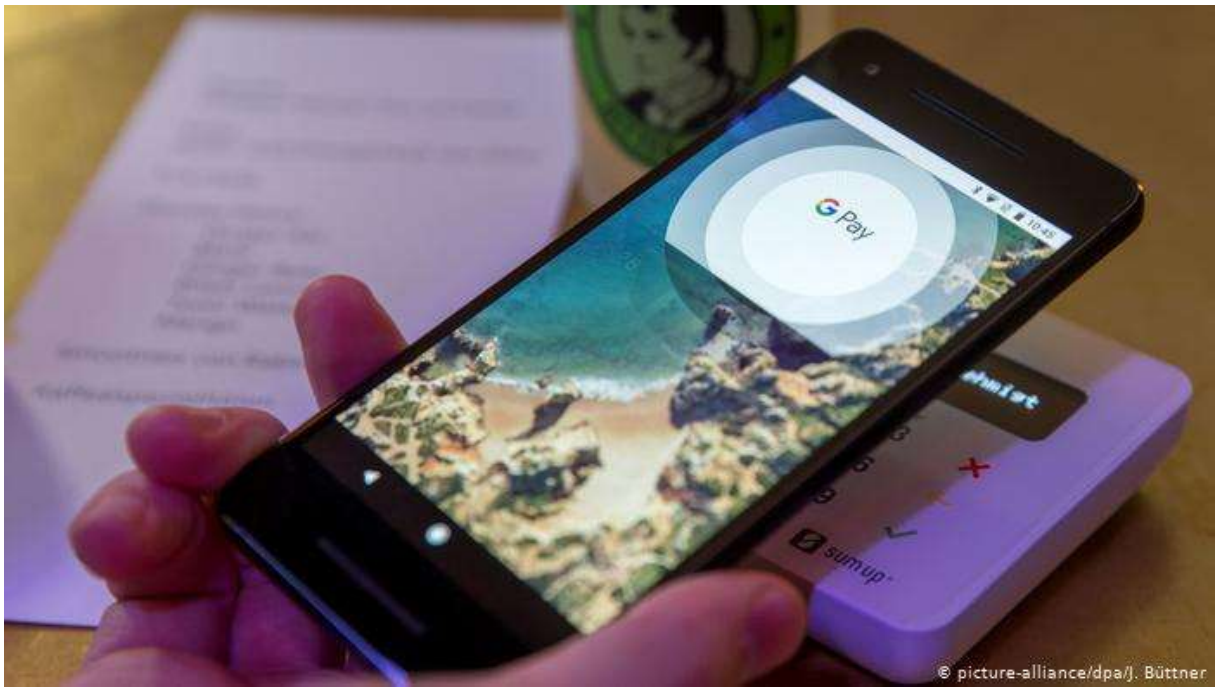
CYBERSECURITY

Pre-installed malware: Your Android phone may spy on you!

US researchers have discovered a large number of vulnerabilities in smartphones. Malware and backdoors are often pre-installed at the root level, and there is nothing a regular user can do about it.



Most people are aware that their cellphone may have certain vulnerabilities and that they should be careful about the settings they choose, cautious when using the device to send and receive sensitive data and wary about what kind of apps to install.

But would you have imagined that a brand-new mobile phone straight from the factory comes with pre-installed spyware? The phone may have an invisible app that manages to obtain elevated admin privileges and do things that you as a user can hardly detect and cannot disable.

That app may even send out data packages to some remote server at night when you as the owner are sleeping and your cellphone is turned off.

That's not fiction, say Angelos Stavrou and Ryan Johnson from the US company Kryptowire.

The cybersecurity experts talked about the vulnerabilities at the Cirosec IT-Defense Conference in Bonn in February.

