

7.7 DDoS : Unknown Secrets and Botnet Counter-Attack



www.issuemakerslab.com
sionics & kaientt

7.7 DDoS

Overview

Botnet Structure

Bot Malware Analysis

Botnet Counter-Attack

Demo

❖ 7.7 DDoS Attack

- Cyber attack against major government, news media, and financial websites of South Korea and US

Simultaneous Cyber Attacks Hit Korea, US

By Jane Han
Staff Reporter

Korea and the United States were hit by cyber attacks almost simultaneously Wednesday.

The massive attack paralyzed major government Web sites here, including Cheong Wa Dae, the Ministry of National Defense and the National Assembly, as well as Shinhan and Korea Exchange banks and Internet portal service provider Naver.

The unprecedented hacking led to a shutdown of the sites or “no

Related Stories on Pages 6 & 8

access” messages.

So far, the identities of the infiltrators are a mystery and the motives behind the attacks are also largely unknown.

Earlier in the day, a virus was sent to many personal computers in both countries directing them to visit the targeted Web sites at the same time. Since July 4, U.S. sites and systems have come under similar attacks, which are believed to be able to overwhelm anti-hacking security

systems in place.

North Korea is suspected of playing a part in the latest round of cyber “warfare” that paralyzed government networks and leading portal servers, sources quoted the National Intelligence Service (NIS) as saying in a briefing to lawmakers Wednesday.

Sites run by the presidential office, the Assembly, the defense ministry and Naver were down from Tuesday evening to beyond midnight.

China, North Korea and Russia were initially thought to be possible culprits. But the NIS briefed the lawmakers on its analysis which tentatively concluded that Pyongyang or its sympathizers were behind the cyber attacks. It was not immediately available how the NIS came to such a conclusion.

Earlier in the day, the Korea Communications Commissions (KCC), the nation’s telecom regulator, said tracking down the source of the DDoS attacks will be difficult, as they involve a huge number of sources and are hard to pin down.

These types of attacks are

North Korea is suspected of playing a part in the latest round of cyber “warfare” that paralyzed government networks and leading portal servers, sources quoted the National Intelligence Service as saying. It was not immediately available how the agency came to such a conclusion.

orchestrated to send a flood of electronic traffic to a targeted Web site, which eventually overloads the computer network and renders it inaccessible. They are known to be easy to launch and are highly disruptive.

No major damage has been reported so far, according to the state-run Korea Information Security Agency (KISA), but it warned that future shutdowns cannot be ruled out as networks remain unstable.

Sites of leading online shopping mall Auction and major daily Chosun Ilbo — as well as Cheong

Wa Dae — also remained inaccessible.

The KCC issued a warning against future attacks, while the defense ministry is considering raising its Information Operations Condition status to a heightened alert level.

According to police data, over the past five years cyber hacking cases have surged 30 percent in Korea, one of the world’s most wired nations with over two-thirds of the population having high-speed Internet access.

KISA spokeswoman Ahn Jeong-eun said hacking attempts are

increasing, but defended the country’s cyber security standards.

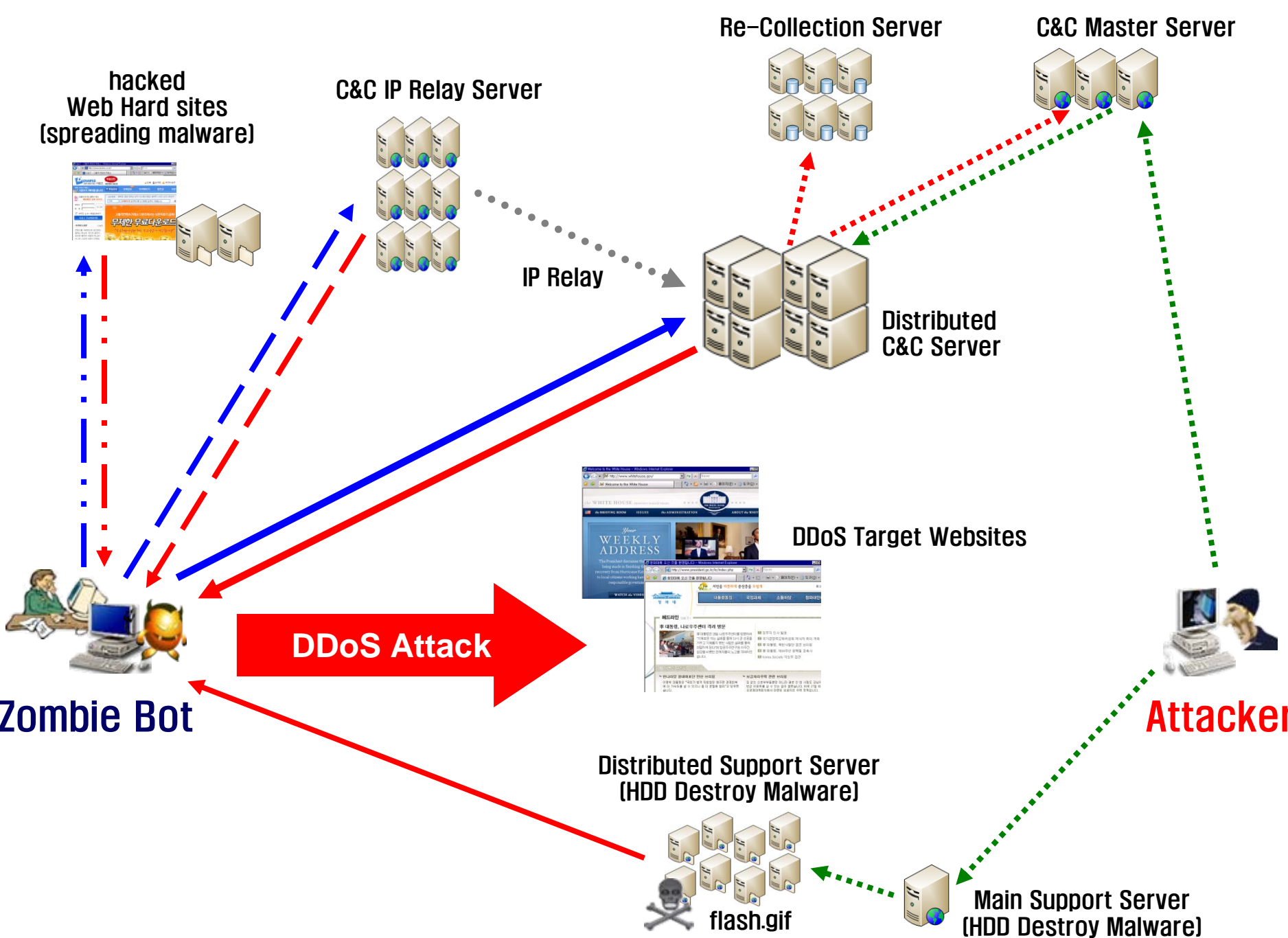
“We uphold high system standards, but it is difficult to stave off a large-scale attack that has been waged for a specific purpose,” she said, adding that Korean Web sites have already been made aware of the recent assaults and are devising solutions.

KISA officials said they are looking at why simultaneous attacks were made starting around 6 p.m. Tuesday evening.

Chung Hee-nam of the National Association of Hacking and Security said that defense against DDoS has been on South Korea’s 2009 information-technology to-do list, but noted that individual personal computer owners must protect their own systems from being exploited to launch a daemon.

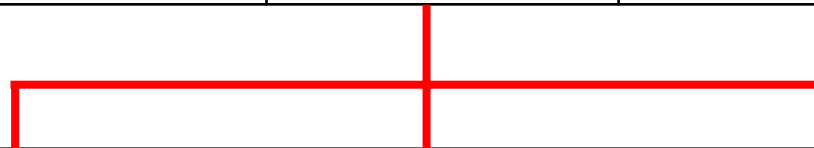
The KCC said more than 18,000 computers have been affected by the latest attack, adding that it requested Internet service providers to distribute vaccine programs to those users whose computers have been infected.

