Embedded devices, an AntiVirus-free safe hideout for Malware

IS YOUR GAMING CONSOLE SAFE?

DongJoo Ha - AhnLab Inc., Security Researcher
KiChan Ahn - Hanyang University, Undergraduate

AhnLab

About

AhnLab

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
- Malware on Console Gaming systems
- Malware injection on Smartphone applications

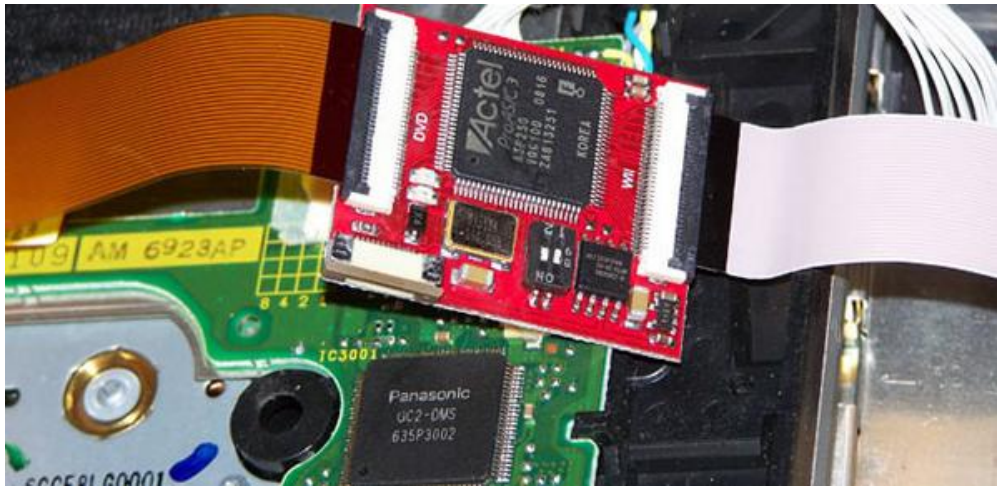
Preparation - Our defenses
- Manufacturers : Steps to take when designing a new device
- Service, Security companies : Measurements in Software or Policies
- Users : Precautions for the general users

Background Knowledge

The pirate scene of Gamine consoles and Smartphones

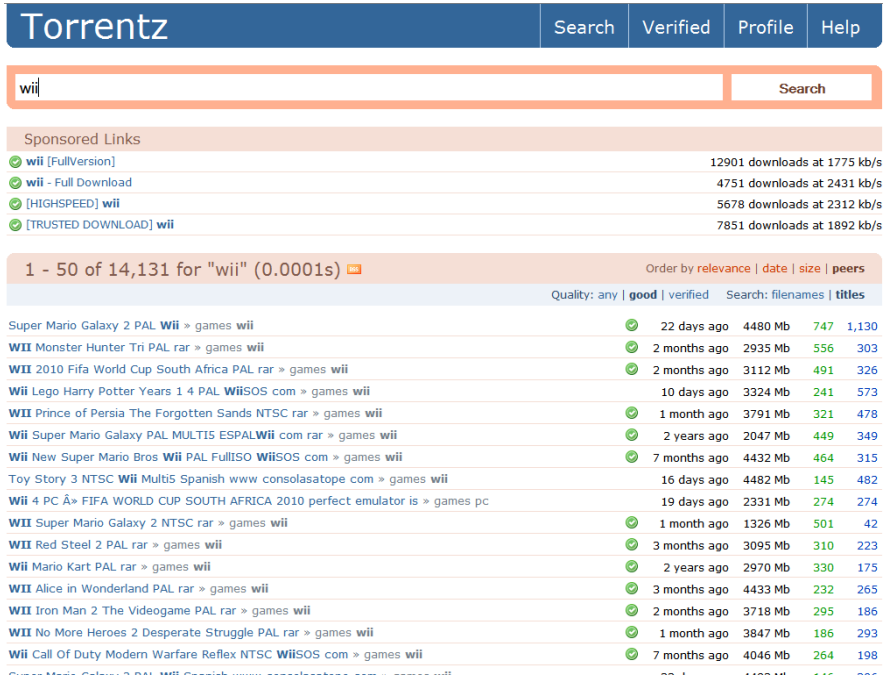
Payed software being illegally downloaded

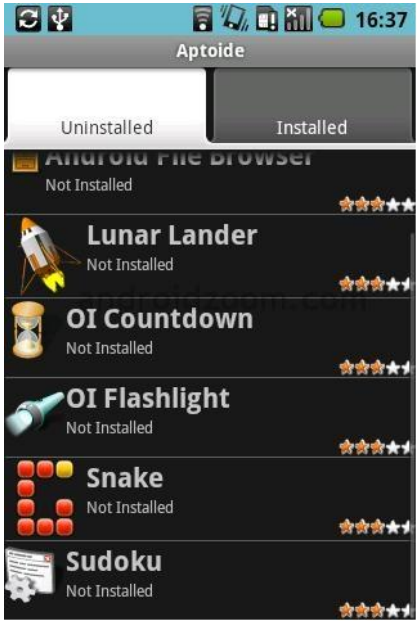
- Most embedded devices implement anti pirate
  Measures by some means, but these protections are
  eventually bypassed



