Embedded devices, an AntiVirus-free safe hideout for Malware

MALWARE MIGRATING TO GAMING CONSOLES

Ahn Ki-Chan - Hanyang University, Undergraduate
Ha Dong-Joo - AhnLab Inc., Security Researcher

AhnLab

About

Introduction

- Embedded systems(gaming consoles, smartphones, etc.) have enough hardware for malware to survive and perform it's job

- There are not so many publicly disclosed issues of malware on these devices which make people think that they are safe

- The possibilities of malware on embedded systems and the resulting effects will be shown in this presentation with some real world examples, along with some possible defenses

Index

Background Knowledge

- The pirate scene of Gamine consoles and Smartphones
- The current state of malware on embedded devices
- The mindset of the general public

The attacker's point of view

- Gaming consoles as an attacking tool - Hacking with NDS
- Malware on Console Gaming systems - Malware on Wii
- Malware injection on Smartphone applications - Malware on Smartphones

Preparation - Our defenses

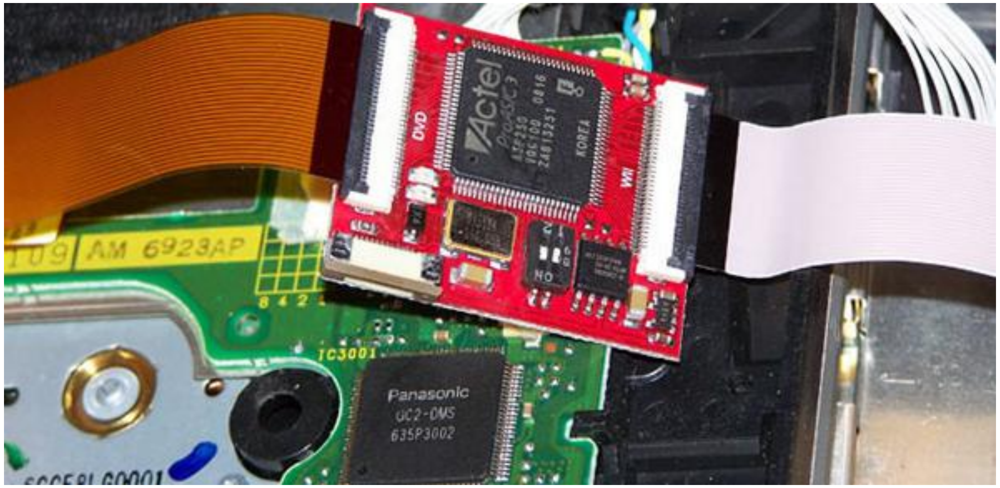
- Manufacturers : Steps to take when designing a new device
- Service, Security companies : Measurements in Software or Policies
- Users : Precautions for the general users

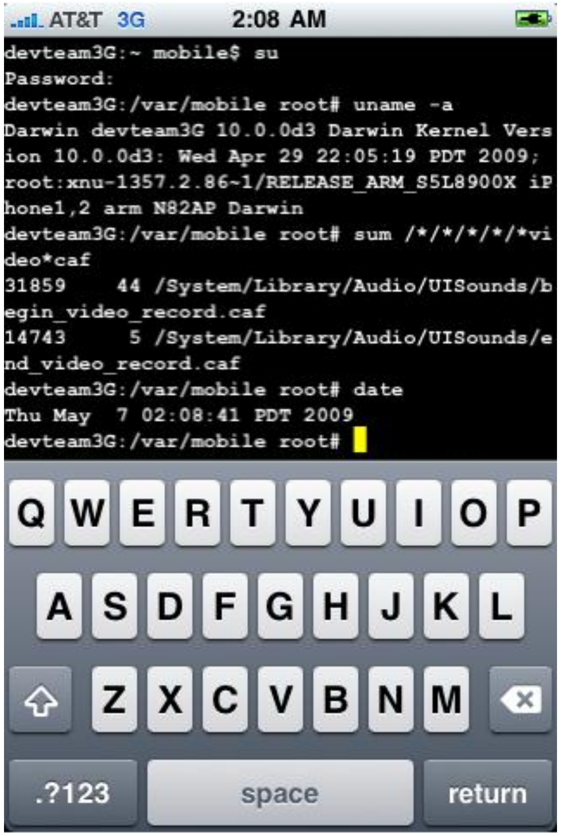
Background Knowledge

The pirate scene of Gamine consoles and Smartphones

Payed software being illegally downloaded

- Most embedded devices implement anti pirate Measures by some means, but these protections are eventually bypassed

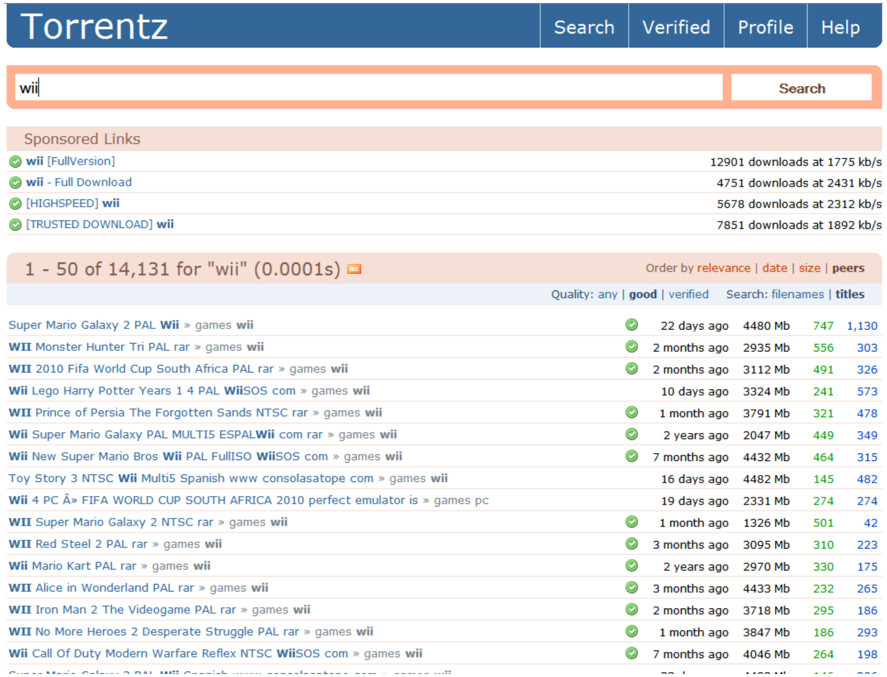




```
devteam3G:~ mobile$ su
Password:
devteam3G:/var/mobile root# uname -a
Darwin devteam3G 10.0.0d3 Darwin Kernel Vers
ion 10.0.0d3: Wed Apr 29 22:05:19 PDT 2009;
root:xnu-1357.2.86~1/RELEASE_ARM_S5L8900X iP
hone1,2 arm N82AP Darwin
devteam3G:/var/mobile root# sum /*/*/*/*/*vi
deo*caf
31859    44 /System/Library/Audio/UISounds/b
egin_video_record.caf
14743     5 /System/Library/Audio/UISounds/e
nd_video_record.caf
devteam3G:/var/mobile root# date
Thu May  7 02:08:41 PDT 2009
devteam3G:/var/mobile root#
```

