Hong Kong Security Watch Report 2020 Q3

45%

Release date: Nov 2020

25%



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.

Type of Attack	Metric used
Defacement, Phishing,	Security events on unique URLs within the reporting period
Malware Hosting	
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

Table 1: Types of Attack

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

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



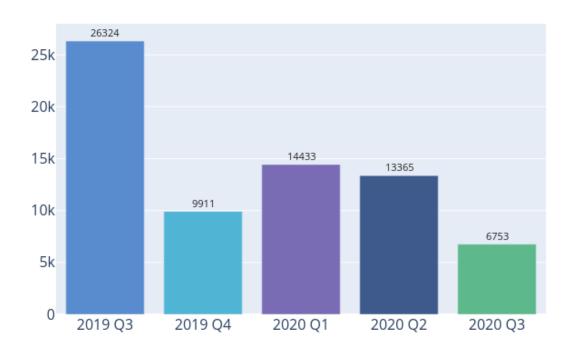
Contents

Re	eport Highlights	5				
Re	eport Details	11				
1	Defacement 1.1 Summary	11 11				
2	Phishing 2.1 Summary	14 14				
3	Malware Hosting 3.1 Summary	16 16				
4	Botnet 4.1 Botnets Command & Control Centers (C&C) 4.2 Botnets (Bots) 4.2.1 Major Botnet Families	18 18 19 19				
Ар	opendix	21				
Α	Sources of information in IFAS	22				
В	Geolocation identification methods in IFAS	22				
С	Major Botnet Families					



Report Highlights

In 2020 Q3, there were 6,753 unique security events related to Hong Kong used for analysis in this report. Data were collected through IFAS¹ with 10 sources of information², and not collected from the incident reports received by HKCERT.



Trend of security events

Figure 1: Trend of security events

Table 2: Trend of security events

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

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

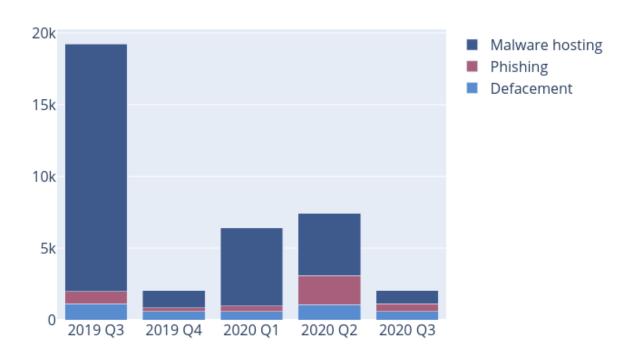
¹IFAS - Information Feed Analysis System is a HKCERT developed system that collects global security intelligence relating to Hong Kong to provide a picture of the security status.

²Refer to Appendix 1 for the sources of information



Server related security events

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



Trend and distribution of server related security events

Figure 2: Trend and distribution of server related security events

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

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

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

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



HKCERT urges system and application administrators to strengthen the protection of servers



- Patch server up-to-date to avoid the known vulnerabilities being exploited
- Update web application and plugins to the latest version
- Follow best practice on user account and password management
- Implement validation check for user input and system output
- Provide strong authentication e.g. two factor authentication, administrative control interface
- Acquire information security knowledge to prevent social engineering attack



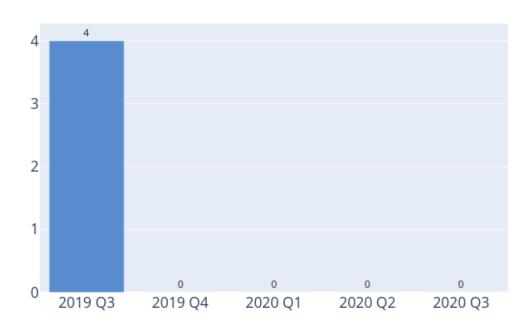
Botnet related security events

Botnet related security events can be classified into two categories:

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

Botnet Command and Control Servers (C&C)

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



Trend of Botnet (C&C) security events

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:



Trend of Botnet (Bots) security events

Figure 4: Trend of Botnet (Bots) security events

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

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

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



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



- Patch the computer
- Install security software and scan for malware
- Set strong passwords to avoid credential based attack
- Do not use Windows, media files and software that have no proper licenses
- Do not use Windows and software that have no security updates
- Do not open files from unreliable sources

HKCERT has been following up the security events received and proactively engaged local ISPs for the botnet cleanup since June 2013. Currently, botnet cleanup operations against major botnet family Avalanche, Pushdo, Citadel, Ramnit, ZeroAccess, GameOver Zeus, VPNFilter and Mirai are still ongoing.

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

Users can follow the HKCERT guideline to detect and clean up botnets

Botnet Detection and Cleanup Guideline https://www.hkcert.org/botnet





Report Details

- 1 Defacement
- 1.1 Summary



Trend of Defacement security events

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





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

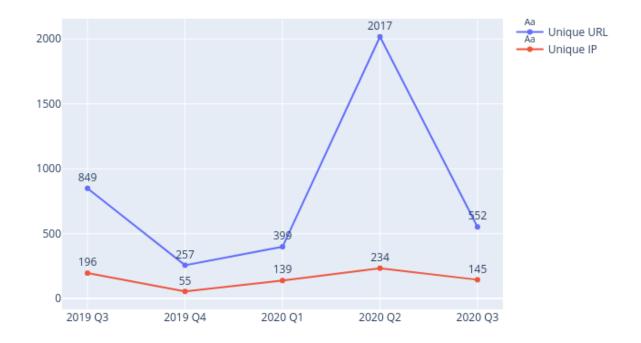
Sources of Information:

• Zone-H



2 Phishing

2.1 Summary



Trend of Phishing security events

Figure 7: Trend of Phishing security events

What is phishing?