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





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

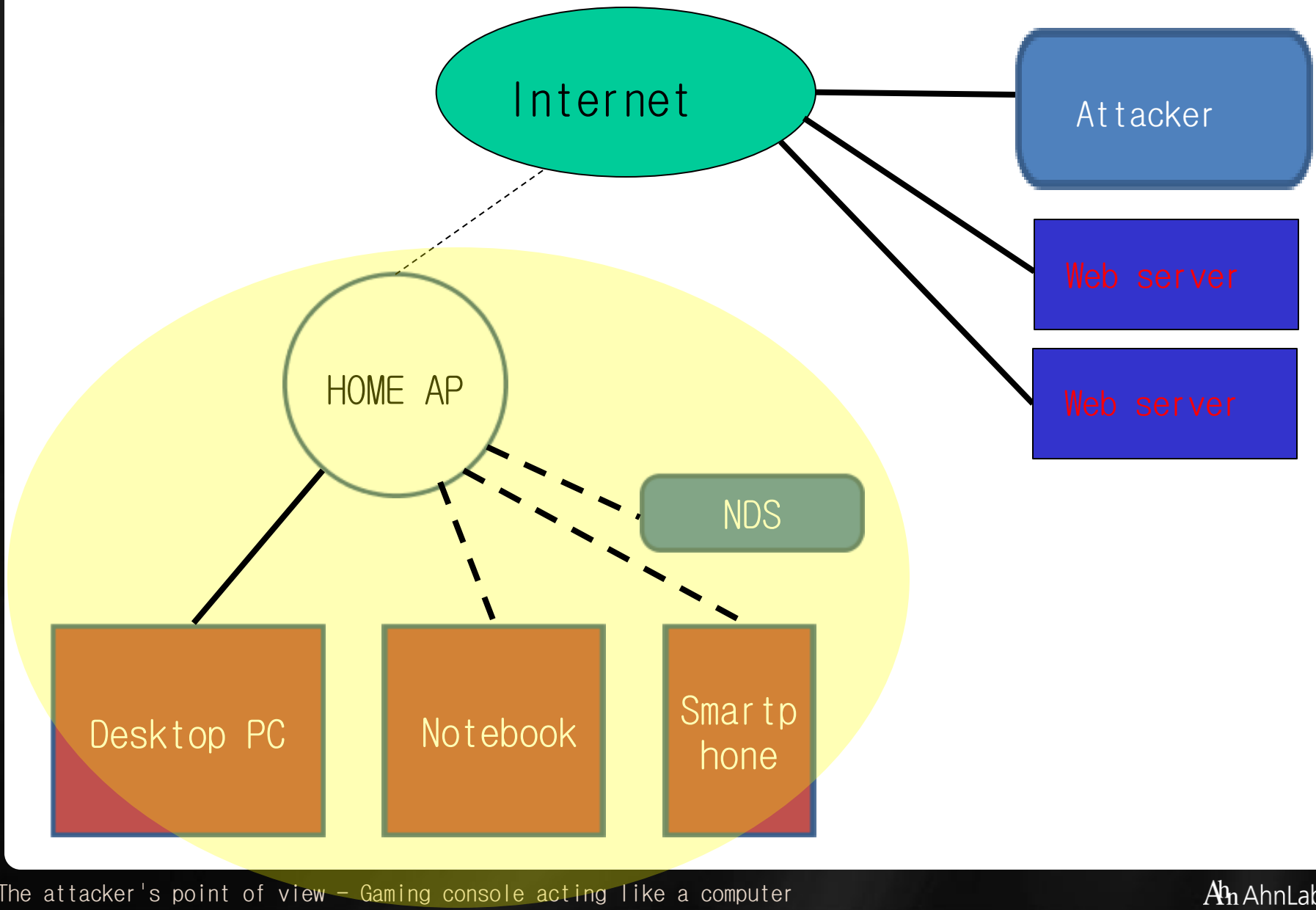
Gaming Consoles as an attacking Tool

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

Hacking with NDS



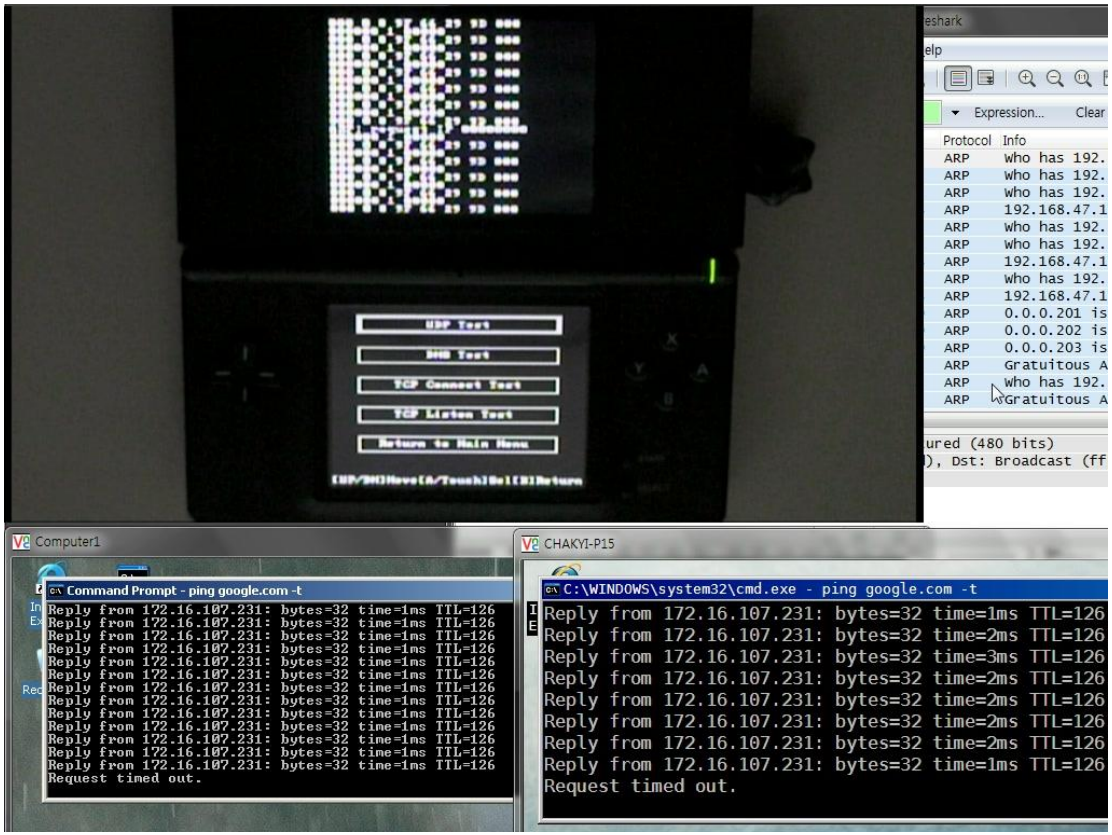
Hacking with NDS

- 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

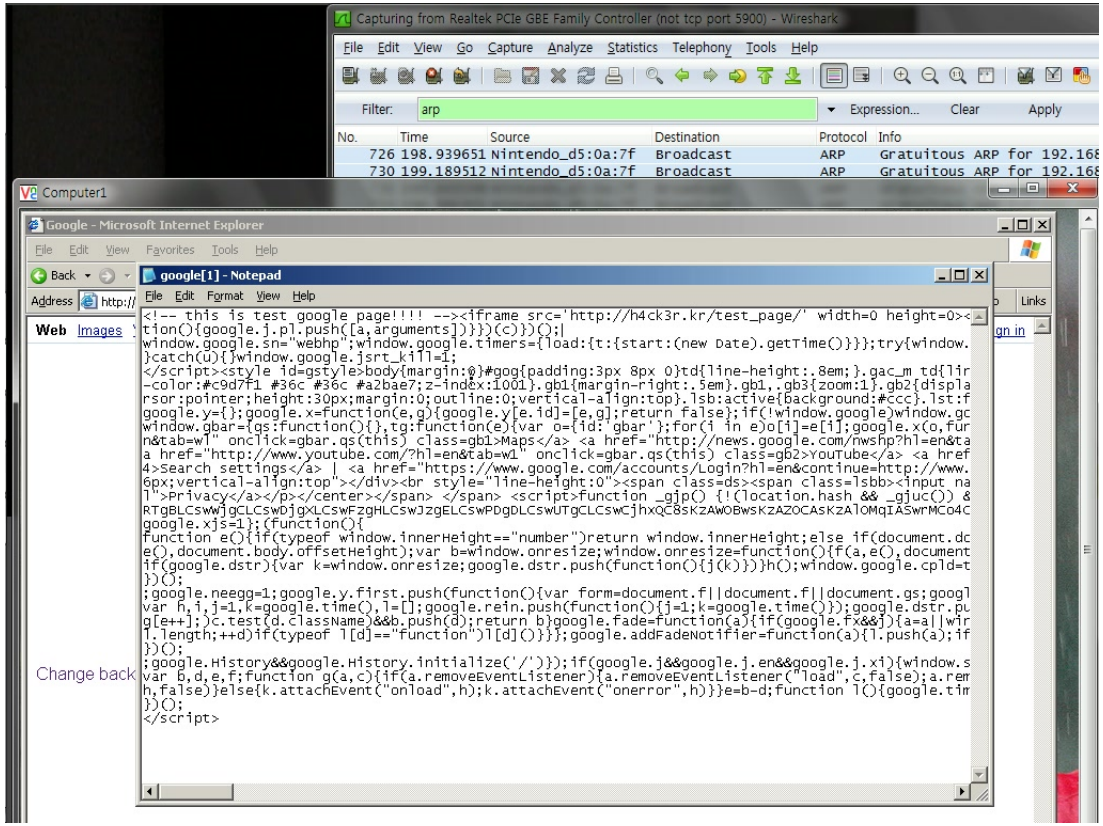
- Attacking the network
- Demo : Using NDS to bring down a network



