Google Play has been spreading advanced Android malware for years

reader comments

56 with 47 posters participating, including story author

Share this story

Hackers have been using Google Play for years to distribute an unusually advanced backdoor capable of stealing a wide range of sensitive data, researchers said on Tuesday.

Researchers from security firm Kaspersky Lab have recovered at least eight Google Play apps that date back to 2018, a Kaspersky Lab representative said, but based on archive searches and other methods, the researchers believe malicious apps from the same advanced group seeded Google's official market since at least 2016.

Google removed recent versions of the malware shortly after the researchers from Kaspersky, and earlier fellow security firm Dr. Web, reported them. Apps from earlier were already removed, and it's not clear what prompted the move. Third-party markets have also hosted the backdoored apps, and many of them remain available.

Command-and-control domains were registered as early as 2015, raising the possibility the operation goes back earlier than 2016. Code in the malware and command servers it connects to contain several overlaps with a known hacking group dubbed OceanLotus (aka APT32, APT-C-00, and SeaLotus), leading

researchers to believe the apps are the work of that advanced group.

Repeatedly bypassing Google security checks

Attackers behind the campaign used several effective techniques to repeatedly bypass the vetting process Google uses in an attempt to keep malicious apps out of Play. One method was to initially submit a benign version of an app and add the backdoor only after the app was accepted. Another approach was to require few or even no permissions during installation and to later request them dynamically using code hidden inside an executable file. One of the recent apps posed as a browser cleaner.

Within time, the apps provided a backdoor that collected data about the infected phone, including the hardware model, the Android version it ran, and the apps that were installed. Based on that information, the attackers could use the malicious apps to download and execute malicious payloads specific to a particular infected device. The payloads could collect locations, call logs, contacts, text messages, and other sensitive information.

By customizing the payloads and not loading down a device with unneeded components, the attackers were further able to evade detection. In a twist, a later app contained the malicious payload in the downloaded APK itself.

“Our main theory about the reasons for all these versioning maneuvers is that the attackers are trying to use diverse techniques to achieve their key goal, to bypass the official Google marketplace filters,” Kaspersky Lab researchers Alexey Firsh and Lev Pikman wrote in a post. “And achieve it they did, as even this version passed Google’s filters and was uploaded to Google Play Store in 2019.”

Google officials declined to say how or even if the company is working to prevent malicious apps from using the described techniques used to bypass the app-vetting process. Instead, the officials issued a statement that said: “We’re always working to improve our detection capabilities. We appreciate the work of the researchers in sharing their findings with us. We’ve since taken action against all the apps they identified.”

Enter PhantomLance

Most of the apps contained functionality that require that phones be rooted. That would require apps to run on devices with known rooting vulnerabilities or for the attackers to exploit flaws that aren’t yet known to Google or the general public. Kaspersky Lab researchers didn’t find any local privilege escalation exploits in the apps themselves, but they haven’t ruled out the possibility such attacks were used. In an email, a researcher wrote:

> *However, there is an important feature, which can partly answer this question: the malware is able to download and execute additional payloads from c2 servers. So the following scenario is possible—at first they could steal some sort of device information like OS version, list of installed apps, etc. Then, based on this initial information, if this particular infected device looks attractive to exfiltrate, the attackers could send a specific payload suited for its Android version which could be LPE exploit for example. We were unable to get any of these payloads; as I mentioned, these guys are pretty good at OPSEC, so we cannot confirm what these payloads exactly look like.*

Another novelty attesting to the sophistication of the apps: when root privileges are accessible, the malware uses a reflection call to an undocumented programming interface called “setUidMode” to obtain the permissions without

requiring user involvement. Apps identified by Kaspersky Lab included:

Package name	Google Play persistence date (at least)
com.zimice.browserturbo	2019-11-06
com.physlane.opengl	2019-07-10
com.unianin.adsskipper	2018-12-26
com.codedexon.prayerbook	2018-08-20
com.luxury.BeerAddress	2018-08-20
com.luxury.BiFinBall	2018-08-20
com.zonjob.browsercleaner	2018-08-20
com.linevialab.ffont	2018-08-20

Kaspersky Lab researchers have dubbed the campaign PhantomLance. Based on the overlaps mentioned earlier, the researchers have medium confidence that the years-long series of attacks are the work of OceanLotus. Researchers say the group primarily attacks Asian governments, dissidents, and journalists, with a particular focus on targets adverse to the interests of Vietnam. App names and other strings are written in Vietnamese. Previous reports on OceanLotus are here, here, and here.

This isn’t the first time advanced hackers with ties to wealthy governments have used Play to spread malware. Earlier this year, researchers found Google Play apps developed by SideWinder, the code name for a malicious hacking group that has been targeting military entities since at least 2012. In 2019, Egypt used the official Google market to infect its own citizens.

There’s little chance that people outside a very narrow range of demographics have been infected by this group. Those who want to check just to be sure can find indicators of compromised apps in the previously mentioned post located

here.

https://arstechnica.com/?p=1672040