The distribution of illegal software

- Just like PC software, illegal software is Being distributed without any restrictions via P2P, torrents, web storage
- Easily accessible by the general public



Torrentz | Search | Verified | Profile | Help

wii | Search

Sponsored Links

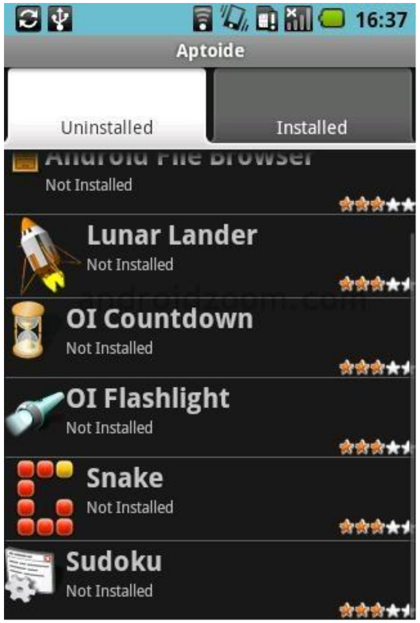
✓ **wii** [FullVersion]	12901 downloads at 1775 kb/s
✓ **wii** - Full Download	4751 downloads at 2431 kb/s
✓ [HIGHSPEED] **wii**	5678 downloads at 2312 kb/s
✓ [TRUSTED DOWNLOAD] **wii**	7851 downloads at 1892 kb/s

1 - 50 of 14,131 for "wii" (0.0001s)

Order by relevance | date | size | **peers**

Quality: any | **good** | verified Search: filenames | **titles**

Super Mario Galaxy 2 PAL **Wii** » games **wii**	✓	22 days ago	4480 Mb	747	1,130
WII Monster Hunter Tri PAL rar » games **wii**	✓	2 months ago	2935 Mb	556	303
WII 2010 Fifa World Cup South Africa PAL rar » games **wii**	✓	2 months ago	3112 Mb	491	326
Wii Lego Harry Potter Years 1 4 PAL **Wii**SOS com » games **wii**		10 days ago	3324 Mb	241	573
WII Prince of Persia The Forgotten Sands NTSC rar » games **wii**	✓	1 month ago	3791 Mb	321	478
Wii Super Mario Galaxy PAL MULTI5 ESPAL**Wii** com rar » games **wii**	✓	2 years ago	2047 Mb	449	349
Wii New Super Mario Bros **Wii** PAL FullISO **Wii**SOS com » games **wii**	✓	7 months ago	4432 Mb	464	315
Toy Story 3 NTSC **Wii** Multi5 Spanish www consolasatope com » games **wii**		16 days ago	4482 Mb	145	482
Wii 4 PC Â» FIFA WORLD CUP SOUTH AFRICA 2010 perfect emulator is » games pc		19 days ago	2331 Mb	274	274
WII Super Mario Galaxy 2 NTSC rar » games **wii**	✓	1 month ago	1326 Mb	501	42
WII Red Steel 2 PAL rar » games **wii**	✓	3 months ago	3095 Mb	310	223
Wii Mario Kart PAL rar » games **wii**	✓	2 years ago	2970 Mb	330	175
WII Alice in Wonderland PAL rar » games **wii**	✓	3 months ago	4433 Mb	232	265
WII Iron Man 2 The Videogame PAL rar » games **wii**	✓	2 months ago	3718 Mb	295	186
WII No More Heroes 2 Desperate Struggle PAL rar » games **wii**	✓	1 month ago	3847 Mb	186	293
Wii Call Of Duty Modern Warfare Reflex NTSC **Wii**SOS com » games **wii**	✓	7 months ago	4046 Mb	264	198
Super Mario Galaxy 2 PAL **Wii** Spanish www consolasatope com » games wii					



Android File Browser
Not Installed

Lunar Lander
Not Installed

OI Countdown
Not Installed

OI Flashlight
Not Installed

Snake
Not Installed

Sudoku
Not Installed

The current state of malware on embedded devices

Malware on Gaming Consoles

- Disguises itself as a useful homebrew application, and lures users to install it

- Disguises itself as an essential bypassing tool or crack, and upon installation, eventually causing havoc or wrecking the device

Malware on Smartphones

- Worm that targets jailbroken iphones using a default password
- Traditional malware techniques incorporated in Windows Mobile and Blackberry
- Social Engineering worm that collects phone information on Symbian Smartphones
- Trojaned Windows Mobile Games
- Toaster Rootkit
- Android Rootkit

The mindset of the general public

User’s thoughts of malware on embedded devices

- Users not being suspicious just by the fact that that they're using ‘normal’ apps that don’t look 'fishy'

- Most people do not even give a second thought before installing downloaded software, and merely just check that the application works

However...

- These devices are capable of bringing similar negative effects of PC malware, and the boundary of these devices and the PC is getting very thin due to the evolution of hardware

- Most recent Gaming Consoles contain hardware to connect to the network, so an almost ideal environment if provided for malware to survive and perform it's task.

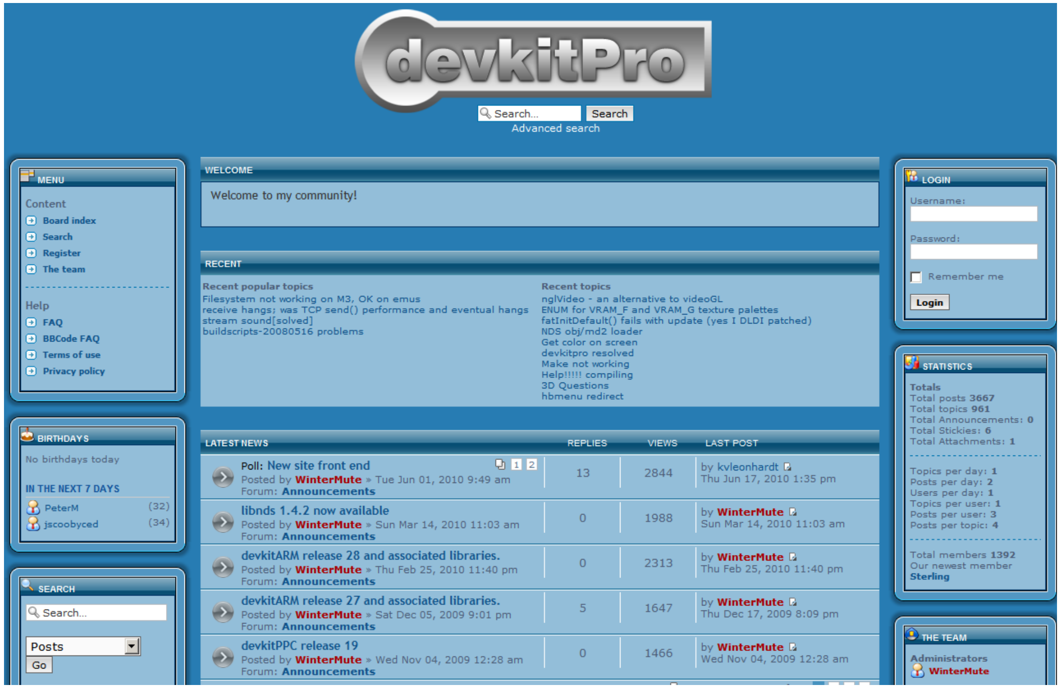
The mindset of an attacker

Gaming Consoles as an attacking Tool

The hardware and software development environment

- Most embedded devices contain a high quality CPU, I/O devices, and network devices

- SDKs not officially provided by the manufacturer, but users can create legit software that runs on the device(via homebrew) with a custom development environment



WELCOME

Welcome to my community!

