gc-forever - Gamecube/Wii Forums

Gamecube/Wii support & news forums
https://www.gc-forever.com/forums/

Open source Drivechip

https://www.gc-forever.com/forums/viewtopic.php?f=36&t=403

Re: Open source Drivechip

by **liquitt** Posted: **Tue Feb 15, 2011 10:14 pm**

interesting that this pops up 5 years after the release and while everybody is talking about it.

come on - who's the author 😛

Re: Open source Drivechip

by **emu_kidid** Posted: **Tue Feb 15, 2011 10:20 pm**

Haven't seen the author around for a while ☹

Re: Open source Drivechip

by **MrSporty** Posted: **Wed Feb 16, 2011 7:57 am**

Never been told but i always assumed the author was a user called Cheqmate. I remember chatting on IRC to him back in the day and he was very knowledgable about the inner workings of the GC (and Wii) drivecodes.

Re: Open source Drivechip

by **andzlay** Posted: **Wed Feb 16, 2011 8:24 am**

But really interesting posting... I got a Xeno 2.0 back in 2009 or more likely 2010 (not sure) from discoAzul (spanish shop).

Re: Open source Drivechip

by **MrSporty** Posted: **Wed Feb 16, 2011 11:13 am**

Quick dissasembly of the last 8 command long block.

```
0x008674:	F474 740A08	MOV	$080A74,A0
0x008679:	F720 4C80		MOV	A0,($804C)
0x00867D:	F474 00D040	MOV	$40D000,A0
0x008682:	F000			JMP	(A0)
```

First two commands look to restore some sort of pointer within the drivecode. The last two obviosuly launch our main payload.

Re: Open source Drivechip

by **emu_kidid** Posted: **Wed Feb 16, 2011 12:05 pm**

😁 nice work MrSporty. Yes, cheqmate, aka cheq, aka adhs.

Re: Open source Drivechip

by **MrSporty** Posted: **Wed Feb 16, 2011 1:17 pm**

Ahh it makes more sense now. Its kinda like a springboard into launching our drivecode payload.

We upload a main block to 0x40D000, then a small "cleanup" routine to 0x008674 and then our final command overwrites what i assume to be an IRQ pointer.

The re-directed IRQ returns to our cleanup routine which restores the original IRQ pointer value and then jumps to our main payload.

Neat. Now to dissasemble the main payload

Re: Open source Drivechip

by **MrSporty** Posted: **Wed Feb 16, 2011 7:05 pm**

Yay, even more progress. Im currently spending a bit of time picking apart the main initial payload. As far as i can tell it basically repurposes the debug port to enable a much higher transmission speed. I also grabbed a more detailed pic of the transition between the regular debug commands and the faster xeno data.

tinypic
This image is no longer available.
Visit tinypic.com for more information.

Pictured in this image you can see the speed of the clock (top most line) change from the debug speed of about 130us per bit to about 9us.

After having upped my L.A's sample rate, i was able to get a nice clear picture of the data. You can see that its still SPI data but at a much faster rate. 😐

Re: Open source Drivechip

by **MrSporty** Posted: **Thu Feb 17, 2011 9:17 pm**

Phew, well after a short while sampling, chopping and coverting i now have the 2109 bytes of the main Xeno payload, Woot !

With a cursory glance it does look like valid drivecode but as i have yet to fully dissasemble the "high speed loader" i have no idea where in memory it is loaded or in how many parts.

It does look valid though. In the high speed loader there is this section of code:

```
F4C000D140              MOV     ($40D100),D0
F7484444                CMP     $4444,D0
```

And in the main payload there is a string of bytes "4444F44000D140" Basically this is using the value 0x4444 at location $40D100 as a signature of data been written.

Im going to spend a bit of time knocking together a basic skeleton of code for an AVR and see what comes of sending just the data i have so far.

Then i will look at the start button functions.

Will keep you posted

Re: Open source Drivechip

by **KirovAir** Posted: **Thu Feb 17, 2011 9:31 pm**

Great progress!
Very interesting reads here, following this daily. 😀

Re: Open source Drivechip

by **emu_kidid** Posted: **Thu Feb 17, 2011 10:00 pm**

MrSporty, nice 😀

Put some LED's on the AVR 😉

Re: Open source Drivechip

by **MrSporty** Posted: **Thu Feb 17, 2011 10:12 pm**

Lol,i could make it look like kitt from knightrider but it wouldn't make it any more funtional 😛

What was catching my interest is the credits payload that it can run via the start button. At first i thought it might be a way of loading swiss but as you mention, it patches the apploader which i assume only runs after a disk has booted.. so no real point cos if you can boot a disk , you can boot a disk with swiss on it.

Must a be a small file that credit payload. The high speed loader and final payload take up about 2.6k. With the SPI code it doesn't leave much more than about 5k on a standard Atmega8.

