

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

# About

# Speakers

Ahn Ki-Chan - Hanyang University, Undergraduate

Ha Dong-Joo - AhnLab Inc., Security Researcher

Member of Song of Freedom

TBD

# Introduction

- Embedded systems (gaming consoles, smartphones, etc.) have enough hardware for malware for malware to survive and perform it's job
- There were 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 destructive 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 acting like computers - Hacking with NDS
- Malware injection on existing games - Malware on Wii
- Malware injected into Smartphone applications - Malware on Smartphones

## Preparation - Our defenses

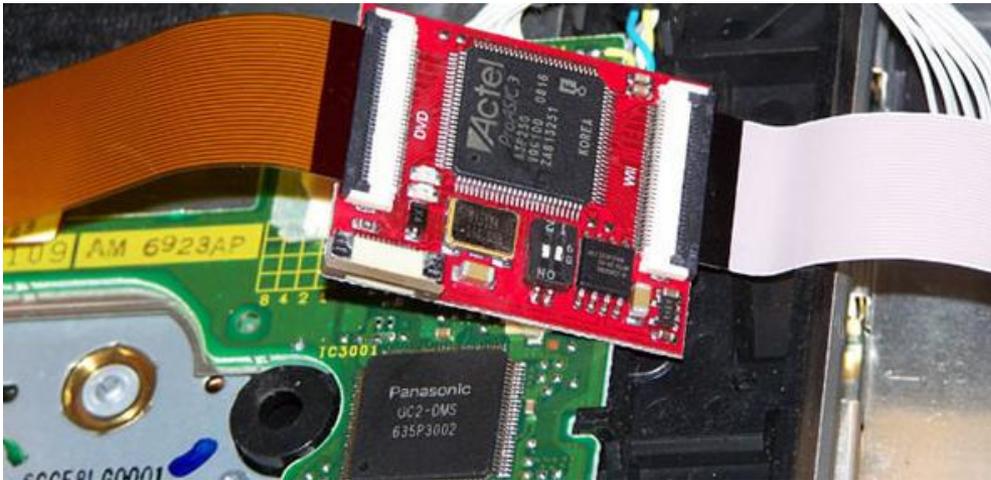
- Manufacturers : When designing a new device
- Service, Security companies : Measurements in Software or Policies
- Users : embedded device users

# 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, these illegal software are being freely distributed via P2P, torrents, web storage, and are easily accessible

The screenshot shows the Torrentz search results for the query 'wii'. The page includes a search bar with 'wii' entered, a 'Search' button, and a list of sponsored links. Below that, it shows search results for 'wii' with columns for title, quality, date, size, and peers. The results list various game titles like 'Super Mario Galaxy 2 PAL Wii' and 'Wii Monster Hunter Tri PAL rar'.

Quality	Downloads	Speed
[FullVersion]	12901	1775 kb/s
[Full Download]	4751	2431 kb/s
[HIGHSPEED]	5678	2312 kb/s
[TRUSTED DOWNLOAD]	7851	1892 kb/s

Title	Quality	Date	Size	Peers
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 Android file browser interface. It features a top navigation bar with 'Uninstalled' and 'Installed' tabs. Below the navigation bar, there is a list of applications, each with a title, a 'Not Installed' status, and a star rating. The applications listed include 'Lunar Lander', 'OI Countdown', 'OI Flashlight', 'Snake', and 'Sudoku'.

# The current state of malware on embedded devices

# Malware on Gaming Consoles

- Acting like a useful homebrew application, and lures the user to install it
- Acting like an essential bypassing tool or crack, and eventually wrecking the device
- TBD

# Malware on Smartphones

- Worm that targets jailbroken iphones using a default password
- TBD

# The mindset of the general public

# Users not concerned about malware on embedded devices

- Users feeling safe by not using apps that look 'fishy'
- Most of those people do not even give a second thought before installing the downloaded software, and merely just check that the application works

## However...

- These devices are capable of bringing the same negative effects of PC malware, and the boundary of these devices and a 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 for malware to survive and perform it's task is provided.

