EXHIBIT O

DECLARATION OF RYAN BRICKER IN SUPPORT OF *EX PARTE* MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INUNCTION; ORDER OF IMPOUNDMENT

DEV-TEAM BLOG

To find yourself, think for yourself © Socrates 469 BC

[   ] [Search]

redsn0w+limera1n fun

It looks like geohot's recent limera1n exploit for iPhone3GS/iPhone4/iPad/ipt3g/ipt4g/atv2g will be very beneficial to jailbreakers and unlockers for the next few months (at least). geohot's limera1n program and the alternative greenpois1on program both use his same exploit (although greenpois0n refuses to tell you that, FWIW), and hopefully SHAtter can be saved for some later device.

In the meantime, we've also incorporated the limera1n exploit into redsn0w. But we've added a few extras:

- custom bootlogos for iPhone3G/iPhone3GS/iPod2G users (with qualifying bootroms)
- an option that implements the "DFU" button in PwnageTool. This button (which you can use from Windows) lets you prepare your device for a custom DFU. Even if you're purely a Windows user, you can get a trusted friend to run PwnageTool over your IPSW to create a custom IPSW. You can now install that custom IPSW on your own Windows box, after you run this redsn0w version.

This latest redsn0w is available at:

- ~~OS X~~ (See our latest redsn0w post)
- ~~Windows~~ (See our latest redsn0w post)

For Windows users who have run redsn0w and chosen "Just enter pwned DFU mode right now", your device is now completely vulnerable. Running iTunes and selecting a custom IPSW from PwnageTool (choose it by pressing Shift+Restore)….you've now convinced your device and iTunes to restore to a custom firmware. Congratulations!

If you are timid about software and running these programs…please just wait! Don't jeopardize your carrier unlock for a firmware upgrade. Wait for even easier methods than this latest redsn0w release.

Update #1: Today Apple released to developers the GM seed for 4.2. Tinkerers will find that yesterday's redsn0w jailbreaks today's 4.2 GM seed, simply by pointing redsn0w at the 4.1 IPSW (rather than the 4.2 one). **Right now it mostly only makes sense for JB app developers to do that** because many apps (including Cydia itself) need to be updated for 4.2. However, if all you want to do is enable afc2 (to use iFunBox or other file browsers), or to tweak settings like Battery % and Homescreen wallpapers, then go for it (if you have valid paid access to the GM seed). Be sure to uncheck the Cydia box, though! **Ultrasn0w unlockers should stay very far away from this!!**

Update #2: By all accounts, we're within a few days of Apple's official public release of Firmware 4.2. Here's what you need to know:

- Thanks to geohot's limera1n exploit, and our original pwnage2 exploit, and @pod2g's ipod2g-MC exploit, absolutely **all** devices at **all** iOS firmware versions are capable of being jailbroken.
- The *untethered* jailbreak of those very latest FWs and latest devices depends on @comex hacks. His hacks so far extend only to 4.1 and 4.2beta3. He's working on a way to extend it to 4.2 and beyond. Just wait for him to work out his method.
- iPhone 3G and 3GS unlockers **will** be covered by our upcoming unlock. Stay away from any updates to Apple FW until our official release and you'll be okay. Just stay away from all Apple IPSWs :)
- iPhone4 unlockers are not left out in the cold. @sherif_hashim has found some very promising avenues to pursue. Those will be explored as soon as possible after all the 4.2 madness.

What does this mean to you?

- If you're an unlocker, just stay where you are. **Please, just stay where you are.** Any mistakes you make now may be permanent.
- If you only care about the jailbreak and you're absolutely sure you have your personalized 4.1 SHSH hashes, feel free to experiment but keep in mind that any mistakes you make may result in your losing pictures or notes or bookmarks that you'd rather keep. Honestly unless you love living on the bleeding edge, it's better to just wait for official updates from Cydia/redsn0w/PwnageTool.
- **Don't buy or donate to any unlock or jailbreak scammers**. Every legitimate solution you will find for unlocks or jailbreaks will be offered without an extended hand. **That's how the iPhone jailbreak/unlock community has succeeded. It's about freedom to do what you want with your $300 device — not about donations, egos, tweets, or "interviews."**

Update #3: *(Warning: if you use the ultrasn0w unlock, please read no further…this doesn't apply to you yet!)* We've made some updates to redsn0w to make it easier for jailbreak developers (and tinkerers) to get their programs ready for 4.2.1. As noted above, the public version of Cydia (and MobileSubstrate too!) is not 4.2.1-compatible. redsn0w will now let you install your own custom bundles independent of Cydia (the bundle can actually **be** Cydia if you've compiled it on your own). These bundles can be up to 15MB in size, and should be in the form of a gzip-compressed tar file.

