Triada: organized crime on Android

By John Snow

Published: 2016-03-03 · Archived: 2026-04-06 03:10:24 UTC

You know how armies typically move: first come the scouts to make sure everything is ok. Then the heavy troops arrive; at least that was how it used to be before the age of cyber wars. It turns out, that Trojans behave quite the same way.

There are a lot of small Trojans for Android capable of leveraging access privileges, in other words — gaining root access. Our malware analysts Nikita Buchka and Mikhail Kuzin can easily name 11 families of such Trojans. Most of them are almost harmless — all they did until recently was injecting tons of ads and downloading others of their kind. If you want to know more about them — our researchers have an article about them on Securelist.

If you follow the military analogy — those are the scouts. As you probably have noticed, gaining root access gives them the capability to download and install applications — that's the reason why once one of them get into the system, in a few minutes there are all the others. But our researchers have predicted that these small Trojans would certainly be used to download some really bad malware that can actually harm the owners of the infected devices.

And that's exactly what has happened recently. Small Trojans like Leech, Ztorg and Gopro now download one of the most advanced mobile Trojans our malware analysts have ever encountered — we call it Triada.

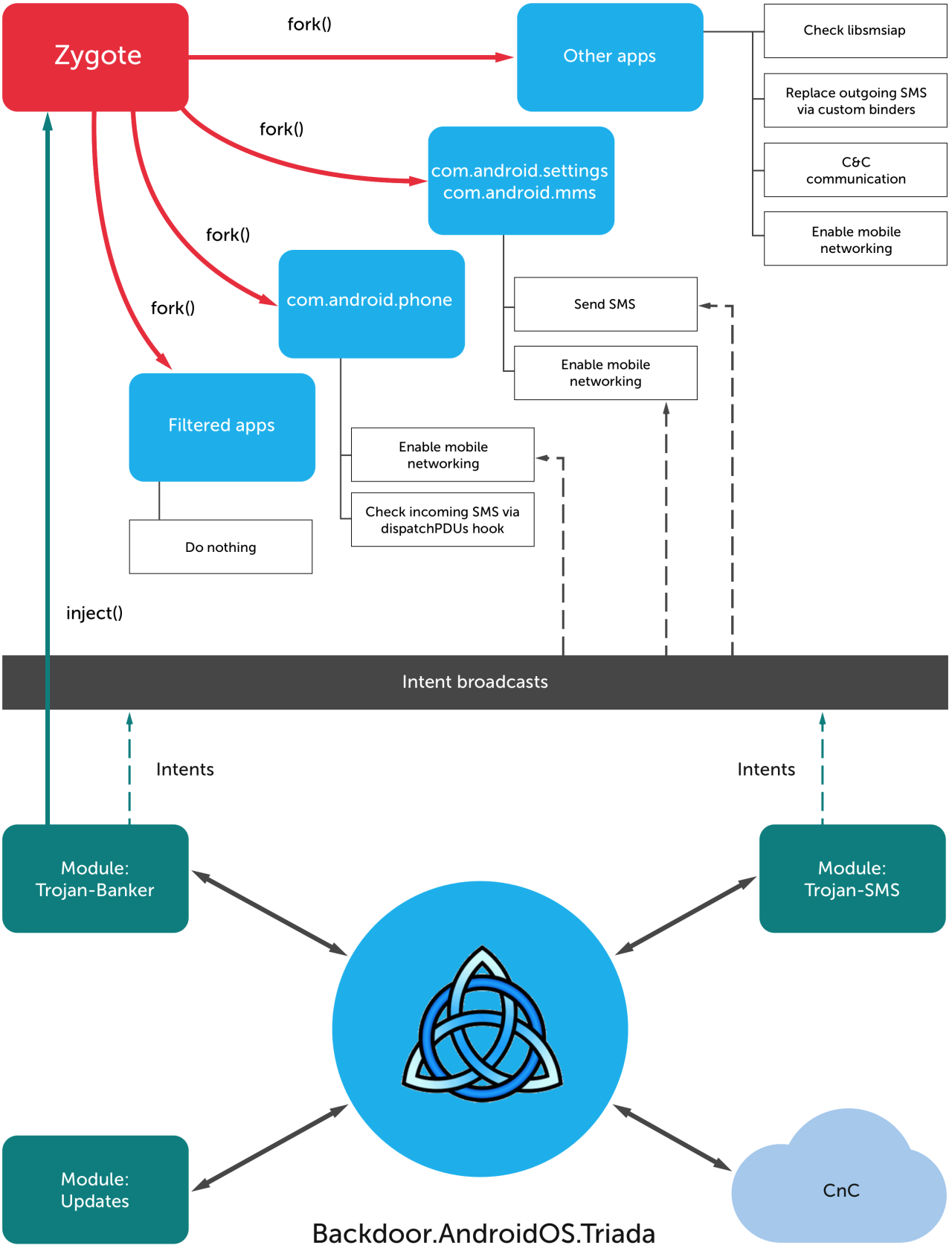
Triada is a modular mobile Trojan that actively uses root privileges to substitute system files and exists mostly in the device's RAM, which makes it extremely hard to detect.

