HKCERT

Hong Kong Security Watch Report

2016 Q4

Foreword

Better Security Decision with Situational Awareness

Nowadays, a lot of "invisible" compromised computers and devices are controlled by attackers with the owner being unaware. The data on these devices may be mined and exposed every day, and the computers 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 computers 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 computers 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 enhancing 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

Contents

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

Highlight of Report

This report is for 2016 Q4. This quarter we have changed the format of the report. Any comments about the new format is welcomed.

In 2016 Q4, there were 13,681 unique security events related to Hong Kong used for analysis in this report. The information is collected with IFAS[2] from 19 sources of information.[3] They are not from the incidents reports received by HKCERT.

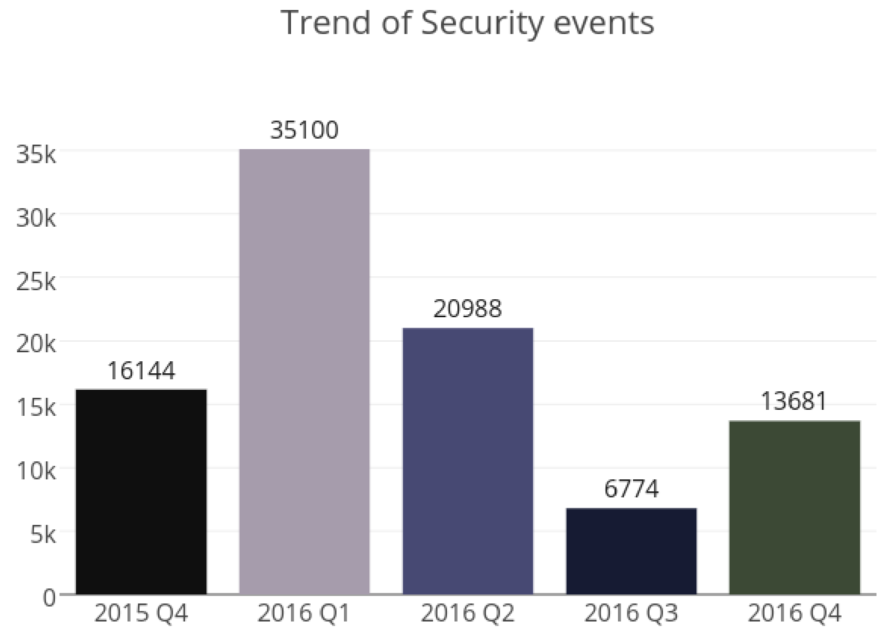

Figure 1: Trend of security events

The total number of security events in 2016 Q4 increased significantly by 102% or 6,907 events. The huge increase was due to the unusually small base last quarter, which was caused by the temporary absence of one of our major data sources, CleanMX. Actually the number this quarter was lower than the average number of the previous four quarters.

Server related security events

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

[2] IFAS - Information Feed Analysis System is a HKCERT developed system that collects global security intelligence relating to Hong Kong to provide a picture of the security status.

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

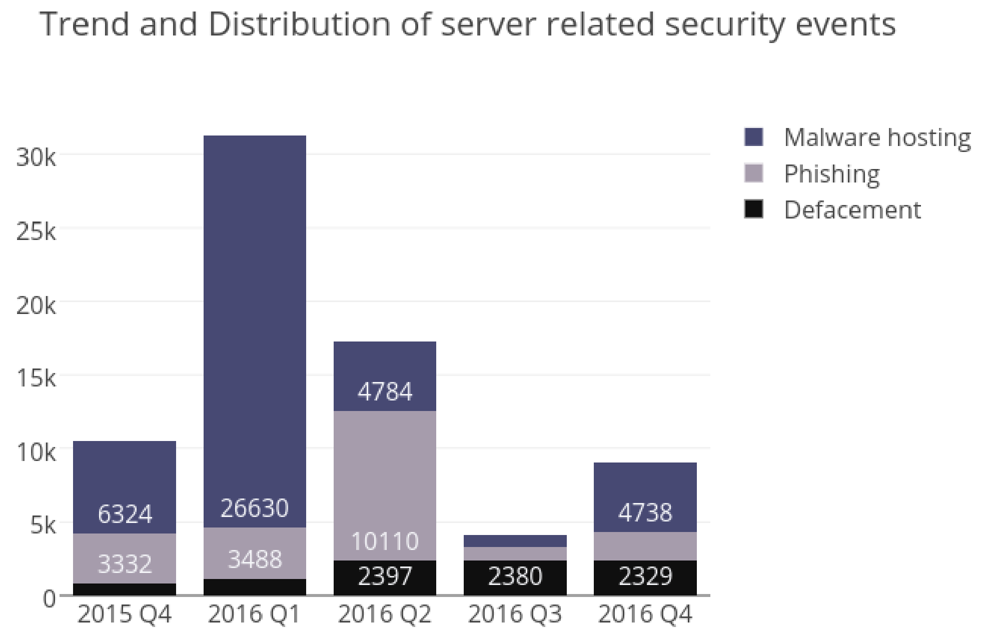

Figure 2: Trend and distribution of server related security events

The number of server related security events increased from 4,139 to 9,025(increased by 118%) this quarter.

The domain that hosted the largest number of malware was btjykjj.com. It hosted 543 or 11% of all malware hosting events. At first sight, this domain looked like a malicious domain: the domain name was composed by seemingly random characters; the administrator email address, dingchun158@gmail.com is used by hundreds of domains. However, WHOIS history [4] showed that a year ago the domain was owned by an organization called "Bao Tou Shi Jiu Yuan Qu Ke Xue Ji Shu Ju" which is the Chinese pinyin roughly translated to The Science and Technology Bureau of Jiu Yuen District, Bao Tou City (a city in inner Mongolia, China), which is a unit in the Chinese Government. btjykjj was the short form of the pinyin name. The domain was not renewed after its expiry a year ago. And then it was registered by its current owner dingchun158@gmail.com.