jhan@koreatimes.co.kr



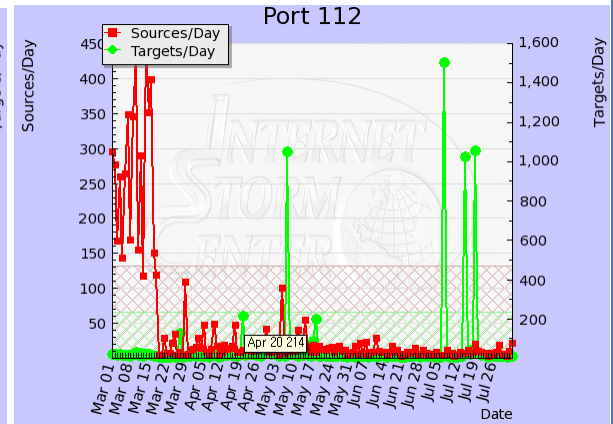
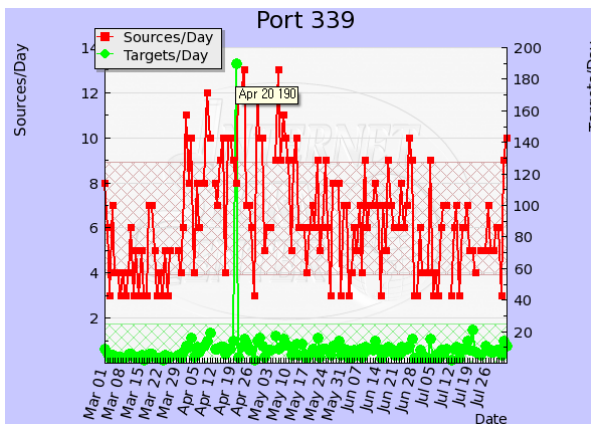
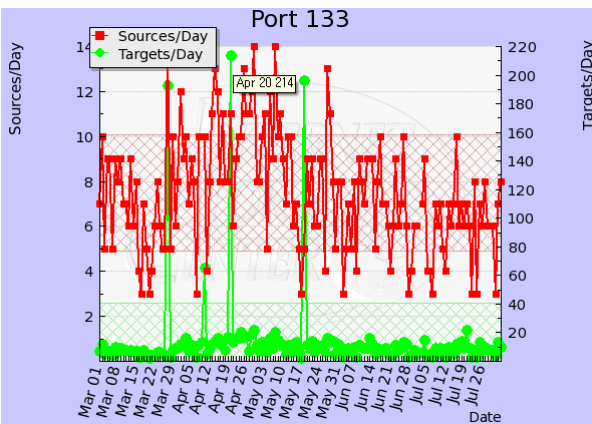
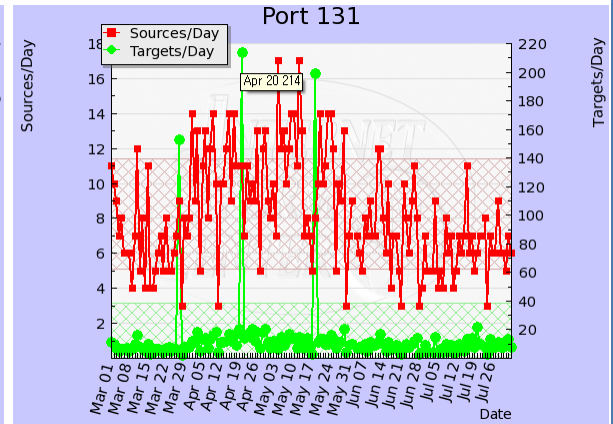
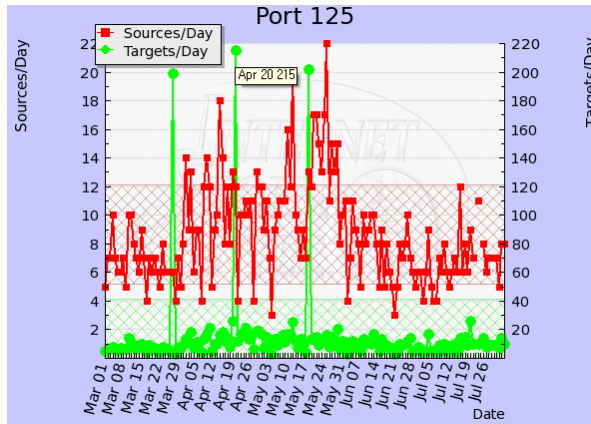
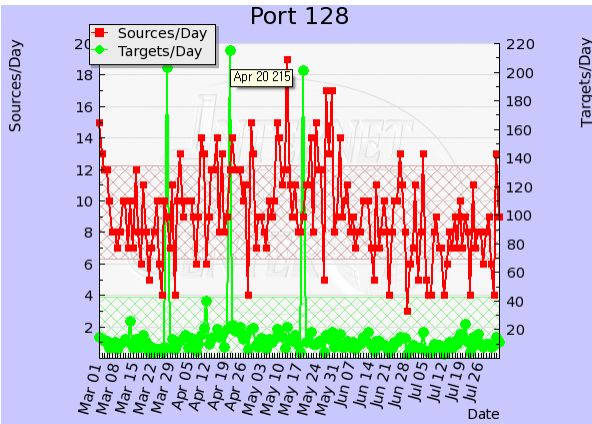
Botnet Begins!

	Encryption Protocol	Filename	Port
X	send: + 0x28) ^ 0x47 recv: ^ 0x47) - 0x28	dvcmgmt.exe	131
		ntdsbcli.exe	143
		ntdcmgt.exe	339
Y	send: ^ 0x92) + 0x61 recv: - 0x61) ^ 0x92	inetsvc.exe	112, 125, 133
		perfmon.exe	112, 125, 133
		tasksc.exe	128, 125, 133



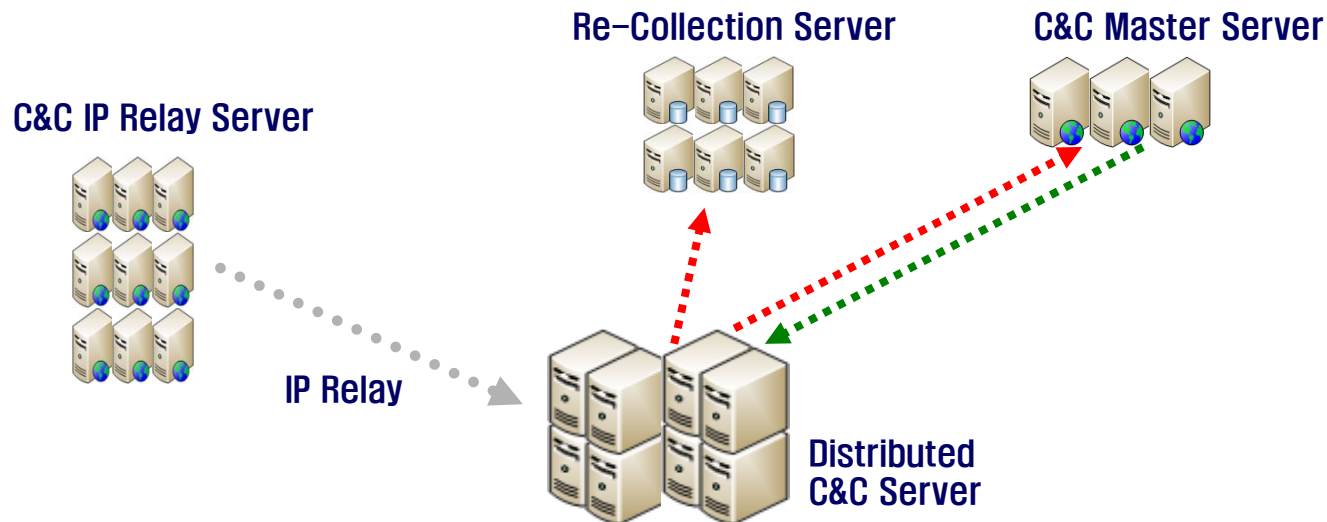
	A	B	C
Encryption Protocol	XOR 0xCC	XOR 0xFC	XOR Ramdom 8 Bytes
C&C Master Server	???	ntmssvc.exe	???
Re-Collection Server	???	???	???
Distributed C&C Server	netlmgr.exe	ntmpcsvc.exe	???
C&C IP Relay Server	213.33.116.41:53	75.144.115.102:53	98.118.201.35:443
	216.199.83.203:80	67.69.18.51:53	93.104.211.61:53
	213.23.243.210:443	220.250.64.246:443	116.68.144.212:80

Botnet Begins!



Structure of Botnet

- ❖ Composed in hierarchical structure
- ❖ C&C Server was operated as a distributed server by more than thousands of units through hacking.



File Information Stealing Malware

- ❖ The hackers first circulated malwares that collect file information beforehand.
- ❖ These are estimated to have been circulated through various ways.
- ❖ The malwares collected information about the files that exist in the directories such as Recent, My Documents, Favorites and etc. from Victim's PCs and sent it to the C&C Server.