RECENT

Recent popular topics
Filesystem not working on M3, OK on emus
receive hangs; was TCP send() performance and eventual hangs
stream sound[solved]
buildscripts-20080516 problems

Recent topics
nglVideo - an alternative to videoGL
ENUM for VRAM_F and VRAM_G texture palettes
fatInitDefault() fails with update (yes I DLDI patched)
NDS obj/md2 loader
Get color on screen
devkitpro resolved
Make not working
Help!!!!! compiling
3D Questions
hbmenu redirect

No birthdays today

IN THE NEXT 7 DAYS
PeterM (32)
jscoobyced (34)

LATEST NEWS	REPLIES	VIEWS	LAST POST
Poll: New site front end 1 2 Posted by **WinterMute** » Tue Jun 01, 2010 9:49 am Forum: **Announcements**	13	2844	by kvleonhardt Thu Jun 17, 2010 1:35 pm
libnds 1.4.2 now available Posted by **WinterMute** » Sun Mar 14, 2010 11:03 am Forum: **Announcements**	0	1988	by **WinterMute** Sun Mar 14, 2010 11:03 am
devkitARM release 28 and associated libraries. Posted by **WinterMute** » Thu Feb 25, 2010 11:40 pm Forum: **Announcements**	0	2313	by **WinterMute** Thu Feb 25, 2010 11:40 pm
devkitARM release 27 and associated libraries. Posted by **WinterMute** » Sat Dec 05, 2009 9:01 pm Forum: **Announcements**	5	1647	by **WinterMute** Thu Dec 17, 2009 8:09 pm
devkitPPC release 19 Posted by **WinterMute** » Wed Nov 04, 2009 12:28 am Forum: **Announcements**	0	1466	by **WinterMute** Wed Nov 04, 2009 12:28 am

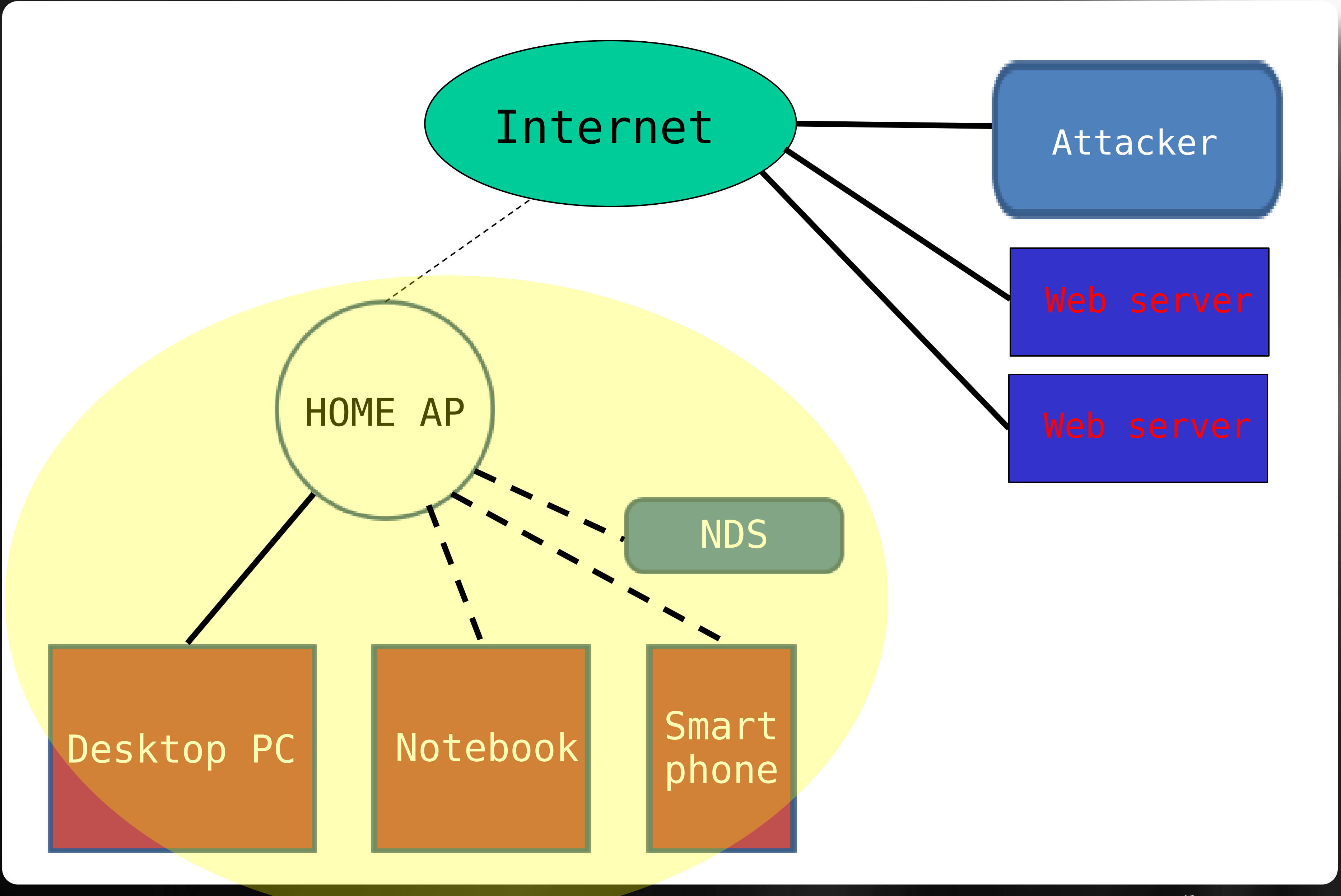
Totals
Total posts **3667**
Total topics **961**
Total Announcements: **0**
Total Stickies: **6**
Total Attachments: **1**

Topics per day: **1**
Posts per day: **2**
Users per day: **1**
Topics per user: **1**
Posts per user: **3**
Posts per topic: **4**

