TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

LineageOS

Continued Support for CyanogenMod

We have written about CyanogenMod (CM) previously in the Update. CyanogenMod was a free and open source alternative operating system for Android devices. Among other things, CM offered more security, privacy, and control than stock Android builds. However, the volunteers who have, until now, maintained CyanogenMod recently decided to drop the project.

CyanogenMod has been abandoned and is no longer supported, but fret not, it's lineage lives on with a new project that vows to keep CM alive. It's now going by the name LineageOS and it is basically CM with some re-branding and a few differences. If you currently run CyanogenMod, LineageOS is offering a temporary migration build, but it is highly recommended that you wipe and start fresh to avoid major software issues down the road. If you are not familiar with custom ROMs (Android Read-Only Memory), you should know that it's not a good idea to "dirty flash" a device as you may cause a lot of unexpected problems. It is, however, very important that you update to the latest version as there are several bugs inbetween versions that have been patched in the newest release.

The developers of LineageOS are very active and are moving quite quickly with releasing updates and support for new phones. They already have a long list of supported devices including many of the newer flagship phones like the LG G5 and the Moto G4. The newer Samsung phones are not yet supported officially, but there are several unofficial ports if you want to go that route. Remember that if you brick your device, it's no one's fault but your own and your phone's manufacturer does not support custom ROMs. The LineageOS developers have a full list of supported devices on their website: **lineageos.org**.

The most obvious difference between LineageOS and it's predecessor is the new logo and name, but one of the major differences is that it is removing the default option of giving you

WhatsApp

Making the Best of a Bad Situation

Last year it was announced that the popular messenger WhatsApp would implement end-to-end encryption using the same protocol found in Signal Private Messenger. This was great news because over one billion people worldwide were already WhatsApp users. The reason we don't recommend WhatsApp as a secure messenger is because it is owned by Facebook. Facebook collects quite a bit of metadata making it less desirable than other options. WhatsApp also requests access to your contacts and photos. So does Signal, but Signal isn't owned by Facebook.

However, there are a couple of reasons you may want to use this messenger service. We have received several reports from operators in the field and in some areas of the world WhatsApp is already on just about everyone's phone. In Africa, for instance, phone minutes are extremely expensive but data is cheap, so WhatsApp is the preferred line of communication for locals. Installing WhatsApp makes sense in this case because almost everyone has it already. Getting them to migrate to a different option would be difficult and take time.

Before jumping in and committing to WhatsApp, you should take a look at some of its settings. Tightening up the app won't make it perfectly secure but it will let you make the best of a bad situation. The specifics will vary depending on your device. There are excellent tutorials from the EFF's Surveillance Self-Defense page:

- Android: **https://ssd.eff.org/en/module/how-use-whatsapp-android**
- iOS: **https://ssd.eff.org/en/module/how-use-whatsapp-ios**

We want to stress that we don't recommend WhatsApp over Signal. However, going to WhatsApp can allow you to encrypt more of your communications which is certainly better than sending plaintext SMS, especially in hostile environments.

Upcoming Events:

Law Enforcement Intelligence Units
May 1-5 2017, Bloomington, MN

Associated Locksmiths of America Expo
June 16-22 2017, Rosemont, IL

National Technical Investigators' Association (NATIA) Annual Conference
July 12-23 2017, Tampa, FL

LineageOS

Continued Support for Cyanogen Mode

<< CONTINUED FROM PREVIOUS PAGE

root access. Instead you will have to separately root your device if you want apps to have full root access to your phone. You do still have the option of gaining root through adb (Android Debug Bridge), but removing root access for apps may get more people on board with getting rid of stock android in favor of a custom ROM. CyanogenMod always gave you the option of turning root access on and off, but LineagOS removes the temptation completely. They have also made some small improvements, such as combining the screen recorder and the sound recorder into one app.

The shutdown of CyanogenMod came with little warning. Before going with any custom ROM you should proceed with caution. Support could be pulled at any time because of lack of funding or even interpersonal conflicts. We don't want to discourage you from using alternative ROMs, but have a backup plan if they suddenly fold.

We are happy to see that CyanogenMod didn't completely die and LineageOS is more than suitable to take its place. We have noticed some issues with getting full disk encryption to work properly on some devices (LGs and Motorolas in particular), but hopefully the developers fix this problem quickly. Although LineageOS is basically just a complete copy of CyanogenMod for now, we are excited to see what the developers have in store for the future. LineageOS is also completely open source and can be found on github. For any additional information visit LineageOS website: **http://lineageos.org/**

If we can help you with the transition to Lineage, contact **admin@tpidg.us**

FLIRC
USB Remote Receiver

FLIRC is a small USB receiver that accepts input from any remote and sends it to the device it's plugged into. It is completely plug and play (after the initial setup) and allows your remote to work with your media center on whatever platform you choose to use. The initial setup is pretty simple: plug the FLIRC into your computer, download and run their setup file and begin programming it to work with your remote. The set up of the remote is quite unique, rather than you choosing the manufacturer and model of the remote, they have you press each button on the remote that corresponds to the button you see in the setup window.

You can actually set it up however you like, for instance, you could have the enter button on the remote correspond to the spacebar or something else depending on your needs. There are no limitations to what buttons are mapped to each function as long as they are each different buttons (which is a limitation for remotes in general). They offer several different controller options including KodiTV, Windows Media, Xbox360, and more. This device is specifically marketed towards being used with the RaspberryPi running OpenELEC or something similar, but the amount of devices that the FLIRC supports is absolutely astounding. Basically, if the media center has a USB port and the remote has an IR sensor, you're in business. Once the FLIRC is set up for a specific remote, you can reuse it anywhere on any device with no additional configuration. This is definitely a must have for anyone who uses something like OpenELEC (see our January 1st edition for more information on OpenELEC and KodiTV) for their entertainment needs. On top of all that, a portion of every sale gets sent to Dr. Lenz's USC Cancer Research Facility because the creator of FLIRC is a cancer survivor. For further details or questions, visit **https://flirc.tv/**.

Course Spotlight
Basic Identity Managment

Taught by one of the country's leading privacy experts, our Identity Management curriculum is the absolute best available. With ambushes on law enforcement personnel becoming more prevalent, and new challenges facing SOF personnel operating in permissive environments, we believe this type of training has never been more important. The Basic Identity Management Course covers:

- **How to assess your level of exposure**. There is a good chance your home address, phone number, and the names of your family members are openly available online.

- **How to remove information from the internet.** There is a good chance your home address, phone number, and the names of your family members are openly available online.
- **How to stop putting information into the system**. Using alternative email address, phone numbers, and masked payment methods you can prevent your information from being bought and sold as a commodity.
- **How to harden your digital footprint, secure your computer and devices.**

The Identity Management course is flexible to meet the needs of your organization. Contact **admin@tpidg.us** for more information.

coming soon >>>

In Future Issues...

- *Little Flocker for Mac*
- *Little Snitch & Micro Snitch*
- *Signal's Expanded Feature Set*
- *Anti-Virus and Anti-Malware*

If you would like to see a specific a product or service reviewed in the Digital Update, please don't hesitate to get in touch. We are always looking to make content as relevant as possible to our readers. You can reach out through www.TPIDG.us or email directly to admin@tpidg.us .