Amazon Application Store and AWS/EC2 Vulnerabilities

9/10/2013
Larry W. Cashdollar,@_larry0

2013-396-NM

How to abuse the 'Try Before You Buy' feature (http://www.engadget.com/2011/03/27/amazon-com-lets-you-play-with-an-and-roid-virtual-machine-try-ap/) in Amazon's Android App store. I've been looking at Android applications for security vulnerabilities and I noticed you can also launch these applications on the android store to test before you download. This action spools up an android instance on the AWS cloud with the application pre-installed.

Some applications aren't written with security in mind (lack of remote authentication) and come with the powerful features that have allow you to Portscan the back end[1] of AWS exposing services (I am thinking cloud pivoting

http://andresriancho.github.io/nimbostratus/pivoting-in-amazon-clouds.pd
f depending on which network 10.x is) or just launching attacks from AWS
on the internet anonymously since you can do ping, traceroute and http
GET externally. You can probably use this feature act as a C&C for a
BroBot botnet.

You can also use certain applications to scan outside / send http requests to external sites from inside the cloud masking the origin of an attack.

Perhaps malicious actors would intentionally upload Android applications specifically to hide themselves in the cloud.

The application I've been testing/using is:

http://www.amazon.com/Ice-Cold-Apps-Servers-Ultimate/dp/B00E00C44G/ref=s
r 1 1?s=mobile-apps&ie=UTF8&gid=1378688647

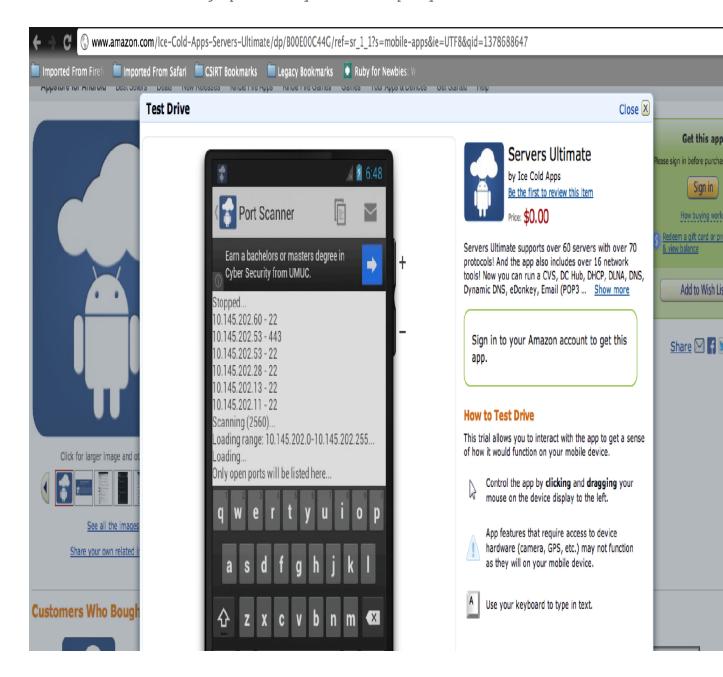
Written as a suite of full featured servers and network tools I decided to use this software to try and gather some information on the back end interfaces of the AWS cloud being used to launch the Try before you buy feature. I would think but didn't test that some of the SSH tunnel applications available would also be good candidate for testing.

I've started writing up a vulnerability advisory on the Ultimate Android Server application itself:

http://vapid.dhs.org/advisory/ultimate-server-android-vulns.html

The above advisory is incomplete and has not been released yet nor have I notified the vendor.

Below is a screen capture of a portscan using the above application on the 10.145.202.x network. I'd be interested in trying an SSH application that allows tunneling / port forwarding to possibly gain remote access or setting up an anonymous SOCKS proxy.



Amazon made a two changes as far as I can see as I have not received a formal document on the fix.



Click for larger image and other views



Share your own related images

Notepad Pro ++

by KongoApps

Platform: Android Rated: <u>All Ages</u>

★★★★★★ (49 customer reviews)

Price: \$0.99

Sold by: Amazon Digital Services, Inc.

Available instantly for your Android device

- Notepad
- Save notes
- Amazing functionalities
- Delete notes
- Sort them



Try this app right now on your computer. You control experience it like you would on your phone. Test drive

How does this work?

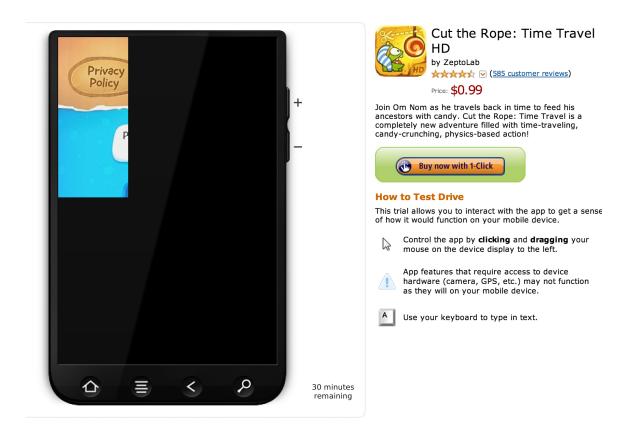
1. Created an ACL where only approved applications can be test driven.

Features





2. The Android cloud instance is only available for thirty minutes. The lower right hand corner of the cloud instance in the browser popup now displays a 30 minute timer. I personally have experienced a bug where only the top left 1/8th of my screen displays during the test drive. You can see this below in the screen capture I've taken.



[1] I've been told this isn't the backend network but a NAT'd frontend.