📄   🗓 January 14, 2015   💬 50 Comments   👤 Diamondback

Micromax Remotely Installing Unwanted Apps on Devices

In the recent past, we witnessed quite a few acts of OEMs messing with devices to achieve various goals, such as increasing benchmark results. We also heard about manufacturers and carriers adding tracing software to their devices, in order to collect data about how the device performs, statistics about voice and data connectivity between the device and radio towers, or even battery runtime data (CarrierIQ are you listening?). Today, however, reports are coming in that users of certain devices by Indian phone manufacturer Micromax noticed apps being silently installed without their consent or permission.

It appears that even uninstalling these apps won't help, as shortly after, they will simply re-appear again. Obviously, this is wrong on so many levels, but I'd like to point out a few key problems here anyway:

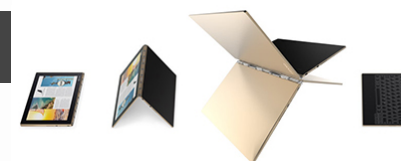- Micromax devices don't tend to be the highest end you can find, so storage space is still considered a luxury (at 4GB total) and having the device's storage filled up with random apps is certainly not the best use of that precious space
- The downloads also happen when using a mobile network, so your expensive full-speed data will reduce significantly if your phone is constantly trying to download apps you don't even want to have

While these practices already sound terribly wrong on their own, it unfortunately doesn't end there. In addition to downloading apps, these device also seem to display ads in the notification bar from time to time. A reddit user reports that 8-10 ads are displayed at once and upon looking up the responsible app for these disturbing notifications, he was presented with a system app called "Software Update".

So at this point, it certainly sounds like Micromax added custom software that remotely installs apps and pushes ads to users' devices. But we wouldn't be here at XDA Developers if we stopped at assuming things and simply telling you about the story of someone claiming things on the internet. Thus, we decided to tear down said app and have a look at what's inside.

The Evidence

When starting to tear down the application (which is actually called FWUpgrade.apk on your filesystem), the first thing you notice is that it's a third-party application. A Chinese company named Adups developed it as a replacement for the stock Google OTA service. Apparently, Micromax decided to use it instead of the stock one. The first hurdle you need to take for further analysis is the byte code level obfuscation, and most of the sources are really not a pleasure to read. However, if you know what you're looking for, the app can't hide its true nature. The evidence presented here starts out with a bit of code that shows you the potential abilities of this app and closes off with something even more interesting.

Let's start with the silently installed apps. To do this from within another app, you either need to use the Android PackageManager API directly, or issue the installation commands from a shell. The second case is true here, as the following pieces of code show (note: this is simplified java code, the actual code looks a bit different due to the obfuscation):
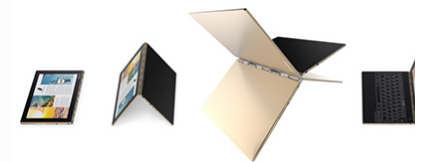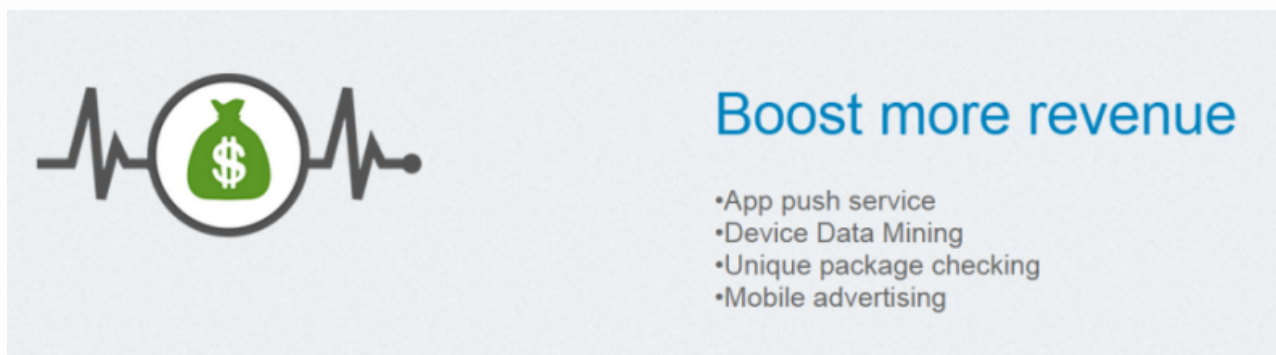
Here you can see a newly created StringBuilder containing the command *pm install*, followed by *s2*, which in this case is a string variable containing a file system path to a downloaded apk file. The finished string then gets passed to a new method doing something like this:

ProcessBuilder processbuilder = new ProcessBuilder(cmd);
Process process = processbuilder.start();

Here you can see that the string with the shell command is used to start-up a process which executes said command and in fact silently installs the apk file. At this point we can be fairly certain that the OTA check service in Micromax ROMs can not only download and flash system OTAs but also has the ability to silently install apps. This in itself doesn't mean too much as it's not necessarily a bad thing, but there's more to come.

