EXHIBIT N

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

geohot Search

Found 6 results for: geohot

3.1.2 and you?

WARNING! At 10.20AM PDT on October 8th 2009 Apple released the 3.1.2 version (7D11) of the iPhoneOS.

If you care about your jailbreak and unlock, don't update your device - 3G and 3G(S) owners ***should pay particular attention to this warning.***

- PwnageTool and redsn0w **are not yet compatible** with 3.1.2
- There is no estimated release time for compatible tools (*please* don't bug us about this).
- Any information we have regarding this update will be posted here.
- You can also follow us on twitter - @iphone_dev
- @wizdaz has made a very cool DevTeam alert widget for his upcoming app called SmartScreen

Update: geohot released a Windows jailbreak called "blackra1n" which is similar to redsn0w in that it covers multiple devices (and it covers beyond just firmware 3.0.1 where redsn0w currently stops). **blackra1n is not a carrier unlock. You must always avoid updating your baseband to maintain your unlockability. If you use blackra1n to jailbreak 3.1 or 3.1.2, the steps you take before running blackra1n will prevent the unlock from working on your iPhone for potentially a very long time.** By the way, we haven't yet tested whether a blackra1n'd device can accept a custom IPSW without tweaks, but if it doesn't then it should only require a minor change.

1 year ago Comments

FRIENDS

Winter Tires

Short version:

ultrasn0w version 0.9 is out! We believe it solves pretty much all of the various random issues that have been reported. Its features include:

- Works on both 3G and 3GS
- Works on hacktivated devices
- Works regardless of how you jailbroke your device
- Doesn't patch any mach-o binary whatsoever. (Doesn't require a separate patch as each new firmware comes out).
- Doesn't install any additional daemon
- Has no race conditions, no popups about "Missing SIM", no network issues
- Is almost 7000 times smaller than its nearest competition :)
- Is available now via Cydia. Source repo is http://repo666.ultrasn0w.com (that last "0" in ultrasn0w is a zero!)

Long version:

The day before yesterday, some fellow named geohot released a program called "purplesn0w" which claims to be a better unlock than our ultrasn0w unlock released last month, and our yellowsn0w unlock released 7 months ago. He was kind enough to provide source, which we naturally took apart to try to validate his claims. ;)

We've found he had come up with two pretty neat ideas, one more pragmatic than the other for the iPhone. The first is a way of patching the actual text of the baseband code by copying it over to RAM and then using the MMU and page tables to have the baseband pretend it is part of the original bootrom. Of course, like yellowsn0w and ultrasn0w, this code has to be reloaded with every reboot of the baseband. However, the advantage of this is that developing unlocking payloads is a lot simpler… in fact, geohot used the same payload in AnySim and BootNeuter. We kicked around this idea ourselves before, but eventually found a work-around for the same problem with the yellowsn0w/ultrasn0w payload. The two pieces of code have the **exact same effect on the baseband**… with the difference that geohot's exploit overwrites an arbitrary block of memory one megabyte in size. The baseband has a total of eight megabytes of memory and every bit of it is earmarked for use (except for 485212 bytes of it which we haven't accounted for yet, but that's still less than 1 MB). This means that eventually the area of memory geohot is using will be corrupted and 1 MB of baseband code will be corrupted (until the next reboot). How soon will this happen? Will it even matter in day-to-day use? We don't know, because we haven't spent much time looking. However, why take the risk when the yellowsn0w/ultrasn0w payload accomplishes the same job with no corruption?

To put it into perspective, ultrasn0w uses 152 bytes of properly malloc'd baseband RAM, which is 0.015% of what purplesn0w uses. Put another way, purplesn0w uses 6900 times more RAM than ultrasn0w (and doesn't let the O/S know that it's using it, so the O/S still thinks it's free to use. When it does use it, the baseband will crash).

Now, the second new idea he had was to patch CommCenter rather than use a daemon. At first, this idea seemed pretty distasteful to us. Binary patches are messy and difficult to maintain (we figure it's partly why he only made a version for 3G S and not 3G as well). In addition, the stated reason of reduced battery life with a daemon is factually incorrect, since any computer science student who's taken a course in operating systems will tell you that a sleeping task takes up exactly NO CPU resources and NO power (it's merely skipped over during context switches). That's right: not "only a little" power, but absolutely NO power. However, ultrasn0w 0.6 did have a problem where the STK refresh command it used crashed the baseband in 3G S. This caused the baseband to continually come up and then restart. That DOES take power and so may explain the issues that people have been seeing. ultrasn0w 0.8 was supposed to have fixed this issue, but perhaps not completely. This is because the STK refreshes we used are inherently unreliable… but we thought they were necessary to avoid people having to reinsert their SIM. Turns out we were wrong on that score. geohot's method shows that we can perform the unlock before CommCenter polls for lock state. When we do it before (instead of after), the STK refreshs are no longer necessary! The only way to do it before the polling, however, is to modify CommCenter.

We've tried to make the best of a bad situation by using MobileSubstrate to perform the modification. This lets us modify the behavior of CommCenter without touching the actual binary. We also used a method to dynamically locate the patch location so that it should work on both 3G and 3G S (and should need to be updated less frequently). We also do it in a different way so that hactivated phones will work with the unlock (unlike purplesn0w). You'll find that this update is now available through Cydia as ultrasn0w 0.9 We thank geohot for contributing to the scene once again. We don't think purplesn0w is the right path, but it has certainly helped us improve ultrasn0w!

P.S. geohot, seriously, stop dicking around and look at the bootrom instead kthx. =P

1 year ago Comments

iBoot unlaced….

For the ***800 of you*** who wanted a video, here it is.

This is the command line to talk to your iPhone's "BIOS" of sorts. It decides what gets run (if it's signed correctly) or not. Normally it's ***very restrictive***. Unless it's been pwned.

Pwnage breaks the chain of trust from the very earliest boot stage, and as the video shows, this chain has now been broken on the iPhone 3G. Given that the only thing lower than this is ROM, Apple will have to change the hardware to prevent us from getting in, and we don't expect them to ask for your phone back so they can "fix" it.

Please note that this has been anything but trivial, and it wasn't as easy as porting our old code to the 3G iPhone. Many of our best hackers have been working in long shifts all weekend on this, and continue to do so as I write this post, we like to think of these guys as our very own master cobblers.

Note that this is indeed what geohot was talking about when we first talked to it almost a year ago, ironically we (that includes geohot at the time) were unable to do anything with it then. iBoot exists because iTunes needs something to interact with when restoring the phone, but as mentioned above, is normally heavily restricted, only allowing Apple-approved code to run, ***obviously this isn't the case anymore*** ;)

Quoting geohot a year ago:
"IT GIVES YOU A FULL INTERACTIVE SHELL
I REPEAT, A FULL INTERACTIVE SHELL"

P.S: n82ap is the model code for the 3G iPhone.

2 years ago Comments