Re: Open source Drivechip

by **emu_kidid** Posted: **Thu Feb 17, 2011 10:31 pm**

MrSporty, yes, it's incredibly small but in essence you can implement a DOL loader if you fake a few reads more 😉

You basically would need to fake the disc authentication to make the cube think a disc is inserted, then fake the disc read id, the region check (0x45b? - I'd need to log what the ipl actually reads first to confirm since it's been too long) and just a part of the apploader.

The apploader as you probably know is executed by the ipl, it blindly calls it without validating that it's actually an apploaoder, so we could just write a piece of code that loads homebrew instead 😀

Re: Open source Drivechip

by **MrSporty** Posted: **Sat Feb 19, 2011 12:23 pm**

Just in case anyone is interested, here are the 2 main payloads for the Xeno1

Payload1 is the smaller high speed loader and associated commands.

Payload2 is the main piece of drive code loaded in the second instance

Re: Open source Drivechip

by **bearteam** Posted: **Sat Feb 19, 2011 1:24 pm**

I hope someone could continue this work and make it into a super GAMECUBE modchip like wiikey fusion which supports reading ISO directly from SD card 😀

Re: Open source Drivechip

by **MrSporty** Posted: **Sat Feb 19, 2011 1:27 pm**

Not that its the final goal of this partiular project but if enough people contribute with any information they can, anything should be possible.

Re: Open source Drivechip

by **stuntpenguin007** Posted: **Tue Mar 22, 2011 9:47 pm**

I realize this is a month old bump, but I'm planning on building a gamecube drivechip based off of an arduino, and this thread looks like the exact same thing I'm trying to do. I'm new to embedded programming, so so some of my questions might be noobish.

I was reading through tmbinc's wiki: http://tmb.elitedvb.net/dvd-game/index. ... l_Commands and it says that a bit is read from SBI3 when SBT3 goes high. SBI3 being pin 4 and SBT3 being pin 2 of the debug connector. From what I can tell, SBT3 is always high. I think it's part of the 5V rail, because when I pull it high (don't worry, the GC was turned off 😳), the power LED lights up.

After skimming this thread I saw that you said the debug connector uses SPI. This means there is a clock signal right? Would you mind giving me a pinout of the CN302 in terms of SPI?

Re: Open source Drivechip

by **MrSporty** Posted: **Sat Mar 26, 2011 11:00 pm**

Only reason i stopped this project is that the original source was released. Grab that and work out the pinout and all will be revealed.

Re: Open source Drivechip

by **Dragoon** Posted: **Sun Mar 27, 2011 11:21 am**

litle problem, you can't compile :s

Re: Open source Drivechip

by **skygames** Posted: **Sat May 07, 2011 8:22 pm**

😁 Hello my friends thanks, wiikey is working on my gamecube, thanks to everyone who helped me without even knowing it, without it this topic would not be possible, I would still be trying to find a modchip fo my beloved cube.Image

Re: Open source Drivechip

by **Hugo_Peters** Posted: **Sat May 14, 2011 5:22 pm**

> ***skygames wrote:***
> 😁 Hello my friends thanks, wiikey is working on my gamecube, thanks to everyone who helped me without even knowing it, without it this topic would not be possible, I would still be trying to find a modchip fo my beloved cube.

Er, well I'm very happy for you, but you probably posted this into the wrong section.
Emu, what do you think?

Re: Open source Drivechip

by **liquitt** Posted: **Sat May 14, 2011 5:45 pm**

> ***Hugo_Peters wrote:***
>
> > ***skygames wrote:***
> > 😁 Hello my friends thanks, wiikey is working on my gamecube, thanks to everyone who helped me without even knowing it, without it this topic would not be possible, I would still be trying to find a modchip fo my beloved cube.
>
> Er, well I'm very happy for you, but you probably posted this into the wrong section.
> Emu, what do you think?

what do you mean?

Re: Open source Drivechip

by **Hugo_Peters** Posted: **Sun May 15, 2011 6:47 pm**

> ***liquitt wrote:***
>
> > ***Hugo_Peters wrote:***
> >
> > > ***skygames wrote:***
> > > 😁 Hello my friends thanks, wiikey is working on my gamecube, thanks to everyone who helped me without even knowing it, without it this topic would not be possible, I would still be trying to find a modchip fo my beloved cube.
> >
> > Er, well I'm very happy for you, but you probably posted this into the wrong section.
> > Emu, what do you think?
>
> what do you mean?

I mean, what does Emu thinks of this misplaced post?

Re: Open source Drivechip

by **liquitt** Posted: **Sun May 15, 2011 7:07 pm**

is it misplaced? thought he reflashed his wiikey somehow 😁

Re: Open source Drivechip

by **KirovAir** Posted: **Mon May 16, 2011 6:48 am**

> ***skygames wrote:***
> 😁 Hello my friends thanks, wiikey is working on my gamecube, thanks to everyone who helped me without even knowing it, without it this topic would not be possible, I would still be trying to find a modchip fo my beloved cube.Image

Nice job!
Also very handy, as there is a huge amount of Wiikeys compared to Xeno's. 😁