Total members **1392**
Our newest member
Sterling

Administrators
WinterMute

Hacking with NDS



The attacker's point of view - Gaming console acting like a computer

Hacking with NDS

- Attacking and taking control of a PC

- Demo : Using NDS to attack a PC on the network with a public remote exploit

Hacking with NDS

- Attacking the network

- Demo : Using NDS to bring down a network

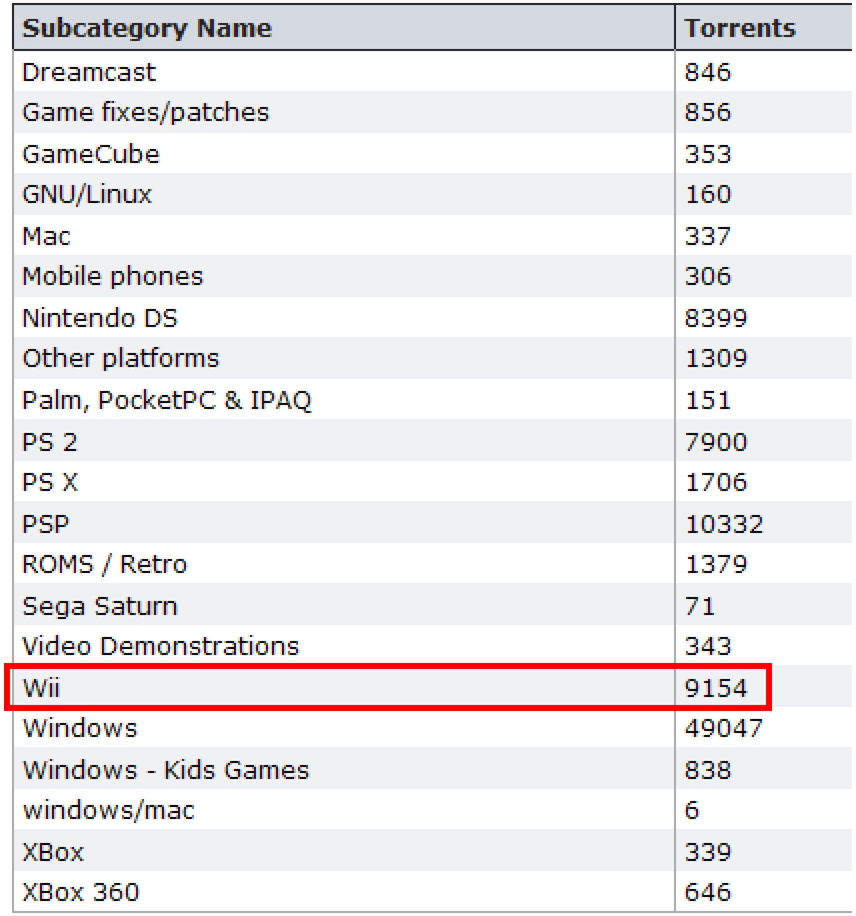
Hacking with NDS

- Injecting malicious code in network packets

- Demo : Using NDS to inject malicious code by
  modifying packets

Malware on Console Gaming systems

Piracy in the gaming industry



Subcategory Name	Torrents
Dreamcast	846
Game fixes/patches	856
GameCube	353
GNU/Linux	160
Mac	337
Mobile phones	306
Nintendo DS	8399
Other platforms	1309
Palm, PocketPC & IPAQ	151
PS 2	7900
PS X	1706
PSP	10332
ROMS / Retro	1379
Sega Saturn	71
Video Demonstrations	343
Wii	9154
Windows	49047
Windows - Kids Games	838
windows/mac	6
XBox	339
XBox 360	646

2nd place among the current gaming console systems, closely following PSP

The inner workings of games running on Wii

- executables files are files with .dol extension

- they are essentially a stripped down version of an elf file

- system menu -> apploader -> .dol

- .dol files(and sometimes .rel files) contain all code needed for the game to run

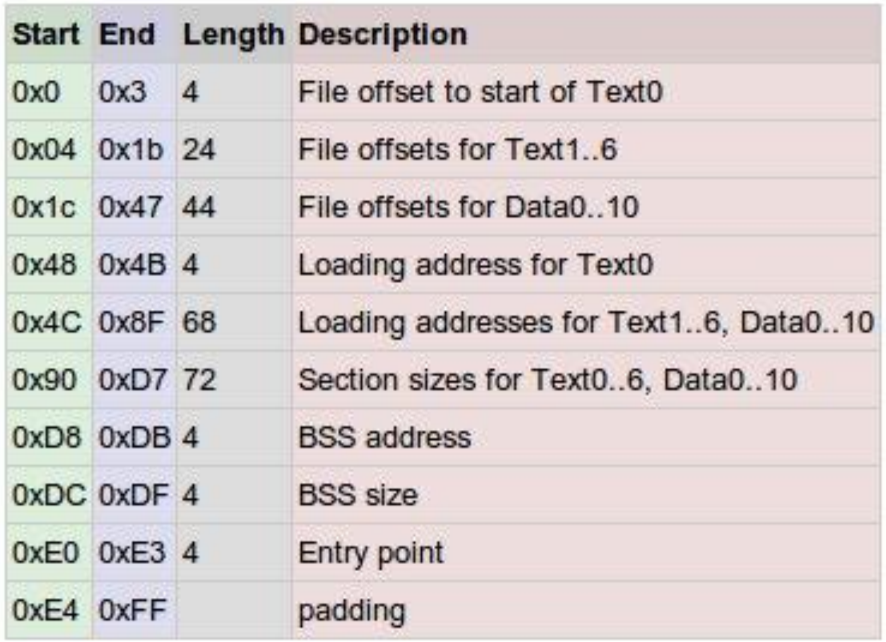
How custom code can be injected

- Merge 2 dol files

- Update header information

- Inject code that transfers execution to the game .dol after the execution of the injected .dol

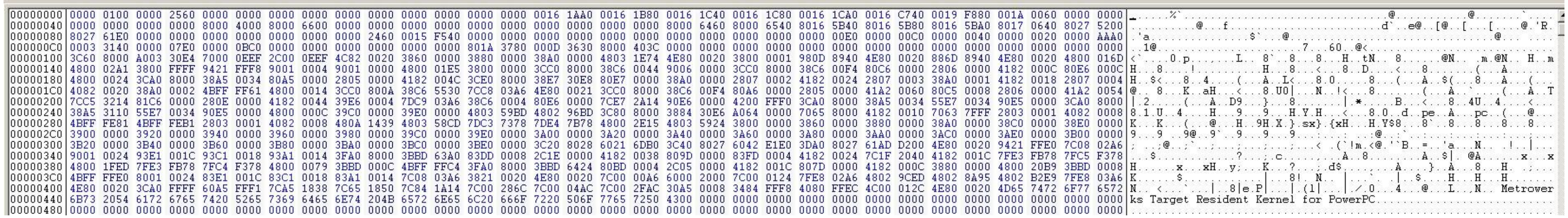
- Fix a few problematic parts in the binary



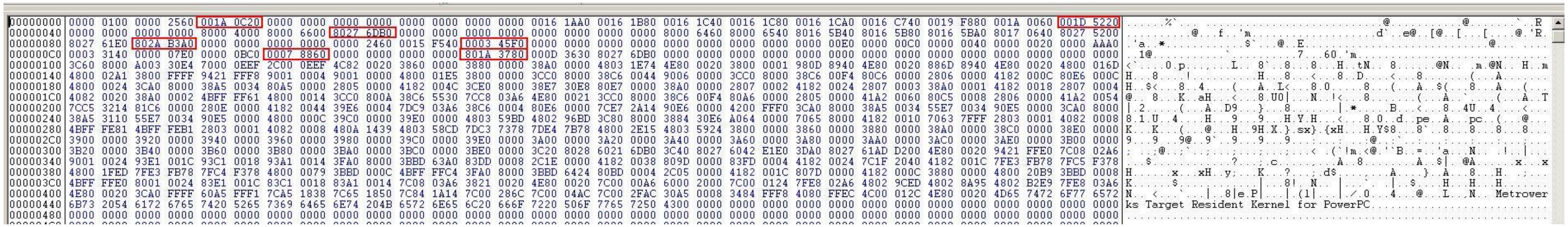
Start	End	Length	Description
0x0	0x3	4	File offset to start of Text0
0x04	0x1b	24	File offsets for Text1..6
0x1c	0x47	44	File offsets for Data0..10
0x48	0x4B	4	Loading address for Text0
0x4C	0x8F	68	Loading addresses for Text1..6, Data0..10
0x90	0xD7	72	Section sizes for Text0..6, Data0..10
0xD8	0xDB	4	BSS address
0xDC	0xDF	4	BSS size
0xE0	0xE3	4	Entry point
0xE4	0xFF		padding