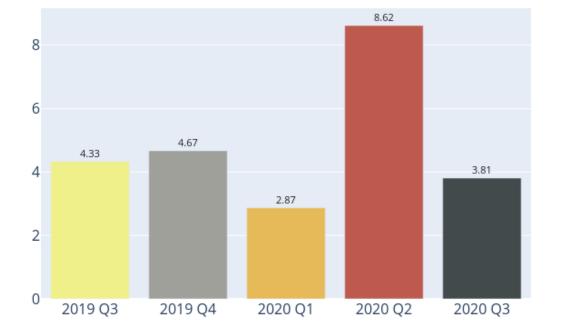


• Phishing is the spoofing of a legitimate website for fraudulent purposes

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





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

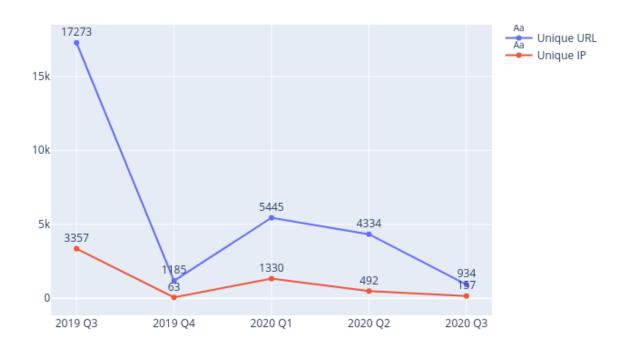
Sources of Information:

- CleanMX phishing
- Phishtank



3 Malware Hosting

3.1 Summary



Trend of Malware Hosting security events

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



URL/IP ratio of Malware Hosting security events

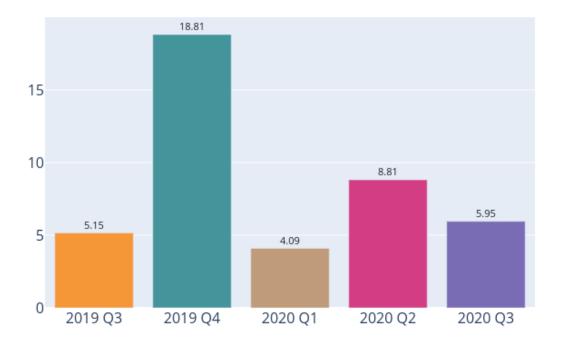


Figure 10: URL/IP ratio of Malware Hosting security events

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

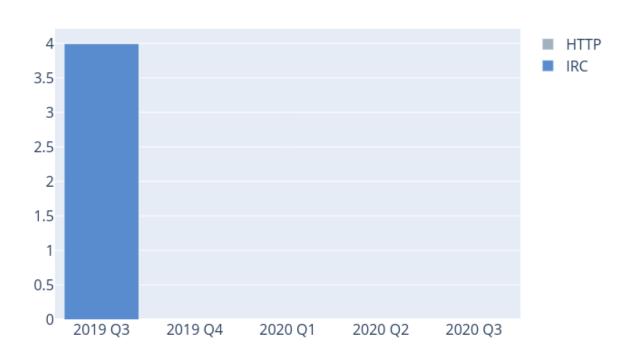
Sources of Information:

- CleanMX Malware
- Malc0de
- MalwareDomainList



4 Botnet

4.1 Botnets Command & Control Centers (C&C)



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?



 Botnet Command & Control Center is a server used by cybercriminals to control the bots, which are compromised computers, by sending them commands to perform malicious activities, e.g. stealing personal financial information or launching DDoS attacks

What are the potential impacts?

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

Sources of Information:

• Shadowserver - C&Cs



4.2 Botnets (Bots)

4.2.1 Major Botnet Families

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

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

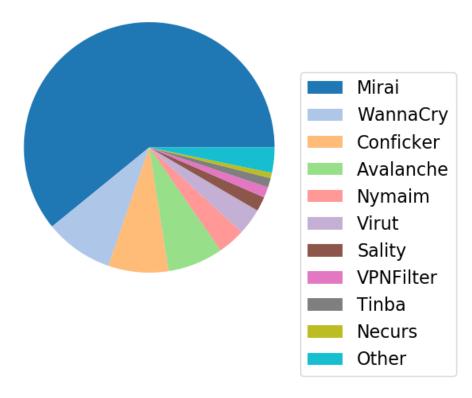


Figure 12: Major Botnet families in Hong Kong network

₩	Concerned Bots	Number of Unique IP addresses	Changes with previous period
\rightarrow	Mirai	2,859	-28.0%
\rightarrow	WannaCry	415	-19.1%
\rightarrow	Conficker	365	-8.8%
\rightarrow	Avalanche	336	-2.6%
↑	Nymaim	166	90.8%
\Downarrow	Virut	160	0.0%
\Downarrow	Sality	88	-9.3%
\rightarrow	VPNFilter	65	-9.7%
\rightarrow	Tinba	56	9.8%
\rightarrow	Necurs	33	-23.3%
	$ \begin{array}{c} \rightarrow \\ \rightarrow \\ \rightarrow \\ \rightarrow \\ \uparrow \\ \downarrow \\ \downarrow \\ \rightarrow \\ \rightarrow \\ \rightarrow \end{array} $	$\begin{array}{ccc} \rightarrow & \text{Mirai} \\ \rightarrow & \text{WannaCry} \\ \rightarrow & \text{Conficker} \\ \rightarrow & \text{Avalanche} \\ \uparrow & \text{Avalanche} \\ \uparrow & \text{Nymaim} \\ \Downarrow & \text{Virut} \\ \downarrow & \text{Sality} \\ \rightarrow & \text{VPNFilter} \\ \rightarrow & \text{Tinba} \end{array}$	$\begin{array}{c c c c c c } & \label{eq:interm} \text{IP addresses} \\ \hline \rightarrow & \text{Mirai} & 2,859 \\ \hline \rightarrow & \text{WannaCry} & 415 \\ \hline \rightarrow & \text{Conficker} & 365 \\ \hline \rightarrow & \text{Avalanche} & 336 \\ \hline \uparrow & \text{Nymaim} & 166 \\ \hline \downarrow & \text{Virut} & 160 \\ \hline \downarrow & \text{Virut} & 160 \\ \hline \downarrow & \text{Sality} & 88 \\ \hline \rightarrow & \text{VPNFilter} & 65 \\ \hline \rightarrow & \text{Tinba} & 56 \\ \end{array}$

Table 3: Major Botnet families in Hong Kong network





Trend of 5 Botnet families in Hong Kong network

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

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

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





What is a Botnet (Bots)?

• A Botnet (Bots) is usually a personal computer that is infected by malicious software to become part of a botnet. Once infected, the malicious software usually hides itself, and stealthily connects to the Command & Control Server to get instructions from the hackers.

What are the potential impacts?

- Computers may be commanded to perform other hacking or criminal activities
- Computer owner's personal and financial data may be stolen which may lead to financial loss
- Commands from hackers may lead to other malicious activities, e.g. spreading malicious software or launching DDoS attacks

Sources of Information:

- ShadowServer botnet_drone
- ShadowServer sinkhole_http_drone
- Shadowserver Microsoft_sinkhole



Appendix

A Sources of information in IFAS

The following information feeds are information sources of IFAS:

Table 5: I	FAS Sources	of Information
------------	-------------	----------------

Event Type	Source	First introduced
Defacement	Zone - H	2013-04
Phishing	CleanMX - Phishing	2013-04
Phishing	Phishtank	2013-04
Malware Hosting	CleanMX - Malware	2013-04
Malware Hosting	Malc0de	2013-04
Malware Hosting	MalwareDomainList	2013-04
Botnet (C&Cs)	Shadowserver - C&Cs	2013-09
Botnet (Bots)	Shadowserver - botnet_drone	2013-08
Botnet (Bots)	Shadowserver - sinkhole_http_drone	2013-08
Botnet (Bots)	Shadowserver - microsoft_sinkhole	2013-08

B Geolocation identification methods in IFAS

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

Table 6: Methods of Geolocation Identification

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



C Major Botnet Families

Table 7: Botnet Families

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Avalanche	Nil	Crimeware-as-	• Depends on underlying	 Send spams
		a-service	malwares	 Host phishing sites
				Host malware
				 Steal sensitive information
Bamital	Nil	Trojan	 Drive-by download via 	Click fraud
			exploit kit	 Search hijacking
			 Via P2P network 	
BankPatch	 MultiBanker 	Banking Trojan	 Via adult web sites 	 Monitor specific
	 Patcher 		 Corrupt multimedia 	banking websites and
	 BankPatcher 		codecs	harvest user's
			 Spam e-mail 	passwords, credit card
			 Chat and messaging 	information and other
			systems	sensitive financial data
Bedep	Nil	Trojan	 Via adult web sites 	 Click fraud
			 Malvertising 	 Download other malwares
BlackEnergy	Nil	DDoS Trojan	 Rootkit techniques to 	 Launch DDoS attacks
			maintain persistence	
			 Uses process injection 	
			technique	
			 Strong encryption and 	
			modular architecture	
Citadel	Nil	Banking Trojan	 Avoid and disable 	 Steal banking
			security tool detection	credentials and
				sensitive information
				 Keystroke logging
				 Screenshot capture
				 Video capture
				 Man-in-the-browser
				attack
				Ransomware
Conficker	 Downadup 	Worm	 Domain generation 	 Exploit the Windows
	• Kido		algorithm (DGA)	Server Service
			capability	vulnerability (MS08-067)
			 Communicate via P2P 	 Brute force attacks
			network	for admin credential to
			 Disable security 	spread across network
			software	 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
		Barring Hojarr		information
				Install other malware
				Backdoor capabilities
				that allow unauthorised
				access
Duro	Nil	Panking Trojan	• Snam a mail	
Dyre	INII	Banking Trojan	 Spam e-mail 	Steal banking credential by tricking
				credential by tricking the victim to call an
				illegitimate number
6		D 1 1 1		Send spams
Gamarue	Andromeda	Downloader/	Via exploit kit	Steal sensitive
		Worm	Spam e-mail	information
			MS Word macro	 Allow unauthorised
			 Removable-drives 	access
				 Install other malware
Ghost Push	Nil	Mobile malware	 Via app installation 	 Gain root access
				 Download other malware
Glupteba	Nil	Trojan	 Drive-by download via 	 Push contextual
			Blackhole Exploit Kit	advertising and
				clickjacking to victims
IRC Botnet	Nil	Trojan	 Communicate via IRC 	 Backdoor capabilities
			network	that allow unauthorised
				access
				 Launch DDoS attack
				 Send spams
Mirai	Nil	Worm	 Telnet with vendor 	Launch DDoS attacks
			default credentials	
Murofet	Nil	Trojan	File infection	 Download other malware
		•	 Via exploit kits 	
Nivdort	Nil	Trojan	• Spam e-mail	 Steal login credentials
		- 3 -		and sensitive information
Nymaim	Nil	Trojan	• Spam e-mail	Lock infected systems
,			Malicious link	Stop victims from
				accessing files
				Ask for ransom
Matsnu	Nil	Trojan	Spam e-mail	Backdoor capabilities
Watshu		nojun	Span e mai	that allow unauthorised
				access
				Lock infected systems
				-
				Encrypt user dataAsk for ransom
Dalava	• Dimonual	Morm	· Corond via instant	
Palevo	Rimecud	Worm	Spread via instant	Backdoor capabilities
	Butterfly		messaging, P2P network	that allow unauthorised
	bot		and removable drives	access
	Pilleuz			Steal login credentials
	Mariposa			and sensitive information
	 Vaklik 			Steal money directly
				from banks using money mules