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

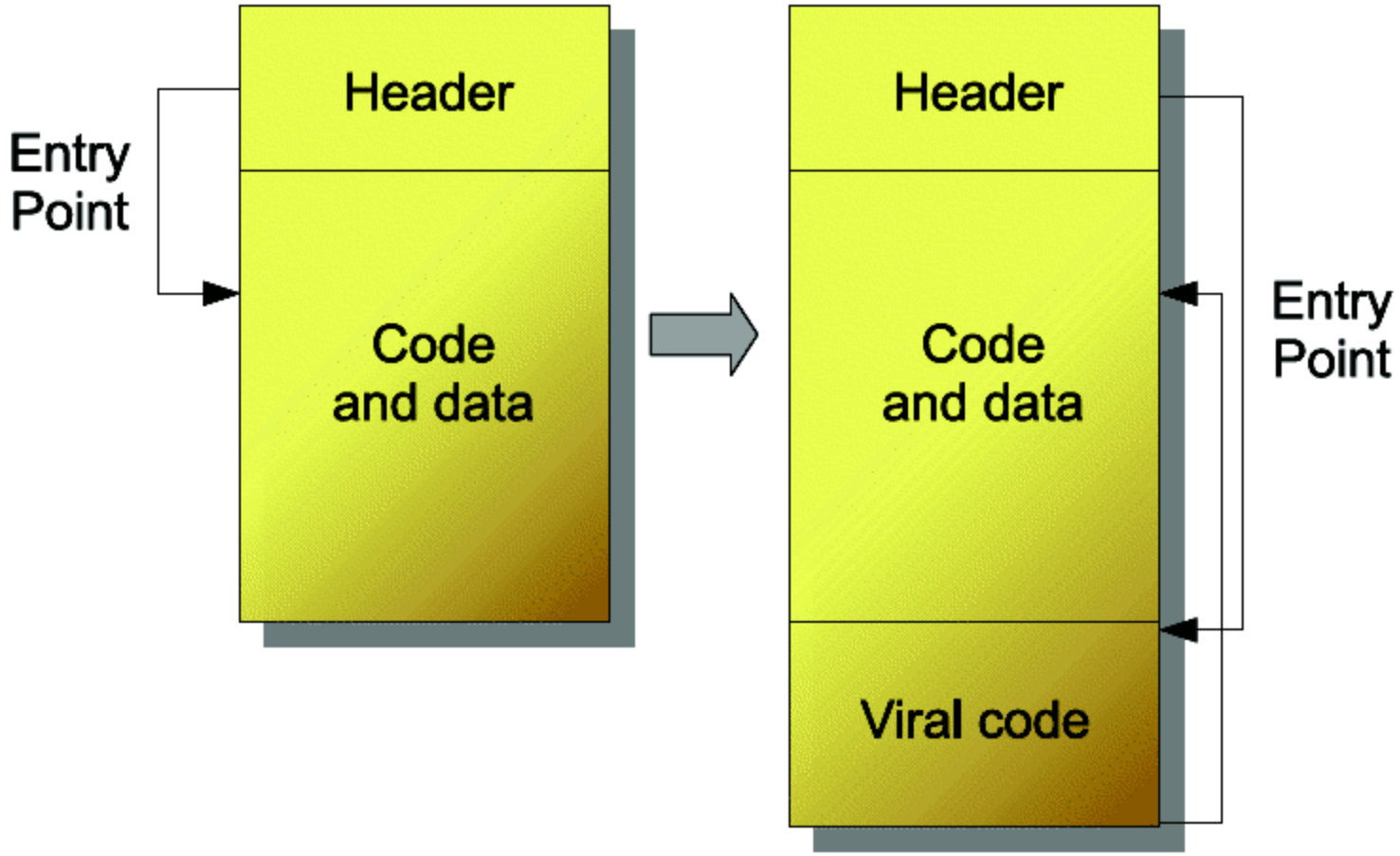
- executables files are files with .dol extension
- they are essentially a stripped down version of an elf file
- system menu -> apploader -> .dol
- .dol files(and sometimes .rel files) contain all code needed for the game to run

