Lookout Coverage – InfectedAds / AgentSmith

Lookout is constantly discovering and researching new threats to protect and advise our customers

Background and Discovery Timeline

In April 2019, Lookout researchers initially investigated InfectedAds (also known as AgentSmith), a family of applications that are able to infect programs installed on Android devices. This family can add its own components to a target Android Package (APK) without changing its digital signature. By doing so, it can install infected applications masked as an update to replace the original version of the application. Infected versions of many applications such as HD Camera, Euro Farming Simulator, and others were found in 3rd party app stores and downloaded to thousands of devices.

Key Facts

1. Leverages the known vulnerabilities to gain access to the device and carry out attack.
2. Tricks user into unknowingly installing a dropper app, which decrypts and installs the main malware.
3. Malware prompts the user to install a false update, which is actually a malicious version of the original app

Capabilities and Affected Parties

The infection process has three main stages. First, the victim installs a dropper app, which has a malicious Feng Shui Bundle encrypted in the asset folder. Then, the dropper decrypts and installs the core malware, which is later responsible for malicious patching and app updates. Finally, the main malware extracts the list of installed applications on the device. If they match with a pre-existing list, the malware will extract the base APK of the legitimate app and patch it with malicious ad modules. InfectedAds generates ads that can be used for financial gain by the attacker. However, the malware could easily be leveraged for much more dangerous activity such as stealing login credentials for banking, travel, or corporate apps because of its discreet nature.

How Lookout Detects and Protects Against Threats like InfectedAds

Lookout Security Intelligence teams are continuously discovering and researching new threats to protect and advise our customers by combining static and dynamic analysis with our machine learning engine. In the case of InfectedAds, we have analyzed thousands of samples of this family installed across our data corpus of 170 million devices in order to get the most accurate understanding of the malware. While it didn't appear in the media until mid-2019, devices with Lookout installed have been protected against InfectedAds since April 2018. Lookout also protects against other sophisticated malware that could normally go undetected.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Threat Advisory