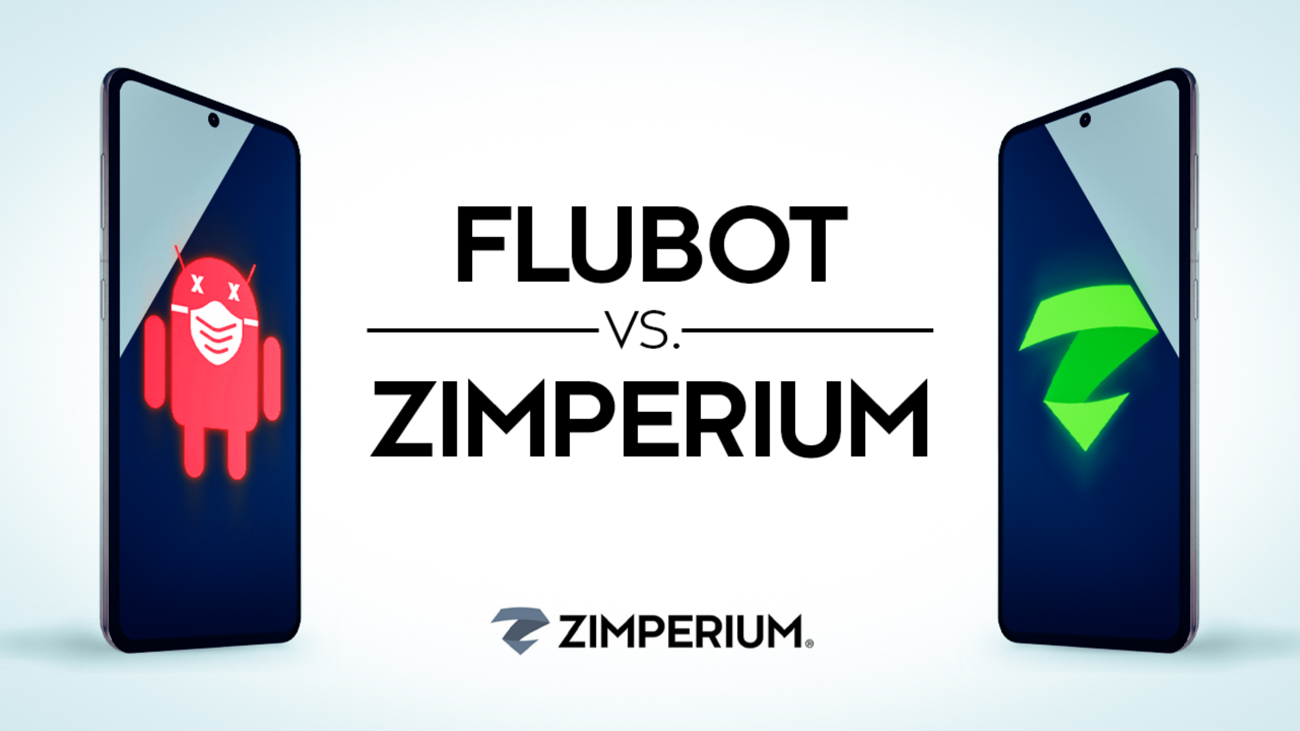
Flubot vs. Zimperium

blog.zimperium.com/flubot-vs-zimperium/

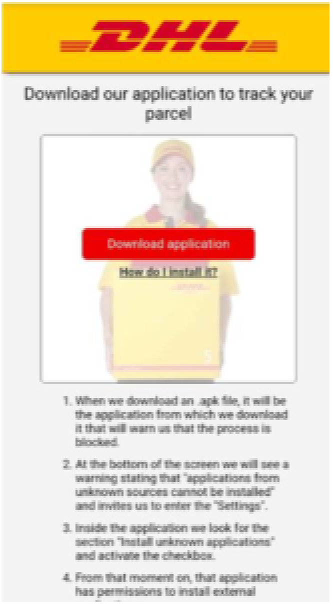
Jon Paterson May 5, 2021



Over the past few weeks, reports of the newest aggressive malware family to impact Android devices have made the rounds. Flubot, the credential and banking malware family, uses SMS phishing techniques to propagate to its victims, purporting to be various vendors and delivery services. The group behind this aggressive malware takes advantage of a common but effective social engineering technique.