The attacker's point of view

# Gaming console acting like a computer

# 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

- 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

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

# Malware injection on existing games

# 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 wii malware injection

```
00000000 0000 0100 0000 2560 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 3940 4800 3800 6600 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000080 8027 61E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0015 F540 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000000C0 0003 3140 0000 07E0 0000 00C0 0000 0000 0000 0000 0000 0000 0000 0000 000D 3E30 8000 403C 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000100 3C60 8000 0003 30E4 7000 0EEF 2C00 0EEF 4C82 0020 3840 0000 3880 0000 38A0 0000 4803 1E74 4E80 0020 3800 0001 980D 8940 4E80 0020 886D 8940 4E80 0020 4800 016D
00000140 4800 02A1 3800 FFF8 9421 FFF8 9001 0004 9001 0000 4800 01E5 3800 0000 38C0 8000 38C6 0044 9006 0000 3C00 8000 38C6 00F4 80C6 0000 2806 0000 4182 000C 80E6 000C
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
000001C0 4082 0020 38A0 0002 4BFF FF61 4800 0014 3C00 800A 38C6 5530 70C8 03A6 4E80 0021 3C00 8000 38C6 00F4 80A6 0000 2805 0000 41A2 0060 80C5 0008 2806 0000 41A2 0054
00000200 70C5 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
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
00000280 4BFF FE81 4BFF FEB1 2803 0001 4082 0008 480A 1439 4803 58CD 7DC3 7378 7DE4 7878 4800 2E15 4803 5924 3800 0000 3860 0000 3880 0000 39A0 0000 38C0 0000 38E0 0000
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
00000300 3B20 0000 3B40 0000 3B60 0000 3B80 0000 3BA0 0000 3BC0 0000 3BE0 0000 3C00 8028 6021 6DB0 3C40 8027 61AD D200 4E80 0020 9421 FFE0 7C08 02A6
00000340 9001 0024 93E1 001C 93C1 0018 93A1 0014 3FA0 8000 3BED 63A0 83DD 0008 2C1E 0000 4182 0038 809D 0000 83FD 0004 4182 0024 7C1F 2040 4182 001C 7FE3 FB78 7FC5 F378
00000380 4000 1FED 7FE3 FB78 7FC4 F378 4800 0079 3BED 000C 4BFF FFC4 3FA0 8000 3BED 6424 80BD 0004 2C05 0000 4182 001C 807D 0000 4182 000C 3880 0000 4800 20B9 3BED 0008
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 9C2C 8A95 4802 B2E5 7FE8 03A6
00000400 4E80 0020 3CA0 FFF8 60A5 FFF1 7CA5 1838 7C65 1850 7C84 1A14 7C00 286C 7C00 04AC 7C00 2FAC 30A5 0000 3484 FFF8 4080 FFEC 4C00 012C 4E80 0020 4D65 7472 6F77 6572
00000440 6B73 2054 6172 6765 7420 5265 7369 6465 6E74 2048 6572 6E65 6C20 66F6 7220 506F 7765 7250 4300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
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
```

```
00000000 0000 0100 0000 2560 001A 0C20 0000 0000 0000 0000 0000 0000 0000 0016 1AA0 0016 1B80 0016 1C40 0016 1C80 0016 1CA0 0016 C740 0019 F880 001A 0060 001B 5220
00000040 0000 0000 0000 0000 8000 0000 8000 6600 8027 50E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000080 8027 61E0 807A 5EAD 0000 0000 0000 0000 0000 2460 0015 F540 000D 46E0 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
000000C0 0003 3140 0000 07E0 0000 00C0 0000 0000 0000 0000 0000 0000 0000 0000 000D 3E30 8000 403C 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
00000100 3C60 8000 0003 30E4 7000 0EEF 2C00 0EEF 4C82 0020 3840 0000 3880 0000 38A0 0000 4803 1E74 4E80 0020 3800 0001 980D 8940 4E80 0020 886D 8940 4E80 0020 4800 016D
00000140 4800 02A1 3800 FFF8 9421 FFF8 9001 0004 9001 0000 4800 01E5 3800 0000 38C0 8000 38C6 0044 9006 0000 3C00 8000 38C6 00F4 80C6 0000 2806 0000 4182 000C 80E6 000C
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
000001C0 4082 0020 38A0 0002 4BFF FF61 4800 0014 3C00 800A 38C6 5530 70C8 03A6 4E80 0021 3C00 8000 38C6 00F4 80A6 0000 2805 0000 41A2 0060 80C5 0008 2806 0000 41A2 0054
00000200 70C5 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
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
00000280 4BFF FE81 4BFF FEB1 2803 0001 4082 0008 480A 1439 4803 58CD 7DC3 7378 7DE4 7878 4800 2E15 4803 5924 3800 0000 3860 0000 3880 0000 39A0 0000 38C0 0000 38E0 0000
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
00000300 3B20 0000 3B40 0000 3B60 0000 3B80 0000 3BA0 0000 3BC0 0000 3BE0 0000 3C00 8028 6021 6DB0 3C40 8027 61AD D200 4E80 0020 9421 FFE0 7C08 02A6
00000340 9001 0024 93E1 001C 93C1 0018 93A1 0014 3FA0 8000 3BED 63A0 83DD 0008 2C1E 0000 4182 0038 809D 0000 83FD 0004 4182 0024 7C1F 2040 4182 001C 7FE3 FB78 7FC5 F378
00000380 4800 1FED 7FE3 FB78 7FC4 F378 4800 0079 3BED 000C 4BFF FFC4 3FA0 8000 3BED 6424 80BD 0004 2C05 0000 4182 001C 807D 0000 4182 000C 3880 0000 4800 20B9 3BED 0008
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 9C2C 8A95 4802 B2E5 7FE8 03A6
00000400 4E80 0020 3CA0 FFF8 60A5 FFF1 7CA5 1838 7C65 1850 7C84 1A14 7C00 286C 7C00 04AC 7C00 2FAC 30A5 0000 3484 FFF8 4080 FFEC 4C00 012C 4E80 0020 4D65 7472 6F77 6572
00000440 6B73 2054 6172 6765 7420 5265 7369 6465 6E74 2048 6572 6E65 6C20 66F6 7220 506F 7765 7250 4300 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
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
```