3 Types of Malware

	A	B	C
Encryption Protocol	XOR 0xCC	XOR 0xFC	XOR Ramdom 8 Bytes
DDoS Malware (July ~)			
Beginning	msiexec?.exe (= ntdll.exe)	wimgat.exe	dhcp32.exe (= ntdll.exe)
C&C IP Relay Server Information	msiexec?.exe (= ntdll.exe)	wimgat.exe	vol32.css
DDoS	wmiconf.dll	ntscfg.dll	perfvwr.dll
Config File	pxdrv.nls	atv04nt5.img	svrms.nls
		wmcfg.exe	
Spam		mstimer.dll	
HDD MBR Destroy		wversion.exe	
File Information Stealing Malware (May ~)			
	netlmgr.dll	ntmpsvc.dll	sysvmd.dll (early: sysenv.dll)
		ssdpupd.dll	regscm.dll (early: rasmcv.dll)
Config File	perfb093.dat	drmkf.inf	maus.dl

Bot Malware Analysis

❖ msiexec?.exe (= ntdll.exe)

- Checks c_10986.nls file
- Drops file and decompresses (inflate)
- Creates Service called “WmiConfig”
- Communicates with C&C IP Relay Server and creates pxdrv.nls file
- Removes the previous version of the services and config files

Bot Malware Analysis

일부 자료 삭제

Bot Malware Analysis

❖ Dropping and inflating file

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0005B760	82	92	35	45	1B	37	6A	81	DB	EF	FF	71	EF	FF	0B	2A
0005B770	B1	34	1F	00	40	01	00	07	00	00	00					

start offset File count

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00014000	77	6D	69	63	6F	6E	Filename				C	6C	00	48	02	48	02	wmiconf.dll.H.H.
00014010	48	02	48	02	48	02	Filename				2	48	02	48	02	7F	91	H.H.H.H.H.H.H.H.I
00014020	00	00	78	9C	EC	BD	7D	7C	14	45	B6	30	DC	33	D3	92	..x? .E?????	

File Size

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
0001D1A0	E6	77	70	63	61	70	Filename				C	00	6C	00	48	02	48	?pcap.dll.1.H.H.
0001D1B0	02	48	02	48	02	48	Filename				3	02	48	02	48	02	84	.H.H.H.H.H.H.H.H.
0001D1C0	A5	01	00	78	9C	EC	3A	6D	74	14	55	96	D5	DD	15	82	?x?:mt.U?R.	