The Zimperium zLabs team has analyzed over 300 variants of Flubot and the URLs used to distribute them, finding that the aggressive credential stealer comes with unique features that make it stand out from many other examples of mobile malware seen in the past. The Android malware has been so effective, the UK's National Cyber Security Centre has issued a cybersecurity warning, providing instructions for removal and reporting of any attempts.

The modern bank robbery is not happening through the front door of a building but with the path of least resistance – banking credentials. Flubot's credential theft effectiveness comes in the form of its delivery and execution. The victim's phone receives an SMS, instructing them to click a link to track their "package" via one of the known global shippers. The victim is redirected to a fake or compromised website where the malicious APK is downloaded and installed via side loading. The user wants to track their package and installs the application via side-loading onto the Android device – even walking the victim through the process if unfamiliar.



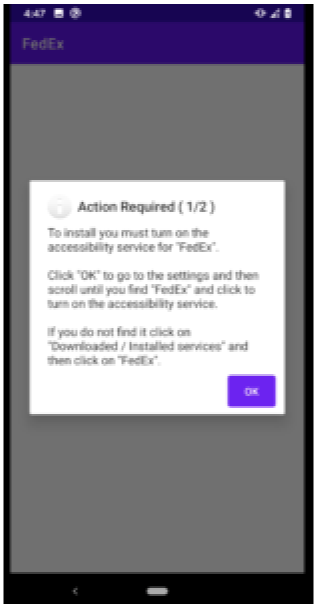
Download our application to track your parcel

1. When we download an .apk file, it will be the application from which we download it that will warn us that the process is blocked.
2. At the bottom of the screen we will see a warning stating that "applications from unknown sources cannot be installed" and invites us to enter the "Settings".
3. Inside the application we look for the section "Install unknown applications" and activate the checkbox.
4. From that moment on, that application has permissions to install external

After installation, a window appears asking for the victim to "Accessibility Services" (a restricted capability allowing monitoring and interaction with all apps/screen content) for the application, enabling the now-installed application to take control without the user even knowing. Once the application has this permission, it uses it to get others such as READ_SMS, RECEIVE_SMS, and READ_CONTACTS. The app registers itself as the main SMS client, which will be later used to steal 2FA credentials.

A key component of credential-stealing malware is an effective command and control (CNC) capability, giving the attacked the ability to grab what they want and not be flooded with untargeted data. In the case of Flubot, the CNC backend is not hardcoded into the malware itself. Instead, it uses a Domain generation algorithm (DGA) – common in advanced desktop malware to generate the CNC URL server address. This enables Flubot to continue to evade its victim's mobile endpoints if a security team was to block one single address.

Its effectiveness on mobile endpoints is made more so by Flubot's capability to automate actions. After disabling Google Play Protect, the Android malware then asks to be set as the default SMS and notification tool, enabling it to continue spreading to more victims by collecting contact lists and preventing the victim from seeing the actions. From the moment the malicious application is installed, it also begins monitoring all the applications installed in the device. When a targeted application is opened, Flubot performs an overlay attack to collect user credentials and send this data back to the CNC. At the same time, Flubot uses SMS permissions to read second-factor authentication codes.

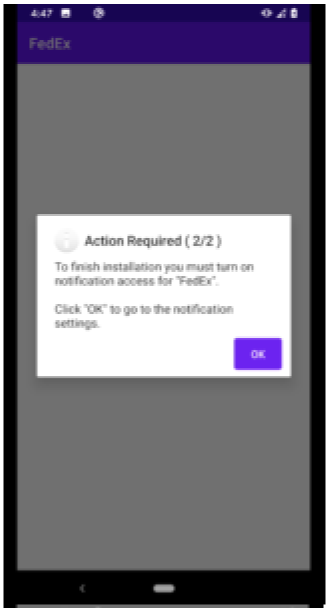


Action Required (1/2)

To install you must turn on the accessibility service for "FedEx".

