Lookout Discovery - Monokle

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

Background and Timeline of Discovery

In 2018, Lookout came across the first sample of Monokle in the wild, and since then has carried out extensive research on the Android surveillanceware. Upon further research, the Lookout team realized that this surveillanceware had a shared signer with an Android antivirus solution called Defender, which is developed by Russian contractor firm Special Technology Centre (STC). STC is one of three Russian-based companies to be sanctioned by the Obama administration after being tied to providing material support for GRU's interference in the 2016 US Presidential election.

СПЕЦИАЛЬНЫЙ ТЕХНОЛОГИЧЕСКИЙ ЦЕНТР

Key Facts

1. Advanced surveillanceware developed by STC, which is sanctioned by the US government
2. Possesses remote access trojan (RAT) functionality. Uses advance data exfil techniques, and can install certificates
3. Appears as legitimate applications in order to hide malicious intent

Capabilities and Affected Parties

Monokle appears in a limited set of applications, which indicates that attacks leveraging the surveillanceware are highly targeted at particular individuals. Since the applications appear legitimate, despite being trojanized, the end user doesn't suspect that they are being attacked. We've seen this before with trojanized applications, Monokle has some functionality that Lookout researchers have never seen before.

In this case, Monokle's remote access trojan (RAT) functionality uses advanced data exfiltration techniques and has the ability to install an attack-specified certificate to the trusted certificates store on an infected device to facilitate a main-in-the-middle attack. It is also incredibly effective at exfiltrating data from third party apps without needing root access on the device, can use predictive-text dictionaries to understand the target's interests and create more curated attacks, and has the ability to record the device's screen during the unlock event and exfiltrate the device's unlock code.

How Lookout Detects and Protects Against Monokle

To protect against Monokle, Lookout customers can build application-based policies in the Lookout platform that will alert them to the trojanized applications and allow them to build in remediation tactics if there is a detection. Devices with Lookout installed have been protected against Monokle since early 2018, and Lookout will continue to research Monokle and update the market on its findings, as there is evidence of continued development on Android and expansion to iOS devices.

Click here to download the full technical report on Monokle

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.