# Malware on Wii

- Modifying the game files and injecting custom code
- Demo : Malware(**network down**) in live action while the game is playing

# Malware on Wii

- Modifying the game files and injecting custom code
- Demo : Malware(**attack remote host**) in live action while the game is playing

# Malware on Wii

- Modifying the game files and injecting custom code
- Demo : Malware(attack ap & dns pharming) in live action while the game is playing

# Malware injected into Smartphone applications

# Malware on Smartphones

- Injecting malware on Android applications
- Demo : POC of code injection on an existing application

# Malware on Smartphones

- Injecting malware on iPhone applications
- Demo : POC of code injection on an existing application

# Preparation - Our defenses

## When designing a new device

- How to prevent embedded devices from attacking other hosts
- How to prevent attacks coming from embedded devices

## Measurements in Software or Policies

- How to detect malicious software for embedded devices and prevent the propagation of malware
- How to effectively verify the integrity of a large number of applications

## embedded device users

- How to safely use an embedded device
- How to protect yourself from potential attacks

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

# References

- Google  
<http://google.com/>
- WiiBrew  
[http://wiibrew.org/wiki/Main\\_Page](http://wiibrew.org/wiki/Main_Page)
- devkitPro.org  
<http://www.devkitpro.org/>
- kkamagui 프로그래밍 세상  
<http://kkamagui.tistory.com/>
- POC  
<http://www.powerofcommunity.net/>