Lookout Discovery – Chinese Surveillanceware

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

Background and Discovery Timeline

The Lookout Threat Intelligence team discovered four Android surveillanceware tools used to target the Uyghur ethnic minority group. Our research indicates these four interconnected malware tools are elements of much larger mAPT (mobile advanced persistent threat) campaigns that have been active since at least 2013. Lookout researchers have been monitoring the development and spread of the surveillanceware families - SilkBean, DoubleAgent, CarbonSteal and GoldenEagle - for years in order to protect customers against these sophisticated threats.

Key Findings

1. Development timeline aligns with Chinese national security directives.
2. Advanced mobile surveillanceware targeting users in at least 14 countries.
3. Languages targeted: Uyghur, Russian, English, Arabic, Chinese, Turkish, Pashto, Persian, Malay, Indonesian, Uzbek and Urdu/Hindi.

Capabilities and Affected Parties

The apps fall into four separate malware families, each of which has its own unique data gathering priorities and techniques. We named these families SilkBean, DoubleAgent, CarbonSteal and GoldenEagle. The primary goal is to gather intelligence to monitor individuals and use their sensitive data to establish a pattern of life for targets. Application titles and in-app functionality of the malware samples suggest the targets are the Uyghur Muslim ethnic minority group, centered in Xinjiang, China. However, these apps were present in at least 15 countries. Some apps and C2 domains appear to impersonate third-party Uyghur language app stores and focus on Uyghur-targeted apps and services. The development timeline and targeting of these families appear to align with Chinese national security directives and "counter-terrorism" efforts as defined by the Chinese government, perhaps suggesting a broader strategic goal behind the campaign.

How Lookout Detects and Protects Against Surveillanceware Campaigns

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. Devices with Lookout installed can detect and will alert users and Mobile Endpoint Security administrators to SilkBean, DoubleAgent, CarbonSteal and GoldenEagle. Lookout also protects against other sophisticated surveillanceware that could go undetected, allowing threat actors to gather sensitive corporate and personal data.

To learn more about the technical specifications of this campaign, including IOCs, read our blog or the full report here.

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 our security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Threat Advisory

© 2020 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, SCREAM®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. EVERYTHING IS OK®, LOOKOUT MOBILE SECURITY®, and PROTECTED BY LOOKOUT®, are registered trademarks of Lookout, Inc. in the United States. POWERED BY LOOKOUT™ is a trademark of Lookout, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.