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

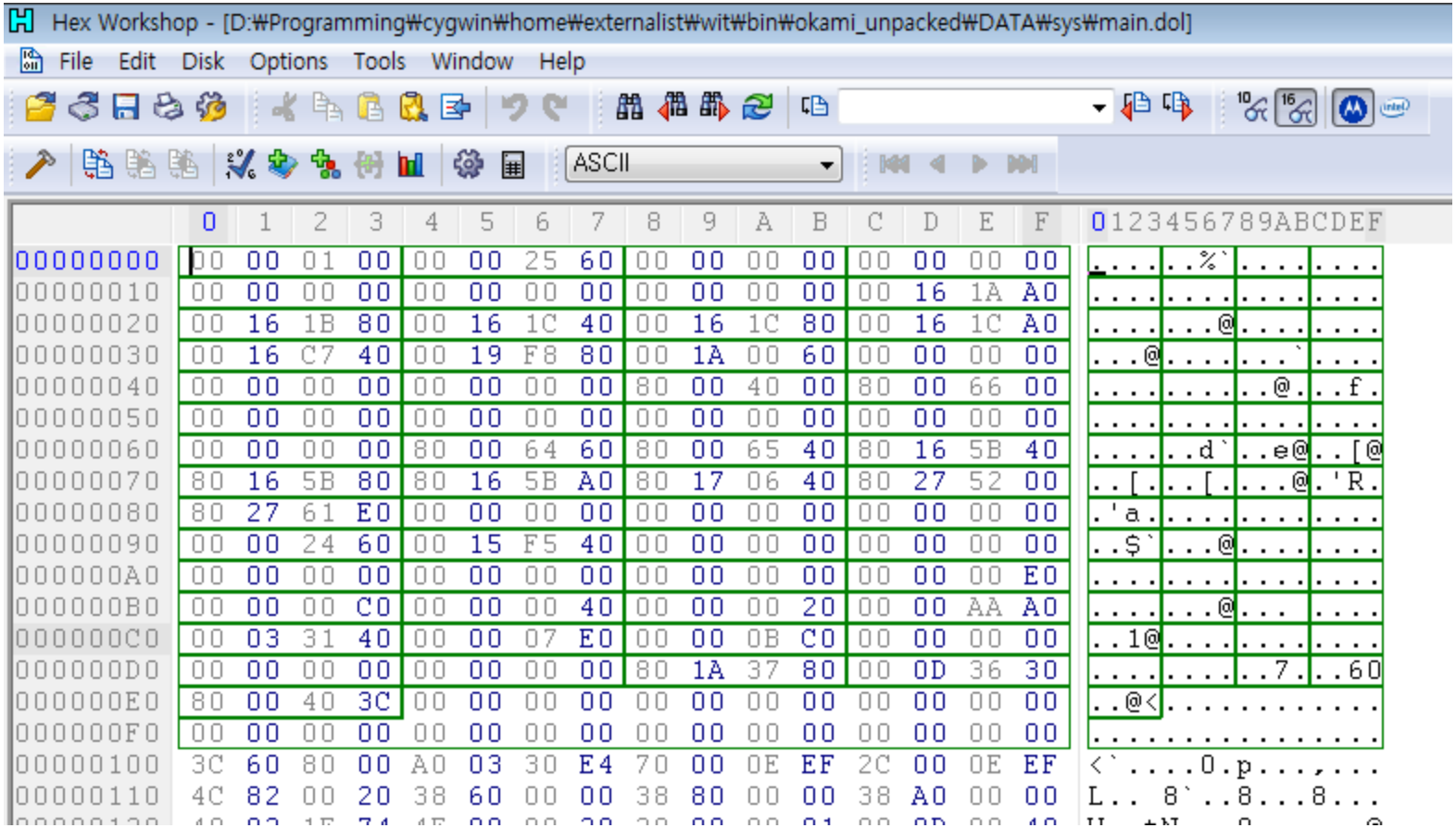
Start	End	Length	Description
0x0	0x3	4	File offset to start of Text0
0x04	0x1b	24	File offsets for Text1..6
0x1c	0x47	44	File offsets for Data0..10
0x48	0x4B	4	Loading address for Text0
0x4C	0x8F	68	Loading addresses for Text1..6, Data0..10
0x90	0xD7	72	Section sizes for Text0..6, Data0..10
0xD8	0xDB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

Basic infection process

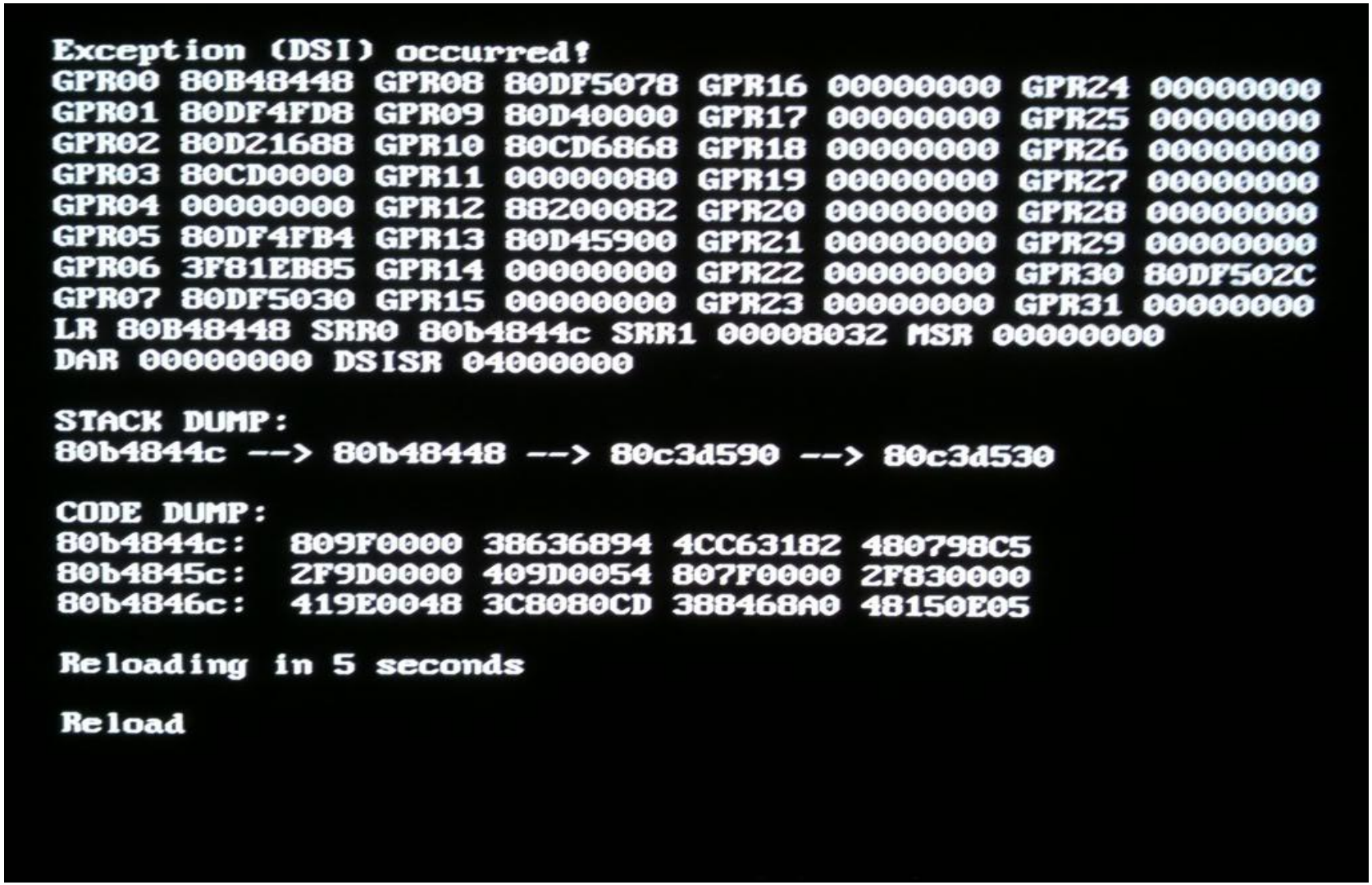


```
lis     %r10, ((__libogc_sbrk_r+0x10000)@h)
lis     %r11, ((__syscalls+0x10000)@h)
addi    %r0, %r10, -0x1520 # __libogc_sbrk_r
addi    %r9, %r11, -0x40C0 # __syscalls
stw     %r0, __syscalls@l(%r11)
lis     %r11, ((__libogc_gettod_r+0x10000)@h)
addi    %r0, %r11, -0x204C # __libogc_gettod_r
lis     %r11, aLibogcRelease1@h # "libOGC Release 1.8.3"
stw     %r0, ((__syscalls+0x20+0x40C0)@l)(%r9)
li      %r0, 1
stw     %r0, 0x284(%r13)
addi    %r0, %r11, aLibogcRelease1@l # "libOGC Release 1.8.3"
