

Embedded devices, an AntiVirus-free safe hideout for Malware

# IS YOUR GAMING CONSOLE SAFE?

KiChan Ahn - Korea Financial Telecommunications  
& Clearings Institute, Security Researcher

DongJoo Ha - AhnLab Inc., Security Researcher

# 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 Game 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

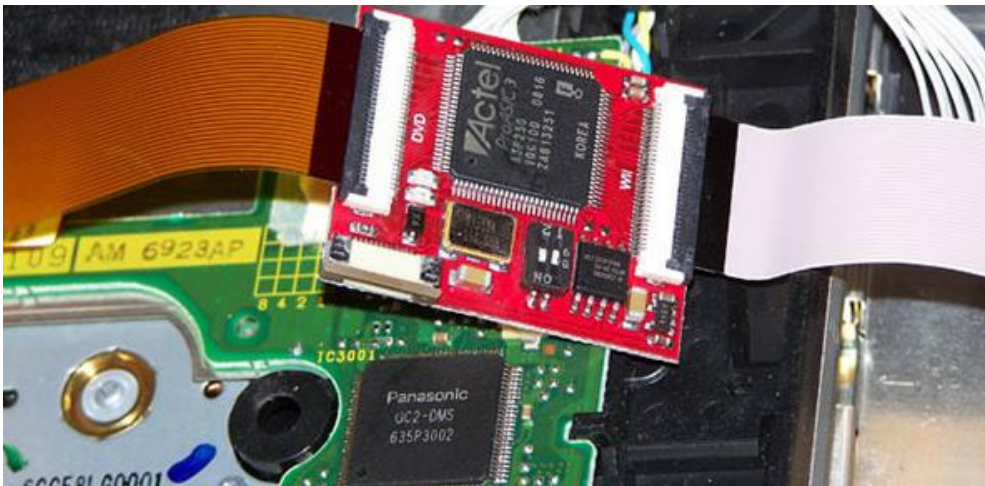
- Manufacturers : Steps to take when designing a new device
- Service, Security companies : Measurements in Software or Policies
- Users : Precautions for the general users

# 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 screenshot shows the Torrentz search results for 'wii'. The search bar contains 'wii' and the search button is labeled 'Search'. Below the search bar, there are sponsored links for 'wii' with various download speeds and download counts. The main results section shows a list of 50 items, with the first few being 'Super Mario Galaxy 2 PAL Wii', 'Wii Monster Hunter Tri PAL rar', and 'Wii 2010 Fifa World Cup South Africa PAL rar'. Each item includes a green checkmark, the date it was added, the file size, and the number of seeds and leechers.

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

The screenshot shows the Aptoide app interface. At the top, there are navigation buttons for 'Uninstalled' and 'Installed'. Below that, there is a section for 'Android File Browser' which is 'Not Installed'. The main list of games includes 'Lunar Lander', 'OI Countdown', 'OI Flashlight', 'Snake', and 'Sudoku', all of which are 'Not Installed'. Each game entry has a star rating and a small icon.



