How Lookout Protects Against iOS Jailbreaking

Jailbroken devices pose security and compliance risks for companies

Security and Business Challenges

iOS jailbreaking has long been practiced by people who want to surpass traditional software restriction on Apple devices in order to do anything from installing certain apps to customizing the appearance of the device's interface. However, jailbreaking gives the user complete access to everything on the device and free reign to modify security and access settings as they would like.

Jailbreaks can also be a large compliance risk to a company as unauthorized modifications to iOS causes that device to fall out of compliance with internal and external parameters. In highly regulated industries such as finance, healthcare, and manufacturing, this can be detrimental to the growth and reputation of the company.

Notable Jailbreak: Checkm8 and Checkra1n

On September 27th, 2019, an independent iOS security researcher going by the Twitter handle axi0mX discovered checkm8. Described as "permanent unpatchable bootrom exploit" for any iOS device with an A5 chip (iPhone 4s/iPad 2) up to an A11 chip (iPhone X), this jailbreak could have massive security implications for anyone using devices with these chip versions. Then, on November 8th, checkra1n was released as a jailbreak that takes advantage of the checkm8 exploit. Lookout researchers immediately obtained and tested a sample of checkra1n - confirming coverage and detection of the jailbreak by Lookout Security Cloud.

Once the device is exploited an attacker can run any code on the device, including running a modified or outdated version of iOS that Apple no longer supports, and insert some sort of backdoor into that modified version. Since the jailbreak is hard-coded to the chip in the device, there is no way for Apple to patch this without issuing a massive recall of any affected devices, which would be roughly 84% of all active iOS devices.

Industry Challenges

1. Jailbreaking allows the user to customize their mobile experience
2. Jailbreaking the device creates massive security and compliance risk
3. Security teams don't have a way to block access for compromised devices

Lookout Critical Capability

Jailbroken devices open up a window of opportunity for malicious actors to take advantage of the device and exfiltrate large amounts of personal and corporate data. By detecting jailbreaks, Lookout can block access to corporate apps and infrastructure normally accessed by the device to ensure protection of the organization's assets and prevent a data breach. Continuous Conditional Access ensures that no compromised devices are touching company resources.

Why Lookout

Lookout Mobile Endpoint Security with Continuous Conditional Access ensures security and compliance on every device, leveraging a large data set fed by over 170 million devices and the analysis of over 70 million mobile apps. With the Lookout Security Cloud, it's easy to deploy Lookout and apply security policies across the entire organization for both managed and unmanaged devices. Users receive alerts and remediation steps on malicious apps, network connections, and system anomalies in real time; accompanied by dynamic device health checks to provide conditional access to sensitive corporate applications and data.