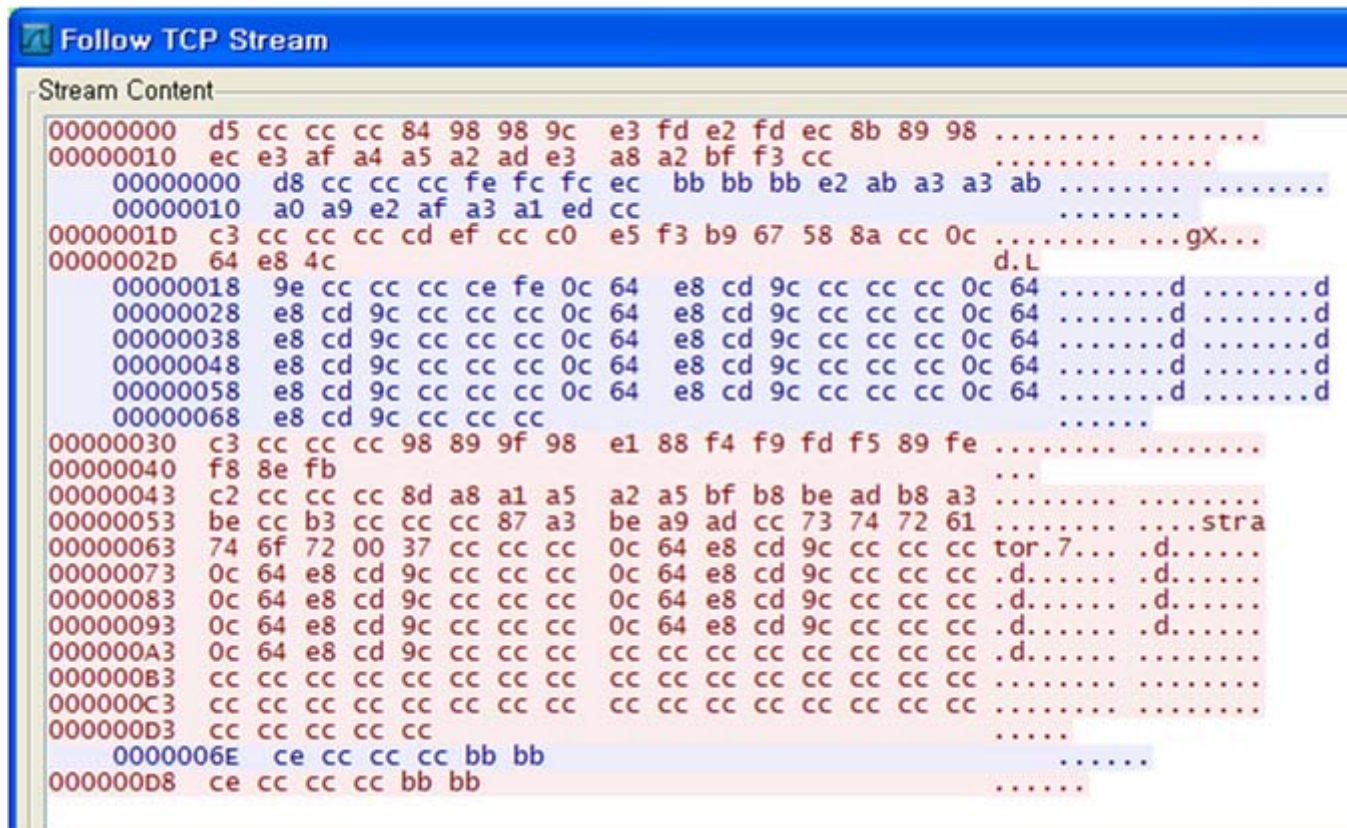
File Size

Bot Malware Analysis

일부 자료 삭제

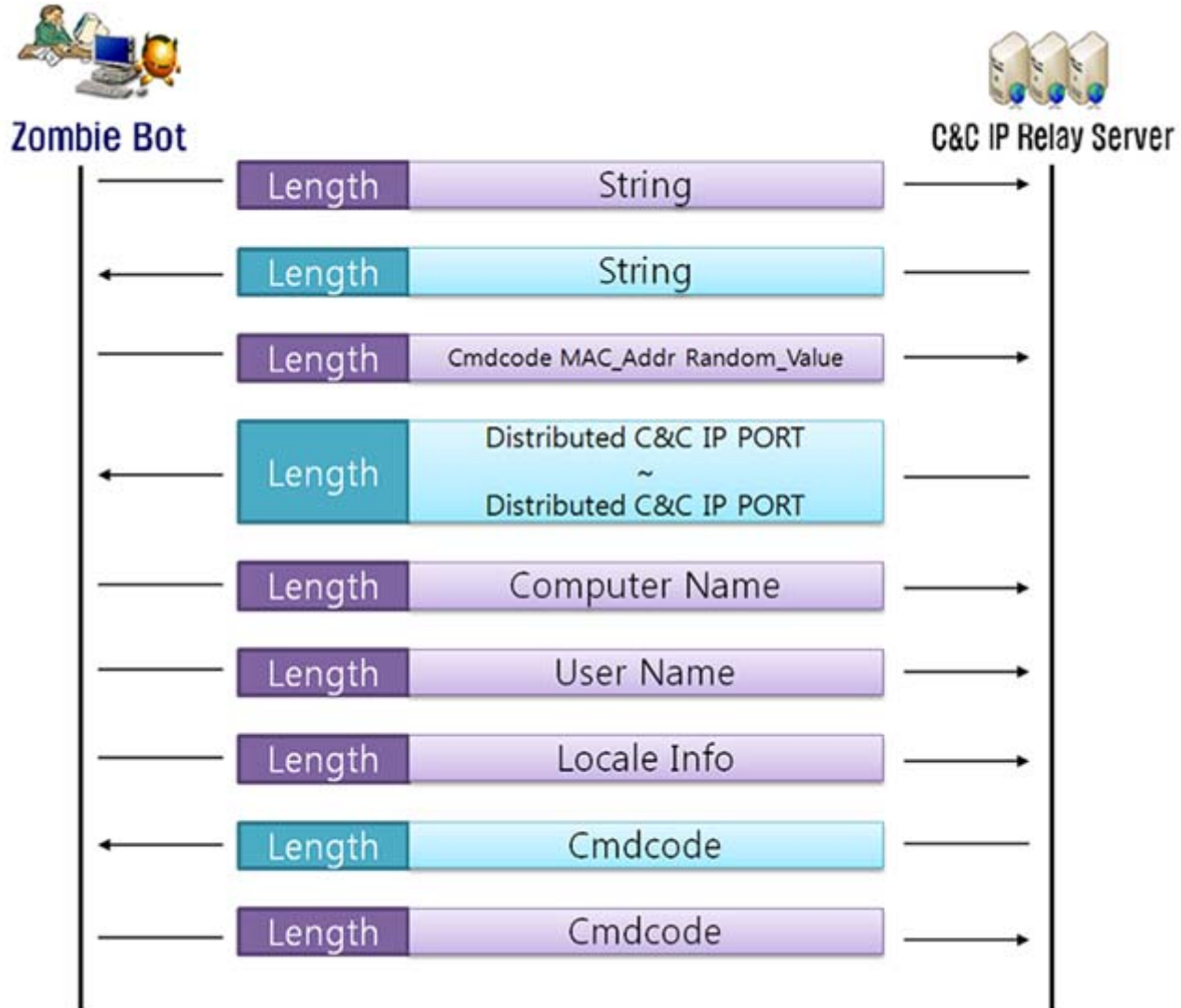
Bot Malware Analysis

❖ Communication Protocol with C&C IP Relay Server

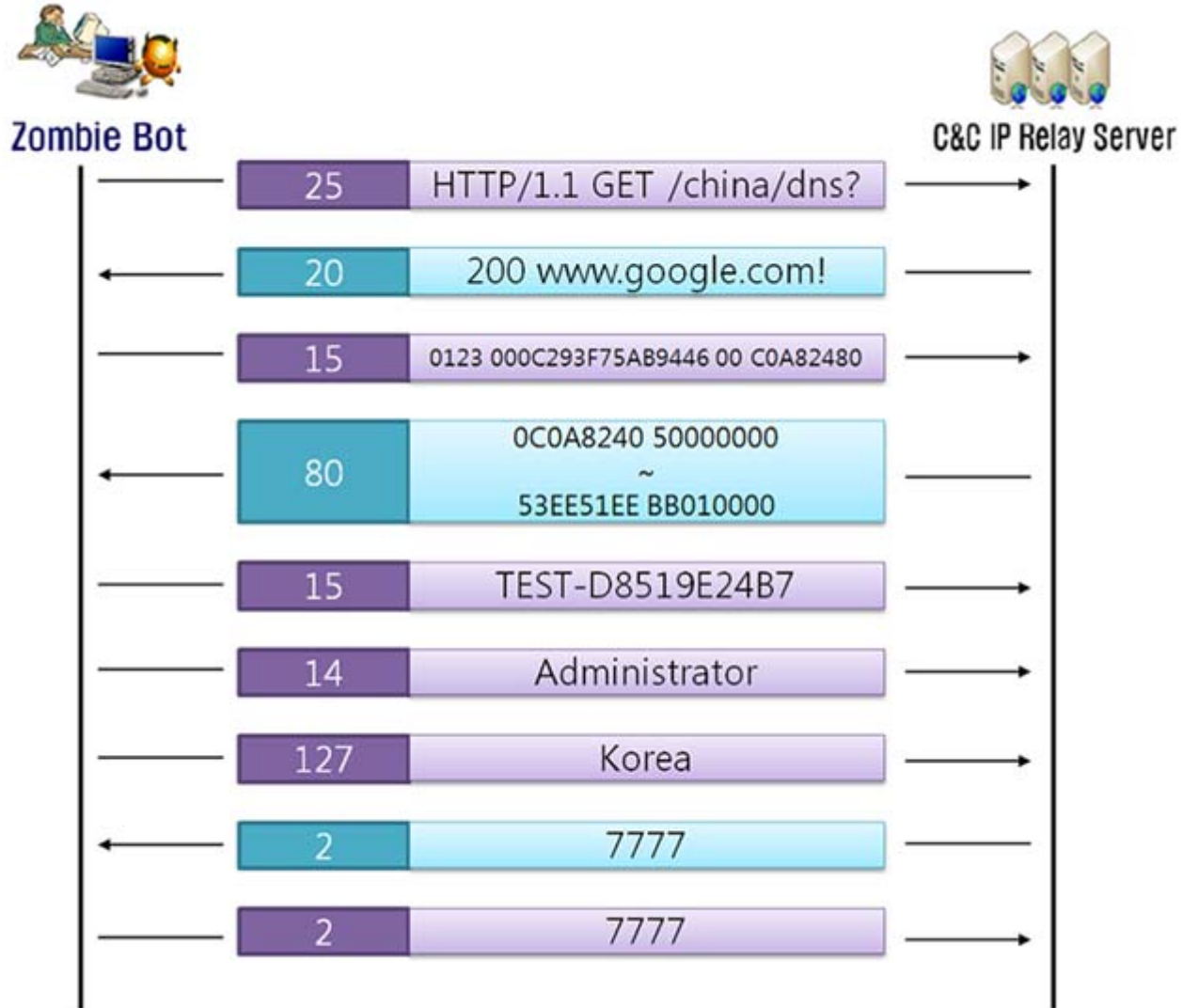


```
Follow TCP Stream
Stream Content
00000000 d5 cc cc cc 84 98 98 9c e3 fd e2 fd ec 8b 89 98 .....
00000010 ec e3 af a4 a5 a2 ad e3 a8 a2 bf f3 cc .....
00000000 d8 cc cc cc fe fc fc ec bb bb bb e2 ab a3 a3 ab .....
00000010 a0 a9 e2 af a3 a1 ed cc .....
0000001D c3 cc cc cc cd ef cc c0 e5 f3 b9 67 58 8a cc 0c .....gX...
0000002D 64 e8 4c .....d.L
00000018 9e cc cc cc ce fe 0c 64 e8 cd 9c cc cc cc 0c 64 .....d .....d
00000028 e8 cd 9c cc cc cc 0c 64 e8 cd 9c cc cc cc 0c 64 .....d .....d
00000038 e8 cd 9c cc cc cc 0c 64 e8 cd 9c cc cc cc 0c 64 .....d .....d
00000048 e8 cd 9c cc cc cc 0c 64 e8 cd 9c cc cc cc 0c 64 .....d .....d
00000058 e8 cd 9c cc cc cc 0c 64 e8 cd 9c cc cc cc 0c 64 .....d .....d
00000068 e8 cd 9c cc cc cc .....
00000030 c3 cc cc cc 98 89 9f 98 e1 88 f4 f9 fd f5 89 fe .....
00000040 f8 8e fb .....
00000043 c2 cc cc cc 8d a8 a1 a5 a2 a5 bf b8 be ad b8 a3 .....
00000053 be cc b3 cc cc cc 87 a3 be a9 ad cc 73 74 72 61 .....stra
00000063 74 6f 72 00 37 cc cc cc 0c 64 e8 cd 9c cc cc cc tor.7... .d.....
00000073 0c 64 e8 cd 9c cc cc cc 0c 64 e8 cd 9c cc cc cc .d..... .d.....
00000083 0c 64 e8 cd 9c cc cc cc 0c 64 e8 cd 9c cc cc cc .d..... .d.....
00000093 0c 64 e8 cd 9c cc cc cc 0c 64 e8 cd 9c cc cc cc .d..... .d.....
000000A3 0c 64 e8 cd 9c cc cc cc cc cc cc cc cc cc cc .d.....
000000B3 cc cc cc cc cc cc cc cc cc cc cc cc cc cc .....
000000C3 cc cc cc cc cc cc cc cc cc cc cc cc cc .....
000000D3 cc cc cc cc cc .....
0000006E ce cc cc cc bb bb .....
000000D8 ce cc cc cc bb bb .....
```

Bot Malware Analysis



Bot Malware Analysis



Bot Malware Analysis

❖ pxdrv.nls file format

Offset	fixed data							mac addr							Random (2Byte)
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
00000000	02	00	00	00	00	00	00	00	0C	29	3F	75	AB	99	5F
00000010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	delete filename (not used)				00	00	00	00	00	00	
00000090	00	00	00	00	delete filename (not used)				00	00	00	00	00	00	
000000A0	00	00	00	00	delete filename (not used)				00	00	00	00	00	00	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	00	00	00	00	00	00	00	00	00	00	80	87	E3	40
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000140	D9	07	07	00	02	00	07	13	00	1C	00	37	00	A9	03
00000150	4E	27	48	03	BB	01	00	42	3F	4C	B4	50	00	00	00
00000160	71	E2	56	AF	00	00	00	00	00	00	00	00	00	00	00
00000170	C3	44	FC	10	C&C server IP 10EA				00	00	00	00	00	00	
00000180	C7	2B	D0	D3	35	00	00	AD	0F	CD	65	50	00	00	00
00000190	CF	B1	6E	47	50	00	00	53	AB	06	0D	35	00	00	00
000001A0	00	0C	29	3F	75	AB	99	5F							

fixed data (2009/7/2 0:0:0)

systemtime

mac addr Random (2Byte)