Table 9: Botnet Families (cont.)

Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
Pushdo	Cutwail	Downloader	 Hiding its malicious 	 Download other banking
	 Pandex 		network traffic	malware (e.g. Zeus and
			 Domain generation 	Spyeye)
			algorithm (DGA)	Launch DDoS attacks
			capability	 Send spams
			 Distribute via drive 	
			by download	
			 Exploit browser and 	
			plugins' vulnerabilities	
Ramnit	Nil	Worm	 File infection 	 Backdoor capabilities
			 Via exploit kits 	that allow unauthorised
			 Public FTP servers 	access
				 Steal login
				credentials and
				sensitive information
Sality	Nil	Trojan	 Rootkit techniques to 	 Send spams
			maintain persistence	 Proxying of
			Communicate via P2P	communications
			network	 Steal sensitive
			 Spread via removable 	information
			drives and shares	Compromise web servers
			 Disable security 	and/or coordinating
			software	distributed computing
			 Use polymorphic and 	tasks for the purpose of
			entry point obscuring	processing intensive
			(EPO) techniques to	tasks (e.g. password
			infect files	cracking)
				 Install other malware
Slenfbot	Nil	Worm	 Spread via removable 	 Backdoor capabilities
			drives and shares	that allow unauthorised
				access
				 Download financial
				malware
				 Sending spam
				Launch DDoS attacks
Tinba	 TinyBanker 	Banking Trojan	 Via exploit kit 	 Steal banking
	 Zusy 		 Spam e-mail 	credential and sensitive
				information
Torpig	Sinowal	Trojan	Rootkit techniques to	Steal sensitive
	Anserin		maintain persistence	information
			(Mebroot rootkit)	Man in the browser
			Domain generation	attack
			algorithm (DGA)	
			capability	
			Distribute via drive by download	

Table 10: Botnet Families (cont.)