The new redsn0w 0.9.6b3 is available at:

- ~~OS X~~ (See <u>our latest redsn0w post</u>)
- ~~Windows~~ (See <u>our latest redsn0w post</u>)

It's very important that you get the file permissions and ownerships right in your custom redsn0w bundles. To give you a practical example of such a bundle, here's one that includes OpenSSH, OpenSSL, and the basic apt installer programs:

- <u>SSH bundle v2</u> *(update: v2 has fixed permissions..you can just drop this one right in even if you installed the first version)*

redsn0w has also been updated to recognize the 4.2.1GM IPSWs. *However*, as noted above, the 4.2.x jailbreak is not yet untethered for most devices! **That means until someone like @comex comes up with a way to untether it, you must use redsn0w (or a similar utility) to boot your device into a jailbroken 4.2.1 state.** (The only exceptions to this are the iPhone3G, non-MC iPod touch 2G, and old-bootrom iPhone3GS. redsn0w will jailbreak those untethered!)

With the above redsn0w and SSH bundle, jailbreak developers and tinkerers can jailbreak and SSH into their 4.2.1 devices, provided they've done a tethered boot (using redsn0w's "Just boot tethered right now" option).

Note: The Cydia that's included in 0.9.6b3 is the same one as in 0.9.6b2, and so it will *not* work on 4.2.1. **Don't try installing it on 4.2.1! Instead, use the SSH bundle, or compile Cydia on your own.** If you're familiar with the apt utilities, you can use "apt-get" to install many programs from the command line. Be sure to do "apt-get update" first to refresh your sources!

PLEASE CONSIDER THIS AN ADVANCED TOPIC!! It's not meant for the masses because it involves rather nerdy things like command lines and tar files. But for those who know how to use this new redsn0w feature, have fun!

Comments (10,327)

Sort by: <u>Date</u>   <u>Rating</u>   **Last Activity**

<u>Login</u> or <u>signup</u> now to comment.

<u>Aswadiyya</u> 1p · *24 minutes ago*   +1

I have the iphone 3gs 16gb with 4.1 and baseband 05.14 (using a mac -but have access to PC(xp)). I would like to unlock since I am on Tmobile. I am a bit confused about the current status/instructions.

None of the shsh are saved (bought it 2nd hand). Is my only route to use the ipad baseband to unlock. I don't necessarily need/want 4.2.1 just need to unlock. I'm hesitant to use ipad bb since phone is still under warranty til 03/11.
Please advise. thx

Reply   Report

AEDan1977 2p · *59 minutes ago*   +1

Hey Guys

I just did a full restore of my iPhone 4 from 4.1 to 4.2.1 so I could try the new untethered jailbreak. All my SHSH blobs are on Cydia and I have them backed up on my computer.

I am having a issue. I can do a tethered jailbreak just fine but whenever I try to do the "Jailbreak Monte" for an untethered JB I choose the 4.2b3 firmware file. It goes ahead and starts the process and once it gets to Decrypting main filesystem, it does it for like 10-15 seconds or so then redsn0w just crashes and closes out.

I have no other applications open and it does this both on this Mac and it does the same exact thing on my hackintosh mac as well. I'm not sure what is going on.

Any ideas?

- Dan

Reply   Report

Ric38 2p · *23 hours ago*   +1

I have a 3GS with the old bootrom 359.3 and BB 04.26.08. It is jail broken @ 4.0 with Pwnage. Can I or can I not JB to 4.2 or 4.2.1? I don't need to unlock, just jailbreak unteathered. Thanks in advance!