How custom code can be injected

- Demo : POC of malware injection on Nintendo Wii games

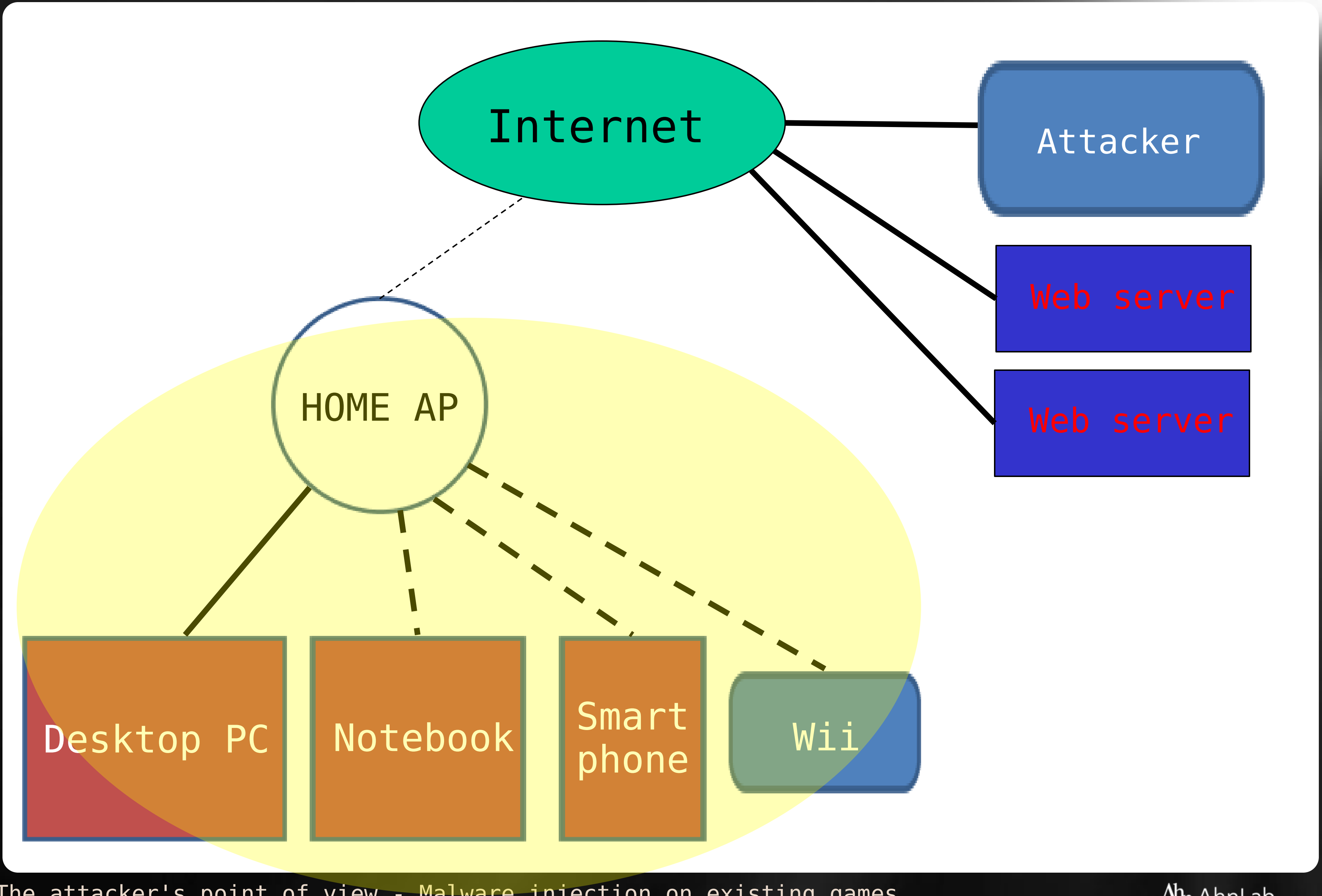


```
00000000 0000 0100 0000 2560 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0016 1AA0 0016 1B80 0016 1C40 0016 1C80 0016 1CA0 0016 C740 0019 F880 001A 0060 0000 0000 ......%`.......................................@...........@.......`....
00000040 0000 0000 0000 0000 8000 4000 8000 6600 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 8000 6460 8000 6540 8016 5B40 8016 5B80 8016 5BA0 8017 0640 8027 5200 ..........@...f...........................d`..e@..[@..[...[....@.'R.
00000080 8027 61E0 0000 0000 0000 0000 0000 0000 0000 2460 0015 F540 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 00E0 0000 00C0 0000 0040 0000 0020 0000 AAA0 .'a...............$`...@...............................@... ....
000000C0 0003 3140 0000 07E0 0000 0BC0 0000 0000 0000 0000 0000 0000 801A 3780 000D 3630 8000 403C 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ..1@....................7...60..@<..............................
00000100 3C60 8000 A003 30E4 7000 0EEF 2C00 0EEF 4C82 0020 3860 0000 3880 0000 38A0 0000 4803 1E74 4E80 0020 3800 0001 980D 8940 4E80 0020 886D 8940 4E80 0020 4800 016D <`....0.p...,...L.. 8`..8...8...H..tN.. 8......@N.. .m.@N.. H..m
00000140 4800 02A1 3800 FFFF 9421 FFF8 9001 0004 9001 0000 4800 01E5 3800 0000 3CC0 8000 38C6 0044 9006 0000 3CC0 8000 38C6 00F4 80C6 0000 2806 0000 4182 000C 80E6 000C H...8....!..........H...8...<...8..D....<...8.......(...A.......
00000180 4800 0024 3CA0 8000 38A5 0034 80A5 0000 2805 0000 4182 004C 3CE0 8000 38E7 30E8 80E7 0000 38A0 0000 2807 0002 4182 0024 2807 0003 38A0 0001 4182 0018 2807 0004 H..$<...8..4....(...A..L<...8.0.....8...(...A..$(...8...A...(...
000001C0 4082 0020 38A0 0002 4BFF FF61 4800 0014 3CC0 800A 38C6 5530 7CC8 03A6 4E80 0021 3CC0 8000 38C6 00F4 80A6 0000 2805 0000 41A2 0060 80C5 0008 2806 0000 41A2 0054 @.. 8...K..aH...<...8.U0|...N..!<...8.......(...A..`....(...A..T
00000200 7CC5 3214 81C6 0000 280E 0000 4182 0044 39E6 0004 7DC9 03A6 38C6 0004 80E6 0000 7CE7 2A14 90E6 0000 4200 FFF0 3CA0 8000 38A5 0034 55E7 0034 90E5 0000 3CA0 8000 |.2.....(...A..D9...}...8.......|.*.....B...<...8..4U..4....<...
00000240 38A5 3110 55E7 0034 90E5 0000 4800 000C 39C0 0000 39E0 0000 4803 59BD 4802 96BD 3C80 8000 3884 30E6 A064 0000 7065 8000 4182 0010 7063 7FFF 2803 0001 4082 0008 8.1.U..4....H...9...9...H.Y.H...<...8.0..d..pe..A...pc..(...@...
00000280 4BFF FE81 4BFF FEB1 2803 0001 4082 0008 480A 1439 4803 58CD 7DC3 7378 7DE4 7B78 4800 2E15 4803 5924 3800 0000 3860 0000 3880 0000 38A0 0000 38C0 0000 38E0 0000 K...K...(...@...H..9H.X.}.sx}.{xH...H.Y$8...8`..8...8...8...8...
000002C0 3900 0000 3920 0000 3940 0000 3960 0000 3980 0000 39C0 0000 39E0 0000 3A00 0000 3A20 0000 3A40 0000 3A60 0000 3A80 0000 3AA0 0000 3AC0 0000 3AE0 0000 3B00 0000 9...9 ..9@..9`..9...9...9...:...: ..:@..:`..:...:...:...:...;...
00000300 3B20 0000 3B40 0000 3B60 0000 3B80 0000 3BA0 0000 3BC0 0000 3BE0 0000 3C20 8028 6021 6DB0 3C40 8027 6042 E1E0 3DA0 8027 61AD D200 4E80 0020 9421 FFE0 7C08 02A6 ; ..;@..;`..;...;...;...;...< .(`!m.<@.'`B..=..'a...N.. .!..|...
00000340 9001 0024 93E1 001C 93C1 0018 93A1 0014 3FA0 8000 3BBD 63A0 83DD 0008 2C1E 0000 4182 0038 809D 0000 83FD 0004 4182 0024 7C1F 2040 4182 001C 7FE3 FB78 7FC5 F378 ...$............?...;.c.....,...A..8........A..$|. @A......x...x
00000380 4800 1FED 7FE3 FB78 7FC4 F378 4800 0079 3BBD 000C 4BFF FFC4 3FA0 8000 3BBD 6424 80BD 0004 2C05 0000 4182 001C 807D 0000 4182 000C 3880 0000 4800 20B9 3BBD 0008 H......x...xH..y;...K...?...;.d$....,...A....}..A...8...H. .;...
000003C0 4BFF FFE0 8001 0024 83E1 001C 83C1 0018 83A1 0014 7C08 03A6 3821 0020 4E80 0020 7C00 00A6 6000 2000 7C00 0124 7FE8 02A6 4802 9CED 4802 8A95 4802 B2E9 7FE8 03A6 K......$............|...8!. N.. |...`. .|..$....H...H...H.......
00000400 4E80 0020 3CA0 FFFF 60A5 FFF1 7CA5 1838 7C65 1850 7C84 1A14 7C00 286C 7C00 04AC 7C00 2FAC 30A5 0008 3484 FFF8 4080 FFEC 4C00 012C 4E80 0020 4D65 7472 6F77 6572 N.. <...`...|..8|e.P|...|.(l|...|./.0...4...@...L..,N.. Metrower
00000440 6B73 2054 6172 6765 7420 5265 7369 6465 6E74 204B 6572 6E65 6C20 666F 7220 506F 7765 7250 4300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ks Target Resident Kernel for PowerPC...........................
00000480 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................................................
