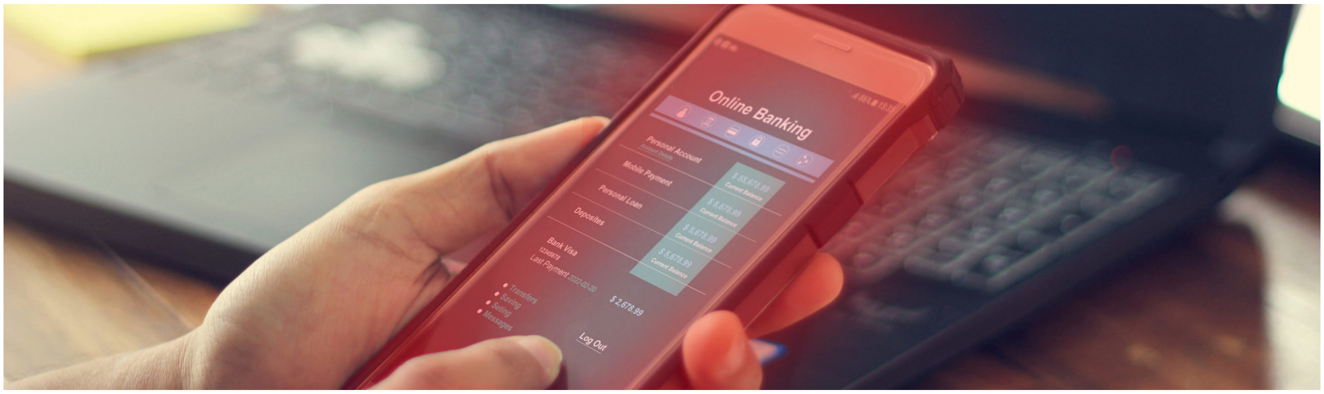
Promon discovers FjordPhantom, Android banking malware

promon.co/security-news/fjordphantom-android-malware/

Posted on November 30, 2023 12:23 am



Malware

Promon discovers new Android banking malware, “FjordPhantom”

By Benjamin Adolphi

Promon has discovered a new type of Android malware, which the company has dubbed FjordPhantom, for its illusiveness and ability to spread covertly. This blog post explores what FjordPhantom is and how it works.

Background

Through longtime Promon partner i-Sprint, our Security Research team received reports of a new Android malware spreading in Southeast Asia in early September, primarily Indonesia, Thailand, and Vietnam. Promon also believes that the malware is active in Singapore and Malaysia. Spreading primarily through messaging services, it combines app-based malware with social engineering to defraud banking customers. In discussions with banks in the region, Promon has learned that one customer was defrauded out of 10 million Thai Baht (approximately $280,000) at the time of writing.

Promon has received a sample of that malware, which was pulled from an end-customer’s device. This sample targets one specific bank but includes code that can also target other banking apps. We did not manage to find more samples of that malware, and we were also unable to find any public information on this malware, so we performed our own technical analysis. Android banking malware is omnipresent, and new malware families are discovered regularly. We found this malware unique because it uses virtualization to attack applications, which we have not seen malware do before. Virtualization typically has been used as a tool in reverse engineering.

How FjordPhantom spreads

FjordPhantom spreads primarily through email, SMS, and messaging apps. A user is prompted to download an app that looks like their bank's own app. In reality, the downloaded app contains the real bank's Android app, but it is run in a virtual environment with additional components that enable attacks on the app.

After downloading, the user is subjected to a social engineering attack. Typically, this is backed by an attack team in a call center. They purport to be customer service for the bank, guiding the customer through the steps to run the app. The malware enables the attackers to follow the user's actions, allowing them to either guide the user to perform a transaction or use the process to steal credentials. They can use these credentials for additional attacks.

How FjordPhantom uses virtualization

The malware is put together using different open source/free projects that can be found on Github. Most importantly, it embeds a virtualization solution and a hooking framework to perform its attacks. We have chosen to omit certain technical details and the names of these tools to limit the reproducibility of the attack.