The dark ways of the Triada

Once downloaded and installed, the Triada Trojan first tries to collect some information about the system — like the device model, the OS version, the amount of the SD card space, the list of the installed applications and other things. Then it sends all that information to the Command & Control server. We have detected a total of 17 C&C servers on 4 different domains, which probably means the bad guys are quite familiar with what redundancy is.

The C&C server then responds with a configuration file, containing the personal identification number for the device and some settings — the time interval between contacting the server, the list of modules to be installed and so on. After the modules are installed they are deployed to the short term memory and deleted from the device storage, which makes the Trojan a lot harder to catch.

There are two more reasons why Triada is so hard to detect and why it had impressed our researchers so much. First, it modifies the Zygote process. Zygote is the core process in the Android OS that is used as a template for every application, which means that once the Trojan gets into Zygote, it becomes a part of literally every app that is launched on the device.



Second, it substitutes the system functions and conceals its modules from the list of the running processes and installed apps. So the system doesn't see any strange processes running and thus does not cry the alarm.

Those are not the only system functions Triada modifies. As our researchers discovered, it also lays its hands on the outgoing SMS and filters the incoming ones. That is actually how the bad guys decided to monetize the Trojan.

Some applications rely on SMS when it comes to in-app purchases — the transaction data is transferred via a short text message. The main reason for developers to choose SMS over traditional payments via Internet is that in the case with SMS no Internet connection is required. Users do not see those SMS because they are processed not by the SMS app, but by the app that has initiated the transaction — e.g a free-to-play game.

Triada's functionality allows it to modify those messages, so the money is sent not to some app developer, but to the malware operators. Triada steals the money either from the users — if they haven't succeeded in purchasing whatever they wanted, or from the app developers, in case the user has completed the purchase successfully.