# 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

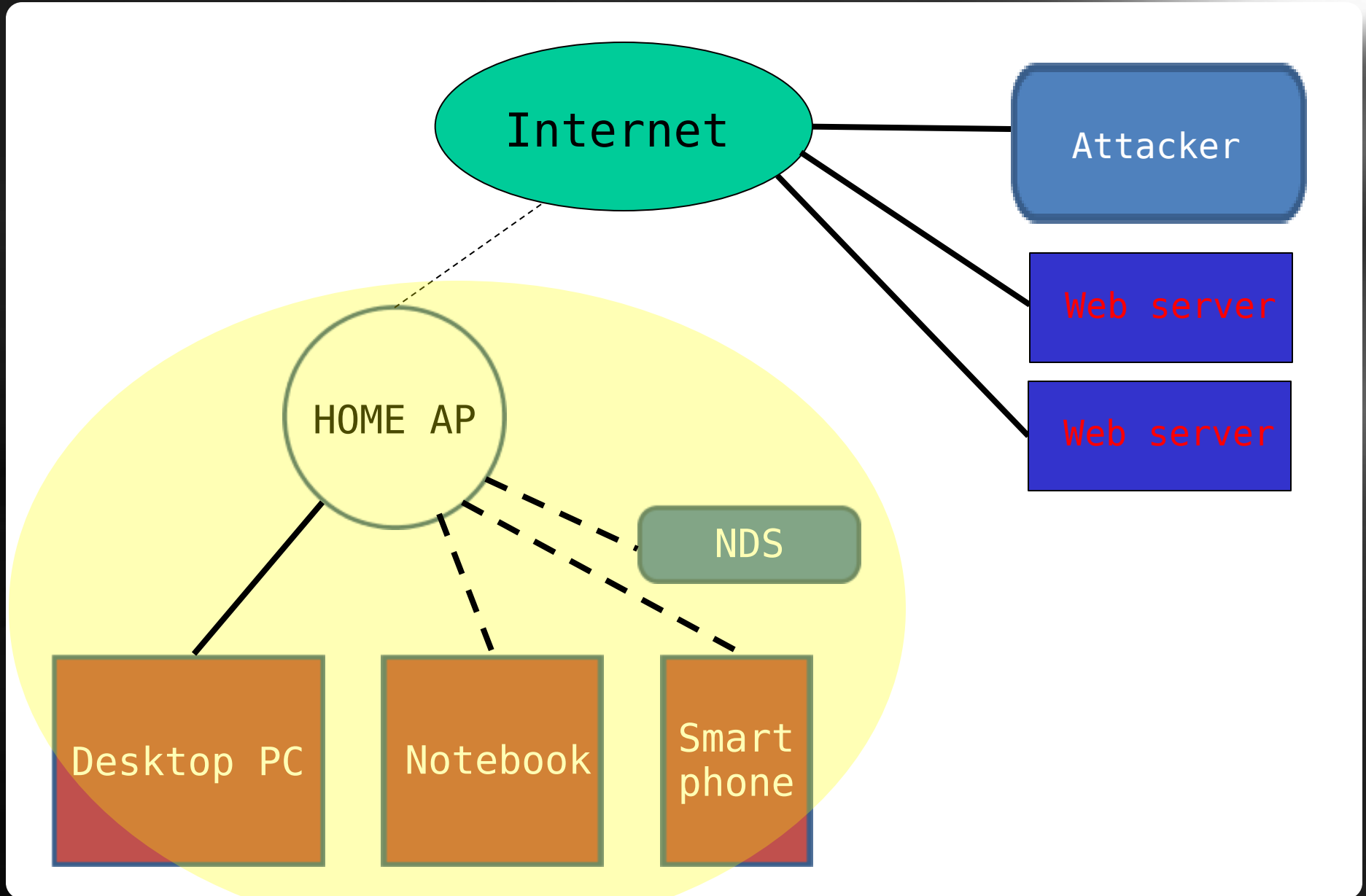


# The hardware and software development environment

- 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



