

Jailbreak entfernen Chimera iOS 13.7

Beitrag von „hackmac004“ vom 22. März 2021, 15:44

Moin,

ich habe vor langer Zeit mal auf meinem iPhone SE 1.Gen einen Chimera jailbreak für ios 13.xx gemacht. Der lief eigentlich nie gut und ich konnte ihn bisher nicht entfernen, da die app die ich dazu auf dem phone hatte immer wieder abgestürzt ist. Mit der App hätte ich ihn entfernen können, was aber nicht ging wegen der Abstürze. Ich hab die app sogar gelöscht in der Hoffnung/Verzweiflung, das ich den jailbreak los werde.

Mein Idee wäre nun ein komplettes backup vom iphone zu machen, es komplett zurückzusetzen und dann das Backup wieder einzuspielen.

Wisst ihr, ob das so funktionieren kann? Ich frage mich auch, ob durch das Backup wieder einspielen der jailbreak dann auch wieder drauf kommt oder bleibt der dann fern?

Falls die Idee nicht gut ist, könnt ihr mir noch etwas anderes raten?

edit: Ich hatte den jailbreak mit 12.xx oder 13.xx durchgeführt (kann mich nicht mehr genau erinnern). Zwischenzeitlich habe ich auf 13.7 ein update gemacht. Die Überreste des jailbreak sind aber dennoch vorhanden.

Vielen Dank!

Beitrag von „bounty96“ vom 22. März 2021, 16:34

Bei einem Backup (egal ob mit iTunes oder iCloud) werden eigentlich nur Userdaten gesichert.

Ich hätte mir schon ein paar mal gewünscht dass auch der Jailbreak mitgesichert wird, wird er aber nicht.

Also wenn du ein Backup machst, dein iPhone wiederherstellst und dein Backup einspielst dann ist der

Jailbreak weg. Die App kann unter Umständen schon wieder mit auf das neu aufgesetzte iPhone kommen

aber dann löschst du sie einfach gleich wieder.

Wenn du es mit iTunes wiederherstellst kommt sowieso iOS14.xx drauf. Soweit ich informiert bin ist

bis jetzt iOS14.0.3 die letzte Version für das SE1 die gejailbreaked werden konnte.

Beitrag von „hackmac004“ vom 22. März 2021, 17:04

[bounty96](#) Danke, das sind ja schon mal gute Neuigkeiten. Das iOS ist also im Backup nicht enthalten? Ich würde gern bei 13.7 bleiben, da ich dafür einen gut funktionierenden jailbreak mit checkra1n habe, der nach aus- und wieder einschalten erstmal deaktiviert ist.

Gibt es noch eine Möglichkeit das ich bei 13.7 bleiben kann oder geht das nicht weil das iOS nicht mehr gesignt ist?

Das iOS hab ich noch auf der Platte liegen.



Beitrag von „bounty96“ vom 22. März 2021, 17:21

[Zitat von hackmac004](#)

Das iOS ist also im Backup nicht enthalten?

Nein ist es nicht. Das würde die Größe des Backups nur unnötig aufblähen und der Vorteil von iOS ist dass es überall gleich ist und nicht jeder Hersteller seine eigene Oberfläche draufpuscht oder das ganze OS vergew.... deswegen muss das nicht mitgesichert werden.

Vor allem wächst iOS ständig. iOS4 hatte um die 630MB beim 14er sind es schon fast 3GB.

Das was man allerdings beachten muss ist dass sich erstellte Backups nur auf eine gleiche oder höhere iOS Version aufspielen lassen. Also ein Backup von 13.x kann man auf z. B. 14.x spielen aber nicht umgedreht.

Wenn du auf 13.7 bleiben willst käme noch das iPhone in der Einstellungsapp (unter allgemein oder bedienhilfen?) auf werkszustand zurückzusetzen. Man kann vorher noch die anderen Punkte auswählen (also Netzwerkeinstellungen zurücksetzen und so) aber ich glaube das wird beim kompletten Zurücksetzen eh gemacht (ich mach es trotzdem immer xD)

Im besten Fall ist dann der JB weg und du kannst dein vorher gemachtes Backup aufspielen. Solange sich der JB nicht zu tief ins System gefressen hat müsste das gehen. Aber ich glaube die heutigen Semi-Tethered JB's gehen eh nicht mehr so tief.

Wenn das nicht klappt, dann bleibt nur noch der Weg über iTunes und du musst leider mit iOS14 leben (was ich auch muss weil ich ausversehen von iOS10 auf iOS14 geupdated habe).

Die IPSW Datei bringt dir leider nichts weil, wie du schon sagst, sie wird nicht mehr signiert. Das ging nur mit den Geräten mit A4 Chip dass man downgraden konnte bzw. seine eigenen IPSW Dateien signieren konnte.

