Hayden Ivey

🏠 > Uncategorized > Chase Android Mobile App Creating WiFi Network Independently

Chase Android Mobile App Creating WiFi Network Independently

👤 **Hayden Ivey**   📅 July 10, 2018   ✎ **Edit This**

-UPDATE-

Chase updated their app to version 3.51-19-g75cadc9 It will not not create a saved WiFi network. Thank you Chase for being quick and fixing the issue.

-ORIGINAL POST-

A couple weeks ago I was doing some testing with my Pineapple TETRA and noticed something interesting with my saved WiFI networks. Now I am not the one to connect to open WiFi networks unless I can use my VPN. However, I

needed to clear saved networks for troubleshooting my Pineapple. That is when I came across something interesting. There was a saved WPA/WPA2 network that Chase created.
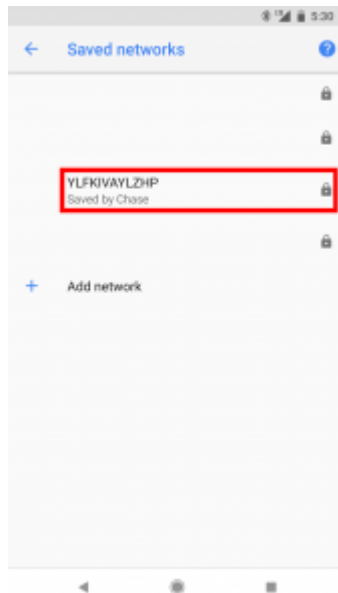
Now I have done quite a bit of testing on various Android devices. These are what I have used and that replicated similar networks that said Saved by Chase:

- Note 8: Android 8 (Oreo)
- Note 3: Android 5.0 (Lollipop)
- Pixel XL: Android 8.1 (Oreo, Rooted)
- LG V30: Android 8 (Oreo)

Now when recreating this problem, I noticed that Chase's app will not install on anything below Android 5.0. The device also needs to be connected to a network that has internet access. Now if the device meets that criteria, it will create the saved network with the following scheme. The first nine characters are randomly generated but the last three are always ZHP. Here is the log off the Pineapple that has it filtered for Chase SSIDs. It has been listening to Probe Requests for 4 days and 6 hours. Source MAC addresses have been removed from the log. (Keep in mind, each line of the log is a unique MAC address. Which means there can be a devices probing for the same SSID but

randomizing the MAC every time or that there are multiple devices that have generated the same SSID)

Date	Type	SSID	Times Probed For The SSID
2018-07-07 01:29:07,	Probe Request,	6YFYO0K55ZHP,	1
2018-07-07 08:30:25,	Probe Request,	I28Q35R4CZHP,	28
2018-07-07 08:48:56,	Probe Request,	WVVGQ7W01ZHP,	8
2018-07-07 09:13:33,	Probe Request,	XWXEQQJ9NZHP,	25
2018-07-07 09:53:28,	Probe Request,	OAR5CZG0KZHP,	17
2018-07-07 18:09:39,	Probe Request,	VAZZZR6GDZHP,	1
2018-07-07 18:11:33,	Probe Request,	VAZZZR6GDZHP,	1
2018-07-08 10:42:42,	Probe Request,	6LWDORL3XZHP,	3
2018-07-09 10:58:21,	Probe Request,	2HIVYRD5SZHP,	77

2018-07-09 16:43:49,	Probe Request,	ZD9HQSU3VZHP,	665
2018-07-10 08:35:20,	Probe Request,	UZ1GJONJ1ZHP,	25
2018-07-10 13:54:11,	Probe Request,	SQAYADAL3ZHP,	1
2018-07-10 13:54:31,	Probe Request,	SQAYADAL3ZHP,	1
2018-07-10 13:56:11,	Probe Request,	SQAYADAL3ZHP,	1
2018-07-10 13:56:35,	Probe Request,	SQAYADAL3ZHP,	1
2018-07-10 14:43:57,	Probe Request,	AA09FS33NZHP,	52
2018-07-10 15:18:20,	Probe Request,	4K8YAXA1MZHP,	53
2018-07-10 16:13:40,	Probe Request,	IETFEOT3TZHP,	18
2018-07-10 17:06:06,	Probe Request,	ZQ6SMBR5AZHP,	28
2018-07-10 17:07:57,	Probe Request,	OX2XBHBBVZHP,	17

Which shows that there are unsuspecting people with the Chase app installed and the phone is probing for the network it created.