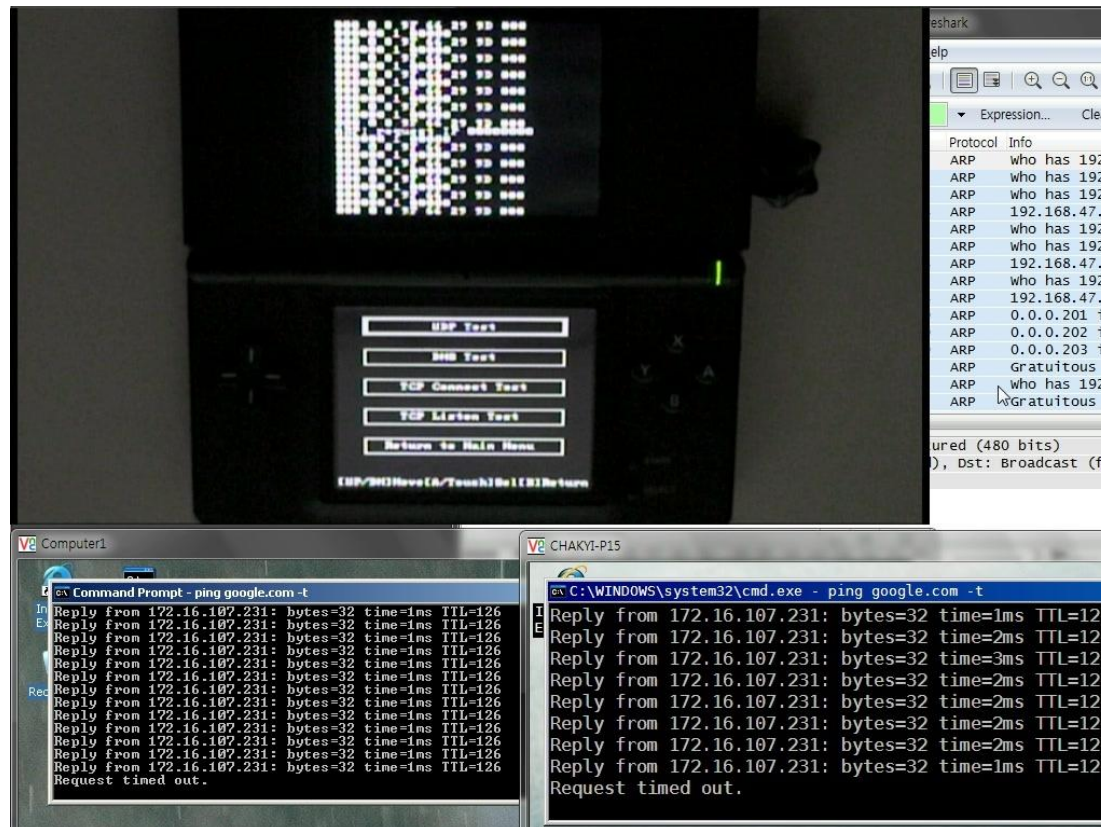
# Hacking with NDS

- Attacking and taking control of a PC
- [Demo](#) : Using NDS to attack a PC on the network with a public remote exploit