Bot Malware Analysis

❖ wmiconf.dll

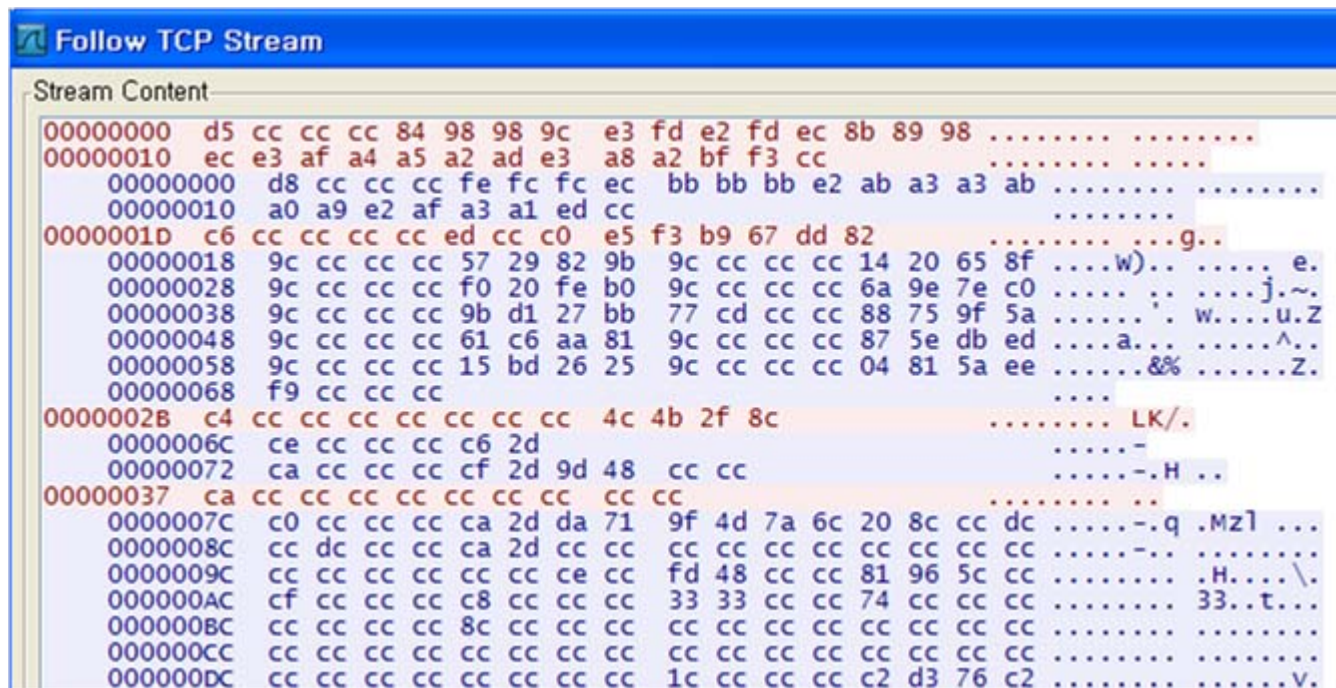
- decodes pxdrv.nls file
- connects Distributed C&C Server and receives 10 Distributed C&C Server IP
- receives the file(~CGF?????.tmp) after sending the time(saved in pxdrv.nls)
- parses the received file and executes
- reads attack targets in uregvs.nls, and starts DDoS attack

Bot Malware Analysis

일부 자료 삭제

Bot Malware Analysis

❖ Communication Protocol with Distributed C&C Server



```
Follow TCP Stream
Stream Content
00000000 d5 cc cc cc 84 98 98 9c e3 fd e2 fd ec 8b 89 98 .....
00000010 ec e3 af a4 a5 a2 ad e3 a8 a2 bf f3 cc .....
00000000 d8 cc cc cc fe fc fc ec bb bb bb e2 ab a3 a3 ab .....
00000010 a0 a9 e2 af a3 a1 ed cc .....
0000001D c6 cc cc cc cc ed cc c0 e5 f3 b9 67 dd 82 .....g..
00000018 9c cc cc cc 57 29 82 9b 9c cc cc cc 14 20 65 8f ....w).. e.
00000028 9c cc cc cc f0 20 fe b0 9c cc cc cc 6a 9e 7e c0 .....j.~.
00000038 9c cc cc cc 9b d1 27 bb 77 cd cc cc 88 75 9f 5a .....w...u.Z
00000048 9c cc cc cc 61 c6 aa 81 9c cc cc cc 87 5e db ed .....a...^..
00000058 9c cc cc cc 15 bd 26 25 9c cc cc cc 04 81 5a ee .....&%...Z.
00000068 f9 cc cc cc .....
0000002B c4 cc cc cc cc cc cc cc 4c 4b 2f 8c .....LK/.
0000006C ce cc cc cc c6 2d .....-
00000072 ca cc cc cc cf 2d 9d 48 cc cc .....-H..
00000037 ca cc cc cc cc cc cc cc cc .....
0000007C c0 cc cc cc ca 2d da 71 9f 4d 7a 6c 20 8c cc dc .....-q .Mz1 ...
0000008C cc dc cc cc ca 2d cc cc cc cc cc cc cc cc .....-..
0000009C cc cc cc cc cc cc ce cc fd 48 cc cc 81 96 5c cc .....H...\.
000000AC cf cc cc cc c8 cc cc cc 33 33 cc cc 74 cc cc cc .....33..t...
000000BC cc cc cc cc 8c cc cc cc cc cc cc cc cc cc .....
000000CC cc cc cc cc cc cc cc cc cc cc cc cc cc .....
000000DC cc cc cc cc cc cc cc cc 1c cc cc cc c2 d3 76 c2 .....V.
```