```



```
00000000 0000 0100 0000 2560 001A 0C20 0000 0000 0000 0000 0000 0000 0000 0000 0016 1AA0 0016 1B80 0016 1C40 0016 1C80 0016 1CA0 0016 C740 0019 F880 001A 0060 001D 5220 ......%`... ...................................@...........@.......`...R 
00000040 0000 0000 0000 0000 8000 4000 8000 6600 8027 6DB0 0000 0000 0000 0000 0000 0000 0000 0000 8000 6460 8000 6540 8016 5B40 8016 5B80 8016 5BA0 8017 0640 8027 5200 ..........@...f..'m.......................d`..e@..[@..[...[....@.'R.
00000080 8027 61E0 802A B3A0 0000 0000 0000 0000 0000 2460 0015 F540 0003 45F0 0000 0000 0000 0000 0000 0000 0000 0000 0000 00E0 0000 00C0 0000 0040 0000 0020 0000 AAA0 .'a..*............$`...@..E............................@... ....
000000C0 0003 3140 0000 07E0 0000 0BC0 0007 8860 0000 0000 0000 0000 801A 3780 000D 3630 8027 6DB0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ..1@...........`........7...60.'m...............................
00000100 3C60 8000 A003 30E4 7000 0EEF 2C00 0EEF 4C82 0020 3860 0000 3880 0000 38A0 0000 4803 1E74 4E80 0020 3800 0001 980D 8940 4E80 0020 886D 8940 4E80 0020 4800 016D <`....0.p...,...L.. 8`..8...8...H..tN.. 8......@N.. .m.@N.. H..m
00000140 4800 02A1 3800 FFFF 9421 FFF8 9001 0004 9001 0000 4800 01E5 3800 0000 3CC0 8000 38C6 0044 9006 0000 3CC0 8000 38C6 00F4 80C6 0000 2806 0000 4182 000C 80E6 000C H...8....!..........H...8...<...8..D....<...8.......(...A.......
00000180 4800 0024 3CA0 8000 38A5 0034 80A5 0000 2805 0000 4182 004C 3CE0 8000 38E7 30E8 80E7 0000 38A0 0000 2807 0002 4182 0024 2807 0003 38A0 0001 4182 0018 2807 0004 H..$<...8..4....(...A..L<...8.0.....8...(...A..$(...8...A...(...
000001C0 4082 0020 38A0 0002 4BFF FF61 4800 0014 3CC0 800A 38C6 5530 7CC8 03A6 4E80 0021 3CC0 8000 38C6 00F4 80A6 0000 2805 0000 41A2 0060 80C5 0008 2806 0000 41A2 0054 @.. 8...K..aH...<...8.U0|...N..!<...8.......(...A..`....(...A..T
00000200 7CC5 3214 81C6 0000 280E 0000 4182 0044 39E6 0004 7DC9 03A6 38C6 0004 80E6 0000 7CE7 2A14 90E6 0000 4200 FFF0 3CA0 8000 38A5 0034 55E7 0034 90E5 0000 3CA0 8000 |.2.....(...A..D9...}...8.......|.*.....B...<...8..4U..4....<...
00000240 38A5 3110 55E7 0034 90E5 0000 4800 000C 39C0 0000 39E0 0000 4803 59BD 4802 96BD 3C80 8000 3884 30E6 A064 0000 7065 8000 4182 0010 7063 7FFF 2803 0001 4082 0008 8.1.U..4....H...9...9...H.Y.H...<...8.0..d..pe..A...pc..(...@...
00000280 4BFF FE81 4BFF FEB1 2803 0001 4082 0008 480A 1439 4803 58CD 7DC3 7378 7DE4 7B78 4800 2E15 4803 5924 3800 0000 3860 0000 3880 0000 38A0 0000 38C0 0000 38E0 0000 K...K...(...@...H..9H.X.}.sx}.{xH...H.Y$8...8`..8...8...8...8...
000002C0 3900 0000 3920 0000 3940 0000 3960 0000 3980 0000 39C0 0000 39E0 0000 3A00 0000 3A20 0000 3A40 0000 3A60 0000 3A80 0000 3AA0 0000 3AC0 0000 3AE0 0000 3B00 0000 9...9 ..9@..9`..9...9...9...:...: ..:@..:`..:...:...:...:...;...
00000300 3B20 0000 3B40 0000 3B60 0000 3B80 0000 3BA0 0000 3BC0 0000 3BE0 0000 3C20 8028 6021 6DB0 3C40 8027 6042 E1E0 3DA0 8027 61AD D200 4E80 0020 9421 FFE0 7C08 02A6 ; ..;@..;`..;...;...;...;...< .(`!m.<@.'`B..=..'a...N.. .!..|...
00000340 9001 0024 93E1 001C 93C1 0018 93A1 0014 3FA0 8000 3BBD 63A0 83DD 0008 2C1E 0000 4182 0038 809D 0000 83FD 0004 4182 0024 7C1F 2040 4182 001C 7FE3 FB78 7FC5 F378 ...$............?...;.c.....,...A..8........A..$|. @A......x...x
00000380 4800 1FED 7FE3 FB78 7FC4 F378 4800 0079 3BBD 000C 4BFF FFC4 3FA0 8000 3BBD 6424 80BD 0004 2C05 0000 4182 001C 807D 0000 4182 000C 3880 0000 4800 20B9 3BBD 0008 H......x...xH..y;...K...?...;.d$....,...A....}..A...8...H. .;...
000003C0 4BFF FFE0 8001 0024 83E1 001C 83C1 0018 83A1 0014 7C08 03A6 3821 0020 4E80 0020 7C00 00A6 6000 2000 7C00 0124 7FE8 02A6 4802 9CED 4802 8A95 4802 B2E9 7FE8 03A6 K......$............|...8!. N.. |...`. .|..$....H...H...H.......
00000400 4E80 0020 3CA0 FFFF 60A5 FFF1 7CA5 1838 7C65 1850 7C84 1A14 7C00 286C 7C00 04AC 7C00 2FAC 30A5 0008 3484 FFF8 4080 FFEC 4C00 012C 4E80 0020 4D65 7472 6F77 6572 N.. <...`...|..8|e.P|...|.(l|...|./.0...4...@...L..,N.. Metrower
00000440 6B73 2054 6172 6765 7420 5265 7369 6465 6E74 204B 6572 6E65 6C20 666F 7220 506F 7765 7250 4300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ks Target Resident Kernel for PowerPC...........................
00000480 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 ................................................................
```