Click "OK" to go to the settings and then scroll until you find "FedEx" and click to turn on the accessibility service.

If you do not find it click on "Downloaded / Installed services" and then click on "FedEx".

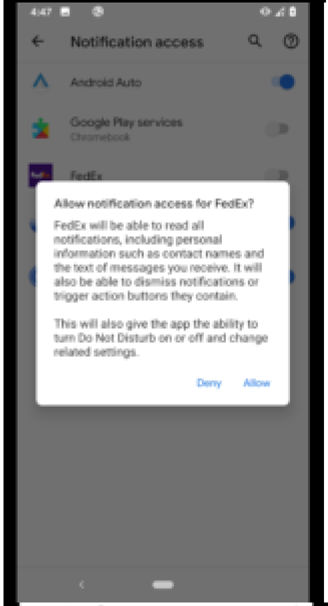


Action Required (2/2)

To finish installation you must turn on notification access for "FedEx".

Click "OK" to go to the notification settings.

OK

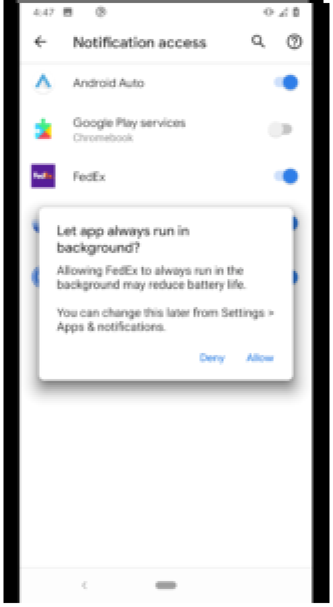


Allow notification access for FedEx?

FedEx will be able to read all notifications, including personal information such as contact names and the text of messages you receive. It will also be able to dismiss notifications or trigger action buttons they contain.

This will also give the app the ability to turn Do Not Disturb on or off and change related settings.

Deny Allow

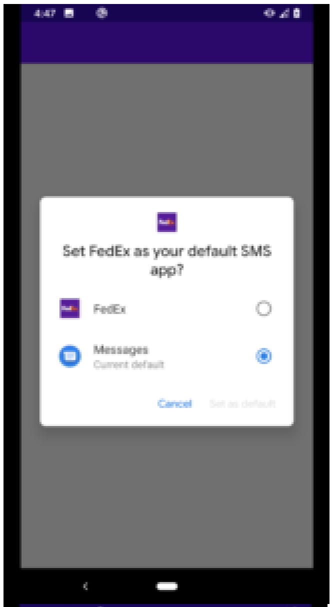


Let app always run in background?

Allowing FedEx to always run in the background may reduce battery life.

You can change this later from Settings > Apps & notifications.

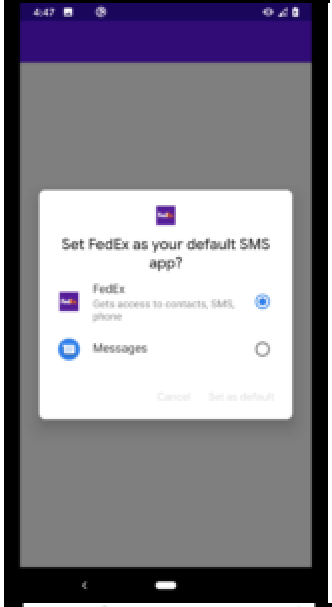
Deny Allow



Set FedEx as your default SMS app?

○ FedEx

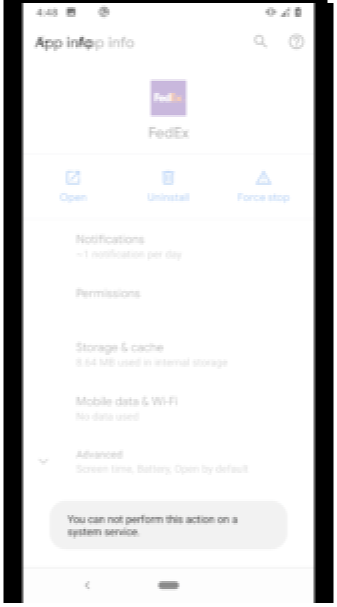
● Messages
Current default



Set FedEx as your default SMS app?