We further discovered that the IP address resolved by this domain was responsible for six more malware hosting events. Among which, at least two of them were suspected to be expired legitimate domains. They were gaqylz.com, which is the short form of "Guang An Yue Lai Zhen", Chinese pinyin translated to Yue Lai Town of Guang An City (a city in Sichuan Province, China) and hfjgg.com, which is the short form of "He Fei Jiu Gong Ge", a decoration company in Anhui Province, China.

These cases showed that cyber crooks are looking for expired legitimate domains for malicious use. These domains can gain trust from the victims easier, due to their seemingly legitimate appearances, especially to the victims who know the legitimate organizations behind. Internet users shouldn't trust a URL solely based on its domain name. When in doubt, always do further checking before accessing the URL.

[4] https://www.passivetotal.org/search/gaqylz.com

HKCERT urges system and application administrators to protect the servers

- provide strong authentication e.g. two factor authentication, administrative control interface
- acquire information security knowledge to prevent social engineering
- verify any suspicious URLs before visiting

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:

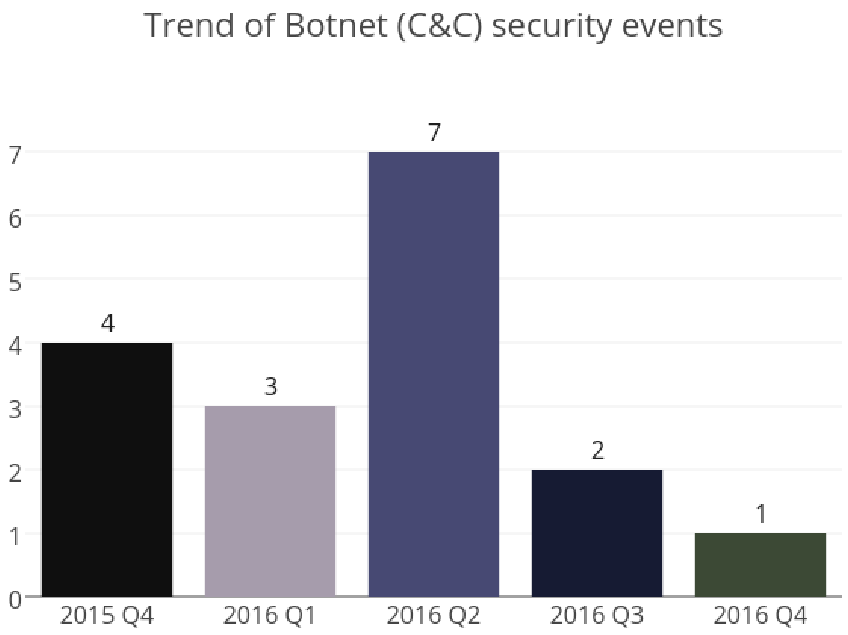

Figure 3: Trend of Botnet (C&Cs) security events

The number of botnet Command and Control Servers decreased this quarter. There was one C&C servers reported in this quarter, which was identified as IRC bot C&C server.

Botnet Bots

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

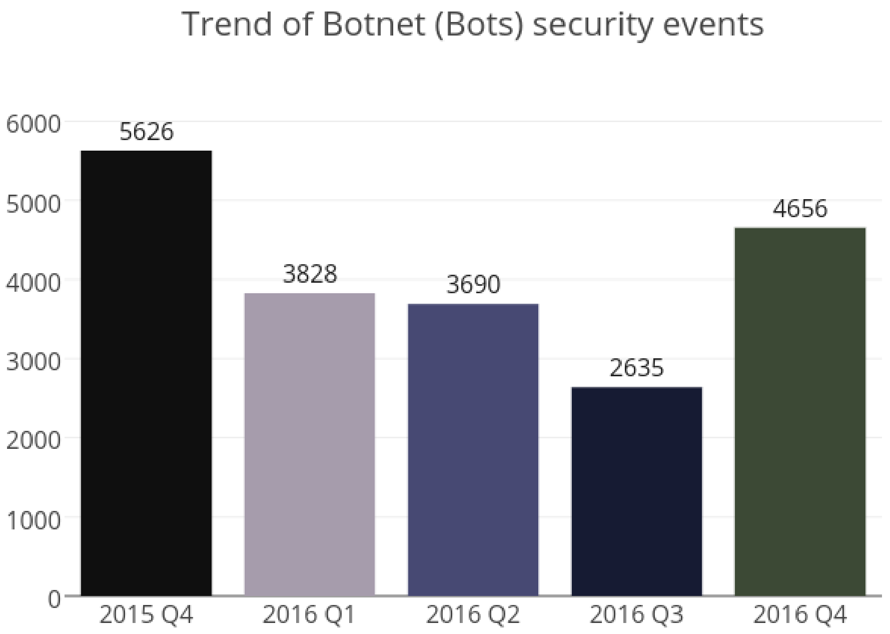

Figure 4: Trend of Botnet (Bots) security events

Number of Botnet (bots) in Hong Kong network increased significantly by 77%. Two new botnets, Mirai and Avalanche contributed almost half of all botnet events.

Mirai

This quarter, the long term dominance of Conficker ended. Conficker has always been on the top of the chart since our first report, leading others by a far distance. However, it was outranked by a new comer, Mirai. (Figure 12).

Mirai is a botnet targeting Internet of Things (IoT) devices. IoT devices are Internet-connected devices such as webcams, routers and smart-TVs, etc. They are usually easy targets as most of them are poorly secured and operated by ordinary people who lack security expertises.

Mirai spreads by using telnet with default passwords to attempt to take control of victim devices. It has a built-in username-password list that contains over 60 default credentials. [5] With this, Mirai easily infected hundreds of thousands of devices over the world. If a user connects an IoT device to the internet without changing the default password, there is a high chance the device will be infected in a short time.

