AbstractEmu

Mobile rooting malware found on Google Play, Amazon Appstore, and the Samsung Galaxy Store.

Key Findings

1. The malware uses rooting to gain privileged access to the device.
2. AbstractEmu exploits several vulnerabilities, including CVE-2020-0041which hadn't been knowingly exploited in the wild before.
3. In-depth technical analysis and IOCs are available here.

Background and Discovery Timeline

Researchers in the Lookout Threat Lab have discovered 19 applications, some with as many as 10,000 downloads, present in mobile app stores. The malware, dubbed AbstractEmu, uses code abstraction and anti-emulation checks to avoid running while under analysis. This helps minimize the chance that it will be uncovered.

Capabilities and Affected Parties

AbstractEmu leverages advanced evasion tactics and has a sophisticated code base, which indicates that the threat actor group behind it is well-resourced and has financial motivations. The malware can exploit several vulnerabilities to gain root access to the device. CVE-2020-0041 had not been previously exploited in the wild, CVE-2020-0069 is a vulnerability found in MediaTek chips which are used by dozens of smartphone manufacturers, then the AbstractEmu actors also modify publicly available code for other CVEs in order to add support for more targets.

Once the device is rooted, AbstractEmu exhibits behaviors similar to banking trojans that Lookout has discovered in the past. This includes the ability to gain permissions that enable them to phish login credentials and two-factor authentication tokens delivered by SMS. In addition, we observed more advanced capabilities such as enabling the threat actor to interact with other apps on the device and capturing content on the screen.

How Lookout Detects and Protects

Cybercriminals will try to use legitimate capabilities to obfuscate malicious activity. The true intentions of an app are oftentimes hidden in the data access permissions and behaviors, and even then, can be difficult to uncover without the right tools. Static and dynamic analysis of the industry's largest mobile dataset enables Lookout researchers to protect customers by continuously discovering and researching new threats. Devices with Lookout installed can detect and be alerted if AbstractEmu is present on the device.

To learn more about the technical specifications of this campaign, including IOCs, read the full article 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 its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

Click here to learn more about Threat Advisory