DDoS attack</li> <li>• send spams</li> </ul>
Mirai	Nil	Worm	<ul style="list-style-type: none"> <li>• telnet with vendor default credentials</li> </ul>	<ul style="list-style-type: none"> <li>• launch DDoS attacks</li> </ul>
Murofet	Nil	Trojan	<ul style="list-style-type: none"> <li>• file infection</li> <li>• via exploit kits</li> </ul>	<ul style="list-style-type: none"> <li>• download other malware</li> </ul>
Nivdort	Nil	Trojan	<ul style="list-style-type: none"> <li>• spam e-mail</li> </ul>	<ul style="list-style-type: none"> <li>• steal login credentials and sensitive information</li> </ul>
Nymaim	Nil	Trojan	<ul style="list-style-type: none"> <li>• spam e-mail</li> <li>• malicious link</li> </ul>	<ul style="list-style-type: none"> <li>• lock infected systems</li> <li>• stop victims from accessing files</li> <li>• ask for ransom</li> </ul>
Palevo	<ul style="list-style-type: none"> <li>• Rimecud</li> <li>• Butterfly bot</li> <li>• Pilleuz</li> <li>• Mariposa</li> <li>• Vaklik</li> </ul>	Worm	<ul style="list-style-type: none"> <li>• spread via instant messaging, P2P network and removable drives</li> </ul>	<ul style="list-style-type: none"> <li>• backdoor capabilities that allow unauthorized access</li> <li>• steal login credentials and sensitive information</li> <li>• steal money directly from banks using money mules</li> </ul>

Table 8: Botnet Families (cont.)

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Pushdo	<ul style="list-style-type: none"> <li>• Cutwail</li> <li>• Pandex</li> </ul>	Downloader	<ul style="list-style-type: none"> <li>• hiding its malicious network traffic</li> <li>• domain generation algorithm (DGA) capability</li> <li>• distribute via drive by download</li> <li>• exploit browser and plugins' vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>• download other banking malware (e.g. Zeus and Spyeye)</li> <li>• launch DDoS attacks</li> <li>• send spams</li> </ul>
Ramnit	Nil	Worm	<ul style="list-style-type: none"> <li>• file infection</li> <li>• via exploit kits</li> <li>• public FTP servers</li> </ul>	<ul style="list-style-type: none"> <li>• backdoor capabilities that allow unauthorized access</li> <li>• steal login credentials and sensitive information</li> </ul>
Sality	Nil	Trojan	<ul style="list-style-type: none"> <li>• rootkit techniques to maintain persistence</li> <li>• communicate via P2P network</li> <li>• spread via removable drives and shares</li> <li>• disable security software</li> <li>• use polymorphic and entry point obscuring (EPO) techniques to infect files</li> </ul>	<ul style="list-style-type: none"> <li>• send spams</li> <li>• proxying of communications</li> <li>• steal sensitive information</li> <li>• compromise web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking)</li> <li>• install other malware</li> </ul>
Slenfbot	Nil	Worm	<ul style="list-style-type: none"> <li>• spread via removable drives and shares</li> </ul>	<ul style="list-style-type: none"> <li>• backdoor capabilities that allow unauthorized access</li> <li>• download financial malware</li> <li>• sending spam</li> <li>• launch DDoS attacks</li> </ul>
Tinba	<ul style="list-style-type: none"> <li>• TinyBanker</li> <li>• Zusy</li> </ul>	Banking Trojan	<ul style="list-style-type: none"> <li>• via exploit kit</li> <li>• Spam e-mail</li> </ul>	<ul style="list-style-type: none"> <li>• steal banking credential and sensitive information</li> </ul>
Torpig	<ul style="list-style-type: none"> <li>• Sinowal</li> <li>• Anserin</li> </ul>	Trojan	<ul style="list-style-type: none"> <li>• rootkit techniques to maintain persistence (Mebrook rootkit)</li> <li>• domain generation algorithm (DGA) capability</li> <li>• distribute via drive by download</li> </ul>	<ul style="list-style-type: none"> <li>• steal sensitive information</li> <li>• man in the browser attack</li> </ul>

Table 9: Botnet Families (cont.)

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Virut	Nil	Trojan	<ul style="list-style-type: none"> <li>spread via removable drives and shares</li> </ul>	<ul style="list-style-type: none"> <li>send spams</li> <li>launch DDoS attacks</li> <li>fraud</li> <li>data theft</li> </ul>
WannaCry	<ul style="list-style-type: none"> <li>WannaCrypt</li> </ul>	Ransomware	<ul style="list-style-type: none"> <li>spread across network</li> <li>exploit Windows SMB vulnerabilities</li> </ul>	<ul style="list-style-type: none"> <li>encrypt user data</li> <li>demand ransom</li> <li>data unrecoverable</li> </ul>
Wapomi	Nil	Worm	<ul style="list-style-type: none"> <li>spread via removable drives and shares</li> <li>infects executable files</li> </ul>	<ul style="list-style-type: none"> <li>backdoor capabilities</li> <li>download and drop additional destructive payloads <ul style="list-style-type: none"> <li>alter important files causing unreliable system performance</li> <li>gather computer activity, transmit private data and cause sluggish computer</li> </ul> </li> </ul>
ZeroAccess	<ul style="list-style-type: none"> <li>max++</li> <li>Sirefef</li> </ul>	Trojan	<ul style="list-style-type: none"> <li>rootkit techniques to maintain persistence</li> <li>communicate via P2P network</li> <li>distribute via drive by download</li> <li>distribute via disguise as legitimate file (eg. media files, keygen)</li> </ul>	<ul style="list-style-type: none"> <li>download other malware</li> <li>bitcoin mining and click fraud</li> </ul>
Zeus	<ul style="list-style-type: none"> <li>GameOver</li> </ul>	Banking Trojan	<ul style="list-style-type: none"> <li>stealthy techniques to maintain persistence</li> <li>distribute via drive by download</li> <li>communicate via P2P network</li> </ul>	<ul style="list-style-type: none"> <li>steal banking credential and sensitive information</li> <li>man in the browser attack</li> <li>keystroke logging</li> <li>download other malware (eg. Cryptolocker)</li> <li>launch DDoS attacks</li> </ul>