Reply   **2 replies** · *active 4 hours ago*   Report

demitator 3p · *7 hours ago*   +1

hope to watch dev team kikin apple ass n release jail n unlock for iphone 3g 4.2 ASAP

Reply   Report

Rajan_toms 9p · *5 days ago*   0

Hi All,

I have a Iphone 3g 8gb version 3.0 (7A341) MODEM FIRMWARE 4.26.08 already jailbreaked

I want to update to latest firmware

can u plz help me with steps how to jailbreak. (windows)

thanks in advance
tom

Reply   **9 replies** · *active 8 hours ago*   Report

gametheory 44p · *9 hours ago*   +1

Can anyone confirm dtac Thailand simcard works on iPhone 4 unlocked with ultrasn0w? Thanks

Reply   Report

uji 16p · *2 days ago*   +3

Happy New Year People of the Dev Team,

Right I have finally activated my Iphone 4, my Ios is 4.2.1 and my baseband is 3.10.01

Does that mean wait? or can something be done to JB and unlock the phone?

Thanks Guys and girls

Reply   **4 replies** · *active 12 hours ago*   Report

harry_01 29p · *1 day ago*   +1

iphone 4 4.1 bb 01.59.00 DFU mode black screen when i connect cable phone to pc itunes show restore your phone

and i use redsn0w 09.6rc8

Just boot tethered right now

my phone work now but when phone switch off or restart again come DFU mode any solution

Reply   **1 reply** · *active 13 hours ago*   Report

jishijet 17p · *21 hours ago*   +1

I have an iphone 4 running on 4.1 and 01.59.00. How do I update to 4.2.1 and jailbreak/unlock it please?

Cheers
J

Reply   Report

danilo101 4p · *3 days ago*   +1

I have a 3G, 4.1 and 5.14 bandwith. My iphone was unlock before until i stupidly upgraded to 4.1 and now it locked itself. I need help on how to unlock this phone again. thanks

Reply   **6 replies** · *active 21 hours ago*   Report

tatomero 1p · *3 weeks ago*   +2

this is the second time i post this comment if u didnt see it but still no reply just tell me plz is it hardware or software my post was as this :
plz i need urgent help , although i have seen the warning about 4.2.1 and 6.15 baseband .i already updated to it , unlocked and everything worked well till my stupidity made me restore my network settings coz i got a safe mode instead my clock , after that i am stuck with itunes error 1015 i tried

every way you mentioned recboot,irecovery.ireb , resdn b6. nothing can get me out of it , thats all coz i made the update of ipad baseband i know . but how can i get rid of this error continue using my iphone ?????????/

Reply   **1 reply** · *active 22 hours ago*   Report

---

tmoiphone 18p · *22 hours ago*   +1

I was restoring my 3g that had been jailbroken and unlocked using redsnow_win_0.9.6rc8 on a pc running the 32bit version of windows which updated my iphone to the ipad baseband 06.15.00 when itunes gave me the message "error code 1015". I have tinyumbrella with all SHSH blobs going back to 4.0.1 and was following the a procedure I found online to restore using tinyumbrella. The phone is currently stuck in the itunes restore screen (with the picture of the USB cable) an I have tried using redsnow, recboot, and limerain to kick it out of recovery mode all without any luck. I would try using tinyumbrella's dedicated "exit recovery" button but it is grayed out and therefore can not be clicked on. Please can anyone help? I should mention that my live in girlfriend is a Smartphone programmer and can help me with the fix if it is over my head, provided she had some instructions. Thanks for your time in advance everybody!

Reply   Report

---

gametheory 44p · *1 day ago*   +1

I guys thanks in advance. iPhone 4 4.0.1 jb unlocked with old ultrasn0w, my question is I'm trying to use a DTAC sim in Thailand, I cut it but is not working, is says no service, my tmobile works just fine, please help

Reply   **1 reply** · *active 1 day ago*   Report

---

mexicocrab 1p · *3 days ago*   0

hi! I just got my 3gs with new bootrom jailbroken by redsn0w 0.9.6rc8 to firmware 06.15.00 successfully. Now i try to unlock it using Cydia. It keeps telling me no internet connection. I do not have SIM card in the phone but do have wi-fi connected. The Safari is not working either. Do I have to have a AT&T SIM card to get this done? The phone was activated by an ATT SIM card before. Thanks,

Reply   **2 replies** · *active 1 day ago*   Report

---

myiphone2011 2p · *1 day ago*   +2

I hav iphone 3g 3.1.3 which i upgraded to4.2.1 but now it says no sim card installed only emergency calls. I dont have access to ATT sim. I tried to JB and unlock via Redsnow but it gets stuck at reboot. Thanks

Reply   **1 reply** · *active 1 day ago*   Report

Jerry4mguam 23p · *1 day ago*   +1

hi is the untethered jailbreak for 3gs i0s 4.2 out yet? and is the unlock for iphone 4g i0s 4.2 baseband 03.10 out yet also? thanks in advance!

