From: Justin Sargent <[redacted]>
Sent: Mon, 2 Jul 2018 21:49:50 +0000 (UTC)
To: Arjan Brussee <[redacted]>
Cc: Anticheat Core <[redacted]>; Chris Babcock <[redacted]>; Chris Dyl <[redacted]>; Daniel Vogel <[redacted]>; Jack Porter <[redacted]>; Kevin Carpenter <[redacted]>; Online-Portal-leads <[redacted]>; Tim Sweeney <[redacted]>
Subject: Re: Android Unknown Sources when Updating

We can certainly do that. But there is no guarantee they installed our app via chrome as there are other browser alternatives. Packages that get installed can be marked by the installer app, as something they did. If the browser does that then we can track which app installed us.
But we can hit the prominent ones if not.

On Mon, Jul 2, 2018, 5:37 PM Arjan Brussee <[redacted]> wrote:

> hey Justin
> **on Android O**, you need to allow Chrome to "Install Unknown Apps" to install Epic Launcher. However, after that, does *Chrome* still need to have this permission to update either the launcher or FN? If the launcher self-updates, it is not going through Chrome.

If this is indeed correct, on Android O, we should ask to Disallow "Install Unknown Apps" for Chrome again after the launcher has run.

(Google raised this as one of their main concerns)

-arjan

On Fri, Jun 29, 2018 at 9:23 AM Arjan Brussee <[redacted]> wrote:

> Exactly! And google is already making global malware and virus scanners ("google play protect") that scan all apps on phone regardless from source. Very much like PC.

There also was this recent clickbait article about that developers can sign and protect APKs. Could be seen as DRM, but it's protection. Is outside google play store
https://www.androidcentral.com/google-drm-android-apps?amp

Remember on Android you cannot even trust the preinstalled OeM software because it often has tracking and malware. Plus Our Chinese phones in the office have 10x slower download speeds since they seem to route through China. (!)

-Arjan

On Thu, Jun 28, 2018 at 23:09 Tim Sweeney <[redacted]> wrote:

> That's the flow. Keep in mind, "degrading security" refers only to not locking users into Google Play as the sole software source on the platform, but is just the status quo on Windows and Mac. Google makes these warnings as scary as possible to create friction that suppresses competing sources of software, so they can get 30% of revenue from other companies' products without doing much of value m. We shouldn't buy into their closed-platform-for-the-sake-of-security FUD. Google Play itself is the #1 source of Android malware, see https://thenextweb.com/hardfork/2018/04/20/google-play-cryptocurrency-apps-malware/, https://www.zdnet.com/article/phony-android-security-apps-in-google-play-store-found-distributing-malware-and-tracking-users/, etc. Google doesn't even have humans review Google Play submissions; it's just a bunch of automated scanners.

Tim

On Jun 28, 2018, at 10:44 PM, Kevin Carpenter <[redacted]> wrote:

> > Tim you raise an interesting point, but is it fair to say that this would be our only supported platform where we are actually requiring our players to actually degrade their security (even if they only choose to do so temporarily) to install our game?
> > I want to better understand what we are asking our players to accept here. What does the current UX look like when this setting is enabled? Quick google search of several diff Android OS's within the past year found these;
> >
> > <image.png>
> <image.png>
>
> > Is this accurate with what our players will experience?
> >
> > Again, InfoSec is not that concerned about newer Android OS's that limit this setting to a given app, but for pre-Oreo this is a global setting. So if this is left enabled we are perhaps indirectly leaving our players at risk...
>
> If this is acceptable risk and I'm beating a dead horse, then I am totally cool with moving on, just want to make sure InfoSec is doing our part to advise folks of potential risk here. :)
>
> KC

On Thu, Jun 28, 2018 at 8:13 PM, Justin Sargent <[redacted]> wrote:

> We tested the updating of products like fortnite, but also the self updating of the Epic Games app, which falls under your scenario. Both require unknown sources.

On Thu, Jun 28, 2018, 8:11 PM Jack Porter <[redacted] wrote:

> Hi Justin,
> Technically can an apk update itself without Unknown Sources? Could the launcher download the updated Fortnite apk, put it on sdcard and then trigger an intent on the existing Fortnite to update itself?

- Jack

On Fri, Jun 29, 2018 at 9:08 AM, Tim Sweeney <[redacted]> wrote:

> Web browsers never auto-run downloaded APKs on Android, so from this point of view, running Android with "allow unknown sources" on is exactly like running Windows 10 in its default state, and I'm fine with that.

Tim

On Jun 28, 2018, at 7:46 PM, Kevin Carpenter <[redacted] wrote:

> Thanks Justin/Tim
> With this new info perhaps it's worthwhile to revisit the security risk here with this option enabled.

I'm not particularly concerned about allowing unknown sources as needed. Current security best practice is to temporarily enable it when needed to install apps from trusted\reputable sources. I'm sure we'll get some negative press for introducing an App that require this to be turned on...

However, for Pre-Andrioid-Oreo devices, I am very concerned about the vulnerability our game and stance to not encourage the disabling of this setting introduces. As a reminder this is a global setting for

On Thu, Jun 28, 2018 at 5:03 PM, Tim Sweeney <[redacted]> wrote:

> Thanks for the update. Yes, I agree, given this new information, we shouldn't encourage users to turn Unknown Sources off after were installed.

Tim

On Jun 28, 2018, at 4:34 PM, Justin Sargent <[redacted]> wrote:

Hey everyone,
We ran some more tests regarding the behavior around Unknown Sources when applying updates and it appears I've been spouting incorrect information.

Unknown Sources is **required** even to apply updates to already installed apks. We had tested this before but obviously, we had done it wrong. To be clear, Unknown Sources is required for self-updates of the Epic Games app, as well as, updates of the products it installs.

We've tested this on 3 different manufacturers, 4 different sdk versions, and 1 external apk updater app used by the community.

My apologies for the bad information.

This doesn't really have an impact on phones on version O and newer. We were not planning to encourage the user to disable the Unknown Sources option as it isn't a security concern.

We had been planning to encourage users to disable Unknown Sources for older phones which can pose a security risk. Doing so would greatly add friction to future updates and I assume means we would not want users to enable and disable the setting every update.

Given the sentiment around feature at the last exec review, I'm planning to **not** move forward with encouraging users to disable Unknown Sources.

@Anti-cheat - I'm happy to talk more about alternatives to keep our users safe or continue with the plan to promote disabling if we get agreement from execs.

-Justin

--
Kevin Carpenter
Information Security Architect
Epic Games

--
Kevin Carpenter
Information Security Architect
Epic Games