Cybersecurity Blog

Everything about threat intelligence, blue team, red team, pentesting, security audit, security review, testing and assessment.

Saturday, July 23, 2016

iOS Application Security - xCON Switch - Enable/Disable Detection without removing xCON Application from Cydia

I was searching for the xCon switch in order to enable/disable injecting xCon file to each application that is launched under iOS device. However, I was unable to find any such resource. So I decided to digg little into that.

Before moving forward, let me show you that my application gives me a messege while it detects the jailbroken device.

Translate Language

Search

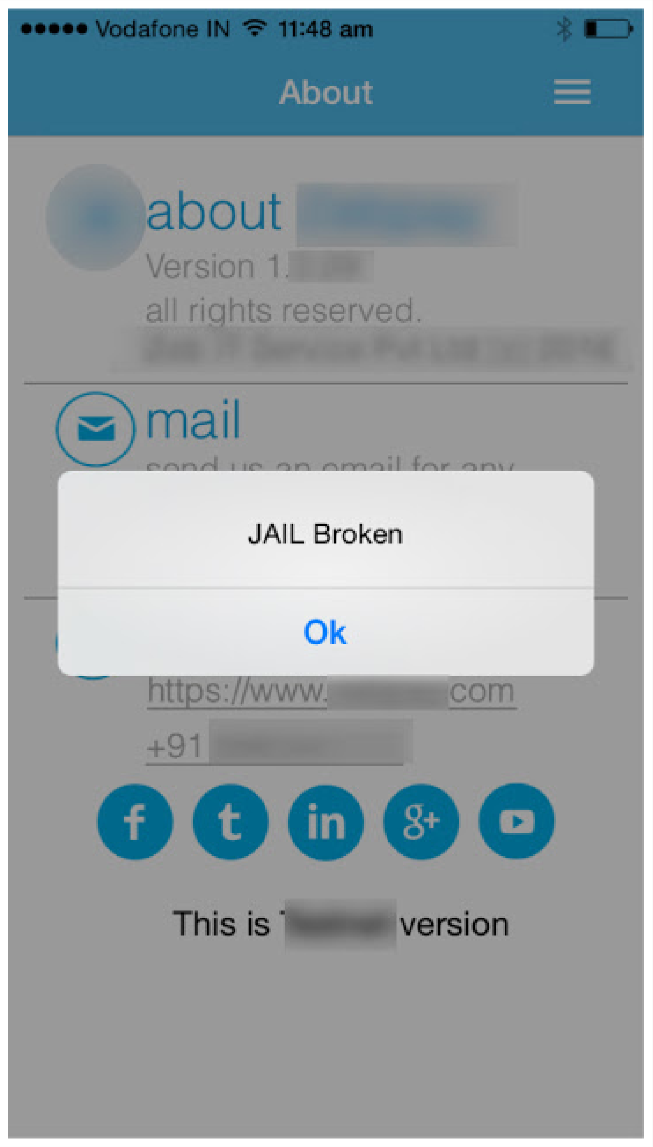
Search

Subscribe via email

Email address... Submit

Blog Archive

- ► 2020 (2)
- ► 2019 (6)
- ► 2018 (4)
- ► 2017 (5)
- ▼ 2016 (11)
  - ► November 13 (1)
  - ► October 30 (1)
  - ► October 23 (1)
  - ► October 9 (1)
  - ► September 11 (1)
  - ► September 4 (1)
  - ▼ July 17 (1)
    - iOS Application Security - xCON Switch - Enable/Di...



●●●●● Vodafone IN 11:48 am

About

about [redacted]

Version 1.[redacted]

all rights reserved.

[redacted]