VirutNilTrojan• Spread via removable drives and shares• Send spamsVPNFilterNilWorm• Possibly exploit device vulnerabilities• Launch DDS attacks • Launch DDS attacksVPNFilterNilWorm• Possibly exploit device vulnerabilities• Launch network attacks • Launch network attacks • Launch network attacks • Disrupt Internet connectionWannaCry• WannaCryptRansomware • Spread across network • Exploit Windows SMB vulnerabilities• Demand ransom • Data unrecoverable • Backdoor capabilities • Download and drop additional destructive payloads • Alter important files causing unreliable system performance • Sirefef• Max++ • Trojan • Rootkit techniques to • Distribute via drive • Distribute via drive	Major Botnets	Alias	Nature	Infection Method	Attacks / Impacts
VPNFilter Nil Worm • Possibly exploit - Launch network attacks device vulnerabilities - Leak network traffic - Dosrupt internet connection WannaCry • WannaCrypt Ransomware • Spread across network • Exploit Windows SMB Wapomi Nil Worm • Spread via removable • Demand ransom Vulnerabilities • Data unrecoverable • Data unrecoverable • Data unrecoverable Wapomi Nil Worm • Spread via removable • Data unrecoverable files • Infects executable additional destructive payloads VeroAccess • Max++ Trojan • Rootkit techniques to • Gather computer • Sirefef maintain persistence • Bitcrin mining and click fraud Vg by download • Distribute via drive • Bitcrin mining and click fraud viguise as legitimate • Distribute via drive • Steal banking creential and sensitive zeus • Gameover Banking Trojan • Stealthy techniques to • Steal banking reductive via drive • Distribute via drive • Distribute via drive • Distrindute via drive	Virut	Nil	Trojan	 Spread via removable 	Send spams
VPNFilterNilWormPossibly exploit device vulnerabilitiesLaunch network traffic flowing through the infected devicesWannaCry• WannaCryptRansomware• Spread across network • Exploit Windows SMB• Encrypt user data • Distrubutevia drives and shares• Demand ransom • Data unrecoverableWapomiNilWorm• Spread via removable drives and shares• Data durecoverable • Distrubutevia drives and shares• Download and drop additional destructive payloads • Alter important files causing unreliable system performance • Gather computer activity, transmit private data and cause sluggish computerZeroAccess• Max++Trojan• Rootkit techniques to maintain persistence • Distribute via drive by download• Steal banking credential and sensitive infert serviceZeroAccess• GameoverBanking Trojan entwork• Steal banking credential and sensitive infert service e Communicate via P2P network• Steal banking credential and sensitive informationZeus• GameoverBanking Trojan maintain persistence • Distribute via drive by download• Steal banking credential and sensitive informationZeus• GameoverBanking Trojan maintain persistence • Distribute via drive by download• Steal banking credential and sensitive informationZeus• GameoverBanking Trojan maintain persistence • Distribute via drive by download• Steal banking credential and sensitive informationZeus• GameoverBanking Trojan maintain persistence • Distribute via drive 			•	-	· · · · · · · · · · · · · · · · · · ·
VPNFilterNilWorm• Possibly exploit device vulnerabilities- Launch network attacks flowing through the infected devicesWannaCry• WannaCryptRansomware • Spread across network • Exploit Windows SMB vulnerabilities• Disrupt Internet connection • Dara unrecoverable drives and shares • Infects executable files• Demand ransom • Data unrecoverable • Data unrecoverable • Data unrecoverable • Data unrecoverable additional destructive payloads • Alter important files causing unreliable system performance • Gather computer • Sirefef• Max++ • Trojan • Rootkit techniques to maintain persistence • Distribute via drive by download • Distribute via drive by download• Steal banking credential and sensitive informationZeus• GameoverBanking 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 atack • Keystroke logging • Download other malware<					Fraud
device vulnerabilities• Leak network traffic flowing through the infected devicesWannaCry• WannaCrypt Ransomware• Spread across network • Exploit Windows SMB • Disrupt Internet connectionWapomiNilWorm• Spread via removable drives and shares • Infects executable files• Data unrecoverableWapomiNilWorm• Spread via removable drives and shares • Infects executable files• Download and drop apaloads • Atter important files causing unreliable system performance • Gather computer activity, transmit private data and cause slugish computerZeroAccess• Max++Trojan• Rootkit techniques to by download • Distribute via drive by download• Distribute via click fraudZeus• GameoverBanking Trojan • Steal by techniques to by download • Distribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive maintain persistence • Distribute via drive by download • Distribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive information • Man in the browser attackZeus• GameoverBanking Trojan e Oormunicate via P2P information• Steal banking redential and sensitive informationZeus• GameoverBanking Trojan e Oormunicate via P2P information• Steal banking redential and sensitive informationZeus• GameoverBanking Trojan e Oormunicate via P2P information• Steal banking redential and sensitive informationZeus• Gameover <td></td> <td></td> <td></td> <td></td> <td>Data theft</td>					Data theft
device vulnerabilities• Leak network traffic flowing through the infected devicesWannaCry• WannaCrypt Ransomware• Spread across network • Exploit Windows SMB • Disrupt Internet connectionWapomiNilWorm• Spread via removable drives and shares • Infects executable files• Data unrecoverableWapomiNilWorm• Spread via removable drives and shares • Infects executable files• Download and drop apaloads • Atter important files causing unreliable system performance • Gather computer activity, transmit private data and cause slugish computerZeroAccess• Max++Trojan• Rootkit techniques to by download • Distribute via drive by download• Distribute via click fraudZeus• GameoverBanking Trojan • Steal by techniques to by download • Distribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive maintain persistence • Distribute via drive by download • Distribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive information • Man in the browser attackZeus• GameoverBanking Trojan e Oormunicate via P2P information• Steal banking redential and sensitive informationZeus• GameoverBanking Trojan e Oormunicate via P2P information• Steal banking redential and sensitive informationZeus• GameoverBanking Trojan e Oormunicate via P2P information• Steal banking redential and sensitive informationZeus• Gameover <td>VPNFilter</td> <td>Nil</td> <td>Worm</td> <td> Possibly exploit </td> <td> Launch network attacks </td>	VPNFilter	Nil	Worm	 Possibly exploit 	 Launch network attacks