Beitrag von „pebbly“ vom 22. März 2021, 18:01

Wenn du auf 13.7 bleiben willst geht nur der Reset. Bei den Semi-Tethered JB's müssten sich die Daten des Jailbreaks der App (checkra1n) im App-Speicher und die weiteren Mods in einem "Profilverzeichnis" befinden. Bei denen ist es ja so, dass nach einem Neustart diese Mods zwar gespeichert sind, aber erst greifen, wenn man checkra1n ausgeführt hat. Wenn du das iPhone

resettet müssten diese ganzen Profildaten verschwinden. Wenn es clean ist, könntest du schauen, wie viel Speicher an "sonstigen" drauf geht und dadurch ableiten ob ich recht habe oder nicht .

Wofür verwendet ihr denn die Jailbreaks noch? Das letzte mal (iOS 13?), als ich damit rum gespielt habe, hatte es für mich keinen größeren Nutzen mehr.

Früher, als man damit auf dem iPad Air (1) Splitscreen aktivieren konnte war es noch nützlich, aber das Ding ist auch schnell zu langsam geworden.

Beitrag von „Erdenwind Inc.“ vom 22. März 2021, 18:12

weil man dann nichts mehr für die ganzen Apps bezahlen muss...Geiz ist halt geil.



Beitrag von „hackmac004“ vom 22. März 2021, 19:18

Ich brauch ihn eigentlich nur um die ganzen "neuen" Wischgesten zu nutzen, wodurch ich die Lebensdauer des Homebuttons verlängern kann. Und geringe optische Veränderungen.

Beitrag von „bounty96“ vom 22. März 2021, 20:28

[Zitat von pebbly](#)

Wofür verwendet ihr denn die Jailbreaks noch?

Ich verwende Jailbreak dafür dass mein iOS zumindest oberflächlich so aussieht wie iOS 6.

Weil ich persönlich das Design ab iOS7 bis jetzt hasse (und es wird immer schlimmer).

Achja und Geiz ist geil... da ist schon was dran xD

Beitrag von „hackmac004“ vom 23. März 2021, 21:11

Ich hab es jetzt komplett zurückgesetzt, das Backup eingespielt und der jailbreak ist dann irgendwo immer noch vorhanden, was ich durch die nette Mitteilung der Banking-app weiß. Cydia ist als app auch noch zu sehen.

Schade, dann werd ich es wohl ums neu aufsetzen nicht drumherum kommen.

edit: Nochmal zurückgesetzt, neu eingerichtet, Cydia ist immer noch drauf. Hab ihr noch eine Idee wie ich Cydia loswerde?

Beitrag von „bounty96“ vom 23. März 2021, 22:27

Hm das Backup sichert ja User Daten mit. Also in dem Fall auch Cydia. Jetzt kommt es halt darauf an wie der Jailbreak arbeitet.

Sollte das Dateisystem immernoch offen sein könntest du dich per SSH aufs Handy schalten und die App einfach direkt löschen.

Aber wenn ich so darüber nachdenke ist

das keine gute Lösung da das Handy ja trotzdem noch gejailbreaked wäre.

In diesem Fall bleibt dann nur noch wiederherstellen mit iTunes.

Dann wäre es aber auch mal interessant zu wissen ob die Cydia App (da sie ja scheinbar mitgesichert ist)

danach wieder drauf ist. Benutzbar dürfte sie nicht sein da ja kein JB vorhanden mehr ist.

Bei mir wurden noch nie JB Apps mitgesichert. Weder Cydia selbst noch Apps aus Cydia.

Beitrag von „hackmac004“ vom 23. März 2021, 22:35

Ich denke sie wurde hier auch nicht mitgesichert, da Cydia ja selbst wenn ich das phone neu einrichte noch mit drauf ist. Einfaches zurücksetzen reicht wohl nicht um das root system wieder zu reparieren.

Da bleibt wohl, wie du schon sagst, nur wiederherstellen und dann bye bye 13.7.

Ich guck aber nochmal ob ich mit Hilfe von den SHSH Blobs 13.7. doch irgendwie noch wiederherstellen kann.

edit: [bounty96](#) Ich musste chekra1n nochmal richtig ausführen und konnte dann innerhalb der app ein restore ausführen. Nun ist der jailbreak komplett weg 😊

Beitrag von „bounty96“ vom 24. März 2021, 00:46

Super dass es doch noch geklappt hat.

Also ich erinnere mich noch daran zur iPhone 4 / iPod Touch 4 Zeit konnte man mit den SHSH Blobs das iPhone downgraden.

Habe ich lustigerweise sogar erst vor ein paar Wochen gemacht um meinen iPod downzugraden xD

Das ging ja entweder mit Tiny Umbrella und installierten Java und dann die Apple Sig Server IP auf localhost umleiten

oder mit Sn0wbreeze.

Ich kann mich auch noch daran erinnern dass ich zur iOS7 Beta mein iPhone 5 geupdatet habe und dann wieder auf iOS6 downgraden

konnte. Aber ich glaube da lag es daran dass es die Beta war und iOS6 noch signiert wurde.

Falls du irgendwann mal an dem Punkt bist mit den SHSH Blobs zu versuchen dein iPhone downzugraden - lass mich wissen ob es geklappt hat.

Weil das mit den A4 Prozessoren war ja ein HW Exploit der ab dem A5 Chip gefixt wurde. Und

seit dem geht das nicht mehr soweit ich weis.