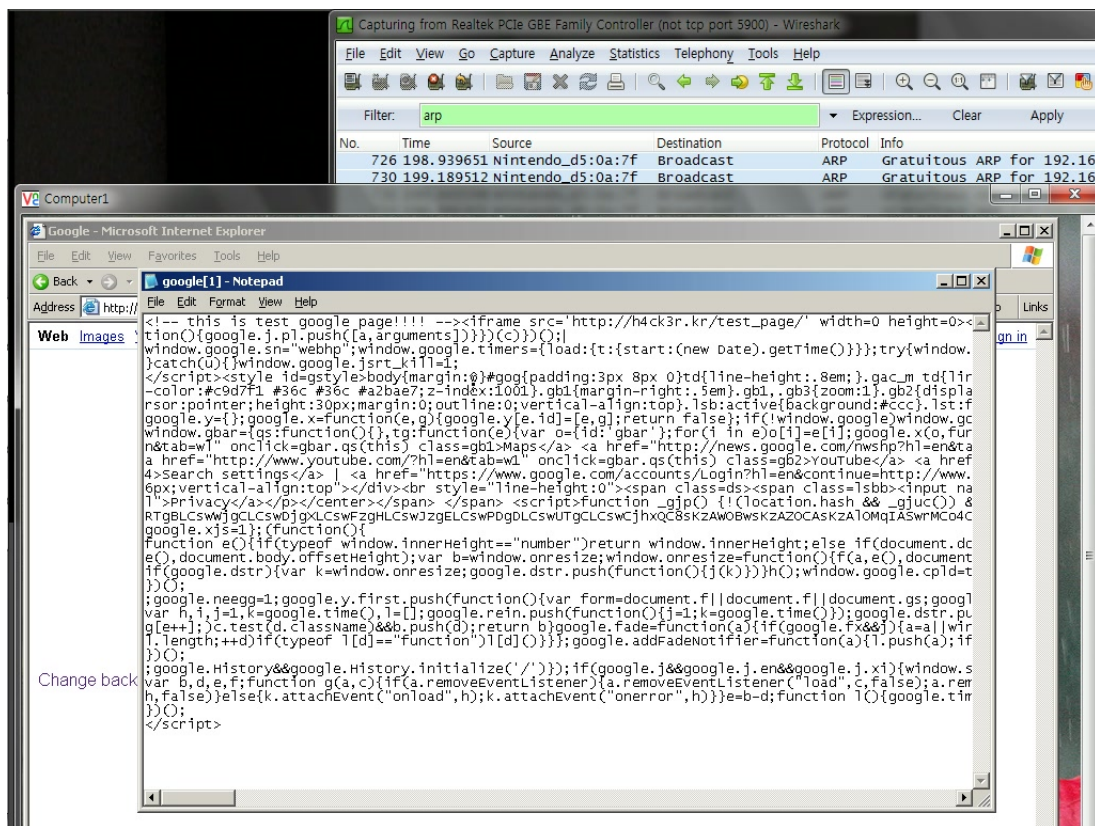
# Hacking with NDS

- 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

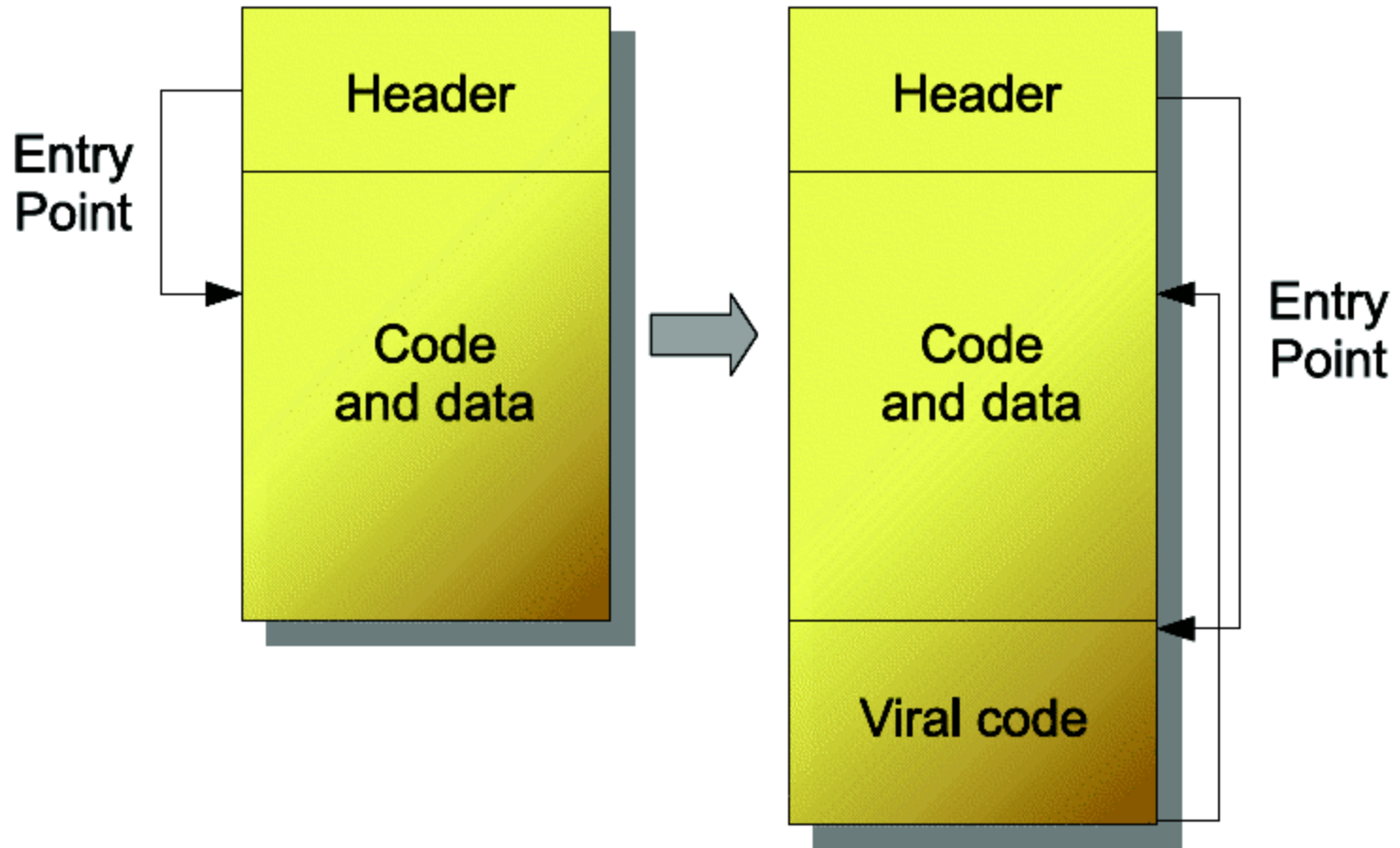


# How custom code can be injected

- 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

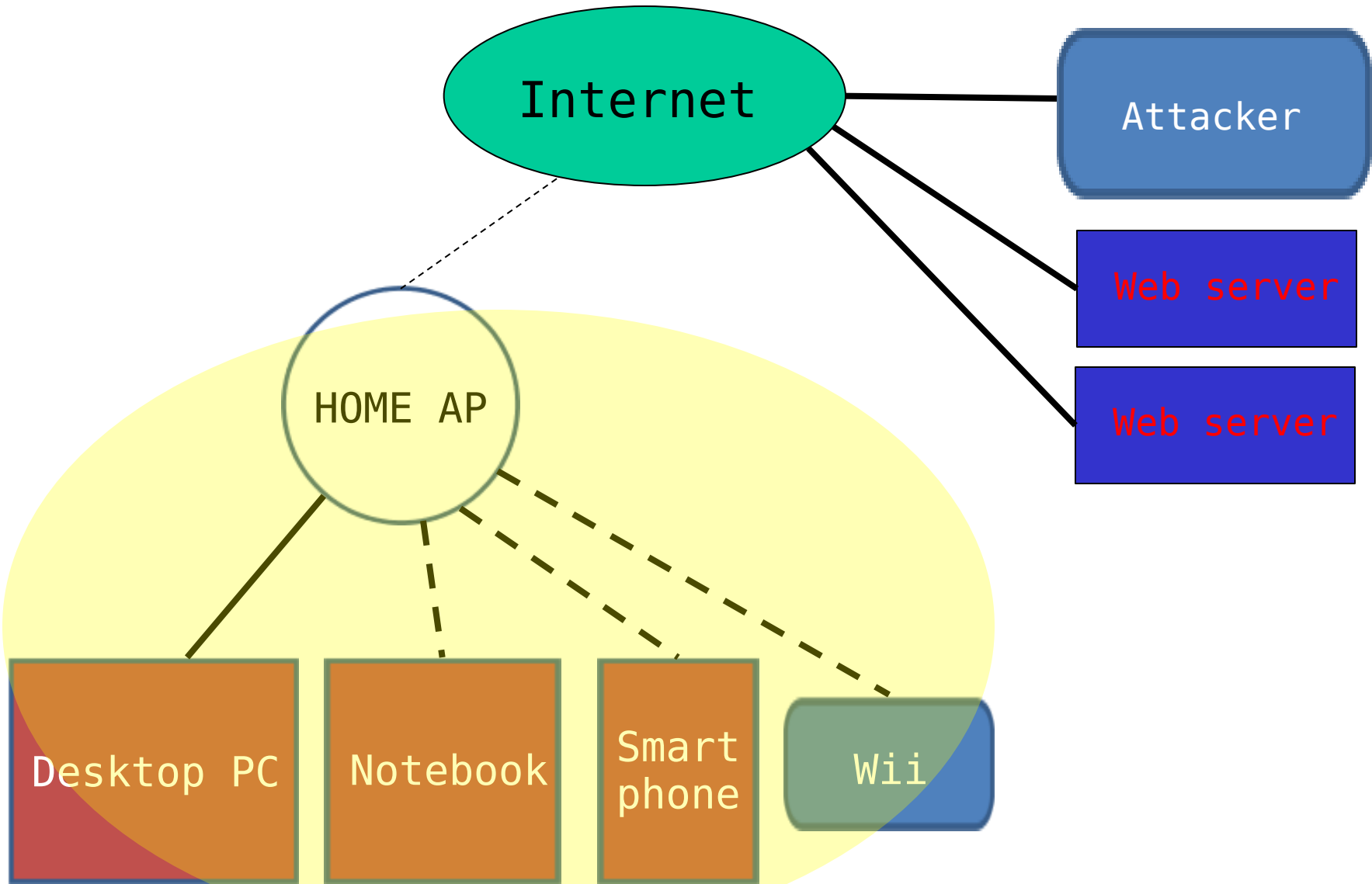
Start	End	Length	Description
0x0	0x3	4	File offset to start of Text0
0x04	0x1b	24	File offsets for Text1..6
0x1c	0x47	44	File offsets for Data0..10
0x48	0x4B	4	Loading address for Text0
0x4C	0x8F	68	Loading addresses for Text1..6, Data0..10
0x90	0xD7	72	Section sizes for Text0..6, Data0..10
0xD8	0xDB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