mail

send us an email for any

JAIL Broken

Ok

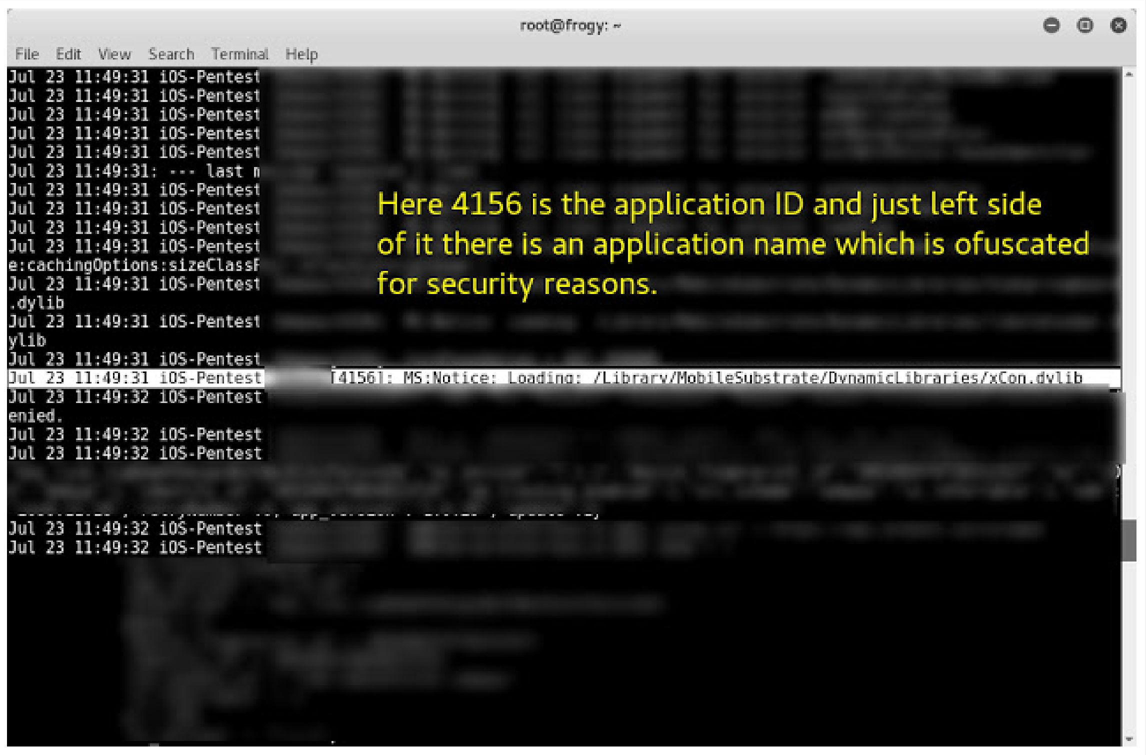
https://www.[redacted]com

+91[redacted]

This is [redacted] version

The trick is very simple. Initially I opened device logs in order to find which xCon file it is injecting into each application in order to bypass jailbreak detection log. I was able to find the exact path as follows:

- ▶ May 1 (1)
- ▶ April 10 (1)
- ▶ April 3 (2)
- ▶ 2015 (4)
- ▶ 2014 (22)
- ▶ 2013 (58)



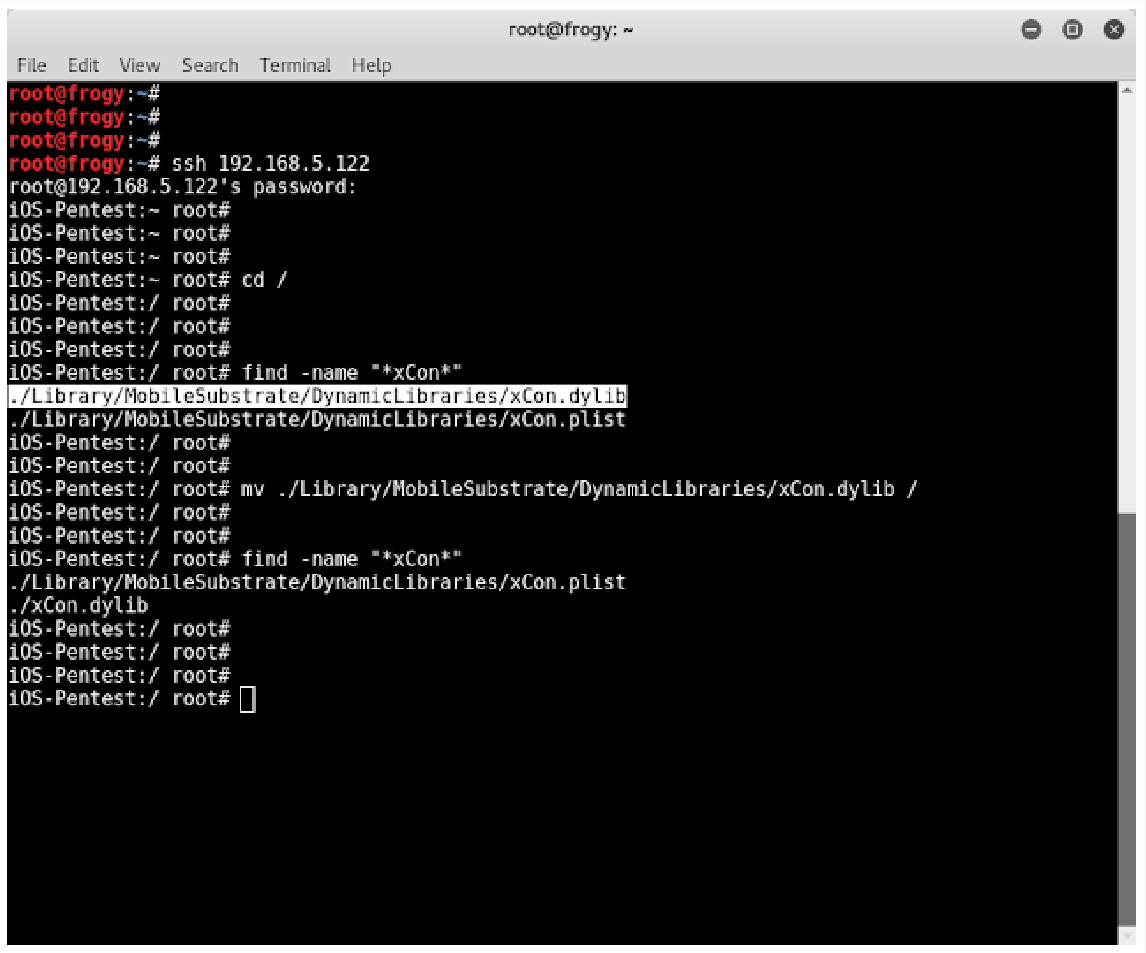
```
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31: --- last m
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest
e:cachingOptions:sizeClassF
Jul 23 11:49:31 iOS-Pentest
.dylib
Jul 23 11:49:31 iOS-Pentest
ylib
Jul 23 11:49:31 iOS-Pentest
Jul 23 11:49:31 iOS-Pentest        [4156]: MS:Notice: Loading: /Library/MobileSubstrate/DynamicLibraries/xCon.dylib
Jul 23 11:49:32 iOS-Pentest
enied.
Jul 23 11:49:32 iOS-Pentest
Jul 23 11:49:32 iOS-Pentest
Jul 23 11:49:32 iOS-Pentest
Jul 23 11:49:32 iOS-Pentest
```