WannaCry WannaCryptRansomware Ransomware· Spread across network · Exploit Windows SMB · Demand ransom · Data unrecoverable· Domand ransom · Data unrecoverableWapomiNilWorm· Spread via removable drives and shares · Download and drop additional destructive payloads · Alter important files causing unreliable system performance · Gather computer · Sirefef· Backdoor capabilities · Download and drop additional destructive payloads · Alter important files causing unreliable system performance · Gather computer · SirefefZeroAccess· Max++ · SirefefTrojan· Rootkit techniques to maintain persistence · Communicate via P2P network · Distribute via drive by download· Download other malware · Bitcoin mining and click fraudZeus· GameoverBanking Trojan · Stealthy techniques to maintain persistence · Distribute via drive by download· Steal banking credential and sensitive · Distribute via drive by downloadZeus· GameoverBanking Trojan · Stealthy techniques to maintain persistence · Distribute via drive by download · Distribute via drive · Stealthy techniques to · Steal banking · Communicate via P2P · Other and sensitive · Distribute via drive · Steal banking · Man in the browser · Communicate via P2P · Other and via drive ·				· · ·	 Leak network traffic
WannaCry WannaCryptRansomware Ransomware· Spread across network · Exploit Windows SMB · Demand ransom · Data unrecoverable· Domand ransom · Data unrecoverableWapomiNilWorm· Spread via removable drives and shares · Download and drop additional destructive payloads · Alter important files causing unreliable system performance · Gather computer · Sirefef· Backdoor capabilities · Download and drop additional destructive payloads · Alter important files causing unreliable system performance · Gather computer · SirefefZeroAccess· Max++ · SirefefTrojan· Rootkit techniques to maintain persistence · Communicate via P2P network · Distribute via drive by download· Download other malware · Bitcoin mining and click fraudZeus· GameoverBanking Trojan · Stealthy techniques to maintain persistence · Distribute via drive by download· Steal banking credential and sensitive · Distribute via drive by downloadZeus· GameoverBanking Trojan · Stealthy techniques to maintain persistence · Distribute via drive by download · Distribute via drive · Stealthy techniques to · Steal banking · Communicate via P2P · Other and sensitive · Distribute via drive · Steal banking · Man in the browser · Communicate via P2P · Other and via drive ·					flowing through the
WannaCry WannaCrypt• WannaCryptRansomware Amsomware• Spread across network • Exploit Windows SMB vulnerabilities • Data unrecoverable • Data unrecoverable • Data unrecoverable • Data unrecoverable • Data unrecoverable • Backdoor capabilities • Download and drop additional destructive payloads • Alter important files causing unreliable system performance • Gather computer activity, transmit private data and cause slugish computerZeroAccess• Max++ • SirefefTrojan • Rootkit techniques to • Distribute via drive by download• Download other malware • Bitribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive • Steal banking credential and sensitive • Steal banking credential and sensitive • Distribute via drive by download• Steal banking credential and sensitive • Steal banking credential and sensitive • Steal banking credential and sensitive • Distribute via drive by download • Man in the browser attack					
WannaCry WannaCrypt• WannaCryptRansomware Amsomware• Spread across network • Exploit Windows SMB vulnerabilities • Data unrecoverable • Data unrecoverable • Data unrecoverable • Data unrecoverable • Data unrecoverable • Backdoor capabilities • Download and drop additional destructive payloads • Alter important files causing unreliable system performance • Gather computer activity, transmit private data and cause slugish computerZeroAccess• Max++ • SirefefTrojan • Rootkit techniques to • Distribute via drive by download• Download other malware • Bitribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive • Steal banking credential and sensitive • Steal banking credential and sensitive • Distribute via drive by download• Steal banking credential and sensitive • Steal banking credential and sensitive • Steal banking credential and sensitive • Distribute via drive by download • Man in the browser attack					• Disrupt Internet connection
Wapomi Nil Worm • Spread via removable drives and shares • Data unrecoverable Wapomi Nil Worm • Spread via removable drives and shares • Backdoor capabilities Infects executable files • Infects executable files • Download and drop additional destructive payloads • Alter important files causing unreliable system performance ZeroAccess • Max++ Trojan • Rootkit techniques to maintain persistence • Oownload other malware • Sirefef maintain persistence • Bitcoin mining and • Distribute via drive by download • Distribute via drive by download Zeus • Gameover Banking Trojan • Stealthy techniques to maintain persistence • Stealthy techniques to network • Stealthy techniques to network • Stealthy techniques to maintain persistence • Stealthy techniques to network • Steal banking credential and sensitive information Zeus • Gameover Banking Trojan • Stealthy techniques to maintain persistence • Steal banking credential and sensitive information • Steal banking credential and sensitive information	WannaCry	 WannaCrypt 	Ransomware	 Spread across network 	•