In September, the botnet launched a massive DDoS attack to the website of cybersecurity blogger Brian Krebs. The website was hit by a scary 620+ Gbps traffic. Shortly after that, a French hosting company, OVH suffered the largest DDoS attack known today – with peak traffic close to 1Tbps. [6] Then, in less than a month, the botnet launched another DDoS attack to a DNS provider DYN. The attack brought down DYN's service as well as a few websites that rely on DYN's service. [7]

In November, 0.9 million routers from a German ISP Deutsche Telekom were forced offline by the Mirai botnet[8]. Researchers found that this variant of Mirai botnet used a new way to spread. In addition to the traditional way of using factory default credentials, it can exploit a vulnerability in specific routers made by Zyxel and Speedport. Then it can remotely infect vulnerable devices through TR-069, which is a remote management protocol.

[5] https://nakedsecurity.sophos.com/2016/10/05/mirai-internet-of-things-malware-from-krebs-ddos-attack-goes-open-source/

[6] http://www.scmagazineuk.com/ovh-suffers-11tbps-ddos-attack/article/524826/

[7] https://www.hkcert.org/my_url/en/blog/16102401

[8] https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/

Cleanup of the malware is difficult. Mirai would disable the port used by TR-069 and telnet so as to cripple the ISP's ability to remotely patch the devices. Users need to power off the routers in order to clear the malware from the memory. However, if the devices are not patched immediately, they may be infected again in minutes as Mirai is active scanning vulnerable internet devices.

In foreseeable future, Mirai will remain a major threat to the internet.

HKCERT urges users to protect computers so as not to become part of the botnets

- change the default passwords of IoT devices immediately
- set strong passwords to avoid credential based attack
- close any web services you don't need, especially telnet.
- do not expose the devices to the internet, unless necessary.
- if you suspect your device is infected, unplug it from the network immediately.

Avalanche

Avalanche, set up in 2009, is a hosting platform made up of around 600 servers worldwide, which was mainly used by cybercriminals to deploy financial crimeware (e.g. Zeus, SpyEye), issue commands to infected devices (e.g. to send out fraudulent emails, conduct money laundering activities). In order to hide the server actual locations, it made use of proxy server and also "double fast flux" techniques, i.e. changing both DNS and IP address of a malicious domain every 5 minutes, for infected devices to connect to the platform.

A joint operation to take down the "Avalanche" cybercrime hosting platform was led by Europol, and conducted with law enforcement, judiciaries, and security researchers from more than 30 countries. In this operation, 5 individuals were arrested, and 39 servers were seized, and 221 servers were put offline by the hosting providers. Over 830,000 website domains were seized, blocked or "sinkholed". [9]

Around 350 Hong Kong IP addresses were affected. HKCERT has notified the corresponding ISP to contact their affected clients.

HKCERT urges users to protect computers so as not to become part of the botnets

- patch their computers
- install a working ocpy of the security software and scan for malware on their machines
- set strong passwords to avoic credential based attack
- do not open files from unreliable sources

[9] https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-opera

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 Pushdo, Citadel, 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

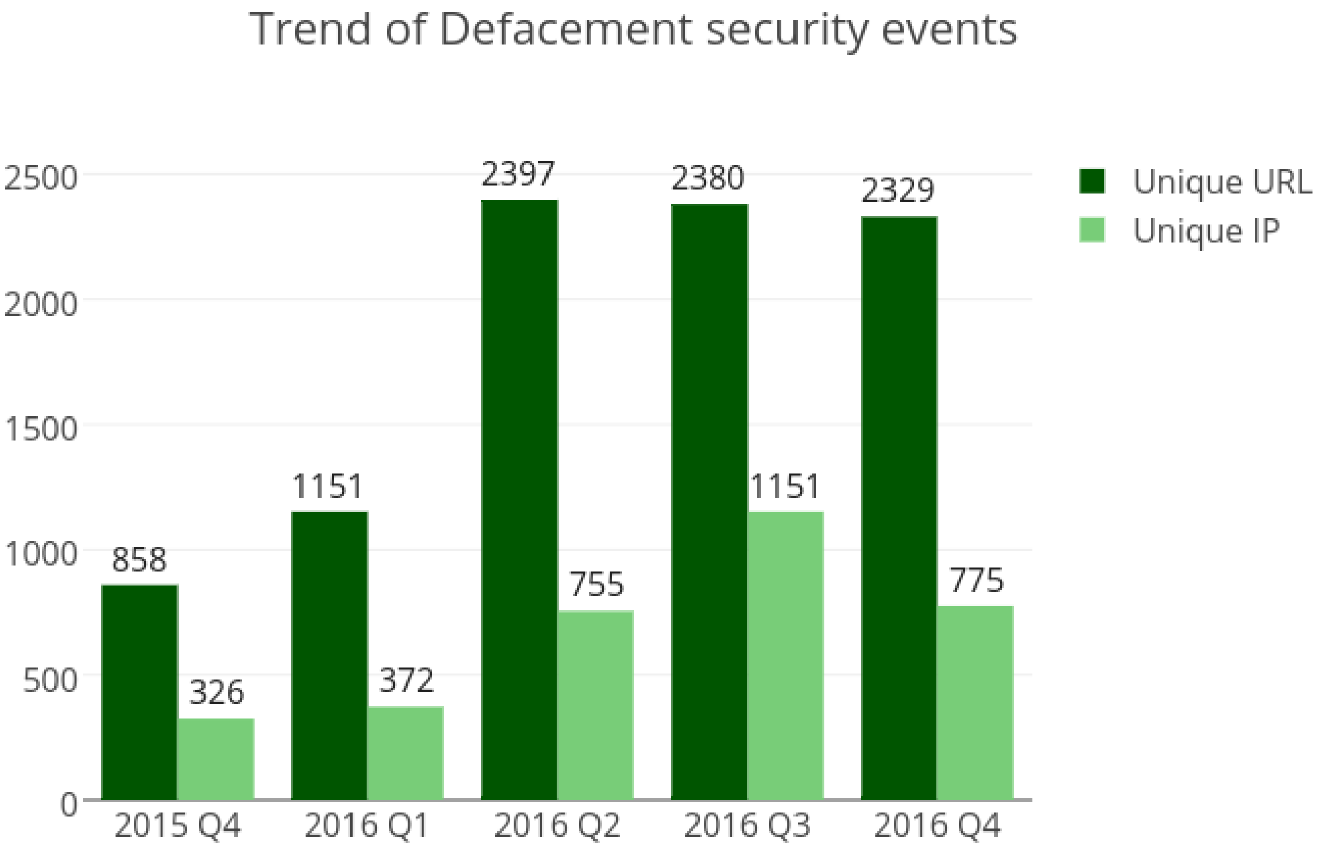

Figure 5: Trend of Defacement security events

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.