# Basic infection process





# Malware on Wii



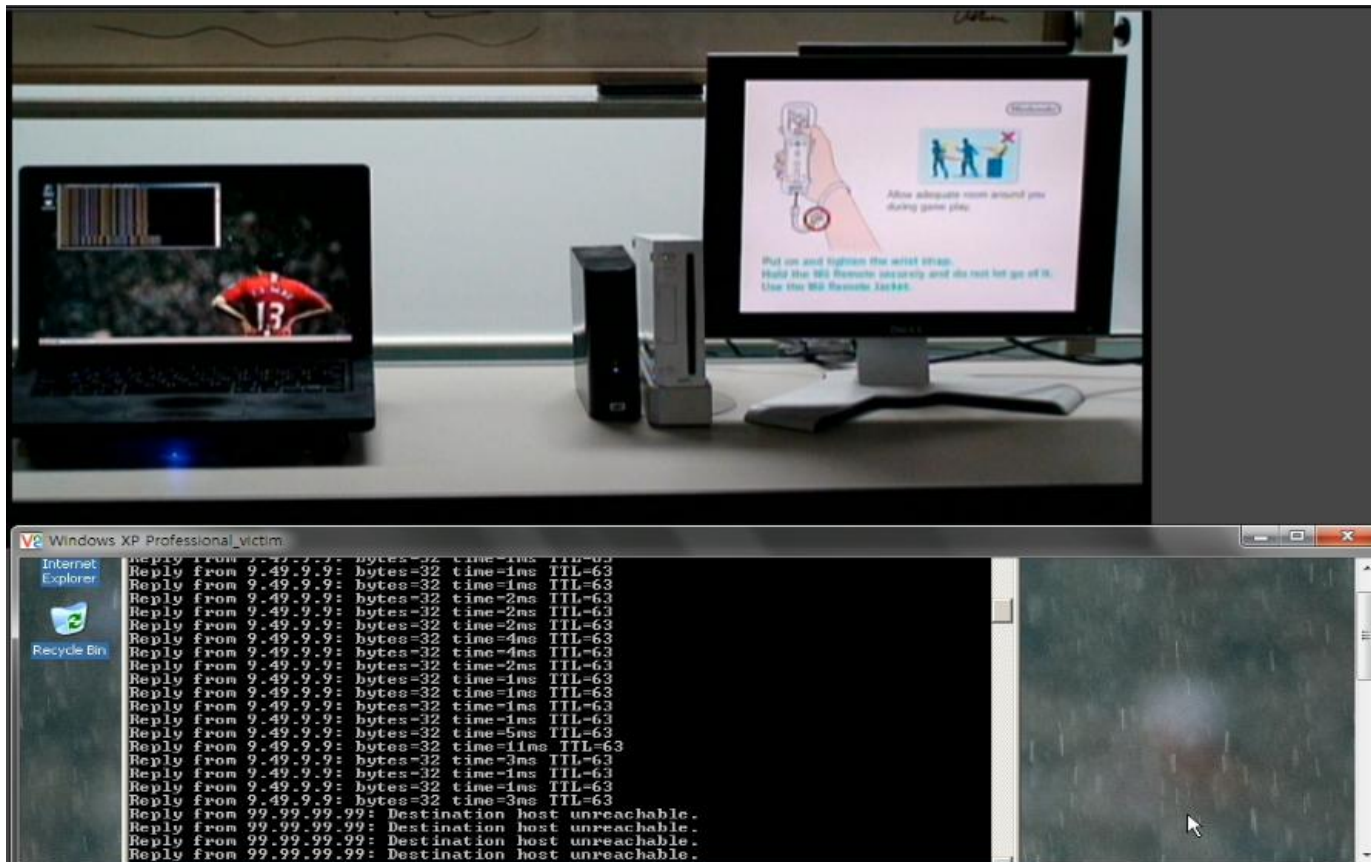
# Malware on Wii

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



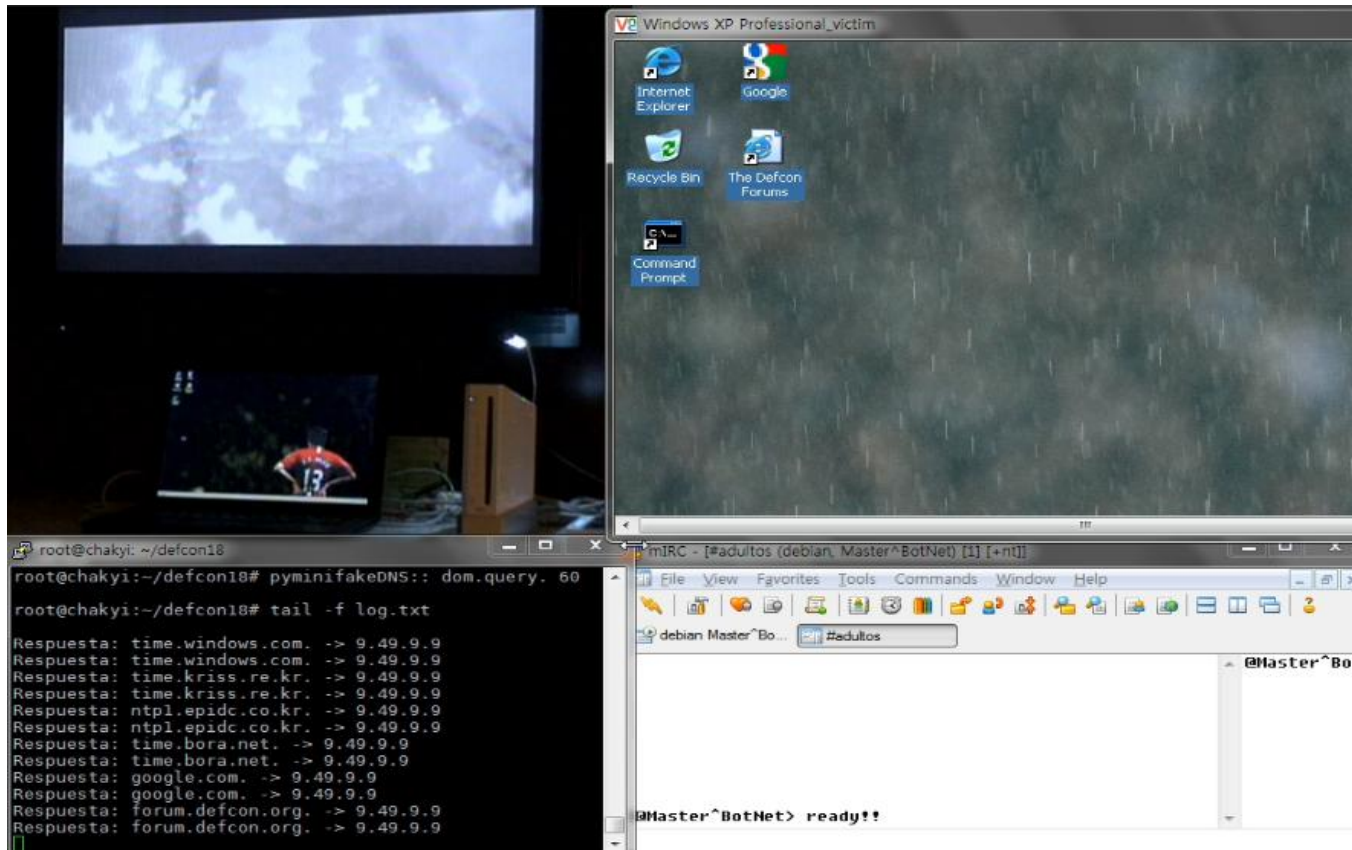
# Malware on Wii

- 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

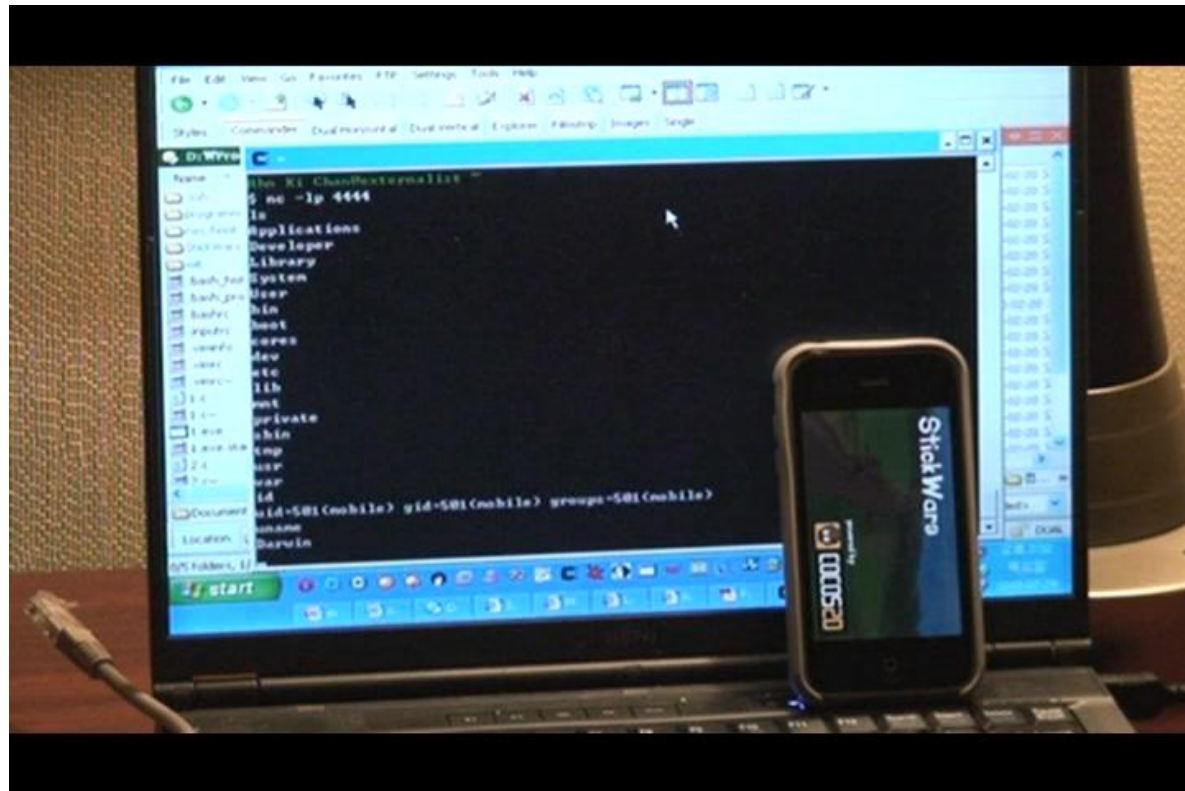


# Malware injection on Smartphone applications



# Malware on iPhone

- Executables are Mach-O binaries
- Lots of malware papers on MAC viruses are public
- [Demo1](#)
- [Demo2](#)
- [Demo3](#)



# Malware on Android

## - Demo

```