Inside the app I found a few references to the company's website, including one that has an extensive feature list. Shall we have a look at the most interesting part?

There you have it, in the company's own words. App push service. Device Data Mining. Mobile advertising. That matches pretty nicely the initial report on reddit, don't you think? So, the bad guy here is in fact Micromax since these are official features of the app by Adups, and it's more than likely that Micromax is getting revenue from the forced app installs and notification ads. They also chose to go with this provider and not use their own servers together with Google's stock OTA service, so they were fully aware of what impact this would have on their users.

The Temporary Solution

So now that we know that these unfortunate reports were true, let's talk about how to get rid of this "functionality". The first step of disabling said features, would be to head to the devices' app settings to disable the rogue system app. However, this is not possible in this case, as Android allows OEMs to deactivate the disable button for certain apps. But do not fear, we have a solution readily available and will tell you how to disable the malicious code.

1. Root your device

The first and most important step is to root your device. A rooted device allows you to do much more than your stock phone would allow, and is a critical step in all system modifications. Since there are quite a few different Micromax devices out there, I won't link to any specific root exploits in this article. Instead, head over to XDA:India and search for a root exploit or guide for your device. Make sure to read everything thoroughly and follow the instructions precisely to not damage your device in the process. Also note that this will most likely void your warranty.

2. Get ADB set up

In order to continue, you'll need to have a working ADB connection to your device. There are many guides on XDA that detail how to achieve exactly this, but for starters, here is a fairly up-to-date guide on how to download the necessary binaries and how to establish a connection to your device.

3. Disable the Software Update application

Now that you have gained root access and ADB is up and running, you can continue with disabling the dreaded application responsible for the silent installs and unwanted ads. All you need to do now is to fire up a command prompt, make sure the prompt is at the directory of your ADB binary, and execute the following command:

access. Please be aware that this process will remove the ability for your device to search for software updates and might generate an error when trying to open the Phone update section in the settings. In case you need the app back (for example when a new update is ready) you can easily enable it again with this command:

adb shell pm enable com.adups.fota

The Wrap-Up

It's unfortunate to have learned that Micromax is indeed responsible for the unwanted app installs. We hope that the above tutorial on disabling the shady application will save you some headache on dealing with random apps and ads. Obviously, all of this won't stop Micromax from continuing these shady practices, but maybe you will consider another OEM for your next device purchase.
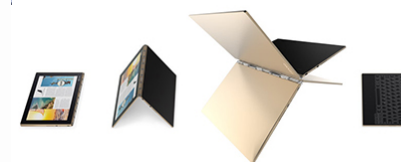
Share this post: f   🐦   g+   🔴   💬 Discuss This Story

🏷 Tags   • malware   • micromax   • spyware

YOU MIGHT ALSO LIKE

search plus

43 Comments

26 Comments

7 Comments

Check out XDA Deals

Betrayal of Hype: Playing Fast and Loose with Release Dates Breeds Consumer Mistrust

Sony's Hero Open Source Developer Title for May-June Awarded to XDA RD Bumble-Bee

### Multi-Window in Android N: What Devs Need to Know to Make the Best of It

0	53861
Your Entries	Total Entries

50 Comments   **XDA-Developers**

Login ▾

Win an Android Yoga from XDA!

♥ Recommend   **4**   ⤴ Share   Sort by Best ▾

Join the discussion…

8 Ways to Enter

mashaal95 • 2 years ago

Loving these detailed articles, as always thank you for informing us about these shady OEM's xda!

33 ∧ | ∨ • Reply • Share ›

Login with: ✉ f 📷 ☁

vvaklnprm • 2 years ago

what the actual fsck!! Absolutely ridiculous!! :@

12 ∧ | ∨ • Reply • Share ›

★ Click For a Daily Bonus Entry

superdragonpt • 2 years ago

Well nothing new about this this OEM... Very sad...

5 ∧ | ∨ • Reply • Share ›

🐦 Follow @xdadevelopers on Twitter

Salamander Calamander • 2 years ago

Instead of re-enabling the adups malware for software updates, why not install the stock Google OTA service?

2 ∧ | ∨ • Reply • Share ›

🐦 Tweet on Twitter

▶ Subscribe to XDA TV!