Here 4156 is the application ID and just left side of it there is an application name which is ofuscated for security reasons.

As you can see the exact directory from whre it is injecting xCon.dylib file is as follows:

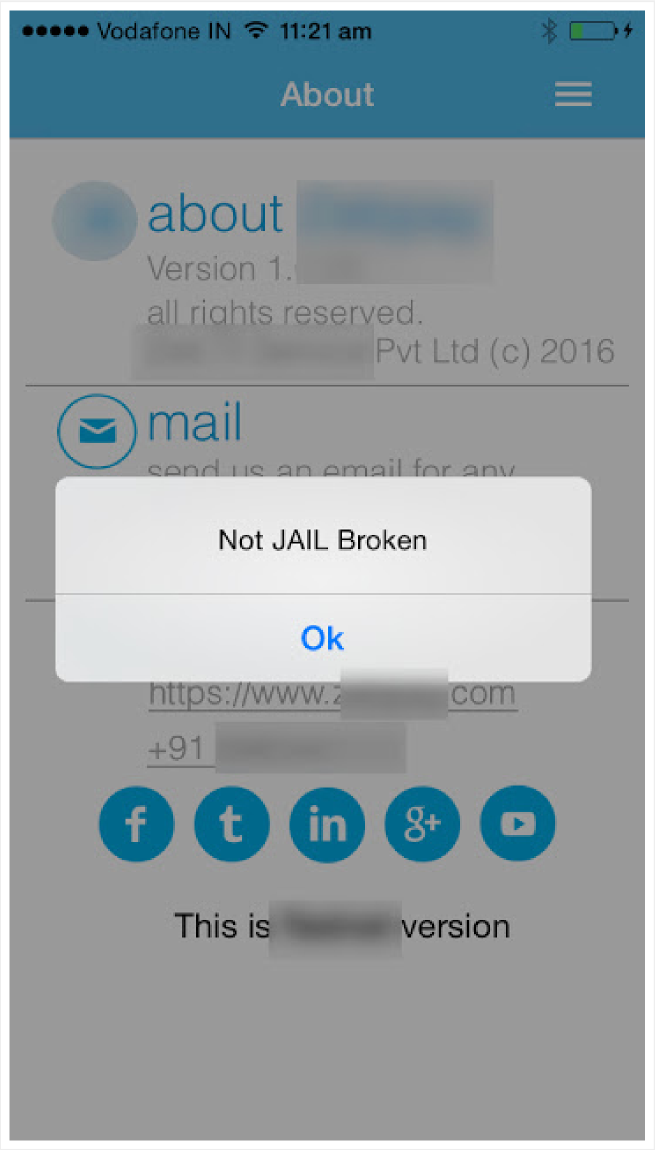
/Library/MobileSubstrate/DynamicLibraries/xCon.dylib