● FedEx
Gets access to contacts, SMS, phone

○ Messages



Notifications
~1 notification per day

Permissions

Storage & cache
8.64 MB used in internal storage

Mobile data & Wi-Fi
No data used

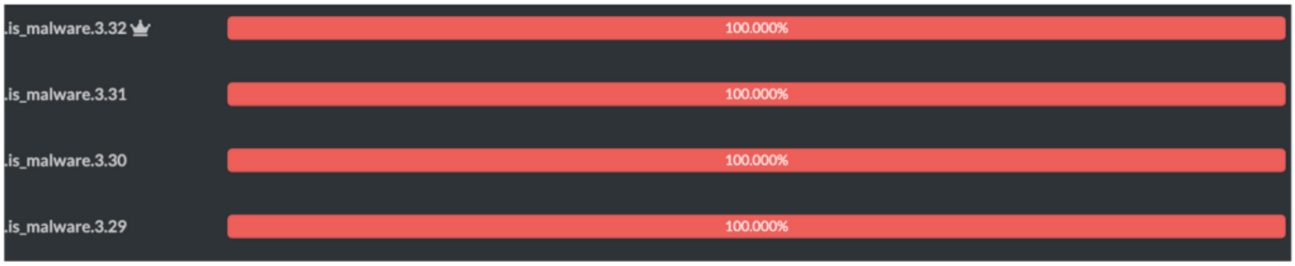
Advanced
Screen time, Battery, Open by default

You can not perform this action on a system service.

One final and very effective trick Flubot pulls on victims is collecting credit card information via a fake Google Play credit card re-verification popup. This is again performed as an overlay attack, looking just like the real popup notification. The unsuspecting victim is encouraged to fill in the necessary details without a second thought.

Zimperium zIPS customers are protected against 100% of the Flubot variants analyzed with our zero-day, on-device z9 Mobile Threat Defense machine learning engine.

As a standard protocol, the Zimperium zLabs team checks new malware samples against not only the current machine learning model but past ones as well. In the case of Flubot, Zimperium zIPS customers were protected against this aggressive credential stealing Android malware since the first variant was first reported in February 2020.



The screenshot above highlights how Flubot samples are detected with extreme accuracy by different releases of our on-device malware classifier. In the Figure, classifiers up to 3 months back in time are displayed, but samples were detected by classifiers going back over one year.
Zimperium's z9 malware engine is also able to correctly identify the family of malware ("banker" in this case) **on device**, allowing customers to create policies around specific malware types, and provide supporting forensics.

The URLs used to deliver the APK consisted 80% of compromised domains (a legitimate website whose hosting server is compromised and a malicious site is stored on it), rendering most traditional phishing prevention techniques obsolete. All reported URLs were analyzed using Zimperium's z9 ML-based phishing engine. In this case, z9 proactively blocked over 98% of the URLs, preventing the attack chain from its inception. This adds to the layer of protection and security coverage for our customers.

To ensure your Android users are protected from this latest malware, we recommend a quick risk assessment. Inside zConsole, admins can review which apps are side-loaded onto the device that could be increasing the attack surface and leaving data and users at risk.

Remediating a Flubot Infection on Android

Non-Zimperium Customers: If you have fallen victim to the Flubot malware on your Android device, immediate action is necessary to avoid more risks. First, disconnect the device from all connections, including cellular and WiFi, by putting the device into airplane mode. Next, the most effective way to remove the Android malware is through a factory reset. This will wipe the mobile device and load a fresh, clean version of the operating system. **Do not restore from backup** if it was created after the malware installation**.** Installing all your user applications fresh from Google Play ensures that you are downloading safe, approved, and secure apps. Finally, reset all your banking passwords, enable 2FA if possible, and notify your banks to increase monitoring on your account.

Not a Zimperium customer? Contact us today for a free mobile risk assessment.

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS and Chromebooks threats. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, contact us today.