Virtualization solutions allow the installation and running of apps in a virtual container. They have become quite popular on Android in recent years. There are legitimate reasons for using such solutions, and Google accepts them because many of these apps can be downloaded from the Google Play Store. A popular reason for using these solutions is to be able to install the same app multiple times to log into them with different accounts. This is something that is usually not possible on Android.

What exactly a "virtual container" means in this context varies between different virtualization solutions.

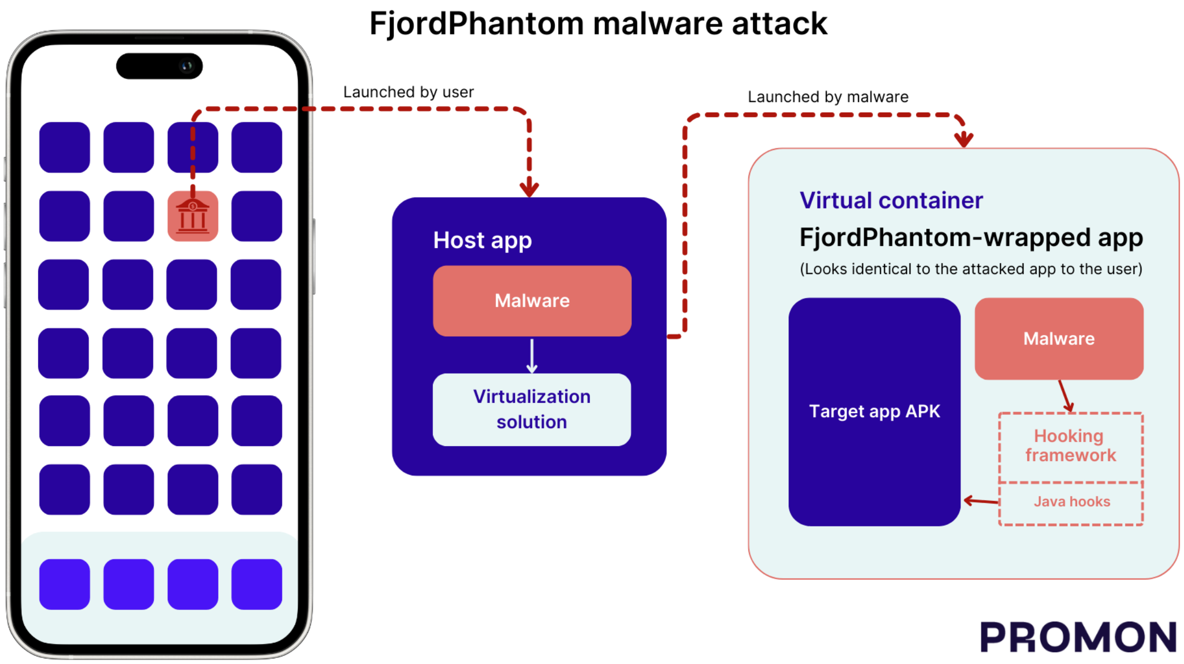
In the case of the solution used by FjordPhantom, the virtualization solution is an app that can host different apps. The hosted apps are installed into a virtual filesystem. When a hosted application is launched, the solution creates a new process that loads the application into it and then launches it. From the point of view of the Android system, there is only one app (the host). This means that when the hosted apps are launched, they would also see that they are being run in the context of the host app, which would cause many issues with different kinds of apps because they expect to be run in a well-defined environment. In addition, as already mentioned, the hosted apps are installed into a virtual filesystem. So, for the hosted apps to execute normally, the virtualization solution heavily relies on hooking, modifying different properties of the Android runtime environment, and proxying a lot of what the hosted applications do.

