STRATUS

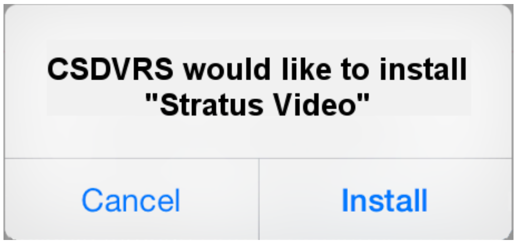
Change to sideloading apps in iOS 9 is a security win

Among the many new features in iOS 9, Apple introduced a critical adjustment enterprises should note: a change in sideloading applications that we think is a serious win for security.

Sideloading is the act of downloading an app to a device, in this case an iOS device, without going through the official App Store. Many people don’t realize it, but you can download apps via links or websites on iPhones and iPads as long as they are signed by an iOS enterprise developer certificate. These certificates are given to companies for the purpose of distributing apps easily to their own employee’s devices. However, you can use these certificates issued from Apple to install an app on any iOS device.

While enterprises often use this as a method for distributing homegrown apps, malicious actors also use sideloading (via enterprise certs in many cases bought on the black market), to distribute their malware. Wirelurker, Hacking Team’s iOS malware, and XAgent are all examples of malware that use this kind of distribution.

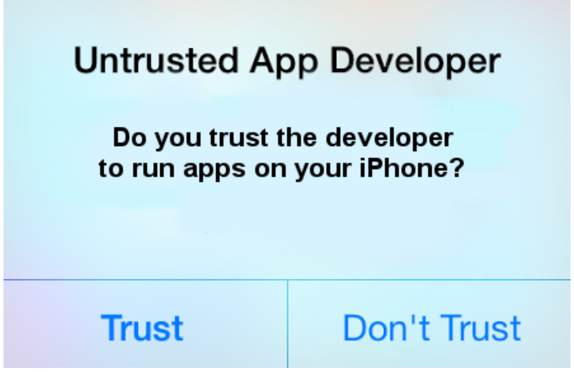
When sideloading, a person must first trust the developer associated with an app. In previous iOS versions, sideloading an app meant approving, on the spot, that you wanted to trust the developer. It was a two-step process:



CSDVRS would like to install "Stratus Video"

First, after clicking on a link in an email or on a website, a dialogue box would appear asking the person if they wanted to install the app at hand:

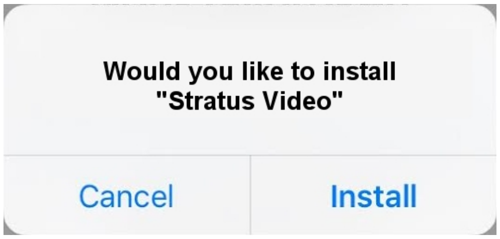
After clicking “install,” the app would download to the phone. When the person then clicked on the newly downloaded app’s icon, a second dialogue box would note that this app is from an untrusted developer and ask whether or not to trust that developer:


Untrusted App Developer

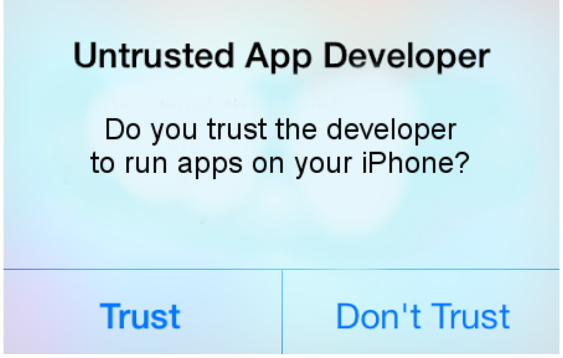
Do you trust the developer to run apps on your iPhone?

This was very easy to click through in order to get to the desired app. Now, however, users aren’t even given the option to trust the developer. Instead, they must intentionally go to settings in order to trust a developer. Here’s the new flow:

It starts off similarly, with a query on installing the app:


Would you like to install "Stratus Video"

Then, once the app has downloaded and a person goes to launch the app, they are notified that this is not a trusted developer and that they will not be able to use the app. The only option is to “dismiss” the notification. If no action is taken from there, this is the dialogue they’ll see each time they try to open the app.



Untrusted App Developer

Do you trust the developer to run apps on your iPhone?

A person can, however, trust developers via the device's settings. They go to settings, then click on General and then Profiles and are given a list of untrusted certificates.

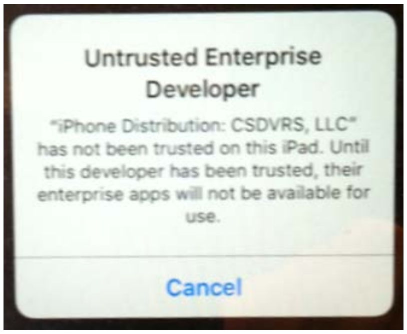
After clicking on one of the certs, the user is given the option to "trust."

After clicking trust, the cert is then remembered by the phone as trusted, and the user can launch the app.

Enterprises that distribute homegrown apps will be happy to know that apps pushed through MDM will be automatically trusted and employees will not have to follow these steps.

Quick Steps:
Untrusted Enterprise Developer message is a new iOS 9 Step when using an IPA file

Go to: Setting
Select: General
Select: Profile
Select: CSDVRS, LL
Select: Trust Developer



Untrusted Enterprise Developer

"iPhone Distribution: CSDVRS, LLC" has not been trusted on this iPad. Until this developer has been trusted, their enterprise apps will not be available for use.