Malware on Wii



The attacker's point of view - Malware injection on existing games

Malware on Wii

- Demo : Malware(**attack remote host**) in live action while the game is playing

Malware on Wii

- Demo : Malware(**network down**) in live action while the game is playing

Malware on Wii

- Demo : Malware(**attack ap & dns pharming**) in live action while the game is playing

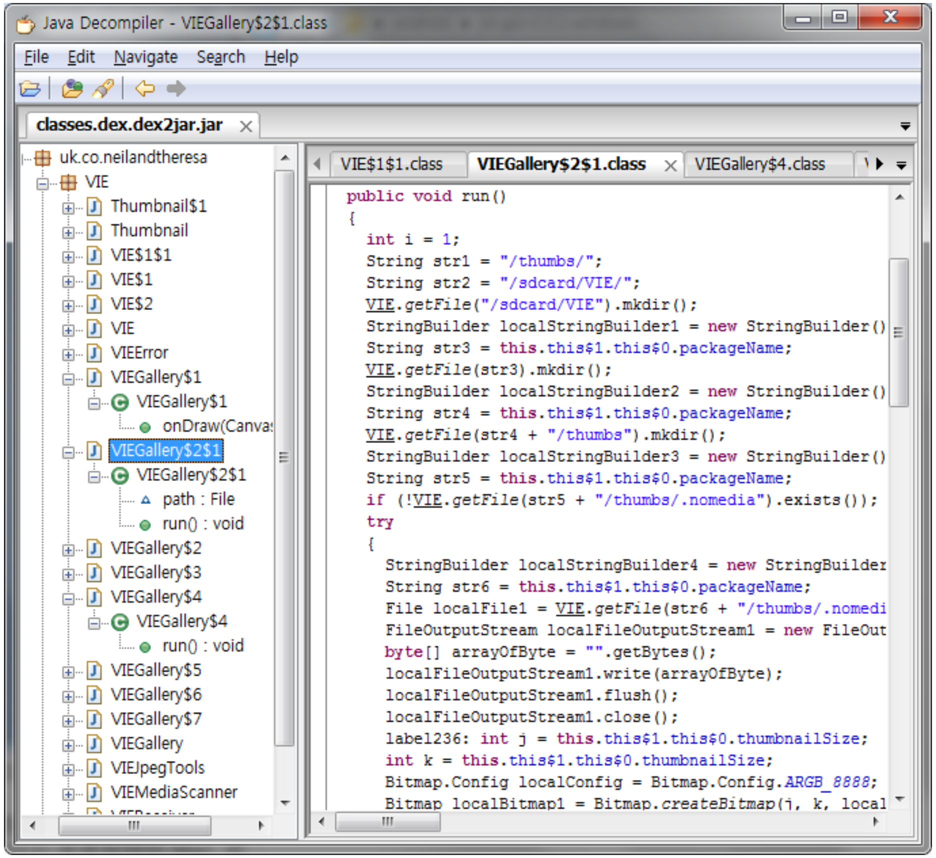
Malware injection on Smartphone applications