WapomiNilWorm• Spread via removable drives and shares • Infects executable dives and shares • Infects executable additional destructive payloadsAlter important files causing unreliable system performance • Gather computer activity, transmit private data and cause sluggish computerZeroAccess• Max++ SirefefTrojan• Rootkit techniques to maintain persistence • Distribute via drive by download• Download other malware otick fraudZeroAccess• Max++ SirefefTrojan• Rootkit techniques to maintain persistence • Distribute via drive by download• Download other malware • Bitcoin mining and click fraudZeus• GameoverBanking Trojan• Stealthy techniques to maintain persistence • Distribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive informationZeus• GameoverBanking Trojan• Stealthy techniques to maintain persistence • Distribute via disguise as legitimate file (eg. media files, keygen)• Steal banking credential and sensitive informationZeus• GameoverBanking Trojan• Stealthy techniques to maintain persistence • Distribute via drive• Steal banking credential and sensitive informationZeus• GameoverBanking Trojan• Stealthy techniques to maintain persistence • Distribute via drive • Distribute via dri		,,		•	
drives and shares• Download and dropadditional destructiveadditional destructivefilespayloads• Alter important filescausing unreliablesystem performancesystem performance· Gather computeractivity, transmitprivate data and causesluggish computerZeroAccess• Max++Trojan• Rootkit techniques to· Sirefef· Nownload other malware• Bitcoin mining and· Sirefef· Communicate via P2P· Click fraud· Sirefef· Distribute via drive· Distribute via drive· Distribute via drive· Distribute via· Steal banking· Sugais· Steal banking Trojan· Steal banking· Communicate via P2P· Steal banking· Credential and sensitive· Distribute via drive· Distribute via· Steal banking· Distribute via drive· Distribute via drive· Steal banking· Distribute via· Steal banking· Credential and sensitive· Distribute via drive· Distribute via drive· Steal banking· Zeus· GameoverBanking Trojan· Stealthy techniques to maintain persistence· Distribute via drive· Distribute via drive· Steal banking· Distribute via drive· Steal banking· Communicate via P2P· Distribute via drive· Distribute via drive· Man in the browser· Distribute via drive· Distribute via drive· Man in the browser· Distribute via drive· Communicate via P2P· Man in the browser<				•	Data unrecoverable
drives and shares• Download and dropadditional destructiveadditional destructivefilespayloads• Alter important filescausing unreliablesystem performancesystem performance· Gather computeractivity, transmitprivate data and causesluggish computerZeroAccess• Max++Trojan• Rootkit techniques to· Sirefef· Nownload other malware• Bitcoin mining and· Sirefef· Communicate via P2P· Click fraud· Sirefef· Distribute via drive· Distribute via drive· Distribute via drive· Distribute via· Steal banking· Sugais· Steal banking Trojan· Steal banking· Communicate via P2P· Steal banking· Credential and sensitive· Distribute via drive· Distribute via· Steal banking· Distribute via drive· Distribute via drive· Steal banking· Distribute via· Steal banking· Credential and sensitive· Distribute via drive· Distribute via drive· Steal banking· Zeus· GameoverBanking Trojan· Stealthy techniques to maintain persistence· Distribute via drive· Distribute via drive· Steal banking· Distribute via drive· Steal banking· Communicate via P2P· Distribute via drive· Distribute via drive· Man in the browser· Distribute via drive· Distribute via drive· Man in the browser· Distribute via drive· Communicate via P2P· Man in the browser<	Wapomi	Nil	Worm	• Spread via removable	Backdoor capabilities
 Infects executable files Alter important files Alter important files Causing unreliable System performance Gather computer Gather computer Gather computer Gather computer Sirefef Nax++ Trojan Rootkit techniques to Download other malware Bitcoin mining and Communicate via PC Distribute via drive Distribute via drive Distribute via Gather computer Sirefef Sirefef Communicate via PC Communicate via PC Distribute via drive Distribute via drive Distribute via Other malware Distribute via Sirefef Sirefibute via Sirefef Sirefe					
 Alter important files Alter important files causing unreliable system performance Gather computer activity, transmit private data and cause sluggish computer ZeroAccess Max++ Trojan Rootkit techniques to Bitcoin mining and click fraud ZeroAccess Max++ Trojan Rootkit techniques to Distribute via drive Bitcoin mining and click fraud ZeroAccess Max++ Sirefef Sirefef Sirefue Communicate via P2P Communicate via P2P network Distribute via drive by download Distribute via drive by download Steal banking credential and sensitive nofrmation by download Man in the browser atack Keystroke logging Download other malware				 Infects executable 	-
 Alter important files Alter important files Causing unreliable system performance Gather computer activity, transmit private data and cause sluggish computer ZeroAccess Max++ Trojan Rootkit techniques to Bitcoin mining and click fraud Sirefef Sirefef Communicate via P2P network Distribute via drive by download Distribute via drive by download Steal banking credential and sensitive notimating persistence Distribute via drive by download Steal banking credential and sensitive notimating persistence Distribute via drive bitribute via drive by download Man in the browser atack Keystroke logging Download other malware				files	payloads
Causing unreliablesystem performancesystem performanceSystem performanceGather computeractivity, transmitprivate data and causesluggish computerStrefefNax++TrojanRootkit techniques toSirefefmaintain persistenceSirefefCommunicate via P2PnetworkDistribute via driveDistribute via driveby downloadSirefefStrefefS					
System performanceGather computeractivity, transmitprivate data and causesluggish computerZeroAccess• Max++Trojan• Rootkit techniques to maintain persistence• Sirefef• Communicate via P2P networkCommunicate via P2P• Bitcoin mining and click fraudCommunicate via P2P• Distribute via drive by downloadPistribute via drive• Distribute via file (gggn)Zeus• GameoverBanking TrojanZeus• GameoverBanking TrojanVerture• Stealthy techniques to maintain persistence· Distribute via drive• Steal banking credential and sensitive information· Distribute via drive• Stealthy techniques to maintain persistence· Distribute via drive• Distribute via drive· Distribute via drive• Steal banking redential and sensitive information· Distribute via drive• Distribute via drive· Distribute via drive•					-
Image: Second					-