Virtualization breaks the Android sandbox

The dangerous part about loading apps into virtual containers like this is that it breaks the Android sandbox. Usually, every app on Android runs isolated in its own sandbox. In the case of virtualization solutions like this, different apps all run in the same sandbox. This enables them to access each other's files and memory and debug each other. This also means that virtualization solutions can be a good choice for attackers. Usually, breaking the sandbox would require root access on a device. However, this is not required when apps are installed into the same sandbox. This makes attacks easier because there is no need to root the device, and it also prevents root detection, a popular check for security-critical apps. Because of that, virtualization solutions have become quite popular among attackers. Until now, all the attacks that we have seen involving virtualization solutions would be performed by an Android device user trying to attack an app they have installed. This can be useful to analyze apps with debuggers like gdb or lldb or hooking frameworks like Frida, or cheating in games using tools like GameGuardian without root access.

In addition to that, virtualization solutions like the one used by the malware can also be used to inject code into an application because the virtualization solution first loads its own code (and everything else found in its app) into a new process and then loads the code of the hosted application. Traditionally, the most popular code injection method has been repackaging the application with additional code. Therefore, many security-critical apps perform detection of repackaging, which makes attacks harder to pull off. However, using virtualization to inject code will bypass these detections because the original application is not modified.

How FjordPhantom works



FjordPhantom uses the virtualization solution described above. It embeds the APK of a specific banking app that it targets, and when it is launched, it installs and launches the embedded app in a virtual container. To the user, it looks like the banking app launches without visible traces of the virtualization solution. Here's what makes FjordPhantom unique: Compared to previous uses of virtualization attacks we have seen, it is not the device user that invokes the virtualization, but the Android malware does so without the user's knowledge.

Hosting the target application in a virtual container enables the malware to perform its attack. As described above, it has many attack possibilities. In the case of FjordPhantom, virtualization is mainly used to load additional code into the process of the hosted application. The code that gets injected is the code of the actual malware itself and a hooking framework that the malware uses.

FjordPhantom itself is written in a modular way to attack different banking apps. Depending on which banking app is embedded into the malware, it will perform various attacks on these apps. In the case of our malware sample, one specific banking app is embedded and targeted directly. But in the malware code, we have seen that it can also target seven other banking apps. There are a couple of different attacks that the malware performs on the apps it targets, which are described below.

How FjordPhantom uses hooking frameworks

FjordPhantom uses the hooking framework it embeds to hook into APIs that apps typically use to determine if Accessibility services are turned on and which services are currently enabled. This is a standard method that apps use to detect malicious Android screenreaders, and by hooking these APIs and returning false information, screenreader detection methods can be bypassed. This makes it possible for attackers to use screenreaders to grab sensitive information from the application's screen without the application knowing about it.

Similarly, the Android malware uses the hooking framework it embeds to hook into APIs related to GooglePlayServices, making it seem like they are not available. The GooglePlayServices are used by SafetyNet, commonly used to detect rooting. By pretending GooglePlayServices are unavailable, apps trying to detect root might be tricked into skipping the SafetyNet part of their rooting checks.

For some apps, the malware also hooks into UI functionality related to dialog boxes, and if they contain certain text, it will close them automatically. We have investigated these dialog boxes in the target apps. They warn the user that some potentially malicious activity has been detected on their device. Most of these dialog boxes cannot be closed, preventing the user from using the app in a potentially malicious scenario. By preventing the user from seeing these dialog boxes and letting the user use the app normally, the malware enables further attacks on these apps without raising suspicion.

Lastly, we have also seen that the malware is placing a lot of hooks that log different things that the target applications do without modifying their behavior. This is most likely debugging functionality left in the malware to develop attacks on different apps. This indicates that FjordPhantom is under active development and potentially will evolve or has evolved to target other apps already.

Conclusion

FjordPhantom is a sophisticated Android malware used to commit real-world fraud. We encourage Promon financial services customers in the affected region to upgrade to one of the latest versions of Promon SHIELD™. We advise end users to exercise vigilance when downloading apps from untrusted sources or outside the primary app stores.