lis     %r11, aSep232010@h # "Sep 23 2010"
stw     %r0, 0x28C(%r13)
addi    %r0, %r11, aSep232010@l # "Sep 23 2010"
lis     %r11, ((__libogc_lock_init+0x10000)@h)
stw     %r0, 0x29C(%r13)
addi    %r0, %r11, -0x1D5C # __libogc_lock_init
lis     %r11, ((__libogc_lock_close+0x10000)@h)
stw     %r0, ((__syscalls+4+0x40C0)@l)(%r9)
addi    %r0, %r11, -0x1DAC # __libogc_lock_close
lis     %r11, ((__libogc_lock_release+0x10000)@h)
stw     %r0, ((__syscalls+8+0x40C0)@l)(%r9)
addi    %r0, %r11, -0x1E24 # __libogc_lock_release
lis     %r11, ((__libogc_lock_acquire+0x10000)@h)
stw     %r0, ((__syscalls+0xC+0x40C0)@l)(%r9)
addi    %r0, %r11, -0x1DE8 # __libogc_lock_acquire
lis     %r11, ((__libogc_malloc_lock+0x10000)@h)
stw     %r0, ((__syscalls+0x10+0x40C0)@l)(%r9)
addi    %r0, %r11, -0x1330 # __libogc_malloc_lock
lis     %r11, ((__libogc_malloc_unlock+0x10000)@h)
stw     %r0, ((__syscalls+0x14+0x40C0)@l)(%r9)
addi    %r0, %r11, -0x138C # __libogc_malloc_unlock
lis     %r11, ((__libogc_exit+0x10000)@h)
```