Read more: Munich Cyber Security Conference considers a world of digital threats

Data extraction camouflaged as 'lovely fonts'

One of the most blatant examples of spyware that Stavrou and Johnson presented includes two tiny programs whose purpose appears to allow users to change and embellish fonts. The programs are called lovelyfonts and lovelyhighfonts.
The Kryptowire experts found that lovelyfonts and lovelyhifonts cooperate in attacking the device. The functionality of the malware is split in two: One of the apps is in charge of the communication; the other functions as a container.
Both appear to the layperson to be inconspicuous applications. They are not accessible through the launcher, which means most users will never even notice them. But they open a backdoor to the computer for possible attackers and also transfer encrypted data to external storage in Shanghai, China.
The server that received the data stopped responding to network requests in November 2018, but that does not mean the dangers posed by pre-installed apps are over.

Read more: TOR, Psiphon, Signal and Co.: How to move unrecognized on the internet

Many more vulnerabilities identified

"Just in November 2019, we disclosed around 146 common vulnerabilities across 26 different vendors," Stavrou says. And he announced that they have already identified " tons more" that they are going to make public soon.

The number of vulnerabilities is likely to increase, Angelos Stavrou warns.

"So it's not something that will end with this disclosure," he warned, adding that "this is not the problem of a specific vendor or a specific company."
Some of the identified vulnerabilities allow attackers to get into the phone remotely, activate keyloggers, take screenshots or simply record everything the owner sees, does, says and hears, including the typing, deleting and correcting of passwords.
"All the apps do not give any sign that they are running" Stavrou adds. "They can be running in the background, collecting all this information without your knowledge."

Read more: Google unveils 'unprecedented' iPhone security flaw

Who is affected?

The problem of pre-installed vulnerabilities is most likely not limited to Android. Similar bugs may also exist in other operating systems. But the sheer number of Android devices makes them a more attractive target to attackers. And the way the system software is

developed and distributed makes it easier for them to get a foothold in the supply chain of the software.

Of the estimated 5 billion people who are using mobile devices, 85% are using models based on a version of the Android operating system. Besides smartphones, Android is also running on a variety of other connected devices like TVs or car entertainment systems. The vulnerabilities extend to those, too.

"Once applications are running on the infotainment system, if they cross the security boundary and potentially get on the car's CAN bus, they can control steering, braking and have very dire effects" Ryan Johnson warns.

Why Android?

It has a lot to do with the way cellphone developers and producers choose the software for the respective model and how they set up their devices.

"Android is open-source," Johnson points out. Google, which bought Android in 2005, makes the code available through the Android Open Source Project (AOSP).

Part of the problem is the vulnerable software supply chain, Ryan Johnson points out.

Software developers, therefore, can freely design their system by choosing from a variety of apps with different functionalities in the AOSP marketplace. Producers and vendors then pick the apps they believe will set their specific product apart from those of other manufacturers.

"Any vulnerability in the AOSP that is going to be in the core Android software gets propagated to the vendors", Johnson warns. "Any vendors that are using this version are going to inherit that vulnerability."

Read more: WannaCry buster Marcus Hutchins pleads guilty to creating malware

Who is in charge of fixing the problem?

Most apps that vendors have pre-installed are embedded at the root level of the respective device. It means that users cannot change, disable or delete those software components.

And many of the components at the root level have elevated privileges: For example, they can open the door to install firmware updates automatically. And malware is able to abuse those privileges.

Because the software comes from a large variety of different sources, the experts at Kryptowire had a hard time even getting the attention of the smartphone producers and vendors whose products had the bugs built into their system.

"When we disclosed the vulnerabilities, we had problems identifying who the responsible party was and actually seeing through who was going to fix it," Stavrou said. "Even if we report something, it takes a long time for them to identify and fix it. And in many cases, we did not get responses from parties that were in foreign countries [outside the US]."

While Kryptowire has developed a software solution to automatically detect the vulnerabilities, it is not yet a solution for ordinary customers buying a new device at their local electronics store. Even if you know what bugs your phone has, you can't necessarily fix them yourself.

And with new software components hitting the market at a breathtaking pace, the bugs and vulnerabilities in pre-installed software are more likely to increase in number than come to an end anytime soon.