Malware on iPhone

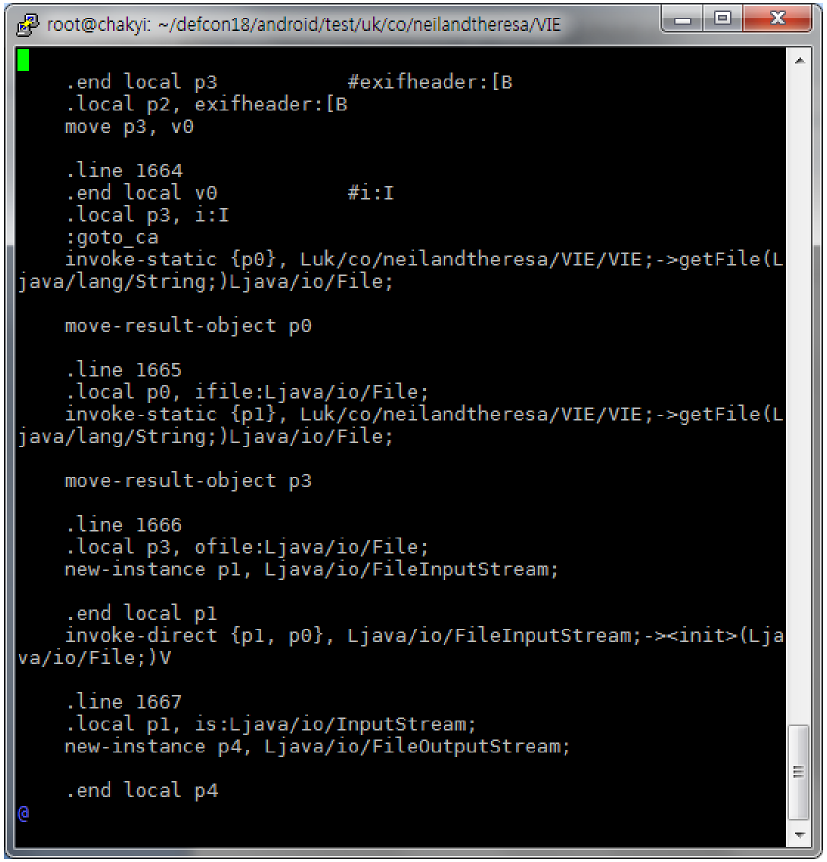
- Executables are Mach-O binaries

- Lots of malware papers on MAC viruses are public

Malware on Android



```
public void run()
{
  int i = 1;
  String str1 = "/thumbs/";
  String str2 = "/sdcard/VIE/";
  VIE.getFile("/sdcard/VIE").mkdir();
  StringBuilder localStringBuilder1 = new StringBuilder()
  String str3 = this.this$1.this$0.packageName;
  VIE.getFile(str3).mkdir();
  StringBuilder localStringBuilder2 = new StringBuilder()
  String str4 = this.this$1.this$0.packageName;
  VIE.getFile(str4 + "/thumbs").mkdir();
  StringBuilder localStringBuilder3 = new StringBuilder()
  String str5 = this.this$1.this$0.packageName;
  if (!VIE.getFile(str5 + "/thumbs/.nomedia").exists());
  try
  {
    StringBuilder localStringBuilder4 = new StringBuilder
    String str6 = this.this$1.this$0.packageName;
    File localFile1 = VIE.getFile(str6 + "/thumbs/.nomedi
    FileOutputStream localFileOutputStream1 = new FileOut
    byte[] arrayOfByte = "".getBytes();
    localFileOutputStream1.write(arrayOfByte);
    localFileOutputStream1.flush();
    localFileOutputStream1.close();
    label236: int j = this.this$1.this$0.thumbnailSize;
    int k = this.this$1.this$0.thumbnailSize;
    Bitmap.Config localConfig = Bitmap.Config.ARGB_8888;
    Bitmap localBitmap1 = Bitmap.createBitmap(j, k, local
```


root@chakyi: ~/defcon18/android/test/uk/co/neilandtheresa/VIE

```
    .end local p3             #exifheader:[B
    .local p2, exifheader:[B
    move p3, v0

    .line 1664
    .end local v0             #i:I
    .local p3, i:I
    :goto_ca
    invoke-static {p0}, Luk/co/neilandtheresa/VIE/VIE;->getFile(L
java/lang/String;)Ljava/io/File;

    move-result-object p0

    .line 1665
    .local p0, ifile:Ljava/io/File;
    invoke-static {p1}, Luk/co/neilandtheresa/VIE/VIE;->getFile(L
java/lang/String;)Ljava/io/File;

    move-result-object p3

    .line 1666
    .local p3, ofile:Ljava/io/File;
    new-instance p1, Ljava/io/FileInputStream;

    .end local p1
    invoke-direct {p1, p0}, Ljava/io/FileInputStream;-><init>(Lja
va/io/File;)V

    .line 1667
    .local p1, is:Ljava/io/InputStream;
    new-instance p4, Ljava/io/FileOutputStream;

    .end local p4
@
```

How to Defend

Defenses

- Manufacturers : Steps to take when designing a new device

- Security Companies : Measurements in Software or Policies

- Users : Precautions for the general users

Conclusion

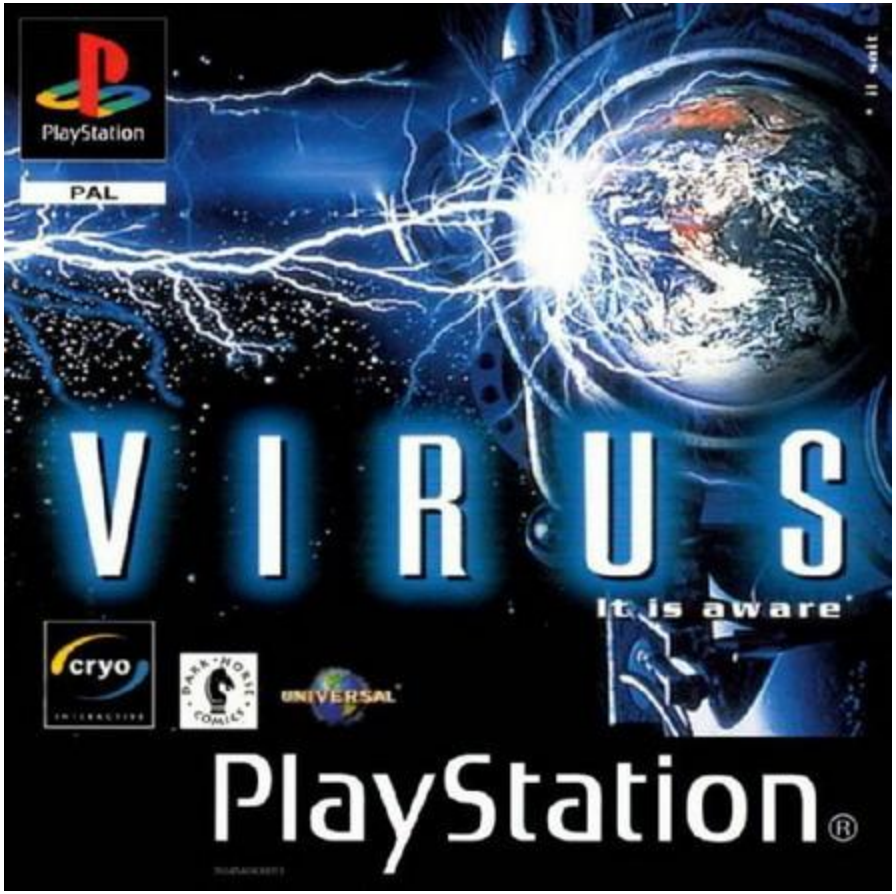
Conclusion

- There are no doubts that malware can run on embedded devices, and there may already be some running in the wild

- These malware can be equally strong as those on PC, so one must be fully aware of their potential

- Not only Gaming Consoles of Smartphones, but any other future embedded device may become a target, so users should be careful and be prepared

Download Games at your own risk!



References

- Google
http://google.com/

- WiiBrew
http://wiibrew.org/wiki/Main_Page

- GBATemp
http://gbatemp.net

- devkitPro.org
http://www.devkitpro.org/

- kkamagui 프로그래밍 세상
http://kkamagui.tistory.com/

- POC
http://www.powerofcommunity.net/