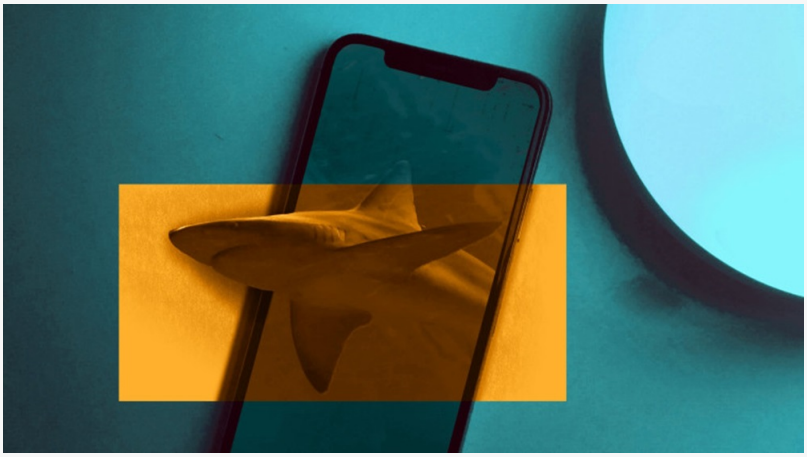
Predatory SpyLoan apps — loan sharks expand their range to Android, ESET Research finds



DUBAI , DUBAI, UNITED ARAB EMIRATES, December 15, 2023 /EINPresswire.com/ -- This year, ESET researchers have observed alarming growth in deceptive Android loan apps, which present themselves as legitimate personal loan services, promising quick and easy access to funds. Despite their attractive appearance, these services are in fact designed to defraud users by offering them high-interest-rate loans endorsed with deceitful descriptions, all while collecting their victims' personal and financial information in order to blackmail them. ESET products therefore recognize these apps using the detection name SpyLoan, which directly refers to their spyware functionality combined with loan claims. SpyLoan apps are marketed through social media and SMS messages, and are available for download from dedicated scam websites, third-party app stores, and also Google Play.

ESET is a member of the App Defense Alliance (ADA) and an active partner in the malware mitigation program, which aims to quickly find Potentially Harmful Applications and stop them before they ever make it onto Google Play. As an ADA member, ESET identified 18 SpyLoan apps and reported them to Google, who subsequently removed 17 of these apps from their platform. These apps had a total of more than 12 million downloads from Google Play before their removal. The final app listed changed its behavior; ESET therefore no longer detects it as a SpyLoan app.

Every instance of a particular SpyLoan app, regardless of its source, behaves identically due to its identical underlying code. It doesn't matter whether the download came from a suspicious website, a third-party app store, or even Google Play — the users will experience the same functions and face the same risks, regardless of where they got the app.

According to ESET telemetry, the enforcers of these apps, who blackmail and harass their victims,

even with death threats, operate mainly in Mexico, Indonesia, Thailand, Vietnam, India, Pakistan, Colombia, Peru, the Philippines, Egypt, Kenya, Nigeria, and Singapore. ESET researchers believe that any detections outside of these countries are related to smartphones that have, for various reasons, access to a phone number registered in one of these countries. There are currently no active campaigns targeting European countries, the USA, or Canada.

Apart from data harvesting and blackmail, these services present a form of modern-day digital usury, which refers to the charging of excessive interest rates on loans, taking advantage of vulnerable individuals. Victims of these apps claim the total annual cost (TAC) of such loans is much higher than stated, and the loan tenure is much shorter than stated. In some cases, borrowers were pressured to pay off their loans in five days, instead of the stated 91 days, and the TAC of a loan was anywhere between 160% and 340%.

“These malicious applications exploit the trust that users place in legitimate loan providers, using sophisticated techniques to deceive people and steal a very wide range of personal information,” says ESET researcher Lukáš Štefanko, who uncovered many of the SpyLoan apps. “It is crucial for individuals to exercise caution, validate the authenticity of any financial app or service, and rely on trusted sources. By staying informed and vigilant, users can better protect themselves from falling victim to such deceptive schemes,” he adds.

ESET Research has traced the origins of the SpyLoan scheme back to 2020. Once a user installs a SpyLoan app, they are prompted to accept the terms of service and grant extensive permissions to access sensitive data stored on the device. According to the privacy policies of these apps, if those permissions are not granted, the loan will not be provided. To complete the loan application process, users are also compelled to provide extensive personal information.

The data that is usually exfiltrated to the Command and Control (C&C) server includes the user’s list of accounts, call logs, calendar events, device information, lists of installed apps, local Wi-Fi network information, and even information about files on the device. Additionally, contact lists, location data, and SMS messages are vulnerable. To protect their activities, the perpetrators encrypt all the stolen data before transmitting it to the C&C server. While legitimate financial institutions are required to collect personal information about their customers, identity verification and risk assessment can be done using much less intrusive data collection methods. ESET Research believes the real purpose of the permissions requested by SpyLoan apps is to spy on their users and harass and blackmail them and their contacts

After such an app is installed and personal data is collected, the app’s enforcers start to pressure their victims into making payments, even if — according to the reviews — the user didn’t apply for a loan or applied but the loan wasn’t approved. Such practices have been described in the reviews of these apps on Facebook and on Google Play.

“There are several reasons behind the rapid growth of SpyLoan apps. One is that the developers of these apps take inspiration from successful FinTech — financial technology — services, which

leverage technology to provide streamlined and user-friendly financial services," explains Štefanko.

For more technical information about deceptive SpyLoan apps, check out the blog post "Beware of predatory fin(tech): Loan sharks use Android apps to reach new depths." Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