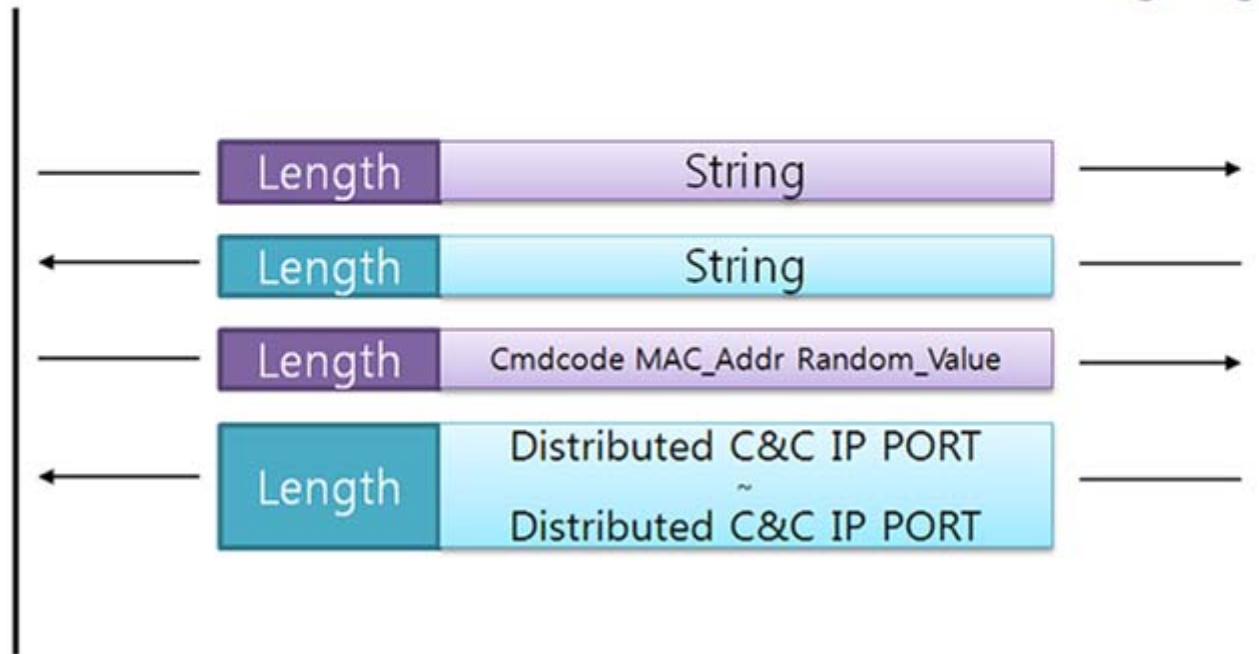
Bot Malware Analysis



Zombie Bot



Distributed C&C Server



Bot Malware Analysis



Zombie Bot



Distributed C&C Server



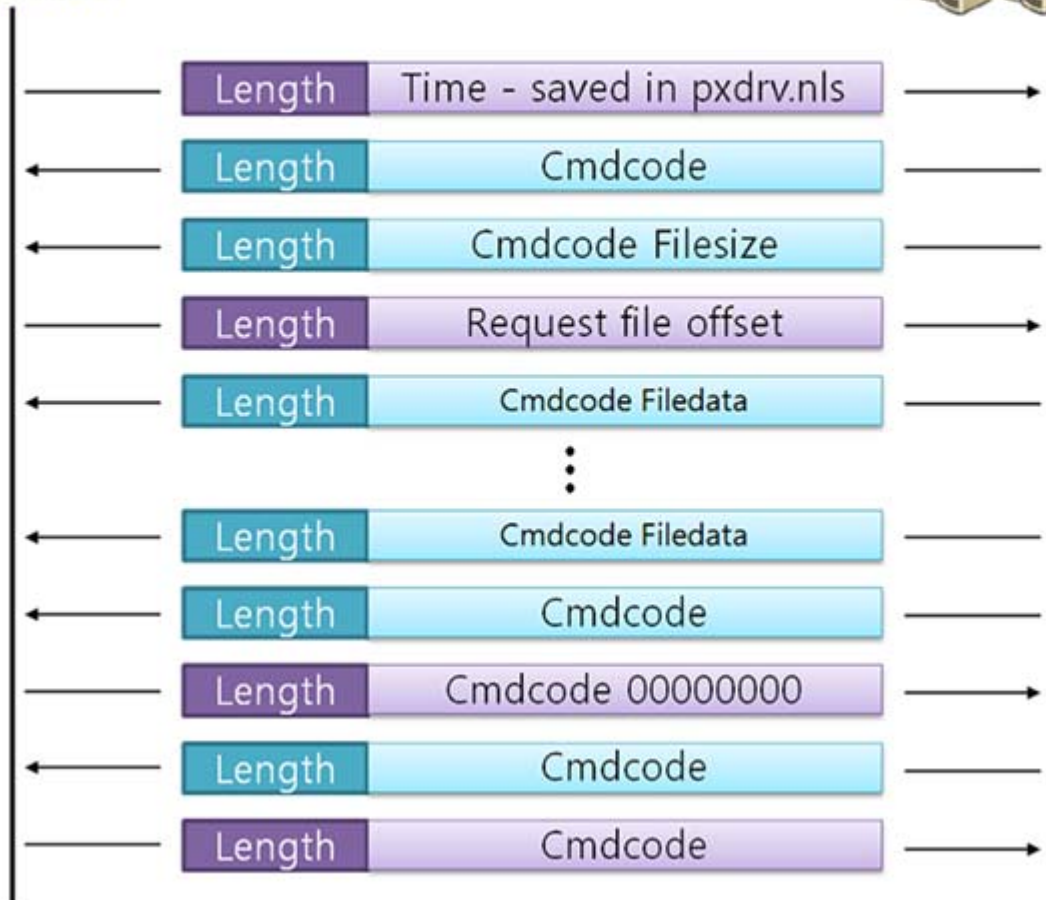
Bot Malware Analysis



Zombie Bot



Distributed C&C Server



Bot Malware Analysis

❖ ~CGF?????.tmp file format

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15		
00000000	16	BD	53	81	A	B6	A0	EC	40	00	B10	00	00	00	C	00	00	00
00000016	00	00	00	00	00	00	D	00	00	00	00	02	E00	31	84	F00	00	00
00000032	4D	5A	90	00	03	00	00	00	00	04	00	00	00	FF	FF	00	00	00
00000048	B8	00	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	00
00000064	00	00	00	00	00	00	00	00	G	00	00	00	00	00	00	00	00	00
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	D0	00	00	00	00

- A : Compare Time
- B : Command Code1
- C : Start Time
- D : End Time
- E : Command Code2
- F : File Size
- G : File Data

Bot Malware Analysis

❖ uregvs.nls file format

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F		
00000000	64	B3	AD	12	A4	18	88	E3	40	1A	00	B0	00	01	C0	77	77	d난.A델@.....ww
00000010	77	2E	70	72	65	73	69	64	65	6E	74	2E	67	6F	2E	6B	w.president.go.k	
00000020	72	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	r.....	
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000110	00	00	00	00	00	00	00	00	00	00	F0	00	50	00	G0	00P...	
00000120	FF	07	H0	00	32	00	I0	00	00	00	00	00	00	00	J0	00	...2.....	
00000130	38	88	E3	40	00	00	00	00	K5	88	E3	40	1E	00	L0	00	8델@....X델@....	
00000140	03	00	M0	00	1E	00	N0	00	50	00	O0	00	1F	00	P0	00P.....	
00000150	C0	67	Q1	40	77	77	77	2E	70	72	65	73	69	64	65	6E	플..www.presiden	
00000160	74	2E	67	6F	2E	6B	72	3B	R3	80	30	3B	67	65	74	3B	t.go.kr;80;get; /	
00000170	3B	3B	00														:::	

Bot Malware Analysis

❖ uregvs.nls file format

- A : Unknown time
- B : Total Target URL Count
- C : URL number
- D : Target URL
- E : Resolved IP address
- F : Total resolved IP address Count
- G : Target Port
- H : Exponent MAX NUM count
- I : Modular value
- J : Time of starting the attack
- K : Time of ending the attack
- L : Related Query Performance Counter value
- M : Sleep term (between target)
- N : Total thread count per Target URL
- O : Related http connection time
- P : R's length
- Q : Allocated memory address of R
- R : Target URL; Port; Attack Type(get, post); Request path;;

Bot Malware Analysis

❖ DDoS Packet Type

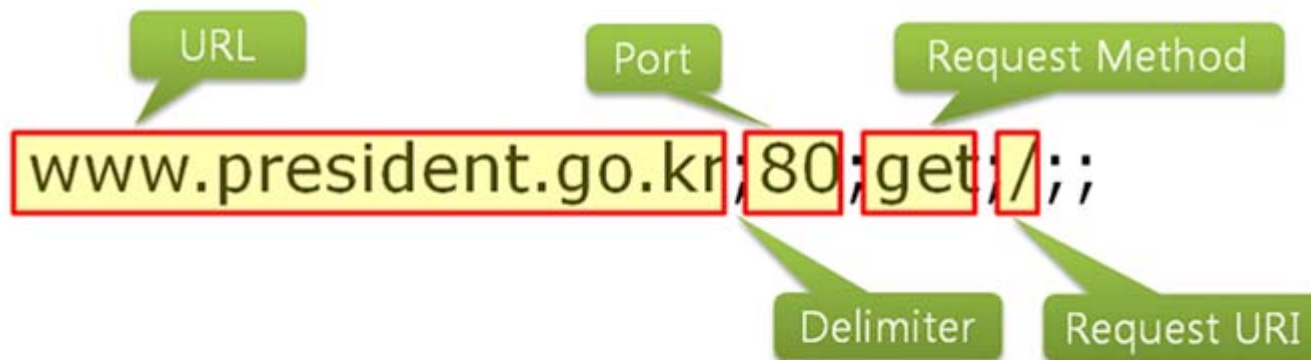
일부 자료 삭제

DDoS Attack Packet Type and Order

circling "packet per thread"

	Source IP	Destination IP	Attack Type	ETC
1	Original	Target	SYN	
2	Spoofing	Target	SYN	
3	Original	Target	ACK	
4	Spoofing	Target	ACK	
5	Original	Target	UDP	
6	Spoofing	Target	UDP	
7	Original	Target	ICMP	
8	Spoofing	Target	ICMP	
9	Target	Broadcast	ICMP	smurfing
10	Original	Target	HTTP GET	User-Agent Random(5)
11	Original	Target	HTTP GET	User-Agent Random(5) Cache-Control

Bot Malware Analysis



User-Agent Type

"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; GTB6; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0;GTB6; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

"Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.20) Gecko/20081217 Firefox/2.0.0.20 (.NET CLR 3.5.30729)"

"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; InfoPath.2; MAXTHON 2.0)"

"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB6; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)"

Bot Malware Analysis

일부 자료 삭제

Bot Malware Analysis

일부 자료 삭제

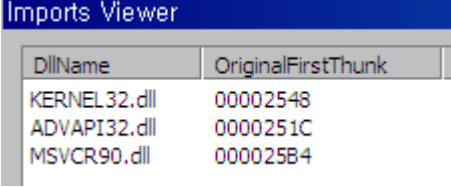
Bot Malware Analysis

No. .	Time	Source	Destination	Protocol	Info
1	0.000000	192.	.128 210.	.195	HTTP Continuation or non-HTTP traffic
2	0.006374	150.	.84 210.	.195	HTTP Continuation or non-HTTP traffic
3	0.042500	192.	.128 210.	.195	HTTP Continuation or non-HTTP traffic
4	0.053372	47.8	3 210.	.195	HTTP Continuation or non-HTTP traffic
5	0.068924	192.	.128 210.	.195	UDP Source port: opswmanager Destination port: http
6	0.084703	90.5	177 210.	.195	UDP Source port: dialpad-voice1 Destination port: http
7	0.100267	192.	.128 210.	.195	ICMP Echo (ping) request
8	0.115871	180.	7.69 210.	.195	ICMP Echo (ping) request
9	0.131643	210.	0.195 192.	255	ICMP Echo (ping) request
10	0.169389	192.	.128 210.	.195	HTTP GET / HTTP/1.1
11	0.204925	192.	.128 210.	.195	HTTP GET / HTTP/1.1

Bot Malware Analysis

❖ wmcfg.exe

- wmcfg.exe is executed only when the msucr90.dll (Microsoft C Runtime Library) file exists.
- drops the following files:
 - %System%\config\SERVICES
 - %System%\config\SERVICES.LOG
 - %System%\mstimer.dll
 - %System%\wversion.exe
- starts the following service:
 - mstimer
- deletes itself



The screenshot shows the 'Imports Viewer' window with a table of imported DLLs. The table has two columns: 'DllName' and 'OriginalFirstThunk'. The imported DLLs are KERNEL32.dll, ADVAPI32.dll, and MSVCR90.dll.