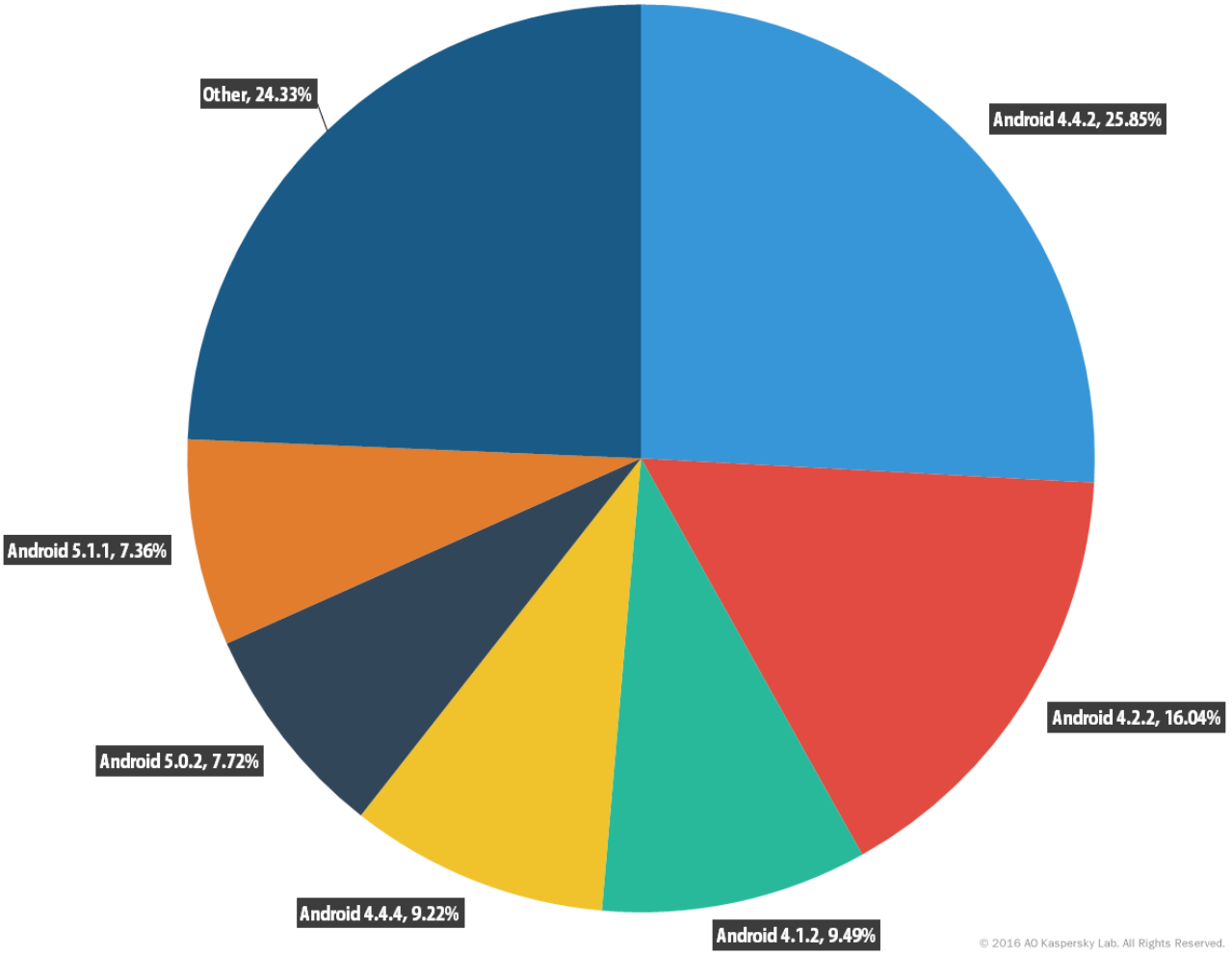
For now, that is the only way how cybercriminals can profit from Triada, but don't forget that it's a modular Trojan, so it can be turned into literally everything on one command from the C&C server.

Fighting organized crime in your phone

One of the main problems with Triada is that it can potentially hurt a LOT of people. As we've mentioned earlier, Triada is downloaded by smaller Trojans that have leveraged the access privileges. And our researchers estimate that in every 10 Android users 1 was attacked by either one or several of those Trojans during the second half of 2015, so there are millions of devices with a huge possibility of being infected with Triada.

So, what can you do to protect yourself from this stealthy beast?

1. Never forget to update your system. It turns out that those smaller Trojans face serious problems trying to get root access on Android 4.4.4 and above, because a lot of vulnerabilities were patched in these versions. So if you have Android 4.4.4 or some more recent version of this OS on your device, your chances of getting infected with Triada are significantly lower. Yet our statistics says that about 60% of Android users are still sitting with Android 4.4.2 and below.



2. Better not to take any chances at all, no matter which version of the OS you use. So we recommend installing an anti-virus solution on your Android device. detects all three of Triada's modules, so it can save your money from cybercriminals that are behind Triada. Just don't forget that the scan does not run automatically in the free version.

But all in all Triada is yet another example of a really bad trend: malware developers are taking Android seriously, and the latest samples are almost as complex and hard to withstand, as their Windows-based kin. The only good way to fight all these threats is to be proactive, and so a good security solution is a must.

Source: https://www.kaspersky.com/blog/triada-trojan/11481/