Activity, transmitprivate data and causesluggish computerZeroAccess• Max++Trojan• Rootkit techniques to• Sirefefmaintain persistence• Sirefef• Communicate via P2P· Communicate via P2P· Bitcoin mining and· Communicate via P2P· Communicate via P2P· Distribute via drive· Distribute via drive· Distribute via drive· Distribute via drive· Distribute via· Cenedia files, · keygen)Zeus· GameoverBanking Trojan· Stealthy techniques to · Distribute via drive· Steal banking· Distribute via drive· Distribute via drive· Distribute via drive· Man in the browser· Distribute via drive· Man in the browser· Communicate via P2P· Man in the browser· Communicate via P2P· Keystroke logging · Download other malware					
Private data and cause sluggish computerZeroAccess• Max++Trojan• Rootkit techniques to maintain persistence • Communicate via P2P• Download other malware• Sirefefmaintain persistence • Communicate via P2P• Bitcoin mining and click fraudImage: Communicate via P2P• Communicate via P2P• Cick fraudImage: Communicate via P2P• Distribute via drive • Distribute via drive • Distribute via drive• Distribute via driveImage: Communicate via P2P• Distribute via drive • Distribute via drive• Distribute via driveImage: Communicate via P2P• Distribute via drive • Distribute via• Distribute viaImage: Communicate via P2P• Distribute via• Distribute viaImage: Communicate via P2P• Steal banking • Distribute via drive • Distribute via drive• Steal bankingImage: Communicate via P2P• Communicate via P2P • Communicate via P2P• Man in the browser attackImage: Communicate via P2P • Download other malware• Download other malware					
ZeroAccess• Max++ • SirefefTrojan• Rootkit techniques to maintain persistence • Communicate via P2P network • Distribute via drive by download • Distribute via drive • Distribute via • Steal banking • Steal banking • Steal banking • Steal banking • Oistribute via drive • Distribute via drive • Man in the browser attackImage: Distribute via drive • Communicate via P2P • Rework• Keystroke logging • Download other malware					•
 Sirefef maintain persistence Bitcoin mining and click fraud Communicate via P2P network Distribute via drive by download Distribute via disguise as legitimate file (eg. media files, keygen) Zeus Gameover Banking Trojan Stealthy techniques to maintain persistence Distribute via drive Steal banking credential and sensitive information Man in the browser tack network Keystroke logging Download other malware 					sluggish computer
 Communicate via P2P click fraud network Distribute via drive by download Distribute via disguise as legitimate file (eg. media files, keygen) Zeus Gameover Banking Trojan Stealthy techniques to maintain persistence Distribute via drive Distribute via drive Man in the browser Keygen Man in the browser Communicate via P2P Keystroke logging Download other malware 	ZeroAccess	• Max++	Trojan	 Rootkit techniques to 	 Download other malware
network Distribute via drive Distribute via drive by download Distribute via Distribute via Distribute via disguise as legitimate file (eg. media files, keygen) Zeus Gameover Banking Trojan Stealthy techniques to maintain persistence Distribute via drive Amaintain persistence Distribute via drive Man in the browser Attack Network Keystroke logging Download other malware 		Sirefef		maintain persistence	 Bitcoin mining and
 Distribute via drive by download Distribute via Distribute via Distribute via disguise as legitimate file (eg. media files, keygen) Zeus Gameover Banking Trojan Stealthy techniques to maintain persistence Distribute via drive Man in the browser Attack Man in the browser Matick Download other malware 				Communicate via P2P	click fraud
by download Distribute via disguise as legitimate file (eg. media files, keygen) Zeus Gameover Banking Trojan Stealthy techniques to maintain persistence Distribute via drive Distribute via drive Distribute via drive by download Man in the browser attack Communicate via P2P network Keystroke logging Download other malware				network	
 Distribute via disguise as legitimate file (eg. media files, keygen) Gameover Banking Trojan Stealthy techniques to maintain persistence Distribute via drive information Man in the browser by download Man in the browser Communicate via P2P Keystroke logging Download other malware 				 Distribute via drive 	
disguise as legitimate file (eg. media files, keygen) Zeus • Gameover Banking Trojan • Stealthy techniques to maintain persistence credential and sensitive • Distribute via drive information • Man in the browser • Communicate via P2P attack • Download other malware				by download	
Image: Second				Distribute via	
ZeusGameoverBanking TrojanStealthy techniques to maintain persistenceSteal banking credential and sensitiveCommunicate via driveDistribute via driveinformationCommunicate via P2PAttackAttackCommunicate via P2PSteystroke logging Download other malware				disguise as legitimate	
ZeusGameoverBanking TrojanStealthy techniques to maintain persistenceSteal bankingGameoverBanking TrojanMaintain persistencecredential and sensitiveDistribute via driveDistribute via driveinformationSealthy techniques toSteal bankingSteal bankingSealthy techniques toDistribute via driveinformationSealthy techniques toSteal bankingSteal bankingSealthy techniques toSteal bankinginformationSealthy techniques toSteal bankingSteal bankingSealthy techniques toSteal banking techniques toSteal banking techniques toSealthy techniques toSteal banking techniques toSteal banking techniques toSealthy techniques toSteal banki				file (eg. media files,	
maintain persistencecredential and sensitive• Distribute via driveinformationby download• Man in the browser• Communicate via P2Pattacknetwork• Keystroke logging• Download other malware				keygen)	
maintain persistencecredential and sensitive• Distribute via driveinformation• by download• Man in the browser• Communicate via P2Pattacknetwork• Keystroke logging• Download other malware	Zeus	Gameover	Banking Trojan	 Stealthy techniques to 	 Steal banking
by download • Man in the browser • Communicate via P2P attack network • Keystroke logging • Download other malware			-	maintain persistence	_
Communicate via P2P attack network Keystroke logging Download other malware				 Distribute via drive 	information
network • Keystroke logging • Download other malware				by download	 Man in the browser
Download other malware				 Communicate via P2P 	attack
				network	Keystroke logging
					 Download other malware
(eg. Cryptolocker)					(eg. Cryptolocker)
Launch DDoS attacks					 Launch DDoS attacks