



Spyware in the Enterprise



Overview

Researchers on the Lookout Threat Intelligence team recently discovered and disclosed an app-based surveillanceware tool dubbed *Hermit*. The team uncovered evidence of the spyware deployed in multiple countries: in Italy by Italian law enforcement, in northern Syria by an unknown actor and in Kazakhstan, likely by the Kazakh government. Hermit is developed by Italian-based RCS Lab, a spyware vendor that has a history of engaging governments with poor human rights records. The spyware can observe device data such as accounts, contacts, text messages, location, calendar, call logs, notifications, phone number and browser data. Hermit can also take pictures from the device's camera, record audio, steal files and run exploits to gain privileged access to all data.

How Lookout Protects Against Mobile Spyware and Surveillanceware

Lookout admins should make sure the default surveillanceware and device exploitation detection policies are turned on and set to block any infected device from internet access. In addition, enabling Phishing and Content Protection will protect both managed and BYOD devices against malicious payloads delivered via phishing links, which is typically how surveillanceware is initially deployed.

Lookout Analysis

While Hermit was only found to be used by nation states at this time, the core functionality exemplifies how mobile surveillanceware could adversely affect enterprise organizations. A threat actor could use mobile spyware like Hermit to target an employee, exploit their device and steal corporate data on that device. By recording audio or taking photos, the attacker could steal proprietary information or even use it to extort the employee and turn them into an insider threat.

Public reporting of the "lawful intercept" industry shows the increasing commercialization of mobile spyware. RCS Lab joins others, such as Gamma Group and Cytrox, that actively develop and sell surveillanceware. Despite claims that they only sell to organizations with legitimate use cases, their products have been used on innocent targets such as journalists, human rights activists and business executives. In fact, Lookout has observed Cytrox's Predator malware being used against devices at a large European manufacturer.

One of the most infamous examples is the NSO Group, which develops the widely known Pegasus surveillanceware. Considering NSO's financial difficulties and sanctions, there will be space at the top of the market for new players to emerge. As this commercialization continues, the goal of deploying this software could shift to broadly targeting organizations and their data.

Lookout Mobile Endpoint Detection and Response (EDR)

[Mobile EDR with Lookout Mobile Endpoint Security](#) grants access to the world's largest mobile security analysis dataset. This enables you to query the Lookout global dataset in the context of your mobile fleet to build proactive protection policies, improve your threat hunting workflow, and quickly identify how attackers leverage sophisticated campaigns to target your organization.