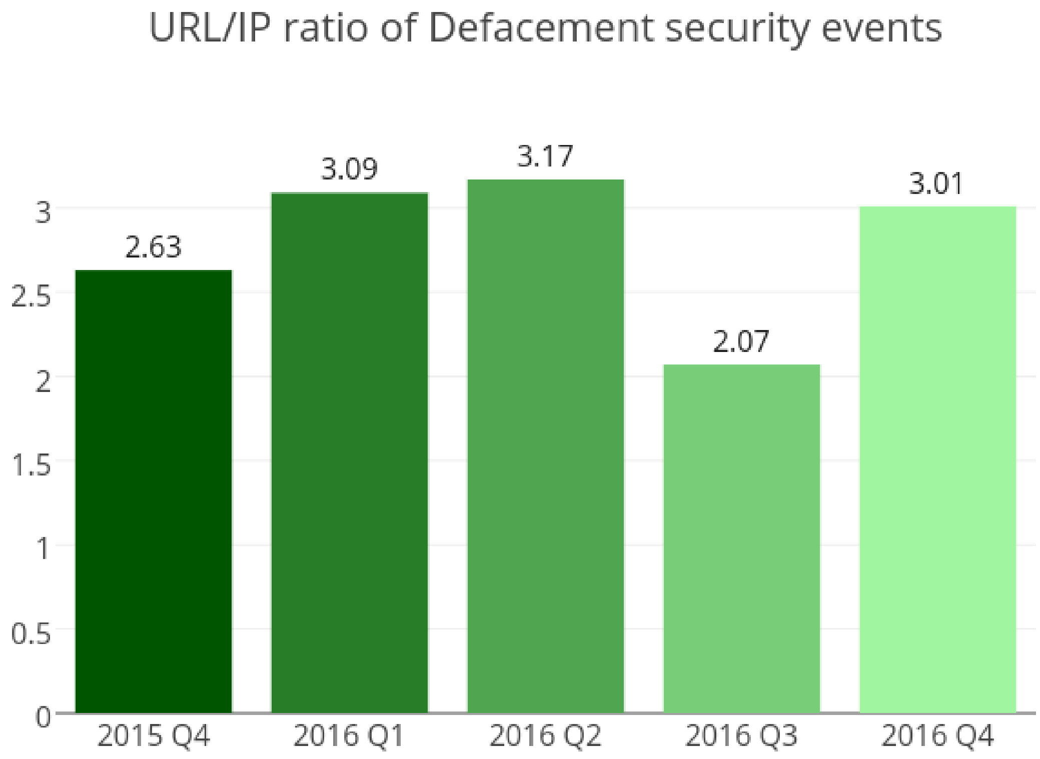

Figure 6: URL/IP ratio of defacement security events

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 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