Manipulating DOL files

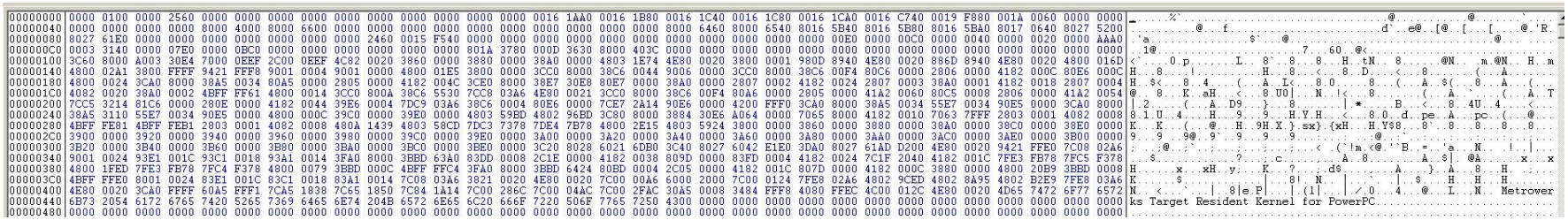


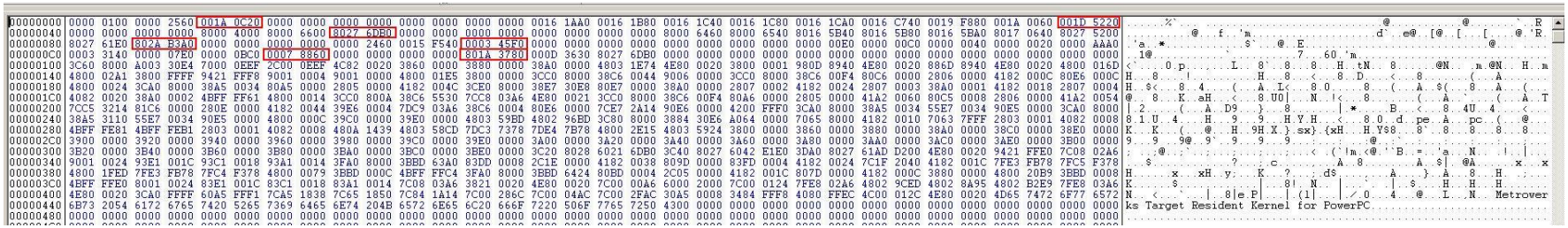
Debugging - Crash Dump



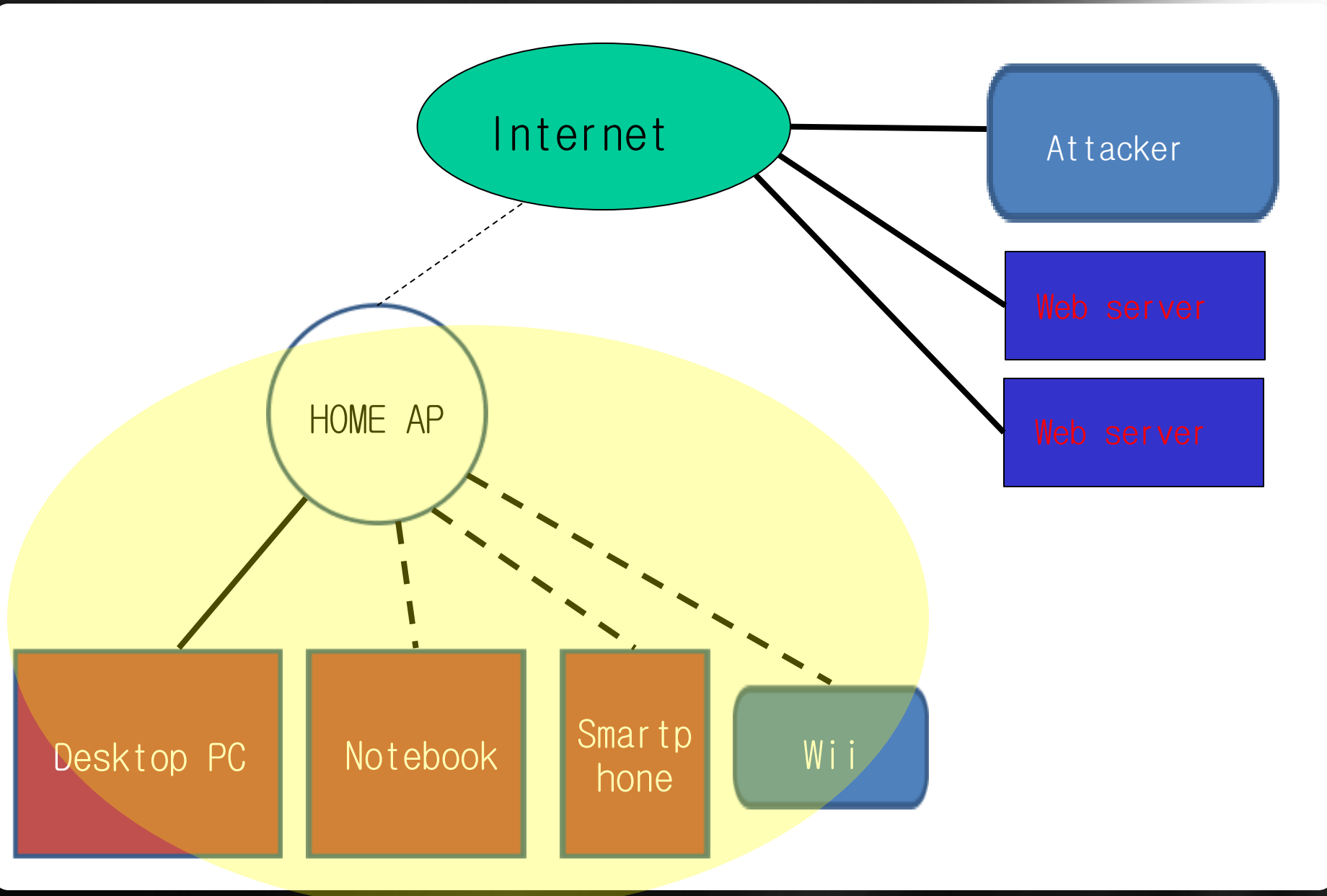
How custom code can be injected

- Demo1 : POC of malware injection on Nintendo Wii games
  Demo2





Malware on Wii