Reply   Report

Mouxy 19p · *1 day ago*   +2

HI Guys!

I'have an I4 and after jailbreak 4.2.1 and restoring it with pgkbackup the phone takes about 8minutes to boot! (with 0.9.6 the phone boots, the pinaple logo shows up and after 5 mnts the phone restars with apple logo, i have to boot tethered again and more 4/5 minutes the phone finaly shows lockscreen) (with 0.9.7b3/4 it's the same thing besides the boot tethered). I've already tried to restore only the apps without defenition lines...

Tks

Reply   Report

Jerrysiphone 2p · *2 days ago*   +3

I think it is awesome what the Iphone Dev Team is doing. Thanks guys!!

I am wanting to Jailbreak and Unlock my Iphone 3g(not s) currently on OS 4.2.1 Modemfirm 5.15.04. I am wanting to JB and Unlock for use on Tmobile. I am confused on which software to use. Some versions say don't on 4.2.1. Some say it's tethered on 4.2.1 while some say it's ok on 4.2.1 and is untethered since it's a 3g(not s). I understand the warning about GPS but would rather have it if possible. I have access to both MAc and Windows....Can anyone make a recommedation of a which version of software to use?

Also, I see the mention of have the current ISPW in the PWNAGE files for both firmware and baseband update. WHere do we get that from?

Thank you in advance :)

Reply   Report

hkl 34p · *3 days ago*   +1

I have iPhone 4, 4.0.1, jailbreakme, ultrasnow 1.2, originally AT&T. When I am using a SIM card different than AT&T then the phone often does not get registered (displays only 1 bar and no operator name). When I switch flight mode on and off I get a message 'Invalid SIM Card'. The only workaround I found is to keep switching the phone off and on until it gets registered. Right now my success rate is 30%. Meaning 30% of the time the phone registers properly. Anyone experienced the same problem? Better work around?

Reply   Report

sazz 1p · *3 days ago*   +2

Hi Dev-Team, I need HELP!!!

I have a 4.1 iPhone 4, I jailbroke it and installed ultrasn0w (I wasn't aware that 2.10.04 was still unhackable) and now I don't have signal even with the original SIM card. I tried uninstalling ultrasn0w and rebooting but still no signal, is there anything I can do besides restoring to fix this?

Reply   Report

Addams2 18p · *1 week ago*   +1

if i had 3.1.2 on my 3gs new boot (JB) and i pushed "make my life easier" in cydia any ideea is gona save shsh for 4.0 .....? how much time gona take ? now i have on my screen "this device has a pending

TSS request " (sorry for my english) ps i`m stupid and i did upgrade to 4.2.1 (custom, i have BB 05.12) and now i have to jb every time i boot my iphone

Reply   **2 replies** · *active 3 days ago*   Report

Ivanfrost 33p · *4 days ago*   +1

Hello Everyone! Real Quick Question: Is there an unteathered unlock and Jailbreak for my Iphone? I want to upgrade the OS to 4.2.1.

I have Iphone 4
os: 4.01(8A306)
bb: 1.59.00

also is there a working source to run Gamecenter on this? I tried all different sources but no luck.

Thanks in advance!!!!

Reply   **2 replies** · *active 3 days ago*   Report

stann219 37p · *2 weeks ago*   +1

Just wondering. I have an iPhone 3G. Should i upgrade to 4.0+ ?
Currently, I have 3.1.3 but it is slow compared to my iTouch.
any suggestions?

Reply   **6 replies** · *active 3 days ago*   Report

Ivanfrost 33p · *4 days ago*   +1

Anyone Know a way to get gamecenter on my Iphone 4
os: 4.01(8A306)???

I tried a few but it seems all the sites are for the 3g... anyway i havent been able to get it working...

Thanks

Reply   **1 reply** · *active 4 days ago*   Report

polski39 8p · *1 week ago*   +4

hey dev team friends :)
first happy new year 2011 to all you hard working people
need help with unlocking my iphone 4 FW:4.1 BB:02.10.04?
is that possible ?
if not do u know when it can be possible ?
thanks so much

Reply   **1 reply** · *active 4 days ago*   Report

Comments by

2 months ago   View Comments (10250)