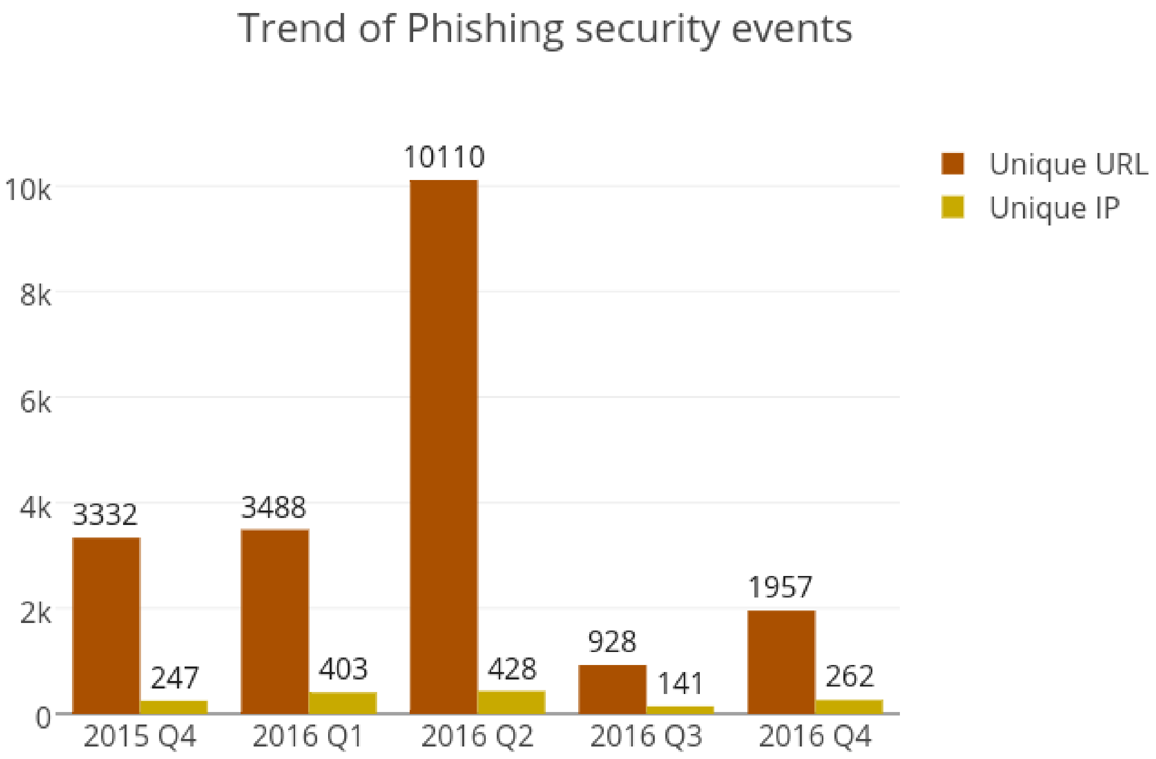

Figure 7: Trend of Defacement security events

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

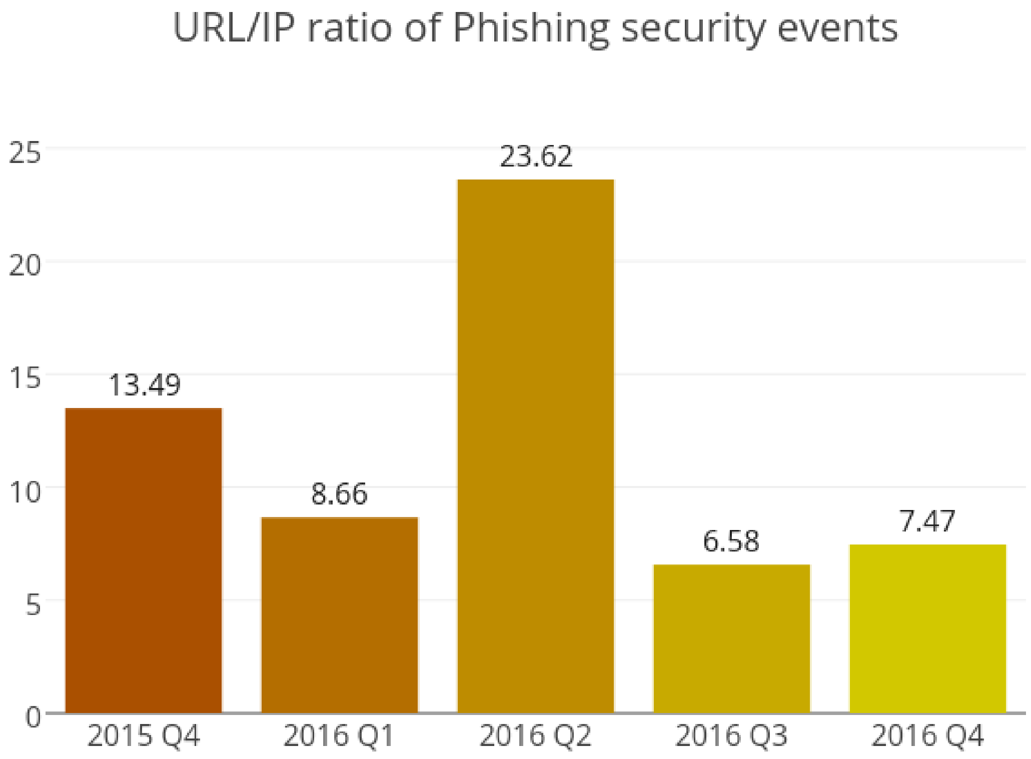

Figure 8: URL/IP ratio of Phishing security events

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 better related to the number of compromised servers
- The higher the ratio is, the more mass compromise happened

Sources of Information:

- ArborNetwork - Atlas SRF
- CleanMX - phishing
- Millersmiles
- Phishtank

3 Malware Hosting

3.1 Summary

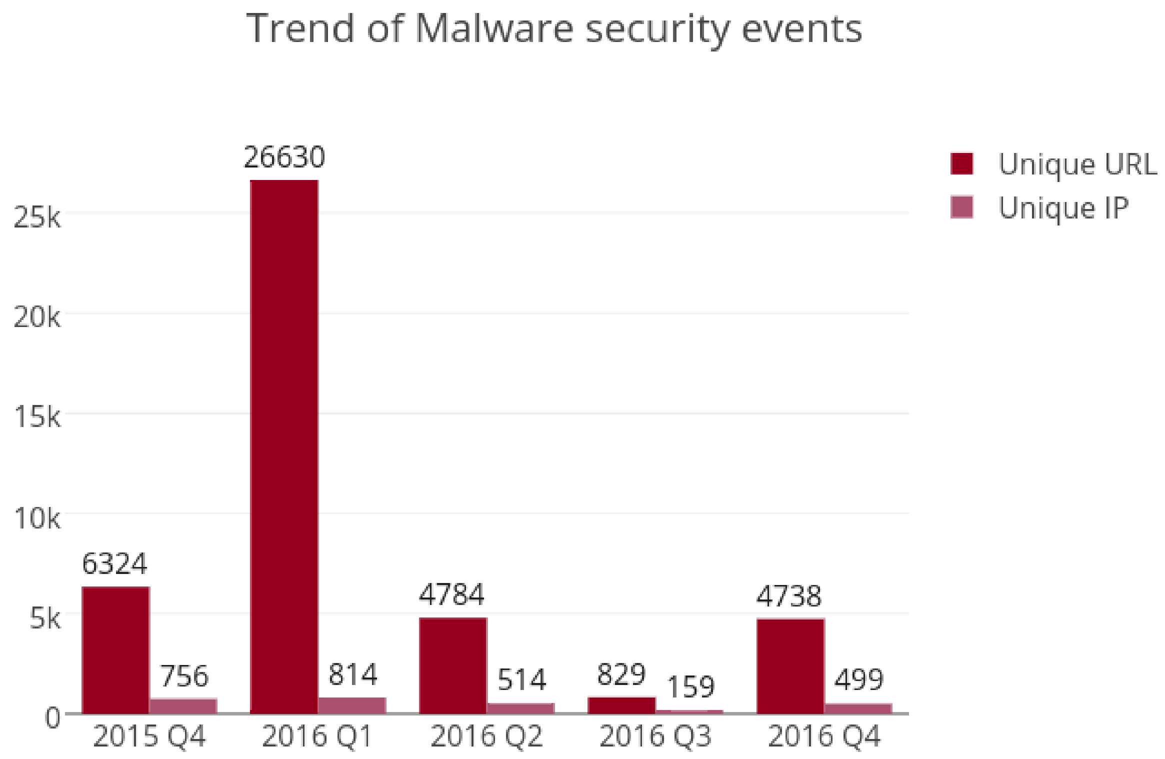

Figure 9: Trend of Malware Hosting security events

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

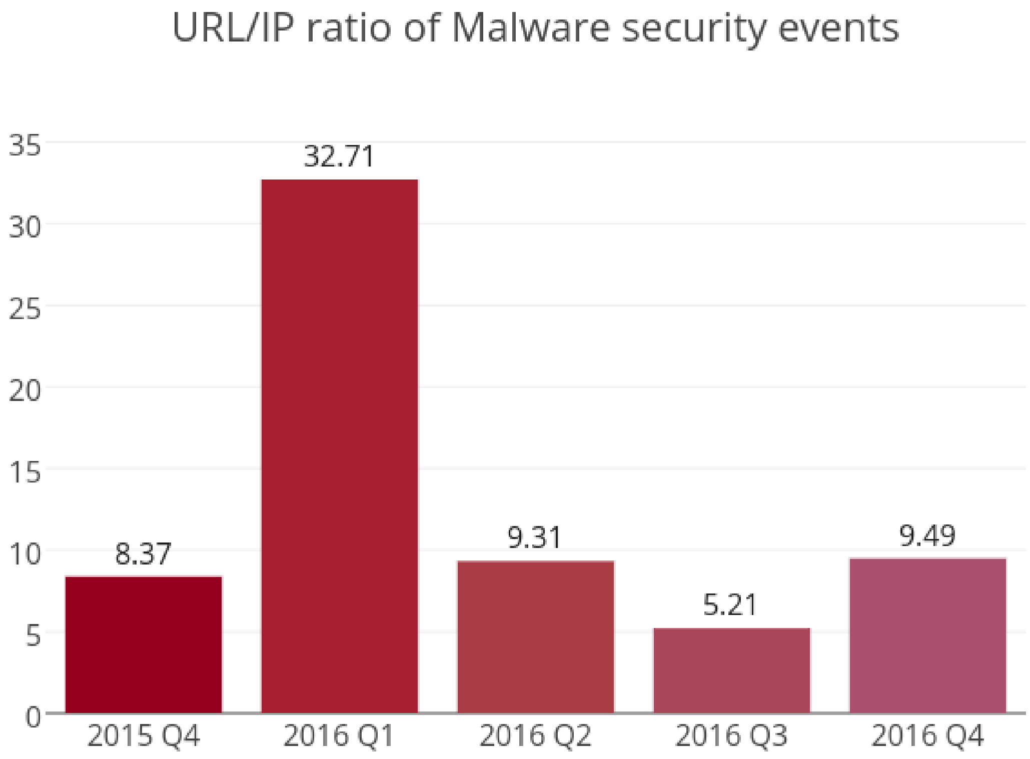

Figure 10: URL/IP ratio of Malware Hosting security events

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 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
- Abuse.ch:SpyEye Tracker - Binary URL
- CleanMX - Malware
- Malc0de
- MalwareDomainList
- Sacour.cn

4 Botnet

4.1 Botnets - Command & Control Servers

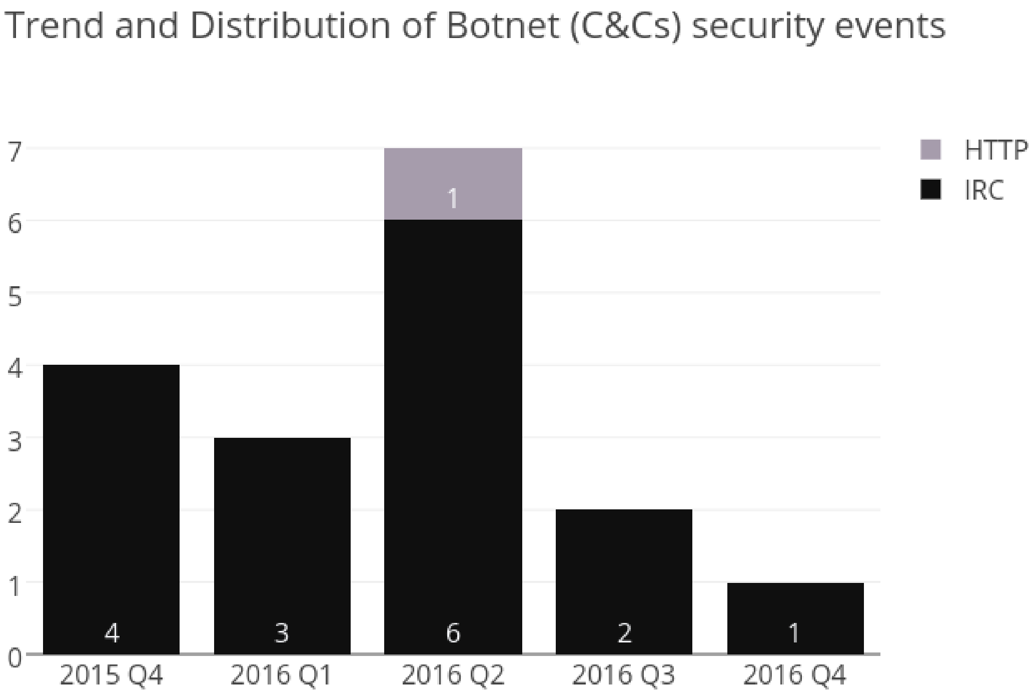

Figure 11: Trend and Distribution of Botnet (C&Cs) security events

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
- SpyEye Tracker
- Palevo Tracker
- Shadowserver - C&Cs

4.2 Botnets - Bots

4.2.1 Major Botnet Families[10]

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.