DllName	OriginalFirstThunk
KERNEL32.dll	00002548
ADVAPI32.dll	0000251C
MSVCR90.dll	000025B4

Bot Malware Analysis

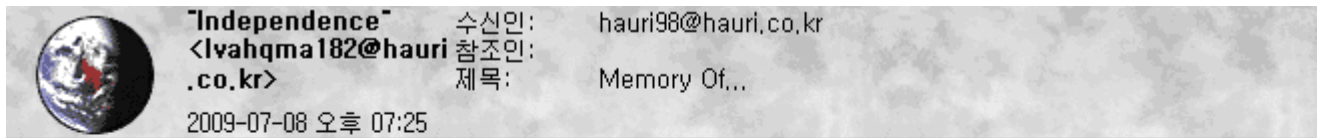
❖ mstimer.dll

- decodes SERVICES.LOG file
- attempts to connect the 8 Distributed Support Servers randomly and requests the flash.gif file.
 - <http://200.6.218.194/flash.gif>
 - <http://92.63.2.118/flash.gif>
 - <http://163.19.209.22/flash.gif>
 - <http://202.14.70.116/flash.gif>
 - <http://75.151.32.182/flash.gif>
 - <http://122.155.5.196/shop/images/flash.gif>
 - <http://201.116.58.131/xampp/img/flash.gif>
 - <http://newrozfm.com/img/glyph/flash.gif>

Bot Malware Analysis

❖ mstimer.dll

- sends the binary at the front part of flash.gif through spam mails to other users.
- However, because the binary is damaged file, the users who received the spam mails don't suffer from any damages substantially.



Bot Malware Analysis

❖ flash.gif file format

Offset	identifier								size										
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F			
00000000	4A	50	47	00	00	00	00	00	34	00	00	00	01	00	00	00	JPG	4	
00000010	0C	00	00	00	28	00	00	00	58	E7	04	21	F8	F2	D1	B0	(X?!剽璣	
00000020	9E	96	00	2C	BC	SERVICES.LOG						A5	D7	20	DF	9D	옴 ,셤긔?濕??		
00000030	A8	3B	19	73	29	AC	70	26	B9	EE	7A	64	9A	1C	82	B7	? s)궑&뵓zd?궑		
00000040	01	00	00	00	80	00	00	00	80	00	00	00	60	00	00	00	,		
00000050	56	2E	E4	D7	59	3E	C6	53	F6	5E	B4	3B	CB	AF	A7	7F	V.궑Y>???궑?		
00000060	FE	C3	B3	DD	EF	40	FF	C9	87	6A	4B	9C	07	C2	9E	C4	넛? ?jK?궑		
00000070	AC	BD	86	D1	33	77	SERVICES						EA	3C	E8	B7	BE	F5	뵓뵓3w7?긔<궑궑
00000080	A2	B4	AE	64	99	80	SERVICES						08	0A	4B	B7	65	41	*궑궑?궑V5 K궑궑A
00000090	04	EC	85	DB	C8	70	AC	8B	50	52	2C	AC	78	43	3B	81	?拜p궑궑PR,궑궑C;		
000000A0	C8	55	BE	AC	9E	F6	7E	10	77	91	7B	77	77	85	attachment file of spam		?궑궑은~M?r?궑궑		
000000B0	14	00	00	00	52	61	72	21	1A	07	00	CF	90	73	00	00	Rar! ?s		
000000C0	0D	00	00	00	00	00	00	00	02	00	00	00	00	A0	00	00	?		
000000D0	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ?		
000000E0	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	? @		
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00000100	00	00	00	00	00	00	00	00	00	00	00	00	F0	00	00	00	?		
00000110	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	? ???L?Th		
00000120	69	73	20	70	72	6F	~AX?.tmp						20	63	61	6E	6E	6F	is program canno
00000130	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS		
00000140	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode. \$		
00000150	69	8A	E3	B6	2D	EB	8D	E5	2D	EB	8D	E5	2D	EB	8D	E5	i궑궑??????		
00000160	56	F7	81	E5	2C	EB	8D	E5	C5	F4	87	E5	26	EB	8D	E5	V???궑궑???		

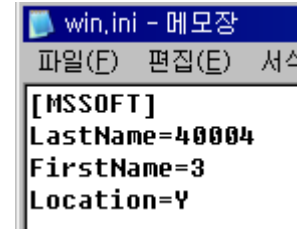
Bot Malware Analysis

❖ ~AX?.tmp

- executed by mstimer.dll
- drops the following file:
 - wversion.exe (HDD MBR Destroyer)
- records the time of execution for wversion.exe in win.ini

- deletes itself

```
call    GetLocalTime
lea     ecx, [esp+140h+pvtime]
lea     edx, [esp+140h+SystemTime]
push   ecx           ; pvtime
push   edx           ; lpSystemTime
mov     [esp+148h+SystemTime.wDay], 10
call    SystemTimeToVariantTime
fld     [esp+140h+pvtime]
lea     eax, [esp+140h+String]
push   0Ah          ; Radix
push   eax           ; DstBuf
call   _ftol
push   eax           ; Val
call   _itoa
```



Bot Malware Analysis

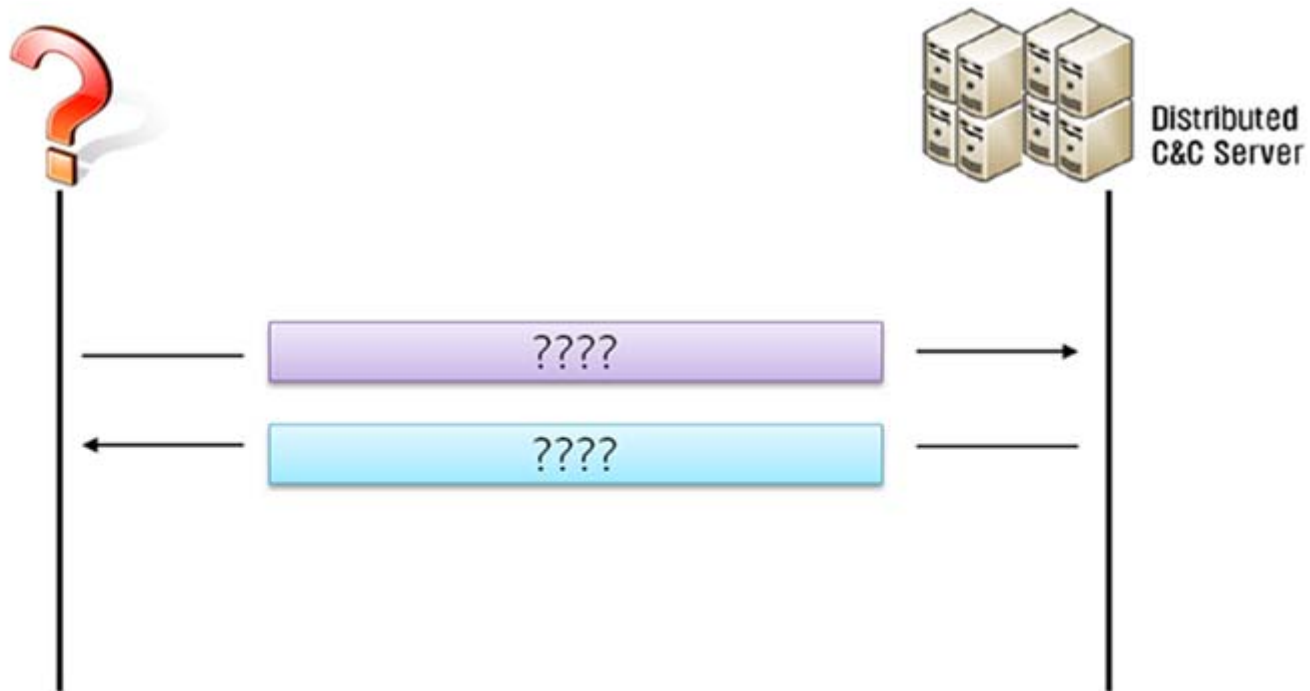
❖ wversion.exe (HDD MBR Destroyer)