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/.nomedia");
        FileOutputStream localFileOutputStream1 = new FileOutputStream(localFile1);
        byte[] arrayOfByte = "".getBytes();
        localFileOutputStream1.write(arrayOfByte);
        localFileOutputStream1.flush();
        localFileOutputStream1.close();
        label1236: 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
```

```
.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(Ljava/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(Ljava/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(Ljava/io/File;)V

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

.end local p4
```

# How to Defend

# Defenses

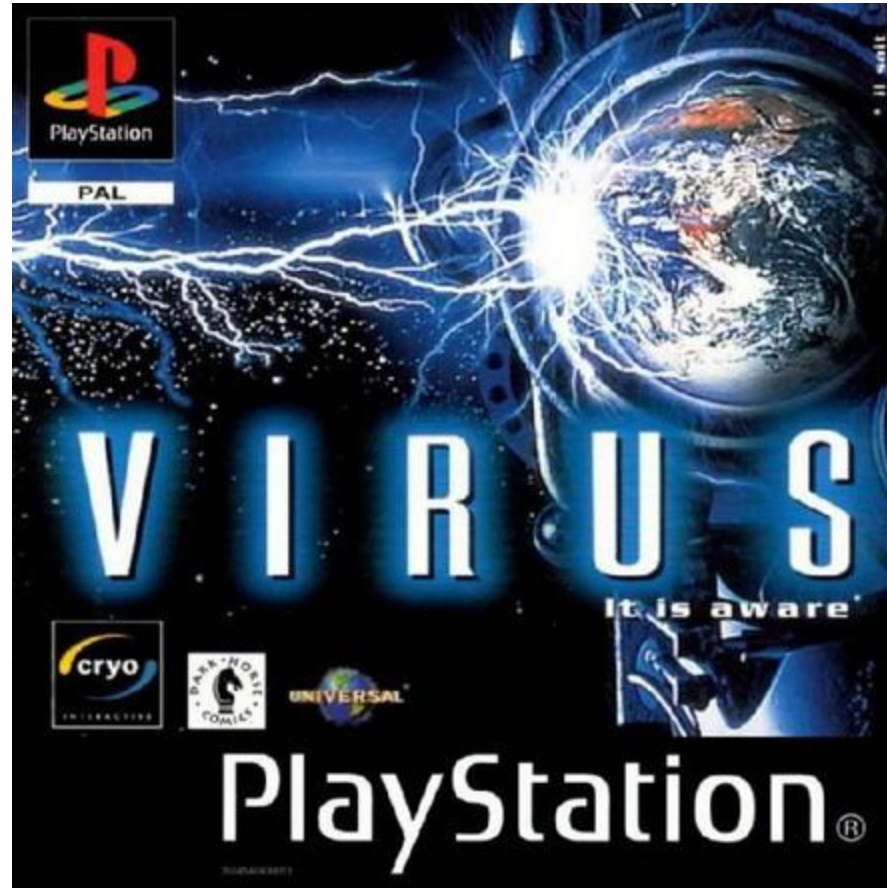
- Manufacturers : Steps to take when designing a new device
- Security Companies : Measurements in Software or Policies ( [Demo](#) )
- Users : Precautions for the general users

# 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 or 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](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