Lookout Discovery - eSurvAgent

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

Background and Discovery Timeline

Early in 2018, Lookout investigated eSurvAgent, a sophisticated Android surveillanceware agent with links to an Italian company called eSurv, formerly known as Connexxa. Also known as Exodus, the agent seems to have been under development for at least five years and is a multi-stage threat with a dropper, a large second stage payload, and a final stage to obtain root access to the device. Recently, Lookout researchers uncovered the iOS component of the same threat, which was delivered to users through phishing sites that imitated customer support sites. Furthermore, through the abuse of Apple's enterprise provisioning system, eSurv applications were signed with legitimate Apple-issued certificates.

Key Facts

1. Appears to have been created for the lawful intercept market
2. Works by abusing Apple's enterprise app provisioning system.
3. Functionality is controlled through push payloads, so an attacker can specify what data is to be retrieved

Capabilities and Affected Parties

The iOS variant contained a subset of the functionality the Android releases offered and did not have full capabilities to exploit a device. However, this version was still able to take advantage of Apple's certification process to appear legitimate and deploy on iOS devices to exfiltrate the following types of data:

Contacts | Photos | GPS Location | Audio Recordings | Videos | Device information

The software was discovered on phishing sites that imitated Italian and Turkmenistani mobile carriers, as well as in the Italian Play Store. It has since been removed from official Play store and Apple has revoked the appropriate certificates.

How Lookout Detects and Protects Against Threats like eSurvAgent

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. We classified the eSurvAgent as surveillanceware when it it started to use HTTPS pinning, asymmetric encryption used for C2 traffic tunneled through HTTPS, and GUIDs being used for all parts of API endpoint URLS and directory paths. Devices with Lookout installed have detected and alerted to eSurvAgent since March 2018. Lookout also protects against other sophisticated surveillanceware that could 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