Atinav Bajaj ➜ Salamander Calamander • a year ago
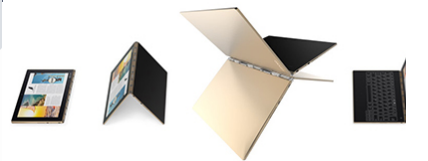
↗ Visit our sponsor (Honor) at Best Buy

Bewear • 2 years ago

This is why you don't buy shitty Chinese devices from shady manufacturers.

3 ∧ | ∨ • Reply • Share ›

xdadevet ↗ Bewear • 2 years ago

Funny actually as there are many decent chinese manufacturers. MicroMax is an Indian company. First they pressure Cyanogenmod to skrew One Plus over, now this. I really beginning to dislike this shitty company. Btw almost all devices are Chinese devices including iPhones and OPPO which make great quality phones.

13 ∧ | ∨ • Reply • Share ›

Bewear ↗ xdadevet • 2 years ago

I know, almost all devices are assembled in China, but I am talking about Chinese devices which are then sold to resellers who then just put their brand on them (like Micromax, BLU, Elife, etc.).

4 ∧ | ∨ • Reply • Share ›

Mubasher96 ↗ Bewear • 2 years ago

But xdadevet is right as many resellers are selling these re-branded Chinese phones but still they don't do anything like what micromax is doing and some even have decent after sales services.

3 ∧ | ∨ • Reply • Share ›

Parikshit Rathod • 8 months ago

Help me brother...I am using Micromax Canvas Knight A350. I have running adb. whenever i run command for uninstalling app, it shows like this -

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb devices

List of devices attached

0123456789ABCDEF device

C:\Program Files (x86)\Android\android-sdk\platform-tools>adb shell pm disable com.adups.fota
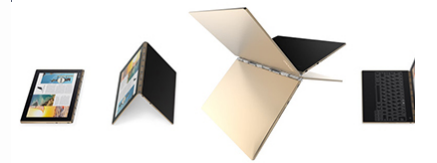
WARNING: linker: libvcfdec_sa.ca7.so has text relocations. This is wasting memory and is a security risk. Please fix.

java.lang.IllegalArgumentException: Unknown package: com.adups.fota

at android.os.Parcel.readException(Parcel.java:1469)

see more

1 ∧ | ∨ • Reply • Share ›

Relayers • 2 years ago

Arent they the new partner of Cyanogen ? Well they deserve each other even more now.

1 ∧ | ∨ • Reply • Share ›

Moscow Desire • 2 years ago

Well, why doesn't it exactly surprise me.....

And what's their sssss....."spin-off" company?? Yu...as in....Yureka???? Ain't say'in some folks have to check for the same, but......the chicken doesn't roost far from the hen-house.

1 ∧ | ∨ • Reply • Share ›

BROKEN1981 ➤ Moscow Desire • 2 years ago

Not sure what your trying to say. Mind using english?

1 ∧ | ∨ • Reply • Share ›

dhruvit.raithatha ➤ BROKEN1981 • 2 years ago

Lol. What he meant was yureka is a chinese name. Micromax (the chicken), isn't roosting (rebranding Chinese phones with Chinese names, here) far from the chicken house (China).

2 ∧ | ∨ • Reply • Share ›

Roger Guenther • 2 years ago

Still can't root my Verizon LG G3 though.

1 ∧ | ∨ • Reply • Share ›

cyanogen • 2 years ago
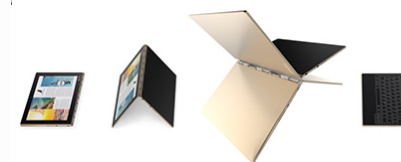
In before tinfoil.. :)

We actually implemented a nice way to deal with preloads for the Yu device- you can uninstall them! There are only 2 extra apps that fall into this category in the shipping build, but it was something I wanted to get right.

1 ∧ | ∨ • Reply • Share ›

Hitesh • 4 months ago

root status is lost after reboot

∧ | ∨ • Reply • Share ›

Ahmad Swalih CK • 5 months ago

The only good phone from Micromax is Canvas A1 because of being in Android One program.

∧ | ∨ • Reply • Share ›

Mayank Kumar Sisodiya • 6 months ago

i have micromax A104 and i have done everything as per above and everything was done correctly but still i am getting apps installed, now what should i do.