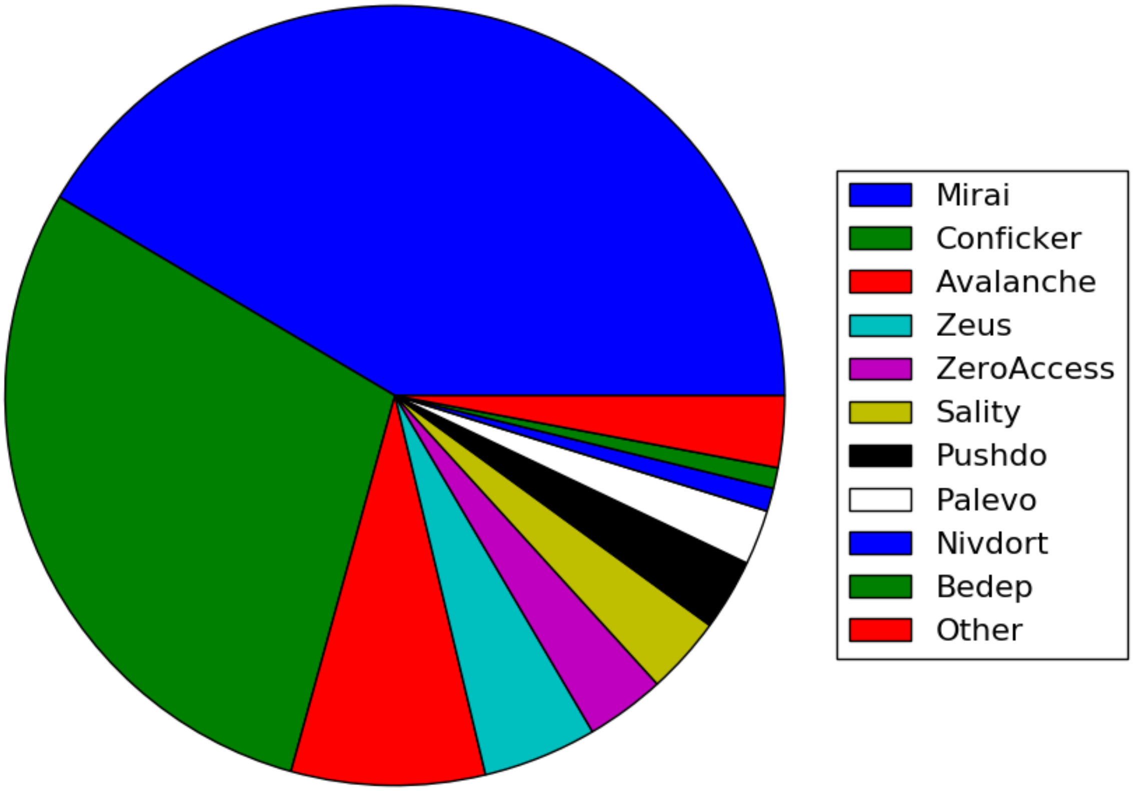

Figure 12: Major Botnet Families in Hong Kong Networks

Table 2: Major Botnet Families in Hong Kong Networks

Rank	⇑⇓	Concerned Bots	Number of Unique IP addresses	Changes with previous period
1	NEW	Mirai	1932	NA
2	⇓	Conficker	1360	-6.9%
3	NEW	Avalanche	374	NA
4	⇓	Zeus	220	-21.7%
5	⇓	ZeroAccess	153	-13.1%
6	⇓	Sality	150	0.0%
7	⇓	Pushdo	138	-22.0%
8	→	Palevo	106	92.7%
9	⇓	Nivdort	45	-27.4%
10	⇓	Bedep	40	-16.7%

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

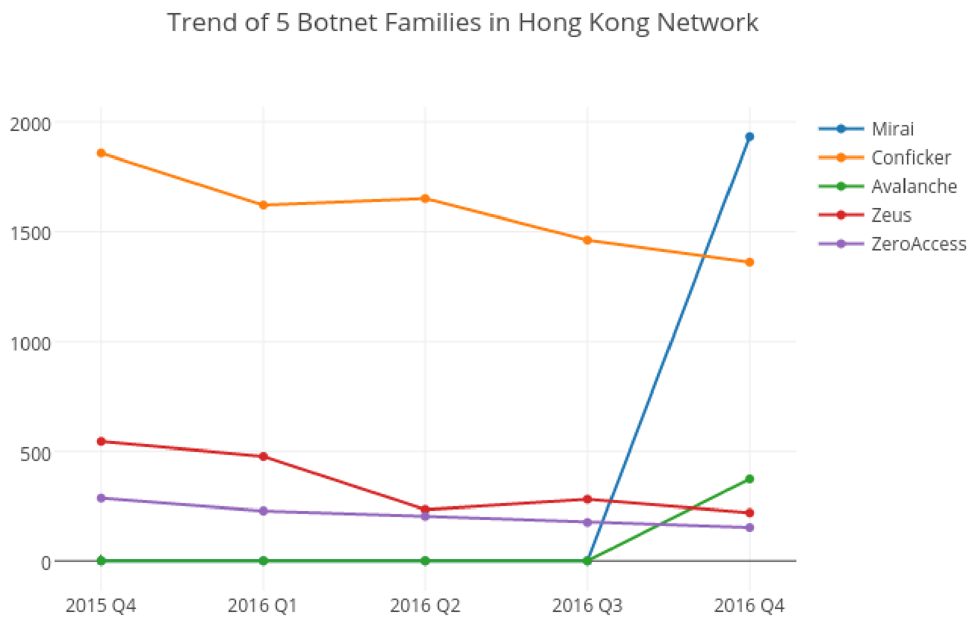

Figure 13: Trend of Top 5 Botnet Famliies in Hong Kong Network

Name	**2015 Q4**	**2016 Q1**	**2016 Q2**	**2016 Q3**	**2016 Q4**
Mirai	0	0	0	0	1932
Conficker	1857	1620	1650	1461	1360
Avalanche	0	0	0	0	374
Zeus	544	477	234	281	220
ZeroAccess	286	228	204	176	153