Now as mentioned in below image, log in into your jail-broken device using SSH and move xCon.dylib file to another location temporary.



```
root@frogy:~#
root@frogy:~#
root@frogy:~#
root@frogy:~# ssh 192.168.5.122
root@192.168.5.122's password:
iOS-Pentest:~ root#
iOS-Pentest:~ root#
iOS-Pentest:~ root#
iOS-Pentest:~ root# cd /
iOS-Pentest:/ root#
iOS-Pentest:/ root#
iOS-Pentest:/ root#
iOS-Pentest:/ root# find -name "*xCon*"
./Library/MobileSubstrate/DynamicLibraries/xCon.dylib
./Library/MobileSubstrate/DynamicLibraries/xCon.plist
iOS-Pentest:/ root#
iOS-Pentest:/ root#
iOS-Pentest:/ root# mv ./Library/MobileSubstrate/DynamicLibraries/xCon.dylib /
iOS-Pentest:/ root#
iOS-Pentest:/ root#
iOS-Pentest:/ root# find -name "*xCon*"
./Library/MobileSubstrate/DynamicLibraries/xCon.plist
./xCon.dylib
iOS-Pentest:/ root#
iOS-Pentest:/ root#
iOS-Pentest:/ root#
iOS-Pentest:/ root#
```

Now close your existing application and run it again, you will notice that as xCon.dylib was unable to inject the application. As a result of that, my application did not ran normally and according to application logic, it gave me a messege saying "Jail broken".



about [redacted]
Version 1.[redacted]
all rights reserved.
[redacted] Pvt Ltd (c) 2016

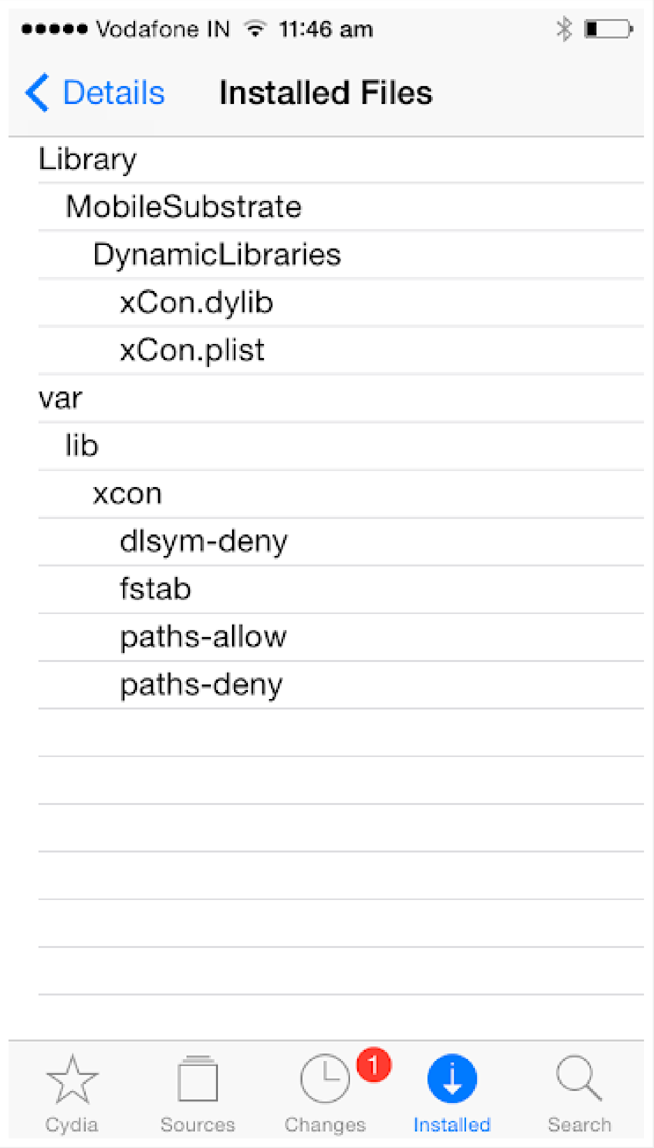
mail
send us an email for any

Not JAIL Broken

https://www.z[redacted]com
+91 [redacted]

This is [redacted] version

This how by just moving its file, you can enable/disable the detection engine of xCon. Also from cydia you can find what all files it will install in which directory so that you can copy and make the bundle for future use if it wont be available in cydia.



●●●●● Vodafone IN 11:46 am

< Details Installed Files

```
Library
  MobileSubstrate
    DynamicLibraries
      xCon.dylib
      xCon.plist
var
  lib
    xcon
      dlsym-deny
      fstab
      paths-allow
      paths-deny
```

Thank you.

Posted by Frogy at 7/23/2016

Labels: ios, ios application pentest, ios application security, ios security, jailbreak, jailbreak detection using xcon, xcon

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)