∧ | ∨ • Reply • Share ›

Moriarty • 8 months ago

WARNING: linker: libvc1dec_sa.ca7.so has text relocations. This is wasting memory and is a security risk. Please fix.
Package com.adups.fota new state: default
what do i do now

∧ | ∨ • Reply • Share ›

Pankaj • 8 months ago

I have a micromax Nitro 2 and I am facing the same problems mentioned here. I realize micromax is the worst choice i made. I have also written to micromax about it but no reply. Shame on micromax. I am truly sick and tired of these notifications and apk's. I don't want to risk rooting my phone but will soon change to a better brand
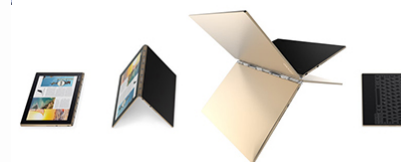

Check out XDA Deals

XDA Interview

Win an Android Yoga from XDA!

8 Ways to Enter

Login with: ✉ f 📷 ☁

★ Click For a Daily Bonus Entry

🐦 Follow @xdadevelopers on Twitter

🐦 Tweet on Twitter

▶ Subscribe to XDA TV!

↗ Visit our sponsor (Honor) at Best Buy

0	53861
Your Entries	Total Entries

great article ... helped me disable this useless service on my mother's mmx... btw it was with name com.rock.gota, they might be changing package names to hide, but who cares... cheers :)

⌃ | ⌄ • Reply • Share ›

bond james • 10 months ago

i have one solution for this problem so if you want solution and this solution so mail me at bond007100007@gmail.com . i have same problem and i try this solution on my mobile and wow that work for me so mail me and this solution for without root

⌃ | ⌄ • Reply • Share ›

bond james • 10 months ago

i have one solution for this problem so if you want solution and this solution so mail me at bond007100007@gmail.com . i have same problem and i try this solution on my mobile and wow that work for me so mail me and this solution for without root

⌃ | ⌄ • Reply • Share ›

Atinav Bajaj • a year ago

Thank you. This has helped a lot.

⌃ | ⌄ • Reply • Share ›

DaksAnkit • a year ago

micromax can suck it , i am getting continous adds even if the phone is not connected to the internet and there is a bulk of it. and i don`t want to root it because it would void warranty but soon.. after the warranty wears of i m gonna .root and flush these bloats

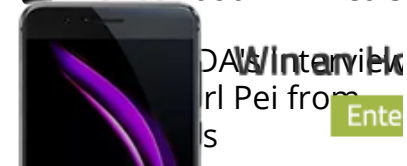⌃ | ⌄ • Reply • Share ›

wargo • a year ago

Hi, I have a Dragon touch e97 with this problem. Someone Knows if there is a final solution for this? Thanks.

⌃ | ⌄ • Reply • Share ›

Biswarup Ray • 2 years ago

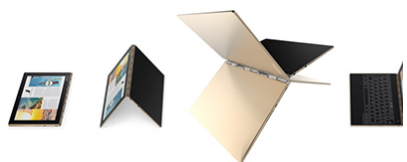I am facing the same problem with a Bolt A065. The homepage of the stock android browser is locked

I think affected micromax users should file a class action suit or something like that.

∧ | ∨ • Reply • Share ›

Arun • 2 years ago

Just restrict the background data for "software update".. It will be the perfect solution for all

∧ | ∨ • Reply • Share ›

Yash Vardhan • 2 years ago

just uninstalling "software updates" worked for me

∧ | ∨ • Reply • Share ›

Denn ➤ Yash Vardhan • 2 years ago

You are missing the point. After uninstalling the updates the installed apps might go for once but they can reapper at anytime as long asFWupgrade.apk runs in the bakground.Only solution is to freeze the app after rooting.You can use many rooted apps fror freezing like Titanium backup, or Link2SD etc.or delete the app permanently,in that case you wont even get future Android upgrades.

∧ | ∨ • Reply • Share ›

Yash Vardhan • 2 years ago

same thing happened with me

micromax unite 2 a106

apps were being downloaded automatically and ads pushed to notifications..

these apps came in on their own .. (newshunt, quickr, snapdeal, MAd, M!Live,etc,...)

∧ | ∨ • Reply • Share ›

ssuds • 2 years ago

Didn't you just announce a new partnership with these guys a few days ago?