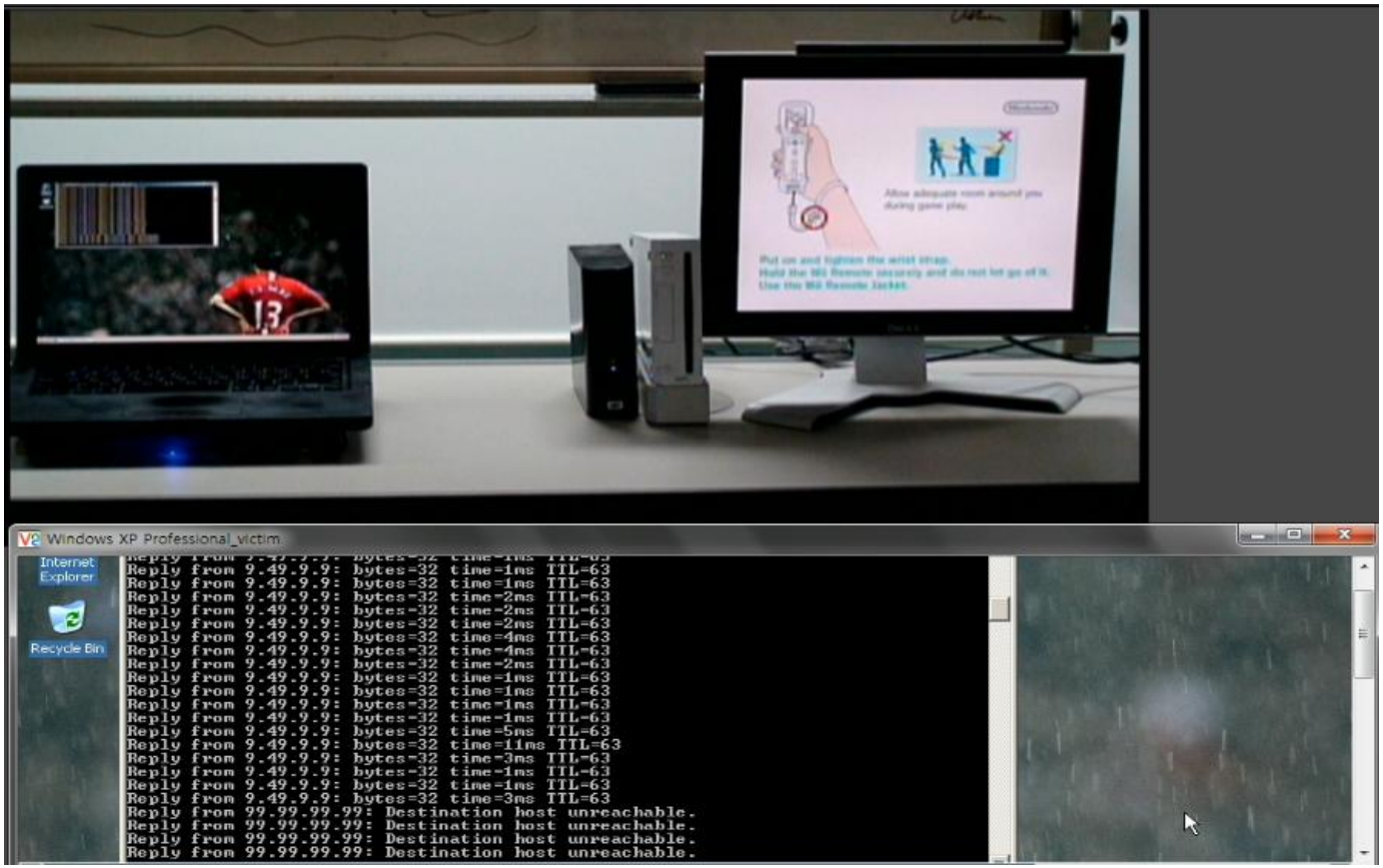


Malware on Wii

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

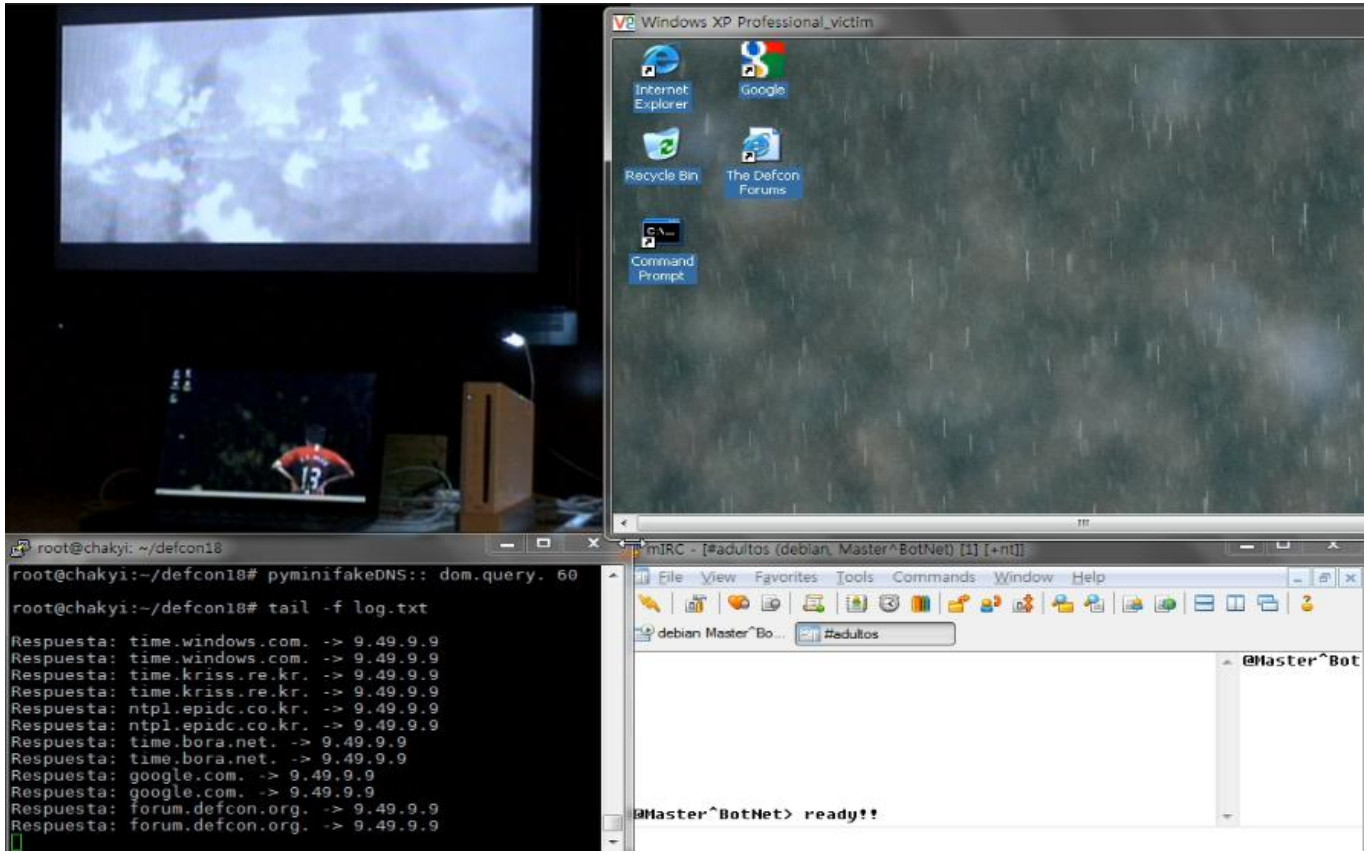
Malware on Wii

- 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



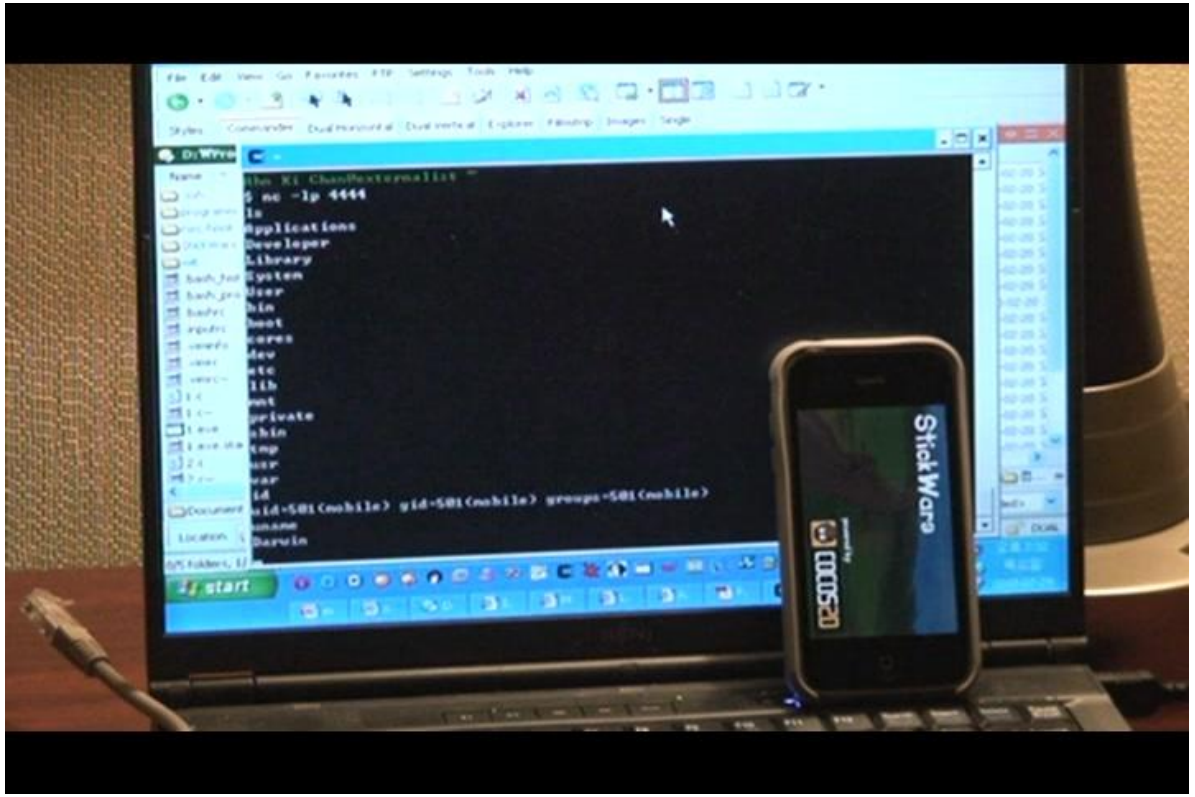
Malware injection on Smartphone applications