- executed by mstimer.dll after midnight on July 10.
- initializes the HDD MBR by 0x55 and inserts the string, "Memory of the Independence Day"
- In addition, in the case of the following extension, it makes the file unavailable by setting a random password and compressing into gz.
 - (zip, pas, c, cpp, java, jsp, aspx, asp, php, rar, gho, alz, xml, pst, eml, kwp, gul, hna, hwp, txt, rtf, dbf, db, accdb, pdf, pptx, ppt, mdb, xlsx, xls, wri, wpx, wpd, docm, docx, doc)
- deletes itself

Bot Malware Analysis

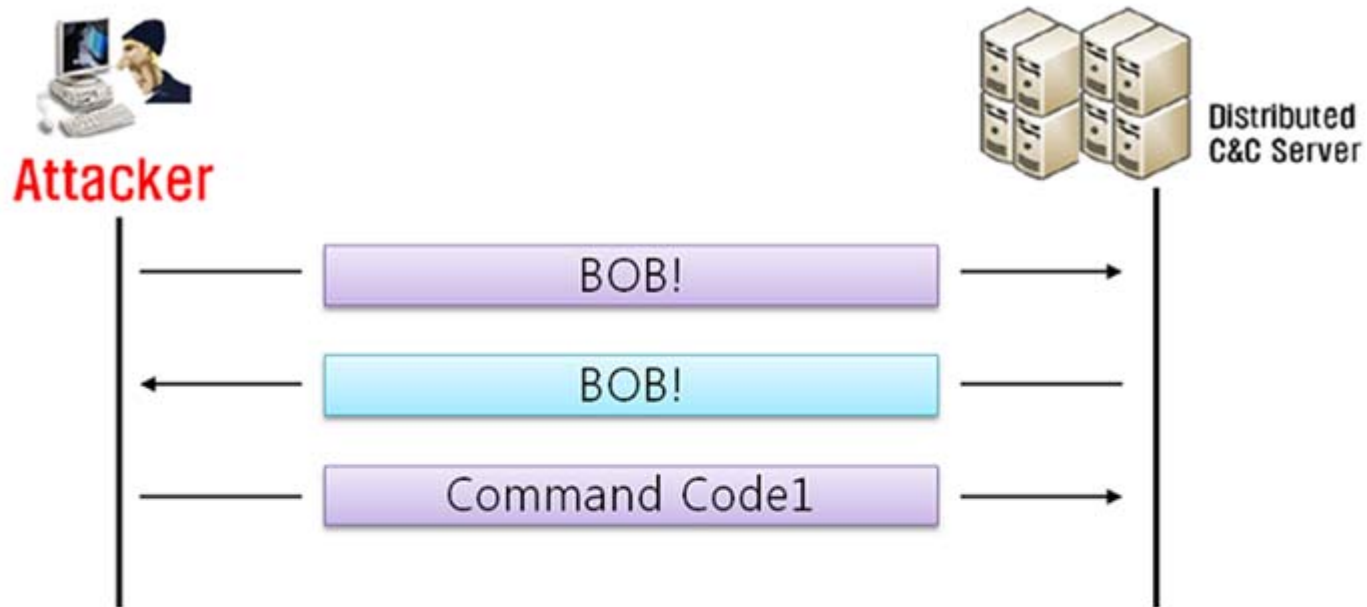
Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	4D	65	6D	6F	72	79	20	6F	66	20	74	68	65	20	49	6E	Memory of the In
00000010	64	65	70	65	6E	64	65	6E	63	65	20	44	61	79	00	00	dependence Day..
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000060	00	00	00	00	55	55	55	55	55	55	55	55	55	55	55	55	...UUUUUUUUUUUU
00000070	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000080	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000090	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
000000A0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
000000B0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
000000C0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
000000D0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
000000E0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
000000F0	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000100	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000110	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000120	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000130	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000140	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000150	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU
00000160	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	55	UUUUUUUUUUUUUU

Botnet Counter-Attack



Command Code	Meaning	Subject
SOS!	Zombie mode	Zombie
BOB!	Administration mode	Bot Master

Botnet Counter-Attack



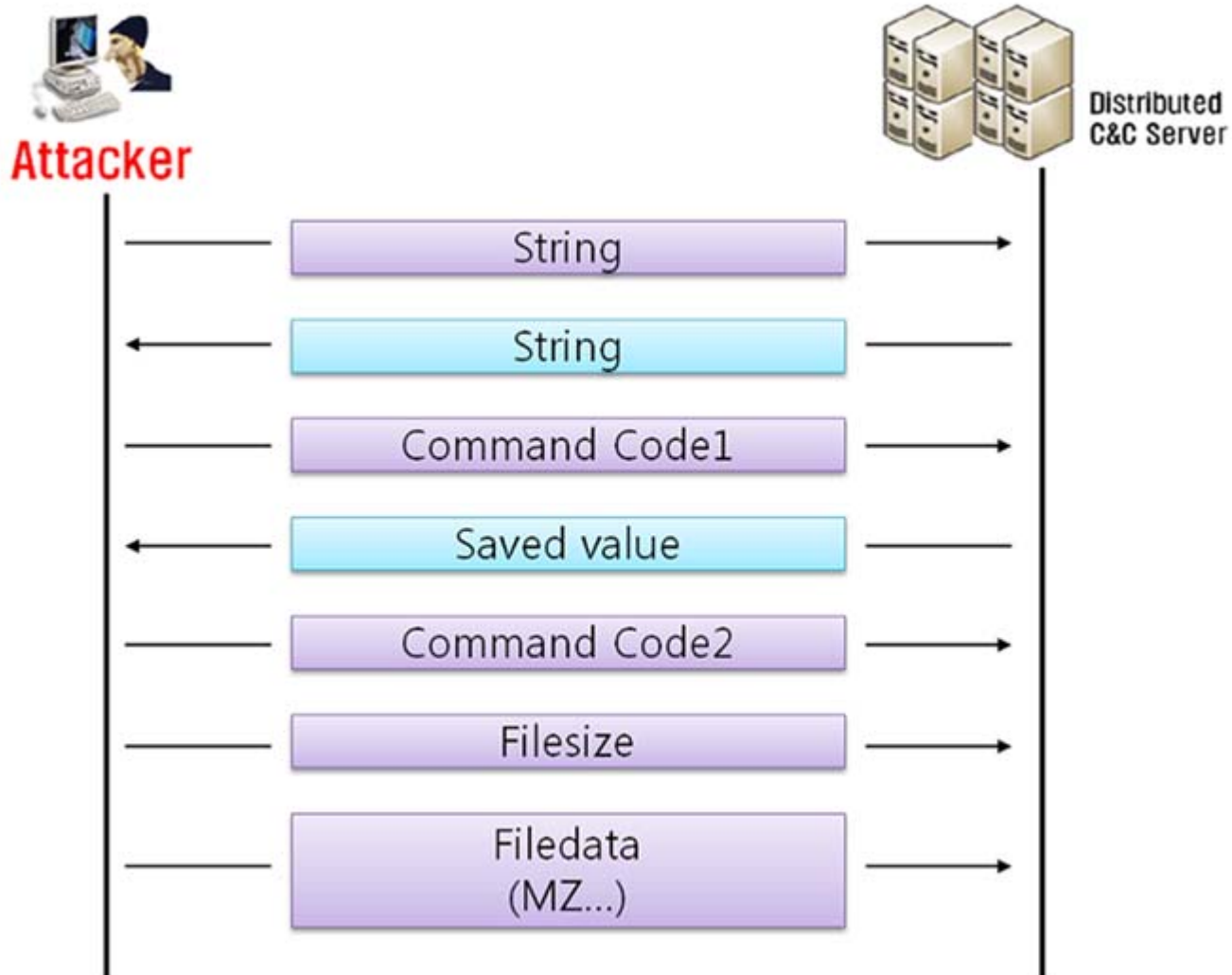
Command Code1	Meaning
0x2050	Sub command
0x2051	Send wmipmf.dll
0x2053	Send DictC Directory Files
0x2054	Send saved value

Botnet Counter-Attack

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000016	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000032	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000048	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000064	3C	00	00	00	14	20	00	00	6A	61	76	61	64	63	6F	6D	<... ..javadcom
00000080	2E	65	78	65	00	00	00	00	00	00	00	00	00	00	00	00	.exe.....
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000144	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000304	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000320	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

Command Code2	Meaning
0x2013	Modify value in maxodb.inf
0x2014	receive and execute file
0x2015	download file from url, execute it
0x2018	Re-Collection Server IP change
0x2019	C&C Master Server IP change

Botnet Counter-Attack



❖ It's Showtime!

❖ Questions?

- contact us via e-mail
 - sionics 0x40 issuemakerslab.com
 - kaientt 0x40 issuemakerslab.com

Thank You !



www.issuemakerslab.com