∧ | ∨ • Reply • Share ›

sophisticatedjoker • 2 years ago

everything is fine when you have cyanogenmod 11 and 12 ported B) and google is the shepherd for your phone... :) nice guide btw (Y)
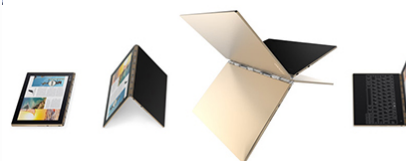
∧ | ∨ • Reply • Share ›

∧   ∨   •   Reply   •   Share ›

Shanky Yadav • 2 years ago

Yup from few day i am having a folder named starting from xing and something in chinese, i deleted it so many time but it still reapears

∧   ∨   •   Reply   •   Share ›

gvijaykumar • 2 years ago

I dont think Micromax is doing that wantedly, probably that third party software developer from China inherently has it inbuilt. Micromax is a stupid company

∧   ∨   •   Reply   •   Share ›

     jerdog76 **XDA Portal Team** → gvijaykumar • 2 years ago

     these things don't get added without the company being aware, much less reaping some reward. Rest assured Micromax knows exactly how and why it's being done.

     22 ∧   ∨   •   Reply   •   Share ›

     debr → gvijaykumar • 2 years ago

     Lmao, Indians trying to blame the chinese for their shitty companies spyware.

     ∧   ∨   •   Reply   •   Share ›

     soumitpl48 → gvijaykumar • 2 years ago

     Nope, knowing Micromax and after using their product for a long time, I think that they definitely are doing this intentionally. And the worst part is, most common user don't even care, to them, Micromax has the best VFM.

     ∧   ∨   •   Reply   •   Share ›

Santiago Postorivo (Persano) • 2 years ago

Im angry with XDA. They dont care about companies like Jiayu or other chinese companies that dont want to release their device source. You must help mediatek device community

∧   ∨   •   Reply   •   Share ›

     jerdog76 **XDA Portal Team** → Santiago Postorivo (Persano) • 2 years ago

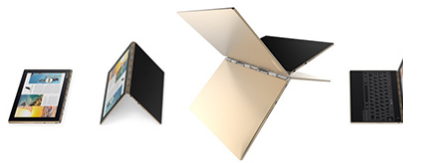ones responsible to release source - but in China no one cares about following copyright laws - their companies are told not to worry about it. So your best bet is to buy a phone that isn't one of those.

24 ∧ | ∨ • Reply • Share ›

Santiago Postorivo (Persano) → jerdog76 • 2 years ago

Give me te money so. Ignorant. My oem is under pressure of mediatek. They must pay money to mediatek to release the source, learn a bit before saying anything

∧ | ∨ • Reply • Share ›

superdragonpt → Santiago Postorivo (Persano) • 2 years ago

Xda has nothing to do with that, keep pressuring your OEM for kernel sources... Also, in fact, xda is doing an great work , and several articles about that issue, where published here...

9 ∧ | ∨ • Reply • Share ›

Santiago Postorivo (Persano) → superdragonpt • 2 years ago

My oem is under pressure of mediatek. They must pay money to mediatek to release the source

∧ | ∨ • Reply • Share ›

xdadevet → Santiago Postorivo (Persano) • 2 years ago

Not even going to go in as to why they aren't really supported as that has already been answered. My question is simpler: Why buy a Mediatek device if you don't want a Mediatek device with no developer support? If you want developer support you have to have the same device that developers target. Developers have no obligation to waste their time trying to piece together unkown brands source code just because they don't release their source code to the public.

2 ∧ | ∨ • Reply • Share ›

Santiago Postorivo (Persano) → xdadevet • 2 years ago

My oem is under pressure of mediatek. They must pay money to mediatek to release the source. This is the real mediatek. I know the reality
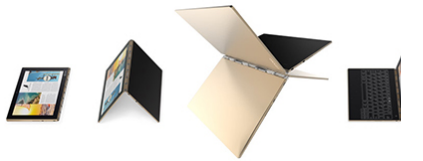
∧ | ∨ • Reply • Share ›

search plus

instead start collecting device tree from various sources if you want some support, the MT6589,MT6582,MT6592 full kernel source(except the device tree) can be obtained from various git Repositories

⌃ | ⌄ • Reply • Share ›

Santiago Postorivo (Persano) → chiragjn • 2 years ago

Yes, but the lcd driver, the camera driver, the bluetooth driver, the touchscreen driver, the wifi drivers and other similar drivers are exclusive of jiayu. I never saw a device with the same screen, wifi modem, touchscreen. I know what i say because i was trying to search compatible drivers

⌃ | ⌄ • Reply • Share ›

ALSO ON XDA-DEVELOPERS

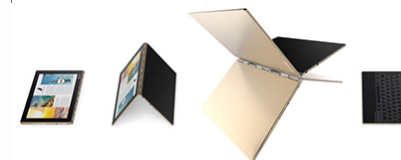**[Exclusive] The Philosophy Behind the OP3T: Why OnePlus Released this Device, and**

Would You Purchase an Updated Variant of Your Current Phone?