Malware on iPhone

- Executables are Mach-O binaries

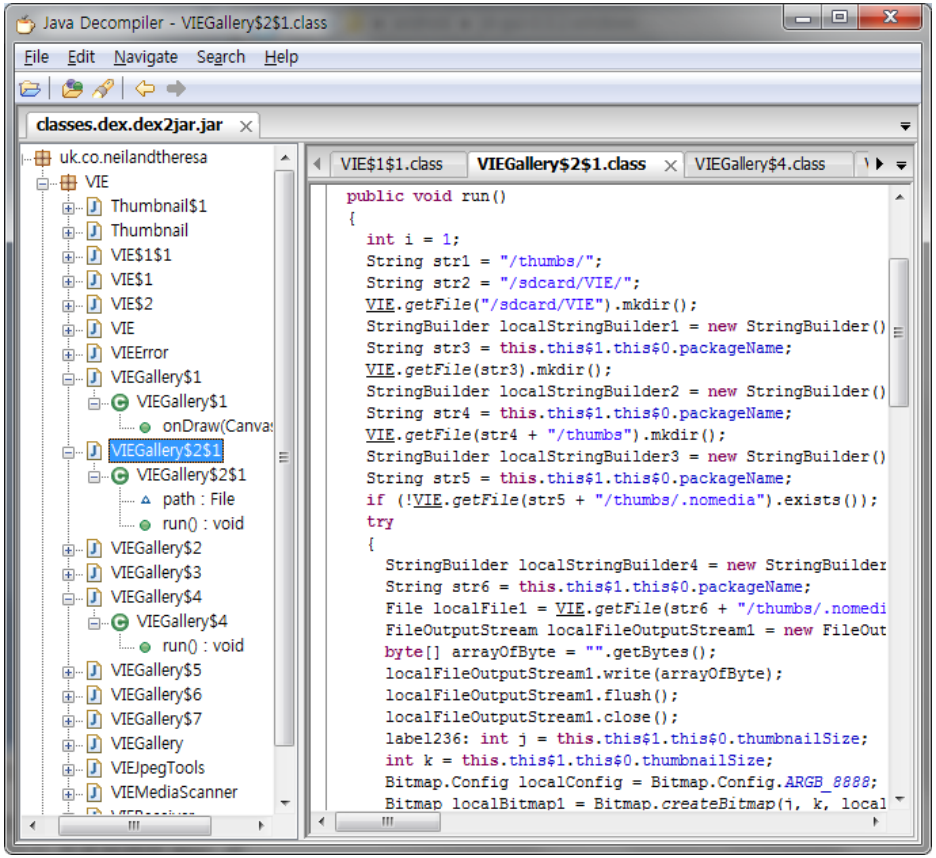
- Lots of malware papers on MAC viruses are public

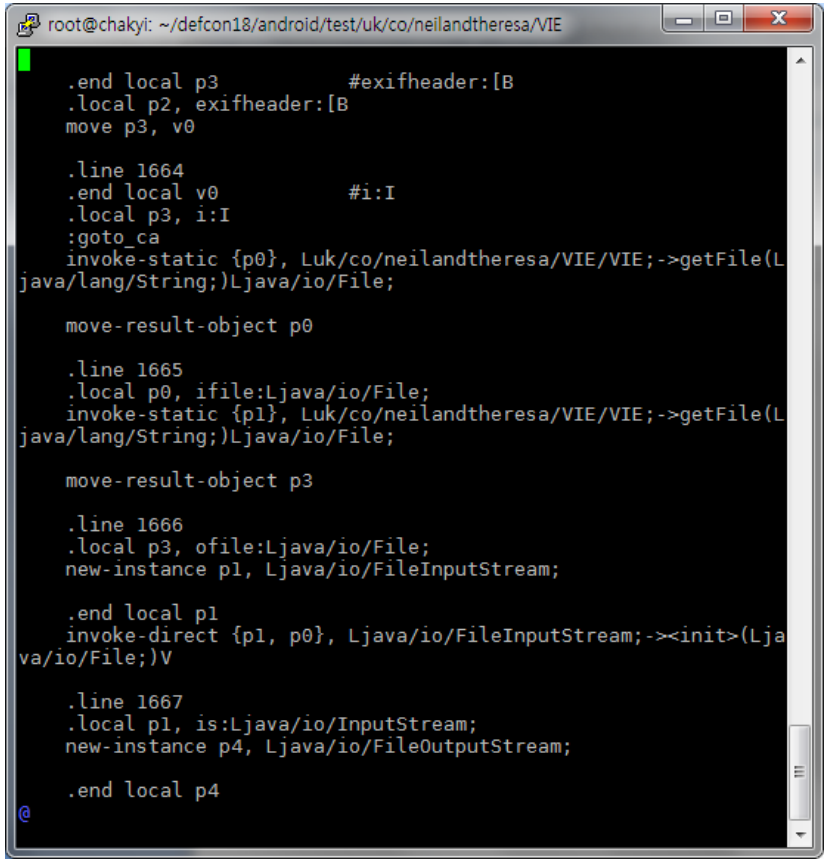
- Demo
- Demo2



Malware on Android

- Demo





How to Defend

Defenses

- Manufacturers : Steps to take when designing a new device

-Security Companies : Measurements in Software or Policies
(Demo)

- Users : Precautions for the general users

Conclusion

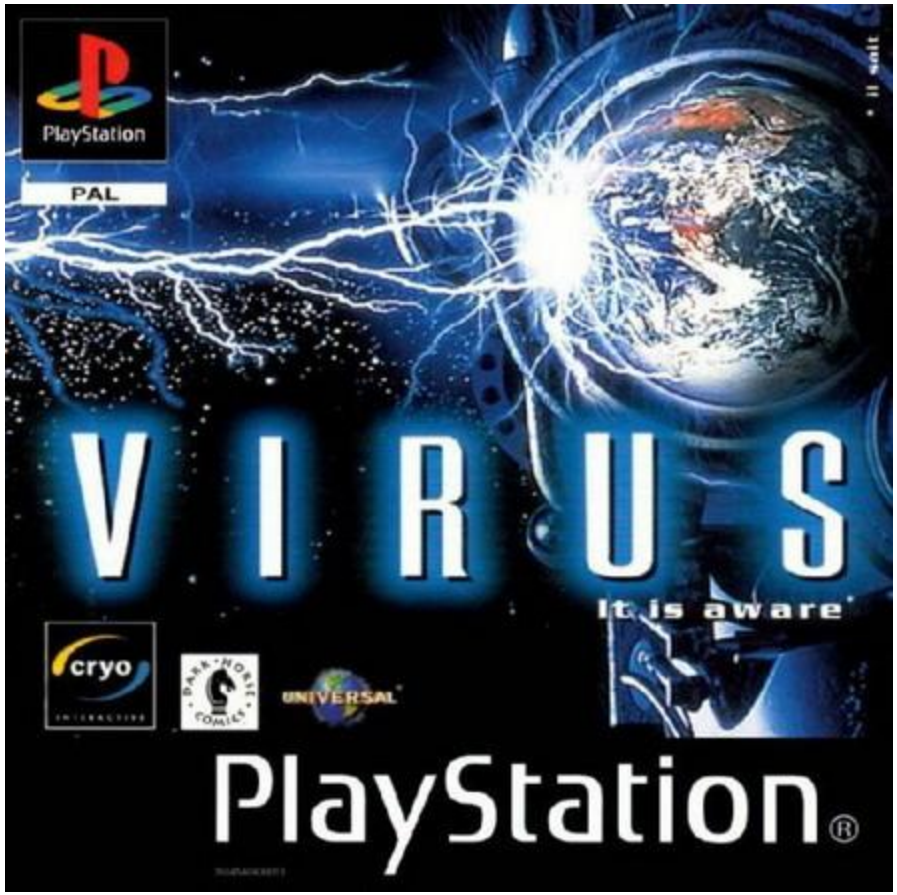
Conclusion

- 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/

Question?

DongJoo Ha (@ChakYi) : lovely@h4ck3r.kr
KiChan Ahn (@Externalist) : wringer@paran.com