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

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 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 acting like computers - Hacking with NDS
- Malware injection on existing games - Malware on Wii
- Malware injected into Smartphone applications - Malware on Smartphones

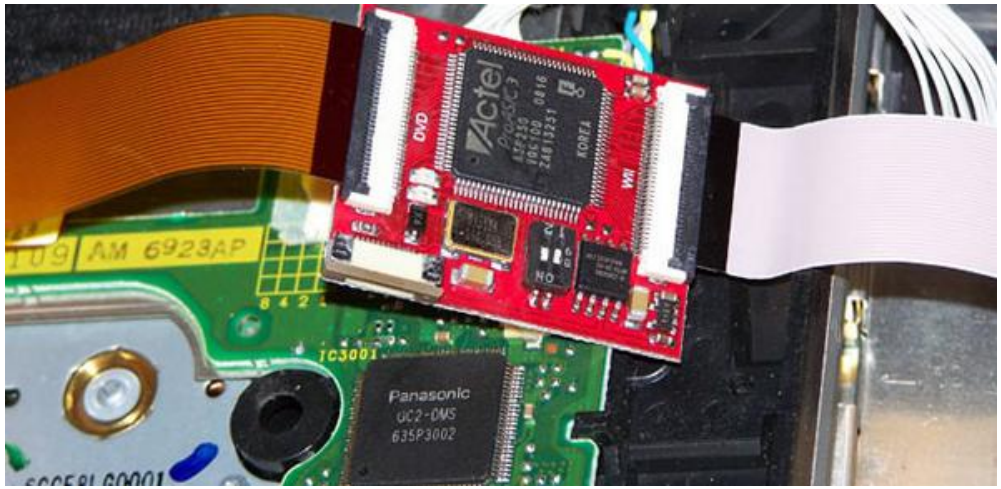
Preparation - Our defenses
- Manufacturers : When designing a new device
- Service, Security companies : Measurements in Software or Policies
- Users : embedded device users

Background Knowledge

The pirate scene of Gamine consoles and Smartphones

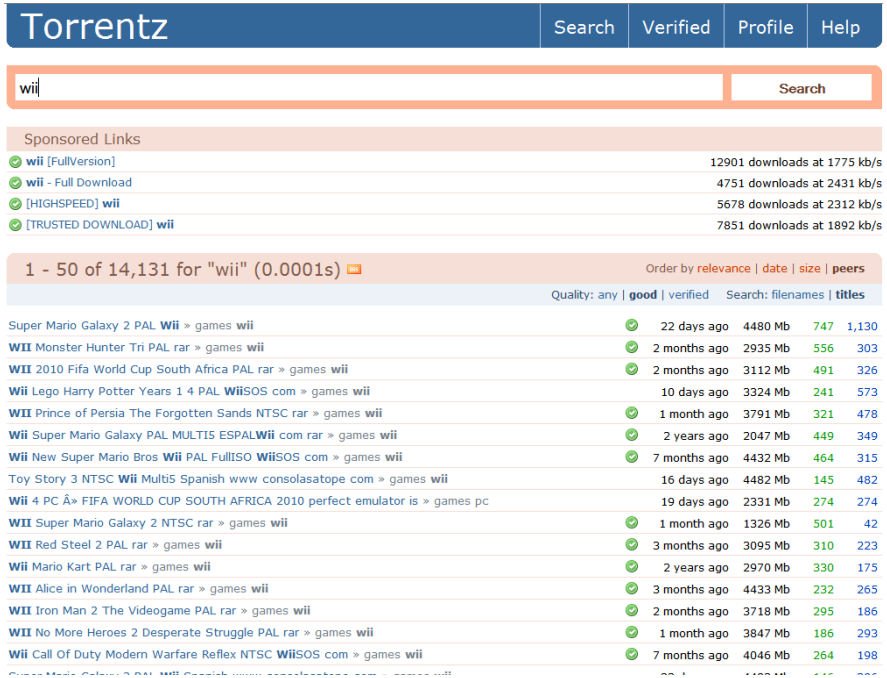
Payed software being illegally downloaded

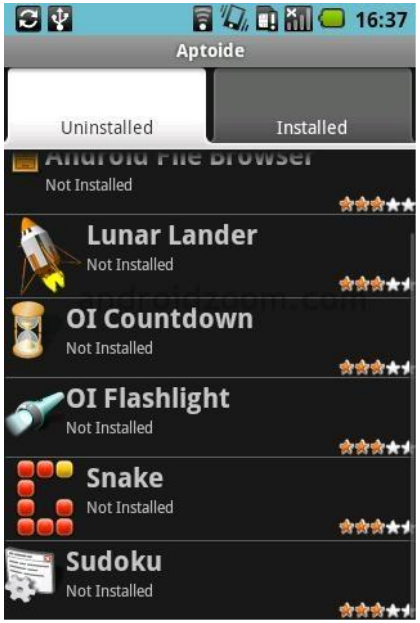
- Most embedded devices implement anti pirate Measures by some means, but these protections are eventually bypassed



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 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 boundry 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

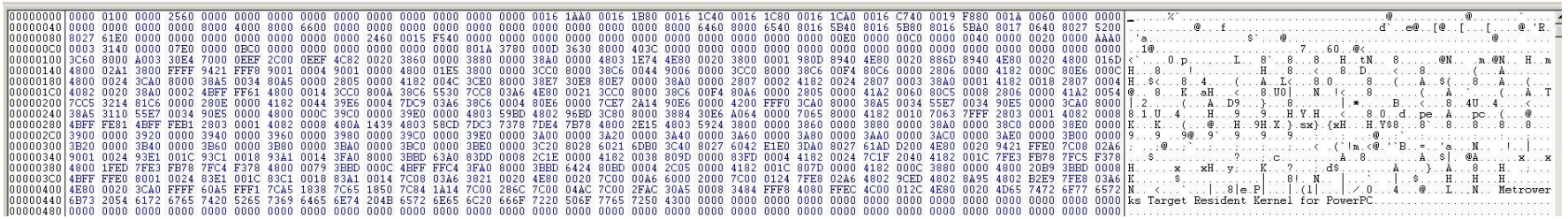
How custom code can be injected

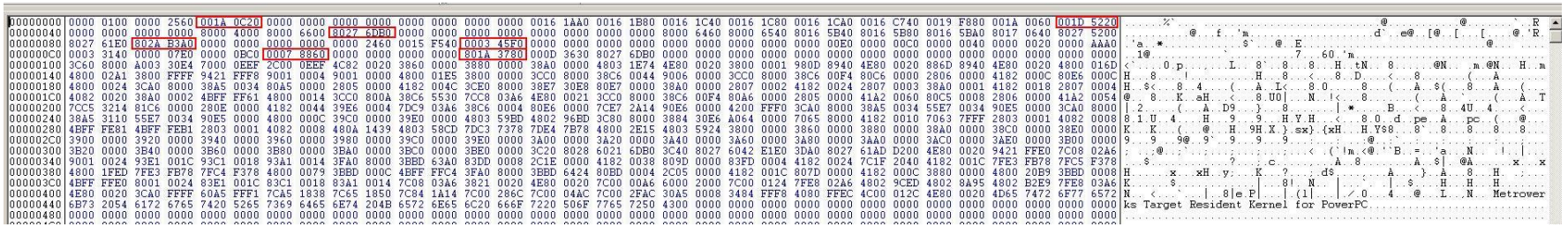
- Merge 2 dol files
- Update header information
- Inject code that transfers execution to the game .dol after the execution of the injected .dol
- Fix a few problematic parts in the binary

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





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

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

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

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