Now lets inspect the saved WiFi config with a phone that is rooted. Here is the snippet.

```xml
1.   <Network>
2.   <WifiConfiguration>
3.   <string name="ConfigKey">&quot;YLFKIVAYLZHP&quot;WPA_PSK</string>
4.   <string name="SSID">&quot;YLFKIVAYLZHP&quot;</string>
5.   <null name="BSSID" />
6.   <string name="PreSharedKey">REDACTED</string>
7.   <null name="WEPKeys" />
8.   <int name="WEPTxKeyIndex" value="0" />
9.   <boolean name="HiddenSSID" value="true" />
10.  <boolean name="RequirePMF" value="false" />
11.  <byte-array name="AllowedKeyMgmt" num="1">02</byte-array>
12.  <byte-array name="AllowedProtocols" num="1">02</byte-array>
13.  <byte-array name="AllowedAuthAlgos" num="1">01</byte-array>
14.  <byte-array name="AllowedGroupCiphers" num="1">0c</byte-array>
15.  <byte-array name="AllowedPairwiseCiphers" num="1">06</byte-array>
16.  <boolean name="Shared" value="true" />
17.  <int name="Status" value="2" />
18.  <null name="FQDN" />
19.  <null name="ProviderFriendlyName" />
20.  <null name="LinkedNetworksList" />
21.  <null name="DefaultGwMacAddress" />
22.  <boolean name="ValidatedInternetAccess" value="false" />
23.  <boolean name="NoInternetAccessExpected" value="false" />
24.  <int name="UserApproved" value="0" />
25.  <boolean name="MeteredHint" value="false" />
26.  <int name="MeteredOverride" value="0" />
27.  <boolean name="UseExternalScores" value="false" />
28.  <int name="NumAssociation" value="0" />
29.  <int name="CreatorUid" value="10148" />
30.  <string name="CreatorName">com.chase.sig.android</string>
31.  <string name="CreationTime">time=07-08 08:00:27.168</string>
32.  <int name="LastUpdateUid" value="10148" />
33.  <string name="LastUpdateName">com.chase.sig.android</string>
34.  <int name="LastConnectUid" value="0" />
35.  <boolean name="IsLegacyPasspointConfig" value="false" />
36.  <long-array name="RoamingConsortiumOIs" num="0" />
37.  </WifiConfiguration>
38.  <NetworkStatus>
39.  <string name="SelectionStatus">NETWORK_SELECTION_ENABLED</string>
40.  <string name="DisableReason">NETWORK_SELECTION_ENABLE</string>
41.  <null name="ConnectChoice" />
42.  <long name="ConnectChoiceTimeStamp" value="-1" />
43.  <boolean name="HasEverConnected" value="false" />
44.  </NetworkStatus>
45.  <IpConfiguration>
46.  <string name="IpAssignment">DHCP</string>
47.  <string name="ProxySettings">NONE</string>
48.  </IpConfiguration>
49.  </Network>
```

This XML shows that the Chase app (com.chase.sig.android) creates a hidden secured WiFi network.

This is what I have found as of right now in the last week. Seems to be only affecting Android 5.0+ Now it comes down to these questions. Why does Chase need a saved WiFi network? Why is it not removed when the app uninstalls? Why does it only generate the WiFi network when connected to a network with Internet access?

-MORE INFO-

On 7/15/18 Chase DMed me "You are welcome. Rest assured, this has been shared to our Digital Team. ^RL"

Further research shows that a couple Reddit threads have been created a day before I went public with this information:

> ## [Question] Odd Chase Mobile App WiFi Activity
>
> I've had the Chase app for several months now and just noticed that it has saved a WiFi network on my phone.
>
> The only thing I can possibly think of is that it's a Chase VPN of sorts or other security measure? I've deleted this wifi network from my settings and have seen it return. The only permission given to this app is storage, which I just removed. My device is a Pixel XL.
>
> I've never seen an app do this. Does anyone have a plausible explantation for why this network is needed by the Chase app?
>
> r/androidapps • [deleted] • 4y ago
> 27 points • 14 comments

" Suspicious WiFi activity by the Chase Mobile app from security "

Share

Posted in Uncategorized

Previous Post: Two Networks Behind A Single Modem (Part 1)
Next Post: Unifi USG Site to Site VPN Using Hostnames

✎ RECENT POSTS

- Chase Android Mobile App Creating WiFi Network Independently July 10, 2018
- Create A Spotify Music Bot for Your TeamSpeak 3 Server (Debian 8 w/ GUI) [04/06/2016] April 6, 2016
- Create A Spotify Music Bot for Your TeamSpeak 3 Server (Debian 7 w/ GUI) [05/30/2015][OUTDATED] May 30, 2015
- Create A Spotify Music Bot for Your TeamSpeak 3 Server (Debian 7 w/ GUI) [11/03/2014] [OUTDATED] November 3, 2014

🗁 CATEGORIES

- Debian Tutorials (3)
- Uncategorized (1)

ⓘ META

- Site Admin
- Log out
- Entries feed
- Comments feed
- WordPress.org

Copyright © 2022 Hayden Ivey. Powered by WordPress and Stargazer.