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:

- ArborNetwork - Atlas SRF - conficker
- 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	ArborNetwork: Atlas SRF-Phishing	2013-04
Phishing	CleanMX - Phishing	2013-04
Phishing	Millersmiles	2013-04
Phishing	Phishtank	2013-04
Malware Hosting	Abuse.ch: Zeus Tracker - Binary URL	2013-04
Malware Hosting	Abuse.ch: SpyEye Tracker - Binary URL	2013-04
Malware Hosting	CleanMX - Malware	2013-04
Malware Hosting	Malc0de	2013-04
Malware Hosting	MalwareDomainList	2013-04
Malware Hosting	Savour.cn	2013-04
Botnet (C&Cs)	Abuse.ch: Zeus Tracker - C&Cs	2013-04
Botnet (C&Cs)	Abuse.ch: SpyEye 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)	Arbor Network: Atlas SRF-Conficker	2013-08
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	2017-1-14

C Major Botnet Families

Table 5: Botnet Families

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Avalanche	Nil	Crimeware-as-a-service	Depends on underlying malwares	• send spams • host phishing sites • host malware • steal sensitive information
Bamital	Nil	Trojan	• drive-by download via exploit kit • via P2P network	• Click fraud • Search hijacking
BankPatch	• MultiBanker • Patcher • BankPatcher	Banking Trojan	• via adult web sites • corrupt multimedia codecs • spam e-mail • chat and messaging systems	• monitor specific banking websites and harvest user's passwords, credit card information and other sensitive financial data
Bedep	Nil	Trojan	• via adult web sites • malvertising	• Click fraud • download other malwares
BlackEnergy	Nil	DDoS Trojan	• rootkit techniques to maintain persistence • uses process injection technique • strong encryption and modular architecture	• launch DDoS attacks
Citadel	Nil	Banking Trojan	• avoid and disable security tool detection	• steal banking credentials and sensitive information • keystroke logging • screenshot capture • video capture • man-in-the-browser attack • ransomware
Conficker	• Downadup • Kido	Worm	• domain generation algorithm (DGA) capability • communicate via P2P network • disable security software	• exploit the Windows Server Service vulnerability (MS08-067) • brute force attacks for admin credential to spread across network • spread via removable drives using "autorun" feature

Table 6: Botnet Families (cont.)

Major Botnets	**Alias**	**Nature**	**Infection Method**	**Attacks / Impacts**
Corebot	Nil	Banking Trojan	• via droppers	• steal sensitive information • install other malware • backdoor capabilities that allow unauthorized access
Dyre	Nil	Banking Trojan	• spam e-mail	• steal banking credential by tricking the victim to call an illegitimate number • send spams
Gamarue	• Andromeda	Downloader/ Worm	• via exploit kit • spam e-mail • MS Word macro • removable-drives	• steal sensitive information • allow unauthorized access • install other malware
Glupteba	Nil	Trojan	• drive-by download via Blackhole Exploit Kit	• push contextual advertising and clickjacking to victims
IRC Botnet	Nil	Trojan	• communicate via IRC network	• backdoor capabilities that allow unauthorized access • launch DDoS attack • send spams
Mirai	Nil	Worm	• telnet with vendor default credentials	• launch DDoS attacks
Nivdort	Nil	Trojan	• spam e-mail	• steal login credentials and sensitive information
Nymaim	Nil	Trojan	• spam e-mail • malicious link	• lock infected systems • stop victims from accessing files • ask for ransom
Palevo	• Rimecud • Butterfly bot • Pilleuz • Mariposa • Vaklik	Worm	• spread via instant messaging, P2P network and removable drives	• backdoor capabilities that allow unauthorized access • steal login credentials and sensitive information • steal money directly from banks using?money mules

Table 7: Botnet Families (cont.)

Major Botnets	**Alias**	**Nature**	**Infection Method**	**Attacks / Impacts**
Pushdo	• Cutwail • Pandex	Downloader	• hiding its malicious network traffic • domain generation algorithm (DGA) capability • distribute via drive by download • exploit browser and plugins' vulnerabilities	• download other banking malware (e.g. Zeus and Spyeye) • launch DDoS attacks • send spams
Ramnit	Nil	Worm	• file infection • via exploit kits • public FTP servers	• backdoor capabilities that allow unauthorized access • steal login credentials and sensitive information
Sality	Nil	Trojan	• rootkit techniques to maintain persistence • communicate via P2P network • spread via removable drives and shares • disable security software • use polymorphic and entry point obscuring (EPO) techniques to infect files	• send spams • proxying of communications • steal sensitive information • compromise web servers and/or coordinating distributed computing tasks for the purpose of processing intensive tasks (e.g. password cracking) • install other malware
Slenfbot	Nil	Worm	• spread via removable drives and shares	• backdoor capabilities that allow unauthorized access • download financial malware • sending spam • launch DDoS attacks
Tinba	• TinyBanker • Zusy	Banking Trojan	• via exploit kit • Spam e-mail	• steal banking credential and sensitive information
Torpig	• Sinowal • Anserin	Trojan	• rootkit techniques to maintain persistence (Mebroot rootkit) • domain generation algorithm (DGA) capability • distribute via drive by download	• steal sensitive information • man in the browser attack

Table 8: Botnet Families (cont.)

Major Botnets	**Alias**	**Nature**	**Infection Method**	**Attacks / Impacts**
Virut	Nil	Trojan	• spread via removable drives and shares	• send spams • launch DDoS attacks • fraud • data theft
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